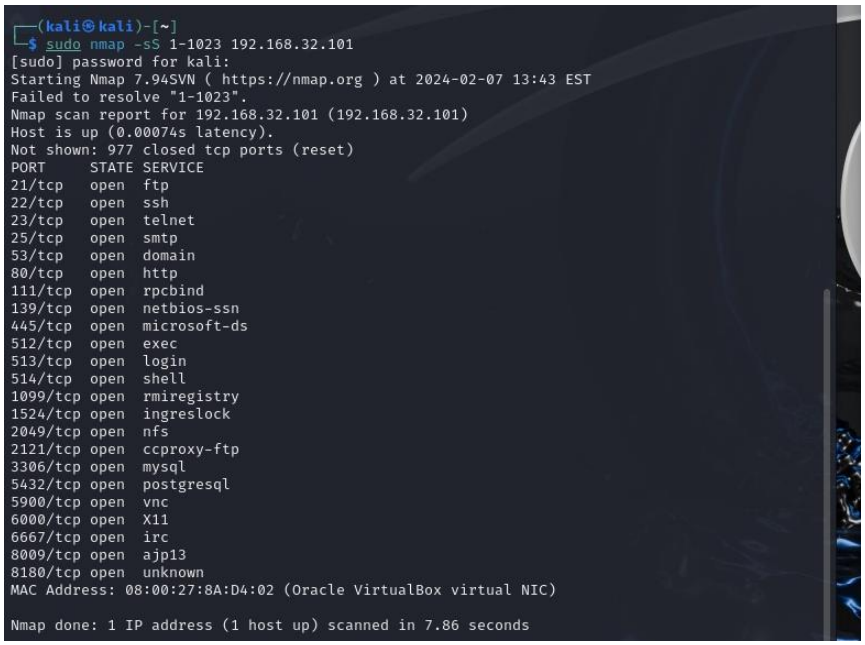
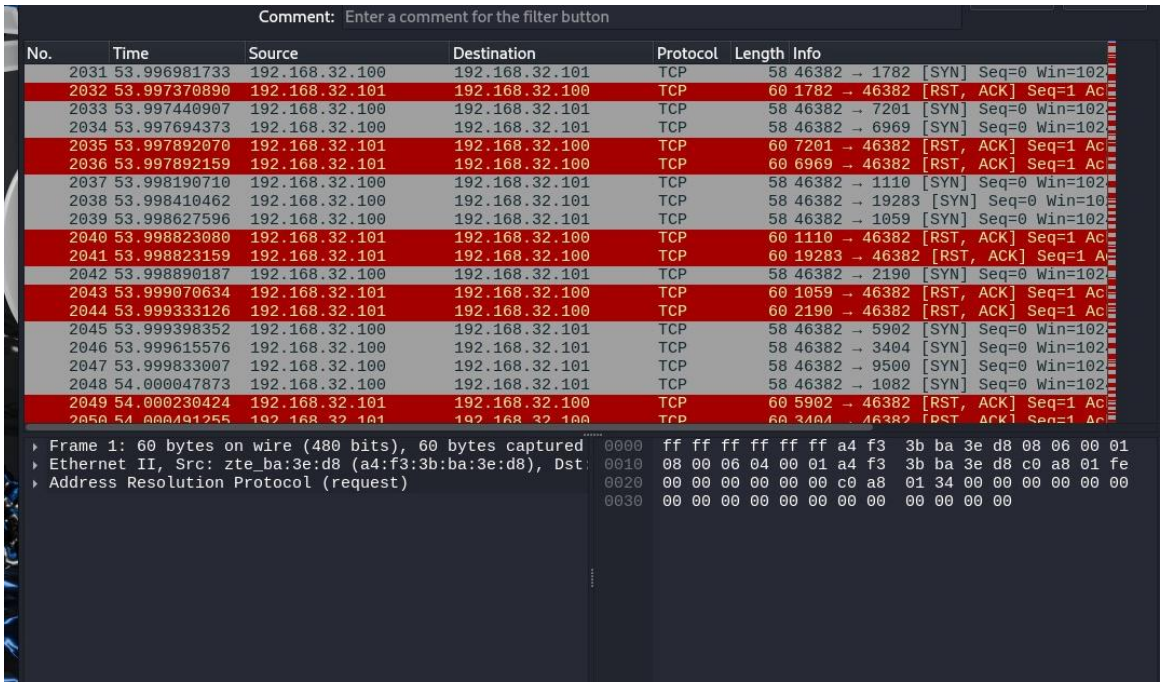
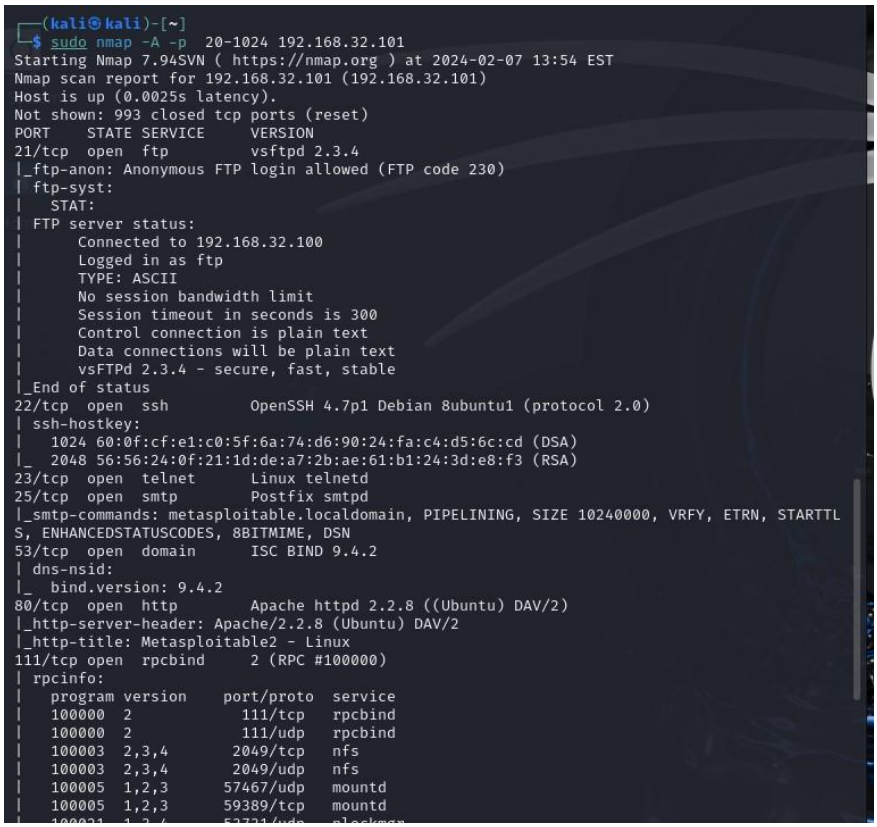
In questo esercizio si sono provati dei comandi nmap pingando la macchina metasploitable e tramite wireshark si sono visti quanti pacchetti passano nella comunicazione con le porte attive

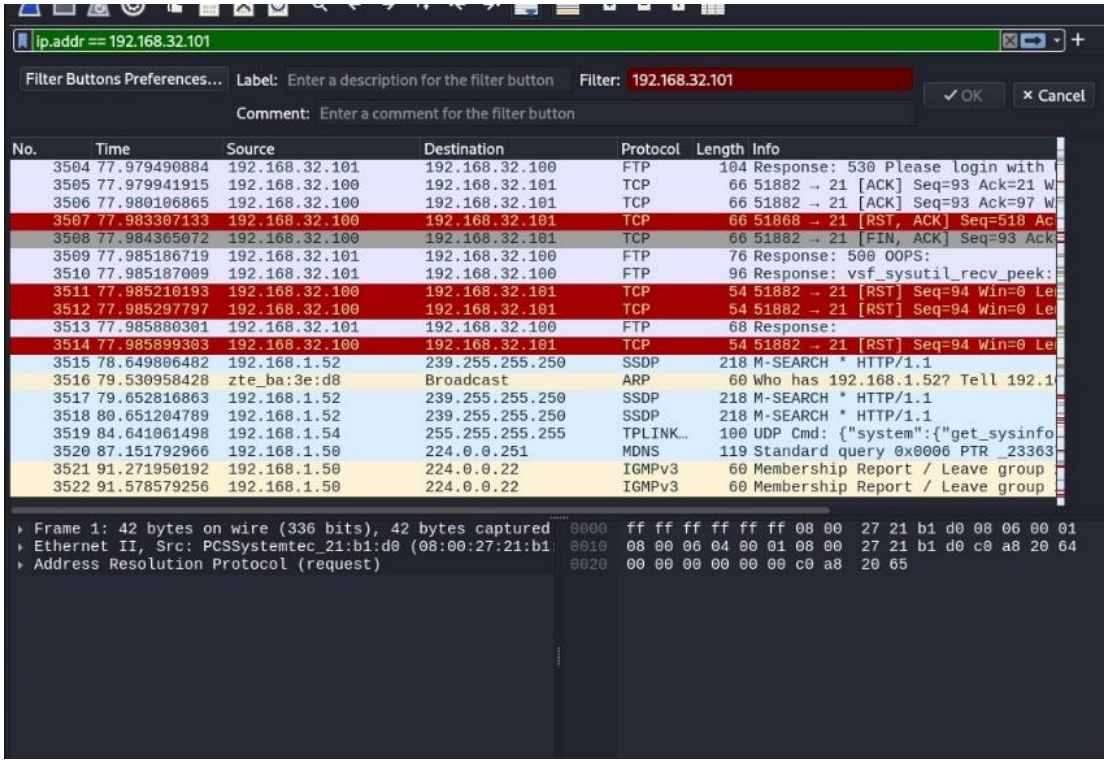
-sS: detto anche SYN, una volta ricevuto il pacchetto SYN/ACK dalla macchina target, non conclude il three-way-handshake, ma appurato che la porta è aperta chiude la comunicazione, di fatto evitando overload dato dalla creazione del canale.



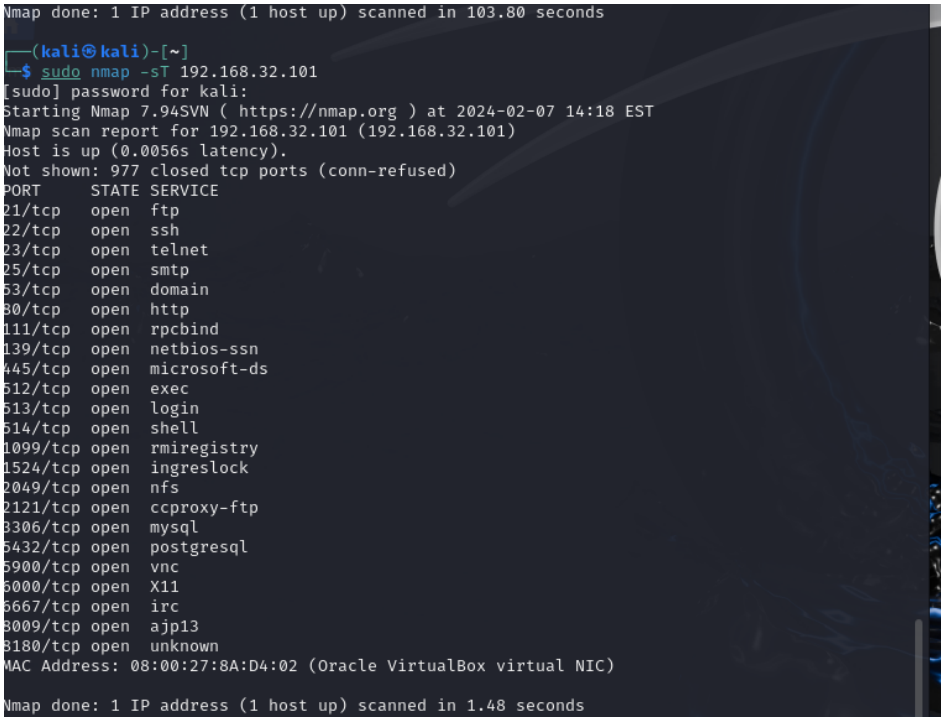


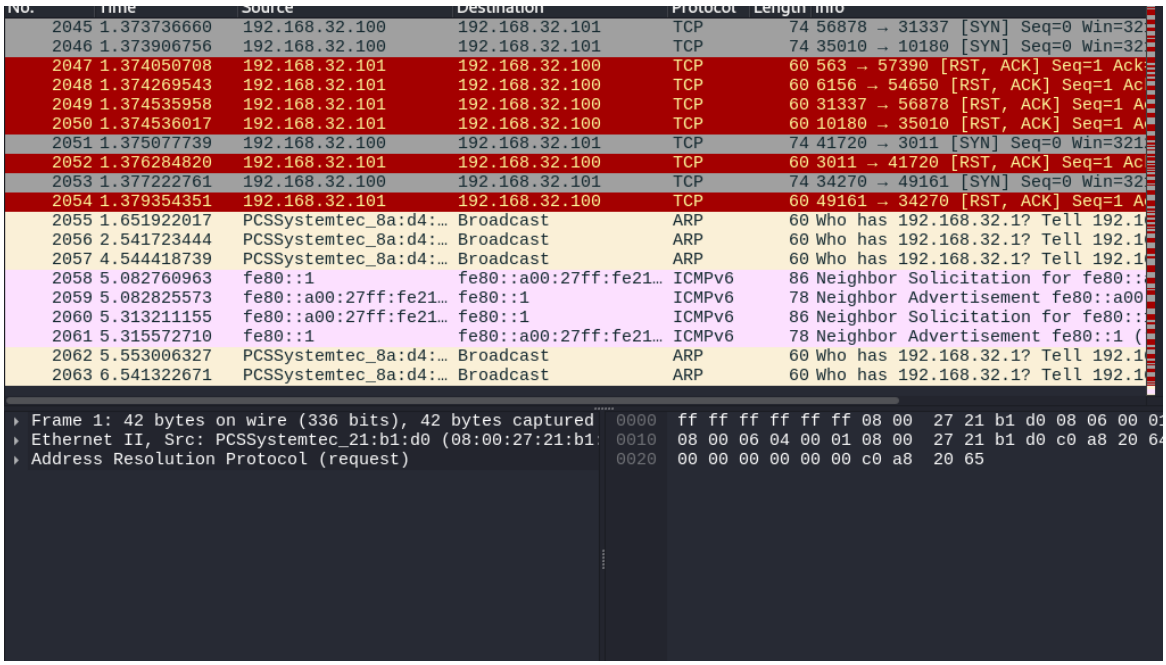
-A: ci permette di recuperare molte informazioni utili sull'ip target, come versione del sistema operativo e dei servizi disponibili in ascolto sulle porte aperte:



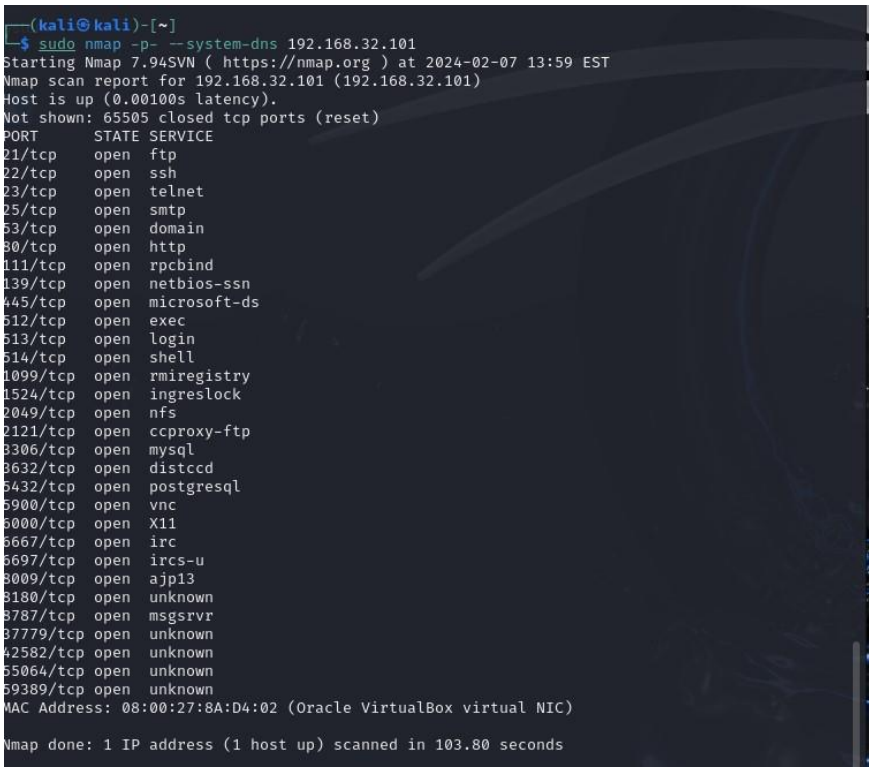


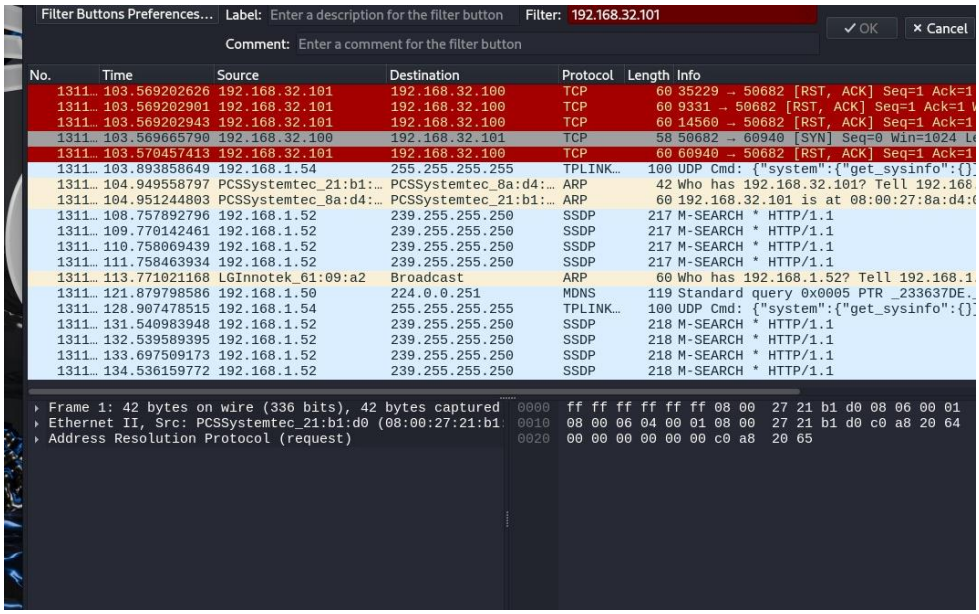
-sT: è un metodo di scansione che controllare se una porta è aperta o meno e recuperare informazioni sul servizio in ascolto, nmap completa tutti i passaggi del 3-way-handshake, stabilendo di fatto un canale.





-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
37779/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
OK
Cancel
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:
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 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