Nessus Vulnerability Management + Windows 10 Pro

horizontal line

# 

### Introduction

Nessus Vulnerability Scanner, developed by Tenable, Inc., is a widely used tool for identifying and managing vulnerabilities in computer systems and networks. It scans systems for security issues, misconfigurations, and compliance violations across various platforms, including operating systems, network devices, databases, and applications. Nessus uses an extensive library of regularly updated plugins to detect new vulnerabilities, performs both remote and agent-based scans, and offers detailed reports with actionable insights for remediation. Key features include vulnerability detection, compliance audits, malware detection, policy enforcement, and user-friendly interfaces. While it provides comprehensive coverage and regular updates, Nessus can produce false positives and may be resource-intensive for large networks. Despite requiring some expertise for effective use, Nessus is essential for cybersecurity professionals to identify and address security weaknesses before they are exploited.

## 

### Download Links

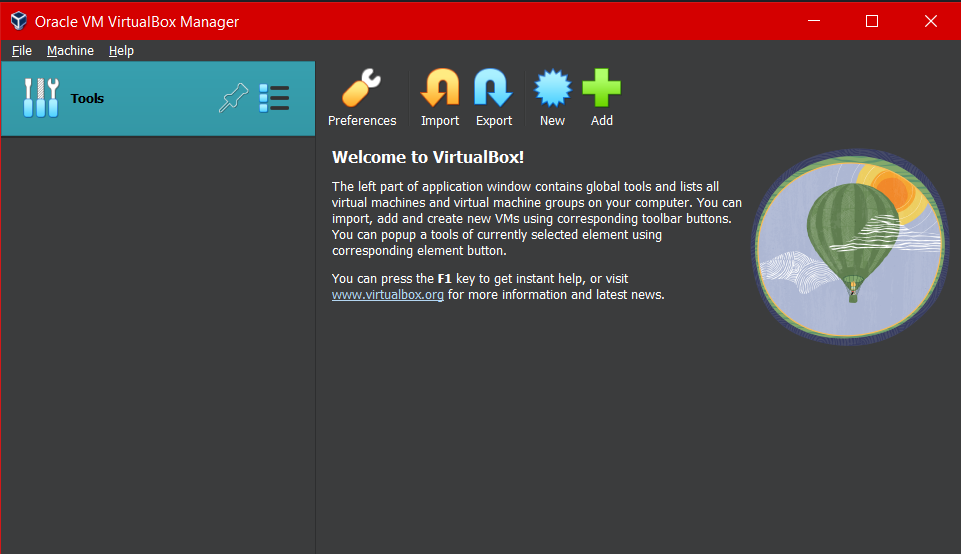
[Tenable Nessus](https://www.tenable.com/products/nessus/nessus-essentials?x-clickref=FUZZ&source=post_page-----56dd9e0265d3--------------------------------) (You will have to register to get a key, though this will be free.)

[Oracle Virtualbox](https://www.virtualbox.org/wiki/Downloads?source=post_page-----56dd9e0265d3--------------------------------)

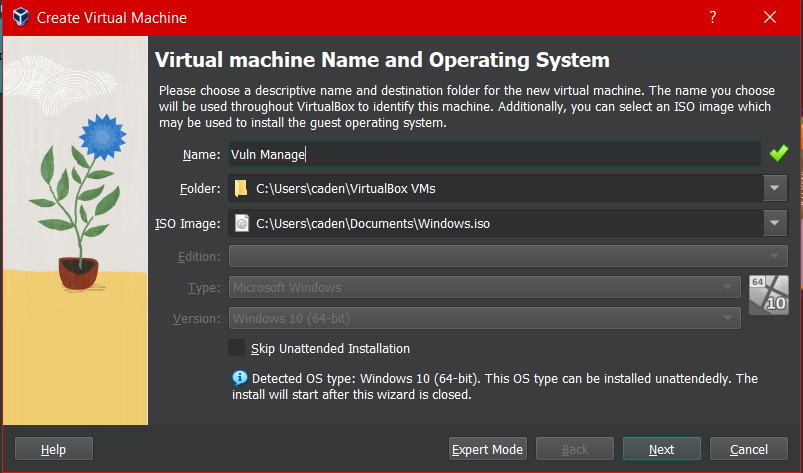
[Windows 10 ISO](https://www.microsoft.com/en-us/software-download/windows10?source=post_page-----56dd9e0265d3--------------------------------) (This will download a image creation tool, run it and use the settings to create a Windows 10 Pro ISO)

### Setting up Virtual Machine

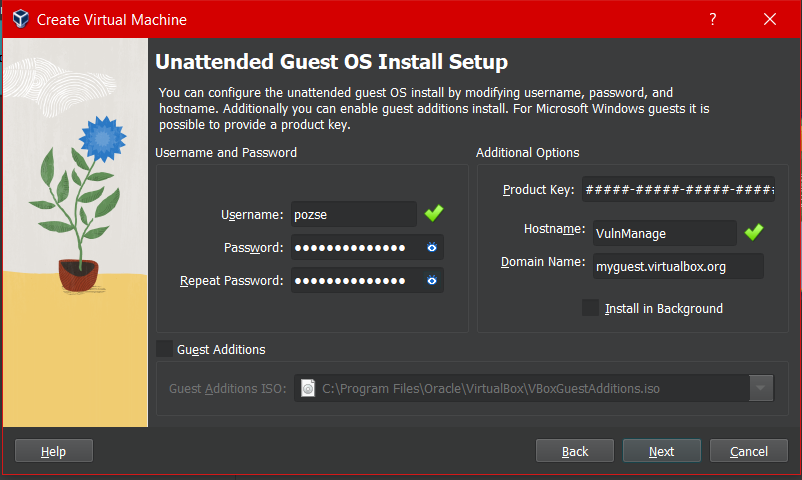
Open up virtual box, and click on ‘new’



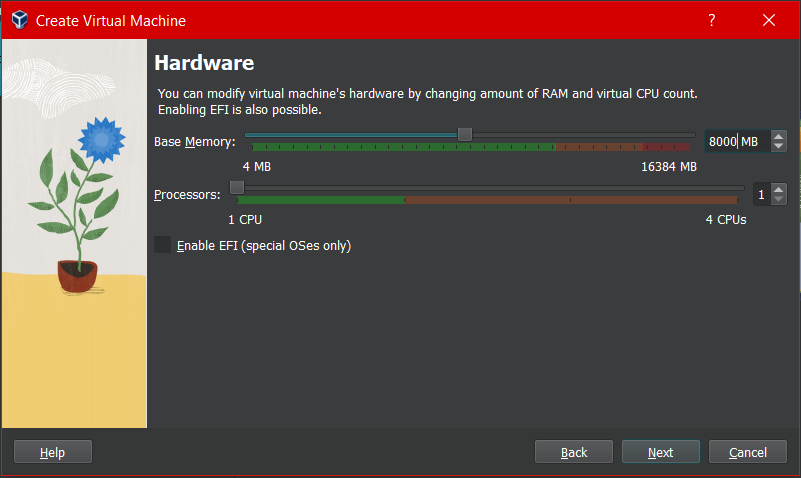
Name your machine, and select the windows 10 image you created from the earlier step as the ISO image.



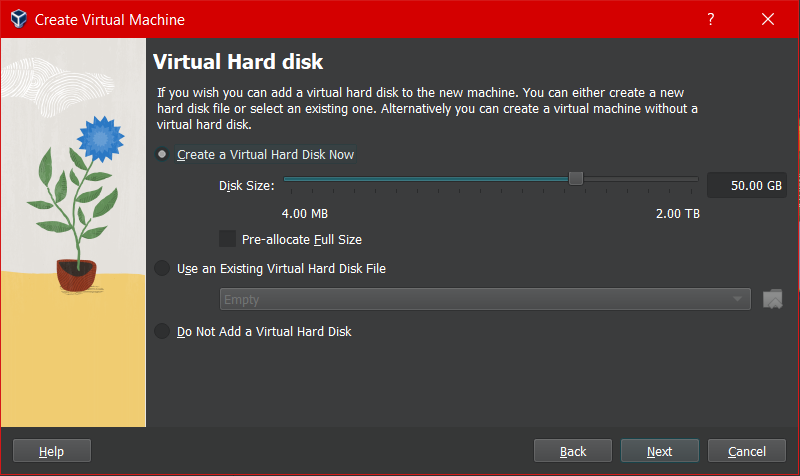
On the ‘Unattended Guest OS Install’ page, create a username and password that will be easy to remember. Nothing else on this page will need to be changed. There will be no product key.



On the following page, you can keep the default settings, or modify them to fit your computer if you have the ability. I will be using 8GB of ram.



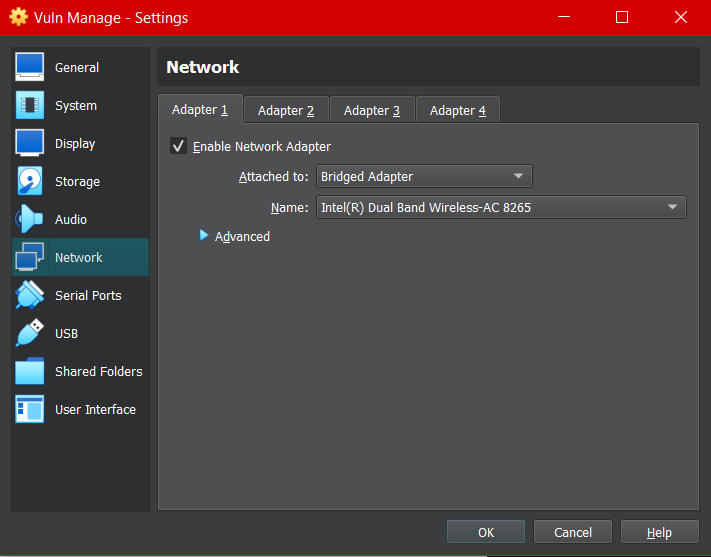
The same thing applies to the next page for storage, I will be using the default amount of 50GB.



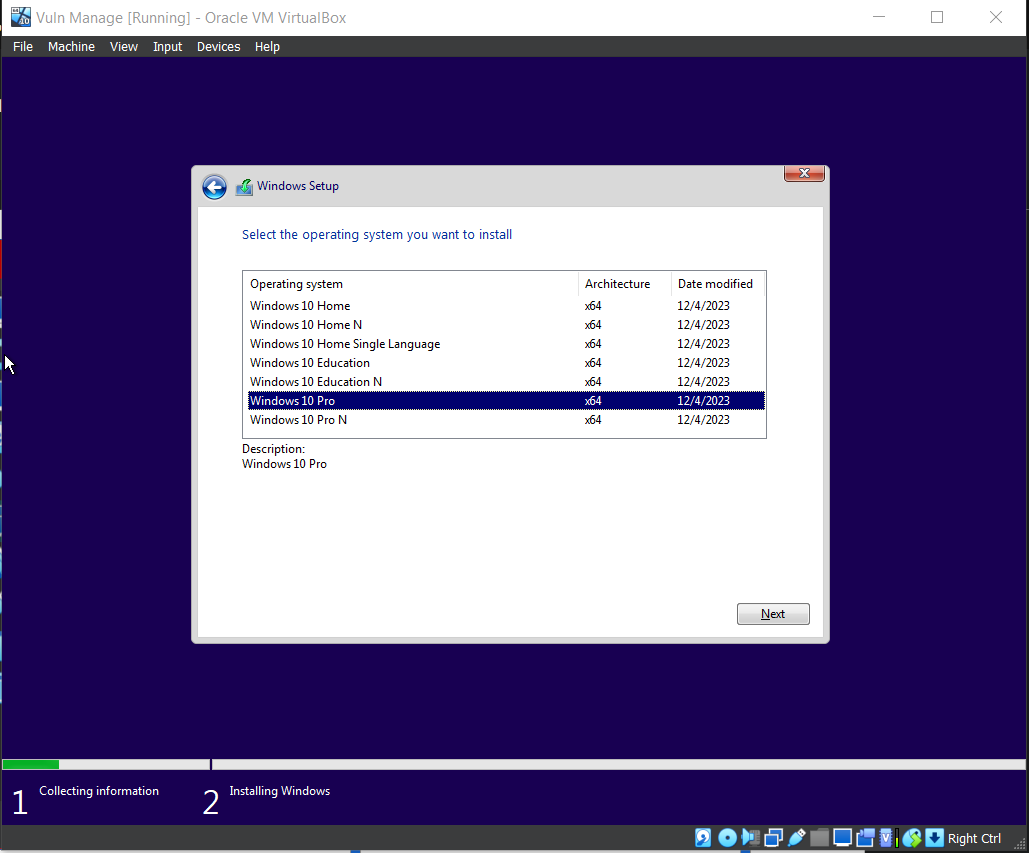
Click next, and then finish.

Right click on your new VM, and click settings.

Go to Network, and switch where it says “Attached to: NAT’ to ‘Bridged Adapter’



Start up your new VM, and install windows.

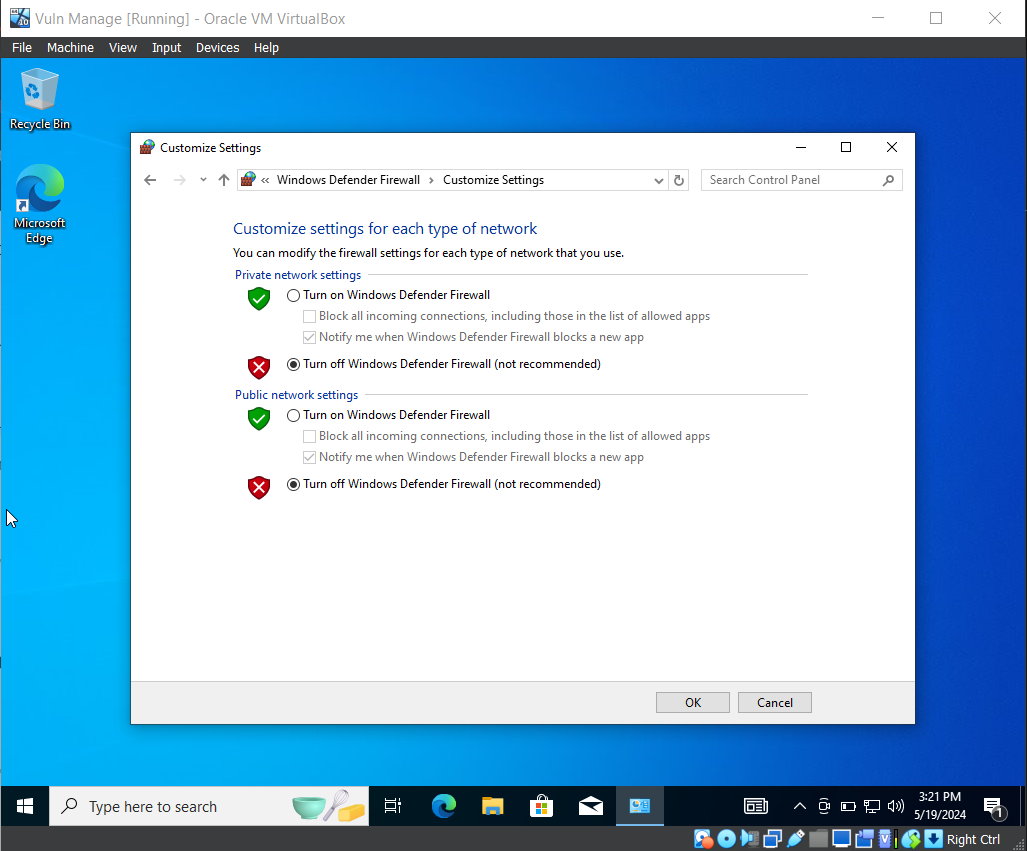


Install Windows 10 Pro, if asked for a product key, select “I do not have a product key”

When the option comes up, select “For personal use” and then select “Offline account” at the bottom left.

Create your username and password.

After starting up, open the RUN (Win + R) and type firewall.cpl.



In the firewall settings, you’ll see text that says ‘Turn Windows Firewall On or Off’. Click this and turn off both Private and Public firewall settings. (This is not best practice to do normally, but we just want to get hands on experience using Nessus)

### 

### Nessus Essentials

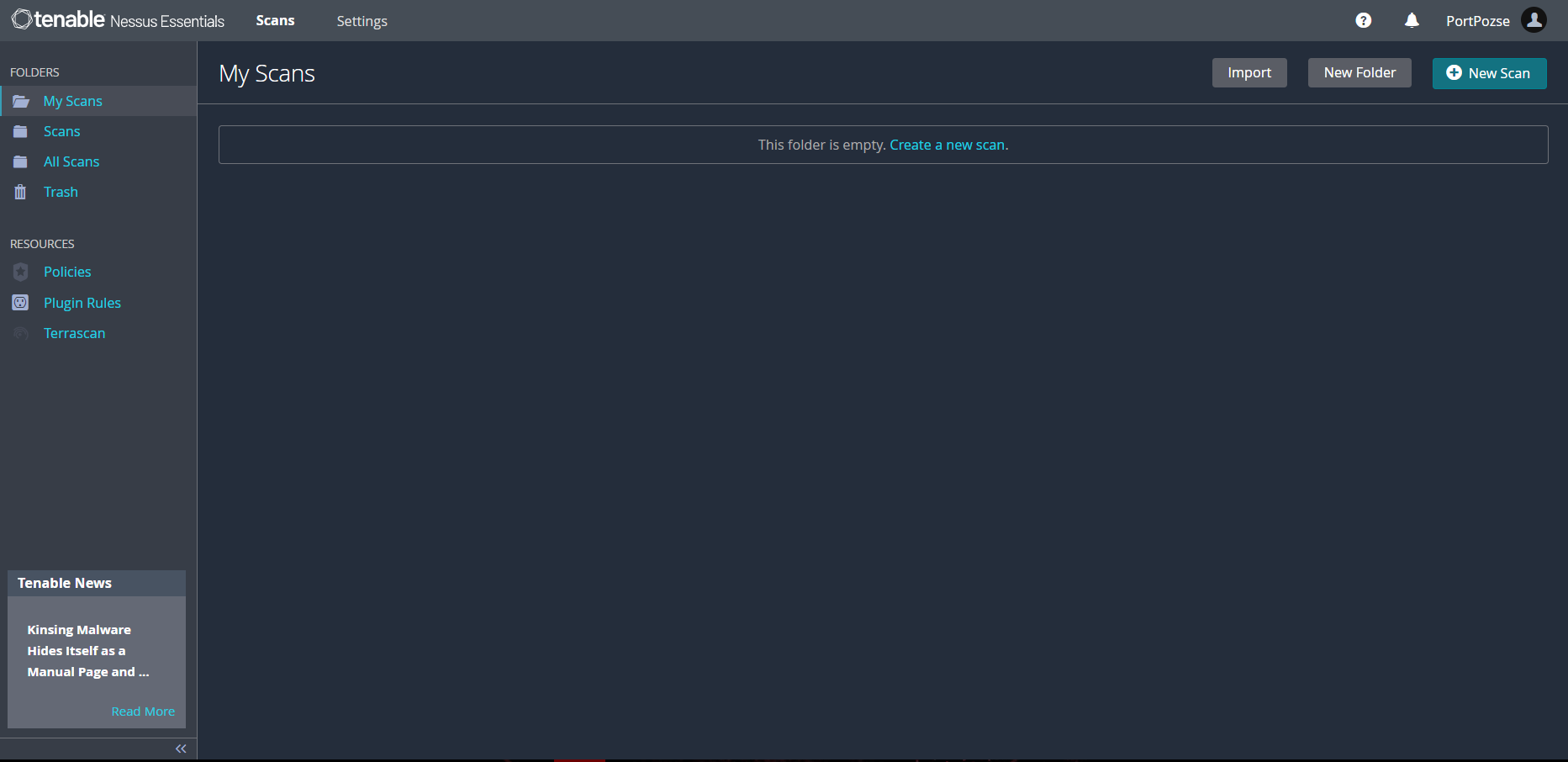
Follow the link and register an account. You will receive a ‘key’ and an installer.

Install Nessus, it will give you a local URL to access the app (save this URL).

Then next through the installation steps, ensuring that you select Nessus Essentials. Wait for it to install and you should be good to go.

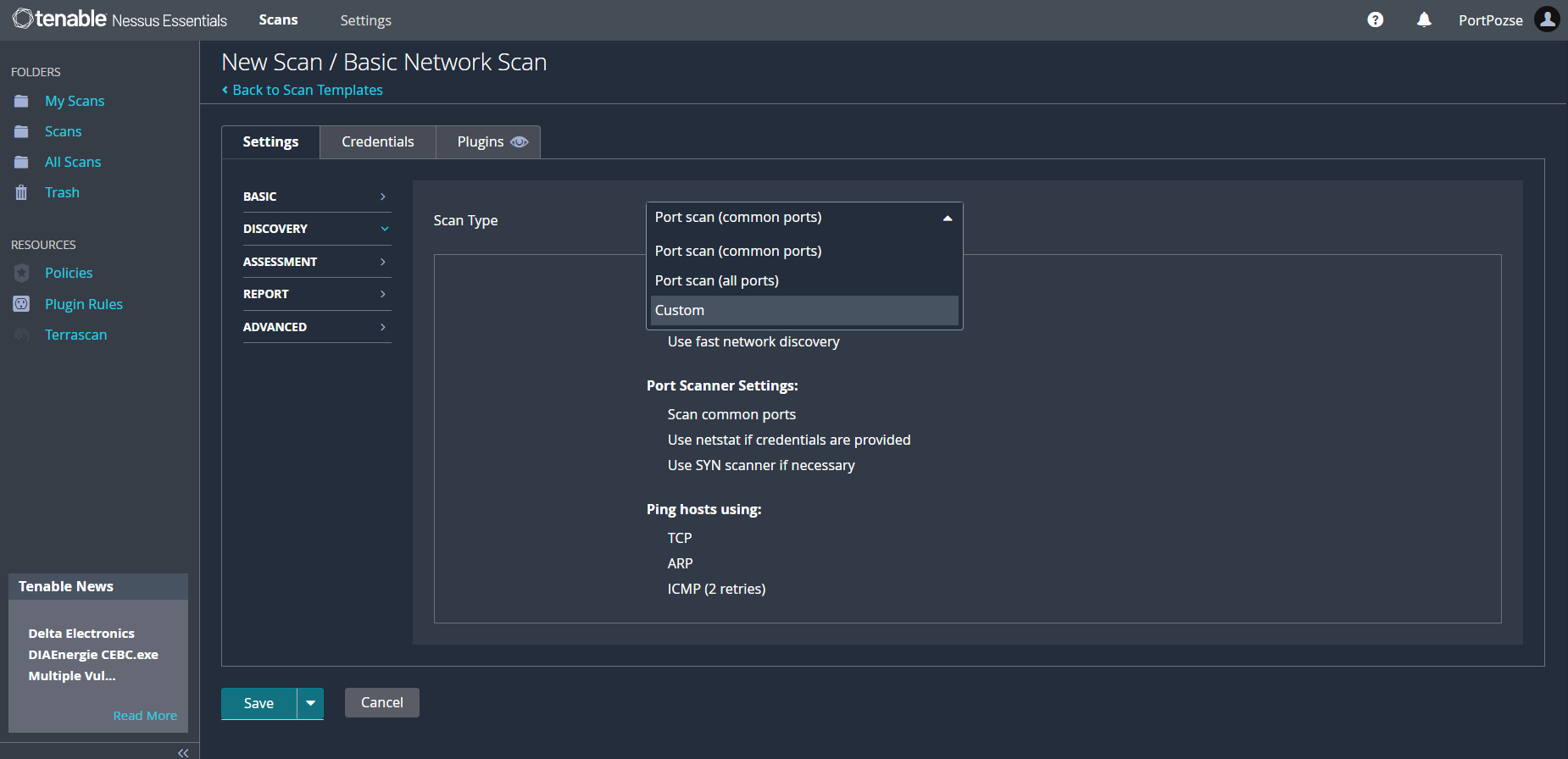
### Scanning your VM

We have turned off the firewall in our VM so that nessus can communicate with our virtual machine. If you know how, you can open up the needed ports instead, to make this project faster, we will just turn it off as a whole.



In Nessus, click New Scan in the top right hand corner and select ‘Basic Network Scan’

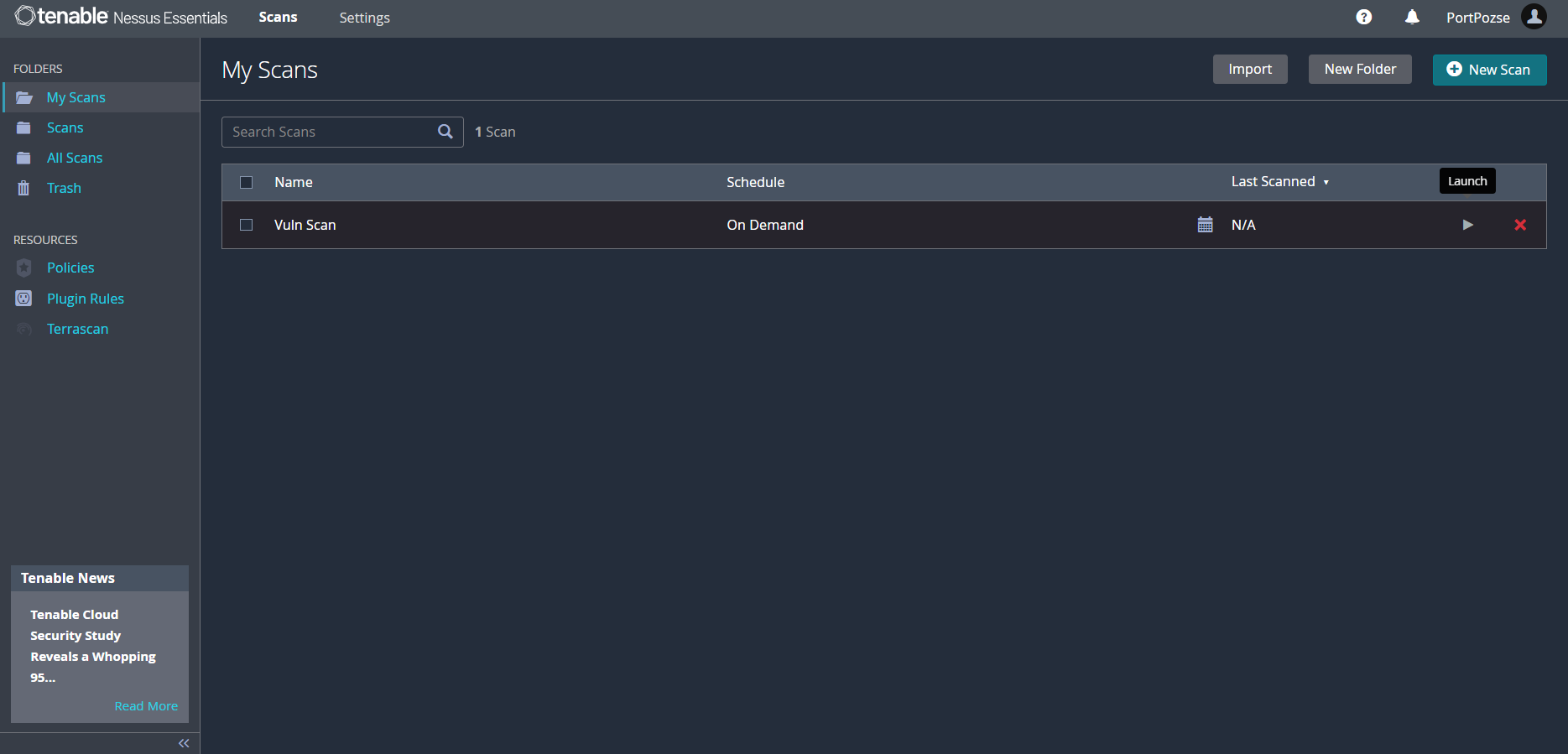
In your virtual machine, open Command Prompt and type ipconfig, enter in your ipv4 address into nessus under ‘Targets’



Next, you will want to select ‘Discovery’ on the left pane, and change it to custom.

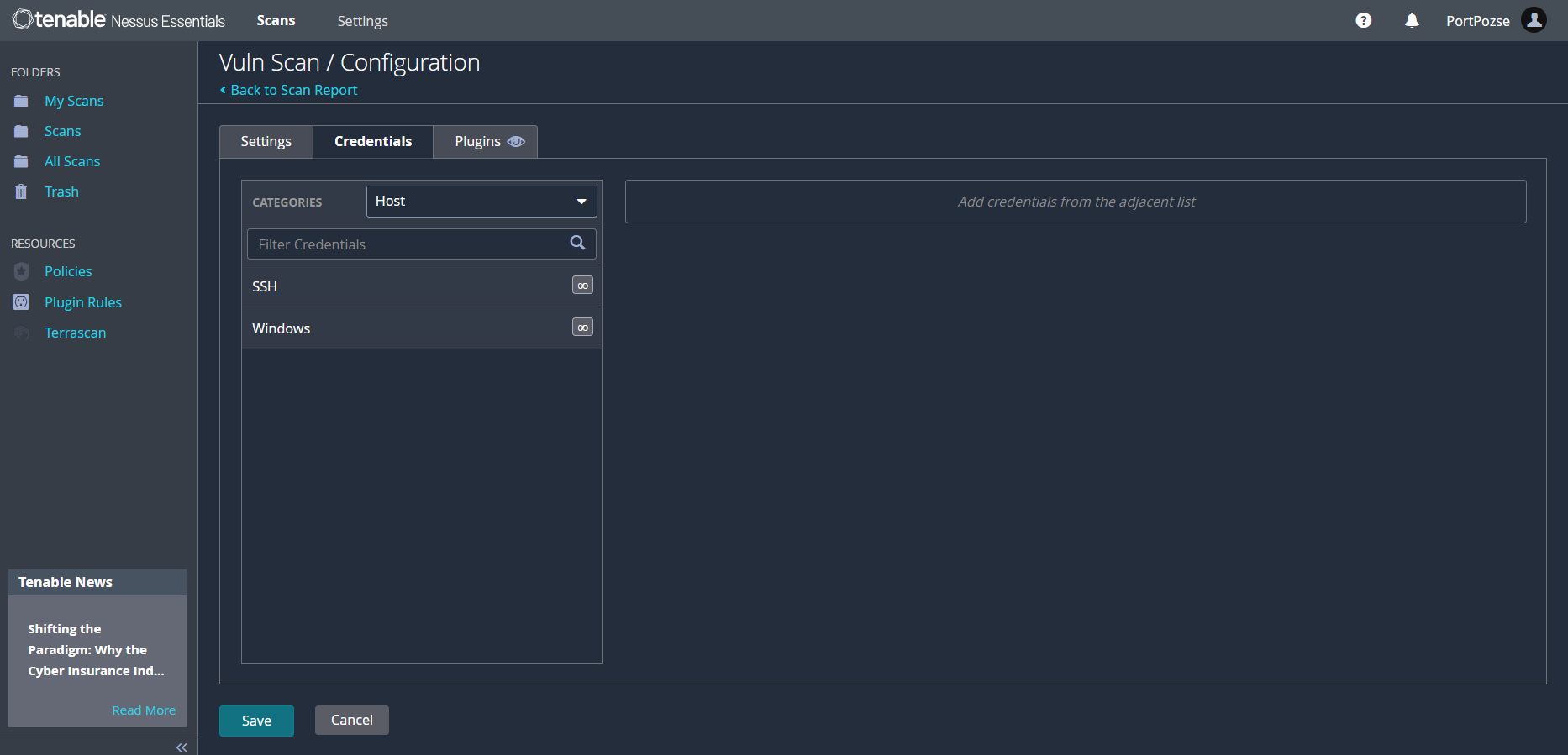
Select ‘Host Discovery’ and turn off ‘ping the remote host’

Click save



Under your Scans, select the play button on the right to launch.

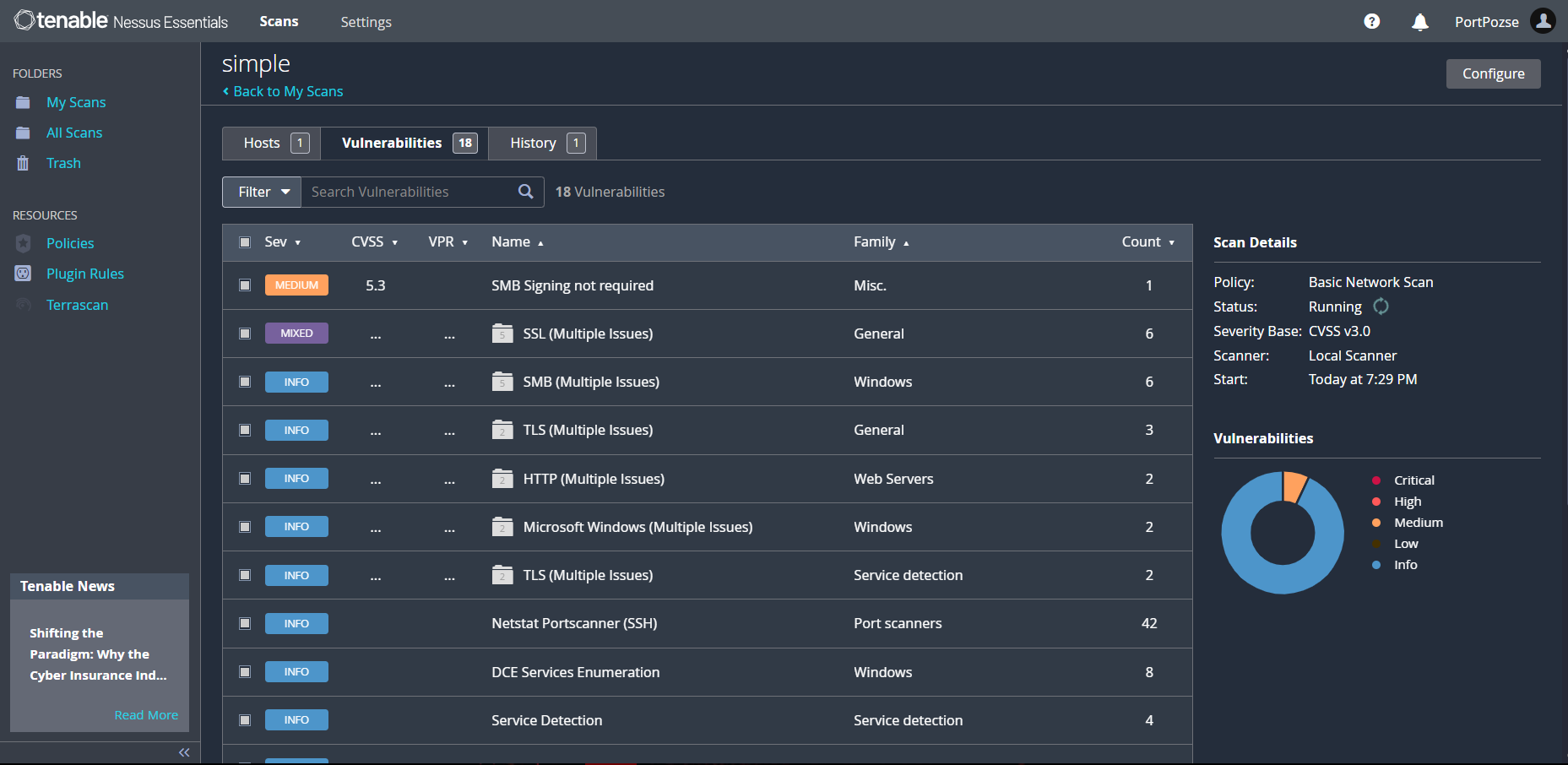
The initial scan takes about a minute, showing real-time results. You can click through to read about each vulnerability and its remediation. They are color-coded and ranked by severity, with a visualization indicating your machine's security level.



To get a more detailed scan, reconfigure the settings. Return to the main screen, click the box next to our scan, and select "More" in the top right, then click "Configure." Next, click the "Credentials" tab beside "Settings" to perform a credentialed scan.

On the left pane, select ‘Windows’ and ‘password’ as the authentication method. Enter in your username and password.

Click Save and re-run your scan.



As you can see, this lists a lot more vulnerabilities.

To get more comfortable with this, I would recommend going through the vulnerabilities that it shows, and fixing them using the recommended steps.

Along with this, you are able to scan a range of ip’s, or even multiple ones.