Network Security - Assignment 6

h.vanhuynegem

June 2025

1 Introduction

2 Data Analysis

2.1 Top Scanners

I identified the top 10 scanner IP addresses by analyzing all TCP SYN (without ACK) and UDP packets in the provided PCAP files. This method accurately captures scanning behavior, since these packets are typical of port and host scanning activity. Table 1 below shows each scanner's packet count and traffic share.

Table 1: Top 10 Scanners by Packet Count

IP Address	**Packets**	**Share (%)**
185.242.226.50	188,293	2.32
185.242.226.46	105,263	1.30
45.14.226.132	74,096	0.91
10.14.176.3	72,407	0.89
10.241.128.246	72,326	0.89
80.75.212.37	59,683	0.74
183.136.225.42	56,189	0.69
212.70.149.138	54,256	0.67
118.123.105.92	51,992	0.64
218.92.0.99	49,420	0.61

2.2 Top Target Ports

I analyzed all TCP SYN (without ACK) and UDP packets to identify the top 10 destination ports targeted by scanners. This approach highlights which services or protocols are most frequently scanned across the dataset. Table 2 and Table 3 below show the most targeted TCP and UDP ports by packet count

Table 2: Top 10 TCP SYN Destination Ports

Port	Packet Count
22	174,938
3389	101,839
80	91,775
8088	82,746
8080	80,344
8728	76,159
5555	69,330
443	53,356
8122	51,620
12103	50,686

Table 3: Top 10 UDP Destination Ports

Port	Packet Count
514	144,733
53	91,131
5060	63,392
1194	40,973
32410	27,957
123	23,558
55001	13,926
1900	13,211
6881	13,013
5353	11,856

2.3 Protocol breakdown

I counted all TCP SYN (without ACK) and UDP packets to compare protocol usage in scanning activity. Figure 1 below shows the relative proportion of TCP SYN and UDP scan attempts. There are 7,411,453 TCP SYN packets, and 698,064 UDP packets.

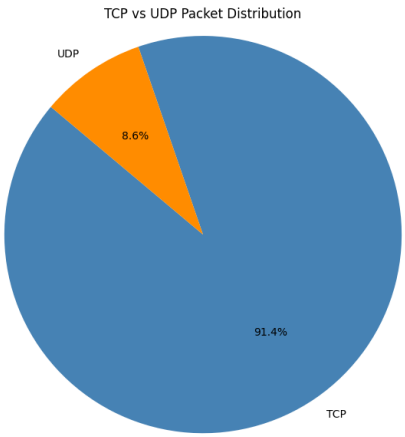

Figure 1: UDP vs TCP packets ratio

2.4 Heavy hitter

I analyzed the scanner with the highest activity, IP address 185.242.226.50. This source generated 188,293 TCP SYN or UDP scan packets, targeting 49,853 unique destination IPs across 4 distinct destination ports. The GeoLite2_City database identified this host as being located in the United States, but external

sources such as AbuseIPDB report the IP as Dutch. This discrepancy likely results from outdated or inconsistent IP geolocation databases, which is common for certain providers or hosting services. Regardless of country, the scanning pattern and wide target range indicate mass, automated reconnaissance rather than a targeted probe. A small summary can be found in Table 4.

Table 4: Heavy Hitter Scanner Summary

Field	**Value**
Heavy Hitter IP Address	185.242.226.50
Total Packets	188,293
Unique Destination IPs	49,853
Unique Destination Ports	4
Country	United States

3 Visualization

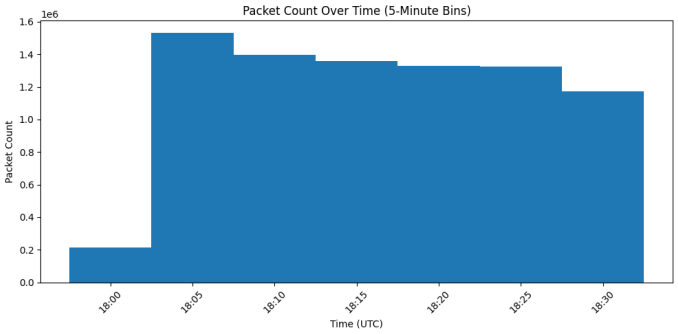

Figure 2: Packet Count over time (5 minute bins)

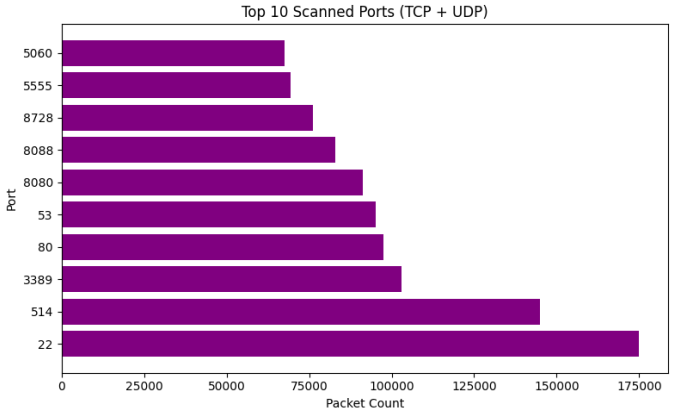

Figure 3: Top 10 scanned ports

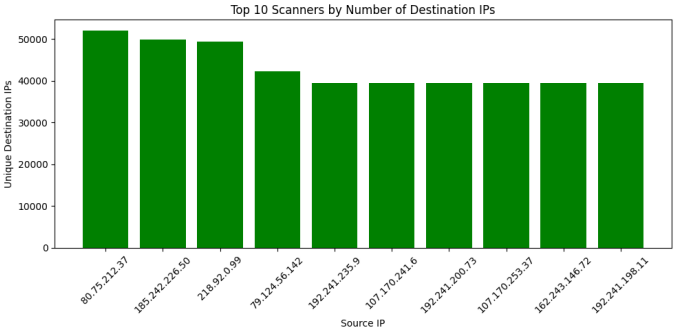

Figure 4: Top 10 scanners sorted by the number of destination IPs

4 Interpretation of results

4.1 Pattern Recognition

Figure 3 reveals a combination of targeted port scanning and broad reconnaissance. The top 10 ports include known service ports like 22 (SSH), 3389 (RDP), and 80 (HTTP), indicating targeted attacks on popular services. However, the inclusion of lesser-used ports such as 8728, 5555, and 5060 suggests some scanners sweep wider port ranges, likely using automated tools.

Figure 2 shows that the scanning pattern over time is mostly steady, with an initial sharp increase followed by consistently high packet counts in each 5-minute bin. This trend points to continuous, automated mass scanning, rather than isolated bursts of manual probing.

Figure 4 supports this, showing that top scanner IPs target tens of thousands

of unique destination IPs, highlighting a widespread, high-volume scanning effort.

4.2 Threat Assessment

The scanner at IP address 185.242.226.50, referenced in subsection 2.4, exhibits typical characteristics of a mass scanner. It sent over 188,000 packets to 49,853 unique IP addresses while targeting only four destination ports, suggesting a broad sweep for specific exposed services. The consistent packet rate and narrow port focus indicate automated behavior, likely driven by a botnet or scanning framework. As shown in Figure 5, the packets are evenly distributed across all four targeted ports, further supporting the hypothesis of systematic, tool-driven scanning.

This scanner poses a moderate to high risk, particularly if commonly exploited services such as SSH (port 22) or RDP (port 3389) are exposed. While this specific host may not carry out direct attacks, it likely collects reconnaissance data for later use by threat actors, who may attempt exploitation, brute-force attacks, or malware deployment based on the discovered vulnerabilities.

Table 5: Mass Scanner

Field	**Value**
IP Address	185.242.226.50
Total Packets	188,293
Unique Destination IPs	49,853
Unique Destination Ports	4

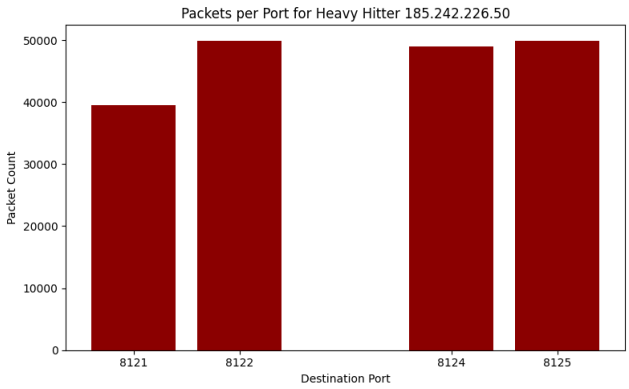

Figure 5: Packets per Port for Mass Scanner 185.242.226.50