Lab - Scanning for Vulnerabilities Using OpenVAS

Overview

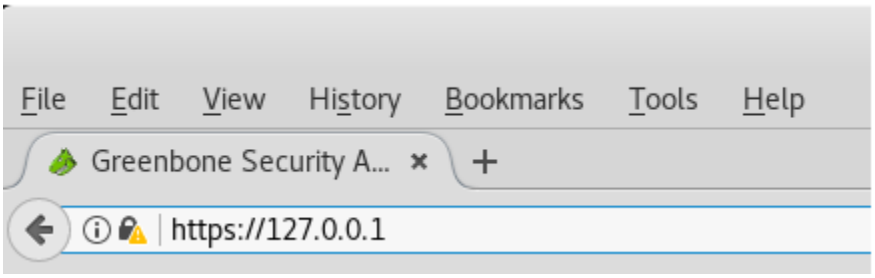
In our previous lab, students installed OpenVAS as a Docker container. This greatly streamlined the process and allowed us to install OpenVAS without having to modify or change any of the files for our Kali configuration.

In this lab, you will launch OpenVAS using you Kali browser and conduct a vulnerability scan of your home network.

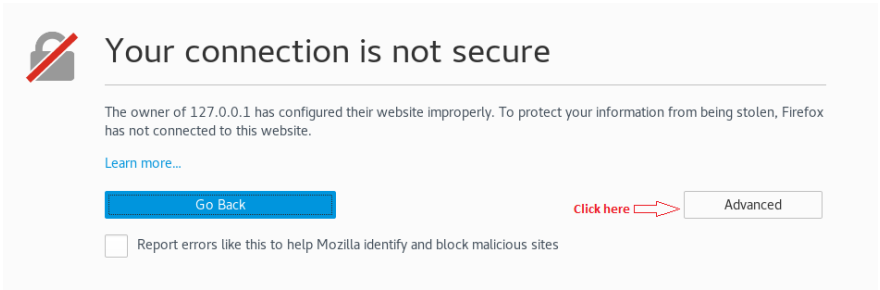
If you shut down or restarted your Kali, the container for OpenVAS will be stopped. You will need to reattach the OpenVAS container to Docker. Refer to the last section of the previous lab, starting on page 8, on how to reattach your OpenVAS container inside of Docker.

To scan your local network, you will need to ensure your Kali adapter is set to bridged. You will find the network adapter settings under the settings for either VirtualBox or the VMWare player.

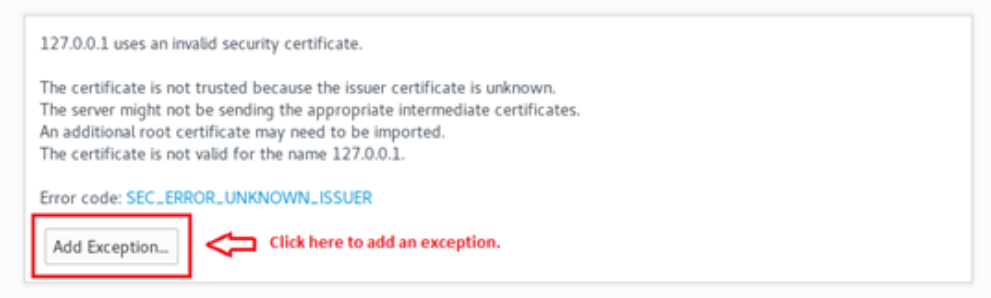
Once it seems like your OpenVAS-9 installation is OK, open your Kali browser and go to https://127.0.0.1



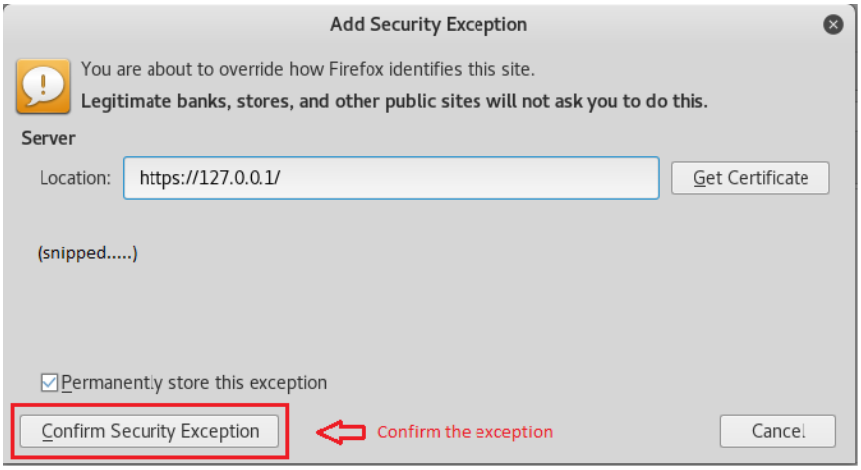
We need to add an exception for the certificate.



Add the exception.



Confirm the exception.

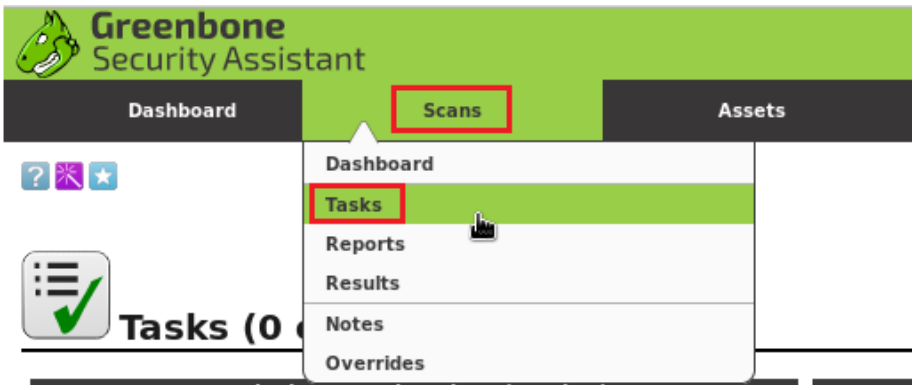


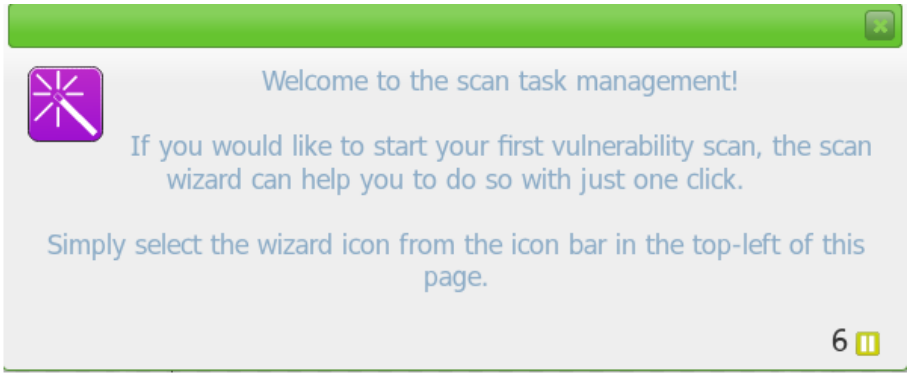
Login to OpenVAS

At the logon screen type in the admin credentials

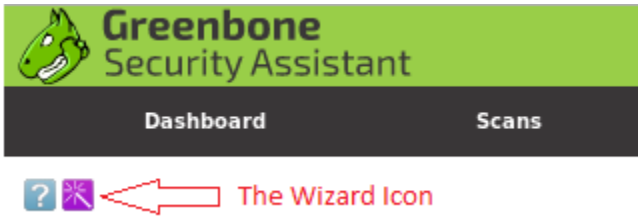
```
Username: admin
Password: admin
```

From the Dashboard, click on Scan and from the context menu, select Task.





Click on the purple button to launch the new scan wizard.



In this example, I am scanning my entire subnet of 192.168.0.0/24. This is my IP range! Your IP range will differ. Move your browser window over to the right of your screen.

From the Kali quick launch bar, open a new terminal.

At the terminal prompt, type, `ifconfig`.

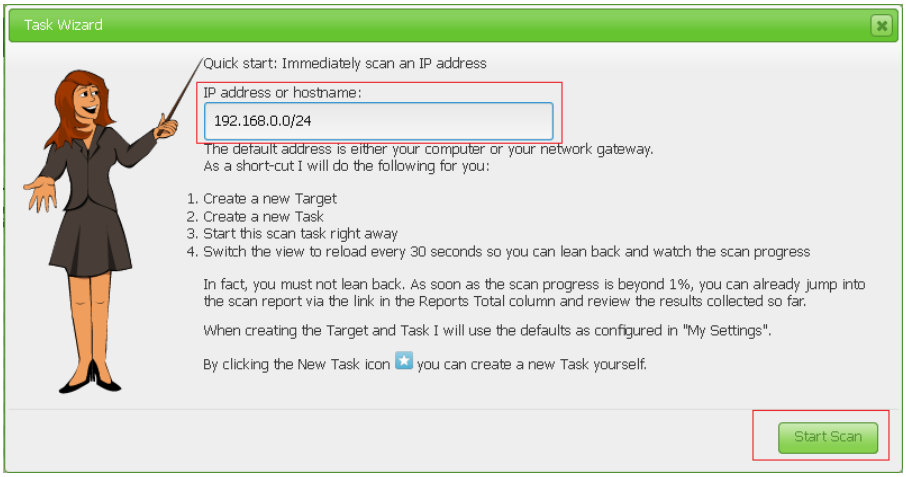
Find the IP address for your eth0 adapter. The first three octets represent your network IP address.

```
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 608536  bytes 918509441 (875.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 212864  bytes 13042550 (12.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The last octet represents your machine's assigned IP address.

```
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 608536  bytes 918509441 (875.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 212864  bytes 13042550 (12.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

To scan the entire range for the subnet, we replace the host IP with a 0 (zero) and add the slash (/) 24. This tells the scanner to ignore the first three octets as they are already full and to scan only the last octet which contains the remaining 8 bits of the 32-bit address. The scanner will scan the entire subnet for any device with an assigned host IP starting with 1 all the way to 255.



Known issue with OpenVAS Scanner 5.1.2

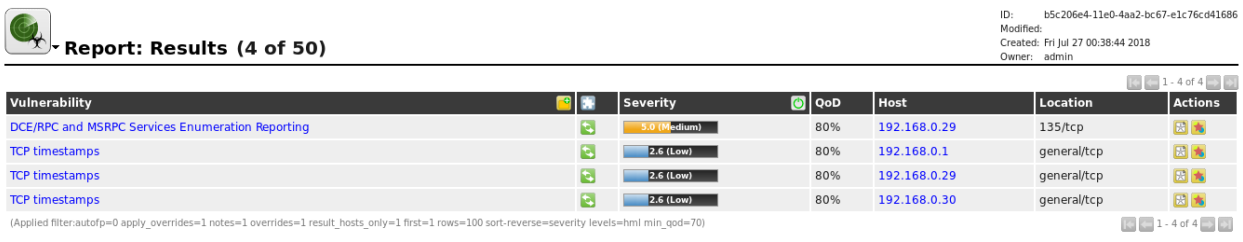
The docker image uses the latest version of OpenVAS which is 9 and openvas-scanner 5.1.2. There is a known issue with openvas-scanner version 5.1.2 where scans stop at 1% and only sometimes progress after many hours due to a bug in task scheduler. This is for scans of even a single target host which should take no more than a few minutes. The most recent version of openvas-scanner (5.1.3) includes a patch to fix the issue. More details on the issue can be found on the greenbone forums at https://community.greenbone.net/t/community-feed-unusable/132/11

Give it second for the scan to start. Down at the bottom of the task page, you will see your scan status. Unless you have a target such as Windows XP or Metesploitable2 running or you network adapter is set to bridged networking, you may not have any scan results.

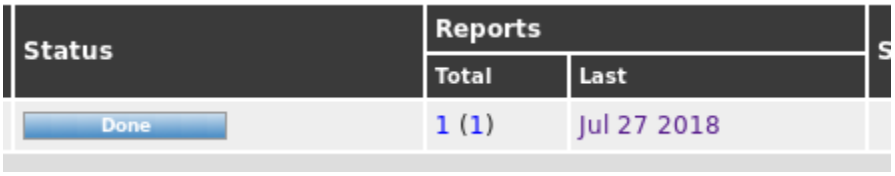
Once the scan starts you will be taken to the task page. Here you can see the results of your scan in real time.

You can click on the percentage for the completed scan to view your scan results by IP address discovered.

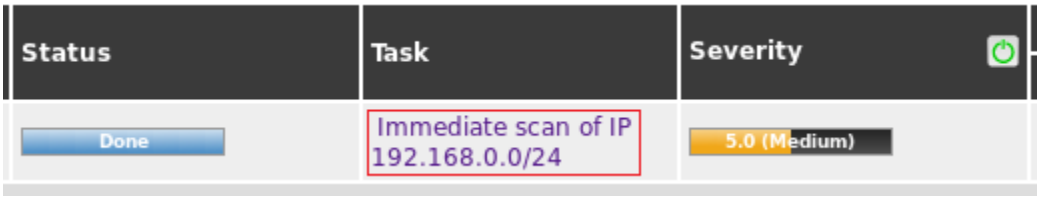
Scan results by IP address.



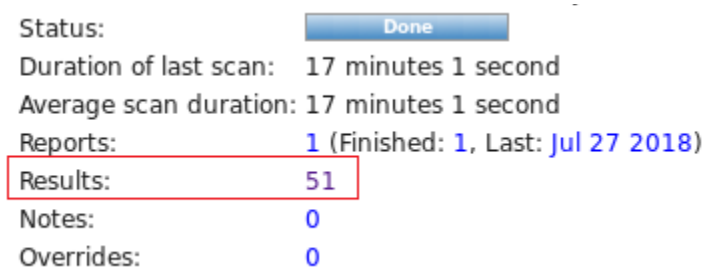
You can use your browser back button to return to the Task page. Here you can view the results of the report by clicking the number of the report located under the report column.



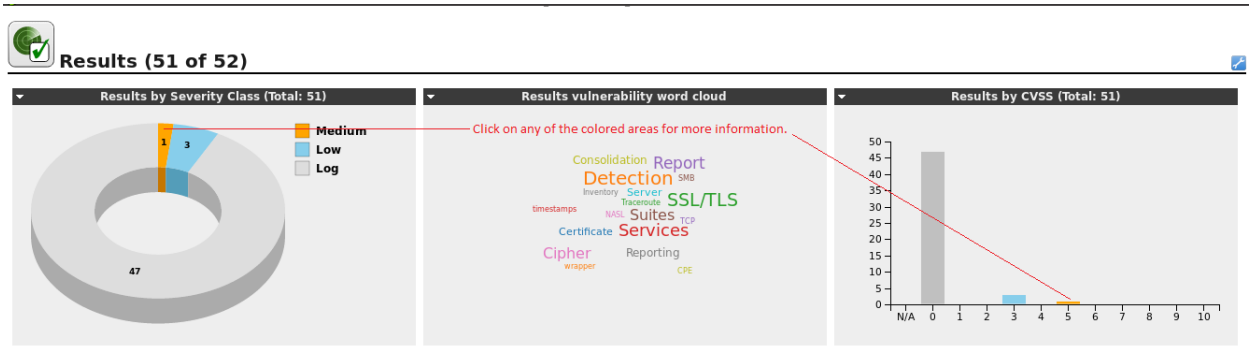
On the reports page, you can click on the severity of the scan results to see results. To see the actual vulnerabilities, from the task running across the bottom of the report page, under the task column, click on the scan results.



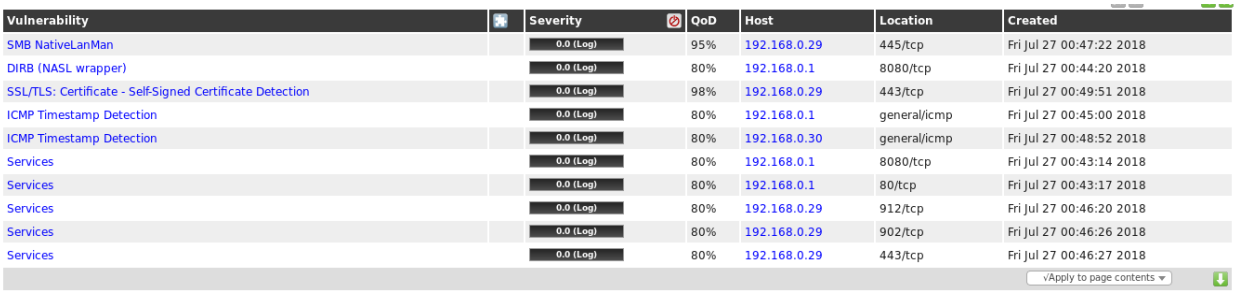
On the next page, click on the number of results.



On the next page, under Results. You can click on any of the colored areas to see what vulnerabilities were discovered and their severity level.



At the bottom of the results page, you can see the vulnerabilities and on which machine they reside.



Vulnerability	Severity	QoD	Host	Location	Created
SMB NativeLanMan	0.0 (Log)	95%	192.168.0.29	445/tcp	Fri Jul 27 00:47:22 2018
DIRB (NASL wrapper)	0.0 (Log)	80%	192.168.0.1	8080/tcp	Fri Jul 27 00:44:20 2018
SSL/TLS: Certificate - Self-Signed Certificate Detection	0.0 (Log)	98%	192.168.0.29	443/tcp	Fri Jul 27 00:49:51 2018
ICMP Timestamp Detection	0.0 (Log)	80%	192.168.0.1	general/icmp	Fri Jul 27 00:45:00 2018
ICMP Timestamp Detection	0.0 (Log)	80%	192.168.0.30	general/icmp	Fri Jul 27 00:48:52 2018
Services	0.0 (Log)	80%	192.168.0.1	8080/tcp	Fri Jul 27 00:43:14 2018
Services	0.0 (Log)	80%	192.168.0.1	80/tcp	Fri Jul 27 00:43:17 2018
Services	0.0 (Log)	80%	192.168.0.29	912/tcp	Fri Jul 27 00:46:20 2018
Services	0.0 (Log)	80%	192.168.0.29	902/tcp	Fri Jul 27 00:46:26 2018
Services	0.0 (Log)	80%	192.168.0.29	443/tcp	Fri Jul 27 00:46:27 2018

vApply to page contents

End of the lab!