QUESTIONS

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 successfully 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 begin by sending broadcast messages to Host A showing your MAC address as belonging to Host B. Simultaneously, you send messages to Host B showing your MAC address as belonging to Host A. What is being accomplished here?

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

   B. ARP poisoning to allow you to see messages from Host A to Host B, and vice versa

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

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

   E. Failed ARP poisoning—you will not be able to see any traffic

4. Which of the following represents the loopback address in IPv6?
   - **A.** fe80::/10
   - **B.** fc00::/7
   - **C.** fec0::/10
   - **D.** ::1
5. An attacker has successfully tapped into a network segment and has configured port spanning for his connection, which allows him to see all traffic passing through the switch. Which of the following protocols protects any sensitive data from being seen by this attacker?
   - **A.** FTP
   - **B.** IMAP
   - **C.** Telnet
   - **D.** POP
   - **E.** SMTP
   - **F.** SSH
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 is true regarding the discovery of sniffers on a network?
   - **A.** To discover the sniffer, ping all addresses and examine 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 useful defense against ARP spoofing? (Choose all that apply.)
   - **A.** Use ARPWALL.
   - **B.** Set all NICs to promiscuous mode.
   - **C.** Use private VLANS.
   - **D.** Use 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 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 7 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. You are attempting to deliver a payload to a target inside the organization; however, it is behind an IDS. You are concerned about successfully accomplishing your task without alerting the IDS monitoring team. Which of the following methods are possible options? (Choose all that apply.)
    - **A.** Flood the network with fake attacks.
    - **B.** Encrypt the traffic between you and the host.
    - **C.** Session hijacking.
    - **D.** Session splicing.

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. What does this line from the Snort configuration file indicate?

```
var RULE_PATH c:\etc\snort\rules
```

    A. The configuration variable is not in the proper syntax.

    B. It instructs the Snort engine to write rule violations in this location.

    C. It instructs the Snort engine to compare packets to the rule set named "rules."

    D. It defines the location of the Snort rules.

16. Which of the following tools is the best choice to use in sniffing NFS traffic?

    A. Macof

    B. Snow

    C. Filesnarf

    D. Snort

17. Examine the Snort output shown here:

```
08/28-12:23:13.014491 01:10:BB:17:E3:C5 ->A5:12:B7:55:57:AB type:0x800
len:0x3C
190.168.5.12:33541 ->213.132.44.56:23 TCP TTL:128 TOS:0x0 ID:12365

IpLen:20 DgmLen:48 DF
***A**S* Seq: 0xA153BD Ack: 0xA01657 Win: 0x2000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOPSackOK
0x0000: 00 02 B3 87 84 25 00 10 5A 01 0D 5B 08 00 45 00 .%..Z..[..E.
0x0010: 00 30 98 43 40 00 80 06 DE EC C0 A8 01 04 C0 A8 .0.C@...
0x0020: 01 43 04 DC 01 BB 00 A1 8B BD 00 00 00 00 70 02 .C....p.
0x0030: 20 00 4C 92 00 00 02 04 05 B4 01 01 04 02 .L.....
```

Which of the following is true regarding the packet capture?

A. The capture indicates a NOP sled attack.

B. The capture shows step 2 of a TCP handshake.

C. The packet source is 213.132.44.56.

D. The packet capture shows an SSH session attempt.

18. 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

19. 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

20. 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.

21. 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

22. 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.

23. 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

24. 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

25. Which command puts Snort into packet logger mode?

A. `./snort -dev -l ./log`

B. `./snort –v`

C. `./snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf`

D. None of the above

26. 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 nonstandard 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.