# MODULO 3
# NMAP

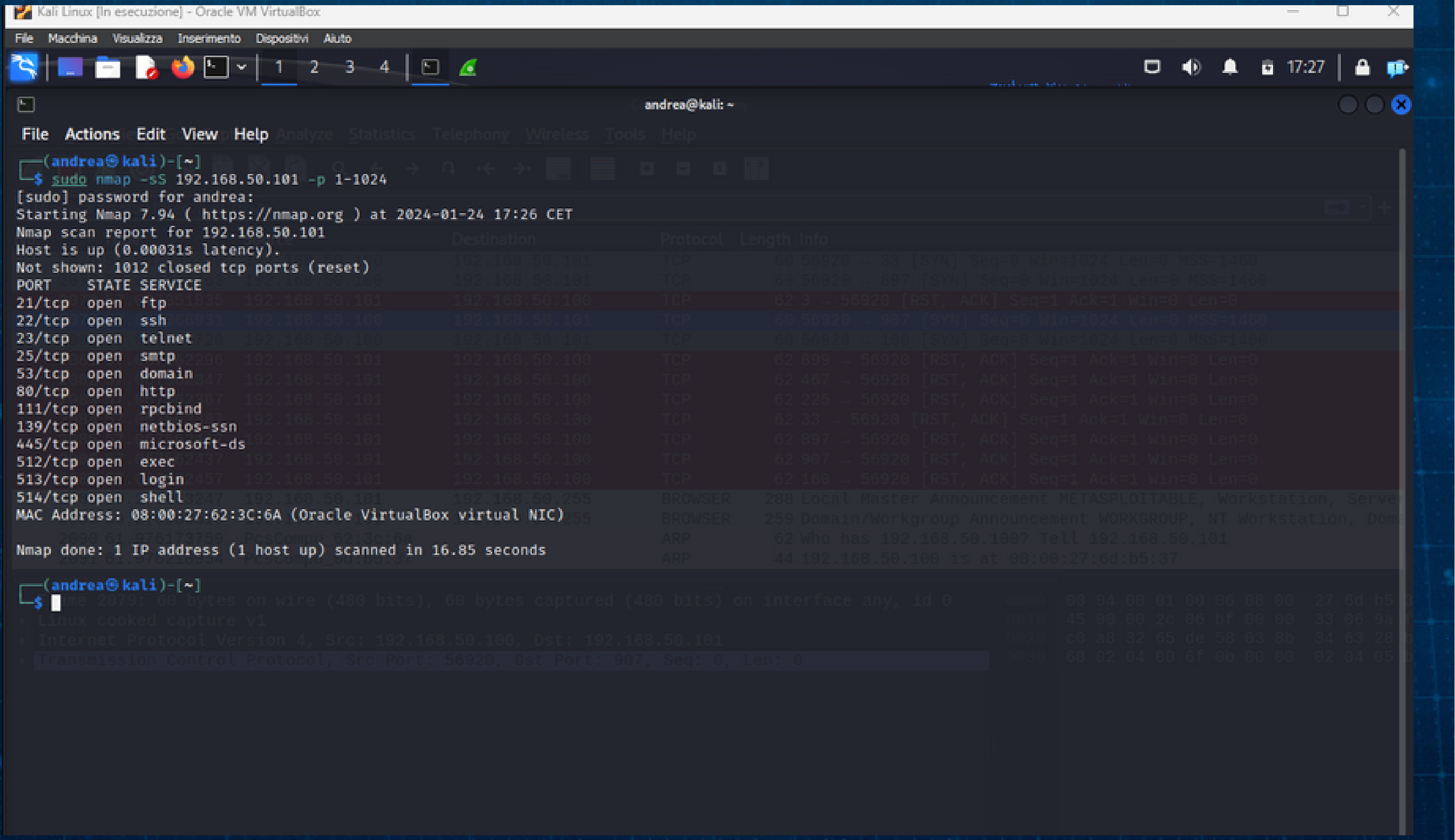
Andrea Ferrantino

**L’esercizio consiste a prendere dimistichezza con i tool nmap effettuando 3 tipi di scansioni (Syn,TCP,-A)  da una macchina (kali linux) a un target (metasploitable).Infine intercetteremo il traffico con wireshark**

# Scansione Syn

Iniziamo lanciamo il comando

- nmap -sS 192.168.50.101 -p 1-1024

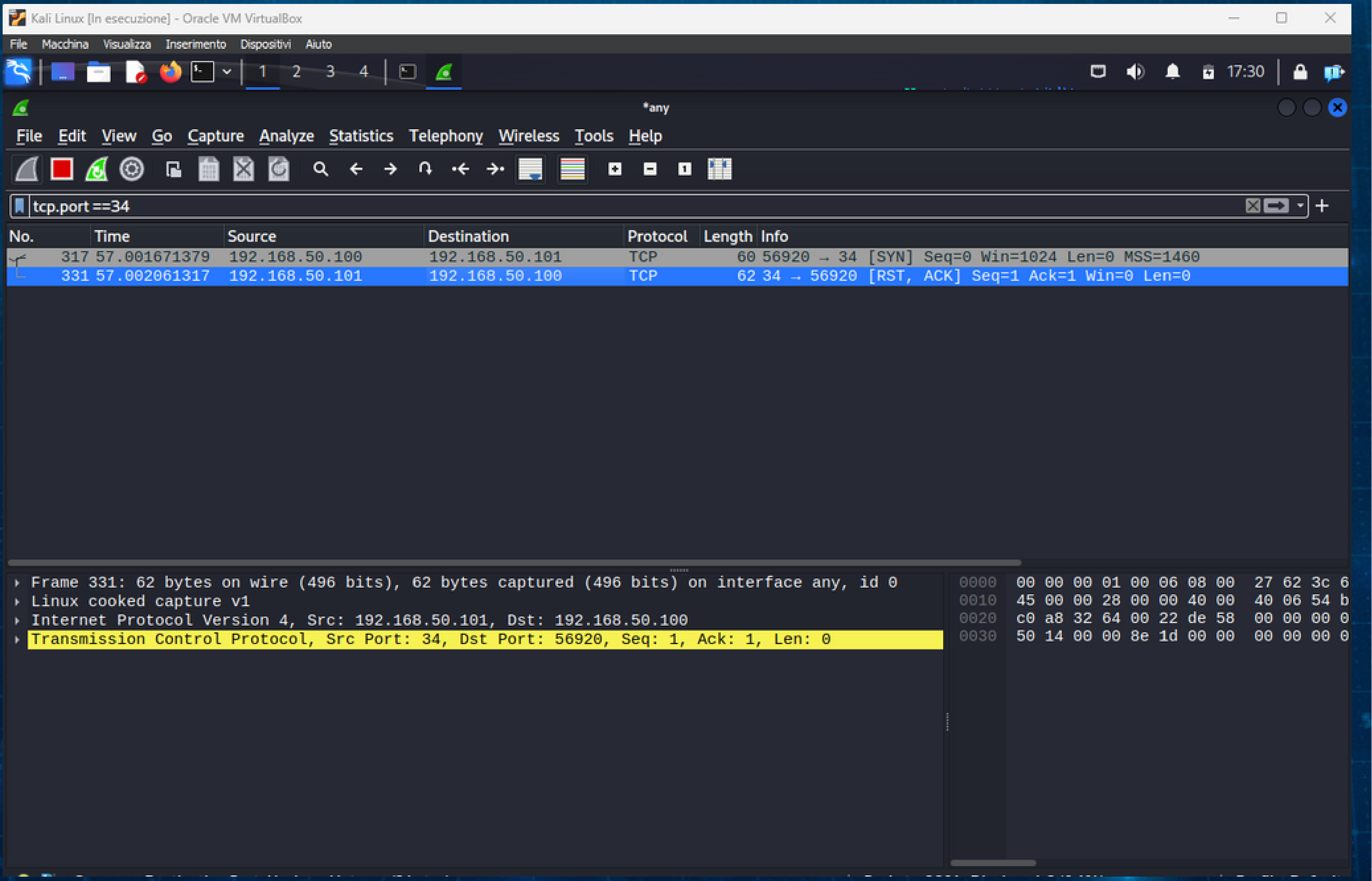

Kali Linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
17:27
andrea@kali: ~
File Actions Edit View Help

```
┌──(andrea㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101 -p 1-1024
[sudo] password for andrea:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-24 17:26 CET
Nmap scan report for 192.168.50.101
Host is up (0.00031s 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: 08:00:27:62:3C:6A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.85 seconds

┌──(andrea㉿kali)-[~]
└─$ 
```

# Usando Wireshark possiamo notare che Mesploitable risponde con un pacchetto Syn/Ack


Kali Linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
17:30
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port ==34

```
No.   Time          Source          Destination     Protocol Length Info
  317 57.001671379  192.168.50.100  192.168.50.101  TCP          60 56920 → 34 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  331 57.002061317  192.168.50.101  192.168.50.100  TCP          62 34 → 56920 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

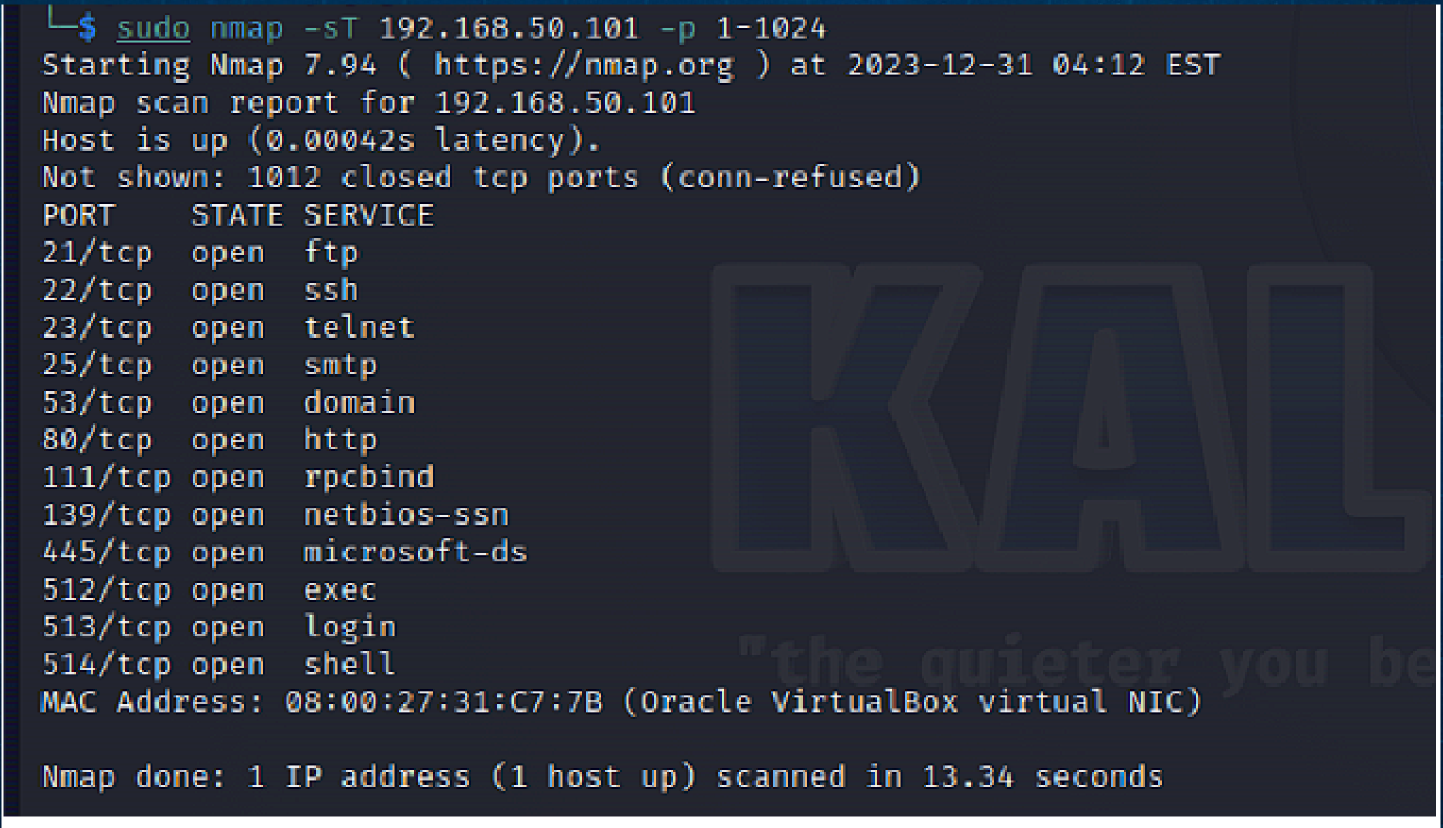
```
▸ Frame 331: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 192.168.50.101, Dst: 192.168.50.100
▸ Transmission Control Protocol, Src Port: 34, Dst Port: 56920, Seq: 1, Ack: 1, Len: 0
```

```
0000  00 00 00 01 00 06 08 00  27 62 3c 6
0010  45 00 00 28 00 00 40 00  40 06 54 b
0020  c0 a8 32 64 00 22 de 58  00 00 00 0
0030  50 14 00 00 8e 1d 00 00  00 00 00 0
```

# Scansione TCP

La scansione -sT stabilisce un canale TCP.E una scansione più invasiva.
Quindi lanciamo il comando:

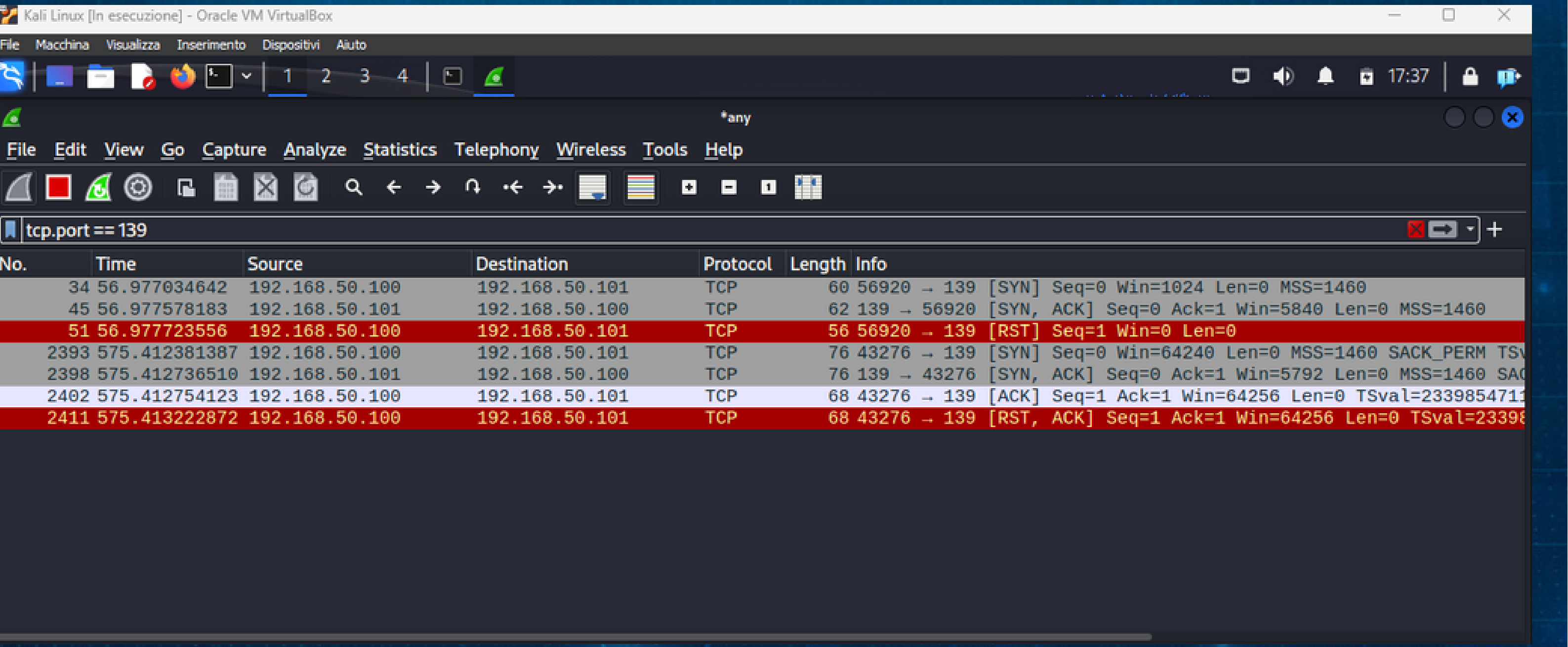
- nmap -sT 192.168.50.101 -p 1-1024



```
└─$ sudo nmap -sT 192.168.50.101 -p 1-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-31 04:12 EST
Nmap scan report for 192.168.50.101
Host is up (0.00042s latency).
Not shown: 1012 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
MAC Address: 08:00:27:31:C7:7B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

Su wireshark possiamo notare che applicando il filtro tcp port 139 avviene la three-way-handshake

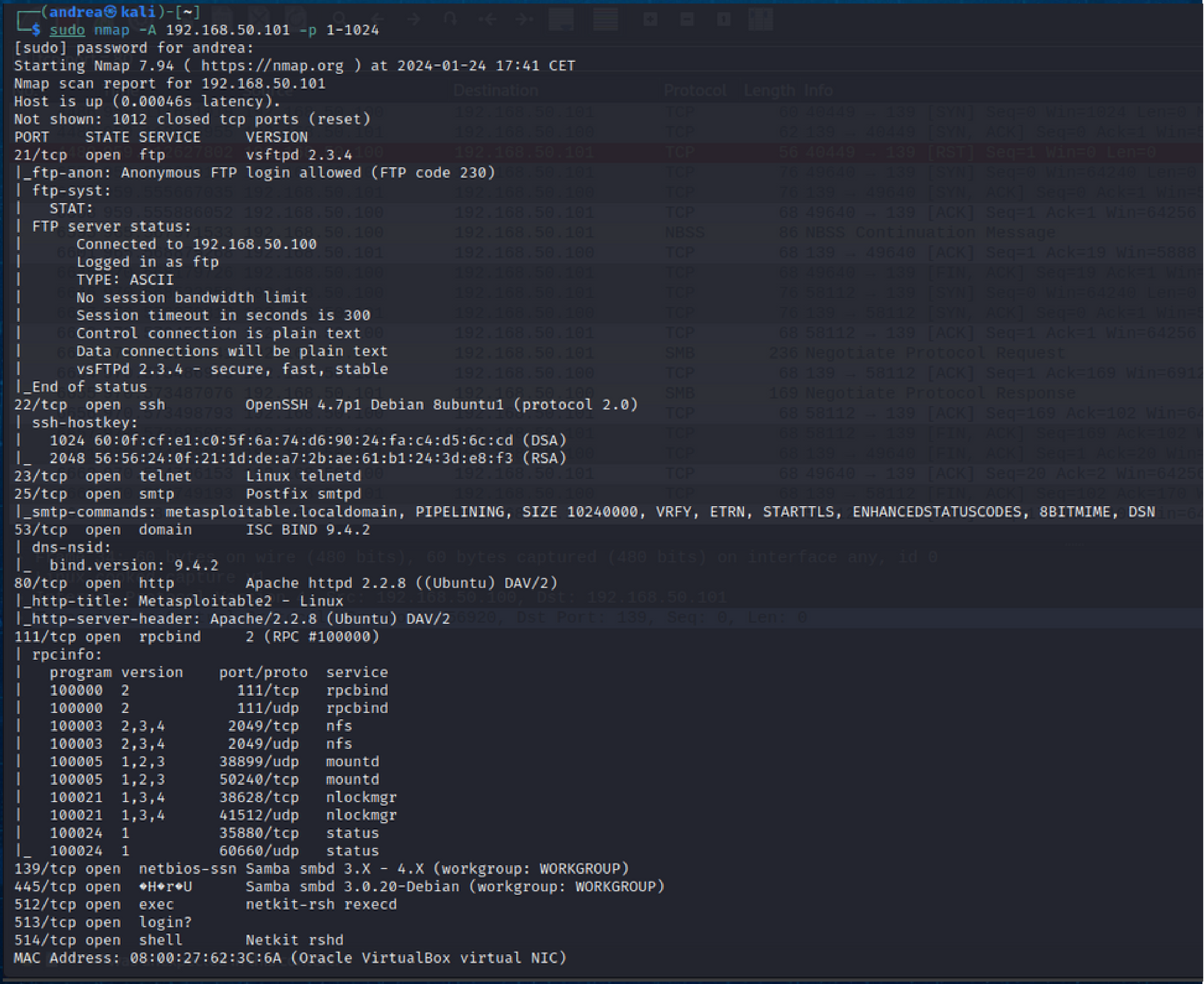

Kali Linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
17:37
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 139

```
No.  Time           Source          Destination     Protocol Length Info
  34 56.977034642   192.168.50.100  192.168.50.101  TCP      60 56920 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  45 56.977578183   192.168.50.101  192.168.50.100  TCP      62 139 → 56920 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
  51 56.977723556   192.168.50.100  192.168.50.101  TCP      56 56920 → 139 [RST] Seq=1 Win=0 Len=0
2393 575.412381387 192.168.50.100  192.168.50.101  TCP      76 43276 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSv
2398 575.412736510 192.168.50.101  192.168.50.100  TCP      76 139 → 43276 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC
2402 575.412754123 192.168.50.100  192.168.50.101  TCP      68 43276 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2339854711
2411 575.413222872 192.168.50.100  192.168.50.101  TCP      68 43276 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=23398
```

# Scansione  -A

Questa è la scansione più rumorosa delle altre ma in compenso ci consente di ottenere molte altre più informazioni sul target



```
┌──(andrea㉿kali)-[~]
└─$ sudo nmap -A 192.168.50.101 -p 1-1024
[sudo] password for andrea:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-24 17:41 CET
Nmap scan report for 192.168.50.101
Host is up (0.00046s latency).
Not shown: 1012 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 192.168.50.100
|      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
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-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      38899/udp   mountd
|   100005  1,2,3      50240/tcp   mountd
|   100021  1,3,4      38628/tcp   nlockmgr
|   100021  1,3,4      41512/udp   nlockmgr
|   100024  1          35880/tcp   status
|_  100024  1          60660/udp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  ♦H♦r♦U      Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:62:3C:6A (Oracle VirtualBox virtual NIC)
```