LAB-2

1. Imagine you are working as a cybersecurity analyst for a financial institution, you have been assigned the critical task of conducting a Nessus vulnerability analysis on a critical host system (windows, Linux) in the local network hosting sensitive customer data. Detail your step-step approach, including pre-scan preparations, specific Nessus configurations for maximum efficacy in an environment, scan the targets, prioritize and analyse the results and generate reports.

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it. Nessus, developed by Tenable Inc, is a widely-used open-source vulnerability scanner Nessus provides a range of services, including vulnerability assessments, network scans, web scans, asset discovery, and more, to aid security professionals, penetration testers, and other cybersecurity enthusiasts in proactively identifying and mitigating vulnerabilities in their networks.

Nessus tool for vulnerability scanner

https://www.tenable.com/products/nessus/nessus-essentials

Installing Nessus on kali Linux

1. Download the Nessus package for Debian on the Nessus website and make sure you set the Platform to Linux-Debian-amd64.

2. When it's finished downloading, open your Linux terminal and navigate to the location you downloaded the Nessus file to.

3. Install Nessus using this command:

```
sudo dpkg -i Nessus-10.4.1-debian9_amd64.deb
```

4. Start the Nessus service with this command:

```
sudo systemctl start nessusd.service
```

5. On your browser, go to https://kali:8834/. It would show a warning page. 6. Click on Advanced. Then, click on Accept Risk and Continue.

7. Choose the Nessus Product you prefer. If you want the free version of Nessus, click on Nessus Essentials.

8. Enter your name and email address to receive an activation code by email. Paste the activation code into the space provided and choose a username and password.

9. Allow Nessus to download the necessary plugins.

10. Once the plugin downloads have completed, you can start using the Nessus service.

Passwd Change

```
/opt/nessus/sbin/nessuscli chpasswd shubha
```

After installing the required plugins, navigate to the 'newscan' module. Enter the IP address of the Metasploitable2 target for scanning. You have the flexibility to schedule scans for specific times or days, or perform OnDemand scanning.

Select from various scan options such as host discovery, basic scan, or advanced scan. Once the scanning process is finished, proceed to analyse the vulnerabilities categorized by their severity levels such as medium, high, or critical, along with their respective CVSS (Common Vulnerability Scoring System) scores.

Check for available remediations for each vulnerability and generate a comprehensive PDF report summarizing the scan results, including identified vulnerabilities, their severity, CVSS scores, and recommended actions for mitigation.

.

Note: After installing Nessus on Kali Linux, ensure that the nessusd service is running every time you log in. This ensures continuous availability of Nessus functionality

```
Systemctl start nessusd.service
```

https://kali:8834 in the browser.