

Building a Cybersecurity Home Lab for Detection & Monitoring

Dissertation submitted to

*Shri Ramdeobaba College of Engineering & Management,
Nagpur in partial fulfillment of requirement for the award
of degree of*

Bachelor of Engineering

In

Computer Science and Engineering cyber security

By

Gaurav Singh

Prasanna Tangade

Vishal Bhutada

Ayush Bhattad

Nandan Partani

Rohan Jangid

Guide

Prof. Charanjeet Dadiyala

RCOEM

**Shri Ramdeobaba College of
Engineering and Management, Nagpur**

Computer Science and Engineering

Shri Ramdeobaba College of Engineering & Management,

Nagpur 440 013

(An Autonomous Institute affiliated to Rashtrasant Tukdoji Maharaj Nagpur University
Nagpur)

November, 2022

ABSTRACT

In Cybersecurity, it could be a daunting task to apply and implement security concepts if there is an unavailability of practical and safe infrastructure to carry out these activities.

We approached this project with that in mind. This home lab walks through the process of configuring, optimizing, and securing an I.T infrastructure. Although this will be at a relatively small scale, you will be able to apply the knowledge gained in a real-world large-scale/enterprise infrastructure.

Home lab is the name given to a server (or multiple server setup) that resides locally in your home and where you host several applications and virtualized systems for testing and developing or for home and functional usage.

A home lab is an environment meant to simulate components of I.T. infrastructure, equipment, and configurations similar to a business or enterprise network. This aims to understand the process of installing, configuring, and optimizing I.T.

One of the best ways to start learning to analyse network traffic for anomalies and malicious activity is to begin looking at your home network traffic as often as you can in a meaningful way. The more you understand what 'normal' looks like the better off you will be.

TABLE OF CONTENTS

1. INTRODUCTION	1
2. PROJECT DEFINITION & DETAILS	2
2.1 Project Definition	2
2.2 Project Objective	2
2.3 Project Details and Area	2
2.4 Function Specifications / Deliverables	2
2.5 Project Outcome	2
3. LITERATURE REVIEW	3
4. TECHNOLOGY USED & BACKGROUND MODELS.....	7
4.1 Technology Used	7
4.2 Background Models.....	7
5. METHODOLOGY	10
5.1 Methodology Applied	10
5.2 Dataset preprocessing.....	10
6. IMPLEMENTATION	11
6.1 Implementation Details	11
6.2 Steps Followed	11
6.2.2 Training.....	11
6.2.3 Testing.....	11
7. RESULTS & DISCUSSION	13
7.1 Results & Discussion	13
8. CONCLUSION & FUTURE SCOPE	14
REFERENCES	17

LIST OF FIGURES

Figure 4.1: Active Directory	16
Fig 4.2 Splunk.....	16
Fig 4.3 Victim network.....	17
Fig 5.1 Topology chart.....	18
Fig 6.1 Implementation details.....	19
Fig 6.2 Implementation details.....	20
Fig 6.3 Implementation details.....	21
Fig 6.4 Implementation details.....	22
Fig 6.5 configuring pfsense.....	23
Fig 6.6 configuring security onion.....	24
Fig 6.7 configuring security onion.....	24
Fig 6.8 installing security onion.....	24
Fig 6.9 setting up final steps in security onion configuration....	25
Fig 6.10 kali linux image file for installation...	25
Fig6.11 resetting default PW in kali linux.....	26
Fig 6.12 setting Pfsense rules.....	26
fig 6.13 pfsense interface/LAN(em1).....	26
Fig 6.14 Configuring Windows Server as a Domain Controller..	27
Fig 6.15 Configuring Windows Server as a Domain Controller..	27
Fig 6.16 JOINING THE PCs TO THE DOMAIN.....	28
Fig 6.17 Installing Splunk on a Ubuntu Server....	29

Fig 6.18 Installing Universal Forwarder on Windows Server..29

Fig 6.19 universal forwarder30

Fig 7.1 IDS logs Dashboard31

CHAPTER 1

INTRODUCTION

1.1 Introduction

In Cybersecurity, it could be a daunting task to apply and implement security concepts if there is an unavailability of practical and safe infrastructure to carry out these activities.

we approached this project with that in mind. This homelab walks through the process of configuring, optimizing, and securing an I.T infrastructure. Although this will be at a relatively small scale, you will be able to apply the knowledge gained in a real-world large-scale/enterprise infrastructure.

What is a Homelab?

A Homelab, as the name implies, is an environment in your home that is used to practice and improve your skills in a specific field. This home lab has components and tools similar to large-scale infrastructures. It's a safe environment to work with these components and learn how they work.

CHAPTER 2

PROJECT DEFINITION AND DETAILS

2.1 Project Definition & details

PROBLEM DEFINITION:

In Cybersecurity, it could be a daunting task to apply and implement security concepts if there is an unavailability of practical and safe infrastructure to carry out these activities.

We approached this project with that in mind. This home lab walks through the process of configuring, optimizing, and securing an I.T infrastructure. Although this will be at a relatively small scale, you will be able to apply the knowledge gained in a real-world large-scale/enterprise infrastructure.

PROBLEM OBJECTIVE:

Home lab is the name given to a server (or multiple server setup) that resides locally in your home and where you host several applications and virtualized systems for testing and developing or for home and functional usage.

A home lab is an environment meant to simulate components of I.T. infrastructure, equipment, and configurations similar to a business or enterprise network. This aims to understand the process of installing, configuring, and optimizing I.T.

One of the best ways to start learning to analyse network traffic for anomalies and malicious activity is to begin looking at your home network traffic as often as you can in a meaningful way. The more you understand what 'normal' looks like the better off you will be.

PROJECT SCOPE:

- 1) Stay out of legal problems
- 2) It will help in security testing & development
- 3) Maintain isolated development environment
- 4) It will be sharpening cyber security skills
- 5) With this one can run a network security device like Sophos UTM (free IIRC) and can evaluate the pros and cons
- 6) Set up labs and pop boxes from Vuln Hub
- 7) During the testing of some techniques which may cause damaging results
- 8) During the testing, if the researcher uses a malware tool, it could spread to the other Internet-connected environment
- 9) It is recommended that you have a basic foundation of networking terminology, computers, cybersecurity concepts, and formidable research skills
- 10) Can set up isolated networks for different tasks
- 11) Capture packets and how to use them for diagnostic information
- 12) Run a malware sandbox in an as-safe-as-possible, isolated, virtualized way
- 13) Try running a honeypot in an as-safe-as-possible, isolated, virtualized way
- 14) Script stuff and make neat projects

CHAPTER 3

LITERATURE REVIEW

3.1 Literature review

The following section is dedicated towards the related and relevant research papers and its literature review.

Smart grid lab research in Europe and beyond on Cybersecurity:

Cybersecurity is crucial for the existence of smart grids, since the enormous data transmission implies that advanced techniques should be applied in order to protect critical information and confidential data, as has also been highlighted in Section . It also includes all the measures for protection of the communication devices against unauthorized access or actions that could lead to alteration or theft of data. Activities related to CS are risk assessment, risk response, confidentiality and privacy, authorization, and authentication, to name some

Assessing Work From Home Security Packages Vulnerabilities:

This project was published in 2022 by Auckland University of Technology.

This research was conducted in anticipation of the time of the COVID-19 pandemic when social distancing and lockdown became a new norm. As part of business continuity measures, employers asked their workforce to work from home, and there is already a known trend of working remotely.

In this research, it is identified in depth what a typical smart home looks like. What are the security challenges faced by home users/staff working from home? What are the security aspects where such users are challenged? Due to the type of devices and audience at home, they cannot be left to fight for themselves. This is of specific and essential importance. There

should be new ways of looking at home networks and ideas to protect home networks that have the same level of security as enterprises have these days.

An application of Countermeasures to Protect a Potential Vulnerable Infrastructure:

This research was published in 18th Dec, 2020 by Ademola, E.O. Professor, BCS & CMI Subject Matter Expert Principal Consultant Power-Age Consulting.

Pen-testing (PT) methodology entails the assessment, which is known as security evaluation or conduct phase. The actual assault execution, and the conclusion. Also, the essential is the post-assessment and report generation as types of PT could depict different stages of knowledge about the Target of Evaluation (ToE). The framework are Black-box testing, White-box testing, and Gray-box testing; which could also require coding, and methodology protocols (Gaugler et al. 2019; see also Pat et al. 2019; Kachhwaha and Purohit 2019) Overall, PT is a technique to assess the security edges for the ToE by reproducing an assault to find vulnerabilities available to assailants' attacks. The test includes a comprehensive analysis of the system configurations, designs, weaknesses, and technical flaws. From an administrative standpoint, it is paramount to check the dimension of the framework; data exposure and misuses which could make the context defenceless for outside foes. The methodology adopted here accentuates a structure, which consists of the PT phases as well as the countermeasures and associated implementation in the ultimate interest of ethical approach and best practice.

In fulfilment of the essential requirements as well as keeping with possible ethical guidelines and avoiding legal constraints, three Virtual Machines (VM) built in the home-lab. On the Campus, there available prepared machines, with Linux Server that use CentOS or Ubuntu Server, just a minimum configuration required. Further, their available domain name server (DNS) configured as the server on the one hand evident in section 2.2.1; and client on the other. Thus, permitting an additional service of choice, in likes of DHCP, FTP, SMTP, and SNMP. In the Campus, the Server operated VM operated Linux with Kali as well as Client on the Win 7. At home Lab available VirtualBox (VB) with essential requirements fulfilled to configure the Server and create multiple copies of the client's VB in other to Vol. 9. No. 1, 2021 35 demonstrate an attack. Apparently, the Attacker machine runs on the most recent

version of Kali Linux. It has been suggested, (Dholey and Shaw 2019; see also Jabir et al. 2016 and Al-Khateeb 2016), that such set up helps in effective management of the practical development of PT in a secured manner.

In a Cloud computing and design of Cyber Warfare Testbed, Chandra and Mishra (2019) maintain that such built up to conducting cyber warfare could ease the overall process as well as help in extension to cyberattacks and corresponding multiple system configuration. Al-Khateeb (2016) underscores such process of designing static IP address in Linux Terminal.

CYBEX Automation & Virtualization:

This research was published in 2018 by Parr, Alexander. Cybersecurity is an issue that affects virtually everybody in the digital age. Attacks such as the Equifax breach or the Wannacry ransomware attack are becoming more and more commonplace and are becoming harder to defend against as attackers become more sophisticated. Many organizations that are breached are often entirely unaware of the breach until after it has occurred, or slow to react during the event. CYBEX is a project to help mitigate this. CYBEX is an automated cybersecurity response system designed to import and analyze log files from many organizations, develop defensive rules against an attack on any one of them, and send the solution out to all other members in order to stop attacks before they can spread. CYBEX primarily targeted at businesses in order to facilitate faster and more effective incident response. CYBEX was successful in testing at being able to securely disseminate security rules out to a group of computers and preemptively stop attacks against them.

CHAPTER 4

TECHNOLOGY USED AND BACKGROUND MODELS

4.1 TECHNOLOGY USED

VM Ware

VMware Workstation is a line of Desktop Hypervisor products which lets users run virtual machines, containers and Kubernetes clusters.

A Virtual Machine (VM) is a compute resource that uses software instead of a physical computer to run programs and deploy apps.

Kali Linux

The most advanced

Penetration Testing Distribution :

Kali Linux :- is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

What is pfSense?

pfSense® software is primarily used as a router and firewall software and is frequently set up as a DHCP server, DNS server, WiFi access point, and VPN server, all on the same physical device.

pfSense is a firewall/router computer software distribution based on FreeBSD. The open source pfSense Community Edition (CE) and pfSense Plus is installed on a physical computer or a virtual machine to make a dedicated firewall/router for a network.

What Is Active Directory?



Active Directory (AD) **allows your IT department to manage and store information** about the devices, users, and objects within your organization's network.

Why Use Active Directory?

- **Easily organize users** into groups and subgroups.
- **Quickly manage file access** and appropriately assign access rights to employees.
- **Maintain a complete overview** of the management of resources and users within the organization.



Active Directory is **universally adopted** within countless organizations' infrastructures.



Through Active Directory usage, organizations of all sizes can **provide the centralized management** of their users.

Fig 4.1 Active Directory

What is Splunk?

Splunk is used for monitoring and searching through big data. It indexes and correlates information in a container that makes it searchable, and makes it possible to generate alerts, reports, and visualizations.



Fig 4.2 Splunk

What is Security Onion?

Security Onion is a free and open source Linux distribution for intrusion detection, security monitoring, and log management.

Security Onion is a free and open source intrusion detection system (IDS),

An Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected.

Victim Network :

A virus is hostile code designed to attach itself to a file (file-infector) or, infrequently, to a sensitive system sector of the victim computer's hard disk. It is Malware that infects files and spreads when the file executes or is executed by another program.

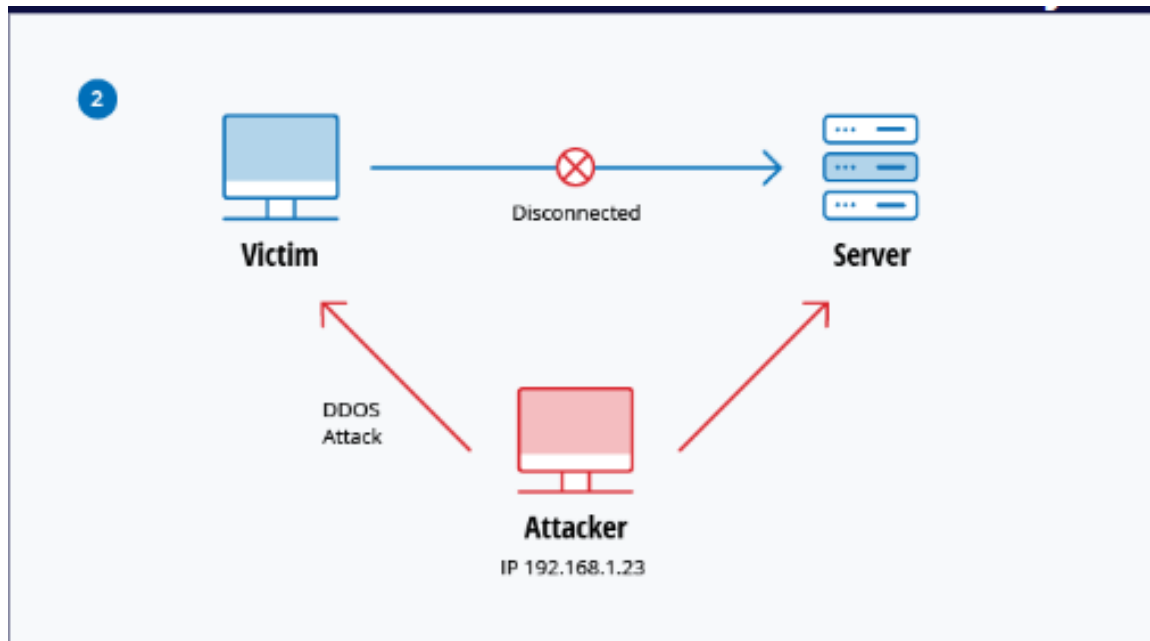


Fig 4.3 Victim network

CHAPTER 5

METHODOLOGY

5.1 Methodology

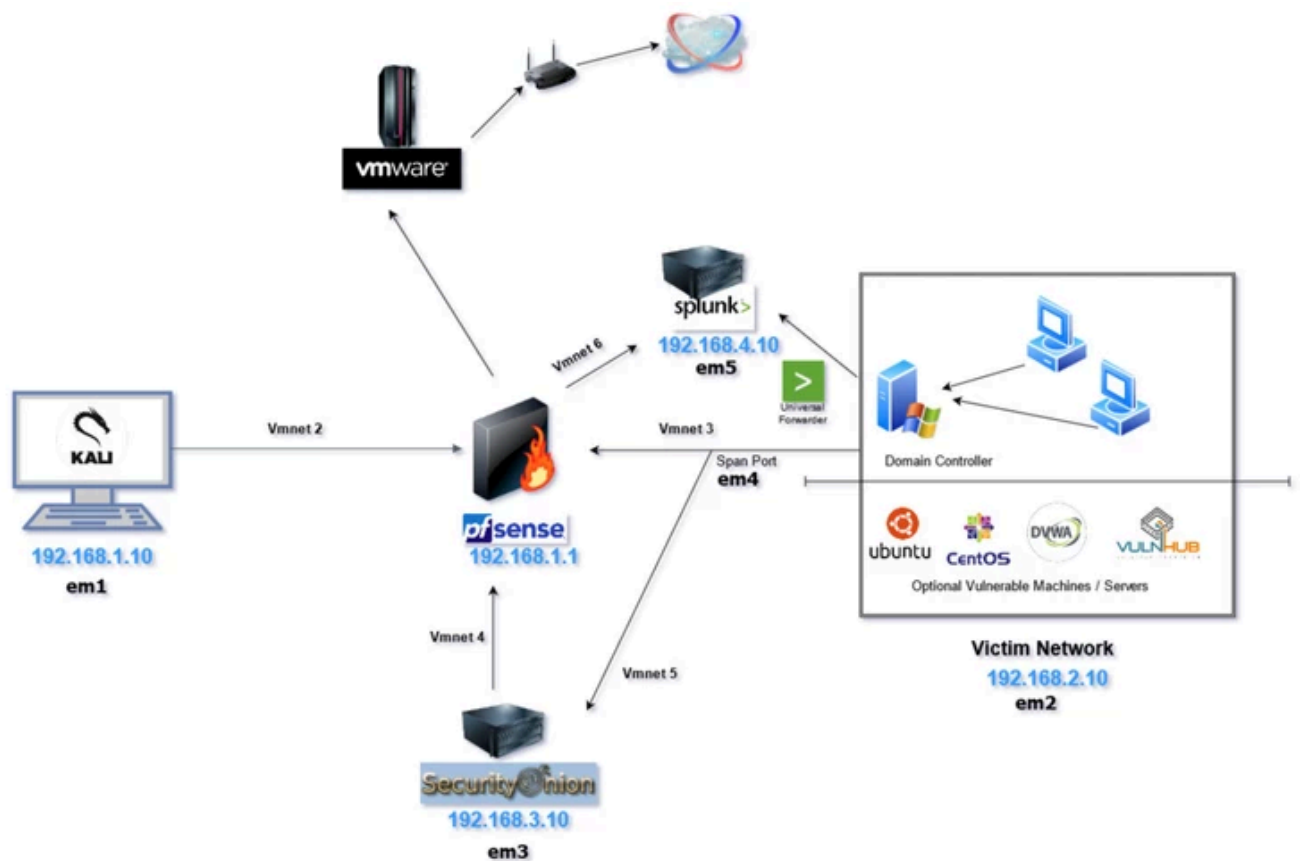


Fig 5.1 Topology chart

Building The Host PC:

For this lab, we'll be using a PC we built a while back specifically for this purpose. The hardware requirements are listed below:

CPU: AMD Ryzen 5 3600X 3.8 GHz 6-Core Processor

RAM: G.Skill Ripjaws V Series 32 GB (2 x 16 GB) DDR4 Memory

STORAGE: Crucial 512GB M.2-2280 NVME SSD

GRAPHICS CARD: MSI GeForce GT 710 2 GB Video Card

MOTHERBOARD: Asus TUF GAMING X570 ATX Motherboard

HOST OPERATING SYSTEM: Windows 11.

CHAPTER 6

IMPLEMENTATION DETAILS

6.1 Implementation details

Downloading & Installing VMware Workstation Pro

For the purpose of this lab, I'll be using VMware Workstation 16 Pro as my hypervisor. This license costs about \$120 with a student discount but I assure you it is a very worthwhile investment.

Download VMware Workstation Player

VirtualBox is also a free and feature-rich alternative Hypervisor from Oracle. If you cannot afford the VMware license, VirtualBox is equally good.

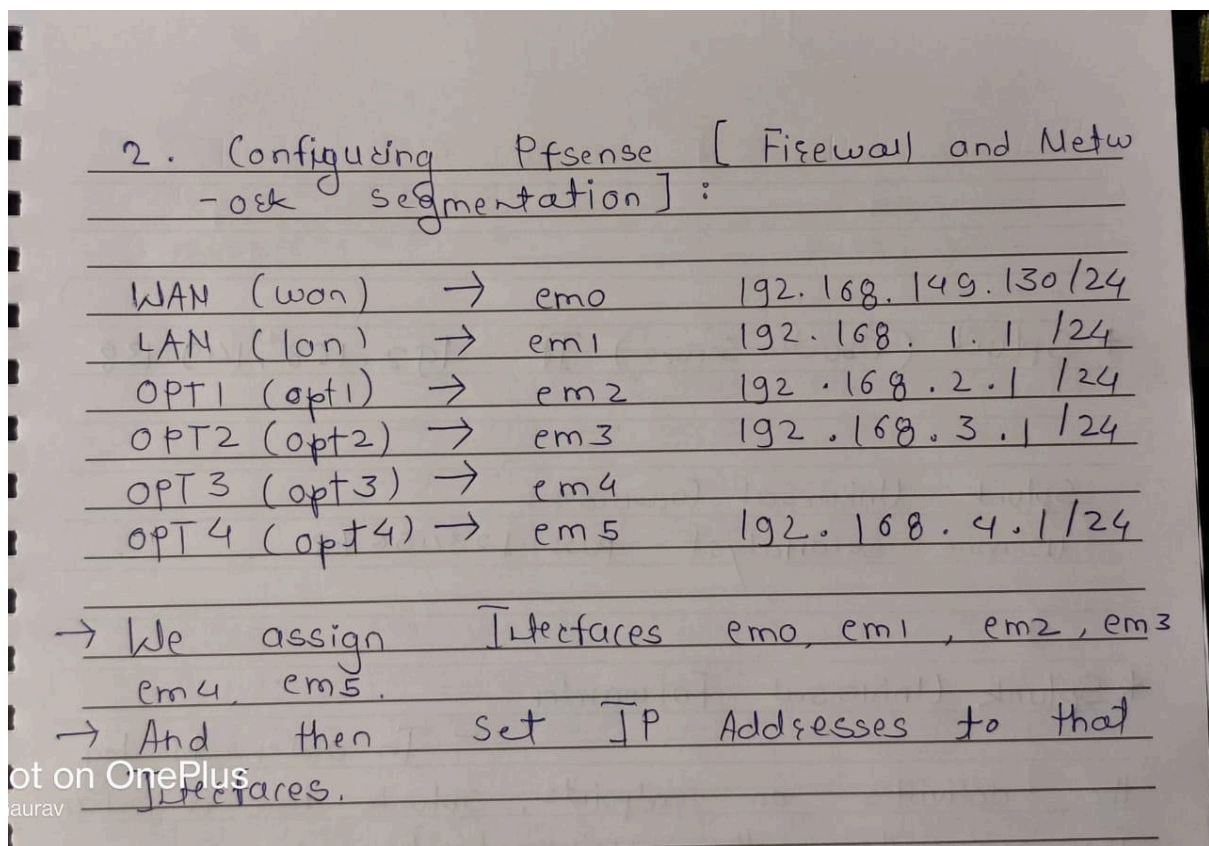


Fig 6.1 Implementation details

* Splunk (Ubuntu Server) IP: 192.168.149.138

Splunk Universal Forwarder:

username: socanalyst pass: 12345678

* Splunk Universal Forwarder:

- In order to log the activities on endpoints, splunk uses a mechanism called the universal forwarder.

- The Universal Forwarder can be installed on windows and mac agents to forward logs to Splunk.

* Ubuntu Server \Rightarrow Splunk

• Splunk username: socanalyst password: 12345678

• To splunk web interface: <http://splunk:8000> or
<http://127.0.0.1:8000>

* On Kali Terminal \rightarrow PfSense 192.168.1.1

Fig 6.2 Implementation details

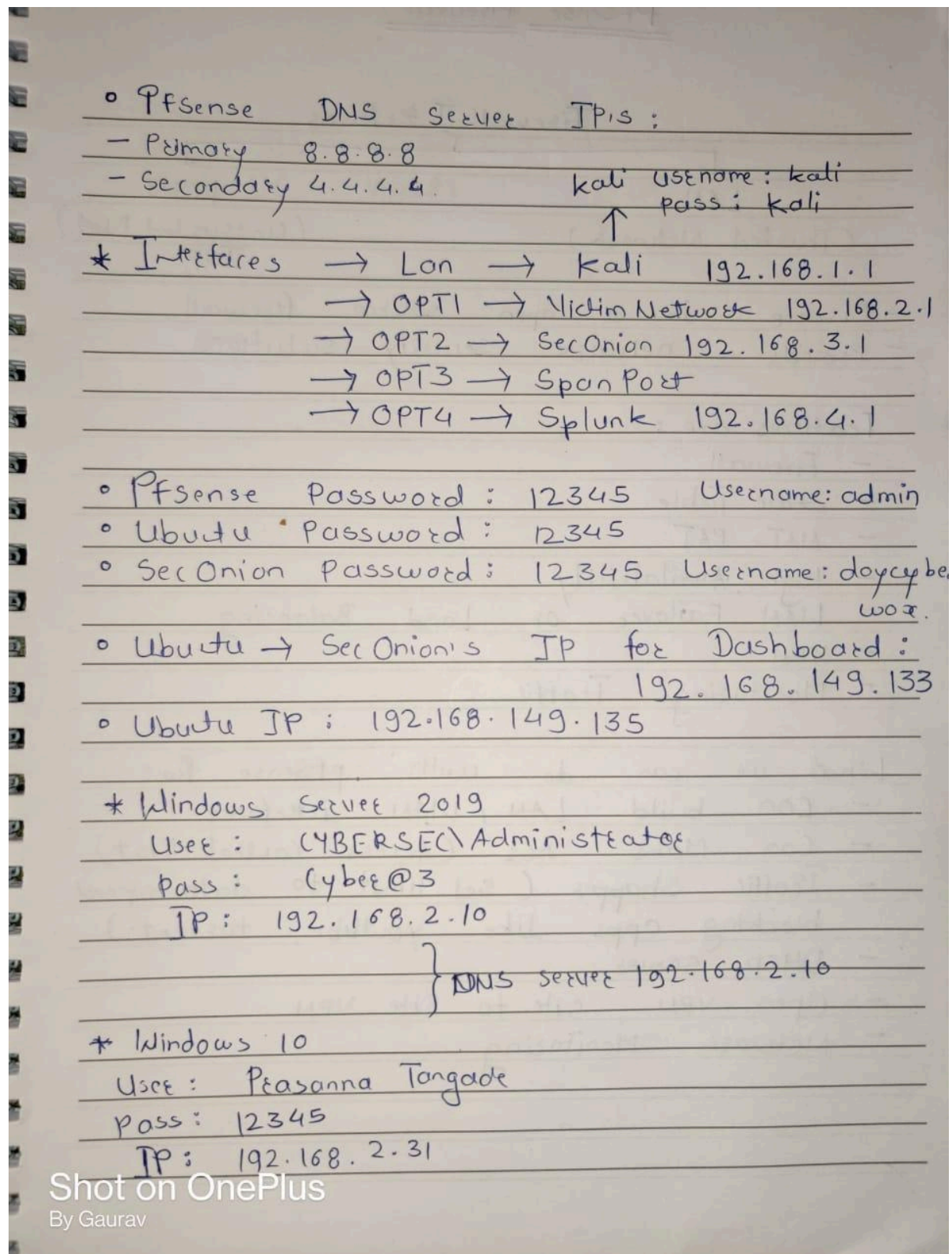
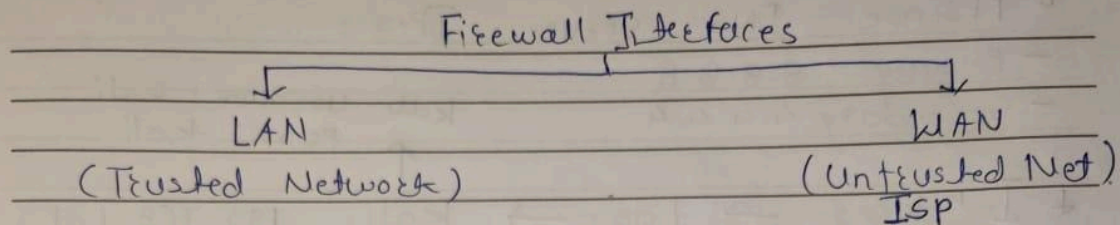


Fig 6.3 Implementation details

PFSense Firewall



- Pfsense is a open source firewall.
- Provide network security solutions.

Features are :

- Firewall
- State Table
- NAT, PAT
- High Availability
- WAN Failover or Load Balancing
- VPN
- Monitoring Traffic

What we can do with pfSense fw:

- Can build LAN / WAN interfaces
- Can Make ACL (Access Control List)
- Traffic Shaper (set limit to data speed, blocking apps like youtube, torrent.)
- DHCP server
- Open VPN, site to site VPN
- Network Monitoring

Shot on OnePlus

By Gaurav

Fig 6.4 Implementation details

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.

Download the pfsense ISO file: [Download pfSense Community Edition](#)

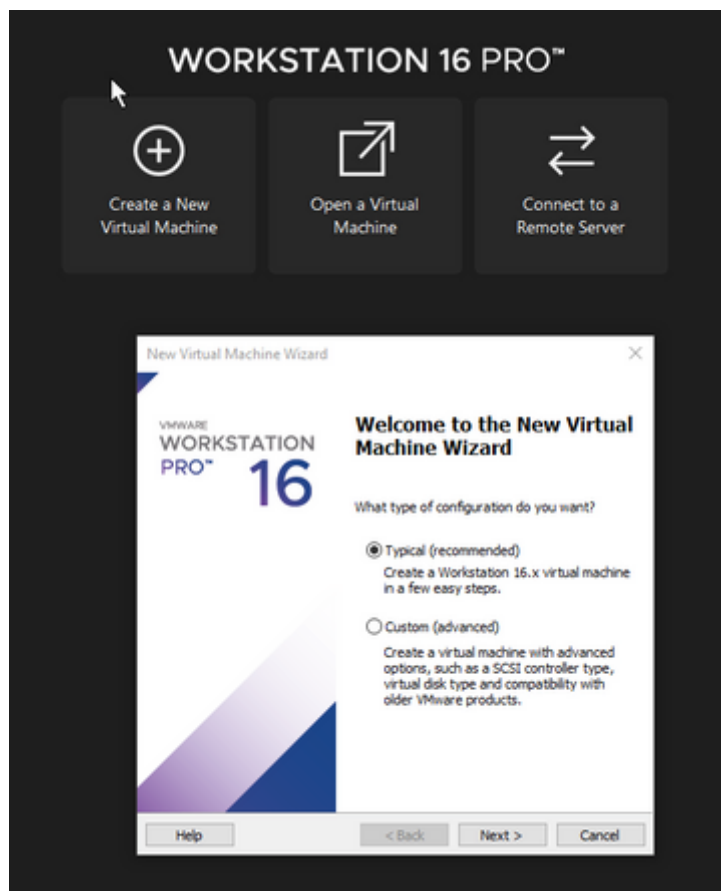


Fig 6.5 configuring pfsense

Configuring Security Onion

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

Download the Security Onion ISO file

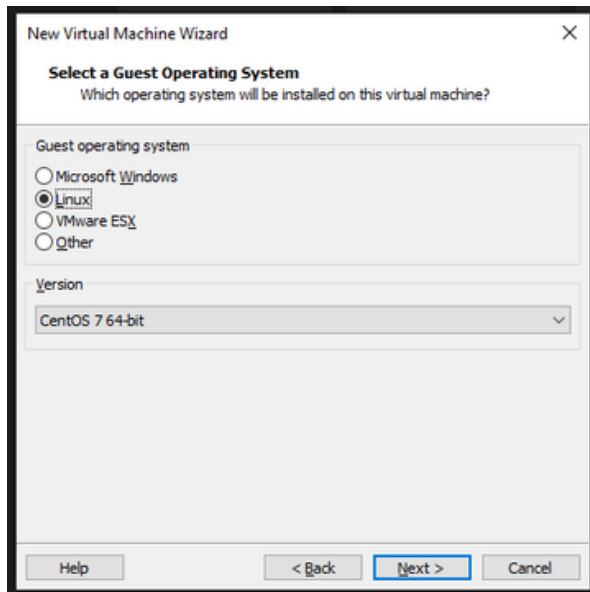


Fig 6.6 configuring security onion

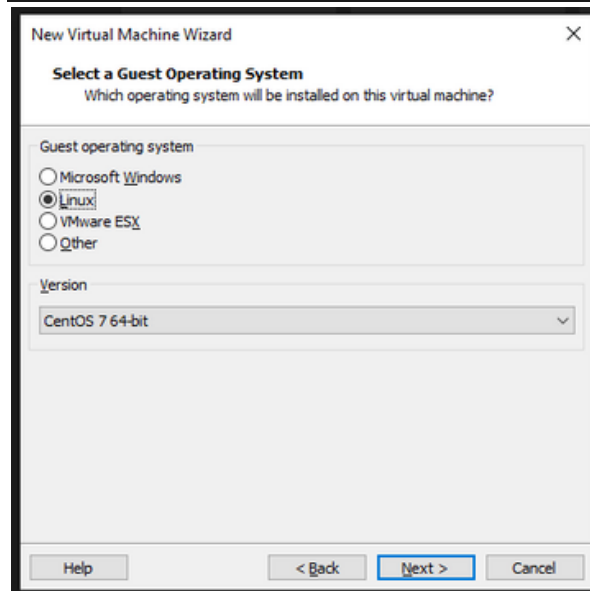


fig 6.7 configuring security onion



Fig 6.8 installing security onion

Navigate to the Security Onion IP Address on your Ubuntu Desktop:

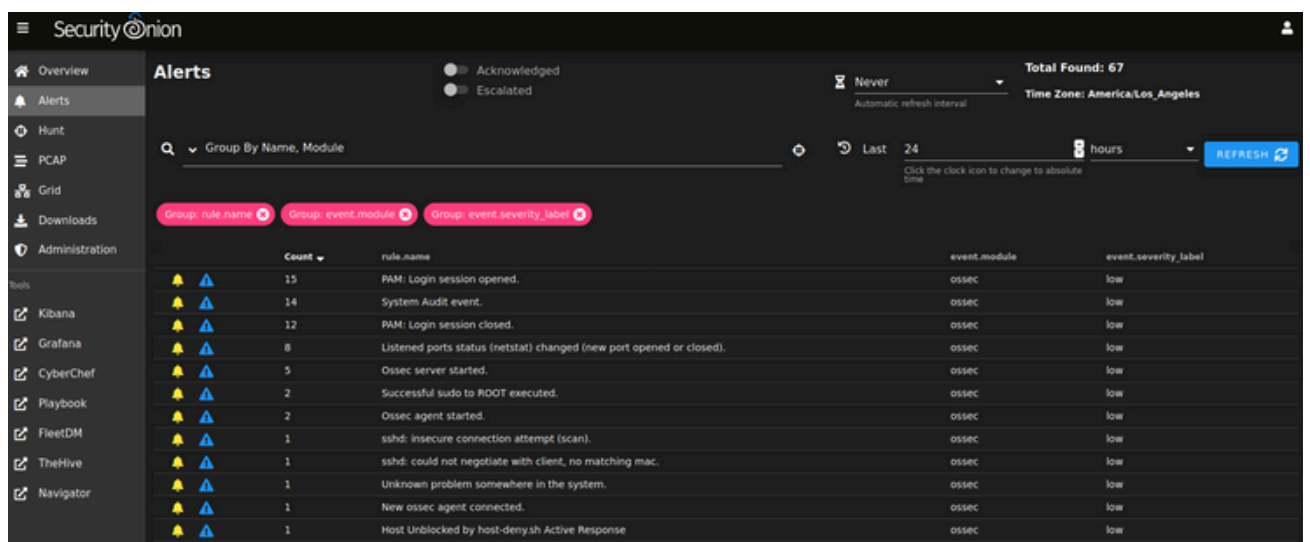


Fig 6.9 setting up final steps in security onion configuration

This ends the configuration of the Security Onion VM.

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.

Download the Kali Linux ISO

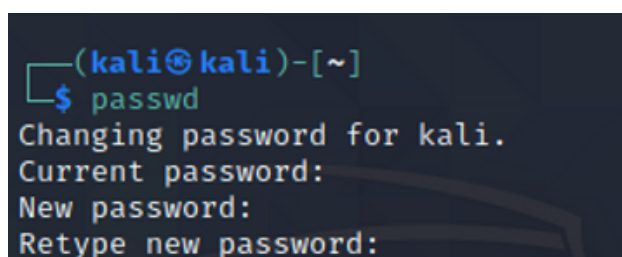
Since you're downloading the VM file, all you'll need to do is to click on the .vmx file from the Kali Folder you downloaded and it will automatically load up the default Kali image in Vmware.



kali-linux-2021.1-vmware-amd64.vmsd	✓	4/13/2021 3:15 AM	vmware snapshot ...	0 KB
kali-linux-2021.1-vmware-amd64.vmx	✓	4/14/2021 10:15 AM	VMware virtual m...	4 KB

Fig 6.10 kali linux image file for installation

After powering on, use this command to change the default password to a more secure one of your choice:



```
(kali@kali)-[~]  
$ passwd  
Changing password for kali.  
Current password:  
New password:  
Retype new password:
```

Fig6.11 resetting default PW in kali linux

pfsense Interfaces and Rules

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

Navigate to the web browser and search for 192.168.1.1

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname
EXAMPLE: myserver

Domain
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

[» Next](#)

Fig 6.12 setting Pfsense rules

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Interfaces / LAN (em1)

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address

fig 6.13

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. This portion of the lab is very easy to set up

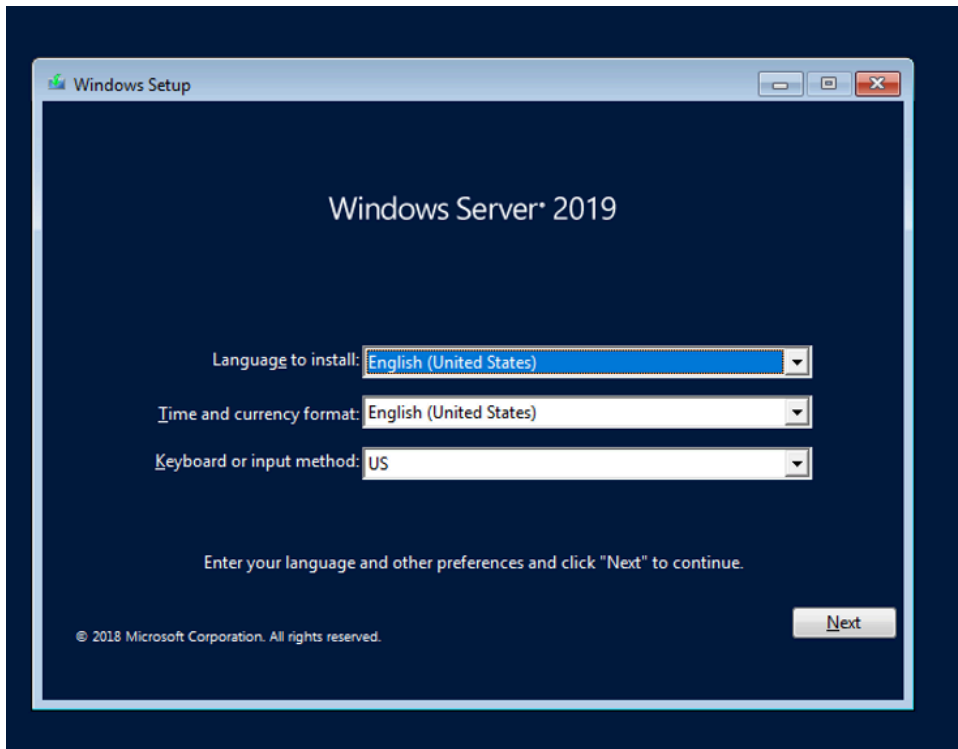
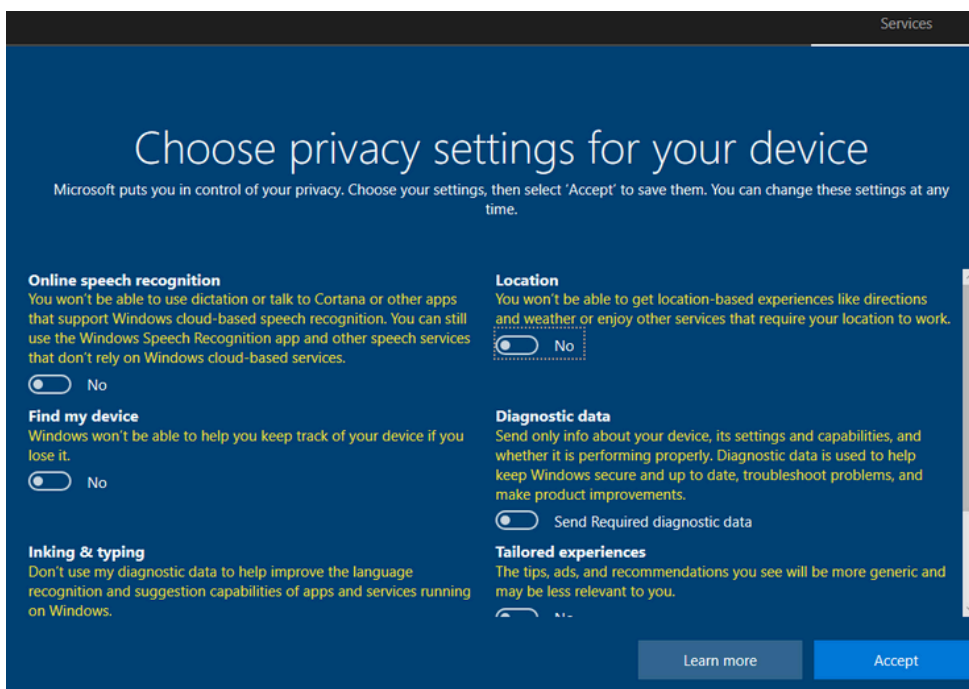


Fig 6.14 Configuring Windows Server as a Domain Controller



6.15 Configuring Windows Server as a Domain Controller

JOINING THE PCs TO THE DOMAIN

Navigate to Network Adapter settings

~ Right-click on Ethernet0 and select properties

~ Select IPV4

~ Add an IP Address(192.168.2.21) & Use 192.168.2.1 as the default gateway

~ Use 192.168.2.10(VictimsNetwork) as the DNS Server

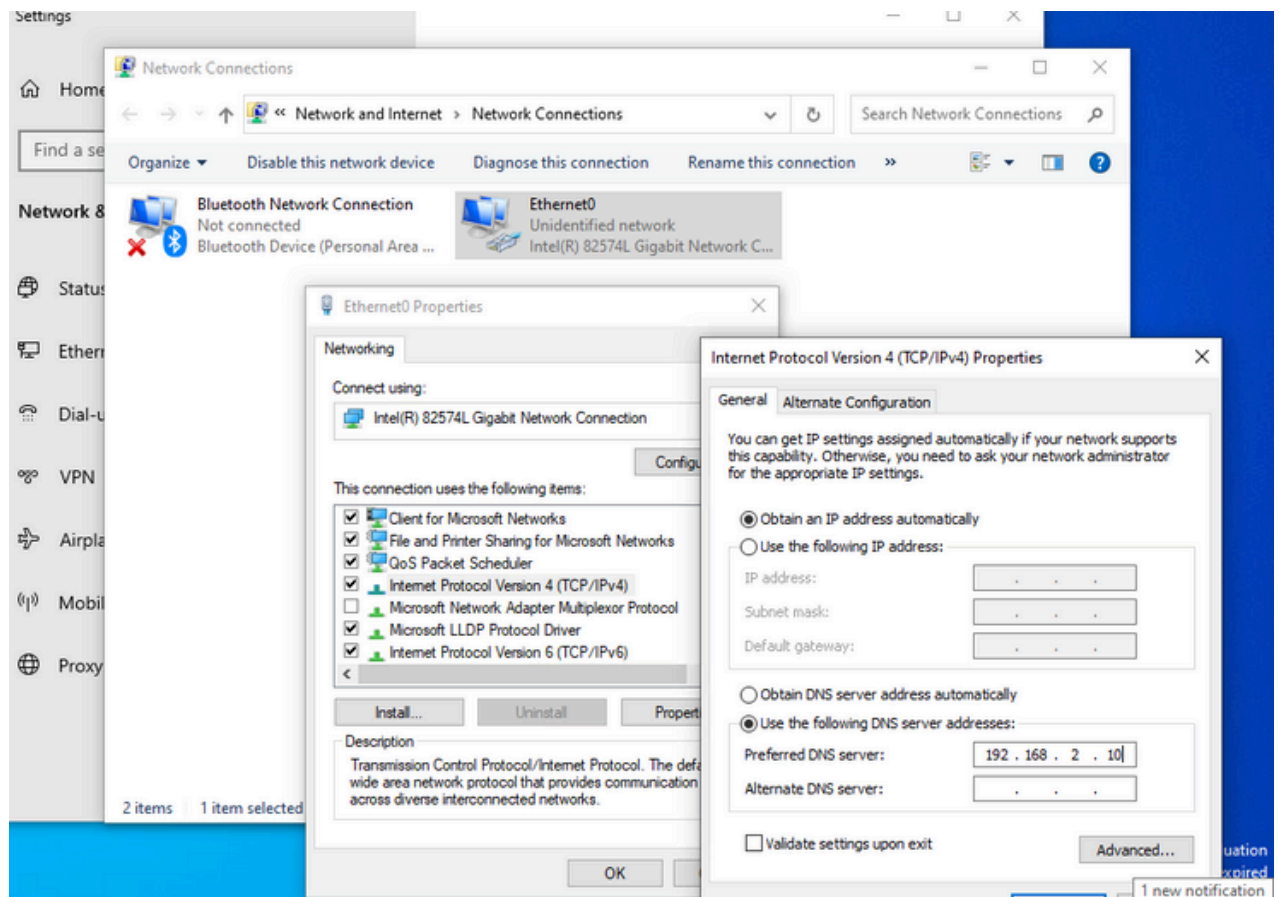


Fig 6.16 JOINING THE PCs TO THE DOMAIN

Installing Splunk on a 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.

```

daycyberwox@splunk:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
daycyberwox@splunk:~$ cd Downloads
daycyberwox@splunk:~/Downloads$ ls
splunk-8.2.0-e053ef3c985f-Linux-x86_64.tgz
daycyberwox@splunk:~/Downloads$

```

Fig 6.17 Installing Splunk on a Ubuntu Server

```

daycyberwox@splunk:~/Downloads$ ls
splunk-8.2.0-e053ef3c985f-Linux-x86_64.tgz
daycyberwox@splunk:~/Downloads$ tar xvzf splunk-8.2.0-e053ef3c985f-Linux-x86_64.tgz

```

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.

Add the Vmnet6 network adapters to the Splunk adapter

Set up “Receiving” on your Splunk server

Navigate to Settings >> Forwarding and Receiving >> New Receiving Port



Fig 6.18 Installing Universal Forwarder on Windows Server

Enter port 9997 and save

Navigate to Settings >> Indexes >> New index

Name the index “wineventlog” and save

On your Windows Server, Download the Universal Forwarder

Now install the forwarder:

Accept the License Agreement & click Next

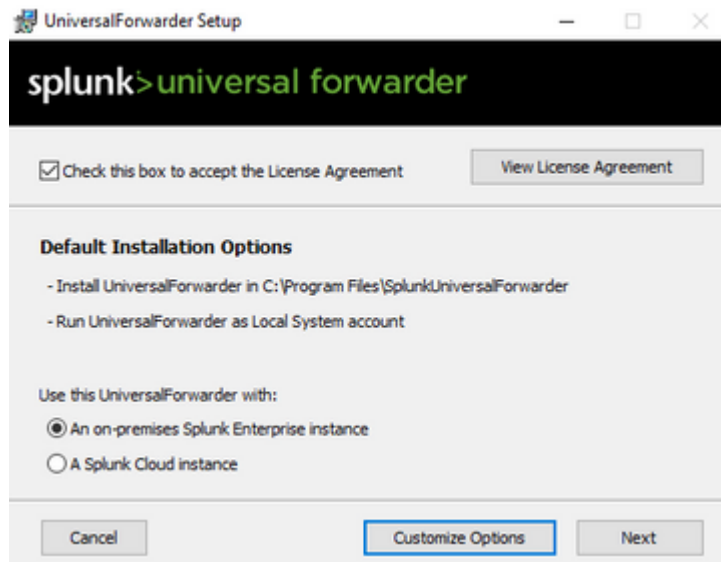
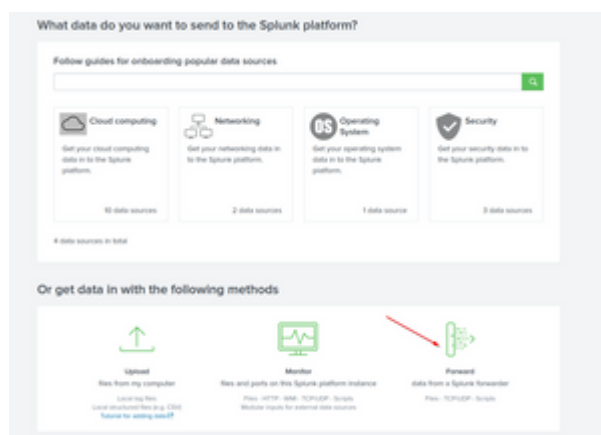


Fig 6.19 universal forwarder



CHAPTER 7

RESULTS AND DISCUSSIONS

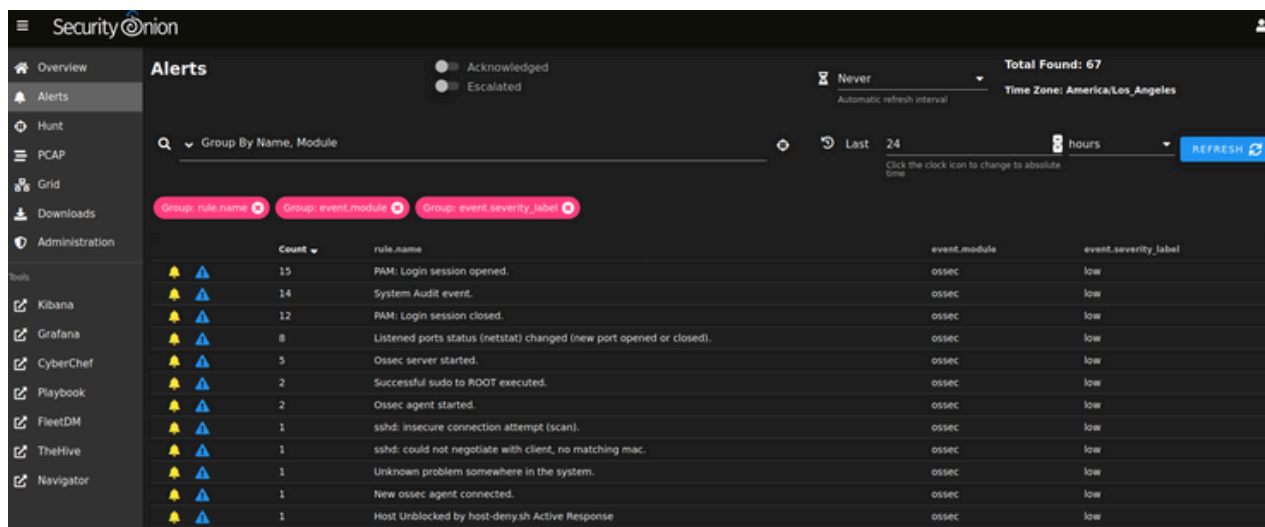


Fig 7.1 IDS logs Dashboard

- As we implemented IDS, IPS, Firewall and SIEM tools from various vendors, we can generate, detect, and monitor logs from these Gateway security devices.
- A secure web gateway protects our network from online security threats and infections by enforcing policy and filtering Internet-bound traffic. A secure web gateway is an on-premise or cloud-delivered network security service. Sitting between users and the Internet, secure web gateways provide advanced network protection by inspecting web requests against security policy to ensure malicious applications and websites are blocked and inaccessible. A secure web gateway includes essential security technologies such as URL filtering, application control, data loss prevention, antivirus, and https inspection to provide organizations with strong web security.
- SIEMs collect logs and events from hundreds of organizational systems (for a partial list, see Log Sources below). Each device generates an event every time something happens, and collects the events into a flat log file or database. The SIEM can collect data in four ways:
 - Via an agent installed on the device (the most common method)
 - By directly connecting to the device using a network protocol or API call
 - By accessing log files directly from storage, typically in Syslog format
 - Via an event streaming protocol like SNMP, Netflow or IPFIX

The SIEM is tasked with collecting data from the devices, standardizing it and saving it in a format that enables analysis.

- Firewall is work on 7 layer that is Application layer but sometimes it may work in 3 and 4 layers of OSI. We implemented our firewall on Kali which having IP: 192.168.2.1. We set rules for web filtering, mail filtering and network inbound and outbound.

CHAPTER 8

FUTURE SCOPE AND CONCLUSION

FUTURE SCOPE

- Stay out of legal problems
- It will help in security testing & development
- Maintain isolated development environment
- Can set up isolated networks for different tasks
- Capture packets and how to use them for diagnostic information
- Run a malware sandbox in an as-safe-as-possible, isolated, virtualized way
- Try running a honeypot in an as-safe-as-possible, isolated, virtualized way

CONCLUSION

- ☒ Stay out of legal problems
- ☐ It will help in security testing & development
- ☐ Maintain isolated development environment
- ☐ It will be sharpening cyber security skills
- ☐ With this one can run a network security device like Sophos UTM (free IIRC) and can evaluate the pros and cons
- ☐ Set up labs and pop boxes from VulnHub
- ☐ During the testing of some techniques which may cause damaging results
- ☐ During the testing, if the researcher uses a malware tool, it could spread to the other Internet-connected environment
- ☐ It is recommended that you have a basic foundation of networking terminology, computers, cybersecurity concepts, and formidable research skills
- ☐ Can set up isolated networks for different tasks
- ☐ Capture packets and how to use them for diagnostic information.

REFERENCES

<https://cybercademy.org/cybersecurity-homelab-project/>

<https://youtu.be/P85L2vwmBKA>

https://youtube.com/playlist?list=PLLDjng0_4bmPWS4lMBEQdBMrQ1EH_mnhh

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

<https://youtube.com/playlist?list=PLDqMNdDvMsRkIGOJBLz2VVJeyt6SKZonD>

<https://youtube.com/playlist?list=PLDqMNdDvMsRkmtiKcZwbhOz7MeLQE0r3G>

<https://scholarworks.unr.edu//handle/11714/3509>

https://www.researchgate.net/publication/357393481_A_Systematic_Literature_Review_on_the_Cyber_Security

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