

## Lab 01 Requirements

- Internet connectivity & VMware Workstation version 15.5.7 or above
- Downloaded VMs from resources link under content on FOL
- FCIV from <http://support.microsoft.com/kb/841290> or another capable checksum verifier
- Folder named **INFO6065** where you can store the VMs for this course
- 7zip software downloaded from: <http://www.7-zip.org/download.html>

## Part 01: Download VMs and verify their integrity

Download the following files from the resources link on FOL and place them into your INFO6065 folder dedicated to VMs for this course. Copy and paste the entire link to download the files.

Verify the integrity of your downloads by checking the **MD5** hash value. Your checksums should match the ones listed below:

<b>kali-linux-2022.3-vmware-amd64.7z</b>	fef1925dc0bd9f243d0b423575da9679
<b>metasploitable-linux-2.0.0.zip</b>	abb0a95bd4422397ed235a7284e2ed7f
<b>W7.7z</b>	99bb1334759ddecda77328cc250d9b4
<b>Win10.7z</b>	f89f48c268e3c37877ba4d0ba0182c41
<b>win2016x64.7z</b>	3f8ba3da966daed290eeb0161c7c8c39

For this step, you may utilize a file integrity checker of your choice. FCIV is a Microsoft checksum verifier tool that is freely available. I'm using PowerShell to give me the **MD5** hashes of all the VMs in my new folder as shown below:

```
Windows PowerShell
PS D:\> Get-FileHash -Algorithm MD5 -Path (Get-ChildItem ".\6065 VMs\*" -Recurse)

Algorithm      Hash                                          Path
-----
MD5            FEF1925DC0BD9F243D0B423575DA9679          D:\6065 VMs\kali-linux-2022.3-vmware-amd64.7z
MD5            ABB0A95BD4422397ED235A7284E2ED7F          D:\6065 VMs\metasploitable-linux-2.0.0.zip
MD5            99BB1334759DDECDAC77328CC250D9B4          D:\6065 VMs\W7.7z
MD5            F89F48C268E3C37877BA4D0BA0182C41          D:\6065 VMs\Win10.7z
MD5            3F8BA3DA966DAED290EEB0161C7C8C39          D:\6065 VMs\win2016x64.7z
```

### Slide 01:

- Take a screenshot showing the MD5 checksum information for all the VMs as shown above and place it into Slide 01

## Part 02: Configure the Kali Linux VM

- Use 7z to extract the **kali-linux-2022.3-vmware-amd64.7z** file
- Open the .vmx file and power on the VM
- When asked whether you have moved or copied this VM, choose **"I Moved it"**
- Once powered on, log in with kali/kali

- Make sure you have an internet connection by pinging **google.ca** (if not, troubleshoot)

## Change the hostname

- Open a terminal window within the GUI environment
- Type **sudo nano /etc/hostname** at the terminal prompt to open the /etc/hostname file with nano
- Replace **kali** with **FOLusername**. (Your FOL username, No underscores, No spaces)
- **Reboot** Kali and login again (you can use the GUI menu, or the CLI with sudo to reboot)

## Update Hosts File

We need to edit our **/etc/hosts** file to prevent some potential issues with name resolution

You need to **add** an entry to your hosts file with your **FOLusername-kali**. If your FOLusername is artmack, the new entry will look as follows: (don't remove any of the existing entries, add a new one)

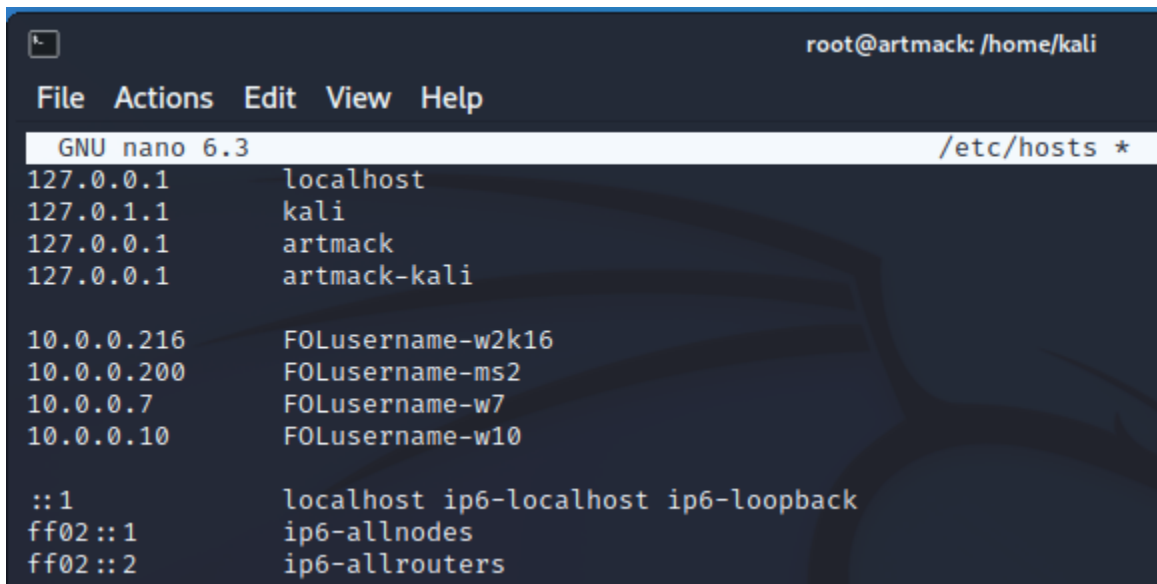
```
127.0.0.1    artmack-kali
```

Your hostname will be the portion of your command prompt following the @ symbol:

Example: root@**artmack**

Now add an entry for the other VMs you have. It is to comprise of your FOLusername followed by an identifying acronym as shown below:

```
10.0.0.216  FOLusername-W2K16
10.0.0.200  FOLusername-MS2
10.0.0.7    FOLusername-W7
10.0.0.10   FOLusername-W10
```



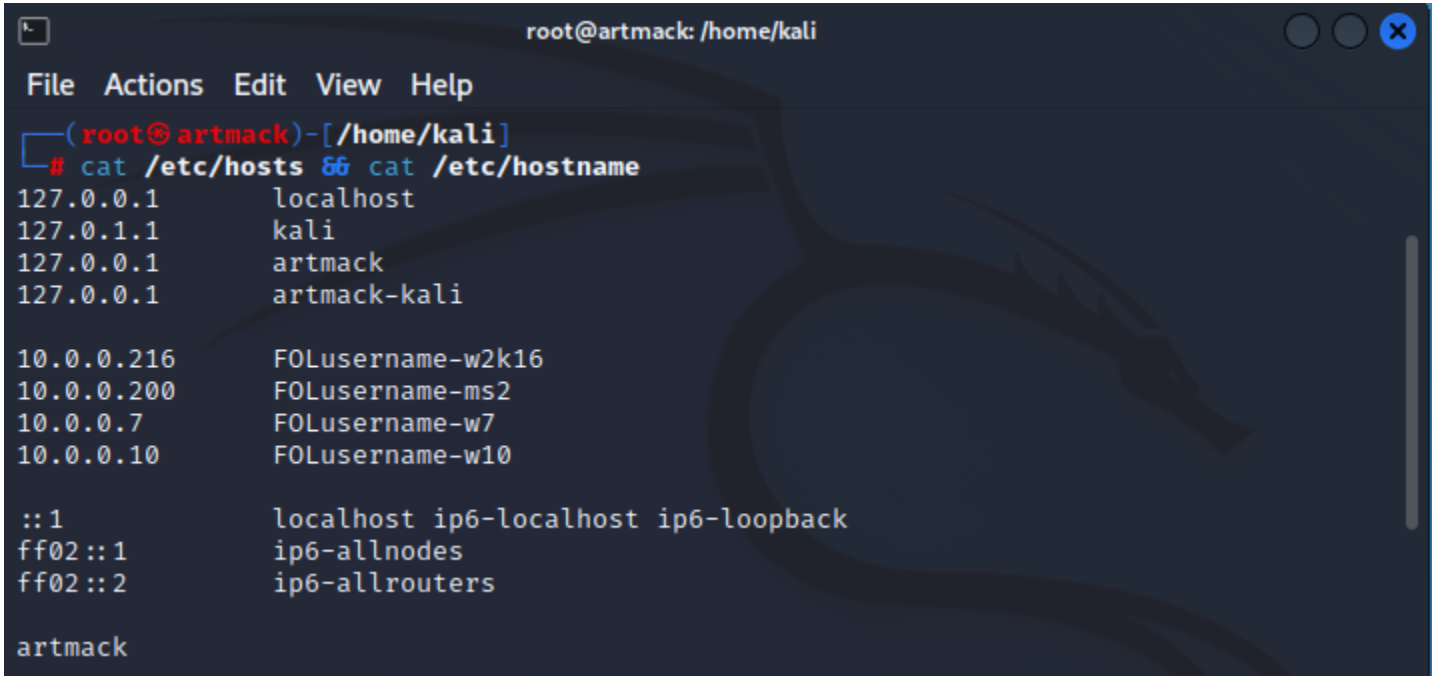
```
root@artmack: /home/kali
File Actions Edit View Help
GNU nano 6.3 /etc/hosts *
127.0.0.1    localhost
127.0.1.1    kali
127.0.0.1    artmack
127.0.0.1    artmack-kali

10.0.0.216   FOLusername-w2k16
10.0.0.200   FOLusername-ms2
10.0.0.7     FOLusername-w7
10.0.0.10    FOLusername-w10

::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

Once you have these entries in place, use the cat command to view the contents of your files:

**cat /etc/hosts && cat /etc/hostname**



```
root@artmack: /home/kali
File Actions Edit View Help
(root@artmack)-[/home/kali]
# cat /etc/hosts && cat /etc/hostname
127.0.0.1      localhost
127.0.1.1      kali
127.0.0.1      artmack
127.0.0.1      artmack-kali

10.0.0.216     FOLusername-w2k16
10.0.0.200     FOLusername-ms2
10.0.0.7       FOLusername-w7
10.0.0.10      FOLusername-w10

::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters

artmack
```

## Slide 02:

- Take a screenshot showing the above information, including your hostname

## Regenerate SSH Keys

We are going to create new SSH keys for use later in the course. This will ensure your keys are unique. At this point you all have the same keys because you are using the same VM

- Move into the **/etc/ssh** directory
  - ✓ Do an **ls -ail** to see all the files
- Create a new directory called **default-kali-keys**
- Move all the files that start with **ssh\_host\_** into the directory you just created (use the **mv** command) (remember you can use the **\*** wildcard to move multiple files at once)
  - ✓ Confirm that the files have moved
- Use the **dpkg-reconfigure openssh-server** command to regenerate the keys
  - ✓ Once the command completes you will have new keys (use **ls -ail** to confirm)
- To confirm that the keys are indeed different we will use the **md5sum** command
  - ✓ From the **/etc/ssh** directory, do an **md5sum** of all the keys that start with **ssh\_host\_**
    - (hint: use a wildcard)
  - ✓ From the **/etc/ssh** directory, do an **md5sum** of all the keys in the **default-kali-keys** directory that start with **ssh\_host\_**
- Now we are going to ensure SSH will start with the **service ssh start** command
- Use the **netstat -antp | grep sshd** command to confirm the port is up and listening

**Slide 03: (all commands executed from the /etc/ssh directory)**

- md5sum of all the new keys that start with ssh\_host\_
- md5sum of all the original keys in the default-kali-keys directory that start with ssh\_host\_
- output of service ssh start (you can run it again without any problems)
- output of netstat -antp | grep sshd

**Add a LAN Segment Network**

- In VMware Workstation, add a new network adapter
- Add the new adapter to a LAN segment named **INFO-6065**
- You will need to configure your **/etc/network/interfaces** file to add a static IP address to the new adapter
- This lab uses 10.0.0.99 as the static IP for Kali Linux (You can choose your own IP if you'd like)

Shutdown the VM and take a Snapshot called **Basic Kali Setup**

**Part 03: Configure Windows 10 Client VM**

Extract the copy of Windows 10 you downloaded into the directory where you are storing the VMs for this course. DO NOT mix these VMs with your other courses!

**Modify the Windows 10 VM**

Before you power on the VM, open the Virtual Machine settings window and make the following changes:

- Remove the floppy drive
- Change the network adapter to LAN Segment **INFO-6065**
- Change the memory allocation to suit your laptop: 2048, 3096, etc.

**Initial Power on of the W10 VM**

- When asked whether you have moved or copied this VM, choose **"I Moved it"**
- The password is **Windows1**
- (You may be prompted to restart. If so, restart the VM)
- Choose the **"Work Network"** if prompted (you identify the network you are connecting to)

**Change Your Computer Name**

Your current computer name will be **DESKTOP-5EOT2G5**

You need to change your computer name to **FOLusername-W10** (use your FOL username):

- Remove any special symbols such as the underscore (\_) or dot (.)
- Your FOLusername should only have letters (a-z) and numbers
- If your FOLusername is more than 12 characters long, use only the first **12 characters**

**Example:**

If my FOLusername is a\_mackiewicz2. I'd be using amackiewicz2 (underscore removed)

If your username is r\_ginger45, you need to use rginger45

You will need to restart the VM once you have made changes to the computer name. Once it reboots, login as FOLusername/Windows1

## Disable Your Firewall

If your Windows Firewall on your Windows 10 VM is on, turn it off

Turn the Windows Firewall off for: **Domain Profile, Private Profile, Public Profile**

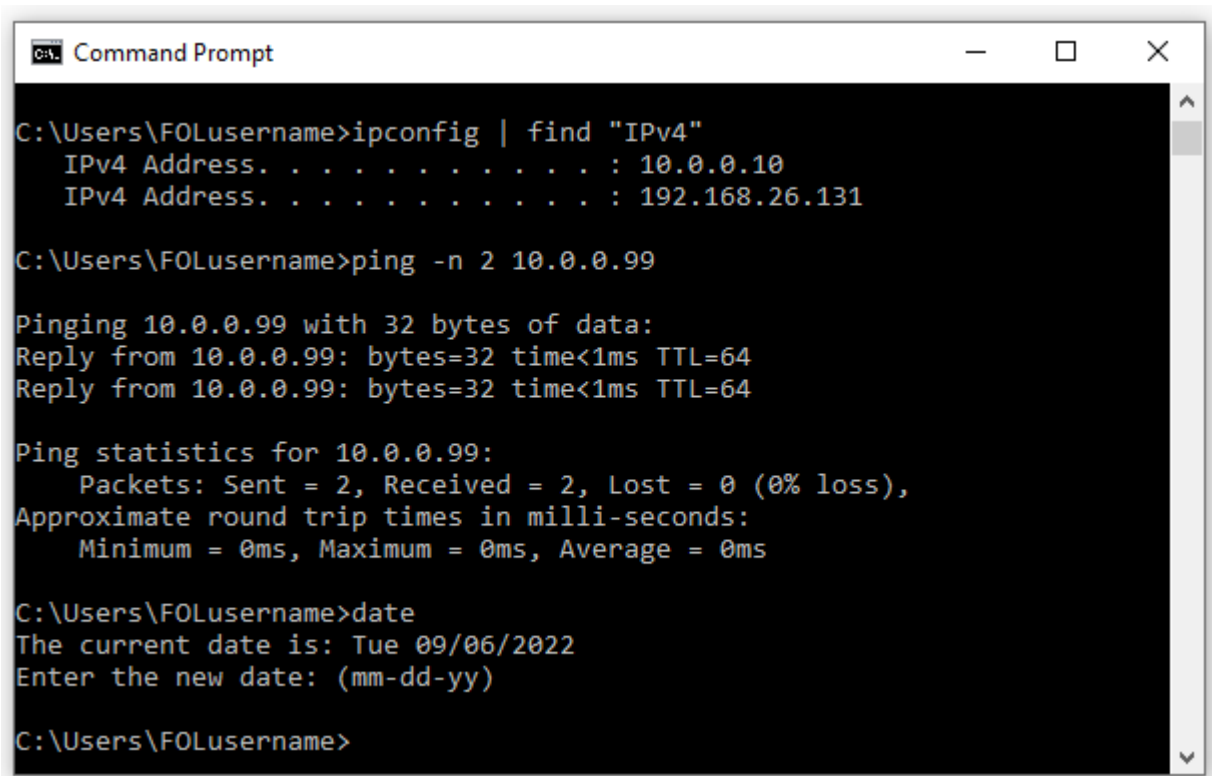
(Remember: The above step is done on your VM – not your host machine)

## LAN Segment IP Settings

Ensure your W10 VM is on the **INFO-6065** LAN segment, then assign it the following IPv4 settings:

- IP Address 10.0.0.10
- Subnet Mask: 255.255.255.0

Confirm your settings and connectivity to the Kali Linux VM using the commands shown below:



```
C:\Users\FOLusername>ipconfig | find "IPv4"
    IPv4 Address. . . . . : 10.0.0.10
    IPv4 Address. . . . . : 192.168.26.131

C:\Users\FOLusername>ping -n 2 10.0.0.99

Pinging 10.0.0.99 with 32 bytes of data:
Reply from 10.0.0.99: bytes=32 time<1ms TTL=64
Reply from 10.0.0.99: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.99:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\FOLusername>date
The current date is: Tue 09/06/2022
Enter the new date: (mm-dd-yy)

C:\Users\FOLusername>
```

### Slide 04:

- Ensure that you are using your FOLusername.
- Take a screenshot showing all the above and place it into slide 04

## Part 04: Configure Windows 7 Client VM

### Modify the Windows 7 VM

Before you power on the VM, open the Virtual Machine settings window, and make the following changes:

- Remove the floppy drive
- Change the network adapter to LAN Segment **INFO-6065**
- Change the memory allocation to suit your laptop: 2048, 3096, etc.

### Initial Power on of the W7 VM

- When asked whether you have moved or copied this VM, choose **“I Moved it”**
- The password is **Windows1**
- (You may be prompted to restart. If so, restart the VM)
- Choose the **“Work Network”** if prompted (you identify the network you are connecting to)

### Change Your Computer Name

Your current computer name will be **User-PC**

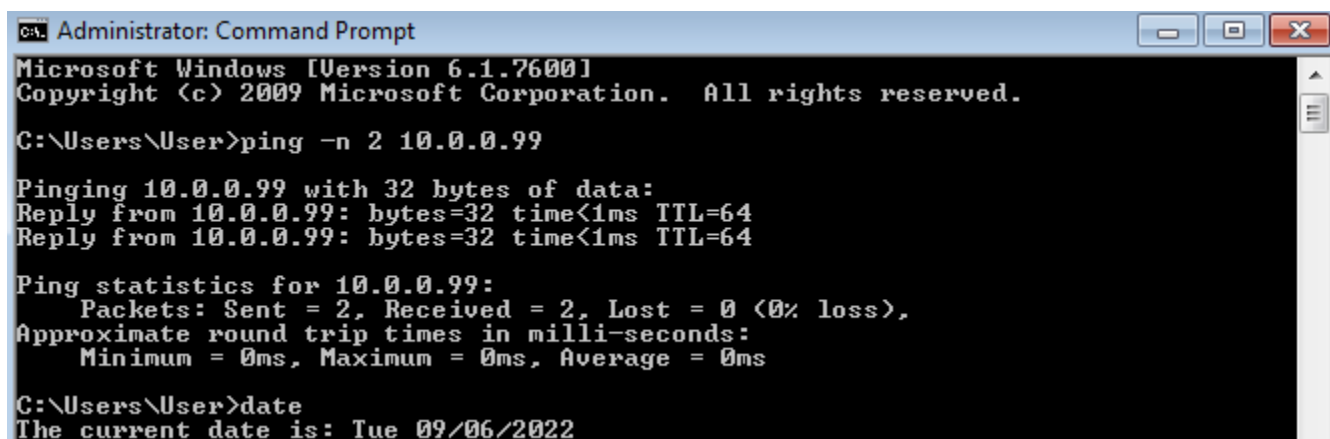
You need to change your computer name to **FOLusername-W7** (use your FOL username):

- Remove any special symbols such as the underscore (\_) or dot (.)
- Your FOLusername should only have letters (a-z) and numbers
- If your FOLusername is more than 12 characters long, use only the first **12 characters**

Ensure your W7 VM is on the **INFO-6065** LAN segment, then assign it the following IPv4 settings:

- IP Address 10.0.0.7
- Subnet Mask: 255.255.255.0

Ensure that you have connectivity between Kali Linux and the W7 VM using ping



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\User>ping -n 2 10.0.0.99

Pinging 10.0.0.99 with 32 bytes of data:
Reply from 10.0.0.99: bytes=32 time<1ms TTL=64
Reply from 10.0.0.99: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.99:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

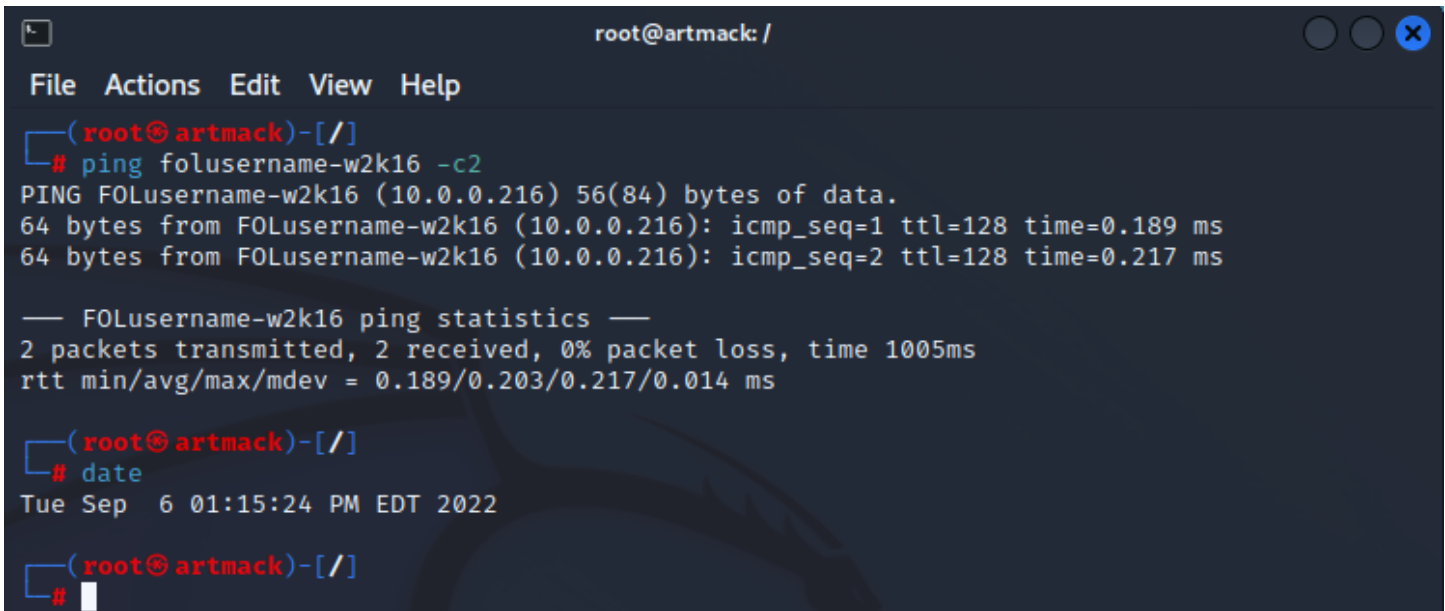
C:\Users\User>date
The current date is: Tue 09/06/2022
```

### Slide 05:

- Ensure that you are using your FOLusername.
- Take a screenshot showing all the above and place it into slide 05

## Part 05: Windows Server 2016 Prep

- Use 7z to unzip the **win2016x64.7z** file with the password of **Juniper**
- Open the .vmx file and change the Network adapter to LAN segment **INFO-6065**
- Power on the VM
- When asked whether you have moved or copied this VM, choose **"I Moved it"**
- Once powered on, log in using the password of **Windows1**
- Change your network settings to:
  - ✓ IP address: 10.0.0.216
  - ✓ Subnet mask: 255.255.255.0
- Turn off the firewall for both Private and Public network settings
- Ping the Windows 2016 server from Kali twice using the hostname



```
root@artmack: /
File Actions Edit View Help
(root@artmack)-[/]
# ping folusername-w2k16 -c2
PING FOUsername-w2k16 (10.0.0.216) 56(84) bytes of data.
64 bytes from FOUsername-w2k16 (10.0.0.216): icmp_seq=1 ttl=128 time=0.189 ms
64 bytes from FOUsername-w2k16 (10.0.0.216): icmp_seq=2 ttl=128 time=0.217 ms

— FOUsername-w2k16 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 0.189/0.203/0.217/0.014 ms

(root@artmack)-[/]
# date
Tue Sep  6 01:15:24 PM EDT 2022

(root@artmack)-[/]
#
```

### Slide 06:

- Take a screenshot showing two successful pings using the correct option
- The output of the date command

## Part 06: Metasploitable2 Server Prep

- Unzip the metasploitable-linux-2.0.0.zip file
- Change the primary network adapter to LAN segment **INFO-6065**
- Remove the secondary network adapter
- Open the .vmx file and power on the VM
- When asked whether you have moved or copied this VM, choose **"I Moved it"**
- Once powered on, log in using the username/password of **msfadmin/msfadmin**



### Change hostname and network adapter settings

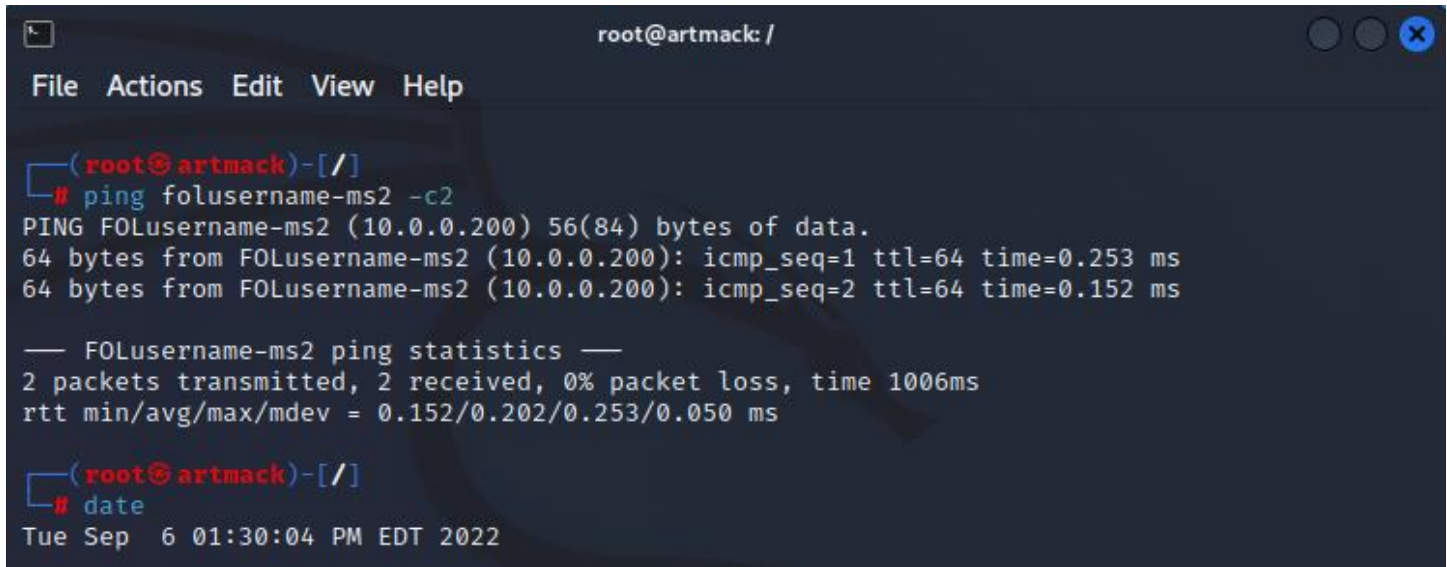
- Adjust the `/etc/hostname` file to `FOLusername-ms2`

Next, modify the `/etc/network/interfaces` file to have the following IP settings for adapter `eth0`:

- address `10.0.0.200`
- netmask `255.255.255.0`
- network `10.0.0.0`
- broadcast `10.0.0.255`

Reboot the VM

- Ping the `Metasploitable2` server from Kali twice using the hostname



```
root@artmack: /  
File Actions Edit View Help  
  
(root@artmack)-[/]  
# ping folusername-ms2 -c2  
PING FOLusername-ms2 (10.0.0.200) 56(84) bytes of data.  
64 bytes from FOLusername-ms2 (10.0.0.200): icmp_seq=1 ttl=64 time=0.253 ms  
64 bytes from FOLusername-ms2 (10.0.0.200): icmp_seq=2 ttl=64 time=0.152 ms  
  
— FOLusername-ms2 ping statistics —  
2 packets transmitted, 2 received, 0% packet loss, time 1006ms  
rtt min/avg/max/mdev = 0.152/0.202/0.253/0.050 ms  
  
(root@artmack)-[/]  
# date  
Tue Sep  6 01:30:04 PM EDT 2022
```

### Slide 07:

- Take a screenshot showing two successful pings using the correct option
- The output of the `date` command



**IMPORTANT!** – Ensure that all your VMs can ping each other on the **INFO-6065 LAN** segment prior to next week's lab

\*\*\* Take a snapshot of all the VMs named **After Lab 01** \*\*\*