

Lab1 Build Testing Environment

Due by midnight January 19, 2023

20 points

Lab Learning Objectives

- To configure and install software on student's device for future class use
- To install extra testing tools on Kali Linux machine
- To be familiar with cyber.ucmo.edu

Lab Instructions

1. Download and install VMWare Workstation 17 Pro

You will receive an invitation from itacademy brightspace through your UCM email. Please follow the instructions posted to the Lab 1 folder to redeem the invitation and create an account to download the software.

If you are using MacOS, please download and Install VMware Fusion 13 Pro instead. Please be advised that Macbook M1 chip does not support VMWare products at this moment.

2. Download and Install Greenshot (screenshot software)

<https://getgreenshot.org/>

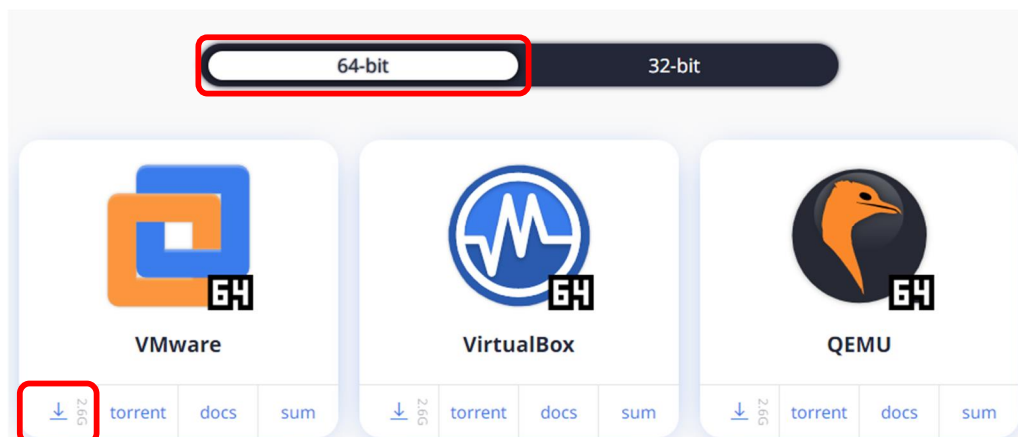
Since Greenshot is a Windows tool, for MacOS user, you can consider using a different tool called Lightshot

<https://app.prntscr.com/en/>

3. Download Kali Linux Virtual Machine

<https://www.kali.org/get-kali/#kali-virtual-machines>

Download the 64bit image (not through the Torrent) for VMware.

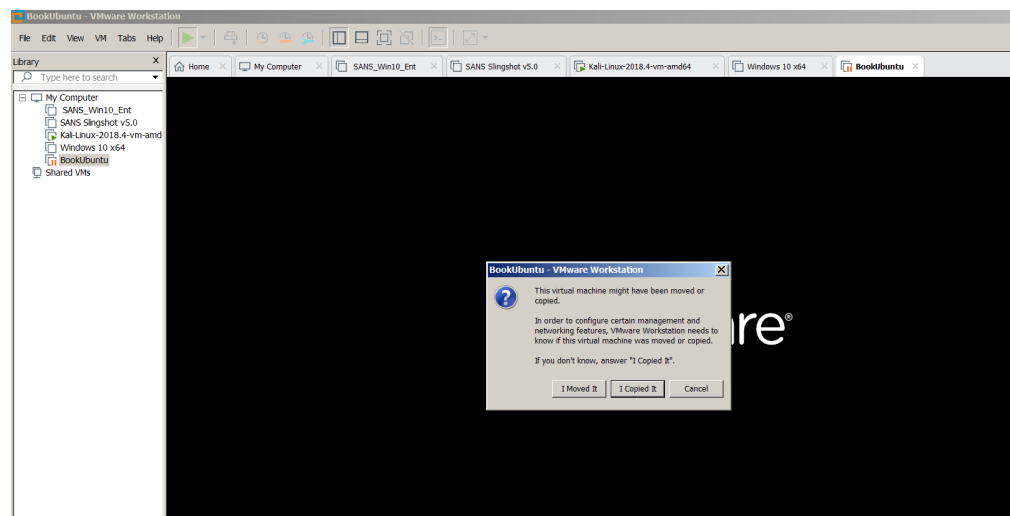


If your host OS is 32 bit, download the 32 bit version instead. Unzip the image. The file is zipped by a utility called 7-zip. If you do not have the utility installed on your computer, please visit <https://www.7-zip.org/download.html> to download and install the software. Choose the 32-bit or 64-bit .exe file based on your operating system. For Mac user, you can use Ez7z at <https://ez7z.en.softonic.com/mac> or Keka at <https://www.keka.io/en/> to unzip the file.

Download 7-Zip 18.06 (2018-12-30) for Windows:

Link	Type	Windows	Description
Download	.exe	32-bit x86	7-Zip for 32-bit Windows
Download	.exe	64-bit x64	7-Zip for 64-bit Windows x64 (Intel 64 or AMD64)
Download	.7z	x86 / x64	7-Zip Extra: standalone console version, 7z DLL, Plugin for Far Manager
Download	.7z	Any	7-Zip Source code
Download	.7z	Any / x86 / x64	LZMA SDK: (C, C++, C#, Java)
Download	.msi	32-bit x86	(alternative MSI installer) 7-Zip for 32-bit Windows
Download	.msi	64-bit x64	(alternative MSI installer) 7-Zip for 64-bit Windows x64 (Intel 64 or AMD64)

Once you unzip the file, open Kali-Linux-2022.4-vmware-amd64.vmx (you may have a newer version with a different file name) from VMWare by clicking "Open a Virtual Machine." Now boot (play) your Kali Linux guest system. If VMware prompts you about whether you "moved" or "copied" this virtual machine, select "I copied it." If it doesn't prompt you, that's okay.



There is one account created for you for this virtual machine

Default username: kali

Default password: kali

4. **Building Ubuntu Virtual Machine from the Google Drive**
(<https://drive.google.com/drive/u/1/folders/1iJ-773pEs3FRhnjbwDFWyxUmUBvRmPKz>)

Download **BookUbuntu-new.7z** and unzip the image. **You must use your UCM email to access the Google drive.** Once you unzip the file, double click on BookUbuntu.vmx and load it into VMWare Workstation 17.

Name ^	Date modified	Type	Size
appListCache	10/26/2012 10:11 ...	File folder	
caches	3/25/2014 9:11 PM	File folder	
screenshotsCache	1/26/2013 6:03 PM	File folder	
BookUbuntu.nvram	3/25/2014 9:11 PM	VMware Virtual Mac...	9 KB
BookUbuntu.plist	3/25/2014 9:11 PM	PLIST File	2 KB
BookUbuntu.vmsd	3/25/2014 9:11 PM	VMware snapshot ...	1 KB
BookUbuntu.vmx	3/25/2014 9:11 PM	VMware virtual mac...	4 KB
BookUbuntu.vmem	3/25/2014 8:53 PM	VMware Team Mem...	4 KB
BookUbuntu.vmsx	3/25/2014 9:11 PM	VMEM File	1,048,576 ...
BookUbuntu.vms	3/25/2014 9:11 PM	VMware suspended ...	1,201 KB
quicklook-cache.png	1/2/2013 5:07 PM	PNG image	801 KB
startMenu.plist	3/25/2014 9:11 PM	PLIST File	971 KB
Virtual Disk.vmdk	3/25/2014 8:53 PM	VMware virtual disk ...	1 KB
Virtual Disk-s001.vmdk	3/25/2014 9:11 PM	VMware virtual disk ...	16,576 KB
Virtual Disk-s002.vmdk	3/25/2014 9:11 PM	VMware virtual disk ...	878,592 KB
Virtual Disk-s003.vmdk	3/25/2014 9:11 PM	VMware virtual disk ...	781,376 KB
Virtual Disk-s004.vmdk	3/25/2014 9:11 PM	VMware virtual disk ...	1,156,288 ...
Virtual Disk-s005.vmdk	3/25/2014 9:11 PM	VMware virtual disk ...	406,016 KB
Virtual Disk-s006.vmdk	3/25/2014 9:11 PM	VMware virtual disk ...	19,392 KB
Virtual Disk-s007.vmdk	3/25/2014 9:11 PM	VMware virtual disk ...	145,984 KB
Virtual Disk-s008.vmdk	3/25/2014 9:11 PM	VMware virtual disk ...	561,088 KB
Virtual Disk-s009.vmdk	3/25/2014 9:11 PM	VMware virtual disk ...	175,936 KB
Virtual Disk-s010.vmdk	3/25/2014 9:11 PM	VMware virtual disk ...	42,432 KB
Virtual Disk-s011.vmdk	3/25/2014 9:11 PM	VMware virtual disk ...	64 KB
vmware.log	3/25/2014 9:11 PM	Text Document	231 KB

Now boot your Ubuntu Linux guest system. If VMWare prompts you about whether you moved or copied this virtual machine, select **I copied it.** If it doesn't prompt you, that's ok.

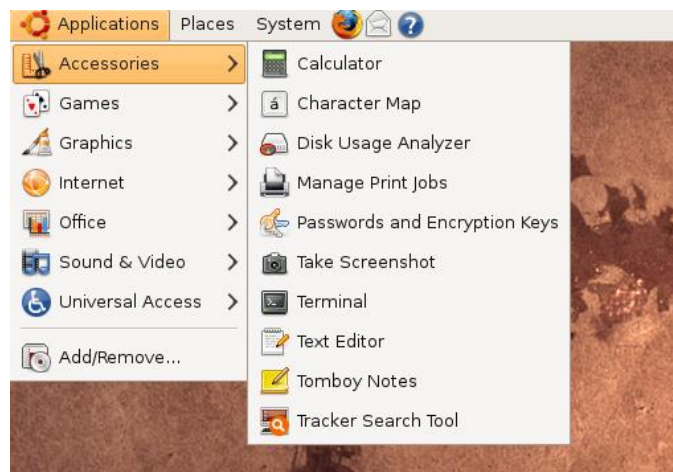
There is one account created for you for this virtual machine

Username: georgia

Password: password

A few preparations need to be done before we can use the Ubuntu virtual machine.

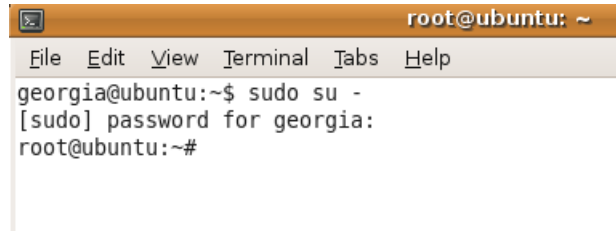
First, let's bring up a terminal at Ubuntu machine by clicking Applications → Accessories → Terminal



Let's su into root by typing

\$ sudo su -

Enter georgia's password, Now you have the root #

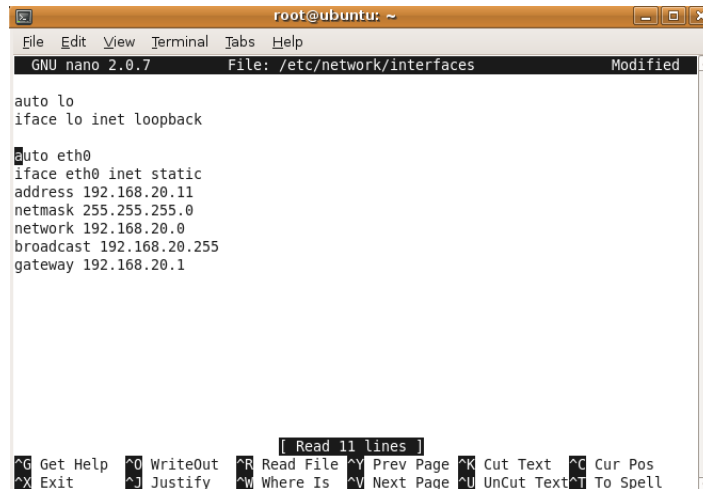


```
root@ubuntu: ~
File Edit View Terminal Tabs Help
georgia@ubuntu:~$ sudo su -
[sudo] password for georgia:
root@ubuntu:~#
```

Next, we will configure the network interface for the Ubuntu machine. At the command line, type

nano /etc/network/interfaces

Please delete all the lines starting from auto eth0, all the way to gateway 192.168.20.1



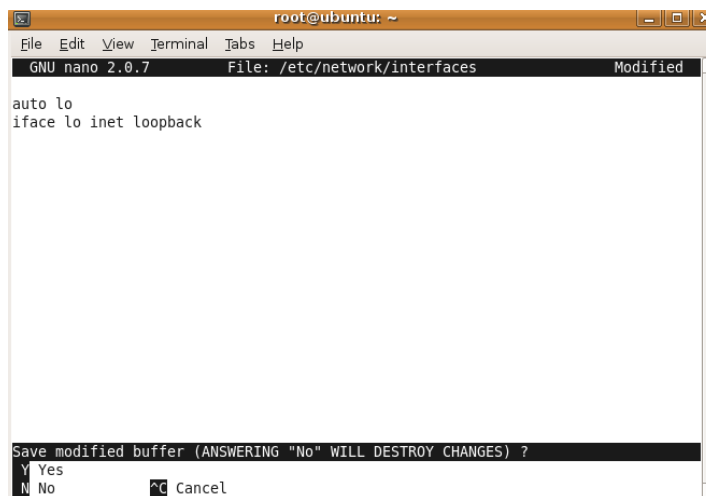
```
root@ubuntu: ~
File Edit View Terminal Tabs Help
GNU nano 2.0.7 File: /etc/network/interfaces Modified

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.20.11
netmask 255.255.255.0
network 192.168.20.0
broadcast 192.168.20.255
gateway 192.168.20.1

[ Read 11 lines ]
^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^N Next Page ^U UnCut Text ^T To Spell
```

Once you finish deleting all those lines, press CTRL-X. The system will ask you whether you want to save the modified buffer, hit y

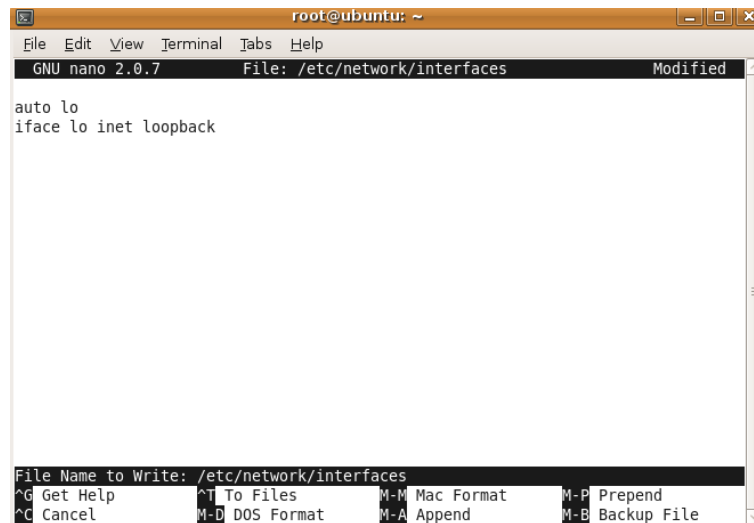


```
root@ubuntu: ~
File Edit View Terminal Tabs Help
GNU nano 2.0.7 File: /etc/network/interfaces Modified

auto lo
iface lo inet loopback

Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
Y Yes
N No ^C Cancel
```

Hit enter in the next screen to finish the save and you will be brought to the original terminal.

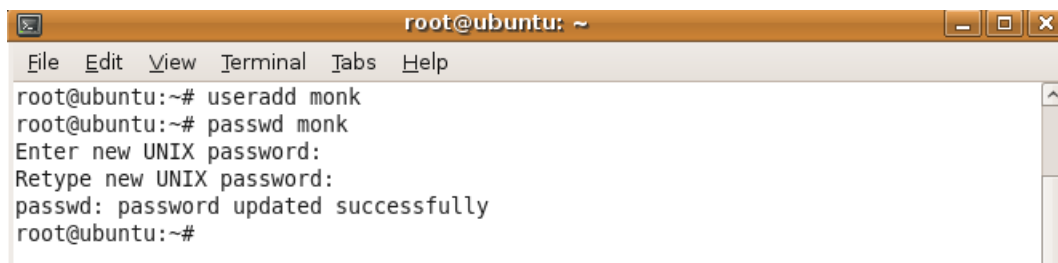


Next we will add another account monk. At the command line, type

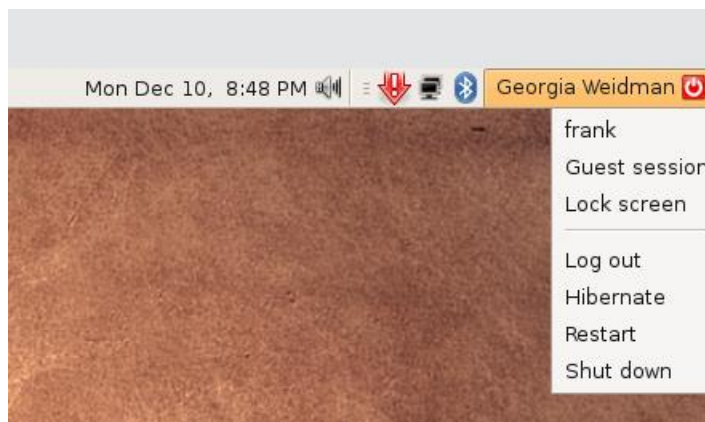
useradd monk

Set the password as **master1** by typing

passwd monk



After that, restart the Ubuntu machine and you are ready to use the virtual machine



5. **Download Metasploitable 2 Linux Virtual Machine from the Google Drive**
(<https://drive.google.com/drive/u/1/folders/1iJ-773pEs3FRhnjbwDFWyxUmUBvRmPKz>)

Download **metasploit2-linux.7z** and unzip the image. **You must use your UCM email to access the Google drive.** Once you unzip the file, double click on Metasploitable.vmx and load it into VMWare Workstation 15. Now boot your Metasploitable 2 Linux guest system. If VMware prompts you about whether you moved or copied this virtual machine, select I copied it. If it doesn't prompt you, that's ok.

Below is the login credential for the virtual machine

Login id: msfadmin

Password: msfadmin

6. Download Windows 7 Virtual Machine from the Google Drive
(<https://drive.google.com/drive/u/1/folders/1iJ-773pEs3FRhnbwDFWyxUmUBvRmPKz>)

Download **Windows 7.7z** and unzip the image. Once you unzip the file, double click on Windows 7.vmx and load it into VMWare Workstation 15. Now boot your Windows 7 guest system. If VMware prompts you about whether you moved or copied this virtual machine, select I copied it. If it doesn't prompt you, that's ok.

There are two administrators accounts created for you

georgia: password

frank: knarf

One non-administrator account

monk: master1

There are many Windows tools stored in C:\Tools folder. Please do not delete that folder.

7. Download Windows XP from the Google Drive (there is no need to complete this step in Lab 1) (<https://drive.google.com/drive/u/1/folders/1iJ-773pEs3FRhnbwDFWyxUmUBvRmPKz>)

Download and unzip the image and load it into VMWare Workstation 15. Once you unzip the file, double click on Windows XP Professional.vmx and load it into VMWare Workstation 15. Now boot your Windows XP guest system. If VMware prompts you about whether you moved or copied this virtual machine, select I copied it. If it doesn't prompt you, that's ok.

There are two administrators accounts created for you

georgia: password

secret: Password123

One non-administrator account

monk: master1

8. Download Windows 10 Virtual Machine from the Google Drive (<https://drive.google.com/drive/u/1/folders/1iJ-773pEs3FRhnbwDFWyxUmUBvRmPKz>)

Download **Windows 10x64.7z** and unzip the image. **You must use your UCM email to access the Google drive.** Once you unzip the file, double click on Windows 10x64.vmx and load it into VMWare Workstation 15. Now boot your Windows 10 guest system. If VMware prompts you about whether you "moved" or "copied" this virtual machine, select "I copied it." If it doesn't prompt you, that's ok.

There is one administrator's account created for you

georgia: password123

Two non-administrator accounts

frank: knarf

monk: master1

9. Install ssh, gedit and open-vm-tools on Kali Linux

```
$ sudo apt-get update
```

```
$ sudo apt-get install ssh
```

```
$ sudo systemctl enable ssh
```

```
$ sudo apt-get install gedit
```

```
$ sudo apt-get install open-vm-tools-desktop
```

10. Install docker-ce on Kali

Visiting the following link and follow the instruction to install docker-ce. Please make sure to install docker-ce not docker.io.

<https://www.kali.org/docs/containers/installing-docker-on-kali/>

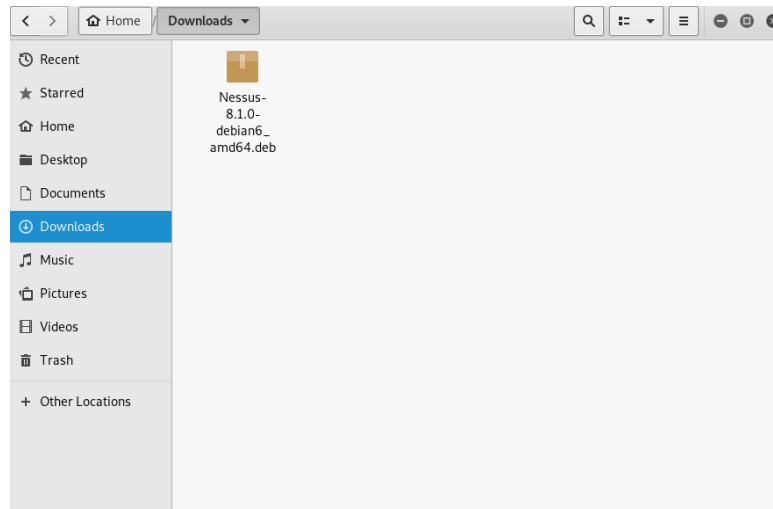
11. Install Nessus Essentials on Kali Linux

In Kali Linux, open Firefox and surf to the following site to register a free account to get your activation code. This is a one-time code. If you uninstall and then reinstall you will need to register the scanner again and receive another activation code.

<https://www.tenable.com/products/nessus/nessus-essentials>

Download Nessus-8.15.0-debian6_amd64.deb (Debian 9, 10 / Kali Linux 1, 2017.3, 2018, 2019, 2020 AMD64) or whatever the newest version (make sure to choose the 64-bit version)

The file should be automatically downloaded to the Downloads folder



Bring up a terminal and type the following commands

\$ cd Downloads

\$ sudo dpkg -i Nessus-8.15.0-debian6_amd64.deb

Please make sure that the Nessus file name used in the above command matches the actual file name you downloaded.

Start Nessusd by typing

\$ sudo service nessusd start

```
kali@kali:~$ cd Downloads/
kali@kali:~/Downloads$ sudo dpkg -i Nessus-8.10.0-debian6_amd64.deb
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 273109 files and directories currently installed.)
Preparing to unpack Nessus-8.10.0-debian6_amd64.deb ...
Unpacking nessus (8.10.0) ...
Setting up nessus (8.10.0) ...
Unpacking Nessus Scanner Core Components...
```

- You can start Nessus Scanner by typing `/etc/init.d/nessusd start`
- Then go to `https://kali:8834/` to configure your scanner

```
Processing triggers for systemd (245.4-3) ...
```

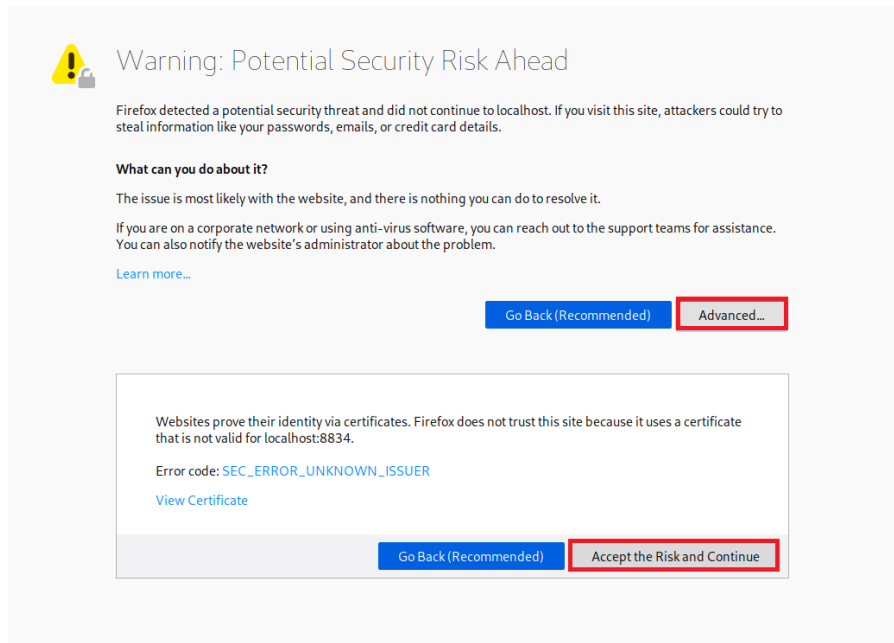
```
kali@kali:~/Downloads$ sudo service nessusd start
```

```
kali@kali:~/Downloads$
```

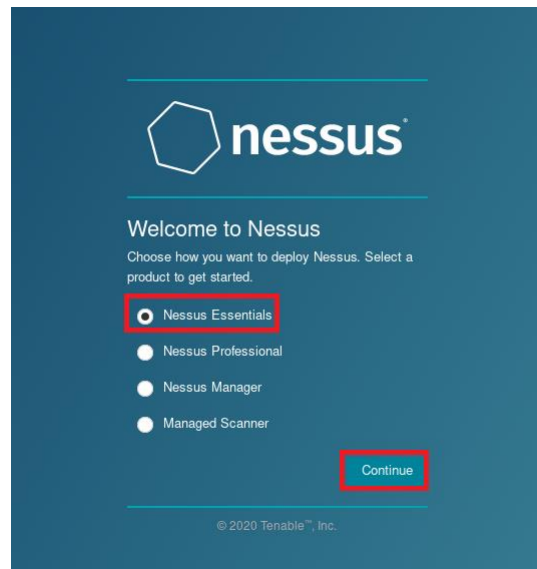
Bring up your Firefox browser in Kali Linux and enter the following url

https://localhost:8834

You will see the following SSL certificate warning

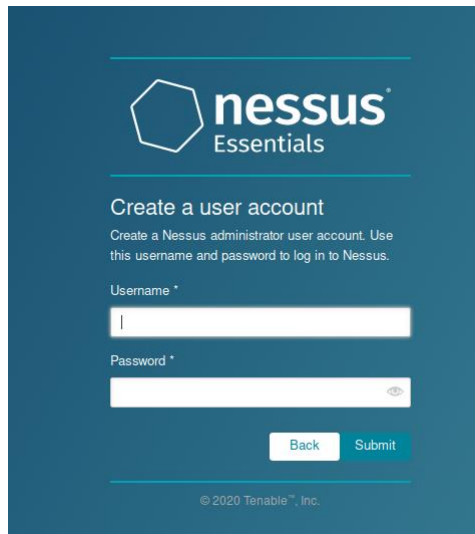


Click **Advanced** button, then click **Accept the Risk and Continue**. On the next screen, leave the default setting (**Nessus Essentials**), then click the **Continue** button (newer version could have different menu).



Click the **Skip** button on the next screen. Enter your activation code in the next screen then click the **Continue** button.

In the next screen, create an account and password. **For username, please use the portion of your UCM email before @ (this information is required for your lab report). Please record your account and password information for future use.**



12. Install PowerShell Empire on Kali Linux

\$ sudo apt install powershell-empire

When installation asks for "Enter server negotiation password", enter for random generation: "o", just hit enter.

13. Install Veil Evasion on Kali Linux

\$ sudo apt -y install veil

\$ sudo /usr/share/veil/config/setup.sh --force --silent

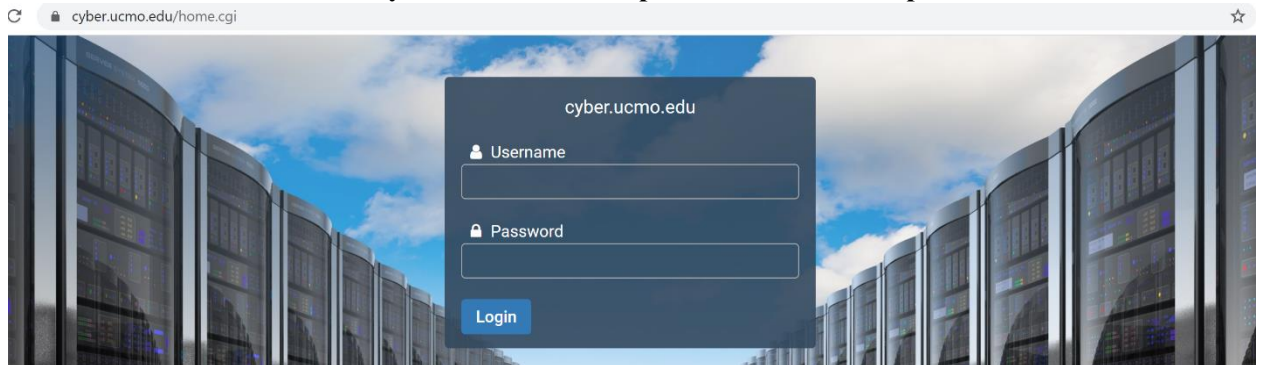
14. Take a Snapshot of VM

Sometime you need to execute some dangerous commands which may corrupt your virtual machine. It is highly recommended that you take a snapshot of your VM before performing those dangerous operations. First select your VM from the left panel of your VMWare workstation. Then click the take a snapshot of this virtual machine button (highlighted in the red square of the following picture).



15. Tour cyber.ucmo.edu (you'll use this system on midterm & final exam)

Type cyber.ucmo.edu as the url and login in using the username and password distributed to you in the class. Please do NOT use your virtual machine to access cyber.ucmo.edu, use your host machine instead. **Please record your username and password in a secure place for future use.**



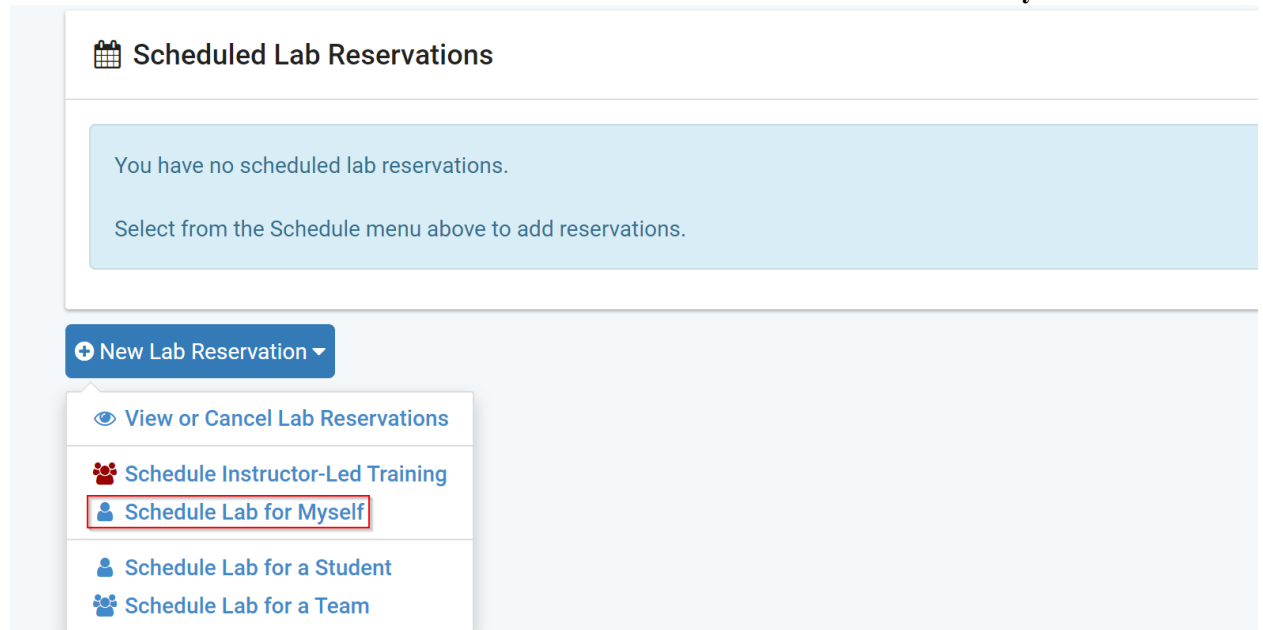
cyber.ucmo.edu

Username

Password

Login

Once you successfully login CyberCentral, you will see a lab reservation page to ask you to reserve a lab. Click the **New Lab Reservation** button and select **Schedule Lab for Myself**.



Scheduled Lab Reservations

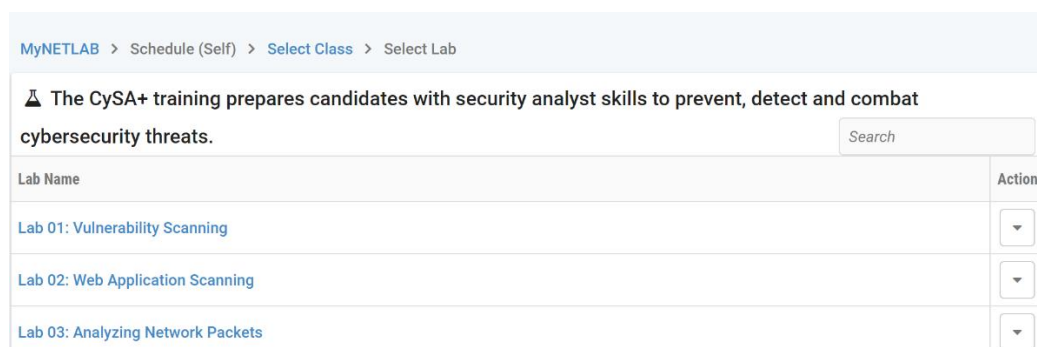
You have no scheduled lab reservations.

Select from the Schedule menu above to add reservations.

New Lab Reservation

- View or Cancel Lab Reservations
- Schedule Instructor-Led Training
- Schedule Lab for Myself**
- Schedule Lab for a Student
- Schedule Lab for a Team

Now, choose a class you'd like to conduct the lab. For our class, we will use **CySA+** lab settings. Let's choose CySA+ by clicking the course name. On the next page, click a lab to schedule your reservation (any lab is fine. We just use its network topology)




MyNETLAB > Schedule (Self) > Select Class > Select Lab

The CySA+ training prepares candidates with security analyst skills to prevent, detect and combat cybersecurity threats.


Search

Lab Name	Action
Lab 01: Vulnerability Scanning	▼
Lab 02: Web Application Scanning	▼
Lab 03: Analyzing Network Packets	▼

Click a Pod (the column with CySA+) to reserve your lab time.

	NDG_Security_CySA+_Pod_01			
19:00				
20:00				
21:00				
22:00				
23:00				

You can modify the **End Time** field as needed so that you have enough time to conduct your lab. After that, click the **Submit** button.

 Add Reservation

Pod

NDG_Security_CySA+_Pod_01

Reservation Type

Instructor Private Reservation

Reserve For

Xiaodong Yue

Lab Exercise

Lab 01: Vulnerability Scanning


Time Zone

Central Time (US & Canada)

Start Time

2021-08-11 20:50

End Time

2021-08-11 21:30

Length of Reservation

29 mins.

Submit

Previous

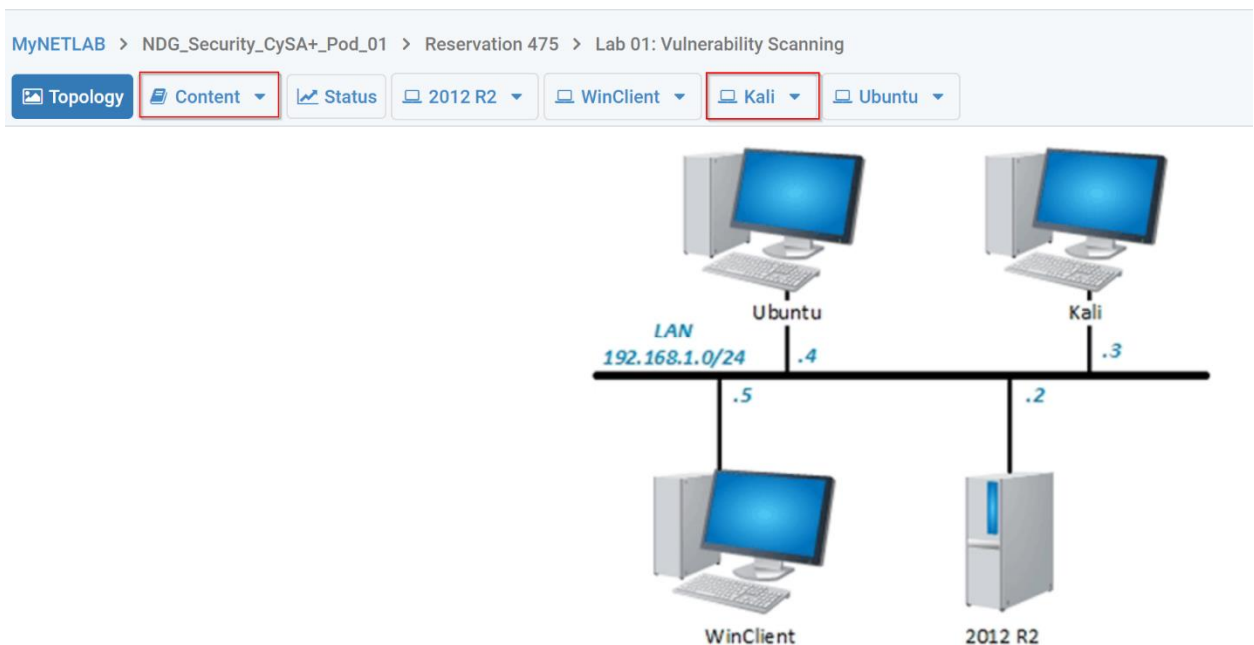
Cancel

On the next pop-up window, click the **OK** button. In the next window, click **Enter Lab** button to start your lab.

Lab Reservations			
Search			
ID	Date/Time	Description	Pod
475	<div> <div>2021-08-11 20:52</div> <div>2021-08-11 21:30</div> <div>26 mins.</div> </div> <div>Enter Lab</div>	Class: CCCCC CySA+ Lab: Lab 01: Vulnerability Scanning Type: Instructor User: Xiaodong Yue	NDG_Security_CySA+_Pod_01

Showing 1 to 1 of 1 items

The networking diagram for the lab setting will be displayed in the next window. You can click the icon of a particular machine in the diagram to access that machine. To obtain the login credentials, click the **Content** button at the top of the screen (go to page 5, Lab Settings).



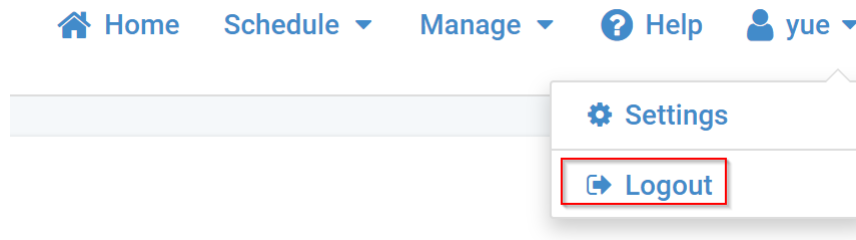
If you need to request more time or end the reservation, click the **Reservation** menu at the top right corner of the Window. In our case, please select **End Reservation Now**. Click the **Yes** button on the next window to confirm. After that click the **OK** button.

[Home](#)
[Reservation](#)
[yue](#)

[Request More Time](#)
[Change Exercise](#)
[End Reservation Now](#)

Time Remaining
 0 20
 hrs. min.

Click your login name at the top right corner of the window then select the **Logout** button to logout CyberCentral.

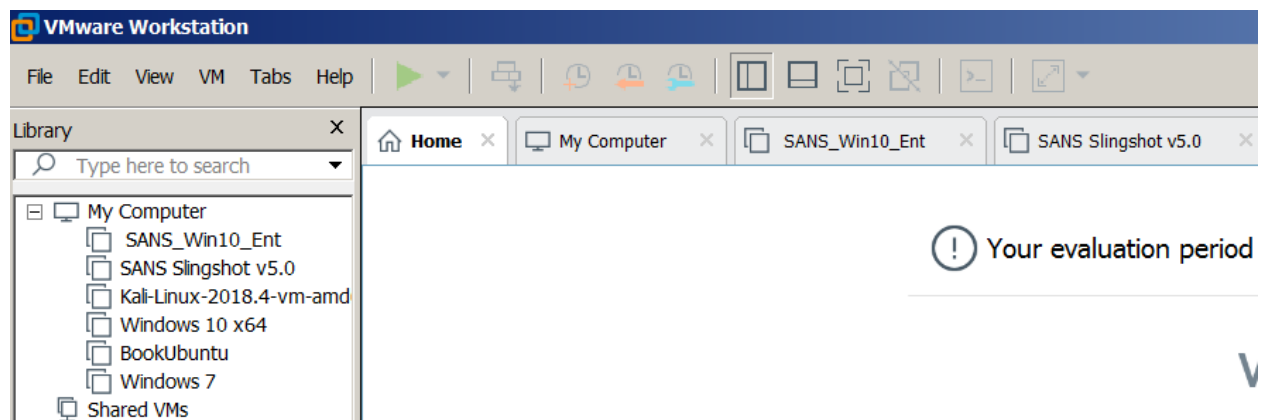


Lab Report

- please include your name and 700# at the beginning of your report
- please upload your report to the Blackboard by the due date
- only word or pdf format is acceptable

In this report, you need to provide 2 screenshots.

1. A screenshot showing all virtual machines (Windows 7, 10, Kali and Ubuntu) loaded in your virtualization product. See sample screenshot below.



2. The screenshot of the first screen after you login Nessus. Make sure to include your account name (upper right corner) in the screenshot. See sample screenshot below.

