

Forum:[Hack Forums](#)

Thread: [Build a Safe Home Pentest Lab](#)

Vectura - October 2, 2025, 3:58 pm

Build a Safe Home Pentest Lab (VirtualBox / VMs)

Intro:

Want to learn security testing without breaking the law? This guide shows how to build an isolated, repeatable homelab with VirtualBox/VMware, vulnerable targets for practice, and network segmentation. Everything here is for legal, self-hosted learning only.

Prerequisites: Desktop or laptop with at least 16GB RAM (8GB minimum)

VirtualBox or VMware Workstation Player

ISO images for Kali Linux, Ubuntu/Windows test VMs

A vulnerable lab VM (OWASP Juice Shop, Metasploitable, DVWA)

Steps:

Install Virtualization Software

- Download VirtualBox/VMware and install. Create a dedicated folder for VM disks.

Create Network Topology

- Use Host-Only for attacker <-> target; NAT for internet access on a separate VM (if needed).

Use snapshots for quick resets.

Example VirtualBox networking:

Code - Host-only Adapter -> 192.168.56.0/24 (attacker & targets)

- NAT Adapter -> (optional) internet access via host Deploy Base VMs

- Kali Linux (attacker): allocate 2–4 vCPU, 4–8GB RAM
- Target VMs: Metasploitable / Juice Shop (small resources)

Harden Host & Isolate Lab

- Disable shared folders/clipboard between host and VMs
- Use snapshots: take one when VM is fresh

Install Tools (safe list)

- nmap, Wireshark, Burp (Community), Gobuster, sqlmap (in lab only)

Code sudo apt update && sudo apt install nmap wireshark burpsuite Create Playbook

- Document test goals, allowed actions, restore procedures

Practice Exercises (lab only)

- Web app mapping: use Burp + browser to explore Juice Shop

Safety & Legal:

Always test only in your own isolated environment. Do not scan or attack systems you do not own or have explicit permission to test.

Post Questions below — share screenshots of your lab setup!