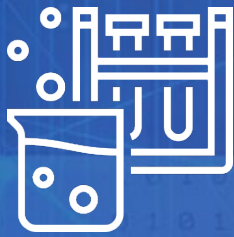


# Project Assignment



Copyright © 1996-2020 HackerU Ltd.  
All Rights Reserved.

Cybersecurity Professional Program  
Network Security

## Final Project

**NS-10-LS1**

**Secure Your Network**

## Project Objective

Analyze each situation and configure services and solutions to address each one of the needs that are raised.

Also, solve some eventual problems that may arise during the process.

## Project Mission

You will be practicing most of the contents presented during this course, and elaborate and implement some security policies to solve some very real problems companies face in today's world.

## Requirements

- Knowledge of firewalls, IPS, and network monitoring.
- Knowledge of VPNs.
- Knowledge of computer networking concepts, and some Linux and Windows skills.

## Resources

You will receive a completely configured scenario. No need to use any of the VMs you have in your lab.

The scenario should be ready for work right at the beginning of the session.

Do not change the configuration of the VMs, or you may experience connectivity issues.

- Environment & Tools
  - VirtualBox
    - Kali Linux VM
    - Debian VM
    - Ubuntu VM with Apache Webserver
    - RedHat VM with pfSense and Suricata
    - CentOS VM with Nagios
  - Extra Lab Files
    - VM1\_PFSense.ova
    - VM2\_NagiosXl.ova
    - VM3\_Kali.ova

- VM4\_Ubuntu.ova
- VM5\_Debian.ova

## Background

Read the following letter:

*“Welcome to GoodCorp’s Family! Congratulations on your new job!! This is really good news!*

*Let’s talk about your new work here: You were hired as a Security Analyst for GoodCorp, Inc., and we are a company that has serious security challenges for our network.*

*For example, users are still able to access some resources they shouldn’t have access to, and some inbound traffic that should be blocked is still allowed. We also lack secure access to remote employees, and need to heighten their understanding of what is going on.*

*A few minutes ago, your new manager assigned you to a position in the SOC. This means that from now on, all security-related requests will be sent to you.*

*Your mission (if you choose to accept it) is to manage the service and security tickets that are raised. You must organize the tasks, configure services, customize rules, or perform any other action or security measure required to resolve detected issues.*

*Remember: As a Security Analyst, you should make use of Best Practices, and be prepared to provide evidence of your work and solutions.*

*Good luck!”*

## Instructions

Please read and become familiar with all the following instructions.

- 1 Read all requests carefully before you start. The instructor can read the task for everyone in class, just to make sure everything is understood. As a wise saying goes: “Sometimes, the answer for a question is in the question itself...”.
- 2 You will need to import the VMs that will be used in this activity. See the next section for specific instructions. The VMs are already installed and configured with the proper connectivity and features you will need to begin the project.
  - a. Important: Don't change anything in the VMs, unless told to do so.  
Changing something may impact the time needed to finish the project.
  - b. Simply follow the steps and power the VMs on. Follow the sequence to import and start each VM.
  - c. After the environment is installed, don't browse the VMs. Everything will be explained later. Proceed with the tests to validate the installation, and wait for instructions.
- 3 The project has three phases:
  - a. The first phase is your preparation time. You will download and start the VMs. You also need to validate the environment and make sure everything is ready to start the tasks. Since this is not part of a typical ‘day-in-the-life of’ a Security Analyst, it is recommended that before starting any task, you assess what you can, and cannot do.
  - b. In the second phase, you will receive five requests to fix or configure security measures in your network. Please take care of them one-by-one, but think and act as fast as you can. Consider that people (an entire department of a company) may be waiting for you to resolve the issue, so that services for GoodCorp customers can continue to be provided.
  - c. In the last phase, you may, or may not face some new challenges. If you encounter a problem, try to calmly (and quickly) troubleshoot it!!  
Your network may be under attack, and you will not want to lose your job on the very first day!!

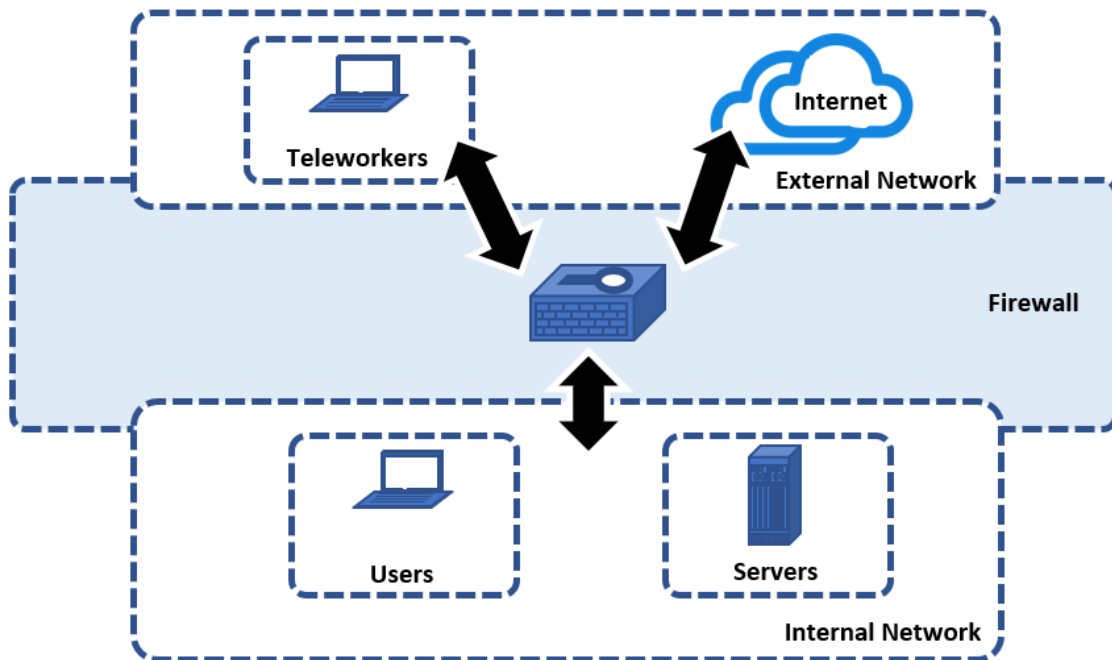
- 
- 4 Some preparations may be needed on your physical host, if they were not done already for previous labs, such as installing the OpenVPN client.
  - 5 If you have a specific problem with your environment, you will be placed in a separate room, so that an instructor can help you with it, outside the class.

**Time is running out! Begin working on the project now!**

## Project Scenario

The description below for your project environment is based on a sample diagram of the actual infrastructure.

Review the following diagram:



(Diagram #1)

### Important:

You can optionally use the detailed image of this diagram in **Appendix I**, and print it out (just that page). That's your topology. Use it as a reference all the time, and write notes on it. There are some blanks as suggestions of notes you should take, but you can also add any note you think is important. Alternatively, you can convert it to PDF and export it to a tablet or another PC. The idea is to have the diagram before you at all times.

About the scenario itself, your physical host (and your own Internet access) will basically mimic the Internet for this activity. Your host, as an external agent, will be required to access some resources in the GoodCorp network.

---

The VMs that you are receiving will, in some cases, be internal resources of the network, or an external machine.

The following is a description of the VMs:

**VM #1** is a *pfSense Firewall*. It separates the Internet from your “local” scenario and works with NAT between the networks. The firewall is configured to get, on the WAN interface, an IP address from the same subnet as VM #1 and your physical host (DHCP client). For the LAN Interface, pfSense is the DHCP server and the default gateway for your “local” environment. pfSense also runs Suricata and OpenVPN for some of the tasks. No need to install anything else on the host.

**Note:** We strongly recommend you become accustomed with taking notes about the information you are receiving. If you are using the optional diagram in **Appendix I** for your notes, you may have noticed you have space to fill in the information about IP addresses for your host, VM #1, and all other VMs. This will be helpful later.

**Note:** We also included a second diagram in **Appendix II**. This is a handwritten example of how a Security Engineer could start the survey work, by gathering information, to understand the scenario.

**VM #2** is a *Nagios Appliance*. It will help you in the monitoring tasks later. Nagios VM has an IP address in the local network.

**VM #3** that you see in the diagram is a *Kali VM*. It may have some important tasks later in the project. It runs in bridged mode, which means that the VM has an IP address on the same subnet as your physical host.

**VM #4** is an *Ubuntu* host. It will host some services, including a web server that will simulate an internal web service for external access. No need to change or configure anything on this host.

**VM #5** is a *Debian* host. This machine represents the local network clients and will be used for remote access tests as well. It is a DHCP client in the local network.

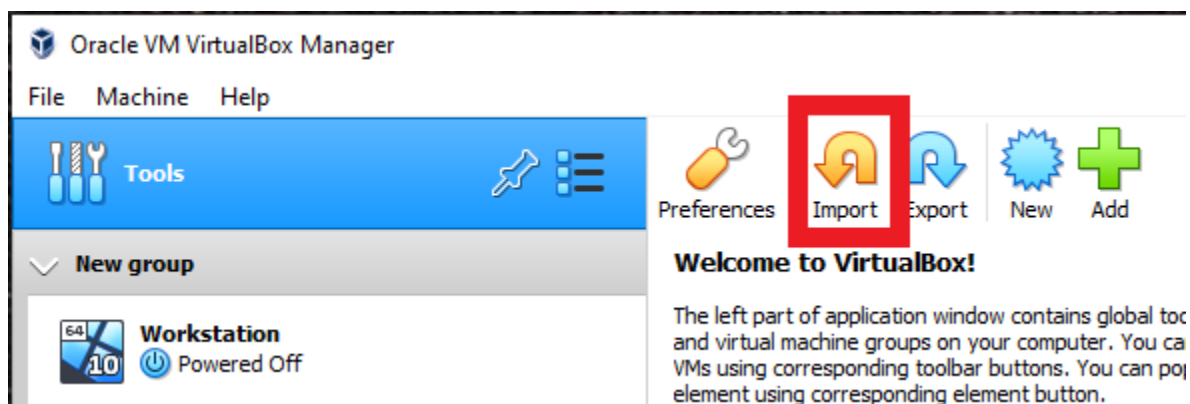
## Instructions for Downloading and Importing the VMs

**Note #1:** These instructions assume that you already have an instance of VirtualBox up and running on your system. If you don't have one, stop here and obtain a working instance of Oracle VirtualBox.

**Note #2:** Some VMs may require access credentials. Please check **Appendix III** of this document for a complete list of user names and passwords.

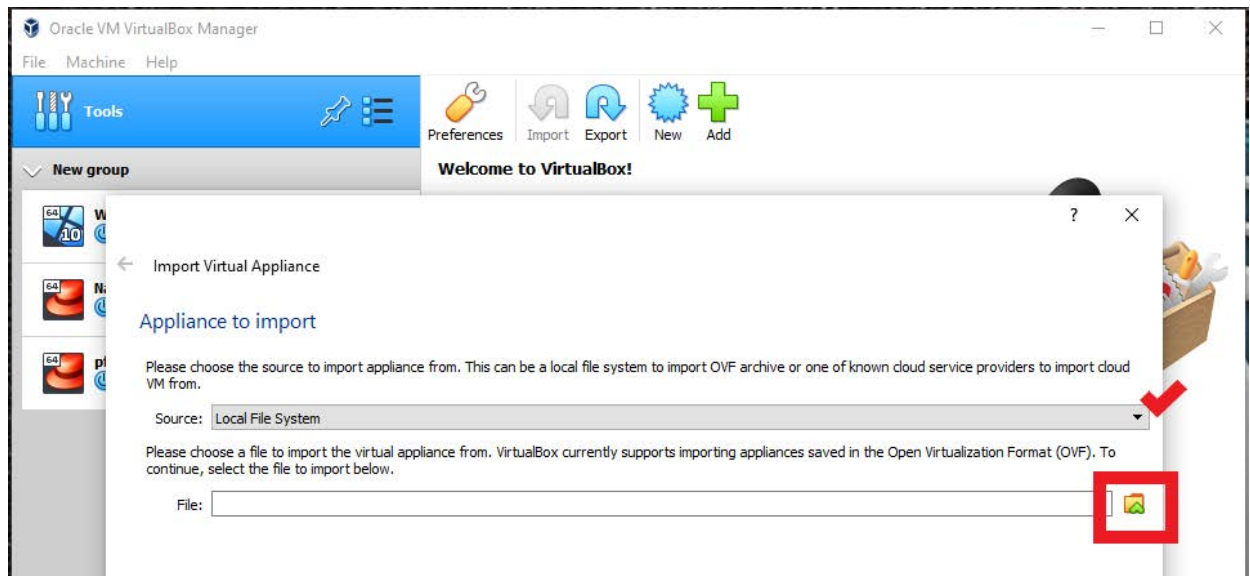
To ensure that your scenario works as it should, please follow these directions:

1. Download the files from the Google Drive. An instructor will give you the link as soon as possible.
  - Due to the size of the files, Google is not able to check the files for viruses. You can trust that the files are clean, and click **Download Anyway**.
  - Is recommended that you download each file in sequence. Most importantly, if you think your Internet bandwidth is not fast enough, separate downloads one after another will be faster than an attempt to download all five files at once.
2. Move all files from your Downloads folder to your VirtualBox working folder.
3. Select **Import** in the **Tools** menu.

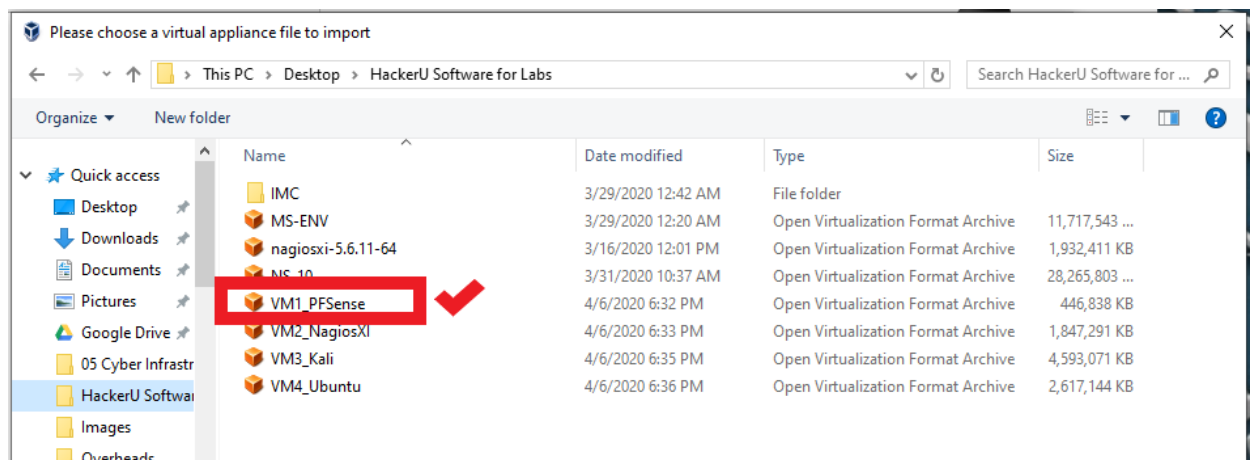




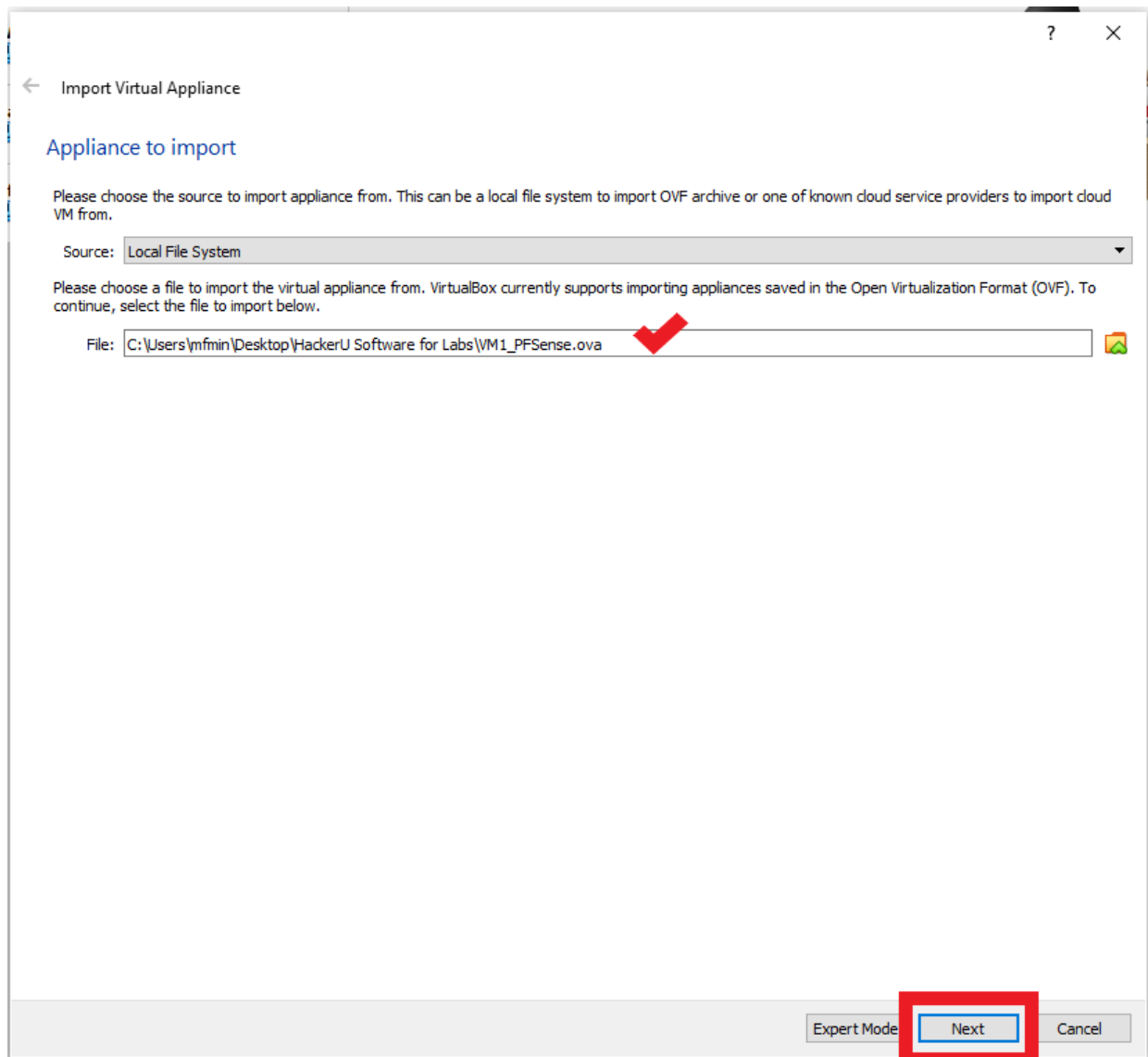
4. In the *Appliance to Import* window that appears, check that *Local File System* is selected as Source, and click **Browse folders** to locate the file you need.



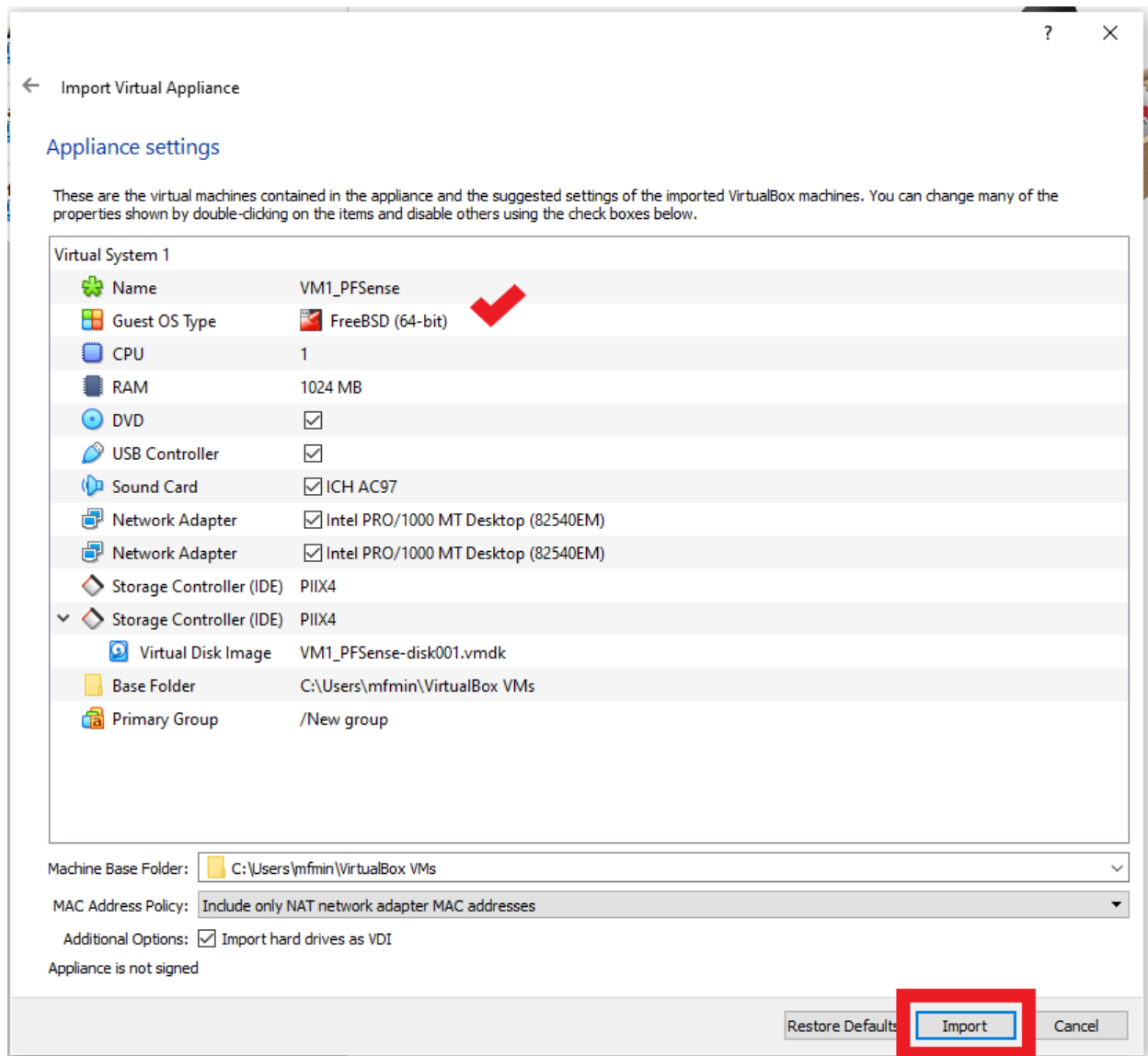
5. Locate the file named "VM1\_PFSense" and import it.



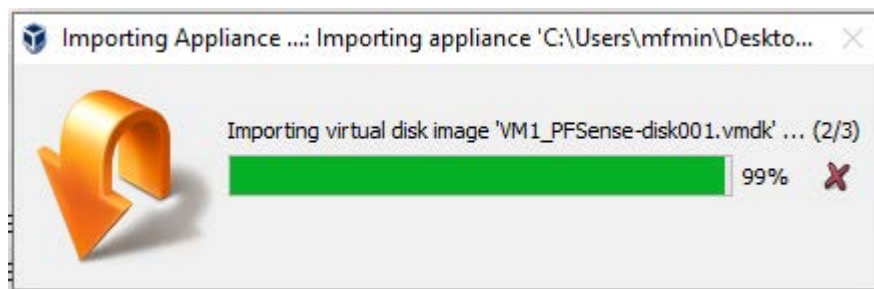
6. In the Appliance to Import window, check that the file name is the one you want, and click Next.



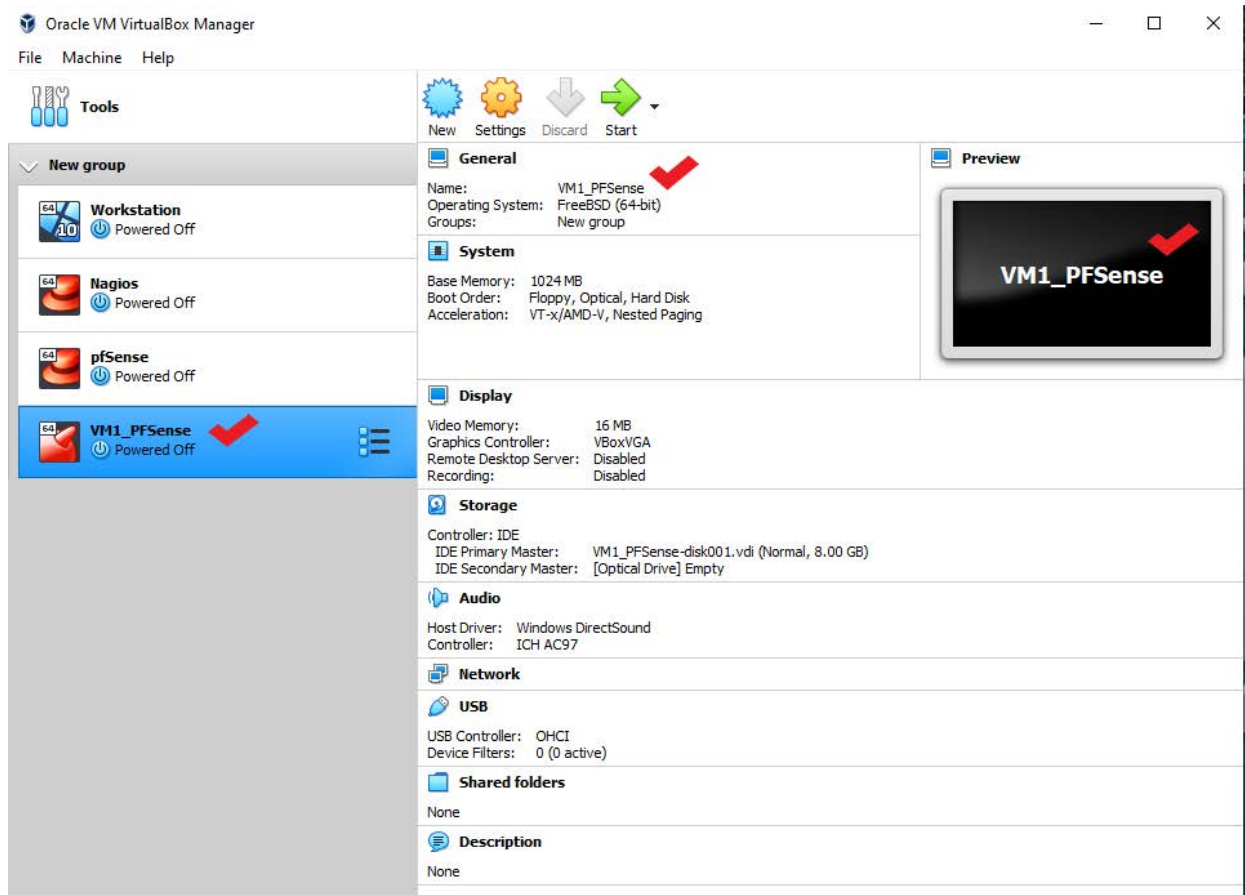
7. In the Appliance Settings window, you can view all the information about the VM you are about to import. Click **Import**.



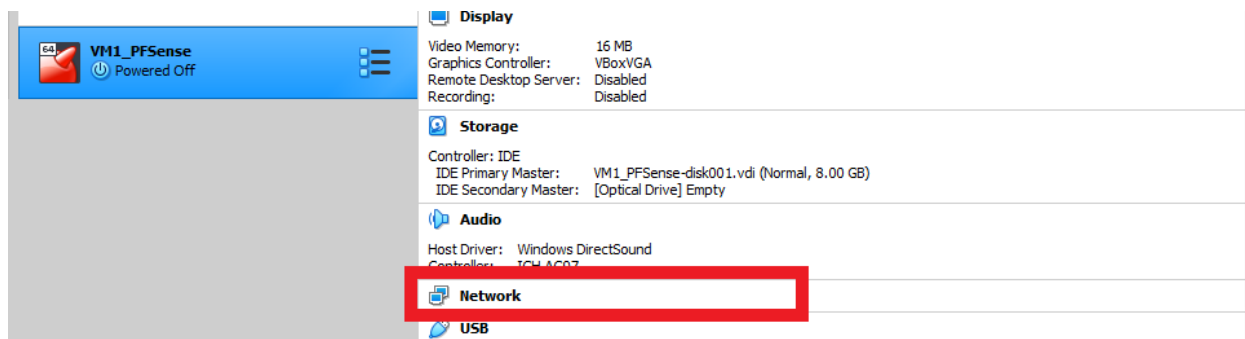
8. The import process will begin and you will see a progress bar.



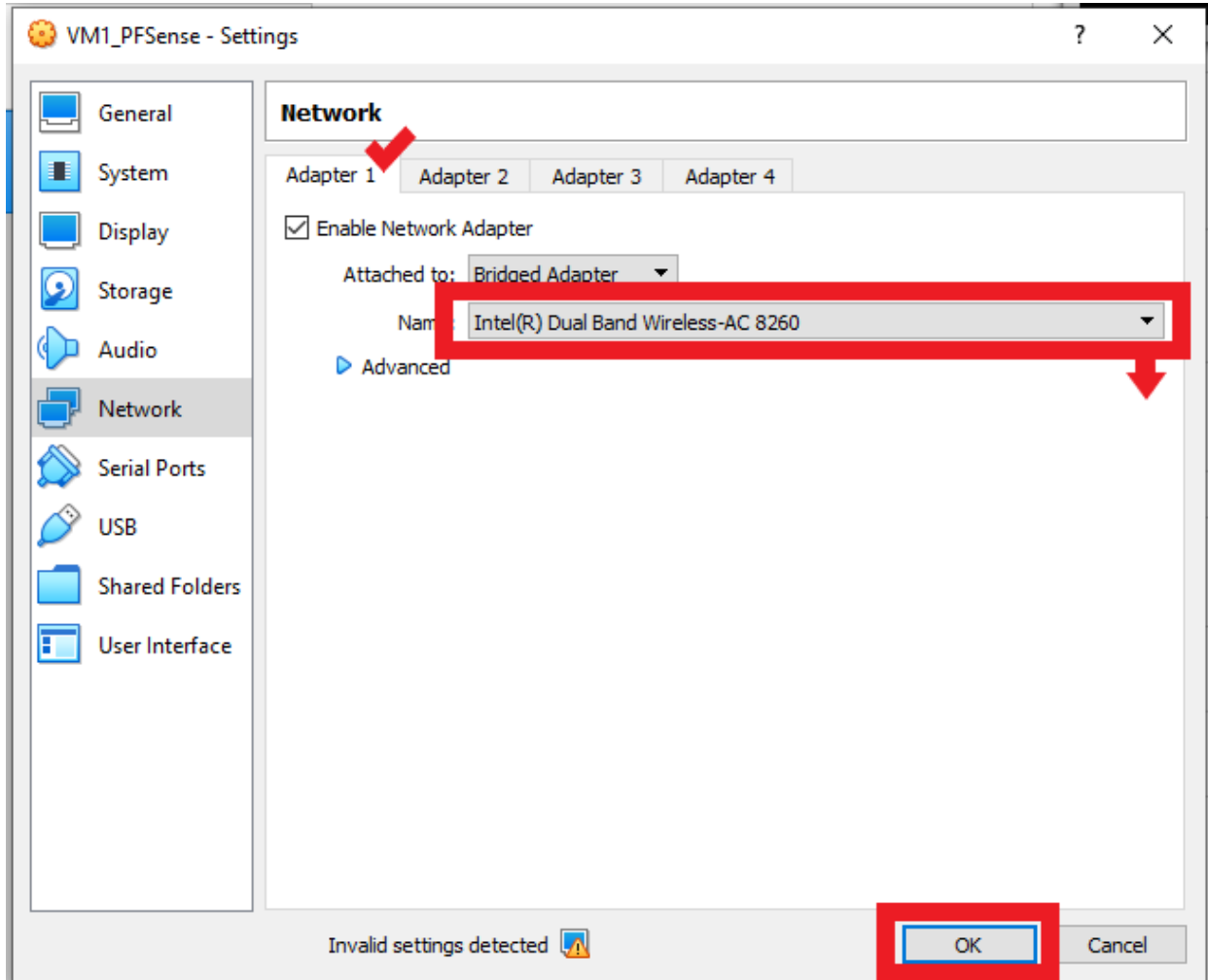
9. When the process ends, you will see the VM imported to your VirtualBox.



10. **Important:** You will need to adjust the Network Adapter name to match the Network Adapter on your VirtualBox host. Click **Network**.

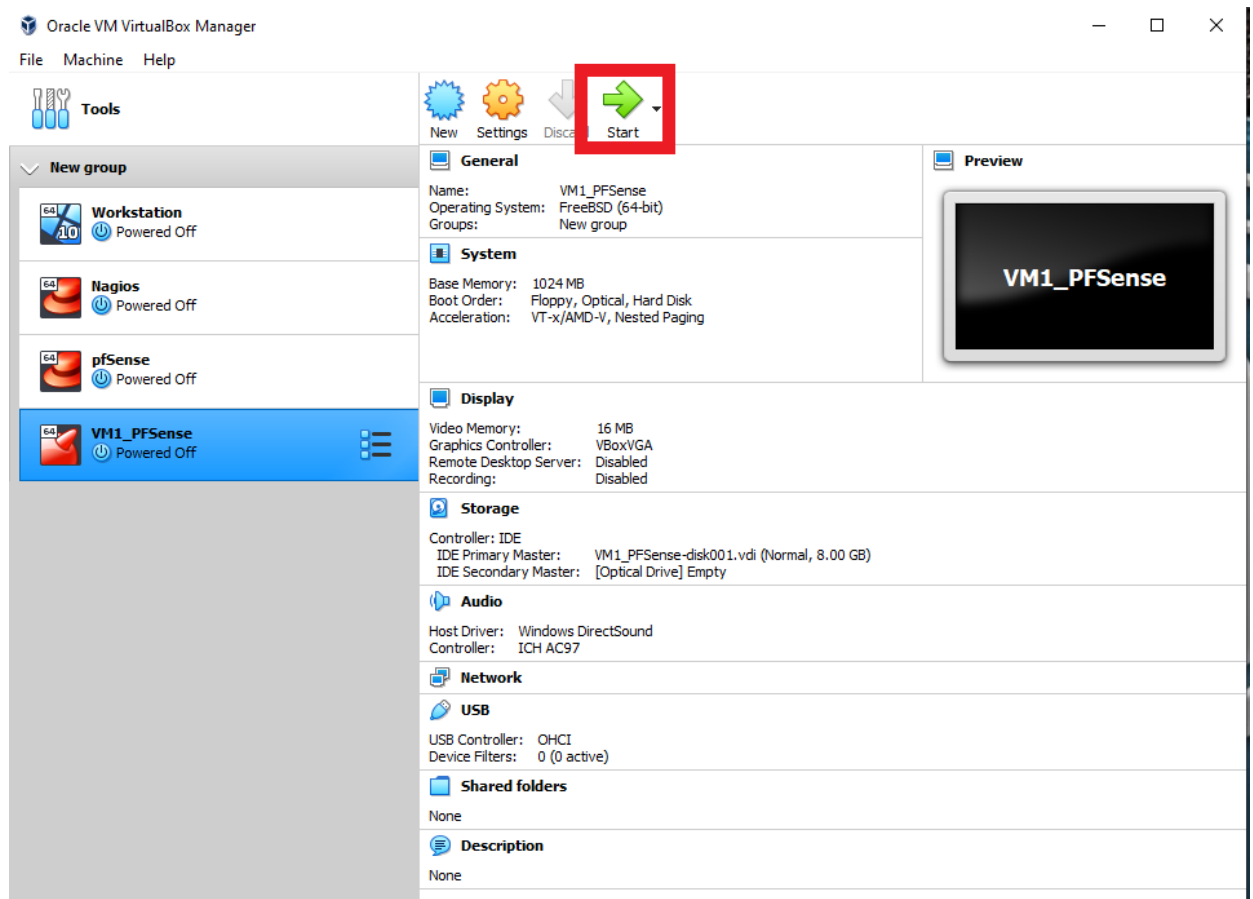


11. In the Settings window, you will see the tab **Adapter 1**. For *Name*, click the drop-down list and select the name of the physical interface that will be used to connect the VM to the network.

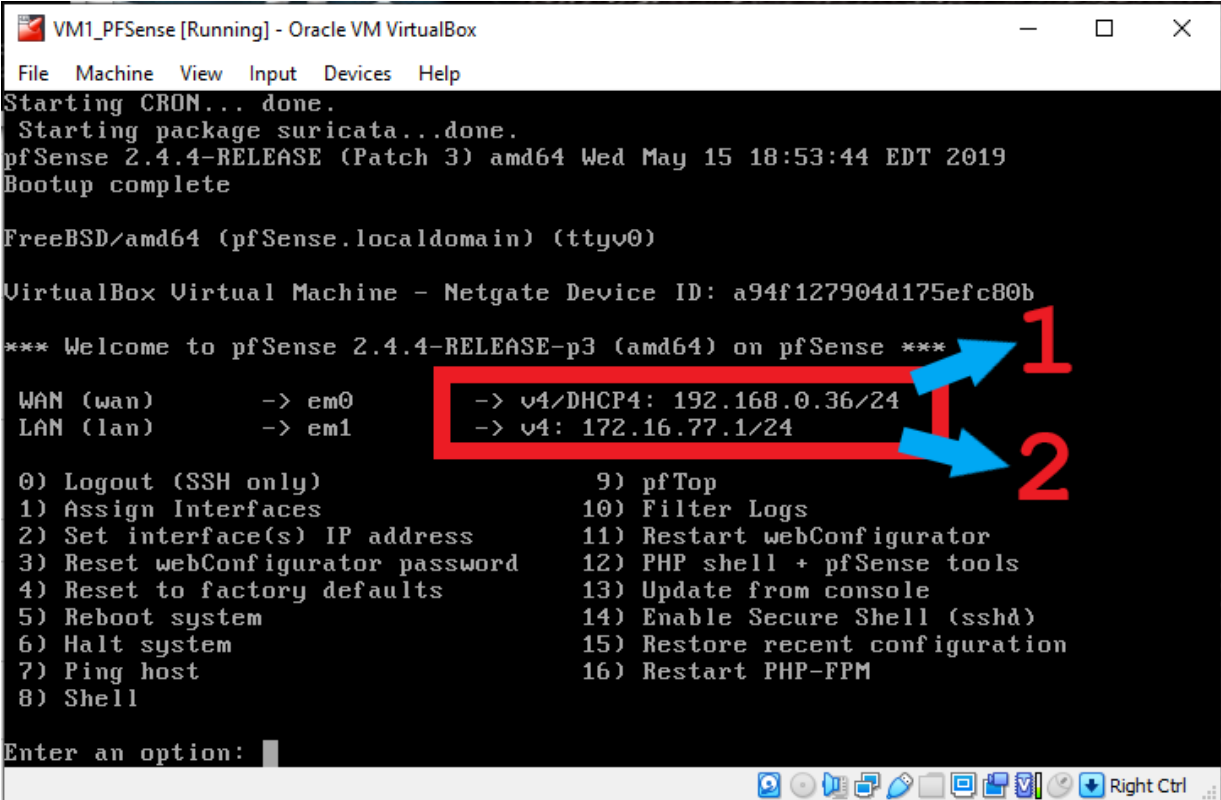


Eventually, just by opening the network settings, VirtualBox will assume your local NIC as an option, so you may see the name already selected. In this case, just click **OK** if that is the one you are planning to use.

12. In the VirtualBox interface, click **Start**.



13. The VM will boot and will reach its final state. In the case of *VM1\_PfSense*, this is what is expected:



The screenshot shows a terminal window titled "VM1\_PfSense [Running] - Oracle VM VirtualBox". The terminal output includes the following text:

```
File Machine View Input Devices Help
Starting CRON... done.
Starting package suricata...done.
pfSense 2.4.4-RELEASE (Patch 3) amd64 Wed May 15 18:53:44 EDT 2019
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: a94f127904d175efc80b

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.36/24
LAN (lan)      -> em1      -> v4: 172.16.77.1/24

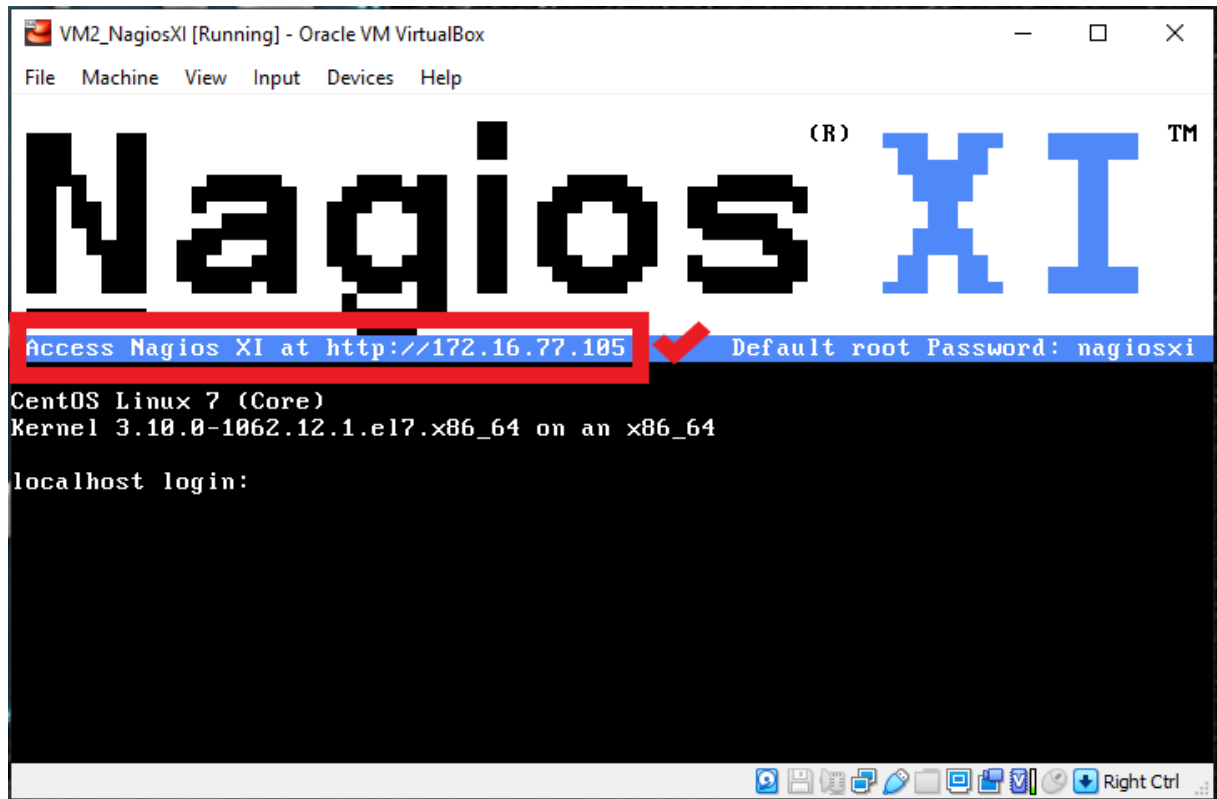
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 
```

Two red arrows labeled "1" and "2" point to the IP addresses in the configuration section. Arrow "1" points to the WAN IP address "192.168.0.36/24". Arrow "2" points to the LAN IP address "172.16.77.1/24".

- The *WAN* (*em0*) IP address should appear as *v4/DHCP4*, and with an address from your physical lab subnet. Note that the address you see in the screen, marked as "1", is just an example.
- The *LAN* (*em1*) IP address should appear as *172.16.77.1/24*, marked as "2" in the image above. This was statically defined for this lab.

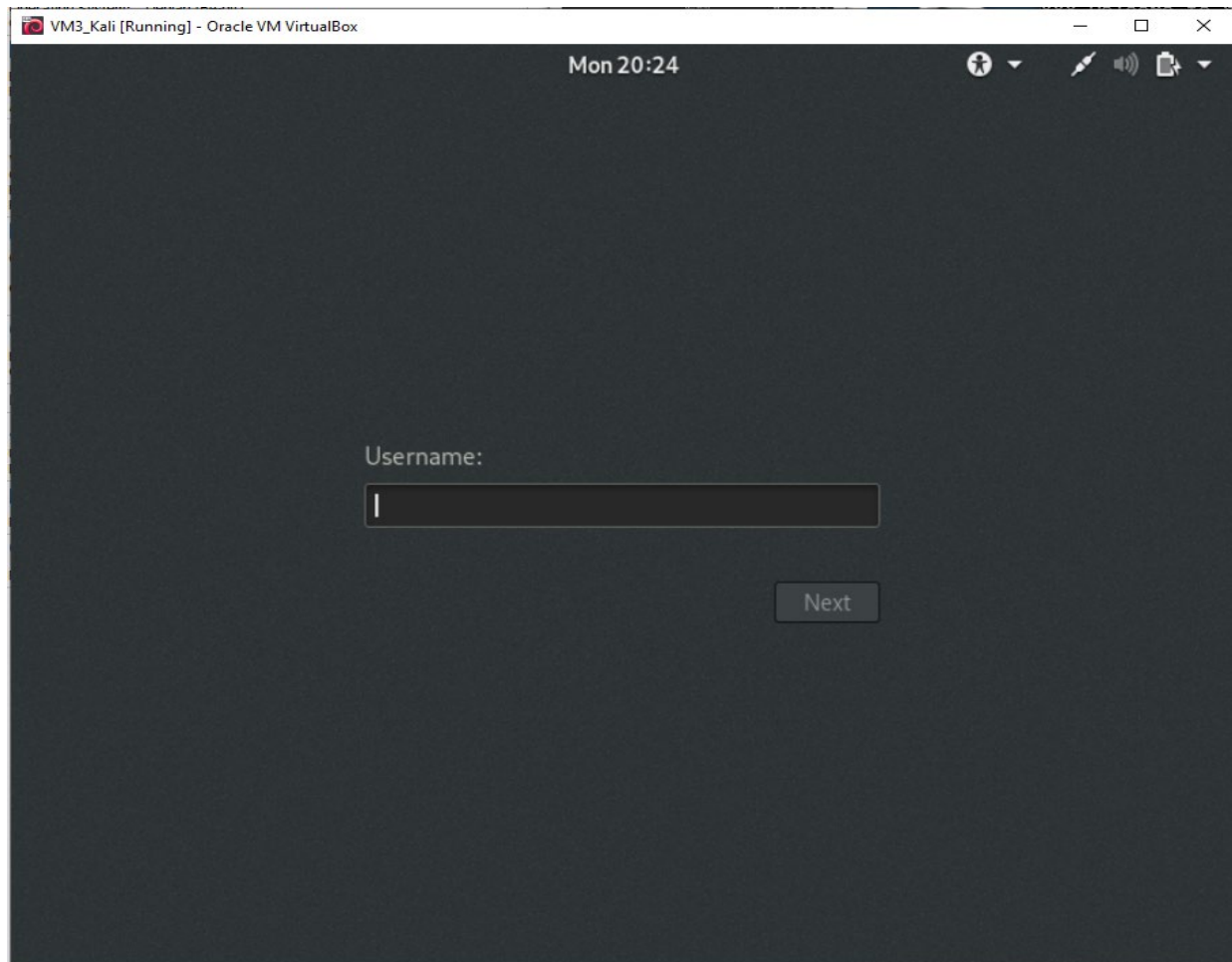
14. Repeat steps 3 through 8 for *VM2\_NagiosXI*, and start the VM.
15. The VM will boot and reach its final state. In the case of *VM2\_NagiosXI*, this is what is expected:



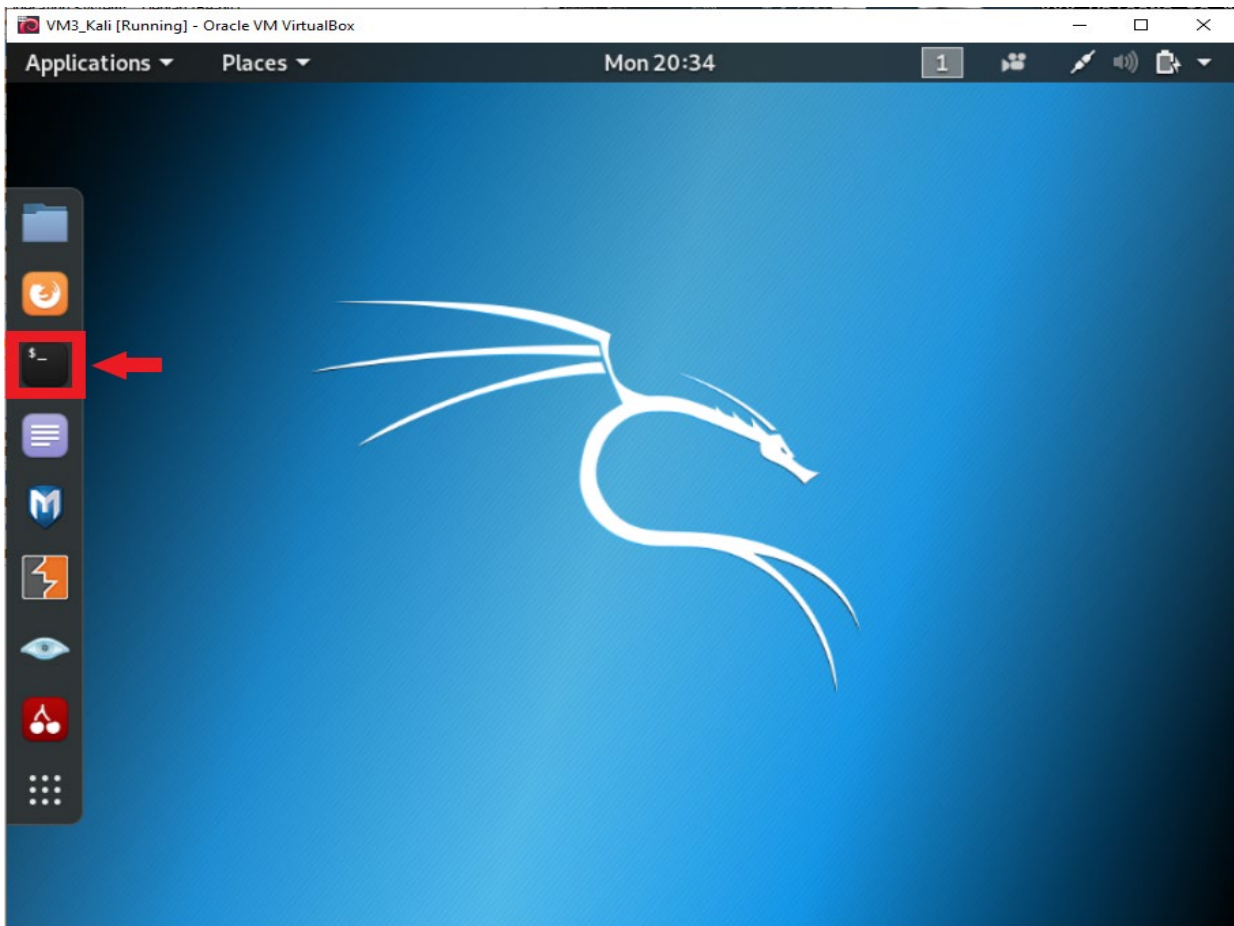
- The address should be in the same subnet as the pfSense LAN interface.
- The address should be provided by the pfSense DHCP Server.



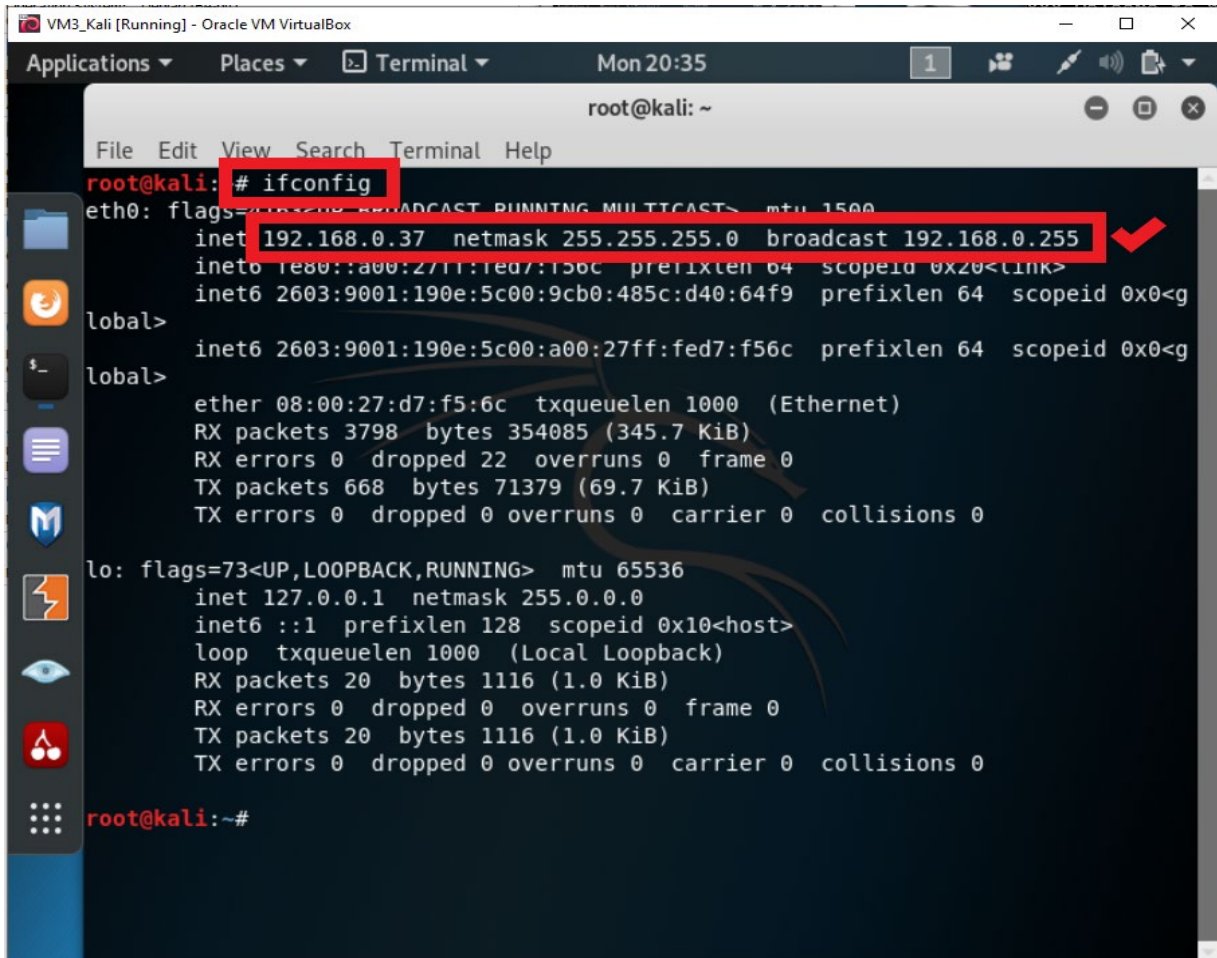
16. Repeat steps 3 through 12 for *VM3\_Kali*, and start the VM.
17. After the boot process ends, you will see a window like the following:



18. Log in using the credentials listed in **Appendix III** and click **Terminal**.



19. At the terminal CLI, type **ifconfig** and make sure you have the VM with an IP address of your local lab subnet.

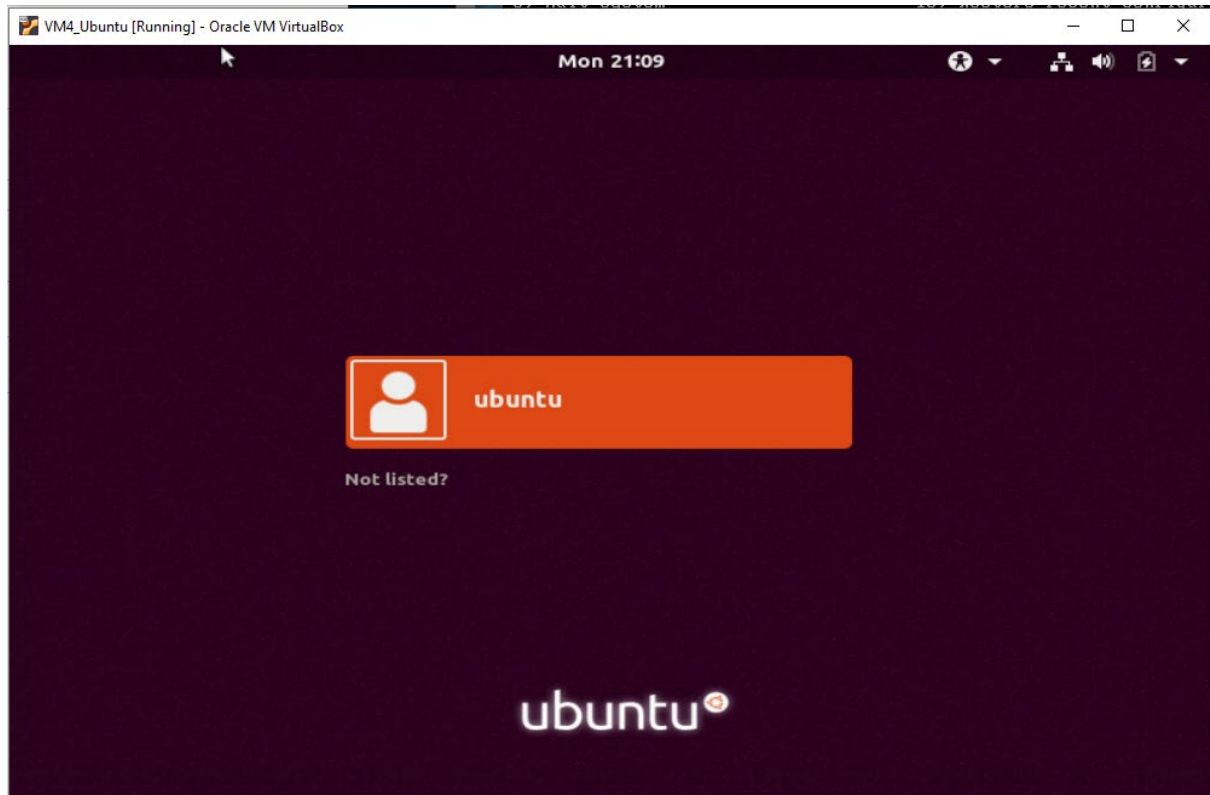


```
VM3_Kali [Running] - Oracle VM VirtualBox
Applications ▾ Places ▾ Terminal ▾ Mon 20:35 1
root@kali: ~
File Edit View Search Terminal Help
root@kali: # ifconfig
eth0: flags=UP,BROADCAST,RUNNING,MULTICAST mtu 1500
    inet 192.168.0.37 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fed7:f56c prefixlen 64 scopeid 0x20<link>
    inet6 2603:9001:190e:5c00:9cb0:485c:d40:64f9 prefixlen 64 scopeid 0x0<g
lobal>
    inet6 2603:9001:190e:5c00:a00:27ff:fed7:f56c prefixlen 64 scopeid 0x0<g
lobal>
    ether 08:00:27:d7:f5:6c txqueuelen 1000 (Ethernet)
    RX packets 3798 bytes 354085 (345.7 KiB)
    RX errors 0 dropped 22 overruns 0 frame 0
    TX packets 668 bytes 71379 (69.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

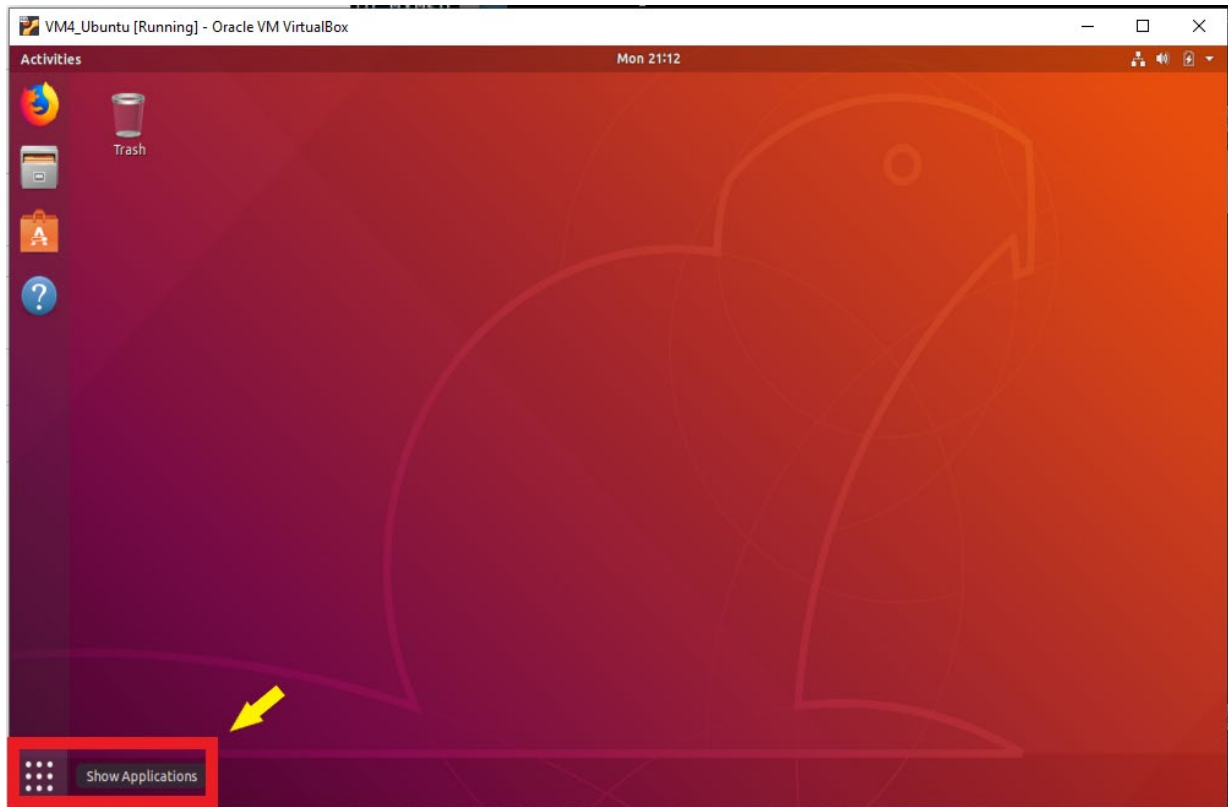
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1116 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1116 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

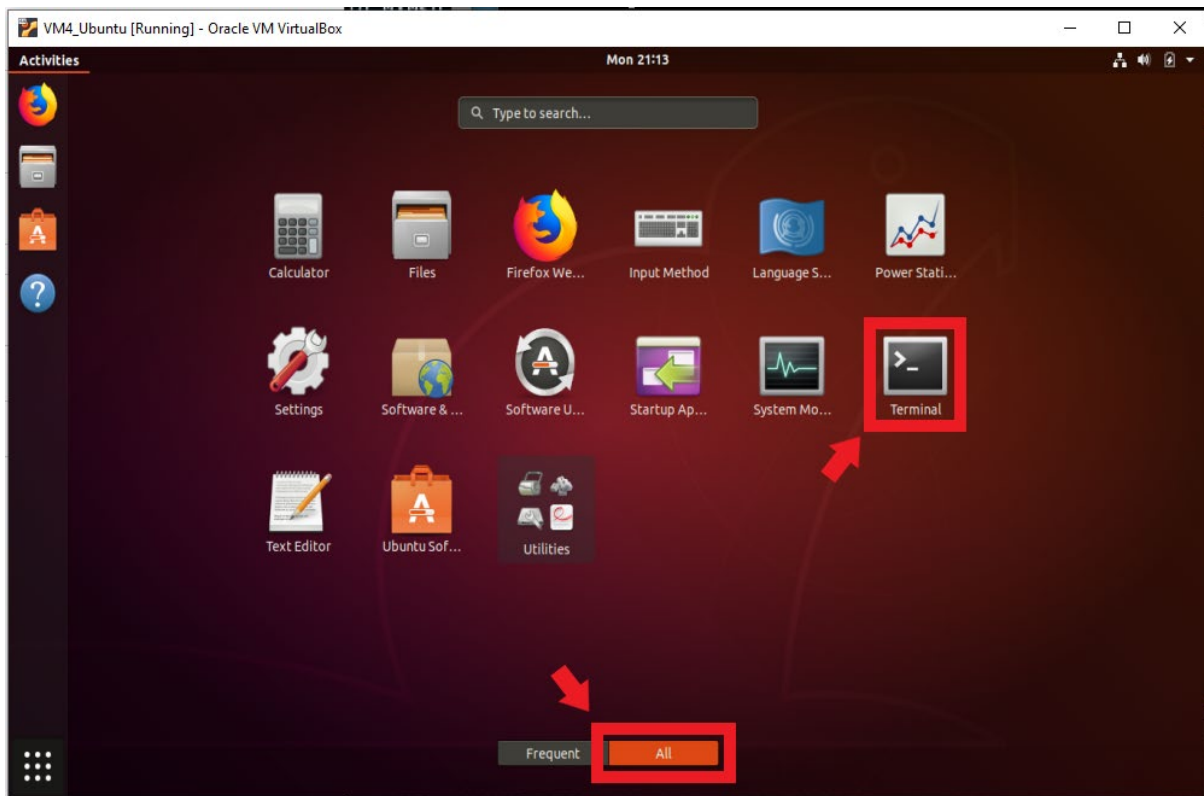
20. Repeat steps 3 through 8 for *VM4\_Ubuntu*, then start the VM.
21. After it boots up, you should see the login window.  
Enter the user name and password provided in ***Appendix III***.



22. In the main desktop, at the bottom left corner, click **Show Applications**.



23. Make sure you see all applications (bottom center) and click **Terminal**.

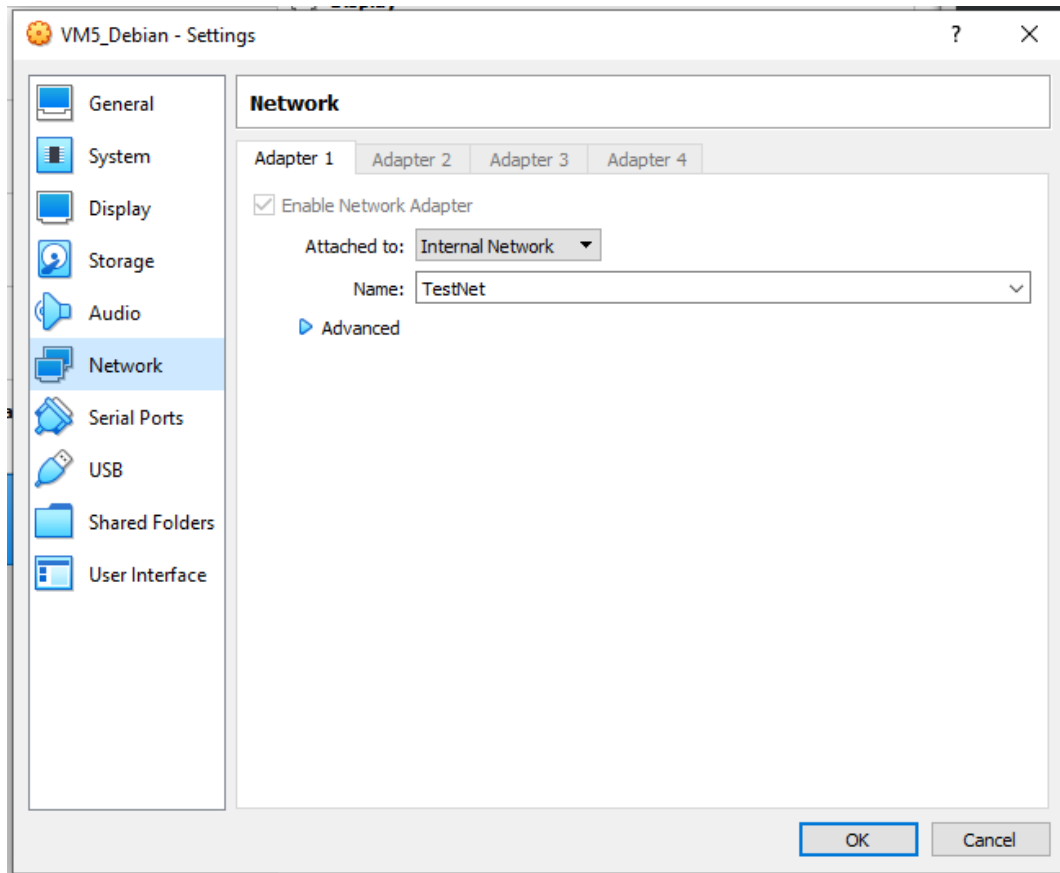


24. In the Terminal CLI, use the command **ip addr** to verify that the VM is in the same subnet as the pfSense LAN interface.

```
ubuntu@ubuntu-VirtualBox: ~  
File Edit View Search Terminal Help  
ubuntu@ubuntu-VirtualBox: ~$ ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default  
    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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:3c:00:00 brd ff:ff:ff:ff:ff:ff  
    inet 172.16.77.106/24 brd 172.16.77.255 scope global dynamic noprefixroute enp0s3  
        valid_lft 5479sec preferred_lft 5479sec  
    inet6 fe80::a499:fb62:da0e:e122/64 scope link noprefixroute enp0s3  
        valid_lft forever preferred_lft forever  
ubuntu@ubuntu-VirtualBox: ~$
```

25. Repeat steps 3 through 12 again for *VM5\_Debian*.

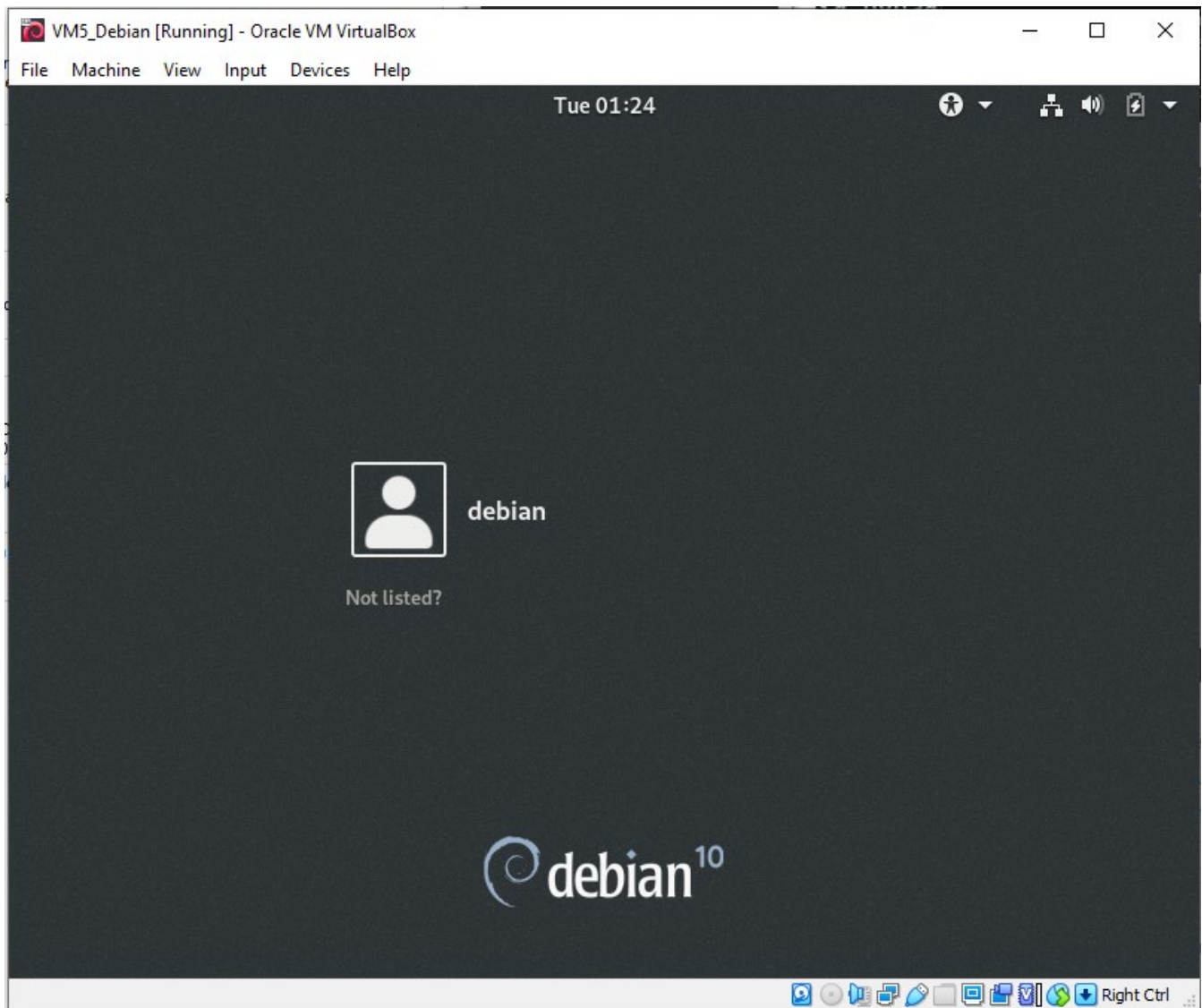
However, in this case, under *Network*, you only need to change “Attached to:” to “Internal Network”.



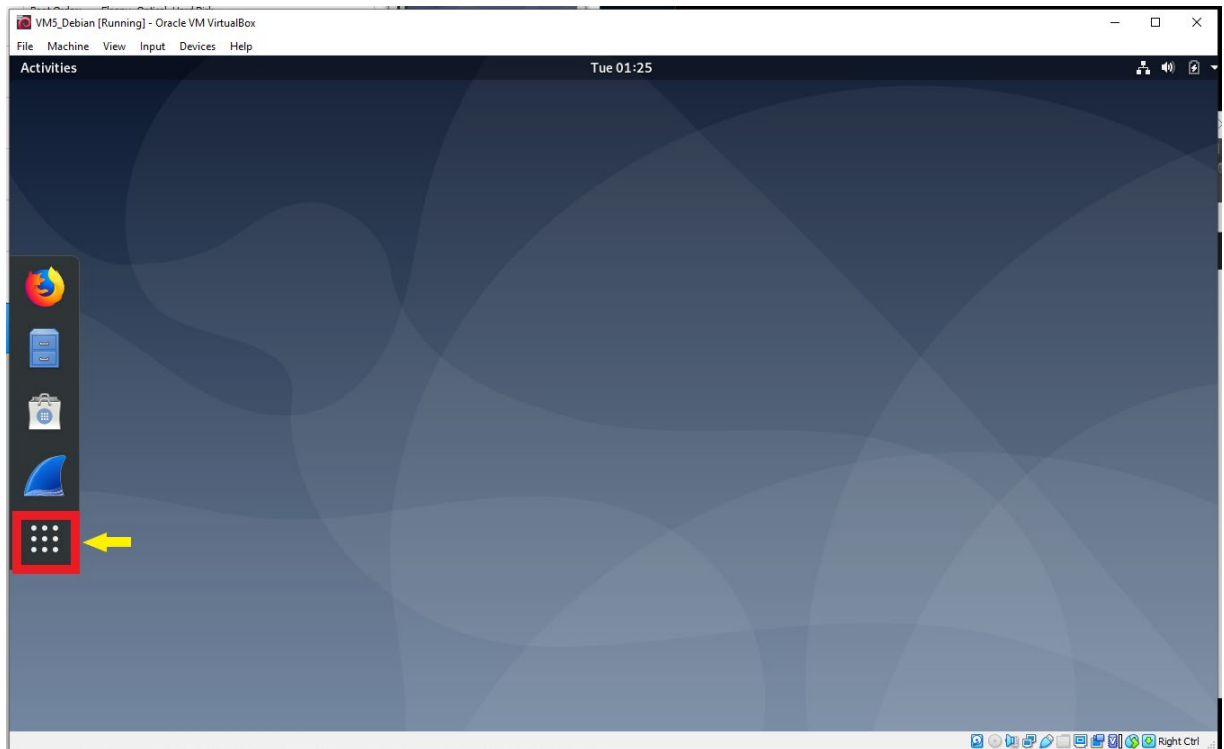
- If you have more than one internal network, choose **TestNet**, click **OK**, and start the VM.



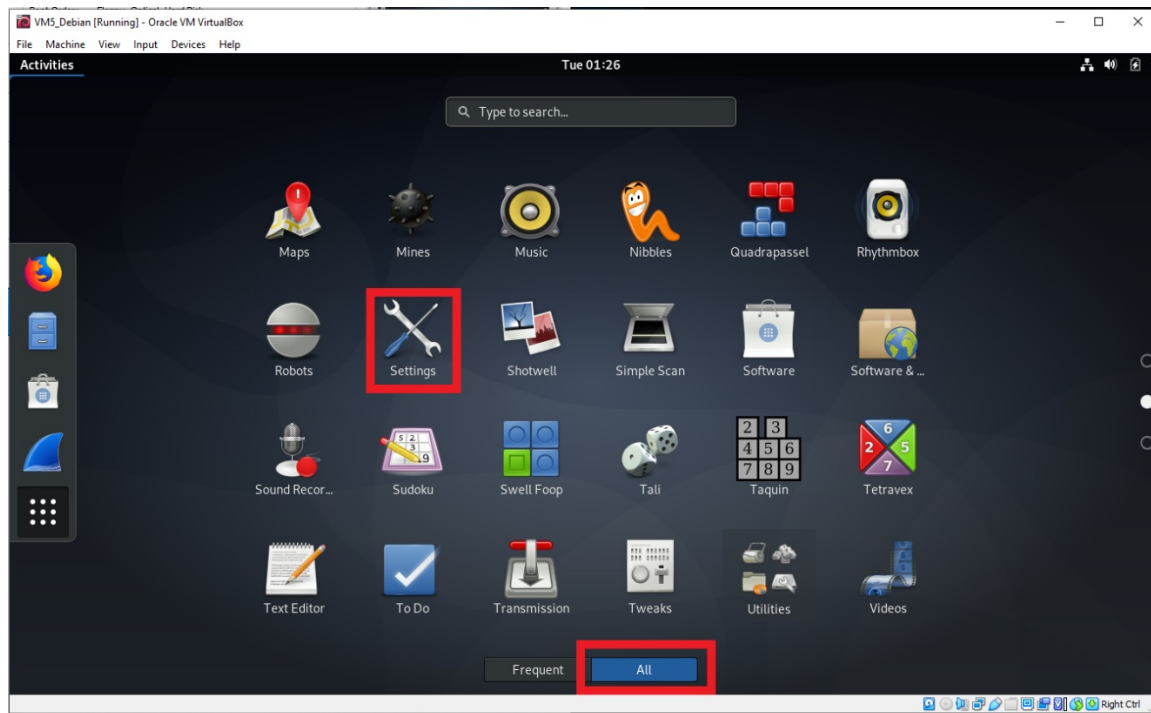
26. After the VM starts, you will see the login screen.



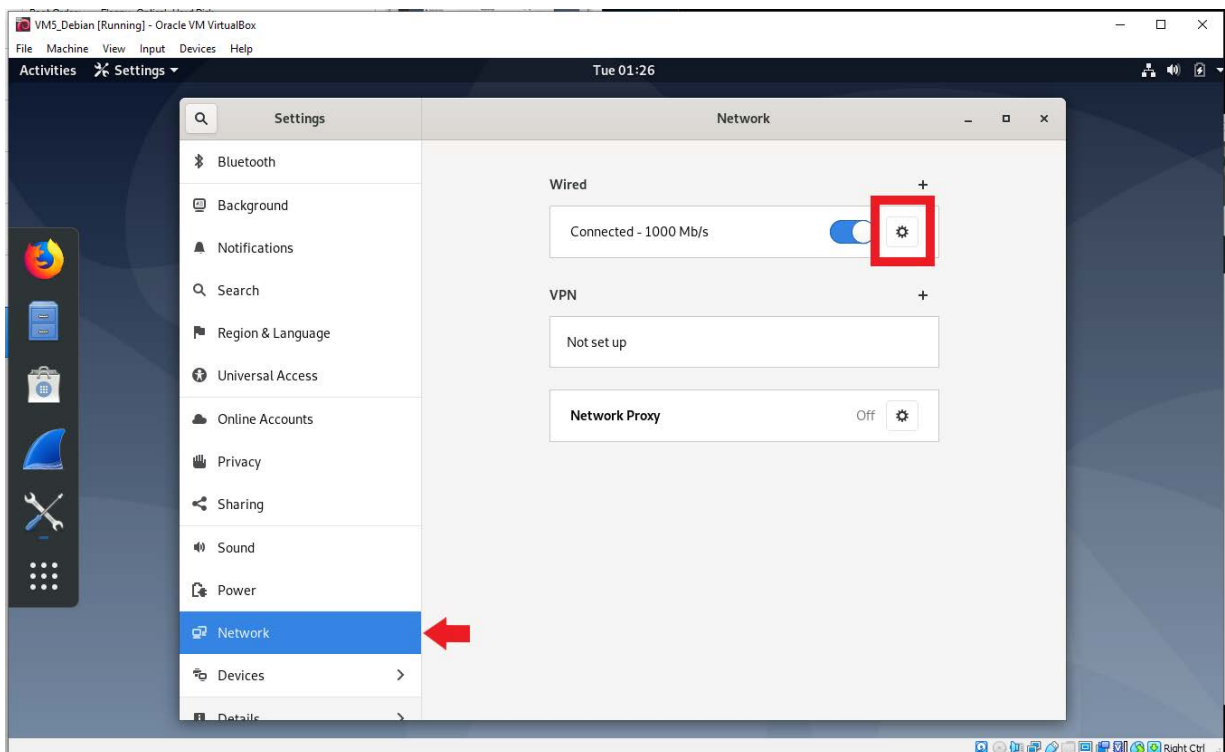
27. Use the credentials provided in **Appendix III** and log in to the VM.
28. Click **Show Applications**.



29. At the bottom center area, verify that **All** is selected, and click **Settings**.



30. Select **Network**, and make sure that *Wired Connection* is enabled. Then click the gear icon.



31. Verify that the IP Address is in the pfSense local interface address range.

Cancel **Wired** Apply

**Details** Identity IPv4 IPv6 Security

Link speed 1000 Mb/s

IPv4 Address 172.16.77.109 ✓

IPv6 Address fe80::a00:27ff:fe13:a

Hardware Address 08:00:27:13:00:0A

Default Route 172.16.77.1 ✓

DNS 172.16.77.1

☒ Connect automatically

☒ Make available to other users

☐ Restrict background data usage  
Appropriate for connections that have data charges or limits.

Remove Connection Profile

32. You have now installed all the VMs required for the scenario.

Everything is prepared and ready for testing!

---

## Scenario Validation

Before you begin the project tasks, it is important that you verify that all VMs are operational. Check the connectivity among them and become familiar with their configurations. Everything was designed to work and run as expected, if the configuration was done properly.

To be sure that the VMs function as they should in your environment, perform the following tests:

- 1** Check IP addresses for all hosts.
- 2** Host xx should be able to ping host yy (list the tests here ...).
- 3** Host zz should be able to ping hosts aa and bb.
- 4** Host ww should NOT be able to ping host hh.
- 5** From host dd, you should be able to open a web page from zzzzzzz.

Please note that these are only preliminary tests and validations to verify that the scenario was correctly imported and runs as it should. Additional verifications may be needed later as you gather information to solve the issues presented in the project.

## Project Task 1: Blocking Unwanted Traffic

A primary complaint of GoodCorp's HR is that some employees spend time with apps they shouldn't use. For example, a user was caught several times playing online games, while he should have been placing orders on supplier websites.

The request from the HR Manager is that you block the games and get that employee to focus more on his job.

You know that HTTP is important for GoodCorp's business, and should be accessible. In fact, web traffic is the most common communication your company has with its customers and suppliers. It should definitely not be blocked.

For this project, ping (ICMP) will be the port that is used for gaming.

**Tip:** In real life, port numbers, destination addresses, and source addresses can be different, but the concept of blocking one traffic type (or destination) while allowing others, is the same. Therefore, in this project, you will only need to create a firewall rule that disables traffic other than HTTP.

These are the steps you need to follow:

- 1** On your Debian VM, test that traffic is authorized.
  - a. Use a terminal to run pings to different destinations.
  - b. Test ping to 4.2.2.2.
  - c. Test ping to 8.8.8.8.
- 2** In pfSense, the first thing to do is to allow traffic (deselect the block) for private networks and loopback addresses.
  - a. Hint: Interfaces → WAN
  - b. Deselect both boxes at the bottom of the page.
- 3** Create a Firewall rule that blocks traffic that is not allowed for a specific destination.
  - a. Use 8.8.8.8 as the destination to be blocked for ICMP.
  - b. Hint: Firewall → Rules → LAN
  - c. Request: Create a name in the policy for future reference.
  - d. Another request: Set pfSense to log packets that match the rule.

---

**4** Now, test ping both addresses once again.

**Before you begin Task #2, think about this:**

- Which Best Practices were involved in the solution for Task #1?
- What evidence can you provide to show that everything works as expected?

## Project Task 2: Quick Solution for Remote Access

During the Covid-19 outbreak, some services needed to be performed remotely.

An employee lives in Safer City and is now working from home. He requires access to systems running on the web server at the HQ office.

The Warehouse Manager requests VPN access for that employee, but wants the employee to have temporary access via other means.

He asks you to make the web server available on the Internet, but because you are not so crazy, you need to come up with an ingenious solution for the issue.

What would that solution be?

**Tip:** What about creating a port forwarding rule on pfSense to make external access to port 80 available?

Keep in mind that you will need to be sure that the web server (Ubuntu VM) is functioning, and the web service is up and running.

In real life, you would probably never create a rule like that.

But, for this project, we will use port 80, because it is easier to verify that it works.

These are the steps you need to follow:

- 1 Test access to your web server from your physical host.
- 2 Test access to your web server from the Debian VM.
- 3 On pfSense, create a NAT rule to translate your external requests to internal addresses.
  - a. Hint: Firewall → NAT
  - b. Request: Create a name in the policy for future reference.
  - c. Another request: Set pfSense to log packets that match the rule.
  - d. One last request: Set the NAT rule to automatically create a firewall rule on the WAN port, to authorize the traffic.
- 4 Test access to your web server from your physical host.



---

**Before you begin Task #3, think about this:**

- Which Best Practices were involved in the solution for Task #2?
- What evidence can you provide to show that everything works as expected?

## Project Task 3: The All-Seeing Eye

One of your colleagues is a control freak, and he is not comfortable with the level of visibility he has with system resources. A network monitoring tool was already installed, but was never activated.

Your control freak colleague is now bullying you to finish his job. He wants to start monitoring the firewall and the web server.

How would you accomplish that?

**Tip:** What do you think about configuring Nagios to monitor the devices?

You may want to make sure that the firewall and web server are properly configured to be monitored.

These are the steps you need to follow:

- 1** Configure pfSense to be monitored by Nagios:
  - a. Hint: Services → SNMP
  - b. Request: add System Information and System Contact, and enable SNMP Traps for the Nagios host.
- 2** The web server is already configured to be monitored.
- 3** Add devices to Nagios.
  - a. Hint: Navigation → Configure → Configuration Wizards
  - b. Add pfSense as a generic network device.
  - c. Don't forget to add pfSense as an SNMP trap generator.
  - d. Add an Ubuntu or Apache VM (instructors will provide the details about how to do that).

**Before you begin Task #4, think about this:**

- Which Best Practices were involved in the solution for Task #3?
- What evidence can you provide to show that everything works as expected?

## Project Task 4: Come On Home!

After these critical situations were resolved, it is time now to help our staff member in Safe City get a secure way to access the services. (Remember: In Task #2 you created a *temporary, and not-so-safe alternative*.)

The IT Manager just approved the request for a definitive solution, and expects you to have a good idea about what to do.

What will you configure?

How can you give the user the access they need in a secure way?

**Tip:** What about a VPN tunnel between the employee's computer at home and the HQ?

Keep in mind:

- After you are done and your solution was tested, don't forget to disable the port forwarding policy you created earlier.
- The RDP service in the Windows machine will still be used, but differently.

These are the steps you need to follow:

- 1 Disable the rule that allows port forwarding to the webserver.
- 2 Create a VPN Server on pfSense to enable receiving connections from OpenVPN clients.
  - a. **Hint:** VPN → OpenVPN, and then look for wizards.
  - b. We will keep it simple, no external LDAP or RADIUS. Local User database only.
- 3 Download and install an OpenVPN client on your physical host.
- 4 Configure the OpenVPN client to allow access your VPN Gateway.
- 5 Test your connection by accessing the webserver page from your physical host.

**Before you complete the project, think about this:**

- Which Best Practices were involved in the solution for Task #4?

- 
- What evidence can you provide to show that everything works as expected?

---

## But Wait!!!

There was a scenario when you began.

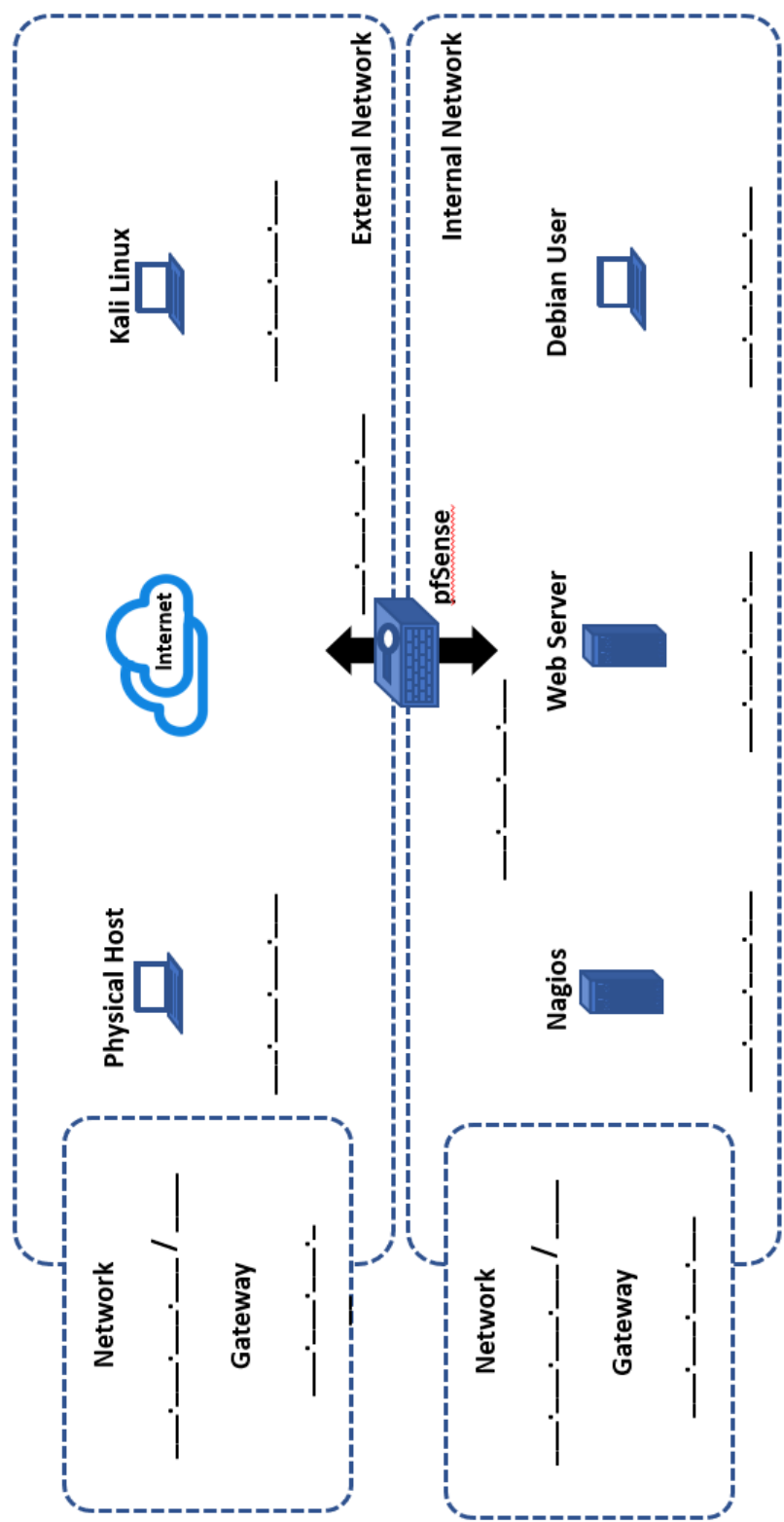
After all the changes you made, perhaps some parts of the machine work differently now.

You need to investigate the firewall logs, IPS logs, and network monitor logs, to be sure that there are no surprises. Check the dashboards too.

Once again: *there may be some surprises!*

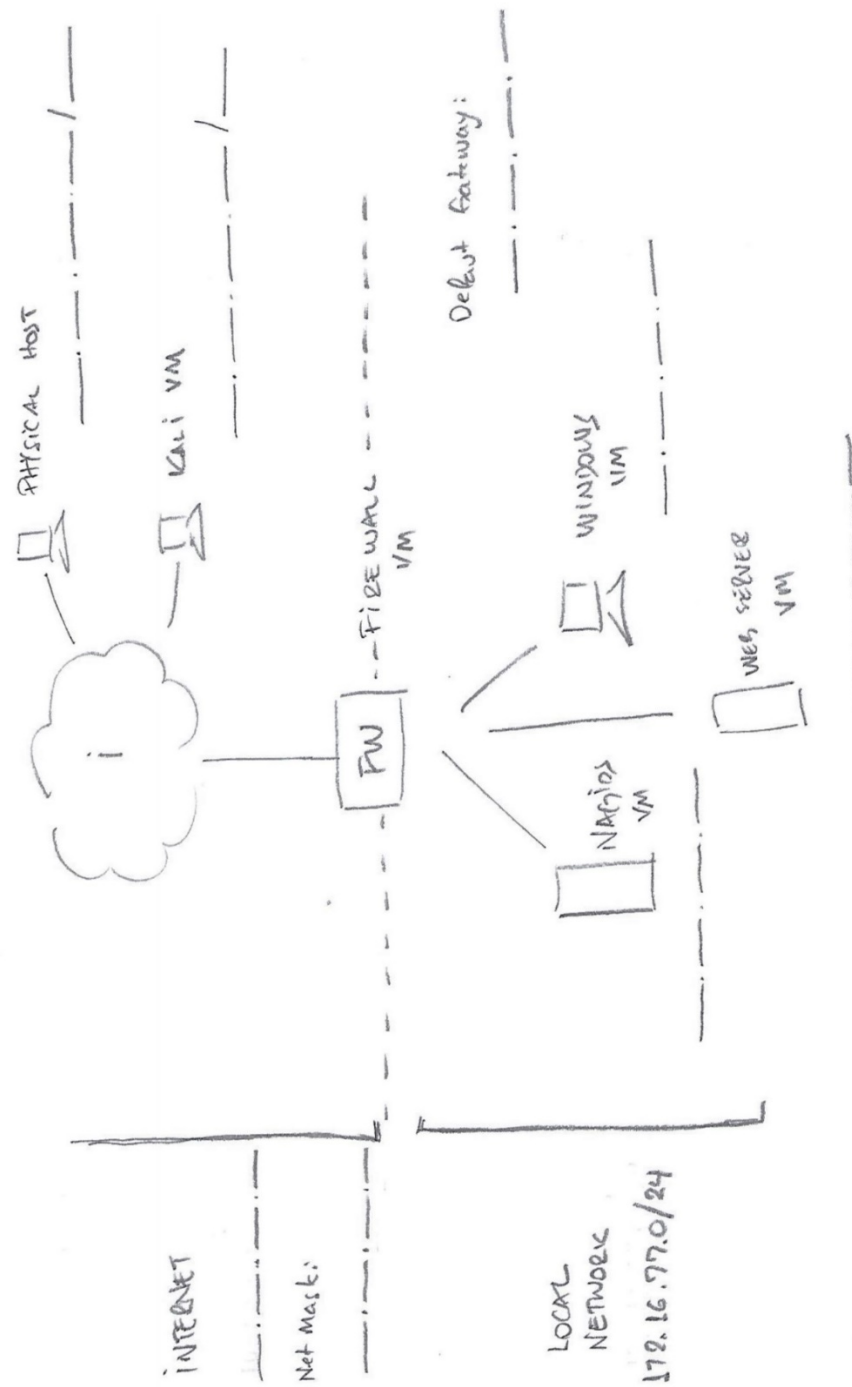
Make notes about your findings.

# Appendix I – Network Diagram



## Appendix II – Network Diagram (Suggestion)

The following diagram is just an idea of how you can take notes about the infrastructure as you get to know the situation.



---

## Appendix III – Credentials for the VMs and Consoles

VM1

VM2

VM3\_Kali

Username: root

Password: UCFCyber

VM4\_Ubuntu

Username: Ubuntu

Password: UCFCyber

VM5

Username: Debian

Password: UCFCyber

pfSense

Username: admin

Password: pfSense

Nagios

Username: nagiosadmin

Password: UCFCyber