Abdelkader Shaaban

Metasploitable VM

Optional

CyberSecPro

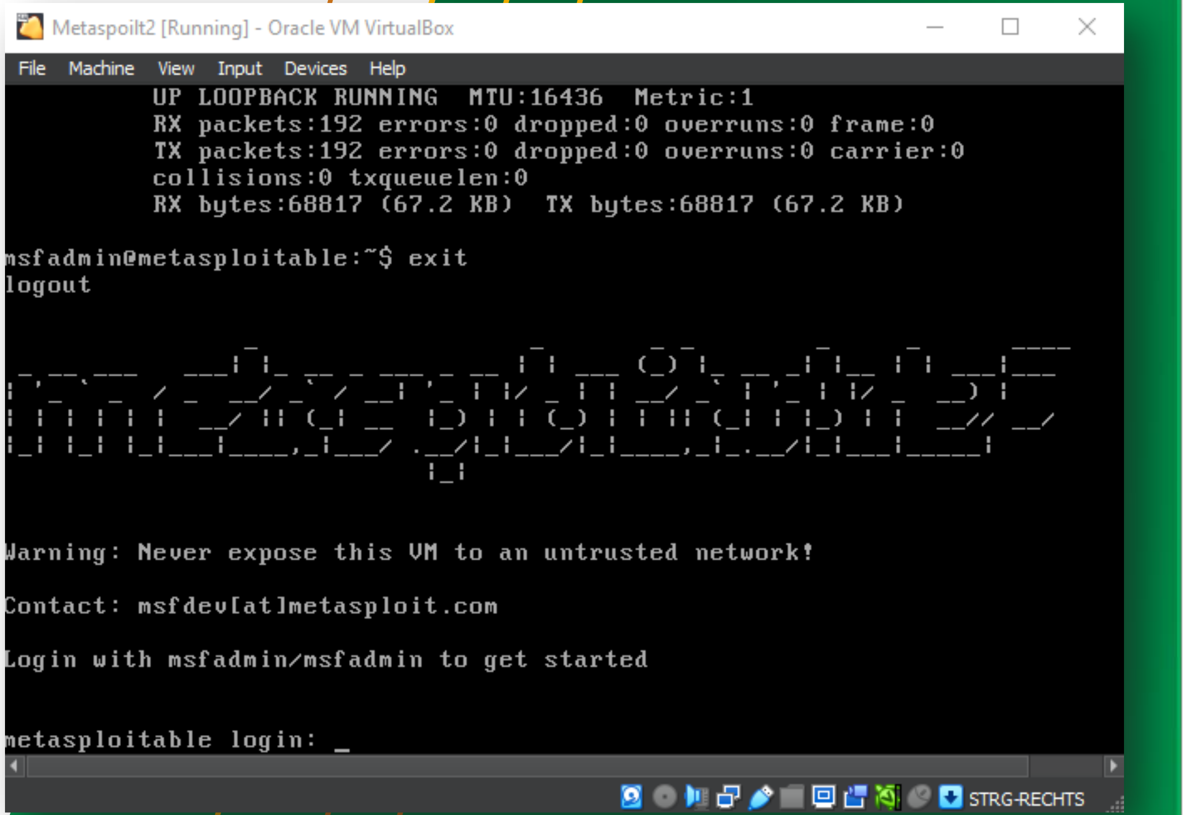
cc BY NC SA

What is Metasploitable?

The world's most widely used penetration testing framework.

You can download it from the following link.

[Metasploitable 2 | Metasploit Documentation (rapid7.com)]



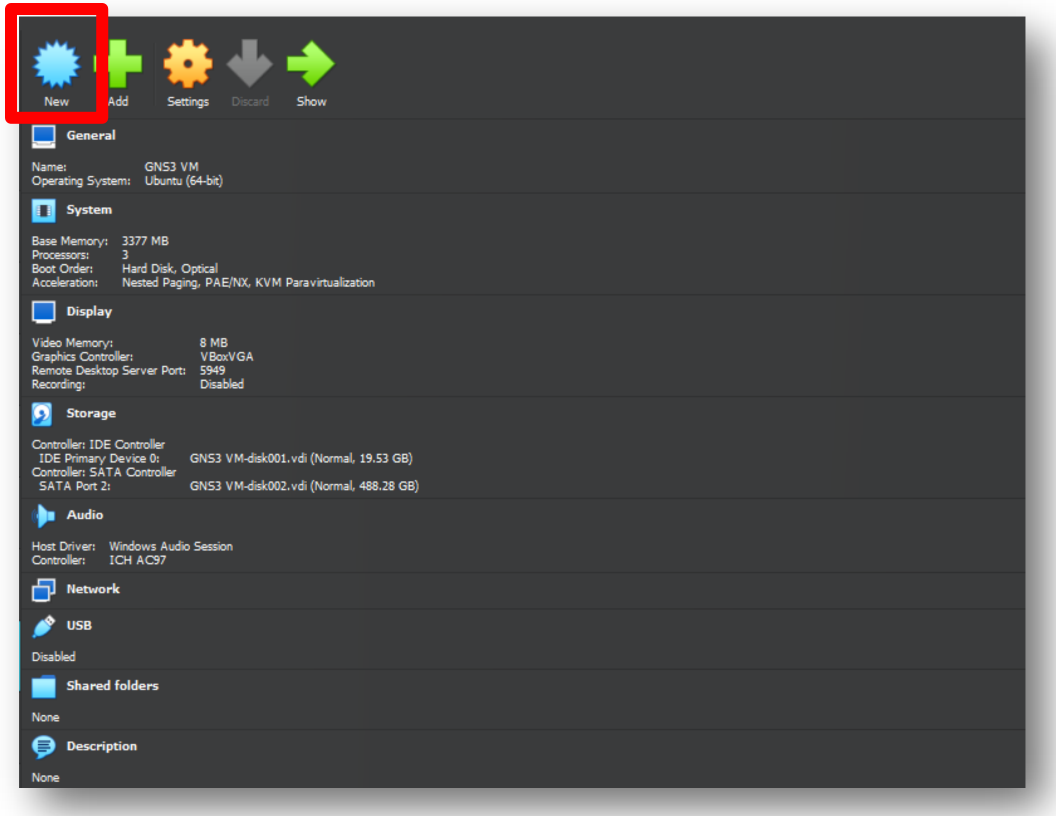
```
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:192 errors:0 dropped:0 overruns:0 frame:0
          TX packets:192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:68817 (67.2 KB)  TX bytes:68817 (67.2 KB)

msfadmin@metasploitable:~$ exit
logout

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

CyberSecPro

BY NC SA

https://www.metasploit.com

Installing Metasploitable



General

Name: GNS3 VM
Operating System: Ubuntu (64-bit)

System

Base Memory: 3377 MB
Processors: 3
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 8 MB
Graphics Controller: VBoxVGA
Remote Desktop Server Port: 5949
Recording: Disabled

Storage

Controller: IDE Controller
IDE Primary Device 0: GNS3 VM-disk001.vdi (Normal, 19.53 GB)
Controller: SATA Controller
SATA Port 2: GNS3 VM-disk002.vdi (Normal, 488.28 GB)

Audio

Host Driver: Windows Audio Session
Controller: ICH AC97

Network

USB

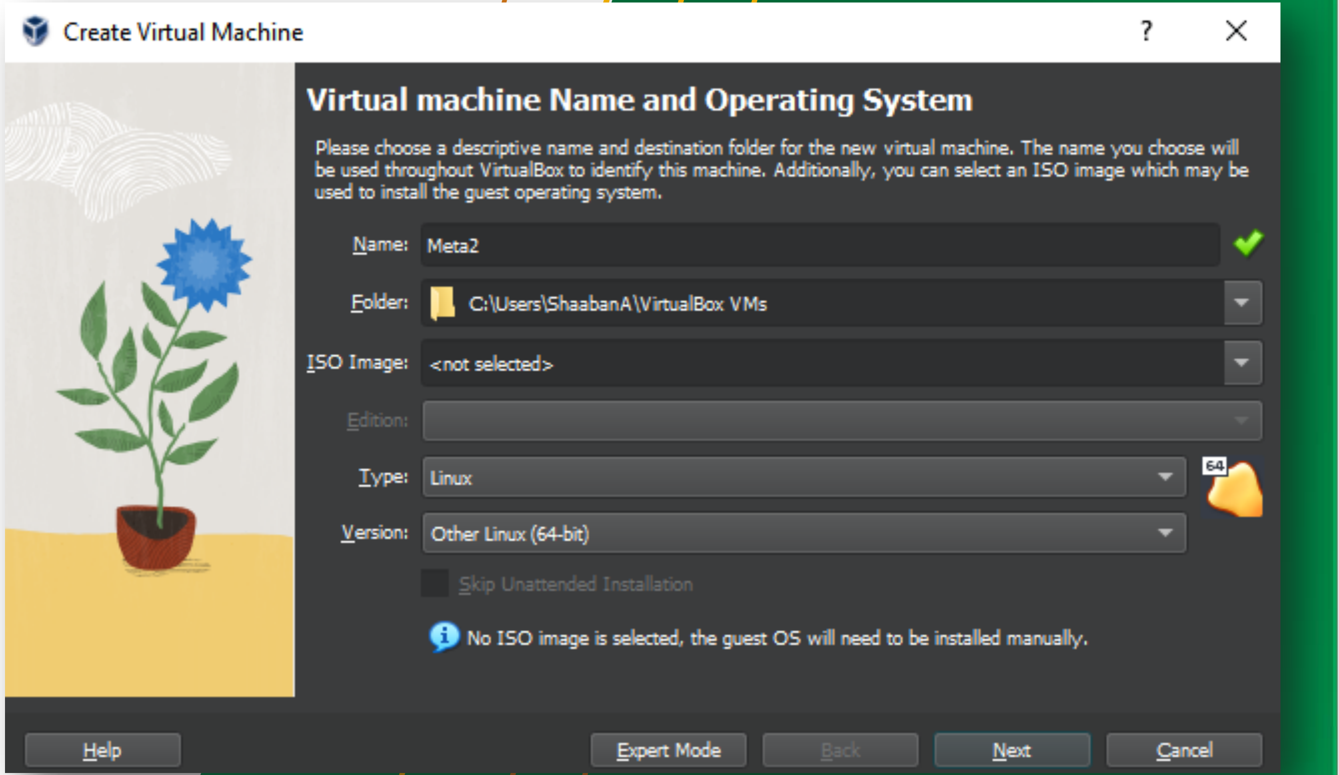
Disabled

Shared folders

None

Description

None



Virtual machine Name and Operating System

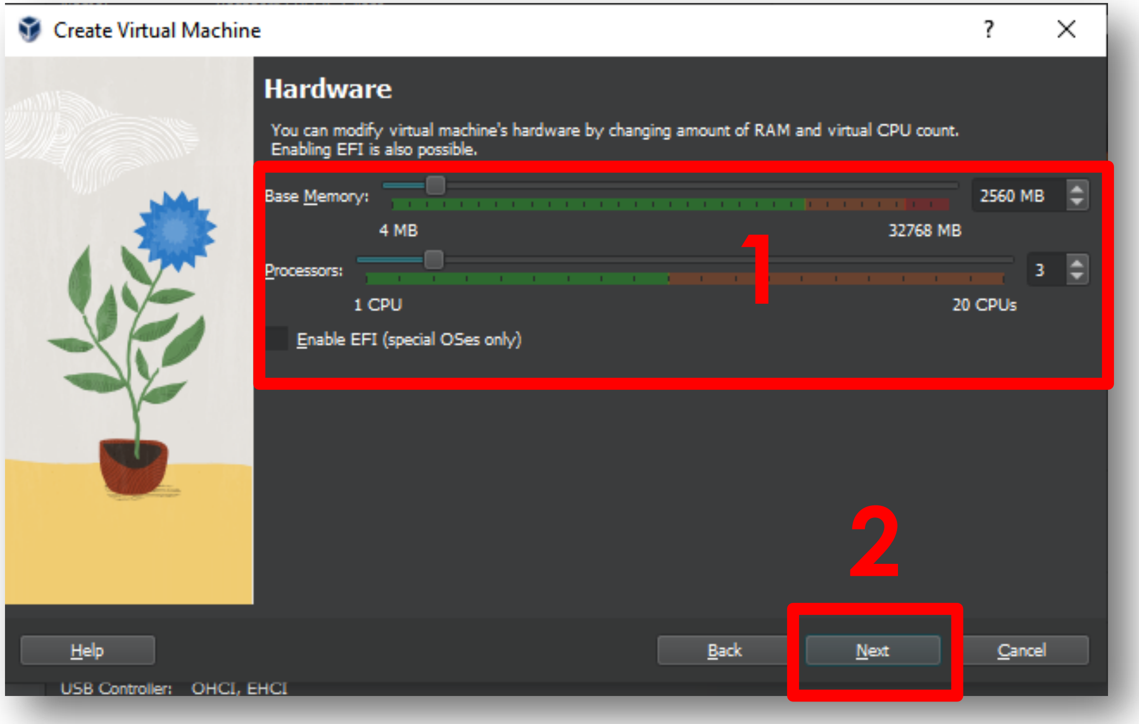
Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: Meta2 ✓
Folder: C:\Users\ShaabanA\VirtualBox VMs
ISO Image: <not selected>
Edition:
Type: Linux
Version: Other Linux (64-bit)
□ Skip Unattended Installation

No ISO image is selected, the guest OS will need to be installed manually.

CyberSecPro
CC BY NC SA

Installing Metasploitable



Create Virtual Machine

Hardware

You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 2560 MB

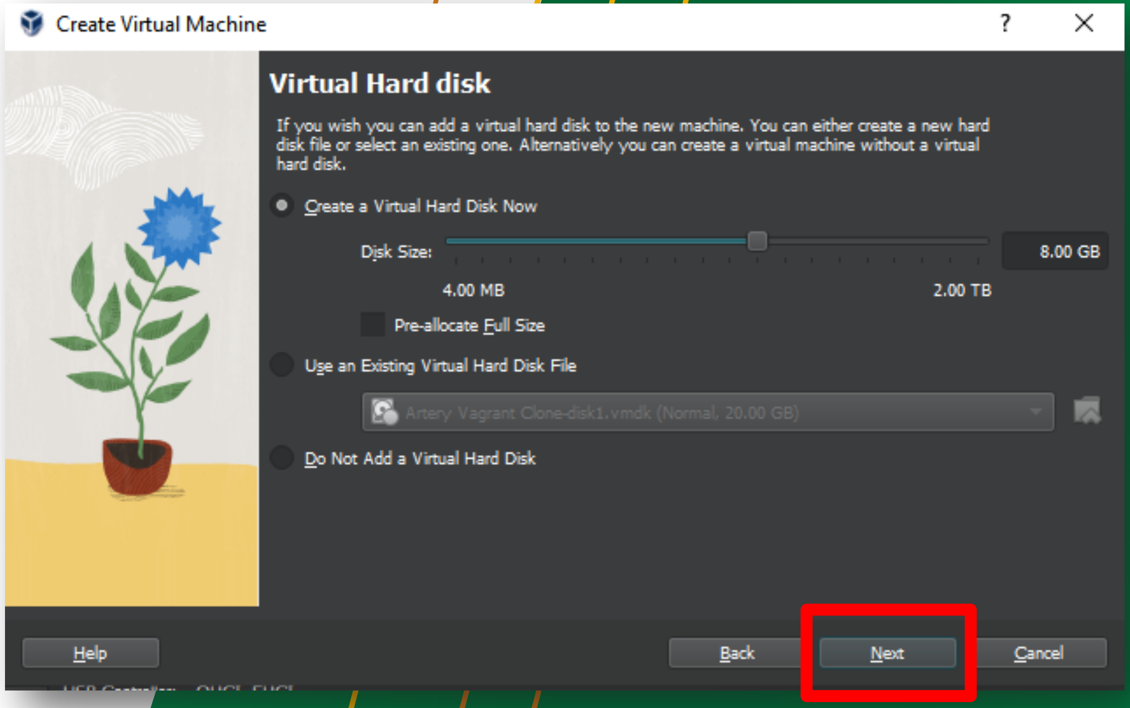
4 MB 32768 MB

Processors: 3

1 CPU 20 CPUs

□ Enable EFI (special OSes only)

USB Controller: OHCI, EHCI



Create Virtual Machine

Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

● Create a Virtual Hard Disk Now

Disk Size: 8.00 GB

4.00 MB 2.00 TB

□ Pre-allocate Full Size

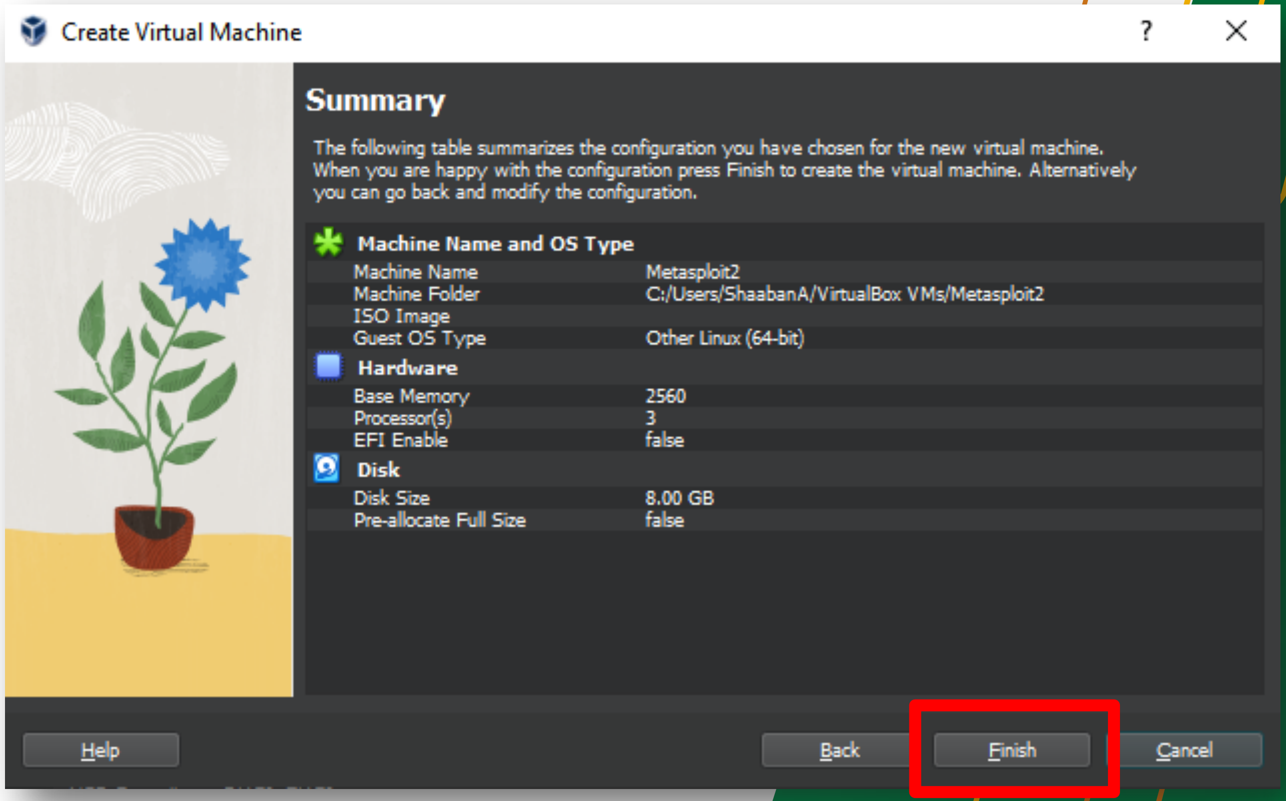
○ Use an Existing Virtual Hard Disk File

Artery Vagrant Clone-disk1.vmdk (Normal, 20.00 GB)

○ Do Not Add a Virtual Hard Disk

CyberSecPro
cc BY NC SA

Installing Metasploitable



Create Virtual Machine

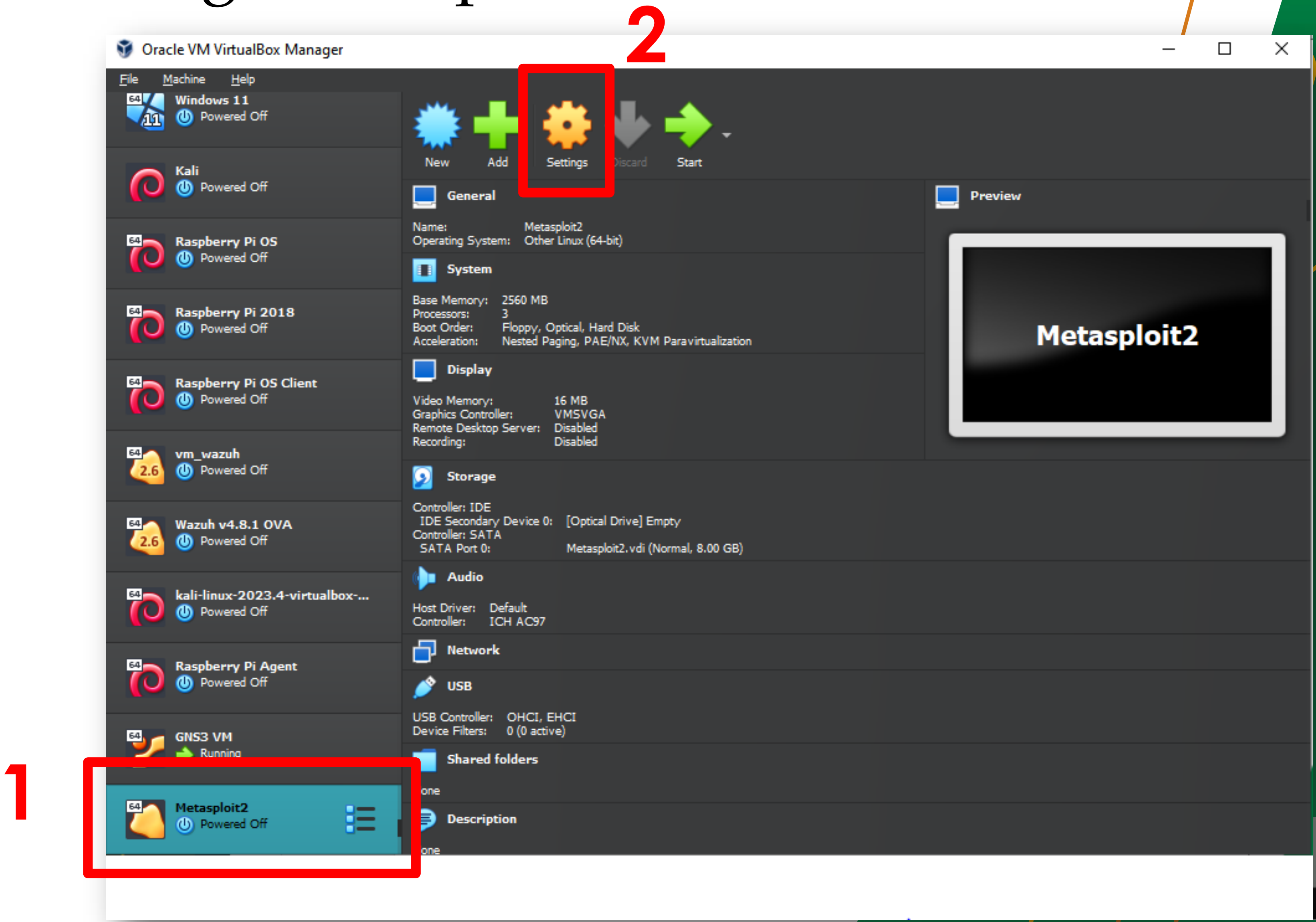
Summary

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

Machine Name and OS Type	
Machine Name	Metasploit2
Machine Folder	C:/Users/ShaabanA/VirtualBox VMs/Metasploit2
ISO Image	
Guest OS Type	Other Linux (64-bit)
Hardware	
Base Memory	2560
Processor(s)	3
EFI Enable	false
Disk	
Disk Size	8.00 GB
Pre-allocate Full Size	false

CyberSecPro
cc BY NC SA

Installing Metasploitable



Windows 11 Powered Off
Kali Powered Off
Raspberry Pi OS Powered Off
Raspberry Pi 2018 Powered Off
Raspberry Pi OS Client Powered Off
vm_wazuh Powered Off
Wazuh v4.8.1 OVA Powered Off
kali-linux-2023.4-virtualbox-... Powered Off
Raspberry Pi Agent Powered Off
GNS3 VM Running
Metasploit2 Powered Off

General

Name: Metasploit2
Operating System: Other Linux (64-bit)

System

Base Memory: 2560 MB
Processors: 3
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Metasploit2.vdi (Normal, 8.00 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders

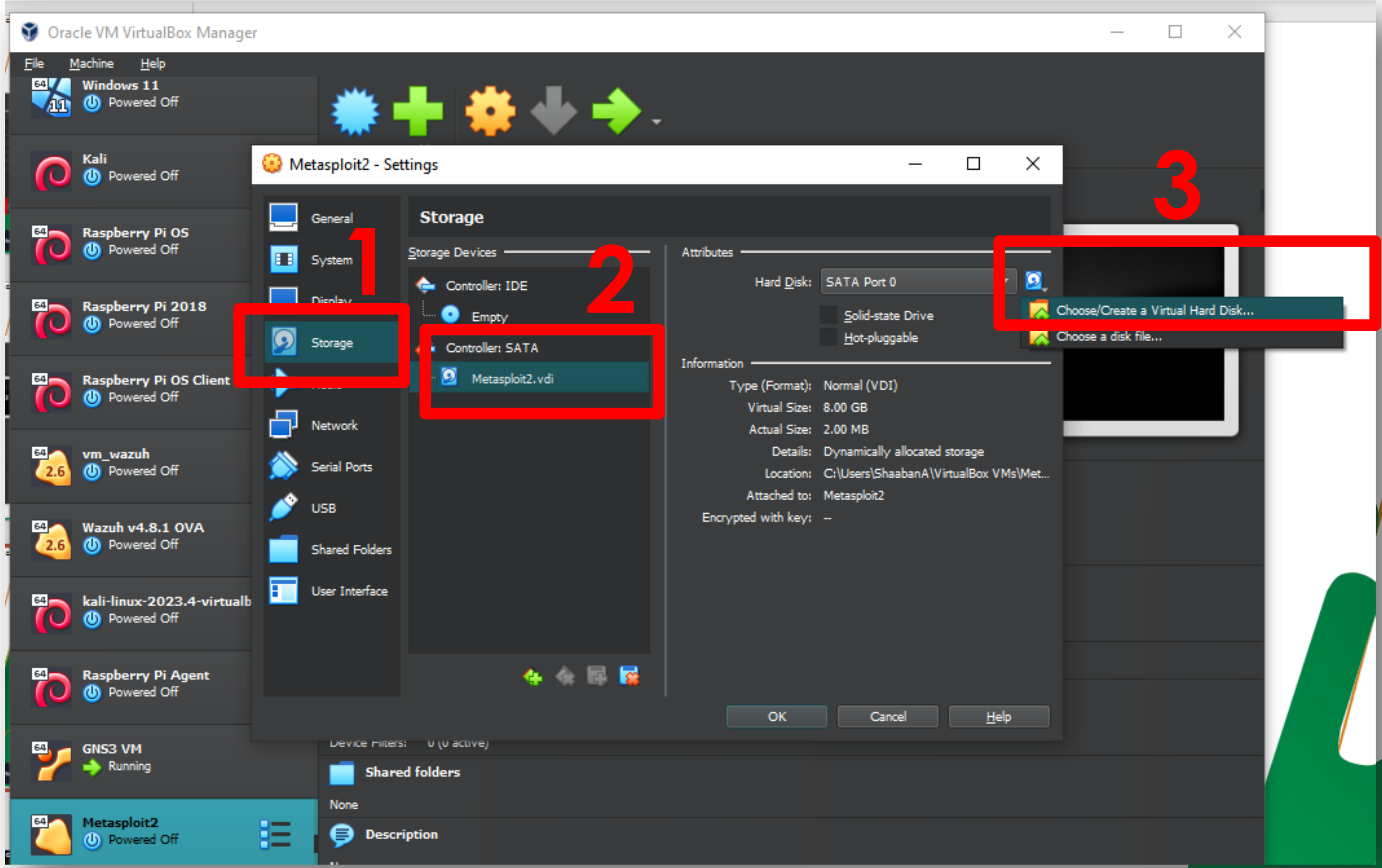
one

Description

one

cc BY NC SA

Installing Metasploitable



Hard Disk: SATA Port 0

Solid-state Drive

Hot-pluggable

Information

Type (Format): Normal (VDI)

Virtual Size: 8.00 GB

Actual Size: 2.00 MB

Details: Dynamically allocated storage

Location: C:\Users\ShaabanA\VirtualBox VMs\Met...

Attached to: Metasploit2

Encrypted with key: --

Device Filters: 0 (0 active)

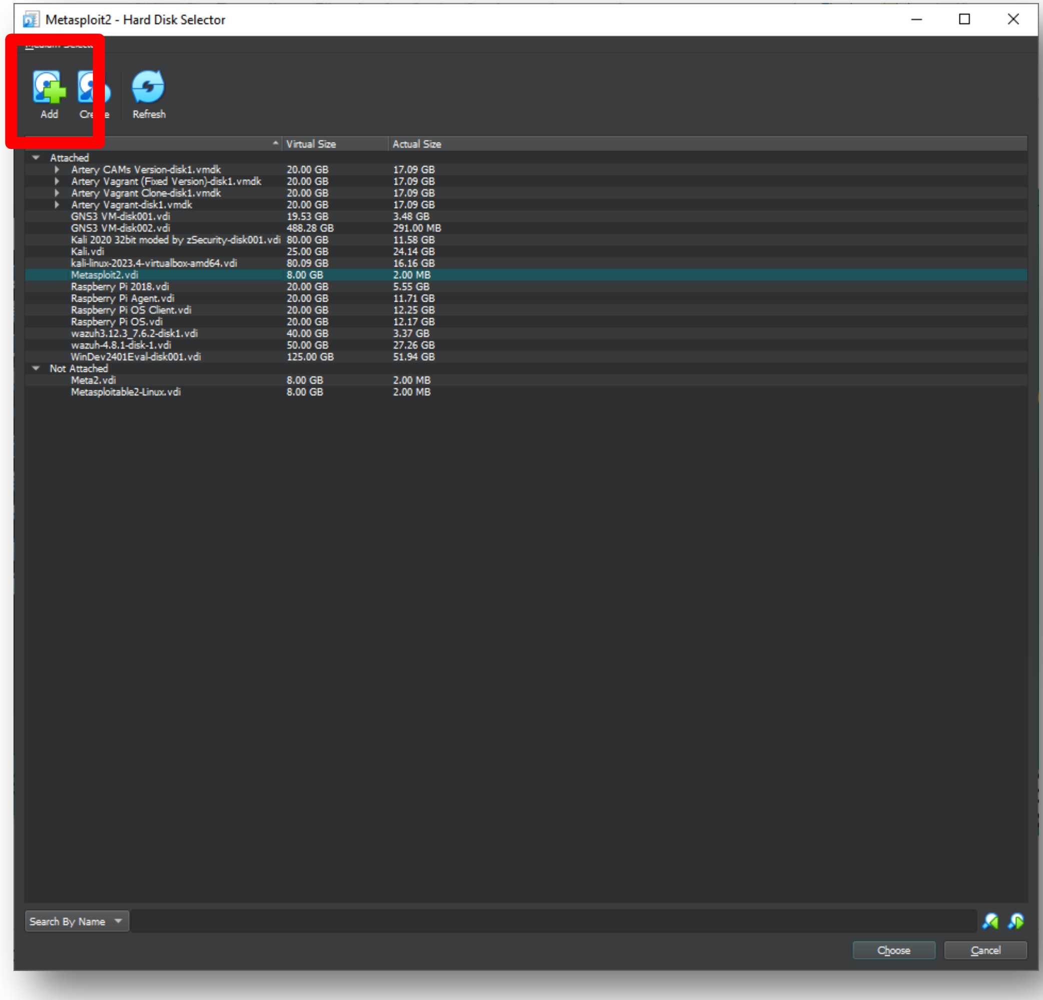
None

CyberSecPro

cc BY NC SA

Installing Metasploitable

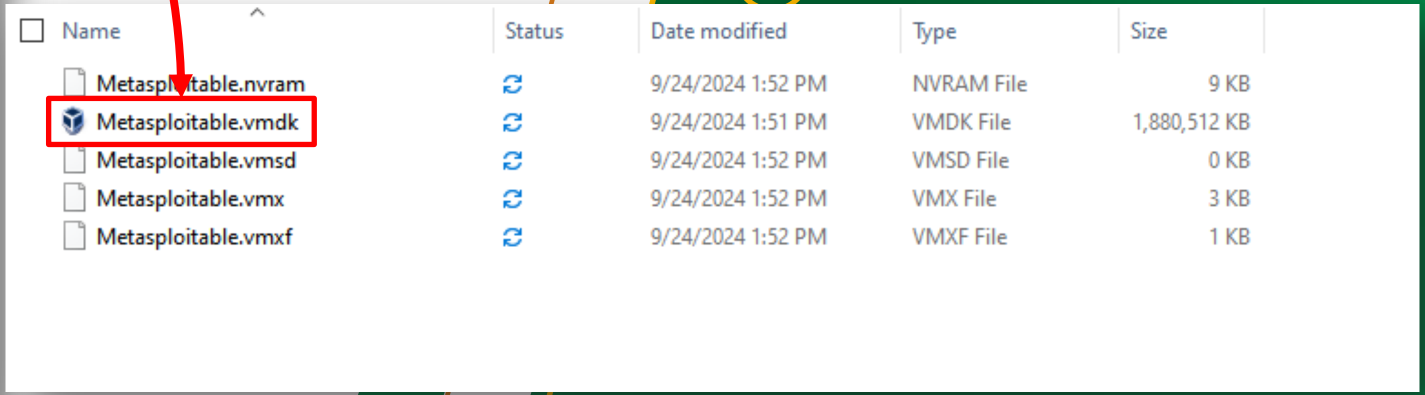
Add the Metasploitable VM file that you downloaded.



	Virtual Size	Actual Size
Attached		
Artery CAMs Version-disk1.vmdk	20.00 GB	17.09 GB
Artery Vagrant (Fixed Version)-disk1.vmdk	20.00 GB	17.09 GB
Artery Vagrant Clone-disk1.vmdk	20.00 GB	17.09 GB
Artery Vagrant-disk1.vmdk	20.00 GB	17.09 GB
GNS3 VM-disk001.vdi	19.53 GB	3.48 GB
GNS3 VM-disk002.vdi	488.28 GB	291.00 MB
Kali 2020 32bit moded by zSecurity-disk001.vdi	80.00 GB	11.58 GB
Kali.vdi	25.00 GB	24.14 GB
kali-linux-2023.4-virtualbox-amd64.vdi	80.09 GB	16.16 GB
Metasploit2.vdi	8.00 GB	2.00 MB
Raspberry Pi 2018.vdi	20.00 GB	5.55 GB
Raspberry Pi Agent.vdi	20.00 GB	11.71 GB
Raspberry Pi OS Client.vdi	20.00 GB	12.25 GB
Raspberry Pi OS.vdi	20.00 GB	12.17 GB
wazuh3.12.3_7.6.2-disk1.vdi	40.00 GB	3.37 GB
wazuh-4.8.1-disk-1.vdi	50.00 GB	27.26 GB
WinDev2401Eval-disk001.vdi	125.00 GB	51.94 GB
Not Attached		
Meta2.vdi	8.00 GB	2.00 MB
Metasploitable2-Linux.vdi	8.00 GB	2.00 MB

Select this file

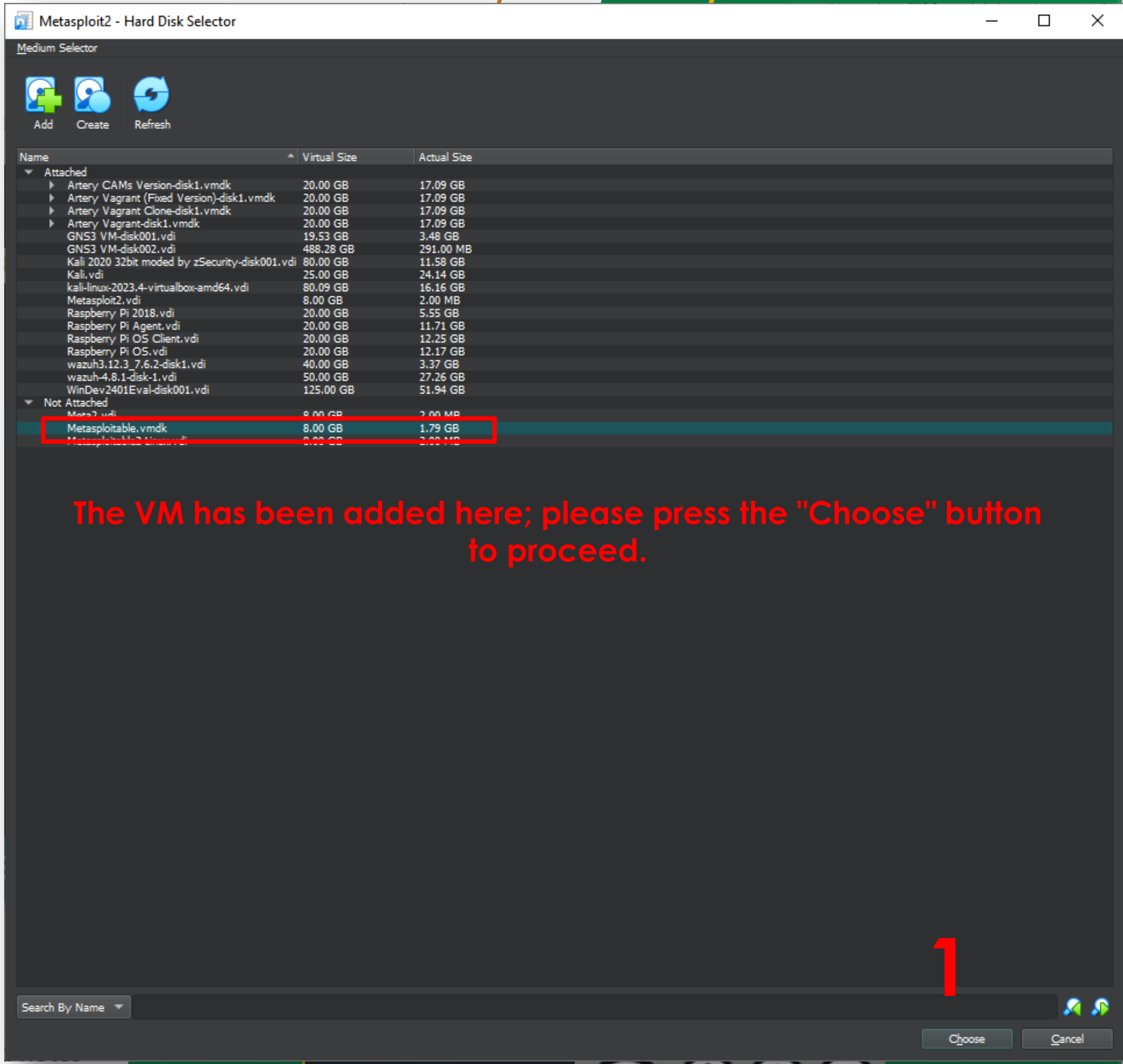
Here are the contents of the Metasploit ZIP file.



□ Name	Status	Date modified	Type	Size
Metasploitable.nvram		9/24/2024 1:52 PM	NVRAM File	9 KB
Metasploitable.vmdk		9/24/2024 1:51 PM	VMDK File	1,880,512 KB
Metasploitable.vmsd		9/24/2024 1:52 PM	VMSD File	0 KB
Metasploitable.vmx		9/24/2024 1:52 PM	VMX File	3 KB
Metasploitable.vmxf		9/24/2024 1:52 PM	VMXF File	1 KB

CyberSecPro
cc BY NC SA

Installing Metasploitable



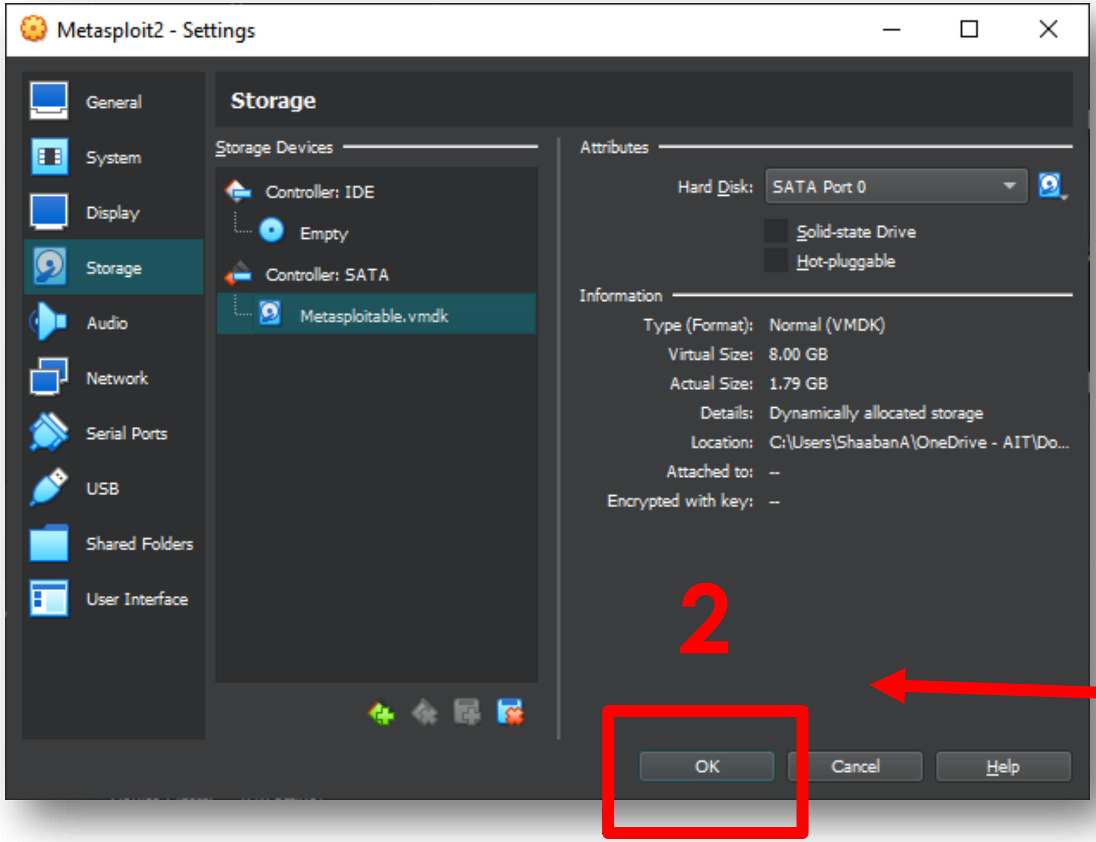
Name	Virtual Size	Actual Size
Attached		
Artery CAMs Version-disk1.vmdk	20.00 GB	17.09 GB
Artery Vagrant (Fixed Version)-disk1.vmdk	20.00 GB	17.09 GB
Artery Vagrant Clone-disk1.vmdk	20.00 GB	17.09 GB
Artery Vagrant-disk1.vmdk	20.00 GB	17.09 GB
GNS3 VM-disk001.vdi	19.53 GB	3.48 GB
GNS3 VM-disk002.vdi	488.28 GB	291.00 MB
Kali 2020 32bit moded by zSecurity-disk001.vdi	80.00 GB	11.58 GB
Kali.vdi	25.00 GB	24.14 GB
kali-linux-2023.4-virtualbox-amd64.vdi	80.09 GB	16.16 GB
Metasploit2.vdi	8.00 GB	2.00 MB
Raspberry Pi 2018.vdi	20.00 GB	5.55 GB
Raspberry Pi Agent.vdi	20.00 GB	11.71 GB
Raspberry Pi OS Client.vdi	20.00 GB	12.25 GB
Raspberry Pi OS.vdi	20.00 GB	12.17 GB
wazuh3.12.3_7.6.2-disk1.vdi	40.00 GB	3.37 GB
wazuh-4.8.1-disk-1.vdi	50.00 GB	27.26 GB
WinDev2401Eval-disk001.vdi	125.00 GB	51.94 GB
Not Attached		
Meta2.vdi	8.00 GB	2.00 MB
Metasploitable.vmdk	8.00 GB	1.79 GB
Metasploitable2-Linux.vdi	8.00 GB	2.00 MB

The VM has been added here; please press the "Choose" button to proceed.

1

cc BY NC SA

Installing Metasploitable



Metasploit2 - Settings

Storage

Storage Devices

- Controller: IDE
  - Empty
- Controller: SATA
  - Metasploitable.vmdk

Attributes

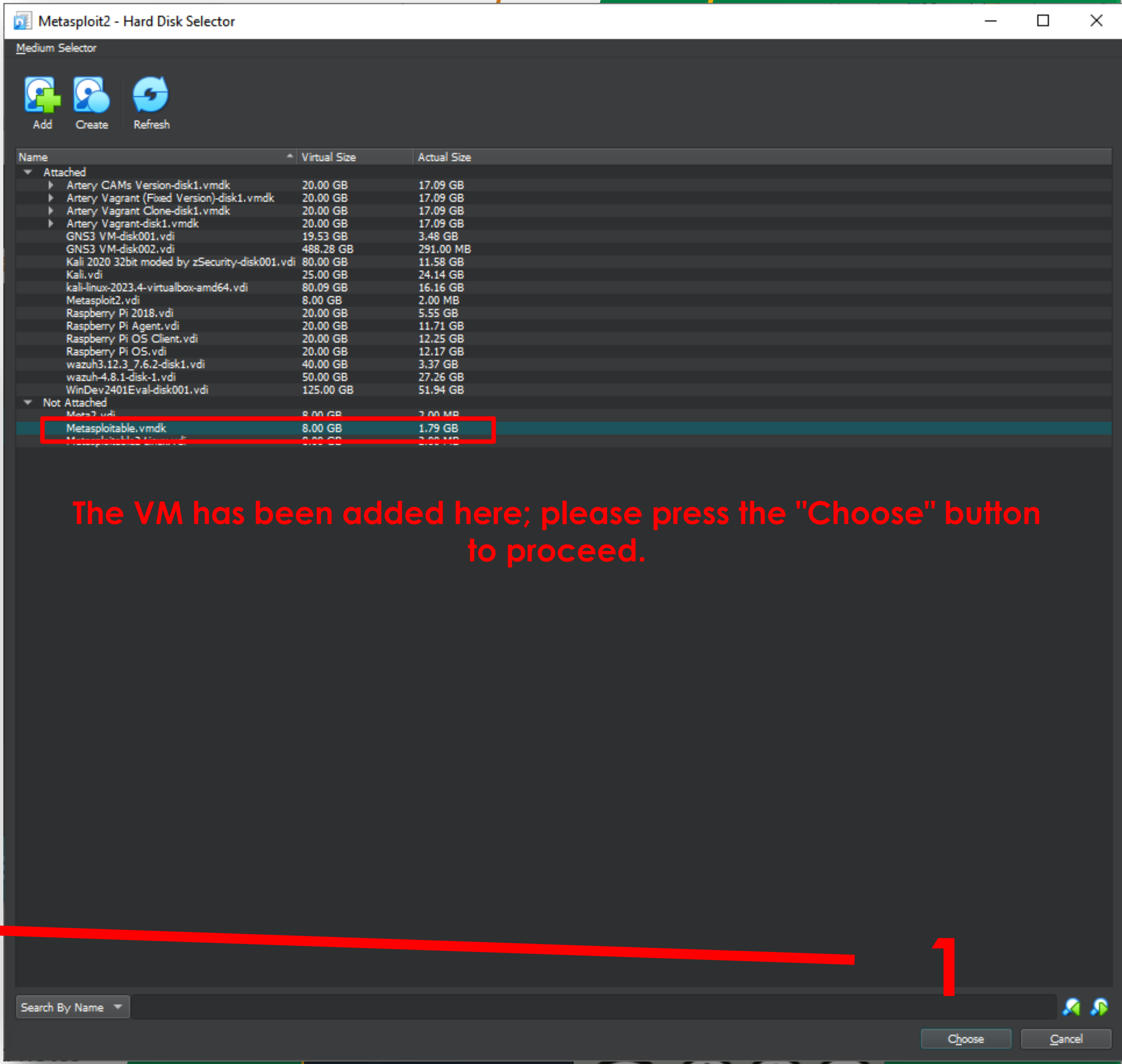
Hard Disk: SATA Port 0

□ Solid-state Drive

□ Hot-pluggable

Information

Type (Format): Normal (VMDK)
Virtual Size: 8.00 GB
Actual Size: 1.79 GB
Details: Dynamically allocated storage
Location: C:\Users\ShaabanA\OneDrive - AIT\Do...
Attached to: --
Encrypted with key: --



Metasploit2 - Hard Disk Selector

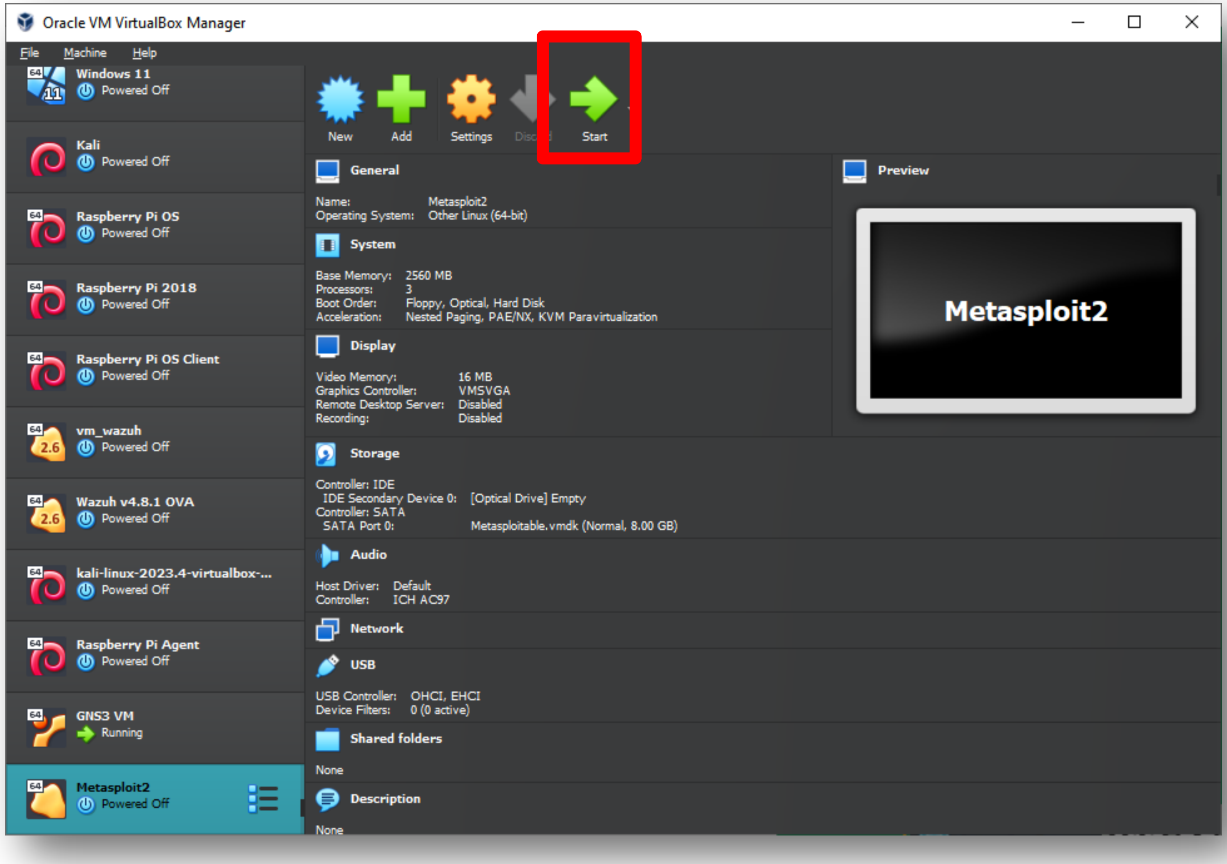
Name	Virtual Size	Actual Size
Attached		
Artery CAMs Version-disk1.vmdk	20.00 GB	17.09 GB
Artery Vagrant (Fixed Version)-disk1.vmdk	20.00 GB	17.09 GB
Artery Vagrant Clone-disk1.vmdk	20.00 GB	17.09 GB
Artery Vagrant-disk1.vmdk	20.00 GB	17.09 GB
GNS3 VM-disk001.vdi	19.53 GB	3.48 GB
GNS3 VM-disk002.vdi	488.28 GB	291.00 MB
Kali 2020 32bit moded by zSecurity-disk001.vdi	80.00 GB	11.58 GB
Kali.vdi	25.00 GB	24.14 GB
kali-linux-2023.4-virtualbox-amd64.vdi	80.09 GB	16.16 GB
Metasploit2.vdi	8.00 GB	2.00 MB
Raspberry Pi 2018.vdi	20.00 GB	5.55 GB
Raspberry Pi Agent.vdi	20.00 GB	11.71 GB
Raspberry Pi OS Client.vdi	20.00 GB	12.25 GB
Raspberry Pi OS.vdi	20.00 GB	12.17 GB
wazuh3.12.3_7.6.2-disk1.vdi	40.00 GB	3.37 GB
wazuh-4.8.1-disk-1.vdi	50.00 GB	27.26 GB
WinDev2401Eval-disk001.vdi	125.00 GB	51.94 GB
Not Attached		
Meta2.vdi	8.00 GB	2.00 MB
Metasploitable.vmdk	8.00 GB	1.79 GB
Metasploitable2-Linux.vdi	8.00 GB	2.00 MB

The VM has been added here; please press the "Choose" button to proceed.

cc BY NC SA

Starting the Metasploitable VM

Start the Metasploit VM



Oracle VM VirtualBox Manager

Windows 11 — Powered Off
Kali — Powered Off
Raspberry Pi OS — Powered Off
Raspberry Pi 2018 — Powered Off
Raspberry Pi OS Client — Powered Off
vm_wazuh — Powered Off
Wazuh v4.8.1 OVA — Powered Off
kali-linux-2023.4-virtualbox-... — Powered Off
Raspberry Pi Agent — Powered Off
GNS3 VM — Running
Metasploit2 — Powered Off

General

Name: Metasploit2
Operating System: Other Linux (64-bit)

System

Base Memory: 2560 MB
Processors: 3
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Metasploitable.vmdk (Normal, 8.00 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

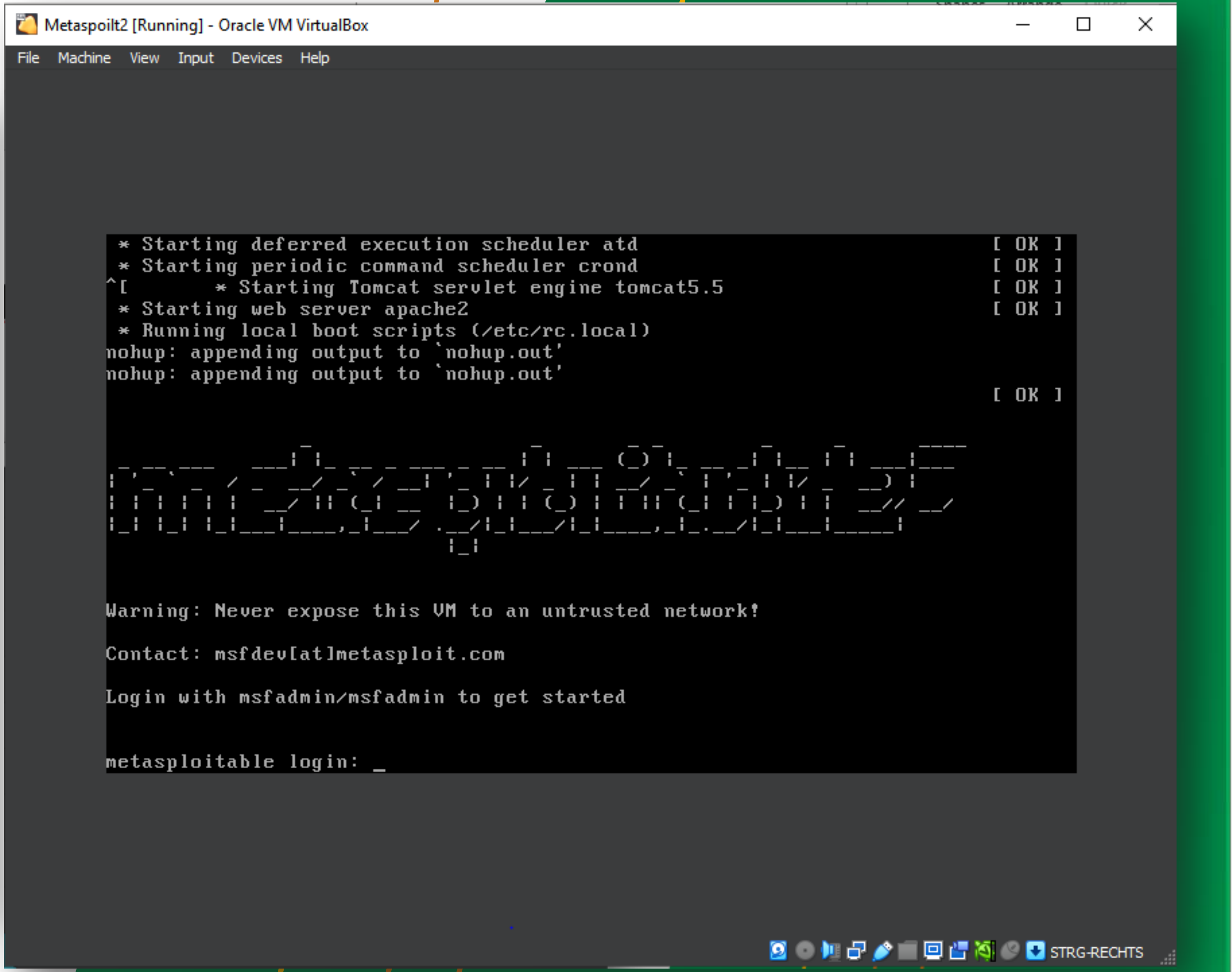
Shared folders

None

Description

None

The Metasploit VM is now running successfully on your computer.



Metaspoilt2 [Running] - Oracle VM VirtualBox

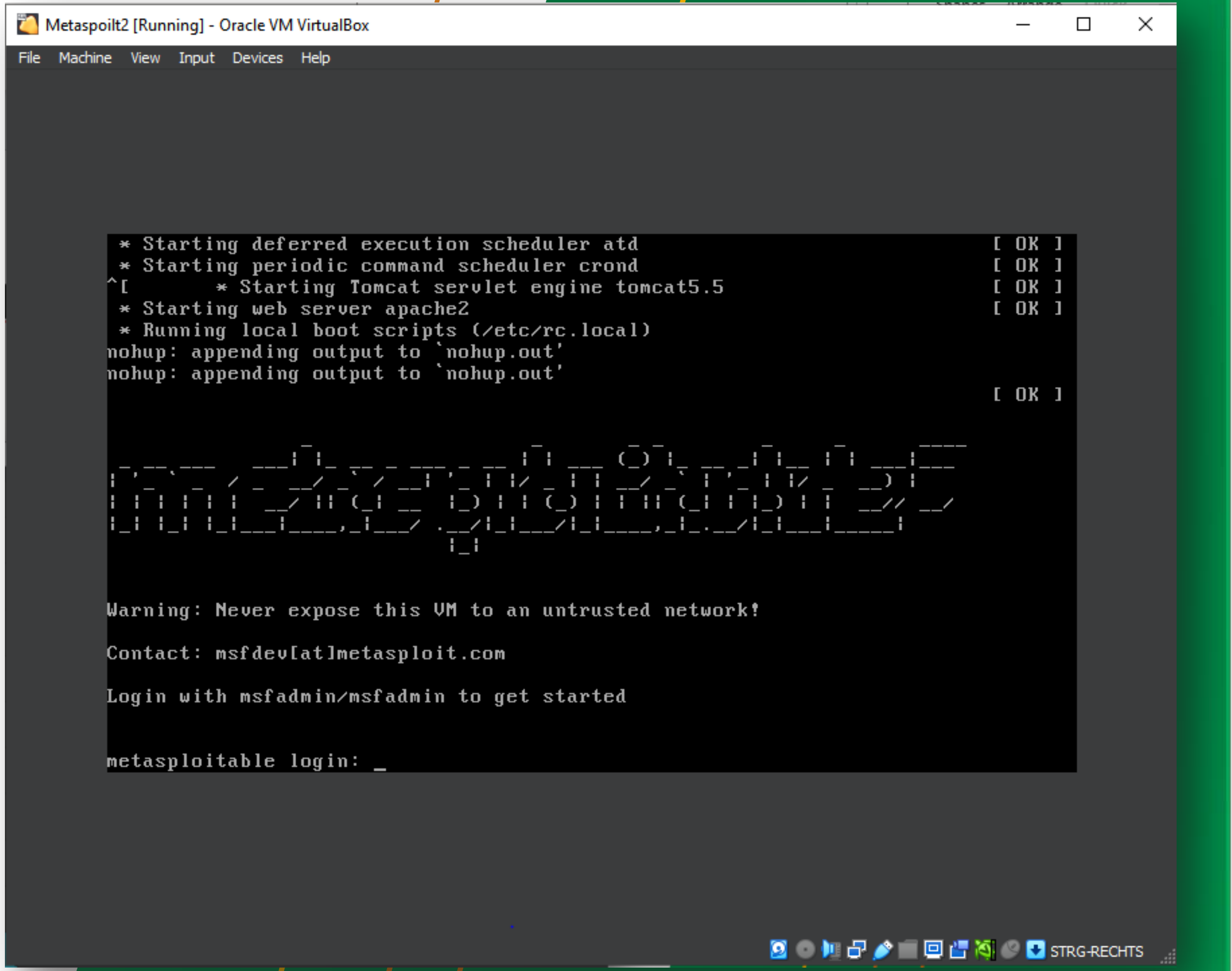
```
 * Starting deferred execution scheduler atd                          [ OK ]
 * Starting periodic command scheduler crond                          [ OK ]
^[        * Starting Tomcat servlet engine tomcat5.5                  [ OK ]
 * Starting web server apache2                                        [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                      [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

CyberSecPro

BY NC SA

Starting the Metasploitable VM

Login: msfadmin
Password: msfadmin


Metaspoilt2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
STRG-RECHTS

```
 * Starting deferred execution scheduler atd                            [ OK ]
 * Starting periodic command scheduler crond                            [ OK ]
^[        * Starting Tomcat servlet engine tomcat5.5                    [ OK ]
 * Starting web server apache2                                          [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                        [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

BY NC SA

Lab's Network Landscape

CyberSecPro

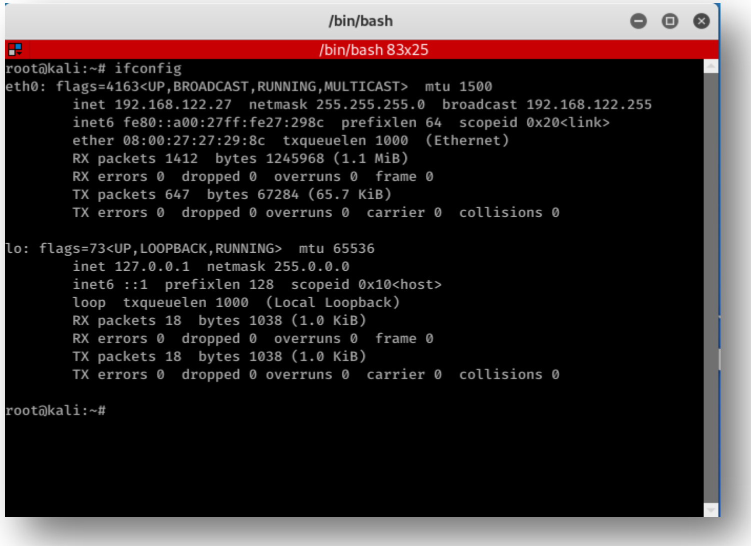
cc BY NC SA

Network IPs

- To ensure the lab is set up correctly, it is important to verify the connectivity of each machine used in the lab.

- Use the **ifconfig** command on the Linux devices to know more about the network configuration

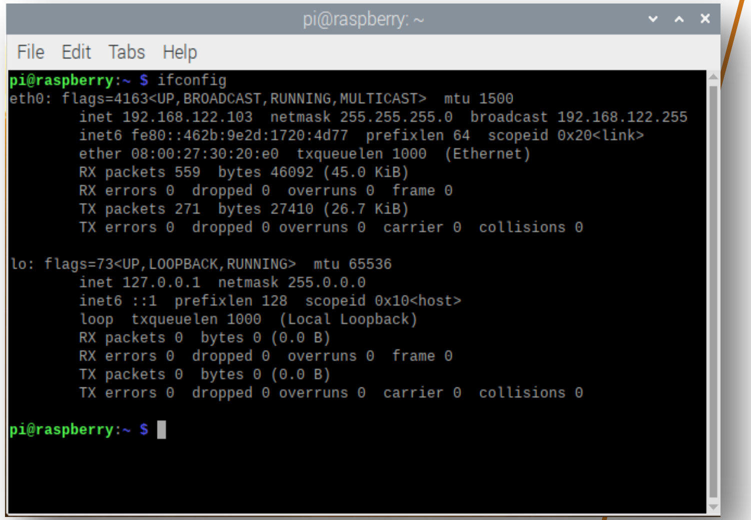
Kali – Attaker



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.122.27  netmask 255.255.255.0  broadcast 192.168.122.255
        inet6 fe80::a00:27ff:fe27:298c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:27:29:8c  txqueuelen 1000  (Ethernet)
        RX packets 1412  bytes 1245968 (1.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 647  bytes 67284 (65.7 KiB)
        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 18  bytes 1038 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 1038 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

192.168.122.27

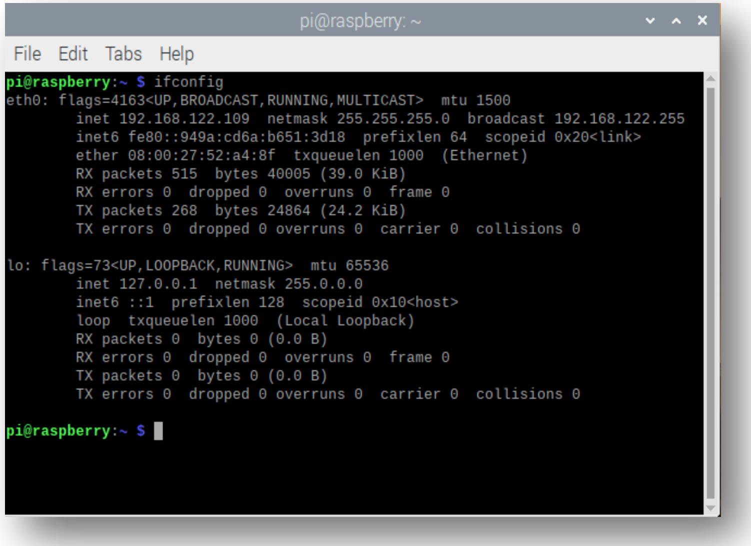
Admin



```
pi@raspberry:~ $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.122.103  netmask 255.255.255.0  broadcast 192.168.122.255
        inet6 fe80::462b:9e2d:1720:4d77  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:30:20:e0  txqueuelen 1000  (Ethernet)
        RX packets 559  bytes 46092 (45.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 271  bytes 27410 (26.7 KiB)
        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 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

pi@raspberry:~ $
```

192.168.122.109

Victim



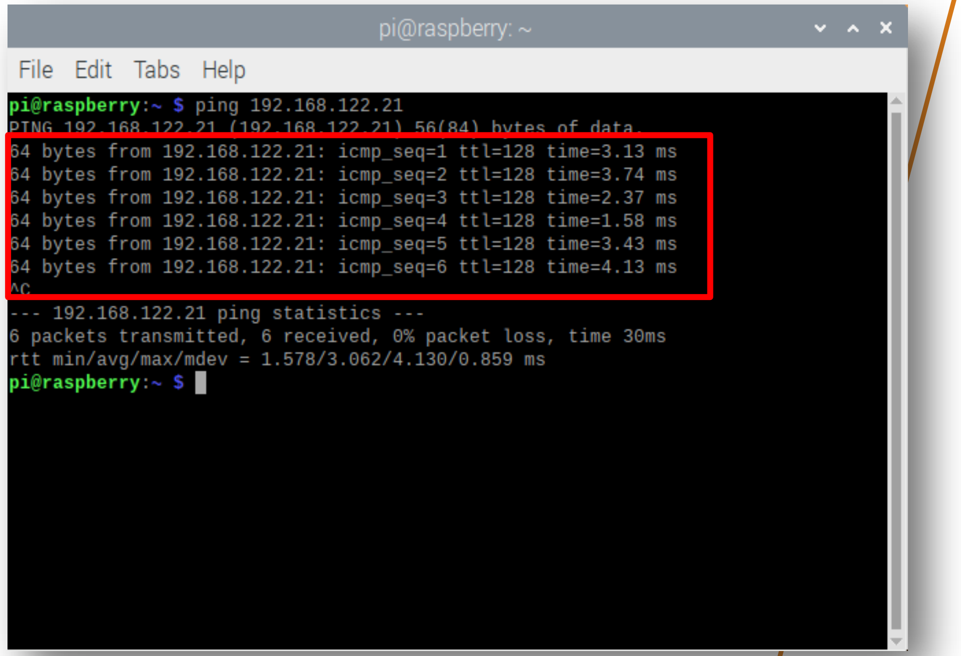
```
pi@raspberry:~ $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.122.109  netmask 255.255.255.0  broadcast 192.168.122.255
        inet6 fe80::949a:cd6a:b651:3d18  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:52:a4:8f  txqueuelen 1000  (Ethernet)
        RX packets 515  bytes 40005 (39.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 268  bytes 24864 (24.2 KiB)
        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 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

pi@raspberry:~ $
```

192.168.122.103

Connectivity Check

- Now we have the IPs of the network devices, be sure that all devices can reach each other.
- Use the **ping <destination IP-address>** to test the successful establishment of the network.

Victim



```
pi@raspberry:~ $ ping 192.168.122.21
PING 192.168.122.21 (192.168.122.21) 56(84) bytes of data.
64 bytes from 192.168.122.21: icmp_seq=1 ttl=128 time=3.13 ms
64 bytes from 192.168.122.21: icmp_seq=2 ttl=128 time=3.74 ms
64 bytes from 192.168.122.21: icmp_seq=3 ttl=128 time=2.37 ms
64 bytes from 192.168.122.21: icmp_seq=4 ttl=128 time=1.58 ms
64 bytes from 192.168.122.21: icmp_seq=5 ttl=128 time=3.43 ms
64 bytes from 192.168.122.21: icmp_seq=6 ttl=128 time=4.13 ms
^C
--- 192.168.122.21 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 30ms
rtt min/avg/max/mdev = 1.578/3.062/4.130/0.859 ms
pi@raspberry:~ $
```

192.168.122.109

Get ready—we will get on more exciting cybersecurity activities together! 🚀 🔒

If you have any questions, please feel free to reach out to me at:

Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at

CyberSecPro

cc BY NC SA