Femlalogy SOC Report

**Project Title:** Threat Detection & Incident Response Using Wireshark, pfSense, and Wazuh  
**Organization:** Femlalogy  
**Analyst:** Agboola David Oluwanifise, Stephen Ankomah, NGONO Pascal Brice, Simon Ayim, Adebambo osinuga, Adekoya Quazim Ayotunde, Prince Emmanuel Okezie.  
**Role:** Security Operations Center (SOC) Analyst  
**Submission Date:** 10/15/2025

# Table of Contents

[**Table of Contents**](#_mum6h3pihy1a) **1**

[**1. Executive Summary**](#_7l582k4tirqd) **1**

[**2. Project Introduction**](#_99ixufoiu166) **2**

[**3. Methodology**](#_fqd5gf1rmkn3) **2**

[**4. Phase-by-Phase Analysis**](#_d9bkp8akanq) **2**

[Phase 1: Wireshark – Network Traffic Capture & Analysis](#_3tj58fqbiojd) 2

[Phase 2: pfSense and Snort– Firewall & Policy Enforcement](#_d8t95lsnt7r4) 3

[Phase 3: Wazuh – Security Event Monitoring & Response](#_y7ix4kl3sn1s) 3

[5. Final Findings & Impact](#_9qz1vleyxp2o) 3

[6. Recommendations](#_1blzqop1pxu5) 3

[7. Conclusion](#_qbahgp980amr) 4

[**8. References (remember this should also include links and short details)**](#_ib60eeeuum0k) **4**

[**9. Appendices**](#_rix6jl5wfus2) **4**

[Appendix A – Wireshark Phase Report](#_rmibk9c3shj2) 4

[Appendix B – pfSense Phase Report](#_xnxv0i15p5p0) 4

[Appendix C – Wazuh Phase Report](#_gk1wrrto85h4) 5

# 1. Executive Summary

The purpose of this project was on how the cybersecurity posture of Femlalogy could be strengthened through the deployment and integration of three key tools, namely, Wazuh, Wireshark and pfSense.Our task was to simulate real world attacks, detect network anomalies,, enforce firewall rules and respond to security incident effectively and timely.

Using Wireshark, suspicious traffic such as Nmap and ping sweeps were captured and analysed by the team. Also, we pfSense integrated with Snort, the team configured and enforced network and firewall policies, thereby blocking ransomware-related IPs, as well as malicious ICMP traffic.

Lastly, Wazuh provided us with a focused security event correlation and monitoring, thereby resulting in actionable alerts and incidents reports. This project depicts the importance of protecting organizational assets against the world of changing cyber threats, proactive monitoring and how relevant the various levels of defense is to an organization.

# 2. Project Introduction

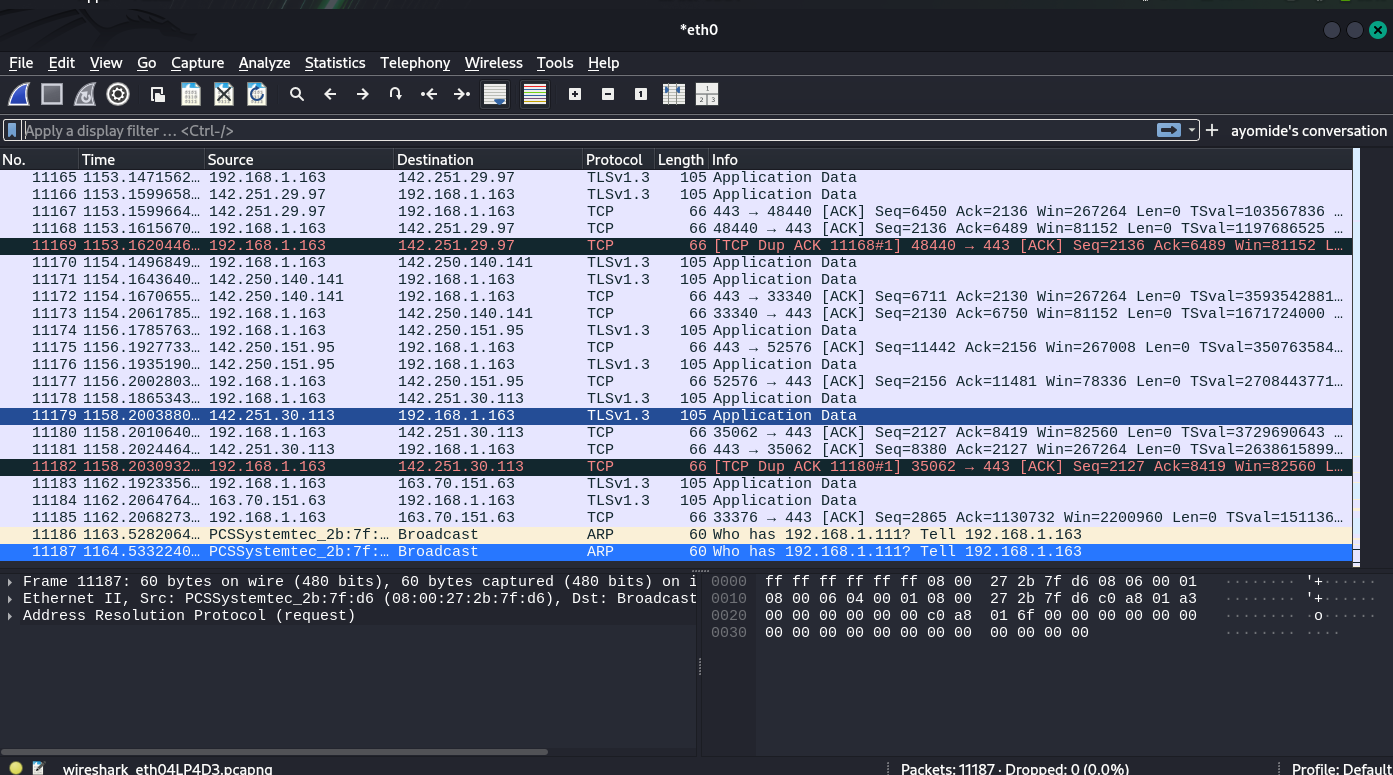
Cybersecurity in today's world remains one of the critical aspects of any organization’s success in this digital age. Therefore, this project aimed to build and access a SOC for Femalogy designed to detect, monitor and respond to cyber threats directed at the organization in real time. By deploying tools such as Wazuh, pfSense and Wireshark, this simulation was done to test the readiness of the organization should a cyber threat occur. Wireshark was used for packet capturing and analysis, while Wazuh was used as the platform that coordinated correlation and reporting. pfSense on the other hand was our barrier between our internal and external network, thereby filtering incoming and outgoing network traffic based on configured rules. These tools provided a demonstration of how all these tools can work together to protect Femlogy’s network from inside and outside threats.

# 3. Methodology

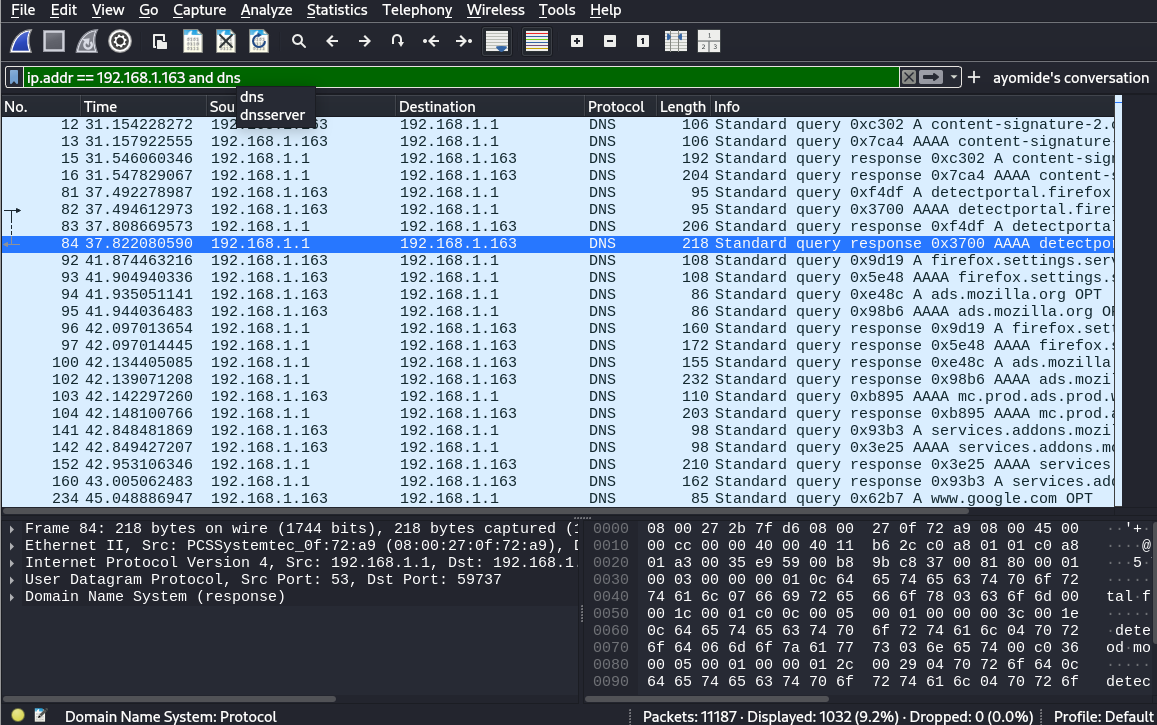
Wireshark was used to capture all of the suspicious traffic i.e. nmap scan and ping sweeps. pfSense and Snort were configured to block ICMP packets, and as intrusion detection. Wazuh was used to track logs and create alerts, and generate an executive report. Kali linux was the attacker machine and ubuntu was the victim agent and the wazuh agent.

# 4. Phase-by-Phase Analysis

## Phase 1: Wireshark – Network Traffic Capture & Analysis



The screenshot above displays the normal traffic on wireshark on kali with no filters to show there was an internet connection.



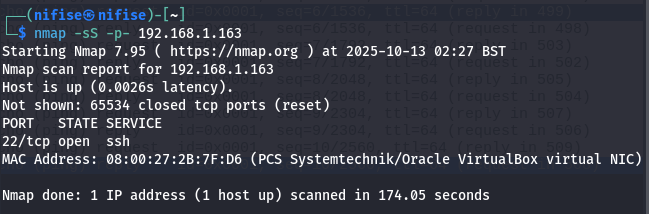


The image above shows the filters used to display the traffic for when the victim IP 192.168.1.163 visited [google.com](http://google.com/) on mozilla firefox browser.

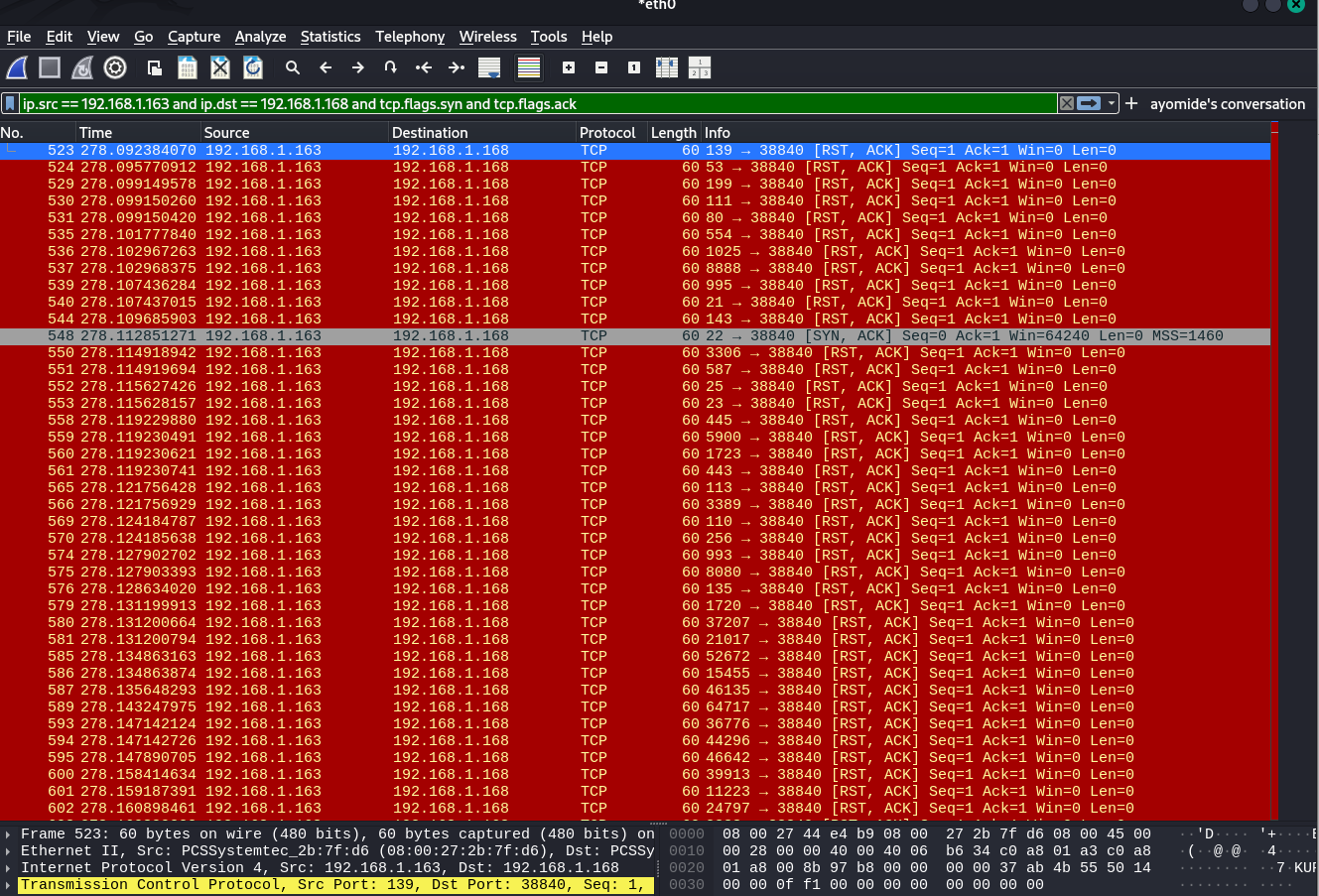
Ping flood was ran to simulate a Denial Of Service (DOS) attack on the victim machine, Using the “icmp” keyword filter in wireshark, it displayed only the ping which was launched from the attacker onto the victim IP.



Nnmap was ran to scan from my kali using the -sS- to perform a stealth scan where Nmap sends SYN packets to start connections but never completes the TCP handshake and the -p- to scan all the ports.

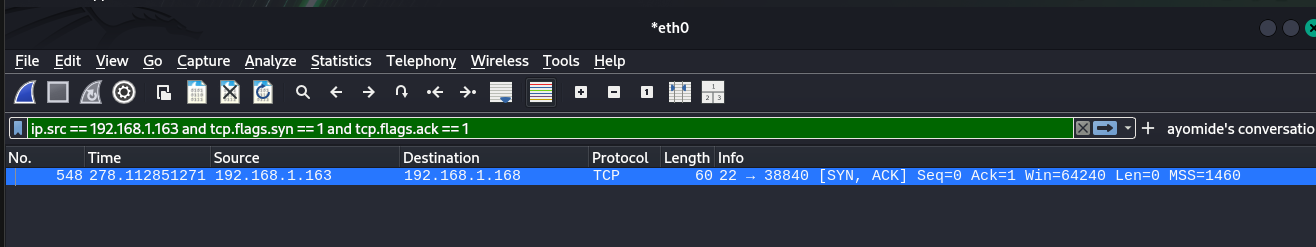


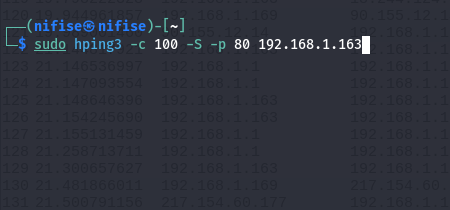
This is the result of the nmap on wireshark:



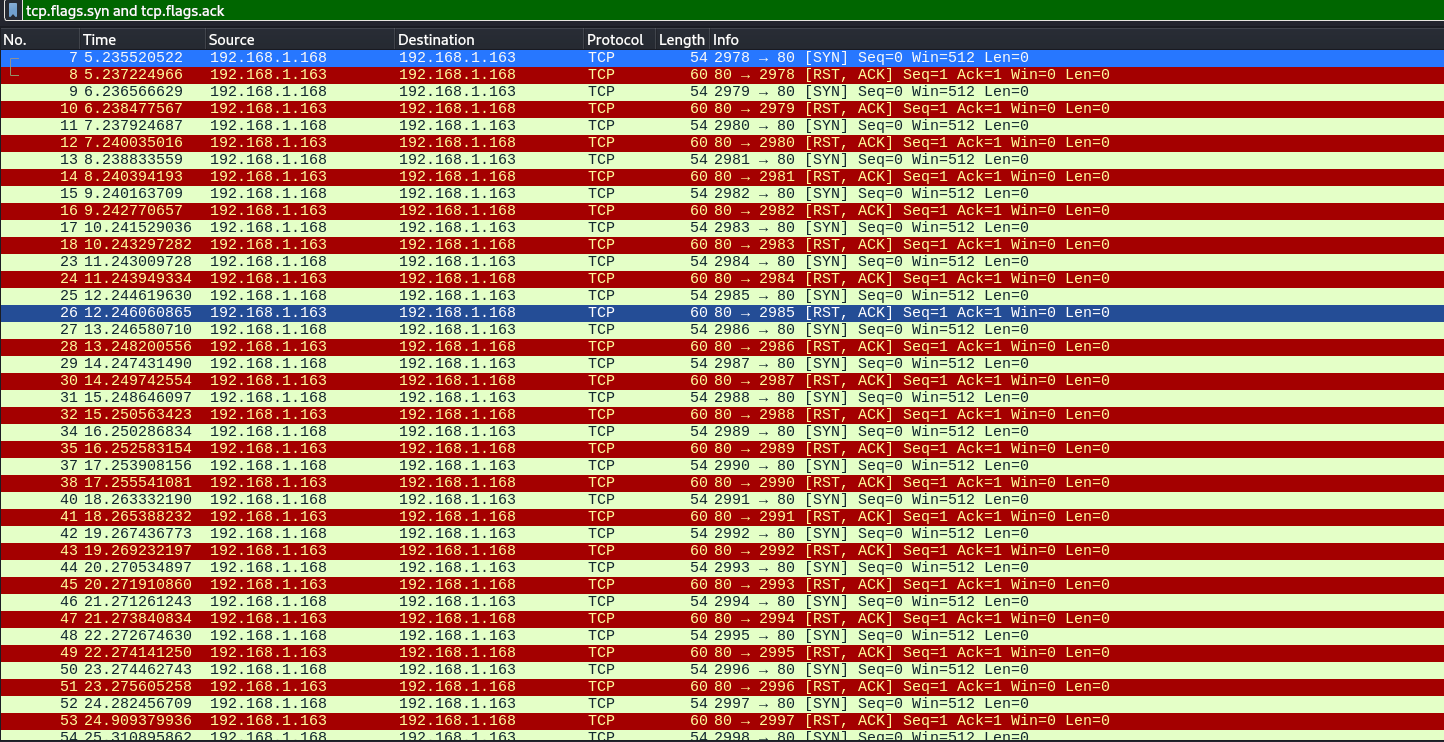
The filter “ip.src == 192.168.1.163 and ip.dst == 192.168.1.168 and tcp.flags.syn and tcp.flags.ack” displays the TCP handshake between the victim machine (ip.src) and the attacker machine (ip.dst). The red portrays the ports which are closed on the victim machine.

And these where there results from the nmap of the only open port, where i filtered the nmap scan using “ip.src == <victim\_ip> and tcp.flags.syn == 1 and tcp.flags.ack == 1”. The “tcps.flags.syn==1” means to give the packet where there was a connection to the three way handshake.



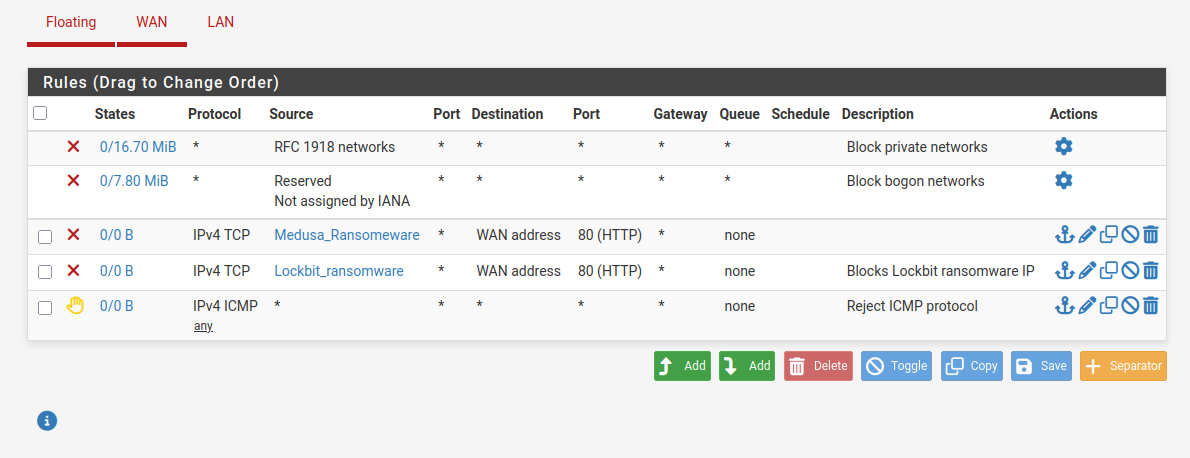


A hping3 ping was ran on the http port 80 to detect anomalous HTTP requests.Proceeded to filtered the attack using “tcp.flags.syn and tcp.flags.ack”.

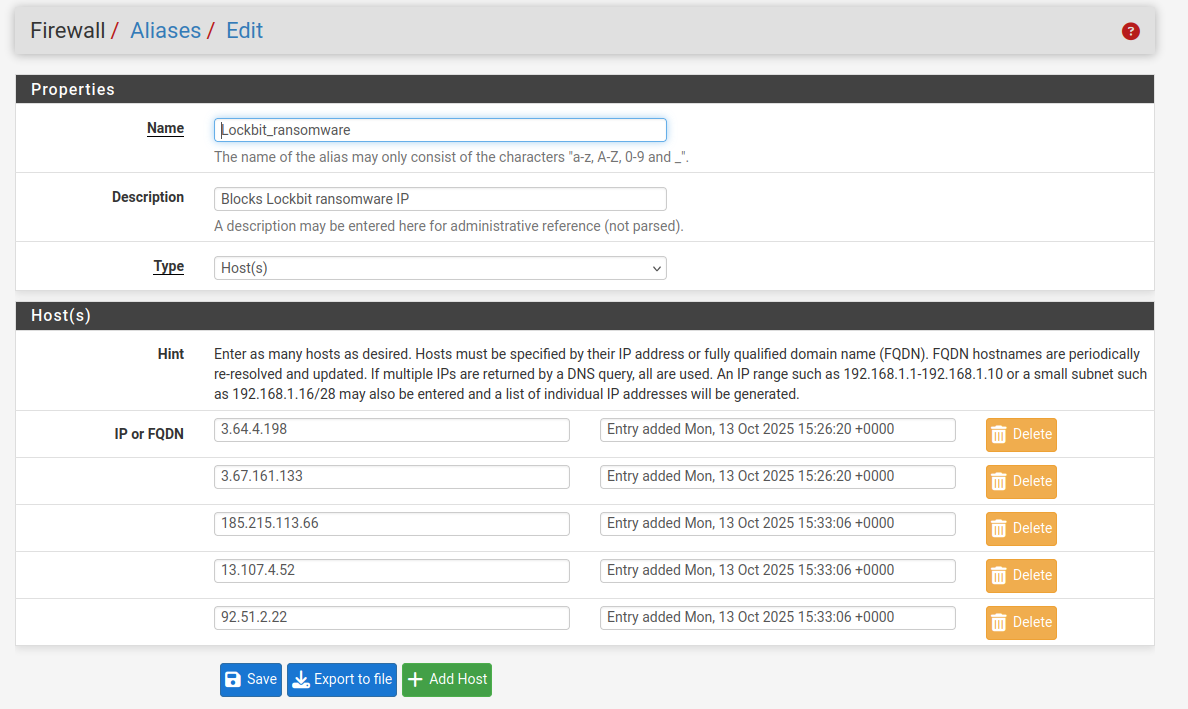


The attacker, 192.168.1.168 repeatedly attempted TCP three-way handshakes to 192.168.1.163 at port 80. The victim responded with a refused connection (RST) for each attempt, indicating no service was listening on port 80. This is consistent with the Nmap scan results showing port 80 as closed.

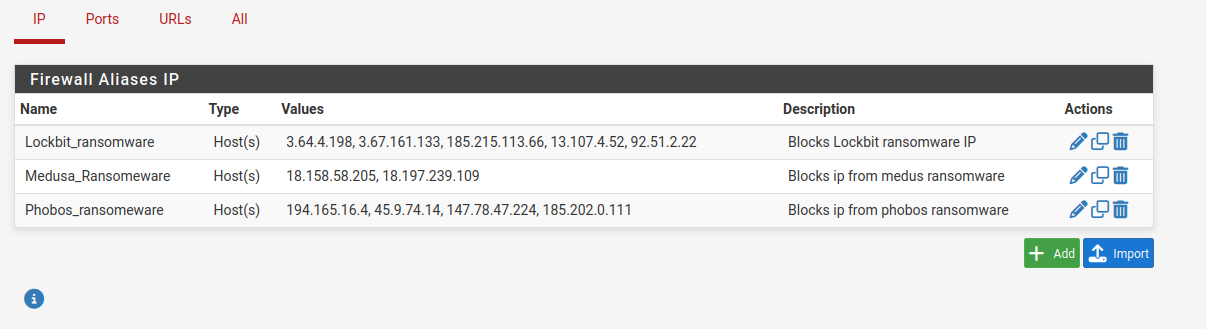
## Phase 2: pfSense and Snort– Firewall & Policy Enforcement



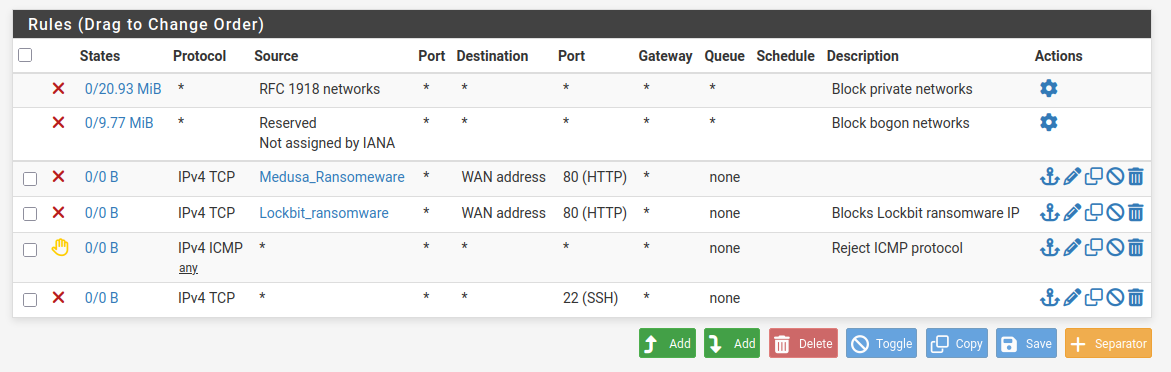
The above screenshot displays the firewall rules which block popular ransomware groups which are Medusa and Lockbit on port 80. It also displays the rule that blocks ICMP packets from happening in the network.



These are the lists IP addresses from Lockbit ransomware group blocked by the firewall.

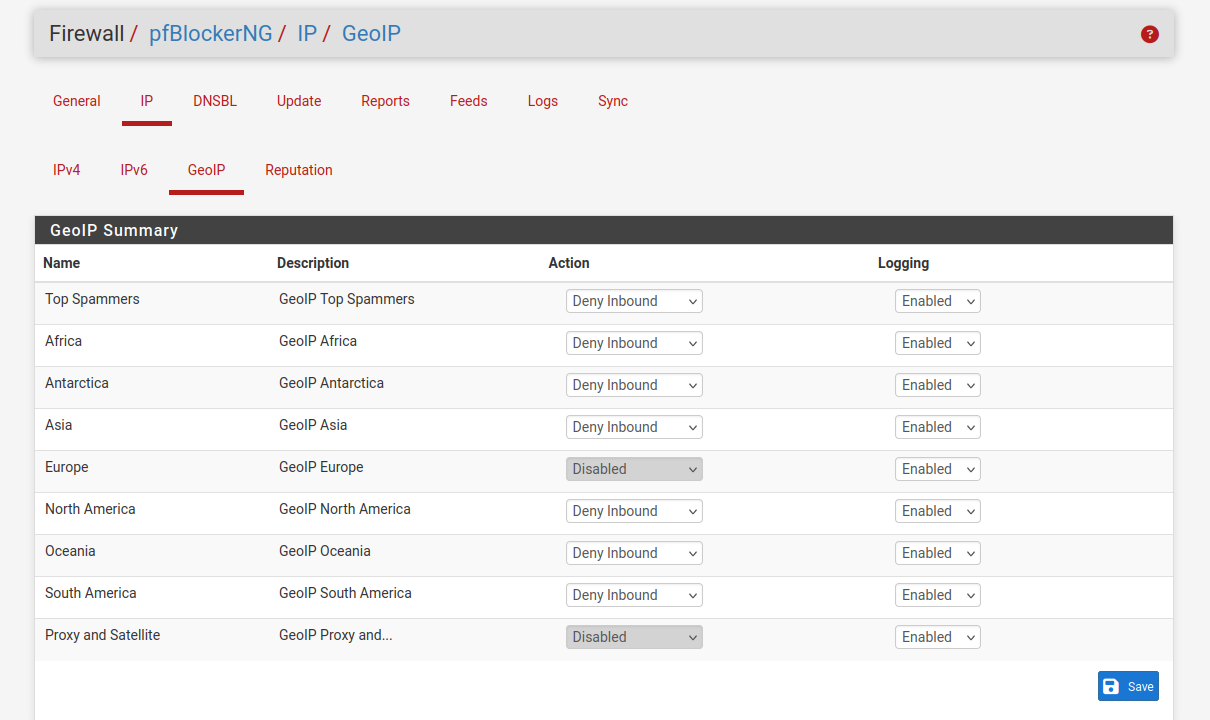


The above screenshot shows the list of IP addresses blocked by the firewall and grouped by the threats.

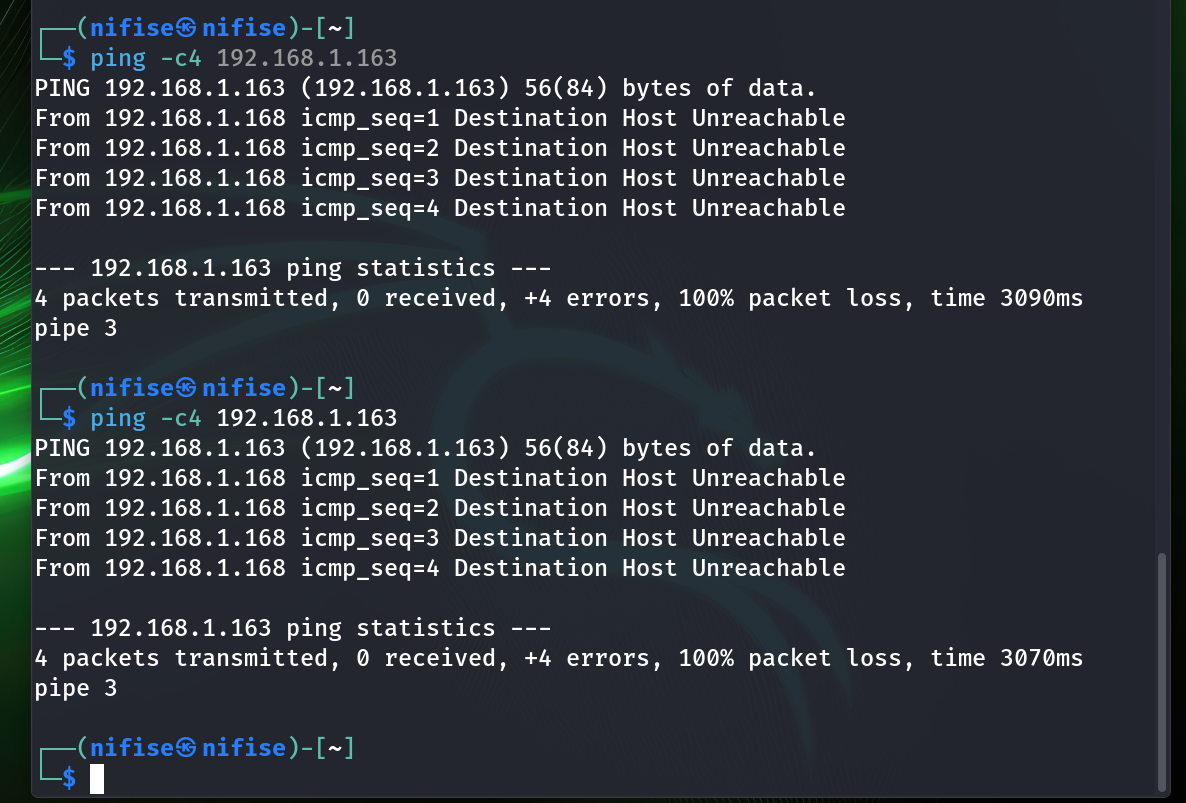


The screenshot above shows the updated firewall rules where SSH is blocked on the WAN.

Below is the firewall rule GeoIP blocking that restricts access from high-risk countries. Blocking most continent’s inbound traffic heavily reduces the attack surface and ensures all legitimate activity comes from inside your lab.

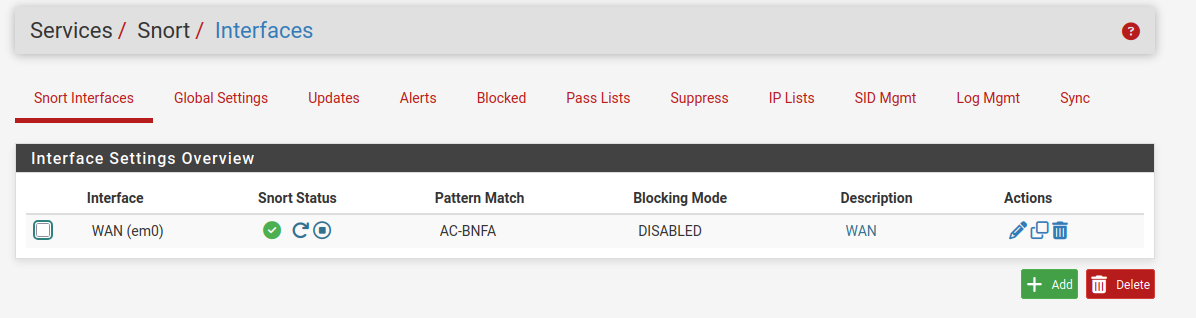


### Testing

Here is the test for the blocked ICMP firewall rule in the network. The ip pinged was the host network and thanks to the rule the pings were dropped, proving the effectiveness of the rule. In this case, the attacker was behind the firewall with the victim.When trying to do similar with an attacker outside of the wirewall, traffic failed to be routed by pfSense.

## Snort Intrusion Detection System

Below’s screenshot shows the IDS rule which detects offenders and raises alerts in pfsense when there is an nmap or a ping flood on the victim.



## Phase 3: Wazuh – Security Event Monitoring & Response

* **Objective:** Correlate logs and respond to security incidents
* **Key Actions:**
  + Configured log forwarding from pfSense and endpoints
  + Detected privilege escalation and suspicious user behavior
* **Tools:** Wazuh SIEM
* **Findings:** Multiple alerts correlated with anomalies identified in Wireshark
* **Artifacts:** *[Attach appropriately placed screenshots here, and also with mini-report in Appendix C]*

## 5. Final Findings & Impact

The engagement confirmed that Femalogy was susceptible to multiple attempts by an attacker to gain access to a victim’s information and identify possible vulnerabilities like open ports. By implementing GeoIP blocking and inbound firewall rules, most malicious scans were successfully filtered by pfSense, the firewall, before reaching the internal LAN. Snort’s Intrusion Detection System alerted the network of the malicious traffic and wazuh was supposed to log the events. This report is incomplete due to some connectivity issues between the attacker and the victim machine. Kali, being outside of the machine, had a different default gateway than that of Ubuntu which was the firewall. And pfSense had issues trying to route traffic from the attacker to the victim, despite being on the same subnet mask. In the process of trying to solve these issues, they took more time than expected, therefore, making the report incomplete.

## 6. Recommendations

Based on findings, the following are recommended for the organization to regularly check the firewall for alerts and constantly update rules. To minimize exposure of network from high risk countries, geoIP blocking should be enabled to protect the network. Restricting SSH to only VPN- tunnel connections should also be done.

## 7. Conclusion

This confirmed that Femalogy’s network was exposed to external reconnaissance attempts. Through the use of GeoIP blocking, strict inbound firewall rules, IDSs with Snort and Wazuh’s logging, the attack surface was reduced, and malicious activity was detected and logged. The improved security measures effectively strengthened the organization’s ability to identify itself and respond to threats. Also, by restricting remote access, enhancing firewall rules, and maintaining constant logging, Femalogy now has an effectively secured network and capable SOC group to protect the network from outsiders..

# 8. References

* Wireshark Documentation
* pfSense and IDS/IPS Configuration - <https://docs.netgate.com/pfsense/en/latest/packages/snort/index.html>
* Wazuh Official Guide - <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html>
* MITRE ATT&CK Framework
* Logs and dashboards from the lab environment
* Raw logs, alert data, and full packet captures

# 9. Appendices

The screenshots were added above with explanations.