# Home Security Lab Report

Author: Alexander T. Ramos | Date: October 05, 2025

Overview:
This document describes the configuration and purpose of the Home Security Lab used for SOC practice, vulnerability scanning, and incident response simulations.

Host System:
Windows 10 Pro Laptop (Primary Host) — 32GB RAM, VirtualBox 7.0

Key Virtual Machines:
- Kali Linux (Attacker)
- Metasploitable 2 (Vulnerable Target)
- Ubuntu (DVWA) (Web App Testing)
- Windows 10 Lab VM (SOC workstation)
- Security Onion (IDS/SIEM)

Network Topology:
Lab uses NAT for internet access, an internal isolated network for testing, and host-only adapters for log collection and monitoring.

Tools and Use Cases:
- Splunk (Log aggregation & dashboards)
- Security Onion (Zeek/Suricata/Wazuh)
- Nessus/OpenVAS (Vulnerability Scanning)
- Metasploit, Nmap, Wireshark (Offensive/DFIR)

Maintenance and Best Practices:
- Take snapshots before major tests - Revert to clean snapshots after experiments - Keep tools and OS patched - Document experiments and results in GitHub