

## PRACTICAL: 1

### AIM:

Installation of Kali Linux or Parrot Security Operating System in Virtual Box.

**THEORY: Kali Linux** is a security distribution of Linux derived from Debian and specifically designed for computer forensics and advanced penetration testing. It was developed through rewriting of Backtrack by Mati Aharoni and Devon Kearns of Offensive Security. Kali Linux contains several hundred tools that are well-designed towards various information security tasks, such as penetration testing, security research, computer forensics and reverse engineering.

Kali Linux has over 600 preinstalled penetration-testing applications to discover. Each program with its unique flexibility and use case.

Kali Linux is truly a unique operating system, as its one of the few platforms openly used by both good guys and bad guys. Security Administrators, and Black Hat Hackers both use this operating system extensively. One to detect and prevent security breaches, and the other to identify and possibly exploit security breaches. The number of tools configured and preinstalled on the operating system, make Kali Linux the Swiss Army knife in any security professional's toolbox.

### Ways to Run Kali Linux:

1. Directly on a PC, Laptop – Utilizing a Kali ISO image, Kali Linux can be installed directly onto a PC or Laptop. This method is best if you have a spare PC and are familiar with Kali Linux. Also, if you plan or doing any access point testing, installing Kali Linux directly onto Wi-Fi enabled laptop is recommended.
2. Virtualized (VMware, Hyper-V, Oracle Virtual Box, Citrix) – Kali Linux supports most known hypervisors and can be easily into the most popular ones. Pre-configured images are available for download from <https://www.kali.org/>, or an ISO can be used to install the operating system into the preferred hypervisor manually.
3. Cloud ([Amazon AWS](#), [Microsoft Azure](#)) – Given the popularity of Kali Linux, both AWS and Azure provide images for Kali Linux.

4. USB Boot Disc – Utilizing Kali Linux's ISO, a boot disc can be created to either run Kali Linux on a machine without actually installing it or for Forensic purposes.

Windows 10 (App) – Kali Linux can now natively run on Windows 10, via the Command Line. Not all features work yet as this is still in beta mode.

OUTPUT:

Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to download Kali Linux in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at <http://cdimage.kali.org/kali-weekly/>. Downloads are **rate limited to 5 concurrent connections**.

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 64-Bit (Installer)	Torrent	2020.4	4.1G	50492d761e400c2b5e22c8f253dd6f75c27e4bc84e33c2eff272476a0588fb02

Figure 1 Download window

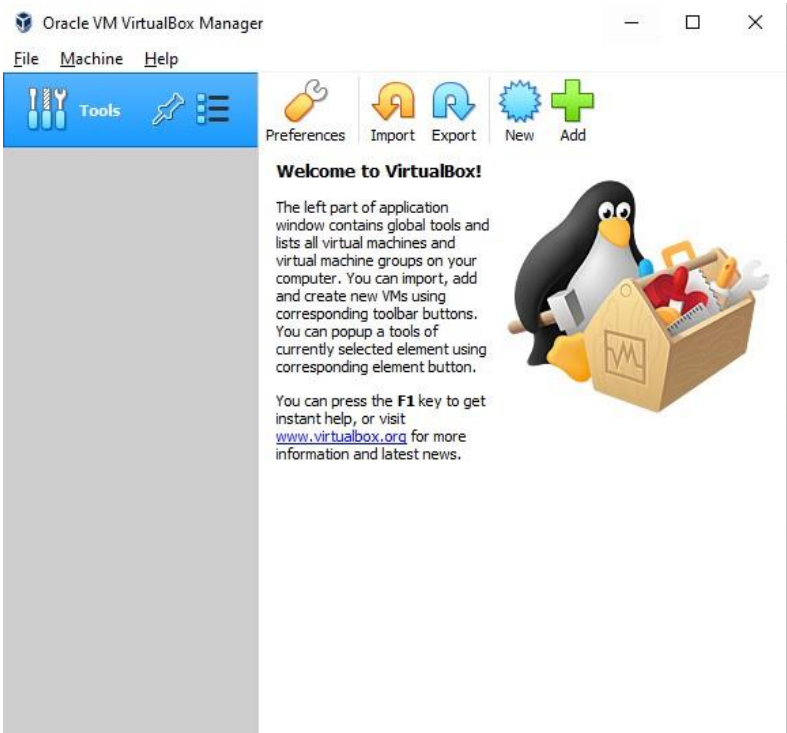
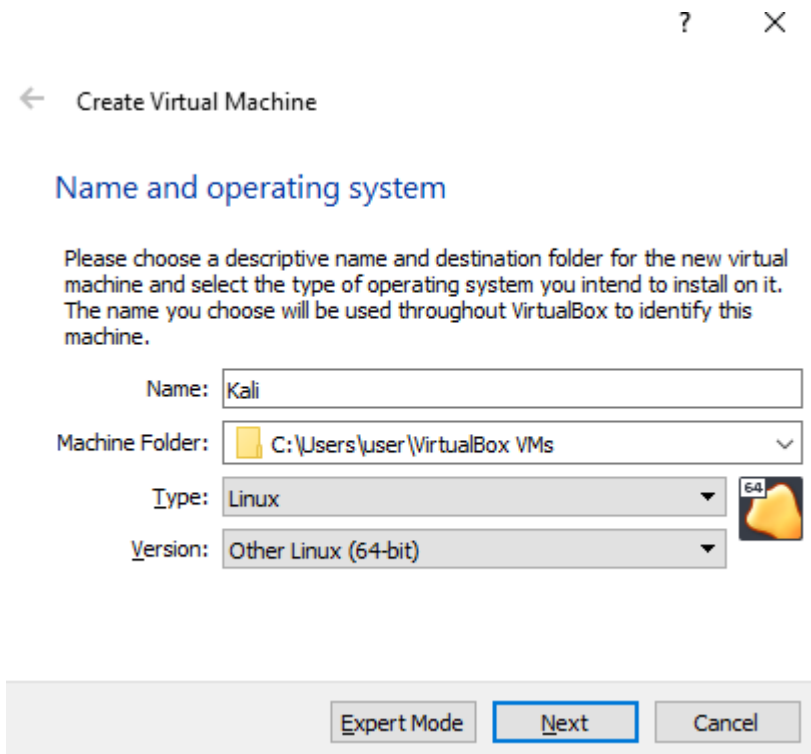


Figure 2 The VMware workstation player




← Create Virtual Machine

### Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

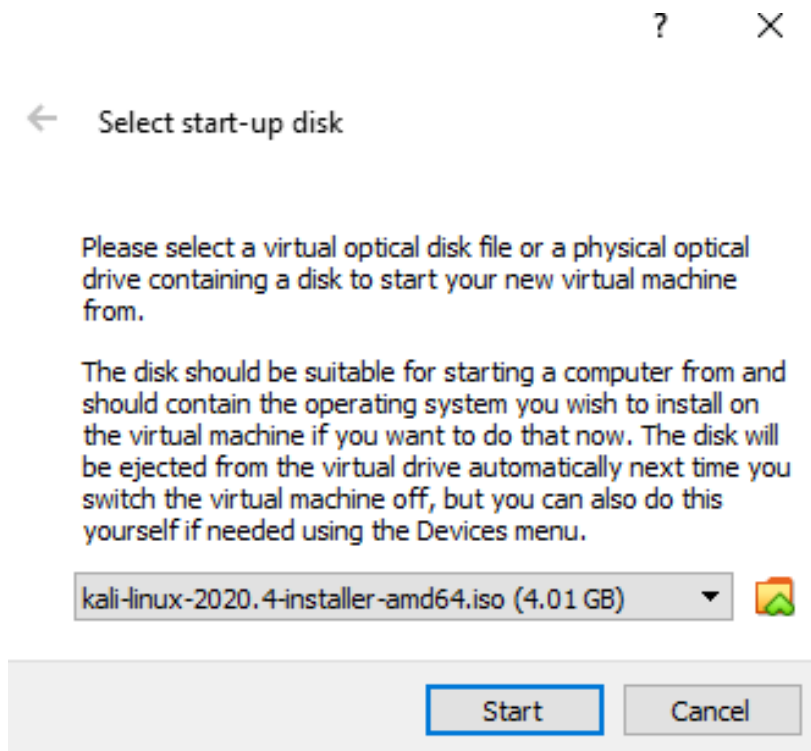
Name:

Machine Folder:

Type:  

Version:

Figure 3 Creating the new virtual machine



← Select start-up disk

Please select a virtual optical disk file or a physical optical drive containing a disk to start your new virtual machine from.

The disk should be suitable for starting a computer from and should contain the operating system you wish to install on the virtual machine if you want to do that now. The disk will be ejected from the virtual drive automatically next time you switch the virtual machine off, but you can also do this yourself if needed using the Devices menu.




Figure 4 Inserting the downloaded file to create the virtual machine

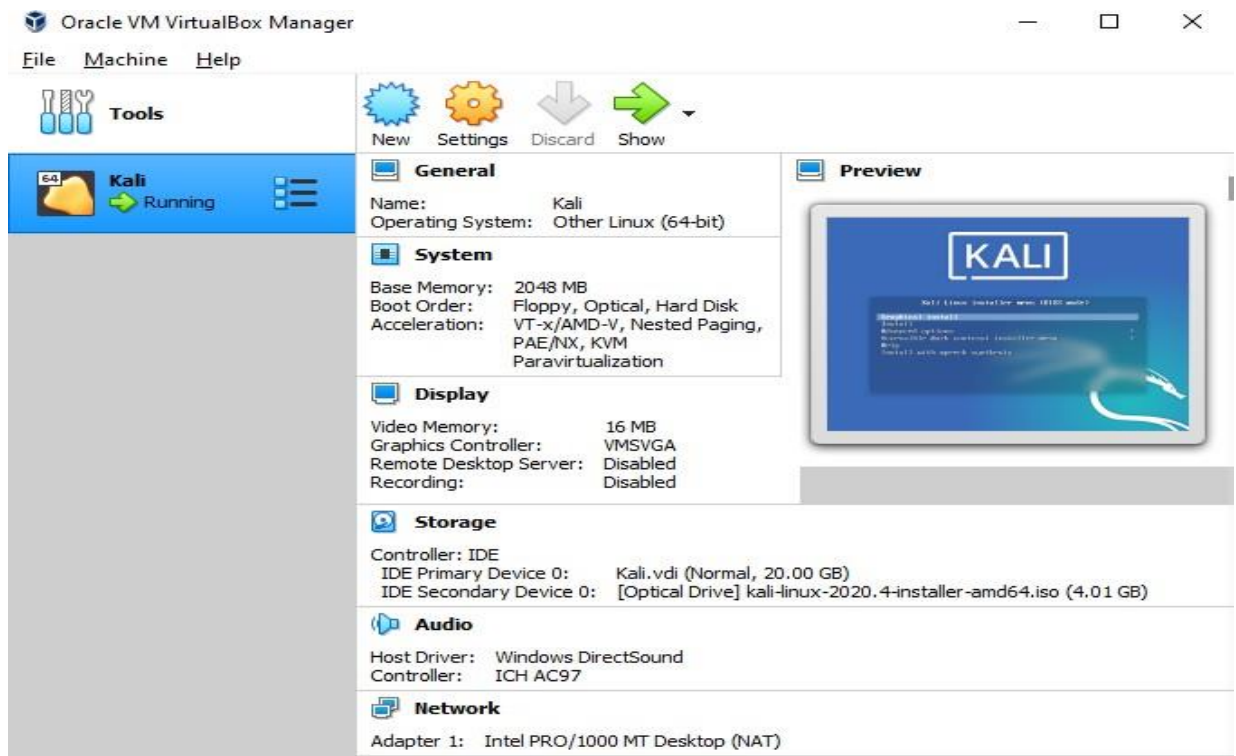


Figure 5 Created Virtual Machine



Figure 6 Installation of Kali Linux and configuring

- After the installation, we need to provide username and password which is used when we log on to the device. So that has to be done and then we proceed to the next step.

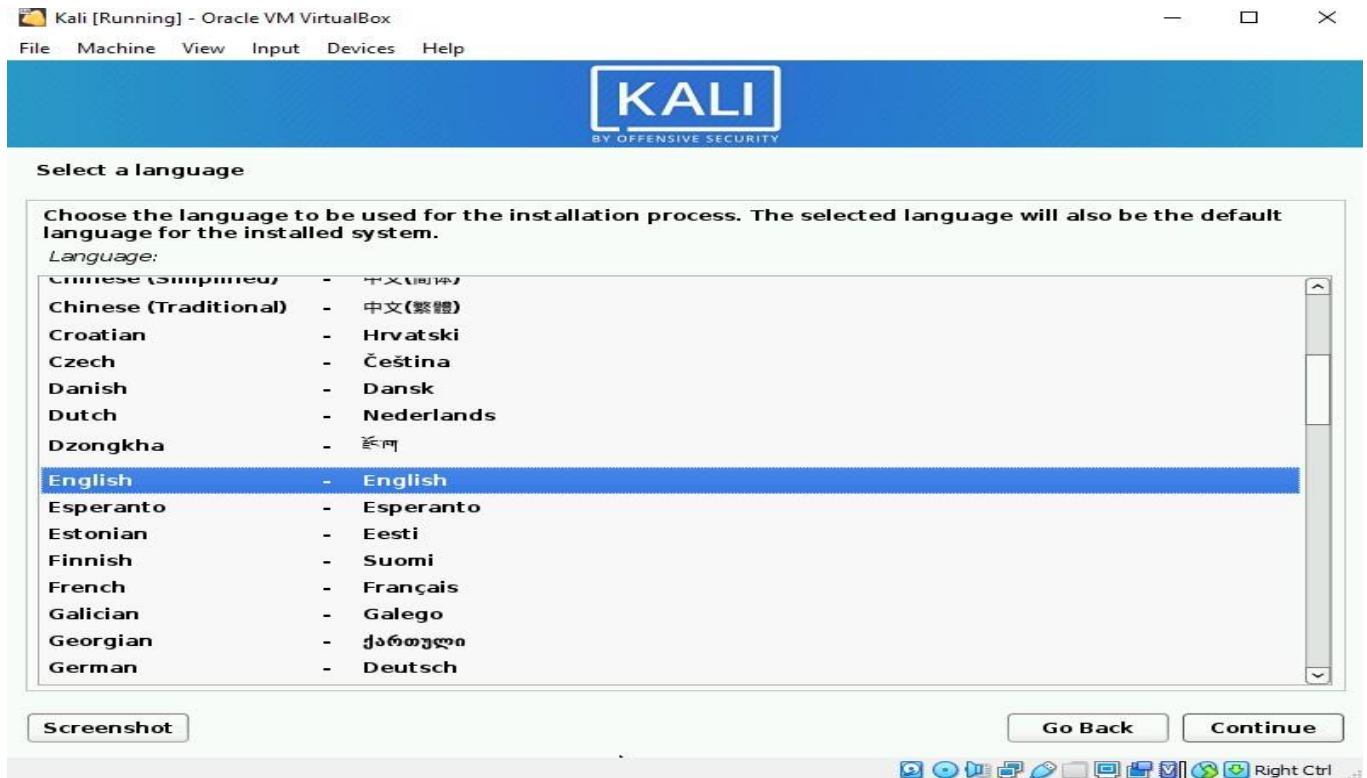


Figure 7 Selecting Language

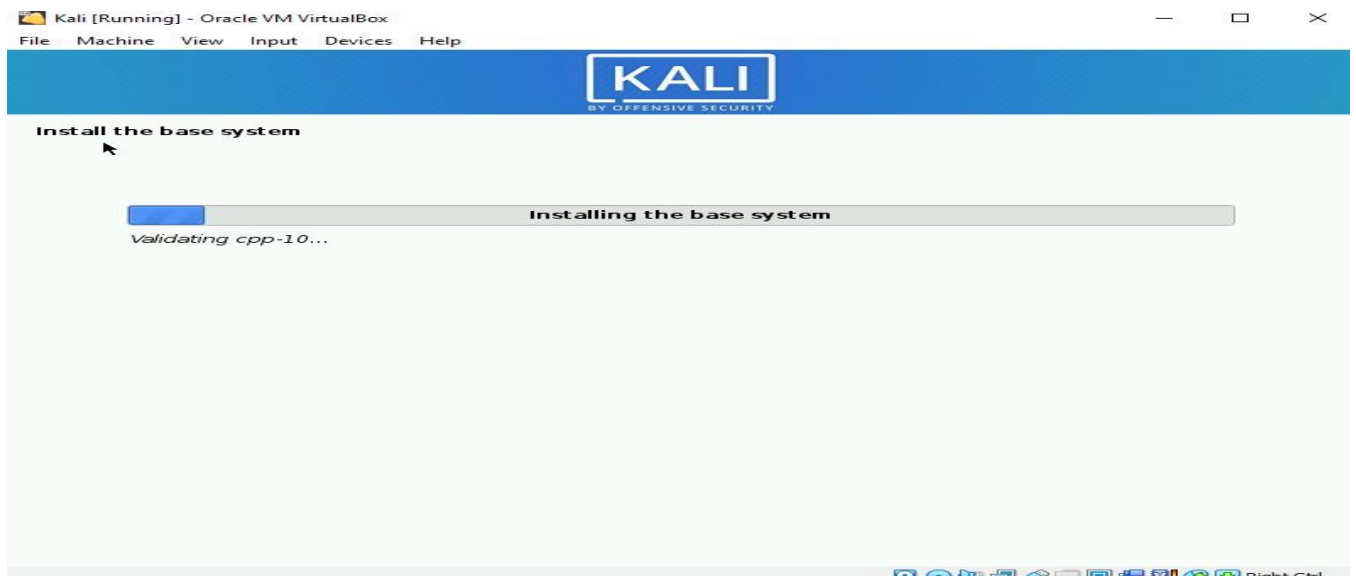


Figure 8 Installing the base system

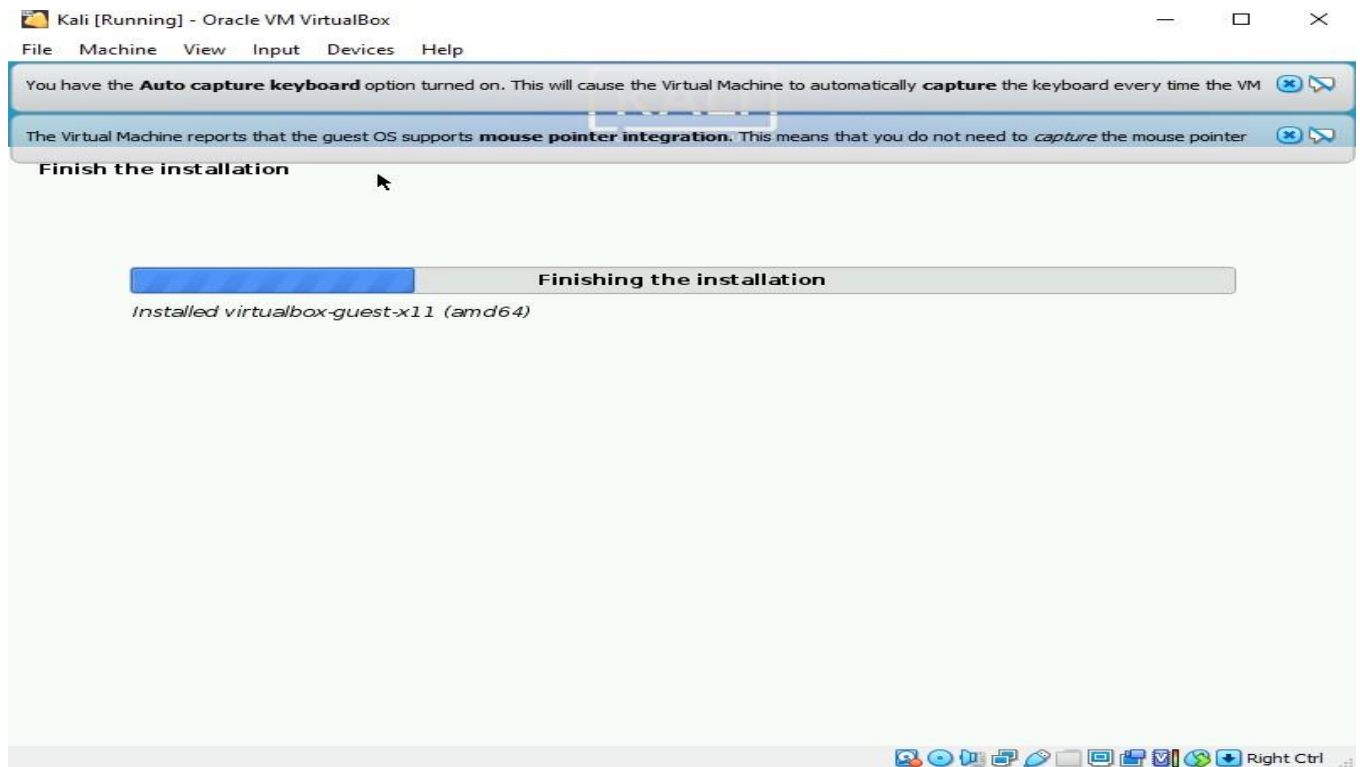


Figure 9 After installation finishing

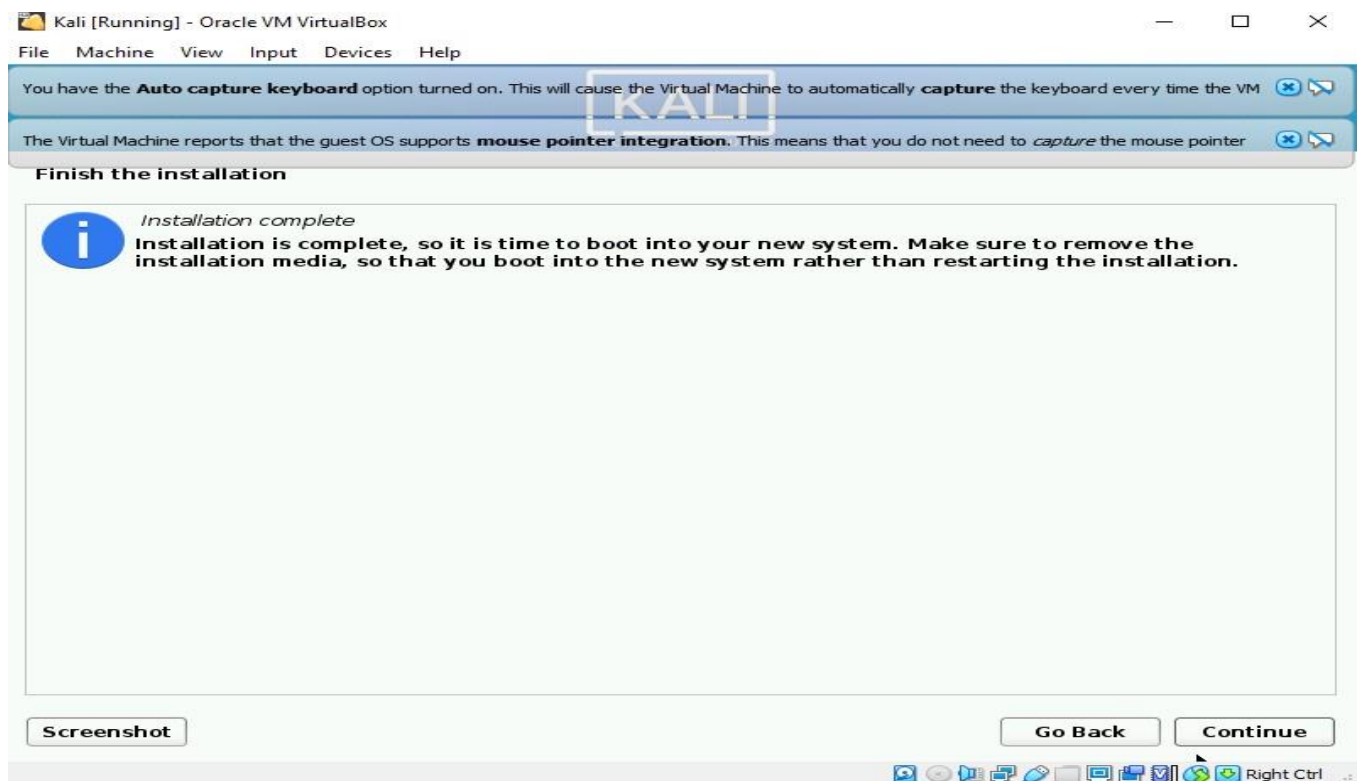


Figure 10 Successful completion of installation





*Figure 11 Kali Linux ready to be used*

## **LATEST APPLICATIONS:**

Kali Linux does excellent job separating these useful utilities into the following categories:

1. Information Gathering
2. Vulnerability Analysis
3. Wireless Attacks
4. Web Applications
5. Exploitation Tools
6. Stress Testing
7. Forensics Tools
8. Sniffing & Spoofing
9. Password Attacks
10. Maintaining Access
11. Reverse Engineering
12. Reporting Tools
13. Hardware Hacking

Professionals that use Kali Linux:

1. Security Administrators – Security Administrators are responsible for safeguarding their institution's information and data. They use Kali Linux to review their environment(s) and ensure there are no easily discoverable vulnerabilities.
2. Network Administrators – Network Administrators are responsible for maintaining an efficient and secure network. They use Kali Linux to audit their network. For example, Kali Linux has the ability to detect rogue access points.
3. Network Architects – Network Architects, are responsible for designing secure network environments. They utilize Kali Linux to audit their initial designs and ensure nothing was overlooked or misconfigured.

4. Pen Testers – Pen Testers, utilize Kali Linux to audit environments and perform reconnaissance on corporate environments which they have been hired to review.
5. CISO – CISO or Chief Information Security Officers, use Kali Linux to internally audit their environment and discover if any new applications or rouge configurations have been put in place.
6. Forensic Engineers – Kali Linux possess a "Forensic Mode", which allows a Forensic Engineer to perform data discovery and recovery in some instances.
7. White Hat Hackers – White Hat Hackers, similar to Pen Testers use Kali Linux to audit and discover vulnerabilities which may be present in an environment.
8. Black Hat Hackers – Black Hat Hackers, utilize Kali Linux to discover and exploit vulnerabilities. Kali Linux also has numerous social engineer applications, which can be utilized by a Black Hat Hacker to compromise an organization or individual.
9. Grey Hat Hackers – Grey Hat Hackers, lie in between White Hat and Black Hat Hackers. They will utilize Kali Linux in the same methods as the two listed above.

Computer Enthusiast – Computer Enthusiast is a pretty generic term, but anyone interested in learning more about networking or computers, in general, can use Kali Linux to learn more about Information Technology, networking, and common vulnerabilities.

## LEARNING OUTCOME:

- Virtualizing Kali Linux inside of VMware, allowing you to have a Kali VM was learnt. This is a great way to use Kali, as it is completely separate from the host, allows you to interact with other VMs (as well as the host, and other machines on the network), and allows you to revert to snapshots.

## REFERENCES:

1. Kali OS: <https://www.youtube.com/watch?v=jk2KGdJU2OI>
2. Parrot Security OS: <https://www.youtube.com/watch?v=4qvFp99rfXw>
3. Download Kali Linux OS: <https://www.kali.org/docs/introduction/download-official-kali-linux-images/>
4. Download Parrot Security OS: <https://parrotlinux.org/download/>