

001 - Webstrike

Overview

- **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.
- **Skills Covered:** IP address lookup (Geolocation), User-Agent Identify, Exploits finding

Tools Used

- Wireshark - PCAP (Packet Capture)

Questions

1. Identifying the geographical origin of the attack

I saw the IP 117.11.88.124 is asking for something related to admin. I know something's off here. It's an attacker that's why I put it into IP address lookup.

70	57.535331	117.11.88.124	24.49.63.79	TCP	74	36270 → 80 [SYN] Seq=0 Win=64240 Len=0
71	57.535455	24.49.63.79	117.11.88.124	TCP	74	80 → 36270 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
72	57.535544	117.11.88.124	24.49.63.79	TCP	66	36270 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
+	73	57.538074	117.11.88.124	HTTP	416	GET /admin/uploads HTTP/1.1
	74	57.538175	24.49.63.79	TCP	66	80 → 36270 [ACK] Seq=1 Ack=351 Win=64240 Len=0
	75	57.538483	24.49.63.79	HTTP	558	HTTP/1.1 404 Not Found (text/html)
	76	57.538547	117.11.88.124	TCP	66	36270 → 80 [ACK] Seq=351 Ack=493 Win=64240 Len=0
	77	62.538698	117.11.88.124	TCP	66	36270 → 80 [FIN, ACK] Seq=351 Ack=493 Win=64240 Len=0
	78	62.538853	24.49.63.79	TCP	66	80 → 36270 [ACK] Seq=493 Ack=351 Win=64240 Len=0

▶ Frame 73: 416 bytes on wire (3328 bits), 416 bytes captured (3328 bits) on interface 0

▶ Ethernet II, Src: VMware_c0:00:09 (00:50:56:c0:00:09), Dst: VMware_61:97:cd (00:0c:29:61:97:cd)

▶ Internet Protocol Version 4, Src: 117.11.88.124, Dst: 24.49.63.79

▶ Transmission Control Protocol, Src Port: 36270, Dst Port: 80, Seq: 1, Ack: 1, Len: 350

▶ Hypertext Transfer Protocol

▶ GET /admin/uploads HTTP/1.1\r\nHost: shoporoma.com\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\n\r\n[Full request URI: http://shoporoma.com/admin/uploads]\r\n[HTTP request 1/1]\r\n[Response in frame: 75]


So it's in China.

1 / 3

Geolocation data from

IP2Location

Product: DB6, 2025-7-15

 IP ADDRESS: 117.11.88.124

 COUNTRY: China 


 REGION: Tianjin

 CITY: Tianjin

 ISP: China Unicom Tianjin Province Network

 ORGANIZATION: Not available

 LATITUDE: 39.1422

 LONGITUDE: 117.1761

Incorrect location?

Contact IP2Location

 view map

2. Attacker's User-Agent

Knowing which browser attacker is using can provide some information.

```
HyperText Transfer Protocol
GET /admin/uploads HTTP/1.1\r\n
Host: shoporoma.com\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
```

3. Malicious web shell

A web shell is a shell-like interface that enables a web server to be remotely accessed, often for the purposes of cyberattacks. A web shell is unique in that a web browser is used to interact with it. Web shells are most commonly written in PHP

We know web shell are commonly in PHP. Use filter to find it.

Packet list	Narrow & Wide	Case sensitive	String	php
Time	Source	Destination	Protocol	Length Info
136 83.726034	24.49.63.79	117.11.88.124	TCP	74 80 → 46658 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK PERM
137 83.726135	117.11.88.124	24.49.63.79	TCP	66 46658 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=643906600 TSecr=30
138 84.150547	117.11.88.124	24.49.63.79	HTTP	480 GET /reviews/uploads/image.jpg.php HTTP/1.1
139 84.150705	24.49.63.79	117.11.88.124	TCP	66 80 → 46658 [ACK] Seq=1 Ack=415 Win=64768 Len=0 TSval=3033575201 TSecr=30
140 84.153968	24.49.63.79	117.11.88.124	TCP	74 54448 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSval=3033575201 TSecr=30
141 84.154398	117.11.88.124	24.49.63.79	TCP	74 8080 → 54448 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK PERM TSval=3033575201 TSecr=30
142 84.154497	24.49.63.79	117.11.88.124	TCP	66 54448 → 8080 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3033575205 TSecr=30
143 84.154602	24.49.63.79	117.11.88.124	TCP	121 54448 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=55 TSval=3033575205 TSecr=30
144 84.154674	117.11.88.124	24.49.63.79	TCP	66 8080 → 54448 [ACK] Seq=1 Ack=56 Win=65152 Len=0 TSval=643907028 TSecr=30
145 88.912034	117.11.88.124	24.49.63.79	TCP	73 8080 → 54448 [PSH, ACK] Seq=1 Ack=56 Win=65152 Len=7 TSval=643911786 TSecr=30
146 88.912162	24.49.63.79	117.11.88.124	TCP	66 54448 → 8080 [ACK] Seq=56 Ack=8 Win=64256 Len=0 TSval=3033579962 TSecr=30
147 88.912892	24.49.63.79	117.11.88.124	TCP	75 54448 → 8080 [PSH, ACK] Seq=56 Ack=8 Win=64256 Len=9 TSval=3033579962 TSecr=30
148 88.912954	117.11.88.124	24.49.63.79	TCP	66 8080 → 54448 [ACK] Seq=8 Ack=65 Win=65152 Len=0 TSval=643911787 TSecr=30
149 88.913086	24.49.63.79	117.11.88.124	TCP	68 54448 → 8080 [PSH, ACK] Seq=65 Ack=8 Win=64256 Len=2 TSval=3033579962 TSecr=30
150 88.913133	117.11.88.124	24.49.63.79	TCP	66 8080 → 54448 [ACK] Seq=8 Ack=67 Win=65152 Len=0 TSval=643911787 TSecr=30
151 93.975996	117.11.88.124	24.49.63.79	TCP	75 8080 → 54448 [PSH, ACK] Seq=8 Ack=67 Win=65152 Len=9 TSval=643916850 TSecr=30
152 93.976778	24.49.63.79	117.11.88.124	TCP	208 54448 → 8080 [PSH, ACK] Seq=67 Ack=17 Win=64256 Len=142 TSval=303358158 TSecr=30
153 93.976854	117.11.88.124	24.49.63.79	TCP	66 8080 → 54448 [ACK] Seq=17 Ack=209 Win=65024 Len=0 TSval=643916851 TSecr=30
154 93.976974	24.49.63.79	117.11.88.124	TCP	68 54448 → 8080 [PSH, ACK] Seq=209 Ack=17 Win=64256 Len=2 TSval=303358515 TSecr=30
155 93.977043	117.11.88.124	24.49.63.79	TCP	66 8080 → 54448 [ACK] Seq=17 Ack=211 Win=65024 Len=0 TSval=643916851 TSecr=30
156 94.151927	117.11.88.124	24.49.63.79	TCP	66 [TCP Keep-Alive] 46658 → 80 [ACK] Seq=414 Ack=1 Win=64256 Len=0 TSval=643916851 TSecr=30
157 94.152025	24.49.63.79	117.11.88.124	TCP	66 [TCP Keep-Alive ACK] 80 → 46658 [ACK] Seq=1 Ack=415 Win=64768 Len=0 TSval=643916851 TSecr=30
158 104.301002	117.11.88.124	24.49.63.79	TCP	66 [TCP Keep-Alive] 46658 → 80 [ACK] Seq=414 Ack=1 Win=64256 Len=0 TSval=643916851 TSecr=30

Frame 138: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface
Ethernet II, Src: VMware c0:00:09 (00:50:56:c0:00:09), Dst: VMware 61:97:cd (00:0c:29:61:97:cd)
Internet Protocol Version 4, Src: 117.11.88.124, Dst: 24.49.63.79
Transmission Control Protocol, Src Port: 46658, Dst Port: 80, Seq: 1, Ack: 1, Len: 414
HyperText Transfer Protocol
GET /reviews/uploads/image.jpg.php HTTP/1.1\r\nHost: shoporoma.com\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\nReferer: http://shoporoma.com/reviews/uploads/\r\nUpgrade-Insecure-Requests: 1\r\n\r\n[Full request URI: http://shoporoma.com/reviews/uploads/image.jpg.php]
[HTTP request 1/1]

4. Exfiltrated file

We know in HTTP POST is data sending, use filter to find it.

Apply a display filter ... <Ctrl-/>

Packet list		Narrow & Wide		Case sensitive	String	post
No.	Time	Source	Destination	Protocol	Length	Info
265	191.372502	117.11.88.124	24.49.63.79	TCP	66	8080 → 54448 [ACK] Seq=100 Ack=3377 Win=64128 Len=0 TS
266	191.372570	24.49.63.79	117.11.88.124	TCP	67	54448 → 8080 [PSH, ACK] Seq=3377 Ack=100 Win=64256 Len
267	191.372660	24.49.63.79	117.11.88.124	HTTP	228	POST / HTTP/1.1 (application/x-www-form-urlencoded)
268	191.372667	117.11.88.124	24.49.63.79	TCP	66	8080 → 54448 [ACK] Seq=100 Ack=3378 Win=64128 Len=0 TS
269	191.372708	24.49.63.79	117.11.88.124	TCP	69	54448 → 8080 [PSH, ACK] Seq=3378 Ack=100 Win=64256 Len
270	191.372725	117.11.88.124	24.49.63.79	TCP	66	443 → 54438 [ACK] Seq=1 Ack=163 Win=65024 Len=0 TSval=
271	191.372794	117.11.88.124	24.49.63.79	TCP	66	8080 → 54448 [ACK] Seq=100 Ack=3381 Win=64128 Len=0 TS
272	191.373055	117.11.88.124	24.49.63.79	TCP	264	443 → 54438 [PSH, ACK] Seq=1 Ack=163 Win=65024 Len=198
273	191.373138	24.49.63.79	117.11.88.124	TCP	66	54438 → 443 [ACK] Seq=163 Ack=199 Win=64128 Len=0 TSva
274	191.373284	24.49.63.79	117.11.88.124	TCP	67	54448 → 8080 [PSH, ACK] Seq=3381 Ack=100 Win=64256 Len
275	191.373358	117.11.88.124	24.49.63.79	TCP	66	8080 → 54448 [ACK] Seq=100 Ack=3382 Win=64128 Len=0 TS
276	191.373414	24.49.63.79	117.11.88.124	TCP	74	54448 → 8080 [PSH, ACK] Seq=3382 Ack=100 Win=64256 Len
277	191.373476	117.11.88.124	24.49.63.79	TCP	66	8080 → 54448 [ACK] Seq=100 Ack=3390 Win=64128 Len=0 TS
278	191.373542	24.49.63.79	117.11.88.124	TCP	67	54448 → 8080 [PSH, ACK] Seq=3390 Ack=100 Win=64256 Len
279	191.373595	117.11.88.124	24.49.63.79	TCP	66	8080 → 54448 [ACK] Seq=100 Ack=3391 Win=64128 Len=0 TS
280	191.373644	24.49.63.79	117.11.88.124	TCP	68	54448 → 8080 [PSH, ACK] Seq=3391 Ack=100 Win=64256 Len
281	191.373697	117.11.88.124	24.49.63.79	TCP	66	8080 → 54448 [ACK] Seq=100 Ack=3393 Win=64128 Len=0 TS
282	191.373772	24.49.63.79	117.11.88.124	TCP	67	54448 → 8080 [PSH, ACK] Seq=3393 Ack=100 Win=64256 Len
283	191.373826	117.11.88.124	24.49.63.79	TCP	66	8080 → 54448 [ACK] Seq=100 Ack=3394 Win=64128 Len=0 TS
284	191.373873	24.49.63.79	117.11.88.124	TCP	68	54448 → 8080 [PSH, ACK] Seq=3394 Ack=100 Win=64256 Len
285	191.373926	117.11.88.124	24.49.63.79	TCP	66	8080 → 54448 [ACK] Seq=100 Ack=3396 Win=64128 Len=0 TS
286	191.374002	24.49.63.79	117.11.88.124	TCP	67	54448 → 8080 [PSH, ACK] Seq=3396 Ack=100 Win=64256 Len
287	191.374056	117.11.88.124	24.49.63.79	TCP	66	8080 → 54448 [ACK] Seq=100 Ack=3397 Win=64128 Len=0 TS

▶ Frame 267: 228 bytes on wire (1824 bits), 228 bytes captured (1824 bits)

▶ Ethernet II, Src: VMware 61:97:cd (00:0c:29:61:97:cd), Dst: VMware_c0:00:09 (00:50:56:c0:00:09)

▶ Internet Protocol Version 4, Src: 24.49.63.79, Dst: 117.11.88.124

▶ Transmission Control Protocol, Src Port: 54438, Dst Port: 443, Seq: 1, Ack: 1, Len: 162

▶ Hypertext Transfer Protocol

▶ HTML Form URL Encoded: application/x-www-form-urlencoded

▶ Form item: "/etc/passwd" = ""

Key: /etc/passwdValue:

WebStrike Lab

Category: Network Forensics

Tactics: Initial Access Execution Persistence Command and Control Exfiltration

Tool: Wireshark

Easy Retired 30mins 4.6

Bookmark Join the Lab Squad Report an Issue Share Achievement

Machine RegionUSA East

Start Lab Machine

6 / 6 Questions100% Completed

Official walkthroughView

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.

6/6 Questions