**Experiment No. 9**

**Name-** Nmap (network mapper)

**Aim:** Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, etc.

**Objectives:** To learn nmap installation & use this to scan different ports.

**Outcomes:** The learner will be able to scan the network using scanning techniques available in NMAP.

NMAP Tool

**Theory:**

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon used to discover hosts and services on a computer network.

Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery.

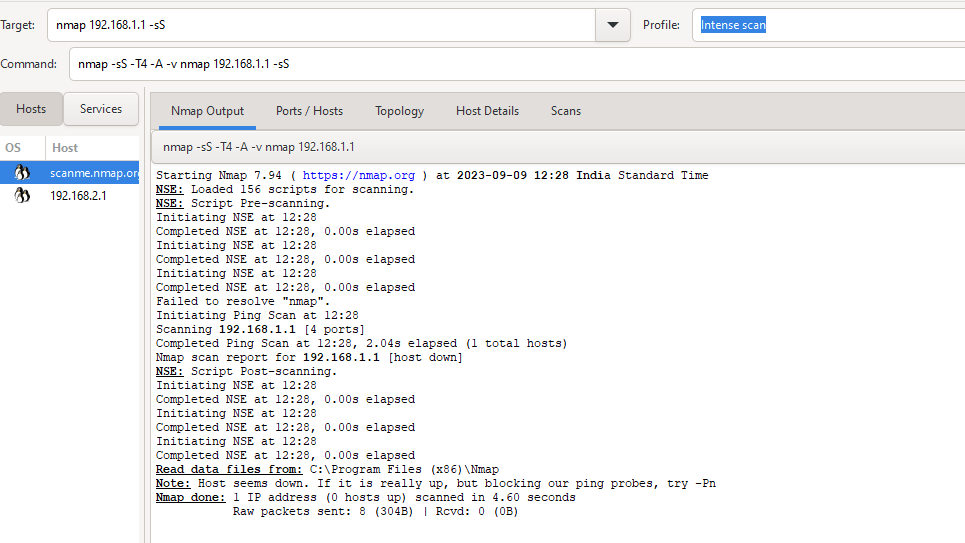
Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.

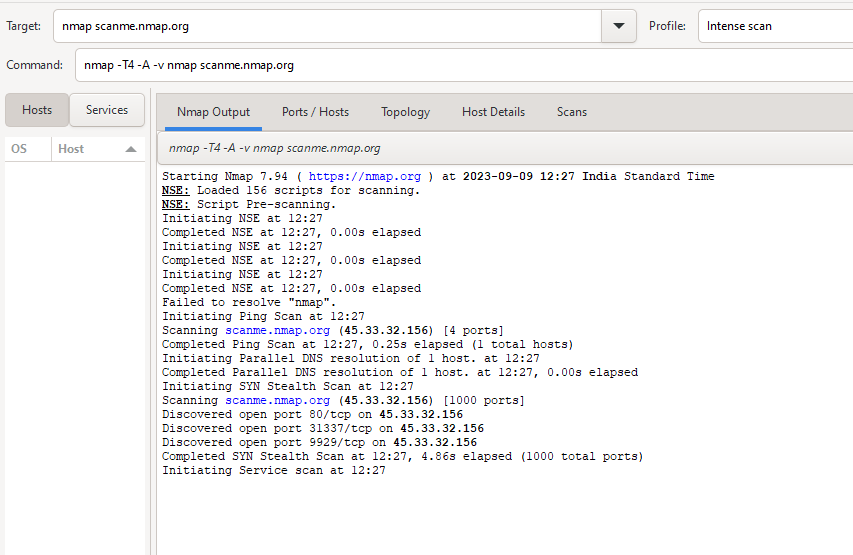
Nmap can be used to monitor single hosts as well as vast networks that encompass hundreds of thousands of devices and multitudes of subnets.

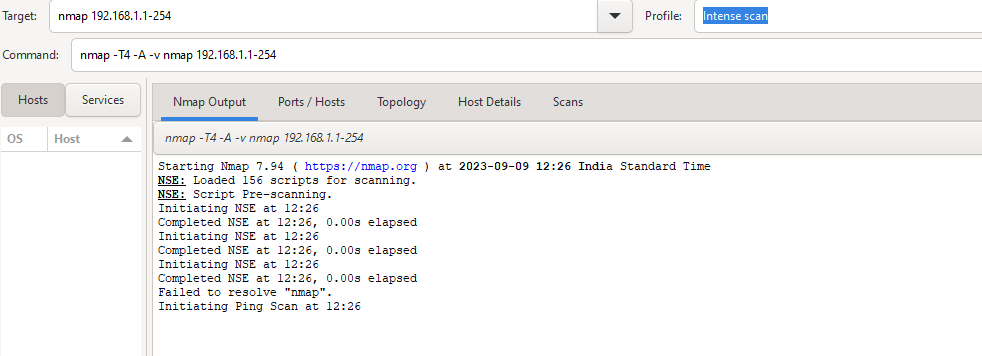
At its core, Nmap is a network scanning tool that uses IP packets to identify all the devices connected to a network and to provide information on the services and operating systems they are running.

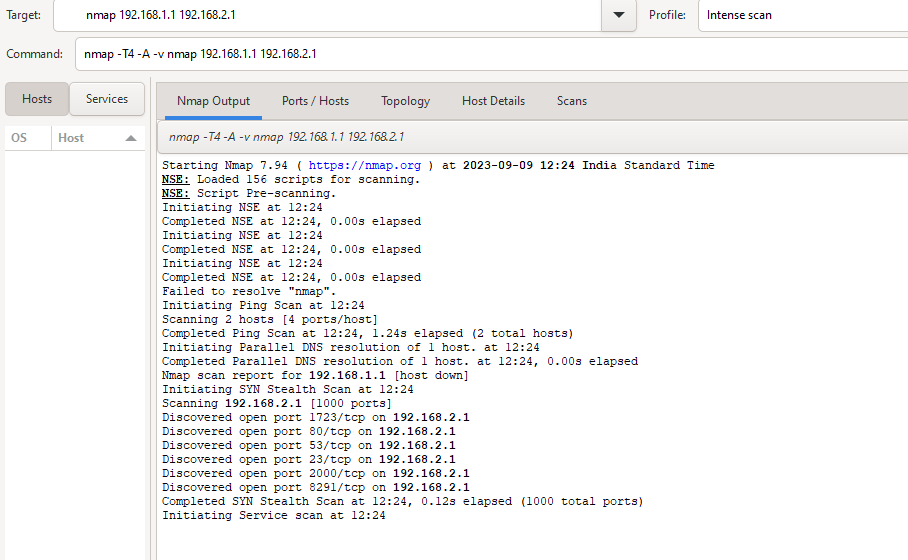
Link for commands- search nmap cheat sheet in google for commands and link is https://www.stationx.net/nmap-cheat-sheet/

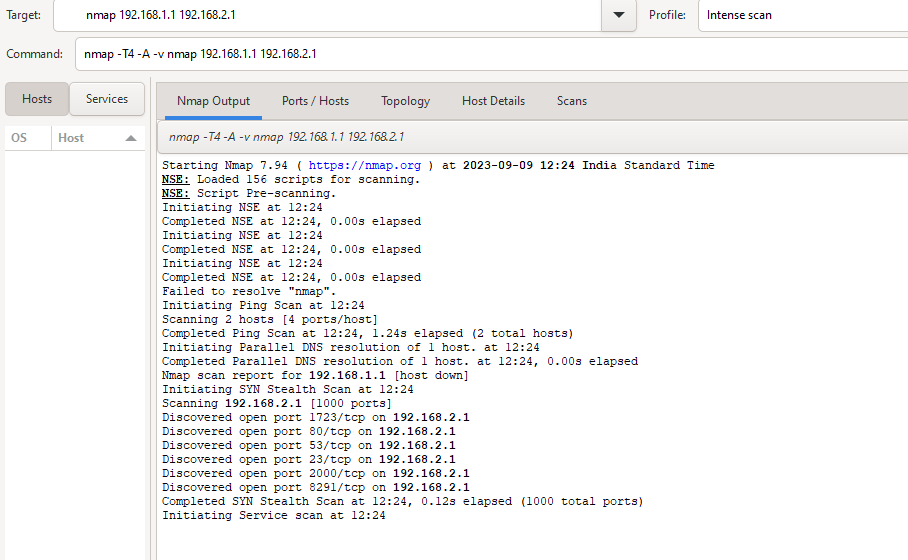
**Output:**











**Conclusion:**

Network scanning provides lot of information about the target network, which is valuable regardless of whether you're trying to attack the network or protect it from attack. Nmap is used to detect IP spoofing and port scanning.