

## Building Your Own Cybersecurity Lab<sup>1</sup>

**Due Wednesday, March 14<sup>th</sup>, 2022 @ 11:59pm**  
(3% of the total course grade)

### 1. Objective

In this lab, you will learn how to build your own Cyber Security Lab by using virtualization technology.

This lab will be graded, but **you will only need to submit your answers to six questions (Q4, Q5, Q6, Q7, Q9, and Q10) to receive credit**. It has to be completed INDIVIUALLY, but you may want to discuss the lab content with your fellow students.

### 2. Environment Setup

#### 1) Install VirtualBox:

Note that you can skip this part if you already have VirtualBox installed.

- Download and Install VirtualBox from VirtualBox.org. We recommend Version 6.0.X (please stay away from the newer versions, as they may have some issues with the VM used).

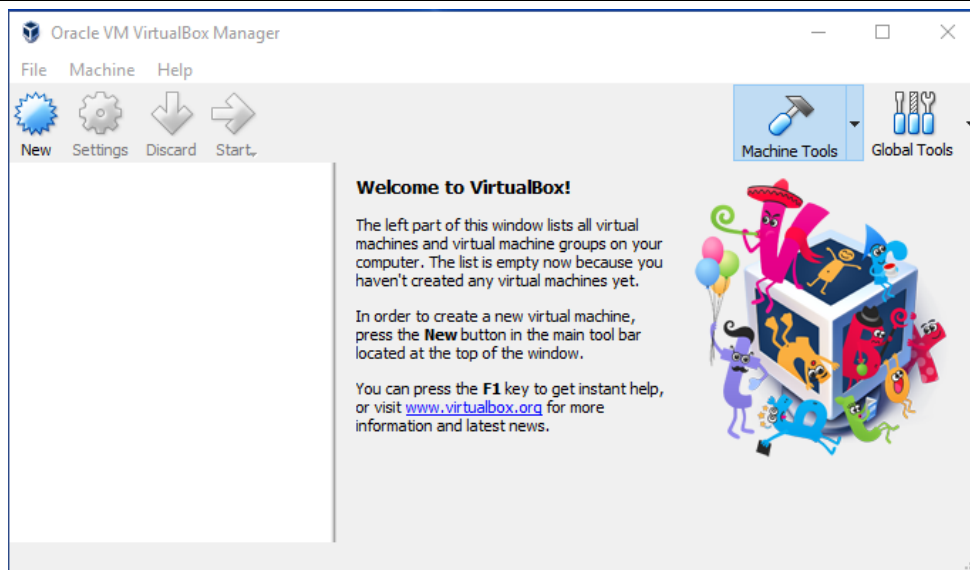


---

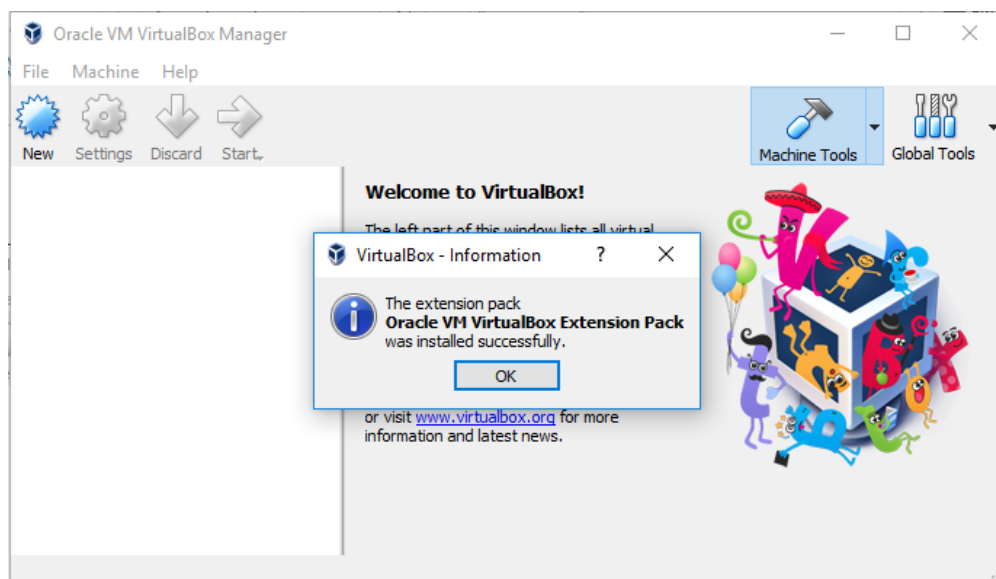
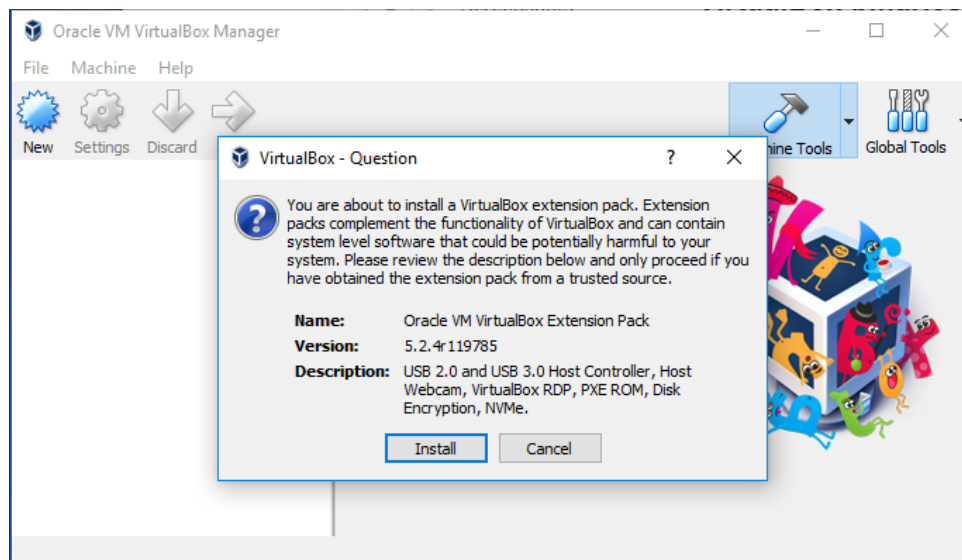
<sup>1</sup> Copyright © 2020 Xiaodong Lin, University of Guelph, Canada.

This lab may not be redistributed or used without written permission.

# Network and Information Security Lab #1



- Download and Install VirtualBox Extension Pack from VirtualBox.org



# Network and Information Security Lab #1

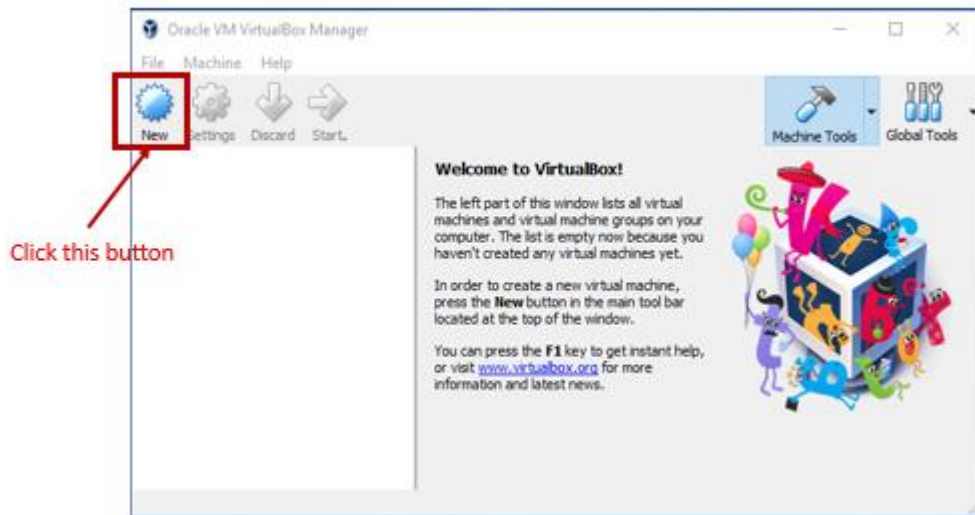


You will need to install the extension pack with the same version as your installed version of VirtualBox.

## 2) Lab Configuration and VirtualBox:

- Download a pre-built SEED Ubuntu16.04 VM image by going to [https://seedsecuritylabs.org/lab\\_env.html](https://seedsecuritylabs.org/lab_env.html)  
Note that the downloaded VM image is a compressed (zipped) file. You will need to unzip it.
- Import pre-built Ubuntu16.04 VM image <sup>[1]</sup>

Step 1: Create a New VM in VirtualBox



Then, please refer to the following document<sup>[2]</sup> for the detailed installation and configuration

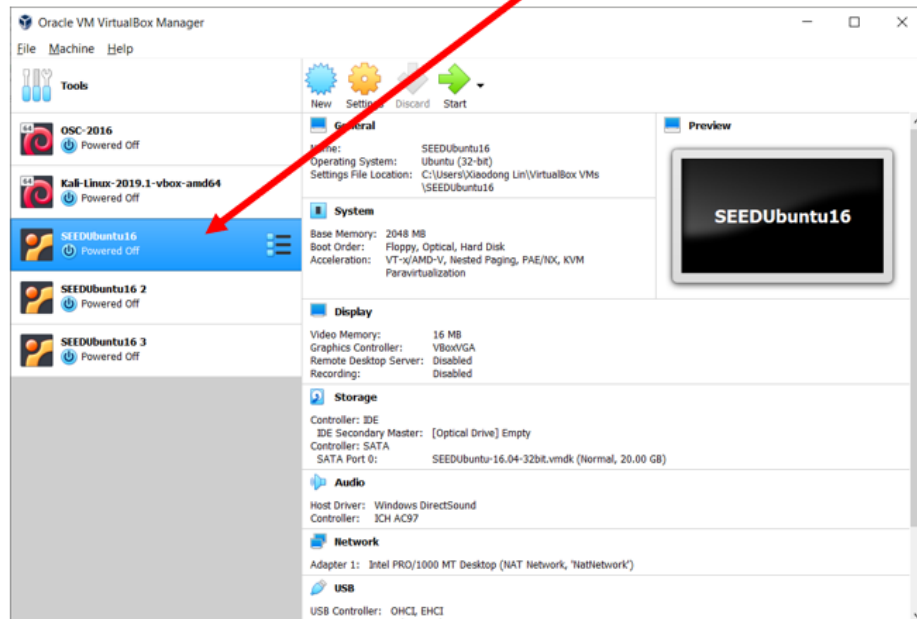
[https://seedsecuritylabs.org/Labs\\_16.04/Documents/SEEDVM\\_VirtualBoxManual.pdf](https://seedsecuritylabs.org/Labs_16.04/Documents/SEEDVM_VirtualBoxManual.pdf)

For your convenience, this important document has been provided on the CourseLink course website.

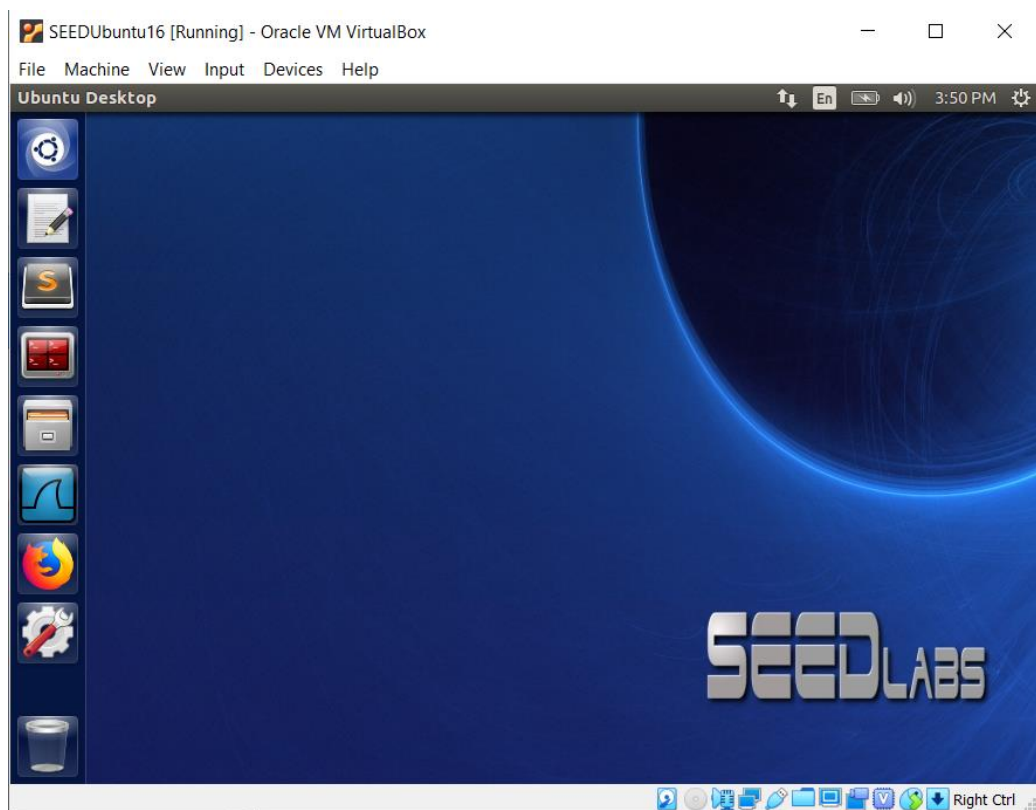
If the VM has been created successfully, you should see the following

# Network and Information Security Lab #1

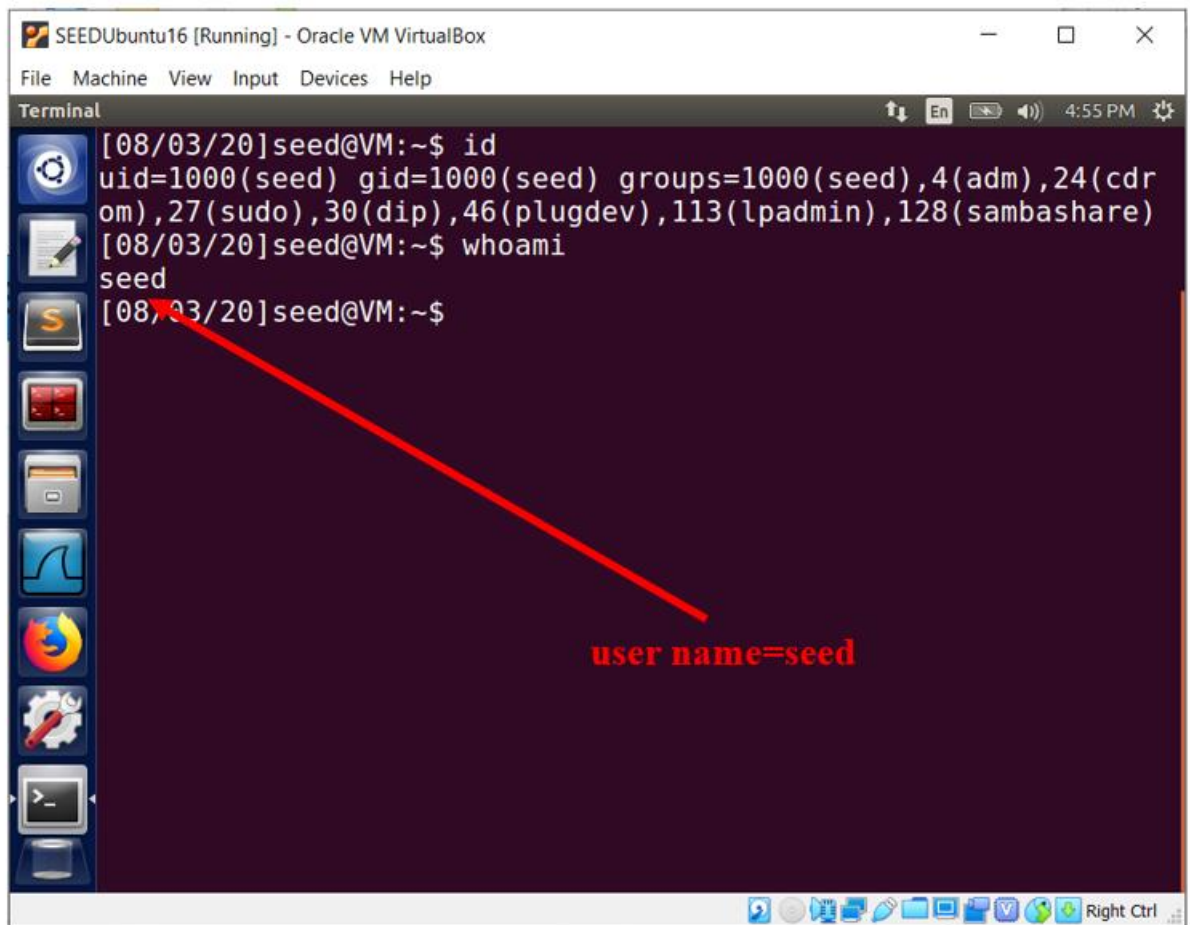
**successfully created**



Step 2: After you successfully created your VM, you can now start your VM. If your installation goes smoothly, you should see the following as you are automatically logged into the VM as the user “seed”.



# Network and Information Security Lab #1



The screenshot shows a terminal window titled "SEEDUbuntu16 [Running] - Oracle VM VirtualBox". The terminal output is as follows:

```
[08/03/20]seed@VM:~$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdr
om),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
[08/03/20]seed@VM:~$ whoami
seed
[08/03/20]seed@VM:~$
```

A red arrow points from the text "user name=seed" to the "seed" output of the `whoami` command.

The pre-built Ubuntu 12.04 VM comes with two accounts:

username: seed

password: dees

This is a regular user account that you can use for most of your Lab assignments.

username: root

password: seedubuntu

**You normally don't need to log into the root account.** This is an administrative account that has full privileges (generally accessed via `sudo`). You can use this to install software, perform updates, enable and disable services, even hack at the kernel! You need to be very careful while logged in as the Root User because you can destroy your VM if you are not careful!

**Note that** by default Ubuntu does not allow root to login directly from the login window. You have to login as a normal user, and then use the command "`su`" to login to the root account. For example, type

**su -**

# Network and Information Security Lab #1

- VirtualBox Network Configuration <sup>[2]</sup>

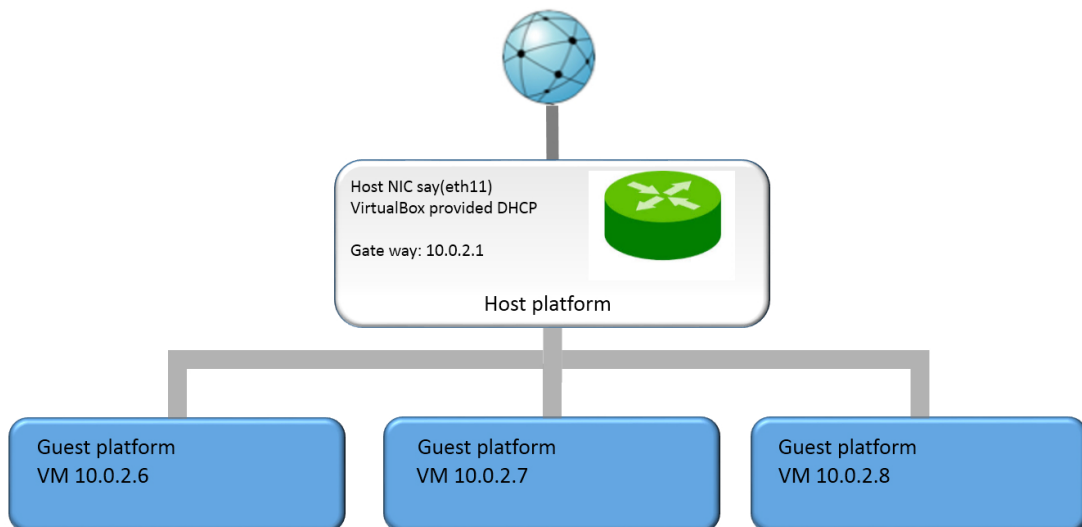


Figure 1. Required Network Environment Settings <sup>[2]</sup>

VirtualBox networking supports many different configurations, including NAT, which is the default provided with DVDK, Host-Only Networking, Bridged Networking, and “NAT Network”, which enable VMs communication within same local network as well as the communication to the internet. In many of our labs, we need to run multiple guest VMs, shown in Figure 1, and these VMs should be able to (1) reach out to the Internet, and (2) communicate with each other. In order to make it happen, we will need to setup the Virtualbox by using “NAT Network” adapter, shown in Fig. 2. Also, we need to configure the VM, allowing your host and guest VMs to share the files.

Please refer to the SEED VM User Manual <sup>[2]</sup> for the detailed installation and configuration.

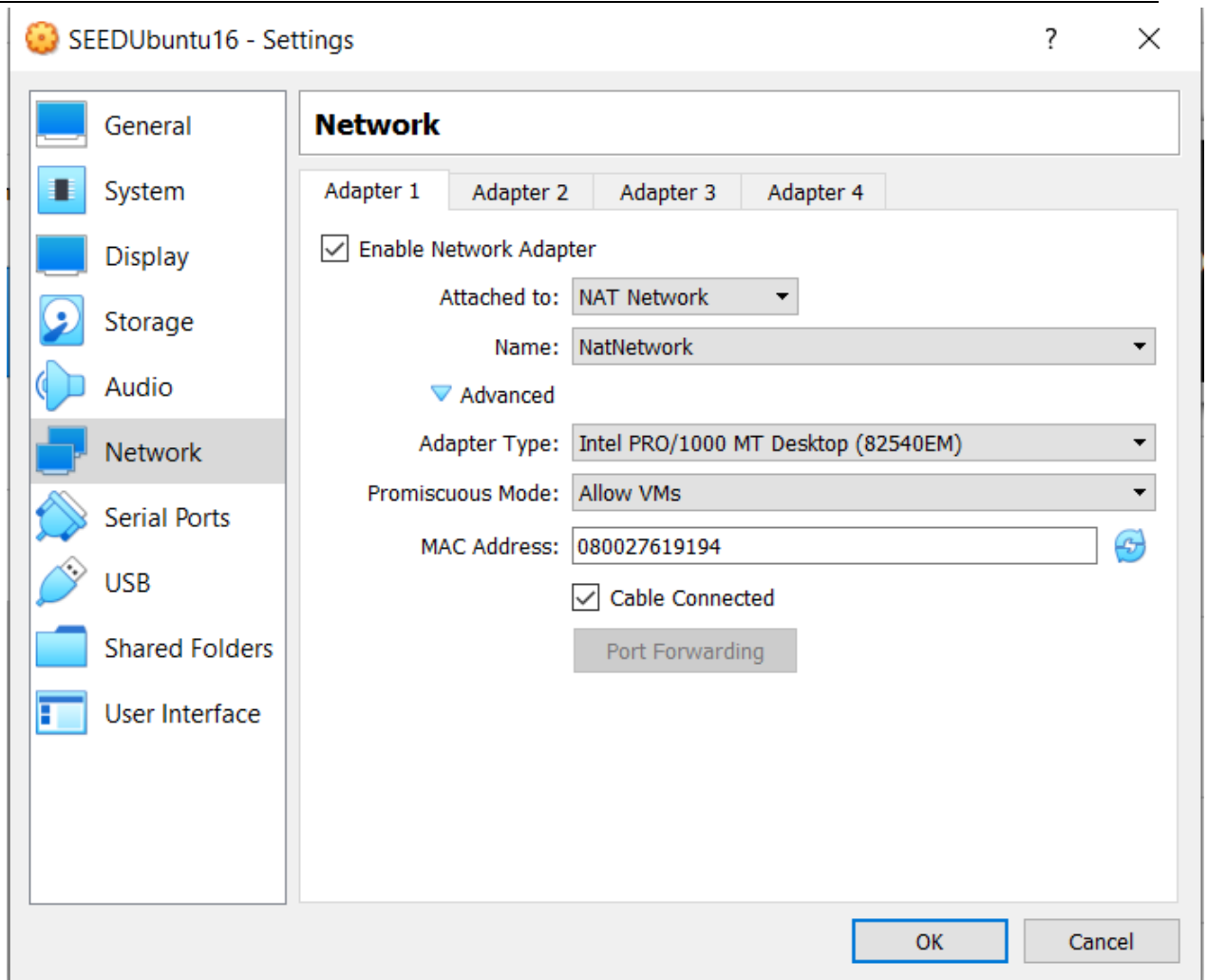


Figure 2. Required Network Environment Settings <sup>[2]</sup>

**Note that you will need to create a new NAT Networks (NatNetwork) adaptor in your VirtualBox if one does not exist. Also, make sure you shut down the VMs that when you do network configuration in VirtualBox.**

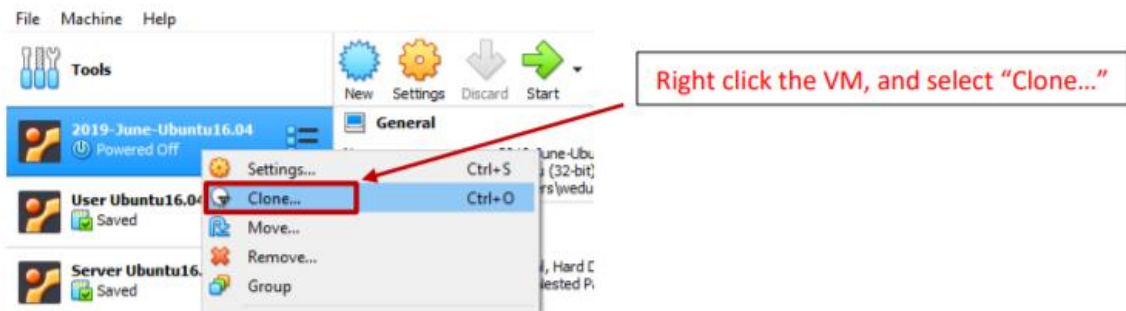
- Setup multiple guest VMs

Many labs in this class require loading multiple VMs into VirtualBox and running at the same time. You can create multiple VirtualBox VMs from the VM image downloaded.

There are many ways to load multiple VMs into VirtualBox but the simplest way is to use the “Clone” mechanism in VirtualBox after you successfully created the first one



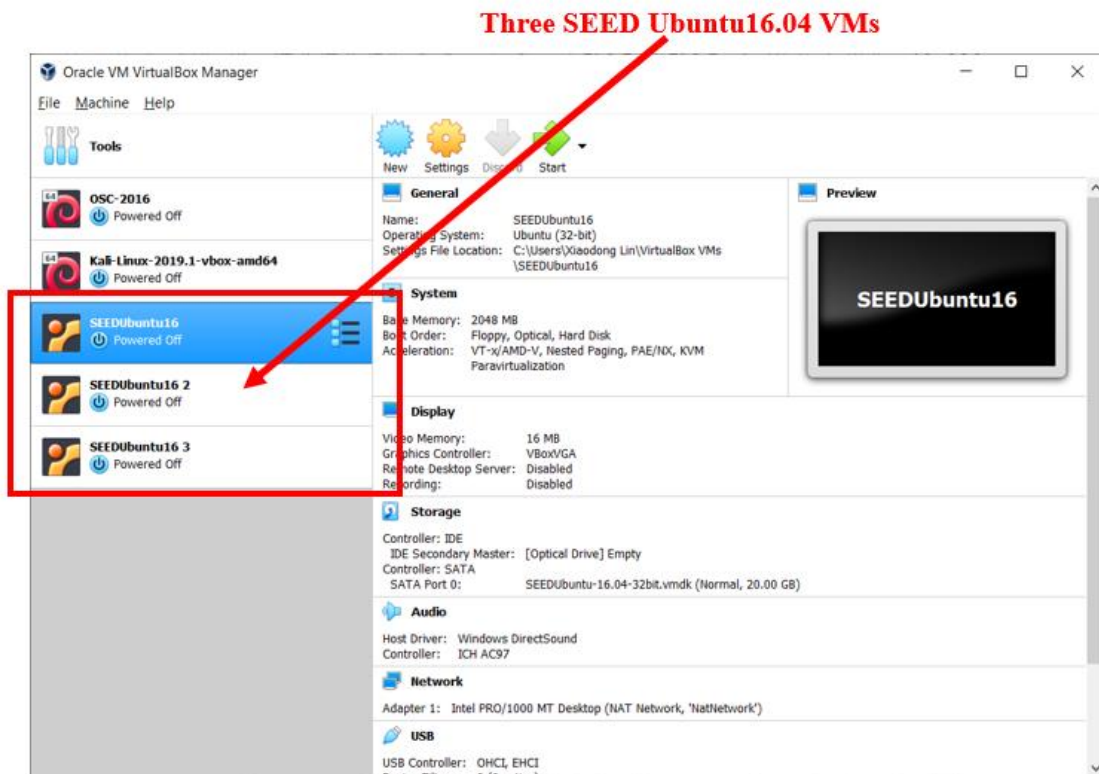
# Network and Information Security Lab #1



**IMPORTANT:** make sure that the VM is fully shutdown (not in a “Saved” state), or there will be all sorts of problems.

Afterwards, we have two VMs. You have to make sure that two VMs use different VM names.

Afterwards, you can create the second new VM (or the 3<sup>rd</sup> VM) in VirtualBox by following the steps described above. Repeat the same steps for the third new VMs (or more if you need to).



**Congratulations!** Your Cyber Security Lab is now ready to go.



## 3. Lab Exercises

### 1) Network Administration

**ping** send ICMP ECHO\_REQUEST to network hosts

**ifconfig** Configure a network interface. For example, if no arguments are given, ifconfig displays the status of the currently active interfaces.

#### Exercises:

**Q1:** Start two VMs and List their IP addresses in the space provided below

**Q2:** Use the ping command to verify the network connectivity between two VMs and write down the command(s) you issued in the space provided.

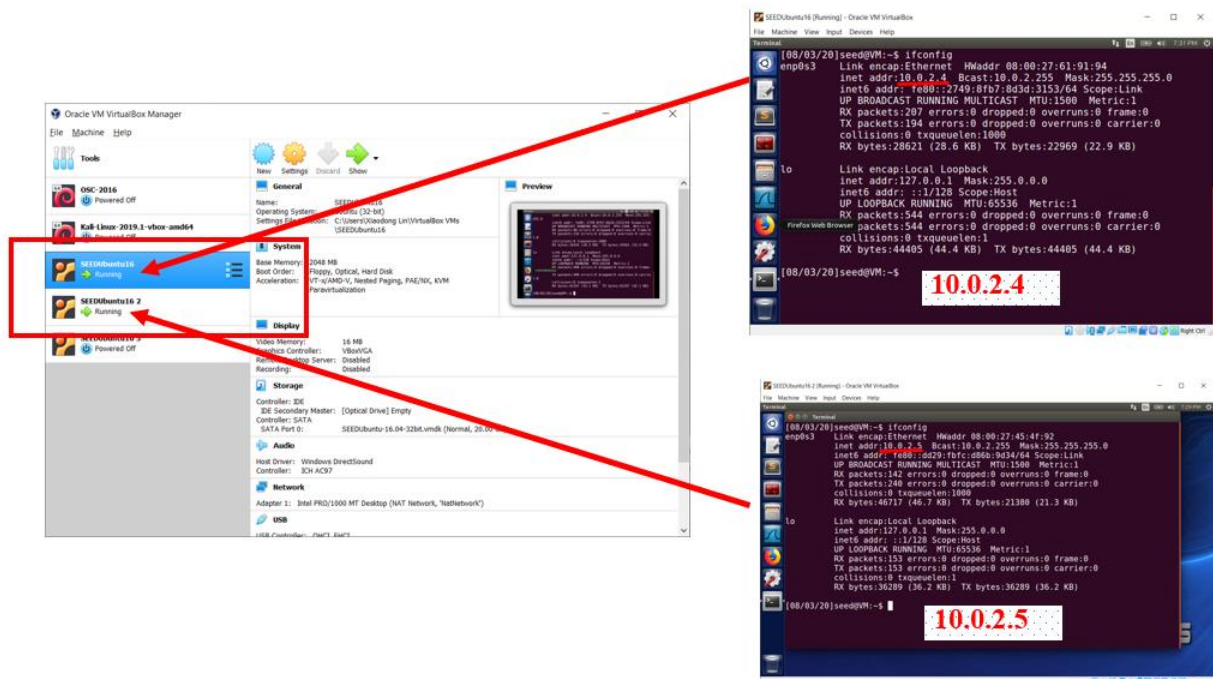


Figure 3. Two running VMs. Note that the IP addresses of your VMs may vary

### 2) Telnet to one VM from another VM

Telnet is one of the oldest of the Internet applications, dating back to 1969 on the ARPANET. Its name is actually an acronym that stands for "telecommunications network protocol." It allows remote login using the client-server paradigm. Figure 7 shows a typical Telnet protocol

## Network and Information Security Lab #1

session. Unfortunately, all information exchanged between the Telnet client and server are unencrypted.

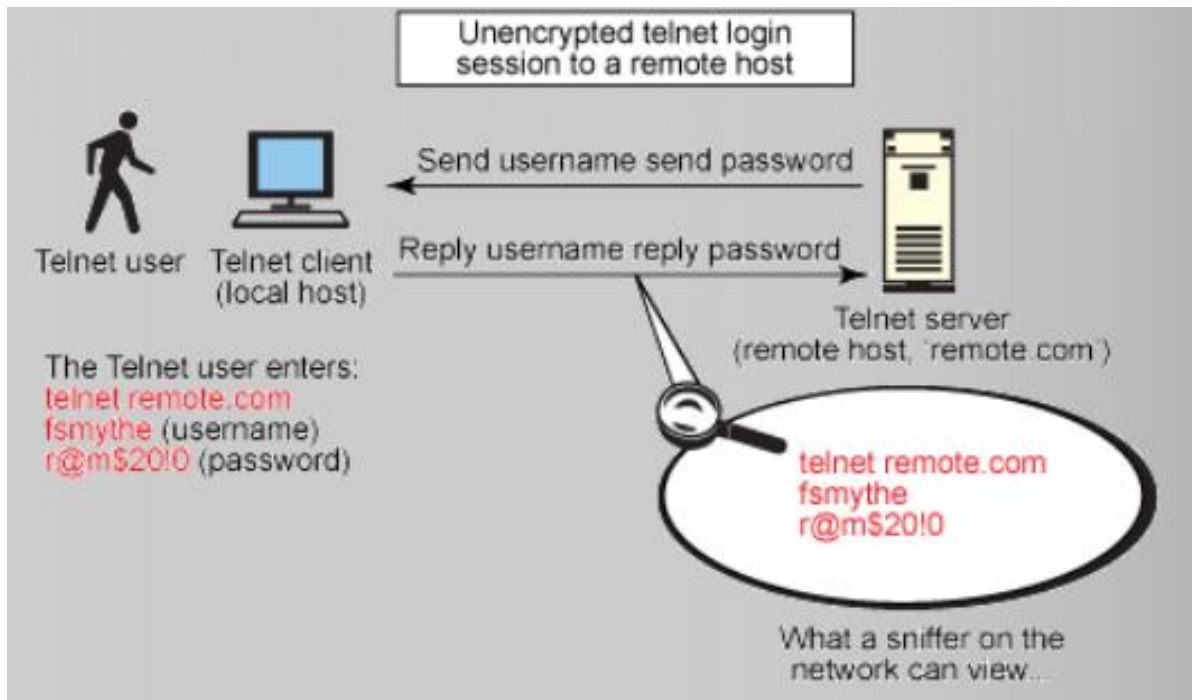


Figure 7. Telnet protocol sessions are unencrypted <sup>[5]</sup>

Note that the `telnetd` server is already installed in the VM provided, and by default, the `telnetd` server will be started when you started your VM. If not, it can be started by running `"service openbsd-inetd start"`. You can check the status of a service if it is running or not by typing the following command

```
#service openbsd-inetd status
```

### Exercise:

**Q3:** Use the `telnet` command to log onto one VM from another VM and write down the command(s) you issued in the space provided.

### Review questions:

**Q4:** The Telnet protocol uses which port? \_\_\_\_\_ (1 mark)

- a) 20
- b) 21
- c) 22
- d) 23

# Network and Information Security Lab #1

**Q5:** The SSH protocol uses which port? \_\_\_\_\_ (1 mark)

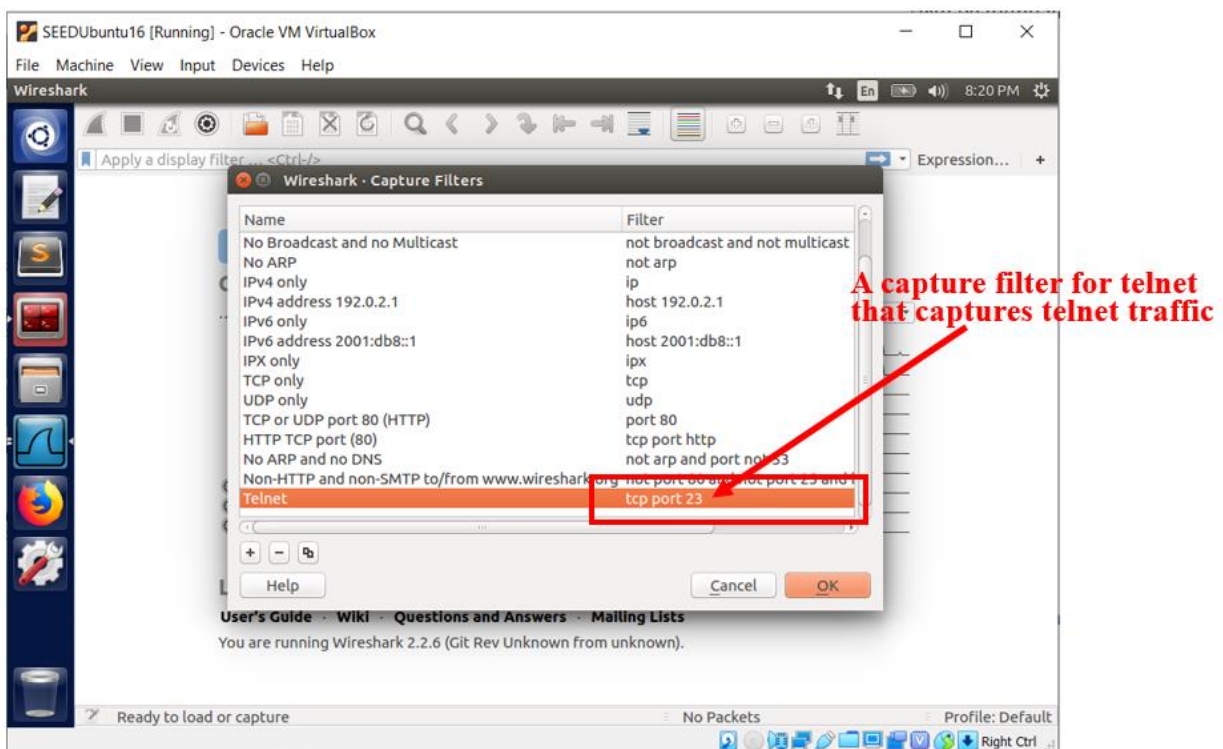
- a) 20
- b) 21
- c) 22
- d) 23

**Q6:** At which layer do Telnet/SSH protocols operate? \_\_\_\_\_ (1 mark)

- a) Application layer
- b) Transport layer
- c) Network layer
- d) Data link Layer

## 3) Capture Telnet password using wireshark

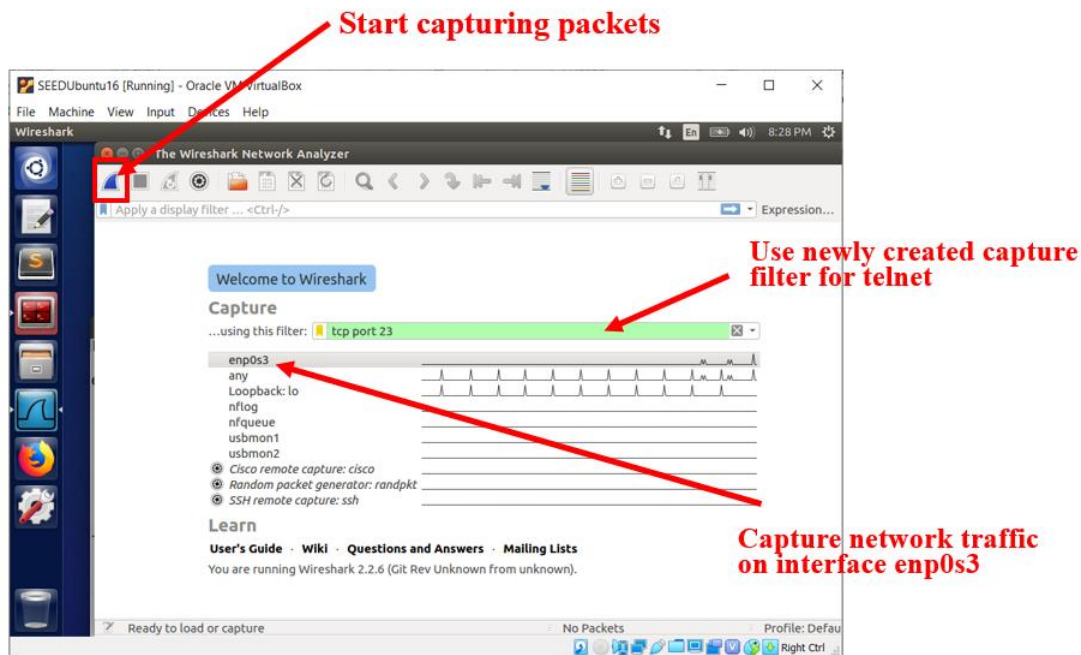
Start Wireshark on one VM and create a capture filter for telnet that captures traffic, as shown below



Afterwards, start capturing packets using the newly created capture filter for telnet. Then, use the telnet command to log onto another VM from this VM.

# Network and Information Security Lab #1

---



**Q7:** Can you sniff telnet traffic and discover the username and password? (Yes/No) (1 mark)

---

## 4) SSH to one VM from another VM

### Exercises:

**Q8:** Use the ssh command to log onto one VM from another VM and write down the command(s) you issued in the space provided.

---

**Q9:** This lab (in part 3) shows how easily a telnet session can be casually viewed by anyone on the network using a network-sniffing application such as Wireshark. In other words, if we use Telnet to gain access to a remote machine, it is not secure. Nowadays, SSH is widely used for remotely accessing another host over the network. Can you sniff SSH traffic and discover the username and password? (Yes/No) (1 mark)

---

**Q10:** If you answer “Yes” to any of Q7 and Q9, please find out that the password is included in **how many TCP packets** (excluding any duplicate or echoed packets). Note that answer the question directly from what you observe in the packet trace you have captured. **Screenshots are mandatory in order to demonstrate how you find out the password. Otherwise, you will receive no credit for the question.** If you answer “No” to both Q7 and Q8, you simply give the answer “N/A” to the question.

(1 mark)

---

### **4. Submission**

You can submit your answers in one pdf file.

## **Reference:**

[1] SEED Ubuntu16.04 VM image.

[https://seedsecuritylabs.org/lab\\_env.html](https://seedsecuritylabs.org/lab_env.html)

[2] Run SEED VM on VirtualBox - User Manual

[https://seedsecuritylabs.org/Labs\\_16.04/Documents/SEEDVM\\_VirtualBoxManual.pdf](https://seedsecuritylabs.org/Labs_16.04/Documents/SEEDVM_VirtualBoxManual.pdf)

[3] SSH security and configuration.

<https://sites.google.com/site/torontoaix/aix-commands/ssh-security>