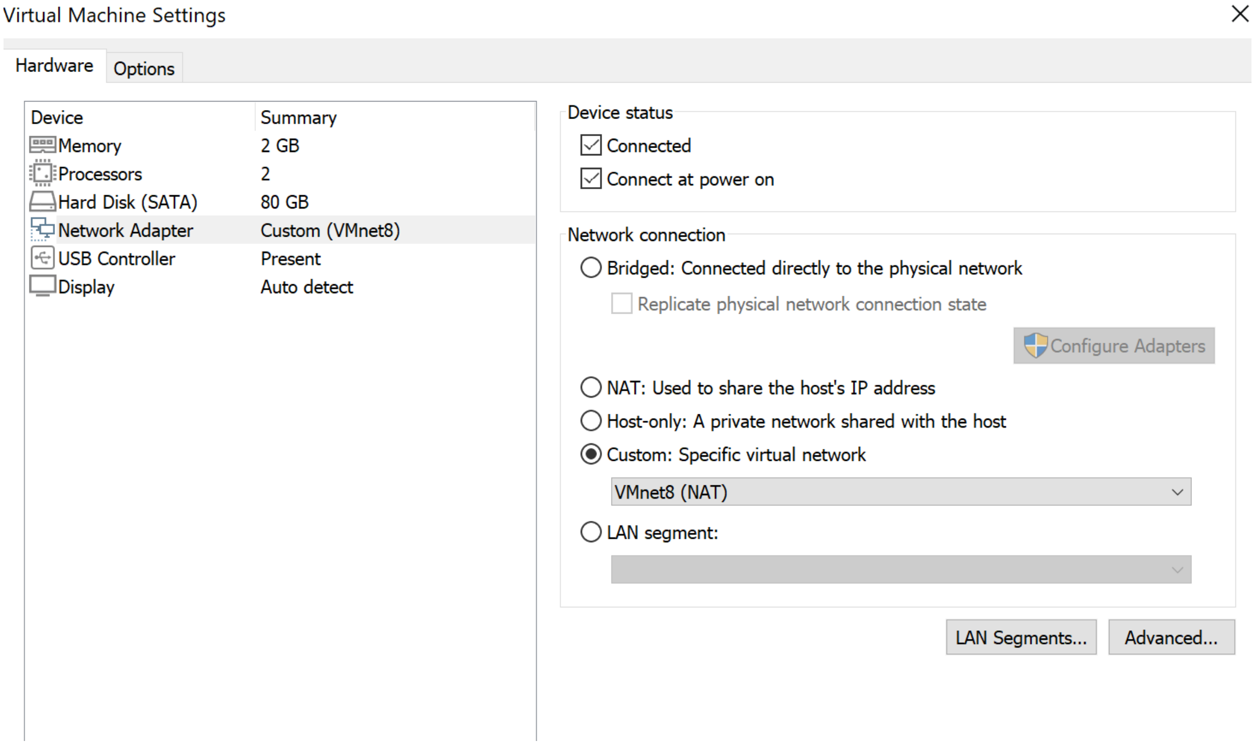
1. Create a NAT network in VirtualBox.

NAT network was created and assigned to Network adapter for both machines



Virtual Machine Settings

Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SATA)	80 GB
Network Adapter	Custom (VMnet8)
USB Controller	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

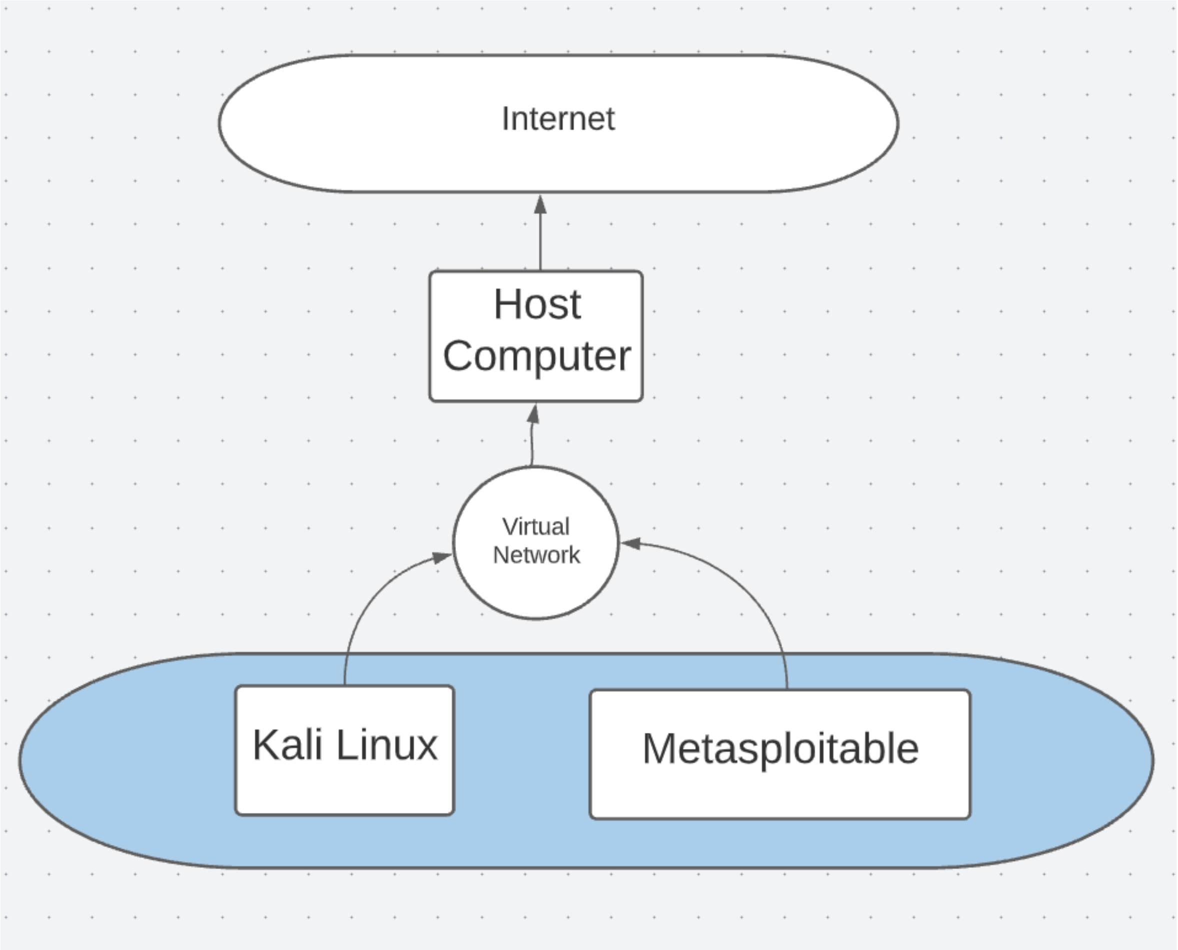
● Custom: Specific virtual network

VMnet8 (NAT)

○ LAN segment:

2. Deploy a VM using each of the provided images.

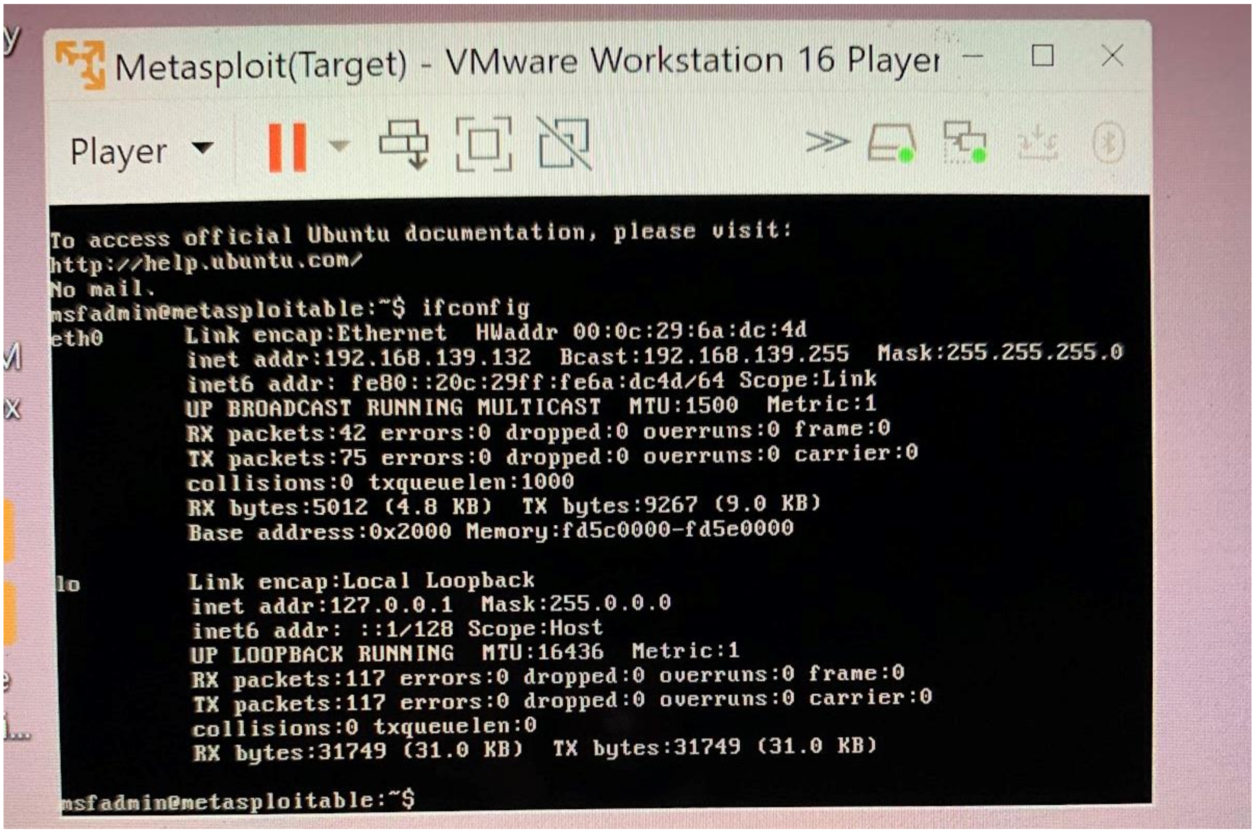
3. Connect the first interface of each VM to the NAT network. Present a simple diagram of the network topology you just created.



4. Access the Kali Linux Image, open a terminal, and ping the IP address assigned to the Metasploitable 2 VM. This step is just required to make sure there is communication between the two VMs. Provide screenshots and explain thoroughly each step.

Step 1:

Use ifconfig command in Metasploitable to identify IP address for metasplotable



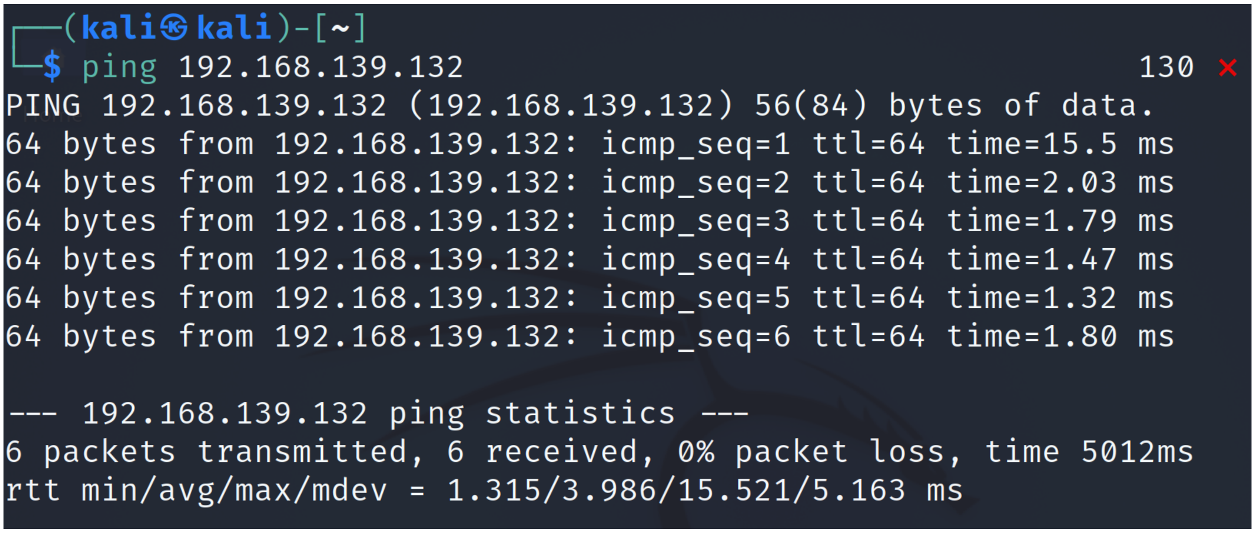
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:6a:dc:4d
          inet addr:192.168.139.132  Bcast:192.168.139.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6a:dc4d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:75 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5012 (4.8 KB)  TX bytes:9267 (9.0 KB)
          Base address:0x2000 Memory:fd5c0000-fd5e0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31749 (31.0 KB)  TX bytes:31749 (31.0 KB)

msfadmin@metasploitable:~$
```

Step 2:

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

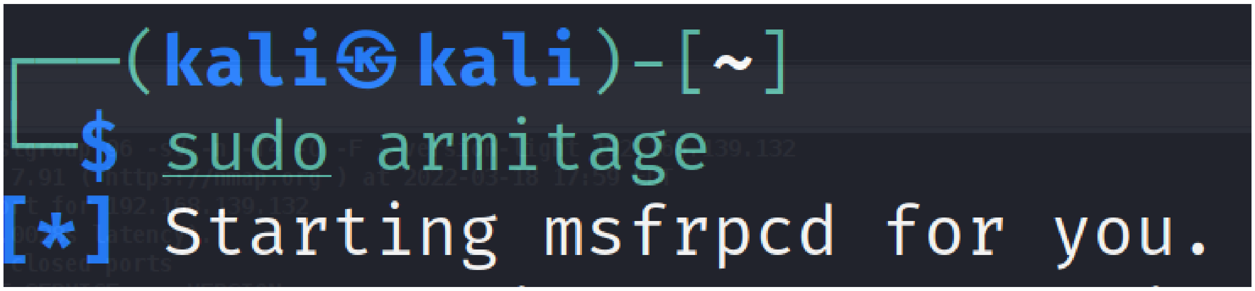


```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.139.132                                          130 ×
PING 192.168.139.132 (192.168.139.132) 56(84) bytes of data.
64 bytes from 192.168.139.132: icmp_seq=1 ttl=64 time=15.5 ms
64 bytes from 192.168.139.132: icmp_seq=2 ttl=64 time=2.03 ms
64 bytes from 192.168.139.132: 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
```

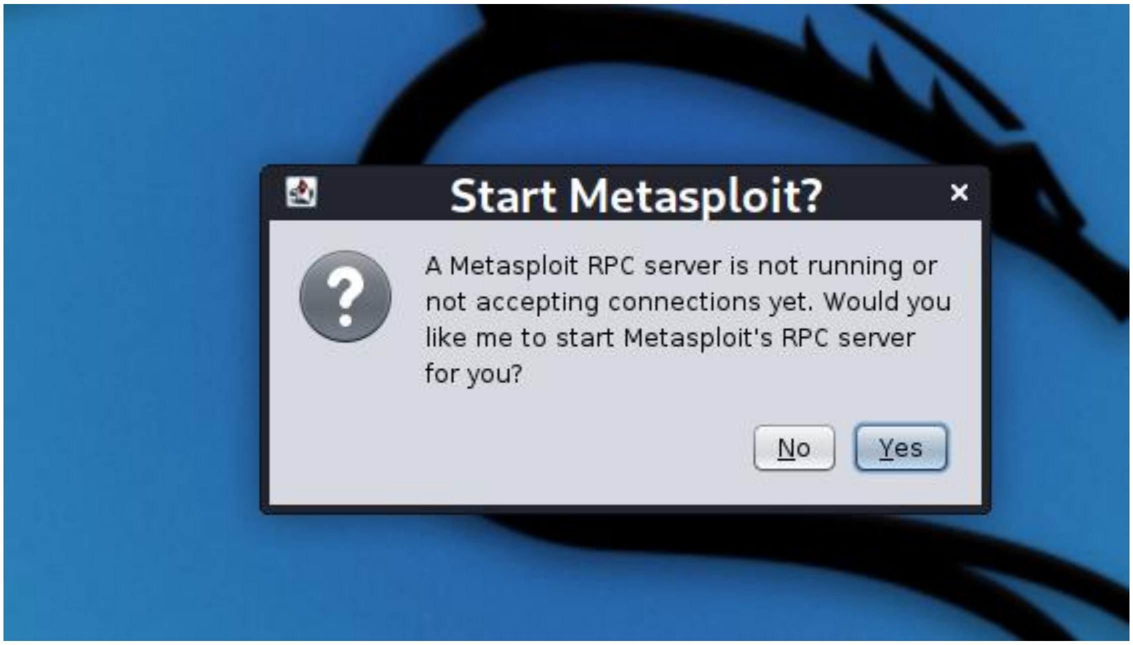
5. Perform a scan using Armitage on the target VM (Metasploitable 2) to ~~**identify the OS, open ports**~~**, and applications running** in this target. Provide screenshots and explain thoroughly each step.

Step1 . Use terminal to Open Armitage via sudo. Armitage is run through the account msfrpcd so it must have route privileges in order to run Nmap and other root restricted operations



```
┌──(kali㉿kali)-[~]
└─$ sudo armitage
[*] Starting msfrpcd for you.
```

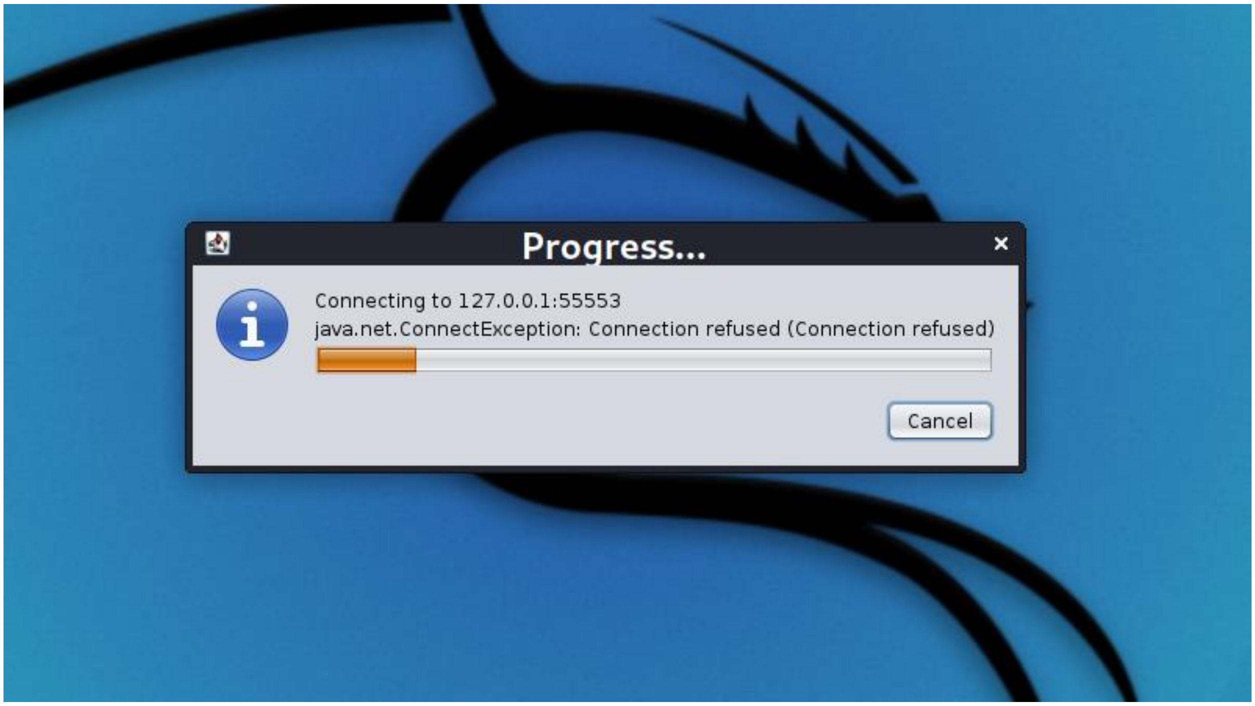
Step 2.Sellect yes option



Start Metasploit?

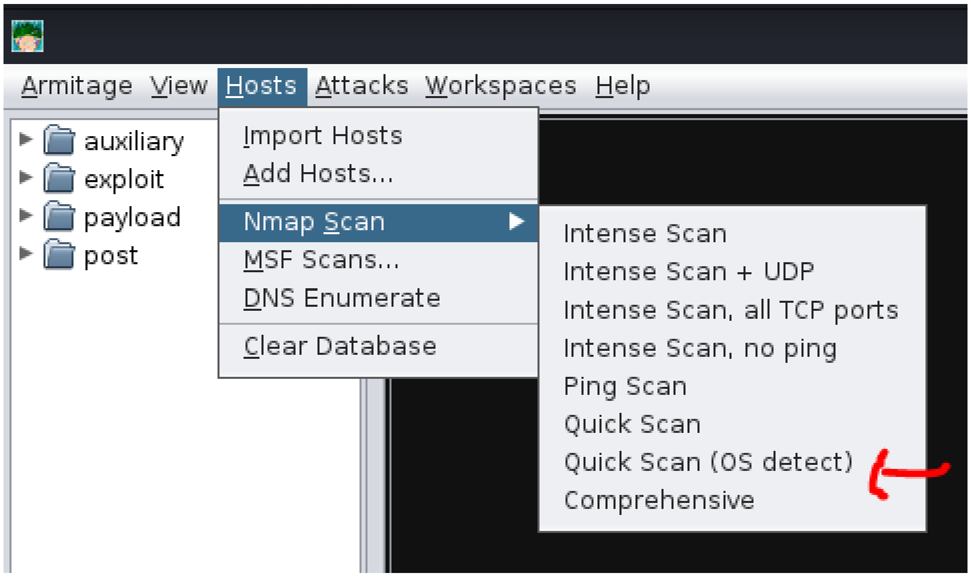
A Metasploit RPC server is not running or not accepting connections yet. Would you like me to start Metasploit's RPC server for you?

Step 3. Wait for initialization

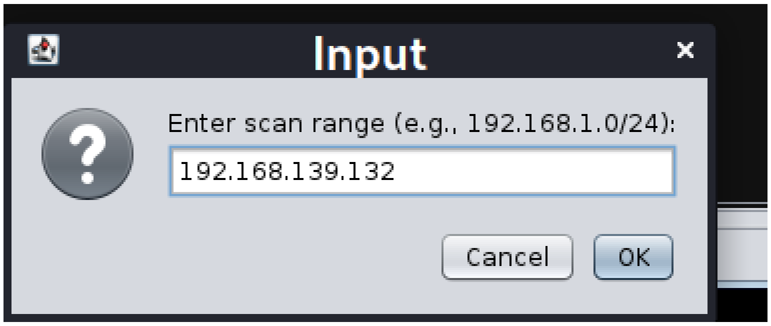


Connecting to 127.0.0.1:55553
java.net.ConnectException: Connection refused (Connection refused)

Step 4. Hosts→Nmap Scan→Quick Scan (OS detect)



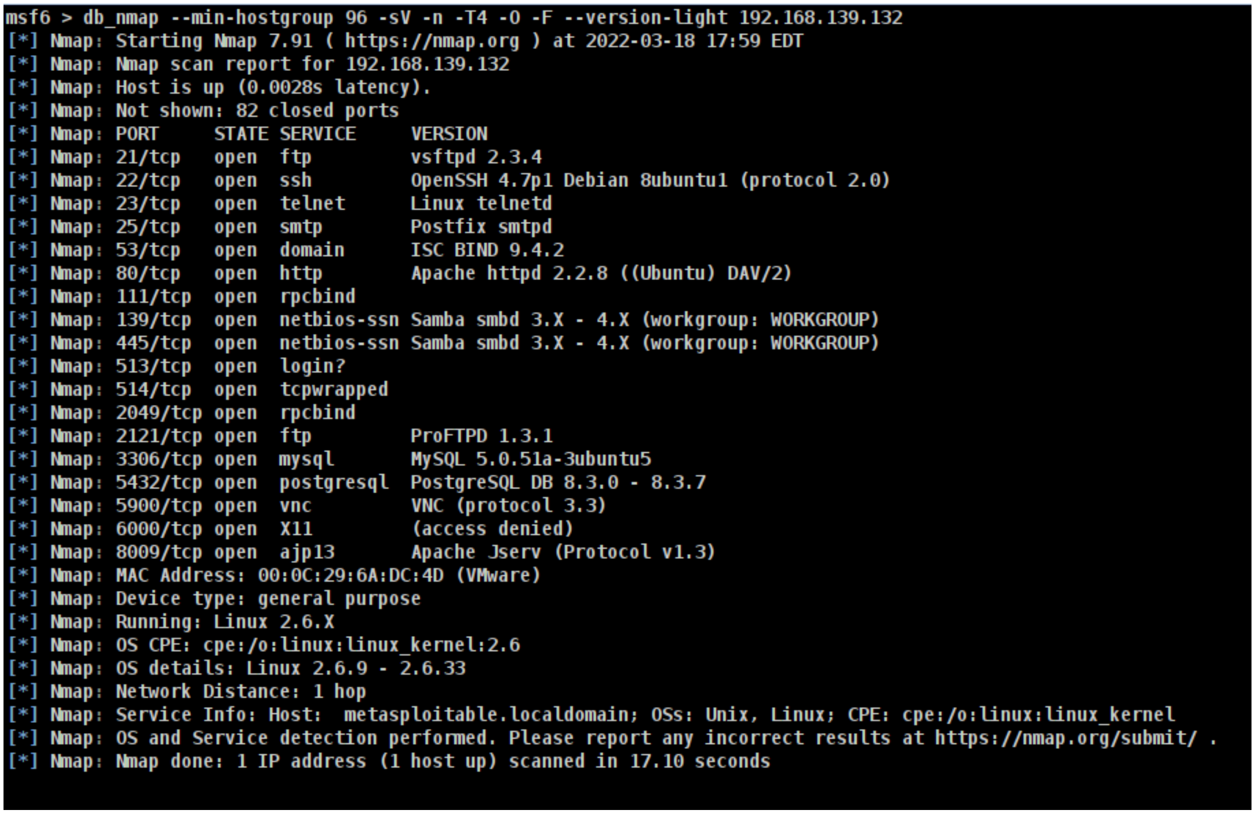
Step 5. Input target OS Ip address and select OK



Enter scan range (e.g., 192.168.1.0/24):

192.168.139.132

Step 6. Nmap scan is performed giving us port and application information on Metasploit

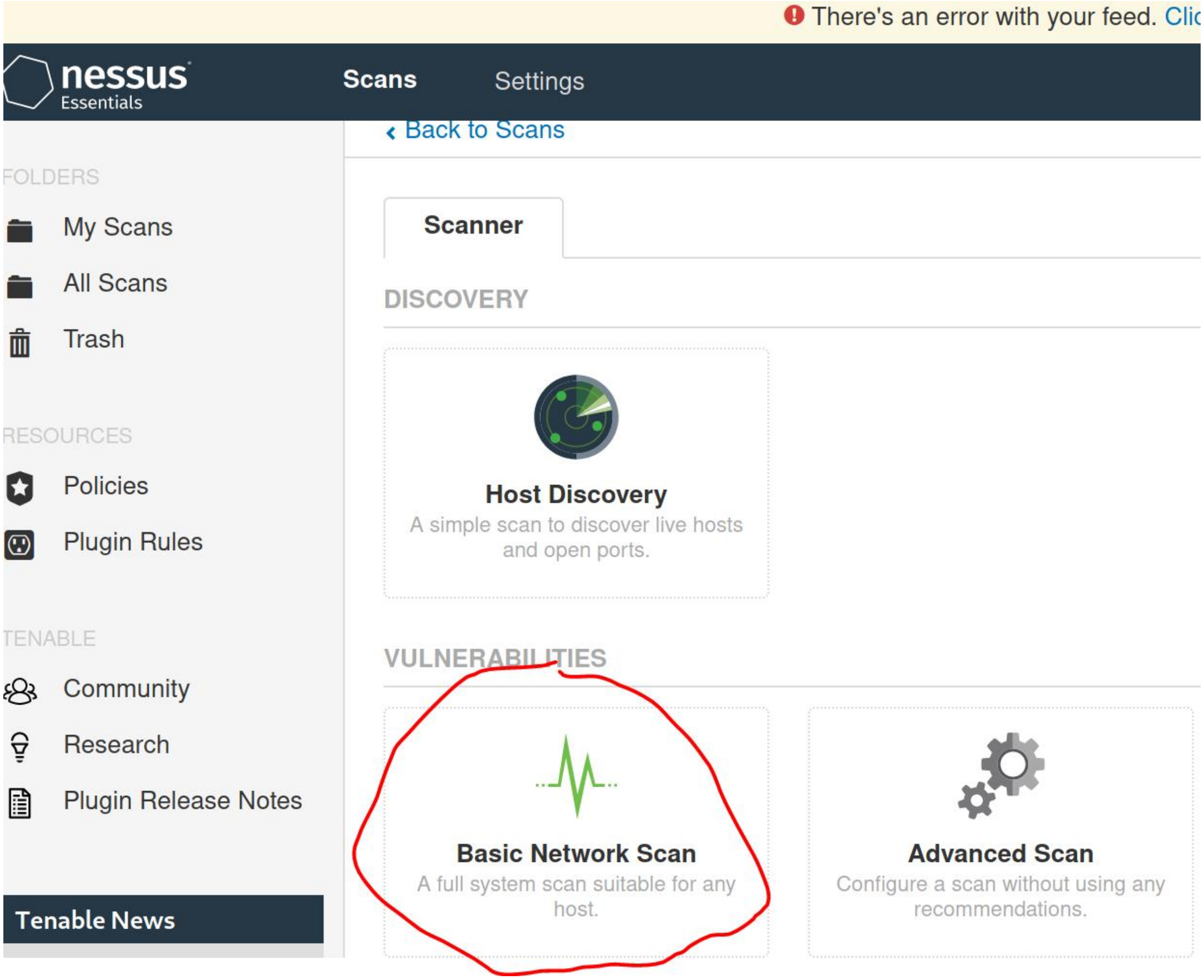


```
msf6 > db_nmap --min-hostgroup 96 -sV -n -T4 -O -F --version-light 192.168.139.132
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-18 17:59 EDT
[*] Nmap: Nmap scan report for 192.168.139.132
[*] Nmap: Host is up (0.0028s latency).
[*] Nmap: Not shown: 82 closed ports
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 21/tcp   open  ftp         vsftpd 2.3.4
[*] Nmap: 22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp   open  telnet      Linux telnetd
[*] Nmap: 25/tcp   open  smtp        Postfix smtpd
[*] Nmap: 53/tcp   open  domain      ISC BIND 9.4.2
[*] Nmap: 80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp  open  rpcbind
[*] Nmap: 139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 513/tcp  open  login?
[*] Nmap: 514/tcp  open  tcpwrapped
[*] Nmap: 2049/tcp open  rpcbind
[*] Nmap: 2121/tcp open  ftp         ProFTPD 1.3.1
[*] Nmap: 3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp open  vnc         VNC (protocol 3.3)
[*] Nmap: 6000/tcp open  X11         (access denied)
[*] Nmap: 8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
[*] Nmap: MAC Address: 00:0C:29:6A:DC:4D (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.9 - 2.6.33
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 17.10 seconds
```

6. Open the Nessus application in the Kali Linux VM.

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

Step 7. Selected Basic Network Scan



There's an error with your feed. Clic

Host Discovery

A simple scan to discover live hosts and open ports.

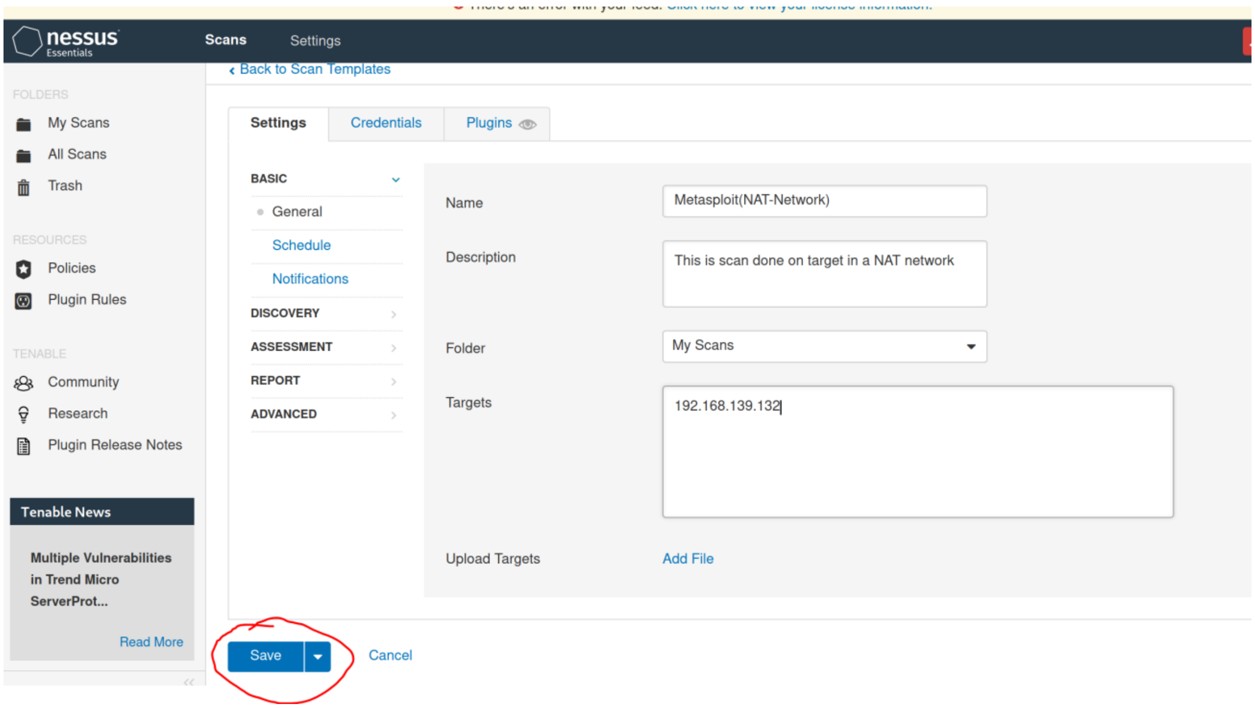
Basic Network Scan

A full system scan suitable for any host.

Advanced Scan

Configure a scan without using any recommendations.

Step 8. Name the target OS. Make a description of target. Input target IP address into “Targets”. Save the scan



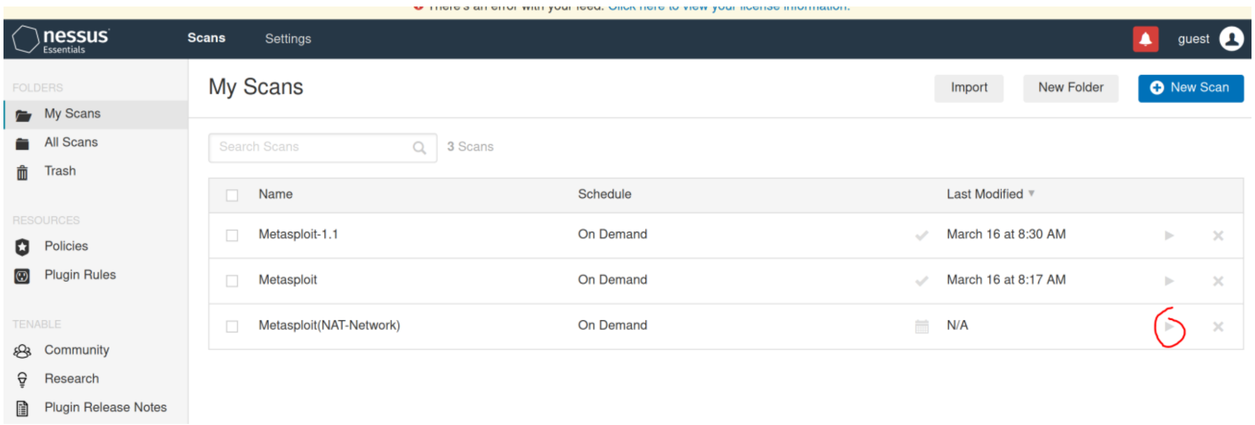
Name: Metasploit(NAT-Network)

Description: This is scan done on target in a NAT network

Folder: My Scans

Targets: 192.168.139.132

Step 9. 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)

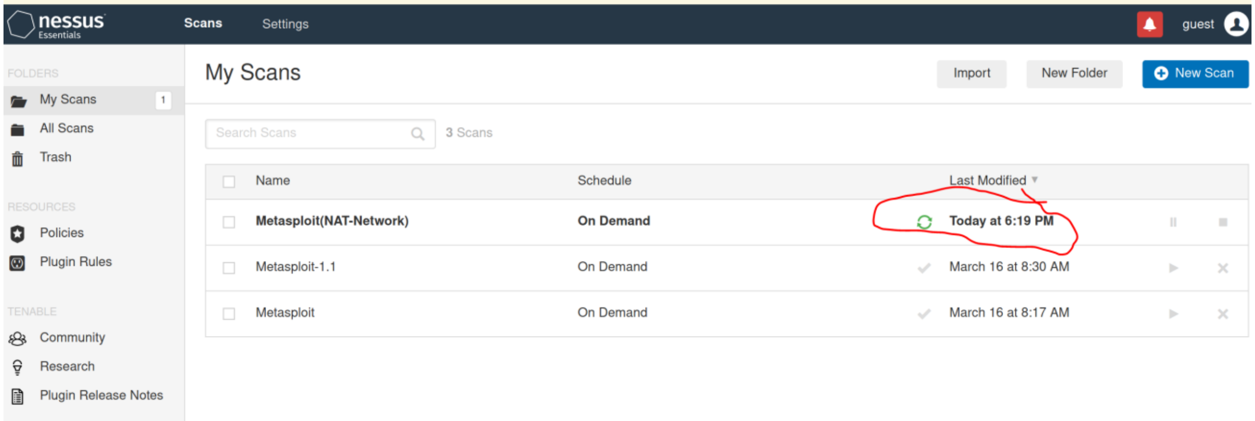


My Scans

3 Scans

	Name	Schedule	Last Modified
□	Metasploit-1.1	On Demand	March 16 at 8:30 AM
□	Metasploit	On Demand	March 16 at 8:17 AM
□	Metasploit(NAT-Network)	On Demand	N/A

Step 10. Wait for scan to complete

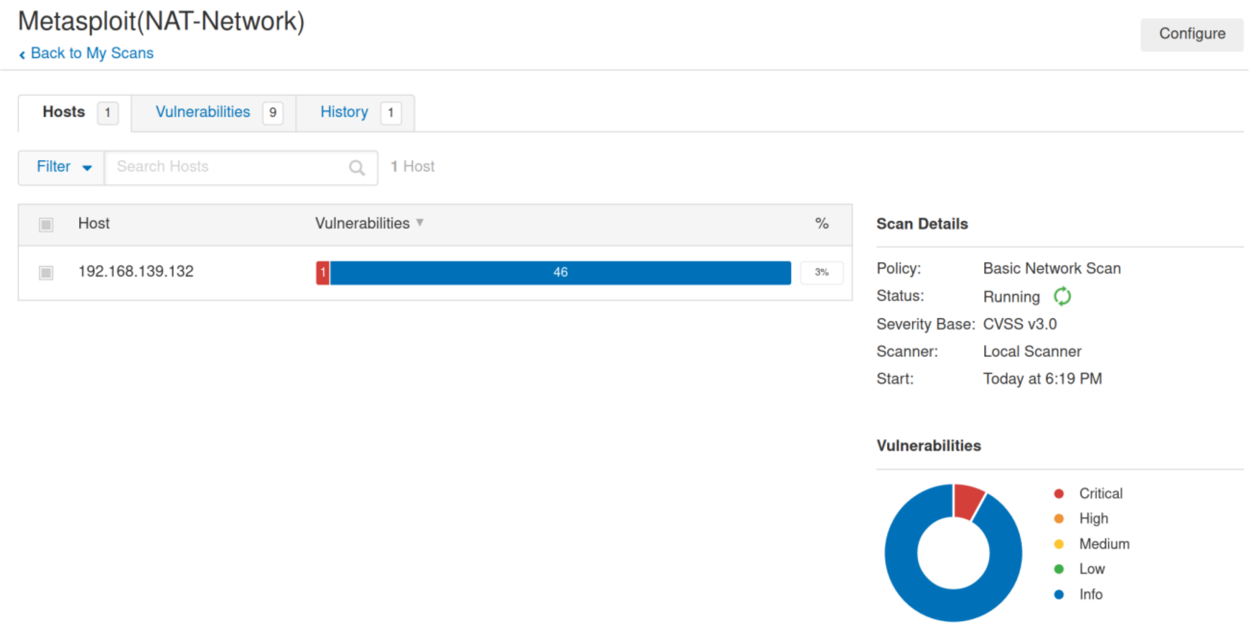


My Scans

3 Scans

□	Name	Schedule	Last Modified ▾
□	**Metasploit(NAT-Network)**	**On Demand**	**Today at 6:19 PM**
□	Metasploit-1.1	On Demand	March 16 at 8:30 AM
□	Metasploit	On Demand	March 16 at 8:17 AM

Step 11. Click on file created to view the progress of scan while it is finding vulnerabilities



Metasploit(NAT-Network)

1 Host

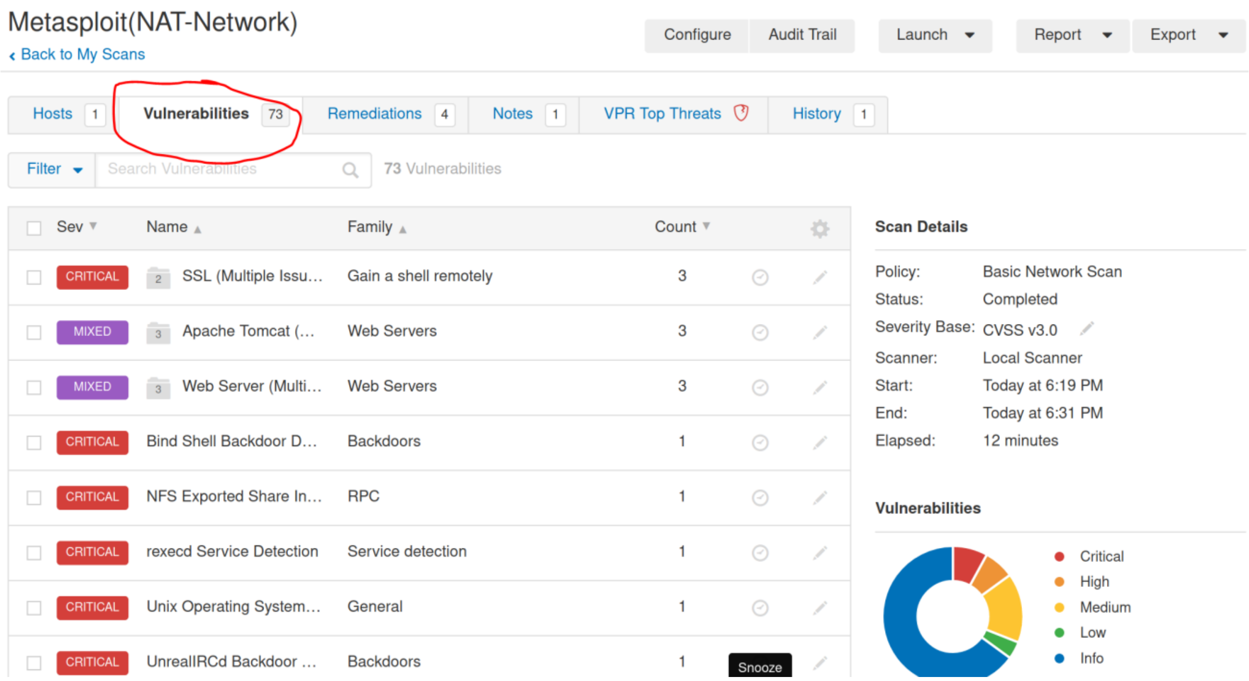
Host	Vulnerabilities ▾	%
192.168.139.132	1 46	3%

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:19 PM

Vulnerabilities

Step 12. Select the vulnerabilities tab to view vulnerabilities found



Metasploit(NAT-Network)

‹ Back to My Scans

Sev	Name	Family	Count
CRITICAL	2 SSL (Multiple Issu…	Gain a shell remotely	3
MIXED	3 Apache Tomcat (…	Web Servers	3
MIXED	3 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

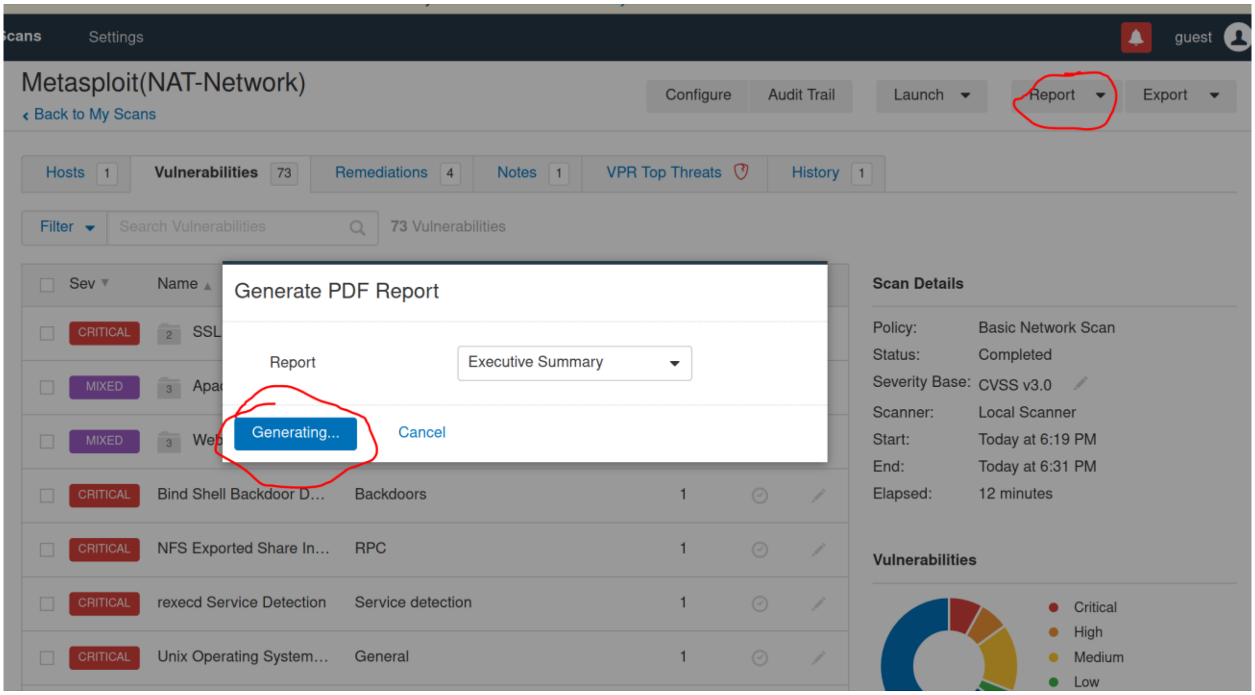
Scan Details

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

8. Download the generated report from Nessus and select 2 vulnerabilities that you would like to exploit.

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



Metasploit(NAT-Network)

‹ Back to My Scans

Generate PDF Report

Report: Executive Summary

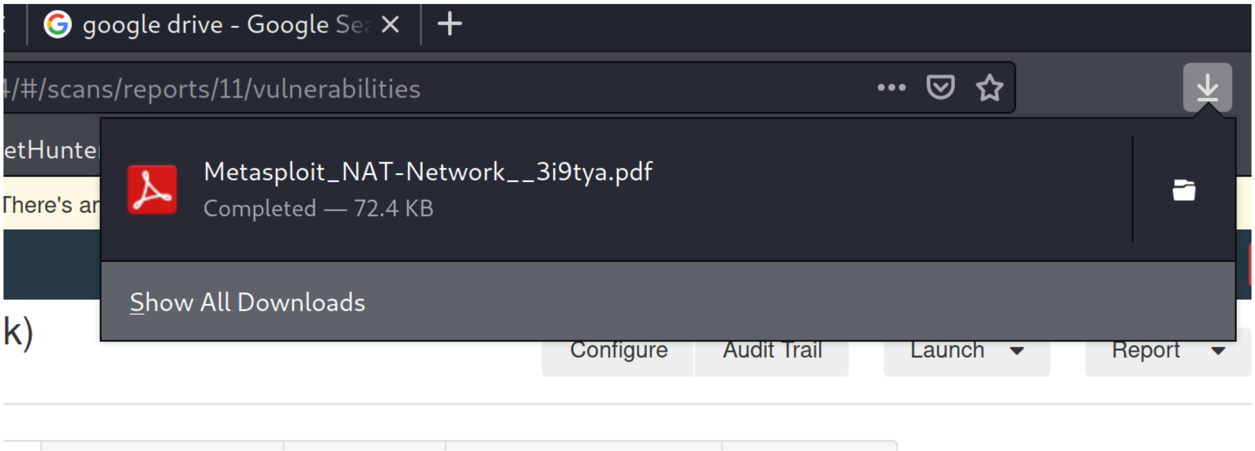
Sev	Name	Family	Count
CRITICAL	2 SSL		
MIXED	3 Apa		
MIXED	3 We		
CRITICAL	Bind Shell Backdoor D…	Backdoors	1
CRITICAL	NFS Exported Share In…	RPC	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	Unix Operating System…	General	1

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

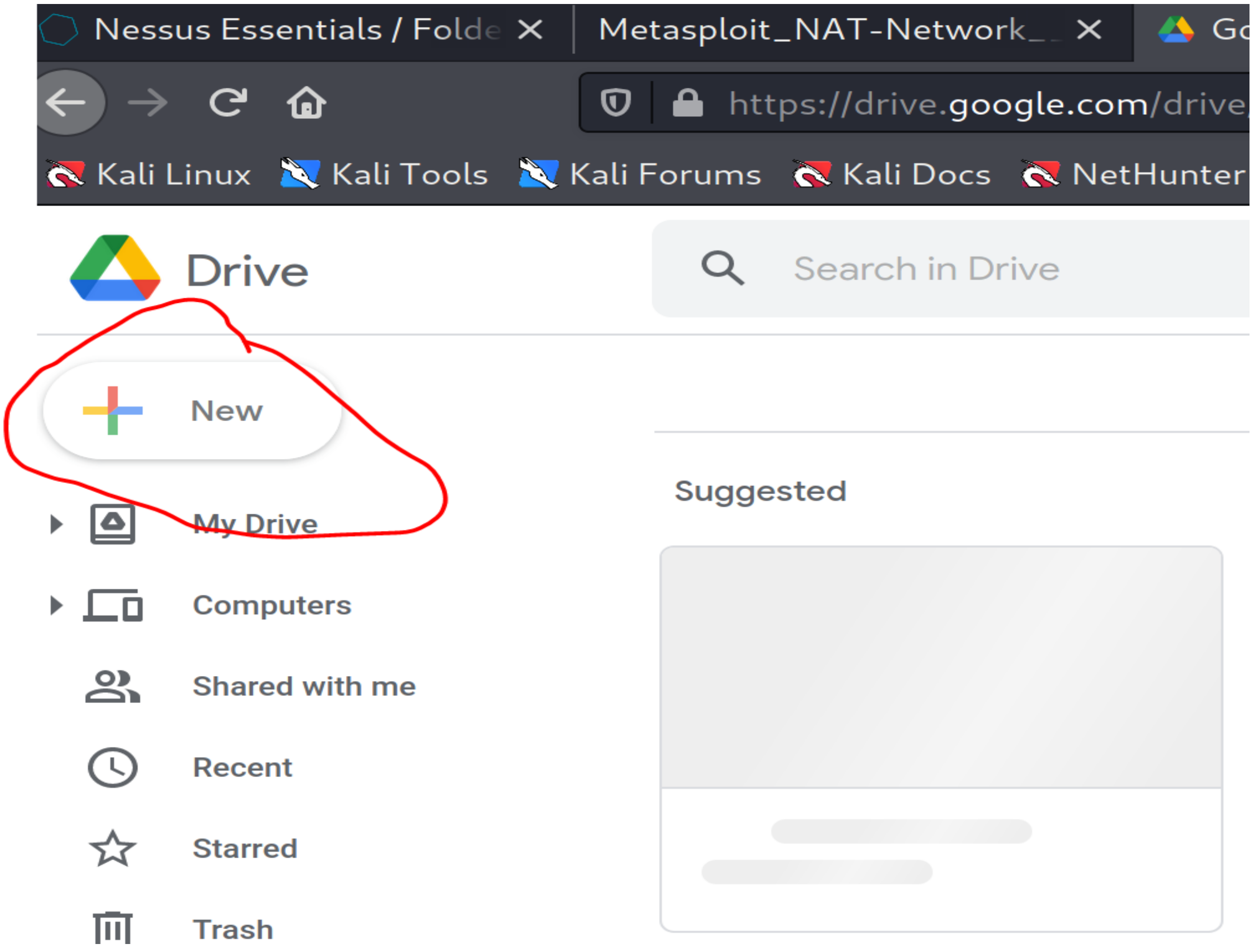
Step 2. Once Report completes save as a file→Go to downloads at top right of screen



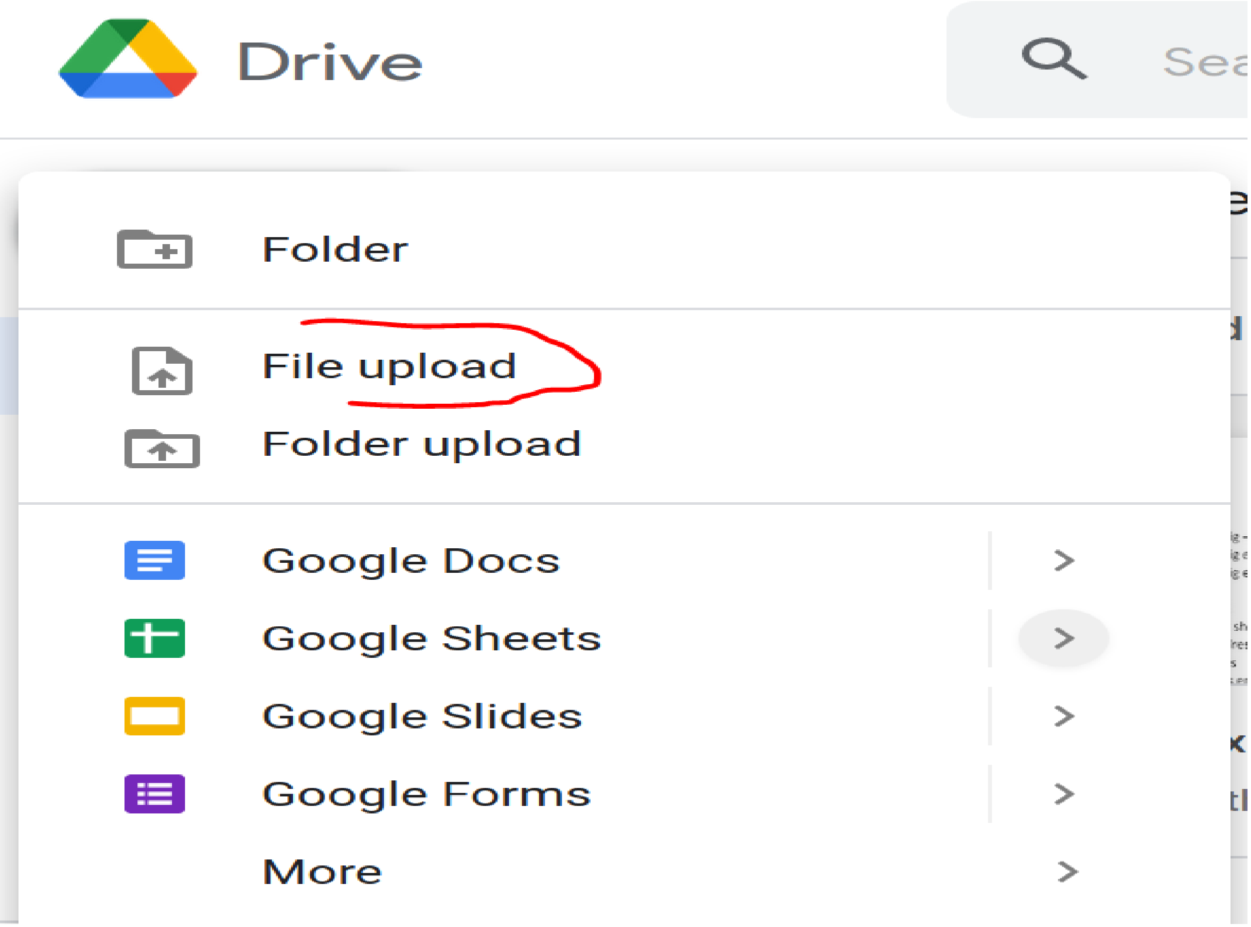
Metasploit_NAT-Network__3i9tya.pdf
Completed — 72.4 KB

Step 2. Open a cloud storage server to store downloaded report into. In theis case we will be using google drive

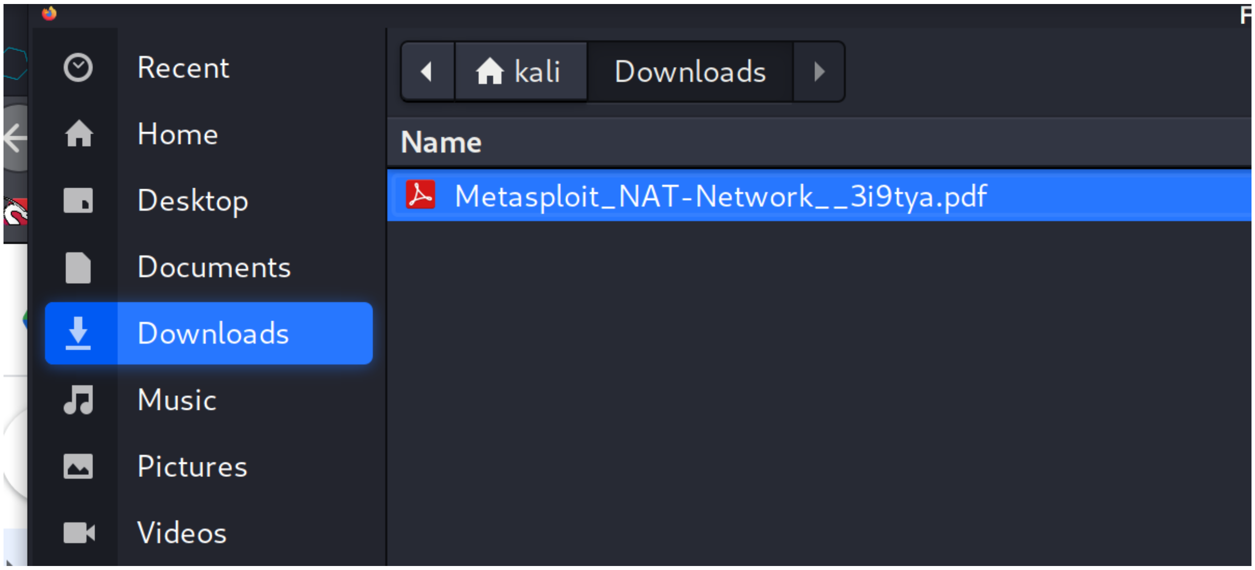
Step 3.Access drive and select the “New” icon



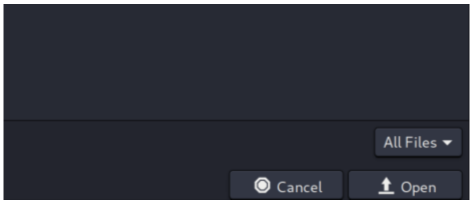
Step 4. Select File upload and



Step 5. Navigate to downloads and select Metaspliot or Report PDF that was downloaded from nessus page



Step 6. Select open at bottom right of the screen



Step 7.

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.