Name- Jay S. Chatpalliwar

PRN-21510018

Assignment 13

Exploring a Vulnerability Assessment Tool

**Nmap (Network Mapper)**

**Overview**

Nmap is a powerful, flexible, and free open-source tool used by network administrators and security professionals for network discovery, security auditing, and vulnerability assessment.

**Key Features**

1. **Host Discovery**: Identifies live hosts on a network.
2. **Port Scanning**: Determines open ports on target systems.
3. **Service/Version Detection**: Identifies services running on open ports and their versions.
4. **OS Detection**: Attempts to determine the operating system of target hosts.
5. **Scriptable Interaction**: Uses Nmap Scripting Engine (NSE) for advanced probing.

**Common Use Cases**

* Network inventory
* Managing service upgrade schedules
* Monitoring host or service uptime
* Discovering open ports
* Detecting security risks
* Auditing the security of a network

**Basic Usage**

Copy

nmap [Scan Type] [Options] {target}

Example: Scan a single IP

Copy

nmap 192.168.1.1

**Advanced Features**

* **Firewall/IDS Evasion Techniques**: Various methods to bypass security measures.
* **Output Formats**: Supports multiple output formats including XML, grepable, and normal.
* **Zenmap**: GUI version of Nmap for easier use.

**Limitations**

* Can be detected by advanced intrusion detection systems
* Intensive scans can be resource-heavy and time-consuming
* Requires root/administrator privileges for certain scan types

**Ethical Considerations**

Always obtain proper authorization before scanning networks you don't own or manage. Unauthorized scanning can be illegal and unethical.