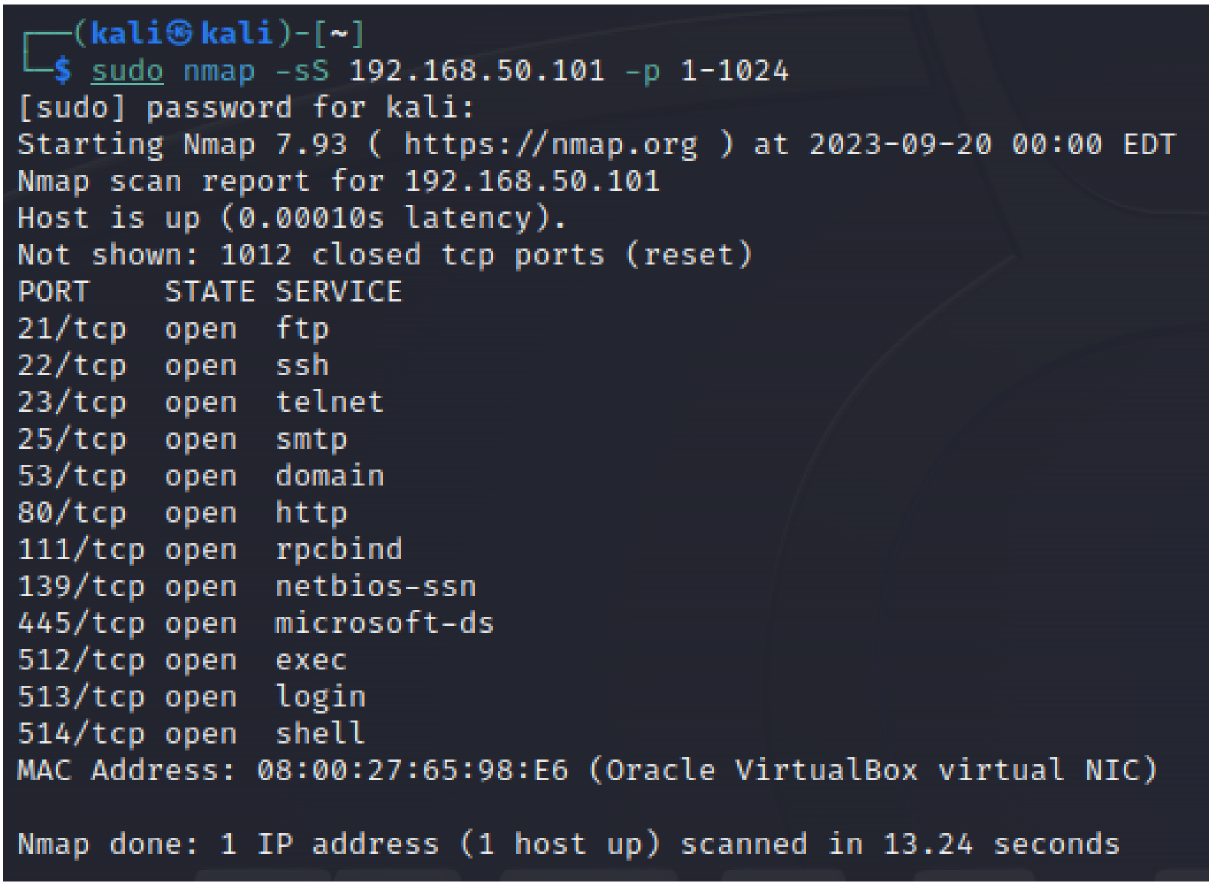
D1 Tools di Kali Linux

Esercizio 1

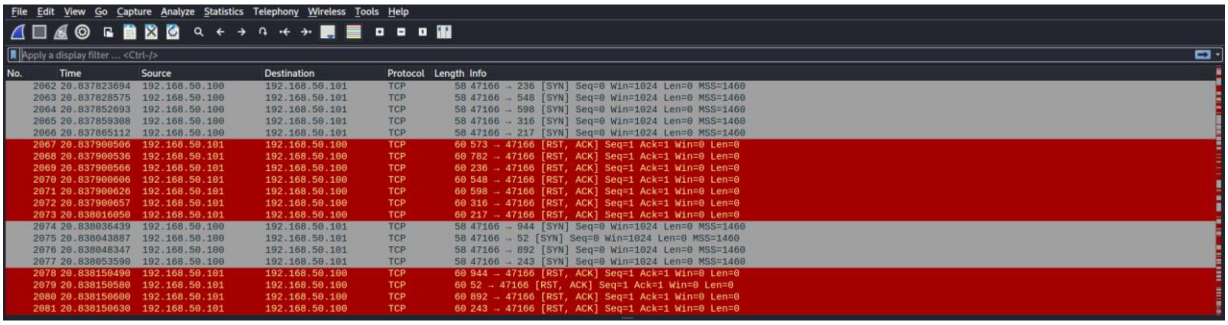


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101 -p 1-1024
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-20 00:00 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00010s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
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: 08:00:27:65:98:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
```

Con questo comando riusciamo a vedere tutti i servizi attivi sulla macchina target (metasploit).

Esercizio 2

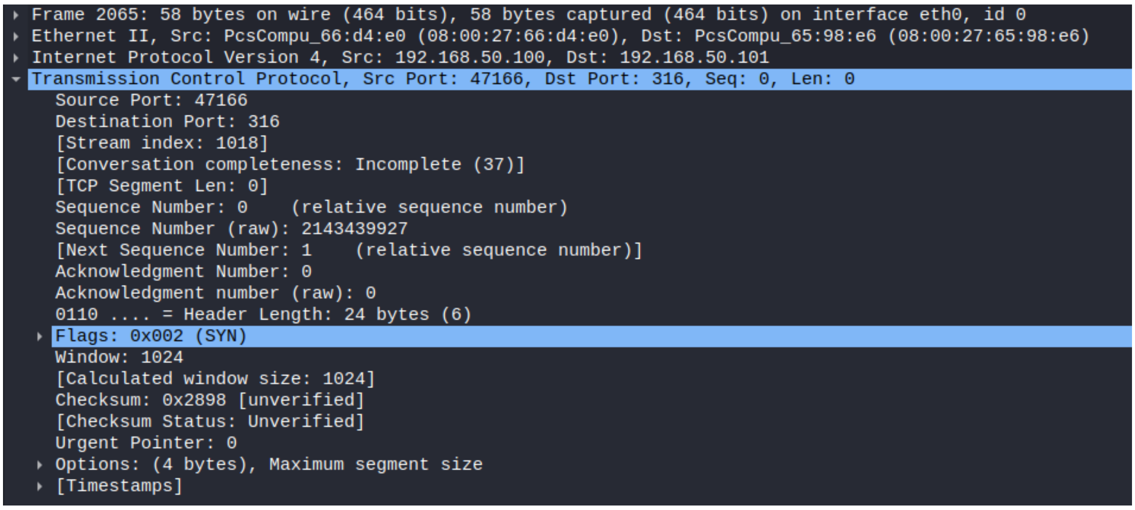


No.	Time	Source	Destination	Protocol	Length	Info
2062	20.837823694	192.168.50.100	192.168.50.101	TCP	58	47166 → 236 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2063	20.837828575	192.168.50.100	192.168.50.101	TCP	58	47166 → 548 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2064	20.837852693	192.168.50.100	192.168.50.101	TCP	58	47166 → 598 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2065	20.837859308	192.168.50.100	192.168.50.101	TCP	58	47166 → 316 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2066	20.837865112	192.168.50.100	192.168.50.101	TCP	58	47166 → 217 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2067	20.837900506	192.168.50.101	192.168.50.100	TCP	60	573 → 47166 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2068	20.837900536	192.168.50.101	192.168.50.100	TCP	60	782 → 47166 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2069	20.837900566	192.168.50.101	192.168.50.100	TCP	60	236 → 47166 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2070	20.837900606	192.168.50.101	192.168.50.100	TCP	60	548 → 47166 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2071	20.837900626	192.168.50.101	192.168.50.100	TCP	60	598 → 47166 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2072	20.837900657	192.168.50.101	192.168.50.100	TCP	60	316 → 47166 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2073	20.838016050	192.168.50.101	192.168.50.100	TCP	60	217 → 47166 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2074	20.838036439	192.168.50.100	192.168.50.101	TCP	58	47166 → 944 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2075	20.838043887	192.168.50.100	192.168.50.101	TCP	58	47166 → 52 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2076	20.838048347	192.168.50.100	192.168.50.101	TCP	58	47166 → 892 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2077	20.838053590	192.168.50.100	192.168.50.101	TCP	58	47166 → 243 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2078	20.838150490	192.168.50.101	192.168.50.100	TCP	60	944 → 47166 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2079	20.838150580	192.168.50.101	192.168.50.100	TCP	60	52 → 47166 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2080	20.838150600	192.168.50.101	192.168.50.100	TCP	60	892 → 47166 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2081	20.838150630	192.168.50.101	192.168.50.100	TCP	60	243 → 47166 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Con lo stesso comando usato in precedenza possiamo vedere tramite la cattura di wireshark che le richieste che inviamo non vengono concluse ma viene inviato solo il SYN dove la porta è aperta ed i servizi sono attivi.

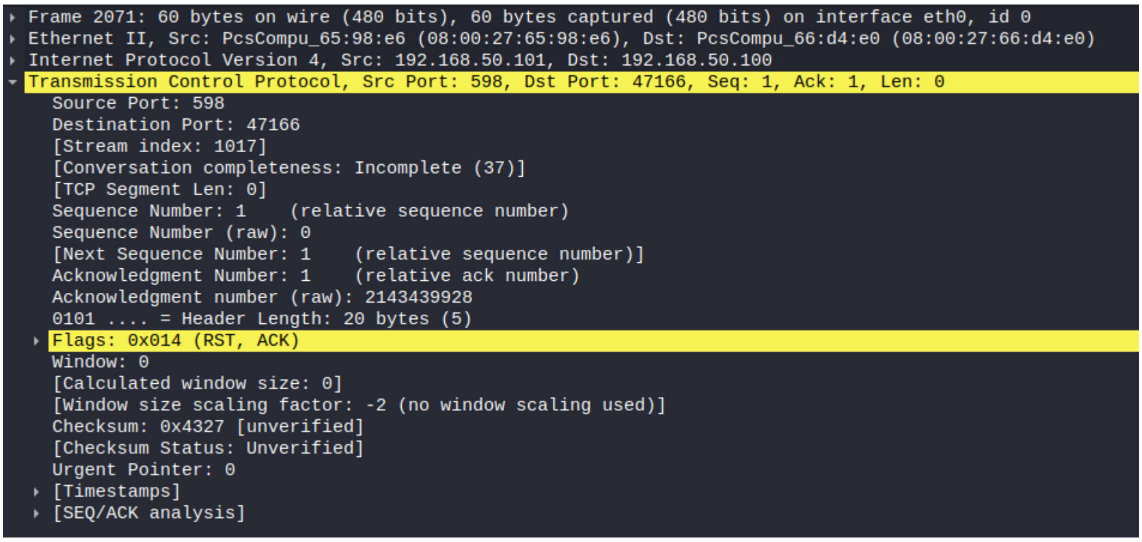
dove invece le richieste trovano la porta chiusa o senza servizi attivi la macchina target risponde inviando un RST, ACK.

Porta aperta con servizio attivo:



```
▸ Frame 2065: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_66:d4:e0 (08:00:27:66:d4:e0), Dst: PcsCompu_65:98:e6 (08:00:27:65:98:e6)
▸ Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101
▾ Transmission Control Protocol, Src Port: 47166, Dst Port: 316, Seq: 0, Len: 0
    Source Port: 47166
    Destination Port: 316
    [Stream index: 1018]
    [Conversation completeness: Incomplete (37)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2143439927
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0110 .... = Header Length: 24 bytes (6)
  ▸ Flags: 0x002 (SYN)
    Window: 1024
    [Calculated window size: 1024]
    Checksum: 0x2898 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (4 bytes), Maximum segment size
  ▸ [Timestamps]
```

Porta chiusa senza servizio:



```
▸ Frame 2071: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_65:98:e6 (08:00:27:65:98:e6), Dst: PcsCompu_66:d4:e0 (08:00:27:66:d4:e0)
▸ Internet Protocol Version 4, Src: 192.168.50.101, Dst: 192.168.50.100
▾ Transmission Control Protocol, Src Port: 598, Dst Port: 47166, Seq: 1, Ack: 1, Len: 0
    Source Port: 598
    Destination Port: 47166
    [Stream index: 1017]
    [Conversation completeness: Incomplete (37)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 0
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2143439928
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x014 (RST, ACK)
    Window: 0
    [Calculated window size: 0]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x4327 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
```