

Lab - Installing CSI Linux

Overview

In this lab, you will learn how to install CSI Linux. CSI Linux was developed by Computer Forensics, Incident Response, and Competitive Intelligence professionals to meet the current needs of their clients, government agencies, and the industry.

Minimum Requirements:

- 8 GB of FREE RAM (16 GB RAM Recommended)
- 70 GB free disk space (150 GB of free disk space recommended)
- 4 Core CPU
- VirtualBox
- VirtualBox Extensions
- Internet Access

Download links

- Main <u>download page</u> for CSI Linux Investigator.
- Main <u>download page</u> for VirtualBox and extension pack.

Caveat

Anytime you update VirtualBox, you will also need to update the VirtualBox extension pack. If VirtualBox is installed, no need to install it a second time.

We will assume you have the latest version of VirtualBox installed for this lab. Since the extension pack is available on the same page, downloading the extension pack should be a nobrainer; download and install the software.

Once you have installed the extension pack for the first time, VirtualBox will present you with the option to upgrade the extension pack each time you update VirtualBox. If you do not have the VirtualBox extension pack installed when you launch CSI Linux, you will receive an error preventing the launch of all three virtual machines.

Install the VirtualBox Extension Pack

VirtualBox Extension Pack is a binary package intended to extend the functionality of VirtualBox. The Extension pack adds the following functionality:

- Support for USB 2.0 and USB 3.0 devices.
- Host webcam pass-through.



- VirtualBox Remote Desktop Protocol (VRDP).
- Disk image encryption with AES algorithm.
- Intel PXE Boot ROM.

Go to the <u>download page</u> of VirtualBox and open the download link for the VirtualBox Extension Pack for **All supported platforms**. The name of the file used in this example is *Oracle_VM_VirtualBox_Extension_Pack-6.1.8.vbox-extpack*, and we saved the file to a specific location on our host machine. Where you save your file is up to you but do remember where you saved it to.

VirtualBox 6.1.18 Oracle VM VirtualBox Extension Pack

G→All supported platforms

Support for USB 2.0 and USB 3.0 devices, VirtualBox RDP, disk encryption, NVMe and PXE boot for Intel cards. See this chapter from the User Manual for an introduction to this Extension Pack. The Extension Pack binaries are released under the VirtualBox Personal Use and Evaluation License (PUEL). Please install the same version extension pack as your installed version of VirtualBox.

Download the extension pack.



Save to your local machine.

👈 Enter name of file	e to save to								×
← → • ↑ ┦	> This PC > Downloads >			~	Ō	,⊂ Sea	rch Down	loads	
Organize 👻 No	ew folder								?
🗸 💻 This PC		^							
> 🧊 3D Objects									
> 📃 Desktop									
> 🔮 Documents									
> 👆 Downloads									
> L System R (C:)								
> Local Disk (D)	h;)	~	<						3
File name:	Oracle_VM_VirtualBox_Extension_Pack-6.1.18.vbox-e	extpa	ck						~
Save as type:	VirtualBox Extension Pack (*.vbox-extpack)								~
∧ Hide Folders						Sav	e	Cancel	

From your VirtualBox management console, click on File, and from the context menu, select preferences.





In the Preferences window, go to the Extensions section. After a fresh installation of VirtualBox, there are no extension packages installed. Click the Add a new package button (the icon with a green plus) to add the extension pack.

🧬 VirtualBo	ox - Pre	ferences		?	\times
General	Exten	sions	 		
 Input Update 	Active	Name			Version
S Language					المك
Display					
Extensions					
Proxy					
			OK		Cancel

Browse to the download location where you save the previously downloaded extension pack.



🔞 Select an extension package file						×
← → ∽ ↑ 🔜 > This PC > Desktop >			ٽ ~	Search Desktop		P
Organize 🔻 New folder					•	?
> 📥 OneDrive	^	Name	Date modified	Туре	Size	
✓ 💻 This PC		Oracle_VM_VirtualBox_Extension_Pack-6	28/03/2020 4:34 PM	VirtualBox Extensi	10,741	KB
> 🧊 3D Objects						
> 📃 Desktop						
File name: Oracle_VM_VirtualBox_	Exter	sion_Pack-6.1.4.vbox-extpack	~	Extension package f	iles (*.vbox	\sim
				Open	Cancel	

You are asked to confirm that you want to install the selected extension pack.

🥜 Virt	🔗 VirtualBox - Question			\times
You are about to install a VirtualBox extension pack. Extension packs complement the functionality of VirtualBox and can contain system level software that could be potentially harmful to your system. Please review the description below and only proceed if you have obtained the extension pack from a trusted source.				
	Name: Oracle VM VirtualBox Extension Pack			
	Version:	6.1.4r136177		
	Description:	Orade Cloud Infrastructure integration, USB 2.0 and USB 3.0 Host Controller, Host Webcam, VirtualBox RDP, PXE ROM, Disk Encryption, NVMe.		
	E	Install Cancel		

On the next screen, scroll to the bottom of the license agreement and then click the "I agree button."





Once the extension pack has been installed, you will receive the following message. Click OK.



You can confirm the extension pack is installed by checking the right windows pane. Click OK to close the VirtualBox preferences.

🔗 VirtualBox - Pre	eferences			?	×
General	Exter	sions			
🔷 Input	Extension	n Packages			
	Active	Name		Version	G
opuace	~	Oracle VM VirtualBox Extension Pack		6.1.4r136177	
🍚 Language					
Display					
Network					
Extensions					
Proxy					
			OK	Cance	el

Download and Install CSI Linux

Point your browser to <u>https://csilinux.com/download.html</u> Scroll to the bottom of the page and select your download method.

CSI Linux 2021.2 Virtual Appliance:

MD5 (.ova): e9815f65cfd7f99d17f1c3f68b94486c

* Installation Document: download here.

Please consider seeding after downloaded.

- CSI Linux 2021.2 Torrent File
- CSI Linux 2021.2 Magnet link
- Dropbox download
- Direct download



I saved a lot of time using the Dropbox download. All other methods were taking 13+ hours. Using the Dropbox download, I was able to cut the download time to less than two hours.

.ova files can't be previewed. CSI Linux 2021.1 VM.ova - 7.11 GB	
Download •	
Direct download Save to my Dropbox	
CSI Linux 2021.1 VM.ova CSI Linux 2021.1 VM.ova 1h 53m left — 171 MB of 7.1 GB (1.0 MB/sec)	×

This is a large OVA file of nearly 7.11 GB. If you struggle with downloading large files, you can install the <u>Free Download Manager</u> and use the torrent download option.





🔁 Free D	Download Manager				- 0	×
+					Q	
All (2)	Active (1) Completed (1) Torrent (0) YouTube (0)	÷				
	Name	Status	Speed	Size	Added 🗸	
	CSI Linux 2021.2.ova	16% 46m 10s	↓2.5 MB/s	1.40 / 8.33 GB	7:04	-

Once you have the OVA downloaded and saved, browse over to the saved location, and x2 left click on the OVA file.

😻 Dropbox	30/07/2020 7:55 AM	File folder	
💗 CSI Linux 2021.2.ova	20/06/2021 7:55 AM	Open Virtualizatio	8,730,709 KB

The file will immediately open inside of your VirtualBox manager. The first screen is Appliance settings. Click the Import button.

			?	×
←	Import Virtual Appliance			
	Appliance settings			
	These are the virtual machines conta You can change many of the propert below.	ined in the appliance and the suggested settings of the imported VirtualBox es shown by double-dicking on the items and disable others using the chec	(machines k boxes	s.
	Virtual System 1			^
	😸 Name	CSI Linux 2021.2		
	Product	CSI Linux		
	Product-URL	https://csilinux.com/download.html		
	🗩 Vendor	CSI Linux		
	🗩 Vendor-URL	https://csilinux.com		
	🗩 Version	2021.2		
	Description	We believe that having the right tools to do the job is critical for fo	rensic	~
	Machine Base Folder: 🚘 F:			\sim
	MAC Address Policy: Include only N	AT network adapter MAC addresses		•
	Additional Options: 🔽 Import hard	l drives as VDI		
	Appliance is not signed			
		Restore Defaults Import	Cancel	



Accept the license agreement.



The import process begins.



Once the import process is finished, you will see three CSI Linux virtual machines in the left window pane.



Congratulations! You have completed the install portion for CSI Linux Investigator.

Feel free to launch the CSI Linux. The username is **csi**, and the password is **csi**, all lower case.



csi 🗸
Log In

Take a Snapshot

Once you have logged on, it is highly recommended that you create a snapshot of your clean configuration. Create your snapshot the same way you did for your install of Kali.

Before update.

👽 Oracle VM VirtualBox Manager File Machine Snapshot Help	
	Take Delete Restore Properties Clone Settings Discard Start
> Microsoft	Name
> New group 2	Current State
V CSI Linux	
CSI Linux (dean Instal of CSI Linux)	

Once you have your snapshot taken, you can update by opening a terminal session and, at the prompt type, **powerup**.

\$_	Terminal - csi@csi-analyst: ~	-	×
File Edit Viev	w Terminal Tabs Help		
csi@csi-ana	alyst:~\$ powerup		$\left[\right]$
-	Information + ×		
i	This will take a long time. Please be patient. Get a bite to eat or go on vacation. Once done, the system will reboot.		
	ОК		



After update

👽 Oracle VM VirtualBox Manager		- 🗆 X
File Machine Snapshot Help		
Tools	Take Delete Restore Properties Cone Settings Discard Show	
> Microsoft	Name	Taken
	🗸 🚳 Clean install, not updated	31/03/2020 12:23 PM (28 minutes ago)
> Linux	✓ ♥ Updated distro	
	🔷 Current State (changed)	
✓ CSI Linux Investigator		
CSI Linux Analyst (Updated distro)	N	

Once you have completed the update, take another snapshot to back up the changes made to the distro.

Summary -

The video Tutorial has more information about the changes and integration of the CSI Linux Gateway, which is now part of the single OVA downloaded for this lab.

The CSI Linux SIEM has been separated and is now separate from CSI Linux. MISP, OTX, Malcolm, Moloch, Elasticsearch, Kibana, Logstash, Zeek, and others have been combined into this growing network monitoring and forensic server environment. This will be able to be downloaded onto CSI Linux or used on another system on the network.

CSI Linux SIEM 2021.1: Follow the link and the instructions at <u>https://github.com/Information-Warfare-Center/CSI-SIEM/blob/master/README.md</u>

End of the lab!