Nmap Project Report

Project Title: Basic Network Scanning and Vulnerability Mapping Using Nmap

Author: Maureen Chepkemoi Mibei

Location: Dubai, UAE

Objective

To perform a basic scan of a test network using Nmap, identify open ports and services, and analyze potential vulnerabilities. This project demonstrates foundational skills in network reconnaissance, documentation, and cybersecurity analysis.

Tools Used

- **Operating System:** Ubuntu
- **Scanner:** Nmap
- **Target:** Localhost (127.0.0.1) and Metasploitable2 VM
- **Commands used**: nmap –sv 127.0.0.1

Results Summary

- **Open Ports Identified:**
  - Port 22 (SSH) – Open
  - Port 80 (HTTP) – Open
  - Port 139 (NetBIOS) – Open
  - Port 445 (SMB) – Open
- **Service Versions:**
  - Apache 2.2.8
  - OpenSSH 4.7p1
- **OS Detection:**
  - Linux 2.6.X (Ubuntu-based)

Vulnerability Analysis

- **Apache 2.2.8**: Known vulnerabilities include directory traversal and denial of service
- **SMB ports (139/445)**: Susceptible to exploits like Eternal Blue if unpatched
- **Recommendations:**
  - Update Apache to the latest stable version
  - Disable unused services
  - Apply firewall rules to restrict access to sensitive ports

Documentation & Reflection

- Created a structured report with findings and screenshots
- Improved command-line fluency and scanning techniques