Lab 5 – Vulnerability Analysis

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Ian Coston

Date – 8th OCT 2023

Introduction

In this lab, perform a vulnerability scan against the lab network and review the scan report for analyzing detected vulnerabilities.

Pre-Lab

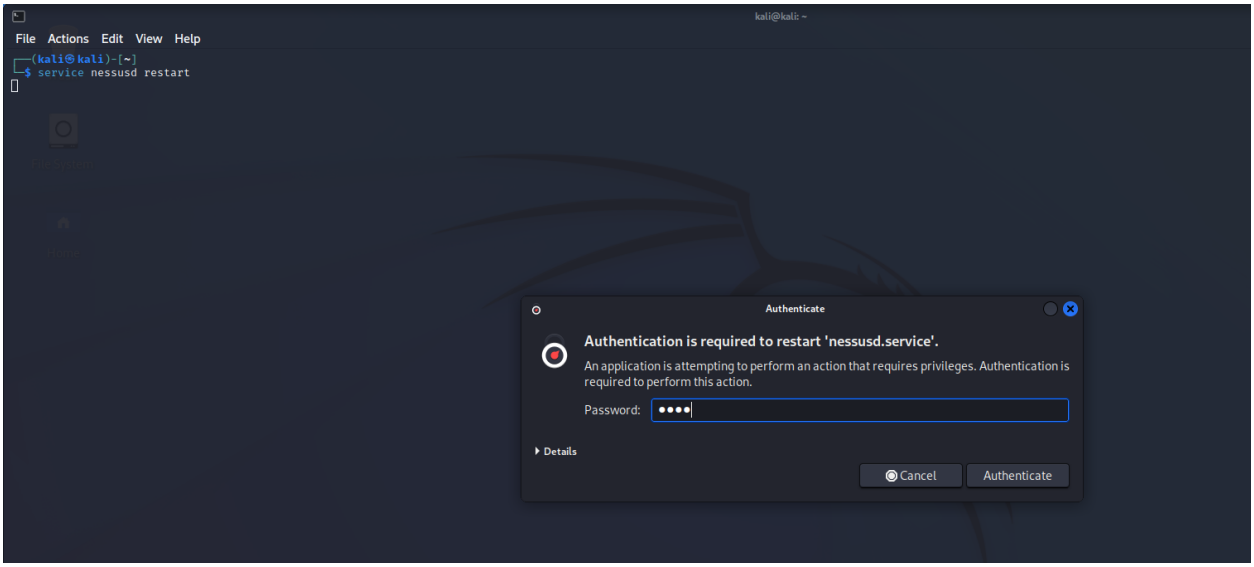
For this lab, you will require Kali Linux and Windows machines,

Practical

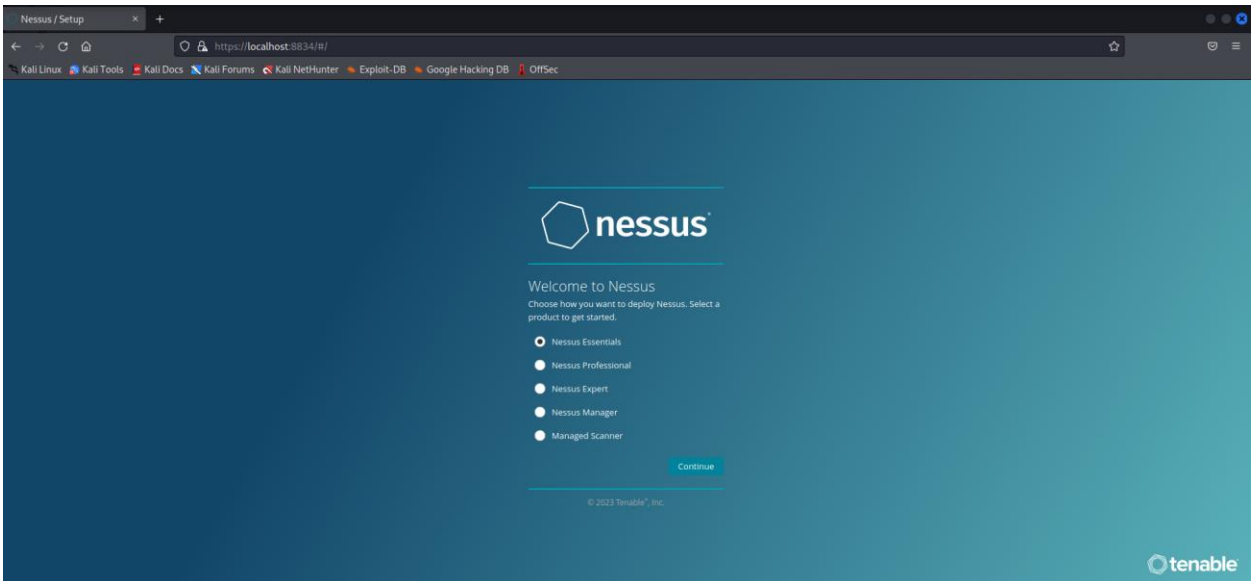
1. Vulnerability Scanning with Nessus

Ensure the Nessus service is running in the Kali VM by running:

Command - `service nessusd restart`

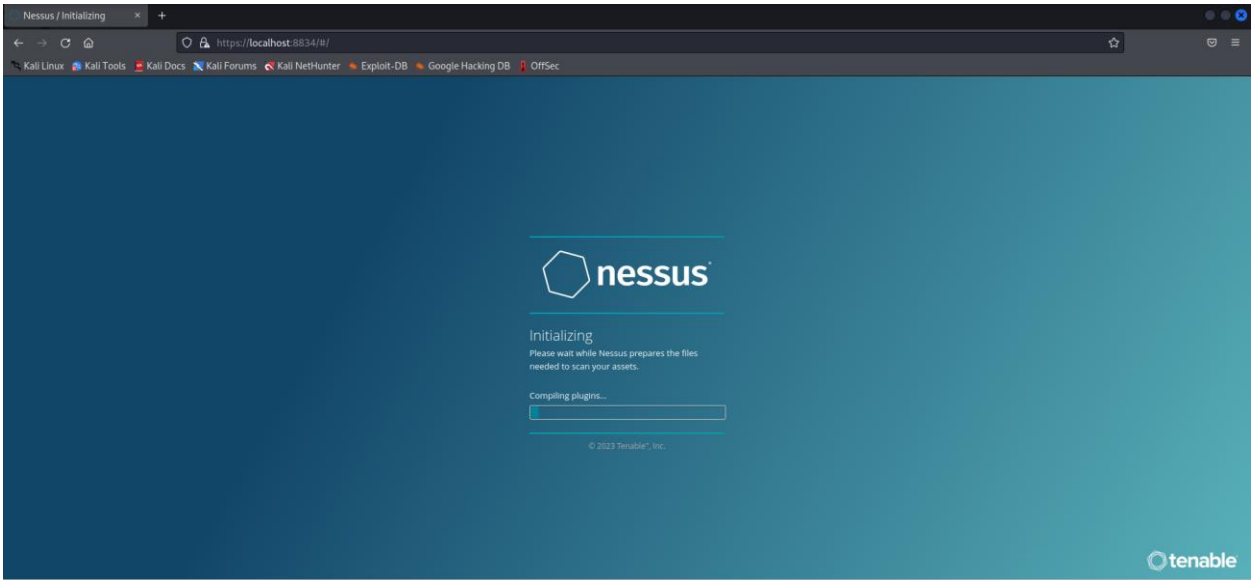


After successful installation, pull up a web browser inside Kali and navigate to https://localhost:8834.



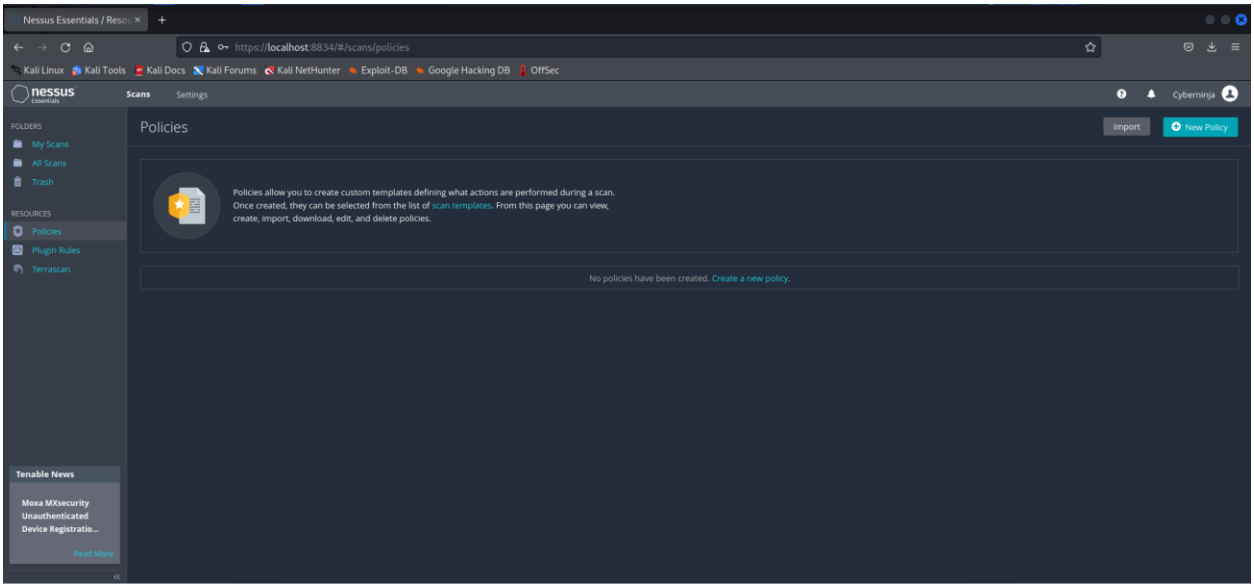
Follow the "wizard" to configure the Nessus engine. It should default to Nessus Essentials. Simply click continue.

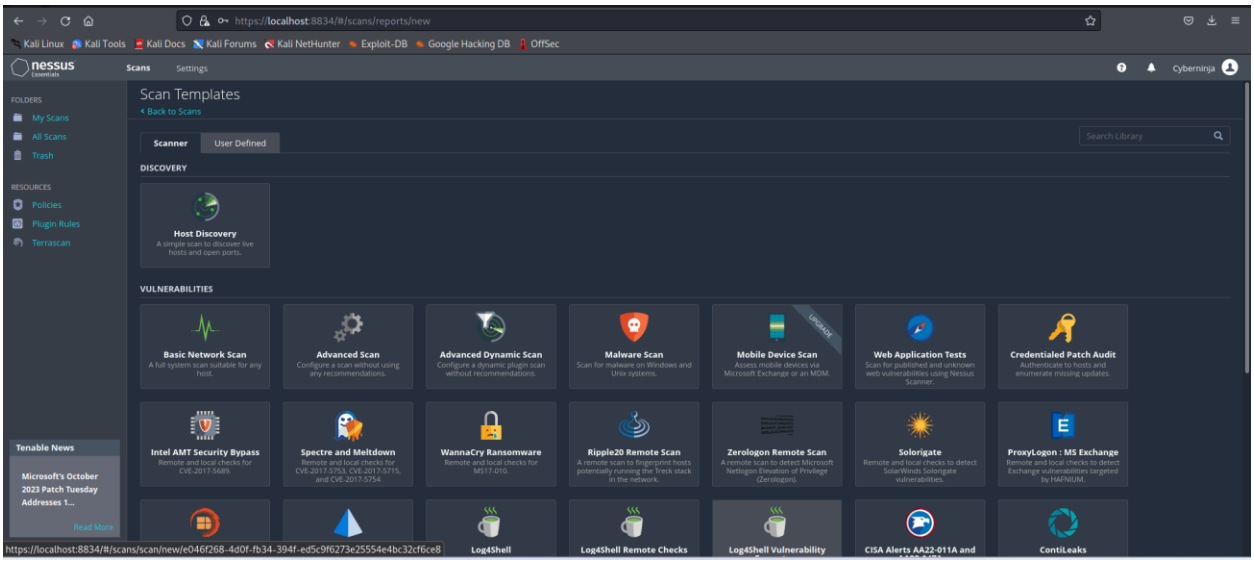
After completing all of the steps, select Download Plugins.



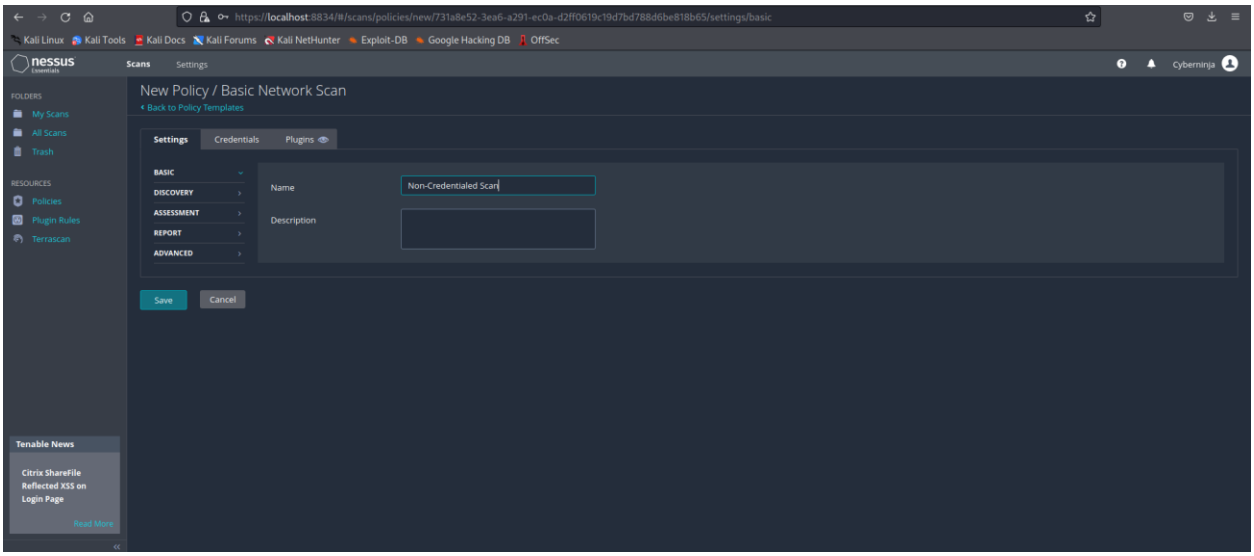
2. Using Nessus to perform a Vulnerability scan

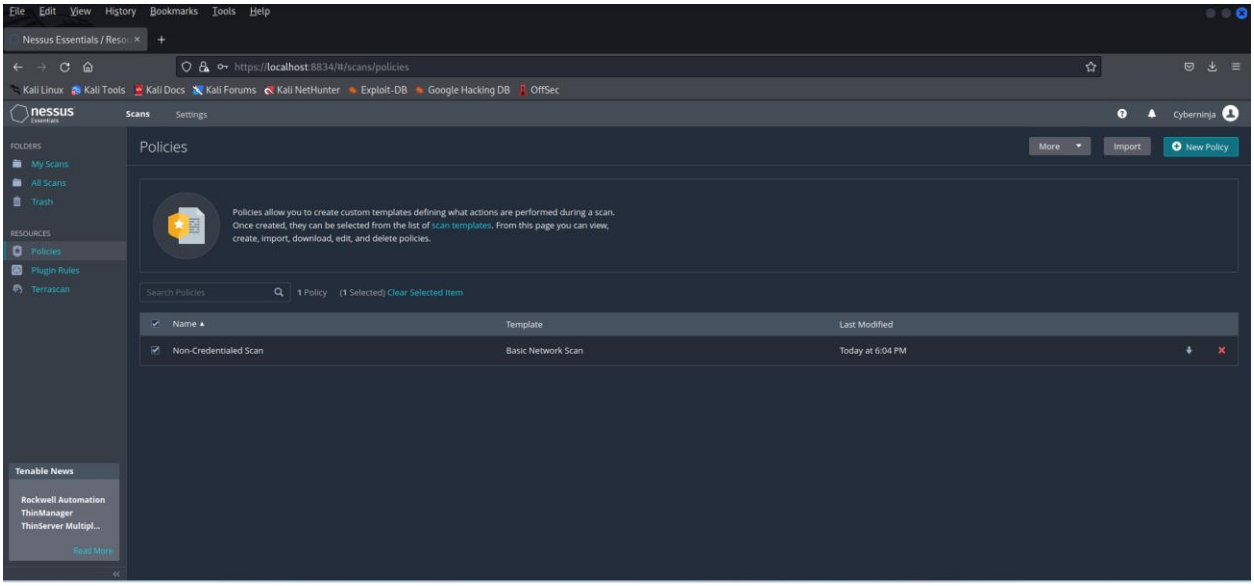
Login to the web console with the username and password created. Go to Policies → Select New Policy → Select Basic Network Scan. Enter a policy name of "Non-Credentialed Scan"



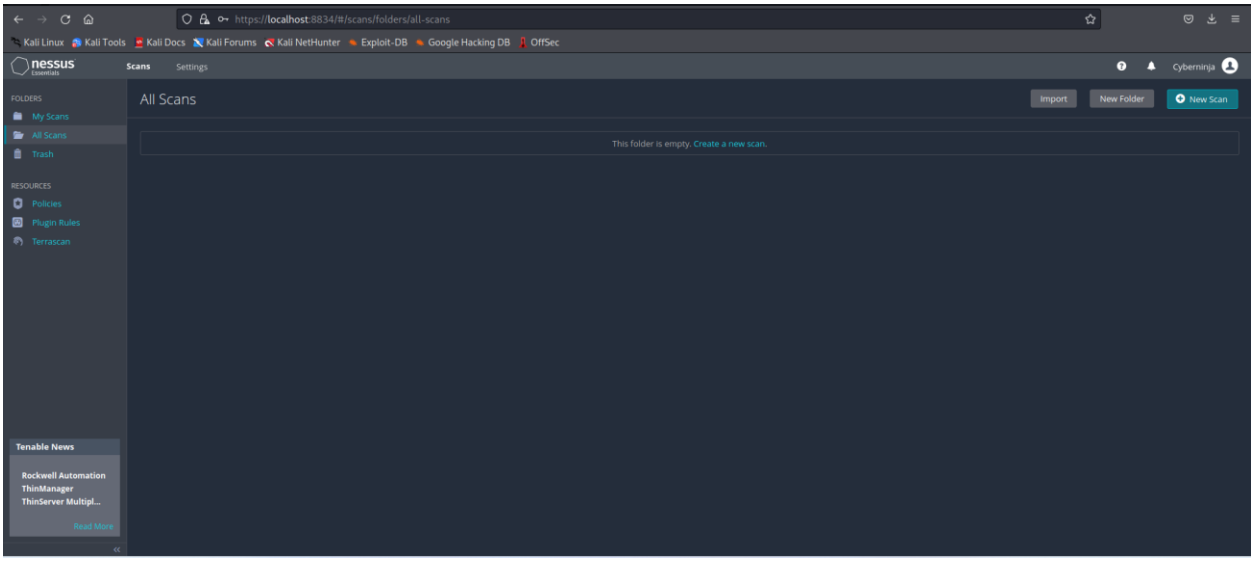


Enter a policy name of "Non-Credentialed Scan". Iterate through the options on the side menu to complete the configuration. When in doubt, select "Default" in the drop down menu.

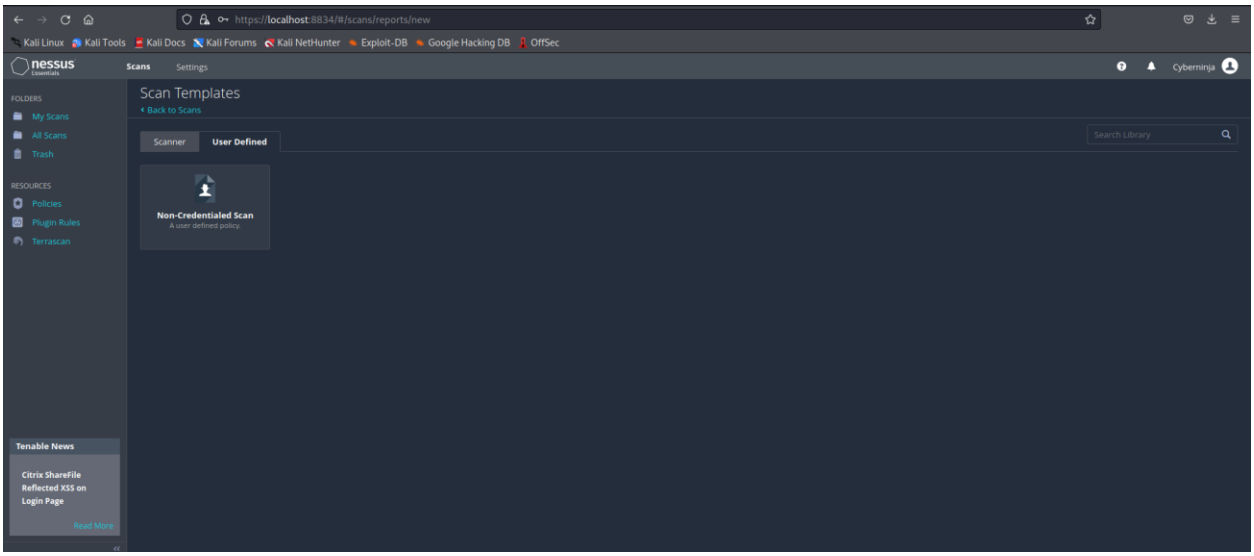


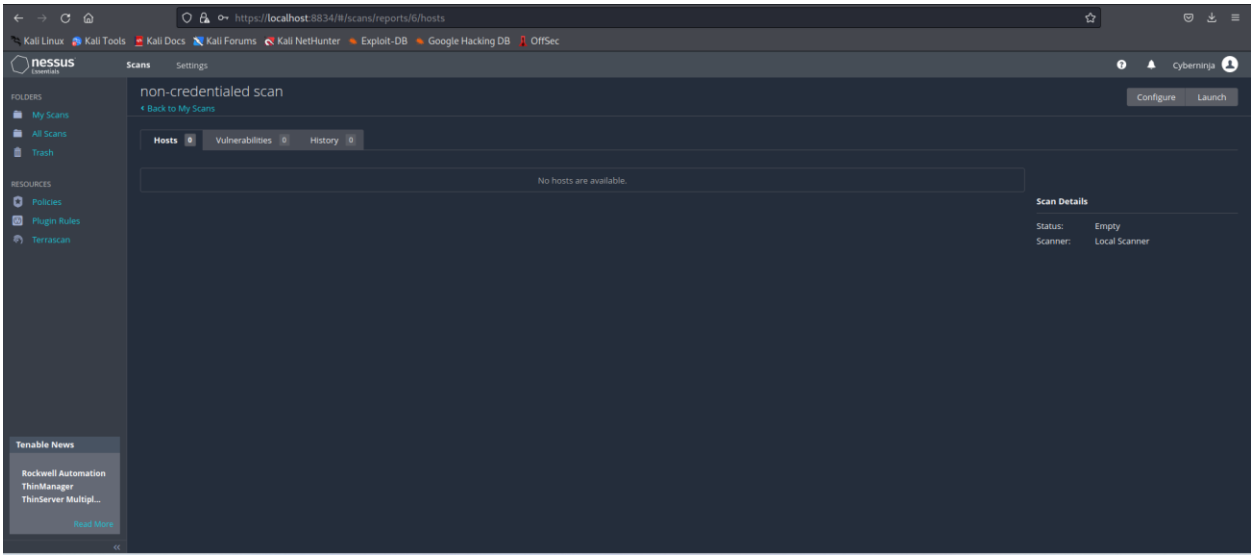


Go to Scans - Select New Scan - Give the scan the name of “non-credentialed scan”



For Policy Select Non-Credentialed Scan. For the Target, select your IP range for your systems (i.e. 192.168.100.1-192.168.100.255). Select Launch; When the scan is finished, double click on it

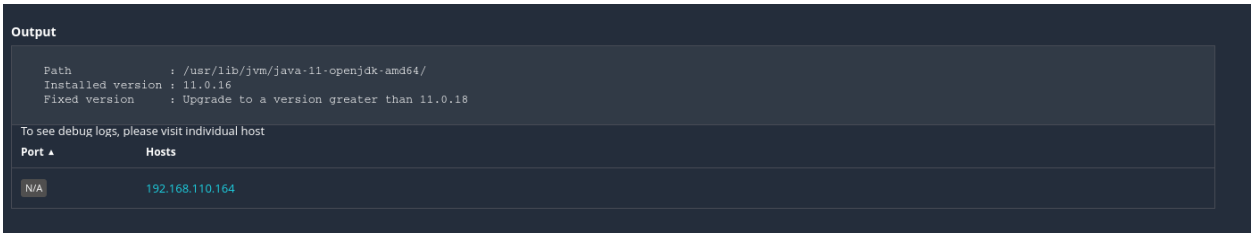




Reviewing a Nessus Vulnerability report:

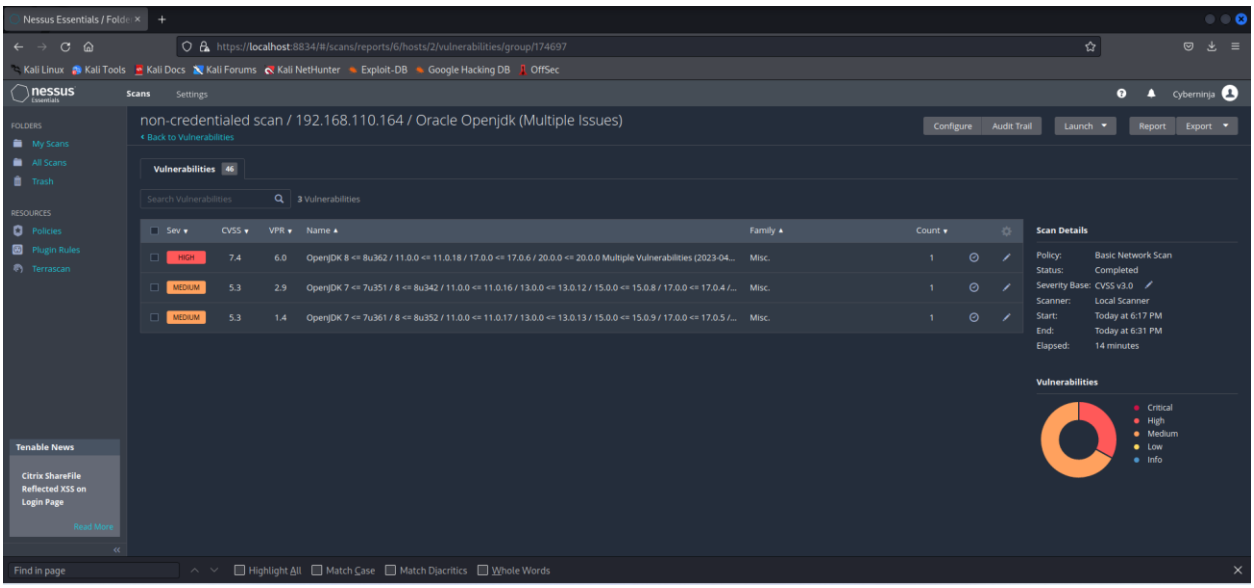
1) What ports were found open in the scan?

- N/A



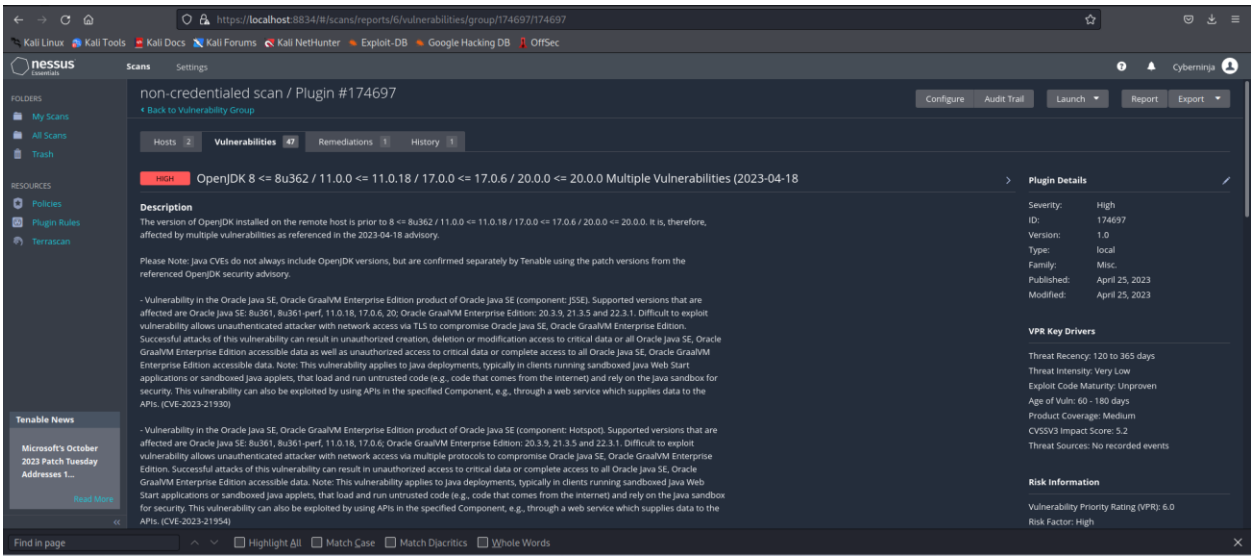
2) How many High vulnerabilities were found?

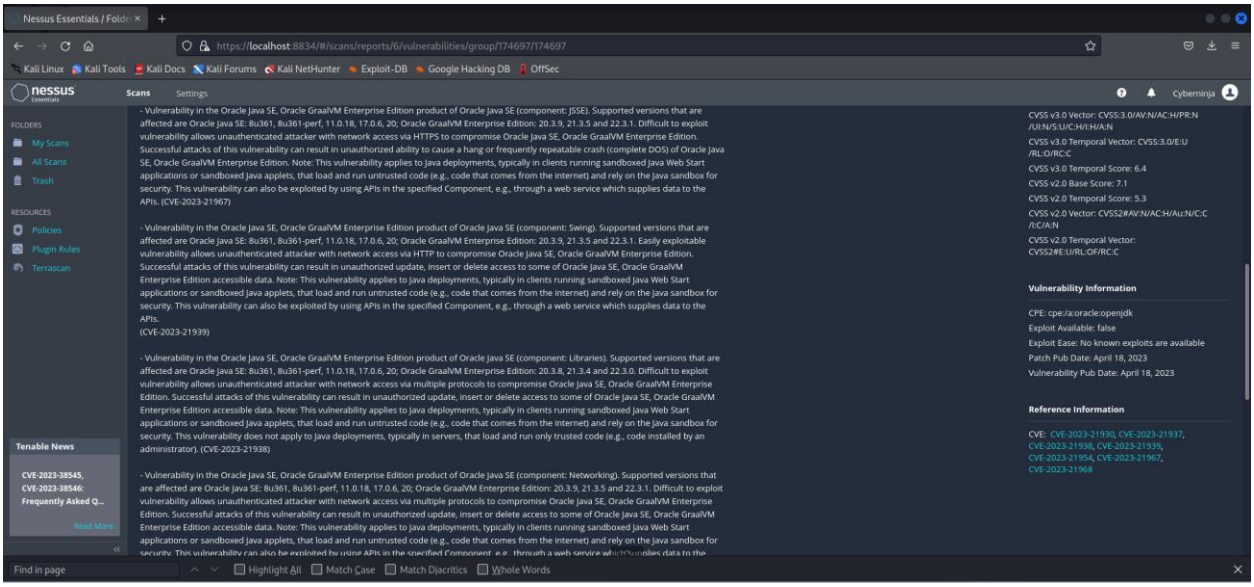
- One



3) Select a vulnerability listed and view the details Nessus provides

- The version of OpenJDK installed on the remote host is prior to 8 <= 8u362 / 11.0.0 <= 11.0.18 / 17.0.0 <= 17.0.6 / 20.0.0 <= 20.0.0. It is, therefore, affected by multiple vulnerabilities



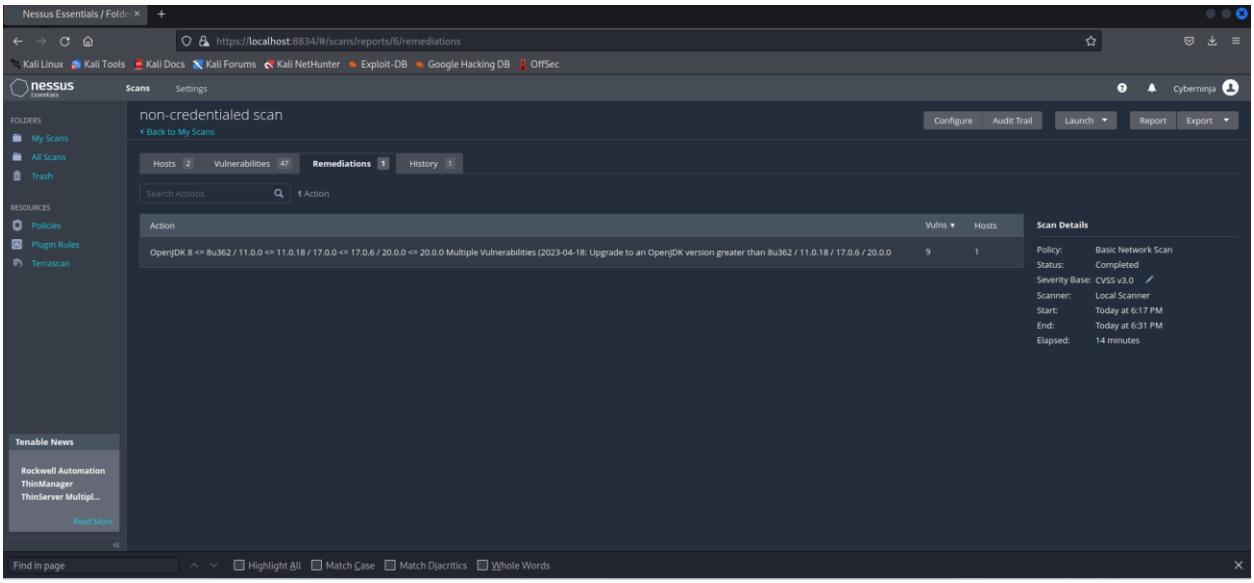


4) What CVE is associated with the finding?

- CVE-2023-21930, CVE-2023-21937, CVE-2023-21938, CVE-2023-21939, CVE-2023-21954, CVE-2023-21967, CVE-2023-21968

5) What solution does Nessus propose?

- Upgrade to an OpenJDK version greater than 8u362 / 11.0.18 / 17.0.6 / 20.0.0

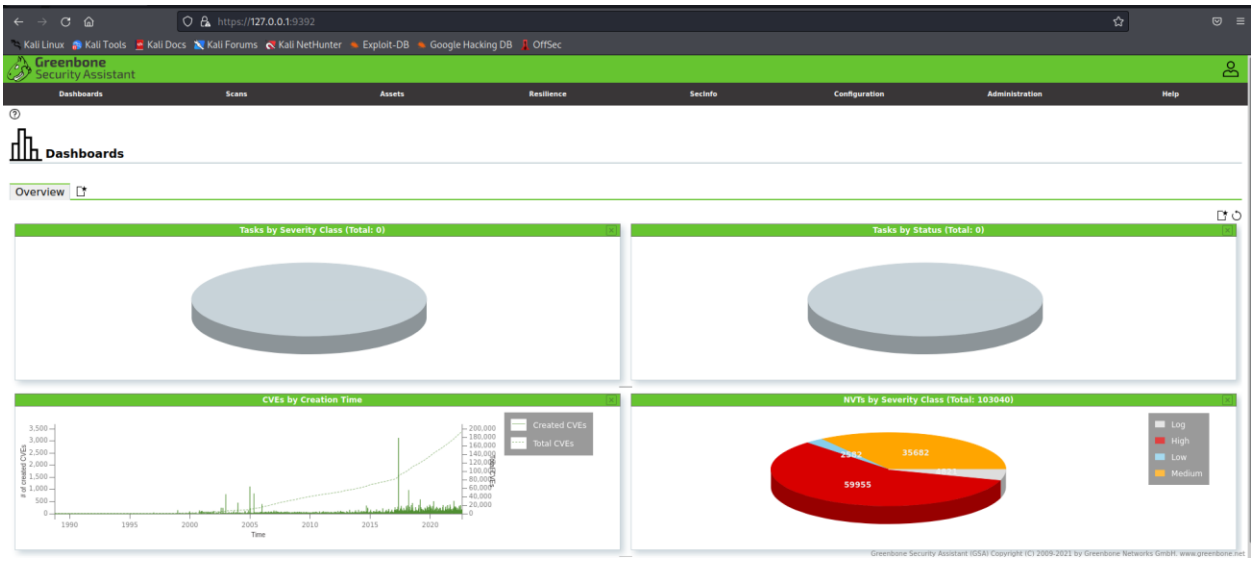


Using OpenVAS

The OpenVAS web interface includes a wizard to help set up scans of target machines. To access the wizard, first start the Greenbone Vulnerability Manager server at a terminal by running.

Command : `sudo gvm-start`

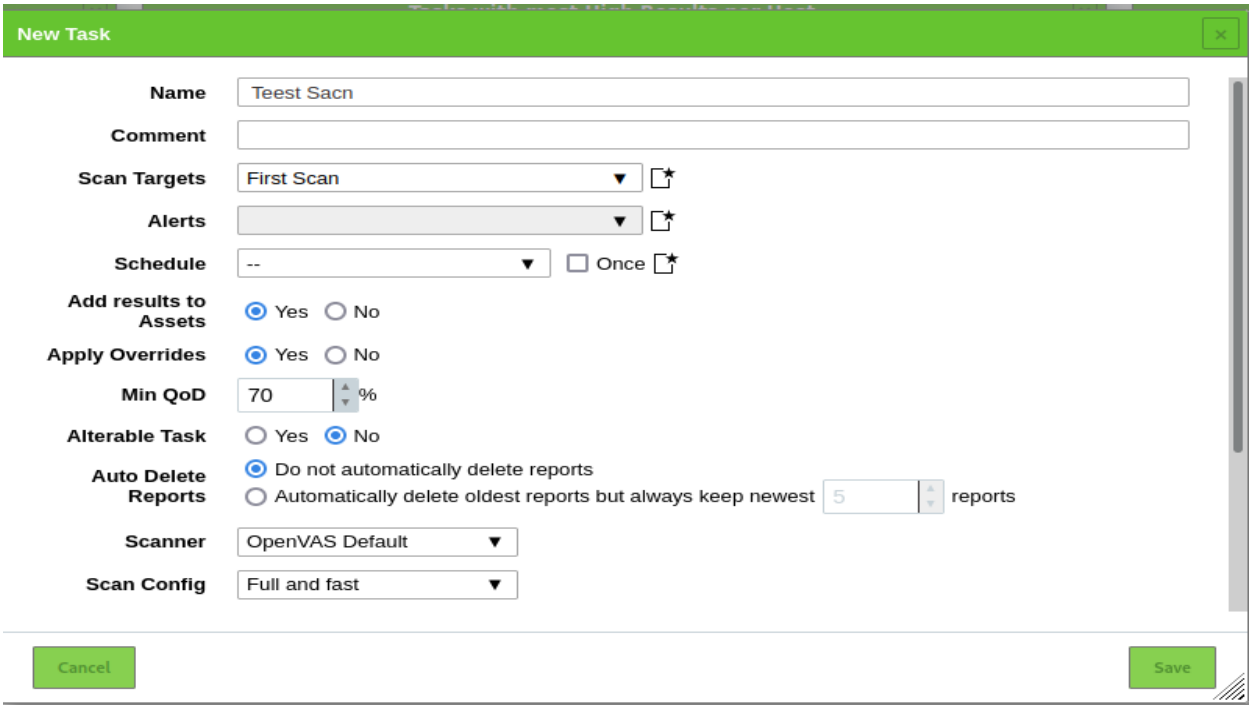
After successfully starting the service, you can navigate to https://localhost:9392 within Firefox.

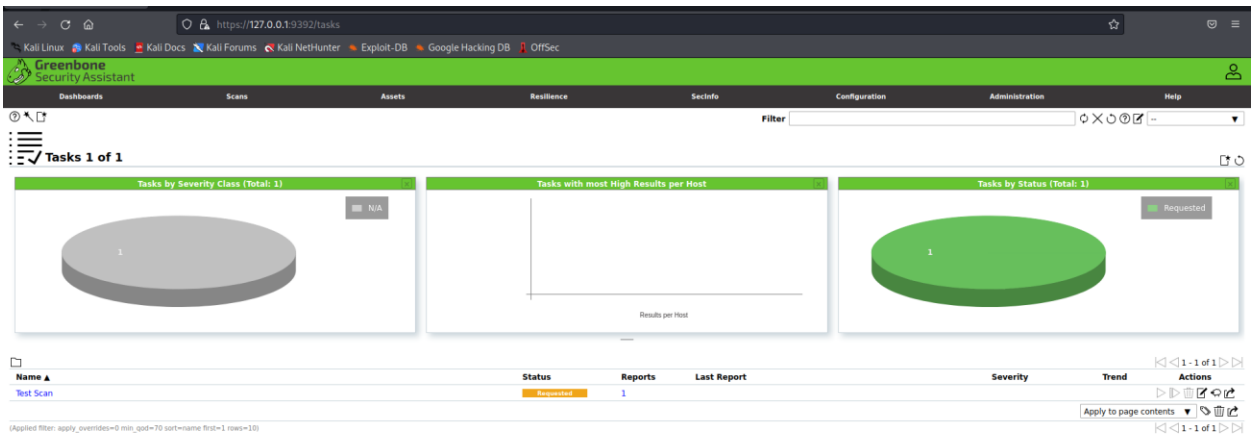


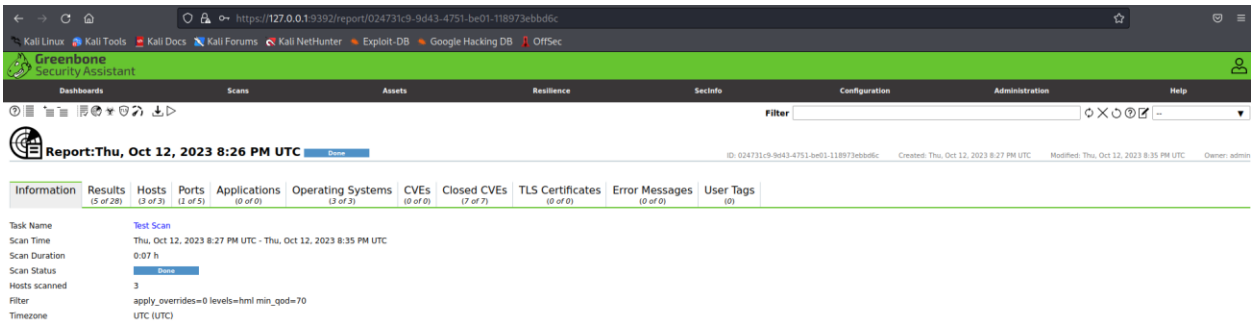
To start a scan, simply click the "wand" icon to start the Task Wizard.

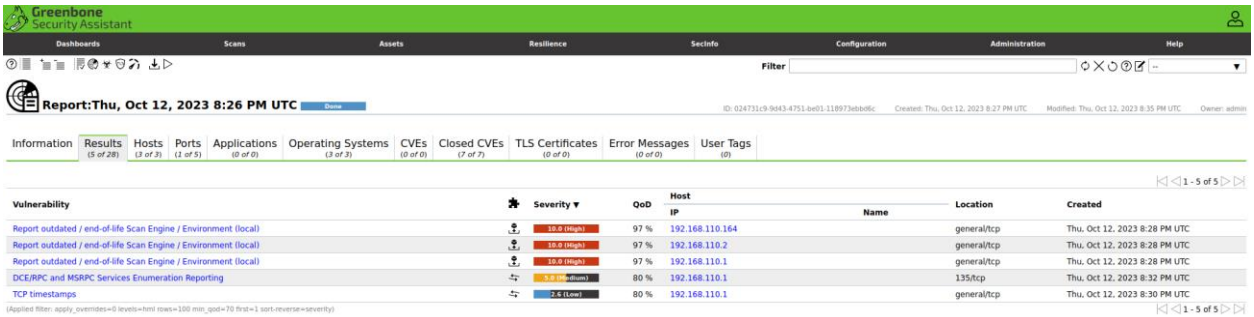
Click on Scan → Tasks → New Task

Fill up the IP range and other details asked

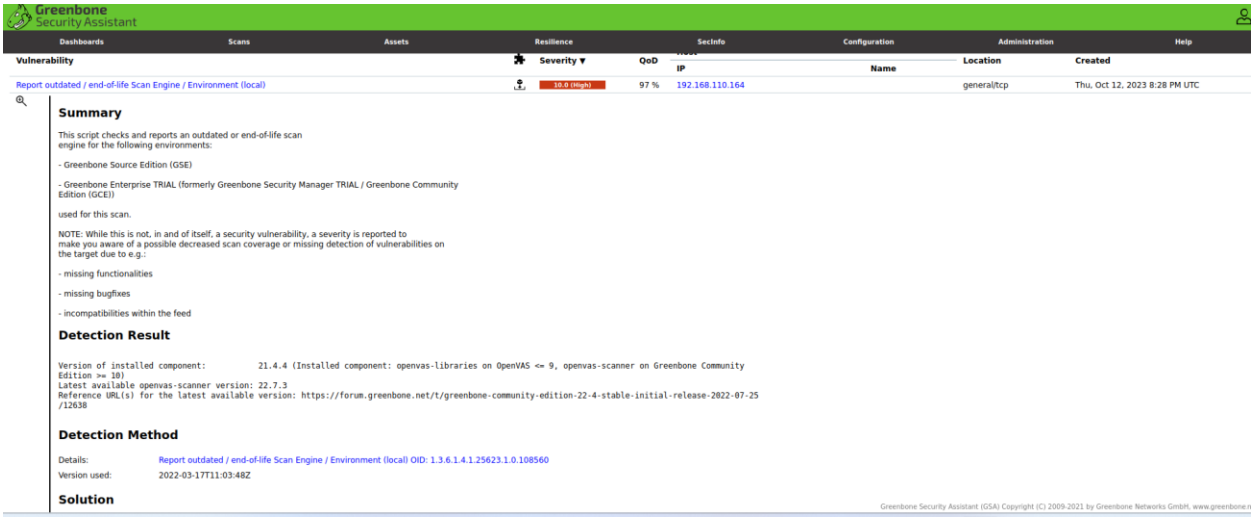


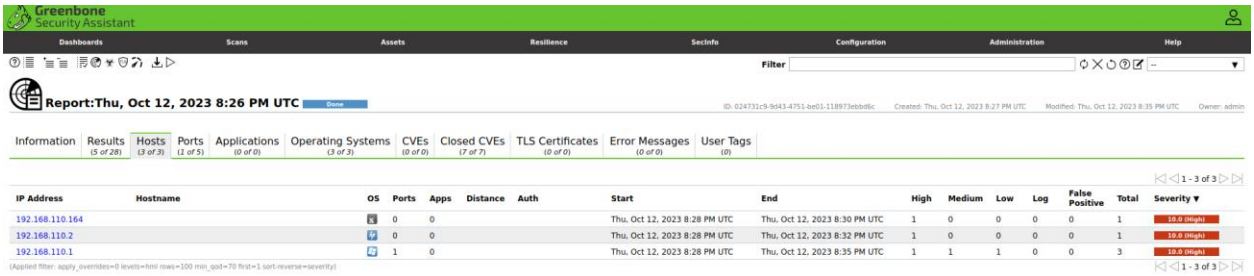


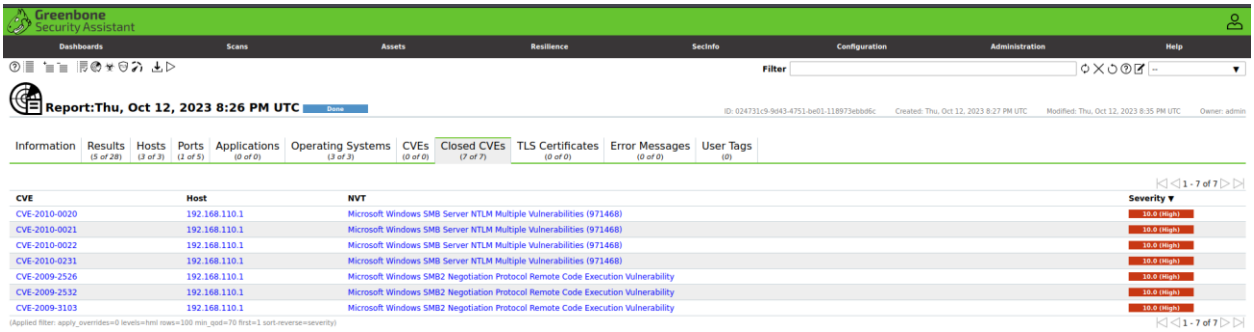




You can click on each reported vulnerability to get details.







OpenVAS provides several default scan configs and allows users to create custom configs. To see the descriptions of scan configs and create new ones, browse to Configuration → Scan Configs. By default, OpenVAS provides eight scan configs (though one is empty) and the details of each config can be seen by clicking on them. To create a new scan config, click the blue star button in the top left corner, create the config, and then click in to edit it.