

Building a Penetration Testing Virtual Computer Laboratory

User Guide

A. Table of Contents

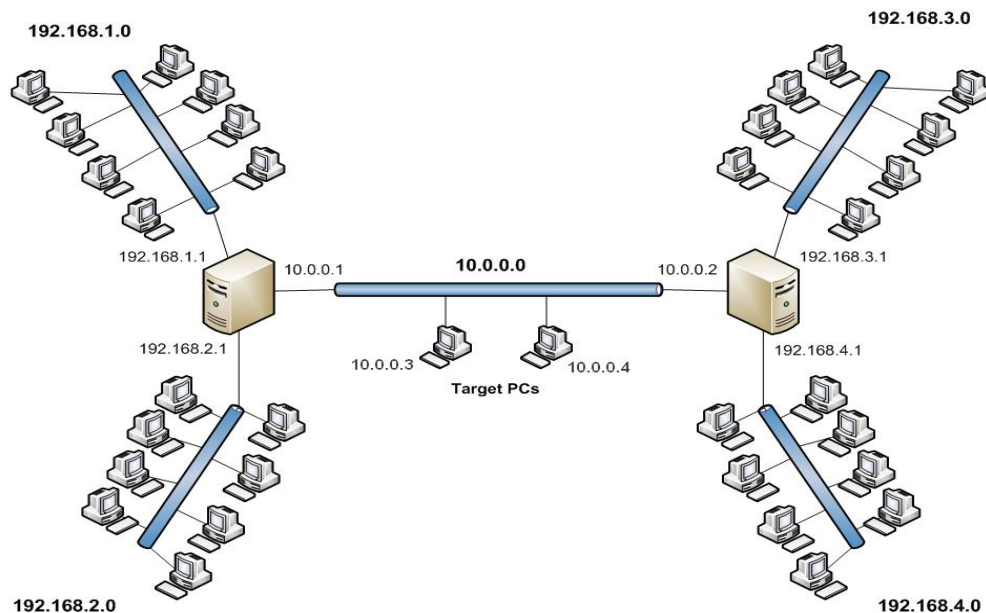
A.	Table of Contents.....	2
B.	Introduction	3
C.	Configure Host Network Hardware.....	4
A.	Creating a Virtual Switch (vSwitch)	4
D.	Create a Virtual Machine	6
A.	Create The Host Virtual Machine for the Ubuntu Gateway/DHCP Server	7
A.1.	Configuring the Virtual Machine	9
A.2.	Install the Ubuntu Operating System	12
A.3.	Install ISO File for Virtual Machine	12
A.4.	VMware Tools.....	13
A.5.	Configure Networking Settings for the Ubuntu Server	14
A.6.	Configure the Dynamic Host Configuration Protocol (DHCP)	2
A.7.	Change the	Error! Bookmark not defined.
E.	Create BackTrack Virtual Machine	Error! Bookmark not defined.

B. Introduction

One successful key in learning about Penetration Testing is by setting up a lab. Building a good penetration testing lab is crucial to ensuring the best possible security posture is in place for the network. There are varieties of reasons for performing a penetration test. One main reason is to find and fix vulnerabilities within your network before an attacker does. In addition, a network penetration test can be used as a secure method to evaluate the true strength of a network defenses, an added measure to proactively mitigate the risk of future threats, and a way to identify a hacker's primary attack route.

This guide describes how to design and deploy a virtual lab using VMware ESXi through VMware vSphere client. The virtual lab will contain 2 Ubuntu Gateway Servers acting as DHCP server routers, a private network connecting both Ubuntu servers and 2 Windows XP virtual target PCs, and 2 separate virtual networks for each Ubuntu server consisting of 8 BackTrack virtual machines connected per network.

Virtual machines provide a secure environment allowing the ability to install, configure, and experiment with operating systems, network, and database software. For this lab you will be using VMware as the virtual environment, 2 Ubuntu servers as the gateway and DHCP server, BackTrack virtual machines as the attacker and Windows XP as the target machine. The gateway machines will have three Network Interface Cards (NIC); one NIC will be used to connect a private network between both Ubuntu servers and the target machines, the remaining NIC will be used to connect two different BackTrack network infrastructures per Ubuntu server.



C. Configure Host Network Hardware

A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use for access to storage and network connectivity. To manage the host, a datacenter within a vCenter Server is installed and configured to point to all host machines within the vSphere environment. The virtual networking components provided by VMware makes it possible to create sophisticated virtual networks. The virtual networks are connected to one or more external networks or they may run entirely on the host computer.

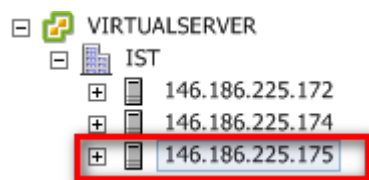
Setting up networking components for the penetration virtual lab is a straightforward process. Therefore, it's an important step that must be done properly to avoid network errors in the penetration lab.

A. Creating a Virtual Switch (vSwitch)

A vSwitch represents networking entities connecting virtual machines in a virtual network. The vSwitch is fully virtual, and can be connected to a NIC (Network Interface Card) on the host machine. The VMware Virtual Switch is a switching fabric built into the VMware infrastructure (ESX or ESXi) that allows the ability to network the Virtual Machines (VMs). vSwitch behaves much like a physical switch and will automatically detect which virtual machines are connected and route the traffic either to other virtual machines using the VMkernel, or the physical network using a physical Ethernet port. A single virtual machine will use one port on the vSwitch.

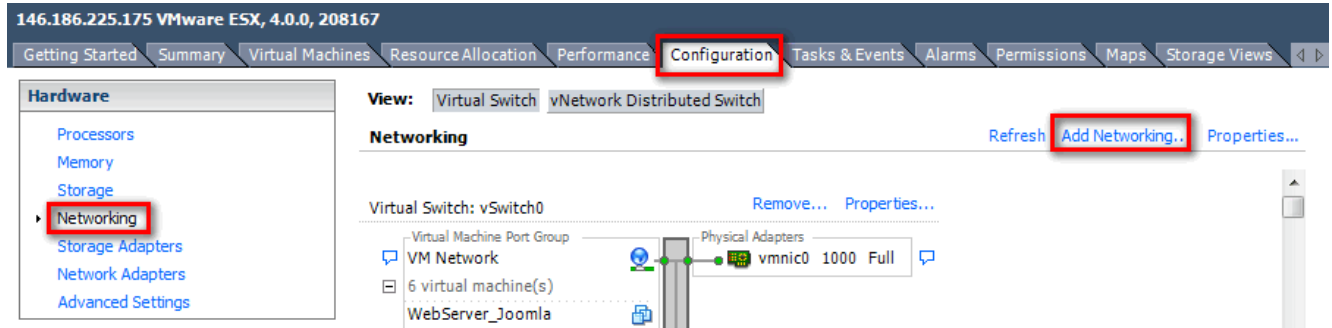
To begin, follow the steps below to create a vSwitch and assign key configuration properties:

1. Select the host machine you want to install the vSwitch.

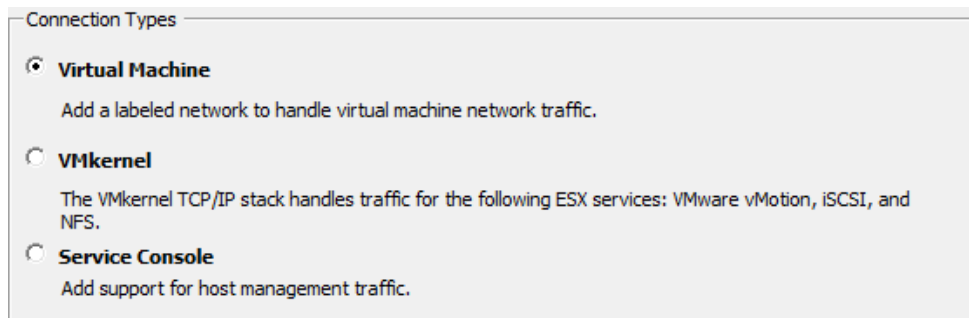


Collaborative Virtual Computer Laboratory
Penn State Berks

2. Select the **configuration tab**, located on the right window pane, and navigate to Networking. Any current networking configurations will be displayed.
3. Click the **Add Networking** link to create a new virtual switch.

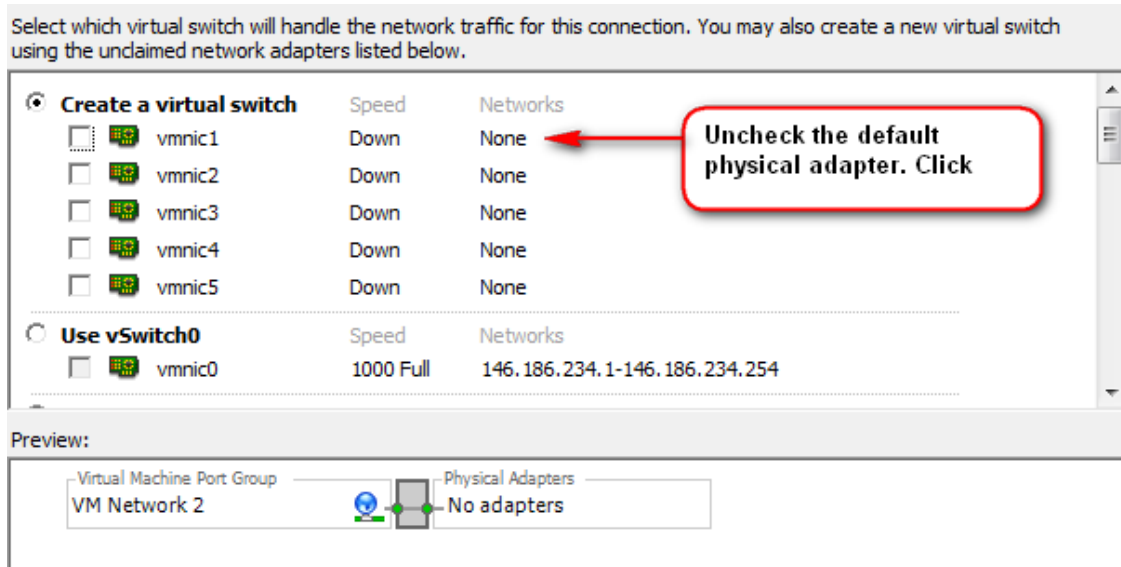


4. Next, a network wizard dialog window will be displayed. Three options will be presented. Choose the default option, “**Virtual Machine**,” which allows you to add a labeled network for virtual machine traffic.
5. Click **next** to continue.



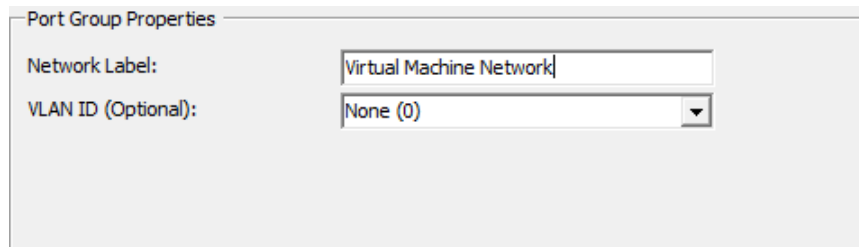
6. Next, select the network type. Select “**Create a virtual switch.**” A new vSwitch can be created with or without Ethernet Adapters assigned to it.
 - a. Access to the Physical Adapter is not required. Uncheck the default physical adapter if one is selected.
7. Click **next** to continue.

Collaborative Virtual Computer Laboratory Penn State Berks



Next, configure the Port Group properties. The Port Group properties section allows you to configure the network label. This is used to identify the network and will be used by the virtual machines to associate itself with that specific network.

8. Under **Network Label** text box, type the name of the network.
9. Leave **VLAN ID** with default option "None (0)."
10. Click **next** to continue.



Once you're done configuring the vSwitch, click **Finish** to create it. The new vSwitch will now be available for use.

D. Create a Virtual Machine

You can use several methods to create virtual machines to add to your inventory. You can create a new virtual machine, convert a physical computer to a virtual machine, deploy from a template, or clone an existing virtual machine. The vSphere client provides a simple and flexible user interface from which you can create virtual machines. A wizard guides you through the steps to produce a complete and working virtual machine.

Collaborative Virtual Computer Laboratory
Penn State Berks

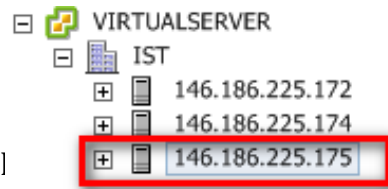
When you create a virtual machine, it's created on the host you select, the virtual machine runs on that host and uses that host's resources. You can move virtual machines from one host to another within the same datacenter.

A. Create The Host Virtual Machine for the Ubuntu Gateway/DHCP Server

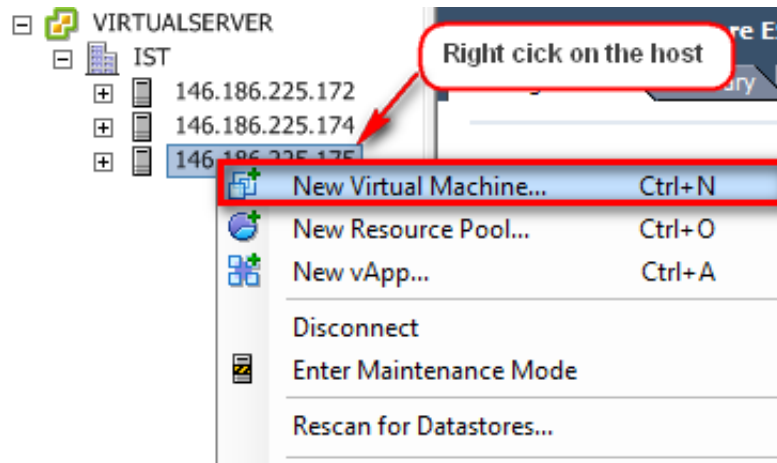
Creating a virtual machine allows you to customize options such as number of processors, memory, network connections, and storage. In this activity, you will create one ubuntu server, install three network adapters, and customize additional settings.

To begin, follow the steps below:

1. To create a new virtual machine, **select the host** or cluster in the inventory you want to run the new virtual machine.



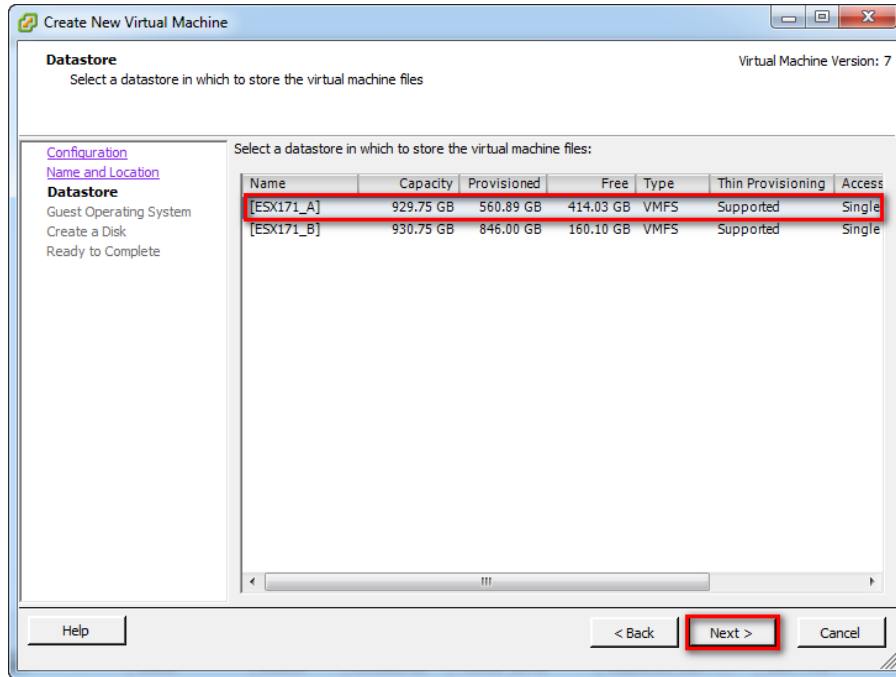
2. Right click the | **machine.**



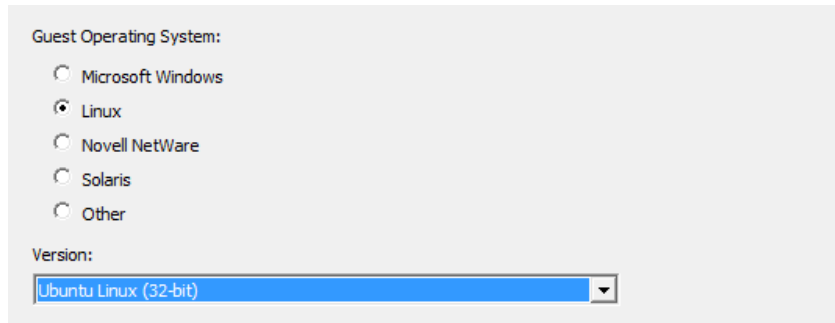
Next, the wizard to create a new virtual machine dialog box will be displayed.

3. For the configuration settings, select **Typical** and click **next**.
4. Next, you will name your virtual machine. For this activity, the name of the virtual machine is **UbuntuServerBT1**. Click **next**.
5. Select a Datastore in which to store the virtual machine files. For this activity, the name of the datastore is **ESX171_A**. Click **next**.

Collaborative Virtual Computer Laboratory Penn State Berks

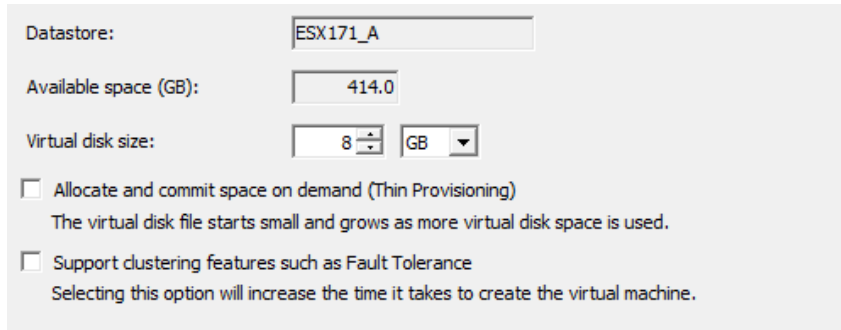


- Next, you will select the guest operating system. For this activity, we are creating an Ubuntu server virtual machine; therefore, the operating system will be **Linux** and version **Ubuntu Linux (32-bit)**. Click **Next**.



- The following screen will allow you to create a disk for your virtual machine. For this activity, leave the default options as is (the default should look like the follow image below). The settings for this section can be changed per your need and requirements. When done, click **next**.

Collaborative Virtual Computer Laboratory Penn State Berks



Datstore: ESX171_A

Available space (GB): 414.0

Virtual disk size: 8 GB

Allocate and commit space on demand (Thin Provisioning)
The virtual disk file starts small and grows as more virtual disk space is used.

Support clustering features such as Fault Tolerance
Selecting this option will increase the time it takes to create the virtual machine.

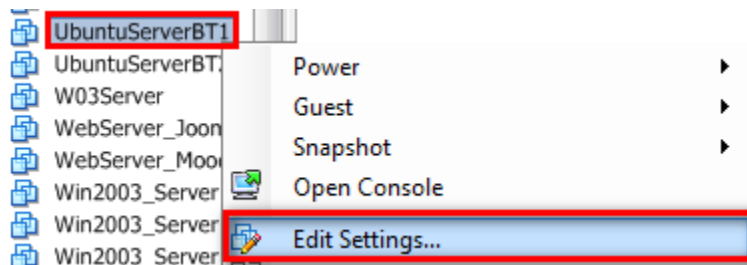
8. Finally, the next screen will display the final summary of the new virtual machine. If everything is correct, click **next**.

The vSphere Client software will now create the virtual machine. The next step is to install the Ubuntu server operating system.

A.1. Configuring the Virtual Machine

Prior to installing the operating system, follow the configuration steps below:

1. Locate new virtual machine created on the inventory.
2. Right click on the selected machine, and select **Edit Settings** to open the Edit Settings dialog box.

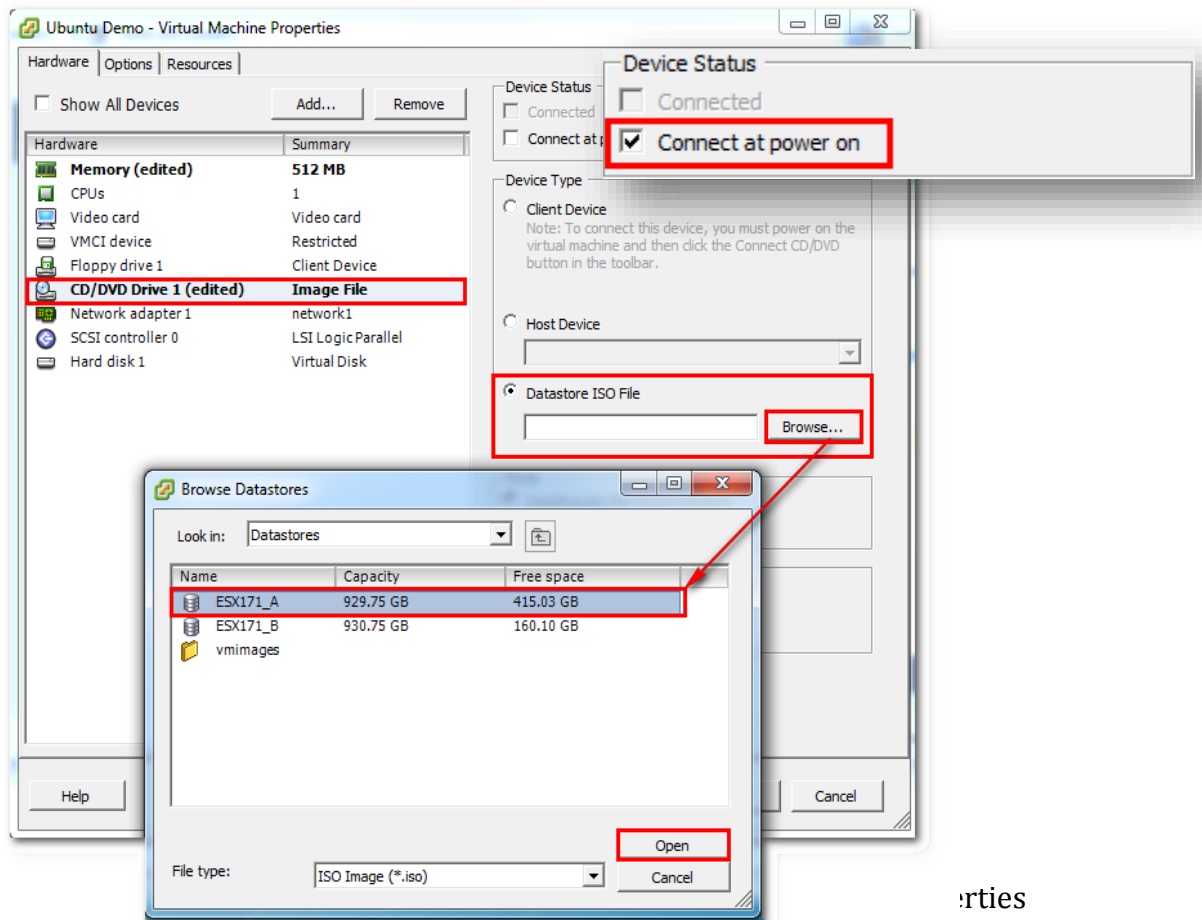


On the **Hardware** tab, you can change the settings of the machine hardware for the specific settings required to handle the operating system. For this activity, the following changes will be made:

3. Select **Memory**, change the memory configurations to the size you prefer to have. For this activity, the memory size will be changed to **512 MB**.
4. Next, leave the default configurations for **CPU, Video Card, VMCI device, and Floppy drive1** hardware devices. You can change the settings if needed to the specific requirements you are looking to have.
5. Next, select **CD/DVD** drive. We will have the virtual machine connect to the datastore ISO file to install the operating system.

Collaborative Virtual Computer Laboratory
Penn State Berks

- To select the datastore ISO file, select the **Datastore ISO file** device type and click **Browse**.
- The Browse Datastore dialog box will be displayed; select the datastore the ISO file is stored in and locate the file.
- For both the Datastore ISO file and Host Device options, check the **Connect to Power On** checkbox above



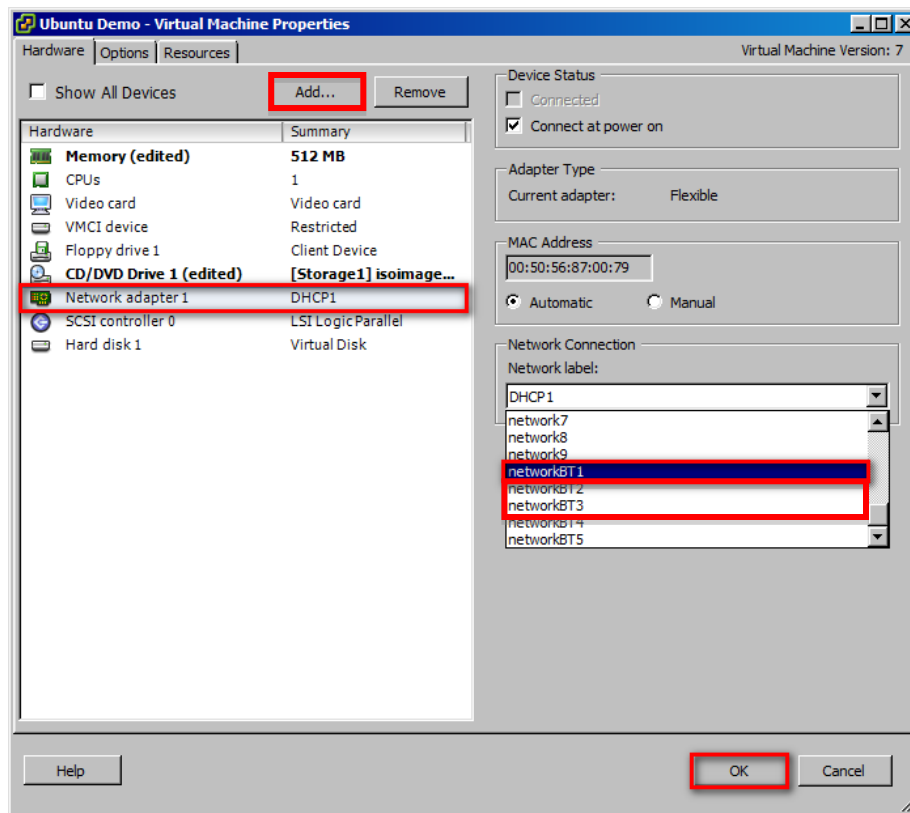
9. Wh
dia

rties

- Next, select **Network adapter**. Under network connections, select the name of the first network adapter that will be included on this server. For this activity, we want to include three network adapters. The first network adapter will be the private network for the two servers and target PCs. The remainder networks (network adapter 2 and 3) will be used for the BackTrack OS (attacker machines). For this activity, I selected **networkBT1** for the first network adapter, **networkBT2** for the second adapter, and **networkBT3** for the third adapter.

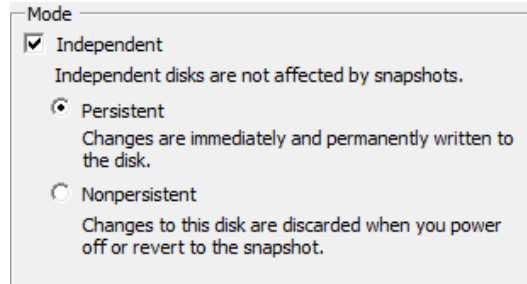
Collaborative Virtual Computer Laboratory
Penn State Berks

- 10.1. To add the second and third NIC card, click on the Add button.
- 10.2. Select Ethernet Adapter, and click Next.
- 10.3. Select an adapter type from the drop-down menu.
- 10.4. In the Network connection panel, select a named network with a specified label.
- 10.5. To connect the virtual NIC when the virtual machine is powered on, select Connect at power on.
- 10.6. Click Next.
- 10.7. Review your selections and click Finish.
- 10.8. Click OK to save your changes and close the dialog box.
- 10.9. Next, repeat the steps for the third NIC adapter.



11. Next, select **Hard Disk**. We want to make this virtual machine persistent. This means the changes are immediately and permanently written to this disk. On the Select mode section, check **Independent** checkbox and select the **Persistent** radio button.

Collaborative Virtual Computer Laboratory Penn State Berks



12. Click **OK** to complete the virtual machine properties.

VMware Client will now reconfigure your Virtual Machine

A.2. Install the Ubuntu Operating System

A new virtual machine is like a physical computer with a blank hard disk. After you create the new virtual machine, you need to install the guest operating system. You can also change the settings of the virtual machine at any time.

Installing a guest operating system on a virtual machine is essentially the same as installing it on a physical computer. You must have a CD-ROM or ISO image containing the installation files from an operating system vendor. As with physical computers, a separate operating system license is required for each installation.

For this activity, the operating system used is an open source OS; therefore, it's free. To download the ISO for the Ubuntu Server copy and paste the following link to your browser. <http://www.ubuntu.com/download/server/download> after downloading the ISO, store the file on the vSphere datacenter. For this activity, the ISO was already downloaded and stored on the datacenter.

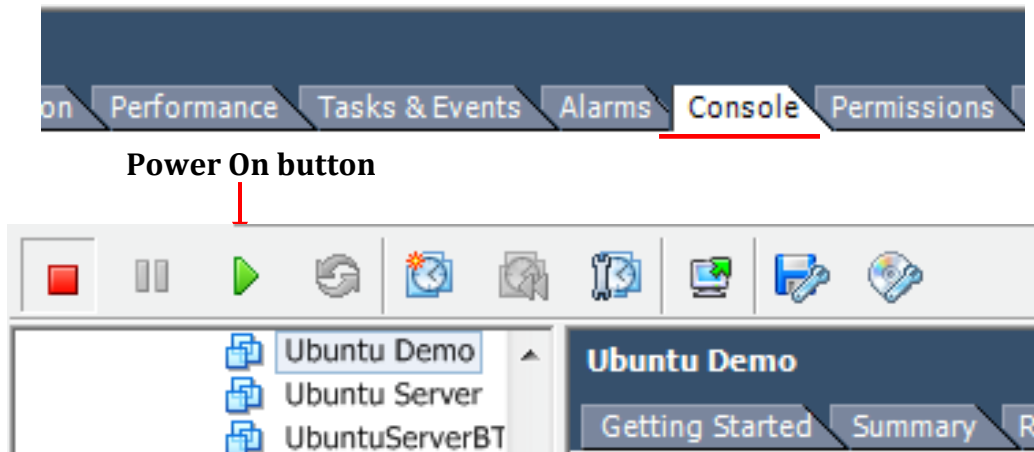
A.3. Install ISO File for Virtual Machine

The next steps will allow you to power on the virtual machine and install the ISO file containing the operating system. The power state of a virtual machine indicates whether the virtual machine is active and functional. A virtual machine has several power states, but the three basic states are: On, Off, and Suspend.



Collaborative Virtual Computer Laboratory
Penn State Berks

1. To power on the virtual machine, select the virtual machine you want to power on.
2. On the **console** tab, click on the **Power On** toolbar button to power on the virtual machine.



3. After the virtual machine is powered on, install the guest operating system as you would on any other computer.

Note: Since the VMware Tools are not installed yet, the cursor will stick. To release cursor, press Ctrl + Alt on your keyboard.

A.4. VMware Tools

After the guest operating system is installed and running, install VMware Tools. This improves the performance of the virtual machine. VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine. It's vital to install the VMware tools in the guest operating system. Although the guest operating system can run without VMware tools, you lose important functionality and convenience. When you install VMware Tools, you install the VMware Tools service and a set of VMware device drivers that enhance display, networking, SCSI, memory control, I/O, and mouse support.

To install VMware Tools, follow the steps below:

1. Select the virtual machine you have installed the guest operating system on.
2. Click on the **Console** tab on the right.
3. Choose **Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools**

4. Follow the instructions in the installation wizard

If the wizard does not automatically appear, open the CD-ROM drive in the guest operating system labeled VMware Tools and run the setup application.

A.5. Configure Networking Settings for the Ubuntu Server

Ubuntu ships with a number of graphical utilities to configure your network devices. This document will focus on managing your network on the command line. We will begin with verifying the Ethernet Interface, which are identified by the system using the naming convention of ethX, where X represents a numerical value. The first Ethernet interface is typically identified, as eth0, the second as eth1 and all others should move up in the numerical order. For this activity, our servers will have the following Ethernet Interface values:

First Ubuntu Server:

- eth12
- eth13
- eth15

Second Ubuntu Server:

- eth17
- eth18
- eth19

For now, we will begin with the first Ubuntu Server. To verify the Ethernet Interfaces are correct, follow the steps below:

1. Log into the Ubuntu Server VM
2. Open the terminal window to use the command line. Go to **Accessories > Terminal**
3. Login in as a root user by typing the following command:

```
sudo -s
```

4. Type the following command line:

```
ifconfig -a | grep eth
```

5. To configure your system to use a static IP address assignment, **add** the static method to the inet address family statement for the eth12 interface in the file **/etc/network/interfaces**. To edit the file, type the following commands:

```
auto lo
iface lo inet loopback

auto eth12
iface eth12 inet static
```

Collaborative Virtual Computer Laboratory
Penn State Berks

```
address 10.0.0.1  
netmask 255.255.255.0  
gateway 10.0.1.1
```

6. Next, save the document and restart networking services by running the following command:

```
/etc/init.d/networking restart
```

7. Next, confirm the ip address has changed:

```
ifconfig
```

A.6. Configure the Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) is a network service that enables host computers to be automatically assigned settings from a server as opposed to manually configuring each network host. Computers configured to be DHCP clients have no control over the settings they receive from the DHCP server, and the configuration is transparent to the computer's user.

The following steps will install the DHCP and configure the proper settings for the Ethernet Interfaces using the DHCP settings.

1. To install the DHCP, run the following command line:

```
sudo apt-get install dhcp3-server
```

Note: Don't be alarmed if the startup fails; that's because you haven't configured it yet.

2. Edit the DHCP server configuration:

```
sudo nano /etc/dhcp3/dhcp.conf
```

3. Start the DHCP server (it should now start without problems):

```
sudo /etc/init.d/dhcp3-server start
```

Collaborative Virtual Computer Laboratory
Penn State Berks

Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irrtt	Iface
192.168.4.0	192.168.4.1	255.255.255.0	UG	0 0		0	eth15
192.168.3.0	192.168.3.1	255.255.255.0	UG	0 0		0	eth15
192.168.2.0	0.0.0.0	255.255.255.0	U	0 0		0	eth13
192.168.1.0	0.0.0.0	255.255.255.0	U	0 0		0	eth12
169.254.0.0	0.0.0.0	255.255.0.0	U	0 0		0	eth12
10.0.0.0	0.0.0.0	255.0.0.0	U	0 0		0	eth15
0.0.0.0	10.0.0.1	0.0.0.0	UG	0 0		0	eth15
0.0.0.0	192.168.2.1	0.0.0.0	UG	0 0		0	eth13
0.0.0.0	192.168.1.1	0.0.0.0	UG	0 0		0	eth12

Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irrtt	Iface
192.168.4.0	0.0.0.0	255.255.255.0	U	0 0		0	eth19
192.168.3.0	0.0.0.0	255.255.255.0	U	0 0		0	eth18
192.168.2.0	192.168.2.1	255.255.255.0	UG	0 0		0	eth17
192.168.1.0	192.168.1.1	255.255.255.0	UG	0 0		0	eth17
169.254.0.0	0.0.0.0	255.255.0.0	U	0 0		0	eth17
10.0.0.0	0.0.0.0	255.0.0.0	U	0 0		0	eth17
0.0.0.0	192.168.4.1	0.0.0.0	UG	0 0		0	eth19
0.0.0.0	192.168.3.1	0.0.0.0	UG	0 0		0	eth18
0.0.0.0	10.0.0.2	0.0.0.0	UG	0 0		0	eth17