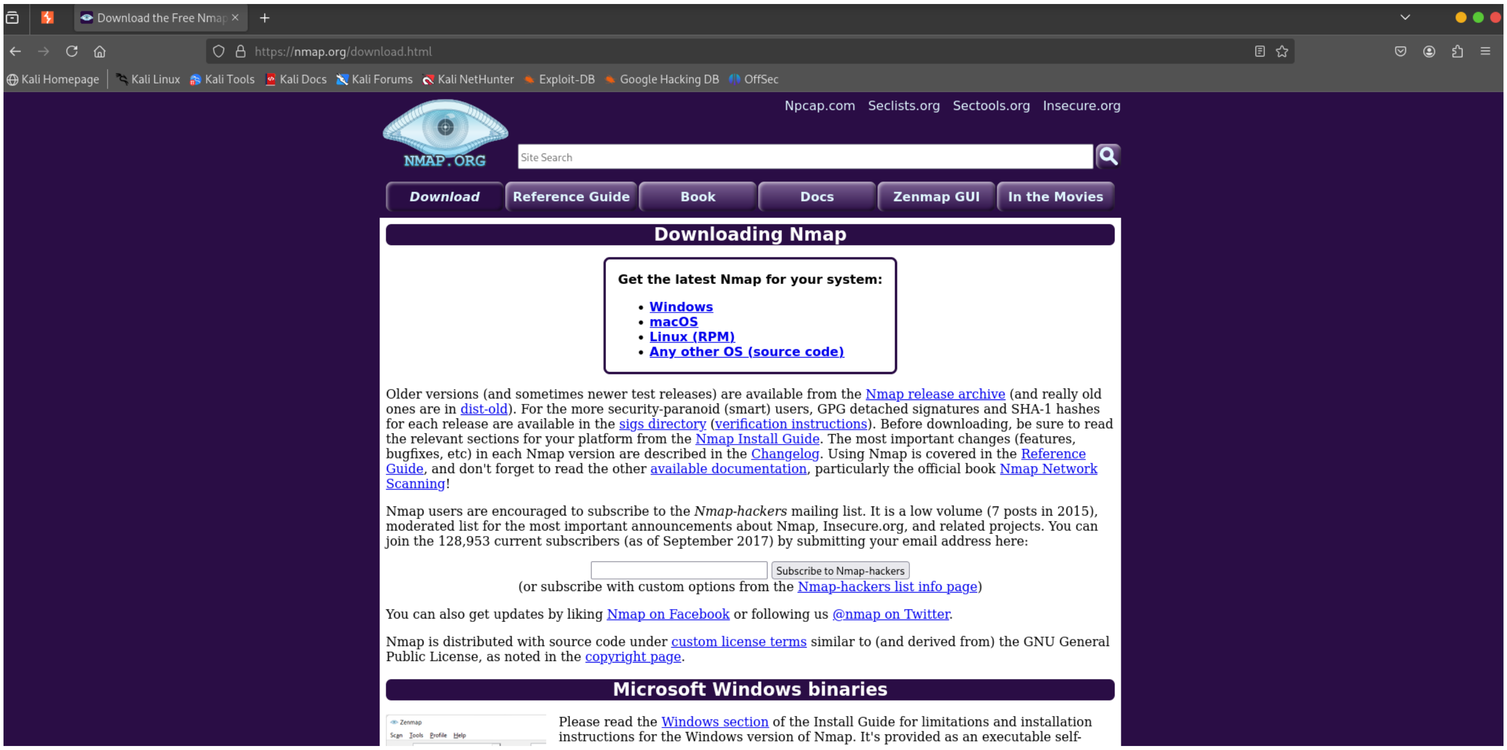


Downloading Nmap

Get the latest Nmap for your system:

- **Windows**
- **macOS**
- **Linux (RPM)**
- **Any other OS (source code)**

Older versions (and sometimes newer test releases) are available from the Nmap release archive (and really old ones are in dist-old). For the more security-paranoid (smart) users, GPG detached signatures and SHA-1 hashes for each release are available in the sigs directory (verification instructions). Before downloading, be sure to read the relevant sections for your platform from the Nmap Install Guide. The most important changes (features, bugfixes, etc) in each Nmap version are described in the Changelog. Using Nmap is covered in the Reference Guide, and don't forget to read the other available documentation, particularly the official book Nmap Network Scanning!

Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address here:

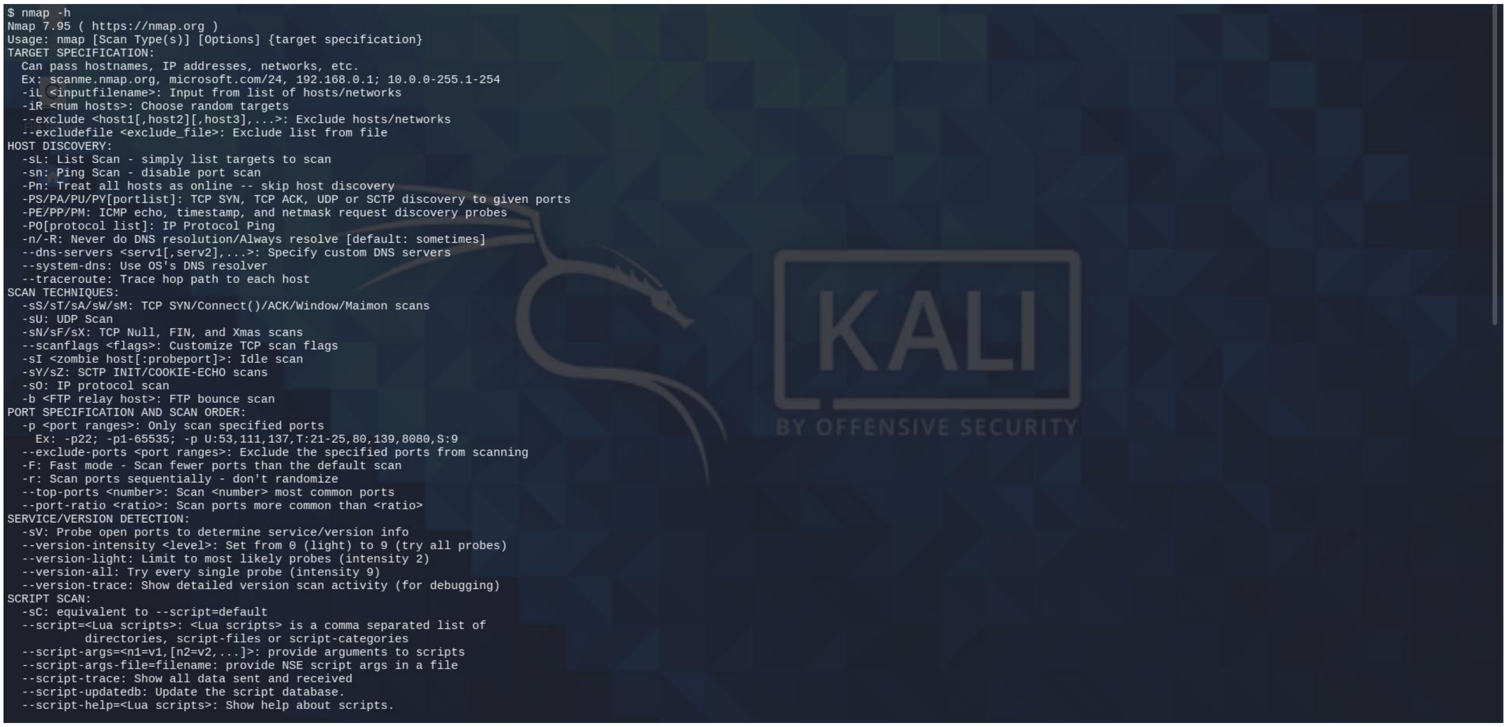
(or subscribe with custom options from the Nmap-hackers list info page)

You can also get updates by liking Nmap on Facebook or following us @nmap on Twitter.

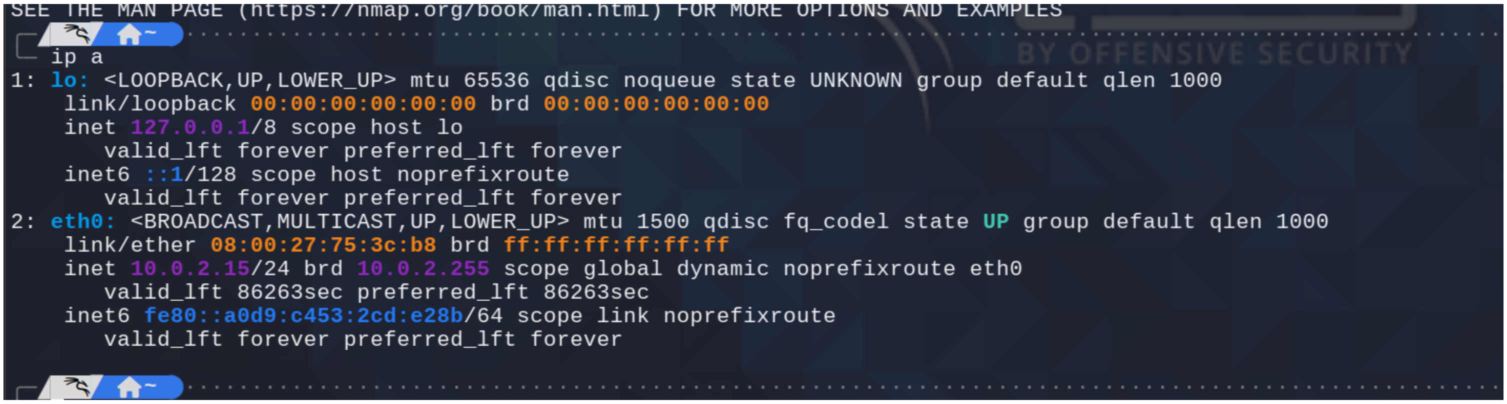
Nmap is distributed with source code under custom license terms similar to (and derived from) the GNU General Public License, as noted in the copyright page.

Microsoft Windows binaries

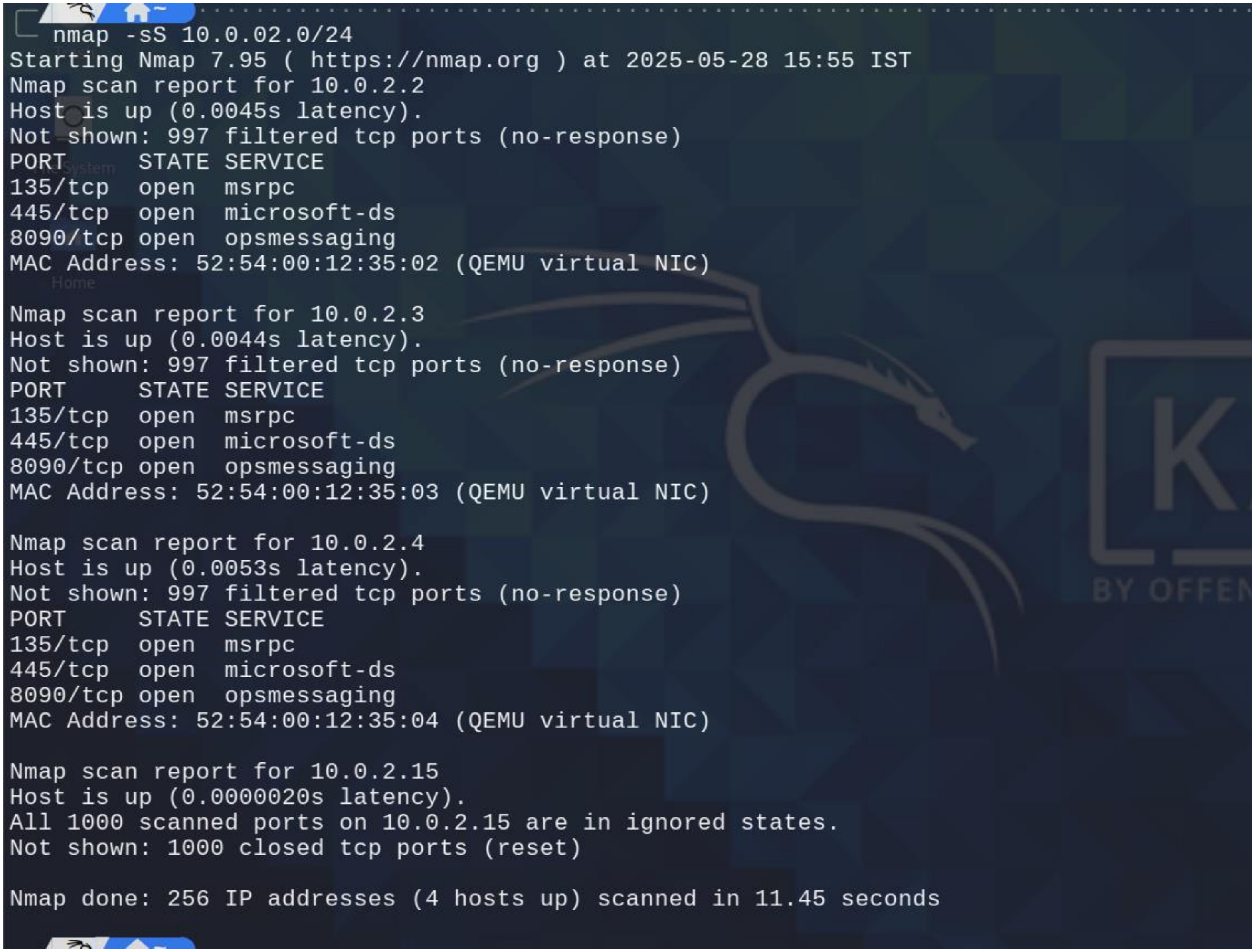
Please read the Windows section of the Install Guide for limitations and installation instructions for the Windows version of Nmap. It's provided as an executable self-



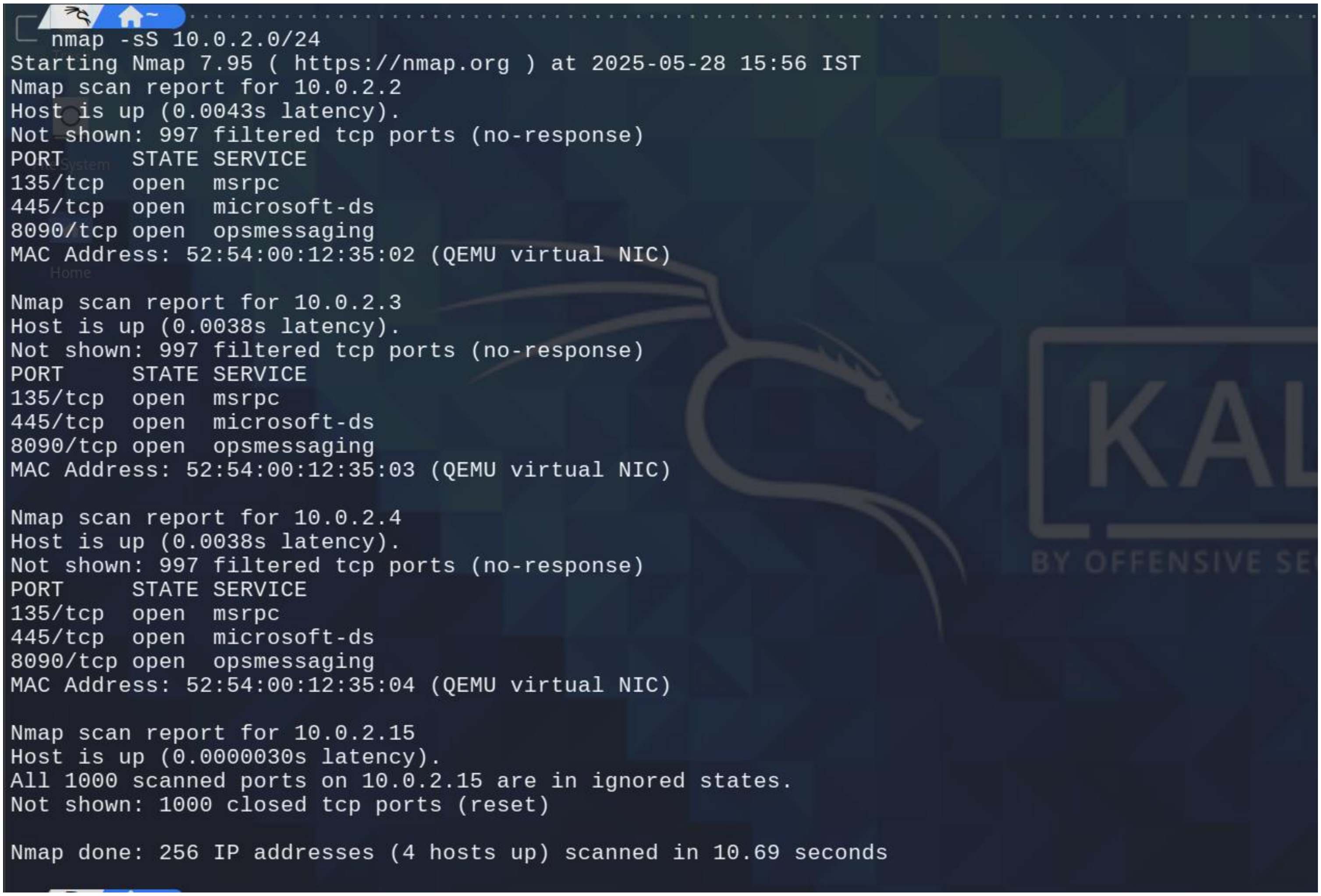
```
$ nmap -h
Nmap 7.95 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
```



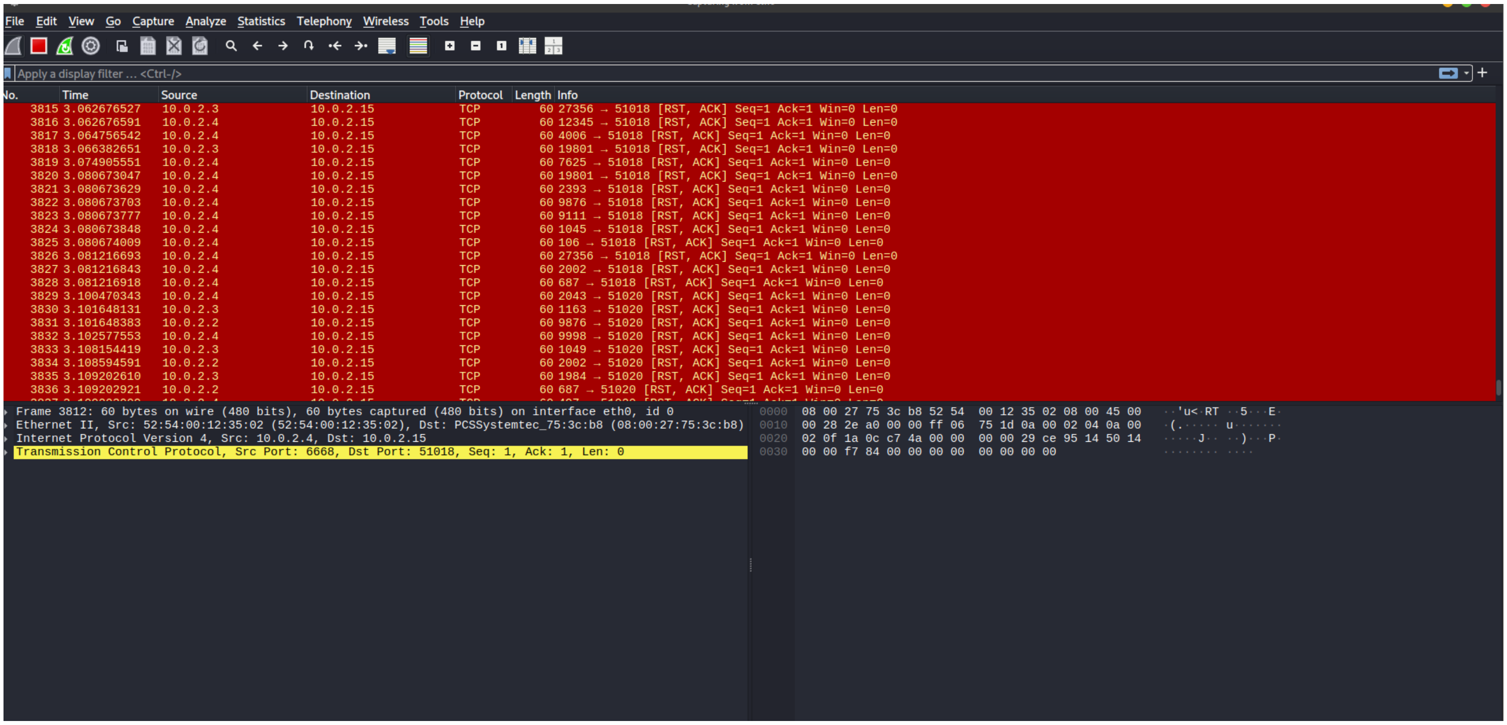
```
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
└─ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:75:3c:b8 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 86263sec preferred_lft 86263sec
    inet6 fe80::a0d9:c453:2cd:e28b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```



```
└─ nmap -sS 10.0.02.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-28 15:55 IST
Nmap scan report for 10.0.2.2
Host is up (0.0045s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
8090/tcp open  opsmessaging
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.0044s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
8090/tcp open  opsmessaging
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.0053s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
8090/tcp open  opsmessaging
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.0000020s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 11.45 seconds
```



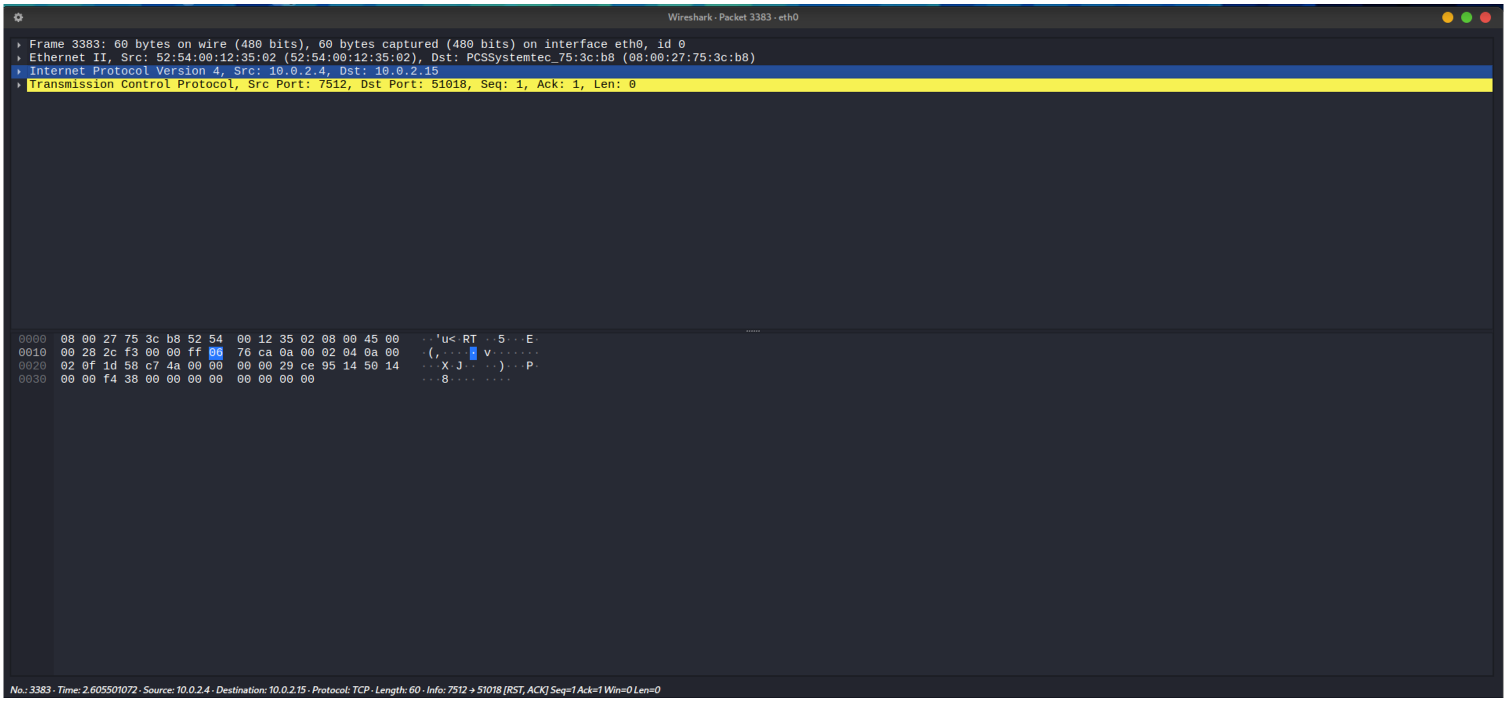
```
nmap -sS 10.0.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-28 15:56 IST
Nmap scan report for 10.0.2.2
Host is up (0.0043s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
8090/tcp open  opsmessaging
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.0038s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
8090/tcp open  opsmessaging
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.0038s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
8090/tcp open  opsmessaging
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 10.69 seconds
```



```
No.   Time         Source      Destination  Protocol Length Info
 3815 3.062676527  10.0.2.3    10.0.2.15    TCP      60 27356 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3816 3.062676591  10.0.2.4    10.0.2.15    TCP      60 12345 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3817 3.064756542  10.0.2.4    10.0.2.15    TCP      60 4006 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3818 3.066382651  10.0.2.3    10.0.2.15    TCP      60 19801 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3819 3.074905551  10.0.2.4    10.0.2.15    TCP      60 7625 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3820 3.080673047  10.0.2.4    10.0.2.15    TCP      60 19801 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3821 3.080673629  10.0.2.4    10.0.2.15    TCP      60 2393 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3822 3.080673703  10.0.2.4    10.0.2.15    TCP      60 9876 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3823 3.080673777  10.0.2.4    10.0.2.15    TCP      60 9111 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3824 3.080673848  10.0.2.4    10.0.2.15    TCP      60 1045 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3825 3.080674009  10.0.2.4    10.0.2.15    TCP      60 106 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3826 3.081216693  10.0.2.4    10.0.2.15    TCP      60 27356 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3827 3.081216843  10.0.2.4    10.0.2.15    TCP      60 2002 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3828 3.081216918  10.0.2.4    10.0.2.15    TCP      60 687 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3829 3.100470343  10.0.2.4    10.0.2.15    TCP      60 2043 → 51020 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3830 3.101648131  10.0.2.3    10.0.2.15    TCP      60 1163 → 51020 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3831 3.101648383  10.0.2.2    10.0.2.15    TCP      60 9876 → 51020 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3832 3.102577553  10.0.2.4    10.0.2.15    TCP      60 9998 → 51020 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3833 3.108154419  10.0.2.3    10.0.2.15    TCP      60 1049 → 51020 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3834 3.108594591  10.0.2.2    10.0.2.15    TCP      60 2002 → 51020 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3835 3.109202610  10.0.2.3    10.0.2.15    TCP      60 1984 → 51020 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3836 3.109202921  10.0.2.2    10.0.2.15    TCP      60 687 → 51020 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
› Frame 3812: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
› Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec_75:3c:b8 (08:00:27:75:3c:b8)
› Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
› Transmission Control Protocol, Src Port: 6668, Dst Port: 51018, Seq: 1, Ack: 1, Len: 0
```

```
0000  08 00 27 75 3c b8 52 54  00 12 35 02 08 00 45 00   ··'u<·RT ··5···E·
0010  00 28 2e a0 00 00 ff 06  75 1d 0a 00 02 04 0a 00   ·(······ u·······
0020  02 0f 1a 0c c7 4a 00 00  00 00 29 ce 95 14 50 14   ·····J·· ··)···P·
0030  00 00 f7 84 00 00 00 00  00 00 00 00               ········ ····
```



```
Frame 3383: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec_75:3c:b8 (08:00:27:75:3c:b8)
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 7512, Dst Port: 51018, Seq: 1, Ack: 1, Len: 0
```

```
0000  08 00 27 75 3c b8 52 54  00 12 35 02 08 00 45 00   ··'u<·RT ··5···E·
0010  00 28 2c f3 00 00 ff 06  76 ca 0a 00 02 04 0a 00   ·(,····· v·······
0020  02 0f 1d 58 c7 4a 00 00  00 00 29 ce 95 14 50 14   ···X·J·· ··)···P·
0030  00 00 f4 38 00 00 00 00  00 00 00 00               ···8···· ····
```

No.: 3383 · Time: 2.605501072 · Source: 10.0.2.4 · Destination: 10.0.2.15 · Protocol: TCP · Length: 60 · Info: 7512 → 51018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0