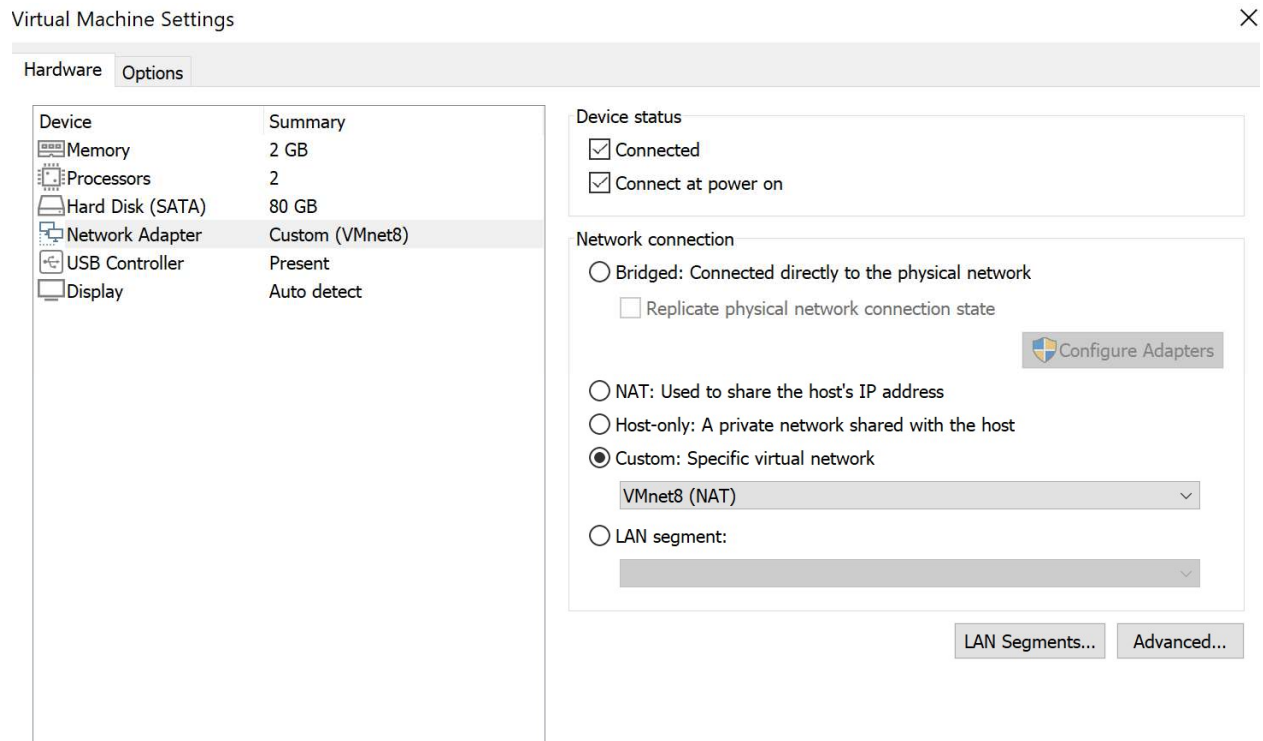


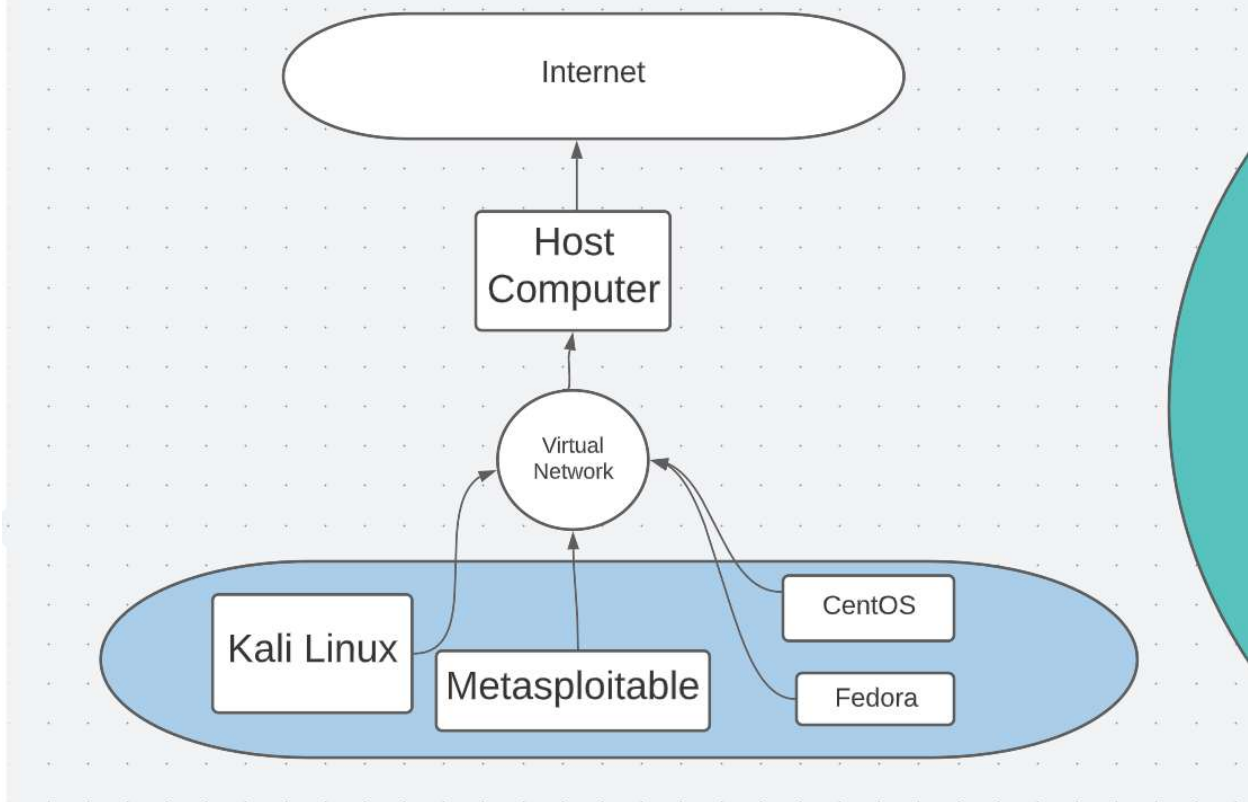
1. Create a NAT network in VMware.

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.

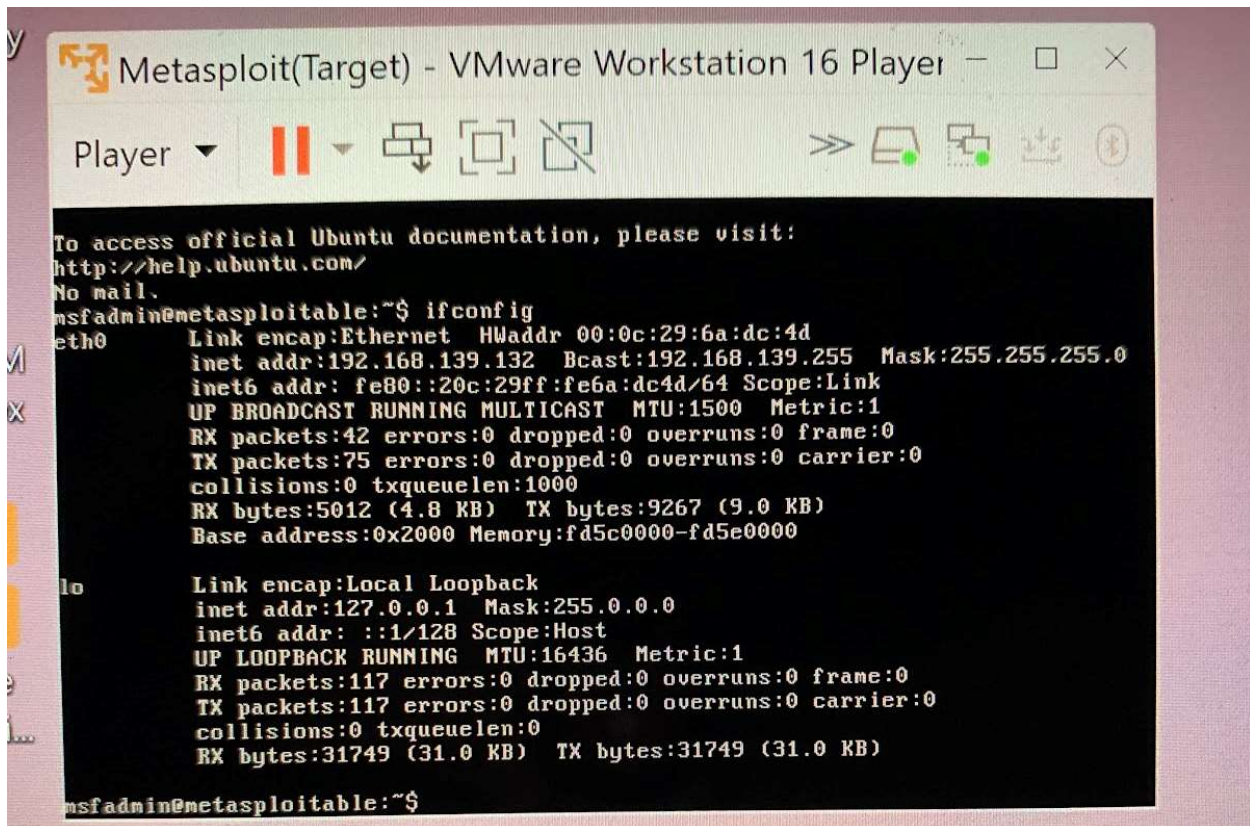
3. Connect the first interface of each VM to the NAT network. Present a simple diagram of the network topology you just created.



Metasploitable

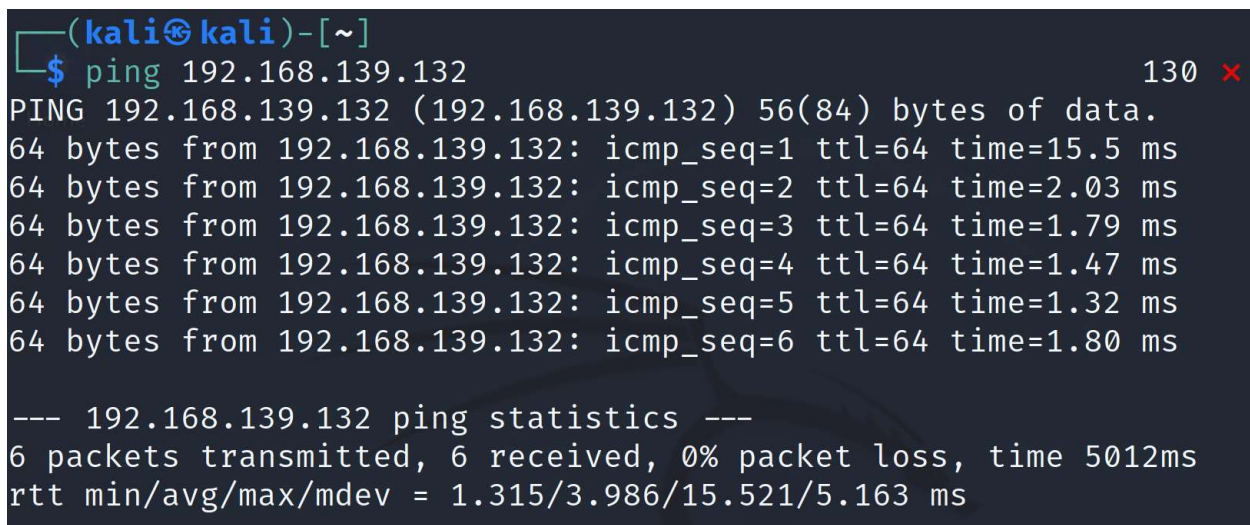
Step 1:

Use ifconfig command in Metasploitable to identify IP address for metasploitable



Step 2:

Open Kali Linux terminal and use command "ping " to check for a connection from metasploitable 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

There's an error with your feed. [Click here](#)

nessus
Essentials

ScansSettings

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

TENABLE

Community


Research

Plugin Release Notes

Tenable News


Scanner

DISCOVERY




Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES



Basic Network Scan
A full system scan suitable for any host.



Advanced Scan
Configure a scan without using any recommendations.

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

The screenshot shows the Nessus Scans Settings page. The left sidebar contains navigation links for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules), TENABLE (Community, Research, Plugin Release Notes), and Tenable News. The main content area has tabs for Settings, Credentials, and Plugins. The Settings tab is active, showing a left-hand menu with categories: BASIC (General, Schedule, Notifications), DISCOVERY, ASSESSMENT, REPORT, and ADVANCED. The right-hand form contains fields for Name (Metasploit(NAT-Network)), Description (This is scan done on target in a NAT network), Folder (My Scans), and Targets (192.168.139.132). At the bottom, there is an 'Upload Targets' section with an 'Add File' link. A red circle highlights the 'Save' button at the bottom left of the form.

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)

The screenshot shows the Nessus Scans page. The left sidebar is the same as in the previous image. The main content area is titled 'My Scans' and includes a search bar and a '3 Scans' indicator. Below is a table listing the scans:

<input type="checkbox"/>	Name	Schedule	Last Modified		
<input type="checkbox"/>	Metasploit-1.1	On Demand	✓ March 16 at 8:30 AM	▶	✕
<input type="checkbox"/>	Metasploit	On Demand	✓ March 16 at 8:17 AM	▶	✕
<input type="checkbox"/>	Metasploit(NAT-Network)	On Demand	📅 N/A	▶	✕

A red circle highlights the play button (▶) for the 'Metasploit(NAT-Network)' scan.

Step 8. Wait for scan to complete

nessus Essentials Scans Settings guest

My Scans Import New Folder New Scan

Search Scans 3 Scans

Name	Schedule	Last Modified
<input type="checkbox"/> Metasploit(NAT-Network)	On Demand	Today at 6:19 PM
<input type="checkbox"/> Metasploit-1.1	On Demand	✓ March 16 at 8:30 AM
<input type="checkbox"/> Metasploit	On Demand	✓ March 16 at 8:17 AM

FOLDERS

- My Scans 1
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules

TENABLE

- Community
- Research
- Plugin Release Notes

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

Step 10. Select the vulnerabilities tab to view vulnerabilities found

Metasploit(NAT-Network) Configure Audit Trail Launch Report Export

[Back to My Scans](#)

Hosts **Vulnerabilities** 73 Remediations 4 Notes 1 VPR Top Threats History 1

Filter Search Vulnerabilities 73 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	SSL (Multiple Issu...	Gain a shell remotely	3
MIXED	Apache Tomcat (...)	Web Servers	3
MIXED	Web Server (Multi...	Web Servers	3
CRITICAL	Bind Shell Backdoor D...	Backdoors	1
CRITICAL	NFS Exported Share In...	RPC	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	Unix Operating System...	General	1
CRITICAL	UnrealIRCd Backdoor ...	Backdoors	1

Scan Details

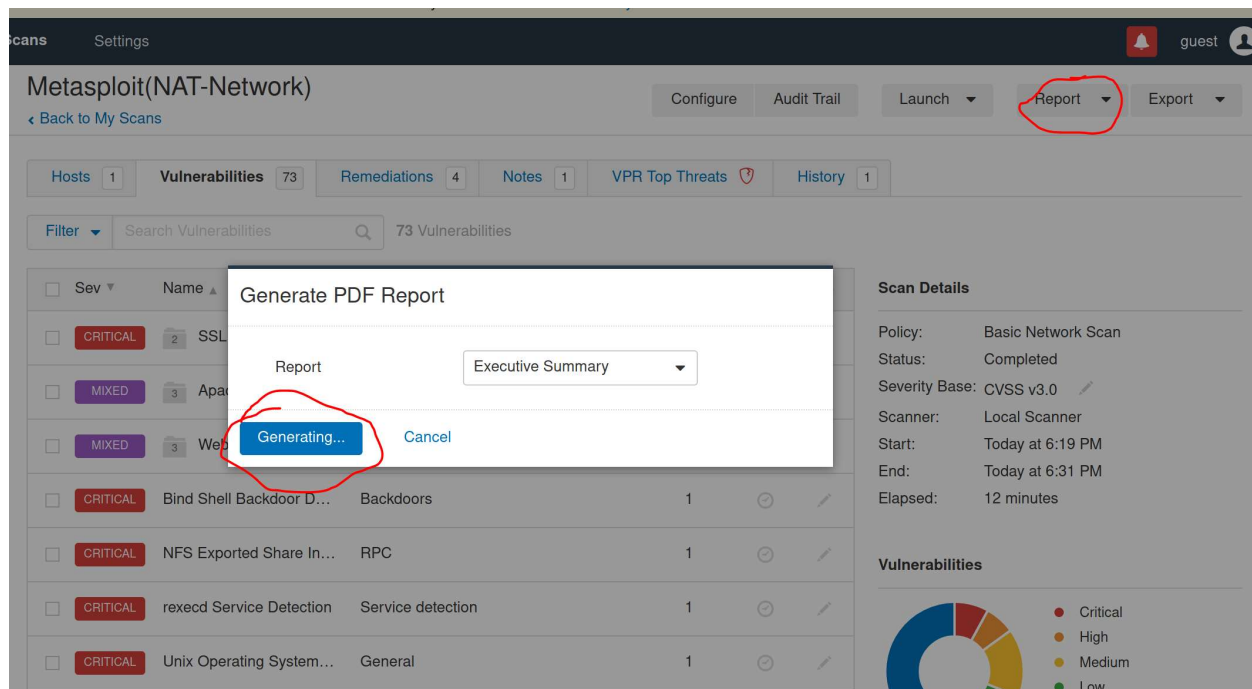
Policy: Basic Network Scan
 Status: Completed
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: Today at 6:19 PM
 End: Today at 6:31 PM
 Elapsed: 12 minutes

Vulnerabilities

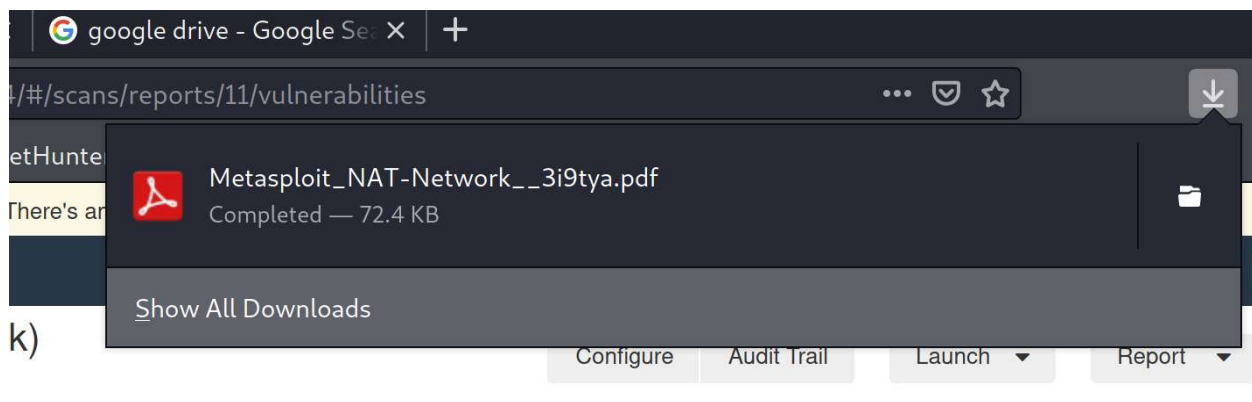
Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Step 11. Download the generated report from Nessus

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

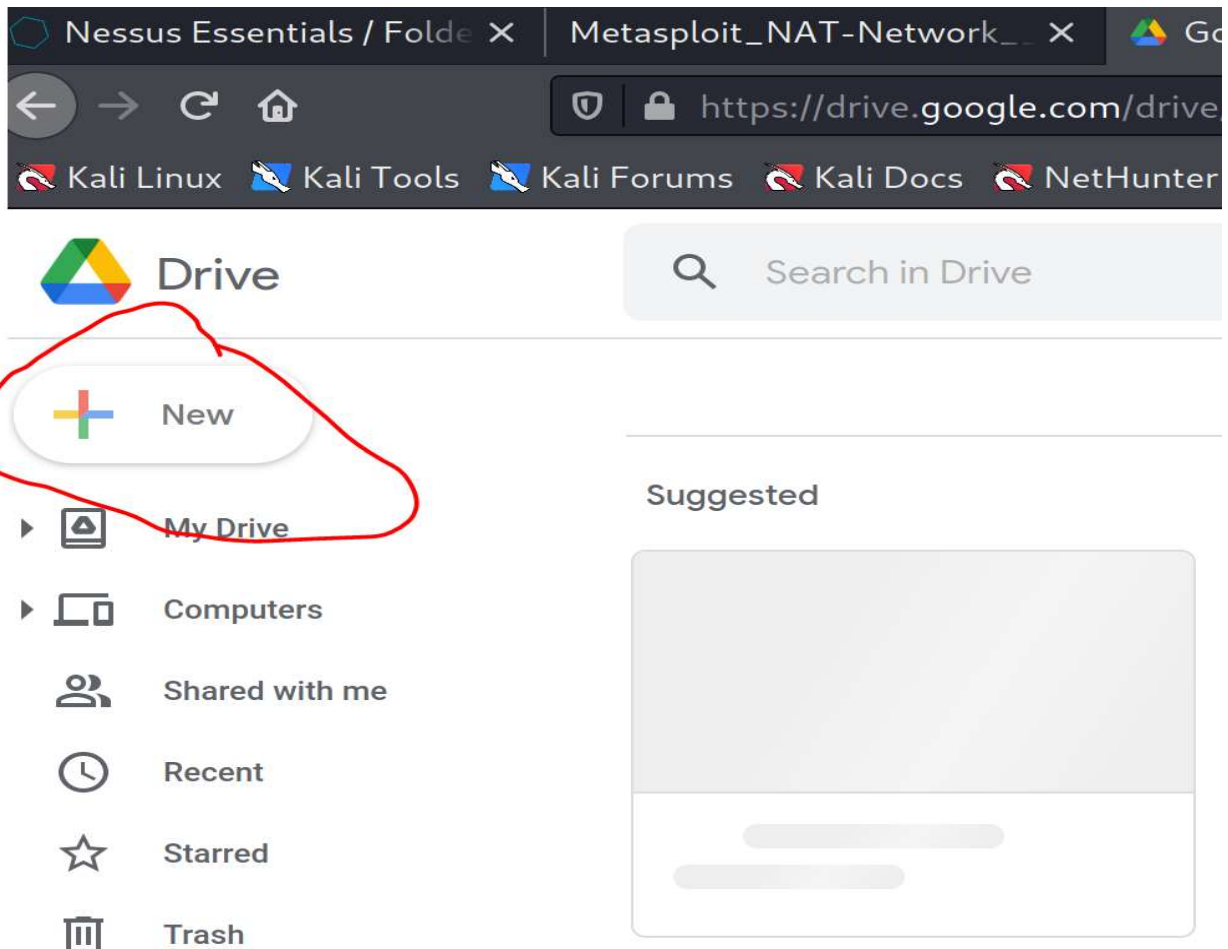


Step 2. Once Report completes save as a file → Go to downloads at top right of screen

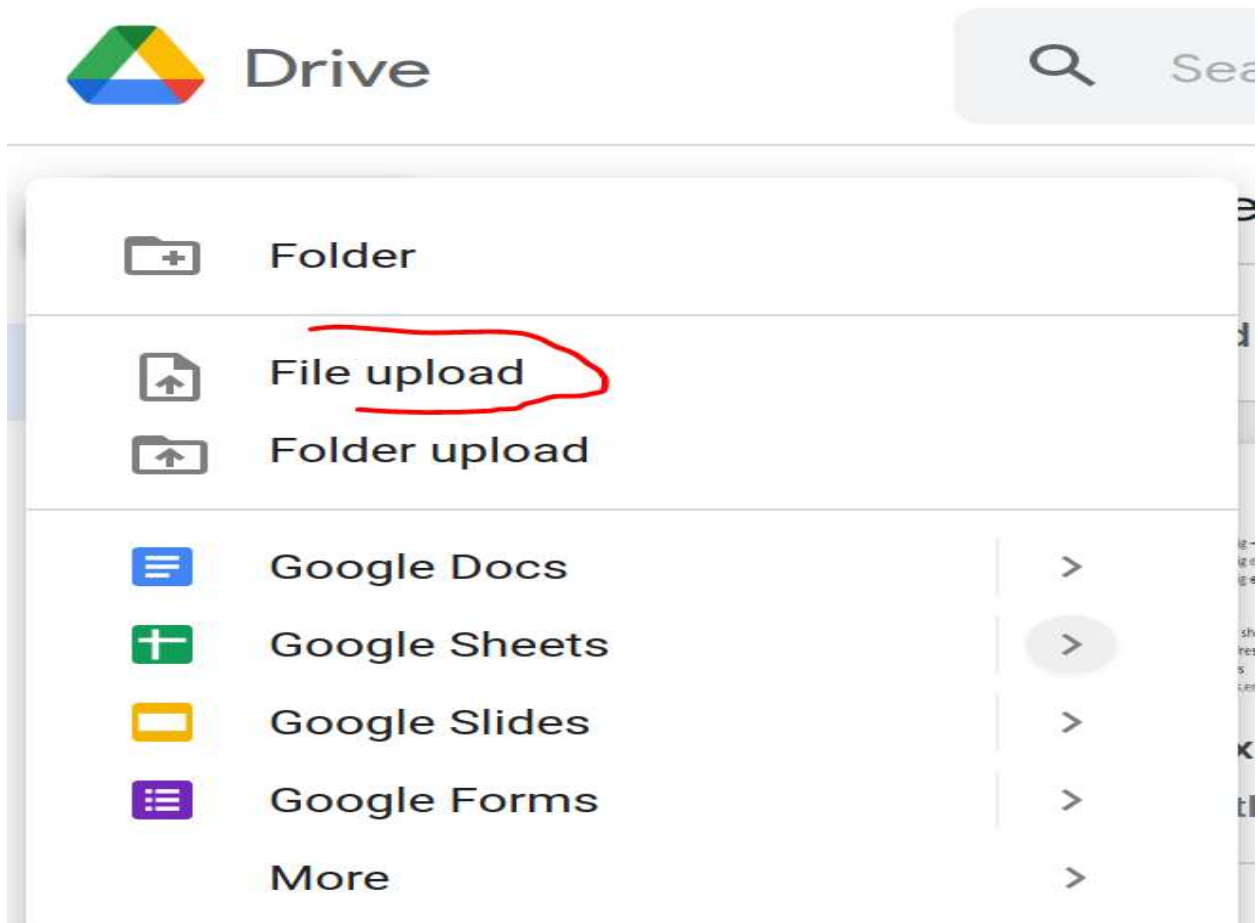


Step 3. Open a cloud storage server to store downloaded report into. In this case we will be using google drive

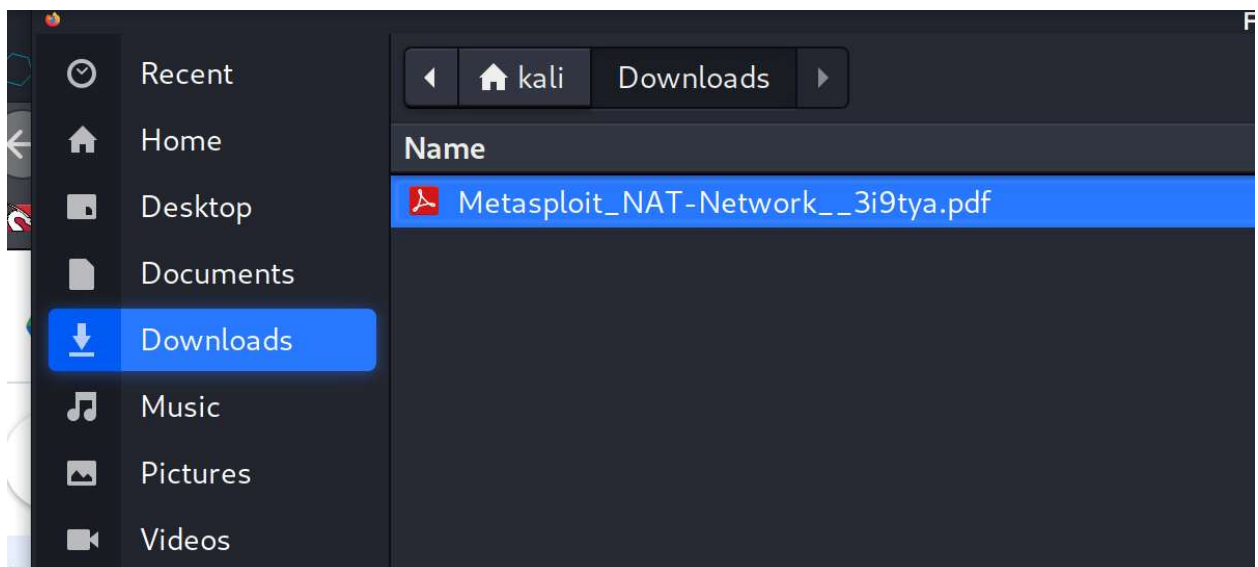
Step 4. Access drive and select the "New" icon



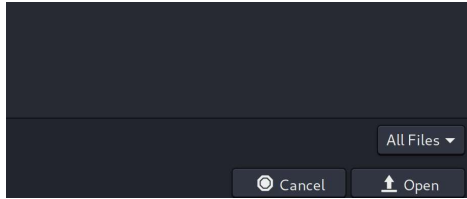
Step 5. Select File upload and



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



Step 7. Select open at bottom right of the screen

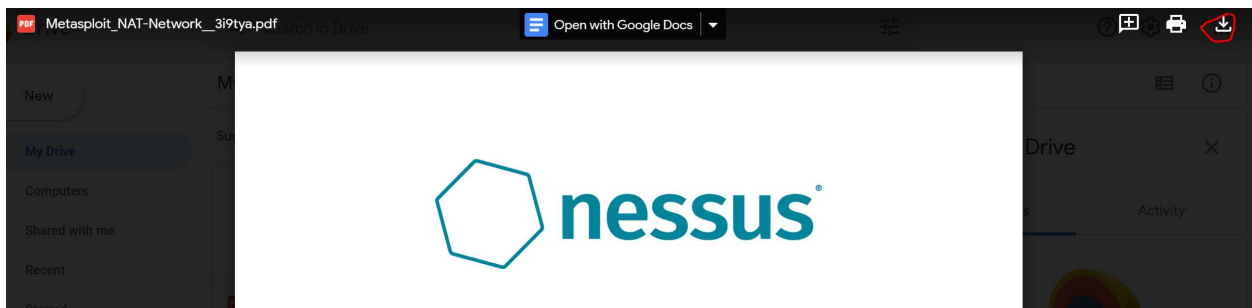


Step 8.

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

```
File Actions Edit View Help
kali@kali: ~/ssl
$ ping 192.168.139.136
PING 192.168.139.136 (192.168.139.136) 56(84) bytes
of data.
64 bytes from 192.168.139.136: icmp_seq=1 ttl=64 tim
e=23.4 ms
64 bytes from 192.168.139.136: icmp_seq=2 ttl=64 tim
e=26.0 ms
64 bytes from 192.168.139.136: icmp_seq=3 ttl=64 tim
e=1.71 ms
64 bytes from 192.168.139.136: icmp_seq=4 ttl=64 tim
e=1.52 ms
^C
--- 192.168.139.136 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, t
ime 3005ms
rtt min/avg/max/mdev = 1.518/13.158/25.982/11.581 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

There's an error with your feed. [Click here](#)


nessus
Essentials

Scans Settings


[Back to Scans](#)


Scanner

DISCOVERY


Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES


Basic Network Scan
A full system scan suitable for any host.


Advanced Scan
Configure a scan without using any recommendations.

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

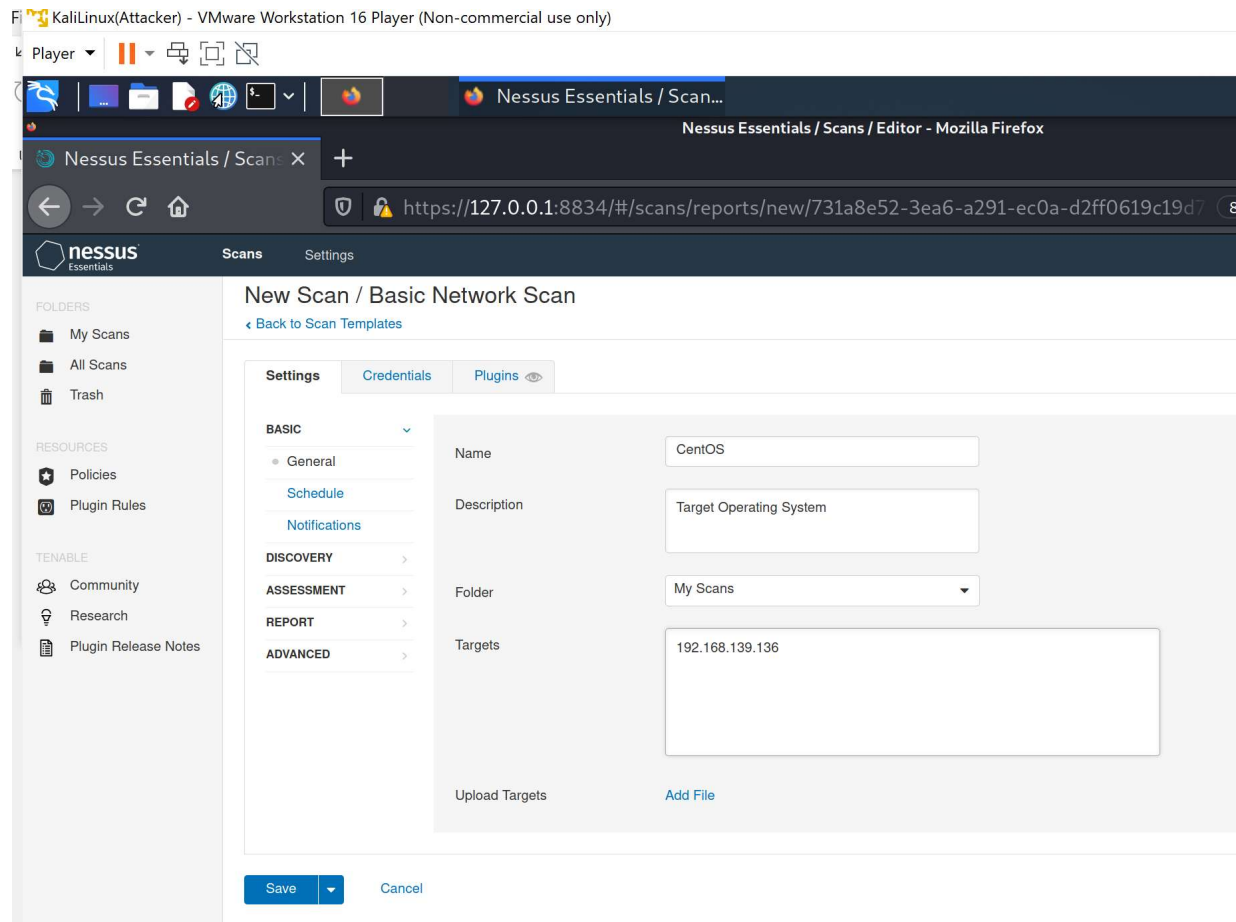
- Policies
- Plugin Rules

TENABLE

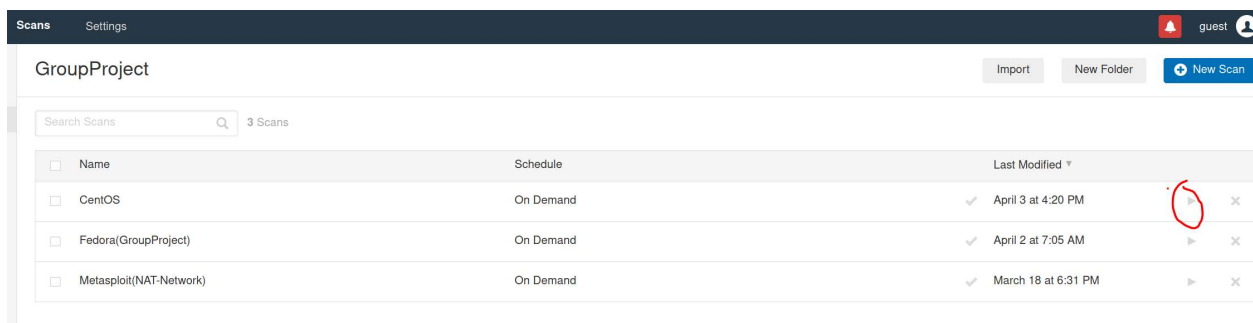
- Community
- Research
- Plugin Release Notes

Tenable News

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

Scans		Settings	guest	
GroupProject		Import	New Folder	New Scan
Search Scans		3 Scans		
<input type="checkbox"/>	Name	Schedule	Last Modified	
<input type="checkbox"/>	CentOS	On Demand	✓ April 3 at 4:20 PM	▶ ×
<input type="checkbox"/>	Fedora(GroupProject)	On Demand	✓ April 2 at 7:05 AM	▶ ×
<input type="checkbox"/>	Metasploit(NAT-Network)	On Demand	✓ March 18 at 6:31 PM	▶ ×

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

Step 10. Select the vulnerabilities tab to view vulnerabilities found

CentOS

Configure

Audit Trail

[Back to GroupProject](#)

Hosts 1

Vulnerabilities 17

Notes 1

VPR Top Threats

History 1

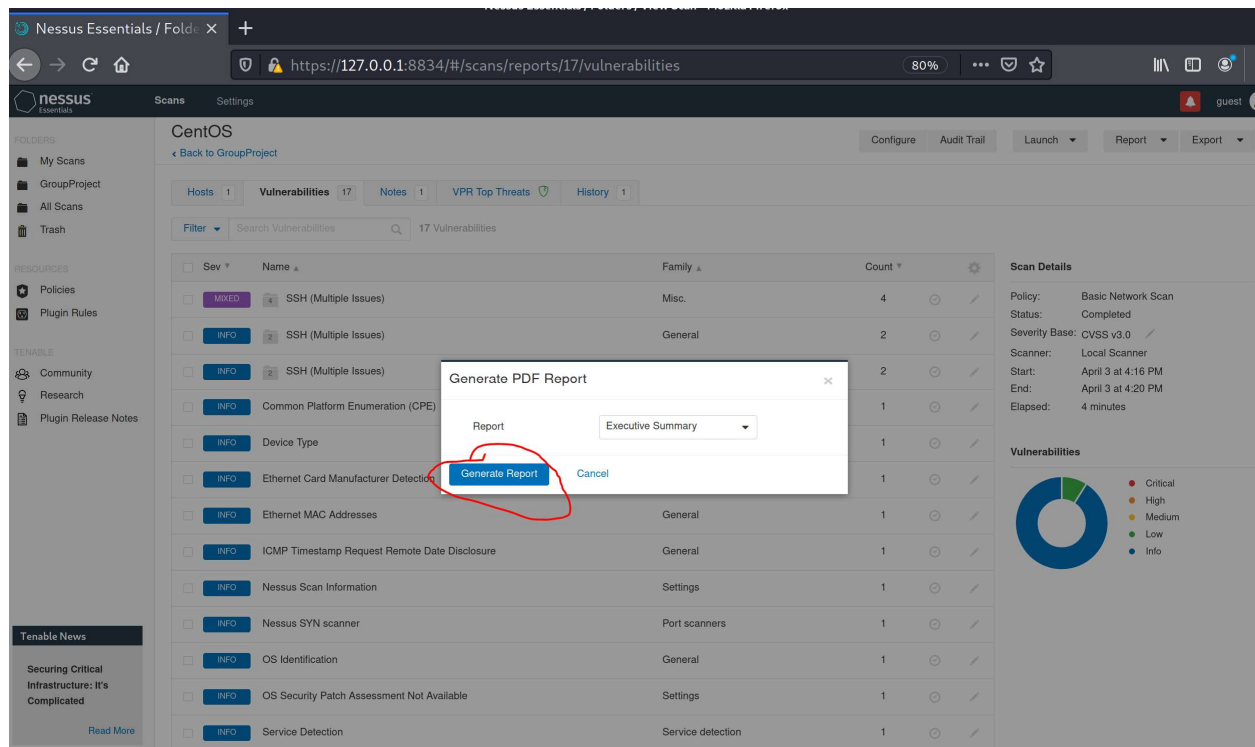
Filter

Search Vulnerabilities

17 Vulnerabilities

<input type="checkbox"/>	Sev	Name	Family	Count	
<input type="checkbox"/>	MIXED	SSH (Multiple Issues)	Misc.	4	
<input type="checkbox"/>	INFO	SSH (Multiple Issues)	General	2	
<input type="checkbox"/>	INFO	SSH (Multiple Issues)	Service detection	2	
<input type="checkbox"/>	INFO	Common Platform Enumeration (CPE)	General	1	
<input type="checkbox"/>	INFO	Device Type	General	1	
<input type="checkbox"/>	INFO	Ethernet Card Manufacturer Detection	Misc.	1	
<input type="checkbox"/>	INFO	Ethernet MAC Addresses	General	1	
<input type="checkbox"/>	INFO	ICMP Timestamp Request Remote Date Disclosure	General	1	
<input type="checkbox"/>	INFO	Nessus Scan Information	Settings	1	
<input type="checkbox"/>	INFO	Nessus SYN scanner	Port scanners	1	
<input type="checkbox"/>	INFO	OS Identification	General	1	
<input type="checkbox"/>	INFO	OS Security Patch Assessment Not Available	Settings	1	

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

```

student@God:~$ ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.139.133  netmask 255.255.255.0  broadcast 192.168.139.255
    inet6 fe80::20c:29ff:feca:2a6e  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:ca:2a:6e  txqueuelen 1000  (Ethernet)
    RX packets 2676  bytes 3742338 (3.5 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 398  bytes 34573 (33.7 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
  
```

Step 2:

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


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

(kali@kali)-[~/ssl]
$ ping 192.168.139.133
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




There's an error with your feed. [Click here](#)

**nessus**
Essentials



ScansSettings

[Back to Scans](#)




FOLDERS

-  My Scans
-  All Scans
-  Trash

RESOURCES

-  Policies
-  Plugin Rules


TENABLE

-  Community
-  Research
-  Plugin Release Notes

Tenable News

Scanner


DISCOVERY



Host Discovery


A simple scan to discover live hosts and open ports.

VULNERABILITIES



Basic Network Scan

A full system scan suitable for any host.



Advanced Scan

Configure a scan without using any recommendations.

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

Fedora(GroupProject) / Configuration

[← Back to Scan Report](#)

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Fedora(GroupProject)

Description

This is a vulnerability scan for a fedora server.
For computer security class Fall 2022

Folder

GroupProject

Targets

192.168.139.133

Upload Targets

Add File

Save

Cancel

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)

Scans

Settings

guest

GroupProject

Import

New Folder

New Scan

Search Scans

3 Scans

<input type="checkbox"/>	Name	Schedule	Last Modified		
<input type="checkbox"/>	CentOS	On Demand	✓ April 3 at 4:20 PM	▶	✕
<input type="checkbox"/>	Fedora(GroupProject)	On Demand	✓ April 2 at 7:05 AM	▶	✕
<input type="checkbox"/>	Metasploit(NAT-Network)	On Demand	✓ March 18 at 6:31 PM	▶	✕

Step 8. Wait for scan to complete

Scans

Settings

guest

GroupProject

Import

New Folder

New Scan

Search Scans

3 Scans

<input type="checkbox"/>	Name	Schedule	Last Modified		
<input type="checkbox"/>	CentOS	On Demand	✓ April 3 at 4:20 PM	▶	✕
<input type="checkbox"/>	Fedora(GroupProject)	On Demand	✓ April 2 at 7:05 AM	▶	✕
<input type="checkbox"/>	Metasploit(NAT-Network)	On Demand	✓ March 18 at 6:31 PM	▶	✕

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

Step 10. Select the vulnerabilities tab to view vulnerabilities found

The screenshot shows the Nessus interface for a scan named 'Fedora(GroupProject)'. The 'Vulnerabilities' tab is selected and highlighted with a red circle. The table below lists the vulnerabilities found:

Sev	Name	Family	Count
MIXED	SSL (Multiple Issues)	General	6
INFO	Service Detection	Service detection	4
INFO	Nessus SYN scanner	Port scanners	3
INFO	HTTP (Multiple Issues)	Web Servers	2
INFO	SSH (Multiple Issues)	Misc.	2
INFO	SSH (Multiple Issues)	Service detection	2
INFO	TLS (Multiple Issues)	Service detection	2
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Ethernet MAC Addresses	General	1
INFO	FTP Server Detection	Service detection	1
INFO	GitLab Web UI Detection	Web Servers	1

The right sidebar shows 'Scan Details' and a 'Vulnerabilities' donut chart. The 'Scan Details' section includes:

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: April 2 at 7:00 AM
- End: April 2 at 7:05 AM
- Elapsed: 6 minutes

The 'Vulnerabilities' donut chart shows the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

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

The screenshot shows the Nessus interface for a scan named 'Fedora(GroupProject)'. The 'Vulnerabilities' tab is selected. A 'Generate PDF Report' dialog box is open, showing the 'Report' dropdown menu with 'Executive Summary' selected. The 'Generate Report' button is highlighted.