THREAT DETECTION & INCIDENT RESPONSE USING WIRESHARK,

PFSENSE AND WAZUH

SoCra Tech

Melvin Baird

Security Operations Centre (SOC) Analyst

25th April, 2025

Table of Contents

Executive summary

Sacra Tech`s network security witnessed increased suspicious network activities. A

comprehensive analyses of the network security using a three-phase SOC approach

with Wireshark, pfSense, and Wazuh was carried out. The objectives were to detect

and respond to network anomalies, block malicious traffic, and investigate potential

threats. This effort led to the identification and mitigation of several critical indicators of

compromise (IoCs), and final recommendations was provided to strengthen their

cybersecurity network frame.

Introduction

Sacra Tech has expressed growing concerns of increased suspicious network activities

such as potential unauthorized access, malware infections and insider threats. I was

tasked to provide solutions and mitigations to these concerns and will highlight the

processes which include using tools like Wireshark, pfSense and Wazuh to strengthen

Socra Tech`s security network posture.

Methodology

Sequentially, a 3 phase approach below were implemented to achieve our task of a

strong and less vulnerable network

• Wireshark was used to for real time data/packet and protocol captures, and

used for proper analysis

• pfSense was configured to implement firewall to control network traffic and

access, and also to put up Intrusion detection and prevention rules.

• Wazuh was deployed to act as our centralized Security information and event

Management (SIEM) alerting tool, log correlation and response tool.

Phase 1: NETWORK TRAFFIC CAPTURE AND ANALYSIS (WIRESHARK)

Wireshark was deployed on Kali Linux to capture Socra Tech`s network traffic logs and used for proper

analysis. The log contains all activities performed on all endpoints on the network. The analysis is done to

identify suspicious activities and immediately, move to mitigate any vulnerabilities noticed on the

network. Packet filtering was done using different protocols (HTTP, DNS). This aided in the analysis and

identification of suspicious traffic

Objective	**To analyze suspicious or unusual network traffic patterns To analyze suspicious or unusual network traffic patterns**
Key actions	**analysis focused on HTTP, DNS and SSH traffic** **Identified multiple suspicious DNS queries** **Identified unusual HTTP patterns**
Tools	**Wireshark on Kali**
Findings	**Multiple suspicious traffic on DNS queries** **Multiple failed connection attempts (brute force)** **Unauthorized data exfiltration attempt**

In our analysis, we filtered packets using different protocols to identify suspicious traffic.

HTTP: - I looked out for packets with

- unusual user-agent string, to know who is making the requests whether its made from a bot or

through a browser.

- user-agents with strings like nmap which is used for Port Scan

- Agents with commands like wget, curl and so on

- Unusually long URLs that contain random characters

- commands like PUT, DELETE, TRACE, CONNECT

- Content length, data packet size, and unusual large number of connections to a server/IP by a

user within a short period, which could indicate brute forcing, scanning and so on.

DNS: I looked for query types- ANY, OPT (for tunneling), Trusted anchor (TA), start of Authority (SOA)

- Investigated high query rates to a single domain

- Large number of requests to command and control server

- Large DNS packets

- TXT records with unusual content.

SSH traffic: I filtered with tcp.port ==22 and analyzed connection patterns, protocol exchanges.

- Also filtered for traffic not on port 22 (tcp.port != 22) to detect whether traffic ran through other

ports

- Checked for SYN packets without ACK and the frequency of connections attempts. (this may

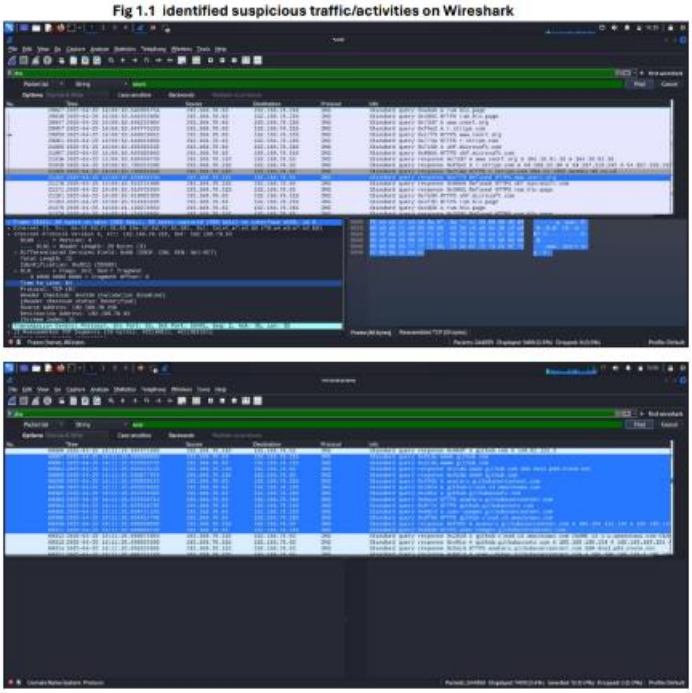
point to brute force)

- Unusual packet sizes or patterns and analyses the TCP stream to see the pattern of data transfer

In the analysis, I found multiple access refusal to some sites (snort.org and Microsoft.com) and high

frequency of connection attempts, which indicate brute forcing. Screenshot below

Fig 1.1 identified suspicious traffic/activities on Wireshark



Phase 2: Firewall implementation & Policy enforcement (pfSense)

To enhance network security and control over network traffic, a robust firewall "pfSense'' was installed

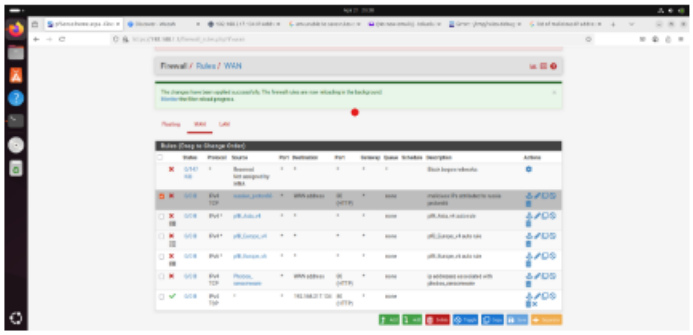
and configured as a gateway for traffic management. This is put in place to effectively manage

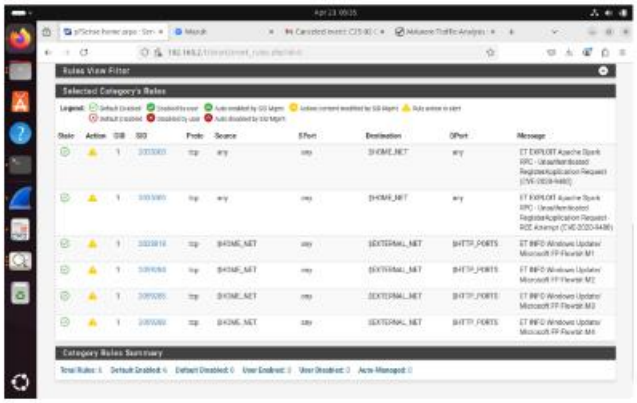
network traffic by blocking malicious traffic using the firewall rules to prevent

unauthorized access to the network environment

Objective	**Protect the network by detecting malicious traffic using Intrusion Detection system (IDS) rules and promptly displaying activity alerts Prevent malicious traffic using Intrusion Prevention system (IPS) and firewall rules**
Key action	**Configured Snort IDS to prompt malicious/suspicious**

	traffic **Configured GeoIP filtering using pfBlockerNg to block network traffic based on** **geographical locations of source IPs. Traffic from some high-risk countries were** **blocked in this stance. (fig 2.5.1 and fig 2.5.2)** **Firewall rules were set to prevent SSH access from external source.** **Brute force attacks were initiated from Kali linux on Ubuntu VM. pfSense monitored** **and blocked the brute force attempts. Screenshot below**
Tools	**pfSense**
Findings	**Blocked multiple unauthorized SSH attempts and malicious IPs**





GeoIP Filtering

Before i set GeoIP filtering rules, I accessed 3 sites from chosen geographical regions I wanted to block traffic to and from and they were accessible (to test the sites for connectivity), and tried to access the site after setting the rules to confirm rule effectiveness.

Figure 2.2 www.aparat.com (Iranian website)

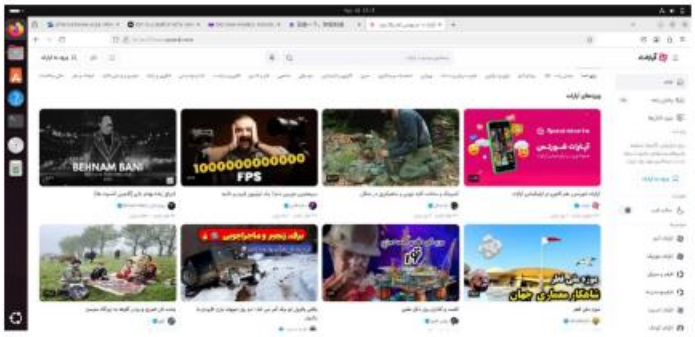


Fig 2.3 www.baidu.com (a Chinese search engine site)

Fig 2.4 www.yandex.ru (a Russian site)

Setting the GeoIP firewall rules

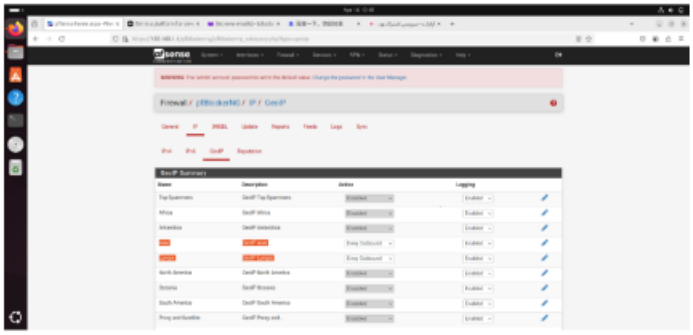


Fig 2.5.1 pfBlockerNG for GeoIP

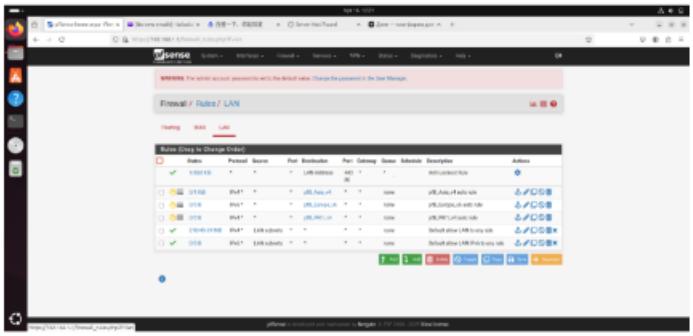


Fig 2.5.2 firewall Rule for GeoIP

Mitigation results: Same Sites visited earlier could not be accessed after the GeoIP filtering rules were enabled which proves that our GeoIP rule worked effectively. Inbound and Outbound traffic were blocked.

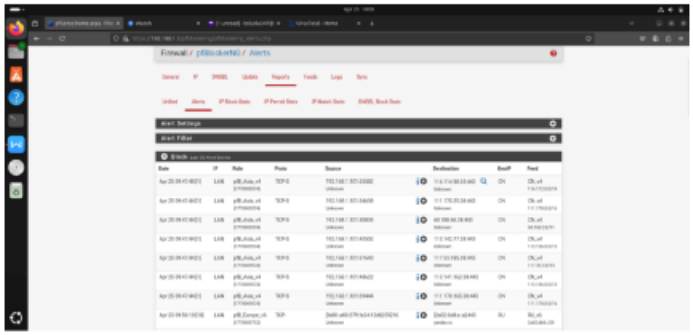


Fig 2.6 blocked traffic from GeoIP rule

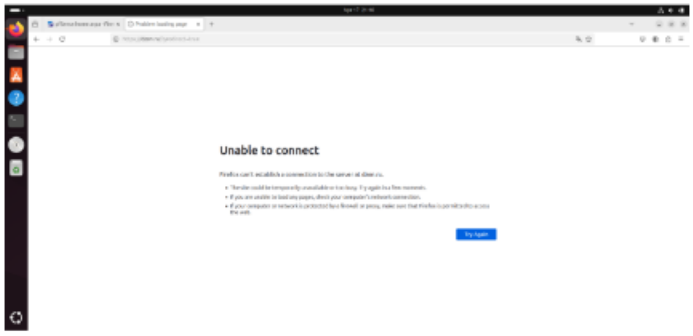


Fig 2.7 yandex.ru blocked on both inbound and outbound traffic

firewall rule set to block specific IPs known for 'proton66' ransomware attacks from a group in Russia as an example. (highlighted)

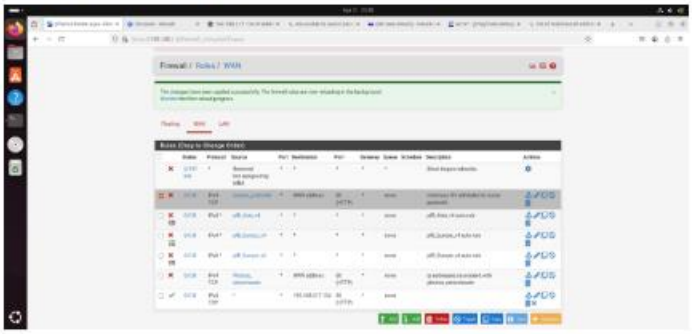
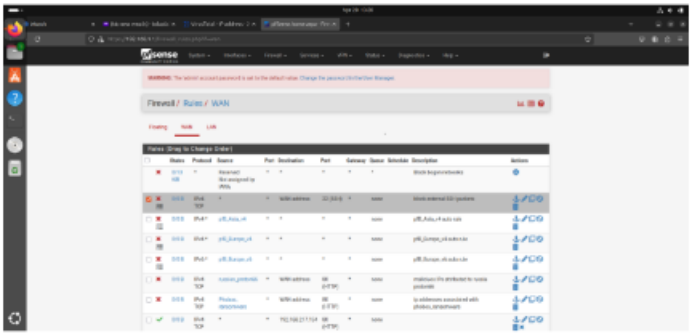
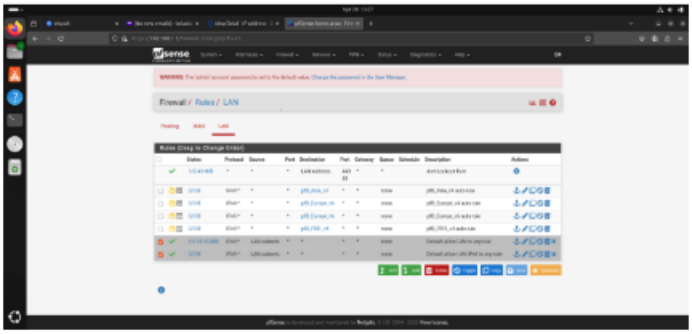


Fig 2.10 Proton66 ransomware IPs blocked on both inbound and outbound traffic

Configure firewall rules to prevent unauthorized SSH access from external sources

The highlighted rules in screenshot below reflect the firewall rule set to prevent unauthorized SSH access from external sources and also SSH access from local host (LAN).





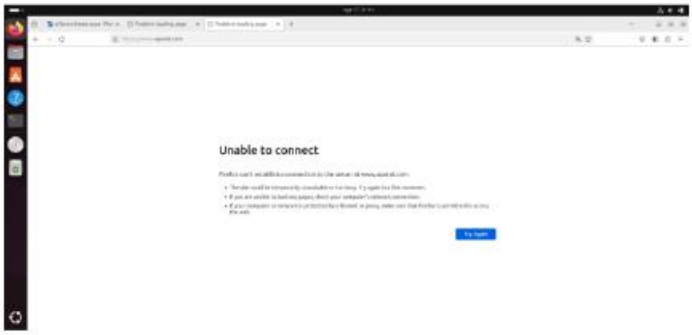


Fig 2.8 Aparat.com blocked on both inbound and outbound traffic

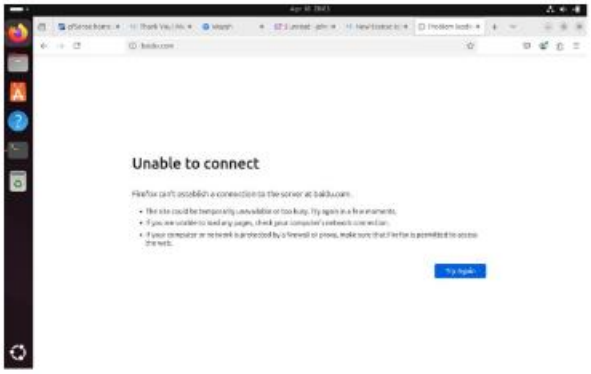
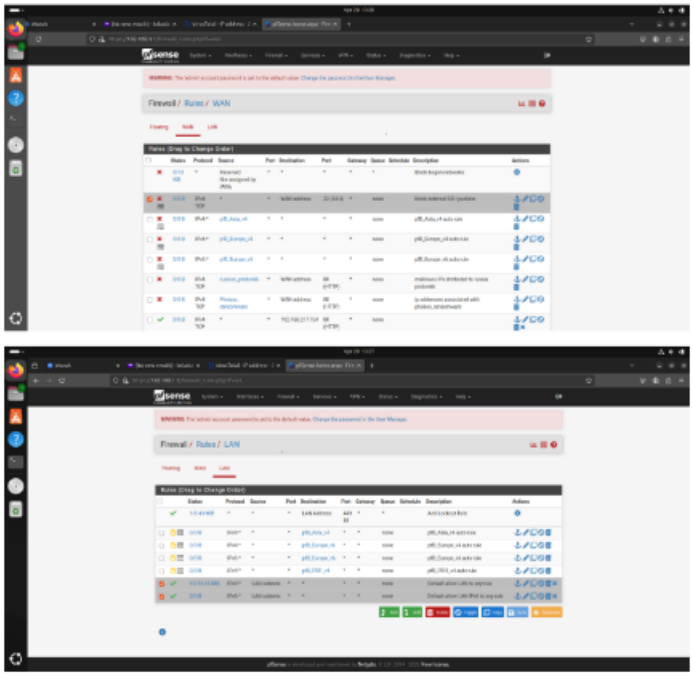


Fig 2.9 Baidu.com blocked on both inbound and outbound traffic

Configure firewall rules to prevent unauthorized SSH access from external sources

The highlighted rules in screenshot below reflect the firewall rule set to prevent unauthorized SSH access from external sources and also SSH access from local host (LAN).



Phase 3: SECURITY EVENT MONITORING AND INCIDENT RESPONSE (WAZUH)

To enhance network security and control over network traffic, a robust firewall "pfSense'' was installed

and configured as a gateway for traffic

Objective	**Deploy Wazuh as the SIEM solution to correlate and analyze logs from different sources, including Wireshark and pfSense**
Key actions	**-Configured Wazuh to aggregate logs from pfSense and endpoints.** **Set up an agent in Wazuh to take logs, with preset rules on Wazuh API for logs on network activities including attacks, and also prompt alerting of such.** **- Initiated hydra and Medusa attacks from Kali linux against Ubuntu VM (IP**

	192.168.1.101) **-Correlation and analysis of Wazuh logs matched the packet captures on Wireshark** **with time stamps.**
Tools	**Wazuh SIEM**
Findings	**- Logs revealed brute force attacks, password guessing, multiple failed SSH** **authentication, (fig 3.4) and denied Mitre tactics ranging from credential access,** **lateral movement across the network, defense evasion, privilege escalation and** **persistence (fig 3.3)**
Identification of IOCs	**- Multiple Failed Login Attempts** **- Unauthorized Access to Sensitive Data/Systems** **- Security Alerts of suspicious activities** **- Unusual Network Traffic**
Mitigation	**Implementing Prevention, Swift detection and response processes** **- Users to adopt strong and complex passwords and Multi-factor** **authentication** **- Install IDS and IPS tools to monitor your network, detect and block** **suspicious activities, enable prompt alert and logs** **- Address patch vulnerabilities promptly** **- Proper configurations on systems** **- Monitoring, logging and prompt alerting by having SIEM installed on the** **network/systems** **- Incident response plan in place to address containment, eradication and** **recovery.** **- Post incident Analysis to identify vulnerability and improve security** **measures.**

A screenshot before the attacks were initiated (fig 3.1)

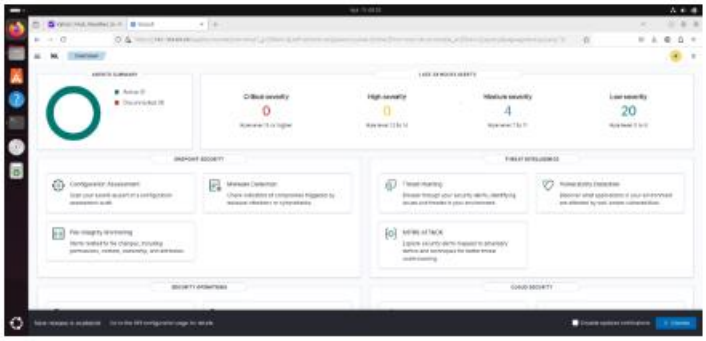


Figure 3.1 Wazuh dashboard before the attack

- **After attack from Kali Linux by Hydra and Medusa**

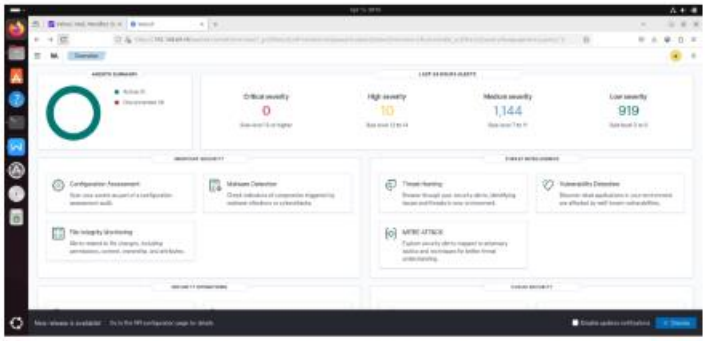


Figure 3.2 Wazuh dashboard after the attack showing number of alerts

Fig 3.3 Wazuh dashboard showing Mitre att&ck

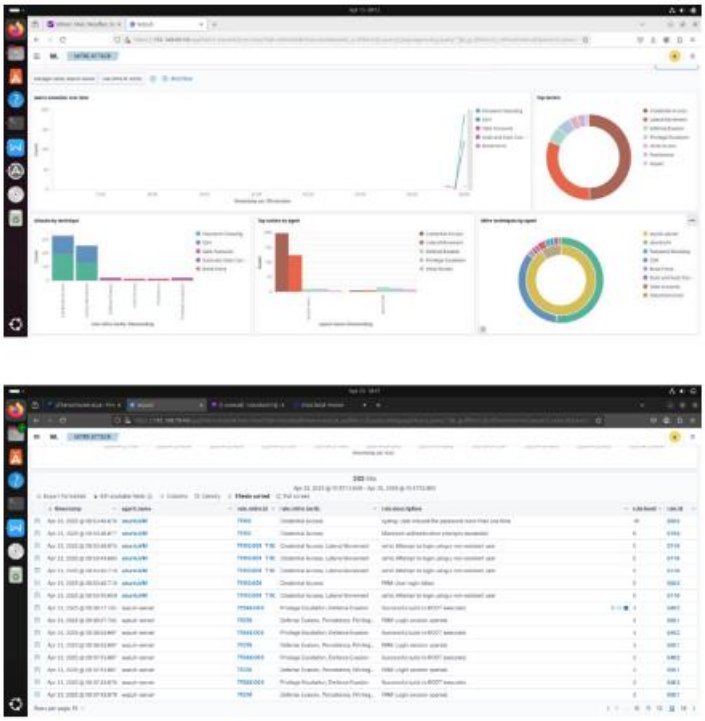


Fig 3.4 Wazuh dashboard showing threat hunting

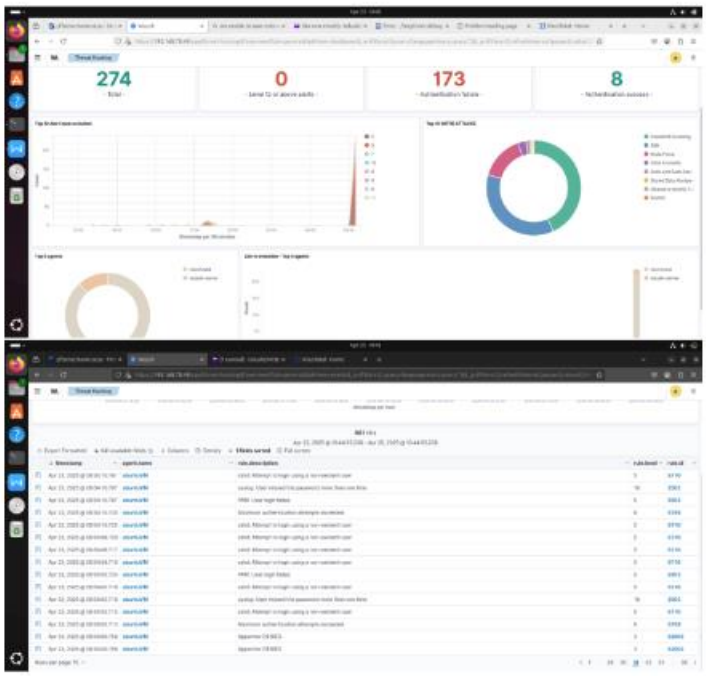


Fig 3.5 Wazuh dashboard showing vulnerability detection

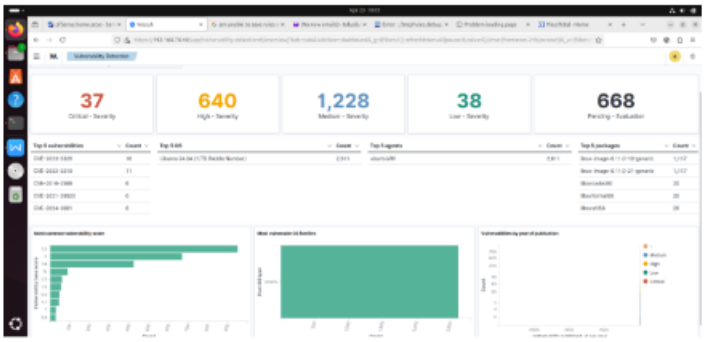
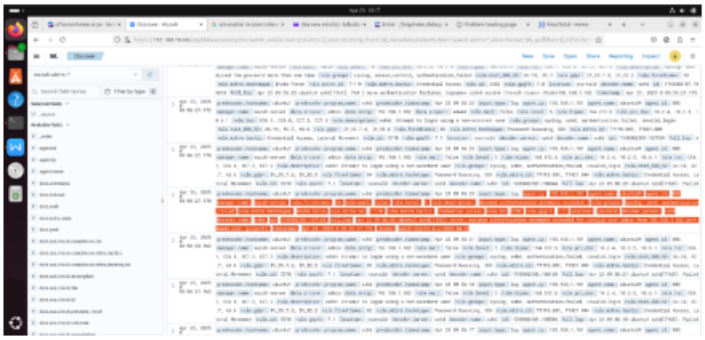


Fig 3.6 Wazuh dashboard showing log details of traffic



Wazuh log

FINAL FINDINGS & IMPACT

The engagement revealed several indicators of Compromise such as

- Multiple Failed brute force login attempts

- Denied Unauthorized Access to Sensitive Data/Systems

- Security Alerts on the security tools (pfsense and Wazuh)

- Unusual Network Traffic

confirmed that SoCra Tech was susceptible to cyberattacks, as their Network security posture was vulnerable to unauthorized access due to lack of IDS and IPS

firewall in place, which could have ultimately led to several other vulnerabilities and

consequences such as data breach/exfiltration, potential malware infections,

financial loss, legal issues, reputational damages and so on.

	Detection and Analysis
Detection and Analysis	**Wireshark was used to capture and detect several failed login attempts on the network among many other activities. I filtered the packet data captured and analyzed for unusual activities and detected the above**
Containment	**pfSense was installed as a firewall to manage such traffic by applying Snort rules to block unauthorized SSH access within the network. Network segmentation was recommended to further limit lateral movement across the network in case of any breach.**
Eradication	**The use of Wazuh in this case was very important as it helped to block such unauthorized access and brute force attacks using preset rules on Wazuh API, took logs of such activities for threat intelligence and digital forensic use.**
Recovery	**There was no recorded actual loss (data, financial or otherwise) as at the time of conducting this exercise, and possible potential losses have been taken care of with our implementation of the above tools**
Post incidence response	**The incident is documented, while the root cause of the unauthorized access was investigated, and found to be an attack with**

	hydra and medusa, guessing passwords to access the network. Reinforcing the security of the network, MFA was recommended and firewall rules updated
Takeaways	**Organizations need to strengthen their network security posture to** **- Avoid Sensitive data being exposed due to unauthorized access,** **Can cause disruption of company operations leading to financial losses, reputational damages, and legal issues** **- Deploy firewall measures to manage in and outbound traffic on their network** **- Strong access control measures to be implemented and RBAC should be enforced.** **- Maintain reliable back-up system/server**
	- Employee training and endpoint security strengthened **- Regular and timely Patching** **- Have layered defenses like IDS, firewalls, and by segmenting networks to isolate malware infections** **- Stay informed on emerging threats and threat actors.** **- Having an incident response plan in place to minimize damage in case of attacks.**

RECOMMENDATIONS

Based on the findings, the following are recommended.

1. To address unauthorised access

- Enhanced Login Monitoring: Implement real-time monitoring and alerting for failed login attempts across all critical systems (servers, applications, databases, cloud services). Focus on repeated failures from the same source or

user.

- Track successful logins, paying close attention to logins from unusual geographic locations (especially if outside of work area and typical business travel).

- Logins outside of normal business hours for specific users and from previously unseen devices or systems.

- Multiple logins from the same user account originating from different locations within a short timeframe.

• Privileged Access Management (PAM) Monitoring: Rigorously monitor the usage of privileged accounts (administrator, root, etc.), alert on any unauthorized attempts to access or use privileged accounts, log and audit all actions performed by privileged accounts, monitor for privilege escalation attempts.

• Network Segmentation Monitoring: Implement and strictly enforce network segmentation, monitor network traffic for any unauthorized attempts to traverse between network segment, alert on any cross-segment communication that violates defined policies.

• Physical Security Integration (if applicable): Correlate physical access logs (e.g badge swipes) with logical access attempts. Alert on discrepancies, such as a login occurring when the user's badge wasn't used to enter the building.

• Multi factor authentication:

- This will further ensure only authorized personnel can access the network, and also Role based access control (RBAC) should be enforced.

2. Potential Malware Infections

• Network Traffic Analysis for Malicious Communication: implement and maintain Intrusion Detection/Prevention Systems (IDS/IPS) with up-to-date signatures for known malware and exploit attempts.

- Analyze network flow data for unusual outbound connections to known malicious IPs or domains, or to geographically suspicious locations.

- Monitor for unusual DNS queries or high volumes of DNS requests to unknown domains.

- Inspect web traffic for access to known command-and-control (C2) servers or suspicious file downloads.

• Sandbox Analysis: Implement a sandbox environment to detonate suspicious files (e.g., email attachments, downloaded files) and analyze their behavior for malicious activity.

• File Integrity Monitoring (FIM): Implement FIM on critical system files, executables, and configuration files to detect unauthorized modifications that could indicate malware activity. Alert on any unexpected changes to these files.

• Regular Security Awareness Training: Educate employees about the risks of phishing, social engineering, and insider threats.

• Regular Vulnerability Assessments and Penetration Testing: Proactively identify and address security weaknesses in the infrastructure.

• Develop and Regularly Test Incident Response Plans: Ensure the SOC team is prepared to effectively respond to security incidents.

CONCLUSION

This SOC analysis project offered a valuable and realistic experience in network defense, providing the opportunity to implement detection, monitoring, and incident response procedures with professional security tools. The threats identified and addressed emphasize the urgent requirement for SoCra Tech to adopt a more proactive approach to improving its overall security posture