Experiment 01

Learning Objective:

Using **Kali Linux** Operating System and Understanding basic **Linux Commands**

Operating System : Kali Linux

Theory Kali Linux is a Debian-based Linux distribution developed for penetration testing, and is especially useful for security specialists and enthusiasts. Kali Linux, formerly known as BackTrack Linux, includes a lot of tools and applications for network audits. Kali can be run as a Live DVD, and can be installed on a computer as a host operating system (OS) as any other Linux. However, it is not recommended that you use Kali as a general-purpose desktop operating system. At the same time, when using Kali Live DVD, settings are not saved after a system reboot. In this situation, virtual machines can be of great help.

The advantages of installing Kali Linux on VirtualBox are:

By running multiple operating systems simultaneously (a host OS and a guest OS or multiple guests), you don't need to reboot a computer as when using dual boot.
A VM running Kali Linux is isolated from your host OS – running Kali on a VM in an isolated environment is secure.

You can take a snapshot and roll back to the previous VM state if something goes wrong. The risk of harm to Kali Linux on a VM is minimal as a result.
You can copy a configured VM on which Kali Linux is installed to other computers.
You can attach physical USB devices, such as external network adapters directly to a VM due to the VirtualBox USB pass-through feature.

Make sure that VirtualBox is installed on your host operating system before continuing, using the latest VirtualBox version if possible. Please install VirtualBox Extension Pack on your host machine to use some advanced features such as USB pass-through.

Implementation:

Downloading the Installation Image of Kali Linux

Step 1: First, go to the official web site and download the ISO image of Kali Linux. There are multiple 32-bit and 64-bit images that have different graphical user interfaces (Gnome, KDE, XFCE, LXDE etc.).

Step 2: Let's download Kali Linux 64-bit v.2019.2 – this distribution has Gnome as a graphical user interface (GUI). You can download images via HTTP and Torrent protocols.

Step 3: Save the ISO file to a custom folder, for example, *C:\VirtualBox\kali-linux-2019.2-amd64.iso*. You can also verify the SHA256 checksum to make sure that your image is consistent after finishing downloading.

Image Name	Download	Size	Version	SHA256Sum
Kali Linux 64-Bit	HTTP | Torrent	3.2G	2019.2	67574ee0039eaf4043a237e7c4b0eb432ca07ebf9c7b2dd0667e83bc3900b2cf
Kali Linux 32-Bit	HTTP | Torrent	3.2G	2019.2	1e03023bbd81fdec9c49717219c2c48f62da3f99009df1bbe73f158eef246282
Kali Linux LXDE 64-Bit	HTTP | Torrent	3.0G	2019.2	cd0d7fc95275de49b40208838f8fca2984d5cbec9472f54656dc351d09edc8dc
Kali Linux MATE 64-Bit	HTTP | Torrent	3.1G	2019.2	f81ca6a35bcd61678f1a84dc8949023b11c7434d80f35be2ac8d6f08dfd93bad
Kali Linux Light armhf	HTTP | Torrent	741M	2019.2	0f3ad59fc2fed868cb3ddaab38c7968a190e54e655c50b9561f847e9d17a7963
Kali Linux KDE 64-Bit	HTTP | Torrent	3.5G	2019.2	b794d360923c1f2c73f60783b8506cbfe3d4746c20e009ad21aa37b47c32749f

Creating a New VM

Step 1: Once you have downloaded the installation image, you can create a new **VM.** Open **VirtualBox** and create a new **VM (*Machine > New* or *Ctrl+N*)** on which **Kali Linux will be installed.**

Set the following VM parameters:

Name: Kali_x64

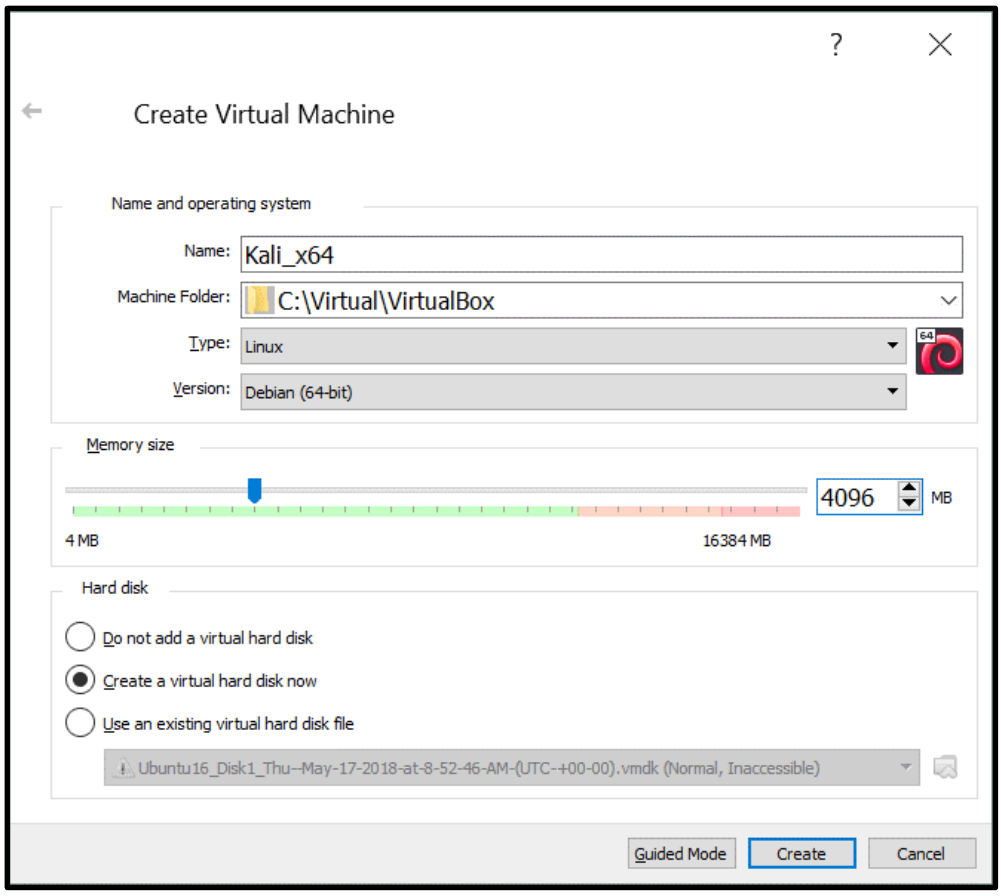
Machine Folder: **C:\Virtual\VirtualBox** (This path is used only for demo purpose. Try not to use a system partition to store VMs).

Type: Linux

Version: Debian (64-bit)

Memory size: 4096 MB. The VM memory size must be large enough to run a guest OS, though you should leave enough unallocated memory to run your host OS. In the current example, a host machine with 16 GB of RAM is used, which provides enough memory left for a host OS.

Hard disk: Create a virtual hard disk now.



Step 2: Set the virtual disk file location, for example ***C:\Virtual\VirtualBox\Kali_x6Kali_x64.vdi***

It is recommended that you store virtual disk files in the VM folder (such folder is selected by default).

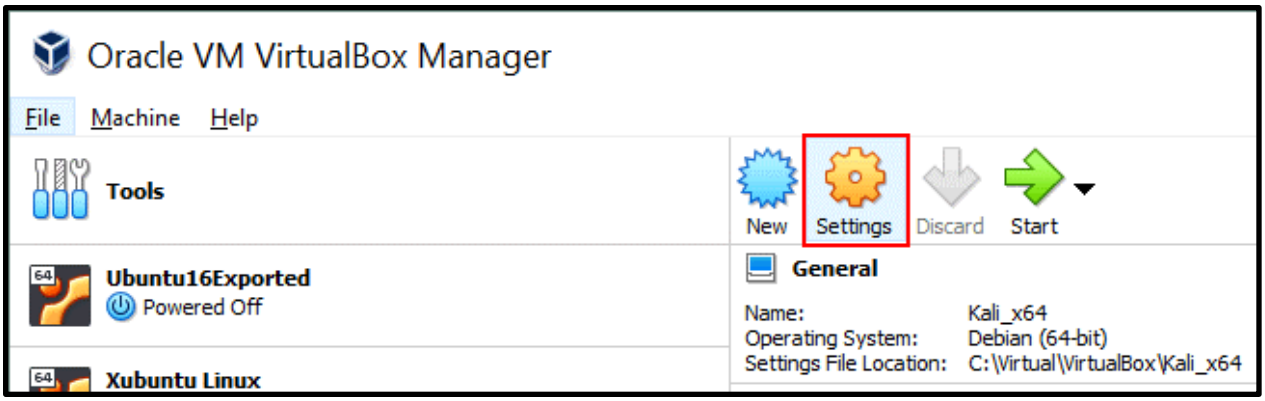
Set the virtual disk file size. It should be at least 20 GB.

Hard disk file type: VDI. A native VirtualBox format is selected.

Storage on physical disk: Dynamically allocated.

Click *Create* to finish creating a new VM.

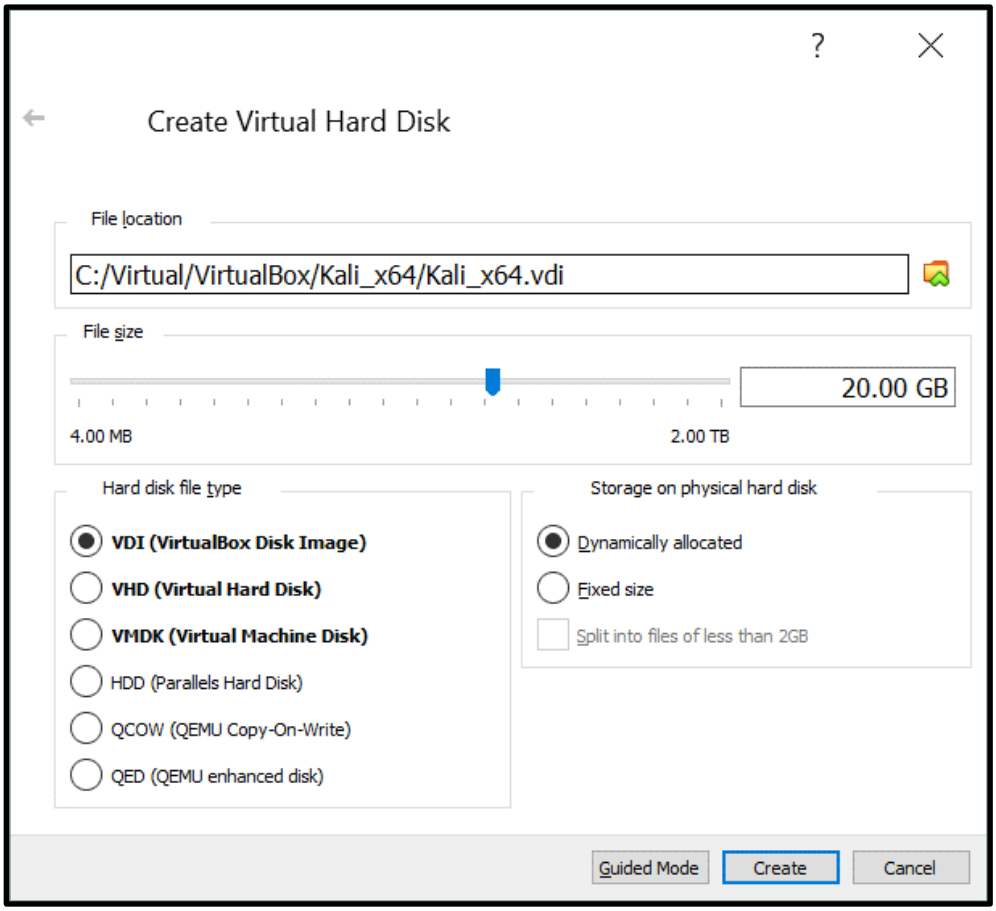
Step 3: After creating a new VM, some additional settings must be configured. Select your recently created virtual machine and open the VM settings.

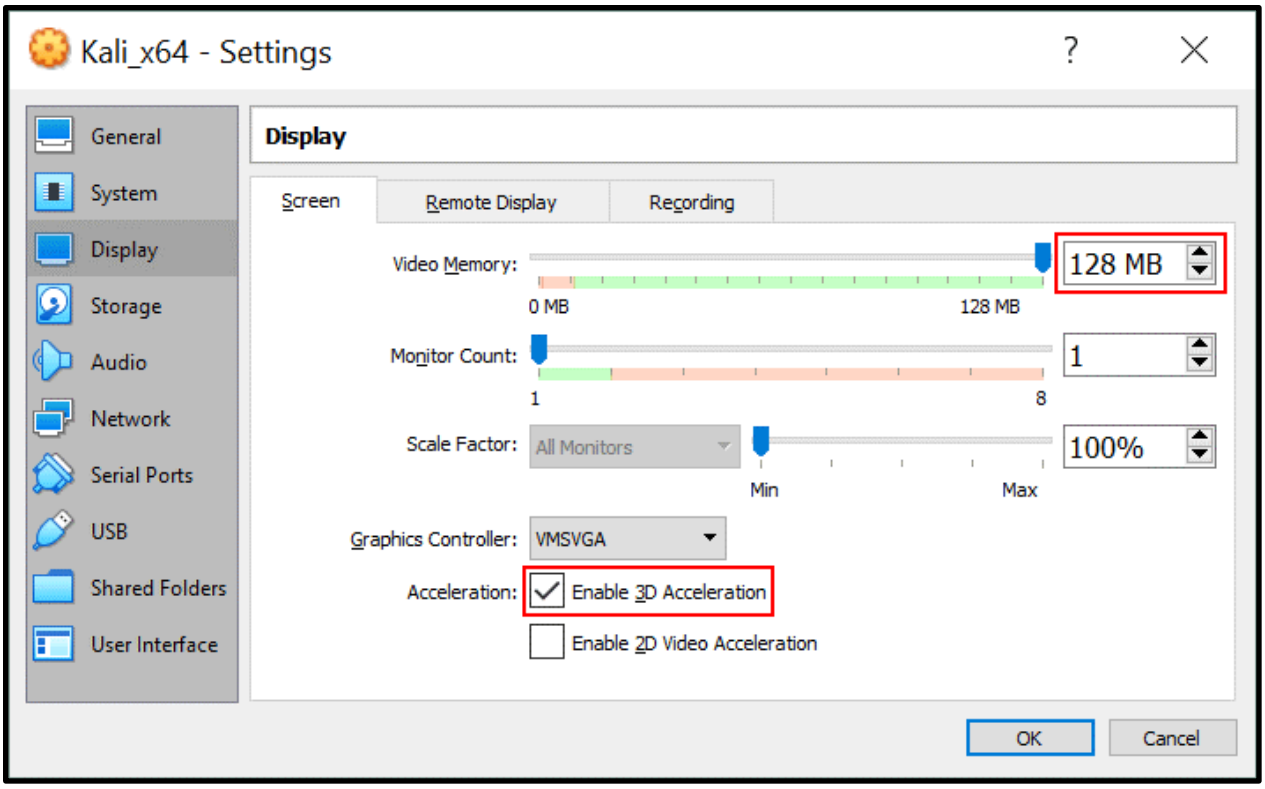


Display options

Step 4: Go to ***Display > Screen*** and set Video Memory to **128 MB**. It will prevent installer hanging.

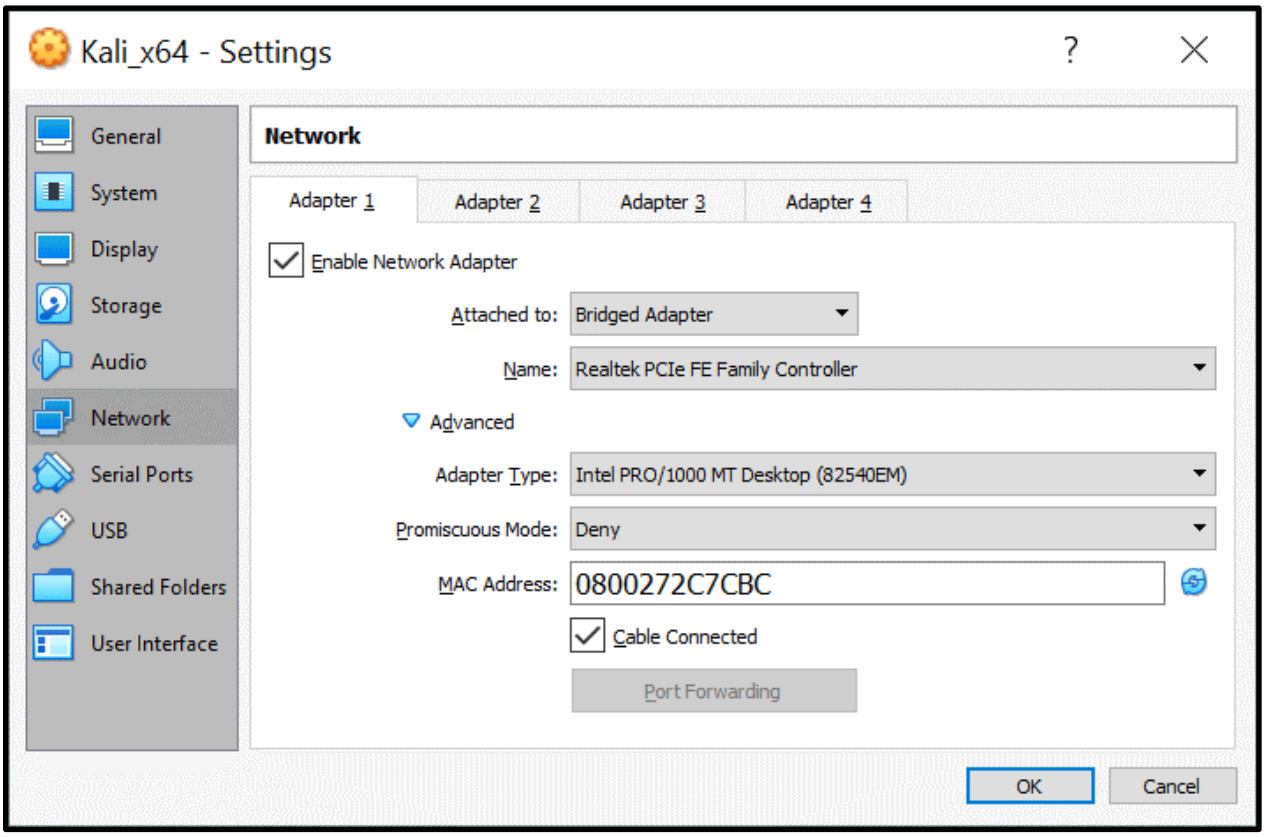
Step 5: Next, tick the checkbox *Enable **3D acceleration*** (optional). It will be useful for applications that need **3D acceleration**.




Kali_x64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Display
Screen
Remote Display
Recording
Video Memory:
128 MB
0 MB
128 MB
Monitor Count:
1
1
8
Scale Factor:
All Monitors
100%
Min
Max
Graphics Controller:
VMSVGA
Acceleration:
Enable 3D Acceleration
Enable 2D Video Acceleration
OK
Cancel

Network options

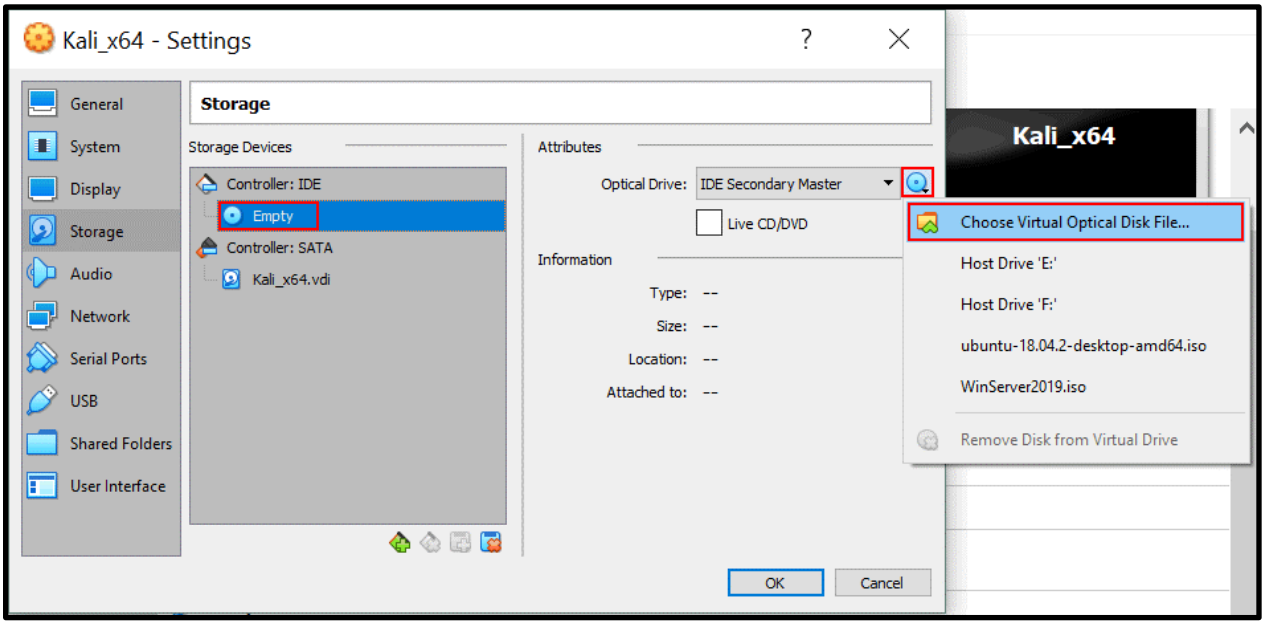
Step 6: Next, go to the network settings and select the networking mode of the virtual network adapter of the VM. Let's select the ***Bridged* mode** to use the VM network adapter much as you would for a physical network adapter of the host machine. In this case, the VM network adapter is connected to the same physical network as the host machine. You can set additional options such as network adapter name, type, MAC address etc.



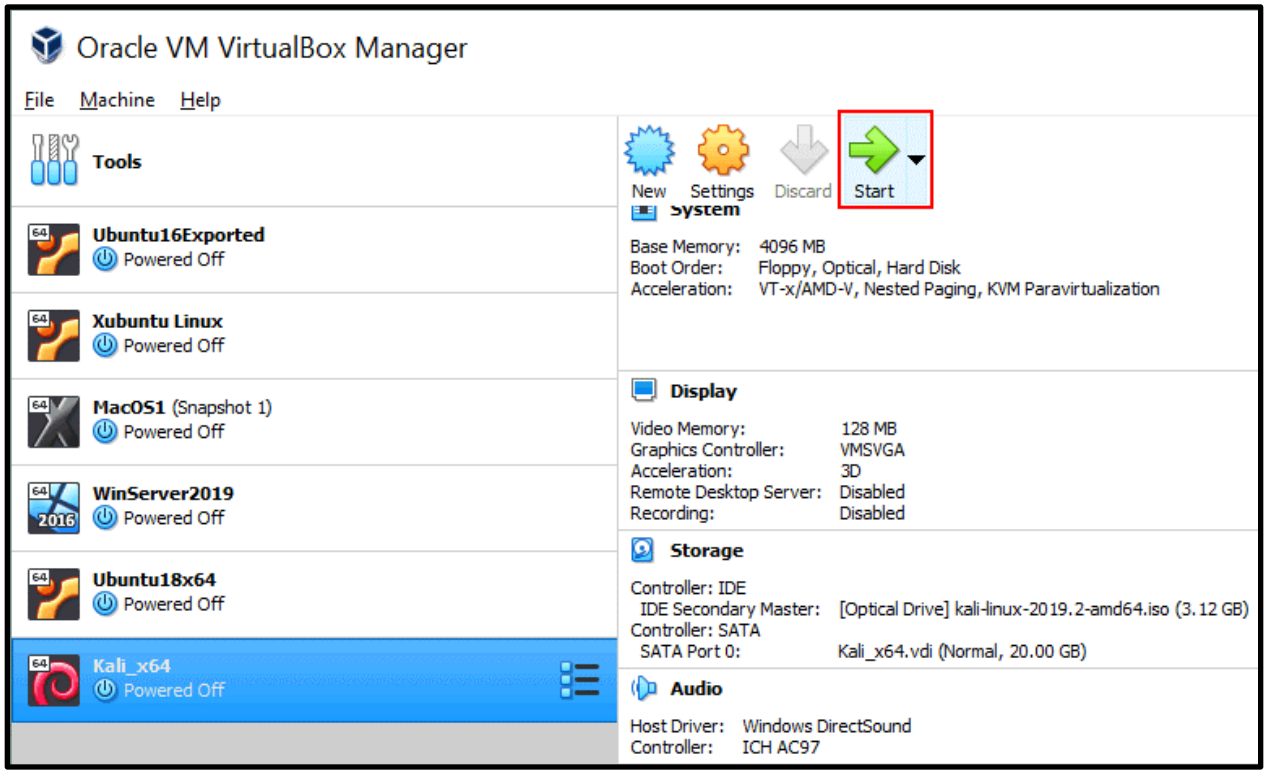
Boot options

Step 7: You have to insert your **virtual ISO DVD image** to a virtual DVD drive of the VM and then boot a virtual machine from that **ISO disk.** In the **VM settings, go to *Storage*,** select an **IDE controller** of your virtual optical drive (it is empty by default)**.** Click the *empty* status, then click the disc icon near **IDE Secondary Master** and in the opened menu, select *Choose Virtual* ***Optical Disk File*.**

Step 8: Kali Linux installation Browse the ISO image that you have downloaded from the official site before **(*kali-linux-2019.2-amd64.iso*).** Hit *OK* to save settings.

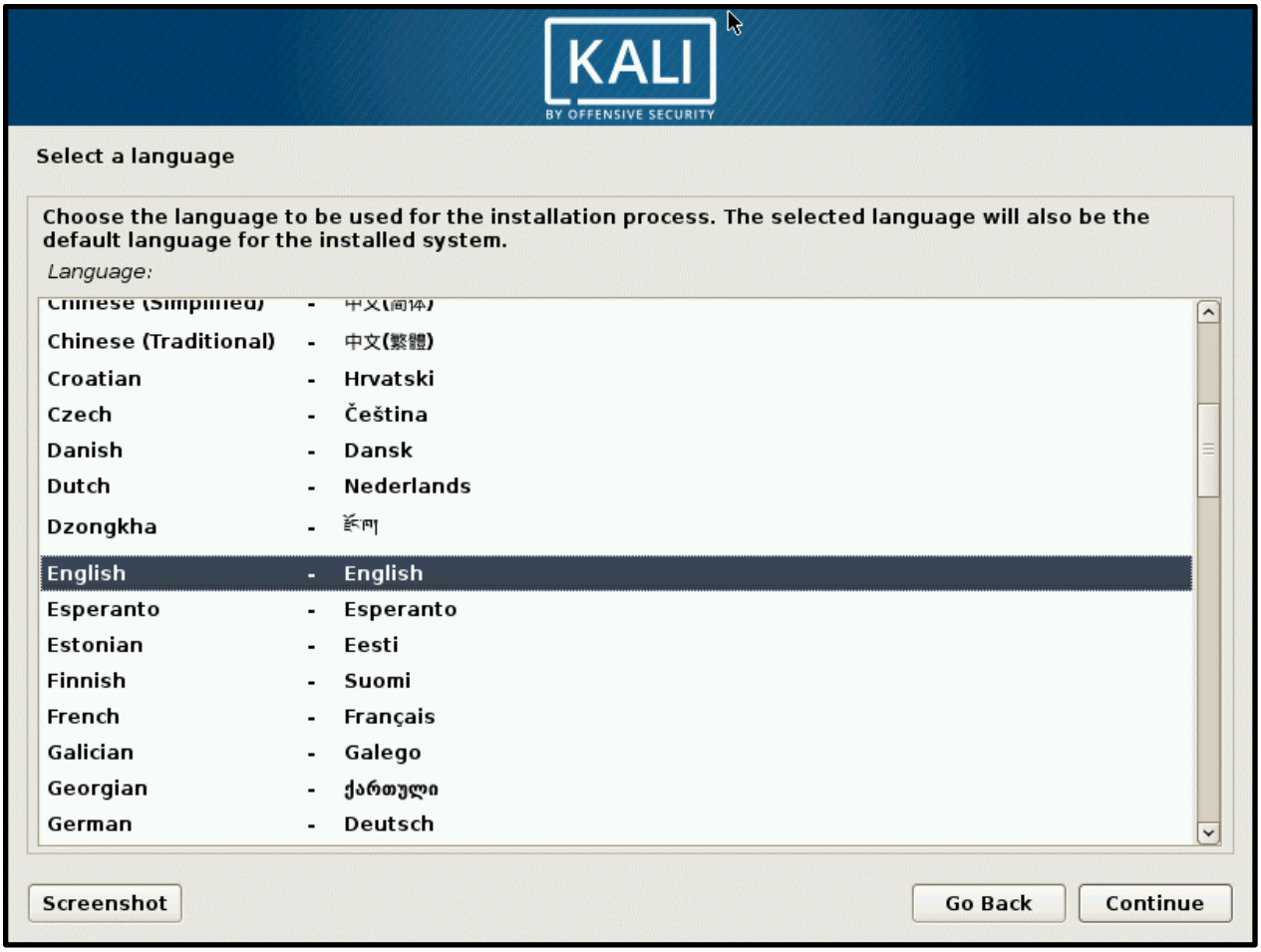


Step 9: Now you can start your new VM **(*Kali_x64* in this case)** and begin the Kali install.

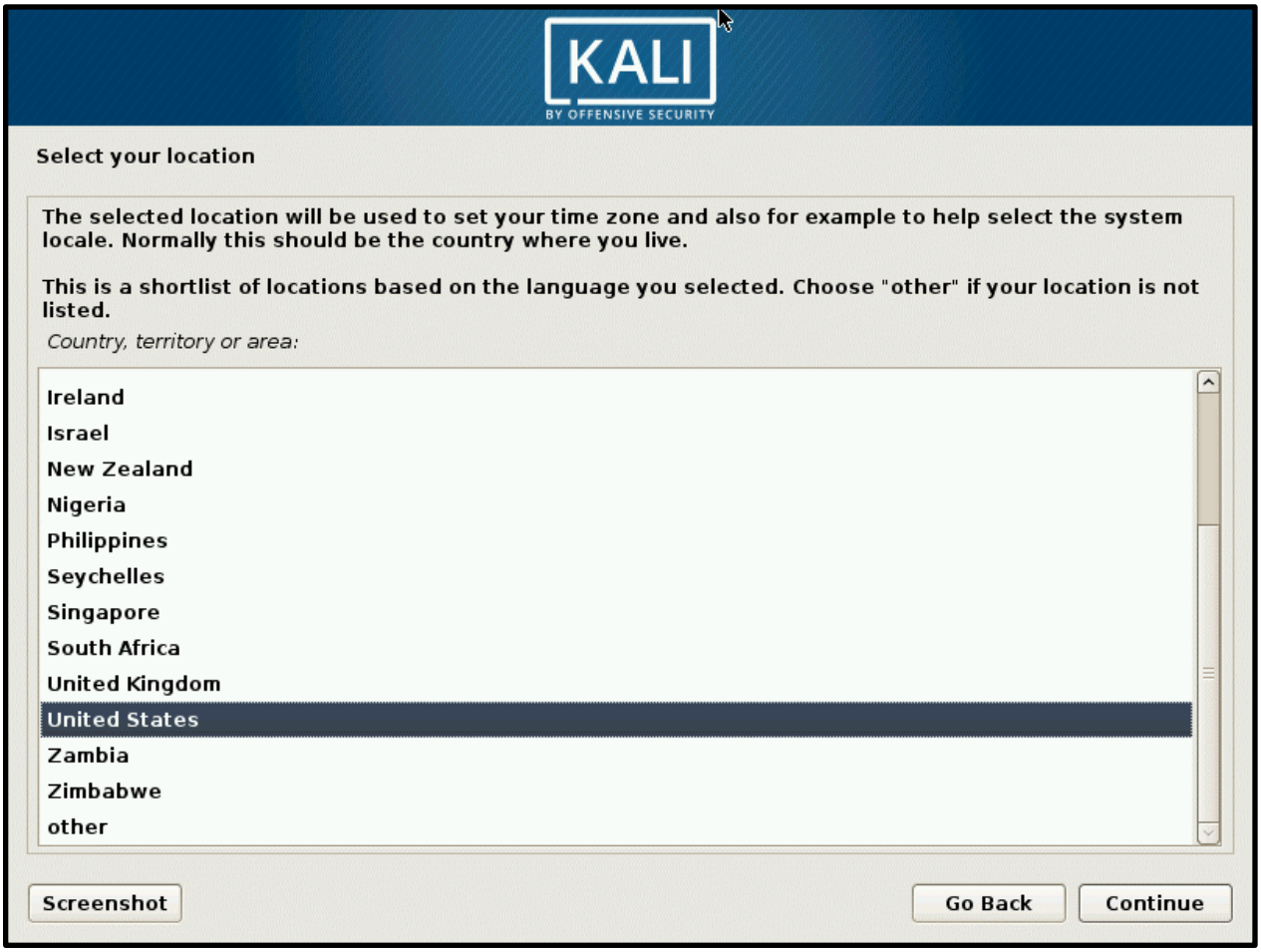


Step 10: After booting from a **virtual DVD,** you will see a boot menu where you can select boot options for Kali Linux such as *Boot from Live DVD*, *Install, Graphical Install* etc. Let's select *Graphical Install*. **Press *Enter* to continue.**

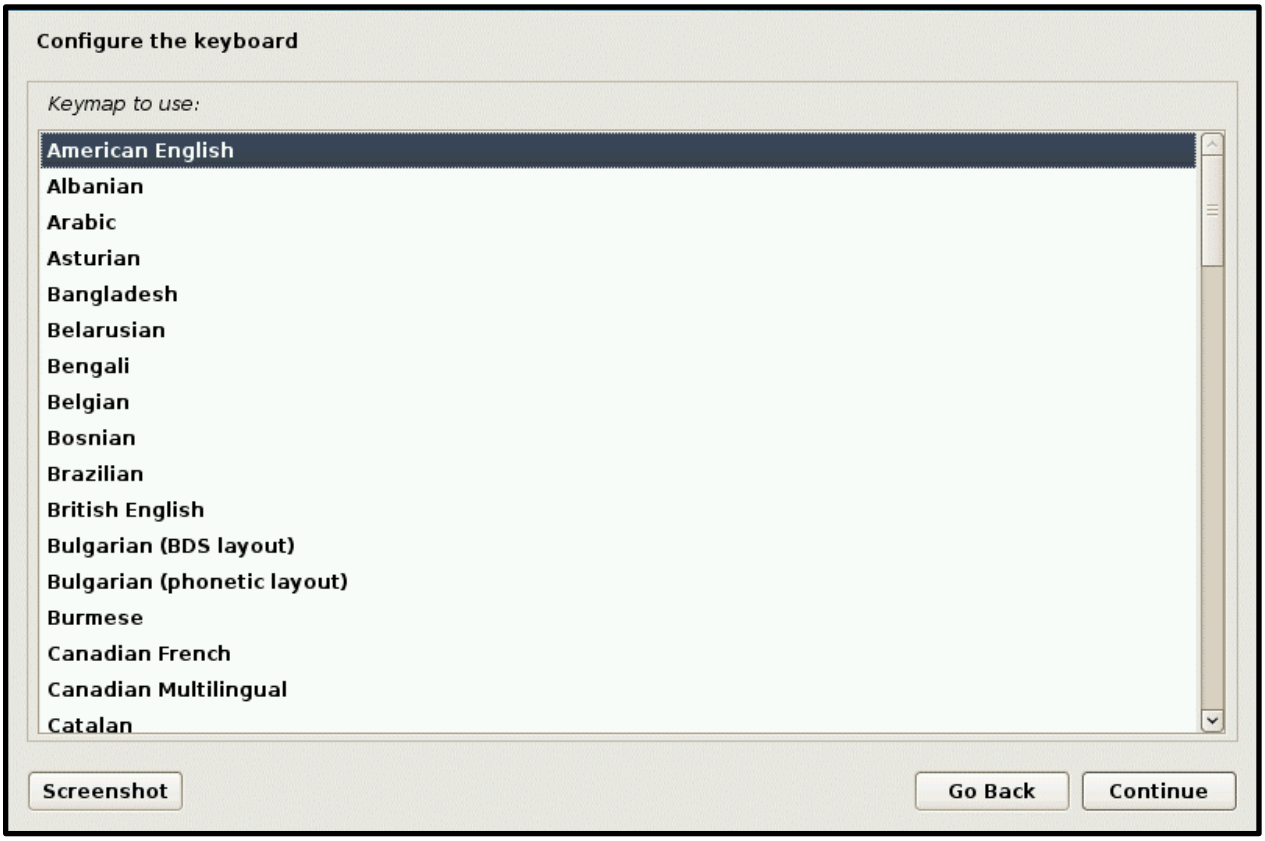
Step 11: Select a language. Choose the language you wish to use for the installation process and the installed system. **English** is selected for the current installation**. Click the *Continue* button on each screen to move forward.**



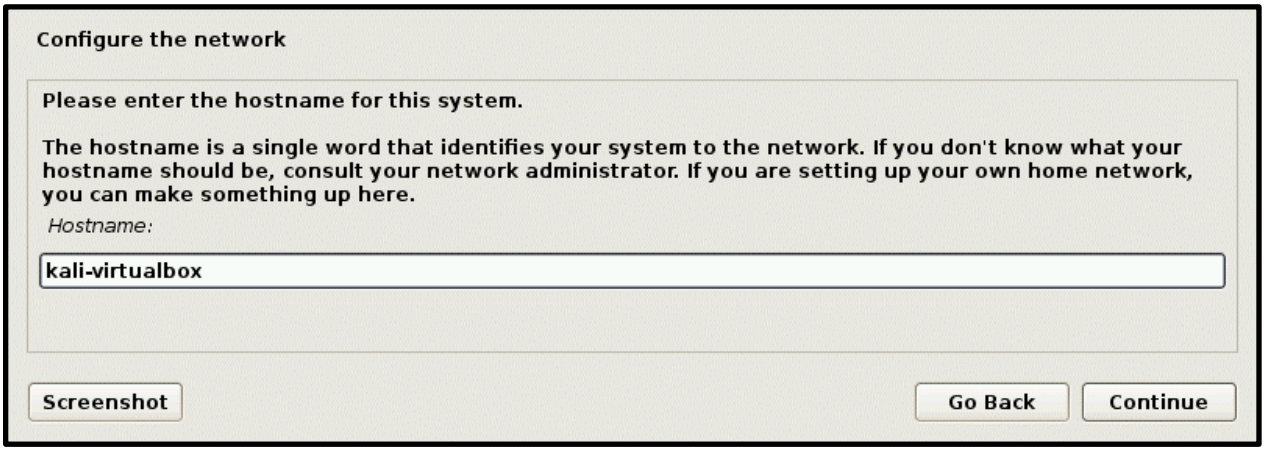
Step 12: Select your location. This option is used to set your time zone, time format, etc. **United States** has been selected in the current example.



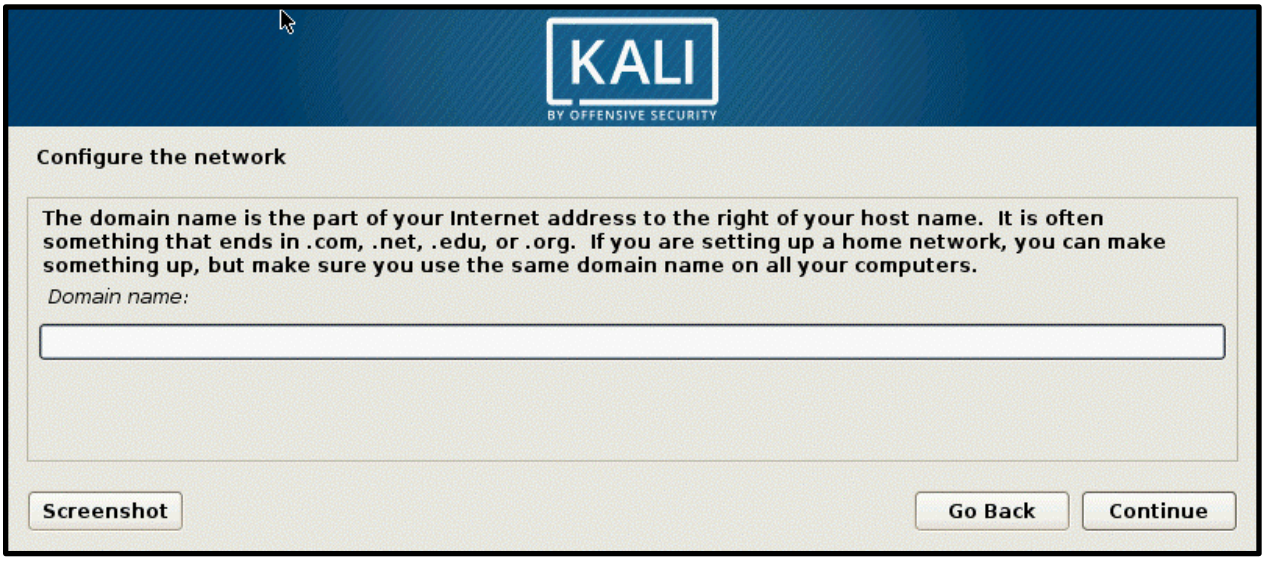
Step 13: Configure the keyboard. Select your keyboard layout. **American English** is used for the current installation.



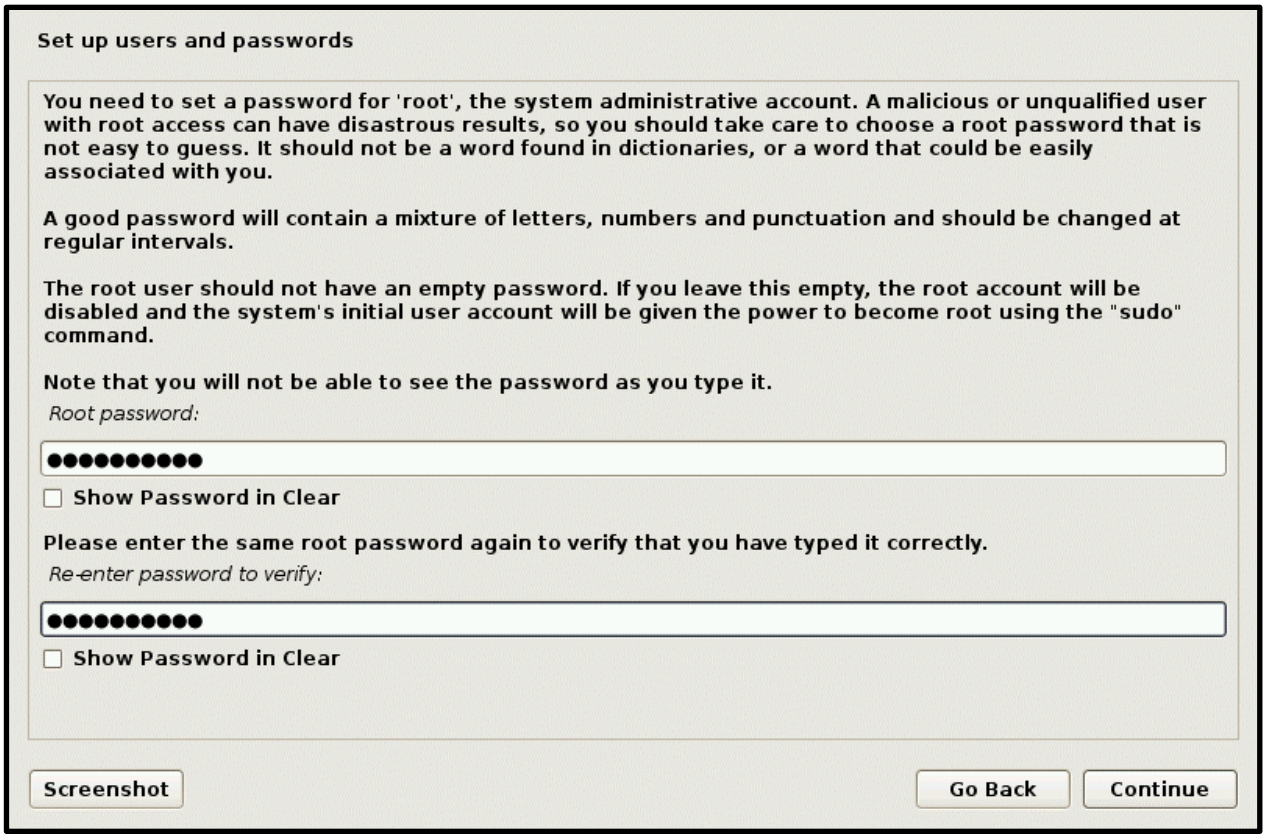
Step 14: Configure the network. Enter the hostname for your **Linux system,** for example, ***kali-virtualbox*.**



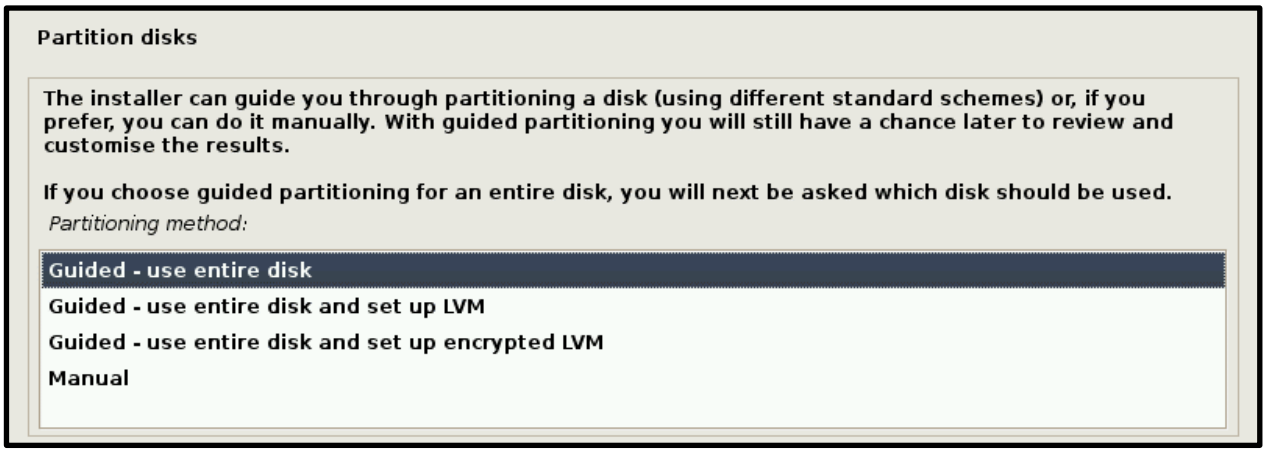
Step 15: Configure the domain name. If you don't use a domain in your network, you may leave this field empty.



Step 16: Set up users and passwords. Read the useful tips on this screen and enter the password for **root.**

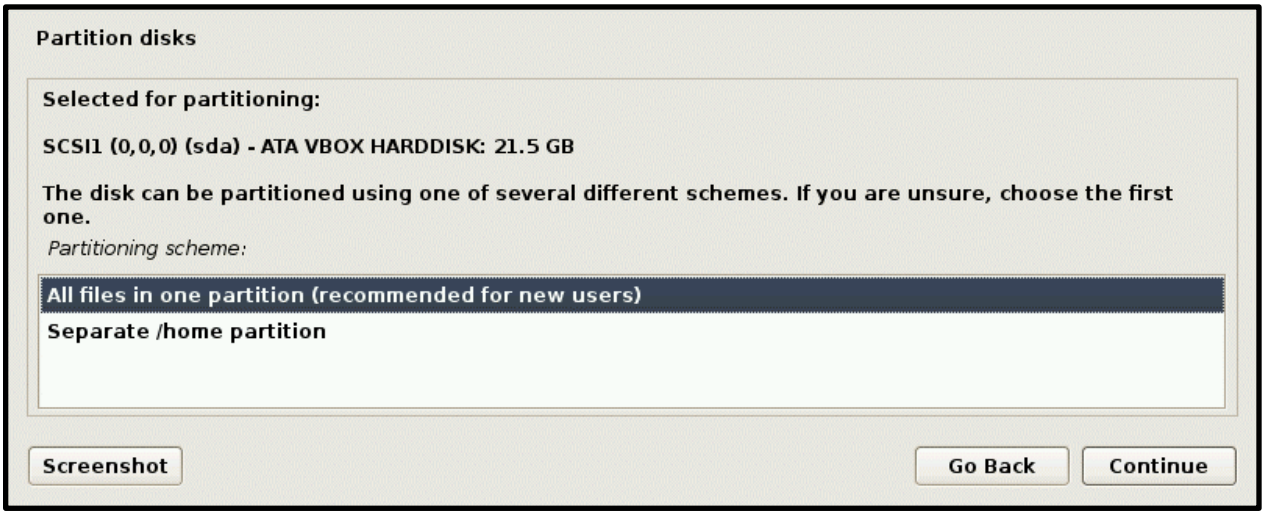


Step 17: Partition disks. You can use manual and guided partitioning of disks. For the first time, you can select *Guided* ***– use entire disk.*** The entire disk will be used for creating one big partition.

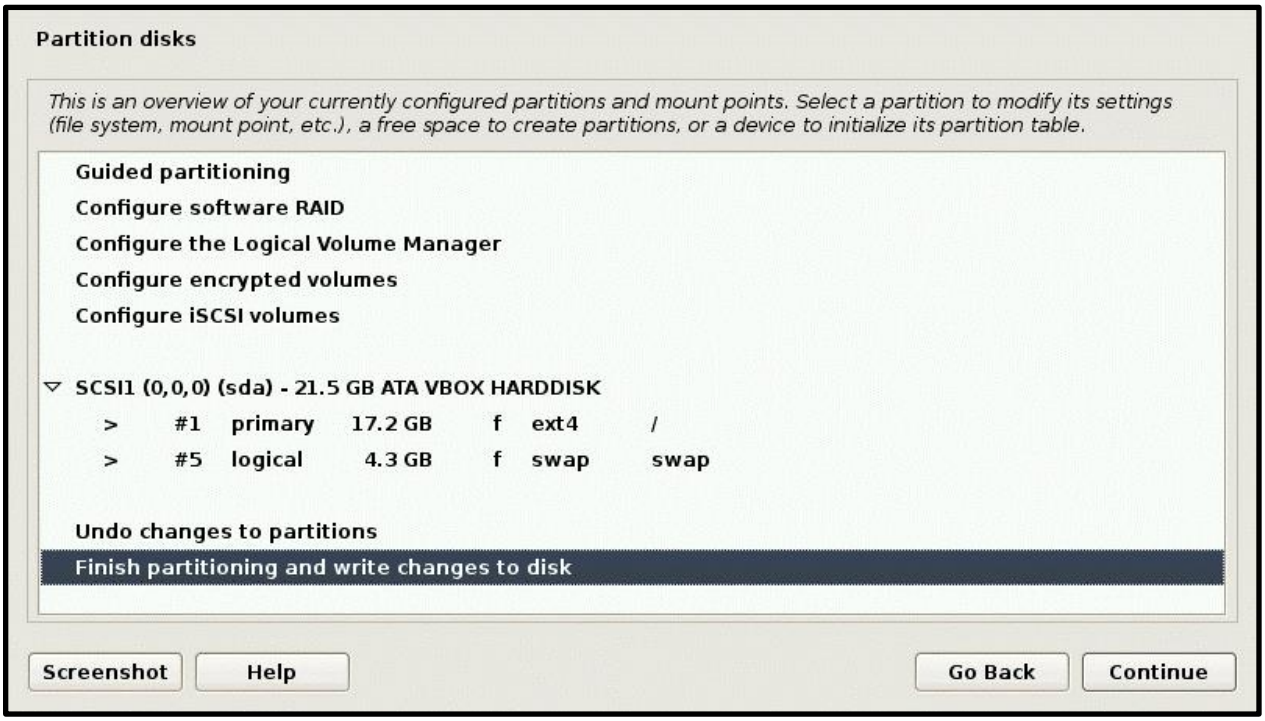


Step 18: Confirm that you want to erase the disk. There is no reason to worry, as in this case, the empty **21.5-GB virtual disk** is used for partitioning.

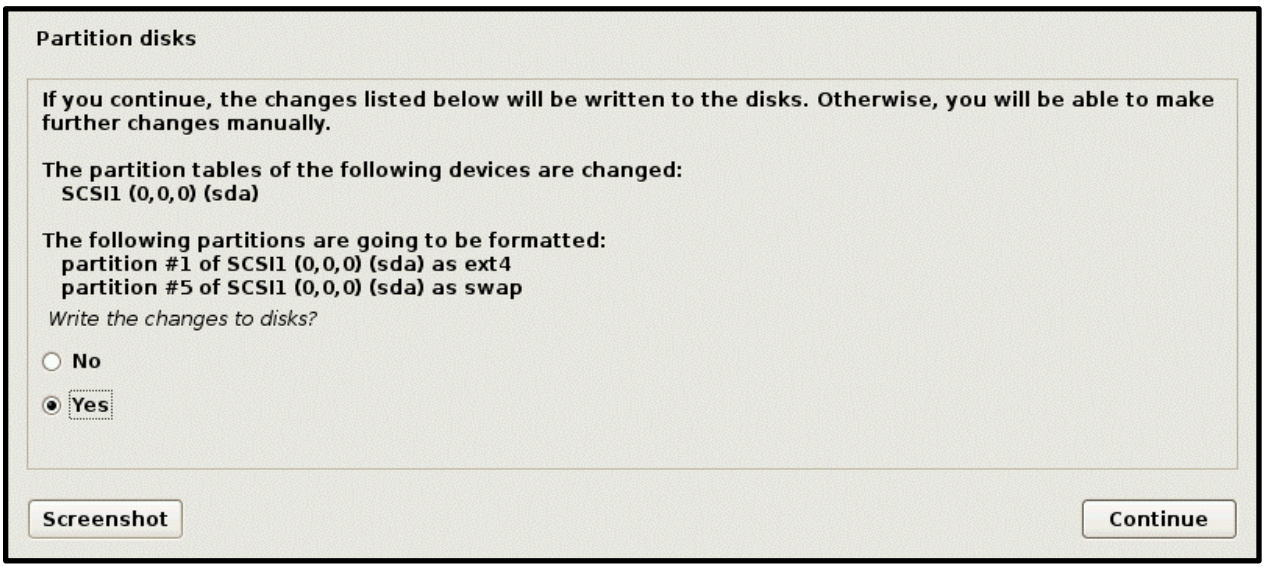
Step 19: Select a preferred **partitioning scheme** for your virtual disk. Let's select *All files in one partition*.



Step 20: Check the overview and **select *Finish partitioning*** *and write changes to disk*.

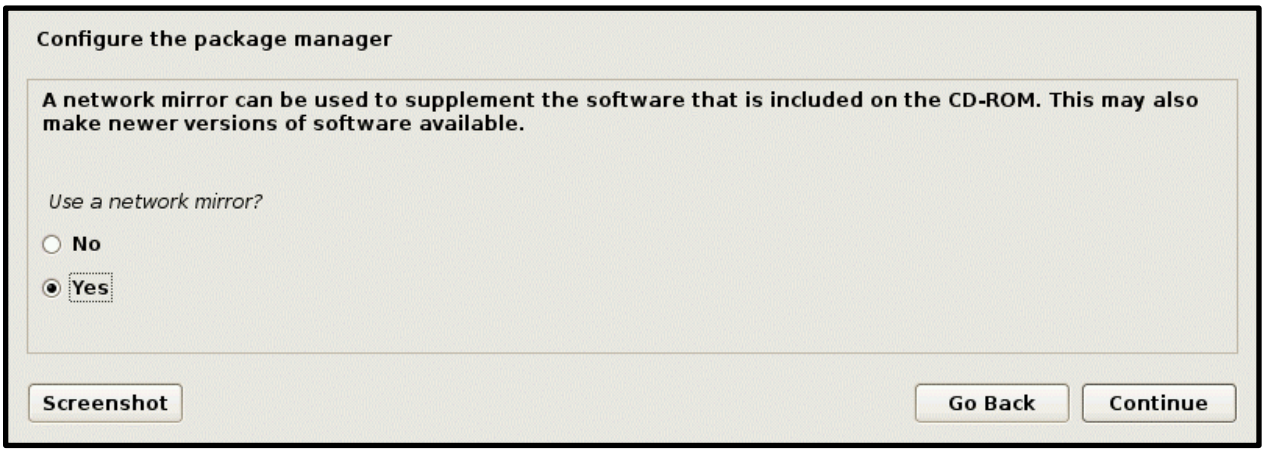


Step 21: Select *Yes* and confirm that you would like to write changes to the disk**.**

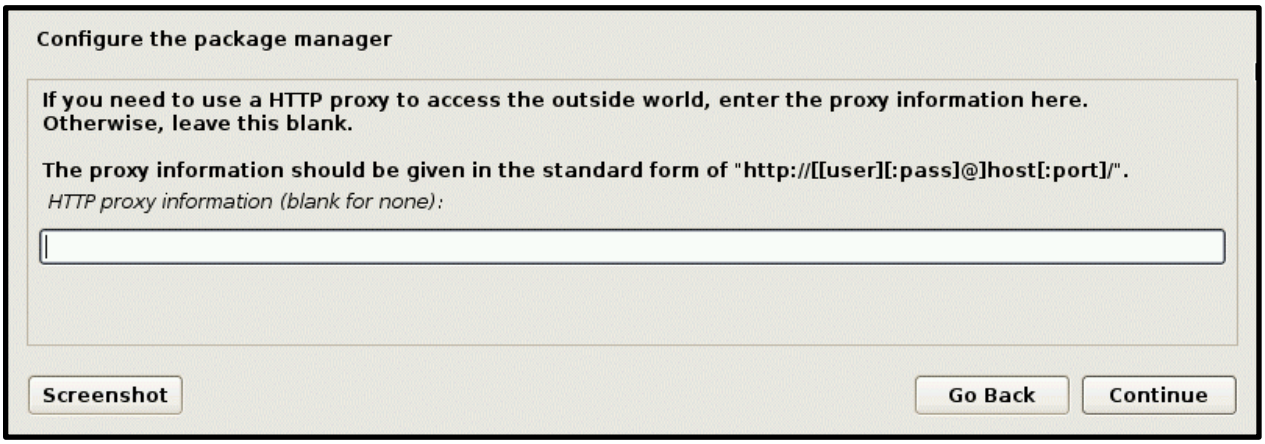


Step 22: Wait for the system to be installed. As **Kali Linux is being installed,** the files are being copied to the virtual disk of the VM.

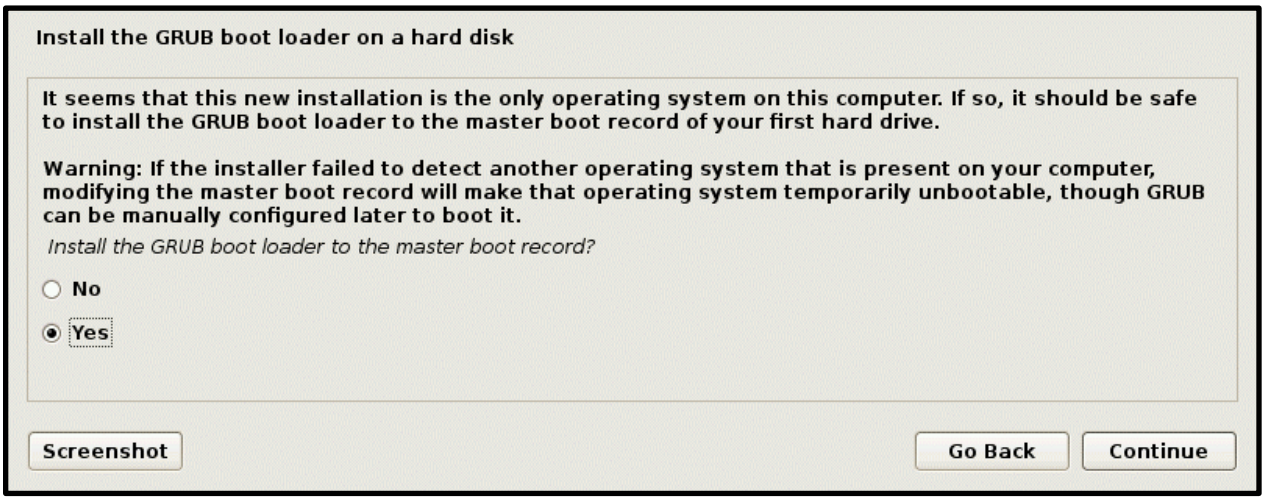
Step 23: Configure the package manager. Click *Yes* if you would like to use a **network mirror.** Selecting this option will allow you to install or update application packages from online software repositories.



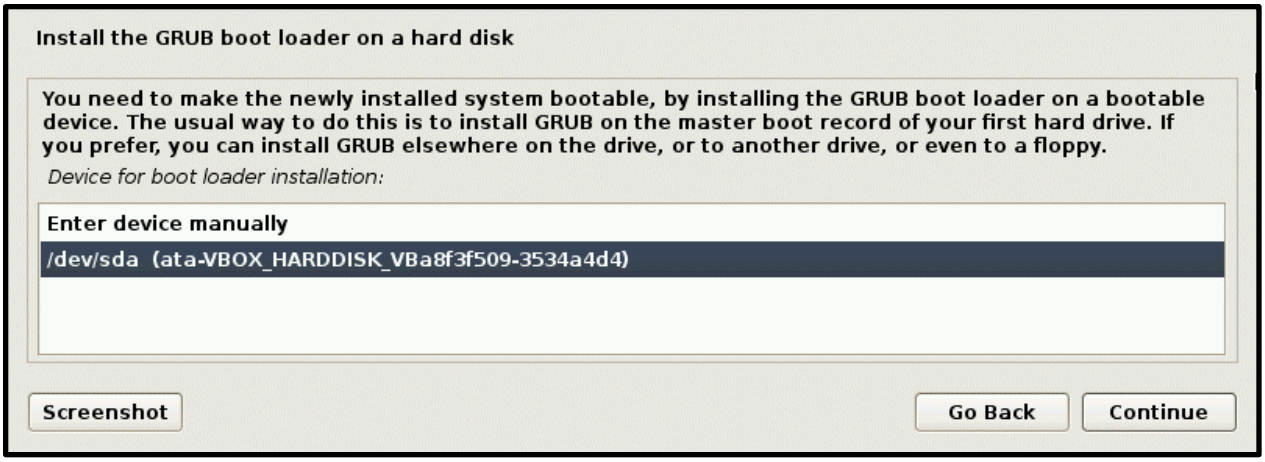
Step 24: Enter the information about your **proxy server** if you use a proxy server for internet access from your network. There is no proxy server in this example; so this field is left empty.



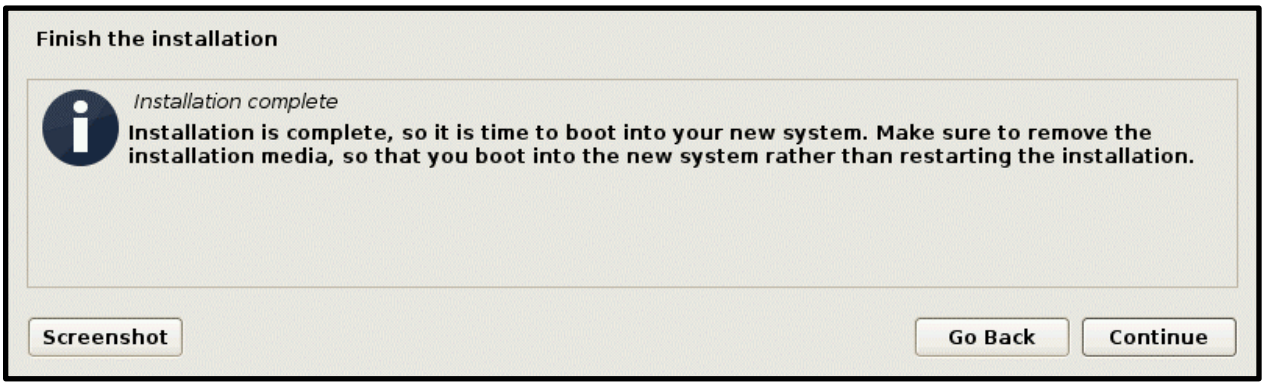
Step 25: Install the GRUB boot loader on a hard disk. Since there is no other operating systems and boot loaders on a virtual disk, it is necessary to install GRUB in this case. **Select *Yes* to install GRUB.**



Step 26: Select a disk to which GRUB must be installed. In this case**, */dev/sda*** is the necessary disk and is the only disk connected to a VM.



Step 27: Finish the installation. When the installation of Kali Linux on VirtualBox is complete, you will see a notification message. Now you can **reboot the virtual machine** to boot the Kali Linux installed on the **VirtualBox VM.**



Step 28: After the reboot, you will see a login screen of **Kali Linux.** Enter **root** as a **username**, then enter the **password** set during installing Kali Linux on **VirtualBox** to sign in.

Step 29: Now you should see the **Gnome Desktop** of **Kali Linux** installed on your **VirtualBox.**

Kali Linux Basic Commands

Kali Linux command is a powerful **penetration testing** distribution by **offensive security**. It is available in **32-bit**, **64-bi**t and ARM flavors. With the help of the Kali Linux features, we can easily create custom complex images. Kali Linux offers various certifications such as **OSCP, OSWE, OSEP, OSWP, OSEE, and KLCP.**

The testing tools of the Kali Linux commands can be categorized into i**nformation gathering**, **password attacks**, **vulnerability assessment**, **web applications**, **exploitation tools**, **sniffing and spoofing**, **maintaining access**, **system services and reporting tools**.

Kali Linux comprises various tools that can be used for **wireless attacks**, **hardware hacking, forensics, stress testing,** and **reverse engineering.** A **USB disk**, **hard disk**, or **Live DVD** can be used to install it. Network services are **HTTP, MYSQL**, and **SSH**. These are quite useful when using the **Kali Linux commands.**

Kali Linux operates on some android devices. Its predecessor is **Backtrack** which was carried over to Kali via **Live Boot**. The system becomes easy to use once the users get command over it.

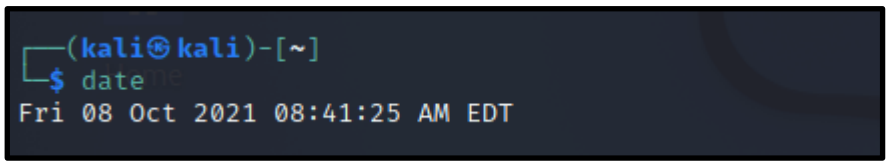
Kali Linux Basic Commands

The following is the list of Kali Linux basic commands:

1. Date Command
2. Cal Command
3. Cd command
4. Cp command
5. Whoami Command
6. Ls command
7. cat command
8. mkdir command
9. rm command
10. mv command
11. Uname command
12. Uptime command
13. Users Command
14. Less command
15. More command
16. Vi Command
17. Free Command
18. Sort Command
19. History Command
20. Pwd Command

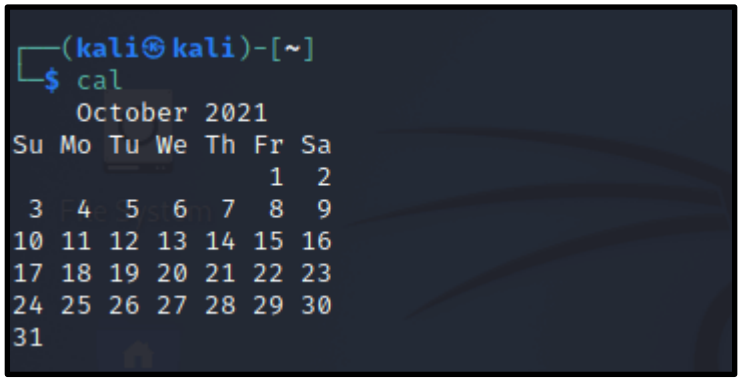
1. Date Command

In Kali Linux, the **'date'** command is used to display the system date and time. In order to display the date, we have to use the following command:



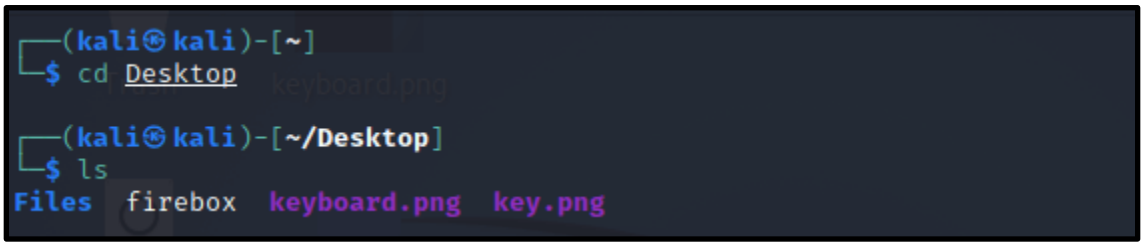
2. Cal Command

The **cal** command displays the current month's formatted calendar on our terminal screen. If we require a more advanced version of **'cal'** we can install the ncal package on our Linux machine, which displays the calendar vertically and provides additional options.



3. Cd Command

The **'cd'** command is also called chdir (Change Directory). We used this command to change or switch the current working directory.



4. cp Command

In Kali Linux, the **'cp'** command is used to copy files or a group of files or directories that create an exact image of a file on a disk with a different file name.

```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
Files  firebox  keyboard.png  key.png

┌──(kali㉿kali)-[~/Desktop]
└─$ cp key.png files
```

5. whoami Command

The **'whoami'** command is used to print the effective user ID whereas the who command prints information regarding users who are presently logged in.

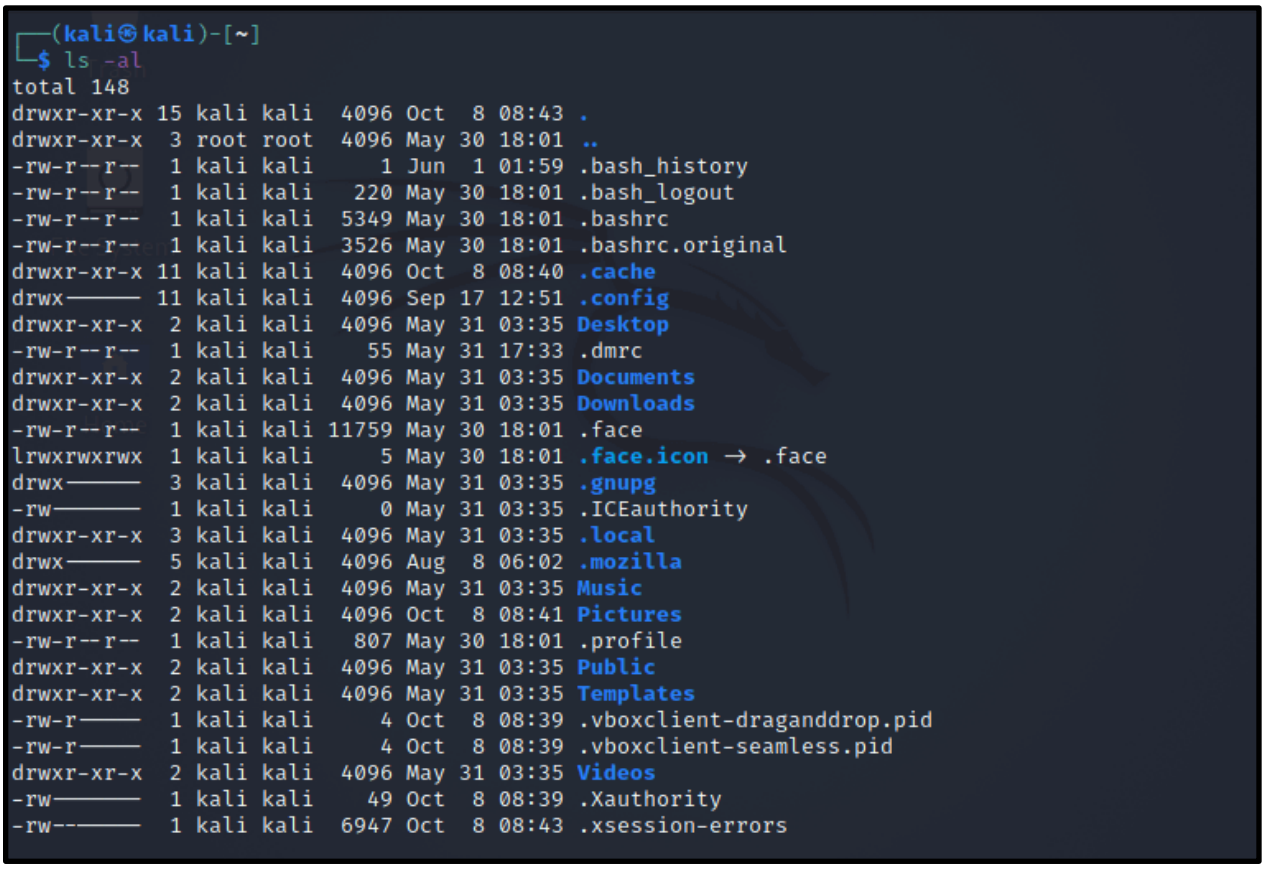
The **"w"** command can also be used to view who is logged on and what they are doing.

```
┌──(kali㉿kali)-[~]
└─$ whoami
kali

┌──(kali㉿kali)-[~]
└─$ who
kali     tty7         2021-10-08 08:39 (:0)
```

6. Ls Command

One of the most useful commands in Kali Linux is the **'ls'** command. The ls command lists the directory contents of files and directories. With the help of the ls command, we can easily list out every hidden file of a directory with the **-a** attribute, and for more detailed output, we can use the **-l** attribute.



7. Cat Command

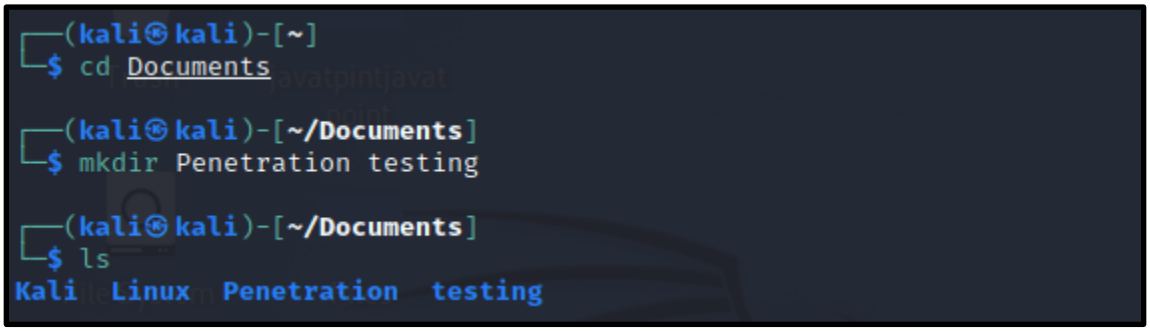
The **'cat'** (concatenate) command is one of Kali Linux's most commonly used commands, permitting us to create single or many files, concatenate files and redirect, view contain of file output in terminal or files.

Usually, we use the cat command to display the content of a file.

8. mkdir Command

The **'mkdir'** command is used to create directories. For example, if we wish to create a directory named 'Penetration testing' under the 'Documents' directory, then we have to open a terminal and enter the below command:

1. cd Documents
2. mkdir Penetration testing



9. rm Command

In Kali Linux, the **'rm'** command is used to delete files. It can be used to delete directories when we use them recursively.

The removal process separates a file name from its associated data in a file system and identifies that space in the storage device as available for future writes. In other words, when we erase a file. the data inside it remains unchanged, but it is no longer linked to a filename.

```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ cd Files

┌──(kali㉿kali)-[~/Desktop/Files]
└─$ ls
image1.png  java.png  pics.png  picture.png  pp.png  screen.png

┌──(kali㉿kali)-[~/Desktop/Files]
└─$ rm pics.png

┌──(kali㉿kali)-[~/Desktop/Files]
└─$ ls
image1.png  java.png  picture.png  pp.png  screen.png
```

10. mv Command

With the help of the **'mv'** command, we can move or rename files and directories on our file system.

```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
files  Files  firebox  keyboard.png

┌──(kali㉿kali)-[~/Desktop]
└─$ mv keyboard.png Files

┌──(kali㉿kali)-[~/Desktop]
└─$ cd Files

┌──(kali㉿kali)-[~/Desktop/Files]
└─$ ls
image1.png  java.png  keyboard.png  key.png  picture.png  pp.png  screen.png
```

11. uname Command

The **'uname'** command displays the current system's information. We can view system information about our Linux environment with the **uname** command in Linux. With the **uname -a** command, we can learn more about our system, including Kernel Name, Node Name, Kernel Release, Kernel Version, Hardware Platform, Processor, and Operating System.

```
┌──(kali㉿kali)-[~]
└─$ uname
Linux

┌──(kali㉿kali)-[~]
└─$ uname -a
Linux kali 5.10.0-kali7-686-pae #1 SMP Debian 5.10.28-1kali1 (2021-04-12) i686 GNU/Linux

┌──(kali㉿kali)-[~]
└─$ users
kali
```

12. uptime Command

The **'uptime'** command displays the amount of time the system has been running. Uptime's basic usage is simple: simply type the name of the command and click Enter.

Use the -p command-line option if we merely want to know how long the system has been up for and in a more human-readable format.

```
┌──(kali㉿kali)-[~]
└─$ uptime
 09:34:53 up 57 min,  1 user,  load average: 0.29, 0.18, 0.16
```

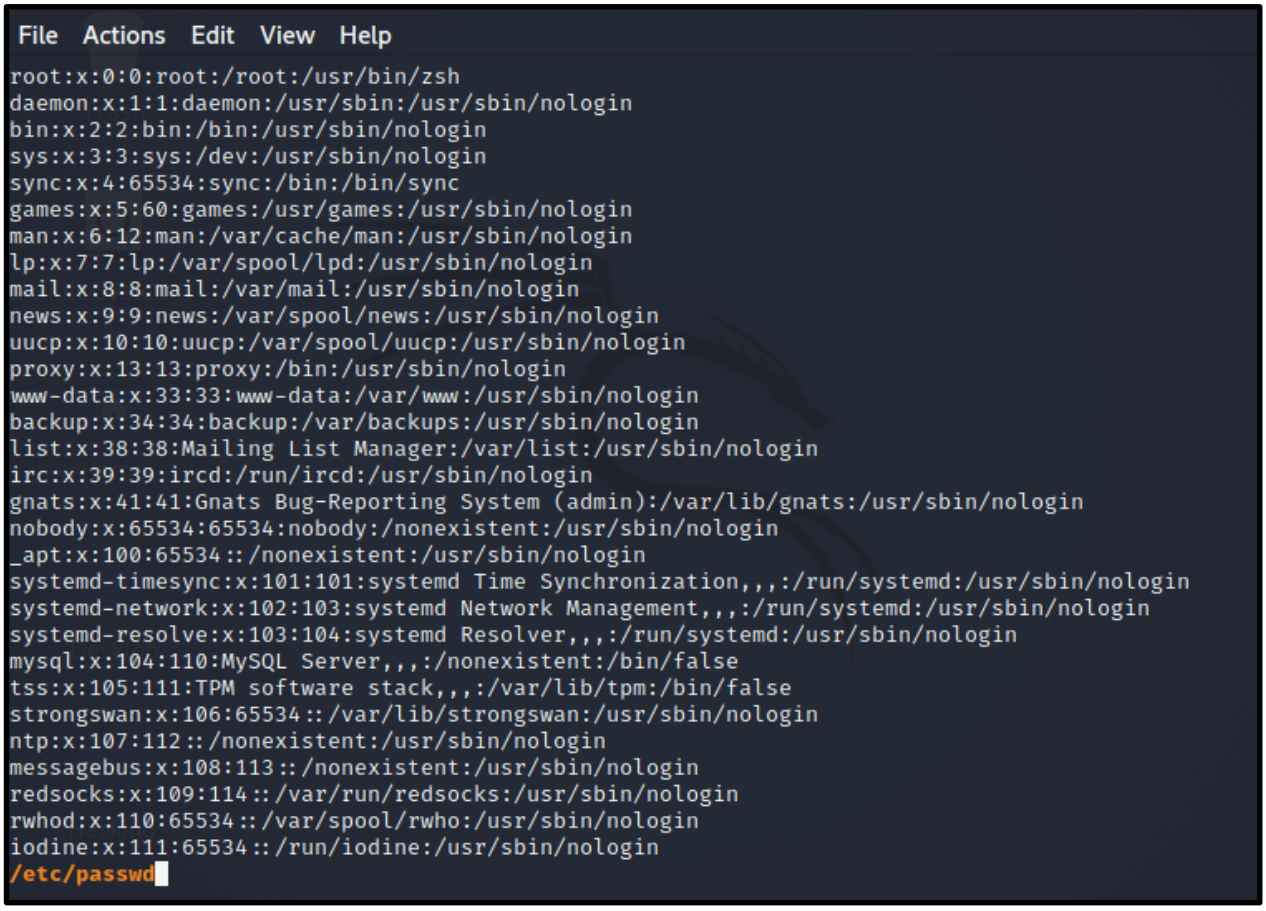
13. users Command

The **'users'** command is used to display the login names of users logged in on the system.

```
┌──(kali㉿kali)-[~]
└─$ users
kali
```

14. less Command

In Kali Linux, the **'less'** command is used to view files instead of opening the file. The **less** command is a more powerful variant of the **"more"** command which is used to show information one page at a time to the terminal.



We can view any text file with the help of the **"less"** command simply by typing the following command into a terminal window:

15. more Command

The **"more"** command permits us to show output in the terminal one page at a time. This is particularly beneficial when using a command that requires a lot of scrolling, such as the **'ls'** command or the **'du'** commands.

The **'more'** command works with any applications that output to the screen. A good way to test this is to type the following command into a terminal window:

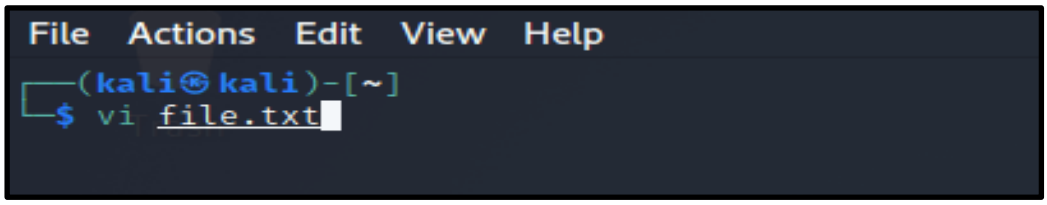
```
┌──(kali㉿kali)-[~]
└─$ more /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
tss:x:105:111:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534::/var/lib/strongswan:/usr/sbin/nologin
ntp:x:107:112::/nonexistent:/usr/sbin/nologin
messagebus:x:108:113::/nonexistent:/usr/sbin/nologin
redsocks:x:109:114::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:110:65534::/var/spool/rwho:/usr/sbin/nologin
```

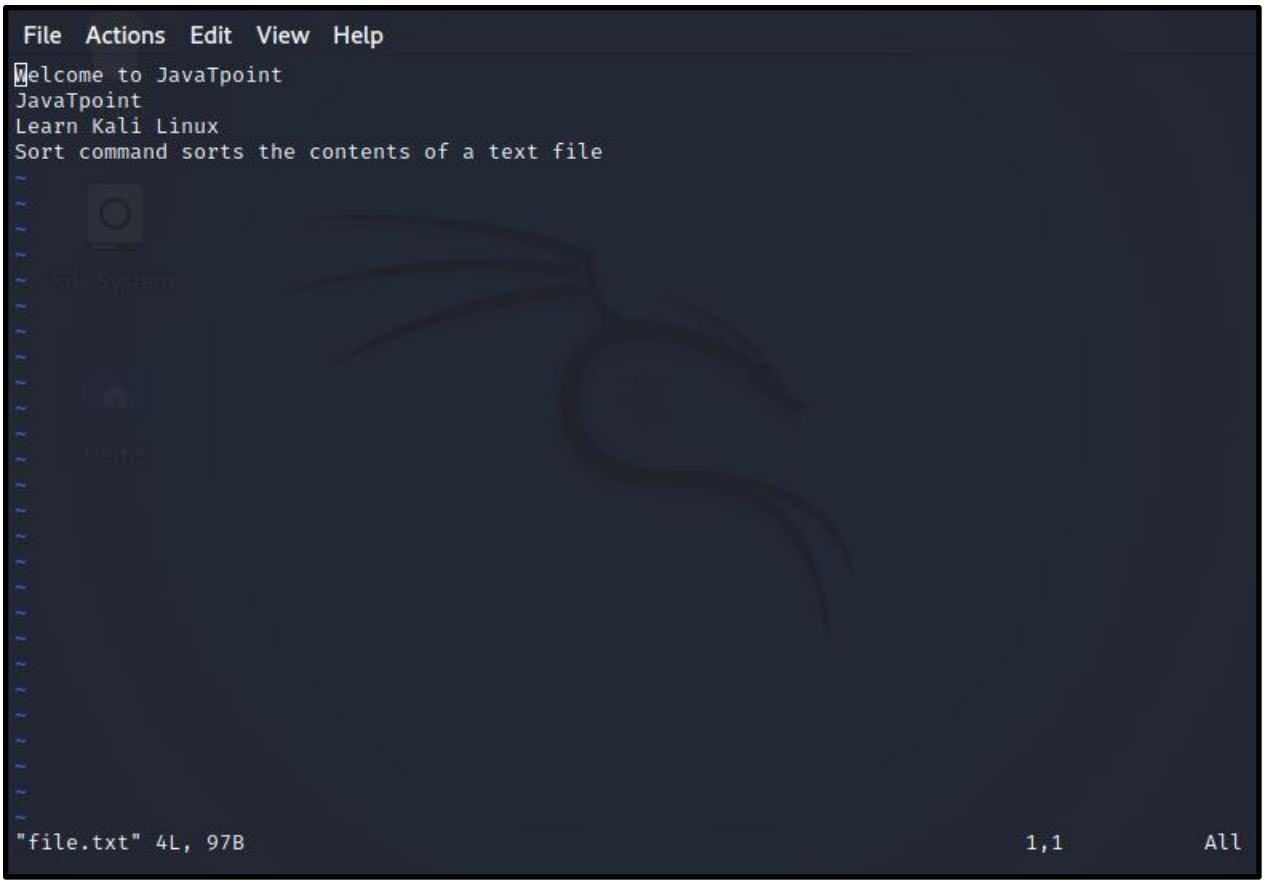
16. vi Command

The **'vi'** editor is a screen editor that comes with practically every UNIX system. The command mode and the insert mode are the two most common nodes in **vi**.

To start entering text in an empty file, we must first switch from the command mode to the insert mode. To accomplish this, start typing the letter i. When we start typing, anything then the type will be entered into the file.

Type some short lines, then press Return at the end of each. **Vi** does not use word wrap like other word processors. It will break a line at the screen's edge. If we make a mistake, we can undo it by pressing the Backspace key. If the Backspace key on our computer is not working, then try the **ctrl + h key** combination.

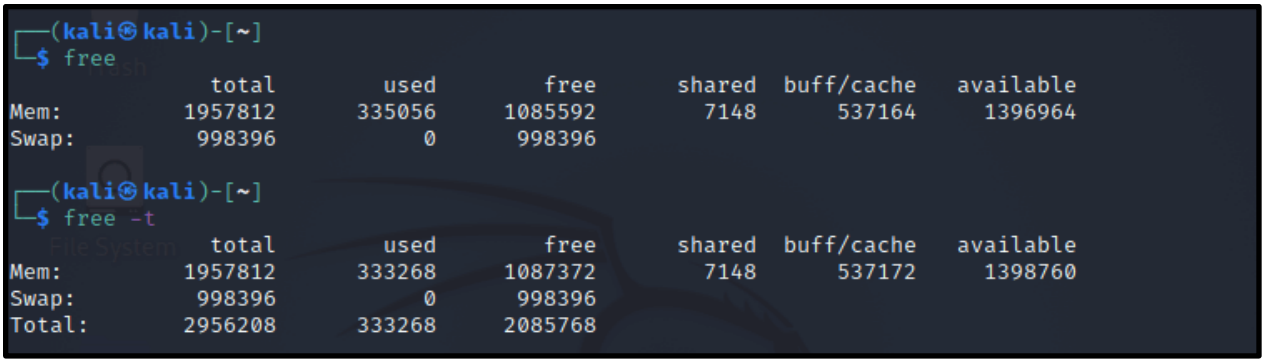




17. free Command

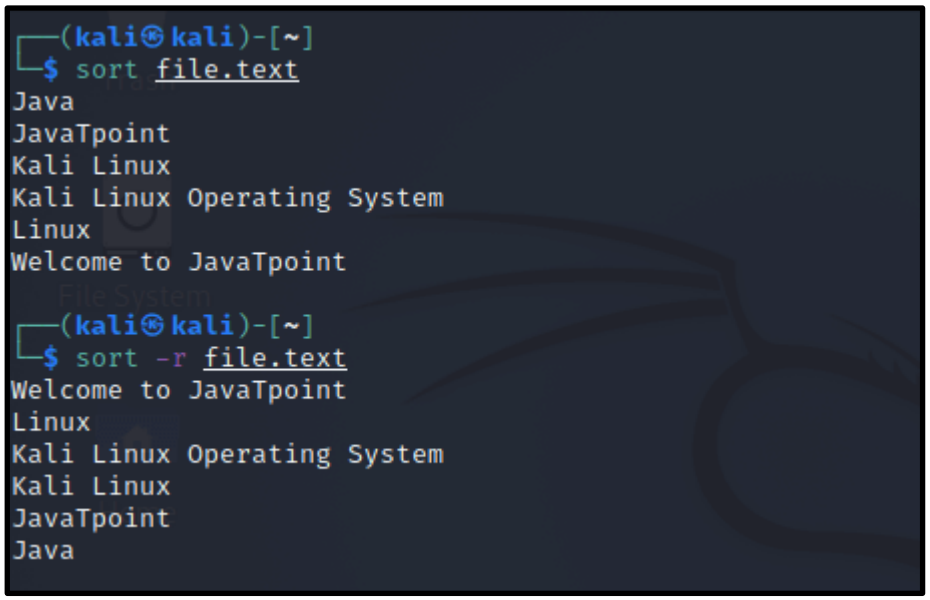
In Kali Linux, the **'free'** command provides us the useful information about the amount of RAM available on a Linux machine. It also displays the entire amount of physical memory used and available space, as well as swap memory with kernel buffers.

If we use the free command with the **-t** option, it will list the total line at the end.



18. sort Command

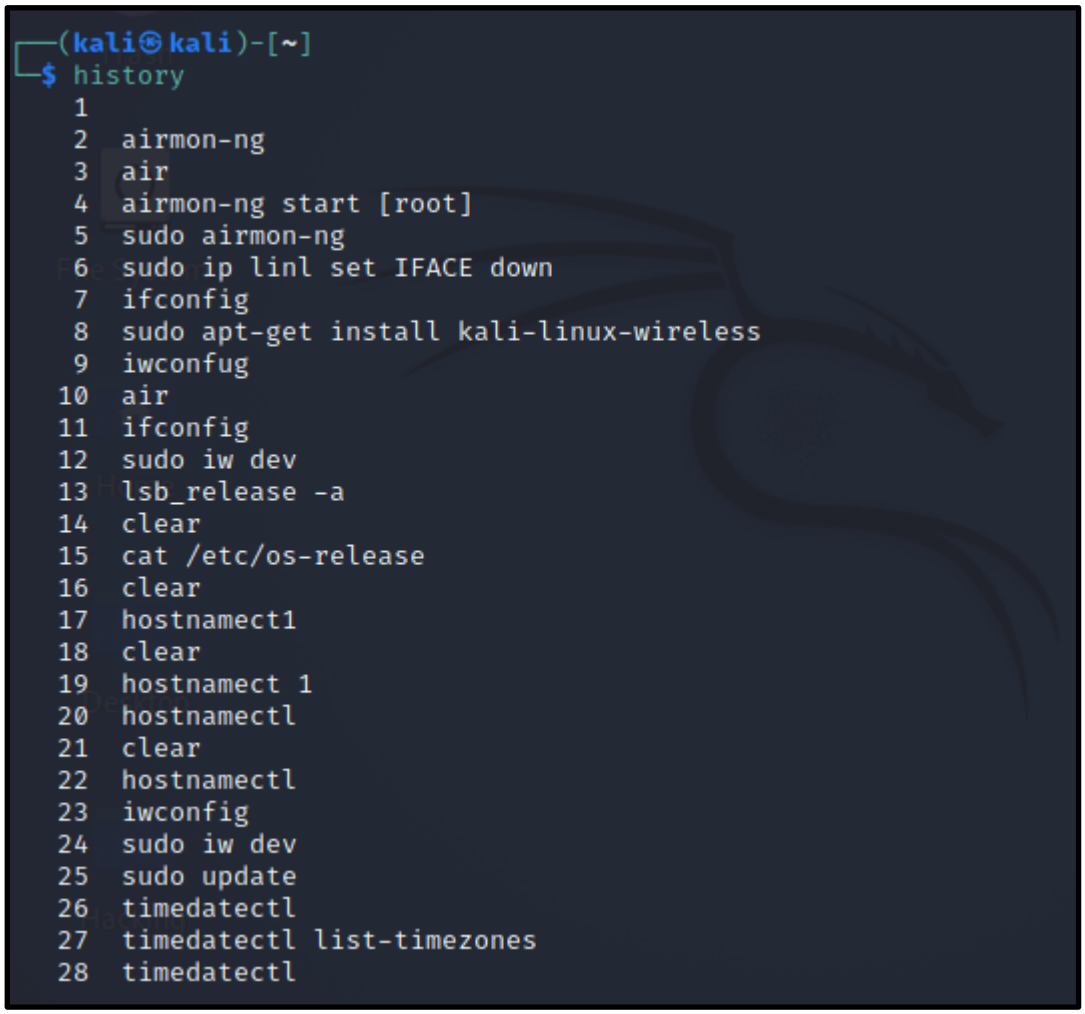
Using the **'sort'** command, we can sort the content of the text file, line by line. Sort is a standard command-line program which prints the lines of its input or concentration of all files listed in its argument list in sorted order. We can reverse the order of any file's contents by using the **-r sort.**



19. history Command

The **'history'** command is one of Kali Linux's most commonly used commands. The history command in the bash shell saves a history of commands entered that can be used to repeat commands.

We can run the history command by itself, and it will just print the current user's bash history on the screen, as shown below:



20. Pwd Command

In Kali Linux, the **'Pwd'** command is used to print working directory. It gives us information about the directory we are now in. This is especially useful if we need to access the directory while in the middle of a complicated process.

21. Sudo Su

The **'sudo'** command is useful for granting temporary privileges to users for specific tasks, without giving them full access to the root user account. This helps to secure the system by preventing users from making accidental or intentional changes to the system as the root user.

Learning Outcomes: The student should have the ability to

LO1: Understand installation of Kali on VirtualBox.

LO2: Learn the Kali Linux basic commands.

Course Outcomes: Understand the fundamental concepts of Kali Linux and its command-line interface. Demonstrate proficiency in using essential Kali Linux commands for penetration testing and security assessments. Successfully installed Kali Linux using an ISO file in VirtualBox virtualization software. Apply gained knowledge to perform basic ethical hacking tasks and security analysis using Kali Linux.

Conclusion: Installing Kali Linux on VirtualBox is not a difficult process but does include a set of crucial features that you need to know. install Kali Linux on VirtualBox as a VM manually and by using a VirtualBox VM template. Manual installation allows you to select your favorite Linux graphical user interface (GUI) as well as configure all necessary parameters such as virtual disk size, disk partitioning etc.

Now that you've understood what Kali Linux is, and for what it's used by people from different professions, let's install the operating system and learn the Kali Linux basic commands.

Correction Parameters	**Formative Assessment [40%]**	**Timely completion of Practical [40%]**	**Attendance / Learning Attitude [20%]**	
Marks Obtained				