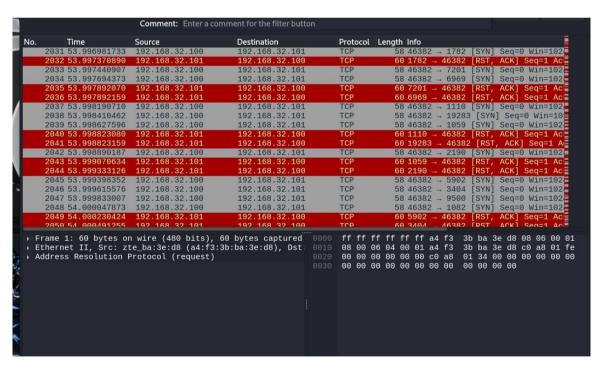In questo esercizio si sono provati dei comandi nmap pingando la macchina metasploitable e tramite wireshark si sono visti quanti pacchetti passano nella comunicazione con le porte attive

-sS:

```
┌──(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
```

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	54.000491255	192.168.32.101	192.168.32.100	TCP	60	3404 → 46382 [RST, ACK] Seq=1 A

```
Comment: Enter a comment for the filter button
```

```
▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured   0000  ff ff ff ff ff ff a4 f3  3b ba 3e d8 08 06 00 01
▶ Ethernet II, Src: zte_ba:3e:d8 (a4:f3:3b:ba:3e:d8), Dst   0010  08 00 06 04 00 01 a4 f3  3b ba 3e d8 c0 a8 01 fe
▶ Address Resolution Protocol (request)                     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
```

-A

-p- --system-dns:

-sT:

```
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	192.168.32.101	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    0000  ff ff ff ff ff ff 08 00  27 21 b1 d0 08 06 00 01
▶ Ethernet II, Src: PCSSystemtec_21:b1:d0 (08:00:27:21:b1:   0010  08 00 06 04 00 01 08 00  27 21 b1 d0 c0 a8 20 64
▶ Address Resolution Protocol (request)                       0020  00 00 00 00 00 00 c0 a8  20 65
```