Weaver Fall 2017	CS 161 Computer Security	Discussion 8

Week of October 16, 2017

Question 1 ***Introduction to Networking*** **(10 min)**

(a) **Protocol Layers.** At which network layer does each of the following operate (physical, link, network, transport, or application)?

- Ethernet
- SMTP (email)
- SYN packet
- UDP
- Fiber optics
- FTP
- DNS request
- BitTorrent
- IP address
- 127.0.0.1
- 802.11n WiFi

(b) **TCP and UDP.** The transmission control protocol (TCP) and user datagram protocol (UDP) are two of the primary protocols of the Internet protocol suite.

i. How do TCP and UDP relate to IP (Internet protocol)? Which of these protocols are encapsulated within (or layered atop) one another? Could all three be used simultaneously?

ii. What are the differences between TCP and UDP? Which is considered "best effort"? What does that mean?

Question 2 ***CS168 in under an hour! (minus routing)*** **(40 min)**

Professor Raluca gets home after a tiring day writing papers and singing karaoke ☺. She opens up her laptop and would like to submit them to a conference. From a networking and web perspective, what are the steps involved in submitting her paper?

(a) **DHCP**

Raluca's computer needs to connect to the wifi. What messages are exchanged in the 4 part handshake in order to achieve this?

Raluca's computer sends: _____. This message is broadcasted/unicasted (Choose one and explain):

A DHCP server replies with a DHCP Offer. What does this message contain? What can a malicious attacker do at this step? Keep in mind that an attacker on the same subnet can hear the discovery message.

Raluca's computer sends: _____. This message is broadcasted/unicasted (Choose one and explain)

The server then responds with: _____.

(b) **ARP**

Raluca would like to print out her paper. Her printer is on a different local network with the IP address 192.168.1.5 and the MAC address: 1E:AT:DE:AD:BE:EF.

Raluca's computer is configured as follows:

```
IP Address: 192.168.0.2
DNS Server: 8.8.8.8
Subnet mask: 255.255.255.0
Default Gateway: 192.168.0.1
MAC Address: F8:DB:88:F8:4C:27
```

What address does Raluca's computer make an ARP request for? _____

The response she gets back is: 16:1D:EA:DB:EE:F1.

Fill out the information for Raluca's packet below:

Raluca's Packet

```
Source IP address:
Destination IP:
Source MAC Address:
Destination MAC Address:
```

The router (router A) routes this packet to the router (router B) of the printer using the destination IP address. The MAC address for router B is C0:FF:EE:C0:FF:EE.

What address does the router B make an ARP request for? _____

Packet: From Router B to Printer.

```
Source IP address:
Destination IP:
Source MAC Address:
Destination MAC Address:
```

Oh no! Raluca has a smart refrigerator that has been taken over by an attacker ☹. Assume her refrigerator is on her local network. How can the attacker intercept Raluca's paper before it gets to the printer?

(c) **DNS + Transport**

After printing out and reading her paper, Raluca would like to submit her papers to the conference, EuroSys 2017. On her laptop she types http://eurosys2017.org/ into Firefox. Assume this is the first time Raluca visits Eurosys on her laptop.

Describe the steps involved in obtaining the DNS record for eurosys2017.org (Assume we have a recursive resolver).

What L4 protocol is used for DNS messages?

What L4 protocol is used for http traffic?

When would you use TCP versus UDP and why?

Question 3 ***Sniffer detection*** **(10 min)**

As the security officer for your company, your network monitoring has observed a download of a "sniffer" tool. This tool passively eavesdrops on traffic, and whenever it sees a web session going to a server in a `*.yahoo.com` domain, it extracts the user's session cookie. It then uses the cookie to create a new connection that automatically logs in as the user and exfiltrates all of their `*.yahoo.com` activity, such as their emails if they use a `yahoo.com` email account.

You become concerned that one of your employees may have installed a network "tap" somewhere among the hundreds of links inside your building, and will use it to run this tool. How might you determine whether such a sniffer is in operation?