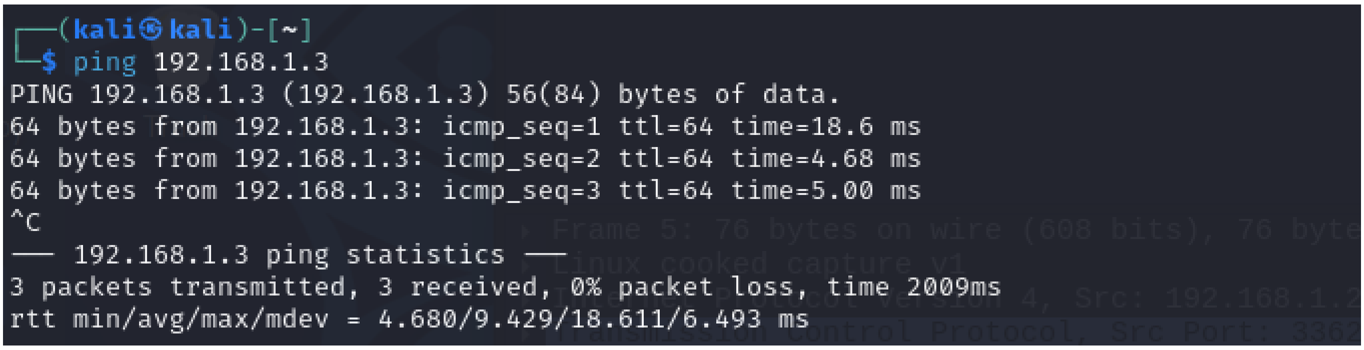
W11D1

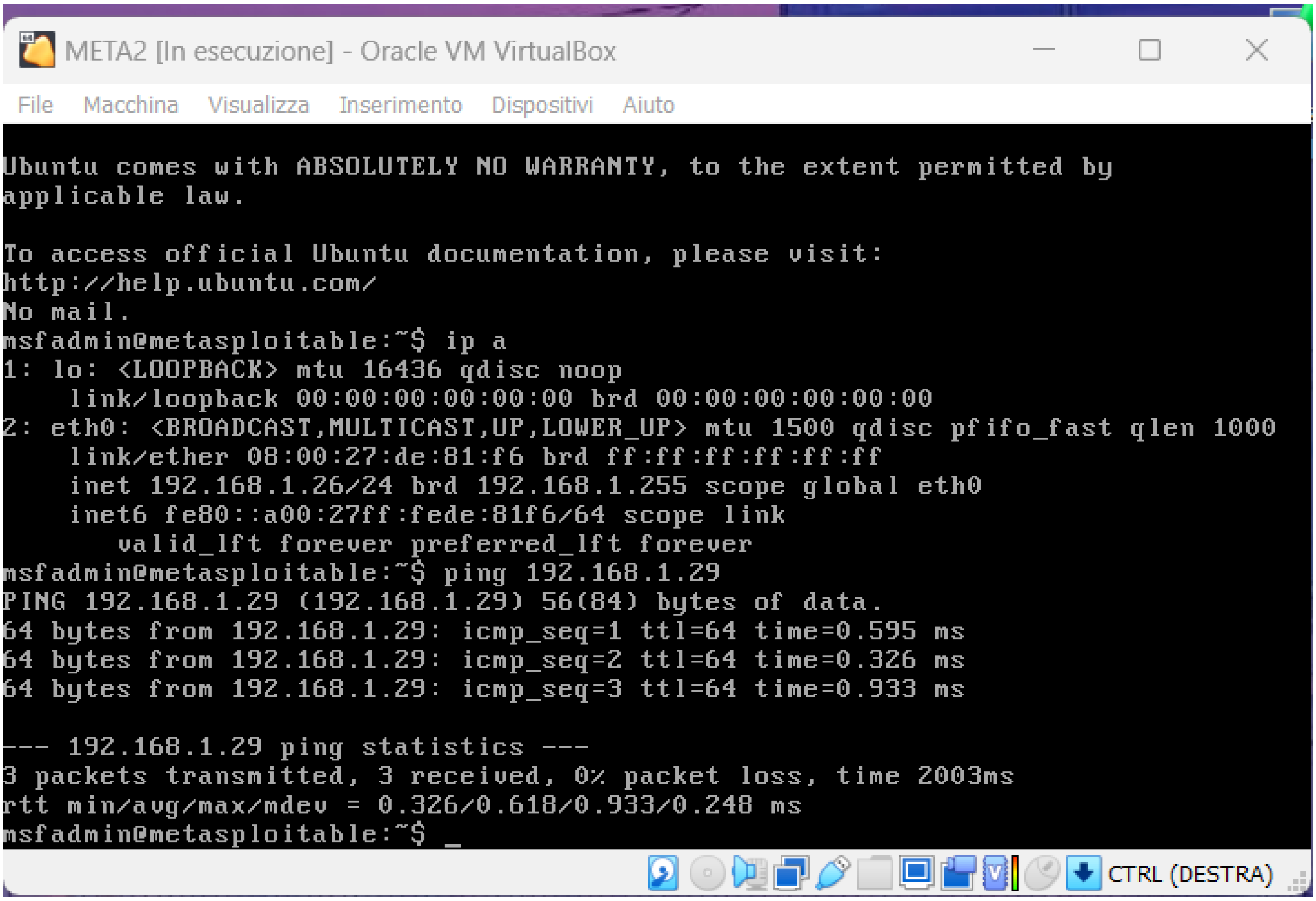
le due macchine si pingano

metasploitable 2 IP 192.168.1.3



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=18.6 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=4.68 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=5.00 ms
^C
--- 192.168.1.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 4.680/9.429/18.611/6.493 ms
```

kali IP 192.168.1.29

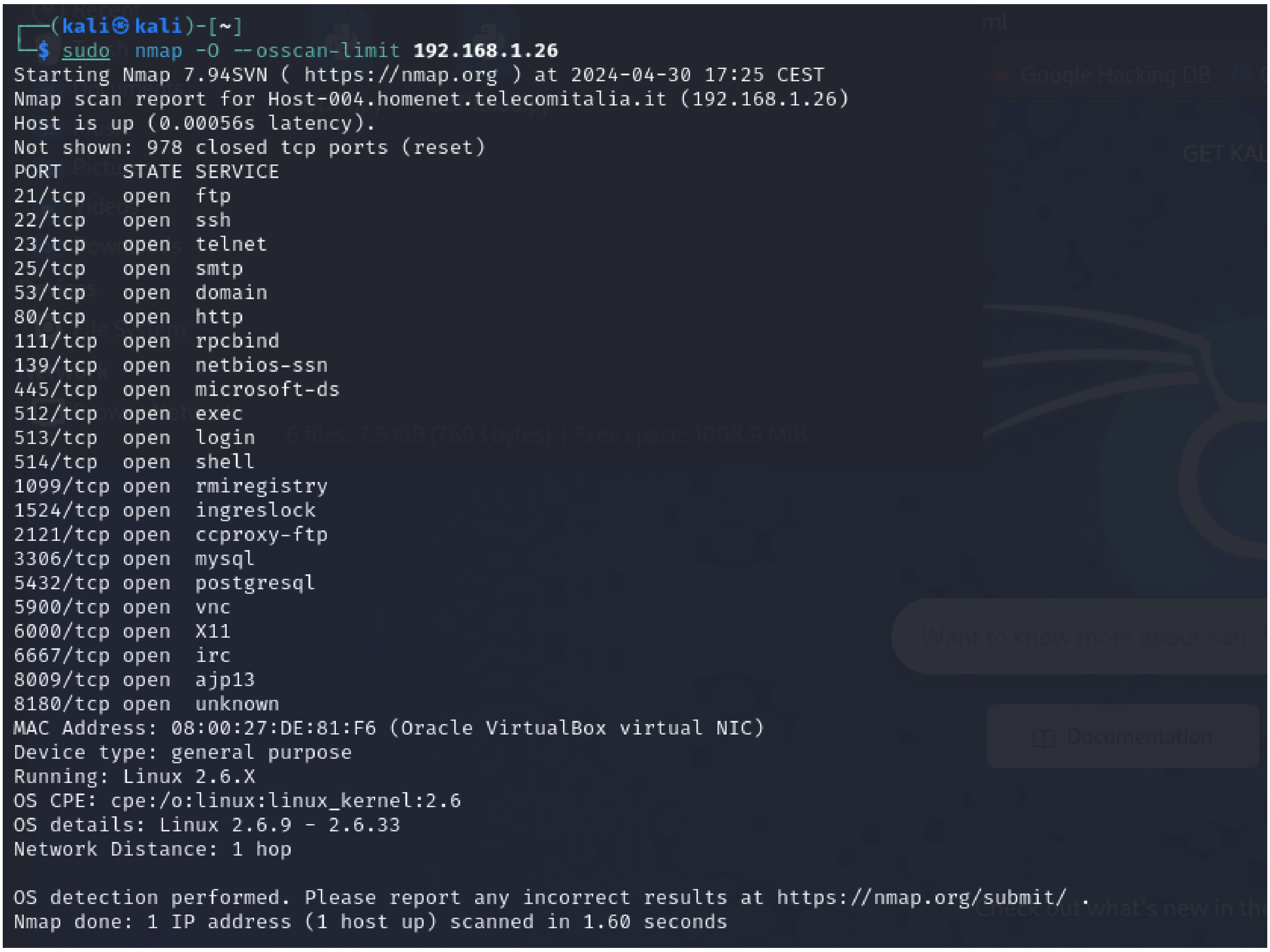


```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK> mtu 16436 qdisc noop
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:de:81:f6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.26/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fede:81f6/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ping 192.168.1.29
PING 192.168.1.29 (192.168.1.29) 56(84) bytes of data.
64 bytes from 192.168.1.29: icmp_seq=1 ttl=64 time=0.595 ms
64 bytes from 192.168.1.29: icmp_seq=2 ttl=64 time=0.326 ms
64 bytes from 192.168.1.29: icmp_seq=3 ttl=64 time=0.933 ms

--- 192.168.1.29 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.326/0.618/0.933/0.248 ms
msfadmin@metasploitable:~$ _
```

OS fingerprint con



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O --osscan-limit 192.168.1.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 17:25 CEST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.26)
Host is up (0.00056s latency).
Not shown: 978 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
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:DE:81: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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

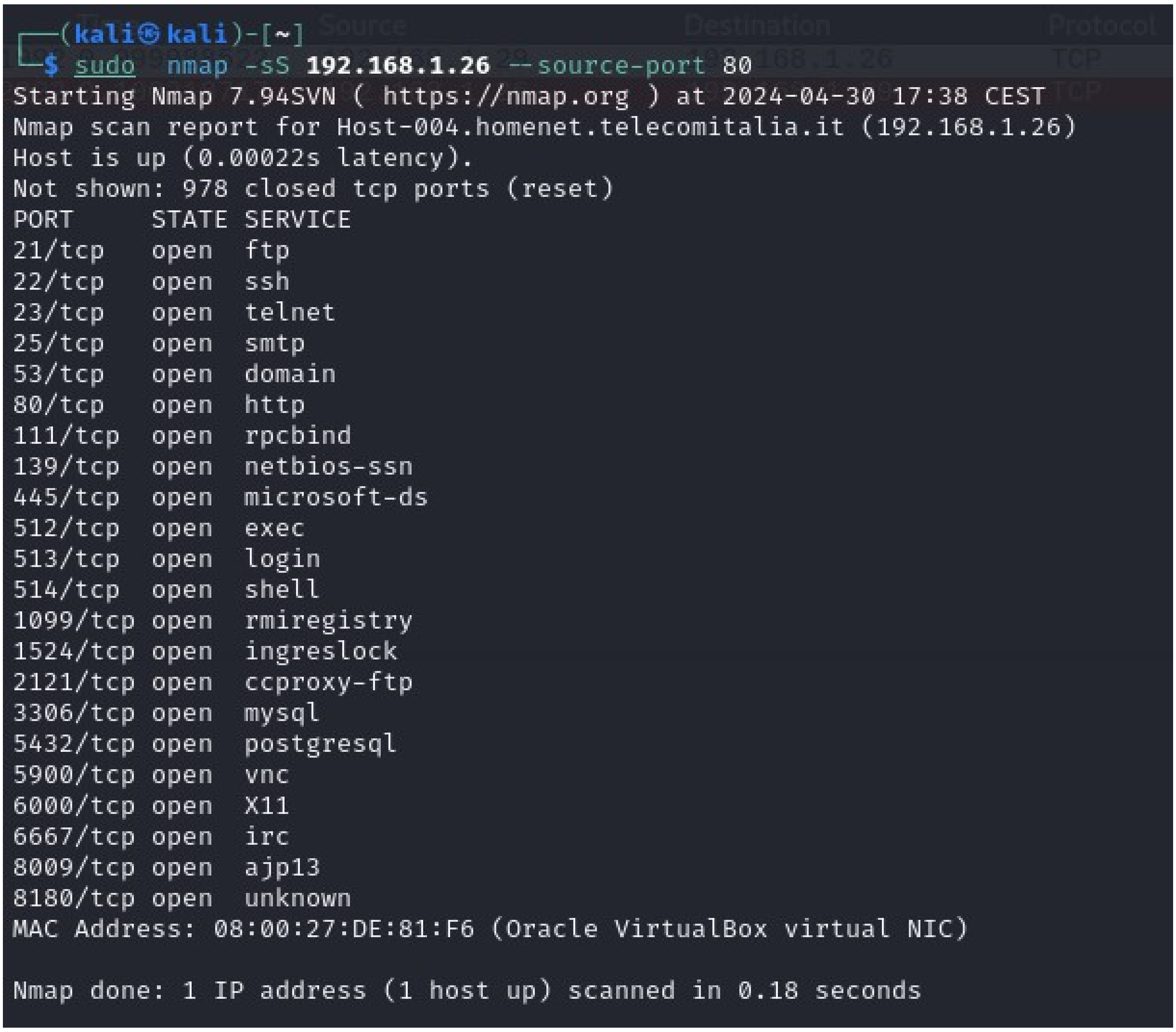
-O

tenta invece di verificare il sistema operativo

--osscan-limit

Questa opzione limita la scansione del sistema operativo di nmap, riducendo il numero di pacchetti inviati per l'identificazione del sistema operativo. Limitare il numero di pacchetti inviati può aiutare a ridurre il rischio di rilevamento da parte di sistemi di protezione, firewall o intrusion detection systems (IDS). Tuttavia, riducendo il numero di pacchetti inviati, si può anche ridurre l'accuratezza dell'identificazione del sistema operativo.

syn scan

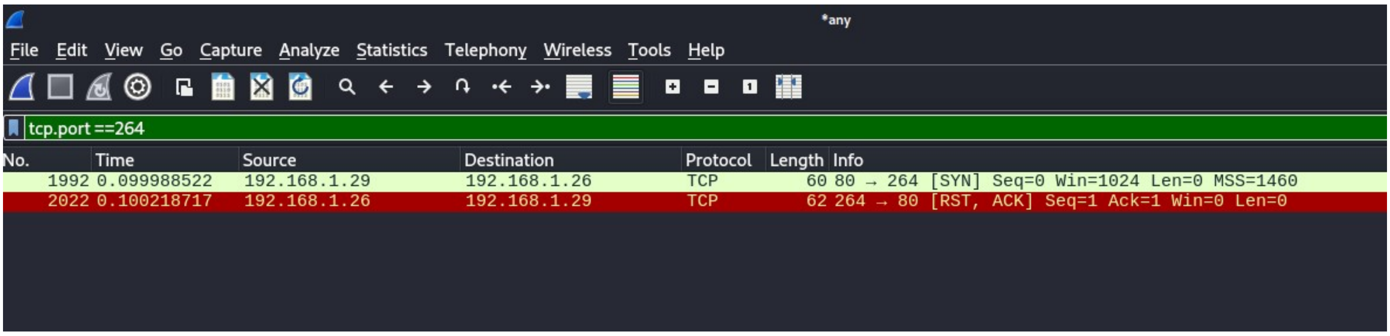


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.26 --source-port 80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 17:38 CEST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.26)
Host is up (0.00022s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
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
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:DE:81:F6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

effettua solo la scansione con il syn senza aspettare il syn ack quindi il Three handshake

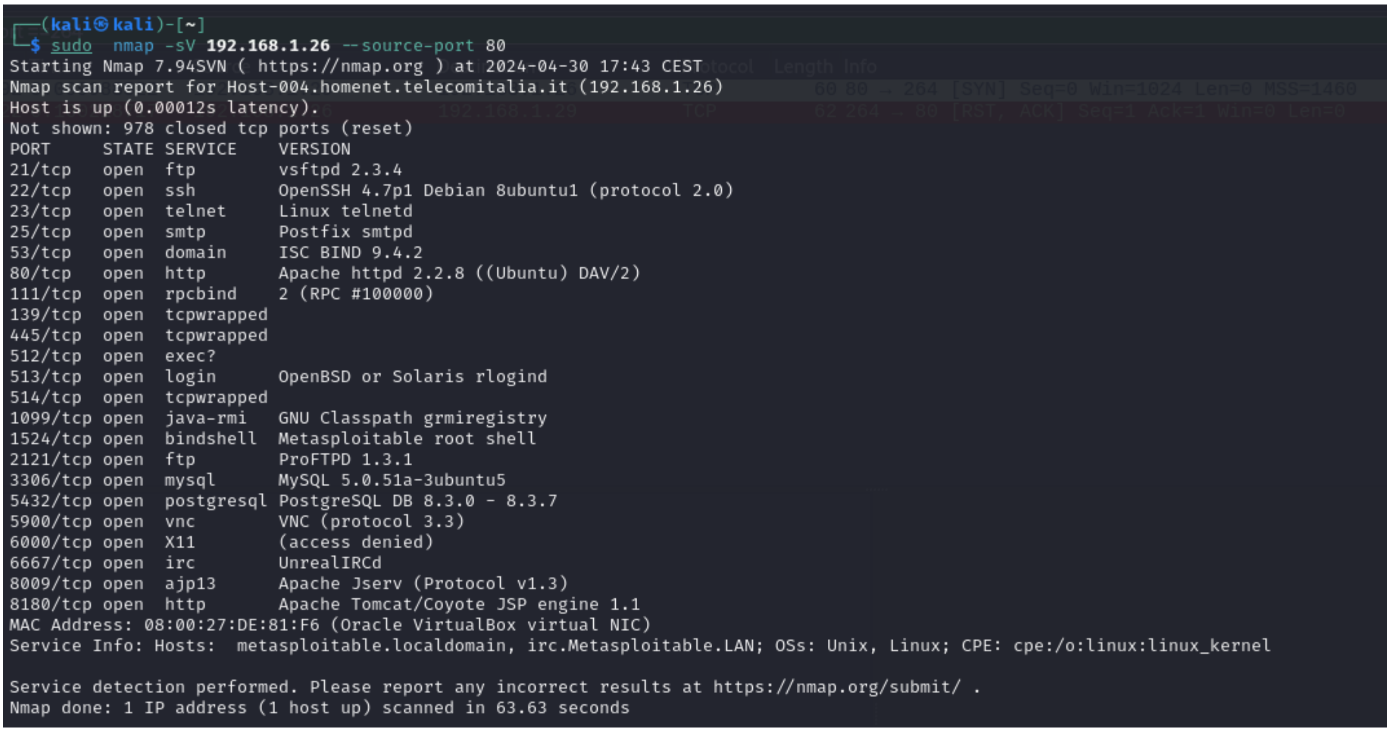
come si può vedere da immagine di wireshark qui sotto



tcp.port ==264

```
No.   Time          Source          Destination     Protocol  Length Info
 1992 0.099988522   192.168.1.29    192.168.1.26    TCP           60 80 → 264 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2022 0.100218717   192.168.1.26    192.168.1.29    TCP           62 264 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

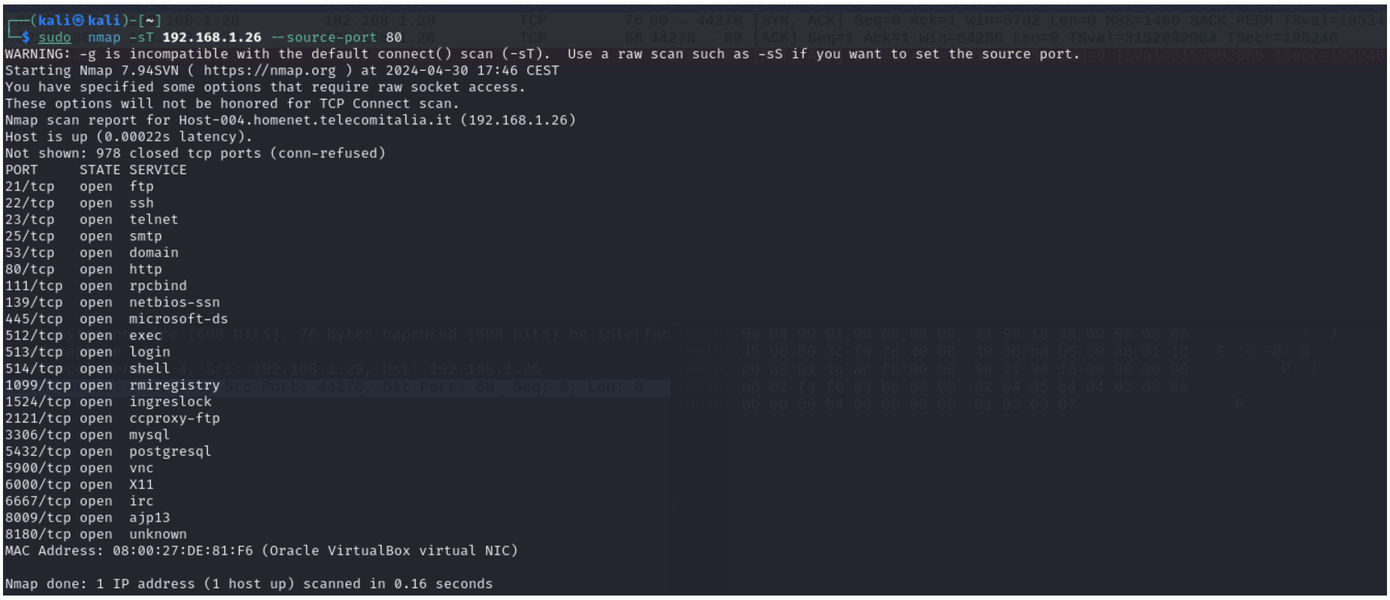
con -SV verifica i servizi attivi



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.26 --source-port 80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 17:43 CEST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.26)
Host is up (0.00012s latency).
Not shown: 978 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 2.0)
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  tcpwrapped
445/tcp  open  tcpwrapped
512/tcp  open  exec?
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
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:DE:81:F6 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.63 seconds
```

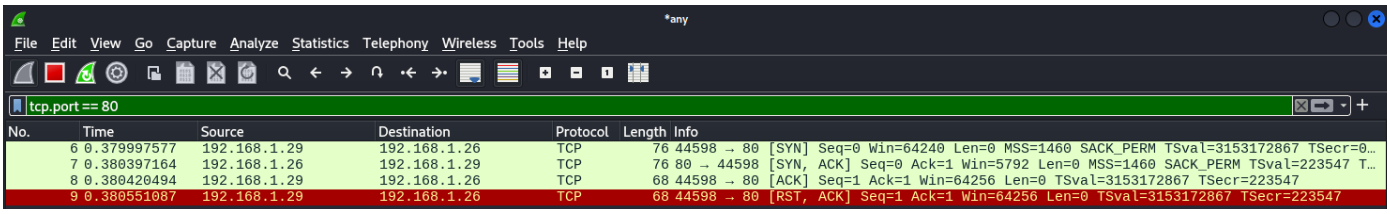
con -sT effettua il 3HS



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.1.26 --source-port 80
WARNING: -g is incompatible with the default connect() scan (-sT).  Use a raw scan such as -sS if you want to set the source port.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 17:46 CEST
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.26)
Host is up (0.00022s latency).
Not shown: 978 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
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:DE:81:F6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

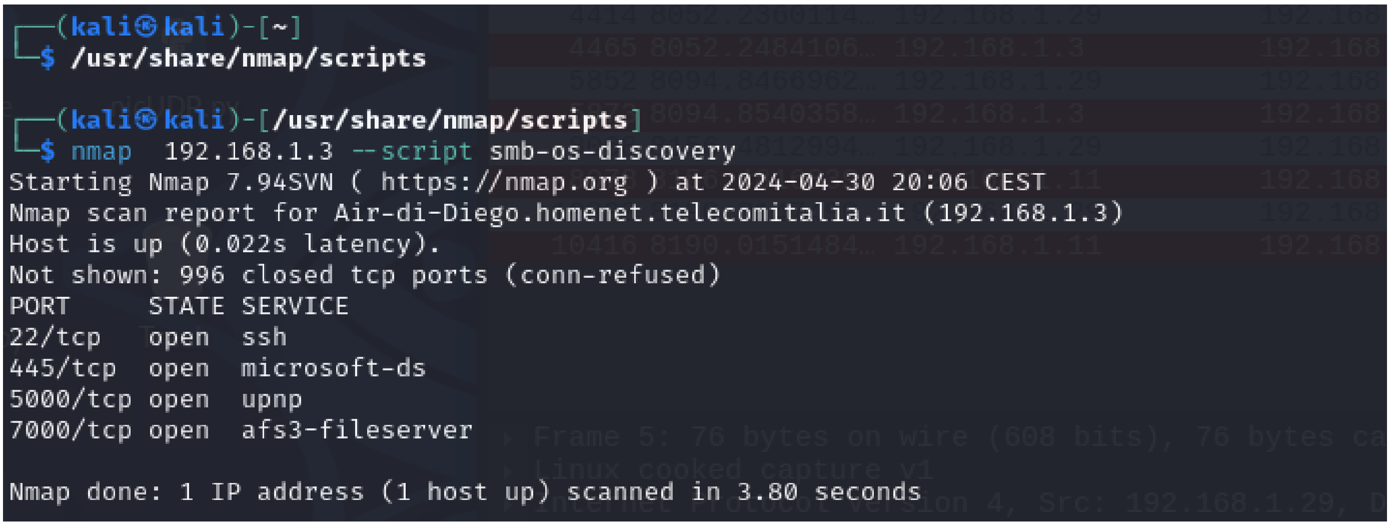
come si può vedere dall'immagine qui sotto



tcp.port == 80

```
No.   Time         Source         Destination    Protocol  Length Info
    6 0.379997577  192.168.1.29   192.168.1.26   TCP         76 44598 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3153172867 TSecr=0…
    7 0.380397164  192.168.1.26   192.168.1.29   TCP         76 80 → 44598 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=223547 T…
    8 0.380420494  192.168.1.29   192.168.1.26   TCP         68 44598 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3153172867 TSecr=223547
    9 0.380551087  192.168.1.29   192.168.1.26   TCP         68 44598 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3153172867 TSecr=223547
```

possiamo utilizzare gli script di nmap che si trovano
/usr/share/nmap/scripts
ma con metasploitable 2 non ritorna nessun risultato utile



```
┌──(kali㉿kali)-[~]
└─$ /usr/share/nmap/scripts

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap  192.168.1.3 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 20:06 CEST
Nmap scan report for Air-di-Diego.homenet.telecomitalia.it (192.168.1.3)
Host is up (0.022s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
445/tcp  open  microsoft-ds
5000/tcp open  upnp
7000/tcp open  afs3-fileserver

Nmap done: 1 IP address (1 host up) scanned in 3.80 seconds
```