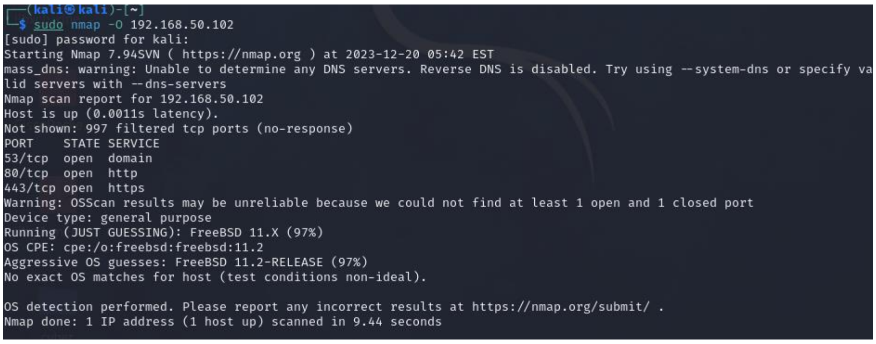
TECNICHE DI SCANSIONE CON NMAP

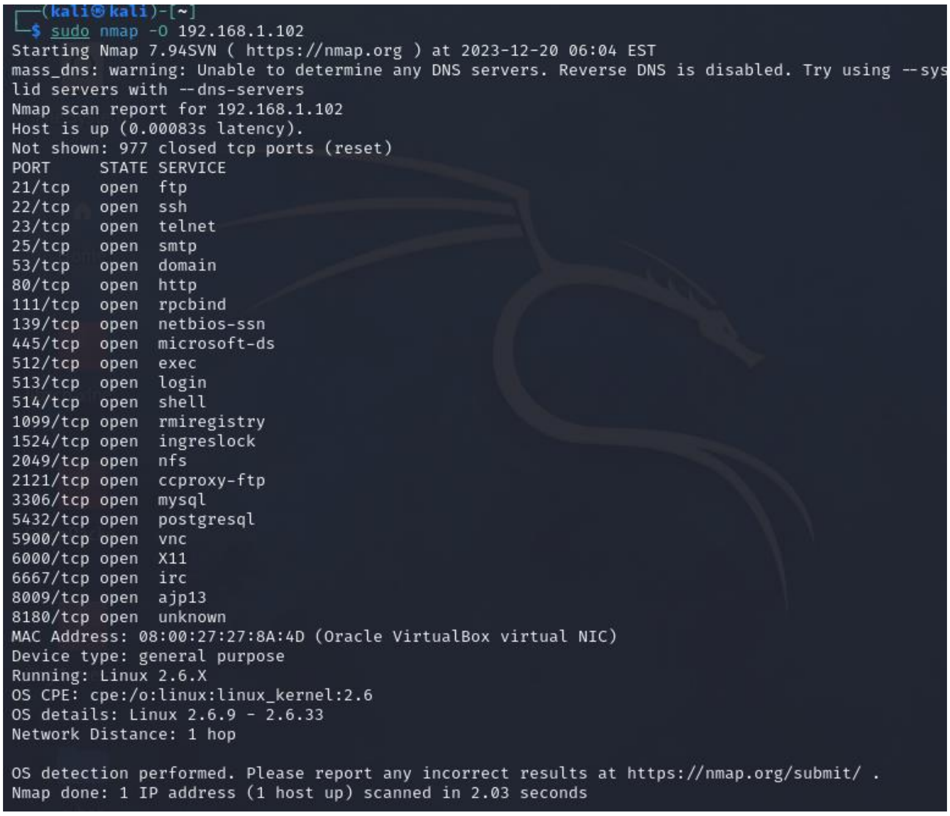
<u>Scansione su Meta</u>

OS fingerprint



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 05:42 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify va
lid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.0011s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (97%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.44 seconds
```

rete esterna

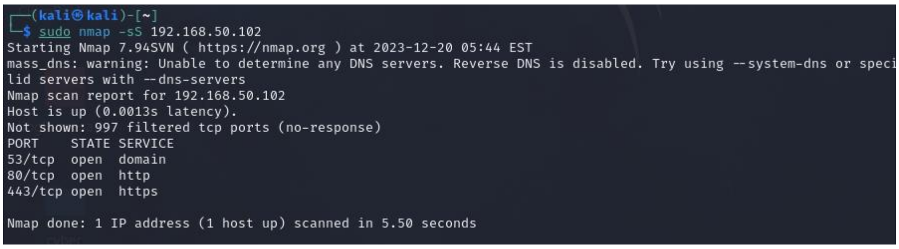


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 06:04 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --sys
lid servers with --dns-servers
Nmap scan report for 192.168.1.102
Host is up (0.00083s 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: 08:00:27:27:8A:4D (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 2.03 seconds
```

rete interna

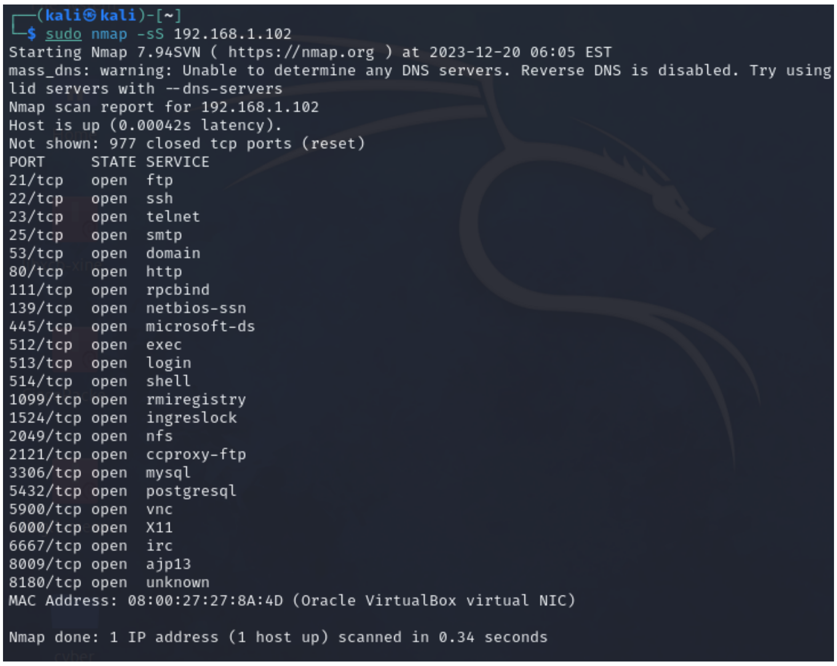
Inviando il comando “nmap -0 indirizzo_ip” possiamo ottenere informazioni sul sistema operativo della macchina target. Nel caso in cui il target è su una rete diversa da quella interna otterremo una risposta non completa, in quanto il firewall di Meta bloccherà la trasmissione dei pacchetti, non permettendo una completa raccolta dei dati; diverso nel caso in cui il target sia su una rete interna. Infatti, eseguendo il comando con il target nella rete interna, possiamo notare come la raccolta delle porte aperte sia più numerosa e le informazioni riguardati il sistema operativo più dettagliate.

Syn Scan



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 05:44 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or speci
lid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.0013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.50 seconds
```

rete esterna

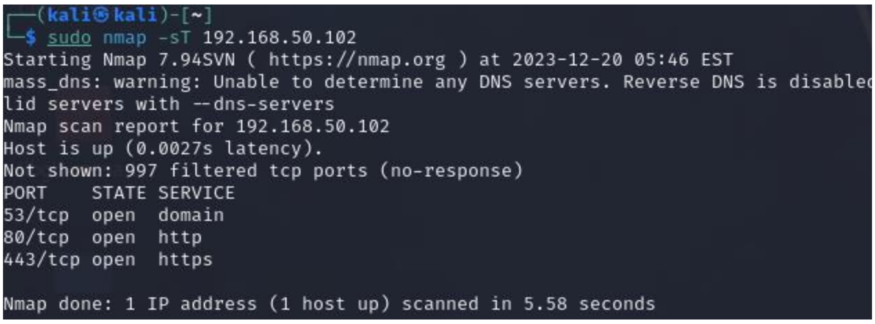


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 06:05 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
lid servers with --dns-servers
Nmap scan report for 192.168.1.102
Host is up (0.00042s latency).
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: 08:00:27:27:8A:4D (Oracle VirtualBox virtual NIC)

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

rete interna

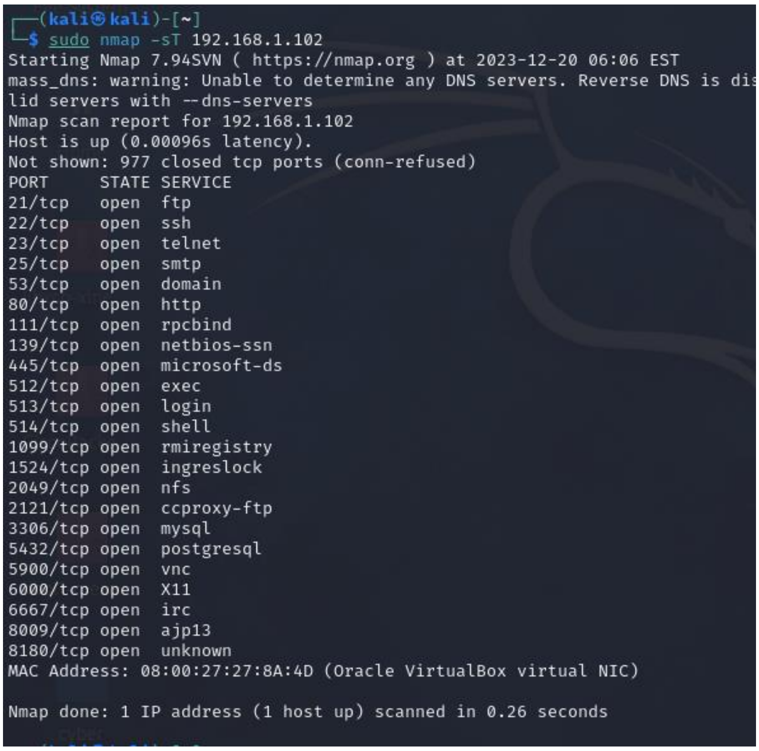
Con il comando “nmap -sS indirizzo_ip”, possiamo effettuare uno stealth scan, così da non essere rilevati dagli IDS/IPS. La differenza tra rete interna e rete esterna rimane sempre quella di una raccolta di dati minori. Bisogna notare che rispetto ad uno scan più completo con pacchetti SYN/ACK, nel caso di scansione Syn, otterremo come risposta un pacchetto reset.

TCP connect



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 05:46 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disablec
lid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.0027s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.58 seconds
```

rete esterna

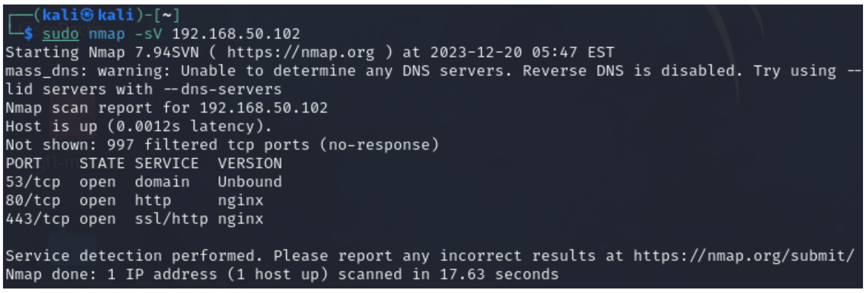


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 06:06 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is dis
lid servers with --dns-servers
Nmap scan report for 192.168.1.102
Host is up (0.00096s latency).
Not shown: 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: 08:00:27:27:8A:4D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

rete interna

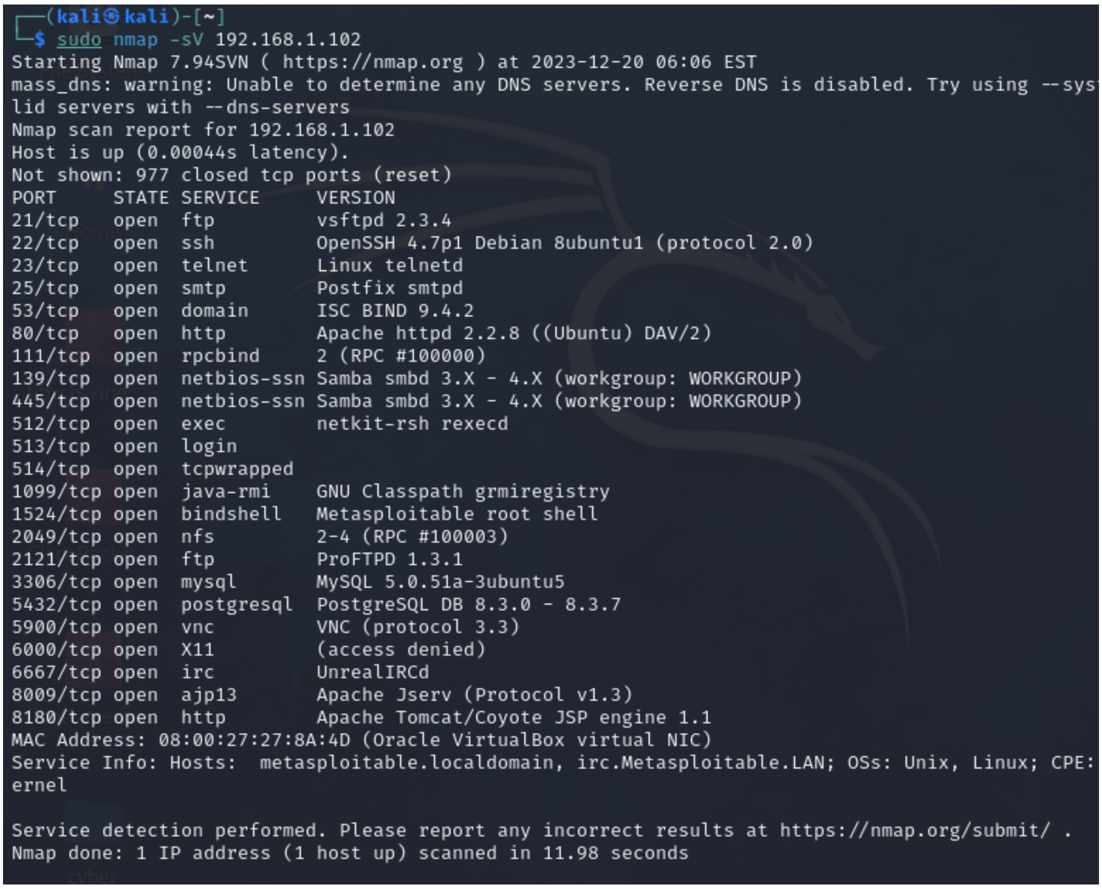
Utilizzando il comando "nmap -sT indirizzo_ip" possiamo effettuare una scansione completa seguendo il protocollo TCP, trovando tutte le porte aperte. La differenza tra i due target rimane sempre quella delle policy del firewall di Meta, che non permette una scansione completa delle porte, bloccando la trasmissione dei pacchetti.

Version detection



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 05:47 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
lid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.0012s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
53/tcp  open  domain   Unbound
80/tcp  open  http     nginx
443/tcp open  ssl/http nginx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 17.63 seconds
```

rete esterna



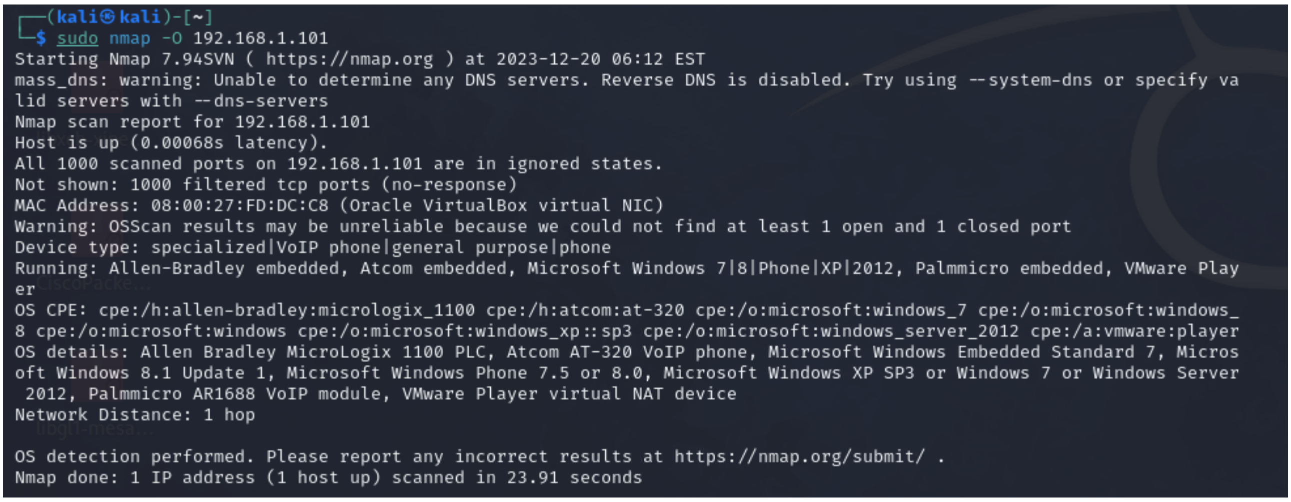
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 06:06 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --sys
lid servers with --dns-servers
Nmap scan report for 192.168.1.102
Host is up (0.00044s 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  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: 08:00:27:27:8A:4D (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
ernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.98 seconds
```

rete interna

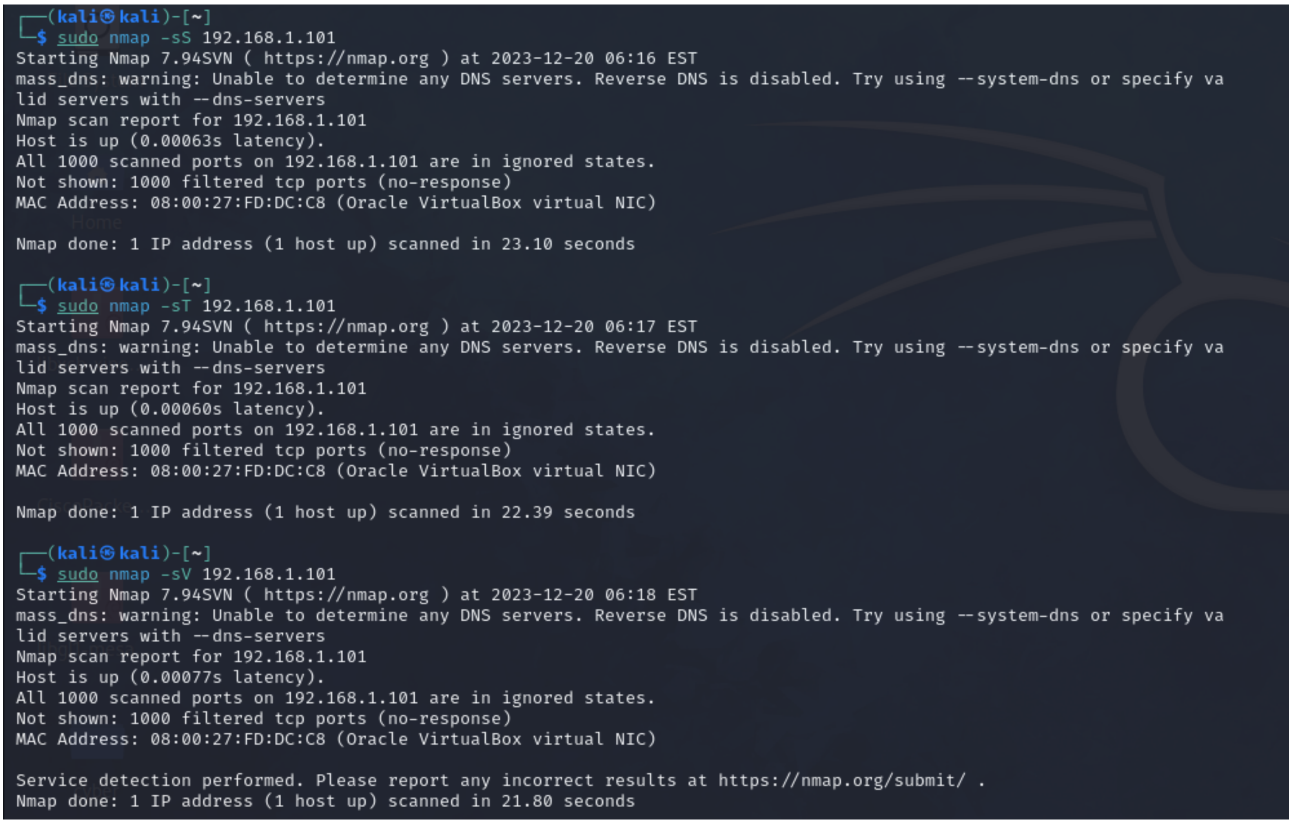
Con il comando “nmap -sV indirizzo_ip” possiamo effettuare una scansione, oltre che dei servizi abilitati, anche della versione e relativi dettagli. La differenza tra effettuare un tipo di scansione del genere su un target interno o esterno rimane la medesima, nel caso di target interno riusciamo a catturare sempre più informazioni, mentre nel caso di rete esterna meno.

Scansione su Windows 7

OS fingerprint



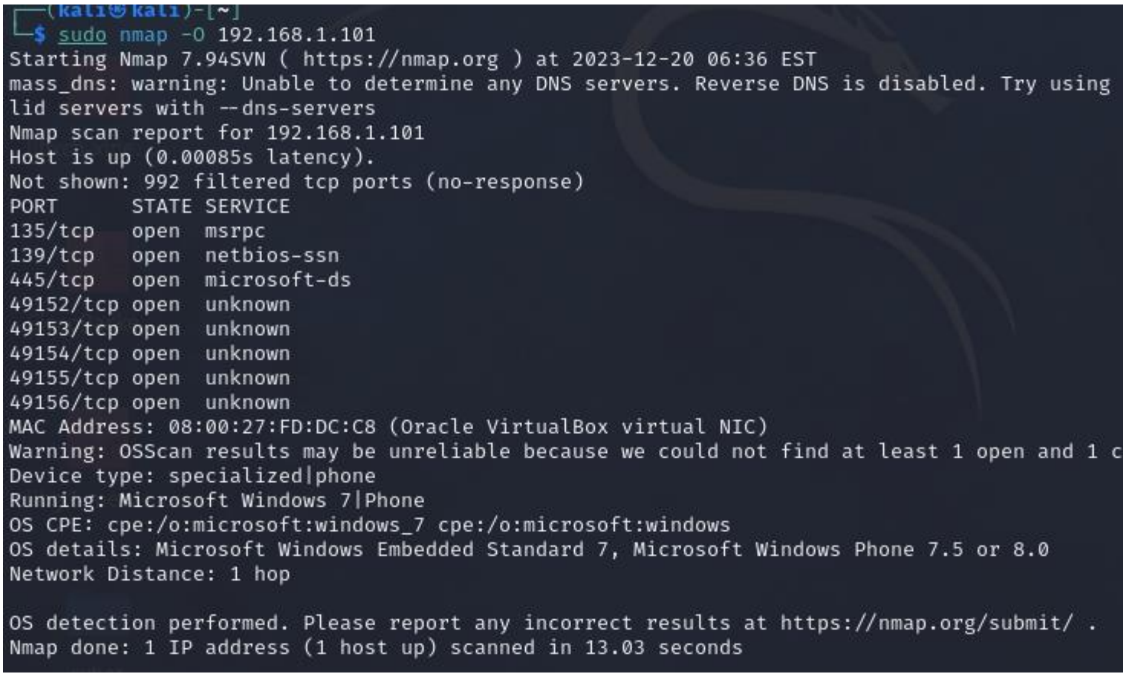
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 06:12 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify va
lid servers with --dns-servers
Nmap scan report for 192.168.1.101
Host is up (0.00068s latency).
All 1000 scanned ports on 192.168.1.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:FD:DC:C8 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Play
er
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_
8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Micros
oft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server
 2012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device
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 23.91 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 06:16 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify va
lid servers with --dns-servers
Nmap scan report for 192.168.1.101
Host is up (0.00063s latency).
All 1000 scanned ports on 192.168.1.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:FD:DC:C8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 23.10 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 06:17 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify va
lid servers with --dns-servers
Nmap scan report for 192.168.1.101
Host is up (0.00060s latency).
All 1000 scanned ports on 192.168.1.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:FD:DC:C8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 22.39 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 06:18 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify va
lid servers with --dns-servers
Nmap scan report for 192.168.1.101
Host is up (0.00077s latency).
All 1000 scanned ports on 192.168.1.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:FD:DC:C8 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.80 seconds
```

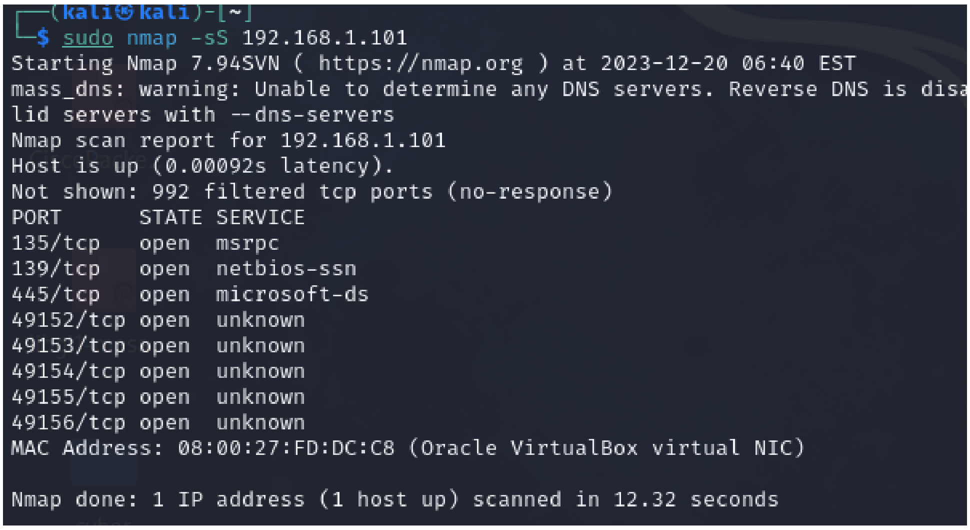
Replicando i comandi con Nmap su Windows 7 possiamo notare come il Firewall del sistema operativo non permette di raccogliere le informazioni richieste, se non indicazioni abbastanza generiche del sistema operativo del target.

Intervenendo quindi sul policy set del Firewall di Windows 7, aggiungendo due regole per permettere la comunicazione TCP-IP e UDP dall'IP di Kali (192.168.1.100), possiamo ottenere le informazioni che cercavamo.



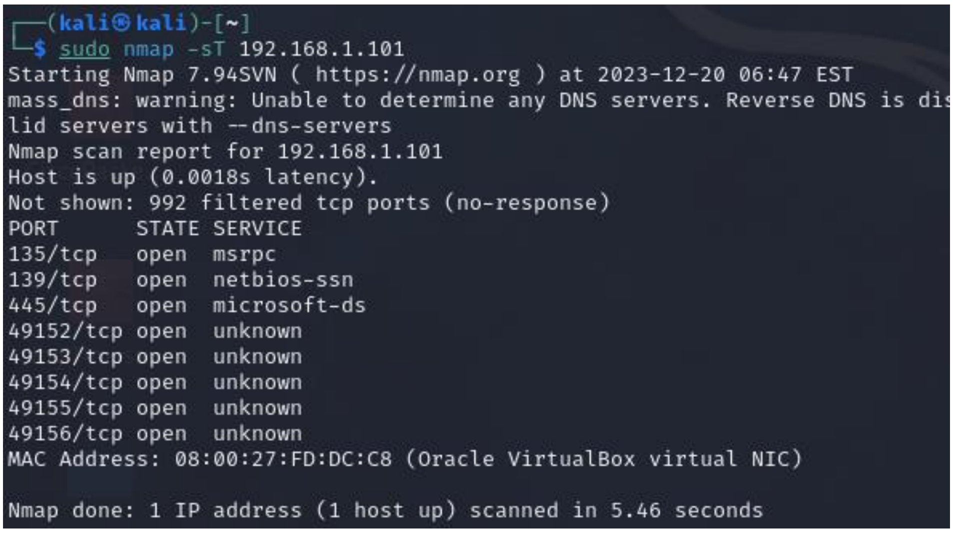
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 06:36 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
lid servers with --dns-servers
Nmap scan report for 192.168.1.101
Host is up (0.00085s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:FD:DC:C8 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 c
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
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 13.03 seconds
```

SO target



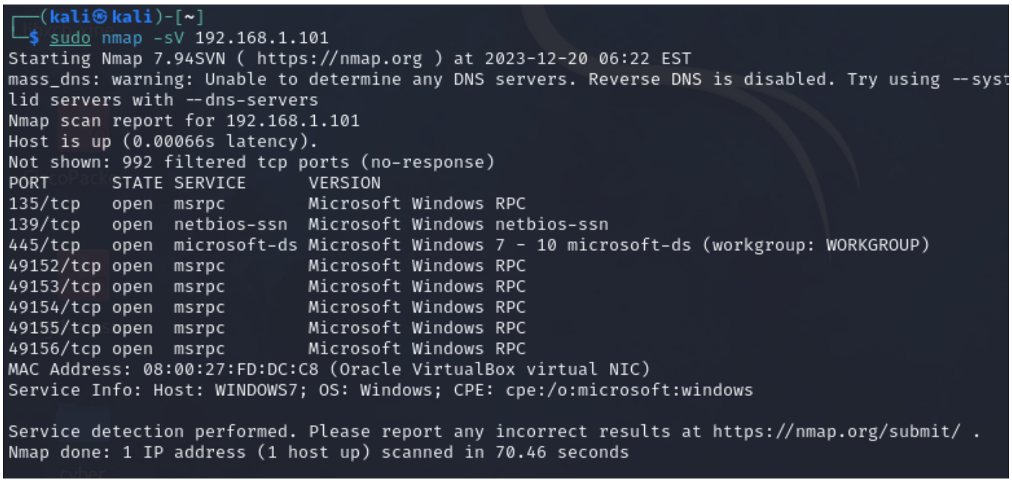
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 06:40 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disa
lid servers with --dns-servers
Nmap scan report for 192.168.1.101
Host is up (0.00092s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:FD:DC:C8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 12.32 seconds
```

SYN scan



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 06:47 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is dis
lid servers with --dns-servers
Nmap scan report for 192.168.1.101
Host is up (0.0018s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:FD:DC:C8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.46 seconds
```

TCP connect



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 06:22 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --syst
lid servers with --dns-servers
Nmap scan report for 192.168.1.101
Host is up (0.00066s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:FD:DC:C8 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 70.46 seconds
```

Version detection