

Setting up System for Attack simulation

The attack we do is in Kali linux which is one of the Linux distribution of Linux which is famous for offensive attacking

Kali linux will be installed in a Virtual box

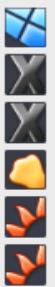
Installing Virtual Box : It is a powerful open-source virtualization software developed by Oracle corporation which allows to create and manage Virtual machines on a host system enabling the installation and operation of multiple operating systems simultaneously on a single physical machine.

A screenshot of a Microsoft Bing search results page. The search bar at the top contains the query "virtual box". Below the search bar, there are several navigation links: SEARCH (which is underlined), COPILOT, VIDEOS, IMAGES, MAPS, NEWS, SHOPPING, MORE, and TOOLS. The main search results section shows a result for "VirtualBox" with a thumbnail image of the software logo, the text "VirtualBox Virtualization hypervisor", and a "Download" button. To the right of the main results, there is a sidebar with a "Virtual" heading, a snippet about Oracle VirtualBox, and links to Wikipedia, Original author, Developer(s), Initial release, Stable release, Repository, Written in, Operating system, and Platform. The sidebar also includes a "Documentation" link and a "Forums" link.

you can download the software in by clicking the download button according your host system (Your personal system Os) Guest OS will be your vm installed in virtual box h which is Kali Linux in this project [Downloads – Oracle VirtualBox](#)

VirtualBox Platform Packages

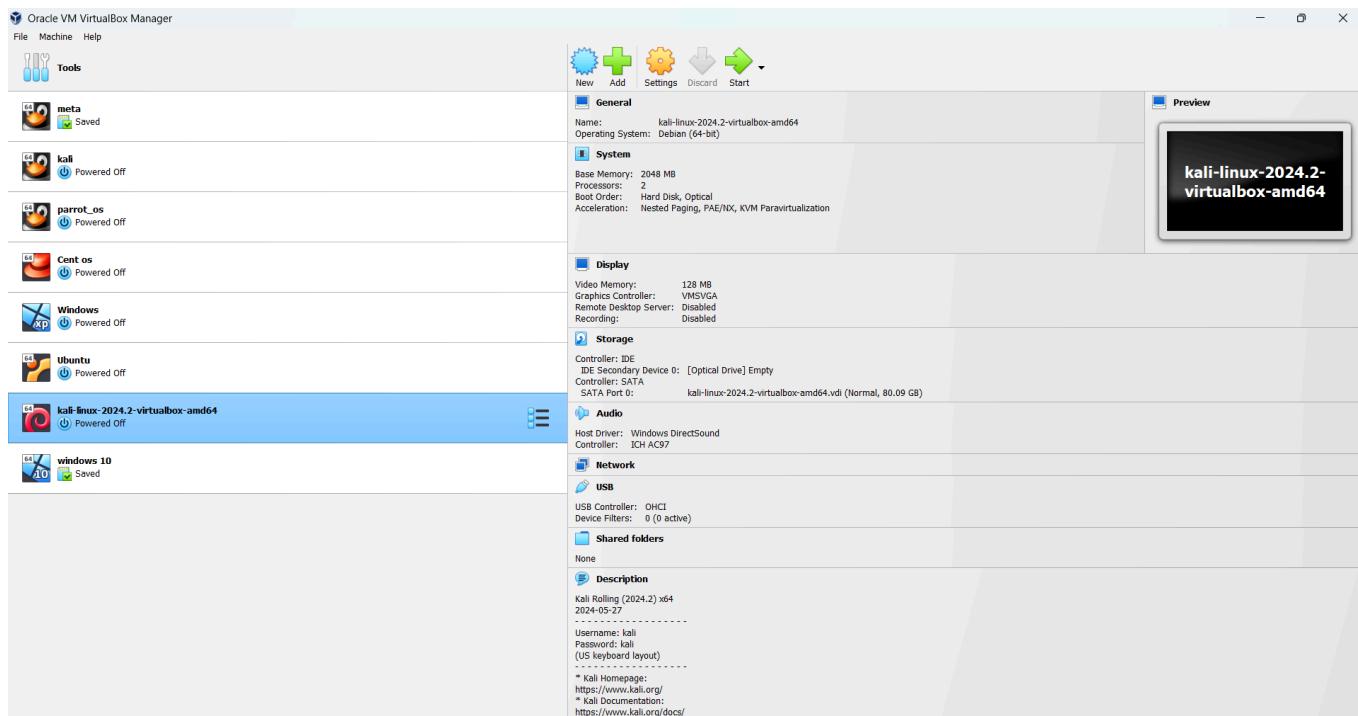
VirtualBox 7.1.4 platform packages



- Windows hosts**
- macOS / Intel hosts**
- macOS / Apple Silicon hosts**
- Linux distributions**
- Solaris hosts**
- Solaris 11 IPS hosts**

Platform packages are released under the terms of the [GPL version 3](#)

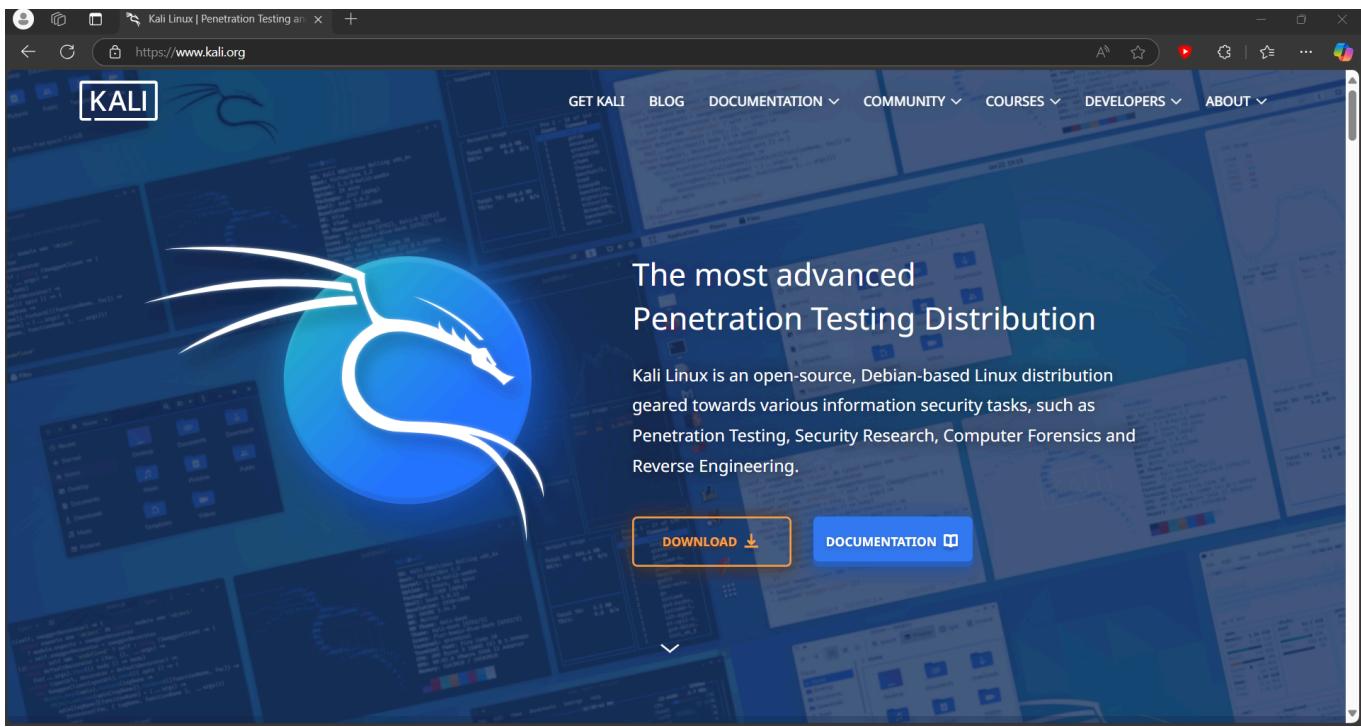
After u install the Virtual box



you will be opened like this

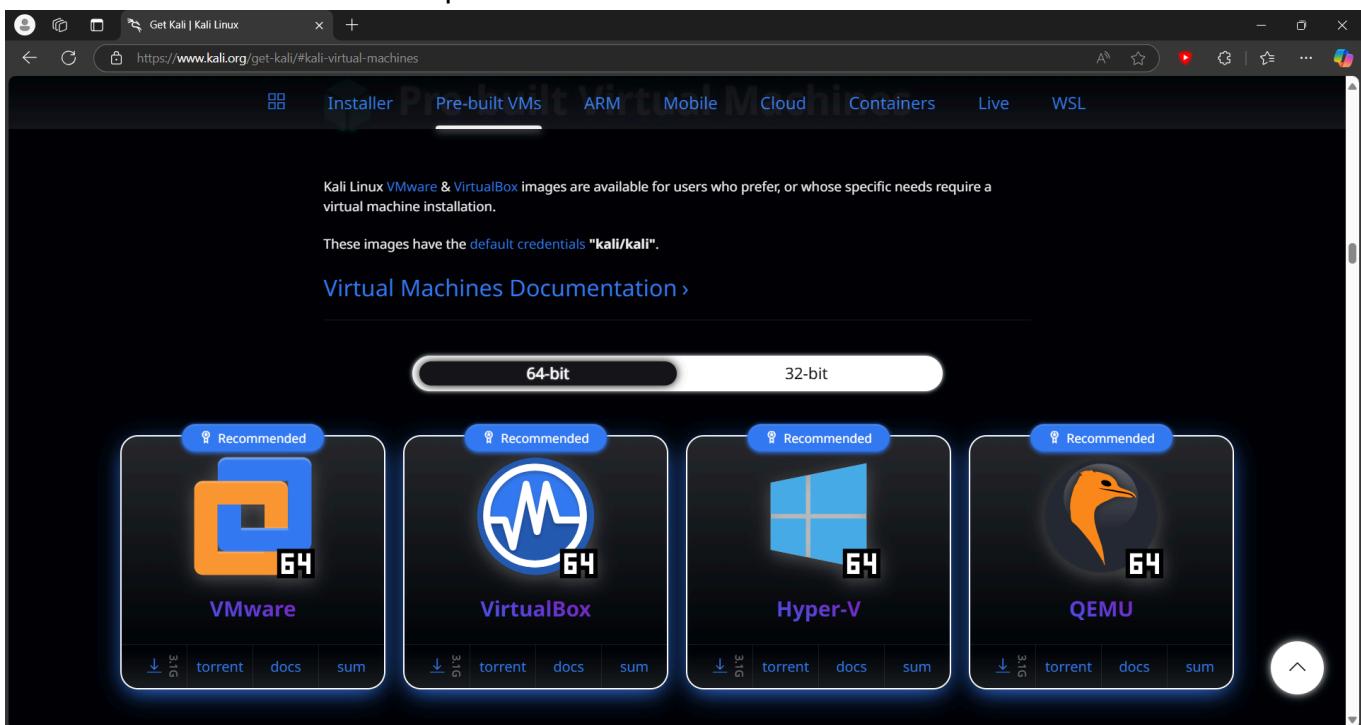
NOTE: I already had installed Other Os in my virtual box

Download and install Kali linux in virtual box



Link : [Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution](https://www.kali.org)

In the above link we can find a pre built vm's of kali linux

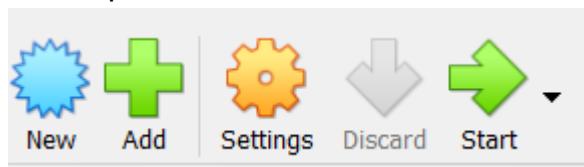


As we are using VirualBox so make sure u are downloading the Kali linux for VirtualBox
CHECK whether ur system is 64-bit or 32-bit.

Then make sure to extract the compressed file

Name	Date modified	Type	Size
64bit	18-01-2022 14:40	File folder	
Cent os_	03-10-2024 14:30	File folder	
kali	23-11-2024 21:12	File folder	
kali-linux-2024.2-virtualbox-amd64	23-11-2024 21:50	File folder	
meta	05-11-2024 18:59	File folder	
parrot_os	03-10-2024 14:37	File folder	
Ubuntu	05-11-2024 15:55	File folder	
Windows	23-11-2024 20:22	File folder	
windows 10_	23-11-2024 21:07	File folder	

Next Open the installed virtual box



click on the add option

since we have pre-defined kali machine not an iso image we need to proceed with add

Select a virtual machine file X

File name: Virtual machine files (*.xml *.vbi)

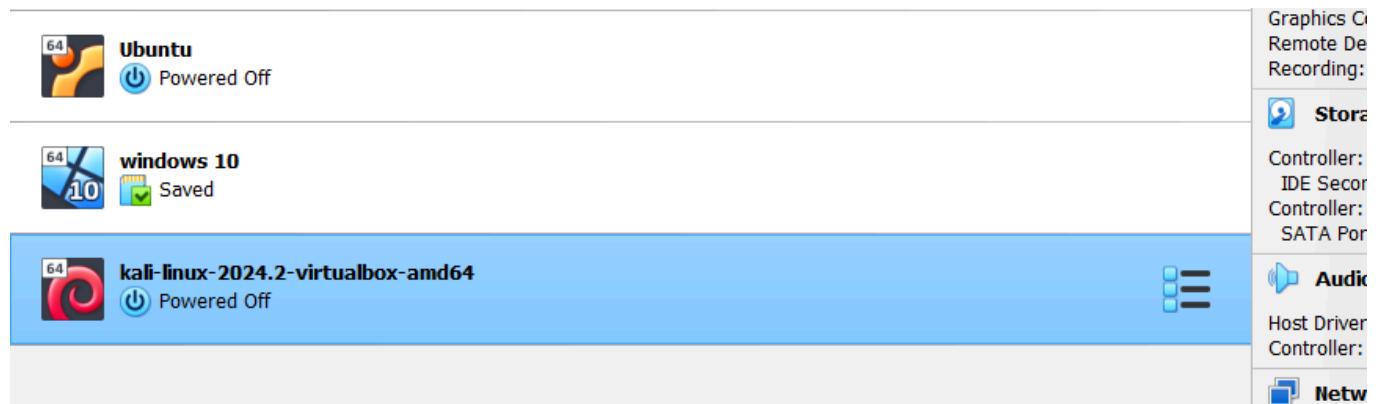
Open Cancel

Organize ▾ New folder

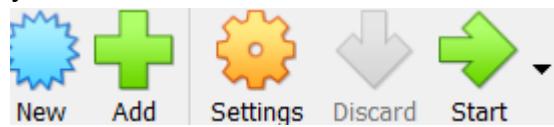
Name	Date modified	Type	Size
64bit	18-01-2022 14:40	File folder	
Cent os_	03-10-2024 14:30	File folder	
kali	23-11-2024 21:12	File folder	
kali-linux-2024.2-virtualbox-amd64	23-11-2024 21:50	File folder	
meta	05-11-2024 18:59	File folder	
parrot_os	03-10-2024 14:37	File folder	
Ubuntu	05-11-2024 15:55	File folder	
Windows	23-11-2024 20:22	File folder	

Desktop Downloads Documents Pictures Music Videos Screenshots

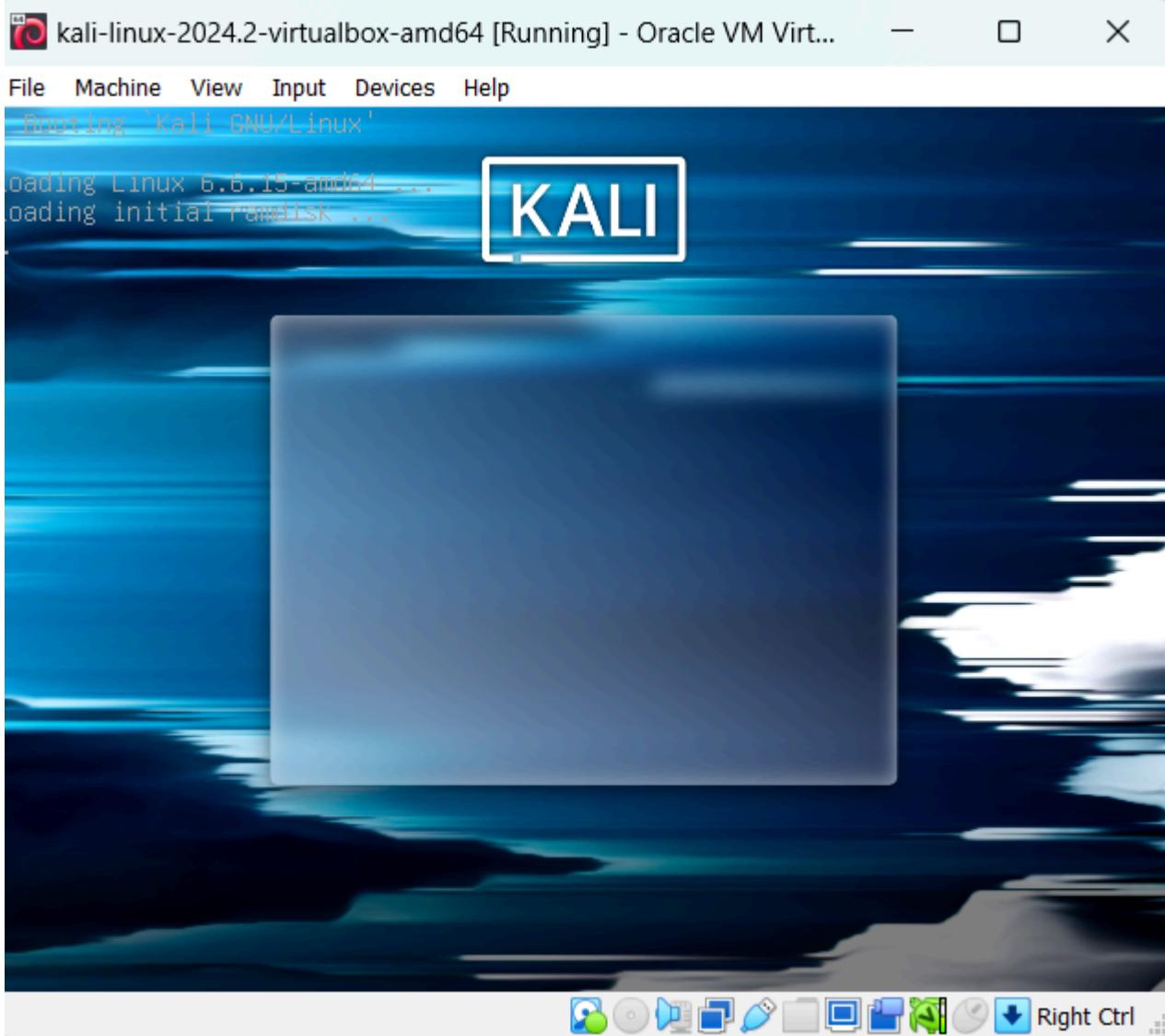
select this from the folder

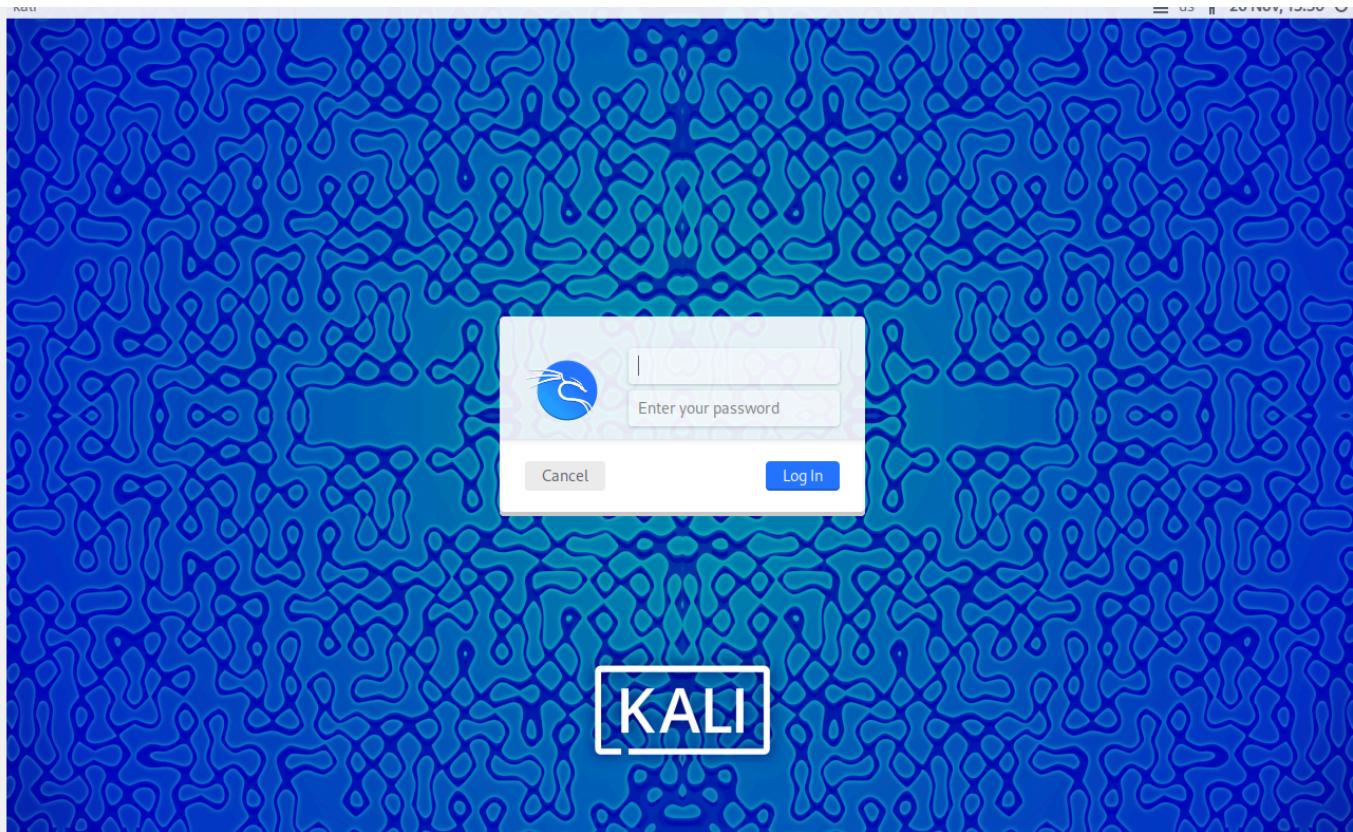


you can see the machine is added

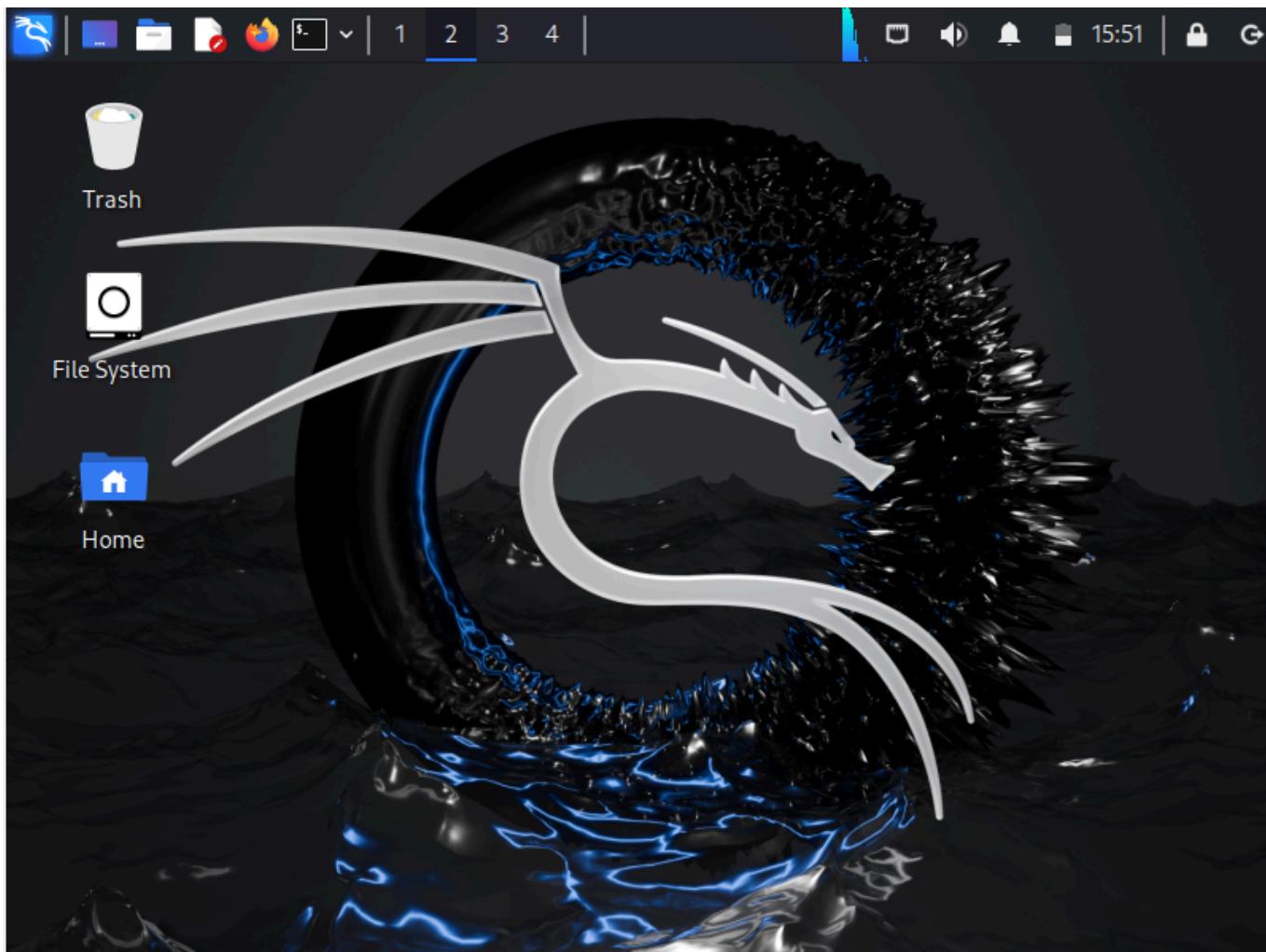


you can start the machine with start button





by default username and password is kali:kali



In this way we can setup the requirements to do the phishing attack for the credential harvesting project