Nessus Tool Tutorial

Introduction

Nessus is a powerful vulnerability scanning tool used by security professionals to identify potential security issues within networks and systems. Developed by Tenable, Nessus provides comprehensive scans, detecting vulnerabilities, misconfigurations, and compliance issues. It is essential for vulnerability management and risk assessment.

Key Features

- In-depth vulnerability scanning and reporting.
- Pre-configured templates for various environments.
- Integration with security information and event management (SIEM) tools.
- Detailed remediation recommendations.

Installation

On Linux

1. Download Nessus from the official Tenable website.
2. Install the downloaded package:
3. sudo dpkg -i Nessus-<version>.deb # For Debian/Ubuntu
4. sudo rpm -ivh Nessus-<version>.rpm # For CentOS/RedHat
5. Start the Nessus service:
6. sudo systemctl start nessusd.service
7. Access Nessus via your browser at https://localhost:8834.

On macOS

1. Download the Nessus installer for macOS from the Tenable website.
2. Open the installer and follow the installation prompts.
3. Start Nessus and access it at https://localhost:8834.

On Windows

1. Download the Nessus installer from the official website.
2. Run the installer and follow the setup instructions.
3. Start Nessus from the application menu and access it at https://localhost:8834.

Basic Usage

Setting Up Nessus

1. Open your browser and navigate to https://localhost:8834.
2. Create an account and enter the activation code provided by Tenable.
3. Choose the scan templates you want to configure and download plugins.

Running a Basic Scan

1. Log in to the Nessus dashboard.
2. Click New Scan and choose a scan template (e.g., Basic Network Scan).
3. Enter a name and the target IP address or range.
4. Save the scan and click Launch.
5. View scan results under the Completed Scans section.

Reviewing Scan Results

- Open the completed scan to view identified vulnerabilities.
- Click on a specific vulnerability to see details like CVSS score, affected assets, and remediation steps.

Advanced Usage

Customizing Scan Templates

1. Select a scan template and click Configure.
2. Adjust settings like scan policies, port ranges, and plugins.
3. Save the customized template for future scans.

Scheduled Scans

1. Create or select a scan.
2. Set a schedule by choosing Advanced Settings > Schedule.
3. Define the frequency (e.g., daily, weekly) and start time.

Exporting Reports

1. Open a completed scan.
2. Click Export and choose the desired format (PDF, CSV, or HTML).
3. Save the file for analysis or sharing.

Integration with SIEM Tools

1. Export scan data in a compatible format.
2. Import the data into your SIEM tool for correlation and monitoring.

Tips and Tricks

- Always update Nessus plugins to ensure scans cover the latest vulnerabilities.
- Use the Policy Compliance Auditing feature to check against industry standards like PCI DSS or HIPAA.
- Leverage Agent-Based Scanning for remote systems or those with intermittent connectivity.
- Regularly review and fine-tune scan policies to reduce false positives.

Examples

Example 1: Scanning a Subnet

1. Log in to Nessus and create a new scan using the Basic Network Scan template.
2. Enter the subnet range (e.g., 192.168.1.0/24) as the target.
3. Launch the scan and monitor its progress.
4. Review the results to identify vulnerable devices within the subnet.

Example 2: Credentialed Scanning

1. Create a new scan and configure it with valid credentials for the target system.
2. Add credentials under the Settings > Credentials tab (e.g., SSH or Windows credentials).
3. Launch the scan to identify vulnerabilities that require authentication to detect.

Example 3: Exporting a Report

1. After completing a scan, click on the scan name to view details.
2. Click Export and select PDF for a comprehensive report.
3. Share the report with stakeholders for review and remediation planning.

Conclusion

Nessus is a robust tool for identifying vulnerabilities and ensuring compliance with security standards. Its flexibility, detailed reporting, and advanced features make it indispensable for any vulnerability management program. Use Nessus responsibly to enhance your organization's security posture and reduce risks.