Task 3: Perform a Basic Vulnerability Scan on Your PC.

To perform a basic vulnerability scan lets make use of free available vulnerability scanner. let us consider Nessus Essentials.

First, download Nessus scanner from <https://www.tenable.com/products/nessus/nessus-essentials> and install the program. While installing you will get product key for registering with tenable and activate the scanner. Follow the web application instructions.

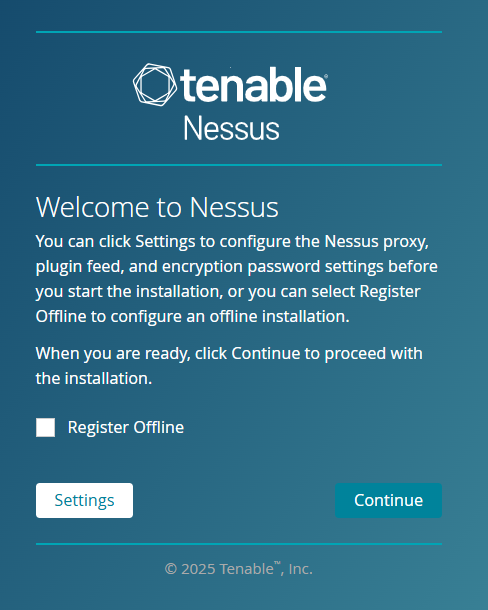


Figure - Register Nessus

A screenshot of a computer

AI-generated content may be incorrect.

Figure - Activate Nessus with Licence Key



Figure - Login with proper credentials via web browser

After logging into Nessus install plugins for scan templates. Plugin link is provided when activating the product. So be careful with the installation steps.

A screenshot of a computer

AI-generated content may be incorrect.

Figure - Install plugins into Nessus

For plugin go to Settings About Software Update Manual Software Update Upload your own plugin archive select your downloaded plugin as .tar and direct it to C:\Program Files\Tenable\Nessus folder. It will take 10 mins to install all the plugins.

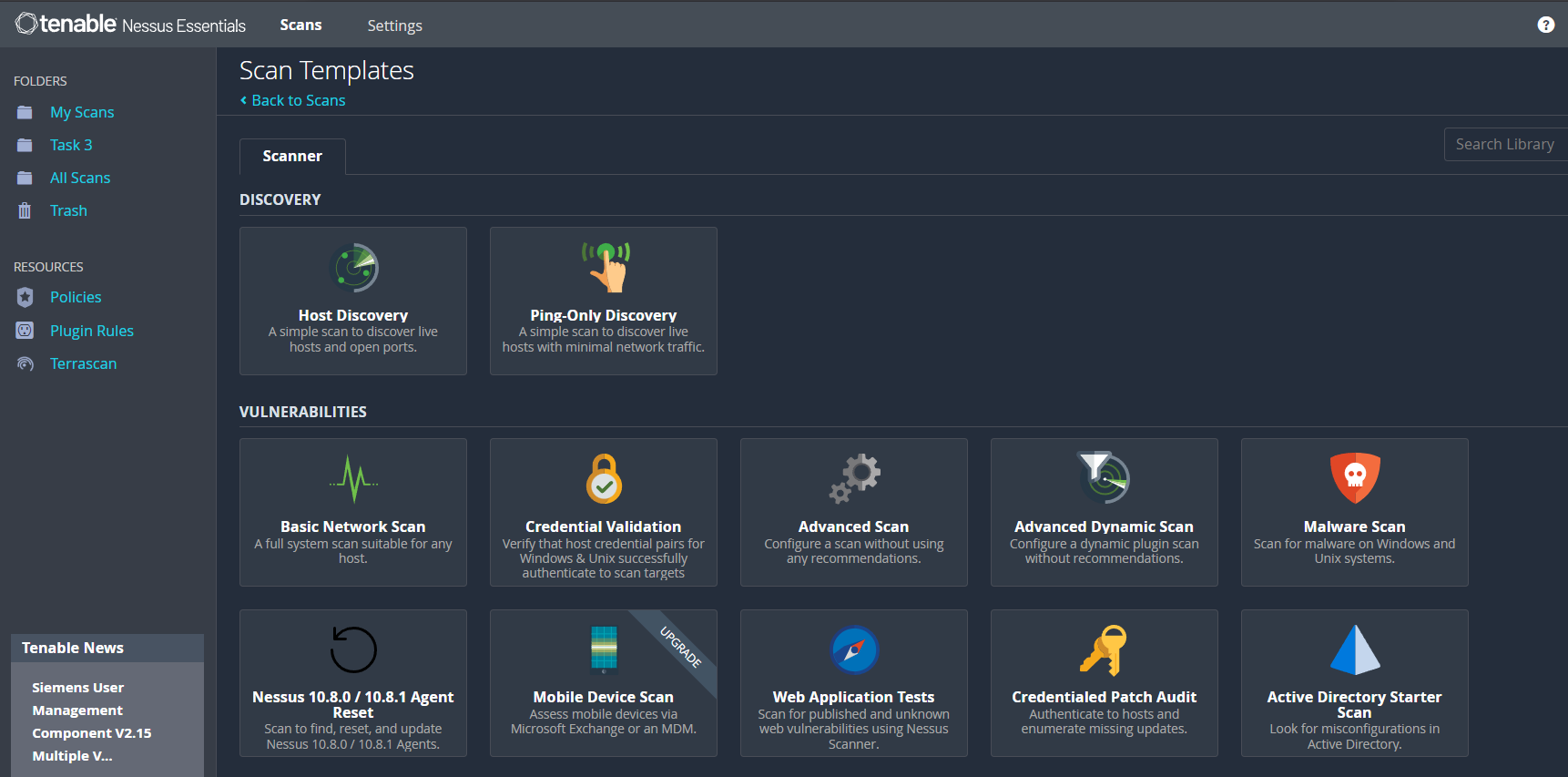


Figure - Nessus scanner templates

First, we will perform personal host scan i.e.: Windows using Advanced Scan which uses logon credentials.

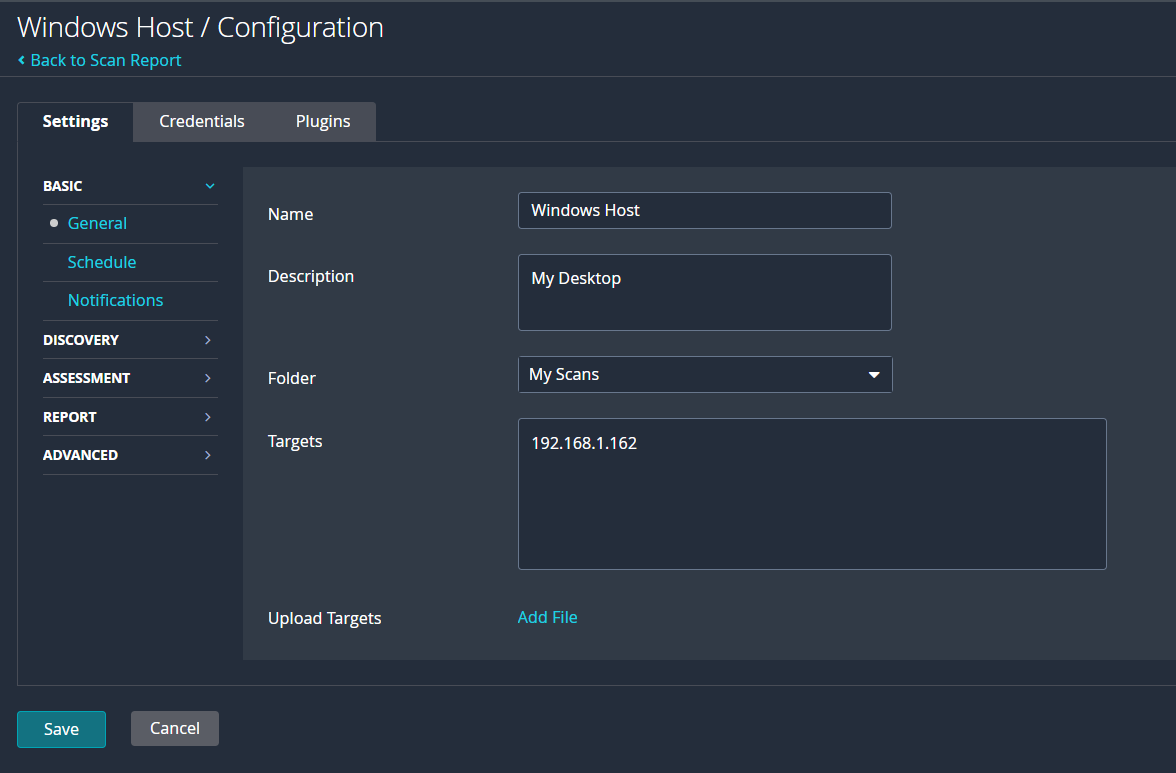


Figure - Windows host scanning config

Input name, description and target within the network. Also, credentials tab would need username and password with OS name as an input for scanning.

A screenshot of a computer

AI-generated content may be incorrect.

Figure - Found Vulnerabilities for Windows Host

A screenshot of a computer

AI-generated content may be incorrect.

Figure - High severity vulnerability for windows

As you can see figure 7 indicates vulnerability found with its severity. Figure 8 explains how SBM server can be exploited for man-in-the-middle attack and below the description, solution has been provided for this problem.

Note that found vulnerability can be manually modified for its severity as per company’s need.

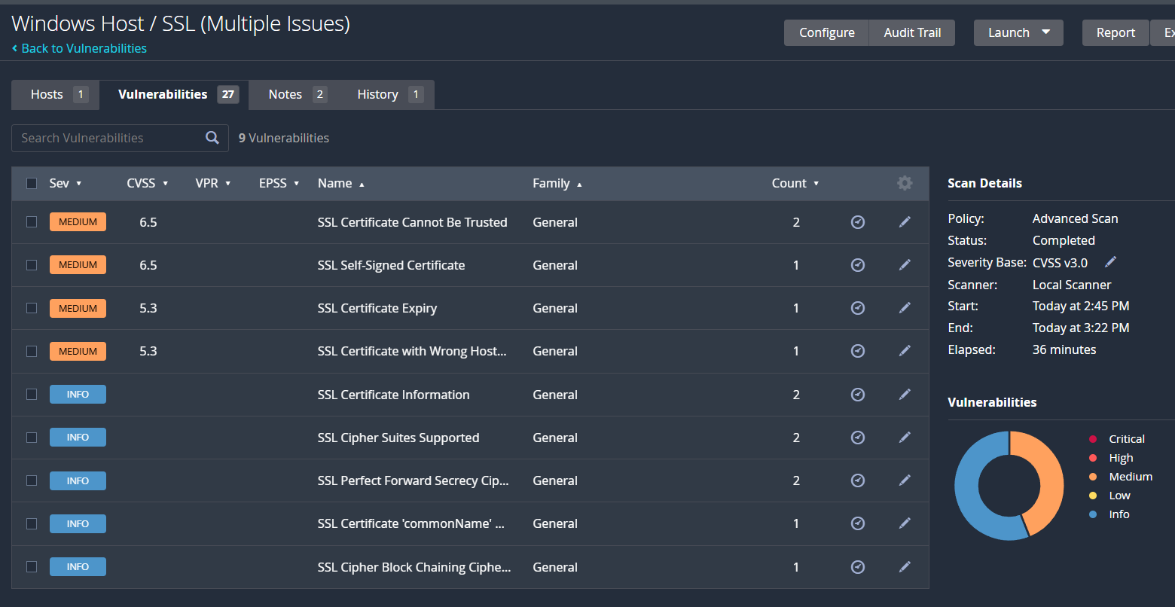


Figure - Mixed SSL Vulnerability

Next, I performed Malware scan and Network scan. Following were the results…

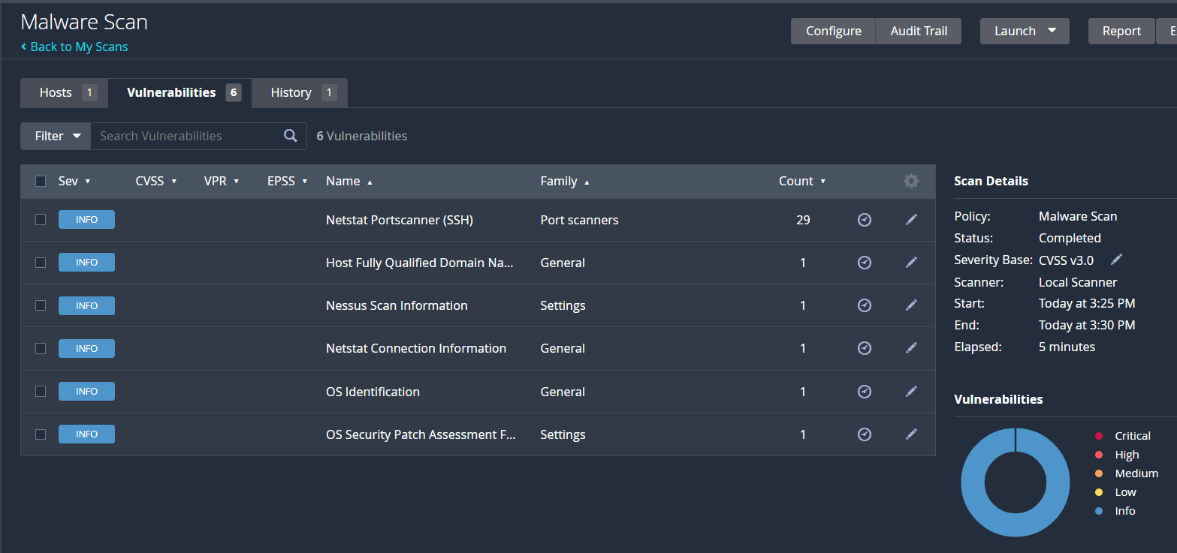


Figure - Malware Scan for open ports

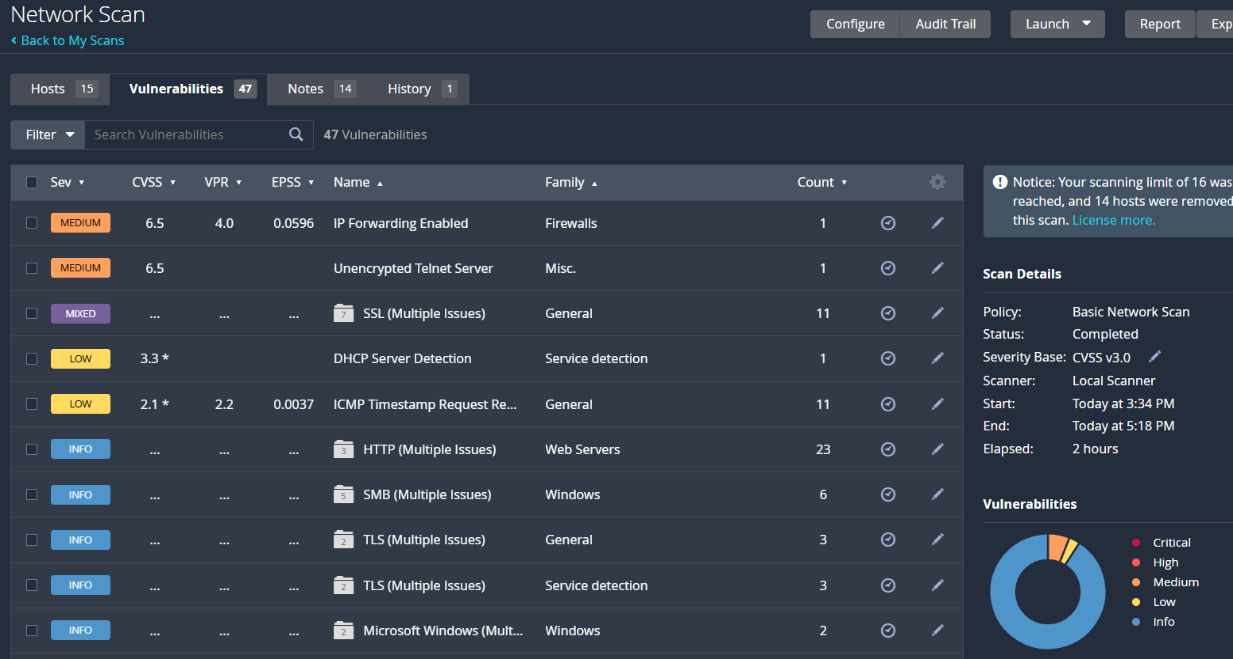


Figure - Network Scan

A screenshot of a computer

AI-generated content may be incorrect.

Figure - IP Forwarding Enabled Vulnerability

As you can see from figure 10 to 12 indicated important information about network. Network scan is as important as the host scan for identifying minor vulnerabilities as it can turn into to threat in future.

In figure 12, we found out that IP forwarding is enabled on 192.168.1.1 as in the description it says that the device is vulnerable to firewall bypass and NAC filtering via route packets unless it is a router. However, in this case it is a router so no need to worry about it.

We also found that the telnet server over the network is running over unencrypted channel. It can be solved by using SSH server. There also needs to be a proper SSL certificate for router to be trusted.

To conclude with the documentation, I understand that vulnerability assessment is crucial to identify vulnerabilities and solve them before it becomes threat. For this reason, Nessus from Tenable is accurate web-based application to solve the problem. With the usage of free version, I got so much insight into the vulnerability assessment, and it has many features for working in collaborative environments.