IntroToCTF:
Intro to VMs and Linux

What is IntroToCTF?

IntroToCTF

- Weekly **hacking tutorials** focusing on **key CTF topics** and **techniques**
- Lessons taught by **specialists in each area**
- Extra sessions run by **Mirek Malinowski** and **WMG sponsors**
- Will be **published online** as a **learning resource**

What is Linux?

What is Linux?

- “**Linux**” refers to **Linux distributions**, a family of **operating systems** built around the open source **Linux kernel**
- The **customisability** of Linux installations has made it the default choice for:
  - **Web servers**
  - **Embedded systems**
  - **Software development infrastructure**

Why do I need to know about Linux?

- CTFs are designed to help you practise **real world offensive security**
- Because so much **network infrastructure** runs on Linux, offensive security involves a lot of **exploiting Linux-based systems**
- The majority of CTF/offensive security **tooling** is designed to run on Linux
- To be **good at CTFs** you need to be **comfortable with Linux**

Virtual Machines

What is a Virtual Machine?

- **Virtual machines** (“**VMs**”) are **self-contained operating systems** which run **within applications** on the “**host**” operating system
- Creating a Linux VM with **VirtualBox** lets you use a **full Linux Operating System** in an app on your windows desktop

Why use a virtual machine?

- Having a **working Linux environment** is essential to **compete in CTFs**
- Competing in CTFs can involve dangerous work, including:
  - Analysing and running **malware**
  - Running **untrusted software**
  - Using **unstable software**, which can **damage the operating system**
  - Connecting to networks with a lot of **hackers**, some of whom might act maliciously
- You should keep all of the above activates **separate from your host OS**

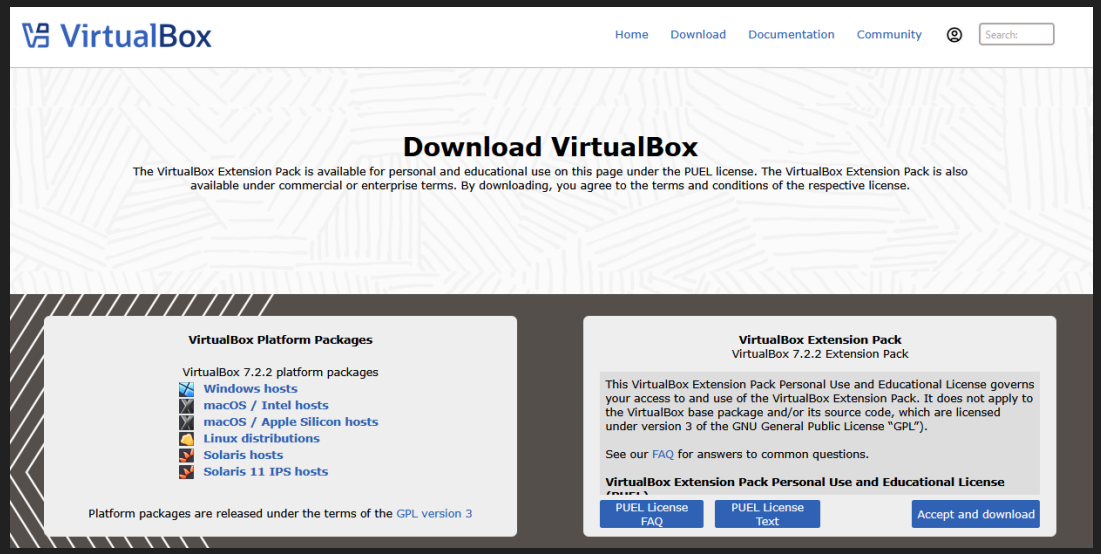
What is Kali Linux?

- **Kali Linux** is an **offensive-security focused** Linux distribution, with a lot of pre-installed tools.
- It's really useful for **creating a CTF VM quickly**, without having to configure those tools yourself
- It's **not very stable**, and you **shouldn't install it as your host OS**

Tutorial – Creating a Kali Linux Virtual Machine

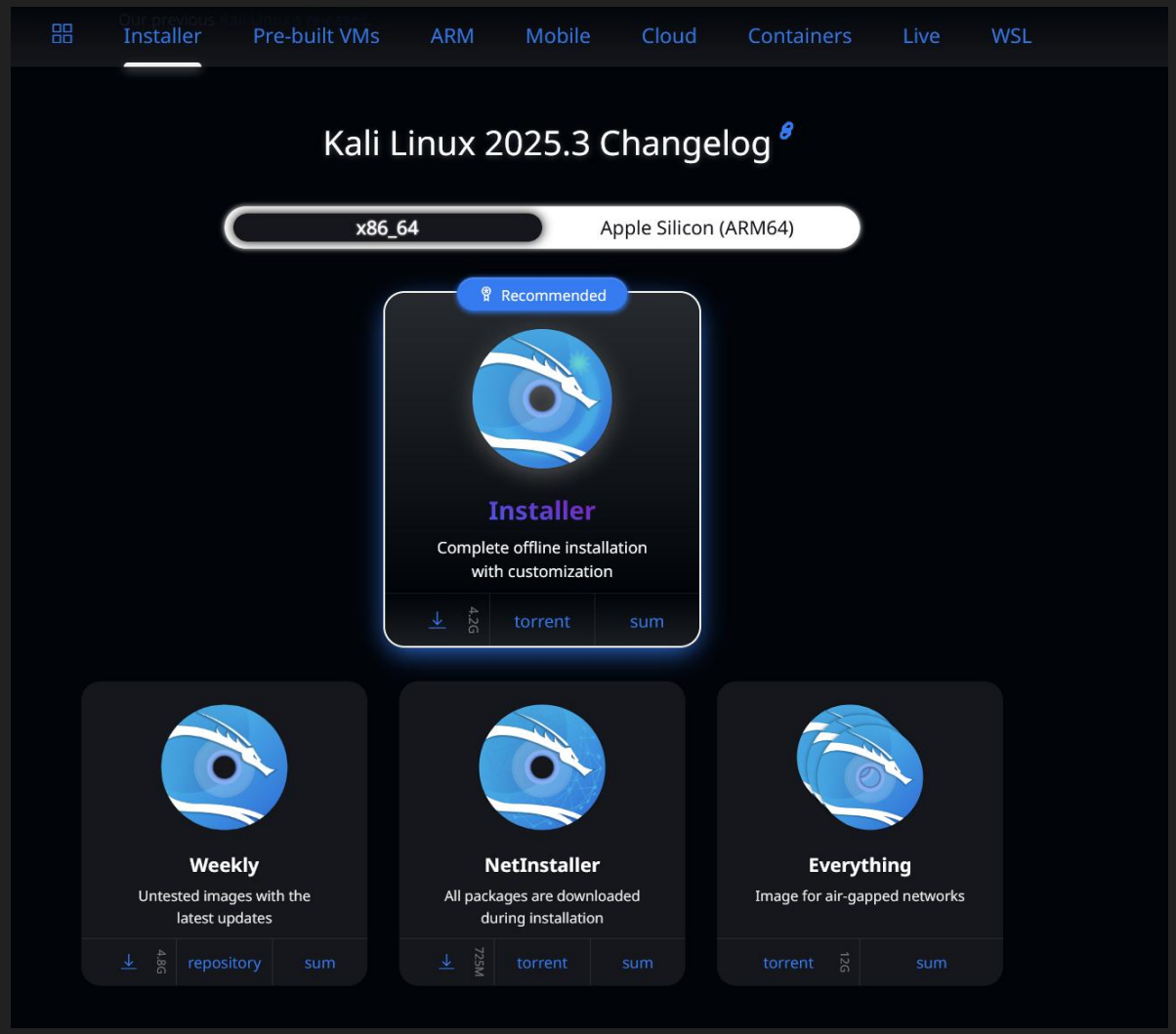
1. Download VirtualBox

- Go to www.virtualbox.org/wiki/Downloads
- Download and run the **Windows** or **MacOS installer**, leaving everything as **default**



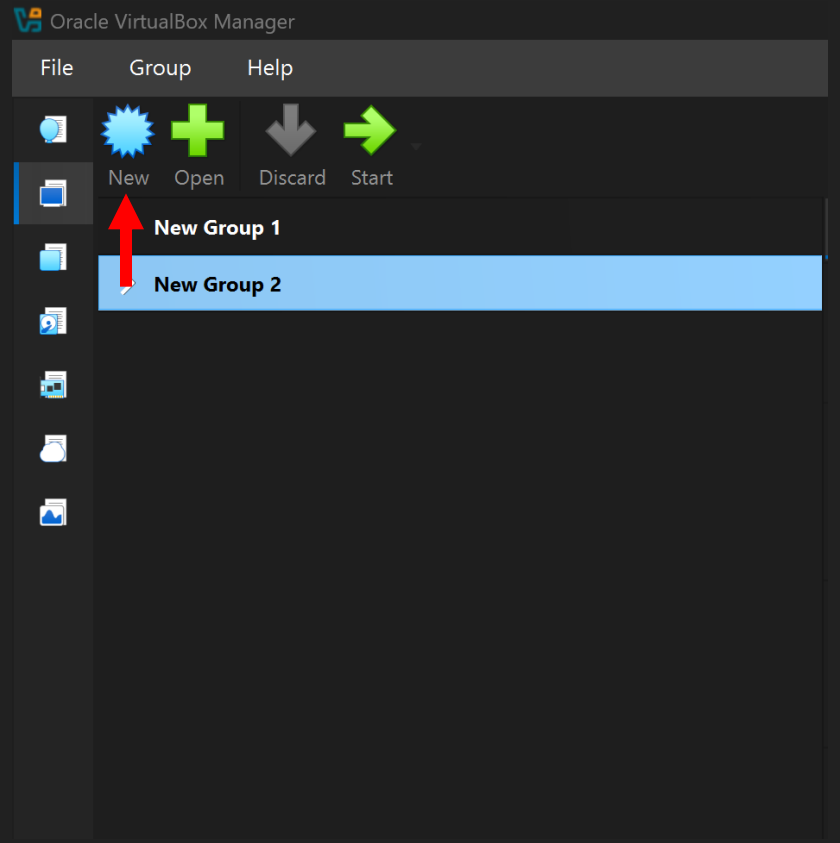
2. Download a Kali Linux ISO

- **.iso files**, or "**images**", are used to **write an operating system to a disk**
- Go to www.kali.org and navigate via **Download** -> **Installer Images** to the following page
- Download the "**Installer**" image. Select "**x86_64**" for **most Windows laptops**, and "**ARM64**" for **M-series Macbooks**



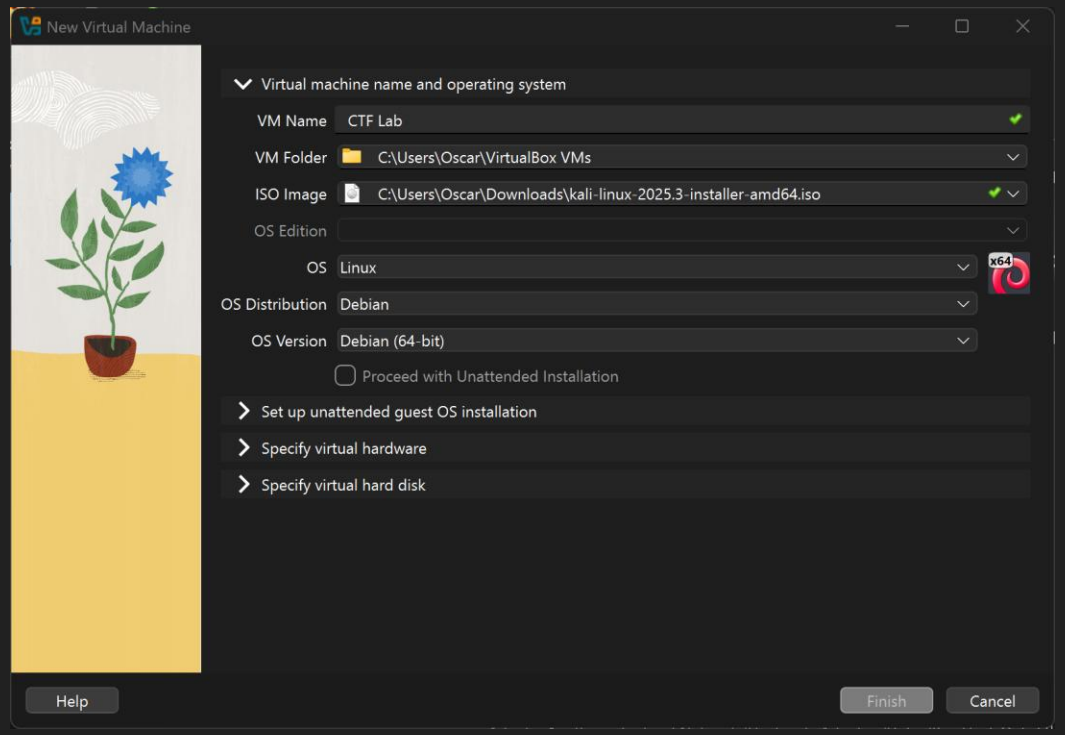
3. Create a new virtual machine in VirtualBox

- Navigate to the “**Machines**” tab (second from the top on the left
- Select “**New**” to create a new VM



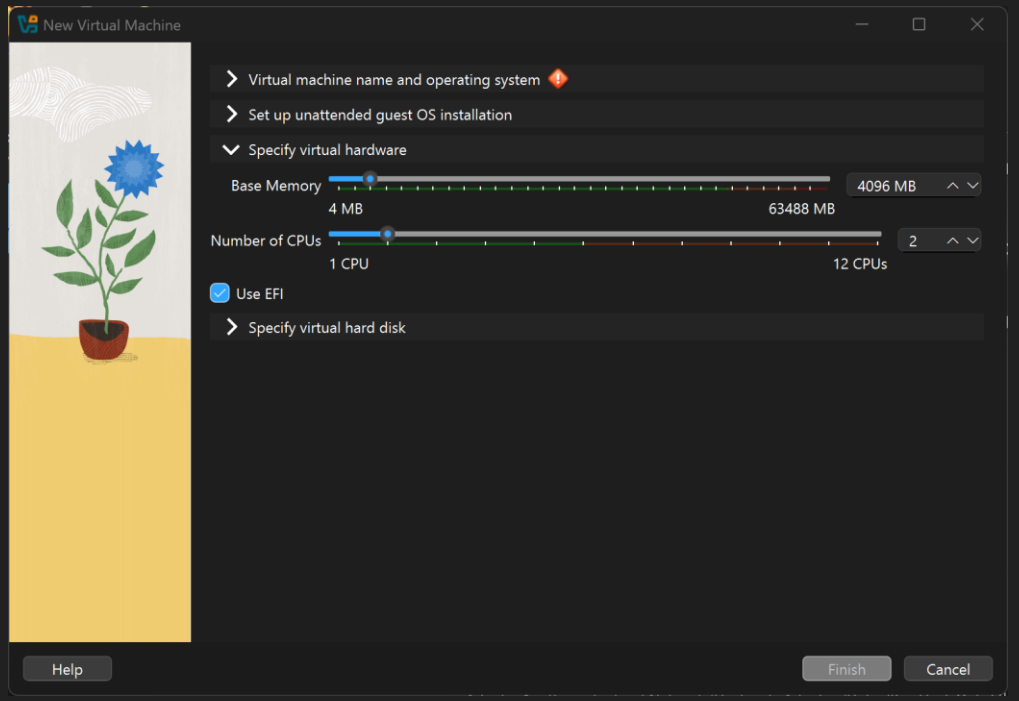
3. Create a new virtual machine – name and operating system

- Give your VM a **sensible name** like “**Kali Lab**”
- For “**ISO Image**” select your **Kali Linux ISO**
- For “**OS Distribution**” Select “**Debian**”
- For “**OS Version**” select “**Debian (64-bit)**”
- Make sure “**Proceed with Unattended Installation**” is **unchecked**



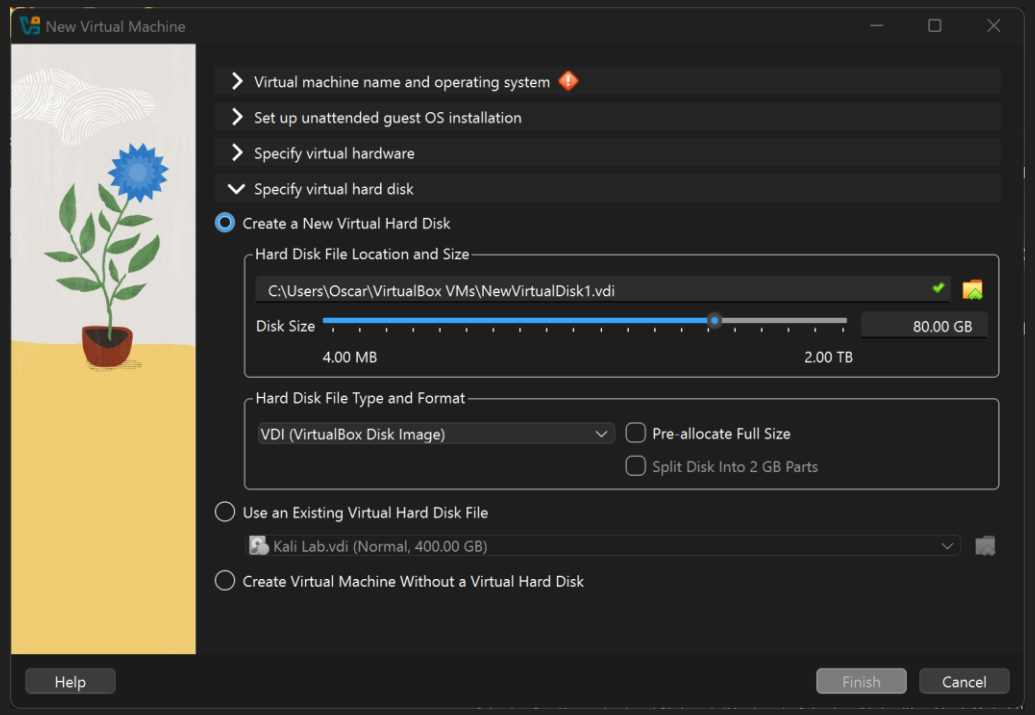
3. Create a new virtual machine – virtual hardware

- Under “**specify virtual hardware**” you can assign a **certain amount of memory** and a **certain number of CPU threads** to your virtual machine
- Assign **at least 2GB of memory**, ideally 4GB or more
- Ideally **2 or more CPU cores**, but **1 will work**
- Make sure the **number of megabytes** you assign for memory is **a multiple of 1024** (e.g. **2048**, **4096**, **8192**)



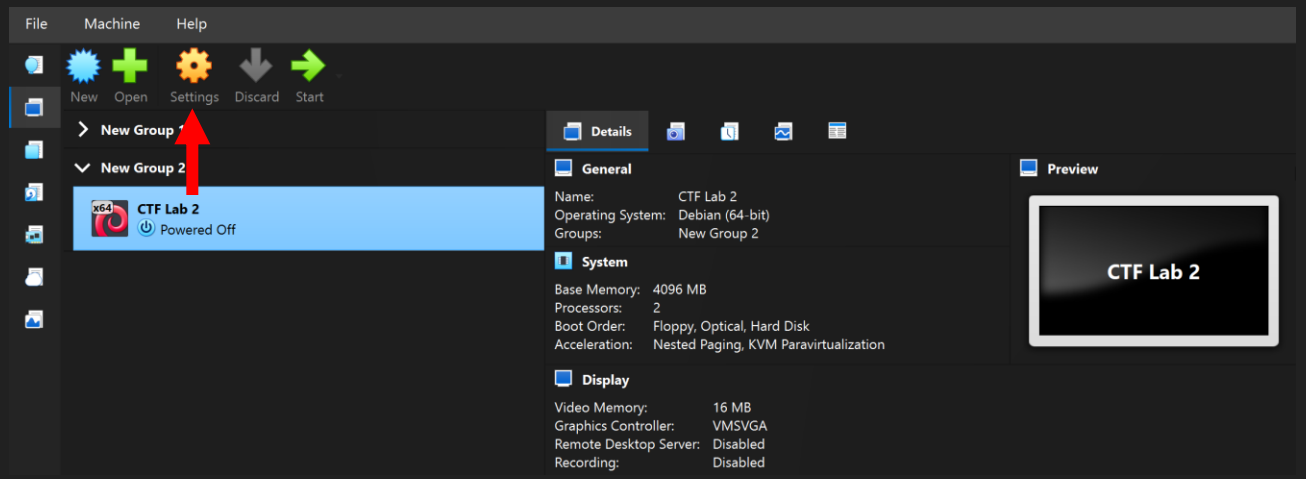
3. Create a new virtual machine – virtual hard disk

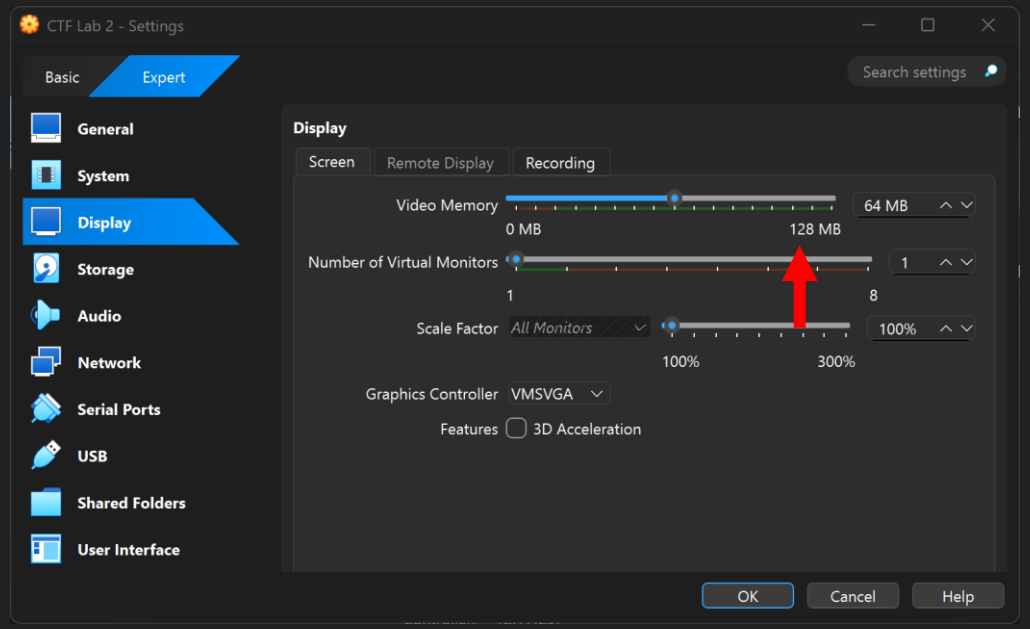
- Under “**Specify virtual hard disk**” select “**Create a New Virtual Hard Disk**”
- Allocate **at least 70GB**. If you can I’d recommend assigning 150+
- The virtual hard disk file will **not start out at that size**. It will **expand as the VM gets larger**, up to that maximum.
- Click “**finish**” once you’re done



4. Change the default settings

- **Select** your new VM (**don't double click**) and click **settings**
- Select the "**Display**" tab in the settings menu, and set "**Video Memory**" to at **least 64MB**
- If we **don't do this**, the VM will **crash a lot**



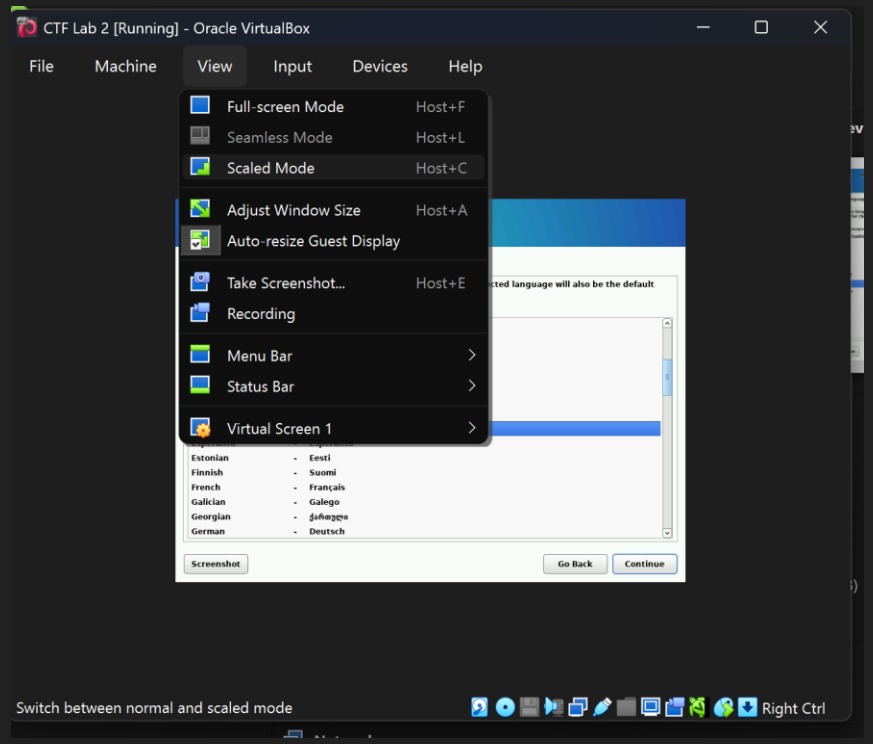


5. Launch the VM

- **Select** your new VM and click “**Start**” (green arrow at the top)
- The VM will boot. Select “**graphical install**”
- If your mouse stops working, **don’t panic**. The VM has “**captured**” your mouse. **Press Right Control** to “**release**” it back to your **host operating system**

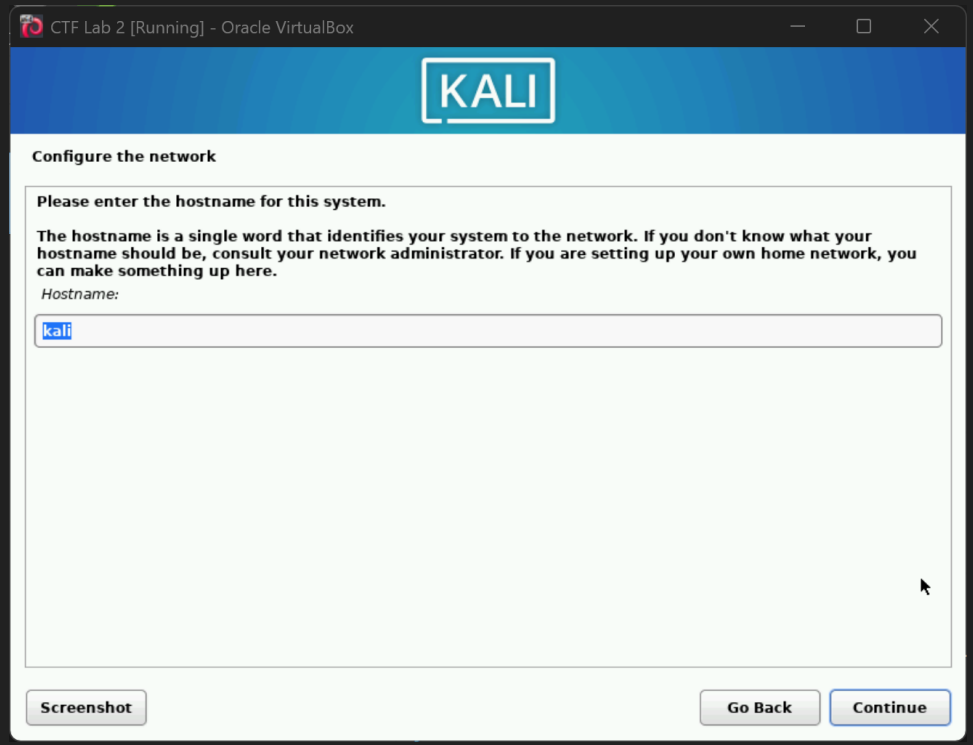
6. Go through the graphical installer

- Go through the **graphical installer**. The first few options are simple and set your **language** and **keyboard layout**
- If the VM window is **too small**, switch to **scaled mode** (under “**View**”) for now to scale it up (as shown)



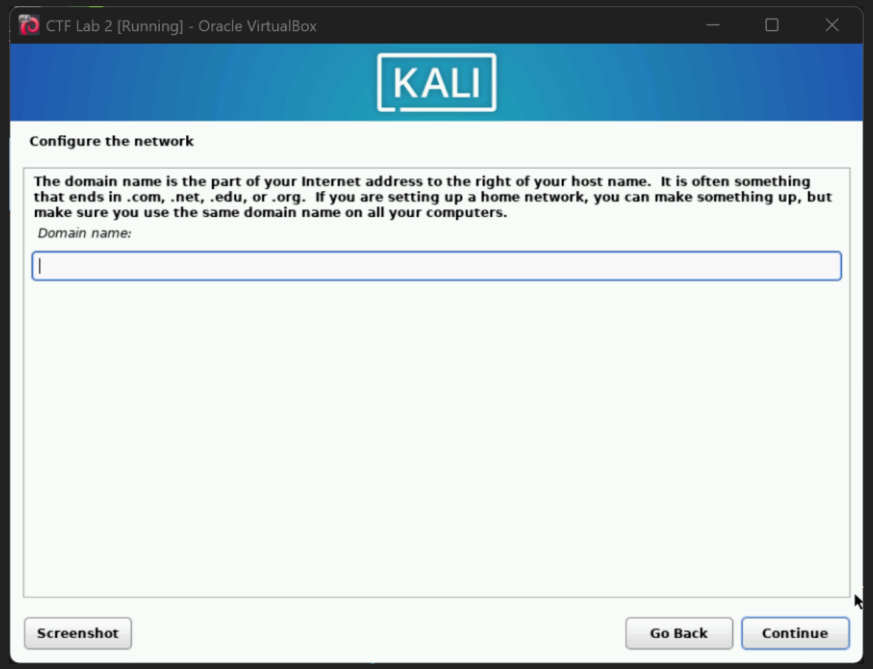
6. Graphical installer - hostname

- The **hostname** is what your installation will be called
- I recommend something simple like “**kali**” or “**kali-lab**”



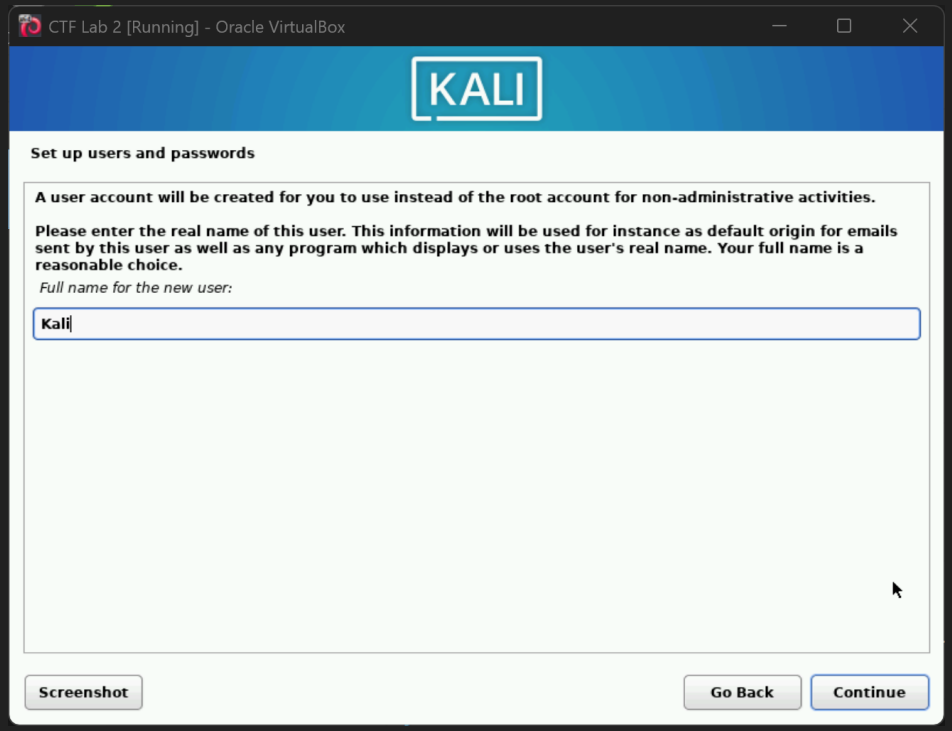
6. Graphical installer – domain name

- Leave the **domain name blank**



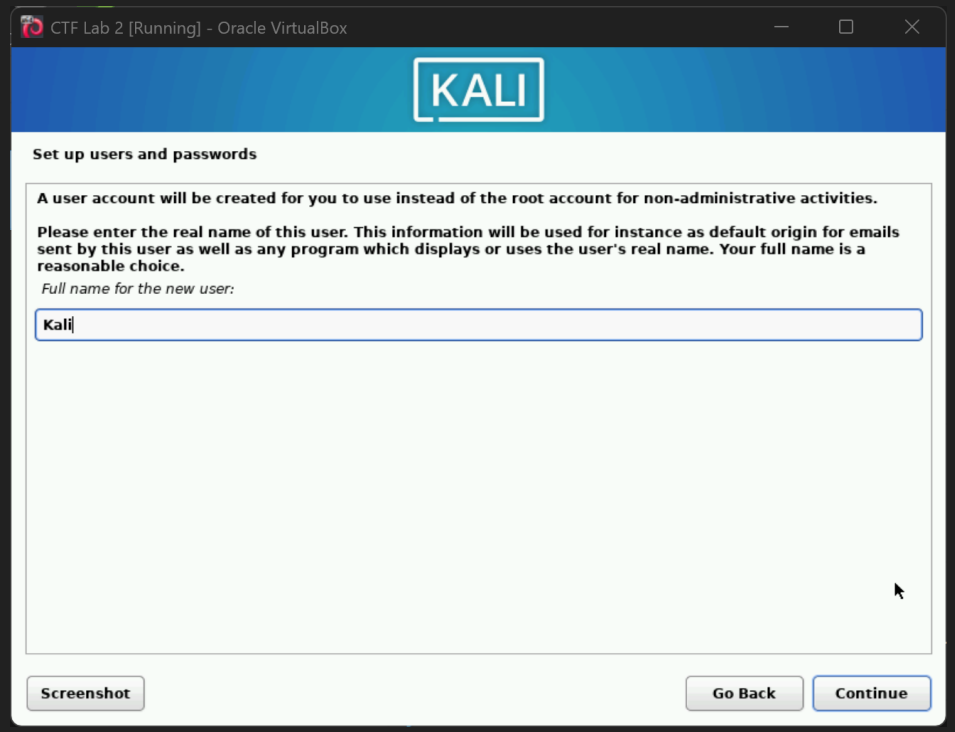
6. Graphical installer – user name

- The installer will ask for your full name. I just say “**Kali**”



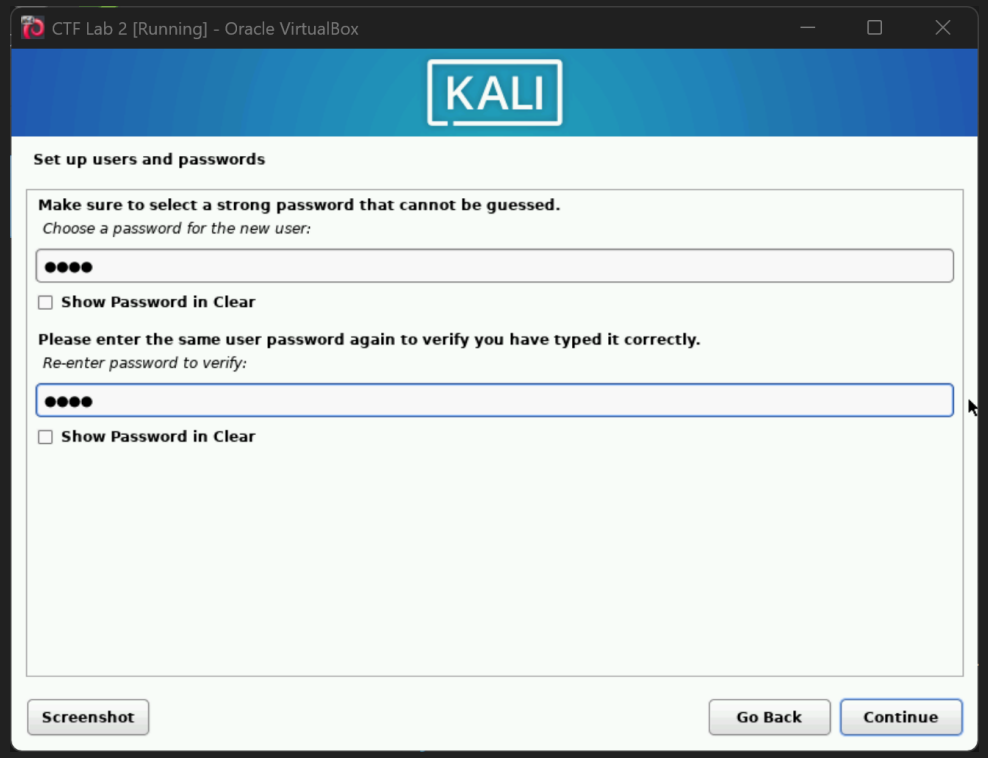
6. Graphical installer – user name

- The installer will ask for your full name. I just say “**Kali**”
- The next page will ask for your actual username. I set that to “**kali**”



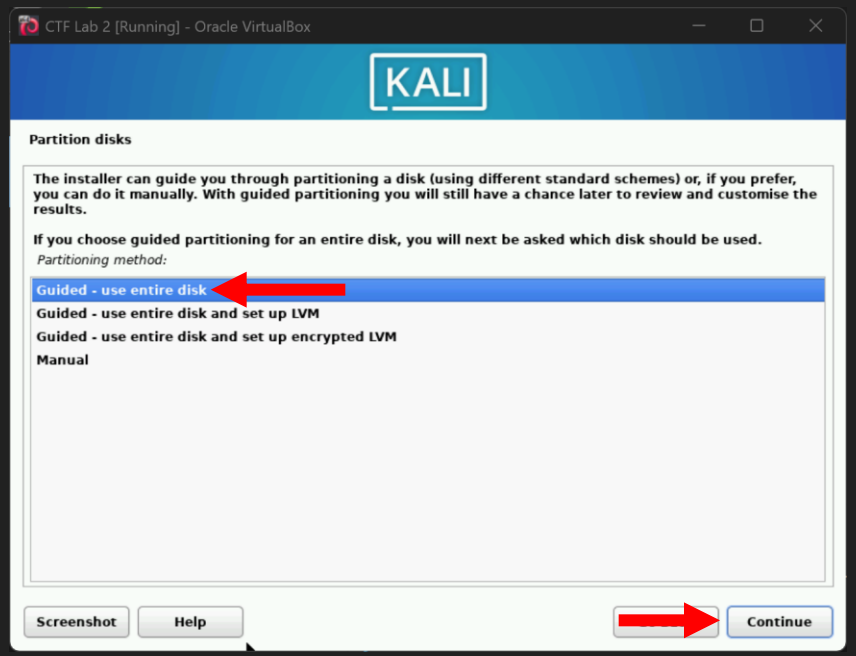
6. Graphical installer – password

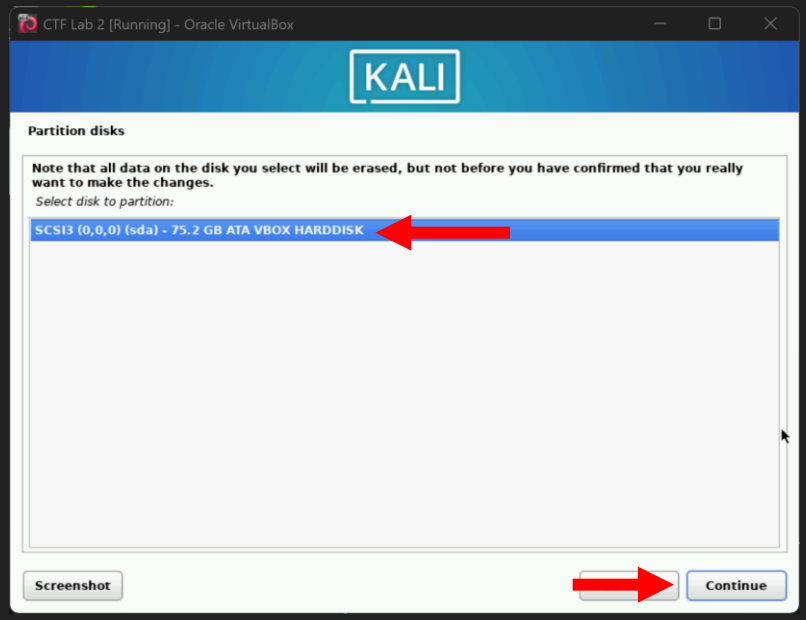
- CTF VMs are meant to be **easily spun up** and **discarded**.
- You shouldn't keep any **sensitive**, **personal**, or **important information** in your VM.
- Therefore, **password strength doesn't matter**. I usually just set it to "**kali**" or something similarly easy to remember.



6. Graphical installer – disk partitioning

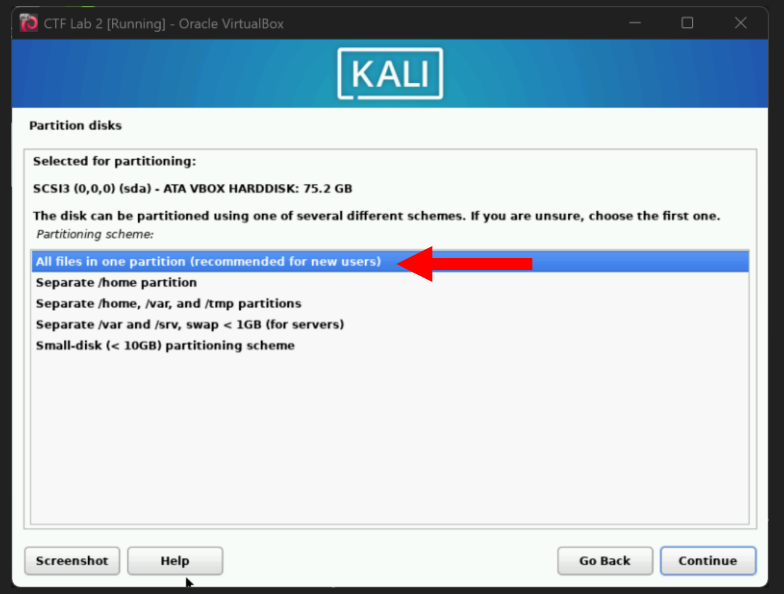
- In the “**Partition disks**” menu, select “**Guided – use entire disk**” and then “**continue**”
- There will only be one available disk. Select it and select continue.

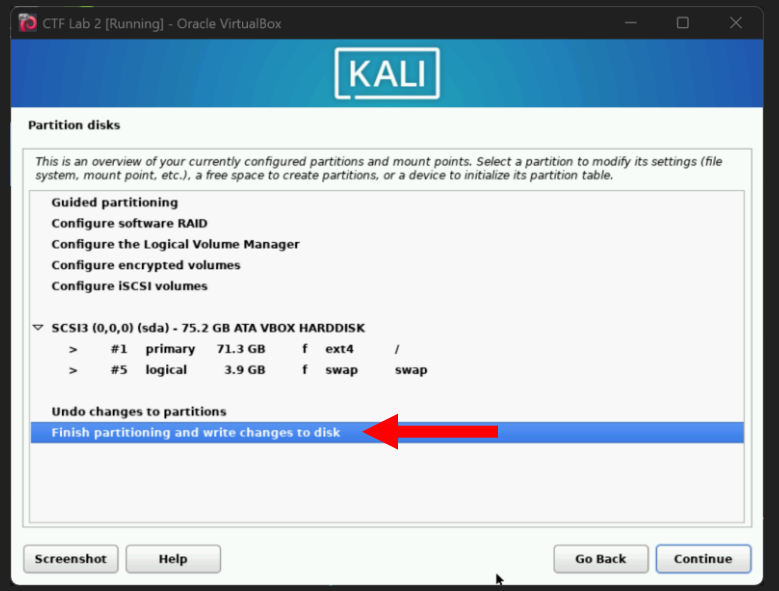




6. Graphical installer – disk partitioning

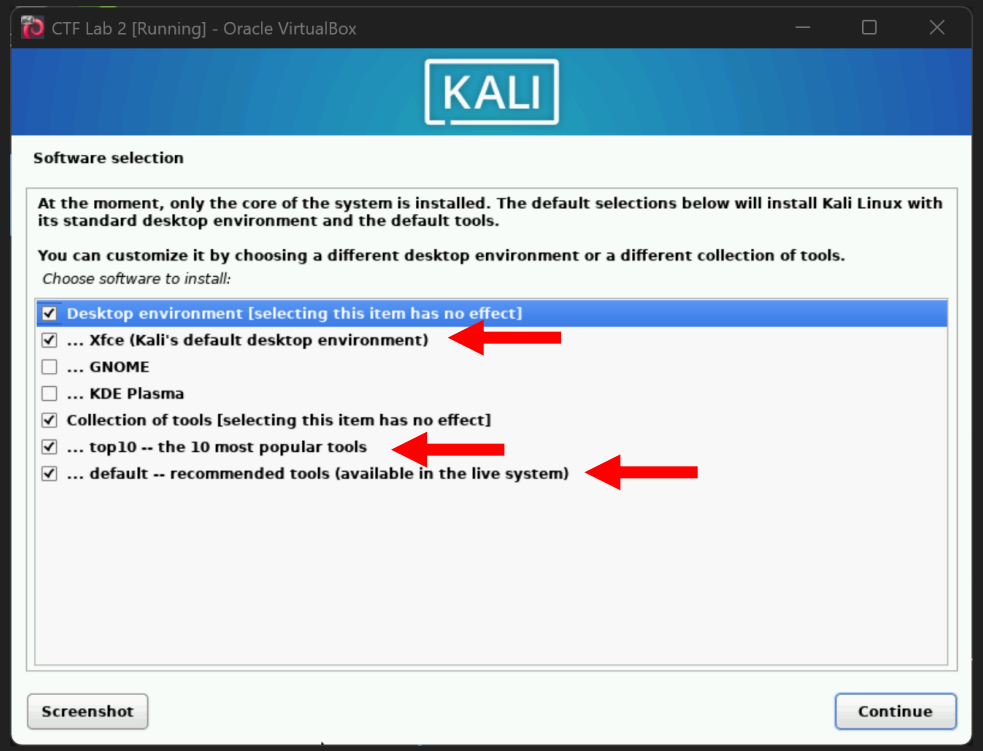
- Select “**All files in one partition**”
- Select “**Finish partitioning and write changes to disk**”





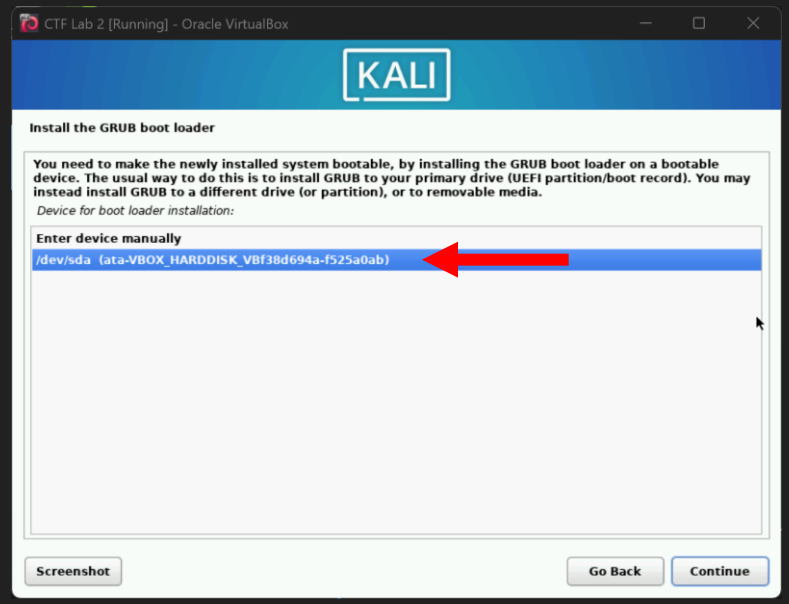
6. Graphical installer – Software Selection

- Select **Xfce**, and make sure **GNOME** and **KDE Plasma** are **unselected**
- (note: I usually like KDE but I've found Kali Linux's version to be buggy. I recommend sticking with Xfce for Kali Linux)
- Select "**top 10**" and "**default**"
- After clicking "**continue**", it **might take a while** to install everything.



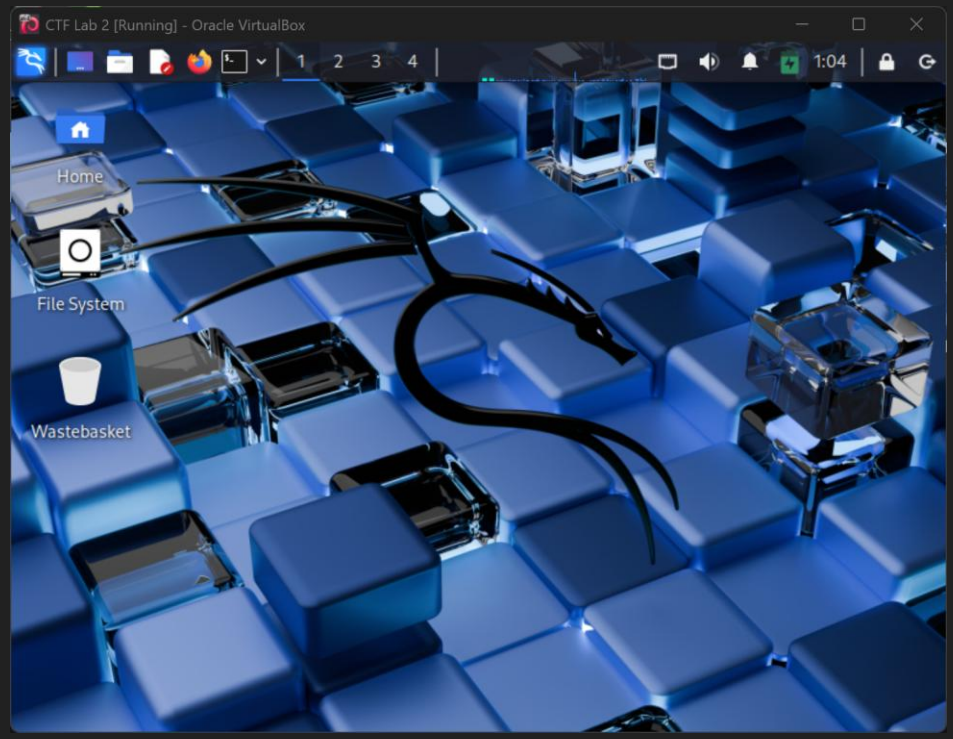
6. Graphical installer – Install GRUB

- Select “**Yes**” for “**Install the GRUB boot loader**”
- Select “**/dev/sda**”



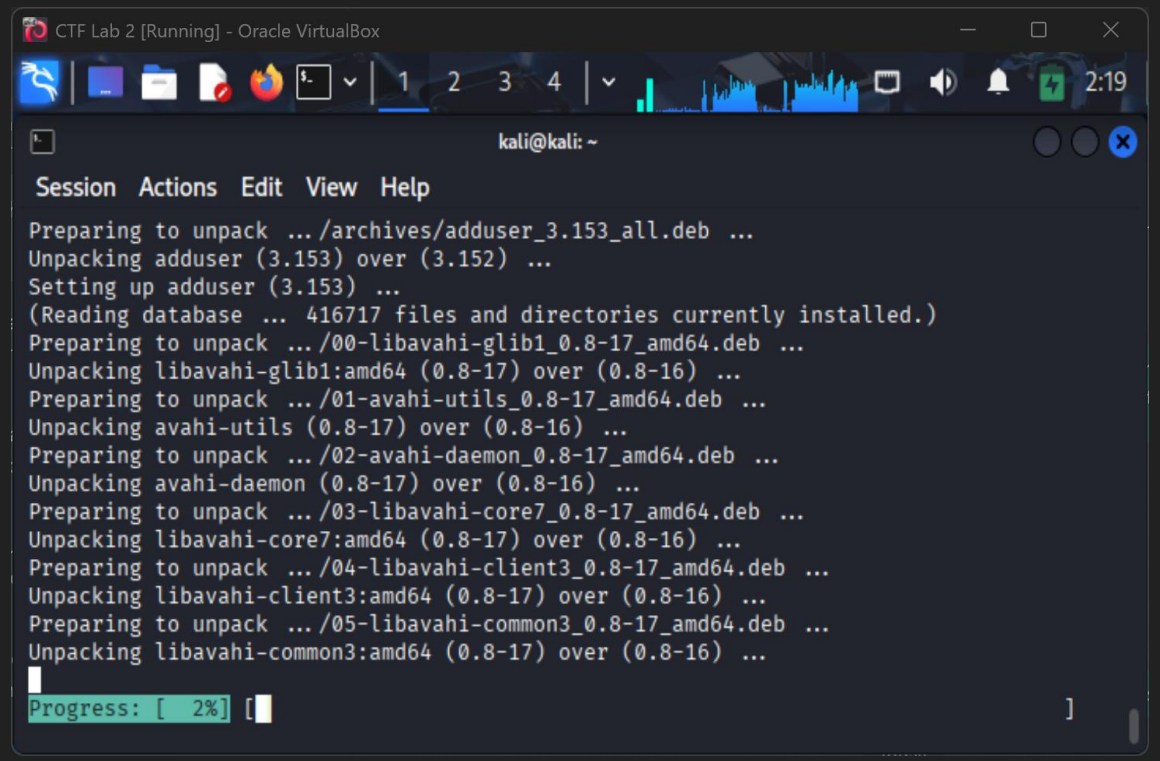
7. Reboot your VM

- **Reboot your VM**
- You should now be able to **log in** with the **credentials** you set up during installation



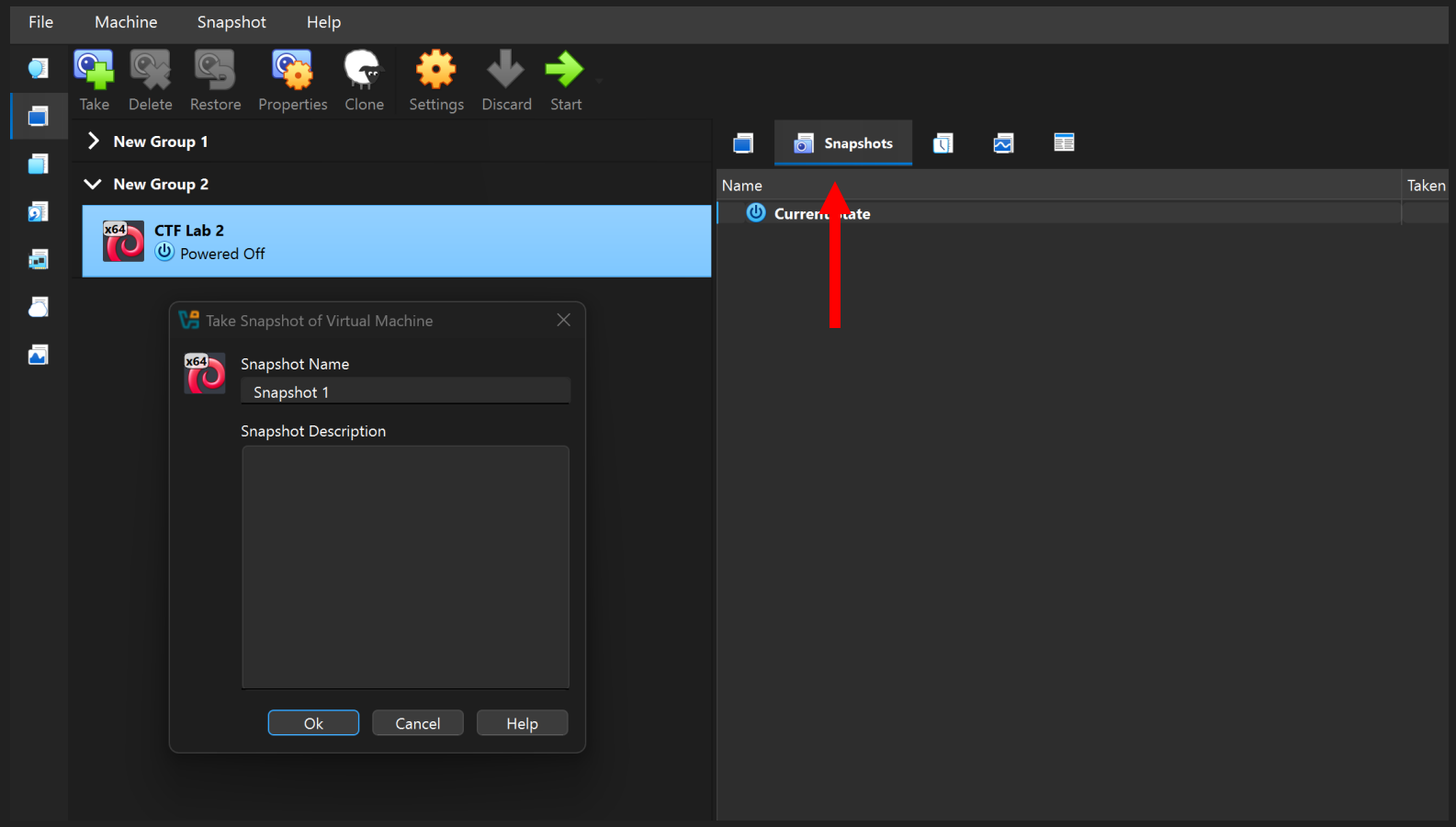
8. Update packages

- Open a **terminal window** in the VM
- Run the following commands (you'll be prompted for a password)
  - **sudo apt update**
  - **sudo apt upgrade**
- This will **update all of the software** in your VM
- Installing these updates (as shown) will take a while



9. Take a snapshot

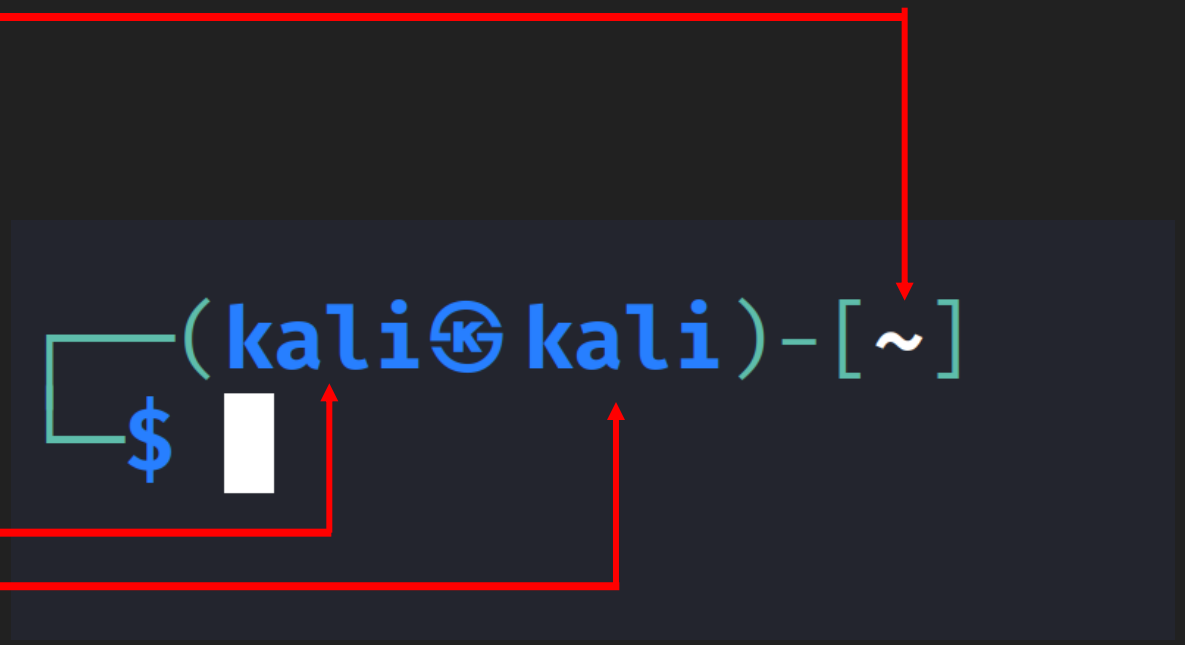
- **Shut down the the VM**
- Select “**snapshots**”
- Select “**take**”
- You can now restore the VM to this state in the future if necessary.



Basics of using Linux

Terminal Prompt

- When you launch a terminal, you're given a **terminal prompt**
- It shows some key information, including:
  - Your **current directory** (folder)
  - Your **username**
  - Your **hostname**
- "~" is your **home directory**. It contains your user's **files**, and contains directories like "**Documents**" and "**Downloads**", similar to windows



Listing Files

- You can use the “**ls**” command to list files **in a directory**
- If you **don’t specify a directory**, it will list files in the **current directory**
- By default, **ls** will **not list files** which **start with a full stop**.
- “**ls -a**” will list all files, including these “hidden” ones.
- “ls -al” will give you more information about each file.

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ ls Desktop
file.txt

┌──(kali㉿kali)-[~]
└─$ ls -a Desktop
.  ..  file.txt  .secret-file.txt

┌──(kali㉿kali)-[~]
└─$ ls -al Desktop
total 8
drwxr-xr-x  2 kali kali 4096 Oct  6 01:41 .
drwx------ 15 kali kali 4096 Oct  6 01:29 ..
-rw-rw-r--  1 kali kali    0 Oct  6 01:40 file.txt
-rw-rw-r--  1 kali kali    0 Oct  6 01:41 .secret-file.txt
```

Directory terminology

- “/” is the **root directory**. Every file on the system is contained somewhere in the root directory
- “~” is your user’s **home directory**. It’s actually **“/home/kali”**, but “~” is used as a **shorthand**
- “.” represents the **current directory**
- “..” represents the **parent directory**, i.e. the one which **contains your current directory**

Changing directories

- You can change directories with the “**cd**” command.
- You can provide an **absolute path** (i.e. **relative to the root directory**), or a **relative path** (i.e. **relative to your current directory**)
- “cd ..” can be used to move to your parent directory

```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ cd ..

┌──(kali㉿kali)-[~]
└─$ cd /home/kali/Documents

┌──(kali㉿kali)-[~/Documents]
└─$ cd /

┌──(kali㉿kali)-[/]
└─$ ls
bin   etc         initrd.img.old  lib64       mnt   root  srv  usr      vmlinuz.old
boot  home        lib             lost+found  opt   run   sys  var
dev   initrd.img  lib32           media       proc  sbin  tmp  vmlinuz

┌──(kali㉿kali)-[/]
└─$
```

Installing Software

- Kali Linux is based on another Linux distribution called **Debian**
- **Debian-based** systems use a package manager called **apt** to **manage software**
- **Package managers** are used to **install**, **remove**, and **update** software
- You can install new packages with “**sudo apt install**”
- “**sudo apt update**” checks what updates are needed, and “**sudo apt upgrade**” installs those updates

```
┌──(kali㉿kali)-[/]
└─$ sudo apt install cmatrix
```

What does sudo mean?

- **Administrator privileges** on Linux are called **root privileges**.
- To avoid damaging your system, you run most of your commands as a normal user.
- When you need to use **root privileges** for a command, e.g. when **installing software**, you prefix it with the "**sudo**" command.

```
┌──(kali㉿kali)-[/]
└─$ apt remove cmatrix
Error: Could not open lock file /var/lib/dpkg/lock-frontend - open (13: Permission denie
d)
Error: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), are you r
oot?

┌──(kali㉿kali)-[/]
└─$ sudo apt remove cmatrix
The following packages were automatically installed and are no longer required:
  amass-common          libyelp0
  libbluray2            python3-bluepy
  libbson-1.0-0t64      python3-click-plugins
```

VM tips

VM tips

- You can take **snapshots** of VMs, which let you **restore the VM** to it's state at that point in time
- You should have **at least one snapshot** to avoid **losing a VM** if its files get corrupted
- For other **Linux VMs**, you'll need to install **VirtualBox Guest Additions**. This is a piece of software which enables the VM to **connect better to the host OS**, e.g. **resizing itself to fit a window**.
- Kali Linux **includes Guest Additions by default**. Instructions to install it on other VMs can be **found on the VirtualBox website**.

IntakeCTF

IntakeCTF

- Our **beginner-focused CTF competition**
- **Opening event** and introduction on **Thursday, 18:00-**
- There are prizes available for the **best team** and the **best named team**
- There’s **free pizza**

Join the discord for regular updates and event announcements!

https://discord.gg/mpdGEQnYuh

https://www.warwicksu.com/societies-sports/societies/61481/

https://www.instagram.com/warwickcybersoc/