## Lab 13: Running a Vulnerability Scan with Nessus

**Scenario**

A hacker breaches a global superstore company's network. The hacker exploits a vulnerability in the network and steals the sales and inventory data of the store. This data is sensitive. The company provides that data to manufacturers to get incentives. The company wants cybersecurity specialists to analyze its database to secure its network against potential breaches in the future.

**Solution**

The company hires you as a certified cybersecurity practitioner because it wants you to hack and find vulnerabilities ethically. As a cybersecurity practitioner, your first step is to identify potential security weaknesses in the target system or network using vulnerability scanning tools. In this lab, we use the Nessus tool to scan the vulnerabilities in the network.

Nessus is an assessment tool for finding malware that can break into networks, identify configuration problems, and detect security holes. It performs vulnerability, configuration, and compliance assessments. It supports various technologies such as OSes, network devices, hypervisors, databases, tablets/phones, web servers, and critical infrastructure.

**Note:** This lab is performed on a Windows 10 virtual machine using the Nessus vulnerability scanning tool. You can download this tool from Tenable’s website: **https://www.tenable.com/products/nessus/nessus-professional**.

|  |
| --- |
| 1. Download and install the Nessus vulnerability scanning tool. After that, open the browser on a Windows 10 machine. In the address bar, type [**https://localhost:8834/**](https://localhost:8834/)**,** and press Enter. **Your connection isn’t private** page appears. Expand the **Advanced** section and click **Continue to localhost (unsafe)**.    2. In the Nessus login page, add your **credentials** to log in, then click on **Sign In**.    3. Nessus begins to initialize; this will take some time. On completion of initialization, the Nessus dashboard and the **Welcome to Nessus Essentials** pop-up appear. Close the pop-up.    4. The Nessus Essentials dashboard opens; select **Policies** from the pane on the left under the **RESOURCES** section.    5. The **Policies** window appears; click **Create a new policy**.    6. The **Policy Templates** window appears; click **Advanced Scan**.    7. The **New Policy / Advanced Scan** section appears. In the Settings tab, under the **BASIC** type, specify a policy name in the **Name** field here, **NetworkScan\_policy**, and give a **Description** of the policy here, **Scanning a Network**.    8. In the **Settings** tab, click the **DISCOVERY** setting type and turn off the **Ping the remote host** option from the right pane.    9. Select the **Port Scanning** option under the **DISCOVERY** setting type, and then click the **Verify open TCP ports found by local enumerator’s** checkbox. Leave the other fields with default options.    10. Select the **ADVANCED** setting type. In the right pane, under the **Performance Options** setting, set the values of **Max number of concurrent TCP sessions per host and Max number of concurrent TCP sessions per scan** to **Unlimited**.    11. To configure the credentials of a new policy, click the **Credentials** tab and select **Windows** from the options.    12. Specify the **Username** and **Password** in the window. Here, the specified credentials are **CEH123/qwertt@123**. Re-enter the created user account credentials and **Admin/password** if a session timeout notification pop-up appears.    13. Click the **Plugins** tab, and do not alter any options in this window. Click the **Save** button.    14. A **Policy saved successfully** notification pop-up appears, and the policy is added to the **Policies** window.    15. Now, click **Scans** from the menu bar to open the **My Scans** window; click **Create a new scan**.    16. The **Scan Templates** window appears. Click the **User Defined** tab and select **NetworkScan\_policy**.  **Note:** If an **API Disabled** pop-up appears, refresh the browser and log in again to the **Nesses Essentials** using credentials **(Admin/password)**. If the API Disabled error still appears, clear the browser’s cache by selecting the three dots in the top right corner of the window, going to History, selecting Clear History, ensuring that Cache and Cookies are selected, then clicking Clear. Then log back into **Nessus Essentials**.    17. The **New Scan/NetworkScan\_Policy** window appears. Under **General Settings** in the right pane, input the **Name** of the scan here, **Local network,** and enter the **Description** for the scan here, **Scanning a local network**. Enter the IP address of the target on which you want to run the vulnerability analysis in the **Targets** field.    18. Click **Schedule** settings; ensure that the **Enabled** switch is turned off. Click the drop-down icon next to the **Save** button and select **Launch** to start the scan.    19. The **Scan saved and launched successfully** notification pop-up appears. Nessus starts scanning the target as soon as the scan is launched. Click **Local Network** to view the detailed results after completing the scan. The scan lasts for roughly 15-20 minutes.    20. The **Local Network** window displays the summary of target hosts and the **Scan Details** and **Vulnerabilities** categorization under the **Hosts** tab.    21. Click the **Vulnerabilities** tab and scroll down to view all the vulnerabilities associated with the target machine. The list of vulnerabilities may differ when you perform this task. Click on any of these vulnerabilities to view a report on it in detail.    22. The **Local Network** window appears, displaying multiple issues in the SMB. Click on any **SMB Medium** issue to view its detailed information. The report regarding the selected vulnerability, **SMB Medium,** appears with detailed information such as plugin details, risk information, vulnerability information, reference information, and solution.    23. Click the **Local Network** window’s **Report tab** from the top-right corner. In the **Generate Report** window, choose a file format, here **HTML,** from the available options, and click **Generate Report**. By downloading a report, you can access it anytime instead of logging in to Nessus again and again.    24. Once the download is finished, a pop-up appears at the top of the browser; click **Open file**.    25. The Nessus scan report appears in the **Edge** web browser. Click the **Expand All** option to view the detailed scan report.    26. A list of discovered vulnerabilities appears. You can further click on plugins, here **57608,** to view more detailed information on the vulnerability.    27. The selected plugin details are displayed.    28. This way, you can select a vulnerability to view the complete details. Once the vulnerability analysis is done, switch back to the tab where Nessus is running by clicking **Admin** > **Sign Out** in the top-right corner.    31. Once the session is logged out, it **Signed out successfully. Goodbye, admin** notification appears. It concludes the demonstration of performing vulnerability assessment using Nessus. |