

Cybersecurity Home Lab Setup (Comprehensive Step-by-Step Guide)

Overview

This document provides a fully detailed, professional, and structured walkthrough of how I built my personal cybersecurity virtual lab environment from scratch.

It includes expanded explanations, configuration guidance, best practices and tool recommendations.

This lab is suitable for penetration testing, malware analysis, SOC monitoring, incident response training, and general cybersecurity skill development.

1. System Requirements

Before building the lab, ensure you have hardware and software that can support multiple virtual machines running simultaneously.

Hardware Requirements:

- Processor: Intel i5/i7 or AMD equivalent with virtualization support (VT-x / AMD-V)
- Memory (RAM): Minimum 16GB (32GB recommended for advanced labs)
- Storage: Minimum 200GB free space (SSD highly recommended)
- Network: Stable connection for updates and package installations

Software Requirements:

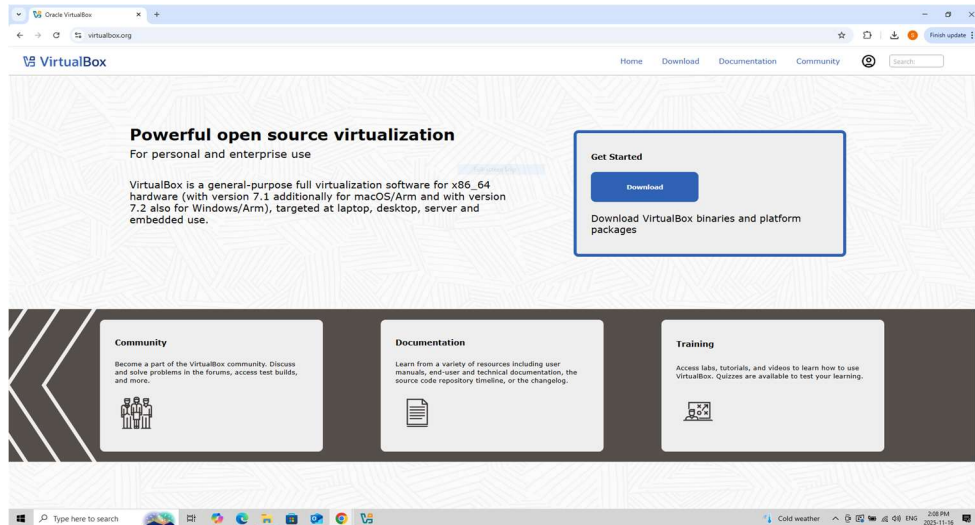
- VirtualBox (free)
Operating system images:
 - Kali Linux (latest)
 - Window server
 - Ubuntu Server
 - Parrot Machine
 - Windows 8.1 ISO or higher
 - pfSense Firewall

2. Install Hypervisor (VirtualBox)

The hypervisor is the foundation of your lab environment, enabling multiple virtual machines to run simultaneously.

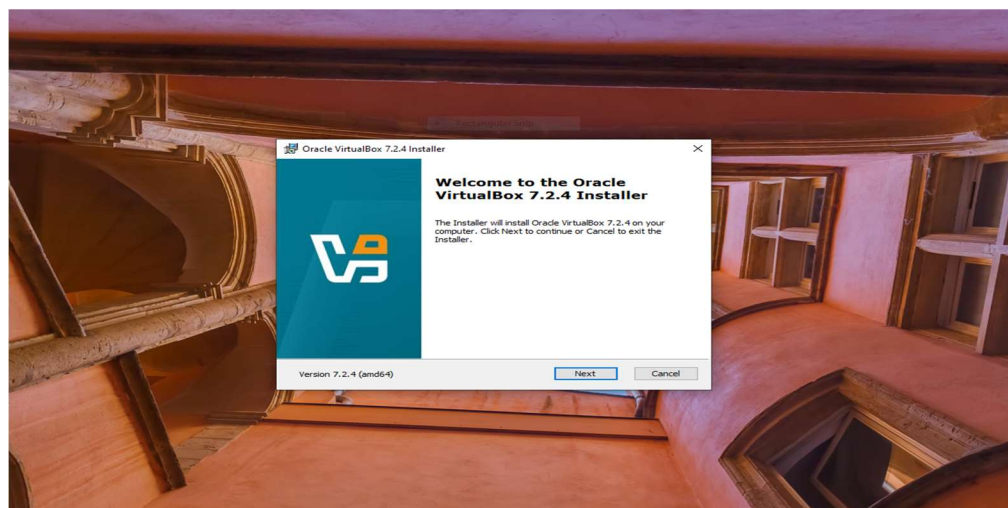
Step 1 — Download VirtualBox

Visit the official website and download the version for your operating system.



Step 2 — Install VirtualBox

Follow the installation wizard and accept default settings unless customization is required.

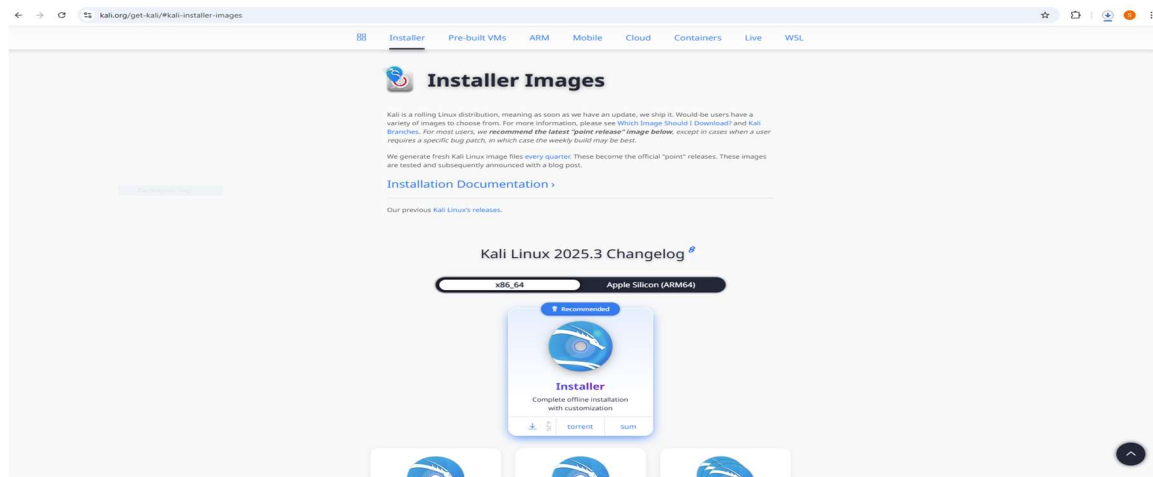


3. Set Up Kali Linux Virtual Machine

Kali Linux will serve as your primary penetration testing machine.

Step 1 — Download Kali ISO or OVA

Visit <https://www.kali.org/get-kali/>.



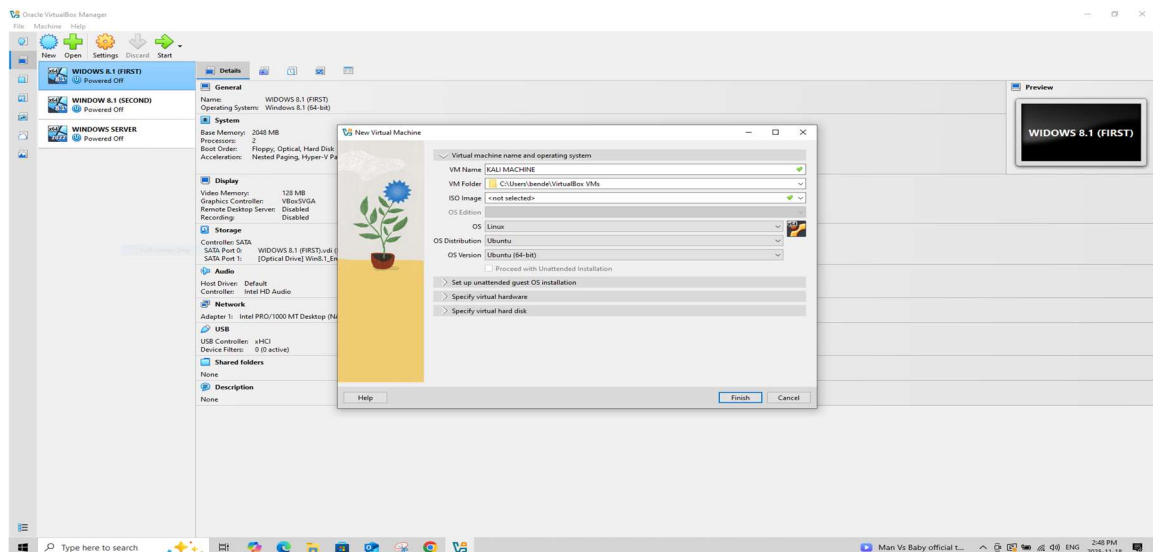
Step 2 — Create and Configure the VM

Assign the following recommended resources:

- RAM: 1GB–8GB

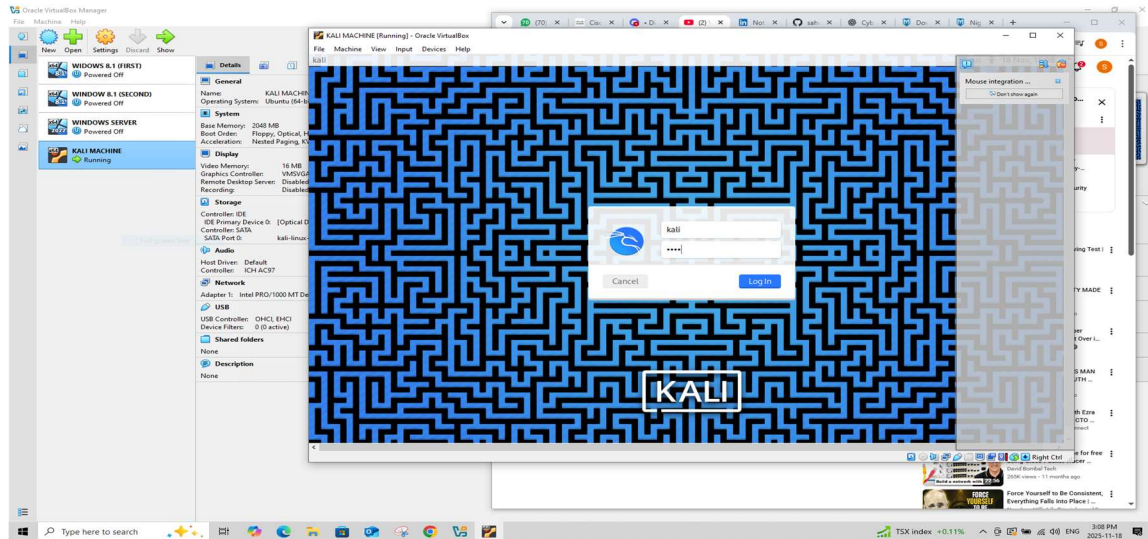
- CPU: 1–4 cores

- Storage: 40GB+



Step 3 — Install Kali Linux

Proceed through the installation wizard, set up a username, timezone, and partitioning options.

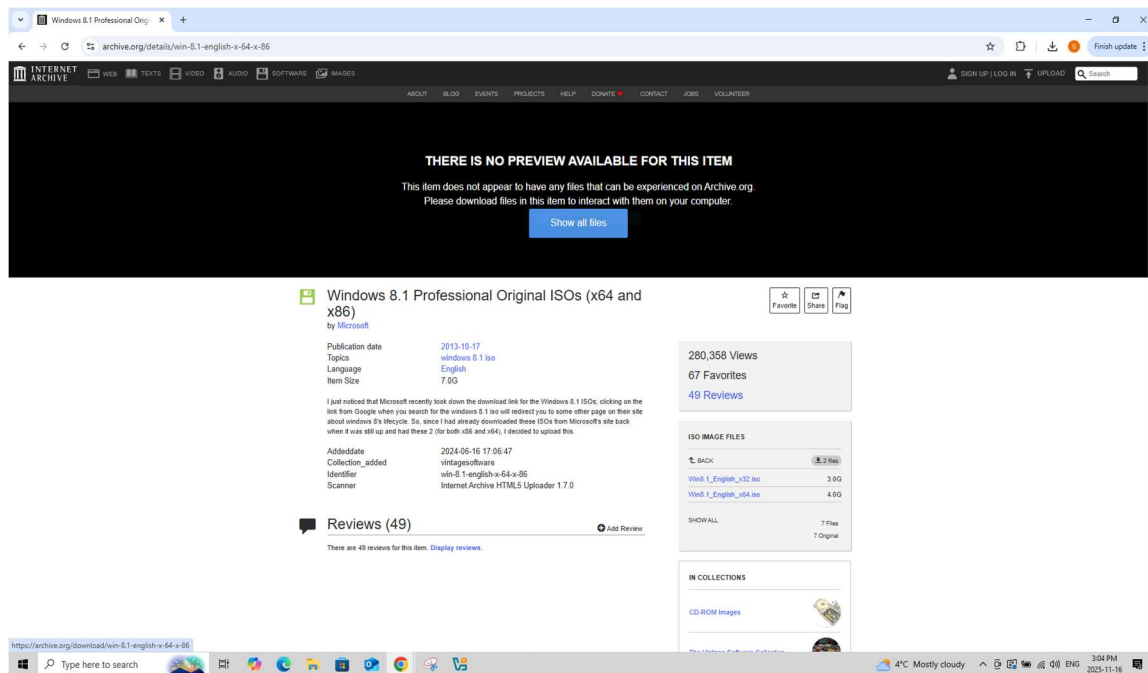


4. Set Up Windows Virtual Machine

Windows is essential for understanding malware behavior, SOC tools, and endpoint security.

Step 1 — Download Windows ISO

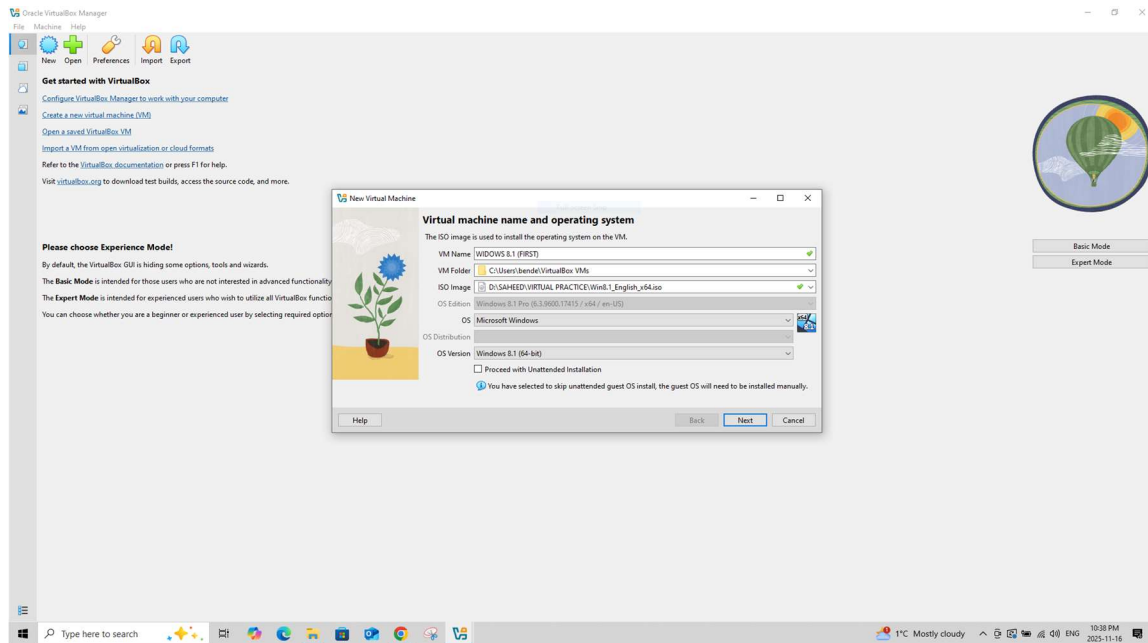
Download from Microsoft official website.



Step 2 — Create Windows VM

Assign:

- RAM: 1GB–4GB
- CPU: 1–4 cores
- Network adapters: NAT NETWORK



5. Configure Lab Network

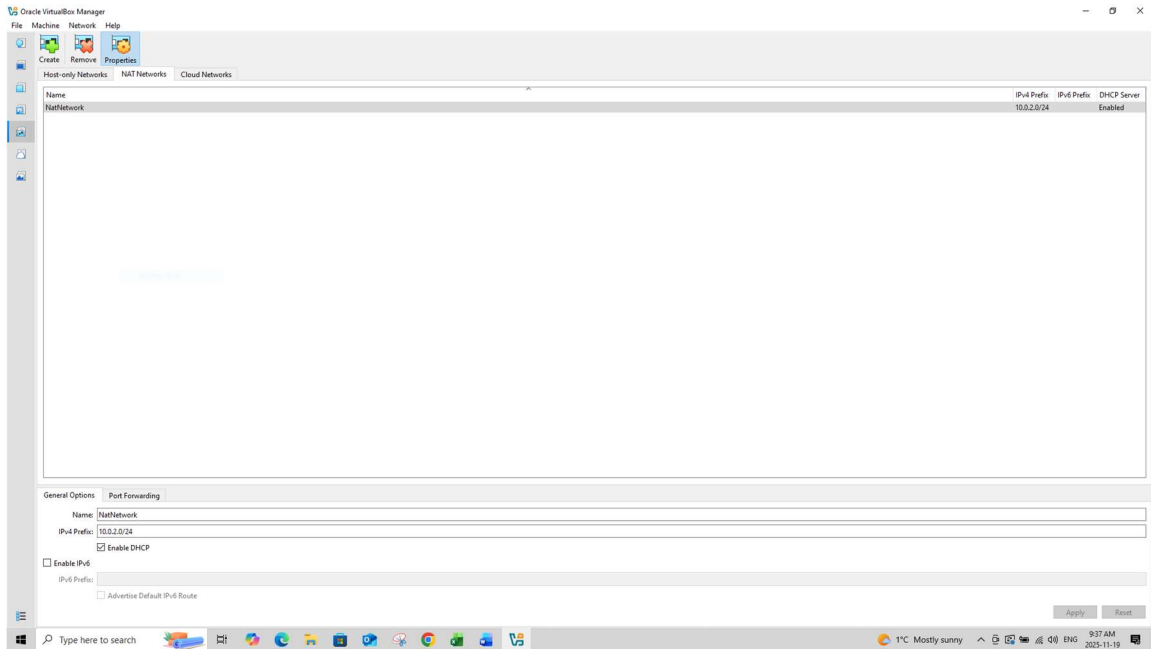
A well-configured network allows safe testing without affecting your main system.

Recommended Network Setup:

- NAT Network: Internet access for updates

Best Practices:

- Assign static IPs for predictability
- Document all IP addresses for future testing
- Disable unwanted communication paths



6. Conclusion

This fully established cybersecurity lab enables hands-on learning in:

- Penetration Testing
- Vulnerability Analysis
- Malware Research (controlled)
- SOC and Incident Response
- Network Traffic Monitoring
- Blue Team Defense Techniques

The modular setup allows unlimited expansion as skills grow.

Thank you