QUESTIONS

1. Examine the Wireshark TCP flow capture here:

```
Host A      --- SYN --- >                Host B Seq = 0 Ack = 13425675
Host A      < --- SYN, ACK ---           Host B Seq = 0 Ack = 1
Host A      --- ACK --- >                Host B Seq = 1 Ack = 1
Host A      --- PSH, ACK Len:700 --- >   Host B Seq = 1 Ack = 1
Host A      < --- ACK ---                Host B Seq = 1 Ack = 701
Host A      < --- ACK Len:1341 ---       Host B Seq = 1 Ack = 701
Host A      --- ACK --- >                Host B Seq = 701 Ack = 1342
Host A      < --- ACK Len : 1322 ---     Host B Seq = 1342 Ack = 701
Host A      --- ACK --- >                Host B Seq = 701 Ack = 2664
Host A      < --- ACK Len : 1322 ---     Host B Seq = 2664 Ack = 701
```

   Which of the following represents the next appropriate acknowledgment from Host A?

   A. Sequence Number 701, Acknowledgment Number 3986

   B. Sequence Number 701, Acknowledgment Number 2664

   C. Sequence Number 2664, Acknowledgment Number 2023

   D. Sequence Number 2664, Acknowledgment Number 701

2. You have established a Netcat connection to a target machine. Which flag can be used to launch a program?

   A. –p

   B. –a

   C. –l

   D. –e

3. Which database type was targeted by the Slammer worm?

   A. Microsoft SQL

   B. MySQL

   C. Oracle

   D. Sybase

4. Which virus type will rewrite itself after each new infection?

   A. Multipartite

   B. Metamorphic

   C. Cavity

   D. Macro

5. A pen test colleague is carrying out attacks. In one attack, she attempts to guess the ISN for a TCP session. Which attack is she most likely carrying out?
   - **A.** XSS
   - **B.** Session splicing
   - **C.** Session hijacking
   - **D.** Multipartite attack
6. Which of the following malware types does not require user intervention to spread?
   - **A.** Trojan
   - **B.** Virus
   - **C.** Worm
   - **D.** Polymorphic
7. An attacker is attempting a DoS attack against a machine. She first spoofs the target's IP address and then begins sending large amounts of ICMP packets containing the MAC address FF:FF:FF:FF:FF:FF. What attack is underway?
   - **A.** ICMP flood
   - **B.** Ping of death
   - **C.** SYN flood
   - **D.** Smurf
   - **E.** Fraggle
8. Tripwire is one of the most popular tools to protect against Trojans. Which of the following statements best describes Tripwire?
   - **A.** Tripwire is a signature-based antivirus tool.
   - **B.** Tripwire is a vulnerability assessment tool used for port scanning.
   - **C.** Tripwire is a file integrity program.
   - **D.** Tripwire is a session-splicing tool.
9. Which of the following tools are good choices for session hijack attempts? (Choose all that apply.)
   - **A.** Ettercap
   - **B.** Netcat
   - **C.** Hunt
   - **D.** Nessus

10. In regard to Trojans, which of the following best describes a wrapper?
    - **A.** The legitimate file the Trojan is attached to
    - **B.** A program used to bind the Trojan to a legitimate file
    - **C.** Encryption methods used for a Trojan
    - **D.** Polymorphic code used to avoid detection by antivirus programs
11. Which of the following are true regarding BugBear and Pretty Park? (Choose three.)
    - **A.** Both programs make use of e-mail.
    - **B.** Pretty Park propagates via network shares and e-mail.
    - **C.** BugBear propagates via network shares and e-mail.
    - **D.** Pretty Park uses an IRC server to send your personal passwords.
    - **E.** Pretty Park terminates antivirus applications.
12. Which of the following is a legitimate communication path for the transfer of data?
    - **A.** Overt
    - **B.** Covert
    - **C.** Authentic
    - **D.** Imitation
    - **E.** Actual
13. In what layer of the OSI reference model is session hijacking carried out?
    - **A.** Data link layer
    - **B.** Transport layer
    - **C.** Network layer
    - **D.** Physical layer
14. A pen test team member types the following command:

    ```
    nc222.15.66.78 -p 8765
    ```

    Which of the following is true regarding this attempt?
    - **A.** The attacker is attempting to connect to an established listening port on a remote computer.
    - **B.** The attacker is establishing a listening port on his machine for later use.
    - **C.** The attacker is attempting a DoS against a remote computer.
    - **D.** The attacker is attempting to kill a service on a remote machine.

15. Examine the partial command-line output listed here:

```
Active Connections
Proto  Local Address          Foreign Address      State
  TCP    0.0.0.0:912           COMPUTER11:0          LISTENING
  TCP    0.0.0.0:3460          COMPUTER11:0          LISTENING
  TCP    0.0.0.0:3465          COMPUTER11:0          LISTENING
  TCP    0.0.0.0:8288          COMPUTER11:0          LISTENING
  TCP    0.0.0.0:16386         COMPUTER11:0          LISTENING
  TCP    192.168.1.100:139     COMPUTER11:0          LISTENING
  TCP    192.168.1.100:58191   173.194.44.81:https  ESTABLISHED
  TCP    192.168.1.100:58192   173.194.44.81:https   TIME_WAIT
  TCP    192.168.1.100:58193   173.194.44.81:https   TIME_WAIT
  TCP    192.168.1.100:58194   173.194.44.81:https   ESTABLISHED
  TCP    192.168.1.100:58200   bk-in-f138:http       TIME_WAIT
```

Which of the following is a true statement regarding the output?

A. This is output from a netstat –an command.

B. This is output from a netstat –b command.

C. This is output from a netstat –e command.

D. This is output from a netstat –r command.

16. You are discussing malware with a new pen test member who asks about restarting executables. Which registry keys within Windows automatically run executables and instructions? (Choose all that apply.)

A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

C. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

D. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

17. Which of the following best describes a covert channel?

A. An application using a port number that is not well-known

B. Using a protocol in a way it is not intended to be used

C. Multiplexing a communication link

D. WEP encryption channels

18. Which denial-of-service attack involves sending SYN packets to a target machine but never responding to any of the SYN/ACK replies?

A. SYN flood

B. SYN attack

C. Smurf

D. LOIC

19. Which of the following takes advantage of weaknesses in the fragment reassembly functionality of TCP/IP?
    - **A.** Teardrop
    - **B.** SYN flood
    - **C.** Smurf attack
    - **D.** Ping of death
20. IPSec is an effective preventative measure against session hijacking. Which IPSec mode encrypts only the data payload?
    - **A.** Transport
    - **B.** Tunnel
    - **C.** Protected
    - **D.** Spoofed
21. Which type of session hijacking is displayed in Figure 8-1?
    - **A.** Cross-site scripting attack
    - **B.** SQL injection attack
    - **C.** Token sniffing attack
    - **D.** Session fixation attack

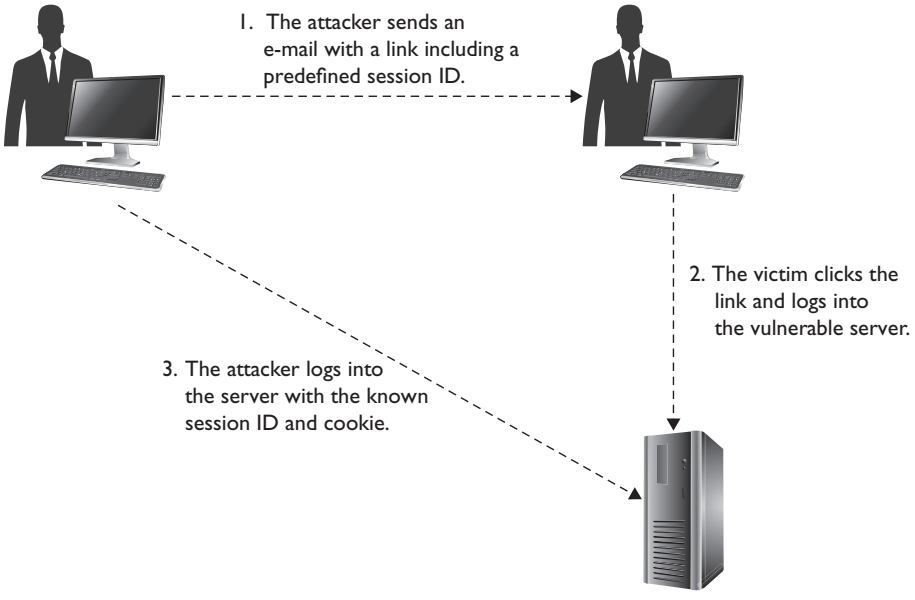

Figure 8-1 Session hijacking example

22. Which of the following best describes the comparison between spoofing and session hijacking?

    A. Spoofing and session hijacking are the same thing.

    B. Spoofing interrupts a client's communication, whereas hijacking does not.

    C. Hijacking interrupts a client's communication, whereas spoofing does not.

    D. Hijacking emulates a foreign IP address, whereas spoofing refers to MAC addresses.

23. Which of the following is an effective deterrent against session hijacking?

    A. Install and use a HIDS on the system.

    B. Install and use Tripwire on the system.

    C. Enforce good password policy.

    D. Use unpredictable sequence numbers.

24. A pen test team member types the following command:

    ```
    ettercap -T -q -M ARP /200.70.55.12
    ```

    Which of the following are true regarding this command? (Choose all that apply.)

    A. Ettercap is being configured for a GUI interface.

    B. Ettercap is being configured as a sniffer.

    C. Ettercap is being configured for text mode.

    D. Ettercap is being configured for manual mode.

    E. Ettercap is being configured for a man-in-the-middle attack.

25. Within a TCP packet dump, a packet is noted with the SYN flag set and a sequence number set at A13F. What should the acknowledgment number in the return SYN/ACK packet be?

    A. A131

    B. A130

    C. A140

    D. A14F

26. When is session hijacking performed?

    A. Before the three-step handshake

    B. During the three-step handshake

    C. After the three-step handshake

    D. After a FIN packet