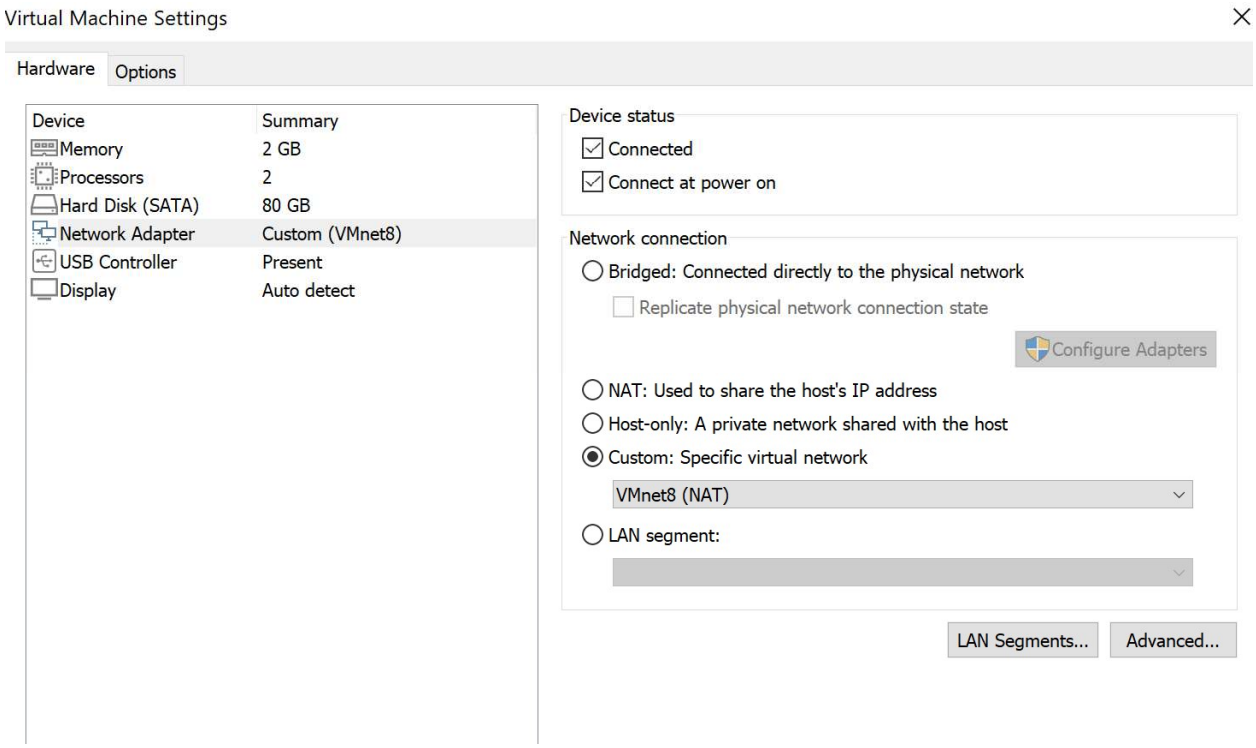
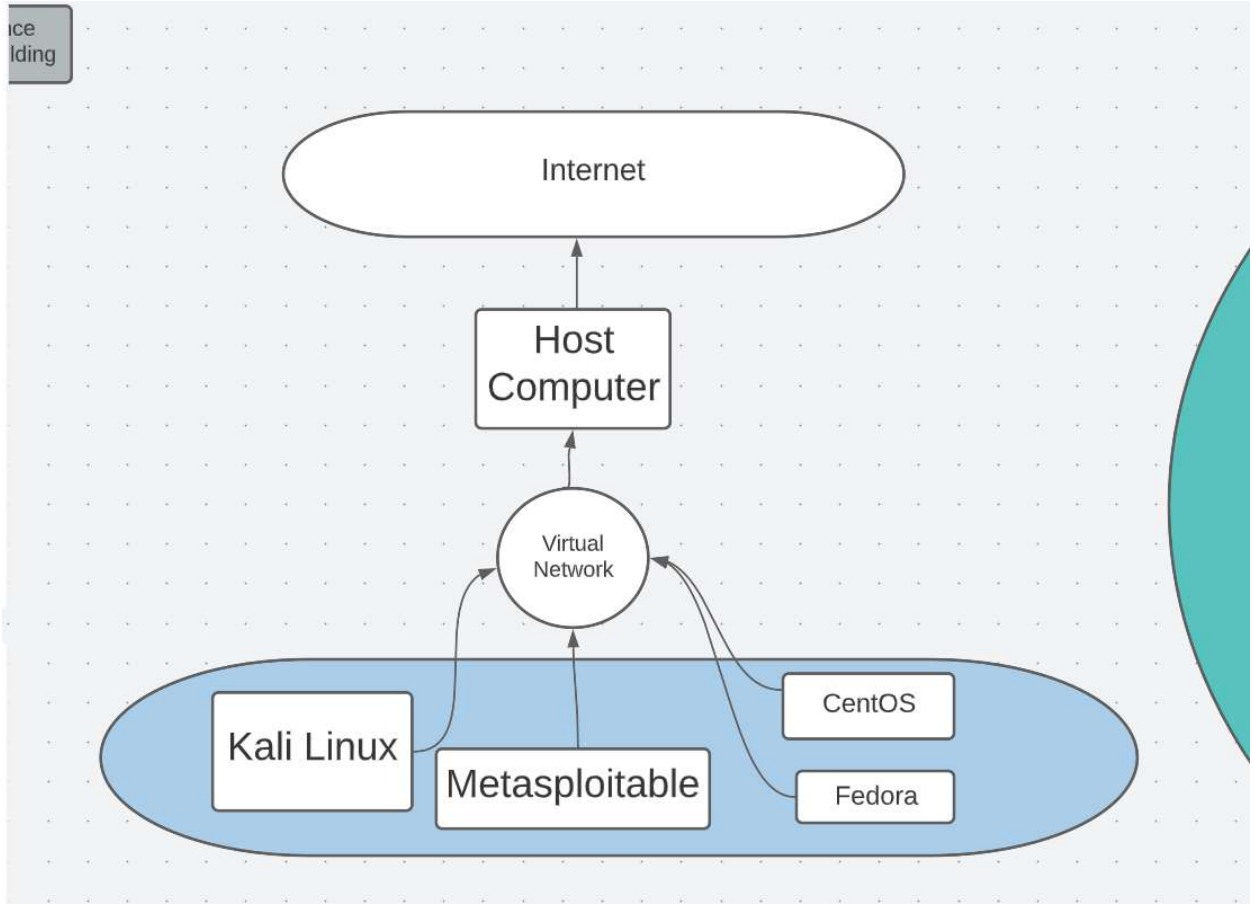
1. Create a NAT network in VMware.

NAT network was created and assigned to the Network adapter for all virtual machines



2. Deploy VM's Fedora, CentOS, Metasploitable using each of the provided images.

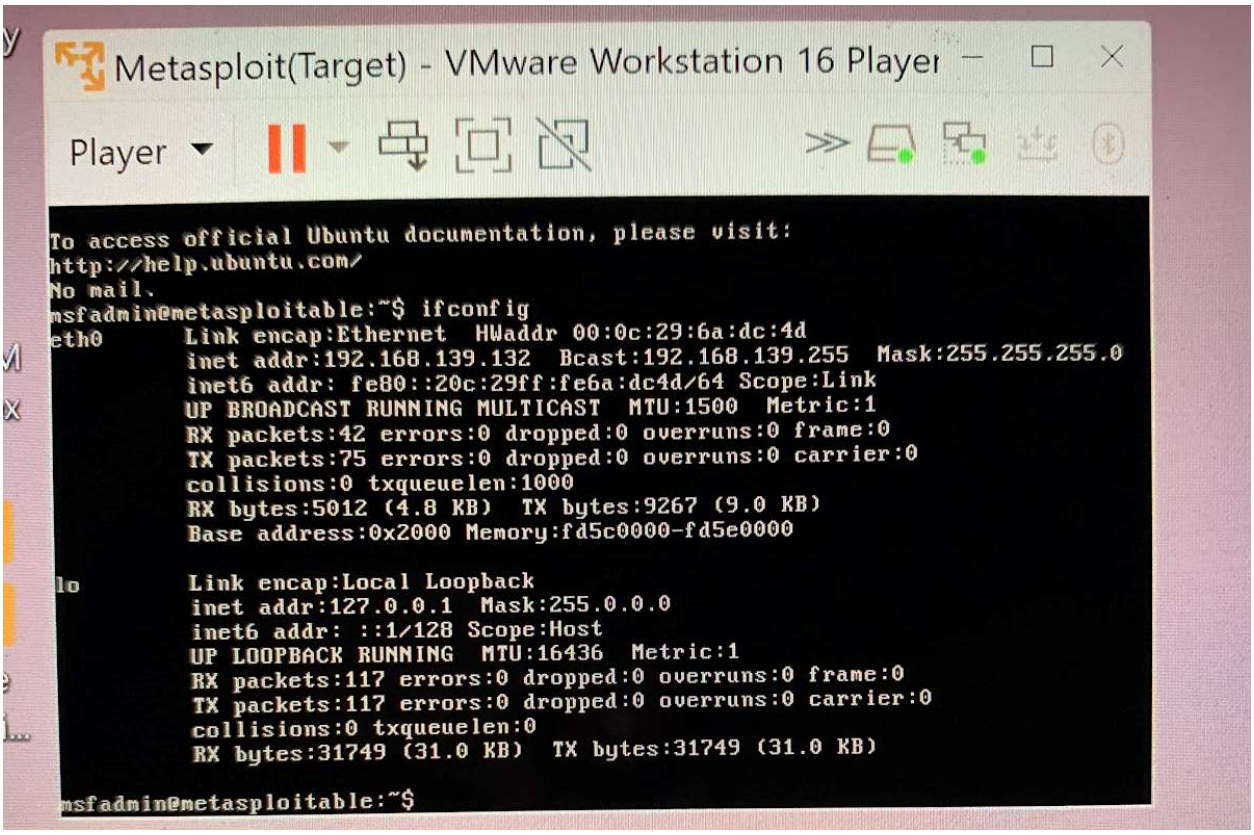
3. Connect the first interface of each VM to the NAT network. Present a simple diagram of the network topology you just created.



Metasplotable

Step 1:

Use ifconfig command in Metasploitable to identify IP address for metasplotable



Step 2:

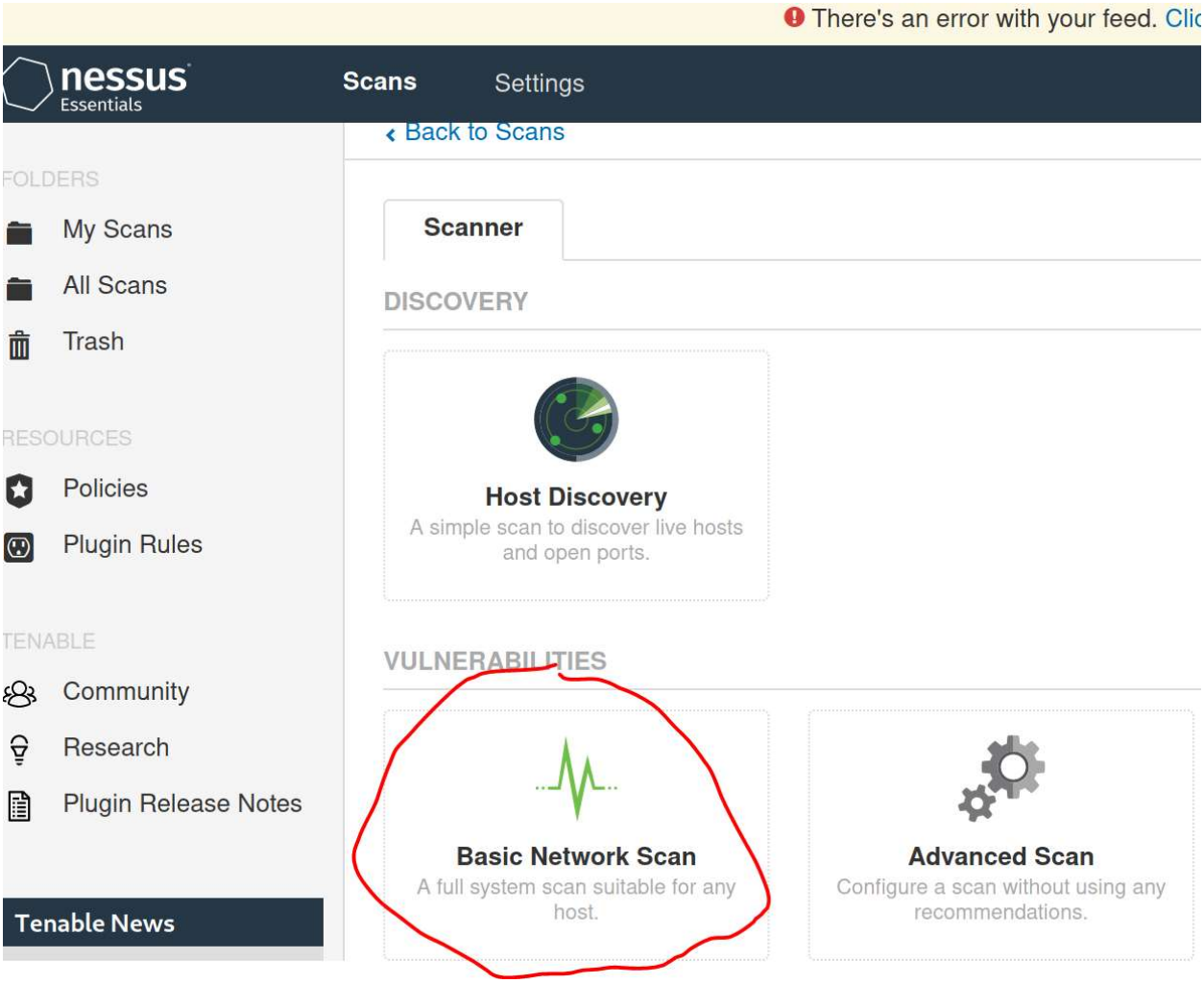
Open Kali Linux terminal and use command “ping “ to check for a connection from metasploitable our target machine

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.139.132                                          130 ✗
PING 192.168.139.132 (192.168.139.132) 56(84) bytes of data.
64 bytes from 192.168.139.132: icmp_seq=1 ttl=64 time=15.5 ms
64 bytes from 192.168.139.132: icmp_seq=2 ttl=64 time=2.03 ms
64 bytes from 192.168.139.132: icmp_seq=3 ttl=64 time=1.79 ms
64 bytes from 192.168.139.132: icmp_seq=4 ttl=64 time=1.47 ms
64 bytes from 192.168.139.132: icmp_seq=5 ttl=64 time=1.32 ms
64 bytes from 192.168.139.132: icmp_seq=6 ttl=64 time=1.80 ms

--- 192.168.139.132 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5012ms
rtt min/avg/max/mdev = 1.315/3.986/15.521/5.163 ms
```

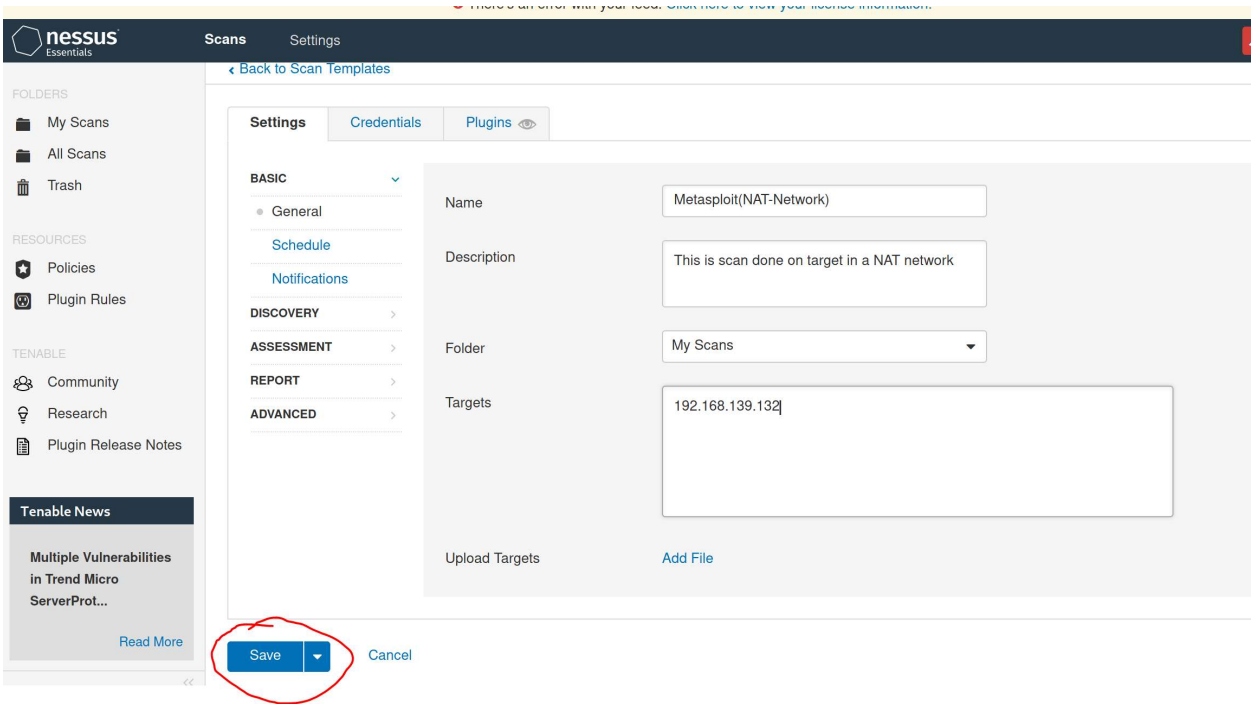
Step 3. Open the Nessus application in the Kali Linux VM.

Step 4. Perform a scan with Nessus on the target VM. Provide screenshots and explain thoroughly each step.

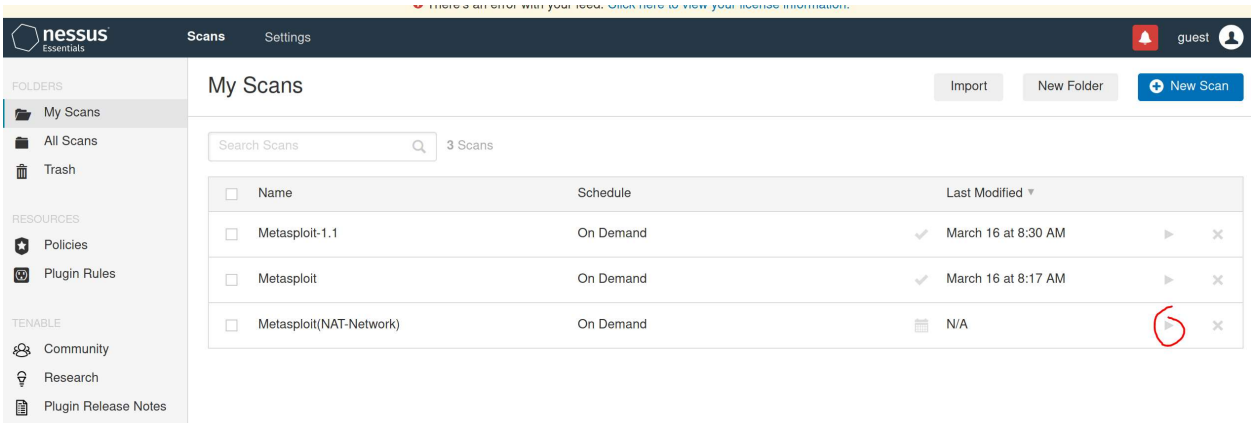
Step 5. Selected Basic Network Scan



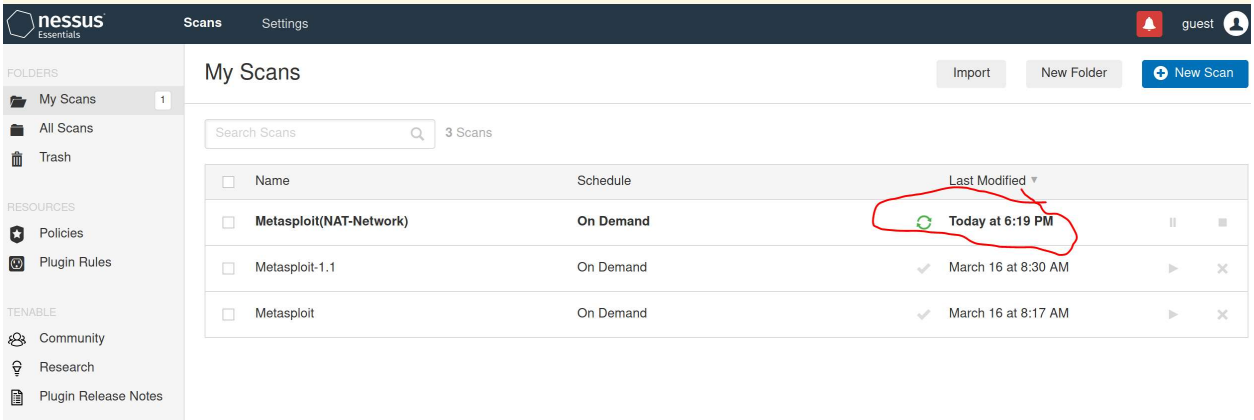
Step 6. Name the target OS. Make a description of target. Input target IP address into “Targets”. Save the scan



Step 7. Find scan that was created and select the play button to launch scan. This will tell Nessus to start the scan on the target OS(Metasploitable)

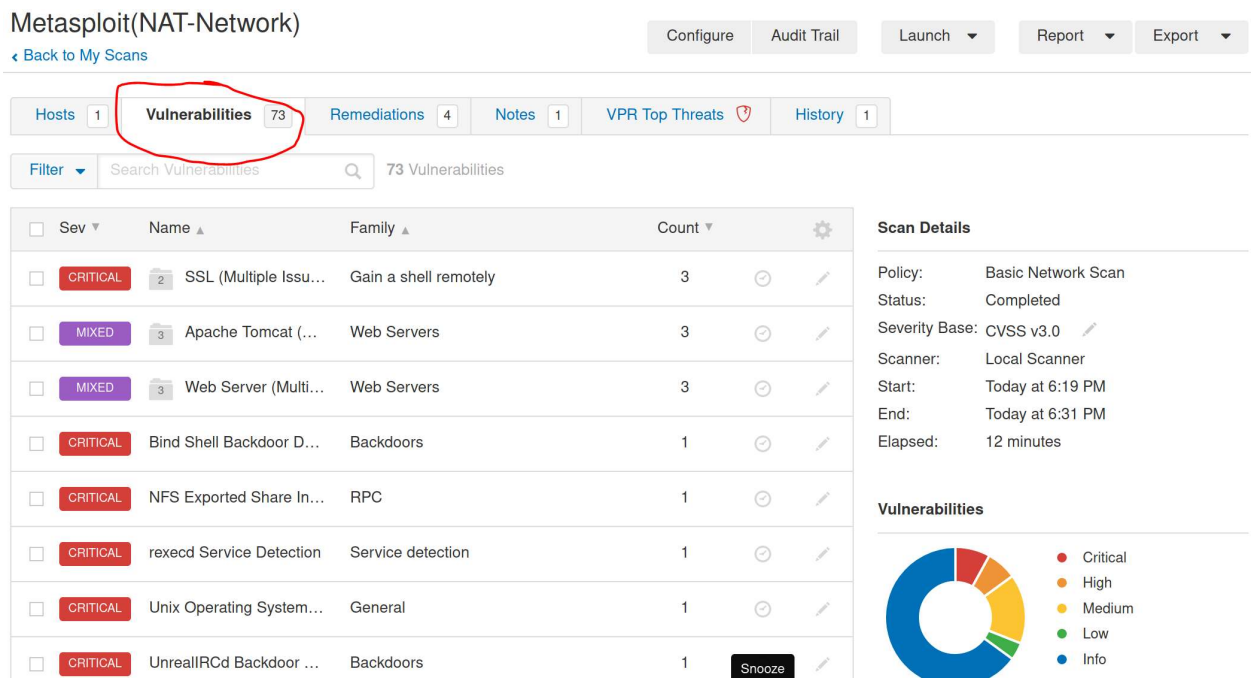


Step 8. Wait for scan to complete



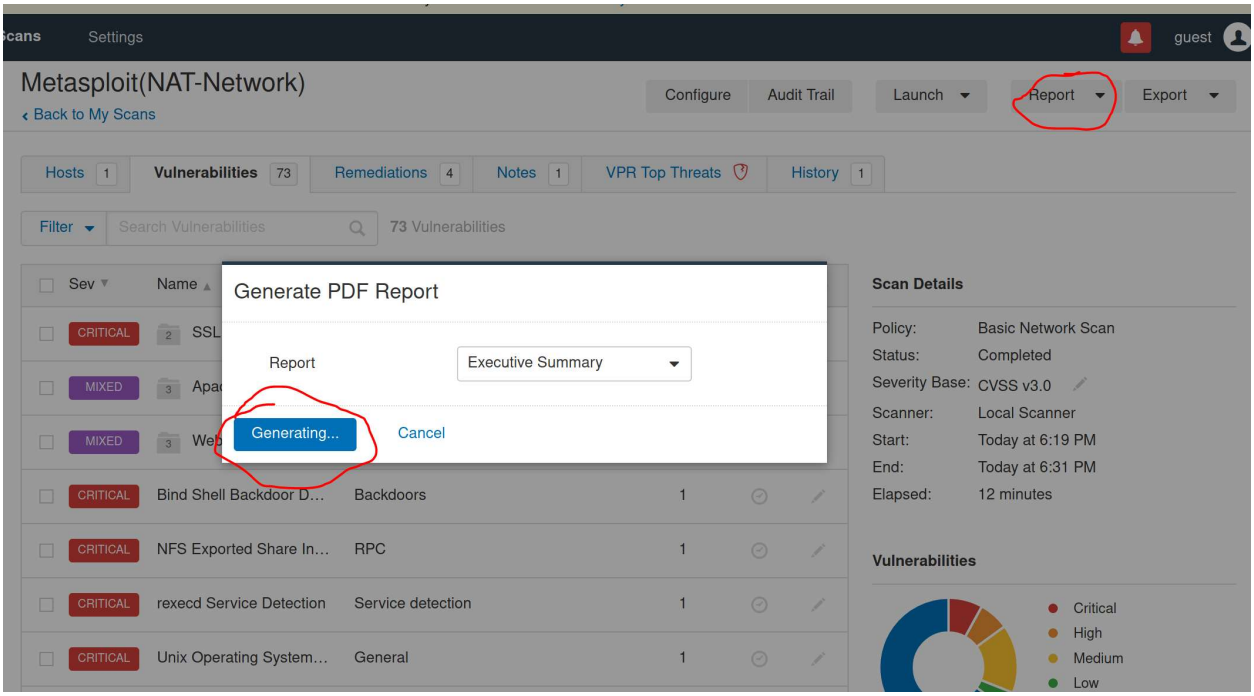
Step 9. Click on the Metasploit(NAT-Network) file created to view the scan

Step 10. Select the vulnerabilities tab to view vulnerabilities found

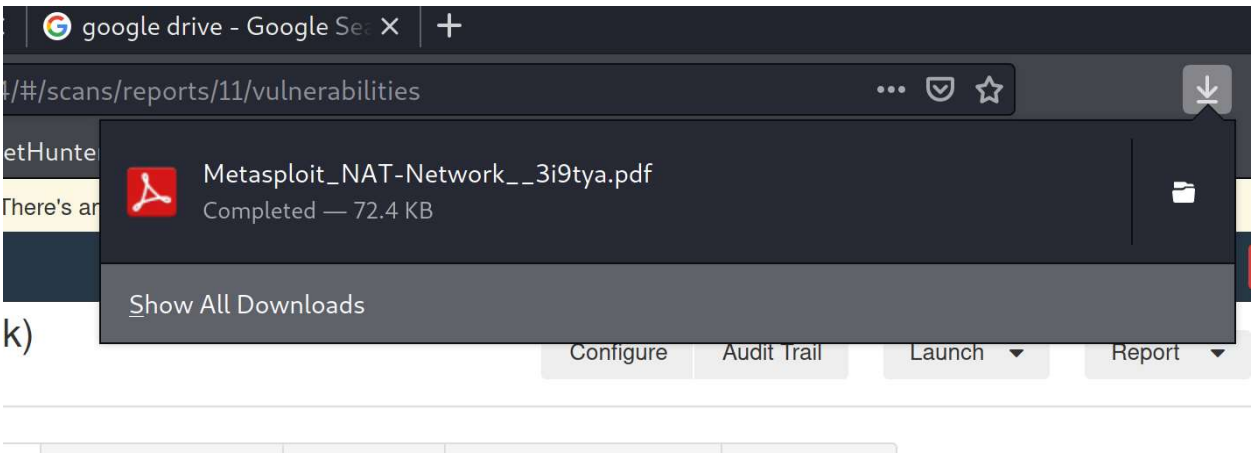


Step 11. Download the generated report from Nessus

Step 1. Select Report→PDF and then generate with the default Executive summary selected

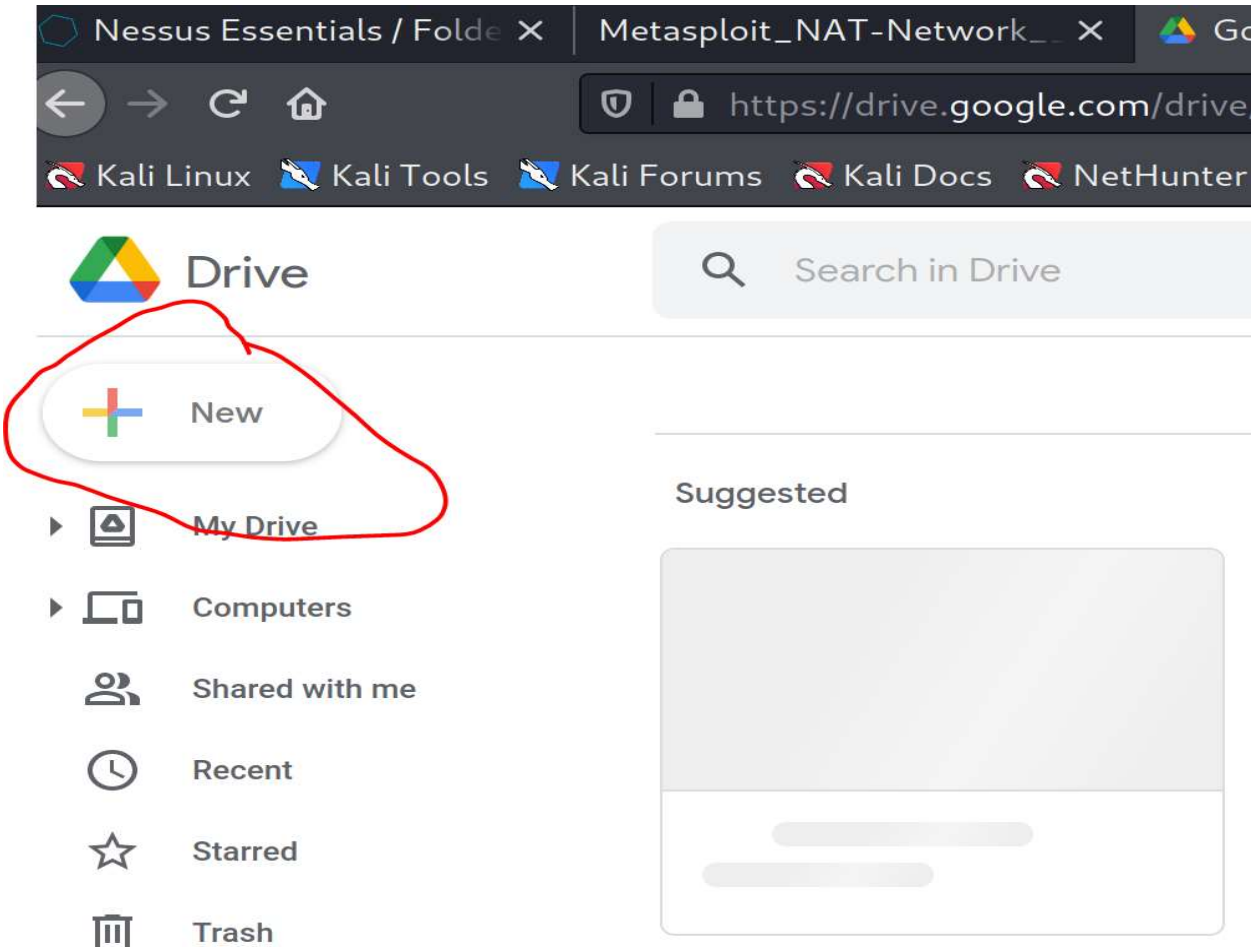


Step 2. Once Report completes save as a file→Go to downloads at top right of screen

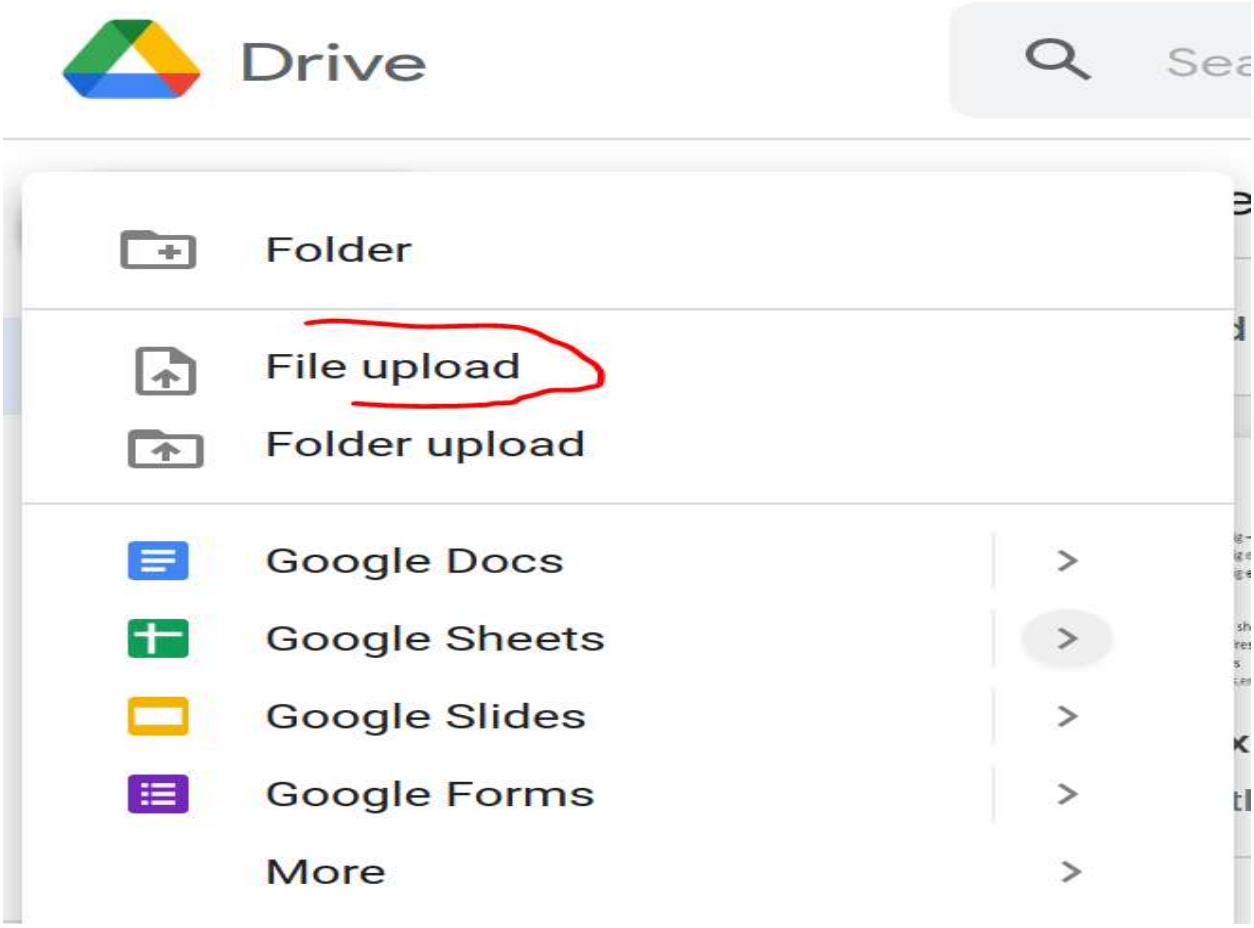


Step 3. Open a cloud storage server to store downloaded report into. In theis case we will be using google drive

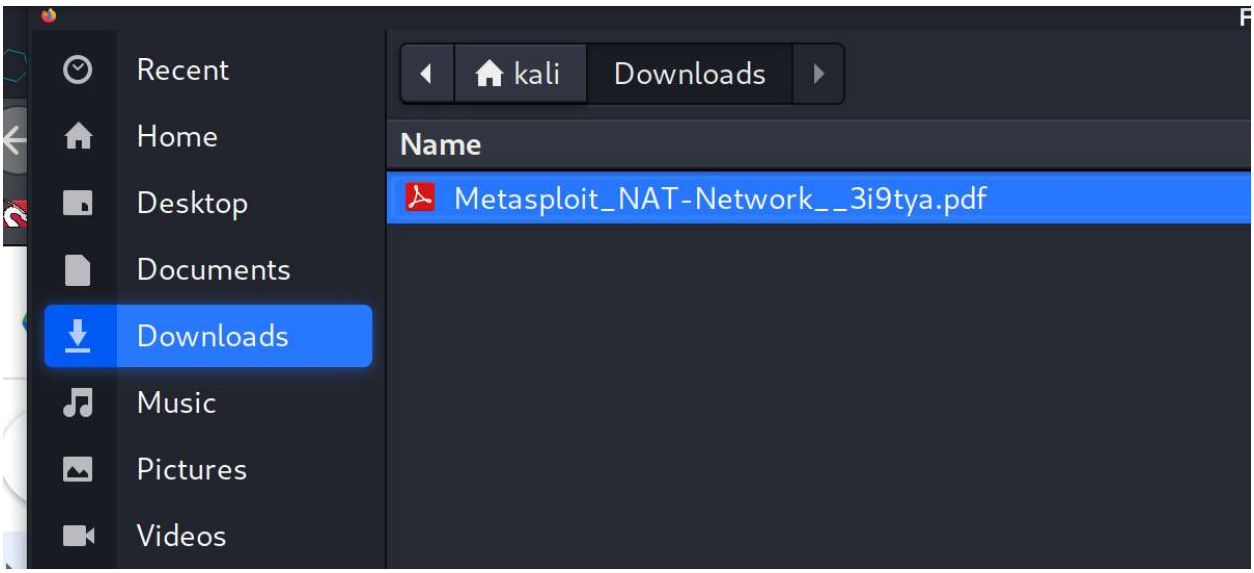
Step 4.Access drive and select the “New” icon



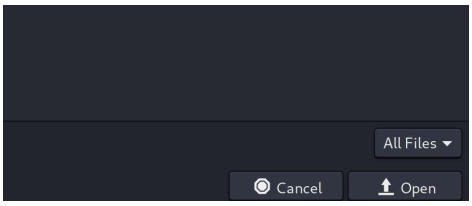
Step 5. Select File upload and



Step 6. Navigate to downloads and select Metaspliot or Report PDF that was downloaded from nessus page



Step 7. Select open at bottom right of the screen

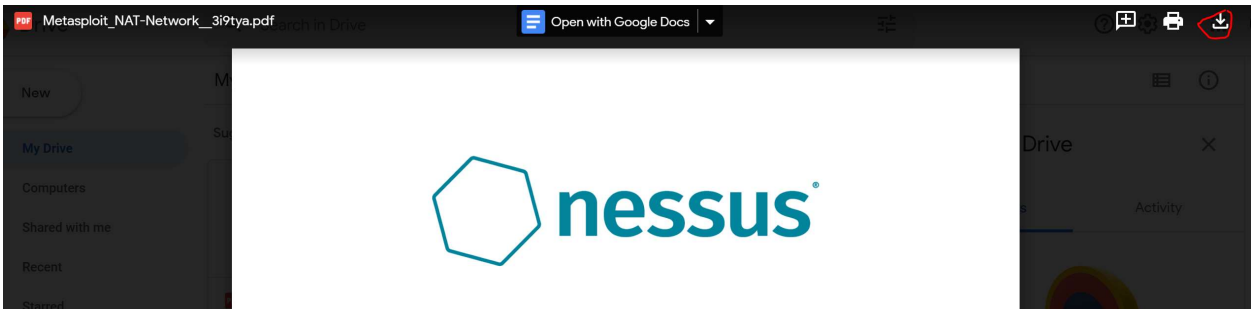


Step 8.

Go to Host computer(Computer that is hosting virtual machines and environment). Access cloud storage services that PDF was stored through. In this case, we visited our google drive and downloaded the Report PDF we had uploaded to the cloud within the virtual machine.

Step 8.

Click on Report PDF and select download option at top right of the screen



Step 9. Upload PDF to Group github

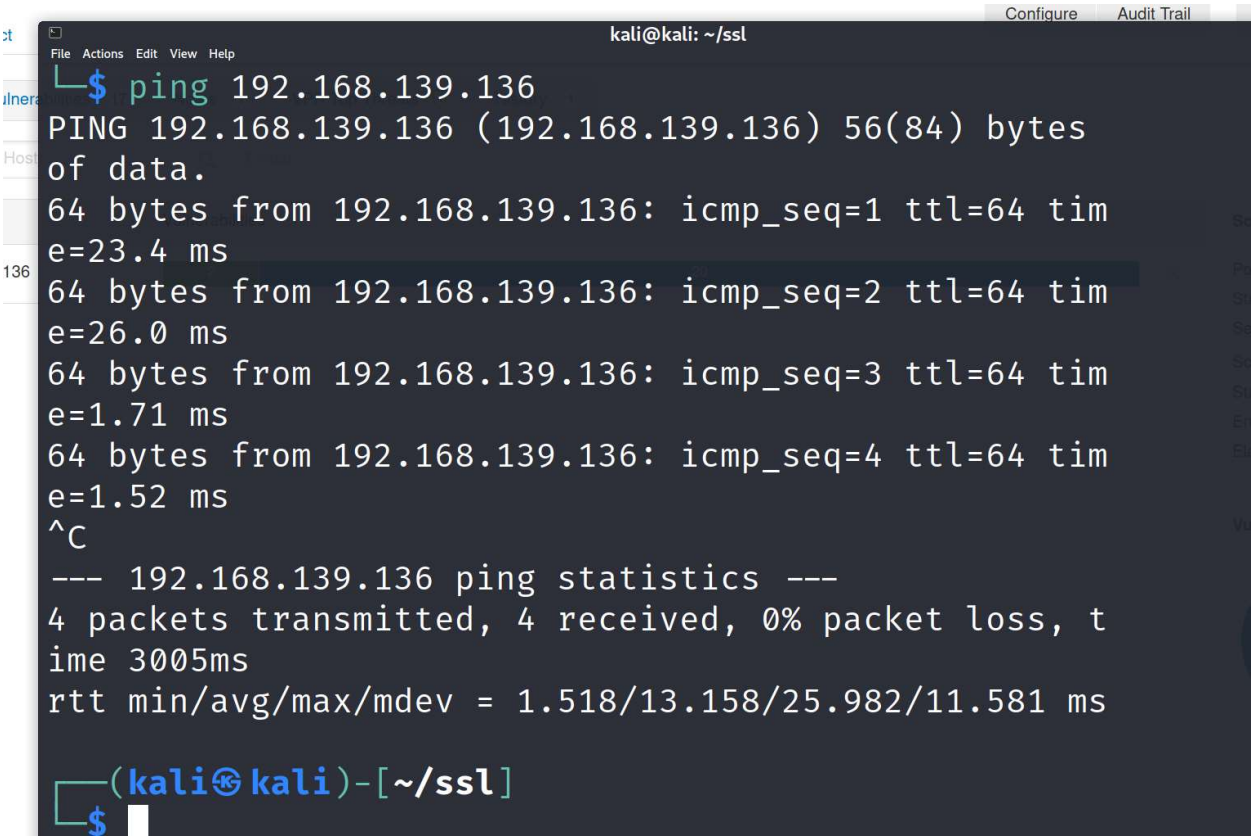
CentOS

Step 1:

Use ifconfig command in CentOS to identify IP address for CentOS

Step 2:

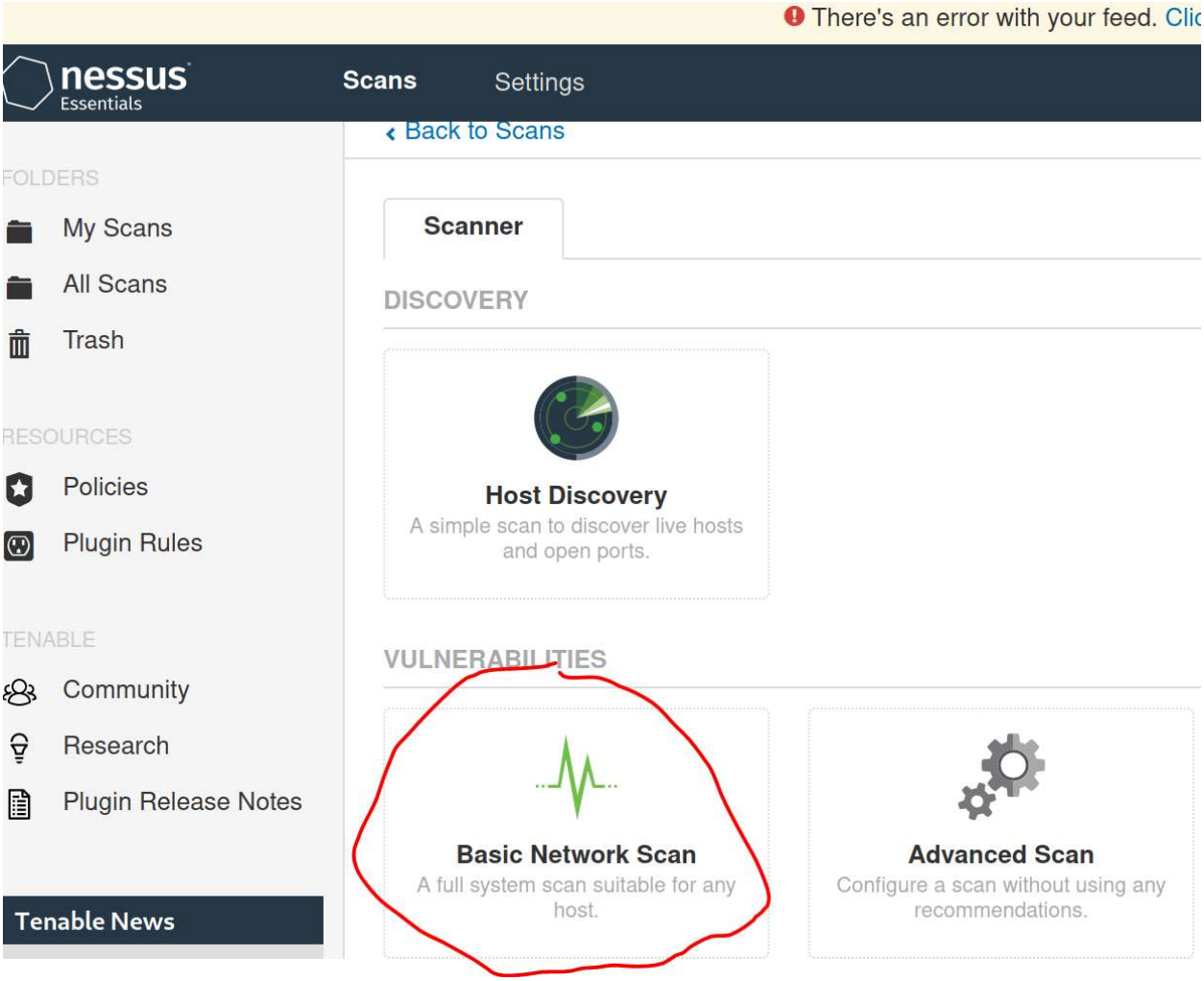
Open Kali Linux terminal and use command “ping “ to check for a connection from CentOS our target machine



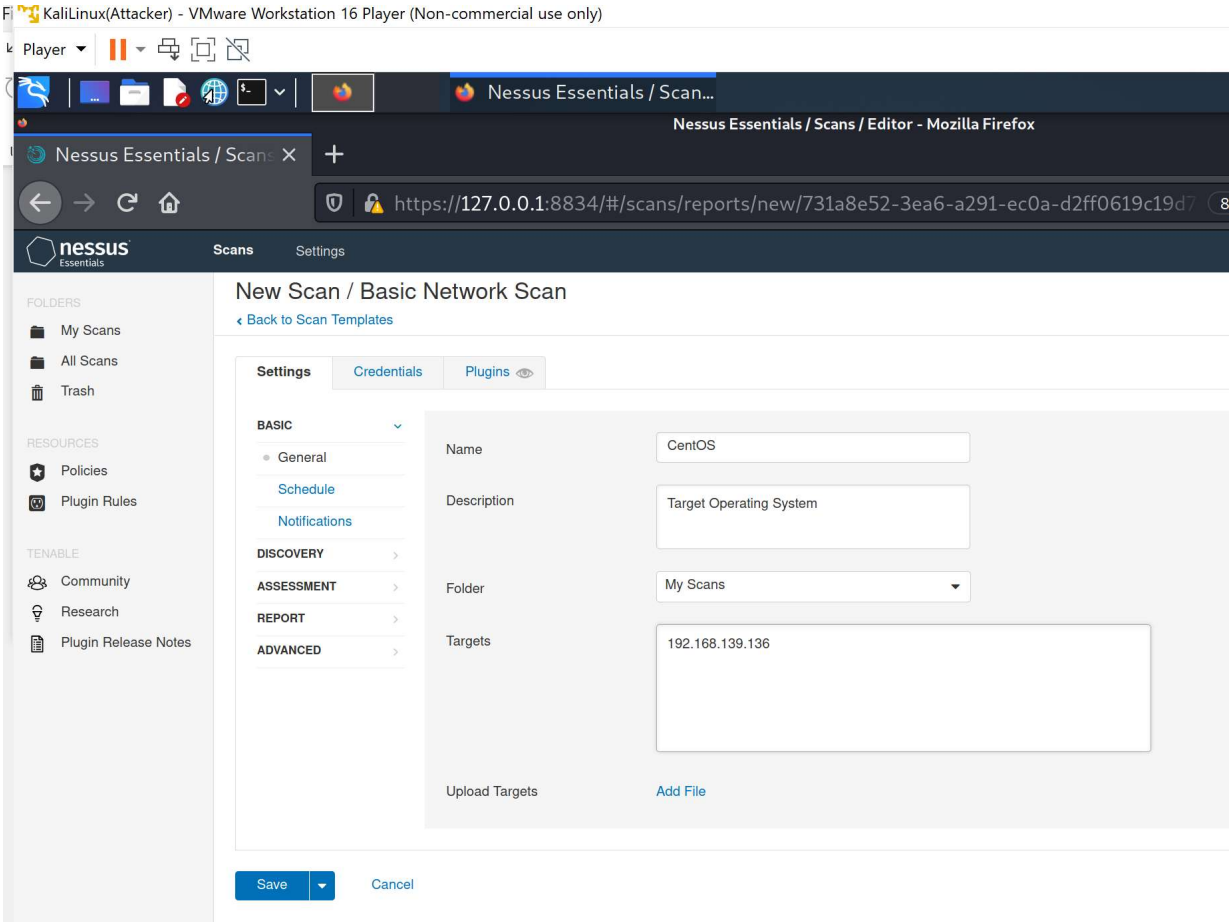
Step 3. Open the Nessus application in the Kali Linux VM.

Step 4. Perform a scan with Nessus on the target VM. Provide screenshots and explain thoroughly each step.

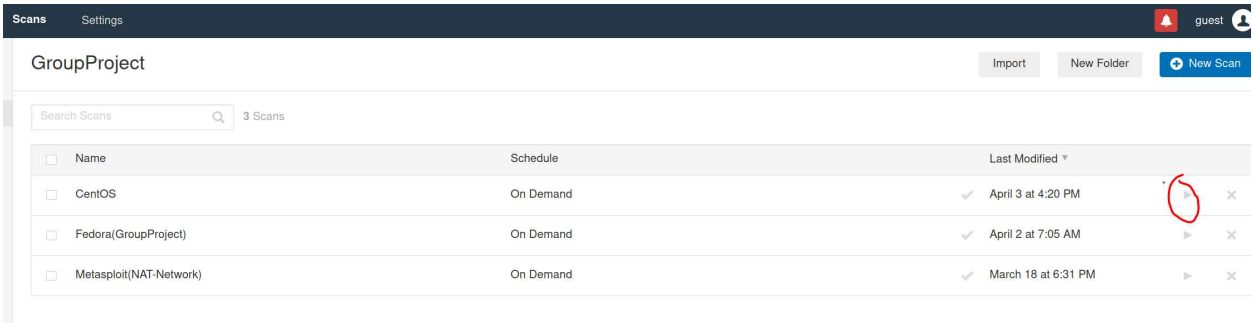
Step 5. Selected Basic Network Scan



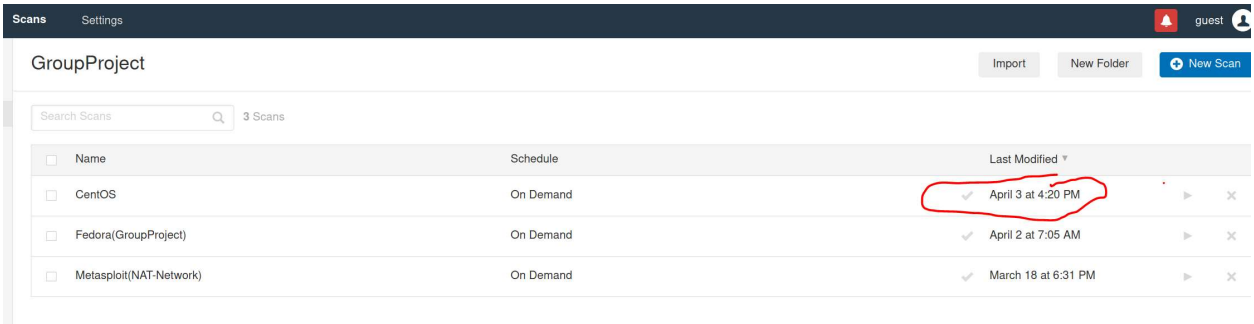
Step 6. Name the target OS. Make a description of target. Input target IP address into “Targets”. Save the scan



Step 7. Find scan that was created and select the play button to launch scan. This will tell Nessus to start the scan on the target OS(CentOS)

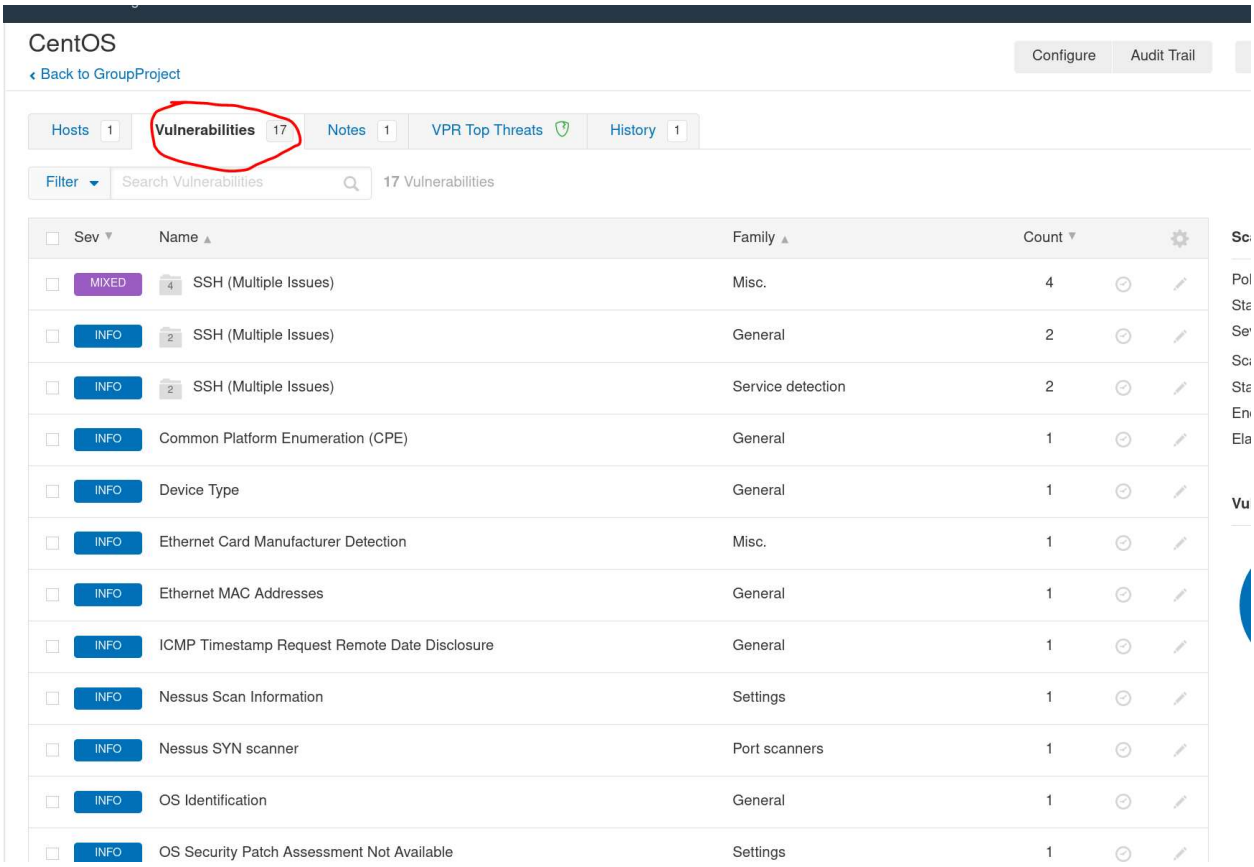


Step 8. Wait for scan to complete

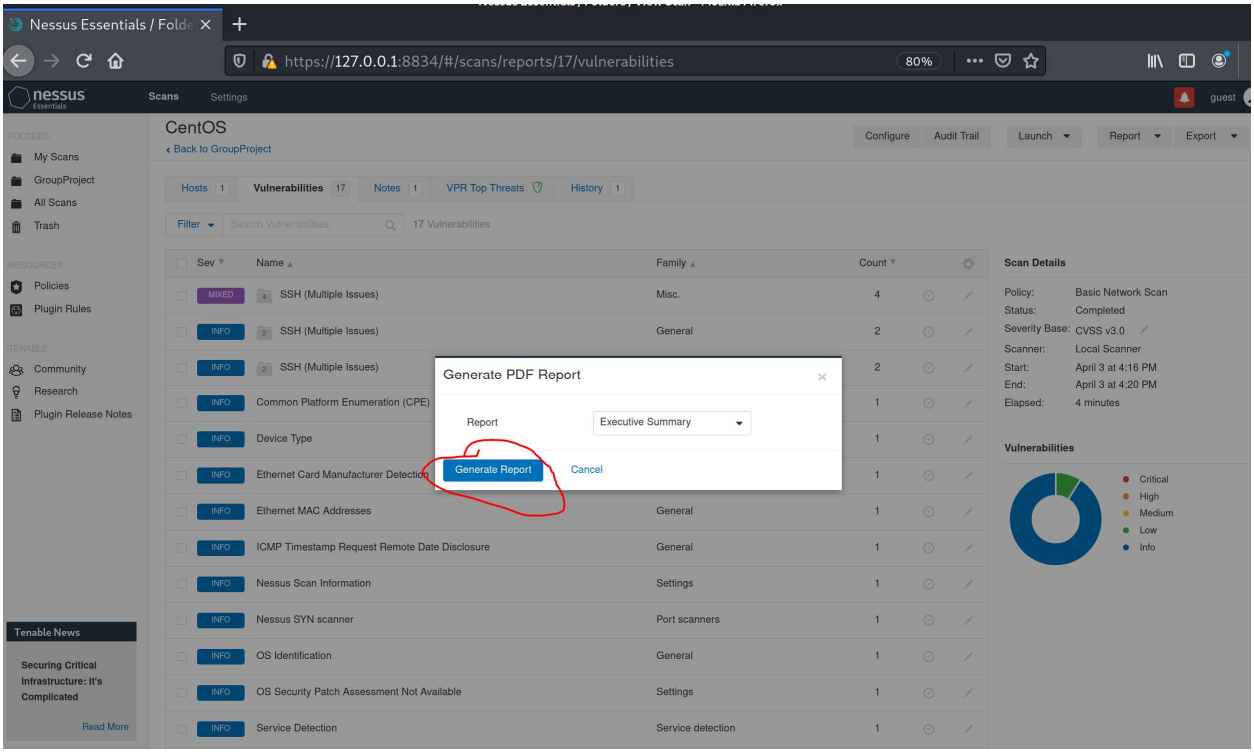


Step 9. Click on the CentOS file created to view the scan

Step 10. Select the vulnerabilities tab to view vulnerabilities found



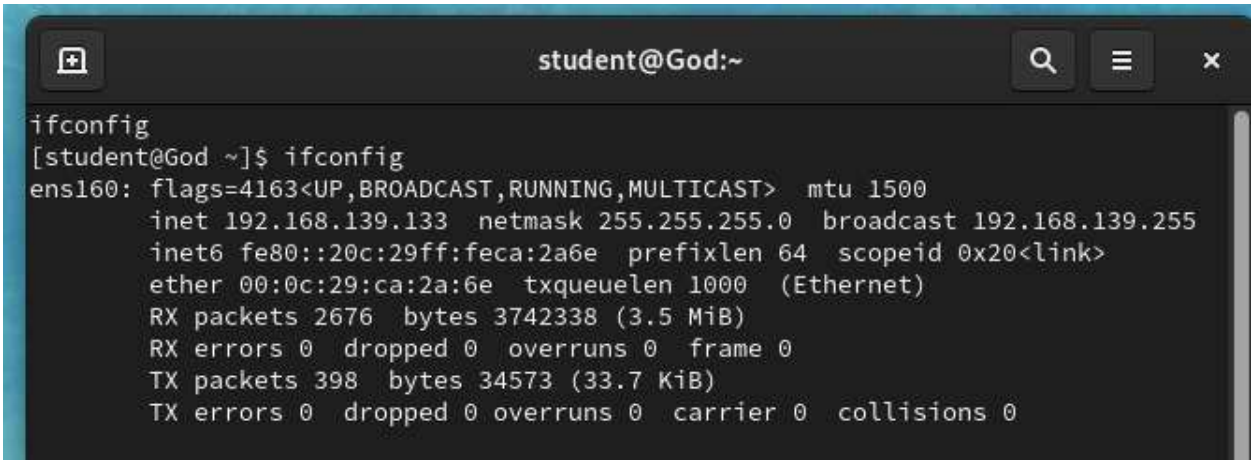
Step 11. Download the generated report from Nessus and upload to github. Following same steps as process from Metasploitable steps



Fedora

Step 1:

Use ifconfig command in Fedora to identify IP address for Fedora



Step 2:

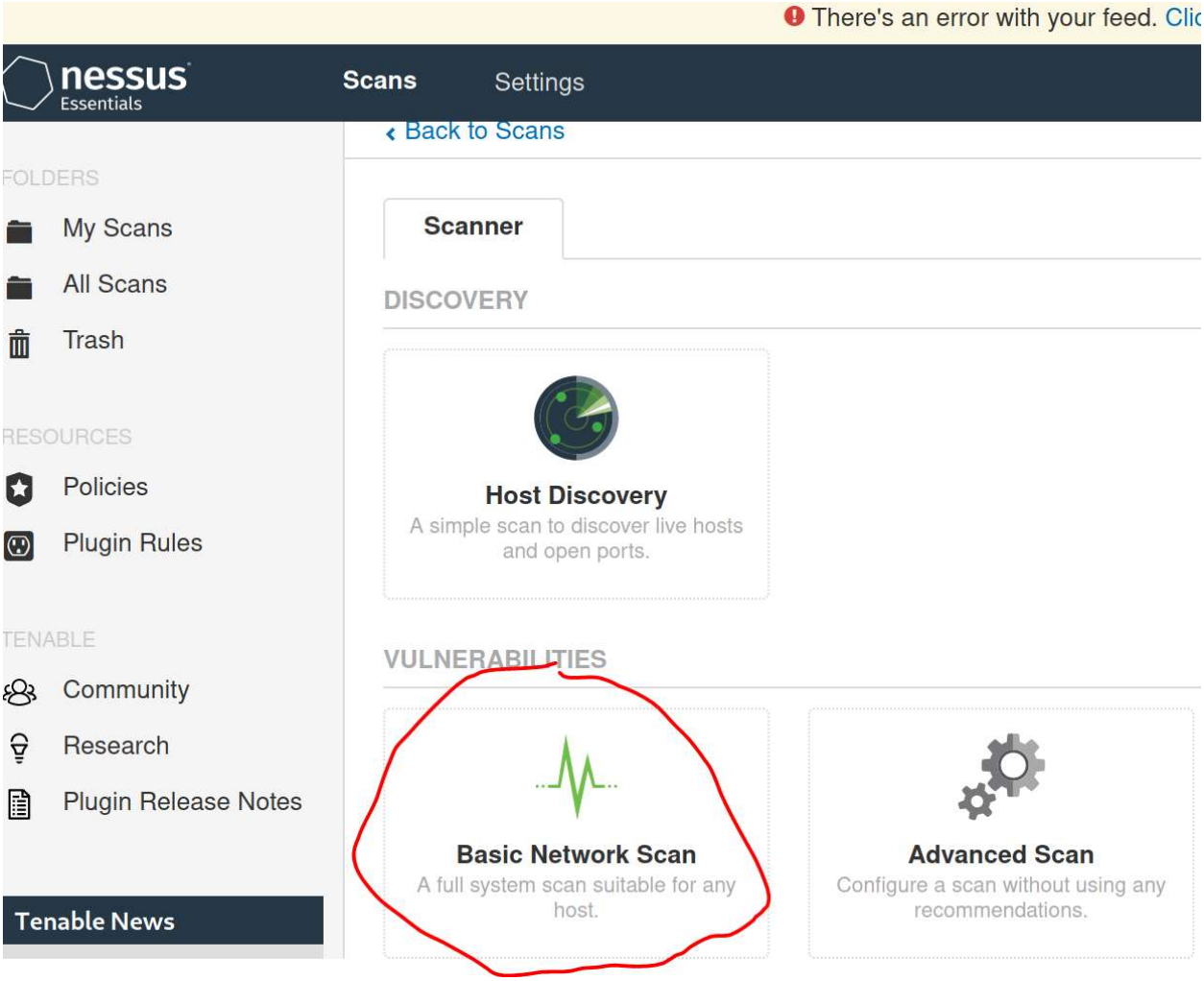
Open Kali Linux terminal and use command “ping “ to check for a connection from Fedora our target machine

```
kali@kali: ~/ssl
File  Actions  Edit  View  Help
3 packets transmitted, 0 received, 100% packet loss, time 2032
ms

┌──(kali㉿kali)-[~/ssl]
└─$ ping 192.168.139.133                                        1 ✗
PING 192.168.139.133 (192.168.139.133) 56(84) bytes of data.
64 bytes from 192.168.139.133: icmp_seq=1 ttl=64 time=7.20 ms
64 bytes from 192.168.139.133: icmp_seq=2 ttl=64 time=1.76 ms
64 bytes from 192.168.139.133: icmp_seq=3 ttl=64 time=1.83 ms
64 bytes from 192.168.139.133: icmp_seq=4 ttl=64 time=1.18 ms
64 bytes from 192.168.139.133: icmp_seq=5 ttl=64 time=2.74 ms
^C
--- 192.168.139.133 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.176/2.941/7.203/2.189 ms

┌──(kali㉿kali)-[~/ssl]
└─$
```

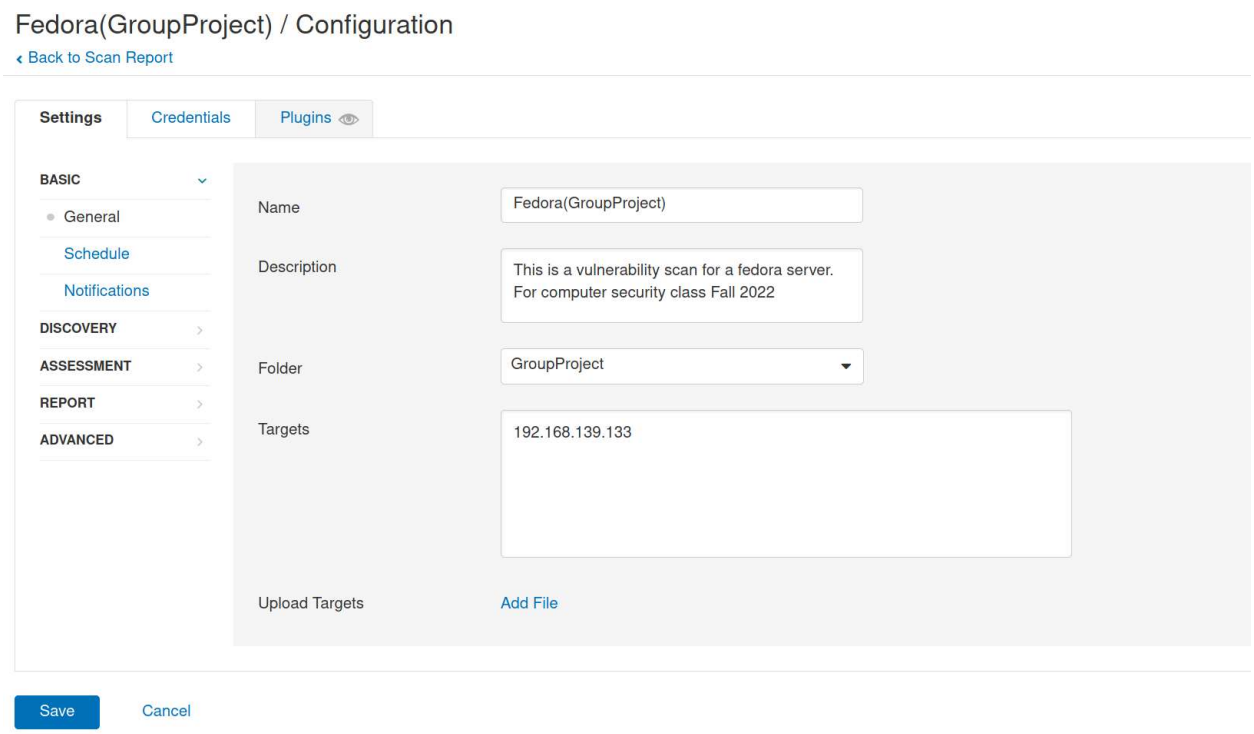
Step 3. Open the Nessus application in the Kali Linux VM.

Step 4. Perform a scan with Nessus on the target VM. Provide screenshots and explain thoroughly each step.

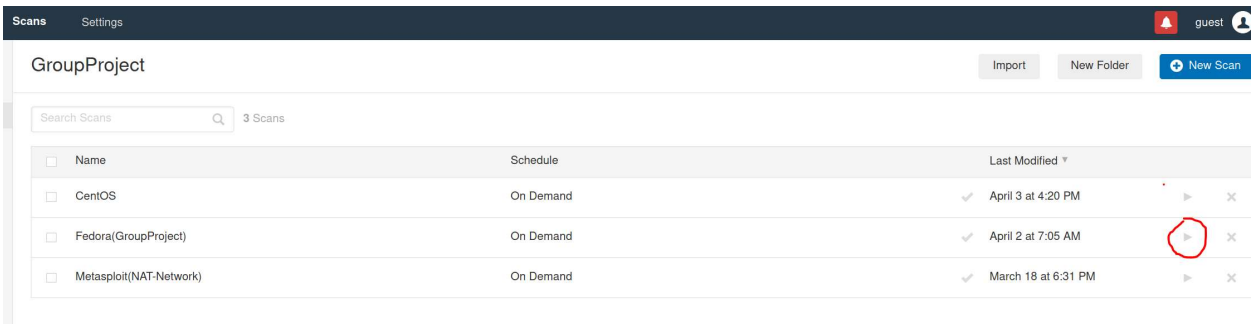
Step 5. Selected Basic Network Scan



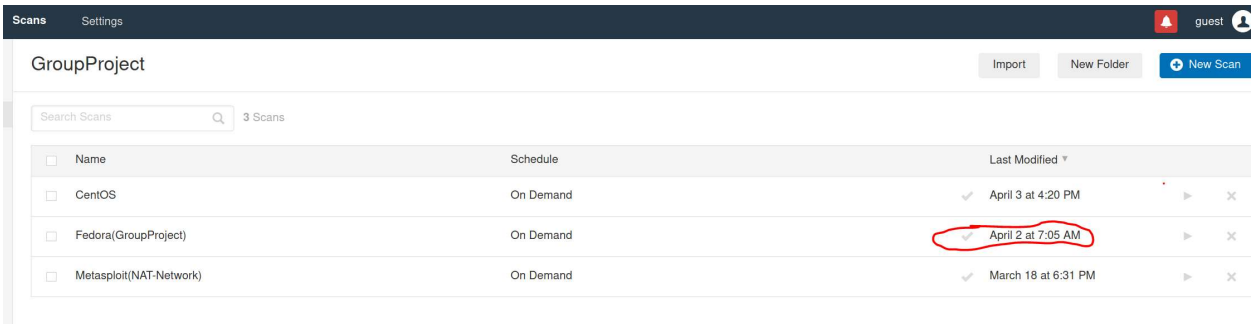
Step 6. Name the target OS. Make a description of target. Input target IP address into “Targets”. Save the scan



Step 7. Find scan that was created and select the play button to launch scan. This will tell Nessus to start the scan on the target OS(Fedora)

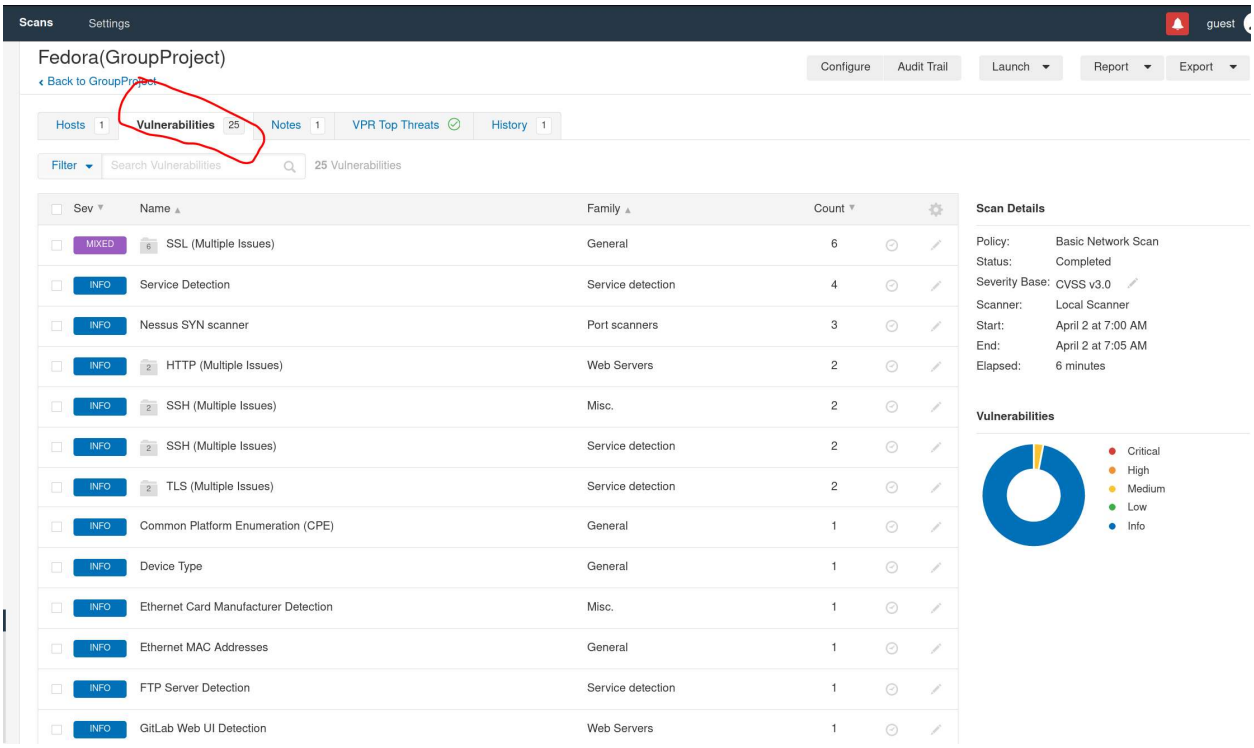


Step 8. Wait for scan to complete



Step 9. Click on the Fedora file created to view the scan

Step 10. Select the vulnerabilities tab to view vulnerabilities found



Step 11. Download the generated report from Nessus and upload to github. Following same steps as process from Metasploitable steps