

Digital SkillUp Africa Final Capstone Project in Cybersecurity

Project Title: Building a Virtual
Cybersecurity Laboratory and Conducting
Android Forensics Investigations

Part Number: THREE

Part Title: Virtual Firewall Implementation

Student Name: ONAEKO, Emmanuel
Oladipupo

Email: eonaeko778@gmail.com

Activites

- Create a virtual pfSense or OPNsense appliance

Configure:

- WAN and LAN interfaces
- NAT, DHCP, and DNS as needed
- Basic firewall rules (e.g., port filtering)
- Connect the Kali and Windows machines to route traffic through the firewall
- Test filtering and logging functionality; document configuration steps and output

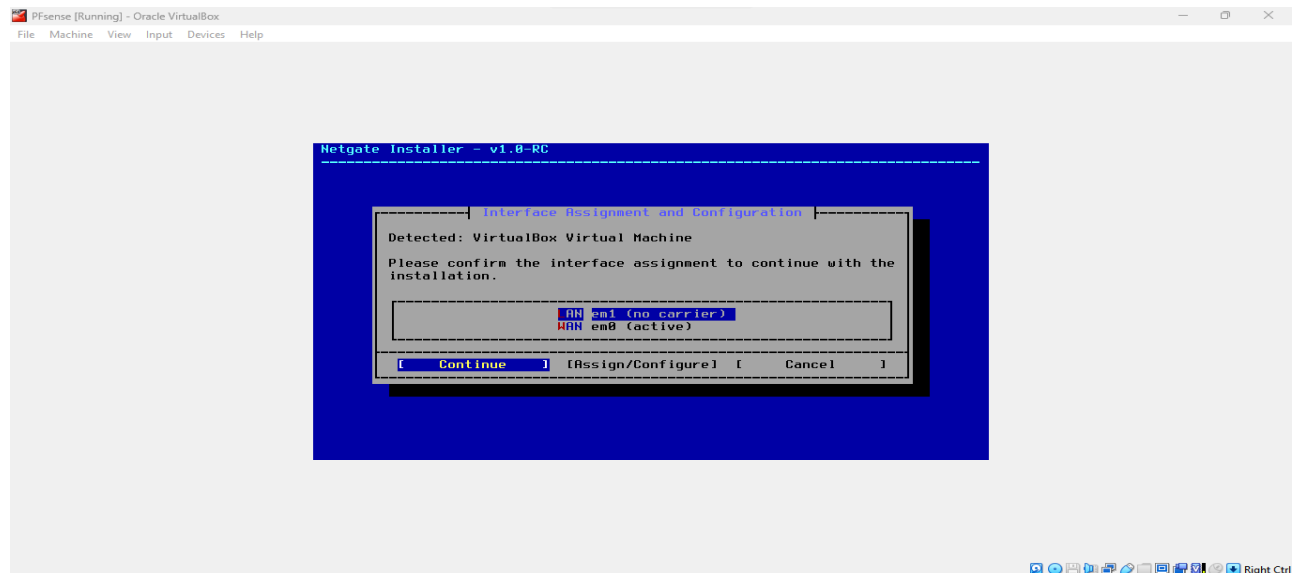
Tools used for this cybersecurity lab setup

Operations	Tools
Hypervisor	Virtual Box
Operating Systems	Kali Linux, Windows
Virtual Firewall	PFsense

pfSense: pfSense is an open-source firewall and router operating system built on FreeBSD. It provides enterprise-grade network security and management features, all accessible through a user-friendly web interface. It can be used by individuals, businesses, schools, and data centers for building reliable and secure network infrastructures.

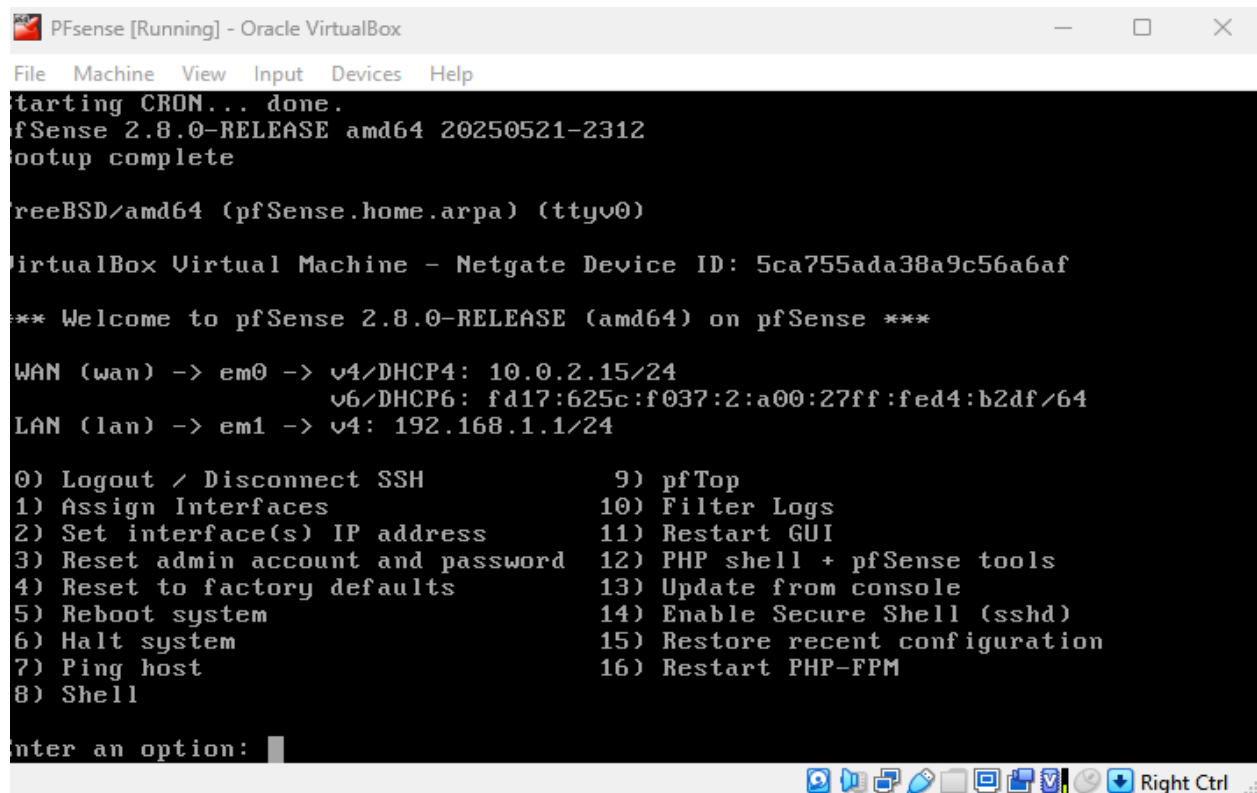
In this report I would five a work through of how I configure and use pfSense as virtual firewall to restrict certain traffic and operations such as visiting certain websites such as altschoolafrica.com and youtube.com and stop pinging from the google DNS server: **8.8.8.8** on my virtual networks which consisted of two virtual machines: Kali Linux and Windows 10

Installation of pfSense

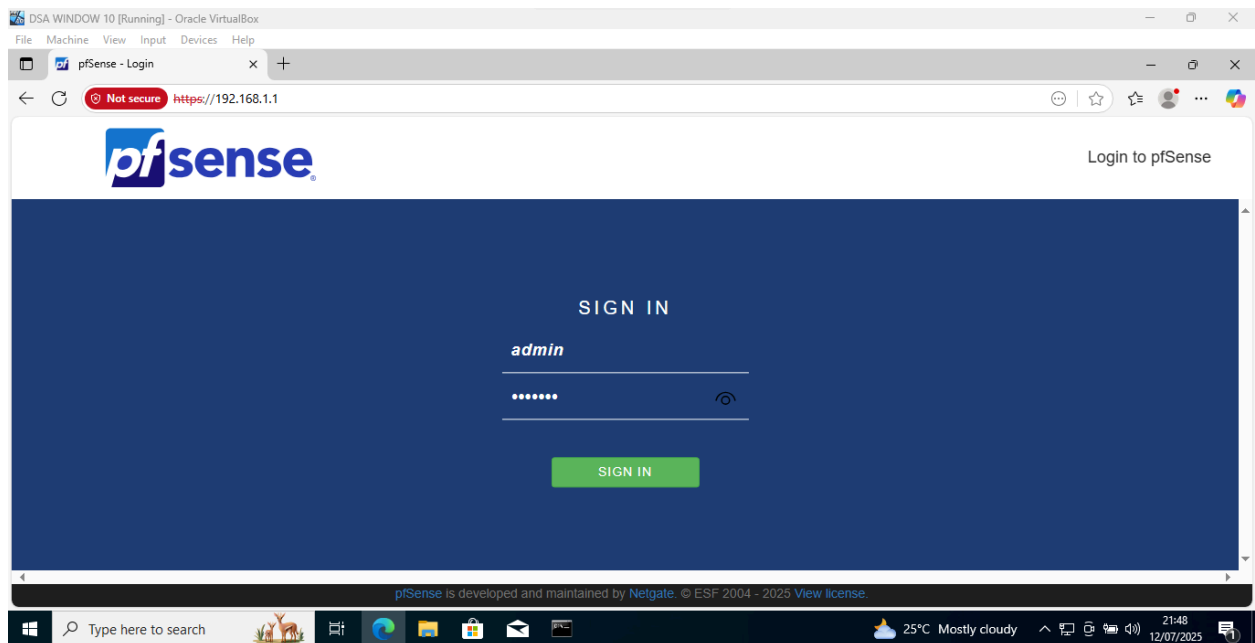


This snippet above shows the installation process of the pfSense virtual appliance on the VirtualBox

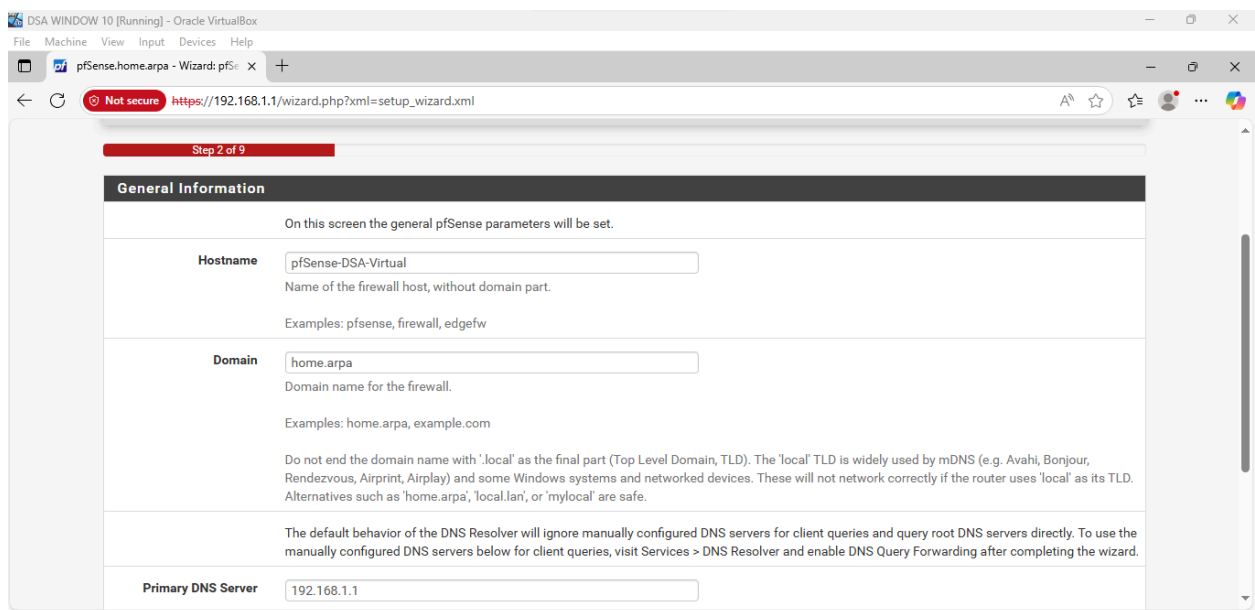
Virtual pfSense installation showing the configuration of LAN and WAN interface

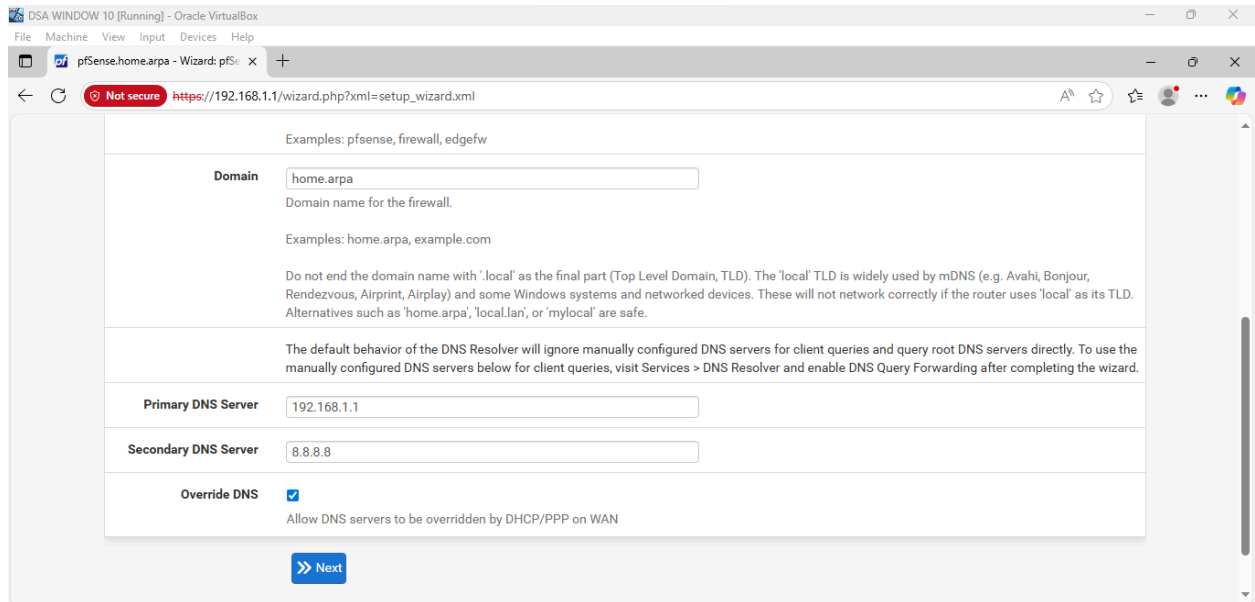


pfSense Start up Interface login

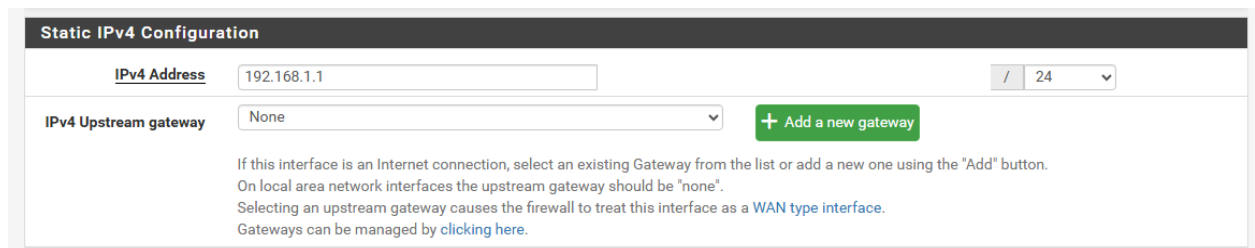


This snippet shows the start up page on the GUI of the pfSense when it was logged in on the windows browser through the **ip address :192.168.1.1** which is the ip address of the pfSense which acted as the default gateway for both VM in the virtual environment and with a default login of **username: admin** and **password :pfsense**, I was able to access the pfSense to access the GUI and make some default configuration which are referenced below

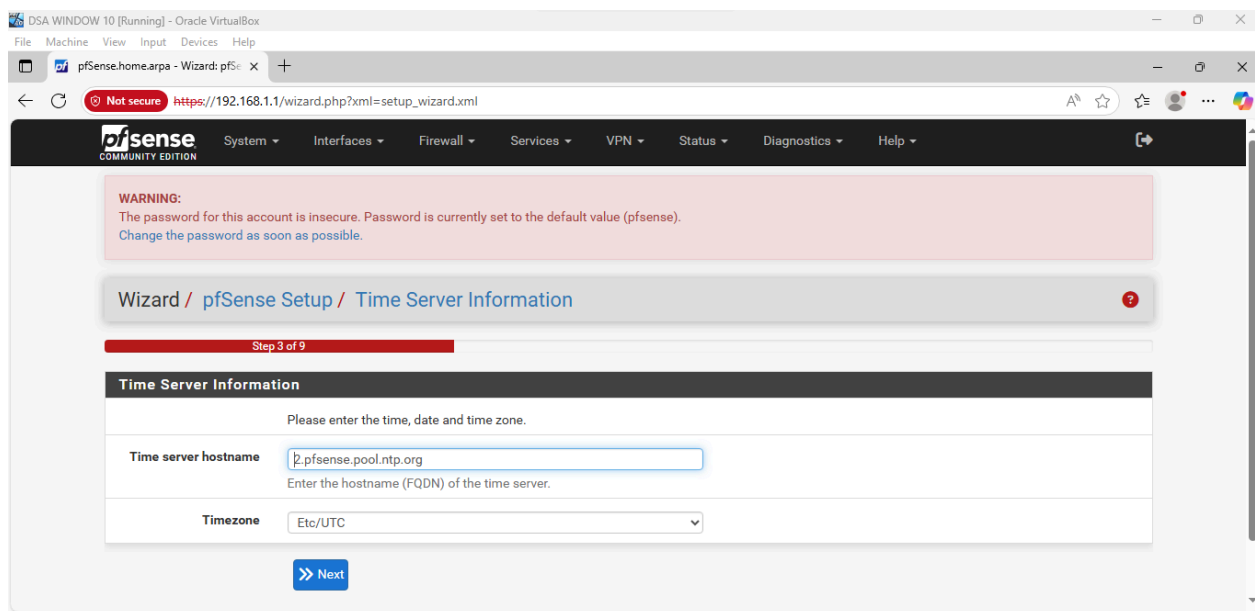




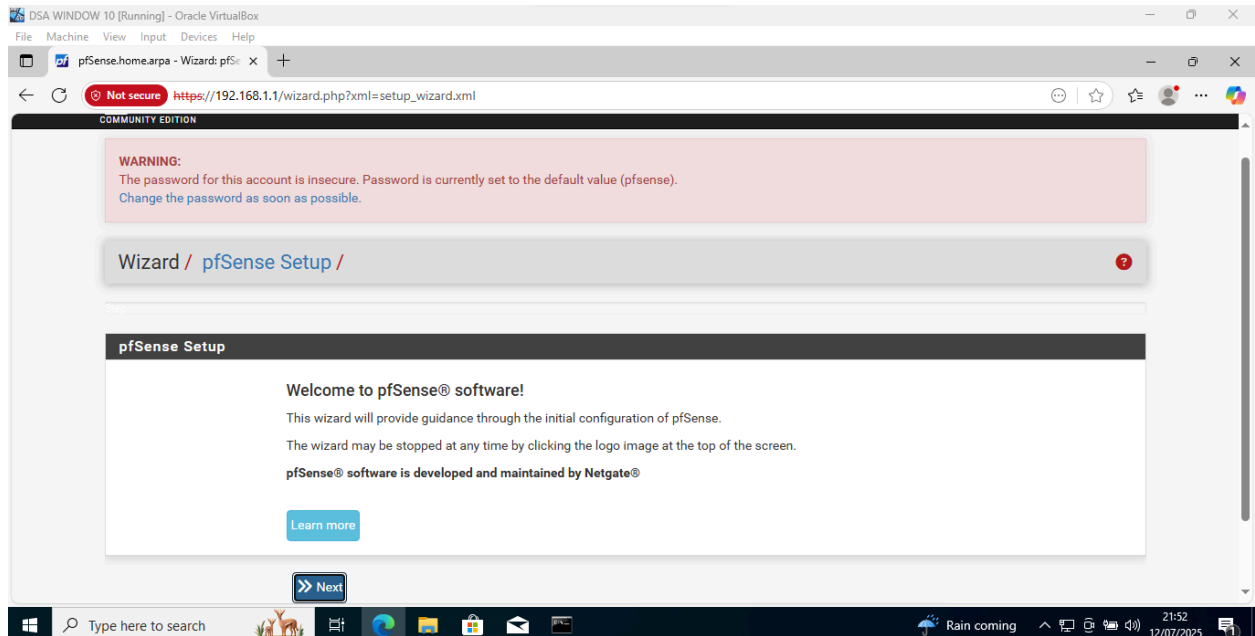
Here i was able to change the hostname and primary DNS server on the pfSense appliance



This shows the static ipv4 configuration of the firewall



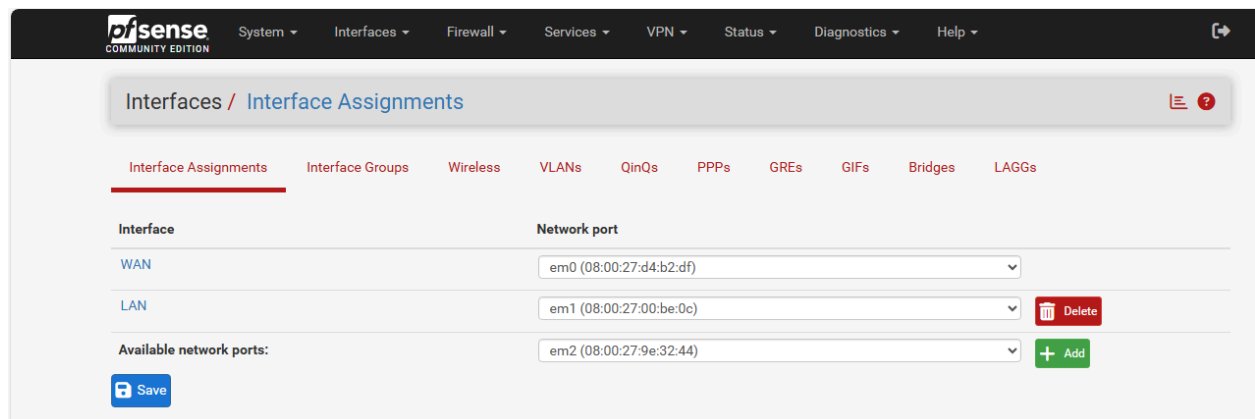
this shows a snippet above shows the configuration of the time server



This snippet above reference the final pfSense setup through the Wizard and further configuration was done manually

Interface Assignments

The section shows the interface assignment on the pfSense showing it WAN and LAN interfaces and what network port are they are on the interface



DSA WINDOW 10 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

pfSense-DSA-Virtual.home.arpa x MSN | Personalized News, Top He x MSN | Personalized News, Top He x +

Not secure https://192.168.1.1/interfaces.php?if=lan

pfSense
COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

Interfaces / LAN (em1)

General Configuration

Enable ☒ Enable interface

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

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type Track Interface

MAC Address xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

DSA WINDOW 10 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

pfSense-DSA-Virtual.home.arpa x MSN | Personalized News, Top He x MSN | Personalized News, Top He x +

Not secure https://192.168.1.1/interfaces.php?if=wan

pfSense
COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

Interfaces / WAN (em0)

General Configuration

Enable ☒ Enable interface

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

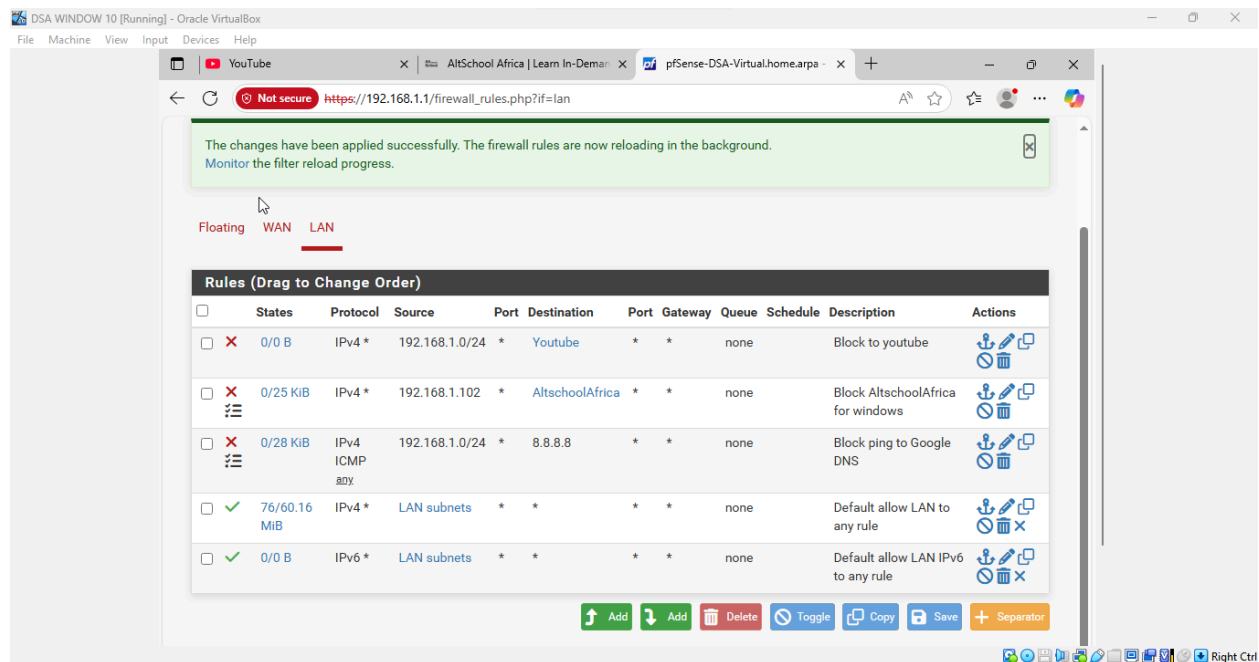
IPv4 Configuration Type DHCP

IPv6 Configuration Type DHCP6

MAC Address xxxxxxxxxxxx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

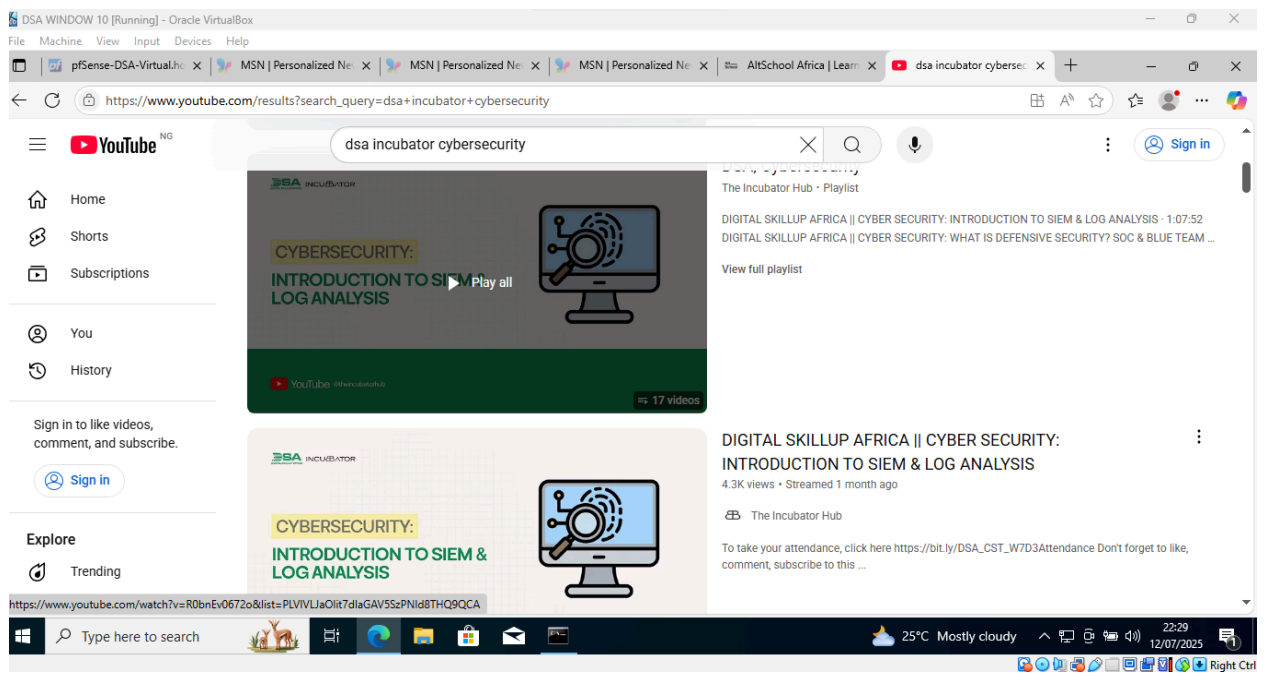
Firewall Rules to block some websites and operations



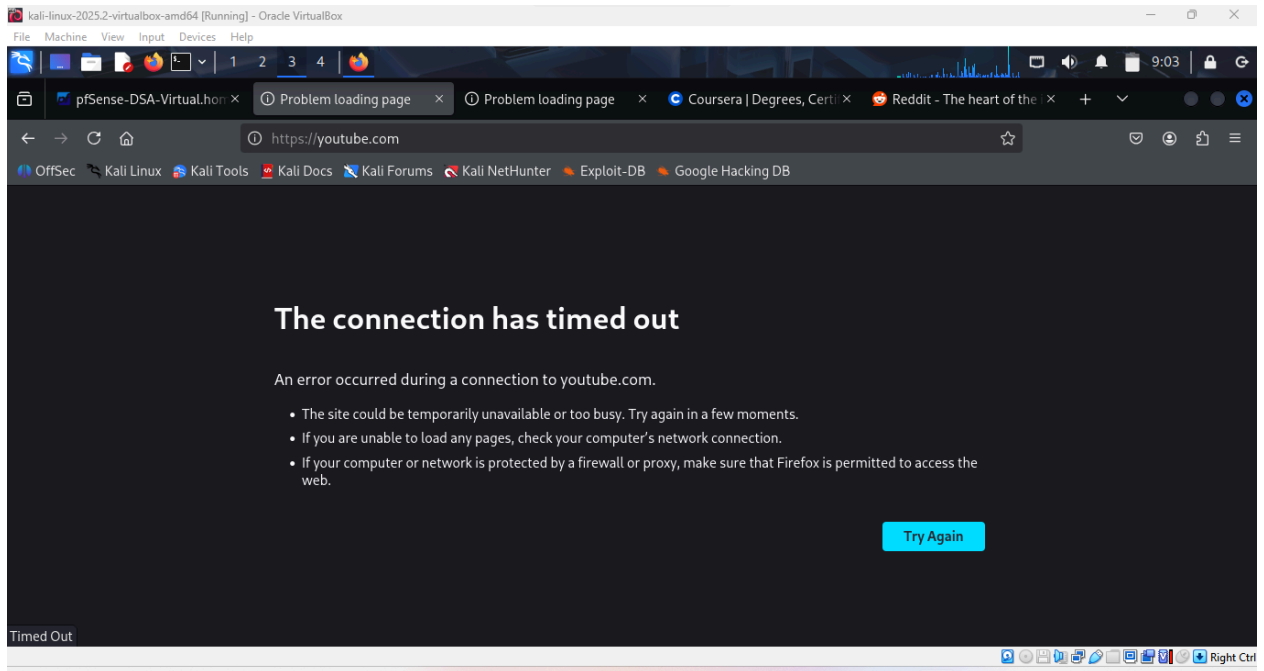
To simulate the functionality of the firewall, I decided to set up some rules of the Firewall section of the GUI and configure the firewall rules on the LAN interface which stated the following

1. Blocking the Whole 192.168.1.0/24 network to from acces the youtube website

Before configuration of Firewall rules, Host were able to access the youtube website

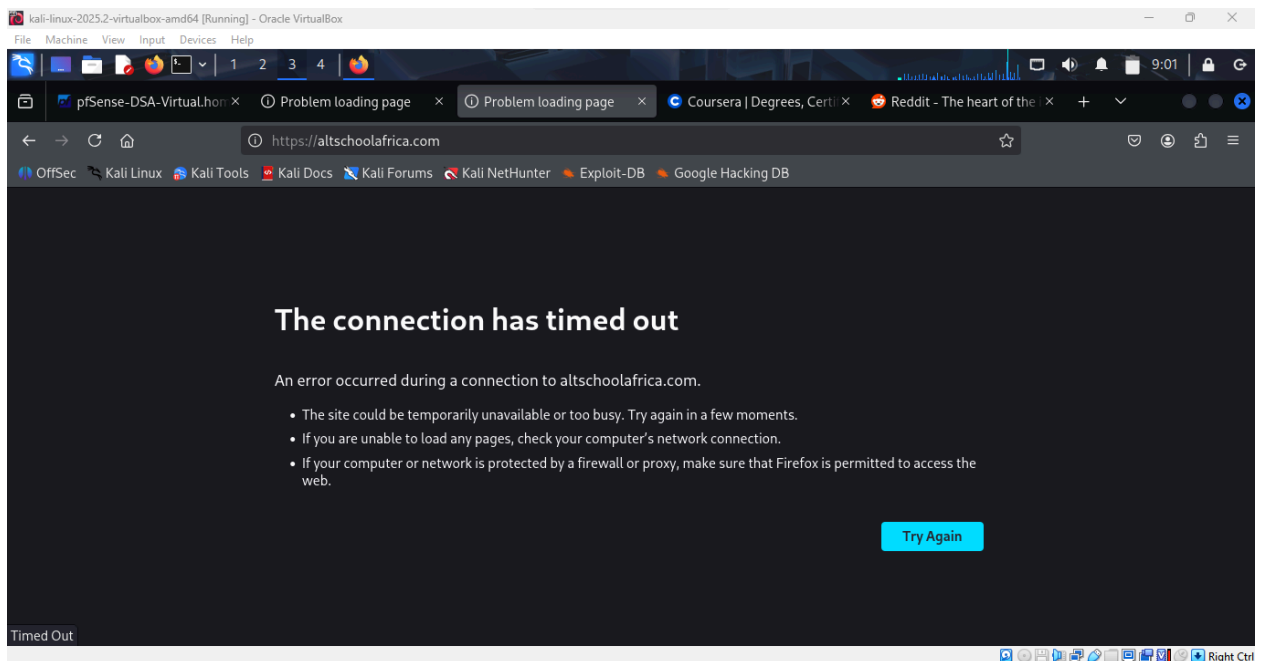


After configuring the Firewall rules applied, Host were unable to access the youtube website

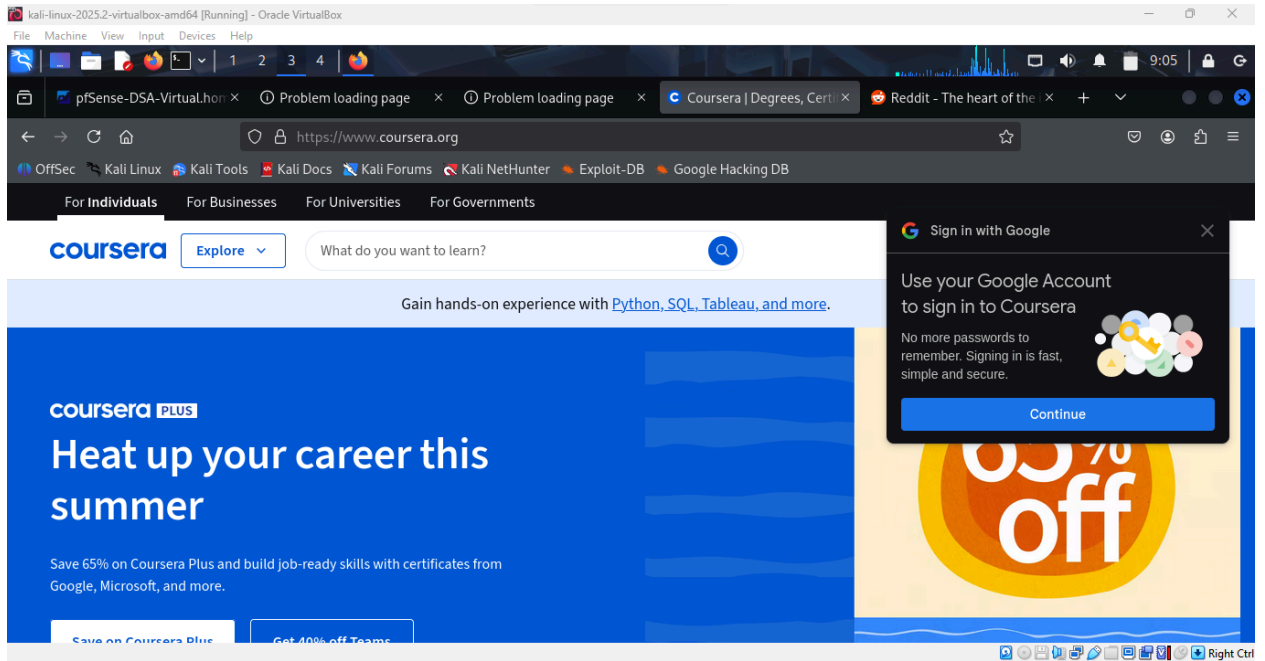


2. Blocking the Kali Linux host from accessing the altschoolafrica.com website

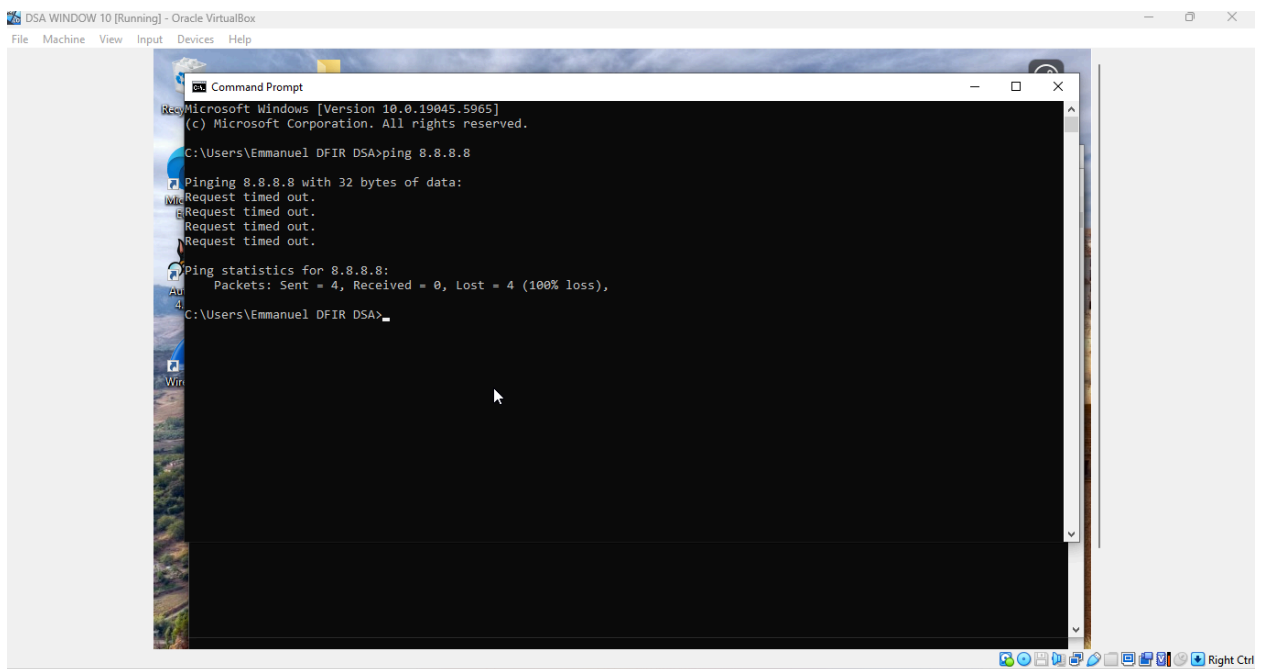
Kali unable to access the altschoolafrica page

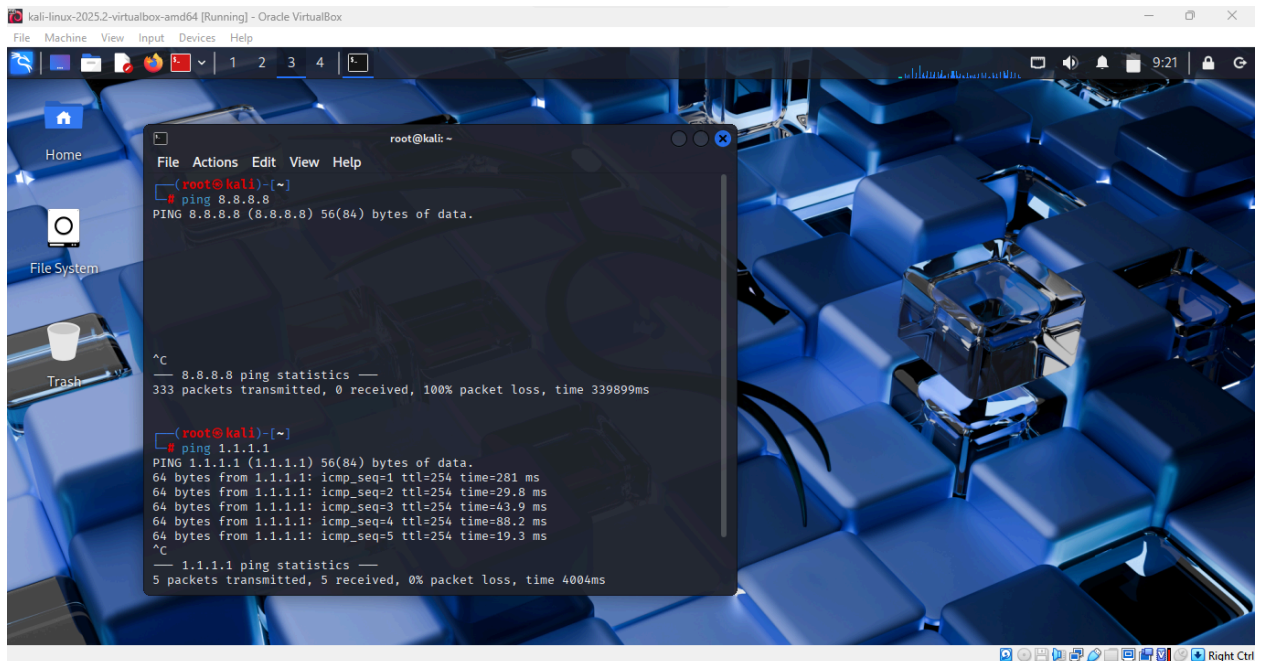


Other websites being able to be accessed buy Kali



3. Blocking the entire LAN network from being able to ping the google DNS server

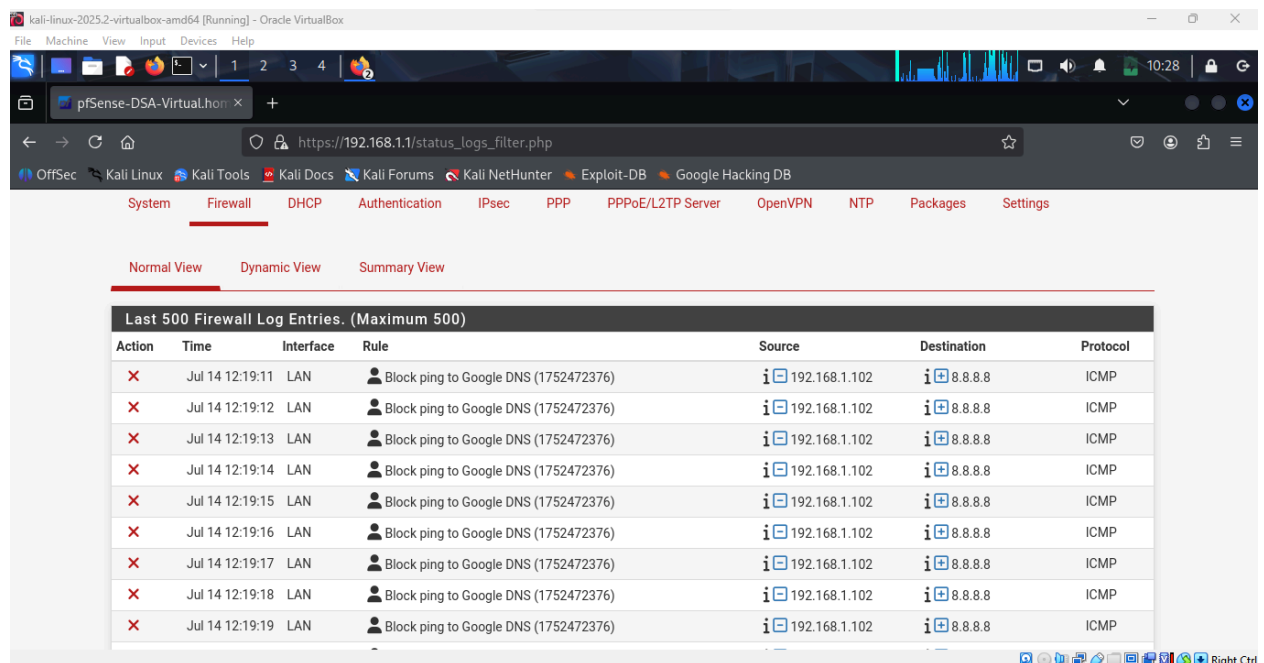




Both Kali and Windows shows a packet drop when pinging the ip address: 8.8.8.8

Firewall Logs

The session below show the firewall logs captured on the firewall giving a view of the functionality of the firewall rules set up



Conclusion

In this project I was exposed the capability and functionality of the firewall in blocking and filtering traffic which open up understanding of traffic engineering and how important it is in network security and ensuring that hosts are safe on the network