BUILD YOUR PERSONAL CYBERSECURITY LAB

Task–2

Internship Program: Cyber Security & Ethical Hacking

Prepared by: Aditya Kamble

I. OBJECTIVE :

The objective of this task is to build a safe and isolated cybersecurity lab environment on a personal computer. This lab will serve as a foundation for performing vulnerability assessment, web application testing, and network validation in a controlled environment.

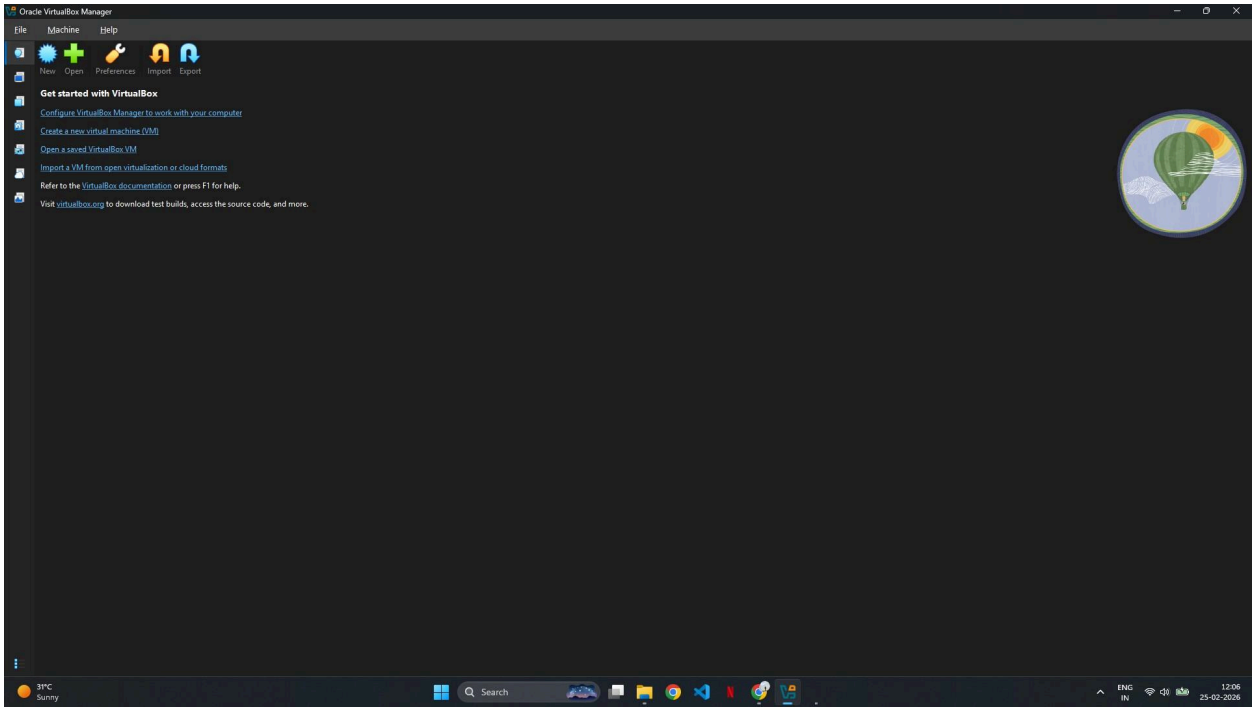
II. SYSTEM REQUIREMENTS :

The lab was built on a system with 16GB RAM and CPU virtualization enabled. Oracle VirtualBox was used as the virtualization platform to create isolated virtual machines.

III. STEPS :

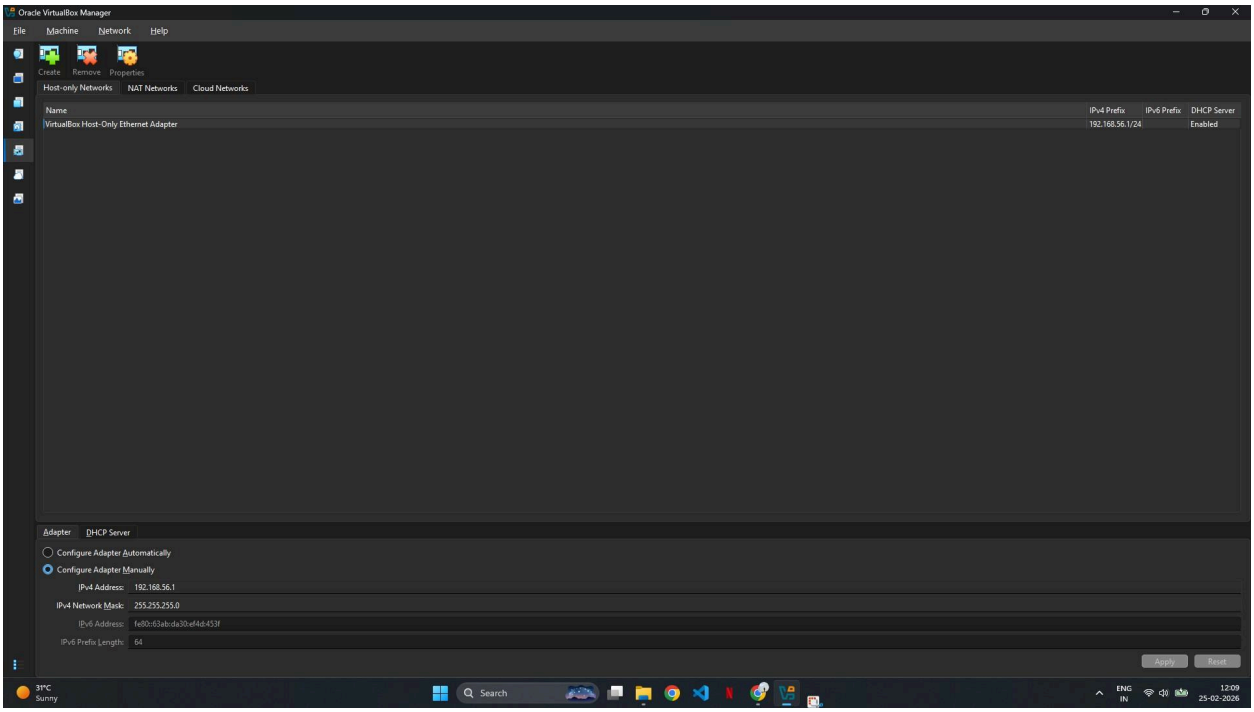
1. Installation of VirtualBox

VirtualBox was installed to create and manage virtual machines for the cybersecurity lab environment. Virtualization allows multiple isolated operating systems to run on a single physical machine, ensuring safe security testing without affecting the host system.



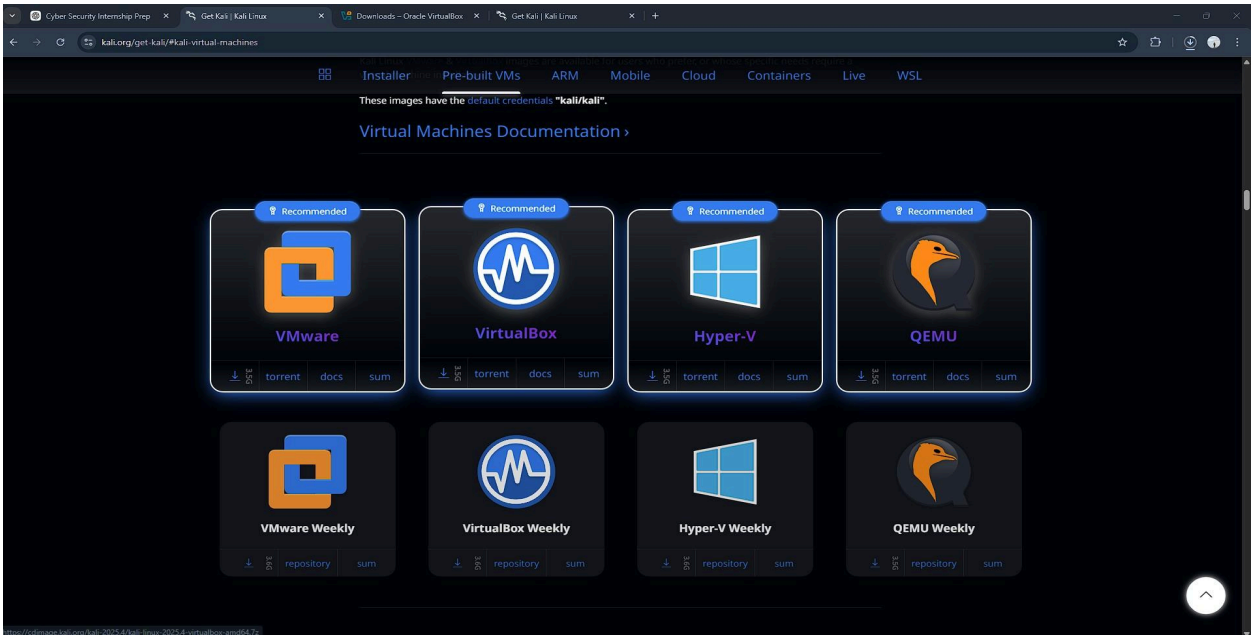
2. Network Configuration (NAT + Host-Only)

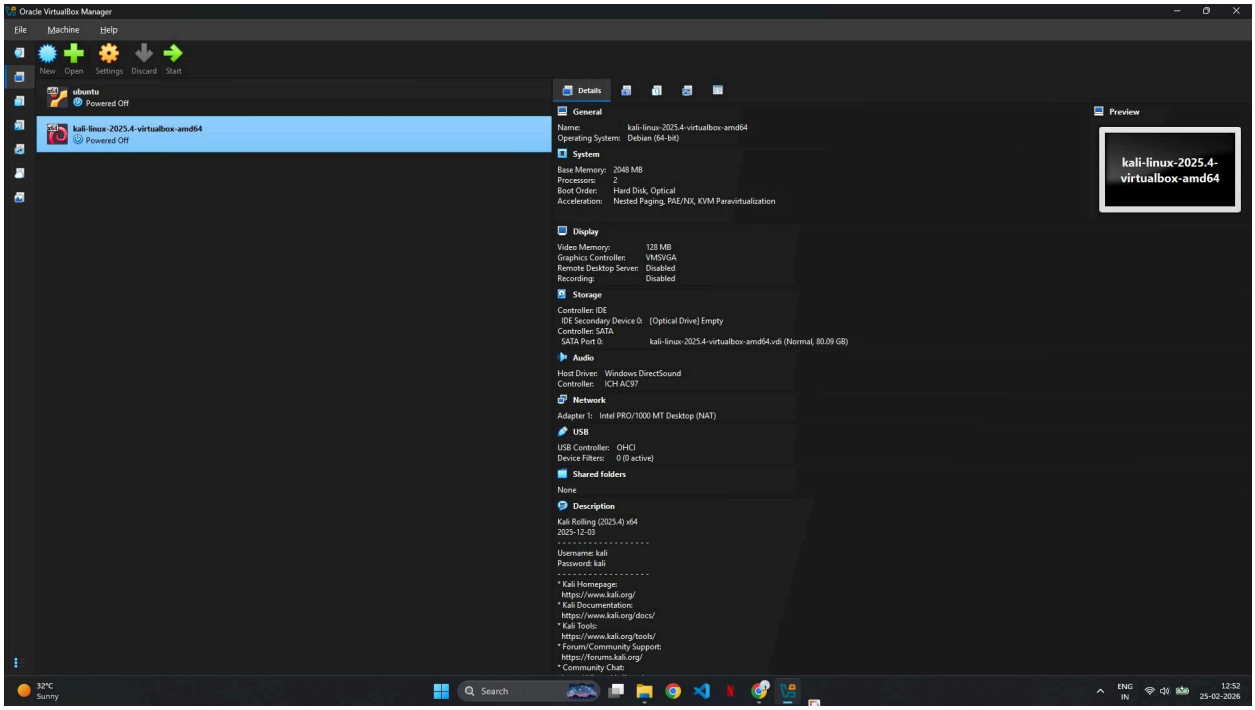
A Host-Only network was created to allow secure communication between the attacker and target machines within an isolated environment. This ensures that lab traffic does not interact with external networks. NAT is used to provide internet access for updates, while Host-Only enables internal lab communication.



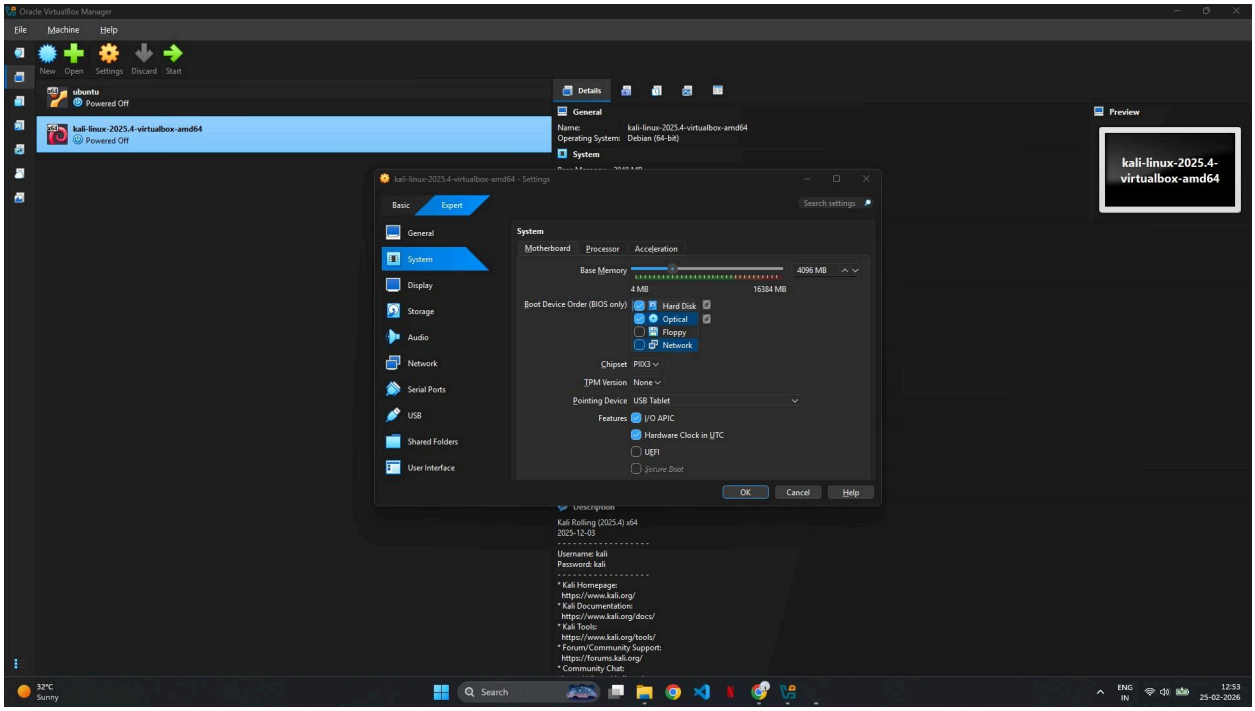
3. Deployment of Attacker Machine (Kali Linux)

i) Kali Linux was deployed as the attacker machine using a prebuilt VirtualBox image. The virtual machine was allocated 2 CPUs and 4GB RAM. Two network adapters were configured: NAT for internet connectivity and Host-Only for internal lab communication.

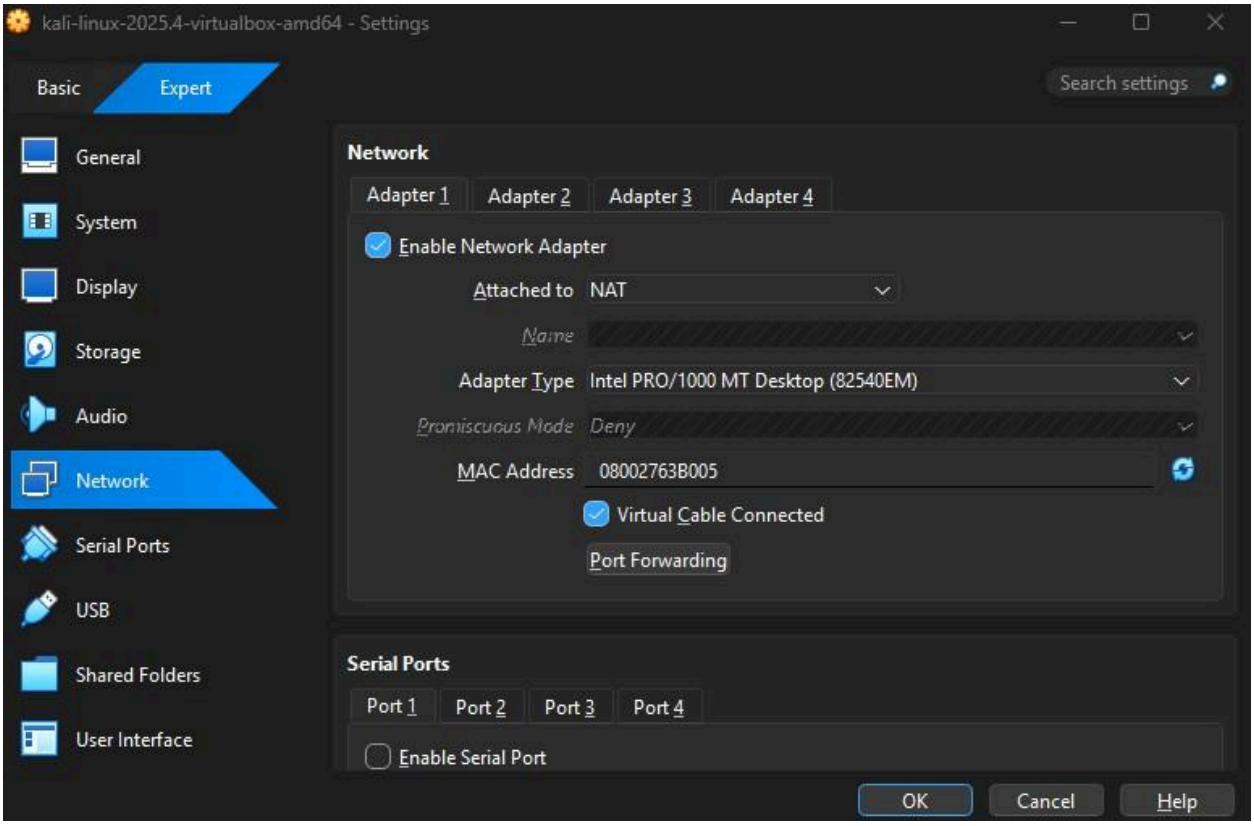


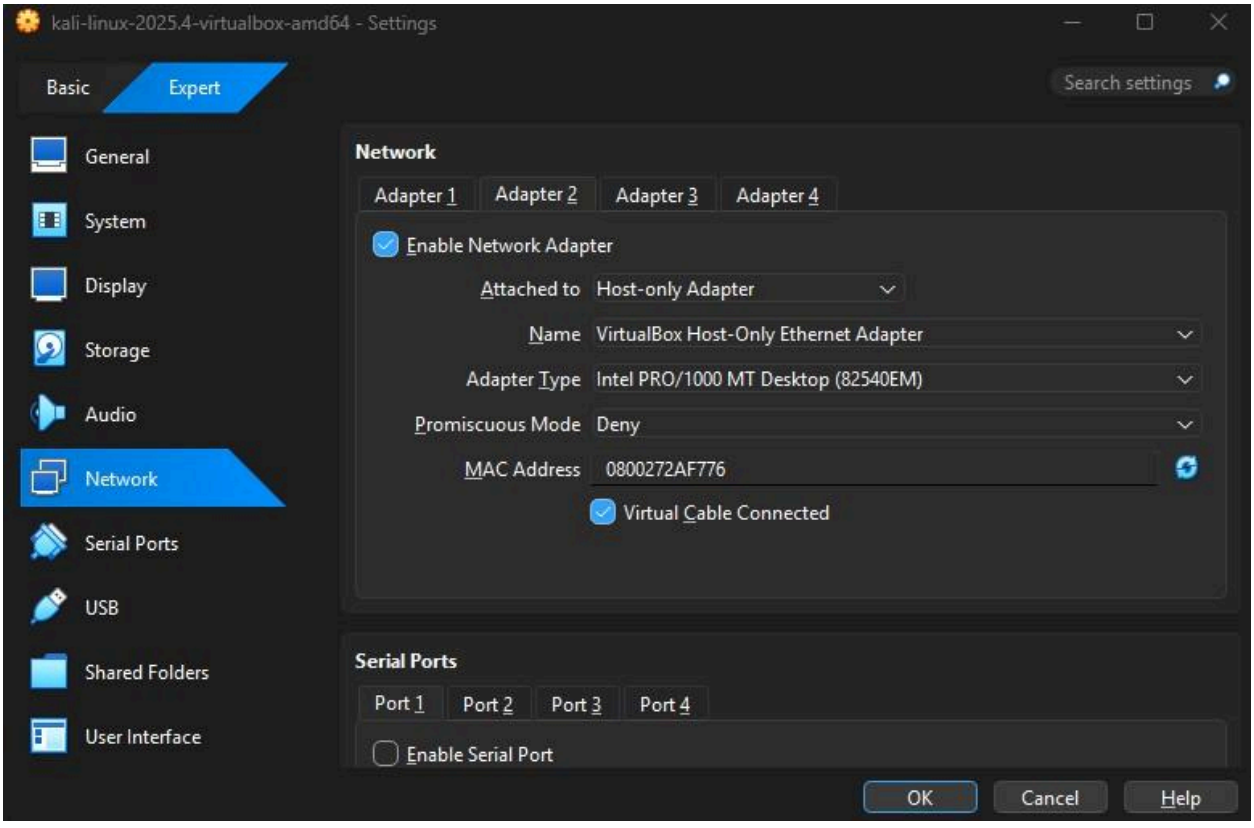


ii) The Kali Linux virtual machine memory was increased to 4GB (4096 MB) to ensure smooth performance during lab operations.



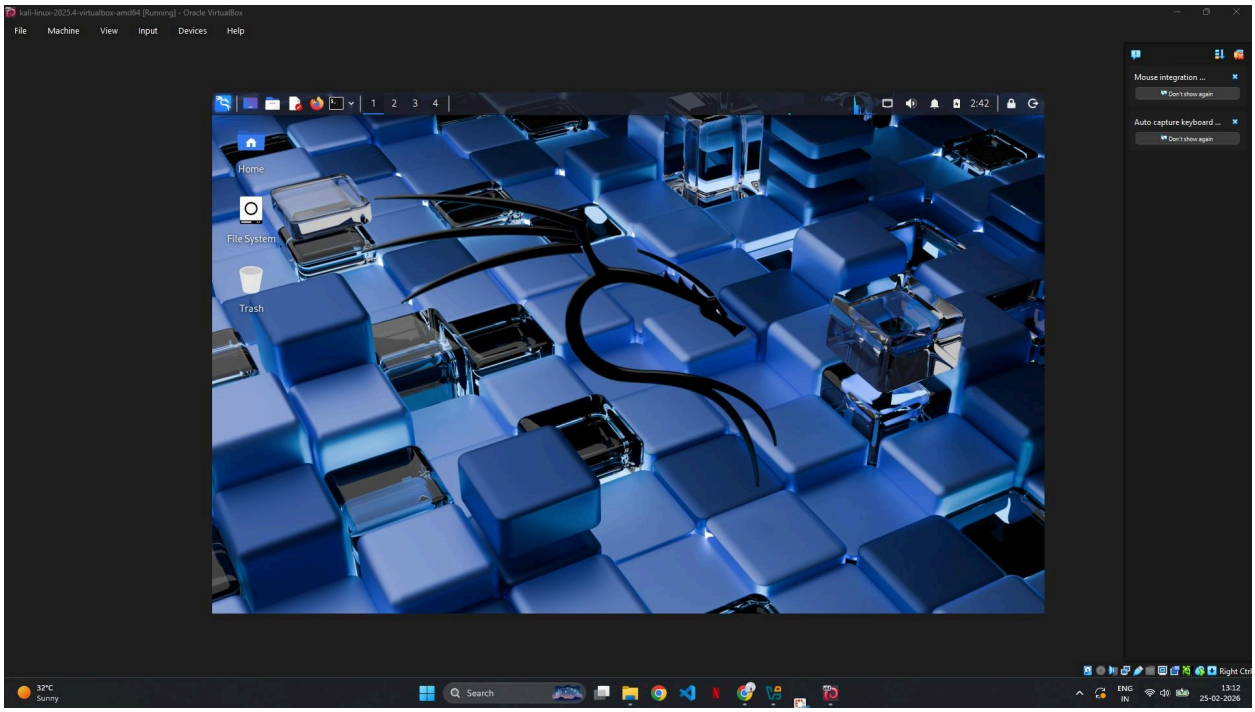
iii) Two network adapters were configured for Kali Linux. Adapter 1 was set to NAT to provide internet connectivity for updates, and Adapter 2 was set to Host-Only to enable secure internal communication within the lab environment.





4. Starting the Attacker Machine

The Kali Linux virtual machine was successfully started after resolving the network configuration issue. The system booted correctly and loaded the Kali desktop environment, confirming proper virtual machine setup.



5. IP Configuration Verification

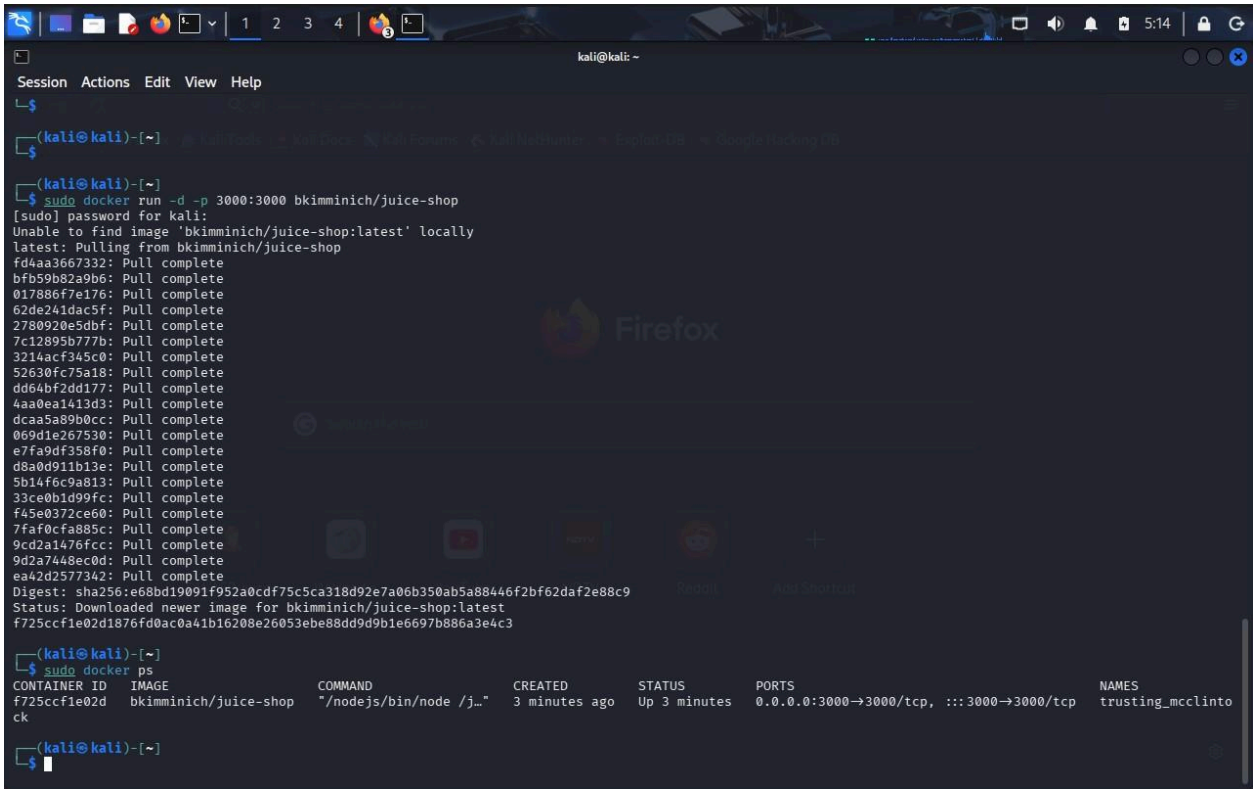
The `ip a` command was executed to verify network interfaces. The Kali Linux machine successfully obtained two IP addresses:

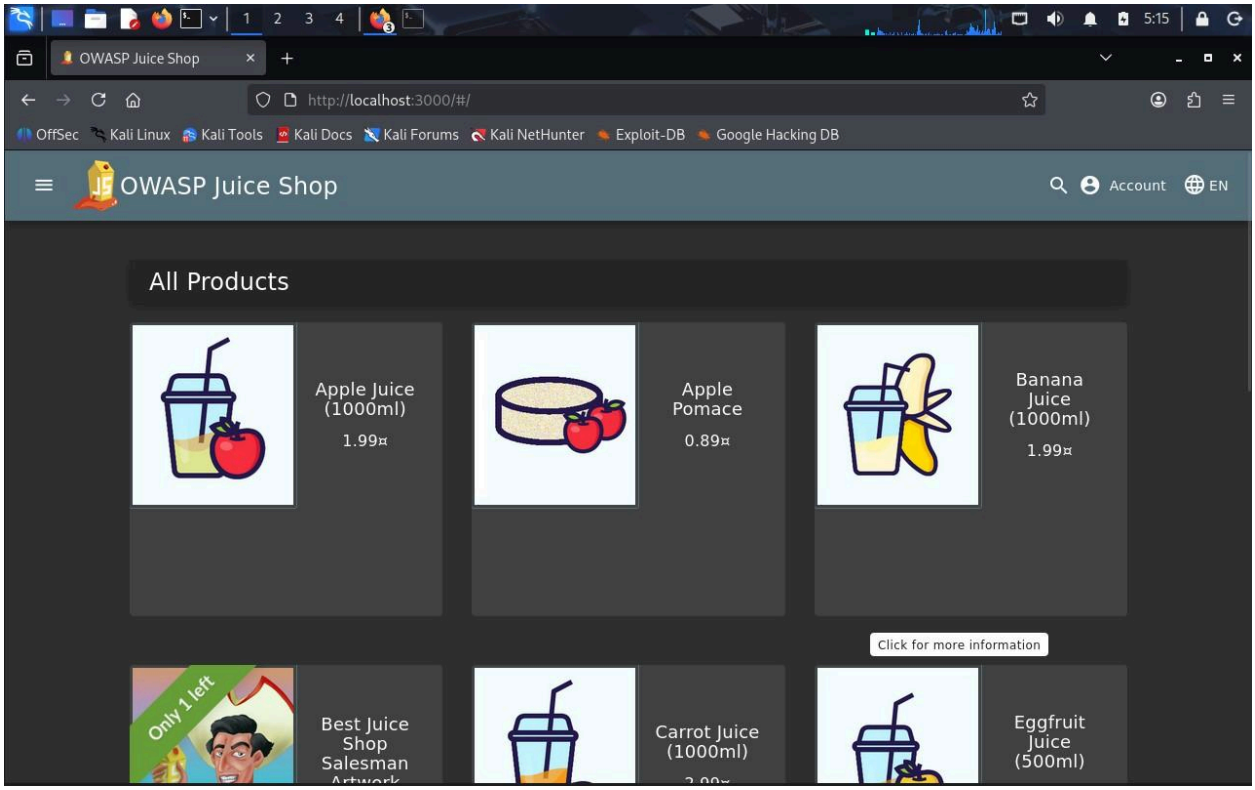
- 10.0.2.15 via NAT adapter (internet connectivity)
- 192.168.56.101 via Host-Only adapter (internal lab communication)

This confirms correct dual-network configuration for secure lab setup.

6. Deployment of Vulnerable Web Application

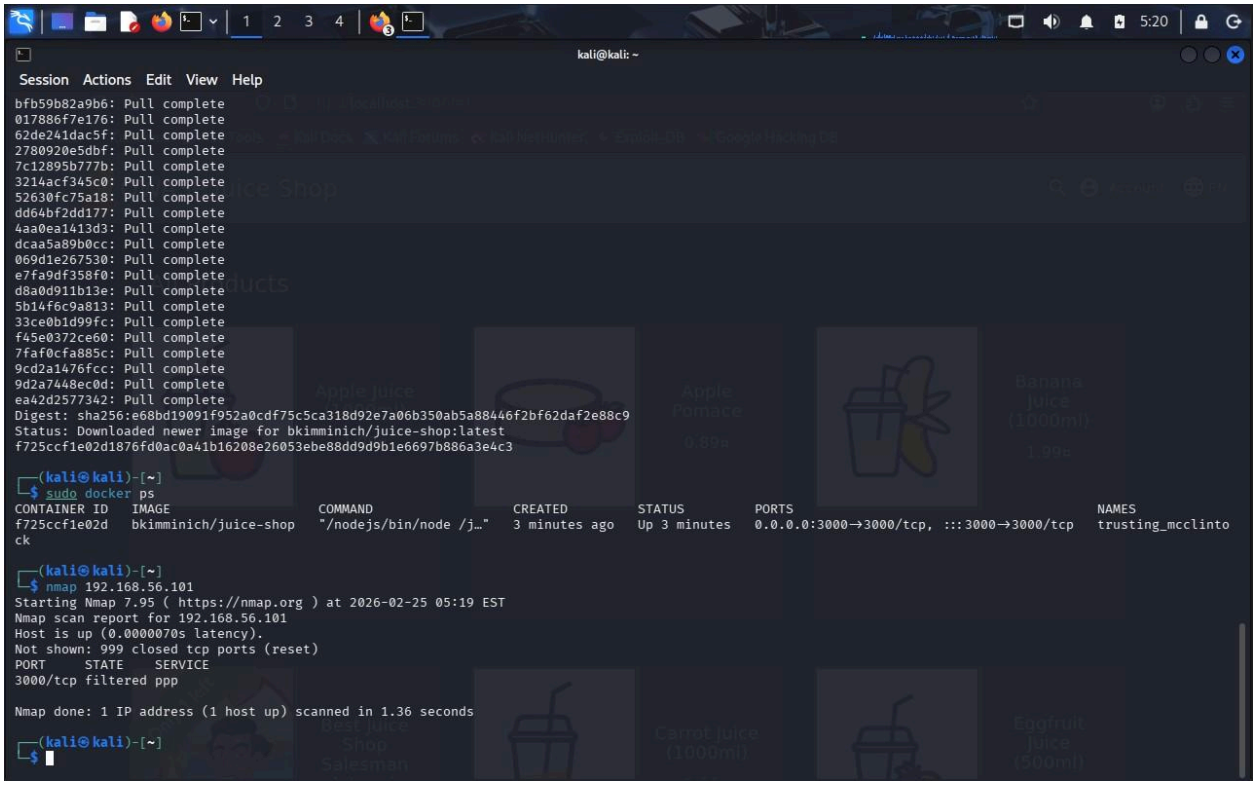
OWASP Juice Shop was deployed using Docker within the Kali Linux environment. The container was launched on port 3000 and verified using the `docker ps` command. The application was successfully accessed via web browser, confirming proper target deployment.





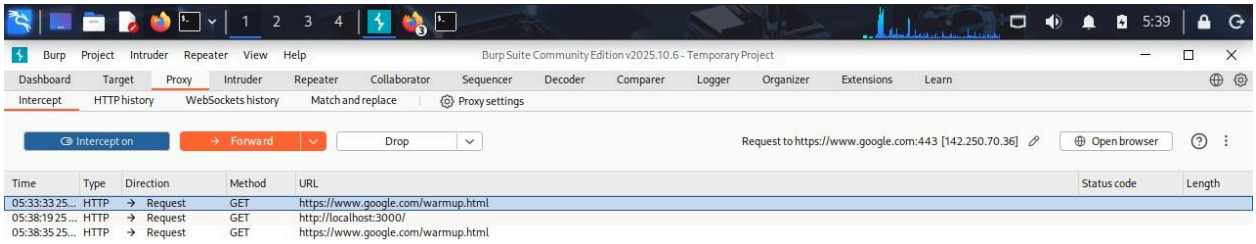
7. Network Validation Using Nmap

A network scan was performed using Nmap against the Host-Only IP address (192.168.56.101). The scan confirmed that the host was active and port 3000 was detected. This validates that the vulnerable web application is reachable within the lab environment.



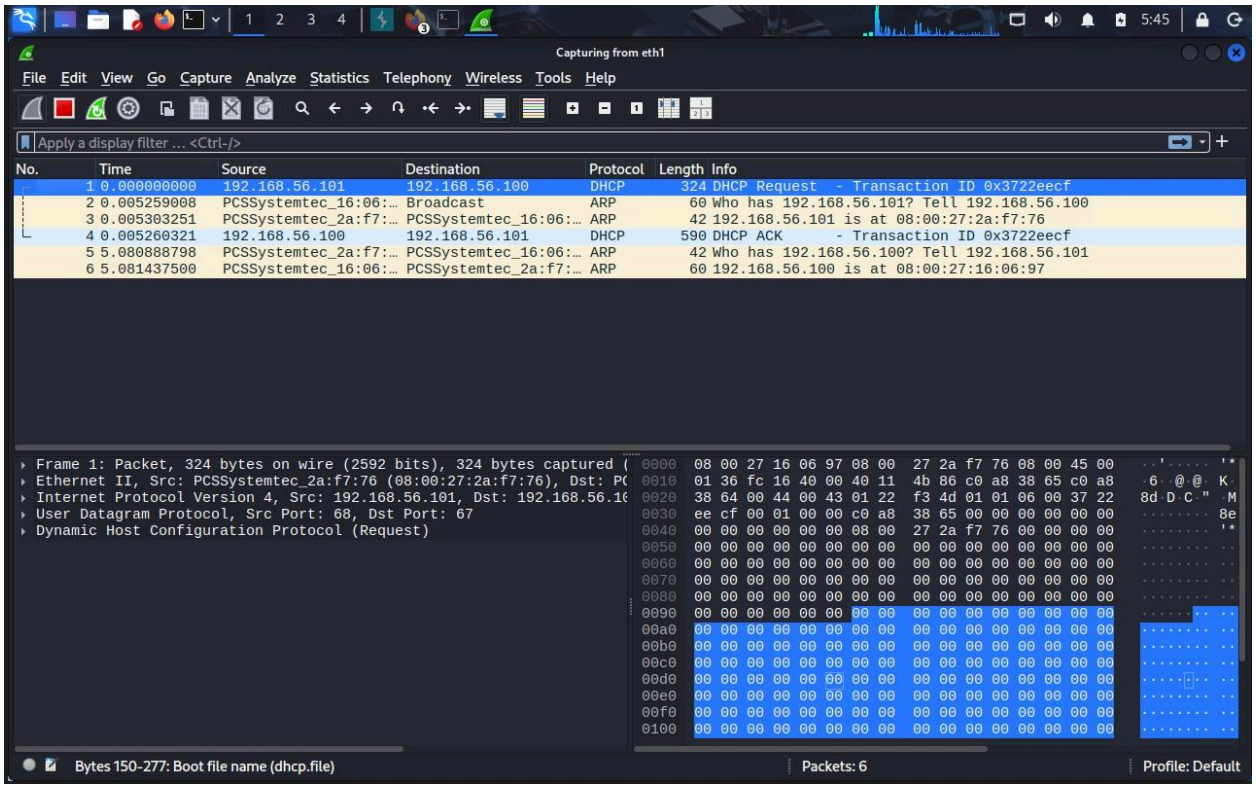
8. Traffic Interception Using Burp Suite

Burp Suite was configured as a local proxy (127.0.0.1:8080) to intercept HTTP traffic from the browser. When accessing OWASP Juice Shop, HTTP requests to `localhost:3000` were successfully captured. This confirms proper proxy configuration and successful traffic interception within the lab environment.



9. Packet Capture Using Wireshark

Wireshark was used to monitor traffic on the Host-Only interface (eth1). During lab activity, DHCP and ARP packets within the 192.168.56.x subnet were captured. This confirms successful internal network communication and packet-level monitoring within the isolated cybersecurity lab.



CONCLUSION :

The objective of this task was to design and deploy a secure and isolated cybersecurity lab environment using virtualization technologies. The lab was successfully built using Oracle VirtualBox with Kali Linux as the attacker machine and OWASP Juice Shop as the intentionally vulnerable target application.

A dual-network configuration was implemented using NAT and Host-Only adapters to ensure both internet connectivity and secure internal communication. Network validation was performed using Nmap to confirm service availability, Burp Suite to intercept HTTP traffic, and Wireshark to capture packet-level communication within the isolated lab network.

The successful deployment and validation of all components demonstrate a foundational understanding of virtualization, networking configuration, traffic analysis, and secure lab isolation. This lab environment now serves as a practical platform for future vulnerability assessment, penetration testing, and cybersecurity experimentation in a controlled and safe manner.