



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 activities **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**

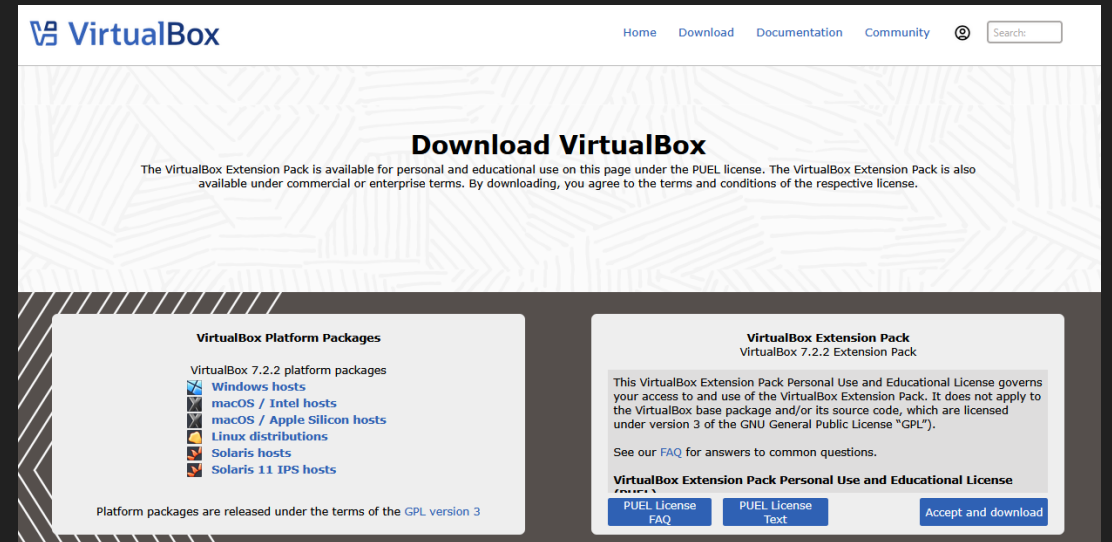




Tutorial – Creating a Kali Linux Virtual Machine

1. Download VirtualBox

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



The screenshot shows the 'Download VirtualBox' page on the official VirtualBox website. The page has a white header with the VirtualBox logo and navigation links: Home, Download, Documentation, and Community. A search bar is located on the right. The main content area has a light gray background with a geometric pattern. The title 'Download VirtualBox' is centered. Below the title, a paragraph states: 'The VirtualBox Extension Pack is available for personal and educational use on this page under the PUEL license. The VirtualBox Extension Pack is also available under commercial or enterprise terms. By downloading, you agree to the terms and conditions of the respective license.'

Below this text, there are two main sections:

- VirtualBox Platform Packages**
VirtualBox 7.2.2 platform packages
List of operating systems with corresponding icons:
 - Windows hosts
 - macOS / Intel hosts
 - macOS / Apple Silicon hosts
 - Linux distributions
 - Solaris hosts
 - Solaris 11 IPS hostsAt the bottom of this section, it says: 'Platform packages are released under the terms of the GPL version 3'
- VirtualBox Extension Pack**
VirtualBox 7.2.2 Extension Pack
This section contains the 'VirtualBox Extension Pack Personal Use and Educational License' text. At the bottom, there are three buttons: 'PUEL License FAQ', 'PUEL License Text', and 'Accept and download'.



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**

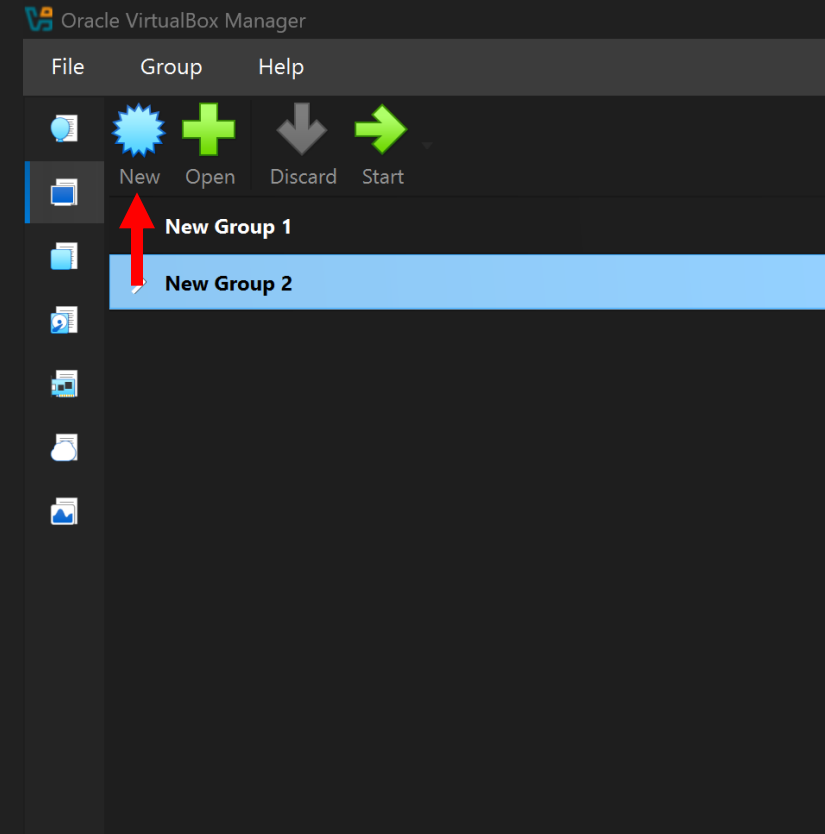


The screenshot shows the Kali Linux 2025.3 Changelog page. At the top, there is a navigation bar with links: [Installer](#), [Pre-built VMs](#), [ARM](#), [Mobile](#), [Cloud](#), [Containers](#), [Live](#), and [WSL](#). Below the navigation bar, the page title is "Kali Linux 2025.3 Changelog". A toggle switch is present, with "x86_64" selected and "Apple Silicon (ARM64)" as an option. The main content area displays four installation options, each with a Kali Linux logo and a description:

- Recommended** (highlighted with a blue border):
 - Installer**: Complete offline installation with customization. Download size: 4.2G. Options: torrent, sum.
- Weekly**: Untested images with the latest updates. Download size: 4.8G. Options: repository, sum.
- NetInstaller**: All packages are downloaded during installation. Download size: 775M. Options: torrent, sum.
- Everything**: Image for air-gapped networks. Download size: 12G. Options: torrent, sum.

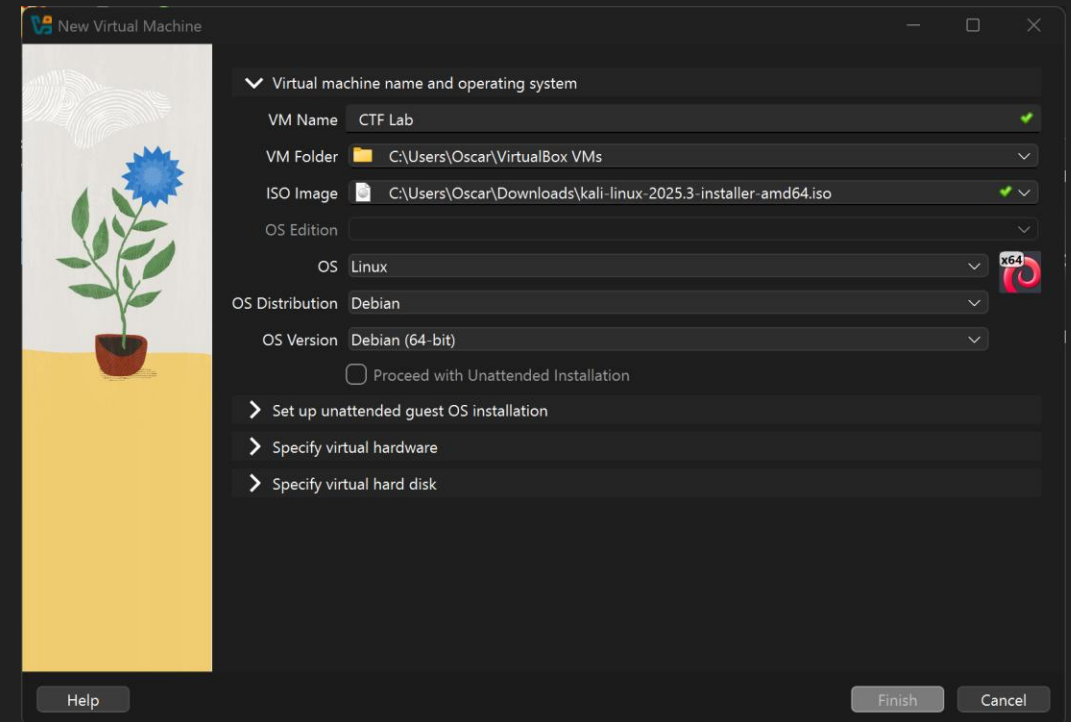
3. Create a new virtual machine in VirtualBox

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



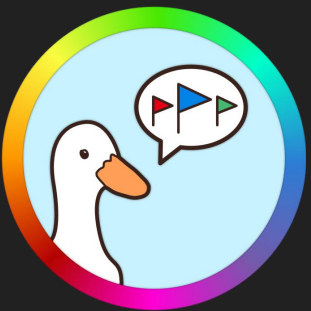
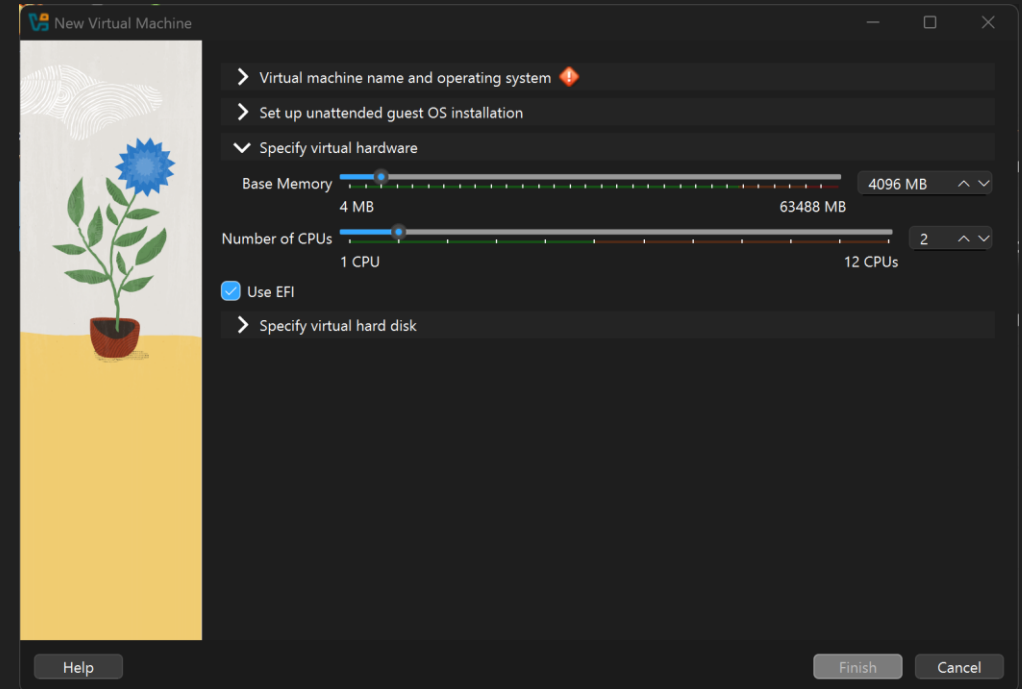
3. Create a new virtual machine – name and operating system

- 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**



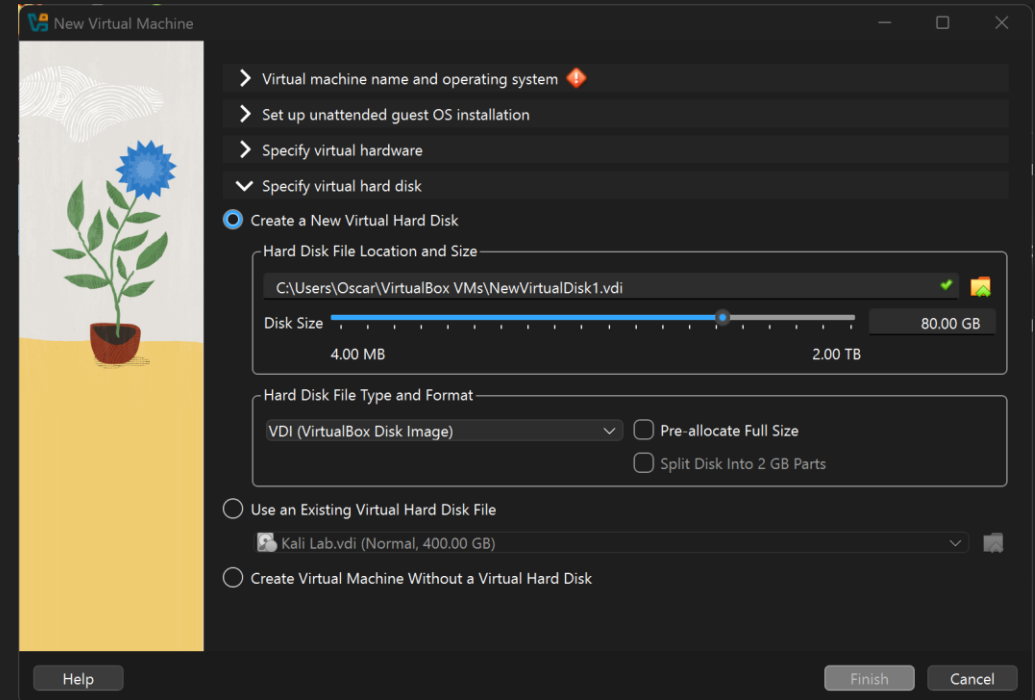
3. Create a new virtual machine – virtual hardware

- 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**)



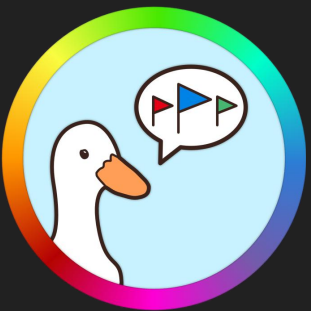
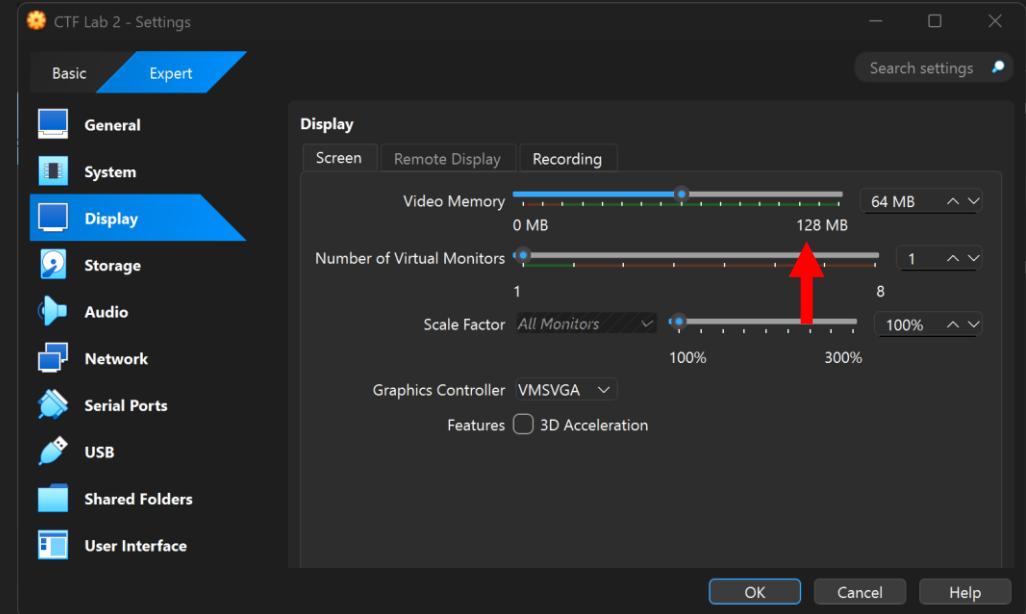
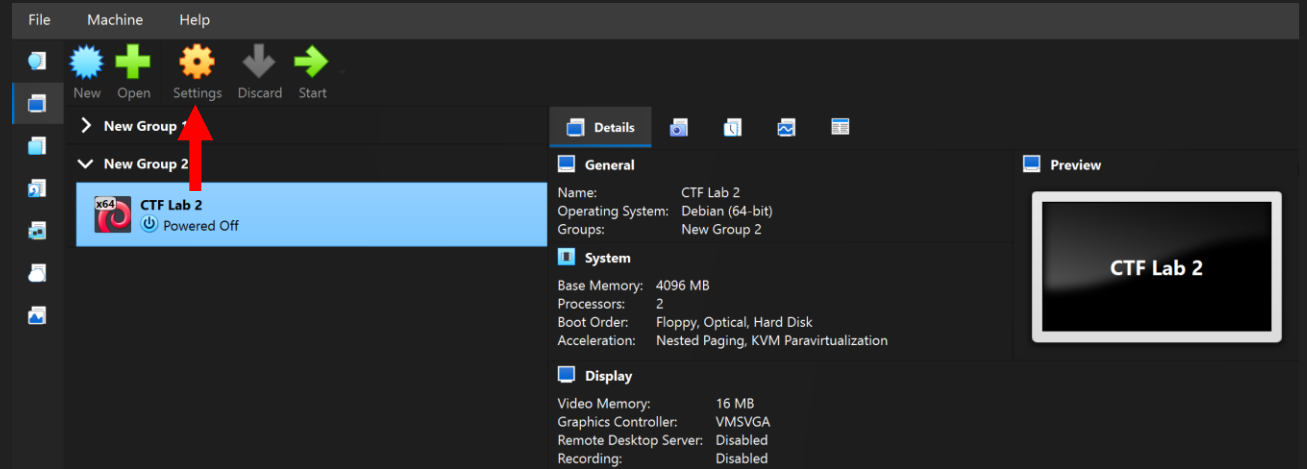
3. Create a new virtual machine – virtual hard disk

- 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



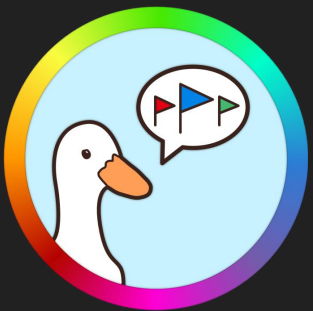
4. Change the default settings

- **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**



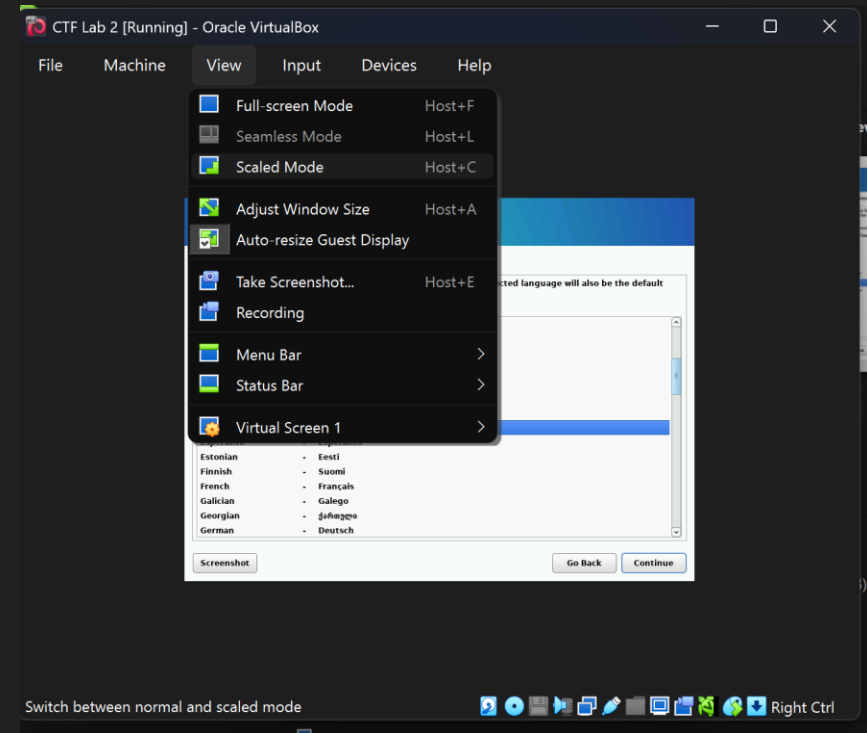
5. Launch the VM

- **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**



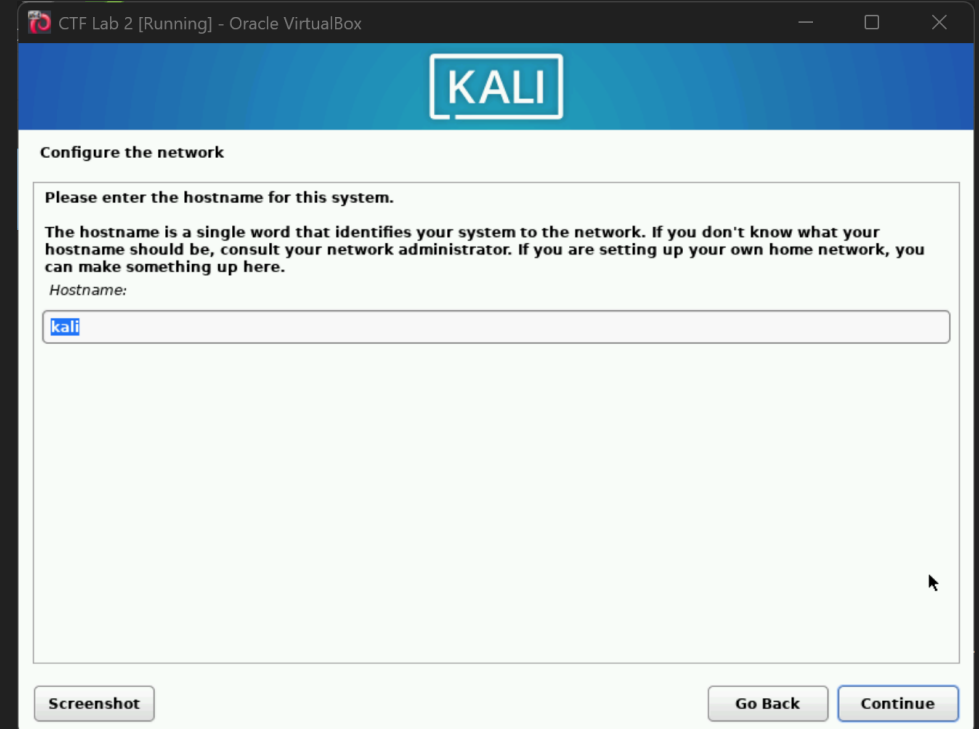
6. Go through the graphical installer

- 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)



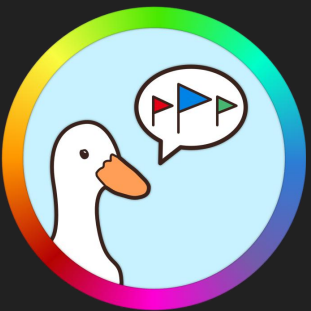
6. Graphical installer - hostname

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



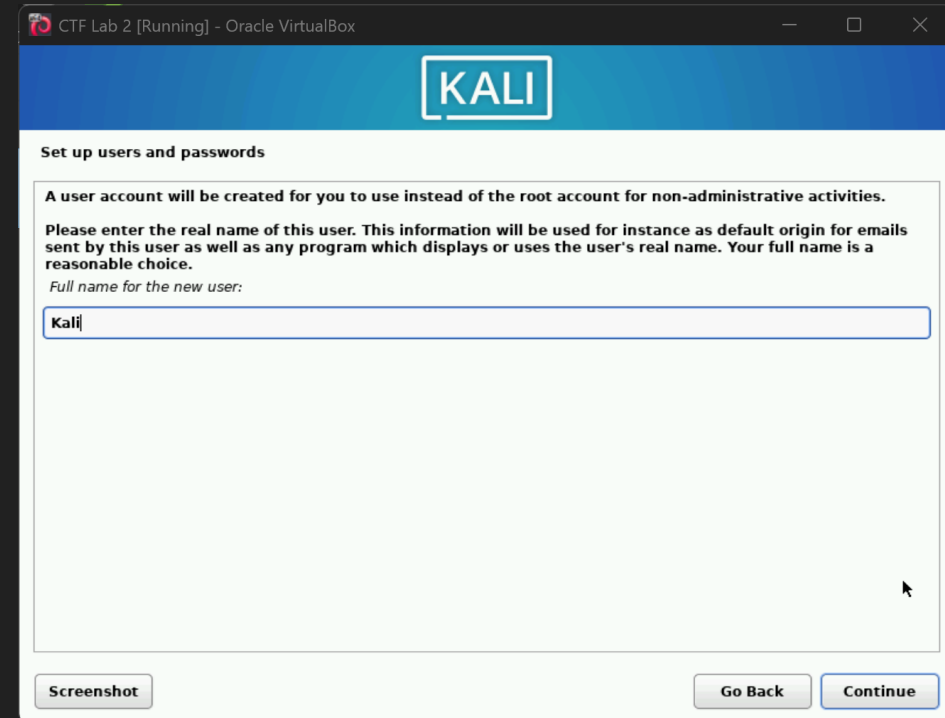
6. Graphical installer – domain name

- 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**”



CTF Lab 2 [Running] - Oracle VirtualBox

KALI

Set up users and passwords

A user account will be created for you to use instead of the root account for non-administrative activities.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:

Screenshot

Go Back Continue

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.



CTF Lab 2 [Running] - Oracle VirtualBox

KALI

Set up users and passwords

Make sure to select a strong password that cannot be guessed.
Choose a password for the new user:

••••

☐ Show Password in Clear

Please enter the same user password again to verify you have typed it correctly.
Re-enter password to verify:

••••

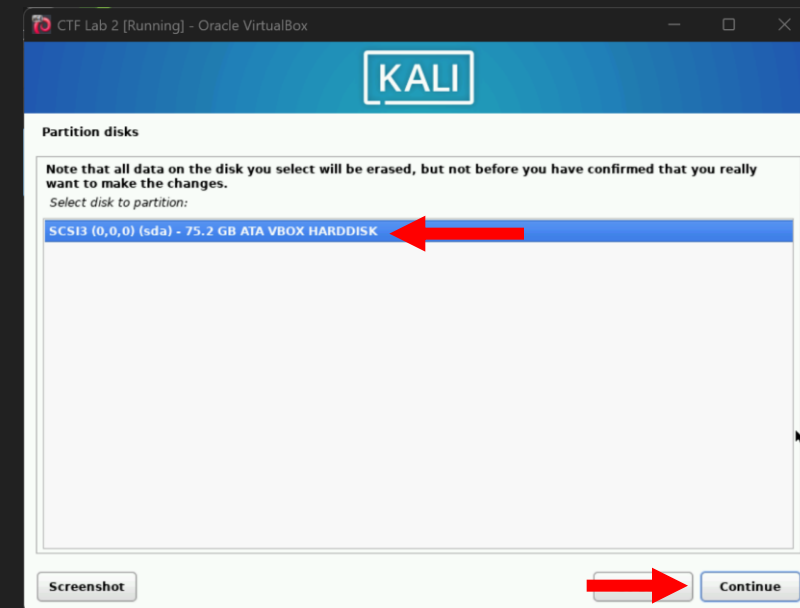
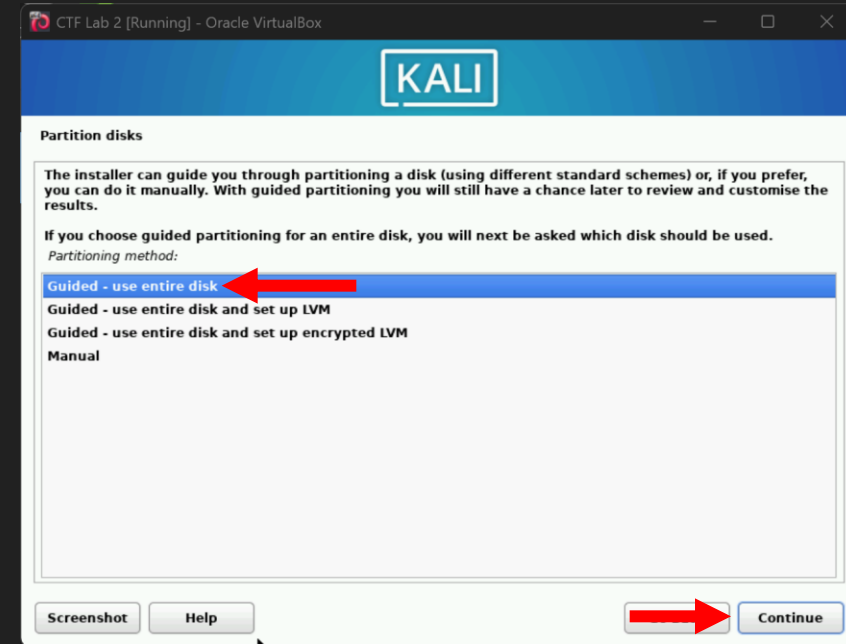
☐ Show Password in Clear

Screenshot

Go Back Continue

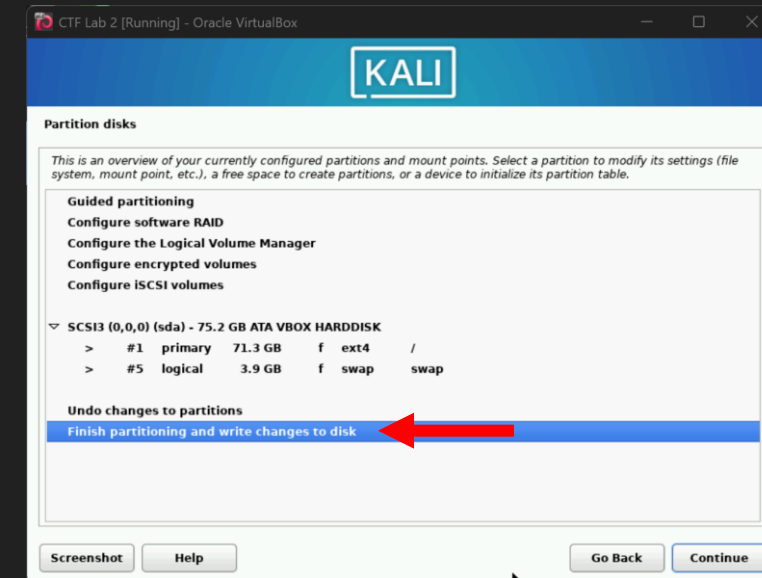
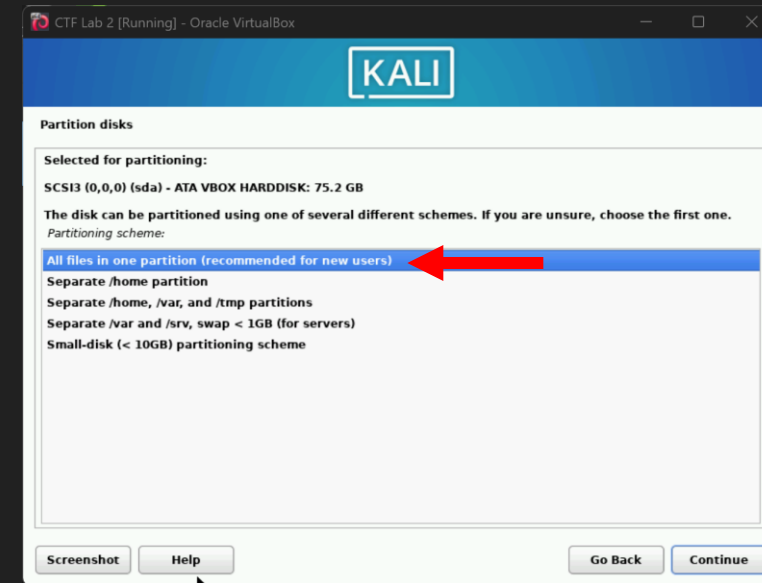
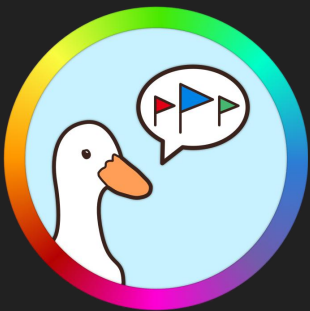
6. Graphical installer – disk partitioning

- 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.



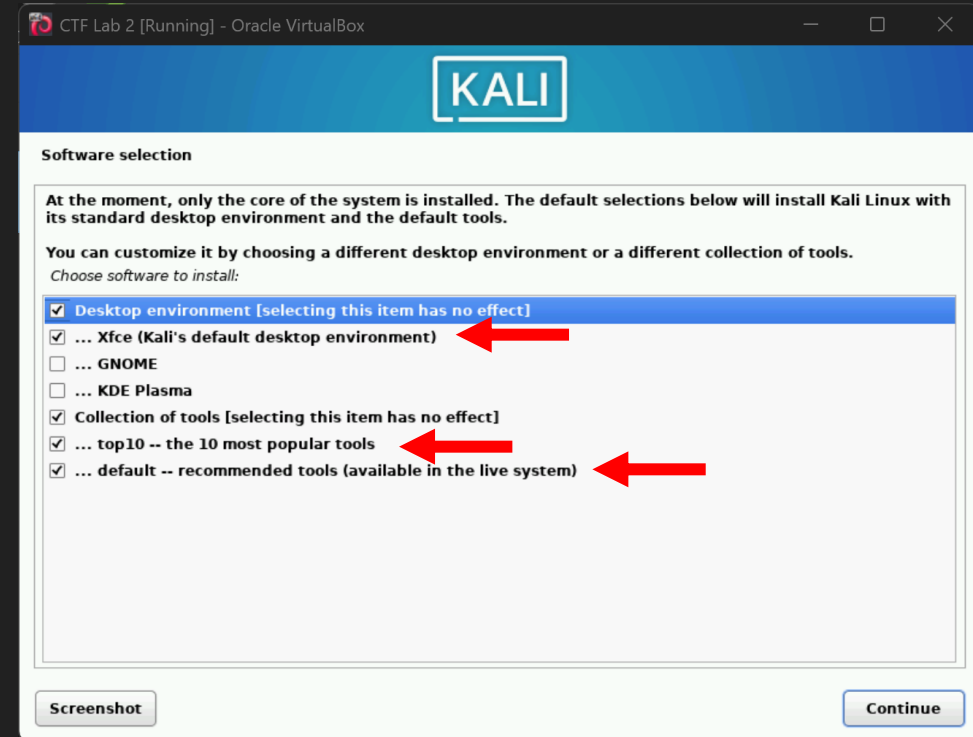
6. Graphical installer – disk partitioning

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



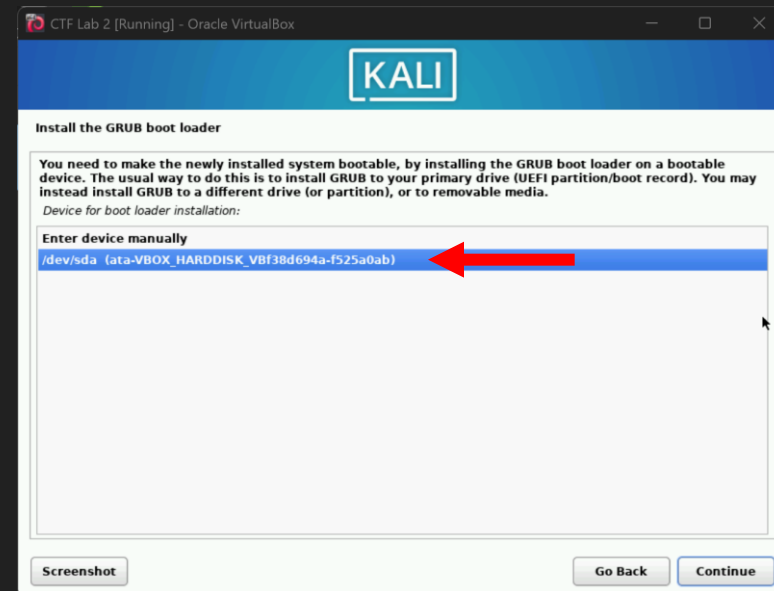
6. Graphical installer – Software Selection

- 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

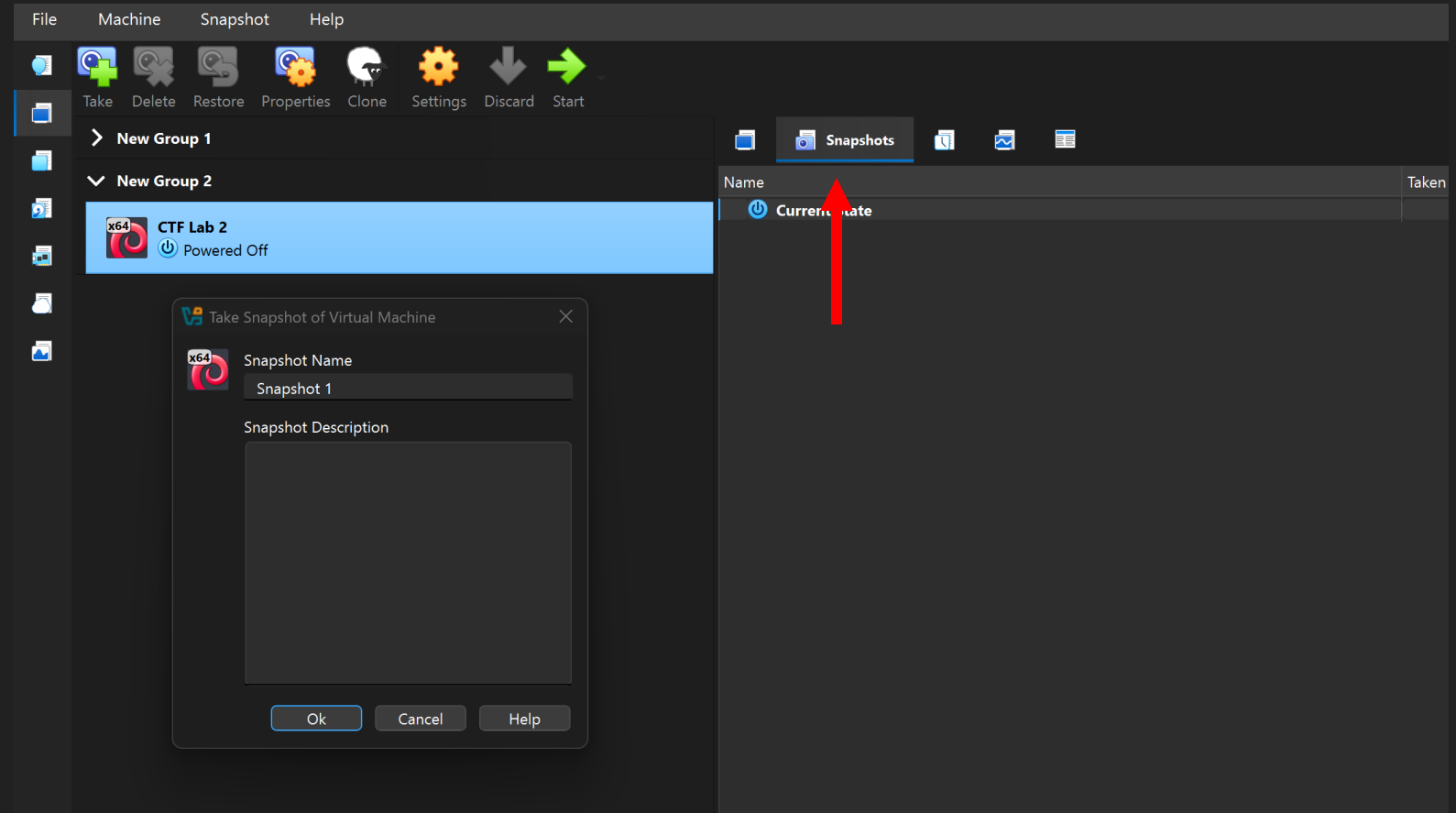
- Open a **terminal window** in the VM
- Run the following commands (you'll be prompted for a password)
 - **sudo apt update**
 - **sudo apt upgrade**
- This will **update all of the software** in your VM
- Installing these updates (as shown) will take a while



```
CTF Lab 2 [Running] - Oracle VirtualBox
kali@kali: ~
Session Actions Edit View Help
Preparing to unpack .../archives/adduser_3.153_all.deb ...
Unpacking adduser (3.153) over (3.152) ...
Setting up adduser (3.153) ...
(Reading database ... 416717 files and directories currently installed.)
Preparing to unpack .../00-libavahi-glib1_0.8-17_amd64.deb ...
Unpacking libavahi-glib1:amd64 (0.8-17) over (0.8-16) ...
Preparing to unpack .../01-avahi-utils_0.8-17_amd64.deb ...
Unpacking avahi-utils (0.8-17) over (0.8-16) ...
Preparing to unpack .../02-avahi-daemon_0.8-17_amd64.deb ...
Unpacking avahi-daemon (0.8-17) over (0.8-16) ...
Preparing to unpack .../03-libavahi-core7_0.8-17_amd64.deb ...
Unpacking libavahi-core7:amd64 (0.8-17) over (0.8-16) ...
Preparing to unpack .../04-libavahi-client3_0.8-17_amd64.deb ...
Unpacking libavahi-client3:amd64 (0.8-17) over (0.8-16) ...
Preparing to unpack .../05-libavahi-common3_0.8-17_amd64.deb ...
Unpacking libavahi-common3:amd64 (0.8-17) over (0.8-16) ...
Progress: [ 2%]
```

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.

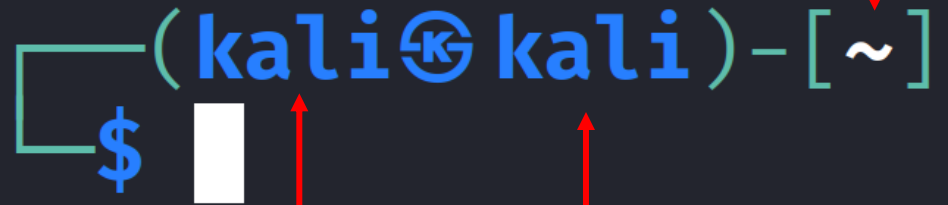




Basics of using Linux

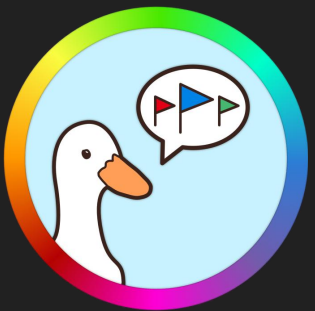
Terminal Prompt

- 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



(kali@kali)-[~]
\$

A diagram of a terminal prompt. The prompt text is "(kali@kali)-[~]" in blue, with a white cursor bar and a blue dollar sign "\$" below it. Red arrows point from the text in the list to the corresponding parts of the prompt: from "current directory" to "[~]", from "username" to "kali", and from "hostname" to "kali". A red line also points from the first bullet point to the entire prompt.



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-frontent - open (13: Permission denied)  
Error: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), are you root?  
  
(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**.





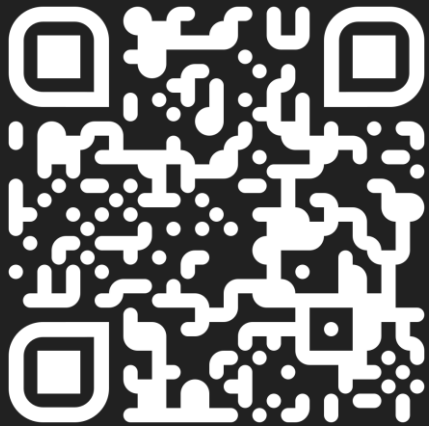
IntakeCTF

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**



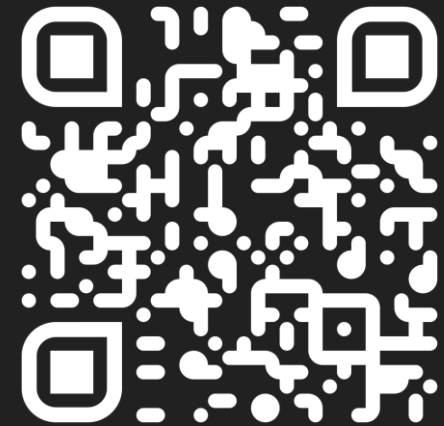
Join the discord for regular updates and event announcements!



[https://discord.gg/
mpdGEQnYuh](https://discord.gg/mpdGEQnYuh)



[https://www.warwicksu.com/societies-
sports/societies/61481/](https://www.warwicksu.com/societies-sports/societies/61481/)



[https://www.instagram.com/
warwickcybersoc/](https://www.instagram.com/warwickcybersoc/)