

In questo esercizio si sono provati dei comandi nmap pingando la macchina metasploitable e tramite wireshark si sono visti quanti pacchetti passano nella comunicazione con le porte attive

-sS: detto anche SYN, una volta ricevuto il pacchetto SYN/ACK dalla macchina target, non conclude il three-way-handshake, ma appurato che la porta è aperta chiude la comunicazione, di fatto evitando overload dato dalla creazione del canale.

```
(kali@kali)-[~]
$ sudo nmap -sS 1-1023 192.168.32.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 13:43 EST
Failed to resolve "1-1023".
Nmap scan report for 192.168.32.101 (192.168.32.101)
Host is up (0.00074s 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: 08:00:27:8A:D4:02 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 7.86 seconds
```

Comment: Enter a comment for the filter button

No.	Time	Source	Destination	Protocol	Length	Info
2031	53.996981733	192.168.32.100	192.168.32.101	TCP	58	46382 → 1782 [SYN] Seq=0 Win=102
2032	53.997370890	192.168.32.101	192.168.32.100	TCP	60	1782 → 46382 [RST, ACK] Seq=1 Ac
2033	53.997440907	192.168.32.100	192.168.32.101	TCP	58	46382 → 7201 [SYN] Seq=0 Win=102
2034	53.997694373	192.168.32.100	192.168.32.101	TCP	58	46382 → 6969 [SYN] Seq=0 Win=102
2035	53.997892070	192.168.32.101	192.168.32.100	TCP	60	7201 → 46382 [RST, ACK] Seq=1 Ac
2036	53.997892159	192.168.32.101	192.168.32.100	TCP	60	6969 → 46382 [RST, ACK] Seq=1 Ac
2037	53.998190710	192.168.32.100	192.168.32.101	TCP	58	46382 → 1110 [SYN] Seq=0 Win=102
2038	53.998410462	192.168.32.100	192.168.32.101	TCP	58	46382 → 19283 [SYN] Seq=0 Win=10
2039	53.998627596	192.168.32.100	192.168.32.101	TCP	58	46382 → 1059 [SYN] Seq=0 Win=102
2040	53.998823080	192.168.32.101	192.168.32.100	TCP	60	1110 → 46382 [RST, ACK] Seq=1 Ac
2041	53.998823159	192.168.32.101	192.168.32.100	TCP	60	19283 → 46382 [RST, ACK] Seq=1 A
2042	53.998890187	192.168.32.100	192.168.32.101	TCP	58	46382 → 2190 [SYN] Seq=0 Win=102
2043	53.999070634	192.168.32.101	192.168.32.100	TCP	60	1059 → 46382 [RST, ACK] Seq=1 Ac
2044	53.999333126	192.168.32.101	192.168.32.100	TCP	60	2190 → 46382 [RST, ACK] Seq=1 Ac
2045	53.999398352	192.168.32.100	192.168.32.101	TCP	58	46382 → 5902 [SYN] Seq=0 Win=102
2046	53.999615576	192.168.32.100	192.168.32.101	TCP	58	46382 → 3404 [SYN] Seq=0 Win=102
2047	53.999833007	192.168.32.100	192.168.32.101	TCP	58	46382 → 9500 [SYN] Seq=0 Win=102
2048	54.000047873	192.168.32.100	192.168.32.101	TCP	58	46382 → 1082 [SYN] Seq=0 Win=102
2049	54.000230424	192.168.32.101	192.168.32.100	TCP	60	5902 → 46382 [RST, ACK] Seq=1 Ac
2050	54.000431255	192.168.32.101	192.168.32.100	TCP	60	3404 → 46382 [RST, ACK] Seq=1 Ac

▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured

▶ Ethernet II, Src: zte_ba:3e:d8 (a4:f3:3b:ba:3e:d8), Dst:

▶ Address Resolution Protocol (request)

0000

ff ff ff ff ff ff a4 f3 3b ba 3e d8 08 06 00 01

0010

08 00 06 04 00 01 a4 f3 3b ba 3e d8 c0 a8 01 fe

0020

00 00 00 00 00 00 c0 a8 01 34 00 00 00 00 00 00

0030

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

-A: ci permette di recuperare molte informazioni utili sull'ip target, come versione del sistema operativo e dei servizi disponibili in ascolto sulle porte aperte:

```
(kali@kali)~$ sudo nmap -A -p 20-1024 192.168.32.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 13:54 EST
Nmap scan report for 192.168.32.101 (192.168.32.101)
Host is up (0.0025s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_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
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_server_header: Apache/2.2.8 (Ubuntu) DAV/2
|_http_title: Metasploitable2 - Linux
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 57467/udp mountd
|_100005 1,2,3 59389/tcp mountd
|_100031 1,2,3 57721/udp clockd
```

ip.addr == 192.168.32.101

Filter Buttons Preferences... Label: Enter a description for the filter button Filter: 192.168.32.101

Comment: Enter a comment for the filter button

OK Cancel

No.	Time	Source	Destination	Protocol	Length	Info
3504	77.979490884	192.168.32.101	192.168.32.100	FTP	104	Response: 530 Please login with
3505	77.979941915	192.168.32.100	192.168.32.101	TCP	66	51882 → 21 [ACK] Seq=93 Ack=21 W
3506	77.980106865	192.168.32.100	192.168.32.101	TCP	66	51882 → 21 [ACK] Seq=93 Ack=97 W
3507	77.983307133	192.168.32.100	192.168.32.101	TCP	66	51868 → 21 [RST, ACK] Seq=518 Ac
3508	77.984365072	192.168.32.100	192.168.32.101	TCP	66	51882 → 21 [FIN, ACK] Seq=93 Ack
3509	77.985186719	192.168.32.101	192.168.32.100	FTP	76	Response: 500 OOPS:
3510	77.985187009	192.168.32.101	192.168.32.100	FTP	96	Response: vsf_sysutil_recv_peek:
3511	77.985210193	192.168.32.100	192.168.32.101	TCP	54	51882 → 21 [RST] Seq=94 Win=0 Le
3512	77.985297797	192.168.32.100	192.168.32.101	TCP	54	51882 → 21 [RST] Seq=94 Win=0 Le
3513	77.985880301	192.168.32.101	192.168.32.100	FTP	68	Response:
3514	77.985899303	192.168.32.100	192.168.32.101	TCP	54	51882 → 21 [RST] Seq=94 Win=0 Le
3515	78.649806482	192.168.1.52	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
3516	79.530958428	zte_ba:3e:d8	Broadcast	ARP	60	Who has 192.168.1.52? Tell 192.1
3517	79.652816863	192.168.1.52	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
3518	80.651204789	192.168.1.52	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
3519	84.641061498	192.168.1.54	255.255.255.255	TPLINK...	100	UDP Cmd: {"system":{"get_sysinfo
3520	87.151792966	192.168.1.50	224.0.0.251	MDNS	119	Standard query 0x0006 PTR _23363
3521	91.271950192	192.168.1.50	224.0.0.22	IGMPv3	60	Membership Report / Leave group
3522	91.578579256	192.168.1.50	224.0.0.22	IGMPv3	60	Membership Report / Leave group

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured

Ethernet II, Src: PCSystemtec_21:b1:d0 (08:00:27:21:b1:

Address Resolution Protocol (request)

0000

ff ff ff ff ff ff 08 00

27 21 b1 d0 08 06 00 01

0010

08 00 06 04 00 01 08 00

27 21 b1 d0 c0 a8 20 64

0020

00 00 00 00 00 00 c0 a8

20 65

-sT: è un metodo di scansione che controlla se una porta è aperta o meno e recuperare informazioni sul servizio in ascolto, nmap completa tutti i passaggi del 3-way-handshake, stabilendo di fatto un canale.

```
Nmap done: 1 IP address (1 host up) scanned in 103.80 seconds

(kali@kali)-[~]
└─$ sudo nmap -sT 192.168.32.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 14:18 EST
Nmap scan report for 192.168.32.101 (192.168.32.101)
Host is up (0.0056s 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  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: 08:00:27:8A:D4:02 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
```

No.	Time	Source	Destination	Protocol	Length	Info
2045	1.373736660	192.168.32.100	192.168.32.101	TCP	74	56878 → 31337 [SYN] Seq=0 Win=32
2046	1.373906756	192.168.32.100	192.168.32.101	TCP	74	35010 → 10180 [SYN] Seq=0 Win=32
2047	1.374050708	192.168.32.101	192.168.32.100	TCP	60	563 → 57390 [RST, ACK] Seq=1 Ack=
2048	1.374269543	192.168.32.101	192.168.32.100	TCP	60	6156 → 54650 [RST, ACK] Seq=1 Ac
2049	1.374535958	192.168.32.101	192.168.32.100	TCP	60	31337 → 56878 [RST, ACK] Seq=1 A
2050	1.374536017	192.168.32.101	192.168.32.100	TCP	60	10180 → 35010 [RST, ACK] Seq=1 A
2051	1.375077739	192.168.32.100	192.168.32.101	TCP	74	41720 → 3011 [SYN] Seq=0 Win=321
2052	1.376284820	192.168.32.101	192.168.32.100	TCP	60	3011 → 41720 [RST, ACK] Seq=1 Ac
2053	1.377222761	192.168.32.100	192.168.32.101	TCP	74	34270 → 49161 [SYN] Seq=0 Win=32
2054	1.379354351	192.168.32.101	192.168.32.100	TCP	60	49161 → 34270 [RST, ACK] Seq=1 A
2055	1.651922017	PCSSystemtec_8a:d4:...	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.1
2056	2.541723444	PCSSystemtec_8a:d4:...	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.1
2057	4.544418739	PCSSystemtec_8a:d4:...	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.1
2058	5.082760963	fe80::1	fe80::a00:27ff:fe21...	ICMPv6	86	Neighbor Solicitation for fe80::
2059	5.082825573	fe80::a00:27ff:fe21...	fe80::1	ICMPv6	78	Neighbor Advertisement fe80::a00
2060	5.313211155	fe80::a00:27ff:fe21...	fe80::1	ICMPv6	86	Neighbor Solicitation for fe80::
2061	5.315572710	fe80::1	fe80::a00:27ff:fe21...	ICMPv6	78	Neighbor Advertisement fe80::1 (
2062	5.553006327	PCSSystemtec_8a:d4:...	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.1
2063	6.541322671	PCSSystemtec_8a:d4:...	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.1

▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured

▶ Ethernet II, Src: PCSSystemtec_21:b1:d0 (08:00:27:21:b1

▶ Address Resolution Protocol (request)

0000

ff ff ff ff ff ff 08 00

27 21 b1 d0 08 06 00 00

0010

08 00 06 04 00 01 08 00

27 21 b1 d0 c0 a8 20 64

0020

00 00 00 00 00 00 c0 a8

20 65

-p- --system-dns

```
(kali@kali)-[~]
└─$ sudo nmap -p- --system-dns 192.168.32.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 13:59 EST
Nmap scan report for 192.168.32.101 (192.168.32.101)
Host is up (0.00100s latency).
Not shown: 65505 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
8779/tcp  open  unknown
42582/tcp open  unknown
55064/tcp open  unknown
59389/tcp open  unknown
MAC Address: 08:00:27:8A:D4:02 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 103.80 seconds
```

Filter Buttons Preferences... Label: Enter a description for the filter button Filter: 192.168.32.101

Comment: Enter a comment for the filter button

No.	Time	Source	Destination	Protocol	Length	Info
1311	103.569202626	192.168.32.101	192.168.32.100	TCP	60	35229 → 50682 [RST, ACK] Seq=1 Ack=1
1311	103.569202901	192.168.32.101	192.168.32.100	TCP	60	9331 → 50682 [RST, ACK] Seq=1 Ack=1
1311	103.569202943	192.168.32.101	192.168.32.100	TCP	60	14560 → 50682 [RST, ACK] Seq=1 Ack=1
1311	103.569665790	192.168.32.100	192.168.32.101	TCP	58	50682 → 60940 [SYN] Seq=0 Win=1024
1311	103.570457413	192.168.32.101	192.168.32.100	TCP	60	60940 → 50682 [RST, ACK] Seq=1 Ack=1
1311	103.893858649	192.168.1.54	255.255.255.255	TPLINK...	100	UDP Cmd: {"system":{"get_sysinfo":{}}
1311	104.949558797	PCSSystemtec_21:b1...	PCSSystemtec_8a:d4...	ARP	42	Who has 192.168.32.101? Tell 192.168.
1311	104.951244803	PCSSystemtec_8a:d4...	PCSSystemtec_21:b1...	ARP	60	192.168.32.101 is at 08:00:27:8a:d4:0
1311	108.757892796	192.168.1.52	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1311	109.770142461	192.168.1.52	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1311	110.758069439	192.168.1.52	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1311	111.758463934	192.168.1.52	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1311	113.771021168	LGInnotek_61:09:a2	Broadcast	ARP	60	Who has 192.168.1.52? Tell 192.168.1
1311	121.879798586	192.168.1.50	224.0.0.251	MDNS	119	Standard query 0x0005 PTR _233637DE.
1311	128.907478515	192.168.1.54	255.255.255.255	TPLINK...	100	UDP Cmd: {"system":{"get_sysinfo":{}}
1311	131.540983948	192.168.1.52	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
1311	132.539589395	192.168.1.52	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
1311	133.697509173	192.168.1.52	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
1311	134.536159772	192.168.1.52	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured

Ethernet II, Src: PCSSystemtec_21:b1:d0 (08:00:27:21:b1

Address Resolution Protocol (request)

0000 ff ff ff ff ff 08 00 27 21 b1 d0 08 06 00 01

0010 08 00 06 04 00 01 08 00 27 21 b1 d0 c0 a8 20 64

0020 00 00 00 00 00 00 c0 a8 20 65