INTRODUCTION TO ETHICAL HACKING INTERVIEW QUESTIONS

1.What is ethical hacking?

Answer: Ethical hacking involves legally breaking into computers and devices to test an organization's defenses. It aims to identify and fix security vulnerabilities before malicious hackers can exploit them.

2.What are the primary goals of ethical hacking?

Answer: The primary goals are to identify security vulnerabilities, ensure compliance with security standards, improve overall security posture, and protect against cyber attacks.

3.What is the difference between ethical hacking and penetration testing?

Answer: Ethical hacking is a broader term that includes a variety of security testing techniques, while penetration testing is a specific type of ethical hacking focused on simulating attacks to identify vulnerabilities.

4.What is a vulnerability assessment?

Answer: A vulnerability assessment is the process of identifying, quantifying, and prioritizing vulnerabilities in a system. It helps in understanding the security weaknesses that need to be addressed.

5.What are the different types of hackers?

Answer: The main types of hackers are white hats (ethical hackers), black hats (malicious hackers), and gray hats (hackers who fall somewhere between ethical and malicious, often hacking without permission but without malicious intent).

6.What are the phases of ethical hacking?

Answer: The phases include reconnaissance, scanning, gaining access, maintaining access, and covering tracks.

7.What is reconnaissance in ethical hacking?

Answer: Reconnaissance is the initial phase where an ethical hacker gathers information about the target system or network to find ways to penetrate it. It can be passive (no direct interaction) or active (direct interaction).

8.What tools are commonly used for network scanning?

Answer: Common tools include Nmap, Nessus, OpenVAS, and Wireshark.

9.What is social engineering, and how is it used in ethical hacking?

Answer: Social engineering involves manipulating people into divulging confidential information or performing actions that compromise security. Ethical hackers use social engineering to test an organization's susceptibility to such attacks.

10.What is the difference between black-box and white-box testing?

Answer: Black-box testing is performed without any knowledge of the internal workings of the system, mimicking an external attacker's perspective. White-box testing is conducted with full knowledge of the system, including its source code and architecture, to find vulnerabilities.

11.What is a zero-day vulnerability?

Answer: A zero-day vulnerability is a previously unknown security flaw that hackers can exploit before the vendor becomes aware of it and issues a patch.

12.Explain the concept of privilege escalation.

Answer: Privilege escalation is the process of gaining higher access rights than initially granted. Attackers exploit vulnerabilities to elevate their privileges and gain control over a system.

13.What is the role of a bug bounty program in ethical hacking?

Answer: Bug bounty programs incentivize ethical hackers to find and report security vulnerabilities in an organization's systems by offering rewards or recognition.

14.What is SQL injection, and how can it be prevented?

Answer: SQL injection is an attack technique where malicious SQL statements are inserted into an input field to manipulate the database. It can be prevented by using parameterized queries, prepared statements, and input validation.

15.What is cross-site scripting (XSS), and how can it be mitigated?

Answer: XSS is an attack where malicious scripts are injected into web pages viewed by other users. It can be mitigated by validating and sanitizing user inputs and using content security policies (CSP).

16.What is the importance of ethical hacking certifications?

Answer: Certifications like CEH (Certified Ethical Hacker) validate an individual's skills and knowledge in ethical hacking, enhance their credibility, and improve their career prospects.

17.What legal and ethical considerations must ethical hackers be aware of?

Answer: Ethical hackers must obtain proper authorization before testing, respect privacy, comply with relevant laws and regulations, and maintain confidentiality of any sensitive information discovered during testing.

18.What is a firewall, and how does it contribute to network security?

Answer: A firewall is a network security device or software that monitors and controls incoming and outgoing traffic based on predetermined security rules. It helps protect networks from unauthorized access and attacks.

19.What is penetration testing methodology?

Answer: Penetration testing methodology is a structured approach to conducting penetration tests, usually involving phases such as planning, information gathering, vulnerability analysis, exploitation, reporting, and remediation.

20.How does ethical hacking contribute to an organization's security posture?

Answer: Ethical hacking helps identify and mitigate security vulnerabilities, test the effectiveness of security measures, ensure compliance with standards, and improve the overall resilience of an organization against cyber threats.