MIT World Peace University

Vulnerability Identification and Penetration Testing

Assignment 2

Naman Soni Roll No. 06

Contents

1 Title

Find sweep IP ranges for live.

2 Theory

2.1 *Introduction to Nmap*

Nmap, short for "Network Mapper" is a versatile and powerful open-source tool primarily used for network exploration, security auditing, and vulnerability scanning. Developed by Fyodor, it allows users to discover hosts and services on a computer network, finding open ports, identifying operating systems, and detecting potential vulnerabilities. With its flexible scanning techniques and scripting capabilities, Nmap is widely used by network administrators, security professionals, and ethical hackers to assess and secure networks.

2.2 *It's need/purpose of Nmap*

The primary purpose of Nmap is to scan computer networks to discover hosts, services, open ports, and operating systems. It serves as a vital tool for network exploration, security auditing, and vulnerability assessment, helping administrators and security professionals identify potential security risks and weaknesses in their networks.

2.3 *Advantages*

- **Versatility:** Offers a wide range of scanning techniques.
- Open Source: Free to use, modify, and distribute.
- Cross-Platform Compatibility: Works on various operating systems.
- Comprehensive Scanning: Identifies hosts, services, ports, OS, and vulnerabilities.
- Scripting Engine (NSE): Allows customization and automation.
- Efficiency: Scans large networks quickly and accurately.
- Stealth Capabsdilities: Conducts discreet scans to evade detection.
- Multiple Output Formats: Provides flexible output options.
- Community Support: Active community for assistance and documentation.