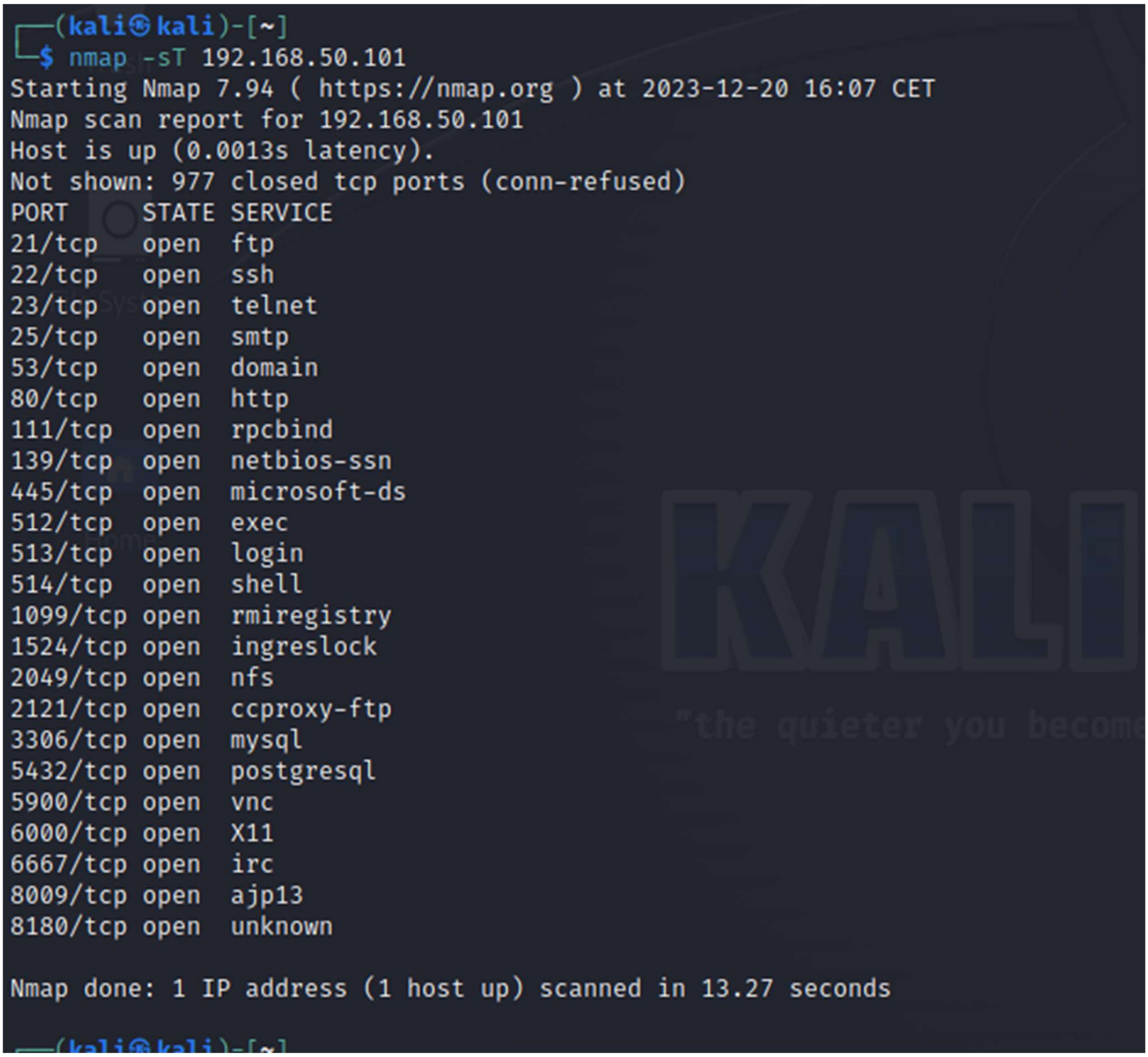
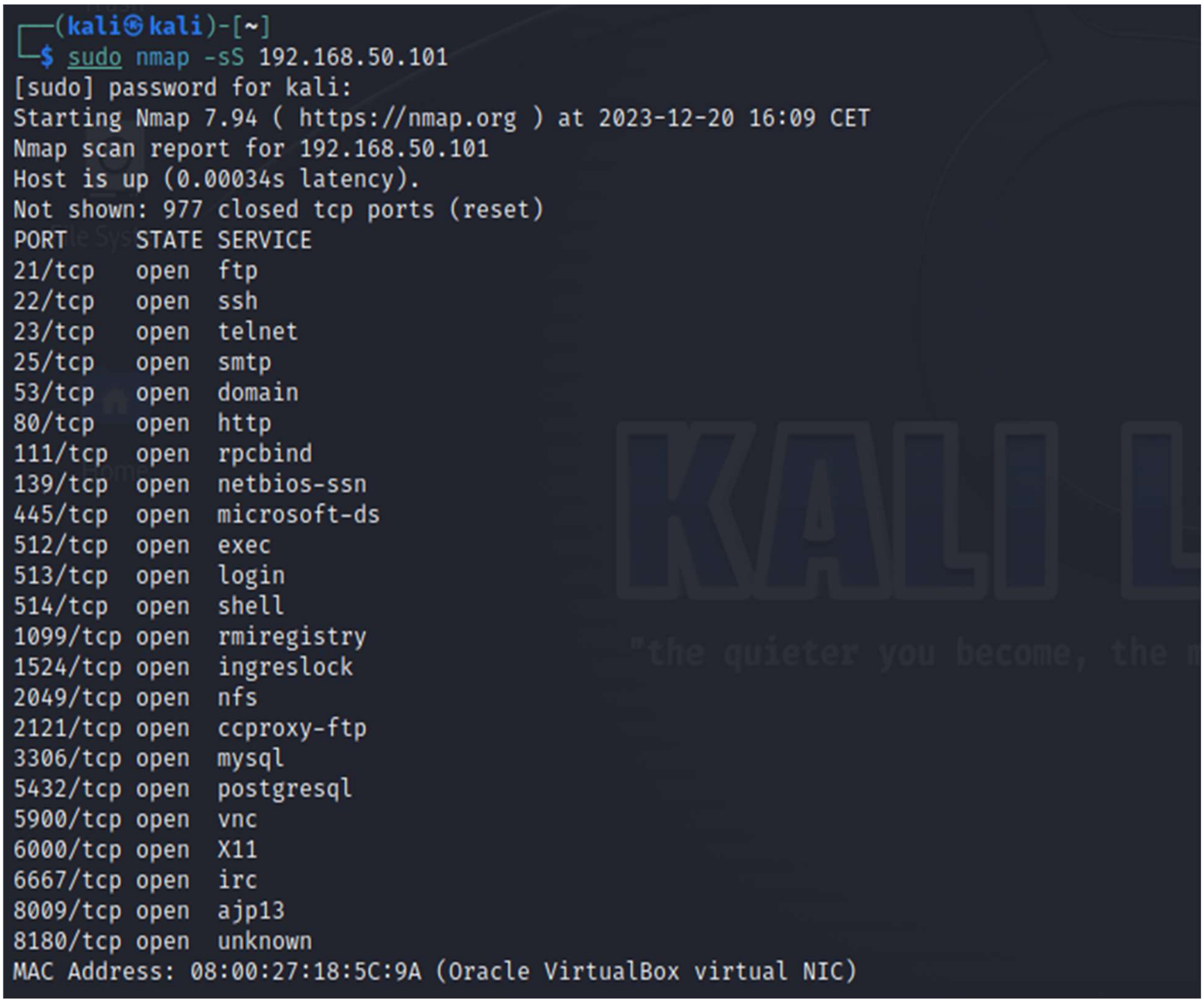
Scan 1



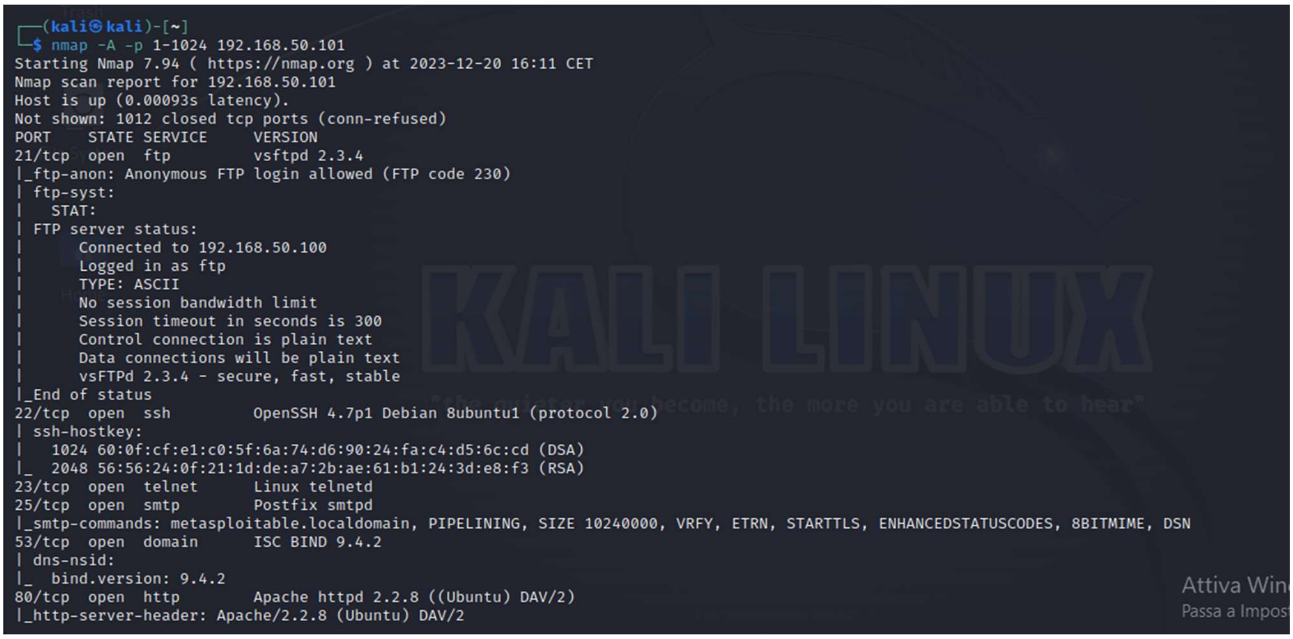
```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 16:07 CET
Nmap scan report for 192.168.50.101
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds

┌──(kali㉿kali)-[~]
```

Scan 2

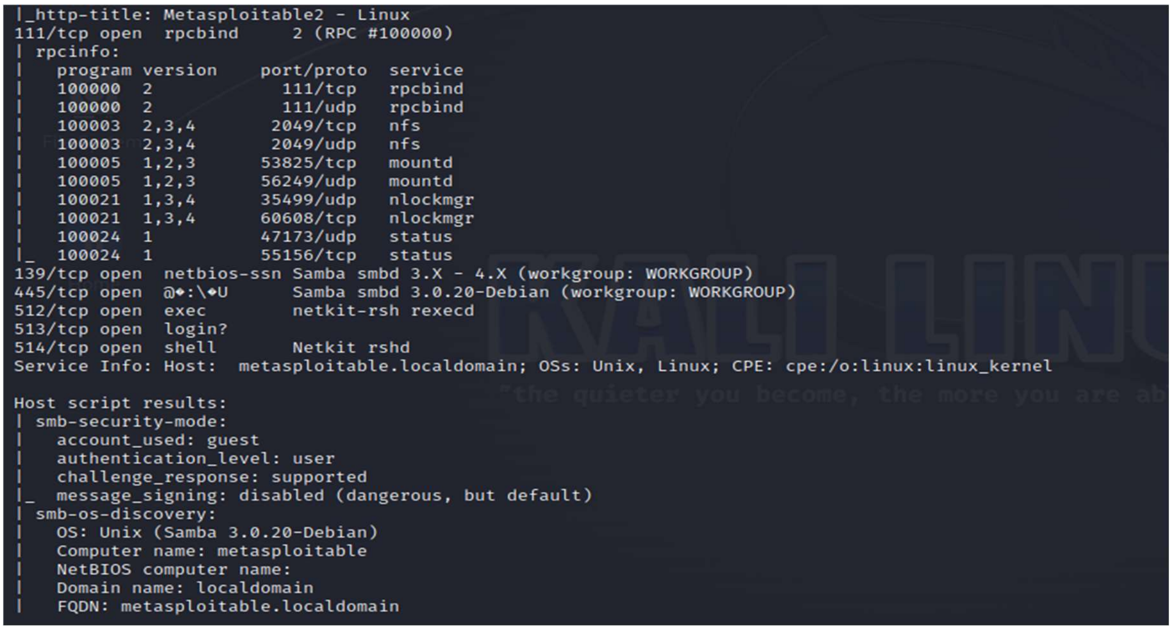


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 16:09 CET
Nmap scan report for 192.168.50.101
Host is up (0.00034s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   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: 08:00:27:18:5C:9A (Oracle VirtualBox virtual NIC)
```

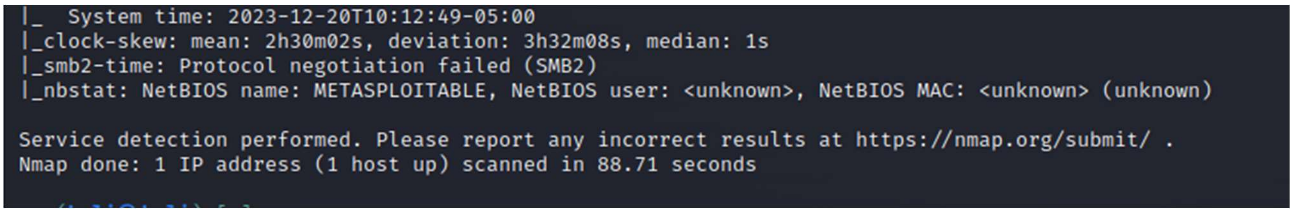
Scan 3



```
┌──(kali㉿kali)-[~]
└─$ nmap -A -p 1-1024 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 16:11 CET
Nmap scan report for 192.168.50.101
Host is up (0.00093s latency).
Not shown: 1012 closed tcp ports (conn-refused)
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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

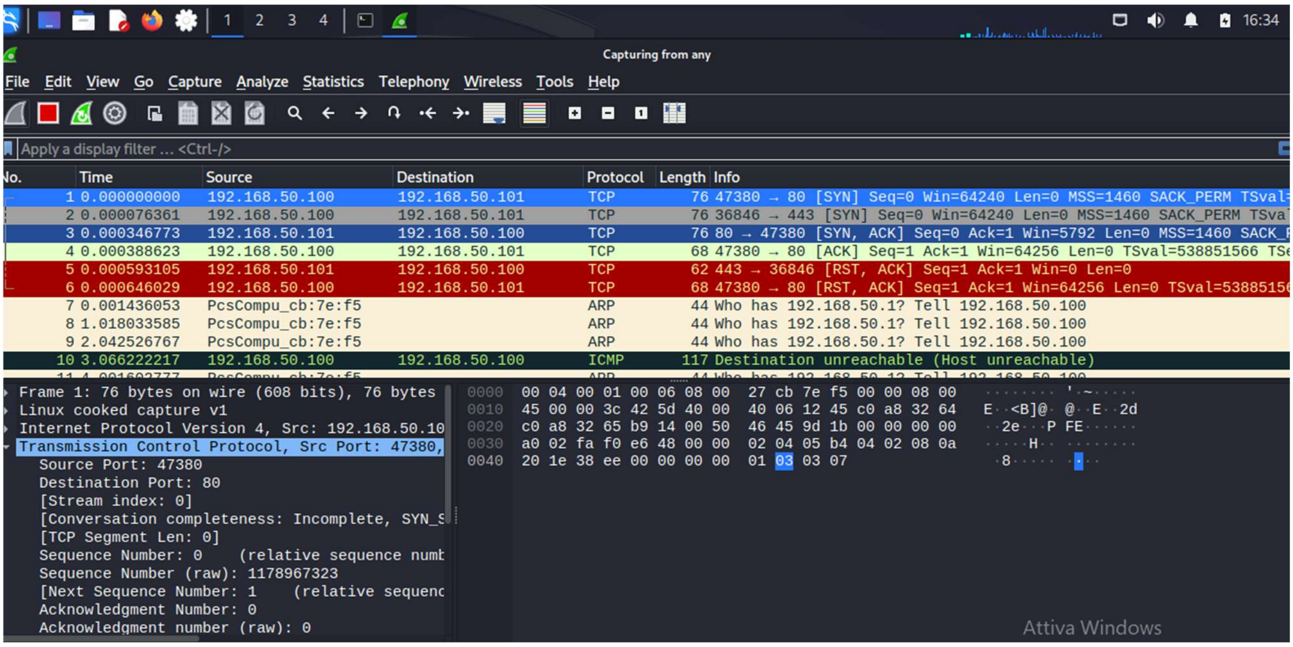


```
|_http-title: Metasploitable2 - Linux
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      53825/tcp   mountd
|   100005  1,2,3      56249/udp   mountd
|   100021  1,3,4      35499/udp   nlockmgr
|   100021  1,3,4      60608/tcp   nlockmgr
|   100024  1          47173/udp   status
|_  100024  1          55156/tcp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  @•:\•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
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
```



```
|_  System time: 2023-12-20T10:12:49-05:00
|_clock-skew: mean: 2h30m02s, deviation: 3h32m08s, median: 1s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 88.71 seconds
```

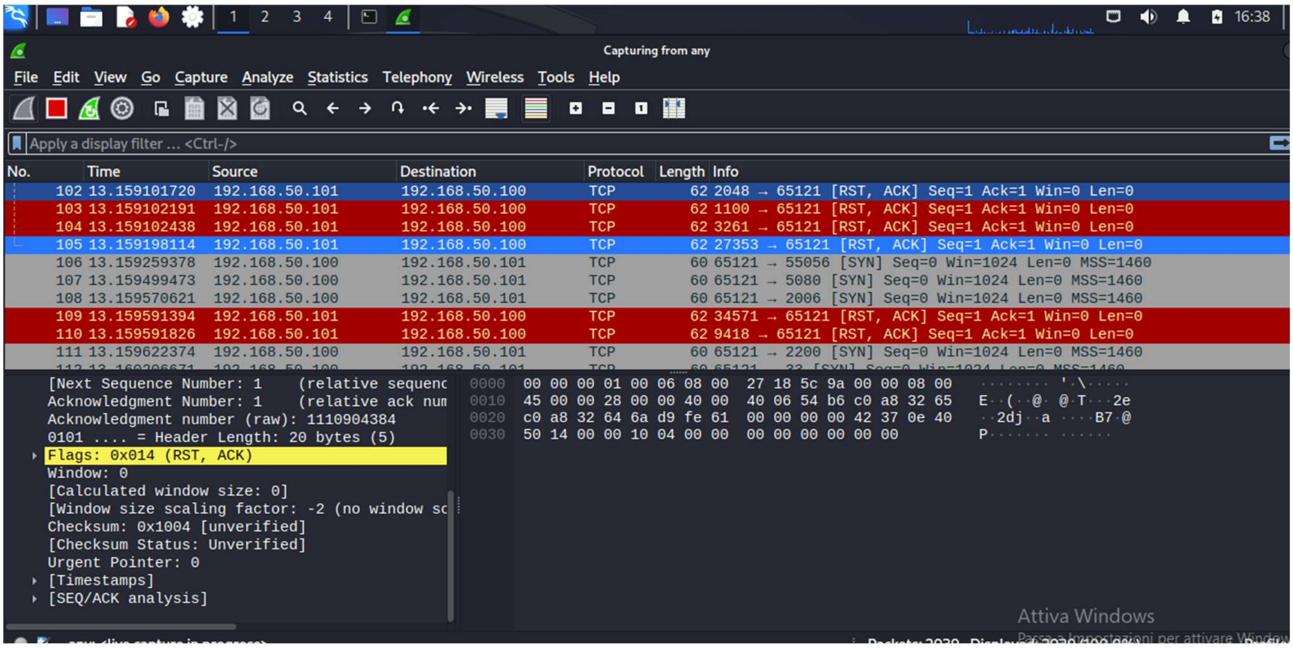
Wireshark



1 2 3 4
16:34
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Attiva Windows

```
No.  Time          Source              Destination      Protocol  Length Info
   1 0.000000000   192.168.50.100      192.168.50.101   TCP         76 47380 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=
   2 0.000076361   192.168.50.100      192.168.50.101   TCP         76 36846 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva
   3 0.000346773   192.168.50.101      192.168.50.100   TCP         76 80 → 47380 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_P
   4 0.000388623   192.168.50.100      192.168.50.101   TCP         68 47380 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=538851566 TSe
   5 0.000593105   192.168.50.101      192.168.50.100   TCP         62 443 → 36846 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   6 0.000646029   192.168.50.100      192.168.50.101   TCP         68 47380 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=5388515
   7 0.001436053   PcsCompu_cb:7e:f5                    ARP         44 Who has 192.168.50.1? Tell 192.168.50.100
   8 1.018033585   PcsCompu_cb:7e:f5                    ARP         44 Who has 192.168.50.1? Tell 192.168.50.100
   9 2.042526767   PcsCompu_cb:7e:f5                    ARP         44 Who has 192.168.50.1? Tell 192.168.50.100
  10 3.066222217   192.168.50.100      192.168.50.100   ICMP       117 Destination unreachable (Host unreachable)
```

```
› Frame 1: 76 bytes on wire (608 bits), 76 bytes      0000  00 04 00 01 00 06 08 00  27 cb 7e f5 00 00 08 00   ········ '·~·····
› Linux cooked capture v1                             0010  45 00 00 3c 42 5d 40 00  40 06 12 45 c0 a8 32 64   E··<B]@· @··E··2d
› Internet Protocol Version 4, Src: 192.168.50.10     0020  c0 a8 32 65 b9 14 00 50  46 45 9d 1b 00 00 00 00   ··2e···P FE······
⌄ Transmission Control Protocol, Src Port: 47380,     0030  a0 02 fa f0 e6 48 00 00  02 04 05 b4 04 02 08 0a   ·····H·· ········
    Source Port: 47380                                0040  20 1e 38 ee 00 00 00 00  01 03 03 07               ·8······ ····
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Incomplete, SYN_S
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence numb
    Sequence Number (raw): 1178967323
    [Next Sequence Number: 1    (relative sequenc
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
```



```
No.   Time         Source          Destination     Protocol Length Info
  102 13.159101720 192.168.50.101  192.168.50.100  TCP      62 2048 → 65121 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  103 13.159102191 192.168.50.101  192.168.50.100  TCP      62 1100 → 65121 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  104 13.159102438 192.168.50.101  192.168.50.100  TCP      62 3261 → 65121 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  105 13.159198114 192.168.50.101  192.168.50.100  TCP      62 27353 → 65121 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  106 13.159259378 192.168.50.100  192.168.50.101  TCP      60 65121 → 55056 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  107 13.159499473 192.168.50.100  192.168.50.101  TCP      60 65121 → 5080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  108 13.159570621 192.168.50.100  192.168.50.101  TCP      60 65121 → 2006 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  109 13.159591394 192.168.50.101  192.168.50.100  TCP      62 34571 → 65121 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  110 13.159591826 192.168.50.101  192.168.50.100  TCP      62 9418 → 65121 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  111 13.159622374 192.168.50.100  192.168.50.101  TCP      60 65121 → 2200 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

```
  [Next Sequence Number: 1    (relative sequenc
  Acknowledgment Number: 1    (relative ack num
  Acknowledgment number (raw): 1110904384
  0101 .... = Header Length: 20 bytes (5)
▸ Flags: 0x014 (RST, ACK)
  Window: 0
  [Calculated window size: 0]
  [Window size scaling factor: -2 (no window sc
  Checksum: 0x1004 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
▸ [Timestamps]
▸ [SEQ/ACK analysis]
```

```
0000  00 00 00 01 00 06 08 00  27 18 5c 9a 00 00 08 00   ········ '·\·····
0010  45 00 00 28 00 00 40 00  40 06 54 b6 c0 a8 32 65   E··(··@· @·T···2e
0020  c0 a8 32 64 6a d9 fe 61  00 00 00 00 42 37 0e 40   ··2dj··a ····B7·@
0030  50 14 00 00 10 04 00 00  00 00 00 00 00 00         P······· ······
```

TABELLA:

Fonte Scan	**Target Scan**	**Tipo Scan**	**Risultati**
NMAP	192.168.50.101 P: 1-1024	TCP	23
NMAP	192.168.50.101 P: 1-1024	SYN	23
NMAP	192.168.50.101 P: 1-1024	-A	12