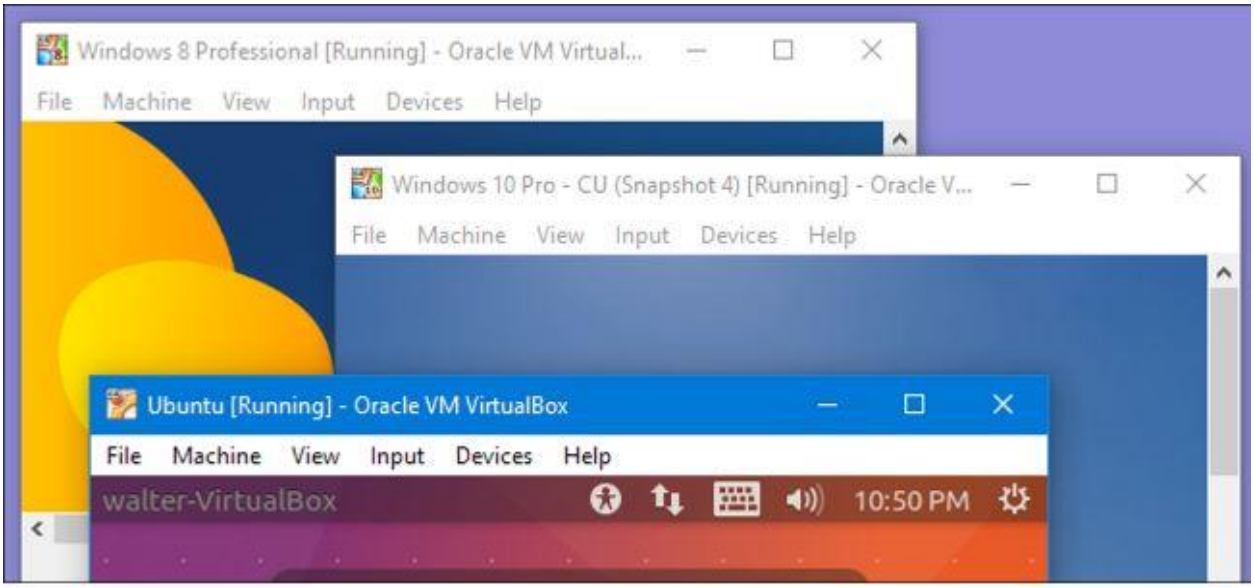
Kali Linux

Introduction of kali Linux

- Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as
    - Penetration Testing
    - Security Research
    - Computer Forensics
    - Reverse Engineering
- Linux is the most popular choice for hackers due to its flexibility, open source platform, portability and command line interface and compatibility with popular hacking tools.

Introduction of virtual machine



- A virtual machine (VM) is a virtual environment that functions as a virtual computer system with its own CPU, memory, network interface or A virtual machine s a virtual environment that works like a computer within a computer

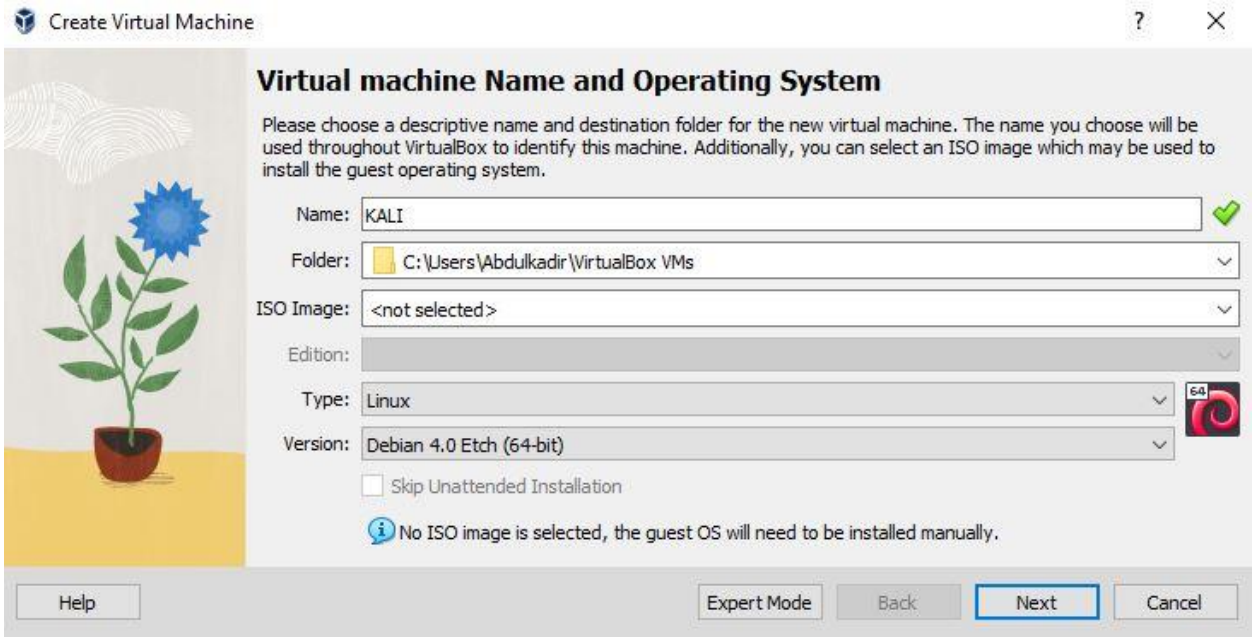
Downloading and installing kali Linux on window computer

- To install kali Linux on your window computer you will need to programs
    1. **VirtualBox**: is an open source Virtual Machine program from Oracle. It allows users to virtually install many operating systems on virtual drives, including Windows, BSD, Linux, Solaris, and more.
       Download here https://www.virtualbox.org/wiki/Downloads
    2. You will also need to download an .iso file for the Kali linux operating system
       Download here https://getintopc.com/softwares/operating-systems/kali-linux-2020-free-download-1874870/

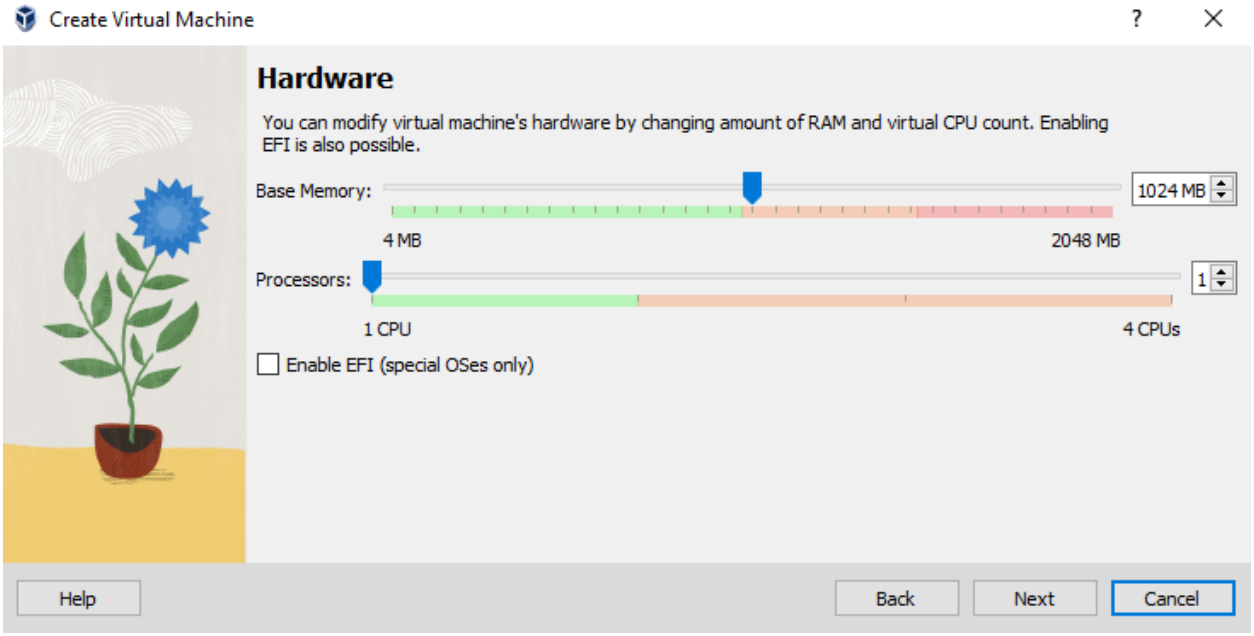
Installation process

Step 1: open oracle VM VirtualBox and click new

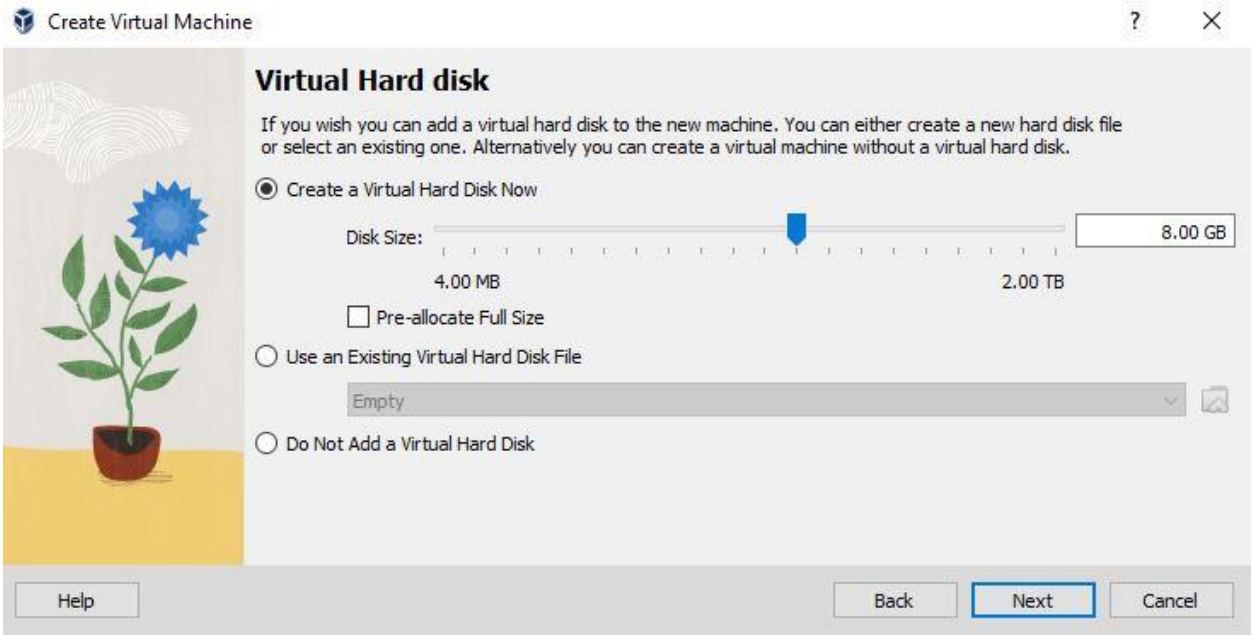
Step 2: Give a name, in the type section select Linux and in the version section select debian 64 bit then click next



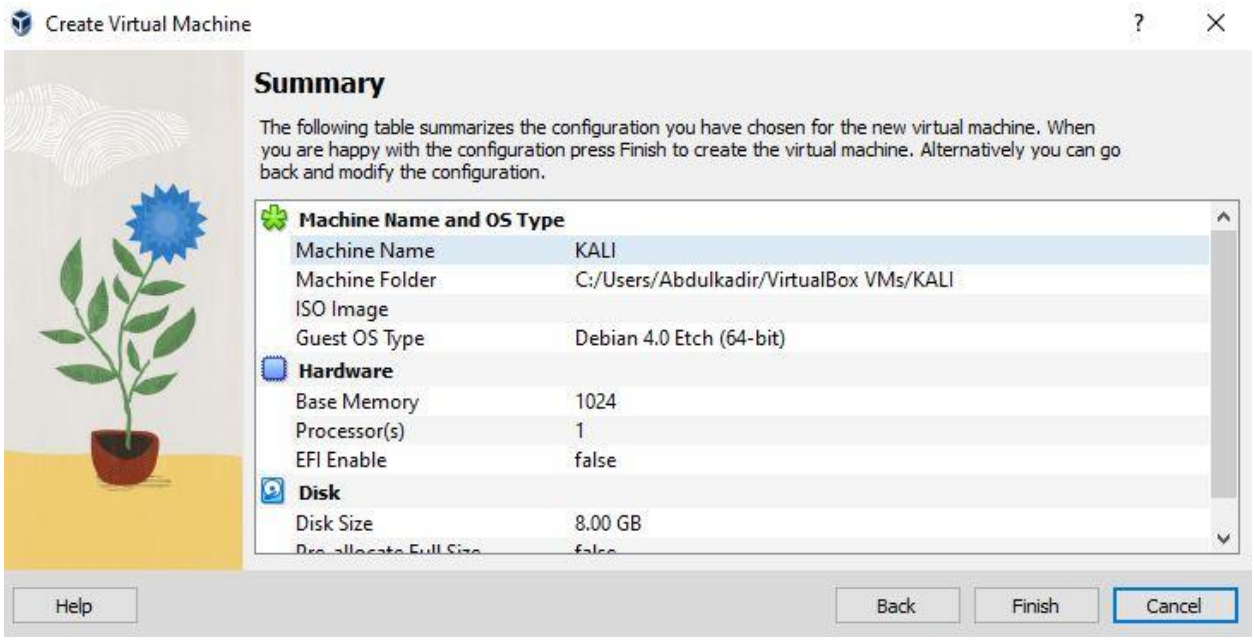
Step 3: You can increase your memory and processor size, but don't cross the green lines. If you are beginner go with default don't change anything and click next



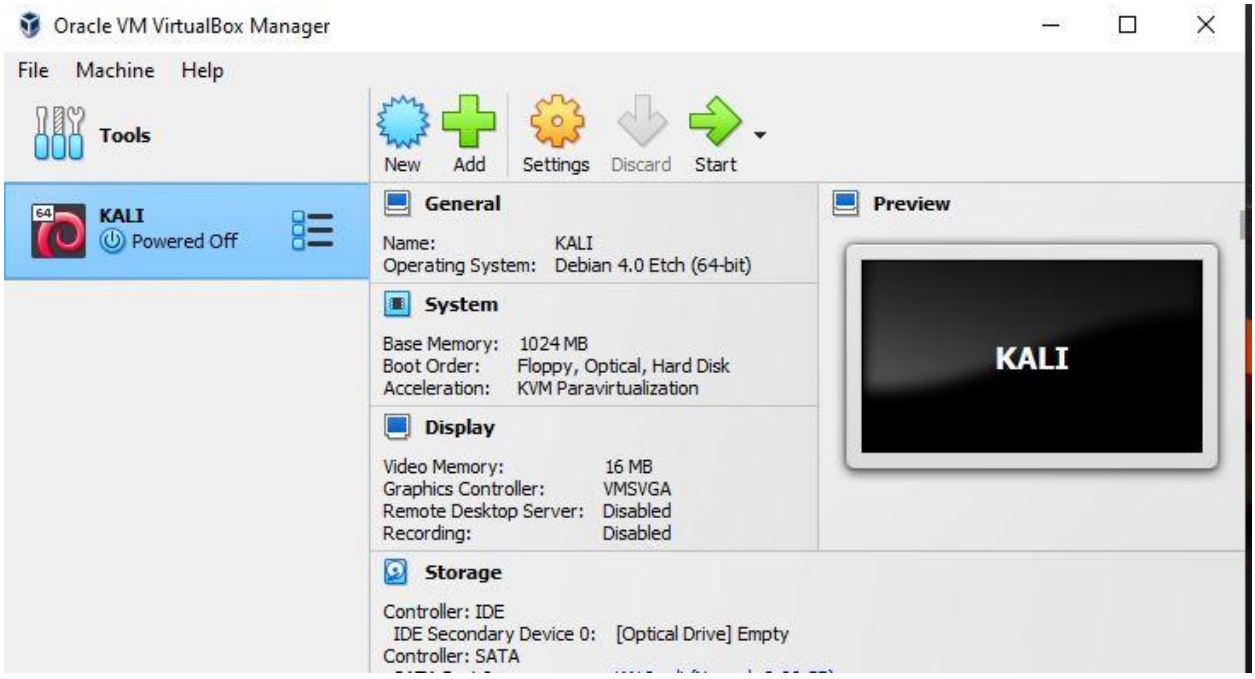
Step 4: You can increase your Disk size, but make sure how many free space you have, if you are beginner go with default and click next



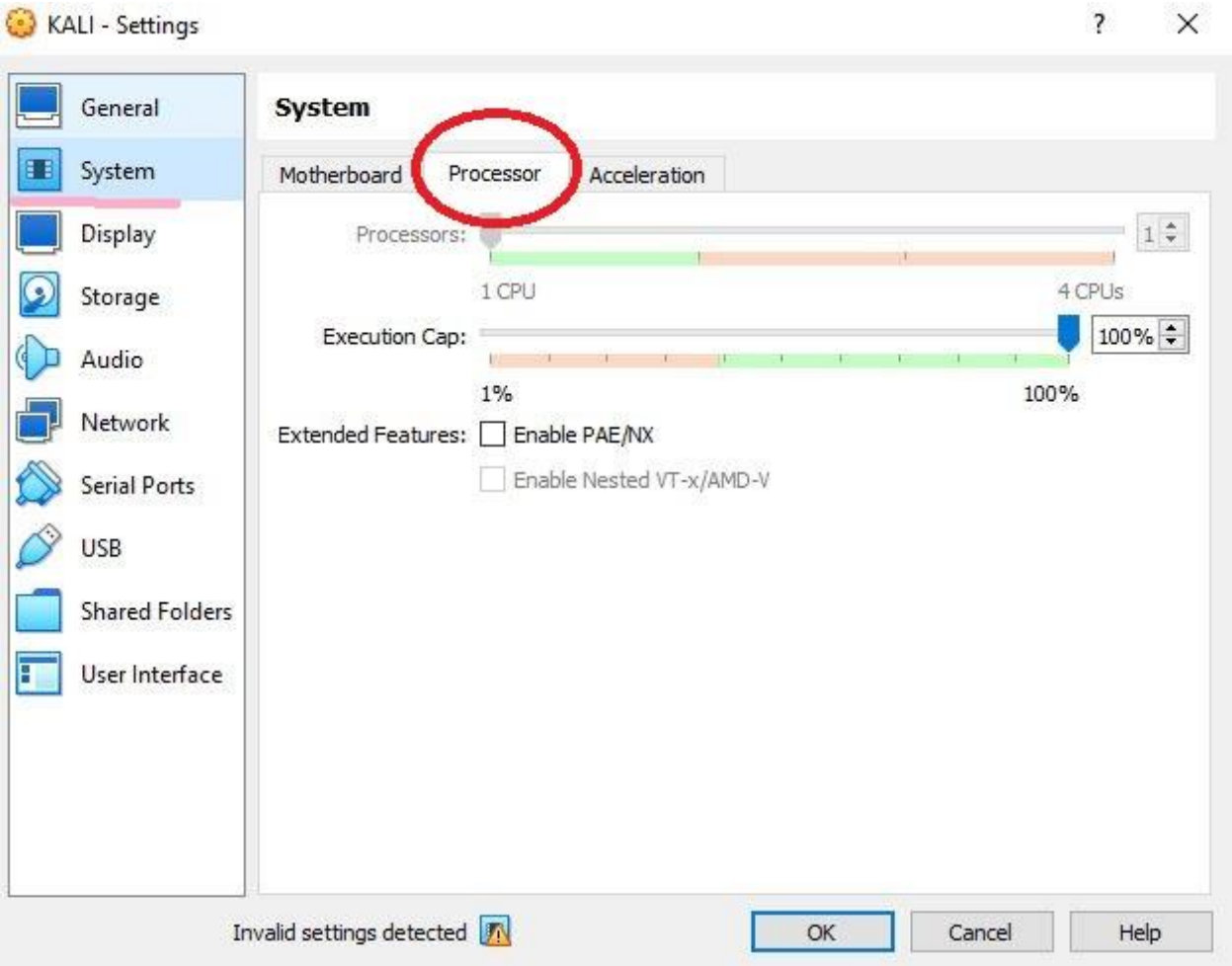
Step 5: Click finish



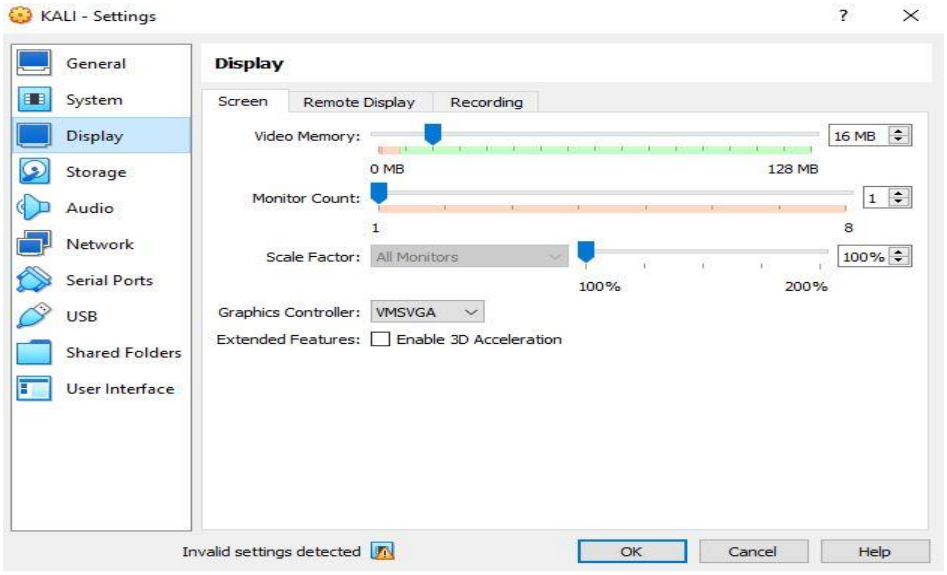
Step 6: Choose you kali and click settings



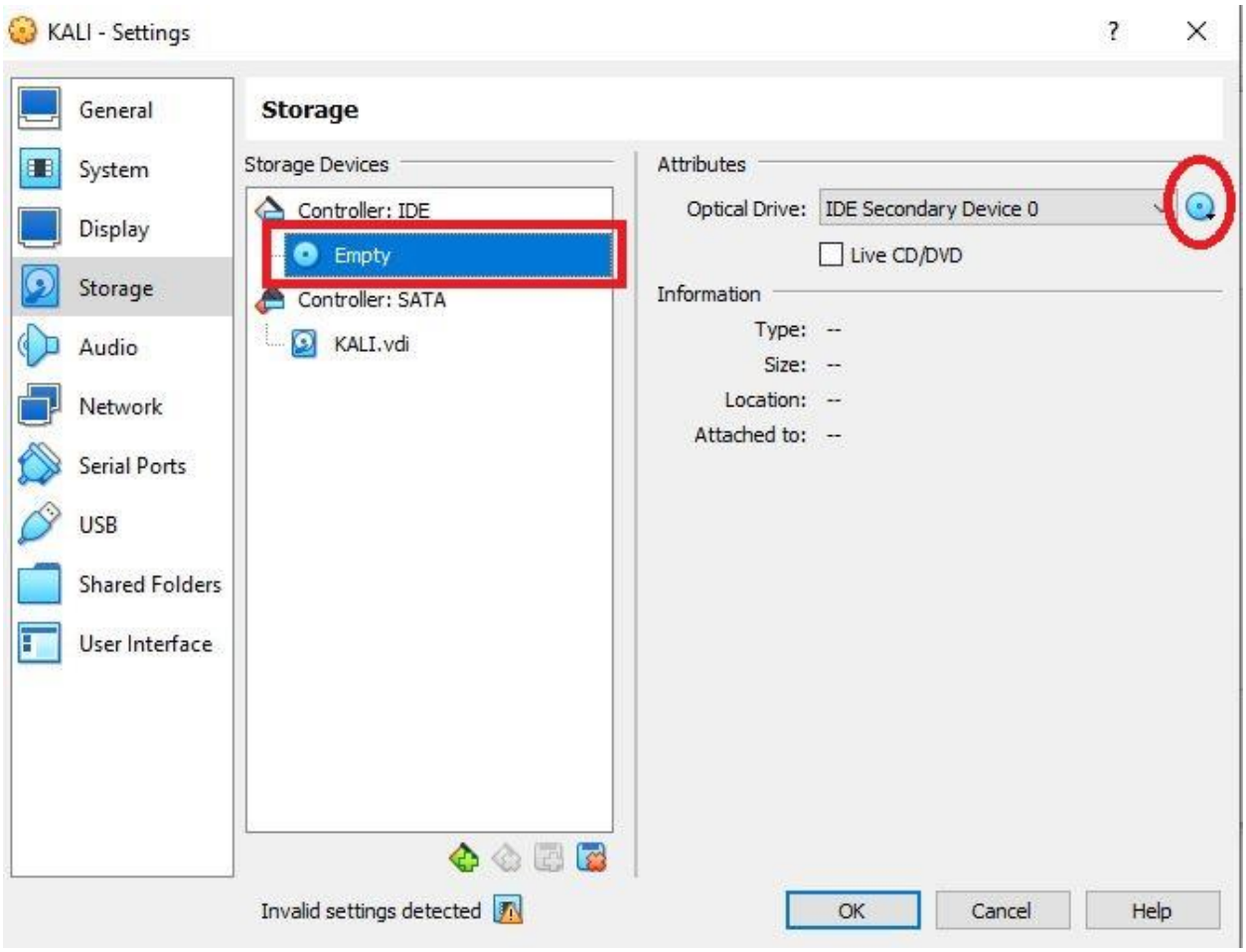
Step 6: System > processor > and change processor to 2

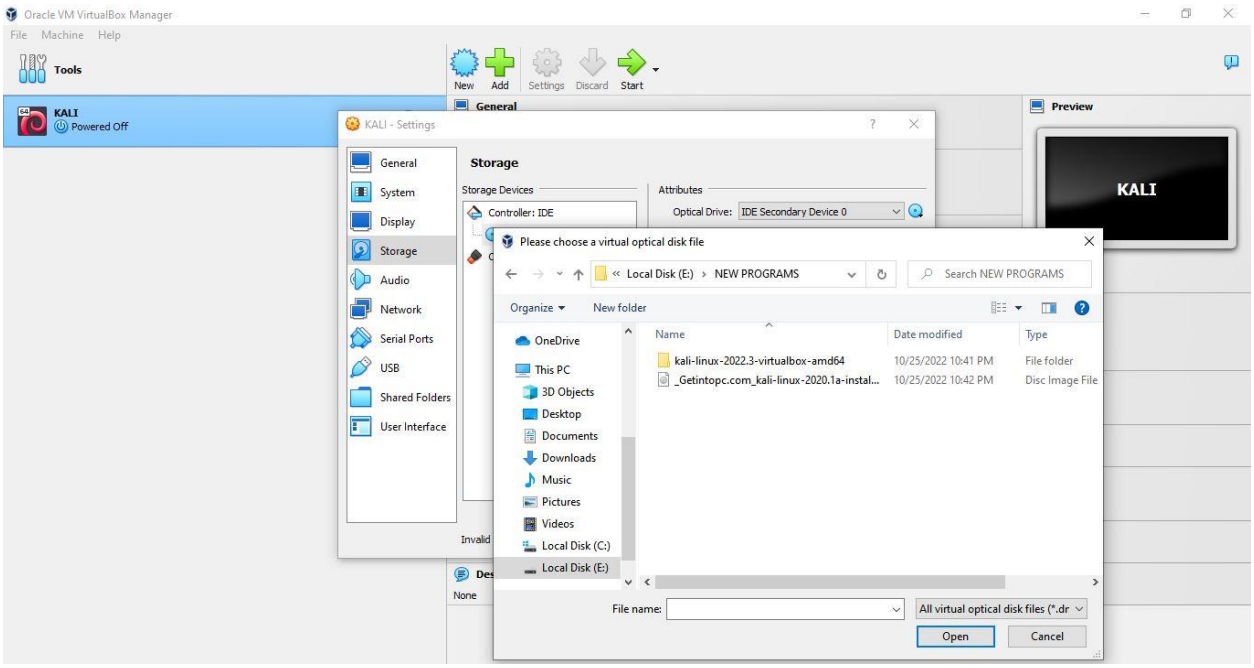


In the video memory you can increase if you want

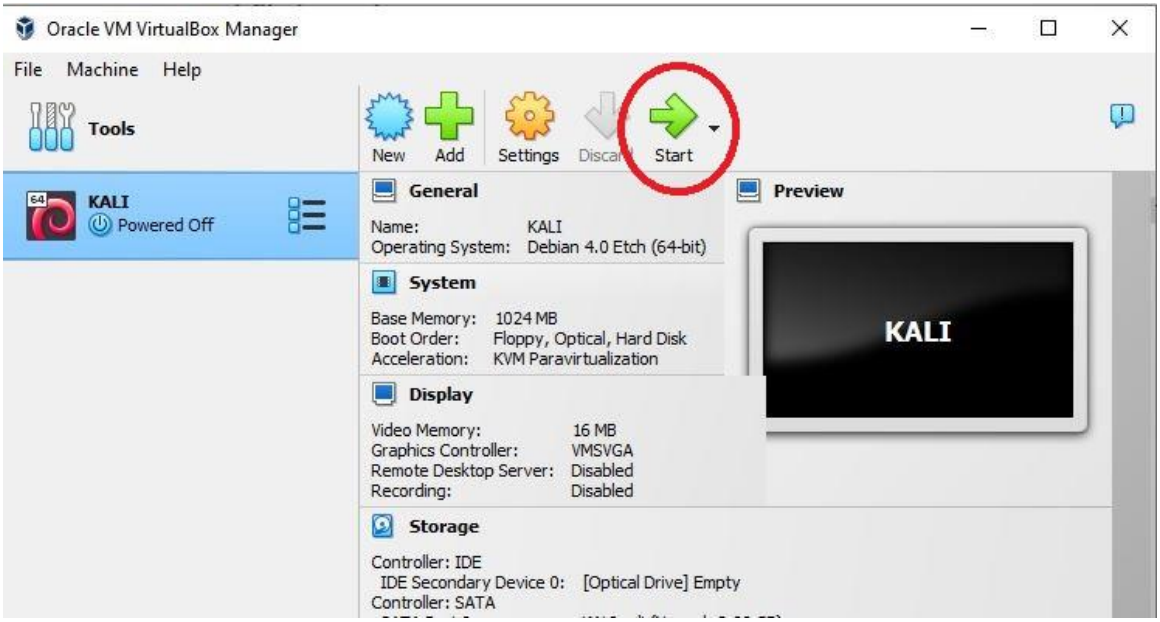


In the storage section, choose empty > the disk in the circle > choose disk file an select your .ISO file and open it





Choose kali and click start



Select Graphical installation

Step 7: To finish the installation follow these steps

I. select your language
II. select your location
III. in configure keyboard select your keyboard type
IV. enter hostname
V. domain name … if you don't have domain name you can leave it
VI. Enter the full name of the user
VII. Select username
VIII. Set a password (remember it's very important)
IX. Choose your time zone
X. Select guided use entire disk
XI. Click continue

XII. Choose your partition (if you don't understand go with the default or recommended for new user)

XIII. Select finish partition and write to disk

XIV. Select yes and then continue

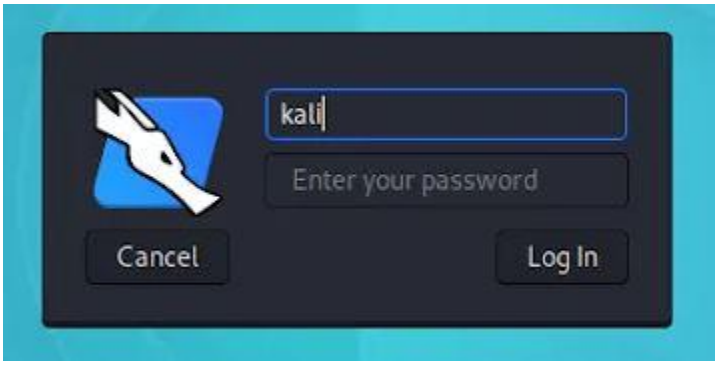
XV. For HTTP proxy leave it empty and click continue

XVI. Choose your software to install (If you don't understand go with default and click continue)

XVII. Select Yes and continue

XVIII. For the install the GRUB select the second option (Not the first option which is enter device manually) and continue

XIX. Wait and the kali Linux will restart it then enter your username and password

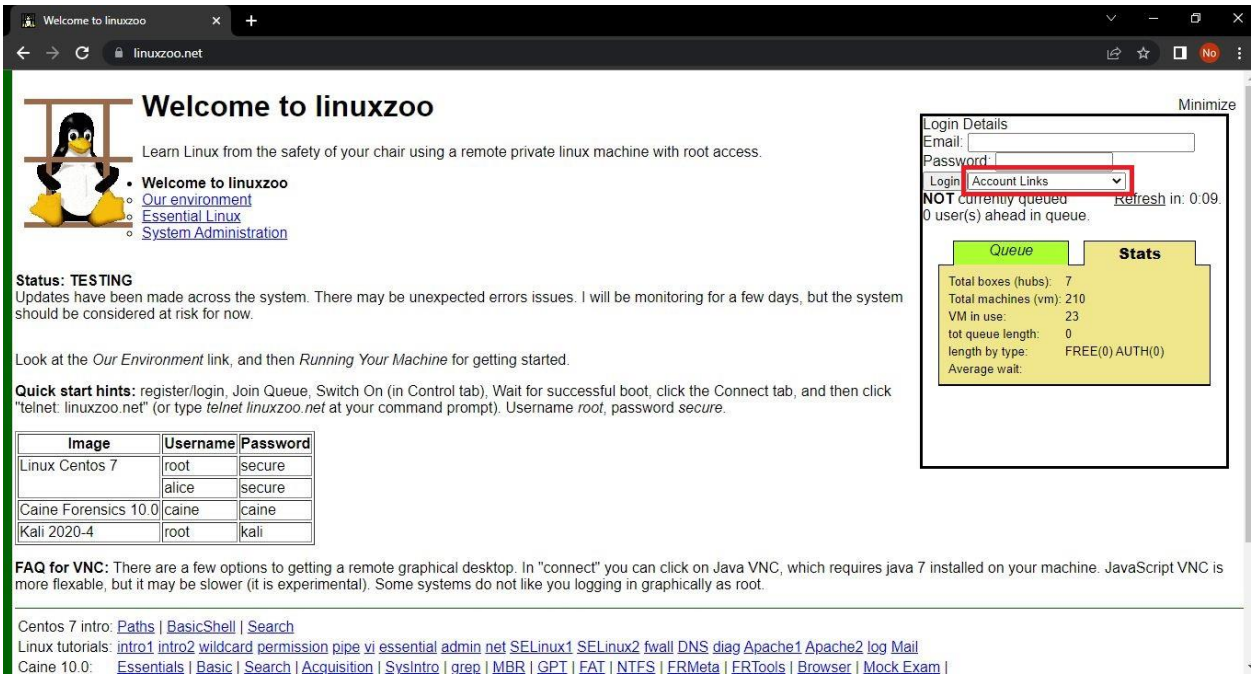


Run kali Linux in your web Browser without virtual machine

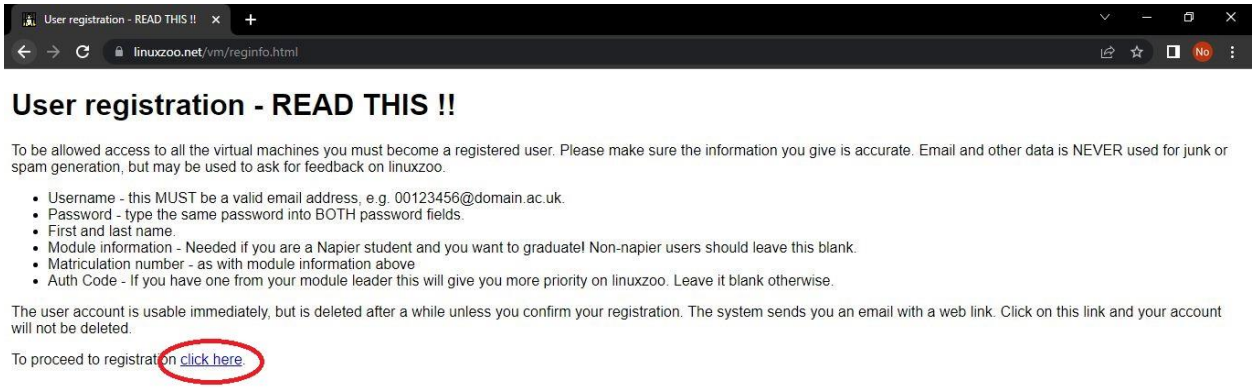
- You need internet to access this Kali Linux
- Your account will expire in 13 days (you can create another account after 13 days)

Installation process

- Step 1: go to https://linuxzoo.net/
- Step 2: click on account links and select register for an account

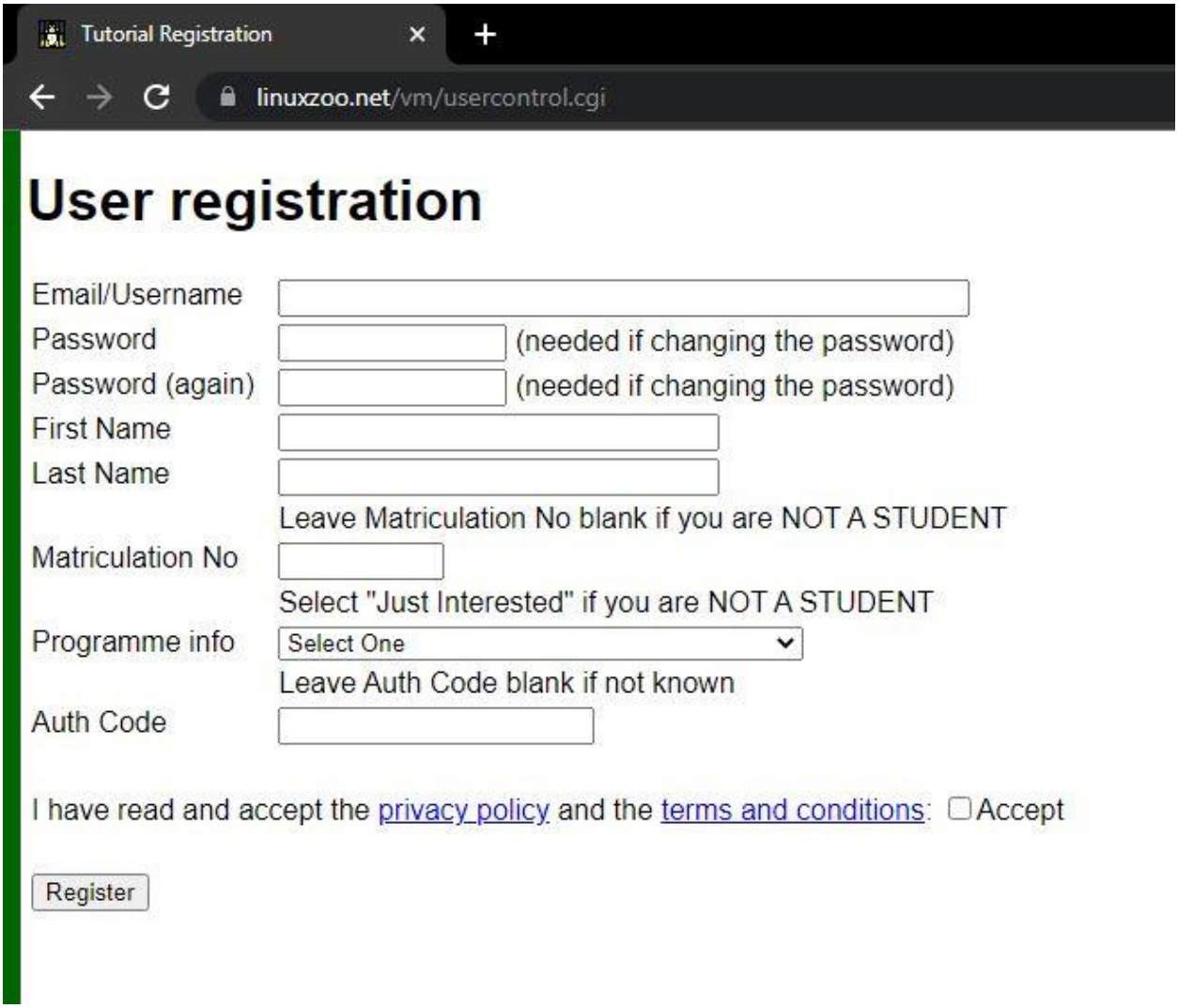


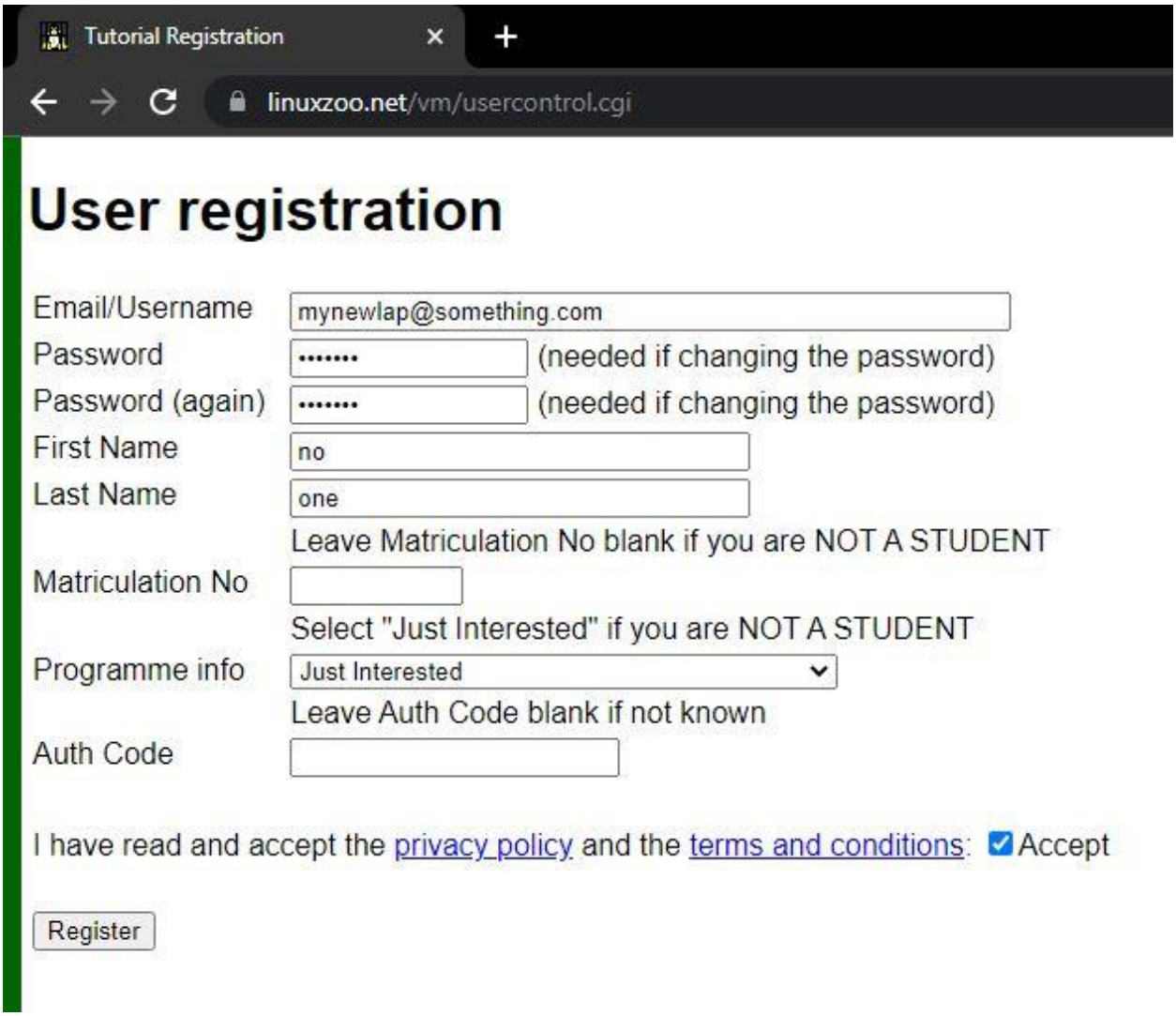
Then

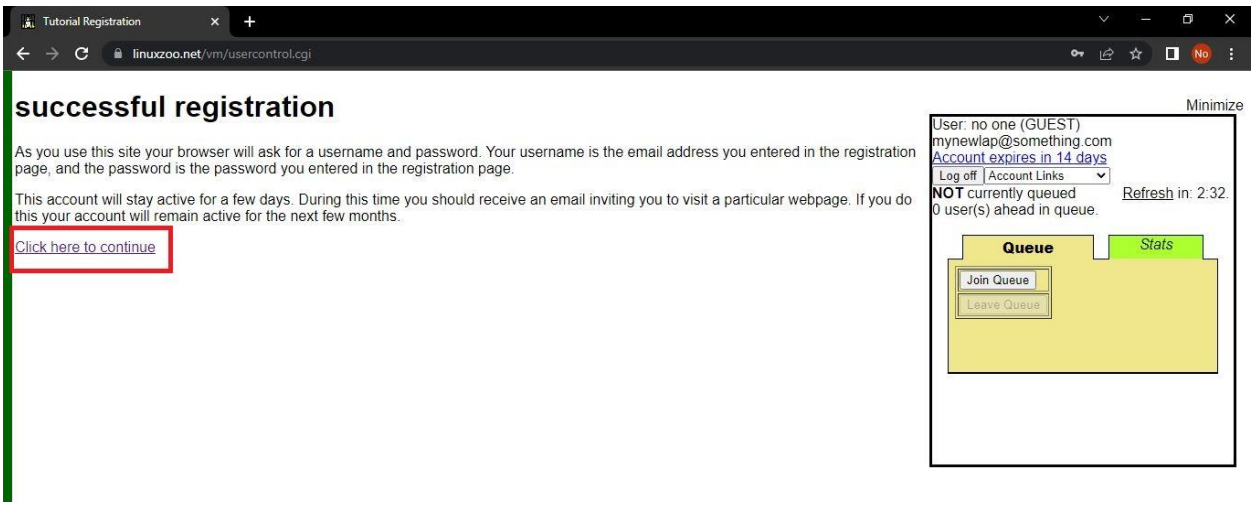


- Step 3: fill the form (it's not necessary to enter your real Email or username you can enter anything you want)
    - Email or username
    - Enter password and re-enter
    - Enter first name and last name
    - In Matriculation No: leave it empty
    - In Programming info choose just interested
    - In Auth Code: leave it empty

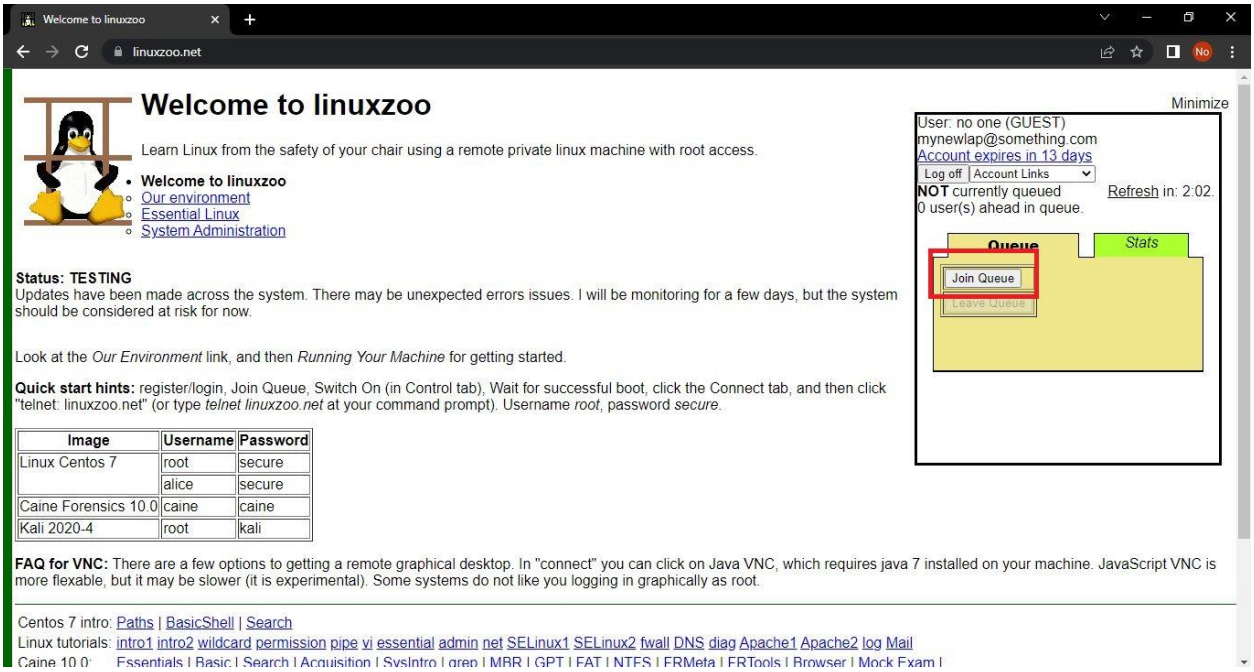
- Check the accept box and click register



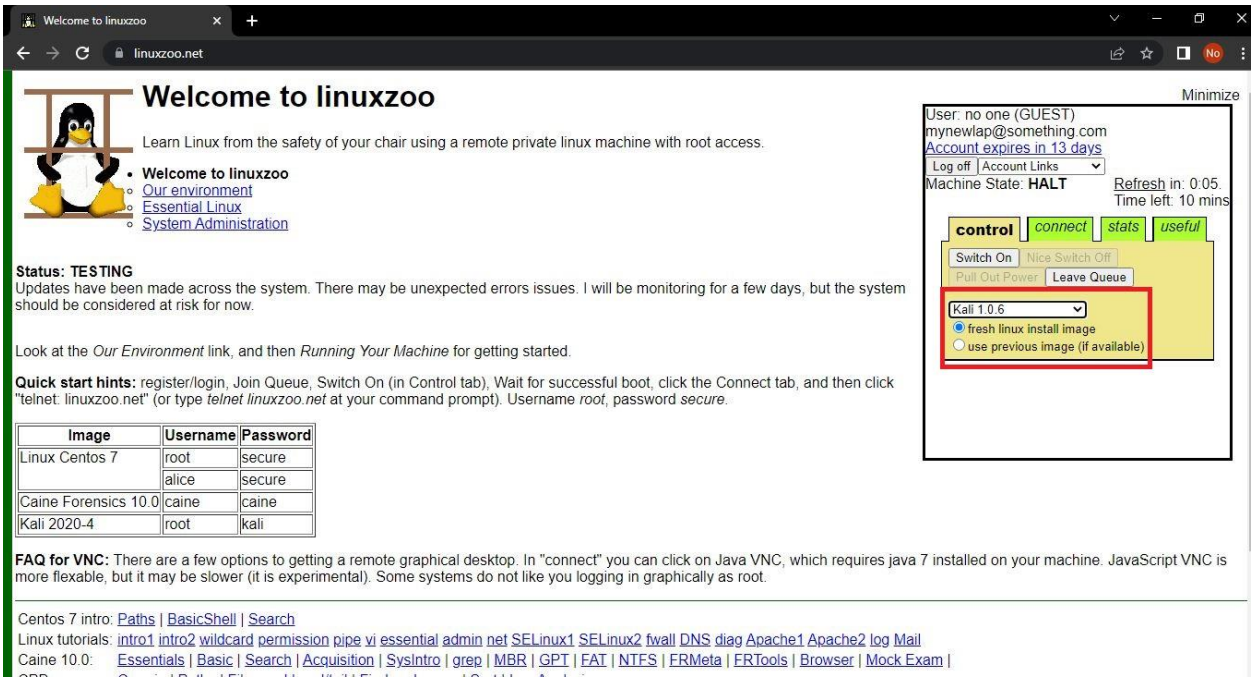

Tutorial Registration
linuxzoo.net/vm/usercontrol.cgi
User registration
Email/Username
mynewlap@something.com
Password
(needed if changing the password)
Password (again)
(needed if changing the password)
First Name
no
Last Name
one
Leave Matriculation No blank if you are NOT A STUDENT
Matriculation No
Select "Just Interested" if you are NOT A STUDENT
Programme info
Just Interested
Leave Auth Code blank if not known
Auth Code
I have read and accept the privacy policy and the terms and conditions: Accept
Register


Tutorial Registration
linuxzoo.net/vm/usercontrol.cgi
successful registration
As you use this site your browser will ask for a username and password. Your username is the email address you entered in the registration page, and the password is the password you entered in the registration page.
This account will stay active for a few days. During this time you should receive an email inviting you to visit a particular webpage. If you do this your account will remain active for the next few months.
Click here to continue
Minimize
User: no one (GUEST)
mynewlap@something.com
Account expires in 14 days
Log off
Account Links
NOT currently queued
Refresh in: 2:32.
0 user(s) ahead in queue.
Queue
Stats
Join Queue
Leave Queue

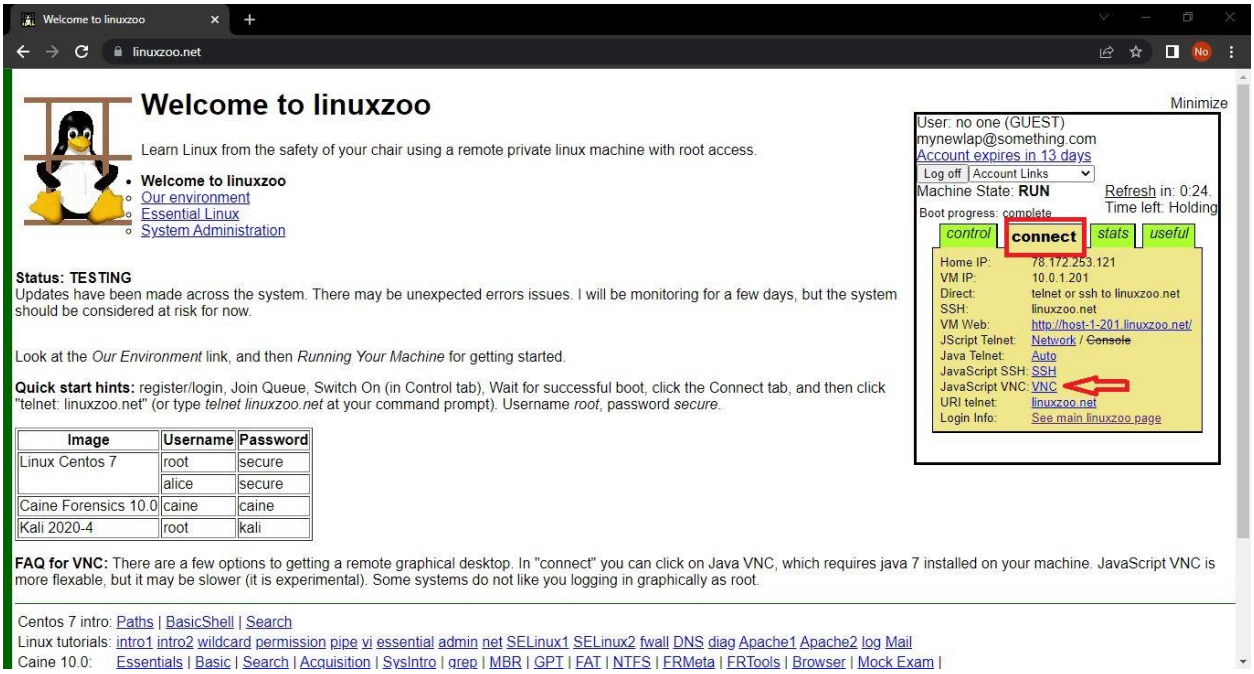
Step 4: Click on join queue



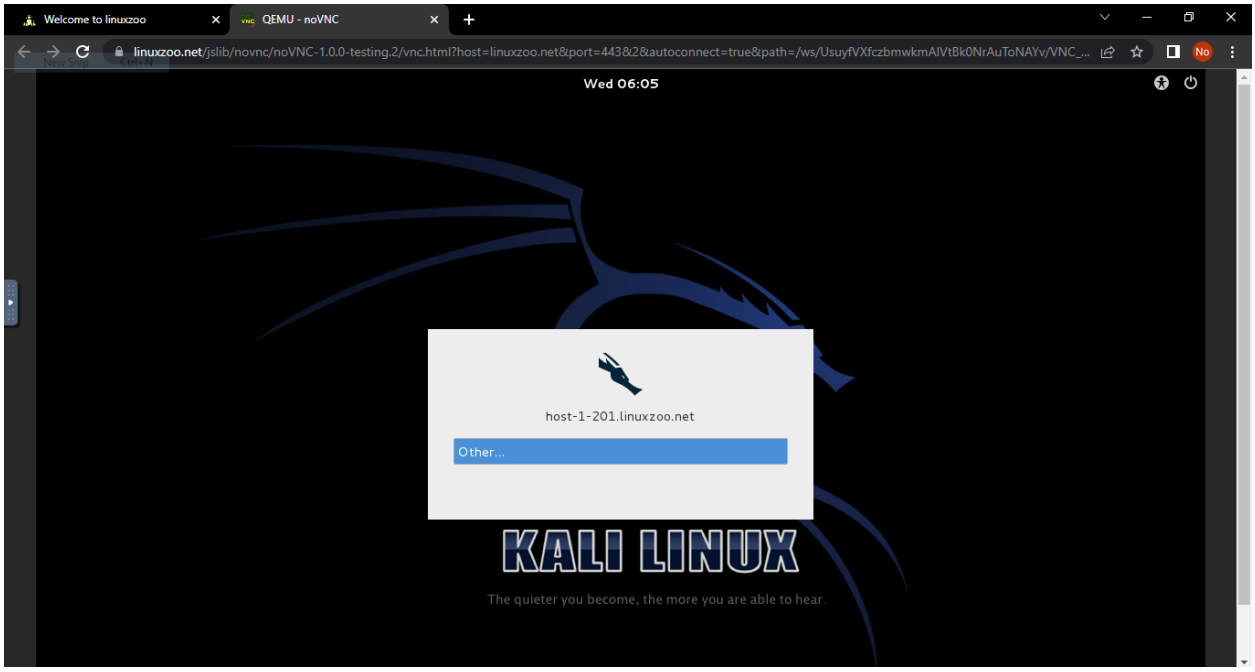
Step 4: check free Linux install image and choose kali 1.0.6 in the selection button and click switch on, then wait to complete boot programs



Step 5: choose connect then select VNC

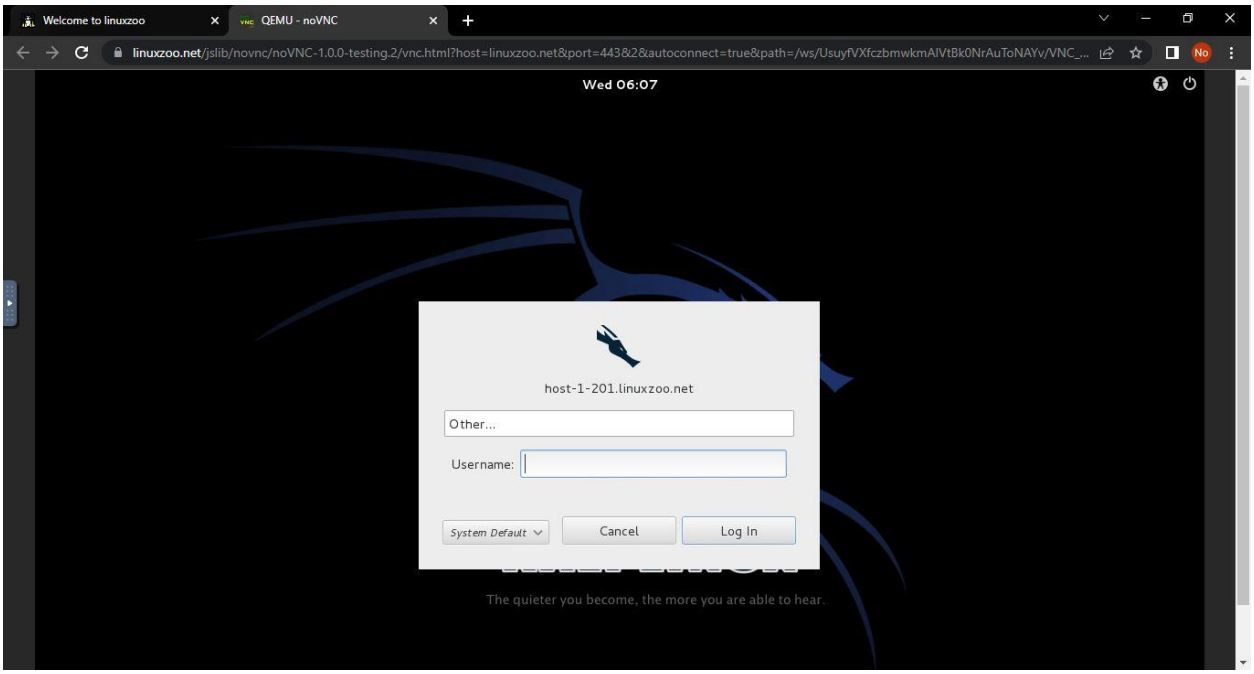


Click other

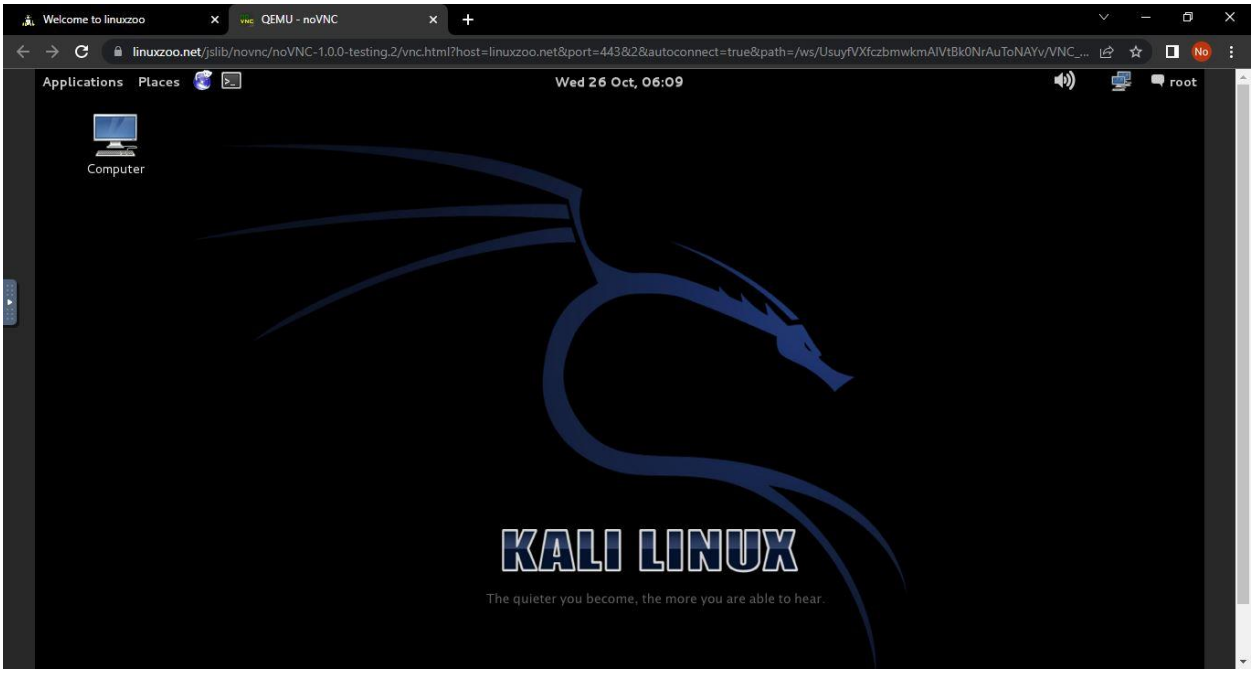


USERNAME: **root**

PASSWORD: **kali**

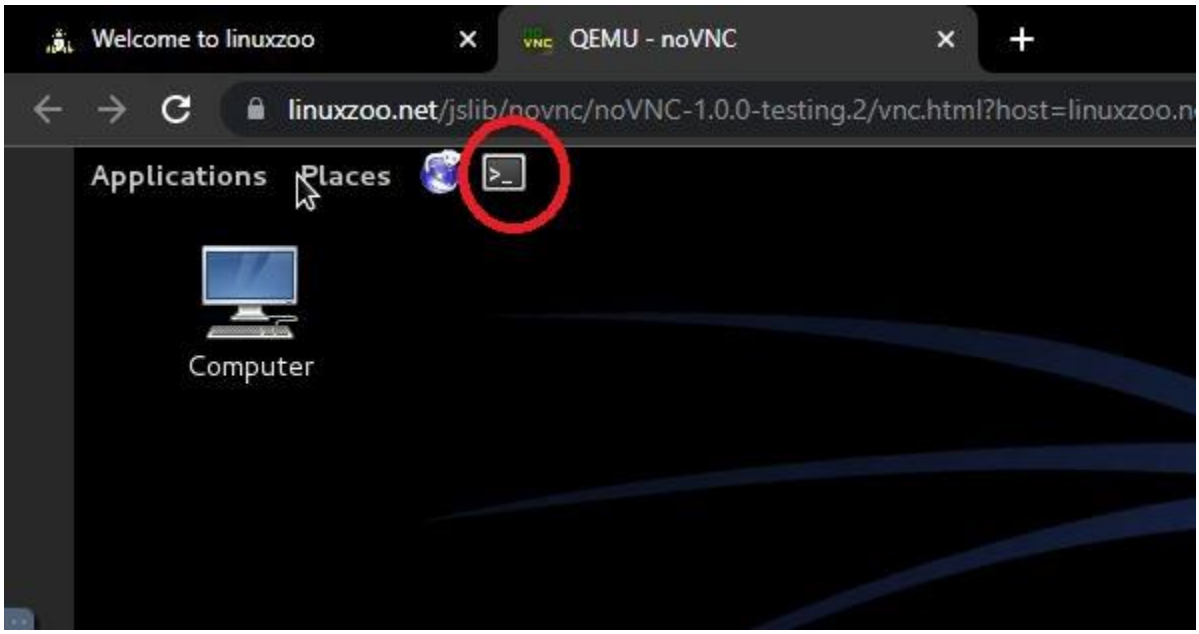


NOW you have kali Linux on your browser



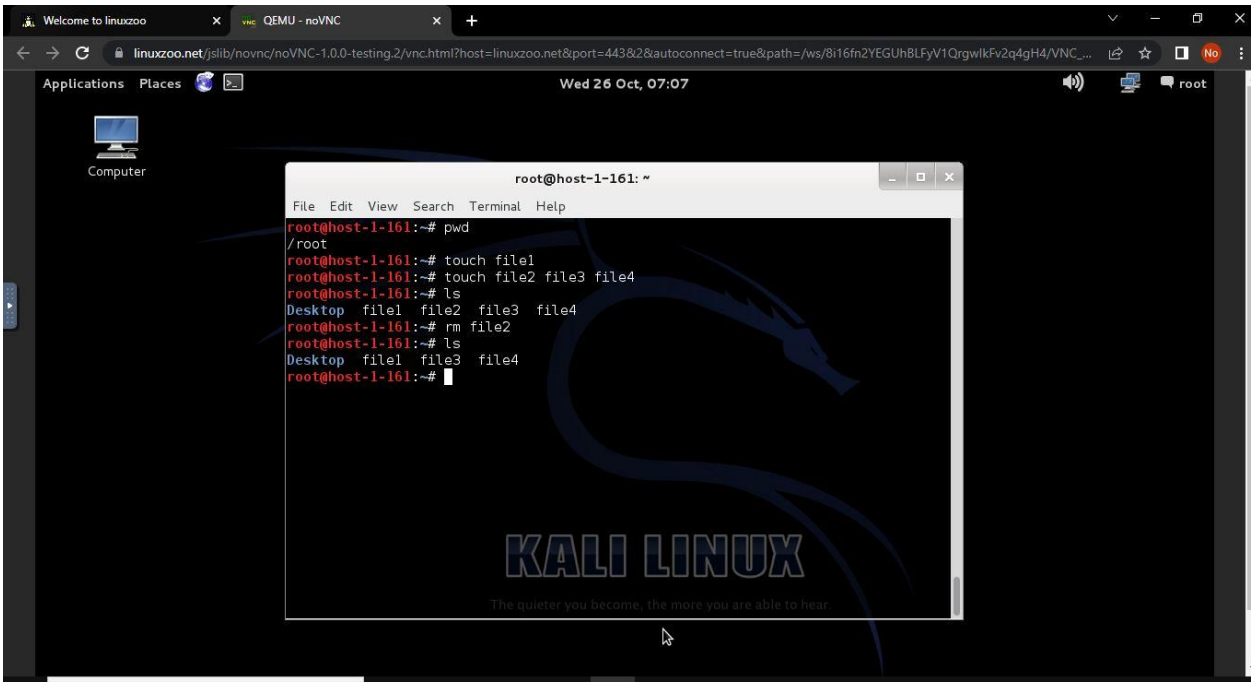
Kali Linux basic commands

- To open Terminal (command line internet)

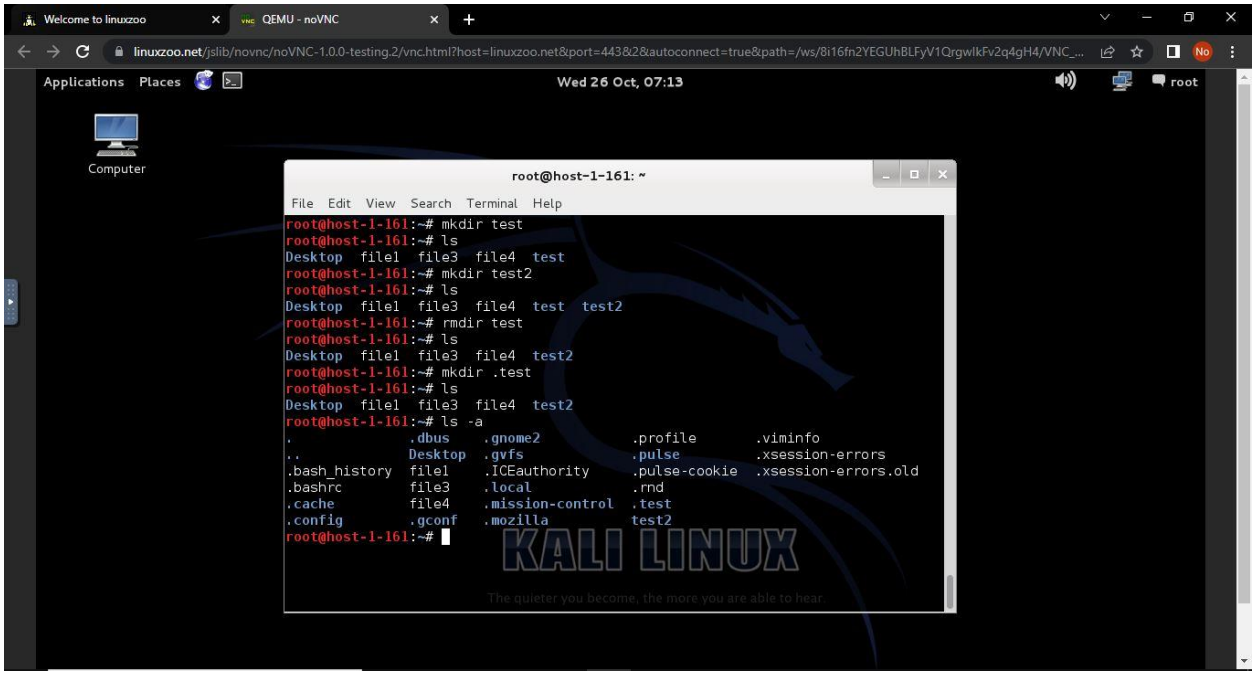


NOTE: Kali Linux is case sensitive, which means the word 'desktop' is not same as 'Desktop', also in Kali Linux everything is file.

1. **Pwd: p**rint **w**orking **d**irectory knowing your current directory
2. **Touch:** Creating files … Touch one or you can create multiple file once ***Touch tesst1 test2 test3,*** if you want delete file **rm test1 test2 test3 …**rm = remove
3. **LS:** lists the content of the working directory
    - **LS –L:** showing contents with details
    - **LS –A:** showing all contents even the hidden ones (Dot files)
    - **LS –LA:** showing all contents even hidden ones (dot files)
    - **LS –R:** showing folder inside folder inside folder …
    - **La –LH:** showing folder with size in KB



4. **CLEAR:** to clear the screen or ***CTRL + L***
5. **MKDIR:** make directory (folder) is used to create directory… ***mkdir test***
6. **RMDIR:** remove directory … **rmdir test**
7. create hidden folder use dot… ***rmdir .test***



To understand more you need to practice these commands

8. **CAT:** printing what is inside of document example: ***Cat list.txt***
    - Combining files & save in another file … ***cat file1 file2 >file3***
9. Changing text in file from lower case to upper case or vice versa
    - Cat ChangingFile | tr from to >NewFile

      Cat file | tr a-z A-Z>newFile … from lower to upper
10. ***Wcfileame***… counting the content of the file ***Lines words bytes***
11. ***Sort fileName***.. printing sorted output without saving it
12. ***Du filename*** ... finding the size of the file
13. Head –n NumberOfLinesFileName … *head –n 3 file1* when you want to know only the first three lines of the file ***tail –n 3 file1*** when you want to know the last three lines of the file
14. Where something ***… where python3***to know where the file is located ***whoami*** … to know which username you are in.
15. **CD:** change directory is used to enter directory
    - **CD.. :** going back one directory, If you only write CD you will go back home directory
16. **CP :** copying something … CP fileNameNewNAME example ***cp test1 test0***
17. **MV:** moving something
    - MvfileNmaeFolderName….***Mv test1 folder1*** if they are in the same directory else use path instead of Folder1
    - **MV fileName ..** (two dots) move back one step, let's say if your file is inside Folder1 which is inside desktop and you want to copy your file from folder1 to desktop
    - ***MvoldNameNewName*** … renaming file
    - ***mv file1 Folder1/file0*** … move the file and give new name
18. **LESS:** opens and prints file on terminal … ***less file1*** tab **q** to quit

- **Less file1 | grepsearchingKeyword …** open and find specific text in the file like names, ETC

19. **Open fileName …** opening file (not in terminal like LESS)
20. **Man commandLine**… to know all command usage example when you want to know the all usage of LESS … ***man less***
21. ***DIFF file1 file2*** … comparing two files to know their difference
22. If you want to change your password type ***PASSWD*** then enter the current password then the new one
23. Echo ‘ massage ‘ … Is like print (‘something’)
24. Saving the result (command result) in the file example if you want to save LS’s result in the file ***LS >fileNAME*** if you want to save another thing don’t use single **>** or it will overwrivte use **>>** .. ***LS >>fileName***
25. **File permission**
    - if it start **–** then it is file
    - if it start **D** then it is directory
    - 9 different characters, and you can only have three letters **R**, **W**, and **X …** **(R=read, W=write, X=execution)**
    - The first three, is permission of the owner of the file,

      The second, is for the group’s permission

      The third, for every body’s permission, example
      - Rwxrw-r- -first it start with – so It’s file, the first three shows the owner can read, write and execute the file, the second three shows the group can read and write but not execution, and lastly the public can only read it
    - Changing permission u will use **U** as user **G** as group **O** as public example

      CHMOD ***permissionSide+Permission file1***

      Chmodo+r file1 file2 … means giving the public (O) the permission they can read file1 and file2, you can use minus symbol to refuse permission ***chmod o-r file1 file2***,

You can give/take three permission as the same time like ***chmod o-xwr file1 file2*** … refusing reading, writing and exeucting at the same time

As numbe: No permission=**0**, Read=**4**, Write=**2** and Execution=**1** example 777 means (1+2+4) … Owner, Group and others have full permission to read, write and execute

26. ZIP and Unzip files

- Zipping files: ***Gzip file1 file2 'file3 file4'*** now we zipped three files ('file3 file4' it is file who has the name file3 file4 because of using ' **'**)
  - ✓ Multiple files in one zip: ***tar cvfzipName files***

    Tar cvfFolderOnefile1 file2 'file3 file4'
- Unzipping files: ***Gunzip file1 file2 'file3 file4'***
  - ✓ Unzipping multiple files

    Tar xvfFolderOnefile1 file2 'file3 file4'

27. Installing packages

Sudo apt install something

Sudo apt update – update every time you want to install new packages

Sudo apt update &&sudo apt full-upgrade … best update

Sudo apt edit-sources – to know the source of your packages

Sudo apt list - - **installed** … to the packages you're installed

Apt list - -installed | grepnmap …finding specific package (namp)

Sudoapt purgenmap … delating/Uninstalling package (nmap)

- From github copy the list (where the script is)

Get clone pastTheLink… when you install and it has requriments example some python package use

Pip3 install -r RequarementFolderName.extension

28. Users

- ***Sudouseradd–m userNAME*** ... sudouseradd mom
  - ✓ Creating system user ***Sudouseradd–r userNAME***

- ***SudopasswduserName*** … sudopasswd mom and set up password

- Create group to manage users as one

  SudogroupaddgroupName … sudogroupadd family

  - ✓ Add user to the group

    sudousermod –aGgroupName Username

    sudousermod –aG family mom

  - ✓ Deleting user from the group

    Sudo**userdel –r userName** … sudouserdel –r mom

  - ✓ To know which group is belong the user

    GroupsuserName … groups mom

  - ✓ Switching between users ***su – Username*** *… type exit t*

  - ✓ To know user's id …. Id username … ***id mom***

  - ✓ ***Sudochage –i mom*** … to know user mom's details

  - ✓ ***Sudochage mom*** … change user mom's details

29. Processor

- **Top:** CPU monitoring
- to know all running program … ***ps–aux***
- **pstree** … the process tree, all program and how they relate and **SystemD** is the root to know all running systems …

  sudosytemctl list-units

  - ✓ all programms running in your currently user checking ***ps –u Username***
  - ✓ if you want to close application by force first fine it's ID using

    pgrepfirefox then use ***kill firefoxID***

  - ✓ to monitor the processor… ***top***
  - ✓ stopping system … sudosystemctl stop something example

    sudosystemctl stop sshd

  - ✓ checking it's active or not ***sudosystemctl status sshd***
  - ✓ starting … ***sudosystemctl start sshd***

- ✓ restart … ***sudosystemctlreload/restartsshd***
- ✓ disabling to start automatically in boot season … ***sudosystemctldisablesshd***
- ✓ Enabling ***sudosystemctlenablesshd***
  Checking it is enable or not
  sudosystemctlis-active sshd

30. Variables

- **V*ariabeNAME='value'* ..**name='mohamed'
- Calling the varaible …***echo $name***
- You can save long path in one variable example varName='\home\home\Desktop\folder ' then you can go that variable instead of going long path … ***cd $varName***

31. Finding files and folders …

- Know file name but not locations: ***sudofind –name file1***
- You know the permissions and location but you don't know the name: ***sudo find /home –perm 777***
- Find directories with their permission
  SudoFind -type d –perm 777(**D** is for directory you can change **F** if you want to search file)
- ***Locate filename*** … locate is faster than find and it also finds files and folders and there is no more complicated options

32. Send fine in your local user to the root so only root user can write or delate that file ***sudochown root filename***

33. ***Nslookup google.com***... finding the ip address of google

34. Creating your own short cut commands

- In the /home/… there is hidden file called .bashsrc open that file as ***nano .bashrc*** then write down your shortcuts with using this ***alias c='clear'*** now I can use C instead of writing clear every time

35. Linking two files … if one of them change content then the other will see it ***LN file1 file2***

36. ***W …*** to know what users are doing

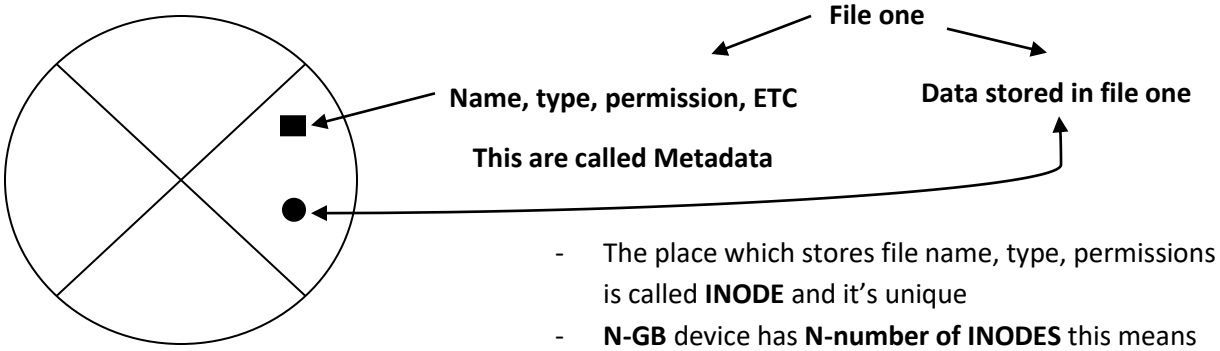
37. Grep something location … example let's find the name MOHA in the fileN … ***grep –imoha /home/moik/Desktop/fileN***

38. Chaining symbol (;) is using multiple commands in one line example ***Mkdir test; cd test; touch file1***

39. ***Lsblk*****:** knowing partitions (Linux everything is file)

40. ***Du –sh ** …** to know the size of all file in your current directory if you want specific file change * to file name … ***du –sh file1***

41. How data are stored in HD



HD with 4 partitions

- The place which stores file name, type, permissions is called **INODE** and it's unique
- **N-GB** device has **N-number of INODES** this means even empty files will have INODES, example if you have 10k and created 10k empty files then your memory is full became there is no INODES

- ***Df –hi***… to know the number of used and free INODES

42. Links

- It is like shortcut icons in window (when you install application you will get shortcut icon on your desktop, so you can easily run the program
- In Linux shortcut is called Links

There are two types of links

i. **Soft link:** if you remove the original file then the shortcut will not work, because they have different INODES

   ln –s original_Pathshortcut_path

   ln –s /home/moik/Desktop/one/two/file1 /home/moik/NewFle

ii. **Hard link:** if you remove the original file then the shortcut will work, because the hard link and original link shares same INODES

   ln /home/moik/Desktop/one/two/file1 /home/moik/NewFle

43. giving file to the group so they can access is

setfact –m "g:student:rw-" fileN… I gave student group permission to access fileN

- ***getfaclfileN***… checking the permission details
- ***setfacl –b fileN***… back to normal (no access for student G)

44. installing softwares

- step 01: download the software, pycharm
- step 02: go to the pycharm location /Document/ or else
- step 03: run the sh file ***./pycharm.sh***

Sharing source b/w host OS and virtual OS

- ✓ create folder in local host computer
- ✓ in virtual box select your OS > settings > shared folders > add > in folder path select others and choose the folder > give permission
- ✓ in your virtual machine (Example Kali Linux) you will see shared folder in home, everything in that folder will be shared both OS