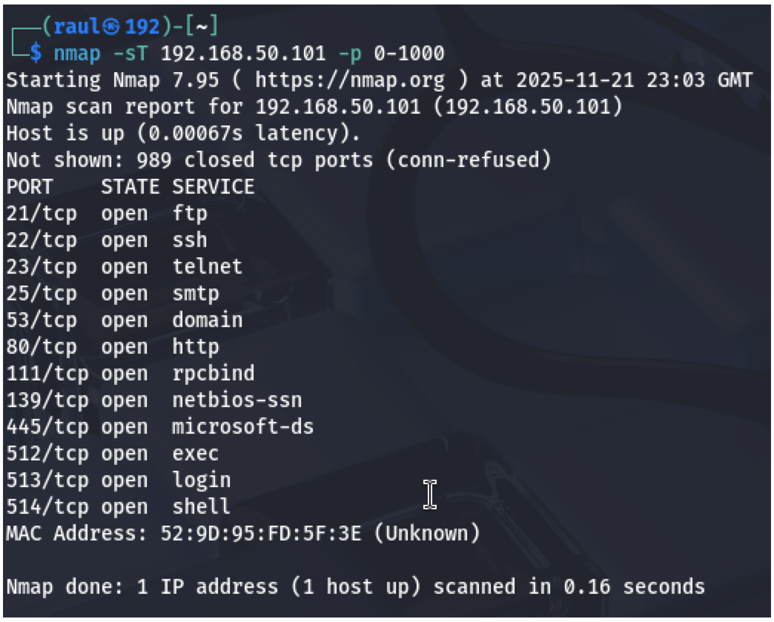
Raul Pastor

Nmap

L'esercizio di oggi riguarda l'utilizzo del tool nmap dalla macchina kali verso la macchina metasploitable con l'utilizzo di tre tipi di scan diversi:

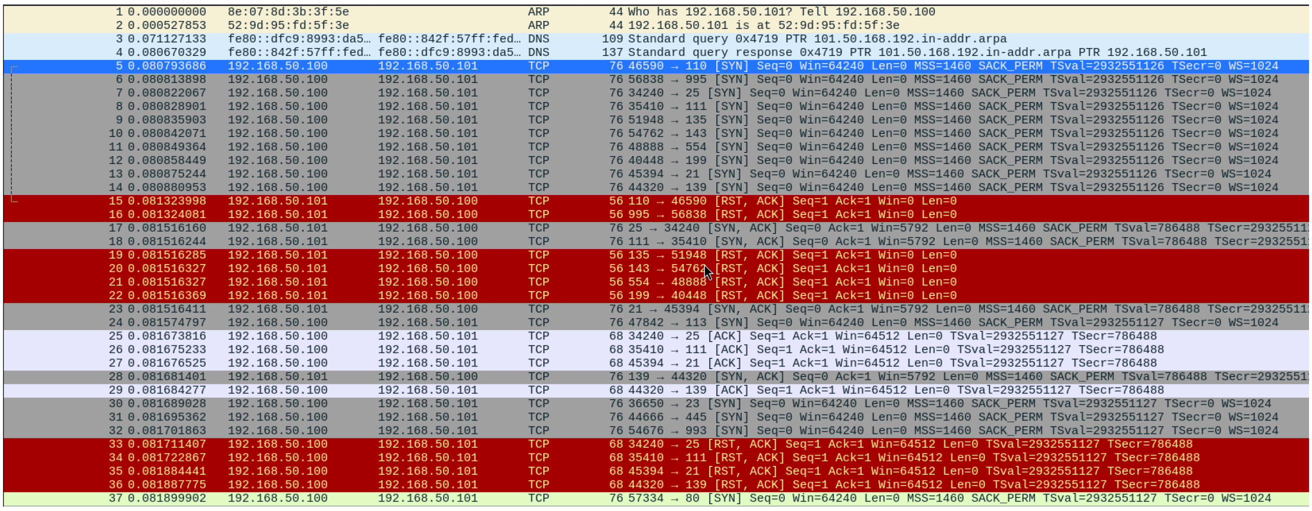
- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well-known
- Scansione con switch «-A» sulle porte well-known

Il primo scan effettuato è il TCP sulle prime mille porte:



```
┌──(raul㉿192)-[~]
└─$ nmap -sT 192.168.50.101 -p 0-1000
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 23:03 GMT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00067s latency).
Not shown: 989 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
MAC Address: 52:9D:95:FD:5F:3E (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

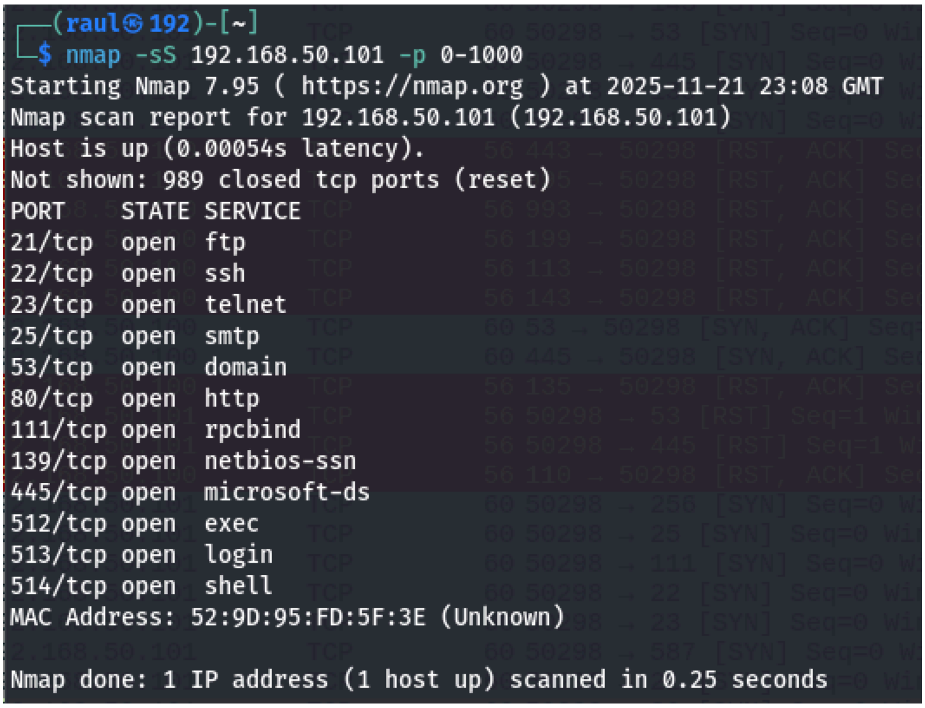
Questo tipo di scan è molto invasivo perché effettua e conclude il three-way handshake, quindi di fatto, creando una vera connessione tra le macchine come possiamo vedere dalla cattura con wireshark:



```
 1 0.000000000  8e:07:8d:3b:3f:5e                        ARP   44 Who has 192.168.50.101? Tell 192.168.50.100
 2 0.000527853  52:9d:95:fd:5f:3e                        ARP   44 192.168.50.101 is at 52:9d:95:fd:5f:3e
 3 0.071127133  fe80::dfc9:8993:da5…  fe80::842f:57ff:fed…  DNS  109 Standard query 0x4719 PTR 101.50.168.192.in-addr.arpa
 4 0.080670329  fe80::842f:57ff:fed…  fe80::dfc9:8993:da5…  DNS  137 Standard query response 0x4719 PTR 101.50.168.192.in-addr.arpa PTR 192.168.50.101
 5 0.080793686  192.168.50.100  192.168.50.101  TCP  76 46590 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551126 TSecr=0 WS=1024
 6 0.080813898  192.168.50.100  192.168.50.101  TCP  76 56838 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551126 TSecr=0 WS=1024
 7 0.080822067  192.168.50.100  192.168.50.101  TCP  76 34240 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551126 TSecr=0 WS=1024
 8 0.080828901  192.168.50.100  192.168.50.101  TCP  76 35410 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551126 TSecr=0 WS=1024
 9 0.080835903  192.168.50.100  192.168.50.101  TCP  76 51948 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551126 TSecr=0 WS=1024
10 0.080842071  192.168.50.100  192.168.50.101  TCP  76 54762 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551126 TSecr=0 WS=1024
11 0.080849364  192.168.50.100  192.168.50.101  TCP  76 48888 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551126 TSecr=0 WS=1024
12 0.080858449  192.168.50.100  192.168.50.101  TCP  76 40448 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551126 TSecr=0 WS=1024
13 0.080875244  192.168.50.100  192.168.50.101  TCP  76 45394 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551126 TSecr=0 WS=1024
14 0.080880953  192.168.50.100  192.168.50.101  TCP  76 44320 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551126 TSecr=0 WS=1024
15 0.081323998  192.168.50.101  192.168.50.100  TCP  56 110 → 46590 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16 0.081324081  192.168.50.101  192.168.50.100  TCP  56 995 → 56838 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17 0.081516160  192.168.50.101  192.168.50.100  TCP  76 25 → 34240 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=786488 TSecr=29325511
18 0.081516244  192.168.50.101  192.168.50.100  TCP  76 111 → 35410 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=786488 TSecr=2932551
19 0.081516285  192.168.50.101  192.168.50.100  TCP  56 135 → 51948 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20 0.081516327  192.168.50.101  192.168.50.100  TCP  56 143 → 54762 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21 0.081516327  192.168.50.101  192.168.50.100  TCP  56 554 → 48888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22 0.081516369  192.168.50.101  192.168.50.100  TCP  56 199 → 40448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 0.081516411  192.168.50.101  192.168.50.100  TCP  76 21 → 45394 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=786488 TSecr=29325511
24 0.081574797  192.168.50.100  192.168.50.101  TCP  76 47842 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551127 TSecr=0 WS=1024
25 0.081673816  192.168.50.100  192.168.50.101  TCP  68 34240 → 25 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=2932551127 TSecr=786488
26 0.081675233  192.168.50.100  192.168.50.101  TCP  68 35410 → 111 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=2932551127 TSecr=786488
27 0.081676525  192.168.50.100  192.168.50.101  TCP  68 45394 → 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=2932551127 TSecr=786488
28 0.081681401  192.168.50.101  192.168.50.100  TCP  76 139 → 44320 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=786488 TSecr=2932551
29 0.081684277  192.168.50.100  192.168.50.101  TCP  68 44320 → 139 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=2932551127 TSecr=786488
30 0.081689028  192.168.50.100  192.168.50.101  TCP  76 36650 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551127 TSecr=0 WS=1024
31 0.081695362  192.168.50.100  192.168.50.101  TCP  76 44666 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551127 TSecr=0 WS=1024
32 0.081701863  192.168.50.100  192.168.50.101  TCP  76 54676 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551127 TSecr=0 WS=1024
33 0.081711407  192.168.50.100  192.168.50.101  TCP  68 34240 → 25 [RST, ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=2932551127 TSecr=786488
34 0.081722867  192.168.50.100  192.168.50.101  TCP  68 35410 → 111 [RST, ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=2932551127 TSecr=786488
35 0.081884441  192.168.50.100  192.168.50.101  TCP  68 45394 → 21 [RST, ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=2932551127 TSecr=786488
36 0.081887775  192.168.50.100  192.168.50.101  TCP  68 44320 → 139 [RST, ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=2932551127 TSecr=786488
37 0.081899902  192.168.50.100  192.168.50.101  TCP  76 57334 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2932551127 TSecr=0 WS=1024
```

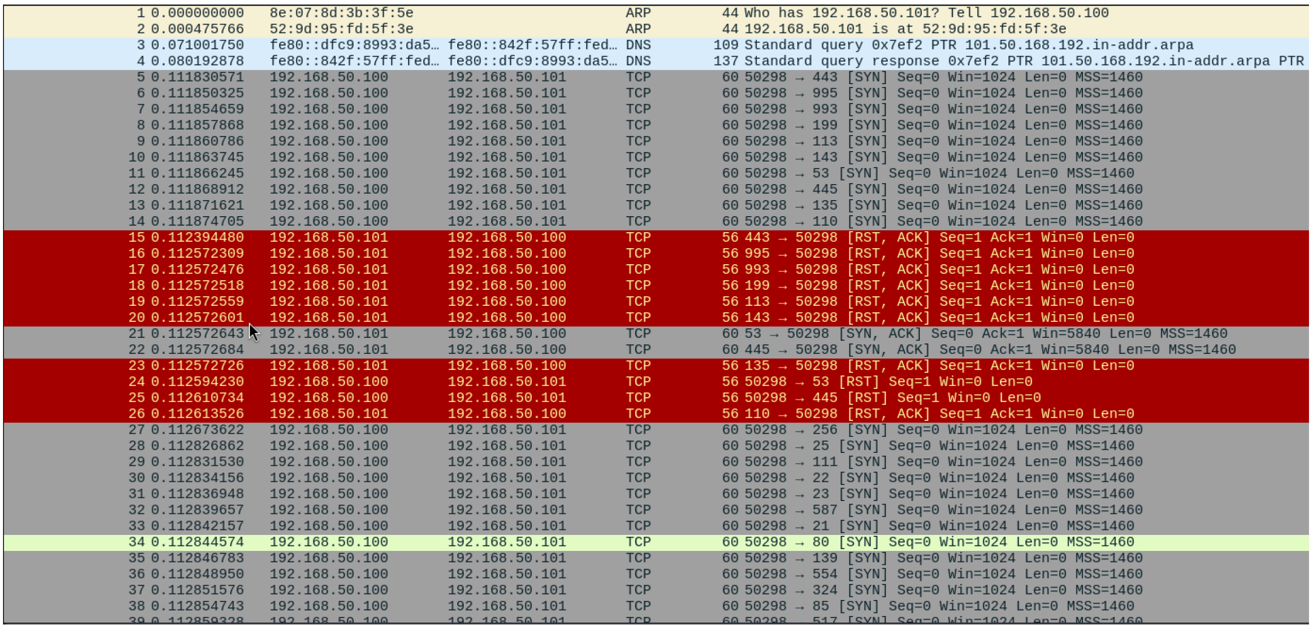
Raul Pastor

Il secondo scan effettuato è il SYN scan che, come suggerisce il nome, si ferma al secondo handshake senza completare la connessione, ci permette solo di sapere se le porte sono chiuse o aperte in base alla risposta dell'host:



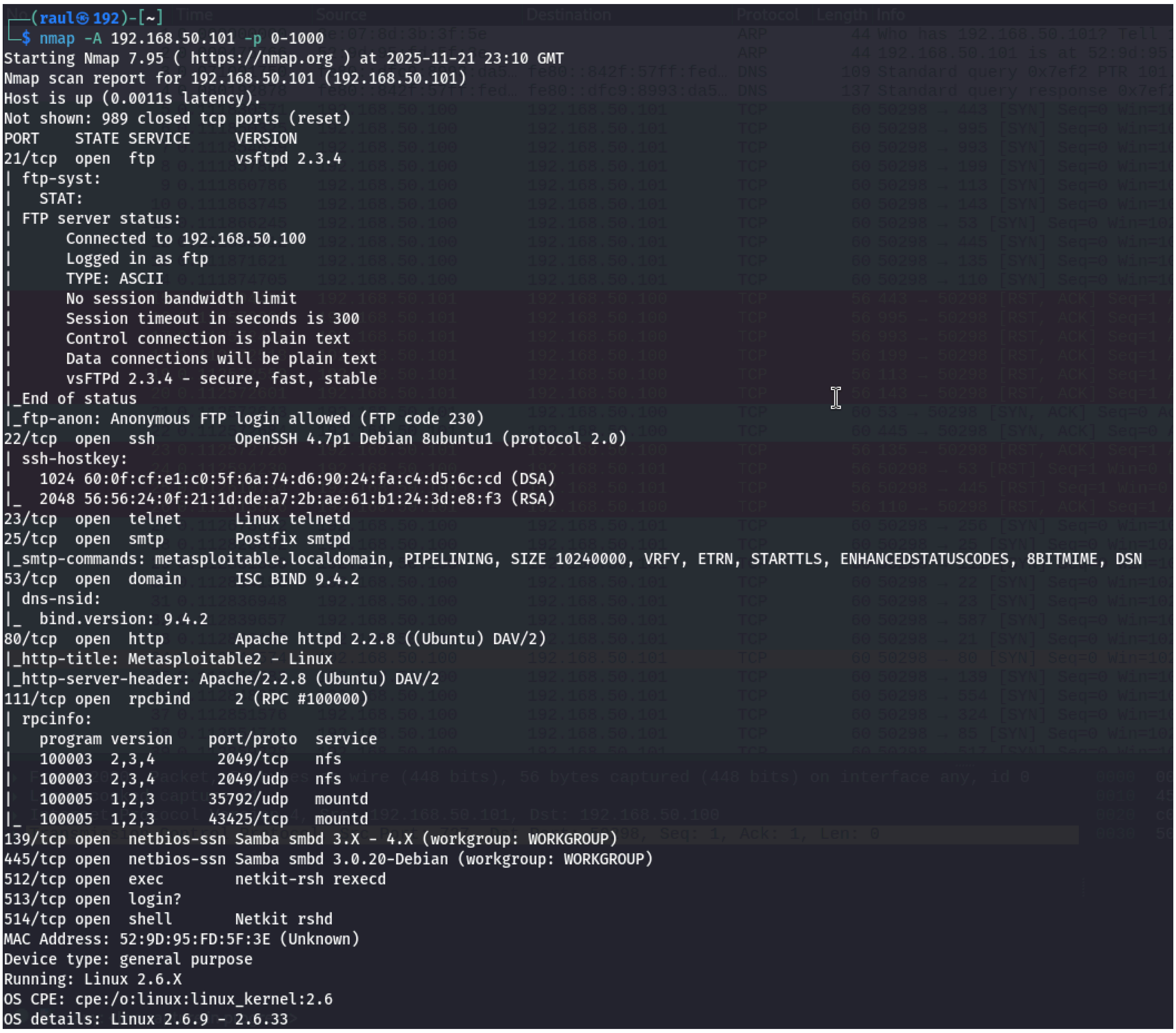
```
┌──(raul㉿192)-[~]
└─$ nmap -sS 192.168.50.101 -p 0-1000
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 23:08 GMT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00054s latency).
Not shown: 989 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  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
MAC Address: 52:9D:95:FD:5F:3E (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Di seguito la cattura di alcuni pacchetti con wireshark:



```
 1 0.000000000  8e:07:8d:3b:3f:5e                            ARP   44 Who has 192.168.50.101? Tell 192.168.50.100
 2 0.000475766  52:9d:95:fd:5f:3e                            ARP   44 192.168.50.101 is at 52:9d:95:fd:5f:3e
 3 0.071001750  fe80::dfc9:8993:da5… fe80::842f:57ff:fed…   DNS  109 Standard query 0x7ef2 PTR 101.50.168.192.in-addr.arpa
 4 0.080192878  fe80::842f:57ff:fed… fe80::dfc9:8993:da5…   DNS  137 Standard query response 0x7ef2 PTR 101.50.168.192.in-addr.arpa PTR
 5 0.111830571  192.168.50.100       192.168.50.101         TCP   60 50298 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 6 0.111850325  192.168.50.100       192.168.50.101         TCP   60 50298 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 7 0.111854659  192.168.50.100       192.168.50.101         TCP   60 50298 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 8 0.111857868  192.168.50.100       192.168.50.101         TCP   60 50298 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 9 0.111860786  192.168.50.100       192.168.50.101         TCP   60 50298 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10 0.111863745  192.168.50.100       192.168.50.101         TCP   60 50298 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11 0.111866245  192.168.50.100       192.168.50.101         TCP   60 50298 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12 0.111868912  192.168.50.100       192.168.50.101         TCP   60 50298 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13 0.111871621  192.168.50.100       192.168.50.101         TCP   60 50298 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14 0.111874705  192.168.50.100       192.168.50.101         TCP   60 50298 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15 0.112394480  192.168.50.101       192.168.50.100         TCP   56 443 → 50298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16 0.112572309  192.168.50.101       192.168.50.100         TCP   56 995 → 50298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17 0.112572476  192.168.50.101       192.168.50.100         TCP   56 993 → 50298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18 0.112572518  192.168.50.101       192.168.50.100         TCP   56 199 → 50298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19 0.112572559  192.168.50.101       192.168.50.100         TCP   56 113 → 50298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20 0.112572601  192.168.50.101       192.168.50.100         TCP   56 143 → 50298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21 0.112572643  192.168.50.101       192.168.50.100         TCP   60 53 → 50298 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
22 0.112572684  192.168.50.101       192.168.50.100         TCP   60 445 → 50298 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
23 0.112572726  192.168.50.101       192.168.50.100         TCP   56 135 → 50298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24 0.112594230  192.168.50.100       192.168.50.101         TCP   56 50298 → 53 [RST] Seq=1 Win=0 Len=0
25 0.112610734  192.168.50.100       192.168.50.101         TCP   56 50298 → 445 [RST] Seq=1 Win=0 Len=0
26 0.112613526  192.168.50.101       192.168.50.100         TCP   56 110 → 50298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27 0.112673622  192.168.50.100       192.168.50.101         TCP   60 50298 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28 0.112826862  192.168.50.100       192.168.50.101         TCP   60 50298 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
29 0.112831530  192.168.50.100       192.168.50.101         TCP   60 50298 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
30 0.112834156  192.168.50.100       192.168.50.101         TCP   60 50298 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31 0.112836948  192.168.50.100       192.168.50.101         TCP   60 50298 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32 0.112839657  192.168.50.100       192.168.50.101         TCP   60 50298 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
33 0.112842157  192.168.50.100       192.168.50.101         TCP   60 50298 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
34 0.112844574  192.168.50.100       192.168.50.101         TCP   60 50298 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
35 0.112846783  192.168.50.100       192.168.50.101         TCP   60 50298 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
36 0.112848950  192.168.50.100       192.168.50.101         TCP   60 50298 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
37 0.112851576  192.168.50.100       192.168.50.101         TCP   60 50298 → 324 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
38 0.112854743  192.168.50.100       192.168.50.101         TCP   60 50298 → 85 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
39 0.112859328  192.168.50.100       192.168.50.101         TCP   60 50298 → 517 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

Infine l’utilizzo dello switch -A permette di vedere molte piu informazioni, sia sul sitema operativo che sui servizi presenti sulle porte, ma è uno dei più invasivi (cioè che invia piu richieste):



```
┌──(raul㉿192)-[~]
└─$ nmap -A 192.168.50.101 -p 0-1000
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 23:10 GMT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.0011s latency).
Not shown: 989 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp  open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      35792/udp   mountd
|_  100005  1,2,3      43425/tcp   mountd
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
MAC Address: 52:9D:95:FD:5F:3E (Unknown)
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
```