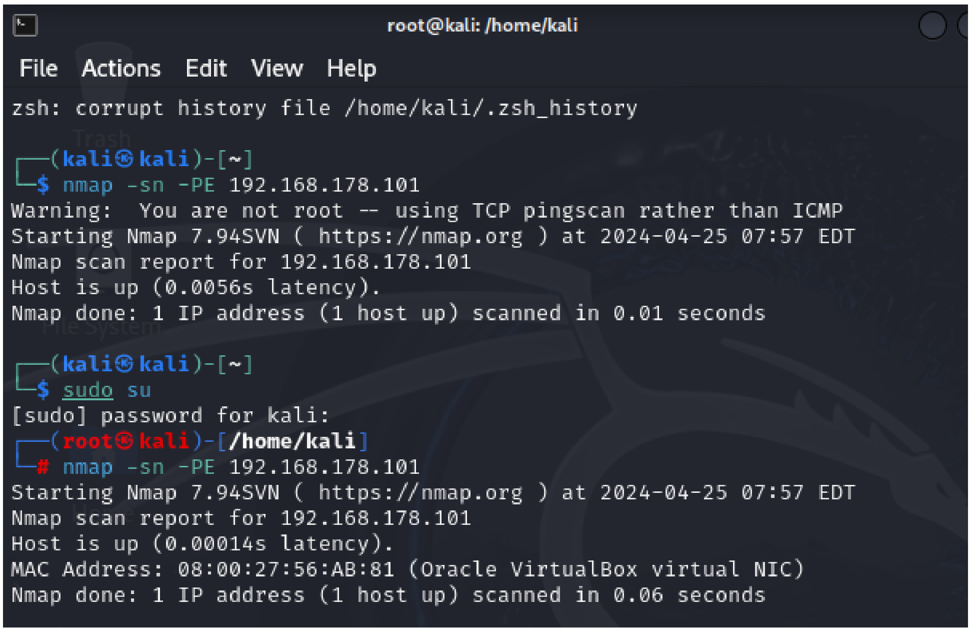
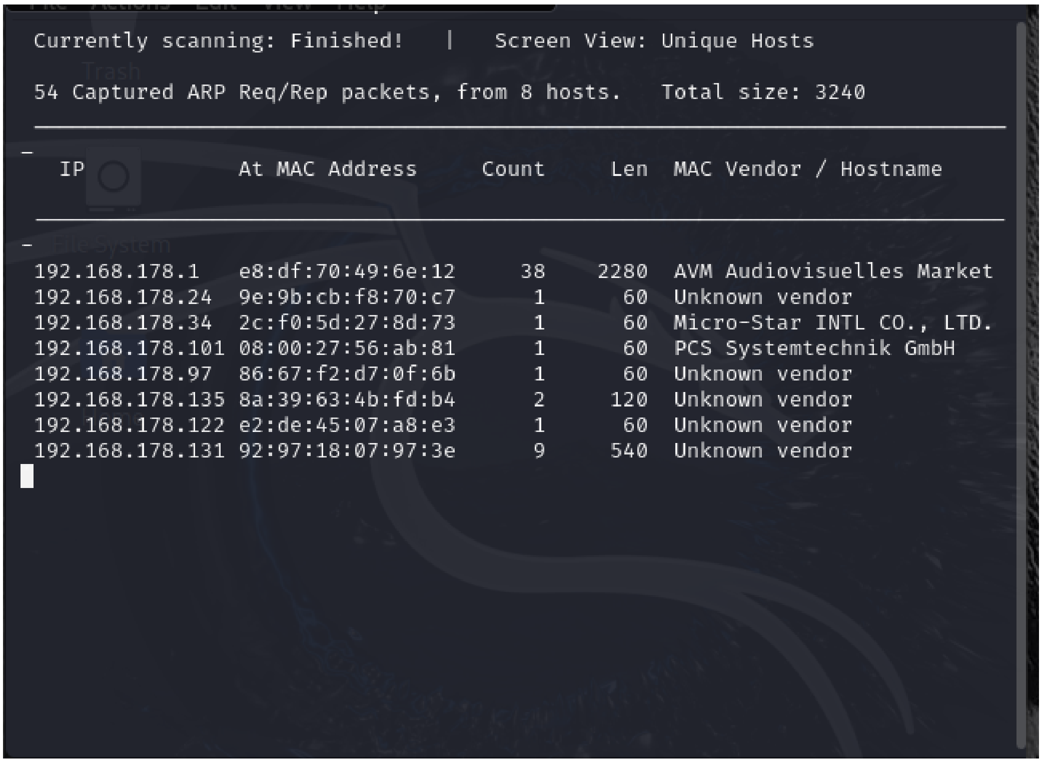
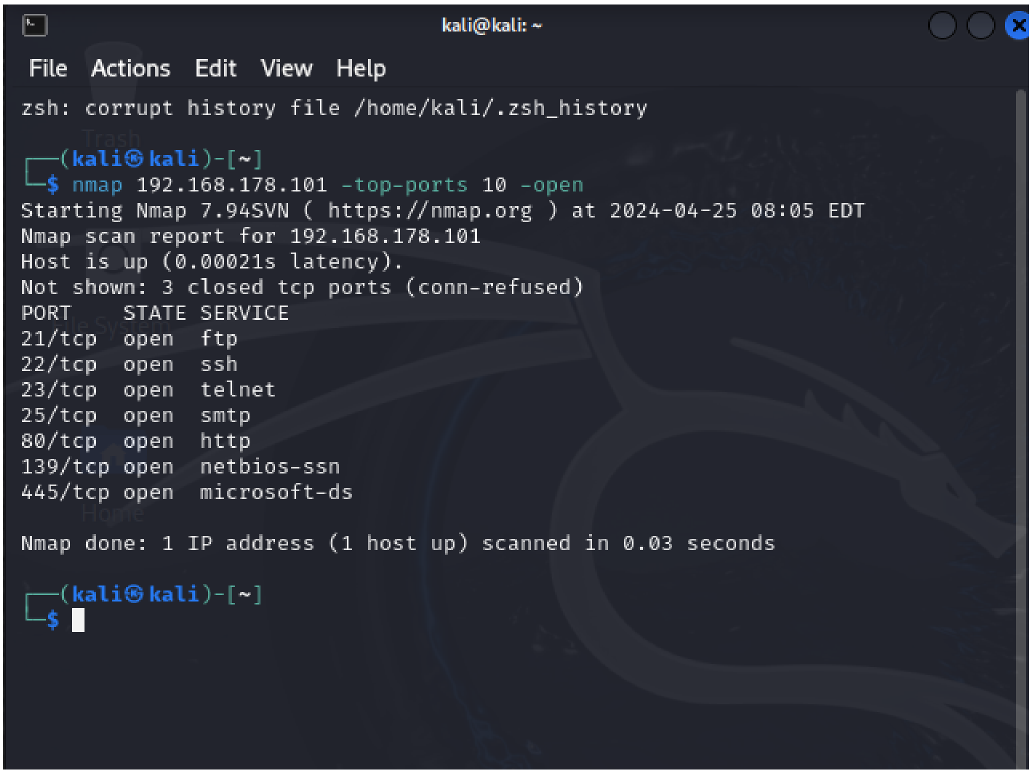


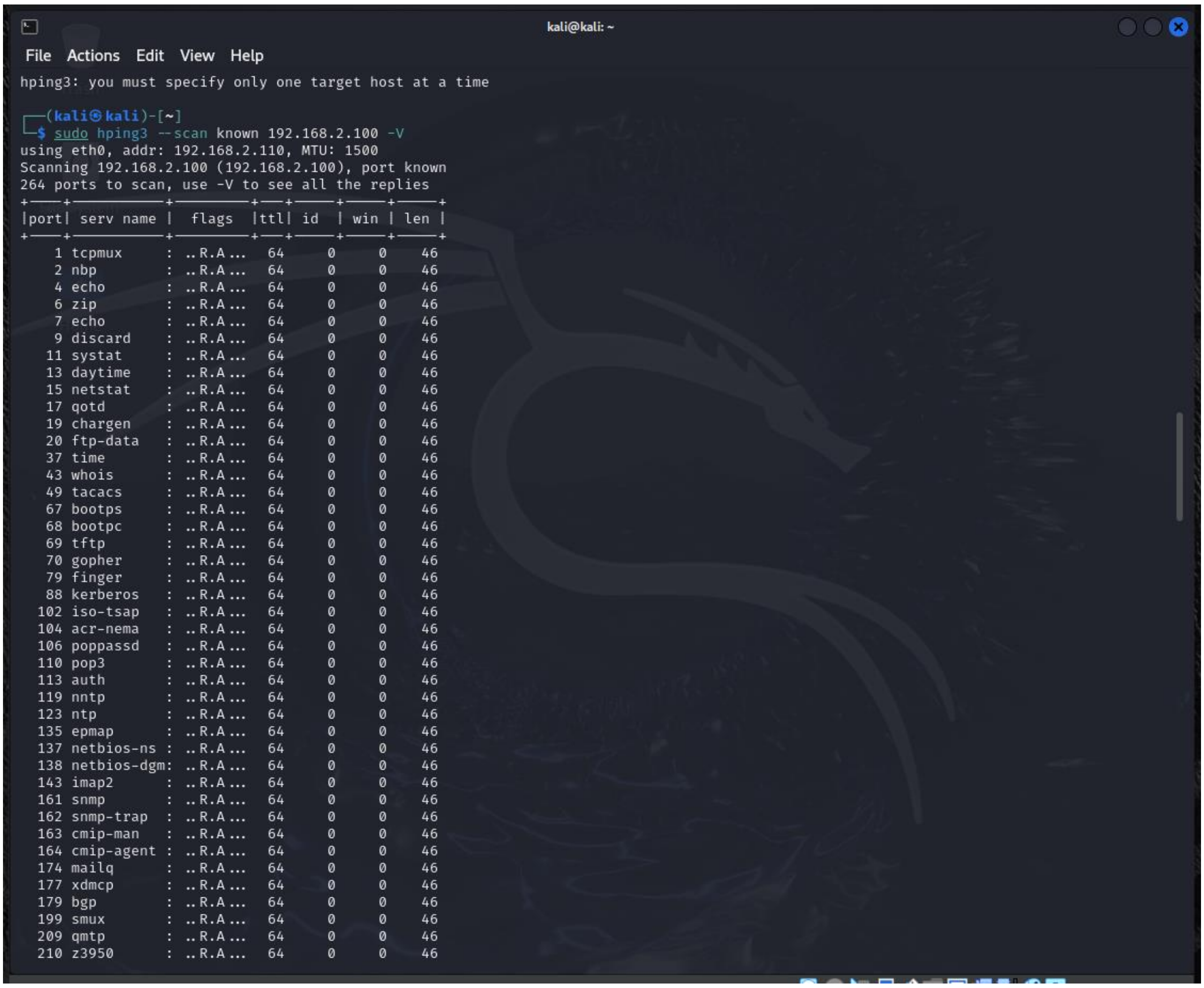
```
zsh: corrupt history file /home/kali/.zsh_history

┌──(kali㉿kali)-[~]
└─$ nmap -sn -PE 192.168.178.101
Warning:  You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-25 07:57 EDT
Nmap scan report for 192.168.178.101
Host is up (0.0056s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds

┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn -PE 192.168.178.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-25 07:57 EDT
Nmap scan report for 192.168.178.101
Host is up (0.00014s latency).
MAC Address: 08:00:27:56:AB:81 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```



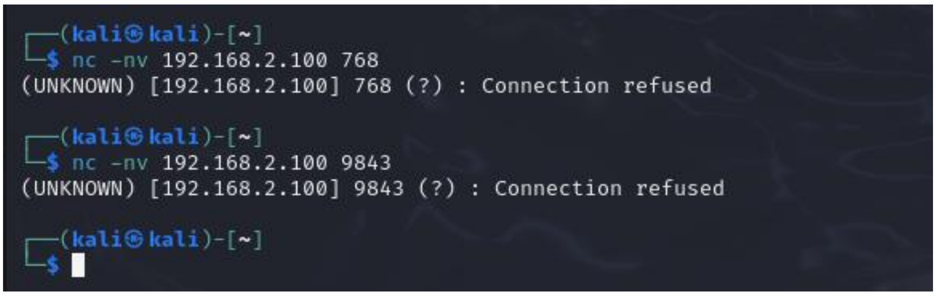
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 54 Captured ARP Req/Rep packets, from 8 hosts.   Total size: 3240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.178.1   e8:df:70:49:6e:12     38    2280  AVM Audiovisuelles Market
 192.168.178.24  9e:9b:cb:f8:70:c7      1      60  Unknown vendor
 192.168.178.34  2c:f0:5d:27:8d:73      1      60  Micro-Star INTL CO., LTD.
 192.168.178.101 08:00:27:56:ab:81      1      60  PCS Systemtechnik GmbH
 192.168.178.97  86:67:f2:d7:0f:6b      1      60  Unknown vendor
 192.168.178.135 8a:39:63:4b:fd:b4      2     120  Unknown vendor
 192.168.178.122 e2:de:45:07:a8:e3      1      60  Unknown vendor
 192.168.178.131 92:97:18:07:97:3e      9     540  Unknown vendor
```



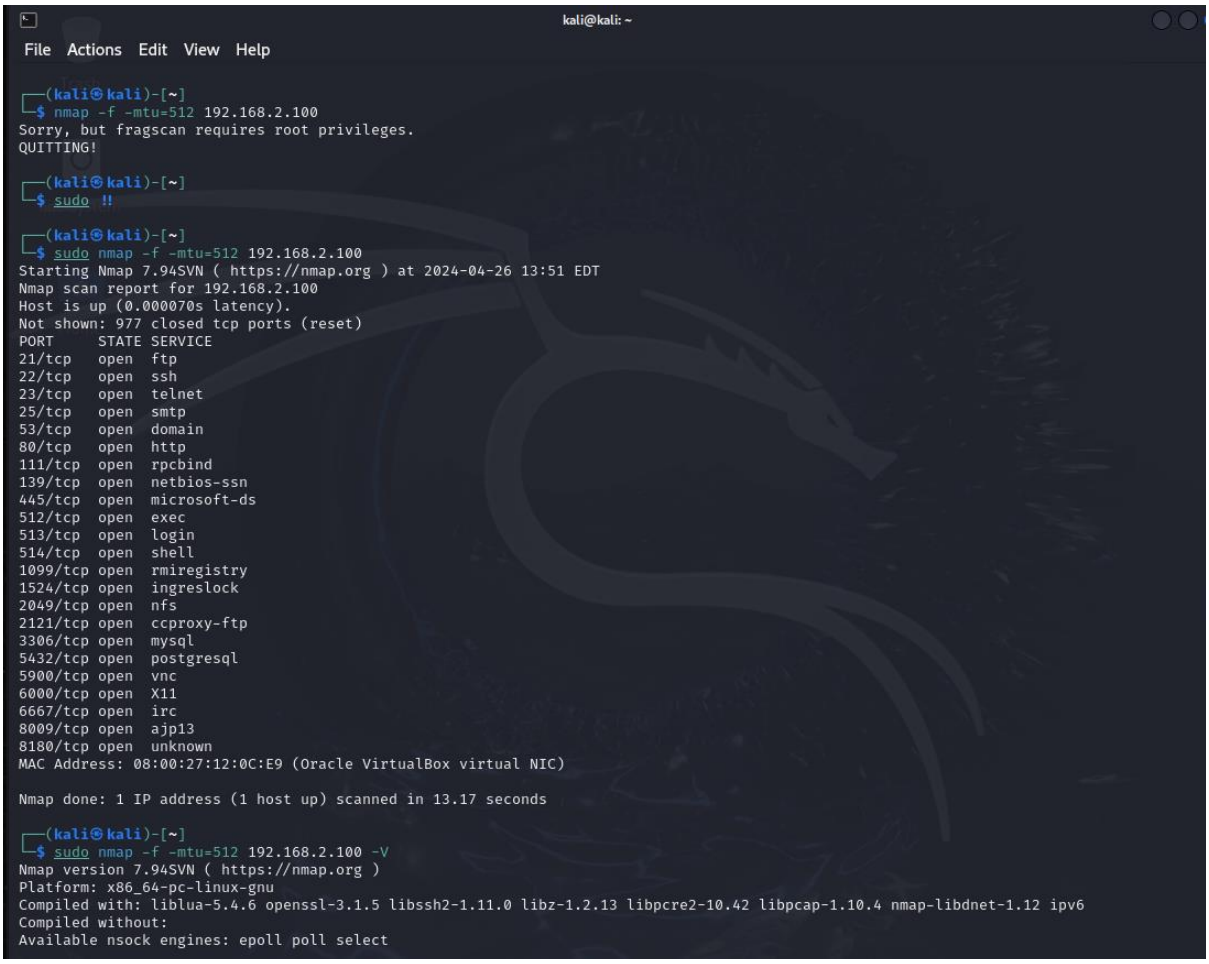
```
zsh: corrupt history file /home/kali/.zsh_history

┌──(kali㉿kali)-[~]
└─$ nmap 192.168.178.101 -top-ports 10 -open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-25 08:05 EDT
Nmap scan report for 192.168.178.101
Host is up (0.00021s latency).
Not shown: 3 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds

┌──(kali㉿kali)-[~]
└─$ 
```



```
hping3: you must specify only one target host at a time

┌──(kali㉿kali)-[~]
└─$ sudo hping3 --scan known 192.168.2.100 -V
using eth0, addr: 192.168.2.110, MTU: 1500
Scanning 192.168.2.100 (192.168.2.100), port known
264 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   1 tcpmux     : ..R.A...  64     0     0    46
   2 nbp        : ..R.A...  64     0     0    46
   4 echo       : ..R.A...  64     0     0    46
   6 zip        : ..R.A...  64     0     0    46
   7 echo       : ..R.A...  64     0     0    46
   9 discard    : ..R.A...  64     0     0    46
  11 systat     : ..R.A...  64     0     0    46
  13 daytime    : ..R.A...  64     0     0    46
  15 netstat    : ..R.A...  64     0     0    46
  17 qotd       : ..R.A...  64     0     0    46
  19 chargen    : ..R.A...  64     0     0    46
  20 ftp-data   : ..R.A...  64     0     0    46
  37 time       : ..R.A...  64     0     0    46
  43 whois      : ..R.A...  64     0     0    46
  49 tacacs     : ..R.A...  64     0     0    46
  67 bootps     : ..R.A...  64     0     0    46
  68 bootpc     : ..R.A...  64     0     0    46
  69 tftp       : ..R.A...  64     0     0    46
  70 gopher     : ..R.A...  64     0     0    46
  79 finger     : ..R.A...  64     0     0    46
  88 kerberos   : ..R.A...  64     0     0    46
 102 iso-tsap   : ..R.A...  64     0     0    46
 104 acr-nema   : ..R.A...  64     0     0    46
 106 poppassd   : ..R.A...  64     0     0    46
 110 pop3       : ..R.A...  64     0     0    46
 113 auth       : ..R.A...  64     0     0    46
 119 nntp       : ..R.A...  64     0     0    46
 123 ntp        : ..R.A...  64     0     0    46
 135 epmap      : ..R.A...  64     0     0    46
 137 netbios-ns : ..R.A...  64     0     0    46
 138 netbios-dgm: ..R.A...  64     0     0    46
 143 imap2      : ..R.A...  64     0     0    46
 161 snmp       : ..R.A...  64     0     0    46
 162 snmp-trap  : ..R.A...  64     0     0    46
 163 cmip-man   : ..R.A...  64     0     0    46
 164 cmip-agent : ..R.A...  64     0     0    46
 174 mailq      : ..R.A...  64     0     0    46
 177 xdmcp      : ..R.A...  64     0     0    46
 179 bgp        : ..R.A...  64     0     0    46
 199 smux       : ..R.A...  64     0     0    46
 209 qmtp       : ..R.A...  64     0     0    46
 210 z3950      : ..R.A...  64     0     0    46
```



```
┌──(kali㉿kali)-[~]
└─$ nc -nv 192.168.2.100 768
(UNKNOWN) [192.168.2.100] 768 (?) : Connection refused

┌──(kali㉿kali)-[~]
└─$ nc -nv 192.168.2.100 9843
(UNKNOWN) [192.168.2.100] 9843 (?) : Connection refused

┌──(kali㉿kali)-[~]
└─$ █
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -f -mtu=512 192.168.2.100
Sorry, but fragscan requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo !!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -f -mtu=512 192.168.2.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 13:51 EDT
Nmap scan report for 192.168.2.100
Host is up (0.000070s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:12:0C:E9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -f -mtu=512 192.168.2.100 -V
Nmap version 7.94SVN ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.6 openssl-3.1.5 libssh2-1.11.0 libz-1.2.13 libpcre2-10.42 libpcap-1.10.4 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

- Molto interessante il comando 13 che permette di bypassare il firewall dividendo i pacchetti in parti più piccole, rendendoli meno grandi in termini di byte. Permette di trovare porte in più, come la 22.

- Interessante anche il comando otto che permette di scansionare una porta singola.

- Il comando tre permette di visualizzare il nome dell'host target e il suo sistema operativo.