Ethical hacking

1. Footprinting and Reconnaissance

1. **What is footprinting?**
   Gathering information about a target system or network.
2. **What is reconnaissance in hacking?**
   It is the preliminary phase where information is collected about a target.
3. **What is Google Hacking?**
   Using search engines like Google to find vulnerabilities in a target.
4. **What is the use of the "site:" operator in Google Hacking?**
   To find indexed pages of a specific website.
5. **How can archived website information be accessed?**
   Using tools like the Wayback Machine.
6. **What is DNS?**
   Domain Name System, which translates domain names to IP addresses.
7. **How can you trace an email?**
   By analyzing its headers.
8. **What tool can fetch DNS information?**
   Tools like nslookup and dig.
9. **What is the purpose of traceroute?**
   To identify the route packets take to a destination.
10. **What is the goal of footprinting?**
    To gather as much information as possible for later attacks.

---

2. Scanning Networks and Enumeration

11. **What is port scanning?**
    Checking for open ports on a network or device.
12. **What is enumeration?**
    Extracting detailed information, such as usernames and shared resources.
13. **Name a network scanning tool.**
    Nmap.
14. **What is a sniffing tool?**
    A tool that intercepts and monitors network traffic, e.g., Wireshark.
15. **What does IDS stand for?**
    Intrusion Detection System.

16. **What is the purpose of network scanning?**
    To discover active devices and services on a network.
17. **What is a SYN scan?**
    A fast, stealthy type of port scan.
18. **What is ARP?**
    Address Resolution Protocol, which maps IP addresses to MAC addresses.
19. **What is the output of the netstat command?**
    Information about network connections, routing tables, and statistics.
20. **What is the difference between active and passive sniffing?**
    Active sniffing involves injecting traffic, while passive sniffing does not.

---

3. Malware Threats

21. **What is a virus?**
    Malicious code that attaches itself to a program or file and spreads.
22. **What is a worm?**
    A self-replicating malware that spreads without user intervention.
23. **What is a trojan?**
    Malware disguised as legitimate software.
24. **What is password cracking?**
    The process of recovering passwords using tools like John the Ripper.
25. **What is a dictionary attack?**
    Attempting passwords using a predefined list of common passwords.
26. **What is DoS?**
    Denial of Service, where a system is overloaded to make it unavailable.
27. **What is ARP poisoning?**
    Manipulating the ARP cache to intercept network traffic.
28. **What is steganography?**
    Hiding information within other files, like images or audio.
29. **What is the function of the ping command?**
    To test connectivity between devices.
30. **What is the use of the ifconfig command?**
    To configure network interfaces.

---

4. Developing and Implementing Malware

31. **What is a keylogger?**
    Software that records keystrokes on a device.

32. **How does a trojan work?**
    By disguising itself as legitimate software and executing malicious actions.
33. **What language can be used to create a keylogger?**
    Python.
34. **What is a payload in malware?**
    The part of malware that performs the intended malicious action.
35. **What is an antivirus?**
    Software that detects and removes malware.
36. **What is a backdoor?**
    A hidden way to bypass normal authentication.
37. **How can a simple virus be created?**
    By writing a script that replicates itself and spreads.
38. **What is the purpose of a keylogger?**
    To capture sensitive information like passwords.
39. **What is an example of trojan malware?**
    Remote Access Trojans (RATs).
40. **Why is Python popular for malware development?**
    It is simple and has extensive libraries for network and file manipulation.

---

5. Hacking Web Servers and Applications

41. **What is Remote File Inclusion (RFI)?**
    A vulnerability where attackers can include external files in the server.
42. **What is a web server?**
    A system that delivers web pages to clients.
43. **How can attackers disguise themselves as Google Bots?**
    By spoofing the user agent string.
44. **What is the purpose of web server hacking?**
    To gain unauthorized access or disrupt services.
45. **What tool can help identify server vulnerabilities?**
    Nikto.
46. **What is a vulnerability?**
    A weakness in a system that can be exploited.
47. **What is a patch?**
    A software update that fixes vulnerabilities.
48. **What is the HTTP protocol?**
    The protocol used for transmitting web pages.

49. **What is the significance of cookies in web hacking?**
    They store session data, which can be hijacked.

50. **What does SSL/TLS provide?**
    Secure communication over the internet.

---

6. SQL Injection and Session Hijacking

51. **What is SQL injection?**
    An attack where malicious SQL code is inserted into queries.

52. **What is session hijacking?**
    Taking over a user session by stealing session tokens.

53. **How does an attacker execute SQL injection?**
    By inputting malicious code in form fields or URLs.

54. **What is a session token?**
    A unique identifier for a user session.

55. **What tool can test for SQL injection?**
    SQLmap.

56. **What is the purpose of input validation?**
    To prevent attacks like SQL injection.

57. **What is the use of the UNION operator in SQL injection?**
    To combine results from multiple queries.

58. **How can session hijacking be mitigated?**
    By using HTTPS and secure cookies.

59. **What is an example of a vulnerable query?**
    SELECT * FROM users WHERE username = '$user'.

60. **What is the OWASP Top 10?**
    A list of the most critical web application security risks.

---

7. Wireless Network Hacking, Cryptography

61. **What is WPA2?**
    A wireless security protocol.

62. **What is Cryptool?**
    A tool for experimenting with cryptographic algorithms.

63. **What is the Caesar Cipher?**
    A substitution cipher that shifts letters by a fixed number.

64. **What is encryption?**
    Converting data into a secure format.

65. **What is decryption?**
    Converting encrypted data back to its original form.
66. **What is the difference between symmetric and asymmetric encryption?**
    Symmetric uses one key; asymmetric uses a public-private key pair.
67. **What is AES?**
    Advanced Encryption Standard, a secure encryption algorithm.
68. **What is RSA used for?**
    Secure data transmission using public-key cryptography.
69. **What is a hash function?**
    A function that converts data into a fixed-size value.
70. **What is the purpose of wireless network hacking?**
    To test or exploit vulnerabilities in wireless networks.

---

8. Penetration Testing

71. **What is penetration testing?**
    Simulating attacks to find vulnerabilities in a system.
72. **What is Metasploit?**
    A framework for penetration testing.
73. **What is Metasploitable?**
    A vulnerable virtual machine for practicing penetration testing.
74. **What are the stages of penetration testing?**
    Reconnaissance, scanning, exploitation, and reporting.
75. **What is a payload in Metasploit?**
    Code executed after exploiting a vulnerability.
76. **What is the use of a reverse shell?**
    To gain remote access to a compromised machine.
77. **What is an exploit?**
    Code that takes advantage of a vulnerability.
78. **What is post-exploitation?**
    Actions performed after gaining access, like privilege escalation.
79. **What is privilege escalation?**
    Gaining higher-level permissions on a system.
80. **What is the difference between black-box and white-box testing?**
    Black-box has no prior knowledge; white-box has full access.

Practical Questions

81. **How do you use nslookup?**
    To query DNS records for a domain.

82. **What is the command for a TCP SYN scan in Nmap?**
    nmap -sS <target>.

83. **How do you use Wireshark?**
    By capturing and analyzing network packets.

84. **What is the output of the traceroute command?**
    A list of hops between the source and destination.

85. **How do you use SQLmap?**
    By providing

a URL with parameters to check for SQL injection.

86. **What is an example of a dictionary attack tool?**
    Hashcat.

87. **What is ARP poisoning?**
    Redirecting network traffic by spoofing MAC addresses.

88. **What does the netstat -an command do?**
    Displays all active network connections.

89. **How can you prevent session hijacking?**
    Use secure cookies and HTTPS.

90. **What is a common tool used for SQL injection testing?**
    SQLmap.

Self-Learning Topics and Tools

91. **What is the purpose of password hashing?**
    To store passwords securely by transforming them into fixed-length hashes.

92. **What are some examples of encryption algorithms?**
    AES, DES, RSA.

93. **What is a botnet?**
    A network of compromised devices controlled by an attacker.

94. **What is social engineering in hacking?**
    Manipulating people into divulging confidential information.

95. **What is the function of the whois command?**
    To retrieve registration information for a domain.

96. **How does a man-in-the-middle attack work?**
    By intercepting communication between two parties.

97. **What is a backdoor?**
    A method of bypassing normal authentication to gain access to a system.

98. **What is the goal of cryptography?**
    To secure communication and protect data integrity.

99. **How can you detect malware?**
    Using antivirus software or system monitoring tools.

100. **What is ethical hacking?**
    Hacking performed to find and fix security flaws, with permission.

---

9. Social Engineering

101. **What is social engineering?**
    The art of manipulating individuals to reveal confidential information.

102. **What is phishing?**

103. **How can social engineering attacks be prevented?**
    Through awareness, security training, and verifying identity before releasing information.

104. **What is the primary goal of social engineering attacks?**
    To exploit human behavior to gain unauthorized access to systems or information.

Implementation

1. Footprinting/Information Gathering

Footprinting is the process of gathering information about a target system to prepare for further attacks.

- **Step 1**: Use tools like WHOIS, Nslookup, or Shodan to gather information on domain names, IP addresses, and servers.
- **Step 2**: Perform DNS zone transfers to find subdomains and gather additional information about the network.
- **Step 3**: Look at social media, public websites, and other open sources to find information about your target.
- **Step 4**: Generate a report by summarizing the IP ranges, DNS records, and discovered subdomains.

Tools: WHOIS, Nslookup, Google Dorking, Recon-ng, Shodan.

2. Network Scanning and Sniffing

This step involves discovering devices on the network and capturing network traffic.

- **Step 1**: Use tools like Nmap for scanning the network to identify live hosts, open ports, and services.

- **Step 2**: Use Wireshark or tcpdump to capture network traffic and analyze packets for unencrypted data.
- **Step 3**: Identify any weaknesses or vulnerabilities by analyzing the open ports and the services running.
- **Step 4**: Create a report highlighting network devices, services, and any security weaknesses identified.

Tools: Nmap, Wireshark, tcpdump, Netcat.

3. Malware Attacks and Other Cyber Attacks

This involves testing how a system responds to various forms of attacks like viruses, worms, and Trojans.

- **Step 1**: Simulate a malware infection using tools like Metasploit or custom payloads to deliver malicious code.
- **Step 2**: Observe how the malware behaves on the target system, such as spreading through the network or stealing data.
- **Step 3**: Conduct other cyber attacks, such as DoS (Denial of Service) or DDoS (Distributed Denial of Service), using tools like LOIC or Hping.
- **Step 4**: Compile the attack details, system responses, and any breach or damage caused.

Tools: Metasploit, LOIC, Hping, RAT (Remote Access Trojans).

4. Implementation of Keyloggers, Viruses, and Trojans

Keyloggers, viruses, and Trojans are forms of malicious software designed to spy or infect a system.

- **Step 1**: Set up a keylogger tool that captures keystrokes from the target system.
- **Step 2**: Use software like Spybot, Keylogger, or create custom viruses to infect a system and monitor behavior.
- **Step 3**: Trojan horses are used to give remote access to a compromised system.
- **Step 4**: Test the malware's effectiveness and report any captured credentials or data from the infected system.

Tools: Keylogger software, Metasploit for Trojans, Remote Access Trojans (RATs).

5. Web Servers and Web Applications Hacking

This involves finding vulnerabilities in web servers or web applications.

- **Step 1**: Scan web servers for open ports and vulnerabilities using tools like Nikto, Nmap, or Burp Suite.
- **Step 2**: Look for vulnerabilities like Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), or misconfigured permissions.
- **Step 3**: Exploit these vulnerabilities by injecting malicious scripts or exploiting weak server configurations.

- **Step 4**: Record findings, including the specific vulnerabilities and their impact on the application.

Tools: Nikto, Burp Suite, DirBuster, OWASP ZAP.

6. SQL Injection and Session Hijacking

SQL Injection allows attackers to manipulate database queries, and session hijacking lets them steal an active session.

- **Step 1**: For SQL injection, test web applications by injecting SQL queries into input fields to see if you can access the database.
- **Step 2**: Use tools like SQLMap to automate SQL injection testing.
- **Step 3**: For session hijacking, intercept web traffic using Burp Suite or Wireshark to steal session cookies.
- **Step 4**: Report the injection points, vulnerabilities, and potential for exploiting session data.

Tools: SQLMap, Burp Suite, OWASP ZAP, Wireshark.

7. Password Encryption and Decryption (Using Caesar Cipher)

Encryption and decryption help protect sensitive data by transforming it into unreadable formats.

- **Step 1**: Use OpenSSL to encrypt and decrypt passwords using algorithms like AES or DES.
- **Step 2**: Implement the Caesar Cipher (a simple cipher shifting letters) for educational purposes to encrypt and decrypt text.
- **Step 3**: Test different inputs to ensure that encryption and decryption are working as expected.
- **Step 4**: Generate a report on how strong or weak the encryption is and suggest better alternatives if necessary.

Tools: OpenSSL, Cryptography libraries in Python/Java.

8. Using Metasploit and Metasploitable for Penetration Testing

Metasploit is a powerful tool used to test the security of a system through exploitation.

- **Step 1**: Set up Metasploit and the Metasploitable virtual machine (a vulnerable machine designed for penetration testing).
- **Step 2**: Use Metasploit's exploits to target vulnerabilities in Metasploitable.
- **Step 3**: Execute attacks like remote code execution, privilege escalation, and reverse shells.
- **Step 4**: Document the vulnerabilities found and the exploitation process in a detailed report.

Tools: Metasploit, Metasploitable.