Lab Setup

For this task, I created a controlled lab environment to simulate real-world cyberattacks and defenses. The setup included:

Host System: Kali Linux as the main operating system, used for attack simulation, payload generation, and monitoring.

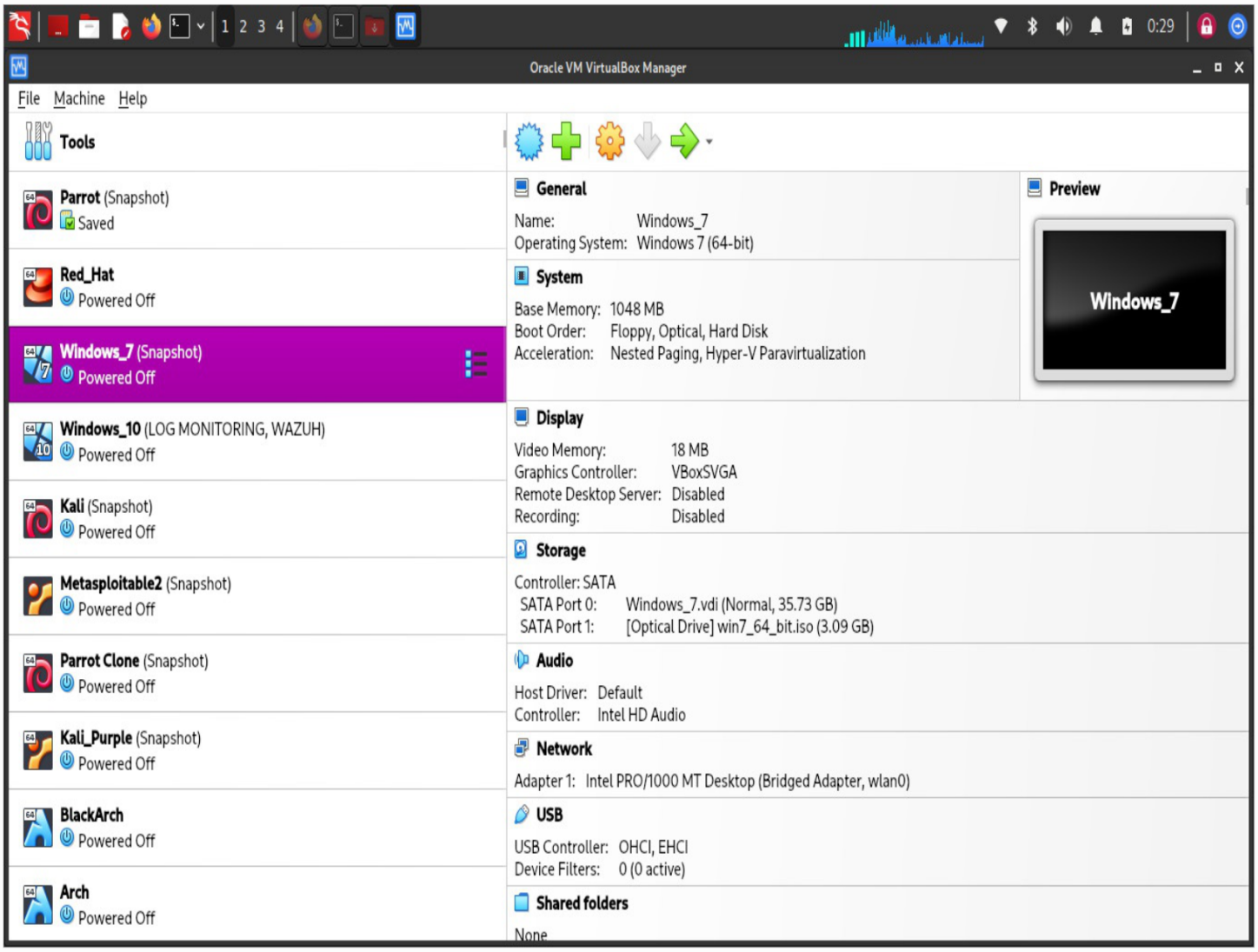
Hypervisor: VirtualBox to virtualize and manage multiple virtual machines.

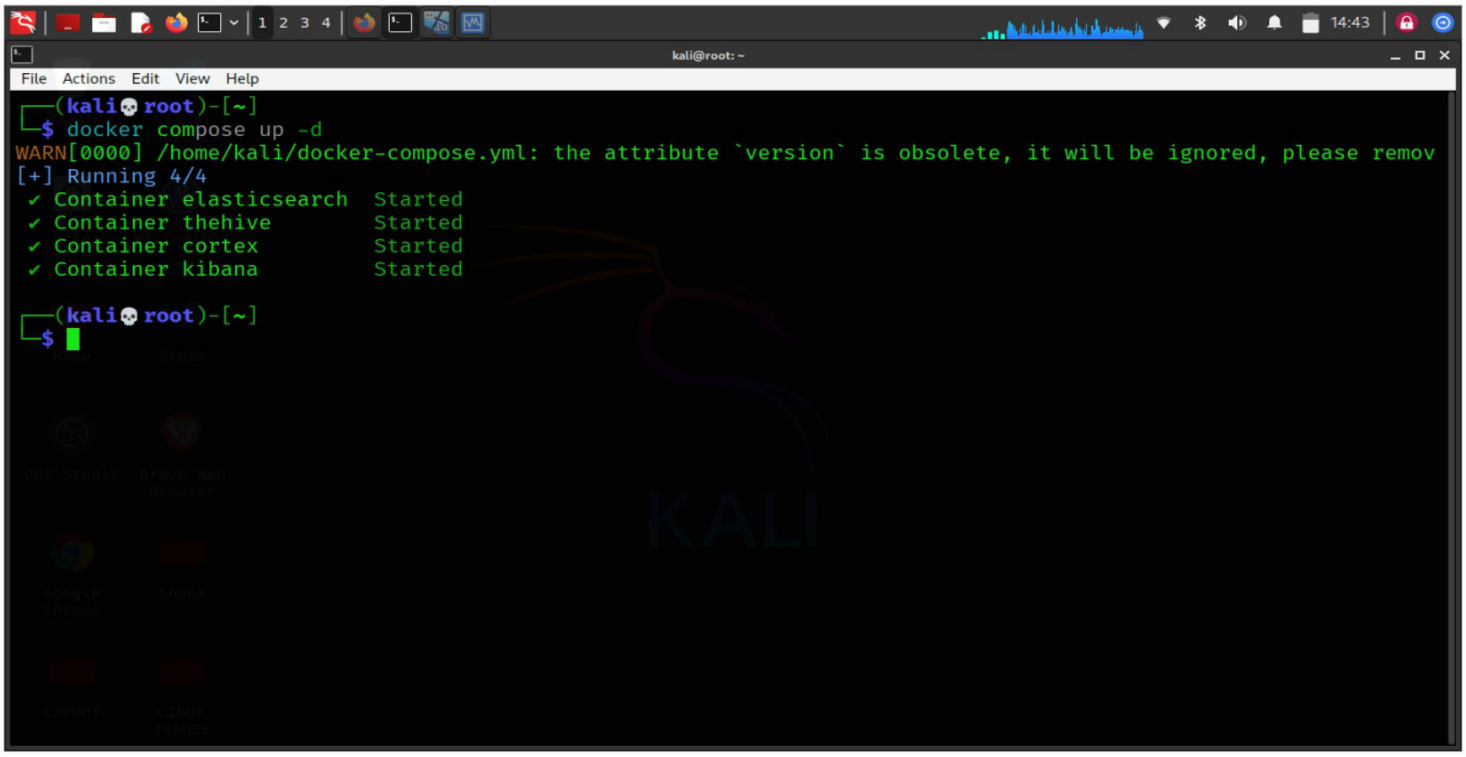
Virtual Machines:

- ☐ Kali Linux VM – attacker machine with Metasploit and supporting tools.

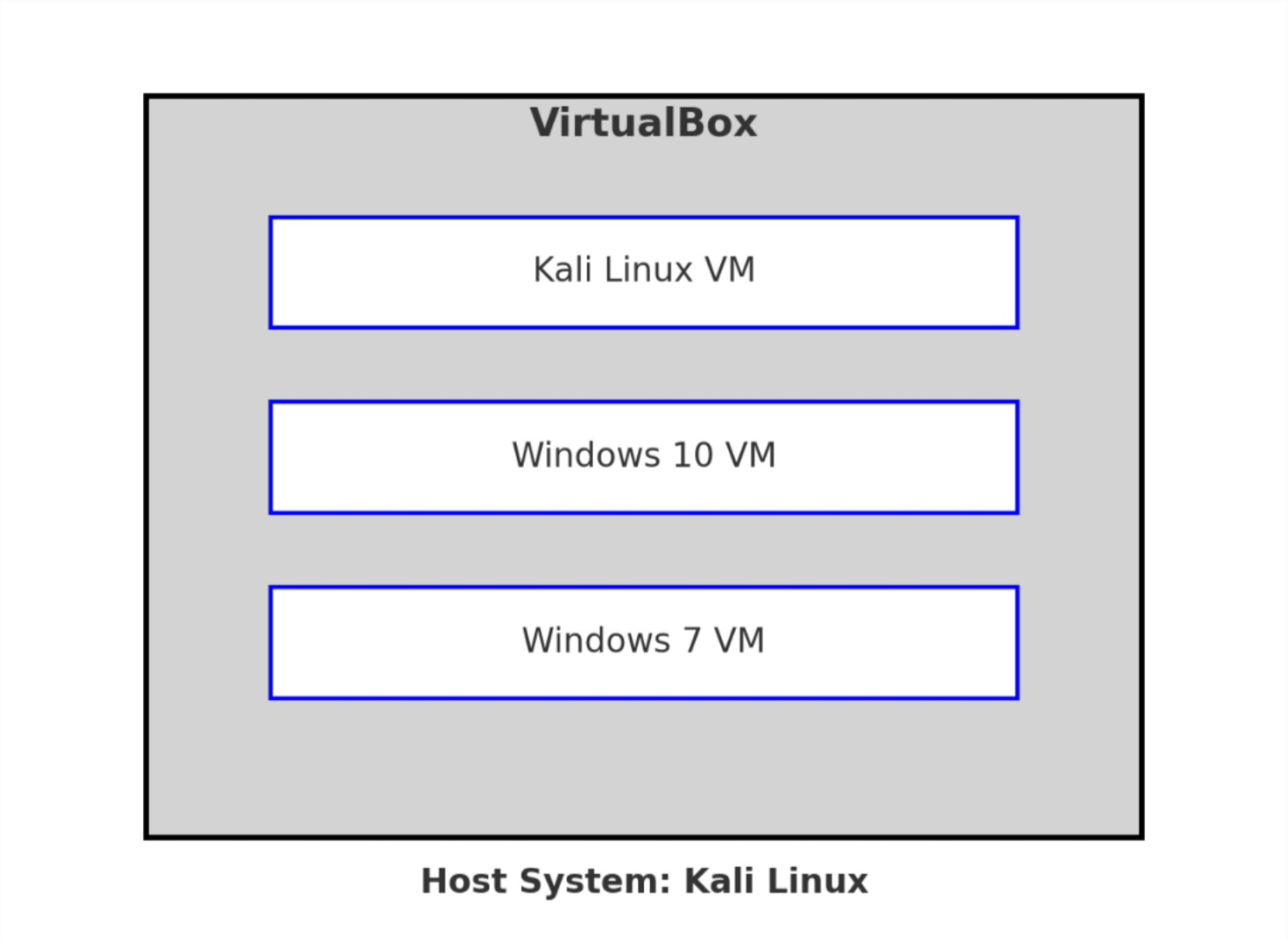
- ☐ Windows 7 VM – legacy victim system for phishing and exploit testing.

- ☐ **Windows 10 VM** – target system for payload execution, persistence, privilege escalation, and exfiltration.





Containerized SIEM Stack: I deployed Elastic, Kibana, Cortex, TheHive, and Wazuh using Docker containers orchestrated with a docker-compose.yaml file. This ensured smooth integration of threat detection, log correlation, and incident investigation.



This lab allowed me to replicate Red Team attack scenarios and Blue Team detection & mitigation workflows in an isolated and safe environment.