**Cybersecurity & Ethical Hacking Internship**

**– ApexPlanet Software Pvt. Ltd. Report**

**Task Number:** 1 – Lab Setup

**Name:** Jai Rane

**Intern ID:** ASPL2518045

**Date:** 11-09-2025

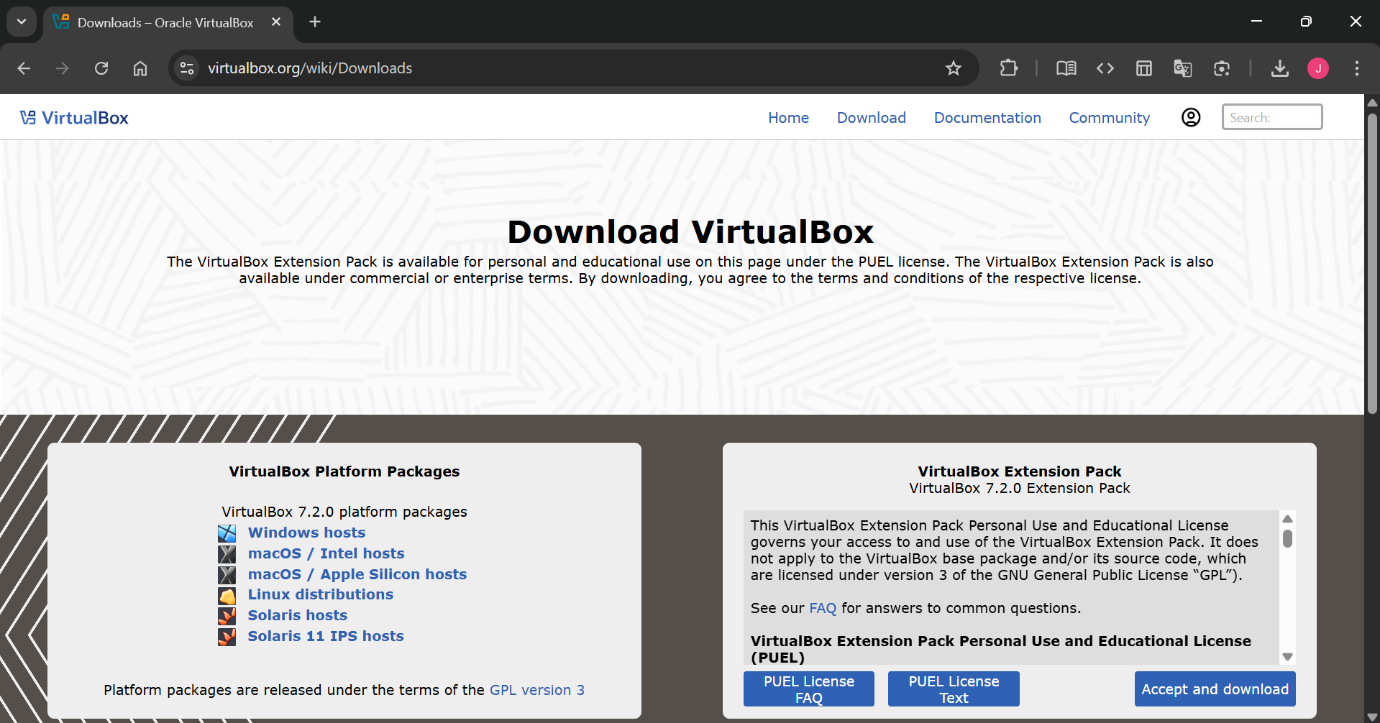
* **Objective: To build strong fundamentals in cybersecurity, networking, cryptography, and set up a professional hacking lab.**
* **Tools & Environment**

|  |  |  |
| --- | --- | --- |
| **Tool / Environment** | **Version / Details** | **Notes** |
| VirtualBox | 7.1.8r168469 | Used to run the virtual machines |
| Kali Linux | 2025.2 (VirtualBox Pre-Built Image, amd64) | Main OS for penetration testing & Linux practice |
| Nmap | 7.95 | To be used for network scanning & vulnerability assessment in future tasks |
| Metasploitable | V6.4.64-dev | Will be used in later tasks for exploitation practice |
| Wireshark | 4.4.6 | Planned for future tasks like packet analysis |
| Host System | Windows 10/11 (64-bit) | Physical machine running VirtualBox |
| Host Hardware | Intel i3, 8 GB RAM, 512 GB SSD | System specifications of the laptop |
| VM Allocation | 4 GB RAM, 2 CPU cores | Resources assigned to Kali VM |

**4. Procedure**

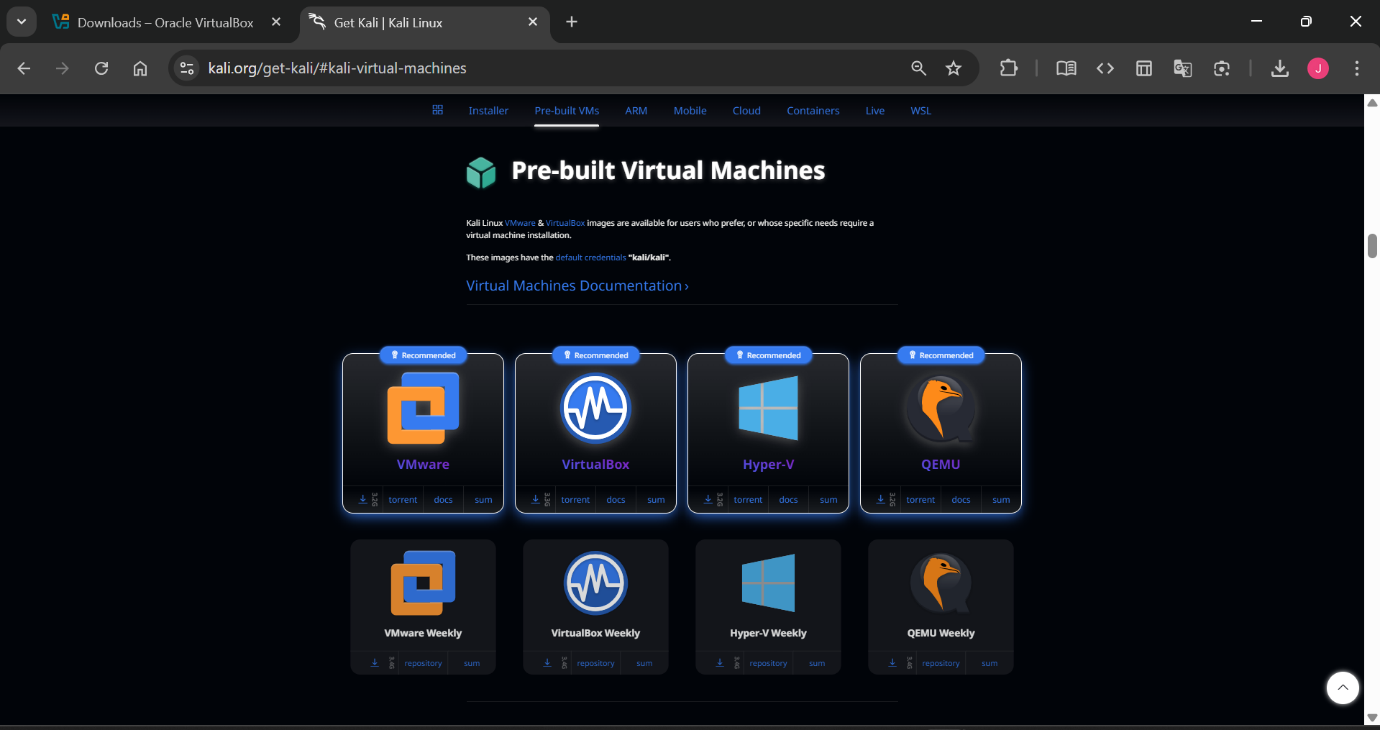
**Step 1**: Downloading VirtualBox and Kali Linux Pre-Built Image

Downloaded VirtualBox 7.x from the official Oracle website.

****

**Screenshot 1: VirtualBox download page**

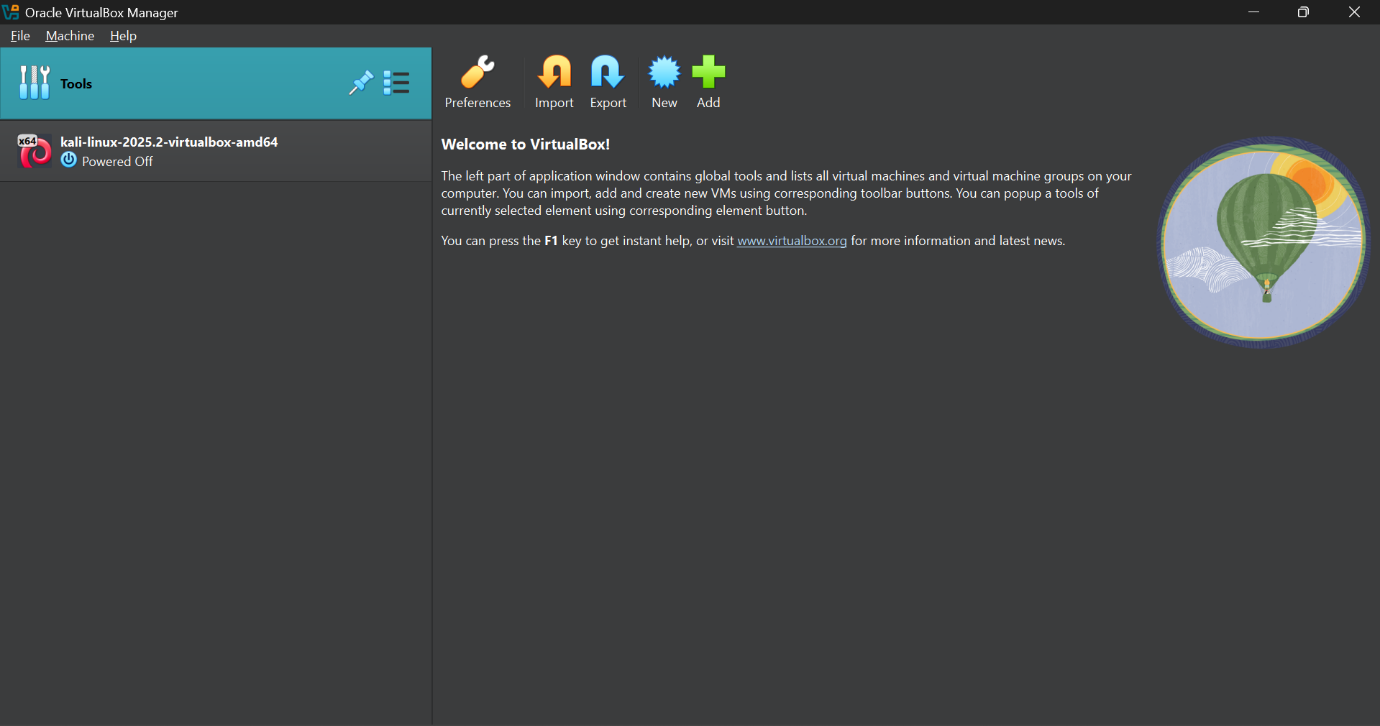
Downloaded the Kali Linux 2025.2 VirtualBox Pre-Built Image (amd64) from Kali’s official page**.**

****

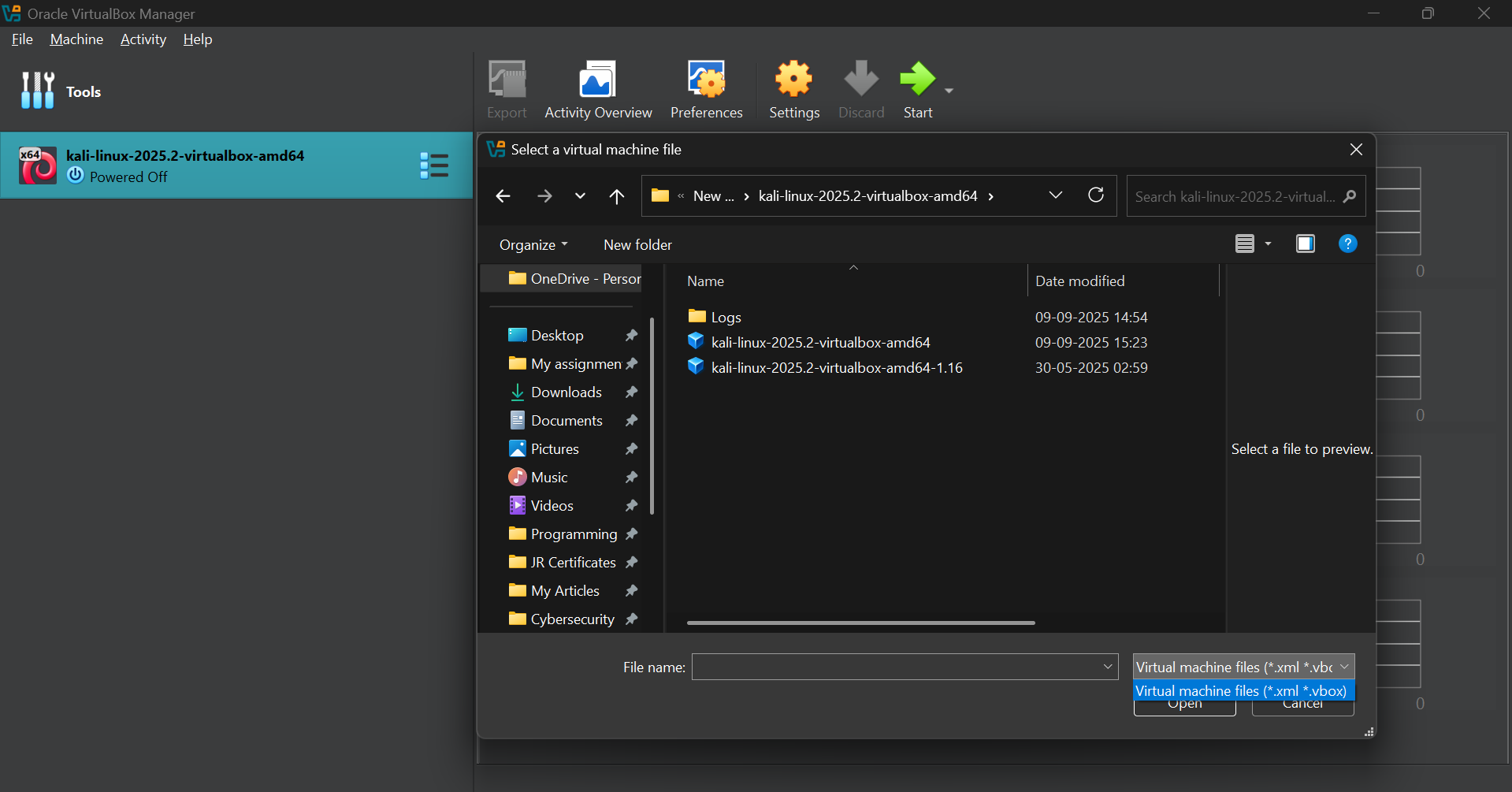
**Screenshot 2: Kali Linux Pre-Built Image download page**

**Step 2: Setting Up VirtualBox**

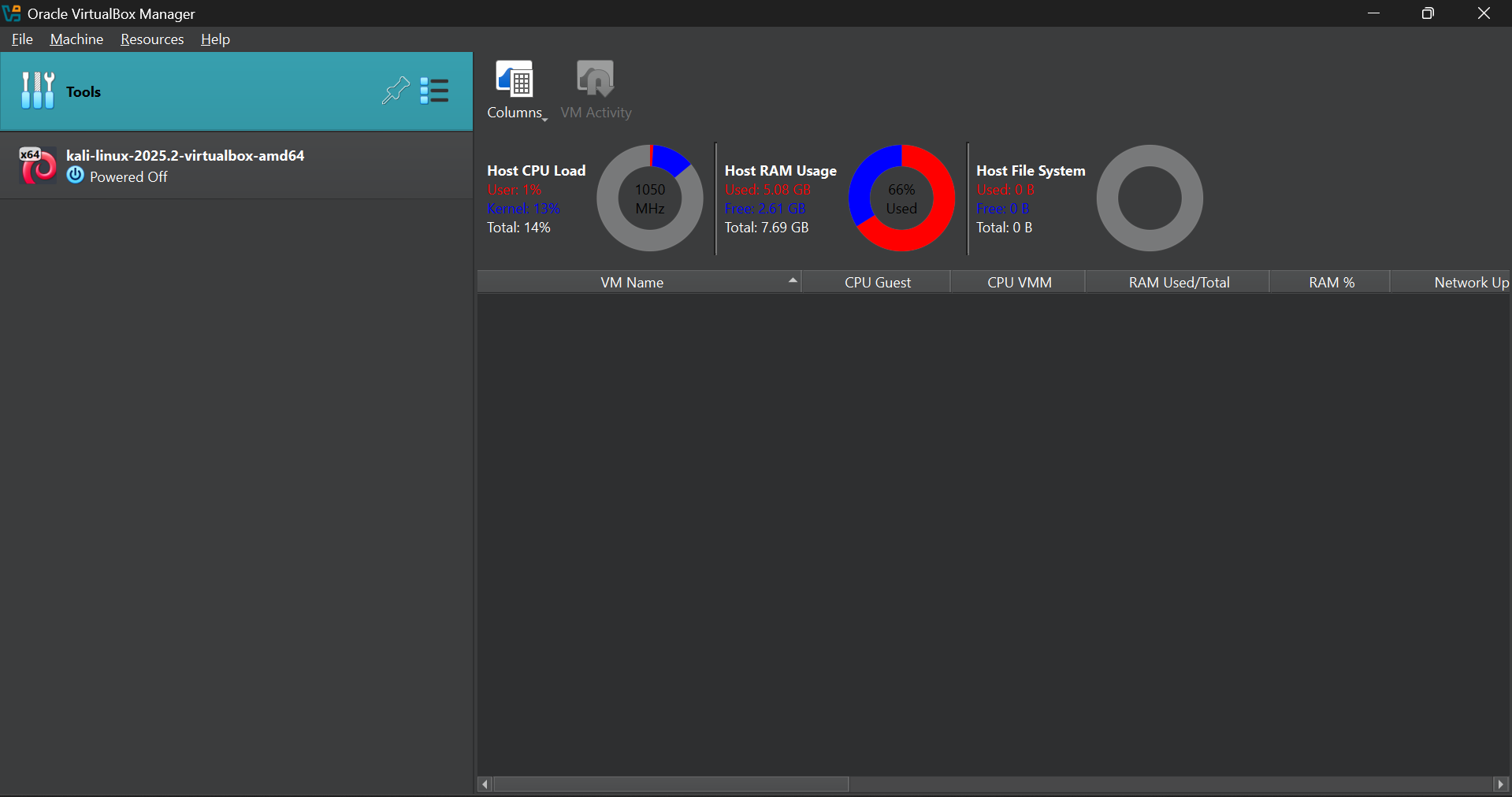
Installed VirtualBox on the host system (Windows 11).

****

**Screenshot 3: Oracle VirtualBox Home screen**

Imported the Kali Linux .ova/.vbox file into VirtualBox**.**

**Screenshot 4: choosing Kali Linux .vbox pre-image file**

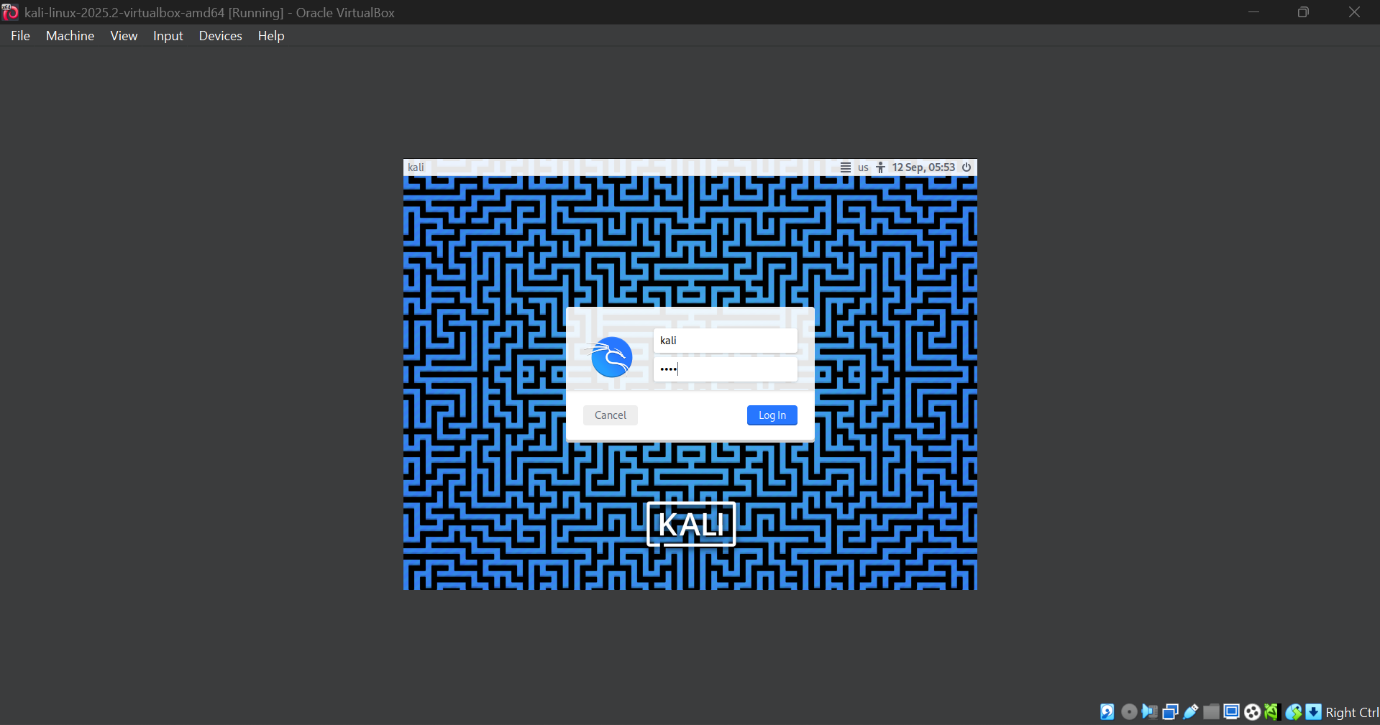
****

**\*Configured VM settings:** 4 GB RAM, 2 CPU cores.

**Screenshot 5: VM settings showing RAM/CPU allocation**

**Step 3: Running Kali Linux for the First Time**

* Booted Kali Linux VM successfully.

****

* Logged in using default credentials**.**

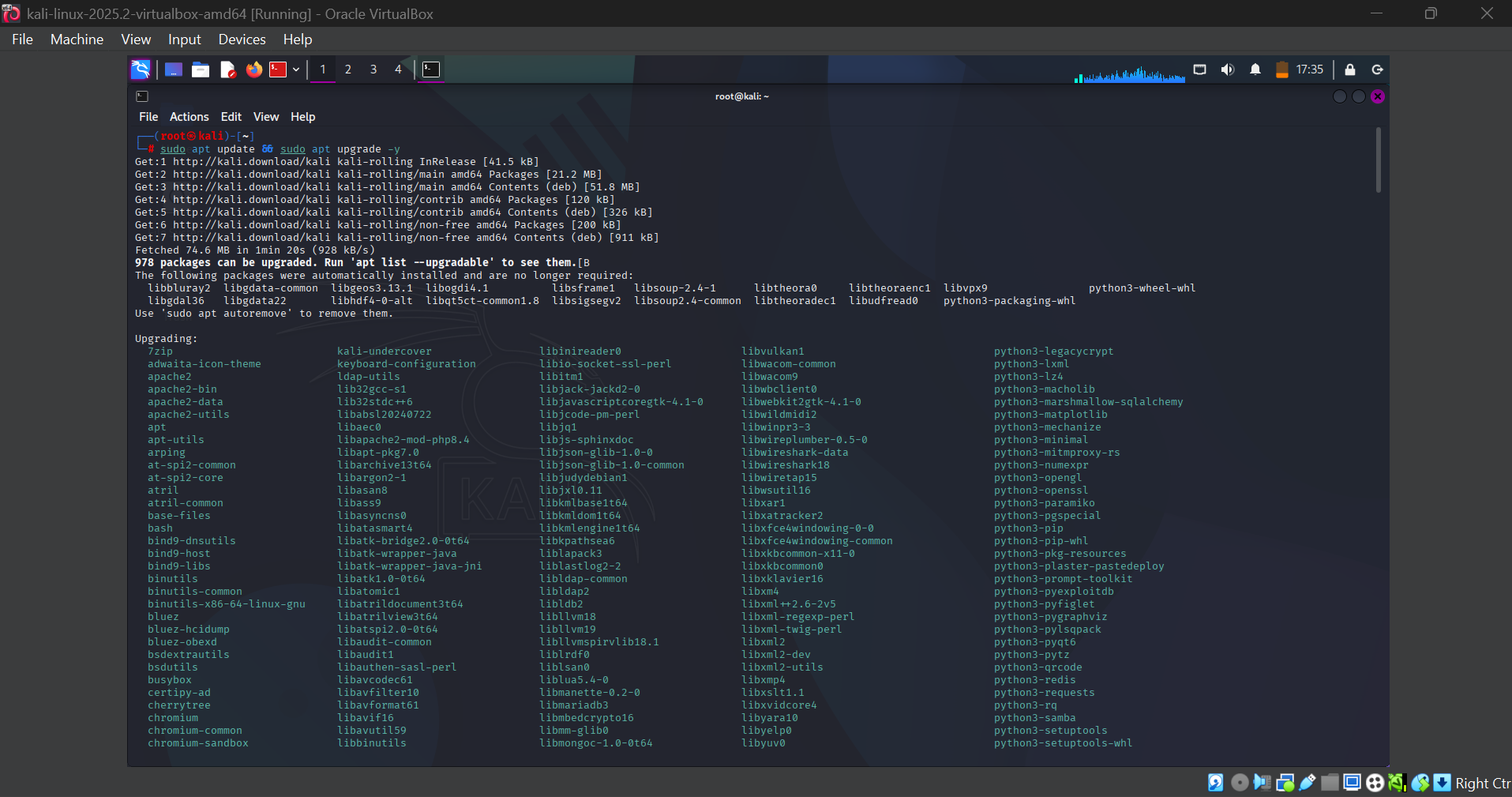
**Screenshot 6 : Kali Linux login screen**

****

* Verified that desktop loaded properly.

**Screenshot 7: Kali Linux desktop environment after login**

**Step 4: Basic Verification & Updates**

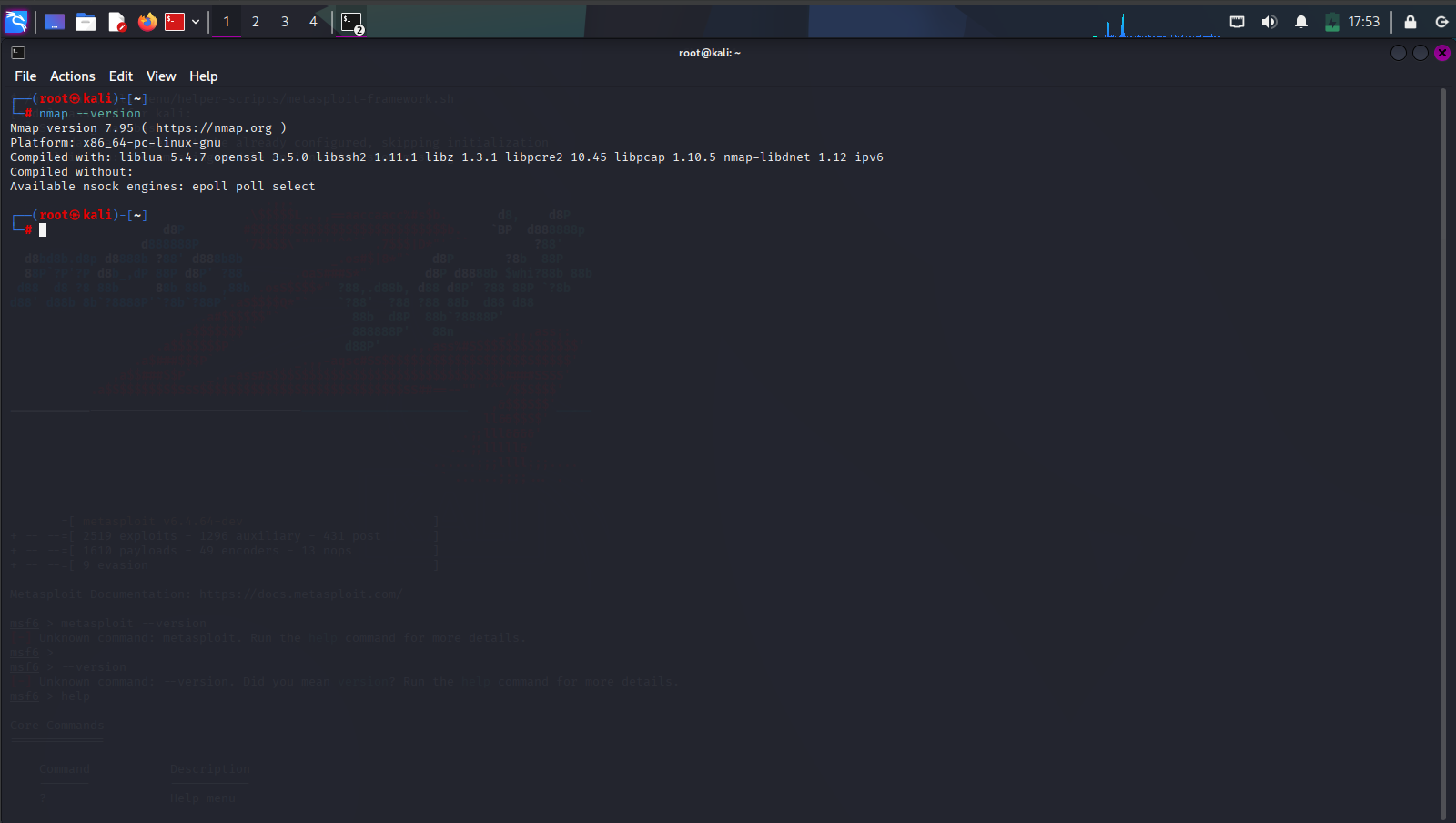
****

Ran initial update **(sudo apt update && sudo apt upgrade -y).**

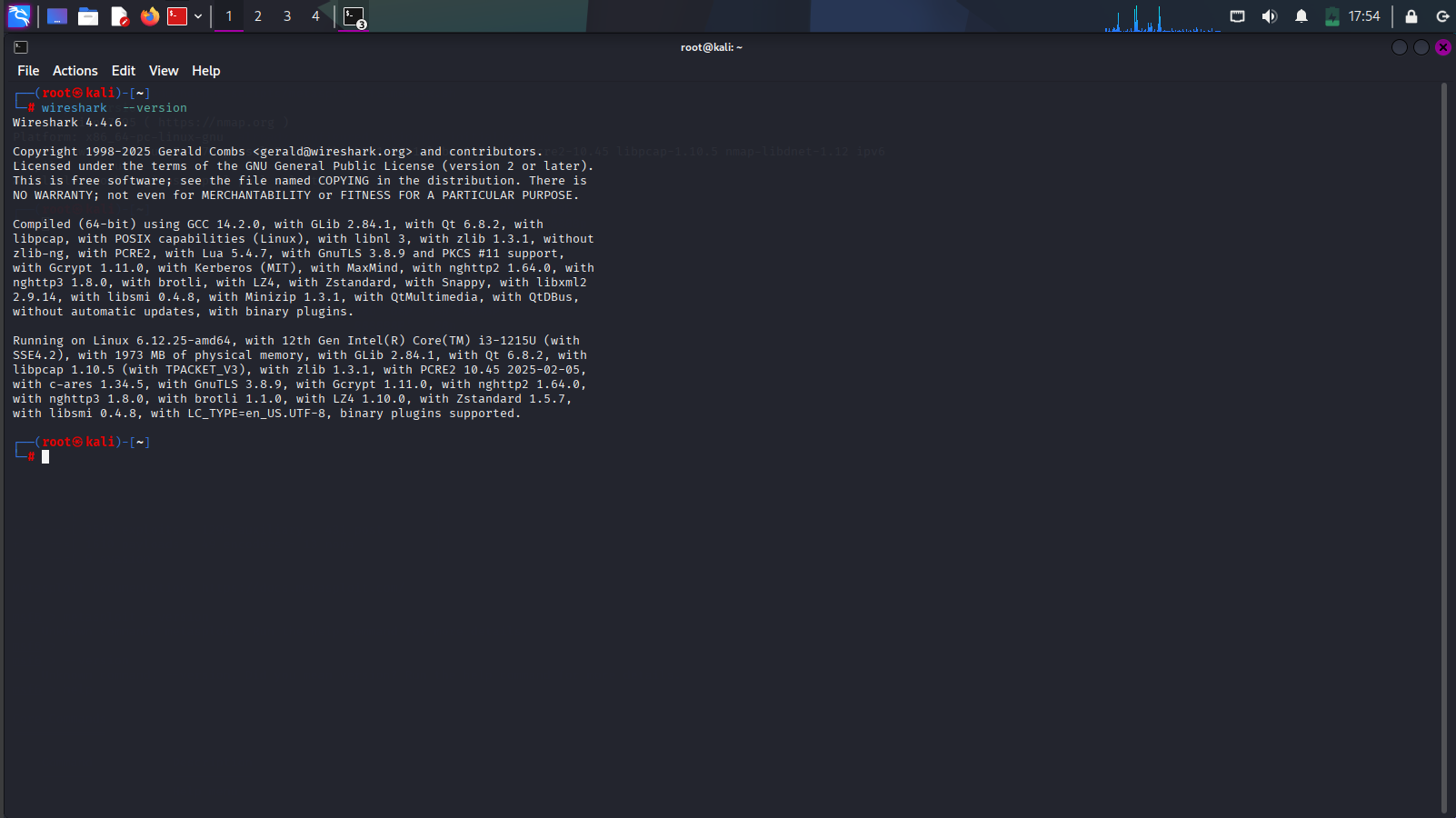
**Screenshot 8: Terminal showing update process**

Verified tools are pre-installed such as the following.

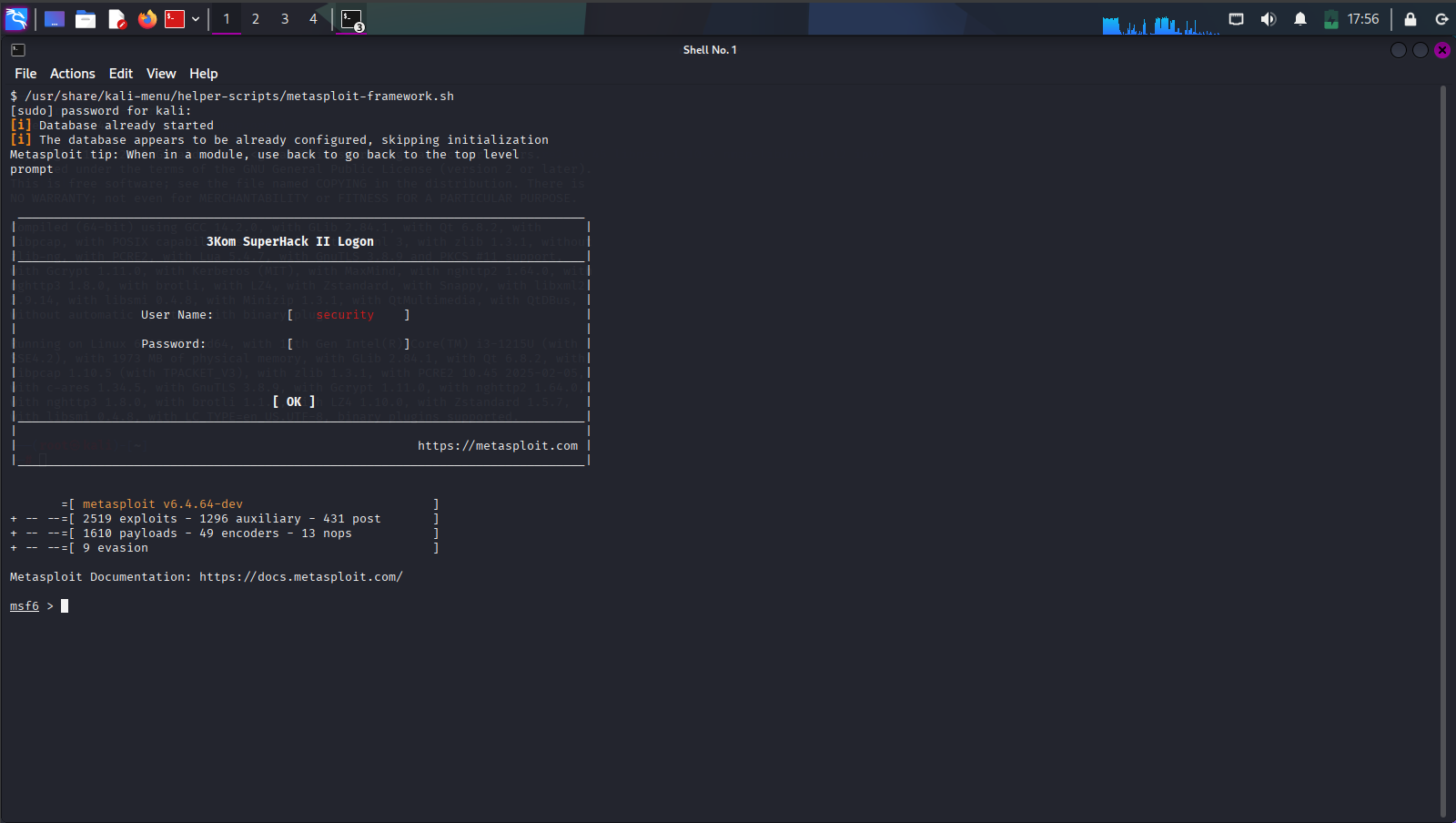
1. **Nmap**
2. **Wireshark**
3. **Metaspoitable**

****

**Nmap Version – 7.95 :** It is an open network source tool for network exploration and security auditing, used to discover hosts, services, operating systems, and potential vulnerabilities on networks

****

**Wireshark Version – 4.4.6 :** to capture, inspect, and analyze network traffic at the packet level to identify and resolve network issues, troubleshoot performance problems, detect security vulnerabilities, understand network protocols, and for education and software development

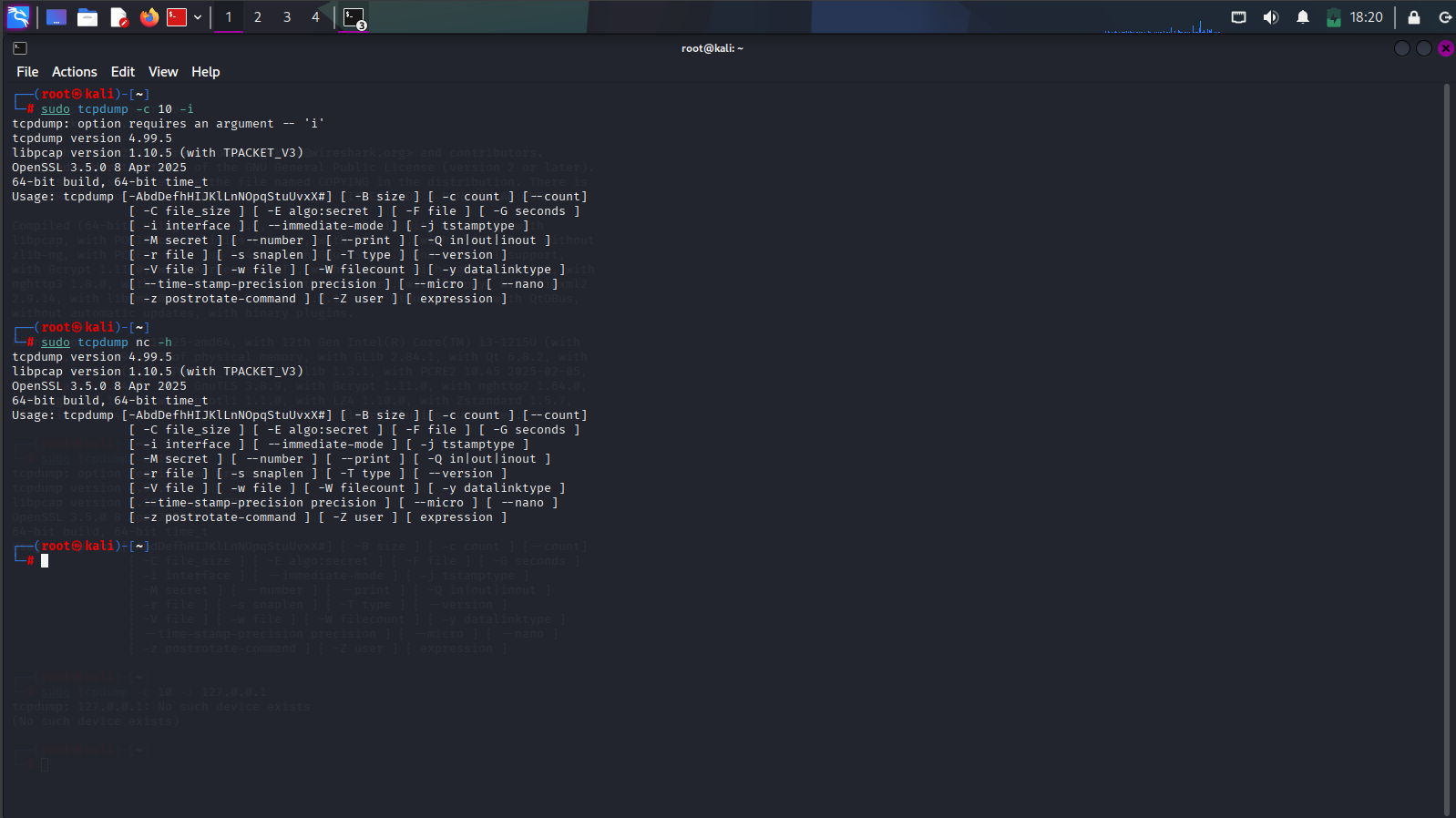
****

**Metasploit Version – v6.6.64 :** Metasploit's purpose is to act as a penetration testing framework, providing a collection of tools for identifying and exploiting security vulnerabilities, helping security professionals to test networks and systems, develop and execute exploit code, and ultimately improve system defence’s against attacks.

**Screenshots 9, 10 & 11: Nmap, Wireshark & Metasploit version check.**

**Additional Screenshots of Commands**

**Net Tools: tcpdump**

****

**Screenshot 12: Nettools version check**

**The setup was completed successfully. The Virtual Machine is now ready for use in further penetration testing and security tasks.**