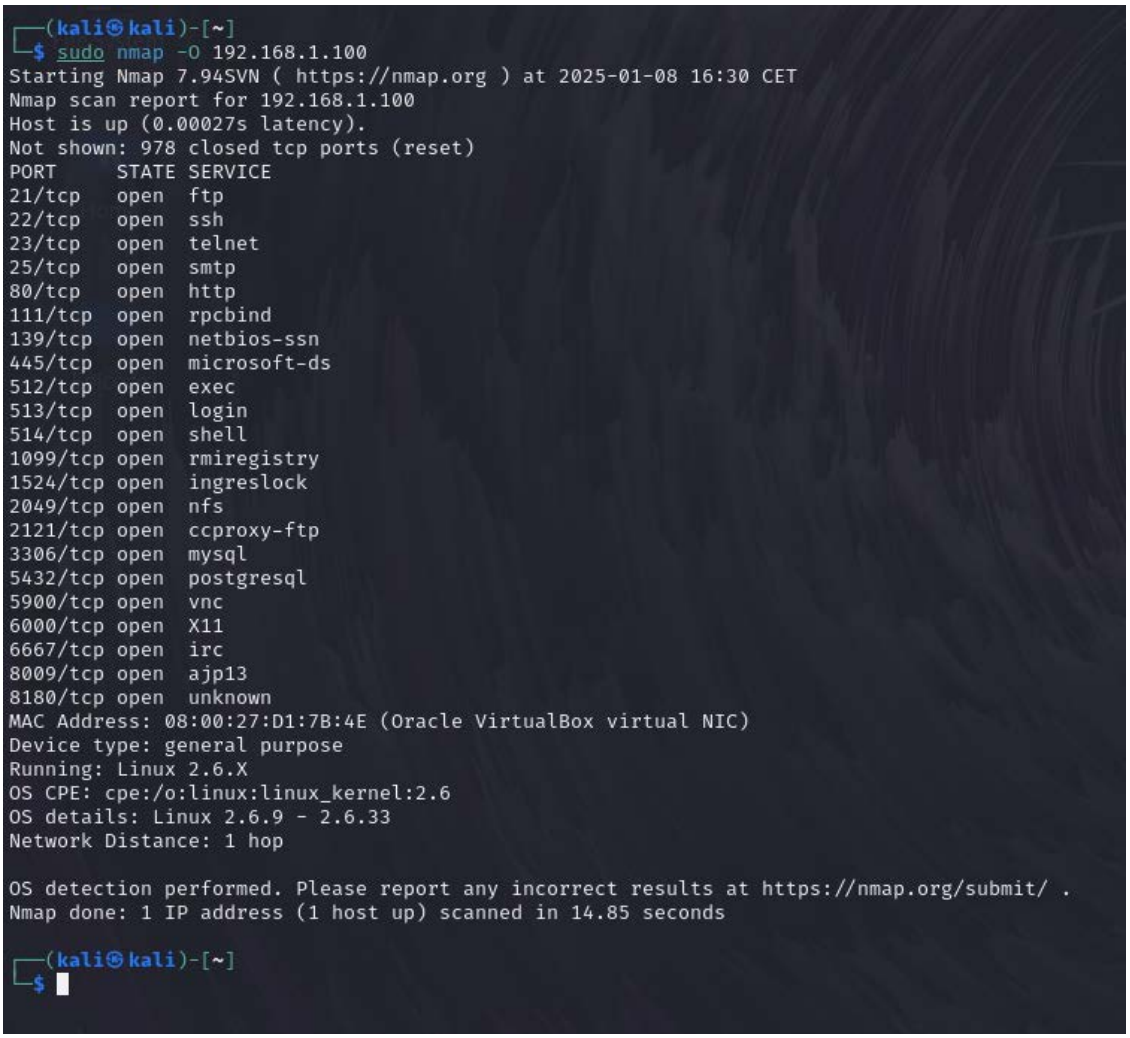
Report scansioni Nmap

Indirizzo IP Metasploitable: 192.168.1.100
Idirizzo IP Windows: 192.168.1.200

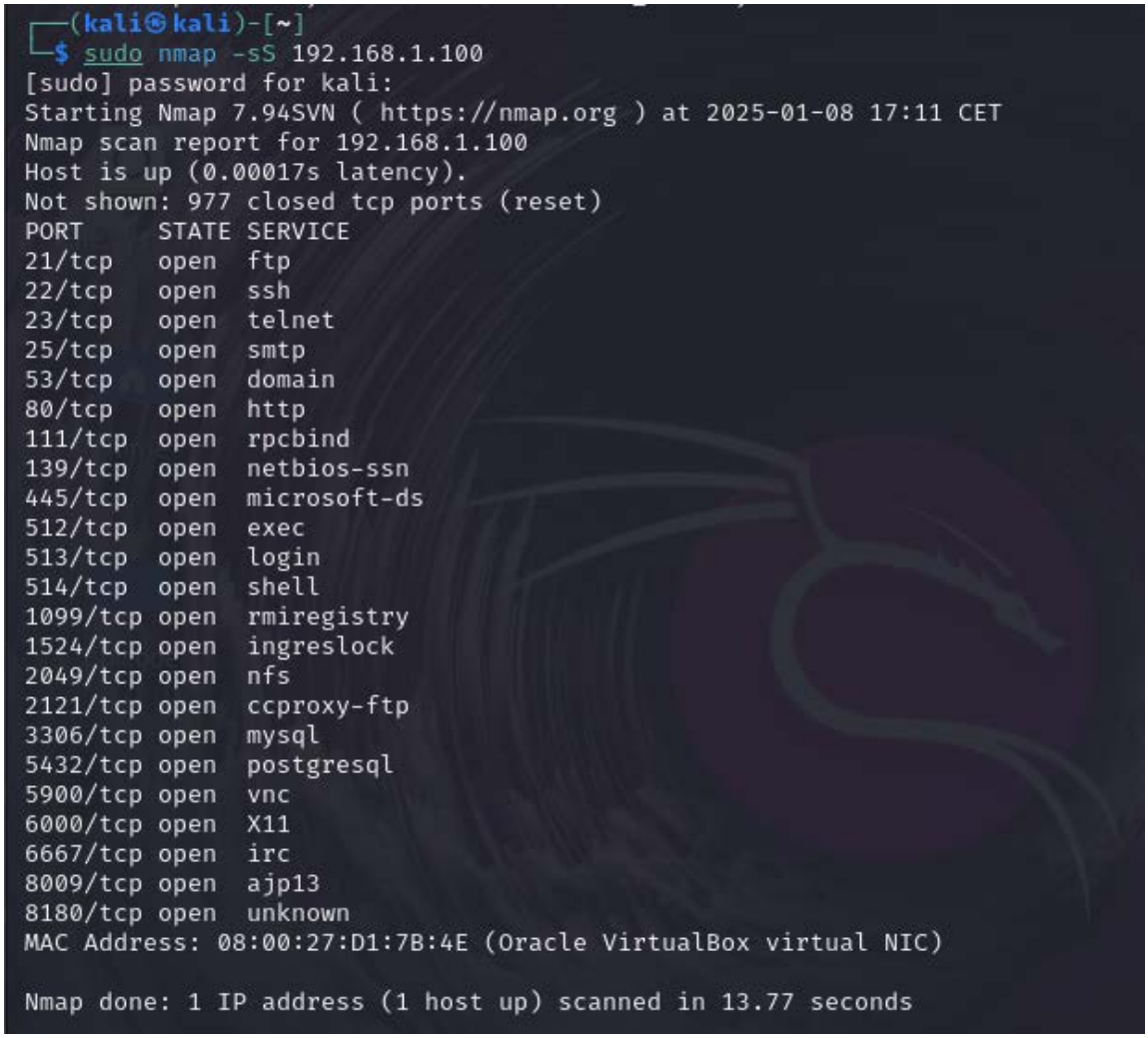
Prima Scansione: OS Fingerprint

Scopo della scansione: In questa scansione l'obbiettivo è determinare il sistema operativo utilizzato dalla macchina target, così da ottenere dei dettagli come la versione del kernel o altre caratteristiche del sistema.
Andremo ad utilizzare il comando "nmap -o + IP del target"



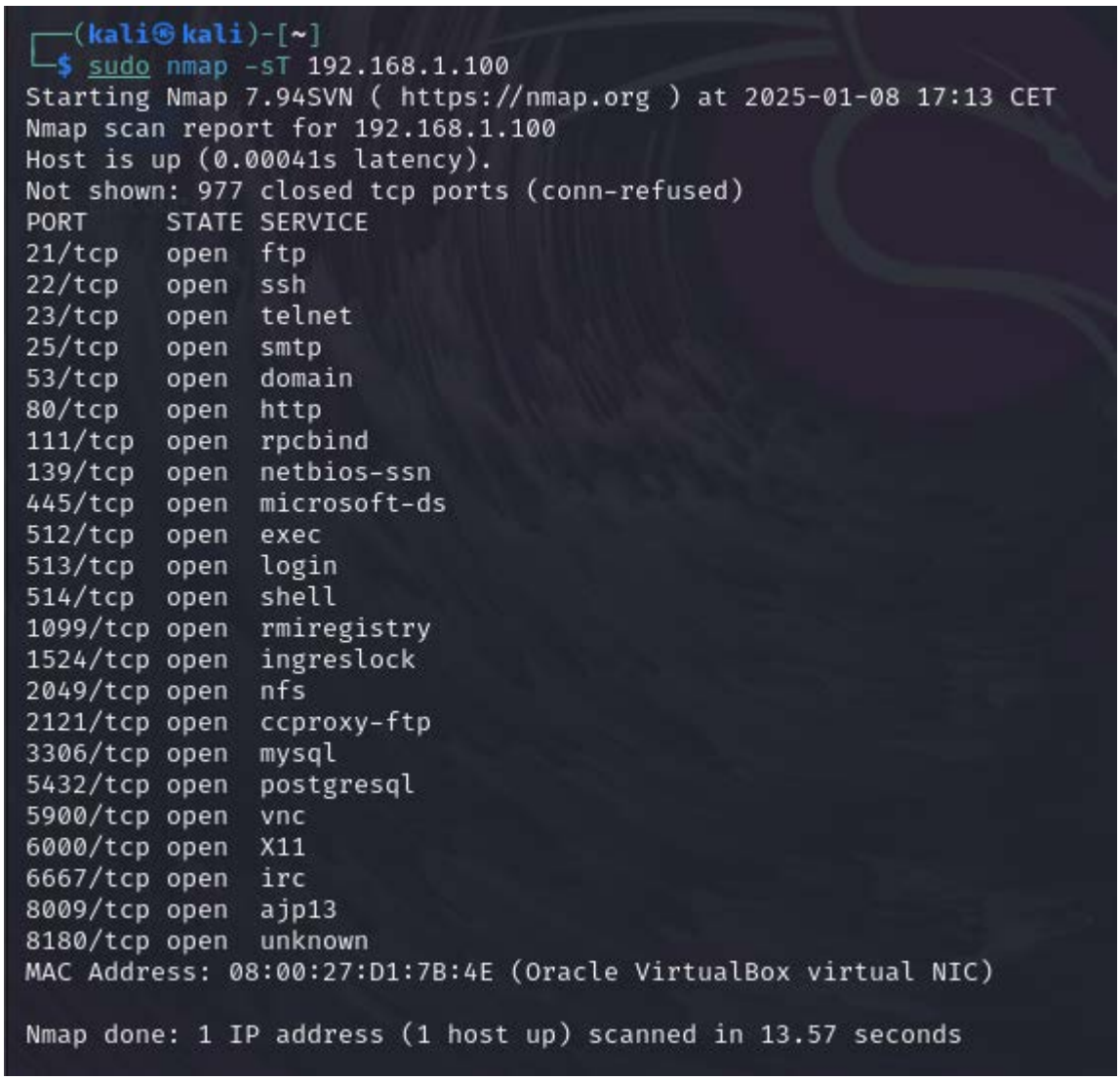
In questo caso il sistema operativo rilevato è Metasploitable.

La seconda scansione che andremo a fare sarà SYN Scan.
Questa scansione viene utilizzata per identificare le porte aperte del sistema senza andare a stabilire una connessione completa.
Il comando che andremo ad utilizzare sarà:
nmap -sS = l'IP della macchina target.



Il comando ha rilevato 23 porte aperte.

Il terzo comando che andremo ad utilizzare sarà il TCP Connect, questo comando viene utilizzato per effettuare una connessione completa alle porte aperte del target, ma non ci sono grandi differenze tra questo metodo ed il SYN Scan.



Otteniamo lo stesso risultato del metodo precedente.

Il quarto metodo è il Version Detection, quest'ultimo ha l'obbiettivo di determinare la versione esatta dei servizi in ascolto sulle porte aperte, ciò ci permette di identificare verioni vulnerabili o versioni obsolete.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 17:15 CET
Nmap scan report for 192.168.1.100
Host is up (0.00015s 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  shell       Netkit rshd
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:D1:7B:4E (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 66.25 seconds

┌──(kali㉿kali)-[~]
```

SCANSIONE OS FINGERPRINT SU WINDOWS 10

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 16:55 CET
Nmap scan report for 192.168.1.200
Host is up (0.00029s 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: 08:00:27:8A:1A:0D (Oracle VirtualBox virtual NIC)
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 24.58 seconds
```

Conclusioni

Metasploitable (192.168.1.100)
OS Fingerprint
IP: 192.168.1.100
Sistema Operativo: Linux 2.6.x (detected: Linux 2.6.9 - 2.6.33)
MAC Address: 08:00:27:D1:78:4E (Oracle VirtualBox virtual NIC)
Device Type: General Purpose
Distanza dalla rete: 1 hop
Porte Aperte

Porta	Stato	Servizio
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
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

Windows Target (192.168.1.200)
OS Fingerprint
IP: 192.168.1.200
Sistema Operativo: Microsoft Windows 10 (1709 - 1909)
MAC Address: 08:00:27:8A:1A:0D (Oracle VirtualBox virtual NIC)
Device Type: General Purpose
Distanza dalla rete: 1 hop
Porte Aperte

Porta	Stato	Servizio
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds