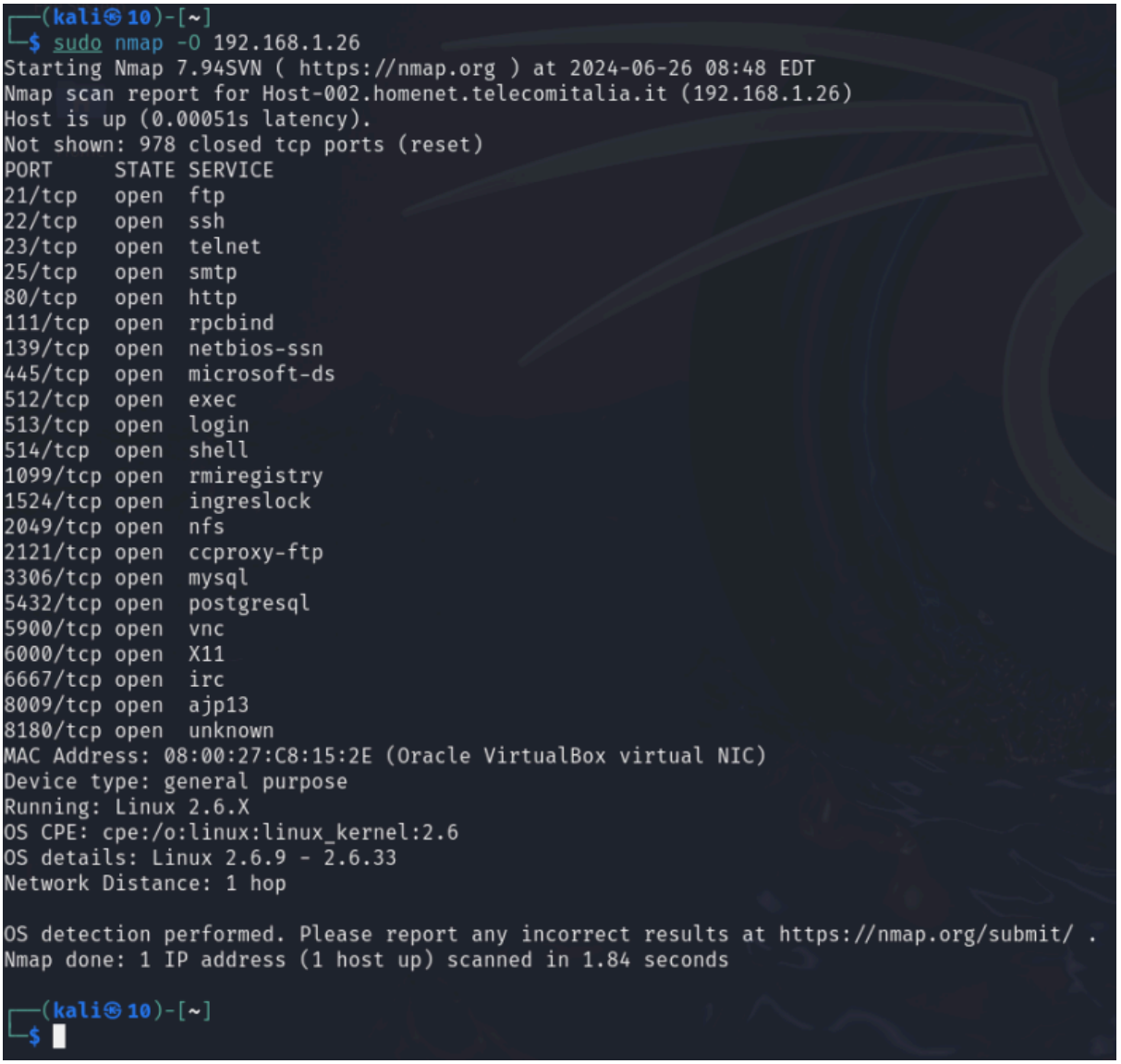
Scan su Metasploitable:

OS FINGERPRINT: (-O)

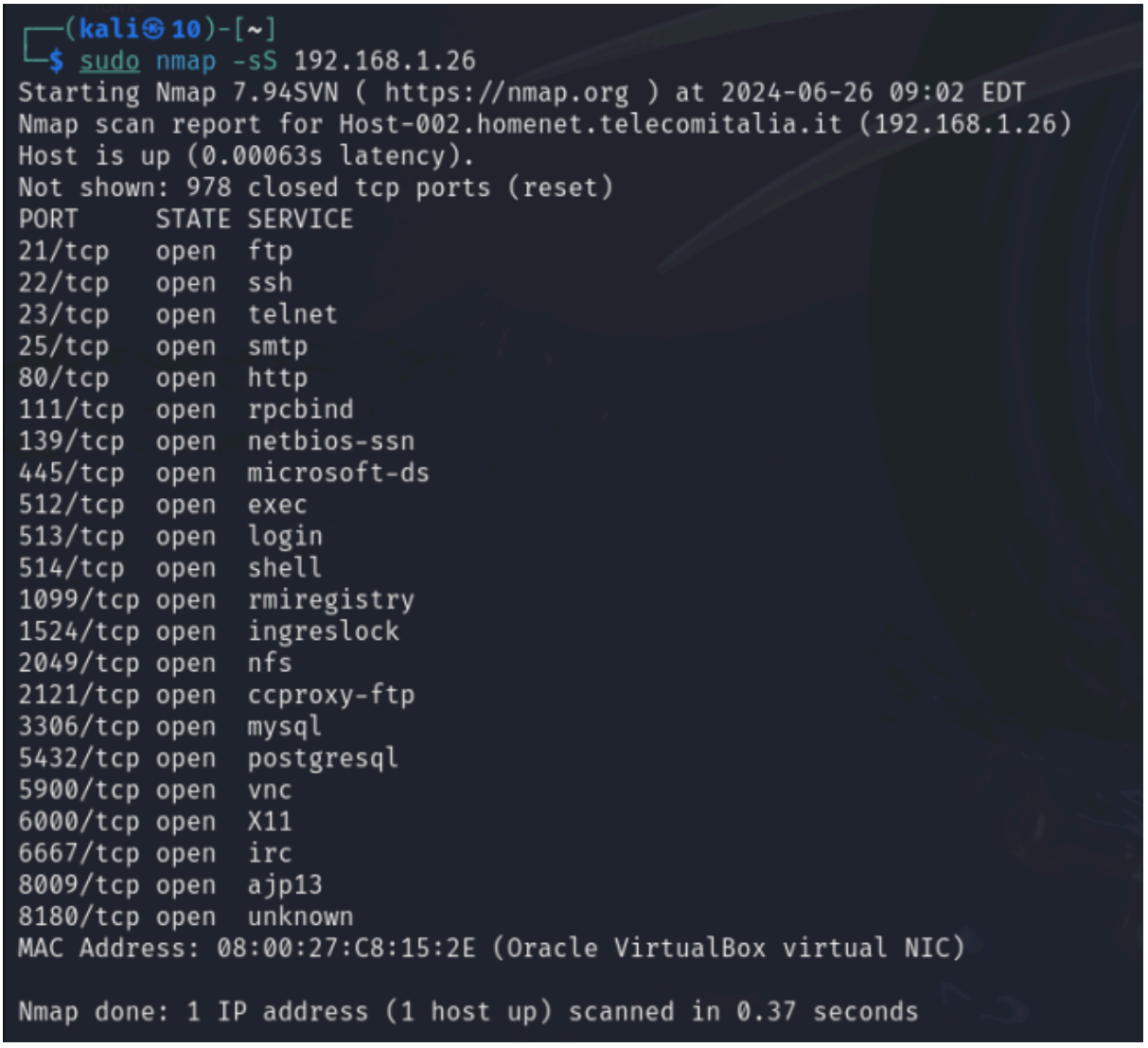
(ip source: 192.168.1.28)
(ip destination: 192.168.1.26)
OS details: Linux 2.6.9 - 2.6.33



SYN SCAN: (-sS)

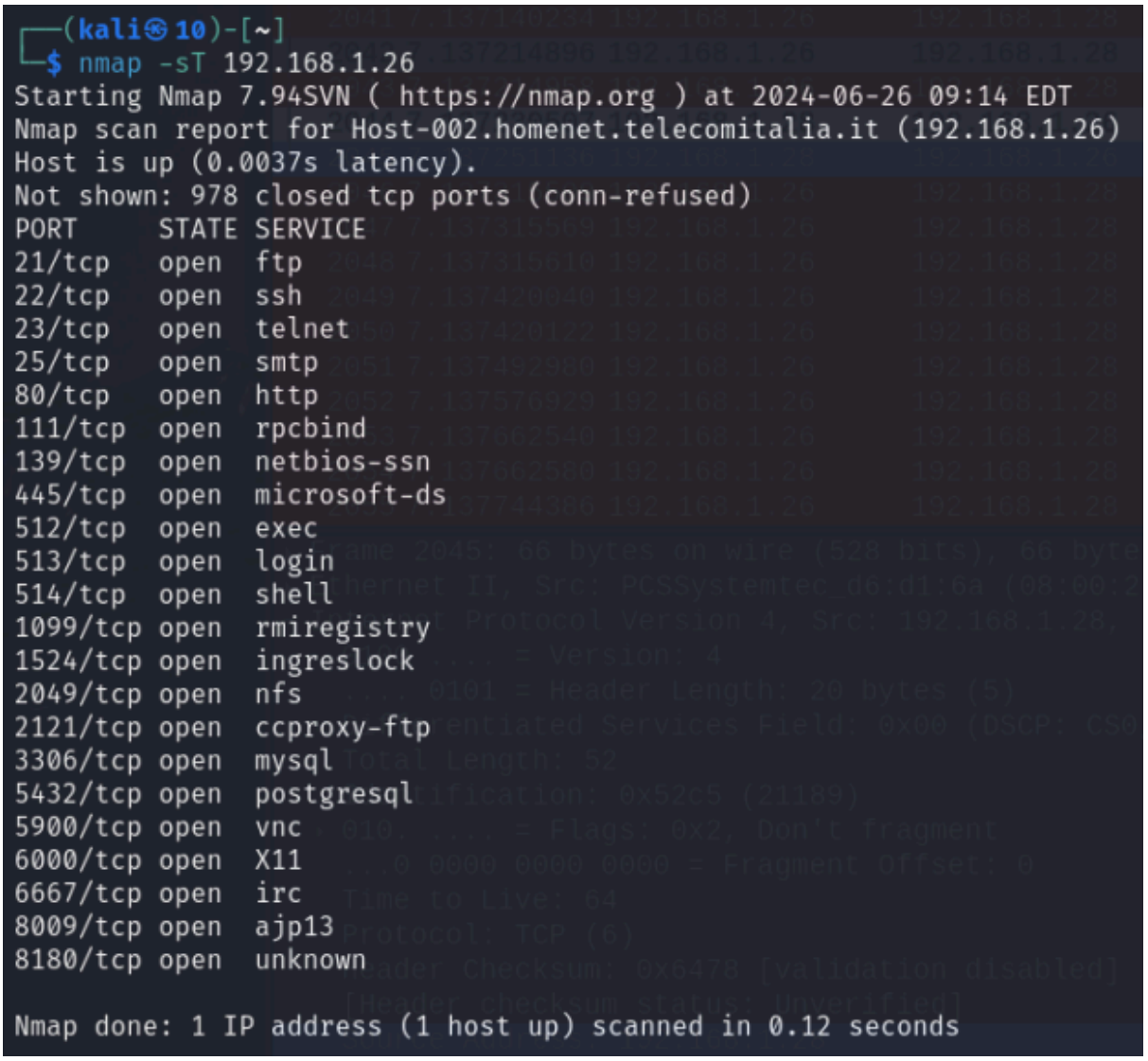
(ip source: 192.168.1.28)

(ip destination: 192.168.1.26)



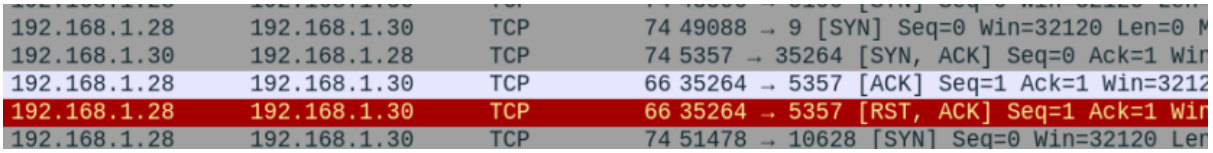
TCP CONNECT: (-sT)

(ip source: 192.168.1.28)
(ip destination: 192.168.1.26)

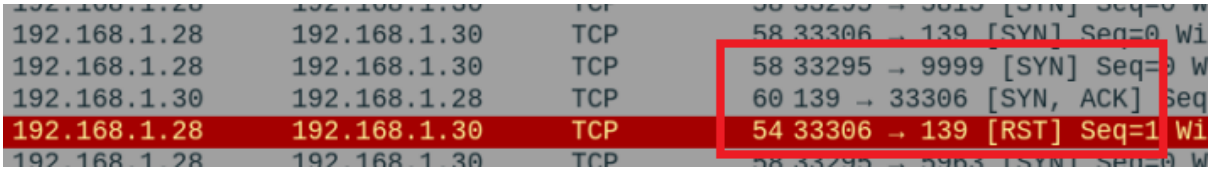


La differenza tra Syn Scan e TCP Connect risiede nel fatto che Syn Scan non completa il 3-way-handshake, ovvero la comunicazione SYN-SYN/ACK-ACK, ma chiude con RST la comunicazione creando meno disturbo in rete.

TCP Connect (nmap -sT)



Syn Scan (nmap -sS)



VERSION DETECTION: (-sV)

(ip source: 192.168.1.28)

(ip destination: 192.168.1.26)

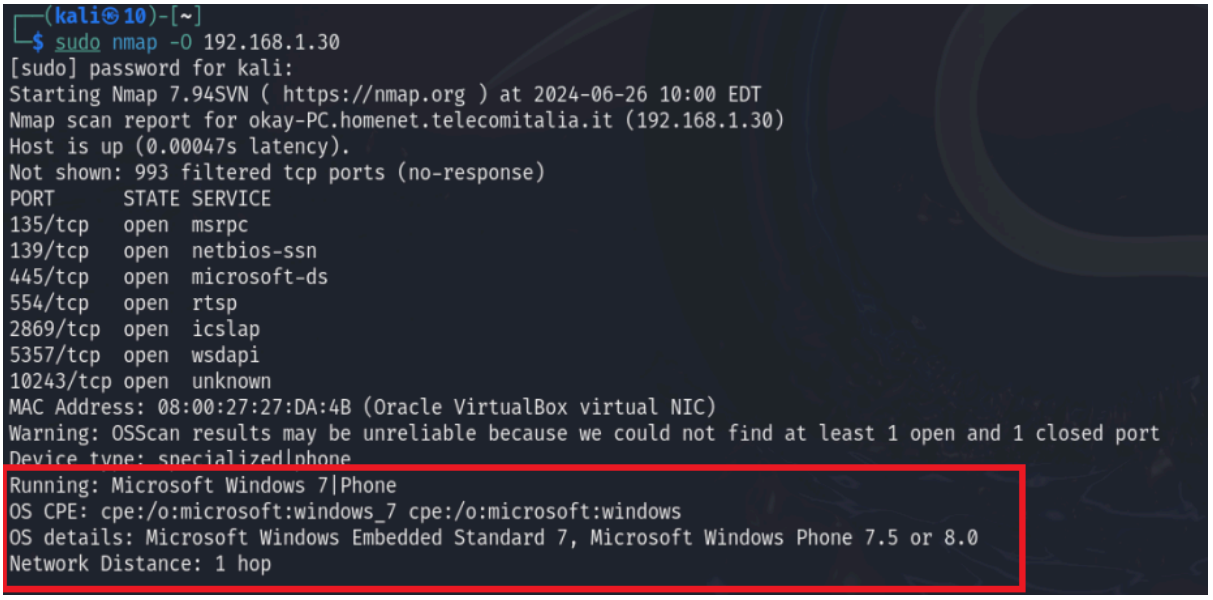
```
┌──(kali㉿10)-[~]
└─$ sudo nmap -sV -p 0-1024 192.168.1.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 09:26 EDT
Nmap scan report for Host-002.homenet.telecomitalia.it (192.168.1.26)
Host is up (0.00040s latency).
Not shown: 1014 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
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
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: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open  exec?
513/tcp open  login?
514/tcp open  tcpwrapped
MAC Address: 08:00:27:C8:15:2E (Oracle VirtualBox virtual NIC)
Service Info: Host:  metasploitable.localdomain; 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 65.09 seconds
```

Scan su Windows 7:

OS Fingerprint

(ip source: 192.168.1.28)
(ip destination: 192.168.1.30)
OS details: Microsoft Windows Embedded Standard 7



REPORT:

IP(source and destination)

(ip source: 192.168.1.28) on Kali Linux
(ip destination: 192.168.1.26) on Metasploitable
(ip destination: 192.168.1.30) on Windows 7

OS:

(ip destination: 192.168.1.26) on Metasploitable
OS details: Linux 2.6.9 - 2.6.33

(ip destination: 192.168.1.30) on Windows 7
OS details: Microsoft Windows Embedded Standard 7

PORTE APERTE:

(ip source: 192.168.1.28)
(ip destination: 192.168.1.26) on Metasploitable