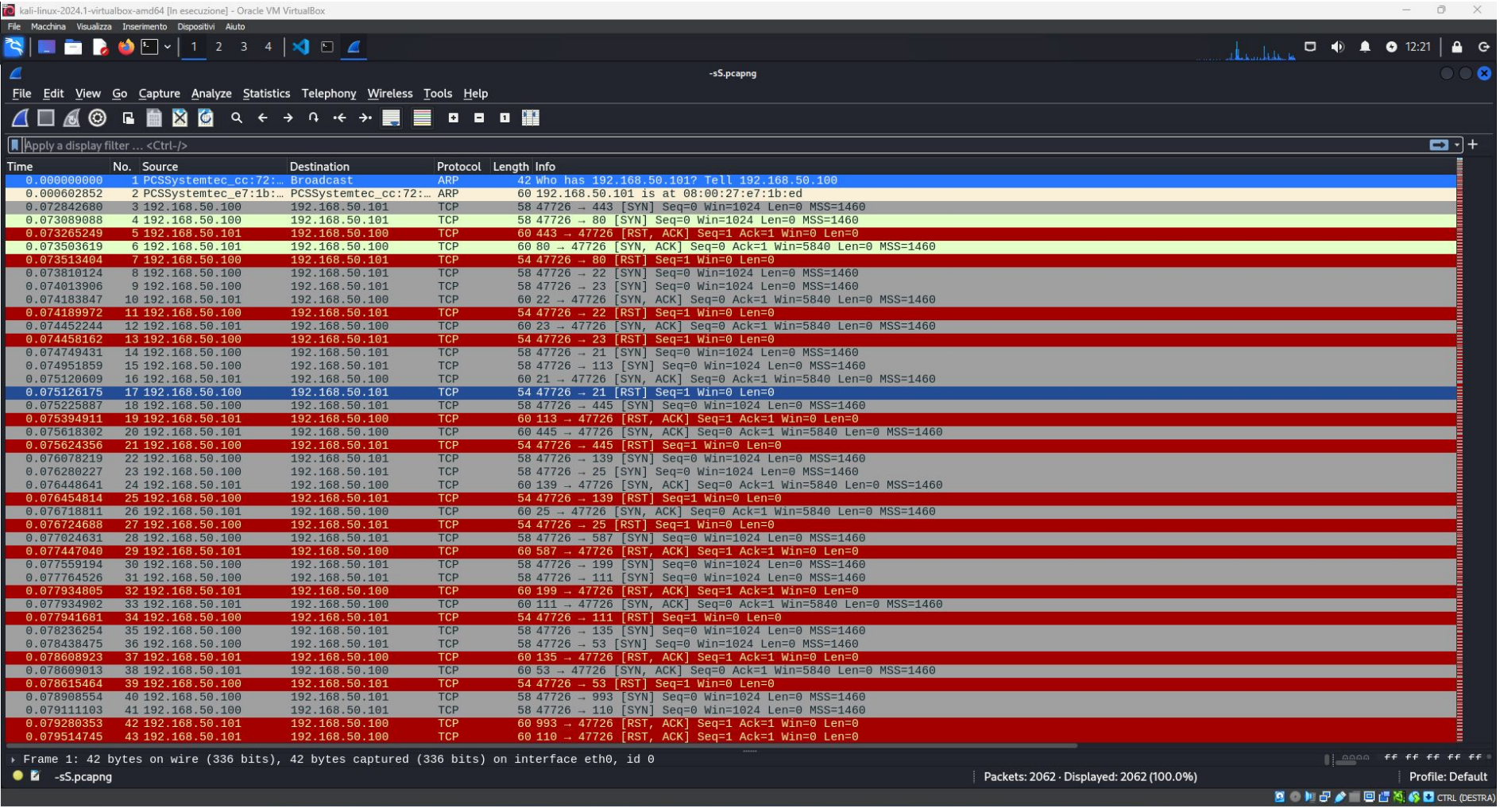
```
┌──(root㉿kali)-[~]
└─# nmap -sS -p 0-1023 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 14:21 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dn
s or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00040s 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:E7:1B:ED (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

┌──(root㉿kali)-[~]
└─# nmap -sT -p 0-1023 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 14:21 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dn
s or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00049s 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:E7:1B:ED (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

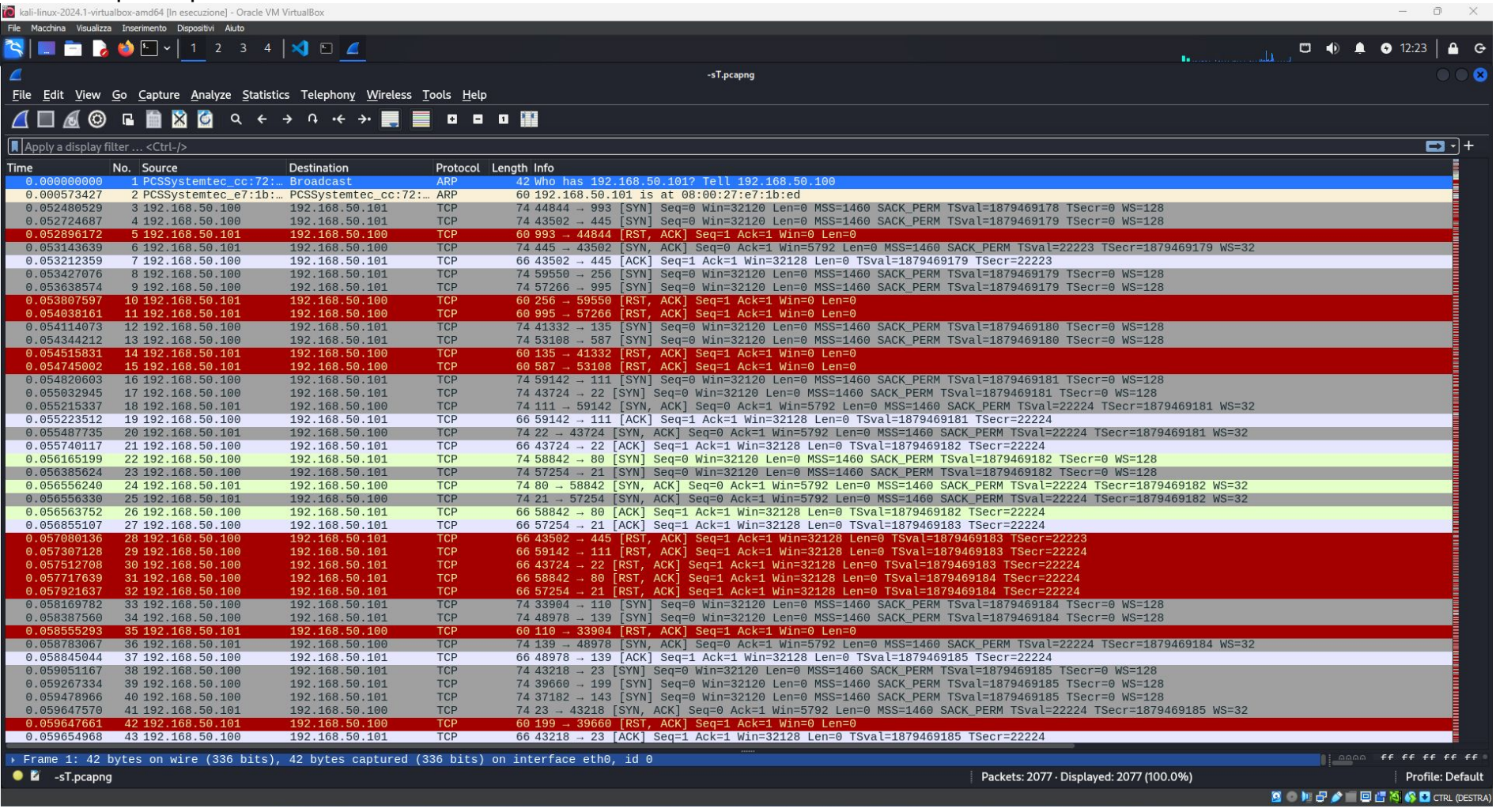
```
┌──(root㉿kali)-[~]
└─# nmap -A -p 0-1023 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 14:22 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dn
s or specify valid servers with --dns-servers
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 16.67% done; ETC: 14:23 (0:00:30 remaining)
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 58.33% done; ETC: 14:23 (0:00:26 remaining)
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 14:23 (0:00:19 remaining)
Stats: 0:01:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 14:25 (0:00:49 remaining)
Stats: 0:03:10 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.58% done; ETC: 14:26 (0:00:00 remaining)
Stats: 0:03:27 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 14:26 (0:00:00 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.00061s 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?
25/tcp  open  smtp?
|_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      44636/udp   mountd
|   100005  1,2,3      59761/tcp   mountd
|   100021  1,3,4      52110/tcp   nlockmgr
|   100021  1,3,4      53097/udp   nlockmgr
|   100024  1          39804/tcp   status
|_  100024  1          40369/udp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec?
513/tcp open  login?
514/tcp open  shell?
MAC Address: 08:00:27:E7:1B:ED (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
```

```
Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| 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: 2024-07-02T14:25:37-04:00
|_clock-skew: mean: 1h59m59s, deviation: 2h49m42s, median: 0s
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.61 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 270.16 seconds
```

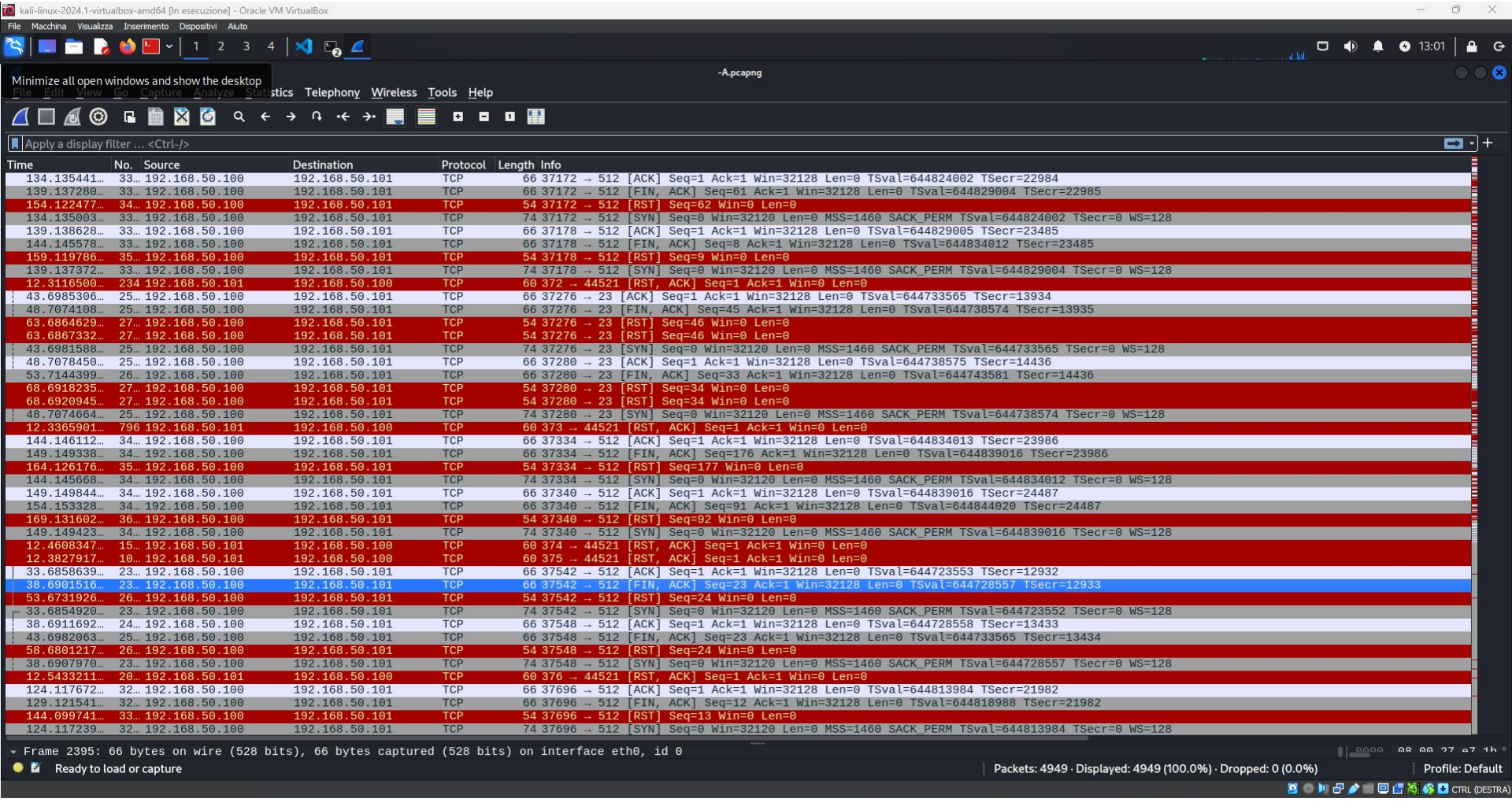
nmap -sS -p 0-1023 192.168.50.101



nmap -sT -p 0-1023 192.168.50.101



nmap -A -p 0-1023 192.168.50.101



Differenze tra Scansioni Nmap `-sS` e `-sT`

Scansione `-sS` (TCP SYN scan)

1. **Protocollo Utilizzato**:
   - Viene utilizzato il protocollo TCP con il flag SYN.
   - Non completa la connessione TCP; invia solo pacchetti SYN e attende le risposte SYN/ACK o RST.
2. **Risposte Rilevate**:
   - La maggior parte delle risposte sono pacchetti RST (Reset) o SYN/ACK.
   - Questo indica che la scansione è più furtiva poiché non completa la stretta di mano TCP.
3. **Tempo di Esecuzione**:
   - Generalmente più veloce rispetto alla scansione `-sT` poiché non richiede la completa instaurazione di una connessione.
4. **Rilevabilità**:
   - Meno rilevabile dai firewall e dai sistemi di rilevamento delle intrusioni (IDS) rispetto alla scansione `-sT`.

Scansione `-sT` (TCP Connect scan)

1. **Protocollo Utilizzato**:
   - Viene utilizzato il protocollo TCP con la connessione completa.
   - Completa la connessione TCP tramite la stretta di mano a tre vie (SYN, SYN/ACK, ACK).
2. **Risposte Rilevate**:
   - Comprende un mix di pacchetti SYN, ACK, e RST.
   - Questo indica che ogni porta viene completamente aperta e chiusa, completando il processo di connessione.
3. **Tempo di Esecuzione**:
   - Può essere più lento rispetto alla scansione `-sS` poiché richiede la completa instaurazione e chiusura della connessione TCP.
4. **Rilevabilità**:
   - Più rilevabile dai firewall e dai sistemi di rilevamento delle intrusioni (IDS) rispetto alla scansione `-sS` perché completa la connessione.

Report Dettagliato

Comandi Utilizzati

- **Scansione `-sS`**: `nmap -sS [target]`
- **Scansione `-sT`**: `nmap -sT [target]`

Analisi dei Pacchetti

Scansione `-sS`

- **Pacchetti TCP SYN**: Vengono inviati pacchetti TCP con il flag SYN.
- **Risposte SYN/ACK**: Se la porta è aperta, il target risponde con SYN/ACK.
- **Risposte RST**: Se la porta è chiusa, il target risponde con RST.

Scansione `-sT`

- **Pacchetti TCP SYN**: Vengono inviati pacchetti TCP con il flag SYN.
- **Completamento della Connessione**: Se la porta è aperta, il target risponde con SYN/ACK e il client risponde con ACK.
- **Risposte RST**: Se la porta è chiusa, il target risponde con RST.