**CS-359 Assignment-1**

Name: P. V. Sriram

Roll No.: 1801CS37

**Problem1: Writing Wireshark filter expressions for packet capture**

**Write the exact packet capture filter expressions to accomplish the following:**

**1. Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account**

**2. Capture all HTTP traffic to/from Facebook, when you log in to your Facebook account**

**3. Find a popular YouTube video and play it while capturing all traffic to/from YouTube**

**Capture Filters:**

1. **To capture TCP Traffic to/from Facebook**

We first find out the Facebook server’s IP using ping facebook.com

Capture Filter: tcp and host 69.171.250.35

Output: 711 packets captured

Display Filter: ip.dst==69.171.250.35

Output: 348 packets captured (To facebook)

Display Filter: ip.src==69.171.250.35

Output: 363 packets captured (From Facebook)

1. **To capture HTTPS traffic to/from Facebook**

We use the previously collected tcp data of Facebook and add a display filter for SSL

Capture Filter: tcp and host 69.171.250.36

Display Filter: tcp.port==443

Output: 678 packets captured

Display Filter: tcp.port==443 && ip.src==69.171.250.35

Output: 347 packets captured (From Facebook)

Display Filter: tcp.port==443 && ip.dst==69.171.250.35

Output: 331 packets captured (From Facebook)

1. **To capture all traffic to/from YouTube**

We first find out the YouTube server’s IP using ping youtube.com

Capture Filter: host 142.250.71.46

Output: 524 packets captured

Display Filter: ip.src==142.250.71.46

Output: 310 packets captured

Display Filter: ip.dst== 142.250.71.46

Output: 214 packets captured

**After you run Wireshark with the above capture filters and collect the data, do the following:**

**1. Write a DISPLAY filter expression to count all TCP packets (captured under item #1) that**

**have the flags SYN, PSH, and RST set. Show the fraction of packets that had each flag set.**

**2. Use a DISPLAY filter expression to separate the packets sent by your computer vs. received from Facebook and YouTube in items #2 and #3 above. Show the fractions for each type.**

**Display Filters:**

1. To capture SYN, PUSH, RESET flags in Facebook’s TCP packets

Using the TCP packets collected from facebook, we apply various Display Filter

1. tcp.flags.syn==1 Output: 6 packets captured (0.8%)
2. tcp.flags.push==1 Output: 329 packets captured (46.3%)
3. tcp.flags.reset==1 Output: 3 packets captured (0.4%)
4. tcp.flags.syn==1 && tcp.flags.reset==1 && tcp.flags.push==1 Output: 0 packets (0%)
5. To capture Facebook’s HTTPS packets which are sent vs received in the machine

First find out the IP address of our machine using ifconfig

1. Tcp.port==443 && ip.dst==10.0.2.15 Output: 202 Packets captured (28.4%) (Received from Facebook)
2. Tcp.port==443 && ip.src==10.0.2.15 Output: 119 Packets captured (16.7%)(Sent from machine)

Next, we capture youtube’s packets which are sent vs received in the machine

We use the data captured initially from youtube and perform following display filters

1. Ip.dst==10.0.2.15 Output: 310 packets captured (59.2%) (Received from youtube)
2. Ip.src==10.0.2.15 Output: 214 packets captured (40.8%) (Sent from machine)

**Problem2: - Captured Data Analysis**

**a. Count how many TCP packets you received from / sent to Facebook or YouTube, and how many of each were also HTTP packets.**

**b. Determine if any TCP packets with SYN or PSH flags set were sent from your host or received from Facebook/YouTube.**

**c. Go flag-by-flag and count how many packets have tcp.flags.push set, then how many have tcp.flags.syn set, and finally, how many have tcp.flags.reset set.**

To capture tcp: Display Filter = tcp

To capture https: Display Filter = tcp.port==443

|  |  |  |
| --- | --- | --- |
| Protocol | Facebook | YouTube |
| TCP | 711 | 524 |
| HTTPS | 678 | 524 |

To capture PUSH flags: Display Filter: tcp.flags.push==1

To capture SYN flags: Display Filter: tcp.flags.syn==1

To capture RESET flags: Display Filter: tcp.flags.reset==1

To capture all flags: Display Filter: tcp.flags.syn==1 && tcp.flags.reset==1 && tcp.flags.push==1

|  |  |  |
| --- | --- | --- |
| Flags | Facebook | YouTube |
| SYN | 6 (0.8%) | 0 (0%) |
| PUSH | 329 (46.3%) | 239 (45.6%) |
| RESET | 3 (0.4%) | 0 (0%) |
| ALL | 0 (0%) | 0 (0%) |