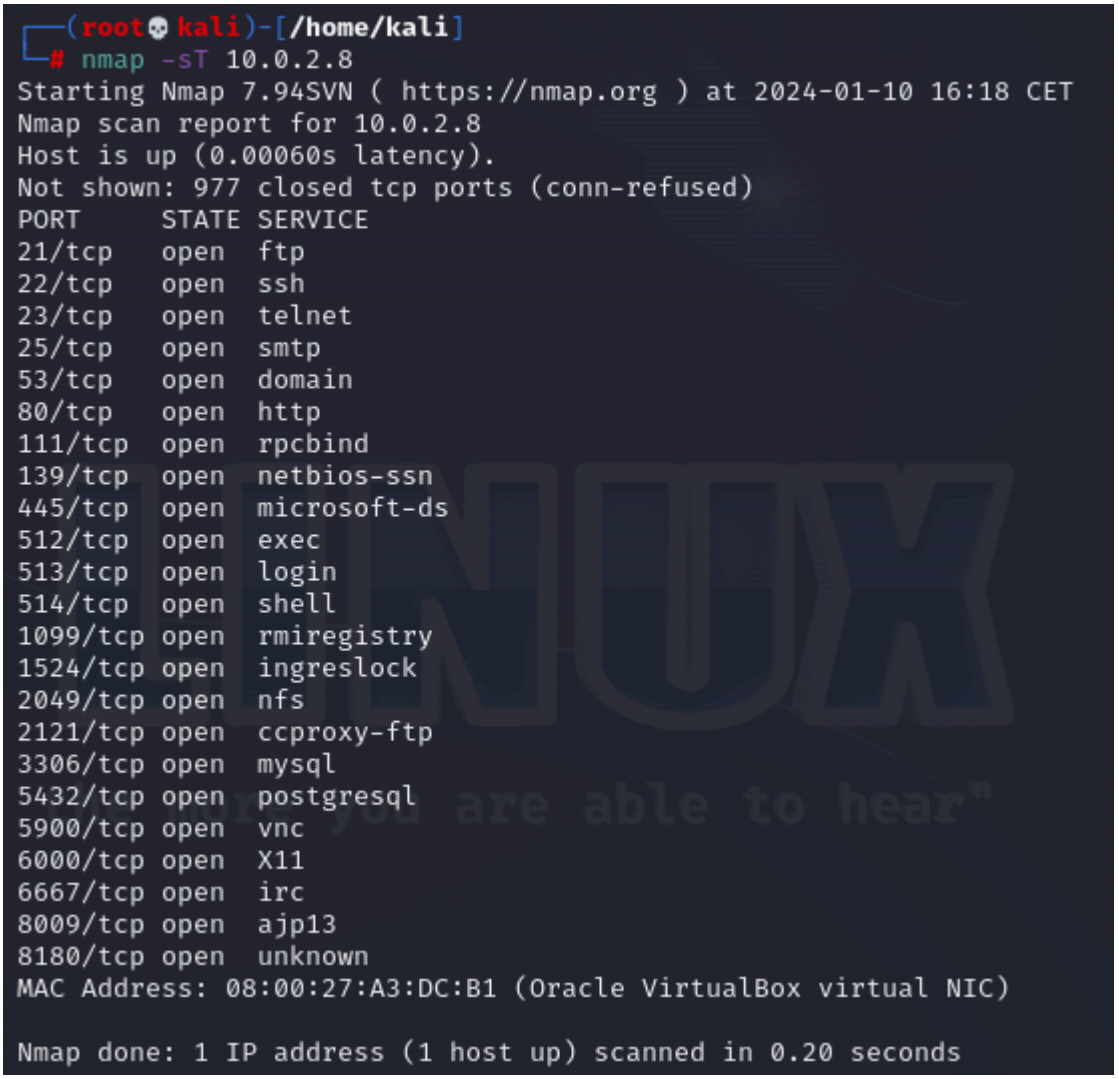
Nell’esercizio di oggi faremo pratica con Nmap. Nmap è un port scanner, un software open source in grado di eseguire la scansione di un target e restituire in output un serie di dati tra cui sistema operativo, porte aperte e chiuse e servizi attivi. Viene usato normalmente per il mapping di rete e per valutazioni di sicurezza. Il nostro primo target sarà metasploitable.

Come possiamo vedere dalla figura sopra tramite riga di comando siamo riusciti a eseguire uno scan delle porte del nostro target. L’opzione -sS sta a indicare una scansione SYN, un tipo di scansione poco invasivo che non conclude il three way handshake con il target per non essere rilevati dai dispositivi di sicurezza. In output ci indica per ogni numero di porta il tipo di protocollo di trasporto usato, se la porta è aperta e il servizio associato.



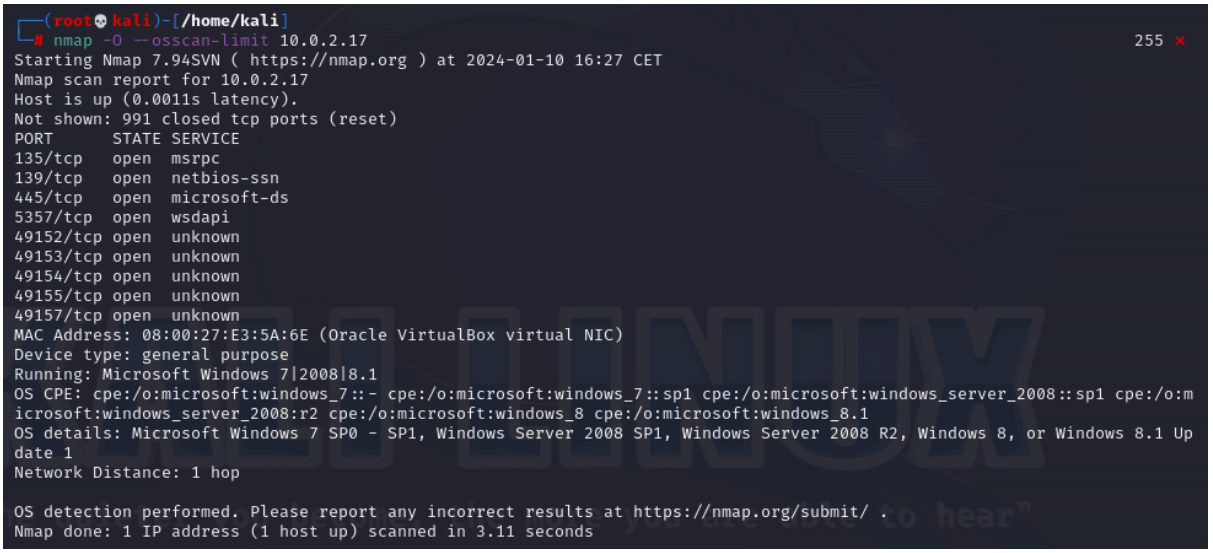
In questo altro esempio, simile al primo, viene usata l'opzione -sT (TCP connect), un altro tipo di scansione più invasiva che completa il three way handshake.

```
┌──(root💀kali)-[/home/kali]
└─# nmap -sV 10.0.2.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 16:03 CET
Nmap scan report for 10.0.2.8
Host is up (0.000084s 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 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  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        netkit-rsh rexecd
513/tcp  open  login?
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
```

L’opzione -sV richiede a Nmap di restituire anche la versione dei servizi attivi sul target.

```
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
```

Con l’opzione -O è possibile richiedere a nmap di cercare di capire che tipo di sistema operativo è in uso sul target. Questo tipo di scansione permette di risalire al sistema operativo inviando delle richieste e studiando le risposte. Ogni SO invierà risposte diverse date dalle differenti implementazioni degli stack di rete. Essendo differenze minime il risultato della scansione sarà una stima.
Il nostro prossimo bersaglio sarà Windows 7.



Possiamo vedere che con l'opzione -O, oltre al consueto scan delle porte, verrà restituito anche la stima del sistema operativo.