performing security assessments - focusing on assessing organizational security with network reconnaissance tools and types.

1. What is the primary goal of performing network reconnaissance during a security assessment?

- A) To identify vulnerabilities in the organization's network.

- B) To detect unauthorized access attempts.

- C) To gather information about the organization's network infrastructure.

- D) To ensure compliance with security policies.

- Answer: C) To gather information about the organization's network infrastructure.

2. Which of the following is NOT a common network reconnaissance tool?

- A) Nmap

- B) Wireshark

- C) Metasploit

- D) Snort

- Answer: D) Snort

3. Which network reconnaissance tool is commonly used for scanning and mapping network topology?

- A) Nmap

- B) Wireshark

- C) Metasploit

- D) Snort

- Answer: A) Nmap

4. What is the purpose of using Wireshark during a security assessment?

- A) To detect vulnerabilities in the network.

- B) To capture and analyze network traffic.

- C) To perform port scanning.

- D) To launch denial of service attacks.

- Answer: B) To capture and analyze network traffic.

5. Which of the following is a passive reconnaissance technique?

   - A) Network scanning
   - B) Port scanning
   - C) Social engineering
   - D) Packet sniffing
   - Answer: D) Packet sniffing

6. Which tool is commonly used to perform DNS enumeration during network reconnaissance?

   - A) Nmap
   - B) Wireshark
   - C) nslookup
   - D) Netcat
   - Answer: C) nslookup

7. What is the purpose of performing SNMP enumeration during network reconnaissance?

   - A) To gather information about network devices and their configurations.
   - B) To launch denial of service attacks.
   - C) To intercept network traffic.
   - D) To exploit vulnerabilities in network protocols.
   - Answer: A) To gather information about network devices and their configurations.

8. Which of the following statements about network reconnaissance is true?

   - A) It involves actively attacking network devices.
   - B) It is illegal and unethical.
   - C) It helps identify security weaknesses in the network.
   - D) It is only performed by external attackers.
   - Answer: C) It helps identify security weaknesses in the network.

9. Which network reconnaissance tool is commonly used to perform OS fingerprinting?

- A) Nmap
- B) Wireshark
- C) Metasploit
- D) Snort
- Answer: A) Nmap

10. What is the purpose of performing banner grabbing during network reconnaissance?
    - A) To identify the operating system of a target system.
    - B) To gather information about services running on a target system.
    - C) To detect intrusion attempts.
    - D) To launch brute-force attacks.
    - Answer: B) To gather information about services running on a target system.

11. Which of the following is NOT a common type of network reconnaissance?
    - A) Passive reconnaissance
    - B) Active reconnaissance
    - C) Social engineering
    - D) SNMP enumeration
    - Answer: C) Social engineering

12. What is the primary goal of performing network reconnaissance using active techniques?
    - A) To avoid detection by security tools.
    - B) To gather information without interacting with the target system.
    - C) To directly interact with the target system to gather information.
    - D) To launch denial of service attacks.
    - Answer: C) To directly interact with the target system to gather information.

13. Which of the following is a common output of a network reconnaissance tool?
    - A) Vulnerability report
    - B) Network diagram
    - C) Traffic analysis

- D) Port scan results
- Answer: D) Port scan results

14. Which of the following network reconnaissance techniques is considered the most stealthy?

- A) Port scanning
- B) Banner grabbing
- C) DNS enumeration
- D) SNMP enumeration
- Answer: C) DNS enumeration

15. What is the purpose of performing network reconnaissance before launching a cyber attack?

- A) To gather information about potential targets.
- B) To disrupt network communication.
- C) To exploit vulnerabilities in network devices.
- D) To bypass firewall rules.
- Answer: A) To gather information about potential targets.

16. Which network reconnaissance tool is commonly used for vulnerability scanning?

- A) Nmap
- B) Wireshark
- C) Nessus
- D) Nikto
- Answer: C) Nessus

17. What is the primary goal of performing passive reconnaissance?

- A) To avoid detection by security tools.
- B) To gather information without alerting the target.
- C) To directly interact with the target system.
- D) To launch denial of service attacks.
- Answer: B) To gather information without alerting the target.

18. Which of the following is a limitation of passive reconnaissance?

- A) It is time-consuming.

- B) It requires specialized tools.

- C) It cannot gather real-time information.

- D) It is easily detectable by security tools.

- Answer: C) It cannot gather real-time information.

19. What is the purpose of performing network reconnaissance using social engineering?

- A) To gather information about network devices.

- B) To exploit human psychology to gain access to the network.

- C) To launch denial of service attacks.

- D) To intercept network traffic.

- Answer: B) To exploit human psychology to gain access to the network.

20. Which of the following is NOT a common network reconnaissance tool?

- A) Maltego

- B) Netcat

- C) Wireshark

- D) Snort

- Answer: D) Snort

21. Which network reconnaissance tool is commonly used to perform vulnerability assessment?

- A) Nmap

- B) Metasploit

- C) Nessus

- D) Wireshark

- Answer: C) Nessus

22. What is the purpose of performing network reconnaissance using Netcat?

- A) To perform port scanning.

- B) To capture and analyze network traffic.

- C) To establish remote connections to network devices.
- D) To launch denial of service attacks.
- Answer: C) To establish remote connections to network devices.

23. Which of the following is NOT a common output of a network reconnaissance tool?

- A) Network diagram
- B) Vulnerability report
- C) Traffic analysis
- D) Port scan results
- Answer: C) Traffic analysis