

WebStrike Write-up

Hashim Alkhateeb

December 2025

1 Scenario

A suspicious file was identified on a company web server, raising alarms within the intranet. The Development team flagged the anomaly, suspecting potential malicious activity. To address the issue, the network team captured critical network traffic and prepared a PCAP file for review.

Your task is to analyze the provided PCAP file to uncover how the file appeared and determine the extent of any unauthorized activity.

Question 1: Identifying the geographical origin of the attack facilitates the implementation of geo-blocking measures and the analysis of threat intelligence. From which city did the attack originate?

To start, I opened the PCAP file with Wireshark and sorted by time. The PCAP file had two unique IP addresses so I had to do distinguish who the attacker and the target were. 24.49.63.79 used port 80, so this is the web server and 117.11.80.124 is the client using random high ports. From the scenario, we know the suspicious file was found on the company's web server so 117.11.80.124 is the attacker. I looked up this IP on iplocation.net to identify the city.

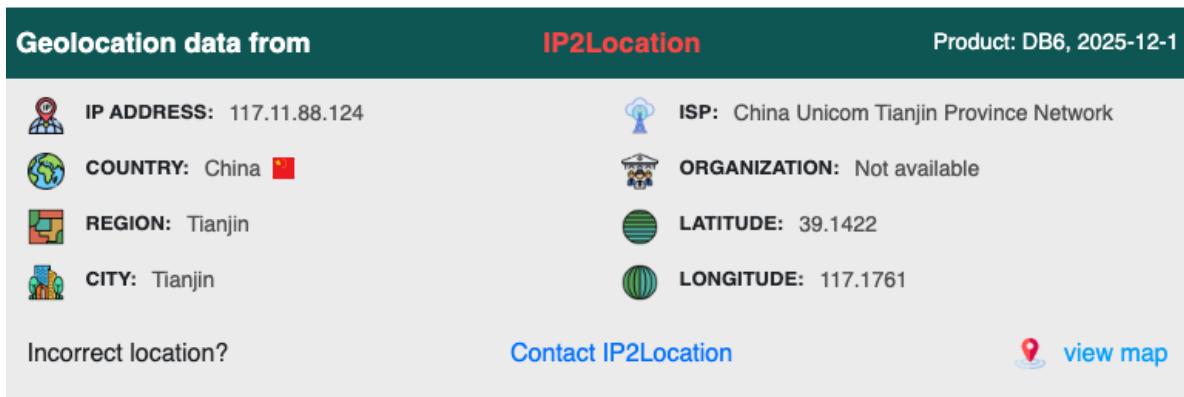


Figure 1: City name identified as Tainjin.

No.	Time	Source	Destination	Protocol	Length	Destination Port	Source Port	Info
1	0.000000	117.11.88.124	24.49.63.79	TCP	74	80	43848	43848 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=643822874 TSecr=0 WS=128
2	0.000024	24.49.63.79	117.11.88.124	TCP	66	80	43848	80 - 43848 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM Tsvl=3033491050 TSecr=643822874
3	0.000426	117.11.88.124	24.49.63.79	HTTP	66	80	43848	GET / HTTP/1.1 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=643822874 TSecr=3033491050
5	0.004936	24.49.63.79	117.11.88.124	TCP	66	80	43848	80 - 43848 [ACK] Seq=1 Ack=338 Win=64896 Len=0 Tsvl=3033491055 TSecr=643822879
6	0.005337	24.49.63.79	117.11.88.124	HTTP	796	43848	80	HTTP/1.1 200 OK (text/html)
7	0.005404	24.49.63.79	117.11.88.124	TCP	66	80	43848	80 - 43848 [ACK] Seq=1 Ack=731 Win=64128 Len=0 Tsvl=643822879 TSecr=3033491055
8	0.037487	117.11.88.124	24.49.63.79	HTTP	356	80	43848	GET /favicon.ico HTTP/1.1
9	0.037886	24.49.63.79	117.11.88.124	HTTP	557	43848	80	43848 - 80 [ACK] Seq=338 Ack=282 Win=64128 Len=0 Tsvl=643822958 TSecr=3033491088
10	0.038344	117.11.88.124	24.49.63.79	TCP	66	80	43848	80 - 43848 [ACK] Seq=1 Ack=1222 Win=64128 Len=0 Tsvl=643822958 TSecr=3033491088
11	4.435385	117.11.88.124	24.49.63.79	HTTP	66	80	43848	HTTP/1.1 200 OK (text/html)
12	4.435764	24.49.63.79	117.11.88.124	HTTP	843	43848	80	43848 - 80 [ACK] Seq=1095 Ack=1999 Win=64128 Len=0 Tsvl=643827310 TSecr=3033495486
13	4.435855	117.11.88.124	24.49.63.79	TCP	66	80	43848	80 - 43848 [ACK] Seq=1095 Ack=1999 Win=64128 Len=0 Tsvl=643827310 TSecr=3033495486
14	4.458038	117.11.88.124	24.49.63.79	HTTP	382	80	43848	GET /products/images/product1.jpg HTTP/1.1
15	4.458219	117.11.88.124	24.49.63.79	TCP	74	80	60240	60240 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=643827332 TSecr=0 WS=128
16	4.458304	24.49.63.79	117.11.88.124	TCP	74	60240	80	80 - 60240 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM Tsvl=3033495508 TSecr=643827332
17	4.458334	24.49.63.79	117.11.88.124	HTTP	347	43848	80	HTTP/1.1 200 OK (text/html)
18	4.458402	117.11.88.124	24.49.63.79	TCP	66	80	60240	60240 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=643827332 TSecr=3033495508
19	4.458504	117.11.88.124	24.49.63.79	HTTP	382	80	60240	GET /products/images/product2.jpg HTTP/1.1

Figure 2: Identify attacker and target IPs.

Question 2: Knowing the attacker's User-Agent assists in creating robust filtering rules. What's the attacker's Full User-Agent?

To solve this, I used CTRL + f to search the entirety of the PCAP file. I changed the search settings to *String* and specified I want to look within the *Packet details*. I then entered *agent* and clicked *find*. I found the *User-Agent* field which reveals the attacker is using a Linux OS and Firefox web browser.

Apply a display filter ... <Ctrl-/>								
No.	Time	Source	Destination	Protocol	Length	Destination Port	Source Port	Info
51	26.922295	24.49.63.79	117.11.88.124	TCP	74	46796	80	80 - 48796 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM Tsvl=3033517972 TSecr=643849796
52	26.922379	117.11.88.124	24.49.63.79	TCP	66	80	48796	48796 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=643849796 TSecr=3033517972
+ 53	26.922481	117.11.88.124	24.49.63.79	HTTP	1384	80	48796	POST /reviews/upload.php HTTP/1.1 (application/x-php)
54	26.922547	24.49.63.79	117.11.88.124	TCP	66	48796	80	80 - 48796 [ACK] Seq=1 Ack=1239 Win=64128 Len=0 Tsvl=3033517972 TSecr=643849796
55	26.923526	24.49.63.79	117.11.88.124	HTTP	290	48796	80	HTTP/1.1 200 OK (text/html)
56	26.92366	117.11.88.124	24.49.63.79	TCP	66	80	48796	48796 - 80 [ACK] Seq=1239 Ack=225 Win=64128 Len=0 Tsvl=643849797 TSecr=3033517974
57	31.924151	117.11.88.124	24.49.63.79	TCP	66	80	48796	48796 - 80 [ACK] Seq=1239 Ack=225 Win=64128 Len=0 Tsvl=643849797 TSecr=3033517974
58	31.924190	24.49.63.79	117.11.88.124	TCP	66	48796	80	80 - 48796 [ACK] Seq=1239 Ack=225 Win=64128 Len=0 Tsvl=643849797 TSecr=3033517974
59	31.924533	117.11.88.124	24.49.63.79	TCP	66	80	48796	48796 - 80 [ACK] Seq=1240 Ack=226 Win=64128 Len=0 Tsvl=643849798 TSecr=3033522974
60	49.757762	117.11.88.124	24.49.63.79	TCP	74	80	47580	47580 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=643872631 TSecr=0 WS=128
61	49.757925	24.49.63.79	117.11.88.124	TCP	74	47580	80	80 - 47580 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM Tsvl=3033540808 TSecr=643872631
62	49.758019	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=643872632 TSecr=3033540808
63	49.758143	117.11.88.124	24.49.63.79	HTTP	1382	80	47580	POST /reviews/upload.php HTTP/1.1 (application/x-php)
64	49.758306	24.49.63.79	117.11.88.124	TCP	66	47580	80	80 - 47580 [ACK] Seq=1 Ack=1237 Win=64128 Len=0 Tsvl=3033540808 TSecr=643872632
65	49.758395	117.11.88.124	24.49.63.79	HTTP	296	47580	80	80 - 47580 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
67	49.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
68	49.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
69	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
70	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
71	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
72	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
73	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
74	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
75	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
76	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
77	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
78	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
79	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
80	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
81	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
82	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
83	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
84	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
85	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
86	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
87	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
88	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
89	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
90	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
91	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
92	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
93	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
94	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
95	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
96	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
97	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
98	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
99	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
100	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
101	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
102	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
103	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
104	54.758588	117.11.88.124	24.49.63.79	TCP	66	80	47580	47580 - 80 [ACK] Seq=237 Ack=231 Win=64128 Len=0 Tsvl=643872633 TSecr=0 WS=128
105	54.758588	117.11.88.124	24.49.63.79					

Question 3: We need to determine if any vulnerabilities were exploited. What is the name of the malicious web shell that was successfully uploaded?

I used the filter `http.request.method == "GET"` to get all http traffic using the GET method. As the results were quite small, I looked for the file name that appeared the most suspicious and it was clear as day.

http.request.method == "GET"						
	Packet details	Narrow & Wide	<input type="checkbox"/> Case sensitive	String	.php	
No.	Time	Source	Destination	Protocol	Length	Info
4	0.004826	117.11.88.124	24.49.63.79	HTTP	403	GET / HTTP/1.1
8	0.037487	117.11.88.124	24.49.63.79	HTTP	356	GET /favicon.ico HTTP/1.1
11	4.435305	117.11.88.124	24.49.63.79	HTTP	444	GET /products/ HTTP/1.1
14	4.458038	117.11.88.124	24.49.63.79	HTTP	382	GET /products/images/product1.jpg HTTP/1.1
19	4.458504	117.11.88.124	24.49.63.79	HTTP	382	GET /products/images/product2.jpg HTTP/1.1
33	12.739450	117.11.88.124	24.49.63.79	HTTP	450	GET /about/ HTTP/1.1
43	18.514912	117.11.88.124	24.49.63.79	HTTP	449	GET /reviews/ HTTP/1.1
73	57.538074	117.11.88.124	24.49.63.79	HTTP	416	GET /admin/uploads HTTP/1.1
83	63.058836	117.11.88.124	24.49.63.79	HTTP	410	GET /uploads HTTP/1.1
93	69.755241	117.11.88.124	24.49.63.79	HTTP	409	GET /admin/ HTTP/1.1
103	75.201187	117.11.88.124	24.49.63.79	HTTP	418	GET /reviews/uploads HTTP/1.1
107	75.207010	117.11.88.124	24.49.63.79	HTTP	419	GET /reviews/uploads/ HTTP/1.1
109	75.228143	117.11.88.124	24.49.63.79	HTTP	376	GET /icons/blank.gif HTTP/1.1
114	75.228890	117.11.88.124	24.49.63.79	HTTP	375	GET /icons/back.gif HTTP/1.1
121	75.229218	117.11.88.124	24.49.63.79	HTTP	377	GET /icons/image2.gif HTTP/1.1
138	84.150547	117.11.88.124	24.49.63.79	HTTP	480	GET /reviews/uploads/image.jpg.php HTTP/1.1
326	288.389226	117.11.88.124	24.49.63.79	HTTP	470	GET /reviews/uploads/ HTTP/1.1
330	288.400569	117.11.88.124	24.49.63.79	HTTP	427	GET /icons/blank.gif HTTP/1.1
335	288.401559	117.11.88.124	24.49.63.79	HTTP	426	GET /icons/back.gif HTTP/1.1
340	288.401886	117.11.88.124	24.49.63.79	HTTP	428	GET /icons/image2.gif HTTP/1.1

Figure 4: File Found: **image.jpg.php**

Question 4: Identifying the directory where uploaded files are stored is crucial for locating the vulnerable page and removing any malicious files. Which directory is used by the website to store the uploaded files?

I used the same method as question 3. The malicious file was located in `"/reviews/uploads/"`.

Question 5: Which port, opened on the attacker's machine, was targeted by the malicious web shell for establishing unauthorized outbound communication?

Since this questions asks for the port of the attacker, I used the filter `"ip.src == 117.11.88.124"` and filtered the source ports. I noticed the src ports were either high random ports or port **8080**.

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
153 93.976854	117.11.88.124	24.49.63.79	24.49.63.79	TCP	66	8088	54448	8088 - 54448 [ACK] Seq=17 Ack=209 Win=6524 Len=0 Tsvl=643916851 Tscr=3033585027
151 88.915996	117.11.88.124	24.49.63.79	24.49.63.79	TCP	75	8088	54448	8088 - 54448 [ACK] Seq=8 Ack=67 Win=65152 Len=0 Tsvl=643916850 Tscr=3033579963
150 88.913133	117.11.88.124	24.49.63.79	24.49.63.79	TCP	66	8088	54448	8088 - 54448 [ACK] Seq=8 Ack=67 Win=65152 Len=0 Tsvl=643911787 Tscr=3033579963
148 88.912954	117.11.88.124	24.49.63.79	24.49.63.79	TCP	73	8088	54448	8088 - 54448 [PSH, ACK] Seq=1 Ack=56 Win=65152 Len=7 Tsvl=643911786 Tscr=3033575205
145 88.912034	117.11.88.124	24.49.63.79	24.49.63.79	TCP	66	8088	54448	8088 - 54448 [ACK] Seq=1 Ack=56 Win=65152 Len=0 Tsvl=643907628 Tscr=3033575205
144 84.154674	117.11.88.124	24.49.63.79	24.49.63.79	TCP	66	8088	54448	8088 - 54448 [SYN, ACK] Seq=0 Ack=1 Win=643897028 MSS=1460 SACK PERM Tsvl=643897028 Tscr=3033575205
141 84.154398	117.11.88.124	24.49.63.79	24.49.63.79	TCP	66	80240	89	60240 - 89 [ACK] Seq=1 Ack=1 Win=643897028 Len=0 Tsvl=643897028 Tscr=303356899
28 9.459011	117.11.88.124	24.49.63.79	24.49.63.79	TCP	66	60240	89	60240 - 89 [ACK] Seq=17 Ack=283 Win=642128 Len=0 Tsvl=643832333 Tscr=3033495509
24 9.459118	117.11.88.124	24.49.63.79	24.49.63.79	TCP	66	60240	89	60240 - 89 [ACK] Seq=317 Ack=283 Win=642128 Len=0 Tsvl=643827333 Tscr=3033495509
19 4.458504	117.11.88.124	24.49.63.79	24.49.63.79	HTTP	382	60240	89	GET /products/images/product2.jpg HTTP/1.1
18 4.458402	117.11.88.124	24.49.63.79	24.49.63.79	TCP	66	60240	89	60240 - 89 [ACK] Seq=1 Ack=Win=64256 Len=0 Tsvl=643827332 Tscr=3033495508
15 4.458210	117.11.88.124	24.49.63.79	24.49.63.79	TCP	74	60240	89	60240 - 89 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERN Tsvl=643827332 Tscr=0 WS=128
99 74.756019	117.11.88.124	24.49.63.79	24.49.63.79	TCP	66	59350	89	59350 - 89 [ACK] Seq=345 Ack=494 Win=64128 Len=0 Tsvl=64397639 Tscr=3033565806
97 69.755666	117.11.88.124	24.49.63.79	24.49.63.79	TCP	74	59350	89	59350 - 89 [ACK] Seq=344 Ack=493 Win=64128 Len=0 Tsvl=643897630 Tscr=3033560806
96 69.755692	117.11.88.124	24.49.63.79	24.49.63.79	TCP	66	59350	89	59350 - 89 [ACK] Seq=344 Ack=493 Win=64128 Len=0 Tsvl=64392629 Tscr=3033560806
93 69.755241	117.11.88.124	24.49.63.79	24.49.63.79	HTTP	409	59350	89	GET /admin/ HTTP/1.1
92 68.863873	117.11.88.124	24.49.63.79	24.49.63.79	TCP	66	59350	89	59350 - 89 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=643891738 Tscr=3033559914
90 68.863612	117.11.88.124	24.49.63.79	24.49.63.79	TCP	74	59350	89	59350 - 89 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERN Tsvl=643891737 Tscr=0 WS=128
89 68.060787	117.11.88.124	24.49.63.79	24.49.63.79	TCP	66	59348	89	59348 - 89 [ACK] Seq=346 Ack=494 Win=64128 Len=0 Tsvl=643899935 Tscr=3033559111
87 68.060534	117.11.88.124	24.49.63.79	24.49.63.79	TCP	66	59348	89	59348 - 89 [FIN, ACK] Seq=345 Ack=493 Win=64128 Len=0 Tsvl=643899934 Tscr=3033554109

Figure 5: Filtering for attacker IP address and source ports.

Question 6: Recognizing the significance of compromised data helps prioritize incident response actions. Which file was the attacker attempting to exfiltrate?

I used the filter "ip.src == 117.11.88.124 && tcp.srcport == 8080" to filter for attacker traffic using the port we found from question 5. I selected a packet and followed the tcp stream which showed the commands the attacker executed.

```
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ uname -a
Linux ubuntu-virtual-machine 6.2.0-37-generic #38~22.1
$ pwd
/var/www/html/reviews/uploads
$ ls /home
ubuntu
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
```

Figure 6: The attacker attempted to access /etc/passwd