



# **Multi-purpose Security Pod (MSEC) Installation and Configuration Guide**

**Designed to Support Information Assurance Security+ Labs**

**Document Version: 2012-08-08**

Copyright © 2003-2012 Center for Systems Security and Information Assurance (CSSIA)

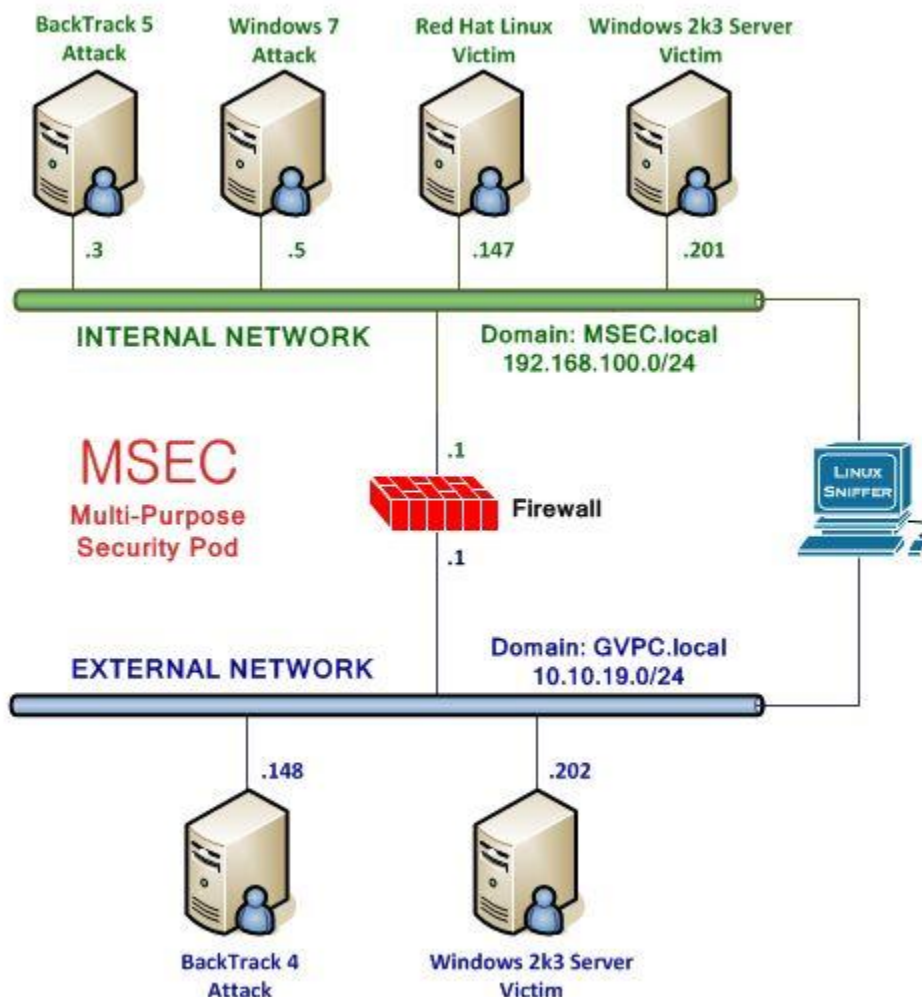
The development of this document is funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) is an entity of Moraine Valley Community College. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation. A copy of this license can be found at <http://www.gnu.org/licenses/fdl.html>.

1	Introduction .....	3
1.1	About Information Assurance Security+ .....	4
1.2	Using NETLAB+ to Deliver Security+.....	4
1.3	Benefits of NETLAB+ for Lab Delivery .....	4
1.4	Introducing the MSEC Pod .....	5
2	Planning.....	7
2.1	Security+ Environment.....	7
2.2	Setup Tasks.....	8
2.3	Security+ Pod Creation Workflow .....	8
2.4	Security+ Pod Storage Requirements .....	9
3	Security+ Pod Configuration .....	10
3.1	Deploying Virtual Machines .....	10
3.2	Convert Virtual Machines to Templates .....	12
3.3	NETLAB+ Virtual Machine Inventory Setup.....	12
3.4	Create Master Security+ Virtual Machines for Configuration .....	14
3.5	Install the Multi Purpose Security (MSEC) Pod .....	15
4	Pod Cloning .....	18
5	Assigning Security+ Pods to Students, Teams and/or Classes.....	18

## 1 Introduction

This document provides detailed guidance on performing the installation and configuration of the virtual machines used for the Information Assurance Security+ Lab Series. Virtual machines are one of many information technologies used to support advanced information systems and assurance education. Their deployment in education has the potential to support larger numbers of students with significantly less hardware and financial resources required.

In this series of lab exercises mapped to the Information Assurance Security+ training standard, a common virtual machine topology is employed throughout the entire lab course. The entirety of the set of virtual machines, referred to as a *pod*, is presented in logical diagram of the pod below:



## 1.1 About Information Assurance Security+

The Security+ course will equip trainees with the knowledge, skills, and abilities to meet the requirements of the CompTIA Security+ certification. Explanations of key components of information systems, security mechanisms, and information assurance practices, will accompany virtual lab exercises and supplemental documents to provide students with necessary educational objectives to meet the Security+ standard.

## 1.2 Using NETLAB+ to Deliver Security+

NDG has partnered with the [Center for Systems Security and Information Assurance \(CSSIA\)](#) to enable NETLAB+ support of the Information Assurance Security+ course. The use of NETLAB+ provides an enormous opportunity for educational organizations seeking a scalable, cost effective solution to offer access to the technology in order to provide students a “sandbox” environment to learn necessary information security skills.

## 1.3 Benefits of NETLAB+ for Lab Delivery

All lab components in the NETLAB+ Multipurpose Security (MSEC) pod are 100% virtualized to achieve a high pod to physical host ratio, at a significantly low cost. Using virtualization and the sharing and scheduling capabilities of NETLAB+, each student (or team of students) has access to their own set of virtual machines.

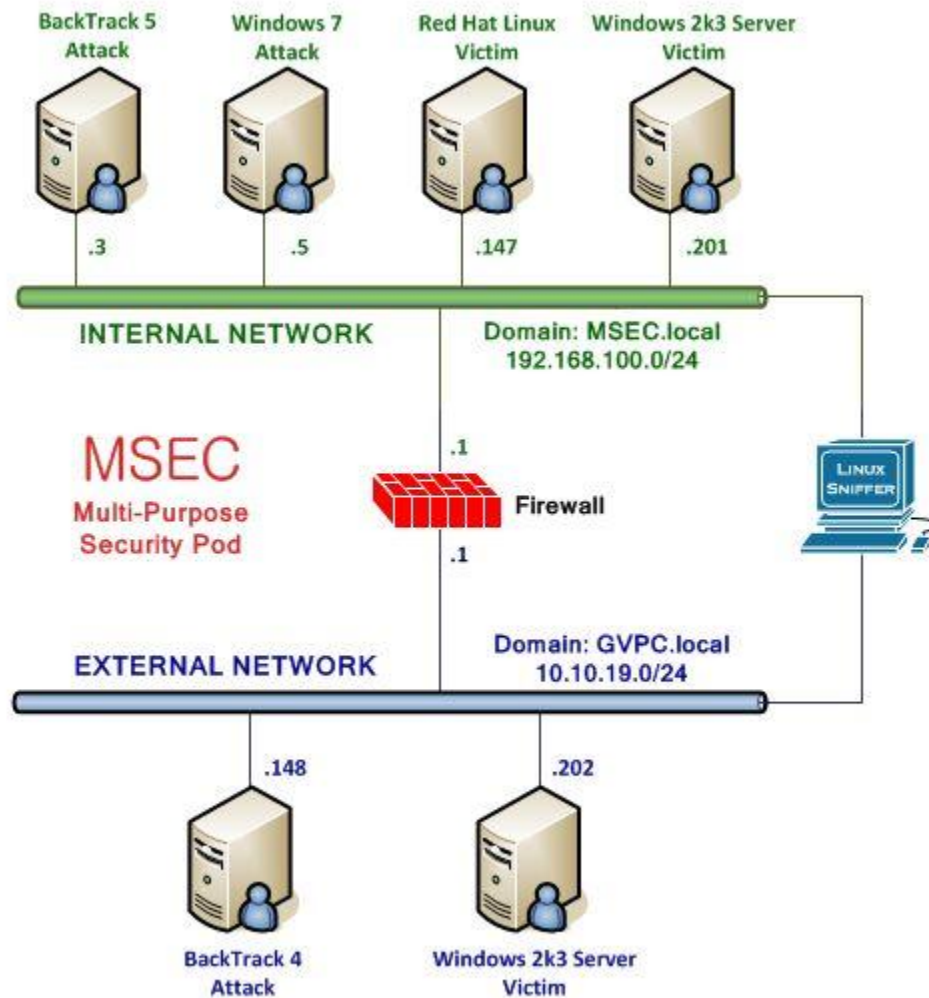
NETLAB+'s use of virtualized lab components results in a significant cost reduction by allowing several pods to run simultaneously on one physical server.

In addition to the virtualized environment, NETLAB+ also provides several software features to easily create and manage MSEC pods:

- Documentation to guide you through the setup of the Information Assurance Security+ course
- Pre-configured virtual machine templates to assist with setup
- Security+ lab exercises designed for online delivery via NETLAB+
- New NETLAB+ software features that help support the Security+ course:
  - Integration with vCenter and the vSphere API to automate many virtual machine tasks
  - A Pod Cloning feature to replicate pods with a few mouse clicks
  - A Pod Assignment feature to dedicate pods to individual students and teams
  - Automated Pod Setup and Teardown. NETLAB+ will automatically setup each pod when it is reserved, including automatic setup of virtual networking and remote display settings. At the end of a reservation, virtual networks used by a pod are deleted to conserve hosts resources.

## 1.4 Introducing the MSEC Pod

The Multi Purpose Security (MSEC) 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 Information Assurance Security+ labs.



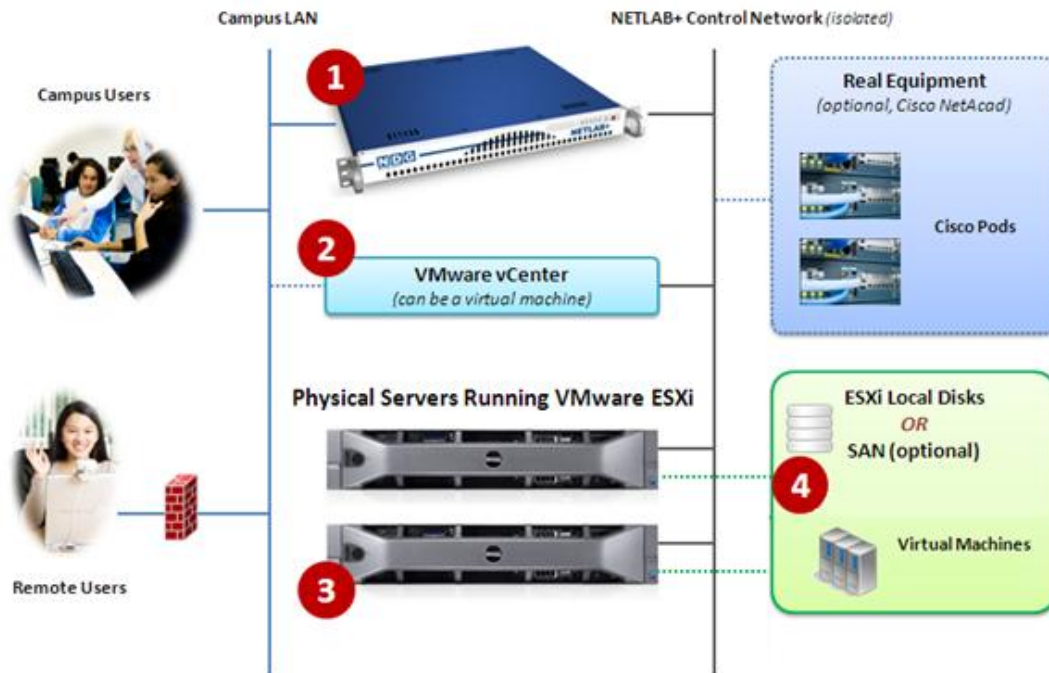
Virtual Machine	Role
BackTrack 5 Attack	BackTrack 5
Windows 7 Attack	Microsoft Windows 7 Professional
Red Hat Linux Victim	Microsoft Windows 2003 Server
Windows 2k3 Server Victim	Microsoft Windows 2003 Server (internal network)
pfSense Firewall	Firewall
Sniffer	Linux based Sniffer
BackTrack 4 Attack	BackTrack 4
Windows 2k3 Server Victim	Microsoft Windows 2003 Server (external network)

Each MSEC pod runs inside a single physical VMware ESXi server. Using the NDG recommended hardware specifications, you can host up to **5** active pods on a single physical ESXi server. A 2nd physical server can be added to host up to 10 active pods.

## 2 Planning

### 2.1 Security+ Environment

The following diagram depicts four major components that make up the Security+ 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 Security+ 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 Security+ pods. The two hosts servers depicted can run up to 10 active Security+ pods.
4. Security+ pods consist of 8 virtual machines that reside on your physical ESXi host server disks. Optionally, these virtual machines can reside on a Storage Area Network (SAN).

## 2.2 Setup Tasks

The following is a summary of Security+ setup tasks in this document. This document assumes that your physical infrastructure has already been installed with the appropriate VMware software as outlined in our Remote PC guide found here: [http://www.netdevgroup.com/support/documentation/NETLAB Remote PC Guide VC enter.pdf](http://www.netdevgroup.com/support/documentation/NETLAB_Remote_PC_Guide_VC_enter.pdf)

1. Obtain software, templates and keys.
2. Create a Master Pod on the first ESXi host.
3. Configure the virtual machines.
4. Replicate Security+ pods using the pod cloning feature.
5. Assign Security+ pods to students or instructors using Pod Assigner.

## 2.3 Security+ Pod Creation Workflow

The following is an overview of the Security+ pod setup process. This assumes you do not have a Storage Area Network (SAN) and you will be storing Security+ pods on each VMware server's local disk. SAN storage for virtual machines is not currently supported by NETLAB+.

1. The 8 virtual machine templates for the Security+ pod are distributed by CSSIA and installed on vCenter.

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. Follow the instructions to complete and submit the form.

2. Master VMs are created from each template VM. The master VMs are added to a Master pod. A *Golden Snapshot* of the Master pod is taken, which becomes the foundation to clone Security+ User pods.
3. The NETLAB+ pod cloning feature is used to quickly create copies from the Security+ Master Pod on the first VMware host (Host A in the diagram).
4. A full replica of the Master Security+ Pod on Host A is made on Host B, using the NETLAB+ Pod Cloning Feature.



5. The cloning feature is used to quickly create Security+ pods from the Security+ Master Pod on Host B.

Without a Storage Area Network (SAN), Security+ pods on Host B cannot be linked to Host A. This is because Host B cannot access Host A's local disks (and vice-versa). Therefore, we create one Master Security+ Pod per host. SAN storage for virtual machines is not currently supported by NETLAB+.

## 2.4 Security+ Pod Storage Requirements

You should budget **28 gigabytes** of storage per Master Security+ pod. You should also budget **15 gigabytes of storage** per Student Security+ pod.

The datastore containing a Security+ pod must be accessible to the VMware host to which it is assigned as directly attached local storage.

### 3 Security+ Pod Configuration

This section will walk you through creating and adding a Master Security+ Pod to the NETLAB+ system. The Master Security+ Pod will be used to quickly create copies of the Security+ pod that can be assigned to classes and students.

The Security+ Pod consists of eight virtual machines: four Linux based clients, two Windows 2003 servers, a Windows 7 client machine, and a firewall appliance.

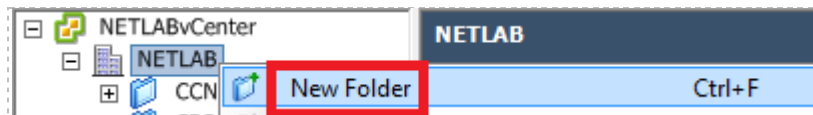
#### 3.1 Deploying Virtual Machines

CSSIA will provide password-protected links that you can use to deploy your virtual machines directly.

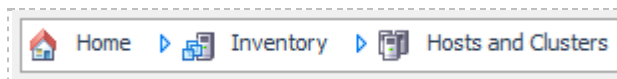
1. Open the vClient on your administration machine. Connect to your vCenter Server.
2. Select **VMs and Templates** in the address bar.



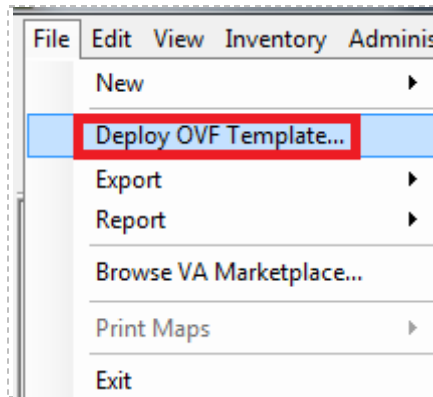
3. Right-click on the **NETLAB** datacenter, and select **New Folder**.



4. Name the new folder “**Master Security+ Pod**”. This is where we will create the master virtual machines to be cloned later.
5. Select **Hosts and Clusters** in the address bar.



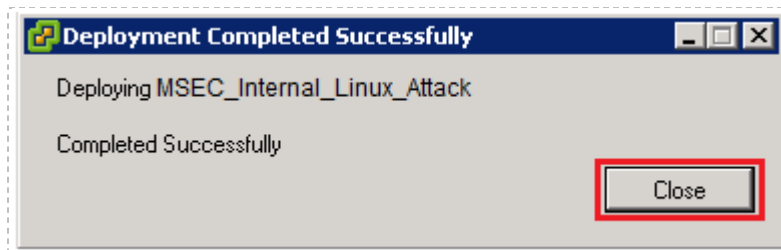
6. Click on your ESXi Host Server.
7. Click on File -> Deploy OVF Template.



8. Enter the link to the OVA file named **MSEC\_Internal\_Linux1\_Attack.ova** that was provided by CSSIA. Enter the username and password you were provided.
9. On the OVF Template Details window, click **Next**.
10. On the Name and Location window, enter **Master\_Internal\_Linux1\_Attack** as the name and select the **Master Security+ Pod** folder you created earlier. Click **Next**.
11. On the Disk Format window, click on **Thin provisioned format**. Click **Next**.
12. On the Network Mapping window, leave the default networks. Click **Next**.

Network mapping is handled automatically by the NETLAB+ system during pod creation.

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**.

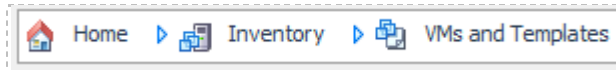


15. Repeat steps 6-14 for the remaining MSEC\_Internal\_Linux2\_Victim, MSEC\_Internal\_Windows1\_Attack, MSEC\_Internal\_Windows2\_Victim, MSEC\_Linux\_Sniffer, MSEC\_Pfsense\_Firewall, MSEC\_External\_Linux3\_Attack, and MSEC\_External\_Windows3\_Victim OVA files.

### 3.2 Convert Virtual Machines to Templates

The deployed OVA files will be displayed in your host server's inventory as Virtual Machines and should be converted into templates for backup purposes. This will ensure that the original OVA files are not accidentally modified.

1. Select **VMs and Templates** in the address bar.



2. Right-click on your **Master\_Internal\_Linux1\_Attack** virtual machine and choose **Template > Convert to Template**.
3. Repeat step 2 for the remaining 7 Security+ virtual machines.

Aside from the configuration of your master lab virtual machines, all Virtual Machine management for the Security+ Pods will be conducted through your NETLAB+ system.

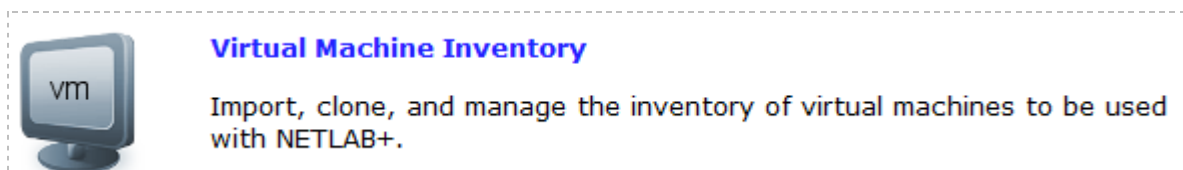
### 3.3 NETLAB+ Virtual Machine Inventory Setup

This section will guide you in adding your templates to the Virtual Machine Inventory of your NETLAB+ system. This guide assumes that your Virtual Machine Host Servers have previously been setup. If this is not the case, please see the *Adding ESXI hosts in NETLAB+* section of the [Remote PC Guide](#).

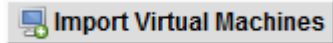
1. Login into your NETLAB+ system using the administrator account.
2. Select the Virtual Machine Infrastructure link.



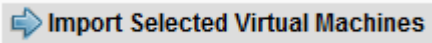
3. Click the Virtual Machine Inventory link.



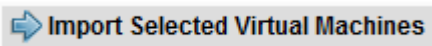
- Click the Import Virtual Machines button.



- Select the check box next to your eight **Master** virtual machine templates and click Import Selected Virtual Machines.




- When the Configure Virtual Machines window loads, you can set your virtual machine parameters.
- Check the drop down box for the correct operating system for each imported virtual machine.
- Add any comments for each virtual machine in the box to the right.
- Verify your settings and click Import Selected Virtual Machines.











- Click OK when the virtual machines have finished loading.
- Verify that your virtual machines show up in the inventory.

**Virtual Machine Inventory**

Admin Logout



Import, clone, and manage the inventory of virtual machines to be used with NETLAB+.

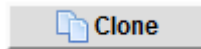
Virtual Machine Name	Operating System	Role	Datacenter	Runtime Host	Host Group	CPUs
 Master_External_Linux3_Attack	Linux	Template				1
 Master_External_Windows3_Victim	Windows Server 2003	Template				1
 Master_Internal_Linux1_Attack	Linux	Template				1
 Master_Internal_Linux2_Victim	Linux	Template				1
 Master_Internal_Windows1_Attack	Windows 7	Template				1
 Master_Internal_Windows3_Victim	Windows Server 2003	Template				1
 Master_Linux_Sniffer	Linux	Template				1
 Master_Pfsense_Firewall	Free BSD	Template				1

- Leave the virtual machine inventory open for the next section.

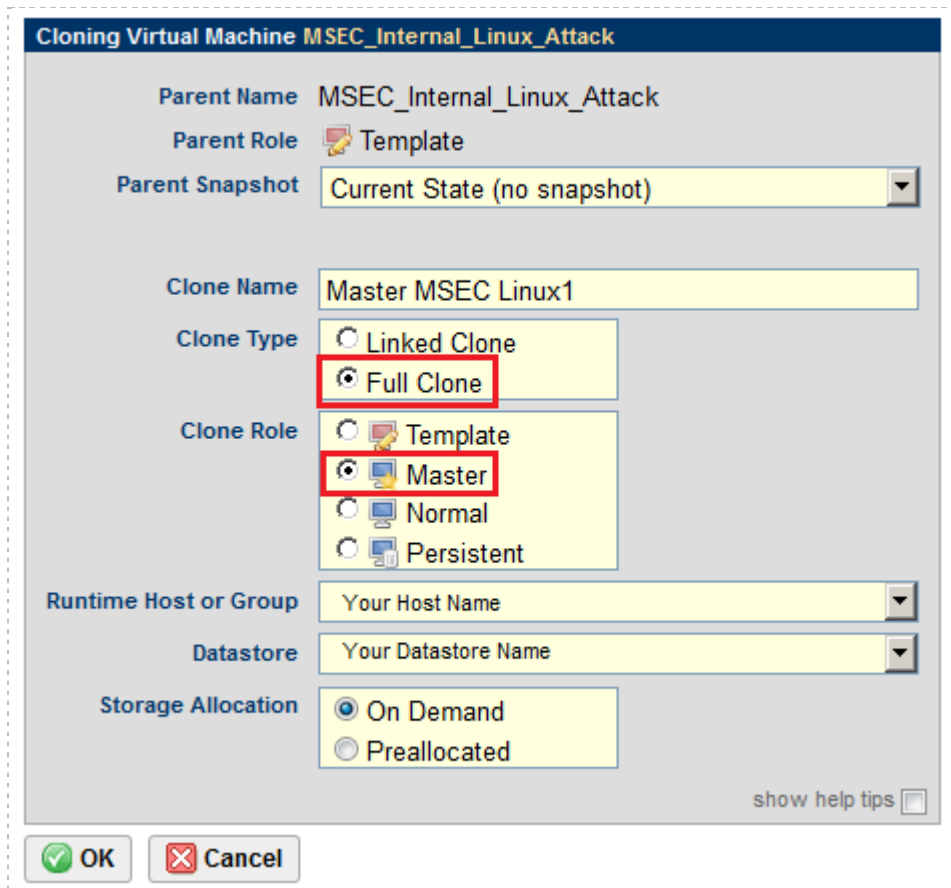
### 3.4 Create Master Security+ Virtual Machines for Configuration

This section will assist you in creating master Security+ virtual machines.

1. Click on the **Master\_Internal\_Linux1\_Attack** template.
2. Click the **Clone** button.




3. Use **Master MSEC Linux1** as the Clone Name.
4. Select the radio button next to **Full Clone** in the Clone Type box.
5. Select the radio button next to **Master** in the Clone Role box.
6. Select your first host server and datastore from the drop down boxes.
7. Verify that your settings resemble the following picture.



**Cloning Virtual Machine MSEC\_Internal\_Linux\_Attack**





Parent Name: MSEC\_Internal\_Linux\_Attack

Parent Role:  Template

Parent Snapshot: Current State (no snapshot)

Clone Name: Master MSEC Linux1

Clone Type:  Linked Clone  
 Full Clone

Clone Role:   Template  
  Master  
  Normal  
  Persistent

Runtime Host or Group: Your Host Name

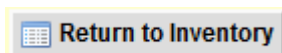
Datastore: Your Datastore Name

Storage Allocation:  On Demand  
 Preallocated

show help tips

OK  Cancel

8. Click **OK**.
9. Click Return to Inventory.



10. Repeat steps 1-9 for the remaining templates, changing their names accordingly:

- Master\_Internal\_Linux2\_Victim > **Master MSEC Linux2**
- Master\_External\_Linux3\_Attack > **Master MSEC Linux3**
- Master\_Internal\_Windows1\_Attack > **Master MSEC Windows1**
- Master\_Internal\_Windows2\_Victim > **Master MSEC Windows2**
- Master\_External\_Windows3\_Victim > **Master MSEC Windows3**
- Master\_PfSense\_Firewall > **Master MSEC Firewall**
- Master\_Linux\_Sniffer > **Master MSEC Sniffer**

11. Some cloning processes will take longer than others, depending on your network connection and hard drive speeds.

12. Return to your vCenter client and right click each VM you just created and select **Snapshot > Take Snapshot**.

13. Use **GOLDEN\_MASTER** as the name for each VM's snapshot.

### 3.5 Install the Multi Purpose Security (MSEC) Pod

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

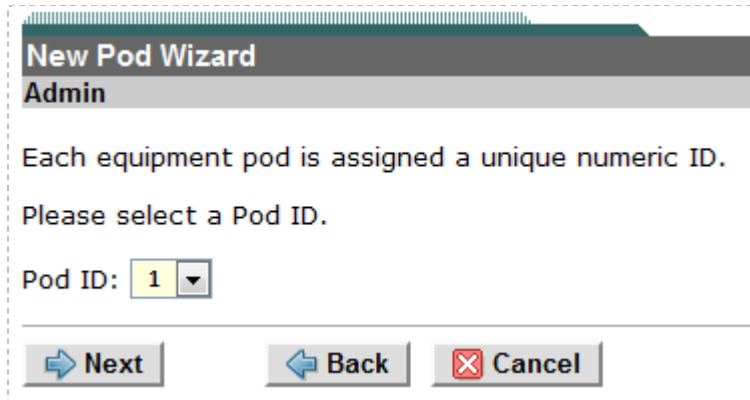
1. Login into NETLAB+ with the administrator account.
2. Select the **Equipment Pods** link.



3. Select Add a Pod.



4. The New Pod Wizard will now help you add an equipment pod to your system.
5. In the New Pod Wizard, click **Next** to continue.
6. When prompted, select the MSEC Pod and click **Next** to continue.
7. Select a Pod ID number. It is best practice to use a block of sequential ID numbers for the number of pods you are going to install. The Pod ID number determines the order in which the pods will appear in the scheduler. Click **Next** to continue.

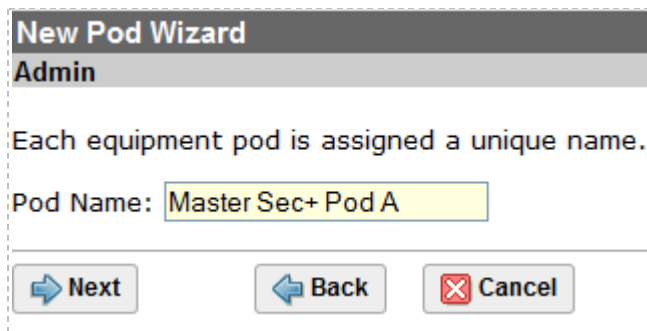


**New Pod Wizard**  
Admin

Each equipment pod is assigned a unique numeric ID.  
Please select a Pod ID.

Pod ID:

8. Assign the pod a unique Pod Name. Click **Next** to continue.

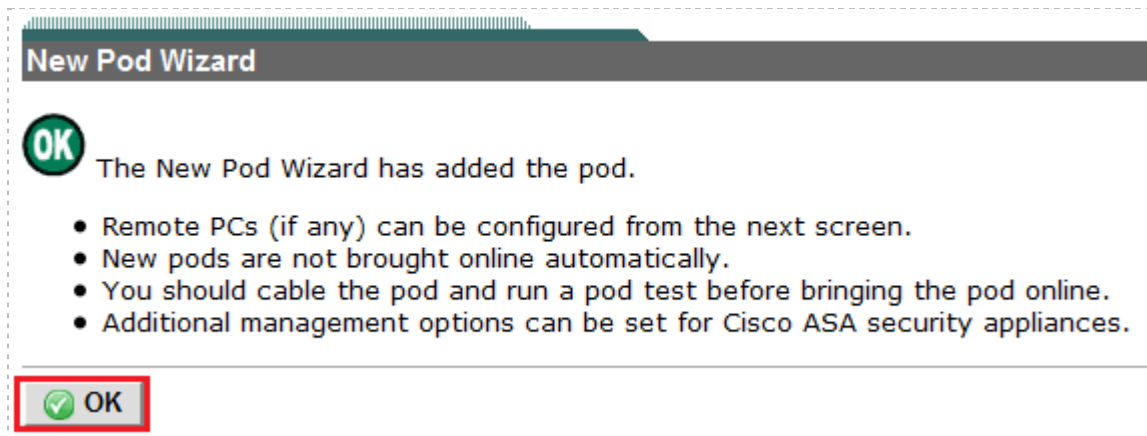


**New Pod Wizard**  
Admin

Each equipment pod is assigned a unique name.

Pod Name:

9. The wizard will add the pod to NETLAB+. When completed, click **OK** to finish.





**New Pod Wizard**

**OK** The New Pod Wizard has added the pod.

















- Remote PCs (if any) can be configured from the next screen.
- New pods are not brought online automatically.
- You should cable the pod and run a pod test before bringing the pod online.
- Additional management options can be set for Cisco ASA security appliances.

10. Click on the **Magnifying Glass** icon next to **VM 1**. Please note that your PC IDs will not match the graphic below.

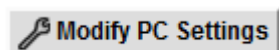


POD 1045 - STATUS					
POD ID	POD NAME	STATUS	ACTIVITY	POD TYPE	
1045	Master Sec+ Pod A	 OFFLINE	IDLE		

POD 1045 - PCs AND SERVERS (click the GO buttons to reconfigure)					
GO	NAME	PC ID	STATUS	TYPE / VM	OPERATING SYSTEM
	 VM 1	8856	ONLINE	ABSENT	
	 VM 2	8857	ONLINE	ABSENT	
	 VM 3	8858	ONLINE	ABSENT	
	 VM 4	8859	ONLINE	ABSENT	
	 VM 5	8860	ONLINE	ABSENT	
	 VM 6	8861	ONLINE	ABSENT	
	 VM 7	8862	ONLINE	ABSENT	
	 VM 8	8863	ONLINE	ABSENT	

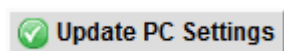
11. Click on Modify PC Settings



12. Change the PC Type drop down box to **Use Virtual Machine Inventory**.

13. In the Base Virtual Machine window, select your **Master MSEC Linux1** virtual machine.

14. Review the information on the screen and click **Update PC Settings**.



15. Click **Show Pod**.

16. Repeat Steps 10-15 for the remaining virtual machines as described below:

- VM 2 > **Master MSEC Windows1**
- VM 3 > **Master MSEC Linux2**
- VM 4 > **Master MSEC Windows2**
- VM 5 > **Master MSEC Firewall**
- VM 6 > **Master MSEC Sniffer**
- VM 7 > **Master MSEC Linux3**
- VM 8 > **Master MSEC Windows3**

17. When you have eight virtual machines' settings updated, you have successfully setup your master pod.

## **4 Pod Cloning**

Please refer to the *Virtual Machine Cloning* section of the [Remote PC Guide](#) for direction on the cloning of student pods.

## **5 Assigning Security+ Pods to Students, Teams and/or Classes**

Please refer to the [Pod Assignment Guide](#) for direction on the different types of pod assignment and their implementation.