



W9D1

«DISCOVERING» DI UN OS LINUX IN RETE

La traccia

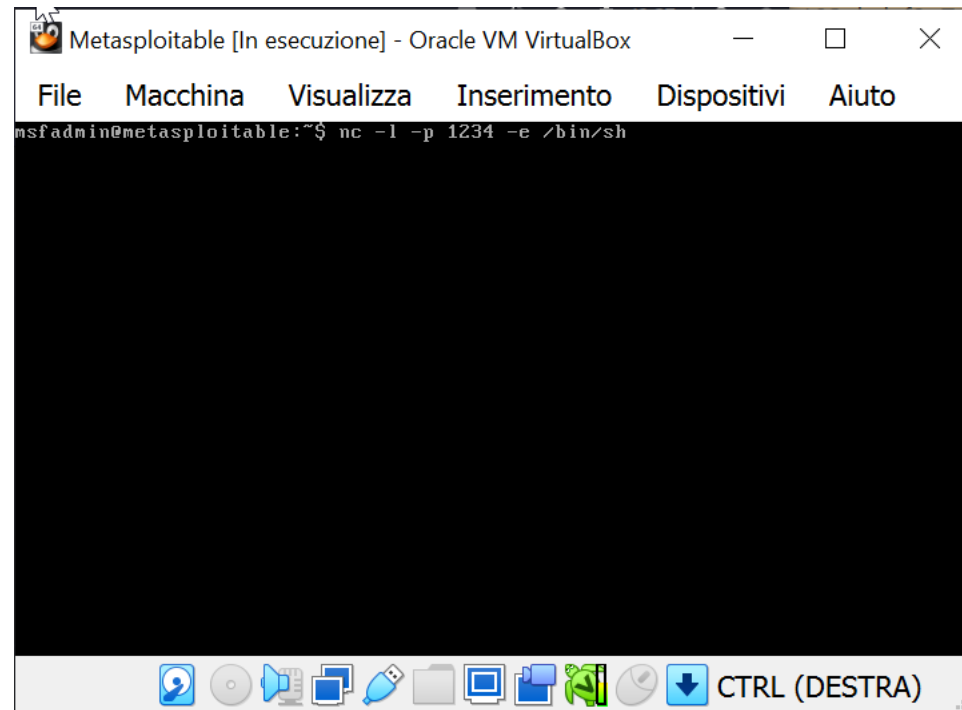
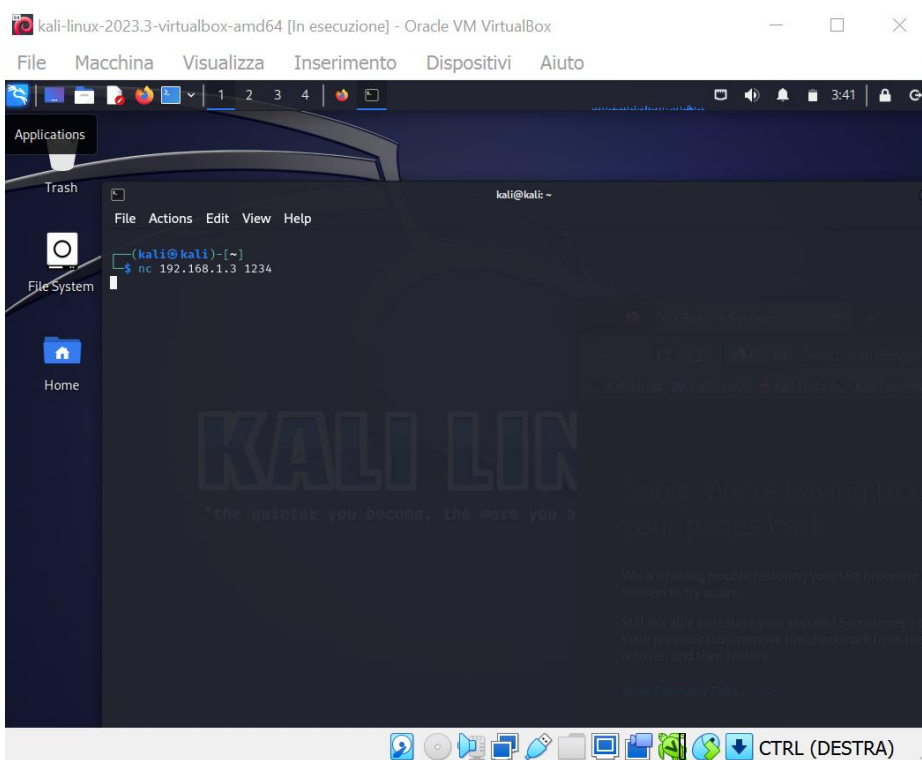
La traccia prevede di svolgere un esercizio di discovering seguendo i seguenti steps:

Proseguiamo per step al fine di estrapolare le seguenti informazioni:

- 1. informazioni di sistema**
- 2. Esplorazione del file system**
- 3. Processi in esecuzione**
- 4. Risorse di rete**
- 5. Utenti e autorizzazioni**

Connessione tra le due macchine virtuali: client e server

Per simulare una connessione tra un client e un server utilizzeremo netcat con i seguenti comandi:



1) Informazioni di sistema

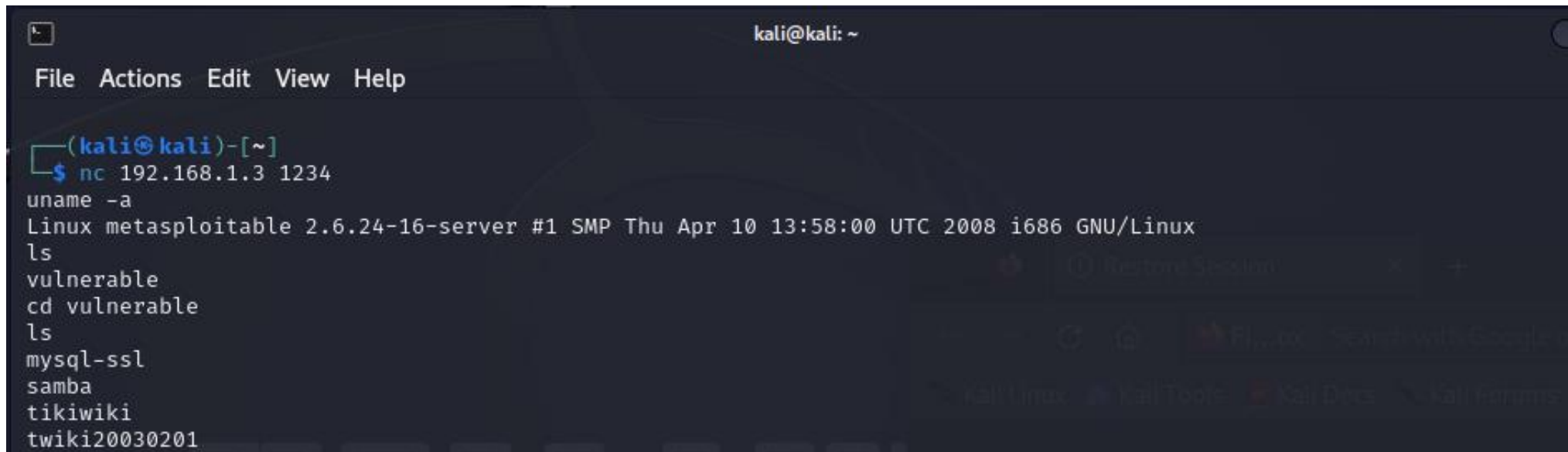
Stabilita la connessione digito il comando da kali(client) per ottenere le informazioni di sistema di metasploitable:

```
(kali@kali)-[~]  
$ nc 192.168.1.3 1234  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Restore Session

2) Esplorazione del file system

Con «ls» e «cd» riusciamo a muoverci all'interno del file system e vedere la composizione di questo su metasploitable:



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc 192.168.1.3 1234  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux  
ls  
vulnerable  
cd vulnerable  
ls  
mysql-ssl  
samba  
tikiwiki  
twiki20030201
```

3) Processi in esecuzione

Con «ls» e cd» riusciamo a muoverci all'interno del file system e vedere la composizione di questo su metaploitable:

```
kali@kali: ~  
File Actions Edit View Help  
twiki20030201  
tree  
ps  
  PID TTY          TIME CMD  
 4767 tty1      00:00:00 bash  
 9844 tty1      00:00:00 sh  
 9859 tty1      00:00:00 ps  
top  
ps aux  
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
root         1  0.0  0.0  2844  1692 ?        Ss   Dec19 0:05   /sbin/init  
root         2  0.0  0.0      0     0 ?        S<   Dec19 0:00   [kthreadd]  
root         3  0.0  0.0      0     0 ?        S<   Dec19 0:00   [migration/0]  
root         4  0.0  0.0      0     0 ?        S<   Dec19 0:00   [ksoftirqd/0]  
root         5  0.0  0.0      0     0 ?        S<   Dec19 0:00   [watchdog/0]  
root         6  0.0  0.0      0     0 ?        S<   Dec19 0:00   [events/0]  
root         7  0.0  0.0      0     0 ?        S<   Dec19 0:00   [khelper]  
root        41  0.0  0.0      0     0 ?        S<   Dec19 0:00   [kblockd/0]  
root        44  0.0  0.0      0     0 ?        S<   Dec19 0:00   [kacpid]  
root        45  0.0  0.0      0     0 ?        S<   Dec19 0:00   [kacpi_notify]  
root        91  0.0  0.0      0     0 ?        S<   Dec19 0:00   [kseriod]  
root       129  0.0  0.0      0     0 ?        S   Dec19 0:00   [pdflush]  
root       130  0.0  0.0      0     0 ?        S   Dec19 0:01   [pdflush]  
root       131  0.0  0.0      0     0 ?        S<   Dec19 0:00   [kswapd0]  
root       173  0.0  0.0      0     0 ?        S<   Dec19 0:00   [aio/0]  
root       1129  0.0  0.0      0     0 ?        S<   Dec19 0:00   [ksnapd]  
root       1298  0.0  0.0      0     0 ?        S<   Dec19 0:00   [ata/0]  
root       1301  0.0  0.0      0     0 ?        S<   Dec19 0:00   [ata_aux]  
root       1310  0.0  0.0      0     0 ?        S<   Dec19 0:00   [scsi_eh_0]  
root       1311  0.0  0.0      0     0 ?        S<   Dec19 0:00   [scsi_eh_1]  
root       1334  0.0  0.0      0     0 ?        S<   Dec19 0:00   [ksuspend_usbd]  
root       1337  0.0  0.0      0     0 ?        S<   Dec19 0:00   [khubd]  
root       2087  0.0  0.0      0     0 ?        S<   Dec19 0:00   [scsi_eh_2]  
root       2275  0.0  0.0      0     0 ?        S<   Dec19 0:00   [kjournald]  
root       2429  0.0  0.0  2092  616 ?        S<s  Dec19 0:00   /sbin/udevmd --daemon  
root       2665  0.0  0.0      0     0 ?        S<   Dec19 0:00   [kpsmoused]  
root       3562  0.0  0.0      0     0 ?        S<   Dec19 0:00   [kjournald]  
daemon     3692  0.0  0.0  1836  524 ?        Ss   Dec19 0:00   /sbin/portmap  
dhcp       3706  0.0  0.0  2436  608 ?        S<s  Dec19 0:00   dhclient3 -e IF_METRIC=100 -pf /var/run/dhclient.eth0.p
```

```
kali@kali: ~  
File Actions Edit View Help  
s-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.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/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap  
root       4602  0.0  0.0  2052  480 ?        S   Dec19 0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/common  
s-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.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/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap  
tomcat55  4604  0.0  4.8 372700 100088 ?        S1  Dec19 0:33 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/common  
s-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.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/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap  
root       4622  0.0  0.1 10596 2564 ?        Ss   Dec19 0:00 /usr/sbin/apache2 -k start  
www-data  4623  0.0  0.0 10596 1952 ?        S   Dec19 0:00 /usr/sbin/apache2 -k start  
www-data  4625  0.0  0.0 10596 1952 ?        S   Dec19 0:00 /usr/sbin/apache2 -k start  
www-data  4628  0.0  0.0 10596 1952 ?        S   Dec19 0:00 /usr/sbin/apache2 -k start  
www-data  4630  0.0  0.0 10596 1952 ?        S   Dec19 0:00 /usr/sbin/apache2 -k start  
www-data  4633  0.0  0.0 10596 1952 ?        S   Dec19 0:00 /usr/sbin/apache2 -k start  
root       4641  0.0  1.2 66344 26476 ?        S1  Dec19 0:00 /usr/bin/rmiregistry  
root       4645  0.0  0.1 12208 2572 ?        S1  Dec19 0:04 ruby /usr/sbin/druby.timeserver.rb  
root       4651  0.0  0.1 8540 2368 ?        S   Dec19 0:10 /usr/bin/unrealircd  
root       4659  0.0  0.0 2568 1196 tty1    Ss   Dec19 0:00 /bin/login --  
root       4663  0.0  0.5 14036 12012 ?        S   Dec19 0:18 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  
daemon    4668  0.0  0.0 2316 216 ?        SN   Dec19 0:00 distccd --daemon --user daemon --allow 0.0.0.0/0  
root       4674  0.0  0.0 2724 1188 ?        S   Dec19 0:00 /bin/sh /root/.vnc/xstartup  
root       4677  0.0  0.1 5936 2572 ?        S   Dec19 0:00 xterm -geometry 80x24+10+10 -ls -title X Desktop  
root       4680  0.0  0.2 8988 4992 ?        S   Dec19 0:12 fluxbox  
root       4712  0.0  0.0 2852 1548 pts/0  Ss+  Dec19 0:00 -bash  
msfadmin  4767  0.0  0.0 4616 1992 tty1    S   Dec19 0:00 -bash  
postfix   7957  0.0  0.0 5420 1644 ?        S   Dec19 0:00 pickup -l -t fifo -u -c  
msfadmin  9844  0.0  0.0 4264 1444 tty1    R+   00:26 0:00 sh  
msfadmin  9861  0.0  0.0 2644 1008 tty1    R+   00:28 0:00 ps aux
```

4) Risorse di rete

Tramite «ifconfig» vedo la configurazione della macchina target:

```
(kali@kali)-[~/Downloads]
$ nc 192.168.1.11 1234
ss
State      Recv-Q Send-Q      Local Address:Port      Peer Address:Port
ESTAB      0      0          192.168.1.11:1234      192.168.1.12:33222
ifconfig
eth0       Link encap:Ethernet  HWaddr 08:00:27:a9:45:82
          inet addr:192.168.1.11  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea9:4582/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:803 errors:0 dropped:0 overruns:0 frame:0
          TX packets:593 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:75894 (74.1 KB)  TX bytes:55581 (54.2 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:29705 (29.0 KB)  TX bytes:29705 (29.0 KB)
```

5) Utenti e autorizzazioni

Tramite i file «group» e «passwd» vedo gli utenti della macchina target, per le autorizzazioni posso vederle sui singoli file vedendo i dettagli delle info di questi.

```
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
```

```
ls
vulnerable
cd vulnerable
ls
vulnerable
cd vulnerable
ls
mysql-ssl
samba
tikiwiki
twiki20030201
ls -l tikiwiki
total 30144
-rw-r--r-- 1 msfadmin msfadmin 10784297 2008-04-08 21:43 tikiwiki-1.9.11.zip
-rw-r--r-- 1 msfadmin msfadmin 10451264 2006-06-11 11:30 tikiwiki-1.9.4.zip
-rw-r--r-- 1 msfadmin msfadmin 9577201 2006-09-05 17:07 tikiwiki-1.9.5.zip
```

```
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:
libuid: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
```