Scan veloce della rete per trovare gli host up, partendo dall'ip della macchina attaccante

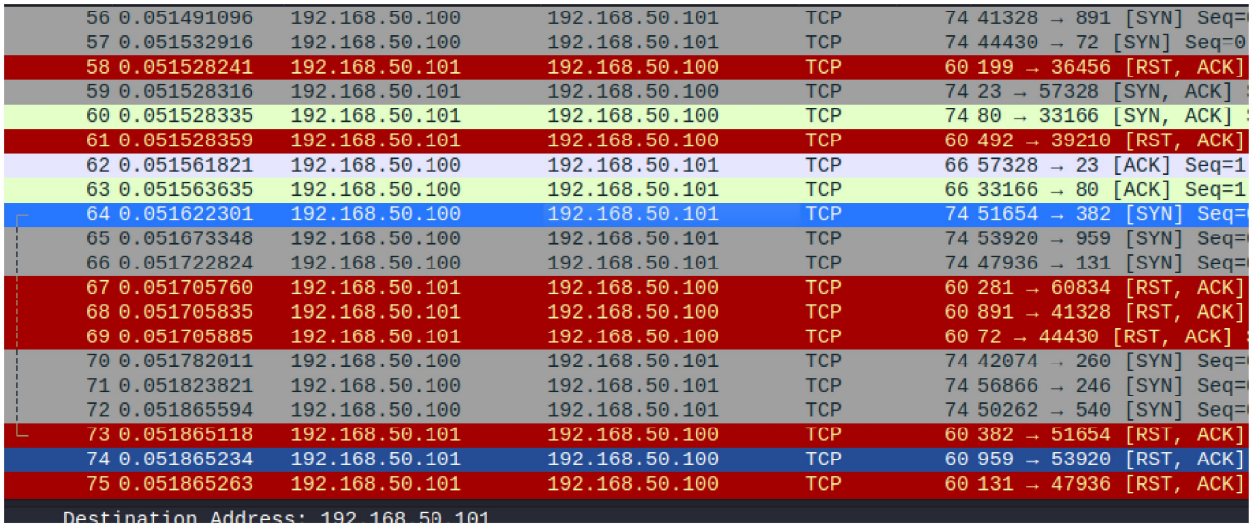
Con lo /24 per scansionare tutta la subnet

```
┌──(alessio㉿kali)-[~]
└─$ nmap -F -T4 192.168.50.100/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 07:30 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
valid servers with --dns-servers
Nmap scan report for 192.168.50.100
Host is up (0.0014s latency).
All 100 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

Nmap scan report for 192.168.50.101
Host is up (0.0017s latency).
Not shown: 82 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
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
8009/tcp open  ajp13

Nmap done: 256 IP addresses (2 hosts up) scanned in 14.11 seconds
```

Scan con TCP

```
┌──(alessio㉿kali)-[~]
└─$ sudo nmap -p 1-1024 -sT 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 07:51 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00041s latency).
Not shown: 1012 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: 08:00:27:A4:A4:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Wireshark del TCP

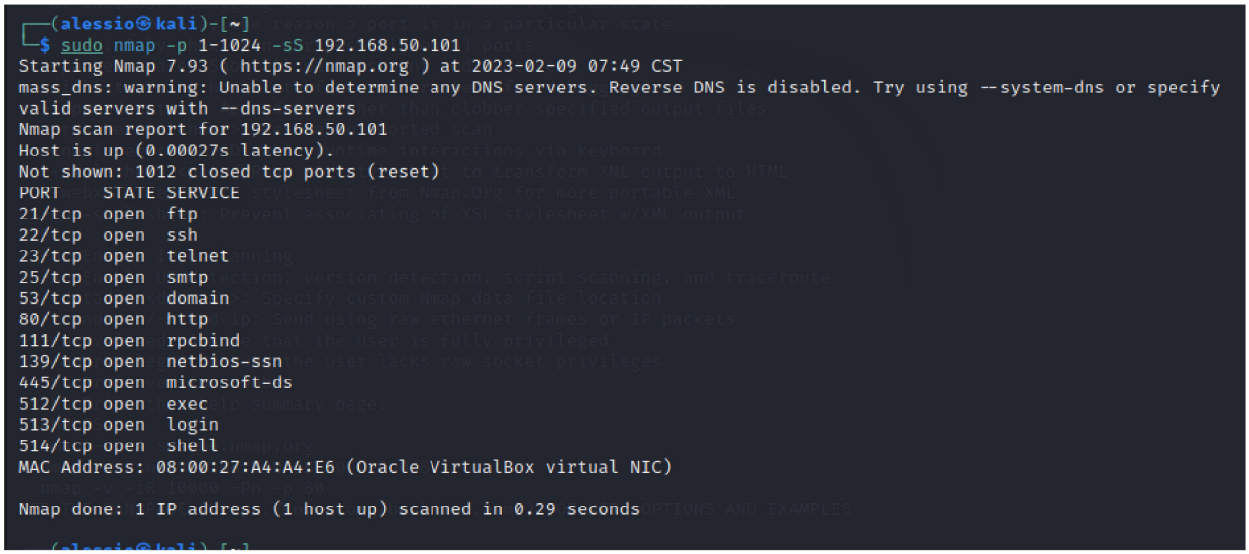


56	0.051491096	192.168.50.100	192.168.50.101	TCP	74 41328 → 891 [SYN] Seq=
57	0.051532916	192.168.50.100	192.168.50.101	TCP	74 44430 → 72 [SYN] Seq=0
58	0.051528241	192.168.50.101	192.168.50.100	TCP	60 199 → 36456 [RST, ACK]
59	0.051528316	192.168.50.101	192.168.50.100	TCP	74 23 → 57328 [SYN, ACK]
60	0.051528335	192.168.50.101	192.168.50.100	TCP	74 80 → 33166 [SYN, ACK]
61	0.051528359	192.168.50.101	192.168.50.100	TCP	60 492 → 39210 [RST, ACK]
62	0.051561821	192.168.50.100	192.168.50.101	TCP	66 57328 → 23 [ACK] Seq=1
63	0.051563635	192.168.50.100	192.168.50.101	TCP	66 33166 → 80 [ACK] Seq=1
64	0.051622301	192.168.50.100	192.168.50.101	TCP	74 51654 → 382 [SYN] Seq=
65	0.051673348	192.168.50.100	192.168.50.101	TCP	74 53920 → 959 [SYN] Seq=
66	0.051722824	192.168.50.100	192.168.50.101	TCP	74 47936 → 131 [SYN] Seq=
67	0.051705760	192.168.50.101	192.168.50.100	TCP	60 281 → 60834 [RST, ACK]
68	0.051705835	192.168.50.101	192.168.50.100	TCP	60 891 → 41328 [RST, ACK]
69	0.051705885	192.168.50.101	192.168.50.100	TCP	60 72 → 44430 [RST, ACK]
70	0.051782011	192.168.50.100	192.168.50.101	TCP	74 42074 → 260 [SYN] Seq=
71	0.051823821	192.168.50.100	192.168.50.101	TCP	74 56866 → 246 [SYN] Seq=
72	0.051865594	192.168.50.100	192.168.50.101	TCP	74 50262 → 540 [SYN] Seq=
73	0.051865118	192.168.50.101	192.168.50.100	TCP	60 382 → 51654 [RST, ACK]
74	0.051865234	192.168.50.101	192.168.50.100	TCP	60 959 → 53920 [RST, ACK]
75	0.051865263	192.168.50.101	192.168.50.100	TCP	60 131 → 47936 [RST, ACK]

Destination Address: 192.168.50.101

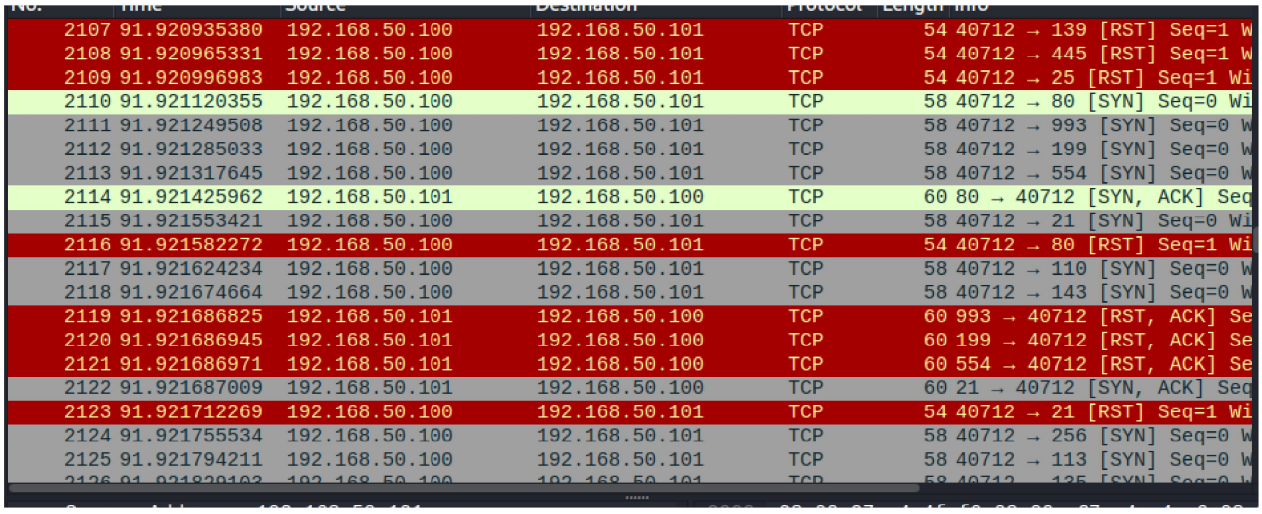
Qui possiamo vedere a sinistra la source in questo caso il pacchetto 60 è la risposta di meta alla richiesta di SYN di kali, dopo la freccina la porta sulla quale stanno comunicando, il pacchetto 63 indica la riposta del protocollo TCP, che non ci sarebbe stata con il SYN

Scan con SYN



```
┌──(alessio㉿kali)-[~]
└─$ sudo nmap -p 1-1024 -sS 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 07:49 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00027s latency).
Not shown: 1012 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: 08:00:27:A4:A4:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

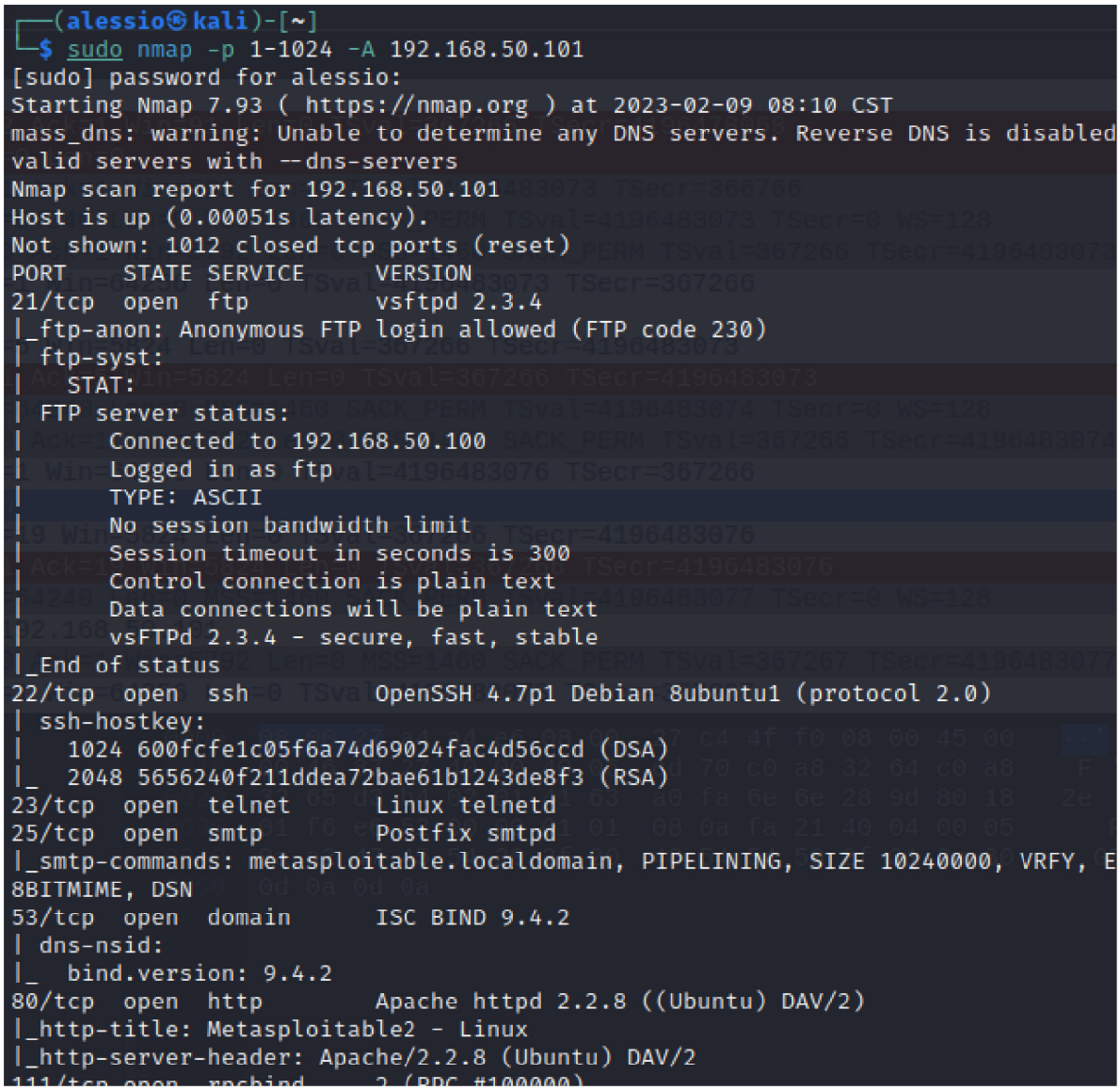
Wireshark con SYN



2107	91.920935380	192.168.50.100	192.168.50.101	TCP	54 40712 → 139 [RST] Seq=1 W
2108	91.920965331	192.168.50.100	192.168.50.101	TCP	54 40712 → 445 [RST] Seq=1 W
2109	91.920996983	192.168.50.100	192.168.50.101	TCP	54 40712 → 25 [RST] Seq=1 Wi
2110	91.921120355	192.168.50.100	192.168.50.101	TCP	58 40712 → 80 [SYN] Seq=0 Wi
2111	91.921249508	192.168.50.100	192.168.50.101	TCP	58 40712 → 993 [SYN] Seq=0 W
2112	91.921285033	192.168.50.100	192.168.50.101	TCP	58 40712 → 199 [SYN] Seq=0 W
2113	91.921317645	192.168.50.100	192.168.50.101	TCP	58 40712 → 554 [SYN] Seq=0 W
2114	91.921425962	192.168.50.101	192.168.50.100	TCP	60 80 → 40712 [SYN, ACK] Seq
2115	91.921553421	192.168.50.100	192.168.50.101	TCP	58 40712 → 21 [SYN] Seq=0 Wi
2116	91.921582272	192.168.50.100	192.168.50.101	TCP	54 40712 → 80 [RST] Seq=1 Wi
2117	91.921624234	192.168.50.100	192.168.50.101	TCP	58 40712 → 110 [SYN] Seq=0 W
2118	91.921674664	192.168.50.100	192.168.50.101	TCP	58 40712 → 143 [SYN] Seq=0 W
2119	91.921686825	192.168.50.101	192.168.50.100	TCP	60 993 → 40712 [RST, ACK] Se
2120	91.921686945	192.168.50.101	192.168.50.100	TCP	60 199 → 40712 [RST, ACK] Se
2121	91.921686971	192.168.50.101	192.168.50.100	TCP	60 554 → 40712 [RST, ACK] Se
2122	91.921687009	192.168.50.101	192.168.50.100	TCP	60 21 → 40712 [SYN, ACK] Seq
2123	91.921712269	192.168.50.100	192.168.50.101	TCP	54 40712 → 21 [RST] Seq=1 Wi
2124	91.921755534	192.168.50.100	192.168.50.101	TCP	58 40712 → 256 [SYN] Seq=0 W
2125	91.921794211	192.168.50.100	192.168.50.101	TCP	58 40712 → 113 [SYN] Seq=0 W

Qui si nota che non ci sono risposte da parte di kali alla ack di meta

Scansione con -A



```
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      33280/udp   mountd
|   100005  1,2,3      35048/tcp   mountd
|   100021  1,3,4      38717/udp   nlockmgr
|   100021  1,3,4      42323/tcp   nlockmgr
|   100024  1          41240/udp   status
|_  100024  1          47940/tcp   status
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: 08:00:27:A4:A4:E6 (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
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-02-09T10:11:02-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_clock-skew: mean: 3h29m59s, deviation: 3h32m07s, median: 59m59s
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.24 seconds
```

Wireshark di -A

192.168.50.101	192.168.50.100	Rlogin	67	Data: \001
192.168.50.101	192.168.50.100	TCP	66	513 → 57622 [RST, ACK] Seq=2 Ack
192.168.50.100	192.168.50.101	TCP	54	57622 → 513 [RST] Seq=1 Win=0 Le
192.168.50.100	192.168.50.101	TCP	66	54186 → 513 [FIN, ACK] Seq=1 Ack
192.168.50.100	192.168.50.101	TCP	74	54192 → 513 [SYN] Seq=0 Win=6424
192.168.50.101	192.168.50.100	TCP	74	513 → 54192 [SYN, ACK] Seq=0 Ack
192.168.50.100	192.168.50.101	TCP	66	54192 → 513 [ACK] Seq=1 Ack=1 Wi
192.168.50.100	192.168.50.101	Rlogin	70	Data: \r\n\r\n
192.168.50.101	192.168.50.100	TCP	66	513 → 54192 [ACK] Seq=1 Ack=5 Wi
192.168.50.101	192.168.50.100	TCP	66	513 → 54192 [RST, ACK] Seq=1 Ack
192.168.50.100	192.168.50.101	TCP	74	54196 → 513 [SYN] Seq=0 Win=6424
192.168.50.101	192.168.50.100	TCP	74	513 → 54196 [SYN, ACK] Seq=0 Ack
192.168.50.100	192.168.50.101	TCP	66	54196 → 513 [ACK] Seq=1 Ack=1 Wi
192.168.50.100	192.168.50.101	Rlogin	84	Data: GET / HTTP/1.0\r\n\r\n
192.168.50.101	192.168.50.100	TCP	66	513 → 54196 [ACK] Seq=1 Ack=19 W
192.168.50.101	192.168.50.100	TCP	66	513 → 54196 [RST, ACK] Seq=1 Ack
192.168.50.100	192.168.50.101	TCP	74	54210 → 513 [SYN] Seq=0 Win=6424
PcsCompu_a4:a4:e6	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.1
192.168.50.101	192.168.50.100	TCP	74	513 → 54210 [SYN, ACK] Seq=0 Ack
192.168.50.100	192.168.50.101	TCP	66	54210 → 513 [ACK] Seq=1 Ack=1 Wi