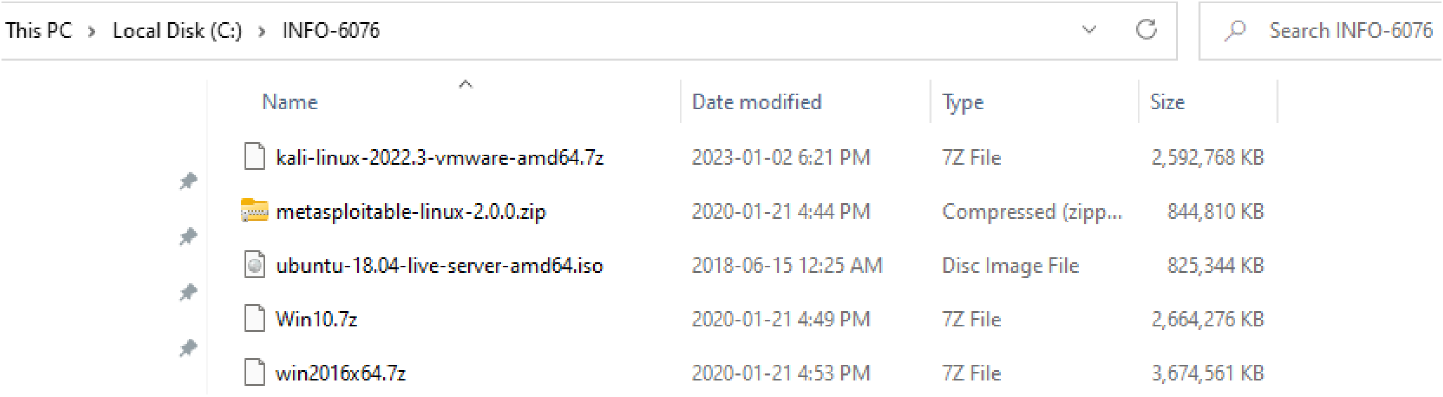
Lab 01 Requirements

- Internet connectivity & VMware Workstation version 15.5.7 or above
- 7zip installed on your host machine: http://www.7-zip.org/download.html

Part 01: Download Client VM zip files and verify SHA1 checksums

You will need to download the following VMs from the ***VM Download links*** section on FOL and place them into a dedicated folder on your host machine for INFO-6076 VMs:

kali-linux-2022.3-vmware-amd64.7z
win10.7z
ubuntu-18.04-live-server-amd64.iso
win2016x64.7z
metasploitable-linux-2.0.0.zip



Name	Date modified	Type	Size
kali-linux-2022.3-vmware-amd64.7z	2023-01-02 6:21 PM	7Z File	2,592,768 KB
metasploitable-linux-2.0.0.zip	2020-01-21 4:44 PM	Compressed (zipp...	844,810 KB
ubuntu-18.04-live-server-amd64.iso	2018-06-15 12:25 AM	Disc Image File	825,344 KB
Win10.7z	2020-01-21 4:49 PM	7Z File	2,664,276 KB
win2016x64.7z	2020-01-21 4:53 PM	7Z File	3,674,561 KB

Slide 01:

- Take a screenshot showing the downloaded files and place it into slide 01

Select a file integrity checker of your preference and do a **SHA1 checksum** of the zipped images

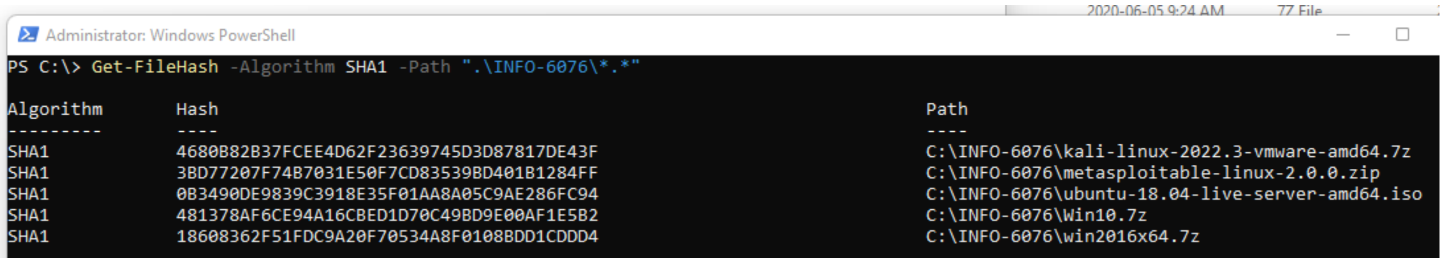
Your **SHA1** hash checksums should match the ones listed below:

kali-linux-2022.3-vmware-amd64.7z	4680B82B37FCEE4D62F23639745D3D87817DE43F
metasploitable-linux-2.0.0.zip	3BD77207F74B7031E50F7CD83539BD401B1284FF
ubuntu-18.04-live-server-amd64.iso	0B3490DE9839C3918E35F01AA8A05C9AE286FC94
Win10.7z	481378AF6CE94A16CBED1D70C49BD9E00AF1E5B2
win2016x64.7z	18608362F51FDC9A20F70534A8F0108BDD1CDDD4

You should see the same checksum results as listed above and shown in the example screenshot. If your checksum does not match, check to ensure that you are using the correct algorithm (i.e., MD5 vs SHA1 etc.). If the correct algorithm is used and your checksum still does not match, your download might be corrupted or incorrect. If this is the case, you will need to download the file(s) again.

As an example, you can use Windows PowerShell to obtain the SHA1 hash value for the downloaded VM files as shown below:

Command used: `Get-FileHash -Algorithm SHA1 -Path ".\INFO-6076\*.*"`



```
PS C:\> Get-FileHash -Algorithm SHA1 -Path ".\INFO-6076\*.*"

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA1            4680B82B37FCEE4D62F23639745D3D87817DE43F                               C:\INFO-6076\kali-linux-2022.3-vmware-amd64.7z
SHA1            3BD77207F74B7031E50F7CD83539BD401B1284FF                               C:\INFO-6076\metasploitable-linux-2.0.0.zip
SHA1            0B3490DE9839C3918E35F01AA8A05C9AE286FC94                               C:\INFO-6076\ubuntu-18.04-live-server-amd64.iso
SHA1            481378AF6CE94A16CBED1D70C49BD9E00AF1E5B2                               C:\INFO-6076\Win10.7z
SHA1            18608362F51FDC9A20F70534A8F0108BDD1CDDD4                               C:\INFO-6076\win2016x64.7z
```

Slide 02:

- Take a screenshot showing your **SHA1** checksums place it into slide 02

Part 02: Kali Linux VM Prep

- Unzip 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 as the credentials
- Make sure you have an internet connection by pinging **google.ca** (if not, troubleshoot)
- You may want to update the VM but it will take some time. Make sure you have enough time before proceeding by entering the following commands:

```
apt-get update
apt-get upgrade
```

If you decide to update and upgrade, it may take some time to complete, and you may receive errors if you have an anti-virus running. If you are unable to upgrade everything, that is okay as this step is optional.

Note: You may want to disable your anti-virus program for this step. This may take some time so ensure that your machine has a power source available

Change hostname

- Open a terminal window within the GUI environment
- Type **vi /etc/hostname** at the terminal prompt to open the /etc/hostname file in VI
- 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)

Update Hosts File

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

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

```
127.0.0.1      artmack
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 webservers you will build. It is to comprise of your FOLusername followed by an identifying acronym as shown below:

```
10.0.0.200    FOLusername-uws
10.0.0.201    FOLusername-iis
10.0.0.202    FOLusername-ms2
```

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

cat /etc/hosts

Change Your Password

Change your password so that it matches your **FOLusername** using the following command:

passwd

Enter new password
Confirm new password

Test the new password by logging out and logging back in
Note: you are still logging into the root account

LAN Segment

Before proceeding, create a LAN segment in VMware called **INFO-6076** by going to VM → Settings in your VMware Workstation and selecting *Network Adapter* under the Hardware tab

Add a new network adapter and set it to LAN segment INFO-6076 and click OK

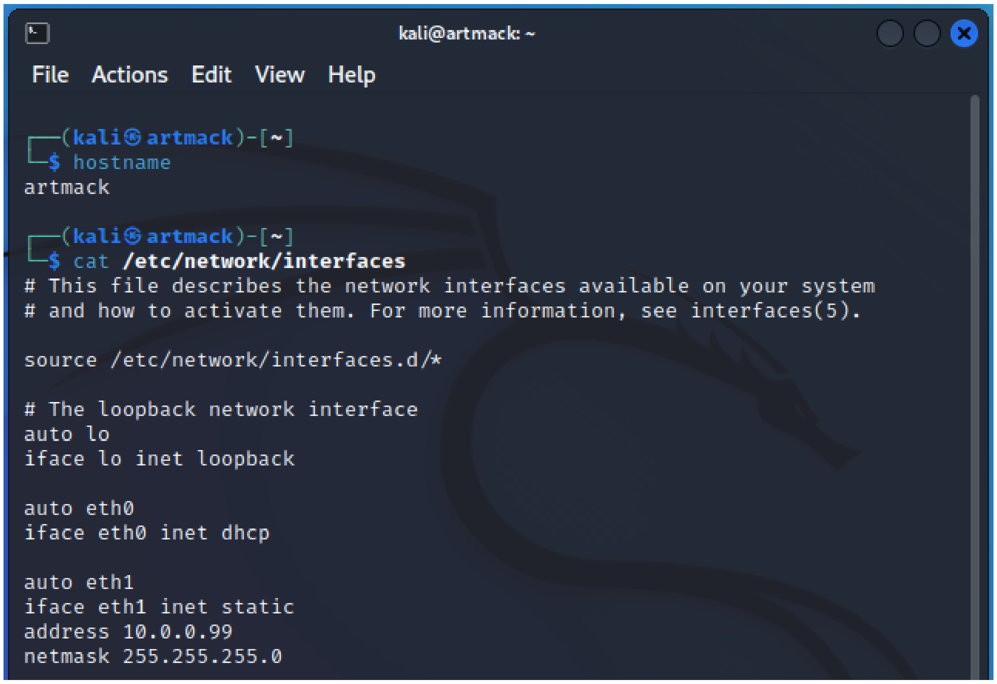
You should now have two network adapters on your Kali Linux VM. The first one (eth0) will be left with DHCP on and NAT as the VMware network setting. The second network adapter (eth1) you created will set to the INFO-6076 LAN segment and use a static IP address.

Next, modify the **/etc/network/interfaces** file to have the following IP information for the newly created network adapter eth1:

- address 10.0.0.99
- netmask 255.255.255.0

Save the file and exit. Reboot your Kali Linux VM

Once it comes back online, show your hostname, and interface settings



```
┌──(kali㉿artmack)-[~]
└─$ hostname
artmack

┌──(kali㉿artmack)-[~]
└─$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet static
address 10.0.0.99
netmask 255.255.255.0
```

Slide 03:

- Take a screenshot showing the output of the **hostname** command & the contents of the **/etc/network/interfaces** file and place it into slide 03

Part 03: Windows 10 VM Prep

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-6076**
- 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:
My FOLusername is a_mackiewicz2. I'll 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

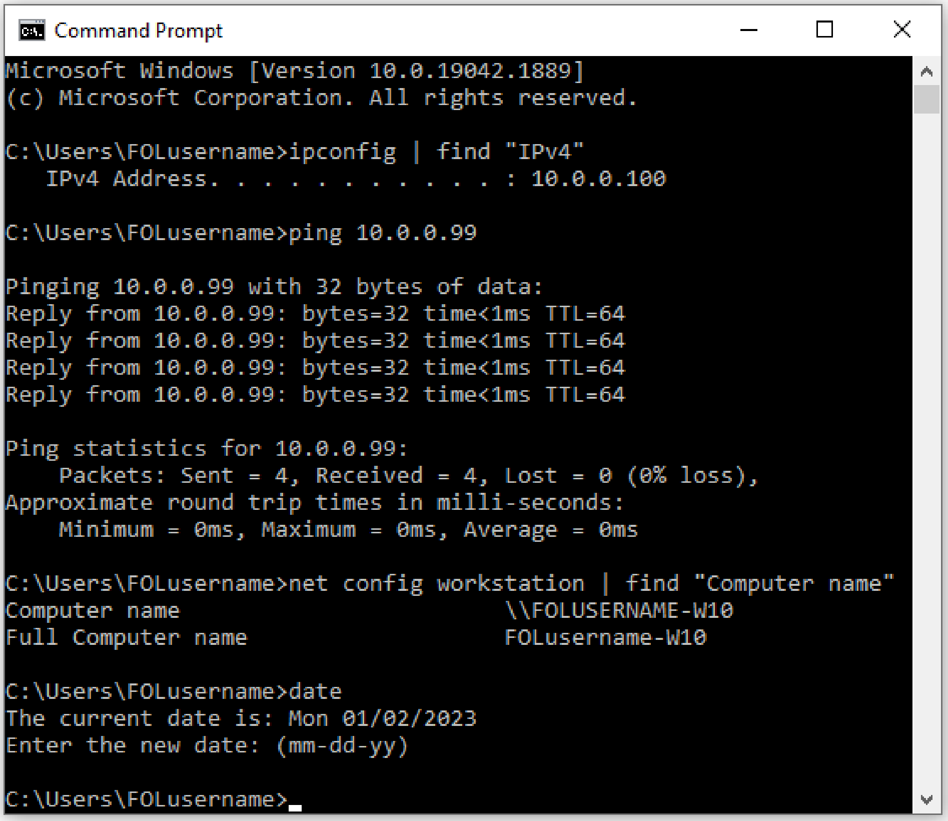
If your Windows Firewall on your Windows 10 VM is on, turn it off
Turn the Windows Firewall off for: **Domain Profile, Private Profile, Public Profile**
(**Remember**: The above step is done on your VM – not your host machine)

LAN Segment IP Settings

Ensure your W10 VM is on the **INFO-6076** LAN segment, then assign it the following IPv4 settings:

- IP Address 10.0.0.100 Subnet Mask: 255.255.255.0

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



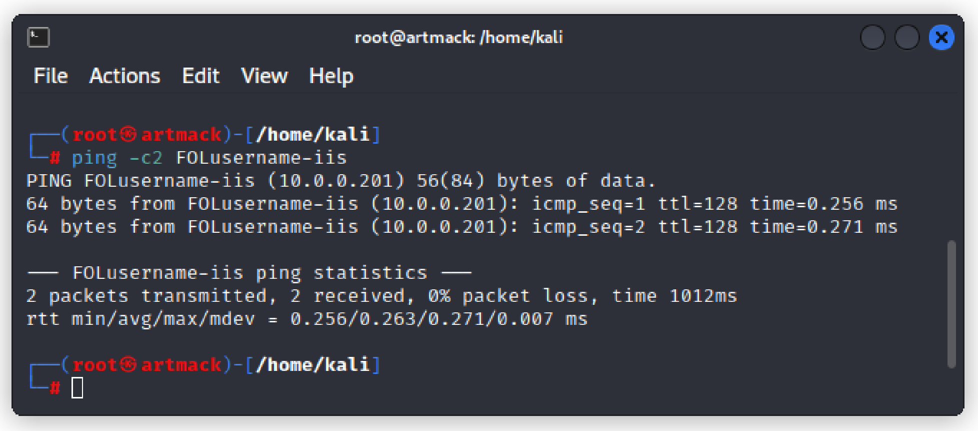
```
Microsoft Windows [Version 10.0.19042.1889]
(c) Microsoft Corporation. All rights reserved.

C:\Users\FOLusername>ipconfig | find "IPv4"
   IPv4 Address. . . . . . . . . . . : 10.0.0.100

C:\Users\FOLusername>ping 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
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 = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\FOLusername>net config workstation | find "Computer name"
Computer name                        \\FOLUSERNAME-W10
Full Computer name                   FOLusername-W10

C:\Users\FOLusername>date
The current date is: Mon 01/02/2023
Enter the new date: (mm-dd-yy)

C:\Users\FOLusername>_
```

Slide 04:

- Take a screenshot showing the output of the following **cmd.exe** commands from your W10 VM:
  - ipconfig | find "IPv4"
  - ping 10.0.0.99
  - net config workstation | find "Computer name"
  - date

Part 04: Windows Server 2016 Prep

- Unzip the **win2016x64.7z** file using the password of **Juniper**
- Change the Network adapter to LAN segment **INFO-6076**
- Open the .vmx file and power on the VM
- If 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: 10.0.0.201
  - ✓ 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)-[/home/kali]
└─# ping -c2 FOLusername-iis
PING FOLusername-iis (10.0.0.201) 56(84) bytes of data.
64 bytes from FOLusername-iis (10.0.0.201): icmp_seq=1 ttl=128 time=0.256 ms
64 bytes from FOLusername-iis (10.0.0.201): icmp_seq=2 ttl=128 time=0.271 ms

── FOLusername-iis ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1012ms
rtt min/avg/max/mdev = 0.256/0.263/0.271/0.007 ms

┌──(root㉿artmack)-[/home/kali]
└─# 
```

Slide 05:

- Take a screenshot showing two successful pings from Kali Linux to **FOLusername-iis** and place it into slide 05

Part 05: Metasploitable2 Server Prep

- Unzip the metasploitable-linux-2.0.0.zip file
- Change the primary network adapter to LAN segment **INFO-6076**
- 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

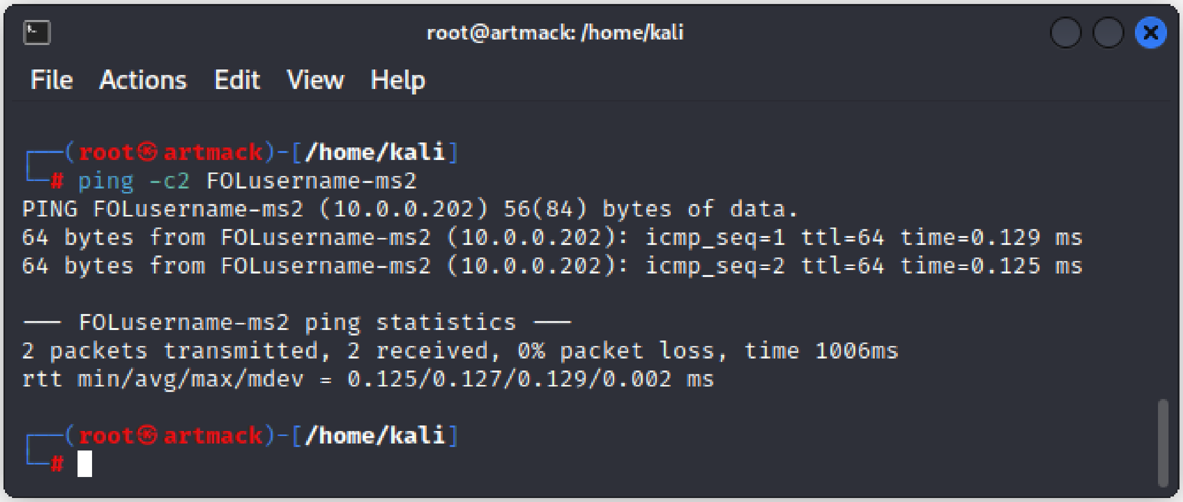
- Adjust the /etc/hostname file to FOLusername-ms2

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

- address 10.0.0.202
- 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)-[/home/kali]
└─# ping -c2 FOLusername-ms2
PING FOLusername-ms2 (10.0.0.202) 56(84) bytes of data.
64 bytes from FOLusername-ms2 (10.0.0.202): icmp_seq=1 ttl=64 time=0.129 ms
64 bytes from FOLusername-ms2 (10.0.0.202): icmp_seq=2 ttl=64 time=0.125 ms

—— FOLusername-ms2 ping statistics ——
2 packets transmitted, 2 received, 0% packet loss, time 1006ms
rtt min/avg/max/mdev = 0.125/0.127/0.129/0.002 ms

┌──(root㉿artmack)-[/home/kali]
└─# 
```

Slide 06:

- Take a screenshot showing two successful pings from Kali Linux to **FOLusername-ms2** and place it into slide 06

Part 06: Ubuntu 18.04 LTS Web Server Prep

Open VMware Workstation and go to File → New Virtual Machine…

- Custom
- Workstation 15.x (default)
- Select Installer disc image file (iso): and Browse to your Ubuntu ISO file that you downloaded
- Make sure your username is your FOLusername in all lowercase characters
- Select a password of **Ubuntu1**
- Name the VM: **Ubuntu Web Server 6076**
- For Location, select your INFO-6076 folder where you keep your VMs for this course and create a new folder called *Ubuntu Web Server 1804*
- Select 1 for *Number of processors* and 2 for *Number of cores per processor*
- Select the amount of RAM/Memory for the VM as your hardware can allow (min. 2048 MB)
- Select *Use network address translation (NAT)*
- Select LSI Logic
- Select SCSI
- Select *Create a new virtual disk*
- Set *Maximum disk size (GB)* to 40
- Select *Split virtual disk into multiple files*
- Leave the default for the Disk File name
- Select *Power on this virtual machine after creation* and click on **Finish**

Once the VM powers on, you will need to go through the installation process

Help can be found here: https://tutorials.ubuntu.com/tutorial/tutorial-install-ubuntu-server?_ga=2.249328455.1774373488.1529036320-128140120.1529036320#3

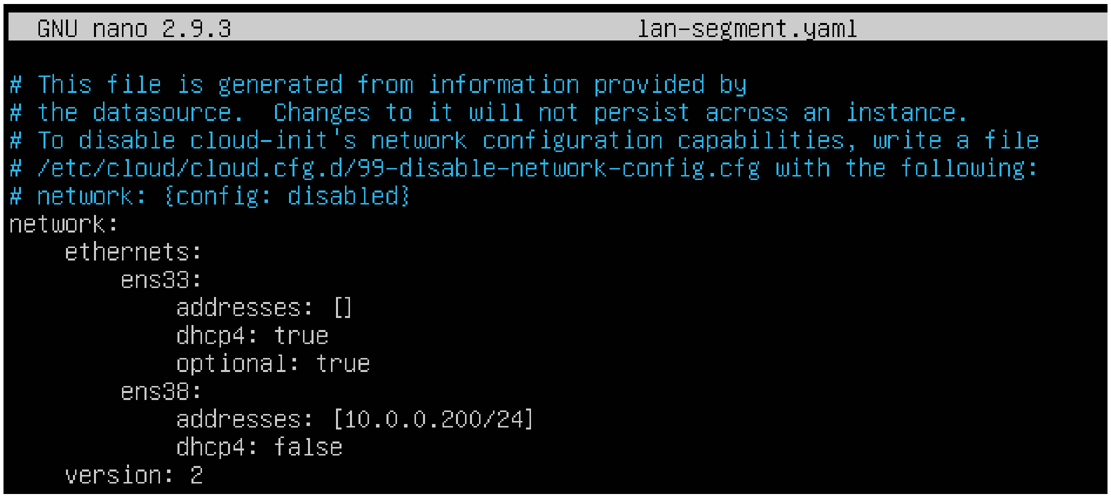
- Select English as your preferred language
- Select the default keyboard layouts
- Install Ubuntu
- Will use DHCP ….
- No proxy so just hit enter for the default
- Select *Use An Entire Disk*
- Your default should say something like /dev/sda (if that's the case, hit enter to continue)
- Leave the Filesystem setup menu at default, hit enter to select *Done*
- When prompted if you want to continue, select *Continue*
  - ✓ Your name: FOLusername
  - ✓ Your server's name: folusername-uws
  - ✓ Pick a username: folusername
  - ✓ Choose a password: Ubuntu1
  - ✓ Confirm your password: Ubuntu1
  - ✓ Import SSH identity: No
- Select *Reboot Now …* Wait for the system to do its thing
- The installation process may take a while, so be patient (If it looks like it is stuck, hit enter)
- Login using folusername/Ubuntu1

Change hostname

- Use a text editor such as **vi** or **nano** to open the **/etc/hostname** file in the terminal window
- Change the contents of the file to reflect your **FOLusername-uws** entry and save the file

LAN Segment

- Add another Network Adapter to the VM place it on the INFO-6076 LAN segment
- Reboot the Ubuntu VM
- Move into the **/etc/netplan** directory and issue the **ls –ail** command
- You should see only one file in there currently. Copy that file using the following command:
  sudo cp 50-cloud-init.yaml lan-segment.yaml
- This will create a copy of the original file and name it lan-segment.yaml allowing us to make changes to the new file by setting a static IP to your new Network Adapter
- Use a text editor to modify **lan-segment.yaml** as shown in the following screenshot example:

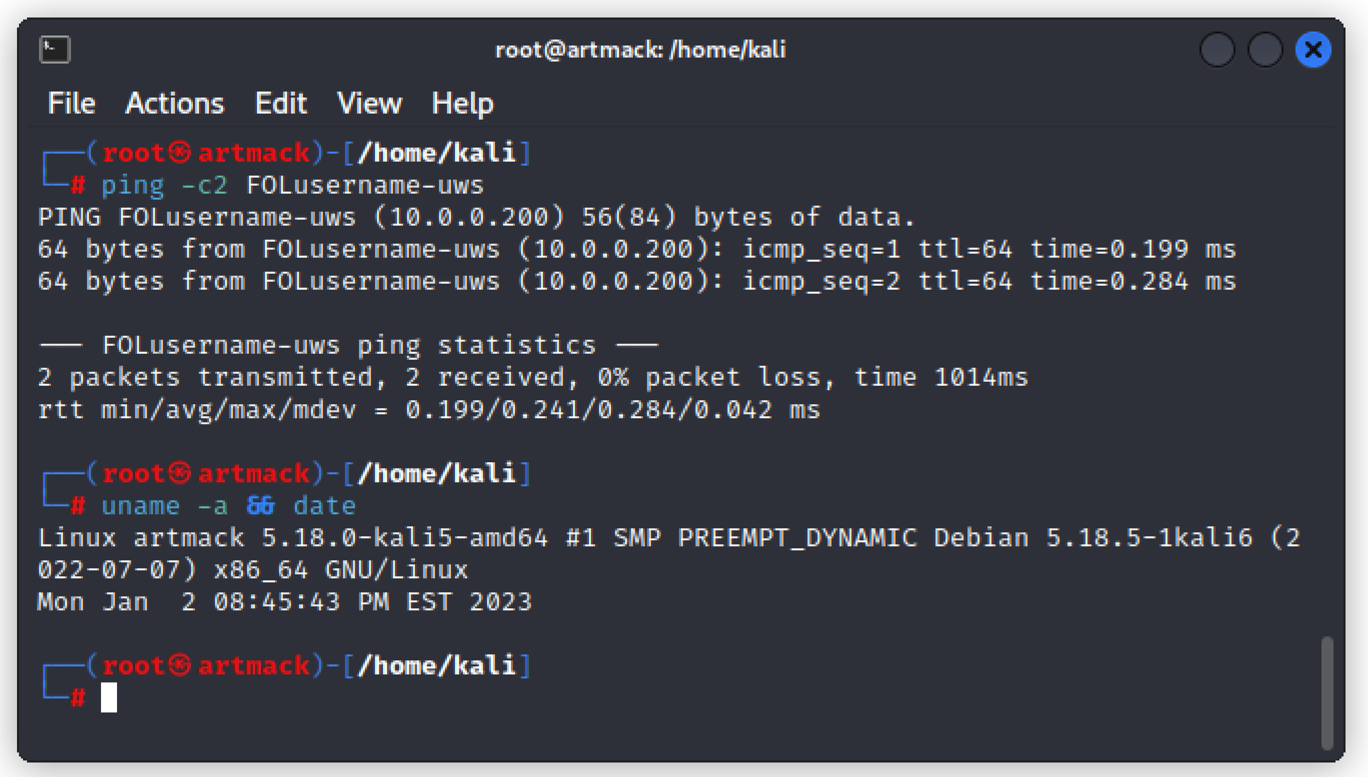


```
  GNU nano 2.9.3                          lan-segment.yaml

# This file is generated from information provided by
# the datasource.  Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        ens33:
            addresses: []
            dhcp4: true
            optional: true
        ens38:
            addresses: [10.0.0.200/24]
            dhcp4: false
    version: 2
```

- Save the file and exit

- Apply the changes
  sudo netplan apply

- From the Kali Linux VM, ping the Ubuntu Web Server twice using the hostname and then issue the **uname –a** and **date** commands



```
┌──(root㉿artmack)-[/home/kali]
└─# ping -c2 FOLusername-uws
PING FOLusername-uws (10.0.0.200) 56(84) bytes of data.
64 bytes from FOLusername-uws (10.0.0.200): icmp_seq=1 ttl=64 time=0.199 ms
64 bytes from FOLusername-uws (10.0.0.200): icmp_seq=2 ttl=64 time=0.284 ms

—— FOLusername-uws ping statistics ——
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.199/0.241/0.284/0.042 ms

┌──(root㉿artmack)-[/home/kali]
└─# uname -a && date
Linux artmack 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2
022-07-07) x86_64 GNU/Linux
Mon Jan  2 08:45:43 PM EST 2023

┌──(root㉿artmack)-[/home/kali]
└─# 
```

Slide 07:

- Take a screenshot showing the following and place it into slide 07:
  - Two successful pings from Kali Linux to **FOLusername-uws**,
  - Output of **uname -a**
  - Output of the **date** command

Part 07: LAMP Stack/Mutillidae Installation on the Ubuntu 18.04 LTS Web Server

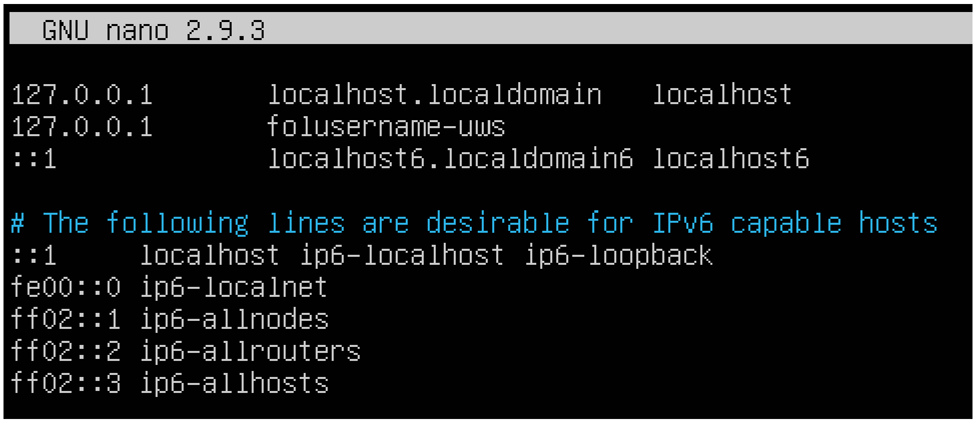
- Select America and Toronto as your location
  sudo dpkg-reconfigure tzdata

- Update the date and time on your Ubuntu Server
  sudo date -s "$(wget -qSO- --max-redirect=0 google.com 2>&1 | grep Date: | cut -d' ' -f5-8)Z"

- Restart the VM:
  sudo shutdown –r now

- Once the VM comes back up, login with your **FOLusername** and password of **Ubuntu1**
- Update your repository list
  sudo apt-get update

- Update your hosts file to include your **FOLusername-uws** in the list. See example below:
  sudo nano /etc/hosts



```
  GNU nano 2.9.3

127.0.0.1       localhost.localdomain   localhost
127.0.0.1       folusername-uws
::1             localhost6.localdomain6 localhost6

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

- Install Apache Server
  sudo apt-get install apache2 apache2-utils

- Install the MYSQL server:
  sudo apt-get install mysql-server

- Configure the MYSQL installation to work with Mutillidae:
  sudo mysql –u root
  use mysql;
  update user set authentication_string=PASSWORD('') where user='root';
  update user set plugin='mysql_native_password' where user='root';
  flush privileges;
  quit;

- Restart MySQL:
  sudo service mysql restart

- Install unzip
  apt-get install unzip
- Download a Mutillidae installation script to your /var/www/ directory by using the following:
  cd /var/www
  sudo wget http://transpirenetworks.com/mutillidae_setup.sh
  (As an alternative, mutillidae_setup.7z is also available with a password of **info6076)**

- Execute the Mutillidae installation script:
  sudo bash mutillidae_setup.sh

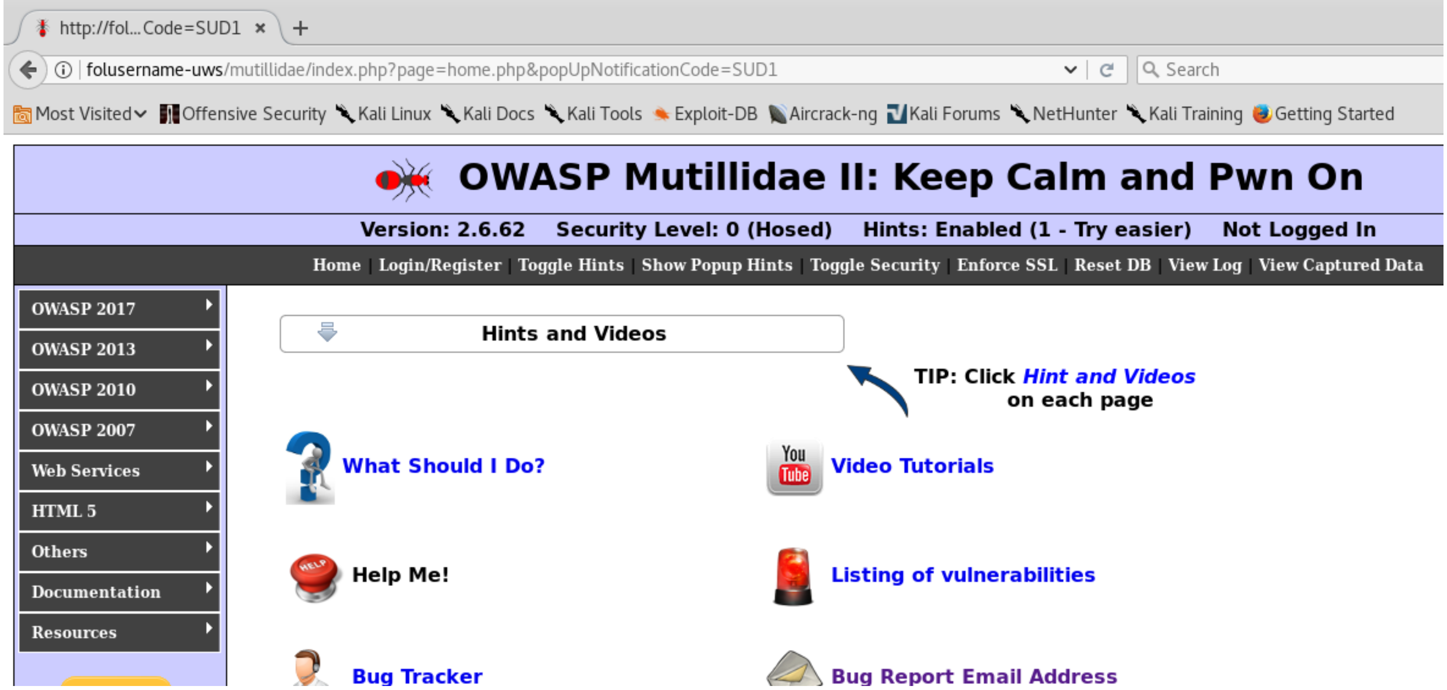
- Unzip the **LATEST-mutillidae-2.6.62.zip** file
  sudo unzip LATEST-mutillidae-2.6.62.zip

IMPORTANT! – Open the **mutillidae_setup.sh** script in a text editor and read through it so that you understand what it is doing. Ensure that you have execute permissions on the script…

If it gets stuck, you can troubleshoot manually by treating each line in the script as a separate command in the Linux terminal.

Navigate to Mutillidae using the Kali Linux VM

- Open the web browser in Kali and navigate to folusername-uws/mutillidae
- You may need to click on setup/reset database
- If you have done everything correctly, your results should look like the example below:



folusername-uws/mutillidae/index.php?page=home.php&popUpNotificationCode=SUD1

Slide 08:

- Take a screenshot showing all the above and place it into slide 08

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