Tomcat Takeover Lab

Platform: cyberdefenders

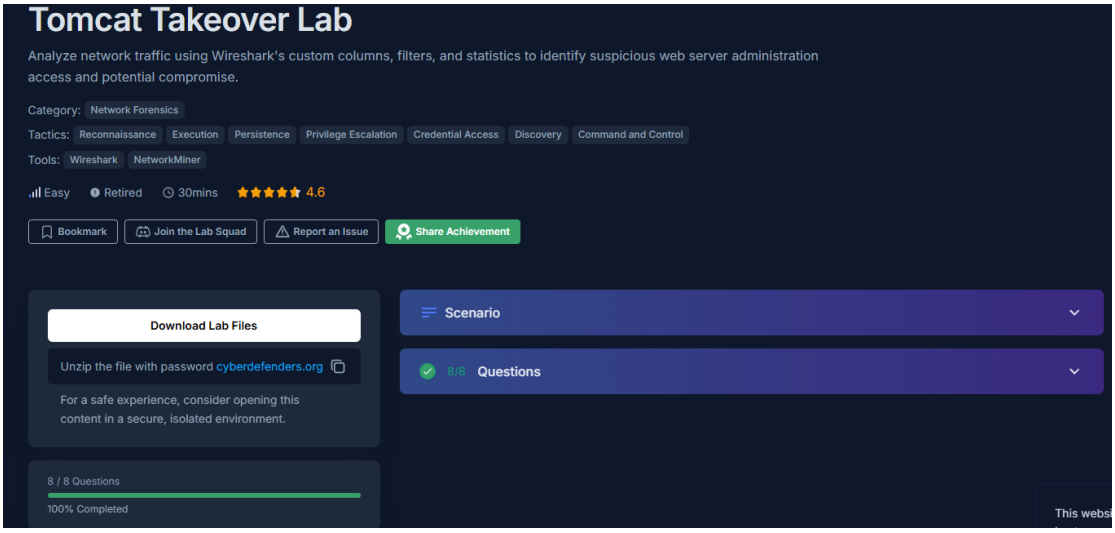
Frome: Asem Reda

Diploma: Cybersecurity 87

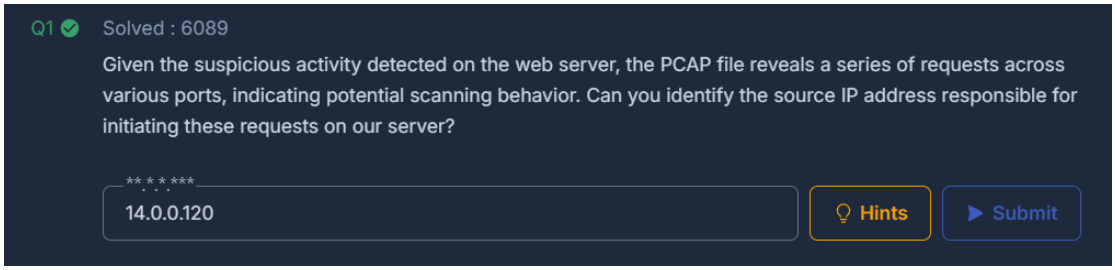
Challenge link: https://cyberdefenders.org/blueteam-ctf-challenges/tomcat-/takeover

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.



First question:



Solution method:

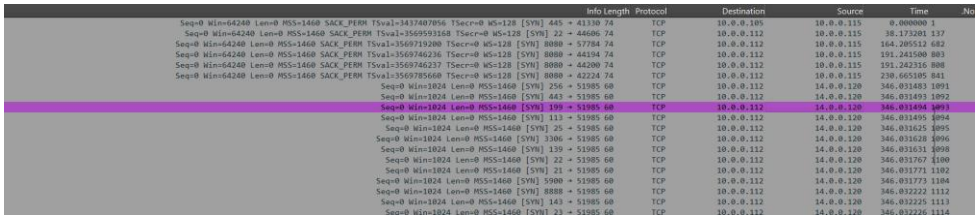
Using the" tcp.flags.syn==1 && tcp.flags.ack==0" filter

to identify who is attempting port scanning. The basis of this process is

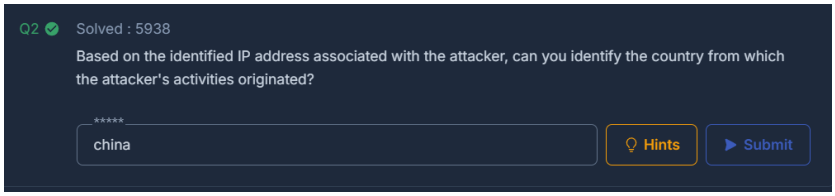
(TCP 3-Way Handshake), which detects which IP address is attempting to open multiple ports

on different ports

in a short period of time

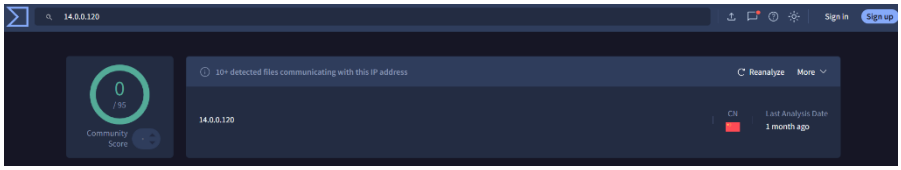


Second question:

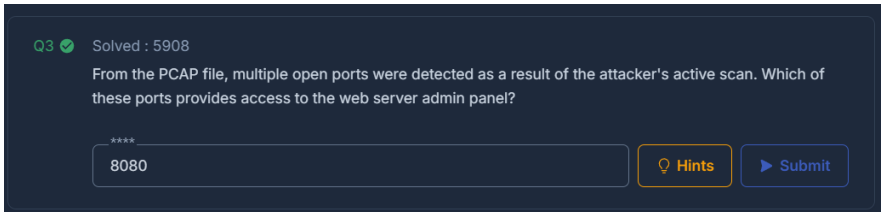


Solution method:

Go to the VirusTotal website and enter the IP address to find the country it belongs to



Third question:

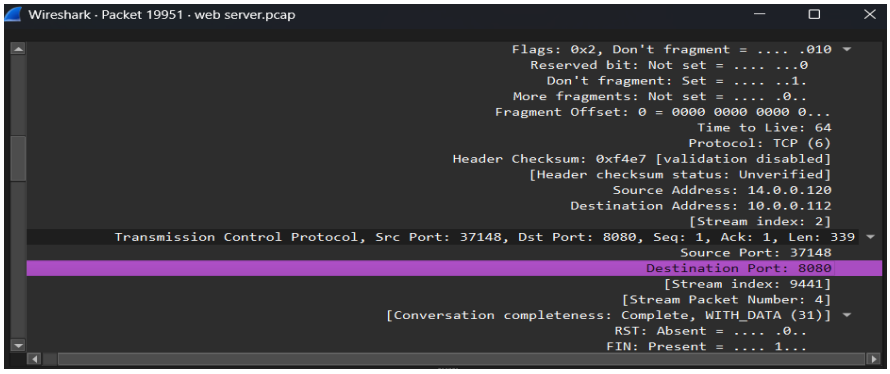


Solution method:

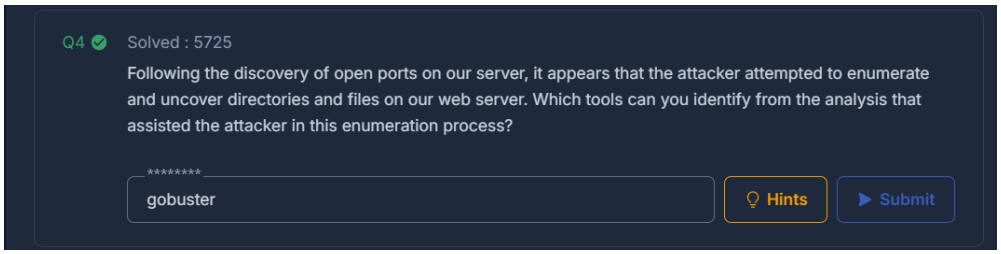
Using the filter "ip.src_host== 14.0.0.120 && ip.dst_host==10.0.0.112 && http"

This narrows down the search to the attacker's IP and the server's IP. The Tomcat admin panel is a web page, therefore

It operates on the HTTP or HTTPS protocol, and that's why we used HTTP, Then we look for the port number

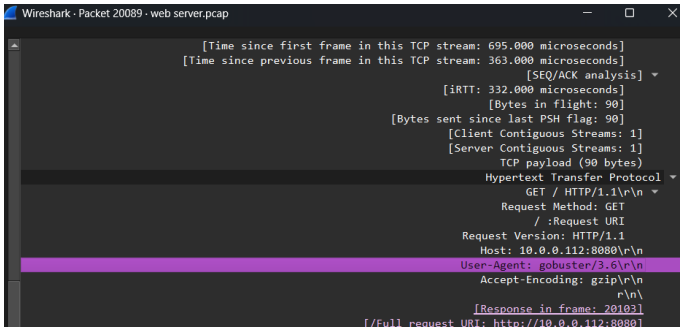


Fourth question:

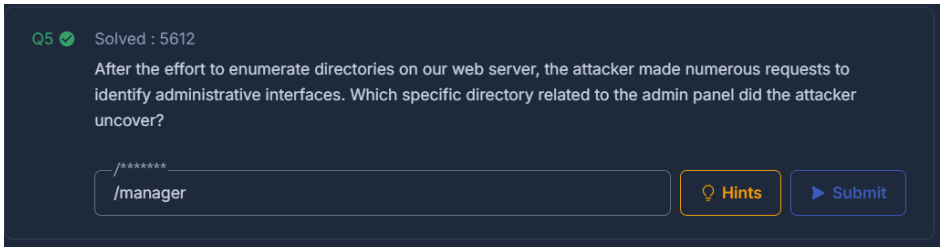


Solution method:

Using the same filter as in the previous question To access any packet, go to Hypertext Transfer Protocol → GET→ User-Agent



Fifth question:



Solution method:

By using the filter:

http.request.uri contains "manager"

Wireshark will focus only on URLs that contain the word “manager.”

You’ll notice many logs because the attacker tried multiple paths related to administrative interfaces. However, the path that was actually discovered and accessed is the Tomcat Manager interface.

The targeted directory is:

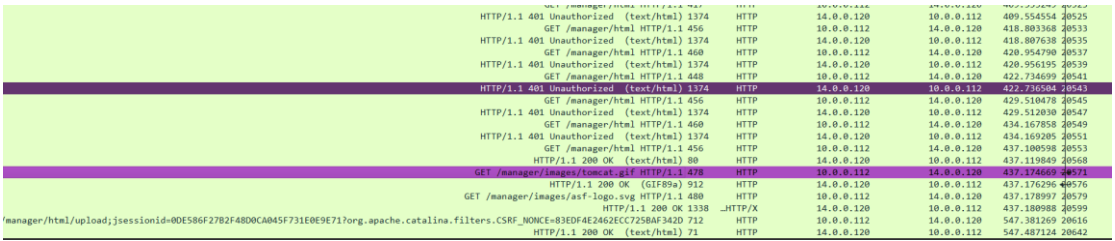
/manager/html

Indicators of actual discovery:

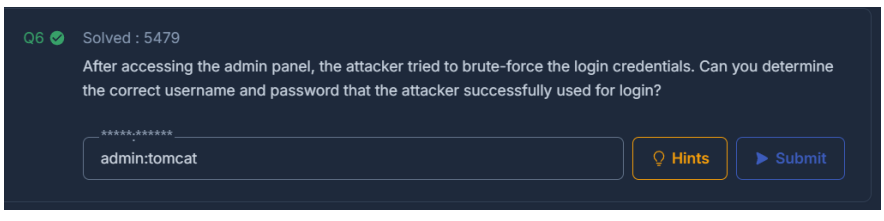
Repeated GET requests to /manager/html returning 401 Unauthorized confirm that the interface exists but requires authentication.

Later, an HTTP/1.1 200 OK response appears, followed by the loading of resources from /manager/images/..., which confirms that the attacker successfully accessed the Manager interface.

Finally, there is a POST /manager/html/upload request that returned 200 OK, which is evidence that the attacker used the Manager panel to upload applications.



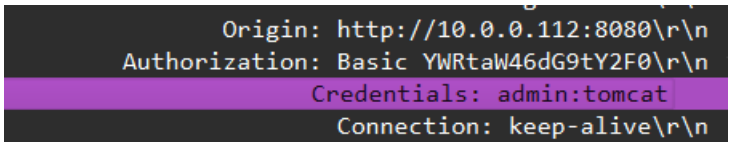
Sixth question:



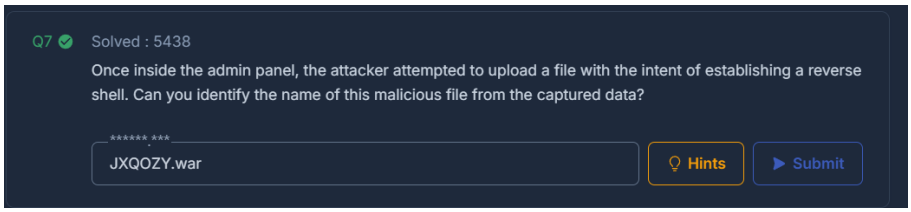
Solution method:

By accessing the file download packages filtered using the previous question, we find in the Authorization: Basic dG9tY2F0OnMzY3JldA==,

Why this package specifically? Because the attacker was able to obtain the username and password, log in, and download the file



Seventh question:

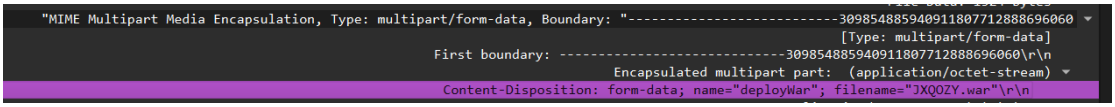


Solution method:

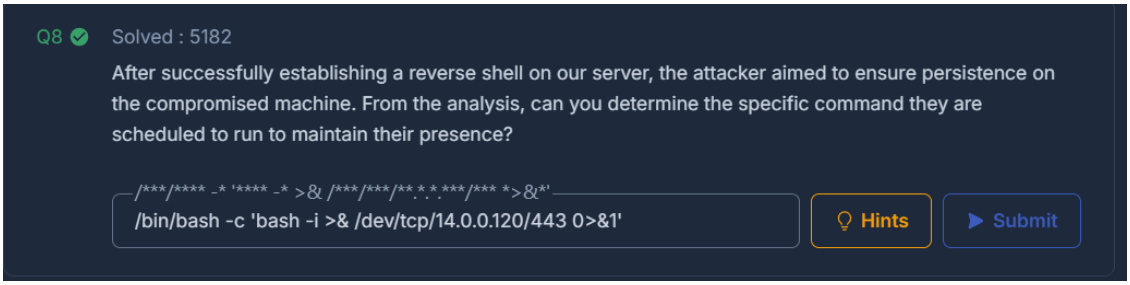
By accessing the file download packages filtered using the previous question, we will find in the list

MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary

This malicious file's name



Eighth question:



Solution method:

Using the filter "ip.src == <Attacker_IP> && tcp.flags == 0x012"

SYN = 0x002 -

ACK = 0x010 -

This allows us to focus on the SYN+ACK packets coming from the attacker, which confirms that a TCP connection has been established with the server

This is done using a **3-Way Handshake** application.