Ethical Hacking

1. Question: What is footprinting in ethical hacking?

Answer: Footprinting involves collecting information about a target system, such as domain names, IP addresses, and network infrastructure, to assess vulnerabilities.

2. Question: How can WHOIS databases be useful in reconnaissance?

Answer: WHOIS databases provide details about domain registrations, including owner information, aiding hackers in identifying potential targets and understanding organizational structures.

3. Question: Explain the significance of DNS interrogation in footprinting.

Answer: DNS interrogation reveals domain-related information, aiding hackers in mapping network infrastructure, identifying servers, and understanding the target's online presence.

4. Question: What role does social engineering play in reconnaissance?

Answer: Social engineering involves manipulating individuals to divulge sensitive information. In reconnaissance, it helps gather details about employees, organizational structure, and potential entry points.

5. Question: How does network scanning contribute to footprinting?

Answer: Network scanning involves identifying active devices on a network, their services, and vulnerabilities. In footprinting, it helps hackers create a map of the target environment for further exploitation.

1. Question: What is network scanning in ethical hacking?

Answer: Network scanning involves discovering active devices and services on a network, providing insights into potential vulnerabilities that can be exploited for further assessment.

2. Question: How does enumeration differ from scanning in ethical hacking?

Answer: Enumeration is the process of extracting detailed information about network services and users, going beyond scanning by revealing specific system attributes and configurations.

3. Question: Why is banner grabbing important during enumeration?

Answer: Banner grabbing involves collecting information from service banners, revealing software versions and configurations. This aids in identifying potential vulnerabilities and attack vectors during enumeration.

4. Question: How can sniffing be employed in ethical hacking?

Answer: Sniffing involves intercepting and analyzing network traffic. In ethical hacking, it helps identify vulnerabilities, passwords, and potential security weaknesses through the analysis of data packets.

5. Question: Explain the significance of NetBIOS and SNMP in network enumeration.

Answer: NetBIOS and SNMP are protocols that, if misconfigured, can expose valuable information about network resources. Ethical hackers leverage this during enumeration to identify potential points of exploitation.

1. Question: What is a worm in the context of ethical hacking?

Answer: A worm is a self-replicating malicious program that spreads across networks without user intervention, often causing harm to systems.

2. Question: How does a virus differ from a worm in ethical hacking?

Answer: A virus requires user interaction to spread, typically by attaching itself to files or programs, whereas a worm spreads autonomously across networks.

3. Question: Define a Trojan horse in ethical hacking.

Answer: A Trojan is a deceptive software that appears benign but conceals malicious functionality. It tricks users into unknowingly executing harmful actions on their systems.

4. Question: What is payload in the context of malware?

Answer: The payload is the malicious code or action executed by malware. It can include activities like data theft, system disruption, or unauthorized access.

5. Question: How can ethical hackers defend against malware?

Answer: Ethical hackers employ antivirus software, conduct regular system audits, and educate users to recognize phishing attempts, reducing the risk of malware infections.

1. Question: What is SQL injection in ethical hacking?

Answer: SQL injection is a technique where attackers inject malicious SQL code into input fields to manipulate a web application's database, potentially gaining unauthorized access.

2. Question: How can web developers prevent SQL injection vulnerabilities?

Answer: Developers can use parameterized queries, input validation, and prepared statements to sanitize user inputs and mitigate the risk of SQL injection attacks.

3. Question: Define session hijacking in ethical hacking.

Answer: Session hijacking involves stealing or manipulating a user's session token to gain unauthorized access. This can be done through various means, like session sniffing or session cookie theft.

4. Question: How can secure coding practices mitigate session hijacking risks?

Answer: Developers should use secure transport protocols (HTTPS), implement session timeouts, and store session data securely to prevent or minimize the impact of session hijacking attacks.

5. Question: Why is it crucial for ethical hackers to test for SQL injection and session hijacking vulnerabilities?

Answer: Testing helps identify and address vulnerabilities, ensuring that systems are secure against SQL injection and session hijacking attacks, thus safeguarding sensitive data and user sessions.

1. Question: How does encryption contribute to cloud computing security?

Answer: Encryption secures data in transit and at rest, safeguarding information stored in the cloud from unauthorized access, ensuring confidentiality.

2. Question: What is a key management system in cryptography?

Answer: A key management system handles the generation, distribution, storage, and disposal of cryptographic keys, crucial for maintaining the security of encrypted data.

3. Question: How does multi-factor authentication enhance cloud security?

Answer: Multi-factor authentication adds an extra layer of security by requiring multiple forms of identification, reducing the risk of unauthorized access to cloud services and data.

4. Question: Explain the concept of homomorphic encryption in cloud security.

Answer: Homomorphic encryption allows computation on encrypted data without decrypting it, enabling secure processing of sensitive information in the cloud without exposing the raw data.

5. Question: Why is continuous monitoring essential for cloud security?

Answer: Continuous monitoring ensures real-time detection of security threats and vulnerabilities in cloud environments, allowing prompt response and mitigation to protect sensitive data and services.

1. Question: What is penetration testing (pen testing) in ethical hacking?

Answer: Pen testing is a simulated cyberattack on a system to identify vulnerabilities and assess security measures, helping organizations enhance their defenses.

2. Question: Why is scoping crucial in penetration testing?

Answer: Scoping defines the boundaries and objectives of the test, ensuring ethical hackers focus on specific systems and vulnerabilities without causing unintended disruptions.

3. Question: How does penetration testing differ from vulnerability scanning?

Answer: Penetration testing goes beyond scanning by simulating real-world attacks, attempting to exploit vulnerabilities and assess the impact, while vulnerability scanning identifies potential weaknesses.

4. Question: Explain the importance of reporting in penetration testing.

Answer: Reporting details the vulnerabilities discovered, their potential impact, and recommendations for mitigation. It guides organizations in strengthening their security posture.

5. Question: Why is it essential to follow ethical guidelines in penetration testing?

Answer: Adhering to ethical guidelines ensures that penetration testing is conducted responsibly, minimizing risks and preventing unintended harm to systems or data during the assessment.