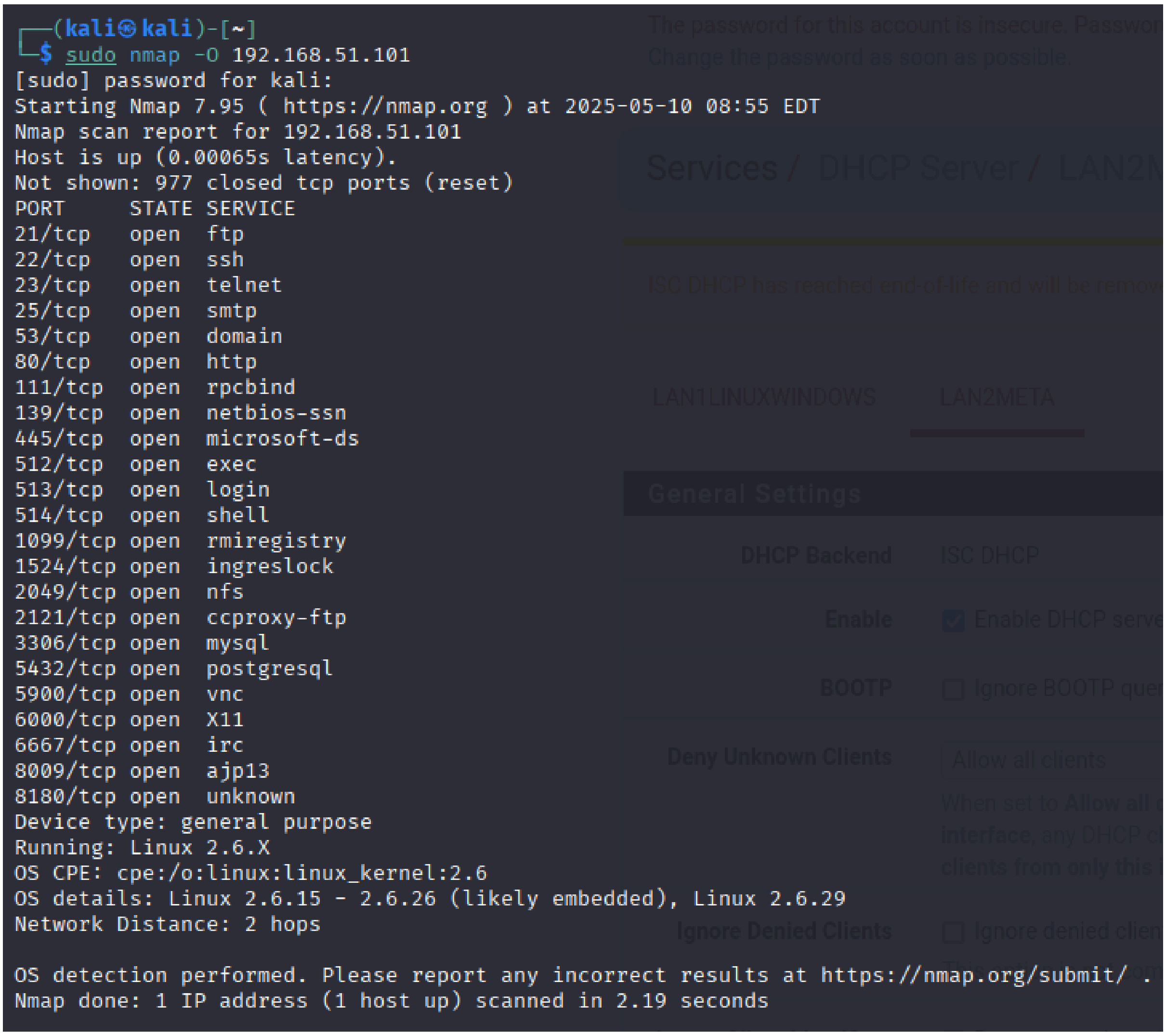
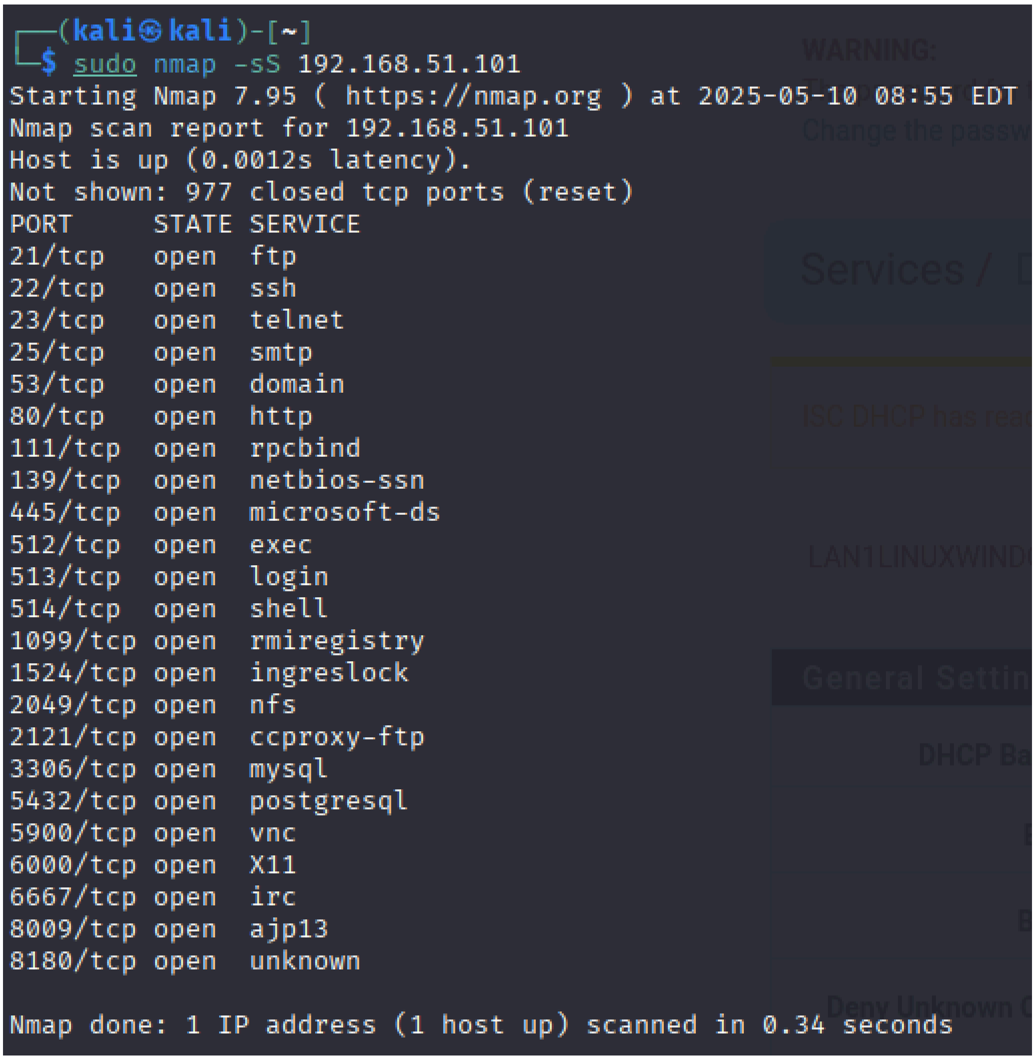


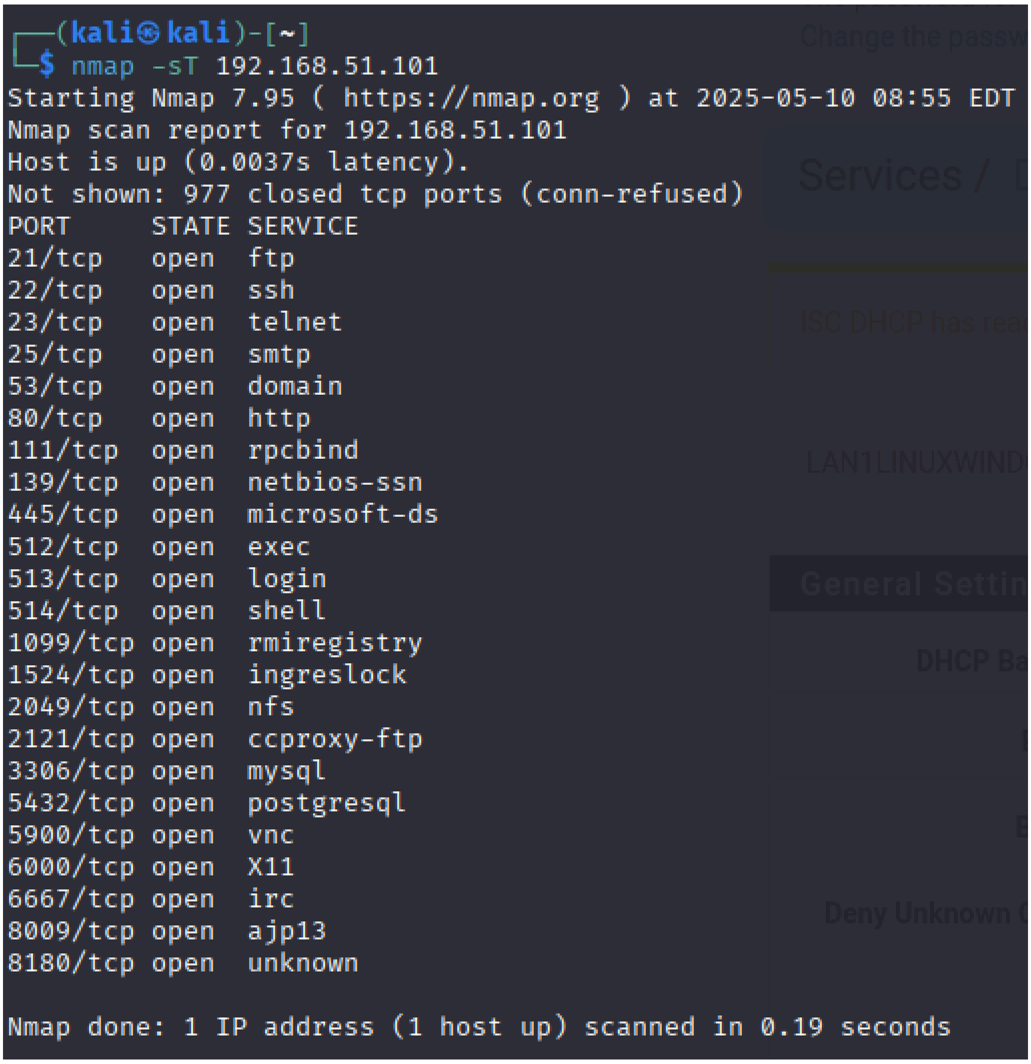
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.51.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 08:55 EDT
Nmap scan report for 192.168.51.101
Host is up (0.00065s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   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
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), Linux 2.6.29
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 2.19 seconds
```



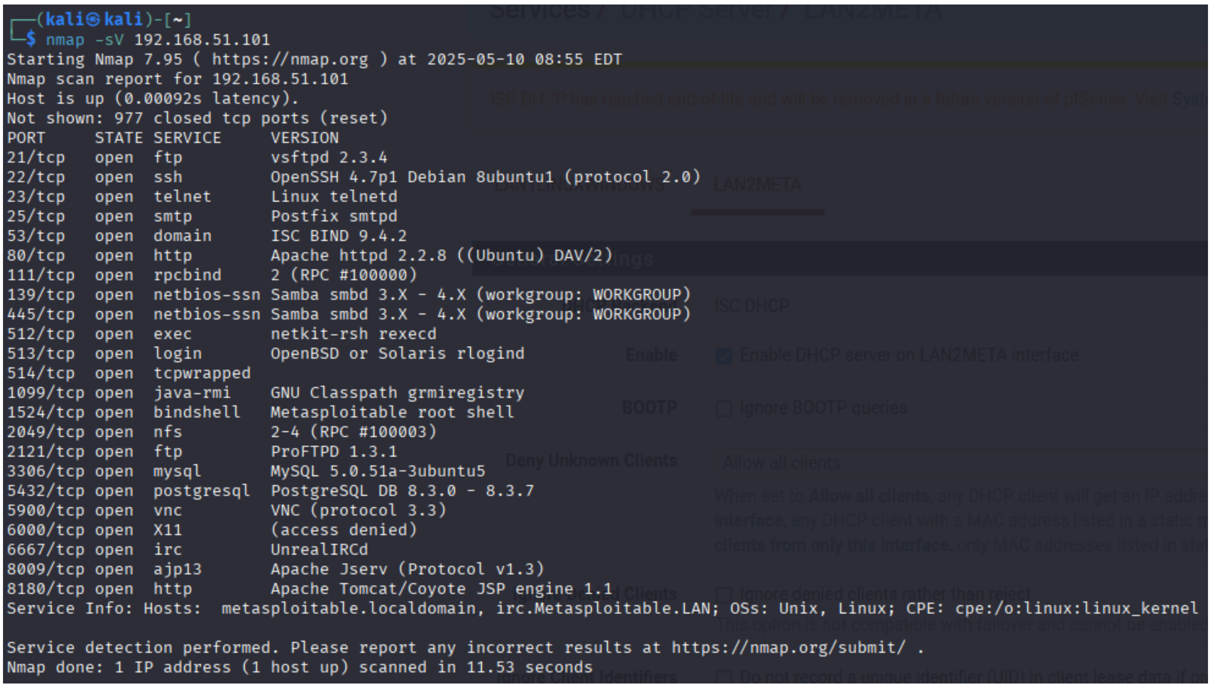
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 08:55 EDT
Nmap scan report for 192.168.51.101
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 08:55 EDT
Nmap scan report for 192.168.51.101
Host is up (0.0037s 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

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 08:55 EDT
Nmap scan report for 192.168.51.101
Host is up (0.00092s 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       OpenBSD or Solaris rlogind
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
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 11.53 seconds
```

Ho eseguito i comandi da kali a meta (192.168.50.100 kali - 192.168.51.101 meta) su reti diverse. -O , -sS , -sT , -sV .

IP Target:

- **IP:** 192.168.51.101

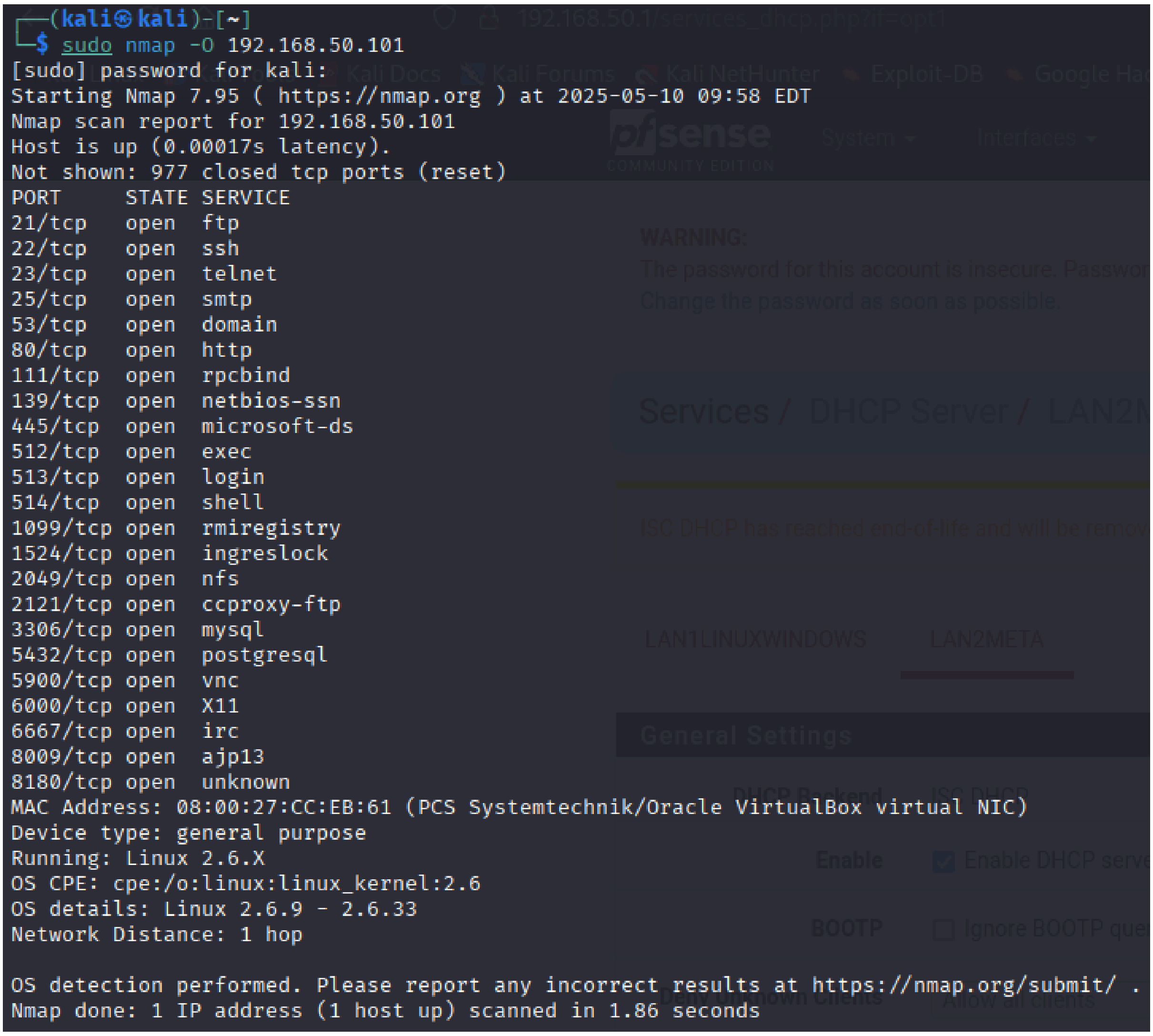
Sistema Operativo:

- **Sistema Operativo:** Linux 2.6.X (Versione probabile: Linux 2.6.15 - 2.6.26 o Linux 2.6.29)

Porte Aperte	Servizi in ascolto con versione	Descrizione dei servizi
21	FTP - vsftpd 2.3.4	Server FTP sicuro (vsftpd 2.3.4), vulnerabile a exploit noti.
22	SSH - OpenSSH 4.7p1 Debian 8ubuntu1	Servizio di comunicazione sicura (OpenSSH 4.7p1).
23	Telnet - Linux telnetd	Protocollo di login remoto non sicuro (Linux telnetd).
25	SMTP - Postfix smtpd	Servizio di invio posta (Postfix smtpd).
53	DNS - ISC BIND 9.4.2	Servizio DNS (ISC BIND 9.4.2).
80	HTTP - Apache httpd 2.2.8	Server web Apache (2.2.8), supporta WebDAV.
111	rpcbind - 2 (RPC #100000)	Mappa porte per RPC, fondamentale per NFS e altri.
139	NetBIOS/SMB - Samba smbd 3.X - 4.X	Servizio file e stampanti via Samba (smbd 3.X - 4.X).
445	NetBIOS/SMB - Samba smbd 3.X - 4.X	Samba smbd per Windows/Linux file sharing.
512	Exec - netkit-rsh rexecd	Esecuzione comandi remota (netkit-rsh rexecd).
513	Login - OpenBSD o Solaris rlogind	Servizio di login remoto (rlogind).
514	Shell - tcpwrapped	Wrapper TCP per l'accesso remoto (tcpwrapped).
1099	Java RMI - GNU Classpath grmiregistry	Invocazione remota metodi Java (grmiregistry).
1524	BindShell - Metasploitable root shell	Shell remota di root (vulnerabilità di Metasploitable).
2049	NFS - 2-4 (RPC #100003)	Condivisione file remota via NFS (versioni 2-4).
2121	FTP - ProFTPD 1.3.1	Server FTP (ProFTPD 1.3.1), sicuro e configurabile.

3306	MySQL - MySQL 5.0.51a-3ubuntu5	Database MySQL (5.0.51a), utilizzato per applicazioni.
5432	PostgreSQL - PostgreSQL DB 8.3.0 - 8.3.7	DBMS PostgreSQL (8.3.0 - 8.3.7), robusto e sicuro.
5900	VNC - VNC (protocol 3.3)	Condivisione desktop remoto via VNC (protocollo 3.3).
6000	X11 - (Access denied)	Servizio grafico per UNIX (accesso negato).
6667	IRC - UnrealIRCd	Chat IRC (UnrealIRCd), per comunicazioni in tempo reale.
8009	AJP13 - Apache Jserv	Protocollo per comunicazione Apache-Tomcat.
8180	HTTP - Apache Tomcat/Coyote JSP engine 1.1	Server HTTP Tomcat/Coyote JSP Engine (versione 1.1).

Ora proviamo a mettere kali e meta sulla stessa rete usando gli stessi comandi, notando delle differenze.



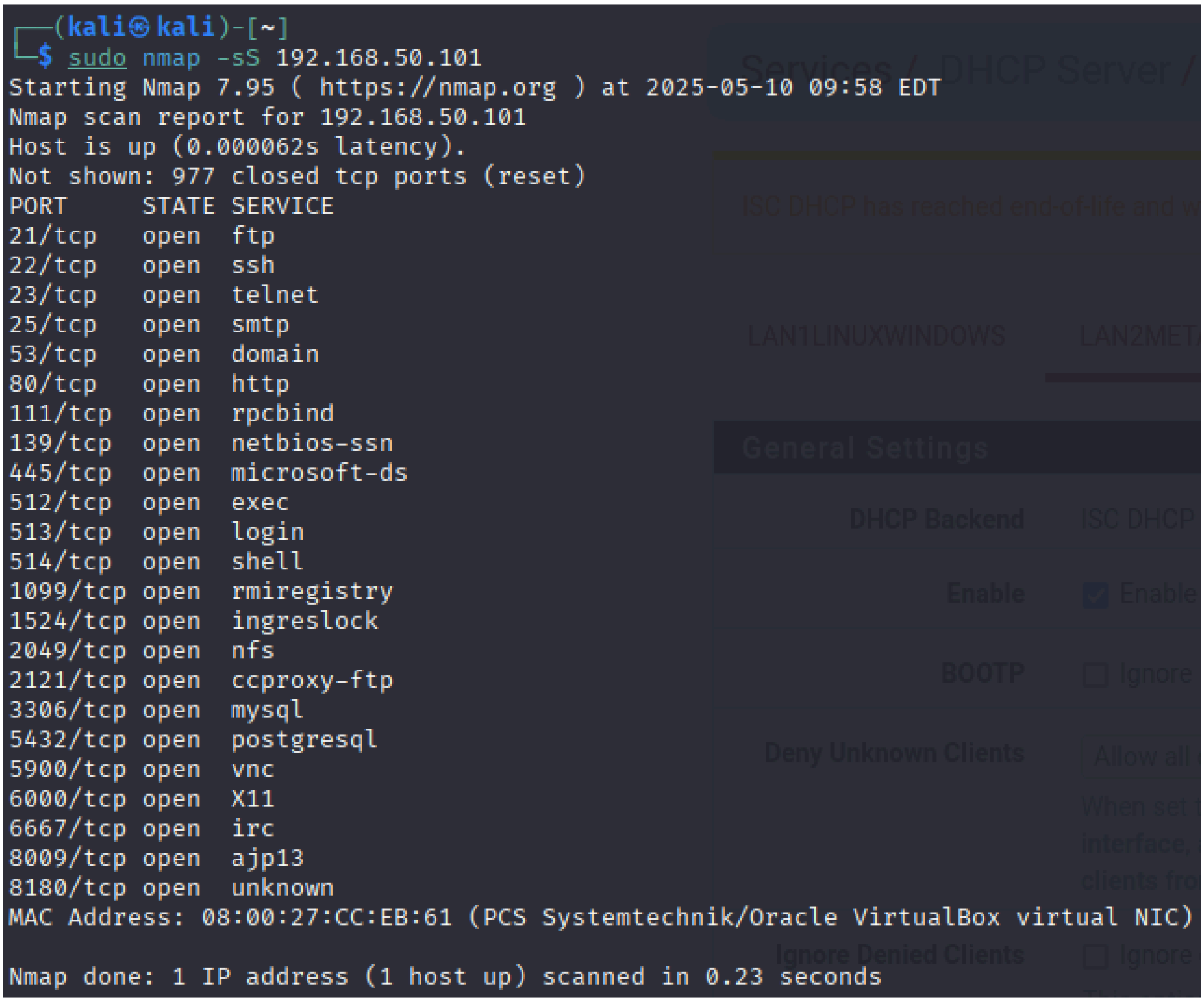
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 09:58 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   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:CC:EB:61 (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 1.86 seconds
```

impiega meno tempo a scannerizzare (quasi irrilevante)

dà il MAC Address

distanza tra network è 1 hop anziché 2



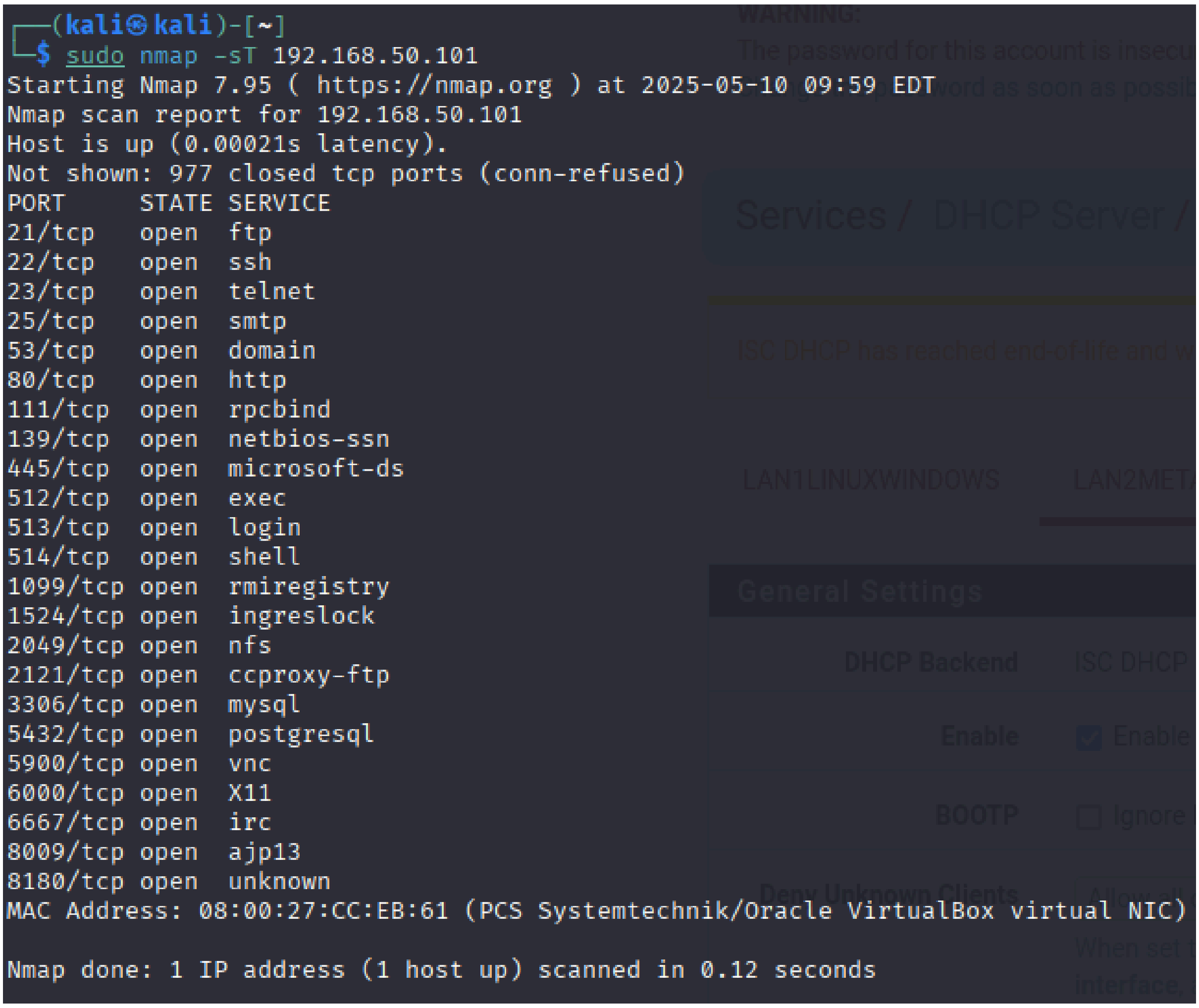
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 09:58 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000062s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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:CC:EB:61 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

nessuna differenza se non minore latenza

MAC Address

porte identiche

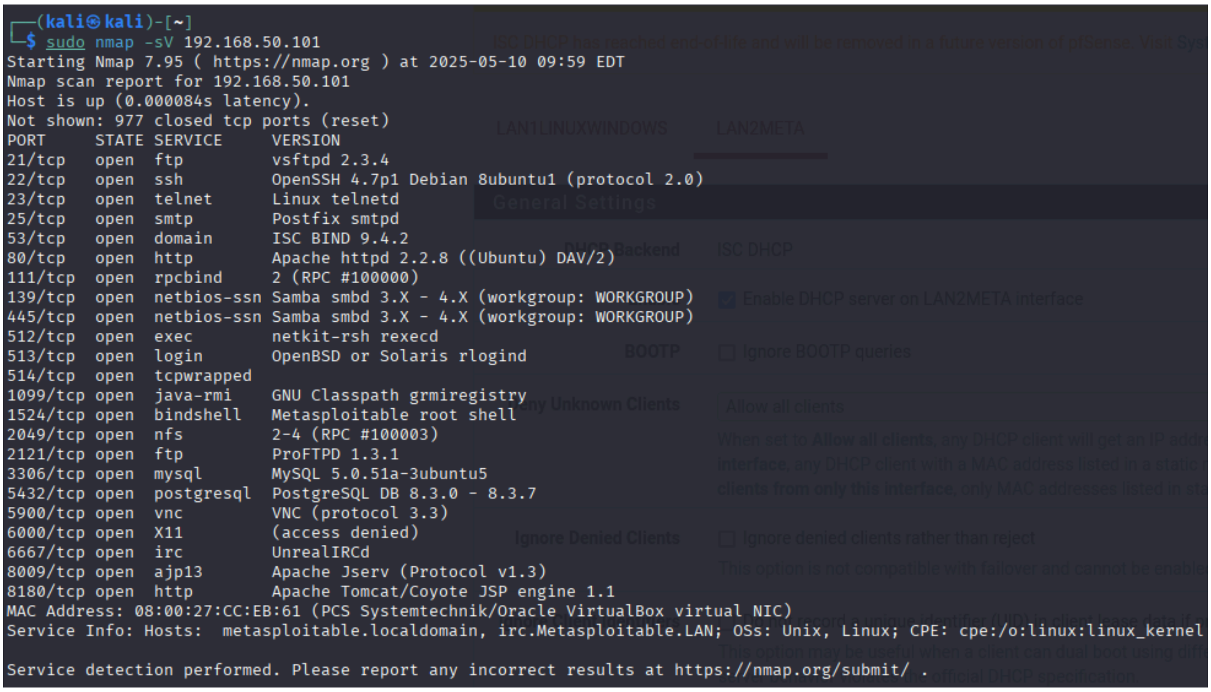


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 09:59 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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:CC:EB:61 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

nessuna differenza

MAC Address , minore latenza (minima)



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 09:59 EDT
Nmap scan report for 192.168.50.101
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       OpenBSD or Solaris rlogind
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
MAC Address: 08:00:27:CC:EB:61 (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/ .
```

nessuna differenza

MAC Address , latenza minima

Osservazioni:

- **Numero di hop** diverso: indica che nella scansione da reti diverse, il pacchetto ha attraversato più "nodi" (es. NAT).
- **Identificazione dei servizi** è rimasta **invariata**, segno che l'host target (Metasploitable) risponde allo stesso modo su entrambe le configurazioni.
- **Velocità di scansione** può leggermente variare (più veloce su stessa rete), ma in questo caso la differenza è minima.