



ESERCITAZIONE

n°W9D1 - Pratica

(1)

esercitazione di discovering
usando netcat da kali a kali

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
~  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.242 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::a00:27ff:feb3:f3ba prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:b3:f3:ba txqueuelen 1000 (Ethernet)  
    RX packets 128 bytes 20016 (19.5 KiB)  
    RX errors 0 dropped 57 overruns 0 frame 0  
    TX packets 37 bytes 11072 (10.8 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
~  
$ nc -l -p 1234 -e /bin/bash  
bash: riga 2: whoiam: comando non trovato  
WARNING: No targets were specified, so 0 hosts scanned.  
█
```

**ip kali: 192.168.1.242
server su cui lanciamo
il listen**

ip kali: 192.168.1.67
client da cui ci
colleghiamo alla shel
lanciata sul server.
esecuzione del comando
ps aux in modo da
visualizzare tutti i
processi avviati da ogni
utente sulla macchina

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali) kali-[~]  
$ ping 192.168.1.242  
PING 192.168.1.242 (192.168.1.242) 56(84) bytes of data.  
64 bytes from 192.168.1.242: icmp_seq=1 ttl=64 time=0.325 ms  
64 bytes from 192.168.1.242: icmp_seq=2 ttl=64 time=0.196 ms  
64 bytes from 192.168.1.242: icmp_seq=3 ttl=64 time=0.213 ms  
^X64 bytes from 192.168.1.242: icmp_seq=4 ttl=64 time=0.193 ms  
64 bytes from 192.168.1.242: icmp_seq=5 ttl=64 time=0.178 ms  
^C  
--- 192.168.1.242 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4074ms  
rtt min/avg/max/mdev = 0.178/0.221/0.325/0.053 ms  
  
(kali) kali-[~]  
$ nc 192.168.1.242 1234  
echo "ciao"  
ciao  
whoiam  
ps aux  
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
root         1  0.2  0.3 167672 12376 ?        Ss   21:47   0:00 /sbin/init splash  
root         2  0.0  0.0    0   0 ?        S    21:47   0:00 [kthreadd]  
root         3  0.0  0.0    0   0 ?        I<   21:47   0:00 [rcu_gp]  
root         4  0.0  0.0    0   0 ?        I<   21:47   0:00 [rcu_par_gp]  
root         5  0.0  0.0    0   0 ?        I<   21:47   0:00 [slub_flushwq]  
root         6  0.0  0.0    0   0 ?        I<   21:47   0:00 [netns]  
root         7  0.0  0.0    0   0 ?        I    21:47   0:00 [kworker/0:0-events]  
root        10  0.0  0.0    0   0 ?        I<   21:47   0:00 [mm_percpu_wq]  
root        11  0.0  0.0    0   0 ?        I    21:47   0:00 [rcu_tasks_kthread]  
root        12  0.0  0.0    0   0 ?        I    21:47   0:00 [rcu_tasks_rude_kthread]  
root        13  0.0  0.0    0   0 ?        I    21:47   0:00 [rcu_tasks_trace_kthread]  
root        14  0.0  0.0    0   0 ?        S    21:47   0:00 [ksoftirqd/0]  
root        15  0.0  0.0    0   0 ?        I    21:47   0:00 [rcu_preempt]  
root        16  0.0  0.0    0   0 ?        S    21:47   0:00 [migration/0]
```



```
ls -la
totale 180
drwx----- 16 kali kali 4096 5 gen 21.53 .
drwxr-xr-x 3 root root 4096 19 dic 21.39 ..
-rw-r--r-- 1 kali kali 220 19 dic 21.39 .bash_logout
-rw-r--r-- 1 kali kali 5551 19 dic 21.39 .bashrc
-rw-r--r-- 1 kali kali 3526 19 dic 21.39 .bashrc.original
drwxr-xr-x 8 kali kali 4096 5 gen 21.53 .cache
drwxr-xr-x 12 kali kali 4096 20 dic 19.29 .config
-rw-r--r-- 1 kali kali 35 19 dic 21.43 .dmrc
drwxr-xr-x 2 kali kali 4096 19 dic 21.43 Documenti
-rw-r--r-- 1 kali kali 11759 19 dic 21.39 .face
lrwxrwxrwx 1 kali kali 5 19 dic 21.39 .face.icon -> .face
drwx----- 3 kali kali 4096 19 dic 21.43 .gnupg
-rw----- 1 kali kali 0 19 dic 21.43 .ICEauthority
drwxr-xr-x 2 kali kali 4096 19 dic 21.43 Immagini
drwxr-xr-x 3 kali kali 4096 19 dic 21.39 .java
drwxr-xr-x 4 kali kali 4096 19 dic 21.43 .local
drwxr-xr-x 2 kali kali 4096 19 dic 21.43 Modelli
drwx----- 4 kali kali 4096 5 gen 21.53 .mozilla
drwxr-xr-x 2 kali kali 4096 19 dic 21.43 Musica
-rw-r--r-- 1 kali kali 807 19 dic 21.39 .profile
drwxr-xr-x 2 kali kali 4096 19 dic 21.43 Pubblici
drwxr-xr-x 2 kali kali 4096 19 dic 21.43 Scaricati
drwxr-xr-x 2 kali kali 4096 19 dic 21.43 Scrivania
-rw-r----- 1 kali kali 4 5 gen 21.47 .vboxclient-clipboard-tty7-control.pid
-rw-r----- 1 kali kali 4 5 gen 21.47 .vboxclient-clipboard-tty7-service.pid
-rw-r----- 1 kali kali 5 5 gen 21.47 .vboxclient-display-svgx-x11-tty7-control.pid
-rw-r----- 1 kali kali 5 5 gen 21.47 .vboxclient-display-svgx-x11-tty7-service.pid
```

**col comando ls -la
visualizziamo tutti i file
e i relativi permessi**

usando “ps aux |grep fire”
filtriamo i risultati cercando
solo processi che contengono il
nome fire

usando “ls” abbiamo una lista
dei file nella posizione attuale
mentre “pwd” ci dice in che
posizione siamo

“ifconfig” invece ci da le
configurazioni di rete
attualmente configurate sulla
macchina

```
kali@kali: ~  
File Actions Edit View Help  
kali 4376 0.0 0.1 11212 4812 pts/0 R+ 21:53 0:00 ps aux  
ps aux | grep fire  
kali 4567 35.4 11.6 11329096 430396 ? Sl 21:53 0:11 /usr/lib/firefox-esr/firefox-esr  
kali 4627 0.1 0.9 208704 36928 ? Sl 21:53 0:00 /usr/lib/firefox-esr/firefox-esr -contentproc -parentBuildID 20230403141754 -prefsLen 2  
2984 -prefMapSize 216174 -appDir /usr/lib/firefox-esr/browser 4567 true socket  
kali 4730 1.7 2.5 2421144 95836 ? Sl 21:53 0:00 /usr/lib/firefox-esr/firefox-esr -contentproc -childID 1 -isForBrowser -prefsLen 33413  
-prefMapSize 216174 -jsInitLen 277276 -parentBuildID 20230403141754 -appDir /usr/lib/firefox-esr/browser 4567 true tab  
kali 4760 2.0 3.0 2436360 113840 ? Sl 21:53 0:00 /usr/lib/firefox-esr/firefox-esr -contentproc -childID 2 -isForBrowser -prefsLen 33413  
-prefMapSize 216174 -jsInitLen 277276 -parentBuildID 20230403141754 -appDir /usr/lib/firefox-esr/browser 4567 true tab  
kali 4851 1.4 2.9 2413280 108972 ? Sl 21:53 0:00 /usr/lib/firefox-esr/firefox-esr -contentproc -childID 3 -isForBrowser -prefsLen 33413  
-prefMapSize 216174 -jsInitLen 277276 -parentBuildID 20230403141754 -appDir /usr/lib/firefox-esr/browser 4567 true tab  
kali 4866 0.4 1.8 2383628 67892 ? Sl 21:53 0:00 /usr/lib/firefox-esr/firefox-esr -contentproc -childID 4 -isForBrowser -prefsLen 33413  
-prefMapSize 216174 -jsInitLen 277276 -parentBuildID 20230403141754 -appDir /usr/lib/firefox-esr/browser 4567 true tab  
kali 4889 0.4 1.8 2383628 67896 ? Sl 21:53 0:00 /usr/lib/firefox-esr/firefox-esr -contentproc -childID 5 -isForBrowser -prefsLen 33413  
-prefMapSize 216174 -jsInitLen 277276 -parentBuildID 20230403141754 -appDir /usr/lib/firefox-esr/browser 4567 true tab  
kali 4921 0.4 1.8 2383632 67388 ? Sl 21:53 0:00 /usr/lib/firefox-esr/firefox-esr -contentproc -childID 6 -isForBrowser -prefsLen 33413  
-prefMapSize 216174 -jsInitLen 277276 -parentBuildID 20230403141754 -appDir /usr/lib/firefox-esr/browser 4567 true tab  
kali 5153 0.0 0.0 6352 2296 pts/0 S+ 21:54 0:00 grep fire  
ls  
Documenti  
Immagini  
Modelli  
Musica  
Pubblici  
Scaricati  
Scrivania  
Video  
pwd  
/home/kali  
ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.1.242 netmask 255.255.255.0 broadcast 192.168.1.255  
inet6 fe80::a00:27ff:feb3:f3ba prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:b3:f3:ba txqueuelen 1000 (Ethernet)  
RX packets 18156 bytes 18013072 (17.1 MiB)
```