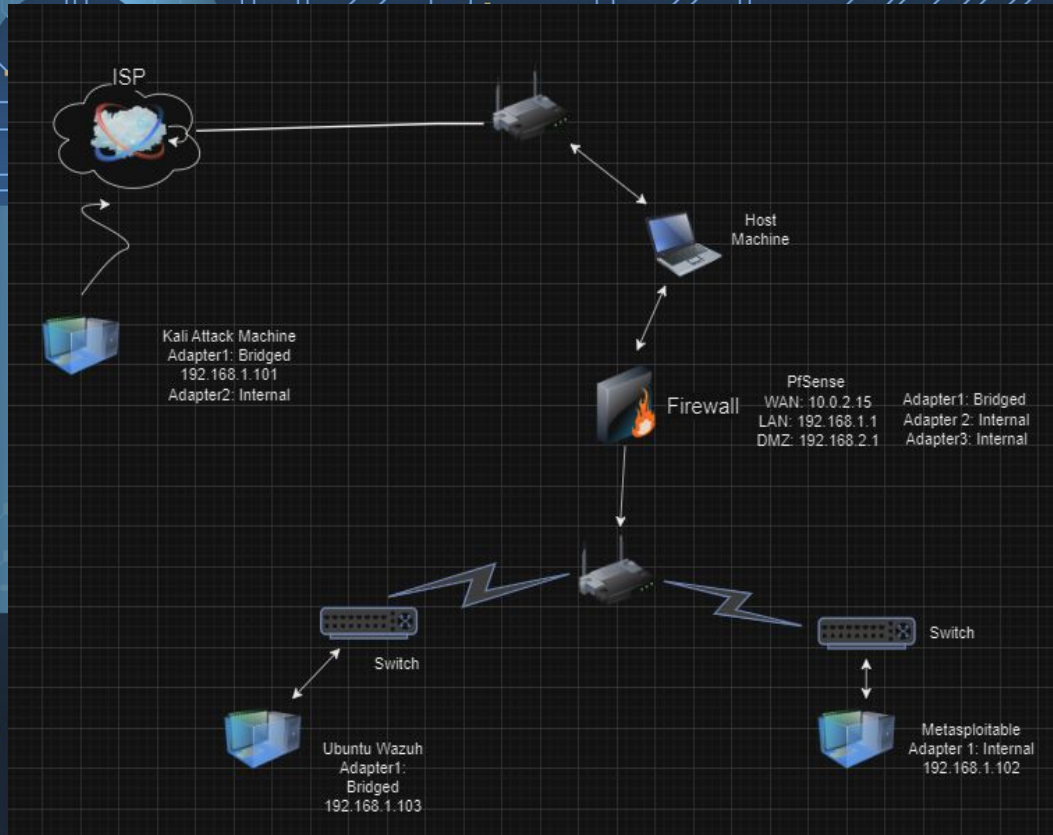
Home Virtual Training Lab

Margaret Edwards

Components of Home Lab

- Attack Machine
  - Kali Linux
- Firewall
  - PfSesnse
- IDS/IPS
  - Snort
- SIEM Tool
  - Wazuh (Ubuntu)
- Target VM machine
  - Metasploitable



Kali Linux - Attack Machine

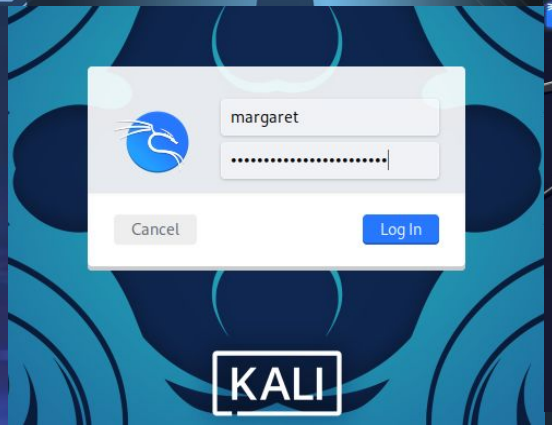
Kali Linux is a powerful Debian-based Linux distribution designed for digital forensics, ethical hacking and penetration testing.

Use Case:

- Simulate real-world cyber attacks.
- Understand offensive strategies and techniques.
- Develop and enhance ethical hacking skills.

Benefit:

- Practical experience in offensive cybersecurity.
- Hands-on exploration of diverse attack scenarios.



PfSense - Firewall

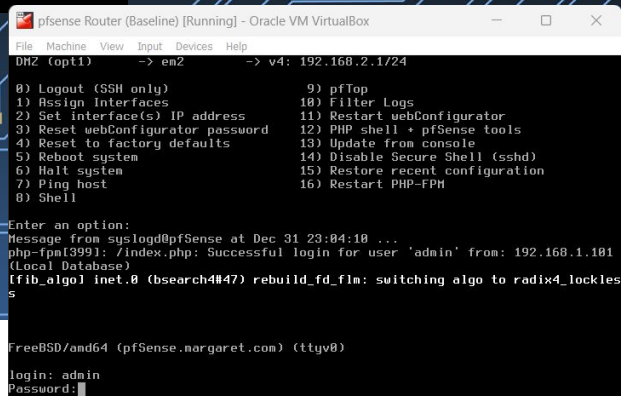
PfSense is an open-source firewall/router that is used to ensure network security.

Use Case:

- Creates a secure perimeter around our network
- Customizable network policies in order to tailor defenses to specific needs
- Controls incoming and outgoing traffic

Benefit:

- Protects against unauthorized access
- Mitigates potential threats at the network level



Snort - IDS/IPS

Snort is an Open-Source Intrusion Detection and Prevention System (IDS/IPS) with real time traffic analysis. Snort uses signature based detection and content matching for threat identification.

Use Case:

- Detects and prevents malicious activity on our network
- Analyzes and responds to security incidents.
- Conduct forensic analysis for investigation

Benefit:

- Proactive defense against potential threats
- Provides real-time monitoring and alerting

Wazuh SIEM Tool

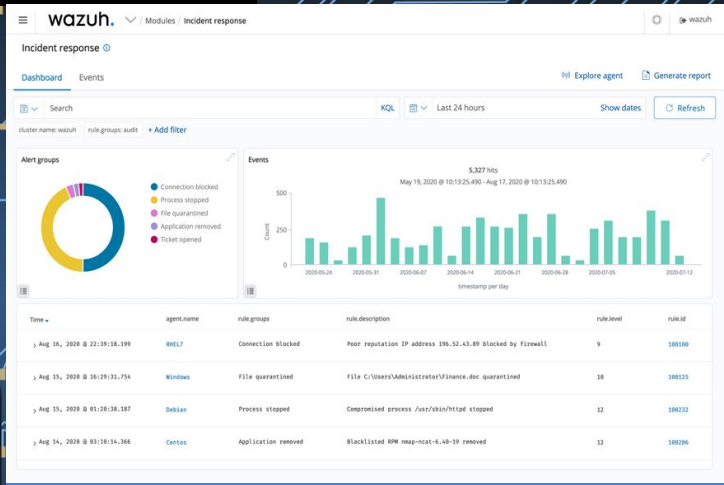
Wazuh is an Open-Source Security Information and Event Management Tool (SIEM) that is used for collecting and analyzing security event data.

Use Case:

- Platform used for threat detection and response
- Correlate events, identify patterns and monitor security posture
- Generate compliance reports for regulatory requirements

Benefit:

- Comprehensive visibility into security events
- Effective incident response and management



Metasploitable2 - Target/Victim Machine

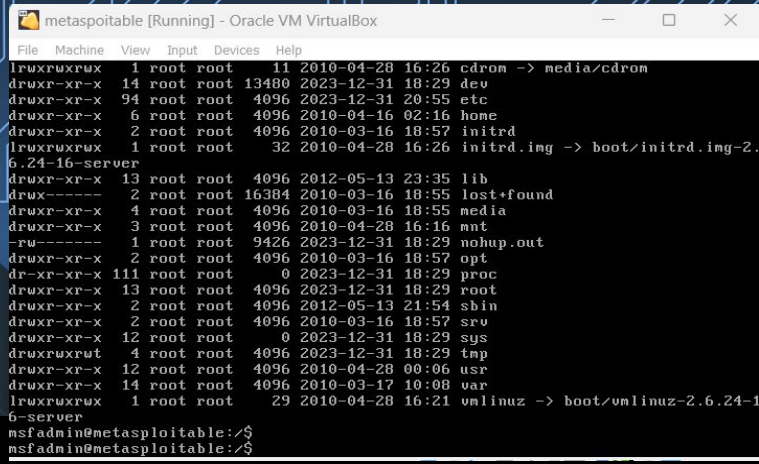
Intentionally vulnerable virtual machine that simulates a range of vulnerabilities for ethical hacking practice. Built specifically for security professionals.

Use Case:

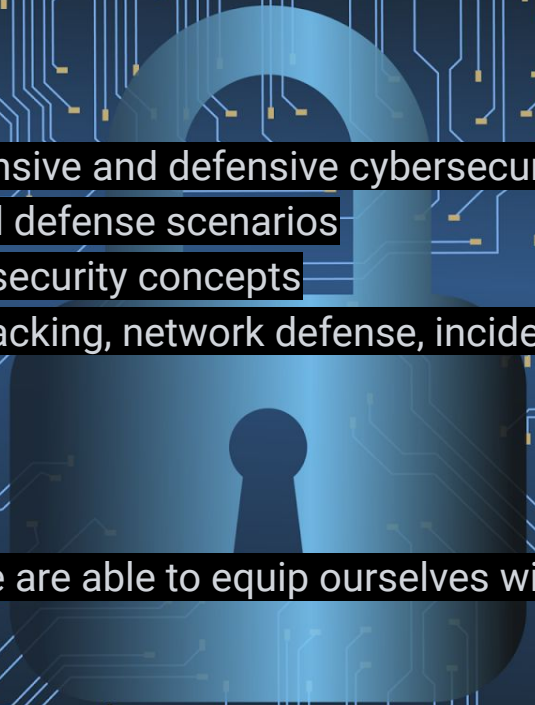
- Practice penetration testing and exploit development
- Safely explore and understand common vulnerabilities

Benefit:

- Realistic, safe and controlled environment for hands-on experience with ethical hacking
- Develop skills in identifying and securing vulnerabilities



Key Takeaways



- Hands-on experience in offensive and defensive cybersecurity
- Safe exploration of attack and defense scenarios
- Practical application of cybersecurity concepts
- Skill development in ethical hacking, network defense, incident response, and compliance reporting

In these home lab environments we are able to equip ourselves with practical skills in cybersecurity.