LAB Manual

PART A

(PART A : TO BE REFFERED BY STUDENTS)

**Experiment No.02**

**A.1 Aim:**

To study and use of open source tool NMAP.

**A.2 Prerequisite:**

Fundamentals of Security concepts

**A.3 Outcome:**

**After successful completion of this experiment students will be able to** 1. Install open source tool NMAP

2. Apply features of NMAP tool in security domain.

**A.4 Theory:**

Nmap (Network Mapper) is a free and open-source network scanner created by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich). Nmap is used to discover hosts and services on a computer network by sending packets and analysing the responses.

Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan.

Nmap started as a Linux utility and was ported to other systems including Windows, macOS, and BSD. It is most popular on Linux, followed by Windows

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 – 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 uses of Nmap:

* 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

**Zenmap** is the official graphical user interface (GUI) for the Nmap Security Scanner. It is a multiplatform, free and open-source application designed to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scans can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

Link to download NMAP: <https://nmap.org/>

Reference guide link : <https://nmap.org/book/man.html>

Link for installation help : <https://www.ceos3c.com/hacking/nmap-on-windows-complete-beginner-guide/>

Wiki how link: <https://www.wikihow.com/Run-a-Simple-Nmap-Scan>

Basic scanning technique video link :

1. <https://www.youtube.com/watch?v=VXlZ9K3y1so>

2. <https://www.youtube.com/watch?v=wgNIva5nRjA>

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

|  |  |
| --- | --- |
| Roll. No. N049 | Name: Tarun Tanmay |
| Class MBATech CE, 3 Year | Batch: B3 |
| Date of Experiment: | Date of Submission: |
| Grade: | |

**B.1 Theory written by student:**

NMap is an open source tool that is used for scanning of a website or an IP Address. This is used to find vulnerabilities in the system and open ports. This program will scan a target and report which ports are open and which are closed. This will also provide us a list of what softwares are open on that address if so configured. This scanning allows us to probe for vulnerabilities in a system setup and test the security.

**B.2 Input and Output:**

**Installation Screenshots:**

**A screenshot of a cell phone

Description automatically generated**

**Here we see the available resources that can be installed with NMap.**

**A screenshot of a cell phone

Description automatically generated**

**Here we select the destination folder for storing all the files of NMap as it is being installed.**

**A screenshot of a cell phone

Description automatically generated**

**A screenshot of a cell phone

Description automatically generated**

**The status bar shows us the progress of the installation.**

**B.3 Observations and learning:**

**Scan 1:**

**Intense Scan:**

**A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated**

**An intense scan shows us all the data and details generated by the software in its pinging process.**

**A screenshot of a cell phone

Description automatically generated**

**This shows us the path followed to reach the server of the website that we were pinging.**

**Scan 2:**

**Quick Scan**

**A screenshot of a cell phone

Description automatically generated**

**This shows all the different services and ports that were detected by the software**

**A screenshot of a cell phone

Description automatically generated**

**These are the ports and their statuses as picked up by the scan. Filtered means the port is blocked from further investigation by a firewall or some other security.**

**This shows us the path followed to reach the server of the website that we were pinging.**

**B.4 Conclusion:**

**After successful completion of this experiment I am able to**

1. Install open source tool NMAP

2. Apply features of NMAP tool in security domain.