**Nmap:**

Nmap ("Network Mapper") is a utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. 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. It was designed to rapidly scan large networks, but works fine against single hosts.

**Features:**

* 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 – using Nmap Scripting Engine (NSE) and Lua programming language.
* Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses

**Typical Usage:**

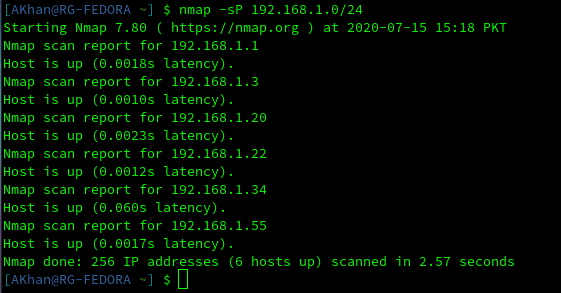
It was built for enterprise-network discovery/documentation but it became a standard in world of networks.

* Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.
* Identifying open ports on a target host in preparation for auditing.
* Network inventory, network mapping, maintenance and asset management.
* Auditing the security of a network by identifying new servers.
* Generating traffic to hosts on a network, response analysis and response time measurement.
* Finding and exploiting vulnerabilities in a network.
* DNS queries and subdomain search

**Sample Commands:**

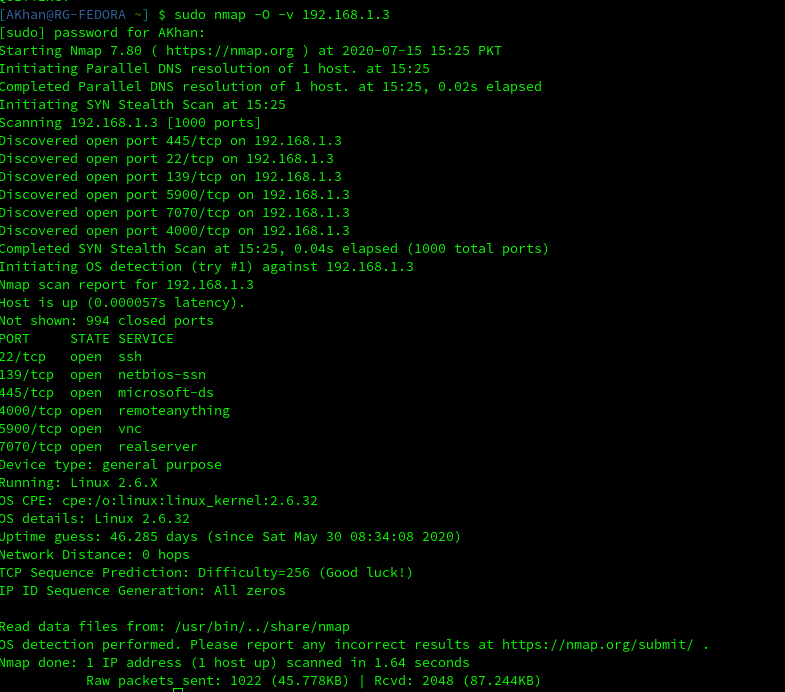
**Scanning a subnet for devices discovery:**

**Command:** nmap -sP 192.168.1.0/24



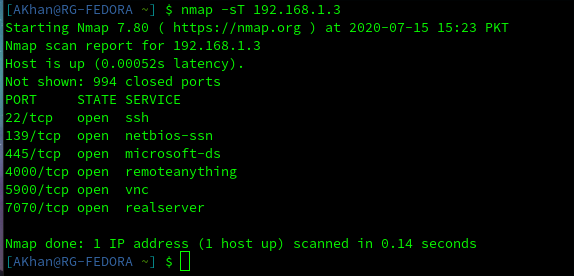
**Detecting OS of a target:**

**Command:** nmap –A 192.168.1.3



**Scanning ports of a target:**

**Command:** nmap -sT 192.168.1.3



**Nmap Broadcast Scan**

**Command:** nmap --script broadcast 192.168.1.3