|  |  |
| --- | --- |
| **Name** | Manish Shashikant Jadhav |
| **UID** | 2023301005 |
| **Subject** | Computer Communication and Networks (CCN) |
| **Experiment No.** | 8 |
| **Aim** | Network Mapping using nmap. |
| **Task 1:** | 1. **Installation and Setup:**  * **Install NMAP on your system if not already installed. (https://www.geeksforgeeks.org/nmap-command-in-linux-with-examples/)** * **Familiarize yourself with the basic syntax and options of NMAP.** |
| **Task 2:** | 1. **Basic Scanning:**  * **Perform a simple ping scan on a target IP address to determine its availability.**      * **Conduct a TCP SYN scan on a target IP range to identify open ports.** |
| **Task 3:** | 1. **Service Version Detection:**  * **Perform a service version detection scan on a target IP to identify the version of services running on open ports.** |
| **Task 4:** | 1. **Operating System Detection:**  * **Use NMAP to detect the operating system of a target device.** |
| **Task 5:** | 1. **Scripting with NMAP:**  * **Write a simple NMAP script to automate a scanning task of your choice.** |
| **Objectives:** | 1. **Scan a given network range and identify all active hosts.**      1. **Identify the top 5 most commonly open ports on a specific target.**      1. **Determine the MAC address of a target device using NMAP.**      1. **Perform a scan to detect the presence of HTTP and HTTPS services on a target network.**      1. **Find out if a particular host has FTP service running on it.**      1. **Identify the SSH version running on a given host.**      1. **Scan a range of IP addresses and list all hosts that have Telnet service running.**      1. **Determine the operating system of a target host using NMAP.**      1. **Identify any SQL services running on a given network.**      1. **Find out if a specific host has Remote Desktop Protocol (RDP) enabled.**      1. **Scan a target network and determine if any hosts are running DNS services.**      1. **Detect if a host has SNMP (Simple Network Management Protocol) enabled.**      1. **Perform a scan to identify any SMTP (Simple Mail Transfer Protocol) servers on a network.**      1. **Determine if a target network has any active FTP servers allowing anonymous login.**      1. **Find out if any hosts in a network are running vulnerable versions of the Apache HTTP server.**      1. **Detect if a target host has any open NFS (Network File System) shares.**   **17. Identify the presence of any MySQL database servers on a given network.**  **18. Scan a network to determine if any hosts have the Remote Procedure Call (RPC) service running.**  **19. Detect if a specific host has any open VNC (Virtual Network Computing) ports.**  **20. Perform a scan to identify any hosts with the Secure Shell (SSH) service running on non-default ports.** |
| **Conclusion** | Hence, by completing this experiment I came to know about Installation and configuration of FTP server. |