CHAPTER 4

Sniffing and Evasion

This chapter includes questions from the following topics:

- Describe sniffing concepts, including active and passive sniffing and protocols susceptible to sniffing
- Describe ethical hacking techniques for Layer 2 traffic
- Describe sniffing tools and understand their output
- Describe sniffing countermeasures
- Learn about intrusion detection system (IDS), firewall, and honeypot types, use, and placement
- Describe IDS, firewall, and honeypot evasion techniques

Overhearing a conversation, whether intentionally or via eavesdropping, is just part of our daily lives. Sometimes we sniff conversations without even meaning or trying to—it just happens. Anyone who has worked in a cube-farm office environment knows how easy it is to overhear conversations even when we don't want to. Or, if you have kids in your house who don't yet understand that sound travels, eavesdropping is a constant part of your day.

Sometimes our very nature makes it impossible not to listen in. A study in *Psychological Science* explored a "paradox of eavesdropping": it's

harder to *not* listen to a conversation when someone is talking on the phone (we hear only one side of the dialogue) than when two physically present people are talking to each other. Although the phone conversation contains much less information, we're much more curious about what's being said. That means we're hardwired to want to listen in. We can't help it.

But come on, admit it—you enjoy it sometimes, too. Overhearing a juicy piece of information just makes us happy and, for the gossip crowd, provides lots of ammunition for the next water-cooler session. And we all really like secrets. In fact, I think the thrill of learning and knowing a secret is matched only by the overwhelming desire to share it. For those working in the classified arena, this paradox of human nature is something that has to be guarded against every single day of their working lives.

Eavesdropping in the virtual world is almost always not accidental—there's purpose involved. You don't necessarily need to put a whole lot of effort into it, but it almost never happens on its own without your purposeful manipulation of something. Sniffing provides a variety of information to the ethical hacker and is a skill all should be intimately familiar with. Just know that the secrets you overhear on your job as a pen tester might be really exciting, and you might *really* want to tell *somebody* about them, but you may find yourself *really* in jail over it too.

STUDY TIPS The good news is, once again there hasn't been very much updated from previous versions regarding sniffing and evasion—so any study you've put in previously will still apply. The bad news is, it's still tough stuff, and sometimes the questions are picky. Just as with everything else, review your basic network knowledge thoroughly. You'll see lots of questions designed to test your knowledge on how networking devices handle traffic, how addressing affects packet flow, what layers sniffing concentrates in (Layer 2, and sometimes Layer 3), and which protocols are more susceptible to sniffing than others.

Additionally, learn Wireshark *very* well. Pay particular attention to filters within Wireshark—how to set them up and what syntax they follow—and how to read a capture (not to mention the "follow TCP stream" option). If you haven't already, download Wireshark and start playing with it—right now, before you even read the questions that follow. On any exam questions that show a Wireshark screen capture, pay close attention to the flags set in the segment, the source and destination addresses, and the protocols listed. These items are easy to pick out for almost anyone who can spell, and they will answer many of the questions you'll see.

IDS types and ways to get around them won't make up a gigantic portion of your test, but they'll definitely be there. These will most likely come in the form of scenario questions, as opposed to straight definitions. While ECC loves fragmentation, session splicing (with something like Whisker), and tunneling (HTTP or even TCP over DNS), just remember there are other ways to get around an IDS, including generating "cover fire" (that is, tons of false positives) and, of course, the ultimate in evasion—encryption. If the traffic is encrypted, the IDS sees nothing.

Lastly, don't forget your firewall types. You won't see many questions on identifying a definition, but you'll probably see at least a couple of scenario questions where this knowledge comes in handy—in particular, how stateful firewalls work and what they do.

QUESTIONS Q

1. Given the following Wireshark filter, what is the attacker attempting to view?

```
((tcp.flags == 0x02) || (tcp.flags == 0x12) ) || ((tcp.flags ==
0x10) && (tcp.ack==1) && (tcp.len==0) )
```

A. SYN, SYN/ACK, ACK

B. SYN, FIN, URG, and PSH

C. ACK, ACK, SYN, URG

D. SYN/ACK only

2. A target machine (with a MAC of 12:34:56:AB:CD:EF) is connected to a switch port. An attacker (with a MAC of 78:91:00:ED:BC:A1) is attached to a separate port on the same switch with a packet capture running. There is no spanning of ports or port security in place. Two packets leave the target machine. Message 1 has a destination MAC of E1:22:BA:87:AC:12. Message 2 has a destination MAC of FF:FF:FF:FF:FF:FF. Which of the following statements is true regarding the messages being sent?

A. The attacker will see message 1.

B. The attacker will see message 2.

C. The attacker will see both messages.

D. The attacker will see neither message.

3. You have tapped into a network subnet of your target organization. You begin an attack by learning all significant MAC addresses on the subnet. After some time, you decide to intercept messages between two hosts. You send broadcast messages to Host A showing your MAC address as belonging to Host B. What is being accomplished here?

A. ARP poisoning to allow you to see all messages from either host without interrupting their communications process

B. ARP poisoning to allow you to see messages from Host A to Host B

C. ARP poisoning to allow you to see messages from Host B to Host A

D. ARP poisoning to allow you to see messages from Host A destined to any address

E. ARP poisoning to allow you to see messages from Host B destined to any address

4. Your target subnet is protected by a firewalled DMZ. Reconnaissance shows the external firewall passes some traffic from external to internal, but blocks most communications. HTTP traffic to a web server in the DMZ, which answers to **www.somebiz.com**, is allowed, along with standard traffic such as DNS queries. Which of the following may provide a method to evade the firewall's protection?

A. An ACK scan

B. Firewalking

C. False positive flooding

D. TCP over DNS

5. Which of the following is the best choice in setting an NIDS tap?

A. Connect directly to a server inside the DMZ.

B. Connect directly to a server in the intranet.

C. Connect to a SPAN port on a switch.

D. Connect to the console port of a router.

6. You have a large packet capture file in Wireshark to review. You want to filter traffic to show all packets with an IP address of 192.168.22.5 that contain the string HR_admin. Which of the following filters would accomplish this task?

A. ip.addr==192.168.22.5 &&tcp contains HR_admin

B. ip.addr 192.168.22.5 && “HR_admin”

C. ip.addr 192.168.22.5 &&tcp string ==HR_admin

D. ip.addr==192.168.22.5 + tcp contains tide

7. Which of the following techniques can be used to gather information from a fully switched network or to disable some of the traffic isolation features of a switch? (Choose two.)

A. DHCP starvation

B. MAC flooding

C. Promiscuous mode

D. ARP spoofing

8. Which of the following statements is true regarding the discovery of sniffers on a network?

A. To discover the sniffer, ping all addresses and examine the latency in responses.

B. To discover the sniffer, send ARP messages to all systems and watch for NOARP responses.

C. To discover the sniffer, configure the IDS to watch for NICs in promiscuous mode.

D. It is almost impossible to discover the sniffer on the network.

9. Which of the following could provide a useful defense against ARP spoofing? (Choose all that apply.)

A. Using ARPWALL

B. Setting all NICs to promiscuous mode

C. Using private VLANs

D. Using static ARP entries

10. Examine the following Snort rule:

```
alerttcp !$HOME_NET any -> $HOME_NET 23 (content:
"admin";msg:"Telnet attempt..admin access";)
```

Which of the following statements are true regarding the rule? (Choose all that apply.)

A. This rule will alert on packets coming from the designated home network.

B. This rule will alert on packets coming from outside the designated home address.

C. This rule will alert on packets designated for any port, from port 23, containing the “admin” string.

D. This rule will alert on packets designated on port 23, from any port, containing the “admin” string.

11. You want to begin sniffing, and you have a Windows laptop. You download and install Wireshark but quickly discover your NIC needs to be in promiscuous mode. What allows you to put your NIC into promiscuous mode?

A. Installing lmpcap

B. Installing npcap

C. Installing WinPcap

D. Installing libPcap

E. Manipulating the NIC properties through Control Panel | Network and Internet | Change Adapter Settings

12. A network and security administrator installs an NIDS. After a few weeks, a successful intrusion into the network occurs and a check of the NIDS during the timeframe of the attack shows no alerts. An investigation shows the NIDS was not configured correctly and therefore did not trigger on what should have been attack alert signatures. Which of the following best describes the actions of the NIDS?

A. False positives

B. False negatives

C. True positives

D. True negatives

13. A pen test member has gained access to an open switch port. He configures his NIC for promiscuous mode and sets up a sniffer, plugging his laptop directly into the switch port. He watches traffic as it arrives at the system, looking for specific information to possibly use later. What type of sniffing is being practiced?

A. Active

B. Promiscuous

C. Blind

D. Passive

E. Session

14. Which of the following are the best preventive measures to take against DHCP starvation attacks? (Choose two.)

A. Block all UDP port 67 and 68 traffic.

B. Enable DHCP snooping on the switch.

C. Use port security on the switch.

D. Configure DHCP filters on the switch.

15. Which of the following tools is the best choice to assist in evading an IDS?

A. Nessus

B. Nikto

C. Libwhisker

D. Snort

16. An attacker somehow manages to connect a rogue switch onto an enterprise network segment. He configures the switch with a priority lower than any other on the network. Assuming this attempt is successful, which of the following statements is true?

A. The rogue switch will cause broadcast loops and eventually DoS the segment.

B. The rogue switch will become the root bridge, allowing the attacker to sniff network traffic.

C. DHCP will no longer function on the segment.

D. None of the above.

17. Your IDS sits on the network perimeter and has been analyzing traffic for a couple of weeks. On arrival one morning, you find the IDS has alerted on a spike in network traffic late the previous evening. Which type of IDS are you using?

A. Stateful

B. Snort

C. Passive

D. Signature based

E. Anomaly based

18. You are performing an ACK scan against a target subnet. You previously verified connectivity to several hosts within the subnet but want to verify all live hosts on the subnet. Your scan, however, is not receiving any replies. Which type of firewall is most likely in use at your location?

A. Packet filtering

B. IPS

C. Stateful

D. Active

19. You are separated from your target subnet by a firewall. The firewall is correctly configured and allows requests only to ports opened by the administrator. In firewalking the device, you find that port 80 is open. Which technique could you employ to send data and commands to or from the target system?

A. Encrypt the data to hide it from the firewall.

B. Use session splicing.

C. Use MAC flooding.

D. Use HTTP tunneling.

20. Which of the following tools can be used to extract Application layer data from TCP connections captured in a log file into separate files?

A. Snort

B. Netcat

C. TCPflow

D. Tcpdump

21. Examine the Wireshark filter shown here:

```
ip.src == 192.168.1.1 &&tcp.srcport == 80
```

Which of the following correctly describes the capture filter?

A. The results will display all traffic from 192.168.1.1 destined for port 80.

B. The results will display all HTTP traffic to 192.168.1.1.

C. The results will display all HTTP traffic from 192.168.1.1.

D. No results will display because of invalid syntax.

22. You need to put the NIC into listening mode on your Linux box, capture packets, and write the results to a log file named my.log. How do you accomplish this with tcpdump?

A. tcpdump -i eth0 -w my.log

B. tcpdump -l eth0 -c my.log

C. tcpdump /i eth0 /w my.log

D. tcpdump /l eth0 /c my.log

23. Which of the following tools can assist with IDS evasion? (Choose all that apply.)

A. Whisker

B. Fragroute

C. Capsa

D. Wireshark

E. ADMmutate

F. Inundator

24. A security administrator is attempting to "lock down" her network and blocks access from internal to external on all external firewall ports except for TCP 80 and TCP 443. An internal user wants to make use of other protocols to access services on remote systems (FTP, as well as some non-standard port numbers). Which of the following is the most likely choice the user could attempt to communicate with the remote systems over the protocol of her choice?

A. Use HTTP tunneling.

B. Send all traffic over UDP instead of TCP.

C. Crack the firewall and open the ports required for communication.

D. MAC flood the switch connected to the firewall.

25. An ethical hacker is assigned to scan a server and wants to avoid IDS detection. She uses a tactic wherein the TCP header is split into many packets, making it difficult to detect what the packets are intended for. Which of the following best describes the technique employed?

A. TCP scanning

B. IP fragment scanning

C. ACK scanning

D. Inverse TCP scanning

QUICK ANSWER KEY

1. A

2. B

3. B

4. D

5. C

6. A

7. B, D

8. D

9. A, C, D

10. B, D

11. C

12. B

13. D

14. B, C

15. C