Review Questions

You can find the answers in the appendix.

1. Which hardware vendor uses the term *SPAN* on switches?
   A. HP
   B. 3COM
   C. Cisco
   D. Juniper

2. If you saw the following command line, what would you be capturing?

```
tcpdump -i eth2 host 192.168.10.5
```

   A. Traffic just from 192.168.10.5
   B. Traffic to and from 192.168.10.5
   C. Traffic just to 192.168.10.5
   D. All traffic other than from 192.168.86.5

3. In the following packet, what port is the source port?

```
20:45:55.272087 IP yazpistachio.lan.62882 > loft.lan.afs3-fileserver: Flags
[P.], seq 915235445:915235528, ack 3437317287, win 2048, options [nop,nop,TS
val 1310611430 ecr 1794010423], length 83
```

   A. lan
   B. fileserver
   C. yazpistachio
   D. 62882

4. What is one downside to running a default `tcpdump` without any parameters?
   A. DNS requests
   B. Not enough information
   C. Sequence numbers don't show
   D. `tcpdump` not running without additional parameters

5. At which protocol layer does the Berkeley Packet Filter operate?
   A. Internetwork
   B. Transport
   C. Data Link
   D. Protocol

6. What do we call an ARP response without a corresponding ARP request?
   A. Is-at response
   B. Who-has ARP
   C. Gratuitous ARP
   D. IP response

7. Which functionality in Wireshark will provide you with percentages for every protocol in the packet capture, ordered by protocol layers?
   A. Conversations
   B. Endpoints
   C. Protocol hierarchy
   D. Statistics view

8. Which program would you use if you wanted to only print specific fields from the captured packet?
   A. `fielddump`
   B. `tcpdump`
   C. `wiredump`
   D. `tshark`

9. The following shows a time stamp. What does the time of this message reflect?

```
630    41.897644    192.168.86.210    239.255.255.250    SSDP    750
NOTIFY * HTTP/1.1    [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
```

   A. The time since 1970.
   B. The time of day.
   C. The time since packet start.
   D. There is no time in the summary.

10. What protocol is being used in the frame listed in this summary?

```
719    42.691135    157.240.19.26    192.168.86.26    TCP    1464    443
→ 61618 [ACK] Seq=4361 Ack=1276 Win=31232 Len=1398 TSval=3725556941
TSecr=1266252437 [TCP segment of a reassembled PDU]
```

   A. TLS
   B. UDP
   C. IP
   D. TCP

11. What program could be used to perform spoofing attacks and also supports plug-ins?
    A. `arpspoof`
    B. `fragroute`
    C. Ettercap
    D. `sslstrip`
12. What would you need to do before you could perform a DNS spoof attack?
    A. Set up a port span
    B. Start up Wireshark
    C. ARP spoof
    D. Configure `sslstrip`
13. Which command-line parameter would you use to disable name resolutions in `tcpdump`?
    A. `-n`
    B. `-i`
    C. `-r`
    D. `-x`
14. Why might you have more endpoints shown at layer 4 than at layer 2?
    A. Layer 4 multiplexes layer 2.
    B. Systems may initiate multiple connections to the same host.
    C. Ports are more numerous than MAC addresses.
    D. The IP addresses dictate the endpoints.
15. What would you use `sslstrip` for?
    A. Getting plaintext traffic
    B. Removing all SSL requests
    C. Converting SSL to TLS
    D. Converting TLS to SSL
16. Why might you have problems with `sslstrip`?
    A. `sslstrip` is deprecated.
    B. `sslstrip` doesn't work with newer versions of TLS.
    C. `sslstrip` doesn't support TLS.
    D. `sslstrip` works only with Ettercap.

17. What does the following line mean?

```
Sequence number: 4361    (relative sequence number)
```

A. The sequence number shown is not the real sequence number.
B. The sequence number shown has not been incremented.
C. The sequence number shown isn't long enough.
D. The sequence number shown is the acknowledgment number.

18. What can you say about `[TCP Segment Len: 35]`, as provided by Wireshark?
A. The window size has changed.
B. Wireshark has inferred this information.
C. Wireshark extracted this from one of the headers.
D. Wireshark has additional detail below.

19. What problem does port spanning overcome?
A. Switches don't support layer 3.
B. Switches aggregate ports.
C. Switches filter traffic.
D. Switches are unreliable.

20. What is the `/etc/ettercap/etter.dns` file used for?
A. Enabling firewall rules for Ettercap
B. Configuring hostnames to IP addresses
C. Setting up mail for Ettercap
D. Disabling ARP spoofing in Ettercap