

# Nmap

## Mappatura di rete

NMAP È UNO STRUMENTO POTENTE PER LA MAPPATURA DI RETE CHE UTILIZZA PACCHETTI RAW PER ESEGUIRE SCANSIONI PRECISE E DETTAGLIATE.

```
ap 7.93SVN ( https://nmap.org )
age: nmap [Scan Type(s)] [Options] {target specification}
RGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.
-iL <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/netw
--excludefile <exclude_file>: Exclude list from file
ST DISCOVERY:
-sL: List Scan - simply list targets to scan
-sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discover
-PE/PP/PM: ICMP echo, timestamp, and netmask request disc
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: s
--dns-servers <serv1[,serv2],...>: Specify custom DNS ser
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
AN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scan
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
```

00 E' fondamentale essere al corrente che questo tipo di pratica non è legale se non previa autorizzazione del bersaglio dello scan.

Nmap è uno scanner di rete.

Ruolo chiave per Nmap sono i pacchetti Raw, ovvero pacchetti personalizzabili. Un esempio pratico è la possibilità di inviare **solo** il segnal SYN, ovvero primo segmento inviato in una 3 way handshake, processo per instaurare una connessione. Oltretutto è possibile gestire il tempo in cui i segmenti di un pacchetto possono essere inviati. Tali pratiche permettono il più delle volte di scavalcare blocchi posti a impedire connessioni, come il firewall.

```
nmap 7.93SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0.0/24
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: scan]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
```

```
File Actions Edit View Help
(root@kali)-[/home/kali]
# nmap -O 192.168.1.80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 14:41 CET
Nmap scan report for 192.168.1.80
Host is up (0.0010s 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: 08:00:27:9B:64:F6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9b:64:f6
          inet addr:192.168.1.80  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9b:64f6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:79 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8951 (8.7 KB)  TX bytes:7112 (6.9 KB)
          Base address:0xd020 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:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)
```

## OS fingerprint

Attraverso il comando “nmap -O 192.168.1.80” il tool nmap ci permette di visionare il sistema operativo corrispondente all’IP di nostro interesse che nell’esempio in foto è 192.168.1.80 , corrispondente a Metasploitable.

```
root@kali: /home/kali
File Actions Edit View Help
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds

(root@kali)-[/home/kali]
# nmap -sS 192.168.1.80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 14:42 CET
Nmap scan report for 192.168.1.80
Host is up (0.00066s 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: 08:00:27:9B:64:F6 (Oracle VirtualBox virtual NIC)

Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9b:64:f6
          inet addr:192.168.1.80  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9b:64f6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:79 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8951 (8.7 KB)  TX bytes:7112 (6.9 KB)
          Base address:0xd020 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:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)
```

## SYN SCAN

Attraverso il comando "nmap -sS 192.168.1.80" abbiamo modo di eseguire una scansione "half-open", inviando pacchetti SYN e attendendo risposte SYN/ACK.



```
root@kali: /home/kali
File Actions Edit View Help

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds

(root@kali)-[/home/kali]
# nmap -sT 192.168.1.80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 14:49 CET
Nmap scan report for 192.168.1.80
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (conn-refused)
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: 08:00:27:9B:64:F6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

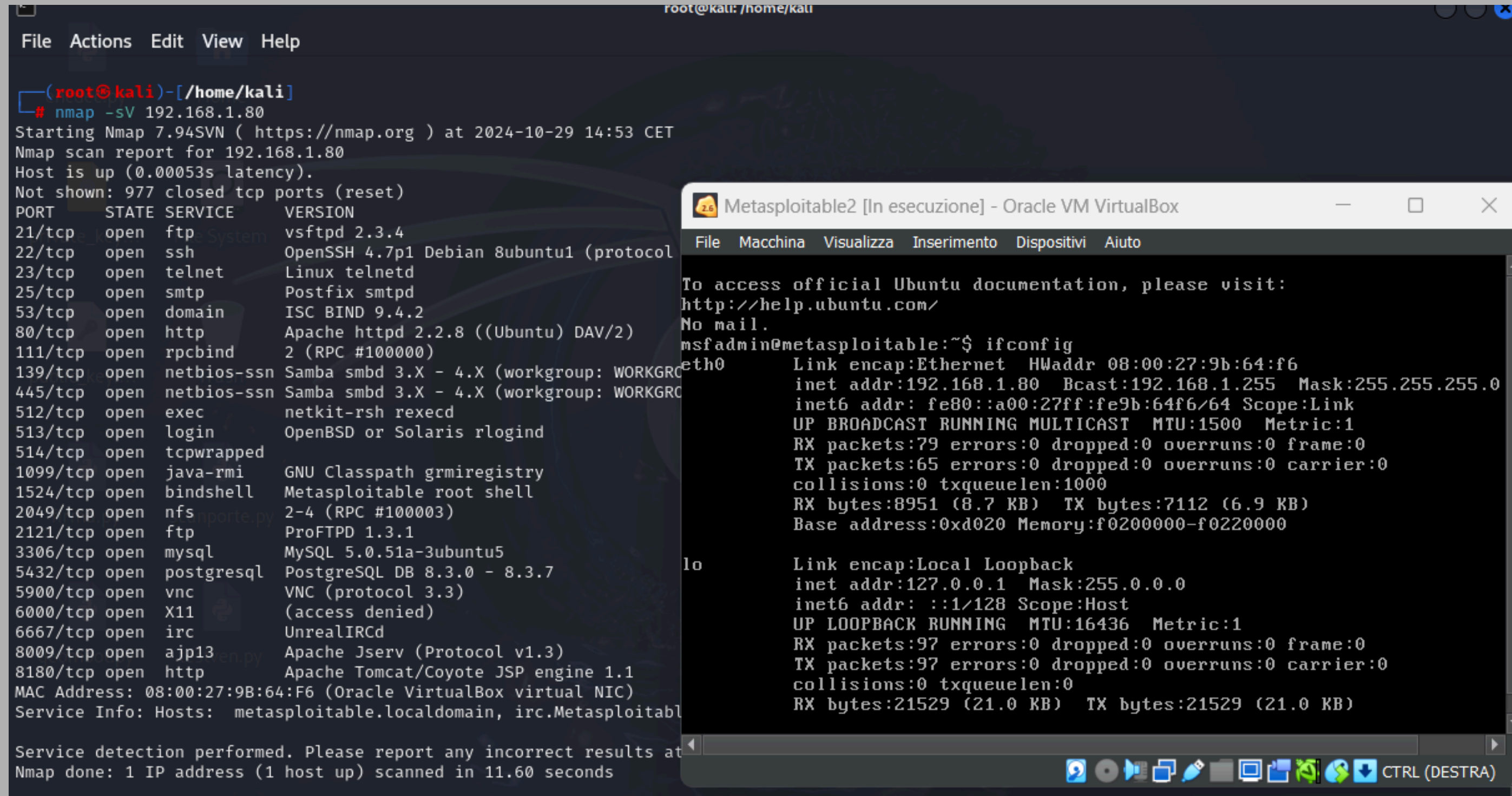
Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9b:64:f6
          inet addr:192.168.1.80  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9b:64f6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:79 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8951 (8.7 KB)  TX bytes:7112 (6.9 KB)
          Base address:0xd020 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:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)
```

## TCP connect

Inserendo il comando “nmap -sT 192.168.1.80” abbiamo la possibilità di eseguire una scansione che nella quale si instaurano connessioni TCP complete. Non compaiono risultati discordanti tra scan tcp e scan syn.



The image shows a Kali Linux terminal window on the left and a Metasploitable2 VM window on the right. The terminal window displays the output of an Nmap scan for 192.168.1.80, showing various open ports and services. The VM window shows the output of the 'ifconfig' command, displaying network configuration for the 'eth0' interface.

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.1.80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 14:53 CET
Nmap scan report for 192.168.1.80
Host is up (0.00053s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGR
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGR
512/tcp   open  exec         netkit-rsh rshd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:9B:64:F6 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable

Service detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 11.60 seconds
```

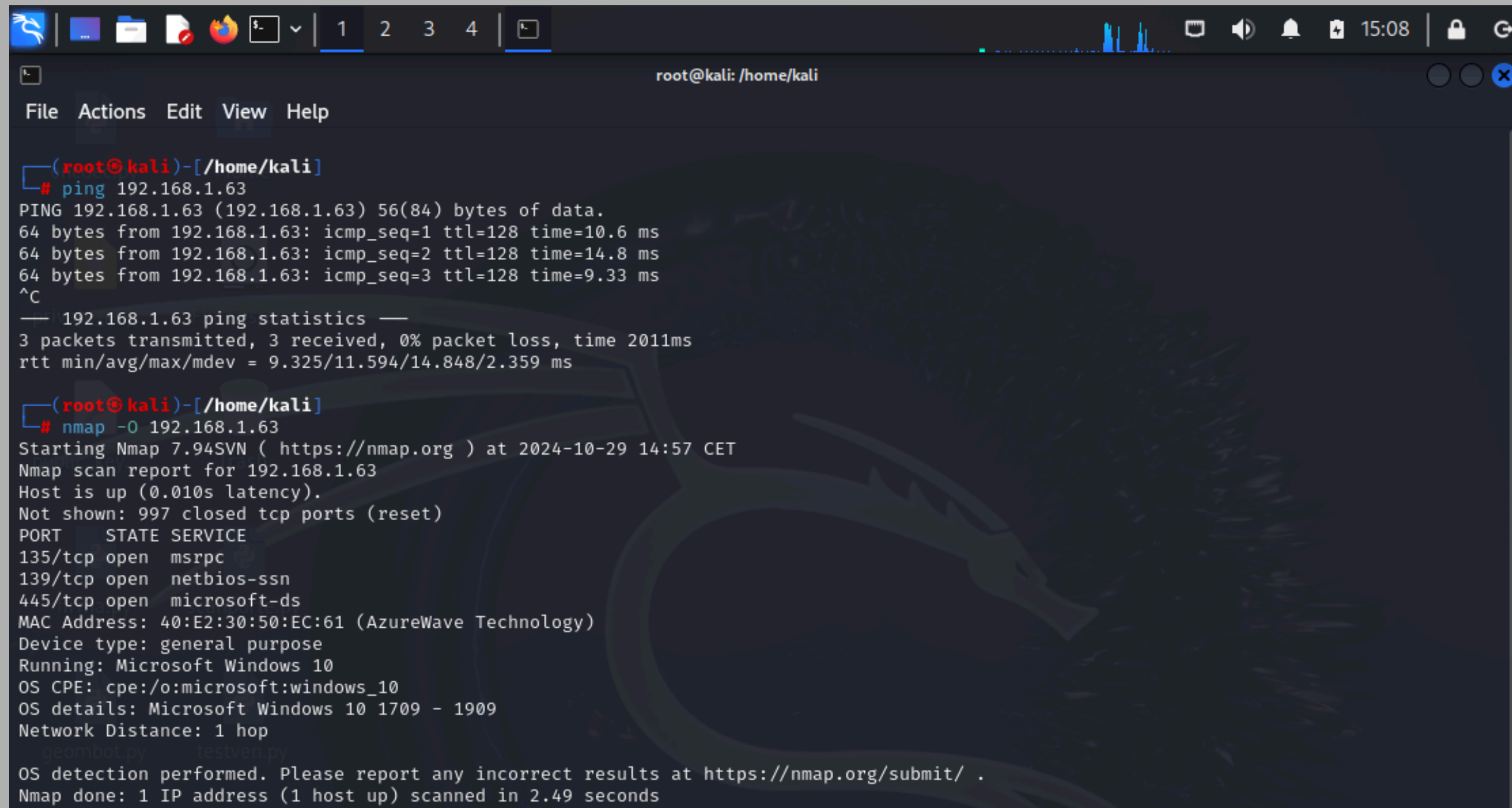
```
Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9b:64:f6
          inet addr:192.168.1.80  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9b:64f6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:79 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8951 (8.7 KB)  TX bytes:7112 (6.9 KB)
          Base address:0xd020 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:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)
```

## Version detection

La funzione “nmap -sV” scopre la versione dei servizi utilizzati nelle porte



The image shows a terminal window on a Kali Linux system. The window title is 'root@kali: /home/kali'. The terminal displays the output of a 'ping' command to 192.168.1.63, followed by an 'nmap -O' scan of the same IP. The nmap scan report identifies the host as running Microsoft Windows 10. The terminal background features a faint dragon logo.

```
(root@kali)-[/home/kali]
# ping 192.168.1.63
PING 192.168.1.63 (192.168.1.63) 56(84) bytes of data.
64 bytes from 192.168.1.63: icmp_seq=1 ttl=128 time=10.6 ms
64 bytes from 192.168.1.63: icmp_seq=2 ttl=128 time=14.8 ms
64 bytes from 192.168.1.63: icmp_seq=3 ttl=128 time=9.33 ms
^C
— 192.168.1.63 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2011ms
rtt min/avg/max/mdev = 9.325/11.594/14.848/2.359 ms

(root@kali)-[/home/kali]
# nmap -O 192.168.1.63
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 14:57 CET
Nmap scan report for 192.168.1.63
Host is up (0.010s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 40:E2:30:50:EC:61 (AzureWave Technology)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.49 seconds
```

## OS fingerprint - Windows

Anche in questo caso, attraverso il comando -O riusciamo a vedere il sistema operativo dell'IP bersaglio. In questo caso si tratta di Windows 10. Fondamentale per svolgere questa funzione è fondamentale abbassare il firewall di Windows al fine di permettere la comunicazione e quindi lo scan.