

**Objective:** Learn to discover open ports on devices in your local network to understand network exposure.

- ```

kali@kali:~$ sudo apt install nmap
[sudo] password for kali:
Upgrading:
  nmap nmap-common

Summary:
  Upgrading: 2, Installing: 0, Removing: 0, Not Upgrading: 2275
  Download size: 6,329 kB
  Space needed: 882 kB / 41.1 GB available

Continue? [y/n] y
Get1: http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.95+dfsg-3kali1 [1,940 kB]
Get2: http://http.kali.org/kali kali-rolling/non-free amd64 nmap-common all 7.95+dfsg-3kali1 [4,399 kB]
Fetched 6,329 kB in 1s (2,291 kB/s)
(Reading database ... 453262 files and directories currently installed.)
Preparing to unpack .../nmap_7.95+dfsg-3kali1_amd64.deb ...
Unpacking nmap (7.95+dfsg-3kali1) over (7.94+git2023087.3be01efb1dfsg-2kali2-b1) ...
Preparing to unpack .../nmap-common_7.95+dfsg-3kali1_all.deb ...
Unpacking nmap-common (7.95+dfsg-3kali1) over (7.94+git20230807.3be01efb1dfsg-2kali2) ...
Setting up nmap-common (7.95+dfsg-3kali1) ...
Setting up nmap (7.95+dfsg-3kali1) ...
Setup worked! Adding configuration to environment
Processing triggers for kali-menu (2023.4.2) ...
Processing triggers for man-db (2.12.1-1) ...
Processing triggers for wordlists (2023.2.0) ...

```

- ```

kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.254 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::505b:129d:8129:99d2 prefixlen 64 scopeid 0%eth0 link-
ether 88:08:c2:96:03:d4:3b txqueuelen 1000 (Ethernet)
    RX packets 81 bytes 5767 (5.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 42 bytes 4395 (4.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0%lo host-
loop txqueuelen 1000 (Local Loopback)
    RX packets 262285 bytes 13118534 (12.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 262285 bytes 13118534 (12.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

- ```

$ nmap 192.168.1.10 -p -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-22 09:47 EDT
Nmap scan report for 192.168.12.129
Host is up (0.000077s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 8.9p1 (Ubuntu Linux; kernel 5.15)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 2.92 seconds

```

- Step 4: Optionally analyze packet capture with Wireshark.

