W9D1 - Pratica (1)

>>>>>>>>>NETCAT<<<<<<<<

DATA

Cybersecurity Analyst

Studente:
Andrea Scarmagnani
Docente:
Giuseppe Placanica

Traccia:
Collegamento tra due macchine una (KALI) e una (METASPLOITABLE-2) tramite NETCAT.
Esercitazione di DISCOVERING nel sistema LINUX.

Obbiettivo:
Ottenere informazioni sensibili e identificare i processi in esecuzione esplorando il sistema operativo.

Elenco degli STEP:
1) Informazioni di sistema;
2) Esplorazione del file system
3) Processi in esecuzione,
4) Risorse di rete;
5) Utenti e autorizzazioni;

ESECUZIONE:
1) Preparo il collegamento con NETCAT nella macchina METASPLOITABLE:
   a.
```
msfadmin@metasploitable:~$ nc -l -p 1234 -e /bin/sh
```

2) Avvio collegamento dalla macchina KALI:
   a.
```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.1.76 1234
```
   b. Una volta avviato non riceverai nessun messaggio ma un semplice puntatore che è andato a capo
```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.1.76 1234
```

1) Informazioni di sistema:
```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.1.76 1234
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

2) Esplorazione del file system:

Con il comando ls, vedo le cartelle presenti:
```
ls
vulnerable
```

Comando pwd:
```
pwd
/home/msfadmin
```

Comando whoami:
```
whoami
msfadmin
```

Comando find -name *pass*:
```
find -name *pass*
./vulnerable/samba/3.0.20/debs/libpam-smbpass_3.0.20-0.1ubuntu1_i386.deb
./vulnerable/samba/3.0.6/debs/libpam-smbpass_3.0.6-0.1ubuntu1_i386.deb
./vulnerable/twiki20030201/twiki-source/bin/installpasswd
./vulnerable/twiki20030201/twiki-source/bin/passwd
./vulnerable/twiki20030201/twiki-source/data/.htpasswd
./vulnerable/twiki20030201/twiki-source/templates/oopsregpasswd.tmpl
./vulnerable/twiki20030201/twiki-source/templates/oopswrongpassword.tmpl
./vulnerable/twiki20030201/twiki-source/templates/oopschangepasswd.tmpl
./vulnerable/twiki20030201/twiki-source/templates/oopsresetpasswd.tmpl
```

Comando mkdir:

```
mkdir KALI
ls
KALI
vulnerable
```

Comando cat:

```
ls > Comando_LS.TXT
cat ComandoLS.TXT
ls
Comando_LS.TXT
KALI
vulnerable
cat Comando_LS.TXT
Comando_LS.TXT
KALI
vulnerable
```

con il comando ls>ComandoLS.TXT ho creato un file e con cat l'ho letto

3) Processi in esecuzione:

Comando top: (non restituisce nulla)

Comando ps:

```
ps
  PID TTY          TIME CMD
 5138 tty1     00:00:00 bash
 5140 tty1     00:00:00 sh
 5162 tty1     00:00:00 ps
```

Processi attivi

Comando ps aux: elenco di tutti i processi .

```
ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3   2712  1736 ?        Ss   14:04   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   14:04   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   14:04   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   14:04   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   14:04   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   14:04   0:00 [migration/1]
root         7  0.0  0.0      0     0 ?        S<   14:04   0:00 [ksoftirqd/1]
root         8  0.0  0.0      0     0 ?        S<   14:04   0:00 [watchdog/1]
root         9  0.0  0.0      0     0 ?        S<   14:04   0:00 [events/0]
root        10  0.0  0.0      0     0 ?        S<   14:04   0:00 [events/1]
root        11  0.0  0.0      0     0 ?        S<   14:04   0:00 [khelper]
root        46  0.0  0.0      0     0 ?        S<   14:04   0:00 [kblockd/0]
root        47  0.0  0.0      0     0 ?        S<   14:04   0:00 [kblockd/1]
root        50  0.0  0.0      0     0 ?        S<   14:04   0:00 [kacpid]
root        51  0.0  0.0      0     0 ?        S<   14:04   0:00 [kacpi_notify]
root        97  0.0  0.0      0     0 ?        S<   14:04   0:00 [kseriod]
root       141  0.0  0.0      0     0 ?        S    14:04   0:00 [pdflush]
root       142  0.0  0.0      0     0 ?        S    14:04   0:00 [pdflush]
root       143  0.0  0.0      0     0 ?        S<   14:04   0:00 [kswapd0]
root       185  0.0  0.0      0     0 ?        S<   14:04   0:00 [aio/0]
root       186  0.0  0.0      0     0 ?        S<   14:04   0:00 [aio/1]
```

4) Risorse di rete con NETSTAT:

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.1.76 1234
netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.1.76:1234       kali.fritz.box:32878    ESTABLISHED
udp        0      0 localhost:49050         localhost:49050         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    5916     @/com/ubuntu/upstart
unix  2      [ ]         DGRAM                    6150     @/org/kernel/udev/udevd
unix  14     [ ]         DGRAM                    11159    /dev/log
unix  2      [ ]         DGRAM                    13794
unix  2      [ ]         DGRAM                    13497
unix  2      [ ]         DGRAM                    13490
unix  3      [ ]         STREAM     CONNECTED     12489    /tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     12488
unix  3      [ ]         STREAM     CONNECTED     12487    /tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     12486
unix  2      [ ]         DGRAM                    12460
unix  2      [ ]         DGRAM                    12420
unix  2      [ ]         DGRAM                    12209
unix  2      [ ]         DGRAM                    12147
unix  3      [ ]         STREAM     CONNECTED     12138
```

Risorse di rete con IFCONFIG:

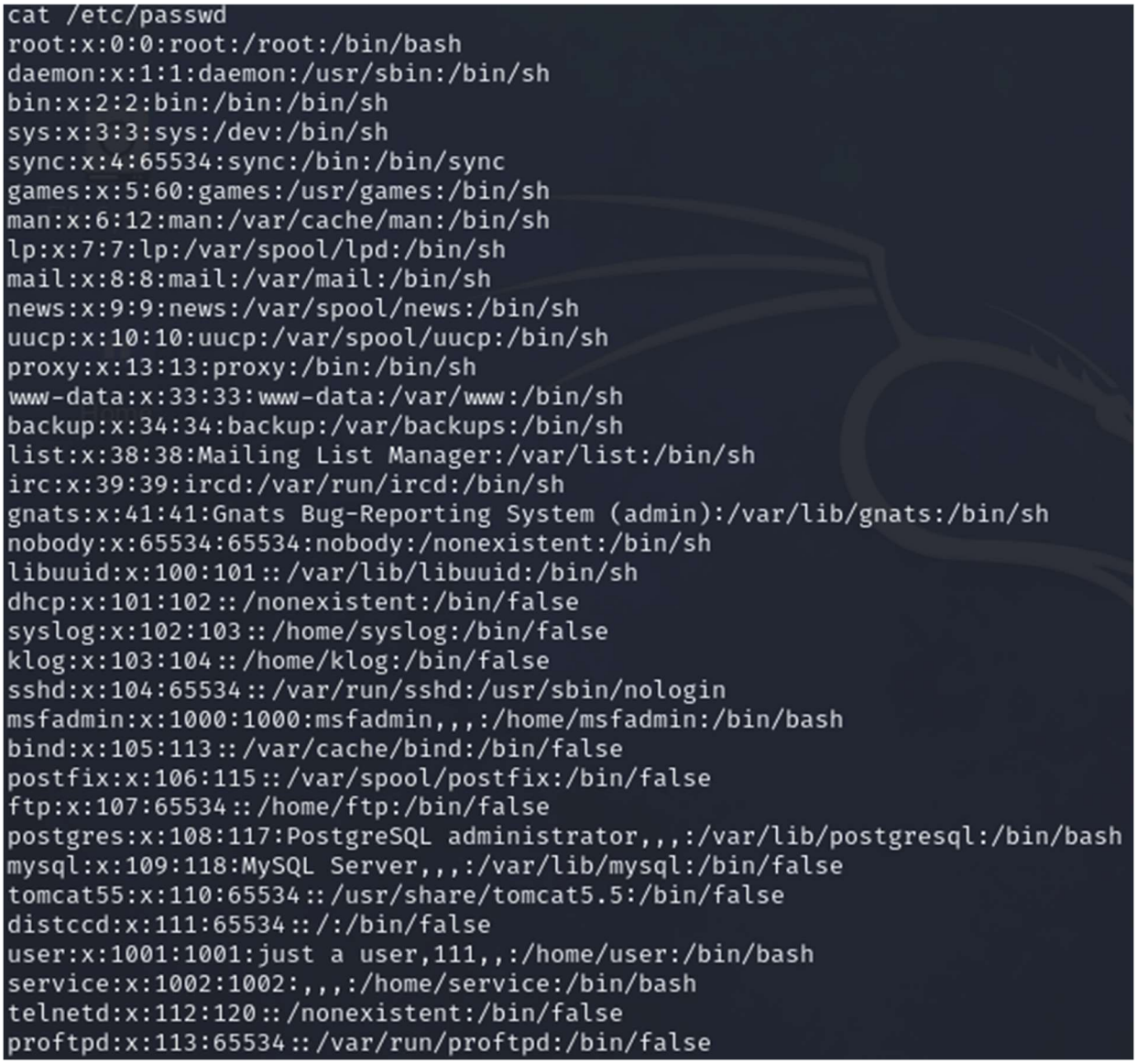
```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:40:10:30
          inet addr:192.168.1.76  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fd00::a00:27ff:fe40:1030/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe40:1030/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21544 errors:0 dropped:0 overruns:0 frame:0
          TX packets:528 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3385172 (3.2 MB)  TX bytes:220835 (215.6 KB)
          Base address:0×d020 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:1026 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1026 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:477393 (466.2 KB)  TX bytes:477393 (466.2 KB)
```

Porte in ascolto:

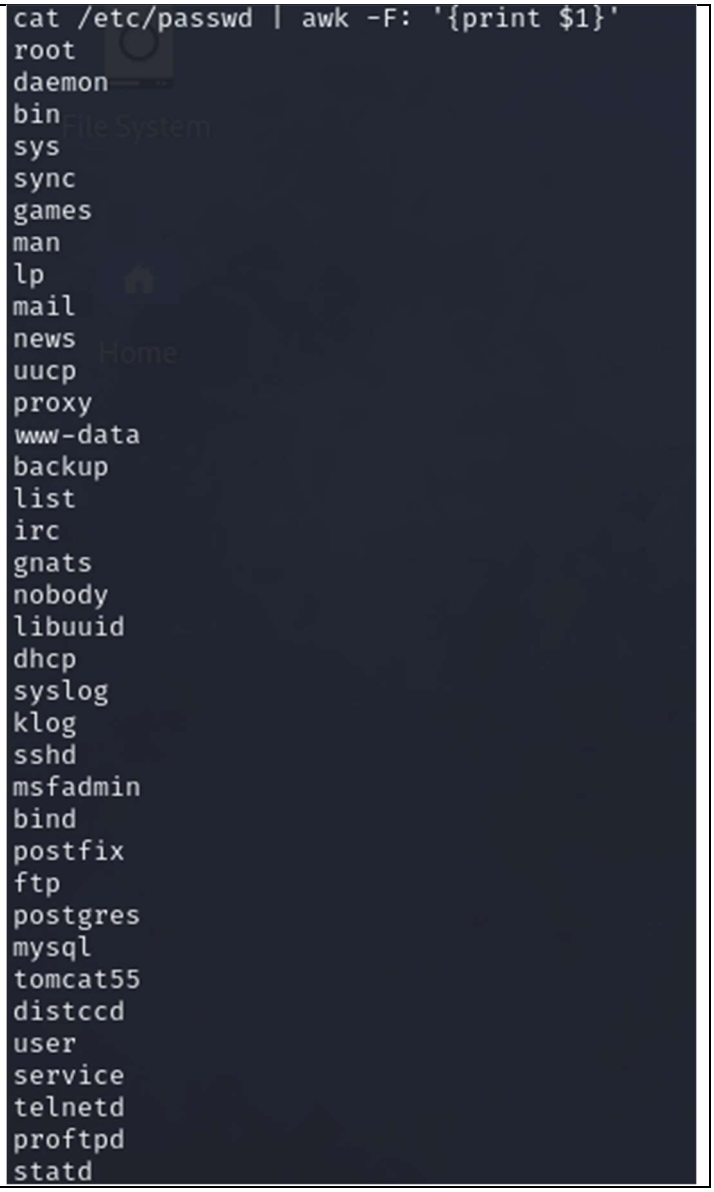
```
netstat -ano | grep "LIST"
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:46890           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:47343           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:8787            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:8180            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 192.168.1.76:53         0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      off (0.00/0/0)
```

5) Utenti e autorizzazioni:

Lista utenti della macchina.



```
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
```

Elenco utenti della macchina:	

Cybersecurity Analyst 2023