Fundamental Skills - Setting up a Virtual Machine

Category	Experience Level
Misc	Novice

Contents

- Fundamental Skills Setting up a Virtual Machine
 - Intro
 - Virtualisation Software
 - Basic VirtualBox Usage
 - Installing a VM
 - What Should I Choose?
 - Downloading a Machine Image
 - Downloading a Disk Image
 - Installing with Virtual Box
 - Installing from a Machine Image
 - Installing from a Disk Image
 - Configuring the Machine
 - Networking a VM
 - <u>Worksheet</u>

Intro

Virtual Machines (VMs) are useful tools for running a 'virtualised' version of a computer as a program on your normal computer.

What does this mean?

- you can run a machine with a different Operating System (OS) to your normal computer; for example, you could run <u>Kali Linux</u>-(a-common-os-that-comeswith-lots-of-cybersecurity-tools) as a sub-program on your normal Windows Computer, without having to worry about Dual Booting or Live USBs
- you can create machines for dangerous activities like exploit development and malware analysis, or just to experiment with a new OS, and be able to safely discard them or revert them to clean states
- you can use machines prebuilt and configured by experts for specific purposes, such as Tracelabs' <u>Open-Source Intelligence VM</u>

- you can create internal networks of machines to practice hacking interconnected machines, such as an Active Directory forest or a mailserver
- you can adjust machine specifications, such as amounts of RAM, on the fly (within the limits of your actual computer!)

Virtualisation Software

You'll need a piece of software that is capable of running Virtual Machines. Some Operating Systems, such as Windows 10 Pro, have such software preinstalled. Most people, however, will need to install the software separately.

We will be teaching VirtualBox in this lesson. You can download it from here:

https://www.virtualbox.org/wiki/Downloads

You will need to pick the right version for your **host** Operating System (the OS of your actual computer). You can then start creating Virtual Machines with many different **guest** Operating Systems.

You'll also need to **enable virtualisation** on your computer - this can often be done in the BIOS, which is an interface that controls many internal aspects of your computer. It can usually be accessed during boot time, but the method for accessing it will vary based on your computer model. Searching "enable virtualisation on *your computer here*" into Google should do the trick!

A good alternative to VirtualBox is VMWare - it is feature rich and has a very clean User Interface, but is a paid product. If you think you'll only need to run one Virtual Machine, you can download the free <u>VMWare Player</u> software - but beware, we may ask you to install other Virtual Machines in our sessions!

Basic VirtualBox Usage

The main screen of VirtualBox lists all your VMs - clicking a VM shows more details:

Oracle VM VirtualBox Manager Sile Machine Hele		- B X
Tools	New Settings Datard Start	
Kali-linux-2019-3a Operated Off	Ceneral Neme: Kał-Lrux-2021.2-virtuałbox-am654 Operatrógsystem: Deban (64-54)	Preview
Call Linux-2021.2-virtualbox-amd64 (Snaphot 3) ① Powered Off	System Searching 64:148 Processors 2 Control Control	Kali-Linux-2021.2- virtualbox-amd64
Powered Off	Acceleration: VT x/JAMD-V, Nested Paging, PAE/NX, KUM Paravirtualization	
Compared Off	Display Video Henory: 128 MB caparias Contraling: WHOYCA	
Stapler @ Powered Off	Remice De Backhos Server: Dasahed Recording: Disabled	
ExySysAdmin @ Powered Off	Controllent IDE De Secondray Device 0: [Optical Drive] Empty Controllent SATA STAT APUT 0: Kak Linux 2022.2-virtualisox-and64-didd01.vd (Normal, 80.00.08)	
Wervy	Audio Hot Divers Windows DirectSound Controller: 10/AS7	
	We Hervork Adapter 1: Intel®C/ICOU HT Deddap (HUT) Adapter 2: Intel®C/ICOU HT Deddap (HUT) Ø UNI Ø UNI <th></th>	

To power on a VM, simply click the green *Start* button. This will start the machine in a new window - you can see that my *host* OS is Windows, but the VM is booting in GRUB (the boot loader for the *guest* OS, Debian):



Powering off a VM is as simple as clicking *File > Close*, or powering it off as normal using the power settings in the machine itself:



Virtual Box will *capture* your mouse and keyboard by default, which means it will direct your mouse and keyboard to the VM when the window is active. To *release* your controls simply press the *Host Key* (**Right Ctrl** by default on Windows) - this will let you interact with the Host OS again.

To make your VM full screen, simply press Host + F (where Host is your Host Key).

You can also pause the machine (Host + P), take snapshots (Host + S), and revert to an earlier state.

Snapshots are a powerful feature that let you save the complete machine state and go back to it later - for example, before running **sudo apt-get dist upgrade** so you can return to your old distribution if something goes wrong.

You can view snapshots by clicking a machine's hamburger menu and selecting the *Snapshots* tab:

👽 Oracle VM VirtualBox Manager File Machine Snapshot Help	-	- 0 ×
Tools	New	
Kali-linux 2019-3a Powered Off	Name v ∰ Supphet1 v ∰ Supphet2 v ∰ Supphet2	Taken 25/08/2021 14:01 25/08/2021 20:29 27/08/2021 09:14
Kali-Linux-2021.2-virtualbox-amd64 (Snapshot 3)	▲ Gurrent State (changed)	21/00/2021 03:14
brainpan © Powered Off		
LemonSqueezy		
Stapler © Powered Off		
LazySysAdmin @ Powered Off		
Percy Bowered Off		

From there you can restore to a specific snapshot, delete a snapshot, and more.

A fresh install won't have any VMs listed - we'll discuss how to add them in the next section, but we first need to go over different VM formats.

Installing a VM

We've shown you what VirtualBox looks like, but not how to actually *install* a Virtual Machine.

What Should I Choose?

There are a few options when setting up a virtual machine.

Perhaps the easiest option is to use a **machine image**, which is a fully configured Virtual Machine that can be loaded straight into VirtualBox and ran straight away. However, machine image files can be very large and slow to download. Choose this option if you want your machine completely configured for you.

The other option is to use a **disk image** to install the guest operating system from. This is a little like installing a fresh copy of Windows from an install disk. It gives you more control over the installation process, but is slower to install once downloaded. Choose this option if you're comfortable following an install wizard and want extra control over your installation.

Downloading a Machine Image

We'll use Kali Linux as an example - Kali is a powerful Operating System built for penetration testing, and comes preconfigured with a large suite of tools. Don't be too overwhelmed by everything that's on it - get used to using a terminal first!

You can get a Kali Machine image from here: <u>https://www.kali.org/get-kali/#kali-virtual-machines</u>. Select the version for VirtualBox, and wait for the download to complete (it may take a while):



Virtual Machines Documentation >

This will download as a large .ova file.

Downloading a Disk Image

If you prefer a Disk Image, you can get the Kali Disk Image from here: <u>https://www.kali.org/get-kali/#kali-bare-metal</u>:

Kali	Linux 2021.3	Change	elog ^ø	
64-bit	32-bit	/	Apple M1	
		9		明
Weekly Untested images with the latest updates	Installer Complete offline insta with customizatio	llation n	NetI All packages during	nstaller are downloaded installation
ע לא vepository sum	<u>↓</u> a torrent	sum		rrent sum

This will download as a .iso file.

Installing with Virtual Box

Once the downloads are complete, you can import whatever VM format you downloaded into VirtualBox.

Installing from a Machine Image

To import a Disk Image, press Ctrl + I or go to File > Import Appliance:

🦸 Oracle VM VirtualBox Manager



Then select the downloaded Machine Image - it should have the **.ova** extension.

Settings ^ Virtual System 1 😓 Name Kali-Linux-2021.2-virtualbox-am... Product Kali Linux Product-URL https://www.kali.org/ 🗐 Vendor Offensive Security Vendor-URL https://www.offensive-security.c... Version Rolling (2021.2) x64 Description Kali Rolling (2021.2) x64... 🙋 Debian (64-bit) 🚼 Guest OS Type 🔲 CPU 2 2048 MB + RAM OVD \checkmark USB Controller
 \checkmark Image: Sound Card CH AC97 Network Adapter Intel PRO/1000 MT Desktop (...

You can edit the settings, such as to give it more RAM:

You can also choose where to install the VM to - if you have a smaller SSD drive and a larger HDD, it may be a good idea to install it to the HDD.

Then press Import, and VirtualBox will load your machine!

Import Virtual Appliance

ocal File System	Version	Rolling (2021.2) x64
s\Kali 2021.2\kali-linux-2021.2-virtualbox-amd64.ova	Description	Kali Rolling (2021.2) x64
	🚼 Guest OS Type	问 Debian (64-bit)
	CPU	2
	RAM	5120 MB
Importing virtual disk 2 minutes, 44 second	nage 'Kali-Linux-2021.2-virtualbox-amd64 remaining	Hdisk001.vmdk' (2/3) 1% X IT Desktop (
Importing virtual disl	nage 'Kali-Linux-2021.2-virtualbox-amd64 remaining	A) AHCI Kali-Linux-2021.2-virtualbox-am
Importing virtual disl 2 minutes, 44 second	nage 'Kali-Linux-2021.2-virtualbox-amd64 remaining Storage Controller (SATA Virtual Disk Image Base Folder	A) AHCI Kali-Linux-2021.2-virtualbox-am D:/Virtual Machines
Importing virtual disl 2 minutes, 44 secon	nage 'Kali-Linux-2021.2-virtualbox-amd64 remaining	A) AHCI Kali-Linux-2021.2-virtualbox-am D:/Virtual Machines
Importing virtual dis 2 minutes, 44 secon	nage 'Kali-Linux-2021.2-virtualbox-amd64 remaining	H-disk001.vmdk' (2/3) 1% X A) AHCI Kali-Linux-2021.2-virtualbox-am D:/Virtual Machines / al Machines
Importing virtual dis 2 minutes, 44 second	nage 'Kali-Linux-2021.2-virtualbox-amd64 remaining Storage Controller (SATA Storage Controll	A) AHCI Kali-Linux-2021.2-virtualbox-am D:/Virtual Machines / al Machines

Most Kali images have around 80GB of disk space assigned, which should be more than enough for most people - this space won't be consumed on your drive immediately, it is simply an upper limit of the size of the VM.

Security Tip: we also recommend changing the default password on your kali image - by default, the credentials are kali:kali

Other Formats

Some Machine Images may be in a format built for VMWare, especially if they were created in VMWare originally. For example, here is the machine <u>Lemonsqueezy</u> from Vulnhub:

🧊 Please choose	a virtual har	d disk file					×
$\leftarrow \rightarrow ~ \star ~ \uparrow$	→ This	PC > New Volume (D:) > VM Images > Lemo	onSqueezy >	~	ې 5	Search LemonSqu	ieezy
Organise 🔻	New folder						
📃 Desktop	* ^	Name	Date modified	Туре	Size		
🕂 Download	s ≉	LemonSqueezy.vmx.lck	26/04/2020 06:48	File folder			
🔮 Documen	ts 🖈	マ LemonSqueezy.vmdk	26/04/2020 06:49	Virtual Machine Di	6,232,832 Ki	3	
Pictures	*						
Mac Docs	*						
Cybersecu	irity 🖈						
Uni	*						
Attachme	nts						
Screensho	+c						
SESH							
OneDrive							
📃 This PC							
i Network	~						
	File nar	ne: LemonSqueezy.vmdk			~ All v	rirtual hard disk file	s (*.vmd $ \smallsetminus $
						Open	Cancel

VirtualBox can still load these files, but the process is slightly different. First, press Ctrl + N or the *New* button to create a new machine:

🖲 🖗	racle \	/M VirtualBox Manager			
<u>F</u> il€	Mac	:hine <u>H</u> elp			\frown
	0	<u>N</u> ew	Ctrl+N		
UL	÷	<u>A</u> dd	Ctrl+A		New Settings Discard Show
64	\odot	Settings	Ctrl+S		🧧 General
(G.	Cl <u>o</u> ne	Ctrl+O		Name: Kali-Linux-2021.2-virtualbox-amd64
	27	Move			Operating System: Debian (64-bit)
64	R	Export to OCI		oshot 3)	System
	83	<u>R</u> emove			Base Memory: 6144 MB Processors: 2
	P	Group			Boot Order: Hard Disk, Optical
2	4	Show			
	00	Pause			Video Memory 179 MP
64	5	Reset			Graphics Controller: VMSVGA
	٩	Close	•		Remote Desktop Server: Disabled Recording: Disabled
64	8=	Tools	•		Storage
	-	10015			Controller: IDE
	\diamond	Discard Saved State			IDE Secondary Device 0: [Optical Drive] Empty Controller: SATA
64	Ū	Show <u>L</u> og	Ctrl+L		SATA Port 0: Kali-Linux-2021.2-virtualbox-amd64-disk001.vdi (Normal, 80.00 GB)
	G	Refresh			(🎾 Audio
64		Show in Explorer			Host Driver: Windows DirectSound
\mathbf{Z}	5	Create Shortcut on Desktop			
	<mark>91</mark>	Sort			Adapter 1: Intel PRO/1000 MT Deskton (NAT)
	0	Search	Ctrl+F		Adapter 2: Intel PRO/1000 MT Desktop (Hor) Adapter, 'VirtualBox Host-Only Ethernet Adapter')
	-	<u>Search</u>	Curri	1	🖉 USB

Then give your machine a name and install location, and assign it some RAM:

Create Virtual Machine

Name and opera	ting system
Name:	LemonSqueezy
Machine Folder:	D:\Virtual Machines ~
Type:	Linux 🗸 🚰
Version:	Debian (64-bit)
Memory size	
	2048 🗘 MB
4 MB	16384 MB
Hard disk	
O Do not add a	a virtual hard disk
Oreate a virt	ual hard disk now
🔿 Use an exist	ing virtual hard disk file
brainpan-dis	sk1.vdi (Normal, 16.00 GB) 🔹 🖂
	Guided Mode Create Cancel

In the bottom, select *Use an existing virtual hard disk file* and click the folder icon to select the .vmdk file for the machine you're importing - if it's not in the list, click *Add* to import it:

Ć	Test	t Kali - Hard Disk Selector				? ×
N	/lediun	n				
(Add	Refresh				
	Name	Ŷ	Virtual Size	Actual Size		
	✓ Att	tached				
		brainpan-disk1.vdi	16.00 GB	2.12 GB		
		kali-linux-2019-3a-2021-08-24-disk001.vdi	50.00 GB	48.39 GB		
	>	Kali-Linux-2021.2-virtualbox-amd64-disk001.vdi	80.00 GB	10.55 GB		
	>	Lazysysadmin-disk1.vmdk	4.00 GB	489.12 MB		
		LemonSqueezy.vmdk	10.00 GB	6.33 GB		
	>	MERCY-disk1.vmdk	20.00 GB	1.23 GB		
	>	Stapler-disk1.vmdk	20.00 GB	722.82 MB		
	No	t Attached				
4						
	Search	By Name 🔻				A 🔊
					Choose	Cancel

The image should now be selected:

Hard disk
O Do not add a virtual hard disk
O Create a virtual hard disk now
Use an existing virtual hard disk file
LemonSqueezy.vmdk (Normal, 10.00 GB) 🔹 🗔

Then click create, and your machine should be ready to go.

Installing from a Disk Image

Similarly to installing from a .vmdk file in the above example, installing from a Disk Image requires creating a new machine (rather than importing one).

To import a downloaded Kali disk image (.iso file), hit Ctrl + N to create a new machine, select the Linux Operating system, and give it whatever specifications you want, but select the Create a virtual hard disk now option:

						?	Х
,	a						
<u> </u>	Create Virtual N	lachine					
	Name and some						
	Name and operat	ing system					_
	Name:	Test Kali					
	Machine Folder:	D:\Virtual Machi	nes				\sim
	<u>Type</u> :	Linux				▼ 64	2
	<u>V</u> ersion:	Oracle (64-bit)				- N	
	Memory size						
	_				1	024 🜲	мв
	4 MR				16294 MR		
	diffe				1000110		
	Hard disk						
	O <u>D</u> o not add a	virtual hard disk					
	Oreate a virt	ual hard disk now					
	🔿 <u>U</u> se an existi	ng virtual hard disk fil	2				
	R Lazysys	admin-disk1.vmdk (No	ormal, 4.00 GB)				
				C ided Made	Create	Control	
				Guidea Mode	Create	Cancel	

Decide what size virtual hard disk you want (we recommend at least 25GB):

? ×

Create Virtual Hard Disk

File size	•
	25 GE
4.00 MB	2.00 TB
Hard disk file type	Storage on physical hard disk
VDI (VirtualBox Disk Image)	Oynamically allocated
🔿 VHD (Virtual Hard Disk)	O Fixed size
🔿 VMDK (Virtual Machine Disk)	Split into files of less than 2GB
O HDD (Parallels Hard Disk)	
QCOW (QEMU Copy-On-Write)	
QED (QEMU enhanced disk)	

Now create the machine and go to Settings - from here, change the machine's boot order under the *System* tab:

🕑 Te	st Kali - Settings			?	×
	General	System			
	System	Motherboard Processor Acceleration			
	Display	Base Memory:	10)24 MB	*
\bigcirc	Storage	4 MB 16384 ME	3		
	Audio	Boot Order: 🗹 🙆 Hard Disk 🛧 🗹 💿 Optical 😱			
Ð	Network	Floppy Floppy Network			
	Serial Ports	<u>C</u> hipset: PIIX3 ▼			
Ø	USB	Pointing Device: PS/2 Mouse			
	Shared Folders	Extended Features: Enable I/O APIC Enable FET (special OSec only)			
	User Interface	Hardware Clock in UTC Time			
		OK		Can	cel

Then you must import the disk image you downloaded into the VM's optical drive - to do this, go to the *Storage* tab and click the entry that says *Empty*:

🕑 Te	st Kali - Settings				?	×	
	General	Storage					
	System	Storage Devices	Attributes				
	Display	Controller: IDE	Optical Drive:	IDE Secondary Device	0 🔻	•	
		Empty		Live CD/DVD			Choose/Create a Virtual Optical Disk
	Storage	left Controller: SATA	Information				Choose a disk file
	Audio	🔤 Test Kali.vdi	Type: Size:			G	Remove Disk from Virtual Drive
	Network		Location:			_	
	Serial Ports		Attached to:				
Ø	USB						
	Shared Folders						
	User Interface						
		🔄 🗟 🚱					
				ОК	Cancel		

Select your **.iso** file from the file explorer, and then press *Start* on the machine. It should now boot from the disk image you just selected, and start the installation process!

Follow the install wizard, selecting the keyboard layout and timezone settings you want, creating a new user, and configuring your disks - Kali's <u>official documentation</u> has a great guide to doing this, and we won't look at it here in the interests of keeping the guide short. If you don't want to go through the installation process, you should use a Machine Image instead.

Configuring the Machine

You can change the amount of RAM on your machine at any time by visiting the machine settings. There are a number of other options available, such as using a bidirectional clipboard.

For some features to work, including two-way copy and paste, you will need the VirtualBox Extension Pack - you can download it here:

https://www.virtualbox.org/wiki/Downloads:

VirtualBox 6.1.26 Oracle VM VirtualBox Extension Pack

Pall supported platforms

Support for USB 2.0 and USB 3.0 devices, VirtualBox ROP, 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 Pacesonal Use and Evaluation License (PUEL). Please install the same version pack as your installed version of VirtualBox.

After you've downloaded it, import them by going to *Tools > Preferences > Extensions* and clicking the **+** button:

🔋 Oracle VM VirtualBox Manager							
File Machine Help							
Tools //	Freferences Import Export New Add						
kali-linux-2019-3a	Welcome to VirtualBox!						
V Powered Off	The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can in popup a tools of currently selected element using corresponding element button.						
Kali-Linux-2021.2-virtualbox-amd64 (Snapshot 3)	You can press the F1 key to get instant help, or visit <u>www.virtualbox.org</u> for more information and latest news.						
Powered Off							
LemonSqueezy	VirtualBox - Preferences ? X						
Stapler W Powered Off	General Extensions						
LazySysAdmin W Powered Off	Update Active Name Version Version Version Active Name Version Active Name Version Active Name Version Active Name Active Name Version Active Name Active Nam						
Mercy Powered Off	Display Display Image: Network						
Test Kali	Extensions						
	Floxy						
	OK Cancel						

Networking a VM

This section is not necessary for a basic VM setup, but will be useful if you intend to connect two VMs together. You might, for example, want to have a Kali VM and a

vulnerable Virtual Machine from VulnHub to attack.

Having the right networking settings is important, as you don't want to have a vulnerable virtual machine exposed to the internet!

To connect two VMs together, the easiest option is to use a VirtualBox Host-Only adapter.

Your Kali VM, for example, will want one adapter still connected to the internet - use a NAT adapter for this:

Network								
Adapter 1 Adapter 2	Adapter 3 Adapter 4							
Enable Network Adapter								
Attached to: NAT								
Name:	7							
V Advanced								
Adapter Type:	Intel PRO/1000 MT Desktop (82540EM)							
Promiscuous Mode:	Deny 👻							
MAC Address:	0800270E348D							
	Cable Connected							
	Port Forwarding							
	OK Cancel							

The second adapter for the Kali machine should be a host-only adapter:

	General	Network							
	System	Adapter 1 Adapter 2 Adapter 3 Adapter 4							
	Display	Enable Network Adapter							
\bigcirc	Storage	Attached to: Host-only Adapter							
\mathbf{P}	Audio	Name: VirtualBox Host-Only Ethernet Adapter Value							
Ð	Network	Adapter Type: Intel PRO/1000 MT Desktop (82540EM)							
	Serial Ports	Promiscuous Mode: Deny 🔻							
Ø	USB	MAC Address: 0800279CCF99							
	Shared Folders	Cable Connected Port Forwarding							
	User Interface								
		OK Cancel							

The vulnerable machine should have **only** a host-only adapter, so that it can only communicate with other VMs (and not the internet):

🕑 br	ainpan - Settings							?	×
	General	Network							
	System	Adapter 1	Adapter 2	Adapter 3	Adapter 4				
	Display	Enable N	etwork Adapt	ter					
\bigcirc	Storage	A	Attached to:	Host-only Adapt	er	•			_
	Audio		Name:	VirtualBox Host-	Only Ethernet A	Adapter			•
	Network	Ad	apter Type:	PCnet-PCI II (Ar	n79C970A)				•
	Serial Ports	Promisc	uous Mode:	Deny					•
0	USB	M	AC Address:	080027975030					9
	Shared Folders			Cable Connec	ted	1			
=	User Interface				2				
		Invalid s	settings dete	cted <u>N</u>			ОК	Car	ncel

The final step will be to make the host-only interface on Kali automatically assign IP addresses - to do this, edit your <a>/etc/network/interfaces file:

\$ sudo nano /etc/network/interfaces

The edited file should look like this, with the ethi interface assigning IPs automatically:



You should now be able to scan the eth1 interface and discover the IP of your vulnerable machine!

```
└──(kali⊛kali)-[~]
└─$ sudo arp-scan --interface eth1 192.168.56.102/24
Interface: eth1, type: EN10MB, MAC: 08:00:27:9c:cf:99, IPv4: 192.168.56.102
WARNING: host part of 192.168.56.102/24 is non-zero
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-
scan)
192.168.56.1
               0a:00:27:00:00:12
                                        (Unknown: locally administered)
192.168.56.101 08:00:27:97:50:30
                                        PCS Systemtechnik GmbH
192.168.56.100 08:00:27:9e:b0:fe
                                        PCS Systemtechnik GmbH
3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.025 seconds (126.42
hosts/sec). 3 responded
```

Above: an arp-scan showing the vulnerable machine with IP address 192.168.56.101

An alternative command to scan this interface is nmap -sn 192.168.56.0/24

Learn more about VirtualBox networking types here: https://www.virtualbox.org/manual/ch06.html

Worksheet

- 1. Install a Kali Virtual Machine, either using a Machine Image or a Disk Image
- 2. Install Pinky's Palace from VulnHub: <u>https://www.vulnhub.com/entry/pinkys-</u> <u>palace-v1,225/</u> - this is an OVA file, so it can be imported as a <u>Machine Image</u>
- 3. Network Kali and Pinky's Palace together with host-only adapters, and discover the IP for Pinky's Palace