ECS 152 Project 1 Part 1

Hammud Haq (996013884) (A03)
Hoai-An Ho (917000915) (A01)

Files: wireshark.py, etrigan.har, peertube.har, tmz.har, videolan.har, youtube.har, etrigan.pcap, peertube.pcap, tmz.pcap, videolan.pcap, youtube.pcap

Answer the following questions:

1. How many UDP and TCP packets did you observe for each website? (3 points)

Website	UDP	TCP	Total
Youtube	115	270	27871
Videolan	28	207	2217
Peertube	89	774	8570
Etrigan News	26	19587	21445
TMZ	3330	77236	1508051

2. How much network traffic (number of packets sent) is secure (HTTPS) vs vulnerable (HTTP) on each site? (https://www.cloudflare.com/learning/ssl/why-is-http-not-secure) (3 points)

Website	HTTP	HTTPS
Youtube	0	70
Videolan	0	76
Peertube	0	57
Etrigan News	0	973
TMZ	1	7006

3. What is the distribution of different types of packets that you observed for each site? Calculate and report the percentage of packets observed for HTTP, HTTPS, DNS, FTP, SSH, DHCP, TELNET, SMTP, POP3, and NTP. (hint: look at port numbers) (6 points)

%/Packet	Youtube	VideoLan	peertube	Etrigan	TMZ
HTTP	0	0	0	0	0.00066310

HTTPS	0.25115	2.07487	0.66511	4.53718	4.6457345
Telnet	0	0	0	0	0
SMTP	0	0	0	0	0
SSH	0	0	0	0	0
POP3	0	0	0	0	0
NTP	0	0	0	0	0
FTP	0	0	0	0	0
DNS	0.0071759	0.63148	.23337	0.041967	0.07758363
DHCP	0	0	0	0	0

4. Report the number of unique destination IP addresses per site. Is there any discernible difference between each site based on the number of destination IP addresses? Do you see any direct relationship between number of destination IP addresses and load time of the site?

Site	# Unique IP addresses
Youtube	53
Videolan	31
Peertube	22
EtriganNews	26
Tmz	286

The load times scale significantly with the number of Unique IPs in between (Especially when using TMZ). Although Youtube was a tad faster than some of the sites with less destination IPs likely due to a variety of factors including distance, and options for traversal for speed

5. List the top 5 destination IP addresses based on the number of packets sent. Can you identify who owns these IP addresses? (hint: making use of Dev Tools and the HAR files generated to determine hostnames of some of the IP addresses can make this easier). (12 points)

(Found in multiple pcap couldn't locate in HAR assuming my own IP)
IP Address: 10.0.0.187 # of packets: 58364
IP Address: 10.0.0.187 # of packets: 15675
IP Address: 10.0.0.187 # of packets: 190
IP Address: 10.0.0.187 # of packets: 118
IP Address: 10.0.0.187 # of packets: 550

Top 5 (Not Including the redundant)
IP Address: 75.101.184.39 # of packets: 3660 (Owned by etriganId)
IP Address: 184.27.199.64 # of packets: 2756 (Owned by tiktok)
IP Address: 108.138.244.149 # of packets: 1063 (Owned by csi.gstatic.com/Google)
IP Address: 104.254.148.251 # of packets: 813 (Owned by yahoo!)
IP Address: 52.94.215.172 # of packets: 620 (Owned By doubleclick)

Top #'s from non-TMZ sources
IP Address: 37.34.60.59 # of packets: 203 (Found in peertube.pcap but not in HAR)
IP Address: 52.8.50.6 # of packets: 95 (Owned by "authority" at fouanalytics)
IP Address: 18.155.202.12 # of packets: 40 (Found in Etrigan.pcap but not in HAR)
IP Address: 142.251.46.226 # of packets: 28 (Google ad services)
IP Address: 195.154.241.219 # of packets: 26 (Found in videolan.pcap but not HAR)
IP Address: 51.104.167.48 # of packets: 23 (Found in Etrigan.pcap but not in HAR)
IP Address: 34.149.211.227 # of packets: 21 (Found in peertube.pcap but not in HAR)
IP Address: 52.5.21.65 # of packets: 20 (Found in peertube.pcap but not in HAR)
IP Address: 20.189.173.6 # of packets: 15 (Found in videolan.pcap but not in HAR)
IP Address: 151.101.42.133 # of packets: 14 (Owned by www.videolan.org)
IP Address: 34.237.34.85 # of packets: 12 (Found in youtube.pcap but not in HAR)

6. Is it possible that different IP addresses are mapped to the same hostname? Can you find an example of this from the sites that you visited and explain why this might be happening. (6 points)

   Yes (found on TMZ)
   108.138.242.159 and 18.155.206.31 are owned by Amazon. They own multiple servers which may have fluctuations in traffic or similar proximity. The connections and IPs may have a TTL that requires them to change. It also serves as a security measure against DDOS attacks