**University of Dhaka**
**Dept. of Computer Science and Engineering**
**Professional Masters in Information and Cyber Security (PMICS) Program**

---

**CSE 808 - Information Infrastructure Protection**

---

# Environment Setup for Cyber Security

Lab Class 1 – Manual

**Conducted by: Md. Shakhawat Hossain Robin**

## Lab Description

Welcome to the Cybersecurity Lab! In this hands-on session, we will delve into the fundamentals of cybersecurity, focusing on setting up a secure lab environment for practical exercises. Our primary goal is to provide you with a comprehensive understanding of the Linux operating system, usage of essential Linux commands and familiarize with the common tools and software used in cybersecurity.

## Lab Objectives:

- Brief overview of cybersecurity principles and the importance of practical hands-on experience
- Step-by-step guidance on configuring a secure and isolated lab environment to simulate real-world scenarios.
- Understanding the basics of the Linux operating system, its architecture, and the role it plays in cybersecurity.
- Exploration of the Linux file system structure, understanding directory hierarchies, and file permissions.
- Hands-on exercises covering essential commands for using the Linux operating system.
- Familiarization with a range of tools and software commonly used in the field of cybersecurity

| Prerequisites | Link to download |
|---|---|
| ➢ A computer with Installed Operating Systems | --- |
| ➢ Oracle VM VirtualBox | https://www.virtualbox.org/wiki/Downloads |
| ➢ Visual C++ Redistributable (if required) | https://aka.ms/vs/17/release/vc_redist.x64.exe |
| ➢ VirtualBox Extension Pack | https://www.virtualbox.org/wiki/Downloads |
| ➢ Pre-built Kali Linux Virtual Image | https://www.kali.org/get-kali/#kali-virtual-machines |

## Virtual Lab

A virtual lab, also known as an isolated lab or sandbox environment, refers to a controlled and isolated computing environment created virtually. It provide a flexible, cost-effective, and scalable solution for creating isolated computing environments for experimentation, testing, learning, and research purposes across various domains, including software development, IT infrastructure management, cybersecurity, and network administration.

In a virtual lab, various software, applications, operating systems, and network configurations are set up within virtual machines or containers, allowing users to simulate real-world scenarios without impacting production systems or networks.

# Different Types of Computing
# (Bare Metal, Virtualization, and Containerization)

- **Bare Metal (Physical):**
  - The bare metal layer, also known as the physical layer, represents the actual physical hardware infrastructure.
  - It consists of physical servers, storage devices, networking equipment, and other physical components.
  - Operating directly on the bare metal layer means that software runs directly on the physical hardware without the need for an intervening operating system.

- **Virtualization:**
  Virtualization is a technology that enables the creation of multiple virtual environments or machines on a single physical server or host. These virtual instances, often referred to as virtual machines (VMs), operate independently, each with its own operating system and applications.

- **Containerization:**
  Containerization is an OS-level virtualization technique that enables the deployment and execution of distributed applications into self-contained units called containers without the need to launch a complete virtual machine (VM) for each application. Each container runs in its own isolated environment, ensuring consistency across different systems.

## Graphical Representation: (Bare Metal, Virtualization, and Containerization)

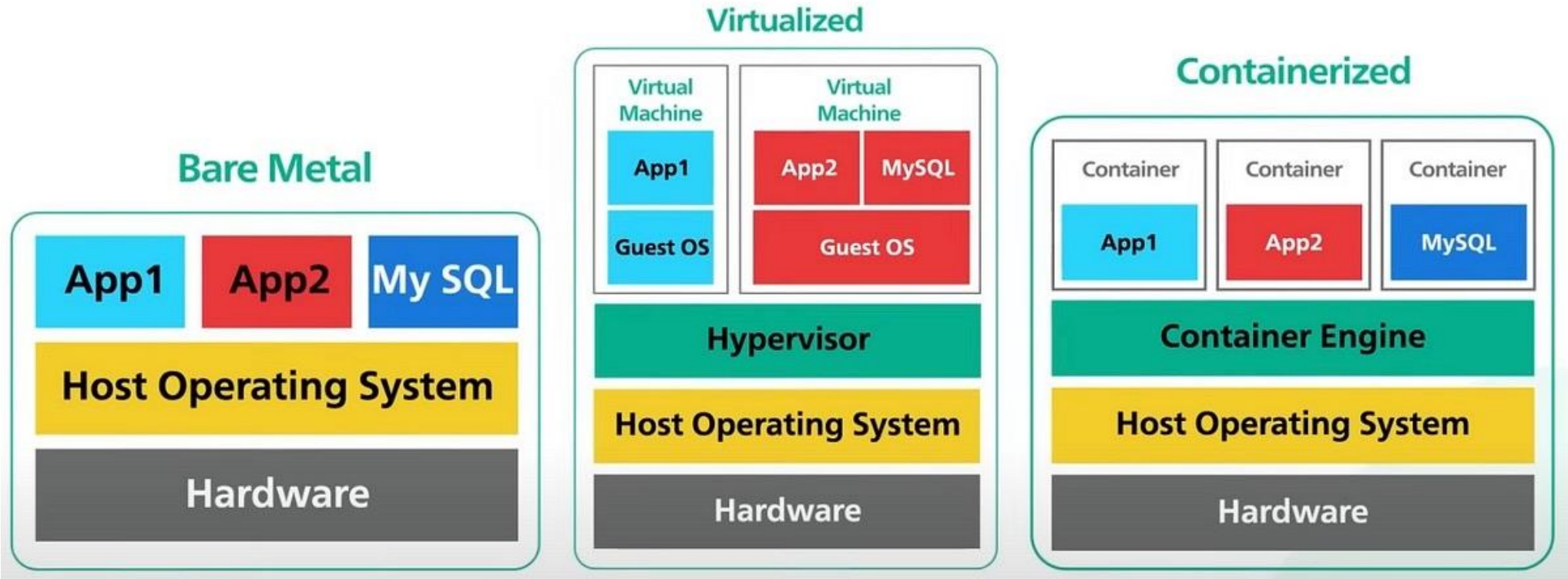


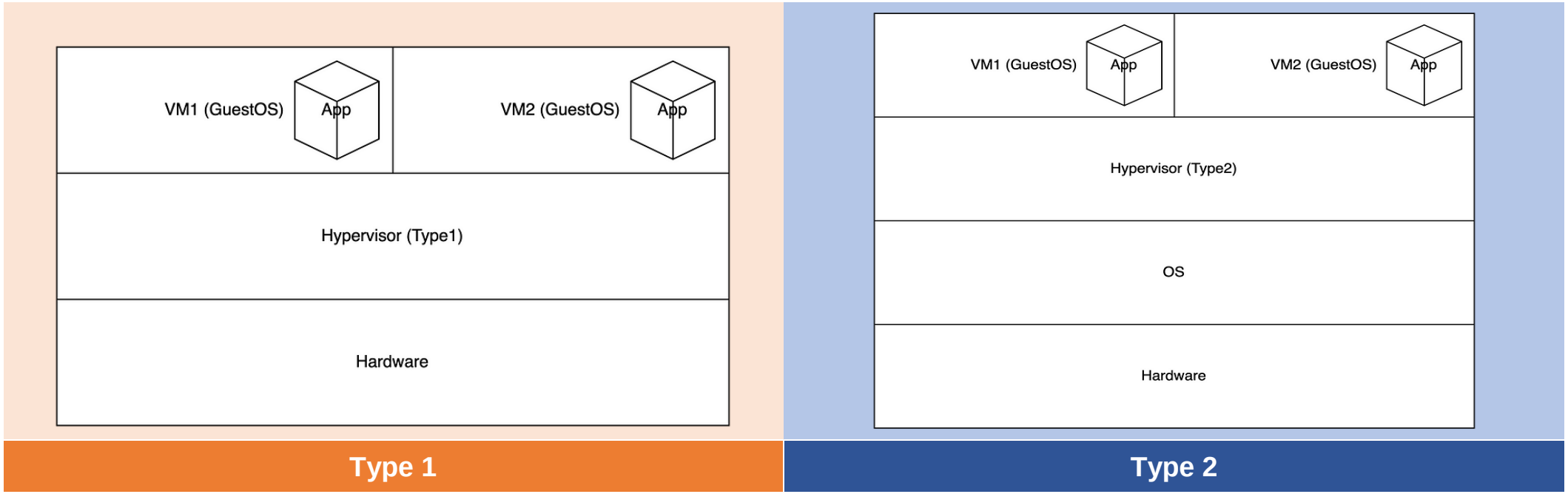

*Fig: Bare Metal, Virtualization, and Containerization*

# Hypervisor

A hypervisor, also known as a virtual machine monitor (VMM), is software or firmware that enables multiple operating systems (OS) to share a single hardware host. It allows for the creation and management of virtual machines (VMs), which are isolated environments that mimic physical computers. Hypervisors abstract physical hardware resources like CPU, memory, storage, and networking, allocating portions of these resources to each virtual machine.

### There are two primary types of hypervisors:-

- **Type 1 -** Hypervisors, which run directly on the physical hardware. (e.g. VMware vSphere/ESXi, Xen, Hyper-V, KVM, etc.)
- **Type 2 -** Hypervisors, which operate on top of a host operating system. (e.g. include Oracle VirtualBox, VMware Workstation, QEMU, etc.)



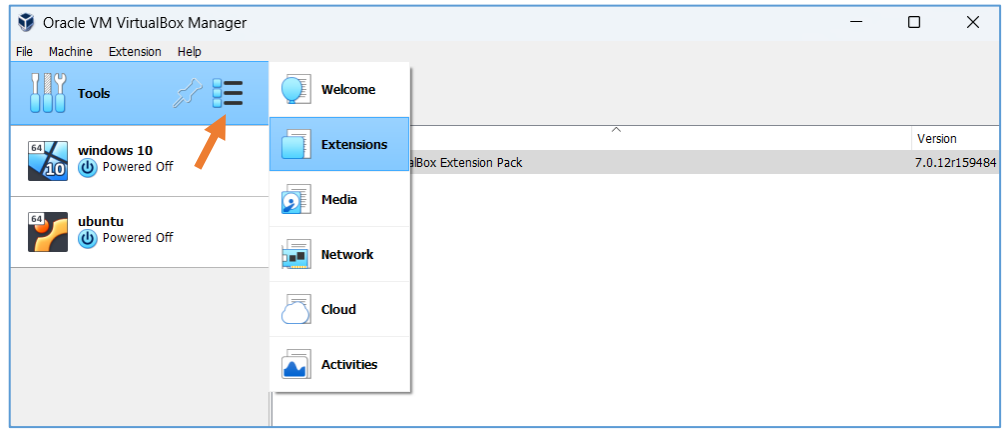
# Setting up Kali Linux Environment

## 1. Download and install VirtualBox

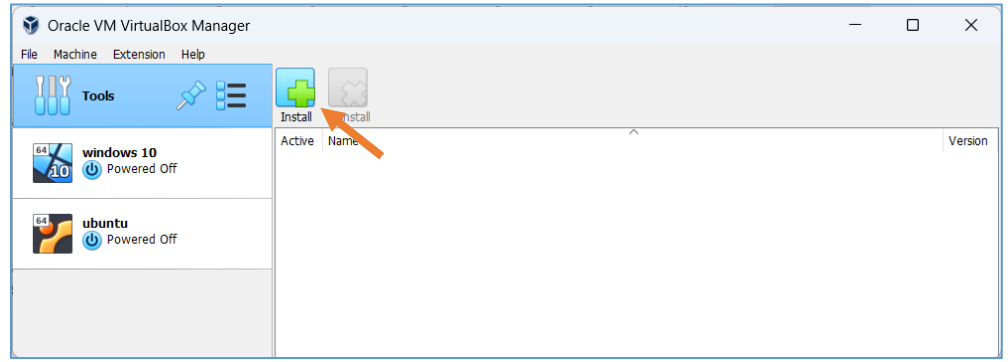
The first thing you need to do is to download and install VirtualBox from Oracle's official website. If you found any error for Visual C++ Redistributable, please install it first then try to install VirtualBox

## 2. Install VirtualBox Extension Pack via GUI

2.1. Open the VirtualBox GUI.
2.2. Click the **Tools tab**: options
2.3. Select the **Extensions**

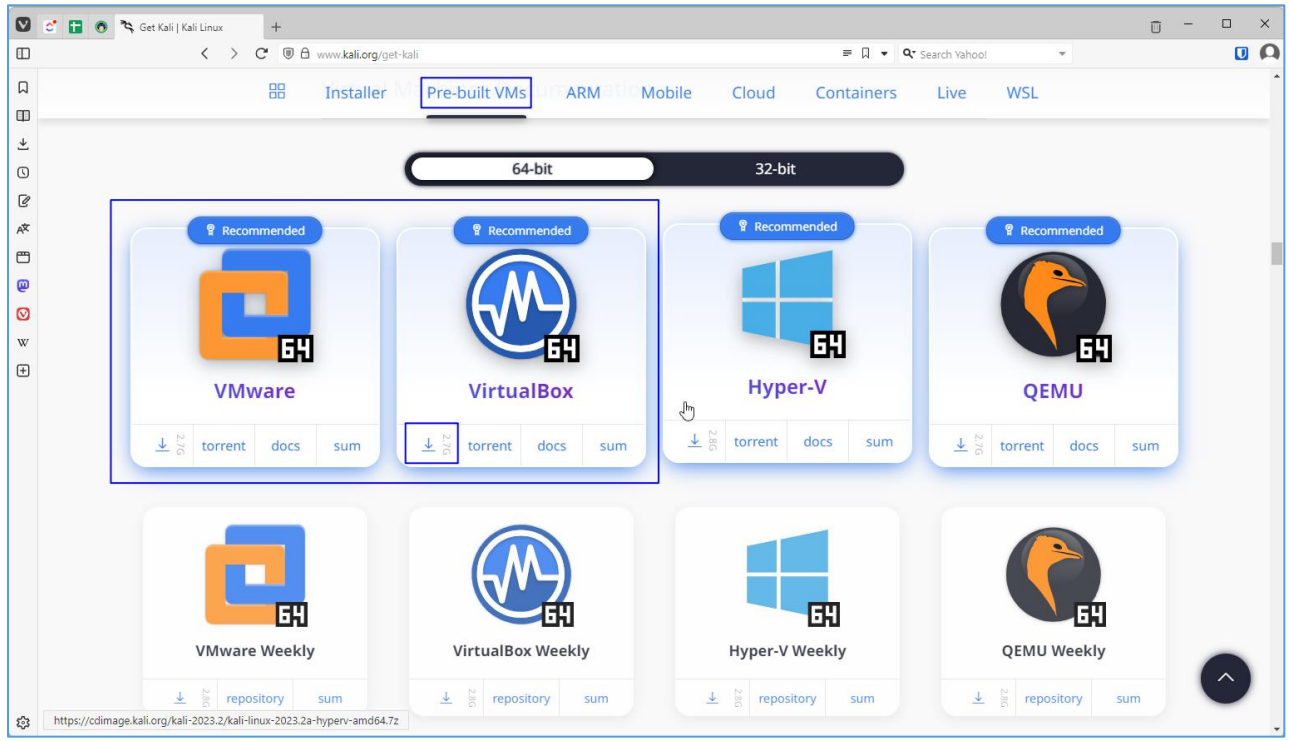



2.4. Now click on **Install**. Then, locate the extension pack file which you download on your computer.



## 3. Download ready-to-use (pre-built) virtual image of Kali Linux

After installing it successfully, head to Kali Linux download page to download the VM image for VirtualBox. Download Kali Linux Virtual Machine Images, Download Kali Linux Virtual Image




If you change your mind about utilizing VMware, that is available too, Download Kali Linux VMware images

## 4. Install Kali Linux on Virtual Box

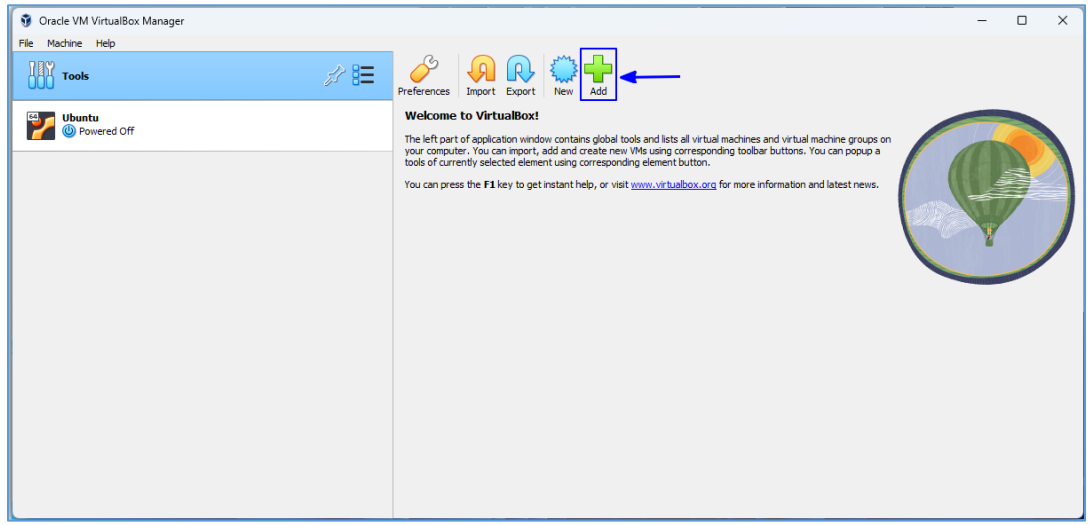
Once you have installed VirtualBox and downloaded the Kali Linux 7z image, you just need to add it to VirtualBox in order to make it work.

Here's how to add the VirtualBox image for Kali Linux:

**Step 1: Extract the downloaded 7z file**.

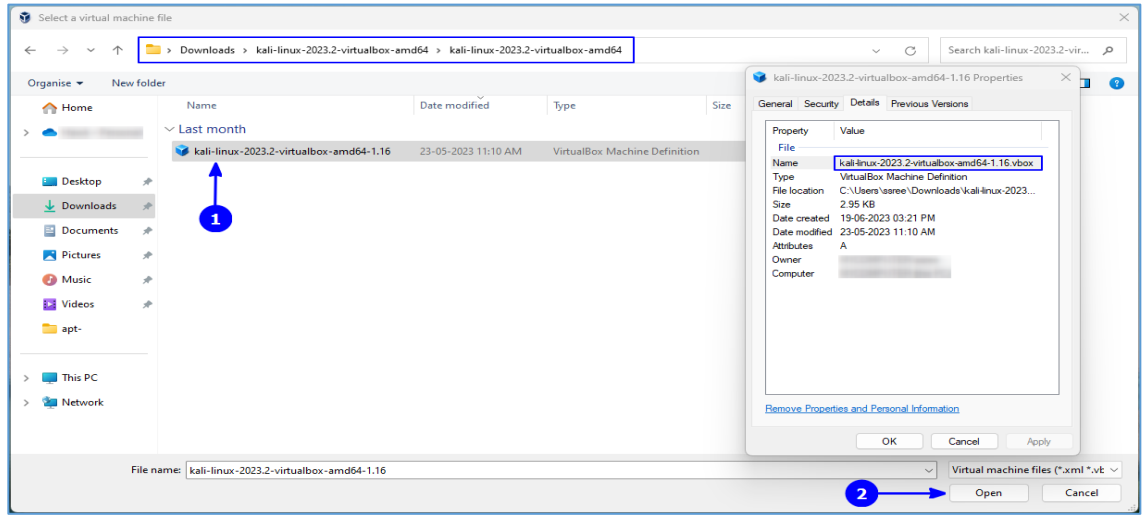
The Kali Linux Virtual Machine storage will be on the same location as you extracted the 7z file. If you want a different location for the VM, you need to extract the 7z file to a location where you have sufficient storage available. I would never recommend the C: drive on Windows.

**Step 2: Launch VirtualBox. You will notice an Add button – click on it.**



**Step 3: Next, browse the folder you just downloaded and extracted.**

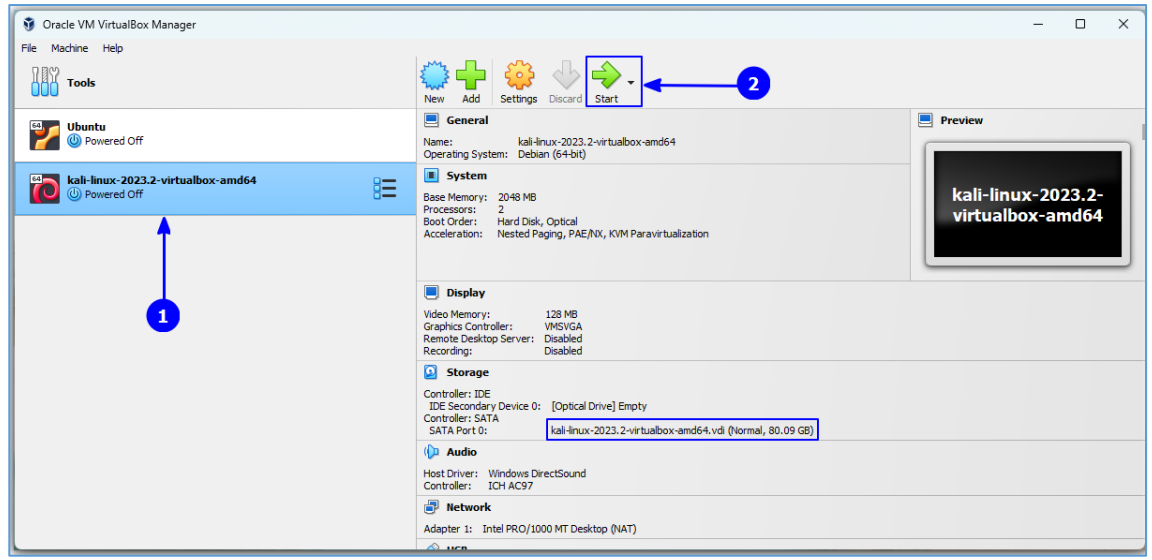
Choose the VirtualBox Machine Definition file to be added (as you can see in the image below). The file name should start with ‘kalilinux‘ and end with .vbox extension. Add Kali Linux



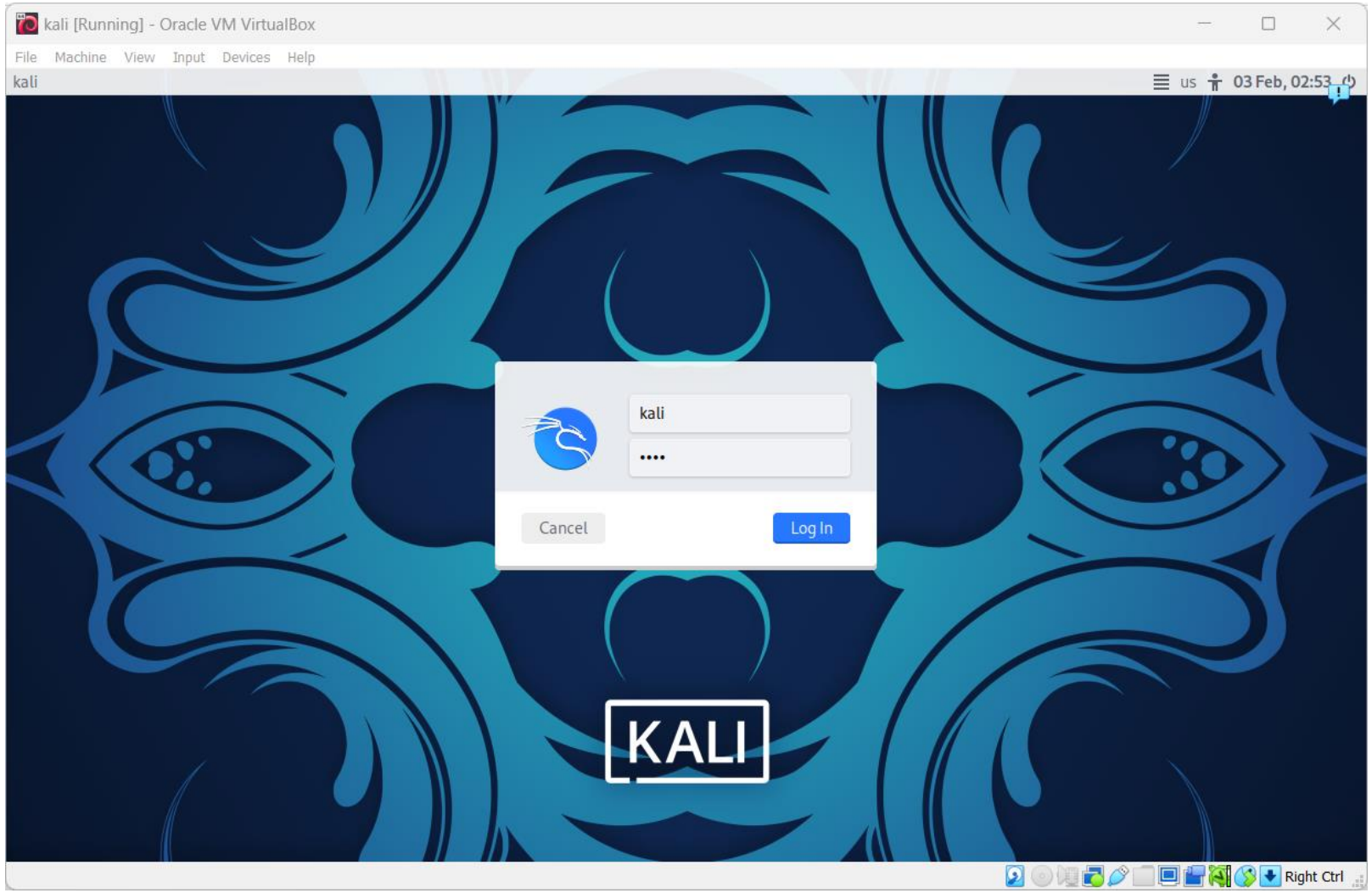

**Step 4:**

Now, you will be shown the settings for the virtual machine you are about to add. So, you can customize them or not – that is your choice. It is okay if you go with the default settings.

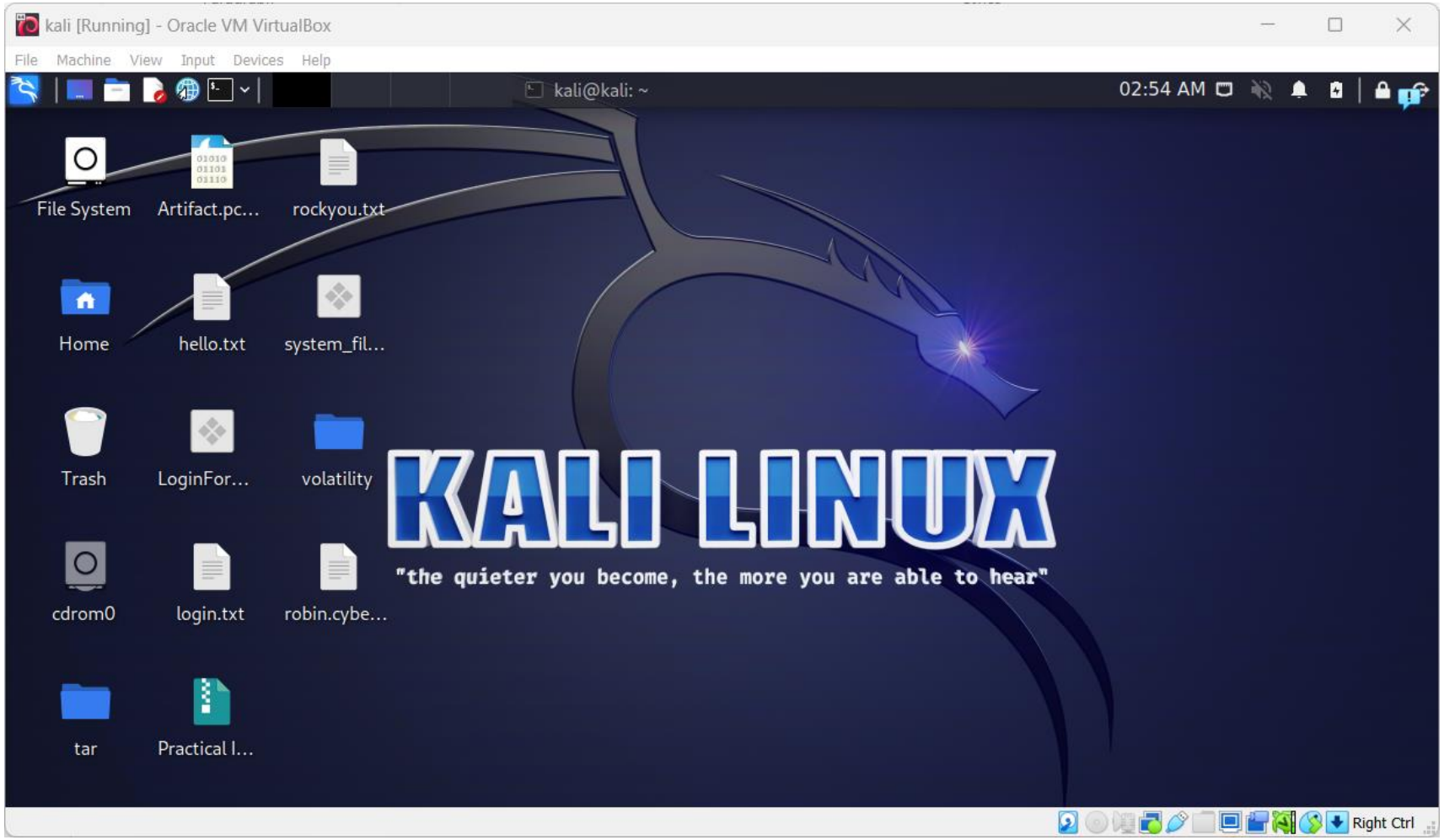
- Set the RAM as per your requirement
- You can use multiple processor for better performance (recommended 2 processor)
- Set the video memory 128mb for better graphics quality
- Set network adapter based on your requirement



When everything is done, **Start** the machine like below and starting do login using the credential username and password: **kali**



**After successfully login a desktop screen will appear.**



# VirtualBox, Network Type’s Details

**1. NAT (Network Address Translation):**

- NAT is the default network mode in VirtualBox.
- In this mode, VirtualBox acts as a router between the host machine and the VMs, performing network address translation to allow VMs to access external networks.
- VMs are assigned IP addresses from a private subnet, and outgoing network traffic from VMs is translated to use the host machine's IP address.
- NAT allows VMs to access the internet and communicate with external networks but does not provide direct inbound connectivity to VMs from external hosts.

**2. Bridged Adapter:**

- In bridged mode, VirtualBox connects a VM's network interface directly to a physical network interface on the host machine.
- This allows the VM to appear as a separate device on the host's physical network, receiving its own IP address from the network's DHCP server or using a static IP configuration.
- Bridged mode provides full network connectivity to the VM, allowing it to communicate with other devices on the physical network as if it were a separate physical machine.

**3. Internal Network:**

- Internal network mode creates a private, isolated network that is internal to the host machine and not visible from external networks.
- VMs connected to the same internal network can communicate with each other but cannot communicate with the host machine or external networks.
- This mode is useful for creating isolated network environments for testing or development purposes.

**4. Host-only Adapter:**

- Host-only mode creates a private network that is visible only to the host machine and its VMs.
- VMs connected to the host-only network can communicate with each other and with the host machine but cannot communicate with external networks.
- This mode is commonly used for creating development or testing environments where external network connectivity is not required.

**5. NAT Network:**

- NAT network is similar to NAT mode but provides more advanced networking capabilities and configuration options.
- It allows VMs to communicate with each other and with external networks through NAT, similar to the default NAT mode.
- NAT network also supports port forwarding and allows the creation of multiple virtual networks with different configurations.

**6. Generic Driver:**

- VirtualBox also supports custom network configurations using generic network drivers, allowing users to create custom networking setups tailored to their specific requirements.
- This mode is less commonly used and requires advanced networking knowledge to configure.

**Thank you**