Vulnerability scanning with Nessus

1. First, the **Welcome to the InstallShield Wizard for Tenable, Inc. Nessus** screen appears. Select **Next** to continue.

2. On the **License Agreement** screen, read the terms of the Tenable, Inc. Nessus software license and subscription agreement.

3. Select the **I accept the terms of the license agreement** option, and then click **Next**.

4. On the **Destination Folder** screen, select the **Next** button to accept the default installation folder. Otherwise, select the **Change** button to install Nessus to a different folder.

5. On the **Ready to Install the Program** screen, select the **Install** button.

The **Installing Tenable, Inc. Nessus** screen appears and a **Status** indication bar shows the installation progress. The process may take several minutes.

After the **InstallShield Wizard** completes, the **Welcome to Nessus** page loads in your default browser.

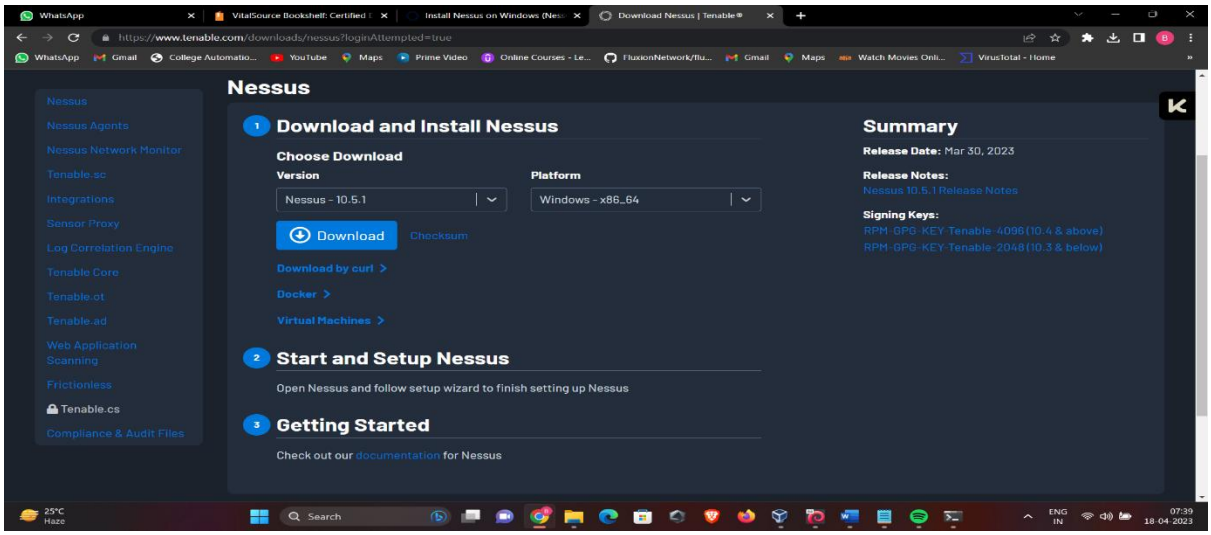
If the page does not load, do one of the following steps to open Nessus in your browser.

- To access a remotely installed Nessus instance, go to https://<remote IP address>:8834 (for example, https://111.49.7.180:8834).

- To access a locally installed Nessus instance, go to https://localhost:8834.

Got to official website of Nessus

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

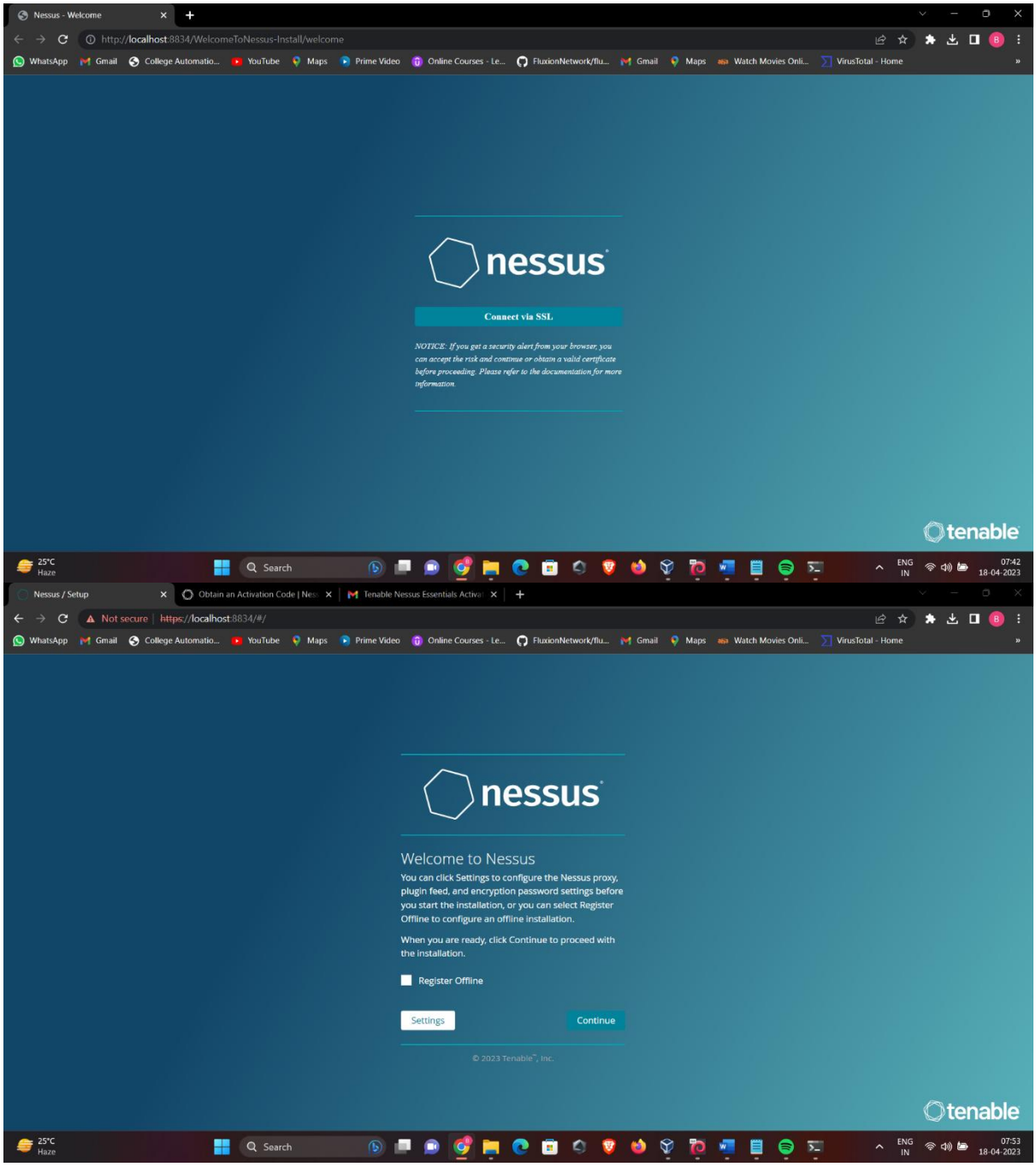


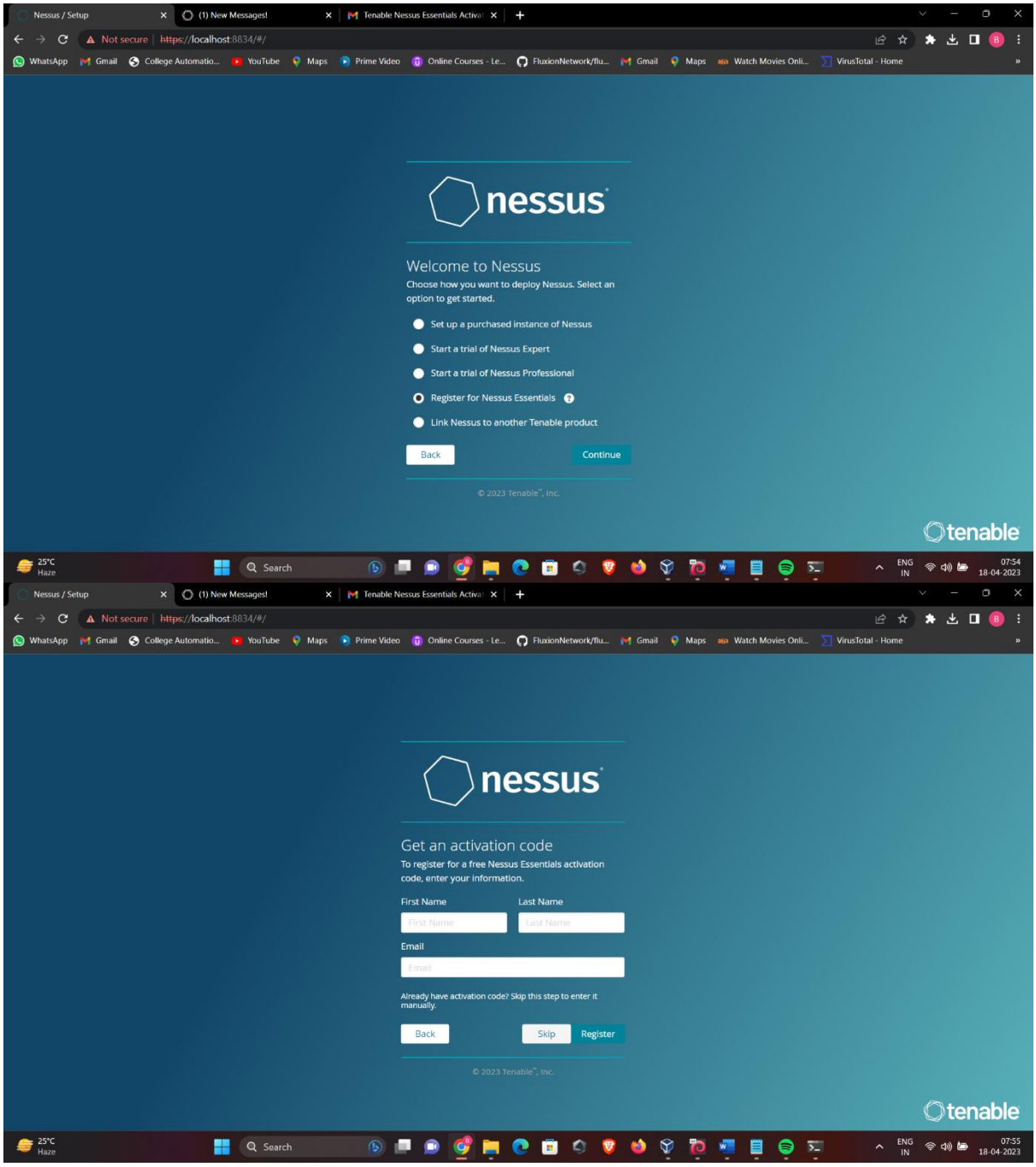
DOWNLOAD THE MSI

Open the file u download and install with the default settings

Just type next if it asks any thing

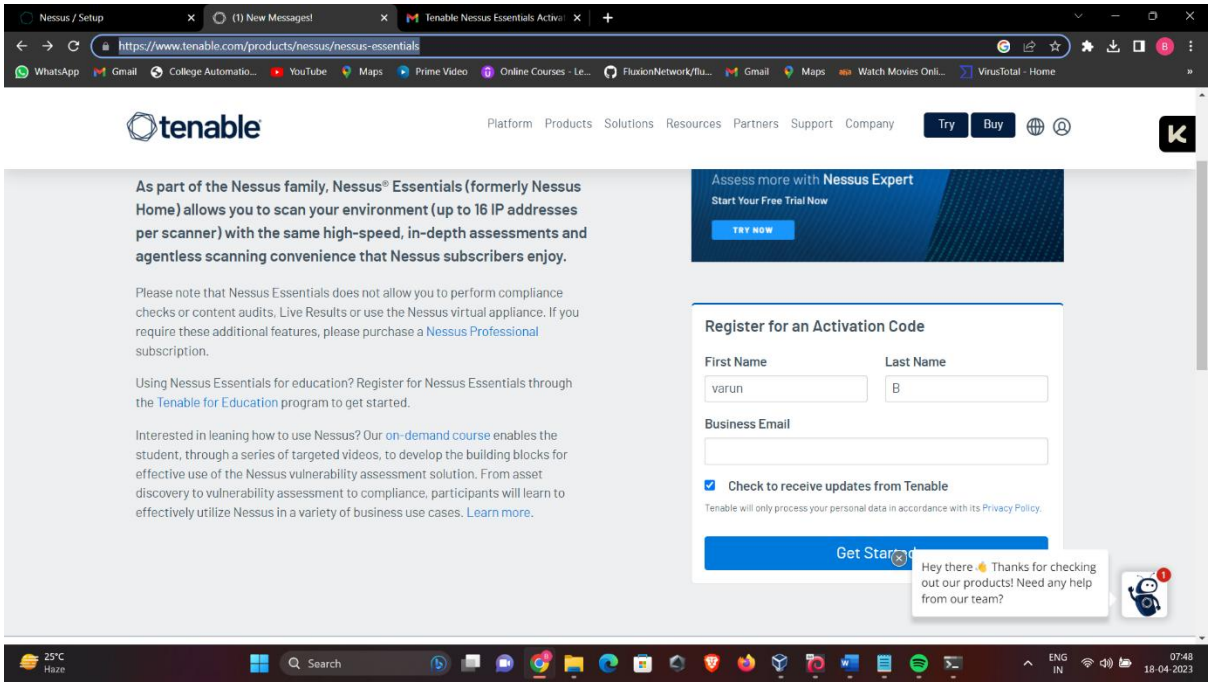
NOW it will open the website



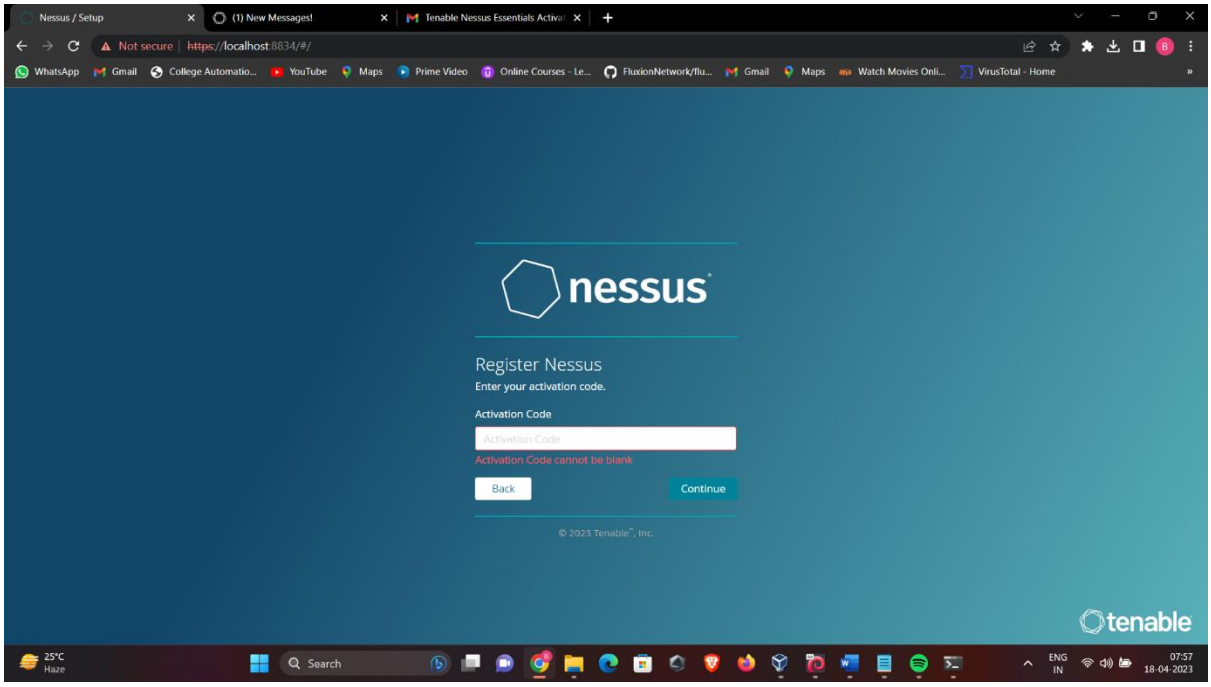


OPEN net table and go to this website

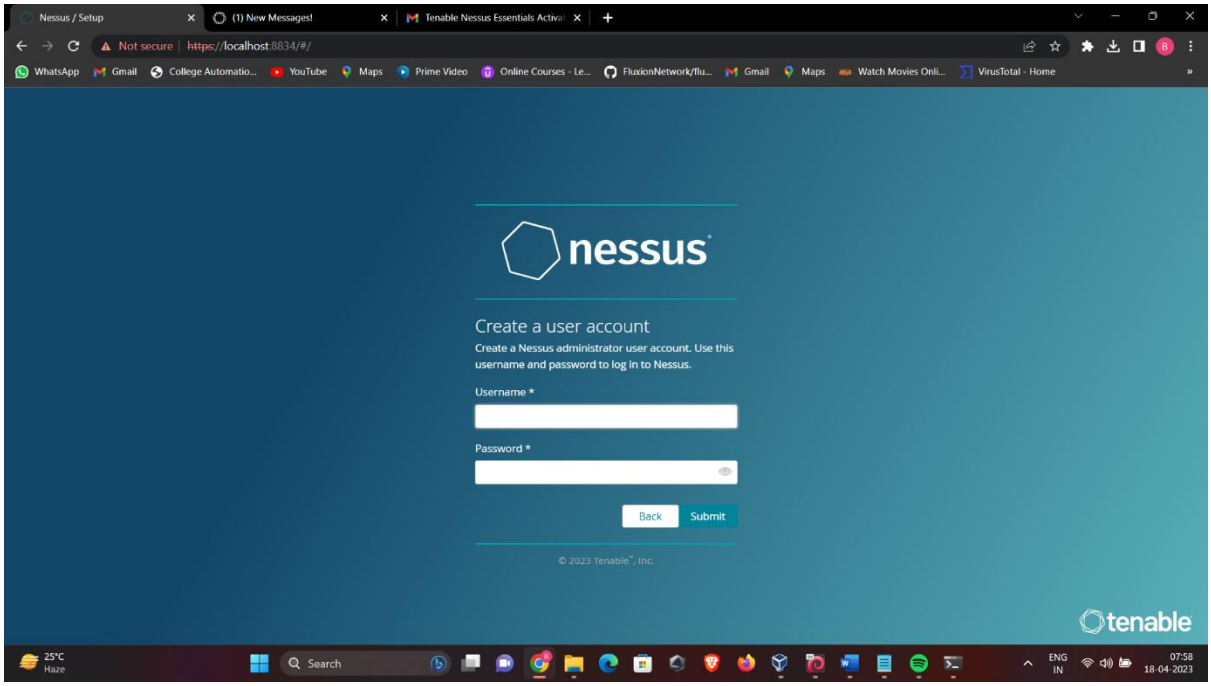
https://www.tenable.com/products/nessus/nessus-essentials



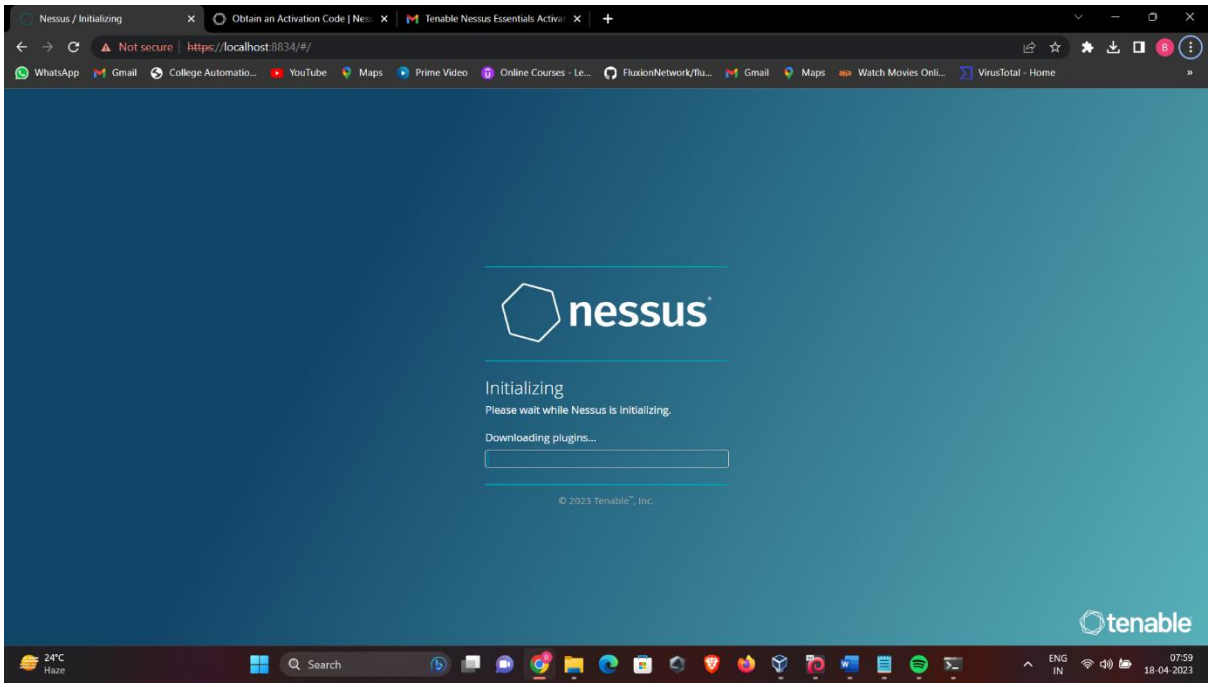
YOU will get a mail after fillig the form of activation key. Copy that code and enter in the



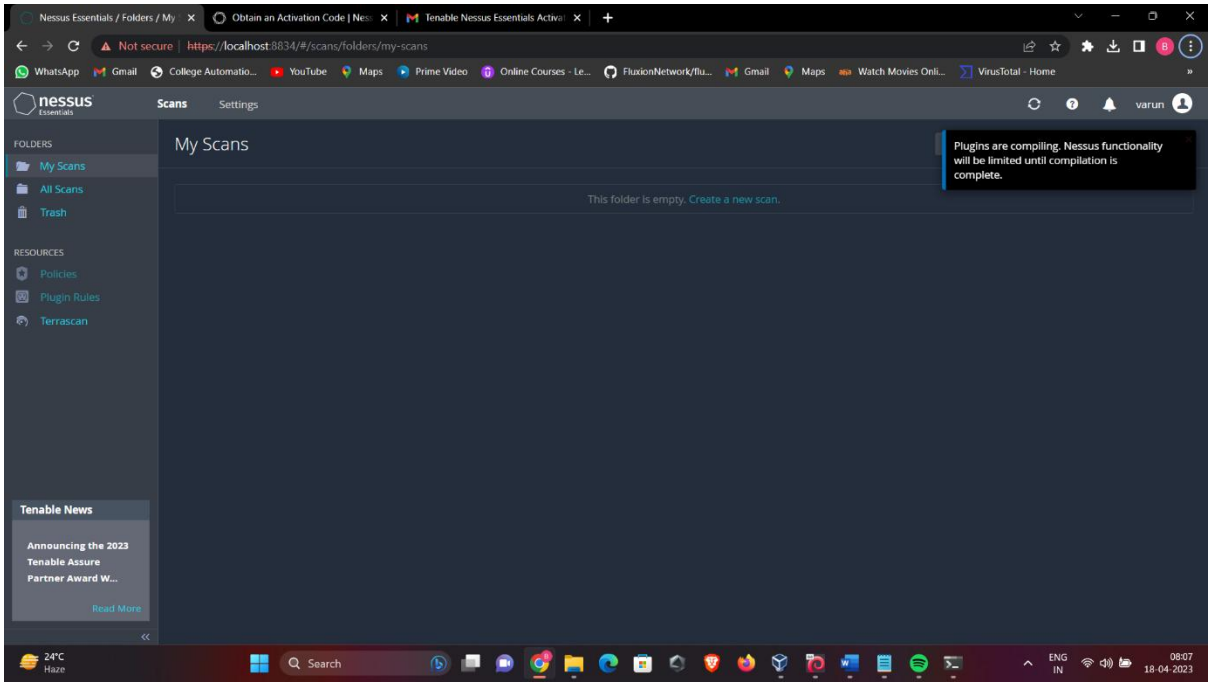
Now next create the user



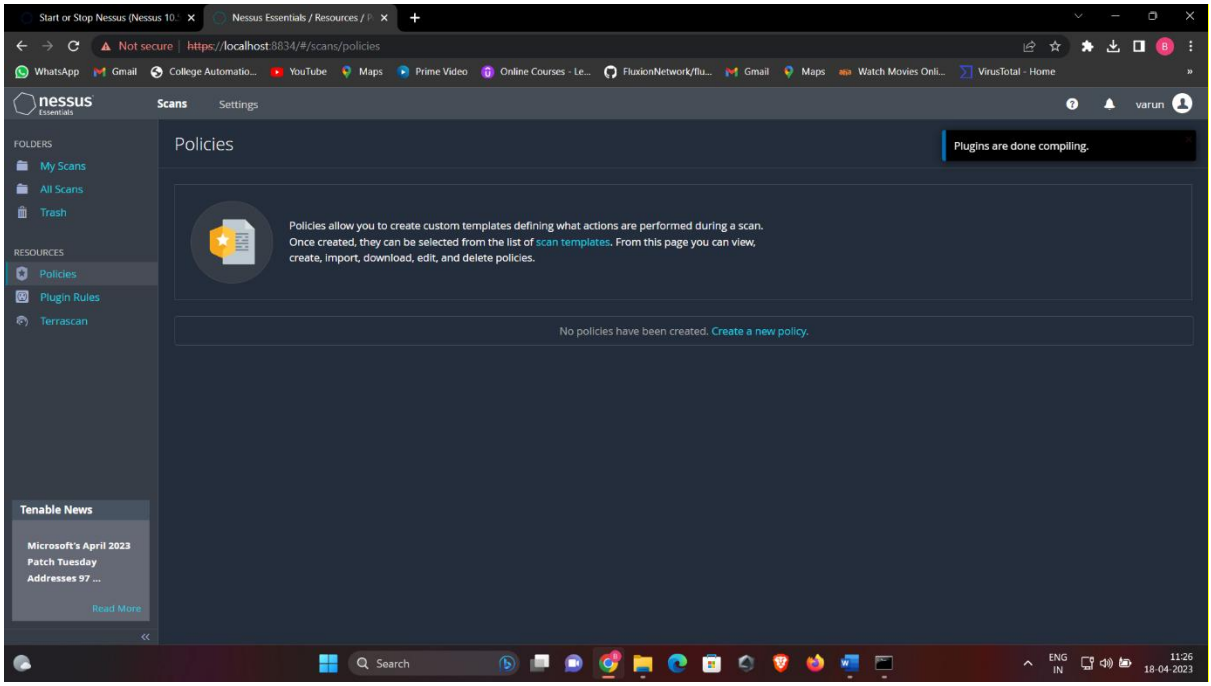
Now click on submit

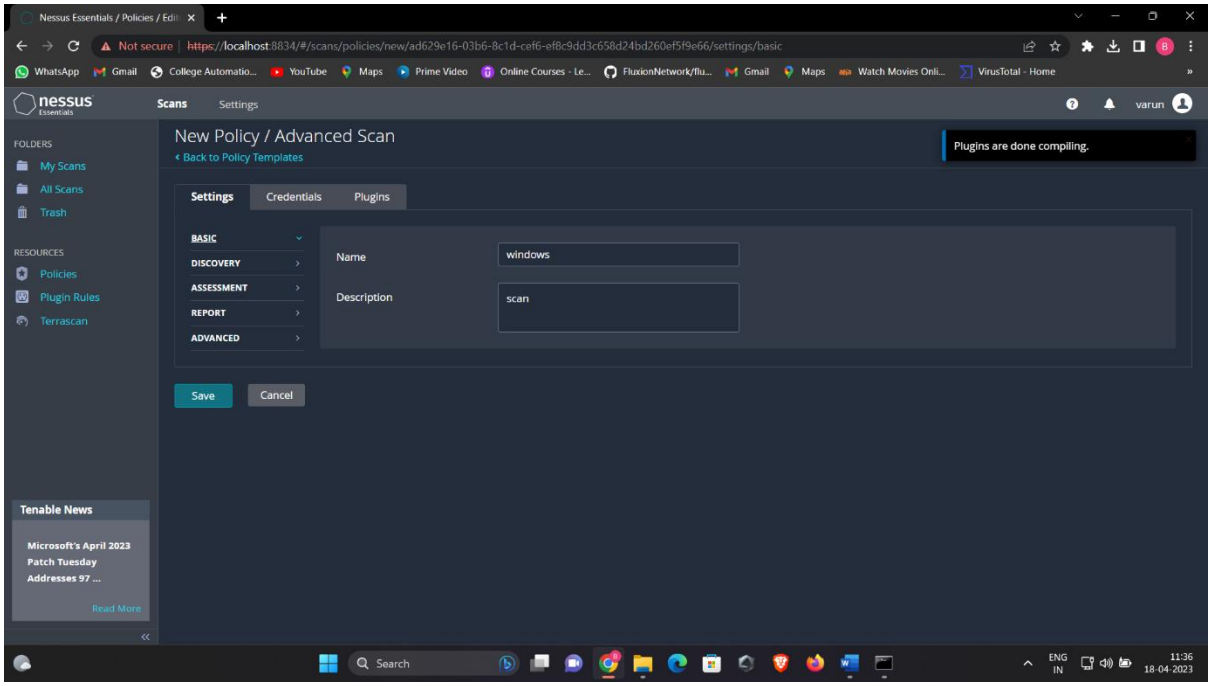


After it will prompt it



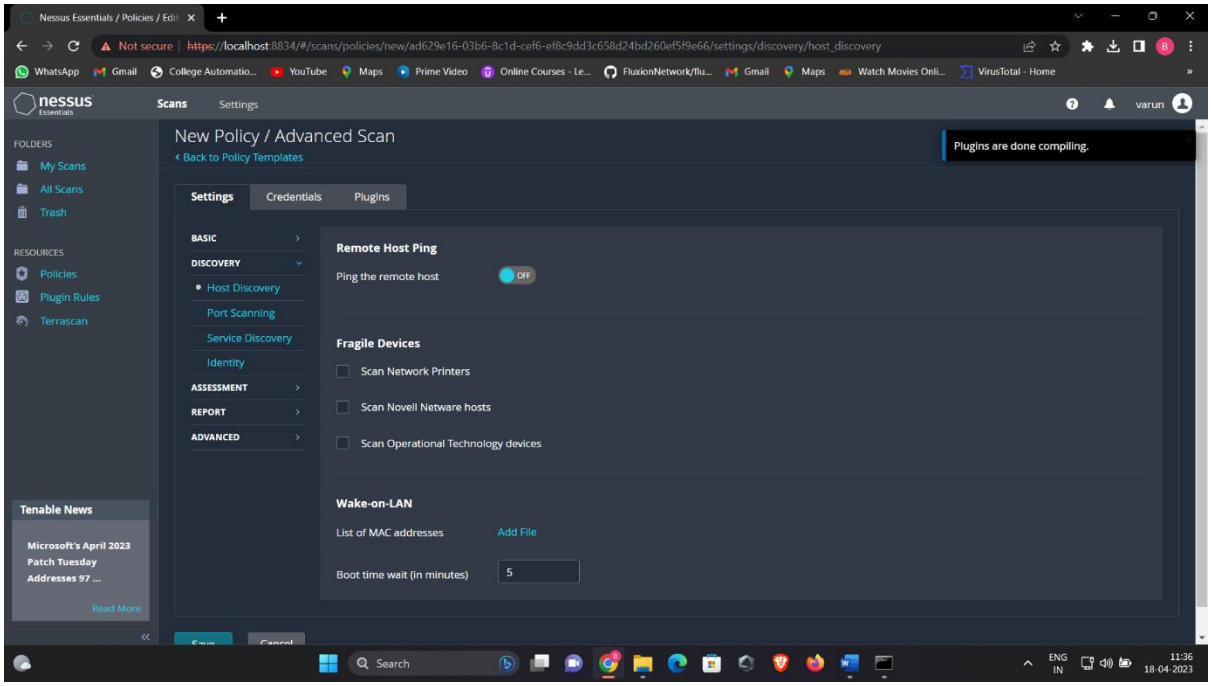
CLICK ON Create a new policy



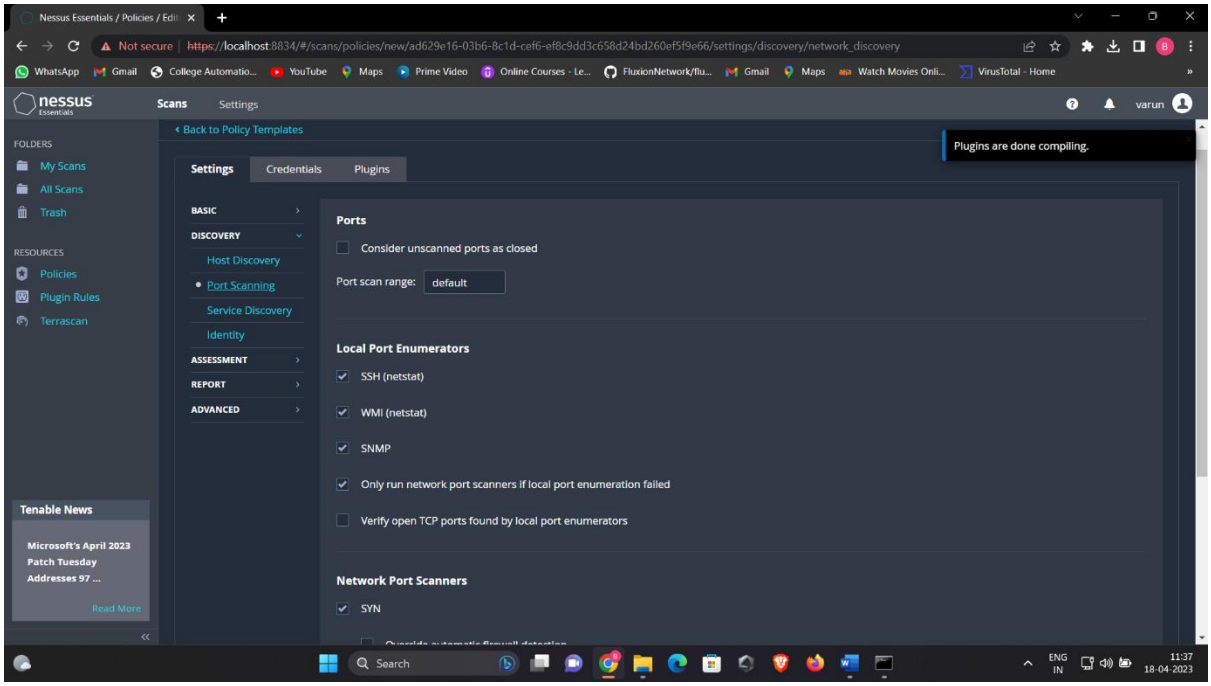


In discover disable

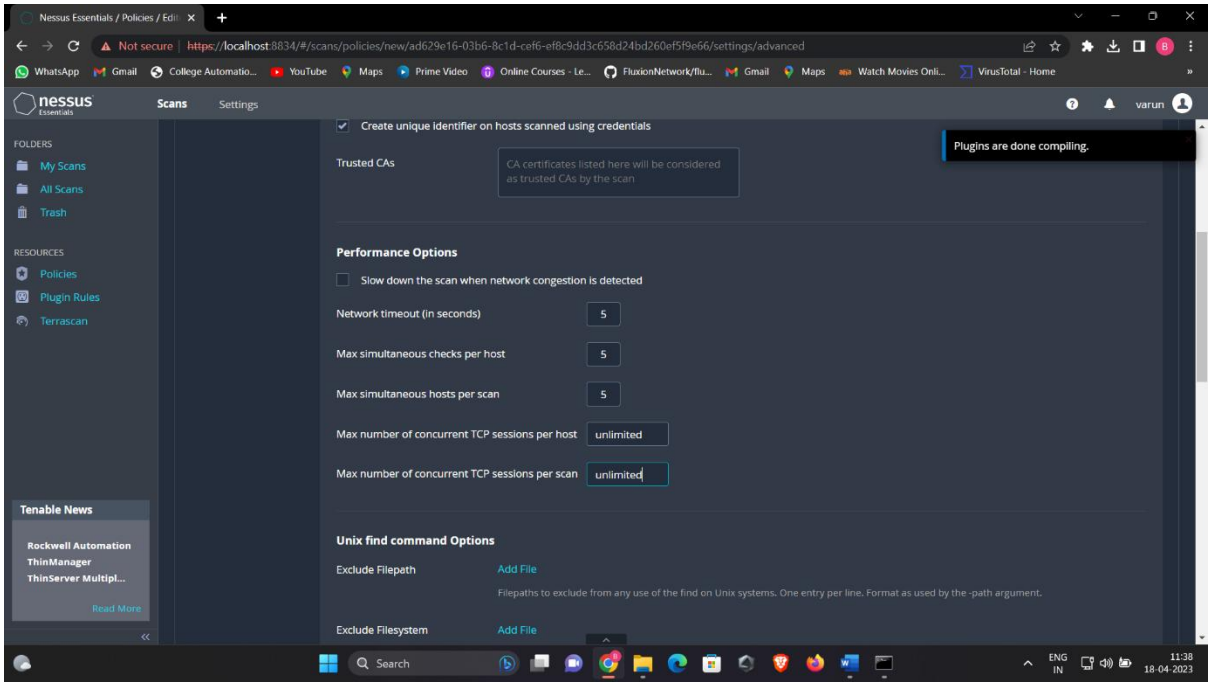
Ping



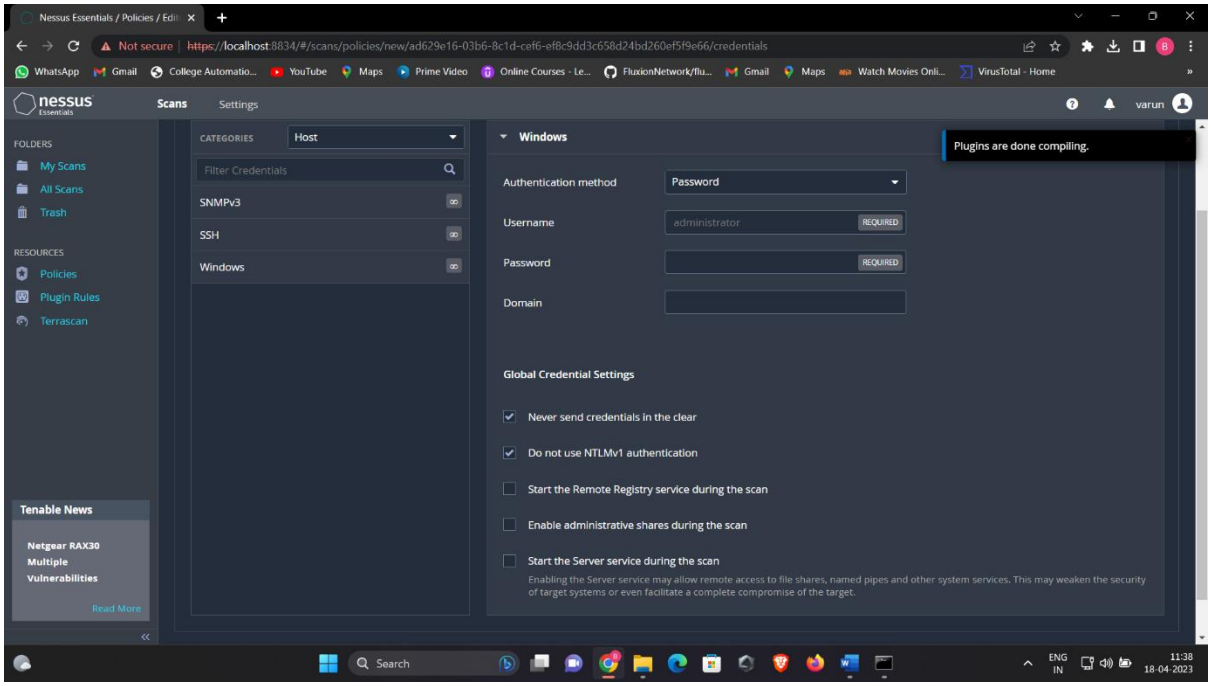
In discovery check the TCP



IN ADVANCE TCP TYPE unlimited in both the boxes



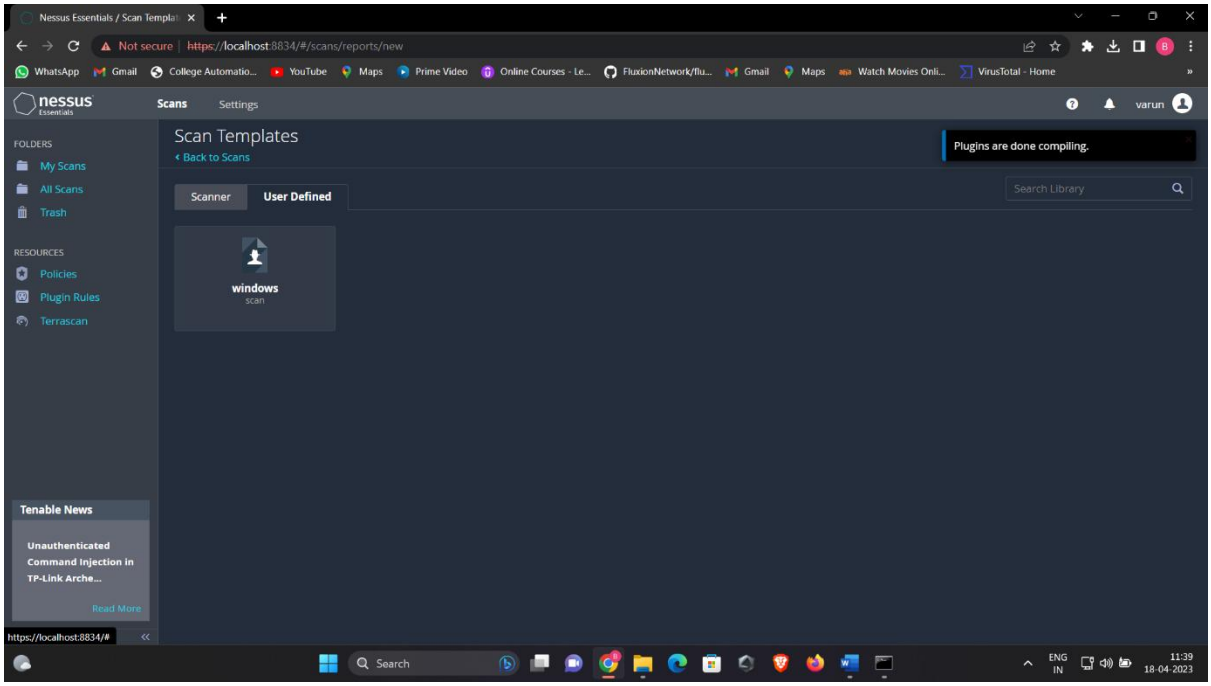
IN credentials select windows and fill the username and passwords



NOW Go to scan and select **New scan**

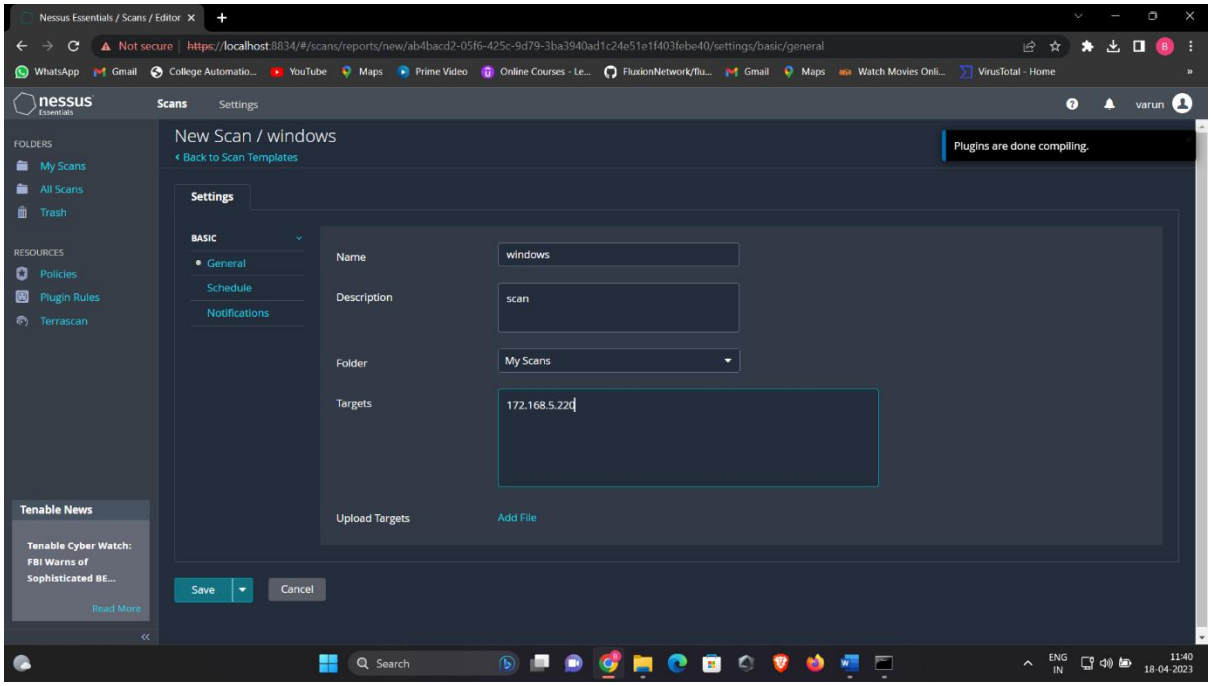
And

select user Defined, select your file.

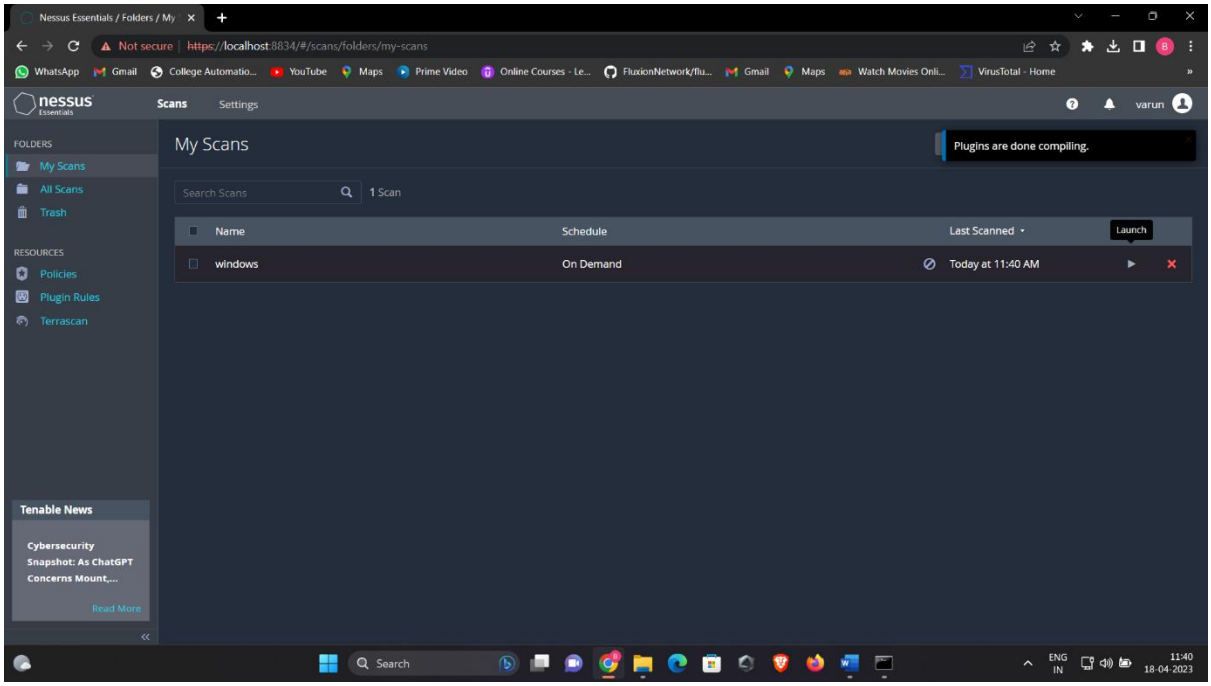


type your ip address of windows machine.

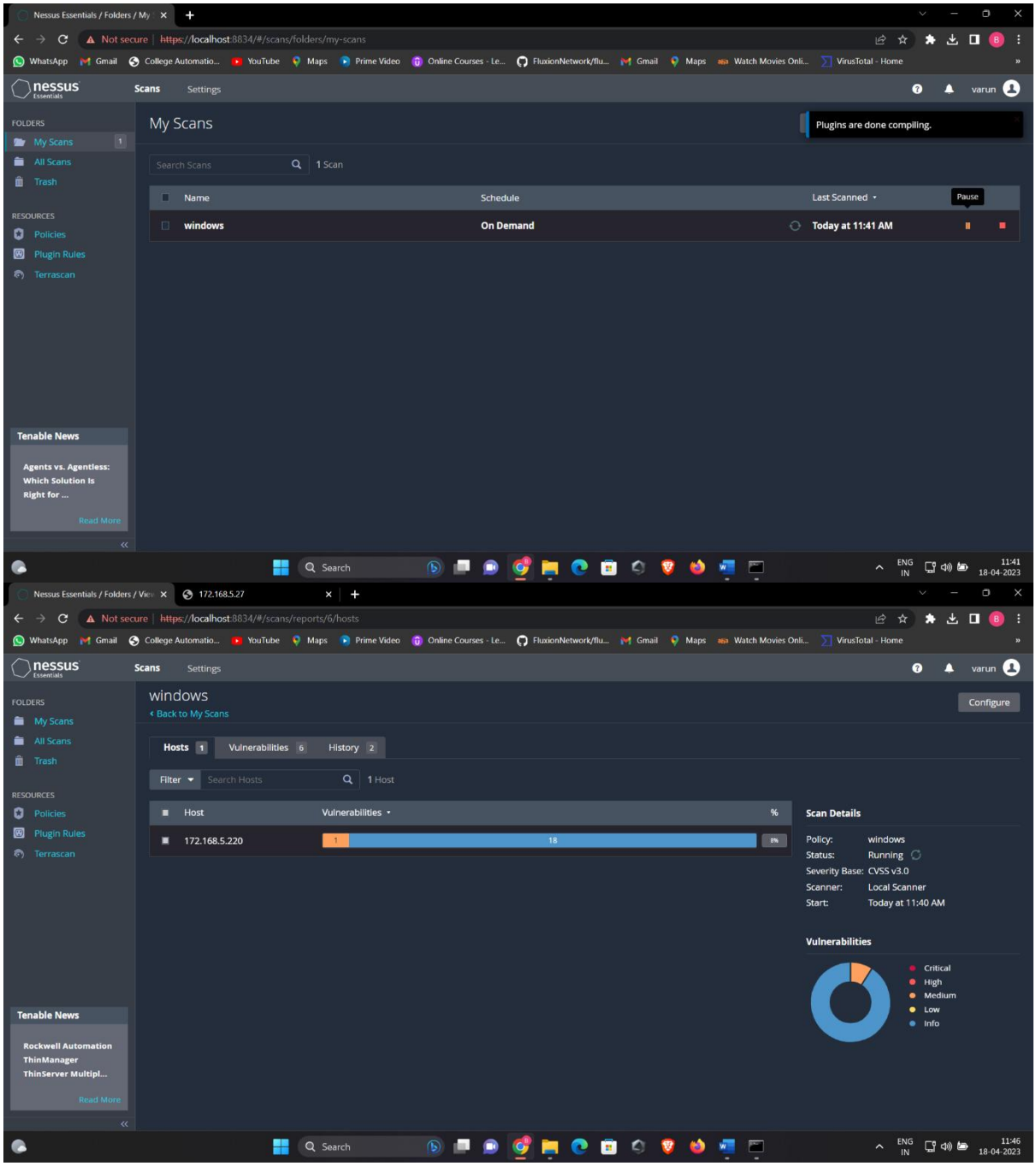
To know your ip type ipconfig in your cmd and fill it

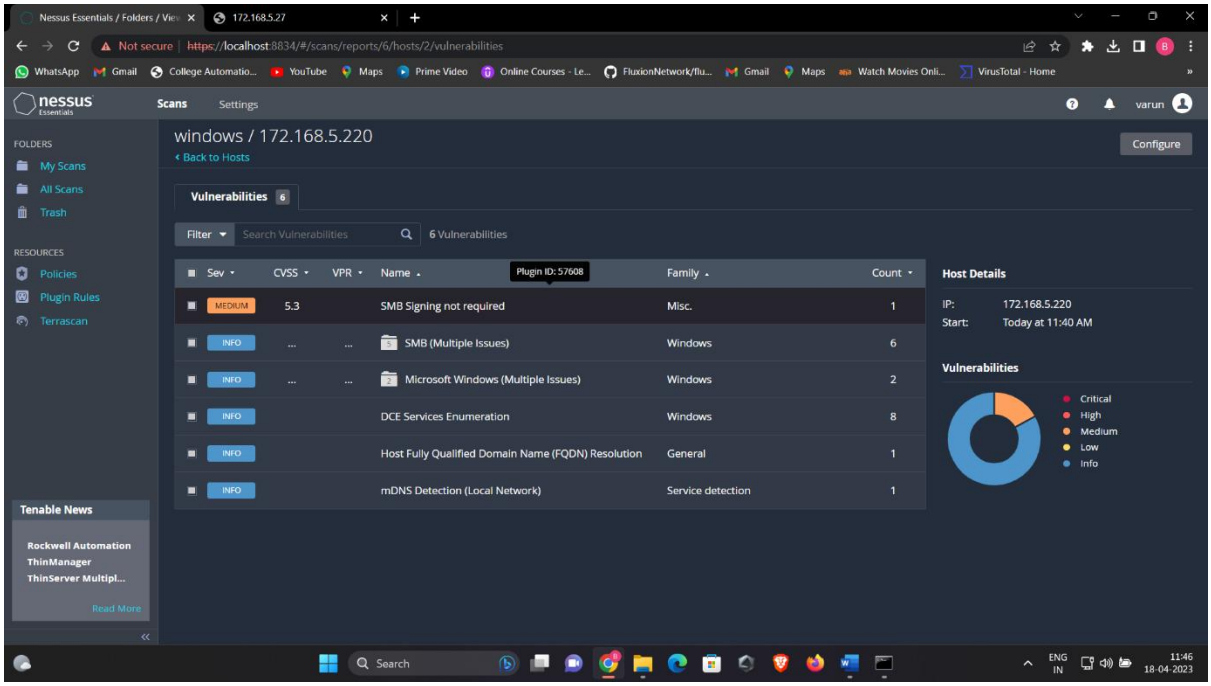


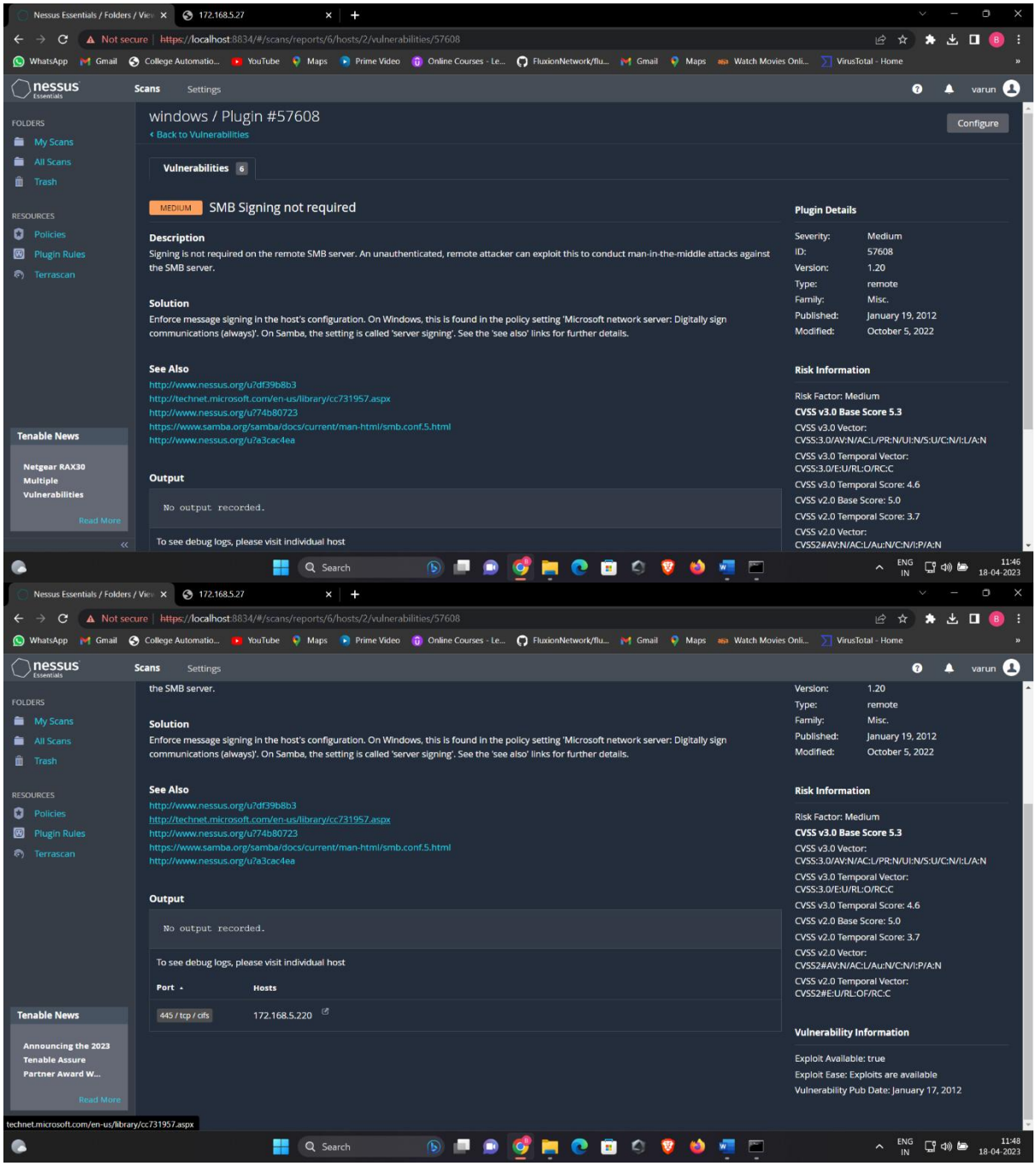
Start the scan. It will take some time



After that u can open the windows and check for report

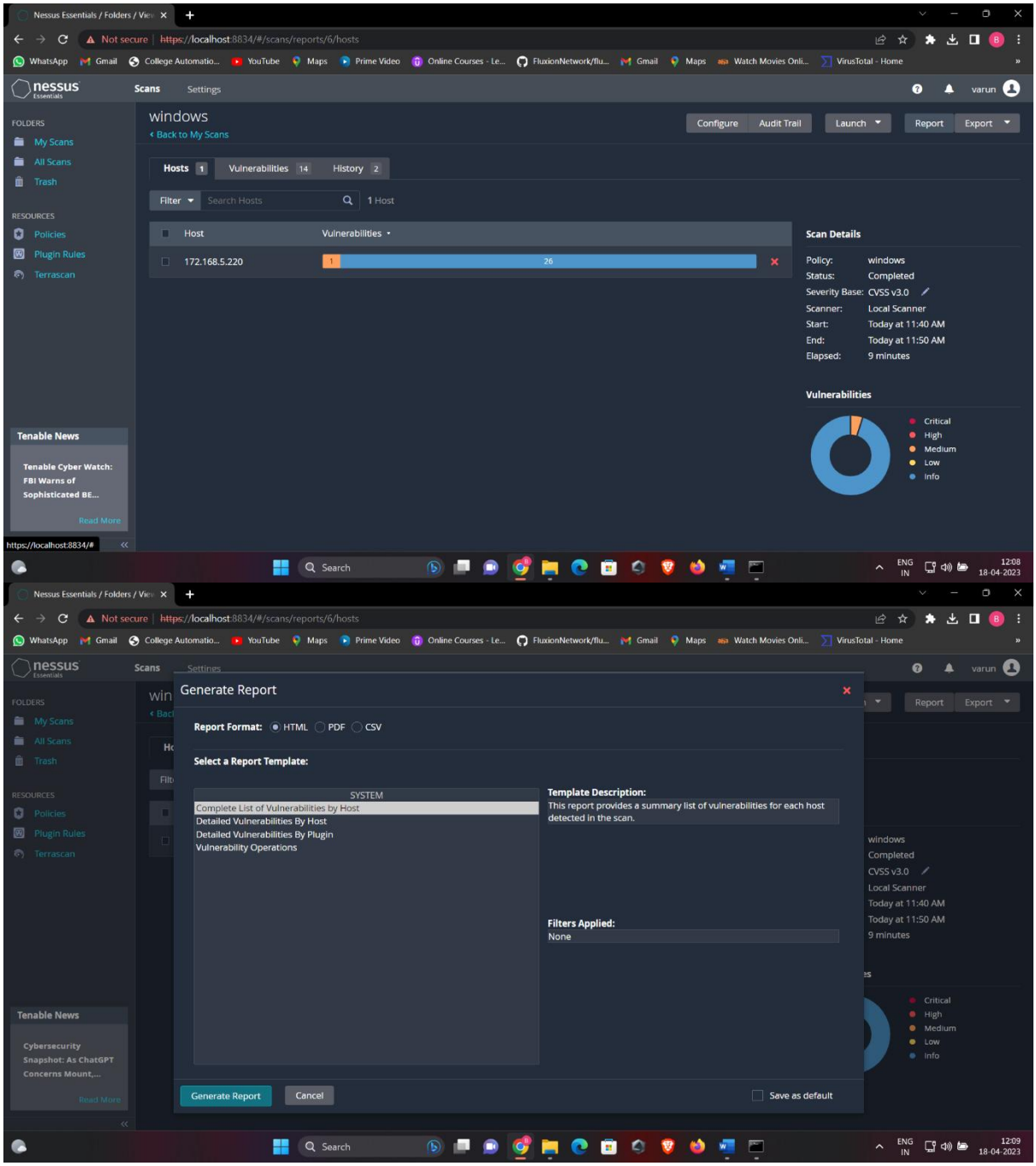

Nessus Essentials / Folders / My
Not secure | https://localhost:8834/#/scans/folders/my-scans
nessus Essentials
Scans
Settings
varun
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
My Scans
Plugins are done compiling.
Search Scans
1 Scan
Name
Schedule
Last Scanned
Pause
windows
On Demand
Today at 11:41 AM
Tenable News
Agents vs. Agentless: Which Solution Is Right for ...
Read More
Search
ENG IN
11:41 18-04-2023
Nessus Essentials / Folders / Vie
172.168.5.27
Not secure | https://localhost:8834/#/scans/reports/6/hosts
nessus Essentials
Scans
Settings
varun
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
windows
Back to My Scans
Configure
Hosts 1
Vulnerabilities 6
History 2
Filter
Search Hosts
1 Host
Host
Vulnerabilities
%
172.168.5.220
1
18
8%
Scan Details
Policy: windows
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:40 AM
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Rockwell Automation ThinManager ThinServer Multipl...
Read More
Search
ENG IN
11:46 18-04-2023


Nessus Essentials / Folders / Vie
172.168.5.27
Not secure | https://localhost:8834/#/scans/reports/6/hosts/2/vulnerabilities
nessus Essentials
Scans
Settings
varun
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Rockwell Automation ThinManager ThinServer Multipl...
Read More
windows / 172.168.5.220
Back to Hosts
Configure
Vulnerabilities 6
Filter
Search Vulnerabilities
6 Vulnerabilities
Sev
CVSS
VPR
Name
Plugin ID: 57608
Family
Count
MEDIUM 5.3 SMB Signing not required Misc. 1
INFO ... ... SMB (Multiple Issues) Windows 6
INFO ... ... Microsoft Windows (Multiple Issues) Windows 2
INFO DCE Services Enumeration Windows 8
INFO Host Fully Qualified Domain Name (FQDN) Resolution General 1
INFO mDNS Detection (Local Network) Service detection 1
Host Details
IP: 172.168.5.220
Start: Today at 11:40 AM
Vulnerabilities
Critical
High
Medium
Low
Info
Search
ENG IN
11:46 18-04-2023

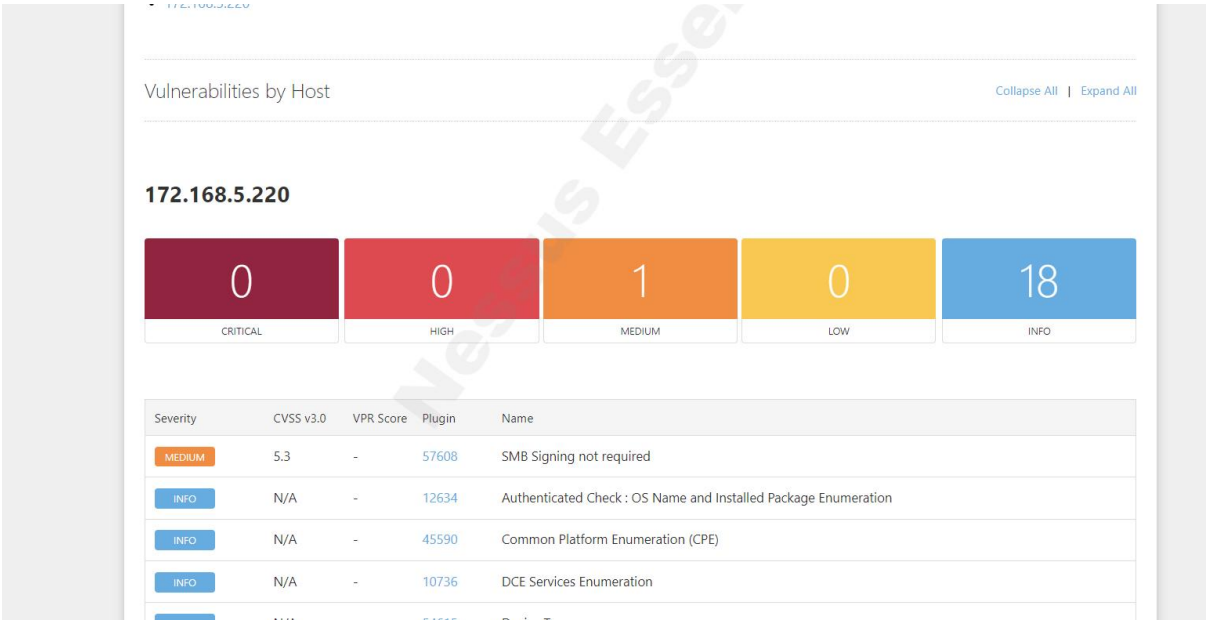


YOU can generate the report by open the windows file

At RIGHT-CORNER click on report and generate it as html



Open html file you can view



Vulnerabilities by Host

Collapse All | Expand All

172.168.5.220

0	0	1	0	18
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	Plugin	Name
MEDIUM	5.3	-	57608	SMB Signing not required
INFO	N/A	-	12634	Authenticated Check : OS Name and Installed Package Enumeration
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration

After all that