Task 1: Basic Network Scanning using Nmap

Name: Daniya shaikh

Internship: OASIS INFOBYTE (OIBSIP)

Objective

The objective of this task was to perform a basic network scan on the local machine using **Nmap** to identify open ports and running services.

Tool Used

- **Nmap version:** 7.98

Platform

- **Operating System:** Microsoft Windows 10

Command Executed

nmap localhost

Scan Summary

- **Target:** localhost (127.0.0.1)
- **Host Status:** Up
- **Latency:** 0.00 seconds
- **Total Ports Scanned:** 1000
- **Closed Ports:** 997
- **Open Ports:** 3

Scan Results

Port	State	Service
80	Open	HTTP
135	Open	MSRPC
445	Open	Microsoft-DS (SMB)

Analysis

Task 1: Basic Network Scanning using Nmap

- **Port 80 (HTTP):** Indicates a web service running on the local machine.
- **Port 135 (MSRPC):** Used for Microsoft Remote Procedure Call services.
- **Port 445 (Microsoft-DS):** Associated with Windows file sharing (SMB).

The presence of these ports suggests that standard Windows services and a web service are active on the system.

Conclusion

The Nmap scan successfully identified open ports and active services on the local machine. This basic scan demonstrates how Nmap can be used for network reconnaissance and security assessment by detecting exposed services that may require monitoring or hardening.
