

INTRODUCTION TO ETHICAL HACKING

Unit Structure

- 1.0 Objectives.
- 1.1 Introduction.
- 1.2 What is ethical hacking?
- 1.3 Type of Hackers.
- 1.4 Difference between White Hacker & Black Hacker?.
- 1.5 Ethical Hacker Roles and Responsibilities.
- 1.6 Ethical Hacking Benefits.
- 1.7 Ethical Hacking Benefits.
- 1.8 Types of Hacking.
- 1.9 Advantages & Disadvantages of Hacking?
- 1.10 Code of Ethics.
- 1.11 Types of Attacks.
- 1.12 Types of Attack Vectors
- 1.13 Prevention from hackers.
- 1.14 Questions.
- 1.15 References.

1.0 OBJECTIVES-

- In Ethical Hacking to evaluate the security policies and identify vulnerabilities in target systems, networks or system infrastructure.
- The process entails finding and then attempting to exploit vulnerabilities to determine whether unauthorized access or other malicious activities are possible.
- Helping to prepare for a cyber attack.
- An ethical hacker needs deep technical expertise in infosec to recognize potential attack vectors that threaten business and operational data.
- Demonstrating methods used by cybercriminals.
- Describe the characteristics of Ethical Hacking & its methods.

1.1 INTRODUCTION-

Ethical Hacking/Hackers Also known as “white hats,” ethical hackers are security experts that perform these security assessments. The proactive work they do helps to improve an organization’s security posture. With prior approval from the organization or owner of the IT asset, the mission of ethical hacking is opposite from malicious hacking.

1.2 WHAT IS ETHICAL HACKING. A)DEFINITION:

The term ‘Hacker’ was coined to describe experts who used their skills to re-develop mainframe systems, increasing their efficiency and allowing them to multi-task. Nowadays, the term routinely describes skilled programmers who gain unauthorized access into computer systems by exploiting weaknesses or using bugs, motivated either by malice or mischief.

For example, a hacker can create algorithms to crack passwords, penetrate networks, or even disrupt network services.

The primary motive of malicious/unethical hacking involves stealing valuable information or financial gain. However, not all hacking is bad. This brings us to the second type of hacking:

Ethical hacking.

So what is ethical hacking, and why do we need it? And in this article, you will learn all about what is ethical hacking and more.

B) Definition:

Ethical Hacking is an authorized practice of bypassing system security to identify potential data breaches and threats in a network. The company that owns the system or network allows Cyber Security engineers to perform such activities in order to test the system’s defenses. Thus, unlike malicious hacking, this process is planned, approved, and more importantly, legal.

Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They collect and analyze the information to figure out ways to strengthen the security of the system/network/applications. By doing so, they can improve the security footprint so that it can better withstand attacks or divert them.

Ethical hackers are hired by organizations to look into the vulnerabilities of their systems and networks and develop solutions to prevent data breaches. Consider it a high-tech permutation of the

old saying “It takes a thief to catch a thief.”

- **They check for key vulnerabilities include but are not limited to:**
- Injection attacks
- Changes in security settings
- Exposure of sensitive data
- Breach in authentication protocols
- Components used in the system or network that may be used as access points

Now, as you have an idea of what is ethical hacking, it's time to learn the type of hackers.

1.3 TYPE OF HACKERS:

Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system. These different terms come from old Spaghetti Westerns, where the bad guy wears a black cowboy hat and the good guy wears a white hat.

1) **White Hat Hackers:**

White Hat hackers are also known as Ethical Hackers. They never intent to harm a system, rather they try to find weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments.

Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

2) **Black Hat Hackers:**

Black Hat hackers, also known as crackers, are those who hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information.

Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

3) **Grey Hat Hackers:**

Grey hat hackers are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner's permission or knowledge.

Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

- **Miscellaneous Hackers**

Apart from the above well-known classes of hackers, we have the following categories of hackers based on what they hack and how they do it –

1) Red Hat Hackers:

Red hat hackers are again a blend of both black hat and white hat hackers. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.

2) Blue Hat Hackers:

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch. They look for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term BlueHat to represent a series of security briefing events.

3) Elite Hackers:

This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

- White Hat vs Black Hat Hacker :**

The best way to differentiate between White Hat and Black Hat hackers is by taking a look at their motives. Black Hat hackers are motivated by malicious intent, manifested by personal gains, profit, or harassment; whereas White Hat hackers seek out and remedy vulnerabilities, so as to prevent Black Hats from taking advantage.

1.4 DIFFERENCE BETWEEN WHITE HAT AND BLACK HAT:

Black Hat Hackers	White Hat Hackers
Their intentions are selfish or harmful in nature.	Their intentions are noble and often aim to benefit or protect others.
Hacking done by black hat hackers is illegal.	Hacking done by white hat hackers is legal.
They infiltrate or control websites, devices, or other systems without permission of the owner/ authorization.	They penetrate the system with the owner's permission. Government agencies and other organizations hire white hats to test the software/devices and carry out non-harmful cyber attacks to find gaps in their security.
Search for the security vulnerabilities to exploit them.	They search for security vulnerabilities and offer suggestions and solutions to patch them.

Write malware to hack devices, servers, and websites.	Develop security software, tools, and techniques to detect and remove malware.
Take advantage of users' lack of awareness about cyber threats to manipulate or defraud them with various phishing techniques.	Educate people about cybersecurity threats and risks, as well as ways to mitigate them.
Deploy ransomware and spyware attacks to blackmail individuals/organizations.	Develop tools and contingency plans to help people deal with ransomware and spyware attacks without paying extortion money.
Steal confidential data that they can use for cybercrime activities or sell to other attackers on the dark web.	Aim to help companies protect sensitive data by strengthening their cyber defenses.
Some countries' governments employ them to deploy cyber attacks, steal confidential data, espionage, and cause political unrest in their enemy countries. These are known as nation-state actors.	Many local, state and national governments employ white hats to protect their servers, websites, databases, and other IT infrastructure.

1.5 ETHICAL HACKER ROLES AND RESPONSIBILITIES:

Ethical Hackers must follow certain guidelines in order to perform hacking legally. A good hacker knows his or her responsibility and adheres to all of the ethical guidelines. Here are the most important rules of Ethical Hacking:

- An ethical hacker must seek authorization from the organization that owns the system. Hackers should obtain complete approval before performing any security assessment on the system or network.
- Determine the scope of their assessment and make known their plan to the organization.
- Report any security breaches and vulnerabilities found in the system or network.
- Keep their discoveries confidential. As their purpose is to secure the system or network, ethical hackers should agree to and respect their non-disclosure agreement.
- Erase all traces of the hack after checking the system for any vulnerability. It prevents malicious hackers from entering the system through the identified loopholes.

1.6 ETHICAL HACKING BENEFITS:

Learning ethical hacking involves studying the mindset and techniques of black hat hackers and testers to learn how to identify and correct vulnerabilities within networks. Studying ethical hacking can be applied by security pros across industries and in a multitude of sectors. This sphere includes network defender, risk management, and quality assurance tester.

However, the most obvious benefit of learning ethical hacking is its potential to inform and improve and defend corporate networks. The primary threat to any organization's security is a hacker: learning, understanding, and implementing how hackers operate can help network defenders prioritize potential risks and learn how to remediate them best. Additionally, getting ethical hacking training or certifications can benefit those who are seeking a new role in the security realm or those wanting to demonstrate skills and quality to their organization.

You understood what is ethical hacking, and the various roles and responsibilities of an ethical hacker, and you must be thinking about what skills you require to become an ethical hacker. So, let's have a look at some of the ethical hacker skills.

1.7 SKILLS REQUIRED TO BECOME AN ETHICAL HACKER:

An ethical hacker should have in-depth knowledge about all the systems, networks, program codes, security measures, etc. to perform hacking efficiently. Some of these skills include:

- Knowledge of programming - It is required for security professionals working in the field of application security and Software Development Life Cycle (SDLC).
- Scripting knowledge - This is required for professionals dealing with network-based attacks and host-based attacks.
- Networking skills - This skill is important because threats mostly originate from networks. You should know about all of the devices present in the network, how they are connected, and how to identify if they are compromised.
- Understanding of databases - Attacks are mostly targeted at databases. Knowledge of database management systems such as SQL will help you to effectively inspect operations carried out in databases.
- Knowledge of multiple platforms like Windows, Linux, Unix, etc.
- The ability to work with different hacking tools available in the market.
- Knowledge of search engines and servers.

1.8 TYPES OF HACKING:

We can segregate hacking into different categories, based on what is being hacked. Here is a set of examples –

1. **Website Hacking** – Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
2. **Network Hacking** – Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.
3. **Email Hacking** – It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.
4. **Ethical Hacking** – Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.
5. **Password Hacking** – This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
6. **Computer Hacking** – This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

1.9 ADVANTAGES & DISADVANTAGES OF HACKING:

- **Advantages of Hacking**
 1. To recover lost information, especially in case you lost your password.
 2. To perform penetration testing to strengthen computer and network security.
 3. To put adequate preventative measures in place to prevent security breaches.
 4. To have a computer system that prevents malicious hackers from gaining access.
- **Disadvantages of Hacking**
 1. Hacking is quite dangerous if it is done with harmful intent. It can cause –
 2. Massive security breach.
 3. Unauthorized system access on private information.
 4. Privacy violation.
 5. Hampering system operation.
 6. Denial of service attacks.
 7. Malicious attack on the system.

1.10 CODE OF ETHICS:

Now computer security training organizations have an ethical code of conduct that people must agree to abide by in order to be certified by them. The most popular hacker code of ethics on the

Internet is the EC-Council Code of Ethics.

It's a good code of ethics, but a bit too focused on penetration testing, and it's growing a bit long over time. This chapter provides a solid, concise code of ethics to operate by, both personally and professionally.

Hackers: Heroes of the Computer Revolution, introduced the world to one of the earliest versions of hacker ethics. Levy was sharing, not necessarily agreeing with, what many hackers felt about the early days of hacking.

1.11 TYPES OF ATTACKS:

1) Malware:

If you've ever seen an antivirus alert pop up on your screen, or if you've mistakenly clicked a malicious email attachment, then you've had a close call with malware. Attackers love to use malware to gain a foothold in users' computers—and, consequently, the offices they work in—because it can be so effective.

“Malware” refers to various forms of harmful software, such as viruses and ransomware. Once malware is in your computer, it can wreak all sorts of havoc, from taking control of your machine, to monitoring your actions and keystrokes, to silently sending all sorts of confidential data from your computer or network to the attacker's home base.

Attackers will use a variety of methods to get malware into your computer, but at some stage it often requires the user to take an action to install the malware. This can include clicking a link to download a file, or opening an attachment that may look harmless (like a Word document or PDF attachment), but actually has a malware installer hidden within.



Fig: Process of Malware Attack

2) Phishing:

Of course, chances are you wouldn't just open a random attachment or click on a link in any email that comes your way—there has to be a compelling reason for you to take action. Attackers know this, too. When an attacker wants you to install malware or divulge sensitive information, they often turn to phishing tactics, or pretending to be someone or something else to get you to take an action you normally wouldn't. Since they rely on human curiosity and impulses, phishing attacks can be difficult to stop.

In a phishing attack, an attacker may send you an email that appears to be from someone you trust, like your boss or a company you do business with. The email will seem legitimate, and it will have some urgency to it (e.g. fraudulent activity has been detected on your account). In the email, there will be an attachment to open or a link to click. Upon opening the malicious attachment, you'll thereby install malware in your computer.

If you click the link, it may send you to a legitimate-looking website that asks for you to log in to access an important file—except the website is actually a trap used to capture your credentials when you try to log in.

In order to combat phishing attempts, understanding the importance of verifying email senders and attachments/links is essential.



Fig: Process of Phishing Attack.

3) SQL Injection Attack:

SQL (pronounced “sequel”) stands for structured query language; it’s a programming language used to communicate with databases. Many of the servers that store critical data for websites and services use SQL to manage the data in their databases.

A SQL injection attack specifically targets this kind of server, using malicious code to get the server to divulge information it normally wouldn’t. This is especially problematic if the server stores private customer information from the website, such as credit card numbers, usernames and passwords (credentials), or other personally identifiable information, which are tempting and lucrative targets for an attacker.

An SQL injection attack works by exploiting any one of the known SQL vulnerabilities that allow the SQL server to run malicious code. For example, if a SQL server is vulnerable to an injection attack, it may be possible for an attacker to go to a website's search box and type in code that would force the site's SQL server to dump all of its stored usernames and passwords for the site.



Fig: Process of SQL Injection Attack

4) Cross-Site Scripting (XSS):

In an SQL injection attack, an attacker goes after a vulnerable website to target its stored data, such as user credentials or sensitive financial data. But if the attacker would rather directly target a website's users, they may opt for a cross-site scripting attack.

Similar to an SQL injection attack, this attack also involves injecting malicious code into a website, but in this case the website itself is not being attacked. Instead, the malicious code the attacker has injected only runs in the user's browser when they visit the attacked website, and it goes after the visitor directly, not the website.

One of the most common ways an attacker can deploy a cross-site scripting attack is by injecting malicious code into a comment or a script that could automatically run. For example, they could embed a link to a malicious JavaScript in a comment on a blog.

Cross-site scripting attacks can significantly damage a website's reputation by placing the users' information at risk without any indication that anything malicious even occurred. Any sensitive information a user sends to the site—such as their credentials, credit card information, or other private data—can be hijacked via cross-site scripting without the website owners realizing there was even a problem in the first place.

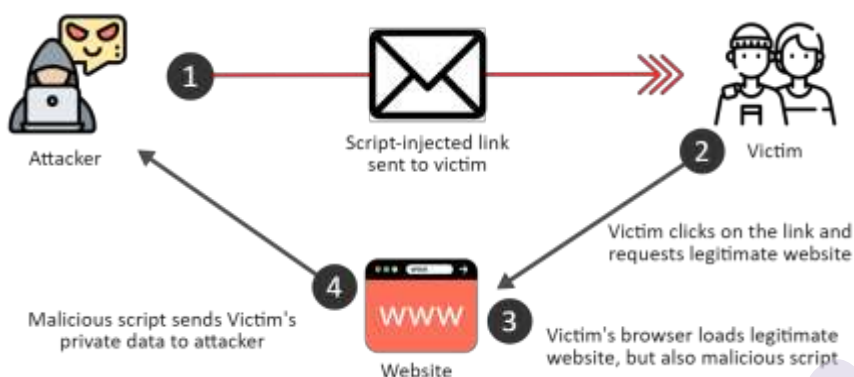


Fig: Process of Cross-Site Scripting (XSS)

5) Denial-of-Service (DoS):

Imagine you're sitting in traffic on a one-lane country road, with cars backed up as far as the eye can see. Normally this road never sees more than a car or two, but a county fair and a major sporting event have ended around the same time, and this road is the only way for visitors to leave town. The road can't handle the massive amount of traffic, and as a result it gets so backed up that pretty much no one can leave.

That's essentially what happens to a website during a denial-of-service (DoS) attack. If you flood a website with more traffic than it was built to handle, you'll overload the website's server and it'll be nigh-impossible for the website to serve up its content to visitors who are trying to access it.

This can happen for innocuous reasons of course, say if a massive news story breaks and a newspaper's website gets overloaded with traffic from people trying to find out more. But often, this kind of traffic overload is malicious, as an attacker floods a website with an overwhelming amount of traffic to essentially shut it down for all users.

In some instances, these DoS attacks are performed by many computers at the same time. This scenario of attack is known as a Distributed Denial-of-Service Attack (DDoS).

This type of attack can be even more difficult to overcome due to the attacker appearing from many different IP addresses around the world simultaneously, making determining the source of the attack even more difficult for network administrators.

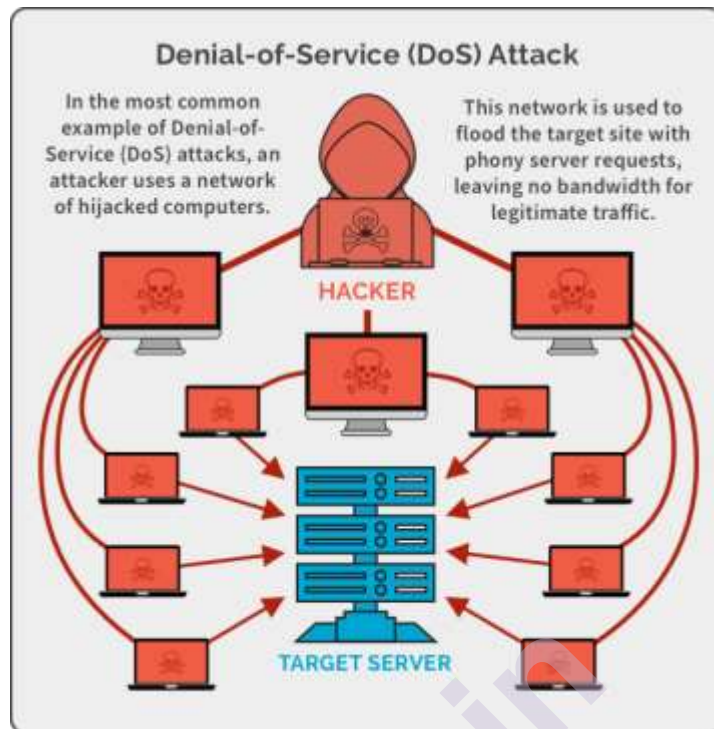


Fig: Process of Denial-of-Service (DoS).

6) Session Hijacking and Man-in-the-Middle Attacks:

When you're on the internet, your computer has a lot of small back-and-forth transactions with servers around the world letting them know who you are and requesting specific websites or services. In return, if everything goes as it should, the web servers should respond to your request by giving you the information you're accessing.

This process, or session, happens whether you are simply browsing or when you are logging into a website with your username and password.

The session between your computer and the remote web server is given a unique session ID, which should stay private between the two parties; however, an attacker can hijack the session by capturing the session ID and posing as the computer making a request, allowing them to log in as an unsuspecting user and gain access to unauthorized information on the web server. There are a number of methods an attacker can use to steal the session ID, such as a cross-site scripting attack used to hijack session IDs.

An attacker can also opt to hijack the session to insert themselves between the requesting computer and the remote server, pretending to be the other party in the session. This allows them to intercept information in both directions and is commonly called a man-in-the-middle attack.

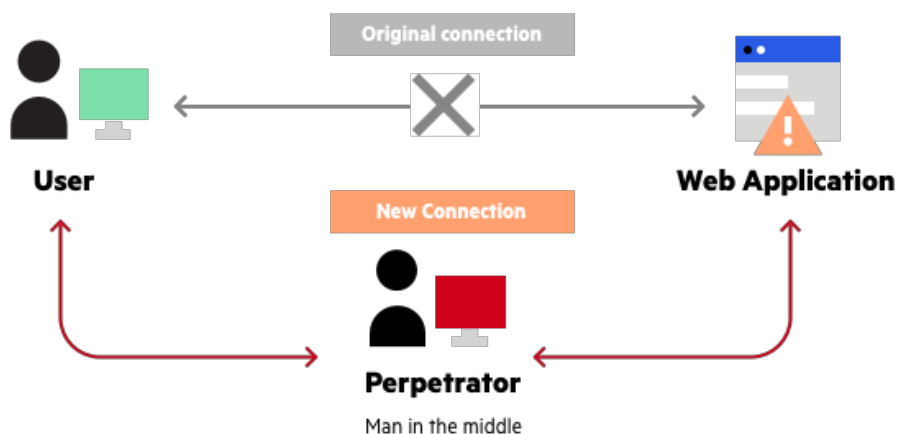


Fig: Process of Session Hijacking and Man-in-the-Middle Attacks.

7) Credential Reuse:

Users today have so many logins and passwords to remember that it's tempting to reuse credentials here or there to make life a little easier. Even though security best practices universally recommend that you have unique passwords for all your applications and websites, many people still reuse their passwords—a fact attackers rely on.

Once attackers have a collection of usernames and passwords from a breached website or service (easily acquired on any number of black market websites on the internet), they know that if they use these same credentials on other websites there's a chance they'll be able to log in.

No matter how tempting it may be to reuse credentials for your email, bank account, and your favorite sports forum, it's possible that one day the forum will get hacked, giving an attacker easy access to your email and bank account. When it comes to credentials, variety is essential. Password managers are available and can be helpful when it comes to managing the various credentials you use.

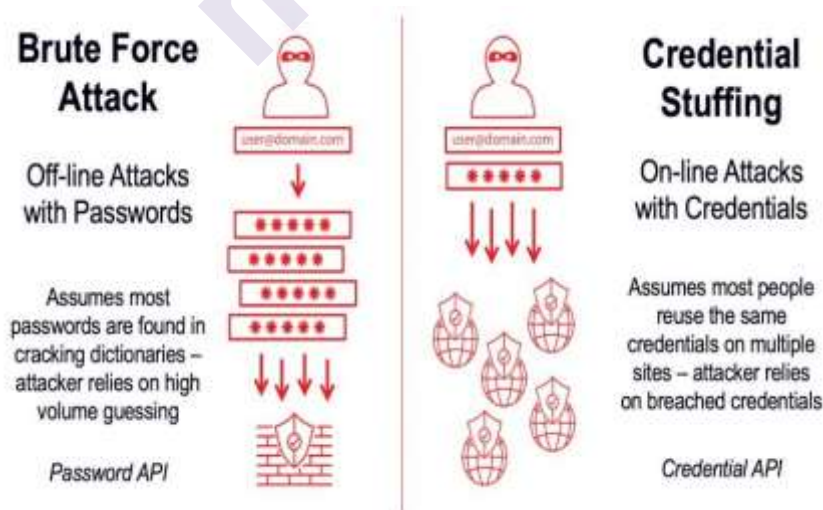


Fig: Process of Credential Reuse.

1.12 TYPES OF ATTACK VECTORS:

1. **Compromised Credentials**

Username and passwords are still the most common type of access credential and continue to be exposed in data leaks, phishing scams and by malware. When lost, stolen or exposed, credentials give attackers unfettered access. This is why organizations are now investing in tools to continuously monitor for data exposures and leaked credentials. Password managers, two-factor authentication and biometrics can reduce the risk of leak credentials resulting in a security incident too.

2. **Weak Credentials**

Weak passwords and reused passwords mean one data breach can result in many more. Teach your organization how to create a secure password, invest in a password manager or a single sign-on tool, and educate staff on their benefits.

3. **Malicious Insiders**

Disgruntled employees can expose private information or provide information about company specific vulnerabilities.

4. **Missing or Poor Encryption**

Common encryption methods like SSL certificates and DNSSEC can prevent man-in-the-middle attacks and protect the confidentiality of data being transmitted. Missing or poor encryption for data at rest can mean that sensitive data or credentials are exposed in the event of a data breach or data leak.

5. **Misconfiguration**

Misconfiguration of cloud services, like Google Cloud Platform, Microsoft Azure, or AWS, or using default credentials can lead to data breaches and data leaks, check your S3 permissions or someone else will. Automate configuration management where possible to prevent configuration drift.

6. **Ransomware**

Ransomware is a form of extortion where data is deleted or encrypted unless a ransom is paid, such as WannaCry. Minimize the impact of ransomware attacks by maintaining a defense plan, including keeping your systems patched and backing up important data.

7. **Phishing**

Phishing is a social engineering technique where the target is contacted by email, telephone or text message by someone who is posing to be a legitimate colleague or institution to trick them into

providing sensitive data, credentials or personally identifiable information (PII). To minimize phishing, educate your staff on the importance of cybersecurity and prevent email spoofing and typosquatting.

8. Vulnerabilities

New vulnerabilities are added to CVE every day and zero-day vulnerabilities are found just as often. If a developer has not released a patch for a zero-day vulnerability before an attack can exploit it, it can be hard to prevent.

9. Brute Force

Brute force attacks are based on trial and error. Attackers may continuously try to gain access to your organization until one attack works. This could be by attacking weak passwords or encryption, phishing emails or sending infected email attachments containing a type of malware. Read our full post on brute force attacks.

10. Distributed Denial of Service (DDoS)

DDoS are cyber attacks against networked resources like data centers, servers or websites and can limit the availability of a computer system. The attacker floods the network resource with messages which cause it to slow down or even crash, making it inaccessible to users. Potential mitigations include CDNs and proxies.

11. SQL Injections

SQL stands for structured query language, a programming language used to communicate with databases. Many of the servers that store sensitive data use SQL to manage the data in their database. An SQL injection uses malicious SQL to get the server to expose information it otherwise wouldn't. This is a huge cyber risk if the database stores customer information, credit card numbers, credentials or other personally identifiable information (PII).

12. Trojans

Trojan horses are malware that misleads users by pretending to be a legitimate program and are often spread via infected email attachments or fake software.

13. Cross-Site Scripting (XSS)

XSS attacks involve injecting malicious code into a website but the website itself is not being attacked, rather it aims to impact the website's visitors. A common way attackers can deploy cross-site scripting attacks is by injecting malicious code into a comment e.g. embed a link to malicious JavaScript in a blog post's comment section.

14. Session Hijacking

When you log into a service, it generally provides your computer with a session key or cookie so you don't need to log in again. This cookie can be hijacked by an attacker who uses it to gain access to sensitive information.

15. Man-in-the-Middle Attacks

Public Wi-Fi networks can be exploited to perform man-in-the-middle attacks and intercept traffic that was supposed to go elsewhere, such as when you log into a secure system.

16. Third and Fourth-Party Vendors

The rise in outsourcing means that your vendors pose a huge cybersecurity risk to your customer's data and your proprietary data. Some of the biggest data breaches were caused by third parties.

1.13 PREVENTION FROM HACKERS:

“how to prevent being hacked,” use some security software or tweak the security settings to prevent hacking. But most importantly, you need to recognize the psychological games attackers play to make you take actions that you shouldn't.

This includes everything from sharing your personal or financial information to downloading and installing malware-infected files/software.

In this article, we'll cover 15 tips to help you understand how to prevent being hacked. We'll also link to “freemium” tools that you can use to prevent hacking.

- **15 Tips to Prevent Hacking**

You don't require a lot of technical expertise to prevent hacking. These are some super easy and yet, efficient ways by which you can avoid hacking.

1. Encrypt Files While Storing and Transferring:

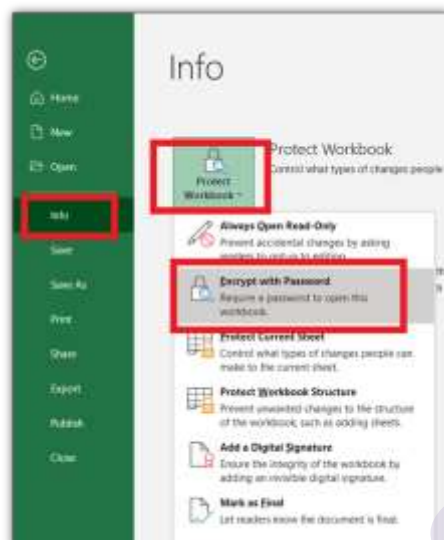
When you're sharing any important Microsoft files with anyone or storing them on your device, USB, or cloud platform, always encrypt them.

Encryption means using mathematical algorithms to “lock” the data with a cryptographic key. Encryption scrambles plaintext data and makes it incomprehensible to protect it from unintended parties without an authentication key.

So that, even if someone gets access to those files, they can't open and read them. All Microsoft files (such as Word, Excel, Access, PowerPoint) have this option.

For example, to encrypt a file in Excel:

- Click on **File** from the upper left corner.
- Select **Info**.
- Click on **Protect Workbook** (or Protect Document, Presentation, etc., as per the file type).
- Select **Encrypt with Password**.



Screenshot from Microsoft Excel showing how to prevent hacking by encrypting the documents

Once you set the password, anyone who wants to access this file would require this password. When you send such a protected file to anyone, be sure to provide the recipient the password via phone, a separate email, or any other communication channel.

- **Use These Tools to Encrypt Any Other Types of Files/Folders**

There are some commercial and “freemium” tools that can help you to enable encryption for any type of files, folders, drives, and documents. Some examples include:

- Folderlock
- VeraCrypt
- 7-Zip
- DiskCryptor
- AxCrypt

2. Use Browser Extensions to Block Malicious Sites and Harmful Downloads:

There are some free browser extensions that maintain a list of malicious and phishing sites and block them. To use them,

you'd need to install these extensions ("add-ons" for Firefox) on your browser to keep the attackers at bay and prevent hacking. These are some well-known free extensions and add-ons:

- Online Security Pro by Comodo
- Anti-Malware Subzero
- Adblocker
- Malwarebytes Browser Guard
- Avira Browser Safety
- Bitdefender TrafficLight

We have already provided the links here. You just need to click on **Add to Chrome** or **Add to Firefox**.

3. Install a Strong Anti-Malware Program:

Although this one is pretty obvious, some people still need a gentle reminder to use antivirus and anti-malware programs. These types of security software regularly scan your device and remove dangerous malware.

They also alert you when you visit a spammy or malicious website or if you download a corrupted file from the internet.

While choosing an antivirus program, be sure to get it from a reputable company only.

Beware of scareware: If you get a random email or see a popup indicating that your PC is infected, it might be scareware.

Scareware is rough antivirus software that can be a virus itself or works as spyware to monitor your actions.

Never click on these links or ads, nor should you install unknown security software. We recommend Comodo Antivirus. It's a highly reputable brand and offers **free and paid versions**.

4. Sanitize Your PC Manually:

There are some advanced types of malware that a firewall/security software can't detect. That's why it is advisable to keep an eye on your device manually to prevent hacking.

Regularly check your C: drive, especially folders like **C:/Program File, C:/Program Files (x86)**, and all the **TEMP** folders.

Also, keep an eye on the **Download** folder. If you find any unusual items that you haven't downloaded, perform an internet search to learn about them. Delete the files if they don't serve any purpose or are linked to malicious activity.

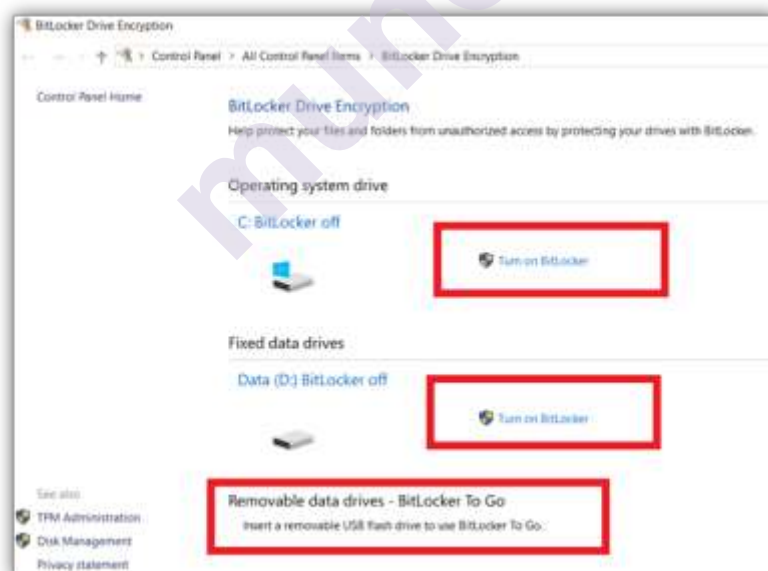
Some malware programs are so stubborn that you won't be able to delete them with regular deleting steps. The good news is, there are some free file shredder and uninstaller programs that can help you to uninstall such programs. Some of these programs are so efficient that they deep scan your device and delete all the hidden traces like cache and shortcuts.

5. Enable Encryption Using BitLocker for Windows 10:

This feature will encrypt your hard drive. If your Windows computer is stolen or you sell it without wiping the memory (note: always wipe the memory first before selling a device!), no one can hack you by stealing data from the hard drive. It also has an encryption facility for the USB drive.

To enable encryption:

- Search **BitLocker** in the Windows search bar and select **Manage BitLocker** • Click on **Turn on BitLocker** for your C: drive, D: drive, and USB.
- You will need the administrator's credentials (if not logged in as admin already)



A screenshot showing how to lock C: and D: drives and removable data drives using BitLocker to prevent hacking

For Mac Users: FileVault provides a similar function as BitLocker. Please follow this resource:

Step-by-step guide to enable FileVault.

6. **Enable Two-Factor Authentication (2FA):**

2FA adds another layer of security along with your traditional passwords. You'll get a unique one-time password (OTP), secret code, or a magic link on your registered mobile number or email address every time you log in to your account or make a transaction. If any of your bank, credit card companies or any other service providers allow you to enable 2FA, do so immediately!

You can also enable 2FA on the cellphone by installing free third-party apps like:

- Google Authenticator,
- Microsoft Authenticator,
- Twilio Authy 2-Factor Authentication

After installation, you'll get the option to enable 2FA for all other apps stored on your mobile that support 2FA. Make sure you enable it for eCommerce sites, cloud storage platforms, and financial platforms.

7. **Don't Log in Via Existing Third-Party Platforms:**

Next on our list for how to prevent hacking: don't link accounts. When you want to sign into a new platform, you may see an option to sign in using your existing accounts like Facebook, Gmail, LinkedIn, etc. Don't use these options. Instead, use your email address or phone number or manually complete the login form (don't be lazy here).

Why? When you sign in/log in using any of these existing accounts, the new app/website can access some information about you stored on such platforms.

Such data sharing can be dangerous if the new app/platform owner or employee has malicious intentions. They can steal such data to hack you or sell it in the dark market to other hackers. Even well-known platforms misuse users' data for creating targeted advertising.

For example, Zoom faced allegations that it shares (or sells) users' data to Facebook. Zoom admitted that such data leaks happened because it gave users the option of logging in to Zoom via a Facebook software development kit (SDK).

8. **Don't Share Any Information via HTTP Sites:**

When you open a website, look at the address bar. If you see "Not secure" or an exclamation sign in a round or triangle, it indicates that the site is running on HTTP, which is an insecure protocol. This means that any sensitive data that transmits

between your browser and the website's server remains unencrypted, which makes it easy for hackers to steal your personal and financial information.

So, a good rule of thumb is to only share information with websites that have a padlock symbol in front of their domain names in the address bar.

This indicates that the website owner has installed an SSL/TLS certificate, and all the data communicated between your browser and the website's server remains encrypted.

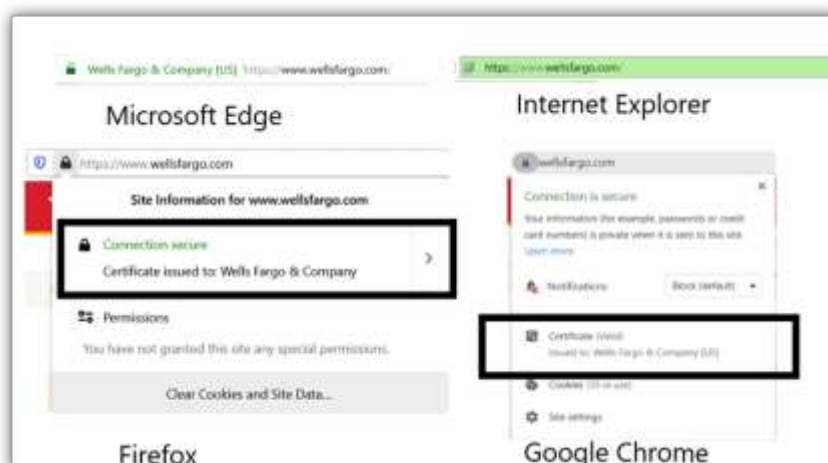


The image is showing how a website with and without an SSL certificate looks like. However, just because a site has a padlock sign doesn't mean it's safe.

A cybercriminal can use a free SSL/TLS certificate on their fake website, too. And then you're using a secure connection, but you're still left with the uncertainty of knowing to whom you are connected on the other end.

The solution is to click on the padlock sign and check out the "issued to" field. If the website has installed an extended validated (EV) SSL certificate, you will be able to see its legal name in front of the "issued to" information.

You'll see the company's name in green colour or with a green address bar in some browsers. Most reputable and legitimate companies use EV SSL certificates, which require a rigorous identity verification process.



An image showing how an EV SSL certificate provides an extra layer of authenticity to prevent hacking and phishing.

9. Recognize Signs of Fake or Malware-Infected Websites:

landed on a website and are not sure whether to trust it. You should look for a few specific things when evaluating any website to prevent hacking as a site visitor.

Here are several signs that a website is fake, risky, spammy, malicious, or “phishy”:

- Too many redirects to unknown, irrelevant, or advertising sites.
- Something downloads onto your device automatically (and without your permission).
- Many different “downloads” or “play” buttons for the content.
- You notice multiple screens or popup windows in the background even if you haven’t opened them.
- The site is claiming unrealistic results of any product or offering “too good to be true” deals and discounts.
- There are many spelling and grammatical mistakes on the site.
- The website is trying to create a sense of urgency and urges you to take any immediate steps.
- The site announces that you have won the big prize in the casino, lucky draw, or games in which you haven’t participated. (Sometimes, you will be asked to take part in some easy game, spin the lucky draw wheel, answer easy questions, etc. But keep in mind that no one there to give you a penny for free, let alone big prizes.)

Beware of Cybersquatting Sites

Some people buy domain names that look similar to popular domain names and have just slight variations in the spelling or top-level domains. This is known as cybersquatting or typosquatting, depending on the specific instance.

For example:

- Amzon.com (instead of amazon.com),
- Goggle.com (instead of google.com),
- Dictionery.com (instead of dictionary.com),
- Facebok.com (instead of facebook.com),
- Linkdin.com (instead of linkedin.com), and
- Insiderbusiness.com (instead of businessinsider.com)

So, be careful while typing a domain name in the address bar. When you share your personal or financial information, check the address bar again to make sure you are on the right site.

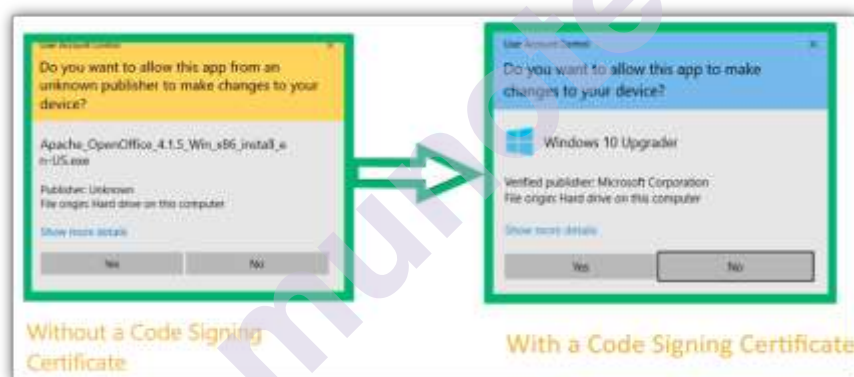
10. Learn to Recognize Fake vs. Legitimate Software and Applications:

When you install software on your device, you permit it to make changes to your device and access data. It is a dangerous step because if the developer has bad intentions or the software contains malware, you're doomed!

When you're downloading software, check out the **publisher's name in the security window**.

If you see the publisher's name as **Unknown**, beware! This indicates that the software's integrity is not vouched for and protected by a code signing certificate. It also tells you that the developer's identity hasn't been verified by a third-party certificate authority (CA).

Legitimate developers and publishers use code signing certificates. If you haven't heard the publisher's name before, conduct a quick internet search and read the reviews.



A side-by-side example of Windows security messages that show the difference between an unverified publisher warning vs. a verified publisher message.

11. Recognize Phishing Emails:

FireEye reports that one in every 101 emails is malicious! Attackers spread malware via email attachments or redirect you to some infected sites. Some cybercriminals try to manipulate you into sharing personal information psychologically.

Luckily, there are a few things you can look out for that will help you to avoid falling victim to phishing schemes:

1. **Carefully check the sender's email address.** If it is unusual or too long, be cautious! Also, if someone is

claiming to be an employee of a well-known organization, their email address will have the company's domain name after "@." For example, "@apple.com, @amazon.com, @wellsfargo.com, etc.

Their messages won't come from a generic email client like Gmail, Hotmail, Yahoo, AOL, etc.

2. **Don't ignore spelling, punctuation, and grammatical errors.** Good companies have strict editorial standards. It's uncommon for them to send an official email with many errors. So, if you see such errors, be on alert because it's likely a scam.
3. **Is the email trying to provoke any strong emotional response from you?** For example, an attacker might want to generate panic in you by sending any fake transaction notice in the hope that you will open the attachment to investigate it. Or they might offer you a great discount on a product/service, hoping that you would click on the link provided in the email in excitement to avail of the deal.

Recognizing a phishing email is the very first and essential step to prevent hacking. If you receive such an email, just delete it.

Don't download anything from it or click any links — and *never* share your personal information in a reply message! If you think the message is legit, go to the original company's site to verify the given deal, offer, transaction history, donation drive, news, claims, etc.

If the sender is claiming to be someone you know, contact them personally to verify the message before taking any actions suggested in the email.

12. **Be Vigilant While Downloading Anything from the Internet:**

It's a common practice to spread viruses and other types of malware via:

- Email attachments
- Advertisements (known as malvertisements)
- Fake software, programs, and apps
- Media files like songs, images, videos, and slideshows
- Social media attachments
- SMS/WhatsApp messages

As we mentioned before, if there are too many "downloads" buttons placed in a deceiving manner, it is also a red flag.

The malware-laden emails, advertisements, or pop ups will try to catch your attention by:

- Showing a sense of urgency.
- Generating a surprise element or curiosity.
- Inciting feelings of curiosity, fear, or panic.

Examples of these types of messages include:

- *“Your account has been suspended due to rules violation. Attached is a document for more information about the violation.”*
- *“Your PC is infected with viruses. Click here to get free scanning.”*
- *“Your order has been shipped from xyz.com (any well-known ecommerce site). Attached is your transaction receipt.”* (When you haven’t placed the order, you may feel curious and tempted to download the attachment to see the transaction details — don’t do this)
- *“\$5,000 has debited from your bank account today. If you haven’t done this transaction, click on this link or download the transaction receipt.”* (If you haven’t made that transaction,
- If you spot a fake email or website, don’t download anything from it. But even if you trust the email sender or the website, always scan the downloads with a robust antivirus program before downloading.

After all, it’s possible that the legitimate organization’s or person’s email account or the site may be compromised.

13. Beware of Phishing SMS Messages:

Hackers send SMS phishing (smishing) messages to defraud people. These fake SMS text messages might offer you a free product or a great discount on your favorite brands.

They might generate panic by sending messages of a fake financial transaction. Attackers also pretend to be your friends/relatives and ask you to send them money immediately.

Such fake SMS messages generally contain links that redirect users to infected sites or phishing sites. Some links enable automatically downloading malware onto your mobile device as soon as you click on them.

Otherwise, the attacker may try to manipulate you into sharing your personal or financial information in a reply message. In short, they will use the same tactics in SMS text messages as they do in phishing emails.

Some tools make it possible for attackers to send you messages pretending to be someone else. Whenever you receive such a message, don't click on the link given in the SMS. Rather, go to the original website to confirm the deal's legitimacy, discount, offer, transaction, etc.

Also, call directly to the friend/relative to confirm whether they sent the message. If you suspect a phishing or fake SMS, block the sender ASAP.

14. Don't Jailbreak Your Devices:

People generally jailbreak their phones or other devices to access banned apps, change service providers, or change the phone's layout and settings.

But jailbreaking (rooting for android) is not a great idea if you want to avoid hacking! When you jailbreak your phone, you unknowingly disable some of the phone manufacturers' default security features.

when you use jailbreaking tools or software, you're giving administrator-level powers to app developers whose intentions are unknown. They can not only access all your data but can also make unauthorized changes in the device's settings.

In short, when you jailbreak your phone, you severely weaken your device's security posture.

Hence, to keep hackers away, refrain from jailbreaking your device.

15. Additional Tips on How to Prevent Being Hacked:

Alright, we're on to the last tip for how to prevent hacking. These are some simple yet important tips to prevent hacking.

- Keep your device, software, operating system, and apps updated with the latest versions.
- Never share your login credentials, one-time passwords (OTP), or other account-related information with anyone.
- Don't use public Wi-Fi. If you must, use a VPN to prevent anyone from identifying or intercepting your device's identity and data transmissions.
- Use haveibeenpwned.com to find out whether your password is compromised in any data breach incidents.
- Store your backup on the third-party cloud platform to keep it more secure.

- Regularly run antivirus software checks. If you suddenly started to see ad popups or security warning popups, your device might be infected with adware or a potentially unwanted program (PUP). Scan your device with a robust anti-malware program immediately.

1.14 QUESTIONS.

- Q.1) Define hacking ? Explain in detail its types.
- Q.2) Explain the purpose of Ethical hacking. With their Advantages & Disadvantages.
- Q.3) Explain in detail types of hackers.
- Q.4) what is code of ethics , Explain in detail.
- Q.5) Explain in detail types of attacks.
- Q.6) Explain in detail how to prevent from the hackers.
- Q.8) summarize the different section in Indian IT Act 2000.
- Q.9) Explain in detail amendments in Indian IT Act 2008.
- Q.10) Explain in detail phases of hacking.

1.15 REFERENCES.

- 1) Manthan Desai Basics of ethical hacking for beginners.
- 2) TutorialsPoint Professionals, Ethical Hacking by TutorialsPoint.
- 3) SunitBelapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives.

INTRODUCTION TO ETHICAL HACKING

Unit Structure

- 2.1 The Indian IT Act 2000 and Amendments to the Indian IT Act(2008)
- 2.2 Phases of hacking.
- 2.3 Questions.
- 2.4 References.

2.1 THE INDIAN IT ACT 2000 AND AMENDMENTS TO THE INDIAN IT ACT(2008) :

The Indian Information Technology Act 2000 (“Act”) was based on the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law^[1]; the suggestion was that all States intending to enact a law for the impugned purpose, give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information.

Thus the Act was enacted to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involved the use of alternatives to traditional or paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies.

Also it was considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records. The Act received the assent of the President on the 9th of June, 2000.

- **DEFINITIONS**

In this Act, unless the context otherwise requires, —

1. "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
2. "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary.

SECTION 3 - AUTHENTICATION OF ELECTRONIC RECORDS BY USE OF DIGITAL SIGNATURE

• AUTHENTICATION OF ELECTRONIC RECORDS

The Act provides that the authentication of the electronic record can be effected by the use of asymmetric crypto system and **hash** function which envelop and transform the *initial electronic* record into *another electronic record*.

A "**hash function**" is an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known 'as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

1. to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
2. that two different electronic records can produce the same hash result using the algorithm.

The record can be accessed by the use of public key of the subscriber. The private key and the public key are unique to the subscriber and constitute a functioning key pair.

SECTION 3A - AUTHENTICATION OF ELECTRONIC RECORDS BY USE OF ELECTRONIC SIGNATURE.

A subscriber can authenticate any electronic record by such an electronic signature or an electronic authentication technique which is considered reliable and may be specified in the schedules. In order for the electronic signature to be reliable

1. The signature creation data or authentication data are, within the context they are used, linked to the signatory, or as the case may be, the authenticator and to no other person;
2. The signature creation data or authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and to no other person;
3. Any alteration to the electronic signature made after affixing such signature is detectable.
4. Any alteration to the information made after its authentication by electronic signature is detectable.
5. It fulfills other prescribed conditions.

The Central Government can prescribe the procedure for the purpose of ascertaining who has affixed the signature. The Central Government can also, by notification in the Official Gazette, add or omit any reliable electronic signature or electronic authentication technique or the procedure

for affixing the same. The notification of such method or procedure is required to be placed before both houses of the Parliament.

ELECTRONIC GOVERNANCE & LEGAL RECOGNITION OF ELECTRONIC RECORDS & ELECTRONIC SIGNATURES.

SECTION 4 - ELECTRONIC RECORDS

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

1. rendered or made available in an electronic form; and
2. accessible so as to be usable for a subsequent reference.

SECTION 5 - LEGAL RECOGNITION OF ELECTRONIC SIGNATURES

Where any law requires that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement will be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature affixed in such manner as prescribed by the Central Government.

- **SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURES**

SECTION 14 - SECURE ELECTRONIC RECORD

Where any security procedure is applied to an electronic record, at a specific point of time, then from such point onwards up to the time of verification, the record is deemed to be a secure electronic record.

SECTION 15 - SECURE ELECTRONIC SIGNATURE

An electronic signature is unique to the subscriber. Once the signature is affixed to an electronic record it can be used to identify the subscriber. It is presumed to be under the exclusive control of the subscriber. The signature signifies the time when it is affixed to an electronic record and the manner in which the signature was created. If any one tries to alter such a signed electronic record, then the signature gets invalidated. An electronic signature will be deemed to be secure if it can be proved that, it was under the exclusive control of the signatory at the time of affixing and the signature data (private key) was stored and affixed in the specified manner.

SECTION 18 - FUNCTIONS OF CONTROLLER

The primary function of the CCA is to regulate the Certifying Authorities(“CA”). For the purpose of regulating the CA the CCA may perform all or any of the following functions, namely:—

- certifying public keys of the Certifying Authorities;
- laying down the standards to be maintained by the Certifying Authorities;
- specifying the qualifications and experience which employees of the Certifying Authorities should possess;
- specifying the conditions subject to which the Certifying Authorities shall conduct their business;
- specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;
- specifying the form and content of a Digital Signature Certificate and the key,
- specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
- specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
- facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
- specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
- resolving any conflict of interests between the Certifying Authorities and the subscribers;
- laying down the duties of the Certifying Authorities;
- maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

SECTION 21 - LICENCE TO ISSUE ELECTRONIC SIGNATURE CERTIFICATES Any person can obtain a license to issue an ESC by making an application to the CCA. After receiving the application the CCA verifies whether or not such an applicant has satisfied the eligibility criteria, as specified by the Central Government in respect of qualification, expertise, manpower, financial resources and other infrastructure facilities. Once the eligibility of the applicant is ascertained, the CCA issues a license to the applicant. The licensee is thereafter subject such terms and conditions as are provided for in the regulations issued in this regards. Any license granted under this section is valid for such period as can be provided for by the Central Government. It may be noted that such a license is not transferable or inheritable.

SECTION 22 - APPLICATION FOR LICENSE:

Every application is required to be in the prescribed form. Along with the application the applicant is also required to file:

- a certification practice statement;
- a statement including the procedures with respect to identification of the applicant;
- payment of such fees, not exceeding twenty-five thousand rupees (as prescribed by the Central Government);
- such other documents, as can be prescribed from time to time by the Central Government. An application for renewal of a license is also required to be in the prescribed form accompanied by such fees, which cannot exceed five thousand rupees and has to be made at least forty-five days before the date of expiry of the period of validity of the existing license.

The CCA can, on receipt of an application, after considering the documents accompanying the application and such other factors, as the CCA deems fit, grant the license or reject the application. The applicant is granted a reasonable opportunity of presenting his case to the CCA before his application is rejected.

SECTION 25 - SUSPENSION OF LICENCE

If the CCA, after making an inquiry is satisfied that a CA has

- made an incorrect or false statement in his application for the issue or renewal of licence;
- failed to comply with the terms and conditions subject to which the licence was granted;
- has not maintained the standards required to be followed under this Act;
- contravened any provisions of this Act, rule, regulation or order made there under then after giving a reasonable opportunity to show cause against the proposed revocation, revoke the license. In the alternative, pending such an inquiry, if the CCA is of the opinion that there exist circumstances for the revocation of the license of the CA, then the CCA can suspend the license till the completion of the inquiry. The period of suspension cannot however exceed a period of 10 days unless the CA has been given a reasonable opportunity of showing cause against the proposed suspension. The CA is barred from issuing any ESCs during his suspension period.

After making an inquiry into an allegation of default and after giving the defaulting CA a reasonable opportunity of being heard, if the CCA is satisfied that the license of the CA need to be suspended or revoked, he can proceed against the CA and suspend or revoke his license. The

notice of such an action of suspension or revocation, as the case may be, by the CCA is required to be published in the database and all the repositories maintained by the CCA. The CCA is required also make available such a notice of suspension or revocation of license, through a website which is accessible round the clock. If considered appropriate by the CCA he may publicise the contents of database in appropriate electronic or other media. The CCA can delegate or authorize the Dy. CA or the ACA to exercise any of its power in respect of the regulation of Certified Authorities.

- **ACCESS TO COMPUTERS AND DATA**

Without prejudice to the provisions of sub-section (1) of section 69, the CCA or any person authorized by him will, if he has reasonable cause to suspect that the provisions related to regulation of CAs, rules or regulations made there under, are being contravened, then they can search or access any computer system, any apparatus, data or any other material connected with such system to obtain any information or data contained in or available to such computer system. In doing so they can direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide such reasonable technical and other assistance as the investigating authority may consider necessary.

ELECTRONIC SIGNATURE CERTIFICATES

SECTION 35 - CERTIFYING AUTHORITY TO ISSUE ELECTRONIC SIGNATURE CERTIFICATE.

Any person can make an application to the CA for the issue of a ESC. The application will be in the form prescribed by the Central Government. The application shall be accompanied with the prescribed fee not exceeding twenty five thousand rupees, to be paid to the Certifying Authority. The fee could be different fees for different classes of applicants'. In addition to the fees the application is also required to be accompanied with a certification practice statement or where there is no such statement, a statement containing such particulars, as may be required by regulations.

The CA can consider such an application accompanied with the certification practice statement, and after making the necessary inquiry, as the CA deems fit, either grant the ESC or for reasons to be recorded in writing, reject the application. The application can be rejected only after giving the applicant a reasonable opportunity of being heard.

- **DUTIES OF SUBSCRIBERS**

Where any Electronic Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Electronic Signature Certificate has been accepted by a subscriber, then, the subscriber will generate the key pair by applying the security procedure. Further the subscriber shall perform such duties as may be prescribed.

- **ACCEPTANCE OF ELECTRONIC SIGNATURE CERTIFICATE**

A subscriber is deemed to have accepted a ESC if he publishes or authorizes the publication of a ESC to one or more persons in a repository, or otherwise demonstrates his approval of the ESC in any manner.

By accepting a ESC the subscriber certifies to all who reasonably rely on the information contained in the ESC that the subscriber holds the private key corresponding to the public key listed in the ESC and is entitled to hold the same. Furthermore all representations made by the subscriber to the CA and all material relevant to the information contained in the ESC are true to the best of his belief.

- **CONTROL OF PRIVATE KEY**

Every subscriber is required to exercise reasonable care to retain control of his private key, which corresponds to the public key listed in his ESC and take all steps to prevent its disclosure to a person not authorized to affix the electronic signature of the subscriber.

If the private key is compromised, then, the subscriber will communicate the same forthwith to the CA in specified manner. The subscriber is liable for all events occurring as a result of the compromising of the private key from the time compromise upto the time he has informed the CA of the private key being compromised.

- **PENALTIES, COMPENSATION AND ADJUDICATION**

The Information Technology Amendment Act 2008 have introduced a host of offencies and prescribed penalties for these offences.

SECTION 43 - PENALTY FOR DAMAGE TO COMPUTER, COMPUTER SYSTEM, ETC

If any person without permission (or the knowledge) of the owner or any other person who is in-charge of a computer, computer system or computer network, —

1. accesses or secures access to such computer, computer system or computer network;
2. downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

3. introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
4. damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
5. disrupts or causes disruption of any computer, computer system or computer network;
6. denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;
7. provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;
8. charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;
9. destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
10. Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;

He can be made liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.— For this purposes,—

1. "computer contaminant" means any set of computer instructions that are designed—
 1. to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
 2. by any means to usurp the normal operation of the computer, computer system, or computer network;
2. "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

3. "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
4. "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.
5. "Computer Source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form

SECTION 43A - COMPENSATION FOR FAILURE TO PROTECT DATA

When a body corporate is in possession, handling or dealing in sensitive personal data or information in a computer resource that it owns, controls or operates, is found negligent in implementing & maintaining reasonable security practices and procedures and thereby causes wrongful loss or gain to any person, then in such a case the body corporate will be held liable to damages as compensation to a sum not exceeding Rs 5 Crores to the person so effected.

For this purpose, "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

"Reasonable security practices and procedures" would include such practices and procedures which are designed to protect information from unauthorized access, damage, misuse, modification, disclosure etc, as may be agreed to between the parties or as determined by law in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

"Sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Note: Refer Notification G.S.R. 313(E).— dated 11th April 2011 for Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Notified by the Central Government.

• PENALTY FOR FAILURE TO FURNISH INFORMATION RETURN, ETC

If any person who under this Act or any rules or regulations made there under to—

1. Is required by the CCA or CA to furnish any document, return or report fails to do so, will be liable to a penalty not exceeding Rs 1,50,000/-for each such failure;
2. Is required to file any return or furnish any information, books or other documents within the time specified by the regulations, fails to do so, within the time specified, will be liable to a penalty not exceeding Rs 5000/- per day of such continuing default;
3. Fails to maintain books of accounts or records as required, will be liable to a penalty not exceeding Rs 10,000/- per day of such continuing default.

- **ESTABLISHMENT & COMPOSITION OF CYBER APPELLATE TRIBUNAL**

The Central Government, by notification, can establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal (“tribunal”). Such notification will also specify the matters and places in relation to which the Cyber Appellate Tribunal can exercise jurisdiction.

- **APPEAL TO CYBER APPELLATE TRIBUNAL**

Any person aggrieved by an order made by Controller or an adjudicating officer under this Act can prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter. However no appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties. The appeal can be filed by the aggrieved person within a period of 45 days from the date of receipt of order in the prescribed form and accompanied by prescribed fee. The Cyber Appellate Tribunal can entertain an appeal after the expiry of the said period of 45 days if it is satisfied that there was sufficient cause for not filing it within the prescribed period. The provisions of the Limitation Act, 1963, will, as far as can be, apply to an appeal made to the Cyber Appellate Tribunal.

The appeal filed before the Cyber Appellate Tribunal is to be dealt with by it as expeditiously as possible and an endeavor will be made by the Cyber Appellate Tribunal to dispose of the appeal finally within six months from the date of receipt of the appeal. The appellant can either appear in person or through an authorized representative (one or more legal practitioners) or any of its officers, to present his or its case before the Cyber Appellate Tribunal.

The Cyber Appellate Tribunal can, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against. The Cyber Appellate Tribunal will send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating office.

- **SECTION 58 - PROCEDURE AND POWERS OF THE CYBER APPELLATE TRIBUNAL**

The Cyber Appellate Tribunal is not be bound by the procedure laid down by the Code of civil Procedure, 1908 but is be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal has the powers to regulate its own procedure including the place at which it shall have its sittings. For the purposes of discharging its functions under this Act, the Cyber Appellate Tribunal has the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely:—

1. summoning and enforcing the attendance of any person and examining him on oath;
2. requiring the discovery and production of documents or other electronic records;
3. receiving evidence on affidavits;
4. issuing commissions for the examination of witnesses or documents;
5. reviewing its decisions;
6. dismissing an application for default or deciding it *ex pane*;
7. any other matter which may be prescribed.

Every proceeding before the Cyber Appellate Tribunal is deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal is deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973. No Civil Court has the jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered, by or under this Act, to determine and no injunction will be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

SECTION 62 - APPEAL TO HIGH COURT

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal can file an appeal to the High Court within sixty days from the date of receipt of order of the Cyber Appellate Tribunal, on any question of fact or law arising out of such order. Any delay in filing the appeal to the High Court can be condoned by the High Court, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

- **OFFENCES**

The Act has specified that Tampering with computer source documents, Hacking computer system, Publishing of information which is obscene in electronic form or failure of a CA or its employees to follow the directions/ Orders of the CCA, failure to comply with Directions of Controller to a subscriber to extend facilities to decrypt information, accessing a protected system without proper authorization, material mis-representation, Penalty for publishing Electronic Signature Certificate false particulars, Publication for fraudulent purpose, sending of grossly offensive information, false information, etc will be offences.

The various offences and corresponding punishments are summarized and tabulated below with detailed explanation in the following paragraphs.

Section	Contents	Imprisonment Up to	Fine Up to
65	Tampering with computer source code documents	3 year or/and	200,000
66	Hacking with computer system dishonestly or fraudulently	3 years or/and	500,000
66B	receiving Stolen computer resource	3 years or/and	100,000
66C	Identity Theft - fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person	3 years and	100,000
66D	cheating by Personation by using computer resource	3 years and	100,000
66E	Violation of Privacy	3 years or/and	200,000

66F	<p>Whoever,-</p> <ol style="list-style-type: none"> 1. with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by – 1. Denial of Access 2. Attempting to Penetrate computer resource 3. Computer containment 2. knowingly or intentionally penetrates and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations, or likely to cause injury to the interests of the sovereignty and integrity of India 	Imprisonment for Life	
67	<p>Publish or transmit Obscene material - 1st time</p> <p>Subsequent Obscene in elec. Form</p>	<p>3 years and</p> <p>5 years and</p>	<p>500,000</p> <p>10,00,000</p>
67A	<p>Publishing or transmitting material containing</p> <p>Sexually Explicit Act - 1st time</p> <p>Subsequent</p>	<p>5 years and</p> <p>7 years and</p>	<p>10,00,000</p> <p>10,00,000</p>

67B	Publishing or transmitting material containing Children in Sexually Explicit Act - 1 st time Subsequent	5 years and 7 years and	10,00,000 10,00,000
67C	Contravention of Retention or preservation of information by intermediaries	3 years and	Not Defined
68	Controller's directions to certifying Authorities or any employees failure to comply knowingly or intentionally	2 years or/and	100,000
69	Failure to comply with directions for Intercepting, monitoring or decryption of any info transmitted through any computer system/network	7 Years and	Not Defined
69A	Failure to comply with directions for Blocking for Public Access of any information through any computer resource	7 Years and	Not Defined
69B	Failure to comply with directions to Monitor and Collect Traffic Data	3 Years and	Not Defined
70	Protected system. Any unauthorised access to such system	10 years and	Not Defined
70B (7)	Failure to provide information called for by the *I.C.E.R.T or comply with directions	1 year or	1,00,000
71	Penalty for Misrepresentation or suppressing any material fact	2 or/and years	100,000

72	Penalty for breach of confidentiality and privacy of el. records, books, info., etc without consent of person to whom they belong.	2 or/and years	100,000
72A	Punishment for Disclosure of information in breach of lawful contract	3 or/and years	500,000
73	Penalty for publishing False Digital Signature Certificate	2 or/and years	100,000
74	Fraudulent Publication	2 or/and years	100,000
75	Act also to apply for offences or contravention committed outside India if the act or conduct constituting the offence involves a computer, computer system or computer network located in India		
76	Confiscation of any computer, computer system, floppies, CDs, tape drives or other accessories related thereto in contravention of any provisions of the Act, Rules, Regulations or Orders made.		
77	Penalty and Confiscation shall not interfere with other punishments provided under any law.		
78	Power to investigate offences by police officer not below rank of Dy. Superintendent of Police.		

- ***I.C.E.R.T** - Indian Computer Emergency Response Team to serve as national agency for incident response – Functions in

the area of Cyber Security, 1. collection, analysis and dissemination of information on cyber incidents

2. forecast and alerts of cyber security incidents
3. emergency measures for handling cyber security incidents
4. coordination of cyber incidents response activities
5. issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
6. such other functions relating to cyber security as may be prescribed.

- **TAMPERING WITH COMPUTER SOURCE DOCUMENTS,**

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, can be punished with imprisonment up to three years, or with fine which can extend up to two lakh rupees, or with both. "Computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

- **UNAUTHORIZED ACCESS TO A COMPUTER SYSTEM**

If any person, dishonestly or fraudulently does any act which results in damage to a computer or a computer system or secures unauthorized access to a secure computer system or down loads or copies data etc (acts described under section 43 of the Act), then he can be punished with a prison term which can extend up to two years or with a fine which can extend up to ₹Five Lakhs or both.

Here the Act refers to the India Penal Code for interpreting the meaning of the words

“dishonestly” and “fraudulently”

- **PUNISHMENT FOR SENDING OFFENSIVE MESSAGES THROUGH COMMUNICATION SERVICE**

Any person who sends, by means of a computer resource or a communication device any information that is grossly offensive or has menacing character; or which he knows to be false, or sends any electronic mail or message so as to mislead the

addressee about the origin of such message but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device, shall be punishable with imprisonment for a term which may extend to three years and with fine. Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

- **PUNISHMENT FOR DISHONESTLY RECEIVING STOLEN COMPUTER RESOURCE OR COMMUNICATION DEVICE**

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

- **PUNISHMENT FOR IDENTITY THEFT**

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

- **PUNISHMENT FOR CHEATING BY PERSONATION BY USING COMPUTER RESOURCE**

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

- **PUNISHMENT FOR VIOLATION OF PRIVACY.**

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

“**Transmit**” means to electronically send a visual image with the intent that it be viewed by a person or persons;

“**Capture**”, with respect to an image, means to videotape, photograph, film or record by any means;

“**Private area**” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

“**Publishes**” means reproduction in the printed or electronic form and making it available for public;

“**Under circumstances violating privacy**” means circumstances in which a person can have a reasonable expectation that he or she could disrobe in privacy, without being concerned that an image of his private area was being captured or any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

- **PUNISHMENT FOR PUBLISHING OR TRANSMITTING OBSCENE MATERIAL IN ELECTRONIC FORM**

Any person who publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to **two three** years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to **five** years and also with fine which may extend to ten lakh rupees.

- **PUNISHMENT FOR PUBLISHING OR TRANSMITTING OF MATERIAL CONTAINING SEXUALLY EXPLICIT ACT,ETC. IN ELECTRONIC FORM**

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to **five** years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to **seven years** and also with fine which may extend to ten lakh rupees.

- **PUNISHMENT FOR PUBLISHING OR TRANSMITTING OF MATERIAL DEPICTING**

CHILDREN IN SEXUALLY EXPLICIT ACT, ETC. IN ELECTRONIC FORM.

Whoever, publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or facilitates abusing children online or records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

The above three provisions shall not be applicable to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form if the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern or which is kept or used for bonafide heritage or religious purposes

"Children" means a person who has not completed the age of 18 years.

• POWER OF CONTROLLER TO GIVE DIRECTIONS

The CCA can direct a CA or the employees of such a CA to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under. Any person intentionally or knowingly failing to comply with such an order will have committed an offence and will be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.

• POWER TO AUTHORIZE TO MONITOR AND COLLECT TRAFFIC DATA OR INFORMATION THROUGH ANY COMPUTER RESOURCE FOR CYBER SECURITY

The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or

spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. The Intermediary or any person in-charge of the Computer resource shall when called upon by such agency provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating , transmitting, receiving or storing such traffic data or information. The government shall prescribe procedure and safeguards for monitoring and collecting traffic data or information.

Any intermediary who intentionally or knowingly contravenes the provisions shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

"Computer Contaminant" shall have the meaning assigned to it in section 43

"Traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

- **INDIAN COMPUTER EMERGENCY RESPONSE TEAM TO SERVE AS NATIONAL AGENCY FOR INCIDENT RESPONSE**

The Central Government has the powers through notification to appoint an agency of the government to be called the Indian Computer Emergency Response Team. The Central Government shall provide such agency with a Director General and such other officers and employees as may be prescribed. The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security,-

1. collection, analysis and dissemination of information on cyber incidents
2. forecast and alerts of cyber security incidents
3. emergency measures for handling cyber security incidents
4. Co-ordination of cyber incidents response activities
5. issue guidelines, advisories, vulnerability notes and white papers relating to information security practices,

procedures, prevention, response and reporting of cyber incidents

6. such other functions relating to cyber security as may be prescribed

For carrying out the above functions, the agency may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person. Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with such direction shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

- **PENALTY FOR MISREPRESENTATION**

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or ESC, as the case may be, can be punished with imprisonment for a term which can extend to two years, or with fine which can extend to one lakh rupees, or with both.

- **PENALTY FOR BREACH OF CONFIDENTIALITY AND PRIVACY**

No person can publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that the CA listed in the certificate has not issued it or the subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended, unless such publication is in the course of verifying a electronic signature created prior to such suspension or revocation. Such a contravention can be punished with imprisonment for a term which can extend to two years, or with fine which can extend to one lakh rupees, or with both.

- **PENALTY FOR PUBLISHING ELECTRONIC SIGNATURE CERTIFICATE FALSE IN CERTAIN PARTICULARS**

Whoever knowingly creates, publishes or otherwise makes available a ESC for any fraudulent or unlawful purpose can be punished with imprisonment for a term which can extend to two years, or with fine which can extend to one lakh rupees, or with both.

2.2 PHASES OF HACKING:

The process of legal and authorized attempts to discover and successfully exploiting the computer system in an attempt to make the computer system

more secure is called Ethical Hacking. This process includes a probe for vulnerability and providing proof of concept (POC) attacks to visualize that vulnerabilities are actually present in the system.

A Good Penetration tester always provides a specific recommendation to remove the flaws in the system discovered during the penetration test.

Penetration testing is also known by some other terms like:

- **Penetration testing**
- **PT**
- **Hacking**
- **Pen Testing**
- **White Hat Hacking**

There is a term called **Vulnerability Assessment** which is quite similar to Penetration Testing. Vulnerability Assessment means reviewing services and systems for security issues. Many people use pen testing and vulnerability assessment interchangeably for each other but they are not the same.

The penetration testing process is a step ahead of vulnerability assessment. Vulnerability Assessment only discovers flaws in the system but PT provides a way to remove those flaws as well.

1. Reconnaissance:

This is the first phase where the Hacker tries to collect information about the target. It may include Identifying the Target, finding out the target's IP Address Range, Network, DNS records, etc. Let's assume that an attacker is about to hack a websites' contacts.

He may do so by using a search engine like maltego, researching the target say a website (checking links, jobs, job titles, email, news, etc.), or a tool like HTTPTrack to download the entire website for later enumeration, the hacker is able to determine the following: Staff names, positions, and email addresses.

2. Scanning:

This phase includes the usage of tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data. Hackers are now probably seeking any information that can help them perpetrate attacks such as computer names, IP addresses, and user accounts. Now that the hacker has some basic information, the hacker now moves to the next phase and begins to test the network for other avenues of attacks.

The hacker decides to use a couple of methods for this end to help map the network (i.e. Kali Linux, Maltego and find an email to contact

to see what email server is being used). The hacker looks for an automated email if possible or based on the information gathered he may decide to email HR with an inquiry about a job posting.

3. Gaining Access:

In this phase, the hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2. The hacker has finished enumerating and scanning the network and now decides that they have some options to gain access to the network.

For example, say a hacker chooses a Phishing Attack. The hacker decides to play it safe and use a simple phishing attack to gain access.

The hacker decides to infiltrate the IT department. They see that there have been some recent hires and they are likely not up to speed on the procedures yet. A phishing email will be sent using the CTO's actual email address using a program and sent out to the techs. The email contains a phishing website that will collect their login and passwords. Using any number of options (phone app, website email spoofing, Zmail, etc) the hacker sends an email asking the users to log in to a new Google portal with their credentials. They already have the Social Engineering Toolkit running and have sent an email with the server address to the users masking it with a bitly or tinyurl.

4. Maintaining Access:

Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Once the hacker owns the system, they can use it as a base to launch additional attacks.

In this case, the owned system is sometimes referred to as a zombie system. Now that the hacker has multiple e-mail accounts, the hacker begins to test the accounts on the domain. The hacker from this point creates a new administrator account for themselves based on the naming structure and tries and blends in. As a precaution, the hacker begins to look for and identify accounts that have not been used for a long time. The hacker assumes that these accounts are likely either forgotten or not used so they change the password and elevate privileges to an administrator as a secondary account in order to maintain access to the network. The hacker may also send out emails to other users with an exploited file such as a PDF with a reverse shell in order to extend their possible access. No overt exploitation or attacks will occur at this time. If there is no evidence of detection, a waiting game is played letting the victim think that nothing was disturbed. With access to an IT account, the hacker begins to make copies of all emails, appointments, contacts, instant messages and files to be sorted through and used later.

5. Clearing Tracks (so no one can reach them):

Prior to the attack, the attacker would change their MAC address and run the attacking machine through at least one VPN to help cover their identity. They will not deliver a direct attack or any scanning technique that would be deemed “noisy”.

Once access is gained and privileges have been escalated, the hacker seeks to cover their tracks. This includes clearing out Sent emails, clearing server logs, temp files, etc. The hacker will also look for indications of the email provider alerting the user or possible unauthorized logins under their account.

2.3 QUESTIONS.

- Q.1) Explain in detail Indian IT Act 2000.
- Q.2) summarize the different section in Indian IT Act 2000.
- Q.3) Explain in detail amendments in Indian IT Act 2008.
- Q.4) Explain in detail phases of hacking.

2.4 REFERENCES.

- 1) TutorialsPoint Professionals, Ethical Hacking by TutorialsPoint.
- 2) SunitBelapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives.
- 3) <https://www.edureka.co/blog/steganography-tutorial>
- 4) [https://www.techtarget.com/whatis/definition/Information-Technology-Amendment-Act-2008-I T-Act-2008](https://www.techtarget.com/whatis/definition/Information-Technology-Amendment-Act-2008-I-T-Act-2008)

FOOTPRINTING AND RECONNAISSANCE

Unit Structure

- 3.0 Objective
- 3.1 What is footprinting?
- 3.2 Active and passive footprinting
- 3.3 Purpose of footprinting
- 3.4 Objectives of footprinting
- 3.5 Footprinting threats
- 3.6 Types of footprinting
- 3.7 Footprinting countermeasures
- 3.8 Self-Learning Topics: footprinting tools
- 3.9 Unit End Questions
- 3.10 References

3.0 OBJECTIVES

This chapter would make you understand the following concepts

- Understanding footprinting and its techniques
- Implementation of footprinting
- To understand footprinting threats and countermeasures
- Various applications of footprinting tools

3.1 WHAT IS FOOTPRINTING?

Footprinting is a technique used in ethical hacking to gather data as much as possible of a specific targeted infrastructure, computer system, networks, employees and third-party partners to trace vulnerabilities to penetrate them.

This information collected can include the Operating System used by the organization, network maps, firewalls, domain name system information, IP addresses, security configurations of the target machine, virtual private networks (VPNs), Universal Resource Locator (URLs), email addresses, staff IDs, and phone numbers.

How do you start footprinting?

Similar to footprinting is Reconnaissance and it is a crucial part in the initial hacking activity. It is basically a passive footprinting activity wherein while

penetration testing we collect information about the target's potential flaws and vulnerabilities to exploit.

Footprinting process starts with the objective of an intrusion and determining the location. Once the ethical hackers identify a specific target, they try to gather information about the network and organization using non-intrusive methods, maybe like accessing the organization's personnel directory, own webpage, or employee bios.

Ethical hackers collect this information and initiate social engineering campaigns to identify any security vulnerabilities and achieve ethical hacking goals.

3.2 ACTIVE AND PASSIVE FOOTPRINTING

In ethical hacking, footprinting is broadly classified into two types:

1. Active footprinting
2. Passive footprinting

What is active footprinting?

Active footprinting is the process of collecting information about a specific target system using various tools and techniques, like using the traceroute commands or a ping sweep - Internet Control Message Protocol sweep. This triggers the specific target's intrusion detection system (IDS). It performs a certain level of creativity and stealth to avoid detection successfully.

Active Foot-printing techniques include:

- Querying exposed name servers of the specific target
- Extracting information of revealed files and documents
- Gathering website information victimization internet dashing and mirroring tools
- Gathering information through email
- Performing whois operation
- Extracting Domain Name Server (DNS) information
- Conducting traceroute analysis
- Implementing social engineering
- Information Obtained in Foot printing

What is passive footprinting?

As the name implies, passive footprinting describes collecting data about a specific target using innocuous methods, like looking through Archive.org, performing a Google search, browsing through employees' social media profiles, using NeoTrace, looking at various job sites and using Whois, viz a website that provides the domain names and associated networks for a specific organization. Since it does not trigger the target's IDS, It is a stealthier approach to footprinting.

Passive Foot-printing techniques include:

- Collecting location information on the target through the internet services
- Finding information through various search engines
- Gathering financial information concerning the target through various financial services
- Finding the ranking Domains (TI-Ds) and subdomains of a target through various internet services
- Gathering infrastructure information of the target organization through various job sites.
- Gathering information using forums, blogs, and teams
- Monitoring target using various alert services
- Stimulating the operative systems used by the target organization
- Monitoring the website traffic of the specific target
- Performing competitive intelligence
- Tracking the web reputation of the specific target
- Extracting information concerning to the target using the web archives
- Collecting information through social engineering on various social networking sites

3.3 PURPOSE OF FOOTPRINTING

In ethical hacking, Footprinting techniques help businesses to identify and secure IT infrastructure before a threat exploits a vulnerability. Users can also construct a database of known loopholes and vulnerabilities.

Footprinting also helps organisations to better understand their current security level through analysis of information gathered about the implemented firewall, security configuration and many more. Users can easily update this list periodically and utilize this list as a reference point during any security audits.

Drawing a network map will help to cover all the trusted servers, routers, and other network topologies. Users can trace a decreased attack surface by narrowing it to a specific range of systems.

3.4 OBJECTIVES OF FOOTPRINTING

The objectives of footprinting are as follows:

- To learn the security posture, analyze the security posture of the target, find loopholes and vulnerabilities, and create an attack plan.

- To identify the focus area using various different tools and techniques, thus narrowing down the range of IP addresses.
- To find vulnerabilities and use the collected information to identify weaknesses in the specified target's security.
- To map the network Graphically, represent the specific target's network and use it as a guide during the attack.

3.5 FOOTPRINTING THREATS

The following are the different possible threats through foot printing:

- **Network and System Attacks:** Foot printing helps an offender to perform network and system attacks. By this, attackers will gather information associated with the specific target organization's system configuration, operating system which is running on the machine, and so on. Victimization of this information, rogues are able to trace vulnerabilities within the target system so as to exploit those vulnerabilities. Attackers can then take control over a specific target system or the whole network.
- **Social Engineering:** Hackers indirectly or directly collect data through persuasion and various different means without using any intrusion technique. Hackers can gather crucial and sensitive information from employees who are unaware of the hackers' intention.
- **Information Leakage:** Data leakage poses a threat to any organization. If crucial and confidential data of an organization falls into the attacker's hands, those attackers will make an attack set up to use the knowledge in a destructive manner, or use it for financial profit.
- **Privacy Loss:** Using footprinting techniques, hackers are able to have an access to the networks and systems of the organization and even obtain the privileges and rights up till the admin levels, endangering the security thus, leading to the loss of organization's privacy as an entire and to its individual personnel.
- **Company Espionage:** Corporate eavesdropping is a major threat to any organizations, as competitors mostly aim to secure crucial and confidential data with the help of footprinting techniques. In this manner, a competitor's measure is able to alter costs, launch similar kinds of products within the market, and customarily have an adverse effect on the market position of any target organization.
- **Business Loss:** Footprinting also has a significant outcome on organizations like different eCommerce websites and on-line businesses, banking and financial connected businesses. There are financial losses every year due to the malicious attacks by hackers.

3.6 TYPES OF FOOTPRINTING

The various types of footprinting are as follows:

DNA footprinting

DNA footprinting is used to scientifically identify the nucleic acid sequence that holds together with proteins.

Ecological footprint

An ecological footprint is an approach for measuring human demand for natural resources or capital. It basically calculates the quantity of natural resources required to support the economy or people. Ecological footprinting utilizes an ecological accounting system to keep track of the demand.

Digital footprint

A digital footprint consists of one's traceable, unique digital activities. These include communications, actions, and contributions expressed on any digital services or the internet. Digital footprints can be either passive or active.

3.7 FOOTPRINTING COUNTERMEASURES

To safeguard each of us from being the victim of footprinting, we would try to follow the countermeasures which are as follows:

- The types of information must be classified which needs to be kept public or private.
- Keep your social networking accounts private and locked and simply don't upload any unnecessary information, or on any website.
- Avoid keeping any of your personal contact number in any organization's or company's phone book, so as to prevent wardialing.
- Avoid posting confidential information on any social media websites.
- Avoid accepting unknown friend requests on any social media platforms.
- Avoid promotion of education on various hacking tricks.
- Footprinting techniques are used for identifying and removing sensitive information from various social media platforms.
- Configure web servers properly to avoid loss of information about system configuration.
- Try to keep external DNS and internal DNS separate.
- Disable and restrict zone transfer to authorized servers.

- **WHOIS Footprinting**



```
ssslit@JavaPoint:~$ whois javatpoint.com
Whois Server Version 2.0

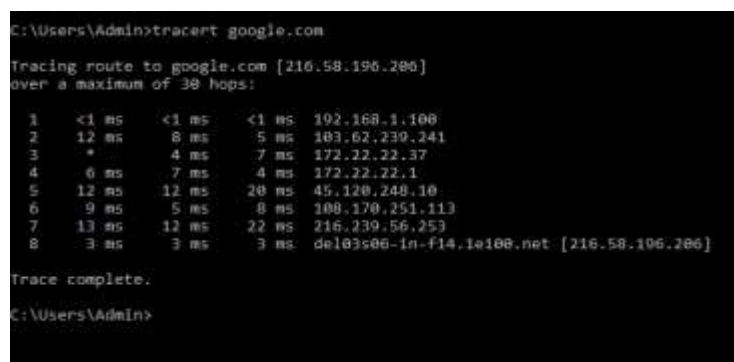
Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Domain Name: JAVATPOINT.COM
Registrar: FOR LTD., D/B/A PUBLICDOMAINREGISTRY.COM
Sponsoring Registrar IANA ID: 383
Whois Server: whois.PublicDomainRegistry.com
Referral URL: http://www.publicdomainregistry.com
Name Server: NS1.CLOUDNS.NET
Name Server: NS1.JAVATPOINT.COM
Name Server: NS2.JAVATPOINT.COM
Name Server: PWS3.CLOUDNS.NET
Name Server: PWS4.CLOUDNS.NET
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Updated Date: 21-Jan-2015
Creation Date: 31-May-2011
Expiration Date: 31-May-2024
```

Figure: WHOIS Footprinting tool

- The WHOIS Footprinting helps to retrieve the information such as IP address, Domain names, Domain Name Server, Netblock data, and etc. Geographical regions which are outside the regions or countries maintain the Regional Internet Registers (RIRs). The Regional Internet Registers (RIR) maintain the database for WHOIS. The RIRs such as APNIC (Asia Pacific Network Information Centre) and LACNIC (Latin American and Caribbean Internet Addresses Registry), maintain the database. For example, Universal Resource Locator (URL) contains the information regarding host name and domain name. Then the Internet Corporation for Assigned Names and Numbers (ICANN) ensures that only a single company shall have that particular domain name. The ICANN shall have a unique registration of domain names. For example, ARINA (American Registry for Internet Numbers) maintains the static IP of North America RIR. The WHOIS tool helps to query the registration database for gathering information related to the domain.

- **Traceroute Tool**



```
C:\Users\Admin>tracert google.com

Tracing route to google.com [216.58.196.206]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms   192.168.1.100
  1  12 ms     8 ms     5 ms    103.62.239.241
  2  *         4 ms     7 ms    172.22.22.37
  3  6 ms      7 ms     4 ms    172.22.22.1
  4  12 ms     12 ms    20 ms   45.120.248.10
  5  9 ms      5 ms     8 ms    108.170.251.113
  6  13 ms     12 ms    22 ms   216.239.56.253
  7  3 ms      3 ms     3 ms    del03s06-in-f14.1e100.net [216.58.196.206]

Trace complete.

C:\Users\Admin>
```

Figure: Traceroute Footprinting tool

In most of the operating systems, the Traceroute tool is used to reach a specific destination address by sending the Internet Control Message Protocol (ICMP) to each hop through a gateway. The number of hops a router receives from the sender can be determined by the hacker. The Traceroute will be timeout if a firewall is encountered in the target system. But, the firewall details will be sent to the hacker by the traceroute. Then, the hacker can also use another technique to bypass the firewall. For example, To locate the destination's network route containing the routers, the tracert command in Traceroute packet tracking tool is used.

- **Nmap Tool**

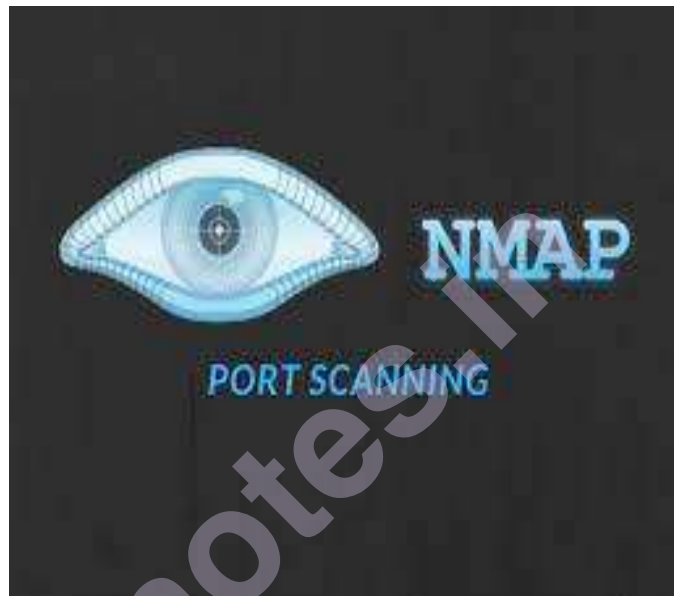


Figure: Nmap Footprinting tool

Nmap is an open source tool mostly used to explore the auditing security and network. Nmap is designed to scan large size networks, it performs optimistically at single hosts. It is used in many cases like host monitoring, network inventory, and to control service upgrade schedules. The Nmap identifies hosts running on the operating system by using IP packets in various ways.

- **NSlookup**

```
student@Comp9:~$ nslookup -type=txt google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
google.com   text = "v=spf1 include:_spf.google.com ~all"
google.com   text = "docuSign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com   text = "facebook-domain-verification=22rm551cu4k0ab0bxs
w536tlds4h95"

Authoritative answers can be found from:

student@Comp9:~$
```

Figure: NSlookup tool

nslookup is a simple yet a practical command-line tool, which principally wants to trace the IP address that corresponds to a domain name or host that corresponds to an IP address (a process known as “Reverse DNS Lookup”). nslookup permits itself to be used in the command-line of the operating system in question; Windows users initiate the service through the command prompt, and Unix users through the terminal window.

- **Sam Spade**

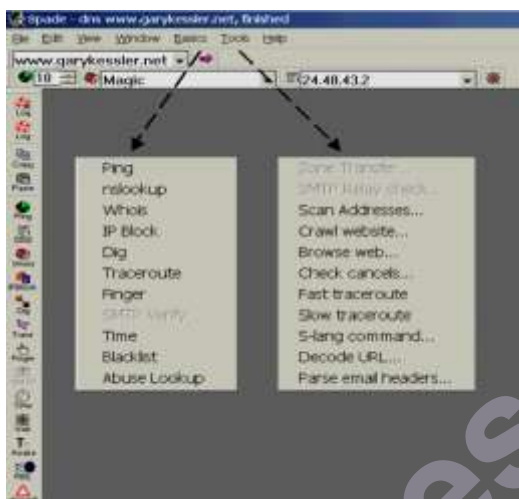


Figure: Sam Spade Footprinting tool

Sam Spade tool executes on all the versions of Windows and makes it simpler to perform a complete analysis and investigation quickly, from learning about the owner of a specific IP address block to examining the contents of a specific internet page. It also has features that are particular to the detection of spam and sites that relay spam. This tool integrates the capabilities found in traceroute, ping, nslookup, time, whois, a packet sniffer, finger, DIG, a port scanner, a scripting language, etc, all with a GUI to boot.

- **SuperScan**

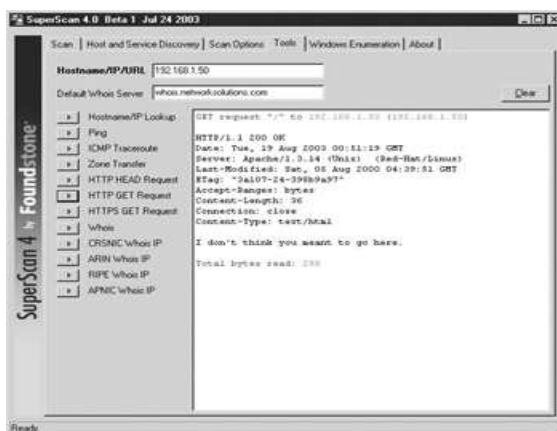


Figure: SuperScan Footprinting tool

SuperScan is a very powerful and quick tool. It allows you to scan TCP ports as well as scan a variety of data processing addresses. It will check some chosen ports or all ports.

- **Nessus**

```
user@ubuntu:~$ sudo bash
[sudo] password for user:
root@ubuntu:~# ls
Desktop  examples.desktop  Pictures  Videos
Documents  Music              Public
Downloads  Nessus-8.2.3-ubuntu910_amd64.deb  Templates
root@ubuntu:~# chmod 777 Nessus-8.2.3-ubuntu910_amd64.deb
root@ubuntu:~# dpkg -i Nessus*.deb
Selecting previously unselected package nessus.
(Reading database ... 159849 files and directories currently installed.)
Preparing to unpack Nessus-8.2.3-ubuntu910_amd64.deb ...
Unpacking nessus (8.2.3) ...
Setting up nessus (8.2.3) ...
Unpacking Nessus Scanner Core Components...

- You can start Nessus Scanner by typing /etc/init.d/nessusd start
- Then go to https://ubuntu:8834/ to configure your scanner

Processing triggers for systemd (237-3ubuntu10.13) ...
Processing triggers for ureadahead (0.100.0-20) ...
```

Figure: Nessus Footprinting tool

Nessus is an efficient tool for scanning vulnerability but it's not a free tool. Once you locate the list of open ports, the next step is to begin searching for vulnerability within the servers.

- **DNS enumerator**

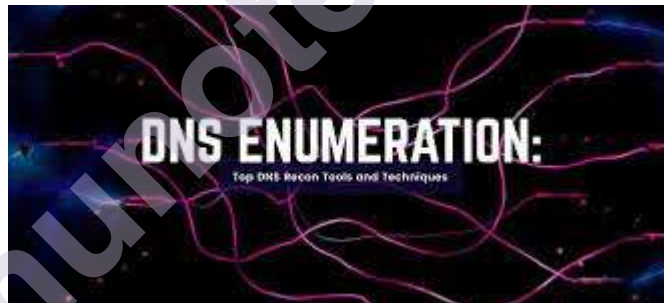


Figure: DNS enumerator Footprinting tool

DNS enumerator is an automated subdomain retrieval tool which can scan google to extract the result

3.9 UNIT END QUESTIONS

1. What is Footprinting? State the purpose of footprinting.
2. What is active footprinting? Explain the active footprinting techniques
3. What is passive footprinting? Explain the passive footprinting techniques
4. State and explain the types of footprinting?
5. State the footprinting countermeasures.
6. State and explain the footprinting tools

3.10 REFERENCES

- <https://info-savvy.com/footprinting-and-scanning-tools/>
- <https://www.geeksforgeeks.org/ethical-hacking-footprinting/>
- <https://www.greycampus.com/opencampus/ethical-hacking/footprinting-methodology>
- <https://study.com/academy/lesson/what-is-footprinting-definition-uses-process.html>
- https://www.researchgate.net/publication/343236950_Footprinting_Techniques_Tools_and_Countermeasures_for_Footprinting

munotes.in

SCANNING NETWORKS

Unit Structure

- 4.0 Objectives
- 4.1 Introduction
- 4.2 Network scanning and its types
 - 4.2.1 What is Scanning?
 - 4.2.2 Types of Scans
- 4.3 Objectives of network scanning
- 4.4 Scanning live systems
- 4.5 Scanning techniques-TCP Connect / Full Open Scan
- 4.6 Types of Stealth scans
- 4.7 Port scanning countermeasures
- 4.8 IDS evasion techniques
- 4.9 Banner grabbing and its tools
- 4.10 Vulnerability scanning
- 4.11 Proxy servers
 - 4.11.1 Proxy Server
 - 4.11.2 Mechanism of Proxy Server
 - 4.11.3 Types of Proxy Server
 - 4.11.4 Advantages of Proxy Server
 - 4.11.5 Need of Proxy Server
 - 4.11.6 Working of Proxy Server
- 4.12 Anonymizers
- 4.13 IP spoofing and its countermeasures
 - 4.13.1 What is IP spoofing?
 - 4.13.2 Countermeasures and Protection from IP Spoofing
- 4.14 Summary
- 4.15 List of References

4.0 OBJECTIVES

- To understand the concept of scanning network along with its types, objectives and application
- Provide a thorough awareness of cyber security challenges, dangers, and concerns, as well as countermeasures to prevent hacking
- Various tools, techniques and its countermeasure involved in ethical hacking

4.1 INTRODUCTION

Ethical hackers, also known as penetration testers, have been around for a long time, but they've gotten increasingly popular in recent years as cybercrime and restrictions have increased. The realisation is that proactively identifying and resolving system flaws and shortcomings is less expensive than dealing with the consequences later. As a result, businesses have attempted to build their own internal penetration testing teams as well as contract with outside experts as needed.

Taking on the talent connected with ethical hacking will put you in the position of analysing environments to discover, exploit, report, and recommend corrective steps to be taken in the case of threats and vulnerabilities swiftly and effectively. However, most pentesters do not perform corrective actions because this is something that the client must determine whether or not to do, but the customer may ask you to do so in some situations.

These businesses have learned to solve their given condition and head off severe problems wherever and whenever possible using a solid and effective combination of technological, administrative, and physical procedures. Security has been aided by technologies such as virtual private networks (VPNs), cryptographic protocols, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), access control lists (ACLs), biometrics, smart cards, and other devices. Over the last decade, administrative countermeasures such as policies, processes, and other rules have also been tightened and implemented. Cable locks, device locks, alarm systems, and similar devices are examples of physical security measures. All of these things, and many more, will be part of your new duty as an ethical hacker.

4.2 NETWORK SCANNING AND ITS TYPES

4.2.1 What is Scanning?

Scanning is the process of engaging and probing a target network with the goal of providing important information that can subsequently be used in later stages of the pen test. It is possible to gain a reasonable image of a

target using network principles, a scanner, and the results of a complete footprinting.

4.2.2 Types of Scan

As not all scans are looking for the same thing or seeking to achieve the same result, it's critical to know what your alternatives are before you begin. All scans have the same fundamental goal of gathering information about a host or group of hosts, but when you dig a little further, you'll see some discrepancies. Each scan will supply you with a different level and sort of information than the others, so each will be useful.

To keep things simple, we'll divide scan types into three categories, each with its own set of features:

1. **Port Scan:** The process of sending carefully designed messages or packets to a target computer in order to learn more about it is known as port scanning. Typically, these probes are associated with well-known port numbers or ones that are less than or equal to 1024. You can learn about the services a system provides to the network as a whole by carefully applying this technique. It's even feasible that you'll be able to distinguish between systems like mail servers, domain controllers, and web servers during this procedure.
2. **Network Scan:** The goal of network scanning is to find all of the active hosts on a network (the hosts that are running). This type of scan will indicate systems that may be targeted later or that should be inspected more thoroughly. Ping sweeps, for example, fall into this category since they quickly scan a range of IP addresses to see if they have a powered-on host linked to them. Nmap and Angry IP, among other tools, can be used to execute this type of scan.
3. **Vulnerability Scan:** A vulnerability scan is used to find flaws or vulnerabilities in a target system. This type of scan is frequently performed as a preventative measure, with the purpose of discovering flaws before an attacker can find and exploit the same vulnerabilities. A typical vulnerability scan will identify hosts, access points, and open ports, as well as analyse service response, classify threats, and provide reports. Companies like vulnerability scans because they can easily execute them on their own to examine their systems. Tenable's Nessus and Rapid7's Nexpose are two popular vulnerability scanners. Specialized scanners such as Burp Suite, Nikto, and WebInspect are also available.

4.3 OBJECTIVES OF NETWORK SCANNING

- 1] To find the victim's live hosts/computers, IP addresses, and open ports.
- 2] To find out what services are running on the host machine.
- 3] To learn about the target's operating system and system architecture.

4.4 SCANNING LIVE SYSTEMS

Let's start by looking for potential targets to investigate and probe. Remember that just because you acquired information on an organization's IP address or range of IP addresses during the previous phase does not mean that each address has a host behind it. To proceed in any meaningful sense, you must first determine which IPs have a "pulse" and which do not. So, how can you check for live systems in a certain location? It turns out that this work can be accomplished in a variety of ways. However, the following are the most widely acknowledged methods for completing this task:

- 1] Wardialing
- 2] Wardriving
- 3] Pinging
- 4] Port scanning

- **Wardialing**

The first form of scan is wardialing, which is an old yet important technique. Since the mid-1980s, Wardialing has existed in a mostly identical state, and it has remained so long because it has shown to be a good information-gathering instrument. In comparison to other types of scanning, wardialing is fairly basic in that it simply dials a block of phone numbers using a regular modem to discover systems that have a modem attached and accept connections. The first form of scan is wardialing, which is an old yet important technique. Since the mid-1980s, Wardialing has existed in a mostly identical state, and it has remained so long because it has shown to be a good information-gathering instrument.

Once you've located a modem and received a response, the next step is to figure out what to do with the data. In such case, you must first understand what devices modems are usually connected to in today's society. Private branch exchanges (PBXs) frequently have modems (nondigital ones) installed, which might present a nice opportunity for the attacking party to cause havoc. Firewalls, routers, and fax machines are examples of other equipment that may have modems attached. An environment can easily become unsecured if an attacker dials into a firewall and gains access.

When an attacker acquires access to a system, keep in mind that they may be exploiting it as a pivot point. A compromised system is used as a pivot point to attack additional systems deeper in the targeted environment. In the case of systems like the ones described here, an attacker may acquire access to the device or system and begin committing more aggressive activities.

Over the years, a number of wardialing applications have been developed. Here are three of the most well-known:

- i] **ToneLoc:** A wardialing application that dials numbers at random or within a range in search of dial tones. It can also look for a modem or fax carrier frequency. ToneLoc works with an input file including the area codes and phone numbers you wish it to dial.
- ii] **THC-SCAN:** This is a DOS-based programme that may search for a carrier frequency from a modem or fax by dialling a range of numbers using a modem.
- iii] **PhoneSweep by NIKSUN:** One of the few commercial choices on the market for wardialing.

- **Using Ping**

Ping is a more well-known tool for scanning. Ping is a tool for determining network connectivity by determining whether a distant server is up or down. While it is a fairly basic utility, it is ideal for the initial scanning phase. Ping uses an Internet Control Message Protocol (ICMP) message to communicate, which is why this method is also known as ICMP scanning. The method works by sending an ICMP echo request to another system, which will respond with an ICMP echo reply if the other system is alive. The system is confirmed to be up, or live, once this response is received. Pinging is useful since it can tell you not only if a system is up, but also the speed at which packets are transferred from one host to another, as well as the time to live (TTL).

Enter the following at the command prompt on Windows to use the ping command:

```
ping < target IP >
```

or

```
ping < target hostname >
```

The command is substantially the same in most Linux versions; however, it will ping the distant client until you press Ctrl+C to stop the process.

You should be aware of another approach to ping a remote system: utilising nmap to do a ping. Enter the following commands at the command prompt in Windows or Linux:

```
nmap -sP -v < target IP address >
```

The ping sweep is a level up from the ICMP scan since it involves scanning or sweeping a range of IP addresses for live hosts. nmap proves useful again again by allowing you to run a rapid scan. Simply type the following command into nmap to accomplish this:

nmap -sP -PE -PA <port numbers> <starting IP/ending IP>

Ping sweeps are quite effective in terms of rapidly accumulating a system inventory; nonetheless, there are some potential downsides. To begin, you must overcome the fact that many network managers block ping at the firewall, making it impossible to ping hosts from outside the network without extra effort. Second, on bigger networks or in enterprise environments, an intrusion-detection system (IDS) or intrusion-prevention system (IPS) will often be present, and these systems will warn the system owner and/or shut down your scan. Finally, due to the way the scan works, it has no method of detecting systems that are down; in such circumstances, the ping will hang for a few moments before alerting you that it is unable to contact a host.

4.5 SCANNING TECHNIQUES-TCP CONNECT / FULL OPEN SCAN

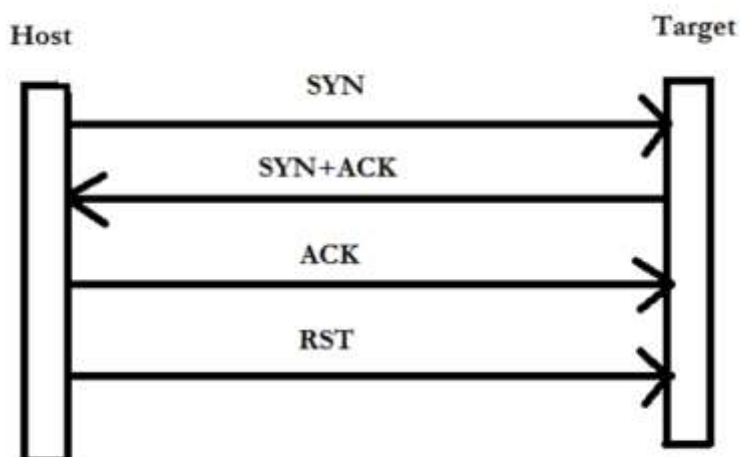
Prior to running any port scans on the target system, a full open scan starts a TCP three-way handshake with the purpose of detecting whether the ports are open or closed.

As it establishes a TCP three-way handshake with the target, this type of scan can quickly detect whether a port is open or closed.

When the initiate no longer needs to interact with the target, it will send a TCP FIN packet to inform the target that it wishes to stop the connection appropriately.

When we send a SYN packet, we are requesting connection initiation; when we receive a SYN+ACK packet, it signifies the port is open and allows us to connect; and finally, we send an ACK package to acknowledge the connection.

nmap can be used to scan in Linux by using the command `nmap -sT urlname`.



4.6 TYPES OF STEALTH SCANS

- **What are stealth scans?**

In a stealth scan packet flags cause the target system to reply without a completely established connection. Hackers utilise stealth scanning to get around intrusion detection systems (IDS), making it a serious threat.

- **Types of stealth scan**

- 1] **Inverse Mapping**

The Inverse Mapping scan, initially reported by the CERT® Coordination Center in 1998, was one of the first stealth scans to arise. The aim was that "intruders send packets to a list of addresses that would typically go unreported or generate no unusual behaviour". Attackers utilise specially created packets with customised flags, such as RST (Reset) and SYN-ACK packets, as well as DNS answer packets in this situation. This type of scan didn't look for specific information about available ports, but rather tested the host to determine if it would react. A network-connected computer would respond to the request, while a non-connected computer would generate an ICMP host unreachable error message. An attacker could map out a network anonymously this way.

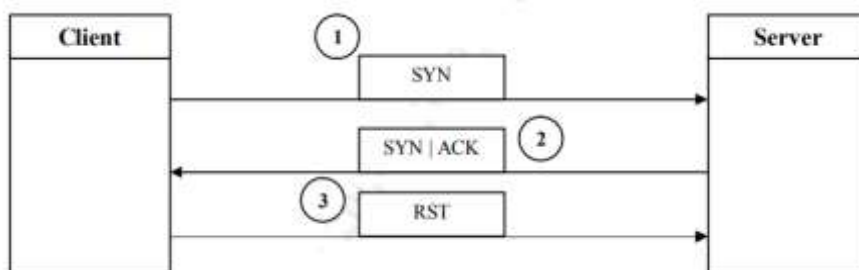
- 2] **Slow Scan**

The slow scan is another method of stealth scanning. This is a low-tech solution to the problem of the remote system logging or noticing you. A "typical" scan will scan thousands of ports in a short amount of time, usually less than a minute. TCP connect() scans are easily logged and found by the system administrator due to their nature. While scanning quickly can quickly fill a log with data, scanning slowly becomes a viable option. Logging applications can be defeated by waiting a certain length of time between scans for different ports. The disadvantage of this sort of stealth is the amount of time it takes. It can take a long time to be covert enough to avoid detection by an intrusion detection system or a system administrator. For example, if a port scanner is programmed to scan one host with ports ranging from 1 to 1024, it will take around 85 hours if each port is scanned every 5 minutes. This method isn't sophisticated, but it does demonstrate that unless a history of all tries to each port is recorded, detection becomes extremely difficult.

- 3] **Half Open Scan**

Through a technique known as SYN scanning, or half-open scanning, the TCP connect() method has evolved to include

stealth. The name comes from the manner of connecting to a host's ports. While the TCP connect() method connects to a port on a host using the full 3-way handshake, the SYN scan employs a modified handshake that only comprises a 2-way communication channel.



The SYN scan starts in the same way as the TCP connect() procedure, with the client sending a packet with the SYN flag set. If the port is open, the server responds with a SYN|ACK packet to the client. A RST (Reset) packet is sent to the client if the port is not open. A final ACK packet is never sent back to the server stating that the client has received the SYN|ACK packet from the server, which is where the SYN scan and the TCP connect() technique differ: In order to terminate the connection, a RST packet is sent to the server. A full TCP connection between the client and server is never created in this manner. Although this technology is relatively undetectable, it has a lot of disadvantages. For starters, port scan attempts using the half-open scan technique will be captured by a logger that is configured to log all SYN connection attempts. Because the half-open scan still employs a SYN packet as the initial step in the communication process, this is the case. Because the packets used in this form of scan must be custom-built, most operating systems require root or administrator access to the system functions. This is a safeguard put in place to prevent any user on the system from creating invalid packets. Because this form of scan is pretty well-known, most firewalls are set up to detect and prevent it.

4] FIN Scan

Scanner techniques and strategies evolve in tandem with the advancement of techniques and software in the fight against stealth scans. The security community is almost always playing catch-up to keep up with the attacker's level of insecurity in the progress of attacking and probing technologies. The FIN (Finish) scan is a response to the SYN scan's prospective logging capabilities. SYN packets to restricted ports are detected by some packet loggers and firewalls. The FIN scan sends a packet with only the FIN flag set. The host returns a RST flag if the port is closed, whereas an open port simply ignores the packet and returns nothing to the client. According

to the Transmission Control Protocol RFC, this is required behaviour. Attackers can probe open ports and perhaps elude detection by taking advantage of TCP's necessity for guaranteeing packets reach at their destination. Because a firewall or packet logger may be configured to detect SYN packets, a FIN packet may pass unnoticed.

5] Xmas Tree Scan

The Xmas tree scan, like the FIN scan, uses incorrect packet header flags to elicit a response from a host about open ports. There have been a number distinct ways used, all of which use the Xmas tree scan name. The Xmas tree scan is carried out by Nmap using three packet header flags: FIN, URG (Urgent), and PSH (Push). This scan is quite similar to the FIN scan; however, it has two additional flags set. Other Xmas tree scanners turn on all TCP header flags, which is where the term comes from. A closed port will return a RST packet, similar to FIN scan, however an open port would disregard the packet.

6] Null Scan

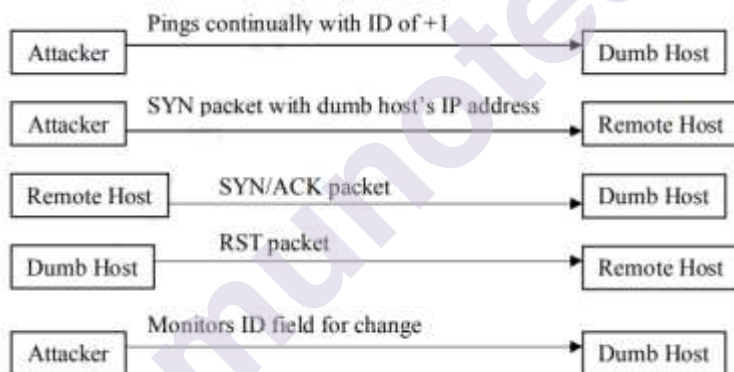
The Null scan has a similar reaction to the FIN and Xmas tree scans, but the packet header flags are different. Instead of turning on header flags that would cause the packet to be treated as an invalid packet by the host, the Null scan disables all header flags. If a port is closed, a RST packet is delivered to the client, but if the port is open, it is ignored. A number of operating systems, including Microsoft's, have ignored the RFC for TCP and implemented it in a way that differs from the standard. On Windows-based operating systems, as well as others like Cisco, HP/UX, and IRIX, the FIN, Xmas tree, and Null scans fail. Instead of ignoring the packet, these operating systems all send an RST if the port is open.

7] UDP Scan

There is some disagreement about the relative use of UDP scanning. On the one hand, UDP is a lot simpler protocol than TCP since it is not connection-oriented, i.e., it is not concerned with ensuring that packets reach their destination properly. UDP scanning, on the other hand, can be a highly valuable tool for locating open, undocumented UDP ports that a certain service might be using. UDP scanning can be used to scan for a variety of vulnerabilities. Without the user's awareness, programmes can easily open high UDP ports. Because these are mostly undocumented, using UDP scanning to track them down makes it much easier. There is currently only one way for performing UDP scanning, which involves sending a 0 byte UDP packet to each port on the host machine. An ICMP port unreachable error will be returned if a port is closed; otherwise, the port will be assumed to be open.

The utilisation of a third-party computer that receives very little or no network traffic is used in the dumb scan method of stealth scanning. A dumb host is another name for this third party. Attackers commonly check for these PCs on cable modem subnets, looking for Windows-based computers that have been left on overnight. A utility to produce modified TCP packets as well as a ping utility are required for the dumb host approach of stealth scanning. The process for dumb scanning that follows is simple yet incredibly effective. To begin, the attacker sends a series of ICMP pings to the dumb host with the ID +1. Second, the attacker sends a faked SYN packet to the host, using the IP address of the dumb host instead of his or her own. The attacker specifies the port he wants to scan as the destination port. Because the dumb host's IP is included in the TCP packet, any response to a connection request will be transmitted back to the dumb host. The dumb host's continual pinging exposes whether or not the port is open on the host. The ID number will typically increase if the port is open, but it will most likely remain at +1 if the port is closed.

Procedure:



The dumb scan is both effective and undetectable. Connection attempts are hidden and most logging features of an intrusion detection system are blocked when a third party is used. Because no information is sent directly from the remote host to the attacker's PC, this is the case.

4.7 PORT SCANNING COUNTERMEASURES

How can you prevent banners from being snatched from publicly accessible resources? You have a few different alternatives to choose from.

First, disable or alter the banner displayed by the server. Given that we've been looking at a variety of services, it's worth mentioning that many of them can have their information updated. For example, in Internet Information Server (IIS), the contents of the banner can be removed or changed so that the system does not appear the same to scans or banner

grabs. This information can be removed using tools like IIS Lockdown, ServerMask, and others.

Second, file extensions can be hidden on systems such as web servers. The goal of this strategy is to mask the technology that is utilised to create web pages. By looking at the file extensions of technologies like ASP.NET and JavaServer Pages (JSP), you can quickly identify them. Removing this detail adds another barrier for an attacker to overcome in order to gain access to a server's inner workings. PageXchanger for IIS, for example, is meant to aid in the removal of page extensions.

4.8 IDS EVASION TECHNIQUES

An intrusion detection system (IDS) is designed to safeguard a system's confidentiality, integrity, and availability. Intrusion detection systems (IDS) are classified as signature-based (SIDS) or anomaly-based (AIDS) and are used to detect certain concerns (AIDS). IDS might take the form of software or hardware.

Fragmentation, Flooding, Obfuscation, and Encryption are some of the strategies a cybercriminal could employ to avoid detection by an IDS. These approaches are difficult for conventional IDS to detect since they work around existing detection mechanisms.

1] Fragmentation

A packet is broken down into smaller pieces. The receiver node then reassembles the fragmented packets at the IP layer before passing them to the Application layer. To properly investigate fragmented traffic, the network detector must reassemble the fragments in the same way as they were at the time of fragmentation. The detector must store the data in memory and match the traffic against a signature database in order to restructure packets. Attackers exploit fragmentation overlap, overwrite, and timeouts to hide attacks as genuine traffic and avoid detection. To create a malicious packet, a fragmentation attack changes information in the constituent fractured packets with new information.



Figure: Fragment overwrite

The fragment overwrite is depicted in the diagram. The attacker generates Packet Fragment 3. The network intrusion detector must keep track of the condition of all packets in the traffic it is monitoring.

The detector's ability to maintain a condition of traffic for a longer period of time may be less than the destination host's

ability to do so. By delivering attack fragments over a long period of time, malware developers strive to exploit any flaws in the detection process.

2] Flooding

The attacker starts the attack by overwhelming the detector, which causes the control mechanism to fail. All traffic would be allowed if the detector failed. Spoofing the genuine User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) is a common way to cause flooding (ICMP). The cybercriminal's aberrant activities are concealed by traffic inundation. As a result, finding fraudulent packets in a large volume of traffic would be extremely challenging for an IDS.

3] Obfuscation

To avoid detection, obfuscation techniques might be utilised, which are methods of masking an attack by making the message difficult to read. Obfuscation is a phrase that refers to modifying programme code while keeping it functionally identical, with the goal of reducing detectability to any form of static analysis or reverse engineering procedure, as well as making it cryptic and less readable. Malware can evade current IDS thanks to this obfuscation.

Obfuscation tries to go around any restrictions in the signature database's capacity to replicate the way the computer host examines the data on the computer. The hexadecimal encoding format should be supported by an effective IDS, and these hexadecimal strings should be included in its set of attack signatures. The Unicode/UTF-8 standard allows a single character to be represented in a variety of ways. Double-encoded data may also be used by cybercriminals, increasing the number of signatures required to detect the attack dramatically.

SIDS uses signature matching to identify malware, with signatures created by human experts by converting malware from machine code to a symbolic language like Unicode. Cybercriminals, on the other hand, can utilise code obfuscation to get around IDSs.

4] Encryption

Encryption provides a variety of security benefits, including data confidentiality, integrity, and privacy. These security features are used by malware programmers to avoid detection and hide attacks that may target a computer system. An IDS, for example, cannot read attacks on encrypted protocols like HyperText Transfer Protocol Secure (HTTPS). If the IDS does not comprehend the encrypted traffic, it will be unable to match

it to the existing Database signatures. Examining encrypted traffic, on the other hand, makes it difficult for detectors to detect assaults. Packet content-based features, for example, have been widely used to distinguish malware from normal traffic, but they can't be used as easily if the packet is encrypted.

These difficulties encourage investigators to employ statistical network flow aspects that are not dependent on packet content. As a result, malware might potentially be detected in ordinary traffic.

4.9 BANNER GRABBING AND ITS TOOLS

Banner grabbing is a technique used by ethical hackers to gather information about the services operating on a system. It is highly valuable throughout the evaluation phase. The technique is usually carried out by utilising Telnet to get banner information about the target that indicates the service's nature.

A service returns a banner to the requesting programme to provide information about the service. The type of server software, version number, when it was last modified, and other information can be revealed by the banner, but in the case of HTTP, it can include the type of server software, version number, and similar information.

In many circumstances, Telnet is the preferred client for getting this data. Although there are other options, we'll concentrate on Telnet because it's the most popular and straightforward. Because most operating systems include the capacity to establish Telnet sessions, this is one of the most used methods of banner snatching. Banners are grabbed by connecting to a host and then submitting a request to a port connected with a certain service, such as port 80 for HTTP, whether using Telnet or another application.

So, how do you get a banner from a machine using Telnet? To pull the services banner, open a Telnet connection to a remote client using the following command:

```
telnet < ip address> : <port> HEAD / HTTP/1.1
```

Use GET instead of HEAD to get both the page and the headers. Use GET / HTTP/1.1 (or HEAD / HTTP/1.1) to get the root document.

Telnet is not the only mechanism for gathering this data, but it is the most basic and straightforward. Here are some other tools you should look into:

- **Netcraft:** It is a web-based utility for gathering information about servers and web servers. This tool was previously mentioned in relation to the footprinting process, but it is equally relevant here.
- **Xprobe:** It is a Linux utility that can acquire system information and pass it on to the collector.

- **pof:** This programme is only accessible on the Linux platform, and it analyses the traffic flowing from client to server. It offers real-time traffic analysis that may be seen onscreen or saved to a file for further review.
- **Maltego:** This application, which is available for Linux and Windows, allows you to not only collect data but also see the links between items. This software can view web server information as well as the technologies that allows a website to function.

4.10 VULNERABILITY SCANNING

Vulnerability scanners are a type of automated tool that detects flaws and vulnerabilities in operating systems and applications. This is accomplished through inspecting coding, ports, variables, banners, and a variety of other potential sources of error. A vulnerability scanner is designed to help companies determine whether they are vulnerable to attack and, if so, what has to be done to eliminate the vulnerability. Vulnerability scanners can analyse complete operating environments, including networks and virtual machines, in addition to software applications.

Vulnerability scanners can be quite useful, but they do have some disadvantages. The scanners are programmed to check for a specific set of known problems, and if they don't find them, they may provide the false impression that there are none. As a result, it is prudent to double-check the outcomes of these applications. Although vulnerability scanners are designed for genuine users who want to make sure their machine or network is secure, attackers may exploit them to further their own goals. An attacker can find out exactly what parts of the network are simple to break into by doing a vulnerability scan.

Vulnerability scanners are only discussed here to discuss them in relation to the other scanning techniques. Popular vulnerability scanners include Nessus, OpenVAS, Nexpose, Retina, and a few others, similar to nmap.

4.11 PROXY SERVERS

Every computer connected to the internet has an IP (Internet Protocol) address that uniquely identifies it. A proxy server, on the other hand, is a network machine with its own IP address. However, there are situations when we need to access restricted websites or servers and do not want to reveal our identity (IP address). The proxy server is activated in such a situation. Using a proxy server, we may achieve the same result. It offers various levels of functionality, security, and privacy, depending on the use case, organisational demands, or policies. In this section, we'll look at what a proxy server is, the many types of proxy servers, their benefits, why they're needed, and how they work.

4.11.1 Proxy Server

The proxy server is a computer connected to the internet that takes client requests and forwards them to the destination server. It functions as a link between the user and the internet. It has its own Internet Protocol (IP) address. It isolates the client and web server from the rest of the network.

To put it another way, a proxy server allows us to access any website using a different IP address. It acts as a link between users and the websites or servers that are being targeted. It gathers and distributes data in response to user requests. A proxy server's most crucial feature is that it does not encrypt traffic.

A proxy server serves two primary functions:

- To keep the system's origins hidden.
- For speeding up access to a resource through caching technique.

4.11.2 Mechanism of Proxy Server

The proxy server's mechanism is depicted in the diagram below

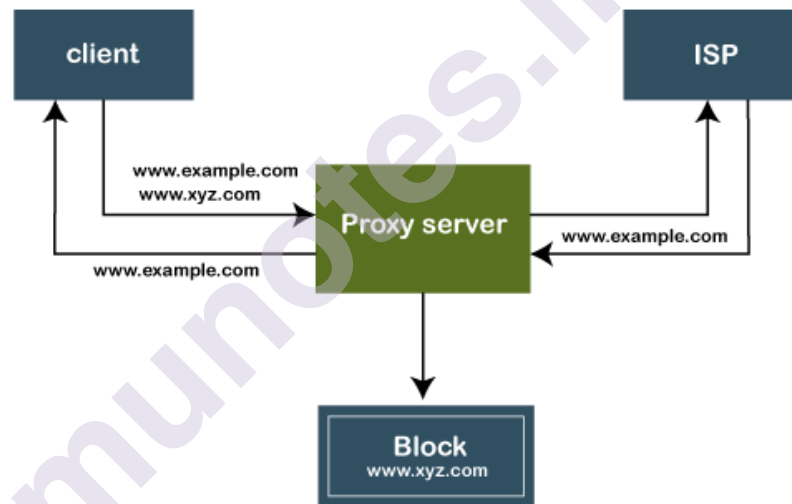


Figure: Mechanism of Proxy Server

The proxy server accepts the client's request and responds according to the following criteria:

- 1] If the requested data or page is already in the proxy server's local cache, the client is not required to retrieve it.
- 2] The proxy server passes the request to the target server if the requested data or page does not exist in the local cache.
- 3] The responses are transferred to the client and cached by the proxy servers.

As a result, the proxy server can be described as both a client and a server.



Figure: Communication without proxy server



Figure: Communication with proxy server

4.11.3 Types of Proxy Server

Proxy servers come in a variety of types. Forward and reverse proxy servers are the two most common types of proxy servers. The other proxy server comes with its own set of features and benefits. Let's take a closer look at each one.

- Open or forward proxy server:** The most well-known sort of intermediary worker that is accessed by the client is the open or forward proxy server. An open or forward proxy server is a type of intermediary that receives requests from web clients and then browses destinations to acquire the requested data. After gathering data from websites, it sends the information straight to internet users. It gets around the authorities' firewall. The configuration of a forward proxy is shown in the image below.

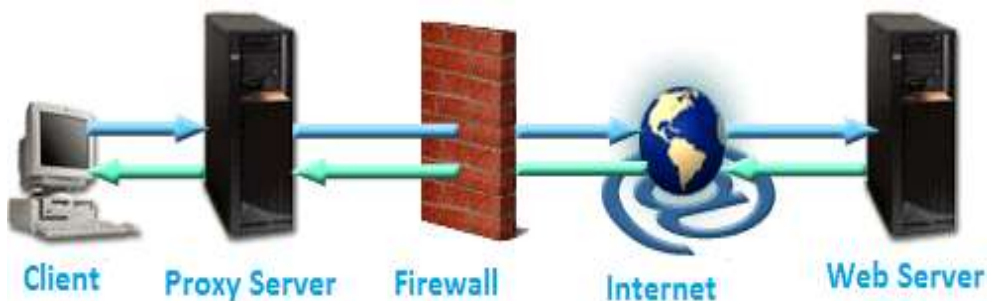


Figure: Forward proxy server

- **Reverse proxy server:** A reverse proxy server is one that is installed near a number of other internal resources. It validated and processed a transaction without requiring direct communication between the clients. Varnish and Squid are the most common reverse proxies. The reverse proxy configuration is shown in the image below.

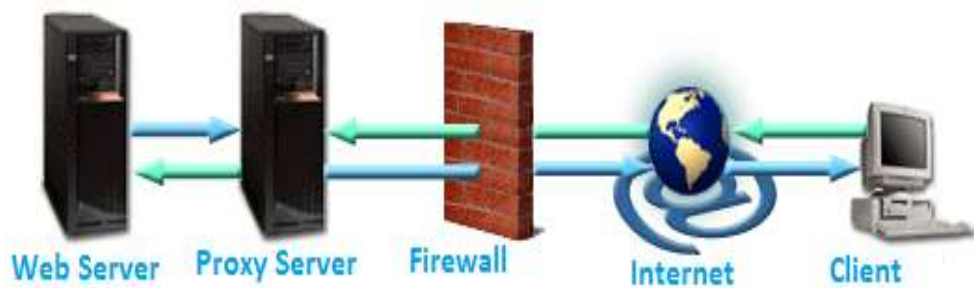


Figure: Reverse proxy server

- **Split Proxy Server:** It consists of two programmes that are installed on two separate machines.
- **Transparent Proxy:** This is a proxy server that only modifies requests and responses to the extent necessary for proxy authentication and identity. It connects to the internet via port 80.
- **Non-Transparent Proxy:** This is an intermediary that modifies the solicitation response in order to provide the client with additional services. Web requests are sent directly from the intermediary, regardless of the worker from whom they originated.
- **Hostile Proxy:** This type of proxy is used to eavesdrop in on data traffic between the client system and the web.
- **Intercepting Proxy Server:** It is a proxy server that also acts as a gateway. It is often used in enterprises to prevent employees from circumventing acceptable use policies and to make management easier.
- **Forced proxy server** Intercepting and non-intercepting policies are combined in a forced proxy server.
- **Caching Proxy Server:** Caching is the process of serving client requests using previously saved content from previous requests instead of connecting with the specified server.
- **Web Proxy Server:** A web proxy server is a proxy that is used to access the internet.
- **Anonymous Proxy:** The server makes an attempt to anonymize web browsing.

- **Socks Proxy:** It is a standard developed by the IETF (Internet Engineering Task Force). It's similar to a proxy system that allows proxy-aware programmes to run. It prevents external network components from collecting information about the client who initiated the request.
- **The proxy server:** It does not include the proxy server type and the client IP address in the request header is known as a high anonymity proxy. Clients who use the proxy are untraceable.
- **Rotating proxy:** Each client connected to it is assigned a unique IP address through a rotating proxy. It's great for people that conduct a lot of web scraping on a regular basis. It enables us to return to the same website on a regular basis. As a result, employing the rotating proxy necessitates greater attention.
- **SSL Proxy Server:** This server decrypts data sent between the client and the server. It means that data is encrypted both ways. Because proxy hides the fact that it exists from both the client and the server. It is best suited for enterprises who want to improve their threat prevention. The encrypted content is not cached in SSL proxy.
- **A shared proxy server:** This is utilised by multiple users at the same time. It assigns the client an IP address that can be shared with other clients. It also allows users to choose the place from which they want to do their search. It's perfect for people who don't want to spend a lot of money on a fast internet connection. It has the benefit of being inexpensive. The negative is that a user may be held responsible for the misdeeds of others. As a result, the user may be barred from the site.
- **Public Proxy:** A public proxy can be used for free. It's ideal for users who are concerned about cost but not about security or speed. It moves at a leisurely pace most of the time. Using a public proxy puts the user at danger because information on the internet can be viewed by others.
- **Residential Proxy:** It gives a specific device an IP address. All of the client's requests were routed through that device. It's perfect for people who wish to double-check advertising that appear on their websites. We can filter undesirable and questionable adverts from competitors using the residential proxy server. The residential proxy server is more dependable than other proxy servers.
- **Distorting Proxy:** It differs from others in that it identifies itself as a proxy for a website while concealing its own identity. By supplying an erroneous IP address, the actual IP address is modified. It's ideal for customers who don't want to reveal their location when browsing.
- **Data Center Proxy:** This is a unique form of proxy that is independent of the ISP. Other corporations provide it through a data centre. Physical data centres are where these servers can be found. It's

perfect for clients who need answers quickly. It does not offer complete anonymity. As a result, it poses a significant risk to customer information.

- **HTTP Proxy:** HTTP proxies are proxy servers that save cache files from websites that are visited. Because cached files are stored in local memory, it saves time and improves performance. If the user wishes to access the same file again, the proxy gives it without the user having to browse the pages.

4.11.4 Advantages of Proxy Server

The following are some of the advantages of using a proxy server:

- It makes the user's security and privacy more secure.
- It conceals the user's identity (IP address).
- It regulates traffic and prevents collisions.
- By caching files and compressing incoming information, it also saves bandwidth.
- Defend our network from malicious software.
- Access to the restricted material is granted.

4.11.5 Need of Proxy Server

- It lowers the risk of data breaches.
- It adds an extra layer of security between the server and the outside world.
- It also safeguards against cyber-attacks.
- It does it by filtering the requests.

4.11.6 Working of Proxy Server

The proxy server, as previously stated, has its own IP address and serves as a gateway between the client and the internet. The client's computer is aware of the proxy server's IP address. When a client makes an internet request, the request is redirected to the proxy. The proxy server then receives the response from the destination or targeted server/site and forwards the page's data to the client's browser (Chrome, Safari, etc.).

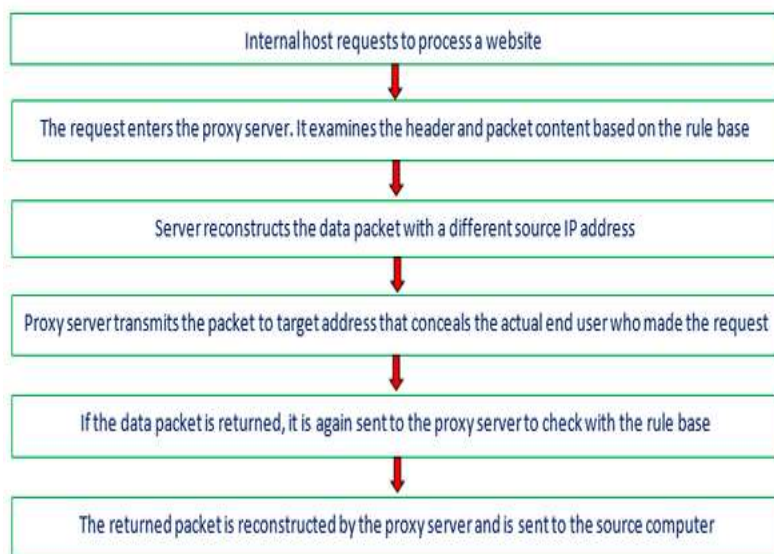
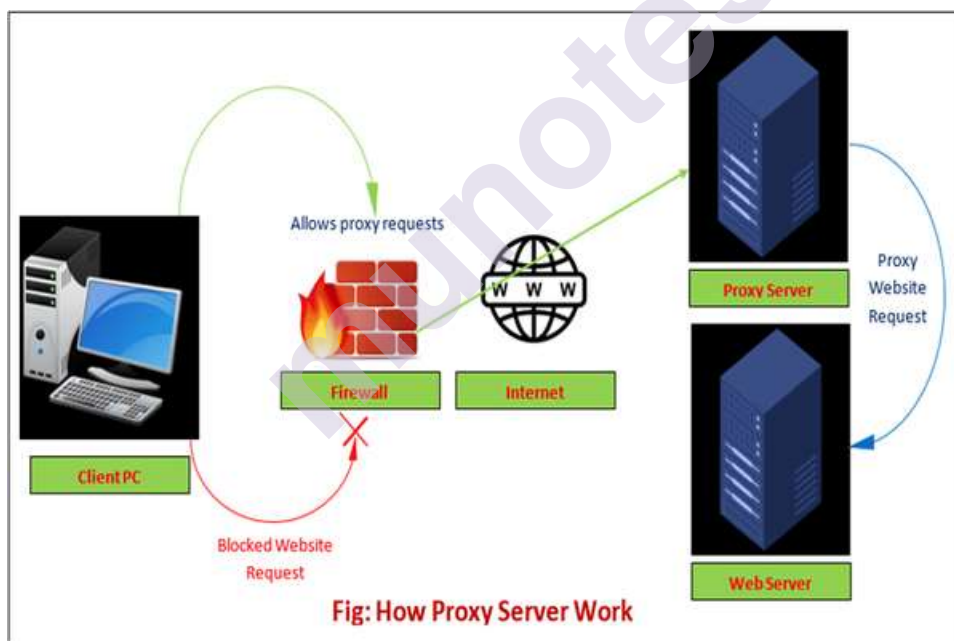


Figure: Working of Proxy Server

In general, the proxy server accesses the targeted site on behalf of the client and collects all requested information before forwarding it to the user (client). The proxy server's operation is depicted in the diagram below



4.12 ANONYMIZERS

An anonymizer, often known as an anonymous proxy, is a tool that aims to make online behaviour untraceable. It's a proxy server computer that serves as a middleman and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user's behalf, masking the client computer's identifying information to protect personal information.

Anonymizers are useful for a variety of reasons. Anonymizers aid in the reduction of danger. They can be used to safeguard search records from public publication or to prevent identity theft. The internet is heavily restricted in several nations. Anonymizers can assist in providing full access to any internet information, but they cannot protect users from being penalized for visiting the Anonymizer website. Furthermore, people are concerned of falling into a government-set trap because knowledge regarding Anonymizer websites is restricted in these countries.

With the rise of specialized marketing and customised information on the internet, anonymizers are also utilised by those who want to obtain objective information. Large news organisations, such as CNN, for example, segment their audiences by location and provide different information to different audiences. Websites like YouTube use information about the most recent videos viewed on a computer to suggest "suggested" videos, and the majority of internet targeted marketing is done by showing ads tailored to that region. Anonymizers are used to prevent this type of targeting and provide a more objective view of data.

- **Types of Anonymizers**

- 1] **Protocol-specific anonymizers:** Anonymizers are sometimes designed to only work with a single protocol. The benefit is that no additional software is required. The surgery is carried out in the following manner: The user establishes a connection with the anonymizer. Anonymizer commands are contained within a standard message. The anonymizer then connects to the inbound command's specified resource and sends the message with the command stripped off. An anonymous e-mail remailer is an example of a protocol-specific anonymizer. Web proxies and bouncers for FTP and IRC are also worth mentioning.
- 2] **Protocol independent anonymizers:** A tunnel to an anonymizer can be used to achieve protocol independence. The technology required for this varies. SOCKS, PPTP, and OpenVPN are some of the protocols utilised by anonymizer services. In this situation, either the desired programme must support the tunnelling protocol, or software to compel all connections through the tunnel must be installed. Unlike telnet, many web browsers, FTP, and IRC clients support SOCKS.

4.13 IP SPOOFING AND ITS COUNTERMEASURES

4.13.1 What is IP spoofing?

IP spoofing, also known as IP address spoofing, is the production of IP packets with a bogus source IP address in order to mimic another computer system. Cybercriminals can use IP spoofing to carry out malicious acts without being detected. Stealing your data, infecting your device with malware, or crashing your server are all possibilities.

IP spoofing has kept security experts on their toes for years, making cyber-security one of the most important areas of IT. The ease with which DoS or DDoS attacks may be launched makes IP manipulation an appealing tool for today's cybercriminals. As a result, there has long been a requirement for internet service providers to perform targeted filtering of outbound data traffic, where packets with sources outside the underlying network are logged and deleted.

The improved characteristics of Internet Protocol Version 6: IPv6 are another cause for the ignorance. Although IPv4 is still widely used, its upgraded version now provides a variety of configurable authentication and encryption options for header and data packets, which will help to avoid future spoofing.

Internet users who want to take the initiative and set up their own protection systems have options to prevent attackers from faking their IP addresses and appropriating others. These are centred on the following two metrics:

- Configure your router or security gateway with a robust packet filtering solution. If inbound data packets contain source addresses of devices on your network, this should be analysed and discarded. Outgoing packets with sender address outside the network should be monitored and filtered as well. According to security experts, this is the responsibility of the internet service provider.
- Host-based authentication solutions should be avoided. Make sure that all of your login methods use encrypted connections. This reduces the possibility of an IP spoofing attack on your network while also establishing the appropriate security requirements.
- IP spoofing is nearly impossible to detect for end users. However, they can reduce the risk of other sorts of spoofing by using secure encryption methods like HTTPS and only visiting websites that employ them. ICMP should be filtered. Use a random sequence number, lower the initial TTLs, encrypt the data, and don't rely on IP for authentication.

Obviously, if outdated operating systems and network devices are still in use, these should be replaced as well. Not only will this improve protection against IP spoofing, but it will also fix a number of other security holes.

4.14 SUMMARY

You may undertake network scanning with a far more targeted and purposeful strategy if you use the information acquired during the footprinting phase. Because you are interacting directly with a target, scanning is an aggressive way to acquiring information about a system. You're scouring the network and systems for everything you can find.

Vulnerability scans, network mapping, port scans, and OS fingerprinting provide information about the system and indicate possible testing paths.

4.15 LIST OF REFERENCES

- **Reference books**

- 1] Manthan Desai Basics of ethical hacking for beginners.
- 2] SunitBelapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives.
- 3] Sean-Philip Oriyano, Sybex, Certified Ethical Hacker Study Guide v9, Study Guide Edition, 2016.

- **Web References**

- 1] https://subscription.packtpub.com/book/networking_and_servers/9781788995177/4/ch04/v1/sec37/full-opentcp-connect-scans
- 2] <https://selflearning.io/study-material/website-penetration-testing/website-penetration-testing/chapter-5-scanning/tcp-connect-full-open-scanning>
- 3] <http://www.csc.villanova.edu/~nadi/csc8580/S11/nmap-tutorial.pdf>
- 4] “Port Numbers.” May 28, 2002. URL: <http://www.iana.org/assignments/port-numbers> (May 30, 2002)
- 5] Maimon, Uriel. “Port Scanning without the SYN flag.” November 8, 1996. URL: <http://www.phrack.org/show.php?p=49&a=15> (May 30, 2002)
- 6] Fyodor. “NMAP Network Security Scanner Man Page.” URL: http://www.insecure.org/nmap/nmap_manpage.html (May 29, 2002)
- 7] “OSDEM Presentation - Network Reconnaissance Techniques”
URL: http://www.insecure.org/nmap/OSDEM_Presentation/ (May 30, 2002)
- 8] “CERT® Incident Note IN-98.04” September 29, 1998.
URL: http://www.cert.org/incident_notes/IN-98.04.html (May 30, 2002)
- 9] “RFC 793 – Transmission Control Protocol.” September 1981.
URL: <http://www.faqs.org/rfcs/rfc793.html> (May 29, 2002)
- 10] Natas. “In Regards to Secured Hosts.”
URL: <http://www.80p.com/sec666/inregards.txt> (June 10, 2002)

- 11] “IP Spoofing.” (2002)
URL: http://www.webopedia.com/TERM/I/IP_spoofing.html (May 30, 2002)
- 12] Whalen, Sean. “An Introduction to Arp Spoofing.” April 2001.
URL:
http://packetstormsecurity.org/papers/protocols/intro_to_arp_spoofing.pdf (May 30, 2002)
- 13] Mateti, Prabhaker. “Port Scanning.” 2001.
URL: <http://www.cs.wright.edu/~pmateti/Courses/499/Probing/> (June 3, 2002)
- 14] “A New Stealth Port Scanning Method” December, 1998
URL:
http://www.securiteam.com/securitynews/A_new_stealth_port_scanning_method.html (June 3, 2002)

4.16 UNIT END EXERCISES

- 1] Define scanning and state its types.
- 2] Explain in detail the concept of scanning live system.
- 3] Write a note on Stealth scan.
- 4] Explain in brief about the countermeasures of port scanning.
- 5] Define intrusion detection system and state its evasion techniques.
- 6] Write a detailed note on fragmentation
- 7] Explain the concept of flooding
- 8] What do you mean by obfuscation?
- 9] What is banner grabbing? State its tools.
- 10] Explain the concept of vulnerability scanning.
- 11] Write a note on proxy server.
- 13] Define and state the types of Anonymizers.
- 14] Write a detailed note on IP spoofing and its countermeasures

ENUMERATION AND SNIFFING

Unit Structure

- 5.0 Objectives
- 5.1 Introduction
- 5.2 What is Enumeration?
- 5.3 Enumeration techniques
- 5.4 Enumeration types
- 5.5 Enumeration countermeasures
- 5.6 What is Sniffing?
- 5.7 Packet sniffing
 - 5.7.1 What is packet sniffing?
 - 5.7.2 Types of packet sniffing
 - 5.7.3 What type of information does packet sniffing gather?
- 5.8 Precautionary Measures on Sniffing Attacks
- 5.9 How does packet sniffing works?
- 5.10 ARP spoofing
 - 5.10.1 What is ARP spoofing?
 - 5.10.2 Steps of an ARP spoofing attack
 - 5.10.3 What ARP spoofing is used for
 - 5.10.4 How to detect ARP spoofing?
 - 5.10.5 Prevention of ARP spoofing
- 5.11 MAC flooding
 - 5.11.1 What is MAC flooding?
 - 5.11.2 How to prevent the MAC flooding attack?
- 5.12 Active and Passive sniffing / Types of sniffing attacks
- 5.13 Sniffing countermeasures
- 5.14 Sniffing detection techniques
 - 5.14.1 How to detect sniffing
 - 5.14.2 Sniffer detection technique
- 5.15 Summary
- 5.16 List of References
- 5.17 Unit End Exercises

5.0 OBJECTIVES

- To understand the concept of enumeration and the ways to tackle them
- To study the detailing and measures of sniffing
- Provide a thorough awareness of cyber security challenges, dangers, and concerns, as well as countermeasures to prevent hacking
- Various tools, techniques and its countermeasure involved in ethical hacking

5.1 INTRODUCTION

It's time to start looking at the target system more closely in order to use the information to hack into it. Enumeration uses a variety of tools and strategies to extract data from a target system, including actively connecting to the system.

Scanning allowed us to locate hosts and determine which ports were open and closed on each one. We now have potential entry points into a system that can be used to learn more about the targeted host or hosts, thanks to this knowledge. Consider enumeration the last step in the process before we start chipping away at a system's armour to get a good look at the target.

5.2 WHAT IS ENUMERATION?

Enumeration is the process of extracting data from a target system in order to learn more about the system's setup and surroundings. Depending on the OS, it is often feasible to extract information such as users, machine names, shares, and services from a system, as well as other data.

Unlike earlier phases, however, you will be making active connections to a system in order to obtain a wide range of data. With this in mind, you should consider enumeration to be a phase with a significantly higher risk of being discovered. Make an extra effort to be exact to avoid being detected.

So, what's the point of making active connections to a target? Simply put, it's the only way to learn more information beyond what we've already learned from footprinting and scanning. We can now conduct directed searches at a host using these active connections, which will extract a lot more data. We can properly examine the system's strengths and flaws once we've gathered enough data. The following types of information are commonly acquired at this phase:

- Shared resources and resources on the network
- Individuals and groups
- Tables of routing
- Auditing and service configurations
- Names of machines
- Banners and applications
- Details about SNMP and DNS

5.3 ENUMERATION TECHNIQUES

So, what are the alternatives accessible to an enumeration attacker? Let's take a look at the techniques.

- **Getting Username and Domain Name Information from Email IDs:** This method is used to get username and domain name information from an email address or ID. There are two pieces to an email address: The username is the first portion before the @, and the domain name is the second part after the @.
- **Using Default Passwords to Get Information:** Every device has default settings, and default passwords are included in this group. It's not uncommon to see default settings left in place, either partially or entirely, allowing an attacker to simply get access to the system and collect data as needed.
- **Using Brute-Force Attacks on Directory Services:** A directory service is a database that stores information that is needed to manage a network. As a result, it's a prime target for an attacker trying to gather a lot of data on a given environment. Many directories are subject to input verification flaws and other security flaws that could be used to identify and compromise user accounts.
- **SNMP Exploitation:** An attacker who can guess the strings and utilise them to obtain usernames can use the Simple Network Management Protocol (SNMP).
- **Exploiting SMTP:** An attacker can utilise the Simple Mail Transport Protocol (SMTP) to connect to an SMTP server and obtain information about usernames.
- **Working with DNS Zone Transfers:** A DNS zone transfer is a common occurrence, but the consequences can be disastrous if this information slips into the wrong hands. A zone transfer is intended to update DNS servers with the most up-to-date information; however, the zone contains data that could map out the network, providing useful information about the environment's structure.
- **User Groups Capture:** This technique entails extracting user accounts from specified groups, storing the results, and assessing whether the session accounts are in the group.
- **Retrieving System Policy Settings:** In business and other environments, policy settings or something similar are usually in place that dictate how security and other issues are addressed. These parameters can occasionally be obtained during the enumeration step, allowing you to gain a better understanding of your target.

Following are several categories of Enumerations that are discussed in this section.

1] NetBIOS (Network Basic Input Output System) Enumeration:

- The NetBIOS name is a unique 16 ASCII character string that is used to identify organisation devices over TCP/IP. The gadget name is 15 characters long, and the sixteenth character is saved for the administration or name record type.
- NetBIOS enumeration is used by programmers to collect a list of PCs that belong to a certain domain, a list of offers on individual hosts in the organisation, and strategies and passwords.
- Microsoft does not support the NetBIOS name objective in Internet Protocol Version 6.
- Exploiting the NetBIOS API is the first step in designing a Windows framework. It began as an Application Programming Interface (API) for accessing LAN assets through custom programming. For document and printer sharing, Windows uses NetBIOS.
- A hacker who discovers a Windows OS with port 139 open can check whether assets are accessible or visible on the remote framework. To count the NetBIOS names, the remote framework most likely enabled document and printer sharing. This type of enumeration may enable the programmer to read or communicate with a remote PC system, depending on the availability of offers, or to launch a DoS.

2] SNMP (Simple Network Management Protocol) devices Enumeration:

- SNMP enumeration is a process of using SNMP to specify client records and devices on an objective framework. A manager and a specialist are included in SNMP; specialists are installed on each organisation device, while the trough is installed on a separate PC.
- To access and design the SNMP specialist from the administrative station, SNMP has two passwords. Of course, the Read Community String is open to the public; it allows for a study of the gadget/framework configuration. The read/write persons group string is, of course, private; it allows for far-reaching changes to the arrangement.
- Hackers use these default network strings to erase information about a device. Hackers use SNMP to extract information about

organisation assets such as has, switches, gadgets, shares, and so on, as well as network data such as ARP tables, routing tables, and traffic.

- SNMP makes use of dispersed engineering, which includes SNMP agents, managers, and a few other components. GetRequest, GetNextRequest, GetResponse, SetRequest, and Trap are all SNMP orders.
- To screen, assess, and research security risks, SNMP Enumeration tools are used to check a single IP address or a range of IP addresses of SNMP enabled enterprise gadgets. NetScanTolls Pro, SoftPerfect Network Scanner, SNMP Informant, and other similar tools are examples of this type of software.

3] LDAP Enumeration

- The Lightweight Directory Access Protocol (LDAP) is an Internet protocol for accessing registry administrations that are spread out throughout the internet.
- Registry administrations can provide any synchronised collection of records, usually in a hierarchical and logical form, such as a corporate email index.
- An LDAP meeting begins when a customer connects to a Directory System Agent on TCP port 389 and then sends an activity solicitation to the DSA.
- Basic Encoding Rules are used to send data between the client and the worker.
- A programmer queries the LDAP administration to gather information such as significant usernames, addresses, division details, and so on that can be utilised to launch attacks.
- There are a variety of LDAP enumeration tools that access the registry posts in Active Directory or other catalogue administrations. Assailants can use these devices to identify data from various LDAP employees, such as significant usernames, addresses, division peculiarities, and so on.
- LDAP Admin Tool, Active Directory Explorer, LDAP Admin, and others are examples of these kind of tools.

4] NTP Enumeration

- The Network Time Protocol is used to synchronise the clocks of many computers.
- Its primary mode of communication is through UDP port 123.

- Over the internet, NTP can check time to within 10 milliseconds (1/100 second).
- Under ideal conditions, it can achieve correctness of 200 microseconds or greater in a neighbourhood.
- When it comes to security, executives frequently neglect the NTP worker. However, when properly questioned, it can provide vital organisational data to the programmers.
- Hackers question NTP workers to gather important information, such as a list of hosts affiliated with NTP workers, clients' IP addresses in an organisation, their framework names and Oss, and internal IPs if NTP worker is in the demilitarised zone.
- NTP enumeration tools are used to monitor the performance of SNTP and NTP workers in the company, as well as to configure and check availability from the time customer to the NTP workers.

5] SMTP Enumeration

- SMTP with POP3 and IMAP are common mail frameworks that enable clients to save messages in the worker letterbox and download them from the mainframe once in a while.
- Mail Exchange (MX) workers are used by SMTP to organise mail across DNS. TCP port 25 is used.
- VRFY, EXPN, and RCPT TO are three built-in instructions in SMTP.
- These servers respond to commands differently for valid and invalid users, allowing us to identify valid users on SMTP servers.
- Hackers can legitimately connect to SMTP using telnet and get a list of important clients on the mainframe.
- Hackers can enumerate SMTP servers using command-line utilities like telnet, netcat, and others, as well as software like Metasploit, Nmap, and NetScanTools Pro.

6] DNS Enumeration using Zone Transfer

- It's a cycle for locating a DNS worker and an objective organization's records.
- A hacker can get important organisation data such as DNS worker names, hostnames, machine names, usernames, IP addresses, and so on.

- A hacker tries to acquire a copy of the whole zone file for a domain from the DNS server in DNS Zone Transfer enumeration.
- To carry out a zone transfer, the hacker poses as a client and submits a zone transfer request to the DNS server, which then provides you a section of its database as a zone. This zone could provide a lot of information regarding how DNS zones are organised.

7] IPsec Enumeration

- To ensure the correspondence between virtual private organisation (VPN) end points, IPsec uses ESP (Encapsulation Security Payload), AH (Authentication Header), and IKE (Internet Key Exchange).
- In a VPN environment, most IPsec-based VPNs employ the Internet Security Association and Key Management Protocol, which is part of IKE, to create, manage, and delete Security Associations and cryptographic keys.
- The presence of a VPN tunnel can be demonstrated simply by looking for ISAKMP on UDP port 500.
- Hackers can conduct more investigation using a device such as IKE-output to identify sensitive information such as encryption and hashing calculations, authentication type, key conveyance calculation, and so on.

8] VoIP (Voice over IP) Enumeration

- SIP (Session Initiation Protocol) is a protocol used by VoIP that allows voice and video communications to be made over an IP network.
- UDP/TCP ports 2000, 2001, 5050, and 5061 are commonly used in SIP management.
- Enumeration of VoIP gateways/servers, IP-PBX systems, client software, and user extensions provides sensitive information.
- This information can be used to perform DoS, Session Hijacking, Caller ID Spoofing, Eavesdropping, Spamming over Internet Telephony, VoIP phishing, and other VoIP assaults.

9] RPC Enumeration

- Customers and employees can communicate in dispersed customer/worker programmes using Remote Procedure Call.
- Aggressors can identify any weak administrations on these administration ports by counting RPC endpoints.
- This portmapper is sorted on a regular basis in networks protected by firewalls and other security measures. Hackers use this technique to identify RPC administrations that are available to coordinate an attack by filtering high port accesses.

- This type of enumeration is one of the most important procedures in doing an enumeration. This displays a list of users together with information such as username, hostname, session start date and time, and so on.
- Users, rwho, finger, and other command-line applications can be used to enumerate Linux users.

11] SMB Enumeration

- Any pen-tester should be familiar with the SMB list. Before we can learn how to count SMB, we must first understand what SMB is. The acronym SMB stands for server message block.
- It's a standard for exchanging assets such as records, printers, and, in general, any item that the server should be able to get or access. It runs on either port 445 or port 139, depending on the server.
- It's really easy to use with Windows, so users don't need to do anything special aside from the basic setup. In any case, it's a little unusual in Linux. Because Linux doesn't use the SMB convention locally, you'll need to install a samba server to make it work.
- Clearly, some type of validation, such as a login and secret word, will be put up, and only specific content will be made shareable. So everyone can get to everything, which is a great confirmation.
- The most obvious flaw is the use of default certificates that are practically guessable, and in some cases, no verification at all, for access to the server's most important assets. For clients who need to access assets via SMB, administrators should make it a point to use strong passwords. The samba server is the next blemish. Samba servers have a reputation for being extremely susceptible.

5.5 ENUMERATION COUNTERMEASURES

1] SNMP

- Turn off the SNMP service or remove the SNMP agent.
- If you can't turn off SNMP, change the name of the default community string.
- Upgrade to SNMP3 for password and message encryption.
- Add the Group Policy security option "Additional restrictions for anonymous connections" to your security settings.
- Access to null session pipes, null session shares, and IPSec filtering should all be limited.

2] DNS

- Allow DNS zone transfers to untrusted hosts to be disabled.
- Ensure that private hosts and their IP addresses are not disclosed in the public DNS server's DNS zone files.
- Use premium DNS registration services to keep sensitive data like HINFO out of the public eye.
- To avoid social engineering attacks, use regular network admin contacts for DNS registrations.

3] SMTP

Configure SMTP servers so that:

- Emails sent to unknown recipients should be ignored.
- In mail answers, do not provide sensitive mail server and local host information.
- Turn off the open relay function.

4] LDAP

- LDAP traffic is sent unencrypted by default; utilise SSL technology to encrypt the traffic.
- Enable account lockout and choose a user name that isn't your email address.

5] SMB

- On web and DNS servers, disable the SMB protocol.
- Disable the SMB protocol on servers that are exposed to the internet.
- Disable the SMB protocol's TCP 139 and TCP 445 ports.
- The Windows Registry's RestrictNullSessAccess setting can be used to limit anonymous access.

5.6 WHAT IS SNIFFING?

Sniffers are tools that you can use as an ethical hacker to gather and scan traffic as it moves across a network. Sniffers are a broad category that includes any application that can capture packets. Sniffers capture traffic by enabling promiscuous mode on the linked network interface, regardless of the build, allowing them to capture all traffic, whether or not it is meant for them. When an interface is set to promiscuous mode, it does not distinguish between traffic destined for its address and all other traffic on the network, allowing you to record and analyse every packet.

Sniffing can be either active or passive. Passive sniffing is generally defined as any sort of sniffing in which traffic is observed but not manipulated in any manner. Passive sniffing essentially entails merely listening. Not only is traffic watched in active sniffing, but it may also be manipulated in some way by the attacking party. For your exam, be aware of the differences.

The basic options of most sniffer utilities are very constant across all versions. Whether it's a Linux-based programme or a Windows counterpart, this constancy holds true. We'll get into the types and specifics later, but first, let's take a look at the similarities. A main window on most sniffers shows the incoming packets and highlights or lists them appropriately. Unless you indicate otherwise by filters or other parameters, the listing is normally linear. In addition, there's usually a subpanel that gives you a closer look at the packet you've chosen. It's critical to become acquainted with your preferred sniffer because it will save you time and hassle in the long run. Having a strong understanding of a sniffer's core functionalities will also allow you to employ a variety of sniffers without too many issues. So, a sniffer's interface selection or activation choice normally starts the capture phase from here.

If you click the capture button, packets should appear in your capture window; if they don't, verify your network interface option. All sniffers allow you to choose from all of your computer's available interfaces. You can easily select a disconnected interface and sulk because your sniffer isn't working. Just double-check everything and you'll be rewarded with real-time traffic! Remember that a sniffer isn't just a pointless programme that lets you view just live traffic. A sniffer is a combination of tools that may provide you with an incredibly detailed and granular picture of what your (or their) network is doing from the inside out.

The relative and inherent insecurity of certain network protocols determines how good you are at sniffing. Protocols like the tried-and-true TCP/IP were never built with security in mind, and hence offer little in this regard. Sniffing is made simple by a number of protocols:

- **Telnet/rlogin:** Keystrokes including users and passwords, for example, can be easily intercepted.
- **HTTP:** Designed to transport data in the clear, without encryption, making it an ideal target for sniffing.
- **Simple Mail Transfer Protocol (SMTP):** This protocol is commonly used for email transfer and is efficient, however it does not include any anti-sniffing security.
- **NNTP:** All communication, including passwords and data, is sent in the clear via the Network News Transfer Protocol (NNTP).
- **POP:** Because passwords and usernames can be intercepted, the Post Office Protocol (POP) is designed to retrieve email from servers and does not include anti-sniffing protection.

- **FTP (File Transfer Protocol):** It is a protocol for sending and receiving files in which all transmissions are sent in clear text.
- **IMAP (Internet Message Access Protocol):** This is similar to SMTP in terms of operation and lack of security.

5.7 PACKET SNIFFING

Packet sniffing is a technique for detecting and observing packet data travelling across a network. Packet sniffing tools are used by network administrators to monitor and validate network traffic, but hackers may use similar tools for malicious purposes.

5.7.1 What is packet sniffing?

The technique of gathering, collecting, and logging some or all packets that transit through a computer network, regardless of how the packet is addressed, is known as packet sniffing. Every packet, or a determined selection of packets, can be gathered in this manner for subsequent analysis. As a network administrator, you can use the obtained data for a range of tasks, including bandwidth and traffic monitoring.

A packet sniffer, also known as a packet analyzer, is made up of two main components. The sniffer must first be connected to an existing network using a network adaptor. Second, software that allows you to log, view, or analyse the data that the device collects.

5.7.2 Types of packet sniffing

Packet sniffers are classified into two main types:

- **Hardware Packets Sniffers**

A hardware packet sniffer is a device that connects to a network and analyses it. When trying to see the activity of a specific network segment, a hardware packet sniffer comes in handy. A hardware packet sniffer can assure that no packets are lost owing to filtering, routing, or other deliberate or incidental causes by inserting directly into the physical network at the proper spot. A hardware packet sniffer either stores or sends the intercepted packets to a collector, which logs the data gathered by the hardware packet sniffer for further analysis.

- **Software Packets Sniffers**

Nowadays, the majority of packet sniffers are software-based. While any network interface connected to a network can receive all network traffic that passes across it, most are not. This setting is changed by a software packet sniffer, which causes the network interface to send all network traffic up the stack. For most network adapters, this is referred to as promiscuous mode. When a packet sniffer is in promiscuous mode, its capability is reduced to isolating, reassembling, and reporting any software packets that flow through

the interface, regardless of their destination addresses. All traffic that goes across the physical network interface is collected by software packet sniffers. That traffic is then logged and used in accordance with the software's packet sniffing requirements.

5.7.3 What type of information does packet sniffing gather?

Packet sniffing gathers each network transmission's full packet. Unencrypted packets can be reassembled and read in their entirety. Intercepted packets from a user accessing a website, for example, would contain the HTML and CSS for the web pages. Users logging onto network resources using unencrypted transmissions are renowned for exposing their username and password in plain text, which can be viewed in recorded packets.

5.8 PRECAUTIONARY MEASURES ON SNIFFING ATTACKS

Sniffing is a hacking technique used by hackers to collect sensitive information or steal identities. However, there are a few precautions that can be taken to avoid sniffing assaults. Let's have a look at some steps you can take to protect the security of your company's networks and systems.

- **Avoid using unencrypted networks:**

We frequently hear about bank data theft, in which criminals take a user's credit card or banking information and exploit it to make unauthorised modifications or purchases. That's because they've been targeted by sniffing attacks. It can happen if a user connects to an insecure Wi-Fi network. Furthermore, attackers utilise such insecure networks to install packet sniffers, which sniff and read every data sent across the network.

An attacker can also sniff network traffic by setting up a fake-free public Wi-Fi network. Remember to avoid free and unsecured public W-Fi the next time you see it.

- **Use a VPN to encrypt your message:**

Sniffing attacks can be avoided by encrypting all incoming and outgoing communications before exchanging them over a virtual private network (VPN). Encryption improves security and makes decrypting packet data more difficult for hackers.

- **Monitoring and scanning of the network**

Network administrators should scan and monitor their networks using bandwidth monitoring or device auditing to ensure that they are secure. As a result, this is a crucial strategy for optimising your network environment and detecting sniffing assaults.

Cybercriminals can break into any network without permission. Attackers can exploit and take data from your network even with the most sophisticated tactics and precautions in place. As a result, your company needs a competent staff of ethical hackers and network administrators who can infiltrate networks and run these checks on a regular basis to uncover network vulnerabilities.

- **Anti-virus software**

Using an updated anti-virus programme to combat sniffing could be advantageous.

- **Websites without encryption**

HTTPS website URLs are safe, however HTTP URLs do not guarantee that no one will be tracking your activities or data. To avoid being exposed to sniffing attacks, avoid visiting insecure websites.

- **Suite for Internet Security**

One of the most reliable strategies for preventing cyber attacks is to implement a full-fledged internet security suite for your business or personal systems.

- **Training**

It is recommended that the organization's workers be trained to properly inspect links and e-mail addresses before clicking on them or sending emails. Conducting training sessions to keep staff educated on cybersecurity threats, modes, and precautions has grown critical in recent years.

- **Endpoint Security**

There are networks that are bridged to devices remotely. Connecting laptops, PCs, and mobile devices to corporate networks opens the door to security dangers. Endpoint security software is required for such paths.

- **Firewall**

Installing a firewall has proven to be effective in thwarting big cyberattacks. Any brute force attacks aimed at the computer system are usually blocked by firewalls before they can harm the network or files.

5.9 HOW DOES PACKET SNIFFING WORKS?

A network is a collection of interconnected nodes, such as computers, servers, and networking hardware. Data can be transmitted between various devices thanks to the network connection. Physical connections can be made with cables, while wireless connections can be made with radio signals. Networks can also be a mix of the two types.

Each transmission is split down into smaller bits called packets as nodes deliver data across the network. The data packets can be examined for completeness and usability because of their set length and shape. Packets destined for different nodes will pass through numerous other nodes on their way to their destination because a network's infrastructure is shared by many nodes. To prevent data from being jumbled up, each packet is given an address that specifies the packet's intended destination.

Each network adapter and connected device examines a packet's address to determine which node it is meant for. If a node detects a packet that is not addressed to it, it ignores the packet and its data under normal working conditions.

Packet sniffing ignores this convention and collects all or a portion of the packets, regardless of how they are addressed.

5.10 ARP SPOOFING

5.10.1 What is ARP spoofing?

When malicious ARP packets are transmitted to a LAN's default gateway, ARP spoofing, also known as ARP poisoning, occurs. This is done to change the ARP table's IP/MAC address pairings. The hacker instructs the gateway that their MAC address should now be linked to the IP address of the target victim. The attacker's IP address is linked to the target's MAC address, and vice versa.

The default gateway then caches the updated IP/MAC relationships and distributes them to the rest of the network's devices. This means that all subsequent messages will be directed to the attacker's system instead of the intended receiver.

ARP spoofing attacks are carried out at a low level, which favours the hackers because victims may find it difficult to notice that their traffic has been tampered with.

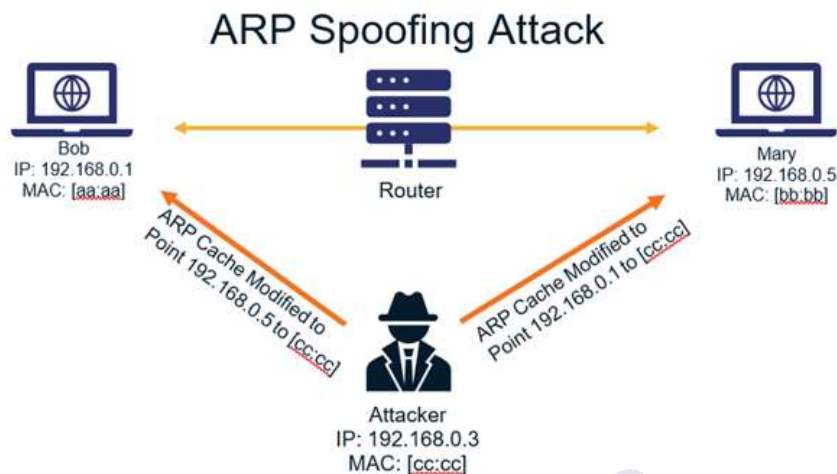
5.10.2 Steps of an ARP spoofing attack

Attacks on ARP spoofing usually follow the same pattern:

- 1] The attacker gains access to the local network and scans it for IP addresses of devices.
- 2] The attacker forges ARP answers using a spoofing tool like Driftnet or Arpspoof. The IP address of the tool is set to match the victim's IP subnet.
- 3] ARP packets with the attacker's MAC and the victim's IP address are sent, tricking the router and PC into connecting to the attacker rather than each other.
- 4] The ARP cache is refreshed, allowing the PC and router to maintain contact with the attacker.

- 5] Other hosts will now transmit data to the attacker instead of the attacker seeing the faked ARP cache entries.

The diagram below shows how all of the pieces go together:



5.10.3 What ARP spoofing is used for

A significant part of what makes ARP spoofing so harmful is because it's frequently used as a platform for more advanced attacks. After successfully executing an ARP spoofing attack, an attacker can quickly proceed to:

- **DDoS attacks:** To initiate a DDoS attack, the attacker might use the address of the server they want to target instead of their own MAC address. The victim will be inundated with traffic if this is repeated for a significant number of IP addresses.
- **Session hijacking:** ARP spoofing can be used to obtain your session ID, which the hacker can then use to gain access to accounts that the victim is logged into.
- **Continued packet hijacking:** The attacker isn't required to take any additional action. They are free to continue sniffing your packets and taking your information (which is why, encrypting your communications via TLS and HTTPS is so important).
- **Disruption in communication:** This would be a man-in-the-middle type of attack. The hacker can intercept and modify traffic, as well as deliver malicious files or websites to the victim's computer.

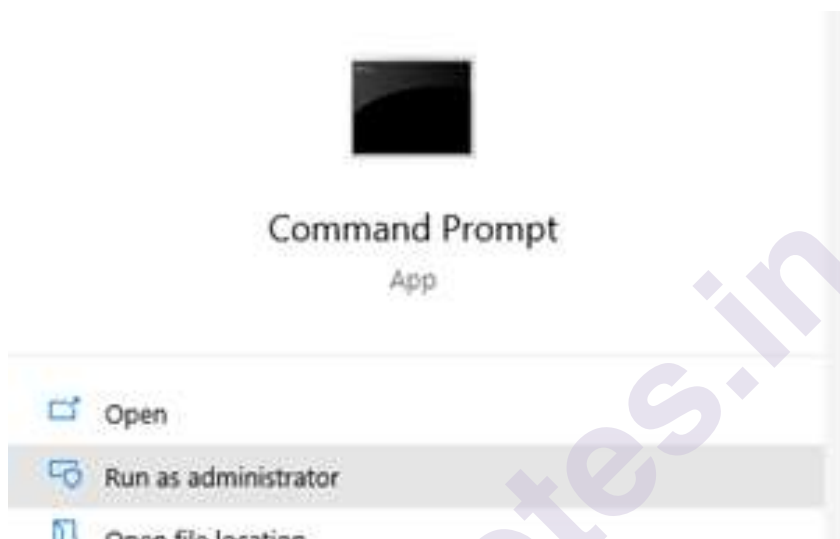
5.10.4 How to detect ARP spoofing?

For detecting ARP spoofing attacks, there are several solutions available. First and foremost, there are third-party software applications. There are two types of them. First, there are more basic networking tools, such as Wireshark (also free and open source), that allow you to examine all of your network traffic and aid in troubleshooting and analysis. Then there are applications like XArp, which are designed specifically to detect ARP

spoofing and continuously monitor your network for ARP spoofing assaults.

Do you prefer not to install a third-party programme? Then you're in luck, because you can utilise your operating system's built-in functionality to identify ARP spoofing. We'll look at how to accomplish it on Windows and Linux in this article (the commands are the same for both):

- 1] As this method relies on the command line, we'll start by logging in as an administrator to an operating system shell. It will look like this in Windows 10:



To see the ARP table, type the following command:

```
arp -a
```

The end product should resemble the following:

```
Command Prompt
Microsoft Windows [Version 10.0.19041.804]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>arp -a

Interface: 192.168.0.191 --- 0x17
 Internet Address      Physical Address      Type
 192.168.0.1           60-63-4c-7b-6e-a5    dynamic
 192.168.0.152         ec-b5-fa-1c-01-56    dynamic
 192.168.0.255         ff-ff-ff-ff-ff-ff    static
 224.0.0.22            01-00-5e-00-00-16    static
 224.0.0.251           01-00-5e-00-00-fb    static
 224.0.0.252           01-00-5e-00-00-fc    static
 239.255.255.250       01-00-5e-7f-ff-fa    static
 255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\WINDOWS\system32>
```

Next, see whether there are any IP addresses with the same MAC address (referred to as "Physical Address" above). This implies that an ARP spoofing attack is taking place.

We are, thankfully, safe. However, if an attack were to take place, it would resemble the image below. The smoking gun is the duplicate MAC addresses belonging to two separate IP addresses (circled in red):

```
Interface: 192.168.56.1 --- 0x11
```

Internet Address	Physical Address	Type
192.168.56.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static


```
Interface: 192.168.43.65 --- 0x16
```

Internet Address	Physical Address	Type
192.168.43.1	08-00-27-89-03-db	dynamic
192.168.43.220	08-00-27-89-03-db	dynamic
192.168.43.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Because the router's IP address is 192.168.43.1 in the case above, it's safe to conclude the attacker's IP address is 192.168.43.220.

Because you'll have to check tens, hundreds, or even thousands of entries (as opposed to just a handful if you're on your home network, for example), the command prompt technique is more laborious and harder to use when dealing with a big network. In that situation, specialised applications like Wireshark or XArp, are probably your best bet for identifying ARP spoofing.

5.10.5 Prevention of ARP spoofing

There are various things your company may take to reduce the likelihood of an ARP spoofing attack on your network. Some are specific activities you should do, while others are best practises that should be followed at all times:

- To help identify poisoned ARP packets, use packet filtering. It operates by determining whether the packets include conflicting source information and, if so, preventing them from reaching other devices.
- Avoid trust relationships that need authentication using IP addresses. As a result, attackers can easily carry out ARP spoofing attacks.

- Use a Virtual Private Network (VPN): VPNs encrypt all of your communications, rendering your traffic useless to any hacker attempting to spoof your ARP. However, as your network grows in size, this becomes less practicable because each computer and server must have its own VPN connection (resulting in a negative performance hit for your network).
- Use Static ARP: ARP allows for the creation of static entries for any IP address. You can prevent others from listening in on ARP responses for that address by using a static ARP entry. If a machine connects to a router on a regular basis, for example, you can define a static ARP entry for the router to prevent ARP spoofing attempts.
- Encrypt data in transit using cryptographic network protocols like Transport Layer Security (TLS), Secure Shell (SSH), or secure HTTP (HTTPS).
- To identify attacks, use ARP spoofing detection software. They work by checking and confirming data before it is sent out, as well as blocking data from faked sources. Other popular utilities include Arpwatch and ARP-Guard, in addition to XArp.
- By monitoring address resolution, intrusion-detection software like Snort can assist stop ARP spoofing attempts.
- To see if your defences are operating properly, simulate a genuine spoofing attack. If the assault succeeds, identify the weak points and address them.

5.11 MAC FLOODING

5.11.1 What is MAC flooding?

MAC Flooding is an attack technique that aims to compromise the security of network switches. The switches usually keep a table structure called the MAC Table. This MAC Table contains the specific MAC addresses of the network's host machines that are linked to the switch's ports. The switches use this table to direct data out of the ports where the recipient is located. We know that, hubs broadcast data throughout the whole network, allowing it to reach all hosts, whereas switches convey data to the specific machine(s) to which the data is supposed to be sent. MAC tables are used to attain this purpose. The goal of MAC Flooding is to bring this MAC Table down. The attacker delivers a large number of Ethernet frames in a conventional MAC Flooding assault. When delivering a large number of Ethernet frames to the switch, the sender addresses will vary. The attacker's goal is to consume the switch's memory, which is utilised to hold the MAC address table. Legitimate users' MAC addresses will be pushed out of the MAC Table. The switch is no longer able to deliver incoming data to the destination system. As a result, a large quantity of incoming frames will flood all ports.

The MAC Address Table is full, and new MAC addresses cannot be saved. It will cause the switch to enter a fail-open state, causing it to operate like a network hub. As if broadcasting, it will forward all incoming data to all ports. Let's look at the advantages of the MAC Flooding assault for the attacker.

Because the attacker is a network node, he will receive data packets intended for the victim machine. So that the attacker can steal sensitive data from the victim's and other machines' communications. A packet analyzer is usually employed to capture this sensitive information.

After successfully starting a MAC Flood attack, the attacker might proceed with an ARP spoofing attack. This will allow the attacker to keep access to privileged data even after the switches have recovered from the MAC Flooding assault.

5.11.2 How to prevent the MAC flooding attack?

MAC Flooding can be avoided using a variety of approaches. Some of these techniques are listed below.

- 1) Port Safety
- 2) Using the AAA server for authentication
- 3) Anti-ARP spoofing and anti-IP spoofing security measures
- 4) Set up IEEE 802.1X networks

- **Port Safety**

Port security is frequently employed as a defence against MAC Flooding attacks. On ports connecting to the end stations, the switches are set to limit the amount of MAC addresses that can be learned. With the regular MAC address database, a small table of 'secure' MAC addresses is also kept. The MAC address table is also a subset of this table. Cisco switches come with an integrated port security system.

- **Using the AAA server for authentication**

The detected MAC addresses are authenticated against an authentication, authorization, and accounting server (AAA Server) and then filtered in this technique.

- **Anti-ARP spoofing and anti-IP spoofing security measures**

In some circumstances, security methods to prevent ARP or IP spoofing may include additional MAC address filtering on unicast packets.

- **Set up IEEE 802.1X networks**

Using IEEE 802.1X suites, a AAA server can explicitly install packet filtering rules based on dynamically learning information about clients, such as the MAC address.

These are the most common strategies for preventing MAC Flooding attacks.

5.12 ACTIVE AND PASSIVE SNIFFING/ TYPES OF SNIFFING ATTACKS

Detecting packet sniffing involves practise and knowledge of the fundamental ideas. As a result, it's critical to understand the many sorts of sniffing attacks in order to recognise them. Active and passive sniffing are the two most common types of sniffing attacks. The main distinction between active and passive sniffing is the way they work. Let's take a closer look at them.

- **Active sniffing**

Attackers use switch-based networks to capture data packets in active sniffing. A switch is a device that connects two network endpoints in today's networks. They employ the switches to forward data to a specific port based on the MAC address of that port. Attackers take advantage of this by introducing traffic into the LAN to facilitate sniffer. MAC flooding, DNS (Domain Name Servers) spoofing, and ARP (address resolution protocol) spoofing are all examples of active sniffing.

- **Passive sniffing**

Passive sniffing occurs through hubs or wireless networks, and attackers read data destination ports using MAC addresses. Unlike active sniffing, they do not communicate directly with the target. Because most packet sniffers are passive, they are difficult to detect.

5.13 SNIFFING COUNTERMEASURES

- **Patch software and disable any unnecessary services:** Check vendor and computer security websites like CERT/CC, Securityfocus, and SANS for information on the newest vulnerabilities, patch releases, and countermeasures, as well as security configuration recommendations.
- **Routinely inspect key binaries:** Because sniffer installation by an intruder is frequently followed by trojanization of important binaries, system administrators should check the system's integrity on a regular basis, using tools like tripwire or anti-virus software, in accordance with the vendor's recommended methods.
- **Use a switched network:** A switched network is meant to prevent packet collisions at each host by having the local hub transmit only broadcast packets to all network devices and packets destined for a specific host to that host alone. On switched networks, sniffers are less effective because unicast traffic, such as telnet, ftp, or smtp (mail), is directed only to the destination host. Using Address Resolution Protocol (ARP) spoofing and/or ARP overloading, an attacker can compel a switch to operate as a dumb hub, forwarding all traffic to all hosts on the network. ARP updates from hosts are

accepted by switches. By flooding a switch with ARP packets, the network is restored to full broadcast mode, and all hosts receive copies of packets transmitted by the switch, allowing an attacker to obtain addressing information that would otherwise be unavailable. By updating the switch with a falsified Ethernet address of the intended receiver, the attacker can reroute traffic intended for another host on the network. By transmitting diverted information back to the intended site, the sniffer host can even evade suspicion. Intruders can use ARP spoofing tools like dsniff and parasite, which are freely available.

- **Disable kernel loading:** An intruder can use a loadable kernel module to change system binaries or the kernel itself to mask the presence of a sniffer at the host level. A system administrator can disable kernel loading by creating a static kernel that lacks the ability to load modules. While an intruder with access to a compiler and source code may rebuild the kernel, due to the time and effort necessary, this is highly unlikely.
- **Use of encryption:** Avoid protocols that deliver data in clear text by utilising encryption. Encrypted authentication, which uses programmes like secure shell and secure copy and protocols like IPv6, ensures not just safe authentication but also the confidentiality of session content.
- **Use one-time passwords:** While one-time passwords cannot prevent sniffers from collecting certain sorts of information, such as mail, they can prevent sniffers from collecting usernames and passwords. One-time password solutions are available in both hardware and software.

5.14 SNIFFING DETECTION TECHNIQUES

5.14.1 How to detect sniffing

- **Promiscuous Mode:** You'll need to figure out which machines are in promiscuous mode. In promiscuous mode, a network device can intercept and read any network packet that comes in.
- **IDS:** Run IDS and see if the MAC addresses of any machines have changed (for example, the MAC address of the router). IDS can provide an alert to the administrator when suspicious activity occurs.
- **Network tools:** Use of network tools like Capsa Network Analyzer to keep an eye on the network for odd traffic. It lets you gather, aggregate, organise, and analyse traffic data from various network resources and technologies.

5.14.2 Sniffer detection technique

- **Ping Method**

Ping the suspect machine using the IP address and the erroneous MAC address. The Ethernet adapter rejects it because the MAC addresses

do not match, but the sniffer on the suspicious system accepts it because it does not reject packets with differing MAC addresses.

- **ARP Method**

The ARP information is cached only by a machine in promiscuous mode (machine C) (IP and MAC address mapping).

A computer in promiscuous mode responds to a ping message because it has accurate information about the host making the ping request in its cache; the rest of the machines will send an ARP probe to find out who sent the ping request.

Packets that were supposed to be filtered by the NIC are now transmitted to the system kernel when the NIC is set to promiscuous mode. We come up with a new approach to detect promiscuous nodes using this mechanism: if we configure an ARP packet without a broadcast address as the destination address, send it to every node on the network, and certain nodes react, then those nodes are in promiscuous mode.

- **DNS Method**

The majority of sniffers use reverse DNS lookup to identify the computer based on its IP address. A sniffer will very certainly be operating on a machine that generates reverse DNS lookup traffic.

- **PromqryUI**

PromqryUI is a Microsoft security application that may be used to identify network interfaces that are in promiscuous mode.

- **Nmap**

The NSE script in Nmap can be used to see if a target on a local Ethernet is in promiscuous mode.

Detect NIC in promiscuous mode with this command:

```
nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]
```

5.15 SUMMARY

This chapter explained how to enumerate a system's resources in preparation for a later attack. You started by looking into several aspects of a system, such as user accounts and group information. The preceding footprinting phase acquired information with little to no contact or disturbance of the target, however this step is more proactive in gathering data. Usernames, IP ranges, share names, and system information are among the data brought into this phase.

If an attacker wishes to become more aggressive and stronger, he or she will need to get more access. This is accomplished by building on the data gathered through thorough inquiry. NetBIOS NULL sessions, SNMP enumeration, SMTP commands, and software like the PsTools suite are all alternatives for doing this research.

You should be able to get a good idea of what the system looks like if you enumerate carefully and methodically. Account information, group information, share information, network data, service data, application profiles, and much more should all be included. Finally, when carrying out each of these activities, you should consider how you may counteract them. You've probably seen that the existence of some open ports, services, and other items can quickly draw attention, much like a bee to honey. Keep in mind, too, that while some services and other products are vulnerable, you won't be able to completely eliminate them. For example, blocking LDAP access too strictly can easily bring your network to a halt. You need to strike a balance between usefulness, ease of use, and security.

The definition and operation of a sniffer were also explained in this chapter. We also looked at some fundamental strategies for getting over the inherent sniffing constraints of switched networks, as well as defensive measures you may take to defend your networks from sniffing and subsequent attacks.

There is no single safeguard that can prevent unwanted sniffers from being installed or being effective. It is not sufficient to track and apply vendor patches. By addressing network design, monitoring the network, following security bulletins, and understanding tool use and limits, system administrators should take all reasonable precautions to make unwanted sniffing impossible.

5.16 LIST OF REFERENCES

- **Reference books**

- 1] Manthan Desai Basics of ethical hacking for beginners.
- 2] SunitBelapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives.
- 3] Sean-Philip Oriyano, Sybex, Certified Ethical Hacker Study Guide v9, Study Guide Edition, 2016.

- **Web References**

- 1) <https://www.geeksforgeeks.org/cyber-security-types-of-enumeration/>
- 2) <http://luizfirmino.blogspot.com/2011/09/enumeration-countermeasures.html>
- 3) <https://heimdalsecurity.com/blog/what-is-a-packet-sniffer/>

- 4) <https://nordvpn.com/blog/packet-sniffing/>
- 5) <https://www.geeksforgeeks.org/what-is-packet-sniffing/>
- 6) <https://in.norton.com/internetsecurity-privacy-what-is-packet-sniffing-and-ways-to-protect-against-sniffing.html>
- 7) <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/mac-flooding-and-cloning/>
- 8) <https://linuxhint.com/mac-flooding-attack/>
- 9) <https://iq.opengenus.org/mac-flooding-attack/>
- 10) <https://www.giac.org/paper/gsec/274/sniffer-detection-tools-countermeasures/100856>
- 11) <https://www.just.edu.jo/~tawalbeh/nyit/incs745/presentations/Sniffers.pdf>

5.17 UNIT END EXERCISES

- 1] Explain Enumeration.
- 2] What are the different techniques and types of enumeration?
- 3] Define sniffing.
- 4] Write a short note on packet sniffing.
- 5] What is ARP spoofing?
- 6] Write a detailed note on detection and prevention of ARP spoofing.
- 7] What is MAC flooding and how you can prevent it?
- 8] Explain the types sniffing attack.
- 9] Write a note on sniffing countermeasures.
- 10] State the various sniffer detection techniques.

TROJANS AND OTHER ATTACKS

Unit Structure

- 6.0 Objective
- 6.1 Introduction
- 6.2 Types of computer worms
 - 6.2.1 How to prevent malware attack
- 6.3 Difference between DoS and DDoS attack
 - 6.3.1 Types of DoS and DDoS attack
 - 6.3.2 How to Improve DoS and DDoS Attack Protection
- 6.4 Watering hole attack
 - 6.4.1 How Does a Watering Hole Attack Work
 - 6.4.2 How to Prevent These Attacks
- 6.5 Brute force attack
 - 6.5.1 How Brute Force Attacks Work
 - 6.5.2 Types of Brute Force Attacks
 - 6.5.3 Examples of Brute Force Attacks
- 6.6 Types of phishing attack
- 6.7 Eavesdropping
 - 6.7.1 Eavesdropping Methods
 - 6.7.2 Prevention techniques of Eavesdropping Attacks
- 6.8 Summary
- 6.9 Unit End Exercise

6.0 OBJECTIVES

- How to prevent malware attack
- Computer worms and its types
- Difference between Dos and DDoS
- Types of DoS and DDoS attack
- Prevention from DoS and DDoS attack

- Watering hole attack and how it works
- Brute force attack and its type
- How brute force attack works and examples
- Common types of phishing attack
- Eavesdrop attack and its type
- Eavesdrop methods and prevention techniques

6.1 INTRODUCTION

Computer Worm

- High Bandwidth is consumed and servers are overloaded with the files that contains the worms and that causes harm to the network.
- It is also responsible for spreading and destroying the network, the codes written program is also destroyed by worm as it is inside systems. The entire network can be destroyed by spam. The codes that are used for program is also called payloads. And this payload will have infected systems which are used to spread spams.
- Computer worms are replicable in nature hence there is no need of assistance.
- The infected system sends mail to through other system and these systems are infected by worms by opening those emails.
- When user open the mail, the worm is automatically gets download and it destroy the program.
- The gets into known condition only after the system is infected.
- Worms are responsible for modify or delete the files of the system in the network.
- Computer worms destroy the data stored in the system.
- All the Security features are exploited by the worms.
- The system setting is also change by some worms.
- Some examples of worms are Morris Worm, Storm Worm, SQL Slammer and so on.

6.2 TYPES OF COMPUTER WORMS

Computer worms are categorized into following types on the basis of distributed systems.

1. Email Worms

The email box is worked as a client for worm. It has infected link or it contains some attachment in which the worm is present and after its open the worm gets download into the system. The contacts also

search by this worm and infect system and sends links so that those systems are also destroyed. This types of worms may have double extensions like mp4 or video extensions so that the user believes it to be media extensions. This type of worm contains short link to open the mail it does not have a downloadable link. With this link is worm is downloaded, and either it deletes the data or modifies the same and the network is destroyed. A famous example is of ILOVEYOU email worm which infected computers in 2000.

2. Internet Worms

In a technological era, everyone knows about Internet and it is used as a medium to connect with the other machines for vulnerable search and affect them. If the system does not installed antivirus that systems are affected easily with these worms. The local area connection or the internet are used to spread the worm in the network.

3. File-Sharing Network Worms

In some cases, user downloads the files from some unknown sources like any link or device such type of files or devices may have the worms which locates a shared folder and destroys other files. The worms are replicated when another system downloads that worm contains file from the same network, And the same process is repeated for all the systems until it reaches to all files or folders in the network. These worms may have the extensions like media files or other hence users attract to download the same thinking that they are an extension of the files. A famous example of this type of worm is worm 'Phatbot' which infected computers in 2004 through sharing files. The personal information such as credit card details and destroyed through this worms on an unprecedented scale.

4. Instant Message and Chat Room Worms

In this types of worms, the user gets an invitation through some link via email or contact it act like human and chat with the other machine via messages. After accepting the invitation and opens the message or link, the system is infected. This worms contains the downloadable attachments or link of any website. User can have easily destroy the worm by changing the security setting or changing the password or simply deleting the messages.

5. IRC Worms

The full form of IRC is Internet Relay Chat this was a messaging application that was a created unique trend once. This worms are responsible for destroying the contact list of IRC as this worms worked in the email and Instant. To destroy this worm's user needs to scan the system and update the security settings and identify the same. Installation of best antivirus can be a solution to this worms also the application should be always update with its software.

6.2.1 How to prevent malware attacks

Strong cybersecurity techniques or setting is the best defence against the oms or malware attacks. As we contain personal hygiene in or day to day life like that only we have to maintain cyber hygiene in network also. Some of the following tips on should follow to prevent malware attacks.

- Software should always update.
- Always use antivirus and antimalware software into the system and also install firewalls and security software.
- User should always follow ethics of email.
- Maintain email security gateways
- Be aware of fake links and attachments.
- Do the setting of access control
- Always do the multifactor authentication
- Monitor for abnormal or suspicious activity.

6.3 DIFFERENCE BETWEEN DOS AND DDoS ATTACK

What Is the Difference Between DoS and DDoS Attacks?

The main important difference between a DoS and a DDoS is that the former is a system-on-system attack, while it also involves many systems attacking a single system. There are other differences too based on involving their nature or detection, including:

1. **Ease of detection/mitigation:** DoS is a single located, hence it makes easy to detect its origin and sever the connection. This is the responsibility of proficient firewall. On the other hand, a DDoS attack are coming from multiple remote locations.
2. **Speed of attack:** the speed of DoS attack id higher as compare to the DDos as it comes from multiple locations, and DoS is come from single location. Hence the difficulties findings are less in DoS.
3. **Traffic volume:** traffic on DoS is very less as compare to DDoS attack because it is coming from multiple location so it sends large volume of data and traffic from multiple resources simultaneously.
4. **Manner of execution:** DoS attack typically uses a script or a tool to carry out the attack from a single machine where as a DDoS infects multiple systems at one time with malware (bots), creating a botnet managed by a command-and-control (C&C) server. In contrast,
5. **Tracing of source(s):** The use of a botnet in a DDoS attack means that tracing the actual origin is much more complicated than tracing the origin of a DoS attack.

6.3.1 Types of DoS and DDoS Attacks

1. Teardrop Attack

Countless Internet Protocol (IP) data fragments sends in a to a teardrop attack which is also a DoS attack. Hence the original packets are unable to recompile the fragments.

For example, in this type of attack the attacker will break down the large packets in to the small multiple fragments and all fragments send to the targeted machine to reassemble. However, the attacker changes the sequence of the packets to confuse the targeted system, which is then unable to reassemble the fragments into the original packets.

2. Flooding Attack

A flooding attack is a DoS attack that's believe in sending multiple connection requests to a server but not waiting for the response to complete the handshake.

For example, in this type the attacker always sends multiple requests to connect as a client, to verify the request if server tries to communicate with the client, the attacker refuses to respond. This process is repeated for many times hence the server gets exhausted with countless pending request and among that request the server is not able to verify the genuine client and in result it becomes "busy" or even crashes.

3. IP Fragmentation Attack

It is type of DoS attack which known as an IP fragmentation attack in which it delivers altered or modified network packets to the receiving network that cannot reassemble. In result the network becomes crashed with bulky unassembled packets, using up all its resources.

4. Volumetric Attack

Type of DDoS attack is a volumetric attack. It used to target bandwidth resources. An instance, the botnet is used are used to send a high volume of request to a network, Protocol Attack

This attack is a type of DDoS attack. In that it exploits weaknesses in 3rd and 4th Layers of OSI model. For example, in this attack the TCP connection is exploit by the attacker, he is sending requests but either not answering as expected or responding with another request using a spoofed source IP address. until the resources being available the unanswered requests use up the resources of the network.

5. Application-based Attack

It is DDoS type of attack which is known as an application-based attack. It targets 7th Layer of the OSI model. For example, the attacker sends partial Hypertext Transfer Protocol (HTTP) requests but does

not complete them. HTTP headers are periodically sent for each request, resulting in the network resources becoming tied up.

Up to the new connection made by sever the attacker continues the onslaught. The detection of this type of attack is very difficult as they sending corrupted partial packets, and it uses little to no bandwidth.

6.3.2 How to Improve DoS and DDoS Attack Protection

The following are Tips for DoS and DDoS protection:

1. Monitor your network continually: always try to monitor the usual traffic pattern so that moderate to critical stage is early detected and mitigated.
2. Run tests to simulate DoS attacks: The assessment of the risk, expose vulnerabilities, and train employees in cybersecurity is done here.
3. Create a protection plan: checklists, form a response team, define response parameters, and deploy protection circulate among the employees.
4. Identify critical systems and normal traffic patterns: The early detection is made with the former help of planning protection, and later it helps in the early detection of threats.
5. Provision extra bandwidth: It may not stop the attack, but it will help the network deal with spikes in traffic and lessen the impact of any attack.

6.4 WATERING HOLE ATTACK

A watering hole attack is a type of cyber-attack which is specifically design to the target a special group of users who are usually visited the websites and that website will infect by this or by luring t users to a malicious site. It is also known as **strategic website compromise attack**, in this attack the main aim is to infect the systems of the targeted users to gain unauthorized access to their organization's network.

In case of spear phishing the user infected are less in count while in Watering hole attacks it seems to **trap more victims at once than spear phishing does**. This type of attack is done by creating the fake sites compromise legitimate applications and websites using difficult and zero-day exploits with no antivirus signatures, ensuring a high attack success rate. The most prominent highlight of watering hole attacks is the user will later know about the site compromise the early known is not at all present in the watering hole attack.

6.4.1 How Does a Watering Hole Attack Work?



Following are the steps of watering hole attack which can be achieved by proper planning and execution by threat actors. To protect a system against such attacks, it is necessary to know how they are carried out.

Step 1: In this step, the hacker will target the audience or user who uses a specific website frequently based on their industry, job title, organization, etc. With this, the hacker can determine which type of websites and applications are often visited by the targeted users or the employees of the targeted organization.

Step 2: After getting the information of the user's website, the hacker either creates a new website or looks for any vulnerabilities in the existing applications and websites to inject malicious code, which redirects the users to a malicious site.

Step 3: After creating a new website or threats, the hacker manages to infect the system of the target with malware.

Step 4: The malware will do its work of destroying a network or data consistent in the system. They try to collect the user's usernames and passwords for launching credential-stuffing attacks on targeted applications, sites, and organizations.

Step 5: After getting the user's system compromised, the threat actors can perform lateral movements within the network to ultimately breach the entire organization.

6.4.2 How to Prevent These Attacks?

- 1. Conduct Periodic VAPT:** Vulnerability Assessment and Penetration Testing (VAPT) is a testing technique that can help users to make sure that the security controls provide satisfactory protection against application and browser-based threats like watering hole attacks.
- 2. Keep the Systems Updated:** Updates keep all the system's hardware and software up-to-date, including the latest security updates.

and patches. If you can't have done this, then weaknesses in your security infrastructure and lead to cyber-attacks.

3. **Be Wary of Third-party Traffic:** the verified process only processed with this as the all third-party traffic, no matter where it comes from, should be treated as untrusted until and unless it has been otherwise verified.
4. **Enable MFA:** always imply with the Multi-Factor Authentication (MFA) to the overall system as it secures the organization's networks. With this the you can reduce the impact of watering hole attacks in case the attackers manage to steal the user credentials of your employees.
5. **Establish a Cyber Resilient Work Environment:** always train and educate your employees after done appointment about watering hole attacks so they can be more vigilant during the work. Train staff with proper cyber security awareness training is the best way of creating a cyber resilient work environment.

6.5 BRUTE FORCE ATTACK

The term "brute force" define the simplistic way in which the attack takes place. The attack is held with guessing credentials to gain unauthorized access. Primitive as they are, brute force attacks can be very effective.

The attack in brute force use bots to do their bidding. With this type of attack, the attackers will have a list of real or commonly used credentials and assign their bots to attack websites using these credentials.

In manual brute force credential cracking is time-consuming, and this can be done through using brute force attack software and tools to aid them. With the tools the attacker will attempt things like inputting numerous password combinations and accessing web applications by searching for the correct session ID, among others.

6.5.1 How Brute Force Attacks Work

This attack is held with guessing login passwords. Brute force password cracking is done here.

For most online systems, a suggestion user to set the password is: the password should be of 8 character and it should contain at least one capital letter one small letter and one special character. If the password is not strong or complex it can be easily guess by the attacker. a guessing of password will be difficult for attacker if the user makes it very complex and confidential. Hence the good practice is changing the password frequently.



6.5.2 Types of Brute Force Attacks

Brute force attack is always deals with cracking the password and gaining the access of the system. But there are some more types of attacks are present in the brute force.



1. Rainbow Table Attacks

Rainbow table attacks are unique as they don't target passwords; instead, they are used to target the hash function, which encrypts the credentials.

The table is a precomputed dictionary of plain text passwords and corresponding hash values. Hackers can then see which plain text passwords produce a specific hash and expose them.

When a user enters a password, it converts into a hash value. If the hash value of the inputted password matches the stored hash value, the user authenticates. Rainbow table attacks exploit this process.

2. Dictionary Attack

In this type of attack, it is having dictionary of all possible passwords and tests them all.

In this the attacker will try every possible combination, with an assumption of common passwords. The attacker builds the common password dictionary and iterate the inputs.

With the password dictionary the attacker will improve his chances of getting successful in hacking the websites. Hence this need a large number of attempts against multiple targets.

3. Simple Brute Force Attack

All the local file access can be gain from this type of attack, as there is unlimited access of attempts. It can have done through passing or inputting all possible password one at a time.

4. Hybrid Brute Force Attack

The combination of the two attacks that are dictionary and simple brute force attack is called as hybrid brute force attack. It uses feature of dictionary attack of using an external logic, and moves on to modify passwords of simple brute force attack.

In this the attacker is having the list of possible password rather than testing every password, he will assume that the changes in the letter and numbers to guess the password.

5. Reverse Brute Force Attack

The reverse brute force attack flips the method of guessing passwords on its head. Rather than guessing the password, it will use a generic one and try to brute force a username.

6. Credential Recycling

As the name implies credential recycling is using the same credential twice, if user is not following the criteria of setting the password and changing the password frequently it leads to use same password next time and make the attacker easier to guess the password, as the attacker is having the possible password list with himself.

6.5.3 Examples of Brute Force Attacks

How common are brute force attacks?

- In 2018, Firefox's *master password* feature was proven to be easily cracked with a brute force attack. It is unknown how many users' credentials were exposed. In 2019, Firefox deployed a fix to resolve this issue.

- In March 2018, Magento was hit by a brute force attack. Up to 1000 admin panels had been compromised.
- In March 2018, several accounts of members of the Northern Irish Parliament had been compromised in a brute force attack.
- In 2016, a brute force attack resulted in a massive data leak in the e-Commerce giant, Alibaba.
- According to Kaspersky, RDP-related brute force attacks rose dramatically in 2020 due to the COVID-19 pandemic.

6.6 COMMON TYPES OF PHISHING ATTACK

In organization the Phishing is the biggest cyber threats faced during the work. As per the Phish Report of Proofpoint's 2021, most of the organisations fell victim to a phishing attack last year.

The fast growing sophisticated of phishing scams has contributed to the same objective that is to steal the user personal data or infect our devices with the new countless ways.

1. Email phishing

In Email phishing the attacks can be done through email. The Email is sent to the user, the attacker will register a fake domain that mimics a genuine organisation and sends thousands of generic requests.

The fake domain created by the attacker involves character substitution, like using 'r' and 'n' together with no space 'rn' which look exactly like 'm'.

In many of the cases, the attacker creates a unique domain that includes the legitimate organisation's name in the URL. The example below is sent from 'olivia@meeshosupport.com'.

The user or recipient might see the word 'Meesho' in the sender's address and assume that it was a genuine email.

User should always identify the user by checking the mail sender's address to spot a phishing email, and also check the content of the mail in which may have a link or download an attachment.

2. Spear phishing

Another type of email phishing is, spear phishing which describes malicious emails sent to a specific person. Here Criminals have the following information about the victim:

- Their name;
- Employment place;
- Title of the Job;

- Email address; and
- Specific information about their job role.

The attacker has the above information so he addresses the individual by name, knows that their job role involves making bank transfers on behalf of the company.

3. Whaling

Taking aim at senior executives, who are targeted by Whaling attacks. Instead of using tricks such as fake links and malicious URLs aren't helpful in this instance, as criminals are attempting to imitate senior staff.

This type of attack on emails also commonly use the pretext of a busy CEO who wants an employee to do them a favour.

Emails such as the above might not be as sophisticated as spear phishing emails, but they play on employees' willingness to follow instructions from their boss. Recipients might suspect that something is amiss but are too afraid to confront the sender to suggest that they are being unprofessional.

4. Smishing and vishing

Smishing and vishing both are the attack done by emails instead of telephones as the method of communication.

In Smishing attacker sending text messages (the content of which is much the same as with email phishing), whereas in vishing attacker give a telephone call for conversation.

Most common technique of smishing is sending pretexts messages supposedly from your bank alerting you to suspicious activity.

hs-internet-cancel-payees.com/login'. The text is in a light gray speech bubble." data-bbox="208 645 655 878"/>

**HSBC ALERT: Request
for NEW payee MR D
FRASER has been made
on your account. If this
was NOT done by you,
visit: [hs-internet-cancel-
payees.com/login](http://hs-internet-cancel-payees.com/login)**

In the above example, the message contains the information about new payee added to the account and have a link to prevent the user if he has not done that transaction it prevents the further damage. But all the time it is not trustable however, the link directs the recipient to a website controlled by the fraudster and designed to capture your banking details.

5. Angler phishing

A new type of attack vector, the growing user of social media offers several ways for criminals to trap people. Fake URLs; cloned websites, posts, and tweets; and instant messaging (which is essentially the same as smishing) can all be used to persuade people to divulge sensitive information or download malware.

Attackers are always use the data that people post on social media to create highly targeted attacks.

The following example demonstrates; angler phishing which is often made possible due to the number of people containing organisations directly on social media with complaints.



Sometime organisations may use these as an opportunity to mitigate the damage by giving refund to the individual.

However, scammers are tried to hijacking responses and asking the customer to provide their personal details. They are seemingly doing this to facilitate some form of compensation, but it is instead done to compromise their accounts.

6.7 EAVESFDROPPING

The data transfer between two devices can be altered, delete or intercepts through an eavesdropping attack by hacker. Eavesdropping, also known as sniffing or snooping, which relies on untrusted or unsecured network communications to access data in transit between devices.

The further explanation of the definition of "attacked with eavesdropping", it typically occurs when a user connects to a network in which traffic is not secured or encrypted and sends sensitive business data to a colleague. across an open network, the data is transmitted which gives an attacker the

opportunity to exploit a vulnerability and intercept it via various methods. It is difficult to spot Eavesdropping attacks.

6.7.1 Eavesdropping Methods

Various methods are used by attacker for eavesdropping, to launch attacks that typically involve the use of various eavesdropping devices to listen in on conversations and review network activity.

A traditional example of an electronic listening device is a concealed in a home or office with the equipment's. in many cases the device fitted under a chair or on a table, or by concealing a microphone within an inconspicuous object like a pen or a bag. This is very easy to installed but very difficult to detect devices being installed, such as microphones within lamps or ceiling lights, books on a bookshelf, or in picture frames on the wall.

Now in this day or any age eavesdropping increasingly with the number of technological advances and also it makes easy to use, however many attacks still rely on intercepting telephones. As the telephones have its own electric power, built-in microphones, speakers, hence the space for hiding bugs, and are easy to quickly install a bug on. Eavesdropping attackers can monitor conversations in the room the telephone is in and calls to telephones anywhere else in the world.

Now a day computerized phone system makes it possible to intercept phones electronically without direct access to the device. Attackers also use technique of sending signals down the telephone line and transmit any conversations that take place in the same room, even if the handset is not active. As well as many of the computers have sophisticated communication tools in which by default eavesdropping technique is there hence the attackers to intercept communication activity, like user voice conversations, their online chats, and even bugs in keyboards to log what the user is intended to type.

Electromagnetic radiation emits by Computers also sophisticated eavesdroppers can use to reconstruct a computer screen's contents. These radiations can be flow up to a few hundred feet and going further through cables and telephone lines, which can be used as antennas.

1. Pickup Device

The Attackers get the information of the user by using devices that pick up sound or images, such as microphones and video cameras, and convert them into an electrical format to eavesdrop on targets. As we know it is an electrical device which is run on power consumption and set in the target room, which eliminates the need for the attacker to access the room to recharge the device or replace its batteries.

In some of the devices they have the capability of storing digital information and transmitting it to a listening post. Sometimes attackers can also make use of mini amplifiers that enable them to remove background noise.

2. Transmission Link

With the help of transmission link the connection between a pickup device and the attacker's receiver can be tapped for eavesdropping purposes. Radio frequency is used to make the transmission or a wire, which includes active or unused telephone lines, electrical wires, or ungrounded electrical conduits. Some of the transmitters can operate continuously, but a more sophisticated approach involves remote activation.

3. Listening Post

A listening post is used to transmit conversations intercepted by bugs on telephones. When a user makes telephone call or telephone is picked to take a call, it automatically triggers a recorder that is automatically turned off when the call is ended.

Listening posts are secure areas in which signals can be monitored, recorded, or retransmitted by the attacker for processing purposes. It can be located anywhere from the next room to the telephone up to a few blocks away. The listening post will have voice-activated equipment available to eavesdrop on and record any activity.

4. Weak Passwords

Attacker can get the unauthorized access of user account if the passwords is weak, which gives them a route enter into corporate systems and networks. This may lead to hackers being able to compromise confidential communication channels, intercept activity and conversations between colleagues, and steal sensitive or valuable business data.

5. Open Networks

If the users desperately connect to open networks on which they don't need any password or encryption techniques to transmit data provide an ideal situation for attackers to eavesdrop. Attackers always monitor user activity and snoop on communications that take place on the network.

6.7.2 Prevention techniques of Eavesdropping Attacks

1. Military-grade encryption:

Encryption is one of the best ways to prevent eavesdropping attacks while doing transmission and private conversations. This will restrict attackers' ability to read data exchanged between two parties. For example, military-grade encryption provides 256-bit encryption, which is near impossible for an attacker to decode.

2. Spread awareness:

As much as organization spread awareness among the employees that much the environment will be secure over the network. Organization

should conduct the training session to train the employees about the security measures. It makes employees are aware of the risks and dangers of cybersecurity which is a crucial first line in protecting organizations from any cyberattack.

3. Network segmentation:

Organizations must do the network segmentation so that it can limit the possibilities of attackers eavesdropping on networks by restricting their availability. this enables the limits the resources to only the people that require access to them. For example, people on a marketing team do not require access to HR systems and people on the IT team do not need view to financial information. Network segmentation divides the network up, which decongests traffic, prevents unwanted activity, and improves security by preventing unauthorized access.

4. Avoid shady links:

Related to spreading awareness is the need to avoid shady or untrusted links. Eavesdropping attackers can spread malicious software that includes eavesdropping malware through shady links. Users should only download official software from trusted resources and providers, and only download applications from official app stores.

5. Update and patch software:

Attackers can also exploit vulnerabilities in software to target organizations and users. This makes it crucial to turn on automatic updates and ensure all software is patched immediately as a new release or update is available.

6. Physical security:

The office spaces of the organizations can also protect their data and users through physical security measures. This is crucial to protecting the office from unauthorized people who may drop physical bugs on desks, phones, and more.

7. Shielding:

The risk of eavesdropping through computer radiation can be prevented by installing security measures and shielding. For example, TEMPEST-protected computers enable organizations to block unintended radiation and keep their data and users secure.

6.8 SUMMARY

High Bandwidth is consumed and servers are overloaded with the files that contains the worms and that causes harm to the network. It is also responsible for spreading and destroying the network, the codes written program is also destroyed by worm as it is inside systems. The entire network can be destroying by spam. The codes that are used for program is

also called payloads. And this payload will have infected systems which are used to spread spams. The main important difference between a DoS and a DDoS is that the former is a system-on-system attack, while it also involves many systems attacking a single system. A watering hole attack is a type of cyber-attack which is specifically design to the target a special group of users who are usually visited the websites and that website will infect by this or by luring t users to a malicious site. The data transfer between two devices can be altered, delete or intercepts through an eavesdropping attack by hacker. Eavesdropping, also known as sniffing or snooping, which relies on untrusted or unsecured network communications to access data in transit between devices.

6.9 UNIT AND EXERCISE

1. Explain in details eavesdropping
2. Define computer worms with its types
3. State and explain the prevention techniques of the brute force attack
4. Write difference between DoS and DDos attack
5. List the Prevention from DoS and DDoS attack
6. Explain Eavesdrop methods and prevention techniques
7. Explain the working of brute force attack
8. Write a note on
 1. Brute force attack
 2. Eavesdrop attack
 3. Phising

TROJANS AND OTHER ATTACKS

Unit Structure

7.0 Objective

7.1 Introduction

7.2 Man in the middle attack

7.2.1 type of man in the middle attack

7.2.2 Technology involved in man in the middle attack

7.2.3 prevention techniques from man in the middle attack

7.2.4 best practice of man in the middle attack

7.3 Buffer Overflow

7.3.1 Types of Buffer overflow

7.3.2 Prevention from buffer overflow

7.4 Address Resolution Protocol

7.4.1 Ways to Protect from ARP Poisoning

7.5 Run spoofing attack

7.5.1 Types of Identity Theft

7.6 Phishing techniques

7.7 Iot attack

7.8 Botnet

7.8.1 Stages of botnet building

7.8.2 Types of Botnet

7.9 Summary

7.10 Unit End Exercise

7.0 OBJECTIVE

1. This chapter will able you to understand the following concept
2. Man-in-the-Middle (MITM) Attack: and I's type and technology
3. Concept of Buffer Overflow

4. Prevention techniques of man in the middle attack
5. Address Resolution Protocol
6. Run spoofing attack
7. Iot attack with its type and prevention techniques
8. Concept of Botnet with its working and types

7.1 INTRODUCTION

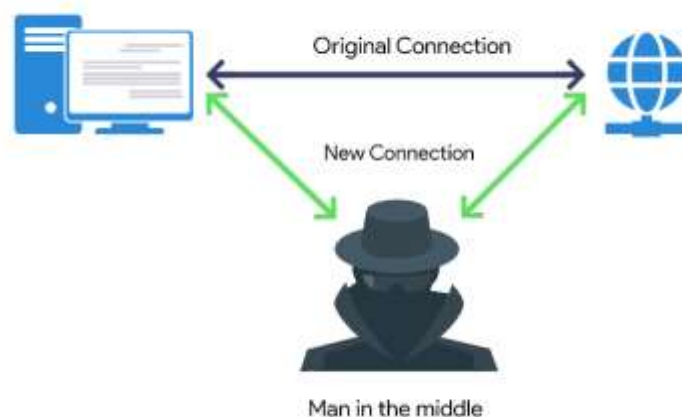
One of the type of Cyber threats in this digital era which is done by the most of the hacker . But one of the most prevalent threats out there that often gets overlooked is manipulator-in-the-middle (previously referred to as ‘man-in-the-middle’) attack. As we know a MITM attack is an attack where the data is being altered or manipulate through the third party where the communication between the parties are not secure and secret hence this attack can affect the medium of communication like device interruption or connection interruption and connected objects (IoT).

7.2 MAN-IN-THE-MIDDLE (MITM) ATTACK

When we established communications between the user and internet through the network which is to be confidential and not to be changed or tampered while in transit. While doing this we made some assumption:

1. The data which we are entered is valid,
2. The data is sending to the server in original format or in correct form
3. During the transmission third parties cannot see, intercept or change your data.

If we are using some websites and online services which are not secure, we could face some security risks such as phishing, fraud, impersonation, malware, and many others.



7.2.1 The two main types of MITM attacks:

The first type of attack is where an adversary may want to read the content of a message which is confidential. The first type of attack is where an adversary may change the content of the message or otherwise modify the communication which is said to be an attack on integrity.

This type of attack involves the physical proximity to the intended target or it involves a malicious software or malware. Like an instance the user receives mail containing the fake link which take to the bank website and ask for login credentials and data theft is happened.

Based on this man-in-the-middle attacks can be categorized into two another types:

Active session attack

While using internet connection two devices are communicated with each other via network, where the attacker involve in the communication and stops the original client from communicating with the server and act as normal and collect all the sensitive information from both the client and then replaces himself within the session.

Passive session attack

In this attack the hacker is passive in nature where he only monitors the data flowing across the network without interrupting the actual communication as well as he is not modifying any messages, he just collect all the data which are transferred to between the clients.

7.2.2 Technology involved in Man-in-the-Middle Attacks

1. Rogue Access Point

The rough access point is the virtual point prepare through wi-fi where the computers can be connected automatically to wi-fi without any authorization of an administrator and introduce a security threat. By doing this the data transfer over the network monitor by the rough access point and steal sensitive information.

2. Address Resolution Protocol (ARP) Spoofing

ARP is a protocol where the MAC address of a particular device can be find whose IP address is known. when two devices are connected with each other over network they also connected with the MAC address. so that the ARP packets can be forged to connect and the hacker will intercept, modify, and drop the incoming messages.

3. Domain Name System (DNS) Spoofing

In Domain Name System (DNS) spoofing the hacker theft sensitive data or login credentials by distracting user from original website to fake website. In this user think that the website is trusted website and pass his login credentials as the website is looking real. The main aim

of the hacker is to divert traffic from the real site or capture user login credentials and other data. This can be done by altering the IP addresses stored in the DNS server with the ones under the control of the attacker. Hence when a user tries to access a particular website, they get directed to the malicious website placed by the attacker in the spoofed DNS server.

4. Email Hijacking

In this type of attack the attacker gain access to a user's email account and watch communications to and from the account. He continuously monitors the transaction or communication between the clients and when he gets opportunity he theft data or transfer the funds from users account.

5. Internet Control Message Protocol (ICMP) redirection

The network devices are compromised in ICMP. The router gets compromised during the communication or transmission between the clients, the data packets are misplaced during the transaction and its pretend to be successfully translated the message.

6. Dynamic Host Configuration Protocol (DHCP) spoofing

DHCP dynamically assigns IP addresses while establishes the connection between the clients. In this the attacker's computer is issued as a DHCP server and sends forged DHCP acknowledgments to any connecting nodes.

7. SSL stripping

It is a secure cryptographic protocol in which the data is transferred over the secure network. In this the HTTP request is altered by the attacker by encrypting the connection between two parties.

In this the attacker intervenes in this redirection of HTTP to HTTPS and allocates himself between the server and client. While the victim and attacker will be in an unsecured connection, the attacker maintains an HTTPS connection with the server.

7.2.3 The prevention techniques of Man-in-the-Middle Attacks

Generally, MITM attacks can be detected or prevented by authentication and tamper detection.

Authentication

The degree of certainty of given message can be gain by authentication which has a valid source and destination. The protocols like TCP and encryption of public key infrastructure, such as TLS, can prevent against MITM attacks.

The best way to authenticated user by multiple authentication like face reading, figure reading, password or PIN hence the attacker will find difficulties while forging the sensitive data

Tamper Detection

The originality of the message can be find through Tamper detection where it will checks whether a message has been altered or not and ensures that the data is safe from corruption. With the help of original hash function used by the user while sending the message and its encryption can be find through this.

7.2.4 Following are some Best Practices to Stay Safe from Man-in-the-Middle Attacks

For Individuals

- Always used SSL/TLS secure website for doing any transformation of message.
- Every secure website has its SSL certificate which is active and issued by a trusted certificate authority. Ensure that while using it.
- Freely available VPNs or proxy servers has virus. Be alert while using it.
- Always update the latest version of your web browser.
- Don't connect your devices with free wireless hotspots in public locations such as coffee shops, hotels or airports.
- While using public Wi-Fi hotspots, don't enter any sensitive data like account credentials and try to avoid downloads and online payments.
- Use Bluetooth connection very carefully
- Always set complex passwords, update them frequently, and use separate passwords for each application.
- Think twice while opening mail which contains any link related to any payment it may have malicious site.

For organizations

- Train staff or employees to protect their sensitive data, do not allowed them to use public networks for any confidential work..
- Always ask for secure connection established by virtual private networks (VPNs) to your business to online applications. And ensure that employees securely connect to your internal private network from remote locations.
- Make habit to staff for updating the browser frequently whichever they are using for daily work always use latest version of any browser.

- Train staff to secure your email using SSL/TLS to protect messages in transit, and consider using PGP/GPG encryption to protect them at rest as well.
- Always motivate staff for implement multi-factor authentication, firewalls and intrusion detection system (IDS) to monitor your network.

7.3 BUFFER OVERFLOW

Buffer is sequential sections of computing memory that hold data temporarily as it is transferred between locations. It is also called as buffer overrun. When the amount of data storage is exceeded with memory and there is no space for upcoming data, to handle this situation the buffer overflow concept is used, as it holds the extra sequential data into adjacent memory location and as and when it requires it passes to the process.

Buffer Overflow Attack

When attacker needs to manipulate the coding error to carry out malicious actions and compromise the affected system he is altering the application's execution path and overwrites elements of its memory, which amends the program's execution path to damage existing files or expose data. It is typically involves violating programming languages and overwriting the bounds of the buffers they exist on.

7.3.1 Types of Buffer Overflow Attacks

1. **Stack-based buffer overflows:** in this type of attack, the attacker sends data containing malicious code to an application, which stores the data in a stack buffer. In this the buffer overwrites the data on the stack, including its return pointer, which hands control of transfers to the attacker.
2. **Heap-based buffer overflows:** A heap-based attack is more difficult to carry out than the stack-based approach. It involves the attack flooding a program's memory space beyond the memory it uses for current runtime operations.
3. **Format string attack:** A format string exploit takes place when an application processes input data as a command or does not validate input data effectively. This enables the attacker to execute code, read data in the stack, or cause segmentation faults in the application. This could trigger new actions that threaten the security and stability of the system.

7.3.2 Preventions against Buffer Overflows

While developing the application using a security measures into the code of the program, also using built in protection while choosing programming language and always test the code for detecting the errors and also fix the same and rerun the code.

While writing code avoid using standard library functions that have not been bounds-checked, which includes `gets`, `scanf`, and `strcpy` as they have memory bound.

Always write a code in modern operating system and deploy runtime protection that enables additional security against buffer overflows with the following techniques.

1. Address space layout randomization (ASLR): the executable code location is accessed by this address and moves at random around locations of data regions to randomize address spaces, which makes overflow attacks almost impossible.
2. Data execution prevention: This method prevents an attack from being able to run code in non-executable regions by flagging areas of memory as executable or non-executable.
3. Structured exception handling overwrite protection (SEHOP): Attackers may look to overwrite the structured exception handling (SEH), which is a built-in system that manages hardware and software exceptions.

7.4 DOMAIN NAME SYSTEM (DNS)

the protocol through which the domain name translate, such as `website.com`, into an IP address such as `208.38.05.149`.

Here is how it works:

- All the IP address are stored into the local cache the DNS resolver looks up the IP address.
- If the server is not getting the address in the cache, it queries a DNS server.
- to find a DNS server that has the correct IP address ,or an authoritative DNS server that stores the canonical mapping of the domain name to its IP address, the recursive nature of DNS servers enables them to query one another .
- for future use the resolver finds the IP address, it returns it to the requesting program and also caches the address.

7.4.1 What Are the 5 Major DNS Attack Types?

1. DNS Tunneling

The DNS queries and response are rely on the DNS tunneling which involves encoding the data of other programs or protocols. Data payload can be handled to take over a DNS server and allow attackers to manage the remote server and applications.

It also relies on the outside network connectivity of a compromised system, which provides a way into an inside DNS server with network access. It also helps in controlling a server and a domain, whose functions as an authoritative server through it carries out data payload executable programs as well as server-side tunneling.

2. DNS Amplification

Distributed Denial of Service (DDoS) on a targeted server is performed by DNS amplification. Publicly available server can be exploited by the open DNS servers that are, in order to overwhelm a target with DNS response traffic.

In this the threat actor sending a DNS lookup request to the open DNS server, spoofing the source address to become the target address as and after getting the DNS server response, it is passed to the new target, which is controlled by the attacker.

3. DNS Flood Attack

User datagram protocol (UDP) flood can be carried out by DNS flood attacks using the DNS protocol. The valid DNS request deploys by the actor or attackers (but spoofed) DNS request packets at an extremely high packet rate and then create a massive group of source IP addresses.

As the requests look valid, the DNS servers reply the entire request made by the attacker. All the requests are stored in DNS server and it can overflow the memory of the server. A DNS attack requires a great amount of network resources, which tire out the targeted DNS infrastructure until it is taken offline. As a result, the target's internet access also goes down.

4. DNS Spoofing

In Domain Name System (DNS) spoofing the hacker theft sensitive data or login credentials by distracting user from original website to fake website. In this user think that the website is trusted website and pass his login credentials as the website is looking real. The main aim of the hacker is to divert traffic from the real site or capture user login credentials and other data. This can be done by altering the IP addresses stored in the DNS server with the ones under the control of the attacker. Hence when a user tries to access a particular website, they get directed to the malicious website placed by the attacker in the spoofed DNS server.

5. NXDOMAIN Attack

A DNS NXDOMAIN flood DDoS attack attempts to overwhelm the DNS server using a large volume of requests for invalid or non-existent records. These attacks are often handled by a DNS proxy server that uses up most (or all) of its resources to query the DNS authoritative server. This causes both the DNS Authoritative server

and the DNS proxy server to use up all their time handling bad requests. As a result, the response time for legitimate requests slows down until it eventually stops altogether.

7.4.2 DNS Attack Prevention

1. Keep DNS Resolver Private and Protected

Always allow authorized user which are on the network and Restrict DNS resolver usage to external users ask them to do not leave it open to external users.

Configure Your DNS Against Cache Poisoning

DNS software should configure security in order to protect your organization against cache poisoning. With the addition of the credentials can add variability to outgoing requests in order to make it difficult for threat actors to slip in a bogus response and get it accepted. Do not use always UDP port 53 to as a source port for the request try randomizing the query ID, as well as use a random source port.

7.5 ADDRESS RESOLUTION PROTOCOL (ARP)

The ARP was first developed in the 1980s for managing the networks connections without an attaching individual device to each. With this two machines can connect more efficiently and it make easier and freely to transmit information.

Security is a persistent problem when using ARP. It is also known as **ARP poisoning**, this attack can be carried out over a Local Area Network (LAN) that sends malicious ARP packets to a default gateway on a LAN.

7.5.1 Ways to Protect from ARP Poisoning

1. Understand the Spoofing Process

First hacker find out the MAC address with the IP address of a legitimate computer or server to sends a false ARP message over a local network, and can start receiving data that was intended for the seemingly-legitimate IP address.

Now you can monitor the abnormal activity on your server and try to determine what information the hacker is targeting. With this continue monitor process one can get clues what type of data might be vulnerable to any attack, not just ARP spoofing.

2. Identify the Spoofing Attack

Now the main thing is to find out what kind of attack is targeting your device after knowing how **ARP spoofing works** and what to look for, it's also crucial to identify. The similar attack process is always following through the ARP spoofing; they can vary in how they access your devices. After determining the experience of attack one

can identify the best course for prevention and resolution. There are 3 types of attack can make your system destroy.

- **Denial-of-service attacks:** the host connection as well as the services provided by the server is compromise in the denial-of-service attack (DoS), this make your site or resources unavailable to their intended audience.
- **Session hijacking: with the session ID the hacker will open the private door and the Session is hijacking with ARP spoofing.** This is why using public WiFi in cafes and busy airports can create a vulnerable situation for your data.
- **Man-in-the-middle attacks:** Man-in-the-middle attacks use ARP spoofing to intercept incoming traffic from a legitimate user and modify it to gain access to the session.

3. Rely on Virtual Private Networks

One way to prevent ARP spoofing is to rely on Virtual Private Networks (VPNs) to work on confidential data. Connect always with VPN rather than Internet Service Provider (ISP) in order to connect to website, as when you use a VPN, you're using an encrypted tunnel that largely blocks your activity from ARP spoofing hackers.

If any user travel frequently avoid using public WiFi hotspots while working with sensitive information or data, always use VPN.

4. Use a Static ARP

Making the static ARP entry in your server can help reduce the risk of spoofing. If the organization is having regular client with whom they regularly communicate, in such cases setting up a static ARP entry creates a permanent entry in your ARP cache that can help add a layer of protection from spoofing.

A CISCO router can help determine the ARP spoofing event is occurring with the help of ARP information.

5. Get a Detection Tool

Use of detection tool is even more preventing method rather than having the knowledge and techniques of ARP spoofing, as it will not always help to detect a spoofing attack. Always focusing of prevention doesn't give the result hence; make sure you have a detection method in place. With the detection tool spoofing attack is finding early and you can work on stopping its tracks.

6. Avoid Trust Relationships

You can also add one extra layer of security by using the on private logins and passwords to identify users rather than rely on IP trust relationships that automatically connect to other devices to play a role of transmit and share information. Because when the connection is

established with another machine through IP addresses, it's easy for a hacker to infiltrate and spoof your ARP.

7. Set-Up Packet Filtering

In some cases ARP attackers will send ARP packets across the LAN that contain an attacker's MAC address and the victim's IP address. After the packet has sent, an attacker can start receiving data or wait and remain relatively undetected as they ramp up to launch a follow-up attack. Packet filtering and inspection deals with cache poisoned packets before they reach their destination.

8. Look at Your Malware Monitoring Settings

The antivirus and malware tools are also very helpful in preventing attacks against ARP spoofing. Always keep eye on the setting of malware monitoring and look for categories and selections that monitor for suspicious ARP traffic from endpoints. You should also enable any ARP spoofing prevention options and stop any endpoint processes that send suspicious ARP traffic.

7.6 RUN SPOOFING ATTACK

Identification and prevention are key to preventing spoofing attacks. However, you can increase your chances of staying safe and protecting your data by running your own spoofing attacks. Work with your security officer or IT team to run a spoofing attack to see if the techniques you're using are enough to keep your system and data safe.

As you detect new vulnerabilities, document your tests and techniques to keep track of what's working and what has failed. Run your own spoofing attacks once a quarter, or even once a month, to stay a step ahead of hackers and their evolving strategies. As you become more comfortable and fluent in the process, run workshops with employees on what to look for in attacks, and create a culture of security in your company.

7.6.1 Types of Identity Theft

Identity theft is always deals with the user's personal information like login credentials which is unavoidable in today's day in age. Following are some common forms of identity theft and steps you can take to mitigate your risk.

1. Financial Identity Theft

Financial identity theft is the most common type of identity theft. It always deals with the financial information of the user like credit card or debit card or some virtual card like gift card, vouchers etc. In this hacker will always claiming the credit card information and try to alter the credit score of the targeted user. This can be damaging to a victim's credit score and their ability to get a loan in the future. In 2014, identity thieves stole \$16 billion from 12.7 million identity fraud victims, according to Javelin Strategy & Research.

2. Medical Identity Theft

Medical identity theft occurs when the hackers get the information details of someone who has the insurance or mediclaims. He uses another individual's personally identifiable information to fraudulently obtain medical service, prescription drugs or medical insurance coverage. Users should always make the information related to the medical history or insurance confidential. So that no one will get the benefit of your sensitive data. As he pretends to be the patient and taking all the advantages provided by the insurer.

3. Criminal Identity Theft

This type of theft can be done through the criminal by giving the false information to police at the time they are arrested. For that they use state-issued identity documents or credentials that they have stolen from someone else, or they have simply created a fake ID. If this type of fraud works, the criminal charges could be filed against the identity theft victim, and the real criminal may be off the hook.

4. Child Identity Theft

This type of theft done with the minor people who are dependent on their parent. This can be done through the minor's personal information like child's age, name or birth date. In many cases, some parents are having the habit of keeping password of child name or birth date hence the attacker gets the information of child and do the theft. This type of fraud can not detect early as most children don't discover the problem until they become adults.

5. Identity Cloning & Concealment

This identity cloning makes the person's double role in the real world like happens in movies. They clone the identity of someone simply hide their true identity. These may be people who are hiding from creditors, illegal immigrants, or people who just want to become "anonymous" for other reasons. In some cases they search the identity like the same as they have and do the photo morphing on social media and act as they are the real one.

6. Synthetic Identity Theft

Synthetic identity theft is a type of identity theft where identities are completely or partially fabricated. This usually means the thief combines a real Social Security number with a name and birthdate that don't match those listed with the number. Synthetic identity theft is sometimes more difficult to recognize because it usually doesn't show up on the victim's credit report directly. Often, the credit report becomes a completely new file with the credit bureau or possibly as a sub-file on just one of the victim's credit reports. The primary victim of synthetic identity theft is the creditors who grant the lines of credit. Individual victims are usually affected if their name gets confused with a synthetic identity, or if negative information in a credit report sub-file damages their credit score.

Threats to IoT systems and devices translate to bigger security risks because of certain characteristics that the underlying technology possesses. These characteristics make IoT environments functional and efficient, but they are likely to be abused by threat actors.

These characteristics include:

- Gathering of abundant data: IoT systems are worked with the help of devices like sensors and accumulators which gather detailed data of the environments and users. With this data only the IoT systems function properly. However, this data can contain very valuable information of user and if it is not secured then it can be or compromised.
- Connection of virtual and physical environments: The IoT devices gathering the information form respective environment and on the basis of that information it acts or functioning. This feature of the IoT makes the distance shorten between virtual and physical system.
- Creation of complex environments: Complex IoT environment can make the availability and diversity of devices. “Complex” keyword use for the connection between the various IoT devices which are working in a single IoT environment that dynamic interactions between its devices are possible. This type of complex connection expands the capabilities of an IoT environment, but at the cost of a wider attack surface.
- Centralization of architecture: Centralization architecture means a main database connected to the various small databases. All data bases information sends to main database. The functions and the storage of data can be also done by applying a traditional centralized architecture.

Attack surface areas of the IoT?

in the following section we will discuss the part of its Internet of Things Project, or the surface areas, or areas in IoT systems and applications where threats and vulnerabilities may exist.

- Devices: Devices are the primary thing by which attacks are initiated. In that also the memory has the major part of vulnerabilities, firmware, physical interface, web interface, and network services. Default settings, outdated components, and unsecure update mechanisms, can also done by the attackers.
- Communication channels: Communication channels are responsible for making the connection of IoT components with one another. The protocols which are use to connect the IoT systems can have security issues that can affect the entire systems. IoT systems are also susceptible to known network attacks such as denial of service (DoS) and spoofing.

- Applications and software: The system gets in compromise situation with the Vulnerabilities in web applications and related software for IoT devices. Web applications can be exploited to steal user credentials or push malicious firmware updates.

How can the IoT be secured?

While creating any IoT device security should be on high priority. As it can be targeted by the attacker, and all of the major components of IoT systems can be exploited. following are some security guidelines to secure the IoT device:

- All data being gathered and information being stored should be accounted for. All the data shared across the network within an IoT system should be mapped properly. This includes all data like user credentials, or the data gathered by the sensors and environment.
- Each device being connected to the network should be configured with security in mind. Always check the setting before connecting a device to the network. This includes using strong username and password combinations, multifactor authentication, and encryption.
- The organization's security strategy should be built on the assumption of compromise. Although avoiding breach and compromise is important, acknowledging that there is no perfect defence against evolving threats can help in creating mitigation protocols that can significantly contain and reduce the effects of a successful attack.
- Each device should be physically secured. It contains the physical availability of the IoT device one should take into consideration while making connection of IoT devices. It should keep in secure place; if it is main system where all the transactions are recorded that should be kept in confidential place. There should be prohibited access for the unauthorized person as well as it should always lock.
- suspicious ARP traffic.

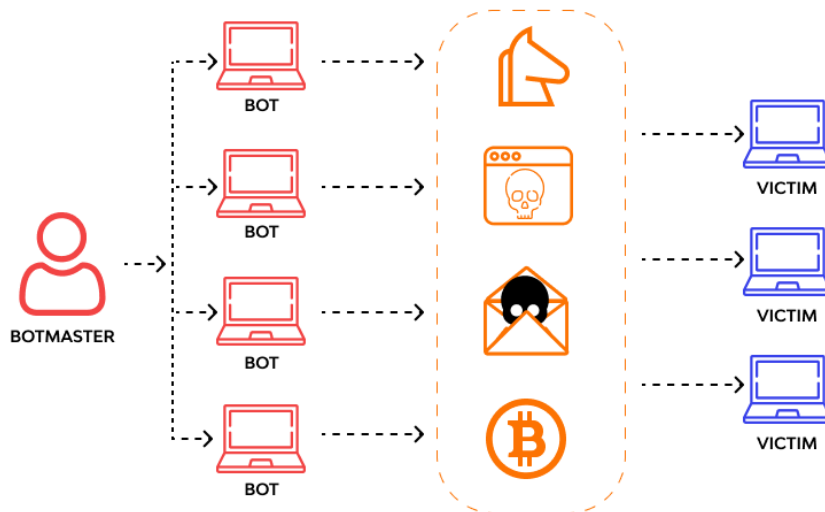
7.8 BOTNET

Botnet

Without the owner permission botnet tries to hijacked computers for the processes like sending spam emails, distributing malware, and framing DDoS attacks. it can be done in online game and in chatbot or chatroom also. it act like a person and talk with the user.

The controlling party of the botnet is known as a bot-herder and each individual machine, concerned in the network, is known as a bot.

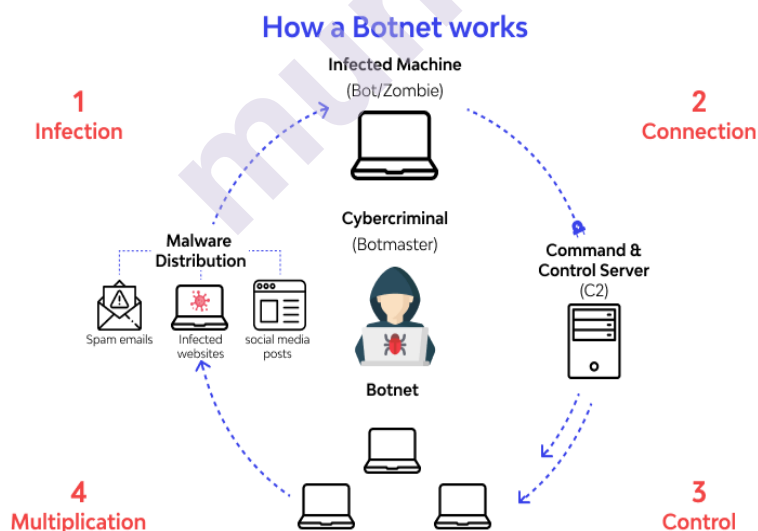
Botnets are responsible for handling the job of eliminating people who are violating the policies. it also keep an eye on the language used during the chats. this features, makes hackers or attackers were succeeded in using for password theft and tracking the keystrokes made on a specific device.



7.8.1 How Does a Botnet Work?

This process contains multiple stages. Botnets, attacks on large scale when it used in full capacity. Here the Hackers will use supplementary machinery to support botnets to enhance the ability of a botnet. Bot herder is what is required to lead the connected corrupted devices in the network. It's functional via remote commands and guides the devices to perform certain actions.

Bot or zombie computer is the term used for the infected system/device used in the creation of a botnet. The bots are mindless devices and behave as instructed or guided by the bot herder's command.



Stages of botnet building

1. Stage 1 - Prepare and Expose

In the first stage the attacker prepare the vulnerability to introduce into the user's device.

This vulnerability takes place in the website, human behavior, and application. By observing all the activities performed by the user, the hacker prepares a set-up to lure the target to get exposed to malware, knowingly or unknowingly.

2. **Stage 2 - Infecting the user via malware**

After preparing vulnerability the botnet performs is activating the malware so that the end-user is infected and has compromised security. Trojan virus or social engineering method can be used to infecting the device, in result the system gets corrupt and the targeted device infected with botnet malware.

Stage 3 - Controlling the targeted devices

Here in the last stage the botnet is gaining control over each device. Attacker prepares the technology to handle the device remotely and try to infect the system as much as he can. the zombie network is used to do this types of changes. after getting done all this changes now the attacker is able to gain admin-like access to the targeted devices or computers.

Types of Botnet Attacks

- **DDoS**

DDoS or Distributed Denial-of-service attack involves disturbing the customary traffic of a server in a way that actual or intended audiences are not able to access the website. The attack gains its efficacy from using the assorted corrupted systems as the sources of creating disturbing traffic. The corrupted devices involved could be computers, PC, IoT devices, and many other data-driven devices.

From another angle, a DDoS attack can look like a traffic jam created intentionally so that desired end-users don't reach their destinations.

- **Phishing**

One of the most common botnet attacks, phishing involves representing bad actors or hackers as reliable sources to lure victims to share crucial information like passwords and banking credentials. Using these details, bad actors can steal data and money. The attack is accomplished by multiple means like email phishing, vishing, and smishing. Phishing attack targeting a huge audience is often performed via spear and whale phishing

- **Brute Force Attacks**

The term "brute force" define the simplistic way in which the attack takes place. The attack is held with guessing credentials to gain unauthorized access. Primitive as they are, brute force attacks can be very effective.

The attack in brute force use bots to do their bidding. With this type of attack, the attackers will have a list of real or commonly used credentials and assign their bots to attack websites using these credentials.

In manual brute force credential cracking is time-consuming, and this can be done through using brute force attack software and tools to aid them. With the tools the attacker will attempt things like inputting numerous password combinations and accessing web applications by searching for the correct session ID, among others.

7.9 SUMMARY

If we are using some websites and online services which are not secure, we could face some security risks such as phishing, fraud, impersonation, malware, and many others. In Domain Name System (DNS) spoofing the hacker theft sensitive data or login credentials by distracting user from original website to fake website. In this user think that the website is trusted website and pass his login credentials as the website is looking real. The term “brute force” define the simplistic way in which the attack takes place. The attack is held with guessing credentials to gain unauthorized access. Primitive as they are, brute force attacks can be very effective. Without the owner permission botnet tries to hijacked computers for the processes like sending spam emails, distributing malware, and framing DDoS attacks. Threats to IoT systems and devices translate to bigger security risks because of certain characteristics that the underlying technology possesses. These characteristics make IoT environments functional and efficient, but they are likely to be abused by threat actors.

7.10 UNIT AND EXERCISE

1. Explain Man-in-the-Middle (MITM) Attack: and I's type and technology
2. Explain the concept of Buffer Overflow
3. State and explain prevention techniques of man in the middle attack
4. What is Address Resolution Protocol?
5. What is Run spoofing attack?
6. Explain Iot attack with its type and also explain prevention techniques
7. Explain the Concept of Botnet with its working and types

TROJANS AND OTHER ATTACKS

Unit Structure

- 8.0 Objective
- 8.1 Introduction
- 8.2 Steganography Overview
 - 8.2.1 Type of steganography
 - 8.2.2 Example of steganography
 - 8.2.3 How steganography is different from obfuscation
- 8.3 Steganography techniques
- 8.4 Social Engineering
 - 8.4.1 Social Engineering attack techniques
- 8.5 Example of physical engineering
- 8.6 Avoiding physical social engineering attack
 - 8.6.1 Remote social engineering test
- 8.7 Hybrid social engineering attack
- 8.8 Summary
- 8.9 Unit End Exercise

8.0 OBJECTIVE

This chapter will able you to understand the following concept

- Steganography and its type
- Some example of steganography
- The working of steganography
- Social engineering attack overview
- Some techniques of social engineering attack
- Physical social engineering attack examples
- How to avoid physical social engineering attack
- Hybrid social engineering attack

8.1 INTRODUCTION

Steganography

Steganography is a way of keeping information secret or media to avoid detection. It comes from the Greek words steganos, which means “covered” or “hidden,” and graph, which means “to write.” Hence, “hidden writing.”

With the help of steganography we can hide text, video, images, or even audio data. It's a one type of data abstraction where we will give access to the user as per their requirement not the hoe document.

Although the technique is used in data structure where we can hide data from user. Hence it is used in cyber security to protect the data from the unauthorized user.

8.2 STEGANOGRAPHY OVERVIEW

8.2.1 Steganography categorized into five types:

- Text Steganography
In this type of steganography it makes use of white spaces, capital letters, tabs, and other characters to hide data.
- Audio Steganography
Audio steganography is deals with digital audio formats which is used by audio manager like WAVE, MIDI, and AVI MPEG, using echo hiding, parity coding, and LSB coding, to name a few.
- Video Steganography
Video steganography making use of video formats like H.264, Mp4, MPEG, and AVI to hide data. And also it employs pictures to carry concealed data.
- Image Steganography
In this type the tool which is used is pixel intensities to hide information.
- Network Steganography
Network protocols use TCP, UDP, and IP as carriers.

The easiest type of attack or work with is Text steganography. As it doesn't require special skills or tools to write something. In everyday use the people can use text steganography but with specific condition. For example, while sending any message to the receivers may be one or more than one everyone in the message chain as well as they must be aware that there's a hidden message. The code should also be secret and if it lost then the reader is

unaware of the code! Remember to let the recipient know that they should be looking for the embedded message.

Steganography also covers many instances of watermarks that may be embedded in images. Whenever the hacker worked with online photo collections he has encountered watermarks on licensed images. Though not all such watermarks are considered steganography, some steganographic techniques store watermarks in data.

8.2.2 Example of steganography

- Invisible ink is used sometime while writing
- Artist using their initials or name with embedding text in a picture
- Backward masking a message in an audio file (remember those stories of evil messages recorded backward on rock and roll records?)
- Concealing concept used in hiding data with metadata or within a file header
- In some case of video it is simple trick of hiding an image in a video, which will be viewable only if the video is played at a particular frame rate
- The RRB image is used to hide data or keeping secret message in either the green, blue, or red channels

Steganography can be used by the user in both ways constructive and destructive purposes. For example, certified ethical hackers use their skills in education and business institutions, intelligence agencies, the military, to protect the data and embed confidential messages and information in plain sight.

Whereas, the other type of user which are making use of steganography for criminal purpose. In which they have use steganography to corrupt data files or hide malware in otherwise innocent documents. For example, attackers can use BASH and PowerShell scripts to launch automated attacks, embedding scripts in Word and Excel documents. When a poor, unsuspecting user clicks one of those documents open, they activate the secret, hidden script, and chaos ensues.



8.2.3 How Steganography Differs From Obfuscation

Other type of steganography is Obfuscation, which is defined as hiding information, but the difference is in the former method which makes the message hard to interpret, read, or decode. Hence the information makes sense since to obfuscate means to render something unclear, unintelligible, or obscure.

Ethical hacker employ obfuscation to protect the data like programming code or sensitive information. This process makes it difficult for hackers to read the codes in the first place, which in turn prevents them from exploiting the data.

To sum it up, while steganography is a form of obfuscation, the reverse doesn't apply.

8.3 STEGANOGRAPHY TECHNIQUES

1. Secure Cover Selection

Secure Cover Selection comes with finding the correct block of image to carry malware to destroy the data. After this the hackers always compare their chosen image medium with the malware blocks. If an image block is exactly matches with the malware, the hackers use that image block to fit it into the carrier image, then he will create an identical image infected with the malware. This image subsequently passes quickly through threat detection methods.

2. Least Significant Bit

The technique is look like put-down action, however, in this scenario the grayscale is considered as well as it refers to pixels. When the image is readable at that time the grayscale image pixels are distributed into eight bits, and the last bit, the eighth one, is called the Least Significant Bit. And this bit is used by hackers to embed malicious code because the overall pixel value will be reduced by only one, and this small change cannot be guess by human and the difference in the image cannot be detected. So, the normal user doesn't know about the image is carrying something dangerous within.

3. Palette-Based Technique

It is just like the Least Significant Bit technique, in this Palette-Based Technique it basically relies on images. Hackers embed their message with image in palette-based with using extensions such as GIF, making it difficult for cybersecurity threat hunters or ethical hackers to detect the attack.

8.4 SOCIAL ENGINEERING

Through human interaction malicious activities are done which is called as Social engineering which has a broad range. It makes user manipulation to trick and influence the user to make security mistakes or giving away sensitive information.

It can be done in one or more steps. A hacker or bad user's first preference is to gather the victim's necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. After this the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information.



Social engineering involves human intervention that makes social engineering very dangerous. Human Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

8.4.1 Social engineering attack techniques

Many of the ways are there of social engineering attacks and can be performed anywhere where human interaction is involved.

1. Baiting

As per the name, in baiting attacks a hacker uses a false promise to pique a victim's greed or curiosity. They trap users and steals their personal information or inflicts their systems with malware.

The physical media is used to revile form of baiting to disperse malware. For example, attackers leave the bait—typically malware-infected flash drives—in conspicuous areas where potential victims are certain to see them (e.g., bathrooms, elevators, the parking lot of

a targeted company). The bait has an authentic look to it, such as a label presenting it as the company's payroll list.

Victims pick up the bait out of curiosity and insert it into a work or home computer, resulting in automatic malware installation on the system.

Baiting scams don't necessarily have to be carried out in the physical world. Online forms of baiting consist of enticing ads that lead to malicious sites or that encourage users to download a malware-infected application.

2. Scareware

False alarms and fictitious threats are used in Scareware in which the user is bombarded with this. This is look like a repairable software techniques which users may think their system is infected with malware, and the system is asking to install software that has no real benefit or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.

A common scareware example is while using the web browser the legitimate-looking popup banners appearing while surfing the web, displaying such text such as, "Your computer has many harmful spyware programs." And it may offers to install the tool often malware-infected, or will direct you to a malicious site where your computer becomes infected.

The spam emails can be used in scareware as it is distributed fast and it also can contain bogus warnings, or makes offers for users to buy worthless/harmful services.

3. Pretexting

Crafted lies prepare by attacker using the obtains information is considered in pretexting. In this scam preparator pretending to need sensitive information from a victim so as to perform a critical task.

The main aim is to gain the trust of the victim hence they starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. After getting the trust they asks questions that are ostensibly required to confirm the victim's identity, and gather important personal data of the victim.

All type information and records is gathered using this scam, this information may consist security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

4. Phishing

It is one of the most popular social engineering type of attack, phishing scams can be done through the email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

The best example is an email sent to users giving an online service that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to false website which look like identical in appearance to its original version prompting the unsuspecting user to enter their current credentials and new password. Once the form submission is done the information is sent to the attacker.

Given that identical, or near-identical, messages are sent to all users in phishing campaigns, detecting and blocking them are much easier for mail servers having access to threat sharing platforms.

5. Spear phishing

Most targeted version of the attack is phishing scam where an attacker chooses specific individuals or enterprises or authorities. And send them messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. It require more efforts as it may consist sensitive information of the user or on behalf of the perpetrator and may take weeks and months to pull off. In this type of attack the attacker who, in impersonating an organization's IT consultant, sends an email to one or more employees. It looks like real emails in which word and signed exactly match with the consultant normally does, hence the recipients thinking it's an authentic message. The message prompts recipients to change their password and provides them with a link that redirects them to a malicious page where the attacker now captures their credentials.

8.5 EXAPMLES OF PHYSICAL ENGINEERING

1. The fake IT guy



The hacker can be known as fake IT guy. Where a hacker shows pretend to be an IT technician, who will check the connection and data maintenance part of the server, printer or other network device. Many smart devices need interval maintenance and when they need maintenance, which gives these kinds of attacks plausibility. In some scenarios these attackers will give fake serial or device numbers to lend credence to their visit. Most companies will run a check on the numbers first, but what if the attacker has done some 'dumpster diving' beforehand? If they've waded through your company's rubbish skips and found legitimate serial and device numbers on discarded boxes, they'll be able to pass your first test. And if it's the only test required, they're in.

2. Tailgating

This type of attack can be made by the attacker by following an authorised person into a secure area to get the information of the user. This happens naturally when multiple people pass through same doors at same time. This can be done while swipes an ID card or taps in a code and the person behind follows through the open door, entering the area without having presented any kind of identification. This is most likely to happen in MNC organization as everyone has its own card to access the door and in case of residential buildings the phone used by the people in lift.

3. The 'coffee trick'



The 'coffee trick' is a more sophisticated form of tailgating. It's where an unauthorised person holding a cup of coffee in each hand walks towards an office door. An unsuspecting person passing through or walking nearby will, wanting to be helpful, hold it open for them. Voila, the attacker has access. This is classic social engineering—preying on people's proclivity for kindness.

4. Shoulder surfing



In this type of attack the hacker keep eye on the authorized person and watching the unsuspecting victim while they're entering passwords and other sensitive information. But it doesn't have to be at close range the hacker literally looking over their shoulder. It could be from a distance using binoculars or hidden cameras.

5. Dumpster diving



The company's wastage are considered in this type of attack , dumpster diving is where attackers find out the company's rubbish skips and looking for documents containing sensitive or confidential information. This information they use to gain access to your company.

6. Theft of documents

This can happen if you leave papers and documents lying around and a visitor to your building sees something they shouldn't. Or worse, they steal the document on their way through.

8.6 AVOIDING PHYSICAL SOCIAL ENGINEERING ATTACK

Following are some tricks to be use to avoiding physical social engineering attacks

Practical measures

One way to secure the data is introducing Anti-tailgating doors, for example, make tailgating virtually impossible to stop the social engineering attack.

Second easy practical solution is to the keep the desk clear when you are not on the chair that may minimize the risk of document theft. Always ensure that the end of the day the document should be kept in drawer and drawer should be locked. Also shared the security policy with your colleagues and tell them to shred any sensitive documents in their possession after they no longer need them. Always used register to make the entry of the outsider guest and the purpose of meeting, name of the person to whom he is going to meet and the nature of work should also be mentioned in register.

Practical measures are all well and good, but in the end, it won't be security barriers, anti-tailgating doors and clear-desk policies that keep your business safe from a social engineering attack. It will be your employees knowing what the risks are and how to avoid them.

Training is the best way of making the employees aware about the security threats. Also maintain a security culture within your organisation so that employees are more alert. This type of alert involves providing them with a rigid physical security policy and continually raising awareness of the importance of upholding it. It also include guidance on clear desks and shredding as well as not holding doors open for people they don't recognise and reporting any tailgating attempts to your security teams.

8.6.1 Remote Social Engineering Test

Remote Social Engineering is ideally performed on a semi-annual basis to provide an accurate representation of your employees' security awareness. It includes a wide range of attacks, each specially designed to give important information on employee reactions.

There are several options for remote social engineering:

Option 1: Phone-based Phishing

Digital Defense will place calls to your internal staff members and, upon request, to your suppliers to assess their security awareness. We specifically attempt to obtain information that could be used to gain unauthorized or falsely authorized access to your network resources or data.

Option 2: Vishing

Digital Defense will send targeted emails with an action request for the user to call a local number for more information. Digital Defense answers the call and conducts social engineering (i.e. “vishing”). We specifically attempt to obtain information that could be used to gain unauthorized or falsely authorized access to your network resources or data.

Option 3: Web-based Phishing

In this Digital Defense the hacker will send targeted emails with an action request for the user to visit a website which is designed to elicit sensitive information (i.e. phishing). This method involves creating a custom website which looks and feels like your intranet or public site and then capturing the input provided.

Option 4: Email-based Phishing

In this Digital Defense the hacker will send email to targeted employees with an action request for the user to reply back to the message with information (i.e. phishing). Data is then captured and analyzed for sensitivity

USB Drops (physical initiation and remote analysis)

With the help of USB drives digital defense check and load the data with custom-developed software that, when inserted into a computer, will auto run and transmit the username, hostname, and IP address in a secure fashion to Digital Defense. The aim is to determine how susceptible staff are to opening these USB drives. Digital Defense will report on the number of incidents of users running this software, the associated user name, system name, and IP address.

8.7 HYBRID SOCIAL ENGINEERING ATTACK



Now a days, Fraud phone calls are increasing day by day and gets high popularity. They create these bogus “bank” calls is to get and utilize personal identification information stolen using malware to give fraudsters credibility with this they collect the missing information required to success their scams.

The general phenomenon of stealing data using is can be done through one channel such as the web and making use of different channel or context such as social engineering attacks. To get defend against the new wave of hybrid attacks requires both technology ae used such as to detect malware and vigilance from the users of online services.

In old days Traditional financial malware fraud can be done through by starting identifying the targeted bank and learning how their online banking service operations are performed. Once all the information get by fraudsters

they do the study and understand the online banking flows and security processes, a fraudulent aim is to design and prepare corresponding malware attack with configuration. At the last, the bank clients are infected with the malware and fraud starts its execution sequence.

In the other forms of financial malware the fraud work in reverse order. Here the malware is first infected in the victims' machines and malware logs online activity and banking credentials, and then the fraudsters use that credential data fished from malware logs to access online banking sites and perpetrate fraud.

However, the problem with this method is, in many cases, the data collected by the malware is insufficient to commit the actual fraud:

The one time password (OTP) authentication credentials originally collected are no longer valid

Banks require Transaction Signing to transfer money

Additional authentication data is required by the bank when logging in from a new IP address.

The professional caller services are used by attackers to obtain the missing data required to make a successful online fraud. They may prepare or train their staff to do the advertisement offers a phone service with professional callers, fluent in English and European languages, who can impersonate male and female, as well as old and young voices. As per the customer requirement these hackers were giving calls to private customers, banks, shops, post offices and any other organisations. They'll also going to prepare the spoof phone numbers to accept calls in case victims should want to call back for any reason. Although the actual caller's scripts are not shared in the forum advertisement we can imagine scripts used to collect the missing data would look something like:

Step 1: Caller establishing credibility

In this step the hacker is having the basic information of the user as the hacker gain data by the malware to gain credibility, for example the hacker will ask "Are you John Smith, living at their address, with credit card number ending with 2345?"

Step 2: Caller collects missing data

Once the caller has established credibility, they will go on to collect:

- a) The SMS OTP – for example "you just get one OTP via SMS can you give me that OTP so that we can make sure you are John Smith, or can you please read it for me?"
- b) Collect other additional authentication information from the user such as "to verify you, can you please give me the last four digits of your card number?"

- c) They can also demand the user to generate a transaction signing code with fraudulent payee and amount information, for example “We need to calibrate your transaction signing reader so could you please enter the following details online and then tell us what happens.”

8.8 SUMMARY

With the help of steganography we can hide text, video, images, or even audio data. It's a one type of data abstraction where we will give access to the user as per their requirement not the whole document. Steganography can be classified into 5 types: text steganography, audio steganography, video steganography, image steganography, and network steganography. There are three techniques of steganography: secure cover selection, least significant bit and palette based technique. Social engineering involves human intervention that makes social engineering very dangerous. Human mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion. The social engineering technique is also called as physical social engineering attack through which the human can make fraud with the user. In this chapter the prevention technique is also discussed with examples like remote social engineering test. Now a days, Fraud phone calls are increasing day by day and get high popularity. They create these bogus “bank” calls to get and utilize personal identification information stolen using malware to give fraudsters credibility with this they collect the missing information required to success their scams. This technique is called as hybrid social engineering attack.

8.9 UNIT AND EXERCISE

1. List and explain types of steganography.
2. State steganography with examples
3. Explain how the steganography is different from obfuscation
4. Write a note on hybrid social engineering attack
5. How attacker perform social engineering attack
6. Explain with examples physical social engineering attack
7. How to avoid physical social engineering attack
8. What is remote social engineering test

SESSION HIJACKING

Unit Structure

- 9.1 Introduction
- 9.2 Session hijacking
- 9.3 How does session hijacking work?
- 9.4 What Do Attackers Gain from Session Hijacking?
- 9.5 How to prevent Session Hijacking
- 9.6 Web Servers
 - 9.6.1 How does Web Server work?
 - 9.6.2 Causes of webserver being compromised
- 9.7 Web Server Attacks
 - 9.7.1 Effects of successful attacks
- 9.8 Stages of Web Server attacks
- 9.9 Countermeasures
- 9.10 Web Application
 - 9.10.1 Web Application Components
 - 9.10.2 Models of Web Application Components
 - 9.10.3 Web Application Architecture Layers
- 9.11 Common Threats to Web Applications and How to Avoid Them

9.1 INTRODUCTION

HTTP is stateless protocol, so application designers had to develop a way to track the state between multiple connections from the same user, instead of requesting the user to authenticate upon each click in a web application. A session is a series of interactions between two communication end points that occurs during the span of a single connection. When a user logs into an application, a session is created on the server to maintain the state for other requests coming from the same user.

Applications use sessions to store parameters that are relevant to the user. The session is kept "alive" on the server as long as user is logged on to the system. The session is destroyed when the user logs-out from the system or after a predefined period of inactivity. When the session is destroyed, the user's data should also be deleted from the allocated memory space.

A **session ID** is an identification string (usually a long, random, alphanumeric string) that is exchanged between client and the server. Session IDs are commonly stored in cookies, URLs and hidden fields of web pages. There are several security problems associated with session IDs. Many popular websites use algorithms based on easily predictable variables, such as time or IP address, in order to generate the Session IDs, causing their session IDs to be predictable. If SSL encryption is not used, Session IDs are transmitted in the clear, plain text and are susceptible to eavesdropping attack.

9.2 SESSION HIJACKING

Session hijacking is an attack where a user session is taken over by an attacker. A session starts when you log into a service and ends when you log out; for example, your banking application. The attack relies on the attacker's knowledge of your session cookie, so it is also called cookie hijacking or cookie side-jacking. Although any computer's session could be hijacked, session hijacking most commonly applies to browser sessions and web applications.

In most cases when you log into a web application (for example, via a username and password), the server sets a temporary session cookie in your browser to remember that you are currently logged in and authenticated. HTTP is a stateless protocol and session cookies attached to every HTTP header are the most popular way for the server to identify your browser or your current session.

To perform session hijacking, an attacker needs to know the victim's session ID (session key). This can be obtained by stealing the session cookie or convincing the user to click a malicious link containing a prepared session ID. In both cases, after the user is authenticated on the server, the attacker can take over (hijack) the session by using the same session ID for their own browser session. The server is then fooled into treating the attacker's connection as the original user's valid session.

9.3 HOW DOES SESSION HIJACKING WORK?

The most popular culprits for carrying out a session hijacking are session sniffing, predictable session token ID, man in the browser, cross-site scripting, session sidejacking, session fixation.

- **Session sniffing**

It is one of the basic techniques used with application-layer session hijacking. The attacker uses a sniffer tool such as Wireshark, or a proxy, such as OWASP Zed, to capture network traffic which contains the session ID between a website and a client. Once an attacker captures this value, he can use this valid token to gain unauthorized access into system.

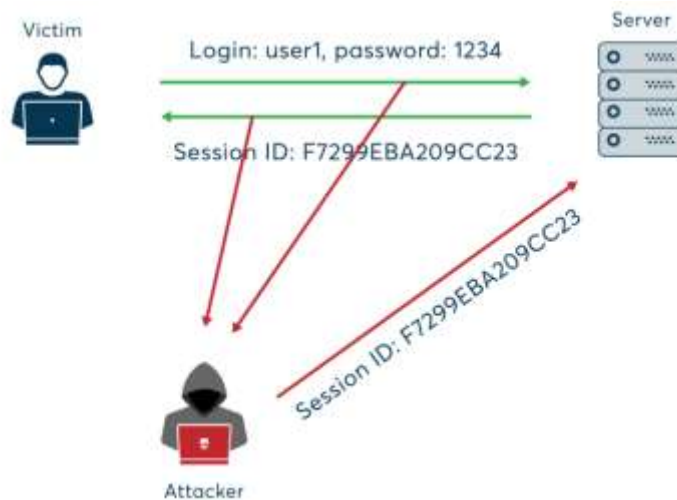


Figure 9.1 Illustration of session hijacking using packet sniffing

- **Predictable sessions token ID**

Many web servers use a custom algorithm or some predefined pattern to generate session IDs. Greater the predictability of a session token, the weaker it is and the easier it is to predict. If an attacker can capture several IDs and analyze its pattern, he may predict a valid session ID.

- **Man-in-the-browser attack**

This is similar to a man-in-the-middle attack, but the attacker must first infect the victim's computer with a Trojan through some form of trickery or deceit. Once the victim is tricked into installing malware onto the system, the malware waits for the victim to visit a targeted site. The man-in-the-browser malware can invisibly modify transaction information and it can also create additional transactions without the user knowing. Because the requests are initiated from the victim's computer, it is very difficult for the web service to detect that the requests are fake.

- **Cross-site scripting**

Cybercriminals exploit server or application vulnerabilities to inject client-side scripts into web pages. This causes the browser to execute arbitrary code when it loads a compromised page. If HttpOnly isn't set in session cookies, cybercriminals can gain access to the session key through injected scripts, giving them the information, they need for session hijacking.

- **Session side jacking**

Cybercriminals can use packet sniffing to monitor a victim's network traffic and intercept session cookies after the user has authenticated on the server. If TLS encryption is only used for login pages and not for the entire session, cybercriminals can hijack the session, act as the user within the targeted web application.

- **Session fixation attacks**

This technique steals a valid session ID that is yet to be authenticated. Then, the attacker tries to trick the user into authenticating with this ID. Once authenticated, the attacker now has access to the victim's computer. Session fixation explores a limitation in the way the web application manages a session ID. Three common variations exist: session tokens hidden in an URL argument, session tokens hidden in a form field and session tokens hidden in a session cookie.

9.4 WHAT DO ATTACKERS GAIN FROM SESSION HIJACKING?

Once cybercriminals have hijacked a session, they can do virtually anything that the legitimate user was authorized to do during the active session. The most severe examples include transferring money from the user's bank account, buying merchandise from web stores, accessing personally identifiable information for identity theft, and even stealing data from company systems.

9.5 HOW TO PREVENT SESSION HIJACKING

There's a lot you can do to help protect yourself online. Take these steps to help prevent session hijacking and increase your online security:

1. **Avoid public Wi-Fi**

Never use public Wi-Fi, for important transactions like banking, online shopping, or logging into your email or social media accounts. There may be a cybercriminal at the next table who is using packet sniffing to capture session cookies and other information.

2. **Use a VPN**

If you want to use public Wi-Fi, get a virtual private network (VPN) to help stay safe and keep session hijackers out of your sessions. A VPN masks your IP address and keeps your online activities private by creating a "private tunnel" through which all your online activity travels. A VPN encrypts the data you send and receive.

3. **Add security software**

Install licensed security software on your devices and make sure to update it regularly. You can also set automatic updates. Security software can detect viruses and protect you from malware, including the malware attackers who perform session hijacking.

4. **Watch out for scams**

Avoid clicking on any link in an email unless you've verified that it's from a legitimate sender. Session hijackers may send you an email with a link and showing an urgency to click it. The link may install

malware on your device or take you to a login page that will log you into a site using a session ID provided by the attacker.

5. Be aware of site security

Reputable banks, email providers, online merchants, and social media sites have safeguards in place to avoid session hijacking. Smart site owners will install HTTPS on the entire site, not just their homepage. They'll also find and close security loopholes promptly.

The possibility of falling victim to a session hijacking attack can be scary. But just taking these steps will go a long way toward protecting you from these attackers who want to steal your session information.

Over the past decade, more individuals have access to the internet than ever before. Many organizations develop web-based applications, which users can use to interact with them. But improper configuration and poorly written codes in web servers are a threat and can be used to gain unauthorized access to the servers' sensitive data.

9.6 WEB SERVERS

Web servers are hardware, computer, or software, used to host websites. **Web server** is a computer where the web content is stored. Web servers run on various operating systems connected to the back-end database and run various applications. The use of web servers has increased in recent years as most online services are implemented as web applications. Web servers are mostly used in web hosting or the hosting of data for websites and web applications.

9.6.1 How does Web Server work?



Figure 9.2 Web Server

A web server can be accessed through a websites' domain name. It delivers the website's content to the requesting user by using Hypertext Transfer Protocol (**HTTP**). A web server can be a hardware or software or both together. It is used in the transfer of files, email communications, and for many other purposes. Web servers are so powerful that they can deliver the contents of the websites to thousands of visitors simultaneously.

9.6.2 Causes of webservers being compromised

1. Personal Computer Security

When a personal computer is hacked, the attack could include stealing saved information for websites and logins. This gives the criminal access to online

resources using your own credentials. These hacks can come from compromised websites, infected software or through bots scanning various IP addresses looking for weakness in a system.

2. Indirect Server Hacks

A direct assault on your website isn't the only way the criminal can gain access to its pages. Many sites are hosted on "shared" server. This means that all accounts hosted on that server are utilizing the same drives, CPUs and memory space. If any one of these websites are compromised, it could lead to hackers accessing your data indirectly. Even a hack aimed specifically at the hosting company can put the information at risk.

3. Responding to Phishing Email

Phishing attacks are **the practice of sending fraudulent communications that appear to come from a reputable source**. It is usually done through email. Its goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

The hacker will create an email that looks legitimate asking for passwords or providing links to "log in" to your account. In many cases, these links lead to hacked websites that are hosting a false page in order to obtain the information.

4. Outdated Scripts

Scripts are often used to develop a website to control everything from graphics to databases. They are also a common element for hackers to gain control of the website itself. When a script is detected as having an exploit, developers will create updates in order to prevent cyber-attacks. Even installation scripts for web-based applications, plugins and add-ons can open the doors to hackers.

5. Lack of security policy and procedures

Lack of a security policy and procedures such as updating antivirus software, patching the operating system and web server software can create security loopholes for attackers.

6. Bugs in the operating system and web servers

Discovered bugs in the operating system or web server software can also be exploited to gain unauthorized access to the system.

9.7 WEB SERVER ATTACKS

Web Server Attacks techniques are given below:

- **Dos/DDoS**

Denial of Service is an attack where an attacker attacks by sending multiple service request packets overwhelming the servicing capability of the web server, resulting in crash and unavailability for the users.

- **DNS Server Hijacking**

DNS Server Hijacking is also known as DNS redirection, where an attacker modifies DNS configurations. DNS redirection's primary use is **pharming**, where attackers display unwanted ads to generate some revenue, and **Phishing**--where attackers show fake websites to steal credentials.

- **Directory Traversal Attacks**

Directory traversal, also is known as Path Traversal, is an HTTP attack that allows attackers to access restricted directories and steal sensitive information about the system using dot and slash sequences.

- **Man in the Middle Attack**

A Man in the Middle / Sniffing attack happens when an attacker sits between a user and the application to sniff the packets. The attacker's goal is to steal sensitive information such as login credentials, credit card details, etc.

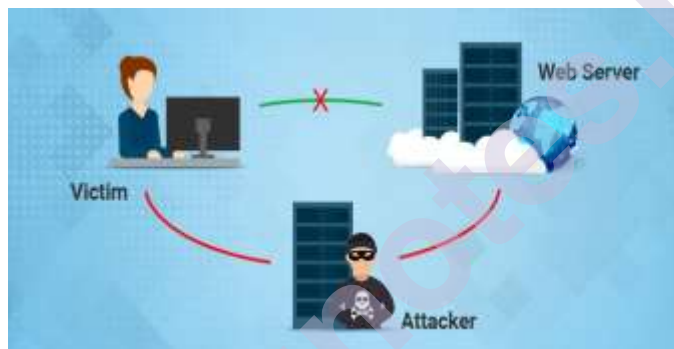


Figure 9.3 Man in the Middle attack

- **Phishing Attacks**

A Phishing attack is done to obtain sensitive, confidential information such as usernames, passwords, credit card numbers, etc. It is a practice of fraudulent attempts that appear to come from a reputable source. Scammers mostly use emails and text messages to trick you in a phishing attack.

- **Website Defacement**

Website Defacement is an attack where an attacker changes the website/web page's visual appearance with their messages. SQL injection attack is mainly used in web defacement. An attacker can add SQL strings to craft a query maliciously and exploit the webserver.

- **Web Server Misconfiguration**

Web Server Misconfiguration is when unnecessary services are enabled, and default configurations are being used. The attacker may

identify weaknesses in terms of remote functions or default certifications and can exploit them. An attacker can easily compromise systems by some attacks such as SQL Injection, Command Injection.

- **Web Cache Poisoning**

A web cache is an information technology for storing web documents such as web pages, passwords and images temporarily. Web Cache Poisoning is a technique where the attacker sends fake entry requests to the server, wipes out all the server's actual caches and redirects the user to the malicious website.

- **SSH Brute Force Attacks**

Brute force is where an attacker uses trial and error to guess login information by submitting many passwords or paraphrases. In an SSH Brute force attack, the intruder brute forces the SSH tunnel to use an encrypted tunnel. The encrypted tunnel is for communicating between the hosts. Hence, the attacker gains unauthorized access to the tunnel.

- **Web Server Password Cracking Attacks**

In this attack, the attacker cracks the server password and uses it to perform more attacks. Some of the common password cracking tools are Hydra, John the Ripper, Hashcat, Aircrack, etc.

9.7.1 Effects of successful attacks

- **An organization's reputation can be ruined** if the attacker edits the website content and includes malicious information or links to a porn website.
- **The web server can be used to install malicious software on user's system who visit the compromised website.** The malicious software downloaded onto the visitor's computer can be a virus, Trojan or Botnet Software, etc.
- **Compromised user data may be used for fraudulent activities** which may lead to business loss or lawsuits from the users who entrusted their details with the organization.

9.8 STAGES OF WEB SERVER ATTACKS

Following are the stages of web server's attack methodology:

1. Information Gathering

Every attacker tries to gather as much information as possible about the target web server. The attacker gathers the information and then analyzes the information so as to seek out lapses within the current **security mechanism** of the online server.

2. Web Server Footprinting

The purpose of **footprinting** is to collect more information about security aspects of an internet server with the help of tools or footprinting techniques. The main purpose is to understand about the online server's remote access capabilities, its ports and services, and other aspects of its security.

3. Website Mirroring

Website mirroring is a method of copying a website and its content onto another server for offline browsing. With a mirrored website, an attacker can view the detailed structure of the web site.

4. Vulnerability Scanning

Vulnerability scanning is a common practice to seek out **vulnerabilities** and misconfiguration of an internet server. Attackers scan for vulnerabilities with the help of automated tools referred to as vulnerability scanners.

Vulnerability scanners are automated tools that allow organizations to check if their networks, systems and applications have security weaknesses that could expose them to attacks.

5. Session Hijacking

A session hijacking attack happens when an attacker takes over your internet session — for instance, while you're checking your credit card balance, paying your bills, or shopping at an online store. Session hijackers usually target browser or web application sessions.

6. Web Server Passwords Hacking

Attackers use **password-cracking** methods such as brute force attacks, hybrid attacks, dictionary attacks, and so on to crack web server's password.

9.9 COUNTERMEASURES

- **Always Keep Your Firewalls and Antivirus Software Updated**

By protecting your own computer system, you can eliminate some of the threats to your website. Even the simplest of malware attacks can lead to severe complications.

- **Use Current Versions of Integrated Software**

If a version of an app, plugin or widget hasn't been updated in more than a year, it may be better to look for an alternative. Older versions of these may be riddled with exploits.

- **Use Hosting Companies That Routinely Update Security**

Most web-hosting companies offer exceptional security precautions. Make sure your hosting provider uses the latest in antivirus, database and programming language support.

- **Never Interact Directly with Unsolicited Email**

Links within emails may lead you to fake websites. It's better to manually type in addresses into your browser to reduce the risk of exposure. Remember, Genuine companies will never ask you for your credentials through an email. You can also incorporate email encryption to boost the security of yourself and your recipients.

- **Always Update Your Scripts and Remove Installation Files**

If you're using third-party scripts, make sure you're using the most current versions. After installing any addition to the site, delete the installation files.

- **Never Underestimate Your Site's Importance to Hackers**

It only takes a moment for a hacker to gain control of an unprotected site for a variety of nefarious purposes. Don't think that because your site isn't as popular as Google that you're safe from a hacking attempt.

9.10 WEB APPLICATION

A website application, popularly known as a web app, is a software application program that uses web-based technology to perform specific tasks. Remote web servers host web applications and store relevant information from several connected computers. You can use a client program to run the web applications and access or enter the required data. That is why web apps are often referred as client-server programs.

Example of a web application

Web applications include shopping carts, online forms, word processors, spreadsheets, video and photo editing, file conversion, file scanning, and email programs such as Gmail, Yahoo and AOL. Popular applications include Google Apps and Microsoft 365.

Google Apps for Work has Gmail, Google Docs, Google Sheets, Google Slides, online storage and more. Other functionalities include online sharing of documents and calendars. This lets all team members access the same version of a document simultaneously.

Typical web application flow looks like this:

1. **User** sends a request to the **web server** over the **Internet**, either through a web browser or the application's user interface.
2. **Web server** forwards this request to the appropriate **web application server**.

3. **Web application server** performs the requested task such as querying the **database** or processing the data and then generates the results of the requested data.
4. **Web application server** sends results to the **web server** with the requested information or processed data.
5. **Web server** responds back to the client with the requested information which then appears on the user's device.

9.10.1 Web Application Components

Web application components are as follows:

- **UI/UX Web Application Components**

This includes activity logs, dashboards, notifications, settings, statistics etc. These components have nothing to do with the operation of a web application architecture. Instead, they are part of the interface layout plan of a web app.

- **Structural Components**

The two major structural components of a web app are client and server side.

- **Client Component**

The client component is developed in CSS, HTML and JS. As it exists within the user's web browser, there is no need for operating system or device-related adjustments. The client component is a representation of a web application's functionality that the end-user interacts with.

- **Server Component**

The server component can be built using combination of several programming languages and frameworks including Java, .Net, NodeJS, PHP, Python, and Ruby on Rails. The server component has at least two parts; app logic and database. The former is the main control center of the web application while the latter is where all the persistent data is stored.

9.10.2 Models of Web Application Components

Depending on the total number of servers and databases used for a web application, the model of a web app is decided. It can be any of the following three types:

1. **One Web Server, One Database**

It is the simplest as well as the least reliable web app component model. This model uses a single server as well as a single database. A

web app builds on such model will go down if the server goes down. Hence, it isn't much reliable.

One web server, one database web application component model is not typically used for real web applications. It is mostly used for running test projects as well as with the intent of learning and understanding the fundamentals of the web application.

2. **Multiple Web Servers, One Database (At a Machine Rather than the Web server)**

The idea with this type of model is that the webserver doesn't store any data. When the webserver gets information from a client, it processes the same and then writes it to the database, which is managed outside of the server. This is sometimes also referred to as a stateless architecture.

At least 2 web servers are required for this web application component model for avoiding failure. Even when one of the web servers goes down, another one takes over immediately.

All requests made will be redirected automatically to the new server and the web app will continue its execution. Hence, reliability is better compared to the single server with inherent database model. However, if the database crashes the web app will follow to do the same.

3. **Multiple Web Server, Multiple Databases**

It is the most efficient web application component model because neither the web servers nor the databases have a single point of failure. There are two options for this type of model either to store identical data in all the employed databases or distribute it evenly among them.

Not more than 2 databases are required typically for the former case, while for the latter case some data might become unavailable in the scenario of a database crash. However, DBMS normalization is used in both scenarios.

When the scale is large i.e. more than 5 web servers or databases or both, it is advised to install load balancers.

9.10.3 Web Application Architecture Layers

Every **web application architecture** is built based on a layered architecture. However, it all depends on the app scale. Large applications may have four to six layers whereas small applications may have three layers. Each layer functions independently and its components are closed. Below are the **four commonest layers of web application architecture**.

1. **Presentation Layer**

The presentation layer aids in communication between the browser and the user interface of the application that eases the overall user

interaction. Every presentation layer is created through JavaScript, HTML, CSS and its frameworks.

2. **Business Layer**

The business layer helps in processing the browser requests, performs the business logic of the requests, and shares the same back to the previous layer. This layer primarily determines the business rules of the web app.

3. **Data Access Layer**

The data access layer is used to access data from XML, binary files, and other types of storage. In addition, it also helps in creating, reading, updating and deleting operations.

4. **Data Service Layer**

The final one is the data service layer which ensures data security and stores the entire data. This layer safeguards the data by separating the app business logic from the client-side.

9.11 COMMON THREATS TO WEB APPLICATIONS AND HOW TO AVOID THEM

- **Security Misconfiguration**

A functioning web application is usually supported by some complex elements that make up its security infrastructure. This includes databases, OS, firewalls, servers, and other application software or devices. All these elements require **frequent maintenance and configuration** to keep the web application running properly.

Before using a web application, communicate with the developers to understand the security and priority measures that have been undertaken for its development.

Whenever possible, schedule penetration tests for web applications to test out its capability of handling sensitive data. This can help to find out web application vulnerabilities immediately.

- **Malware**

The presence of malware is yet another most common threats that companies commonly have to guard against. Upon downloading malware, severe repercussions like activity monitoring, access to confidential information, and backdoor access to large scale data breaches can be incurred.

Malware can be categorized into different groups since they work to achieve different goals- Spyware, Viruses, Ransomware, Worms, and Trojans.



To overcome this problem, make sure to install and keep firewalls up to date. Ensure that all your operating systems have been updated as well. You can also engage developers and antispam/virus experts to come up with **preventative measures to remove and spot malware infections**.

Make sure to backup important files in external safe environments. This essentially means that if you are locked out, you will be able to access all your information without having to pay due to ransomware.

Do perform checks on your security software, the browsers used and third-party plugins. If there are patches and updates for the plugins, make sure to update it.

- **Injection Attacks**

These types of attacks come in a variety of different injection types and are primed to attack the data in web applications since web applications require data to function.

The more data is required, the more opportunities for injection attacks to target. Some examples of these attacks include **SQL injection, code injection, and cross-site scripting**.

SQL injection attacks usually hijack control over the website owner's database through the act of data injection into the web application. The data injected gives the website owner's database instructions that have not been authorized by the site owner themselves.

This results in data leaking, removal, or manipulation of stored data. Code injection, on the other hand, involves the injecting of source codes into the web application while cross-site scripting injects code (javascript) into browsers.

These injection attacks primarily function to give your web application instructions that are not authorized as well.

To overcome it, business owners are advised to implement input validation techniques and robust coding. Business owners are also encouraged to make use of '**least privilege**' principles so that the user rights and authorization for actions are minimized.

- **Phishing Scam**

These types of threats are designed to look like emails that are from legitimate sources, with the goal of **acquiring sensitive information** like login credentials, bank account numbers, credit card numbers and other information.

If an individual is not aware of the differences and indications that the email messages are suspicious, it can be deadly since they may respond to it. Alternatively, they can also be used to send in malware that, upon clicking, may end up gaining access to the user's information.

To prevent such incidents from happening, ensure that all employees are aware and capable of identifying suspicious emails.

Preventative measures should be taken so that further actions can be undertaken.

For example, scanning links and information before downloading as well as contacting the individual to which the email is sent to verify its legitimacy.

- **Brute Force**

In Brute force attacks, hackers **attempt to guess passwords** and forcefully gain access to the web application owner's details.

There is no effective way to prevent this from happening. However, business owners can deter this form of attack by limiting the number of logins attempts as well as making use of an encryption.

References:

1. <https://www.knowledgehut.com/blog/security/hacking-web-server>
2. <https://geekflare.com/common-web-application-threats/>

SQL INJECTION

Unit Structure

10.1 Introduction

10.1.1 The Flow of the Web Application

10.1.2 How does a web- application work?

10.1.3 Benefits of a web application

10.1.4 Disadvantages of the Web Applications

10.1.5 Client and Server model

10.1.6 Advantages of Client-server networks

10.2 SQL Injection

10.2.1 How SQL injection attack works?

10.2.2 What is the impact of a successful SQL injection attack?

10.3 Types of SQL Injections

10.4 How to detect SQL injection vulnerabilities

10.5 How to Prevent SQL Injection

10.5.1 How to Prevent SQL Injections (SQLi) -Generic Tips

10.1 INTRODUCTION

A web-application is an application program that is usually stored on a remote server, and users can access it using **Software** known as **web-browser**. Web applications include online forms, shopping carts, video and photo editing, email programs such as Gmail, Yahoo and AOL. If we talk about the web application in general, a web application usually uses a combination of the server-side scripts such as **PHP**, **ASP** for handling the information storage and retrieval of the data. Some of them also use the client-side scripts such as **JavaScript**, **HTML** to present the information to the users, and few web applications are using both **server-side** and **client-side** at the same time.

10.1.1 The Flow of the Web Application

Let's understand how the flow of the typical web application looks like.

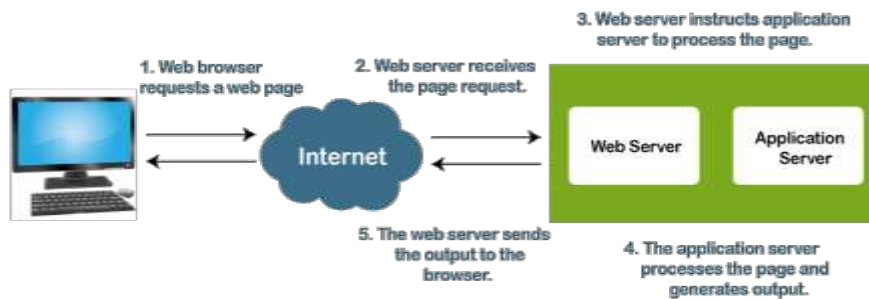


Figure 10.1 Flow of the web application

1. User sends a request to the web server using web browsers such as **Google Chrome, Microsoft Edge, Firefox**, etc over the **internet**.
2. Then, the request is forwarded to the appropriate web **application server** by the **web-server**.
3. Web application server performs the requested operations/ tasks like **processing the database, querying the databases; produces** the result of the requested data.
4. The obtained result is sent to the **webserver** by the **web application server** along with the requested data/information or processed data.
5. The web server responds to the user with the requested or processed data/information and provides the result to the user's browser.

10.1.2 How does a web- application work?

In general, web-application do not require downloading them because, as we have already discussed, the web application is a computer program that usually resides on the remote server. Any user can access it by using web browsers such as **Google Chrome, Safari, Microsoft Edge, etc.,** and most of them are available free for everyone. Web applications are generally coded using the languages supported by almost every web-browsers such as HTML, JavaScript because these are the languages that rely on the web browsers to render the program executable.

Some of the web applications are completely static due to which they do not require any processing on the server at all while, on the other hand, some web applications are dynamic and require server-side processing. The application server performs the task requested by the clients, which also need a database to store the information. Application server technologies range from **ASP.NET, ASP and ColdFusion** to **PHP and JSP**.

A standard web application can be easily developed with a small team of developers. As we all know, majority of the web applications available on internet are written using the programming languages such as the **HTML (or HyperText Markup Language), CSS (or Cascading Style Sheets) and Javascript**. These are used in creating **front-end interface (Client-side programming)**. Server-side programming is done by using

programming languages such as **Java**, **Python**, **PHP**, **Ruby** etc. **Python** and **Java** are the languages that are usually used for server-side programming.

10.1.3 Benefits of a web application

Lets see some of the significant benefits offered by a web application:

- Any typical web application can run on any operating system such as the Windows, Mac, Linux as long as the browser is compatible.
- A web application is usually not required to install in the hard drive of the computer system; thus, it eliminates all the issues related to the space limitation.
- All the users can access the same version of the web application, which eliminates all compatibility issues.
- It also reduces software piracy in subscription-based web applications, for example, **SAAS (or Software as a service)**.
- They also reduce the expense for end-users, business owners because the maintenance needed by the business is significantly less.
- Web applications are flexible. A user can work from any geographical location if she/he has a working internet connection.
- It just takes a moment to create a new user by providing a username, password and URL.
- On cloud, storage space is now virtually unlimited as long as you can afford it.
- A web application can be programmed to run on a wide variety of operating systems unlike native applications that can run on a specific platform.
- Any standard web application is developed with basic programming languages like HTML, CSS that are compatible and well known among the IT professionals.

10.1.4 Disadvantages of the Web Applications

- Internet connection is required to access any web application. It is very easy to get an internet connection in modern cities but still in rural areas internet connectivity is not so well.
- Many people believe that their data on the cloud is not secure and they like to stick with old methods and don't want to use new methods.
- Different users use different web browsers according to their needs and choices. So, while creating a web application, developer must remember that an application must support all web browsers, including new and old versions of browsers.

- Speed-related issues are also affecting the web application's performance because there are several factors on which the performance of a web application depends, and these all factors affect the performance of the web application in their own way.
- If a user's web application faces any kind of issues or if he does not have a good quality corporate website, his web application will not run correctly, smoothly.
- A user must have to spend enough money to maintain the good condition of his web application, provide an update whenever an issue occurs, and make an attractive user interface, which is not so cheap at all.
- A web application must be programmed in such a way that it will run regardless of the device's operating system.
- A web application may face issues while running on Windows, Android, or several other operating systems if it is not responsive.

10.1.5 Client-Server model

- A client - server networking model is a model in which computers such as servers provide the network services to the other computers called as clients. This model is known as client-server networking model.
- The application programs using the client-server model should follow the given below strategies:

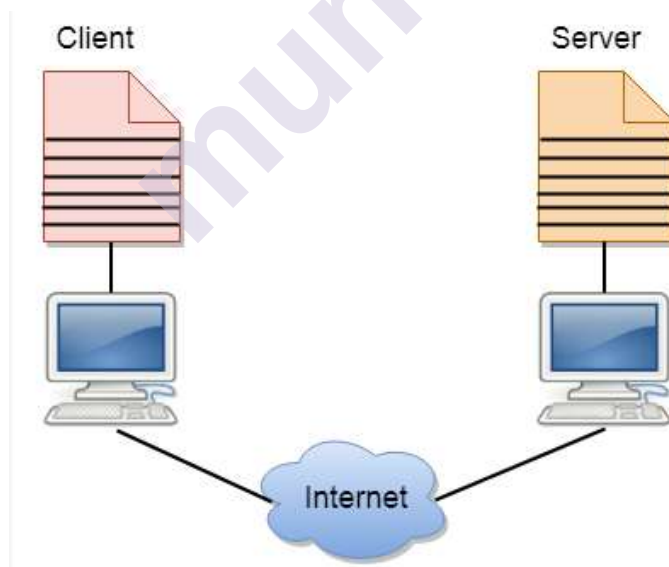


Figure 10.2 Client-Server Model

- An application program is known as a **client program**, running on the local machine that requests for a service from an application program known as a **server program**, running on the remote machine.

- A client program runs only when it requests for a service from the server while the server program runs all time as it does not know when its service is required.
- A server provides a service to many clients not just for a single client. Many clients can use the service of one server.

- **Client**

A client is a program that runs on the local machine requesting service from the server. In client program the service is started by the user and terminates when the service is completed.

- **Server**

A server is a program that runs on the remote machine providing services to the clients. When the client requests for a service, the server opens the door for the incoming requests, but it never initiates the service.

A server program is an infinite program means that when it starts, it runs infinitely unless the problem arises. The server waits for the incoming requests from the clients. When the request arrives at the server, then it responds to the request.

10.1.6 Advantages of Client-server networks

- **Centralized**

Centralized back-up is possible in client-server networks, i.e., all the data is stored in a server at a single place.

- **Security**

These networks are more secure as all the shared resources are centrally administered.

- **Performance**

The use of the dedicated server increases the speed of sharing resources. This increases the performance of the overall system.

- **Scalability**

We can increase the number of clients and servers separately, i.e., the new element can be added, or we can add a new node in a network at any time.

10.2 SQL INJECTION

In a SQL injection attack, an attacker submits an information to a website that has been deliberately formulated in such a way that it results in that website misinterpreting it and taking unintended actions. More specifically, the website interprets the data submitted by the attacker as a database

command, which it then executes. If the command is to modify entries in a database, or even to delete the entire database, then the results can understandably be catastrophic. For that reason, it is vital that organizations take steps to prevent SQL injection attacks.

SQL injection attacks pose a serious security threat to organizations. A successful SQL injection attack can result in confidential data being deleted, lost or stolen; websites being defaced; unauthorized access to systems or accounts and, ultimately, compromise of individual machines or entire networks.

10.2.1 How SQL injection attack works

Imagine someone has to appear in court and is asked to provide their name. Instead of giving their real name, “John Dey,” they give the name “Release John Dey.” When the case comes up, the judge calls out “Release John Dey,” so the bailiff releases him.

This illustrates the concept of a SQL injection attack. Instead of providing a real name, the accused deliberately formulates a name that is interpreted as a command, resulting in an unintended action – in this case, an unintended release.

SQL injection examples

Below is an example of how a SQL injection attack could be carried out in practice. The attack is designed to gain access to all data about a user from the database table USERS without knowing a username or matching password.

The SQL application code might be:

```
SELECT * FROM Users WHERE Username='$username' AND Password='$password'
```

Using a web interface, when prompted for their username and password, an attack might enter:

I' OR 'I' = 'I

and

I' OR 'I' = 'I

By entering this deliberately formulated username and password pair, the attacker has effectively injected two whole OR conditions into the authentication process.

Let's take a closer look to see how it works.

The SQL application code was expecting a simple text string such as **johndey** for the username, and another simple string such as **password123** for the password.

It would then parse the line:

```
SELECT * FROM Users WHERE Username='$username' AND
Password='$password'
```

as

```
SELECT * FROM Users WHERE Username='johndey' AND
Password='password123'
```

and access the data for a user johndey (if there is one) if the password for that user is password123.

But here's the problem. Application was not expecting that an attacker would enter a username and password formulated in this way, with a clever use of apostrophes.

The result is that the query is parsed as:

```
SELECT * FROM Users WHERE Username='1' OR '1' = '1' AND
Password='1' OR '1' = '1'
```

Now the application will access data for any user if their password is 1 or if 1=1. And since the condition 1=1 is always true, this SQL query will always result in the password authentication process being bypassed.

(Code sample sourced from OWASP)

In the SQL injection example above, the two OR conditions are injected when the application was expecting a username and password string, but an attack can well inject a database command such as **DROP DATABASE**, which results in the loss of all the information stored in a database.

For example, imagine a database application that enables an employee to enter their name into one field, and a number such as a social security number into the next field, and stores this information in a database called **employee**.

The application will likely have a form with some code behind it to accept a name in the form 'employee name'. A malicious employee (or outside attacker) might be able to carry out a SQL injection attack that causes the application to execute the SQL command **DROP DATABASE employee**, which results in the deletion and complete loss of the information stored in that database.

10.2.2 What is the impact of a successful SQL injection attack?

A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period.

SQL injections typically fall under three categories: In-band SQLi (Classic), Inferential SQLi (Blind) and Out-of-band SQLi.

- **In-band SQLi**

In this method, the attacker uses the same channel of communication to launch their attacks and to gather their results. In-band SQLi's simplicity and efficiency make it one of the most common types of SQLi attack. There are two sub-variations of this method:

- **Error-based SQLi**

The attacker performs actions that cause the database to produce error messages. The attacker can potentially use these error messages to gather information about the structure of the database.

- **Union-based SQLi**

This technique takes advantage of the **UNION SQL** operator, which fuses multiple select statements generated by the database to get a single HTTP response. This response may contain data that can be leveraged by the attacker.

- **Inferential (Blind) SQLi**

The attacker sends data payloads to the server and sees the response and behavior of the server to learn more about its structure. This method is called blind SQLi because the data is not transferred from the website database to the attacker, thus the attacker cannot see information about the attack in-band.

Blind SQL injections rely on the response and behavioral patterns of the server so they are typically slower to execute but may be just as harmful. Blind SQL injections can be classified as follows:

- **Boolean**

In this technique, the attacker sends a SQL query to the database prompting the application to return a result. The result may vary depending on whether the query is true or false. Based on the result, the information within the HTTP response will modify or stay unchanged. The attacker can then work out if the message generated a true or false result.

- **Time-based**

In this technique, an attacker sends a SQL query to the database, which makes the database wait (for a period in seconds) before it can react. The attacker can see from the time the database takes to respond, whether a query is true or false. Based on the result, an HTTP response will be generated instantly or after a waiting period. The

attacker can thus work out if the message they used returned true or false, without relying on data from the database.

- **Out-of-band SQLi**

The attacker can only carry out this form of attack when certain features are enabled on the database server used by the web application. This form of attack is primarily used as an alternative to the in-band and inferential SQLi techniques.

Out-of-band SQLi is performed when the attacker can't use the same channel to launch the attack and gather information, or when a server is too slow or unstable for these actions to be performed. These techniques count on the capacity of the server to create DNS or HTTP requests to transfer data to an attacker.

10.4 HOW TO DETECT SQL INJECTION VULNERABILITIES

- Routine application database audits should be used to determine if your application has been compromised.
- Querying the database for common HTML tags used by worms can reveal signs that the application is spreading malware. These tags include "iframe", "http-equiv="refresh"" or the IP address of known malicious servers.
- An easier way to detect a compromise is by examining webpages created from dynamic content for unexpected behavior, including the addition of hidden iframes -- code elements used to embed an HTTP document in another HTTP document -- in the HTML. These routine audits help detect a compromised system, but this method only allows for fixes to be created after the fact.

Recovering an application from an exploited state, especially when data may have been altered, can be an extremely costly process and does not prevent future attacks.

10.5 HOW TO PREVENT SQL INJECTION

- The only way to prevent SQL Injection attacks is input validation and parametrized queries including prepared statements. The application code should never use the input directly.
- The developer must sanitize all input, not only web form inputs such as login forms. They must remove potential malicious code elements such as single quotes. It is also a good idea to turn off the visibility of database errors on your production sites. Database errors can be used with SQL Injection to gain information about your database.

Preventing SQL Injection vulnerabilities is not easy. Specific prevention techniques depend on the subtype of SQLi vulnerability, on the SQL database engine, and on the programming language. However, there are certain general tips that you should follow to keep your web application safe.

Step 1: Train and maintain awareness

To keep your web application safe, everyone involved in building the web application must be aware of the risks associated with SQL Injections. You should provide suitable security training to all your developers, QA staff, DevOps, and SysAdmins.

Step 2: Don't trust any user input

Treat all user input as untrusted. Any user input that is used in an SQL query introduces a risk of an SQL Injection. Treat input from authenticated and/or internal users the same way that you treat public input.

Step 3: Use whitelists, not blacklists

Don't filter user input based on blacklists. A clever attacker will almost always find a way to circumvent your blacklist. If possible, verify and filter user input using strict whitelists only.

Step 4: Adopt the latest technologies

Older web development technologies don't have SQLi protection. Use the latest version of the development environment, language and the latest technologies associated with that environment/language. For example, in PHP use PDO instead of MySQLi.

Step 5: Employ verified mechanisms

Don't try to build SQLi protection from scratch. Most modern development technologies can offer you mechanisms to protect against SQLi. Use such mechanisms instead of trying to reinvent the wheel. For example, use parameterized queries or stored procedures.

Step 6: Scan regularly

SQL Injections may be introduced by your developers or through external libraries/modules/software. You should regularly scan your web applications using a web vulnerability scanner tool.

References

- i) <https://www.javatpoint.com/web-application>
- ii) <https://www.acunetix.com/websitesecurity/sql-injection/>

WIRELESS NETWORK HACKING

Unit Structure

11.0 Objectives

11.1 Introduction to Wireless Network

11.1.1 Overview of WEP, WPA Authentication Mechanisms, and Cracking Techniques

11.1.2 Wireless Network Architectures

11.1.3 Overview of Locating SSIDs and MAC Spoofing

11.1.4 Understand Rogue Access Points

11.2 Wireless encryption techniques

11.2.1 Wireless encryption algorithm

11.2.2 Differentiation between WEP, WPA and WPA2

11.3 Breaking WEP/WPA and defending WPA encryption

11.4 Wireless Sniffing

11.5 Wireless Hacking Techniques

11.6 Wireless Threats: Authentication Attacks

11.7 Methods Used to Secure Wireless Networks

11.8 Summary

11.9 Unit End Exercise

11.10 References

11.11 Bibliography

11.0 OBJECTIVES

After this chapter, student will be able to:

- Define Wireless Network.
- Describe the Overview of WEP, WPA Authentication Mechanisms, and Cracking Techniques.
- State various Wireless Network Architectures
- Understand how to Locate SSIDs and MAC Spoofing

- Understand Rogue Access Points:
- Define and understand various Wireless encryption techniques and Wireless algorithm.
- State and make distinction between WEP, WPA and WPA2
- Understanding and breaking WEP/WPA and also defending WPA encryption
- State the Overview of Wireless Sniffers
- Understand Wireless Hacking Techniques
- Explain Various Wireless Threats: Authentication Attacks
- Describe the Methods Used to Secure Wireless Networks

11.1 INTRODUCTION TO WIRELESS NETWORK:

- A wireless network is a set of two or more devices connected with each other via radio waves within a limited space range.
- Wireless networks add another entry point into a network for hackers. Much has been written about wireless security and hacking because wireless is a relatively new technology and ripe with security holes.
- Because of the broadcast nature of Radio Frequency (RF) wireless networks and the rapid adoption of wireless technologies for home and business networks, many vulnerabilities and exploits exist.
- Most wireless LANs (WLANs) are based on the IEEE 802.11 standards and amendments, such as 802.11a, 802.11b, 802.11g, and 802.11n. The 802.11 standard included only rudimentary security features and was fraught with vulnerabilities.
- The 802.11i amendment is the latest security solution that addresses the 802.11 weaknesses.
- The Wi-Fi Alliance created additional security certifications known as Wi-Fi Protected Access (WPA) and WPA2 to fill the gap between the original 802.11 standard and the latest 802.11i amendment.
- The devices in a wireless network have the freedom to be in motion, but be in connection with the network and share data with other devices in the network.
- One of the most crucial point that they are so spread is that their installation cost is very cheap and fast than the wire networks.



Fig. 11.1: Wireless Router

- In a wireless network, we have **Access Points** which are extensions of wireless ranges that behave as logical switches.



Fig. 11.2: Access Points

- Although wireless networks offer great flexibility, they have their security problems. A hacker can sniff the network packets without having to be in the same building where the network is located. As wireless networks communicate through radio waves, a hacker can easily sniff the network from a nearby location.
- Most attackers use network sniffing to find the SSID and hack a wireless network. When our wireless cards are converted in sniffing modes, they are called monitor mode.
- **Kismet:-** Kismet is a powerful tool for wireless sniffing that is found in Kali distribution. It can also be downloaded from its official webpage – <https://www.kismetwireless.net>.

- **NetStumbler:-** NetStumbler is another tool for wireless hacking that is primarily meant for Windows systems. It can be downloaded from <http://www.stumbler.net/>
- **Wired Equivalent Privacy:-** Wired Equivalent Privacy (WEP) is a security protocol that was invented to secure wireless networks and keep them private. It utilizes encryption at the data link layer which forbids unauthorized access to the network. The key is used to encrypt the packets before transmission begins. An integrity check mechanism checks that the packets are not altered after transmission. Note that WEP is not entirely immune to security problems. It suffers from the following issues: CRC32 is not sufficient to ensure complete cryptographic integrity of a packet, it is vulnerable to dictionary attacks and WEP is vulnerable to Denial of Services attacks too.
- **WEPCrack: -** WEPCrack is a popular tool to crack WEP passwords. It can be downloaded from – <https://sourceforge.net/projects/wepcrack/>
- **Aircrack-ng:-** Aircrack-ng is another popular tool for cracking WEP passwords. It can be found in the Kali distribution of Linux.
- **Wireless DoS Attacks:-** In a wireless environment, an attacker can attack a network from a distance and therefore, it is sometimes difficult to collect evidences against the attacker. The first type of DoS is **Physical Attack**. This type of attack is very basic and it is in the base of radio interferences which can be created even from cordless phones that operate in 2.4 GHz range. Another type is **Network DoS Attack**. As the Wireless Access Point creates a shared medium, it offers the possibility to flood the traffic of this medium toward the AP which will make its processing more slowly toward the clients that attempt to connect. Such attacks can be created just by a ping flood DoS attack.

11.1.1 Overview of WEP, WPA Authentication Mechanisms, and Cracking Techniques:-

- Two methods exist for authenticating wireless LAN clients to an access point: open system or shared key authentication. Open system does not provide any security mechanisms but is simply a request to make a connection to the network. Shared key authentication has the wireless client hash a string of challenge text with the WEP key to authenticate to the network.
- Wired Equivalent Privacy (WEP) was the first security option for 802.11 WLANs. WEP is used to encrypt data on the WLAN and can optionally be paired with shared key authentication to authenticate WLAN clients. WEP uses an RC4 64-bit or 128-bit encryption key to encrypt the layer 2 data payload. This WEP key comprises a 40-bit or 104-bit user-defined key combined with a 24-bit Initialization Vector (IV), making the WEP key either 64- or 128-bit.

- The process by which RC4 uses IVs is the real weakness of WEP: It allows a hacker to crack the WEP key. The method, known as the FMS attack, uses encrypted output bytes to determine the most probable key bytes. It was incorporated into products like AirSnort, WEPCrack, and aircrack to exploit the WEP vulnerability. Although a hacker can attempt to crack WEP by brute force, the most common technique is the FMS attack.
- WPA employs the Temporal Key Integrity Protocol (TKIP) which is a safer RC4 implementation—for data encryption and either WPA Personal or WPA Enterprise for authentication. WPA Personal uses an ASCII passphrase for authentication while WPA Enterprise uses a RADIUS server to authenticate users. WPA Enterprise is a more secure robust security option but relies on the creation and more complex setup of a RADIUS server. TKIP rotates the data encryption key to prevent the vulnerabilities of WEP and, consequently, cracking attacks.
- WPA2 is similar to 802.11i and uses the Advanced Encryption Standard (AES) to encrypt the data payload. AES is considered an uncrackable encryption algorithm. WPA2 also allows for the use of TKIP during a transitional period called mixed mode security. This transitional mode means both TKIP and AES can be used to encrypt data. AES requires a faster processor, which means low-end devices like PDAs may only support TKIP.
- WPA Personal and WPA2 Personal use a passphrase for authentication WLAN clients. WPA Enterprise and WPA2 Enterprise authenticate WLAN users via a RADIUS server using the 802.1X/Extensible Authentication Protocol (EAP) standards.
- 802.11i and WPA2 use the same encryption and authentication mechanisms as WPA2. However, WPA2 doesn't require vendors to implement preauthorization. Preauthorization enables fast, secure roaming, which is necessary in very mobile environments with time-sensitive applications such as wireless voice over IP.

	Encryption	Authentication	Weakness
Original IEEE 802.11 standard	WEP	<u>WEP</u>	IV weakness allows the WEP key to be cracked. The same key is used for encryption and authentication of all clients to the WLAN.
WPA	TKIP	Passphrase or RADIUS (802.1x/EAP)	Passphrase is <u>suscep- tible</u> to a dictionary attack.
WPA2	AES (can use TKIP while in mixed mode)	Passphrase or RADIUS (802.1x/EAP)	Passphrase is <u>suscep- tible</u> to a dictionary attack.
IEEE 802.11i	AES (can use TKIP <u>while</u> in mixed mode)	Passphrase or RADIUS (802.1x/EAP)	Passphrase is <u>suscep- tible</u> to a dictionary attack.

Table 11.1 summarizes the authentication and encryption options for WLANs.

- In planning the wireless network, we will have to determine which wireless network architecture to adopt in the network environment. There are two architectures available, namely standalone and centrally coordinated wireless network.
- **Standalone architecture (Ad hoc mode)**

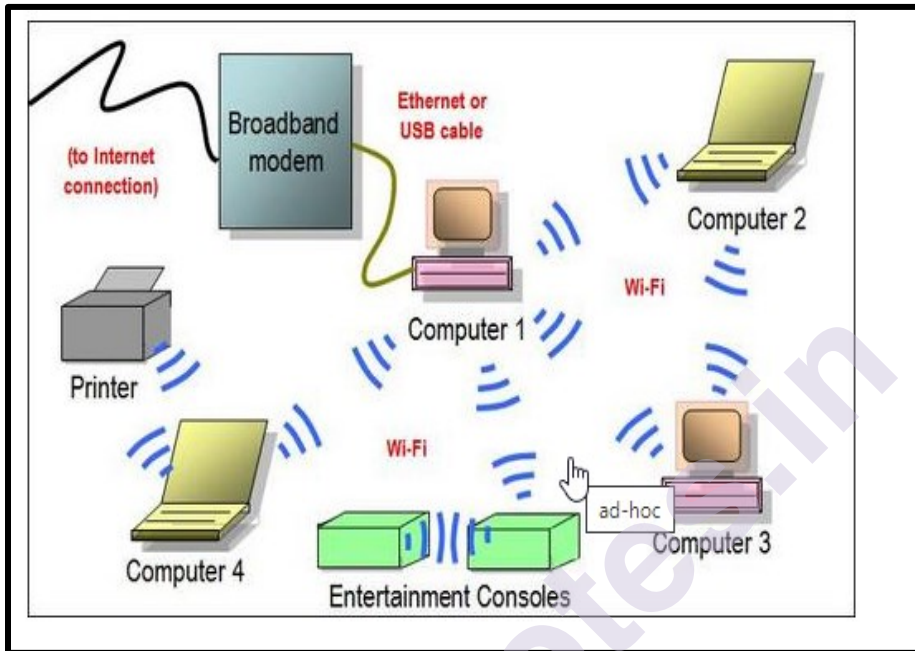


Fig. 11.3: Standalone architecture (Ad hoc mode)

- By using ad hoc mode, all devices in the wireless network are directly communicating with each other in peer to peer communication mode. No access point (routers/switches) is required for communication between devices.
- For setting up ad hoc mode, we need to manually configure the wireless adaptors of all devices to be at ad hoc mode instead of infrastructure mode, and all adaptors must use the same channel name and same SSID for making the connection active.
- Ad hoc mode is most suitable for small group of devices and all of these devices must be physically present in close proximity with each other.
- The performance of network suffers while the number of devices grows. Disconnections of random device may occur frequently and also, ad hoc mode can be a tough job for network administrator to manage the network.
- Ad hoc mode has another limitation is that, ad hoc mode networks cannot bridge to wired local area network and also cannot access internet if without the installation of special gateways.

- An ad hoc mode uses the integrated functionality of each adaptor to enable wireless services and security authentication. The characteristics of an Ad hoc wireless network are listed as below:
 - All access points in the network operate independently and has own configuration file.
 - Access point is responsible for the encryption and decryption.
 - The network configuration is static and does not respond to changing network conditions.
- **Centrally Coordinated Architecture (Infrastructure mode):-**

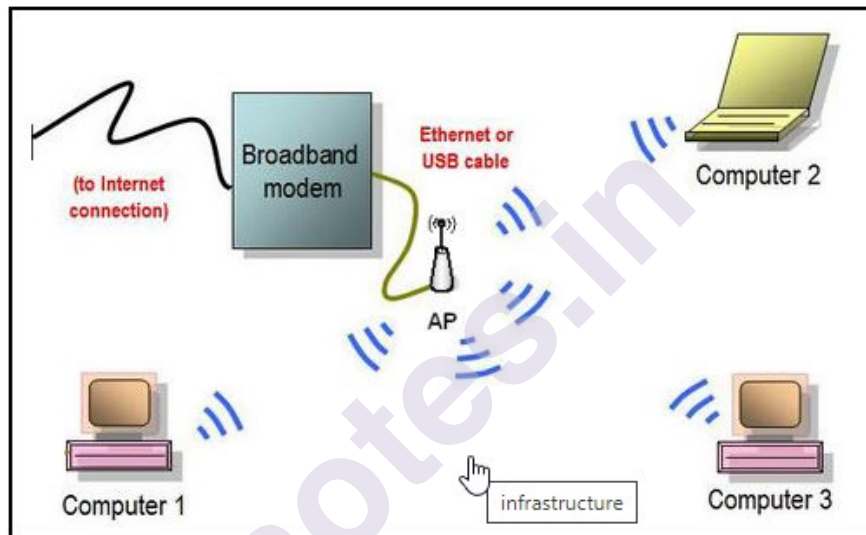


Fig. 11.4: Centrally Coordinated Architecture (Infrastructure mode):-

- The other architecture in wireless network is centrally coordinated (infrastructure mode). All devices are connected to wireless network with the help of Access Point (AP). Wireless APs are usually routers or switches which are connected to internet by broadband modem.
- Infrastructure mode deployments are more suitable for larger organizations or facility. This kind of deployment helps to simplify network management, and allows the facility to address operational concerns. And resiliency is also assured while more users can get connected to the network subsequently.
- The infrastructure mode provides improved security, ease of management, and much more scalability and stability. However, the infrastructure mode incurs extra cost in deploying access points such as routers or switches.
- An infrastructure mode wireless network has the characteristics as below:

- The wireless centralized controller coordinates the activity of access point.
- The controller is able to monitor and control the wireless network by automatically reconfiguring the access point parameters in order to maintain the health of the network.
- The wireless network can be easily expanded or reduced by adding or removing access points and the network can be reconfigured by the controller based on the changes in RF footprint.
- Tasks such as user authentication, fault tolerance, control of configuration, policy enforcement and expansion of network are done by the wireless network controller.
- Redundant access points can be deployed in separate locations to maintain control in the event of an access point or switch failure.

11.1.3 Overview of Locating SSIDs and MAC Spoofing:

- The **SSID** is the name of the WLAN and can be located in a beacon. If two wireless networks are physically close, the SSIDs are used to identify and differentiate the respective networks. The SSID is usually sent in the clear in a beacon packet. Most APs allow the WLAN administrator to hide the SSID. However, this isn't a robust security mechanism because some tools can read the SSID from other packets such as probe and data packets.
- An early security solution in WLAN technology used MAC address filters: A network administrator entered a list of valid MAC addresses for the systems allowed to associate with the AP. MAC filters are cumbersome to configure and aren't scalable for an enterprise network because they must be configured on each AP. **MAC spoofing** is easy to perform and negates the effort required to implement MAC filters. A hacker can identify a valid MAC address because the MAC headers are never encrypted.

11.1.4 Understand Rogue Access Points:

- Rogue access points are WLAN access points that aren't authorized to connect to a target network.
- Rogue APs open a wireless hole into the network. A hacker can plant a rogue AP, or an employee may unknowingly create a security hole by plugging an access point into the network so the user can be mobile.
- Any rogue AP can be used by anyone who can connect to the AP, including a hacker, giving them access to the wired LAN.

- This is why it's critical for organizations that have a no wireless policy to perform wireless scanning to ensure no rogue APs are connected to the network.

11.2 WIRELESS ENCRYPTION TECHNIQUES:-

- **WEP: Wired Equivalent Privacy:** - It is the simple encryption technique which used the 40-bit key with the 24-bit initialization vector and utilized the RC4 algorithm for encryption. It also used CRC-32 for integrity check mechanism; because the initialization vector was very small, there was a possibility that the IV's getting reused. This weakness caused the algorithm to be broken easily.
- **WPA: Wi-Fi Protected Access:** - This algorithm uses 48 bit IV and is based on the 802.11i standard. The RC4 algorithm used temporal keys of 128-bit size and 64 bit MIC check which made the encryption stronger than WEP. Here 128-bit temporal keys, mixed with 48 bit IV and MAC address of the sender create the key stream to encrypt the data using RC4. Temporal keys are changed every 10,000 packets.
- **WPA2: Wi-Fi Protected Access with EAP:-** This is for enterprise use with strong data protection and network access control. Here, instead of RC4, AES (Advanced encryption standard) is used for encryption with temporal keys. The key size is 128-bit keys. It makes use of centralized RADIUS server for authentication.

11.2.1 Wireless encryption algorithm:-

The attacks on wireless networks are increasing day by day with the increasing use of wireless networks. Therefore, from this emerging technology have come various types of wireless encryption algorithms to make the wireless network more secure. Each wireless encryption algorithm has advantages and disadvantages. The following are the various wireless encryption algorithms developed so far:

- **WEP:** A WLAN clients authenticating and data encryption protocol and it is an old, original wireless security standard that can be cracked easily.
- **WPA:** It is an advanced WLAN clients authenticating and data encryption protocol using TKIP, MIC, and AES encryption. It uses a 48-bit IV, 32-bit CRC, and TKIP encryption for wireless security.
- **WPA2:** WPA2 uses AES (128-bit) and CCMP for wireless data encryption.
- **WPA2 Enterprise:** It integrates EAP standards with WPA encryption.
- **TKIP:** A security protocol used in WPA as a replacement for WEP.

- **AES:** It is a symmetric-key encryption, used in WPA2 as a replacement of TKIP.
- **9 EAP:** Uses multiple authentication methods, such as token cards, Kerberos, certificates, etc.
- **LEAP:** A proprietary WLAN authentication protocol developed by Cisco.
- **RADIUS:** A centralized authentication and authorization management system.
- **802.11i :** An IEEE standard that specifies security mechanisms for 802.11 wireless networks.
- **CCMP:** CCMP utilizes 128-bit keys, with a 48-bit initialization vector (IV) for replay detection.

11.2.2 Differentiation between WEP, WPA and WPA2

Encryption	Attributes			
	Encryption Algorithm	IV Size	Encryption Key Length	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bit	CRC-32
WPA	RC4, TKIP	48-bit	128-bit	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bit	128-bit	CBC-MAC

WEP		Should be replaced with more secure WPA and WPA2
WPA, WPA2		Incorporates protection against forgery and replay attacks

Fig. 11.5: Differentiation between WEP, WPA and WPA2

11.3 BREAKING WEP/WPA AND DEFENDING WPA ENCRYPTION

- **How to Break WEP Encryption?**
 - There are many possible tools that one can use to crack WEP, but all of the approaches follow the same idea and order of steps.
 - Assuming that we have found our target network, we do as follows –

- Collect (sniff) WEP encrypted packets flying over the air. This step may be performed using a Linux tool called "airodump-ng".
 - When enough packets are collected (we have collected a set of frames with duplicate IV vector), you try to crack the network using a tool called "aircrack-ng".
 - On a highly congested network, the above mentioned two steps can take around 5-10 minutes or even less. It is that easy! The detailed step by step guide for hacking WEP will be shown under the topic of "Pen Testing WEP Encrypted WLAN".
- **How to Break WPA Encryption?**
- The way to break a WPA encryption has a slightly different approach. Wireless frames using WPA, are using TKIP encryption that still uses the concept of IV and RC4 algorithm, however it is modified in order to be more secure. TKIP modifies WEP with the following pointers –
 - It uses temporal, dynamically created keys instead of static ones used by WEP.
 - It uses sequencing to defend against replay and injection attacks.
 - It uses an advanced key mixing algorithm in order to defeat IV collisions and weak-key attacks in WEP.
 - It introduces Enhanced Data Integrity (EDI) to defeat bit-flipping attack possible in WEP.
 - Taking all of these points into account, it makes WPA standard computationally not-possible to crack (it does not say it is not possible, but it may take reasonably a very long time, assuming you have advanced resources for breaking the algorithm). Authentication used in WPA standard has also advanced in respect to one used in WEP. WPA uses 802.1x (EAP-based authentication) for authentication of the clients. In fact, this is the only weak point, where you may try your chances for breaking the WPA (and WPA2 in fact).
 - WPA and WPA2 standards supports two types of authentications - Pre-Shared Key (PSK) and true 802.1x based on external authentication server. When using 802.1x authentication - it is simply not possible to break the password; it is only doable where local PSK mode is used. Just as a side-note - all the enterprise wireless deployments, they use true 802.1x authentication, based on the external RADIUS server, therefore, your only possible target might be very small businesses or home networks.

- One more remark is that, PSK used for protecting WPA/WPA2 must be reasonably short in size (max 10 characters - in opposite to 64 characters allowed as max length), if you have the intention to break it. The reason for that requirement is that, PSK is only transmitted once (not in clear text) between wireless client and the AP during the initial 4-way handshake, and the only way to derive the original key from those packets is by brute-forcing or using a good dictionary.
- There is a pretty nice online calculator that can estimate the time it would take to brute-force the PSK - <http://lastbit.com/pswcalc.asp>. Assuming that you have 1 PC that can try 1000 password per second (composed of lower-case, upper-case, digits and common punctuations) it would take 28910 years to break the password (as maximum of course, if we are lucky it might take a few hours).

The screenshot shows a web-based calculator for estimating the time to brute-force a PSK. The inputs are: Password length: 8, Speed: 1000 passwords per second, and Number of computers: 1. The character set options are: chars in lower case (checked), chars in upper case (checked), digits (checked), common punctuation (checked), and full ASCII (unchecked). A 'Calculate!' button is present. The result at the bottom states: 'Brute Force Attack will take up to 28910 years'.

Fig. 11.6: Screenshot (example) Break of WPA Encryption

- The general process of breaking a WPA/WPA2 encryption (only when they use PSK) is as follows –
 - Collect (sniff) wireless packets flying over the air. This step may be performed using the Linux tool called "airodump-ng".
 - While packets are being collected, you should de-authenticate the current clients. By doing that, you are getting to the situation, when the client would need to authenticate again in order to use a Wi-Fi network. This is exactly what you wanted! By doing this, you prepare a good environment to sniff a wireless user authenticating to the network. You can use Linux based tool "aireplay-ng" to de-authenticate the current wireless clients.

- As we have a 4-way handshake sniffed (and saved in the dump file), you can once again use "aircrack-ng" to crack the PSK. In this step, you have to reference a dictionary file containing all the combinations of the password, that aircrack-ng tool will use. That is why, a good dictionary file is a most important element here.
- **How to Defend Against WPA Cracking?**

If WPA cracking not possible (or rather say: impossible within a reasonable period of time). **Following are some pointers of the best practices for securing your home/small business wireless network –**

- If there is a chance for that, use WPA2 instead of WPA. It has a direct impact on the encryption scheme used by a suite. AES (used by WPA2) is much safer than TKIP (used by WPA).
- As we saw earlier, the only way to break WPA/WPA2 is by sniffing the authentication 4-way handshake and brute-force the PSK. To make it computationally impossible, use a password of at least 10 characters composed of random combination (not any plain word that you can meet in any dictionary) of lower case, upper case, special characters and digits.
- **Disable Wi-Fi Protected Setup (WPS)** - WPS is one of the "cool features" invented to make connecting new wireless clients to the network much easier - just by putting a special 8-digit PIN number of the AP. This 8-digit is a very short work for a brute-force attack, and also this 8-digit may be found on the back of the AP box itself. Give yourself a try and have a look at our home router - do we see WPS PIN on the back? Do we have WPS feature enabled on our home router?



Fig. 11.7: Screenshot (example) Defend against WPA Cracking

11.4 WIRELESS SNIFFING:

- Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of

“tapping phone wires” and get to know about the conversation. It is also called wiretapping applied to the computer networks.

- There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network. Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.
- In other words, Sniffing allows us to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

- **What can be sniffed?**

One can sniff the following sensitive information from a network –

- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic
- **How it works:-**
 - A sniffer normally turns the NIC of the system to the promiscuous mode so that it listens to all the data transmitted on its segment.
 - Promiscuous mode refers to the unique way of Ethernet hardware, in particular, network interface cards (NICs), that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.

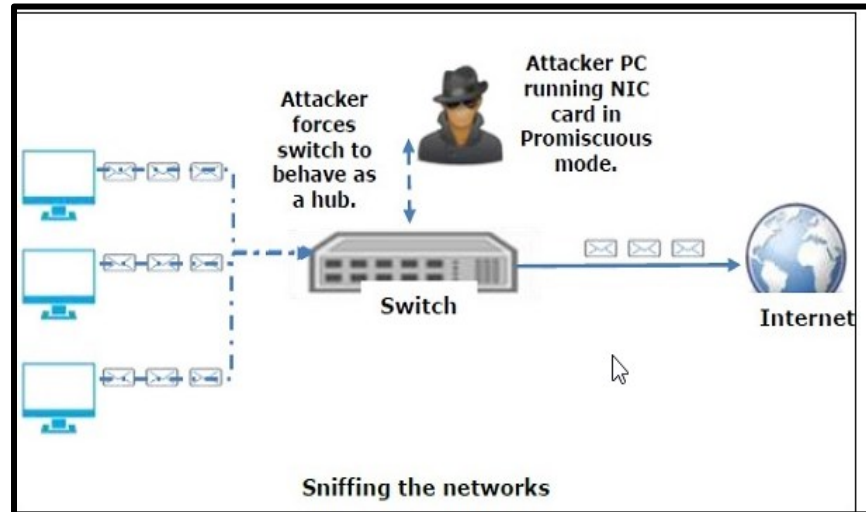


Fig. 11.8: Sniffing the network

A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

Types of Sniffing

Sniffing can be either Active or passive in nature.

- **Passive Sniffing:** - In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

The good news is that hubs are almost obsolete nowadays. Most modern networks use switches. Hence, passive sniffing is no more effective.

- **Active Sniffing:-**In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting address resolution packets (ARP) into a target network to flood on the switch content addressable memory (CAM) table. CAM keeps track of which host is connected to which port.

Following are the Active Sniffing Techniques –

- MAC Flooding
- DHCP Attacks
- DNS Poisoning
- Spoofing Attacks
- ARP Poisoning

- **Protocols which are affected:-**

Protocols such as the tried and true TCP/IP were never designed with security in mind and therefore do not offer much resistance to potential intruders. Several rules lend themselves to easy sniffing –

- **HTTP** – It is used to send information in the clear text without any encryption and thus a real target.
- **SMTP (Simple Mail Transfer Protocol)** – SMTP is basically utilized in the transfer of emails. This protocol is efficient, but it does not include any protection against sniffing.
- **NNTP (Network News Transfer Protocol)**– It is used for all types of communications, but its main drawback is that data and even passwords are sent over the network as clear text.
- **POP (Post Office Protocol)** – POP is strictly used to receive emails from the servers. This protocol does not include protection against sniffing because it can be trapped.
- **FTP (File Transfer Protocol)** – FTP is used to send and receive files, but it does not offer any security features. All the data is sent as clear text that can be easily sniffed.
- **IMAP (Internet Message Access Protocol)** – IMAP is same as SMTP in its functions, but it is highly vulnerable to sniffing.
- **Telnet** – Telnet sends everything (usernames, passwords, keystrokes) over the network as clear text and hence, it can be easily sniffed.

Sniffers are not the dumb utilities that allow you to view only live traffic. If we really want to analyze each packet, save the capture and review it whenever time allows.

11.5 WIRELESS HACKING TECHNIQUES

Most wireless hacking attacks can be categorized as follows:

- **Cracking encryption and authentication mechanisms:-**These mechanisms include cracking WEP, WPA preshared key authentication passphrase, and Cisco's Lightweight EAP authentication (LEAP). Hackers can use them to connect to the WLAN using stolen credentials or can capture other users' data and decrypt/encrypt it.
- **Eavesdropping or sniffing:-** This involves capturing passwords or other confidential information from an unencrypted WLAN or hotspot.
- **Denial of Service:-** DoS can be performed at the physical layer by creating a louder RF signature than the AP with an RF transmitter, causing an approved AP to fail so users connect to a rogue AP. DoS can be performed at the Logical Link Control (LLC) layer by generating deauthentication frames (deauth attacks) or by continuously generating bogus frames (Queensland attack).

- **AP masquerading or spoofing Rogue:** - APs pretend to be legitimate APs by using the same configuration SSID settings or network name.
- **MAC spoofing:-** The hacker pretends to be a legitimate WLAN client and bypasses MAC filters by spoofing another user's MAC address.

Wireless networks give a hacker an easy way into the network if the AP isn't secured properly. There are many ways to hack or exploit the vulnerabilities of a WLAN.

11.6 Wireless Threats: Authentication Attacks


 Wireless Threats: Authentication Attacks The objective of authentication attacks is to steal the identity of Wi-Fi clients, their personal information, login credentials, etc. to gain unauthorized access to network resources.		
Type of Attack	Description	Method and Tools
Application Login Theft	Capturing user credentials (e.g., email address and password) from cleartext application protocols.	Ace Password Sniffer, Dsniff, PHoss, WinSniffer
PSK Cracking	Recovering a WPA PSK from captured key handshake frames using a dictionary attack tool.	coWPAtty, KisMAC, wpa_crack, wpa-psk-bf
Shared Key Guessing	Attempting 802.11 Shared Key Authentication with guessed vendor default or cracked WEP keys.	WEP cracking tools
Domain Login Cracking	Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes, using a brute-force or dictionary attack tool.	John the Ripper, L0phtCrack, Cain

Fig. 11.9: Wireless Threats: Authentication Attacks

11.7 METHODS USED TO SECURE WIRELESS NETWORKS

Because wireless networking is a relatively new technology compared to wired networking technologies, fewer security options are available. Security methods can be categorized by the applicable layer of the OSI model.

Layer 2 or MAC layer security options are as follows:

- WPA
- WPA2
- 802.11i

Layer 3 or Network layer security options are as follows:

- IPSec or SSL VPN

Layer 7 or Application layer security options are as follows:

- Secure applications such as Secure Shell (SSH), HTTP Over SSL (HTTPS), and FTP/SSL (FTPS)

11.8 SUMMARY

- A wireless network is a set of two or more devices connected with each other via radio waves within a limited space range.
- Understand the inherent security vulnerabilities of using a WLAN. RF is a broadcast medium, and therefore all traffic is able to be captured by a hacker.
- Understand the security solutions implemented in the IEEE 802.11 standard. WEP, shared key, and MAC filters are security solutions offered in the original IEEE 802.11 standard.
- Understand the security solutions offered by the Wi-Fi Alliance. WPA and WPA2 are Wi-Fi Alliance equipment security certifications.
- Know what an SSID is used for on a WLAN. The SSID identifies the network name and shouldn't be used as a security mechanism.
- There are two architectures available with wireless network, namely **standalone and centrally coordinated wireless network**.
- **Know different Wireless encryption techniques:** **WEP:** Wired Equivalent Privacy, **WPA:** Wi-Fi Protected Access and **WPA2:** Wi-Fi Protected Access with EAP.
- **Know different Wireless encryption algorithm:-**WEP, WPA, WPA2, WPA2 Enterprise, TKIP, AES, LEAP, RADIUS, 802.11i and CCMP.
- Listing and understanding differentiation between WEP, WPA and WPA2.
- Understanding the Steps for Breaking WEP/WPA and also defending against WPA Cracking.
- Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. Types of Sniffing are active and passive sniffing.
- **Wireless Threats: Authentication Attacks:** - Application Login theft, PSK Cracking, Shared Key guessing, Domain Login Cracking.
- **Knowing Wireless Hacking Techniques:** Cracking encryption and authentication mechanisms, Eavesdropping or sniffing, Denial of Service, AP masquerading or spoofing Rogue and MAC spoofing.
- **Methods Used to Secure Wireless Networks:** Security methods can be categorized by the applicable layer of the OSI model. **Layer 2 or**

MAC layer security options are as follows: WPA, WPA2, 802.11i and for **Layer 3 or Network** layer security options are as follows: IPSec or SSL VPN and for **Layer 7 or Application** layer security options are as follows: Secure applications such as Secure Shell (SSH), HTTP Over SSL (HTTPS), and FTP/SSL (FTPS).

- Know what security mechanisms should not be used for WLAN security. WEP and MAC filters shouldn't be used as the sole means to secure the WLAN.

11.9 UNIT END EXERCISE

1. Define and explain Wireless Network Architectures.
2. Explain in brief about WEP, WPA Authentication Mechanisms, and Cracking Techniques.
3. How to Locate SSIDs and MAC Spoofing? Explain.
4. Write a short note on Rogue Access Points.
5. Write a short note on Wireless encryption techniques.
6. Write a short note on Wireless encryption algorithm.
7. Differentiate between WEP, WPA and WPA2.
8. Explain in detail the Breaking of WEP/WPA
9. How to defend WPA encryption? Explain.
10. Write a short note on Wireless Sniffing.
11. Describe in brief Wireless Hacking Techniques.
12. Explain Wireless Threats: Authentication Attacks.
13. What are the different Methods Used to Secure Wireless Network? Explain.

11.10 REFERENCES

- Matt Walker, All-In-One-CEH-Certified-Ethical-Hacker-Exam-Guide.
- Tutorials Point Professionals, Ethical Hacking by TutorialsPoint.

11.11 BIBLIOGRAPHY

- Kimberly Graves (26th-April-2010), "CEH Certified Ethical Hacker Study Guide" 1st Edition, ISBN-13: 978-0470525203, ISBN-10: 0470525207, Sybex- Wiley Publishing.
- Sean-Philip Oriyano, Sybex, Certified Ethical Hacker Study Guide v9, Study Guide Edition, 2016.

CLOUD COMPUTING SECURITY

Unit Structure

- 12.0 Objectives
- 12.1 What is Cloud Computing Security?
 - 12.1.1 History of Cloud Computing
 - 12.1.2 Characteristics Cloud Computing security
 - 12.1.3 Cloud Computing Architecture
- 12.2 Types of Cloud Computing
- 12.3 Service Models of Cloud
- 12.4 Benefits/Advantages of Cloud Computing
- 12.5 Disadvantages of Cloud Computing Services
- 12.6 Threats and attacks to cloud computing
- 12.7 Summary
- 12.8 Unit End Exercise
- 12.9 References
- 12.10 Bibliography

12.0 OBJECTIVES

After this chapter, student will be able to:

- Define Cloud Computing Security
- Know and understand History of Cloud Computing
- State various Characteristics Cloud Computing security
- Understand different types of Cloud Computing services
- Identify and explain various Service Models of Cloud Computing
- List and describe various benefits of Cloud Computing
- List and describe various disadvantages of Cloud Computing
- State and understand various Threats and attacks related with cloud computing

12.1 WHAT IS CLOUD COMPUTING SECURITY?

- Cloud security, is also known as cloud computing security, is a collection of security measures designed to protect cloud-based infrastructure, applications, and data.
- These measures ensure user and device authentication, data and resource access control, and data privacy protection.

- They also support regulatory data compliance. Cloud security is employed in cloud environments to protect a company's data from distributed denial of service (DDoS) attacks, malware, hackers, and unauthorized user access or use.
- Security risk is normally an accidental error that occurs while developing and implementing the software. **For example**, configuration errors, design errors, and software bugs, etc.
- Cloud computing is a term referred to storing and accessing data over the internet. It doesn't store any data on the hard disk of our personal computer. In cloud computing, we can access data from a remote server.

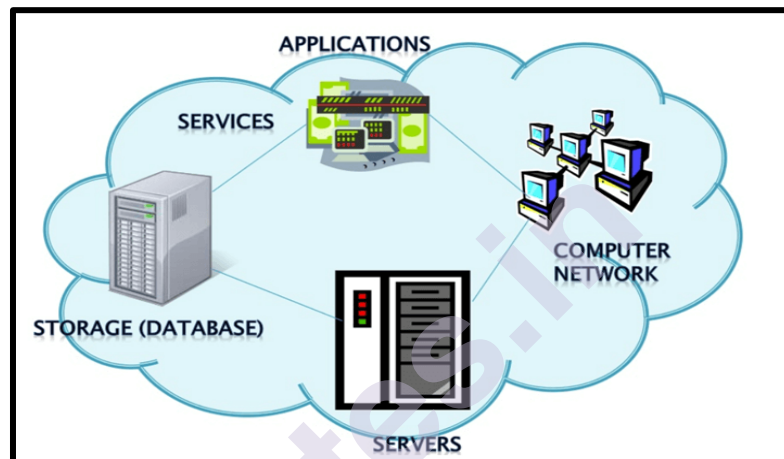


Fig. 12.1: Overview of Cloud Computing

12.1.1 History of Cloud Computing:

The concept of Cloud Computing came into existence in the year 1950 with implementation of mainframe computers, accessible via thin/static clients. Since then, cloud computing has been evolved from static clients to dynamic ones and from software to services. The following diagram explains the evolution of cloud computing:

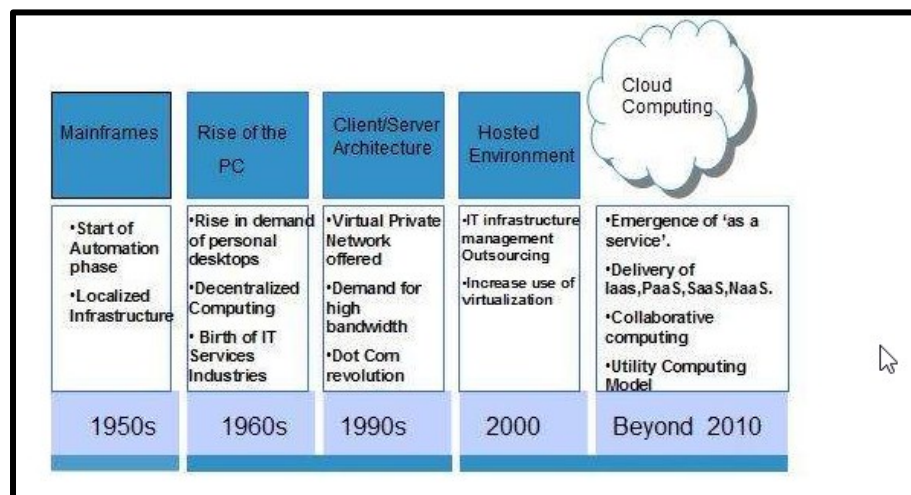


Fig. 12.2: History of Cloud

12.1.2 Characteristics Cloud Computing security:

There are basically **5 essential characteristics** of Cloud Computing:-

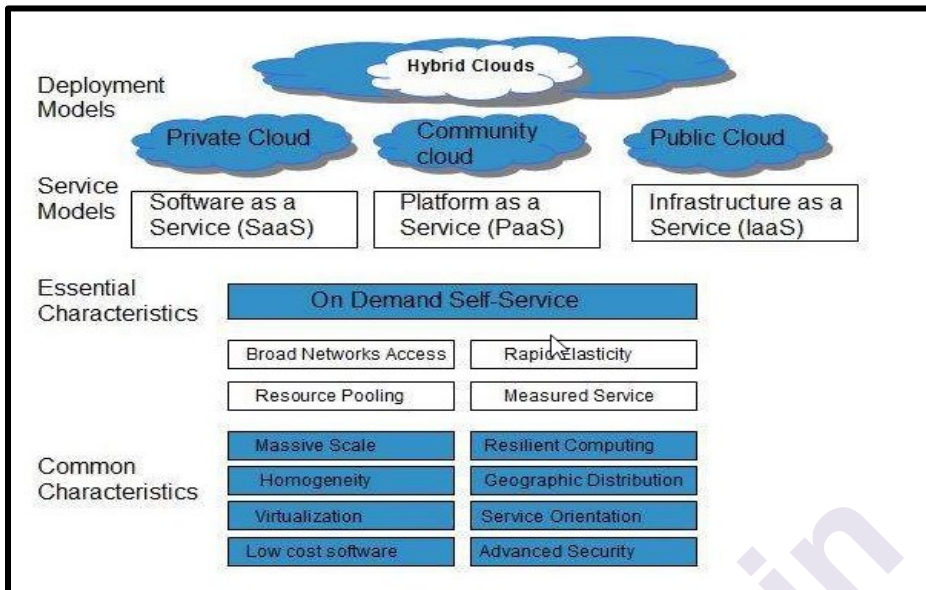


Fig. 12.3: Characteristics of Cloud Computing

- **On-demand self-services:** The Cloud computing services does not require any human administrators, user themselves are able to provision, monitor and manage computing resources as needed.
- **Broad network access:** The Computing services are generally provided over standard networks and heterogeneous devices.
- **Rapid elasticity:** The Computing services should have IT resources that are able to scale out and in quickly and on as needed basis. Whenever the user require services it is provided to him and it is scale out as soon as its requirement gets over.
- **Resource pooling:** The IT resource (e.g., networks, servers, storage, applications, and services) present are shared across multiple applications and occupant in an uncommitted manner. Multiple clients are provided service from a same physical resource.
- **Measured service:** The resource utilization is tracked for each application and occupant, it will provide both the user and the resource provider with an account of what has been used. This is done for various reasons like monitoring billing and effective use of resource.

12.1.3 Cloud Computing Architecture:-

- Cloud Computing architecture comprises of many cloud components, which are loosely coupled. We can broadly divide the cloud architecture into two parts:
 - Front End
 - Back End

- Each of the ends is connected through a network, usually Internet. The following diagram shows the graphical view of cloud computing architecture:

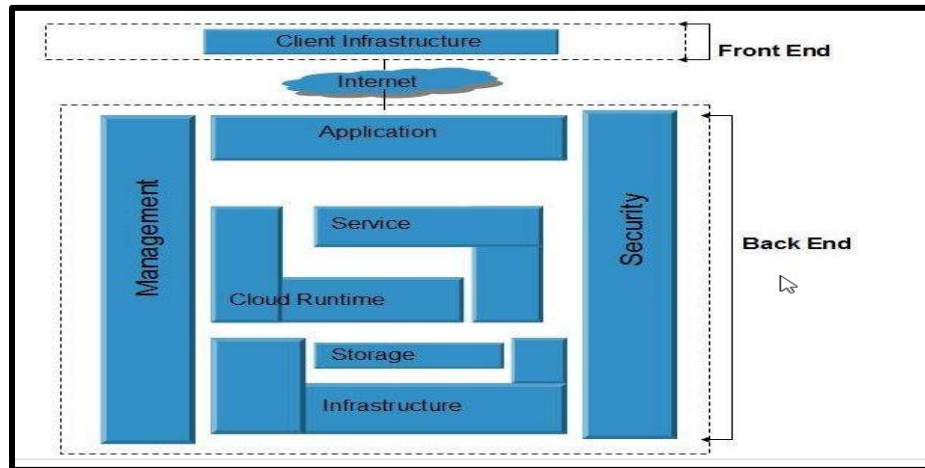


Fig. 12.4: Cloud Computing Architecture

- Front End:-** The front end refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, Example - Web Browser.
- Back End:-** The back End refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

12.2 TYPES OF CLOUD COMPUTING SERVICES

Cloud computing is typically classified in two ways:

- Location of the cloud computing
- Type of services offered

Location of the cloud:- Cloud computing is typically classified in the following three ways:

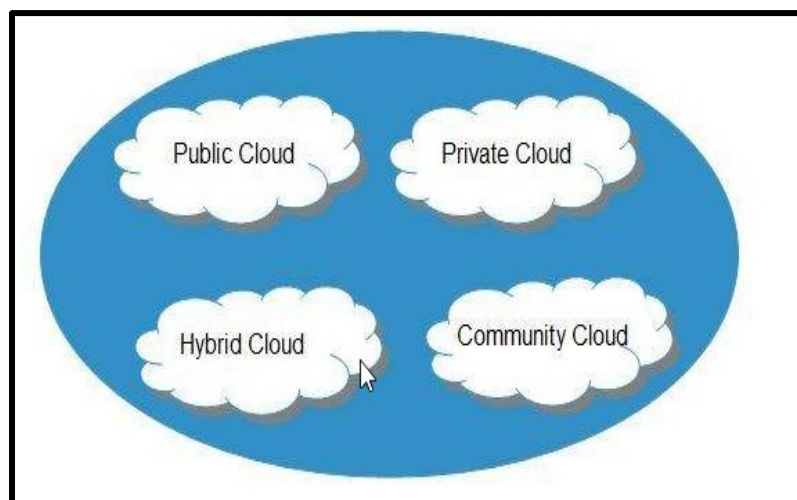


Fig. 12.5: Types of Cloud

- **Public cloud:** In the Public cloud, the computing infrastructure is hosted by the cloud vendor at the vendor's premises, it is open for public use. It allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness. The Public Cloud Model is shown in the diagram below:-

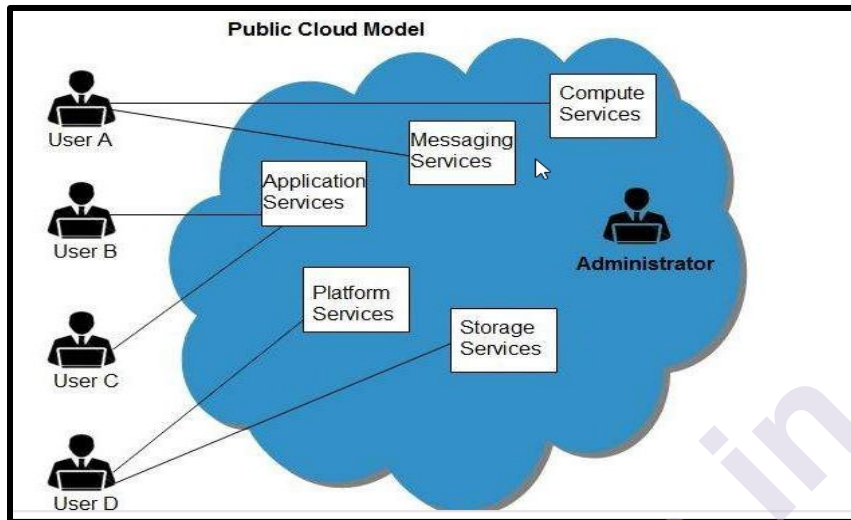


Fig. 12.6: Public Cloud Model

- **Benefits:-** There are many benefits of deploying cloud as public cloud model. The following diagram shows some of those benefits:

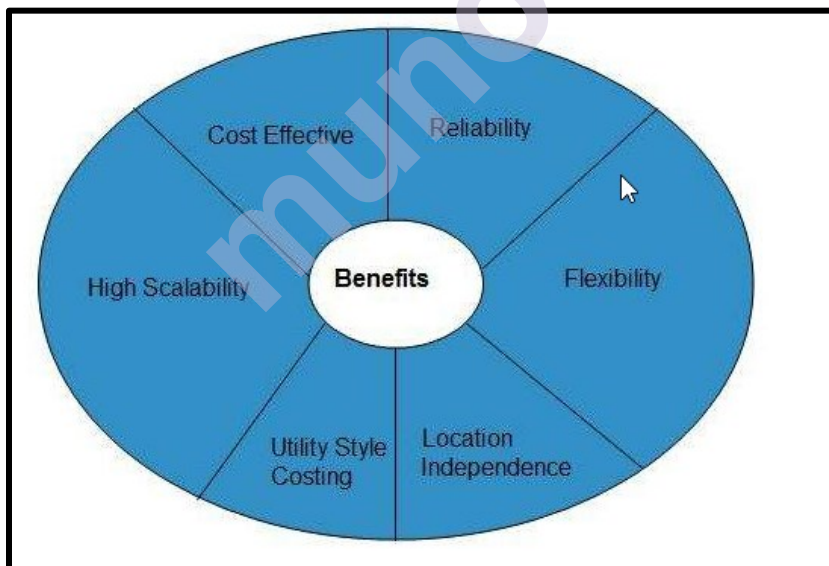


Fig. 12.7: Benefits of Public Cloud

- **Cost Effective:-** Since public cloud shares same resources with large number of customers it turns out inexpensive.
- **Reliability:-** The public cloud employs large number of resources from different locations. If any of the resources fails, public cloud can employ another one.

- **Flexibility:-** The public cloud can smoothly integrate with private cloud, which gives customers a flexible approach.
- **Location Independence:-** Public cloud services are delivered through Internet, ensuring location independence.
- **Utility Style Costing:-** Public cloud is also based on pay-per-use model and resources are accessible whenever customer needs them.
- **High Scalability:-** Cloud resources are made available on demand from a pool of resources, i.e., they can be scaled up or down according to the requirement.
- **Disadvantages:-** Here are some disadvantages of public cloud model:
 - **Low Security:-** In public cloud model, data is hosted off-site and resources are shared publicly, therefore does not ensure higher level of security.
 - **Less Customizable:-** It is comparatively less customizable than private cloud.
- **Private cloud:** The computing infrastructure is dedicated to a particular organization and not shared with other organizations. Private clouds are more expensive and more secure when compared to public clouds. The private cloud allows systems and services to be accessible within an organization. It is more secured because of its private nature. It is operated only within a single organization. However, it may be managed internally by the organization itself or by third-party. The private cloud model is shown in the diagram below.

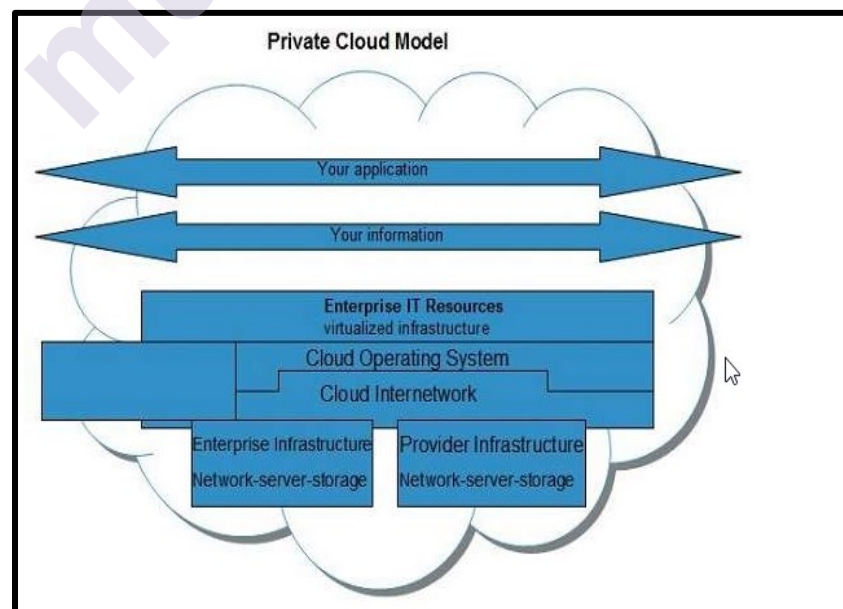


Fig. 12.8: Private Cloud Model

- **Benefits:-** There are many benefits of deploying cloud as private cloud model. The following diagram shows some of those benefits:

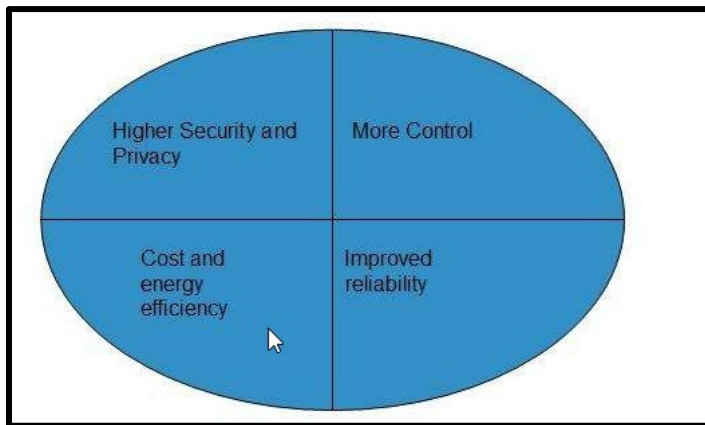


Fig. 12.9: Benefits of Private Cloud

- **High Security and Privacy:-** Private cloud operations are not available to general public and resources are shared from distinct pool of resources. Therefore, it ensures high security and privacy.
- **More Control:-** The private cloud has more control on its resources and hardware than public cloud because it is accessed only within an organization.
- **Cost and Energy Efficiency:-** The private cloud resources are not as cost effective as resources in public clouds but they offer more efficiency than public cloud resources.
- **Disadvantages:-** Here are the disadvantages of using private cloud model:
 - **Restricted Area of Operation:** - The private cloud is only accessible locally and is very difficult to deploy globally.
 - **High Priced:-** Purchasing new hardware in order to fulfill the demand is a costly transaction.
 - **Limited Scalability:-** The private cloud can be scaled only within capacity of internal hosted resources.
 - **Additional Skills:-** In order to maintain cloud deployment, organization requires skilled expertise.
- **Hybrid cloud:** It is a combined hosting of two or more clouds. Organizations may host critical applications on private clouds and other applications on the public cloud. The entities are unique but are bound together. The hybrid cloud is a mixture of public and private cloud, in which the critical activities are performed using private cloud while the non-critical activities are performed using public cloud. The Hybrid Cloud Model is shown in the diagram below.

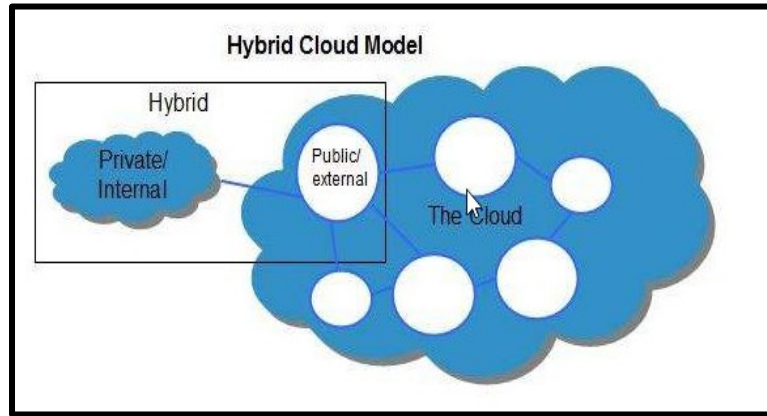


Fig. 12.10: Hybrid Cloud Model

- **Benefits:** - There are many benefits of deploying cloud as hybrid cloud model. The following diagram shows some of those benefits:

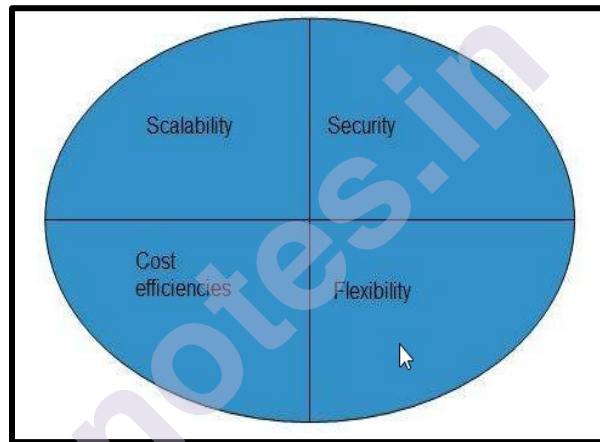


Fig. 12.11: Benefits of Hybrid Cloud

- **Scalability:-** It offers features of both, the public cloud scalability and the private cloud scalability.
- **Flexibility:-** It offers secure resources and scalable public resources.
- **Cost Efficiency:-** Public clouds are more cost effective than private ones. Therefore, hybrid clouds can be cost saving.
- **Security:-** The private cloud in hybrid cloud ensures higher degree of security.
- **Disadvantages:-**
 - **Networking Issues:-** Networking becomes complex due to presence of private and public cloud.
 - **Security Compliance:-** It is necessary to ensure that cloud services are compliant with security policies of the organization.

- **Infrastructure Dependency:-** The hybrid cloud model is dependent on internal IT infrastructure, therefore it is necessary to ensure redundancy across data centers.
- **Community cloud:** Involves sharing of computing infrastructure in between organizations of the same community. The community cloud allows systems and services to be accessible by a group of organizations. It shares the infrastructure between several organizations from a specific community. It may be managed internally by organizations or by the third-party. The Community Cloud Model is shown in the diagram below:-

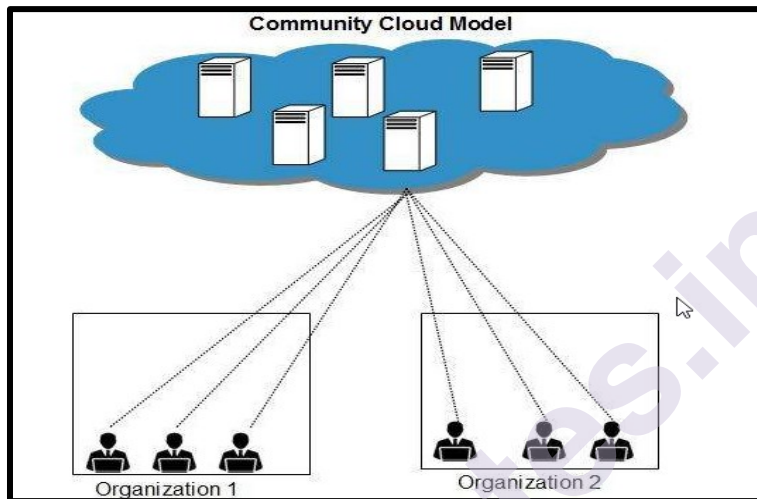


Fig. 12.12: Community Cloud Model

- **Benefits:-** There are many benefits of deploying cloud as community cloud model.

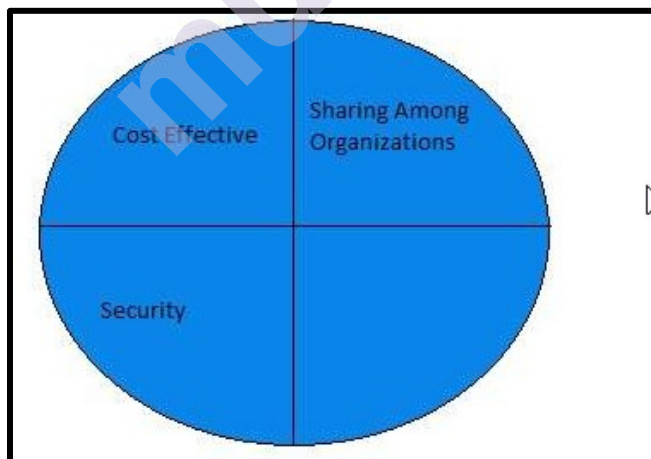


Fig. 12.13: Benefits of Community Cloud

- **Cost Effective:-** Community cloud offers same advantages as that of private cloud at low cost.

- **Sharing Among Organizations:-** Community cloud provides an infrastructure to share cloud resources and capabilities among several organizations.
- **Security: -** The community cloud is comparatively more secure than the public cloud but less secured than the private cloud.
- **Issues:-**
 - Since all data is located at one place, one must be careful in storing data in community cloud because it might be accessible to others.
 - It is also challenging to allocate responsibilities of governance, security and cost among organizations.
- **Types of Services Offered: -** Cloud computing is based on service models. They are categorized into three basic service models which are based upon the services offered, clouds are classified in the following ways:
 - Infrastructure-as-a-Service (IaaS)
 - Platform-as-a-Service (PaaS)
 - Software-as-a-Service (SaaS)
 - **Anything-as-a-Service (XaaS)** is yet another service model, which includes Network-as-a-Service, Business-as-a-Service, Identity-as-a-Service, Database-as-a-Service or Strategy-as-a-Service.
- **Infrastructure as a service (IaaS):** The Infrastructure-as-a-Service (IaaS) is the most basic level of service. Each of the service models inherit the security and management mechanism from the underlying model, **as shown in the following diagram:**

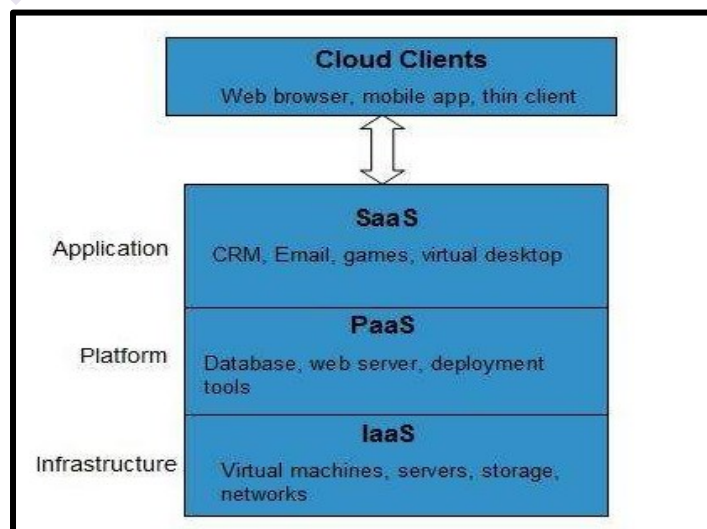


Fig. 12.14: Services offered by Cloud

Involves offering virtual machines, abstracted hardware and operating systems using the principles of cloud computing. As the name implies, only the infrastructure is purchased while the software is owned by the user. Leading vendors that provide Infrastructure as a service are, Amazon EC2, Amazon S3, Rackspace Cloud Servers and Flexi scale. **IaaS** provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

- **Platform as a Service (PaaS):** It provides the runtime environment for applications, development and deployment tools, etc. Involves offering a development platform, configuration management on the cloud. Platforms provided by different vendors are typically not compatible. **Examples include** Google's Application Engine, Microsoft's Azure, Salesforce.com, force.com.
- **Software as a service (SaaS):** This model allows to use software applications as a service to end-users. Provides complete software offering on the cloud. Users can use on-demand basis, **e.g.** Salesforce.com, Google cs and Microsoft online version of office called BPOS (Business Productivity Online Standard Suite).

12.3 MODELS OF CLOUD COMPUTING SECURITY

According to NIST there are three service models: infrastructure as a service (IaaS), platform as a service (PaaS), and software as-a-service (SaaS).

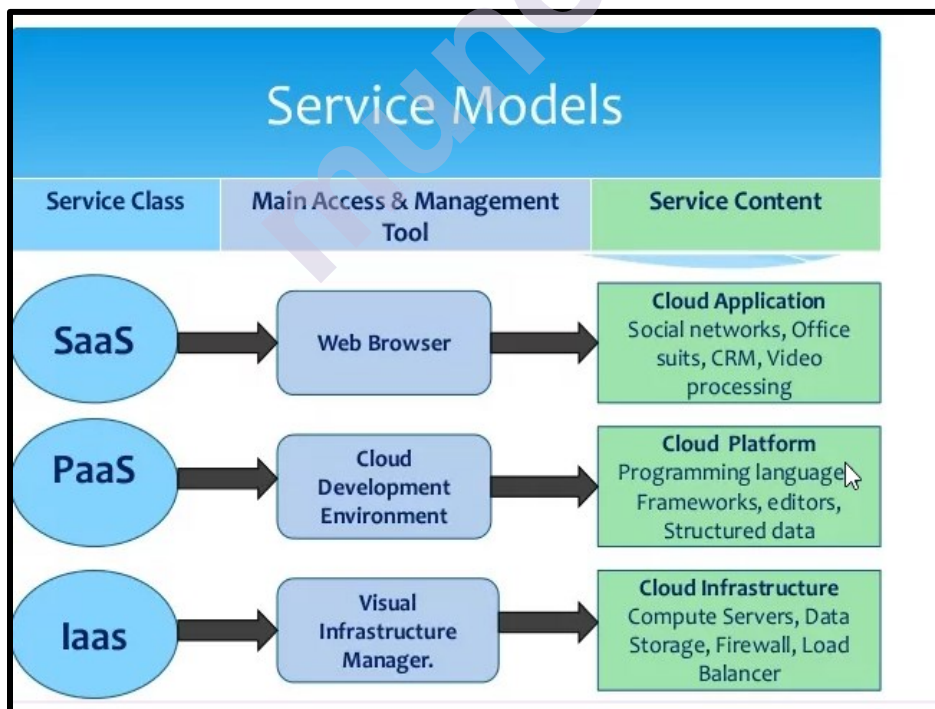


Fig. 12.15: Services Models of Cloud

To get a better understanding on what each of the service models comprises,

refer to the following image that depicts the layers of which a typical IT solution consists:

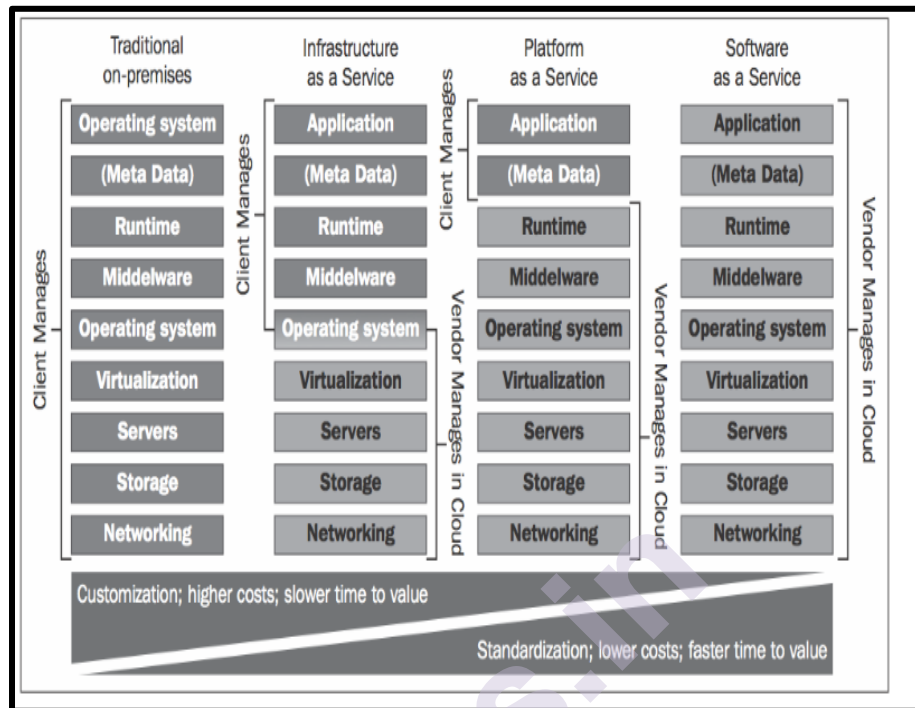


Fig. 12.16: Layers of Cloud Service Models

- An infrastructure as a service solution should include vendor-managed network, storage, servers, and virtualization layers for a client to run their application and data on. Next, platform as a service build on top of infrastructure as a service adding vendor-managed middleware such as web, application, and database software. Software as a service again builds on top of that, most of the time adding applications that implement specific user functionality such as email, CRM, or HRM.
- Interestingly enough, IBM and other major IT and analyst firms have added a fourth service model, namely business process as a service (BPaaS). BPaaS, as the term implies, offers an entire horizontal or vertical business process and builds on top of any of the previously depicted cloud service models.

12.4 BENEFITS/ADVANTAGES OF CLOUD COMPUTING:

Cloud computing is the on-demand delivery of IT capabilities on metered services. It is the practice of using a network of remote servers hosted on the internet to store, manage, and process data; rather than a local server, or a personal computer. Its various benefits are as follows:-

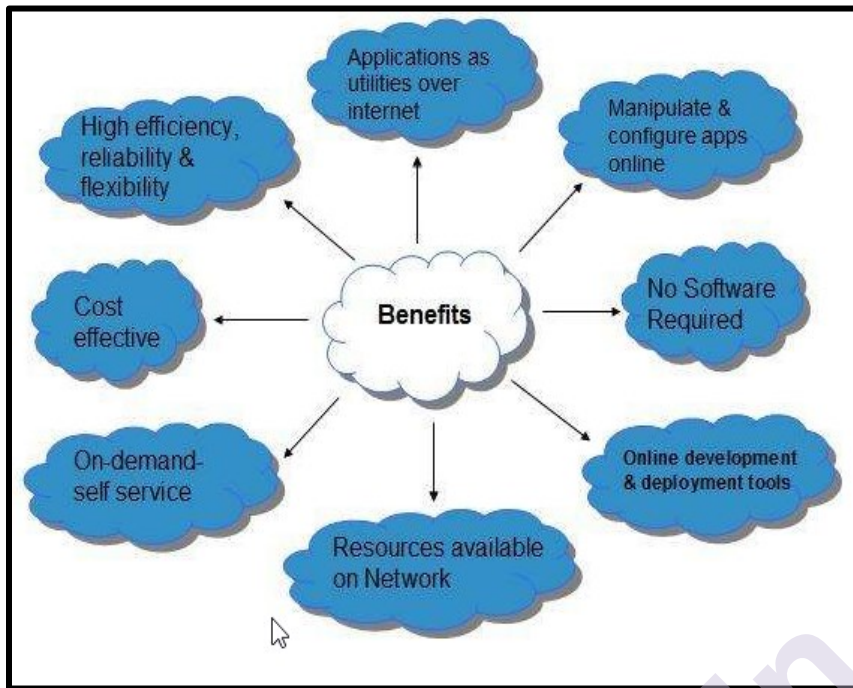


Fig. 12.17: Benefits of Cloud Computing

- **Cost Savings:** - Cost saving is one of the biggest Cloud Computing benefits. It helps us to save substantial capital cost as it does not need any physical hardware investments. Also, we do not need trained personnel to maintain the hardware. The buying and managing of equipment is done by the cloud service provider.
- **Strategic edge:-** Cloud computing offers a competitive edge over your competitors. It is one of the best advantages of Cloud services that helps us to access the latest applications any time without spending our time and money on installations.
- **High Speed:-** Cloud computing allows us to deploy our service quickly in fewer clicks. This faster deployment allows us to get the resources required for our system within fewer minutes.
- **Back-up and restore data:** - Once the data is stored in a Cloud, it is easier to get the back-up and recovery of that, which is otherwise very time taking process on-premise.
- **Automatic Software Integration:** - In the cloud, software integration is something that occurs automatically. Therefore, we don't need to take additional efforts to customize and integrate our applications as per our preferences.
- **Reliability:-** Reliability is one of the biggest benefits of Cloud hosting. We can always get instantly updated about the changes.
- **Mobility:** - Employees who are working on the premises or at the remote locations can easily access all the cloud services. All they need is an Internet connectivity.
- **Unlimited storage capacity:-** The cloud offers almost limitless storage capacity. At any time you can quickly expand our storage capacity with very nominal monthly fees.

- **Collaboration:-** The cloud computing platform helps employees who are located in different geographies to collaborate in a highly convenient and secure manner.
- **Quick Deployment:-** Last but not least, cloud computing gives us the advantage of rapid deployment. So, when we decide to use the cloud, our entire system can be fully functional in very few minutes. Although, the amount of time taken depends on what kind of technologies are used in our business.

Other Important Benefits of Cloud Computing:- Apart from the above, some other Cloud Computing advantages are:

- On-Demand Self-service
- Multi-tenancy
- Offers Resilient Computing
- Fast and effective virtualization
- Provide you low-cost software
- Offers advanced online security
- Location and Device Independence
- Always available, and scales automatically to adjust to the increase in demand
- Allows pay-per-use
- Web-based control & interfaces
- API Access available.

12.5 DISADVANTAGES OF CLOUD COMPUTING SERVICES

There are significant challenges of using Cloud Computing:



Fig. 12.18: Challenges for Cloud Computing

- **Performance Can Vary:-** When we are working in a cloud environment, our application is running on the server which simultaneously provides resources to other businesses. Any greedy behavior or DDOS attack on your tenant could affect the performance of our shared resource.
- **Technical Issues:-** Cloud technology is always prone to an outage and other technical issues. Even, the best cloud service provider companies may face this type of trouble despite maintaining high standards of maintenance.
- **Security Threat in the Cloud:-** Another drawback while working with cloud computing services is security risk. Before adopting cloud technology, we should be well aware of the fact that you will be sharing all our company's sensitive information to a third-party cloud computing service provider. Hackers might access this information.
- **Downtime:-** Downtime should also be considered while working with cloud computing. That's because our cloud provider may face power loss, low internet connectivity, service maintenance, etc.
- **Internet Connectivity:-** Good Internet connectivity is a must in cloud computing. We can't access cloud without an internet connection. Moreover, we don't have any other way to gather data from the cloud.
- **Lower Bandwidth:-** Many cloud storage service providers limit bandwidth usage of their users. So, in case if our organization surpasses the given allowance, the additional charges could be significantly costly.
- **Lacks of Support:-** Cloud computing companies fail to provide proper support to the customers. Moreover, they want their user to depend on FAQs or online help, which can be a tedious job for non-technical persons.

12.6 THREATS AND ATTACKS TO CLOUD COMPUTING

- **Deletion without a backup**
- **Data Breach:-** Data Breach is the process in which the confidential data is viewed, accessed, or stolen by the third party without any authorization, so organization's data is hacked by the hackers.
 - Hardware failures
 - Natural disasters
 - Authentication attacks
 - VM level attacks
- **Malicious insiders:-** Insider threats are a major security issue for any organization. A malicious insider already has authorized access to an

organization's network and some of the sensitive resources that it contains. Attempts to gain this level of access are what reveals most attackers to their target, making it hard for an unprepared organization to detect a malicious insider. On the cloud, detection of a malicious insider is even more difficult. With cloud deployments, companies lack control over their underlying infrastructure, making many traditional security solutions less effective. This, along with the fact that cloud-based infrastructure is directly accessible from the public Internet and often suffers from security misconfigurations, makes it even more difficult to detect malicious insiders.

- Unknown risk profile
- Vulnerable co-existents
- Compliance risks
- E-discovery is difficult across cross-borders.
- Loss of the encoding key
- **Unauthorized access:** - Unlike an organization's on-premises infrastructure, their cloud-based deployments are outside the network perimeter and directly accessible from the public Internet. While this is an asset for the accessibility of this infrastructure to employees and customers, it also makes it easier for an attacker to gain unauthorized access to an organization's cloud-based resources. Improperly-configured security or compromised credentials can enable an attacker to gain direct access, potentially without an organization's knowledge.
- **Account, Service & Traffic Hijacking:** - Account hijacking is a serious security risk in cloud computing. It is the process in which individual user's or organization's cloud account (bank account, e-mail account, and social media account) is stolen by hackers. The hackers use the stolen account to perform unauthorized activities. Almost every organization has adopted cloud computing to varying degrees within their business. However, with this adoption of the cloud comes the need to ensure that the organization's cloud security strategy is capable of protecting against the top threats to cloud security.
- **Man-in-the-middle attacks**
- **Denial-of-service attacks:-** Denial of service (DoS) attacks occur when the system receives too much traffic to buffer the server. Mostly, DoS attackers target web servers of large organizations such as banking sectors, media companies, and government organizations. To recover the lost data, DoS attackers charge a great deal of time and money to handle the data.
- Cloud service provider may go out of business.

- Cloud service provider may decide to hold the data as a hostage if there is a dispute.
- Need to ensure that its private data is stored separately from others. If another client is the victim of a hack attack, it might affect the availability or integrity of the data of other companies located in the same environment.
- Data transfer across borders makes the laws to be applied even more complicated and consequently resulting in the private information to be even more vulnerable.
- SQL injection attacks allow attackers to gain unauthorized access to a database.
- Cross Site Scripting (XSS)
- Cryptanalysis attacks
- Side channel attacks
- Social engineering attacks
- DNS attacks
- **Cyberattacks:-** Cybercrime is a business, and cybercriminals select their targets based upon the expected profitability of their attacks. Cloud-based infrastructure is directly accessible from the public Internet, is often improperly secured, and contains a great deal of sensitive and valuable data. Additionally, the cloud is used by many different companies, meaning that a successful attack can likely be repeated many times with a high probability of success. As a result, organizations' cloud deployments are a common target of cyberattacks.
- **Accidental Exposure of Credentials:** - Phishers commonly use cloud applications and environments as a pretext in their phishing attacks. With the growing use of cloud-based email (G-Suite, Microsoft 365, etc.) and document sharing services (Google Drive, Dropbox, OneDrive), employees have become accustomed to receiving emails with links that might ask them to confirm their account credentials before gaining access to a particular document or website. This makes it easy for cybercriminals to learn an employee's credentials for cloud services. As a result, accidental exposure of cloud credentials is a major concern for 44% of organizations since it potentially compromises the privacy and security of their cloud-based data and other resources.
- **Main Cloud Security Concerns in 2021:-** In the Cloud Security Report, organizations were asked about their major security concerns regarding cloud environments. Despite the fact that many organizations have decided to move sensitive data and important applications to the cloud, concerns about how they can protect it there abound.

- **Unauthorized Access:-** Unlike an organization's on-premises infrastructure, their cloud-based deployments are outside the network perimeter and directly accessible from the public Internet. While this is an asset for the accessibility of this infrastructure to employees and customers, it also makes it easier for an attacker to gain unauthorized access to an organization's cloud-based resources. Improperly-configured security or compromised credentials can enable an attacker to gain direct access, potentially without an organization's knowledge.

Some most common Security Risks of Cloud Computing are given below-

- **Data Loss:** - Data loss is the most common cloud security risks of cloud computing. It is also known as data leakage. Data loss is the process in which data is being deleted, corrupted, and unreadable by a user, software, or application. In a cloud computing environment, data loss occurs when our sensitive data is somebody else's hands, one or more data elements cannot be utilized by the data owner, hard disk is not working properly, and software is not updated.
- **Hacked Interfaces and Insecure APIs:** - As we all know, cloud computing is completely depends on Internet, so it is compulsory to protect interfaces and APIs that are used by external users. APIs are the easiest way to communicate with most of the cloud services. In cloud computing, few services are available in the public domain. These services can be accessed by third parties, so there may be a chance that these services easily harmed and hacked by hackers.
- **Data Breach:** - Data Breach is the process in which the confidential data is viewed, accessed, or stolen by the third party without any authorization, so organization's data is hacked by the hackers.
- **Vendor lock-in:** - Vendor lock-in is the biggest security risks in cloud computing. Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that can cause difficulty moving one cloud to another.
- **Increased complexity strains IT staff:** - Migrating, integrating, and operating the cloud services is complex for the IT staff. IT staff must require the extra capability and skills to manage, integrate, and maintain the data to the cloud.
- **Spectre & Meltdown:** - It allows programs to view and steal data which is currently processed on computer. It can run on personal computers, mobile devices, and in the cloud. It can store the password, your personal information such as images, emails, and business documents in the memory of other running programs.
- **Denial of Service (DoS) attacks:** - This attacks occur when the system receives too much traffic to buffer the server. Mostly, DoS attackers target web servers of large organizations such as banking sectors, media companies, and government organizations. To recover

the lost data, DoS attackers charge a great deal of time and money to handle the data.

- **Account hijacking:** - It is a serious security risk in cloud computing. It is the process in which individual user's or organization's cloud account (bank account, e-mail account, and social media account) is stolen by hackers. The hackers use the stolen account to perform unauthorized activities. Almost every organization has adopted cloud computing to varying degrees within their business. However, with this adoption of the cloud comes the need to ensure that the organization's cloud security strategy is capable of protecting against the top threats to cloud security.
- **Misconfiguration:** - Misconfigurations of cloud security settings are a leading cause of cloud data breaches. Many organizations' cloud security posture management strategies are inadequate for protecting their cloud-based infrastructure.

12.7 SUMMARY

- Define Cloud Computing Security
- **Know the history:** The concept of Cloud Computing came into existence in the year 1950 with implementation of mainframe computers, accessible via thin/static clients.
- Cloud Computing architecture comprises of many cloud components, which are loosely coupled. We can broadly divide the **cloud architecture into two parts: Front End and Back End.**
- State Various Characteristics Cloud Computing security i.e. on-demand self-services, Broad network access, Rapid elasticity, Resource pooling and measured service.
- Understand different types of Cloud Computing services that: based on Location of the cloud computing: Cloud computing is typically classified in the following three ways: Public cloud, Private cloud, Hybrid cloud, Community cloud.
- Types of Services Offered:- Based upon the services offered, clouds are classified in the following ways: Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a service (SaaS)
- Identify and explain various Service Models of Cloud Computing
- List and describe various benefits of Cloud Computing i.e. Cost Savings, Strategic edge, High Speed, Back-up and restore data, Automatic Software Integration, Reliability, Mobility, Unlimited storage capacity, Collaboration, Quick Deployment etc.
- **Know various disadvantages of Cloud Computing: Performance Can Vary:-**
- Technical Issues, Security Threat in the Cloud, Downtime, Internet Connectivity and Lower Bandwidth.

- **Know various** threats and attacks related with cloud computing i.e. Deletion without a backup, Data Breach, Hardware failures, Natural disasters, Authentication attacks, VM level attacks, Unknown risk profile, Vulnerable co-existents, Compliance risks, E-discovery is difficult across cross-borders, Loss of the encoding key, Unauthorized access, Account, Service & Traffic Hijacking, Denial-of-service attacks, SQL injection attacks allow attackers to gain unauthorized access to a database, Cross Site Scripting (XSS), Cryptanalysis attack, Side channel attack, Social engineering attacks, DNS attacks etc.

12.8 UNIT END EXERCISE

1. Define Cloud Computing security.
2. Explain history of Cloud Computing.
3. Explain the architecture of Cloud Computing in brief.
4. Explain Various Characteristics of Cloud Computing security.
5. Explain different types of Cloud Computing in detail.
6. Explain benefits and disadvantages of Public Cloud.
7. Explain benefits and disadvantages of Private Cloud.
8. Explain benefits and disadvantages of Hybrid Cloud.
9. Explain benefits and disadvantages of Community Cloud.
10. Explain different services offered by Cloud Computing in detail.
11. With the help of neat labelled diagram explain Cloud Computing Service Models.
12. Explain various Benefits/Advantages of Cloud Computing.(any five)
13. Explain various disadvantages of Cloud Computing. (any five).
14. Explain various threats and attacks related to cloud computing security.
15. Explain various risks associated with cloud computing security.(any five)

12.9 REFERENCES

- Matt Walker, All-In-One-CEH-Certified-Ethical-Hacker-Exam-Guide.
- Tutorials Point Professionals, Ethical Hacking by Tutorials Point.

12.10 BIBLIOGRAPHY

- Sean-Philip Oriyano, Sybex, Certified Ethical Hacker Study Guide v9, Study Guide Edition, 2016.

CRYPTOGRAPHY

Unit Structure

13.0 Objectives

13.1 Cryptography and its Objectives

13.1.1 Overview of Cryptography and Encryption Techniques

13.1.2 Generation of Public and Private Keys

13.1.3 Overview of the MD5, SHA, RC4, RC5 and Blowfish

Algorithms

13.2 Cryptography types

13.3 Cryptography attacks and its Categories

13.4 Ciphers and their classification

13.5 Data encryption standard and advanced encryption standard

13.6 Digital signature algorithm and related signature schemes

13.7 Digital signatures

13.8 Public key infrastructure

13.9 Certifying authorities with its types

13.10 Disk encryption

13.11 Code breaking techniques

13.12 Summary

13.13 Unit End Exercise

13.14 References

13.15 Bibliography

13.0 OBJECTIVES

After this chapter, student will be able to:

- Define Cryptography
- State various Objectives of Cryptography
- Understand Cryptography and Encryption Techniques
- Explain the generation of Public and Private Keys
- State and understand the Outline of MD5, SHA, RC4, RC5 and Blowfish Algorithms.
- Identify and understand various Cryptography types
- Describe Cryptography attacks and its various Categories
- Understand and define Ciphers and their classification
- State Data encryption standard and Advanced encryption standard

- Explain Digital signature algorithm and related signature schemes
- State Public key infrastructure
- Understand different types of Certifying authorities
- Describe Disk encryption
- Identify and state different types Code breaking techniques

13.1 CRYPTOGRAPHY AND ITS OBJECTIVES

- Cryptography is the study of encryption and encryption algorithms. In a practical sense, encryption is the conversion of messages from a comprehensible form (clear text) into an incomprehensible one (cipher text), and back again.
- The purpose of encryption is to render data unreadable by interceptors or eavesdroppers who do not know the secret of how to decrypt the message. Encryption attempts to ensure secrecy in communications.
- Cryptography defines the techniques used in encryption.
- Everyone has secrets, and when it is necessary to transfer that secret information from one person to another, it's very important to protect that information or data during the transfer.
- Cryptography takes plaintext and transforms it into an unreadable form (ciphertext) for the purpose of maintaining security of the data being transferred. It uses a key to transform it back into readable data when the information reaches its destination.
- The word crypto is derived from the Greek word kryptos. Kryptos was used to depict anything that was concealed, hidden, veiled, secret, or mysterious. Graph is derived from graphia, which means writing; hence, cryptography means the art of "the secret writing."
- Cryptography is the study of mathematical techniques involved in information security such as confidentiality, data integrity, entity authentication, and data origin authentication.
- Cryptography transforms plaintext messages to ciphertext (encrypted messages) by means of encryption. Modern cryptography techniques are virtually unbreakable, though it is possible to break encrypted messages by means of cryptanalysis, also called code breaking.

There are **four main objectives of cryptography**:

- **Confidentiality:**
 - According to the International Standards Organization (ISO), confidentiality is "ensuring that the information/data can be accessed only by those authorized." Confidentiality is the term used to describe the prevention of revealing information to unauthorized computers or users.

- Any breach in confidentiality may lead to both financial and emotional distress. There have been instances of organizations going bankrupt due to a system breach by rival organizations.
- Moreover, personal information in the wrong hands can ruin the lives of system users. Therefore, only authorized users should possess access to information.
- **Integrity:**
 - Integrity is "ensuring that the information is accurate, complete, reliable, and is in its original form/" Valuable information is stored on the computer. Any data corruption/modification can reduce the value of the information. The damage that data corruption/modification can do to an organization is unfathomable.
 - Integrity of the data is affected when an insider (employee) of an organization or an attacker deletes/alters important files or when malware infects the computer.
 - Although it may be possible to restore the modified data to an extent, it is impossible to restore the value and reliability of the information.
 - Examples of **violating the data integrity include:**
 - A frustrated employee deleting important files and modifying the payroll system.
 - Vandalizing a website and so on
- **Authentication:**
 - Authenticity is "the identification and assurance of the origin of information." It is important to ensure that the information on the system is authentic and has not been tampered with. It is also important to ensure that the computer users or those who access information are who they claim to be.
- **Nonrepudiation:**
 - In digital security, nonrepudiation is the means to ensure that a message transferred has been sent and received by the persons or parties who actually intended to. Let us assume that party A is sending a message M with the signature S to the party B.
 - Then party A cannot deny the authenticity of its signature S. It can be obtained through the use of:
- **Digital signatures:** A digital signature functions as unique identifier for an individual, like a written signature. It is used to ensure that a message or document is electronically signed by the person.

- **Confirmation services:** It is possible to indicate that messages are received and/or sent by creating digital receipts. These digital receipts are generated by the message transfer agent.

13.1.1 Overview of Cryptography and Encryption Techniques:-

- Encryption can be used to encrypt data while it is in transit or while it's stored on a hard drive.
- Cryptography is the study of protecting information by mathematically scrambling the data so it cannot be deciphered without knowledge of the mathematical formula used to encrypt it. This mathematical formula is known as the **encryption algorithm**.
- Encryption algorithms can use simple methods of scrambling characters, such as substitution (replacing characters with other characters) and transposition (changing the order of characters).
- Encryption algorithms are mathematical calculations based on substitution and transposition. The two primary types of encryption are **symmetric and asymmetric key encryption**.
- Symmetric key encryption means both sender and receiver use the same secret key to encrypt and decrypt the data.
- The drawback to symmetric key encryption is there is no secure way to share the key between multiple systems. Systems that use symmetric key encryption need to use an offline method to transfer the keys from one system to another.
- This is not practical in a large environment such as the Internet, where the clients and server could be on opposite sides of the world.
- Asymmetric (or public) key cryptography was created to address the weaknesses of symmetric key management and distribution.

13.1.2 Generation of Public and Private Keys:-

- When a client and a server use asymmetric cryptography, both create their own pairs of keys for a total of four keys: **the server's public key, the server's private key, the client's public key, and the client's private key**.
- A system's key pair has a mathematical relationship that allows data encrypted with one of the keys to be decrypted with the other key. These keys have a mathematical relationship based on factoring prime numbers such that each key can be used to decrypt data encrypted with the other key.
- When a client and a server want to mutually authenticate and share information, they each send their own public key to the remote system, but never share their private keys.
- Each message is encrypted with the receiver's public key. Only the receiver's private key can decrypt the message.

- The server would encrypt a message to the client using the client's public key. The only key that can decrypt the message is held by the client, which ensures confidentiality.

13.1.3 Overview of the MD5, SHA, RC4, RC5, and Blowfish

Algorithms:-

- Algorithms vary in key length from 40 bits to 448 bits. The longer the key length, the stronger the encryption algorithm. To brute-force crack a key of 40 bits ranges from 1.4 minutes to .2 seconds, depending on the strength of the processing computer.
- In comparison, a 64-bit key requires between 50 years and 37 days to break, again depending on the speed of the processor. Currently, any key with a length over 256 bits is considered uncrack-able.
- **Message Digest 5 (MD5), Secure Hash Algorithm (SHA), RC4, RC5, and Blowfish** are all names for different mathematical algorithms used for encryption. As a CEH, we need to be familiar with these algorithms:
 - **MD5:-** MD5 is a hashing algorithm that uses a random-length input to generate a 128-bit digest. It is popular to create a digital signature to accompany documents and e-mails to prove the integrity of the source. The digital signature process involves the creation of an MD5 message digest of the document, which is then encrypted by the sender's private key. MD5 message digests are encrypted by a private key in the digital signature process.
 - **SHA: -** SHA is also a message digest, which generates a 160-bit digest of encrypted data. SHA takes slightly longer than MD5 and is considered a stronger encryption. It is the preferred algorithm for use by the government.
 - **RC4 and RC5:-** RC4 is a symmetric key algorithm and is a streaming cipher, meaning one bit is encrypted at a time. It uses random mathematical permutations and a variable key size. RC5 is the next generation algorithm: It uses a variable block size and variable key size. RC5 has been broken with key sizes smaller than 256.
 - **Blowfish: -** Blowfish is a 64-bit block cipher, which means that it encrypts data in chunks or blocks. It is stronger than a stream cipher and has a variable key length between 32 and 448 bits.

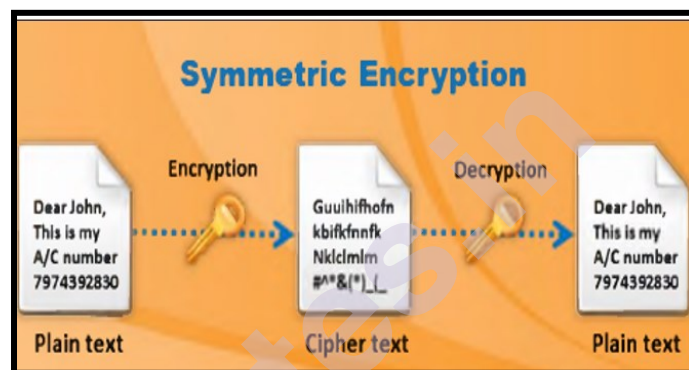
13.2 CRYPTOGRAPHY TYPES

The following are the two types of cryptography:

- Symmetric encryption (secret key cryptography)
- Asymmetric encryption (public key cryptography)

Symmetric encryption:-

- The symmetric encryption method uses the same key for encryption and decryption.
- As shown in the following figure, the sender uses a key to encrypt the plaintext and sends the ciphertext to the receiver.
- The receiver decrypts the ciphertext with the same key that is used for encryption and reads the message in plaintext. As a single secret key is used in this process symmetric encryption is also known as secret key cryptography.
- This kind of cryptography works well when you are communicating with only a few people.

**Fig. 13.1: Symmetric encryption**

- The problem with the secret key is transferring it over the large network or Internet while preventing it from falling into the wrong hands.
- In this process, anyone who knows the secret key can decrypt the message. This problem can be fixed by asymmetric encryption.

Asymmetric cryptography:

- Asymmetric cryptography uses different keys for encryption and decryption.
- In this type of cryptography, an end user on a public or private network has a pair of keys: a public key for encryption and a private key for decryption. Here, a private key cannot be derived from the public key.
- The asymmetric cryptography method has been proven to be secure against attackers.
- In asymmetric cryptography, the sender encodes the message with the help of a public key and the receiver decodes the message using a random key generated by the sender's public key.

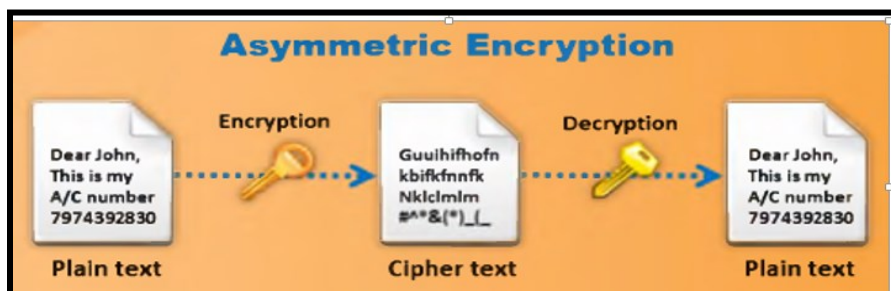


Fig. 13.2: Asymmetric encryption

13.3 CRYPTOGRAPHY ATTACKS AND ITS CATEGORIES

- Cryptographic attacks are the means by which the attacker decrypts the cipher text (breaks the cipher text) without the knowledge of the key. In these attacks, the attacker subverts the cryptographic system's security by exploiting the loopholes in code, cipher, cryptographic protocol or key management scheme.
- Cryptography attacks are based on the assumption that the cryptanalyst has knowledge of the information encrypted. Attackers have found various attacks for defeating the crypto system and they are categorized in to **eight types**:
- Cipher text only attack
- Known-plain text attack
- Chosen-plaintext
- Chosen-cipher text attack
- Chosen key attack
- Adaptive chosen-plain text attack
- Timing attack
- Rubber hose attack

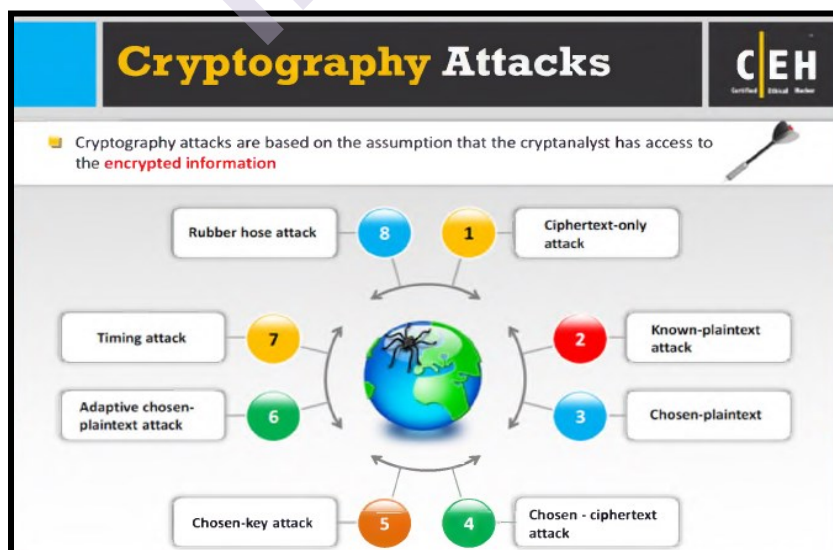


Fig. 13.3: Cryptography Attacks

- Attackers gain access to the content of the encrypted message through cryptanalysis by defeating the cryptographic security algorithms, even without the knowledge of encryption details.
- Though the algorithms are strong and are resistant to all attacks, the demands of practical cryptosystem easily introduce vulnerabilities.
- These vulnerabilities are the sources of various cryptography attacks.
- As discussed previously, there are eight types of cryptography attacks. All these attacks try either to retrieve the key or expose the plaintext. These attacks are distinguished based on the information available to the cryptanalyst to mount an attack.
- The main goal of attackers in all the cases is to decrypt the new pieces of encrypted message without additional information.

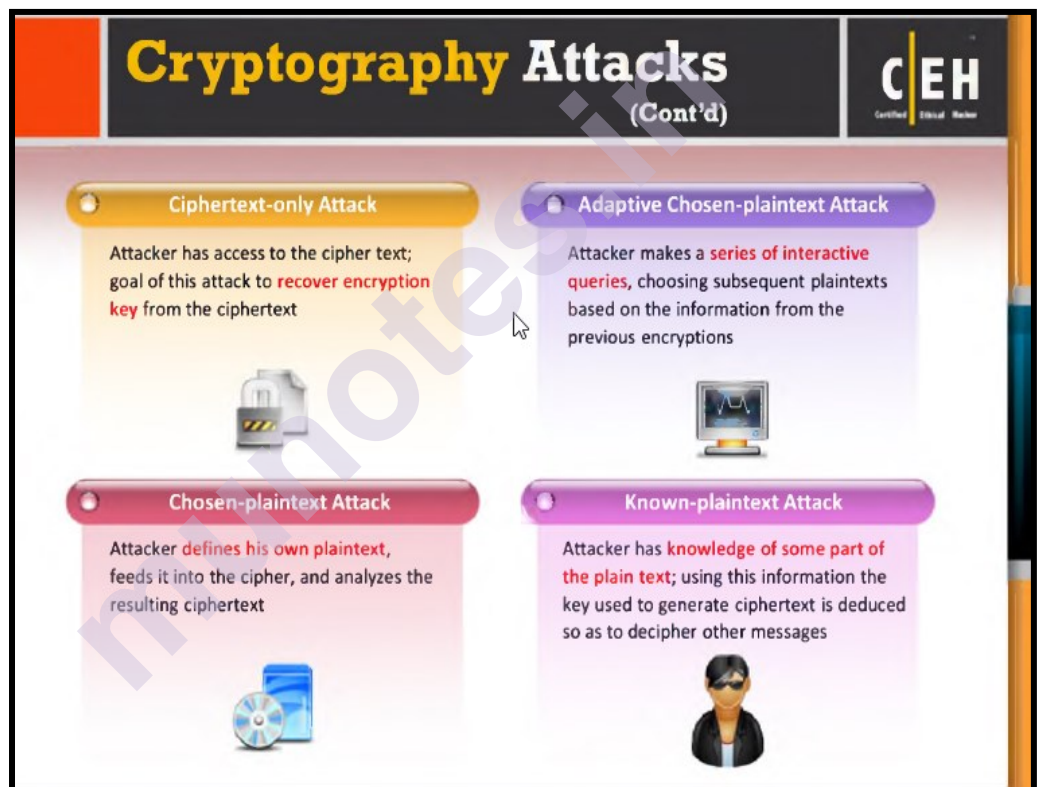


Fig. 13.4: Cryptography Attacks (a)

- **Cipher text only attack:** A ciphertext only attack is one of the basic types of active attacks because it is very easy for the attacker to get ciphertext by sniffing the traffic of any individual. In this type of attack, the attacker will have access only to ciphertext of several messages, all of which were encrypted using the same encryption algorithm. Finding the key used for encryption is the main objective of the attacker as it allows the attacker to decode all the messages encrypted with the respective key.

- **Adaptive chosen-plain text attack:** An adaptive chosen-cipher text is the collaborative version of the chosen-plain text attack. In this type of attack, the attacker chooses further cipher texts based on prior results. Here the cryptanalyst not only chooses the plain text that is encrypted but can also modify his or her choice based on the results of the previous encryption.
- **Chosen-cipher text attack:** In a chosen-cipher text attack, the attacker chooses some part of cipher text to be decrypted and tries to find out the corresponding decrypted plaintext. This is usually done with the help of a decryption oracle (a machine that decoded the text without disclosing the key). Basically, this type of attack is applicable to public-key crypto systems. This attack is harder to perform when compared to other attacks, and the attacker needs to have complete control of system containing crypto system in order to carry out this attack.
- **Rubber hose attack:** In a rubber hose attack, the attacker extracts the secret key from the user by threatening, blackmailing, or torturing him or her until the key is handed over.

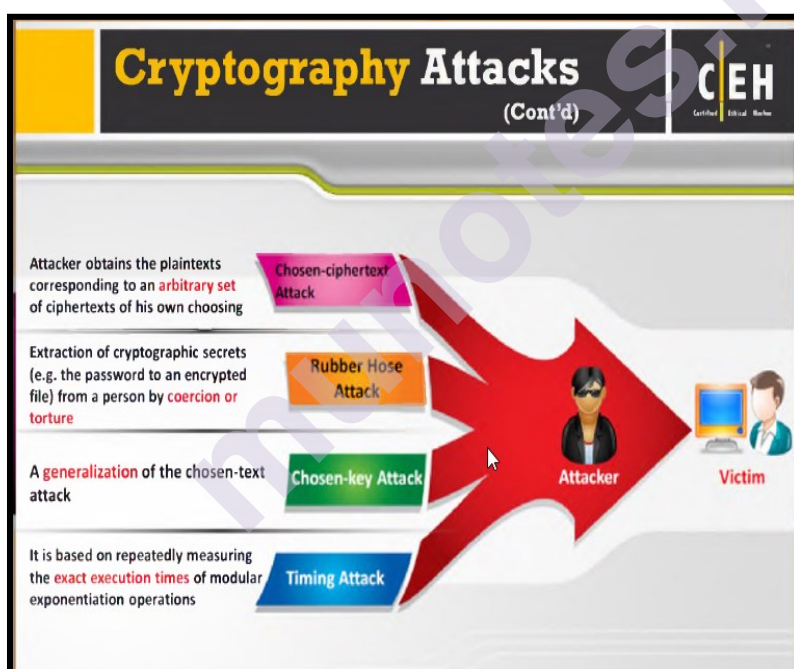


Fig. 13.5: Cryptography Attacks (b)

- **Chosen-plain text:-** This is more powerful than a plaintext attack. In this type of attacker, the attacker not only has access to the cipher text and associated plain text for several messages, but also chooses the plain text that is encrypted, and obtains the resulting cipher text.
- **Known-plaintext attack:** - In a known-plain text attack, the attacker has access to the cipher text of one or more messages as well as access to the respective plaintext. With the help of both these items, the cryptographic key can easily be extracted. The attacker can recover the

remaining encrypted, zipped files with the help of the extracted key. In general, most people start their messages with the same type of beginning notes such as greetings and close with the same type of ending such as specific salutations, contact information, name, etc. Attackers can use this as an advantage to launch known-plaintext attacks. Here the attacker has some plaintext (i.e., the data that are the same on each message) and can capture encrypted message, and therefore capture the ciphertext. Once the few parts of the message rediscovered, the remaining can easily be accomplished with the help of reverse engineering, frequency analysis, or brute force attempts.

- **Chosen key attack:** - A chosen key attack is a generalization of the chosen text attack. In this attack, the attacker has some knowledge about the relationship between the different keys, but cannot choose the key.
- **Timing Attack:** - A timing attack also is known as a side channel attack. In this type of attack, the attacker tries to compromise a crypto system by analyzing the time taken to execute cryptographic algorithms.

13.4 CIPHERS AND THEIR CLASSIFICATION

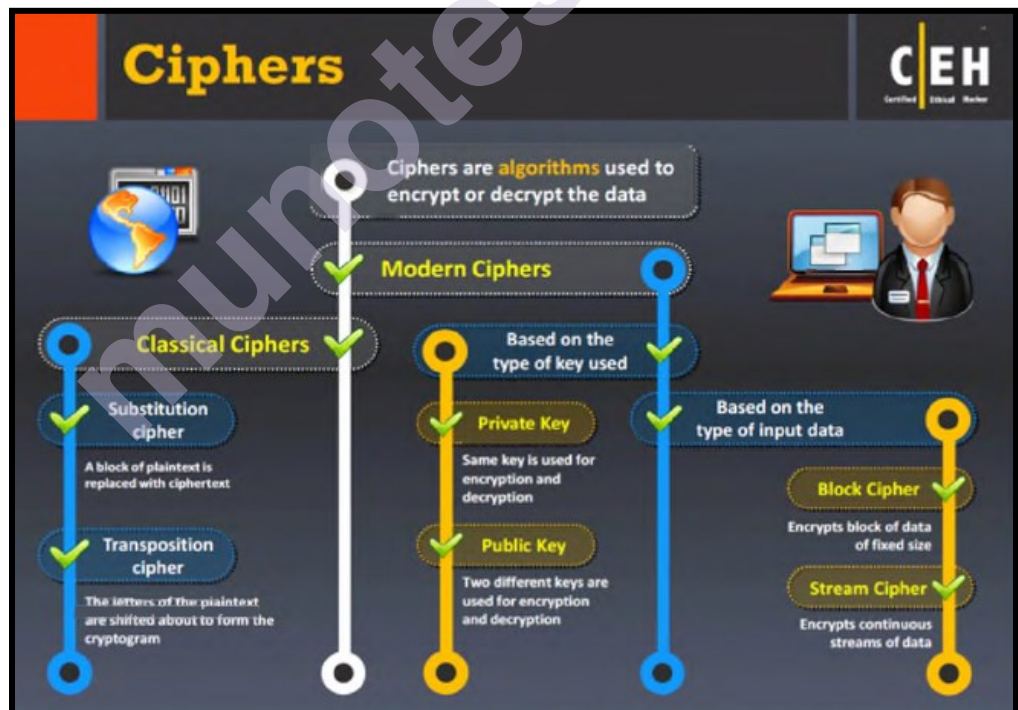


Fig. 13.6: Ciphers

- **Ciphers:** Cryptography refers to secret writing and a cipher is nothing more than an algorithm used for both encryption as well as decryption. The traditional method of encoding and decoding used to be in a different format, which provided numbering for each letter of the alphabet and used to encode the given message. If the attacker also

knew the numbering system, he or she could decode it. In cryptography, the cipher algorithm used for encoding is known as enciphering and decoding is known as deciphering.

- **Example:** abcdefgh...z are given in codes of numerical numbers, such as 12345...26. The message can be encoded based on this example and can be decoded as well. In a cipher, the message appears as plaintext but has been encoded through a key. Based on the requirements the key could be a symbol or some other form of text. If the message is highly confidential, then the key is restricted to the sender and recipient, but in some cases in open domains, some keys are shared without affecting the main data.

There are various types of ciphers:

- **Classical ciphers:** - They are the most basic type of ciphers that operate on alphabet letters, such as A-Z. These are usually implemented either by hand or with simple mechanical devices. These are not very reliable. There are two types of classical ciphers:
- **Substitution cipher:** The units of plain text are replaced with ciphertext. It replaces bits, characters, or blocks of characters with different bits, characters, or blocks.
- **Transposition cipher:** The letters of the plaintext are shifted to form the cryptogram. The cipher text is a permutation of the plaintext.
- **Modern ciphers:** Modern ciphers are designed to withstand a wide range of attacks. Modern ciphers provide message secrecy, integrity, and authentication of the sender. The modern ciphers are calculated with the help of a one-way mathematical function that is capable of factoring large prime numbers. Modern ciphers are again classified in to two categories based on the type of key and the input data. They are:

Based on the type of key used:

- **Private-key cryptography (symmetric key algorithm):** The same key is used for encryption and decryption.
- **Public-key cryptography (asymmetric key algorithm):** Two different keys are used for encryption and decryption.

Based on the type of input data:

- **Block ciphers:** Refer to an algorithm operating on block (group of bits) of fixed size with an unvarying transformation specified by a symmetric key.
- **Stream ciphers:** Refer to symmetric key ciphers. This is obtained by combining the plain text digits with a key stream (pseudorandom cipher digit stream).

13.5 DATA ENCRYPTION STANDARD AND ADVANCED ENCRYPTION STANDARD



Fig. 13.7: Data Encryption Standard

- **DES:**
 - DES is the name of the Federal Information Processing Standard (FIPS) 46-3 that describes the data encryption algorithm (DEA). It is a symmetric crypto system designed for implementation in hardware and used for single-user encryption, such as to store files on a hard disk in encrypted form.
 - DES gives 72 quadrillion or more possible encryption keys and chooses a random key for each message to be encrypted. Though DES is considered to be strong encryption, at present, triple DES is used by many organizations. Triple DES applies three keys successively.
- **AES:**

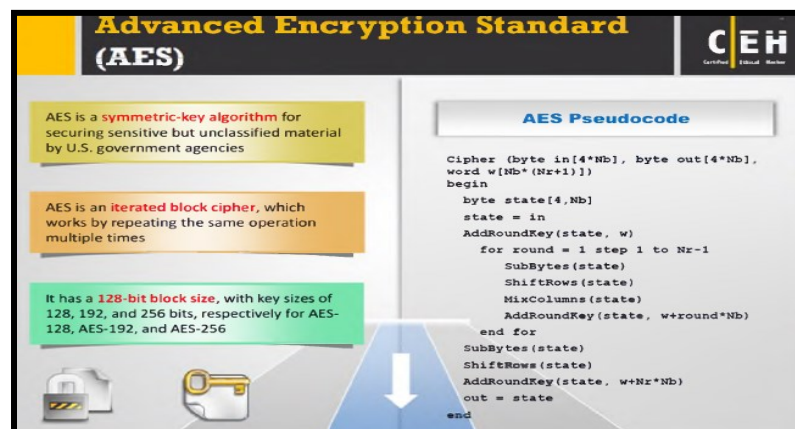


Fig. 13.8: Advanced Encryption Standard

- The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data. It can be used to encrypt digital information such as telecommunications, financial, and government data.
- AES consists of asymmetric-key algorithm, i.e., both encryption and decryption are performed using the same key.
- It is an iterated block cipher that works by repeating the defined steps multiple times. This has a 128-bit block size, with key sizes of 128, 192, and 256 bits, respectively, for AES-128, AES-192, and AES-256.
- AES Pseudo code initially, the cipher input is copied in to the internal state and then an initial round key is added.
- The state is transformed by iterating a round function in a number of cycles. Based on the block size and key length, the number of cycles may vary. Once rounding is completed, the final state is copied into the cipher output. Cipher (byte in $[4*Nb]$, byte out $[4*Nb]$, word $w[Nb*(Nr+1)]$)

begin

 byte state $[4, Nb]$

state = in

 AddRoundKey (state, w)

 for round= 1 step 1 to $Nr-1$

 SubBytes (state)

 Shift Rows(state)

 Mix Columns(state)

 Add Round Key(state, $w+round*Nb$)

 end for

 Sub Bytes state)

 Shift Rows(state)

 Add Round Key(state, $w+Nr*Nb$)

out=state

end

13.6 DIGITAL SIGNATURE ALGORITHM AND RELATED SIGNATURE SCHEMES

The DSA and Related Signature Schemes

Digital Signature Algorithm
FIPS 186-2 specifies the Digital Signature Algorithm (DSA) that may be used in the generation and verification of digital signatures for sensitive, unclassified applications

Digital Signature
The digital signature is computed using a set of rules (i.e., the DSA) and a set of parameters such that the identity of the signatory and integrity of the data can be verified

Each entity creates a public key and corresponding private key

1. Select a prime number q such that $2^{159} < q < 2^{160}$
2. Choose t so that $0 \leq t \leq 8$
3. Select a prime number p such that $2^{512+64t} < p < 2^{512+64(t+1)}$ with the additional property that q divides $(p-1)$
4. Select a generator α of the unique cyclic group of order q in \mathbb{Z}_p^*
5. To compute α , select an element g in \mathbb{Z}_p^* and compute $g^{(p-1)/q} \bmod p$
6. If $\alpha = 1$, perform step five again with a different g
7. Select a random a such that $1 \leq a \leq q-1$
8. Compute $y = \alpha^a \bmod p$

The public key is (p, q, α, y) . The private key is a .

Fig. 13.9: DSA and related signature schemes

- A digital signature is a mathematical scheme used for the authentication of a digital message. Digital Signature Algorithm (DSA) is intended for its use in the U.S. Federal Information Processing Standard (FIPS 186) called the Digital Signature Standard (DSS).
- DSA was actually proposed by the National Institute of Standards and Technology (NIST) in August 1991. NIST made the U.S. Patent 5,231,668 that covers DSA available worldwide freely. It is the first digital signature scheme recognized by any government.
- A digital signature algorithm includes a signature generation process and a signature verification process.
- **Signature Generation Process:** The private key is used to know who has signed it.
- **Signature Verification Process:** The public key is used to verify whether the given digital signature is genuine or not.
- As to the popularity of online shopping grows, e-payment systems and various other electronic payment modes rely on various systems like DSA.

Benefits of DSA:

- Less chances of forgery as it is in the case of written signature,

- Quick and easy method of business transactions,
- Fake currency problem can be drastically reduced.
- DSA, with its uses and benefits, may bring revolutionary changes in the future.

13.7 DIGITAL SIGNATURES

- A digital signature is a cryptographic means of authentication. Public key cryptography, which uses an asymmetric key algorithm, is used for creating the digital signature. The two types of keys in public key cryptography are the private key (which is known only to the signer and used to create the digital signature) and the public key (which is more widely known and is used by a relying party to verify the digital signature).
- A hash function is a process, or an algorithm, that is used in creating and verifying a digital signature. This algorithm creates a digital representation of a message, which is also known as a "fingerprint." This fingerprint is of a "hash value" of a standard length, which is much smaller than the message, but is unique to it. If any change is made to the message, it will automatically produce a different hash result; it is not possible to derive the original message from the hash value in case of a secure hash function, which is also known as a one-way hash function.
- The hash result of the original message and the hash function that is used to create the digital signature are required to verify the digital signature. With the help of the public key and the new result, the verifier checks:
- If the digital signature is created with the related private key. If the new hash result is the same as the original hash result, which was converted into a digital signature during the signing process.
- To correlate the key pair with the respective signer, the certification authority presents a certificate that is an electronic record of the public as the subject of the certificate, and confirms the identity of the signer as the related private key owner. The future signer is called the subscriber.
- The main function of a certificate is to bind a pair of public and private keys to a particular subscriber. The recipient of the certificate relies on a digital signature created by the subscriber named in the certificate. The public key listed can be used to verify that the private key is used to create the related digital signature.
- The certification authority digitally signs the certificate to assure the authenticity of both the public key and the subscriber's identity. The authority's digital signature on the certificate can be verified with the help of the public key of the certification authority recorded in another certificate, which belongs to another certification's authority. This

certificate can be authenticated with the help of another public key recorded in another certificate and so on.

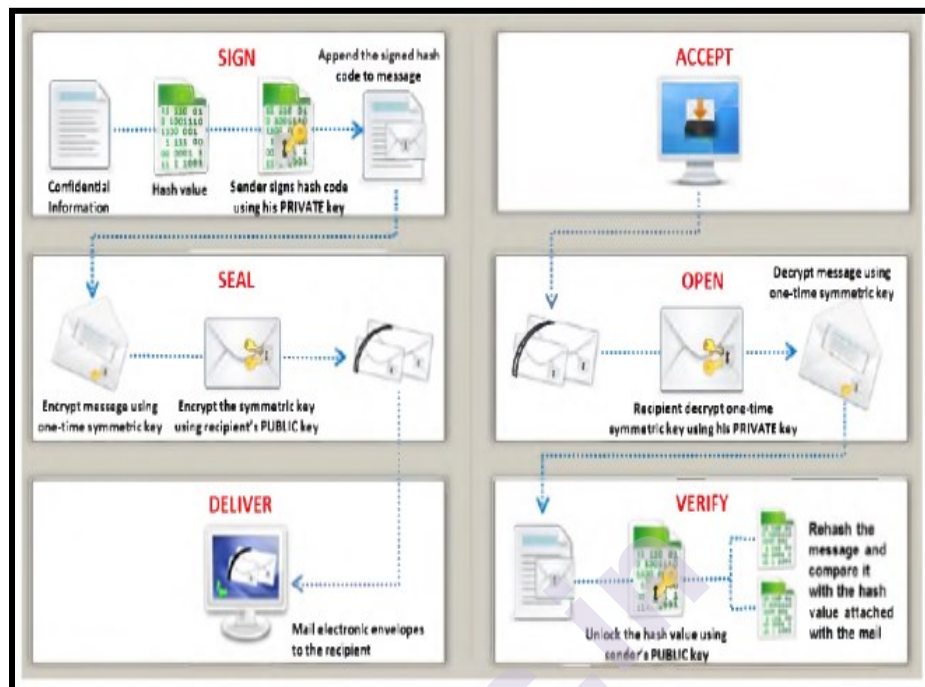


Fig. 13.10: Digital signatures

- The repository can be made to publish the certificate; the public key and its id entity are available for verification of the certificate. The retrieval and verification of the digital signature is made with the help of an online database called repositories, which holds the certificates and other information. The certification authority may suspend or revoke the certificate.

13.5 PUBLIC KEY INFRASTRUCTURE

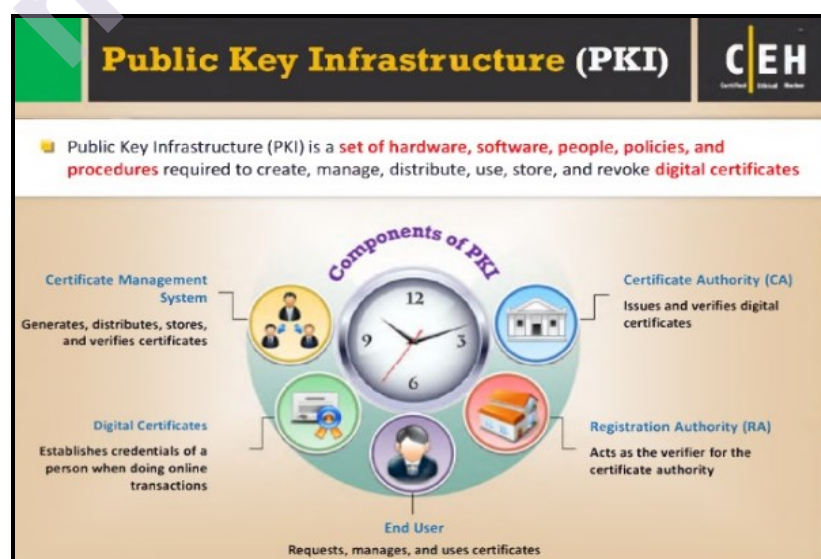


Fig. 13.11: Components of Public Key Infrastructure (PKI)

- Public Key Infrastructure (PKI) is a security architecture developed to increase the confidentiality of information being exchanged over the insecure Internet. It includes hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates.
- In cryptography, the PKI helps to bind public keys with corresponding user identities by means of a certificate authority (CA).

The following are the components of PKI:

- A certificate authority(CA) that issues and verifies digital certificates
- A certificate management system for generation, distribution, storage, and verification of certificates.
- One or more directories where the certificates (with their public keys) are held.
- A registration authority(RA) that acts as the verifier for the certificate authority
 - Cryptographic keys can be delivered securely between users by PKI.
 - The public key cryptosystem uses a pair of a public key and a private key to assure
 - Secure communication over the Internet. In public key cryptosystem authentication, it is important to connect the correct person and the public key.
 - This is accomplished with the help of Public Key Infrastructure (PKI).
 - Asymmetric (public key) cryptography is the foundation technology of PKI, when sender and receiver agreed upon a secret communication using public key encryption with a digital signature.
 - The figure that follows shows how a message gets digitally signed by the organization involved in authentication and certification by means of PKI. In public key cryptosystems, the correspondence between a public key and the private key is taken care by the certification authority (CA), i.e., based on the public key the CA determines the owner of the respective private key.
 - Initially, the user requests the certification authority for binding his or her public key; a certification authority digitally signs it and issues a public key certificate to the user.
 - It binds the user's identity with the user's public key. In between the user and the CA, there exists an organization, the Registration Authority (RA). The job of the RA is to verify the identity of the user requesting the certificate face-to-face. There exists another authority in PKI, i.e., the validation authority (VA).

- The job of the VA is to check whether the certificate was issued by Trust worthy a CA or not, i.e., is it valid or not. The sender and receiver can then exchange a secret message using public key cryptography.

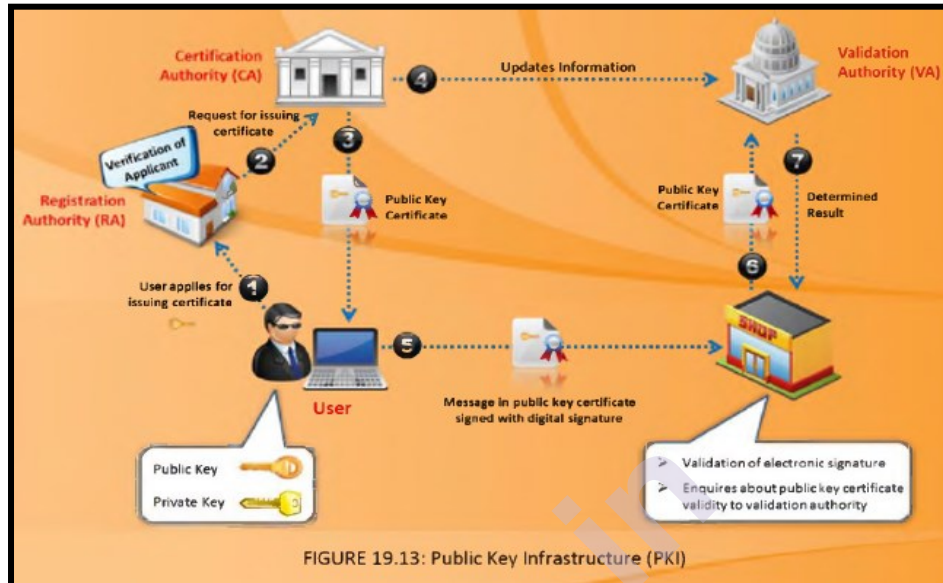


Fig. 13.12: Public Key Infrastructure (PKI)

13.9 CERTIFYING AUTHORITIES AND ITS DIFFERENT TYPES

Certification authorities are the entities that issue digital certificates. The following are some of the certificate authorities:

- **Comodo:** It offers a complete range of PKI digital certificates with strong SSL encryption available. It ensures standards of confidentiality, system reliability, and pertinent business practices as judged through qualified independent audits. The PKI (Public Key Infrastructure) management solutions offered by Comodo include Comodo Certificate Manager and Comodo EPKI Manager.
 - Available Digital Certificates:
 - Extended validation (EV)-SSL
 - Multi-domain EV SSL
 - Wildcard SSL
 - Unified communications (UC)
 - Intel Pro Series
 - General purpose SSL
 - 9 Secure Email - S/MIME

- 9 Client authentication
- 9 Codesigning
- **thwate:** thawte is a Certification Authority , thawte offers SSL and code signing digital certificates to secure servers, provides data encryption, authenticates users, protects privacy, and assures online identifies through stringent authentication and verification processes. The SSL certificates offered by thawte include Wildcard SSL Certificates, SAN /UC Certificates, SGC SuperCerts, and Extended Validation SSL Certificates.
- **Verisign:** VeriSign Authentication Services, now part of Symantec Corp. (NASDAQ:SYMC), provides solutions that allow companies and consumers to engage in communications and commerce online with confidence.

SSL Certificates:

- Secure Site Pro with EV
- Secure Site with EV
- Secure Site Pro
- Secure Site
- Managed PKI for SSL
- SSL for the Enterprise
- SSL Partner Programs
- Symantec Certificate Intelligence Center
- **Entrust:** - Entrust provides identity-based security solutions that empower enterprises, consumers, citizens, and the web. Entrust solutions include strong authentication, fraud detection, digital certificates, SSL, and PKI. Entrust can deploy appropriate security solutions to help protect digital identities and information at multiple points to address ever-evolving threats.

13.10 DISK ENCRYPTION

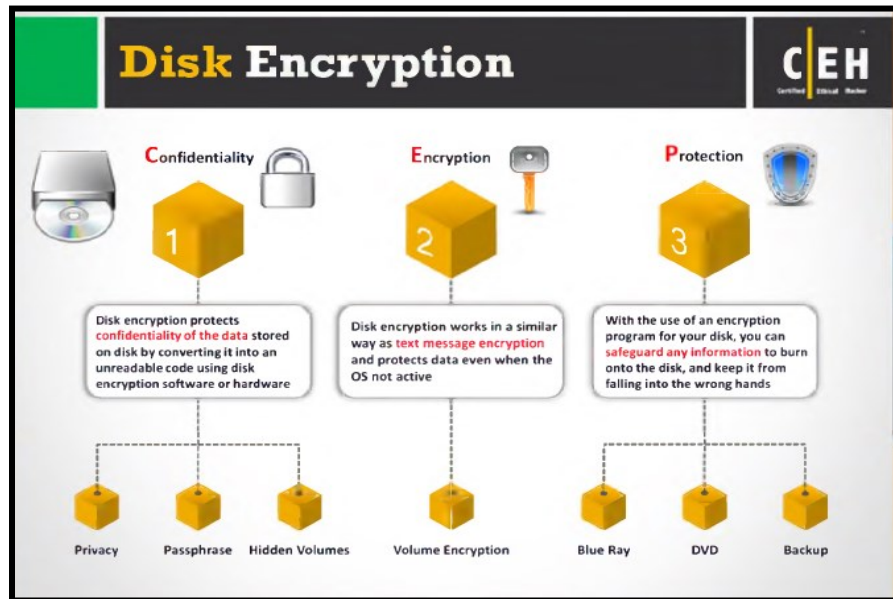


Fig. 13.13: Disk Encryption

Disk Encryption:

- Disk encryption is the process of securing data by transferring it into unreadable code that cannot be deciphered by unauthorized persons. We can use disk encryption software or hardware to encrypt every bit of information that is written on the disk.
- Disk encryption works similar to text message encryption. With the use of an encryption program for the user's disk, the user can safeguard any, and all, information burned onto the disk and save it from falling into wrong hands.
- A computer disk is a round plate onto which data is recorded and/or burned. If the user needs to store information on a disk, and keep it safe, it is recommended that an encryption program be used.
- Encryption software, for disks, scrambles the information burned on the disk into an illegible code. It is only after the disk information is decrypted, that it can be read and/or used.
- Encryption for disks is useful when the user needs to send sensitive information through the mail. For instance, the user needs to mail his or her friend a disk, but cannot take the risk of it being stolen and the information is being compromised.
- In this case, the user could simply encrypt the information on the disk and then rest assured, even if the disk is lost or stolen, the information on it would not be compromised.
- In addition, disk encryption can also be useful in protecting the real-time exchange of information from being compromised. When the exchange of information is made in an encrypted form, the chances of the information being compromised are minimized.

- The only way the attacker can access the information is by decrypting the message, which can only be done via the authentication process.
- Furthermore, the encryption software installed on one's system ensures the security of the system. Thus, it is recommended to install encryption software on systems that hold valuable information and/or are exposed to unlimited data transfer in order to protect the data and information from compromise.

13.11 CODE BREAKING TECHNIQUES

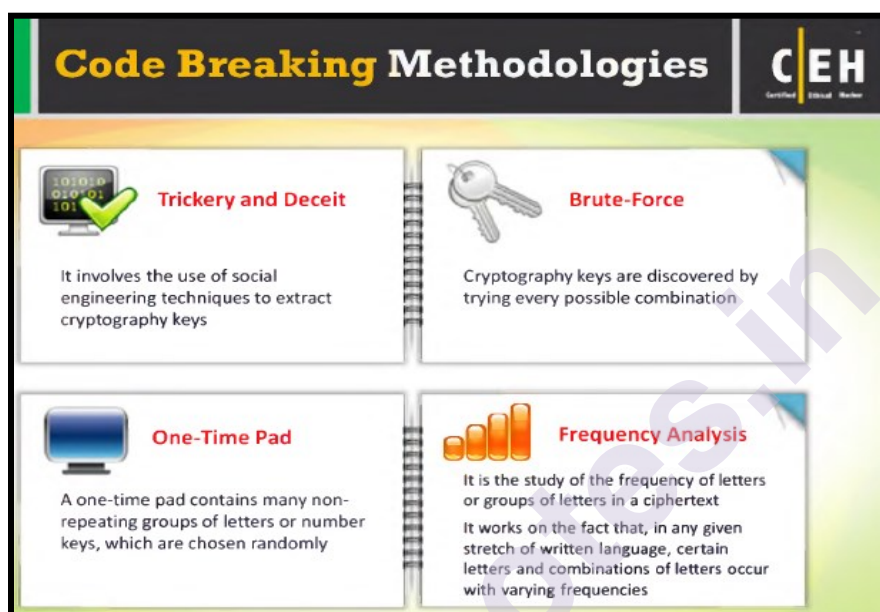


Fig. 13.14: Code Breaking Methodologies

Code Breaking Methodologies: - The strength of an encryption algorithm is measured, in large part by cryptanalysts, by using various code breaking techniques. The various code-breaking techniques that are available are:

- Brute-Force
- Frequency Analysis
- Trickery and Deceit
- One-Time Pad
- **Brute-Force:**
 - Code-breakers, or cryptanalysts, want to recover the plain text of a message without knowing the required key in advance. They may first try to recover the key, or go after the message itself.
 - One of the familiar ways of the cryptanalytic technique is brute-force attack or an exhaustive search, (where the keys are guessed by trying every possible combination).

- The efficiency of the brute-force depends on the hardware configuration. Usage of faster processors means testing more keys per second.
- Michael Weiner, put forth a brute-force attack on the DES with the help of specially designed computers with crypto graphers sounding the old standard's death knell.
- Moreover, the combination of advanced factoring and the faster computers used in the recent attacks on RSA-129, makes algorithms appear weak. The NSA that has top computing power is the center of the brute-force attack.
- **Frequency Analysis:-**
 - Frequency analysis of the letters makes the brute-force method not a suitable method for attacking the cipher.
 - For example the letter "e" is the common word in the English language and the letter "k" appears commonly in the cipher text, it can be concluded reasonably that k=e, and so on. Encrypted source codes are more exposed to the attacks because few words like "# define," "Struct," "else," "and" "return" are repeated frequently.
 - Frequency analysis was first used by papal courts in the Middle Age, which built frequency tables for Latin and Italian words. Sophisticated crypto systems are required to maintain the security of the messages.
- **Trickery and Deceit:-**
 - There has always been a need for a high level of mathematical and crypto graphic skills, but trickery and deceit have a long history in code-breaking as well the value of the encrypted data must be below the cost entitled to break the algorithm.
 - In the modern world, computers are faster and cheaper, therefore it would be better to check the limits of these two parameters.
- **One-time Pad:-**
 - It is considered that any cipher can be cracked if sufficient time and resources are provided. But there is an exception called a one-time pad, which is considered to be unbreakable even after infinite resources are provided.
 - A one-time pad contains many non-repeating groups of letters or number keys, which are chosen randomly. These are then pasted together on a pad. Bob encrypts only one plain text character with the pad and Alice decrypts each and every character of the cipher text with the help of the same key characters from an identical pad.

- After the use, the characters are securely removed from the pad. The major drawback of the one-time padding is the length of the pads.
- The length of key is same as the length of the message, which makes it impossible to encrypt and send large messages.
- The Soviet spies commonly used one-time pads during the Cold War. The agent carried the encrypted message to the field, leaving the identical pad at the headquarters.
- The well-known, one-time padding was used on the communication lines between Moscow and Washington.

13.12 SUMMARY

- Cryptography is the study of encryption and encryption algorithms. The four main **objectives of cryptography** are Confidentiality, Integrity, Authentication and Nonrepudiation.
- Understand the two types of encryption. **Symmetric key and asymmetric key encryption** are the two main types of encryption.
- Understand the methods used to scramble data during encryption. Substitution and transposition methods are the basis of encryption and are used to scramble data during the encryption process.
- Know the common encryption algorithms. MD5, SHA, RC4, RC5, and Blowfish are the most common encryption algorithms.
- Know how public and private keys are created. A public key and a private key are created simultaneously as a key pair and are used to encrypt and decrypt data. Data encrypted with one member of the key pair can only be decrypted by the other.
- Understanding two types of cryptography i.e. **symmetric encryption (secret key cryptography)** and **Asymmetric encryption (public key cryptography)**.
- Cryptographic attacks are the means by which the attacker decrypts the cipher text (breaks the cipher text) without the knowledge of the key.
- Attackers have found various attacks for defeating the crypto system and they are categorized in to eight types: Cipher text only attack, Known-plain text attack, Chosen-plaintext, Chosen-cipher text attack, Chosen key attack, Adaptive chosen-plain text attack, Timing attack and Rubber hose attack.
- **Ciphers and their classification:** Classical ciphers, Substitution cipher, Transposition cipher and Modern ciphers.
- DES is the name of the Federal information Processing Standard (FIPS) 46-3 that describes the data encryption algorithm (DEA).

- The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data.
- A digital signature is a mathematical scheme used for the authentication of a digital message and knowing various benefits of it.
- A digital signature is a cryptographic means of authentication.
- Public Key Infrastructure (PKI) is a security architecture developed to increase the confidentiality of information being exchanged over the insecure Internet.
- Certification authorities are the entities that issue digital certificates. The following are some of the certificate authorities: **Comodo, thwate, Verisign and Entrust.**
- Disk encryption is the process of securing data by transferring it into unreadable code that cannot be deciphered by unauthorized persons.
- **Code Breaking Methodologies:** - The strength of an encryption algorithm is measured, in large part by cryptanalysts, by using various code breaking techniques. The various code-breaking techniques that are available are: **Brute-Force, Frequency Analysis, Trickery and Deceit and One-Time Pad.**

13.13 UNIT END EXERCISE

1. Define and explain Cryptography and encryption techniques.
2. Explain the formation of Public and Private Keys.
3. Explain MD5, SHA, RC4, RC5, and Blowfish Algorithms in detail.
4. Explain different types of Cryptography.
5. What is Cryptography attacks? Also explain its various Categories in detail.
6. What are ciphers? How are they classified?
7. Explain data encryption standard and advanced encryption standard.
8. Explain digital signature algorithm and related signature schemes.
9. What are digital signatures? How do they work?
10. What is public key infrastructure? Explain in detail.
11. Who are certifying authorities? List three certifying authorities with the types of certificates they provide.
12. What is disk encryption? What is its use?
13. What are the different code breaking techniques? Explain.

13.14 REFERENCES

- Matt Walker, All-In-One-CEH-Certified-Ethical-Hacker-Exam-Guide.
- Tutorials Point Professionals, Ethical Hacking by Tutorials Point.

13.15 BIBLIOGRAPHY

- Kimberly Graves (26th-April-2010), "CEH Certified Ethical Hacker Study Guide" 1st Edition, ISBN-13: 978-0470525203, ISBN-10: 0470525207, Sybex- Wiley Publishing.
- Sean-Philip Oriyano, Sybex, Certified Ethical Hacker Study Guide v9, Study Guide Edition, 2016.

munotes.in

PEN TESTING

Unit Structure

14.0 Objectives

14.1 What is Pen testing?

14.1.1 Defining Security Assessments

14.1.2 Overview of Penetration Testing Methodologies

14.2 Why is Penetration Testing Required?

14.2.1 When to Perform Penetration Testing?

14.2.2 How is Penetration Testing Beneficial?

14.3 Types of Penetration Testing

14.4 Penetration Testing – Method

14.4.1 Steps of Penetration Testing Method

14.4.2 Areas of Penetration Testing

14.5 Overview of the Pen-Test Legal Framework

14.6 Automated Penetration Testing Tools

14.6.1 Overview of the Pen-Test Deliverables

14.7 Penetration Testing – Testers

14.7.1 Qualification of Penetration Testers

14.7.2 Certification

14.7.3 Past Experience

14.7.4 Role of a Penetration Tester

14.8 Penetration Testing - Report Writing

14.8.1 Report Writing Stages

14.8.2 Content of Penetration Testing Report

14.9 Summary

14.10 Unit End Exercise

14.11 References

14.12 Bibliography

14.0 OBJECTIVES

After this chapter, student will be able to:

- Define Pen testing & Security Assessment
- State various Penetration Testing Methodologies
- Understand the need of Penetration Testing
- Identify various Penetration testing types.
- Describe various benefits of Penetration testing
- Identify various areas of Penetration testing and also when to perform it
- State and understand various Steps or Phases of Penetration testing.
- Identify and understand various automated Penetration testing tools.
- State and identify legal framework and test deliverables of Pen-test.
- Understand the report writing stages of penetration test.
- Know the contents for writing penetration test report.

14.1 WHAT IS PEN TESTING?

- Pen Testing is also known as Penetration testing.
- It is a type of Security testing used to cover vulnerabilities, threats and risks that an attacker could exploit in software applications, networks or web applications and also used to test the insecurity of an application.
- It is conducted to find the security risk which might be present in the system.
- If a system is not secured, then any attacker can disrupt or take authorized access to that system.
- Security risk is normally an accidental error that occurs while developing and implementing the software. For example, configuration errors, design errors, and software bugs, etc.
- A penetration test simulates methods that intruders use to gain unauthorized access to an organization's network and systems and to compromise them.
- The purpose of a penetration test is to identify and test all possible security vulnerabilities that are present in the software application and also to test the security implementations and security policy of an

organization: basically to see if the organization has implemented security measures as specified in the security policy.

- A hacker whose intent is to gain unauthorized access to an organization's network is very different from a professional penetration tester who lacks malice and intent and uses their skills to improve an organization's network security without causing a loss of service or a disruption to the business.
- Penetration testing can also cause problems such as system malfunctioning, system crashing, or data loss. Therefore, a company should take calculated risks before going ahead with penetration testing. The risk is calculated as follows and it is a management risk.

$$\text{RISK} = \text{Threat} \times \text{Vulnerability}$$

- Penetration testing is conducted by professional ethical hackers who mainly use commercial, open-source tools, automate tools and manual checks. There are no restrictions; the most important objective here is to uncover as many security flaws as possible.
- **Example**

Suppose we have an online e-commerce website that is in production. We want to do a penetration testing before making it live. Here, we have to weigh the pros and cons first. If we go ahead with penetration testing, it might cause interruption of service. On the contrary, if we do not wish to perform a penetration testing, then we can run the risk of having an unpatched vulnerability that will remain as a threat all the time.

Before doing a penetration test, it is recommended that we put down the scope of the project in writing. We should be clear about what is going to be tested. **For example –**

- Our company has a VPN or any other remote access techniques and we want to test that particular point.
- Our application has web servers with databases, so we might want to get it tested for SQL injection attacks which is one of the most crucial tests on a web server. In addition, we can check if our web server is immune to DoS attacks.

14.1.1 Defining Security Assessments

- A penetration tester assesses the security posture of the organization as a whole to reveal the potential consequences of a real attacker compromising a network or application. Security assessments can be categorized as security audits, vulnerability assessments, or penetration testing. Each security assessment requires that the people conducting the assessment have different skills based on the scope of the assessment.

- A security audit and a vulnerability assessment scan IP networks and hosts for known security weaknesses with tools designed to locate live systems, enumerate users, and identify operating systems and applications, looking for common security configuration mistakes and vulnerabilities.
- A vulnerability or security assessment only identifies the potential vulnerabilities while a pen test actually tries to gain access to the network.
- **An example** of a security assessment is looking at a door and thinking if that door is unlocked it could allow someone to gain unauthorized access, whereas a pen test actually tries to open the door to see where it leads. A pen test is usually a better indication of the weaknesses of the network or systems but is more invasive and therefore had more potential to cause disruption to network service.

14.1.2 Overview of Penetration Testing Methodologies:

- There are two types of security assessments: **external and internal assessments**. An external assessment tests and analyses publicly available information, conducts network scanning and enumeration, and runs exploits from outside the network perimeter, usually via the Internet. An internal assessment is performed on the network from within the organization, with the tester acting either as an employee with some access to the network or as a black hat with no knowledge of the environment.
- A black-hat penetration test usually involves a higher risk of encountering unexpected problems. The team is advised to make contingency plans in order to effectively utilize time and resources.
- We can outsource our penetration test if we don't have qualified or experienced testers or if we're required to perform a specific assessment to meet audit requirements such as the Health Insurance Portability and Accountability Act (HIPAA).
- An organization employing an assessment term must specify the scope of the assessment, including what is to be tested and what is not to be tested.
- **For example**, a pen test may be a targeted test limited to the first 10 systems in a Demilitarized Zone (DMZ) or a comprehensive assessment uncovering as many vulnerabilities as possible. In the scope of work, a service-level agreement (SLA) should be defined to determine any actions that will be taken in the event of a serious service disruption.
- Other terms for engaging an assessment team can specify a desired code of conduct, the procedures to be followed, and the interaction or lack of interaction between the organization and the testing team.

- A security assessment or pen test can be performed manually with several different tools, usually freeware or shareware. A different approach is to use a more expensive auto-mated tool.
- Assessing the security posture of our organization using a manual test is sometimes a better option than just using an automated tool based on a standard template.
- The company can benefit from the expertise of an experienced professional who analyzes the information. While the automated approach may be faster and easier, something may be missed during the audit.
- However, a manual approach requires planning, scheduling, and diligent documentation.

14.2 WHY IS PENETRATION TESTING REQUIRED?

Penetration testing normally evaluates a system's ability to protect its networks, applications, endpoints and users from external or internal threats. It also attempts to protect the security controls and ensures only authorized access.

Penetration testing is essential because –

- It identifies a simulation environment i.e., how an intruder may attack the system through white hat attack.
- It helps to find weak areas where an intruder can attack to gain access to the computer's features and data.
- It supports to avoid black hat attack and protects the original data.
- It estimates the magnitude of the attack on potential business.
- It provides evidence to suggest, why it is important to increase investments in security aspect of technology.

14.2.1 When to Perform Penetration Testing?

Penetration testing is an essential feature that needs to be performed regularly for securing the functioning of a system. In addition to this, it should be performed whenever –

- Security system discovers new threats by attackers.
- Adding a new network infrastructure.
- Updating our system or installing new software.
- Relocating our office.
- For set up a new end-user program/policy.

14.2.2 How is Penetration Testing Beneficial?

Penetration testing offers the following benefits –

- **Enhancement of the Management System** – It provides detailed information about the security threats. In addition to this, it also categorizes the degree of vulnerabilities and suggests us, which one is more vulnerable and which one is less. So, we can easily and accurately manage our security system by allocating the security resources accordingly.
- **Avoid Fines** – Penetration testing keeps our organization's major activities updated and complies with the auditing system. So, penetration testing protects us from giving fines.
- **Protection from Financial Damage** – A simple breach of security system may cause millions of dollars of damage. Penetration testing can protect our organization from such damages.
- **Customer Protection** – Breach of even a single customer's data may cause big financial damage as well as reputation damage. It protects the organizations who deal with the customers and keep their data intact.

14.3 TYPES OF PENETRATION TESTING

We have five types of penetration testing –

- **Black Box:-** Here, the ethical hacker doesn't have any information regarding the infrastructure or the network of the organization that he is trying to penetrate. In black-box penetration testing, the hacker tries to find the information by his own means.
- **Grey Box:-** It is a type of penetration testing where the ethical hacker has a partial knowledge of the infrastructure, like its domain name server.
- **White Box:-** In white-box penetration testing, the ethical hacker is provided with all the necessary information about the infrastructure and the network of the organization that he needs to penetrate.
- **External Penetration Testing:** - This type of penetration testing mainly focuses on network infrastructure or servers and their software operating under the infrastructure. In this case, the ethical hacker tries the attack using public networks through the Internet. The hacker attempts to hack the company infrastructure by attacking their webpages, web servers, public DNS servers, etc.
- **Internal Penetration Testing:** - In this type of penetration testing, the ethical hacker is inside the network of the company and conducts his tests from there.

These main types of penetration testing methods can be further subdivided into specific categories. Other types of penetration tests include:

- **Social engineering tests:** The pen test scenario tries to get an employee or third party to reveal sensitive information, such as a password, business data, or other user data. This can be done through targeting help desks or sales representatives through the phone or internet.
- **Web application tests:** The pen test uses software to assess the security vulnerability of web apps and software programs.
- **Physical penetration tests:** Mostly used in government sites or other secure facilities, the pen test tries to access physical network devices and access points in a mock security breach.
- **Network services test:** This is the most common pen test scenario, in which a user tries to either locally or remotely identify openings in the network.
- **Client-side test:** This is when an MSP tries to exploit vulnerabilities in client-side software programs.
- **Wireless security test:** The pen test identifies open, unauthorized, or low-security hotspots and Wi-Fi networks and tries to infiltrate through them.

All types of penetration testing should consider both internal and external components of an IT infrastructure. There are different phases of a penetration test that will ensure a holistic and regularly updated approach to an organization's cyber security.

14.4 PENETRATION TESTING – METHOD

Penetration testing is a combination of techniques that considers various issues of the systems and tests, analyzes, and gives solutions. It is based on a structured procedure that performs penetration testing step-by-step.

This chapter describes various steps or phases of penetration testing method.

14.4.1 Steps of Penetration Testing Method

The following are the seven steps or phases of penetration testing –

Note: - Penetration testing includes three phases: - **Pre-attack phase, Attack phase and Post-attack phase.** All these three phases or steps are carried out with the help of seven different activities that are as follows.

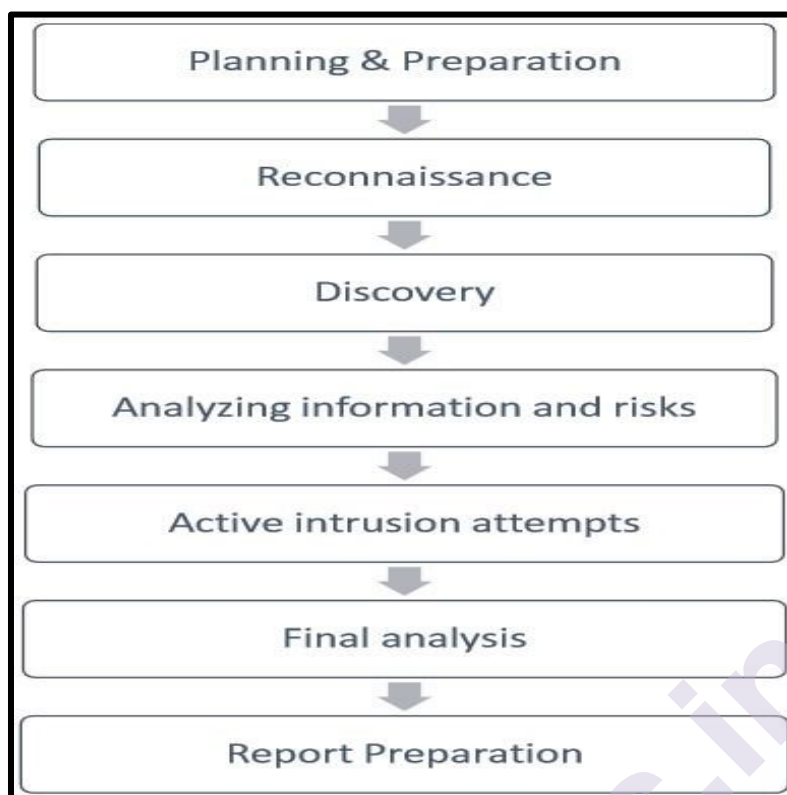


Fig. 14.1: Phases/Steps of Penetration testing

- **Planning & Preparation**
 - Planning and preparation starts with defining the goals and objectives of the penetration testing.
 - The client and the tester jointly define the goals so that both the parties have the same objectives and understanding. The common **objectives of penetration testing** are –
 - To identify the vulnerability and improve the security of the technical systems.
 - Have IT security confirmed by an external third party.
 - Increase the security of the organizational/personnel infrastructure.
- **Reconnaissance**
 - Reconnaissance includes an analysis of the preliminary information. Many times, a tester doesn't have much information other than the preliminary information, i.e., an IP address or IP address block.
 - The tester starts by analyzing the available information and, if required, requests for more information such as system descriptions, network plans, etc. from the client. This step is the passive penetration test, a sort of. The sole objective is to obtain a complete and detailed information of the systems.

- **Discovery**
 - In this step, a penetration tester will most likely use the automated tools to scan target assets for discovering vulnerabilities.
 - These tools normally have their own databases giving the details of the latest vulnerabilities. However, tester discover:-
 - **Network Discovery** – Such as discovery of additional systems, servers, and other devices.
 - **Host Discovery** – It determines open ports on these devices.
 - **Service Interrogation** – It interrogates ports to discover actual services which are running on them.
- **Analyzing Information and Risks**
 - In this step, tester analyzes and assesses the information gathered before the test steps for dynamically penetrating the system. Because of larger number of systems and size of infrastructure, it is extremely time consuming. While analyzing, the tester considers the following elements –
 - The defined goals of the penetration test.
 - The potential risks to the system.
 - The estimated time required for evaluating potential security flaws for the subsequent active penetration testing.
 - However, from the list of identified systems, the tester may choose to test only those which contain potential vulnerabilities.
- **Active Intrusion Attempts**
 - This is the most important step that has to be performed with due care.
 - This step entails the extent to which the potential vulnerabilities that was identified in the discovery step which possess the actual risks.
 - This step must be performed when a verification of potential vulnerabilities is needed.
 - For those systems having very high integrity requirements, the potential vulnerability and risk needs to be carefully considered before conducting critical clean up procedures.
- **Final Analysis**
 - This step primarily considers all the steps conducted (discussed above) till that time and an evaluation of the vulnerabilities present in the form of potential risks.

- Further, the tester recommends to eliminate the vulnerabilities and risks. Above all, the tester must assure the transparency of the tests and the vulnerabilities that it disclosed.
- **Report Preparation**
 - Report preparation must start with overall testing procedures, followed by an analysis of vulnerabilities and risks.
 - The high risks and critical vulnerabilities must have priorities and then followed by the lower order. However, while documenting the final report, the following points needs to be considered –
 - Overall summary of penetration testing.
 - Details of each step and the information gathered during the pen testing.
 - Details of all the vulnerabilities and risks discovered.
 - Details of cleaning and fixing the systems.
 - Suggestions for future security.

14.4.2 Areas of Penetration Testing

Penetration testing is normally done in the following three areas –

- **Network Penetration Testing:-** In this testing, the physical structure of a system needs to be tested to identify the vulnerability and risk which ensures the security in a network. In the networking environment, a tester identifies security flaws in design, implementation, or operation of the respective company/organization's network. The devices, which are tested by a tester can be computers, modems, or even remote access devices, etc.
- **Application Penetration Testing:-** In this testing, the logical structure of the system needs to be tested. It is an attack simulation designed to expose the efficiency of an application's security controls by identifying vulnerability and risk. The firewall and other monitoring systems are used to protect the security system, but sometime, it needs focused testing especially when traffic is allowed to pass through the firewall.
- **The response or workflow of the system:-** This is the third area that needs to be tested. Social engineering gathers information on human interaction to obtain information about an organization and its computers. It is beneficial to test the ability of the respective organization to prevent unauthorized access to its information systems. Likewise, this test is exclusively designed for the workflow of the organization/company.

14.5 OVERVIEW OF THE PEN-TEST LEGAL FRAMEWORK

A penetration tester must be aware of the legal ramifications of hacking a network, even in an ethical manner. The documents that an ethical hacker performing a penetration test must have signed with the client are as follows:

- Scope of work, to identify what is to be tested
- Nondisclosure agreement, in case the tester sees confidential information
- Liability release, releasing the ethical hacker from any actions or disruption of service caused by the pen test.

14.6 AUTOMATED PENETRATION TESTING TOOLS

A 2006 survey of the hacker's mailing list created a top-10 list of vulnerability scanning tools; more than 3,000 people responded. Fyodor (<http://insecure.org/fyodor/>), which created the list, says, "Anyone in the security field would be well advised to go over the list and investigate tools they are unfamiliar with." The following should be considered the top pen testing tools in a hacker's toolkit:

- **Nessus:-** This freeware network vulnerability scanner has more than 11,000 plug-ins available. It includes remote and local security checks, a client/server architecture with a GTK graphical interface, and an embedded scripting language for writing your own plug-ins or understanding the existing ones.
- **GFI LANguard:-** This is a commercial network security scanner for Windows. It scans IP networks to detect what machines are running. It can determine the host operating system, what applications are running, what Windows service packs are installed, whether any security patches are missing, and more.
- **Retina:-** This is a commercial vulnerability assessment scanner by eEye. Like Nessus, Retina scans all the hosts on a network and reports on any vulnerabilities found.
- **CORE IMPACT:-** It is an automated pen testing product that is widely considered to be the most powerful exploitation tool available (it's also very costly). It has a large, regularly updated database of professional exploits. Among its features, it can exploit one machine and then establish an encrypted tunnel through that machine to reach and exploit other machines.
- **ISS Internet Scanner:-** This is an application-level vulnerability assessment. Internet Scanner can identify more than 1,300 types of

networked devices on your network, including desktops, servers, routers/switches, firewalls, security devices, and application routers.

- **X-Scan:** - It is a general multithreaded plug-in-supported network vulnerability scanner. It can detect service types, remote operating system types and versions, and weak usernames and passwords.
- **SARA Security Auditor's Research Assistant (SARA):-** is a vulnerability assessment tool derived from the System Administrator Tool for Analyzing Networks (SATAN) scanner. Updates are typically released twice a month.
- **QualysGuard:-** This is a web-based vulnerability scanner. Users can securely access Qualys-Guard through an easy-to-use web interface. It features more than 5,000 vulnerability checks, as well as an inference-based scanning engine.
- **SAINT Security Administrator's Integrated Network Tool (SAINT):-** It is a commercial vulnerability assessment tool.
- **MBSA Microsoft Baseline Security Analyzer (MBSA):-** It is built on the Windows Update Agent and Microsoft Update infrastructure. It ensures consistency with other Microsoft products and, on average, scans more than 3 million computers each week.

In addition to this list, we should be familiar with the following vulnerability exploitation tools:

- **Metasploit Framework:** - This is an open-source software product used to develop, test, and use exploit code.
- **Canvas:** - It is a commercial vulnerability exploitation tool. It includes more than 150 exploits.

14.6.1 Overview of the Pen-Test Deliverables

The main deliverable at the end of a penetration test is the pen testing report. The report should include the following:

- List of our findings, in order of highest risk Analysis of our findings.
- Conclusion or explanation of our findings Remediation measures for our findings.
- Log files from tools that provide supporting evidence of our findings.
- Executive summary of the organization's security posture.
- Name of the tester and the date testing occurred.
- Any positive findings or good security implementations

14.7 PENETRATION TESTING – TESTERS

There is the issue of protecting the most critical data of the organization; therefore, the role of a penetration tester is much critical, a minor error can put both the parties (tester and his client) on risk.

Therefore, this chapter discusses various aspects of a penetration tester including his qualification, experience, and responsibilities.

14.7.1 Qualification of Penetration Testers

- This test can be performed only by a qualified penetration tester; therefore, qualification of a penetration tester is very important.
- Either qualified internal expert or a qualified external expert may perform the penetration test until they are organizationally independent.
- It means that the penetration tester must be organizationally independent from the management of the target systems.
- For example, if a third-party company is involved in the installation, maintenance, or support of target systems, then that party cannot perform penetration testing.

Here are some guidelines that will help us while calling a penetration tester.

14.7.2 Certification

A certified person can perform penetration testing. Certification held by the tester is the indication of his skill sets and competence of capable penetration tester.

Following are the important examples of penetration testing certification –

- Certified Ethical Hacker (CEH).
- Offensive Security Certified Professional (OSCP).
- CREST Penetration Testing Certifications.
- Communication Electronic Security Group (CESG) IT Health Check Service certification.
- Global Information Assurance Certification (GIAC) Certifications for example, GIAC Certified Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), Advance Penetration Tester (GXPN), and GIAC Exploit Researcher.

14.7.3 Past Experience

The following questions will help us to hire an effective penetration tester

—

- How many years of experience does the penetration tester has?
- Is he an independent penetration tester or working for an organization?
- With how many companies he worked as penetration tester?
- Has he performed penetration testing for any organization, which has similar size and scope as yours?
- What type of experience does the penetration tester has? For example, conducting network-layer penetration testing etc.
- We may also ask for the reference from other customers for whom he worked.

When hiring a penetration tester, it is important to evaluate the past year testing experience of the organization for which he (tester) has worked as it is related to the technologies specifically deployed by him within the target environment.

In addition to the above, for complex situations and typical client requirements, it is recommended to evaluate a tester's capability to handle similar environment in his/her earlier project.

14.7.4 Role of a Penetration Tester

A penetration tester has the following roles –

- Identify inefficient allocation of tools and technology.
- Testing across internal security systems.
- Pinpoint exposures to protect the most critical data.
- Discover invaluable knowledge of vulnerabilities and risks throughout the infrastructure.
- Reporting and prioritizing remediation recommendations to ensure that the security team is utilizing their time in the most effective way, while protecting the biggest security gaps.

14.8 PENETRATION TESTING - REPORT WRITING

It is not necessary that an experienced penetration tester can write a good report, as writing report of penetration testing is an art that needs to be learnt separately.

- **What is Report Writing?**

In penetration testing, report writing is a comprehensive task that includes methodology, procedures, proper explanation of report content and design, detailed example of testing report, and tester's personal experience. Once the report is prepared, it is shared among the senior management staff and technical team of target

organizations. If any such kind of need arises in future, this report is used as the reference.

14.8.1 Report Writing Stages:-

Due to the comprehensive writing work involved, penetration report writing is classified into the following stages –

- Report Planning
- Information Collection
- Writing the First Draft
- Review and Finalization

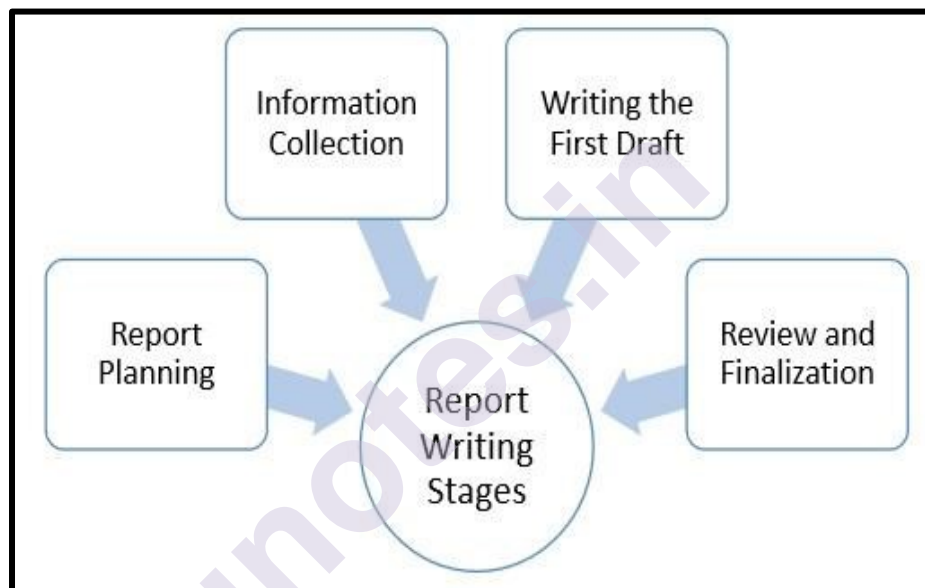


Fig. 14.2: Report Writing Stages of Penetration testing

- **Report Planning**

Report planning starts with the objectives, which help readers to understand the main points of the penetration testing. This part describes why the testing is conducted, what the benefits of pen are testing, etc. Secondly, report planning also includes the time taken for the testing.

Major elements of report writing are –

- **Objectives** – It describes the overall purpose and benefits of pen testing.
- **Time** – Inclusion of time is very important, as it gives the accurate status of the system. Suppose, if anything wrong happens later, this report will save the tester, as the report will illustrate the risks and vulnerabilities in the penetration testing scope during the specific period of time.

- **Target Audience** – Pen testing report also needs to include target audience, such as information security manager, information technology manager, chief information security officer, and technical team.
- **Report Classification** – Since, it is highly confidential which carry server IP addresses, application information, vulnerability, threats, it needs to be classified properly. However, this classification needs to be done on the basis of target organization which has an information classification policy.
- **Report Distribution** – Number of copies and report distribution should be mentioned in the scope of work. It also needs to mention that the hardcopies can be controlled by printing a limited number of copies attached with its number and the receiver's name.

- **Information Collection:-**

Because of the complicated and lengthy processes, pen tester is required to mention every step to make sure that he collected all the information in all the stages of testing. Along with the methods, he also needs to mention about the systems and tools, scanning results, vulnerability assessments, details of his findings, etc.

- **Writing the First Draft:-**

Once, the tester is ready with all tools and information, now he needs to start the first draft. Primarily, he needs to write the first draft in the details – mentioning everything i.e. all activities, processes, and experiences.

- **Review and Finalization:-**

Once the report is drafted, it has to be reviewed first by the drafter himself and then by his seniors or colleagues who may have assisted him. While reviewing, reviewer is expected to check every detail of the report and find any flaw that needs to be corrected.

14.8.2 Content of Penetration Testing Report:-

Following is the typical content of a penetration testing report –

Executive Summary

- Scope of work
- Project objectives
- Assumption
- Timeline
- Summary of findings
- Summary of recommendation

Methodology

- Planning
- Exploitation
- Reporting

Detail Findings

- Detailed systems information
- Windows server information

References

- Appendix

14.9 SUMMARY

- Penetration testing is a type of security testing that is used to test the insecurity of an application.
- Know the definition of a security assessment. A security assessment is a test that uses hacking tools to determine an organization's security posture.
- **Know the two types of security assessments.** Security assessments can be performed either internally or externally.
- Penetration testing offers the following benefits –**Enhancement of the Management System, Avoid Fines, and Protection from Financial Damage & Customer Protection.**
- The five types of penetration testing are **Black Box, Grey Box, White Box, External Penetration Testing and Internal Penetration Testing.**
- Main types of penetration testing methods can be further subdivided into specific categories. Other types of penetration tests include: **Social engineering tests, Web application tests, Physical penetration tests, Network services test, Client-side test & Wireless security test.**
- List the penetration testing steps : **Pre-attack, attack, and post-attack are the three phases of pen testing** performed with the help of seven different activities that are **Planning & Preparation, Reconnaissance, Discovery, Analyzing Information and Risks, Active Intrusion Attempts, Final Analysis & Report Preparation**
- Penetration testing is normally done in the following three areas:- **Network Penetration Testing, Application Penetration Testing and the response or workflow of the system.**

- Automated Penetration Testing Tools are **Nessus, GFI LANguard, Retina, CORE IMPACT, ISS Internet Scanner, X-Scans, SARA Security Auditor's Research Assistant (SARA), QualysGuard, SAINT Security Administrator's Integrated Network Tool (SAINT) and MBSA Microsoft Baseline Security Analyzer (MBSA)**
- Various vulnerability exploitation tools are **Metasploit Framework and Canvas**
- **Know pen testing deliverables.** A pen testing report of the findings of the penetration test should include suggestions to improve security, positive findings, and log files.
- **Know the legal requirements of a pen test.** A pen tester should have the client sign a liability release, a scope of work, and a nondisclosure agreement.
- Penetration tester qualification, certifications, experience, and responsibilities.
- Penetration **report writing Stages** is classified into the following: Report Planning, Information Collection, Writing the First Draft and Review and Finalization.
- Content of Penetration Testing Report are Executive, Executive Summary, Methodology and Detail Findings.

14.10 UNIT END EXERCISE

1. Define and explain Pen-testing.
2. Write a short note on Security Assessment of Pen-test.
3. Explain the outline of Penetration Testing Methodologies.
4. What is the need of Penetration testing? Explain.
5. Explain the benefits of Penetration testing.
6. When to perform Penetration testing? Explain.
7. Explain various Penetration testing types.
8. Explain various phases/steps of Penetration testing method.
9. List and explain any five automated Penetration testing tools.
10. Explain the overview of Pen-Test Legal Framework.
11. List and explain the Areas of Penetration Testing.
12. What is the main deliverable at the end of a penetration testing? And also mention what it includes?

13. What qualifications are required to become penetration tester? Explain.
14. Which certifications are needed by penetration tester? Explain.
14. Which questions/past experiences will help us to hire an effective penetration tester?
16. Explain various roles of Penetration Tester.
17. Explain Report Writing Stages of Penetration Testing.
18. List and mention the Contents included in Penetration Testing Report.

14.11 REFERENCES

- Matt Walker, All-In-One-CEH-Certified-Ethical-Hacker-Exam-Guide.
- Tutorials Point Professionals, Ethical Hacking by Tutorials Point.

14.12 BIBLIOGRAPHY

- Kimberly Graves(26th-April-2010), "CEH Certified Ethical Hacker Study Guide" 1st Edition, ISBN-13: 978-0470525203, ISBN-10: 0470525207, Sybex- Wiley Publishing.
- Sean-Philip Oriyano, Sybex, Certified Ethical Hacker Study Guide v9, Study Guide Edition, 2016.
