LAB NO: 8 **Date:**

NMAP

Objectives:

In this lab, students will be able to:

- scan networks and discover devices and hosts on a network, allowing network admin to understand the network more efficiently.
- Port Scanning: Determine which ports are open and which services are running on those ports, which is critical for security assessments and vulnerability scanning.
- OS Fingerprinting: Identify the operating system running on a target host by analyzing various characteristics of network packets.
- Vulnerability Assessment: It's a valuable tool for identifying potential vulnerabilities in systems and services, aiding in proactive security measures.
- Network Monitoring: Nmap can be used for continuous monitoring to detect changes in the network environment.

Description:

Nmap is an open-source network scanning and host discovery tool, which was created by Gordon Lyon and has been actively developed and maintained over two decades. Nmap was first released in 1997 by Fyodor Vaskevitch. Since then, it has grown into one of the most widely used network scanning tools in the world. it has a rich history of development and community contributions, which are constantly expanding its capabilities and ensuring to change according to the ever-changing network security. Nmap allows users to do a bunch of things that are related to a wide range of network-related tasks. Nmap is a network mapper that has emerged as one of the most popular, free network discovery tools on the market. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection. A number of recent cyberattacks have re-focused attention on the type of network auditing that Nmap provides.

Features of Nmap

Nmap offers a wide range of features to its users, including:

1. **Comprehensive Scanning:** Nmap can scan a variety of protocols and perform different types of scans.
2. **Scripting Engine:** Nmap Scripting Engine(NSE) allows users to write and run their custom scripts to automate various tasks of Nmap such as Network auditing and vulnerability scanning.
3. **OS Detection:** Nmap can used to identify the operating system of the target hosts based on their responses to the network probes.
4. **Service and Version Detection:** Nmap can accurately identify the services and versions that are running on the open ports of the target hosts.
5. **Output Formats:** Nmap supports multiple output formats for the scan results like plain text, XML, and greppable output.

LAB EXERCISES

1. Write down the command to do Host Discovery using Nmap tool: To discover hosts on the network, use the following command:

```
sudo nmap -sn www.manipal.edu
```

2. Write down the command to do Port Scanning: To perform a port scan on a specific host, use the following command:

```
sudo nmap -p 1-65535 192.168.1.100
```

3. Write down the command to do a Ping Scan using Nmap

4. Write down the command to do A Host Scan

5.Write down the command to do port scanning using Nmap ie
a.SYN scan b.TCP connect scan c.UDP scans d.TP INIT scan e.TCP NULL

6. Write down the command to do OS Scanning

7. Install Zenmap and perform all the operation as mention for Nmap tool.