Network Vulnerability Scanning using Nessus

Introduction

In today's digital environment, networks are constantly exposed to security threats and vulnerabilities. Vulnerability assessment is a critical process used to identify, evaluate, and mitigate security weaknesses in network systems before they can be exploited by attackers. Nessus is one of the most widely used vulnerability scanning tools that helps security professionals detect misconfigurations, outdated software, open ports, and known security flaws.

Theory

To perform a network vulnerability scan using Nessus, we first set up the Nessus scanner, define the target network range, configure scan policies with required checks, initiate the scan, analyze the results, prioritize critical vulnerabilities, and take corrective actions.

Nessus works by sending probes to network devices, analyzing responses, identifying vulnerabilities, and generating a detailed report for remediation.

Procedure

1. Install Nessus

Use the following command to install Nessus:

```
# dpkg -i Nessus-10.8.3-ubuntu1604_amd64.deb
```

Screenshot: Installation Process

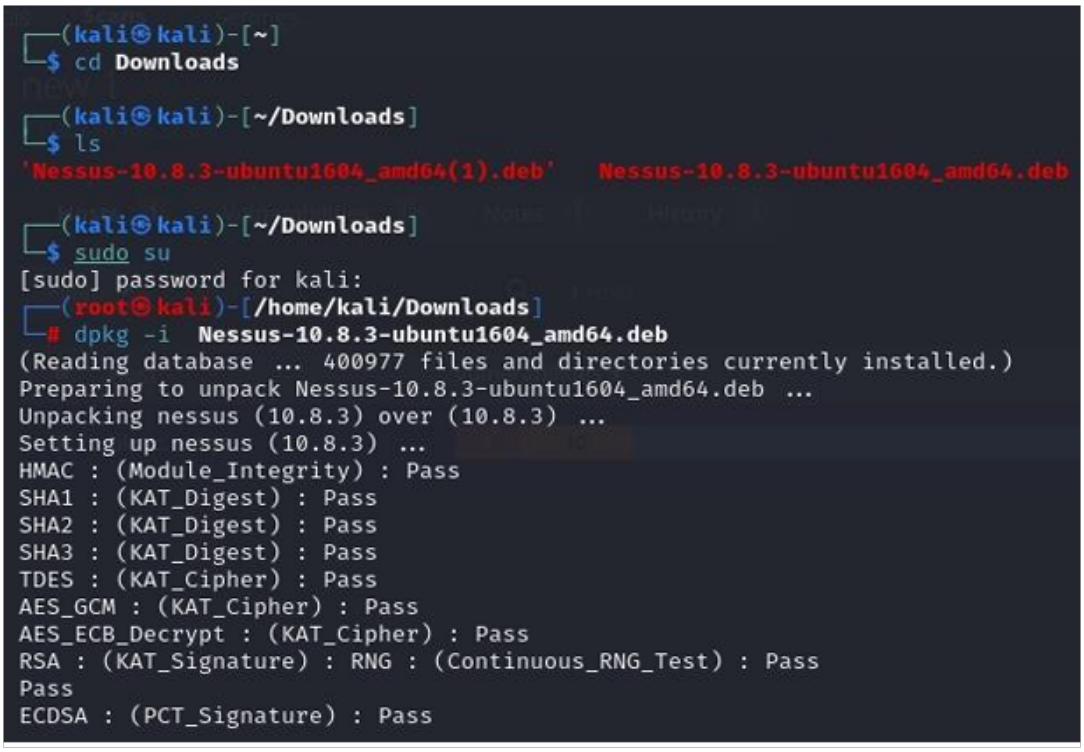

Figure 1: Nessus Installation

2. Start Nessus Service

Start the Nessus service:

```
# service nessusd start
```

Check service status:

```
# service nessusd status
```

Screenshot: Service Started

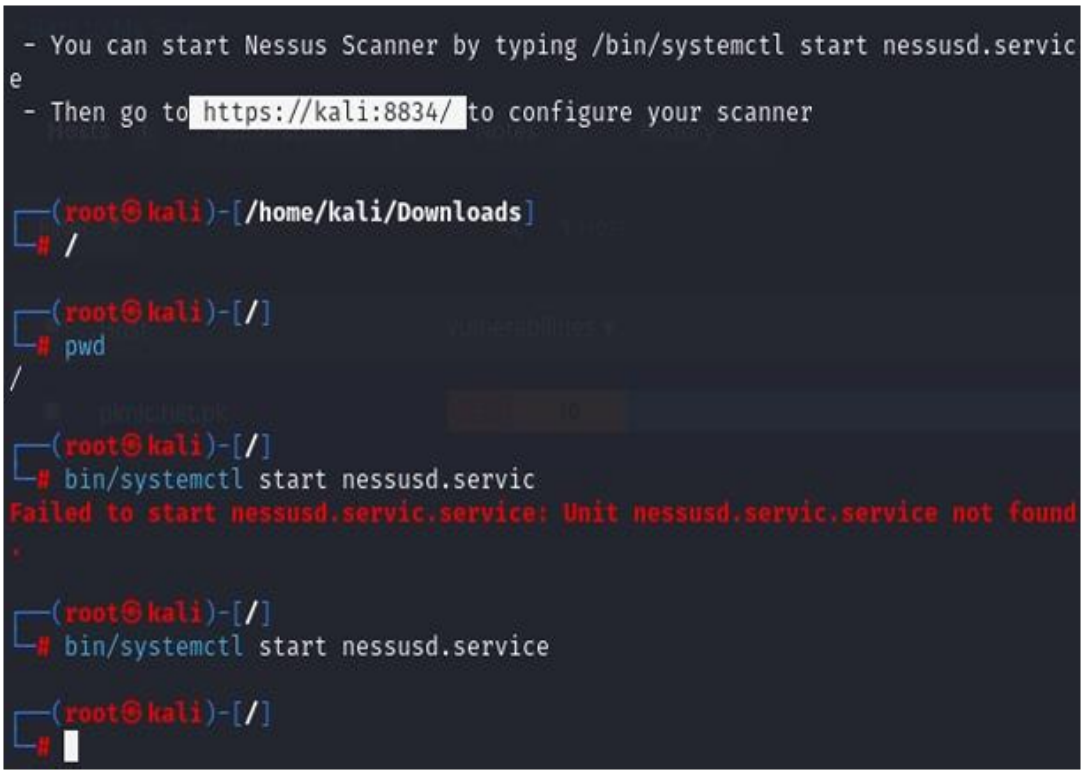

Figure 2: Nessus Service Status

3. Initial Setup

Open browser and access:

```
https://localhost:8834/
```

Register offline and create a new user account with username and password.
Screenshot: Nessus Dashboard Login

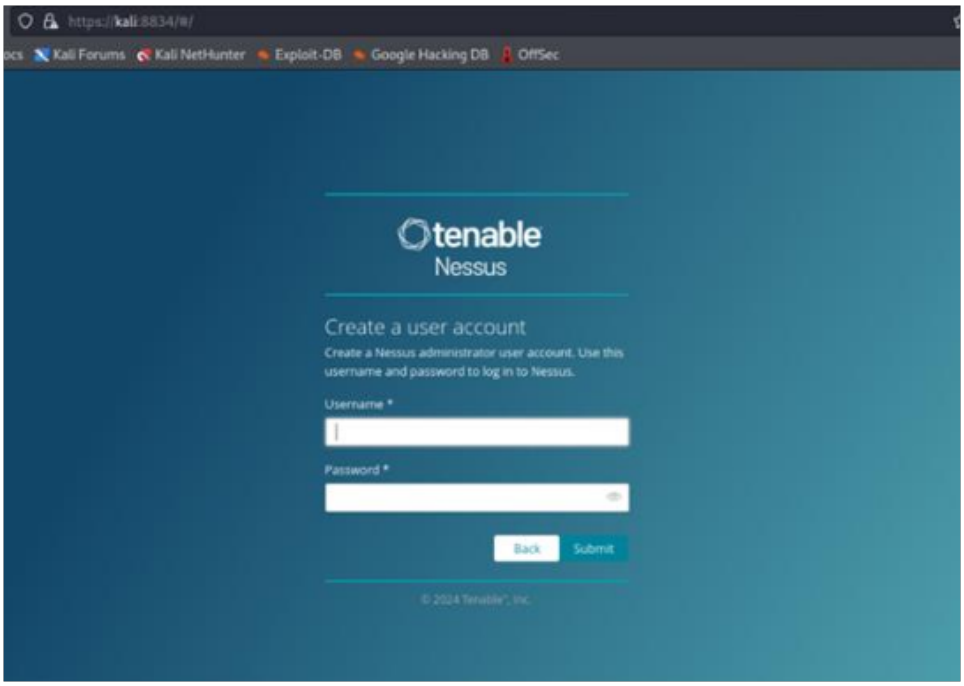

Figure 3: Nessus Login Dashboard

Performing Vulnerability Scan

4. Create New Scan

- Navigate to **Scans**
- Click on **New Scan**
- Select **Basic Network Scan**

Screenshot: New Scan Template

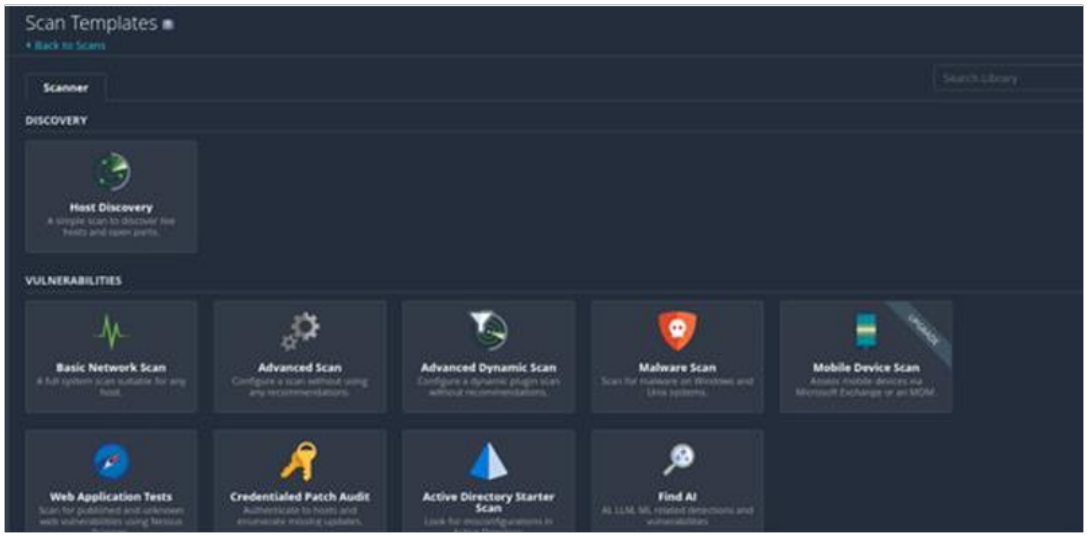

Figure 4: Basic Network Scan Template

5. Configure Scan Settings

Fill in:

- Name: Internal Network Scan
- Target: Enter IP address or range (e.g., 192.168.1.0/24)
- Description: Provide scan details
- Save output in scan folder

Screenshot: Scan Configuration

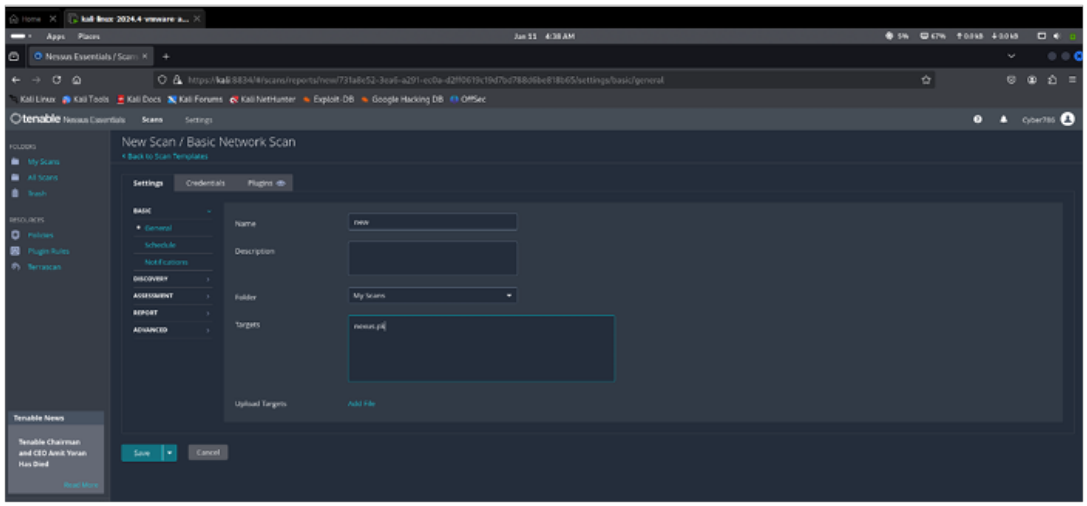

Figure 5: Scan Configuration Settings

6. Launch the Scan

- Click **Save**
- Click **Launch**

7. Monitor Scan Progress and View and Analyze Results

Monitor scan under the **Scans** tab. The dashboard shows:

- Percentage completed
- Time elapsed
- Vulnerabilities detected

After completion, Nessus generates a detailed report categorizing vulnerabilities by severity:

- Critical
- High

- Medium
- Low
- Informational

Screenshot: Vulnerability Report

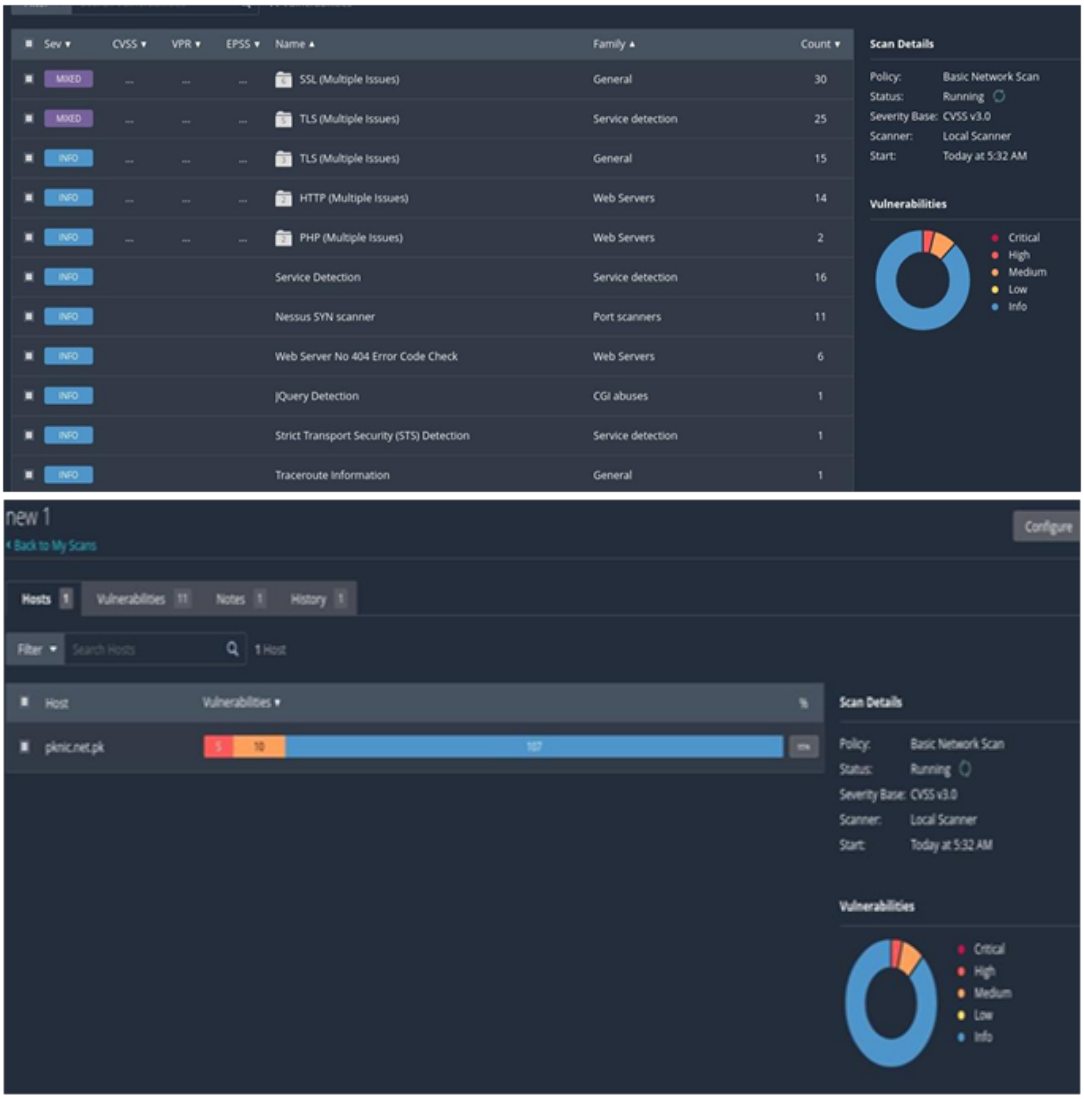

Figure 6: Vulnerability Scan Results

Conclusion

Nessus is a powerful vulnerability assessment tool used to identify security weaknesses in networks. In this practical, we installed Nessus on Kali Linux, started its service, configured the scanner through the web interface, created a Basic Network Scan, and analyzed the results.

This practical demonstrates the importance of systematic vulnerability scanning and remediation to enhance network security and minimize potential risks.