

# 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](mailto: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

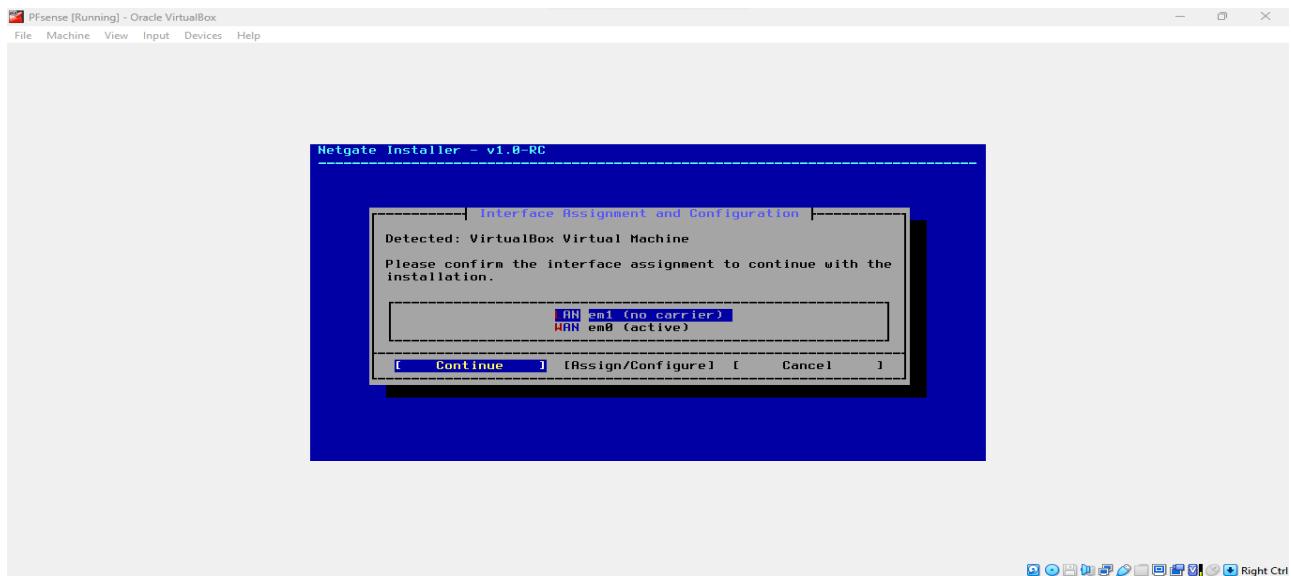
## Tools used for this cybersecurity lab setup

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.

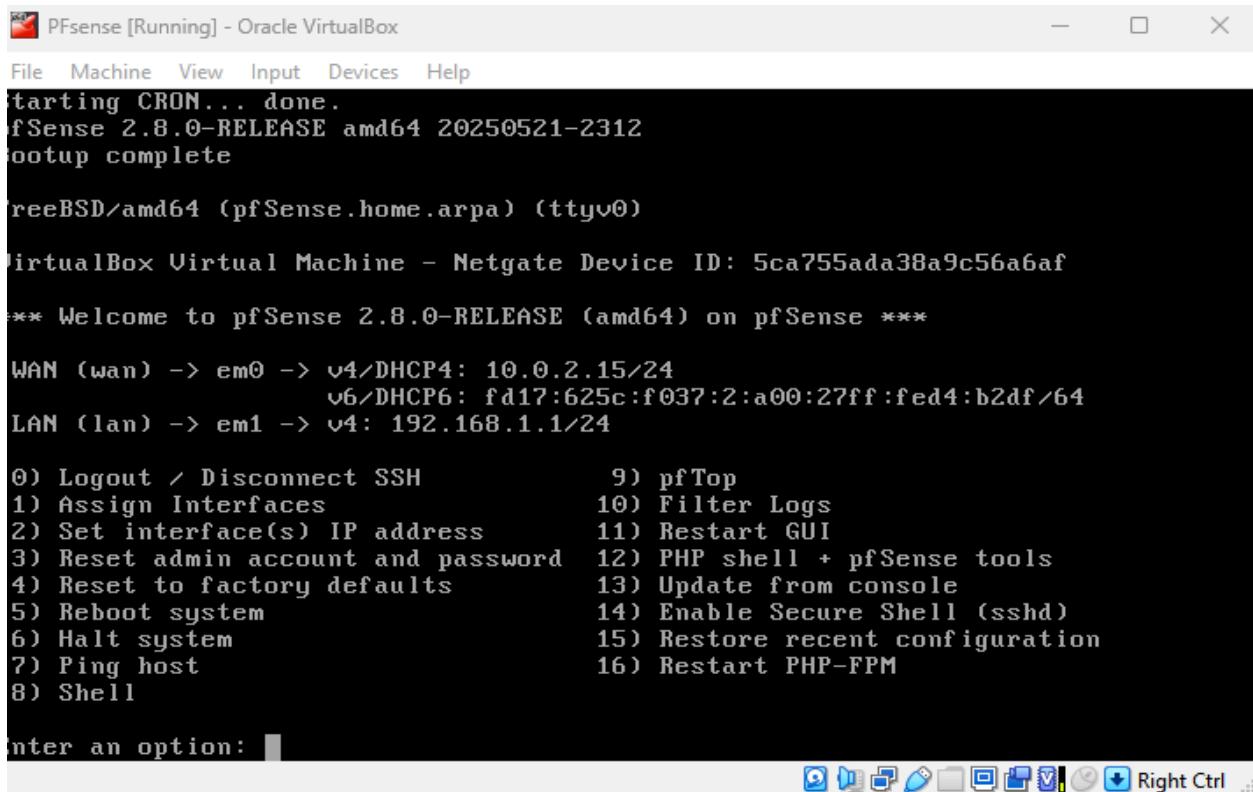
In this report I would give a work through of how I configure and use pfSense as virtual firewall to restrict certain traffic and operations such as visiting certain websites such as [altschoolafica.com](http://altschoolafica.com) and [youtube.com](http://youtube.com) and stop pinging from the google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

## Installation of pfSense

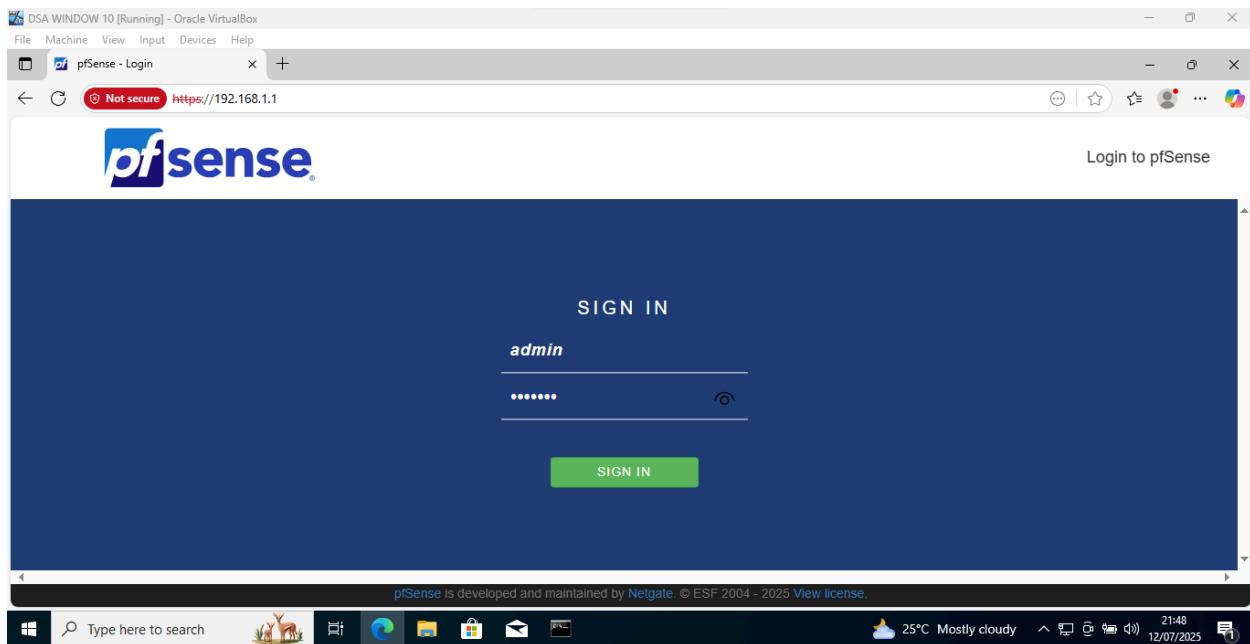


This snippet above shows the installation process of the pfSense virtual appliance on the VirtualBox

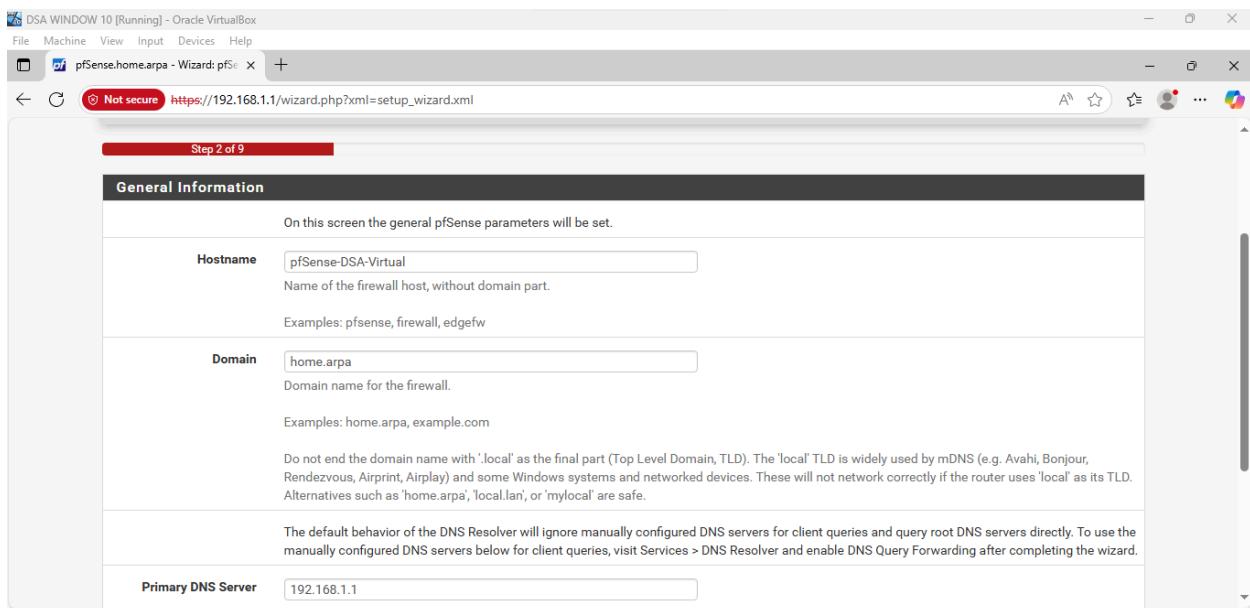
## Virtual pfSense installation showing the configuration of LAN and WAN interface

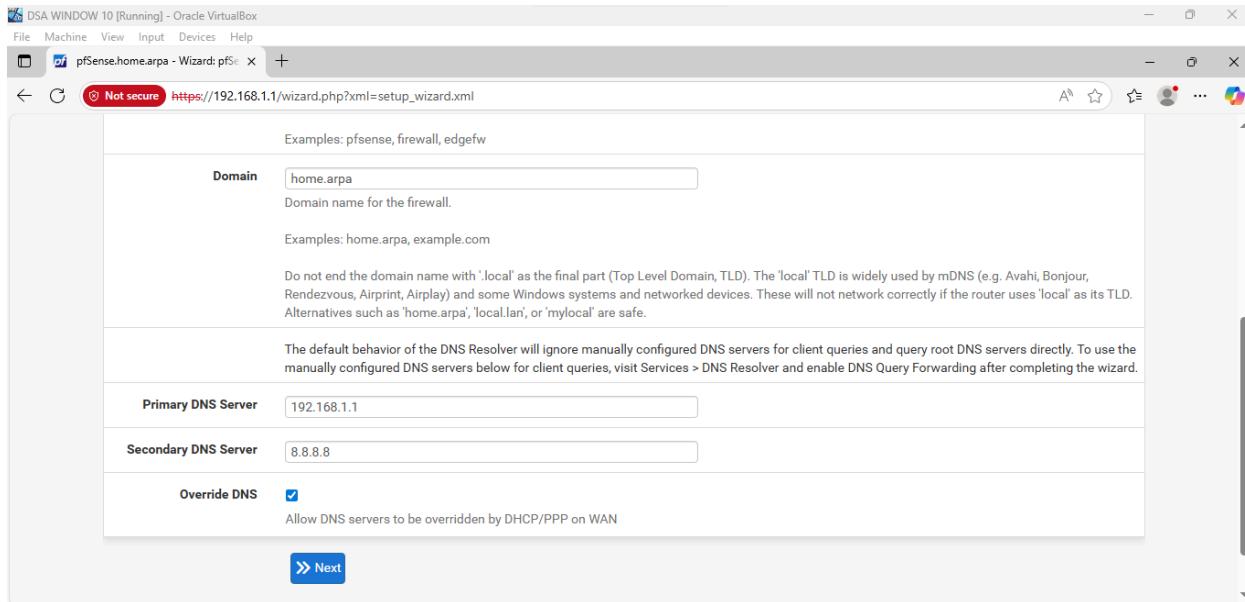


## pfSense Start up Interface login

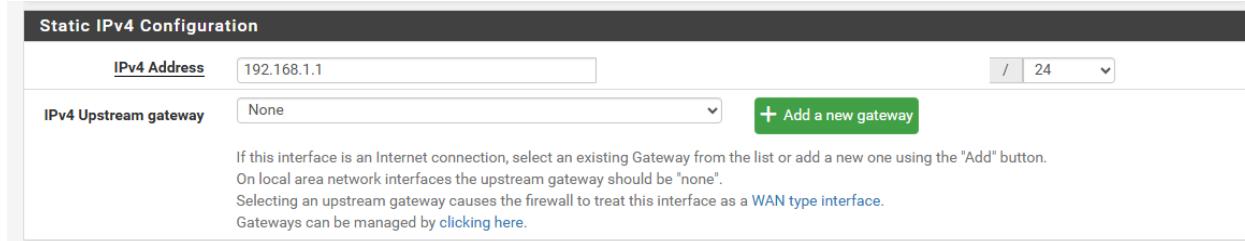


This snippet shows the start up page on the GUI of the pfSense when it was logged in on the windows browser through the **ip address :192.168.1.1** which is the ip address of the pfSense which acted as the default gateway for both VM in the virtual environment and with a default login of **username: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

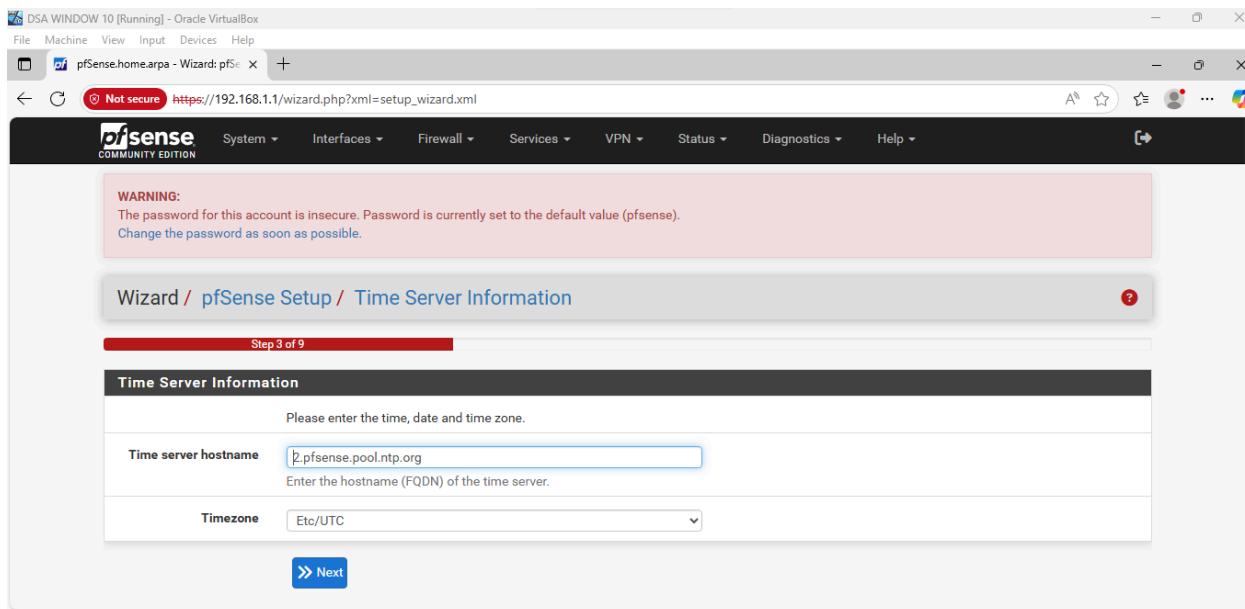




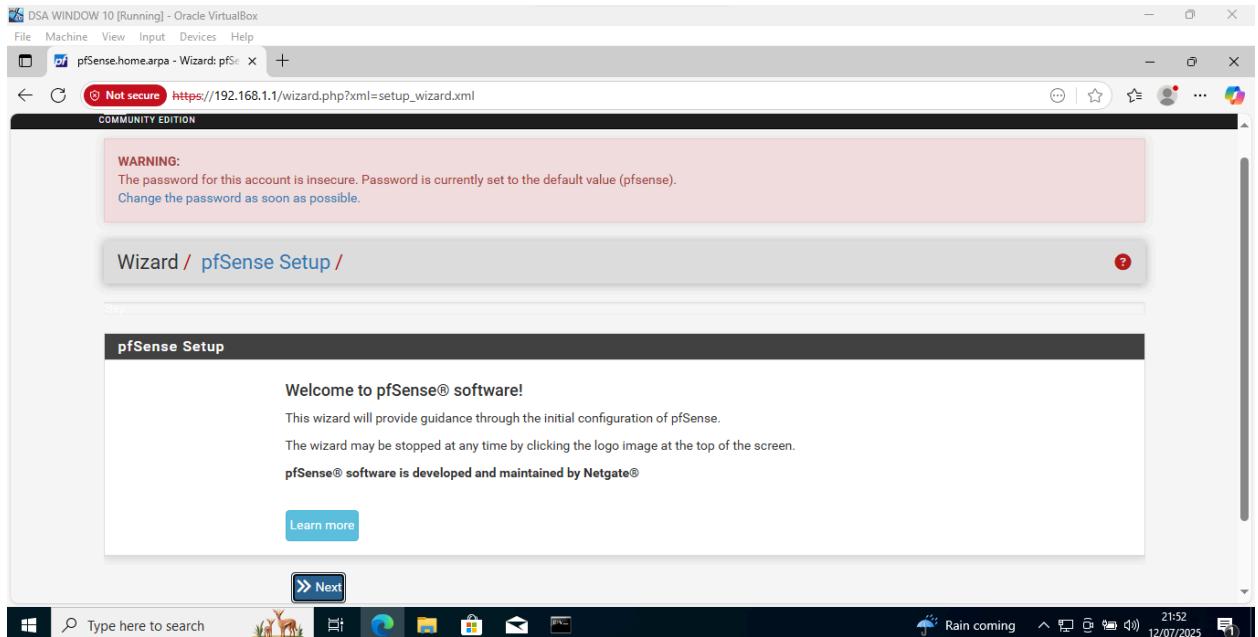
Here i was able to change the hostname and primary DNS server on the pfSense appliance



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

Interface	Network port
WAN	em0 (08:00:27:d4:b2:df)
LAN	em1 (08:00:27:00:be:0c) <span style="color:red;">Delete</span>
Available network ports:	em2 (08:00:27:9e:32:44) <span style="color:green; border:1px solid green; padding:2px;">+ Add</span>

DSA WINDOW 10 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

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.

https://192.168.1.1

DSA WINDOW 10 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

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** 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.

## Firewall Rules to block some websites and operations

The screenshot shows the pfSense Firewall Rules configuration page. A message at the top states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." Below this, there are tabs for Floating, WAN, and LAN, with LAN selected. The main area displays a table of rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	192.168.1.0/24	*	Youtube	*	*	none		Block to youtube	
0/25 KIB	IPv4 *	192.168.1.102	*	AltschoolAfrica	*	*	none		Block AltschoolAfrica for windows	
0/28 KIB	IPv4 ICMP any	192.168.1.0/24	*	8.8.8.8	*	*	none		Block ping to Google DNS	
76/60.16 Mib	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

At the bottom are buttons for Add, Delete, Toggle, Copy, Save, and Separator.

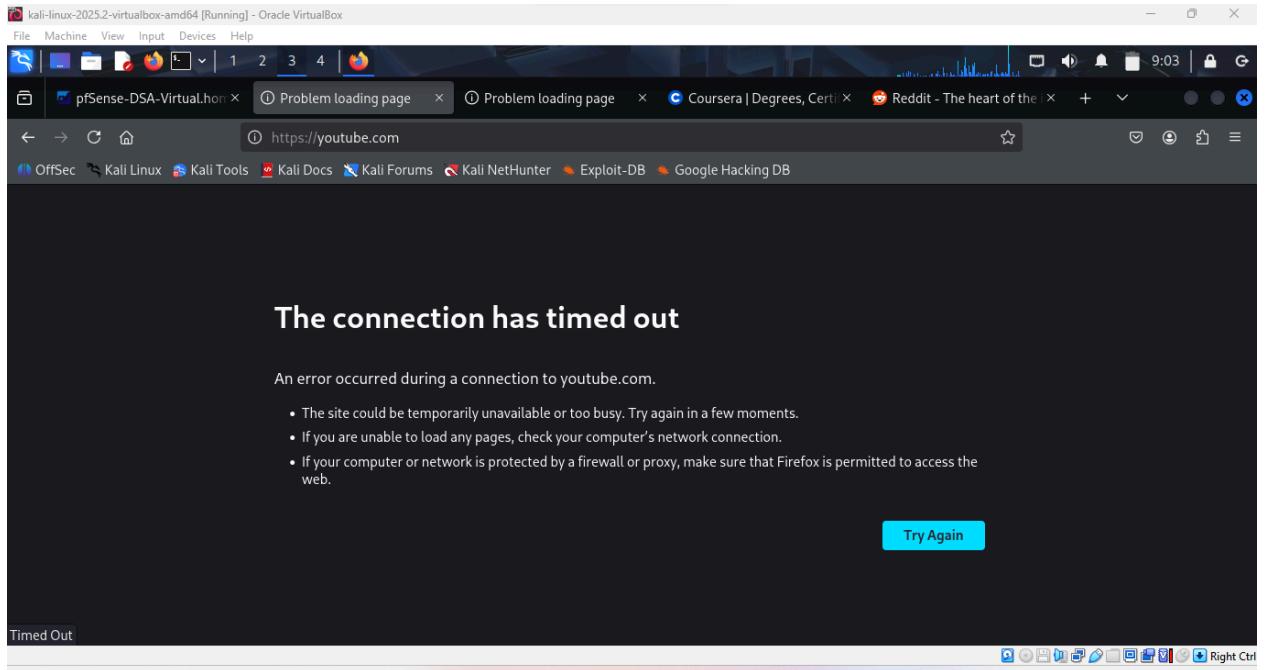
To simulate the functionality of the firewall, I decided to set up some rules of the Firewall section of the GUI and configure the firewall rules on the LAN interface which stated the following

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**

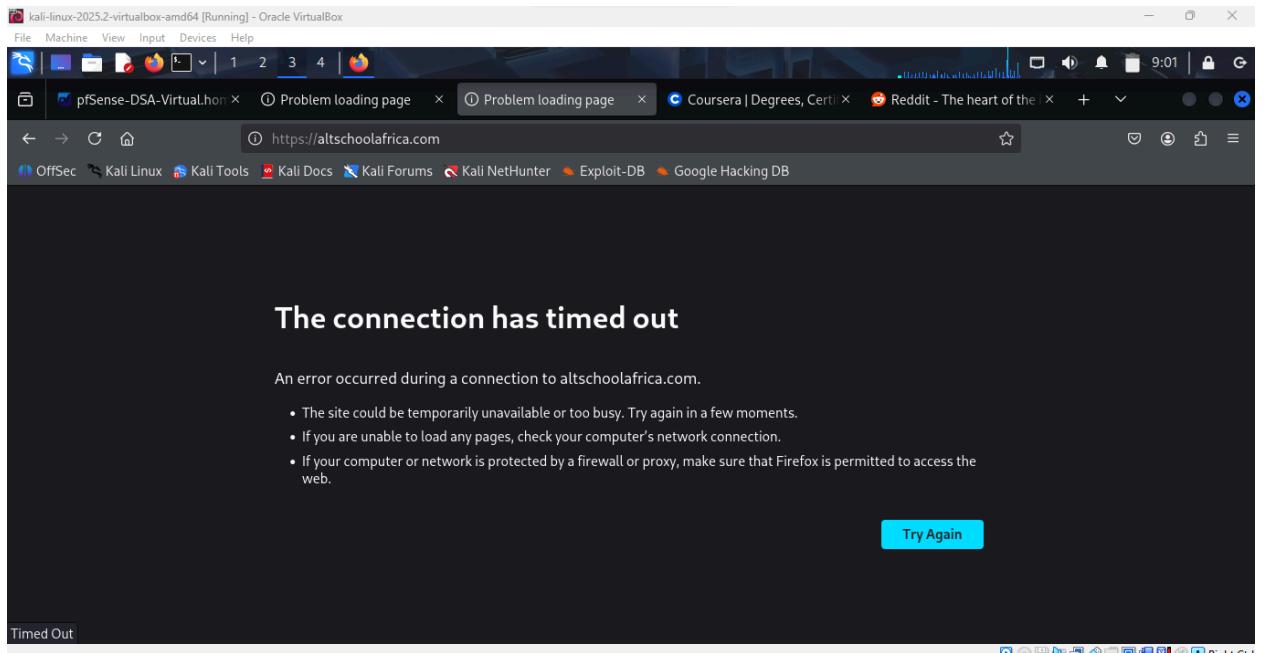
The screenshot shows a browser window displaying the results of a YouTube search for "dsa incubator cybersecurity". The search results page shows a video thumbnail for "CYBERSECURITY: INTRODUCTION TO SIEM & LOG ANALYSIS" by "The Incubator Hub". The video has 17 views and was uploaded 1 month ago. The browser's address bar shows the URL: [https://www.youtube.com/results?search\\_query=dsa+incubator+cybersecurity](https://www.youtube.com/results?search_query=dsa+incubator+cybersecurity).

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

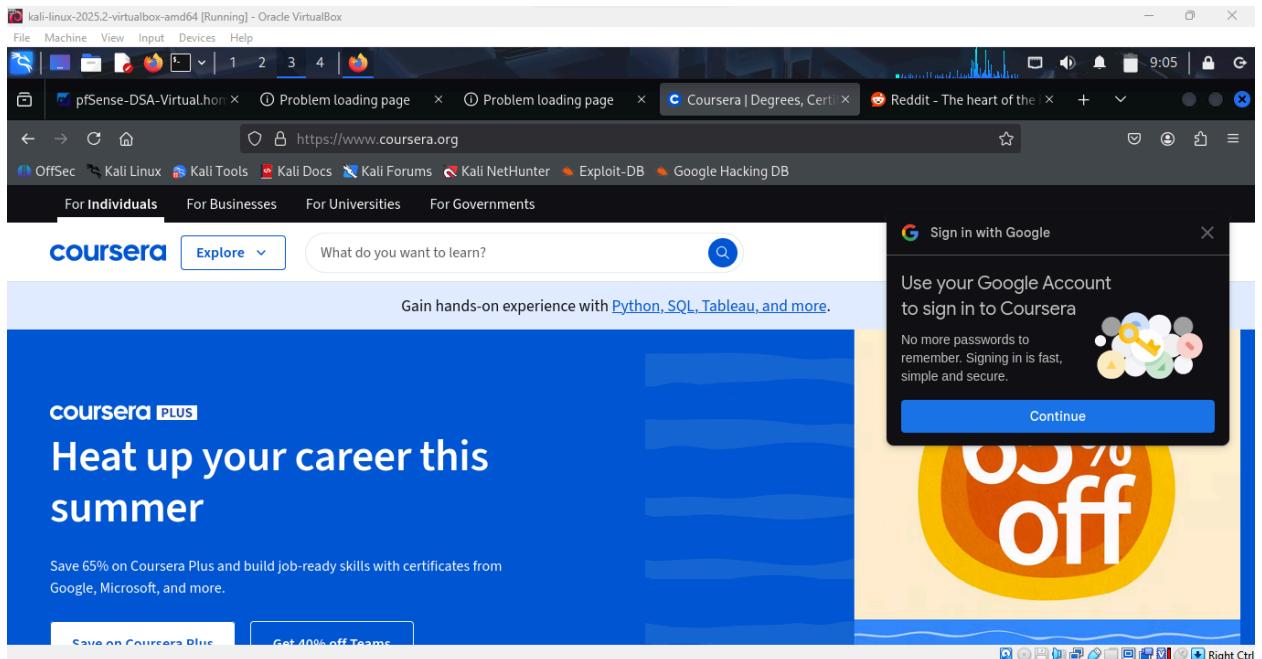


**2. Blocking the Kali Linux host from accessing the [altschoolafrica.com](https://altschoolafrica.com) website**

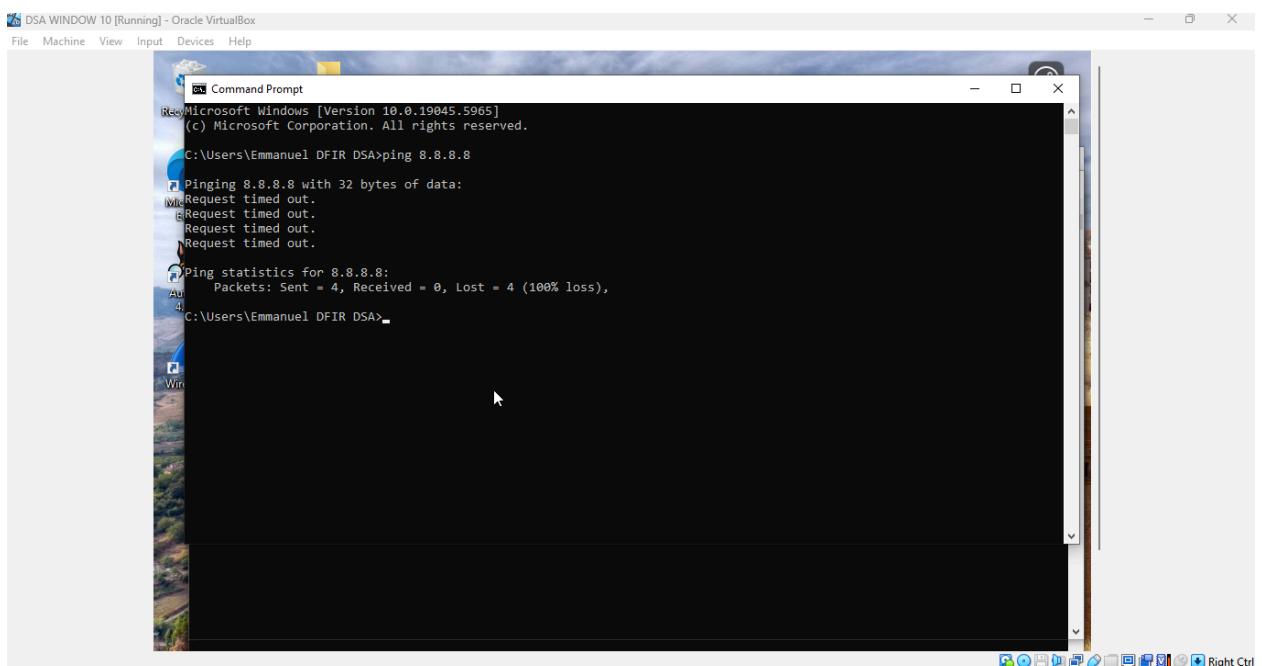
**Kali unable to access the altschoolafrica page**



**Other websites being able to be accessed by Kali**



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



```

root@kali: ~
File Actions Edit View Help
[root@kali ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

^C
8.8.8.8 ping statistics --
333 packets transmitted, 0 received, 100% packet loss, time 339899ms

[root@kali ~]# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=254 time=281 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=254 time=29.8 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=254 time=43.9 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=254 time=88.2 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=254 time=19.3 ms
^C
1.1.1.1 ping statistics --
5 packets transmitted, 5 received, 0% packet loss, time 4004ms

```

**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

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Jul 14 12:19:11	LAN	Block ping to Google DNS (1752472376)	i 192.168.1.102	i 8.8.8.8	ICMP
✗	Jul 14 12:19:12	LAN	Block ping to Google DNS (1752472376)	i 192.168.1.102	i 8.8.8.8	ICMP
✗	Jul 14 12:19:13	LAN	Block ping to Google DNS (1752472376)	i 192.168.1.102	i 8.8.8.8	ICMP
✗	Jul 14 12:19:14	LAN	Block ping to Google DNS (1752472376)	i 192.168.1.102	i 8.8.8.8	ICMP
✗	Jul 14 12:19:15	LAN	Block ping to Google DNS (1752472376)	i 192.168.1.102	i 8.8.8.8	ICMP
✗	Jul 14 12:19:16	LAN	Block ping to Google DNS (1752472376)	i 192.168.1.102	i 8.8.8.8	ICMP
✗	Jul 14 12:19:17	LAN	Block ping to Google DNS (1752472376)	i 192.168.1.102	i 8.8.8.8	ICMP
✗	Jul 14 12:19:18	LAN	Block ping to Google DNS (1752472376)	i 192.168.1.102	i 8.8.8.8	ICMP
✗	Jul 14 12:19:19	LAN	Block ping to Google DNS (1752472376)	i 192.168.1.102	i 8.8.8.8	ICMP

## **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