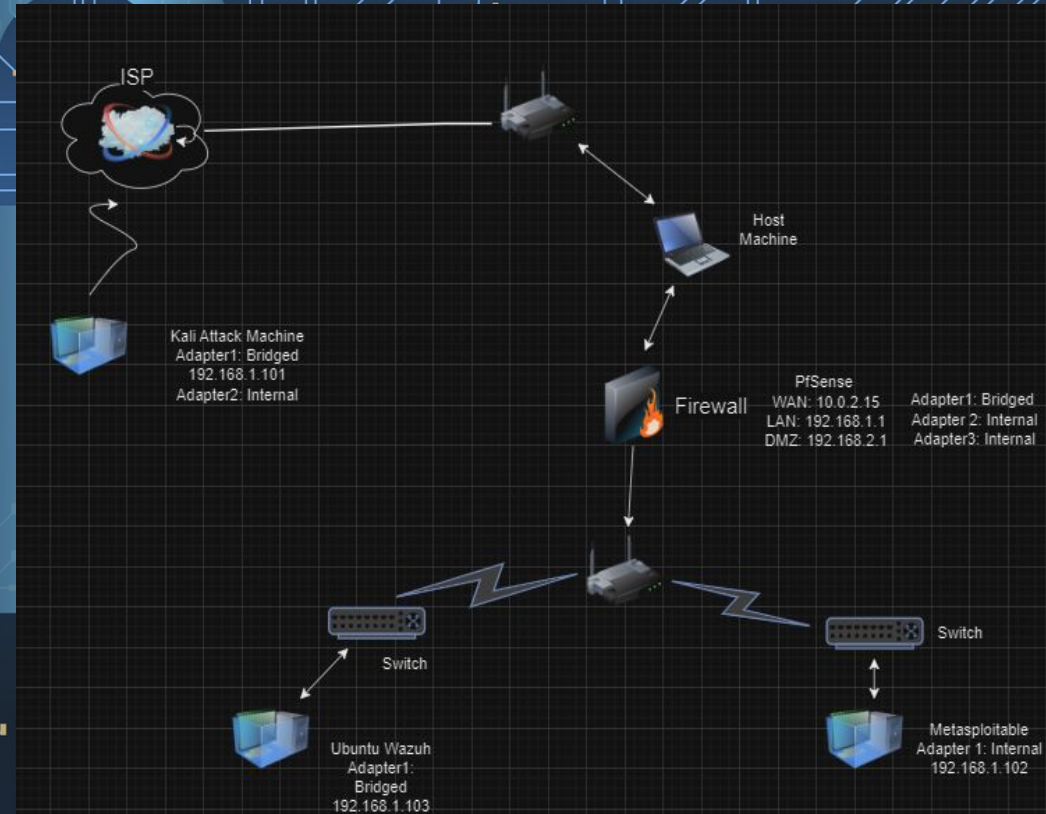


Home Virtual Training Lab

Margaret Edwards

Components of Home Lab

- Attack Machine
 - Kali Linux
- Firewall
 - PfSense
- 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

```
pfSense Router (Baseline) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
DH2 (opt1) -> en2 -> v4: 192.168.2.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at Dec 31 23:04:10 ...
php-fpm(399): /index.php: Successful login for user 'admin' from: 192.168.1.101
(Local Database)
[[fib_algo] inet.0 (bsearch4#47) rebuild_fd_fib: switching algo to radix4_lockless
s

FreeBSD/amd64 (pfSense.margaret.com) (ttyv0)
login: admin
Password:
```



sense®



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

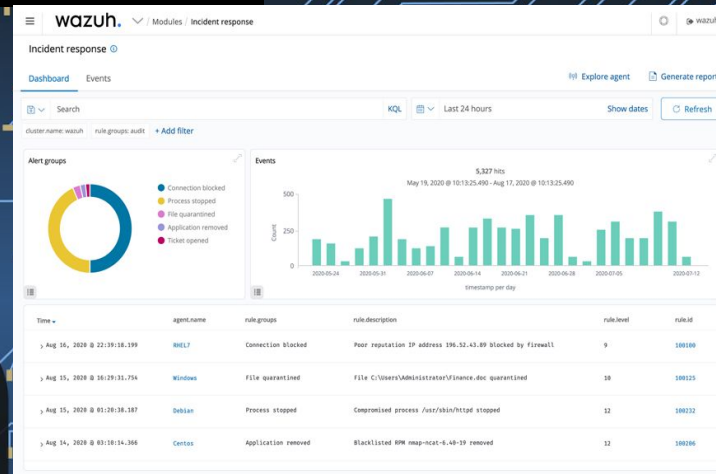
Wazuh is an Open-Source Security Information and Event Management Tool (SIEM) that is used for collecting and analyzing security event data.

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

```
metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
lrwxrwxrwx 1 root root 11 2010-04-28 16:26 cdrom -> media/cdrom
drwxr-xr-x 14 root root 13480 2023-12-31 18:29 dev
drwxr-xr-x 94 root root 4096 2023-12-31 20:55 etc
drwxr-xr-x 6 root root 4096 2010-04-16 02:16 home
drwxr-xr-x 2 root root 4096 2010-03-16 18:57 initrd
lrwxrwxrwx 1 root root 32 2010-04-28 16:26 initrd.img -> boot/initrd.img-2.
6.24-16-server
drwxr-xr-x 13 root root 4096 2012-05-13 23:35 lib
drwx----- 2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x 4 root root 4096 2010-03-16 18:55 media
drwxr-xr-x 3 root root 4096 2010-04-28 16:16 mnt
-rw----- 1 root root 9426 2023-12-31 18:29 nohup.out
drwxr-xr-x 2 root root 4096 2010-03-16 18:57 opt
dr-xr-xr-x 111 root root 0 2023-12-31 18:29 proc
drwxr-xr-x 13 root root 4096 2023-12-31 18:29 root
drwxr-xr-x 2 root root 4096 2012-05-13 21:54/sbin
drwxr-xr-x 2 root root 4096 2010-03-16 18:57 srv
drwxr-xr-x 12 root root 0 2023-12-31 18:29 sys
drwxrwxrwt 4 root root 4096 2023-12-31 18:29 tmp
drwxr-xr-x 12 root root 4096 2010-04-28 00:06 usr
drwxr-xr-x 14 root root 4096 2010-03-17 10:08 var
lrwxrwxrwx 1 root root 29 2010-04-28 16:21 vmlinuz -> boot/vmlinuz-2.6.24-1
6-server
msfadmin@metasploitable:/$
msfadmin@metasploitable:/$
```



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.