

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 Kali to see my internal network, whether it's my home or my business. It will pick up the DHCP information from whatever DHCP server runs on my home or my business network and configure its adapter with an IP address from that network range.

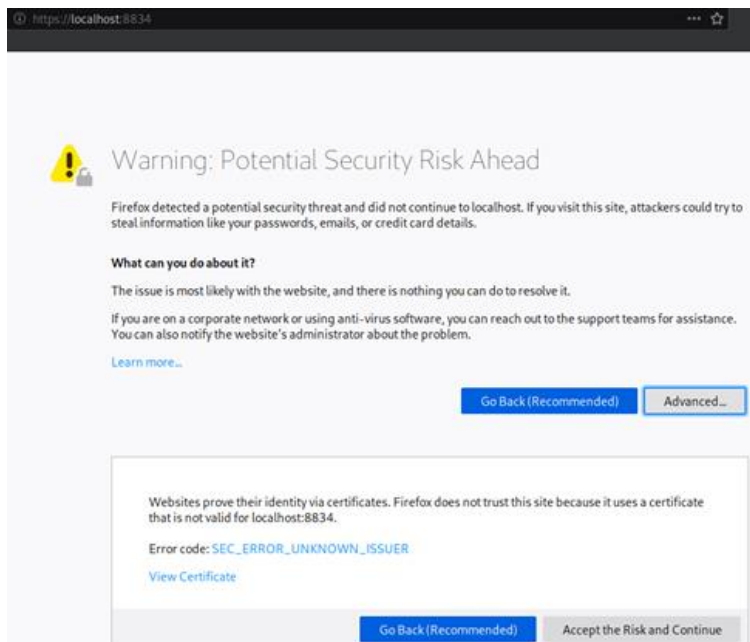
Once we have assured ourselves that Nessus is up and running inside Docker, we can open our Firefox browser inside Kali to access the Nessus web interface.

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

<https://localhost:8834>

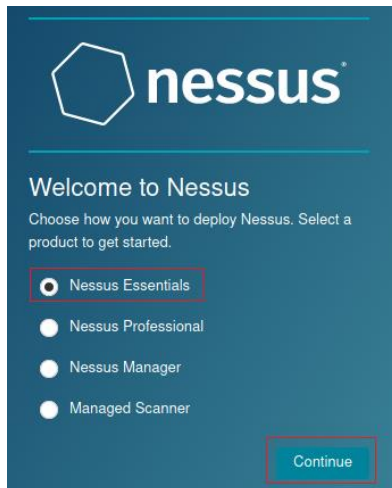
Potential Security Risk Ahead

The first time you launch NESSUS using Firefox, you will receive the following error. Click on the Advanced button.

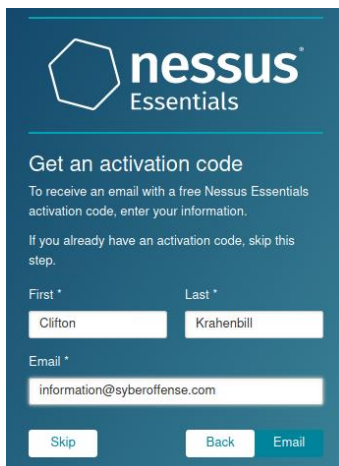


The error has to do with a self-signed certificate. Click on the Accept the Risk and Continur button.

You are presented with the NESSUS main page. Accept the default to deploy NESSUS using NESSUS Essential. NESSUS Essentials was previously known as NESSUS Home Version. Click Continue.



On the next page, you will need to register with Tenable to receive an activation code. Make sure you use a valid address. A school or business address works best. Press Email. Check your email for the activation code.



Welcome to Nessus Essentials

Welcome to Nessus Essentials and congratulations on taking action to secure your network! We offer the latest plugins for vulnerability scanning today, helping you identify more vulnerabilities and keep your network protected.

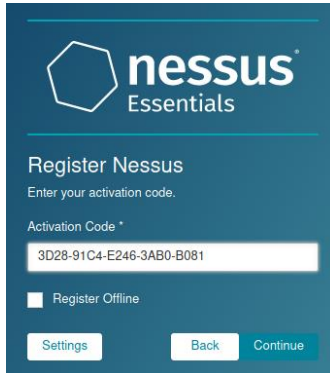
If you're looking for more advanced capabilities, such as live results and configuration checks – as well as the ability to scan unlimited IPs, check out Nessus Professional. To learn more view the [Nessus Professional datasheet](#).

Activating Your Nessus Essentials License

Your activation code for Nessus Essentials is:

3D28-91C4-E246-3AB0-B081

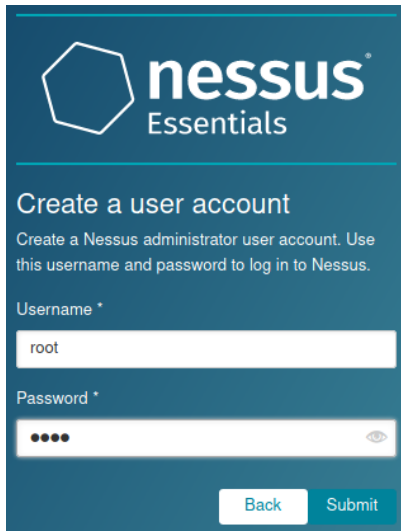
Copy and paste the activation code into the text box. Press Continue.



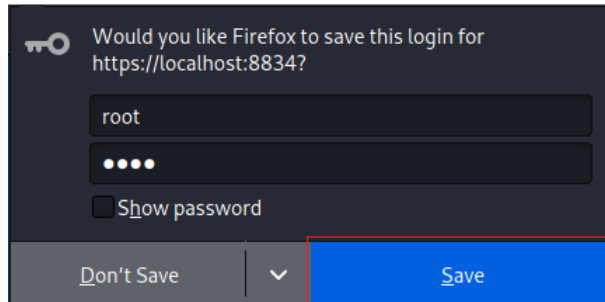
The image shows the 'Register Nessus' screen for Nessus Essentials. It features the Nessus logo at the top. Below it, the text 'Register Nessus' is followed by 'Enter your activation code.' There is a text input field for the 'Activation Code' containing the value '3D28-91C4-E246-3AB0-B081'. Below the input field is a checkbox labeled 'Register Offline'. At the bottom, there are three buttons: 'Settings', 'Back', and 'Continue'.

You next need to create a user account. I used **root** for my username and **toor** for my password. Same username and password I use to login to Kali. Be smart, not clever. If you lose or forget your NESSUS username and password, it can be replaced but try and be smart about it. Click Submit.

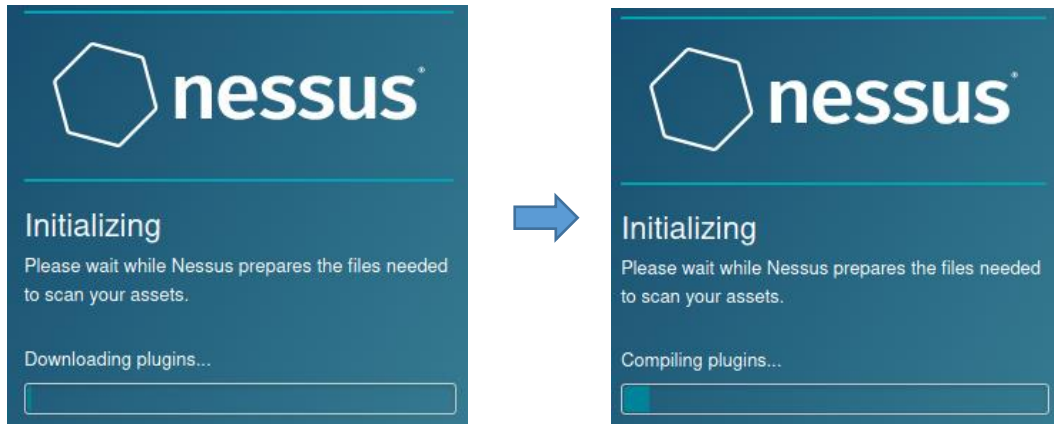
When prompted to save your NESSUS login information, click on the Save button if you want Firefox to log you on automatically.



The image shows the 'Create a user account' screen for Nessus Essentials. It features the Nessus logo at the top. Below it, the text 'Create a user account' is followed by 'Create a Nessus administrator user account. Use this username and password to log in to Nessus.' There are two text input fields: 'Username' with the value 'root' and 'Password' with masked characters. At the bottom, there are two buttons: 'Back' and 'Submit'.

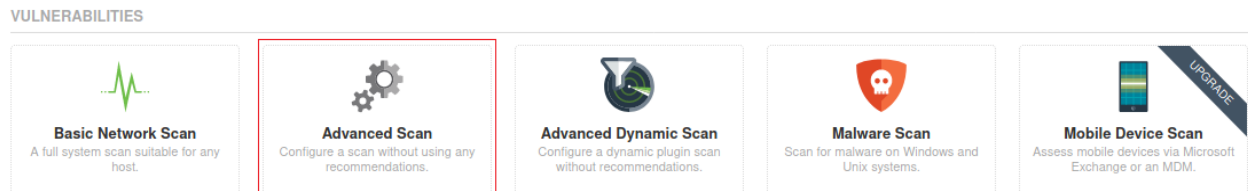


The image shows a Firefox login save prompt. It asks 'Would you like Firefox to save this login for https://localhost:8834?'. There are two input fields: the first contains 'root' and the second contains masked characters. Below the input fields is a checkbox labeled 'Show password'. At the bottom, there are two buttons: 'Don't Save' and 'Save'.

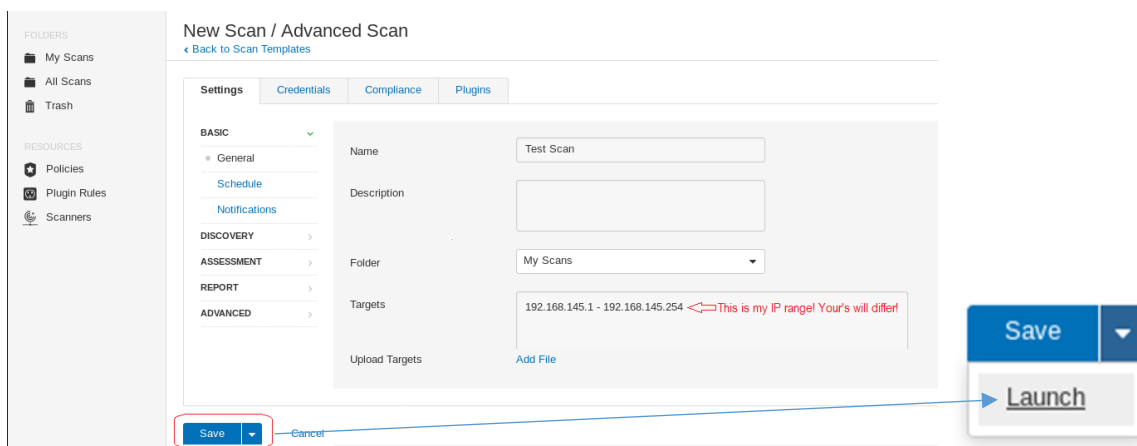


The plug-in initialization can take 5 to 45 minutes, sometimes longer to complete, **but do not interrupt this process!**

The first page you will be introduced to is the Scans Templates. 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



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

Warning!!! The following IP addresses are examples! Your actual IP range may differ. To find the network range of your network or your machine's existing IP, 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 we are interested in. You must use the IP address range for your eth0 adapter

```

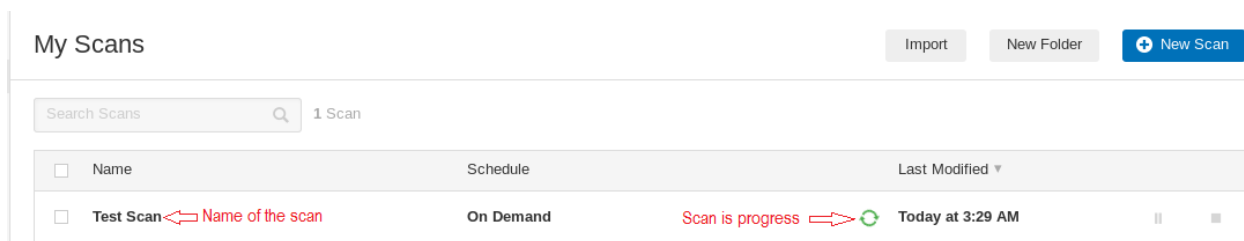
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    inet6 fe80::42:a5ff:fe8d:58a6 prefixlen 64 scopeid 0x20<link>
    ether 02:42:a5:8d:58:a6 txqueuelen 0 (Ethernet)
    RX packets 38911 bytes 3971680 (3.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 29223 bytes 62404649 (59.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.30 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fe27:6d4 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:27:06:d4 txqueuelen 1000 (Ethernet)
    RX packets 60489 bytes 64308020 (61.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 37322 bytes 3023695 (2.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4620 bytes 2170792 (2.0 MiB)
  
```

Scan Target 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.

Once the scan completes, you can click on My Scans in the left window pane to see the scan process in the right windowpane. 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 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.

Test Scan

[← Back to My Scans](#)

Hosts 1
Vulnerabilities 21
History 1

Filter ▾ Search Hosts 1 Host

Host	Vulnerabilities ▾	%
192.168.145.1	1 1	36 0%

From left to right...The IP of the host, the number of moderate vulnerabilities, the number of 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.

Vulnerabilities 48
Switch Host 192.168.145.1 ▾

Filter ▾ Search Vulnerabilities 48 Vulnerabilities

Sev ▾	Name ▲	Family ▲	Count ▾
CRITICAL	MS11-030: Vulnerability in DNS Resolution Could...	Windows	1
HIGH	MS12-020: Vulnerabilities in Remote Desktop Co...	Windows	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	2

Host Details

IP: 192.168.145.1

MAC: 00:50:56:c0:00:08

OS: Microsoft Windows 7 Ultimate

Start: Today at 3:30 AM

Vulnerabilities

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

Vulnerabilities 48

CRITICAL MS11-030: Vulnerability in DNS Resolution Could Allow Remote...**Description**

A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.

Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Plugin Details

Severity:	Critical
ID:	53514
Version:	1.10
Type:	remote
Family:	Windows
Published:	April 21, 2011
Modified:	August 30, 2017

Risk Information

Warning!!! Nessus will often list Windows-specific vulnerabilities by their Security Bulletin number, such as M11-030. This number will often correspond 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. Still, 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 second scan using OpenVAS, 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. You will often find that Nessus will give you the actual exploit that you can use or enough information to 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 that the vulnerability was a false positive when you go to exploit the machine. Again, this is why we like to get a second opinion using an additional vulnerability scan.

Troubleshooting NESSUS

If your NESSUS install becomes corrupted or no longer working as it should, remove the NESSUS container from Docker and create a new one. Use the **docker ps -a** command to find the name of your NESSUS container.

Remove Nessus as a Docker Container

When you remove Nessus running as a Docker container, no data is retained.

To remove Nessus as a docker container:

1. In your terminal, stop the container from running using the `docker stop` command.

```
$ docker stop <container name>
```

2. Remove your container using the `docker rm` command.

```
$ docker rm <container name>
```

Create a new NESSUS container.

End of the Lab!