Information Assurance CNSS 4011 Lab Series

Installation and Configuration Guide

Document Version: 2012-12-07

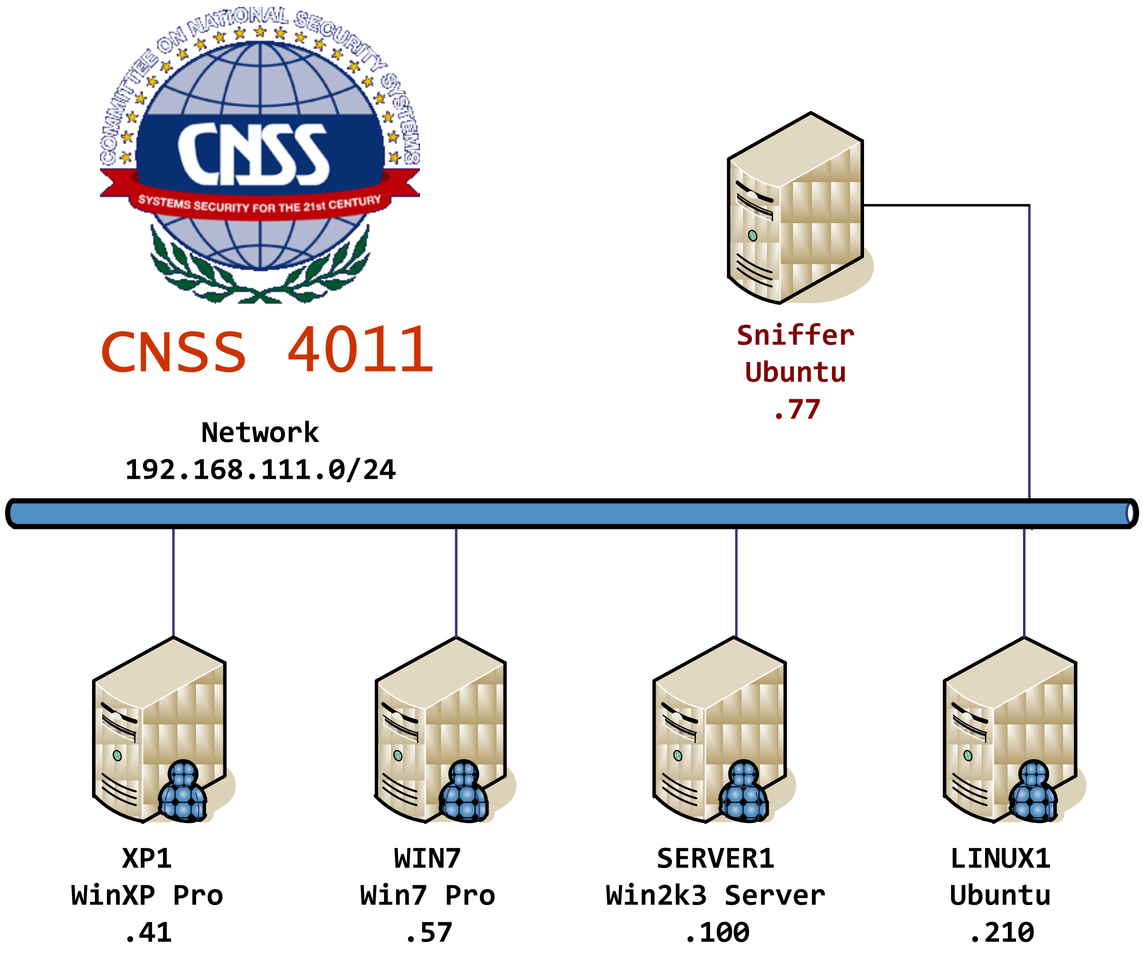
Copyright © 2003-2012 Center for Systems Security and Information Assurance (CSSIA)

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

This document provides detailed guidance on performing the installation and configuration of the virtual machines used for the Information Assurance CNSS 4011 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 CNSS 4011 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:



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

1.1 About the Information Assurance CNSS 4011 course

The CNSS 4011 course will equip trainees with the knowledge, skills, and abilities to meet the requirements of the Committee on National Security Systems 4011 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 CNSS 4011 standard.

1.2 Using NETLAB+ to Deliver CNSS 4011

NDG has partnered with the Center for Systems Security and Information Assurance (CSSIA) to enable NETLAB+ support of the Information Assurance CNSS 4011 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+ CNSS 4011 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 that will automatically reset after each lab.

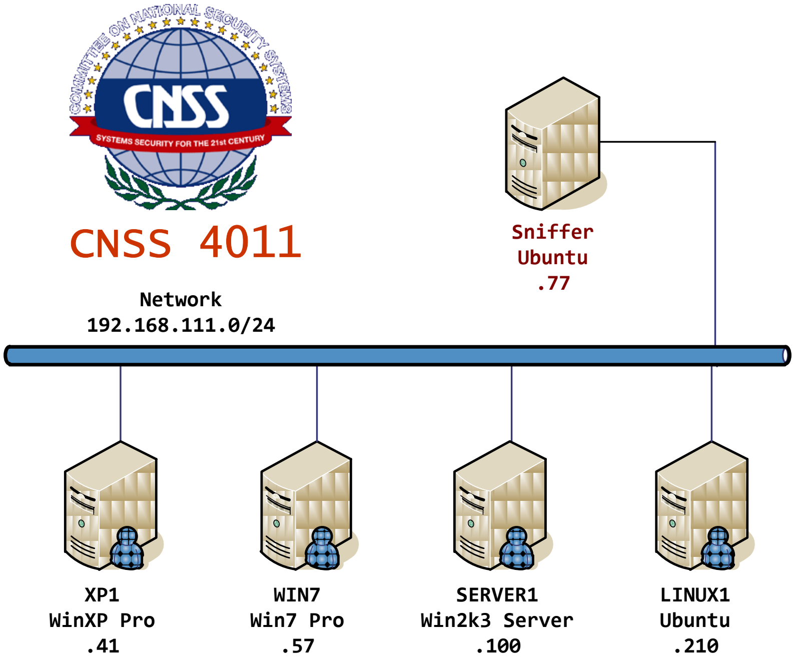
NETLAB+'s use of virtualized lab components results in a significant cost reduction by allowing several pods to run simultaneously on one physical server.

In additional to the virtualized environment, NETLAB+ also provides several software features to easily create and manage CNSS 4011 pods:

- Documentation to guide you through the setup of the CNSS 4011 course
- Pre-configured virtual machine templates to assist with setup
- CNSS 4011 lab exercises designed for online delivery via NETLAB+
- New NETLAB+ software features that help support the CNSS 4011 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 CNSS 4011 Pod

The NDG CNSS 4011 pod is a 100% virtual machine pod consisting of 5 virtual machines. Linked together through virtual networking, these 5 virtual machines provide the environment for a student or team to perform the Information Assurance CNSS 4011 labs.



Virtual Machine	Role
XP1	Microsoft Windows XP Professional.
WIN7	Microsoft Windows 7 Professional.
SERVER1	Microsoft Windows 2003 Server.
LINUX1	Ubuntu v10.10.
Sniffer	Ubuntu v10.10.

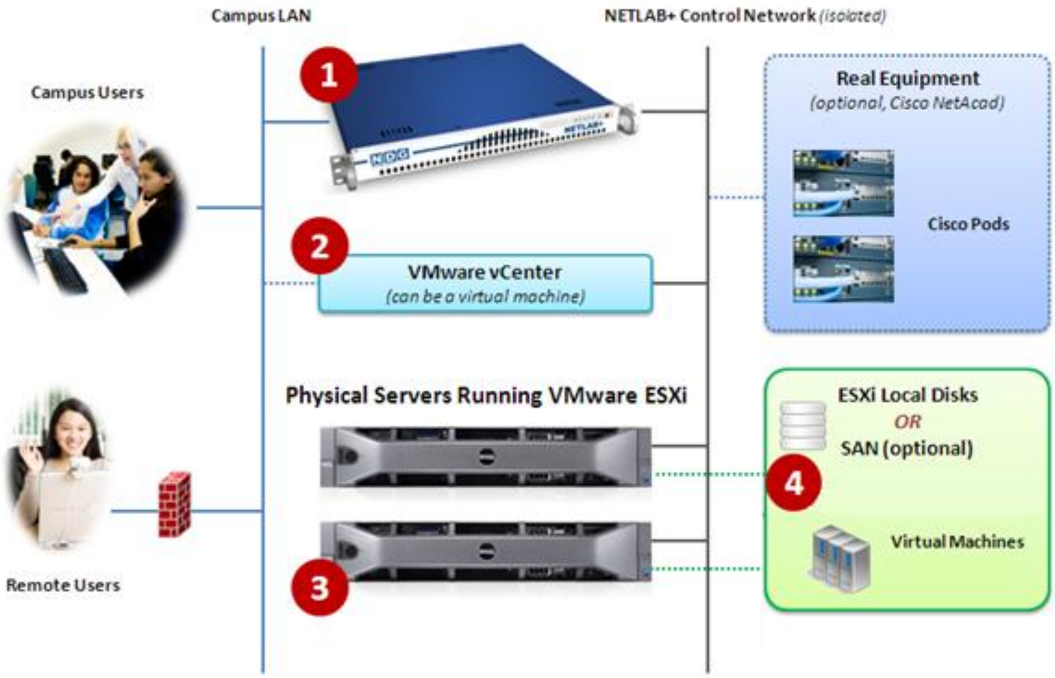
Each CNSS 4011 pod runs inside a single physical VMware ESXi server. Using the hardware specifications in this document, you can host up to 8 active pods on a single physical ESXi server. A 2nd physical server can be added to host up to 16 active pods.

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

2 Planning

2.1 CNSS 4011 Environment

The following diagram depicts four major components that make up the CNSS 4011 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 CNSS 4011 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 CNSS 4011 pods. The two hosts servers depicted can run up to 16 active CNSS 4011 pods.
4. CNSS 4011 pods consist of 5 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 CNSS 4011 setup tasks in this document.

1. Obtain software, templates and keys.
2. Setup Physical VMware ESXi Hosts Server.
3. Install VMware vCenter Server.
4. Create a Master Pod on the first ESXi host.
5. Configure the virtual machines; add Microsoft software and ISO files.
6. Replicate CNSS 4011 pods using the pod cloning feature.
7. Assign CNSS 4011 pods to students or instructors using Pod Assigner.

2.3 CNSS 4011 Pod Creation Workflow

The following is an overview of the CNSS 4011 pod setup process. This assumes you do not have a Storage Area Network (SAN) and you will be storing CNSS 4011 pods on each VMware server's local disk. SAN storage for virtual machines is not currently supported by NETLAB+.

1. The 5 virtual machine templates for the CNSS 4011 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 CNSS 4011 User pods.

3. The NETLAB+ pod cloning feature is used to quickly create copies from the CNSS 4011 Master Pod on the first VMware host (Host A in the diagram).

4. A full replica of the Master CNSS 4011 Pod on Host A is made on Host B, using the NETLAB+ Pod Cloning Feature.

5. The cloning feature is used to quickly create CNSS 4011 pods from the CNSS 4011 Master Pod on Host B.

Without a Storage Area Network (SAN), CNSS 4011 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 CNSS 4011 Pod per host. SAN storage for virtual machines is not currently supported by NETLAB+.

2.4 Software Requirements

For the purpose of software licensing, each virtual machine is treated as an individual 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, server software, operating systems, and applications.

2.5 CNSS 4011 Pod Storage Requirements

You should budget **55 gigabytes** of storage per Master CNSS 4011 pod. You should also budget **15 gigabytes of storage** per Student CNSS 4011 pod.

The datastore containing a CNSS 4011 pod must be accessible to the VMware host to which it is assigned as directly attached local storage.

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

3 CNSS 4011 Software Configuration

This section will walk you through creating and adding a Master CNSS 4011 Pod to the NETLAB+ system. The Master CNSS 4011 Pod will be used to quickly create copies of the CNSS 4011 pod that can be assigned to classes and students.

The CNSS 4011 Pod consists of five virtual machines: two Linux clients, a Windows 2003 server, a Windows XP client machine, and a Windows 7 client machine.

If you have completed and returned the form requesting the preinstalled CNSS 4011 virtual machines from CSSIA (see section 2.3), skip to Section 3.3 and continue following the instructions.

It is preferred that you request the preinstalled CNSS 4011 virtual machines from CSSIA. Otherwise, you must complete sections 0 and 0.

3.1 Download Required Software for CNSS 4011 Virtual Machines

If you have completed and returned the form requesting the preinstalled CNSS 4011 virtual machines from CSSIA (see section 2.3), skip to Section 3.3 and continue following the instructions.

This section will assist you in downloading the necessary software files needed for installation on the virtual machines.

1. Create a folder on your desktop named 4011 Software.
2. Download the following installation files from the following sites:
    - SlavaSoft HashCalc http://www.slavasoft.com/hashcalc/index.htm
    - CrypTool http://www.cryptool.org/
    - ophcrack http://ophcrack.sourceforge.net
    - Zenmap http://nmap.org
    - Wireshark http://www.wireshark.org
    - Eraser http://eraser.heidi.ie/download.php
    - Restoration http://www.snapfiles.com/get/restoration.HTML
    - PuTTY http://www.chiark.greenend.org.uk/~sgtatham/putty/
    - Advanced Port Scanner http://www.download3k.com/Install-Advanced-Port-Scanner.html
3. Move each of the installation files into the 4011 Software folder.
4. Right-click on a blank area of your CNSS 4011 Software folder and select New > Text Document.
5. Name the file **map-h.drive.bat**.
6. Add the following two lines to the file:

    ```
    net use H: \\192.168.111.100\SECRET
    /user:shareuser P@ssw0rd /persistent:yes
    ```

7. Save and close the file.
8. Use an ISO Image creator to create an ISO containing the 4011 Software folder. A free ISO creator can be found at: http://download.cnet.com/Free-ISO-Creator/3000-2242_4-10902634.html

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

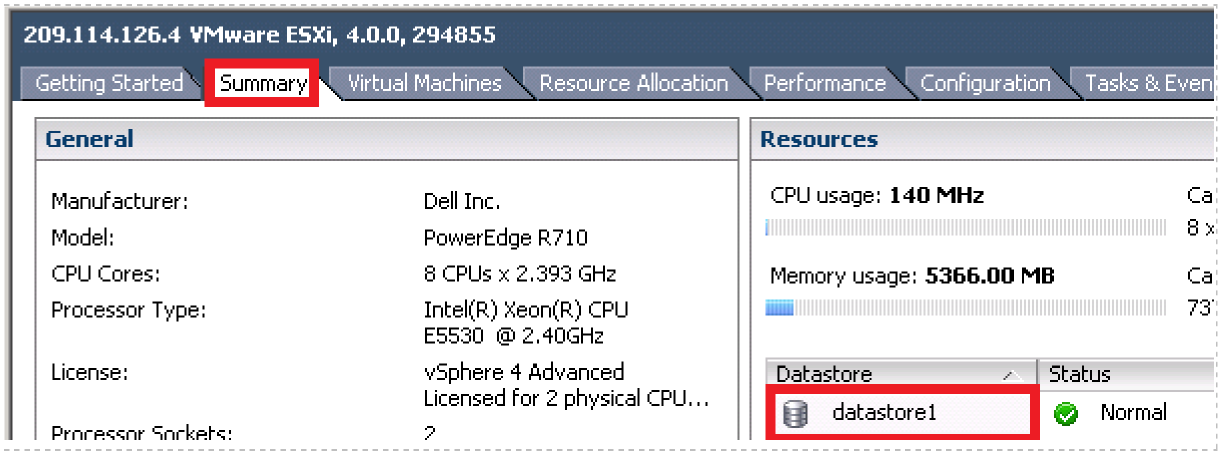
3.2 Uploading ISO files to Datastore

This section will assist you in preparing the local datastore with the files needed for the lab machines.

Software	Source
CNSS 4011 Software ISO	Created in Task 3.1
Windows XP Professional ISO	Not Provided
Windows 7 Professional ISO	Not Provided
Windows Server 2003 R2 32-bit ISO	Not Provided

To upload the ISO files (OVA files are covered in the next task):

1. In vCenter, click on your host in the inventory.
2. Click the **Summary** tab at the top.



209.114.126.4 VMware ESXi, 4.0.0, 294855

General

Manufacturer:	Dell Inc.
Model:	PowerEdge R710
CPU Cores:	8 CPUs x 2.393 GHz
Processor Type:	Intel(R) Xeon(R) CPU E5530 @ 2.40GHz
License:	vSphere 4 Advanced Licensed for 2 physical CPU...
Processor Sockets:	2

Resources

CPU usage: **140 MHz** Ca
8 x

Memory usage: **5366.00 MB** Ca
73

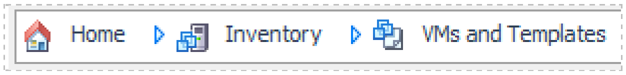
Datastore	Status
datastore1	✓ Normal

3. Right-click the datastore on the right hand side.
4. Click Browse Datastore.
5. Click the new folder icon at the top.
6. Name the new folder **CNSS 4011 Setup**.
7. Double-click the new folder.
8. Click the upload files icon at the top.
9. Select Upload File.
10. Locate your first ISO image and click **Open**.
11. Repeat these steps for the remaining 3 ISO images.

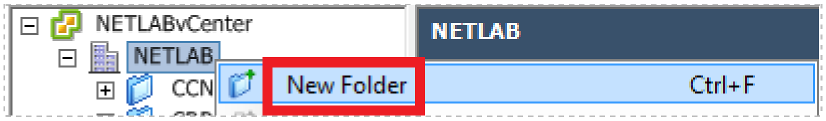
3.3 Deploying Virtual Machines

CSSIA uses two methods for distributing OVA files. They will either mail you the OVA files on storage media or provide password protected links that you can use to deploy your virtual machines directly.

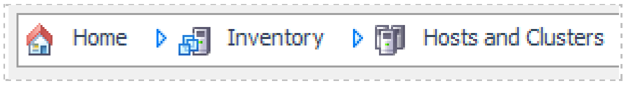
1. Open the vClient on your administration machine. Connect to your vCenter Server.
2. Select **VMs and Templates** in the address bar.



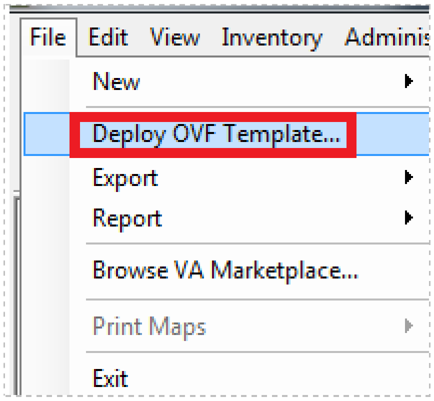
3. Right-click on the **NETLAB** datacenter, and select **New Folder**.



4. Name the new folder "**Master CNSS 4011 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.

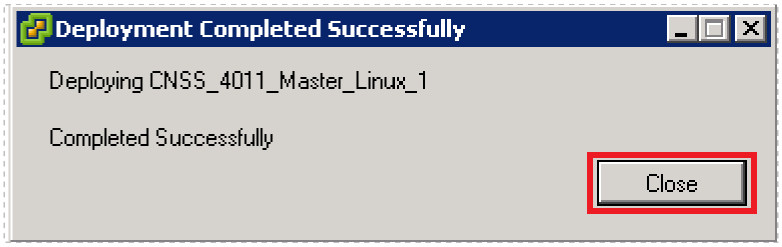


8. If you received storage media from CSSIA, click on **Browse** and locate the **LINUX1.ova** file you received from the Lab Resource Center. Click **Next** to continue. If you were provided links to the ova files, enter the link that points to the **LINUX1.ova** and click **Next**.
9. If you are utilizing the CSSIA links, enter the username and password you were provided, if you are using storage media, skip to **step 10**.

10. On the OVF Template Details window, click **Next.**
11. On the Name and Location window, enter **Master CNSS 4011 LINUX1** as the name and select the **Master CNSS 4011 Pod** folder you created earlier. Click **Next.**
12. On the Disk Format window, click on **Thin provisioned format**. Click **Next.**
13. On the Network Mapping window, leave the default networks. Click **Next**.

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

14. On the Ready to Complete window, confirm the information and click **Finish**.
15. 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**.



Deployment Completed Successfully

Deploying CNSS_4011_Master_Linux_1

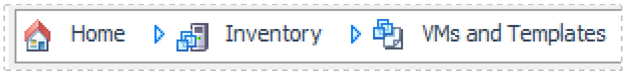
Completed Successfully

16. Repeat steps 6-15 for the remaining XP1, WIN7, LINUX2 and SERVER1 OVA files, changing the names to **Master CNSS 4011 XP1**, **Master CNSS 4011 WIN7, Master CNSS 4011 LINUX2** and **Master CNSS 4011 SERVER1**.

3.4 Convert Virtual Machines to Templates

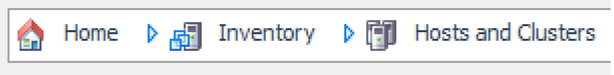
The deployed OVA files will be displayed in your host server's inventory as Virtual Machines and should be converted into templates for backup purposes. This will ensure that the original OVA files are not accidentally modified.

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



2. Right-click on your **Master CNSS 4011 LINUX1** virtual machine and choose **Template > Clone to Template**.
3. Use **CNSS 4011 Template LINUX1** as the Template name, select the **Master CNSS 4011 Pod** folder and click **Next**.
4. On the Host/Cluster screen choose your host server and click **Next**.
5. On the Datastore screen select your datastore and click **Next**.
6. On the Disk Format screen leave the defaults and click **Next**.
7. Review the settings on the Ready to Complete screen and click **Finish**.

8. Repeat Steps 2-7 for the four remaining virtual machines using **CNSS 4011 Template XP1**, **CNSS 4011 Template WIN7**, **CNSS 4011 Template SERVER1** ,and **CNSS 4011 Template LINUX2** as the Template names.
9. When the tasks complete, you should have five templates and five virtual machines in your inventory.
10. Select **Hosts and Clusters** in the address bar.



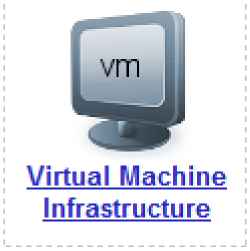
11. Right-click each one of your five virtual machines in the inventory and select Delete from Disk. When you are done, it will appear that you have nothing in your Hosts and Clusters inventory view. The templates will only appear in your VMs and Templates inventory view.

Aside from the configuration of your master lab virtual machines, all Virtual Machine management for the CNSS 4011 Pods will be conducted through your NETLAB+ system.

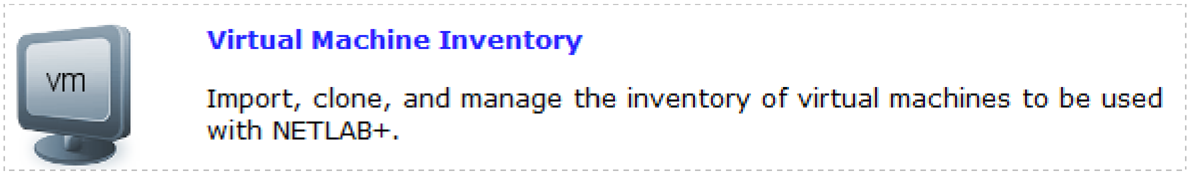
3.5 NETLAB+ Virtual Machine Inventory Setup

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.

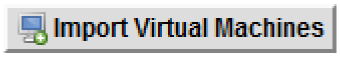


3. Click the Virtual Machine Inventory link.

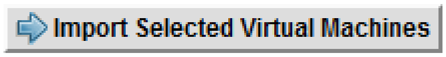


Import, clone, and manage the inventory of virtual machines to be used with NETLAB+.

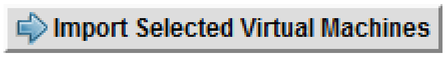
4. Click the Import Virtual Machines button.



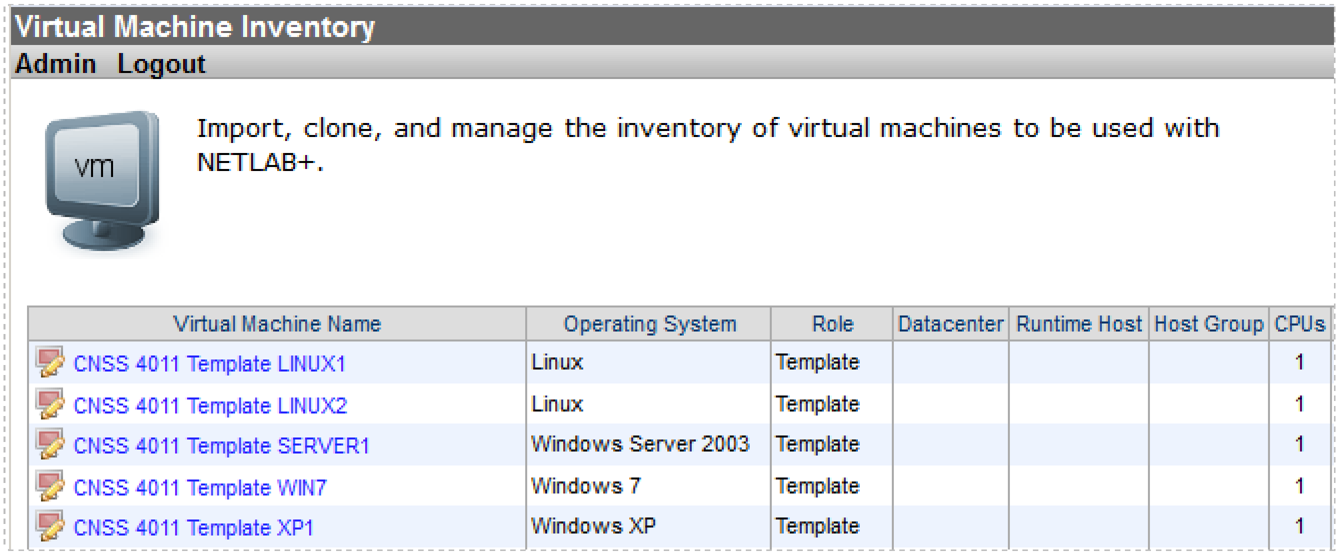
5. Select the check box next to your CNSS 4011 Template XP1, WIN7, SERVER1, LINUX1, and LINUX2 virtual machines and click Import Selected Virtual Machines.



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



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



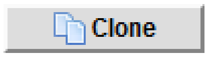
Import, clone, and manage the inventory of virtual machines to be used with NETLAB+.

Virtual Machine Name	Operating System	Role	Datacenter	Runtime Host	Host Group	CPUs
CNSS 4011 Template LINUX1	Linux	Template				1
CNSS 4011 Template LINUX2	Linux	Template				1
CNSS 4011 Template SERVER1	Windows Server 2003	Template				1
CNSS 4011 Template WIN7	Windows 7	Template				1
CNSS 4011 Template XP1	Windows XP	Template				1

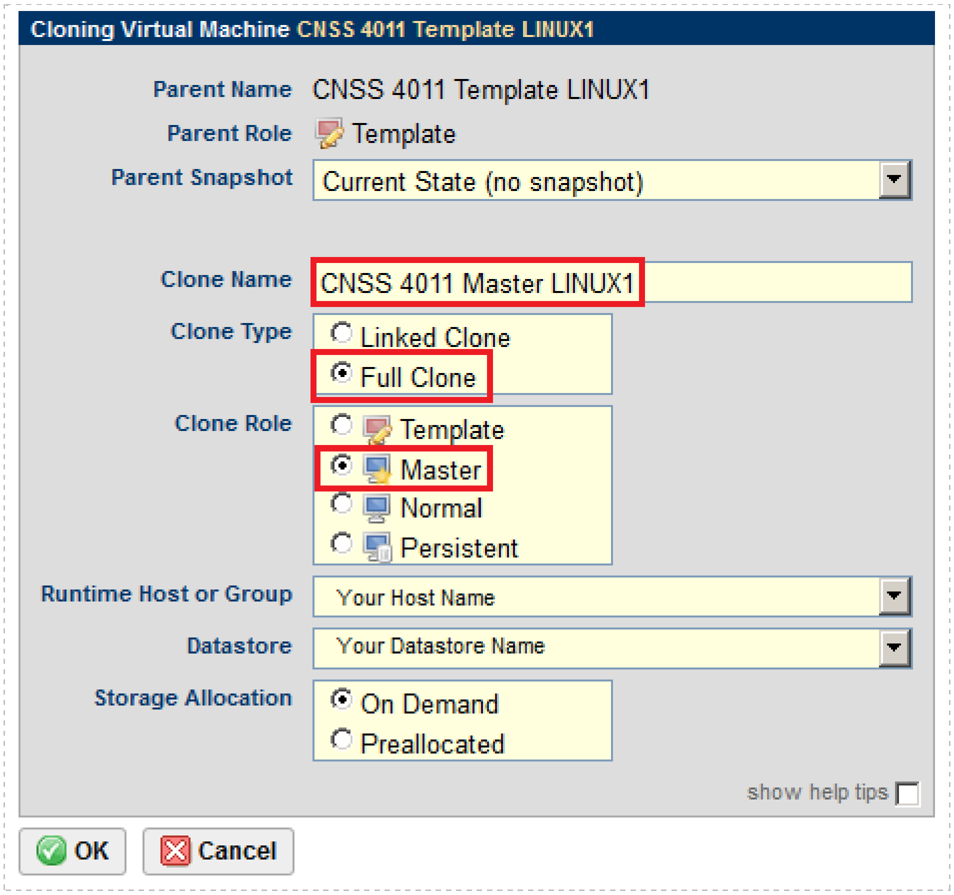
3.6 Create Master CNSS 4011 Virtual Machines for Configuration

This section will assist you in creating master CNSS 4011 virtual machines. These VMs will be used in section 4 for software configuration.

1. Click on CNSS 4011 Template LINUX1.
2. Click the **Clone** button.



3. Use **CNSS 4011 Master 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.

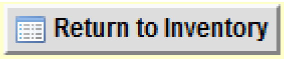


Cloning Virtual Machine CNSS 4011 Template LINUX1

Parent Name: CNSS 4011 Template LINUX1
Parent Role: Template
Parent Snapshot: Current State (no snapshot)

Clone Name: CNSS 4011 Master 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

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

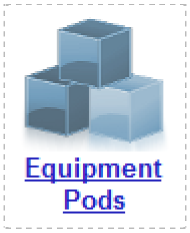


10. Repeat steps 1-9 for the XP1, WIN7, LINUX2, and SERVER1 templates, assigning the following clone names (case sensitive):
    - CNSS 4011 Master XP1
    - CNSS 4011 Master WIN7
    - CNSS 4011 Master LINUX2
    - CNSS 4011 Master SERVER1
11. Some cloning processes will take longer than others depending on your network connection and hard drive speeds.

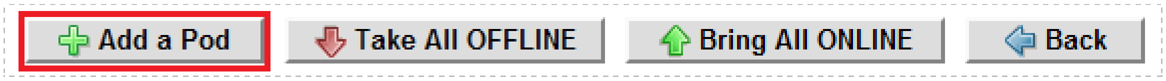
3.7 Install the Master CNSS 4011 Pod

This section will assist you in adding the CNSS 4011 Pod to your NETLAB+ system.

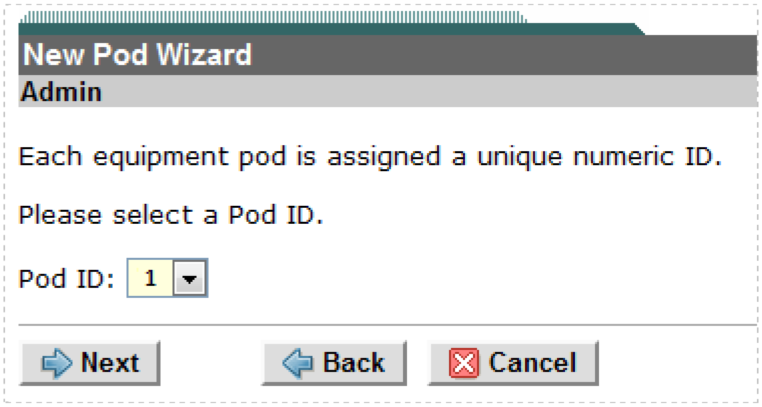
1. Login into NETLAB+ with the administrator account.
2. Select the **Equipment Pods** link.



3. Select Add a Pod.



4. The New Pod Wizard will now help you add an equipment pod to your system.
5. Add a CNSS 4011 Pod.
6. In the New Pod Wizard, click **Next** to continue.
7. When prompted, select the CNSS 4011 Pod and click **Next** to continue.
8. 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

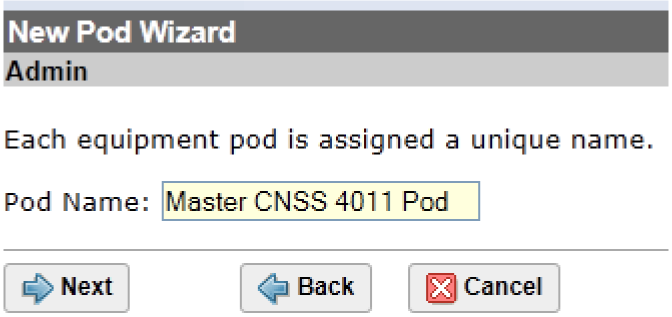
Admin

Each equipment pod is assigned a unique numeric ID.

Please select a Pod ID.

Pod ID: 1

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



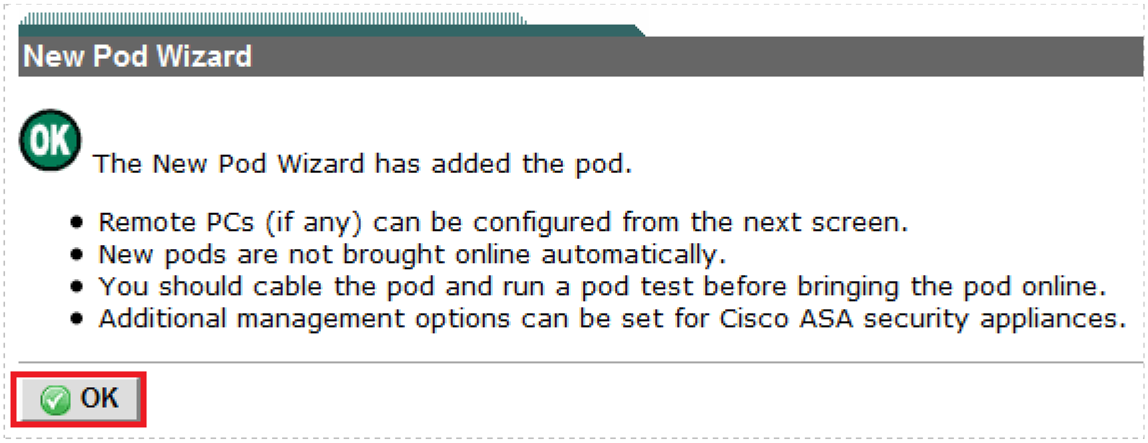
New Pod Wizard

Admin

Each equipment pod is assigned a unique name.

Pod Name: Master CNSS 4011 Pod

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

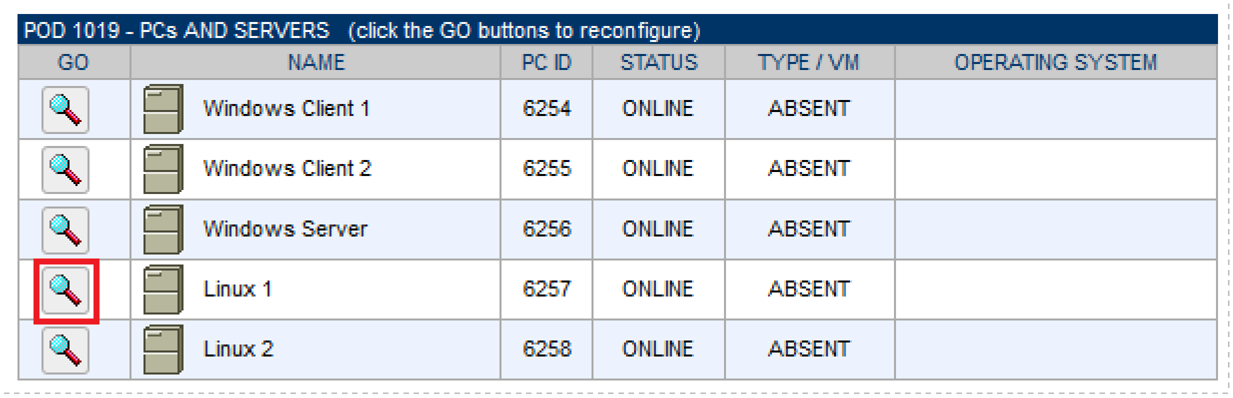


New Pod Wizard

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.

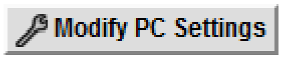
11. Click on the Magnifying Glass icon next to Linux 1. Please note that your PC IDs will not match the graphic below.



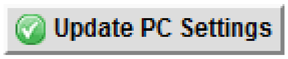
POD 1019 - PCs AND SERVERS (click the GO buttons to reconfigure)

GO	NAME	PC ID	STATUS	TYPE / VM	OPERATING SYSTEM
🔍	Windows Client 1	6254	ONLINE	ABSENT	
🔍	Windows Client 2	6255	ONLINE	ABSENT	
🔍	Windows Server	6256	ONLINE	ABSENT	
🔍	Linux 1	6257	ONLINE	ABSENT	
🔍	Linux 2	6258	ONLINE	ABSENT	

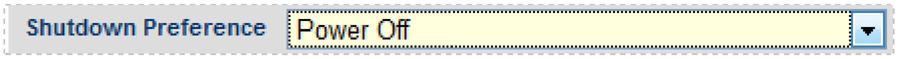
12. Click on Modify PC Settings



13. Change the PC Type drop down box to **Use Virtual Machine Inventory**.
14. In the Base Virtual Machine window, select your **CNSS 4011 Master LINUX1** virtual machine.
15. Review the information on the screen and click **Update PC Settings**.



16. Click **Show Pod**.
17. Repeat Steps 11-16 for the XP1, WIN7, LINUX2, and SERVER1 virtual machines.



Shutdown Preference: Power Off

18. When you have four virtual machines' settings updated, click on **Online** to bring the pod online.
19. Click on **Admin** at the top left of the screen and then click **Logout**.

4 Virtual Machine Configuration

If you have completed and returned the form requesting the preinstalled CNSS 4011 virtual machines from CSSIA (see section 2.3), skip to Section 5 for information about pod cloning and continue following the instructions.

It is preferred that you request the preinstalled CNSS 4011 virtual machines from CSSIA. The configuration of the windows virtual machines follows below. Currently, the Linux based virtual machine configurations are not available. Please contact CSSIA for more information.

Configuration of the virtual machines is only required one time on the Master Pod. Subsequent pods will be created using the pod cloning feature. The *Building Virtual Machines* section of the *Remote PC Guide* covers the creation of virtual machines and the installation of the base Operating systems. When your virtual machines have operating systems installed and have been optimized, you may continue with this section.

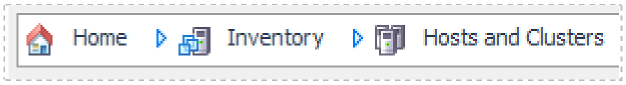
4.1 Virtual Machine Requirements

The memory and hard drive settings for each virtual machine follow below.

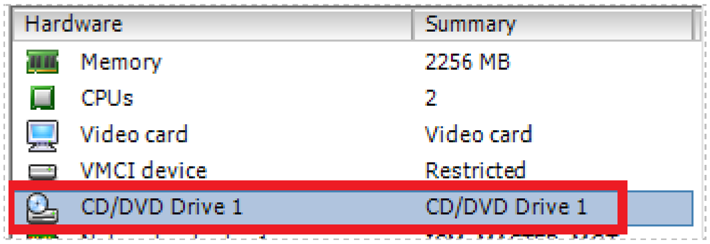
1. **CNSS 4011 Master LINUX1**
    a. Memory – 1 GB
    b. Hard Drive – 10 GB
    c. Operating System – Ubuntu 32-bit
2. **CNSS 4011 Master LINUX2**
    a. Memory – 1 GB
    b. Hard Drive – 10 GB
    c. Operating System – Ubuntu 32-bit
3. **CNSS 4011 Master XP1**
    a. Memory – 1 GB
    b. Hard Drive – 10 GB
    c. Operating System – Windows XP 32-bit
4. **CNSS 4011 Master WIN7**
    a. Memory – 1 GB
    b. Hard Drive – 15 GB
    c. Operating System – Windows 7 32-bit
5. **CNSS 4011 Master SERVER1**
    a. Memory – 1 GB
    b. Hard Drive – 10 GB
    c. Operating System – Windows Server 2003 32-bit

4.2 SERVER1 Setup

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

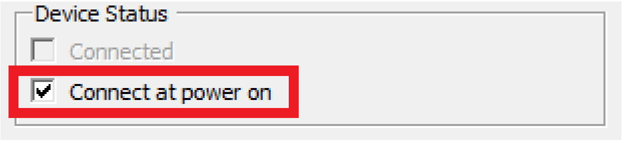


3. Right-click on the virtual machine, **CNSS 4011 Master SERVER1**, under your first ESXi host and select **Edit settings…**
4. Click on **CD/DVD Drive 1** under Hardware.



Hardware	Summary
Memory	2256 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
CD/DVD Drive 1	CD/DVD Drive 1

5. Under Device Type on the right, click on **Datastore ISO File**.
6. Click Browse. Select *your datastore* -> CNSS 4011 Setup -> CNSS 4011 Software.iso. Click OK.
7. Make sure **Connect at power on** is selected under Device Status.



Device Status

□ Connected

☑ Connect at power on

8. Click on **OK** to save changes.
9. Right-click on the virtual machine, **CNSS 4011 Master SERVER1,** under your first ESXi host and select **Power -> Power On.**
10. Right-click on the virtual machine and select **Open Console.**
11. Install Slavasoft Hashcalc.
    a. In the virtual machine console, open My Computer and double click on the CD-ROM.
    b. Open the **CNSS 4011 Software** folder.
    c. Double-click the **hashcalc.zip** file.
    d. Double-click the **setup.exe** file.
    e. On the welcome page, click N**ext**.
    f. On the License Agreement page, accept the license agreement and click **Next**.
    g. On the Destination Folder page, leave the default and click **Next**.
    h. On the Select Start Menu Folder page, leave the default name and click **Next**.

- i. Check the box next to **Create a desktop icon**, leave the box next to **Create a Quick Launch** icon unchecked, and click **Next**.
- j. On the Ready to Install the Program page, click **Install**. The installation should not take long to finish.
- k. Uncheck both check boxes and click **Finish** when the installation is complete.

12. Install Cryptool.
    - a. In the virtual machine console, open My Computer and double click on the CD-ROM.
    - b. Open the **CNSS 4011 Software** folder.
    - c. Double-click the **SetupCrypTool_1_4_30_en.exe** file.
    - d. On the Welcome screen, click **Next**.
    - e. On the License Agreement page, accept the license agreement by clicking **I Agree**.
    - f. On the Destination Folder page, leave the default and click **Install**.
    - g. On the Installation Complete window, click **Next**.
    - h. Uncheck all boxes and click **Finish**.
    - i. Open the Start Menu and navigate to the Cryptool entry.
    - j. Drag the Cryptool icon to the desktop to create a new shortcut.
13. Disconnect the VM from the datastore iso.
    - a. Click on **VM** at the top of the virtual machine console.
    - b. Select **Edit Settings**.
    - c. Click on **CD/DVD Drive 1** on the left hand side under hardware. Uncheck the box next to **Connected** and click the radio button next to **Client Device**.
    - d. Click **OK.**
14. Install DNS and IIS Services.
    - a. Click the **Start** button and choose **Control Panel > Add or Remove Programs**.
    - b. Click the **Add/Remove Windows Components** button.
    - c. Click on **Application Server** and click the **Details** button.
    - d. Check the box next to **Internet Information Service** and click **OK**.
    - e. Click on **Networking Services** and click the **Details** button.
    - f. Check the box next to **Domain Name System** and click **OK**.
    - g. Click on **VM** in the menu bar and choose **Edit Settings**.
    - h. Click on the **CD/DVD Drive** and choose the radio button next to **Datastore ISO file**.
    - i. Navigate to and select the main Windows Server 2003 ISO file (CD 1).
    - j. Check the boxes next to **Connected** and **Connect at power on**.
    - k. Click **OK**.
    - l. Return to the Add Windows components screen and click **Next**.
    - m. You will be asked to setup static IP addressing, use the following values:
        - i. IP Address: **192.168.111.100**
        - ii. Subnet: **255.255.255.0**
        - iii. DNS: **192.168.111.100**
    - n. Click **OK**.

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

   o. Click **Close**.
   p. Click **Finish**.

15. Install Active Directory.
   a. Click the **Start** button.
   b. Click on **Run…**
   c. Enter **dcpromo.exe** in the text box and press **Enter**.
   d. Click **Next**.
   e. Click **Next**.
   f. Choose **Domain controller for a new domain** and click **Next**.
   g. Choose **Domain in a new forest** and click **Next**.
   h. Enter **test.com** in the text box and click **Next**.
   i. Click **Next**.
   j. Click **Next** on the Database and Log folders window.
   k. Click **Next** on the Shared System Volume window.
   l. On the DNS Registration Diagnostics window, select **Install and configure DNS server…** and click **Next**.
   m. Choose **Permissions compatible only…** (second selection) and click **Next**.
   n. Make the Restore Mode Password: **P@ssw0rd** and click **Next**.
   o. Click **Next** on the Summary window. The configuration will take a few minutes.
   p. Click **Finish**.
   q. Click **Restart Now**.

16. Configure Active Directory.
   a. Login to the SERVER1 virtual machine.
   b. Click the **Start** button and navigate to **Administrative Tools > Active Directory Users and Computers**.
   c. Click on the plus sign next to test.com.
   d. Right-click on the **Users** folder and navigate to **New > Group**.
   e. Set the name as **IT Group**, select the radio button next to **Global**, and the radio button next to **Security** and click **OK**.

17. Add User Accounts.
   a. Right-click on the **Users** folder and navigate to **New > User**.
   b. Enter the following credentials:
      i. First name: **Joe**
      ii. Last name: **Admin**
      iii. User logon name: **jadmin**
   c. Click **Next**.
   d. Set the password as **P@ssw0rd**.
   e. The only box that should be checked is **Password never expires**.
   f. Click **Next**.
   g. Click **Finish**.
   h. Right-click the **Joe Admin** user and select **Add to a group**.
   i. Enter **IT Group** in the text box and click **OK**.
   j. Click **OK**.
   k. Right-click on the **Users** folder and navigate to **New > User**.
   l. Enter the following credentials:

        i. First name: **Hacker**
        ii. Last name: **Bob**
        iii. User logon name: **hbob**

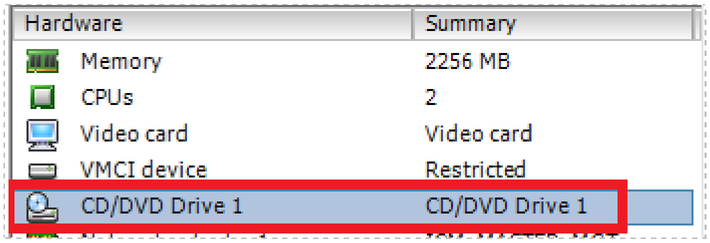
    m. Click **Next**.
    n. Set the password as **P@ssw0rd**.
    o. The only box that should be checked is **Password never expires**.
    p. Click **Next**.
    q. Click **Finish**.
    r. Close the Active Directory Users and Computers window.

18. Disable Windows Firewall.
    a. Click the Start button and select **Control Panel**.
    b. Click the **Windows Firewall** button.
    c. Click the radio button next to **Off (not recommended)** and click **OK**.
19. Create Lab Folders and change file settings.
    a. Click the **Start** button and choose **My Computer**.
    b. Double-click the **Local Disk (C:)** drive.
    c. Right-click a blank area in the window and choose **New > Folder**.
    d. Name the folder **SECRET**.
    e. Right-click the **SECRET** folder and select **Sharing and Security…**
    f. Click the radio button next to **Share this folder**.
    g. Click the **Permissions** button.
    h. Place a check mark next to **Full Control** in the **Allow** column.
    i. Click **OK** in the Permissions window.
    j. Click **OK** in the Properties window.
20. Close all of the open windows and shutdown the virtual machine.
21. Restart the virtual machine and login to each of the user accounts to verify their setup.
22. Shutdown the virtual machine and close the console window.
23. Right-click the **SERVER1** virtual machine and choose **Snapshot > Take Snapshot**.
24. Name the Snapshot **GOLDEN_MASTER**.

4.3 XP1 Setup

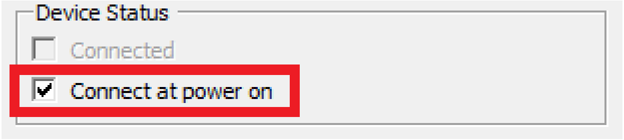
1. Open the vClient on your management workstation. Connect to your vCenter Server.
2. Select **Hosts and Clusters** in the address bar.

3. Right-click on the virtual machine, **CNSS 4011 Master XP1**, under your first ESXi host and select **Edit settings…**
4. Click on **CD/DVD Drive 1** under Hardware.



Hardware	Summary
Memory	2256 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
CD/DVD Drive 1	CD/DVD Drive 1

5. Under Device Type on the right, click on **Datastore ISO File**.
6. Click Browse. Select *your datastore* -> CNSS 4011 Setup -> CNSS 4011 Software.iso. Click **OK**.
7. Make sure **Connect at power on** is selected under Device Status.



Device Status
□ Connected
☑ Connect at power on

8. Click on **OK** to save changes.
9. Right-click on the virtual machine, **CNSS 4011 Master XP1,** under your first ESXi host and select **Power -> Power On.**
10. Right-click on the virtual machine and select **Open Console.**
11. Install Slavasoft Hashcalc.
    a. In the virtual machine console, open My Computer and double click on the CD-ROM.
    b. Open the **CNSS 4011 Software** folder.
    c. Double-click the **hashcalc.zip** file.
    d. Double-click the **setup.exe** file.
    e. On the welcome page, click N**ext**.
    f. On the License Agreement page, accept the license agreement and click **Next**.
    g. On the Destination Folder page, leave the default and click **Next**.
    h. On the Select Start Menu Folder page, leave the default name and click **Next**.
    i. Check the box next to Create a desktop icon, leave the box next to **Create a Quick Launch icon** unchecked, and click **Next**.
    j. On the Ready to Install the Program page, click **Install**. The installation should not take long to finish.
    k. Uncheck both check boxes and click **Finish** when the installation is complete.
12. Install Nmap.
    a. In the virtual machine console, open My Computer and double click on the CD-ROM.
    b. Open the **CNSS 4011 Software** folder.
    c. Double-click the **nmap-5.51-vs9-setup.exe** file. (You may have downloaded a newer version, which should not affect the labs.)

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

   d. On the License Agreement page, accept the license agreement by clicking **I Agree**.
   e. Leave the defaults and click **Next**.
   f. On the Destination Folder page, leave the default and click **Next**.
   g. Click **Install**.
   h. On the Create Shortcuts window, verify both boxes are checked and click **Next**.
   i. Click **Finish**.

13. Install PuTTy.
   a. In the virtual machine console, open My Computer and double click on the CD-ROM.
   b. Open the **CNSS 4011 Software** folder.
   c. Drag the **putty.exe** icon from the CNSS 4011 folder to the desktop.
14. Install the map-h.drive.bat file.
   a. In the virtual machine console, open My Computer and double click on the CD-ROM.
   b. Open the **CNSS 4011 Software** folder.
   c. Drag the **map-h.drive.bat** icon from the CNSS 4011 folder to the desktop.
15. Install Wireshark.
   a. In the virtual machine console, open My Computer and double click on the CD-ROM.
   b. Open the **CNSS 4011 Software** folder.
   c. Double-click the **wireshark-win32-1.6.1** file. (You may have downloaded a newer version, which should not affect the labs.)
   d. On the Welcome page, click **Next**.
   e. On the License Agreement page, accept the license agreement by clicking **I Agree**.
   f. Check the Start Menu Item and Desktop Icon boxes, uncheck the Quick Launch Icon box, and click **Next**.
   g. On the Destination Folder page, leave the default and click **Next**.
   h. Click **Install**.
   i. Click **Finish**.
16. Install Ophcrack.
   a. In the virtual machine console, open My Computer and double click on the CD-ROM.
   b. Open the **CNSS 4011 Software** folder.
   c. Double-click the **ophcrack-win32-installer-3.3.1.exe** file. (You may have downloaded a newer version, which should not affect the labs.)
   d. If you see a security warning window open, click **Run**.
   e. On the Welcome screen, click **Next**.
   f. On the License Agreement page, click the check box next to **I accept…** and click **Next**.
   g. On the Choose Setup Type window, click **Typical**.
   h. Click **Install**.
   i. On the Installation Complete window, click **Next**.
   j. Click **Finish**.

17. Install Cryptool.
    a. In the virtual machine console, open My Computer and double click on the CD-ROM.
    b. Open the **CNSS 4011 Software** folder.
    c. Double-click the **SetupCrypTool_1_4_30_en.exe** file.
    d. On the Welcome screen, click **Next**.
    e. On the License Agreement page, accept the license agreement by clicking **I Agree**.
    f. On the Destination Folder page, leave the default and click **Install**.
    g. On the Installation Complete window, click **Next**.
    h. Uncheck all boxes and click **Finish**.
    i. Open the Start Menu and navigate to the Cryptool entry.
    j. Drag the Cryptool icon to the desktop to create a new shortcut.
18. Install Eraser.
    a. In the virtual machine console, open My Computer and double click on the CD-ROM.
    b. Open the **CNSS 4011 Software** folder.
    c. Double-click the **Eraser 6.0.8.2273.exe** file. (You may have downloaded a newer version that should not affect the labs.)
    d. On the Welcome screen, click **Next**.
    e. On the License Agreement page, accept the license agreement by clicking **I Agree**.
    f. Click **Install**.
    g. On the Installation Complete window, click **Finish**.
19. Install Advanced Port Scanner.
    a. In the virtual machine console, open My Computer and double click on the CD-ROM.
    b. Open the **CNSS 4011 Software** folder.
    c. Double-click the **pscan13.zip** file. (You may have downloaded a newer version, which should not affect the labs.)
    d. Extract the **pscan13.exe** file to the desktop.
    e. Double-click the **pscan13.exe** file that is now on your desktop.
    f. On the License Agreement page, click the check box next to **I accept…** and click **Next**.
    g. On the Destination Folder page, leave the default and click **Start**.
    h. After installation, an empty window may open. If it does, close it.
    i. Go to the Start Menu and find the Advanced Port Scanner entry.
    j. Drag the Advanced Port Scanner Icon to the desktop to create a new shortcut.
20. Install Restoration.
    a. In the virtual machine console, open My Computer and double click on the CD-ROM.
    b. Open the **CNSS 4011 Software** folder.
    c. Double-click **REST2514.EXE**.
    d. Click **Run**.
    e. Leave the default location and click **Unzip**.

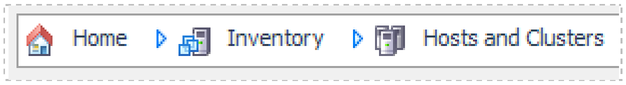
f. Click **OK**.
g. Click **Close**.
h. Open **My Computer** and double-click the **C:** drive.
i. Double-click the **Restoration** folder.
j. Right-click the Restoration file and select **Create Shortcut**.
k. Drag the new shortcut to the desktop.
l. Close any windows that are currently open.

21. Disconnect the VM from the datastore iso.
    a. Click on **VM** at the top of the virtual machine console.
    b. Select **Edit Settings**.
    c. Click on **CD/DVD Drive 1** on the left hand side under hardware. Uncheck the box next to **Connected** and click the radio button next to **Client Device**.
    d. Click **OK.**
22. Change network settings.
    a. Click the **Start** Button and choose **Control Panel**.
    b. Click on **Network and Internet Connections**.
    c. Click **Network Connections** in the lower right portion of the screen.
    d. Right-click the **Local Area Connection** and choose **Properties**.
    e. Click on **Internet Protocol (TCP/IP)** and click the **Properties** button.
    f. Enter the IP address as **192.168.111.41**, the Subnet mask as **255.255.255.0**, and the Preferred DNS Server as **192.168.111.100**.
    g. Click **OK**.
23. Change system settings.
    a. Click on the **Switch to Classic View** link in the Control Panel window.
    b. Double-click on the **System** icon.
    c. Change to the **Computer Name** tab.
    d. Click the **Change** button and change the computer name to **XP1**.
    e. Click on the **Domain:** radio button.
    f. Make **test.com** the domain and click **OK**.
    g. Click **OK** in the Computer Name Changes window.
    h. Click **OK** in the System Properties window.
    i. Close the Control Panel window and return to the desktop.
24. Create Local Accounts.
    a. Click the **Start** button and choose **Control Panel**.
    b. Click on **User Accounts**.
    c. Click on the **Advanced** tab.
    d. Click the **Advanced** button under Advanced user management.
    e. Right-click on the **Users** folder and choose **New User**.
    f. Enter **jadmin** for the username, **Joe Admin** for the full name, and **password** as the password.
    g. Uncheck the checkbox next to **User must change password** at logon.
    h. Check the checkbox next to **Password never expires** and click **Create**.
    i. Repeat the process to create the **hbob** user, with a full name of **Hacker Bob** and the password as **password**.
    j. Keep the Local Users and Groups window open for the next step.

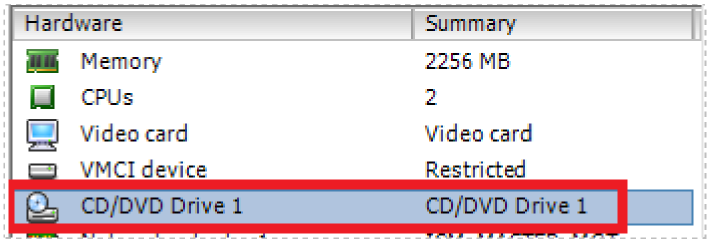
25. Manage Local Accounts.
    a. Right-click on the **Administrator** user and choose **Set Password**.
    b. You will get a warning window. Click **OK.**
    c. Change the Administrator password to **P@ssw0rd** and click **OK**.
    d. Right-click on the **Guest** user and choose **Set Password**.
    e. Change the Guest password to **password1** and click **OK**.
26. Disable Windows Firewall.
    a. Close all windows except **Control Panel**.
    b. Double-click the **Windows Firewall** button.
    c. Click the radio button next to **Off (not recommended)** and click **OK**.
    d. Close **Control Panel**.
27. Create Lab Folders and change file settings.
    a. Click the **Start** button and choose **My Computer**.
    b. Double-click the **Local Disk (C:)** drive.
    c. Right-click a blank area in the window and choose **New > Folder**.
    d. Name the folder **SECRET**.
    e. Use the same process to create the **IMPORTANT** folder.
    f. Click **Tools** on the menu bar and choose **Folder Options**.
    g. Verify that the checkbox next to **Hide extensions for known file types** is unchecked and click **OK**.
28. Close all of the open windows and shutdown the virtual machine.
29. Restart the virtual machine and login to each of the user accounts to verify their setup.
30. Shutdown the virtual machine and close the console window.
31. Right-click the XP1 virtual machine and choose **Snapshot > Take Snapshot**.
32. Name the snapshot **GOLDEN_MASTER**.

4.4 WIN7 Setup

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

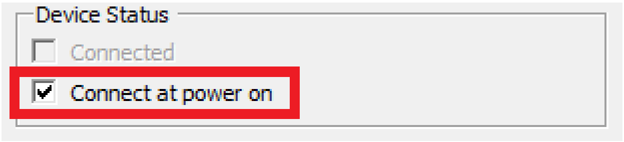


3. Right-click on the virtual machine, **CNSS 4011 Master WIN7**, under your first ESXi host and select **Edit settings…**
4. Click on **CD/DVD Drive 1** under Hardware.



Hardware	Summary
Memory	2256 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
CD/DVD Drive 1	CD/DVD Drive 1

5. Under Device Type on the right, click on **Datastore ISO File**.
6. Click Browse. Select *your datastore* -> CNSS 4011 Setup -> CNSS 4011 Software.iso. Click OK.
7. Make sure **Connect at power on** is selected under Device Status.



Device Status
□ Connected
☑ Connect at power on

8. Click on **OK** to save changes.
9. Right-click on the virtual machine, **CNSS 4011 Master WIN7,** under your first ESXi host and select **Power -> Power On.**
10. Right-click on the virtual machine and select **Open Console.**
11. Install PuTTy.
    a. In the virtual machine console, open My Computer and double click on the CD-ROM.
    b. Open the **CNSS 4011 Software** folder.
    c. Drag the **putty.exe** icon from the CNSS 4011 folder to the desktop.
12. Install the map-h.drive.bat file.
    a. In the virtual machine console, open My Computer and double click on the CD-ROM.
    b. Open the **CNSS 4011 Software** folder.
    c. Drag the **map-h.drive.bat** icon from the CNSS 4011 folder to the desktop.
13. Install Wireshark.
    a. In the virtual machine console, open My Computer and double click on the CD-ROM.
    b. Open the **CNSS 4011 Software** folder.
    c. Double-click the **wireshark-win32-1.6.1** file. (You may have downloaded a newer version, which should not affect the labs.)
    d. On the Welcome page, click **Next**.
    e. On the License Agreement page, accept the license agreement by clicking **I Agree**.
    f. Check the **Start Menu Item** and **Desktop Icon** boxes, uncheck the **Quick Launch Icon** box, and click **Next**.
    g. On the Destination Folder page, leave the default and click **Next**.
    h. Click **Install**.
    i. Click **Finish**.
14. Disconnect the VM from the datastore iso.

   a. Click on **VM** at the top of the virtual machine console.
   b. Select **Edit Settings**.
   c. Click on **CD/DVD Drive 1** on the left hand side under hardware. Uncheck the box next to **Connected** and click the radio button next to **Client Device**.
   d. Click **OK.**

15. Change network settings.
    a. Click the **Start** Button and choose **Control Panel**.
    b. Click on **Network and Sharing Center**.
    c. Click **Change adapter settings** in the upper left portion of the screen.
    d. Right-click the **Local Area Connection** and choose **Properties**.
    e. Click on **Internet Protocol Version 4(TCP/IPv4)** and click the **Properties** button.
    f. Enter the IP address as **192.168.111.57**, the Subnet mask as **255.255.255.0**, and the Preferred DNS Server as **192.168.111.100**.
    g. Click **OK**.
16. Change system settings.
    a. Click on the **Switch to Classic View** link in the Control Panel window.
    b. Double-click on the **System** icon.
    c. Click on the **Advanced system settings** link.
    d. Change to the **Computer Name** tab.
    e. Click the **Change** button and change the computer name to **WIN7**.
    f. Click on the **Domain:** radio button.
    g. Make **test.com** the domain and click **OK**.
    h. Click **OK** in the Computer Name Changes window.
    i. Click **OK** in the System Properties window.
    j. Return to the desktop.
17. Create Local Accounts.
    a. Click the **Start** button and choose **Control Panel**.
    b. Click on **User Accounts**.
    c. Change the Administrator password to **P@ssw0rd**.
    d. Create the **Guest** account with **password1** as the password.
    e. Create the **User** account with the password **P@ssw0rd**.
18. Disable Windows Firewall.
    a. Close all windows except **Control Panel**.
    b. Click the **Windows Firewall** link.
    c. Click the **Turn Windows Firewall on or off** link.
    d. Click the radio button next to **Turn Off Windows Firewall (not recommended)** and click **OK**.
    e. Close **Windows Firewall**.
19. Install Internet Information Services.
    a. Click the **Start** button and choose **Control Panel**.
    b. Click on **Programs and Features**.
    c. Click on **Turn Windows features on or off** in the upper left of the window.
    d. Click the check box next to **Internet Information Services** and **Telnet Server.**

e. Click **OK**.
f. Click **Restart Now**. This process may take a few minutes.

20. Create the default web page.
    a. Login to the User account.
    b. Right-click the desktop and select **New > Text Document**.
    c. Double-click **New Text Document.txt**.
    d. Type the following lines into the file:

```
<HTML>
<HEAD>
<TITLE>
Broken Internet
</TITLE>
<b>WOW</b>
I broke the internet.<br/>
Thank you and have a nice day. :) <br/>
</HEAD>
</HTML>
```

    e. Click **File > Save As…**
    f. Scroll down to **Computer** in the left pane and click on it.
    g. Select **Local Disk (C:)**.
    h. Double-click **inetpub**.
    i. Double-click **wwwroot**.
    j. Change the filename to **index.html** and click **Save**.
    k. If you get a warning that the file already exists, click **Yes** to continue.
    l. Close Notepad and delete the New Text Document.txt from the desktop.
21. Close all of the open windows and shutdown the virtual machine.
22. Restart the virtual machine and login to each of the user accounts to verify their setup.
23. Shutdown the virtual machine and close the console window.
24. Right-click the **WIN7** virtual machine and choose **Snapshot > Take Snapshot**.
25. Name the snapshot **GOLDEN_MASTER**.

5 Pod Cloning

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

6 Assigning CNSS 4011 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.

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