TECNICHE DI SCANSIONE CON #NMAP

TECNICHE DI SCANSIONE CON NMAP - SCANSIONE DI UN HOST, SENZA E CON COMPLETAMENTO DEL 3-WAY HANDSHAKE

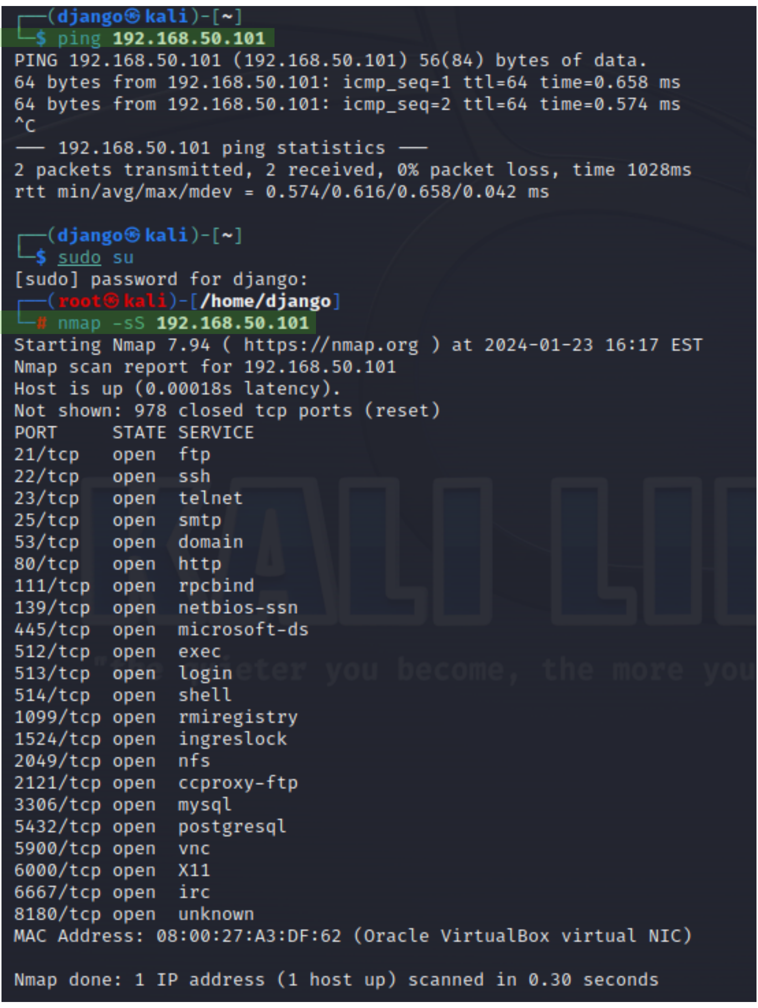
QUESTO ESERCIZIO PUÒ ESSERE UTILE PER LO STUDENTE PER PRENDERE DIMESTICHEZZA CON I VARI COMANDI DI NMAP. POICHÉ SU LINUX È UN POTENTE TOOL DI SCANSIONE DELLA RETE, SI RICHIEDE DI UTILIZZARE I SEGUENTI COMANDI E TRASCRIVERE I VARI RISULTATI SU UN REPORT:

- **TCP: # nmap -sS ip address**
- **scansione completa: # nmap -sV ip address**
- **output su file: # nmap -sV -oN file.txt ip address**
- **scansione su porta: # nmap -sS -p 8080 ip address**
- **scansione tutte le porte: # nmap -sS -p ip address**
- **scansione UDP: # nmap -sU -r -v ip address**
- **scansione sistema operativo: # nmap -O ip address**
- **scansione versione servizi: # nmap -sV ip address**
- **scansione common 100 ports: # nmap -F ip address**
- **scansione tramite ARP: # nmap -PR ip address**
- **scansione tramite PING: # nmap -sP ip address**
- **scansione senza PING: # nmap -PN ip address**

INFINE, DISEGNARE 3-4 GRAFICI DELLE SCANSIONI EFFETTUATE, ESPLICITANDO LE VARIE FASI DI SYN, SYN/ACK ECC.

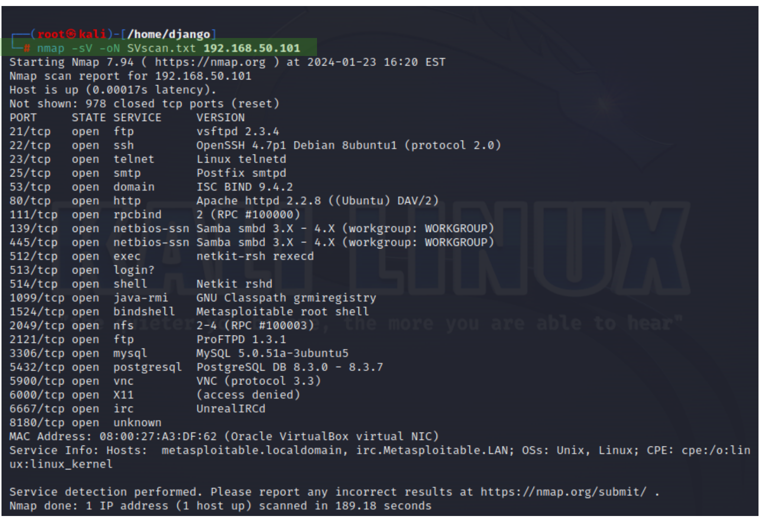
UTILIZZIAMO COME TARGET DELL'ESERCIZIO METASPLOITABLE CON L'IP 192.168.50.101, MENTRE QUELLO DI KALI LINUX RESTA 192.168.50.100

#PING + TCP SYN SCAN: nmap -sS 192.168.50.101



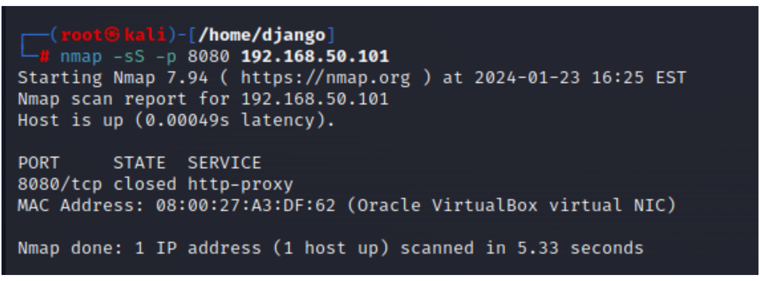
```
┌──(django㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.658 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.574 ms
^C
── 192.168.50.101 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1028ms
rtt min/avg/max/mdev = 0.574/0.616/0.658/0.042 ms

┌──(django㉿kali)-[~]
└─$ sudo su
[sudo] password for django:
┌──(root㉿kali)-[/home/django]
└─# nmap -sS 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 16:17 EST
Nmap scan report for 192.168.50.101
Host is up (0.00018s 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:A3:DF:62 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

#SCANSIONE COMPLETA (VERSIONE SERVIZI) CON OUTPUT SU FILE: nmap -sV -oN file.txt 192.168.50.101



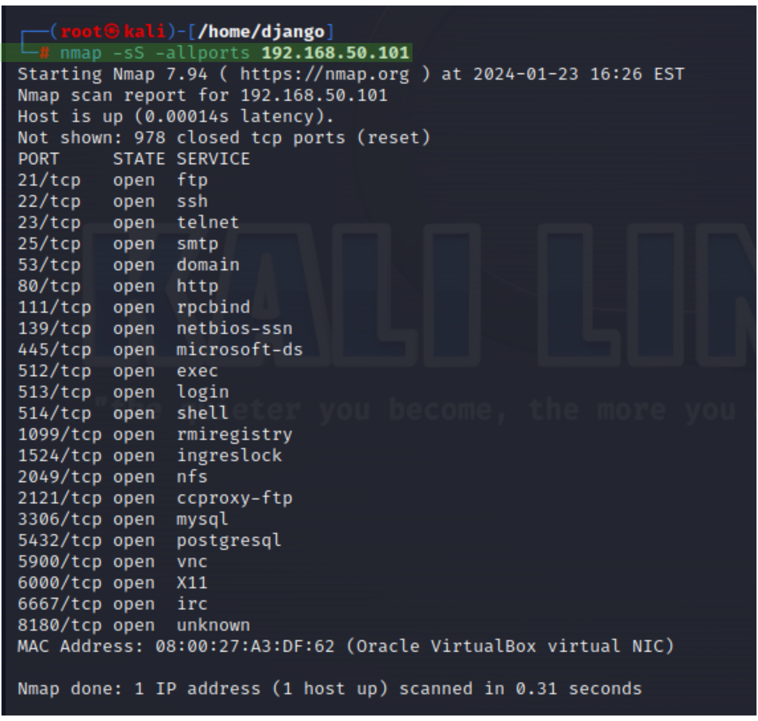
```
┌──(root㉿kali)-[/home/django]
└─# nmap -sV -oN SVscan.txt 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 16:20 EST
Nmap scan report for 192.168.50.101
Host is up (0.00017s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         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  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
8180/tcp open  unknown
MAC Address: 08:00:27:A3:DF:62 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:lin
ux: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 189.18 seconds
```

#SCANSIONE SU UNA PORTA SPECIFICA: nmap -sS -p 8080 192.168.50.101



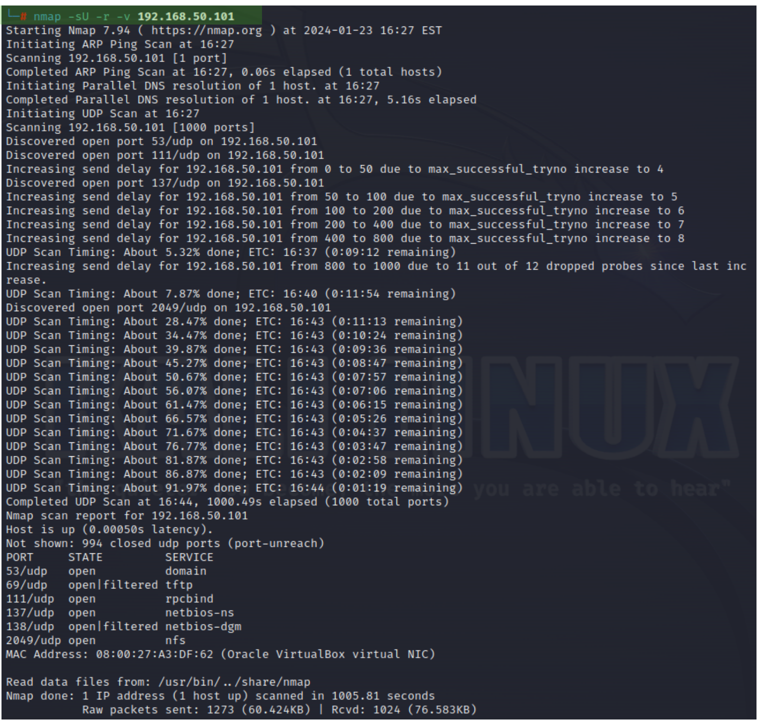
```
┌──(root㉿kali)-[/home/django]
└─# nmap -sS -p 8080 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 16:25 EST
Nmap scan report for 192.168.50.101
Host is up (0.00049s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:A3:DF:62 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.33 seconds
```

#SCANSIONE SU TUTTE LE PORTE: nmap -sS -allports 192.168.50.101



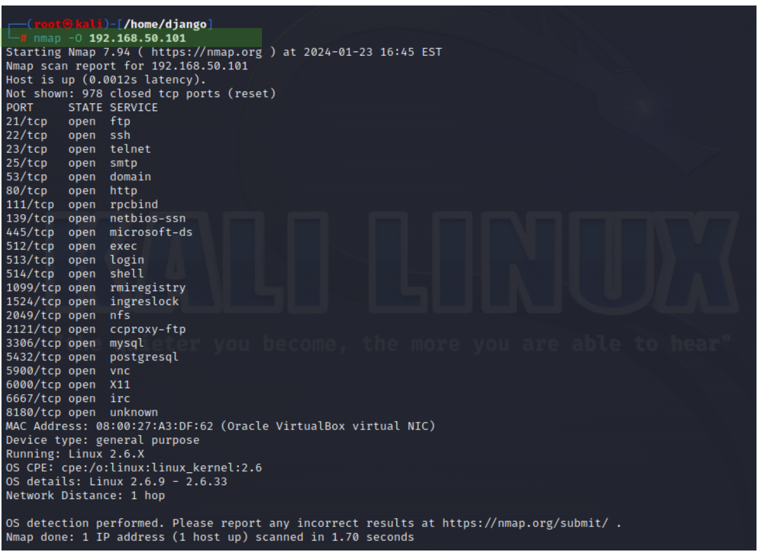
```
┌──(root㉿kali)-[/home/django]
└─# nmap -sS -allports 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 16:26 EST
Nmap scan report for 192.168.50.101
Host is up (0.00014s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
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:A3:DF:62 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

#SCANSIONE UDP (scansione porte in ordine sequenziale crescente e verbosità aumentata): nmap -sU -r -v 192.168.50.101



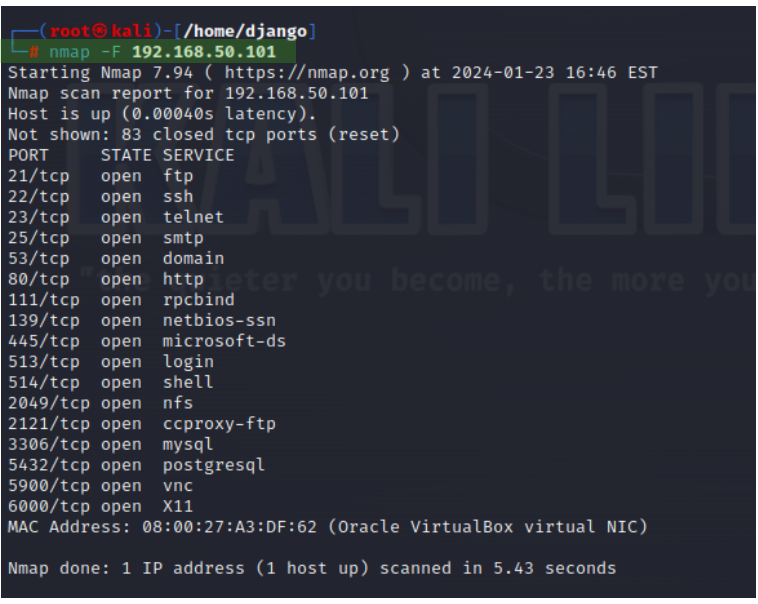
```
└─# nmap -sU -r -v 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 16:27 EST
Initiating ARP Ping Scan at 16:27
Scanning 192.168.50.101 [1 port]
Completed ARP Ping Scan at 16:27, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:27
Completed Parallel DNS resolution of 1 host. at 16:27, 5.16s elapsed
Initiating UDP Scan at 16:27
Scanning 192.168.50.101 [1000 ports]
Discovered open port 53/udp on 192.168.50.101
Discovered open port 111/udp on 192.168.50.101
Increasing send delay for 192.168.50.101 from 0 to 50 due to max_successful_tryno increase to 4
Discovered open port 137/udp on 192.168.50.101
Increasing send delay for 192.168.50.101 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.50.101 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.50.101 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.50.101 from 400 to 800 due to max_successful_tryno increase to 8
UDP Scan Timing: About 5.32% done; ETC: 16:37 (0:09:12 remaining)
Increasing send delay for 192.168.50.101 from 800 to 1000 due to 11 out of 12 dropped probes since last inc
rease.
UDP Scan Timing: About 7.87% done; ETC: 16:40 (0:11:54 remaining)
Discovered open port 2049/udp on 192.168.50.101
UDP Scan Timing: About 28.47% done; ETC: 16:43 (0:11:13 remaining)
UDP Scan Timing: About 34.47% done; ETC: 16:43 (0:10:24 remaining)
UDP Scan Timing: About 39.87% done; ETC: 16:43 (0:09:36 remaining)
UDP Scan Timing: About 45.27% done; ETC: 16:43 (0:08:47 remaining)
UDP Scan Timing: About 50.67% done; ETC: 16:43 (0:07:57 remaining)
UDP Scan Timing: About 56.07% done; ETC: 16:43 (0:07:06 remaining)
UDP Scan Timing: About 61.47% done; ETC: 16:43 (0:06:15 remaining)
UDP Scan Timing: About 66.57% done; ETC: 16:43 (0:05:26 remaining)
UDP Scan Timing: About 71.67% done; ETC: 16:43 (0:04:37 remaining)
UDP Scan Timing: About 76.77% done; ETC: 16:43 (0:03:47 remaining)
UDP Scan Timing: About 81.87% done; ETC: 16:43 (0:02:58 remaining)
UDP Scan Timing: About 86.87% done; ETC: 16:43 (0:02:09 remaining)
UDP Scan Timing: About 91.97% done; ETC: 16:44 (0:01:19 remaining)
Completed UDP Scan at 16:44, 1000.49s elapsed (1000 total ports)
Nmap scan report for 192.168.50.101
Host is up (0.00050s latency).
Not shown: 994 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs
MAC Address: 08:00:27:A3:DF:62 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1005.81 seconds
           Raw packets sent: 1273 (60.424KB) | Rcvd: 1024 (76.583KB)
```

#SCANSIONE SISTEMA OPERATIVO: nmap -O 192.168.50.101



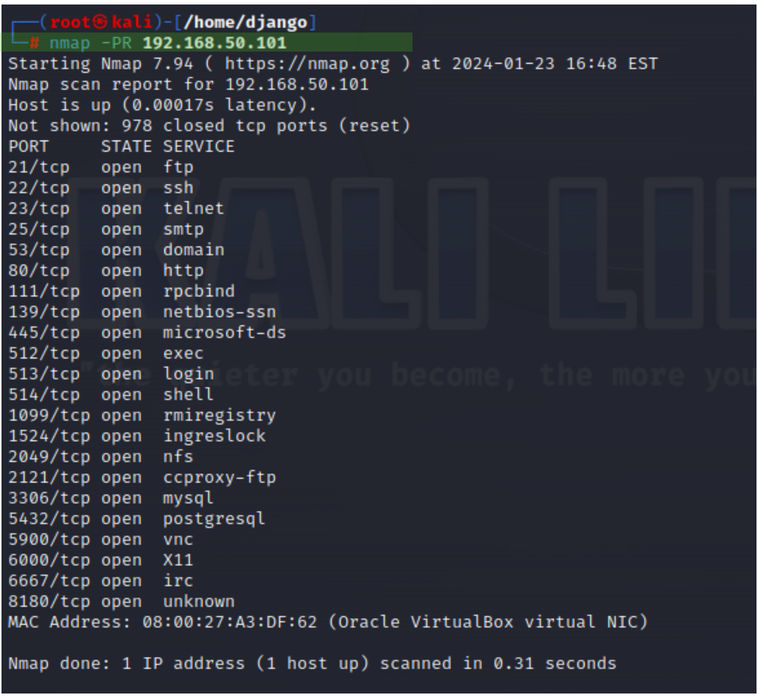
```
┌──(root㉿kali)-[/home/django]
└─# nmap -O 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 16:45 EST
Nmap scan report for 192.168.50.101
Host is up (0.0012s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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:A3:DF:62 (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 1.70 seconds
```

#SCANSIONE COMMON 100 PORTS: nmap -F 192.168.50.101



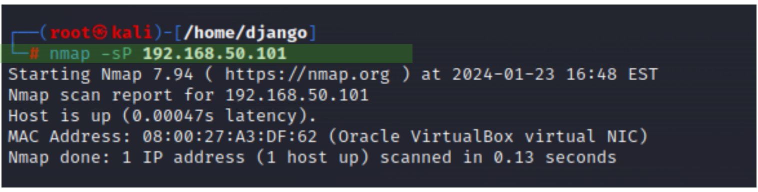
```
┌──(root㉿kali)-[/home/django]
└─# nmap -F 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 16:46 EST
Nmap scan report for 192.168.50.101
Host is up (0.00040s latency).
Not shown: 83 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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
513/tcp  open  login
514/tcp  open  shell
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
MAC Address: 08:00:27:A3:DF:62 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.43 seconds
```

#SCANSIONE TRAMITE ARP: nmap -PR 192.168.50.101



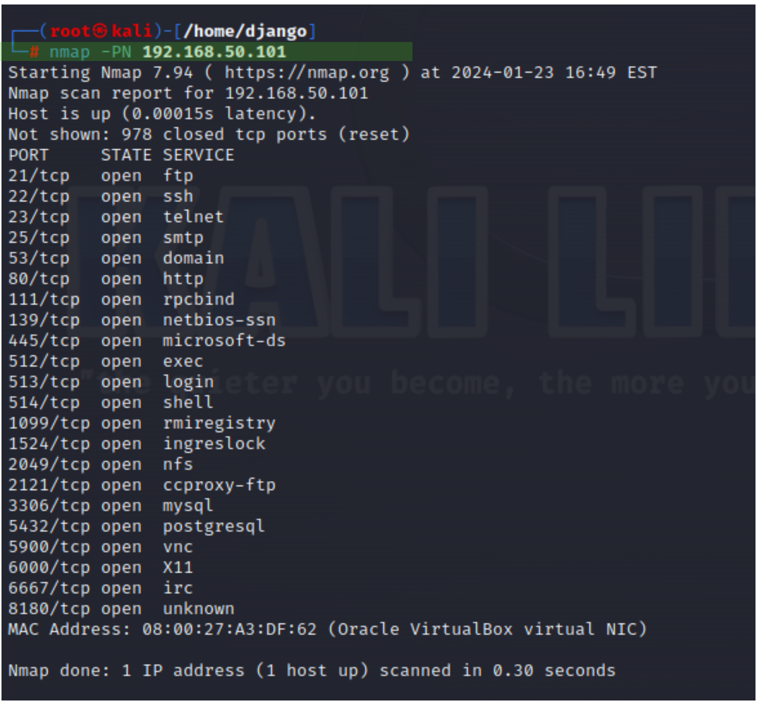
```
┌──(root㉿kali)-[/home/django]
└─# nmap -PR 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 16:48 EST
Nmap scan report for 192.168.50.101
Host is up (0.00017s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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:A3:DF:62 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

#SCANSIONE TRAMITE PING: nmap -sP 192.168.50.101



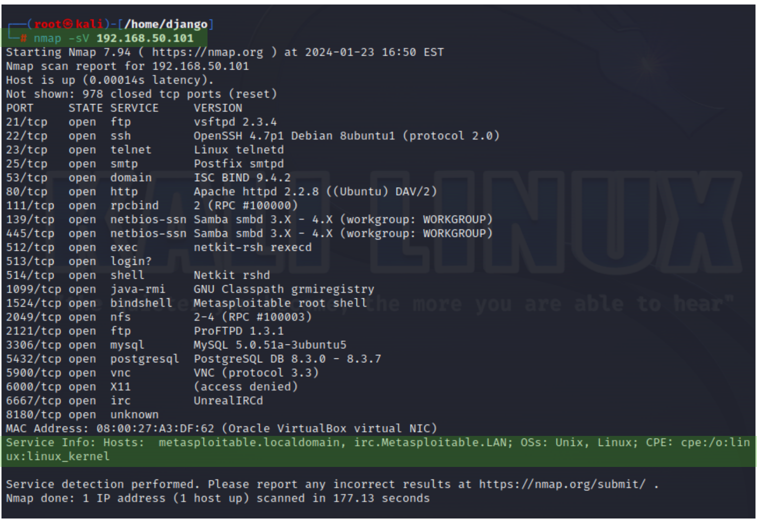
```
┌──(root㉿kali)-[/home/django]
└─# nmap -sP 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 16:48 EST
Nmap scan report for 192.168.50.101
Host is up (0.00047s latency).
MAC Address: 08:00:27:A3:DF:62 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

#SCANSIONE SENZA PING: nmap -PN 192.168.50.101



```
┌──(root㉿kali)-[/home/django]
└─# nmap -PN 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 16:49 EST
Nmap scan report for 192.168.50.101
Host is up (0.00015s 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:A3:DF:62 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

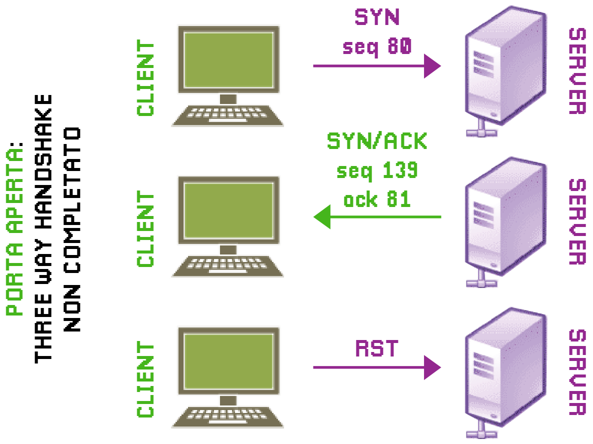
#SCANSIONE VERSIONE SERVIZI: nmap -sV 192.168.50.101

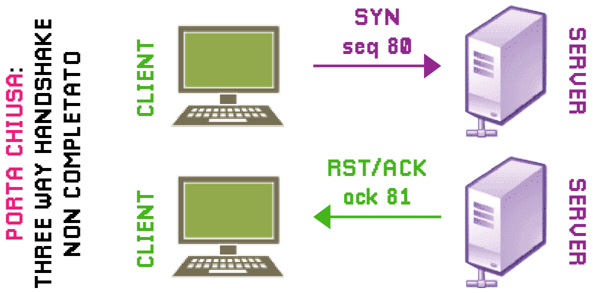


```
┌──(root㉿kali)-[/home/django]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 16:50 EST
Nmap scan report for 192.168.50.101
Host is up (0.00014s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 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  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
8180/tcp open  unknown
MAC Address: 08:00:27:A3:DF:62 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:lin
ux: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 177.13 seconds
```

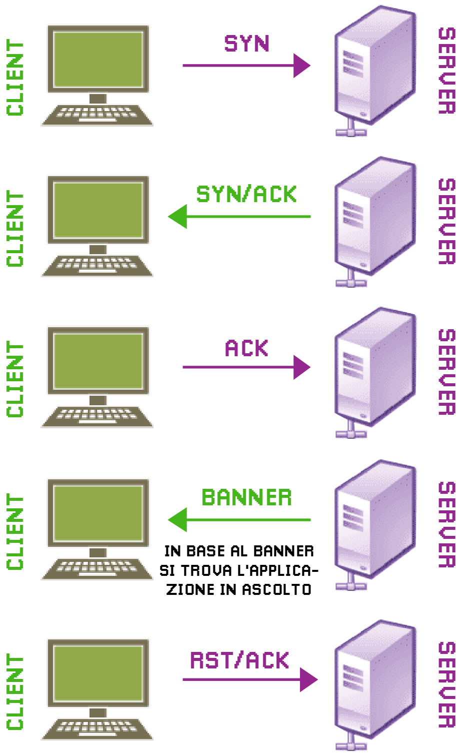
#GRAFICI DELLE SCANSIONI EFFETTUATE, ESPLICITANDO LE VARIE FASI DI SYN, SYN/ACK, ECC

#SCANSIONE DI TIPO SYN (STEALTH) SCAN: nmap -sS <IP>
NASCOSTO E POCO INVASIVO, POICHÉ NON COMPLETA MAI LE CONNESSIONI TCP (CASO DI PORTA APERTA / CHIUSA)

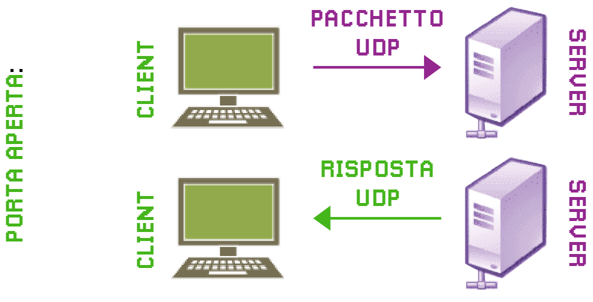




#SCANSIONE DI TIPO VERSIONE SERVIZI: nmap -sV <IP>
SCANSIONE DI TIPO TCP, ABILITA IL VERSION DETECTION COSÌ DA RICONOSCERE VERSIONE E NOME DEL SERVIZIO RPC. È RUMOROSA E GENERA MOLTO TRAFFICO DI RETE



#SCANSIONE DI TIPO UDP: nmap -sU <IP>
PIÙ LENTO E PIÙ DIFFICOLTOSO DI QUELLO SU TCP, FUNZIONA INVIANDO PACCHETTI UDP AD OGNI PORTA DI DESTINAZIONE (ALCUNE PORTE COMUNI: 53 E 161)


PORTA APERTA:
CLIENT
PACCHETTO
UDP
SERVER
CLIENT
RISPOSTA
UDP
SERVER