Prelab 2 - HTTP, DNS, and TCP:

Suggested Resources:

https://www.ietf.org/rfc/rfc2616.txt
https://www.ietf.org/rfc/rfc1035.txt
https://linux.die.net/man/
http://www.tcpipguide.com/free/

HTTP Questions

1. [7 pts] Choose 5 HTTP status codes and describe each one.
2. [7 pts] List the 8 HTTP 1.1 methods and explain what they do.

wget and *telnet* are two commonly known command line tools for testing and debugging. Answer the following questions by using your Mininet VM's terminal or the Unix timeshare (see Lab 1 for instructions on connecting to the timeshare).

3. [7 pts] Use *wget* on *example.com* to view the last modified date of the webpage. What was the HTTP return status given and what command was used to do this? (The command should not download the file! Hint: Look into the wget man page.)
4. [7 pts] Look up the *telnet* command. Use *telnet* to connect to *www.telehack.com*, then type *starwars* What does this telnet server do?

DNS Questions

5. [7 pts] In your own words describe what a DNS resource record (RR) is. Now using the command line tool *nslookup* find the *MX* resource record of *ucsc.edu*. What does this resource record mean?
6. [7 pts] What does the command *nslookup -type=ns .* do*?* Explain its output. (Note: the . is part of the command!)

TCP Questions

7. [10 pts] How can multiple application services running on a single machine with a single IP address be uniquely identified?
8. [9 pts] What is the purpose of the window mechanism in TCP?
9. [9 pts] What is an MTU? What happens when a packet is larger than the MTU?

Lab 2 - HTTP, DNS, and TCP:

Suggested Resources:

http://packetbomb.com/understanding-the-tcptrace-time-sequence-graph-in-wireshark/
https://wiki.linuxfoundation.org/networking/netem

Part 1: HTTP

In this section, we will observe how the HTTP protocol operates. We will do this by using the Mininet VM. Begin by opening Wireshark and listening on the 'any' interface.

Open Chromium and navigate to http://httpbin.org

1. [10 pts] Find the HTTP packet that corresponds to the initial request that your computer made. Take a screenshot of this packet. What HTTP method did your computer use to make this request?

2. [10 pts] Find the HTTP packet that corresponds to the initial response the server made to your request. Take a screenshot of this packet. What HTTP status code did the server return? What is the content type of the response the server is sending back?

Using Chromium and navigate to http://ucsc.edu

3. [10 pts] Find the HTTP packets that correspond to the initial request and response that your computer made. Take a screenshot of these packets. What's different? Explain.

Using Chromium (or any other Linux utility you are comfortable with), find a way to make a HTTP packet with a method other than GET.

4. [10 pts] Take a screenshot of your packet, and explain what you did to create it.

Part 2: DNS

In this section, we will observe how the DNS protocol operates. We will do this by using the Mininet VM. Begin by opening Wireshark and listening on the 'any' interface.

Open Chromium and navigate to www.example.com.

5. [10 pts] Were any steps taken by your computer before the web page was loaded? If so, using your captured packets in Wireshark, find the packets that allowed your computer to successfully load http://neverssl.com/ or http://www.example.com. Take a screenshot of these packets, and explain why you think these are the correct packets. What's the IP address of www.example.com?

6. [10 pts] Open a terminal window. Execute the command to flush your DNS cache:

   sudo /etc/init.d/networking restart

   (if your VM doesn't allow you to do so, you can skip this step and add "--no-dns-cache" flag for the next step when using "wget")

   Using wget, download the same content of www.example.com with its IP address you discovered in question 5, without sending DNS requests.

   What command did you use to accomplish that? Take a screenshot of related packets and explain why you think these are the correct packets.

Open a terminal window. Using nslookup, find the A records for www.google.com. (If you can't access Google, for example, you are in China, you could replace the domain name with www.baidu.com)

7. [10 pts] Take a screenshot of the packets corresponding to your request, and the response from the server. If the request was resolved, what is the IP address you were given for www.google.com?

8. [10 pts] Did your computer want to complete the request recursively? How do you know? Take a screenshot proving your answer.

Using nslookup, find the A records for ucsc.edu.

9. [10 pts] Take a screenshot of the packets corresponding to your request, and the response from the server. If the request was resolved, what is the IP address you were given for ucsc.edu?

10. [10 pts] What is the authoritative name server for the ucsc.edu domain? How do you know? Take a screenshot proving your answer.

Part 3: TCP

In this section, we will observe how the TCP protocol operates. We will do this by using the Mininet VM. Begin by opening Wireshark and listening on the 'any' interface.

Open a terminal window. Using wget, download the file http://ipv4.download.thinkbroadband.com/10MB.zip

11. [10 pts] Find the packets corresponding with the SYN, SYN-ACK, and ACK that initiated the TCP connection for this file transfer. Take a screenshot of these packets. What was the initial window size that your computer advertised to the server? What was the initial window size that the server advertised to you?

12. [10 pts] Find a packet from the download with a source of the server and a destination of your computer. Create a tcptrace graph with this packet selecrated. Take a screenshot of the graph and explain what it is showing. Look into the Wireshark documentation if you need assistance making this graph.

In the next section, we will be simulating loss, the command *tc qdisc* will be needed. When you first use the command you should use *add dev* for the device you plan on changing. It only needs to be set on the sender's side. After adding the device use *change dev*.

Example:

```
sudo tc qdisc add dev eth0 root netem loss 0%
sudo tc qdisc change dev eth0 root netem loss 100%
```

Read through the following paragraph before starting the next step. Open 2 terminals and have the commands typed and ready before you begin. In one terminal, download the 10MB.zip file again. While the download is in progress, change loss to 100%. After a few seconds, change loss to 0%.

13. [10 pts] Find a packet from the download with a source of the server and a destination of your computer. Create a tcptrace graph with this packet selected. Take a screenshot of the graph and explain what it is showing. Using an image editting program, circle the areas where the 0% loss is shown, as well as where TCP is in slow-start and congestion-avoidance.