**Review Questions**

|  |  |  |
| --- | --- | --- |
| **1.** | What is sniffing?   1. Sending corrupted data on the network to trick a system 2. Capturing and deciphering traffic on a network 3. Corrupting the ARP cache on a target system 4. Performing a password-cracking attack | [Sniffing is the process of capturing and analyzing data on a network.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N14) |
| **2.** | What is a countermeasure to passive sniffing?   1. Implementing a switched network 2. Implementing a shared network 3. ARP spoofing 4. Port-based security | [By implementing a switched network, passive sniffing attacks are prevented.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N39) |
| **3.** | What type of device connects systems on a shared network?   1. Routers 2. Gateways 3. Hubs 4. Switches | [A network connected via hubs is called a shared network.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N64) |
| **4.** | Which of the following is a countermeasure to ARP spoofing?   1. Port-based security 2. WinTCPkill 3. Wireshark 4. MAC-based security | [Port-based security implemented on a switch prevents ARP spoofing.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N89) |
| **5.** | What is dsniff?   1. A MAC spoofing tool 2. An IP address spoofing tool 3. A collection of hacking tools 4. A sniffer | [Dsniff is a group of hacking tools.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N114) |
| **6.** | At what layer of the OSI model is data formatted into packets?   1. Layer 1 2. Layer 2 3. Layer 3 4. Layer 4 | [Packets are created and used to carry data at Layer 3.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N139) |
| **7.** | What is snort?   1. An IDS and packet sniffer 2. Only an IDS 3. Only a packet sniffer 4. Only a frame sniffer | [Snort is both an intrusion detection system (IDS) and a sniffer.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N164) |
| **8.** | What mode must a network card operate in to perform sniffing?   1. Shared 2. Unencrypted 3. Open 4. Promiscuous | [A network card must operate in promiscuous mode in order to capture traffic destined for a different MAC address than its own.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N189) |
| **9.** | The best defense against any type of sniffing is \_\_\_\_\_\_\_\_\_\_\_.   1. Encryption 2. A switched network 3. Port-based security 4. A good security training program | [Encryption renders the information captured in a sniffer useless to a hacker.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N214) |
| **10.** | For what type of traffic can WinSniffer capture passwords? (Choose all that apply.)   1. POP3 2. SMTP 3. HTTP 4. HTTPS | [WinSniffer can capture passwords for POP3, SMTP, and HTTP traffic.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N239) |
| **11.** | Which of the following software tools can perform sniffing? (Choose all that apply.)   1. Dsniff 2. Wireshark 3. NetBSD 4. Netcraft | [Dsniff and Wireshark are sniffer software tools.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N264) |
| **12.** | At what layer of the OSI model is data formatted into frames?   1. Layer 1 2. Layer 2 3. Layer 3 4. Layer 4 | [Data is formatted into frames at Layer 2.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N289) |
| **13.** | In which type of header are MAC addresses located?   1. Layer 1 2. Layer 2 3. Layer 3 4. Layer 7 | [MAC addresses are added in the Layer 2 header.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N314) |
| **14.** | In which type of header are IP addresses located?   1. Layer 1 2. Layer 2 3. Layer 3 4. Layer 7 | [IP addresses are added in the Layer 3 header.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N339) |
| **15.** | In which header do port numbers appear?   1. IP 2. MAC 3. Data Link 4. Transport | [Port numbers are in the Transport layer.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N364) |
| **16.** | What is the proper Wireshark filter to capture traffic only sent from IP address 131.1.4.7?   1. ip.src == 131.1.4.7 2. ip.address.src == 131.1.4.7 3. ip.source.address == 131.1.4.7 4. src.ip == 131.1.4.7 | [ip.src == 131.1.4.7 will capture traffic sent from IP address 131.1.4.7.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N389) |
| **17.** | Which Wireshark filter will only capture traffic to [www.google.com](http://www.google.com/)?   1. ip.dst = [www.google.com](http://www.google.com/) 2. ip.dst eq [www.google.com](http://www.google.com/) 3. ip.dst == [www.google.com](http://www.google.com/) 4. http.dst == [www.google.com](http://www.google.com/) | [ip.dst eq  www.google.com is the filter that will capture traffic with the destination www.google.com .](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N425) |
| **18.** | Passwords are found in which layer of the OSI model?   1. Application 2. IP 3. Data Link 4. Physical | [Most passwords such as HTTP, FTP, and telnet passwords are found at the Application layer of the OSI model.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N489) |
| **19.** | Wireshark was previously known as \_\_\_\_\_\_\_\_\_\_\_.   1. Packet Sniffer 2. Ethereal 3. EtherPeek 4. SniffIT | [Wireshark was previously called Ethereal.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N514) |
| **20.** | Cain & Abel can perform which of the following functions? (Choose all that apply.)   1. Sniffing 2. Packet generation 3. Password cracking 4. ARP poisoning | [Cain & Abel can perform sniffing, password cracking, and ARP poisoning.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=417774458&rowid=259&noteMenuToggle=0&leftMenuState=1#answer.N539) |

**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](http://www.google.com/) is the filter that will capture traffic with the destination [www.google.com](http://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. |