Kerun Chen

916332888

Python file:

MonitoringTraffic.py

Pcap files:

youtube.pcap

videolan.pcap

joinpeertube.pcap

etrigannews.pcap

tmz.pcap

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

   UDP/TCP

   Youtube: 50123/502

   Videolan: 262/3911

   Joinpeertube: 409/17515

   Etrigannews: 853/33506

   Tmz: 23148/78968

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)

   HTTPS/HTTP

Youtube: 228/2

Videoland: 252/1117

Joinpeertube: 6611/13

Etrigannews: 12194/0

Tmz: 30776/30

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)

   % = (HTTP+HTTPS+…+NTP) / total packets *100%

   %youtube: 0.45%

   %videolan: 32.8%

   %joinpeertube: 36.96%

   %etrigannews:35.49%

   %tmz: 30.14%

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?

   Youtube: 12

   Videolan: 9

   Joinpeertube: 15

Etrigannews: 12

Tmz: 240

Shorter PLT with less unique destination IP addresses

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)

Youtube:

- **20.54.25.4 Microsoft Corporation**
- **10.0.0.173: private**
- **224.0.0.251 unknown**
- **151.101.188.193 Fastly**
- **151.101.65.69 Fastly**

Videoland:

- **224.0.0.251 unknown**
- **75.75.75.75 Comcast Cable**
- **10.0.0.173 unknown**
- **62.210.246.226 Free SAS**
- **151.101.188.193 Fastly**

Joinpeertube:

- **10.0.0.173 unknown**
- **62.210.246.226 Free SAS**

- **224.0.0.251 unknown**
- **239.255.255.250 unknown**
- **75.75.76.76 Comcast Cable**

Etrigannews:

- **172.64.108.25 Cloudflare**
- **10.0.0.173 unknown**
- **75.75.75.75 Comcast Cable**
- **54.204.238.15 Amazon.com**
- **151.101.188.193 Fastly**

Tmz:

- **10.0.0.173 unknown**
- **151.101.188.193 Fastly**
- **151.101.65.69 Fastly**
- **151.101.1.69 Fastly**
- **52.25.88.229 Amazon.com**

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. From my data, all IP addresses in 151.101.xxx.xxx format are owned by Fastly. I think it may be for the convenience of management. ISPs can categorize all their addresses for different services.