(2½ Hours) **[Total Marks: 75]**

N.B. 1) **All** questions are **compulsory.**
2) **Figures** to the **right** indicate marks.
3) **Illustrations**, in-depth answers and diagrams will be appreciated.
4) **Mixing** of sub-questions is **not allowed.**

Q. 1 Attempt All the Questions **(15M)**

(a) Multiple Choice Questions:

1. The security, functionality, and ease of use triangle illustrates which concept?
   a) As security increases, functionality and ease of use increase.
   b) As security decreases, functionality and ease of use increase.
   c) As security decreases, functionality and ease of use decrease.
   d) Security does not affect functionality and ease of use.

2. What is the next step to be performed after footprinting?
   a) Enumeration b) Scanning
   c) System hacking d) Active information gathering

3. Nslookup can be used to gather information regarding which of the following?
   a) Host names and IP addresses b) Whois information
   c) DNS server locations d) Name server types and operating systems

4. What are the three types of scanning?
   a) Port, network and vulnerability b) Port, network and services
   c) Grey, black and white hat d) Server, client and network

5. Which of the following attacks can be perpetrated by a hacker against an organization with weak physical security controls?
   a) Denial of service b) Radio frequency jamming
   c) Hardware keylogger d) Banner grabbing

(b) Fill in the blanks (Use following pool to answer questions)
[**Encryption, active, honeypot, DoS, LAND, passive, hash, packet**]

1. In _____ attack, an attacker finds an active session and takes over the session by using tools that predict the next sequence number used in the TCP session.
2. A _____ attack works by preventing legitimate users from accessing the system.
3. _____ sniffing allows individuals to capture data as transmitted over the network.
4. _____ is the best countermeasure to session hijacking.
5. _____ is a system designed to attract probes, attacks and potential exploits.

(c) Answer in ONE or TWO sentences:

1. Define IPSpoofing
2. What is click Jacking?
3. What is reverse WWW shell?
4. What are the ways in which an IDS is able to detect intrusion attempts?
5. What is a Security log?

Q. 2 Attempt the following (Any THREE) **(15M)**

(a) What is malware? Explain in brief concept of Virus.

(b) What is Information Security? Explain Asset, Risk, Threat, Vulnerability with respect to Information Security.

(c) Explain the following terms:
a. Eavesdropping b. Man-in-the-middle

(d) What is Cookie Theft? Explain its functionality.

(e) Define session Hijacking. Describe the three steps involved in session hijacking.

(f) Explain the term DoS and list the types of DoS attack.

Q. 3 Attempt the following (Any THREE) **(15M)**

(a) Explain Black, Gray and White Box Penetration Testing methods in detail.

(b) Write a short note on Crawling with suitable example.

(c) What is Scanning? List and explain types of scanning performed.

(d) Write a short note on security testing plan.

(e) Explain Cross site request forgery.

(f) Define Threat. Explain iterative process in Threat Modelling.

Q. 4 Attempt the following (Any THREE) **(15M)**

(a) Write a short note on MAC Spoofing.

(b) Compare Windows and Linux operating systems on the basis of following point:
a. Customizable b. Security c. Efficiency

(c) Explain in brief Steganography with respect to hacking.

(d) What is VOIP? Explain in detail any two VOIP vulnerabilities.

(e) Explain in brief the metasploit framework.

(f) Describe the Intrusion detection system.

Q. 5 Attempt the following (Any THREE) **(15M)**

(a) Define Attack and Explain types of attacks.

(b) Define the Term Vulnerability. Explain any two from the following.
a. XSS b. SQL Injection c. Insufficient logging and monitoring

(c) Explain pattern matching to known vulnerability Database

(d) Define the Following:
a. Penetration testing b. Vulnerability Assessment c. NDA
d. d. Packet Sniffing e. Scanning

(e) What is OWASP mobile top 10? Explain any one in detail.