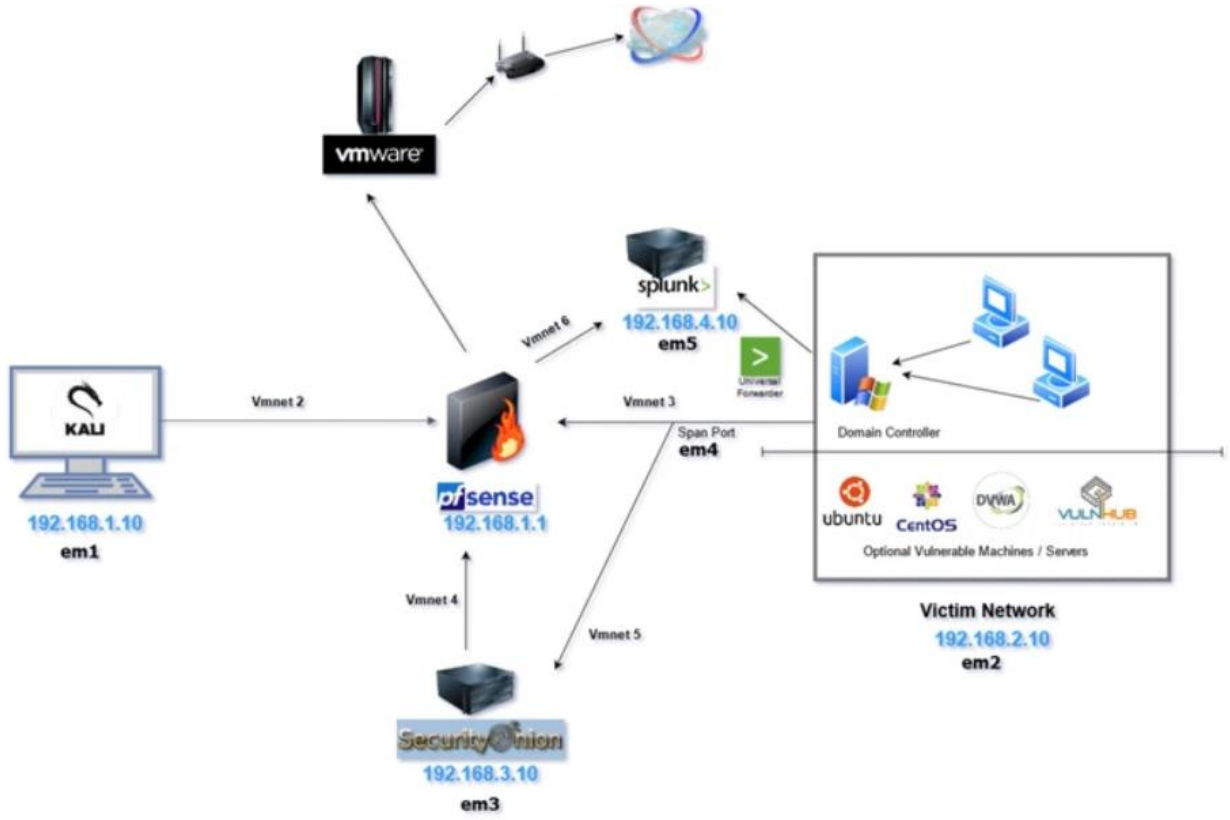
HOMELAB NETWORK DESIGN & TOPOLOGY



Step 1

Use VMWare workstation Pro as Hypervisor.

Step 2

Configuring pfsense

pfsense will be configured as a firewall to segment our private homelab network and will be only accessible from our Kali Linux machine.

Step 3

Configuring Security Onion

This will be the all-in-one IDS, Security Monitoring, and Log Management solution.

Step 4

Configuring Kali Linux

Kali Linux will be used as an attack machine to propagate different forms of offensive actions against the Domain Controller and the other machines attached to it.

Step 5

pfsense Interfaces and Rules

Now that the Kali machine is set up, the pfsense WebConfigurator can be accessed in order to make some changes to the pfsense interface and firewall rules.

Step 6

Configuring Windows Server as a Domain Controller

The goal of this portion of the lab is to set up an Active Directory domain with a Windows 2019 Server as the Domain Controller and 2 Windows 10 machines.

Step 7

Configuring Windows 10 Desktop & Adding a User to the AD Domain

The goal of this portion of the lab is to add 2 Windows 10 desktops to the Domain and complete the active directory lab.

Step 8

Joining the pcs to the domain

Step 9

Installing Splunk on Ubuntu Server

Splunk is one of the most widely used SIEMs in the Cybersecurity industry. Splunk essentially aggregates logs and datasets from various data sources and correlates all that information for easy searching, parsing & indexing.

Step 10

Installing Universal Forwarder on Windows Server

*In order to log the activities on endpoints, Splunk uses a mechanism called the universal forwarder. The universal forward can be installed on windows, *nix & mac agents to forward logs to your Splunk instance.*

Reference(Please see for detailed overview)

https://cyberwoxacademy.com/building-a-cybersecurity-homelab-for-detection-monitoring/