NAME : Shrishti Vishwakarma

CLASS : BVOC (First year) Sem 2

TITLE : Upgrading the Working of a Port Scanner

INSTRUCTOR : Shubham Sir

TABLE OF CONTENT

INTRODUCTION

Port scanning is a crucial technique in cybersecurity that helps identify open ports and services on a network. This project focuses on upgrading the functionality of a basic port scanner by integrating it with Nmap using Python. The upgraded scanner allows for more advanced features such as OS detection, service version detection, and more detailed results. This enhancement makes it suitable for network administrators and security professionals to perform comprehensive network audits.

OBJECTIVE

- To develop an advanced and automated port scanner.
- To integrate Python with the Nmap tool using the python-nmap library.
- To enable scanning for open ports, service detection, and OS fingerprinting.
- To help users identify potential vulnerabilities in a network.

TOOLS USED

- Python
- Nmap
- python-nmap library

METHODOLOGY

1. Environment Setup:
   - Installed Nmap and Python on the system.
   - Installed the 'python-nmap' library using pip.

2. Script Development:
   - Wrote a Python script that utilizes the Nmap tool for scanning.
   - Enabled options for basic scans, OS detection, and service version checks.

3. Execution:
   - Run the script on a local or remote IP.
   - Display and log the scan results in a structured format.

4. Testing:
   - Tested on localhost and simulated vulnerable machines.

- Verified detection of open ports, services, and OS details.

RESULTS

The script successfully performed various types of scans, including:

- Fast scans for open ports.
- Service and version detection.
- OS fingerprinting.

CONCLUSION

This project demonstrates the enhancement of a basic port scanner using Python and Nmap. By integrating the python-nmap library, the scanner became capable of providing deeper insights into a network's security status. This project highlights the importance of automation and tool integration in cybersecurity.