Review Questions

1. What is sniffing?
   A. Sending corrupted data on the network to trick a system
   B. Capturing and deciphering traffic on a network
   C. Corrupting the ARP cache on a target system
   D. Performing a password-cracking attack
2. What is a countermeasure to passive sniffing?
   A. Implementing a switched network
   B. Implementing a shared network
   C. ARP spoofing
   D. Port-based security
3. What type of device connects systems on a shared network?
   A. Routers
   B. Gateways
   C. Hubs
   D. Switches
4. Which of the following is a countermeasure to ARP spoofing?
   A. Port-based security
   B. WinTCPkill
   C. Wireshark
   D. MAC-based security
5. What is dsniff?
   A. A MAC spoofing tool
   B. An IP address spoofing tool
   C. A collection of hacking tools
   D. A sniffer
6. At what layer of the OSI model is data formatted into packets?
   A. Layer 1
   B. Layer 2
   C. Layer 3
   D. Layer 4
7. What is snort?
   A. An IDS and packet sniffer
   B. Only an IDS
   C. Only a packet sniffer
   D. Only a frame sniffer
8. What mode must a network card operate in to perform sniffing?
   A. Shared
   B. Unencrypted
   C. Open
   D. Promiscuous
9. The best defense against any type of sniffing is _____.
   A. Encryption
   B. A switched network
   C. Port-based security

D. A good security training program

10. For what type of traffic can WinSniffer capture passwords? (Choose all that apply.)

A. POP3
B. SMTP
C. HTTP
D. HTTPS

11. Which of the following software tools can perform sniffing? (Choose all that apply.)

A. Dsniff
B. Wireshark
C. NetBSD
D. Netcraft

12. At what layer of the OSI model is data formatted into frames?

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 4

13. In which type of header are MAC addresses located?

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 7

14. In which type of header are IP addresses located?

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 7

15. In which header do port numbers appear?

A. IP
B. MAC
C. Data Link
D. Transport

16. What is the proper Wireshark filter to capture traffic only sent from IP address 131.1.4.7?

A. `ip.src == 131.1.4.7`
B. `ip.address.src == 131.1.4.7`
C. `ip.source.address == 131.1.4.7`
D. `src.ip == 131.1.4.7`

17. Which Wireshark filter will only capture traffic to www.google.com?

A. `ip.dst =` www.google.com
B. `ip.dst eq` www.google.com
C. `ip.dst ==` www.google.com
D. `http.dst ==` www.google.com

18. Passwords are found in which layer of the OSI model?

A. Application
B. IP
C. Data Link
D. Physical

19. Wireshark was previously known as _____.

A. Packet Sniffer
B. Ethereal
C. EtherPeek
D. SniffIT

20. Cain & Abel can perform which of the following functions? (Choose all that apply.)

A. Sniffing
B. Packet generation
C. Password cracking
D. ARP poisoning

Answers

1. Sniffing is the process of capturing and analyzing data on a network.
2. By implementing a switched network, passive sniffing attacks are prevented.
3. A network connected via hubs is called a shared network.
4. Port-based security implemented on a switch prevents ARP spoofing.
5. Dsniff is a group of hacking tools.
6. Packets are created and used to carry data at Layer 3.
7. Snort is both an intrusion detection system (IDS) and a sniffer.
8. A network card must operate in promiscuous mode in order to capture traffic destined for a different MAC address than its own.
9. Encryption renders the information captured in a sniffer useless to a hacker.
10. WinSniffer can capture passwords for POP3, SMTP, and HTTP traffic.
11. Dsniff and Wireshark are sniffer software tools.
12. Data is formatted into frames at Layer 2.
13. MAC addresses are added in the Layer 2 header.
14. IP addresses are added in the Layer 3 header.
15. Port numbers are in the Transport layer.
16. `ip.src == 131.1.4.7` will capture traffic sent from IP address 131.1.4.7.
17. `ip.dst eq` www.google.com is the filter that will capture traffic with the destination www.google.com.
18. Most passwords such as HTTP, FTP, and telnet passwords are found at the Application layer of the OSI model.
19. Wireshark was previously called Ethereal.
20. Cain & Abel can perform sniffing, password cracking, and ARP poisoning.