

NAME: Sarvesh Patil

CLASS: D15A

ROLL NO: 52

LAB 14

LAB 14: Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities.

ROLL NO	52
NAME	Sarvesh Patil
CLASS	D15A
SUBJECT	Internet Security Lab
LO MAPPED	L05: Use open-source tools to scan the network for vulnerabilities and simulate attacks.

AIM:

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

INTRODUCTION:

What is NESSUS and How Does it Work?

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Tenable.io is a subscription-based service. Tenable also contains what was previously known as Nessus Cloud, which used to be Tenable Software-as-a-Service solution. Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. In fact, Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. Nessus is a tool that checks computers to find vulnerabilities that hackers COULD exploit.

Nessus works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack.

Nessus can't scan these vulnerabilities and exposures:

- Vulnerabilities that could allow unauthorized control or access to sensitive data on a system
- Misconfiguration (e.g. open mail relay)
- Denials of service (Dos) vulnerabilities
- Default passwords, a few common passwords, and blank/absent passwords on some system accounts

Software flaws, missing patches, malware and misconfiguration errors across a wide range of operating systems, devices and applications are dealt with by Nessus.

The Nessus server is currently available for

- Unix
- Linux
- FreeBSD

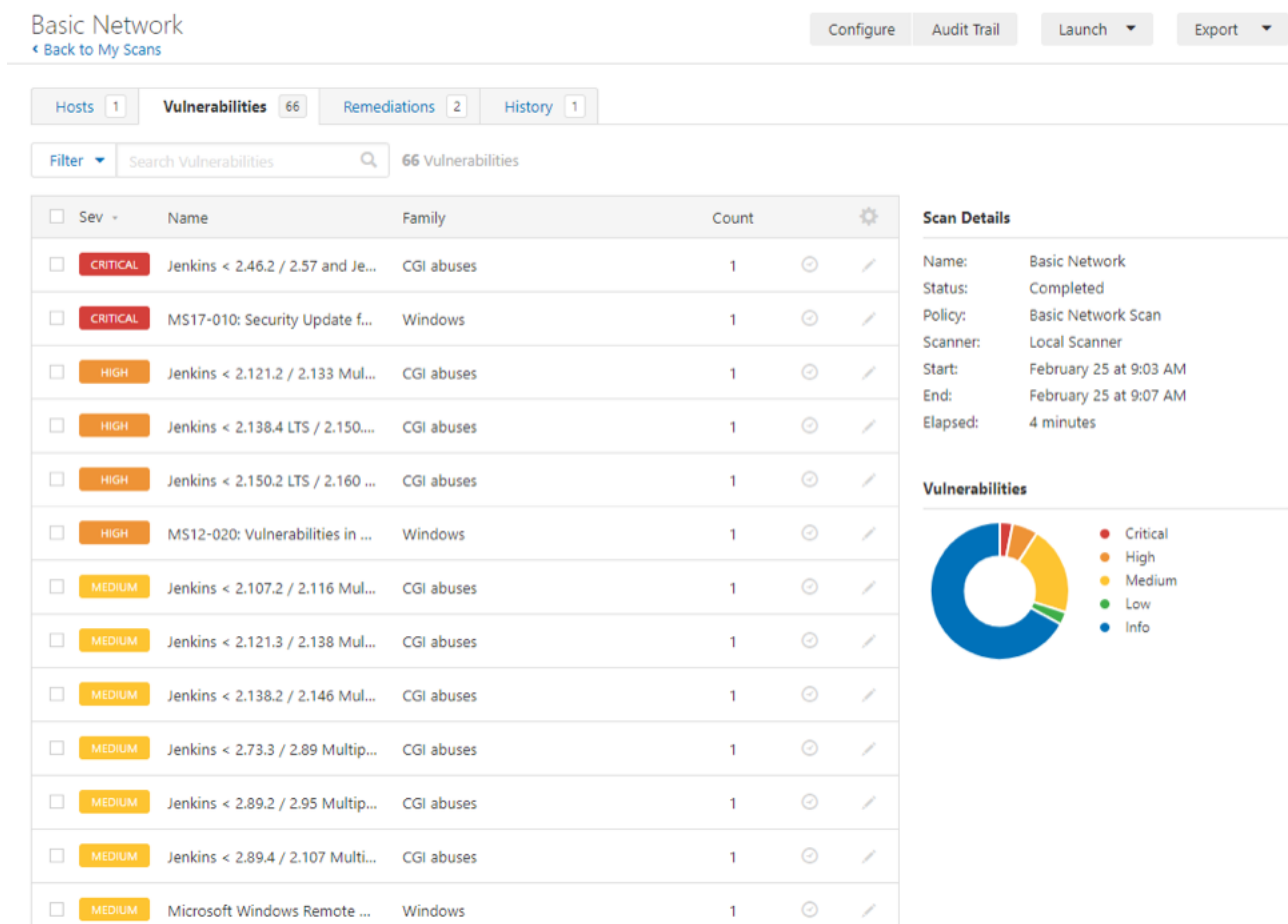
Also, the client is available for:

- Unix-based operating systems
- Windows-based operating systems

Significant capabilities of Nessus include:

- Scheduled security audits
- Detection of security holes in local or remote hosts
- Simulated attacks to pinpoint vulnerabilities
- Detection of missing security updates and patches
- Nessus Professional performs internal network scans as required by the PCI DSS 11.2.1 requirement.

The results of the scan can be reported in various formats, such as plain text, XML, and HTML. You cannot use Nessus on a system with a Host-based Intrusion Prevention System (HIPS) installed. Because during the process of scanning a remote target, Nessus must forge TCP/UDP packets and send probes that are often considered “malicious” by HIPS software. If the HIPS system is configured to block malicious traffic, it will interfere with Nessus and cause the scan results to be incomplete or unreliable.



Nessus Features

- Vulnerability Scanning
- Asset Discovery
- Network Scanning
- Vulnerability Assessment
- Prioritization
- Policy Management
- Web Scanning

What is Nessus Agent?

Nessus Agents provide a flexible way of scanning hosts within your environment without necessarily having to provide credentials to hosts. The agents enable scans to be carried out even when the hosts are offline.

Nessus Agents provide a subset of the coverage in a traditional network scan:

- Scanning of transient endpoints that are not always connected to the local network.
- Scanning assets for which you do not have credentials or could not easily obtain credentials.
- Improving overall scan performance: With agents, the network scan can be reduced to just remote network checks, speeding scan completion time.

Nessus Agents currently support a variety of operating systems including

- Windows Server 2008 and 2012, and Windows 7 and 8
- Amazon Linux
- CentOS
- Debian Linux
- OS X
- Red Hat Enterprise Linux
- Ubuntu Linux

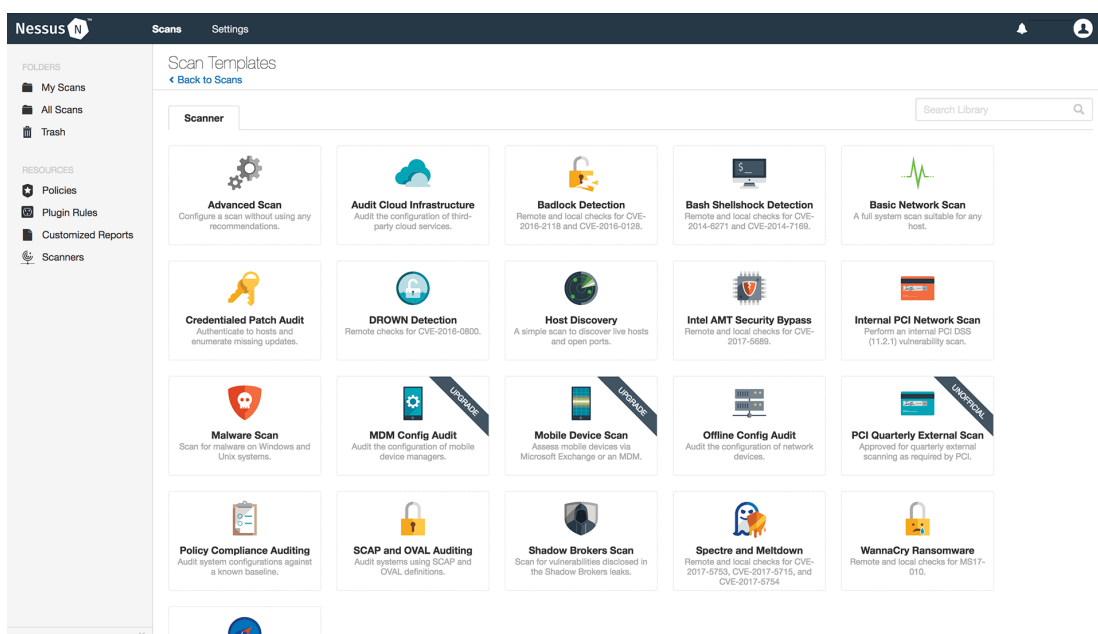
Versions and Licensing

Nessus includes two versions:

- **Nessus Professional:** This version is ideal for consultants, pen testers and security practitioners. With the ability to scan unlimited IPs, a use anywhere, and advanced features such as configuration assessment, Live Results, and custom reporting. Anyway, the IP addresses or hosts that you are scanning from must be licensed. This version does not support Mobile Device Management (MDM).
- **Nessus® Essentials:** This version is free to use to scan any environment, but is limited to 16 IP addresses per scanner.

Other advantages and features of the professional version include:

- Advanced Detection Means More Protection
- Plugins Provide Timely Protection
- Accommodate Growth and Scale Safely
- Cost Effective for Companies of All Sizes
- Accurate Visibility into Your Networks



Vulnerability Scanning with Nessus

Nessus performs its scans by utilizing plugins, which run against each host on the network in order to identify vulnerabilities. For instance, a plugin could be launched and targeted at a host to:

- Identify which operating systems and services are running on which ports
- Identify which software components are vulnerable to attacks (FTP, SSH, SMB and more)

The steps that are followed during scanning are:

- Define scan parameters
- Create scan
- Launch scan
- Analyze scan results

Once all the steps are complete, Nessus runs each host against a database of known vulnerabilities in an attempt to discover which host contains which vulnerabilities.

Ports can be defined in ranges or individually, with valid ports ranging from 1 to 65535.

Nessus gives you the ability to configure your scan based on different scan and policy templates.

These templates will determine the settings that will be found within the scan policy settings:

- **Basic:** With this setting, you can specify security-related and organizational aspects of the scan or policy, such as name of the scan, the targets of the scan, whether or not it is scheduled and who has access to it.
- **Discovery:** For defining the ports to be scanned and the methods to be used while conducting this discovery.
- **Assessment:** This setting allows you to determine the type of vulnerability scan to perform and how they are performed.
- **Report:** For determining how scan reports are generated and the information that should be included within them.
- **Advanced:** Here you will define scan efficiency and the operations that the scan should perform.

RESULTS:**1. Download and install NESSUS :**

In order to download Nessus, you'll first need to sign up for an online account so you can download the software and get an activation code.

The screenshot shows the Tenable Downloads page for Nessus. The page has a sidebar with links to various Tenable products and a main content area. The main content area is titled "Nessus" and includes a "Need an Activation Code?" section with a "Get Activation Code" button. Below this, there is a section for "Nessus - 10.3.0" with a table of download links for different operating systems.

Download Link	Operating System	File Size	Release Date	Checksum
Nessus-10.3.0-ubuntu1404_amd64.deb	Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 16.04, 17.10, 18.04, and 20.04 AMD64	53.3 MB	Jul 10, 2022	Checksum
Nessus-10.3.0-amzn2.aarch64.rpm	Amazon Linux 2 (Graviton 2)	50 MB	Jul 10, 2022	Checksum

The screenshot shows the Tenable Activation Code page. The page has a dark blue header with the Tenable logo and navigation links. The main content area is titled "Obtain an Activation Code" and features three columns for different Nessus products: Nessus Expert, Nessus Professional, and Nessus Essentials. Each column has a "Try for Free" or "Buy Now" button, a description of the product, and a "Register Now" button.

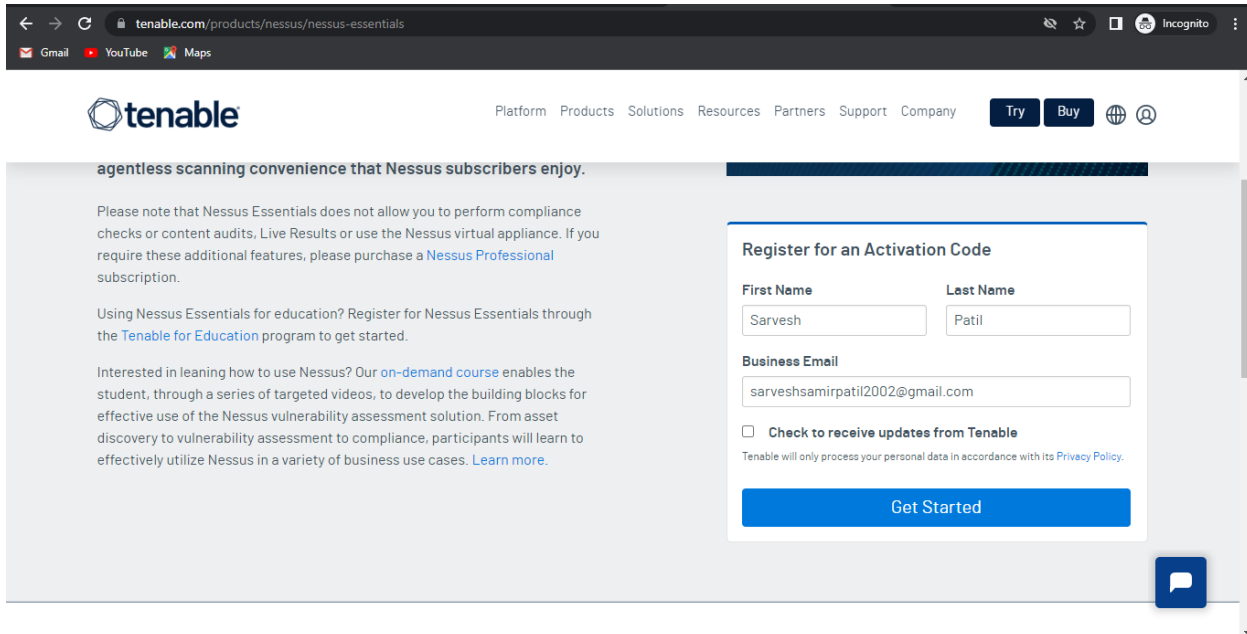
Nessus Expert	Nessus Professional	Nessus Essentials
Try for Free Buy Now	Try for Free Buy Now	Register Now
Nessus Expert is for security pros who need more assessment capabilities that go beyond traditional IT assets. Security pros can secure cloud infrastructure and gain visibility into the internet-connected attack surface.	Nessus Professional is for security pros on the front lines who need to quickly and easily identify and fix vulnerabilities - including software flaws, missing patches, malware, and misconfigurations - across a variety of operating systems, devices and applications.	Nessus Essentials is a free vulnerability scanner that provides an entry point for vulnerability assessment. You get the same powerful scanner enjoyed by Nessus Professional subscribers, with the ability to scan 16 IPs.
For Consultants, Pen Testers, Developers and Security Practitioners	For Consultants, Pen Testers and Security Practitioners	For Educators, students and individuals starting their careers in Cyber Security

Head to the Nessus Home landing page, enter a name and email address, and then click the Register button. You'll want to use a real email address here because Nessus sends you an activation code that you'll need in a step later.

NAME: Sarvesh Patil

CLASS: D15A

ROLL NO: 52



The screenshot shows the Tenable website's registration page for Nessus Essentials. The browser's address bar displays 'tenable.com/products/nessus/nessus-essentials'. The page features the Tenable logo and a navigation menu with links to Platform, Products, Solutions, Resources, Partners, Support, and Company. There are 'Try' and 'Buy' buttons. The main content area includes a heading 'agentless scanning convenience that Nessus subscribers enjoy.' followed by two paragraphs of text. The first paragraph states that Nessus Essentials does not allow compliance checks or content audits, and users must purchase a Nessus Professional subscription for these features. The second paragraph mentions an 'on-demand course' for students and a 'Tenable for Education' program. A registration form titled 'Register for an Activation Code' is on the right, with fields for First Name (Sarvesh), Last Name (Patil), and Business Email (sarveshsamirpatil2002@gmail.com). There is a checkbox for 'Check to receive updates from Tenable' and a 'Get Started' button. A chat bubble is visible in the bottom right corner.

agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Essentials does not allow you to perform compliance checks or content audits, Live Results or use the Nessus virtual appliance. If you require these additional features, please purchase a [Nessus Professional](#) subscription.

Using Nessus Essentials for education? Register for Nessus Essentials through the [Tenable for Education](#) program to get started.

Interested in learning how to use Nessus? Our [on-demand course](#) enables the student, through a series of targeted videos, to develop the building blocks for effective use of the Nessus vulnerability assessment solution. From asset discovery to vulnerability assessment to compliance, participants will learn to effectively utilize Nessus in a variety of business use cases. [Learn more.](#)

Register for an Activation Code

First Name
Sarvesh

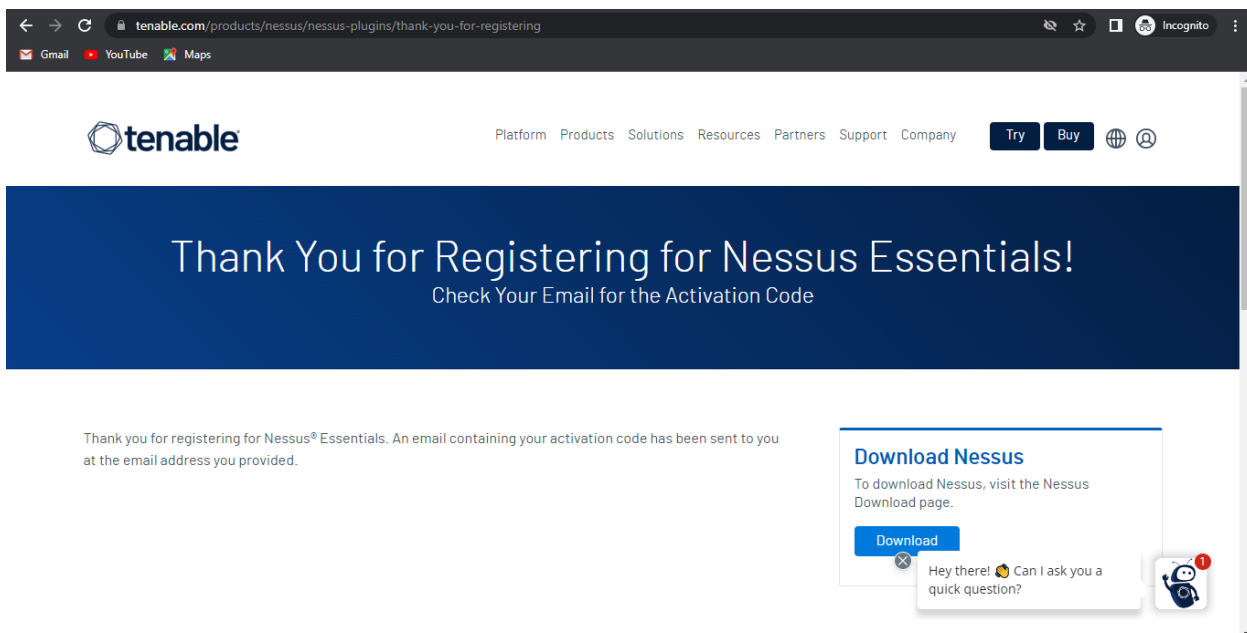
Last Name
Patil

Business Email
sarveshsamirpatil2002@gmail.com

☐ **Check to receive updates from Tenable**
Tenable will only process your personal data in accordance with its [Privacy Policy](#).

Get Started

Click the Download button, then download Nessus for your operating system. It's available for Windows, Mac, and Linux.



The screenshot shows the Tenable website's thank-you page for registering for Nessus Essentials. The browser's address bar displays 'tenable.com/products/nessus/nessus-plugins/thank-you-for-registering'. The page features the Tenable logo and a navigation menu with links to Platform, Products, Solutions, Resources, Partners, Support, and Company. There are 'Try' and 'Buy' buttons. The main content area has a large blue banner with the text 'Thank You for Registering for Nessus Essentials! Check Your Email for the Activation Code'. Below the banner, there is a paragraph of text stating that an email containing the activation code has been sent to the user. A 'Download Nessus' button is visible, with a tooltip that says 'To download Nessus, visit the Nessus Download page.' and a 'Download' button. A chat bubble is visible in the bottom right corner.

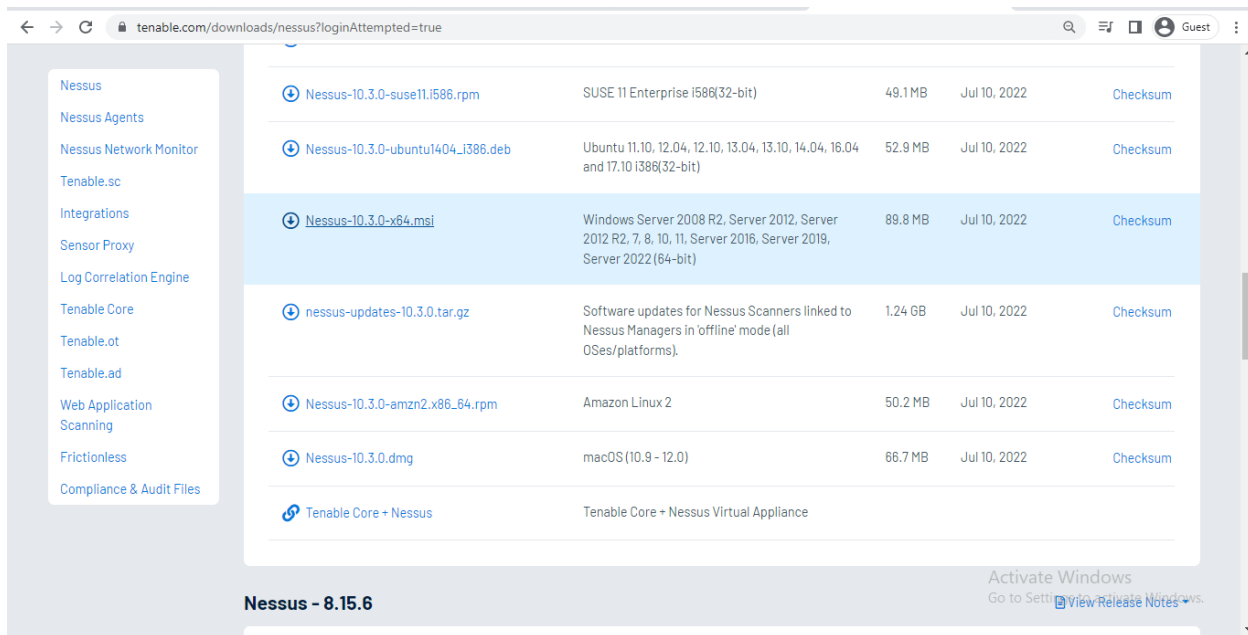
Thank You for Registering for Nessus Essentials!
Check Your Email for the Activation Code

Thank you for registering for Nessus® Essentials. An email containing your activation code has been sent to you at the email address you provided.

Download Nessus
To download Nessus, visit the Nessus Download page.

Download

Hey there! 🤖 Can I ask you a quick question?



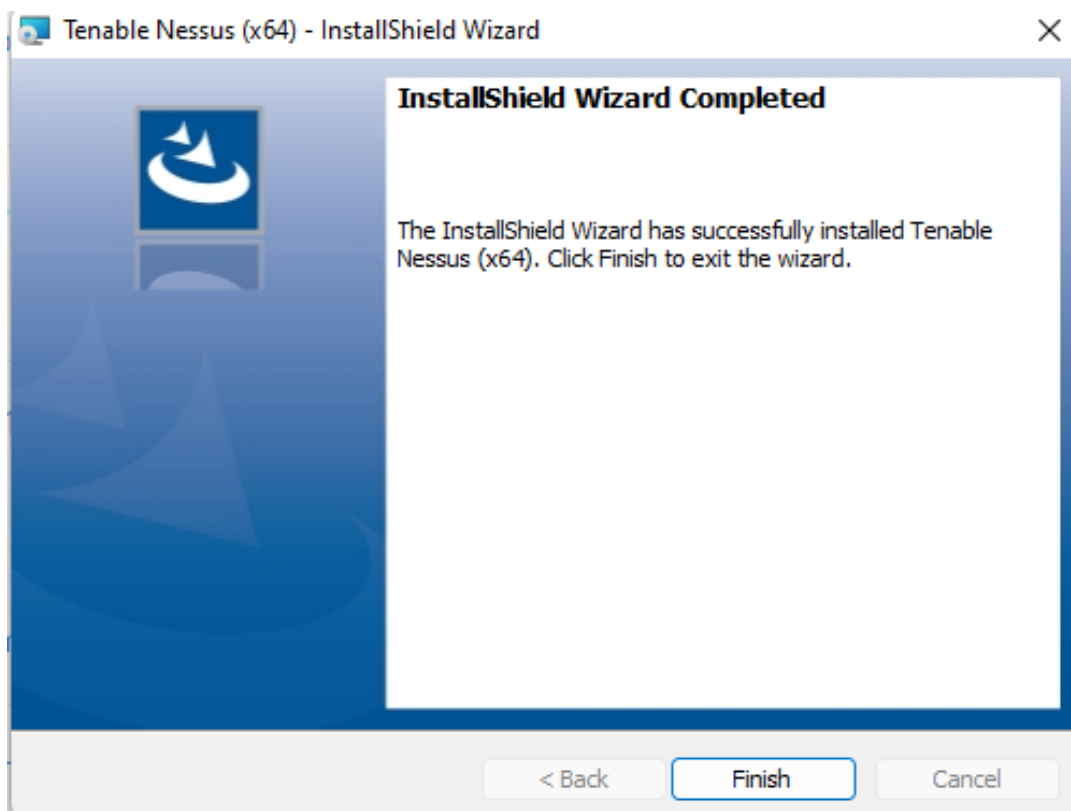
The screenshot shows the Tenable Nessus download page. The left sidebar lists various components: Nessus, Nessus Agents, Nessus Network Monitor, Tenable.sc, Integrations, Sensor Proxy, Log Correlation Engine, Tenable Core, Tenable.ot, Tenable.ad, Web Application Scanning, Frictionless, and Compliance & Audit Files. The main content area displays a table of download links for different operating systems. The table has columns for the download link, the operating system, the file size, the release date, and a checksum link. The operating systems listed are SUSE 11 Enterprise i586(32-bit), Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 16.04 and 17.10 i386(32-bit), Windows Server 2008 R2, Server 2012, Server 2012 R2, 7, 8, 10, 11, Server 2016, Server 2019, Server 2022 (64-bit), Software updates for Nessus Scanners linked to Nessus Managers in 'offline' mode (all OSes/platforms), Amazon Linux 2, macOS (10.9 - 12.0), and Tenable Core + Nessus Virtual Appliance.

Download Link	Operating System	File Size	Release Date	Checksum
Nessus-10.3.0-suse11.i586.rpm	SUSE 11 Enterprise i586(32-bit)	49.1 MB	Jul 10, 2022	Checksum
Nessus-10.3.0-ubuntu1404_i386.deb	Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 16.04 and 17.10 i386(32-bit)	52.9 MB	Jul 10, 2022	Checksum
Nessus-10.3.0-x64.msi	Windows Server 2008 R2, Server 2012, Server 2012 R2, 7, 8, 10, 11, Server 2016, Server 2019, Server 2022 (64-bit)	89.8 MB	Jul 10, 2022	Checksum
nessus-updates-10.3.0.tar.gz	Software updates for Nessus Scanners linked to Nessus Managers in 'offline' mode (all OSes/platforms).	1.24 GB	Jul 10, 2022	Checksum
Nessus-10.3.0-amzn2.x86_64.rpm	Amazon Linux 2	50.2 MB	Jul 10, 2022	Checksum
Nessus-10.3.0.dmg	macOS (10.9 - 12.0)	66.7 MB	Jul 10, 2022	Checksum
Tenable Core + Nessus	Tenable Core + Nessus Virtual Appliance			

Nessus - 8.15.6

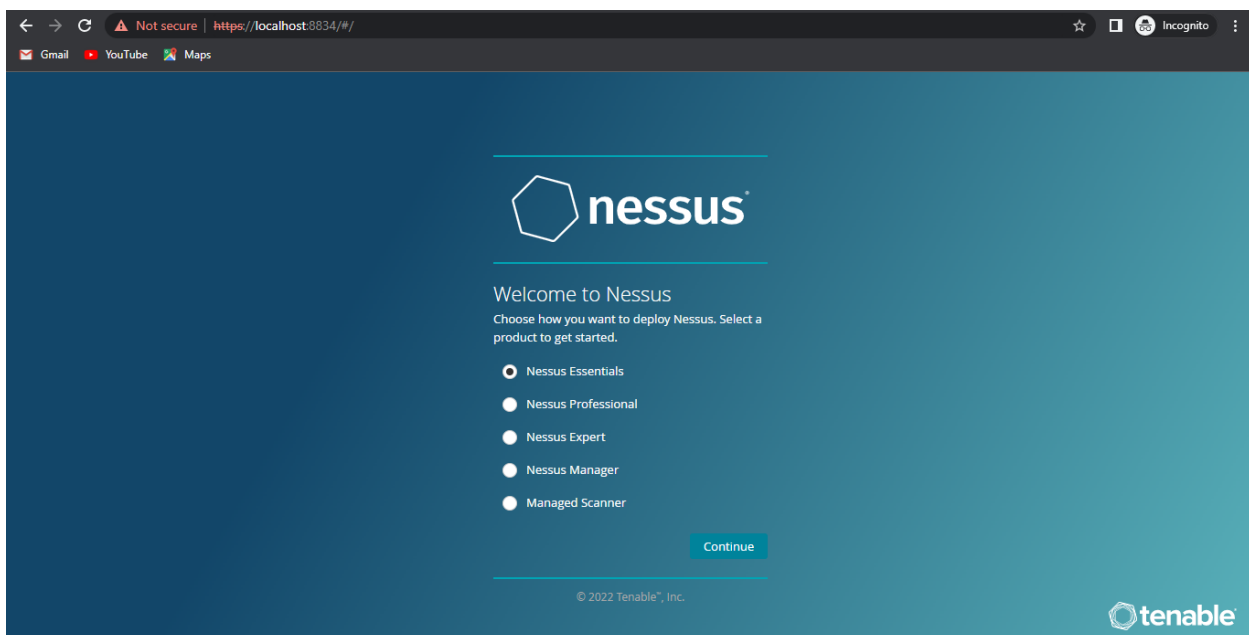
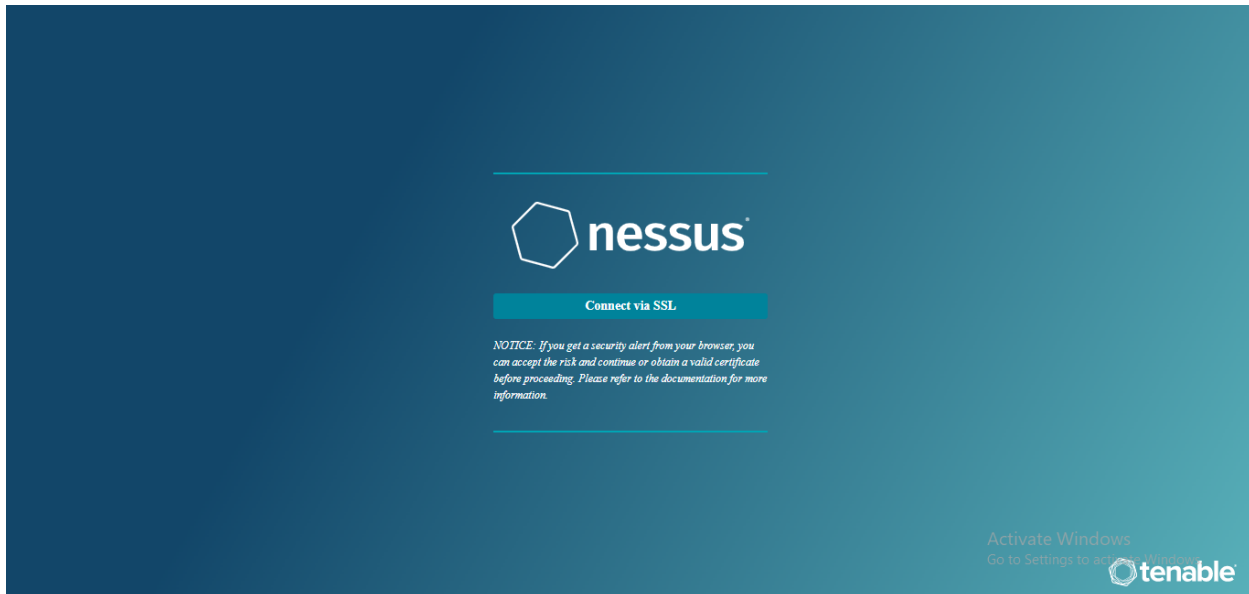
Activate Windows
Go to Settings to activate Windows.
[View Release Notes](#)

Once the download is complete, run the installer package and follow the on-screen instructions to finish the installation.



2. Set Up Your Nessus Account and Activation Code:

Once Nessus is installed, point your web browser to <https://localhost:8834/>. This is where we'll complete the signup process and activate your copy of Nessus.



Create an account on the Account Setup screen, leave the Registration as “Home, Professional, or Manager,” and then enter the Activation Code from your email. Click “Continue.”


NAME: Sarvesh Patil

CLASS: D15A

ROLL NO: 52

← → ↻ ⚠ Not secure | https://localhost:8834/#/ ☆ Incognito

Gmail YouTube Maps




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 * Last *


Email *

© 2022 Tenable®, Inc. 

(6) WhatsApp x Inbox (1,121) - 2020.s... x Download Nessus | T... x D15A_15_UPENDRA x Nessus / Setup x Copy of D15A_15_U... x

← → ↻ ⚠ Not secure | https://localhost:8834/#/ ☆ Incognito

Gmail YouTube Maps




Register Nessus

Enter your activation code.

Activation Code *

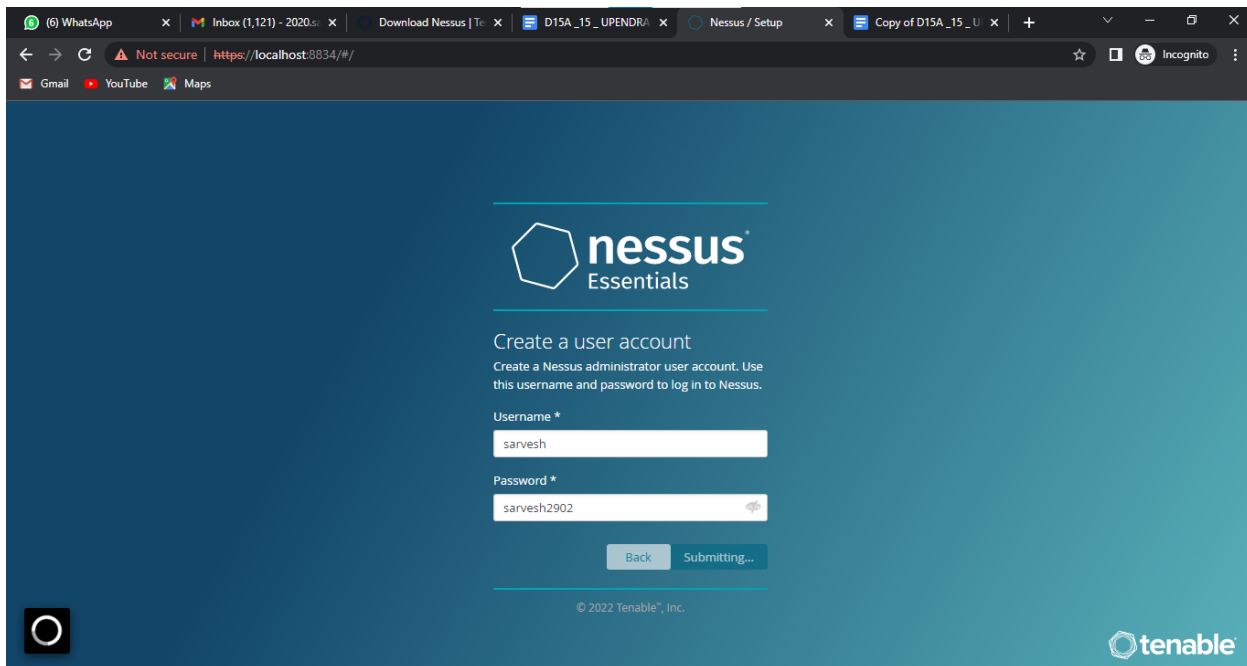
☐ Register Offline

© 2022 Tenable®, Inc. 

NAME: Sarvesh Patil

CLASS: D15A

ROLL NO: 52



The screenshot shows a web browser window with the URL `https://localhost:8834/#/`. The page displays the Nessus Essentials logo and a form to create a user account. The form includes fields for Username and Password, both marked with an asterisk. The Username field contains the text 'sarvesh' and the Password field contains 'sarvesh2902'. Below the fields are 'Back' and 'Submitting...' buttons. The footer of the page includes the copyright notice '© 2022 Tenable, Inc.' and the Tenable logo.

nessus[®]
Essentials

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

Username *

sarvesh

Password *

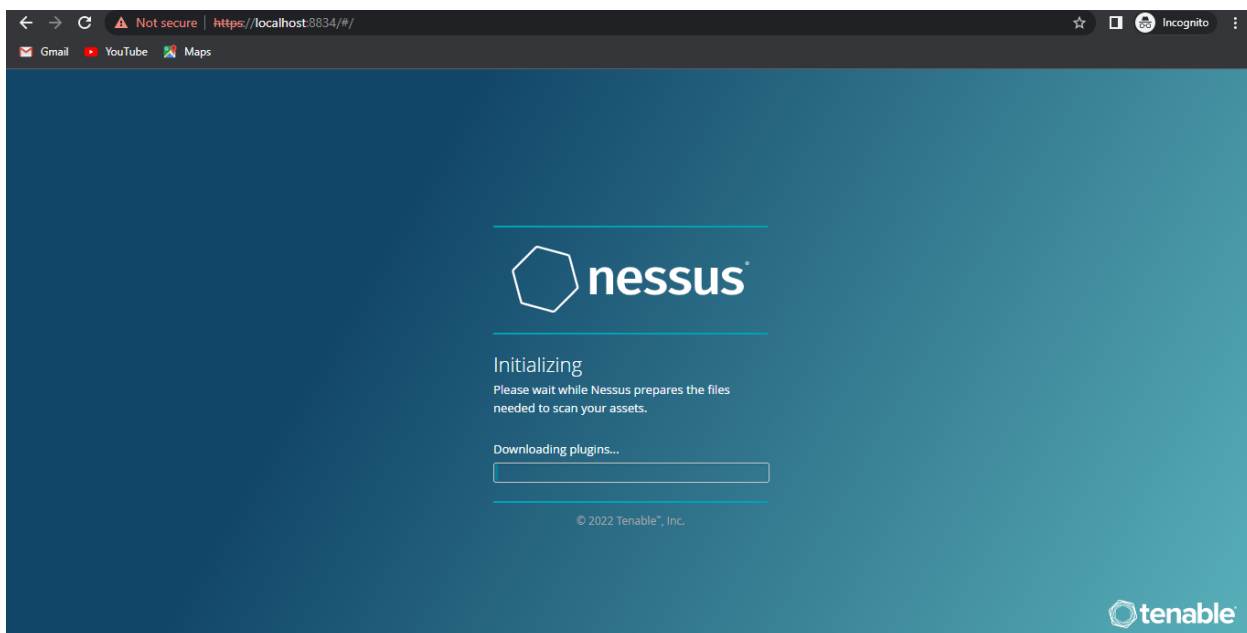
sarvesh2902

Back Submitting...

© 2022 Tenable, Inc.

tenable

Nessus will download a number of tools and plugins so it can properly scan your network with updated utilities.



The screenshot shows the same web browser window, but the page has progressed to the 'Initializing' stage. The Nessus Essentials logo is still present. Below the logo, the text 'Initializing' is displayed, followed by the instruction 'Please wait while Nessus prepares the files needed to scan your assets.' A progress bar labeled 'Downloading plugins...' is shown, which is currently empty. The footer remains the same with the copyright notice and Tenable logo.

nessus[®]

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

Downloading plugins...

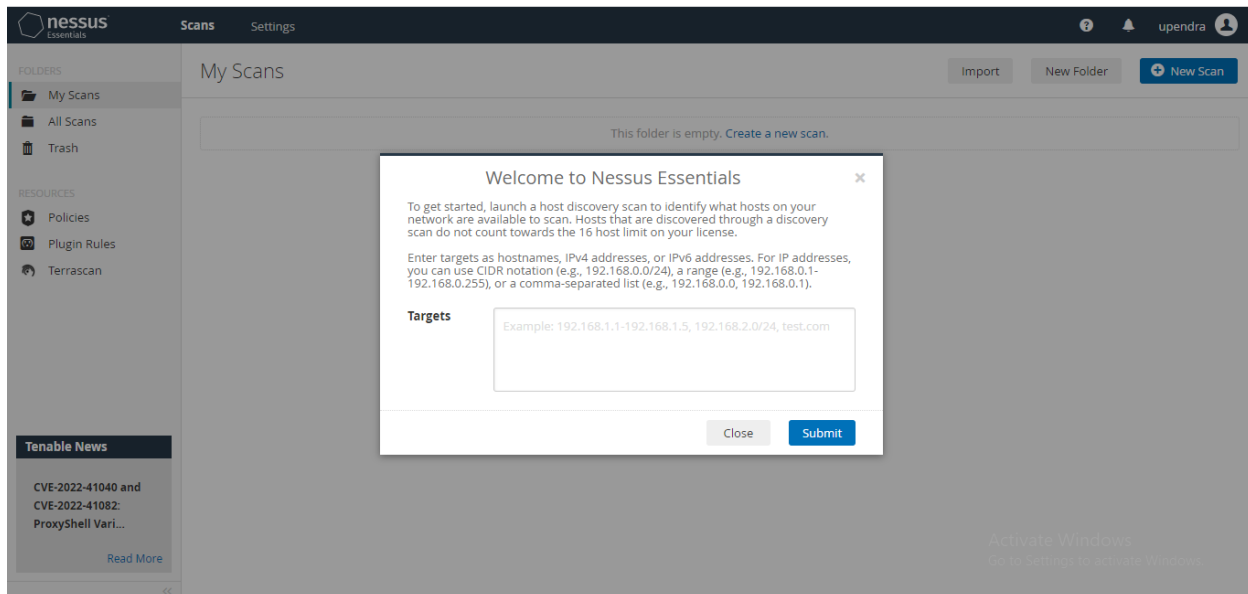
© 2022 Tenable, Inc.

tenable

NAME: Sarvesh Patil

CLASS: D15A

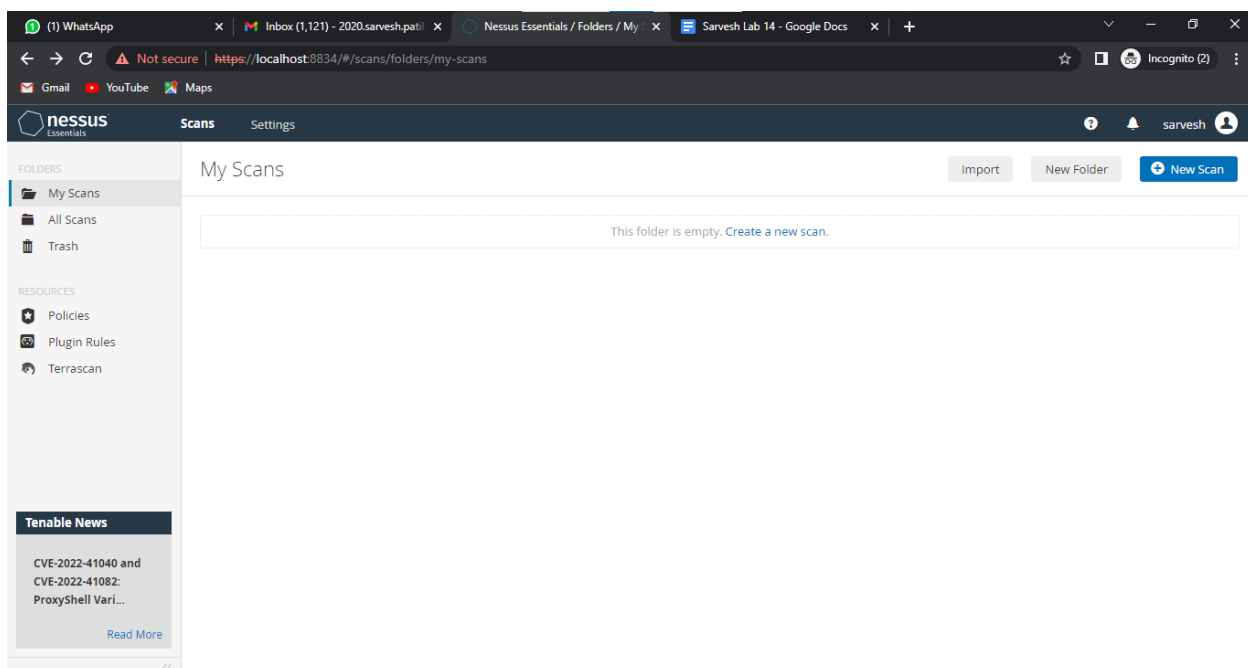
ROLL NO: 52



3. Start a Vulnerability Scan:

Nessus can actually scan for quite a few different problems, but most of us will be content using the Basic Network Scan because it offers a good overview.

Click on “New Scan.”

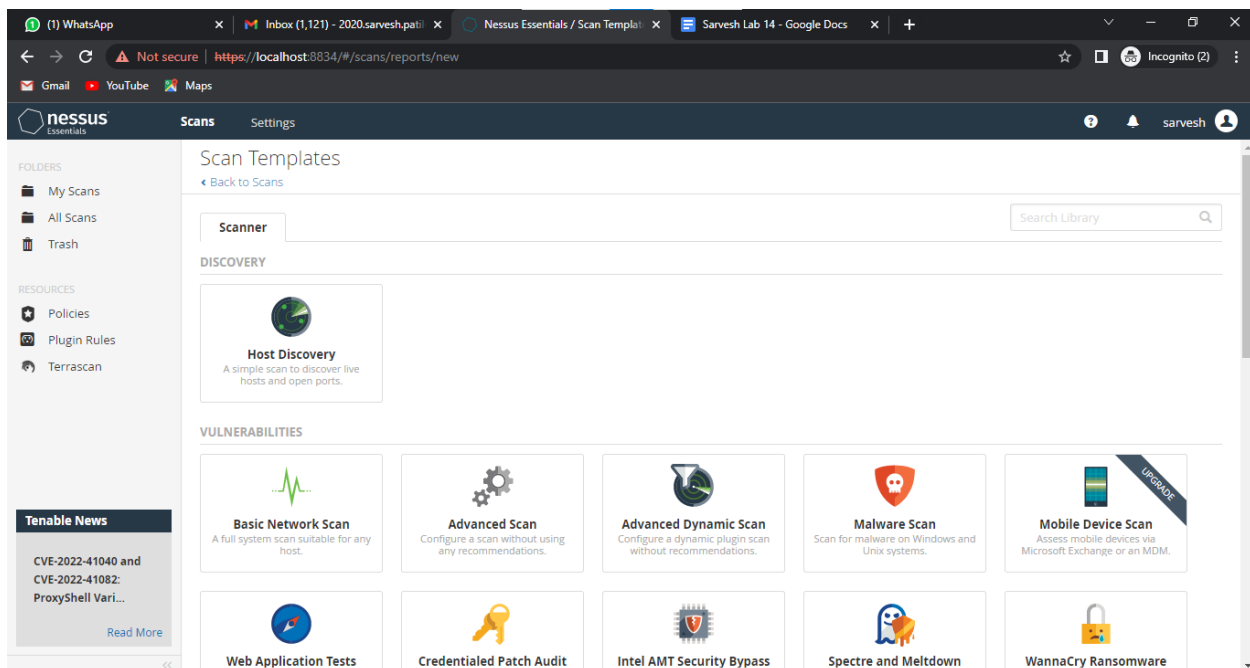


NAME: Sarvesh Patil

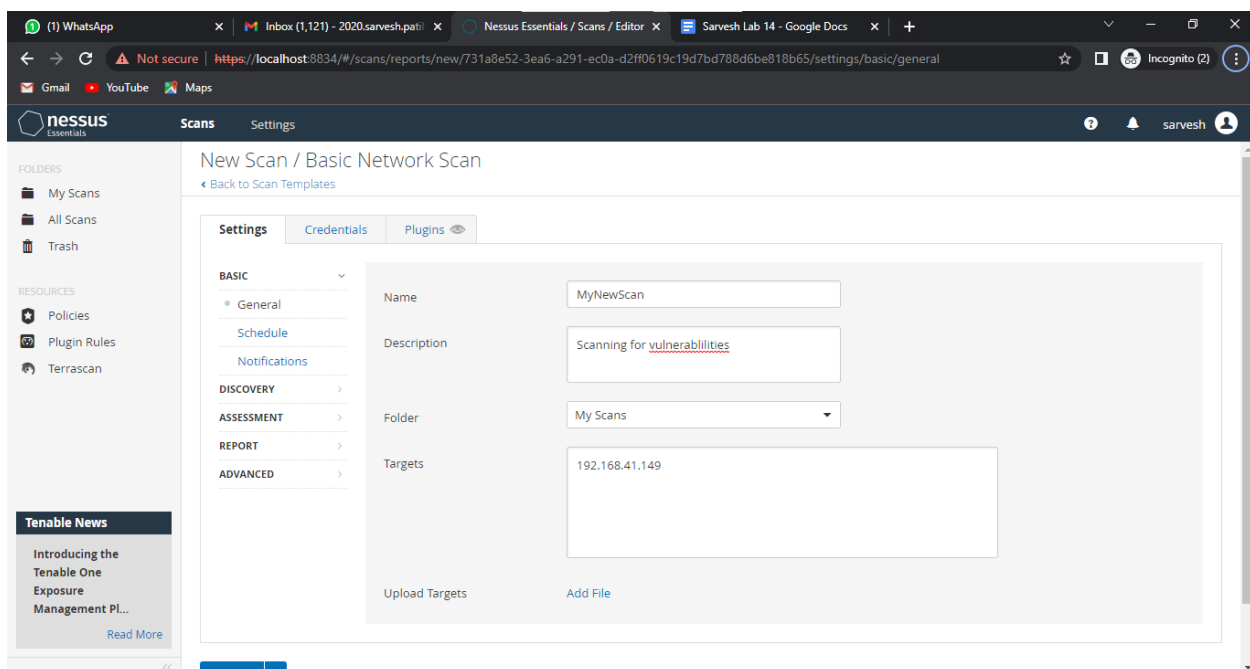
CLASS: D15A

ROLL NO: 52

Click “Basic Network Scan.”



Name your scan and add a description. In the “Targets” field, you’ll want to enter IP scanning details about your home network. For example, I have entered the IP address of my machine 192.168.41.230. This will make it so Nessus scans all the devices on your network.



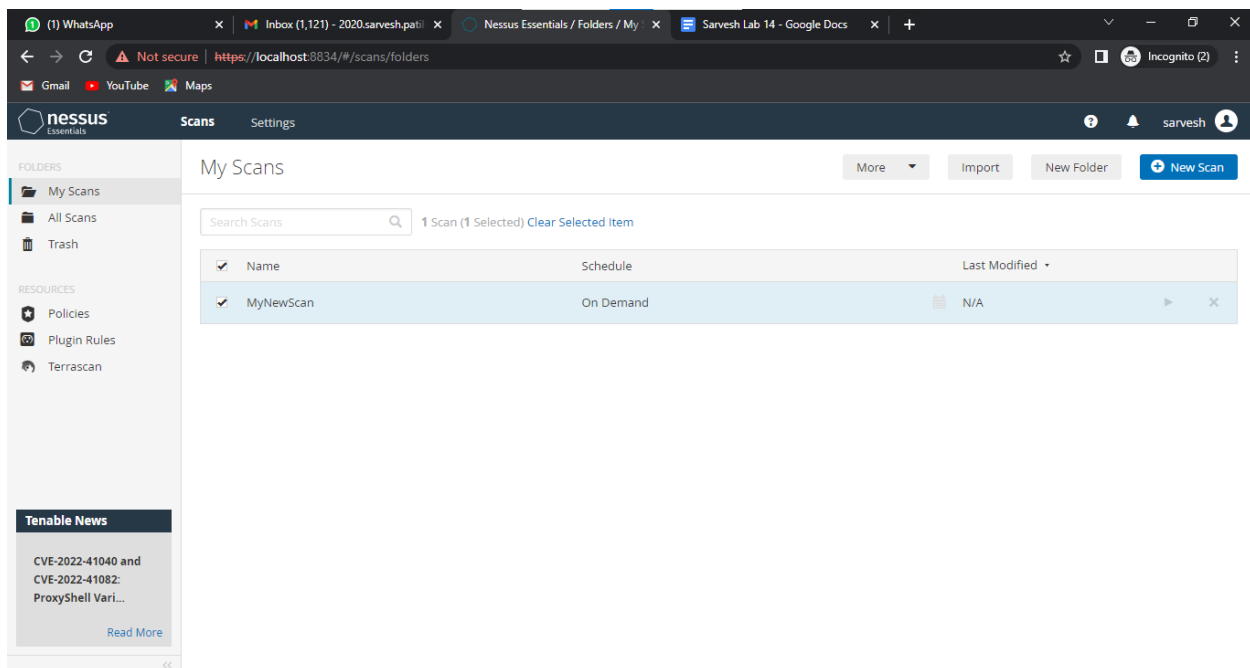
Click “Save.”

NAME: Sarvesh Patil

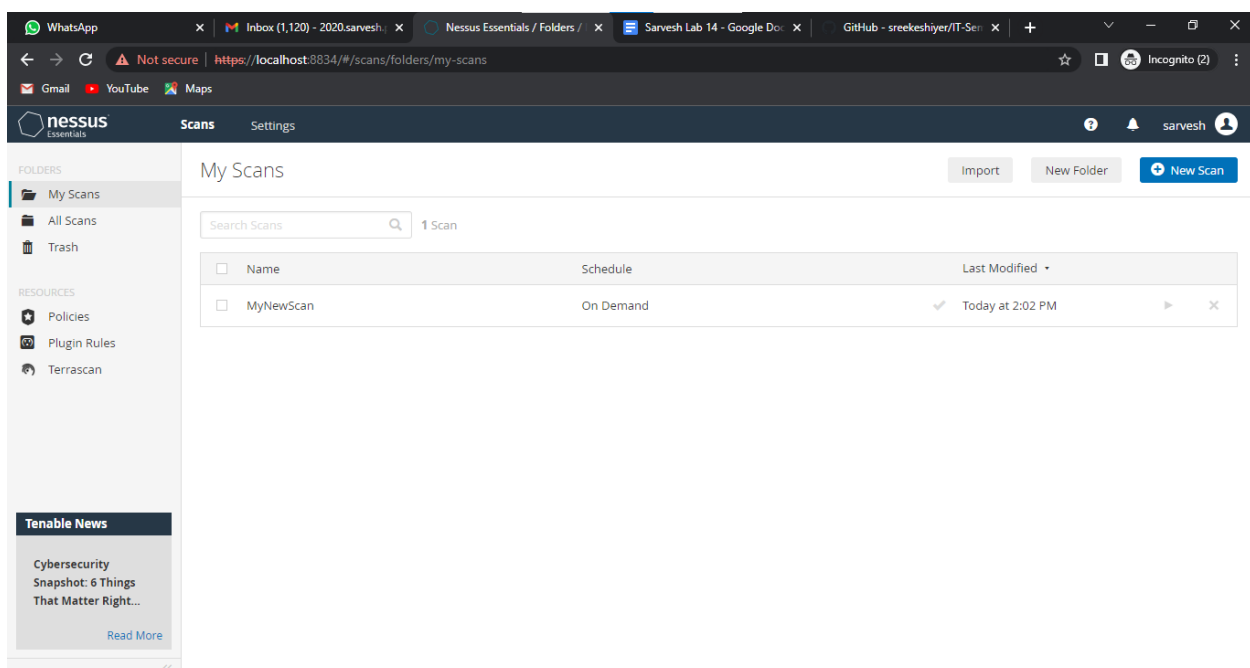
CLASS: D15A

ROLL NO: 52

On the next screen, click the Play icon to launch the scan.



The scanning process may take a few minutes to execute the scan.



The History shows the status of the scan and the time at which the scan was done.

The screenshot shows the Nessus Essentials web interface. The 'History' tab is selected, displaying a table with one scan entry. The scan is named 'MyNewScan' and is in a 'Completed' status. The scan was performed on 'Today at 1:52 PM' and lasted for '10 minutes'. The 'Scan Details' panel on the right shows the policy as 'Basic Network Scan', the scanner as 'Local Scanner', and the severity base as 'CVSS v3.0'. A 'Vulnerabilities' donut chart is also visible, showing a distribution of vulnerability severity levels.

Start Time	Last Modified	Status
Today at 1:52 PM	Today at 2:02 PM	Completed

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 1:52 PM
- End: Today at 2:02 PM
- Elapsed: 10 minutes

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

4. Viewing Your Results:

Once Nessus finishes scanning, you'll see a bunch of color-coded graphs for the. Each color of the graph signifies the danger of a vulnerability, from low to critical.

The screenshot shows the Nessus Essentials web interface with the 'Vulnerabilities' tab selected. It displays a list of 17 vulnerabilities. The table includes columns for Severity (Sev), Score, Name, Family, and Count. The vulnerabilities are color-coded by severity: MIXED (purple), INFO (blue), and CRITICAL (red). The 'Scan Details' panel on the right shows the same scan information as the previous screenshot. The 'Vulnerabilities' donut chart shows a distribution of severity levels.

Sev	Score	Name	Family	Count
MIXED	2	SMB (Multiple Issues)	SMB (Multiple Issues)	2
INFO	6	SMB (Multiple Issues)	Windows	7
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		Inconsistent Hostname a...	Settings	1

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 1:52 PM
- End: Today at 2:02 PM
- Elapsed: 10 minutes

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

We will go through a few of the vulnerabilities to check their information and the threats they would cause to the system.

NAME: Sarvesh Patil

CLASS: D15A

ROLL NO: 52

The screenshot shows the Nessus Essentials web interface. The browser address bar displays the URL: `https://localhost:8834/#/scans/reports/5/vulnerabilities/group/57608/57608`. The interface is titled "MyNewScan / Plugin #57608". The left sidebar contains navigation options: "FOLDERS" (My Scans, All Scans, Trash), "RESOURCES" (Policies, Plugin Rules, Terrascan), and "Tenable News". The main content area shows the details for the vulnerability "SMB Signing not required" (Medium severity). The description states: "Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server." The solution suggests enforcing message signing in the host's configuration. The "Plugin Details" section on the right lists: Severity: Medium, ID: 57608, Version: 1.20, Type: remote, Family: Misc, Published: January 19, 2012, Modified: October 5, 2022. The "Risk Information" section shows a Risk Factor of Medium and a CVSS v3.0 Base Score of 5.3.

The screenshot shows the Nessus Essentials web interface. The browser address bar displays the URL: `https://localhost:8834/#/scans/reports/5/vulnerabilities/group/57608/96982`. The interface is titled "MyNewScan / Plugin #96982". The left sidebar contains navigation options: "FOLDERS" (My Scans, All Scans, Trash), "RESOURCES" (Policies, Plugin Rules, Terrascan), and "Tenable News". The main content area shows the details for the vulnerability "Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated c..." (Info severity). The description states: "The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues." The solution suggests disabling SMBv1 according to the vendor instructions in Microsoft KB2696547. The "Plugin Details" section on the right lists: Severity: Info, ID: 96982, Version: 1.7, Type: remote, Family: Misc, Published: February 3, 2017, Modified: September 22, 2020. The "Risk Information" section shows a Risk Factor of None. The "Vulnerability Information" section shows "In the news: true".

CONCLUSION:

We have successfully used the NESSUS tool to scan the network for vulnerabilities and also studied various vulnerabilities in our PC's IP address.