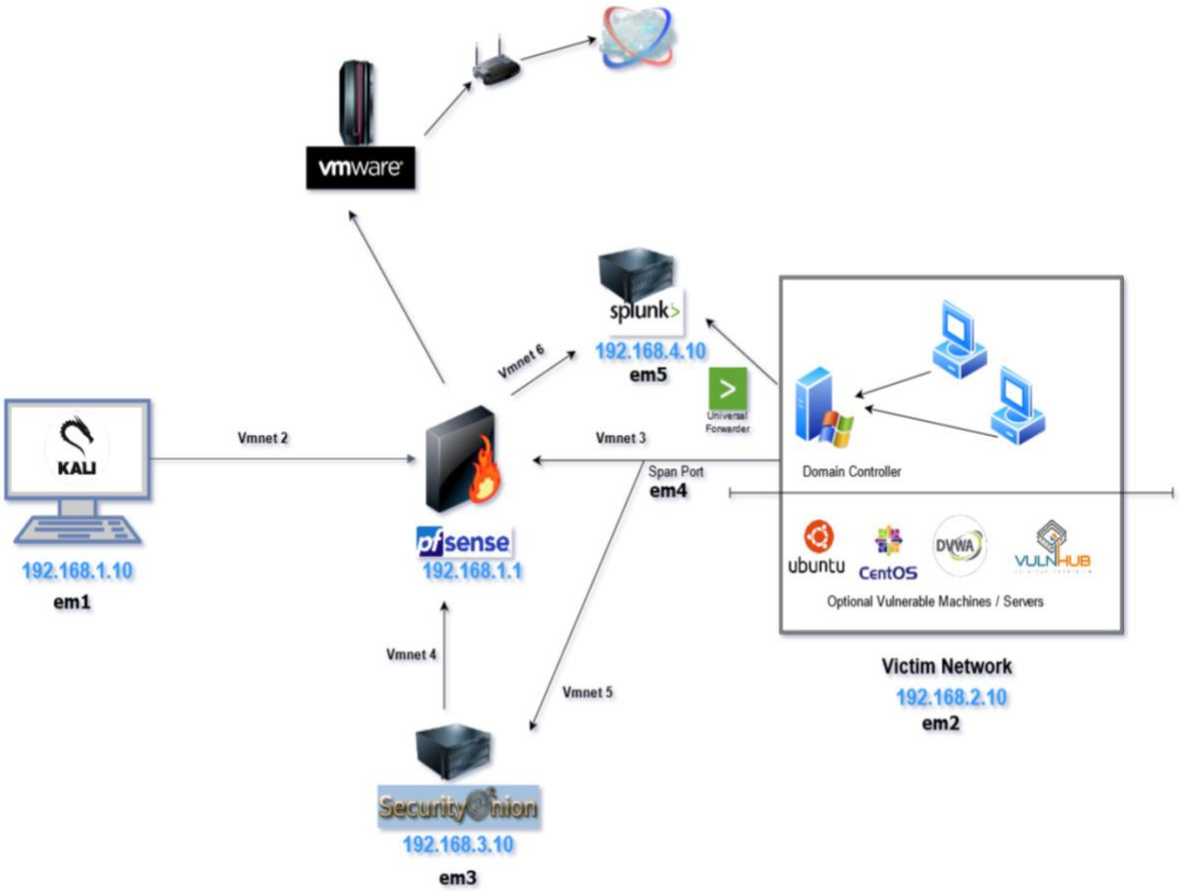
Aufbau eines Cybersecurity HomeLabs

In der Lage zu sein, das Gelernte anzuwenden, ist immer wichtig, wenn es um I.T. und Cybersicherheit geht. Ohne reale Anwendung ist es schwieriger zu verstehen, wie Konzepte in der Industrie tatsächlich umgesetzt werden. Um das Gelernte anwenden zu können, müssen Sie ein grundlegendes Verständnis dafür entwickeln, wie verschiedene Komponenten zusammenarbeiten.

Die Anwendung in der realen Welt kann alle Arten von Formen annehmen, von praktischen Projekten bis hin zu virtualisierten Umgebungen, in denen Sie neue Ansätze für ein Problem testen.
Mit diesem Gedanken bin ich an dieses Projekt herangegangen. Dieses Homelab führt durch den Prozess der Konfiguration, Optimierung und Sicherung einer I.T.-Infrastruktur.

1. Was ist ein HomeLab in I.T. / Cybersecurity?
2. Typologie Aufschlüsselung
3. Ubuntu Image installieren
4. Einrichten von VMware Workstation 15 Player
5. Konfigurieren eines Windows-Servers als Domänencontroller
6. Konfigurieren von Kali Linux als Angriffsmaschine
7. Absicherung des Heimnetzwerks mit PFsense Firewall
8. Konfiguration von Splunk
9. Nessus auf Kali konfigurieren
10. Ubuntu/Centos/Metasploitable/DVWA/Vulnhub-Rechner: All dies sind potenzielle Linux-Rechner, die dem Netzwerk für Exploitation-, Erkennungs- oder Überwachungszwecke hinzugefügt werden können.
11. Portscanning mit Python, Nmap und Kali Linux



Quellen

1. https://link.springer.com/chapter/10.1007/978-3-030-49932-7_95
2. https://robertscocca.medium.com/building-an-active-directory-lab-82170dd73fb4
3. https://subscription.packtpub.com/book/networking_and_servers/9781783550999/1/ch01lvl1sec13/nessus-system-configuration
4. https://subscription.packtpub.com/book/networking_and_servers/9781783550999/1/ch01lvl1sec12/user-management
5. https://www.security-insider.de/was-ist-ein-siem-a-772821/
6. https://link.springer.com/chapter/10.1007/978-3-030-49932-7_95