Experiment 14

AIM:Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities

Roll No.	70
Name	MAYURI SHRIDATTA YERANDE
Class	D15-B
Subject	Internet Security Lab
LO Mapped	LO6: Demonstrate the network security system using open source tools.

AIM: Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities.

THEORY:

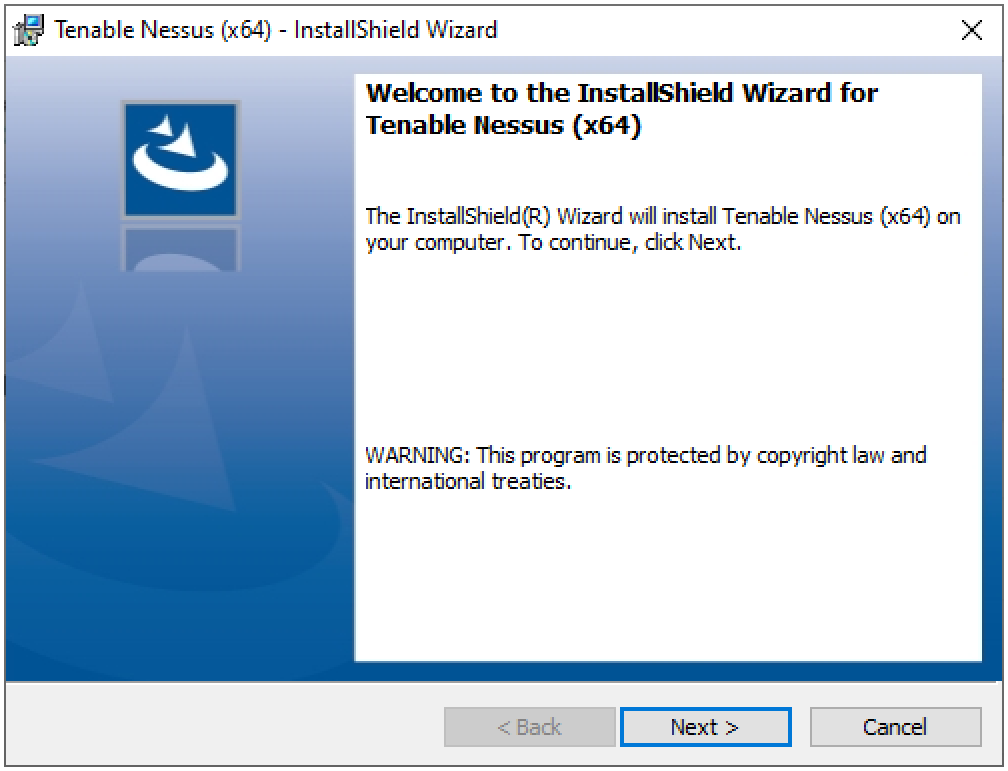
Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. This article will focus on this vulnerability scanner, discussing the fundamentals that one needs to have before getting started with the tool, the different scanning capabilities that it provides, what it takes to run the tool and how results appear once scans are complete.

Nessus is the most trusted, accurate, and reliable vulnerability scanner on the market, making it a perfect complement to your penetration tests and security assessments. Nessus Manager (and Nessus Cloud) allows you to further extend your vulnerability scanning program by engaging others in IT and auditing through sharing of scanning resources (including assigning roles, scanners, reports, policies, and more). Tenable other products, such as the Passive Vulnerability Scanner and SecurityCenter Continuous View, enable IT organizations to implement a continuous monitoring solution to collect vulnerability and operational data via scanning, sniffing and logging. All of these technologies combined allow for deep insights into your network, and any threats that may be lurking.

IMPLEMENTATION:

Installation:

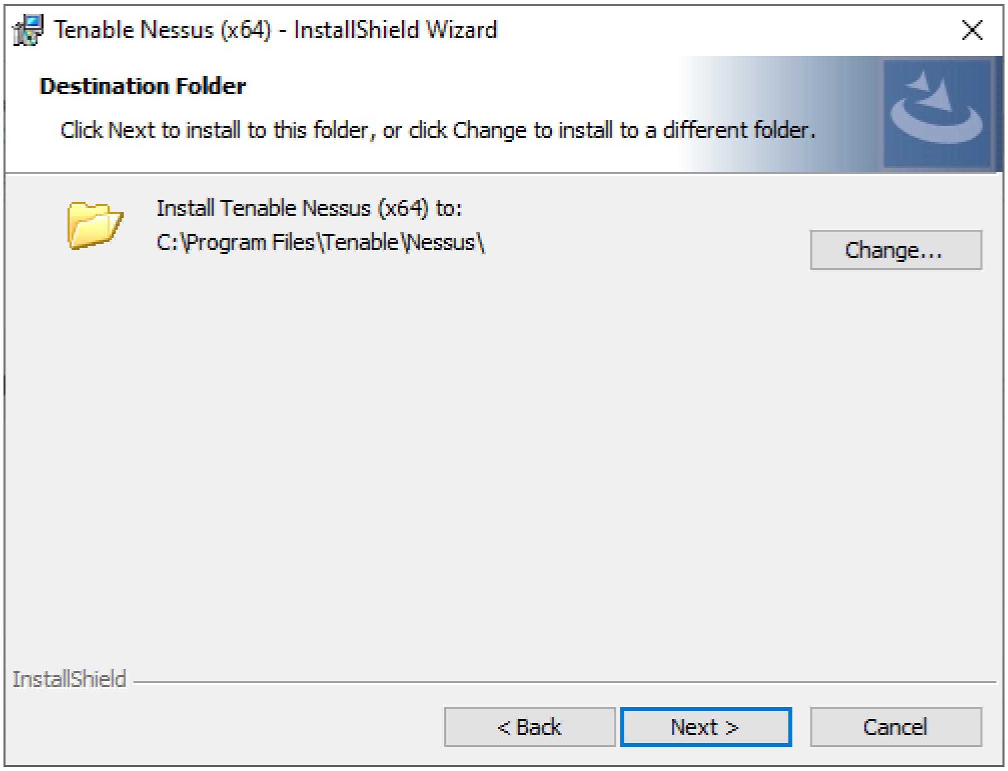
- Download Link:- https://www.tenable.com/downloads/nessus?loginAttempted=true


Tenable Nessus (x64) - InstallShield Wizard

Welcome to the InstallShield Wizard for Tenable Nessus (x64)

The InstallShield(R) Wizard will install Tenable Nessus (x64) on your computer. To continue, click Next.

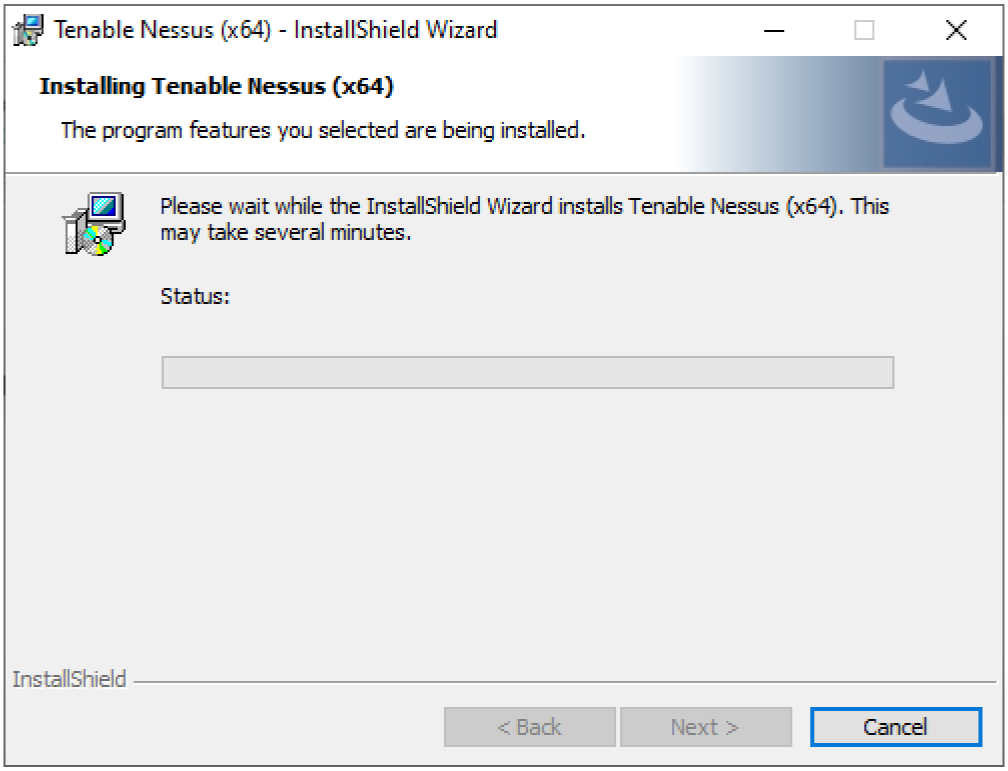
WARNING: This program is protected by copyright law and international treaties.


Tenable Nessus (x64) - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Tenable Nessus (x64) to:
C:\Program Files\Tenable\Nessus\



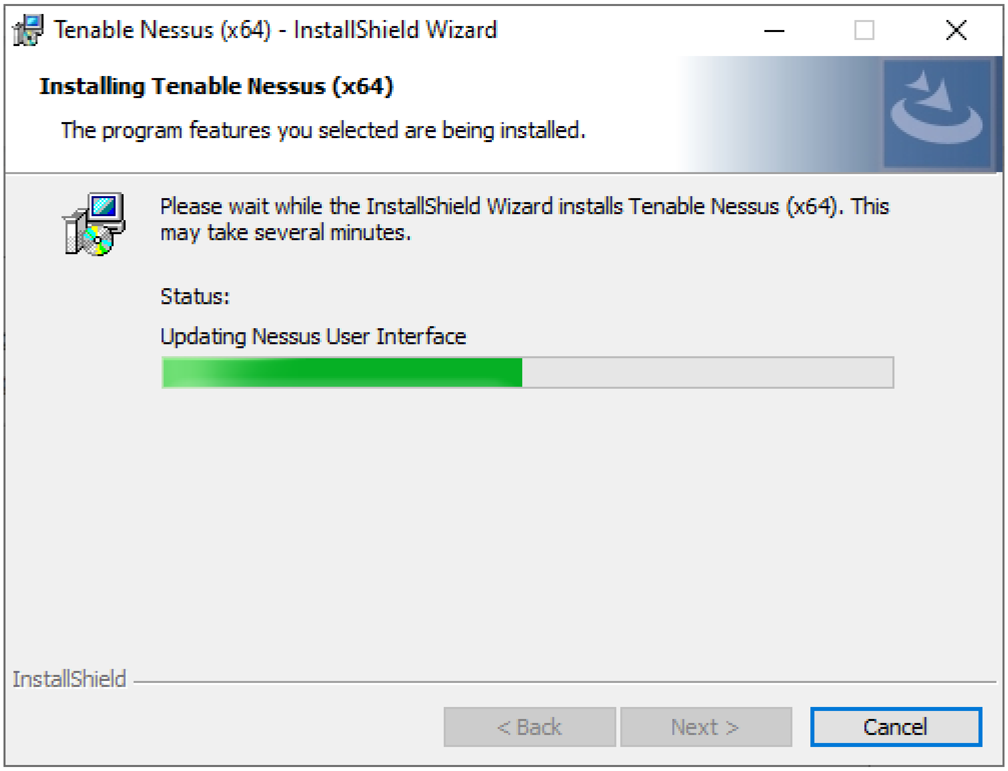
Tenable Nessus (x64) - InstallShield Wizard

Installing Tenable Nessus (x64)

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs Tenable Nessus (x64). This may take several minutes.

Status:



Tenable Nessus (x64) - InstallShield Wizard

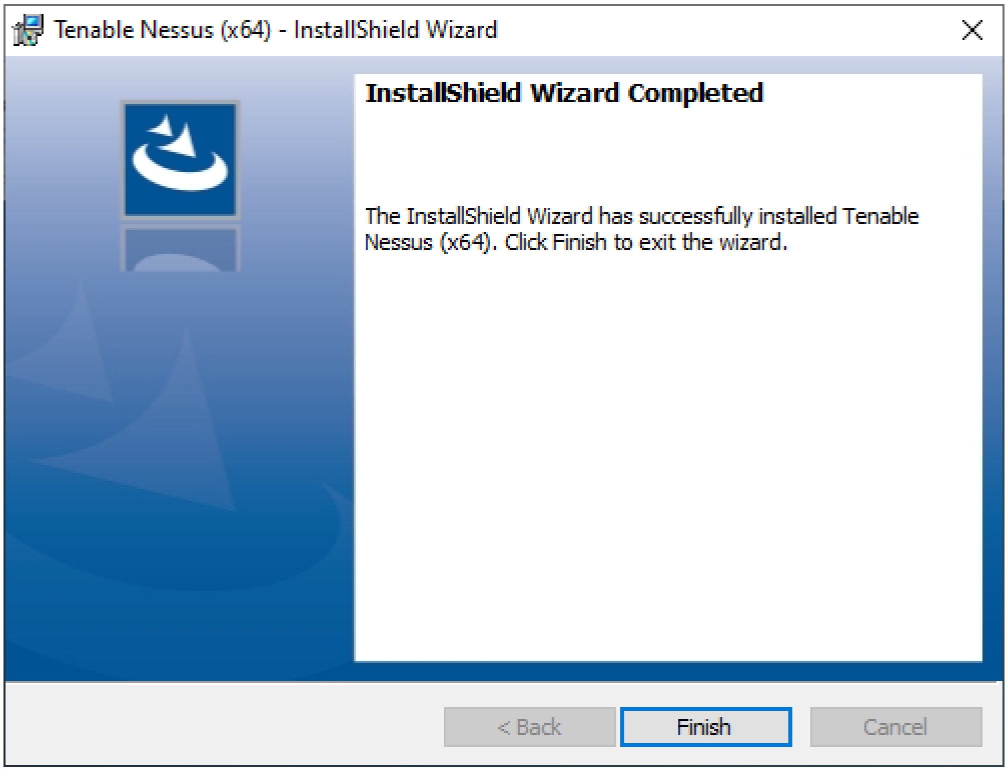
Installing Tenable Nessus (x64)

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs Tenable Nessus (x64). This may take several minutes.

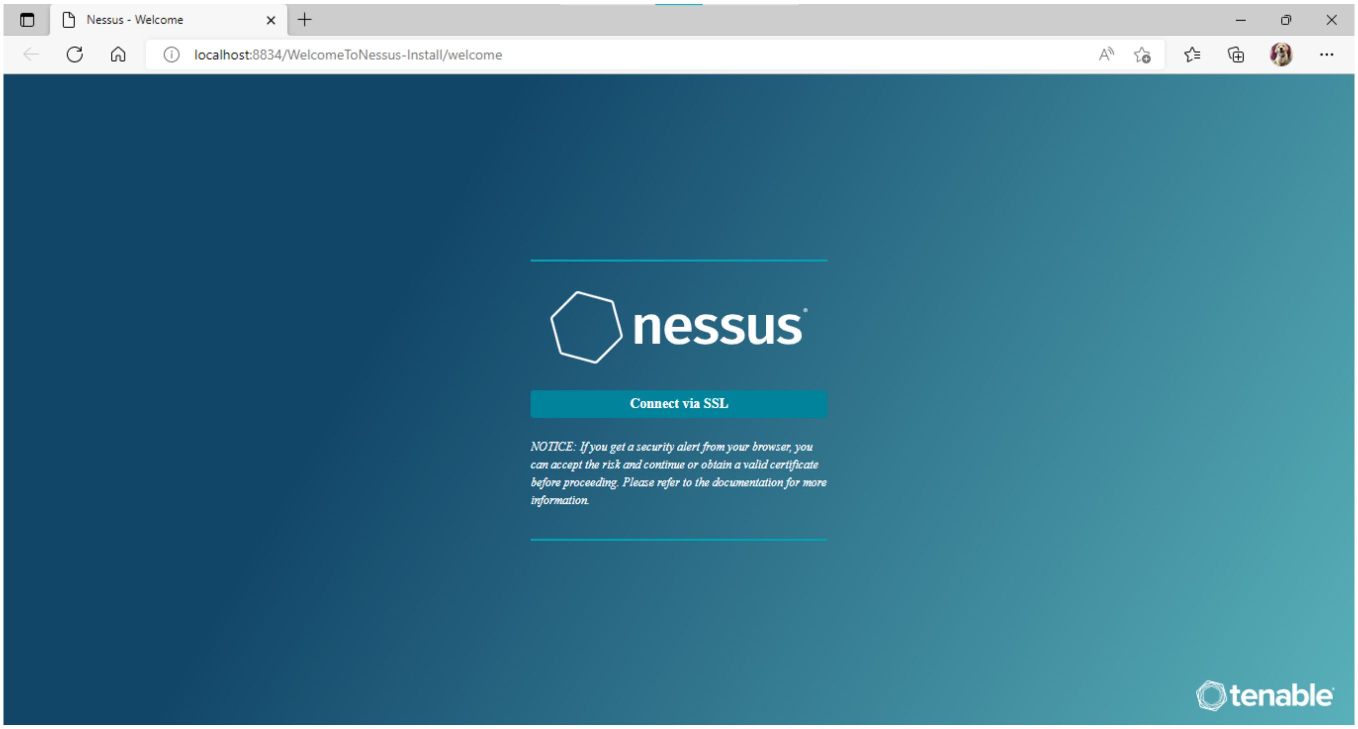
Status:

Updating Nessus User Interface



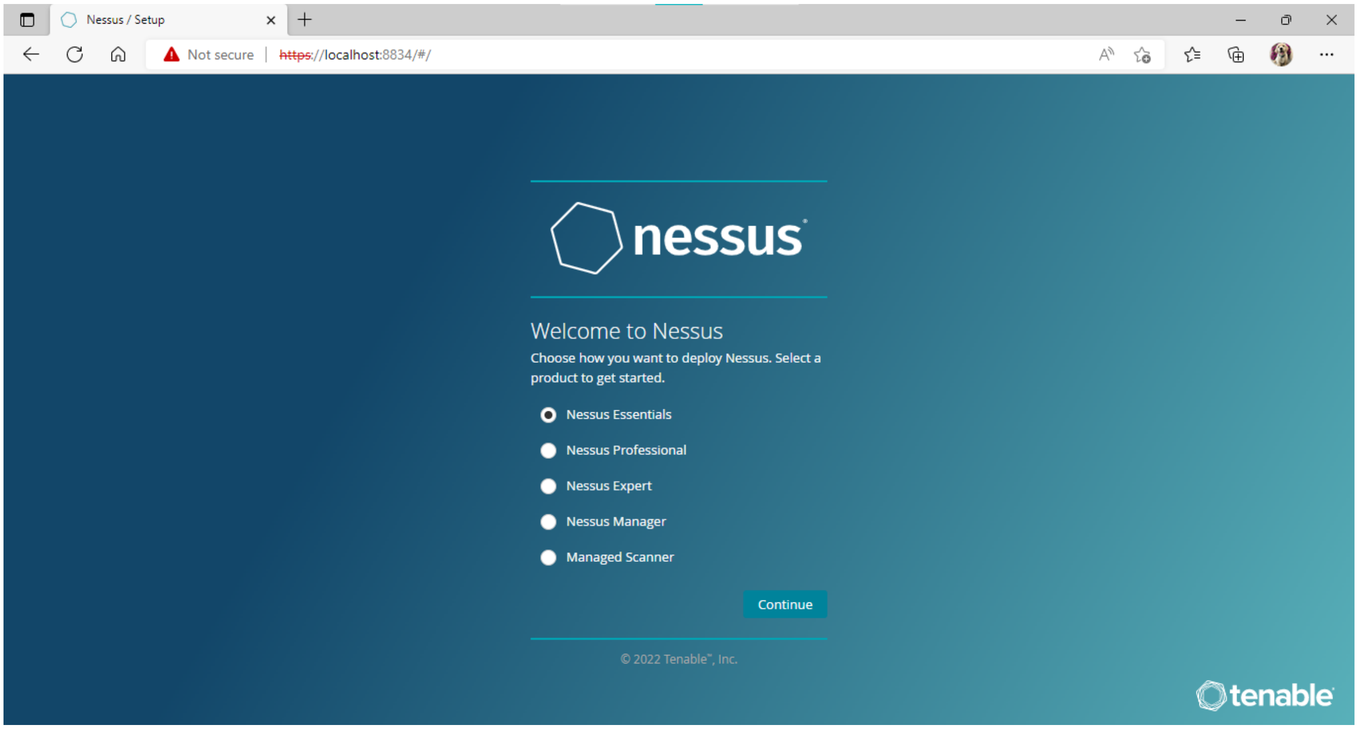
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Tenable Nessus (x64). Click Finish to exit the wizard.



NOTICE: If you get a security alert from your browser, you can accept the risk and continue or obtain a valid certificate before proceeding. Please refer to the documentation for more information.

- Nessus is successfully installed
- “Go to connect Via SSL”



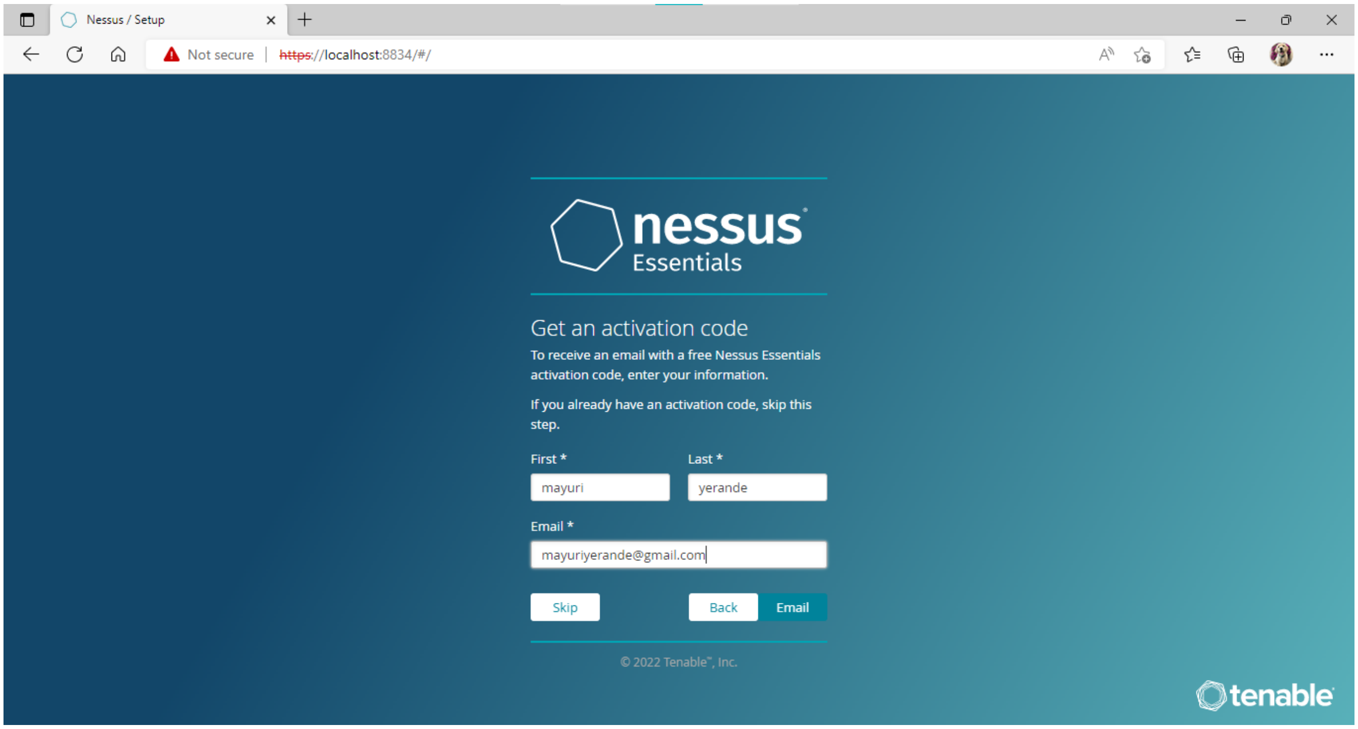
Welcome to Nessus

Choose how you want to deploy Nessus. Select a product to get started.

- ● Nessus Essentials
- ○ Nessus Professional
- ○ Nessus Expert
- ○ Nessus Manager
- ○ Managed Scanner

© 2022 Tenable™, Inc.

- Choose “nessus essential”
- enter your details



Get an activation code

To receive an email with a free Nessus Essentials activation code, enter your information.

If you already have an activation code, skip this step.

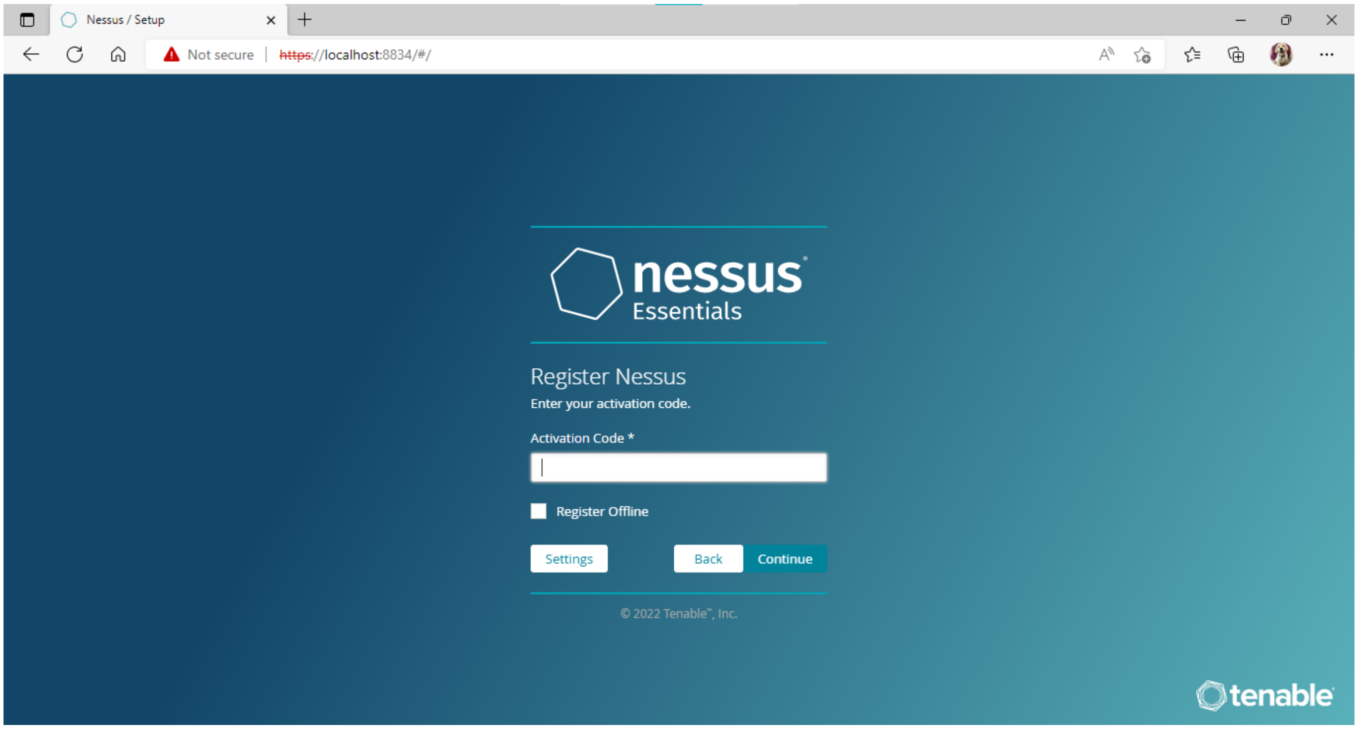
First * mayuri

Last * yerande

Email * mayuriyerande@gmail.com

© 2022 Tenable™, Inc.

- Enter the activation code that you received on your email



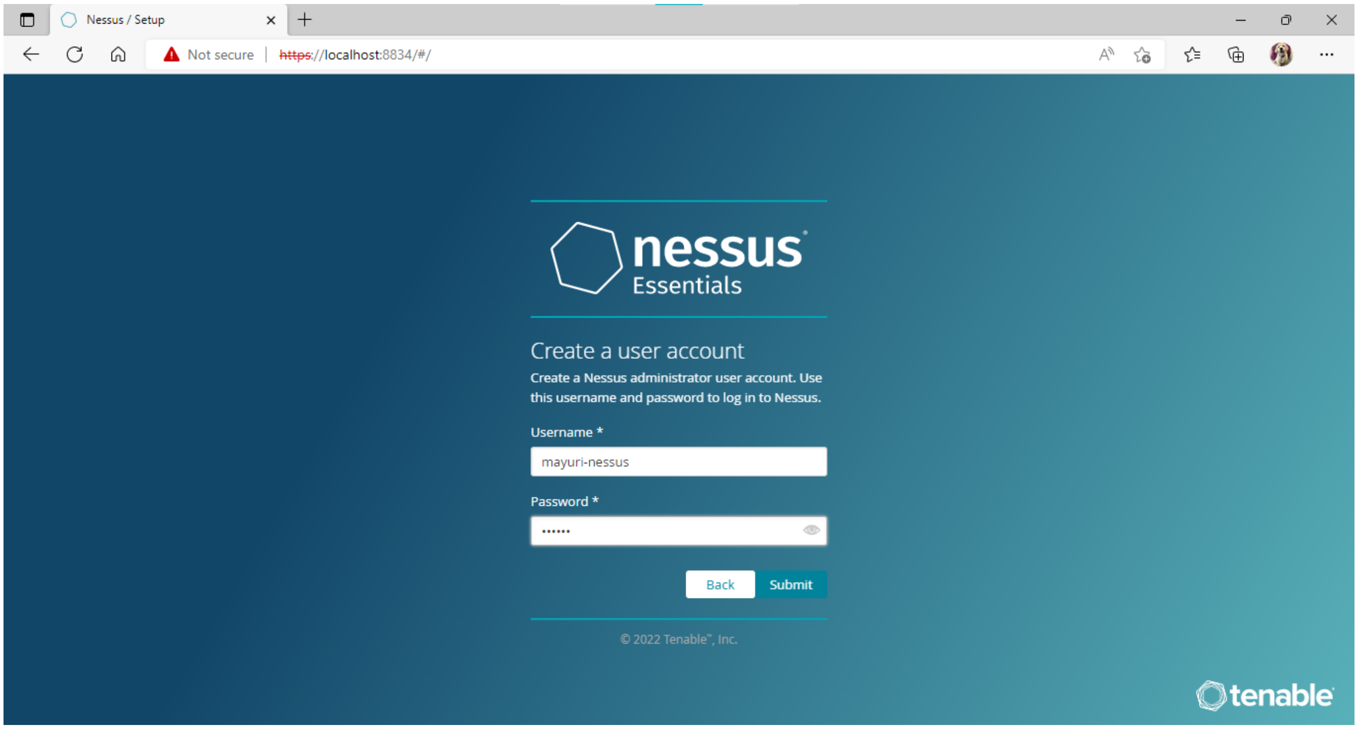
Register Nessus

Enter your activation code.

Activation Code *

□ Register Offline

- Create username



Create a user account

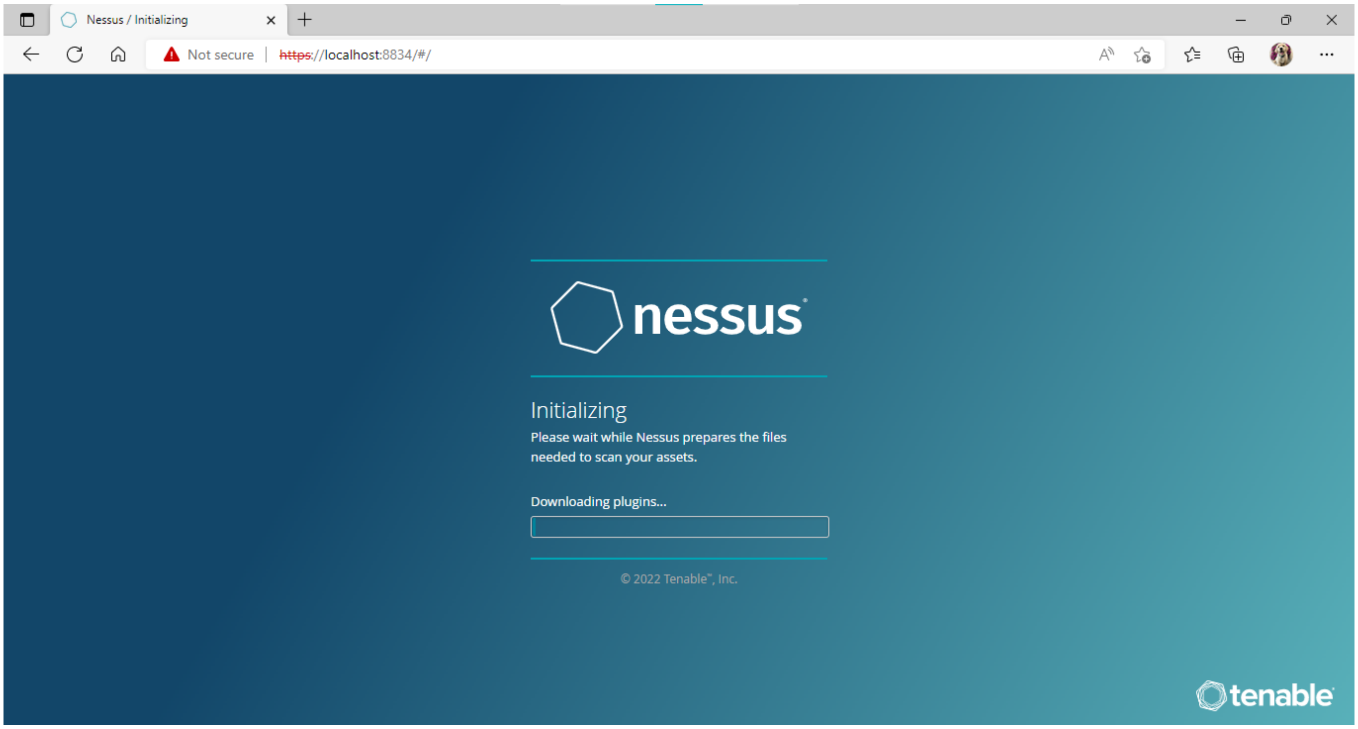
Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *

mayuri-nessus

Password *

••••••

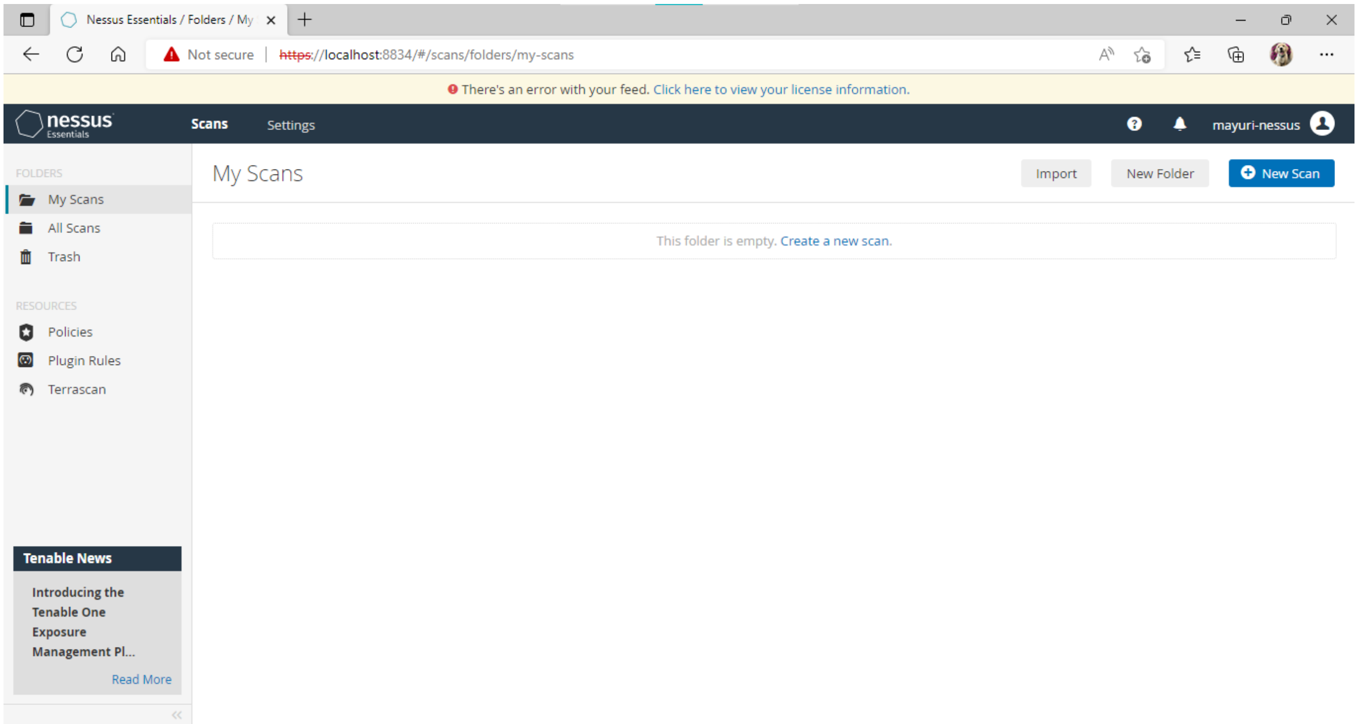


Initializing

Please wait while Nessus prepares the files needed to scan your assets.

Downloading plugins...

© 2022 Tenable™, Inc.



There's an error with your feed. Click here to view your license information.

My Scans

This folder is empty. Create a new scan.

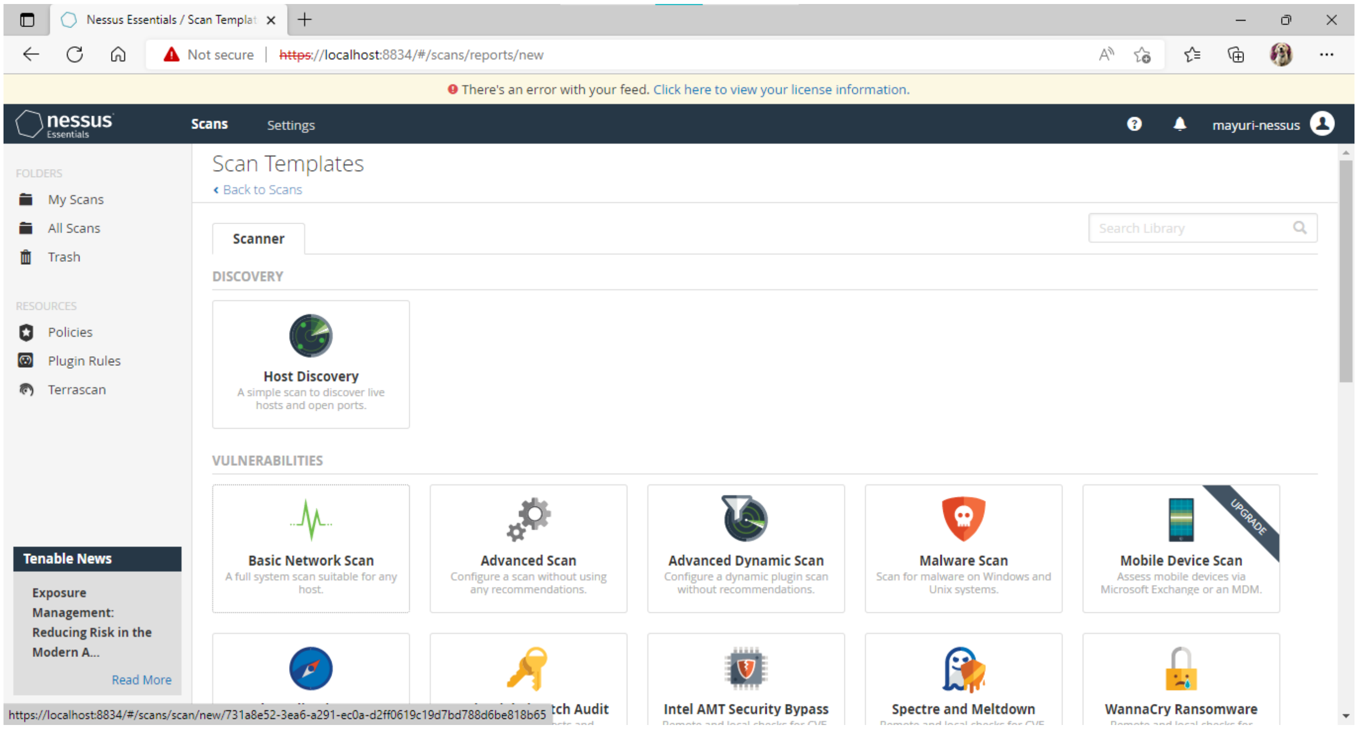
Tenable News

Introducing the Tenable One Exposure Management Pl...

Read More

- You can now use nessus.

- Go to “new scan”
- open up “basic network scan”

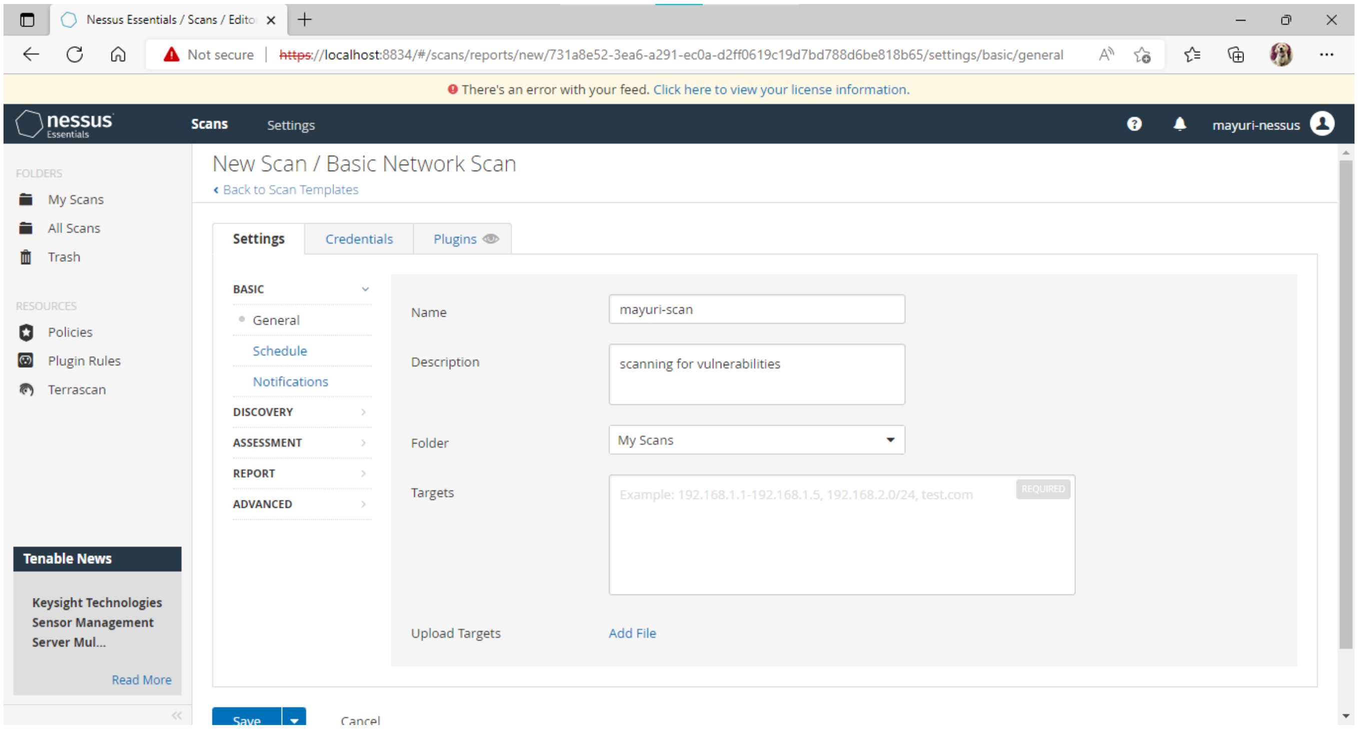


https://localhost:8834/#/scans/reports/new

There's an error with your feed. Click here to view your license information.

Nessus Essentials / Scan Templat
Not secure
nessus Essentials
Scans
Settings
mayuri-nessus
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Exposure Management: Reducing Risk in the Modern A...
Read More
Scan Templates
Back to Scans
Scanner
Search Library
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
UPGRADE
tch Audit
Intel AMT Security Bypass
Spectre and Meltdown
WannaCry Ransomware
https://localhost:8834/#/scans/scan/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65

- Enter the details:



https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general

There's an error with your feed. Click here to view your license information.

New Scan / Basic Network Scan

Name: mayuri-scan

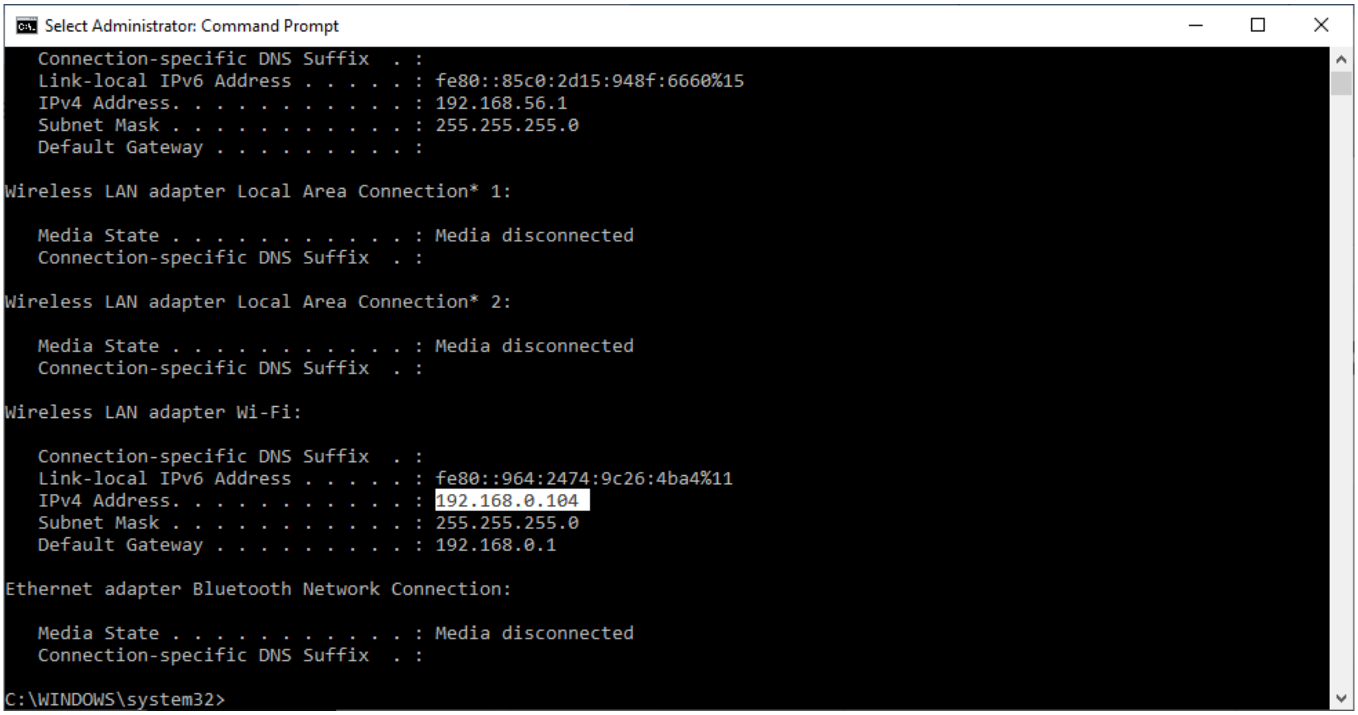
Description: scanning for vulnerabilities

Folder: My Scans

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com REQUIRED

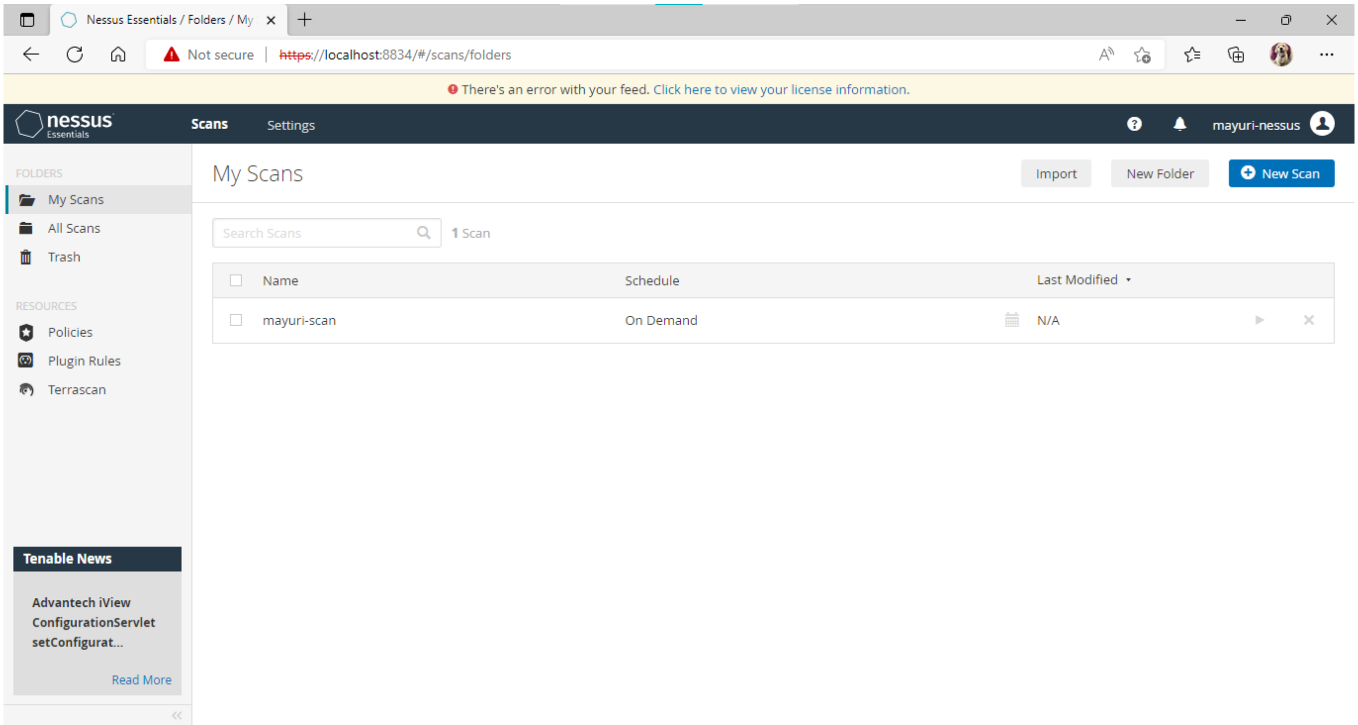
Upload Targets: Add File

- Now to get the IP address to input that in “targets” section. Go to command prompt
- and put the command “ipconfig”



```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::85c0:2d15:948f:6660%15
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::964:2474:9c26:4ba4%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\WINDOWS\system32>
```

- copy the ip address and paste it in “targets”
- Now save the scan



There's an error with your feed. Click here to view your license information.

My Scans

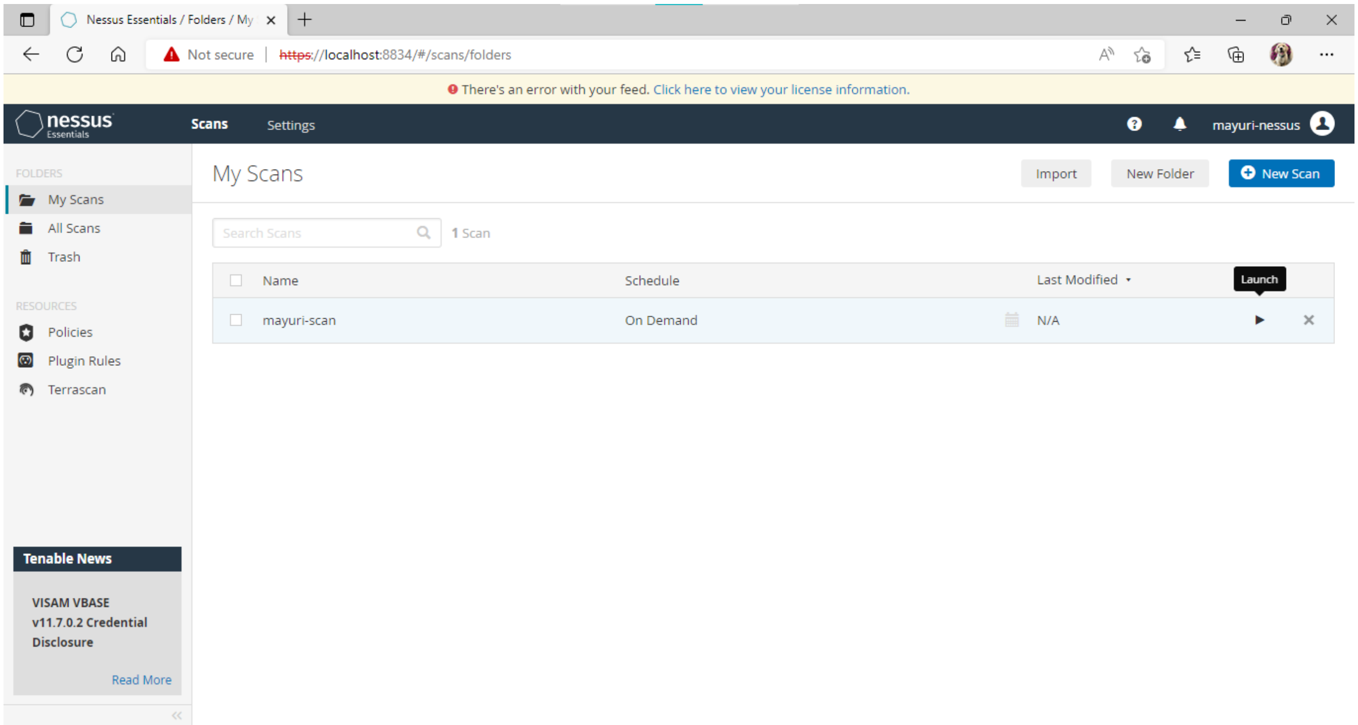
1 Scan

	Name	Schedule	Last Modified ▾
□	mayuri-scan	On Demand	N/A

Tenable News

Advantech iView ConfigurationServlet setConfigurat...

- Click on the launch button



There's an error with your feed. Click here to view your license information.

My Scans

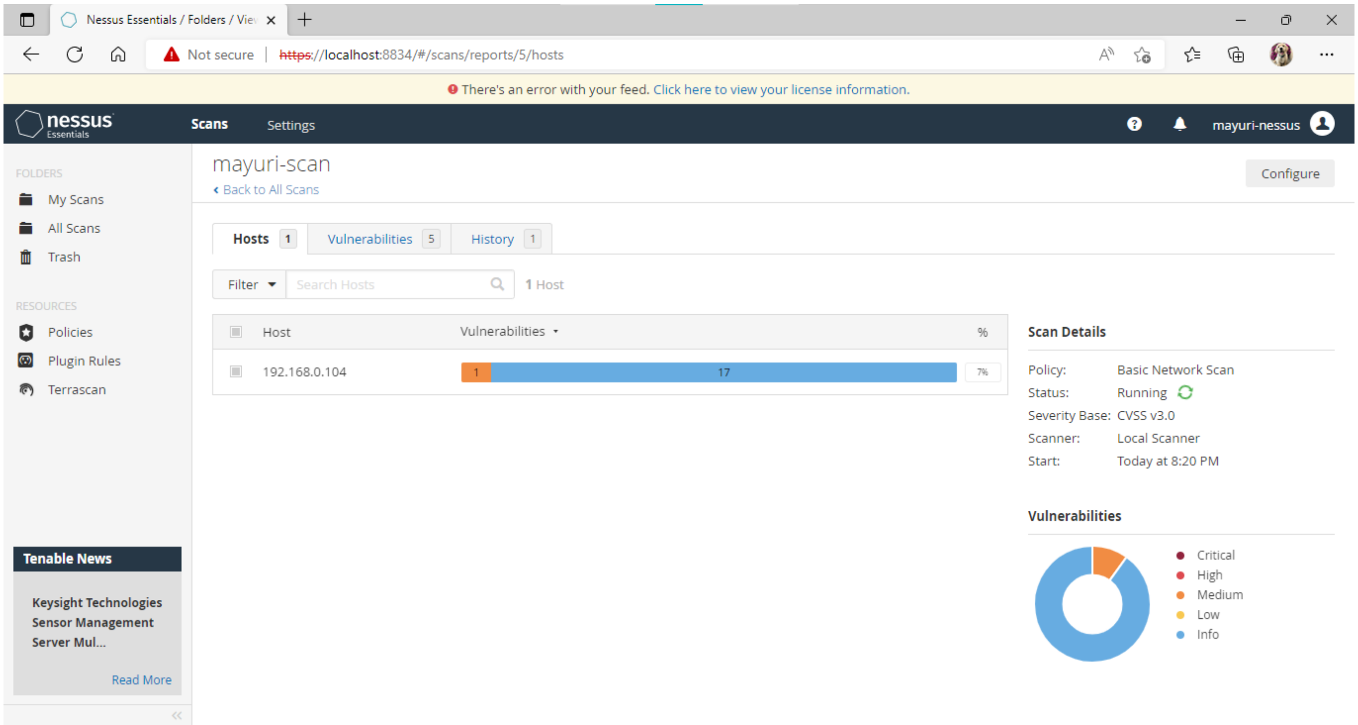
1 Scan

Name	Schedule	Last Modified
mayuri-scan	On Demand	N/A

Tenable News

VISAM VBASE v11.7.0.2 Credential Disclosure

- Your system is getting scanned



There's an error with your feed. Click here to view your license information.

mayuri-scan

1 Host

Host	Vulnerabilities	%
192.168.0.104	1 17	7%

Scan Details

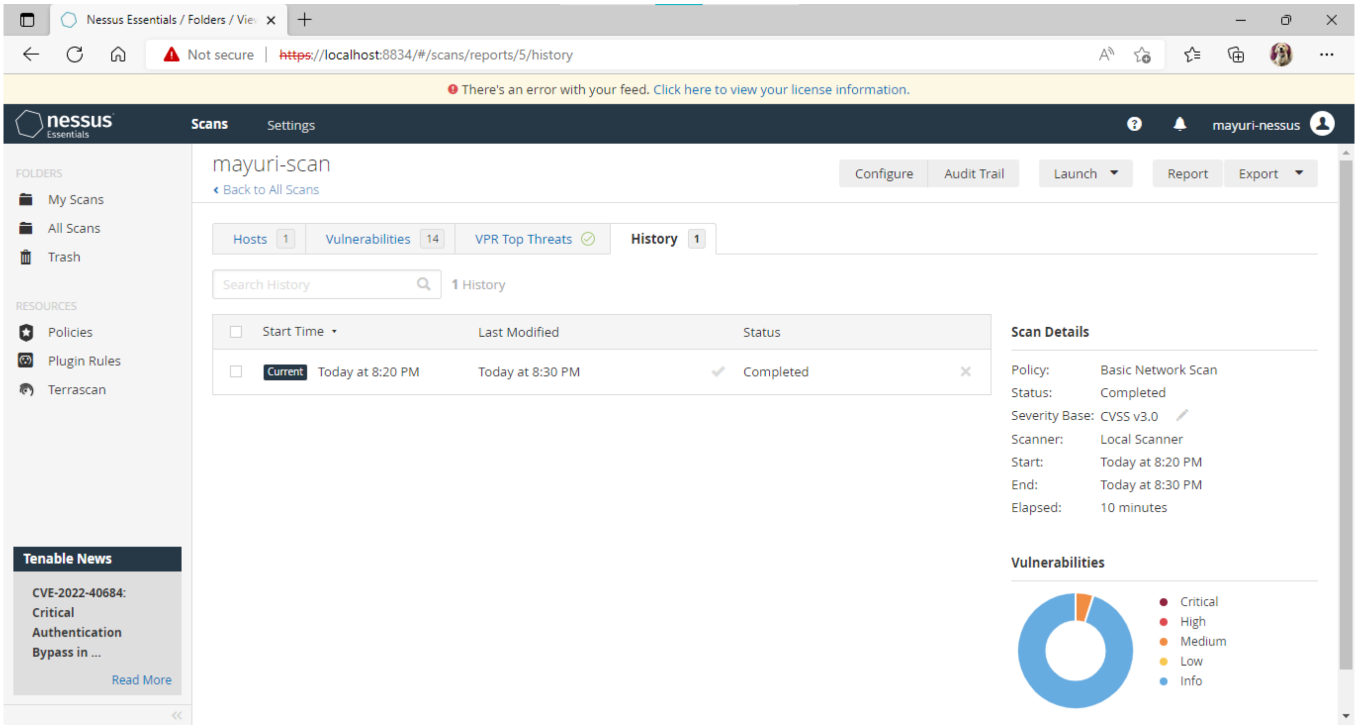
Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 8:20 PM

Vulnerabilities

Tenable News

Keysight Technologies Sensor Management Server Mul...

- Scanning is completed



There's an error with your feed. Click here to view your license information.

mayuri-scan

‹ Back to All Scans

1 History

	Start Time	Last Modified	Status
□	Current Today at 8:20 PM	Today at 8:30 PM	Completed

Scan Details

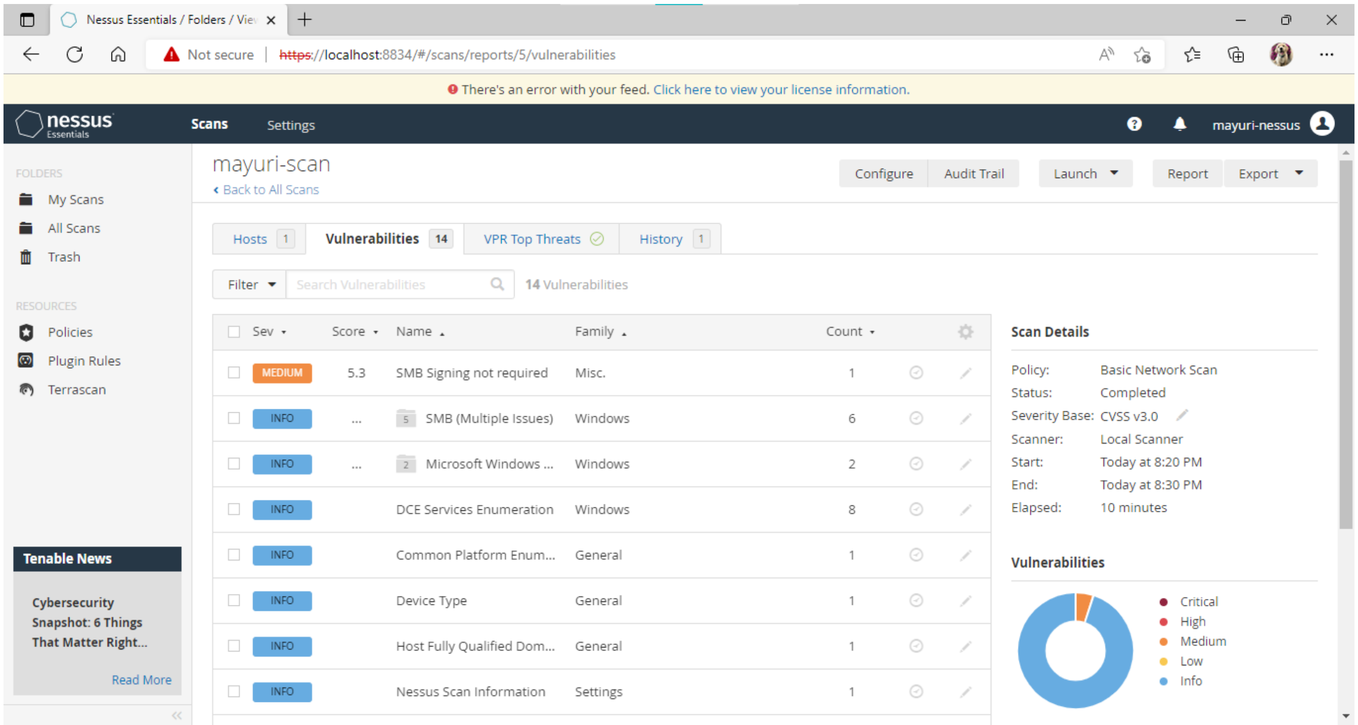
Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:20 PM
End:	Today at 8:30 PM
Elapsed:	10 minutes

Vulnerabilities

Tenable News

CVE-2022-40684: Critical Authentication Bypass in ...

- Here are the scanned vulnerabilities



There's an error with your feed. Click here to view your license information.

mayuri-scan

‹ Back to All Scans

14 Vulnerabilities

	Sev	Score	Name	Family	Count
□	MEDIUM	5.3	SMB Signing not required	Misc.	1
□	INFO	...	5 SMB (Multiple Issues)	Windows	6
□	INFO	...	2 Microsoft Windows ...	Windows	2
□	INFO		DCE Services Enumeration	Windows	8
□	INFO		Common Platform Enum...	General	1
□	INFO		Device Type	General	1
□	INFO		Host Fully Qualified Dom...	General	1
□	INFO		Nessus Scan Information	Settings	1

Scan Details

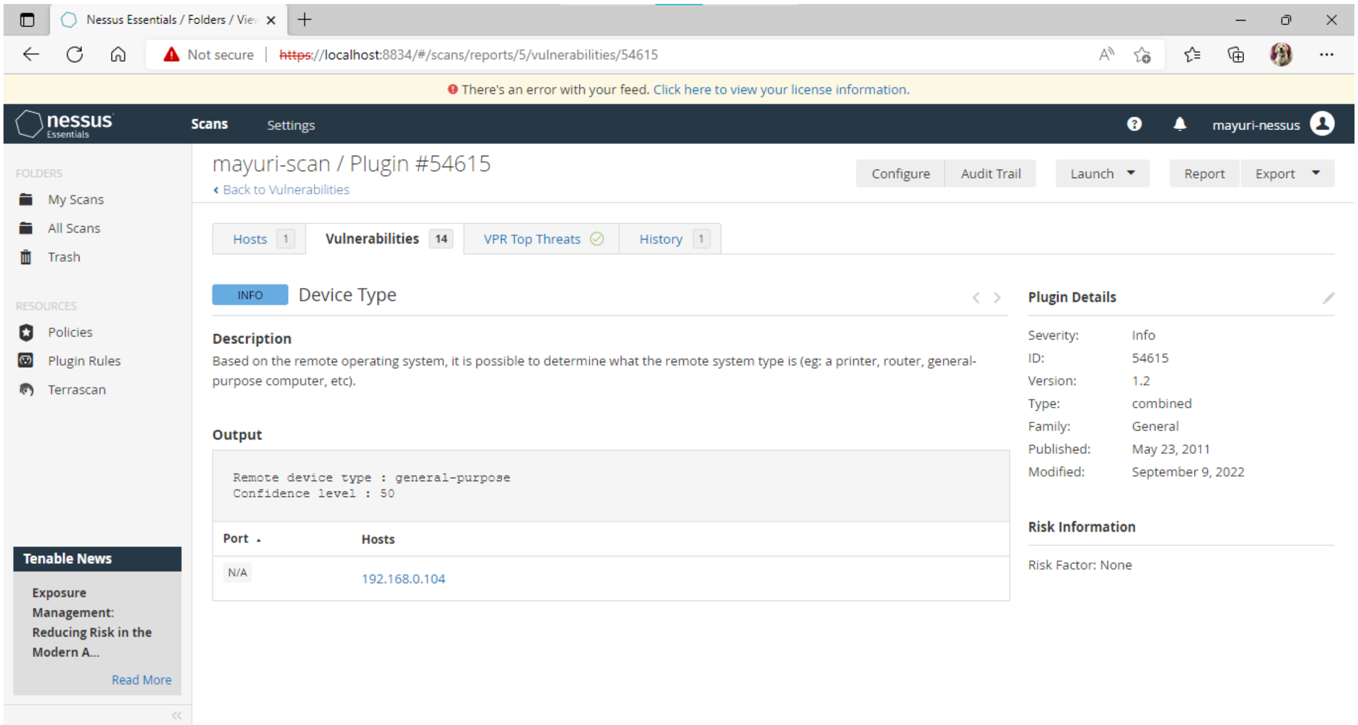
Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:20 PM
End:	Today at 8:30 PM
Elapsed:	10 minutes

Vulnerabilities

Tenable News

Cybersecurity Snapshot: 6 Things That Matter Right...

- Click on any vulnerability to check its information



Nessus Essentials / Folders / Vie

Not secure | https://localhost:8834/#/scans/reports/5/vulnerabilities/54615

There's an error with your feed. Click here to view your license information.

mayuri-scan / Plugin #54615

‹ Back to Vulnerabilities

Hosts 1 | Vulnerabilities 14 | VPR Top Threats | History 1

INFO Device Type

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Output

```
Remote device type : general-purpose
Confidence level : 50
```

Port	Hosts
N/A	192.168.0.104

Plugin Details

Severity:	Info
ID:	54615
Version:	1.2
Type:	combined
Family:	General
Published:	May 23, 2011
Modified:	September 9, 2022

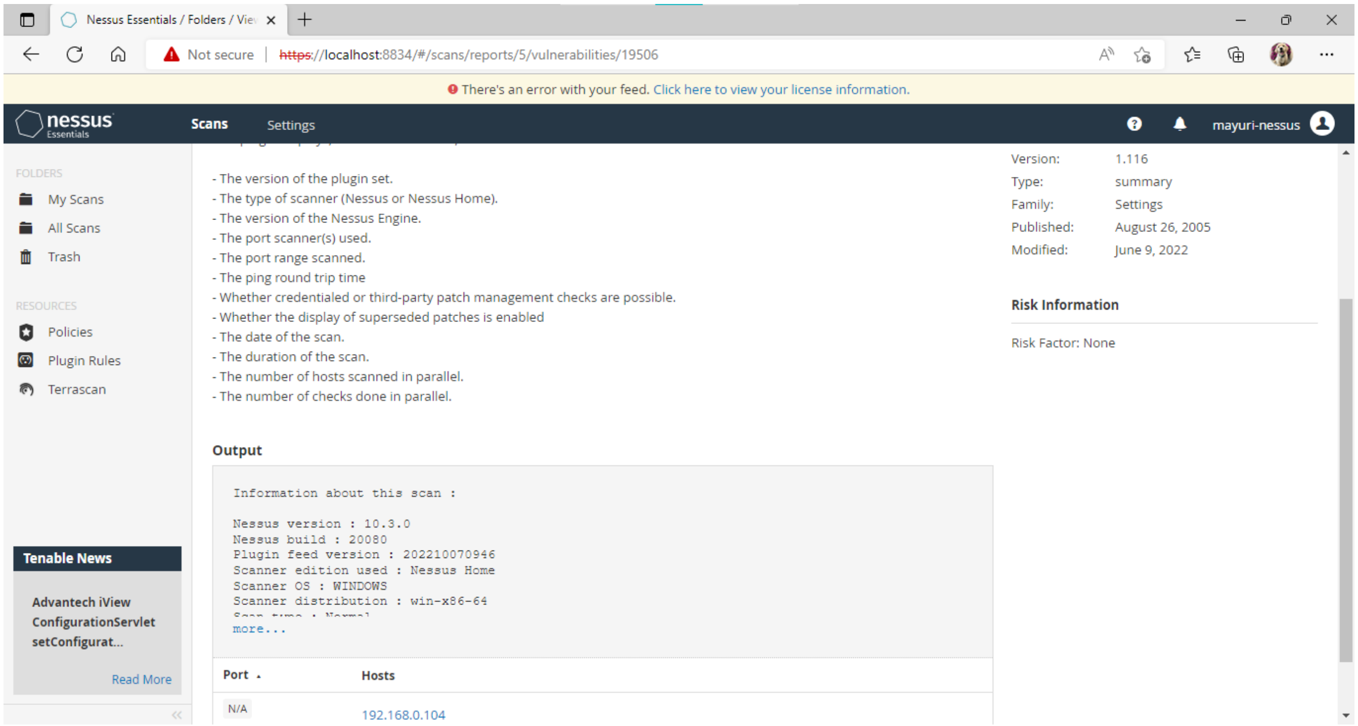
Risk Information

Risk Factor: None

Tenable News

Exposure Management: Reducing Risk in the Modern A...

Read More



Nessus Essentials / Folders / Vie

Not secure | https://localhost:8834/#/scans/reports/5/vulnerabilities/19506

There's an error with your feed. Click here to view your license information.

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Output

```
Information about this scan :

Nessus version : 10.3.0
Nessus build : 20080
Plugin feed version : 202210070946
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
more...
```

Port	Hosts
N/A	192.168.0.104

Version:	1.116
Type:	summary
Family:	Settings
Published:	August 26, 2005
Modified:	June 9, 2022

Risk Information

Risk Factor: None

Tenable News

Advantech iView ConfigurationServlet setConfigurat...

Read More

- Thus by using the “basic network scan” tool , we scanned the network for vulnerabilities.

<u>CONCLUSION:</u> We have successfully used NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities.