Final Incident Report & Recommendations

Cover Page

Project Title: Threat Detection & Incident Response Using Wireshark, pfSense, and Wazuh
Organization: SoCra Tech
Analyst: Tega Olomu
Role: Security Operations Center (SOC) Analyst
Submission Date: April 24, 2025

Table of Contents

---

1. Executive Summary

In order to evaluate and improve the cyber security measures in SoCra Tech, a growing technology solutions provider, I performed a detailed SOC analysis which involved 3 phases. Using Wireshark for traffic monitoring, pfSense for firewall management, and Wazuh for threat detection, I monitored the network for suspicious activity. Critical and high-risk Indicators of Compromise (IoCs) were discovered and acted upon as soon as they were found. I provided the organization with relevant recommendations to improve the organization's overall cybersecurity posture.

---

2. Project Introduction

SoCraTech has been experiencing abnormal network activities, possible breaches, malware infection, and

internal cybersecurity threats. I was brought in as a SOC analyst in order to implement a proactive defense strategy. Part of my responsibilities included deploying monitoring systems, analyzing security events in real-time through traffic capturing, identifying vulnerabilities and responding to events. In this report, I detail the methods employed, the findings and impact, resolutions and recommendations.

---

3. Methodology

The engagement followed a structured multi-phase approach:

- **Wireshark** was used for packet capture and protocol analysis.
- **pfSense** was configured to implement firewall and IDS/IPS rules.
- **Wazuh** served as a centralized SIEM for alerting, log correlation, and response.

---

4. Phase-by-Phase Analysis

Phase 1: Wireshark – Network Traffic Capture & Analysis

- **Objective:** Capture and analyze SoCraTech's network traffic for suspicious activities.
- **Key Actions:**
    - Focused on HTTP, DNS, SSH traffic
    - Identified suspicious DNS queries and unusual HTTP patterns
- **Tools:** Wireshark and Kali
- **Findings:** Potential malware beaconing; unauthorized data exfiltration attempts; brute force attack
- **Artifacts:** *Screenshots and mini-report attached in Appendix A.*

Phase 2: pfSense – Firewall & Policy Enforcement

- **Objective:** Detect and block malicious traffic using firewall rules and IPS
- **Key Actions:**
    - Configured Snort IDS, GeoIP filtering
    - Set up firewall rules to block malicious IP addresses
    - Monitored and blocked brute force attempts
- **Tools:** pfSense; Snort (IPS/IDS)
- **Findings:** Blocked multiple unauthorized SSH attempts and malicious IPs
- **Artifacts:** *Screenshots and mini-report attached in Appendix B*

Phase 3: Wazuh – Security Event Monitoring & Response

- **Objective:** Correlate logs and respond to security incidents
- **Key Actions:**

- Configured log forwarding from endpoints
- Detected privilege escalation attack and suspicious user behavior

- **Tools:** Wazuh SIEM
- **Findings:** Multiple alerts correlated with anomalies identified in Wireshark
- **Artifacts:** *Screenshots and mini-report attached in Appendix C*

---

5. Final Findings & Impact

Incident Response Plan (IRP)

- **Preparation:** The security & monitoring tools were deployed for network monitoring and intrusion detection, tasks of the SOC team were defined and ensured that logs were centralized and retained for analysis.
- **Identification:** Indicators of Compromise were noticed as unusual traffic patterns, unauthorized login attempts from external IPs, alerts triggered by Wazuh indicating malware activity.
- **Containment:** In order to limit the spread and impact of the incident, affected systems were isolated from the network, suspicious IP addresses and domains were blocked by setting pfSense firewall rules.
- **Eradication:** Malware infected files were removed and suspicious processes terminated.
- **Recovery:** Reconnected cleaned systems to the network in a controlled environment, closely monitored systems post-recovery and verified all systems were functioning properly.
- **Lessons Learned:** Learned from the malicious attacks and weakness identified, recommended the implementation of core security measures to prevent the events identified from recurring in the future.

Security Risks

The engagement confirmed that SoCraTech was susceptible to the following risks:

- Data theft, ransomware deployment, and loss of system control.
- Intellectual property loss, regulatory violations (e.g., GDPR, HIPAA), and reputational damage.
- Compromised credentials, especially for critical infrastructure or privileged accounts.
- Total system compromise, unauthorized access to sensitive files, lateral movement across the network.
- Malware or threat actors could operate undetected for extended periods
- Possible exposure to state-sponsored or organized cybercrime activity.

---

6. Recommendations

Based on findings, the following are recommended:

- The implementation of Multi-Factor Authentication (MFA) for all employees for remote access, as well as internally for privileged accounts and sensitive systems. This adds an extra layer of protection, even if passwords are compromised.

• Invest in tools that monitor employee accounts and company devices for unusual behavior. This helps detect threats early like unauthorized access or data theft.

• Put systems in place that track and prevent unauthorized sharing or sending of data outside the company. This reduces the risk of accidental or malicious data leaks.

• Separate critical systems (like HR, Finance, and servers) from general employee access. If a breach happens, this limits how far it can spread.

• Regularly update systems to block known malicious websites, IP addresses, attack patterns and close known security holes. This prevents attackers from even reaching the network. Many attacks take advantage of vulnerabilities like outdated software.

• Provide ongoing cybersecurity awareness training. Employees are the first line of defense and need to stay informed.

• Ensure scheduled regular audits, updated incident response documentation and refined incident detection plan.

---

7. Conclusion

SoCraTech's SOC analysis showed vulnerabilities like malware attack, unauthorized access, and possible data breaches. While threats were mitigated through traffic monitoring, firewall configurations, and log reviews, recommendations were given to enhance the organization's security strategy. Adopting the recommendations provided will enhance the company's security posture and prevent incidents from occurring in the future.

---

8. References

• Wireshark Documentation: https://www.wireshark.org/docs/

• pfSense IDS/IPS Configuration: https://docs.netgate.com/pfsense/en/latest/

• Wazuh Official Guide: https://documentation.wazuh.com/

• MITRE ATT&CK Framework: https://attack.mitre.org/

• Logs and dashboards from the lab environment: Pls see screenshots in Appendices

• Raw logs, alert data, and full packet captures: Pls see screenshots in Appendices

- IOC lists: Brute Force attack, SSH login attempts, malware, C2 server communications.
- Threat intelligence references: https://rules.emergingthreats.net/

---

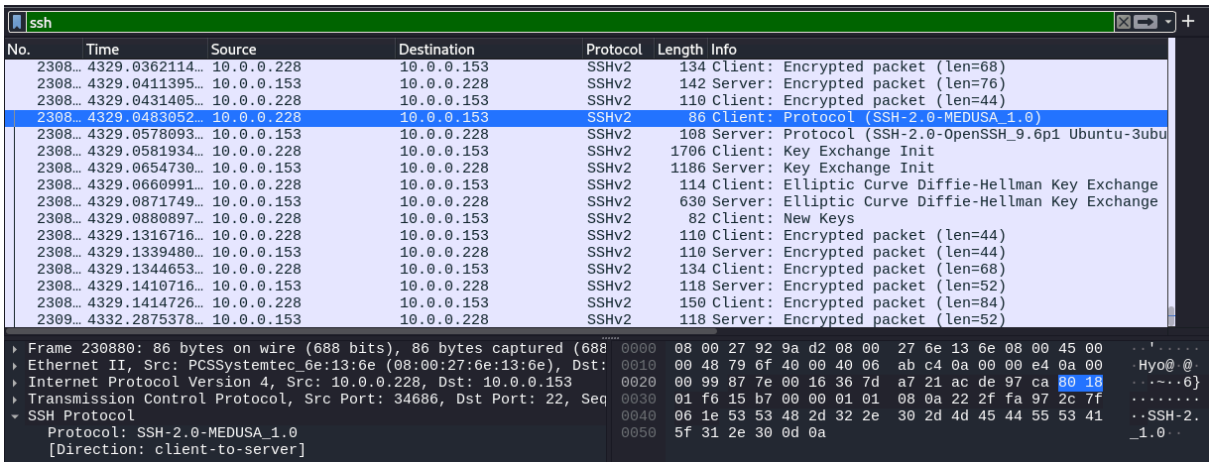
9. Appendices

Appendix A – Wireshark Phase Report

Activity:

Using wireshark to analyze traffic, the below were the findings.

1. Brute force attack - Performing a Wireshark analysis, there was a lot of traffic between the company system's IP address and an external IP address (10.0.0.228) using Medusa (an SSH brute-force attacking tool), signaling a brute force attack.



2. There was an employee who clicked on a link and downloaded a suspicious file. As a result, malware gained access to the company's system. From the screenshot below, there was an attempt to navigate to the Google Authenticator page. However, they were redirected to a fake Google Authenticator page - *authenticatoor.org* where the malicious software file was downloaded.

No.	Time	Source	Destination	Protocol	Length	Info
2327	38.224908	10.1.17.215	23.205.110.143	TCP	60	50131 → 443 [ACK] Seq=115498 Ack=184671 Win=129792 Len=0
2328	38.244292	23.205.110.143	10.1.17.215	TCP	60	443 → 50131 [ACK] Seq=184671 Ack=115498 Win=177920 Len=0
2329	38.250143	10.1.17.2	10.1.17.215	DNS	215	Standard query response 0xcc42 A google-authenticator.burleson-appliance.net A 104.21.64.1 A 104.21.48.1 A 104.21.32.1 A 104.21…
2330	38.269839	10.1.17.2	10.1.17.215	DNS	351	Standard query response 0xe4c2 HTTPS google-authenticator.burleson-appliance.net HTTPS
2331	38.270196	10.1.17.215	104.21.64.1	TCP	66	50133 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2332	38.299460	23.205.110.143	10.1.17.215	TLSv1.3	1060	Application Data
2333	38.299471	23.205.110.143	10.1.17.215	TCP	1430	443 → 50131 [ACK] Seq=185677 Ack=115498 Win=177920 Len=1376 [TCP PDU reassembled in 2337]
2334	38.299519	23.205.110.143	10.1.17.215	TCP	1430	443 → 50131 [PSH, ACK] Seq=187053 Ack=115498 Win=177920 Len=1376 [TCP PDU reassembled in 2337]
2335	38.299520	10.1.17.215	23.205.110.143	TCP	60	50131 → 443 [ACK] Seq=115498 Ack=187053 Win=130816 Len=0
2336	38.299815	23.205.110.143	10.1.17.215	TCP	1430	443 → 50131 [ACK] Seq=188429 Ack=115498 Win=177920 Len=1376 [TCP PDU reassembled in 2337]
2337	38.299816	23.205.110.143	10.1.17.215	TLSv1.3	243	Application Data
2338	38.299816	10.1.17.215	23.205.110.143	TCP	60	50131 → 443 [ACK] Seq=115498 Ack=189994 Win=130816 Len=0
2339	38.309955	104.21.64.1	10.1.17.215	TCP	66	443 → 50133 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM WS=8192
2340	38.310137	10.1.17.215	104.21.64.1	TCP	60	50133 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
2341	38.310759	10.1.17.215	104.21.64.1	TCP	1434	50133 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1380 [TCP PDU reassembled in 2342]
2342	38.310760	10.1.17.215	104.21.64.1	TLSv1.3	491	Client Hello (SNI=google-authenticator.burleson-appliance.net)
2343	38.350037	104.21.64.1	10.1.17.215	TCP	60	443 → 50133 [ACK] Seq=1 Ack=1381 Win=73728 Len=0
2344	38.351597	104.21.64.1	10.1.17.215	TCP	60	443 → 50133 [ACK] Seq=1 Ack=1818 Win=73728 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
2364	38.863141	10.1.17.215	10.1.17.2	DNS	78	Standard query 0xbcc7 A authenticatoor.org
2365	38.863149	10.1.17.215	10.1.17.2	DNS	78	Standard query 0xe6f7 HTTPS authenticatoor.org
2375	39.097981	10.1.17.2	10.1.17.215	DNS	147	Standard query response 0xe6f7 HTTPS authenticatoor.org SOA siti.ns.orangewebsite.com
2376	39.387854	10.1.17.2	10.1.17.215	DNS	94	Standard query response 0xbcc7 A authenticatoor.org A 82.221.136.26

http.request.method != "POST"

No.	Time	Source	Destination	Protocol	Length	Info
211	13.020372	10.1.17.215	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
349	16.033316	10.1.17.215	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
641	19.043836	10.1.17.215	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
5031	60.297799	10.1.17.215	5.252.153.241	HTTP	371	GET /api/file/get-file/264872 HTTP/1.1
5063	62.145732	10.1.17.215	5.252.153.241	HTTP	144	GET /api/file/get-file/29842.ps1 HTTP/1.1
5073	62.366091	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7279	67.602135	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7602	72.778372	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7688	77.950821	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7696	83.150518	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7762	86.704060	10.1.17.215	199.232.214.172	HTTP	411	HEAD /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1737884967&P2=404&P3=2&P4=DQ%2frdpZetb6%2bCA7SUqmOgjEU…
7765	86.771540	10.1.17.215	199.232.214.172	HTTP	462	GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1737884967&P2=404&P3=2&P4=DQ%2frdpZetb6%2bCA7SUqmOgjEUa…
7841	88.342574	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7851	90.825252	10.1.17.215	199.232.214.172	HTTP	403	HEAD /filestreamingservice/files/2a0d597c-a09c-4400-be86-87596dd2e696?P1=1737884967&P2=404&P3=2&P4=W7WOpOZ6ahXXhvqsFdcWAJHdZVPv…
7854	90.887901	10.1.17.215	199.232.214.172	HTTP	454	GET /filestreamingservice/files/2a0d597c-a09c-4400-be86-87596dd2e696?P1=1737884967&P2=404&P3=2&P4=W7WOpOZ6ahXXhvqsFdcWAJHdZVPv8…

3. IP addresses - *45.125.66.32* and *45.125.66.252* have been identified as known malware command-and-control (C2) servers for this attack.

No.	Time	Source	Destination	Protocol	Length	Info
19302	889.561525	10.1.17.215	45.125.66.32	TCP	66	49792 → 2917 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
19303	889.754217	45.125.66.32	10.1.17.215	TCP	66	2917 → 49792 [SYN, ACK] Seq=0 Ack=1 Win=65280 Len=0 MSS=1340 SACK_PERM WS=128
19304	889.755043	10.1.17.215	45.125.66.32	TCP	60	49792 → 2917 [ACK] Seq=1 Ack=1 Win=65280 Len=0
19305	889.755043	10.1.17.215	45.125.66.32	TLSv1.2	173	Client Hello (SNI=45.125.66.32)
19306	889.939392	45.125.66.32	10.1.17.215	TCP	60	2917 → 49792 [ACK] Seq=1 Ack=120 Win=65280 Len=0
19307	889.939650	45.125.66.32	10.1.17.215	TLSv1.2	1092	Server Hello, Certificate, Server Hello Done
19310	889.941490	10.1.17.215	45.125.66.32	TLSv1.2	372	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
19311	890.134125	45.125.66.32	10.1.17.215	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
19312	890.147686	10.1.17.215	45.125.66.32	TLSv1.2	730	Application Data
19313	890.364851	45.125.66.32	10.1.17.215	TLSv1.2	1262	Application Data
19314	890.365594	45.125.66.32	10.1.17.215	TCP	1414	2917 → 49792 [ACK] Seq=2298 Ack=1114 Win=64384 Len=1360 [TCP PDU reassembled in 19315]
19315	890.365595	45.125.66.32	10.1.17.215	TLSv1.2	1081	Application Data
19316	890.365781	45.125.66.32	10.1.17.215	TLSv1.2	642	Application Data
19317	890.365781	45.125.66.32	10.1.17.215	TCP	1414	2917 → 49792 [ACK] Seq=5273 Ack=1114 Win=64384 Len=1360 [TCP PDU reassembled in 19321]
19318	890.366061	45.125.66.32	10.1.17.215	TCP	1414	2917 → 49792 [PSH, ACK] Seq=6633 Ack=1114 Win=64384 Len=1360 [TCP PDU reassembled in 19321]
19319	890.366062	10.1.17.215	45.125.66.32	TCP	60	49792 → 2917 [ACK] Seq=1114 Ack=5273 Win=65280 Len=0
19320	890.366063	45.125.66.32	10.1.17.215	TCP	1414	2917 → 49792 [ACK] Seq=7993 Ack=1114 Win=64384 Len=1360 [TCP PDU reassembled in 19321]
19321	890.366250	45.125.66.32	10.1.17.215	TLSv1.2	719	Application Data

ip.addr == 45.125.66.252

No.	Time	Source	Destination	Protocol	Length	Info
23420	917.407874	10.1.17.215	45.125.66.252	TCP	66	49822 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
23421	917.594835	45.125.66.252	10.1.17.215	TCP	66	443 → 49822 [SYN, ACK] Seq=0 Ack=1 Win=65280 Len=0 MSS=1340 SACK_PERM WS=128
23422	917.595824	10.1.17.215	45.125.66.252	TCP	60	49822 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
23423	917.595825	10.1.17.215	45.125.66.252	TLSv1.2	256	Client Hello
23430	917.784326	45.125.66.252	10.1.17.215	TCP	60	443 → 49822 [ACK] Seq=1 Ack=203 Win=65152 Len=0
23466	917.804372	45.125.66.252	10.1.17.215	TLSv1.2	1414	Server Hello, Certificate
23467	917.804374	45.125.66.252	10.1.17.215	TLSv1.2	144	Server Key Exchange, Server Hello Done
23468	917.804660	10.1.17.215	45.125.66.252	TCP	60	49822 → 443 [ACK] Seq=203 Ack=1451 Win=65280 Len=0
23492	917.817167	10.1.17.215	45.125.66.252	TLSv1.2	240	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
23536	918.008575	45.125.66.252	10.1.17.215	TLSv1.2	241	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
23537	918.012381	10.1.17.215	45.125.66.252	TLSv1.2	244	Application Data
23540	918.198952	45.125.66.252	10.1.17.215	TLSv1.2	82	Application Data
23541	918.199106	45.125.66.252	10.1.17.215	TLSv1.2	81	Application Data
23542	918.199344	10.1.17.215	45.125.66.252	TCP	60	49822 → 443 [ACK] Seq=579 Ack=1693 Win=65280 Len=0
23543	918.199346	10.1.17.215	45.125.66.252	TLSv1.2	81	Application Data
23551	918.424344	45.125.66.252	10.1.17.215	TCP	60	443 → 49822 [ACK] Seq=1693 Ack=606 Win=64896 Len=0
23562	923.384220	45.125.66.252	10.1.17.215	TLSv1.2	81	Application Data
23563	923.384970	10.1.17.215	45.125.66.252	TLSv1.2	81	Application Data

Appendix B – pfSense Phase Report

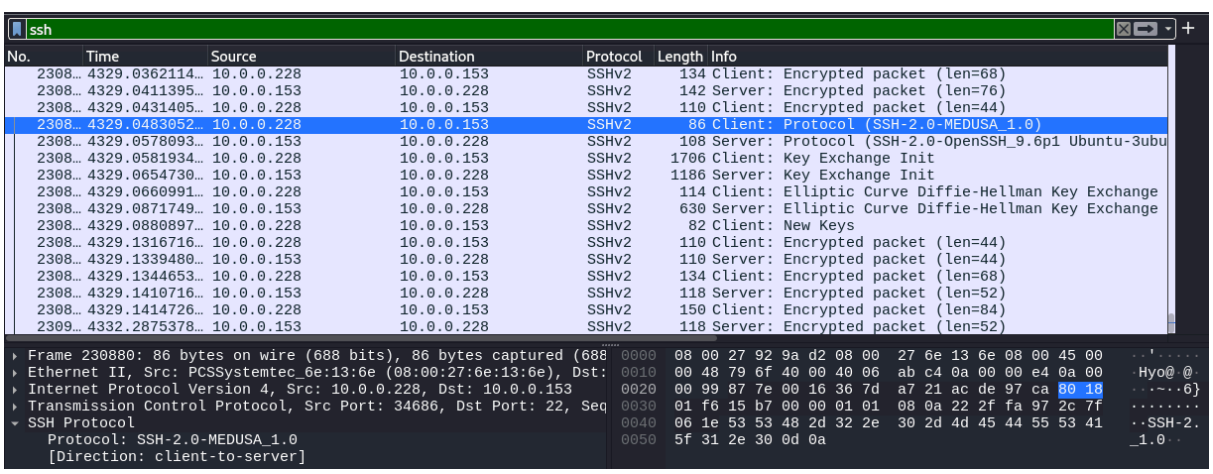
Activity:

1. It was discovered based on cybersecurity news that threat actors were using a list of high risk malicious IP addresses to gain access to systems and take advantage of the system vulnerabilities. Among these IP addresses are;
    - 23.126.71.110
    - 23.242.140.232
    - 24.23.185.95
    - 24.32.75.63
    - 24.98.165.40
    - 176.59.56.133 (from high-risk countries)
    - 117.86.57.51 (from high-risk countries)

The traffic was monitored to check if these IP addresses were used to gain unauthorized access to the company system.

Brute Force Attack Detection

Brute force attack - Performing a Wireshark analysis, there was a lot of traffic between the company system's IP address and an external IP address (10.0.0.228) using Medusa (an SSH brute-force attacking tool), signaling a brute force attack.



These IP addresses were blacklisted to prevent incidents/events while continuing with traffic and logs monitoring and detection.

https://10.0.0.169/firewall_aliases.php?tab=ip

pfsense COMMUNITY EDITION | System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help

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

Firewall / Aliases / IP

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

IP | Ports | URLs | All

Firewall Aliases IP

Name	Type	Values	Description	Actions
GeoIPs	Host(s)	176.59.56.133, 117.86.57.51	GeoIPs from high risk countries	
Malicious_IPs	Host(s)	10.0.0.228, 23.126.71.110, 23.242.140.232, 24.23.185.95, 24.32.75.63, 24.98.165.40	Malicious IP addresses	
Phobos_ransomware	Host(s)	45.89.127.159, 88.198.21.27, 45.9.74.14, 147.78.47.224, 179.43.172.241	IP addresses associated with Phobos	

Add | Import

https://10.0.0.169/firewall_rules.php?if=wan

pfsense COMMUNITY EDITION | System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help

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

Firewall / Rules / WAN

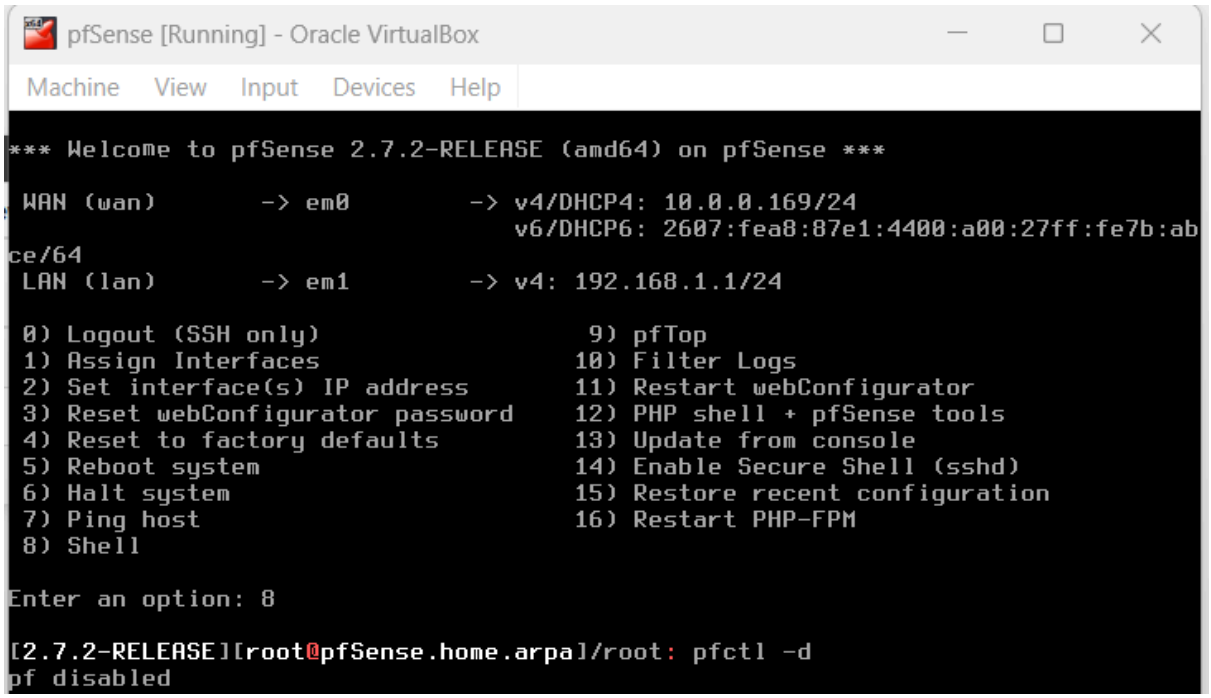
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating | WAN | LAN

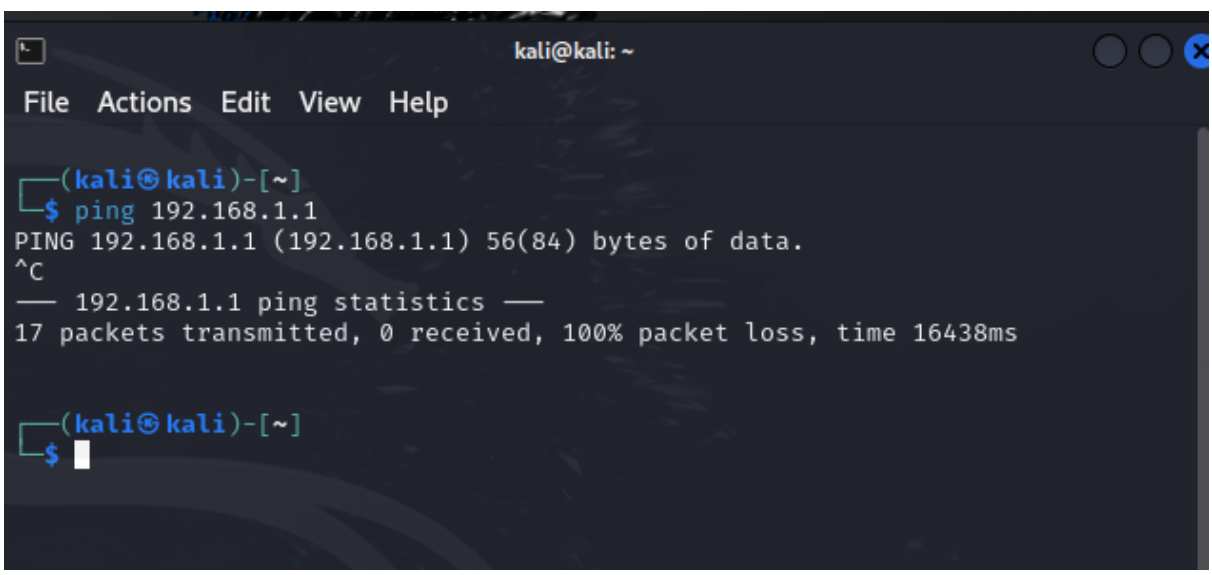
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0/634 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
	0/0 B	IPv4 TCP	GeoIPs	*	WAN address	80 (HTTP)	*	none		GeoIPs from high risk countries	
	0/0 B	IPv4 TCP	Malicious_IPs	*	WAN address	80 (HTTP)	*	none		Malicious IP addresses	
	0/0 B	IPv4 TCP	Phobos_ransomware	*	WAN address	80 (HTTP)	*	none		IP addresses associated with Phobos	
	0/2 KiB	IPv4 TCP	*	*	10.0.0.169	80 (HTTP)	*	none			

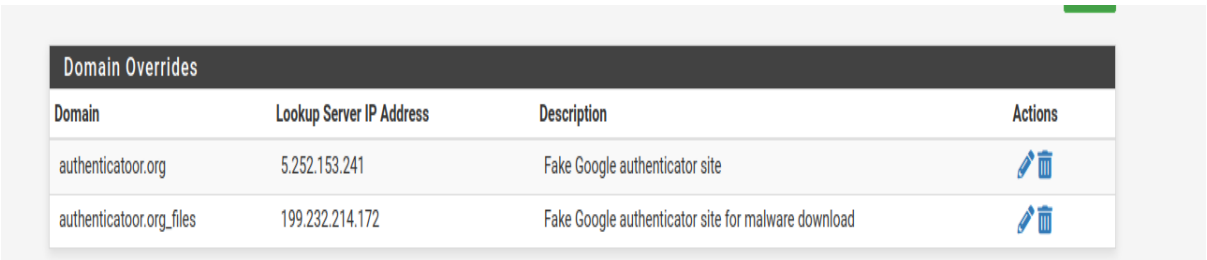
Add | Add | Delete | Toggle | Copy | Save | Separator



Using Kali as the attacker machine, the company's system IP address (192.168.1.1) was pinged. There was 100% packet loss, showing that the attacker is unable to gain unauthorized access.



2. Also firewall rules were set to block IP addresses associated with Phobos ransomware.
   In addition, in order to prevent future access to the fake google authenticator site used by the attackers during the wireshark traffic analysis, access from the company system to the associated IP addresses were blocked. These IP addresses were:
   - 5.252.153.241
   - 199.232.214.172

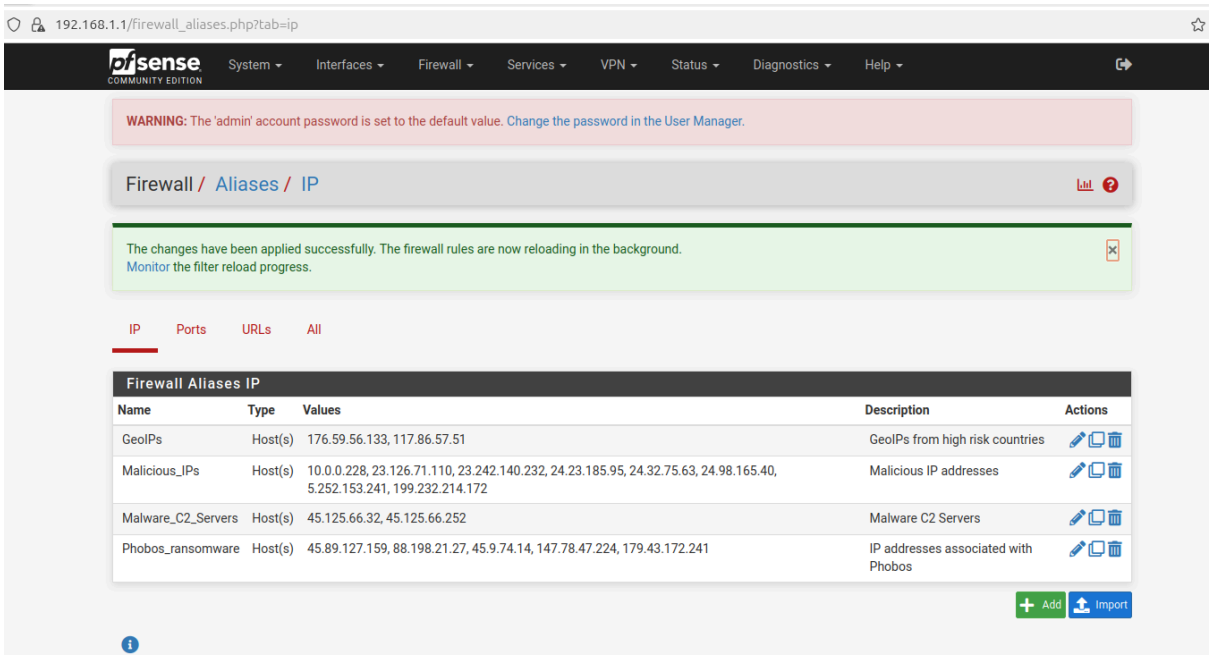


Domain Overrides

Domain	Lookup Server IP Address	Description	Actions
authenticatoor.org	5.252.153.241	Fake Google authenticator site	
authenticatoor.org_files	199.232.214.172	Fake Google authenticator site for malware download	

These IP addresses were also blocked from gaining access to the systems as well.

The IP addresses associated with the malware command-and-control (C2) servers 45.125.66.32 and 45.125.66.252 were also blocked.



192.168.1.1/firewall_aliases.php?tab=ip

pfsense COMMUNITY EDITION | System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help

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

Firewall / Aliases / IP

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

IP | Ports | URLs | All

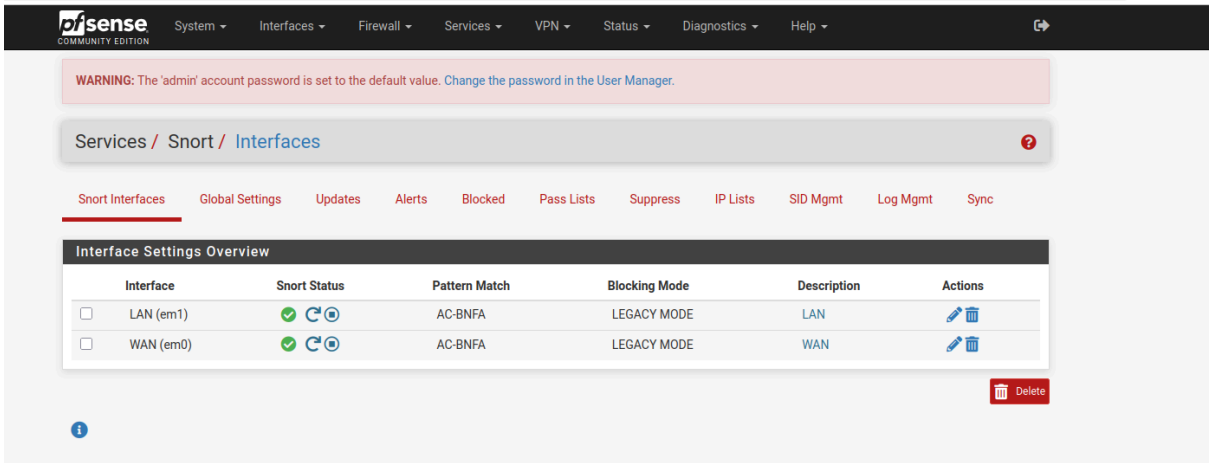
Firewall Aliases IP

Name	Type	Values	Description	Actions
GeoIPs	Host(s)	176.59.56.133, 117.86.57.51	GeoIPs from high risk countries	
Malicious_IPs	Host(s)	10.0.0.228, 23.126.71.110, 23.242.140.232, 24.23.185.95, 24.32.75.63, 24.98.165.40, 5.252.153.241, 199.232.214.172	Malicious IP addresses	
Malware_C2_Servers	Host(s)	45.125.66.32, 45.125.66.252	Malware C2 Servers	
Phobos_ransomware	Host(s)	45.89.127.159, 88.198.21.27, 45.9.74.14, 147.78.47.224, 179.43.172.241	IP addresses associated with Phobos	

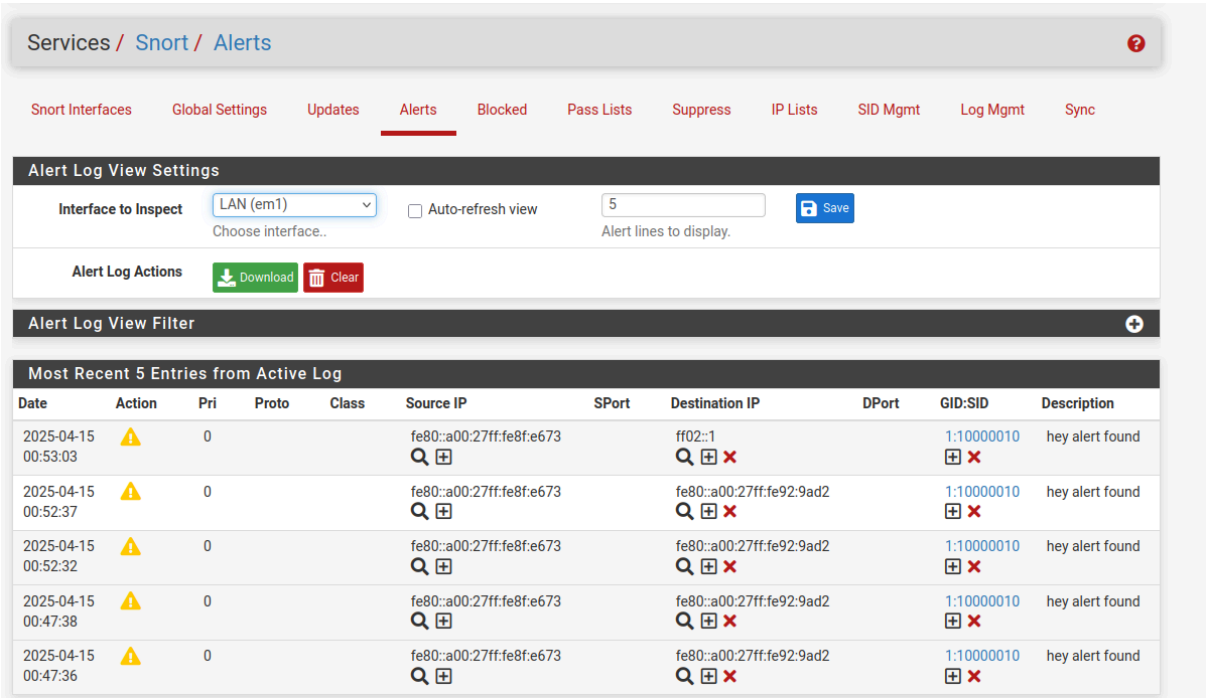
Add | Import

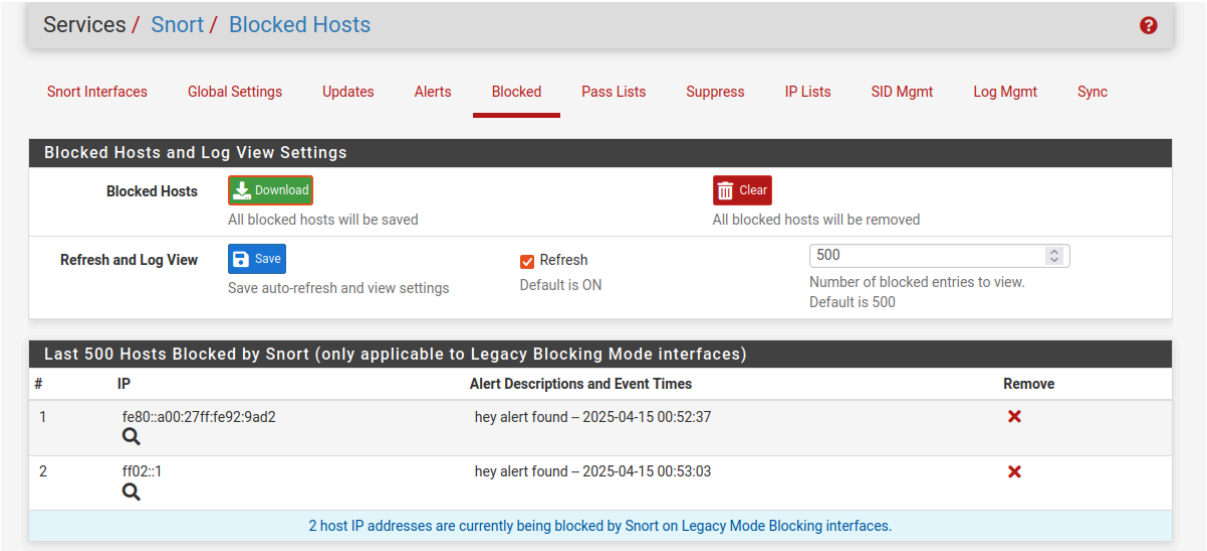
Intrusion Detection System (SNORT)

Snort Interfaces have been set up for LAN and WAN with blocking mode to block hosts that generate a snort alert, while the host machine's IP has been added to pass list.



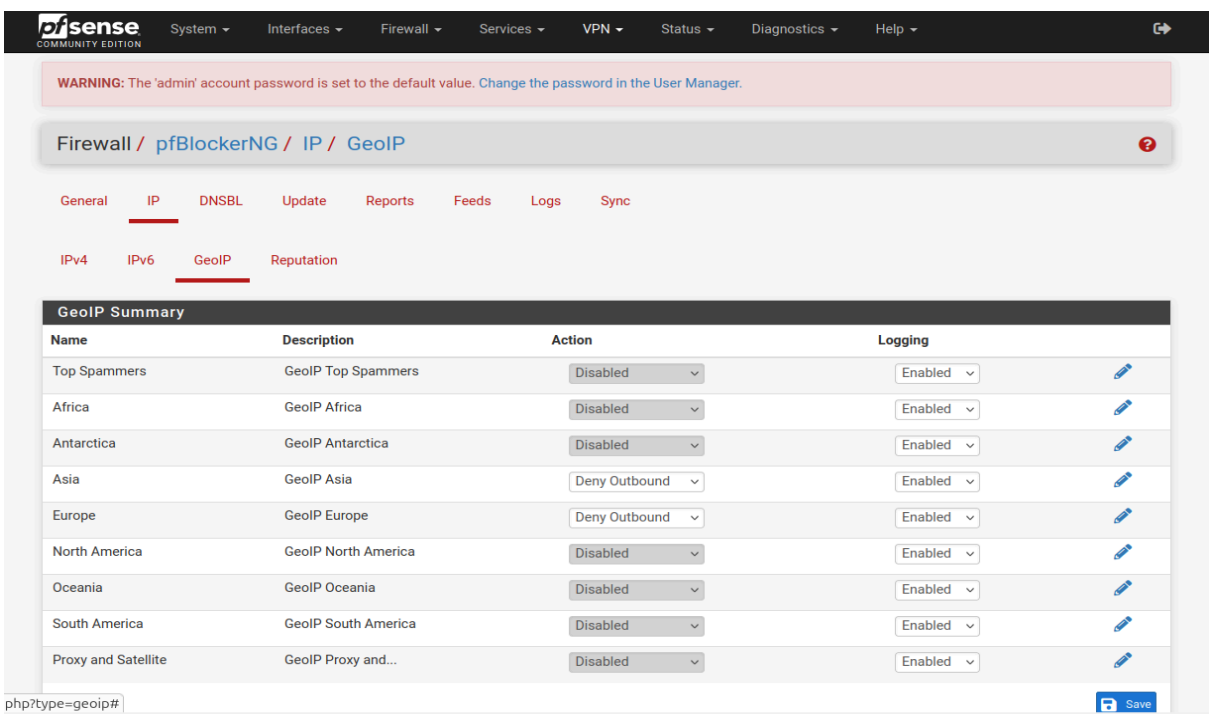
The below alerts were generated with automatic blocking as seen in screenshots.

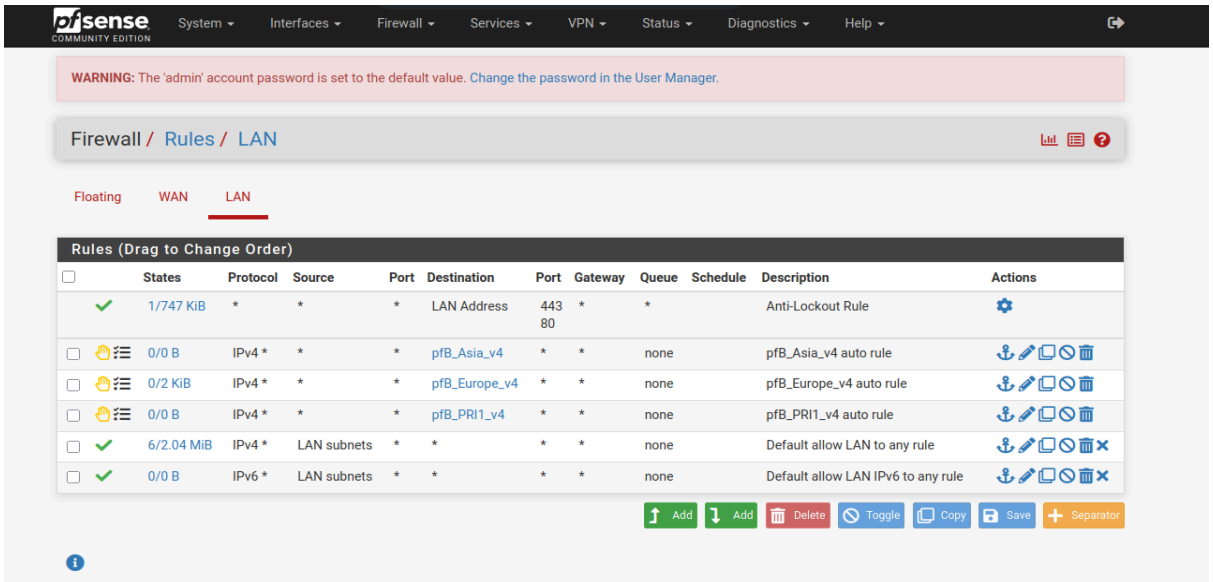




GeoIP Blocking

Using pfBlockerNG for GeoIP blocking, high risk countries in Asia (China) and Europe (Russia) were blocked.

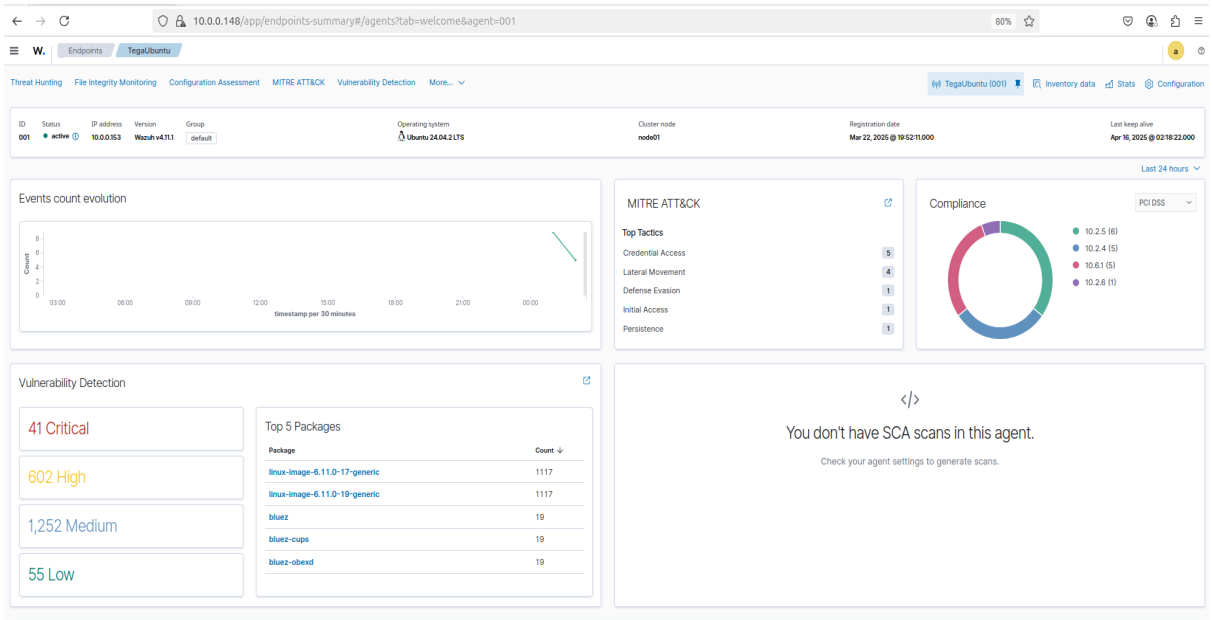




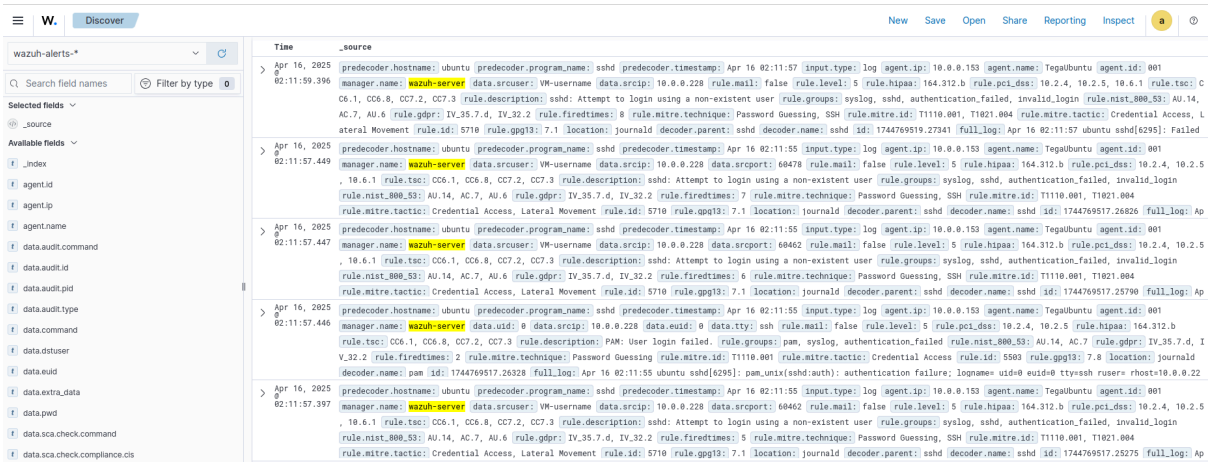
Appendix C – Wazuh Phase Report

Activity:

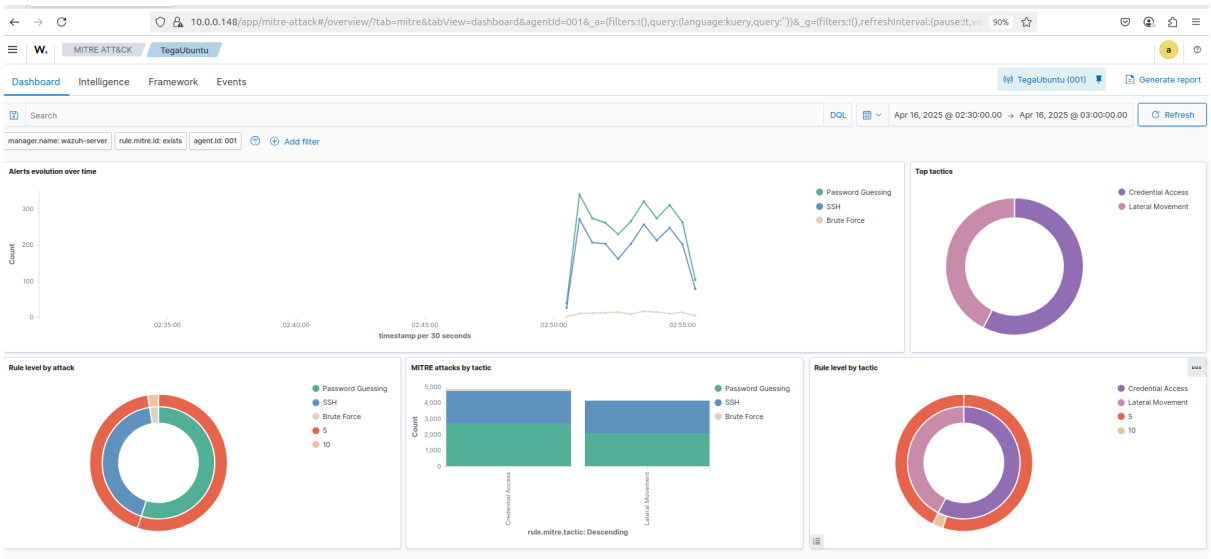
1. There were alerts received in Wazuh SIEM signaling a malicious attack on the endpoints.



2. Found logs from the Wazuh dashboard on login and password guessing attempts from external sources.



3. There were brute force attacks detected from the Wazuh dashboard showing active system vulnerabilities.

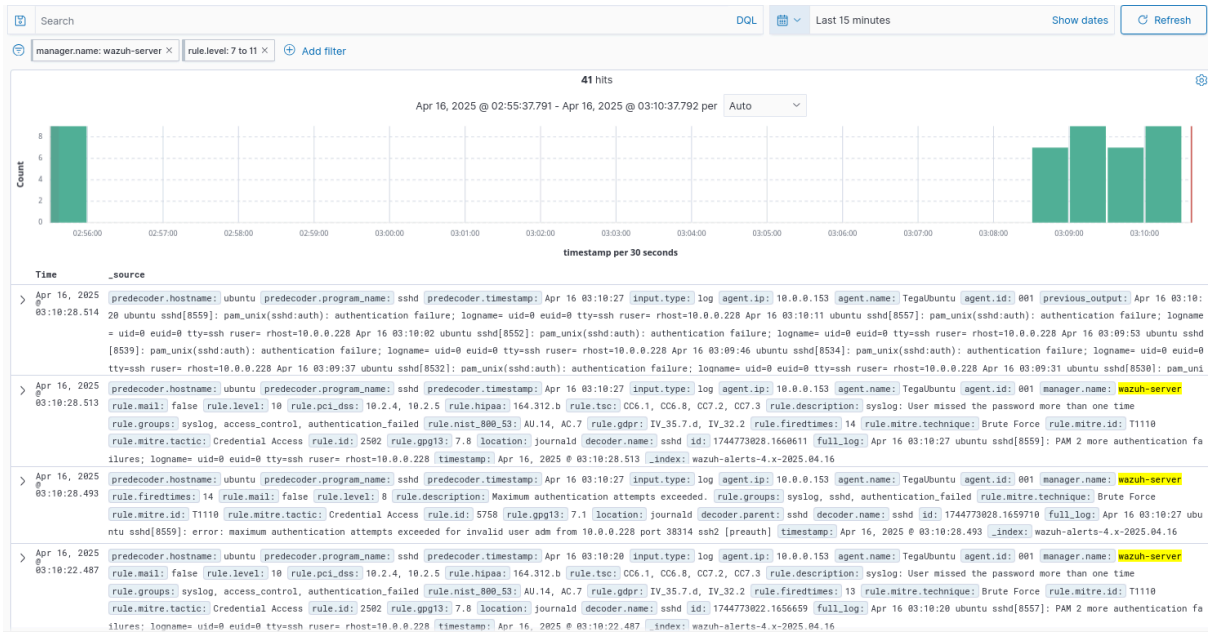


Here are the logs identifying Indicators of Compromise (IoCs);

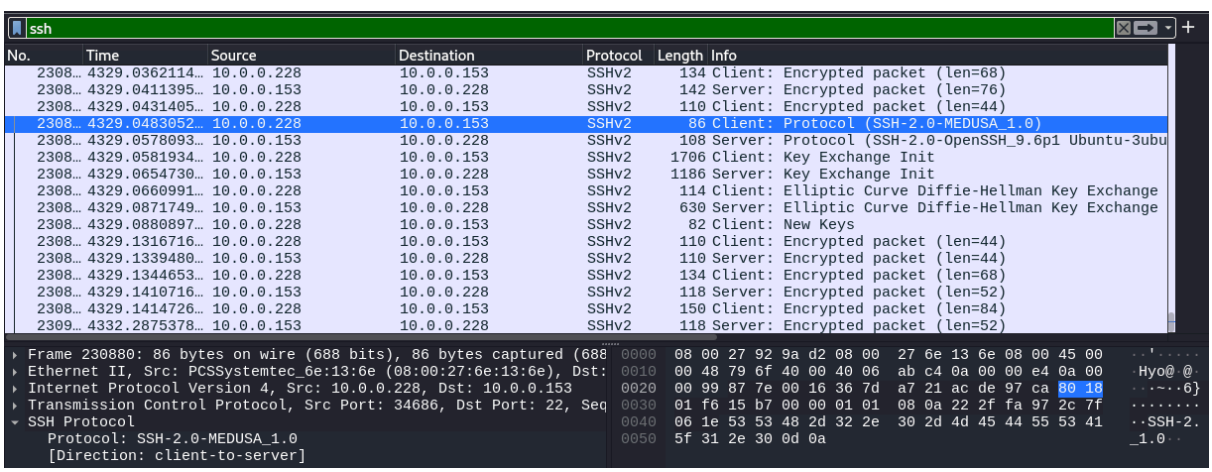
```
Apr 16, 2025 @ 02:55:31.562
predecoder.hostname: ubuntu predecoder.program_name: sshd predecoder.timestamp: Apr 16 02:55:30 input.type: log agent.ip: 10.0.0.153 agent.name: TegaUbuntu agent.id: 001 manager.name: wazuh-server
data.srcuser: toor data.srcip: 10.0.0.228 data.srcport: 50168 rule.mail: false rule.level: 5 rule.hipaa: 164.312.b rule.pci_dss: 10.2.4, 10.2.5, 10.6.1 rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3
rule.description: sshd: Attempt to login using a non-existent user rule.groups: syslog, sshd, authentication_failed, invalid_login rule.nist_800_53: AU.14, AC.7, AU.6 rule.gdpr: IV_35.7.d, IV_32.2
rule.firedtimes: 1,440 rule.mitre.technique: Password Guessing, SSH rule.mitre.id: T1110.001, T1021.004 rule.mitre.tactic: Credential Access, Lateral Movement rule.id: 5710 rule.gpg13: 7.1 location: jo
urnald decoder.parent: sshd decoder.name: sshd id: 1744772131.1498662 full_log: Apr 16 02:55:30 ubuntu sshd[8208]: Disconnected from invalid user toor 10.0.0.228 port 50168 [preauth] timestamp: Apr 16, 2

Apr 16, 2025 @ 02:55:31.556
predecoder.hostname: ubuntu predecoder.program_name: sshd predecoder.timestamp: Apr 16 02:55:29 input.type: log agent.ip: 10.0.0.153 agent.name: TegaUbuntu agent.id: 001 manager.name: wazuh-server
data.srcuser: toor data.srcip: 10.0.0.228 data.srcport: 50152 rule.mail: false rule.level: 5 rule.hipaa: 164.312.b rule.pci_dss: 10.2.4, 10.2.5, 10.6.1 rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3
rule.description: sshd: Attempt to login using a non-existent user rule.groups: syslog, sshd, authentication_failed, invalid_login rule.nist_800_53: AU.14, AC.7, AU.6 rule.gdpr: IV_35.7.d, IV_32.2
rule.firedtimes: 204 rule.mitre.technique: Password Guessing, SSH rule.mitre.id: T1110.001, T1021.004 rule.mitre.tactic: Credential Access, Lateral Movement rule.id: 5710 rule.gpg13: 7.1 location: jour
nald decoder.parent: sshd decoder.name: sshd id: 1744772131.1498129 full_log: Apr 16 02:55:29 ubuntu sshd[8206]: Disconnected from invalid user toor 10.0.0.228 port 50152 [preauth] timestamp: Apr 16, 202

Apr 16, 2025 @ 02:55:31.540
predecoder.hostname: ubuntu predecoder.program_name: sshd predecoder.timestamp: Apr 16 02:55:29 input.type: log agent.ip: 10.0.0.153 agent.name: TegaUbuntu agent.id: 001 manager.name: wazuh-server
data.uid: 0 data.srcip: 10.0.0.228 data.euid: 0 data.tty: ssh rule.mail: false rule.level: 5 rule.pci_dss: 10.2.4, 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3
rule.description: PAM: User login failed. rule.groups: pam, syslog, authentication_failed rule.nist_800_53: AU.14, AC.7 rule.gdpr: IV_35.7.d, IV_32.2 rule.firedtimes: 588 rule.mitre.technique: Password
Guessing rule.mitre.id: T1110.001 rule.mitre.tactic: Credential Access rule.id: 5503 rule.gpg13: 7.8 location: journald decoder.name: pam id: 1744772131.1497629 full_log: Apr 16 02:55:29 ubuntu sshd[8
228]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.0.228 timestamp: Apr 16, 2025 @ 02:55:31.540 _index: wazuh-alerts-4.x-2025.04.16
```



4. Performing a Wireshark analysis, there was a lot of traffic between the company system's IP address and an external IP address (10.0.0.228) using Medusa (an SSH brute-force attacking tool).



The malicious IP address was blocked in pfSense (pls see screenshots in Appendix B).