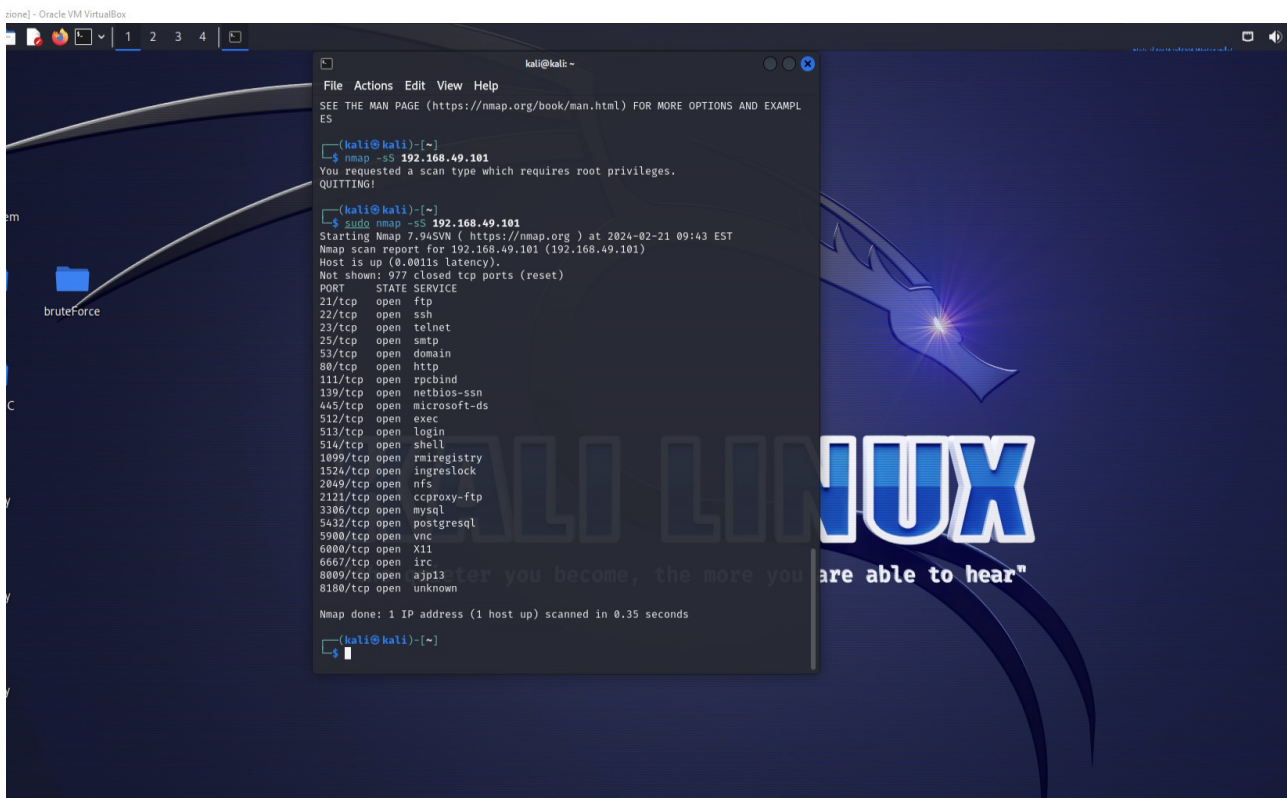


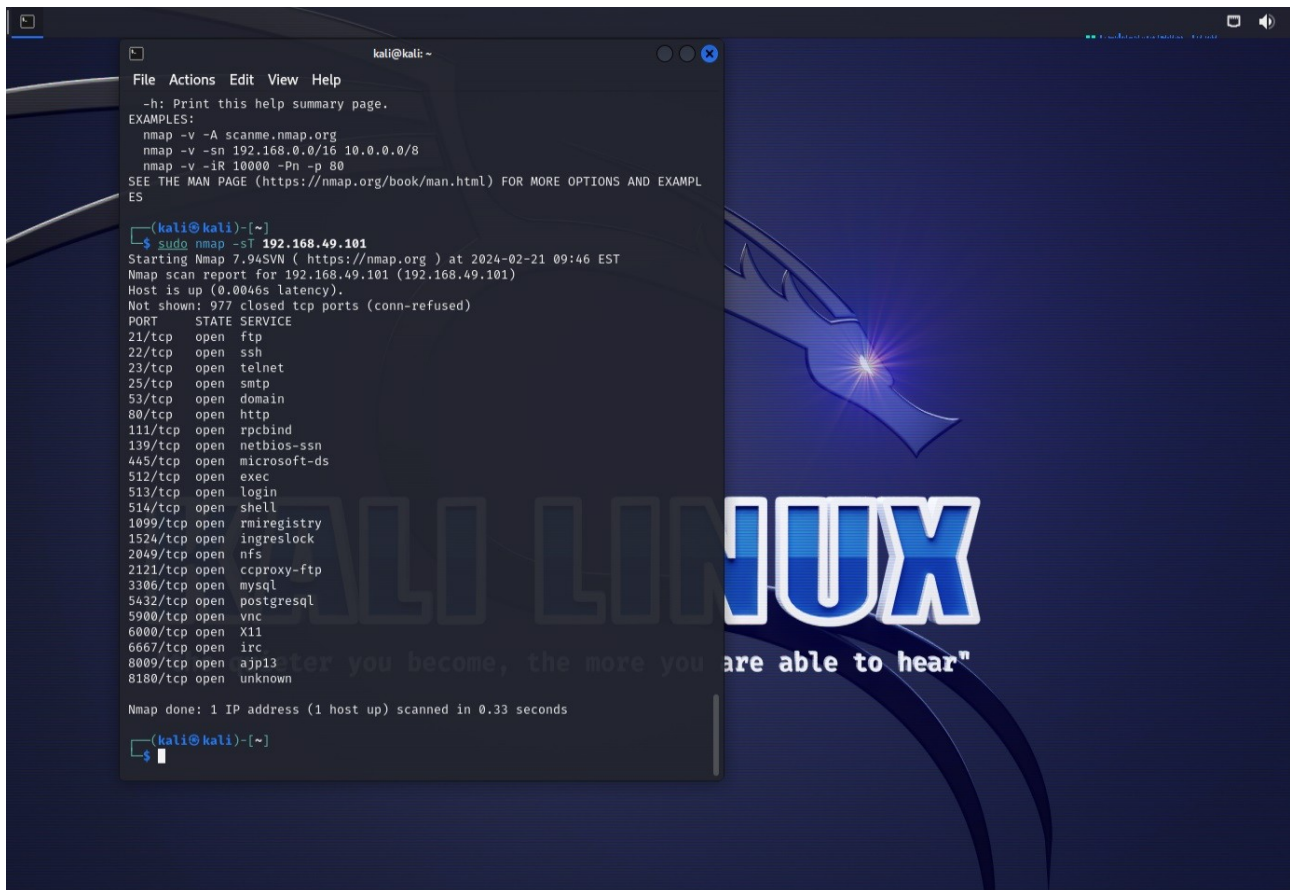
```
kali@kali: ~  
File Actions Edit View Help  
└─(kali@kali)-[~]  
└─$ sudo nmap -O 192.168.49.101  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:31 EST  
Nmap scan report for 192.168.49.101 (192.168.49.101)  
Host is up (0.0012s latency).  
Not shown: 977 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  cproxy-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)  
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 2.59 seconds  
└─(kali@kali)-[~]  
└─$
```

Alla scansione di finger print sono state rilevate alcune porte aperte con i rispettivi servizi, lo scopo del dispositivo i dettagli del sistema operativo e quanti salti ha fatto nella rete; non risulta possibile individuare l'esatto sistema operativo e quindi il programma fa una supposizione su un dato range di versioni



```
kali@kali: ~  
File Actions Edit View Help  
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES  
└─(kali@kali)-[~]  
└─$ nmap -sS 192.168.49.101  
You requested a scan type which requires root privileges.  
QUITTING!  
└─(kali@kali)-[~]  
└─$ sudo nmap -sS 192.168.49.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:43 EST  
Nmap scan report for 192.168.49.101 (192.168.49.101)  
Host is up (0.0011s 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  cproxy-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 0.35 seconds  
└─(kali@kali)-[~]  
└─$
```

alla scansione sS viene fatto solo il primo passaggio della 3 way handshake e quindi il syn;



nella scansione sT, quindi con il 3 way handshake completo, si riportano gli stessi identici risultati della scansione sS; e' logico dedurre che, a parita' di risultati, conviene utilizzare il comando sS in quanto non completa la connessione e quindi risultiamo meno rilevabili e impattiamo meno sulla rete

```
kali@kali: ~  
File Actions Edit View Help  
nmap -v -iR 10000 -Pn -p 80  
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES  
  
(kali@kali)-[~]  
$ sudo nmap -sV 192.168.49.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:52 EST  
Nmap scan report for 192.168.49.101 (192.168.49.101)  
Host is up (0.0032s 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?          
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 66.29 seconds  
  
(kali@kali)-[~]  
$
```

con sV riusciamo a vedere in piu le versioni dei vari servizi aperti sulle porte

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -O 192.168.49.102  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:12 EST  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.61 seconds  
  
(kali@kali)-[~]  
$ sudo nmap -O -Pn 192.168.49.102  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:12 EST  
Nmap scan report for 192.168.49.102 (192.168.49.102)  
Host is up.  
All 1000 scanned ports on 192.168.49.102 (192.168.49.102) are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
Too many fingerprints match this host to give specific OS details  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 221.11 seconds  
  
(kali@kali)-[~]  
$
```

per quanto riguarda l'os fingerprint su windows, all'inizio ho usato il comando semplice e risulta che il protocollo icmp viene impedito dal firewall e quindi ho messo l'opzione pn che esclude quel protocollo; nonostante tutto non e' stato possibile avere info

un metodo utilizzabile potrebbe essere il timing, ridurre i tempi di comunicazione con la porta in modo tale che il firewall non rilevi un tentativo di connessione