INTRODUCTION TO CYBER ATTACKS INTERVIEW QUESTIONS

1.What is a denial of service (DoS) attack?

Answer: A denial of service attack is an attempt to make a machine or network resource unavailable to its intended users by overwhelming the target with a flood of illegitimate requests, thereby disrupting normal operations.

2.How does a distributed denial of service (DDoS) attack differ from a DoS attack?

Answer: In a DDoS attack, multiple compromised systems, often infected with malware, are used to launch the attack simultaneously, amplifying its impact.

3.Explain the concept of a buffer overflow attack.

Answer: A buffer overflow attack occurs when a program writes more data to a buffer than it can handle, leading to overflow. This can corrupt adjacent memory locations, crash the program, or even execute arbitrary code.

4.What are some common consequences of buffer overflow attacks?

Answer: Consequences include crashing of the targeted system or program, execution of malicious code injected into the buffer, unauthorized access to sensitive data, or even complete system compromise.

5.How can buffer overflow attacks be prevented?

Answer: Techniques such as input validation, proper bounds checking, using safe string functions, and employing address space layout randomization (ASLR) can help prevent buffer overflow vulnerabilities.

6.What is IP spoofing?

Answer: IP spoofing is a technique where an attacker falsifies the source IP address in a packet to disguise their identity or impersonate another system.

7.How can IP spoofing be used in an attack?

Answer: IP spoofing can be used to bypass access controls, launch DoS attacks by flooding the victim with packets that appear to come from legitimate sources, or to conduct session hijacking.

8.What measures can be taken to mitigate IP spoofing attacks?

Answer: Implementing ingress and egress filtering at network borders, deploying authentication mechanisms such as TCP sequence number validation, and using cryptographic techniques like IPsec can help mitigate IP spoofing attacks.

9.Explain session hijacking.

Answer: Session hijacking involves an attacker intercepting and taking over a legitimate session between two parties, allowing the attacker to impersonate one of the parties and gain unauthorized access to sensitive information or resources.

10.What are some common methods used for session hijacking?

Answer: Methods include session fixation, man-in-the-middle (MITM) attacks, session sniffing, and exploiting session tokens or cookies.

11.How can session hijacking be prevented?

Answer: Employing HTTPS to encrypt communications, implementing strong session management practices, regularly regenerating session identifiers, and using secure cookies can help prevent session hijacking.

12.What is the role of encryption in preventing session hijacking?

Answer: Encryption helps protect the confidentiality and integrity of data exchanged between parties, making it harder for attackers to intercept and manipulate sessions.

13.Can firewalls prevent buffer overflow attacks?

Answer: Firewalls alone cannot prevent buffer overflow attacks, but they can help mitigate the risk by filtering out malicious traffic and enforcing access controls.

14.How does a SYN flood attack work?

Answer: A SYN flood attack floods a target system with TCP connection requests (SYN packets) but does not complete the handshake process, exhausting the target's resources and preventing legitimate connections.

15.What countermeasures can be used against SYN flood attacks?

Answer: Techniques such as SYN cookies, rate limiting, and deploying intrusion prevention systems (IPS) can help mitigate SYN flood attacks.

16.How can intrusion detection systems (IDS) help in detecting DoS attacks?

Answer: IDS can analyze network traffic patterns and behavior to identify anomalies indicative of DoS attacks, allowing for timely response and mitigation.

17.Explain the difference between passive and active session hijacking.

Answer: Passive session hijacking involves monitoring and intercepting communications without altering them, while active session hijacking involves actively manipulating or controlling the intercepted sessions.

18.What is a CSRF (Cross-Site Request Forgery) attack, and how is it related to session hijacking?

Answer: CSRF attacks trick a user into executing unauthorized actions on a web application while they are authenticated. While not directly related to session hijacking, CSRF attacks can compromise the integrity of sessions by exploiting the user's active session.

19.How can multi-factor authentication (MFA) enhance security against session hijacking?

Answer: MFA requires users to provide multiple forms of authentication, such as passwords and one-time codes sent to their mobile devices, making it more difficult for attackers to hijack sessions solely by obtaining login credentials.

20.What are the legal implications of conducting DoS attacks, buffer overflow attacks, IP spoofing, or session hijacking?

Answer: Engaging in such activities is illegal in many jurisdictions and can result in severe penalties, including fines and imprisonment. Additionally, individuals or organizations responsible for such attacks may face civil lawsuits for damages incurred by victims.