**NMAP is an Open Source Tool**

**Use for Network Discovery & Security Auditing**

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.

### Nmap features include:

* **Host discovery –** Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
* **Port scanning –** Enumerating the open ports on target hosts.
* **Version detection –** Interrogating network services on remote devices to determine application name and version number.
* **OS detection –** Determining the operating system and hardware characteristics of network devices.
* Scriptable interaction with the target
* Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses

**Let’s get started with installation and how to use nmap:**

Install nmap on your kali machine, type command **-** sudo apt install nmap

In order to run the ifconfig command, we need to have net-tools installed on machine, type command - sudo apt install net-tools

**Basic commands,**

**Scan network for connected devices**

**Scan a single IP**



**Scan a host**



**Scan a port**



**Scan using TCP connect**



**Some more basic commands which we can use are :**

**Target Selection**

* Scan a range of IPs – nmap 172.16.44.10-200
* Scan a subnet – nmap 172.16.44.0/24
* Scan targets from Text file – nmap -iL ips.txt

**Port Selection**

* Scan a range of ports – nmap -p 1-100 172.16.44.141
* Scan 100 common ports – nmap -F 172.16.44.141
* Scan all ports – nmap -p- 172.16.44.141
* Specify UDP or TCP scan- nmap -p U:137,T:139 172.16.44.141

**Scan Types**

* Scan using TCP SYN scan – nmap -sS 172.16.44.141
* Scan UDP ports – nmap -sU -p 123,161,162 172.16.44.141
* Scan Selected ports (Ignore Discovery) – nmap -Pn -F 172.16.44.141

**Service and OS Detection**

* Detect OS and Services – nmap -A 172.16.44.141
* Standard service detection – nmap -sV 172.16.44.141
* Aggressive service detection – nmap -sV –version-intensity 5  172.16.44.141

**Output Formats**

* Save default output to file – nmap -oN result.txt 172.16.44.141
* Save results as XML – nmap -oX resultxml.xml 172.16.44.141
* Save formatted results (Grep) – nmap -oG formattable.txt 172.16.44.141
* Save in all formats – nmap -oA allformats 172.16.44.141

**Scripting Engine**

* Scan using default safe scripts – nmap -sV -sC 172.16.44.141
* Get help for a script – nmap –script-help=ssl-heartbleed
* Scan using a specific script – nmap -sV -p 443 -script=ssl-heartbleed 172.16.44.141
* Update script database – nmap –script-updatedb

**Some Useful NSE Scripts**

* Scan for UDP DDOS reflectors – nmap -sU -A -PN -n -pU:19,53,123,161 -script=ntp-monlist,dns-recursion,snmp-sysdescr 172.16.44.2/24
* Gather page titles from HTTP Servers – nmap –script=http-title 172.16.44.141
* Get HTTP headers of web services – nmap –script=http-headers 172.16.44.141
* Find web apps from known paths – nmap –script=http-enum 172.16.44.141
* Find exposed Netbios servers – nmap -sU –script nbtstat.nse -p 137 172.16.44.141