SCANNING NETWORK INTERVIEW QUESTIONS

1.What is network scanning?

Answer: Network scanning is a process used to identify active devices on a network and gather information about them, including their IP addresses, open ports, and services running.

2.Name some common network scanning techniques.

Answer: Common techniques include ping sweeps, port scanning (TCP/UDP), SYN scanning, ACK scanning, FIN scanning, Xmas scanning, and OS fingerprinting.

3.What is a ping sweep?

Answer: A ping sweep, or ICMP sweep, is a network scanning technique used to determine which range of IP addresses map to live hosts.

4.Explain TCP SYN scanning.

Answer: TCP SYN scanning, also known as half-open scanning, sends a SYN packet to the target port and waits for a response. If a SYN-ACK is received, the port is open. If an RST is received, the port is closed.

5.What is a port scan?

Answer: A port scan is a method used to identify open ports and services available on a host by sending packets to various ports and analyzing the responses.

6.Describe UDP scanning.

Answer: UDP scanning sends UDP packets to a target's ports. If no response or an ICMP port unreachable message is received, the port is considered closed. Otherwise, the port is likely open or filtered.

7.What is OS fingerprinting?

Answer: OS fingerprinting is a technique used to determine the operating system of a host by analyzing the responses to various network probes.

8.Explain the purpose of FIN scanning.

Answer: FIN scanning sends packets with the FIN flag set. Closed ports typically respond with an RST packet, while open ports generally do not respond.

9.What is an Xmas scan?

Answer: An Xmas scan sends packets with the FIN, PSH, and URG flags set. It works similarly to FIN scanning, attempting to elicit responses that indicate whether a port is open or closed.

10.How does ACK scanning work?

Answer: ACK scanning is used to map firewall rulesets, determining whether a firewall is stateful or stateless. It sends ACK packets to target ports; RST responses indicate that the port is not filtered.

11.What are common countermeasures to protect against network scanning?

Answer: Common countermeasures include firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), network segmentation, and using security tools to detect and block scans.

12.How can a firewall help prevent network scanning?

Answer: A firewall can block unwanted inbound and outbound traffic, including suspicious scanning activities, by applying rules that filter packets based on IP addresses, ports, and protocols.

13.What role does an IDS play in detecting network scans?

Answer: An IDS monitors network traffic for suspicious activity, such as scanning attempts, and can alert administrators to potential threats.

14.Explain the concept of network segmentation as a countermeasure.

Answer: Network segmentation involves dividing a network into smaller, isolated segments to limit the spread of attacks and reduce the exposure of sensitive systems to scanning activities.

15.How can IP blocking help prevent scanning?

Answer: IP blocking can prevent known malicious IP addresses from accessing the network, thus reducing the risk of scanning and subsequent attacks.

16.What is the purpose of using a honeypot in network security?

Answer: A honeypot is a decoy system set up to attract attackers. It can be used to detect and analyze scanning and attack attempts, providing valuable information about attack vectors and techniques.

17.How does rate limiting help mitigate scanning attacks?

Answer: Rate limiting controls the number of requests a user or IP address can make to a server within a specific time frame, reducing the likelihood of successful network scans.

18.Describe the use of port knocking as a security measure.

Answer: Port knocking involves sending a series of connection attempts to closed ports in a specific sequence to open a port temporarily, thus hiding open ports from unauthorized users.

19.What is the benefit of using encrypted traffic to counter network scanning?

Answer: Encrypted traffic makes it more difficult for attackers to interpret the content of network packets, reducing the effectiveness of scanning techniques that rely on packet inspection.

20.How can log analysis help in identifying scanning attempts?

Answer: Regular log analysis can help identify patterns indicative of scanning attempts, such as multiple connection attempts to different ports from the same IP address, allowing for timely responses to potential threats.