Lab - Scanning for Vulnerabilities Using Nessus

This lab picks up where our previous lab left off. If you have shut down Nessus or you have stopped the Nessus service, you will need to go back into docker using the Kali terminal and reattach the container running the Nessus image. The steps for reattaching a container inside of docker are available in the previous lab.

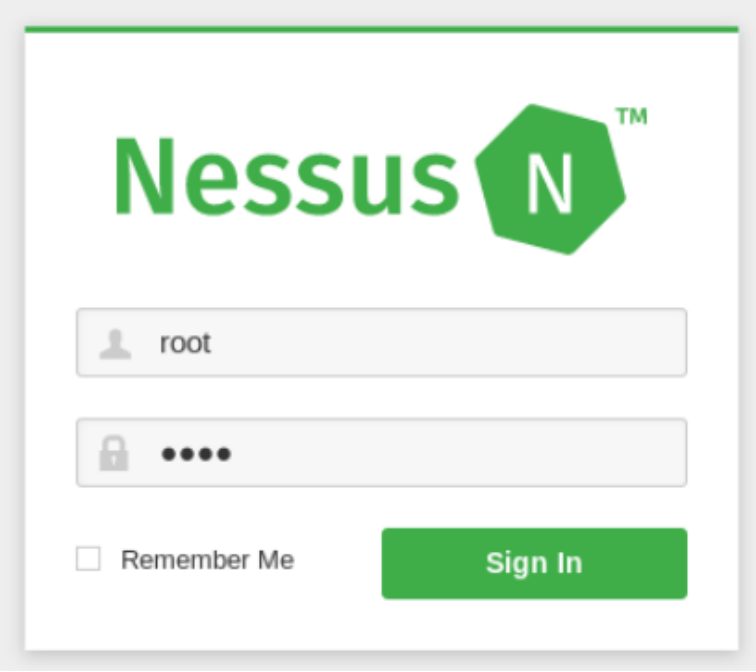
Since I want to scan my entire network, I'm going to need to configure my network adapter for Kali to use bridged networking. This will allow Callie to see my internal network whether it's my home or it's my business it will pick up the DHCP information from whatever DHCP server is running on my home or my business network and configure its adapter with an IP address from that network range.

Once we have assured ourselves that Nessus is up and running inside of docker, we can open our Firefox browser inside of Kali to access the Nessus web interface.

To do this, we direct our browser to look locally at port 8834 where will find the Nessus service running.

```
https://localhost:8834
```

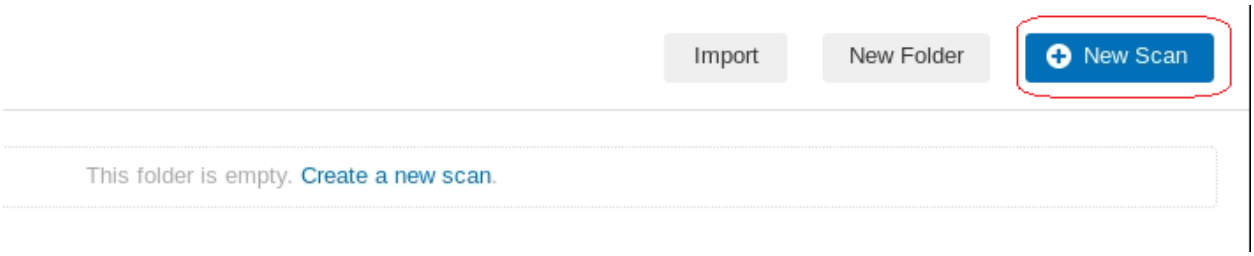
Once Nessus has completed initializing its plug-ins, you will be presented with the logon window. The plug-in initialization can take 5 to 7 minutes, sometimes longer to complete but do interrupt this process.



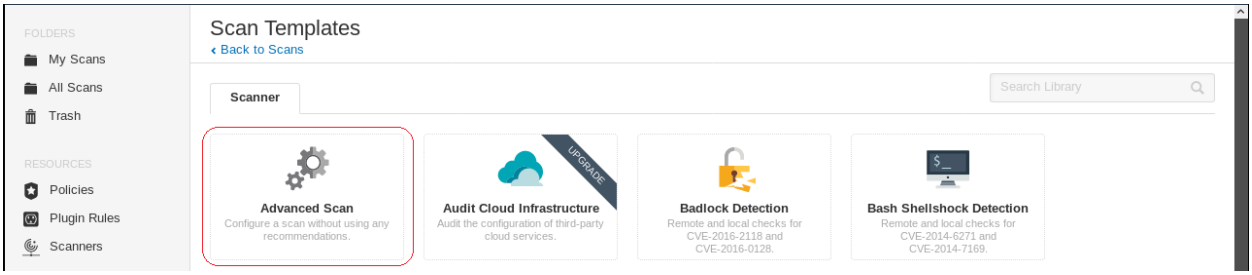
Once you type in your username and your password, click the sign in button.

The first page you will be introduced to is the, My Scans page

Click on the New Scan Button.



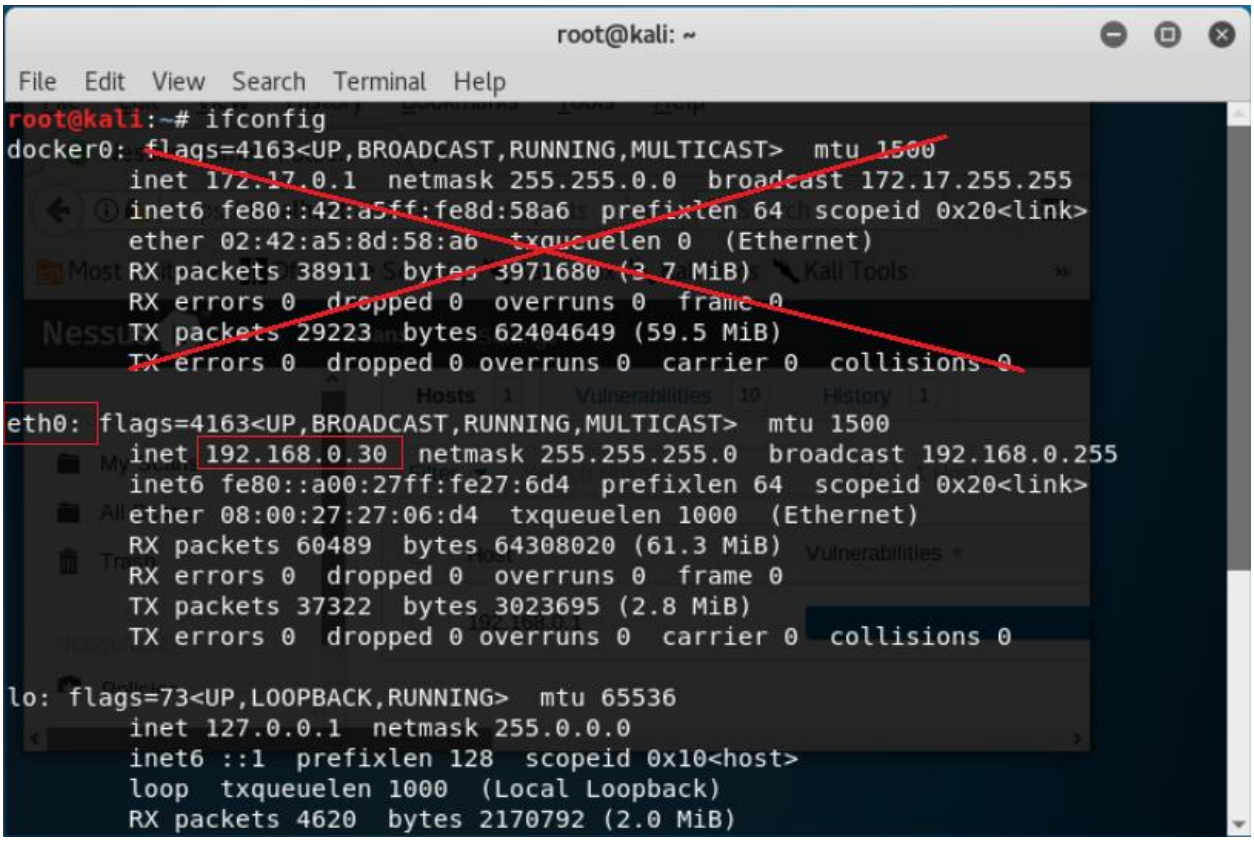
Inside the Scan Template page, click on the tile that reads Advanced Scan. This takes you to the Scan Library page where you can set up your scan target(s). Click on **Advanced Scan.**



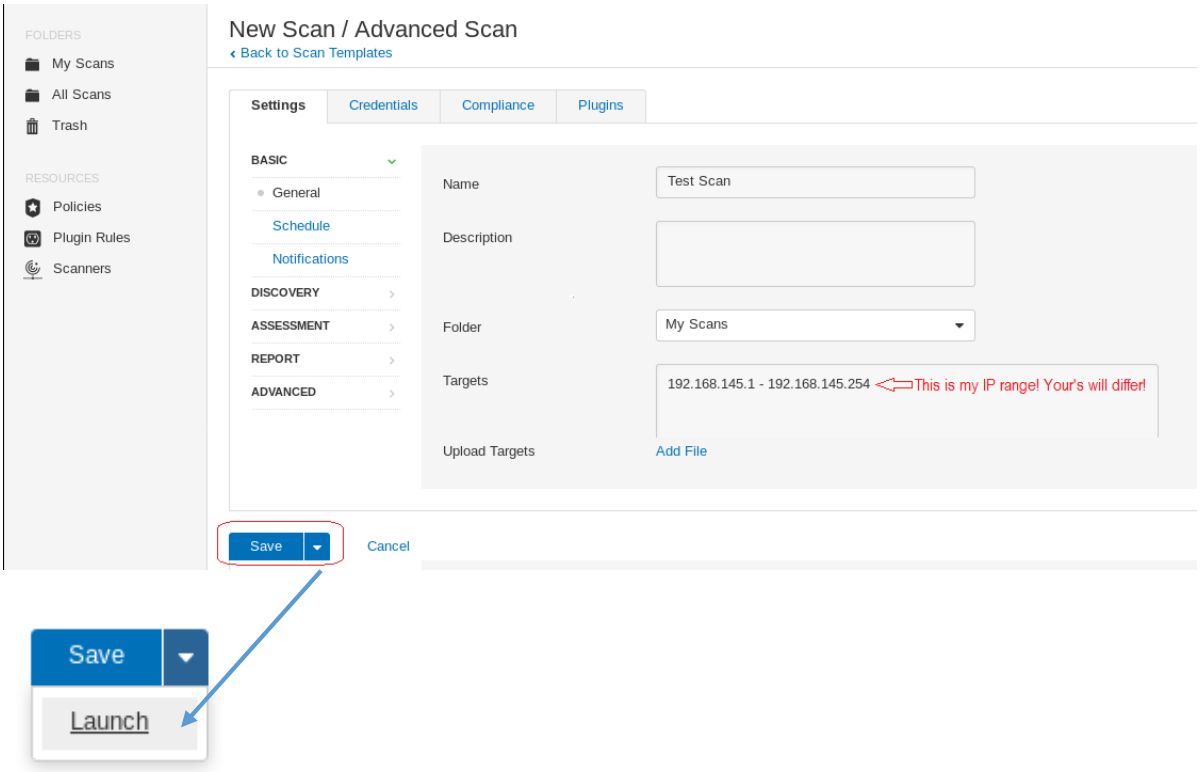
Name the scan whatever you want, insert your IP range such as 192.168.145.1-192.168.145.254

Warning!!! The following IP addresses are examples! Your actual IP range may differ. To find the network range of your network or the actual IP of your machine, open up a terminal session and type IFCONFIG. Find your working network adapter and look at the results. Use the instructions that follow to figure out what IP within your range to scan.

Your docker program will have an IP address of its own but that's not the IP address were interested in. You must use the IP address range for your eth0 adapter

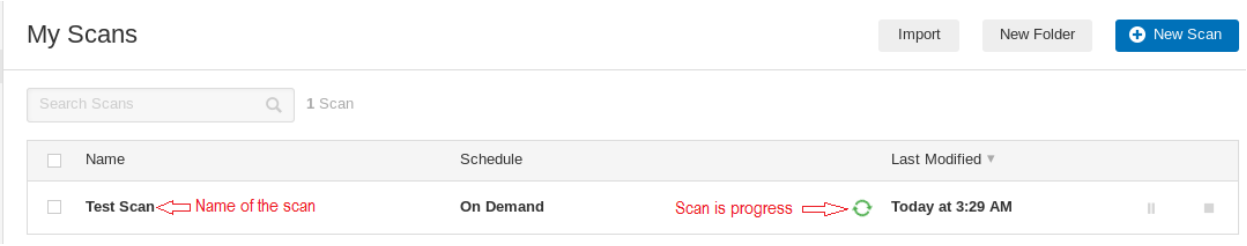


When done, click on Save at the bottom of the screen, pull down the window and select launch.



As for Scan Target you can either a single host IP address, 192.168.145.1, or multiple addresses, 192.168.145.1,192.168.145.4,192.168.145.22, an address range, 192.168.145.1-10, or an entire subnet, 192.168.145.0/24.

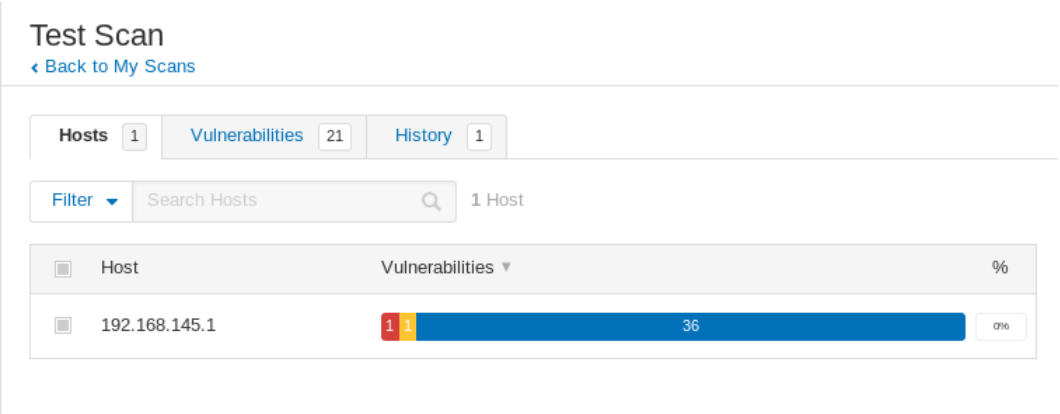
This opens up the My Scans page. As long as the green arrows are circling, the scan is in progress.



Warning!!! When scanning highly vulnerable targets, Nessus may crash it. Best practices would be to run the scan after hours and ensure the machine has a current backup.

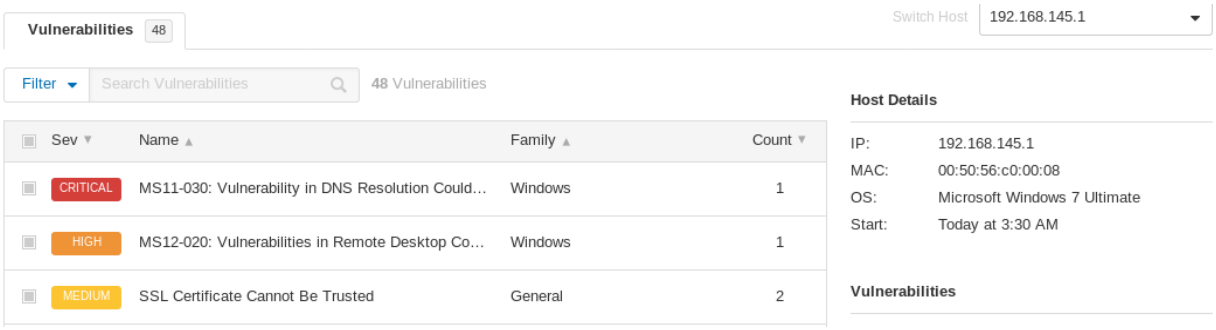
An example would be ATMs running Windows XP. Nessus will cause them to crash. Only scan targets that you own or targets that you have secured the permission to scan.

Notice the rotating green turning arrow…..your scan is in progress….click on the rotating arrow to watch the scan results to show up in real time.

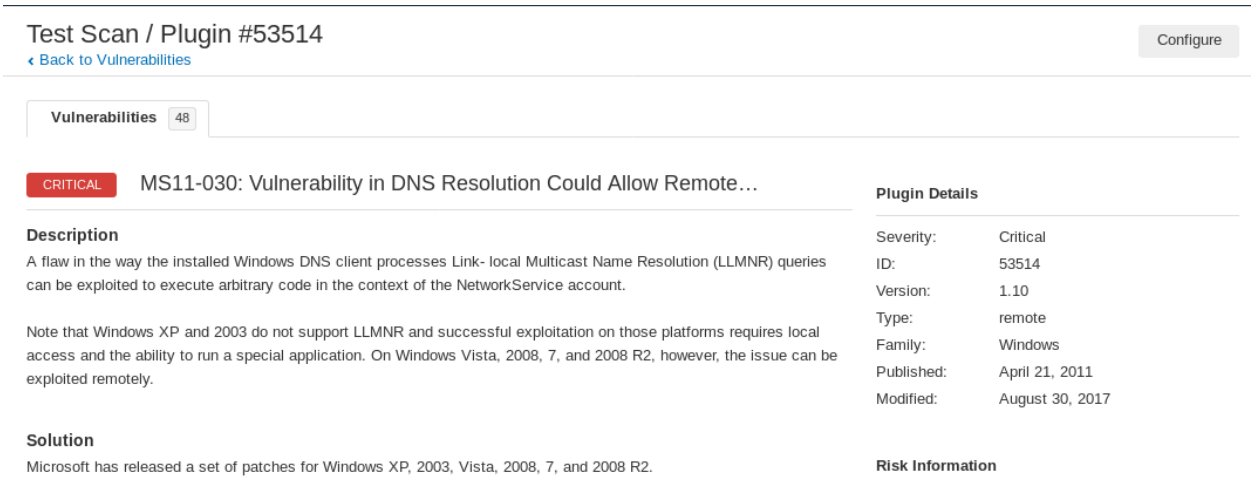


From left to right…The IP of the host, the number of moderate vulnerabilities, the number if low vulnerabilities and finally, the percentage of the scan completed.

12. Once the scan completes, you'll be shown the scan results. Click the vulnerabilities for each host.



Click on any vulnerability listed, and you will be given a detail explanation of what the vulnerability is.



Warning!!! Nessus will often list Windows-specific vulnerabilities by their Security Bulletin number, such as M11-030. This number often corresponds to a known vulnerability within Metasploit allowing you to transition from vulnerability analysis to exploitation execution easily.

Summary

There are plenty of different vulnerability scanners available on the market, but Nessus is considered the industry standard and it is the one that most pen testers will use when conducting their initial vulnerability scan of any network. There's nothing wrong with following up your Nessus scan with a secondary scan using open bass or core impact or some other third-party scanner that will give you a second opinion.

You can punch in the information from your scan results into Searchsploit and other vulnerability databases to see if there is a known attack vector. Treat your Nessus scan results the same way you treat any scan results. Often you will find that Nessus will give you the actual exploit that you can use or enough information that you can take the CVE or the Microsoft security bulletin number and search through the vulnerability database or the Internet to find out best to confirm if the vulnerability exists. You can end up with some exciting scan results only to find when you go to exploit the machine the vulnerability was a false positive. Again, this is why we like to get a second opinion using an additional vulnerability scan.

End of the Lab!