Experiment 14

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

Roll No.	19
Name	Manav Jawrani
Class	D15-A
Subject	Security Lab
LO Mapped	LO5: 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:

Nessus Introduction:

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 scan these vulnerabilities and exposures:

1. Vulnerabilities that could allow unauthorized control or access to sensitive data on the system.
2. Misconfiguration (e.g. open mail relay)
3. Denials of service (Dos) vulnerabilities
4. Default passwords, a few common passwords, and blank/absent passwords on some system accounts.
5. 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:

1. Unix
2. Linux
3. FreeBSD

Also, the client is available for:

1. Unix-based operating systems
2. Windows-based operating systems

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:

1. Vulnerability Scanning
2. Asset Discovery
3. Network Scanning
4. Vulnerability Assessment
5. Prioritization
6. Policy Management
7. 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.

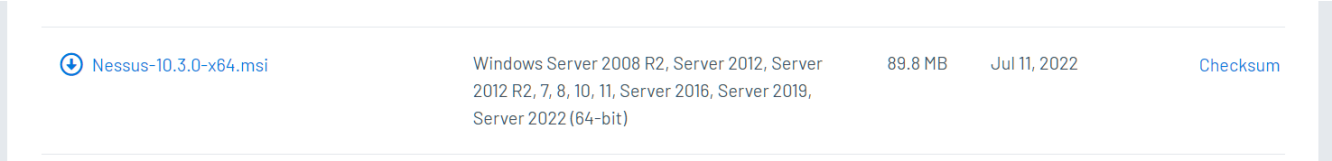
Nessus Agents provide a subset of the coverage in a traditional network scan:
Scanning of transient endpoints that are not always connected to the local network.
Scanning assets for which you do not have credentials or could not easily obtain credentials. Improving overall scan performance: With agents, 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:

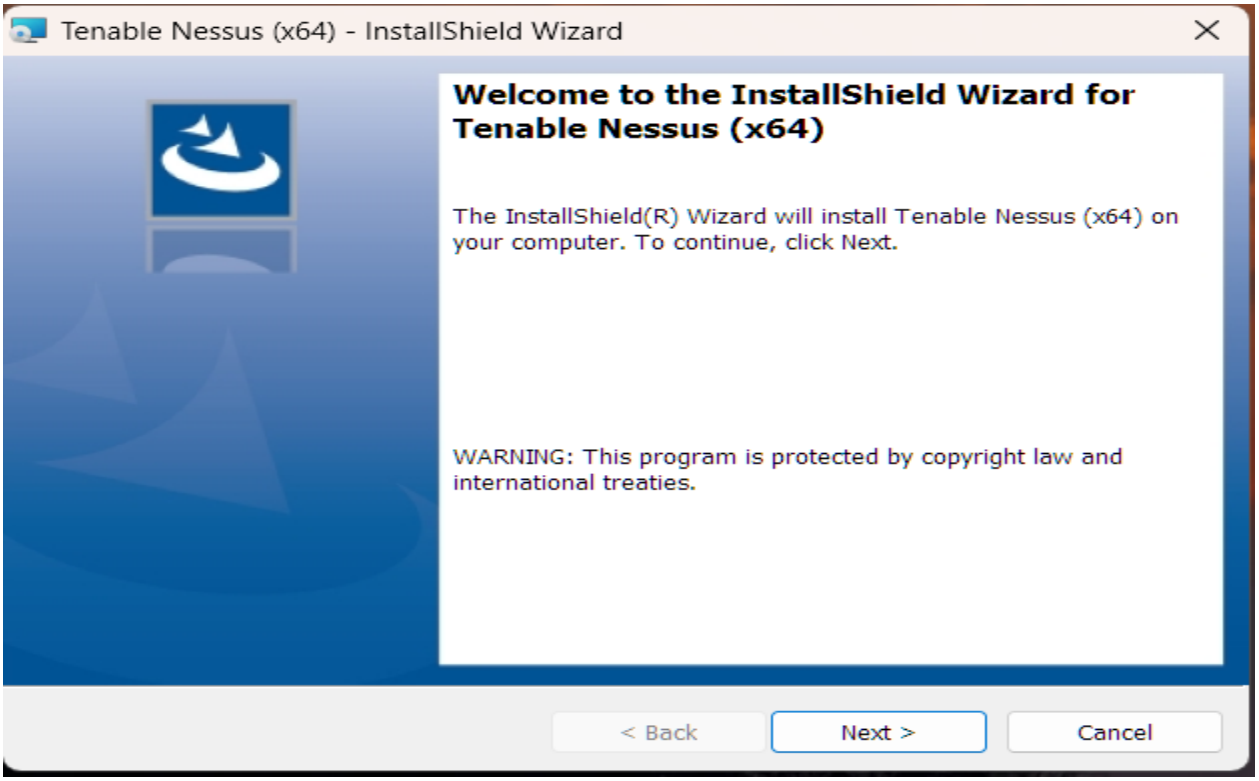
1. Windows Server 2008 and 2012, and Windows 7 and 8
2. Amazon Linux
3. CentOS
4. Debian Linux
5. OS X
6. Red Hat Enterprise Linux
7. Ubuntu Linux

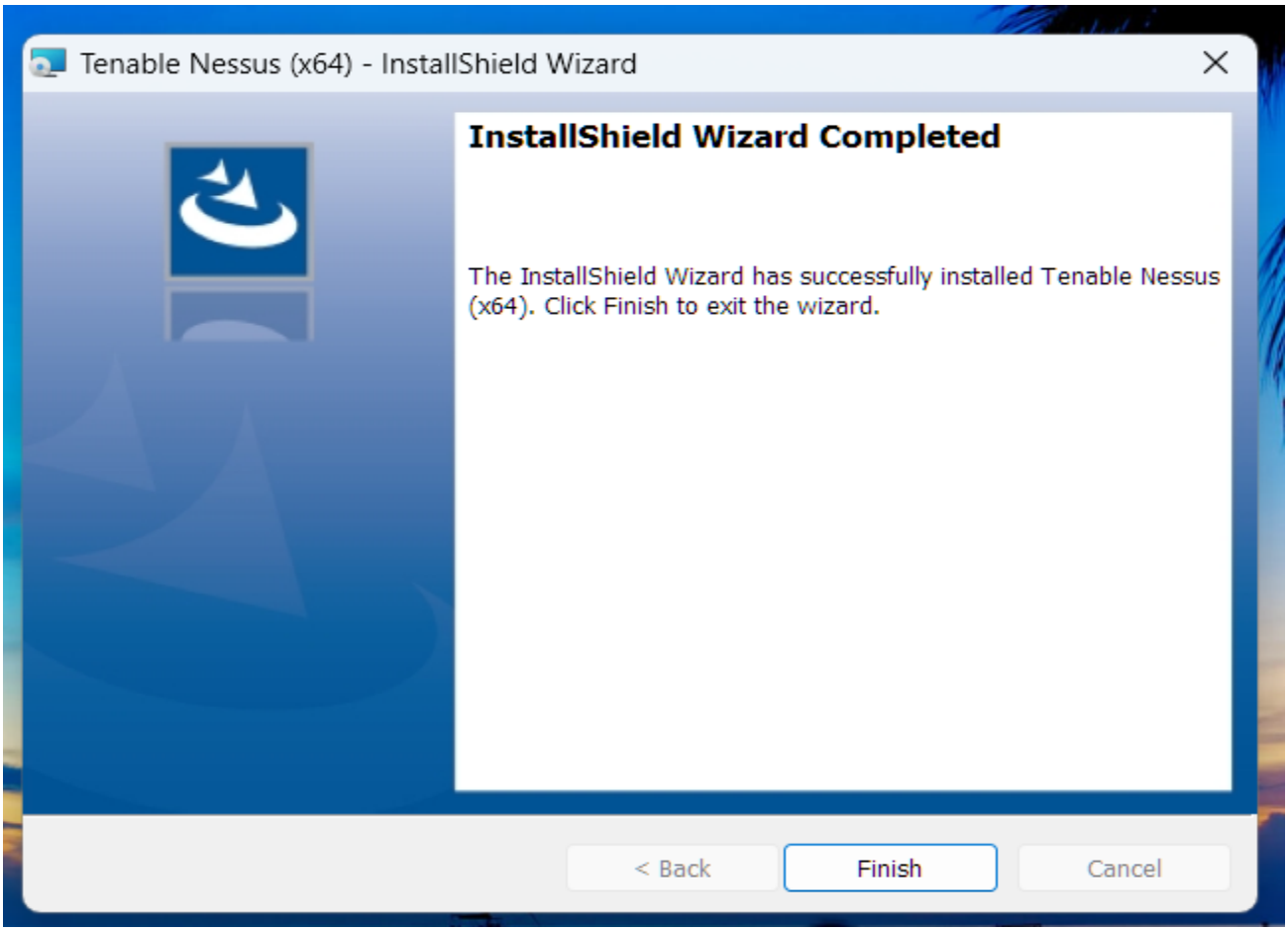
Methods:

Step 1: Go to this website:
https://www.tenable.com/downloads/nessus?loginAttempted=true
and search for the Windows Server 2008 msi installer and Download.

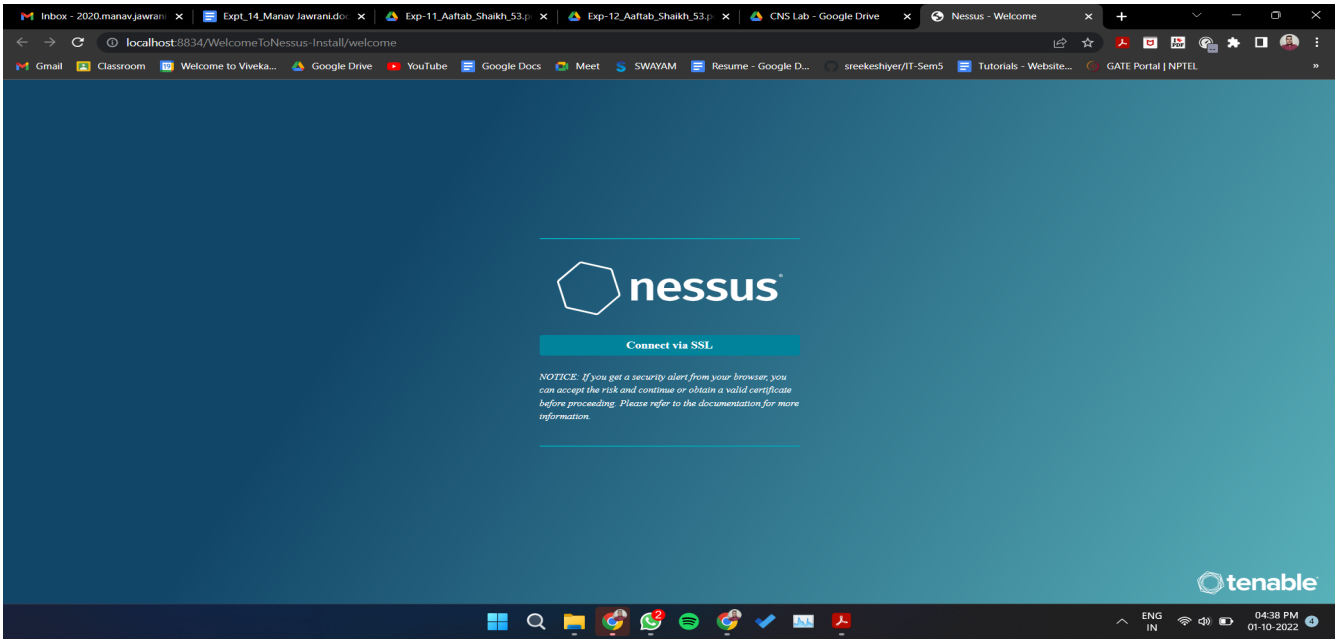


Install Nessus:

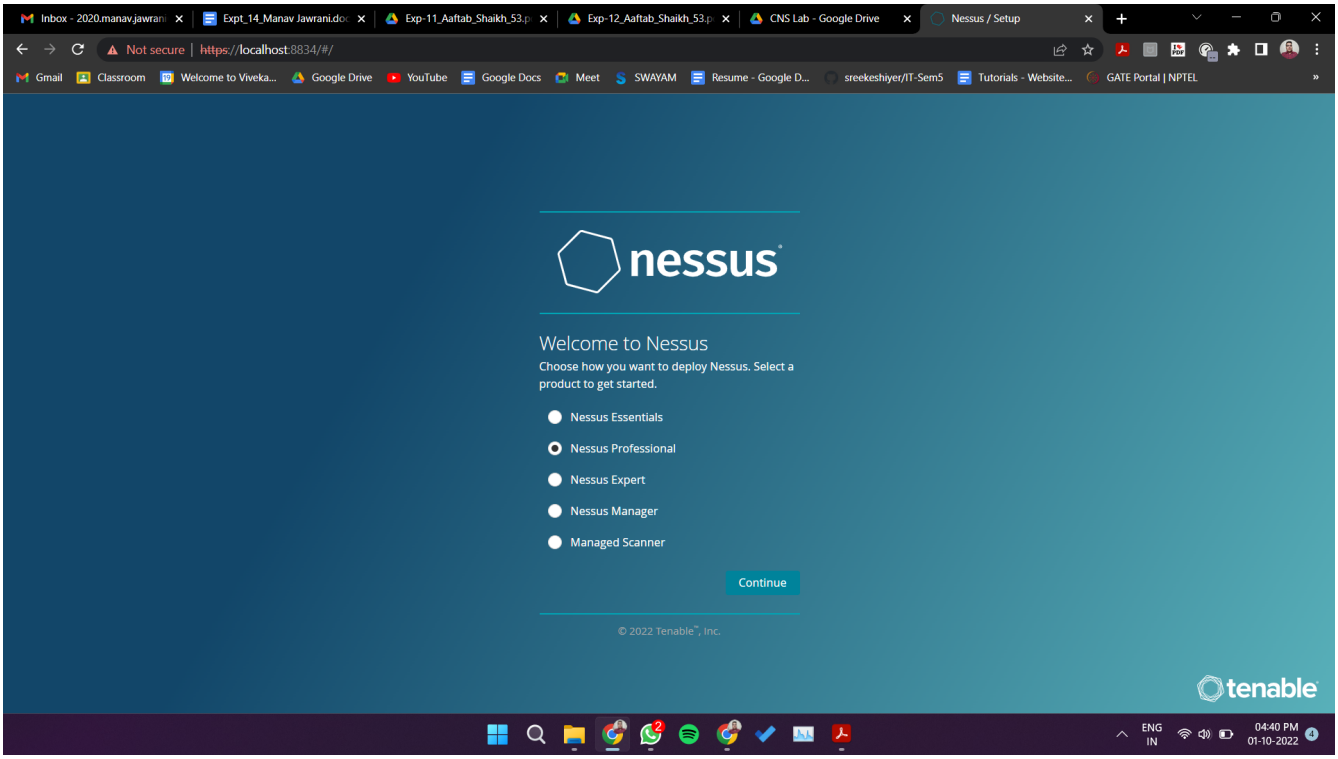




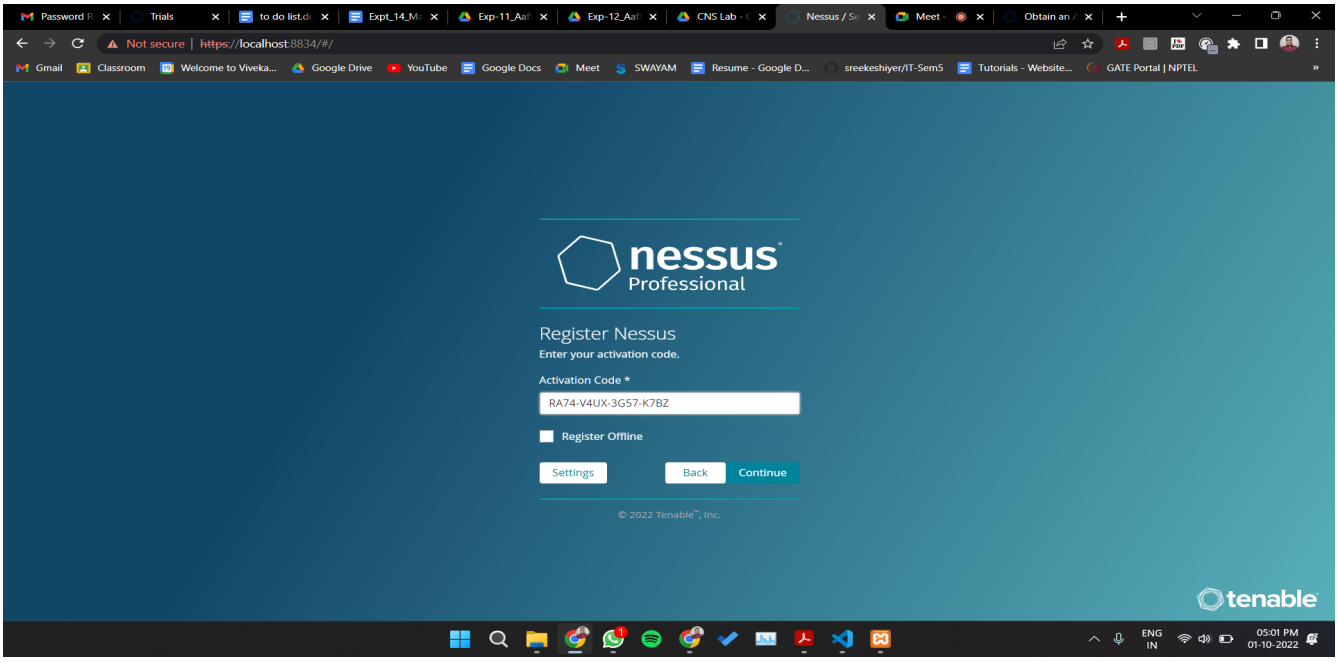
After successfully installing it you will be redirected to this page



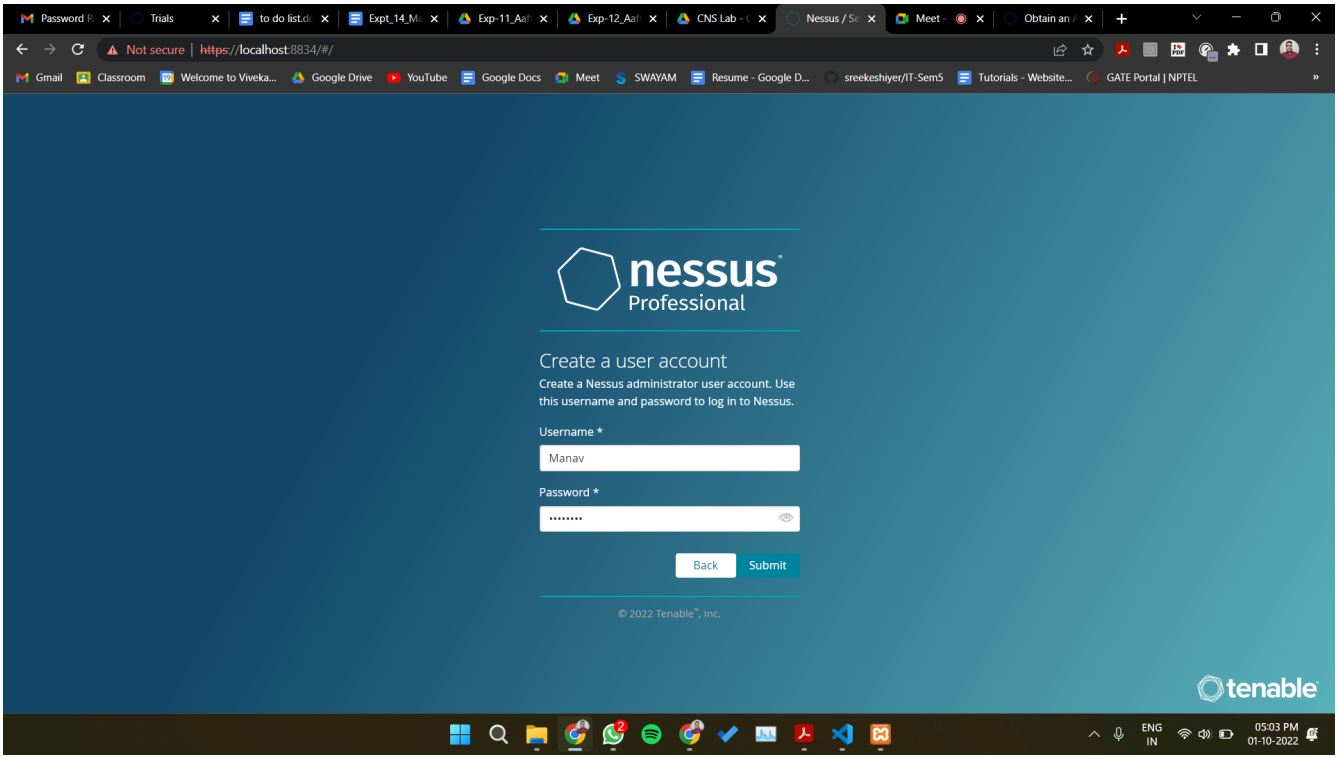
Next it will ask you which version you want to install



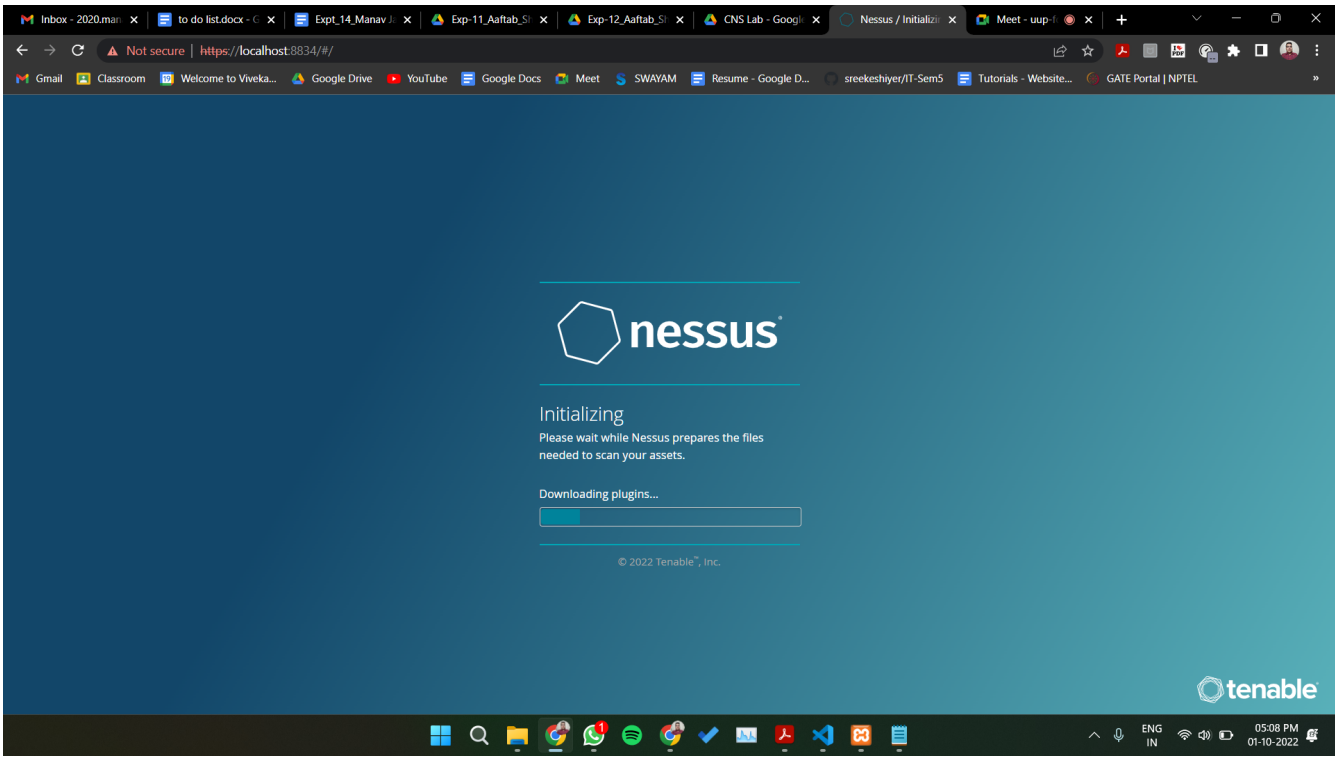
Now go to this website https://www.tenable.com/products/nessus/activation-code and get an activation code which will be used further.
Copy the activation code and paste it here



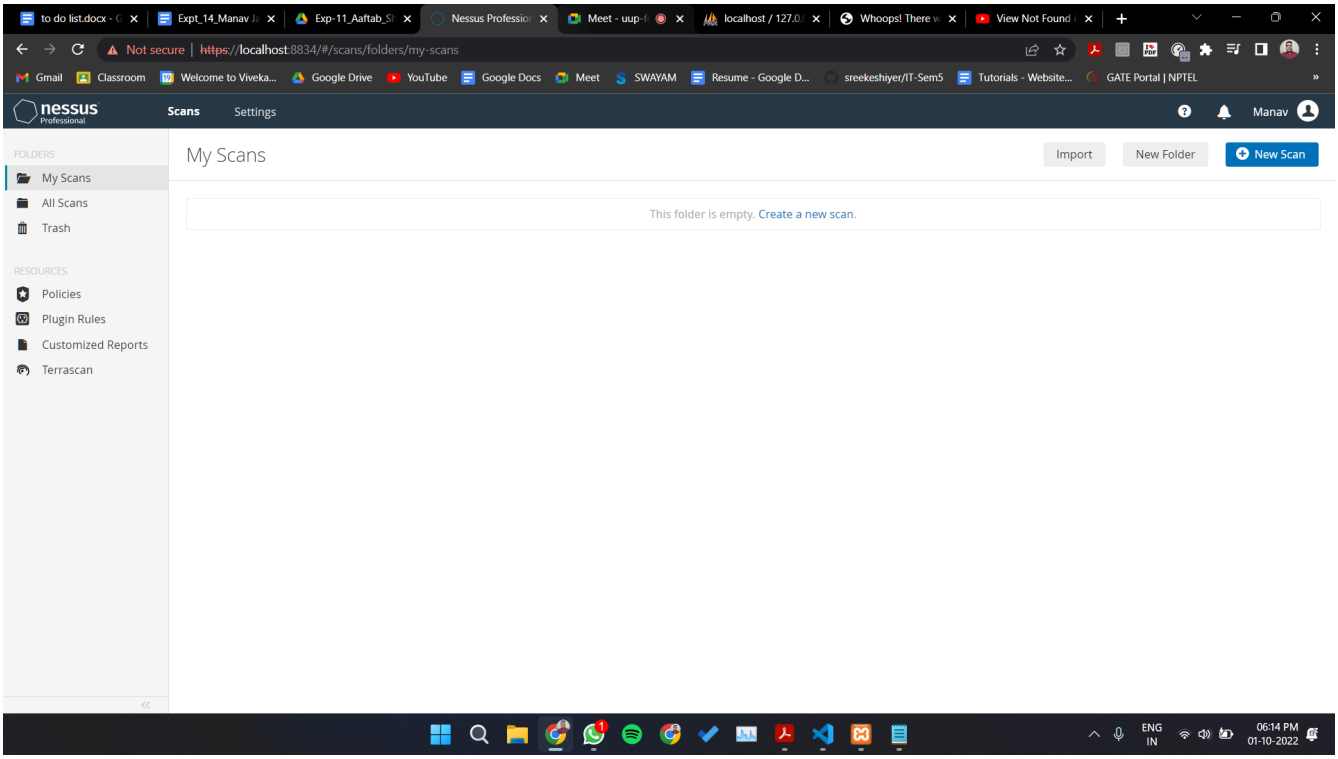
Create the username and password



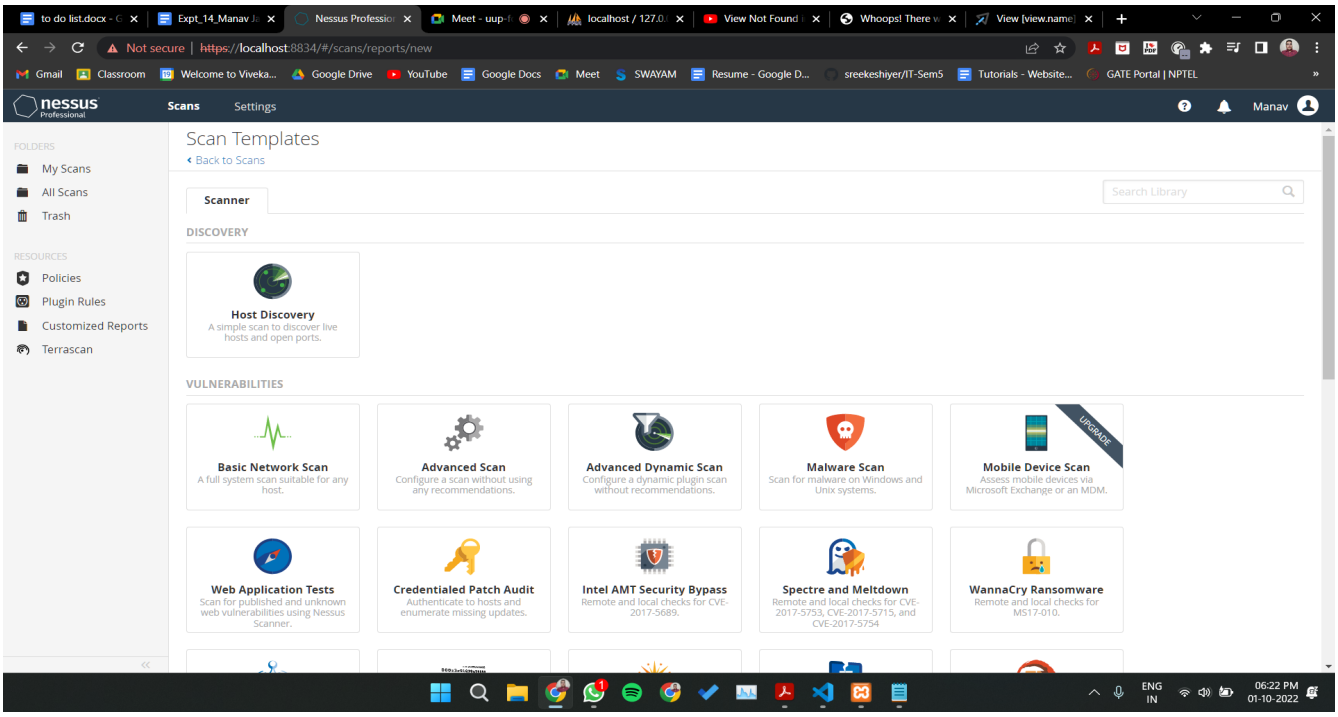
It will download some plugins



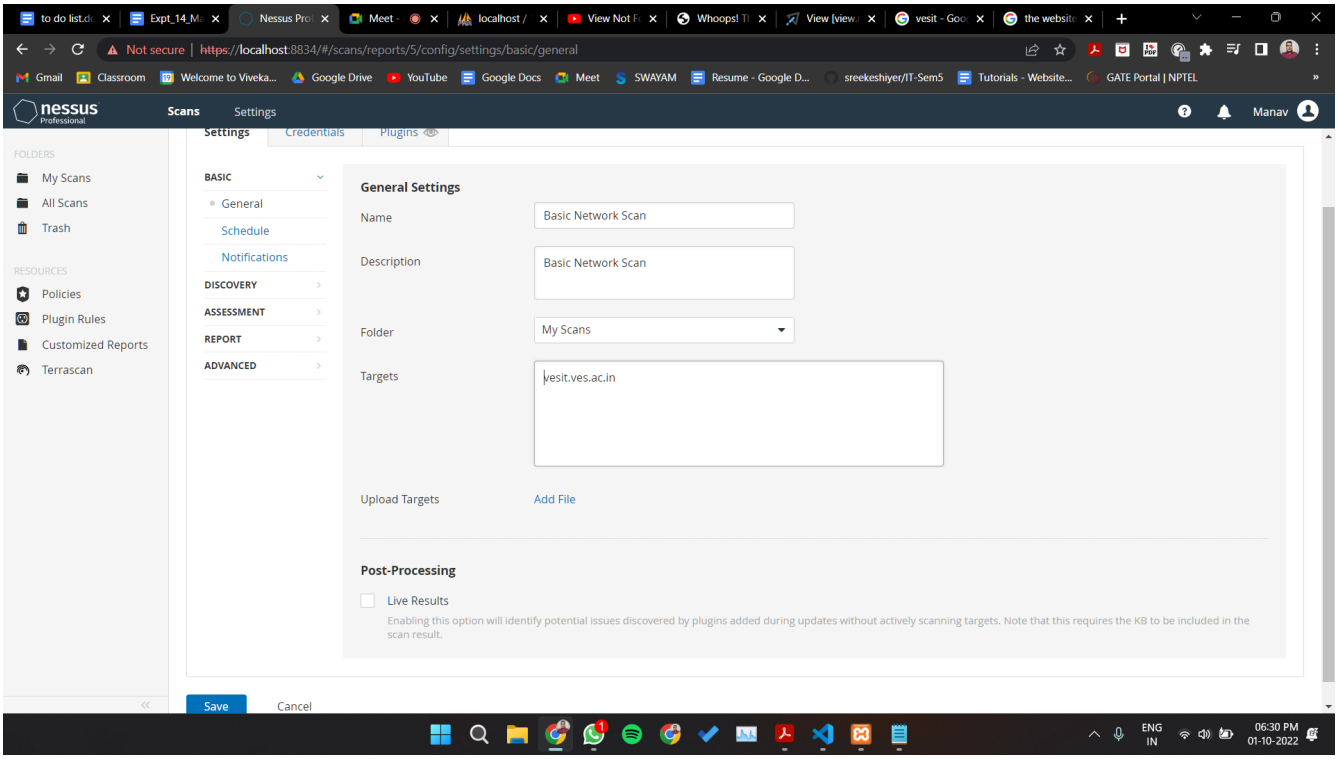
This will be the Home Page where you will be redirected after installation



Now we will perform a **Basic Network Scan**

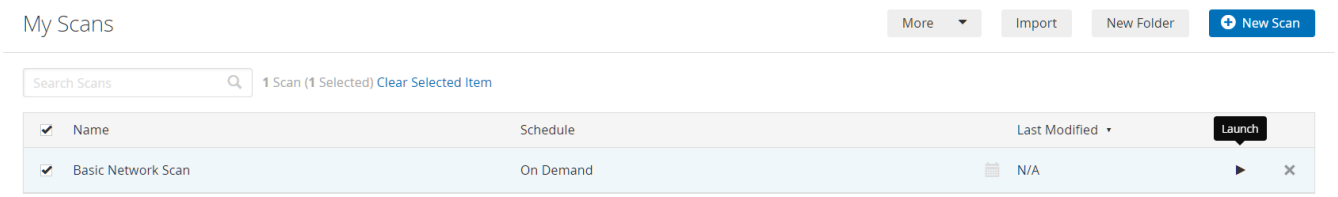


Enter the details

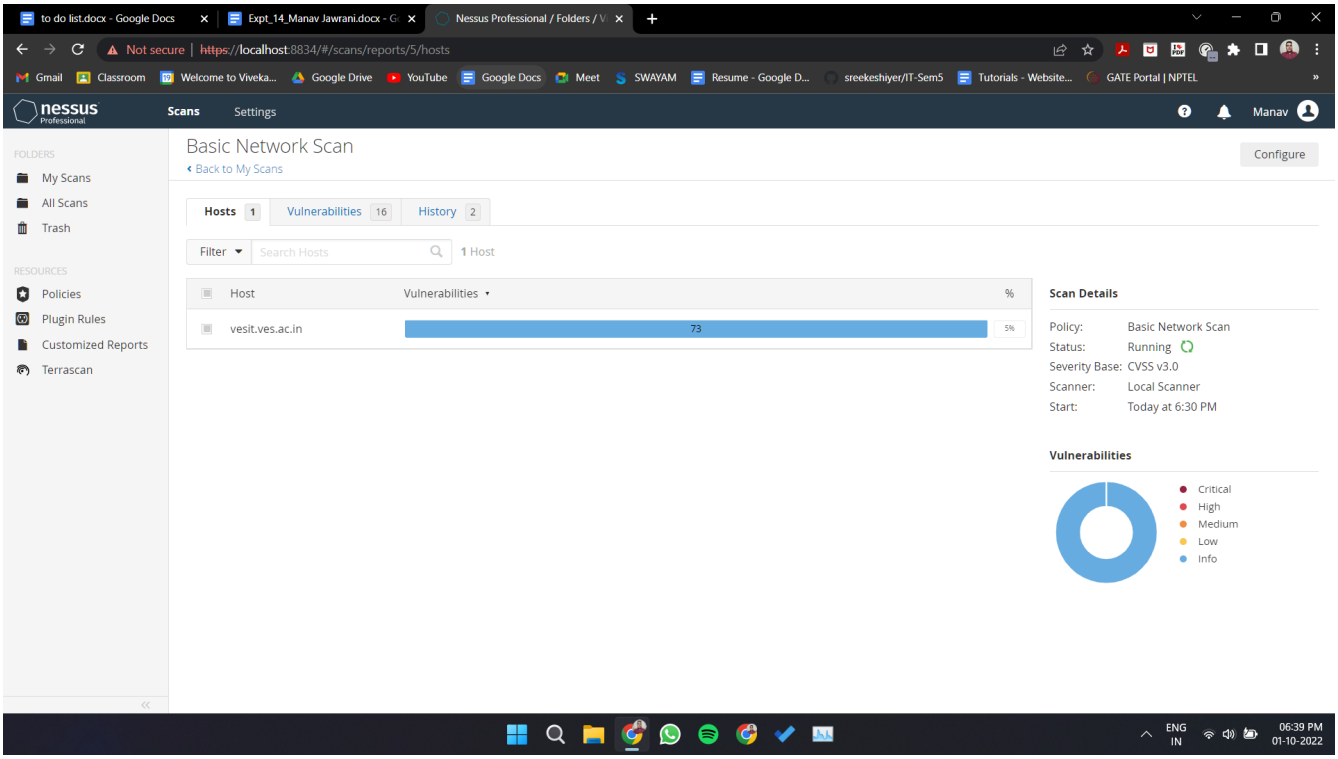


Our targeted website for scan in www.vesit.ves.ac.in

Now **Launch** the scan

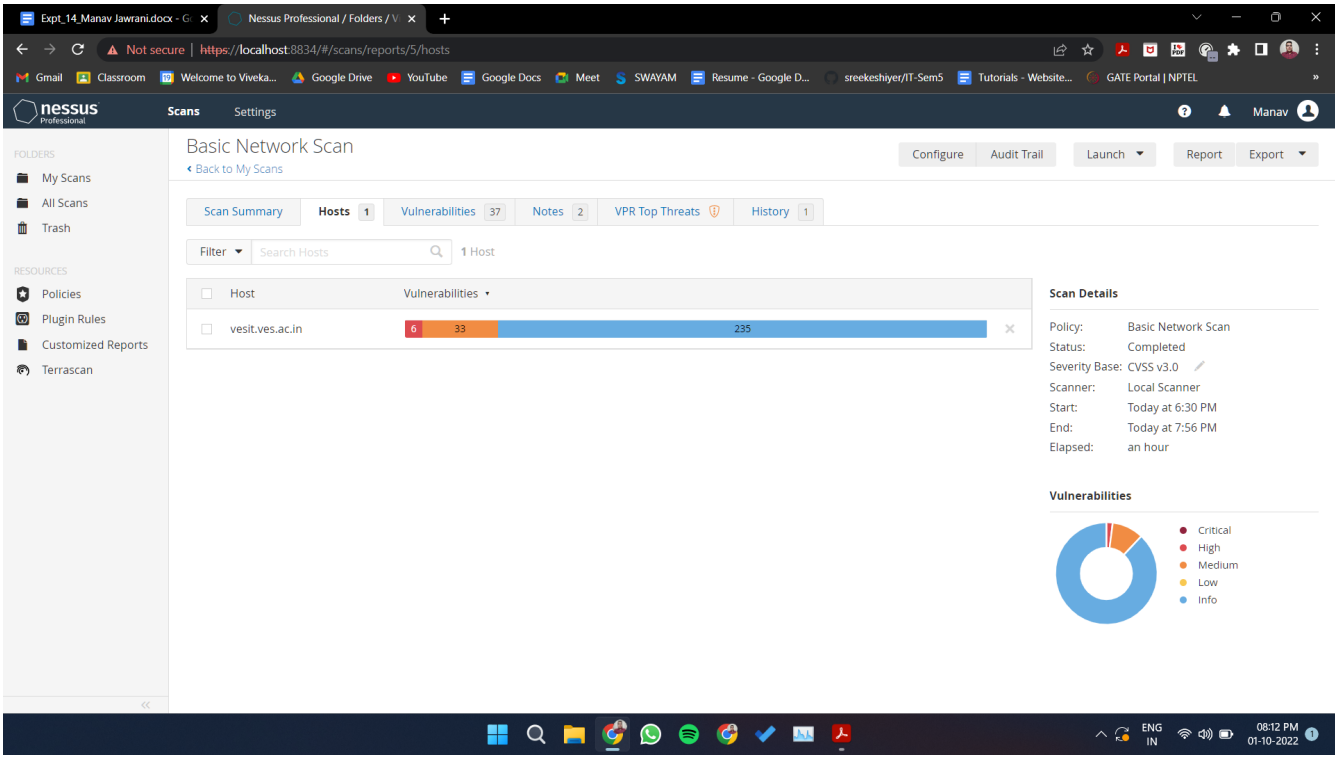


Scan is running

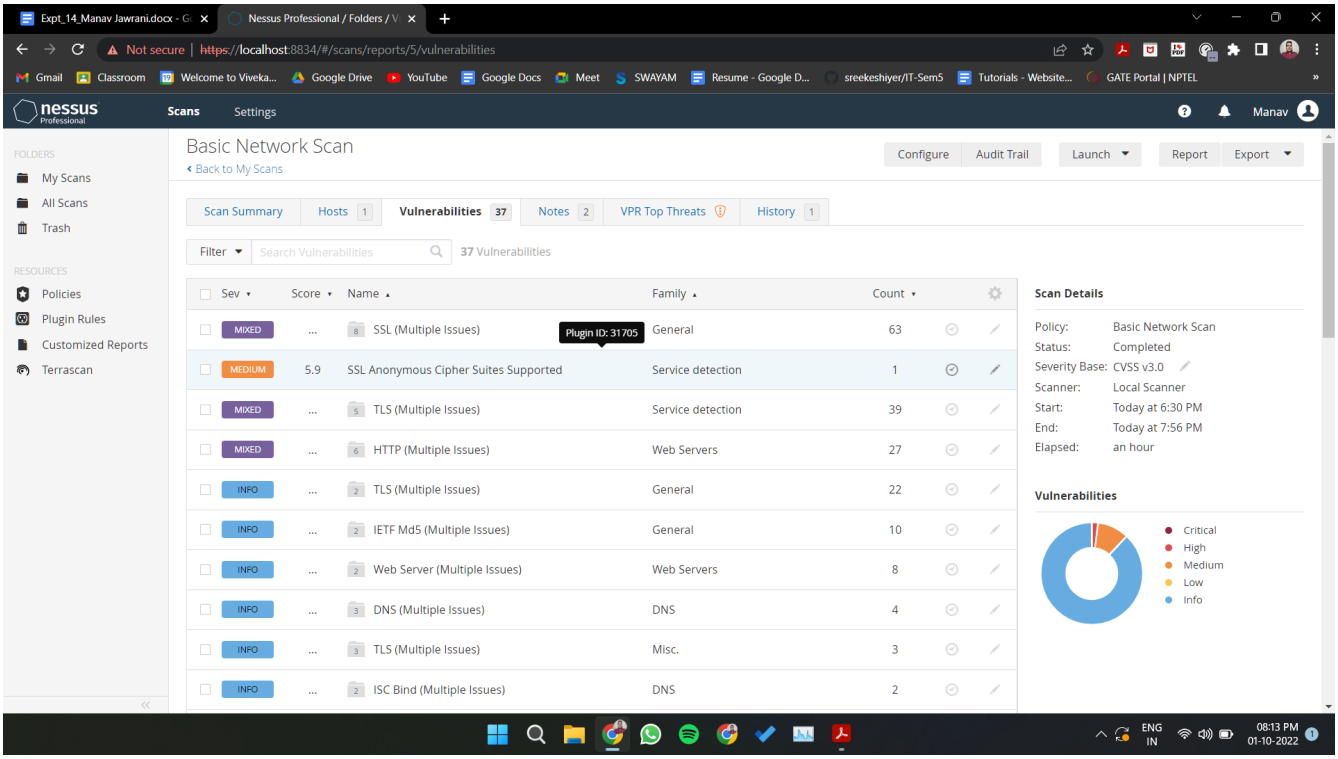


Results

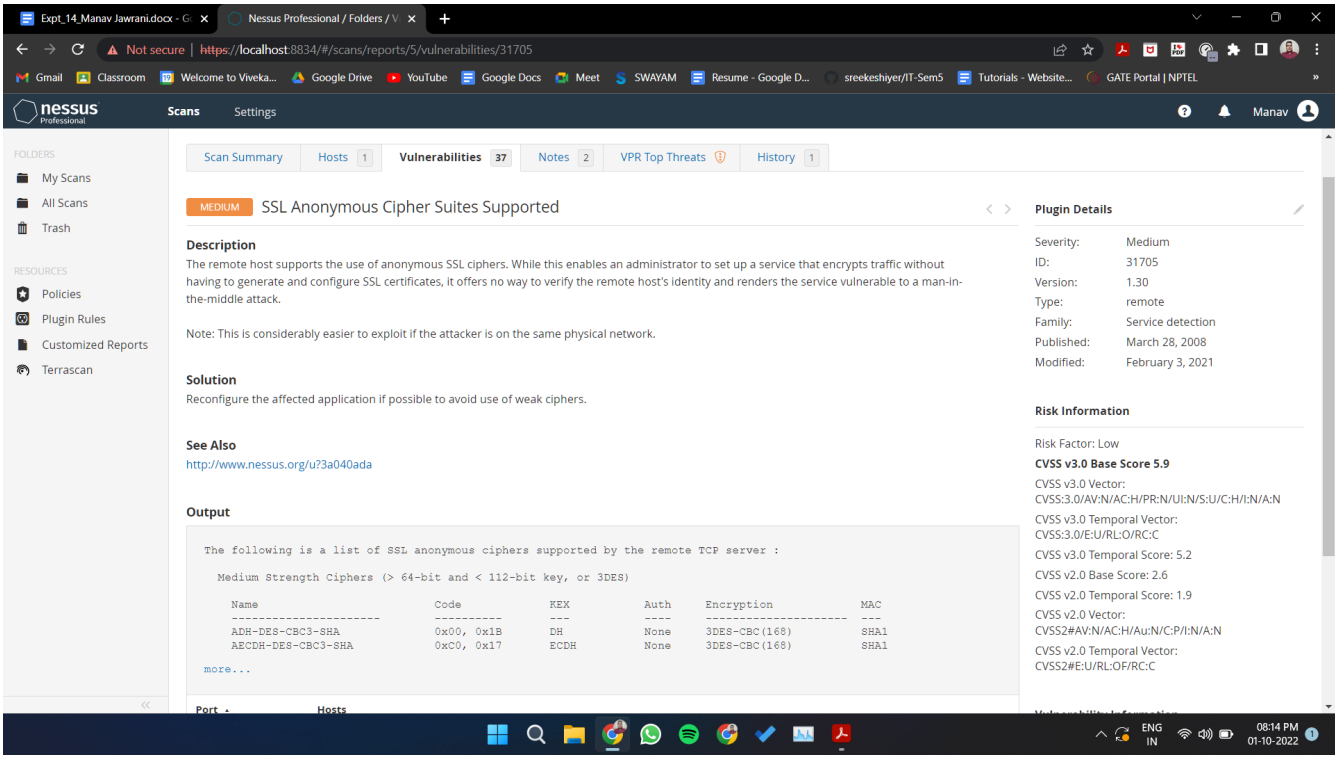
After scanning these are the results



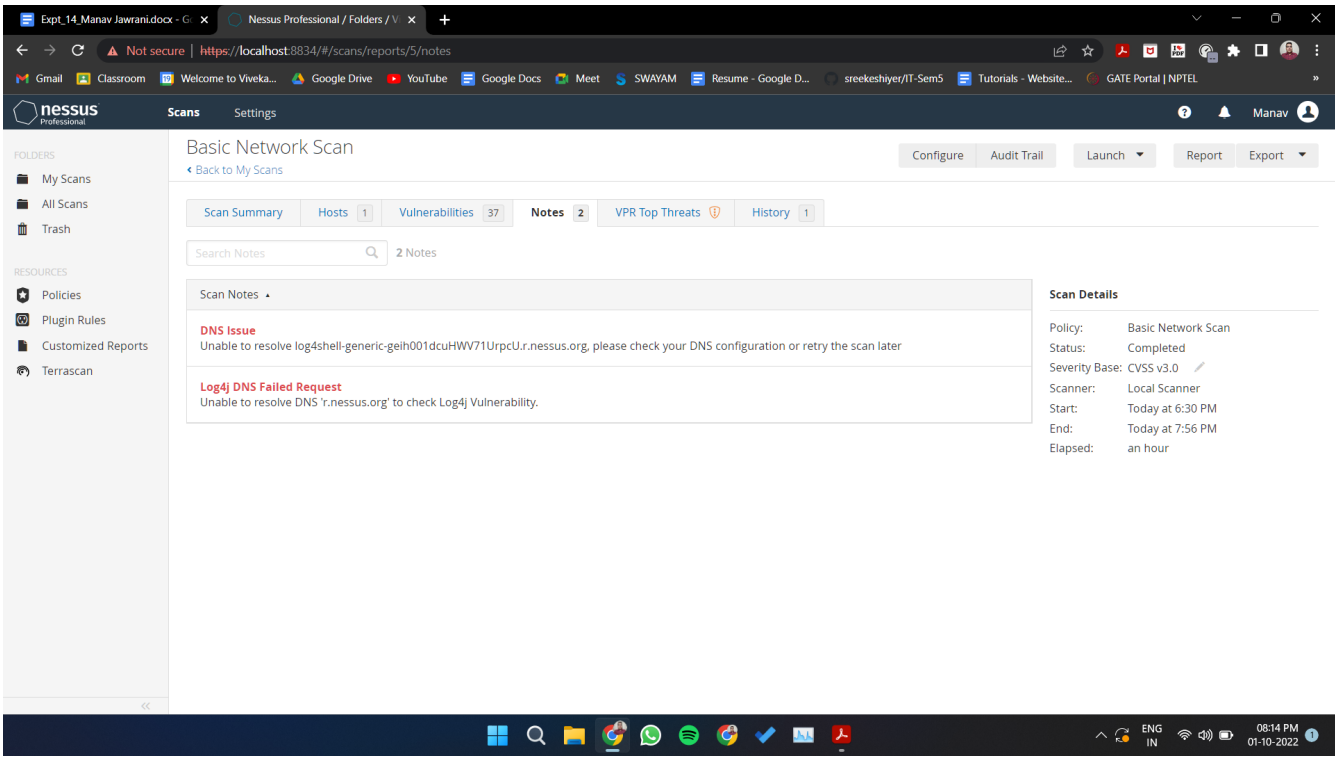
Vulnerabilities:



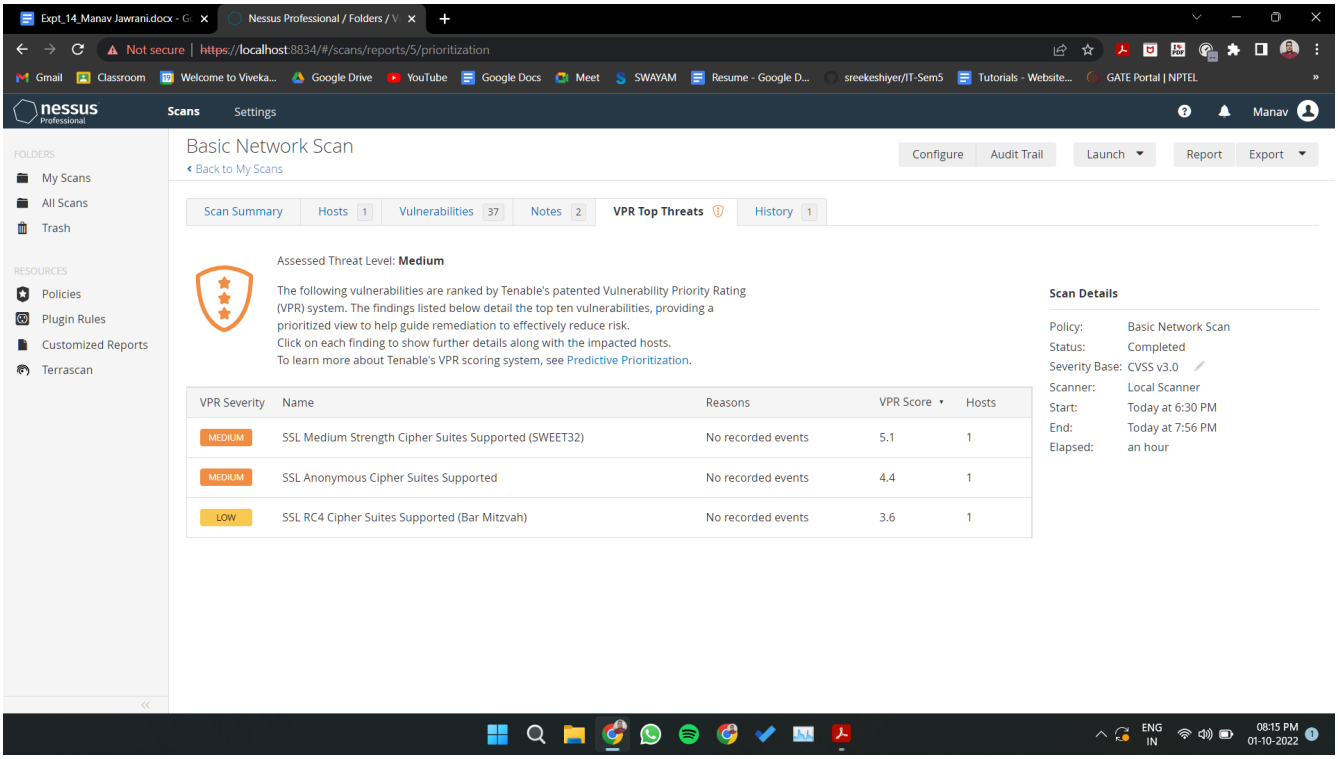
Analyzing one of the vulnerabilities:



Notes:



Top Threats:



Conclusion:

Thus we have successfully downloaded, installed and configured the Nessus tool on Windows.