Nessus Usage Procedure

# Introduction

Nessus is a vulnerability assessment tool developed by Tenable. It scans systems, applications, and networks to identify vulnerabilities including misconfigurations, missing patches, and weak credentials. Nessus is commonly used for vulnerability assessments and penetration testing (VAPT).

# Types of Scans

* Host Discovery: Identifies live hosts and open ports for quick network mapping.
* Ping-Only Discovery: Uses ICMP pings to detect online systems with minimal traffic.
* Basic Network Scan: Performs a full vulnerability scan suitable for most hosts; detects software flaws and misconfigurations.
* Credential Validation: Tests login credentials for authenticated scans, increasing accuracy.
* Advanced Scan: Customizable scan for experts; allows tuning of ports, plugins, etc.
* Malware Scan: Checks for known malware on Windows and Unix systems.
* Agent Reset: Manages Nessus Agents for distributed scans; useful for troubleshooting communications.
* Mobile Device Scan (upgrade required): Assesses mobile devices via Microsoft Exchange or MDM.
* Credentialed Patch Audit: Authenticates hosts to check for missing security patches.
* Active Directory Starter Scan: Detects AD misconfigurations.
* AI Vulnerabilities: Finds AIML-related risks in AI-driven applications.

# Installing Nessus

1. Download Nessus from Tenable’s official website and follow installation instructions for your OS.
2. After installation, register Nessus (free or paid license).
3. Start the Nessus service and access the web interface on default port 8834.

# Basic Configuration

1. Log in to the Nessus web interface.

2. Create a New Scan: Click 'New Scan' and select the appropriate template (Basic Network Scan, Host Discovery, etc.).

3. Configure Scan Settings: Enter target IP addresses or hostnames, define credentials for authenticated scans (Windows/Unix, HTTP, SSH, etc.), fine-tune scan options (ports, plugins, schedule).

4. Save and launch the scan.

# Reviewing Results

After the scan completes, view the report in the web interface. Examine findings for vulnerabilities such as missing patches, outdated software, and weak configurations. Evaluate Nessus risk ratings and recommended mitigations.

# Common Findings and Remediation

* Missing Security Patches: Apply all recommended updates from Nessus results.
* Outdated Software: Update critical services such as Node.js, Apache, Tomcat, etc.
* Weak SSL/TLS: Disable old protocols (SSLv2, SSLv3, TLS 1.0/1.1), enforce strong ciphers and TLS 1.2/1.3.
* Open SSH Configurations: Disable root login and outdated algorithms; enforce key-based authentication.
* SMB Signing (Windows): Enable via Group Policy to avoid MITM attacks.
* Backdoors (DVWA, UnrealIRCd, Bind Shell): Sanitize user inputs, rebuild compromised systems, enforce strong passwords, and restrict default credentials.
* HTTP Response Header Issues: Add security headers like X-Frame-Options, Content-Security-Policy, etc., to web server configs.

# Advanced Exercises

* Scanning Virtual Machines: Configure target VMs (e.g., Metasploitable, Windows 11) and perform scans using tailored credentials.
* Web Application Scanning: Enable specific plugins for web vulnerabilities like SQL injection, XSS, weak cookies, etc.
* Privilege Escalation Checks: Use commands (find, make, git, script, join) to identify SUID binaries and test escalation risk, referencing GTFOBins for exploit scenarios.

# Advantages and Disadvantages

## Advantages:

* Comprehensive coverage (OS, apps, devices)
* Regular plugin and CVE updates
* Automated, scheduled scanning
* Customizable scan policies
* User-friendly interface and detailed reports
* Compliance check support

## Disadvantages:

* Paid version is costly; free version is limited
* May generate false positives
* Detects but cannot exploit vulnerabilities
* Resource intensive for large scans
* Free version scans up to 16 IPs only

# Uses of Nessus

* Vulnerability scanning and assessment for networks
* Patch management
* Configuration auditing of servers, firewalls, routers
* Compliance validation against standards
* Asset discovery
* Pre-penetration testing reconnaissance