Experiment no.3: Analyze the tool nmap and use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc

Learning Objective: Student should be able to:

- Download, install & use nmap tool
- Understand port scanning
- Understand the how nmap helps to scan various ports
- Explore various nmap options for OS fingerprinting and gathering detailed network and remote hosts information

Tools: nmap tool

Theory:

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyses the responses. Unlike many simple port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions (latency fluctuations, network congestion, the target interference with the scan) during the run. Also, owing to the large and active user community providing feedback and contributing to its features, Nmap has been able to extend its discovery capabilities beyond simply figuring out whether a host is up or down and which ports are open and closed; it can determine the operating system of the target, names and versions of the listening services, estimated uptime, type of device, and presence of a firewall.

Nmap features include:

Host Discovery – Identifying hosts on a network. For example, listing the hosts which respond to pings or have a particular port open.

Port Scanning – Enumerating the open ports on one or more target hosts.

Version Detection – Interrogating listening network services listening on remote devices to determine the application name and version number.

OS Detection – Remotely determining the operating system and some hardware characteristics of network devices.

Basic commands working in Nmap:

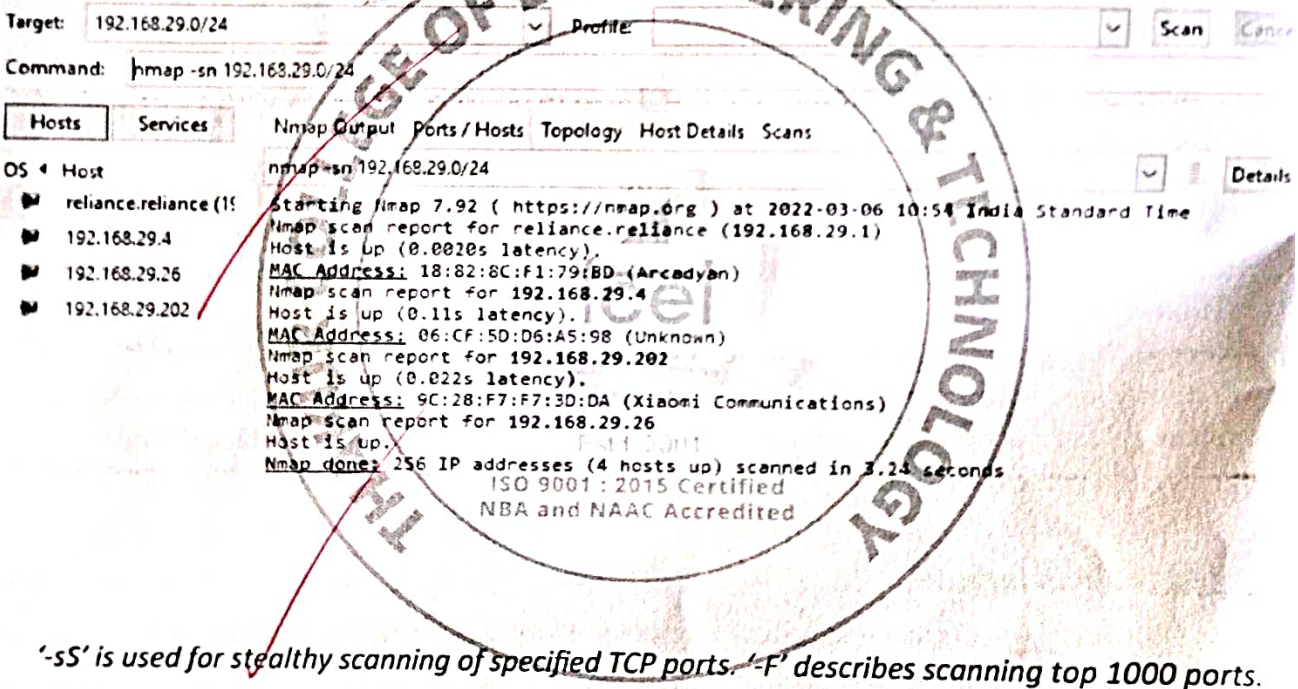
- For target specifications: nmap <target's URL or IP with spaces between them>
- For OS detection: nmap -O <target-host's URL or IP>
- For version detection: nmap -sV <target-host's URL or IP>

SYN scan is the default and most popular scan option for good reasons. It can be performe quickly, scanning thousands of ports per second on a fast network not hampered by restricti firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections

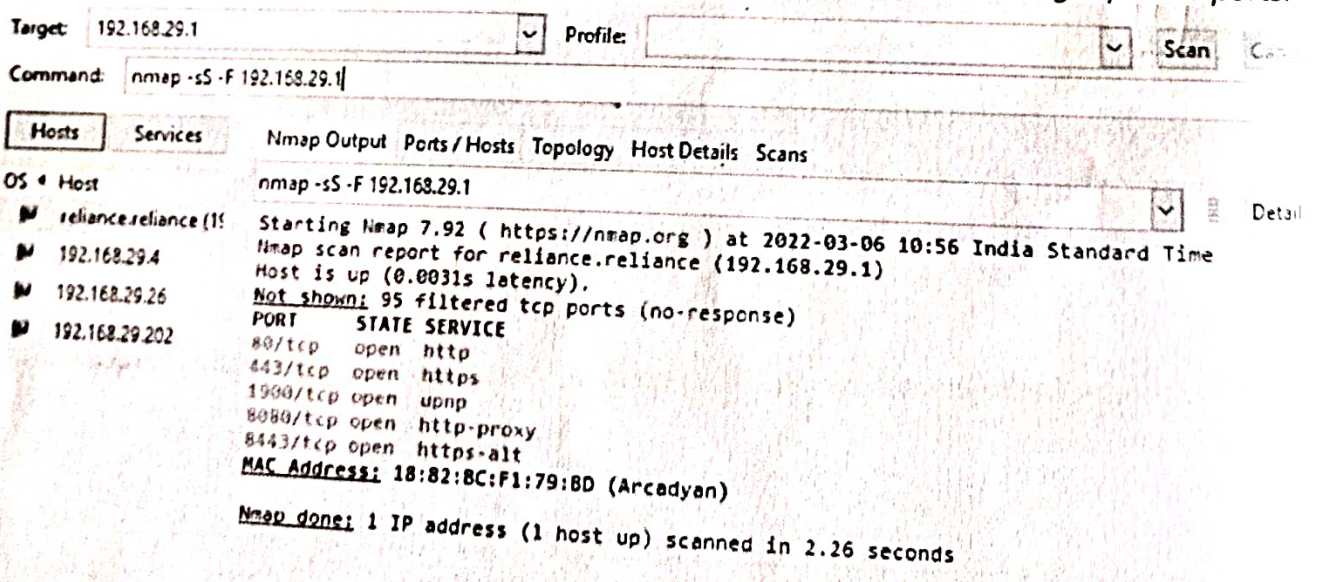
---

Output: *Screenshots of installation & use of various commands using nmap tool*

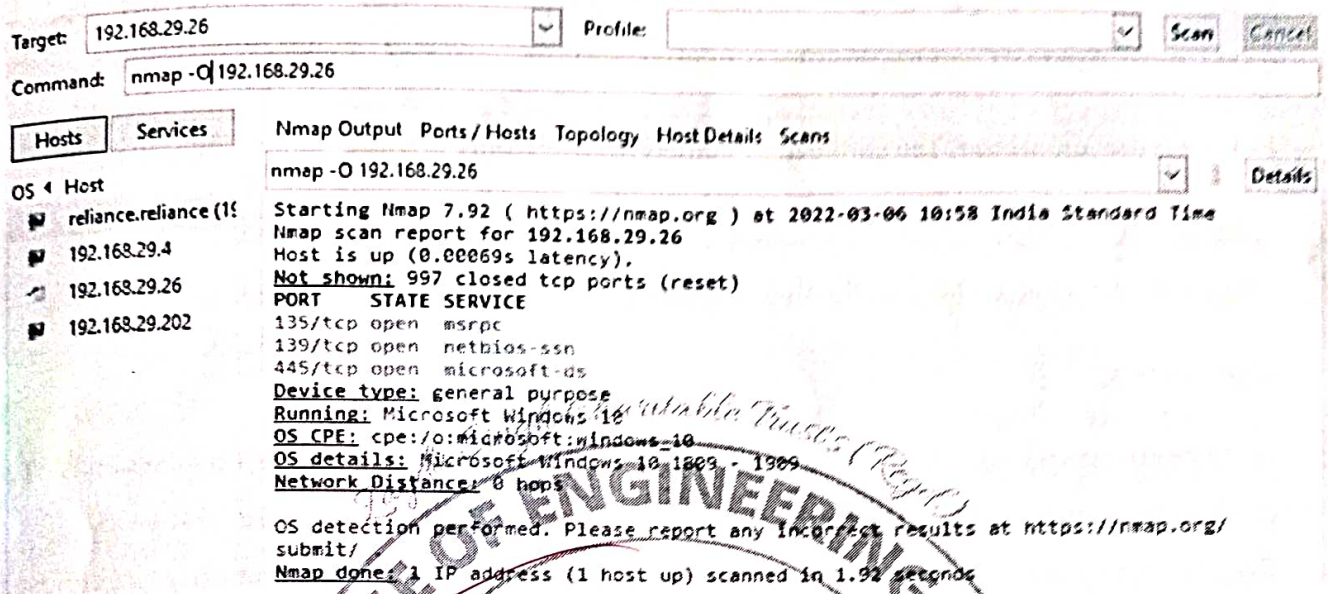
'-sn' is used for scanning all the available hosts in a network



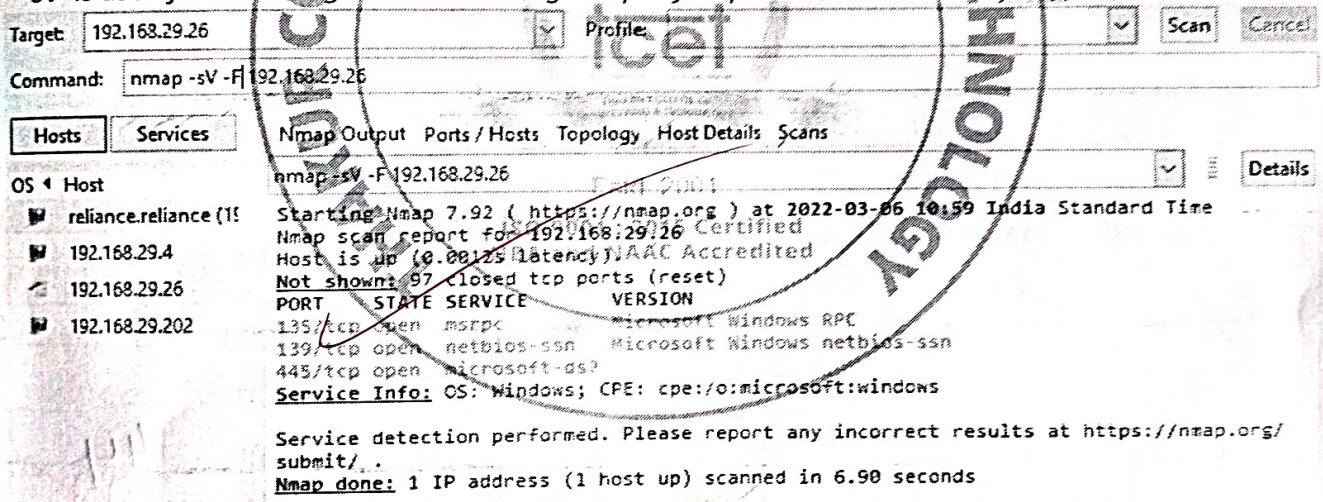
'-sS' is used for stealthy scanning of specified TCP ports. '-F' describes scanning top 1000 ports.



'O' is used for performing OS fingerprinting to determine target's OS.



'-sV' is used for detecting services running on specified ports. '-F' is used to specify top 1000 ports.



Applications:

1. Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications/services.
2. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.