

NMAP

Scansione nmap con wireshark da kali 192.168.50.100 a metasploitable2 192.168.50.101

Scansione TCP >nmap -sT 192.168.50.101

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101
2	0.000028466	PcsCompu_fe:15:08		ARP	62	192.168.50.101 is at 08
3	0.043173803	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101
4	1.055381100	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101
5	2.078931706	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101
6	3.099359625	192.168.50.100	192.168.50.100	ICMP	117	Destination unreachable
7	4.044999562	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101
8	5.087868203	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101
9	6.111055606	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101
10	7.130851254	192.168.50.100	192.168.50.100	ICMP	117	Destination unreachable
11	8.046552966	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101
12	9.055626197	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101
13	10.079154118	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101
14	11.103216608	192.168.50.100	192.168.50.100	ICMP	117	Destination unreachable
15	13.047236734	192.168.50.100	192.168.50.101	TCP	76	59444 → 587 [SYN] Seq=0
16	13.047379359	192.168.50.100	192.168.50.101	TCP	76	35216 → 199 [SYN] Seq=0
17	13.047558222	192.168.50.100	192.168.50.101	TCP	76	40514 → 53 [SYN] Seq=0
18	13.047634164	192.168.50.100	192.168.50.101	TCP	76	45304 → 995 [SYN] Seq=0
19	13.047739993	192.168.50.100	192.168.50.101	TCP	76	59526 → 443 [SYN] Seq=0
20	13.048072897	192.168.50.100	192.168.50.101	TCP	76	60912 → 8888 [SYN] Seq=0
21	13.048994902	192.168.50.100	192.168.50.101	TCP	76	45712 → 554 [SYN] Seq=0
22	13.049109734	192.168.50.100	192.168.50.101	TCP	76	46996 → 445 [SYN] Seq=0
23	13.049315535	192.168.50.101	192.168.50.100	TCP	62	587 → 59444 [RST, Seq=0
24	13.049315676	192.168.50.101	192.168.50.100	TCP	62	199 → 35216 [RST, Seq=0
25	13.049315716	192.168.50.101	192.168.50.100	TCP	76	53 → 40514 [SYN, Seq=0
26	13.049315795	192.168.50.101	192.168.50.100	TCP	62	995 → 45304 [RST, Seq=0
27	13.049315867	192.168.50.101	192.168.50.100	TCP	62	443 → 59526 [RST, Seq=0
28	13.049553921	192.168.50.100	192.168.50.101	TCP	68	40514 → 53 [ACK] Seq=65536
Frame 11: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0						
Linux cooked capture v1						
Address Resolution Protocol (request)						
65	13.170627092	192.168.50.100	192.168.50.101	TCP	76	34696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
67	13.171364110	192.168.50.101	192.168.50.100	TCP	76	80 → 34696 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
69	13.171374794	192.168.50.100	192.168.50.101	TCP	68	34696 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=18949
95	13.178683494	192.168.50.100	192.168.50.101	TCP	68	34696 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1

(kali@kali) ~

```
$ sudo nmap -sT 192.168.50.101
```

Starting Nmap 7.92 (<https://nmap.org>) 22-11-10 05:19 EST

Nmap scan report for 192.168.50.101

Host is up (0.0033s latency).

Not shown: 977 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

1099/tcp open rmiregistry

1524/tcp open ingreslock

2049/tcp open nfs

2121/tcp open cproxy-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:FE:15:08 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.50 seconds

in totale c'è stato un traffico di circa 2000 pacchetti, e qui sopra c'è la cattura della porta 80 con la sequenza corretta.

Scansione SYN >nmap -sS 192.168.50.101

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_fe:15:08		ARP	62	Who has 192.168.50.100?
2	0.000013689	PcsCompu_22:46:4f		ARP	44	192.168.50.100 is at 08
3	13.746727220	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101?
4	13.747737599	PcsCompu_fe:15:08		ARP	62	192.168.50.101 is at 08
5	13.802434546	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101?
6	14.839153786	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101?
7	15.854155517	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101?
8	16.862812714	192.168.50.100	192.168.50.100	ICMP	117	Destination unreachable
9	17.805647403	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101?
10	18.829926855	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101?
11	19.854454808	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101?
12	20.878616282	192.168.50.100	192.168.50.100	ICMP	117	Destination unreachable
13	21.808368782	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101?
14	22.832131002	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101?
15	23.855416317	PcsCompu_22:46:4f		ARP	44	Who has 192.168.50.101?
16	24.878936324	192.168.50.100	192.168.50.100	ICMP	117	Destination unreachable
17	26.838450338	192.168.50.100	192.168.50.101	IPv4	44	Fragmented IP protocol
18	26.838805242	192.168.50.100	192.168.50.101	IPv4	44	Fragmented IP protocol
19	26.839663311	192.168.50.100	192.168.50.101	TCP	44	62716 → 8888 [SYN] Seq=0
20	26.839337755	192.168.50.100	192.168.50.101	IPv4	44	Fragmented IP protocol
21	26.839575578	192.168.50.101	192.168.50.100	TCP	62	8888 → 62716 [RST, ACK] Seq=1
22	26.839661471	192.168.50.100	192.168.50.101	IPv4	44	Fragmented IP protocol
23	26.839960064	192.168.50.100	192.168.50.101	TCP	44	62716 → 139 [SYN] Seq=0
24	26.840650685	192.168.50.101	192.168.50.100	TCP	62	139 → 62716 [SYN, ACK] Seq=0
25	26.840664795	192.168.50.100	192.168.50.101	TCP	56	62716 → 139 [RST] Seq=1
26	26.841435524	192.168.50.100	192.168.50.101	IPv4	44	Fragmented IP protocol
27	26.842349065	192.168.50.100	192.168.50.101	IPv4	44	Fragmented IP protocol
28	26.842650300	192.168.50.100	192.168.50.101	TCP	44	62716 → 139 [RST] Seq=1
Frame 3313: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0						
Linux cooked capture v1						
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101						
21	13.111990501	192.168.50.100	192.168.50.101	TCP	60	50082 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31	13.112655947	192.168.50.101	192.168.50.100	TCP	62	80 → 50082 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
33	13.112785853	192.168.50.100	192.168.50.101	TCP	56	50082 → 80 [RST] Seq=1 Win=0 Len=0

(kali@kali) ~

```
$ sudo nmap -sS 192.168.50.101
```

Starting Nmap 7.92 (<https://nmap.org>) 22-11-10 05:17 EST

Nmap scan report for 192.168.50.101

Host is up (0.0011s 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 cproxy-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:FE:15:08 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.68 seconds

in totale c'è stato un traffico di circa 4000 pacchetti, e qui sopra c'è la cattura della porta 80 con la sequenza corretta.

Scansione ALL >nmap -A 192.168.50.101

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

No.	Time	Source	Destination	Protocol	Length	Info
4626	158.386194350	192.168.50.101	192.168.50.100	SMTP	138	S: 502 5.5.2 Error
4627	158.386218572	192.168.50.100	192.168.50.101	TCP	68	51598 → 25 [ACK] Seq=6851598 Win=0 Len=0
4628	158.419802057	192.168.50.100	192.168.50.101	TCP	68	51598 → 25 [RST, Seq=6851598 Win=0 Len=0]
4629	158.428340223	192.168.50.100	192.168.50.101	TCP	68	41122 → 25 [RST, Seq=6841122 Win=0 Len=0]
4630	151.114558518	PcsCompu, fe:15:08	192.168.50.101	ARP	62	Who has 192.168.50.101
4631	152.113822978	PcsCompu, fe:15:08	192.168.50.101	ARP	62	Who has 192.168.50.101
4632	153.113656234	PcsCompu, fe:15:08	192.168.50.101	ARP	62	Who has 192.168.50.101
4633	153.161283649	192.168.50.100	192.168.50.101	TCP	68	45944 → 2121 [FIN, Seq=6845944 Win=0 Len=0]
4634	153.161509567	192.168.50.100	192.168.50.101	TCP	76	35472 → 2121 [SYN, Seq=7635472 Win=0 Len=0]
4635	153.162564722	192.168.50.100	192.168.50.101	TCP	76	2121 → 35472 [SYN, Seq=762121 Win=0 Len=0]
4636	153.162654112	192.168.50.100	192.168.50.101	TCP	68	35472 → 2121 [ACK, Seq=6835472 Win=0 Len=0]
4637	153.162748209	192.168.50.100	192.168.50.101	TLSv1	585	Client Hello
4638	153.163161389	192.168.50.101	192.168.50.100	TCP	68	2121 → 45944 [ACK, Seq=682121 Win=0 Len=0]
4639	153.163722755	192.168.50.101	192.168.50.100	TCP	68	2121 → 35472 [ACK, Seq=682121 Win=0 Len=0]
4640	154.163572287	192.168.50.100	192.168.50.101	TCP	68	35472 → 2121 [FIN, Seq=6835472 Win=0 Len=0]
4641	154.202354282	192.168.50.101	192.168.50.100	TCP	68	2121 → 35472 [ACK, Seq=682121 Win=0 Len=0]
4642	156.162565463	192.168.50.101	192.168.50.100	TCP	76	52802 → 113 [SYN, Seq=565113 Win=0 Len=0]
4643	156.162598506	192.168.50.100	192.168.50.101	TCP	56	113 → 52802 [RST, Seq=56113 Win=0 Len=0]
4644	156.163383359	192.168.50.101	192.168.50.100	TCP	127	2121 → 45944 [PSH, Seq=682121 Win=0 Len=0]
4645	156.163398697	192.168.50.100	192.168.50.101	TCP	56	45944 → 2121 [RST, Seq=5645944 Win=0 Len=0]
4646	158.178334901	PcsCompu, fe:15:08	192.168.50.101	ARP	62	Who has 192.168.50.101
4647	159.169660788	PcsCompu, fe:15:08	192.168.50.101	ARP	62	Who has 192.168.50.101
4648	168.169607194	PcsCompu, fe:15:08	192.168.50.101	ARP	62	Who has 192.168.50.101
4649	163.159478427	192.168.50.101	192.168.50.100	TCP	76	48146 → 113 [SYN, Seq=5648146 Win=0 Len=0]
4650	163.159495078	192.168.50.100	192.168.50.101	TCP	56	113 → 48146 [RST, Seq=56113 Win=0 Len=0]
4651	163.161573358	192.168.50.101	192.168.50.100	TCP	127	2121 → 35472 [PSH, Seq=682121 Win=0 Len=0]
4652	163.161596154	192.168.50.100	192.168.50.101	TCP	56	35472 → 2121 [RST, Seq=5635472 Win=0 Len=0]

Frame 11: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0

Linux cooked capture v1

Address Resolution Protocol (request)

0000 00 04 00 01 00 06 08 00 27 22 46 4f 00 00 08 00 "FO

0010 00 01 08 06 04 00 01 08 00 27 22 46 4f 00 00 "FO

0020 32 64 00 00 00 00 00 c0 a8 32 65 20 2e

Not shown: 977 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

| ftp-syst:

| STAI:

| 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:cfa:1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)

| 2048 95:55:24:0c:21:fddc:72:b2:ae:61:b1:24:3d:e8:f3 (RSA)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

| smtp-command: metaspoitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCO

DES, 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

| 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 35670/udp mountd

| 100005 1,2,3 42892/tcp mountd

| 100021 1,3,4 33935/udp nlockmgr

| 100021 1,3,4 42833/tcp nlockmgr

| 100024 1 36345/udp status

| 100024 1 60651/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)

tcp.port == 80

No.	Time	Source	Destination	Protoc	Leng	Info
47	13.184243208	192.168.50.100	192.168.50.101	TCP	60	61560 → 80 [SYN] Seq=0 Win=1924 Len=0 MSS=1460
61	13.185083946	192.168.50.101	192.168.50.100	TCP	62	80 → 61560 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
65	13.184967786	192.168.50.100	192.168.50.101	TCP	56	61560 → 80 [RST] Seq=1 Win=0 Len=0
2853	13.362529076	192.168.50.100	192.168.50.101	TCP	76	35602 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1896695653 TSecr=0 WS=128
2854	13.362927139	192.168.50.100	192.168.50.101	TCP	76	80 → 35602 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=1896695653 TSecr=1896695653 WS=64
2855	13.363294367	192.168.50.100	192.168.50.101	TCP	68	35602 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1896695654 TSecr=468282
2134	16.554051029	192.168.50.101	192.168.50.100	TCP	76	[TCP Retransmission] 80 → 35602 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=468802 TSecr=1896695654 WS=64
2135	16.554675532	192.168.50.100	192.168.50.101	TCP	68	[TCP Dup ACK 2855#1] 35602 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1896698845 TSecr=468282
2146	19.381475206	192.168.50.100	192.168.50.101	HTTP	80	GET / HTTP/1.0
2148	19.382396256	192.168.50.100	192.168.50.101	TCP	68	80 → 35602 [ACK] Seq=1 Ack=19 Win=5824 Len=0 TSval=468884 TSecr=1896781672
2244	19.440623119	192.168.50.100	192.168.50.101	HTTP	11	HTTP/1.1 200 OK (text/html)
2245	19.440633015	192.168.50.100	192.168.50.101	TCP	68	35602 → 80 [ACK] Seq=19 Ack=1087 Win=64128 Len=0 TSval=1896781731 TSecr=468890
2246	19.441397518	192.168.50.100	192.168.50.100	TCP	68	80 → 35602 [FIN, ACK] Seq=1087 Ack=19 Win=5824 Len=0 TSval=468890 TSecr=1896781731
2251	19.444781024	192.168.50.100	192.168.50.101	TCP	68	35602 → 80 [FIN, ACK] Seq=19 Ack=1088 Win=64128 Len=0 TSval=1896781735 TSecr=468890
2253	19.445379903	192.168.50.100	192.168.50.100	TCP	68	80 → 35602 [ACK] Seq=1088 Ack=20 Win=5824 Len=0 TSval=468891 TSecr=1896781735
2613	50.834349046	192.168.50.100	192.168.50.101	TCP	76	48680 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1896733125 TSecr=0 WS=128
2614	50.835317323	192.168.50.100	192.168.50.101	TCP	76	80 → 48680 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=472831 TSecr=1896733125 WS=64
2615	50.835461075	192.168.50.100	192.168.50.101	TCP	68	48680 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1896733126 TSecr=472831
2616	50.837111729	192.168.50.100	192.168.50.101	TCP	76	48680 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1896733128 TSecr=0 WS=128
2617	50.837895744	192.168.50.100	192.168.50.100	TCP	76	80 → 48680 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=472832 TSecr=1896733128 WS=64
2618	50.837910810	192.168.50.100	192.168.50.101	TCP	68	48680 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1896733129 TSecr=472832
2619	50.839754518	192.168.50.100	192.168.50.101	TCP	76	48692 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1896733130 TSecr=0 WS=128
2620	50.840581718	192.168.50.100	192.168.50.100	TCP	76	80 → 48692 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=472832 TSecr=1896733130 WS=64
2621	50.840519717	192.168.50.100	192.168.50.101	TCP	68	48692 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1896733131 TSecr=472832
2625	50.843355055	192.168.50.100	192.168.50.101	TCP	76	48696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1896733134 TSecr=0 WS=128
2626	50.844128573	192.168.50.100	192.168.50.100	TCP	76	80 → 48696 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=472832 TSecr=1896733134 WS=64

in totale c'è stato un traffico di circa 4600 pacchetti, e qui sopra c'è la cattura della porta 80. Con lo scan all possiamo vedere molte più informazioni rispetto agli altri due tipi di scan.

La differenza tra TCP(-sT>Scan TCP) e SYN(-sS>Scan Stealth) é che il TCP completa il 3 way handshake mentre SYN non lo completa ed é meno rilevabile rispetto al TCP scan.

Questo lo possiamo notare già dagli screen in alto con la sequenza dei pacchetti.