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

---

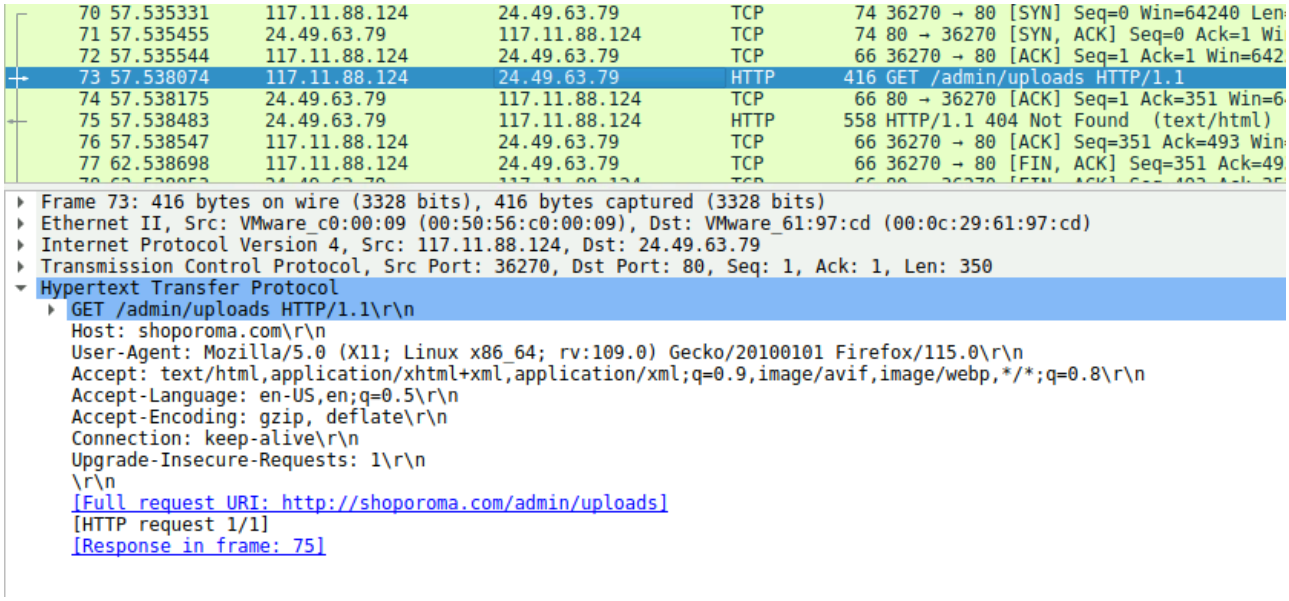
Tools Used

- Wireshark - PCAP (Packet Capture)

Questions

1. **Identifying the geographical origin of the attack**

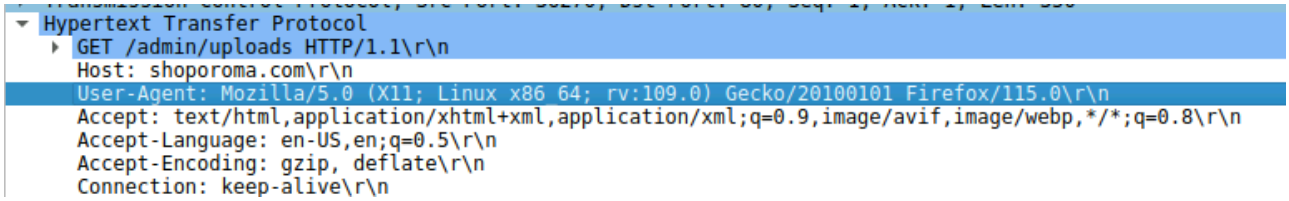
   I saw the IP 117.11.88.124 is asking for something related to admin. I know something's off here. It's an attacker that's why I put it into IP address lookup.



   So it's in China.

2. **Attacker's User-Agent**

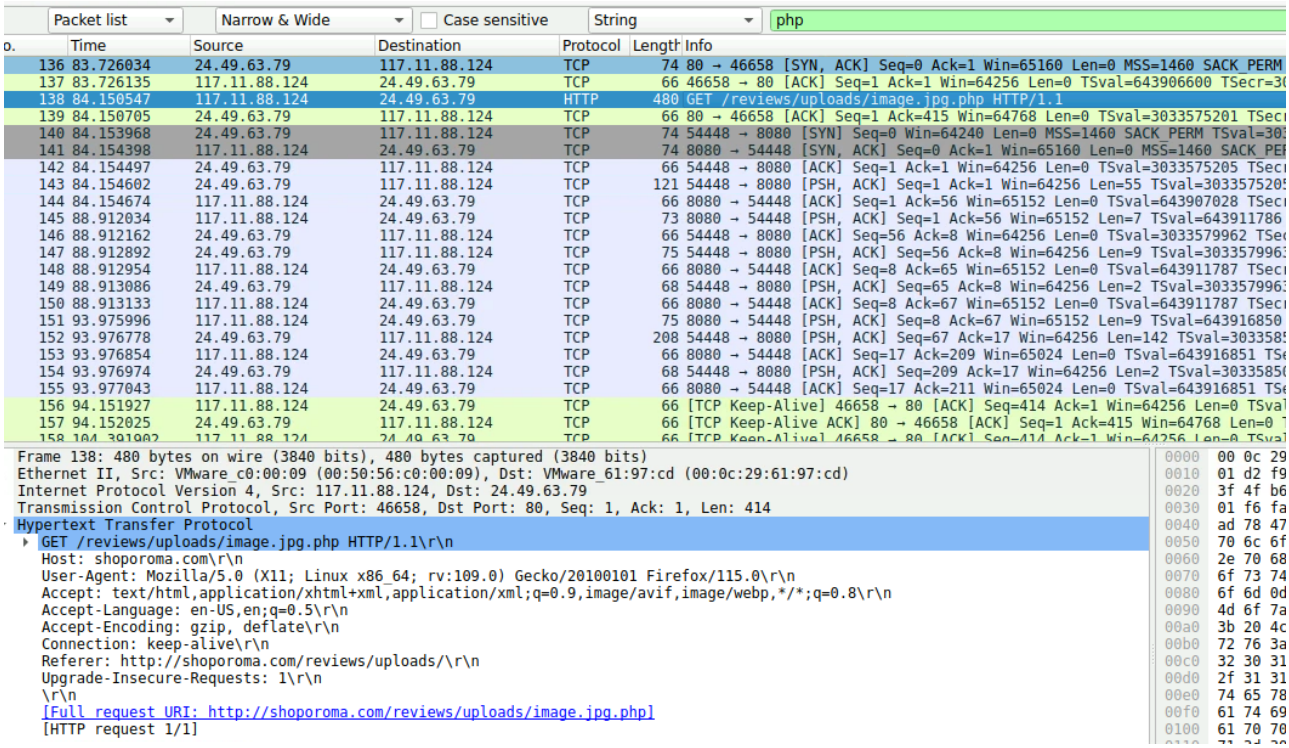
   Knowing which browser attacker is using can provide some information.



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.



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/passwd
      Value:
```

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 Region: USA East

Start Lab Machine

6 / 6 Questions

100% Completed

Official walkthrough — View

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