Building a Kali Linux Hacking Lab for Ethical Penetration Testing

Overview

This project involved creating a secure, self-contained hacking lab using Kali Linux to practice ethical hacking and penetration testing techniques. The goal was to simulate real-world cybersecurity environments in a legal, controlled space and to gain hands-on experience with common exploits, tools, and testing methods used by cybersecurity professionals.

Tools & Technologies Used

- Kali Linux (Debian-based penetration testing distribution)
- VirtualBox (Virtualization software)
- Metasploitable2 (Intentionally vulnerable Linux machine)
- DVWA (Damn Vulnerable Web Application)
- Nmap, Metasploit, Burp Suite, Wireshark

Lab Setup Process

1. Installed Oracle VirtualBox on host machine (Windows 11, 8GB RAM, 256GB SSD)
2. Downloaded Kali Linux ISO and installed it as a virtual machine
3. Imported Metasploitable2 as the vulnerable target VM
4. Set both VMs to Host-Only Adapter for safe, local network traffic

Hacking & Testing Scenarios

- Scanned open ports using Nmap to identify vulnerable services
- Used Metasploit to exploit FTP vulnerabilities and gain shell access
- Used Burp Suite to intercept HTTP traffic and simulate XSS/SQL injections
- Captured packets using Wireshark to observe insecure network activity

Key Learnings

- How to set up a virtual penetration testing lab safely and legally
- Gained hands-on experience with core cybersecurity tools
- Understood how to identify, exploit, and document vulnerabilities
- Learned the value of documentation and structured testing

Screenshots & Documentation (To Include)

- Kali Linux VM terminal showing active tools

- Exploit output (e.g., shell access from Metasploit)
- Burp Suite request/response view
- Wireshark packet capture display
- VirtualBox settings for both Kali and Metasploitable