



UNIVERSITY OF
SOUTH CAROLINA

Cybersecurity Fundamentals v1.0

Installation and Configuration Guide

Document Version: **2024-04-08**

Copyright © 2024 Network Development Group, Inc.
www.netdevgroup.com

Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and other countries.
KALI LINUX™ is a trademark of Offensive Security.
NETLAB+ is a registered trademark of Network Development Group, Inc.
VMware is a registered trademark of VMware, Inc.

Contents

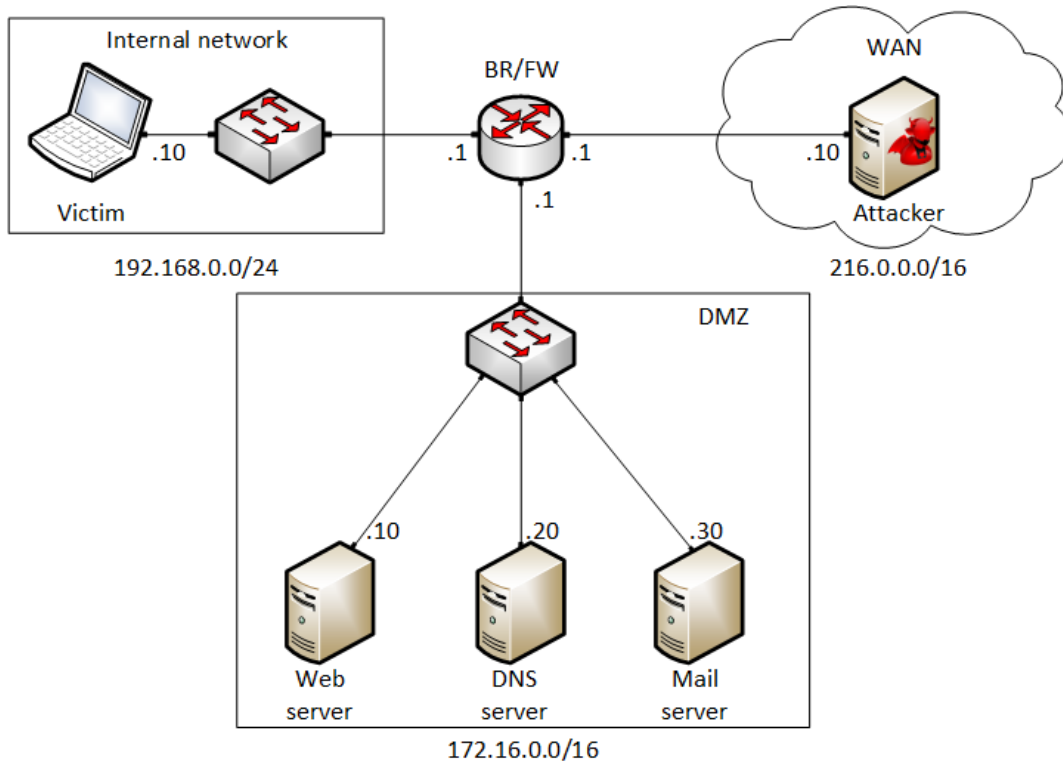
1	Introduction	3
1.1	Introducing the Cybersecurity Fundamentals v1.0 Pod	3
2	Planning.....	4
2.1	Pod Creation Workflow.....	4
2.2	Pod Resource Requirements.....	5
2.3	ESXi Host Server Requirements	5
2.4	NETLAB+ Requirements	5
2.5	NETLAB+ Virtual Machine Infrastructure Setup	6
2.6	Software Requirements	6
2.7	Networking Requirements.....	6
3	Software and Licenses	7
3.1	Obtaining Windows Software Licenses	7
3.2	Downloading OVF Files	7
4	Master Pod Configuration.....	9
4.1	Deploying Virtual Machine OVF/OVA Files.....	9
4.1.1	Modify Virtual Machines.....	10
4.2	NETLAB+ Virtual Machine Inventory Setup	13
4.3	Building the Master Cybersecurity Fundamentals v1.0 Pod	14
4.3.1	Enabling Labs in Course Manager.....	14
4.3.2	Create the Master Pod.....	14
4.3.3	Attach Virtual Machines to the Master Pod	16
4.3.4	Create Snapshots for the Master Virtual Machines	17
4.3.5	Set the Revert to Snapshot	19
4.4	Make changes to the Master Pod.....	20
4.4.1	Virtual Machine Credentials	21
4.4.2	Bring the Master Pod Online	21
4.4.3	Create Class and Schedule the Master Pod	21
4.4.4	Provide Temporary Internet Access to the Victim VM	22
4.4.5	License and Activate the Victim VM	22
4.4.6	Revert Back the Original TCP/IP Settings.....	23
4.4.7	Shut Down the Victim VM.....	23
4.4.8	Reset the NIC to SAFETY NET	23
4.4.9	Take New Snapshots for the Changed Master Virtual Machines.....	23
4.4.10	End Reservation	23
5	Pod Cloning.....	23
5.1	Linked Clones and Full Clones.....	24
5.2	Creating User Pods.....	24
5.3	Copying Your Master Pod to the Second Host	26
5.4	Creating User Pods on the Second Host	28
5.5	Assigning Pods to Students, Teams, or Classes	28

1 Introduction

This document provides detailed guidance on performing the installation and configuration of the *Cybersecurity Fundamentals v1.0* pod on the *NETLAB+ VE* system.

1.1 Introducing the Cybersecurity Fundamentals v1.0 Pod

The *Cybersecurity Fundamentals v1.0* pod is a 100% virtual machine pod consisting of six virtual machines. Linked together through virtual networking, these six virtual machines provide the environment for a student or a team to perform the *Cybersecurity Fundamentals v1.0* labs.



2 Planning

This guide provides specific information pertinent to delivering the *Cybersecurity Fundamentals v1.0* pod. 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 Pod Creation Workflow

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

1. Obtain the master virtual machine images required for the master pod.
2. Deploy the master virtual machine images to your *VMware vCenter Appliance*.
 - a. Deploy virtual machines using **Thin Provisioning** to reduce storage consumption.
 - b. Make necessary adjustments to each virtual machine in the environment.
 - i. Insert/Verify manual **MAC** addresses.
 - ii. Change the default network to **SAFETY NET**.
 - iii. Any other configuration changes mentioned in this guide.
3. Import the deployed virtual machines to the *NETLAB+ Virtual Machine Inventory*.
4. Activate or license the required software on each virtual machine when prompted.
5. Take a snapshot of each virtual machine in the master pod labeled **GOLDEN_MASTER** after all configurations and licensing have taken effect. The *GOLDEN_MASTER* snapshot is used to clone virtual machine images for the user pods.
6. Use the *NETLAB+ Pod Cloning* feature to create student pods from the master pod.
7. If multiple hosts are used in the *NETLAB+* environment, make a **Full Clone** of the master pod on the initial host (Host A) to the subsequent host (Host B) and so on using the *NETLAB+ Pod Cloning* feature.

2.2 Pod Resource Requirements

The *Cybersecurity Fundamentals v1.0* course will consume 70.0 GB of storage per each master pod instance.

The following table provides details of the storage requirements for each of the virtual machines in the pod.

Virtual Machine	OVF/OVA	Initial Master Pod (Thin Provisioned)	Maximum Allocated Memory
Attacker	10.2 GB	28.2 GB	4 GB
BF/FW	1.3 GB	3.8 GB	2 GB
DNS server	1.2 GB	2.9 GB	2 GB
Mail server	3.0 GB	7.2 GB	4 GB
Victim	13.2 GB	23.2 GB	8 GB
Web server	1.3 GB	4.7 GB	2 GB
Total	30.2 GB	70.0 GB	22 GB

2.3 ESXi Host Server Requirements

Please refer to the *NDG* website for specific *ESXi* host requirements to support virtual machine delivery: <https://www.netdevgroup.com/products/requirements/>

The deployment of the *Cybersecurity Fundamentals v1.0* pod requires VMware ESXi version of **6.0** or greater.

Please Note

The number of **active** pods that can be used simultaneously depends on the *NETLAB+* product license and the number of *VMware ESXi* host servers meeting the hardware requirements specifications.

For current *ESXi* server requirements and active pod count, refer to the following URL:

http://www.netdevgroup.com/support/remote_pc.html#vm_host_server_specifications.

2.4 NETLAB+ Requirements

Installation of *Cybersecurity Fundamentals v1.0* pods, as described in this guide, requires that you are running *NETLAB+ VE*.

Previous versions of *NETLAB+* do not support requirements for the *Cybersecurity Fundamentals v1.0* course on the physical host servers.

Please refer to the [NETLAB+ Remote PC Guide Series](#).

2.5 NETLAB+ Virtual Machine Infrastructure Setup

The *NETLAB+ Virtual Machine Infrastructure* setup is described in the following sections of the [NETLAB+ Remote PC Guide Series](#):

- *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.

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

Virtual Infrastructure Requirements	
Software	Version
vSphere ESXi	6.0
vCenter Server	6.0

Please refer to the *Software and Licenses* section regarding the software requirements for virtual machines in the pod.

2.7 Networking Requirements

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

The two standard networking models recommended to interconnect your servers are described in detail in the *Networking Models* section of the [Remote PC Guide Series, Volume 1 - Introduction and Planning](#).

3 Software and Licenses

3.1 Obtaining Windows Software Licenses

The following table lists the software that is required for the virtual machines inside the *Cybersecurity Fundamentals v1.0* pod. Your organization needs to be a member of the vendor programs listed in the *Source* column to obtain and use the licenses. To subscribe to the *Microsoft Azure Dev Tools for Teaching* program, visit: <https://azureforeducation.microsoft.com/en-us/Institutions>.

Pod Software Requirements		
Software	Version	Source
Windows	10 Education (64-bit)	Azure Dev Tools for Teaching

To enable all features of the *Windows*-based virtual machines, licensing will be required, followed through with activations for the master virtual machines only. This needs to be done before cloning.



For more information regarding the *Microsoft Azure Dev Tools for Teaching* program, you may visit their FAQ page: <https://azure.microsoft.com/en-us/education/institutions/dev-tools-for-teaching-faq/>.

It is recommended to acquire the *Multiple Activation Key (MAK)* lab key license for a specified *Windows* product. This type of key enables you to activate multiple installations of a product with the same key.

Please note that activating licenses is only required on master pods. Doing a *Link Clone* of the master pod will preserve the activation on the cloned VMs in the user pods. It is important to note that when activating *Windows*, the VMs have temporary Internet access so that they can contact *Microsoft Licensing Servers*.

3.2 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: <https://www.cssia.org/cssiaresources/>
2. Select **CSSIA VM Image Sharing Agreement**.
3. Complete and submit your access request by following the instructions on the request form.

4. CSSIA will provide, via email, password-protected download links. Access to the download links 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, Red Hat Academy, and/or Palo Alto Networks*).
5. Once all virtual machines have been downloaded, they can be deployed following the steps in the appropriate pod installation guide. Each virtual machine is deployed individually.

4 Master Pod Configuration

4.1 Deploying Virtual Machine OVF/OVA Files

Deploy on your host server the pod virtual machine *OVF/OVA* files you have downloaded.

1. Navigate to your **vSphere Client** using your management workstation, ensure that your downloaded *OVA/OVF* files are accessible on this machine, and then connect to your **vCenter Server**.
2. From the *vSphere Client* interface, navigate to **Hosts and Clusters**.
3. Right-click on the target **ESXi Host Server** and select **Deploy OVF Template**.
4. In the *Deploy OVF Template* window, on the *Select source* step, select the **Local File** radio button and click **Browse**.
5. Locate and select one of the VMs for the pod, click **Open**.

VM Name	VM OS	Virtual Machine OVA Name
Attacker	Kali	UofSC_CSF_FM.Attacker
BF/FW	CentOS 7	UofSC_CSF_FM.BRFW
DNS server	CentOS 7	UofSC_CSF_FM.DNS
Mail server	CentOS 7	UofSC_CSF_FM.Mail
Victim	Windows 10 Education	UofSC_CSF_FM.Victim
Web server	CentOS 7	UofSC_CSF_FM.Web

Please Note

Only one VM can be selected using this wizard. The process will have to be repeated for the remaining VMs.

6. Verify that the VM information populates next to the *Browse* button and click **Next**.
7. On the *Review details* step, make sure to fill the checkbox for **Accept extra configuration options (if present)** and click **Next**.
8. On the *Select name and folder* step, change the name of the virtual machine to something that is easy to manage. You can use the names provided in the list below as names for the virtual machines if you do not have a set naming convention. Select the appropriate **datacenter** and click **Next**.

VM Name	VM OS	Virtual Machine Deployment Name
Attacker	Kali	UofSC_CSF_Master.Attacker
BF/FW	CentOS 7	UofSC_CSF_Master.BRFW
DNS server	CentOS 7	UofSC_CSF_Master.DNS
Mail server	CentOS 7	UofSC_CSF_Master.Mail
Victim	Windows 10 Education	UofSC_CSF_Master.Victim
Web server	CentOS 7	UofSC_CSF_Master.Web

9. On the *Select Storage* step, choose the appropriate storage device and make sure that **Thin Provision** is selected. Click **Next**.
10. In the *Setup networks* section, select **SAFETY NET** as the destination and click **Next**.



If *SAFETY NET* is not available, refer to the *Create a Safe Staging Network* section in the [Remote PC Guide Series – Volume 2](#).

11. In the *Ready to complete* section, make sure **Power on after deployment** is **unchecked** and confirm the settings. Click **Finish**.
12. *vCenter* will begin deploying the virtual machine. This may take some time, depending on the speed of your connection, HDDs, etc. Repeat the previous steps for each remaining virtual machine in the master pod.

4.1.1 Modify Virtual Machines

Once the virtual machines are imported onto the host, verify the configurations. The following steps will guide you through the process.


1. In the *vSphere Client* interface, right-click on the imported virtual machine and select **Edit Settings**.
2. For all the virtual machines, manually assign the *MAC* addresses for each *NIC*. The table below identifies the *MAC* addresses per *NIC*.

Virtual Machine	NIC	MAC
Attacker	1	00:50:56:b3:ae:10
BR/FW	1	00:50:56:b3:57:c3
	2	00:50:56:b3:f7:38
	3	00:50:56:b3:69:2c
DNS server	1	00:50:56:b3:bd:6c
Mail server	1	00:50:56:b3:ee:d5
Victim	1	00:50:56:b3:1a:e7
Web server	1	00:50:56:b3:f7:b0

Edit Settings | UofSC_CSF_Master.Attacker



Virtual Hardware VM Options ADD NEW DEVICE ▾

> CPU	2 ▾	
> Memory	4 ▾	GB ▾
> Hard disk 1	30	GB ▾
> SCSI controller 0	VMware Paravirtual	
▾ Network adapter 1	SAFETY NET ▾	
Status	<input checked="" type="checkbox"/> Connect At Power On	
Adapter Type	VMXNET 3 ▾	
DirectPath I/O	<input checked="" type="checkbox"/> Enable	
MAC Address	00:50:56:b3:ae:10	Manual ▾
> CD/DVD drive 1	Client Device ▾	<input type="checkbox"/> Connect...
> Video card	Specify custom settings ▾	
VMCI device		
> Other	Additional Hardware	

3. While in the *Edit Settings* window, click on the **VM Options** tab and expand the **VMware Tools** section. Check the checkbox for **Synchronize guest time with host/Synchronize at startup and resume** to enable the feature. Click **OK** to save the configuration.

Edit Settings | UofSC_CSF_Master.Attacker X

Virtual Hardware VM Options

> General Options	VM Name: UofSC_CSF_Master.Attacker
> VMware Remote Console Options	<input type="checkbox"/> Lock the guest operating system when the last remote user disconnects
> Encryption	Expand for encryption settings
> Power management	Expand for power management settings
v VMware Tools	
Power Operations	<input type="checkbox"/> Power On / Resume VM <input type="checkbox"/> Shut Down Guest (Default) v <input type="checkbox"/> Suspend (Default) v <input type="checkbox"/> Restart Guest (Default) v
Tools Upgrades	<input type="checkbox"/> Check and upgrade VMware Tools before each power on
Synchronize Time with Host i	<input checked="" type="checkbox"/> Synchronize at startup and resume (recommended) <input type="checkbox"/> Synchronize time periodically
Run VMware Tools Scripts	<input checked="" type="checkbox"/> After powering on <input checked="" type="checkbox"/> After resuming <input checked="" type="checkbox"/> Before suspending <input checked="" type="checkbox"/> Before shutting down guest
> Boot Options	Expand for boot options
> Advanced	Expand for advanced settings
> Fibre Channel NPIV	Expand for Fibre Channel NPIV settings

CANCEL
OK

- Repeat the previous steps for each of the remaining virtual machines in the master pod.

4.2 NETLAB+ Virtual Machine Inventory Setup

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

1. Log in to your *NETLAB+ VE* system using the administrator account.
2. Select the **Virtual Machine Infrastructure** icon.



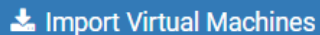
3. Click the **Virtual Machine Inventory** icon.




Virtual Machine Inventory

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

4. Click the **Import Virtual Machines** button located at the bottom of the list.

A blue rectangular button with rounded corners. On the left, there is a white download icon (a square with a downward arrow). To the right of the icon, the text "Import Virtual Machines" is written in white.

5. Select the appropriate datacenter from the list where your master VMs reside.
6. Select the checkbox next to the virtual machines you had just deployed and click **Import Selected Virtual Machines**.


A blue rectangular button with rounded corners. On the left, there is a white download icon (a square with a downward arrow). To the right of the icon, the text "Import Selected Virtual Machines" is written in white.

7. When the *Configure VMs* window loads, you can set your virtual machine parameters.
 - a. Check the dropdown box for the correct operating system for each imported virtual machine.
 - b. Change *Role* to **Master** for each VM.
 - c. Add any comments for each virtual machine in the last column.



It is advised to leave the *Version* and *Build* numbers for reference when requesting *NDG* support.

- d. Verify your settings and click **Import (X) Virtual Machines** (notice the number in parenthesis is dynamic, depending on the amount of VMs selected).

A blue rectangular button with rounded corners. On the left is a white download icon (a square with a downward-pointing triangle). To the right of the icon, the text "Import (6) Virtual Machines" is written in white. The number "6" is in parentheses.

- e. Verify all *Import Statuses* report back with *OK* and then click on the **Dismiss** button.
- f. Verify that your virtual machines show up in the inventory.

For additional information, please refer to the [NETLAB+ VE Administrator Guide](#).

4.3 Building the Master Cybersecurity Fundamentals v1.0 Pod

This section will assist you in adding the *Cybersecurity Fundamentals v1.0* pod to your *NETLAB+* system.

4.3.1 Enabling Labs in Course Manager

Please refer to the *Course Manager* section of the [NETLAB+ VE Administrator Guide](#) on how to enable content. Please install the **UofSC – Cybersecurity Fundamentals – v1.0** course.

4.3.2 Create the Master Pod


1. Log into **NETLAB+ VE** with the *administrator* account.
2. Select the **Pods** icon.



3. Create a new pod by scrolling to the bottom and clicking the **Create New Pod** button.

A blue rectangular button with rounded corners. On the left is a white plus sign icon. To the right of the icon, the text "Create New Pod" is written in white.


- Then, click on the **UofSC Cybersecurity Fundamentals** pod entry from the list of installed pod types.

	<p>UofSC Cybersecurity Fundamentals</p> <p>The Cybersecurity Fundamentals training helps provide learners the skills to safeguard digital systems, detect vulnerabilities, and ethically defend against cyber threats.</p> <p>2024 Copyright (C) Network Development Group, Inc.</p> <p>https://www.netdevgroup.com/support/tech_support.html</p>
---	--

- On the *New Pod* window, input a value into the **Pod ID** and **Pod Name** fields. Click **Next**.

New Pod

Pod Type



Pod ID

Pod Name

Used Pod IDs

1
2
1005
1010
1015
1020
1025



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

The **Pod Name** identifies the pod and is unique per pod. Here we used the name of the lab set or course in a shortened form along with a host identifier (H120), the type and number of the pod (M1000).

- To finalize the wizard, click **OK**.

For additional information, please refer to the [NETLAB+ VE Administrator Guide](#).

4.3.3 Attach Virtual Machines to the Master Pod

Update the master pod to associate the virtual machines with the newly created pod.

1. Select the **Cybersecurity Fundamentals v1.0** master pod from the pod list.

1000	 UNIVERSITY OF SOUTH CAROLINA Cybersecurity Fundamentals	UofSC_CSF_H120_M1000
------	--	----------------------

2. Click on the **Action** dropdown next to the virtual machine you are about to assign and select **Attach VM**.

Remote PC 6						
	PC Name	VM	Operating System	VM Role	Runtime Host	Action
	Victim	ABSENT				
	BR/FW	ABSENT				<ul style="list-style-type: none"> View Settings <li style="border: 2px solid red;"> Attach VM Remove VM From... Snapshots
	Attacker	ABSENT				
	Web server	ABSENT				
	DNS server	ABSENT				
	Mail server	ABSENT				

3. Select the corresponding virtual machine from the inventory list.

Victim (select virtual machine)		
Virtual Machine Name	Operating System	Role
UofSC_CSF_Master.Attacker	Linux	Master
UofSC_CSF_Master.BRFW	Linux	Master
UofSC_CSF_Master.DNS	Linux	Master
UofSC_CSF_Master.Mail	Linux	Master
UofSC_CSF_Master.Victim	Windows 10	Master
UofSC_CSF_Master.Web	Linux	Master

- Click **OK** to confirm the VM attachment and repeat the previous steps for the remaining virtual machines.


















4.3.4 Create Snapshots for the Master Virtual Machines

In order to proceed with pod cloning, snapshots must be created on each of the pod's virtual machines.



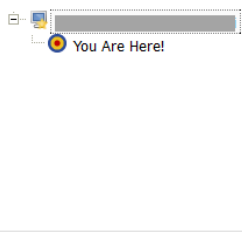
Verify that all VMs are powered off before taking snapshots.

- Make sure to view the **Cybersecurity Fundamentals v1.0** master pod you just assigned machines to. In the pod view, click on the dropdown menu option underneath the *Action* column for a specific VM and select **Snapshots**.

Remote PC 6						
PC Name	VM	Operating System	VM Role	Runtime Host	Action	
 Victim	UofSC_CSF_Master.Victim	Windows 10	MASTER			
 BR/FW	UofSC_CSF_Master.BRFW	Linux	MASTER	1	<ul style="list-style-type: none">  View  Settings  Attach VM  Remove VM From...  Snapshots 	
 Attacker	UofSC_CSF_Master.Attacker	Linux	MASTER	1		
 Web server	UofSC_CSF_Master.Web	Linux	MASTER	1		
 DNS server	UofSC_CSF_Master.DNS	Linux	MASTER			
 Mail server	UofSC_CSF_Master.Mail	Linux	MASTER			

- In the *Snapshot Manager* window, click on the **Take** button. This will take a snapshot of the current state of the virtual machine.



Snapshot Manager







You Are Here!

Name:

Description:

 Take
 Delete All

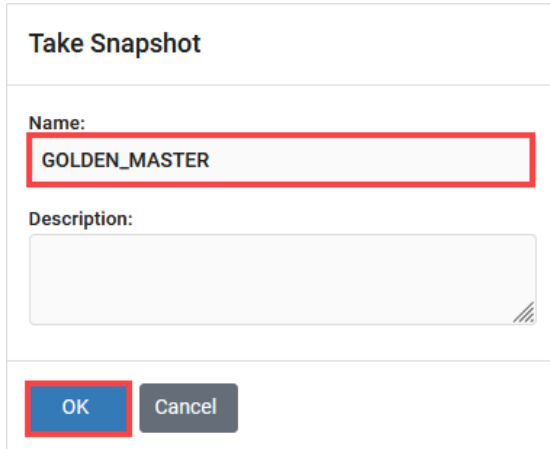
 Go To
 Edit
 Delete

 Dismiss



Any changes made after this will require a new snapshot or those changes will not reflect in the reset state of the pod or its clones.

3. In the *Take Snapshot* window, type `GOLDEN_MASTER` into the *Name* text field, or you may choose another naming convention as long as it is consistent for easy management. Click **OK**.



Take Snapshot

Name:
`GOLDEN_MASTER`

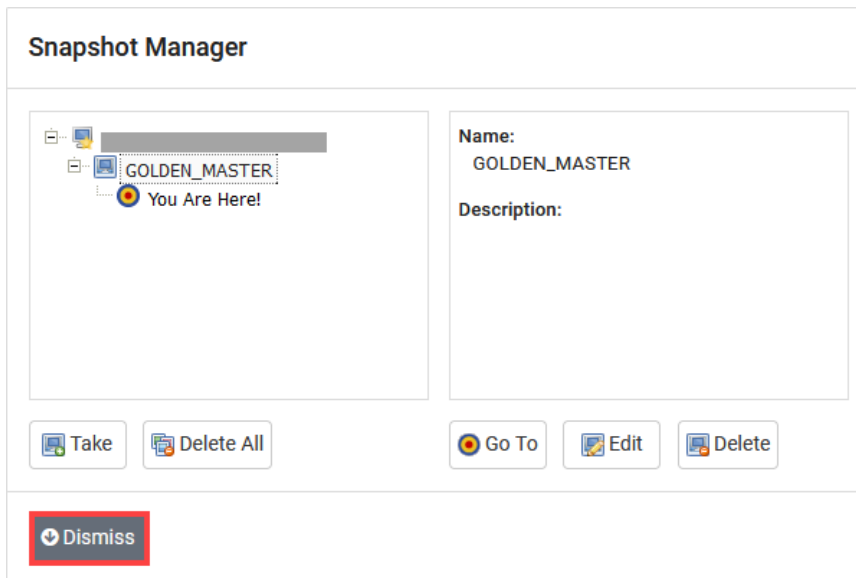
Description:

OK Cancel

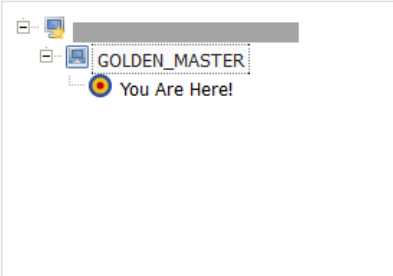


It is recommended to use `GOLDEN_MASTER` as the snapshot name when working with normalized pod types.

4. In the *Snapshot Manager* window, notice the snapshot is created. Click the **Dismiss** button.


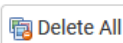





Snapshot Manager



Name:
GOLDEN_MASTER

Description:

Dismiss



At this point it is good to verify that you have only one snapshot on the virtual machine. Multiple snapshots increase the likelihood of having problems, especially if the snapshots are named the same. Also, the more snapshots a virtual machine has, the slower the performance and the more drive space is used.

5. Repeat the previous steps for the remaining virtual machines.

4.3.5 Set the Revert to Snapshot

1. Make sure to view the **Cybersecurity Fundamentals v1.0** master pod you just created snapshots for. In the pod view, click on the dropdown menu option underneath the *Action* column and select **Settings**.

Remote PC 6						
PC Name	VM	Operating System	VM Role	Runtime Host	Action	
Victim	UofSC_CSF_Master.Victim	Windows 10	MASTER	<div style="background-color: #ccc; width: 20px; height: 10px;"></div>		
BR/FW	UofSC_CSF_Master.BRFW	Linux	MASTER	1	<div style="border: 1px solid #ccc; padding: 5px;"> <ul style="list-style-type: none"> View Settings Attach VM Remove VM From... Snapshots </div>	
Attacker	UofSC_CSF_Master.Attacker	Linux	MASTER	1		
Web server	UofSC_CSF_Master.Web	Linux	MASTER	1		
DNS server	UofSC_CSF_Master.DNS	Linux	MASTER	<div style="background-color: #ccc; width: 20px; height: 10px;"></div>		
Mail server	UofSC_CSF_Master.Mail	Linux	MASTER	<div style="background-color: #ccc; width: 20px; height: 10px;"></div>		

- In the virtual machine's *Settings* window, click on the *Revert to Snapshot* dropdown and select **GOLDEN_MASTER** and then click the **Submit** button.



This sets the snapshot on the virtual machine that will get reverted to each time the pod is scheduled.

Victim Settings

PC Name: Victim

PC Type: Virtual Machine

Datacenter: [Redacted]

Virtual Machine: UofSC_CSF_Master.Victim

Role: Master

Revert to Snapshot: **GOLDEN_MASTER**

Shutdown Preference: Graceful Shutdown

Guest Operating System: Windows 10

Options:

- enable remote display auto-configuration
- enable network auto-configuration
- enable advanced setting auto-configuration
- enable minimum requirements verification

- Click **OK** to confirm.
- Return to the pod view page and repeat the previous steps for the remaining virtual machines.

4.4 Make changes to the Master Pod

Some pods have software that needs to be altered on the host machine before it can be used properly. This normally happens when software requires licenses to function.

If there are changes that need to be made to the master pod prior to link cloning, either student pods or full cloning other master pods on other hosts, you will need to follow this set of instructions to ready your master pod.

For the *Cybersecurity Fundamentals v1.0* master pod, you will need to license all the *Microsoft Windows* machines. This process consists of:

- Scheduling the master pod
- Providing temporary internet access to the *Victim* VM

- Licensing/Activating the *Victim* VM
- Reverting back the original *TCP/IP* settings
- Shutting down the *Victim* VM
- If necessary, resetting the network interface cards to *SAFETY NET*
- Taking a new *GOLDEN_MASTER* snapshot for *Victim*
- Ending the reservation

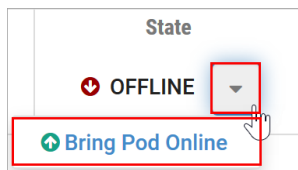
4.4.1 Virtual Machine Credentials

For your reference, the following table provides a list of the credentials for the systems in the pod:

Machine	User name	Password
Attacker	kali	password
BR/FW	root	password
DNS server	admin	password
Mail server	admin	password
Victim	admin	password
Web server	admin	password

4.4.2 Bring the Master Pod Online

1. In the pod view, click the drop arrow under *State* and select **Online**.



4.4.3 Create Class and Schedule the Master Pod

Create a class as identified in the *Add Classes* section of the [NETLAB+ VE Instructor Guide](#) then schedule the *Master Pod* to license the *Victim* virtual machine (if available, choose the “*No Lab: Launch Cyber Range*” from the list of labs as this selection will boot up all VMs available in the pod, otherwise, just choose any lab).



When scheduling the *Master Pod*, it is important to schedule the pod for enough time to complete the following steps.

4.4.4 Provide Temporary Internet Access to the Victim VM

1. Moving away from the *NETLAB+* interface, navigate to your **vSphere Client** using your management workstation, and then connect to your **vCenter Server**.
2. From the *vSphere Client* dashboard, select **Hosts and Clusters**.
3. Select your host under the **NETLAB** datacenter and expand its view to see the virtual machines attached.
4. Locate the *Victim* virtual machine. Right-click on the virtual machine and select **Edit Settings**.
5. Change *Network adapter 1* to a virtual machine port group that is linked to an internet-accessible physical adapter.



Alternatively, you can add a new *vNIC* to the VM and use it to link to a virtual machine port group that is linked to an internet accessible physical adapter.

6. Click **OK** to confirm the changes.

4.4.5 License and Activate the Victim VM

1. Log on to the **Victim** virtual machine in the pod. If necessary, click the dropdown arrow for the VM's tab and select **Send CTRL+ALT+DEL**.
2. Log in as `admin` with `password` as the password.
3. Once logged in, make sure the TCP/IP settings are temporarily configured correctly so that the internet is reachable. This can vary depending on how your environment is set up.



If you added a new temporary *vNIC* from the previous section, make sure to configure the *TCP/IP* settings for the newly added network adapter and use it to connect out to the internet.

4. Right-click on the **Start** icon in the lower-left and select **System**.
5. Scroll down and click **Change product key or upgrade your edition of Windows** in the *Windows activation* section.
6. Click **Change product key** in the *Activate Windows now* section.
7. Enter the product key and follow the on-screen instructions.
8. Windows should now be activated. If you received an error, make sure that the key entered is valid and click the **Troubleshoot** link from the *Activation Settings* to troubleshoot the problem.

4.4.6 Revert Back the Original TCP/IP Settings

1. After successfully activating the *Victim* VM, if you temporarily changed the TCP/IP settings for *vNIC1*, make sure to change the TCP/IP settings to what they were before.

4.4.7 Shut Down the Victim VM

1. On the *Victim* machine, click the **Start** button, followed by clicking the **Power** icon.
2. Click **Shut down**.

4.4.8 Reset the NIC to SAFETY NET

1. Outside the *NETLAB+* web interface, navigate to your **vSphere Client** using your management workstation, and then connect to your **vCenter Server**.
2. From the *vSphere Client* dashboard, select **Hosts and Clusters**.
3. Select your host under the **NETLAB** datacenter.
4. Locate the **Victim** virtual machine. Right-click on the virtual machine and select **Edit settings**.
5. Change *Network adapter 1* to **SAFETY NET**.



If you added a new temporary *vNIC* from the previous section, make sure to remove the extra *vNIC*.

6. Click **OK** to confirm settings.

4.4.9 Take New Snapshots for the Changed Master Virtual Machines

1. Right-click on the **Victim** virtual machine and select **Snapshots > Manage Snapshots**.
2. Click **Delete** to delete the current snapshot. Remember the name of this snapshot, as the new snapshot will need to have the exact same name.
3. Click **Yes** on the *Confirm Delete* window.
4. Click **Close** on the *Manage Snapshots* window.
5. Right-click on the **Victim** virtual machine and select **Snapshots > Take Snapshot**.
6. In the *Take Snapshot* window, type **GOLDEN_MASTER** or whatever prior snapshot name the virtual machine had. Click **OK** to take the snapshot.

4.4.10 End Reservation

You may now end the reservation of the master pod.

5 Pod Cloning

This section will help you create multiple 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. The ongoing operation of a full clone is entirely separate from the parent virtual machine.

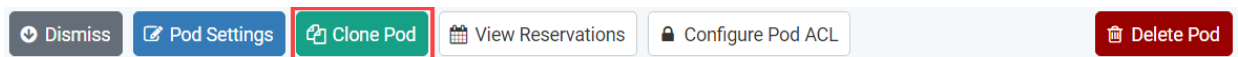
5.2 Creating User Pods

The following section describes how to create 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. Log in to **NETLAB+ VE** with the *administrator* account.
2. Select the **Pods** icon.



3. Click on your master pod.
4. Make sure the pod is offline by selecting **Take Pod Offline**.
5. Click the **Clone Pod** button to create a new pod, based on the settings and snapshots of this pod.



6. Input a new ID value into the **New Pod ID** field. 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. Click **Next**.
7. Enter a name for the cloned pod into the **New Pod Name** field. For example, **UofSC_CSF_H120_S1001**. Click **Next**.



The **Pod Name** identifies the pod and is unique per pod. Here we used the name of the lab set or course in a shortened form along with a host identifier (H120), the type and number of the pod (S1001).

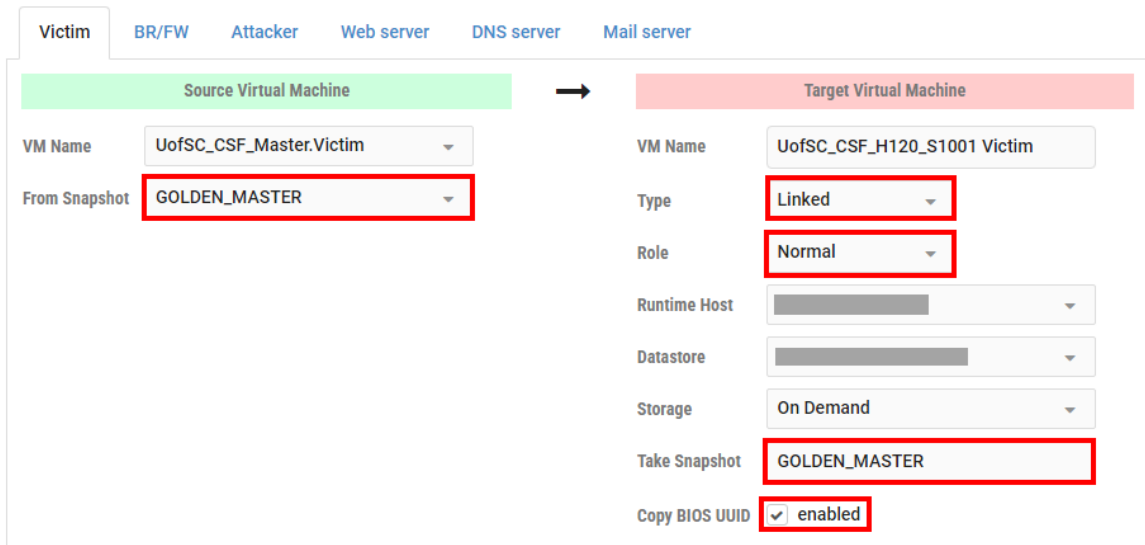
8. When the action has finished processing, you are presented with a settings screen. Notice each VM has its own tab. Go through each tab and verify the following:

Source Virtual Machine:

- a. *From Snapshot* should be set to the **GOLDEN_MASTER** snapshot you created previously.

Target Virtual Machine:

- a. For *Type*, verify that **Linked** is selected.
- b. For *Role*, verify that the **Normal** role is selected.
- c. For *Take Snapshot*, verify that **GOLDEN_MASTER** is inputted.
- d. For *Copy BIOS UUID*, only choose this option if you wish to preserve the sources VM's BIOS UUID for the targeted clone VM (when this option is checked, it can help with keeping licensing intact such as *Microsoft Windows Licensing/Activation*).



The screenshot shows a configuration interface for cloning a pod. At the top, there are tabs for different VM roles: Victim, BR/FW, Attacker, Web server, DNS server, and Mail server. The 'Victim' tab is selected. Below the tabs, there are two main sections: 'Source Virtual Machine' (highlighted in green) and 'Target Virtual Machine' (highlighted in red). An arrow points from the Source to the Target section.

Source Virtual Machine settings:

- VM Name: UofSC_CSF_Master.Victim
- From Snapshot: GOLDEN_MASTER (highlighted with a red box)

Target Virtual Machine settings:

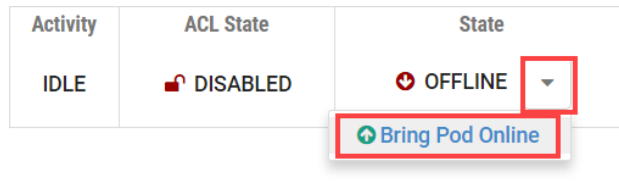
- VM Name: UofSC_CSF_H120_S1001 Victim
- Type: Linked (highlighted with a red box)
- Role: Normal (highlighted with a red box)
- Runtime Host: [Dropdown menu]
- Datastore: [Dropdown menu]
- Storage: On Demand
- Take Snapshot: GOLDEN_MASTER (highlighted with a red box)
- Copy BIOS UUID: enabled (highlighted with a red box)

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

 Clone Pod

10. When the pod clone process is finished, click **OK**.
11. If you want to dedicate this pod to a particular class, team, or student, use the *Pod ACLs* feature. For details, see the [NETLAB+ VE Instructor Guide](#).

- Click the **Online** Button on the *Pod Management* page to make the pod available.



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



The *GOLDEN_MASTER* snapshot is the starting point for all pods. We recommend that you reserve the 1st pod and conduct some labs to make sure the snapshot images work correctly. If there are defects, make corrections to the images to the master pod and retake the *GOLDEN_MASTER* snapshot before creating additional pods.

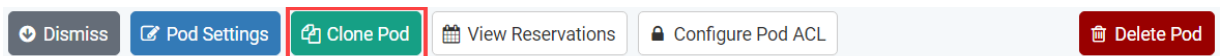
5.3 Copying Your Master Pod to the Second Host

For this task, we will use the pod cloning utility to copy our master pod to the second host.

- Log in to *NETLAB+* with the administrator account.
- Select the **Pods** icon.



- Click on the master pod.
- Make sure the pod is offline by selecting **Take Pod Offline**.
- Click the **Clone** button to create a new pod, based on the settings of this pod.



- Input a new ID value into the **New Pod ID** field. 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. Click **Next**.

7. Enter a name for the cloned pod into the **New Pod Name** field. For example, **UofSC_CSF_H130_M1000**. Click **Next**.



The **Pod Name** identifies the pod and is unique per pod. Here we used the name of the lab set or course in a shortened form along with a host identifier (H130), the type and number of the pod (M1000).

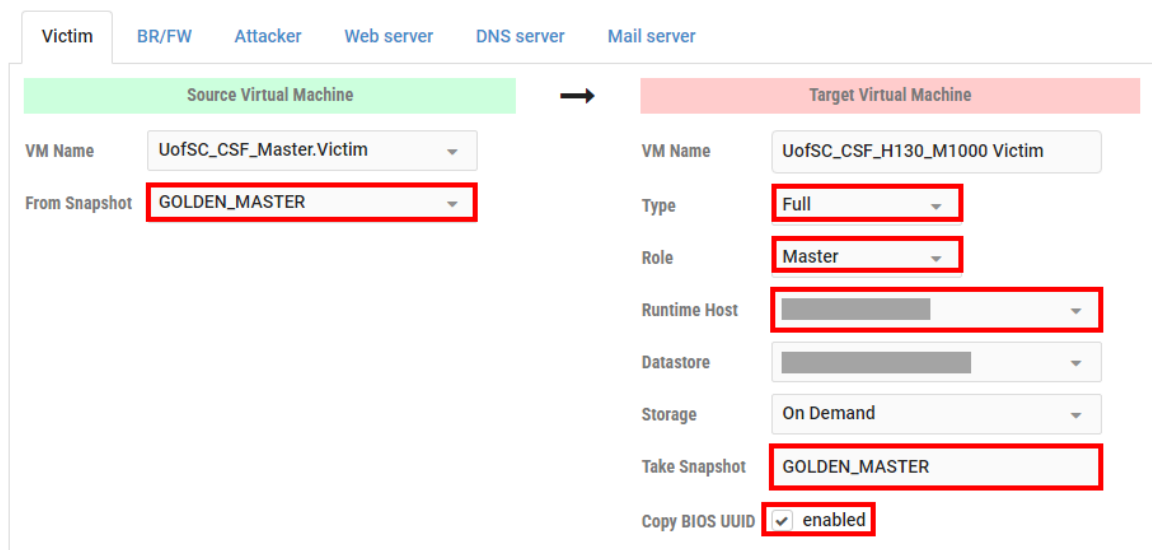
8. When the action has finished processing, you are presented with a settings screen. Notice each VM has its own tab. Go through each tab and verify the following:

Source Virtual Machine:

- a. *From Snapshot* should be set to the **GOLDEN_MASTER** snapshot you created previously.

Target Virtual Machine:

- a. For *Type*, verify that **Full** is selected.
- b. For *Role*, verify that the **Master** role is selected.
- c. For *Take Snapshot*, verify that **GOLDEN_MASTER** is inputted.
- d. For *Runtime Host*, select the second host system (which should be different than the system you are cloning from).
- e. For *Copy BIOS UUID*, only choose this option if you wish to preserve the sources VM's BIOS UUID for the targeted clone VM (when this option is checked, it can help with keeping licensing intact such as *Microsoft Windows Licensing/Activation*).



The screenshot shows a configuration interface for a Victim VM. At the top, there are tabs for 'Victim', 'BR/FW', 'Attacker', 'Web server', 'DNS server', and 'Mail server'. The 'Victim' tab is active. Below the tabs, there are two main sections: 'Source Virtual Machine' (highlighted in green) and 'Target Virtual Machine' (highlighted in red). An arrow points from the Source to the Target section.

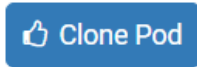
Source Virtual Machine settings:

- VM Name: UofSC_CSF_Master.Victim
- From Snapshot: GOLDEN_MASTER (highlighted with a red box)

Target Virtual Machine settings:

- VM Name: UofSC_CSF_H130_M1000 Victim
- Type: Full (highlighted with a red box)
- Role: Master (highlighted with a red box)
- Runtime Host: [Redacted] (highlighted with a red box)
- Datastore: [Redacted]
- Storage: On Demand
- Take Snapshot: GOLDEN_MASTER (highlighted with a red box)
- Copy BIOS UUID: enabled (highlighted with a red box)

9. 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.



10. When the pod clone process is finished, click **OK**.
11. It is likely that you will need to reactivate the licensing on any Windows VMs in the Master pod on the second (third, etc.) host. Please test the master pod prior to cloning student pods.

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 (see [Creating User Pods](#)), substituting the second master pod (created in the previous section) as the cloning source.

5.5 Assigning Pods to Students, Teams, or Classes

Please refer to the [NETLAB+ VE Instructor Guide](#) for details on using the *Pod ACLs* feature.