

System Preparation: Virtualization and Linux OS Installation

© 2016

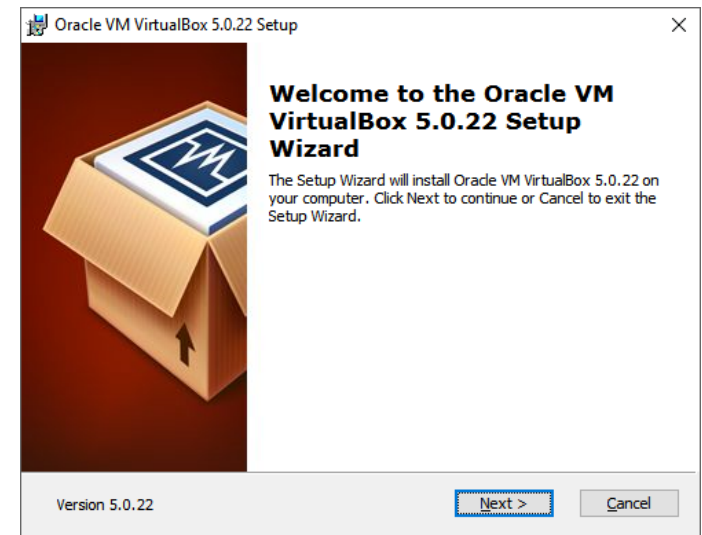
David Raymond, Ph.D.

Virtual Machines and VirtualBox

- A Virtual Machine is a computer running inside a computer
- Oracle's VirtualBox provides the ability to host almost any OS as a guest inside a host OS.
- We will install VirtualBox, then create a new virtual machine and install a Linux operating system
- Not the only virtualization software
 - HyperV, VirtualPC, VMWare, Xen, Linux Vserver, DOSBox...

Installing VirtualBox

- Download from <https://www.virtualbox.org/wiki/Downloads>
 - (Or Google “virtualbox download”)
 - Select VirtualBox 5.0.2.2 for Windows hosts
- VirtualBox is open-source software
 - Free to use and modify
- ***Once downloaded, install using default paths and settings.***



Having trouble? Get on IRC and ask for help!

Building a Virtual Machine in VirtualBox

Download Kali Linux ISO

www.kali.org/downloads

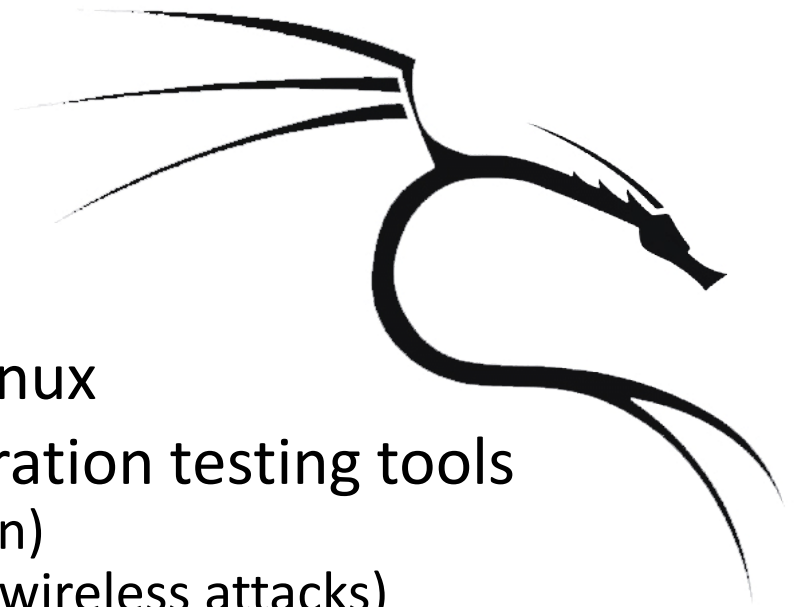


The screenshot shows a web browser window with the address bar containing the URL <https://www.kali.org/downloads/>, which is circled in red. The page title is "Kali Linux Downloads". Below the title, there is a section "Download Kali Linux Images" with a paragraph explaining that fresh Kali Linux image files are generated every few months. Below this, there is a section for "Kali Linux armelImageTorrent0.7G" with a version "2016.1" and a SHA1Sum "b40781f0427924256ce8c7d1c3cbbb5cc824b5fa". A table lists the available images.

Image Name	Direct	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit	ISO	Torrent	2.6G	2016.1	deaa41c5c8f26b7854cafb34b6f1b567871c4875
Kali Linux 32 bit	ISO	Torrent	2.6G	2016.1	23dadf9c6d3fcd190e345ee070aa57155e93b745
Kali Linux 64 bit Light	ISO	Torrent	0.8G	2016.1	4132238042deba9e3bc1702afbdb1b4672b64bcb
Kali Linux 32 bit Light	ISO	Torrent	0.8G	2016.1	addd89b750e31030e96c6cbd5a3da4f0f17287a8
Kali Linux armhf	Image	Torrent	0.7G	2016.1	cd750dde538eae9f8e4efea011a9b9dc1e75143

- An **ISO image** is an archive for an optical drive
 - Name is taken from ISO 9660, the file system used with CD-ROM media.

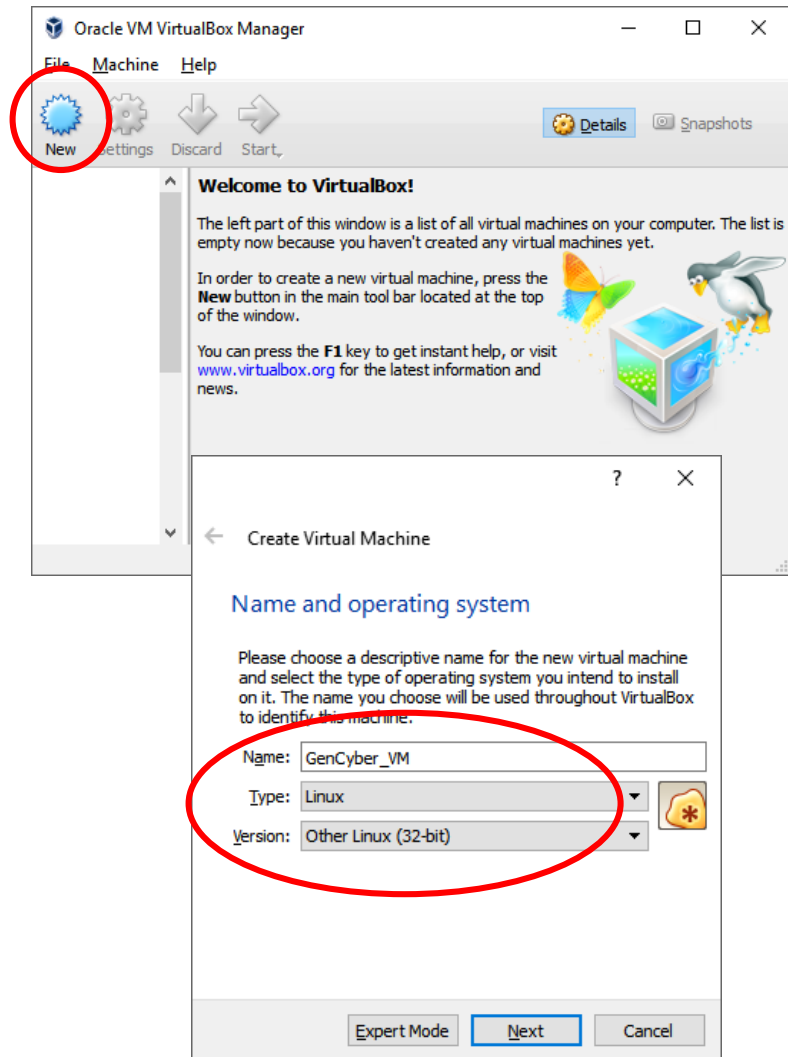
Kali Linux



- Linux distro based on Debian Linux
- Packaged with extensive penetration testing tools
 - Metasploit/Armitage (exploitation)
 - Aircrack-ng/Kismet/Bluesnarfer (wireless attacks)
 - Burp suite/Maltego/Paros/Zaproxy (web app attacks)
 - Foremost/P0f/RegRipper/Volatility (forensics)
 - Nmap/sslstrip/Wireshark/tcpdump (recon/analysis)
 - John the Ripper/Ncrack/Rainbow crack (password cracking)
 - Edb-debugger/OllyDbg/YARA (reverse engineering)
 - And hundreds of other tools
- Root user login by default!
- Widely used by security professionals and “hackers”

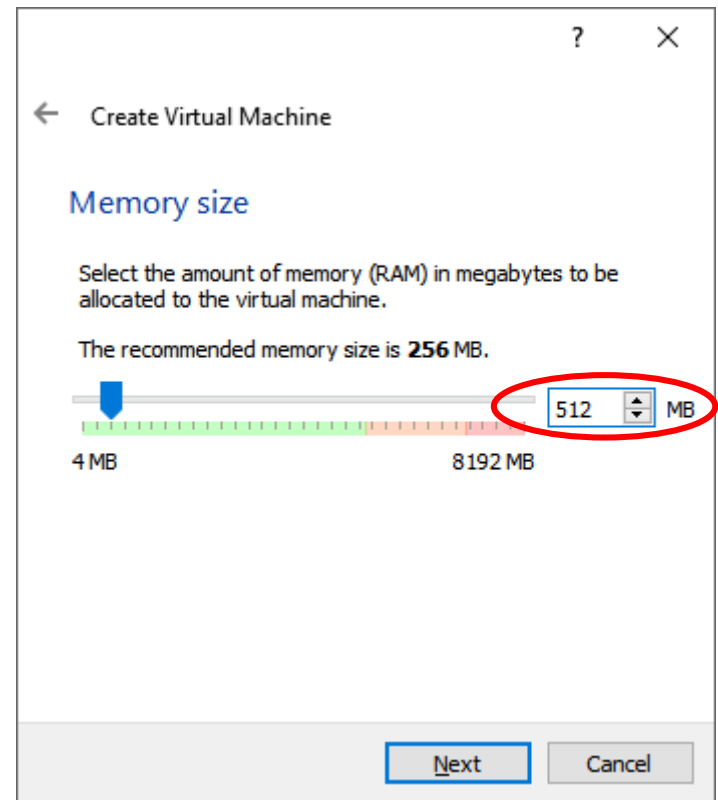
Create New Virtual Machine

- Start VirtualBox
- In the VirtualBox window, click the **New** button
- In the Create Virtual Machine dialog:
 - Name: **GenCyber_VM**
 - Type: **Linux**
 - Version: **Other Linux (32-bit)**
- Click **Next**



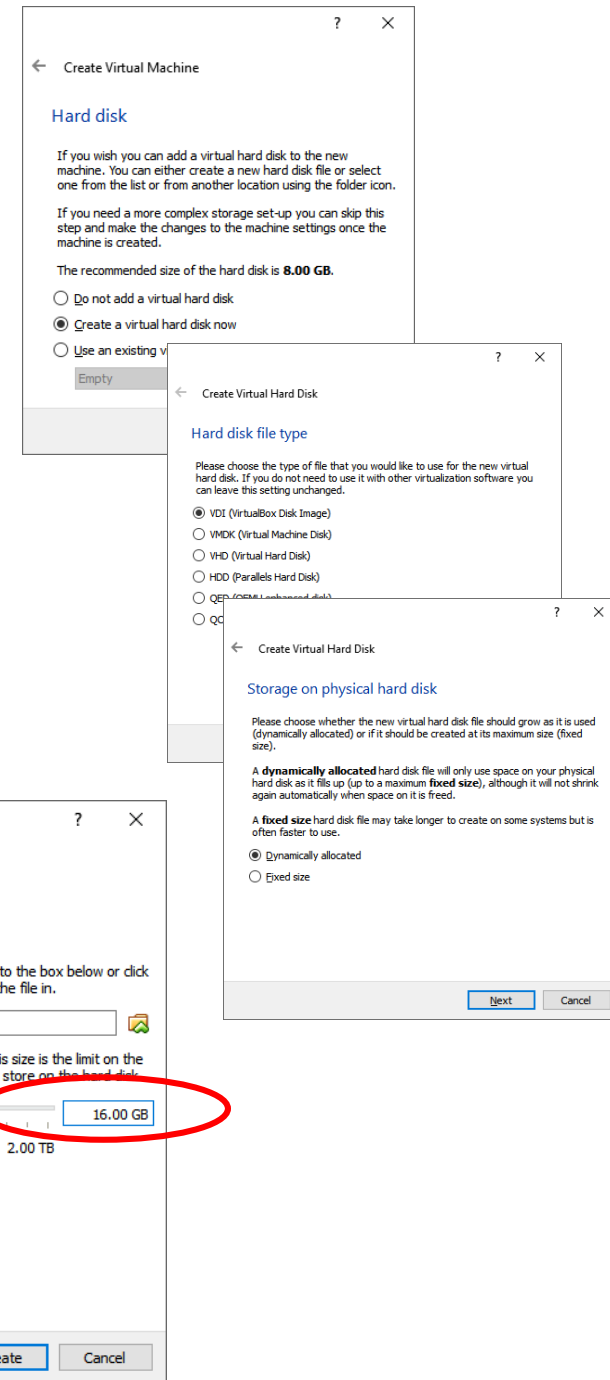
Create New VM (cont)

- Change Memory Size to **512 MB**
- Click “**Next**”



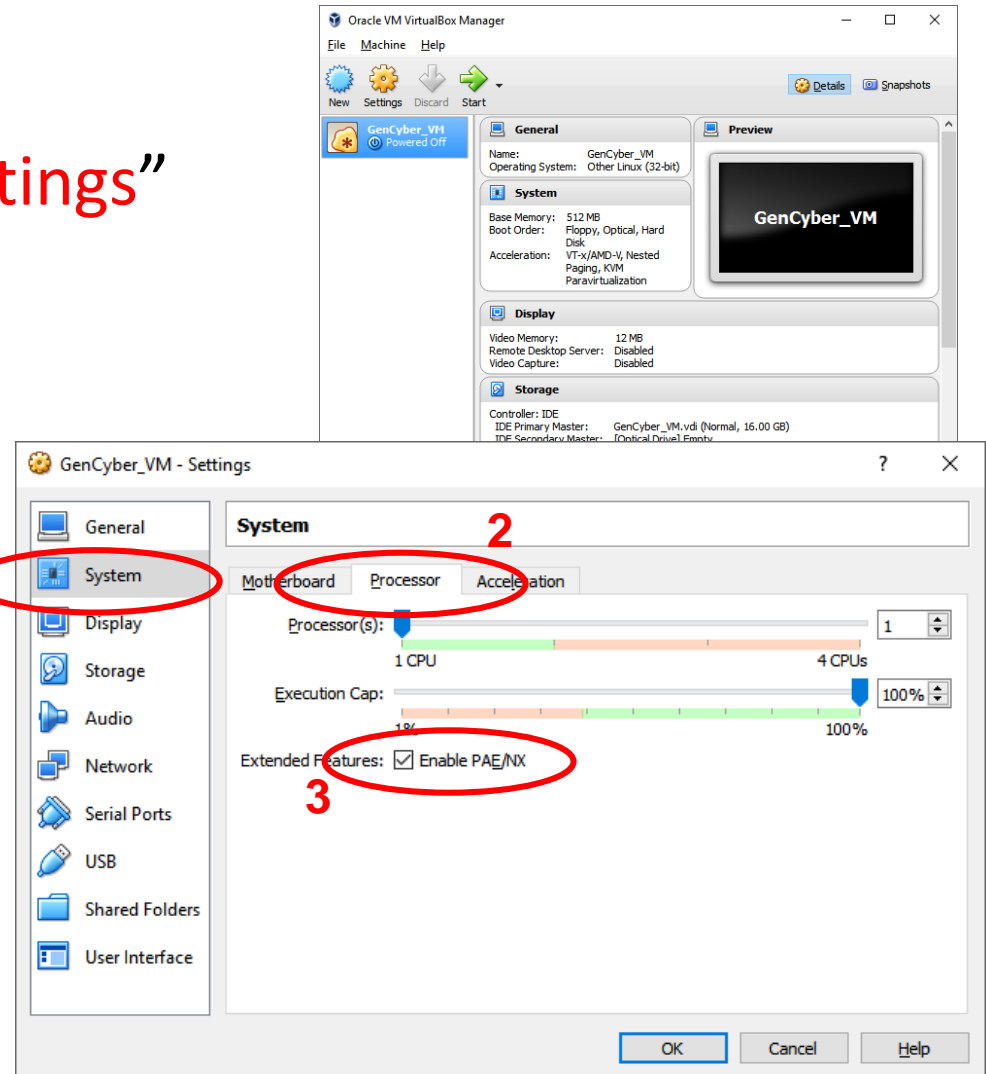
Create VM: Hard Disk

- Select “Create a virtual hard disk now”
 - Then “Create”
- Select “VDI (VirtualBox Disk Image)”,
 - Then “Next”
- Select “Dynamically allocated”
 - Then “Next”
- Change size to “16.00 GB”
 - Then “Create”



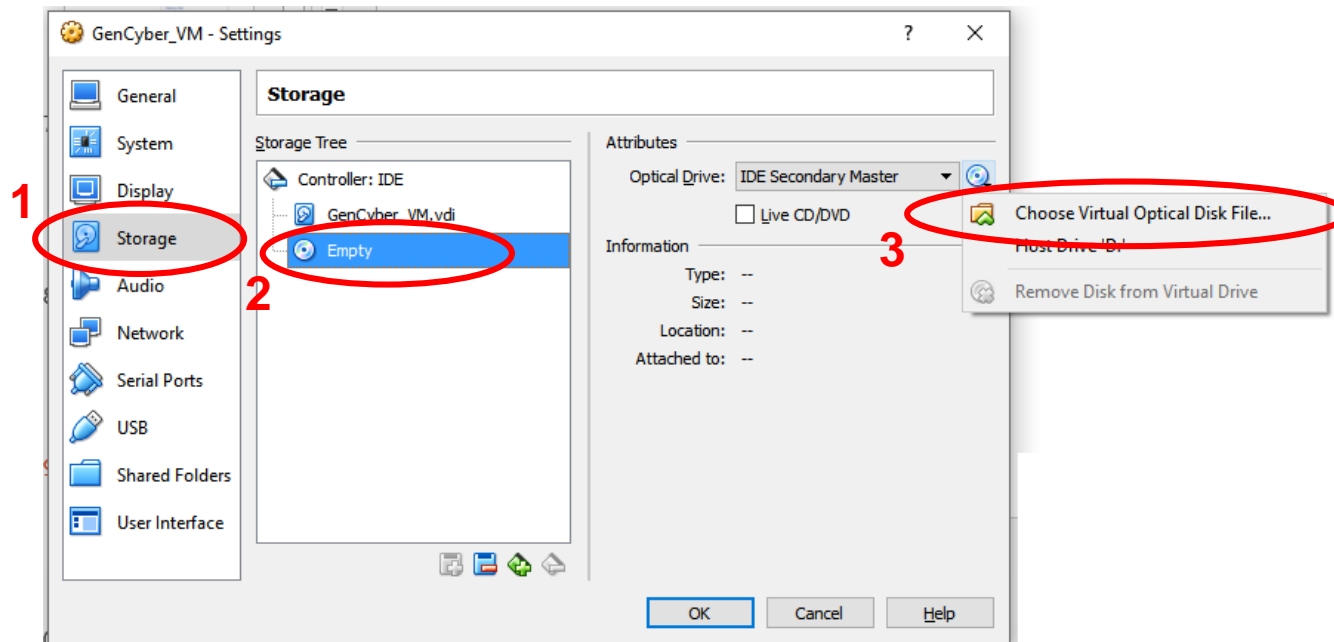
Configure Settings (1 of 3)

- With GenCyber VM selected, click on “Settings” button
- In Settings window . . .
 - Select “System”
 - “Processor” tab
 - Click “Enable PAE/NX” checkbox



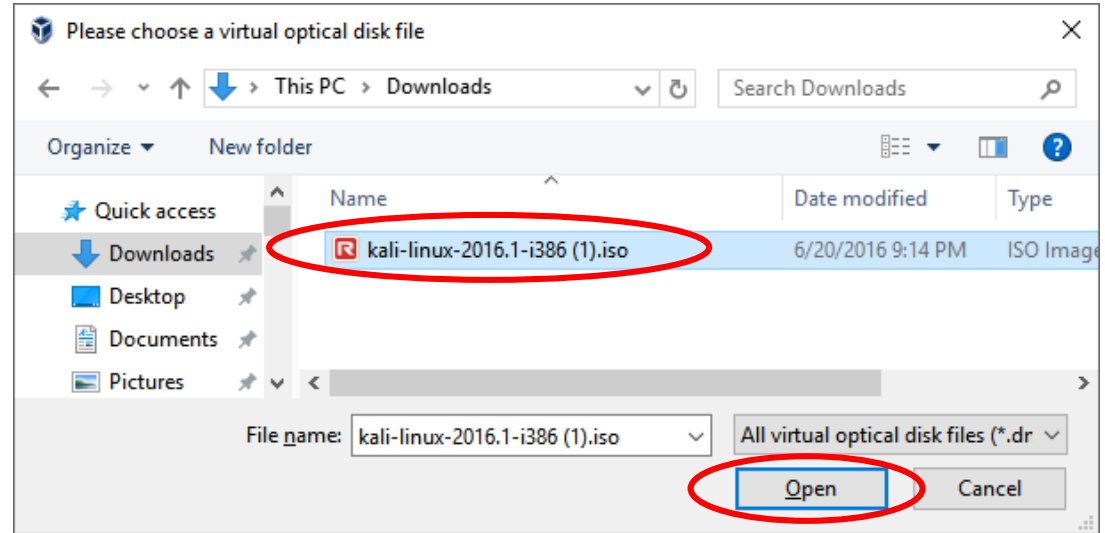
Configure Settings (2 of 3)

- Select “**Storage**”
- Select the “**Empty**” CD tray
- Click CD icon on the far right of the Settings dialog and click “**Choose Virtual Optical Disk File . . .**”

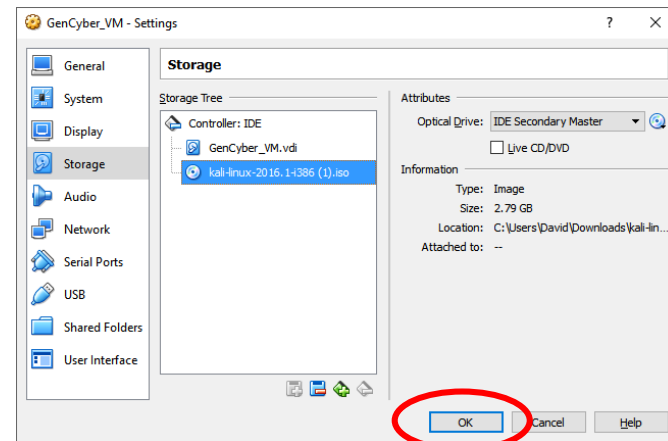


Configure Settings (3 of 3)

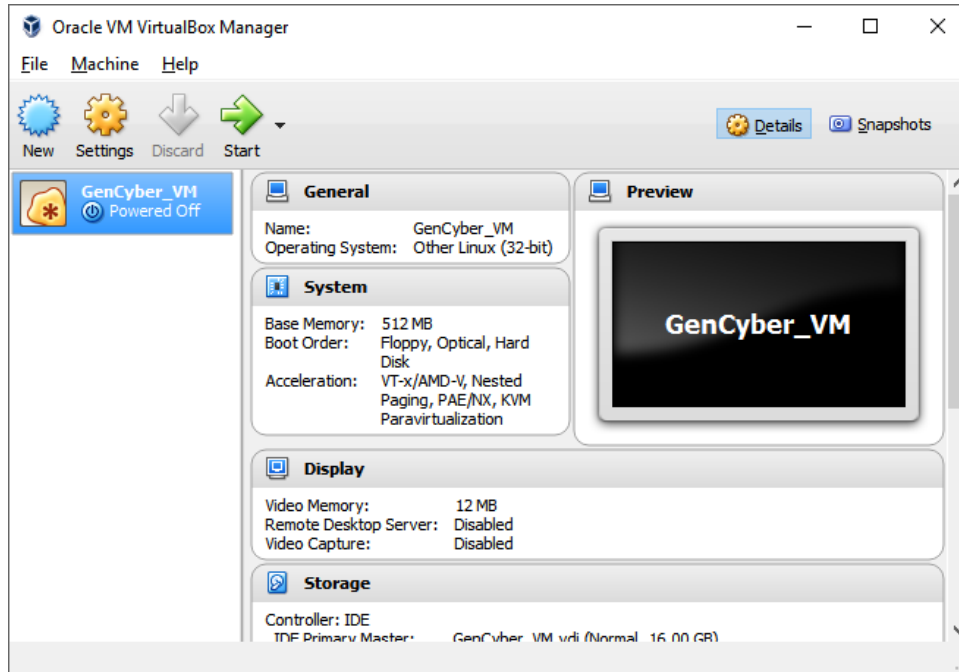
- Browse to the Kali Linux ISO you grabbed earlier and click “Open”
 - It is probably in your Downloads folder



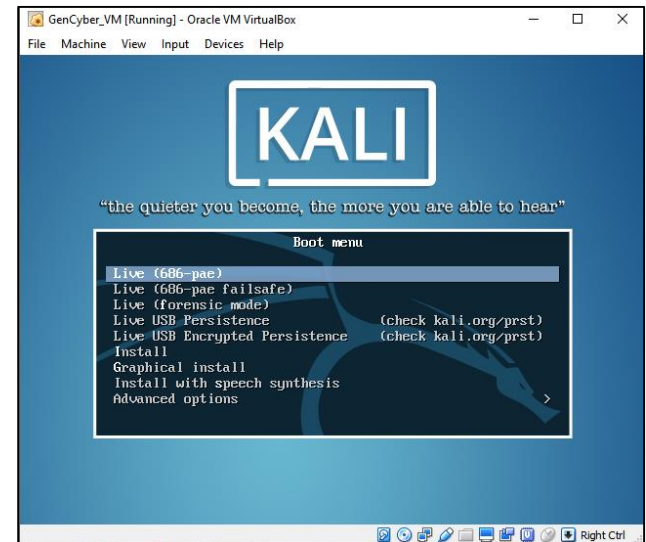
- Finally, click “OK”



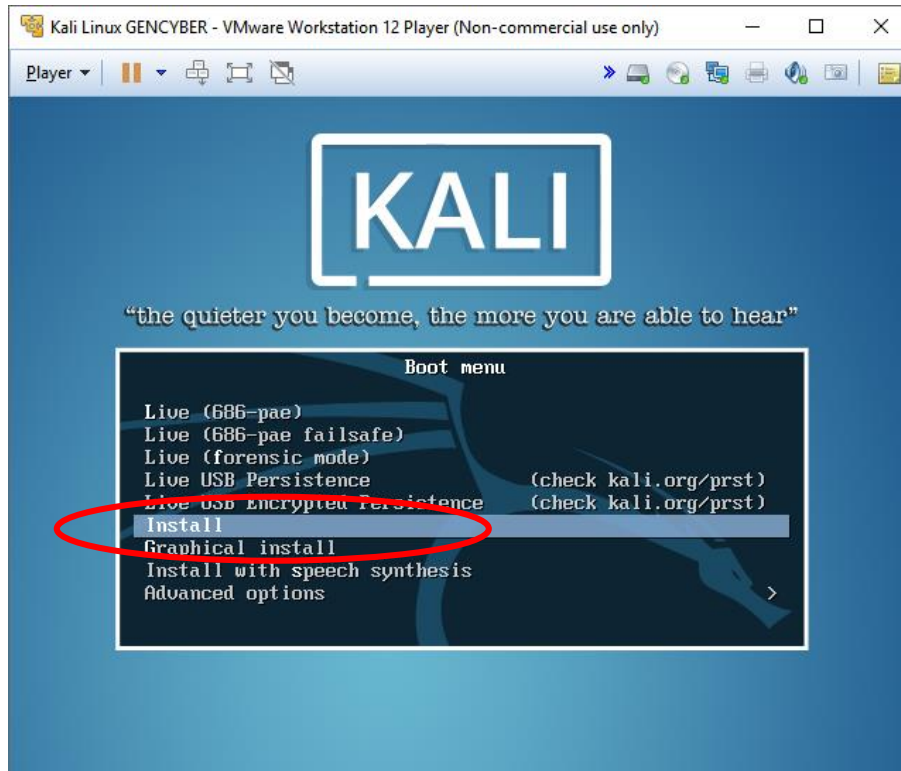
All set up! Now Start the VM!



- If everything works, you'll end up here.



Getting ready to install OS



- You are now running a virtual machine – a computer within your computer!
- Click inside the VM window – you will lose your mouse because the VM isn't ready to react to mouse commands yet.
- Use down arrow key to select 'Install', then press enter

- Press the right "CTRL" key to return control back to the host machine – this will give you your mouse back.

Install Linux OS on your virtual computer

- You can accept defaults for (almost) everything . . .
 - Language: **English** [Enter]
 - Location: **United States**
 - Keyboard: **American English**
 - (wait for additional components)
 - Hostname: **Kali** (or change it if you would like)
 - Domain name: **leave blank**
 - Root password: **You pick**, but make sure it is something you will remember! (and write it down).
 - Clock: **Eastern**
 - (wait for install/configuration)
 - Partition disks: Use default settings
 - **Guided – use entire disk**
 - **SCSI3 (0, 0, 0) (sda) – 17.2 GB ATA VBOX HARDDISK`**
 - **All files in one partition**
 - **Finish partitioning and write files to disk**

Install OS (continued)

```
[[!]] Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you
will be able to make further changes manually.

The partition tables of the following devices are changed:
  SCSI3 (0,0,0) (sda)

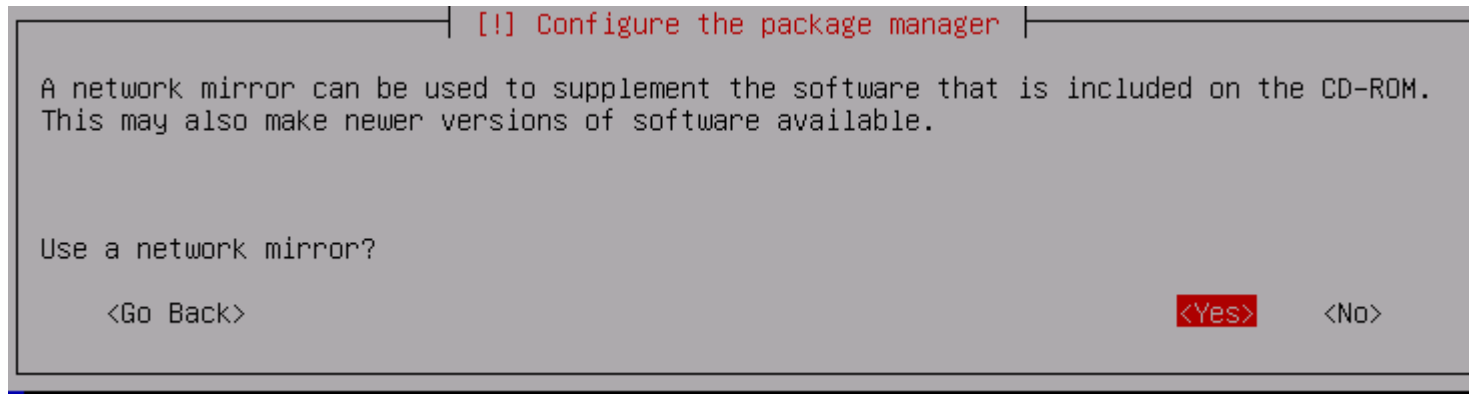
The following partitions are going to be formatted:
  partition #1 of SCSI3 (0,0,0) (sda) as ext4
  partition #5 of SCSI3 (0,0,0) (sda) as swap

Write the changes to disks?
<Yes>                                     <No>
```

- This screen is here help ensure you don't accidentally overwrite a hard drive. Since this is inside your VM, it is perfectly safe.
- Use Tab key to select **<Yes>** and hit enter.

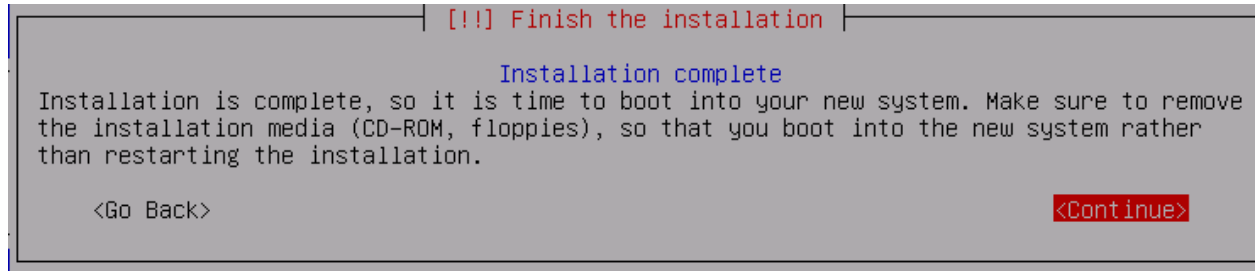
- Now sit back and wait – installation will take 15 min or so.
- Press Ctrl/Alt to escape your VM and get back to Windows.

Install OS: Getting close(r)

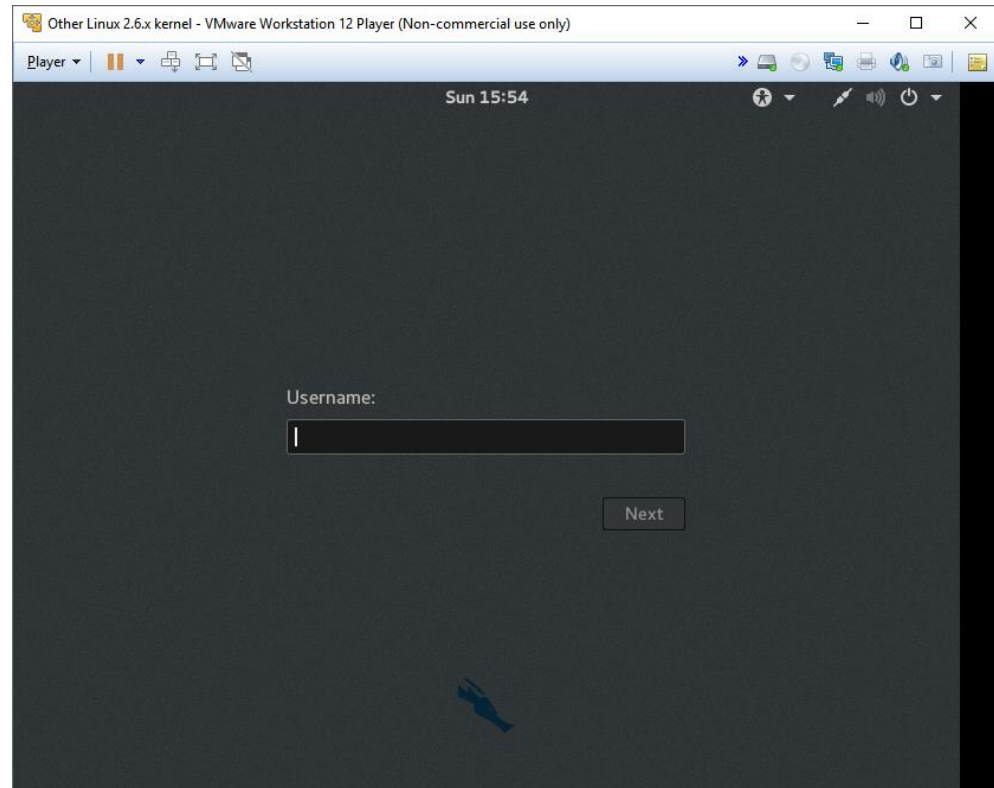


- Use a network mirror? **<Yes>**
- Leave the 'proxy setting' page **blank** (just press Enter)
 - Updated packages will download and install
- GRUB boot loader? **<Yes>**
- Device? Down arrow to **'/dev/sda'** to install on primary partition

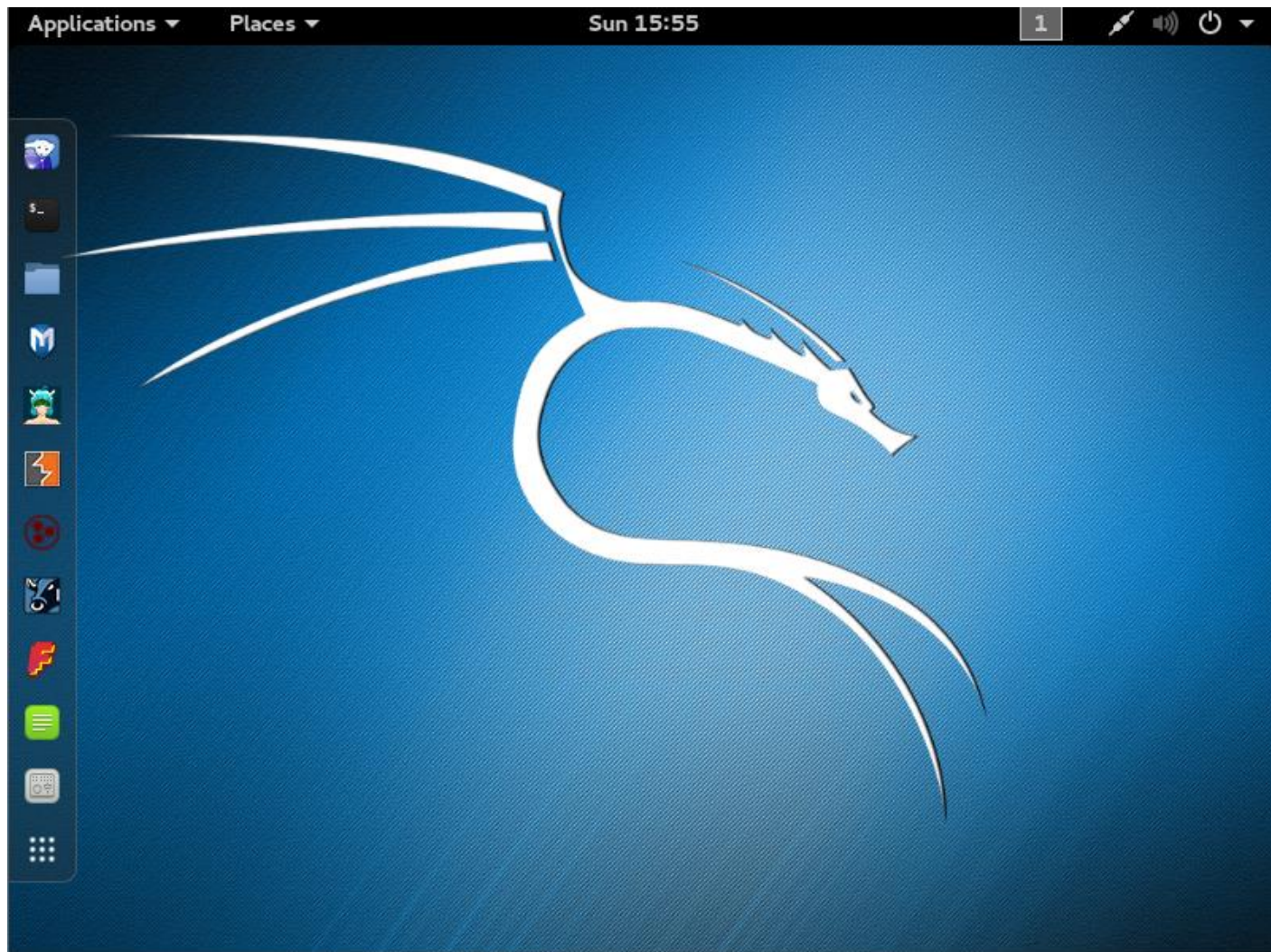
Finished!



- Press Enter (<Continue>) to boot into your new Kali Linux computer!
 - Again, this will take a few minutes . . .
- Wait until you get to this screen
 - Username: **root**
 - Password: *what did you pick?*



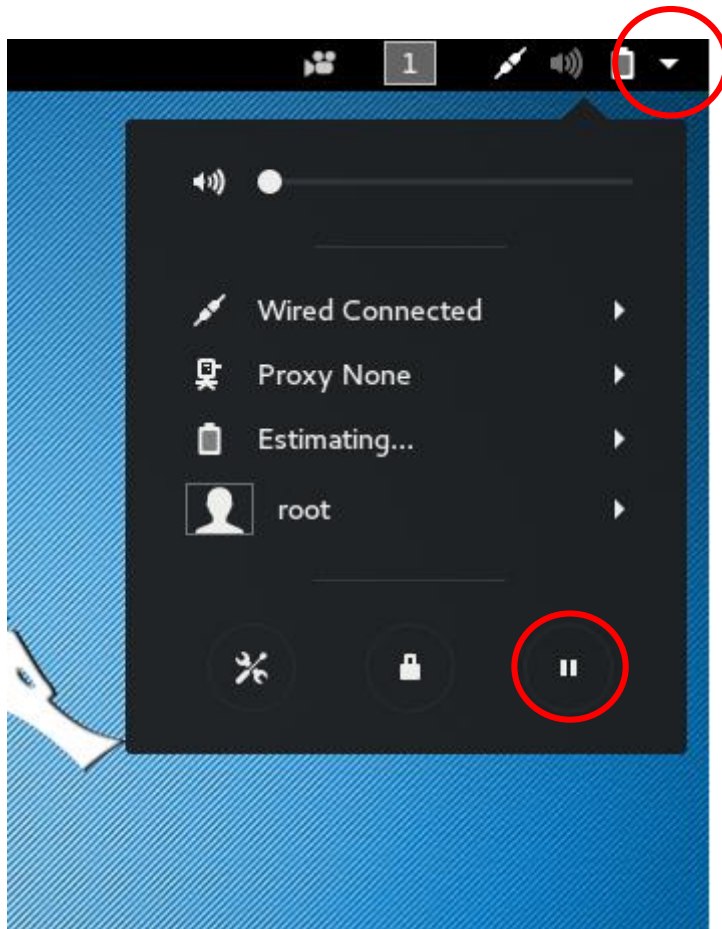
Kali Linux!



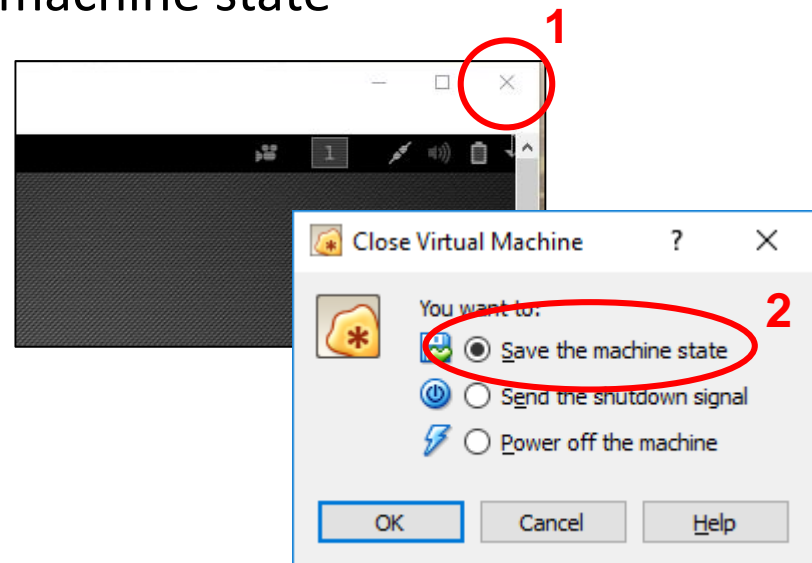
VM Settings and Tools

- Escape a VM: Right Ctrl key (you can change this in settings)
- Menu:
 - Machine:
 - Snapshot
 - Pause
 - View – full screen
 - Devices

Shutting down and pausing VMs



- To shut down VM, select the down arrow at the upper-right corner of the Kali desktop, then the “pause” button . . .
- Or simply close the VirtualBox window and choose to “Save the machine state”



Other Recommended Software

- Other tools you can install in Windows 10 (we'll discuss these throughout the week)
 - FoxIT PDF Reader
 - <https://www.foxitsoftware.com/products/pdf-reader/>
 - Wireshark for packet analysis
 - <https://www.wireshark.org/download.html>
 - Nmap for network mapping
 - <https://nmap.org/download.html>
 - Putty for remote system access
 - <http://www.putty.org/>
- Install VirtualBox Guest Additions for Kali Linux
 - You'll need to do some Googling here!
 - *Snapshot your VM before you do this – you can break things!*