Esercizio Unit 2

S1L2

MIRKA FEBBO

Scansioni Nmap su Metasploitable

Relazione tecnica – Tecniche di scansione

Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection. E la seguente sul target Windows:
- OS fingerprint.

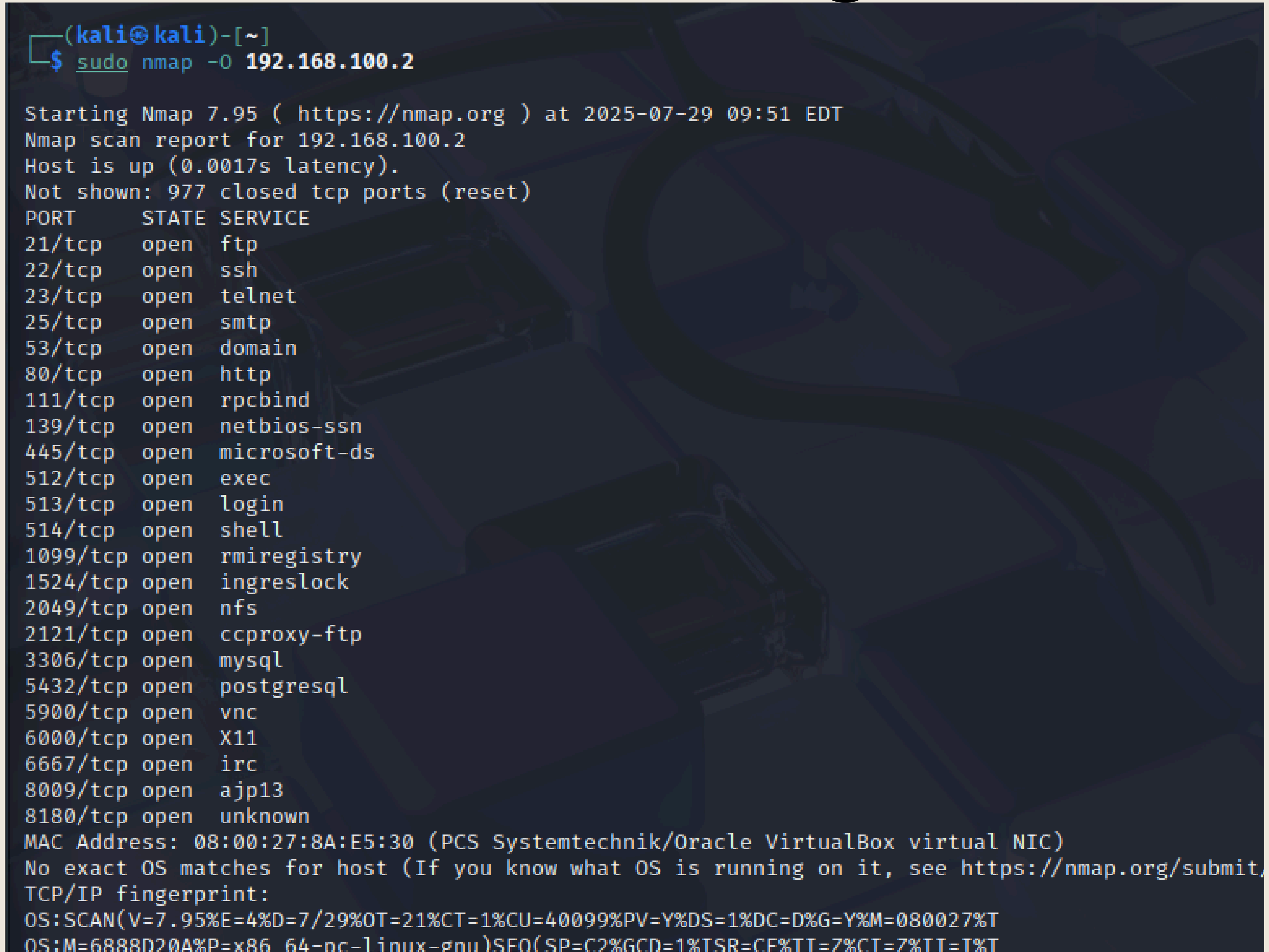
Topologia del laboratorio

Sistema	IP	Sistema Operativo	Ruolo
Kali Linux	192.168.100.10	Kali Linux Rolling	Scanner/Attaccante
Metasploitable 2	192.168.100.2	Linux vulnerabile	Bersaglio
Windows 10 Pro	192.168.100.30	Windows 10 Pro	Bersaglio

Tutte le VM sono collegate in modalità "Rete Interna" (VirtualBox), consentendo il traffico diretto tra loro.

Comando eseguito:

sudo nmap -O 192.168.100.2 effettua un fingerprinting passivo del sistema operativo, analizzando il comportamento TCP/IP del target.



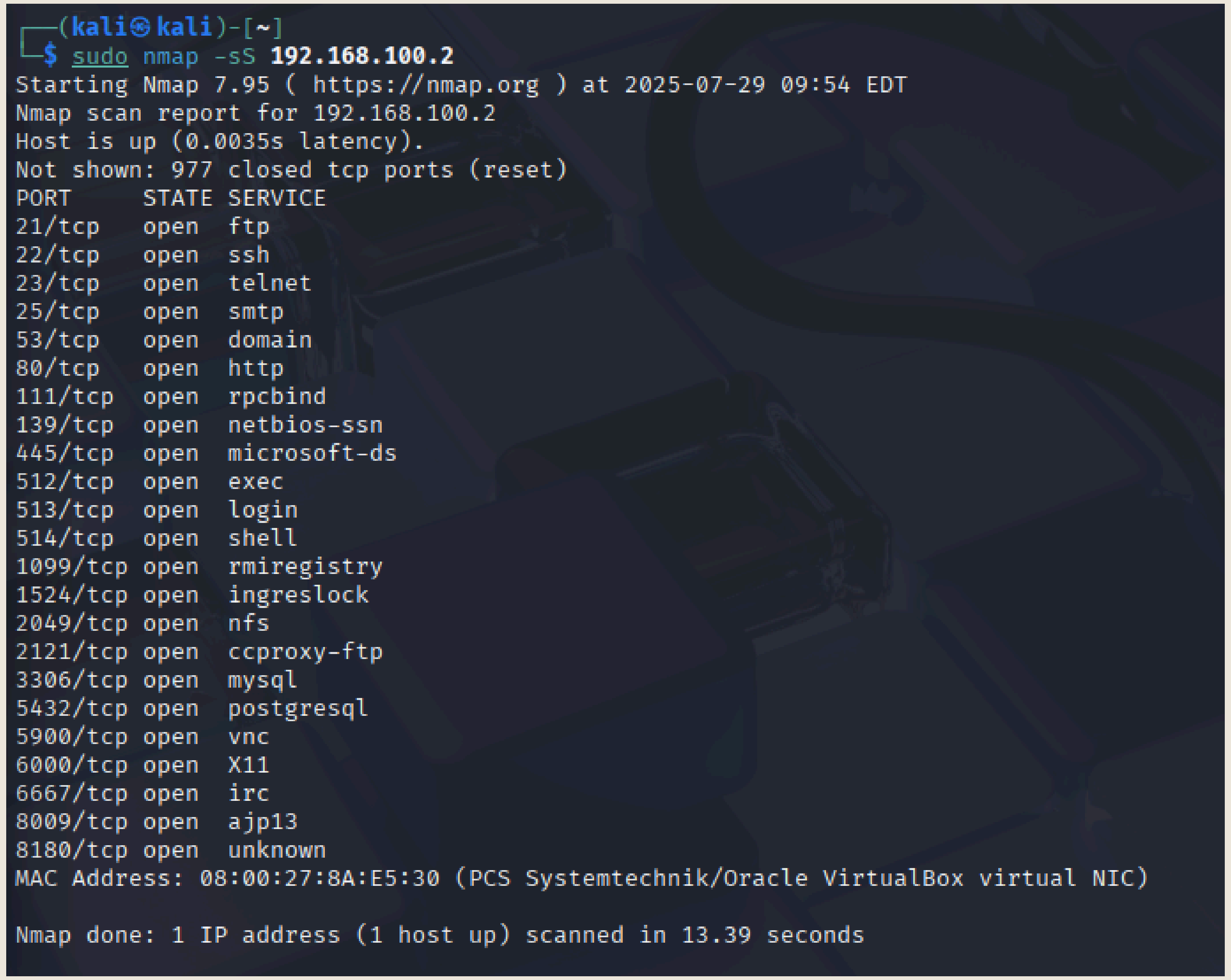
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.100.2

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:51 EDT
Nmap scan report for 192.168.100.2
Host is up (0.0017s 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: 08:00:27:8A:E5:30 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=7/29%OT=21%CT=1%CU=40099%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=6888D20A%P=x86_64-pc-linux-gnu)SEQ(SP=C2%GCD=1%ISR=CE%TI=Z%CI=Z%II=I%T
```

Comando eseguito:

sudo nmap -sS 192.168.100.2

La scansione SYN è una tecnica stealth che invia solo il pacchetto iniziale del handshake TCP. Non completa la connessione, riducendo la probabilità di rilevamento.

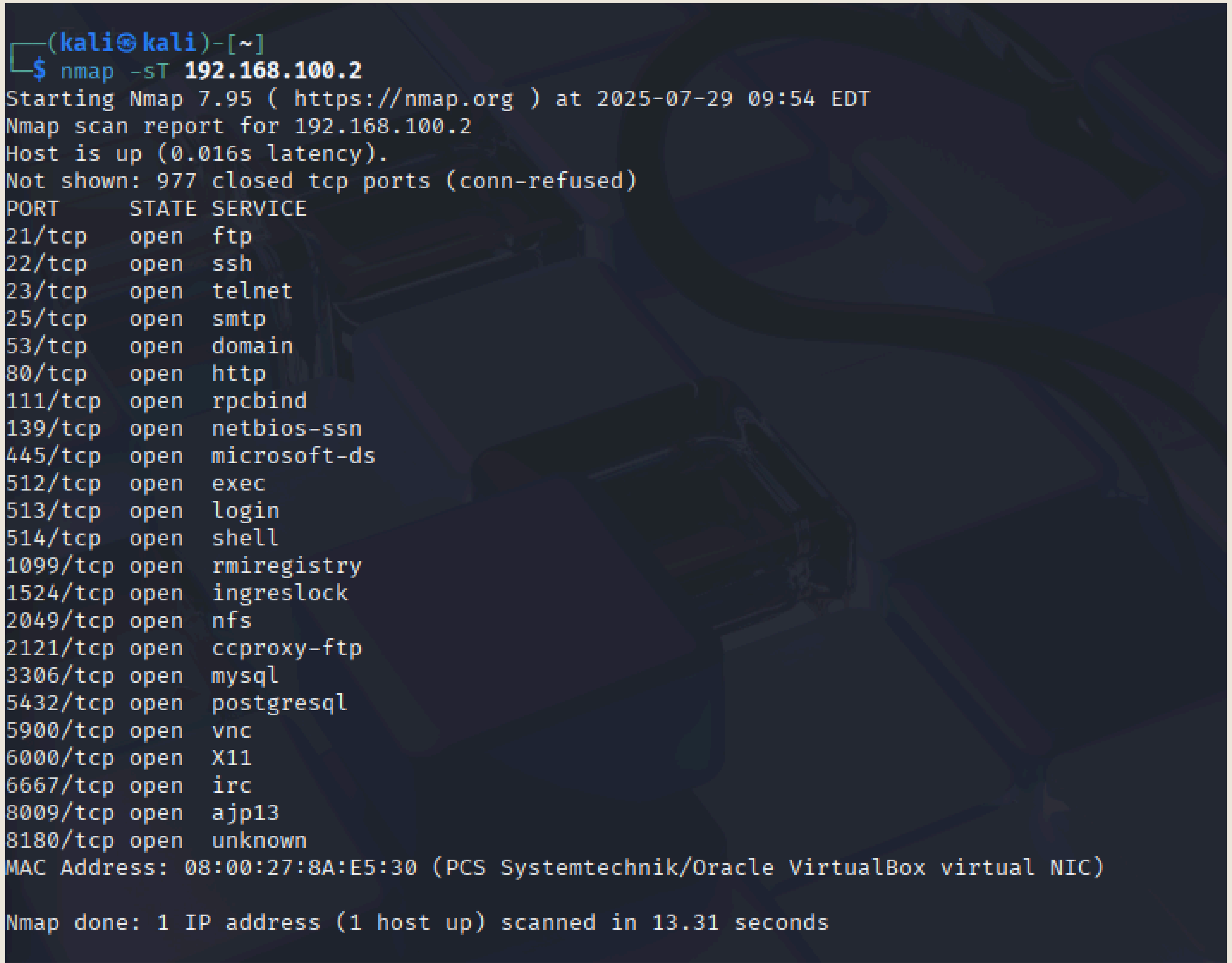


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.100.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:54 EDT
Nmap scan report for 192.168.100.2
Host is up (0.0035s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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: 08:00:27:8A:E5:30 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
```

Comando eseguito:

nmap -sT 192.168.100.2
Questa modalità esegue un handshake TCP completo. È utile quando l’utente non ha privilegi root, ma è più facile da rilevare da firewall o IDS.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.100.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:54 EDT
Nmap scan report for 192.168.100.2
Host is up (0.016s 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: 08:00:27:8A:E5:30 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
```

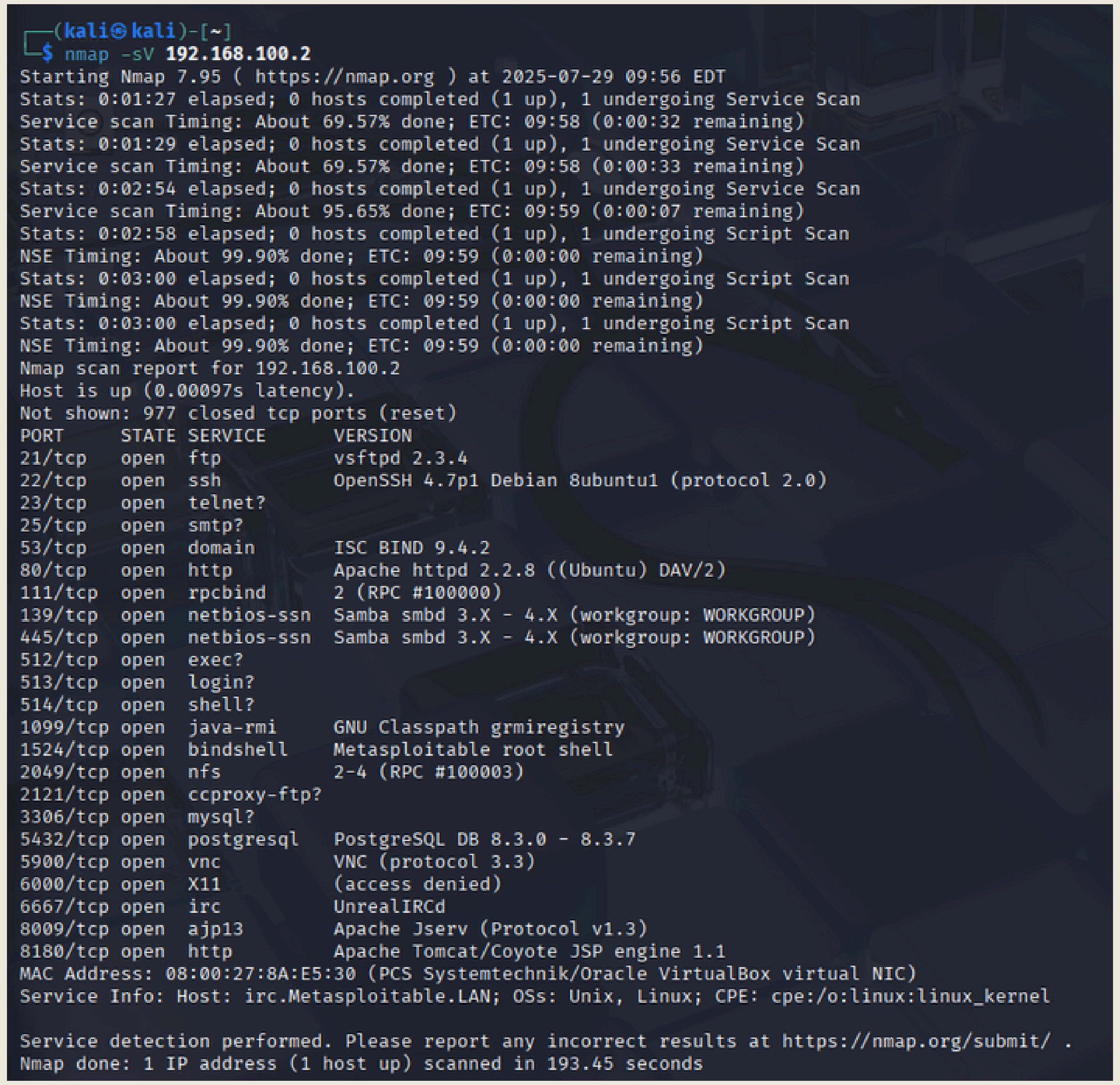
Confronto: SYN vs TCP Connect

Caratteristica	SYN Scan (-sS)	TCP Connect (-sT)
Privilegi richiesti	Sì (sudo)	No
Modalità	Handshake parziale (stealth)	Handshake completo
Visibilità	Bassa (non loggato)	Alta (più facile da tracciare)
Velocità	Maggiore	Leggermente inferiore
Accuratezza	Alta	Alta

Comando eseguito:

nmap -sV 192.168.100.2

Il flag -sV effettua una scansione di banner e fingerprint dei servizi attivi per identificarne nome e versione.



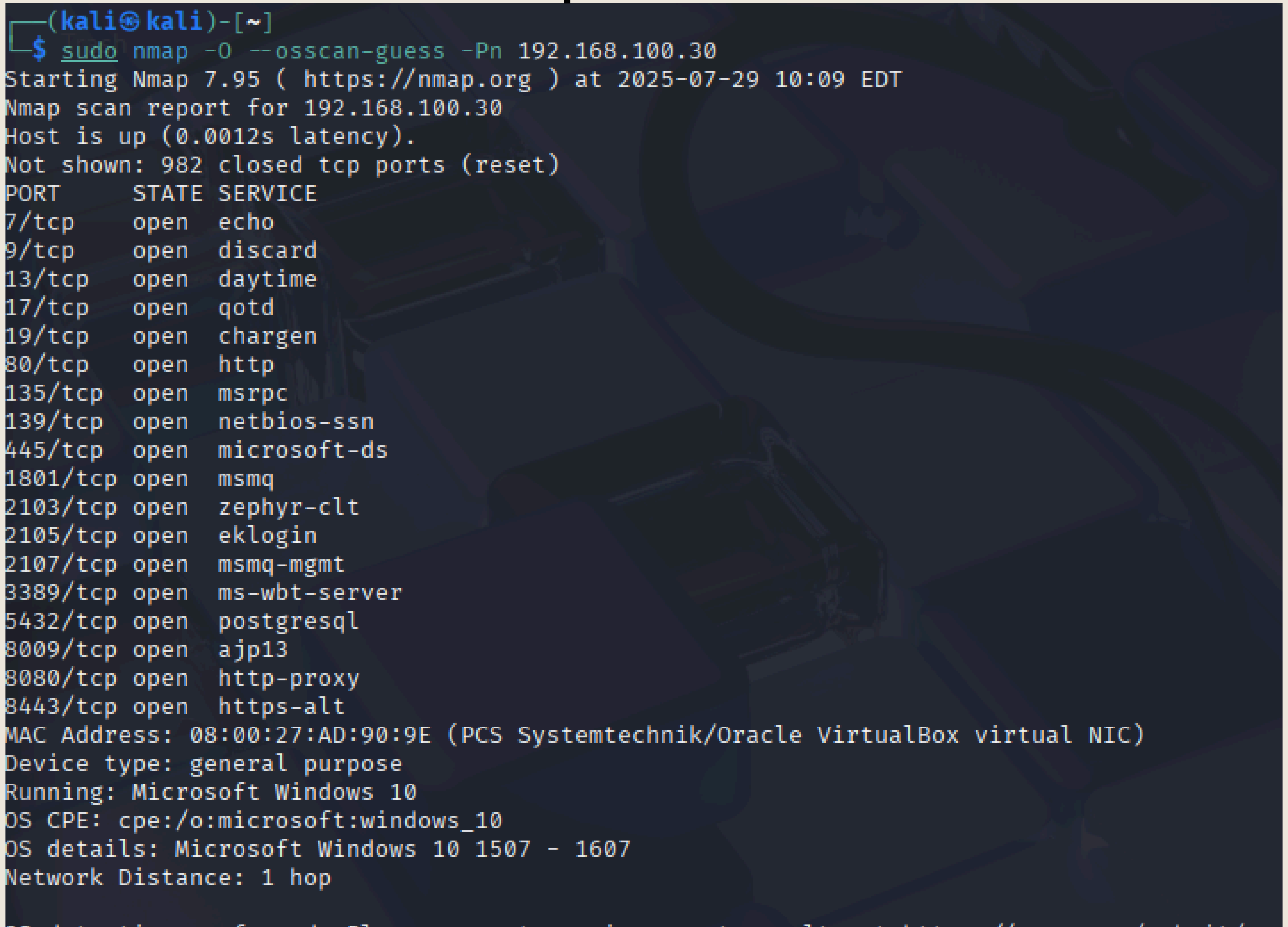
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.100.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:56 EDT
Stats: 0:01:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 69.57% done; ETC: 09:58 (0:00:32 remaining)
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 69.57% done; ETC: 09:58 (0:00:33 remaining)
Stats: 0:02:54 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 09:59 (0:00:07 remaining)
Stats: 0:02:58 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 09:59 (0:00:00 remaining)
Stats: 0:03:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 09:59 (0:00:00 remaining)
Stats: 0:03:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 09:59 (0:00:00 remaining)
Nmap scan report for 192.168.100.2
Host is up (0.00097s 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?
25/tcp   open  smtp?
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?
513/tcp  open  login?
514/tcp  open  shell?
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  ccproxy-ftp?
3306/tcp open  mysql?
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: 08:00:27:8A:E5:30 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 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 193.45 seconds
```

Comando eseguito:

sudo nmap -O --osscan-guess 192.168.100.30

Su sistemi Windows, il firewall può bloccare i pacchetti usati per il fingerprint. Con --osscan-guess, Nmap tenta una stima anche con informazioni parziali.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O --osscan-guess -Pn 192.168.100.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 10:09 EDT
Nmap scan report for 192.168.100.30
Host is up (0.0012s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
5432/tcp open  postgresql
8009/tcp open  ajp13
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: 08:00:27:AD:90:9E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 1 hop
```

Conclusioni

La suite di scansioni Nmap ha permesso di:
Mappare accuratamente i servizi esposti su Metasploitable e Windows
Identificare versioni di software obsolete o potenzialmente vulnerabili
Comparare due approcci di scansione TCP (SYN vs TCP Connect)
Comprendere i limiti del fingerprinting su sistemi moderni protetti (es. Windows 10)
Questo tipo di ricognizione rappresenta una fase fondamentale nel ciclo di un penetration test. Per un report più dettagliato allegherò anche il report di nmap in html, è stato bellissimo anche con qualche difficolta su windows e le varie macchine.