

-sS (SYN scan stealth – opzione di base di nmap)

```
(davide@kali)-[~]
$ sudo nmap -sS 192.168.50.101
[sudo] password di davide:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 16:58 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00012s 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: 08:00:27:7F:1D:B7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.57 seconds
```

-sV (Abilita il version detection. In alternativa, è possibile utilizzare l'opzione -A che attiva il version detection, tra le altre cose.)

```
(davide@kali)-[~]
$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 16:59 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000056s 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  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
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:7F:1D:B7 (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 66.17 seconds
```

-sV -oN (System version + creazione di file txt)

```
(davide@kali)-[~]
$ sudo nmap -sV -oN scansione_metasploitable 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 17:01 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000087s 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  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
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:7F:1D:B7 (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 65.84 seconds
```

-sS porta 8080 (SYN stealth scan su porta singola 8080)

```
(davide@kali)-[~]
$ sudo nmap -sS -p 8080 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 17:03 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00016s latency).

PORT      STATE SERVICE
8080/tcp  closed http-proxy
MAC Address: 08:00:27:7F:1D:B7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

-p senza range di porte

```
(davide@kali)-[~]
$ sudo nmap -sS -p 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 17:03 CEST
Error #487: Your port specifications are illegal. Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!
```


-sU -r -v (scan UDP in ordine numerico -r e aumento della verbosità della scansione con -v)

```
(davide@kali)-[~]
$ sudo nmap -sU -r -v 192.168.50.101 -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-05 19:28 CEST
Initiating ARP Ping Scan at 19:28
Scanning 192.168.50.101 [1 port]
Completed ARP Ping Scan at 19:28, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:28
Stats: 0:00:09 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Completed Parallel DNS resolution of 1 host. at 19:28, 13.30s elapsed
Initiating UDP Scan at 19:28
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
Warning: 192.168.50.101 giving up on port because retransmission cap hit (2).
Discovered open port 137/udp on 192.168.50.101
Discovered open port 2049/udp on 192.168.50.101
Increasing send delay for 192.168.50.101 from 0 to 50 due to 11 out of 23 dropped probes since last increase.
Increasing send delay for 192.168.50.101 from 50 to 100 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 192.168.50.101 from 100 to 200 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 192.168.50.101 from 200 to 400 due to 11 out of 23 dropped probes since last increase.
UDP Scan Timing: About 71.67% done; ETC: 19:30 (0:00:30 remaining)
Increasing send delay for 192.168.50.101 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 74.47% done; ETC: 19:31 (0:00:36 remaining)
UDP Scan Timing: About 78.00% done; ETC: 19:31 (0:00:40 remaining)
UDP Scan Timing: About 82.17% done; ETC: 19:32 (0:00:40 remaining)
UDP Scan Timing: About 86.27% done; ETC: 19:33 (0:00:36 remaining)
Completed UDP Scan at 19:35, 418.78s elapsed (1000 total ports)
Nmap scan report for 192.168.50.101
Host is up (0.00020s latency).
Not shown: 608 open|filtered udp ports (no-response), 388 closed udp ports (port-unreach)
PORT      STATE SERVICE
53/udp    open  domain
111/udp   open  rpcbind
137/udp   open  netbios-ns
2049/udp  open  nfs
MAC Address: 08:00:27:7F:1D:B7 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 432.26 seconds
Raw packets sent: 2438 (101.107KB) | Rcvd: 432 (37.130KB)
```

-O (Abilita la OS detection). In alternativa, è possibile utilizzare l'opzione **-A** per attivare sia l'OS detection, tra le altre cose.

```
(davide@kali)-[~]
$ sudo nmap -O 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 17:04 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00013s 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: 08:00:27:7F:1D:B7 (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 14.95 seconds
```

-sV (version detection – alias: **-sR**)

```
(davide@kali)-[~]
$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 16:59 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000056s 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  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
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:7F:1D:B7 (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 66.17 seconds
```

-f (fast scan)

```
(davide@kali)-[~]
$ sudo nmap -f 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 17:06 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00011s 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: 08:00:27:7F:1D:B7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
```

-PR (ARP/Neighbor Discovery)

```
(davide@kali)-[~]
$ sudo nmap -PR 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 17:06 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000099s 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: 08:00:27:7F:1D:B7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

-sP (opzione -sn, ovvero senza port scan).

Port scan dopo un host discovery e di mostrare gli host che hanno risposto. Quest'opzione è spesso conosciuta come «ping scan», ma si può anche richiedere il traceroute ed eseguire script host NSE. Quest'azione è un gradino più invadente della List Scan, e spesso può essere usata per lo stesso scopo. Essa permette una mappatura di una rete obiettivo senza attrarre molta attenzione. Sapere quanti host sono attivi è più utile ad un attaccante rispetto ad una semplice List Scan di ogni indirizzo IP e nome di host.

```
(davide@kali)-[~]
$ nmap -sP 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 17:20 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00041s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```




k-rad

→ SYN (Request port 22 connection)

← SYN/ACK (It's open, go ahead)

→ RST (No, forget it!)



scanme