Interview Question Of Ethical Hacking

1. What is ethical hacking?

- **Answer**: Ethical hacking is the practice of testing and evaluating the security of computer systems, networks, or applications with the permission of the organization. The goal is to identify vulnerabilities and weaknesses so they can be fixed before malicious hackers exploit them. Ethical hackers follow a structured approach and adhere to legal and ethical guidelines.

2. What are the different types of hackers?

- **Answer**: Hackers are typically classified into three categories:
  - **White Hat Hackers**: Ethical hackers who are authorized to test systems for vulnerabilities.
  - **Black Hat Hackers**: Malicious hackers who exploit vulnerabilities for personal gain or harm.
  - **Gray Hat Hackers**: Hackers who may violate ethical standards but do not have malicious intent, often discovering vulnerabilities without permission but reporting them afterward.

3. What is penetration testing?

- **Answer**: Penetration testing, or pen testing, is a simulated cyberattack on a system, network, or application to assess its security. Ethical hackers use penetration testing to identify vulnerabilities and weaknesses by attempting to exploit them, thereby providing insights into how an attacker could gain unauthorized access.

4. What is the difference between vulnerability assessment and penetration testing?

- **Answer**:
  - **Vulnerability Assessment**: A systematic examination of a system or application to identify security weaknesses without attempting to exploit them. It provides a prioritized list of vulnerabilities but does not test their actual exploitability.
  - **Penetration Testing**: Involves simulating attacks on a system to determine the effectiveness of security measures. It not only identifies vulnerabilities but also tests their exploitability.

5. What are some common tools used in ethical hacking?

- **Answer**: Common tools used by ethical hackers include:
  - **Nmap**: A network scanning tool used to discover hosts and services on a network. o **Wireshark**: A network protocol analyzer that captures and inspects data packets.
  - **Metasploit**: A penetration testing framework that allows security professionals to find and exploit vulnerabilities.
  - **Burp Suite**: A web application security testing tool that helps identify vulnerabilities in web applications.
  - **OWASP ZAP**: An open-source web application security scanner for finding vulnerabilities.

6. What is social engineering?

- **Answer**: Social engineering is the psychological manipulation of people into divulging confidential information or performing actions that compromise security. It often involves tactics such as phishing emails, pretexting, baiting, and tailgating to trick individuals into providing access to sensitive data or systems.

7. What is the purpose of using a firewall in ethical hacking?

- **Answer**: A firewall is a security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. In ethical hacking, firewalls are important for assessing network security, as they can help protect against unauthorized access and attacks. Ethical hackers may test firewalls to ensure they are configured correctly and effectively blocking unwanted traffic.

8. What is the OWASP Top Ten?

- **Answer**: The OWASP Top Ten is a list of the ten most critical web application security risks compiled by the Open Web Application Security Project (OWASP). It serves as a guideline for organizations to understand and mitigate the most common vulnerabilities. The latest version includes risks like Injection, Broken Authentication, Sensitive Data Exposure, and Cross-Site Scripting (XSS).

9. What is a security policy, and why is it important?

- **Answer**: A security policy is a documented set of guidelines and procedures that outline how an organization protects its physical and information technology assets. It is important because it establishes clear expectations and responsibilities for employees regarding security practices, helps mitigate risks, and provides a framework for incident response.

10. What is a backdoor?

- **Answer**: A backdoor is a method of bypassing normal authentication procedures to gain unauthorized access to a system or application. Backdoors can be intentionally created by developers for legitimate purposes (e.g., for maintenance) or installed by attackers to maintain access to a compromised system. Ethical hackers seek to identify and eliminate backdoors during security assessments.

11. What is the role of encryption in ethical hacking?

- **Answer**: Encryption is the process of converting data into a coded format to prevent unauthorized access. In ethical hacking, encryption plays a critical role in protecting sensitive information both at rest and in transit. Ethical hackers may evaluate the strength of encryption methods used in an organization and attempt to identify weaknesses that could be exploited by attackers.