Vulnerability Scanning using NMAP and Nessus

1. Introduction

Vulnerability scanning is a process of identifying security weaknesses and vulnerabilities in a system or network. Two of the most commonly used tools for vulnerability scanning are NMAP and Nessus.

2. NMAP (Network Mapper)

NMAP is an open-source tool for network discovery and security auditing. It is used to:

- - Discover hosts and services on a network
- - Identify open ports
- - Detect operating systems and versions
- - Perform network inventory and manage service upgrade schedules

Key NMAP Commands:

1. Scan a single host: `nmap 192.168.1.1`

2. Scan multiple IPs: `nmap 192.168.1.1 192.168.1.2`

3. Scan an entire subnet: `nmap 192.168.1.0/24`

4. Scan for specific ports: `nmap -p 22,80,443 192.168.1.1`

5. Detect OS and services: `nmap -A 192.168.1.1`

3. Nessus

Nessus is a widely used vulnerability scanner developed by Tenable. It scans for vulnerabilities, misconfigurations, and compliance issues in operating systems, applications, and devices.

Key Features of Nessus:

- - Over 50,000 plugins for vulnerability detection
- - Detects CVEs, missing patches, and configuration issues
- - Intuitive web-based interface for scanning and reporting
- - Supports both credentialed and non-credentialed scans

Steps to Use Nessus:

1. Install Nessus and activate with a license.

2. Create a scan by selecting a scan template (e.g., Basic Network Scan).

3. Configure scan targets and credentials (if needed).

4. Run the scan and review results.

5. Export the scan report for remediation.

4. NMAP vs Nessus - A Comparison

Feature	NMAP	Nessus
Primary Use	Network mapping & port scanning	Vulnerability scanning
License	Free & open-source	Commercial (free trial available)
User Interface	Command-line	Web-based GUI
Vulnerability Detection	Limited	Extensive (with CVEs, plugins)
Ease of Use	Requires CLI knowledge	User-friendly interface

5. Conclusion

Both NMAP and Nessus are essential tools in the cybersecurity toolkit. While NMAP is more focused on network discovery, Nessus provides comprehensive vulnerability assessment capabilities. Mastering both tools is critical for any ethical hacker or security analyst.