PARSHWANATH CHARITABLE TRUST'S

A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering

Data Science

Class: - T.E.D.S. **Semester: - VI**

Subject: Cryptography and System Security **A.Y: - 2023-24**

Experiment No.6

Analyze the network using nmap and netcat

Aim: To analyze the network using tools such as nmap and netcat

Software used: Linux Terminal

Theory:

What is nmap?

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.

Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

Features of Nmap include:

- Ability to quickly recognize all the devices including servers, routers, switches, mobile devices, etc on single or multiple networks.
- Helps identify services running on a system including web servers, DNS servers, and other common applications.
- Nmap can find information about the operating system running on devices.
- During security auditing and vulnerability scanning, you can use Nmap to attack systems using existing scripts from the Nmap Scripting Engine.

There are the following Nmap functions, as follows:

1. Ping Scanning: The ping scanning gives information about every active IP on your Network.
2. Port Scanning: Port scanning is one of the most popular forms of reconnaissance ahead of a hack, helping attackers determine which ports are most susceptible.
   # sS TCP SYN scan
   # sT TCP connect scan
   # sU UDP scans
3. Host scanning
   Host scanning provides a detailed description of a particular host or IP address.
   # Nmap -sp <target IP range>
4. OS Scanning
   OS scanning is the most powerful feature of Nmap. It sends TCP and UDP packets to a port and analyzes the response when using this type of scan.`
   Nmap -O <target IP>

Netcat: The Netcat utility program supports a wide range of commands to manage networks and monitor the flow of traffic data between systems.

Netcat functions as a back-end tool that allows for port scanning and port listening. In addition, you can transfer files directly through Netcat or use it as a backdoor into other networked systems.

Conclusion: Thus we have analyzed the network using nmap and netcat tools.