## ****1. Lab Setup Report****

## ****Introduction****

This report outlines the process of setting up a virtual lab environment for cybersecurity tasks using VMware Workstation and Kali Linux. The setup ensures a stable and secure environment for penetration testing, ethical hacking, and security analysis. Screenshots have been included to provide a visual reference for the setup process.

## ****Requirements****

To set up the virtual lab, the following hardware and software requirements were met:

**Software:**

VMware Workstation / VirtualBox

Kali Linux ISO image

**Hardware:**

Minimum **4GB RAM** (8GB recommended)

**20GB storage** (SSD preferred for better performance)

Multi-core processor for efficient virtualization

## ****Steps to Setup****

The virtual lab setup was completed through the following steps:

**Download and Install VMware Workstation:**

Download the latest version of VMware Workstation or VirtualBox from the official website.

Install the software following the guided installation process.

**Create a New Virtual Machine (VM):**

Open VMware Workstation and select "Create a New Virtual Machine."

Choose the Kali Linux ISO file and proceed with the setup.

Allocate resources (RAM, storage, and processor cores) based on system capabilities.

**Install Kali Linux on the VM:**

Boot the VM using the Kali Linux ISO.

Follow the installation wizard to set up the operating system.

Configure the username, password, and system settings.

**Configure Network Settings:**

Select **NAT** or **Bridged** networking mode based on connectivity needs.

Ensure internet access and proper network configuration.

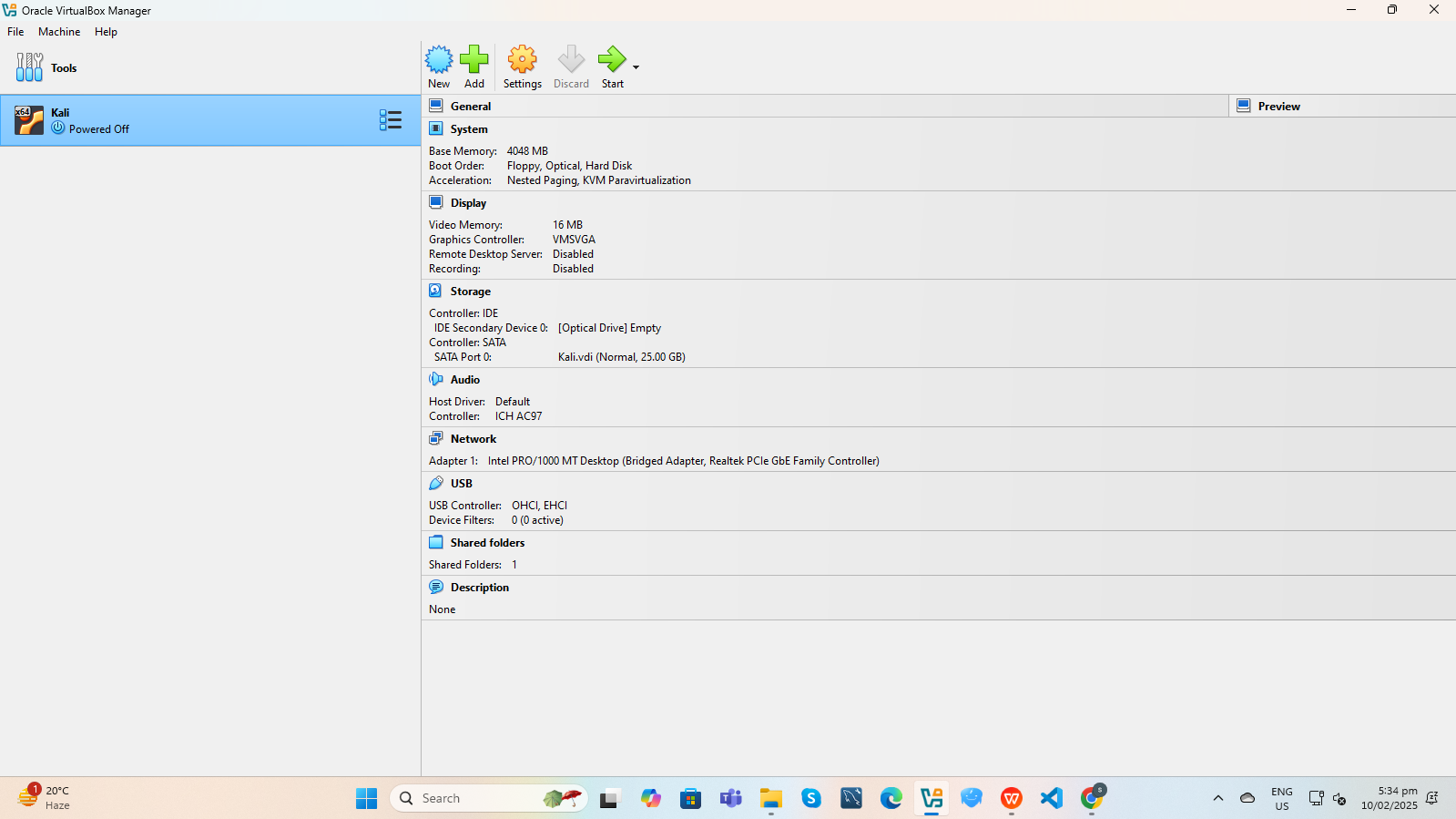
**Verify Installation:**

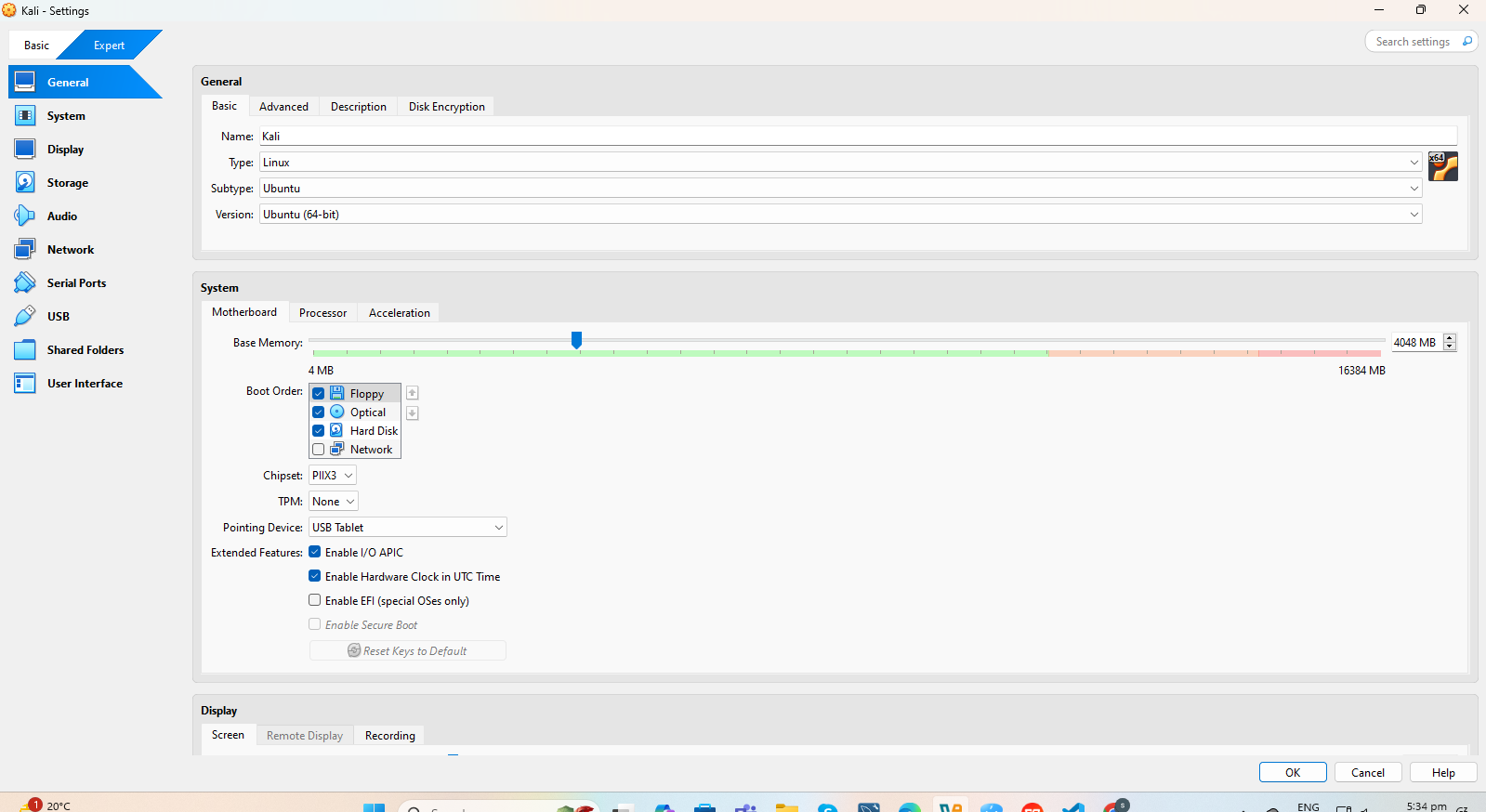
Reboot the VM and log into Kali Linux.

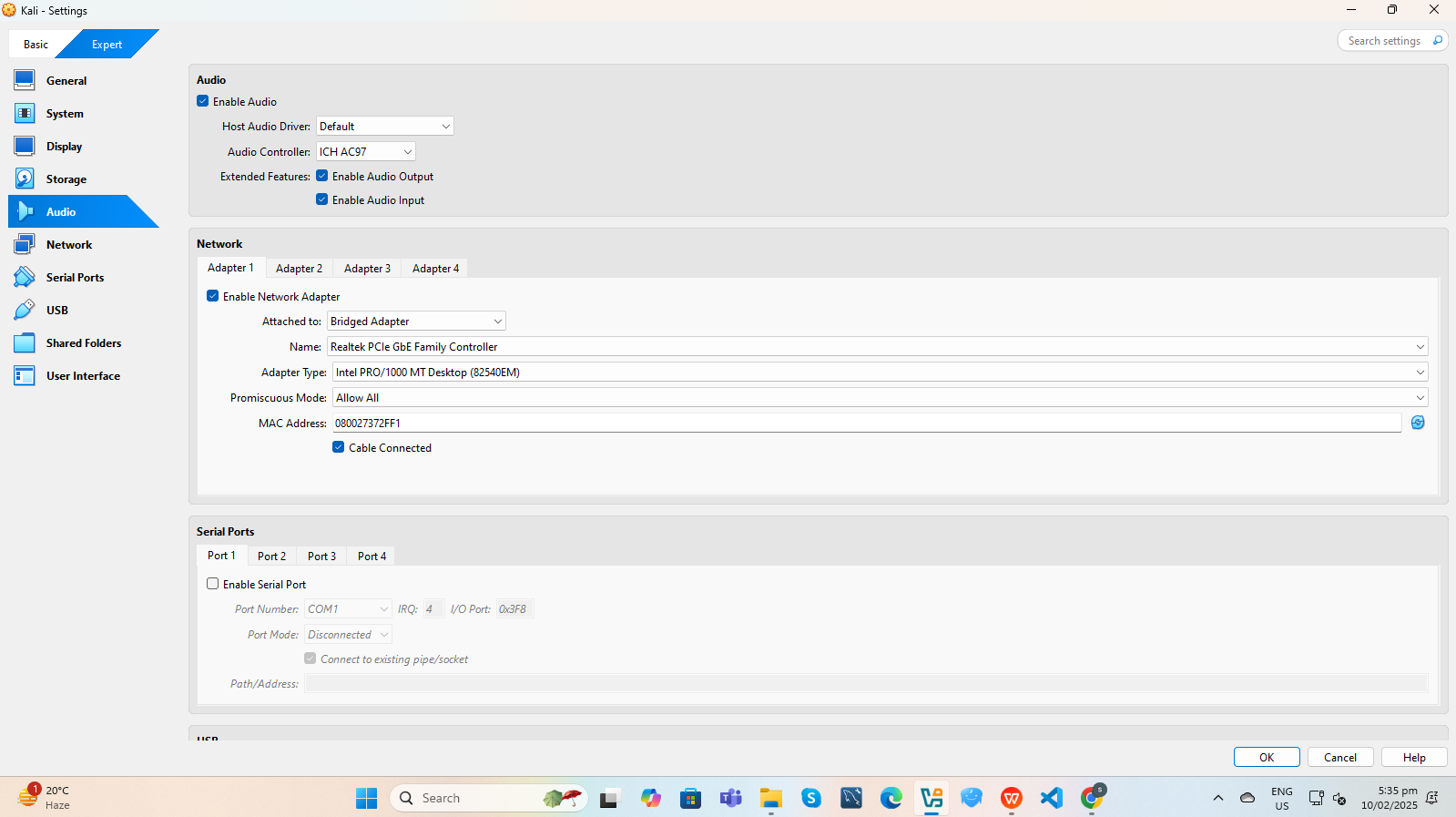
Update and upgrade system packages.

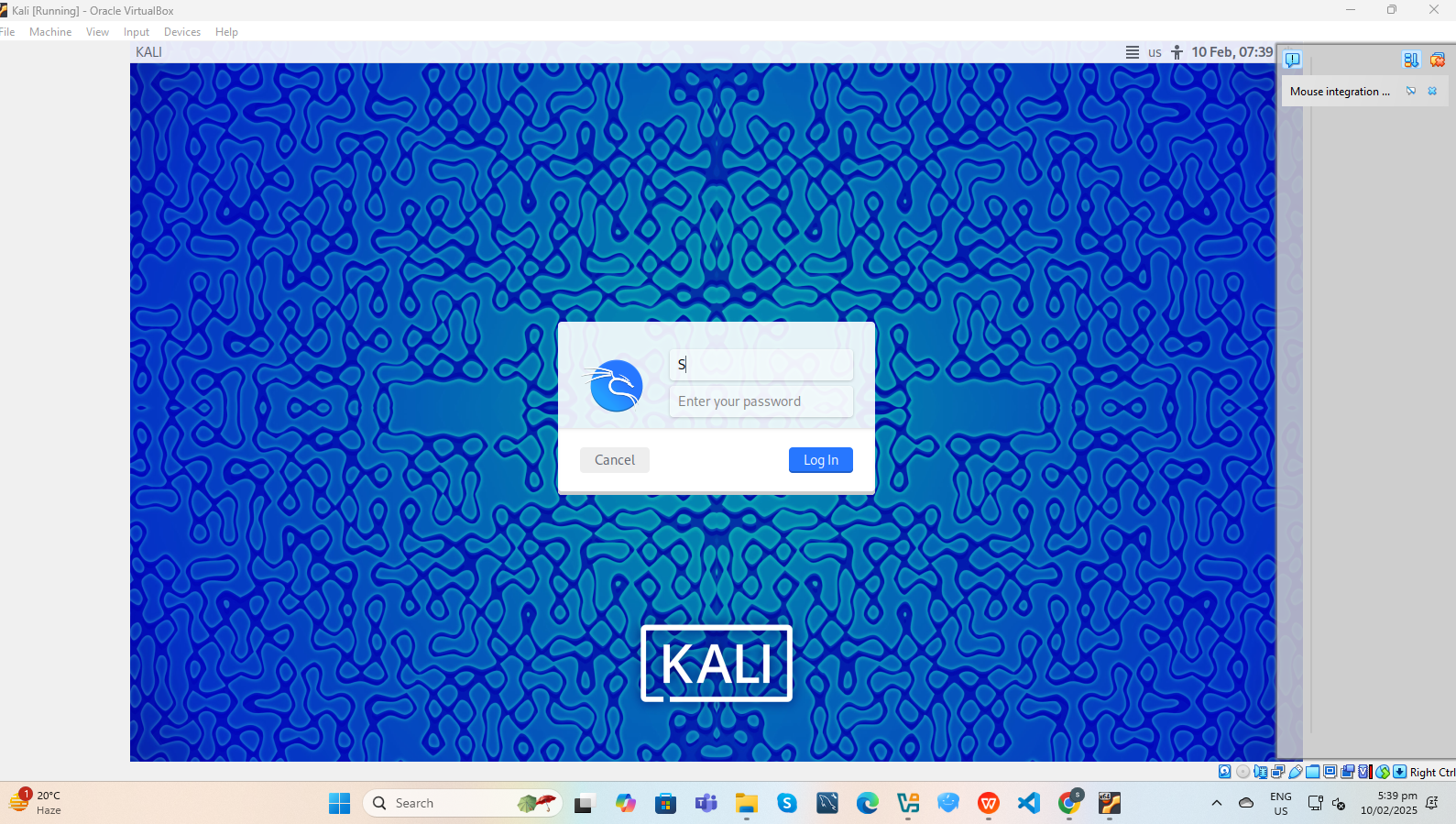
Check for network connectivity and tool availability.

### ****Screenshots****









### ****Conclusion****

The lab setup is successfully configured and ready for cybersecurity tasks.