

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

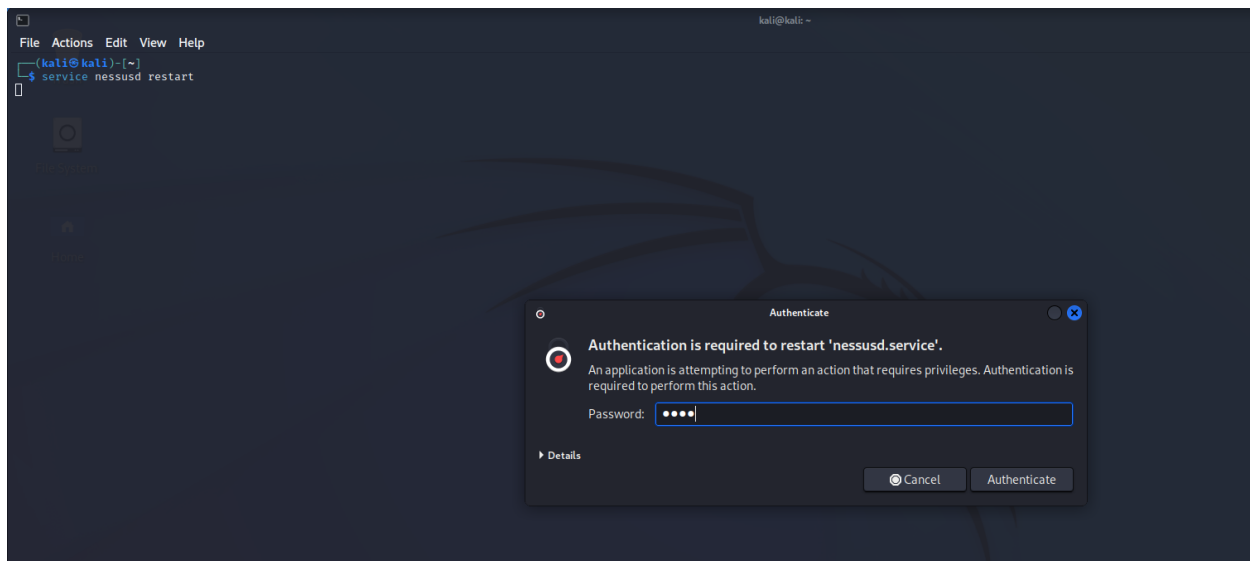
For this lab, you will require Kali Linux and Windows machines,

Practical

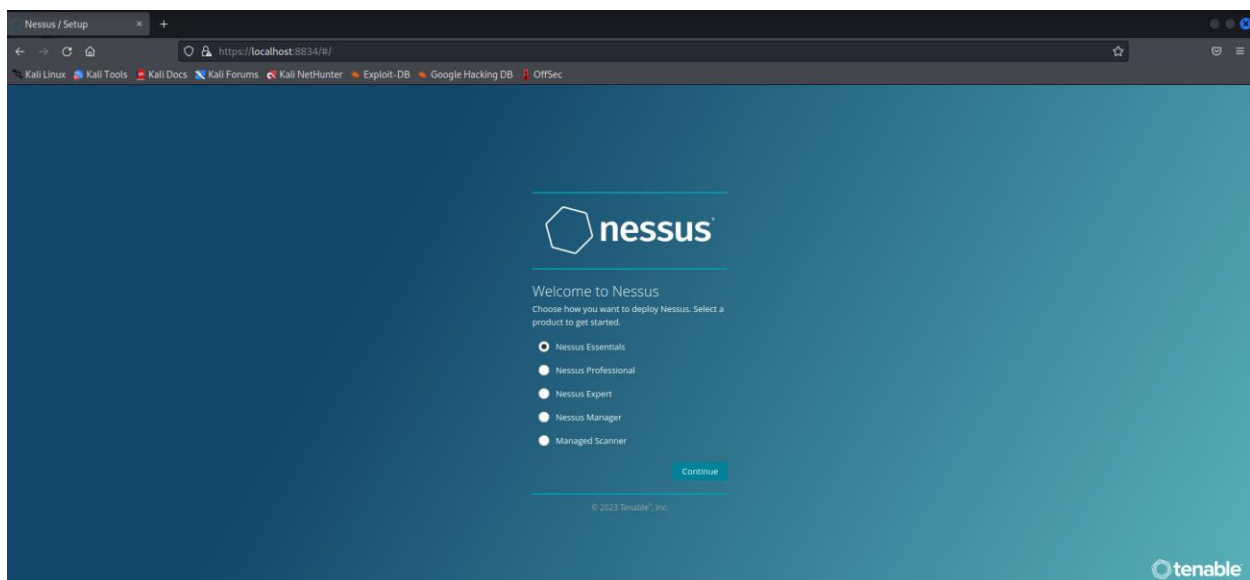
1. Vulnerability Scanning with Nessus

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

Command - `service nessusd restart`

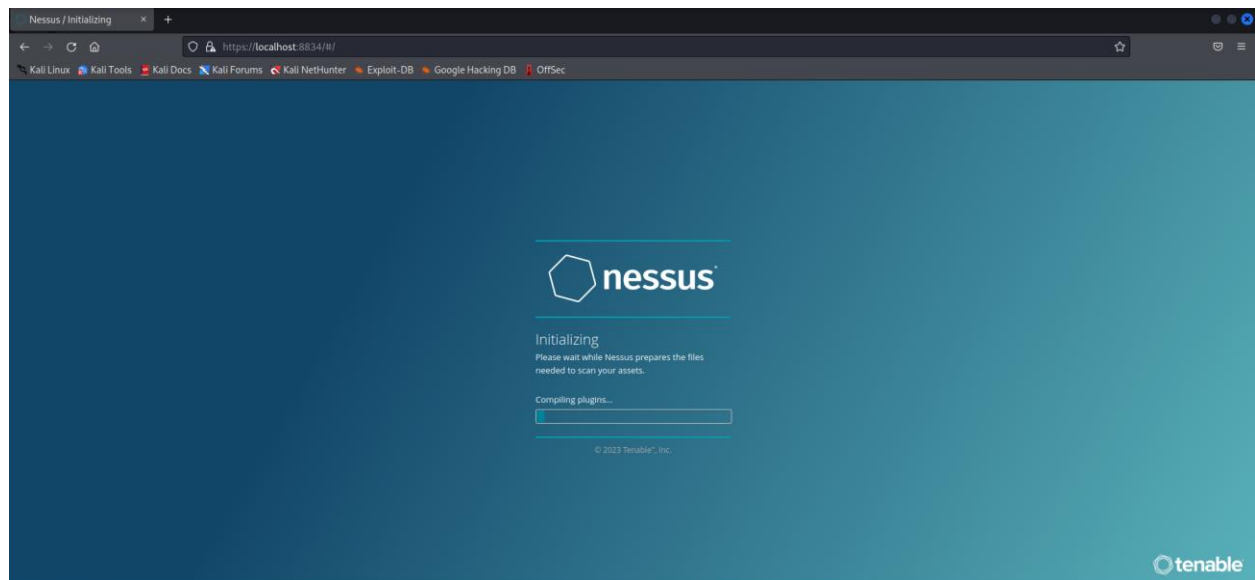


After successful installation, pull up a web browser inside Kali and navigate to <https://localhost:8834>.



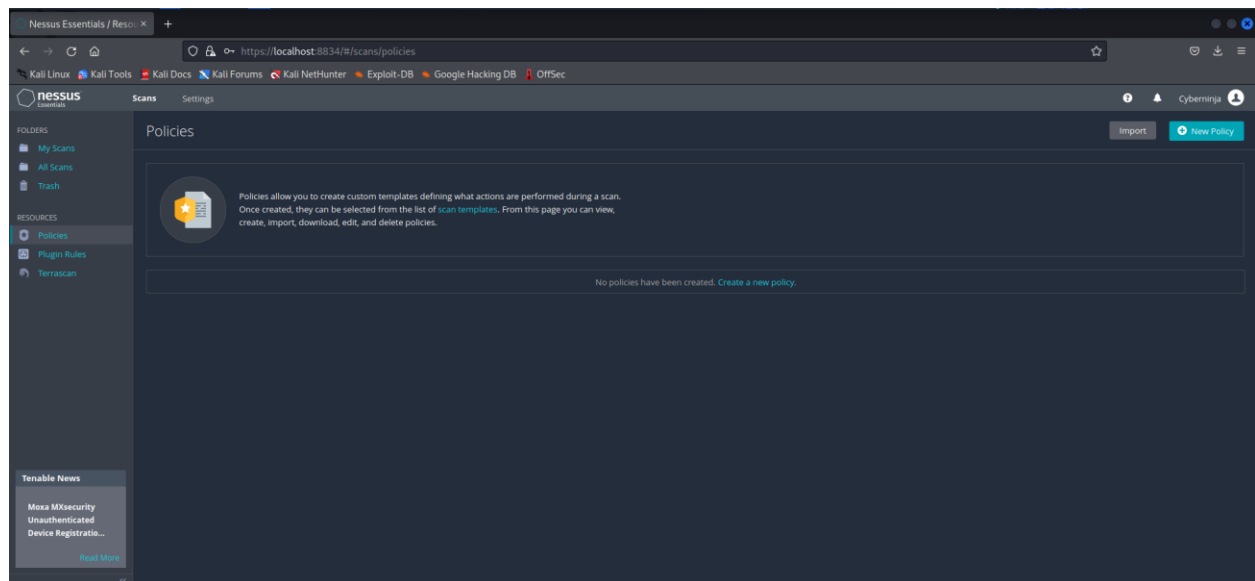
Follow the "wizard" to configure the Nessus engine. It should default to Nessus Essentials. Simply click continue.

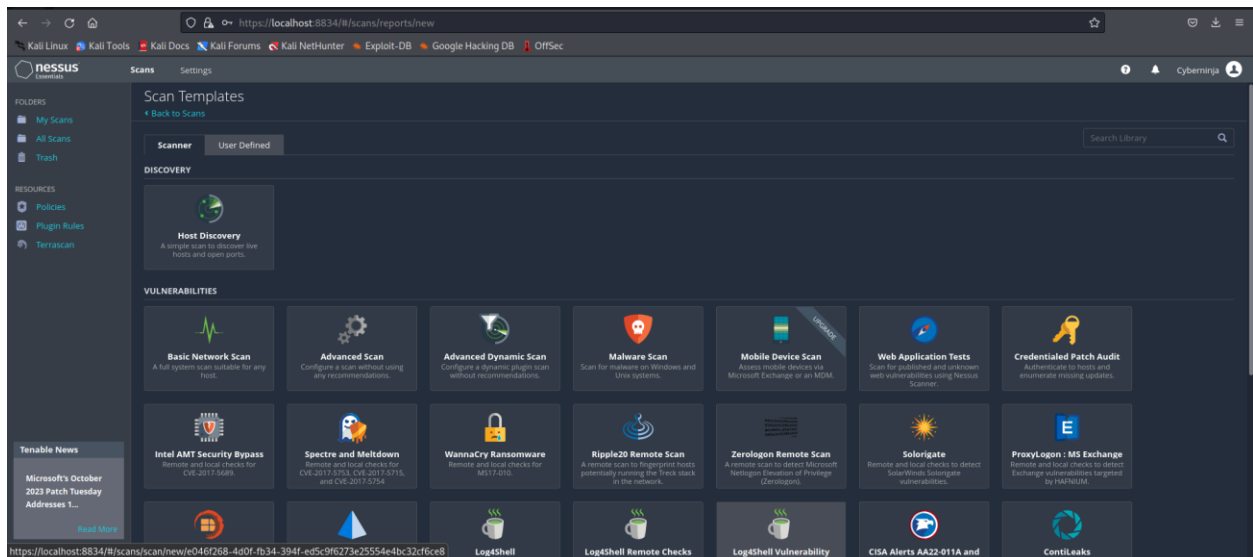
After completing all of the steps, select Download Plugins.



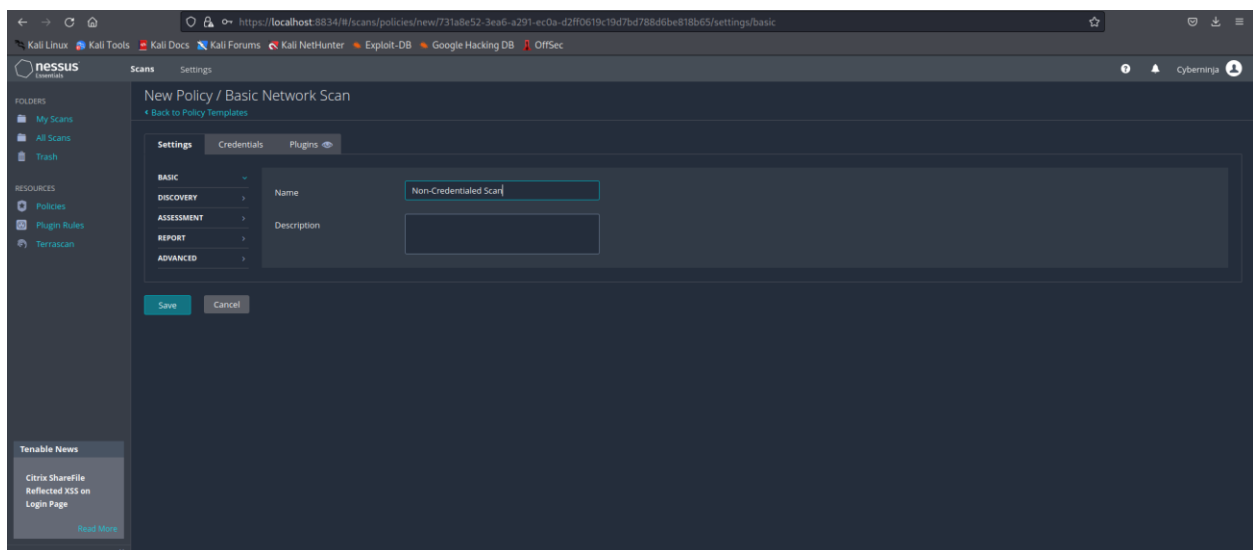
2. Using Nessus to perform a Vulnerability scan

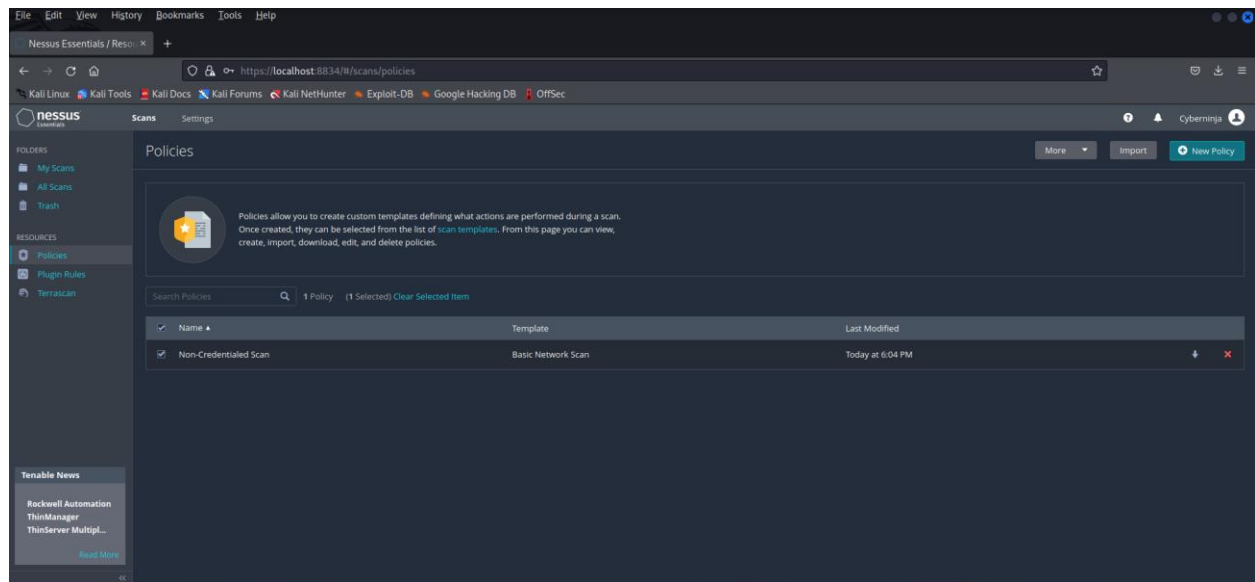
Login to the web console with the username and password created. Go to Policies → Select New Policy → Select Basic Network Scan. Enter a policy name of "Non-Credentialed Scan"



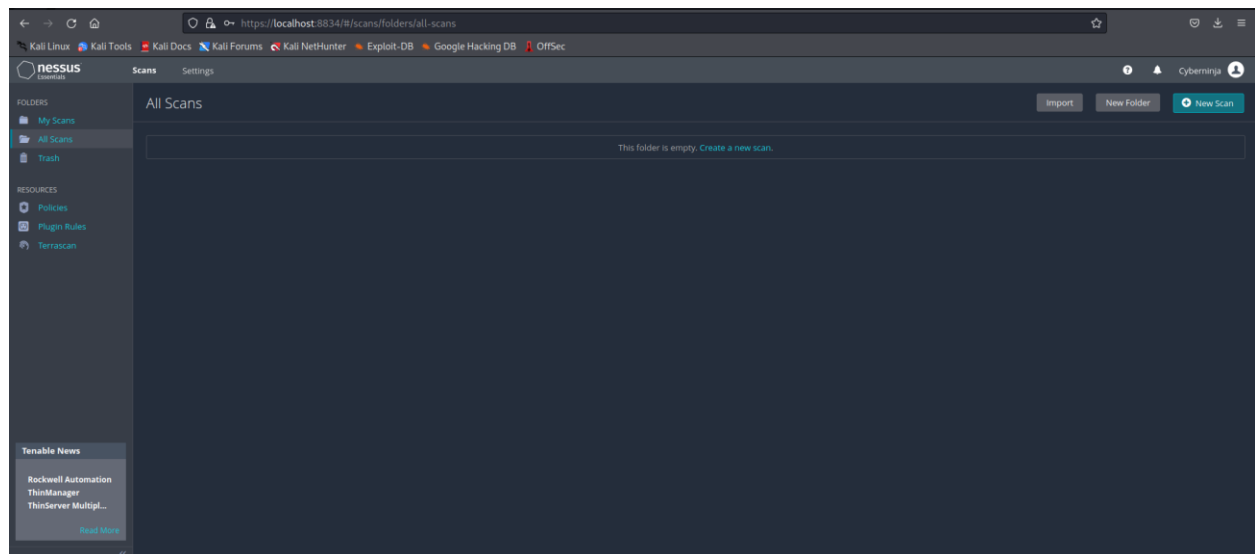


Enter a policy name of "Non-Credentialed Scan". Iterate through the options on the side menu to complete the configuration. When in doubt, select "Default" in the drop down menu.

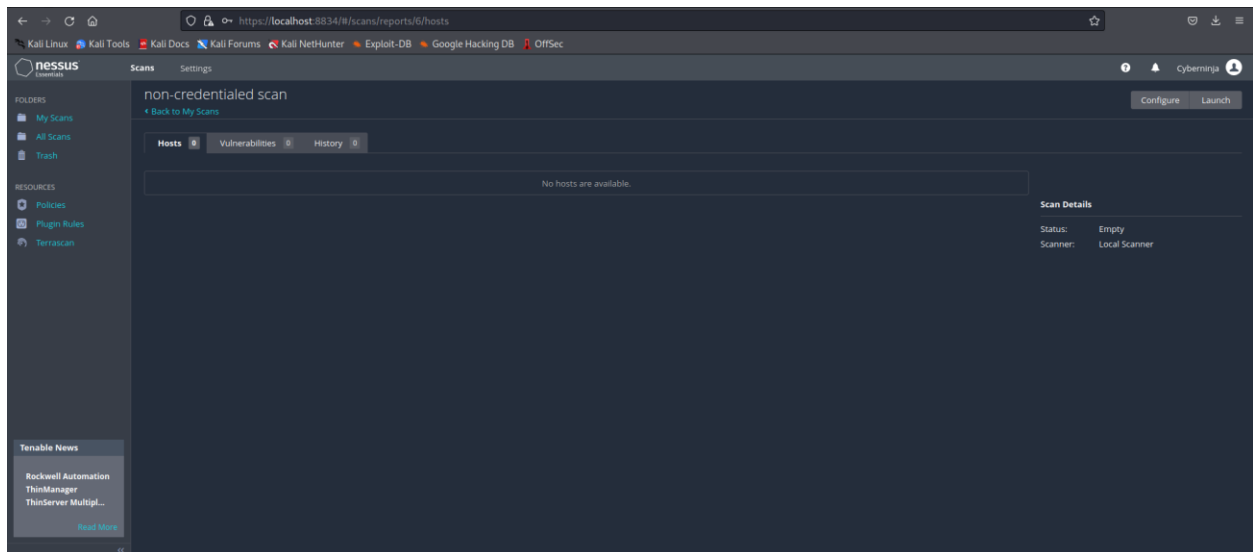
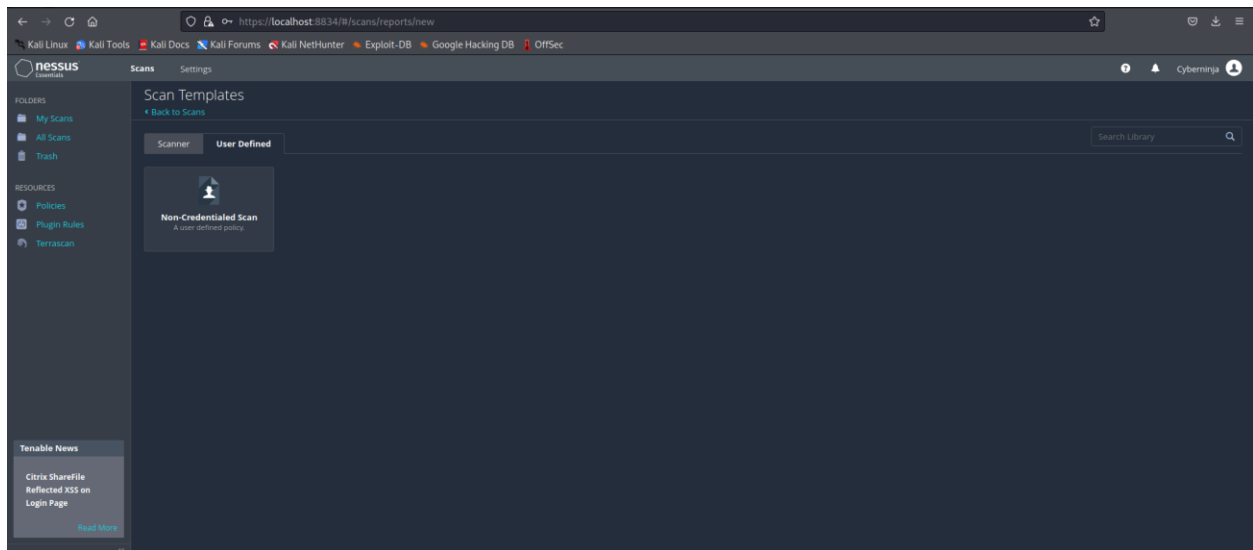




Go to Scans - Select New Scan - Give the scan the name of “non-credentialed scan”



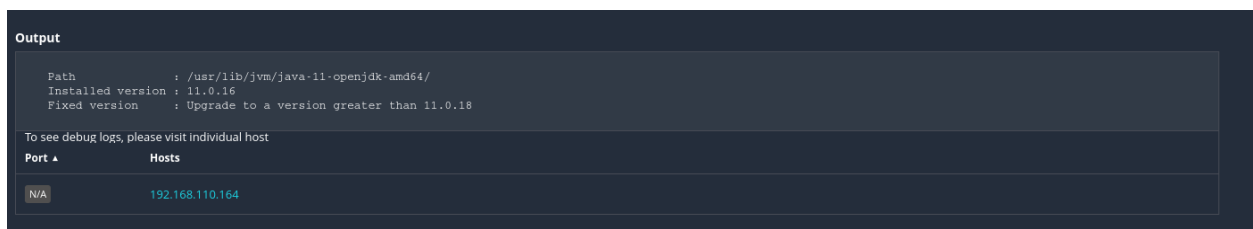
For Policy Select Non-Credentialed Scan. For the Target, select your IP range for your systems (i.e. 192.168.100.1-192.168.100.255). Select Launch; When the scan is finished, double click on it



Reviewing a Nessus Vulnerability report:

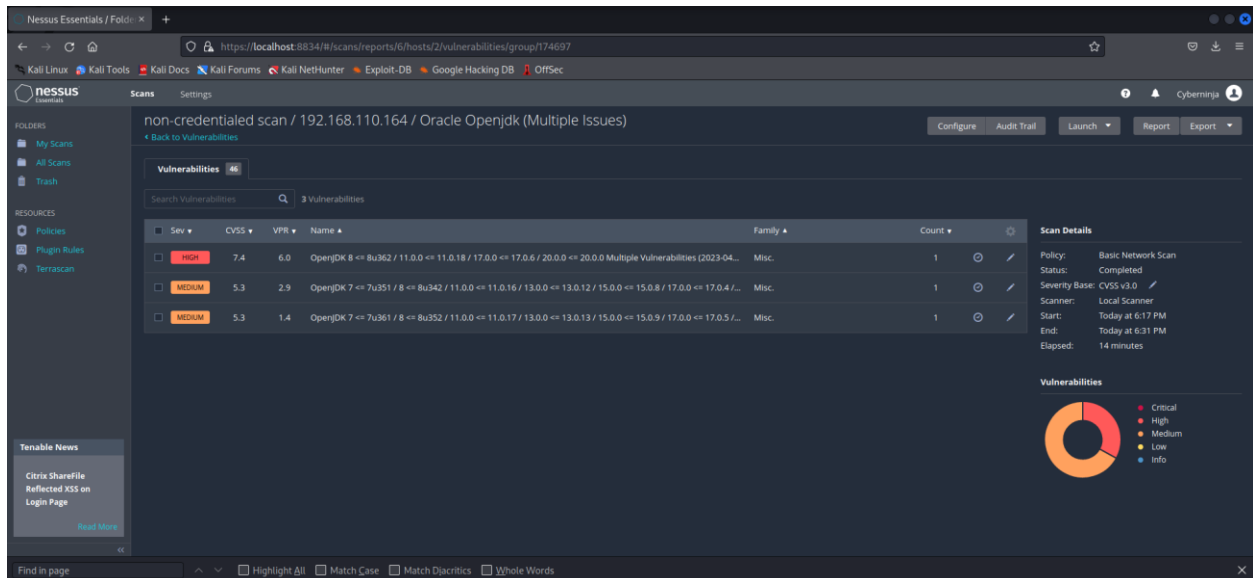
1) What ports were found open in the scan?

- N/A



2) How many High vulnerabilities were found?

- One

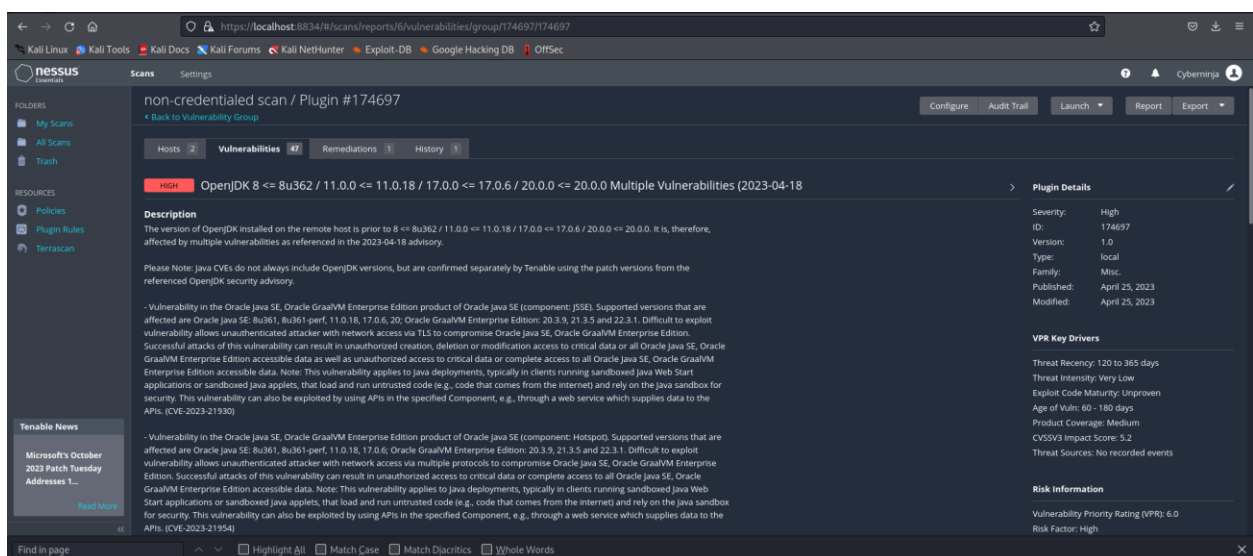


The screenshot shows the Nessus Essentials interface. The main panel displays a non-credentialed scan report for 192.168.110.164 / Oracle Openjdk (Multiple Issues). The report lists three vulnerabilities, all of which are High severity. A donut chart shows the distribution of vulnerability severities: 1 Critical, 1 High, 1 Medium, 0 Low, and 0 Info.

Sev	CVSS	VPR	Name	Family	Count
HIGH	7.4	6.0	OpenJDK 8 <= 8u362 / 11.0.0 <= 11.0.18 / 17.0.0 <= 17.0.6 / 20.0.0 <= 20.0.0 Multiple Vulnerabilities (2023-04-18)	Misc.	1
MEDIUM	5.3	2.9	OpenJDK 7 <= 7u251 / 8 <= 8u342 / 11.0.0 <= 11.0.16 / 13.0.0 <= 13.0.12 / 15.0.0 <= 15.0.8 / 17.0.0 <= 17.0.4 / ...	Misc.	1
MEDIUM	5.3	1.4	OpenJDK 7 <= 7u261 / 8 <= 8u352 / 11.0.0 <= 11.0.17 / 13.0.0 <= 13.0.13 / 15.0.0 <= 15.0.9 / 17.0.0 <= 17.0.5 / ...	Misc.	1

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



The screenshot shows the Nessus Essentials interface with the details of a High severity vulnerability (OpenJDK 8 <= 8u362 / 11.0.0 <= 11.0.18 / 17.0.0 <= 17.0.6 / 20.0.0 <= 20.0.0 Multiple Vulnerabilities (2023-04-18)). The details include a description, a list of affected versions, and a list of CVEs.

Description
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 as referenced in the 2023-04-18 advisory.

Please Note: Java CVEs do not always include OpenJDK versions, but are confirmed separately by Tenable using the patch versions from the referenced OpenJDK security advisory.

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit: vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2023-21930)
- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit: vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2023-21954)

Plugin Details

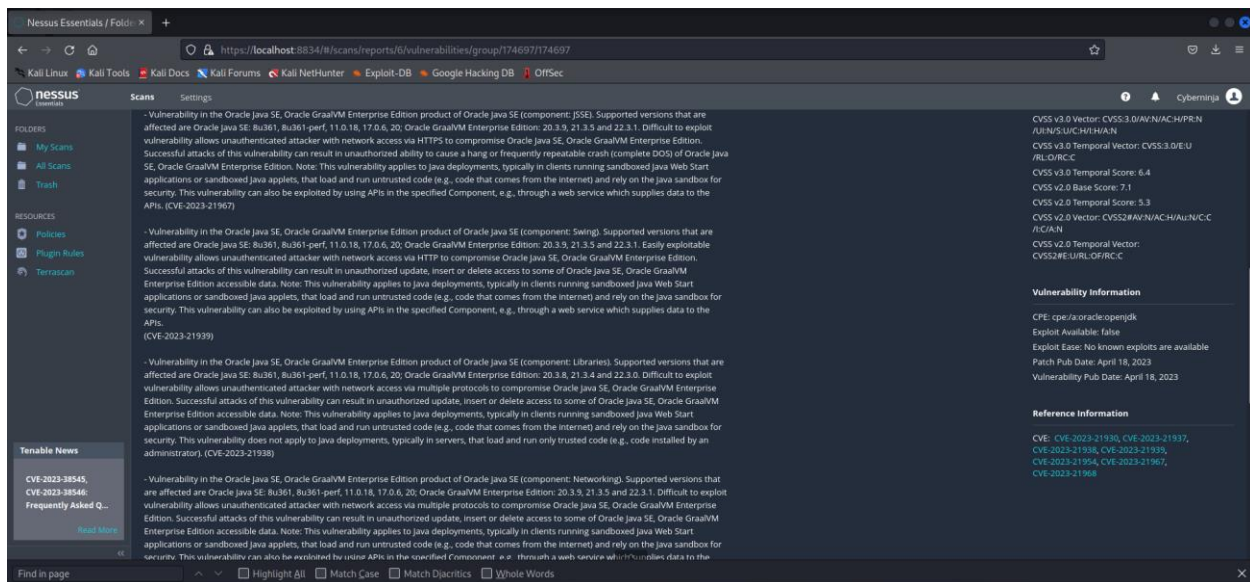
- Severity: High
- ID: 174697
- Version: 1.0
- Type: local
- Family: Misc.
- Published: April 25, 2023
- Modified: April 25, 2023

VPR Key Drivers

- Threat Recency: 120 to 365 days
- Threat Intensity: Very Low
- Exploit Code Maturity: Unproven
- Age of Vuln: 60 - 180 days
- Product Coverage: Medium
- CVSSv3 Impact Score: 5.2
- Threat Sources: No recorded events

Risk Information

- Vulnerability Priority Rating (VPR): 6.0
- Risk Factor: High

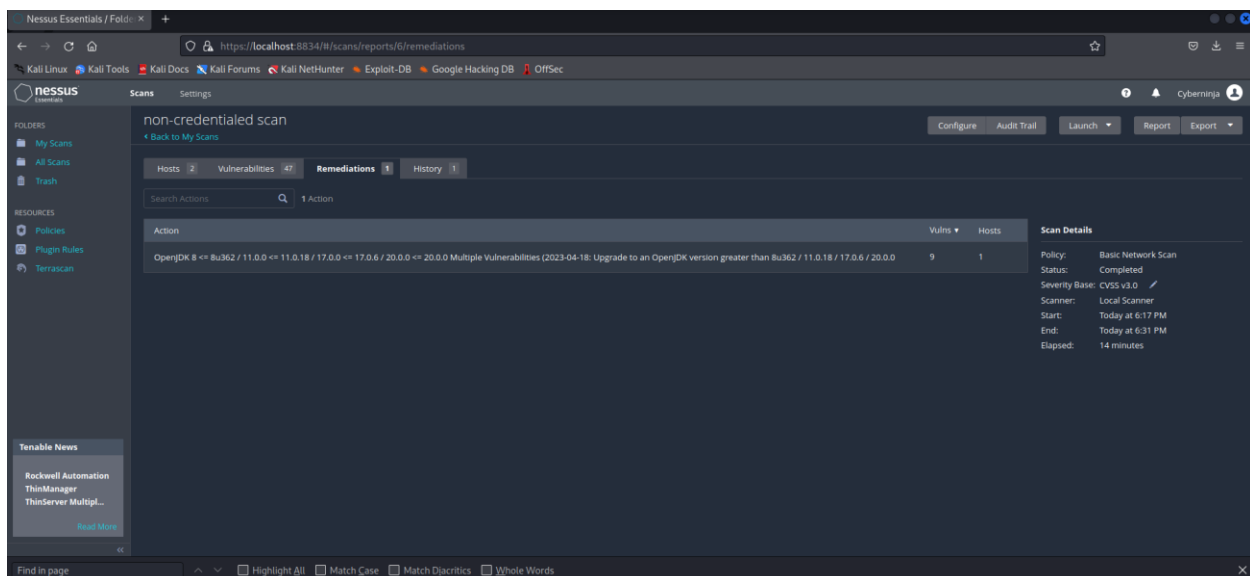


4) What CVE is associated with the finding?

- 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

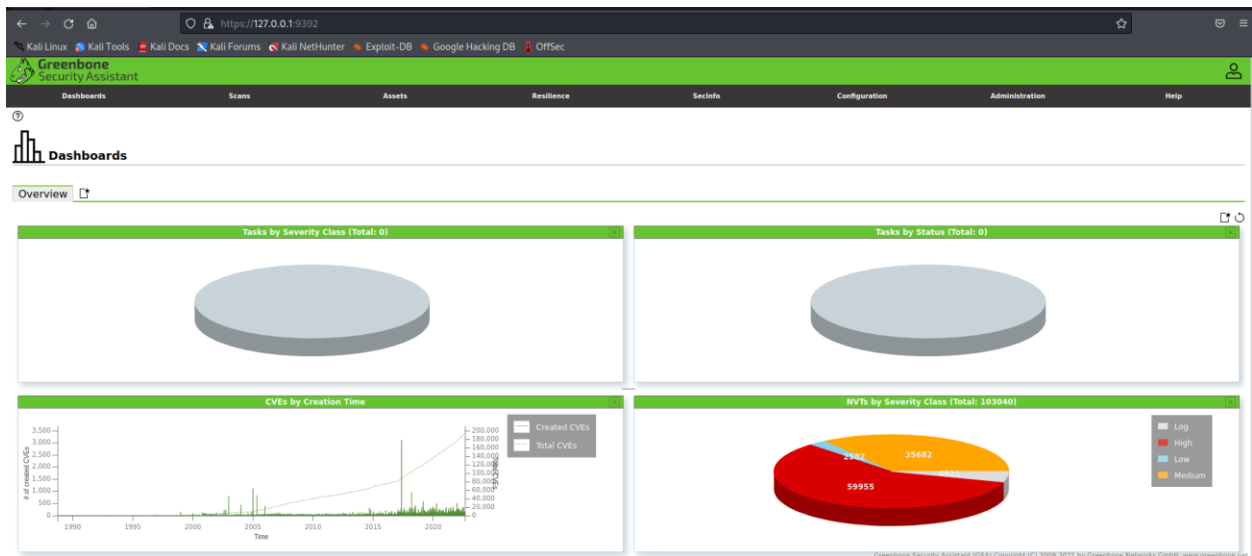


Using OpenVAS

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

New Task

Name

Teest Sacn

Comment

Scan Targets

First Scan

Alerts

Schedule

--

☐ Once

Add results to Assets

☒ Yes ☐ No

Apply Overrides

☒ Yes ☐ No

Min QoD

70

%

Alterable Task

☐ Yes ☒ No

Auto Delete Reports

☒ Do not automatically delete reports

☐ Automatically delete oldest reports but always keep newest

5

reports

Scanner

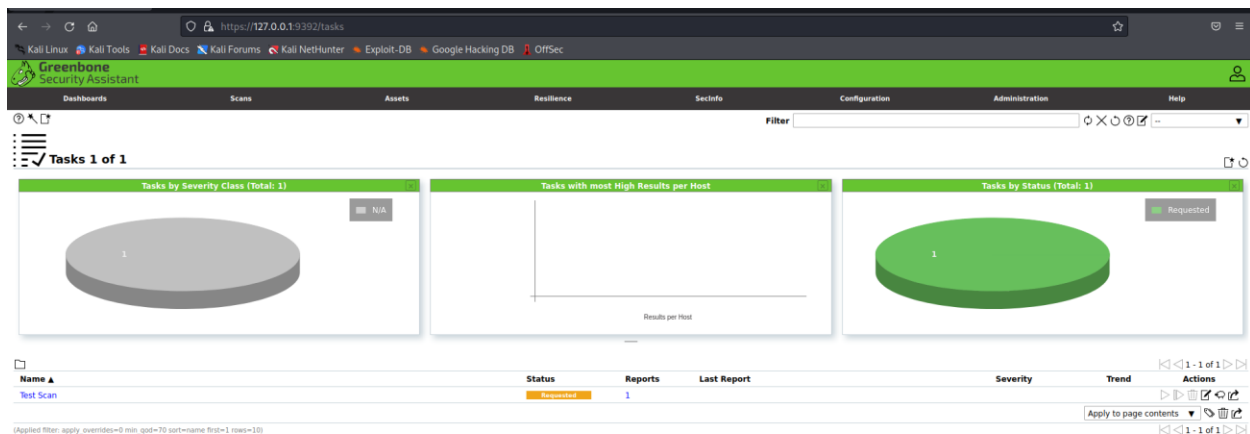
OpenVAS Default

Scan Config

Full and fast

Cancel

Save



Greenbone Security Assistant

Report: Thu, Oct 12, 2023 8:26 PM UTC

Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags

Task Name: Test Scan

Scan Time: Thu, Oct 12, 2023 8:27 PM UTC - Thu, Oct 12, 2023 8:35 PM UTC

Scan Duration: 0:07 h

Scan Status: Done

Hosts scanned: 3

Filter: apply_overrides=0 levels=html_min_qod=70

Timezone: UTC (UTC)

Greenbone Security Assistant

Report: Thu, Oct 12, 2023 8:26 PM UTC

Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags

Vulnerability

Severity	QoD	Host IP	Name	Location	Created
10.0 (High)	97 %	192.168.110.164	Report outdated / end-of-life Scan Engine / Environment (local)	general/tcp	Thu, Oct 12, 2023 8:28 PM UTC
10.0 (High)	97 %	192.168.110.2	Report outdated / end-of-life Scan Engine / Environment (local)	general/tcp	Thu, Oct 12, 2023 8:28 PM UTC
10.0 (High)	97 %	192.168.110.1	Report outdated / end-of-life Scan Engine / Environment (local)	general/tcp	Thu, Oct 12, 2023 8:28 PM UTC
10.0 (High)	80 %	192.168.110.1	DCE/RPC and MSRPC Services Enumeration Reporting	135/tcp	Thu, Oct 12, 2023 8:32 PM UTC
5.0 (Low)	80 %	192.168.110.1	TCP timestamps	general/tcp	Thu, Oct 12, 2023 8:30 PM UTC

(Applied filter: apply_overrides=0 levels=html_min_qod=70 first=1 sort=reverse=severity)

You can click on each reported vulnerability to get details.

Greenbone Security Assistant

Vulnerability

Report outdated / end-of-life Scan Engine / Environment (local)

Summary

This script checks and reports an outdated or end-of-life scan engine for the following environments:

- Greenbone Source Edition (GSE)
- Greenbone Enterprise TRIAL (formerly Greenbone Security Manager TRIAL / Greenbone Community Edition (GCE))

used for this scan.

NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.:

- missing functionalities
- missing bugfixes
- incompatibilities within the feed

Detection Result

Version of installed component: 21.4.4 (Installed component: openvas-libraries on OpenVAS <= 9, openvas-scanner on Greenbone Community Edition <= 18)

Latest available openvas-scanner version: 22.7.3

Reference URL(s) for the latest available version: <https://forum.greenbone.net/t/greenbone-community-edition-22-4-stable-initial-release-2022-07-25/12638>

Detection Method

Details: [Report outdated / end-of-life Scan Engine / Environment \(local\)](#) OID: 1.3.6.1.4.1.25623.1.0.108560

Version used: 2022-03-17T11:03:48Z

Solution

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.nl

Greenbone

Security Assistant

Dashboard

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

Filter

Report: Thu, Oct 12, 2023 8:26 PM UTC

ID: 024711c9-9643-4751-b611-118973ebbb5c

Created: Thu, Oct 12, 2023 8:27 PM UTC

Modified: Thu, Oct 12, 2023 8:35 PM UTC

Owner: admin

Information

Results
(3 of 28)

Hosts
(2 of 3)

Ports
(1 of 5)

Applications
(0 of 0)

Operating Systems
(3 of 3)

CVEs
(0 of 0)

Closed CVEs
(7 of 7)

TLS Certificates
(0 of 0)

Error Messages
(0 of 0)

User Tags
(0)

CVE

Host

NVT

Severity

CVE-2010-0020

192.168.110.1

Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

Critical

CVE-2010-0021

192.168.110.1

Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

Critical

CVE-2010-0022

192.168.110.1

Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

Critical

CVE-2010-0231

192.168.110.1

Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

Critical

CVE-2009-2526

192.168.110.1

Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability

Critical

CVE-2009-2532

192.168.110.1

Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability

Critical

CVE-2009-3103

192.168.110.1

Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability

Critical

Applied filter: apply_overrides=0 level=info rows=100 min_age=70 (unit=d) sort=reverse(severity)

<<

1 - 7 of 7

>>

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.

Scan Configs 7 of 7									
Name ▲	Type	Family	Trend	NVTs Total	Trend	Actions			
Base <small>(Basic configuration template with a minimum set of NVTs required for a scan. Version 20200827.)</small>	OpenVAS	2	→	3	→	🗑️ 🔍 ↺ ⌂			
Discovery <small>(Network Discovery scan configuration. Version 20201215.)</small>	OpenVAS	10	↗	3137	↗	🗑️ 🔍 ↺ ⌂			
empty <small>(Empty and static configuration template. Version 20201215.)</small>	OpenVAS	0	→	0	→	🗑️ 🔍 ↺ ⌂			
Full and fast <small>(Most NVT's optimized by using previously collected information. Version 20201215.)</small>	OpenVAS	58	↗	103027	↗	🗑️ 🔍 ↺ ⌂			
Host Discovery <small>(Network Host Discovery scan configuration. Version 20201215.)</small>	OpenVAS	2	→	2	→	🗑️ 🔍 ↺ ⌂			
Log4shell <small>(Configuration with checks for Log4j and CVE-2021-44228. Version 20211227.)</small>	OpenVAS	10	↗	29	→	🗑️ 🔍 ↺ ⌂			
System Discovery <small>(Network System Discovery scan configuration. Version 20201215.)</small>	OpenVAS	5	→	30	→	🗑️ 🔍 ↺ ⌂			

(Applied filter: sort=name first=1 rows=10)

