**Lab – CTF Lab Build for HA: Forensics**

**Overview**

HA: Forensics is Capture the Flag (CTF) designed for those interested in learning digital forensics. This lab is based on the famous investigator’s journey on solving the Curious Case of Harshit's murder.

This is a Forensic based capturing points and not a Boot-to-Root. The objective is to find all 100 points.

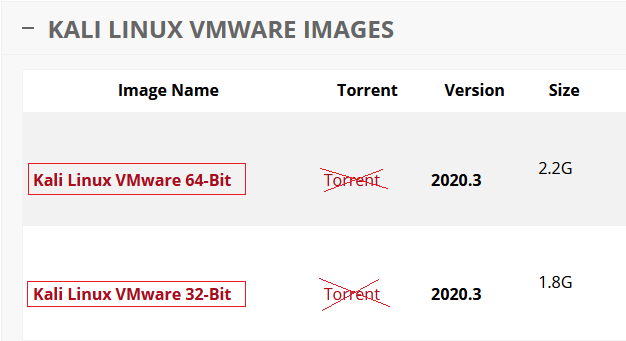
**Lab Requirements**

**Disclaimer: This machine works on VMWare. There might be IP related issues with Virtual Box.**

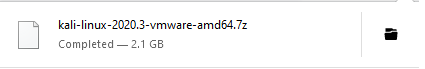
This lab requires the use of VMware Workstation Player. The forensic target was built using VMware, and though it is an OVA file, it will not acquire an IP address using DHCP when imported into VirtualBox.

* Install of [**VMware Workstation Player**](https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html)
* Once virtual install of [**Kali Linux in VMWare**](https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/).
* OVA image file for HA: Forensic Target downloaded from [**Vulnhub**](https://download.vulnhub.com/ha/forensics.ova)

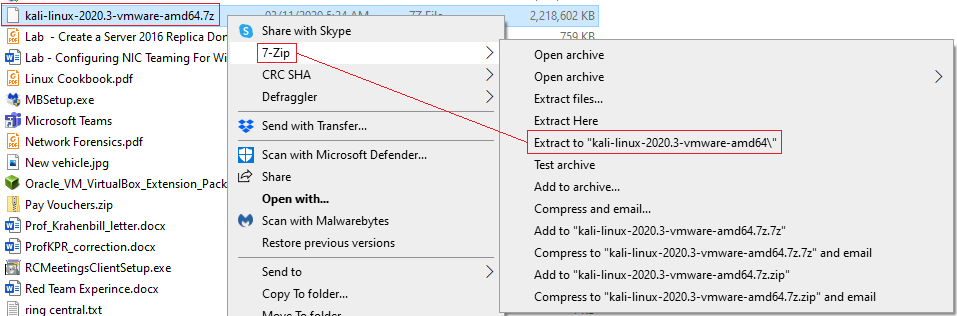
Make sure you download the correct virtual machine for VMware.



Once you have the 7zip folder downloaded, you will need to extract the contents. Click on the folder icon. This will take you to the download location.



Once you locate the downloaded VMware image, right-click on the downloaded archive, and from your 7zip menu, select **Extract to….** This will extract the contents to the same location as the downloaded image.

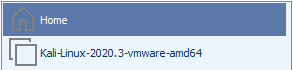


Open your VMware Player management console. Click on the **Open a Virtual Machine** option.



Browse to your extracted folder. You will see one option that can be imported. X2 click the following file to complete the importation of Kali Linux.

You can launch Kali Linux from the left windowpane.



**Create Your Target Machine**

Once you have the OVA image downloaded from Vulnhub, launch a second instance of VMWare Player from your Start Menu>Programs>VMware folder. From the right windowpane, select, Open a Virtual Machine.



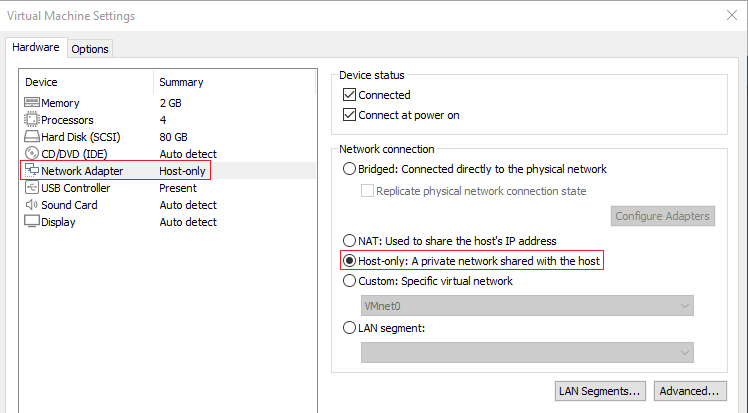
On the next screen, browse to your download location.

Find your **forensics.ova** file, x2 click, and allow the import to complete.



Once your image file has been imported, from the left windowpane of your VMware management console, find your newly created virtual disk, right-click on the name of your image, and select Settings from the context menu.

From the setting properties, select network. And configure your network to use Host-only networking.



**Start your Lab**

VMware requires a separate instance of the program for each virtual machine. Start both your install of Kali Linux and your Forensics virtual machine.

Minimize the install of your target machine.

Logon to your install Kali Linux.

**Log on as Root**

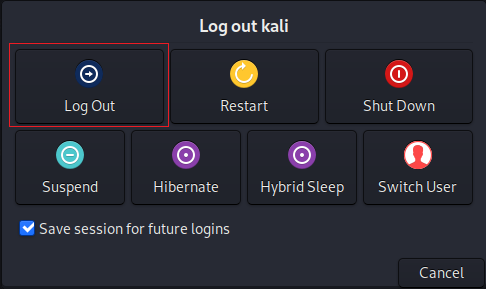
From your Kali desktop, open terminal. At the prompt, type **sudo passwd.** When prompted for your Kali password, type in kali, all lower case.

You will be prompted to type in your new password for root. In this example, I used the password of **toor**. Retype your password.

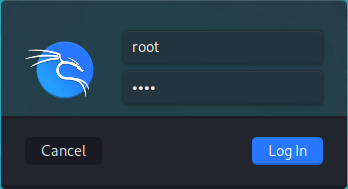
From the quick start menu located at the top right of your Kali, press the power button.



Log off your Kali install.



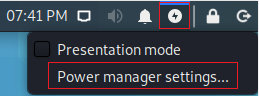
Type in root as your username and your root password.



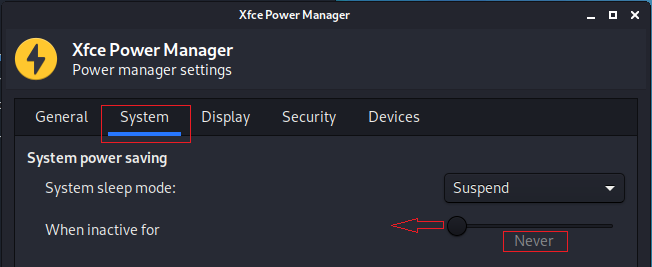
When logged in as root, you will not be prompted for your sudo password.

**Configure the Idle Time Out**

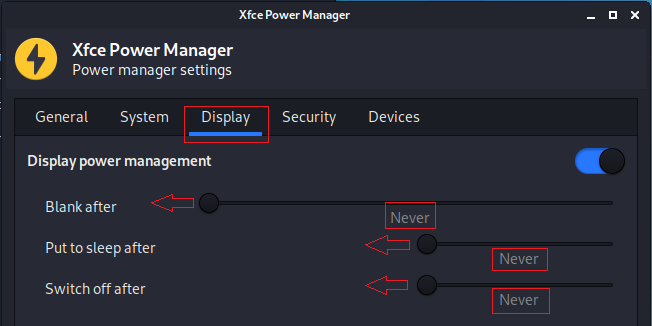
From the quick launch menu, click on Power Management. From the context menu, click on Power manager settings.



Click on System. Move the slider to the left until the indicator shows, never.



Click on display. Click on three blue lines until they read **Never**. This will prevent you from being logged off when idle for more than 10 minutes.



**End of this lab**