vulnerability-management with NESSUS

Lab Overview

This lab guide will walk you through setting up and using Nessus Essentials (formerly Nessus Home) for vulnerability scanning and management.

Task 1: Installation and Initial Setup

1. Download Nessus Essentials
    - Visit https://www.tenable.com/products/nessus/nessus-essentials
    - Register for a free activation code
    - Download the appropriate package for your OS
2. Initial Configuration
    - Access https://localhost:8834
    - Accept the SSL warning
    - Create an admin account
    - Enter your activation code
    - Wait for initial plugin download (may take 15-30 minutes)

Task 2: Basic Scanning

1. Create Your First Scan
    - Click "New Scan"
    - Select "Basic Network Scan"
    - Configure scan settings:
        - Name: "First Basic Scan"
        - Description: "Initial vulnerability assessment"
        - Targets: Enter your target IP (e.g., your local IP@)

Task 3: Advanced Scanning Techniques

1. Credentialed Scans
    - Create a new scan using "Credentialed Patch Audit"
    - Configure credentials:

```
Windows:
- Domain or local username
- Password

Linux:
- SSH username
```

```
- Password or SSH key
- Elevation method (sudo/su)
```

Task 4: Results Analysis

1. Understanding Scan Results
    - Vulnerability severity levels:
        - Critical (CVSS 9.0-10.0)
        - High (CVSS 7.0-8.9)
        - Medium (CVSS 4.0-6.9)
        - Low (CVSS 0.1-3.9)
        - Info (CVSS 0.0)
2. Remediation Planning
    - Sort vulnerabilities by:
        - Risk (CVSS score)
        - Exploit availability
        - Ease of remediation
        - Business impact
3. Creating Reports
    - Generate executive summary
    - Detailed technical reports
    - Compliance reports
    - Delta reports for changes