NMAP Description

**nmap:**

1. Network exploration tool and security / port scanner.

2. Nmap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many **port scanning techniques**, **version detection** (determine service protocols and application versions listening behind ports), and **TCP/IP fingerprinting** (remote host OS or device identification). Nmap also offers flexible target and port specification, decoy/stealth scanning, sun RPC scanning, and more. Most Unix (linux) and Windows platforms are supported in both GUI and command line modes. Several popular handheld devices are also supported, including the Sharp Zaurus and the iPAQ.

* **Installed size:** 4.44 MB
* **How to install:** sudo apt install **nmap**

3. **Nmap is default in kali Linux**. we can use that very easy.

**Using Nmap:**

Nmap has a lot of features, but getting started is as easy as running nmap scanme.nmap.org. Running nmap without any parameters will give a helpful

list of the most common options, which are discussed in depth in the man page. Users who prefer a graphical interface can use the included Zen map front-end.

**Nmap original websites:** https://nmap.org/

**Nmap Download in Windows, linux, mac :**

**DISCRIPTION:**

****

**Nmap (“Network Mapper”)** is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the “interesting ports table”. That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested.

When an IP protocol scan is requested (-sO), Nmap provides information on supported IP protocols rather than listening ports.

In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and Mac address.