Ethical Hacking
Pod Installation and Configuration Guide

Document Version: 2018-12-14

Contents

1   Introduction

This document provides detailed guidance on performing the installation and configuration of the Ethical Hacking pod on the NETLAB+ system.

1.1   About the Ethical Hacking Course

The Ethical Hacking course equips trainees with the knowledge and understanding of methods, tools and techniques used by hackers to gain access to systems. Understanding the methods, tools and techniques used to penetrate a system is vital to knowing how to thwart such attacks and prevent compromising systems to unintended users.

1.2   Using NETLAB+ to Deliver Ethical Hacking

NDG has partnered with the National Information, Security & Geospatial Technologies Consortium (NISGTC) to enable NETLAB+ support of the Ethical Hacking course. The use of NETLAB+ provides an enormous opportunity for educational organizations seeking a scalable, cost effective solution to offer access to the technology required for the NISGTC program, which introduces students to Ethical Hacking technologies and equips them with valuable security skills.

1.3   Introducing the Ethical Hacking Pod

The Ethical Hacking pod is a 100% virtual machine pod consisting of 8 virtual machines. Linked together through virtual networking, these 8 virtual machines provide the environment for a student or team to perform the Ethical Hacking labs.
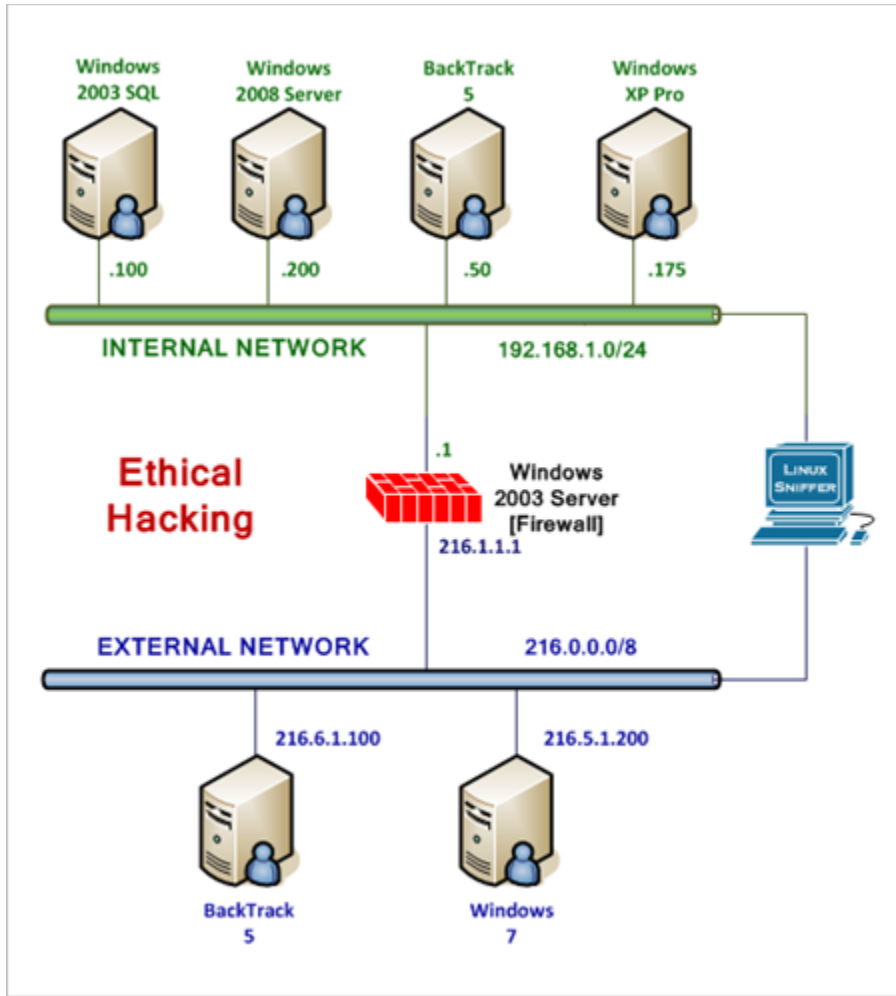
Image Name	Virtual Machine Name
EH_Master_VM_1	Windows 2003 SQL
EH_Master_VM_2	Windows 2008 Server
EH_Master_VM_3	Backtrack 5 (Internal)
EH_Master_VM_4	Windows XP Pro
EH_Master_VM_5	Windows 2003 Firewall
EH_Master_VM_6	Linux Sniffer
EH_Master_VM_7	Backtrack 5 (External)
EH_Master_VM_8	Windows 7

2   Planning

This guide provides specific information pertinent to delivering the Ethical Hacking course. The *NETLAB+ Remote PC Guide Series* provides the prerequisite guidance for setting up your VMware infrastructure, including:

- An introduction to virtualization using NETLAB+.
- Detailed setup instructions for standing up VMware vCenter and VMware ESXi.
- Virtual machine and virtual pod management concepts using NETLAB+.

This document assumes that you have set up virtual machine infrastructure in accordance with the *NETLAB+ Remote PC Guide Series*. The planning information below refers to specific sections in the Remote PC Guide when applicable.

2.1   Ethical Hacking Environment

The following diagram depicts four major components that make up the Ethical Hacking training environment.
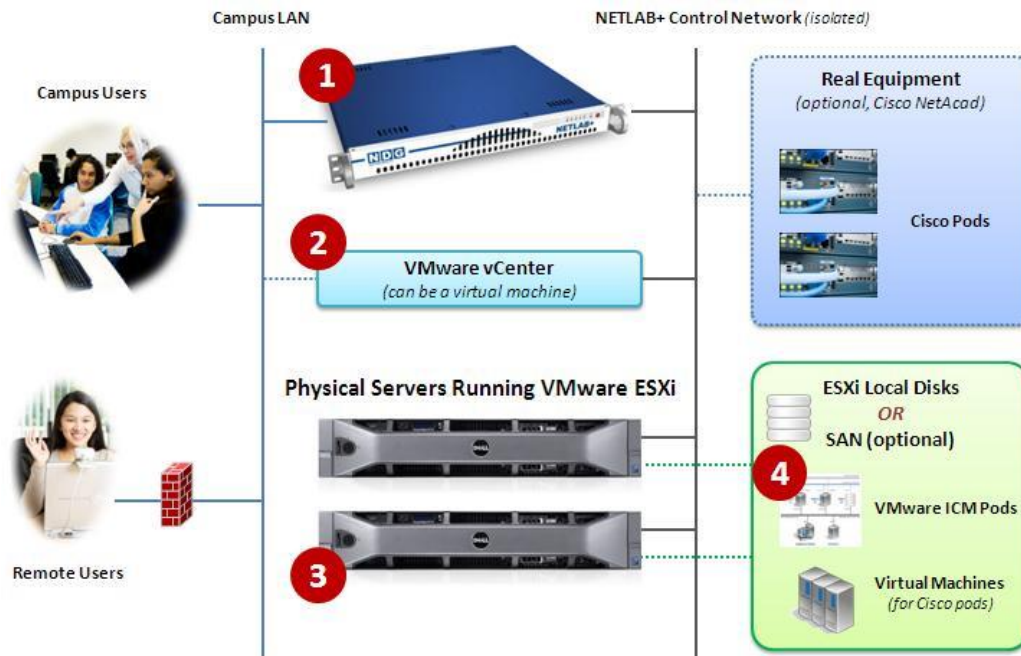
1. The NETLAB+ server provides the user interface for student and instructor access, an interface to manage virtual machines, and software features to automate pod creation.   This document assumes you have already setup your NETLAB+ server.

2. VMware vCenter is used to manage your physical VMware ESXi servers, to create virtual machines, and to take snapshots of virtual machines. NETLAB+ communicates with vCenter to perform automated tasks and virtual machine management.

3. Physical VMware ESXi servers host the virtual machines in your pods. The host server's capabilities are discussed in section 2.5.

4. The Ethical Hacking pod consists of 8 virtual machines that reside on your ESXi host(s).

2.2   Setup Tasks

The following is a summary of the setup tasks in this document.

1. Obtain virtual machine packages (OVF/OVA).
2. Deploy virtual machines for the Master Pod.
3. Attach virtual machines to NETLAB+.
4. Replicate Ethical Hacking pods using the pod cloning feature.
5. Assign Ethical Hacking pods to students or instructors.

2.3   Ethical Hacking Pod Creation Workflow

The following list is an overview of the Ethical Hacking pod setup process.

1. The Ethical Hacking virtual machine packages are distributed by CSSIA.
2. Master VMs are created from the deployed virtual machines. The master VMs are added to a Master pod. A *Golden_Snapshot* of the Master pod is taken, which becomes the foundation to clone Ethical Hacking User pods.
3. The NETLAB+ pod cloning feature is used to quickly create copies from the Ethical Hacking Master Pod on the first VMware host.
4. A full replica of the Ethical Hacking Master Pod on Host A is made on Host B, using the NETLAB+ Pod Cloning Feature.
5. The cloning feature is used to quickly create Ethical Hacking pods from the Ethical Hacking Master Pod on Host B.

2.4   Pod Resource Requirements

The Ethical Hacking course will consume 27 GB of storage per each user pod instance.

Details of the storage requirements for each of the lab virtual machines are provided in the tables below.

Virtual Machine	Initial Master Pod (using full clones) GB
Windows 2003 SQL	3.2
Windows 2008 Server	6.1
Backtrack 5 (Internal)	11.3
Windows XP Pro	3.2
Windows 2003 Firewall	2.9
Linux Sniffer	7.7
Backtrack 5 (External)	11.3
Windows 7	9.1
Total Recommended	**27**

2.5   ESXi Host Server Requirements

The number of **active** pods that can be used simultaneously depends on the NETLAB+ product edition and the number of VMware ESXi host servers meeting the hardware requirements specifications (see link below).

For current ESXi server requirements refer to the following URL:
http://www.netdevgroup.com/support/remote_pc.html#vm_host_server_specifications.

2.6 NETLAB+ Requirements

Installation of Ethical Hacking pods as described in this guide requires that your NETLAB+ system is equipped with NETLAB+ version 2011.R5 or later.

For additional information regarding NETLAB+ requirements, please see: http://www.netdevgroup.com/content/cybersecurity/requirements/

Please also refer to: *NETLAB+ Remote PC Guide Series*

2.7 Software Requirements

For the purpose of software licensing, each virtual machine is treated as an individual machine, PC or server. Please refer to the specific vendor license agreements (and educational discount programs, if applicable) to determine licensing requirements for your virtual machines' software, operating system and applications.

The virtual infrastructure software required for standing up this pod is in the following table.

Virtual Infrastructure Requirements	
Software	**Version**
vSphere ESXi	4.1
vCenter Server	4.1

The pod software requirements as shown in the following table lists the licensed software that is required for virtual machines inside the Ethical Hacking pod. Your organization needs to be a member of the vendor programs listed in the source column to obtain and use the licenses appropriately.

Pod Software Requirements		
Software	**Version**	**Source**
Windows Server	2008 R2	Dreamspark
Windows Server	2003	Dreamspark
Windows XP	SP3	Dreamspark
Windows 7	Professional x86	Dreamspark

2.8   Networking Requirements

To accommodate the movement of large VMs, OVF/OVAs and ISO disk images from one host to another, a Gigabit Ethernet switch is recommended to interconnect your NETLAB+, vCenter Server system and ESXi host systems.

Two standard networking models are used to interconnect your servers, which are described in detail in the *Networking Models* section of the *Remote PC Guide Series – Volume 1*.

3   Obtaining Software and Licenses

3.1   Downloading OVF Files

The virtual machines are made available as Open Virtualization Format (OVF) or Open Virtualization Archive (OVA) files. These files are available for download from CSSIA.

To request access to the preconfigured virtual machine templates from CSSIA:

1. Go to the CSSIA Resources page: http://www.cssia.org/cssia-resources.cfm.
2. Select **VM Image Sharing Agreement – Image Sharing Agreement**.
3. Select **VM Image Sharing Agreement** to open the request form.
4. Complete and submit your access request by following the instructions on the request form.
5. CSSIA will email a link, along with a username and password to access the download server. Access to the download server is provided only to customers who are current with their NETLAB+ support contract and are participants in the appropriate partner programs (i.e. Cisco Networking Academy, VMware IT Academy, and/or EMC Academic Alliance).
6. Once access to the download server has been established, the virtual machines can be deployed directly to the vCenter Server by clicking on File > Deploy OVF Template in the vClient window and copying the link into the location field.
7. The deployment will start after the username and password are entered.
8. Each virtual machine is deployed individually.

## 4   Ethical Hacking Master Pod Configuration

4.1   Deploying Virtual Machine OVF/OVA Files

The OVF/OVA files that you downloaded from CSSIA must be deployed to your host server.

1. Open the vClient on your administration machine where you downloaded the files from NDG. Connect to your vCenter Server.
2. Select **Hosts and Clusters** in the address bar.
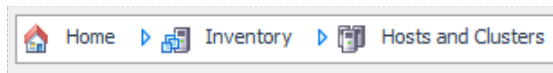
3. Click on the first ESXi Host Server.
4. Click on **File -> Deploy OVF Template.**
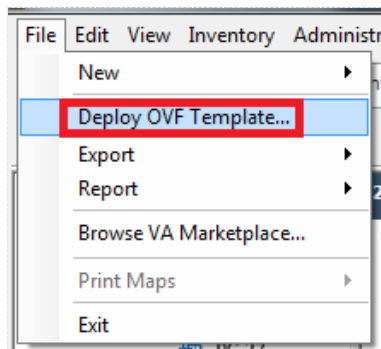
5. Click on **Browse** and locate the OVF/OVA files you downloaded from CSSIA. Click **Next** to continue.
6. On the OVF Template Details window, click **Next.**
7. On the Name and Location window, change the name to **Ethical_Hacking_Master_01** (Increment the number to correspond to the virtual machine number). Click **Next.**
8. On the Datastore window, select the appropriate **datastore** for your system and click **Next**.
9. On the Disk Format window, select **Thin provisioned format** and click **Next.**
10. On the Network Mapping window, select **SAFETY NET**. Click **Next**.

> If SAFETY NET is not available, please refer to the *NETLAB+ Remote PC Guide - Volume 2* for the installation and configuration of the safe staging network.
>
> Network mapping is handled automatically by the NETLAB+ system during pod creation.

11. If deploying virtual machine #2, #3 or #7 use the MAC addresses in the following table and statically apply them to the NIC of the associated virtual machine.

Virtual Machine	MAC Address
2	00:50:56:3f:2e:1d
3	00:50:56:1b:2c:3d
7	00:50:56:9d:01:79

12. To change the MAC address, select the Network adapter and click on the **Manual** radio button and type in the MAC Address from the table above in the MAC **Address** text box.
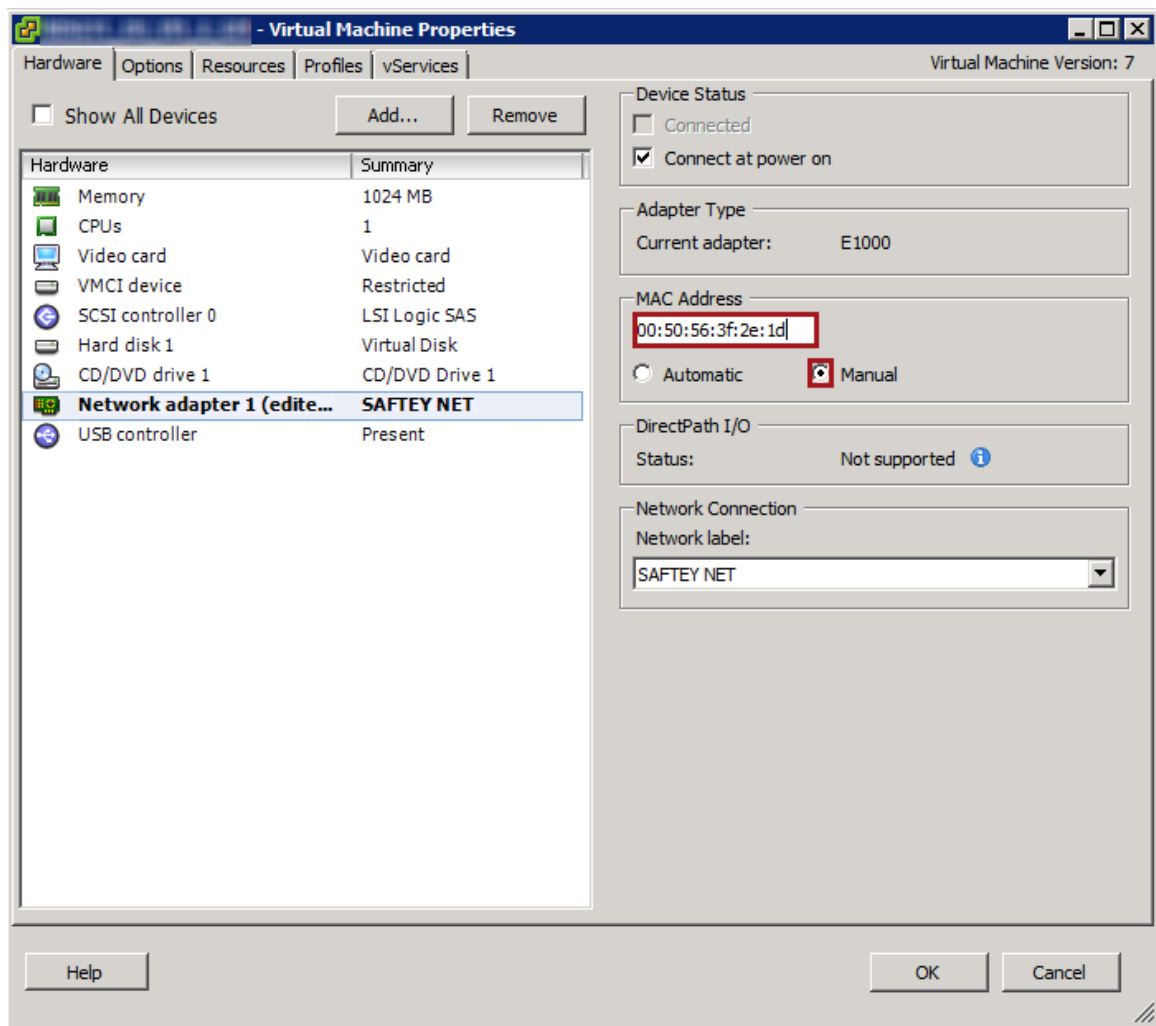
13. On the Ready to Complete window, confirm the information and click **Finish**.
14. vCenter will begin deploying the virtual machine. This may take some time depending on the speed of your connection, HDDs, etc. When completed, click on **Close**.
15. Repeat steps 4 – 14 for each of the downloaded files then continue to the next section.

4.2   Modify and Activate Virtual Machines

Once the virtual machines are imported onto the host, you will need to activate Microsoft Windows on them. This needs to be done prior to snapshot, pod assignment and cloning.

For each of the Windows machines you will need to power them on in vCenter. While accessing them via remote console you can follow the steps offered in the Microsoft KB articles listed below to activate your Microsoft software:

Windows XP: http://support.microsoft.com/kb/307890
Windows 2008:   http://technet.microsoft.com/en-us/library/ee355153.aspx

Listed below are the images that may require activation once the OVF is deployed.

- Windows 2003 SQL
- Windows 2008 Server
- Windows XP Pro
- Windows 2003 Firewall
- Windows 7

The following table contains the passwords required to access the virtual machines for account activation.

Firewall (Windows 2003 Server)	192.168.1.1
Administrator Password	ethical
Windows 2008 Server	192.168.1.200
Admin Password	none
Internal Windows XP	192.168.1.175
Windows XP **hacker** user password	toor
Windows 2003 Exchange SQL	192.168.1.100
Administrator password	P@ssw0rd

4.3 NETLAB+ Virtual Machine Infrastructure Setup

The NETLAB+ Virtual Machine Infrastructure setup is described in the following sections of the *Remote PC Guides for NETLAB+*:

- *Registering a Virtual Datacenter in NETLAB+*
- *Adding ESXi hosts in NETLAB+*
- *Proactive Resource Awareness*

It is important to configure Proactive Resource Awareness to maximize the number of active pods per physical ESXi host.

4.4 NETLAB+ Virtual Machine Inventory Setup

This section will guide you in adding your templates to the Virtual Machine Inventory of your NETLAB+ system.

1. Login into your NETLAB+ system using the administrator account.
2. Select the Virtual Machine Infrastructure link.

Virtual Machine Infrastructure

3. Click the Virtual Machine Inventory link.

Virtual Machine Inventory

Import, clone, and manage the inventory of virtual machines to be used with NETLAB+.
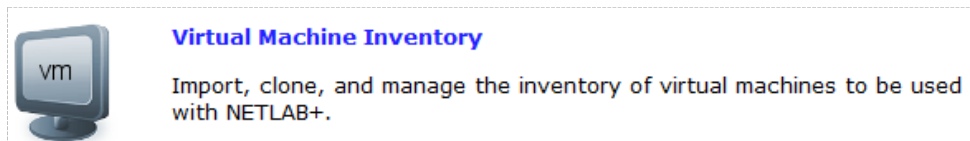
4. Click the Import Virtual Machines button.

5. Select the check box next to your Ethical Hacking virtual machines and click Import Selected Virtual Machines.
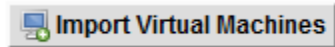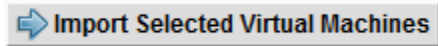

6. When the Configure Virtual Machines window loads, you can set your virtual machine parameters.
   a. Check the drop down box for the correct operating system for each imported virtual machine.
   b. Add any comments for each virtual machine in the box to the right.
   c. Verify your settings and click Import Selected Virtual Machines.
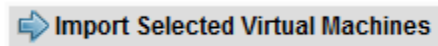
   d. Click OK when the virtual machines have finished loading.
   e. Verify that your virtual machines show up in the inventory.

For additional information, please refer to the *NETLAB+ Remote PC Guide - Volume 3*.

4.5 Install the Master Ethical Hacking Pod

This section will assist you in adding the Ethical Hacking Pod to your NETLAB+ system.

1. Login into NETLAB+ with the administrator account.
2. Select the **Equipment Pods** link.

3. Create a new pod by scrolling to the bottom and clicking the **Add a Pod** button.
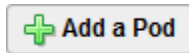
4. On the New Pod Wizard page, click **Next**.
5. Then select the Ethical Hacking pod radio button and click **Next**.
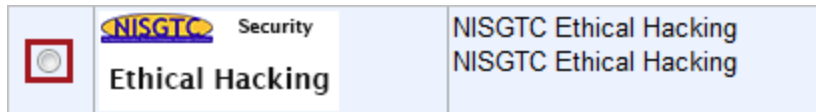
6. Select a Pod ID and click **Next**.

It is best practice to use a block of sequential ID numbers for the number Ethical Hacking pods you are going to install. The Pod ID number determines the order in which the Ethical Hacking pods will appear in the scheduler.

7. Type in **Ethical_Hacking_Master** for the Pod Name and click **Next**.
8. To finalize the wizard click **OK**.

For additional information, please refer to the *NETLAB+ Administrator Guide*.

4.6 Create Snapshots for the Ethical Hacking Master Virtual Machines

In order to proceed with pod cloning, snapshots must be created for the Ethical Hacking Master virtual machines.

Verify that all VMs are powered off before taking snapshots.

1. Open the vClient on your management workstation. Connect to your vCenter Server.
2. Select **Hosts and Clusters** in the address bar.

3. Right-click on each virtual machine and select **Snapshot > Take Snapshot**.
4. Enter **Golden_Master** as the Snapshot Name.
5. Enter a description. It is a good idea to include the date in the description for later reference.
6. Click **OK**.
7. Repeat Steps 3-6 for the remaining virtual machines in the pod.
8. When all tasks have completed, log out of the vClient software.

4.7 Update the Ethical Hacking Master Pod
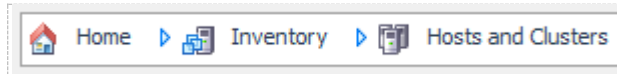
1. Update Ethical Hacking Master Pod on your NETLAB+ system.
   a. Login into NETLAB+ with the administrator account.
   b. Select the **Equipment Pods** link.

2. Click on the Magnifying Glass icon next to VMV-ESXi. Please note that your PC IDs will not match the graphic below.

3. Click on Modify PC Settings
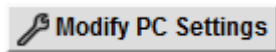
4. Change the PC Type drop down box to **Use Virtual Machine Inventory**.
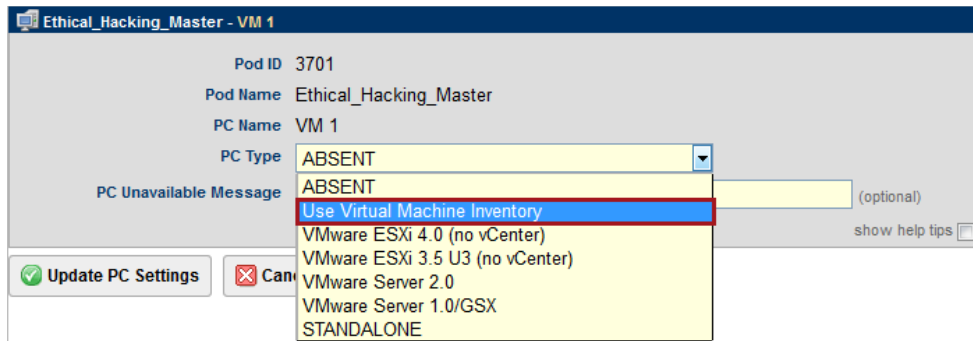
5. In the Base Virtual Machine window, select your Ethical Hacking virtual machine to associate with the spot held for it in the pod.
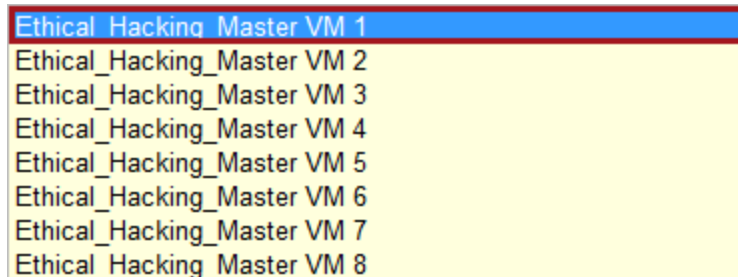
6. Update **Base Snapshot** to your *Golden_Master* snapshot.

7. Change **Shutdown Preference** to the associative entry from the table below:

Virtual Machine	Shutdown Preference
Windows 2003 SQL	Graceful Shutdown from Operating System
Windows 2008 Server	Graceful Shutdown from Operating System
Backtrack 5 (Internal)	Graceful Shutdown from Operating System
Windows XP Pro	Graceful Shutdown from Operating System
Windows 2003 Firewall	Graceful Shutdown from Operating System
Linux Sniffer	Graceful Shutdown from Operating System
Backtrack 5 (External)	Graceful Shutdown from Operating System
Windows 7	Graceful Shutdown from Operating System

8. Review the information on the screen and click **Update PC Settings**.
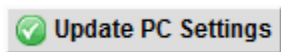
9. Click on **Show Pod**.
10. Repeat steps 2-9 for each of the Ethical Hacking virtual machines.

Make sure the pod status is **Offline** prior to continuing. The cloning process requires the pod be offline, and since this is our master pod used for cloning other pods with, we will keep it offline to create the instructor and student pods.

5　Pod Cloning

This section will help you create multiple Ethical Hacking student pods. The following sections describe the NETLAB+ pod cloning feature used to create student pods on one or two host systems.

5.1　Linked Clones and Full Clones

NETLAB+ can create *linked clones* or *full clones*.

- A **linked clone** (or linked virtual machine) is a virtual machine that shares virtual disks with the parent (or master) virtual machine in an ongoing manner. This conserves disk space, and allows multiple virtual machines to use the same software installation. Linked clones can be created very quickly because most of the disk is shared with the parent VM.

- A **full clone** is an independent copy of a virtual machine that shares nothing with the parent virtual machine after the cloning operation. Ongoing operation of a full clone is entirely separate from the parent virtual machine.

5.2　Creating User Pods on the First Host

The following section describes how to create Ethical Hacking user pods on the same VMware Host system that holds your Master Pod's virtual machines. In this scenario, we will create linked virtual machines using the NETLAB+ pod cloning utility.

1. Login into NETLAB+ with the administrator account.
2. Select the **Equipment Pods** link.

Equipment Pods

3. Click on your Ethical Hacking Master Pod.
4. Click the Clone button to create a new pod based on the settings of this pod.
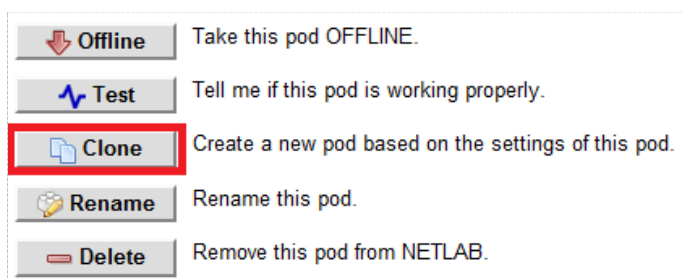
5. Select the New Pod ID. It is advised to keep the pods in numerical order. If the pod IDs are not in numerical order, they will not show up in the scheduler in numerical order.

6. Click **Next**.

7. Enter a New Pod Name. For example, **Ethical_Hacking_Pod_1.** Click **Next**.

8. When the action has finished processing, you are presented with a settings screen.

| PC Name	Source Virtual Machine	Source Snapshot	⇒	Clone Name	Clone Type	Clone Role	Runtime Host or Group	Clone Datastore	Storage Allocation
VM 1	NISGTC_EH_VM_1_GM	Golden_Master		Ethical_Hacking_Pod_1 VM 1	Linked	Normal	Host 209.114.126.6	LocalSATA	On Demand
VM 2	NISGTC_EH_VM_2_GM	Golden_Master		Ethical_Hacking_Pod_1 VM 2	Linked	Normal	Host 209.114.126.6	LocalSATA	On Demand
VM 3	NISGTC_EH_VM_3_GM	Golden_Master		Ethical_Hacking_Pod_1 VM 3	Linked	Normal	Host 209.114.126.6	LocalSATA	On Demand
VM 4	NISGTC_EH_VM_4_GM	Golden_Master		Ethical_Hacking_Pod_1 VM 4	Linked	Normal	Host 209.114.126.6	LocalSATA	On Demand
VM 5	NISGTC_EH_VM_5_GM	Golden_Master		Ethical_Hacking_Pod_1 VM 5	Linked	Normal	Host 209.114.126.6	LocalSATA	On Demand
VM 6	NISGTC_EH_VM_6_GM	Golden_Master		Ethical_Hacking_Pod_1 VM 6	Linked	Normal	Host 209.114.126.6	LocalSATA	On Demand
VM 7	NISGTC_EH_VM_7_GM	Golden_Master		Ethical_Hacking_Pod_1 VM 7	Linked	Normal	Host 209.114.126.6	LocalSATA	On Demand
VM 8	NISGTC_EH_VM_8_GM	Golden_Master		Ethical_Hacking_Pod_1 VM 8	Linked	Normal	Host 209.114.126.6	LocalSATA	On Demand

9. The three key columns for this Master Pod clone are Source Snapshot, Clone Type and Clone Role. The following settings should be applied to all 5 virtual machines:

   a. Source Snapshot should be set to the **Golden_Master** snapshot you created previously.

   b. Under Clone Type, click the dropdown menu and verify that **Linked** is selected.

   c. Under Clone Role, click the dropdown menu and verify that **Normal** is selected.

10. When you are done changing settings, Click **Clone Pod**. This should complete within a minute as we are creating linked virtual machines.

11. When the pod clone process is finished, click **OK**.

12. Now we must snapshot the virtual machines. The follow procedure needs to be done for each virtual machine in the pod.

   a. Under NETLAB+ Administration, click on the **Virtual Machine Infrastructure** icon.

   b. On the Virtual Machine Infrastructure page, click on the **Virtual Machine Inventory** hyperlink.
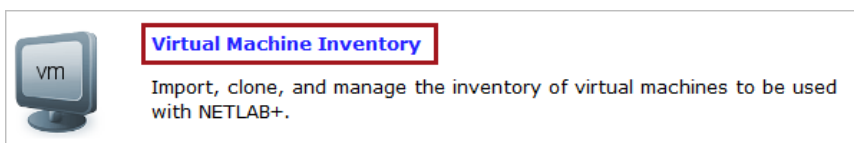
c. In the virtual machine inventory identify the virtual machines that are associated with the pod you created. Click on the **hyperlink** for the virtual machine you wish to create a snapshot on.

The name of the virtual machine is created by combining the pod name and the name of the virtual machine in the pod design.

Ethical_Hacking_Pod_1 VM 1	Windows Server 2003	Normal	NDGNL01	209.114.126.6
Ethical_Hacking_Pod_1 VM 2	Other	Normal	NDGNL01	209.114.126.6
Ethical_Hacking_Pod_1 VM 3	Linux	Normal	NDGNL01	209.114.126.6
Ethical_Hacking_Pod_1 VM 4	Windows XP	Normal	NDGNL01	209.114.126.6
Ethical_Hacking_Pod_1 VM 5	Windows Server 2003	Normal	NDGNL01	209.114.126.6
Ethical_Hacking_Pod_1 VM 6	Linux	Normal	NDGNL01	209.114.126.6
Ethical_Hacking_Pod_1 VM 7	Linux	Normal	NDGNL01	209.114.126.6
Ethical_Hacking_Pod_1 VM 8	Windows 7	Normal	NDGNL01	209.114.126.6

d. On the Showing VM form click on the **Snapshots** button.

Showing VM Ethical_Hacking_Pod_1 VM 1

|		
Virtual Machine Name	Ethical_Hacking_Pod_1 VM 1	Rename
Operating System	Windows Server 2003	
Role	🖥 Normal	Change Role
Datacenter	NDGNL01	
Runtime Host	209.114.126.6	
Host Group	n/a	
CPUs	1	
Memory (MB)	1024	
Pod ID	3701	🔍
Pod Name	Ethical_Hacking_Pod_1	🔍
PC Name	VM 1	🔍
Parent	NISGTC_EH_VM_1_GM	🔍
Parent Snapshot	Golden_Master	
Children	0	
Datacenter Unique Identifier	5010838c-1f7f-a329-c66a-b670dffa40ed	
Datacenter Storage Location	[LocalSATA] Ethical_Hacking_Pod_1 VM 1/Ethical_Hacking_Pod_1 VM 1.vmx	
Comments		

|	
🔧 Edit	Change virtual machine parameters.
📄 Clone	Clone this virtual machine.
🖥 Snapshots	Manage this virtual machine's snapshots.
🖥 Remove	Remove this virtual machine from the NETLAB+ inventory (and optionally from the datacenter).

e. A Snapshot Manager window will appear. In the Snapshot Manager window click on the **Take** button.
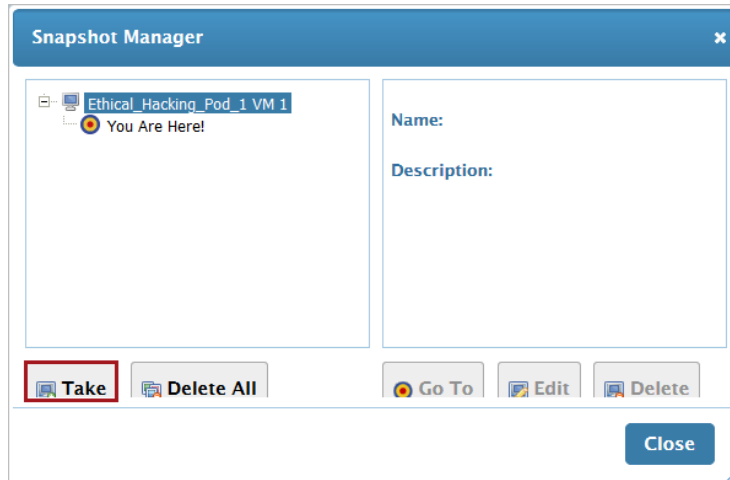
f. In the Take Snapshot popup window enter `Golden_Master` in the **Name** field, enter the *current date* in the **Description** field then click the **OK** button.
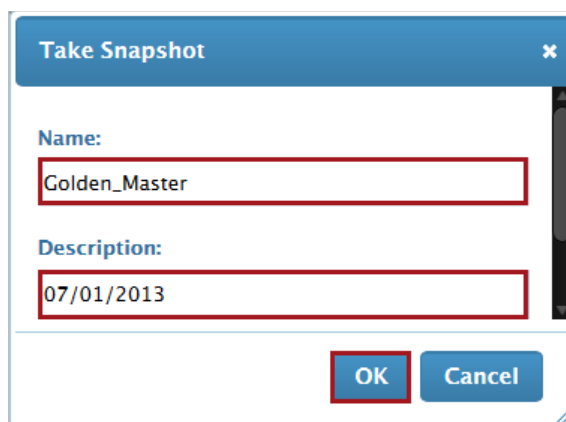
g. The snapshot is now created. Click the **Close** button in the Snapshot Manager window.

h. On the Showing VM form click the **Exit** button to return to the Virtual Machine Inventory.

13. If you want to dedicate this pod to a particular class, team, or student, use the Pod Assignment feature. For details, see the *Pod Assignment Guide*.

14. Click the **Online** Button in the Pod Management page to activate the pod.

The user pod can now be reserved. When the reservation becomes active, NETLAB+ will automatically configure virtual machines and virtual networking for your new Ethical Hacking pod.

The Golden Snapshot is the starting point for all Ethical Hacking pods. We recommend that you reserve the 1st Ethical Hacking pod and conduct some Ethical Hacking labs to make sure the Golden Snapshot is correct. You should correct any defects on the Master Ethical Hacking pod and Golden Snapshot before creating additional pods.

You may repeat the pod cloning process to create up to 15 more Ethical Hacking user pods on this host.

> **Time Saver:** If you clone the 1st Ethical Hacking user pod instead of the Master pod, the defaults will all be set correctly, and you will not have to change the Clone Type and Clone Role each time. NETLAB+ will still assume you want to link to the Master VMs as Masters are ranked higher than Normal or Persistent VMs in the default pod cloning selections.
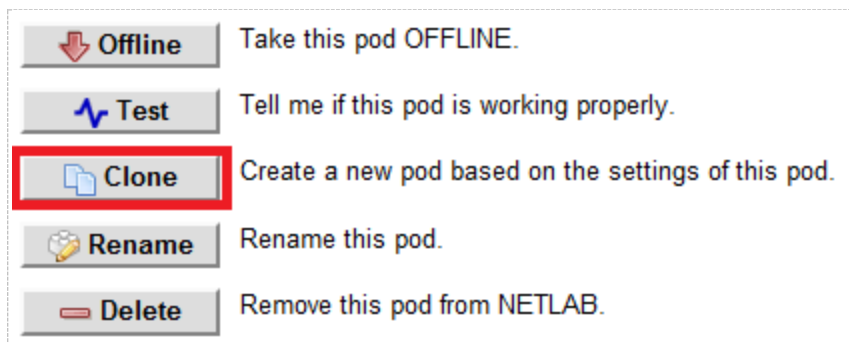
5.3 Copying Your Master Pod to the Second Host

For this task, we will use the pod cloning utility to copy our Master Pod to the 2nd host.

1. Login into NETLAB+ with the administrator account.
2. Select the **Equipment Pods** link.

Equipment Pods

3. Click on your Ethical Hacking Master Pod that was created on the 1st VMware host server.
4. Click the Clone button to create a new pod based on the settings of this pod.

⬇ Offline	Take this pod OFFLINE.
∿ Test	Tell me if this pod is working properly.
🗇 Clone	Create a new pod based on the settings of this pod.
🐝 Rename	Rename this pod.
⊖ Delete	Remove this pod from NETLAB.

5. Select the New Pod ID.

> It is advised to keep the pods in numerical order. If the pod IDs are not in numerical order, they will not show up in the scheduler in numerical order.

6. Click **Next**.

7. Enter a New Pod Name. For example, Ethical Hacking **Master Pod 2**. Click **Next**.
8. When the action has finished processing, you are presented with a settings screen.

PC Name	Source Virtual Machine	Source Snapshot	⇒	Clone Name	Clone Type	Clone Role	Runtime Host or Group	Clone Datastore	Storage Allocation
VM 1	NISGTC_EH_VM1_GM	Golden_Master		Security+_Pod_01 VM 1	Linked	Master	Host 209.114.126.6	LocalSATA	On Demand
VM 2	NISGTC_EH_VM2_GM	Golden_Master		Security+_Pod_01 VM 2	Linked	Master	Host 209.114.126.6	LocalSATA	On Demand
VM 3	NISGTC_EH_VM3_GM	Golden_Master		Security+_Pod_01 VM 3	Linked	Master	Host 209.114.126.6	LocalSATA	On Demand
VM 4	NISGTC_EH_VM4_GM	Golden_Master		Security+_Pod_01 VM 4	Linked	Master	Host 209.114.126.6	LocalSATA	On Demand
VM 5	NISGTC_EH_VM5_GM	Golden_Master		Security+_Pod_01 VM 5	Linked	Master	Host 209.114.126.6	LocalSATA	On Demand
VM 6	NISGTC_EH_VM6_GM	Golden_Master		Security+_Pod_01 VM 6	Linked	Master	Host 209.114.126.6	LocalSATA	On Demand
VM 7	NISGTC_EH_VM7_GM	Golden_Master		Security+_Pod_01 VM 7	Linked	Master	Host 209.114.126.6	LocalSATA	On Demand
VM 8	NISGTC_EH_VM8_GM	Golden_Master		Security+_Pod_01 VM 8	Linked	Master	Host 209.114.126.6	LocalSATA	On Demand

9. The four key columns for this Master Pod clone are Source Snapshot, Clone Type and Clone Role, and Runtime Host.
    a. Source Snapshot should be set to the **Golden_Master** snapshot you created previously.
    b. Under Clone Type, click the dropdown menu and verify that **Full** is selected.
    c. Under Clone Role, click the dropdown menu and select **Master**.
    d. Under Runtime Host, select the 2nd host system (which should be different than the system you are cloning from).
10. When you are done changing settings, Click **Clone Pod**. This may take up to 30 minutes as full copies are being made. You may navigate away from the cloning progress screen, and then later return to the pod to check progress.

> The NETLAB+ software does not clone the snapshots of the Ethical Hacking Master VMs. It is necessary to login into your Management Workstation and create the snapshots manually as you did in section 4.6.

11. When the cloning process is complete, you should create a Golden_Snapshot on each virtual machine in the 2nd Master pod.

5.4   Creating User Pods on the Second Host

To create user pods on the second host, repeat the steps to create user pods on the first host, substituting the 2nd Master pod (created in the previous section) as the cloning source.

6   Assigning Pods to Students, Teams , or Classes

Please refer to the *Pod Assignment Guide* for details on using the Pod Assignment feature.