**ST. FRANCIS INSTITUTE OF TECHNOLOGY**

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**SECURITY LAB**

**Experiment – 8: Study of network scanning tool NMAP/ZENMAP**

**Aim:** To scan the network for vulnerabilities using different NMAP/ZENMAP commands.

**Objective:** After performing the experiment, the students will be able to Install and use nmap and use it for gathering detailed network and remote host information.

**Lab objective mapped:** L502.6: Students should be able to Apply network security basics, analyse different attacks on networks and evaluate the performance of firewalls and security protocols, such as SSL, IPSEC, and PGP, and authentication mechanisms to design secure applications.

**Prerequisite:** Basic knowledge of network security.

**Requirements:** Windows OS/Unix/Linux, NMAP or ZENMAP

**Pre-Experiment Theory:**

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon. It is 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 analyzes 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 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

**Implementation & Procedure:**

Zenmap is the official graphical user interface (GUI) for the Nmap Security Scanner. It is a multi-platform, 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.

1. Learn the steps to install Zenmap tool on the system.
2. Study the Zenmap documentation for using its GUI.
3. Scan the network with following scan types.
   1. Ping scan
   2. Quick scan
   3. Intense scan

Choose following targets,

1. scanme.nmap.org
2. Public IP address of SFIT website
3. Observe following features of Zenmap,
   1. Host
   2. Services
   3. Nmap output, Ports/Hosts, Topology, Host Details, Scans
4. Take Screenshots (SS) for all features. Write observations for each SS.

**Post Experimental Exercise-** *(to be handwritten on journal sheets)*

Answer the following Questions:

1. What is Nmap?
2. What is port scanning?
3. Explain the features of Nmap that you have studied.
4. Explain the commands used in Nmap.

**Conclusion:**

In this experiment Network mapping tool ‘Nmap’ was studied and different types of Nmap scans were used to gather host and network related information. We also learned that Nmap is an active reconnaissance tool which directly probes the target/victim for information gathering.

**References:** *(Mention your references here.)*

1. ‘Nmap official website’, <https://nmap.org/> *(Use for installation of Nmap)*
2. “Chapter 12. Zenmap GUI Users' Guide”, https://nmap.org/book/zenmap.html