

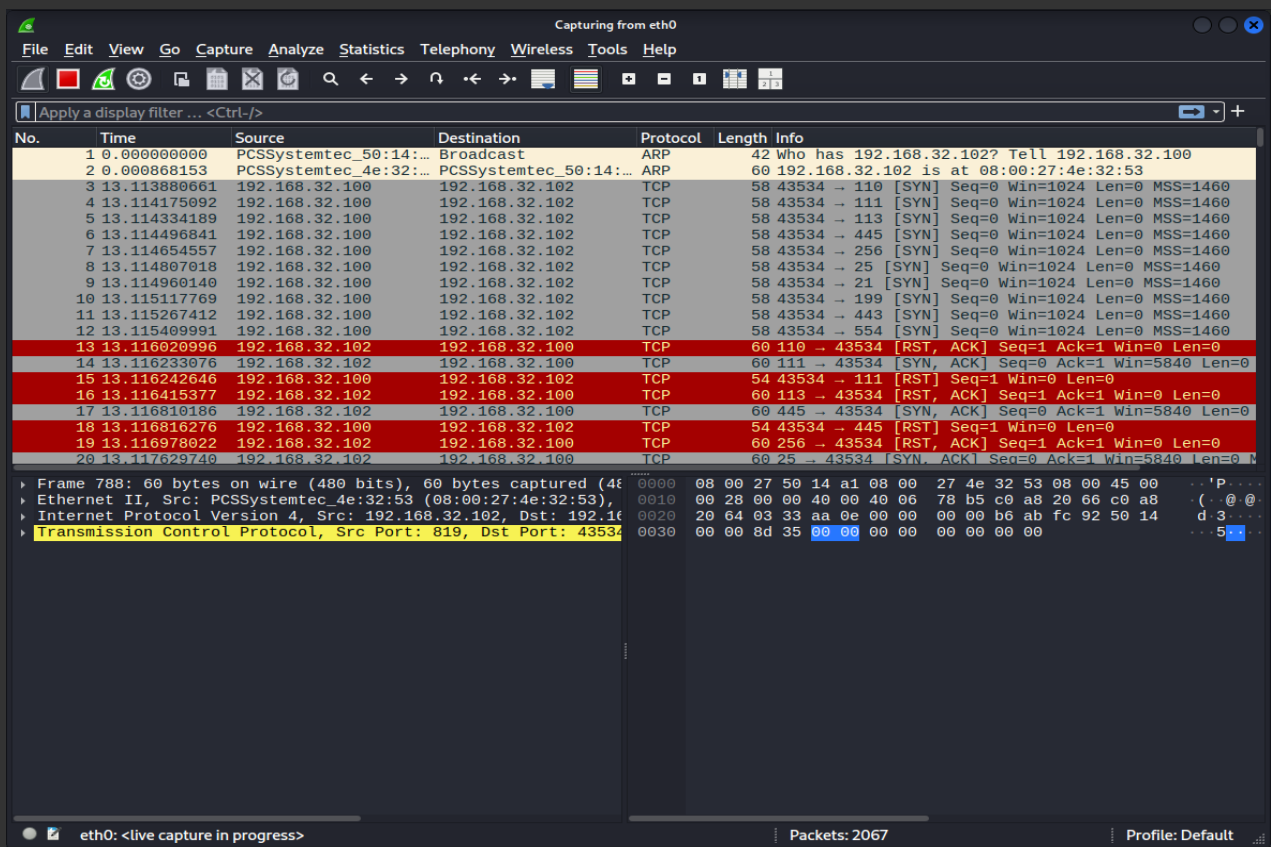
Si utilizza Nmap per raccogliere informazioni sulla macchina Meta.

Effettuando il comando `nmap -sS` e selezionando il range di porte da analizzare con `-p` si visualizzano in maniera più “stealth” le porte con lo stato aperto.

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.32.102 -p 1-1024
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 12:53 EST
Nmap scan report for 192.168.32.102
Host is up (0.00079s 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: 08:00:27:4E:32:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds
```

Possiamo vedere su Wireshark come il Syn Scan non completa il 3 way handshake, ma si ferma solo al primo passaggio.



Con nmap -sT invece andiamo a completare il 3 way handshake, quindi risulta meno “stealth” e più lento.

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.32.102 -p 1-1024
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 13:05 EST
Nmap scan report for 192.168.32.102
Host is up (0.0032s 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: 08:00:27:4E:32:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds
```

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
67	13.100338229	192.168.32.100	192.168.32.102	TCP	74	111 → 36786 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
68	13.100342153	192.168.32.100	192.168.32.102	TCP	74	51290 → 391 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
69	13.100479026	192.168.32.100	192.168.32.102	TCP	66	36786 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
70	13.100551347	192.168.32.100	192.168.32.102	TCP	60	968 → 45290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
71	13.100649360	192.168.32.100	192.168.32.102	TCP	74	35540 → 279 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
72	13.100731708	192.168.32.100	192.168.32.102	TCP	60	1000 → 60908 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
73	13.100892947	192.168.32.100	192.168.32.102	TCP	74	41892 → 442 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
74	13.101157165	192.168.32.100	192.168.32.102	TCP	66	47442 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
75	13.101200032	192.168.32.100	192.168.32.102	TCP	66	52310 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
76	13.101232173	192.168.32.100	192.168.32.102	TCP	66	36786 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
77	13.101307751	192.168.32.100	192.168.32.102	TCP	74	40388 → 887 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
78	13.101326192	192.168.32.100	192.168.32.102	TCP	74	512 → 49758 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
79	13.101326260	192.168.32.100	192.168.32.102	TCP	60	287 → 52730 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	13.101345327	192.168.32.100	192.168.32.102	TCP	66	49758 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
81	13.101392272	192.168.32.100	192.168.32.102	TCP	74	36064 → 385 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
82	13.101498849	192.168.32.100	192.168.32.102	TCP	74	32996 → 572 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
83	13.101502220	192.168.32.100	192.168.32.102	TCP	60	866 → 46286 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	13.101537065	192.168.32.100	192.168.32.102	TCP	74	50730 → 708 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
85	13.101570480	192.168.32.100	192.168.32.102	TCP	74	58012 → 941 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
86	13.101603947	192.168.32.100	192.168.32.102	TCP	74	49042 → 333 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S

Frame 77: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on eth0

Ethernet II, Src: PCSSystemtec_50:14:a1 (08:00:27:50:14:a1), Dst: 192.168.32.102

Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.102

Transmission Control Protocol, Src Port: 40388, Dst Port: 887

0000 08 00 27 4e 32 53 08 00 27 50 14 a1 08 00 45 00 ...N2S...

0010 00 3c a5 3e 40 00 40 06 d3 62 c0 a8 20 64 c0 a8 ...<>@.0...

0020 20 66 9d c4 03 77 45 8f 34 25 00 00 00 00 a0 02 ...f...wE...

0030 fa f0 c2 49 00 00 02 04 05 b4 04 02 08 0a 92 3f ...I...I...

0040 65 ca 00 00 00 01 03 03 07 ...e...

eth0: <live capture in progress> Packets: 2074 Profile: Default

Invece con nmap -A si riesce, in un tempo ancora meno breve, ad avere un analisi molto più completa.

```
(root@kali)-[/home/kali]
# nmap -A 192.168.32.102 -p 1-1024
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 13:07 EST
Nmap scan report for 192.168.32.102
Host is up (0.0012s latency).
Not shown: 1012 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.32.100
|_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/dns    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
|_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 37793/tcp mountd
|_100005 1,2,3 56670/udp mountd
|_100021 1,3,4 41661/udp nlockmgr
|_100021 1,3,4 52996/tcp nlockmgr
|_100024 1 41455/tcp status
|_100024 1 57005/udp 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: 08:00:27:4E:32:53 (PCS Systemtechnik/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:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 2h30m00s, deviation: 3h32m07s, median: 0s
|_smb2-time: Protocol negotiation failed (SMB2)
|_smb-security-mode:
|_account_used: guest
|_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: 2025-12-05T13:08:32-05:00
```

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-I>

No.	Time	Source	Destination	Protocol	Length	Info
3458	78.764844327	192.168.32.100	192.168.32.102	SMTP	154	C: DATA fragment, 88 bytes
3459	78.765775954	192.168.32.102	192.168.32.100	TCP	66	25 → 43328 [ACK] Seq=1 Ack=89 Win=5792 Len=0 TSval=
3460	78.870186744	192.168.32.100	192.168.32.102	TCP	66	39518 → 25 [RST, ACK] Seq=1673 Ack=56 Win=64256 Len=0
3461	79.720858677	PCSSystemtec_4e:32:...	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.102
3462	80.720303242	PCSSystemtec_4e:32:...	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.102
3463	82.516158277	192.168.32.100	192.168.32.102	TCP	66	43314 → 25 [FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0
3464	82.517652556	192.168.32.102	192.168.32.100	TCP	66	25 → 43314 [ACK] Seq=1 Ack=2 Win=5792 Len=0 TSval=
3465	83.719010945	PCSSystemtec_4e:32:...	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.102
3466	84.717829481	PCSSystemtec_4e:32:...	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.102
3467	85.428000112	192.168.32.102	192.168.32.100	SMTP	121	S: 220 metasploitable.localdomain ESMTP Postfix (L
3468	85.428022283	192.168.32.100	192.168.32.102	TCP	54	43314 → 25 [RST] Seq=2 Win=0 Len=0
3469	85.717365527	PCSSystemtec_4e:32:...	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.102
3470	88.706251678	192.168.32.102	192.168.32.100	SMTP	121	S: 220 metasploitable.localdomain ESMTP Postfix (L
3471	88.706315638	192.168.32.100	192.168.32.102	TCP	66	43328 → 25 [ACK] Seq=89 Ack=56 Win=64256 Len=0 TSv
3472	88.706843500	192.168.32.102	192.168.32.100	SMTP	177	S: 502 5.5.2 Error: command not recognized 502 5
3473	88.706855689	192.168.32.100	192.168.32.102	TCP	66	43328 → 25 [ACK] Seq=89 Ack=167 Win=64256 Len=0 TS
3474	88.708286507	192.168.32.100	192.168.32.102	TCP	66	43328 → 25 [RST, ACK] Seq=89 Ack=167 Win=64256 Len=0
3475	331.250811848	192.168.32.102	192.168.32.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Workstat
3476	331.250965818	192.168.32.102	192.168.32.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workst

Frame 2272: 74 bytes on wire (592 bits), 74 bytes captured (5920 bits) on interface eth0

Ethernet II, Src: PCSSystemtec_50:14:a1 (08:00:27:50:14:a1), Dst: 01:00:5e:00:00:01

Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.102

Transmission Control Protocol, Src Port: 41682, Dst Port: 5135