Lab – CTF Lab Build for HA: Forensics

Overview

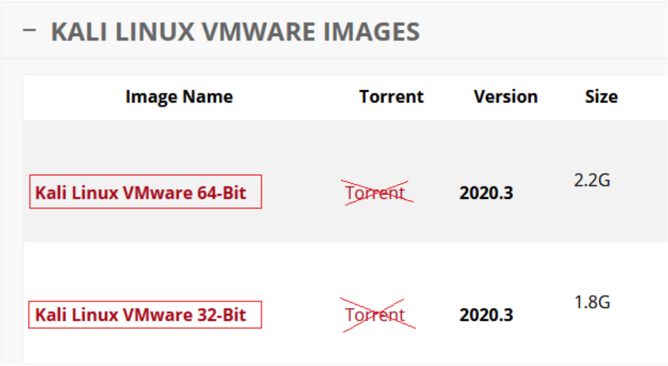
HA: Forensics is Capture the Flag (CTF) designed for those interested in learning digital forensics. This CTF contains FOUR flags that reveal themselves as the lab progresses based on hints.

Lab Requirements

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**
- Once virtual install of **Kali Linux for VMWare**.
- OVA image file for HA: Forensics Target downloaded from **Vulnhub**

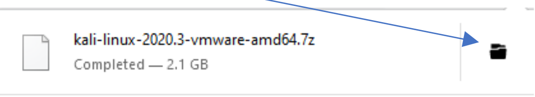
Make sure you download the correct virtual machine for VMware.



− KALI LINUX VMWARE IMAGES

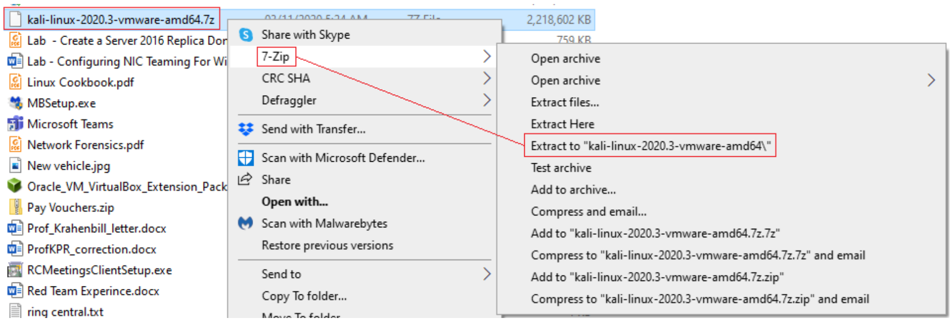
Image Name	Torrent	Version	Size
Kali Linux VMware 64-Bit	~~Torrent~~	2020.3	2.2G
Kali Linux VMware 32-Bit	~~Torrent~~	2020.3	1.8G

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.

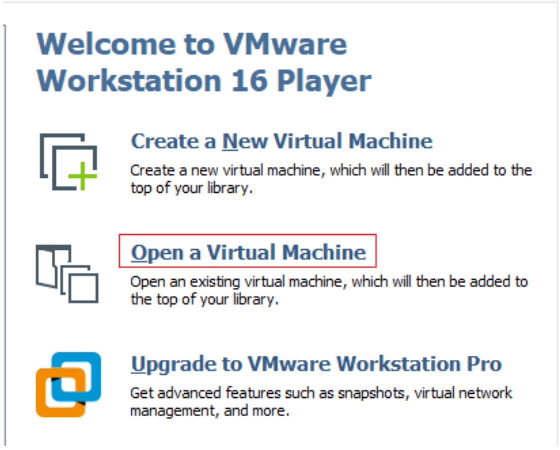


kali-linux-2020.3-vmware-amd64.7z
Completed — 2.1 GB

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.


kali-linux-2020.3-vmware-amd64.7z
2,218,602 KB
Lab - Create a Server 2016 Replica Dor
Lab - Configuring NIC Teaming For Wi
Linux Cookbook.pdf
MBSetup.exe
Microsoft Teams
Network Forensics.pdf
New vehicle.jpg
Oracle_VM_VirtualBox_Extension_Pack
Pay Vouchers.zip
Prof_Krahenbill_letter.docx
ProfKPR_correction.docx
RCMeetingsClientSetup.exe
Red Team Experince.docx
ring central.txt
759 KB
Share with Skype
7-Zip
CRC SHA
Defraggler
Send with Transfer...
Scan with Microsoft Defender...
Share
Open with...
Scan with Malwarebytes
Restore previous versions
Send to
Copy To folder...
Open archive
Open archive
Extract files...
Extract Here
Extract to "kali-linux-2020.3-vmware-amd64\"
Test archive
Add to archive...
Compress and email...
Add to "kali-linux-2020.3-vmware-amd64.7z.7z"
Compress to "kali-linux-2020.3-vmware-amd64.7z.7z" and email
Add to "kali-linux-2020.3-vmware-amd64.7z.zip"
Compress to "kali-linux-2020.3-vmware-amd64.7z.zip" and email

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



Welcome to VMware Workstation 16 Player

Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine

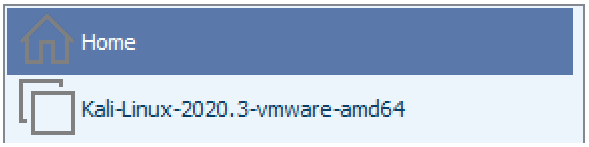
Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation Pro

Get advanced features such as snapshots, virtual network management, and more.

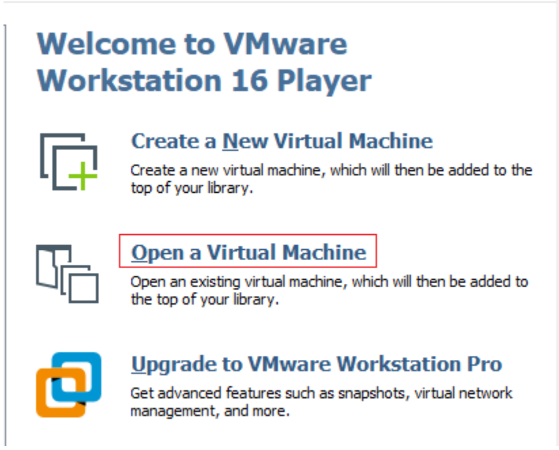
Browse to your extracted folder. You will see one option that can be imported. X2 click the following file to complete the importation of Kali Linux.

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.



Welcome to VMware Workstation 16 Player

Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine

Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation Pro

Get advanced features such as snapshots, virtual network management, and more.

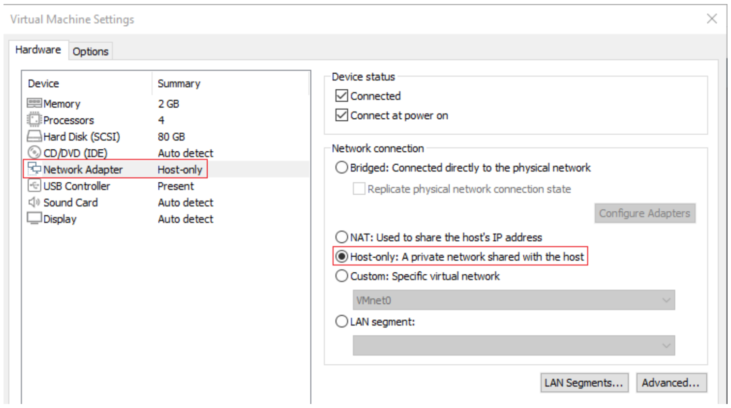
On the next screen, browse to your download location.

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

forensics.ova

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.



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	2 GB
Processors	4
Hard Disk (SCSI)	80 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

Configure Adapters

○ NAT: Used to share the host's IP address

● Host-only: A private network shared with the host

○ Custom: Specific virtual network

VMnet0

○ LAN segment:

LAN Segments... | Advanced...

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.

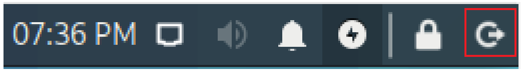
Logon to your install Kali Linux.

Log on as Root

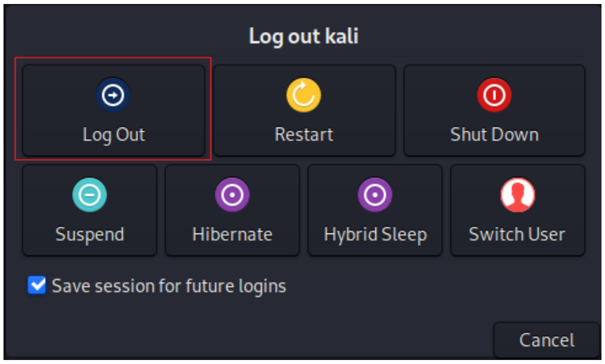
From your Kali desktop, open terminal. At the prompt, type **`sudo passwd`.** When prompted for your Kali password, type in kali, all lower case.

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.

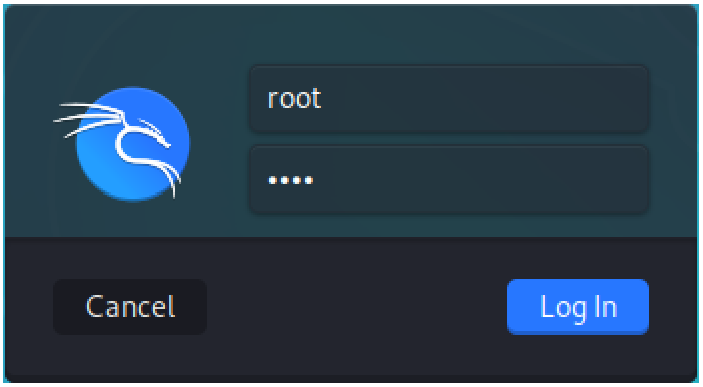


Log off your Kali install.



☑ Save session for future logins

Type in root as your username and your root password.



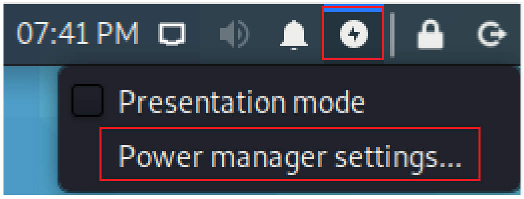
root

••••

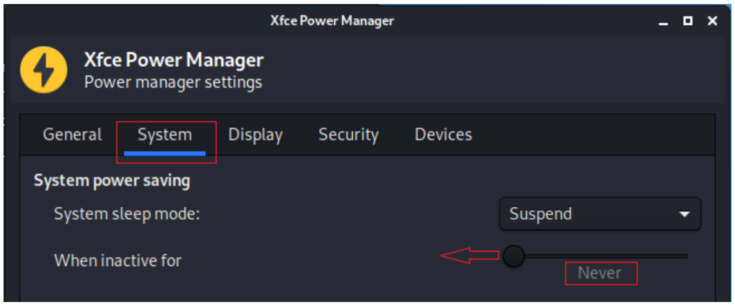
When logged in as root, you will not be prompted for your sudo password.

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.

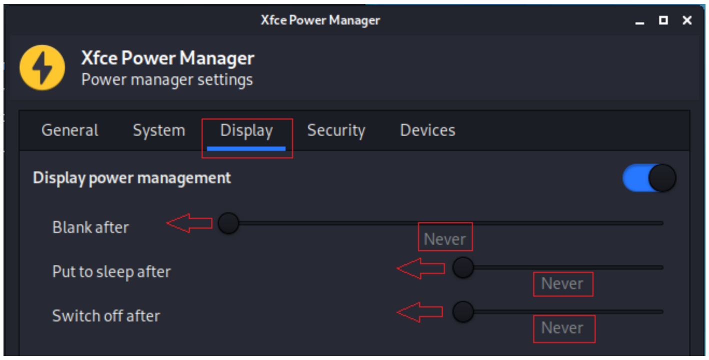


System power saving

System sleep mode: Suspend

When inactive for 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.



Display power management

Blank after Never

Put to sleep after Never

Switch off after Never

End of this lab