Project Title "Design and Implementation of a Network Security Monitoring System"

Project Description

In this project, you will set up a virtual lab to simulate a secure network environment. You will use tools like pfSense, Snort, and Suricata for network monitoring and intrusion detection, and you will practice active and passive information gathering techniques. The goal is to learn how to monitor and secure a network by identifying threats and anomalies in network traffic.

Project Objectives

1. Understand and implement active and passive information-gathering techniques.

2. Set up and configure pfSense as a firewall and network gateway.

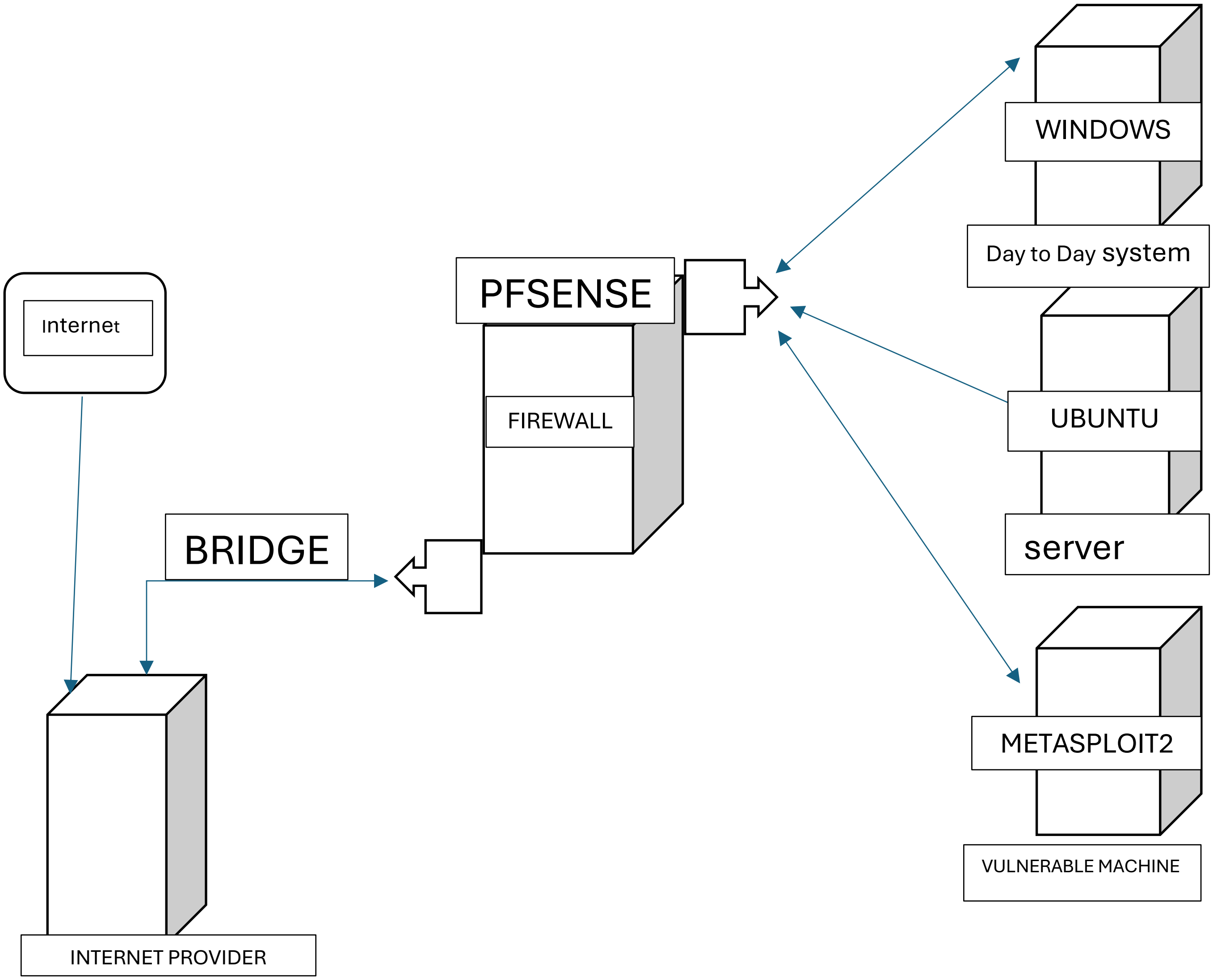
3. Install and configure Snort and Suricata for intrusion detection and prevention.

4. Analyze network traffic to identify malicious activities using IP addresses and protocols.

5. Document findings and propose security recommendations.

1. Pfsense: as a firewall has two interfaces, one for the internal network and the other for external network and each interface with its own IP address. The internal network IP is used as a default gateway for OS in the internal network. The bridge interface IP is used by the pfsense to browse with the help of the Network provider. 2. Metaspoiltable 2: Has only one interface so we Connect its adapter to the internal network. 3. The other OS (windows 10 , Ubuntu): Can power two adapters at once, so they are connected to the bridge and internal network interfaces. a. Bridge network: Enables the OS go to the network provider independently outside the internal network connection. b. Internal network: Binds the OS together under an internal LAN and it doesn't browse, that is why the bridge network is included in the network design.
2. The other OS (windows server, windows 10 & 11, Ubuntu): Can power two
3. adapters at once, so they are connected to the bridge and internal network
4. interfaces.
5. a. Bridge network: Enables the OS go to the network provider independently
6. outside the internal network connection.
7. b. Internal network: Binds the OS together under an internal LAN and it doesn't
8. browse, that is why the bridge network is included in the network design.

NETWORK DIAGRAM



1.Ubuntu (attack system)

2.Windows 10 (victim system)

3.Metasploit 2 (down vulnerable machine

4.pfsense (firewall)

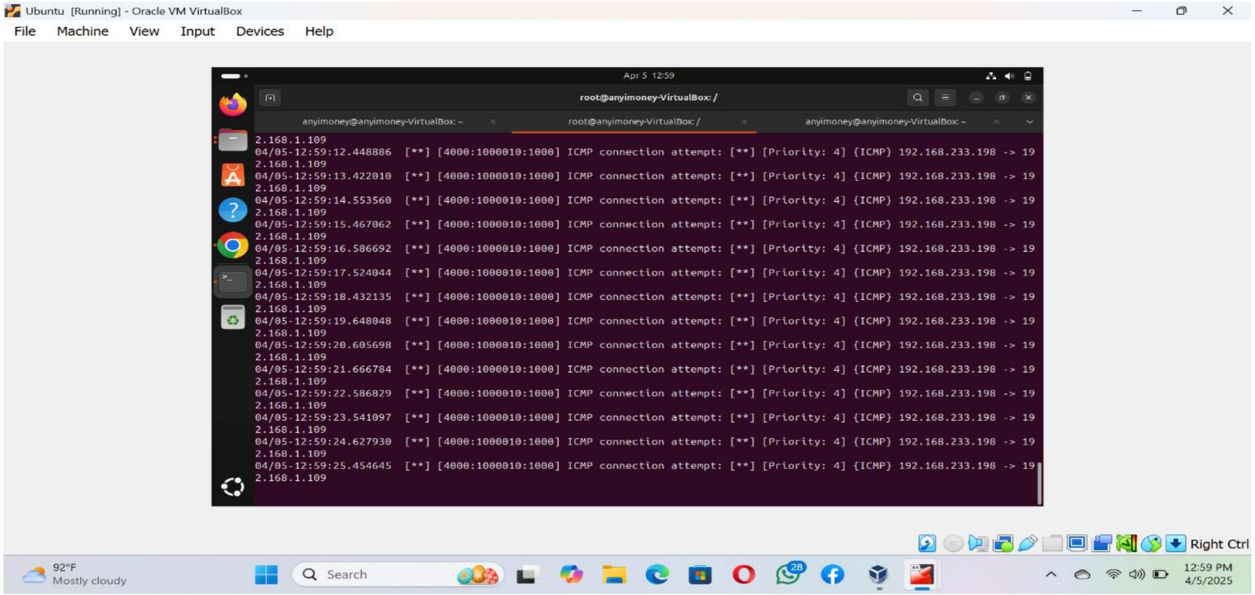
Note: I used a network configuration of bridge and internal network for a good result

Then you confirm the connection by pinging each machine to one another.

Step 1. {Using Snort as intrusion detection services.}

Then once the pinging is successful, you enter your ubuntu machine update and upgrade your ubuntu and install snort via the curl process (Sudo apt install snort-y) while install you will be asked for the network you wants to monitor, if you are going with internal network then you will have to go with an Ip like this 192.168.1.0/24 then click okay and wait for it to fully load.

Then once it has fully downloaded, locate your part of the newly downloaded snort via your terminal configure your HOME_NET and set up the rest configuration then set up your local rules correctly with the message you wants it to drop once a traffic is detected, after that you update your snort if it went successful then restart the snort, then go and ping your ubuntu with kali after you might have turn on the console mode command at your ubuntu terminal then you should able to see the rules you wrote displaying at your dashboard with the message along with it


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Apr 5 12:59
root@anyimoney-VirtualBox: /
anyimoney@anyimoney-VirtualBox: ~
root@anyimoney-VirtualBox: /
anyimoney@anyimoney-VirtualBox: ~
Right Ctrl
92°F
Mostly cloudy
Search
12:59 PM
4/5/2025

```
2.168.1.109
04/05-12:59:12.448886  [**] [4000:1000010:1000] ICMP connection attempt: [**] [Priority: 4] {ICMP} 192.168.233.198 -> 19
2.168.1.109
04/05-12:59:13.422010  [**] [4000:1000010:1000] ICMP connection attempt: [**] [Priority: 4] {ICMP} 192.168.233.198 -> 19
2.168.1.109
04/05-12:59:14.553560  [**] [4000:1000010:1000] ICMP connection attempt: [**] [Priority: 4] {ICMP} 192.168.233.198 -> 19
2.168.1.109
04/05-12:59:15.467062  [**] [4000:1000010:1000] ICMP connection attempt: [**] [Priority: 4] {ICMP} 192.168.233.198 -> 19
2.168.1.109
04/05-12:59:16.586692  [**] [4000:1000010:1000] ICMP connection attempt: [**] [Priority: 4] {ICMP} 192.168.233.198 -> 19
2.168.1.109
04/05-12:59:17.524044  [**] [4000:1000010:1000] ICMP connection attempt: [**] [Priority: 4] {ICMP} 192.168.233.198 -> 19
2.168.1.109
04/05-12:59:18.432135  [**] [4000:1000010:1000] ICMP connection attempt: [**] [Priority: 4] {ICMP} 192.168.233.198 -> 19
2.168.1.109
04/05-12:59:19.648048  [**] [4000:1000010:1000] ICMP connection attempt: [**] [Priority: 4] {ICMP} 192.168.233.198 -> 19
2.168.1.109
04/05-12:59:20.605698  [**] [4000:1000010:1000] ICMP connection attempt: [**] [Priority: 4] {ICMP} 192.168.233.198 -> 19
2.168.1.109
04/05-12:59:21.666784  [**] [4000:1000010:1000] ICMP connection attempt: [**] [Priority: 4] {ICMP} 192.168.233.198 -> 19
2.168.1.109
04/05-12:59:22.586829  [**] [4000:1000010:1000] ICMP connection attempt: [**] [Priority: 4] {ICMP} 192.168.233.198 -> 19
2.168.1.109
04/05-12:59:23.541097  [**] [4000:1000010:1000] ICMP connection attempt: [**] [Priority: 4] {ICMP} 192.168.233.198 -> 19
2.168.1.109
04/05-12:59:24.627930  [**] [4000:1000010:1000] ICMP connection attempt: [**] [Priority: 4] {ICMP} 192.168.233.198 -> 19
2.168.1.109
04/05-12:59:25.454645  [**] [4000:1000010:1000] ICMP connection attempt: [**] [Priority: 4] {ICMP} 192.168.233.198 -> 19
2.168.1.109
```

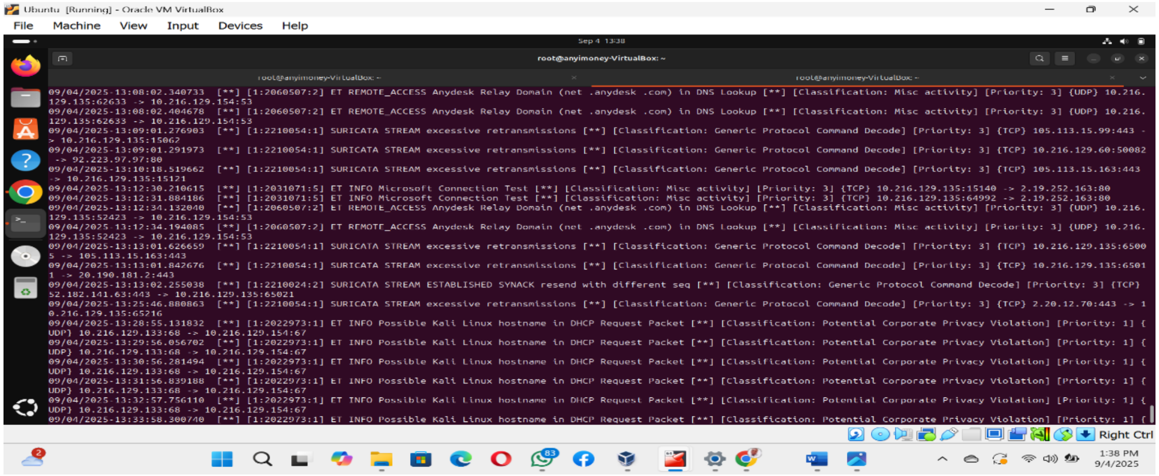
Step 2. {Using Suricata as Ips, Intrusion prevention services}.

Still making use of your Ubuntu machine install suricata via curl:{sudo apt install suricata –y, then once it has successfully download} locate the part of the downloaded suricata via your ubuntu terminal then locate the HOME_NET and input your network IP and also set the network interface you want to monitor Enp0s8 or Ether, make the community id true and make sure you set the right interface you wants to monitor after that you locate your default rule then test it with your console mode if it went well you are going to receive a successful message, then after that you locate your suricata.conf look for the costume roles then create your own role folder and file inside then nano it and add your costume role inside you can make use of snorpy to write a blocking role copy and paste it there save and exit then update your suricata once it's done successful then you should go to kali browser and search for suricata documentation then locate the suricata rules copy the curl command and paste on the kali terminal then you should restart your suricata and activate the console mode which should stop your kali from pinging your ubuntu then you should check your log file for the message concerning the rule you have written.

Step 3. Active and passive information gathering via Nmap {Nmap –T4 –A –v –Pn {internal network}

Report = total host [255] , Total host up [3] = 255 –3 = 252, Total host down [252]

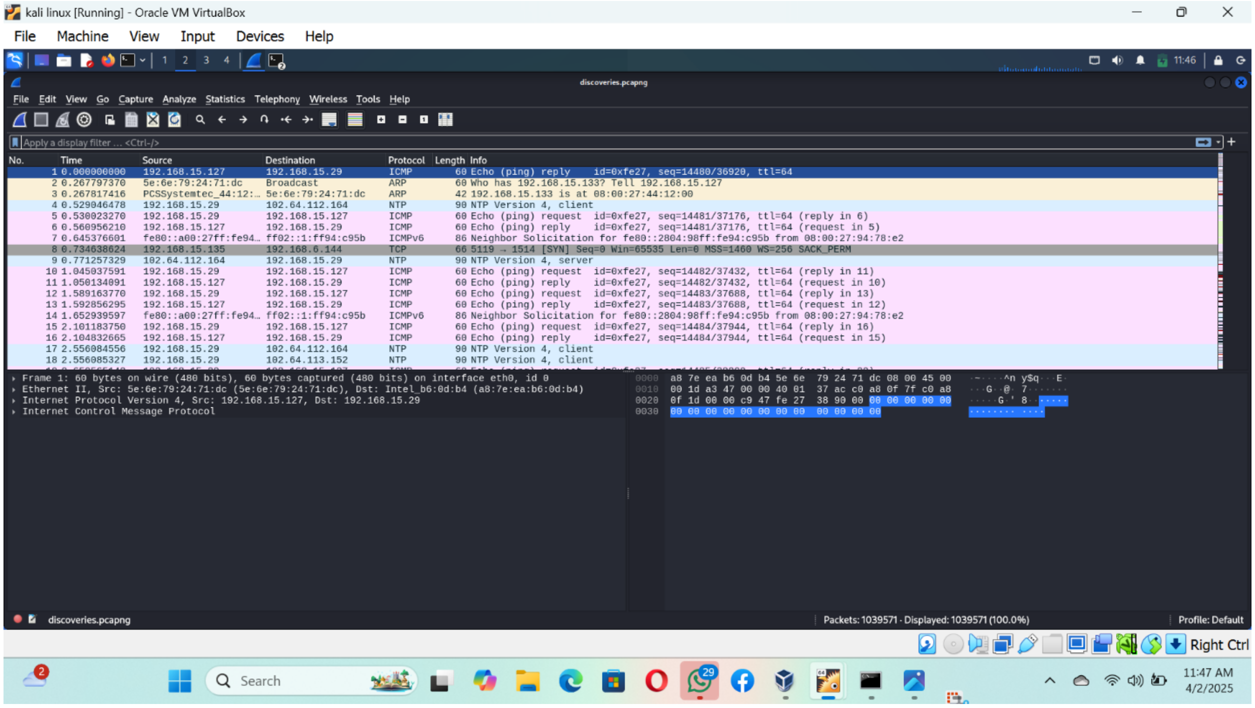
Dns resolution = 0 Syn Scan = 10.216.129.198



Ubuntu [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Sep 4 13:38
root@anyimoney-VirtualBox: ~
root@anyimoney-VirtualBox: ~
root@anyimoney-VirtualBox: ~
Right Ctrl
1:38 PM
9/4/2025

```
09/04/2025-13:08:02.340733  [**] [1:2060507:2] ET REMOTE_ACCESS Anydesk Relay Domain (net .anydesk .com) in DNS Lookup [**] [Classification: Misc activity] [Priority: 3] {UDP} 10.216.
129.135:62633 -> 10.216.129.154:53
09/04/2025-13:08:02.404678  [**] [1:2060507:2] ET REMOTE_ACCESS Anydesk Relay Domain (net .anydesk .com) in DNS Lookup [**] [Classification: Misc activity] [Priority: 3] {UDP} 10.216.
129.135:62633 -> 10.216.129.154:53
09/04/2025-13:09:01.276903  [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 105.113.15.99:443 -
> 10.216.129.135:15062
09/04/2025-13:09:01.291973  [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.216.129.60:50082
 -> 92.223.97.97:80
09/04/2025-13:10:18.519662  [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 105.113.15.163:443
-> 10.216.129.135:15121
09/04/2025-13:12:30.210615  [**] [1:2031071:5] ET INFO Microsoft Connection Test [**] [Classification: Misc activity] [Priority: 3] {TCP} 10.216.129.135:15140 -> 2.19.252.163:80
09/04/2025-13:12:31.884186  [**] [1:2031071:5] ET INFO Microsoft Connection Test [**] [Classification: Misc activity] [Priority: 3] {TCP} 10.216.129.135:64992 -> 2.19.252.163:80
09/04/2025-13:12:34.132040  [**] [1:2060507:2] ET REMOTE_ACCESS Anydesk Relay Domain (net .anydesk .com) in DNS Lookup [**] [Classification: Misc activity] [Priority: 3] {UDP} 10.216.
129.135:52423 -> 10.216.129.154:53
09/04/2025-13:12:34.194085  [**] [1:2060507:2] ET REMOTE_ACCESS Anydesk Relay Domain (net .anydesk .com) in DNS Lookup [**] [Classification: Misc activity] [Priority: 3] {UDP} 10.216.
129.135:52423 -> 10.216.129.154:53
09/04/2025-13:13:01.626659  [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.216.129.135:6500
5 -> 105.113.15.163:443
09/04/2025-13:13:01.842676  [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.216.129.135:6501
1 -> 20.190.181.2:443
09/04/2025-13:13:02.255038  [**] [1:2210024:2] SURICATA STREAM ESTABLISHED SYNACK resend with different seq [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP}
52.182.141.63:443 -> 10.216.129.135:65021
09/04/2025-13:25:46.880863  [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 2.20.12.70:443 -> 1
0.216.129.135:65216
09/04/2025-13:28:55.131832  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {
UDP} 10.216.129.133:68 -> 10.216.129.154:67
09/04/2025-13:29:56.056702  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {
UDP} 10.216.129.133:68 -> 10.216.129.154:67
09/04/2025-13:30:56.281494  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {
UDP} 10.216.129.133:68 -> 10.216.129.154:67
09/04/2025-13:31:56.839188  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {
UDP} 10.216.129.133:68 -> 10.216.129.154:67
09/04/2025-13:32:57.756110  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {
UDP} 10.216.129.133:68 -> 10.216.129.154:67
09/04/2025-13:33:58.300740  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {
```

Then you will be analyzing your traffic from wireshark


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
discoveries.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Search
Right Ctrl
11:46
11:47 AM
4/2/2025

```
No.  Time          Source                Destination          Protocol Length Info
   1 0.000000000   192.168.15.127        192.168.15.29        ICMP       60 Echo (ping) reply    id=0xfe27, seq=14480/36920, ttl=64
   2 0.267797370   5e:6e:79:24:71:dc     Broadcast            ARP        60 Who has 192.168.15.133? Tell 192.168.15.127
   3 0.267817416   PCSSystemtec_44:12:…  5e:6e:79:24:71:dc    ARP        42 192.168.15.133 is at 08:00:27:44:12:00
   4 0.529046478   192.168.15.29         102.64.112.164       NTP        90 NTP Version 4, client
   5 0.530023270   192.168.15.29         192.168.15.127       ICMP       60 Echo (ping) request  id=0xfe27, seq=14481/37176, ttl=64 (reply in 6)
   6 0.560956210   192.168.15.127        192.168.15.29        ICMP       60 Echo (ping) reply    id=0xfe27, seq=14481/37176, ttl=64 (request in 5)
   7 0.645376601   fe80::a00:27ff:fe94…  ff02::1:ff94:c95b    ICMPv6     86 Neighbor Solicitation for fe80::2804:98ff:fe94:c95b from 08:00:27:94:78:e2
   8 0.734638624   192.168.15.135        192.168.6.144        TCP        66 5119 → 1514 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   9 0.771257329   102.64.112.164        192.168.15.29        NTP        90 NTP Version 4, server
  10 1.045037591   192.168.15.29         192.168.15.127       ICMP       60 Echo (ping) request  id=0xfe27, seq=14482/37432, ttl=64 (reply in 11)
  11 1.050134091   192.168.15.127        192.168.15.29        ICMP       60 Echo (ping) reply    id=0xfe27, seq=14482/37432, ttl=64 (request in 10)
  12 1.589163770   192.168.15.29         192.168.15.127       ICMP       60 Echo (ping) request  id=0xfe27, seq=14483/37688, ttl=64 (reply in 13)
  13 1.592856295   192.168.15.127        192.168.15.29        ICMP       60 Echo (ping) reply    id=0xfe27, seq=14483/37688, ttl=64 (request in 12)
  14 1.652939597   fe80::a00:27ff:fe94…  ff02::1:ff94:c95b    ICMPv6     86 Neighbor Solicitation for fe80::2804:98ff:fe94:c95b from 08:00:27:94:78:e2
  15 2.101183750   192.168.15.29         192.168.15.127       ICMP       60 Echo (ping) request  id=0xfe27, seq=14484/37944, ttl=64 (reply in 16)
  16 2.104832665   192.168.15.127        192.168.15.29        ICMP       60 Echo (ping) reply    id=0xfe27, seq=14484/37944, ttl=64 (request in 15)
  17 2.556084556   192.168.15.29         102.64.112.164       NTP        90 NTP Version 4, client
  18 2.556085327   192.168.15.29         102.64.113.152       NTP        90 NTP Version 4, client
```

```
› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
› Ethernet II, Src: 5e:6e:79:24:71:dc (5e:6e:79:24:71:dc), Dst: Intel_b6:0d:b4 (a8:7e:ea:b6:0d:b4)
› Internet Protocol Version 4, Src: 192.168.15.127, Dst: 192.168.15.29
› Internet Control Message Protocol
```

```
0000  a8 7e ea b6 0d b4 5e 6e  79 24 71 dc 08 00 45 00   ·~····^n y$q···E·
0010  00 1d a3 47 00 00 40 01  37 ac c0 a8 0f 7f c0 a8   ···G··@· 7·······
0020  0f 1d 00 00 c9 47 fe 27  38 90 00 00 00 00 00 00   ·····G·' 8·······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

discoveries.pcapng   Packets: 1039571 · Displayed: 1039571 (100.0%)   Profile: Default

Step 4. Configure pfsense as gateway

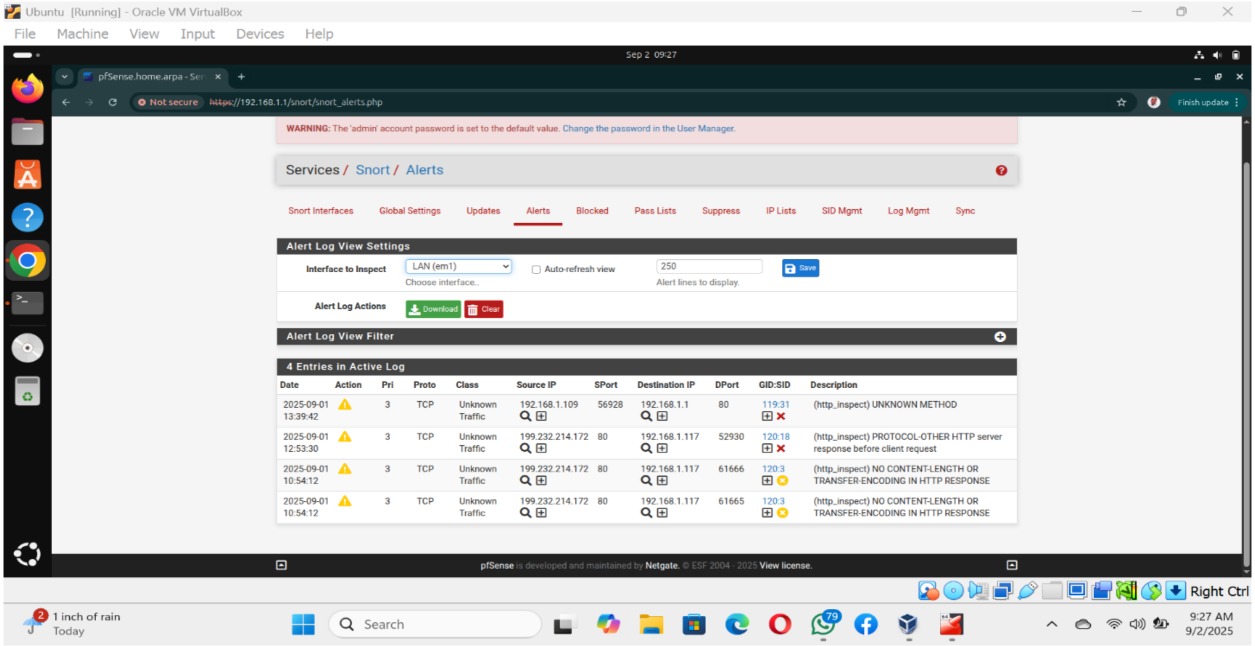
Pfsense firewall role = pass. Any. Lan subnet. Any . this firewall . Any. Msg [passing role]

Then ping it with your kali after which you will go and check the result at the firewall log file in pfsense.

When you go into the pfsense dashboard you navigate to the package manager and download snort so you can push and analyze your snort logs over there.

Then launch your attack from the attack system which is kali to snort which is in Ubuntu and after that you give your pfsense some time to capture the traffic packets.

Then check your snort alert on pfsense.



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Services / Snort / Alerts

Alert Log View Settings

Interface to Inspect: LAN (em1) — Choose interface..

□ Auto-refresh view

250 — Alert lines to display.

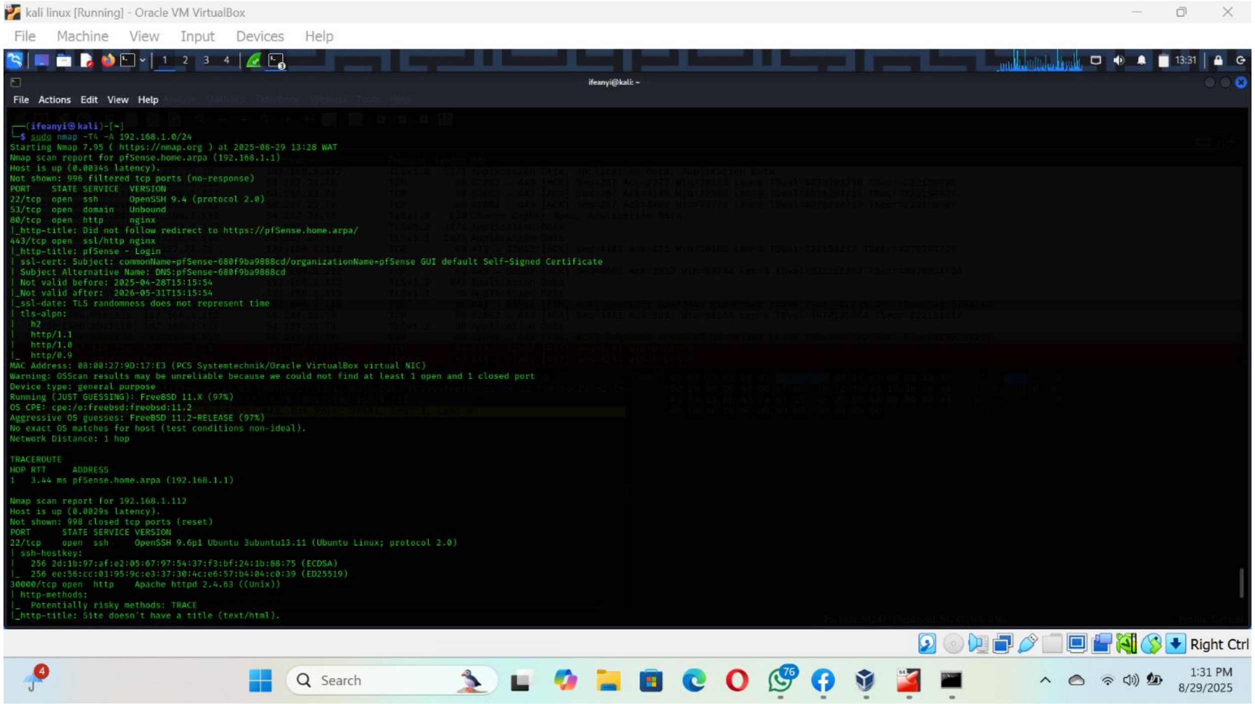
4 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-09-01 13:39:42	⚠	3	TCP	Unknown Traffic	192.168.1.109	56928	192.168.1.1	80	119:31	(http_inspect) UNKNOWN METHOD
2025-09-01 12:53:30	⚠	3	TCP	Unknown Traffic	199.232.214.172	80	192.168.1.117	52930	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
2025-09-01 10:54:12	⚠	3	TCP	Unknown Traffic	199.232.214.172	80	192.168.1.117	61666	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2025-09-01 10:54:12	⚠	3	TCP	Unknown Traffic	199.232.214.172	80	192.168.1.117	61665	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Sep 2 09:27
pfSense.home.arpa - Ser
Not secure https://192.168.1.1/snort/snort_alerts.php
Finish update
Right Ctrl
1 inch of rain
Today
Search
9:27 AM
9/2/2025

Then launch an active information gathering attack with your kali to see the os, ports, and services running in that entire network.



```
┌──(ifeanyi㉿kali)-[~]
└─$ sudo nmap -T4 -A 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 13:28 WAT
Nmap scan report for pfSense.home.arpa (192.168.1.1)
Host is up (0.0034s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 9.4 (protocol 2.0)
53/tcp  open  domain   Unbound
80/tcp  open  http     nginx
|_http-title: Did not follow redirect to https://pfSense.home.arpa/
443/tcp open  ssl/http nginx
|_http-title: pfSense - Login
| ssl-cert: Subject: commonName=pfSense-680f9ba9888cd/organizationName=pfSense GUI default Self-Signed Certificate
| Subject Alternative Name: DNS:pfSense-680f9ba9888cd
| Not valid before: 2025-04-28T15:15:54
|_Not valid after:  2026-05-31T15:15:54
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|   http/1.1
|   http/1.0
|_  http/0.9
MAC Address: 08:00:27:9D:17:E3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (97%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   3.44 ms pfSense.home.arpa (192.168.1.1)

Nmap scan report for 192.168.1.112
Host is up (0.0029s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 2d:1b:97:af:e2:05:67:97:54:37:f3:bf:24:1b:88:75 (ECDSA)
|_  256 ee:56:cc:01:95:9c:e3:37:30:4c:e6:57:b4:04:c0:39 (ED25519)
30000/tcp open  http    Apache httpd 2.4.63 ((Unix))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
```

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ifeanyi@kali: ~
File Actions Edit View Help
13:31
Right Ctrl
Search
1:31 PM
8/29/2025

Then I discovered the ports running which are port: 22,53,80,443, which are majorly SSH & Tcp which is not secure.

Then I discovered the ip in the network through the help of Nmap which are:

Pfsense – 192.168.1.1

Windows-192.168.1.117

Ubuntu-192.168.1.112

SECURITY RECOMMENDATION

1. Keep the operating system and installed open-source software up to date by regularly applying security patches and updates. Open-source systems often release frequent security fixes for vulnerabilities. 2. Disable unused ports and services that are not required, for example, disable the SSH service if not needed or restrict access using firewalls. 3. Secure essential services like SSH by configuring SSH key-based authentication and disabling password-based authentication.
2. 4. Implement network segmentation to isolate sensitive systems or critical services from less secure parts of the network. 5. Review configuration files regularly, especially for critical services (such as Apache, SSH), and ensure they follow secure configuration guidelines. 6. Encrypt data in transit using protocols like TLS/SSL for web traffic (if hosting websites or services) and ensure SSH connections are secured using strong cryptographic algorithms. 7. Encrypt sensitive data both at rest and in transit.
3. By following these recommendations, you can strengthen the security posture of the firewall at 192.168.1.1, helping to protect your network from a variety of cyber threats.

   Following this recommendation above your will be able to have a better and more secure network…