

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:

① Host Discovery – Identifying hosts on a network. For example, listing the hosts which respond to pings or have a particular port open.

② Port Scanning – Enumerating the open ports on one or more target hosts.

③ Version Detection – Interrogating listening network services listening on remote devices to determine the application name and version number.

④ 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 performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive 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

Target: 192.168.29.0/24 Profile: Scan Cancel

Command: nmap -sn 192.168.29.0/24

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans

OS 4 Host

reliance.reliance (192.168.29.1) Starting Nmap 7.92 (https://nmap.org) at 2022-03-06 10:54 India Standard Time
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0020s latency).
MAC Address: 18:82:8C:F1:79:BD (Arcadyan)

192.168.29.4 Nmap scan report for 192.168.29.4
Host is up (0.11s latency).
MAC Address: 06:CF:5D:D6:A5:98 (Unknown)

192.168.29.26 Nmap scan report for 192.168.29.26
Host is up (0.022s latency).
MAC Address: 9C:28:F7:F7:3D:DA (Xiaomi Communications)

192.168.29.202 Nmap scan report for 192.168.29.202
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.24 seconds
ISO 9001 : 2015 Certified
NBA and NAAC Accredited

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

Target: 192.168.29.1 Profile: Scan Cancel

Command: nmap -sS -F 192.168.29.1

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans

OS 4 Host

reliance.reliance (192.168.29.1) Starting Nmap 7.92 (https://nmap.org) at 2022-03-06 10:56 India Standard Time
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0031s latency).
Not shown: 95 filtered tcp ports (no-response)

PORT STATE SERVICE
80/tcp open http
443/tcp open https
1900/tcp open upnp
8080/tcp open http-proxy
8443/tcp open https-alt

MAC Address: 18:82:8C:F1:79:BD (Arcadyan)

Nmap done: 1 IP address (1 host up) scanned in 2.26 seconds

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

Target: 192.168.29.26 Profile: ☐ Scan

Command: nmap -O 192.168.29.26

Hosts **Services** Nmap Output Ports/Hosts Topology HostDetails Scans

OS 4 Host

- reliance.reliance (1)
- 192.168.29.4
- 192.168.29.26
- 192.168.29.202

nmap -O 192.168.29.26 ☐ Details

Starting Nmap 7.92 (<https://nmap.org>) at 2022-03-06 10:58 India Standard Time
Nmap scan report for 192.168.29.26
Host is up (0.00069s latency).
Not shown: 997 closed tcp ports (reset)
PORT **STATE** **SERVICE**
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows-10
OS details: Microsoft Windows 10 1809 - 1909
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at <https://nmap.org/>
submit/.
Nmap done: 1 IP address (1 host up) scanned in 1.92 seconds

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

Target: 192.168.29.26 Profile: ☐ Scan

Command: nmap -sV -F 192.168.29.26

Hosts **Services** Nmap Output Ports/Hosts Topology HostDetails Scans

OS 4 Host

- reliance.reliance (1)
- 192.168.29.4
- 192.168.29.26
- 192.168.29.202

nmap -sV -F 192.168.29.26 ☐ Details

Starting Nmap 7.92 (<https://nmap.org>) at 2022-03-06 10:59 India Standard Time
Nmap scan report for 192.168.29.26
Host is up (0.00125s latency) **Certified**
Not shown: 97 closed tcp ports (reset)
PORT **STATE** **SERVICE** **VERSION**
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at <https://nmap.org/>
submit/.
Nmap done: 1 IP address (1 host up) scanned in 6.90 seconds

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.