W11D1

Nmap Service Scan Report
&
[Optional] Same Subnet Scans

⋆ INDICE 1

1 Objective 2

2 Network Configuration 3

3 Scan Results 4

3.1 OS Fingerprint 4
3.2 SYN Scan 5
3.3 TCP Connect Scan 6
2.4 Version Detection 7 - 8
2.5 Confronto SYN vs TCP Connect 9

3 Description of Services 10- 11

4 [Optional] Same Subnet Scans 12

5 Objective 12

6 Network Configuration Updated 13

7 Scan Results |Same Subnet| 14

7.1 OS Fingerprint 14
7.2 SYN Scan 15
7.3 TCP Connect Scan 16
7.4 Version Detection 17 - 18

8 Differences from the Previous Configuration 19

1 Objective

- L'obiettivo di questo esame è eseguire scansioni di rete utilizzando Nmap sul target Metasploitable2 per identificare il sistema operativo, le porte aperte, i servizi attivi con le relative versioni e descriverne le funzionalità.

- Le scansioni effettuate includono OS fingerprint, SYN scan, TCP connect scan e version detection, con un confronto tra i risultati di SYN e TCP connect

2 Network Configuration

❍ **Attacking Machine** Kali Linux

- IP 192.168.50.100
- Operating System Kali Linux [latest version]

- Role: Esegue le scansioni Nmap

❍ **MachineTarget** Metasploitable2

- IP 192.168.51.101
- Operating System Linux [Ubuntu-based]

- Role: Sistema target per le scansioni

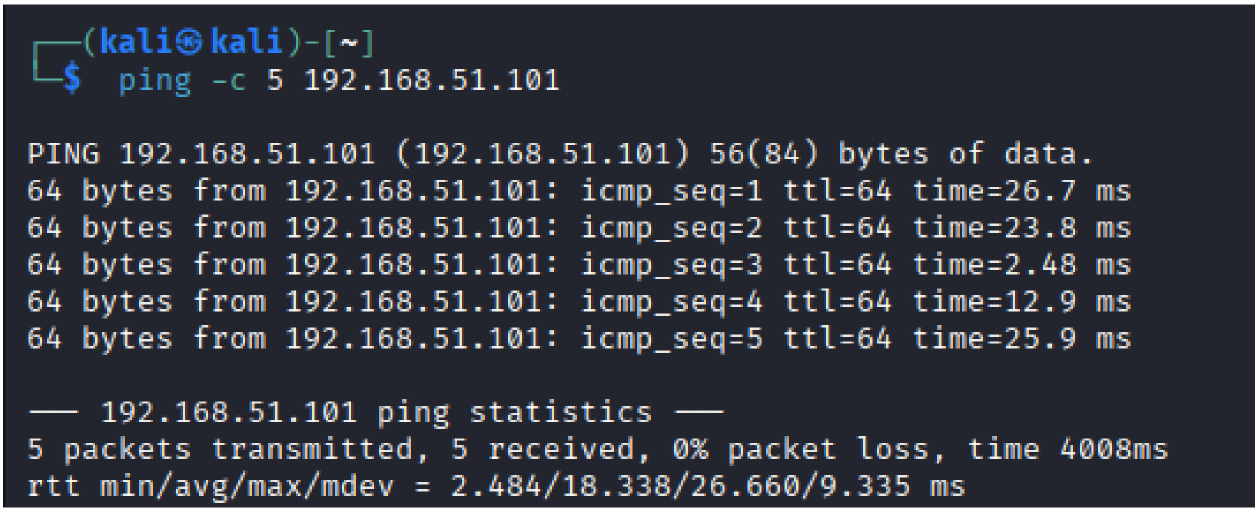
❍ **Router/Firewall** pfSense

- Latest version:

- WAN 192.168.1.197/25
- LAN1 [vtnet1] 192.168.50.1/24 [connessa a Kali]
- LAN2 [vtnet2] 192.168.51.1/24 [connessa a Metasploitable]

- Role: Instrada il traffico tra le due subnet [192.168.50.0/24 e 192.168.51.0/24]

❍ **Confirm Connectivity**: Eseguo ping da Kali a Metasploitable:



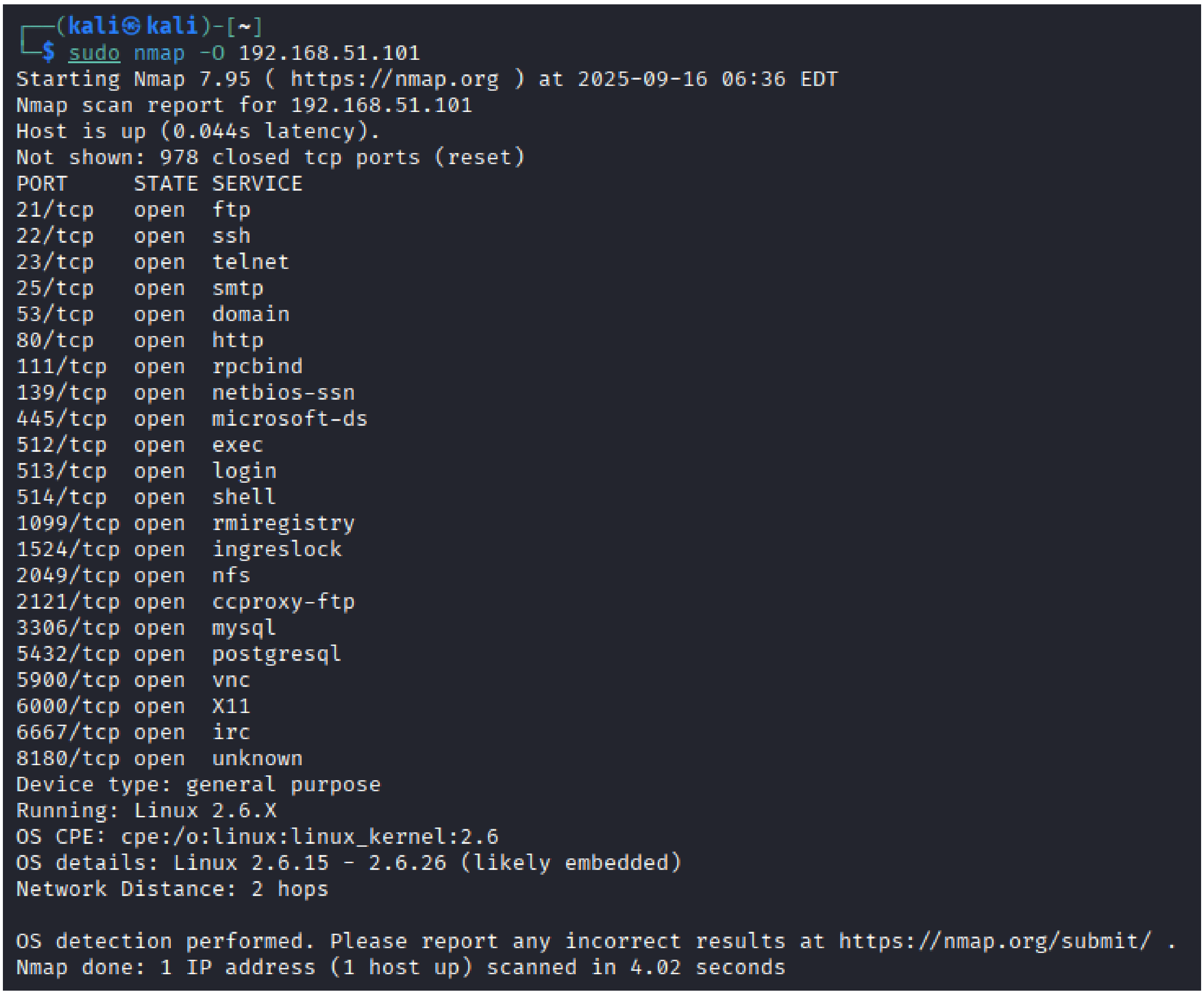
```
┌──(kali㉿kali)-[~]
└─$ ping -c 5 192.168.51.101

PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=64 time=26.7 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=64 time=23.8 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=64 time=2.48 ms
64 bytes from 192.168.51.101: icmp_seq=4 ttl=64 time=12.9 ms
64 bytes from 192.168.51.101: icmp_seq=5 ttl=64 time=25.9 ms

--- 192.168.51.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 2.484/18.338/26.660/9.335 ms
```

❍ Il ping conferma che il target è raggiungibile attraverso pfSense

3 Scan Results

3.1 OS Fingerprint

- Eseguo sudo nmap -O 192.168.51.101

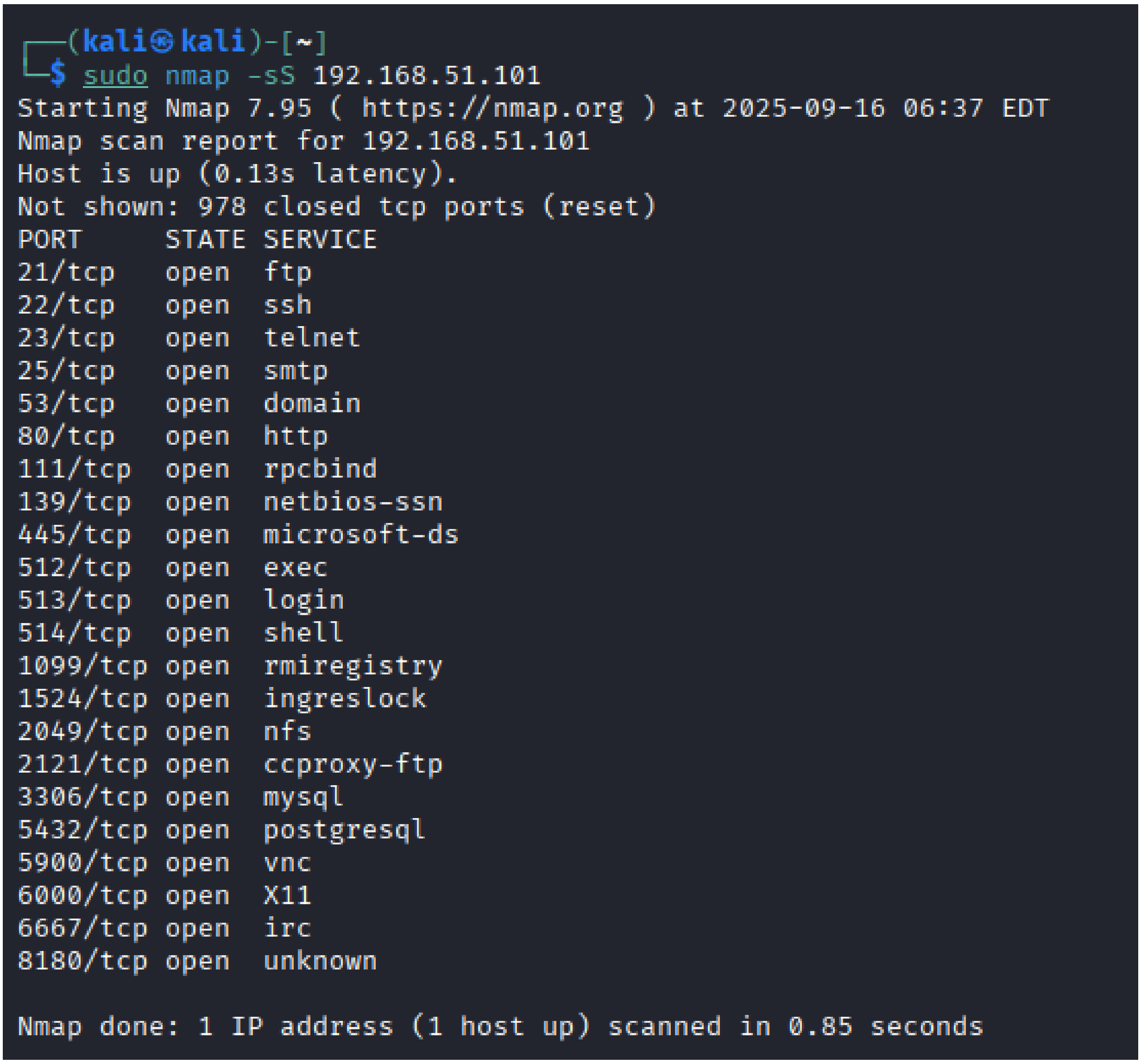


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-16 06:36 EDT
Nmap scan report for 192.168.51.101
Host is up (0.044s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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
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
8180/tcp open  unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.02 seconds
```

- **IP** 192.168.51.101
- Sistema Operativo: Linux 2.6.15 - 2.6.26 (likely embedded)
- **Details:** Linux kernel, probabilmente Ubuntu-based (Metasploitable2)
- **Open Ports**: 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8180 (TCP)

3.2 SYN Scan

- Esegio sudo nmap -sS 192.168.51.101

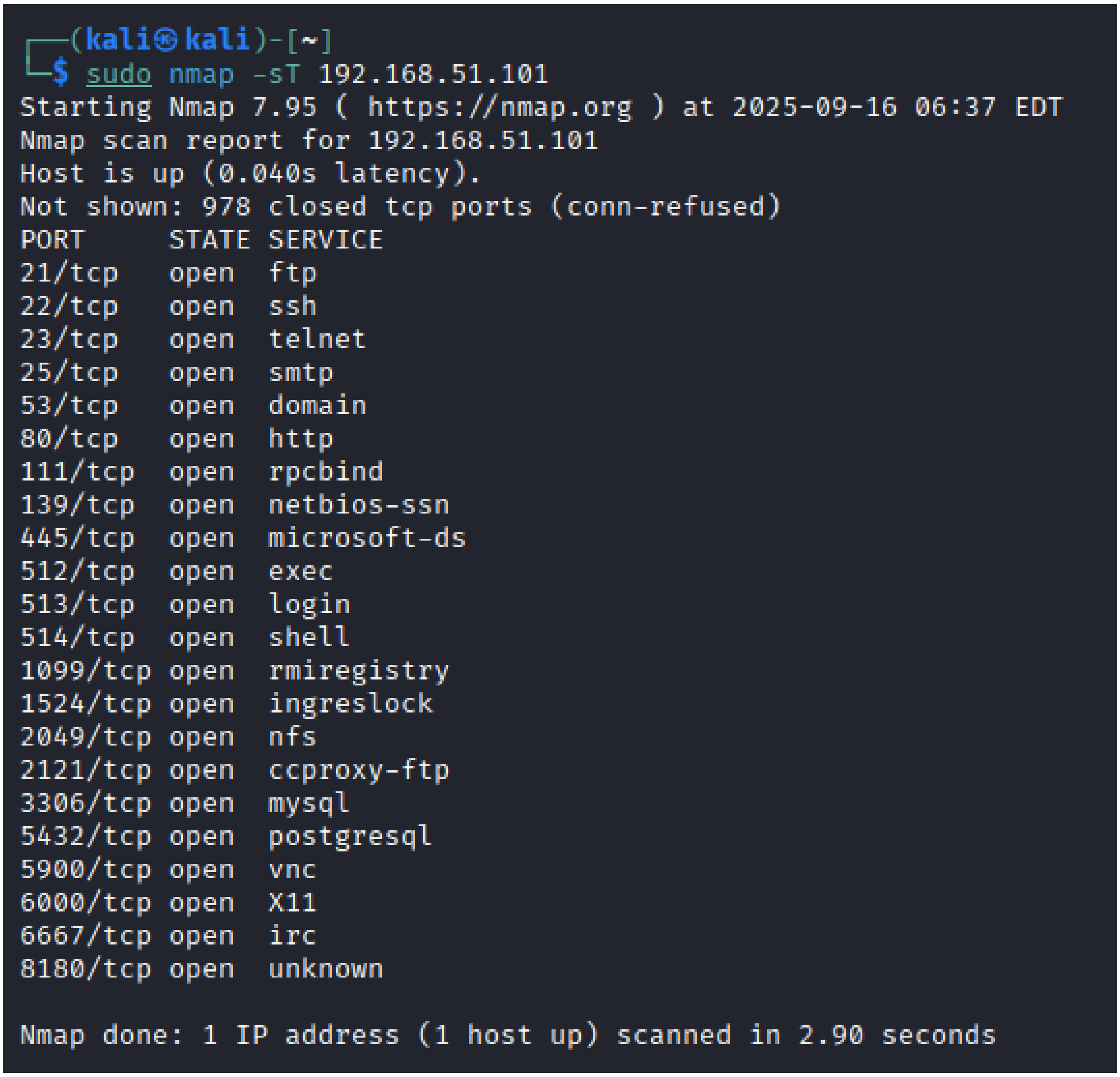


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-16 06:37 EDT
Nmap scan report for 192.168.51.101
Host is up (0.13s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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
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
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.85 seconds
```

- **Open Ports**: Identiche a OS fingerprint (21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8180)
- **Times**:0.85 secondi [scansione stealth, fast]

3.3 TCP Connect Scan

- Eseguo sudo nmap -sT 192.168.51.101



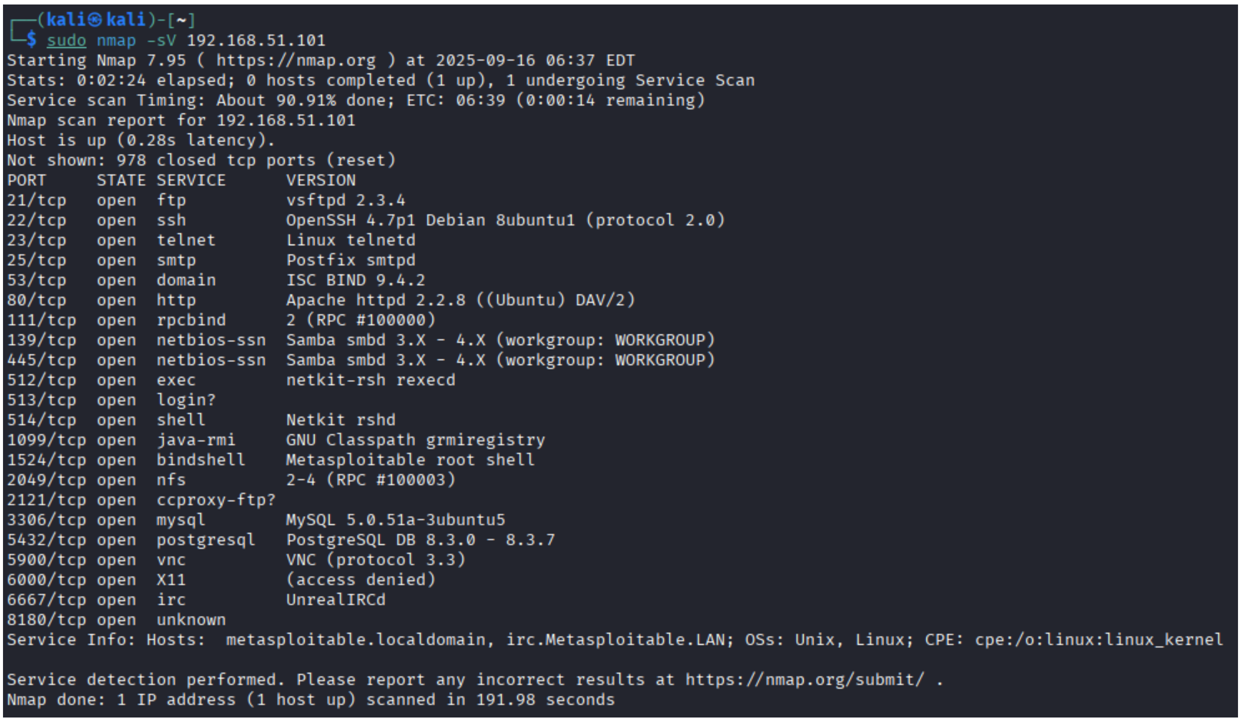
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-16 06:37 EDT
Nmap scan report for 192.168.51.101
Host is up (0.040s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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
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
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.90 seconds
```

- **Open Doors**: Identiche a SYN scan

- **Times**: 2.90 secondi [più lento, completa il 3-way-handshake]

2.4 Version Detection

- Eseguo sudo nmap -sV 192.168.51.101



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-16 06:37 EDT
Stats: 0:02:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 90.91% done; ETC: 06:39 (0:00:14 remaining)
Nmap scan report for 192.168.51.101
Host is up (0.28s 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  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  ccproxy-ftp?
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
8180/tcp  open  unknown
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 191.98 seconds
```

- **Open Doors and Services**:

- 21/tcp: vsftpd 2.3.4
- 22/tcp: OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
- 23/tcp: Linux telnetd
- 25/tcp: Postfix smtpd
- 53/tcp: ISC BIND 9.4.2
- 80/tcp: Apache httpd 2.2.8 (Ubuntu, DAV/2)
- 111/tcp: rpcbind 2 (RPC #100000)
- 139/tcp: Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
- 445/tcp: Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
- 512/tcp: netkit-rsh rexecd
- 513/tcp: login
- 514/tcp: Netkit rshd
- 1099/tcp: GNU Classpath grmiregistry
- 1524/tcp: Metasploitable root shell
- 2049/tcp: nfs 2-4 (RPC #100003)
- 2121/tcp: ccproxy-ftp
- 3306/tcp: MySQL 5.0.51a-3ubuntu5
- 5432/tcp: PostgreSQL DB 8.3.0 - 8.3.7
- 5900/tcp: VNC (protocol 3.3)
- 6000/tcp: X11 (access denied)
- 6667/tcp: UnrealIRCd
- 8180/tcp: unknown

- **Times** 191.98 secondi [più lento per rilevazione banner]
- **Info additional Hostnames**:
  - metasploitable.localdomain
  - irc.Metasploitable.LAN
  - OS: Unix/Linux

2.5 Confronto SYN vs TCP Connect

- **Open Doors**: Identiche in entrambe le scansioni [22 porte TCP aperte]

- **Differences**:

- **Speed**: SYN scan (0.85s) più veloce di TCP connect (2.90s) perché non completa il 3-way-handshake.

- **Stealth**: SYN è più furtivo [non loggato dalle applicazioni target] mentre TCP connect genera log visibili.

- **Output**: SYN riporta porte chiuse come "reset", TCP come "conn-refused", ma nessuna discrepanza pratica nel rilevamento delle porte aperte in questo caso, molto probabilmente perché pfSense non filtra attivamente.

3 Description of Services

- **21/tcp (FTP, vsftpd 2.3.4)**: File Transfer Protocol per trasferimento file.
  - Vulnerabile a backdoor note (vsftpd 2.3.4).

- **22/tcp (SSH, OpenSSH 4.7p1)**: Secure Shell per accesso remoto sicuro.
  - Versione datata, potenzialmente vulnerabile.

- **23/tcp (Telnet, Linux telnetd)**: Accesso remoto non sicuro (plain-text), alto rischio di intercettazione.

- **25/tcp (SMTP, Postfix)**: Simple Mail Transfer Protocol per invio email.
  - Configurazioni errate possono essere sfruttate.

- **53/tcp (DNS, ISC BIND 9.4.2)**: Domain Name System per risoluzione nomi.
  - Versione vecchia, nota per vulnerabilità.

- **80/tcp (HTTP, Apache 2.2.8)**: Web server, supporta DAV/2.
  - Potenzialmente vulnerabile a exploit noti.

- **111/tcp (rpcbind)**: Gestisce servizi RPC, usato per NFS/Samba.
  - Espone informazioni sensibili.

- **139/445 (Samba smbd 3.X-4.X)**: Condivisione file/stampanti.
- Versioni vulnerabili a exploit come EternalBlue.

- **512/513/514 (rsh/rexecd/login)**: Servizi remoti obsoleti, non sicuri, permettono accesso non autenticato in alcune configurazioni.

- **1099/tcp (Java RMI)**: Registro per applicazioni Java, potenzialmente sfruttabile per esecuzione remota.

- **1524/tcp (Metasploitable root shell)**: Backdoor nota di Metasploitable, accesso root diretto.

- **2049/tcp (NFS)**: Network File System, condivisione file.
  - Configurazioni deboli permettono accessi non autorizzati.

- **2121/tcp (ccproxy-ftp)**: Servizio FTP alternativo, dettagli non chiari, possibile misconfigurazione.

- **3306/tcp (MySQL 5.0.51a)**: Database MySQL, versione vulnerabile a exploit noti.

- **5432/tcp (PostgreSQL 8.3.0-8.3.7)**: Database PostgreSQL, versione datata con potenziali vulnerabilità.

- **5900/tcp (VNC)**: Virtual Network Computing per desktop remoto.
  - Protocollo 3.3, rischio se password deboli.

- **6000/tcp (X11)**: Sistema grafico, accesso negato ma presente.
  - Possibile configurazione errata.

- **6667/tcp (UnrealIRCd)**: Server IRC, versione vulnerabile a exploit noti.

- **8180/tcp (unknown)**: Servizio non identificato, richiede ulteriori indagini.

4 [Optional] Same Subnet Scans

5 Objective

- L'obiettivo per questo esame facoltativo è spostare Metasploitable2 dalla subnet 192.168.51.0/24 [collegata a pfSense vtnet2] alla subnet 192.168.50.0/24 [stessa di Kali, collegata a pfSense vtnet1] così che entrambe le macchine siano sulla stessa rete.

6 Network Configuration Updated

- **Attacking Machine** Kali Linux

- IP 192.168.50.100
- Operating System Kali Linux [latest version]

- Role: Esegue le scansioni Nmap

- **MachineTarget** Metasploitable2

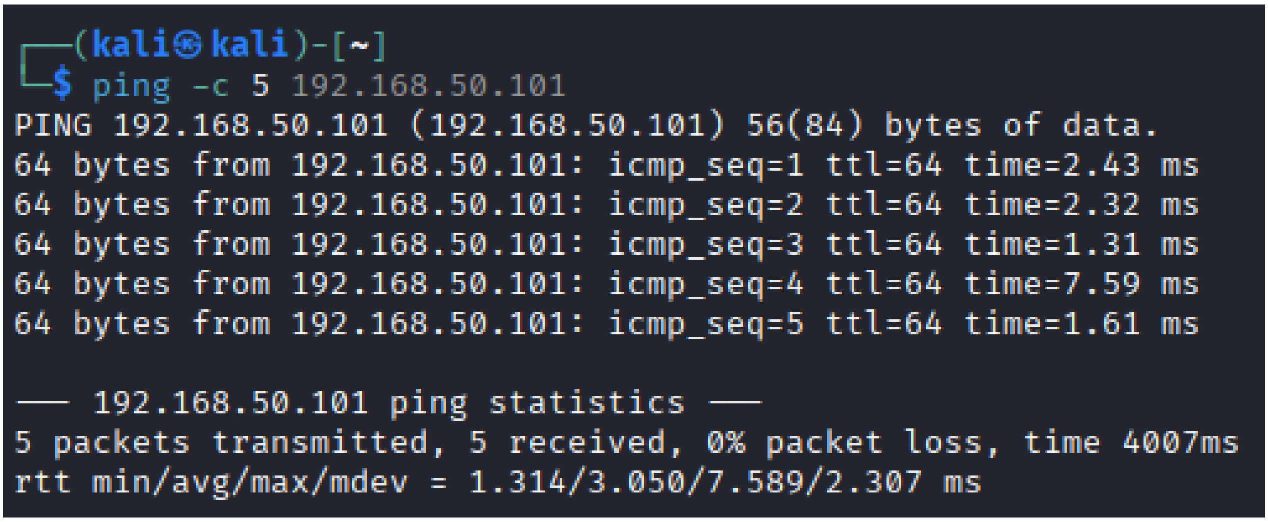
- IP 192.168.50.101 [precedentemente 192.168.51.101]
- Operating System Linux [Ubuntu-based]

- Role: Sistema target per le scansioni

- **Net** Entrambe le macchine sulla subnet 192.168.50.0/24, connesse direttamente senza routing tramite pfSense.

- **Info additional** Metasploitable2 era già configurato in passato per operare sia sulla rete 192.168.51.0/24 (con pfSense) sia sulla rete 192.168.50.0/24.

- **Confirm Connectivity** Eseguo ping da Kali a Metasploitable



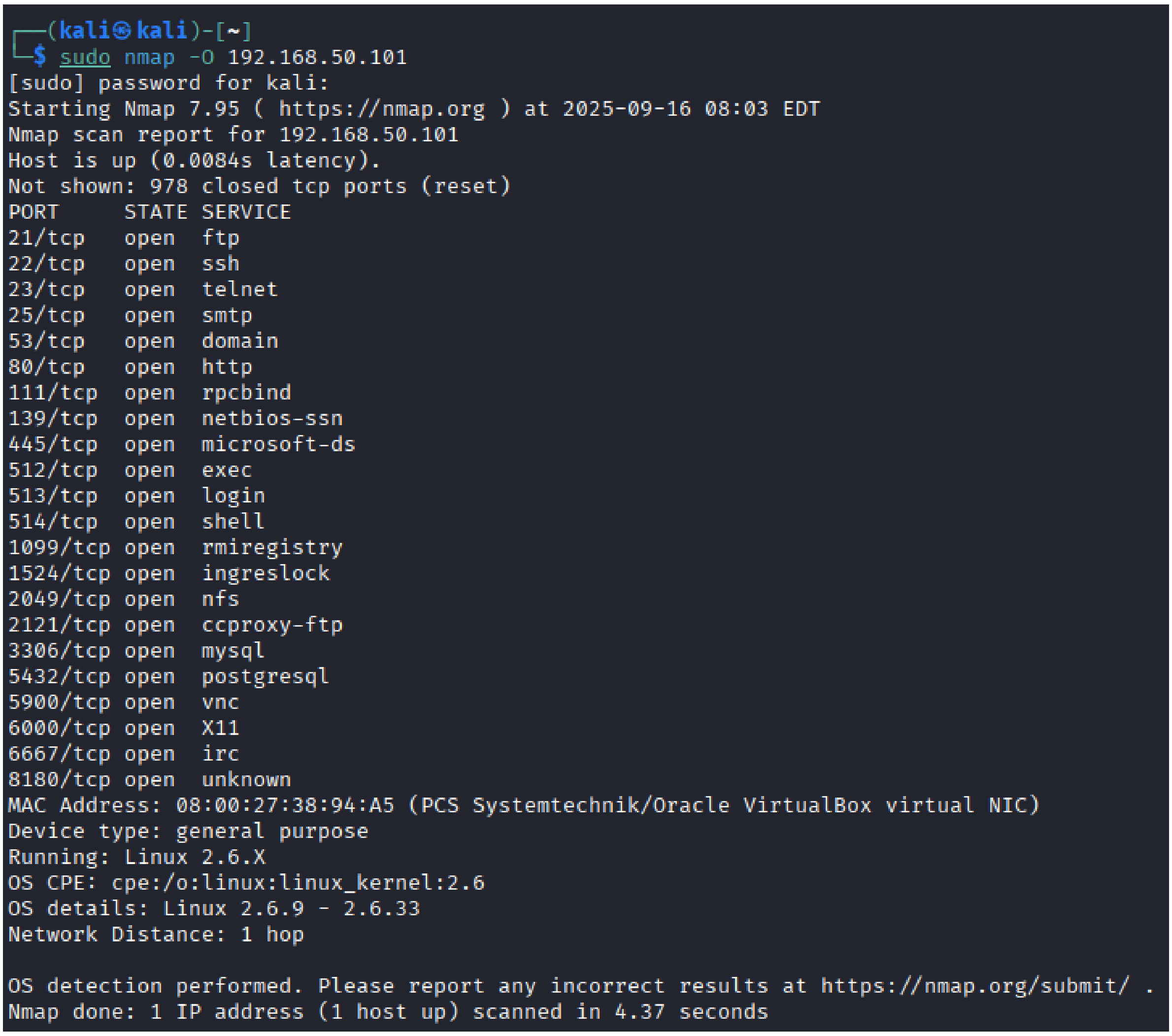
```
┌──(kali㉿kali)-[~]
└─$ ping -c 5 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=2.43 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=2.32 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=1.31 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=7.59 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=1.61 ms

--- 192.168.50.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.314/3.050/7.589/2.307 ms
```

- Il ping conferma che il target è raggiungibile attraverso Kali

7 Scan Results |Same Subnet|

7.1 OS Fingerprint

- Eseguo sudo nmap -O 192.168.50.101



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-16 08:03 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0084s 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
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
8180/tcp open  unknown
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/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 4.37 seconds
```

- **IP** 192.168.50.101

- **Operating System** Linux 2.6.9 - 2.6.33

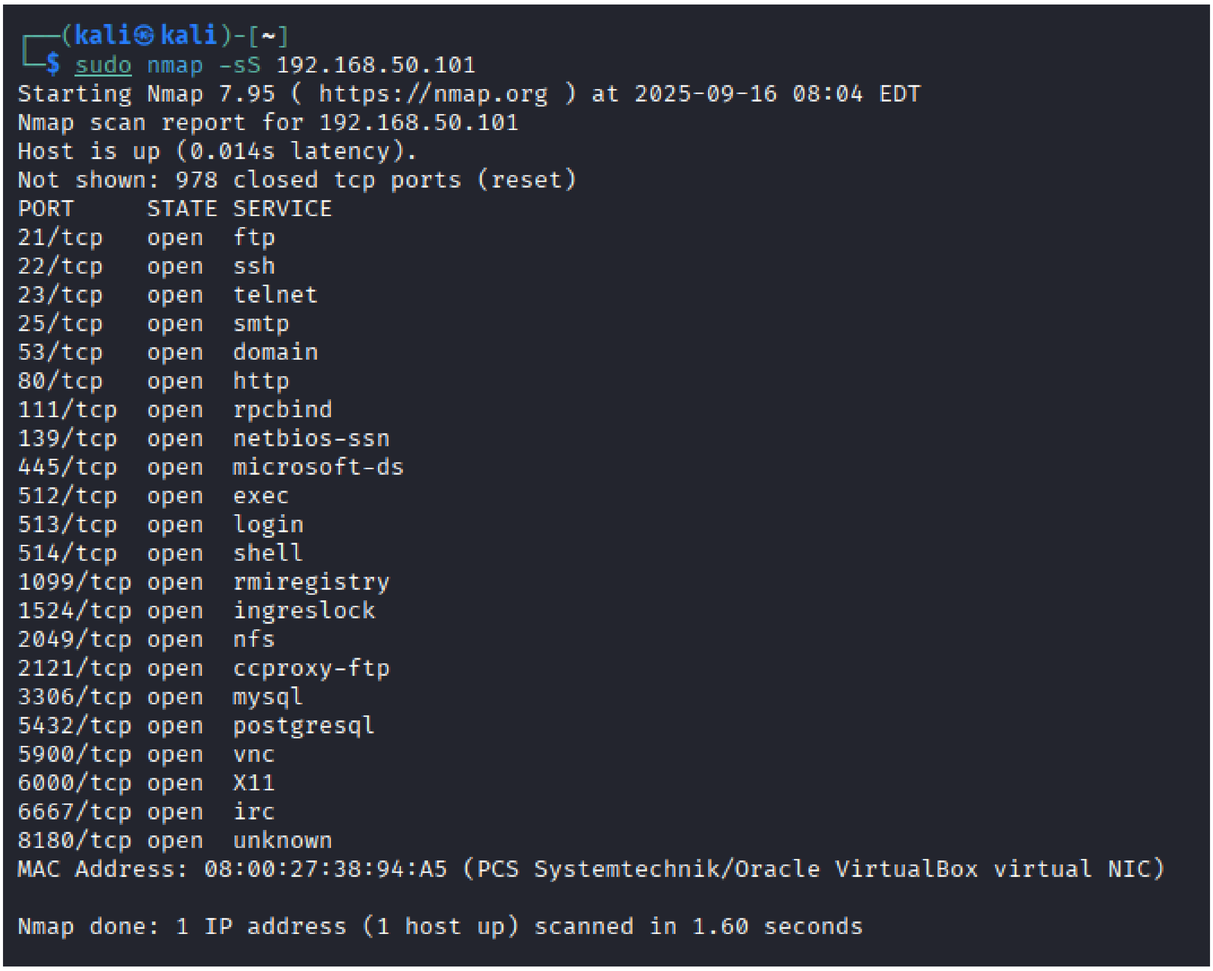
- **Open Doors** 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8180 (TCP)

- **Times** 4.37 secondi

- **Details** Network Distance: 1 hop [rispetto a 2 hop configurazione precedente]

7.2 SYN Scan

- Eseguo sudo nmap -sS 192.168.50.101



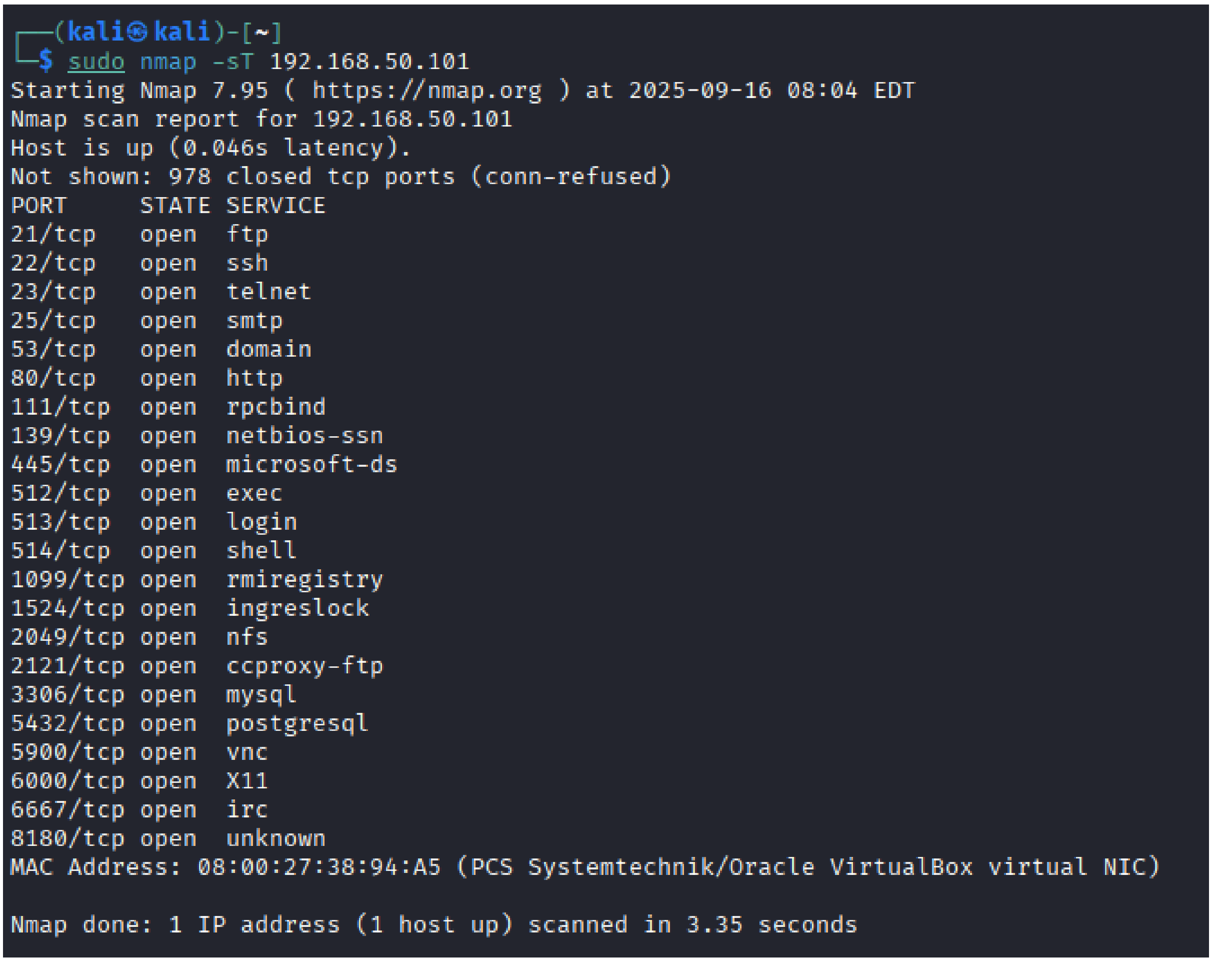
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-16 08:04 EDT
Nmap scan report for 192.168.50.101
Host is up (0.014s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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
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
8180/tcp open  unknown
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

- **Open Doors** 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8180 (TCP)

- **Times** 1.60 secondi

7.3 TCP Connect Scan

- Eseguo sudo nmap -sT 192.168.50.101



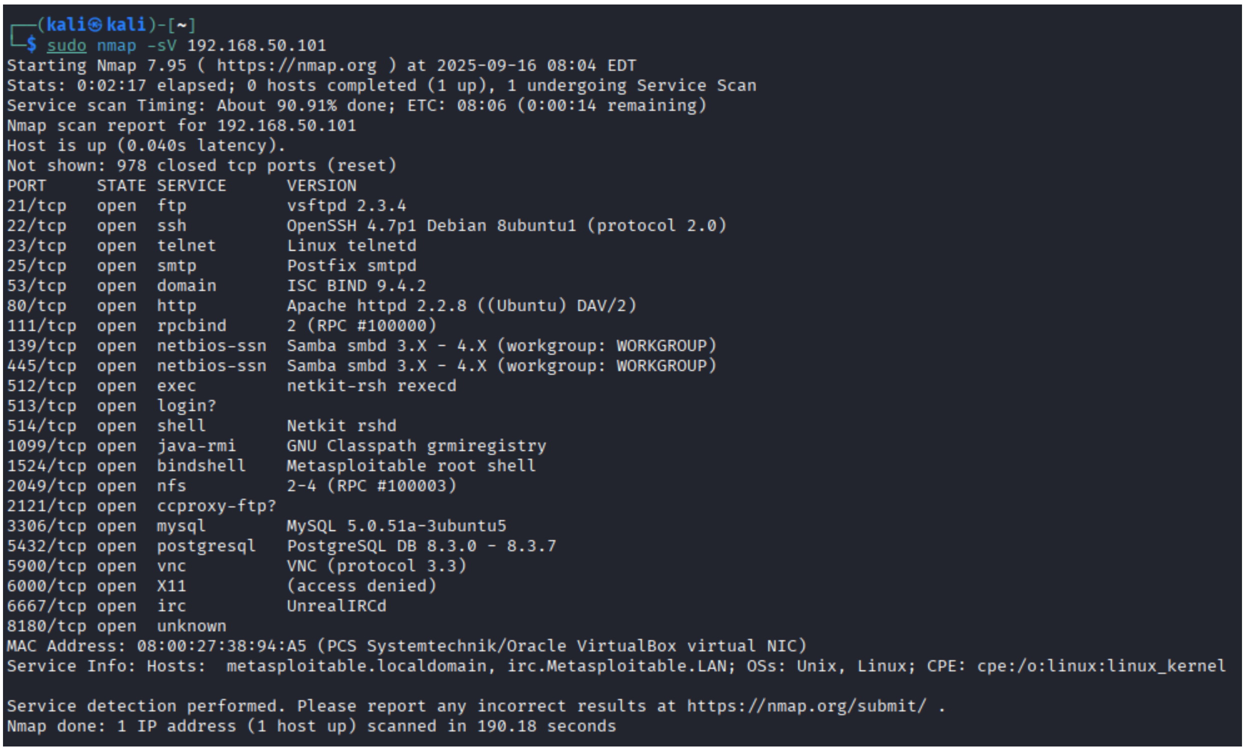
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-16 08:04 EDT
Nmap scan report for 192.168.50.101
Host is up (0.046s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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
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
8180/tcp open  unknown
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.35 seconds
```

- **Open Doors** Identiche a SYN scan

- **Times** 3.35 secondi

7.4 Version Detection

- Eseguo sudo nmap -sV 192.168.50.101



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-16 08:04 EDT
Stats: 0:02:17 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 90.91% done; ETC: 08:06 (0:00:14 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.040s 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  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  ccproxy-ftp?
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
8180/tcp open  unknown
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/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 190.18 seconds
```

- **Open Doors and Services**:

- 21/tcp: vsftpd 2.3.4
- 22/tcp: OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
- 23/tcp: Linux telnetd
- 25/tcp: Postfix smtpd
- 53/tcp: ISC BIND 9.4.2
- 80/tcp: Apache httpd 2.2.8 ((Ubuntu) DAV/2)
- 111/tcp: rpcbind 2 (RPC #100000)
- 139/tcp: Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
- 445/tcp: Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
- 512/tcp: netkit-rsh rexecd
- 513/tcp: login
- 514/tcp: Netkit rshd
- 1099/tcp: GNU Classpath grmiregistry
- 1524/tcp: Metasploitable root shell
- 2049/tcp: nfs 2-4 (RPC #100003)
- 2121/tcp: ccproxy-ftp
- 3306/tcp: MySQL 5.0.51a-3ubuntu5
- 5432/tcp: PostgreSQL DB 8.3.0 - 8.3.7
- 5900/tcp: VNC (protocol 3.3)
- 6000/tcp: X11 (access denied)
- 6667/tcp: UnrealIRCd
- 8180/tcp: unknown

- **Times** 190.18 secondi
- **Info additional Hostnames**:
  - metasploitable.localdomain
  - irc.Metasploitable.LAN
  - OS: Unix/Linux

8 Differences from the Previous Configuration

- **Network Configuration** Nella configurazione precedente, Kali [192.168.50.100]e Metasploitable2 [192.168.51.101]erano su subnet diverse, con pfSense [vtnet1: 192.168.50.1, vtnet2: 192.168.51.1] come router intermedio. Ora entrambe le macchine sono sulla stessa subnet [192.168.50.0/24] eliminando il routing tramite pfSense.

- **Speed**:

  - **Ping**: Latenza media ridotta da 11.884 ms a 3.050 ms grazie alla comunicazione diretta nella stessa subnet.

  - **OS Fingerprint**: Tempo simile [4.37s vs 4.02s] ma latenza inferiore [0.0084s vs 0.044s] e distanza di rete ridotta [1 hop vs 2 hop].

  - **SYN Scan**: Tempo aumentato da 0.85s a 1.60s, potenzialmente dovuto a variazioni nell'ambiente VirtualBox [tipo carico CPU].

  - **TCP Connect Scan**: Tempo aumentato da 2.90s a 3.35s, stesso motivo.

  - **Version Detection**: Tempo leggermente ridotto da 191.98s a 190.18s.

- **Filtering**: Nessuna porta "filtered" in entrambe le configurazioni indicando che pfSense non applicava filtri significativi nella configurazione precedente.

- **Porte e Servizi**: Nessuna differenza nelle porte aperte [22 in totale] o nei servizi/versioni rilevati poiché il target [Metasploitable2] è invariato.

- **Rilevabilità**: La configurazione su stessa subnet è più stealth, poiché l'assenza di pfSense riduce la possibilità di rilevamento da parte di un IDS/IPS. Tuttavia è meno rappresentativa di scenari reali con reti segmentate.

- **Nota sull'OS**: La rilevazione del sistema operativo è leggermente diversa [2.6.9 - 2.6.33 vs 2.6.15 - 2.6.26] ma entrambe indicano un kernel Linux coerente con Metasploitable2 [Ubuntu-based].