

CYBER SECURITY INTERNSHIP TASK -1

1. Install Nmap from Official Website

- Nmap (Network Mapper) is an open-source tool used for network discovery and security auditing.
- On Kali Linux, it is pre-installed. If not:

Command:

```
sudo apt update  
sudo apt install nmap -y
```

```
(kali@kali):~$ sudo apt install nmap  
[sudo] password for kali:  
nmap is already the newest version (7.95-efsg-3kali1).  
nmap set to manually installed.  
The following packages were automatically installed and are no longer required:  
  crackmapexec  libavfilter5  libgail-common  libgo2j  libhsoncqp25  libpython3.12-dev  libwinpr2-2164  python3-pendulum  python3.12  
  firebird3.0-common  libbfsio1  libgail18t64  libgsPELL-1-2  liblibfsgb0  libpython3.12-minimal  libzip4t64  python3-pluggy  python3.12-dev  
  firebird3.0-common-doc  libboost-iostreams1.83.0  libgd3t64  libgt2.0-0t64  libhomedcrypto7t64  libpython3.12-stdlib  libpython3.12-minimal  python3-pyinstaller-hooks-contrib  python3.12-minimal  
  fonts- liberation2  libboost-thread1.83.0  libgo2j-1.164  libgt2.0-bin  libhomed  libpython3.12t64  openjdk-17-jre  python3-pytestdata  python3.12-minimal  
  freerdp2-x11  libcapstone4  libgfsapi0  libgt2.0-common  libhomed3  librados2  libpython3.12t64  perl-modules-5.38  python3-pyverview  ruby-zeitwerk  ruby3.1  
  gccgo-14  libcephfs2  libgfrce0  libgtksourcview-3.0-1  libndct6  libredasm1t64  python3-aioconsole  python3-requests-ntlm  python3-rsa  ruby3.1-dev  ruby3.1-doc  ruby3.1-  
  gccgo-14-x86-64-linux-gnu  libconfig9v5  libgfrdr0  libgtksourcview-3.0-common  libnetcdf19t64  libre2-10  python3-appdirs  python3-diskcache  python3-setproctitle  rwho  samba-vfs-modules  
  golang-1.23-go  libconfig9  libgt1-mesa-dev  libgtksourcview-3.0-0v5  libopen264-7  libroc0.3  python3-hatch-vcs  python3-hatchling  python3-jose  python3-mistune0  python3-ntlm-auth  python3.11-dev  python3.11-minimal  
  golang-1.23-src  libdasc11  libgtapi-mesa  libgumbo2  libpaper1  libsuperlu6  python3-hatch-vcs  python3-setuptools-scm  python3-time-machine  python3-trove-classifiers  python3-wheel-whl  python3.11-dev  python3.11-minimal  
  hydra-gtk  libdirectfb-1.7-7t64  libgles-dev  libhdf5-103-1t64  libperl5.38t64  libtag1v5  libtag1v5-vanilla  libtaglib  libu2f-udev  python3-packaging-whl  python3-pathspec  python3.11-dev  python3.11-minimal  
  ibverbs-providers  liblgl-dev  libgles1  libhdf5-hl-100t64  libplacebo338  libtagmem  libtaglib  libu2f-udev  python3-packaging-whl  python3-pathspec  python3.11-dev  python3.11-minimal  
  icu-devtools  liblgl12t64  liblinterfs0  libhdf5-hl-100t64  libplacebo338  libtagmem  libtaglib  libu2f-udev  python3-packaging-whl  python3-pathspec  python3.11-dev  python3.11-minimal  
  libabsl20230802  liblgl12t64  liblinterfs0  libhdf5-hl-100t64  libplacebo338  libtagmem  libtaglib  libu2f-udev  python3-packaging-whl  python3-pathspec  python3.11-dev  python3.11-minimal  
  libmad12t64  liblgl12t64  liblinterfs0  libhdf5-hl-100t64  libplacebo338  libtagmem  libtaglib  libu2f-udev  python3-packaging-whl  python3-pathspec  python3.11-dev  python3.11-minimal  
  libassuan0  liblgl12t64  liblinterfs0  libhdf5-hl-100t64  libplacebo338  libtagmem  libtaglib  libu2f-udev  python3-packaging-whl  python3-pathspec  python3.11-dev  python3.11-minimal  
Use 'sudo apt autoremove' to remove them.  
Summary:  
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 82
```

2. Find Your Local IP Range

- You need to identify the **subnet** (range of IPs) to scan.
- Run:

Command:

```
ip a
```

```
(kali@kali):~$ 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 00:0c:29:5f:ad:8c brd ff:ff:ff:ff:ff:ff  
    inet 10.10.10.1/24 brd 10.10.10.255 scope global dynamic noprefixroute eth0  
        valid_lft 1564sec preferred_lft 1564sec  
    inet6 fe80::6617:c896:ba76:e331/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default  
    link/ether 02:42:5a:e1:43:ba brd ff:ff:ff:ff:ff:ff  
    inet 172.17.0.1/16 brd 172.17.0.255 scope global docker0  
        valid_lft forever preferred_lft forever
```

3. Run: `nmap -sS 192.168.1.0/24` to Perform a TCP SYN Scan

- This is a stealth scan (also known as half-open scan).
- It sends TCP SYN packets to all ports on each host in the subnet.

Command:

`sudo nmap -sS 192.168.40.0/24`

```
(kali@kali)-[~]
└─$ sudo nmap -sS 192.168.40.141/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 11:16 EDT
Nmap scan report for 192.168.40.1
Host is up (0.00084s latency).
All 1000 scanned ports on 192.168.40.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.40.2
Host is up (0.00027s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:F2:06:F1 (VMware)

Nmap scan report for 192.168.40.254
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.40.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E8:41:4C (VMware)

Nmap scan report for 192.168.40.141
Host is up (0.0000080s latency).
All 1000 scanned ports on 192.168.40.141 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 8.66 seconds
```

4: Note IP Addresses and Open Ports

- IP addresses
- Open ports
- Service names

Command:

`sudo nmap -sS -T4 -v 192.168.1.0/24`

```
(kali@kali)-[~]
$ sudo nmap -sS -T4 -v 192.168.40.141/24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 11:17 EDT
Initiating ARP Ping Scan at 11:17
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 11:17, 1.87s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 3 hosts. at 11:17
Completed Parallel DNS resolution of 3 hosts. at 11:17, 0.01s elapsed
Nmap scan report for 192.168.40.0 [host down]
Nmap scan report for 192.168.40.1 [host down]
Nmap scan report for 192.168.40.2 [host down]
Nmap scan report for 192.168.40.3 [host down]
Nmap scan report for 192.168.40.4 [host down]
Nmap scan report for 192.168.40.5 [host down]
Nmap scan report for 192.168.40.6 [host down]
Nmap scan report for 192.168.40.7 [host down]
Nmap scan report for 192.168.40.8 [host down]
Nmap scan report for 192.168.40.9 [host down]
Nmap scan report for 192.168.40.10 [host down]
Nmap scan report for 192.168.40.11 [host down]
Nmap scan report for 192.168.40.12 [host down]
Nmap scan report for 192.168.40.13 [host down]
Nmap scan report for 192.168.40.14 [host down]
Nmap scan report for 192.168.40.15 [host down]
Nmap scan report for 192.168.40.16 [host down]
Nmap scan report for 192.168.40.17 [host down]
Nmap scan report for 192.168.40.18 [host down]
Nmap scan report for 192.168.40.19 [host down]
Nmap scan report for 192.168.40.20 [host down]
Nmap scan report for 192.168.40.21 [host down]
Nmap scan report for 192.168.40.22 [host down]
Nmap scan report for 192.168.40.23 [host down]
Nmap scan report for 192.168.40.24 [host down]
Nmap scan report for 192.168.40.25 [host down]
Nmap scan report for 192.168.40.26 [host down]
Nmap scan report for 192.168.40.27 [host down]
Nmap scan report for 192.168.40.28 [host down]
Nmap scan report for 192.168.40.29 [host down]
Nmap scan report for 192.168.40.30 [host down]
Nmap scan report for 192.168.40.31 [host down]
Nmap scan report for 192.168.40.32 [host down]
Nmap scan report for 192.168.40.33 [host down]
Nmap scan report for 192.168.40.34 [host down]
Nmap scan report for 192.168.40.35 [host down]
Nmap scan report for 192.168.40.36 [host down]
Nmap scan report for 192.168.40.37 [host down]
Nmap scan report for 192.168.40.38 [host down]
Nmap scan report for 192.168.40.39 [host down]
Nmap scan report for 192.168.40.40 [host down]
Nmap scan report for 192.168.40.41 [host down]
Nmap scan report for 192.168.40.42 [host down]

540 58.587041026 192.168.40.141 192.168.40.1 TCP 58 57993 - 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
Nmap scan report for 192.168.40.2 40.141 192.168.40.2 TCP 58 57993 - 80 [SYN] Seq=0 Win=1024 Le
Host is up (0.00074s latency). 40.141 192.168.40.2 TCP 58 57993 - 135 [SYN] Seq=0 Win=1024 L
Not shown: 999 closed tcp ports (reset) 41 192.168.40.254 TCP 58 57993 - 80 [SYN] Seq=0 Win=1024 Le
PORT STATE SERVICE
53/tcp open domain
MAC Address: 00:50:56:F2:06:F1 (VMware) 41 192.168.40.2 TCP 58 57993 - 8888 [SYN] Seq=0 Win=1024
192.168.40.254 TCP 58 57993 - 135 [SYN] Seq=0 Win=1024 L
192.168.40.1 TCP 58 57993 - 135 [SYN] Seq=0 Win=1024 L
192.168.40.2 TCP 58 57993 - 110 [SYN] Seq=0 Win=1024 L
192.168.40.254 TCP 58 57993 - 8888 [SYN] Seq=0 Win=1024 L
192.168.40.1 TCP 58 57993 - 110 [SYN] Seq=0 Win=1024 L
192.168.40.254 TCP 58 57993 - 8888 [SYN] Seq=0 Win=1024 L
192.168.40.1 TCP 58 57993 - 854 [SYN] Seq=0 Win=1024 L

Initiating SYN Stealth Scan at 11:17
Scanning 192.168.40.141 [1000 ports]
Completed SYN Stealth Scan at 11:17, 0.03s elapsed (1000 total ports)
Nmap scan report for 192.168.40.141
Host is up (0.000080s latency).
All 1000 scanned ports on 192.168.40.141 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E8:41:4C (VMware)

Read data files from: /usr/share/nmap
Nmap done: 256 IP addresses (4 hosts up) scanned in 8.01 seconds
Raw packets sent: 6516 (278.512KB) | Rcvd: 3012 (124.388KB)
```

5. Optionally Analyze Packet Capture with Wireshark

- Open Wireshark:

sudo wireshark

- Select your network interface (e.g., wlan0, eth0)
- Start capture.

- While Wireshark is running, perform your Nmap scan.
- Use this filter to see SYN packets:

Search this in the wireshark filter:

`tcp.flags.syn == 1 && tcp.flags.ack == 0`

```
(kali@kali)~$ sudo wireshark
sudo wireshark: Error Protocol: No valid protocol list found. Seq=0, Len=0
** (Wireshark:8445) 11:23:37.718657 [GUI WARNING] -- QtStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
** (Wireshark:8445) 11:23:38.484659 [WSUTIL WARNING] ./wsutil/filter_files.c:242 -- read_filter_list(): /usr/share/wireshark/cfilters' line 1 doesn't have a quoted filter name.
** (Wireshark:8445) 11:23:38.484748 [WSUTIL WARNING] ./wsutil/filter_files.c:242 -- read_filter_list(): /usr/share/wireshark/cfilters' line 2 doesn't have a quoted filter name.
** (Wireshark:8445) 11:23:54.242500 [Capture MESSAGE] -- Capture Start ...
** (Wireshark:8445) 11:23:54.324643 [Capture MESSAGE] -- Capture started
** (Wireshark:8445) 11:23:54.324705 [Capture MESSAGE] -- File: /tmp/wireshark_ethVBBKA3.pcapng*
** (Wireshark:8445) 11:25:29.321752 [Capture MESSAGE] -- Capture Stop ...
** (Wireshark:8445) 11:25:29.368800 [Capture MESSAGE] -- Capture stopped.
```



