Experiment 14

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

| Roll No. | 37 |
| --- | --- |
| Name | Mikil Lalwani |
| Class | D15-B |
| Subject | Security Lab |
| LO Mapped | LO4: Use tools like sniffers, port scanners, and other related tools for analyzing packets in a network. |

**Aim:**

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

**Theory:**

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.

Suppose you are an administrator in charge of any computer (or group of computers) connected to the internet. In that case, Nessus is a great tool to help keep their domains free of the easy vulnerabilities that hackers and viruses commonly look to exploit.

**Features of Nessus:**

1. Unlike other scanners, Nessus does not make assumptions about your server configuration (such as assuming that port 80 must be the only web server) that can cause other scanners to miss real vulnerabilities.

2. Nessus is very extensible, providing a scripting language to write tests specific to your system once you become more familiar with the tool. It also provides a plug-in interface; many free plugins are available from the Nessus plug-in site. These plugs are often specific to detecting a common virus or vulnerability.

3. Up-to-date information about new vulnerabilities and attacks. The Nessus team updates the list

of what vulnerabilities to check for on a daily basis in order to minimize the window between an

exploit appearing in the wild, and you being able to detect it with Nessus.

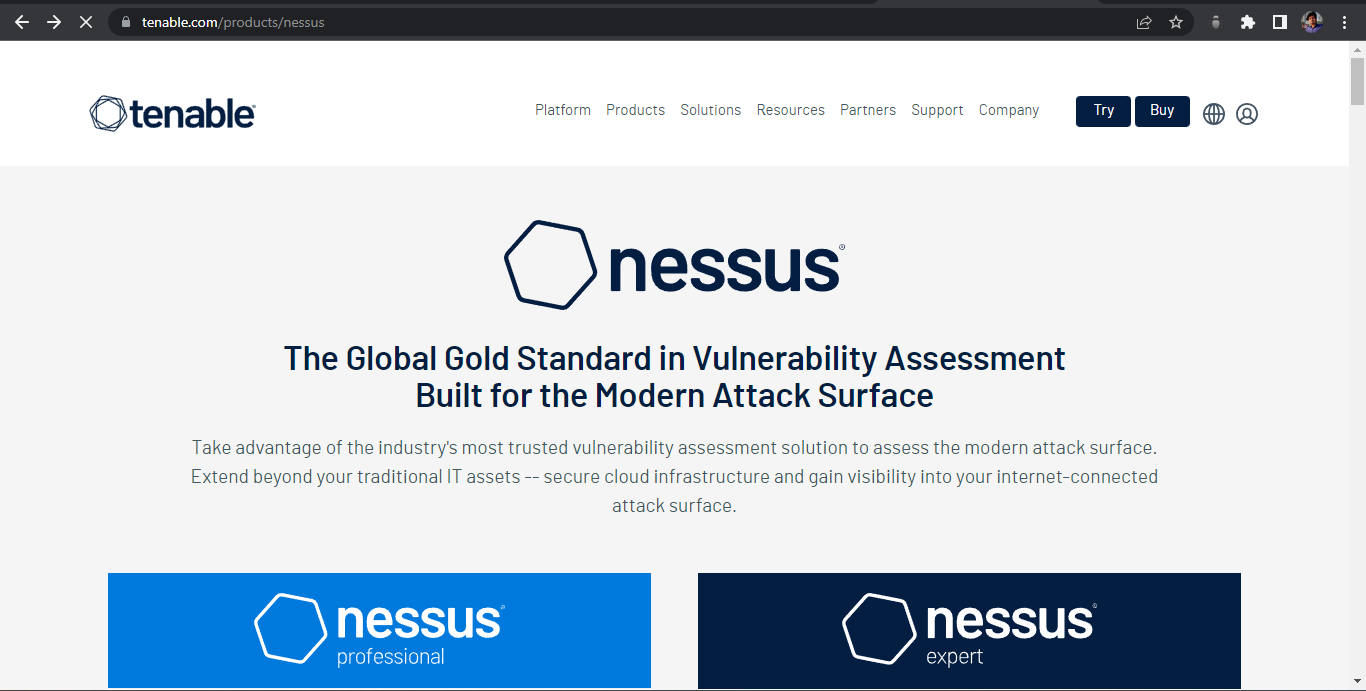
4. Open-source. Nessus is open source, meaning it costs nothing, and you are free to see and modify the source as you wish.

5. Patching Assistance: When Nessus detects a vulnerability, it is also most often able to suggest the best way you can mitigate the vulnerability.

**Output:**

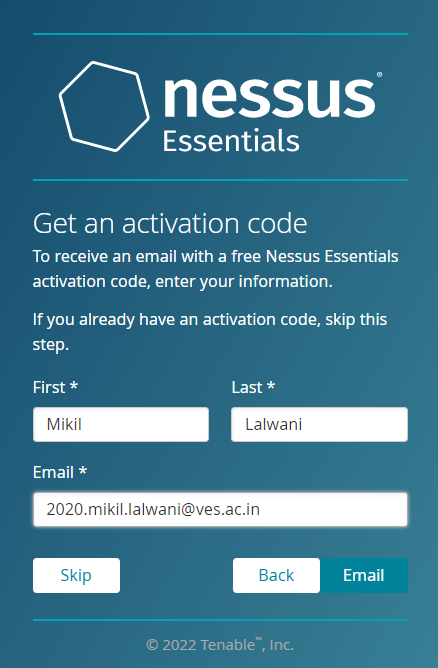
**STEP 1:**

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.

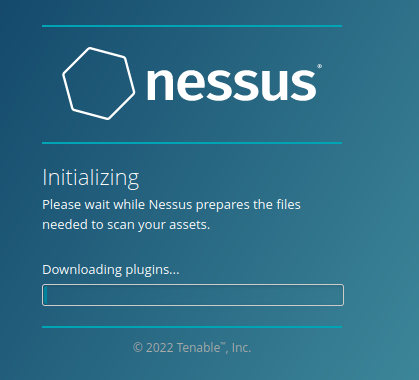


**STEP 2:**

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.

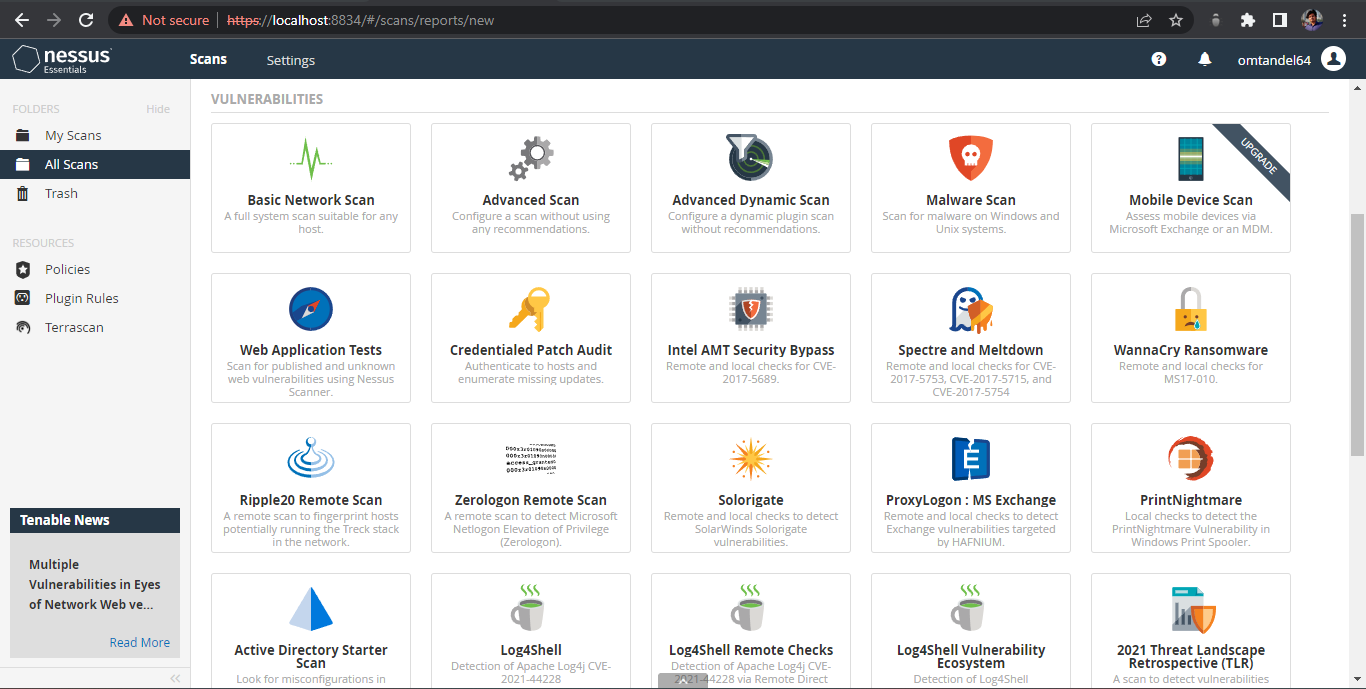






**STEP 3:**

Start a Vulnerability Scan It’s time to actually test your network. 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.

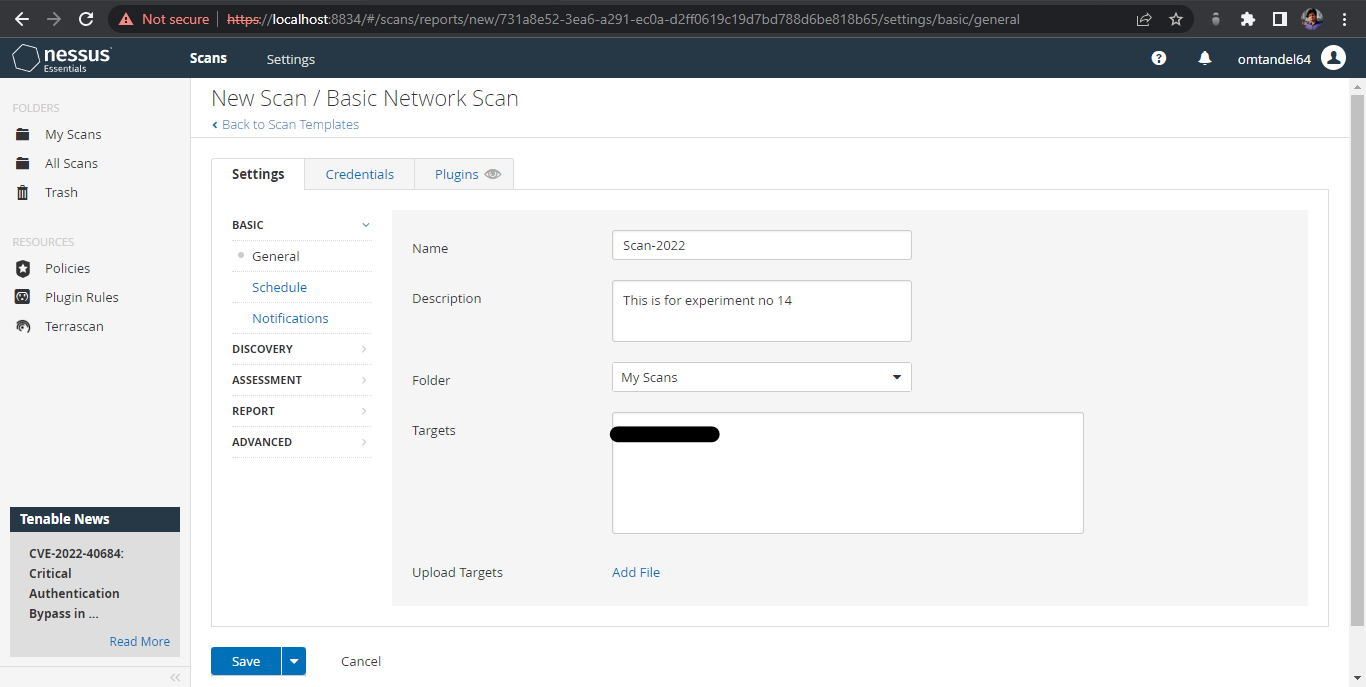


a. Click the “New Scan.”

b. Click “Basic Network Scan.”

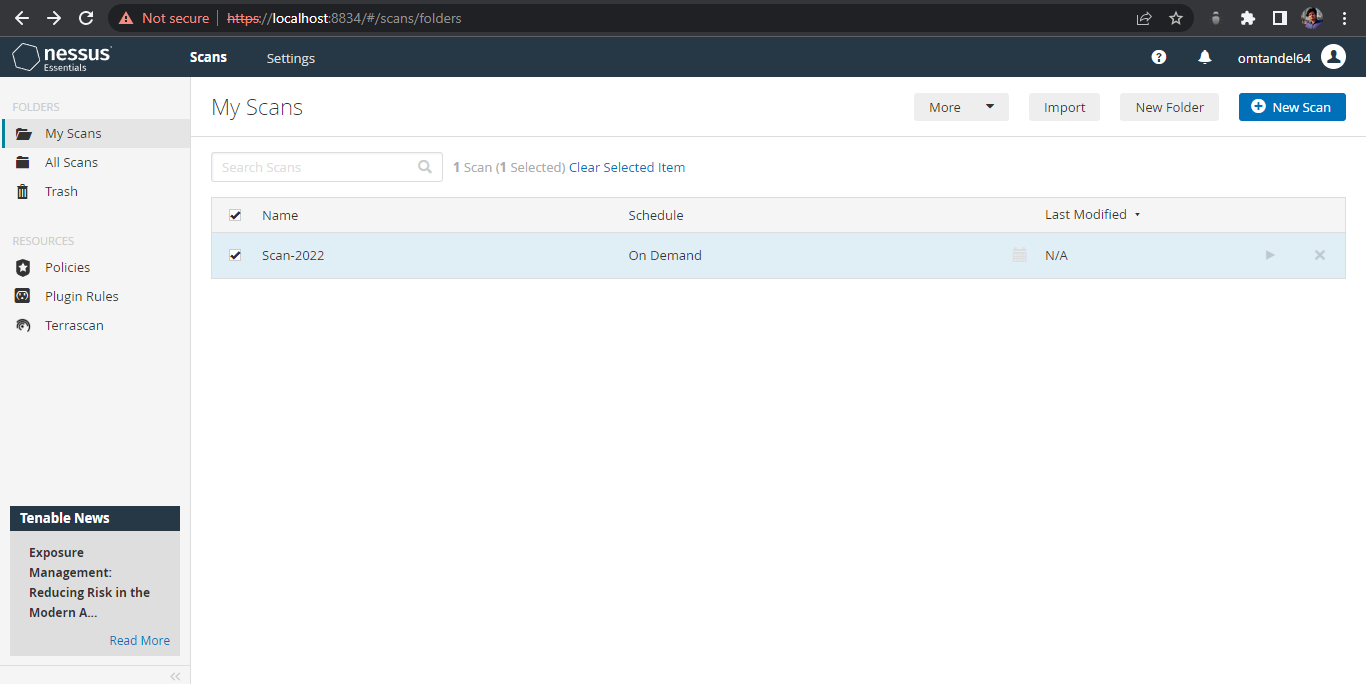
c. Name your scan and add a description.

d. In the “Targets” field, you’ll want to enter IP scanning details about your home network. For example, if your router is at 192.168.0.1, you’d want to enter 192.168.0.1/24. This will make it so Nessus scans all the devices on your network (unless you have a ton of devices this is probably as high as you’d need to go).



5. Click “Save.”

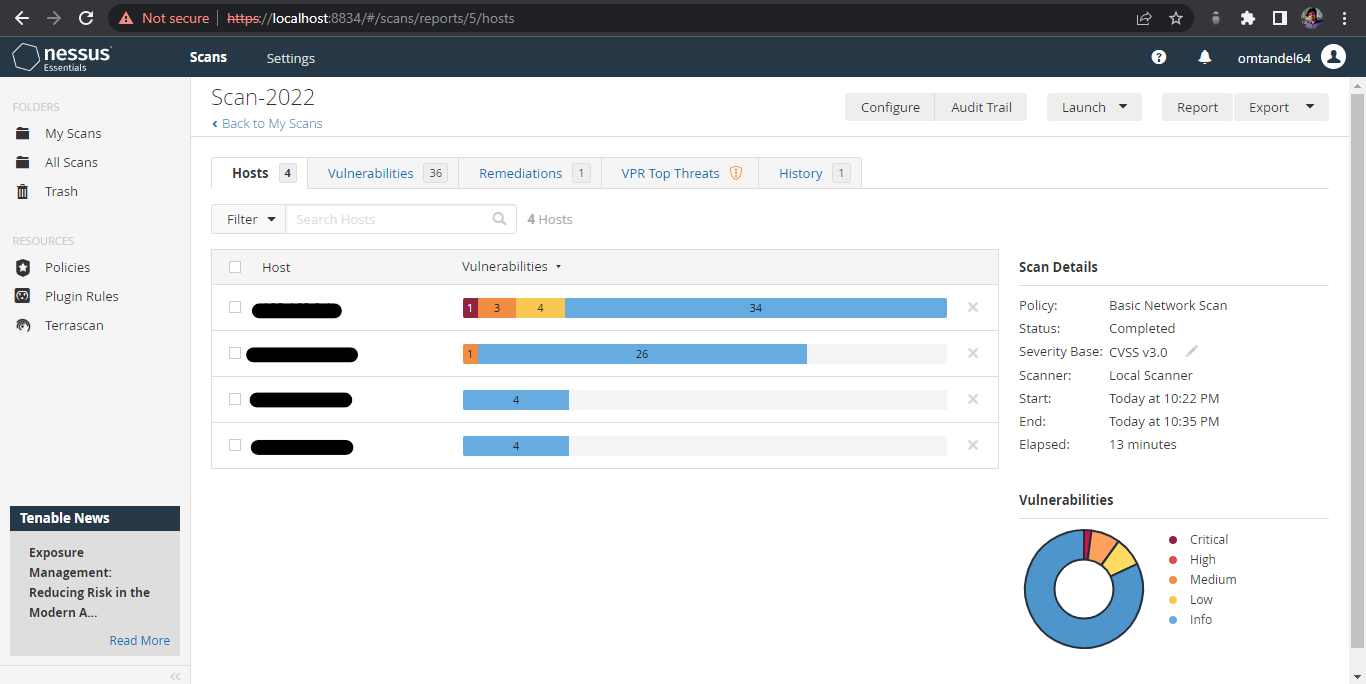
6. On the next screen, click the Play icon to launch the scan.



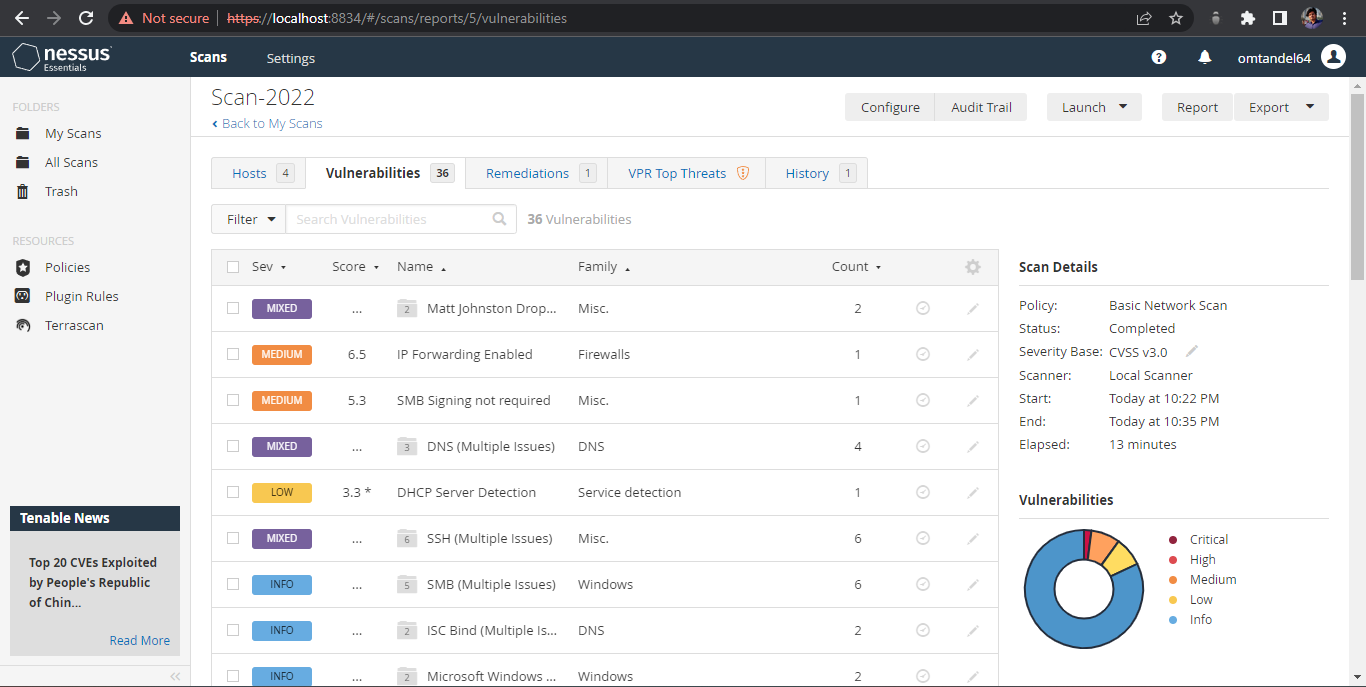
Depending on what and how many devices you have on your network, the scan takes a while.

**STEP 4:**

Viewing Your Results Once Nessus finishes, you’ll see a bunch of color-coded graphs for each device (referred to as hosts) on your network. Each color of the graph signifies the danger of a vulnerability, from low to critical.



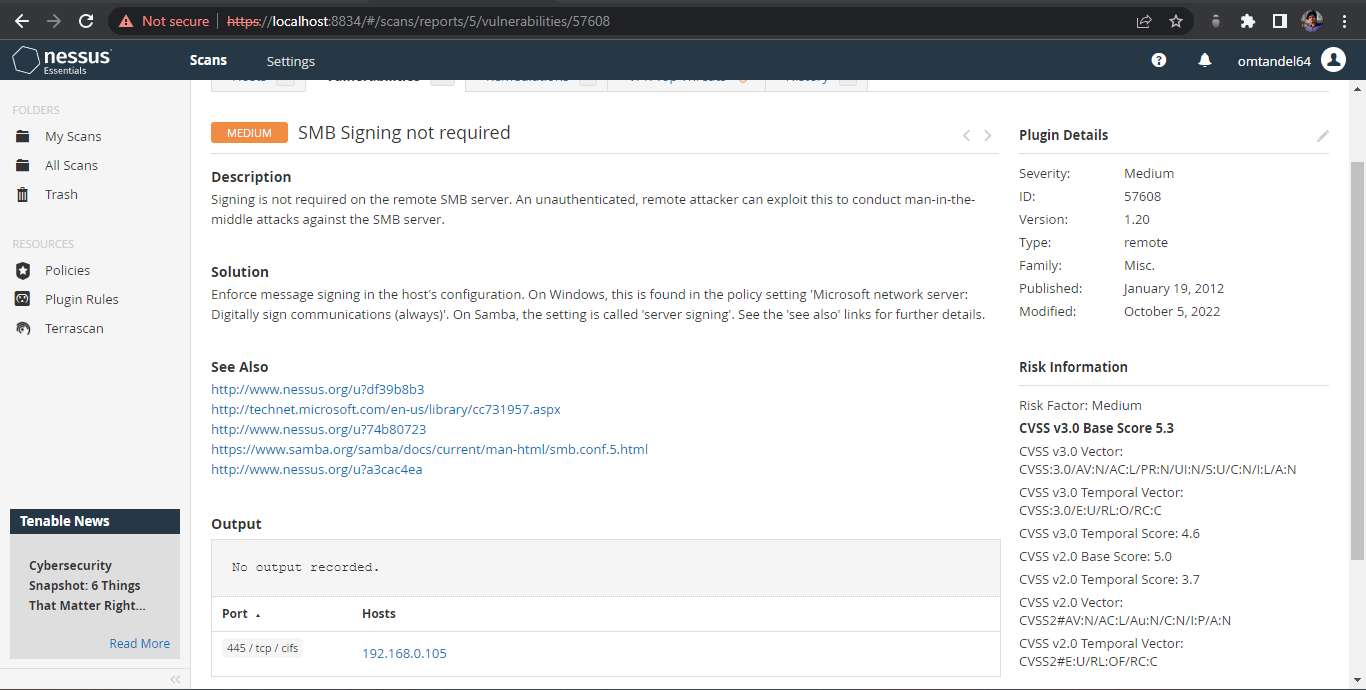
(My IP address has been blacked out)



Your results should include all the devices on your local network, from your router to your Wi-Fi-enabled printer. Click the graph to reveal more information about the vulnerabilities on each device. Vulnerabilities are listed as “plugins,” which is just Nessus’ way of discovering vulnerabilities. Click on any plugin to get more information about the vulnerability, including white papers, press releases, or patch notes for potential fixes. You can also click the Vulnerabilities tab to see an overview of all the potential vulnerabilities on the network as a whole.

**STEP 5:**

Reporting Your Results Nessus gives you all this data, but what exactly are you supposed to do with it? That depends on which vulnerabilities Nessus finds. After your scan is complete, you’ll find the biggest potential security holes in your network. All of these issues are easily remedied by either updating or deleting old software. While all this might sound a little scary, it’s worth noting that while Nessus gives you a lot of the potential ways into a network, it’s not a foolproof guide. On top of needing to be in your network in the first place (which of course, isn’t terribly complicated), they’d also need to know how to actually use the variety of exploitation tools Nessus suggests.



**Conclusion:**

Hence, we understood how to use the NESSUS to scan the network for vulnerabilities.