

```
(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-dns
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:el: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, 8BITIME, 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 4636/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:
|_nbtstat: 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

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Auto

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

| Time | No. | Source | Destination | Protocol | Length | Info |
|-------------|-----|------------------------|------------------------|----------|--------|--|
| 0.000000000 | 1 | PCSSystemtec_cc:72:... | Broadcast | ARP | 42 | Who has 192.168.50.101? Tell 192.168.50.100 |
| 0.000602852 | 2 | PCSSystemtec_e7:1b:... | PCSSystemtec_cc:72:... | ARP | 60 | 192.168.50.101 is at 08:00:27:e7:1b:ed |
| 0.072842680 | 3 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.073089088 | 4 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.073205249 | 5 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 443 → 47726 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 0.073593619 | 6 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 80 → 47726 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 0.073513404 | 7 | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 47726 → 80 [RST] Seq=1 Win=0 Len=0 |
| 0.073810124 | 8 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.074013906 | 9 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.074183847 | 10 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 22 → 47726 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 0.074189972 | 11 | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 47726 → 22 [RST] Seq=1 Win=0 Len=0 |
| 0.074452244 | 12 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 23 → 47726 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 0.074458162 | 13 | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 47726 → 23 [RST] Seq=1 Win=0 Len=0 |
| 0.074749431 | 14 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.074951859 | 15 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.075120609 | 16 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 21 → 47726 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 0.075126175 | 17 | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 47726 → 21 [RST] Seq=1 Win=0 Len=0 |
| 0.075225887 | 18 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.075394911 | 19 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 113 → 47726 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 0.075618302 | 20 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 445 → 47726 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 0.075624356 | 21 | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 47726 → 445 [RST] Seq=1 Win=0 Len=0 |
| 0.076078219 | 22 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.076280227 | 23 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.076448641 | 24 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 139 → 47726 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 0.076454814 | 25 | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 47726 → 139 [RST] Seq=1 Win=0 Len=0 |
| 0.076718811 | 26 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 25 → 47726 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 0.076724688 | 27 | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 47726 → 25 [RST] Seq=1 Win=0 Len=0 |
| 0.077024631 | 28 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.077447040 | 29 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 587 → 47726 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 0.077559194 | 30 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.077764526 | 31 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.077934805 | 32 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 199 → 47726 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 0.077934902 | 33 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 111 → 47726 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 0.077941681 | 34 | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 47726 → 111 [RST] Seq=1 Win=0 Len=0 |
| 0.078236254 | 35 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.078438475 | 36 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.078608923 | 37 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 135 → 47726 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 0.078609013 | 38 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 53 → 47726 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 0.078615464 | 39 | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 47726 → 53 [RST] Seq=1 Win=0 Len=0 |
| 0.078908554 | 40 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.079111103 | 41 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 47726 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 0.079280353 | 42 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 993 → 47726 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 0.079514745 | 43 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 110 → 47726 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0

-sS.pcapng

Packets: 2062 · Displayed: 2062 (100.0%)

Profile: Default

CTRL (DESTRA)

nmap -sT -p 0-1023 192.168.50.101

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-I>

| Time | No. | Source | Destination | Protocol | Length | Info |
|-------------|-----|----------------------|----------------------|----------|--------|---|
| 0.000000000 | 1 | PCSSystemtec_cc:72:: | Broadcast | ARP | 42 | Who has 192.168.50.101? Tell 192.168.50.100 |
| 0.000573427 | 2 | PCSSystemtec_e7:1b:: | PCSSystemtec_cc:72:: | ARP | 60 | 192.168.50.101 is at 08:00:27:e7:1b:ed |
| 0.052480529 | 3 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 44844 → 993 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469178 TSecr=0 WS=128 |
| 0.052724687 | 4 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 43502 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469179 TSecr=0 WS=128 |
| 0.052896172 | 5 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 993 → 44844 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 0.053143639 | 6 | 192.168.50.101 | 192.168.50.100 | TCP | 74 | 445 → 43502 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=22223 TSecr=1879469179 WS=32 |
| 0.053212359 | 7 | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 43502 → 445 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1879469179 TSecr=22223 |
| 0.053427076 | 8 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 59558 → 256 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469179 TSecr=0 WS=128 |
| 0.053638574 | 9 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 57266 → 995 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469179 TSecr=0 WS=128 |
| 0.053807597 | 10 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 256 → 59550 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 0.054038161 | 11 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 995 → 57266 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 0.054114073 | 12 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 41332 → 135 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469180 TSecr=0 WS=128 |
| 0.054344212 | 13 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 53108 → 587 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469180 TSecr=0 WS=128 |
| 0.054515831 | 14 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 135 → 41332 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 0.054745002 | 15 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 587 → 53108 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 0.054820603 | 16 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 59142 → 111 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469181 TSecr=0 WS=128 |
| 0.055032945 | 17 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 43724 → 22 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469181 TSecr=0 WS=128 |
| 0.055215337 | 18 | 192.168.50.101 | 192.168.50.100 | TCP | 74 | 111 → 59142 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=22224 TSecr=1879469181 WS=32 |
| 0.055223512 | 19 | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 59142 → 111 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1879469181 TSecr=22224 |
| 0.055487735 | 20 | 192.168.50.101 | 192.168.50.100 | TCP | 74 | 22 → 43724 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=22224 TSecr=1879469181 WS=32 |
| 0.055740117 | 21 | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 43724 → 22 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1879469182 TSecr=22224 |
| 0.056165199 | 22 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 58842 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469182 TSecr=0 WS=128 |
| 0.056385624 | 23 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 57254 → 21 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469182 TSecr=0 WS=128 |
| 0.056556240 | 24 | 192.168.50.101 | 192.168.50.100 | TCP | 74 | 80 → 58842 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=22224 TSecr=1879469182 WS=32 |
| 0.056556330 | 25 | 192.168.50.101 | 192.168.50.100 | TCP | 74 | 21 → 57254 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=22224 TSecr=1879469182 WS=32 |
| 0.056563752 | 26 | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 58842 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1879469182 TSecr=22224 |
| 0.056855107 | 27 | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 57254 → 21 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1879469183 TSecr=22224 |
| 0.057080136 | 28 | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 43502 → 445 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1879469183 TSecr=22223 |
| 0.057307128 | 29 | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 59142 → 111 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1879469183 TSecr=22224 |
| 0.057512708 | 30 | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 43724 → 22 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1879469183 TSecr=22224 |
| 0.057717639 | 31 | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 58842 → 80 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1879469184 TSecr=22224 |
| 0.057921637 | 32 | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 57254 → 21 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1879469184 TSecr=22224 |
| 0.058169782 | 33 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 33904 → 110 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469184 TSecr=0 WS=128 |
| 0.058387560 | 34 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 48978 → 139 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469184 TSecr=0 WS=128 |
| 0.058555293 | 35 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 110 → 33904 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 0.058783067 | 36 | 192.168.50.101 | 192.168.50.100 | TCP | 74 | 139 → 48978 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=22224 TSecr=1879469184 WS=32 |
| 0.058845044 | 37 | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 48978 → 139 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1879469185 TSecr=22224 |
| 0.059051167 | 38 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 43218 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469185 TSecr=0 WS=128 |
| 0.059267334 | 39 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 39660 → 199 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469185 TSecr=0 WS=128 |
| 0.059478966 | 40 | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 37182 → 143 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1879469185 TSecr=0 WS=128 |
| 0.059647570 | 41 | 192.168.50.101 | 192.168.50.100 | TCP | 74 | 23 → 43218 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=22224 TSecr=1879469185 WS=32 |
| 0.059647661 | 42 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 199 → 39660 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 0.059654968 | 43 | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 43218 → 23 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1879469185 TSecr=22224 |

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0

-sT.pcapng

Packets: 2077 · Displayed: 2077 (100.0%)

Profile: Default

CTRL (DESTRA)

nmap -A -p 0-1023 192.168.50.101

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

1 2 3 4

- Apcaping

Minimize all open windows and show the desktop

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

| Time | No. | Source | Destination | Protocol | Length | Info |
|--------------|------|----------------|----------------|----------|--------|---|
| 134.135441.. | 33.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37172 → 512 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=644824002 TSecr=22984 |
| 139.137280.. | 33.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37172 → 512 [FIN, ACK] Seq=61 Ack=1 Win=32128 Len=0 TSval=644829004 TSecr=22985 |
| 154.122477.. | 34.. | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 37172 → 512 [RST] Seq=62 Win=0 Len=0 |
| 134.135003.. | 33.. | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 37172 → 512 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=644824002 TSecr=0 WS=128 |
| 139.138628.. | 33.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37178 → 512 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=644829005 TSecr=23485 |
| 144.145578.. | 33.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37178 → 512 [FIN, ACK] Seq=8 Ack=1 Win=32128 Len=0 TSval=644834012 TSecr=23485 |
| 159.119786.. | 35.. | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 37178 → 512 [RST] Seq=9 Win=0 Len=0 |
| 139.137372.. | 33.. | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 37178 → 512 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=644829004 TSecr=0 WS=128 |
| 12.3116500.. | 234 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 372 → 44521 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 43.6985306.. | 25.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37276 → 23 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=644733565 TSecr=13934 |
| 48.7074108.. | 25.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37276 → 23 [FIN, ACK] Seq=45 Ack=1 Win=32128 Len=0 TSval=644738574 TSecr=13935 |
| 63.6864629.. | 27.. | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 37276 → 23 [RST] Seq=46 Win=0 Len=0 |
| 63.6867332.. | 27.. | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 37276 → 23 [RST] Seq=46 Win=0 Len=0 |
| 43.6981588.. | 25.. | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 37276 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=644733565 TSecr=0 WS=128 |
| 48.7078450.. | 25.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37280 → 23 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=644738575 TSecr=14436 |
| 53.7144399.. | 26.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37280 → 23 [FIN, ACK] Seq=33 Ack=1 Win=32128 Len=0 TSval=644743581 TSecr=14436 |
| 68.6918235.. | 27.. | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 37280 → 23 [RST] Seq=34 Win=0 Len=0 |
| 68.6920945.. | 27.. | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 37280 → 23 [RST] Seq=34 Win=0 Len=0 |
| 48.7074664.. | 25.. | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 37280 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=644738574 TSecr=0 WS=128 |
| 12.3365901.. | 796 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 373 → 44521 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 144.146112.. | 34.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37334 → 512 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=644834013 TSecr=23986 |
| 149.149338.. | 34.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37334 → 512 [FIN, ACK] Seq=176 Ack=1 Win=32128 Len=0 TSval=644839016 TSecr=23986 |
| 164.126176.. | 35.. | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 37334 → 512 [RST] Seq=177 Win=0 Len=0 |
| 144.145668.. | 34.. | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 37334 → 512 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=644834012 TSecr=0 WS=128 |
| 149.149844.. | 34.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37340 → 512 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=644839016 TSecr=24487 |
| 154.153328.. | 34.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37340 → 512 [FIN, ACK] Seq=91 Ack=1 Win=32128 Len=0 TSval=644844020 TSecr=24487 |
| 169.131602.. | 36.. | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 37340 → 512 [RST] Seq=92 Win=0 Len=0 |
| 149.149423.. | 34.. | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 37340 → 512 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=644839016 TSecr=0 WS=128 |
| 12.4608347.. | 15.. | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 374 → 44521 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 12.3827917.. | 10.. | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 375 → 44521 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 33.6858639.. | 23.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37542 → 512 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=644723553 TSecr=12932 |
| 38.6901516.. | 23.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37542 → 512 [FIN, ACK] Seq=23 Ack=1 Win=32128 Len=0 TSval=644728557 TSecr=12933 |
| 53.6731926.. | 26.. | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 37542 → 512 [RST] Seq=24 Win=0 Len=0 |
| 33.6854920.. | 23.. | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 37542 → 512 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=644723552 TSecr=0 WS=128 |
| 38.6911692.. | 24.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37548 → 512 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=644728558 TSecr=13433 |
| 43.6982063.. | 25.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37548 → 512 [FIN, ACK] Seq=23 Ack=1 Win=32128 Len=0 TSval=644733565 TSecr=13434 |
| 58.6801217.. | 26.. | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 37548 → 512 [RST] Seq=24 Win=0 Len=0 |
| 38.6907970.. | 23.. | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 37548 → 512 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=644728557 TSecr=0 WS=128 |
| 12.5433211.. | 20.. | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 376 → 44521 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 124.117672.. | 32.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37696 → 512 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=644813984 TSecr=21982 |
| 129.121541.. | 32.. | 192.168.50.100 | 192.168.50.101 | TCP | 66 | 37696 → 512 [FIN, ACK] Seq=12 Ack=1 Win=32128 Len=0 TSval=644818988 TSecr=21982 |
| 144.099741.. | 33.. | 192.168.50.100 | 192.168.50.101 | TCP | 54 | 37696 → 512 [RST] Seq=13 Win=0 Len=0 |
| 124.117239.. | 32.. | 192.168.50.100 | 192.168.50.101 | TCP | 74 | 37696 → 512 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=644813984 TSecr=0 WS=128 |

Frame 2395: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0

Ready to load or capture

Packets: 4949 · Displayed: 4949 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

CTRL (DESTRA)

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.