Introduction to Malware Analysis

Assignment 1 – Virtual Machines for Malware Analysis

10 points

LAB

Please read Chapter 2 of the textbook, notes and slides. There are two lab environments: **Error! Reference source not found.** and **Error! Reference source not found.**.

- Students have to download VMs if they use personal computers
- Cyber Range has everything installed. Students have to go to Cyber Range physically to use Cyber Range computers

DOWNLOADING VMS FOR PERSONAL COMPUTERS

If you plan to use your personal computer for the labs, please use this link to download Win10-CR-50G.ova, Kali-CR-25G.ova and Metasploitable-CR.ova . Please do NOT download at last minute since downloading takes a long time.

Here are the steps to start (Click the links embedded in the blue and unlined text to watch videos):

1. Install VirtualBox on Windows 10 and Mac OS X
2. Import .ova file into VirtualBox
3. If a student feels the VM is slow, please watch How to Speed up your VMs in VirtualBox! For Windows and How to improve Linux performance in a VirtualBox VM.

PLEASE REFER TO BLACKBOARD FOR CREDENTIALS FOR VMS.

- The Windows 10 VM is restricted for the UML student use and cannot be distributed to non UML students.
- If there are errors when trying to use the two VMs, students may try to install VirtualBox Extension Pack. Please refer to the slides or watch YouTube videos such as Install VirtualBox 6.1 in Windows 10 | With Extension Pack. Students shall always use the newest version of VirtualBox.
    a. VirtualBox does not work on new Apple computers with ARM chips.
    b. VirtualBox can only be downloaded off campus.

QUESTIONS

Try the following four networking options on these two VMs [3]:

1. Network Address Translation (NAT)
2. NAT Network

3. Bridged Adapter
4. Internal Network
5. Host-only Adaptor

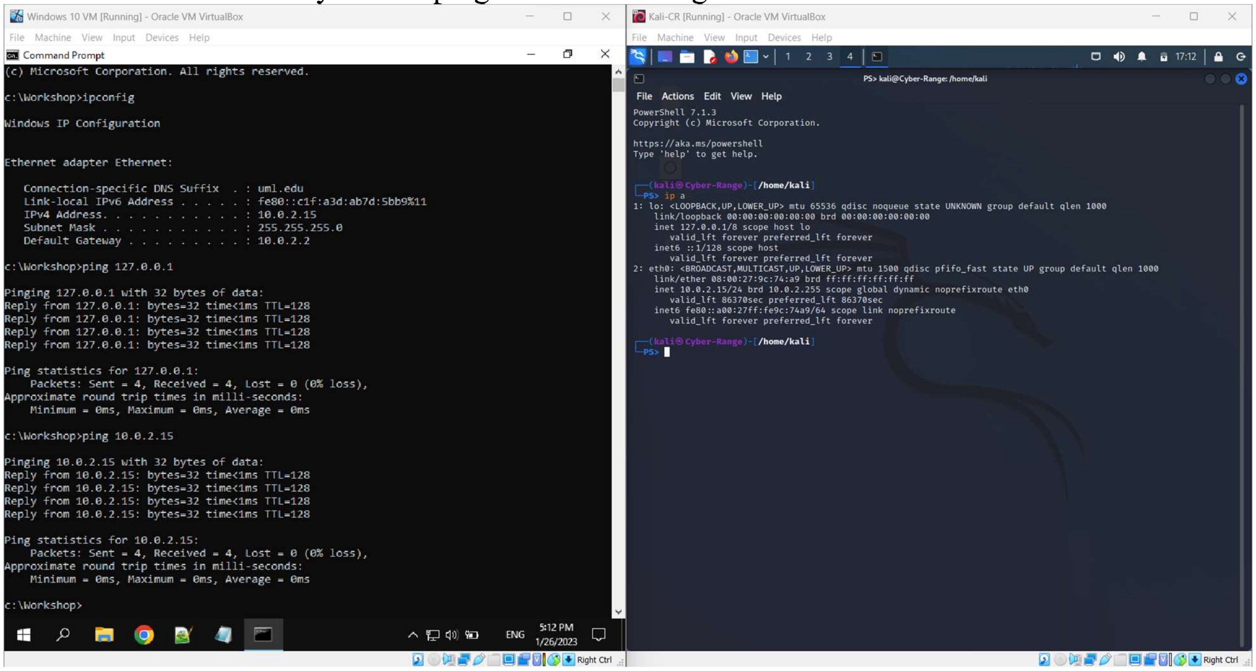
Please explain each networking option. Please refer to [3][1] for VirtualBox's virtual networking. For each networking option, please use *ping* to show that Windows 10 VM and Kali VM can reach each other.

1. NAT
   - Explain what NAT is within VirtualBox. (0.5 point)

A guest operating system can access a host in a physical LAN using NAT. A guest machine is not accessible from a host machine. Best for people who only want to use it for Internet access.

- Please provide at least one screenshot showing if Windows can ping Kali. (0.5 point)

Virtual machines actually cannot ping each other using NAT.


Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt
ENG
5:12 PM
1/26/2023
Right Ctrl
Kali-CR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
17:12
PS> kali@Cyber-Range: /home/kali
File Actions Edit View Help
Right Ctrl

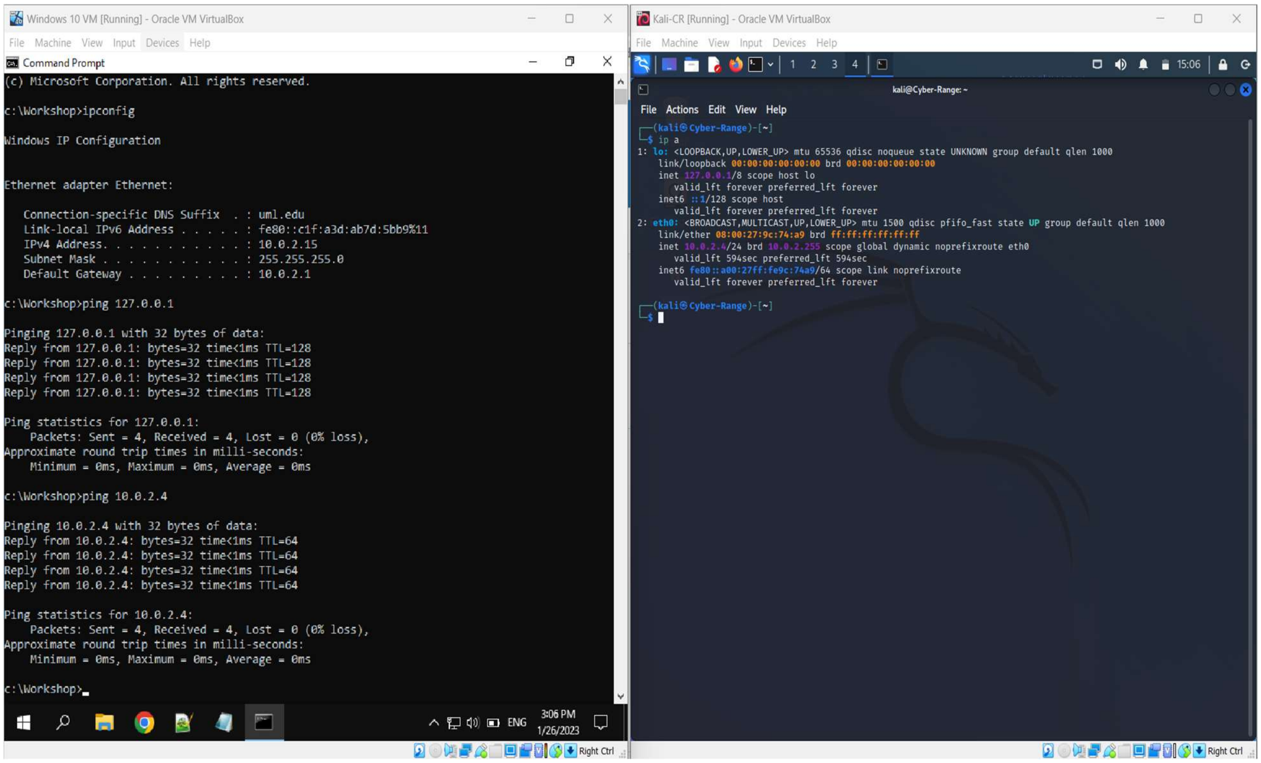
```
(c) Microsoft Corporation. All rights reserved.

c:\Workshop>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : uml.edu
   Link-local IPv6 Address . . . . . : fe80::c1f:a3d:ab7d:5bb9%11
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.2

c:\Workshop>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

c:\Workshop>ping 10.0.2.15

Pinging 10.0.2.15 with 32 bytes of data:
Reply from 10.0.2.15: bytes=32 time<1ms TTL=128
Reply from 10.0.2.15: bytes=32 time<1ms TTL=128
Reply from 10.0.2.15: bytes=32 time<1ms TTL=128
Reply from 10.0.2.15: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.2.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

c:\Workshop>
```

```
PowerShell 7.1.3
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

┌─(kali㉿Cyber-Range)-[/home/kali]
└─PS> ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:9c:74:a9 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 86370sec preferred_lft 86370sec
    inet6 fe80::a00:27ff:fe9c:74a9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌─(kali㉿Cyber-Range)-[/home/kali]
└─PS> 
```

2. NAT Network
   - Explain what NAT Network is within VirtualBox. (1 point)

If you are using this mode on multiple virtual machines, than they can communicate with each other over the network.

- Please provide at least one screenshot showing if Windows can ping Kali. (1 point)


Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt
3:06 PM
1/26/2023
Right Ctrl
Kali-CR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
15:06
kali@Cyber-Range: ~
File Actions Edit View Help

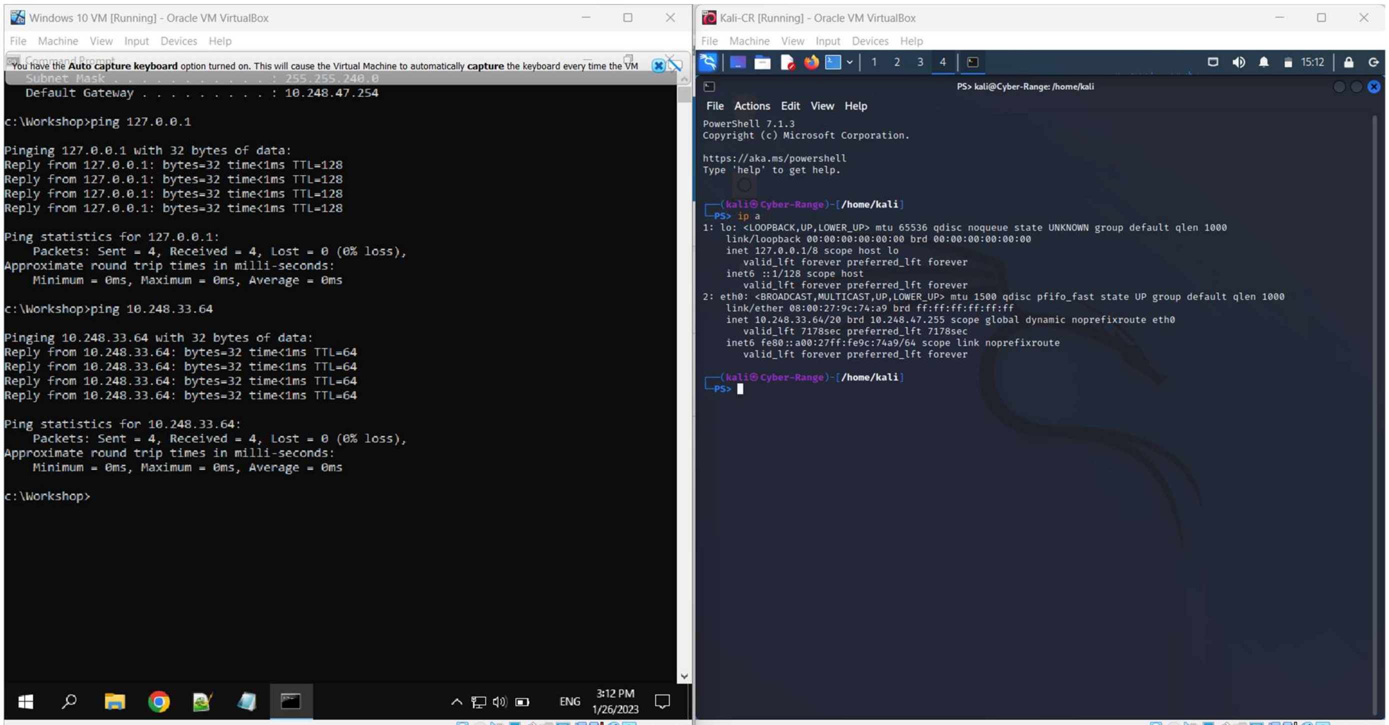
```
(c) Microsoft Corporation. All rights reserved.

c:\Workshop>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : uml.edu
   Link-local IPv6 Address . . . . . : fe80::c1f:a3d:ab7d:5bb9%11
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

c:\Workshop>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

c:\Workshop>ping 10.0.2.4

Pinging 10.0.2.4 with 32 bytes of data:
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

c:\Workshop>_
```

```
┌──(kali㉿Cyber-Range)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:9c:74:a9 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 594sec preferred_lft 594sec
    inet6 fe80::a00:27ff:fe9c:74a9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿Cyber-Range)-[~]
└─$ █
```

3. Bridged Adapter
   - Explain what Bridged Adapter is within VirtualBox. (1 point)

Used for connecting the virtual network adapter of a VM to a physical network to which to which a physical network adapter of the virtual box host machine is connected. Network packets are sent and received directly from/to virtual network adapter without additional routing.

- Please provide at least one screenshot showing if Windows can ping Kali. (1 point)


Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM
3:12 PM
1/26/2023
Kali-CR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
15:12
PS> kali@Cyber-Range: /home/kali
File Actions Edit View Help

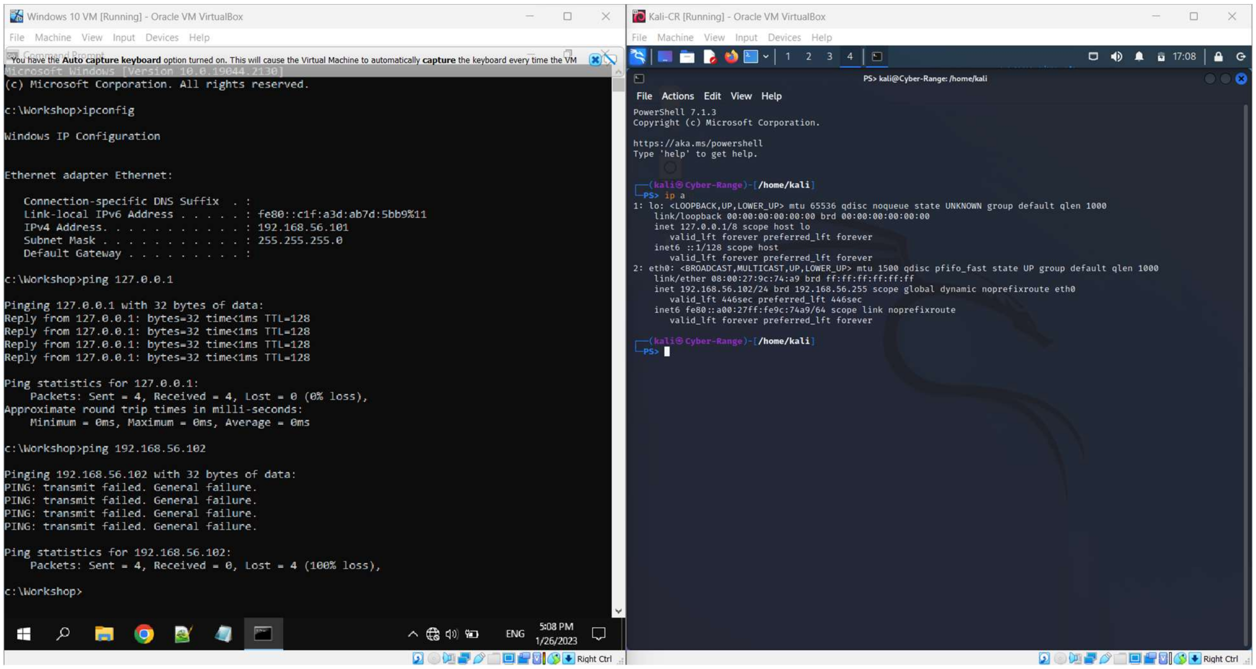
```
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.248.47.254

c:\Workshop>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

c:\Workshop>ping 10.248.33.64

Pinging 10.248.33.64 with 32 bytes of data:
Reply from 10.248.33.64: bytes=32 time<1ms TTL=64
Reply from 10.248.33.64: bytes=32 time<1ms TTL=64
Reply from 10.248.33.64: bytes=32 time<1ms TTL=64
Reply from 10.248.33.64: bytes=32 time<1ms TTL=64

Ping statistics for 10.248.33.64:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

c:\Workshop>
```

```
PowerShell 7.1.3
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.


┌──(kali㉿Cyber-Range)-[/home/kali]
└─PS> ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:9c:74:a9 brd ff:ff:ff:ff:ff:ff
    inet 10.248.33.64/20 brd 10.248.47.255 scope global dynamic noprefixroute eth0
       valid_lft 7178sec preferred_lft 7178sec
    inet6 fe80::a00:27ff:fe9c:74a9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿Cyber-Range)-[/home/kali]
└─PS> █
```

4. Internal Network
    - Explain what Internal Network is within VirtualBox. (1 point)

VMs are connected to an isolated virtual network. VMs connected to this can communicate with each other but not with a VirtualBox host machine, or other hosts on physical or external host.

- Please provide at least one screenshot showing if Windows can ping Kali. (1 point)


Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt
You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM
ENG
5:08 PM
1/26/2023
Right Ctrl
Kali-CR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
17:08
PS> kali@Cyber-Range: /home/kali
File Actions Edit View Help
Right Ctrl

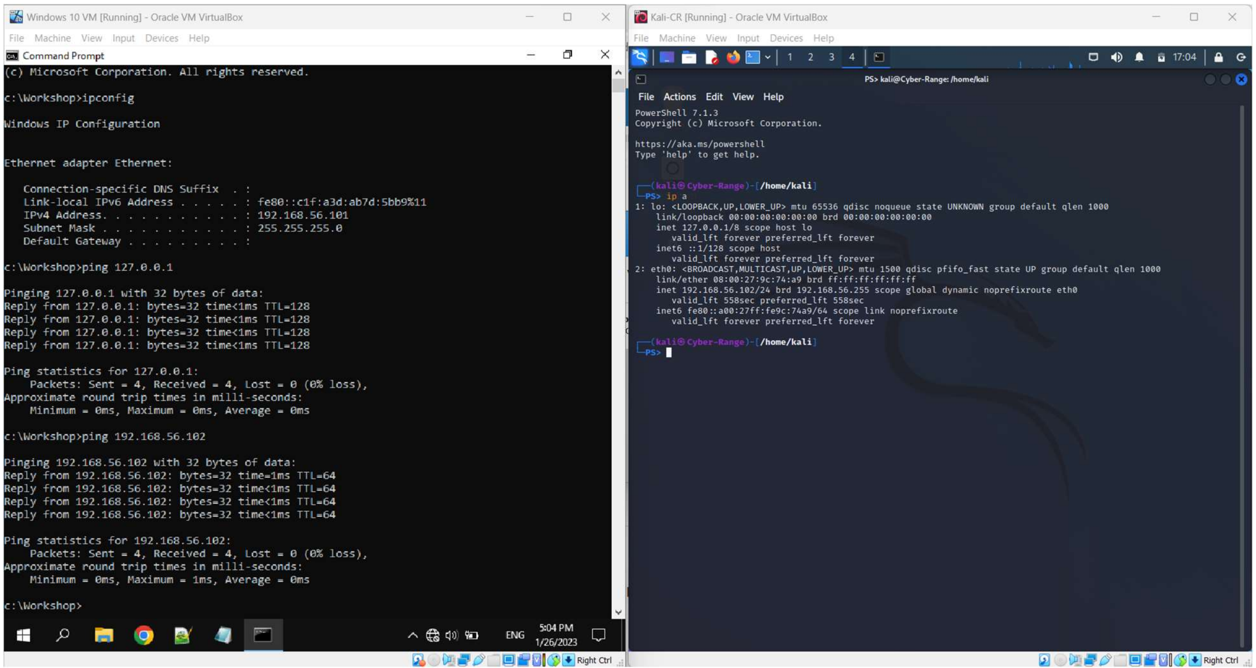
```
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

c:\Workshop>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c1f:a3d:ab7d:5bb9%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

c:\Workshop>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

c:\Workshop>ping 192.168.56.102

Pinging 192.168.56.102 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 192.168.56.102:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

c:\Workshop>
```

```
PowerShell 7.1.3
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.


┌──(kali㉿Cyber-Range)-[/home/kali]
└─PS> ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:9c:74:a9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
       valid_lft 446sec preferred_lft 446sec
    inet6 fe80::a00:27ff:fe9c:74a9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿Cyber-Range)-[/home/kali]
└─PS> 
```

5. Host-only Adaptor
    - Explain what Host-only Adaptor is within VirtualBox. (1 point)

Used for communicating between hosts and guests. VMs on this mode can communicate with each other and the host.

- Please provide at least one screenshot showing if Windows can ping Kali. (1 point)


Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt
ENG
5:04 PM
1/26/2023
Right Ctrl
Kali-CR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
17:04
PS> kali@Cyber-Range: /home/kali
File Actions Edit View Help
Right Ctrl

```
(c) Microsoft Corporation. All rights reserved.

c:\Workshop>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c1f:a3d:ab7d:5bb9%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

c:\Workshop>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

c:\Workshop>ping 192.168.56.102

Pinging 192.168.56.102 with 32 bytes of data:
Reply from 192.168.56.102: bytes=32 time=1ms TTL=64
Reply from 192.168.56.102: bytes=32 time<1ms TTL=64
Reply from 192.168.56.102: bytes=32 time<1ms TTL=64
Reply from 192.168.56.102: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

c:\Workshop>
```

```
PowerShell 7.1.3
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.


┌──(kali㉿Cyber-Range)-[/home/kali]
└─PS> ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:9c:74:a9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
       valid_lft 558sec preferred_lft 558sec
    inet6 fe80::a00:27ff:fe9c:74a9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿Cyber-Range)-[/home/kali]
└─PS> 
```

6. Please provide any notes the student believes valuable for setting up the VMs for malware analysis. For example, any notes for lecture notes the student wants to complement? (1 point)

Not sure if I remember this correctly since I used the VMs last semester. But I went to Settings and than System to lower the base memory for Kali and Windows. I did this so Kali and Windows can work at the same time otherwise they work very slow and can freeze your laptop.

References

[1] Chapter 6. Virtual Networking, Accessed on Feb. 16, 2020
[2] VirtualBox for a Kali Guest, Accessed on Feb. 19, 2020
[3] VirtualBox Network Settings: Complete Guide, July 16, 2019