Investigating and Reporting Suspicious Activities

Organization: North Bridge Fintech
Analyst: Daniel Nwachukwu
Role: Security Operations Center (SOC) Analyst
Submission Date: January 23, 2026

1. Executive Summary

Purpose:
The purpose of this assessment was to simulate real-world attacks in a controlled lab environment to validate the effectiveness of deployed security measures. The evaluation focused on intrusion detection, log monitoring, and incident alerting using pfSense, Snort IDS/IPS, Wazuh SIEM, and Ubuntu services (FTP and HTTP).

Key Findings:

ICMP ping attempts from Kali to Ubuntu were successfully detected by Snort.

FTP (Port 21) and HTTP (Port 80) services were confirmed open on the Ubuntu VM.

Apache web server activities were successfully logged and monitored via Wazuh.

Web vulnerability scan using detected by Wazuh agent.

Reconnaissance and brute-force attacks were detected by wazuh agent.

Several network scans detected by Wireshark.

2. Project Introduction

This project involved a controlled security exercise designed to assess network and system defenses within a lab environment. The primary focus was on detecting and reporting network reconnaissance, port scanning, and basic web vulnerability scanning activities. The lab environment consisted of:

Ubuntu VM: Target server hosting FTP,HTTP and HTTPS services.

Kali VM: Attacker/source machine performing ping tests, port scans, and web vulnerability scans.

pfSense with Snort: Network perimeter firewall and IDS/IPS for intrusion detection.

Wazuh SIEM: Centralized logging, correlation, and alerting platform.

The project aimed to validate alerting workflows, ensure logging coverage, and demonstrate SOC response capability.

3. Methodology & Scope

Target Asset: Ubuntu VM (192.168.1.105)

Source Asset: Kali VM (192.168.1.101)

Monitored Services: FTP (Port 21), HTTP (Port 80), ICMP traffic

Tools Used:

Nmap: Port scanning to discover live host and open and vulnerable ports

Hydra-wizard: SSH brute-forcing for gaining access(authorized) into the system

Wireshark: Packet filtering and network analysis

Apache2:Web server for hosting HTTP/HTTPS

Snort on pfSense: IDS/IPS for detecting ICMP pings.

Wazuh Dashboard/AGENT (Dan007): Centralized logging, alerting, and monitoring.

Timeline:

Lab setup and configuration: January 30, 2026.

Attack simulation and alert validation: January 30–31, 2026.

3.1 Lab Architecture

Network Topology

Attacker VM: Kali Linux

Target VM: Ubuntu Server

Security Devices:

pfSense Firewall

Snort IDS/IPS (custom rule)

Wazuh Agent (installed on Ubuntu)

Monitoring Tool: Wireshark

[Kali Linux]
|
| (Attack Traffic)

[pfSense Firewall] ---> [Snort IDS/IPS]
|
[Ubuntu Server]
- SSH (22)
- FTP (21)
- HTTP (80 / Apache2)
- Wazuh Agent

3.2 MONITORING OVERVIEW

The Security Operations Center (SOC) monitoring phase focused on continuous visibility into host-based and network-based activities using **Wazuh, Snort,** and **Wireshark.** These tools were deployed to detect, analyze and investigate potential security threats across multiple stages of the attack lifecycle.

During the monitoring period, a total of five (5) different significant security events were logged by the Wazuh agent. These events spanned key adversarial techniques, including reconnaissance, defense evasion, privilege escalation, and lateral movement, demonstrating the system's ability to detect activity across different phases of a potential intrusion.The monitoring infrastructure generated Two (2) PAM login session (Pluggable Authentication Modules) with low severity level, four (4) failed credential access alerts with medium severity level, Wazuh agent generated six (6) web vulnerability alerts, indicating suspicious or potentially malicious web-based activities targeting the monitored host with a high severity level. Additionally, one(1) defense evasion success was recorded with a crictical severity, another one (1) network-based alert was generated by Snort IPS/IDS with a high severity level highlighting suspicious traffic patterns detected at the network level from a source IP address 192.168.1.1 to destination 192.168.1.105. Other numerous forms of attacks where captured and investigated on wire-shark.

All generated alerts were actively investigated by the SOC analyst. Network reconnaissance activities, including Nmap scans and Netdiscover scans, were identified and confirmed using Wireshark, validating the presence of active host discovery and port scanning behavior. The web vulnerability alerts generated by Wazuh were analyzed to assess exposure to common web-based attack vectors. Furthermore, a privilege escalation alert detected by Wazuh was investigated to evaluate potential unauthorized elevation of user privileges. Reconnaissance-related alerts and the Snort network alert were also reviewed to correlate host and network telemetry.Overall, the monitoring process demonstrated effective detection, alerting, and

investigation capabilities, highlighting the importance of layered visibility using both host-based and network-based security tools within a SOC environment.

Overall Risk Score: Crictical

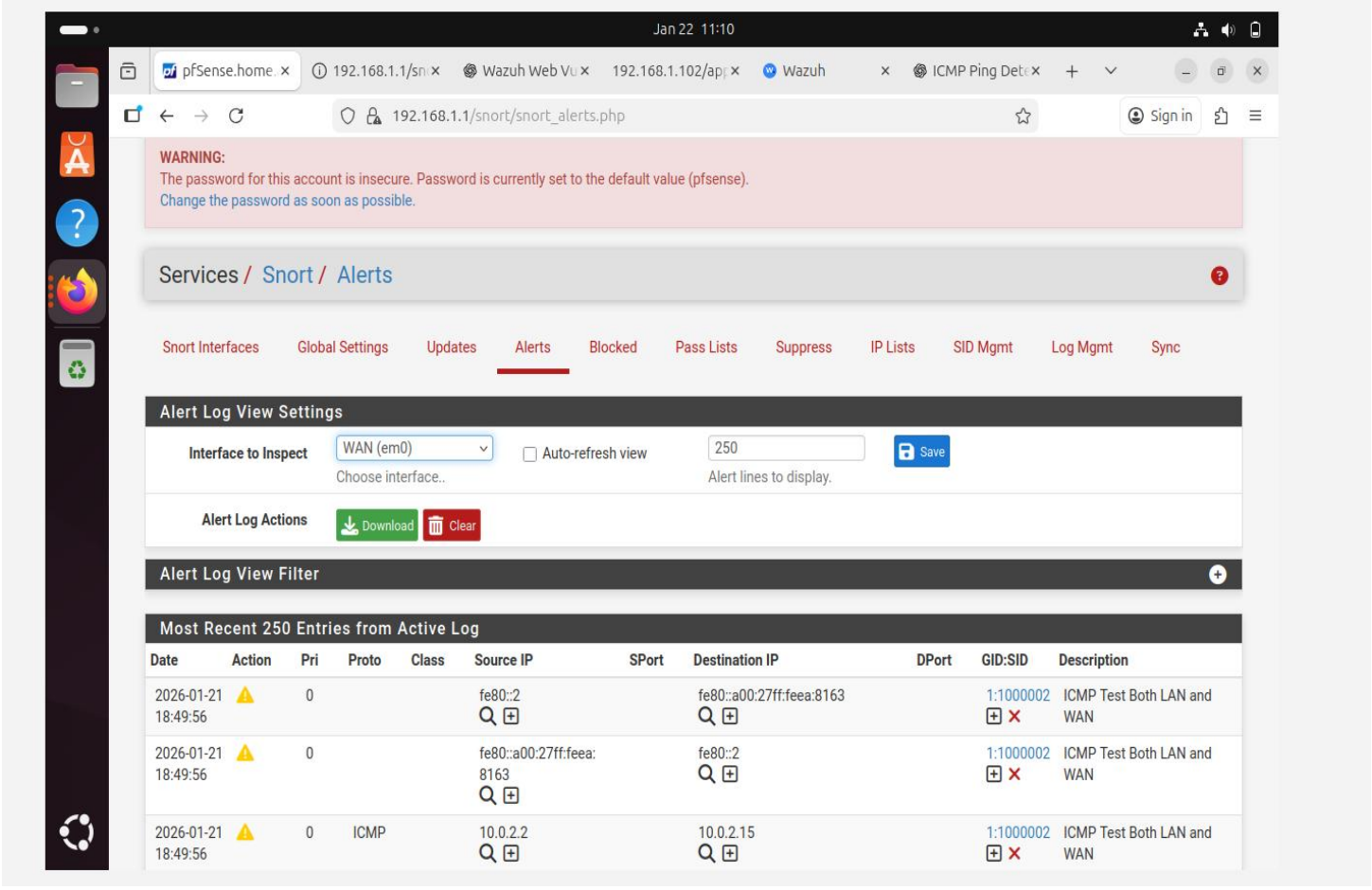
4. Detailed Technical Findings

4.1 ICMP Ping Detection

Description: ICMP echo requests sent fromAttackr (Kali)to Ubuntu.

Severity Level: Low

Classfication: False positive



4.2 OPEN PORTS ON UBUTU VM (193.168.1.105)

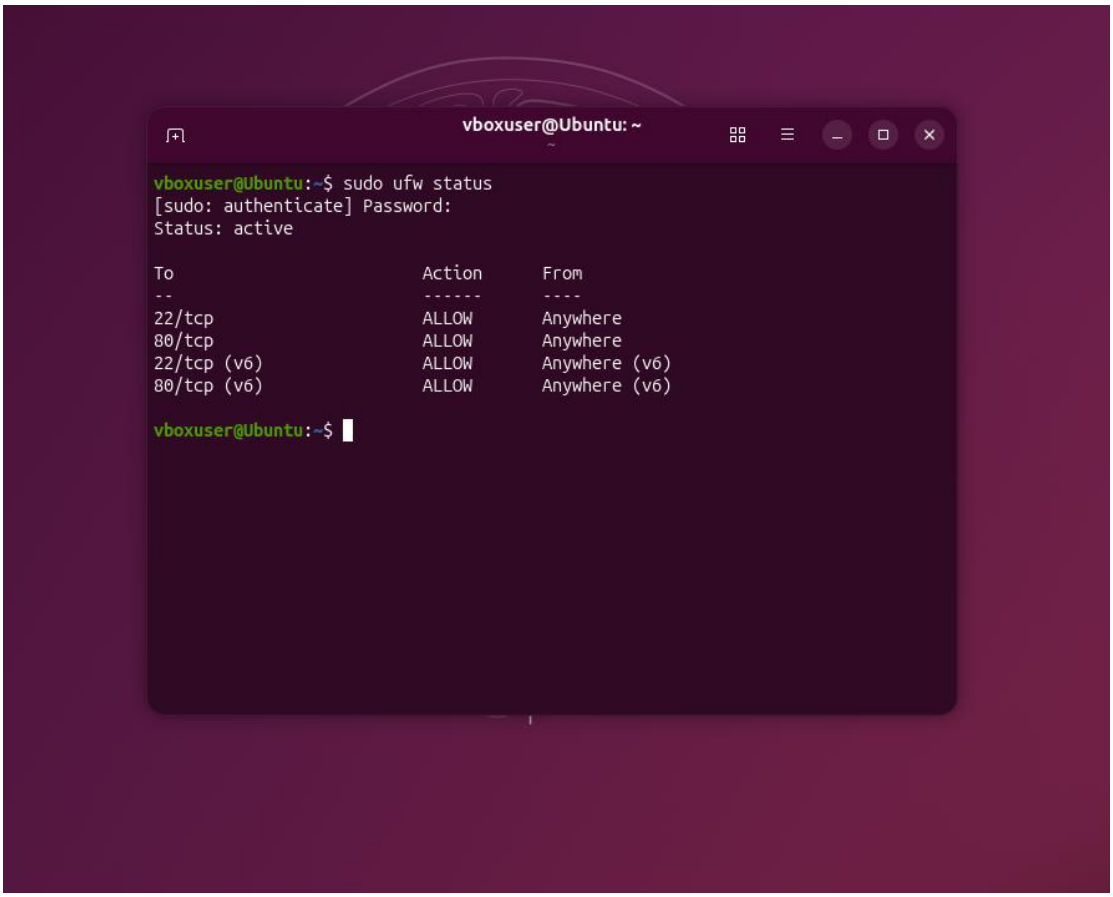
21/FTP

22/SSH

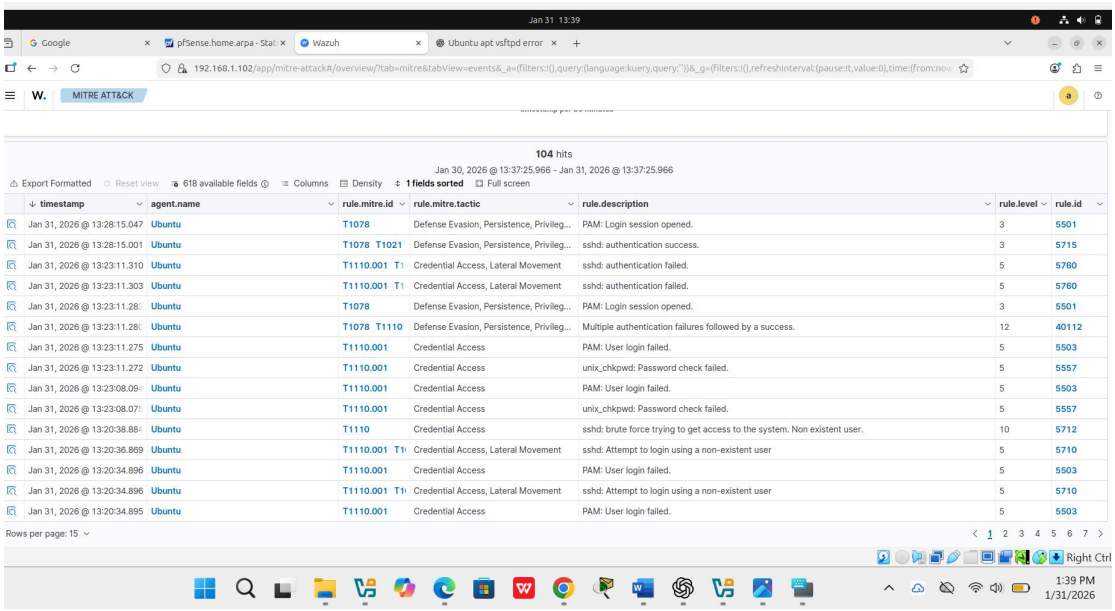
80/HTTP

Status: Service running, accessible from attacker VM.

Evidence



4.3. **Description :** Two (2) PAM login session from admin
Evidence: Wazuh alerts generated from admin login:
Severity Level: (3) Low
Classification: false Positive



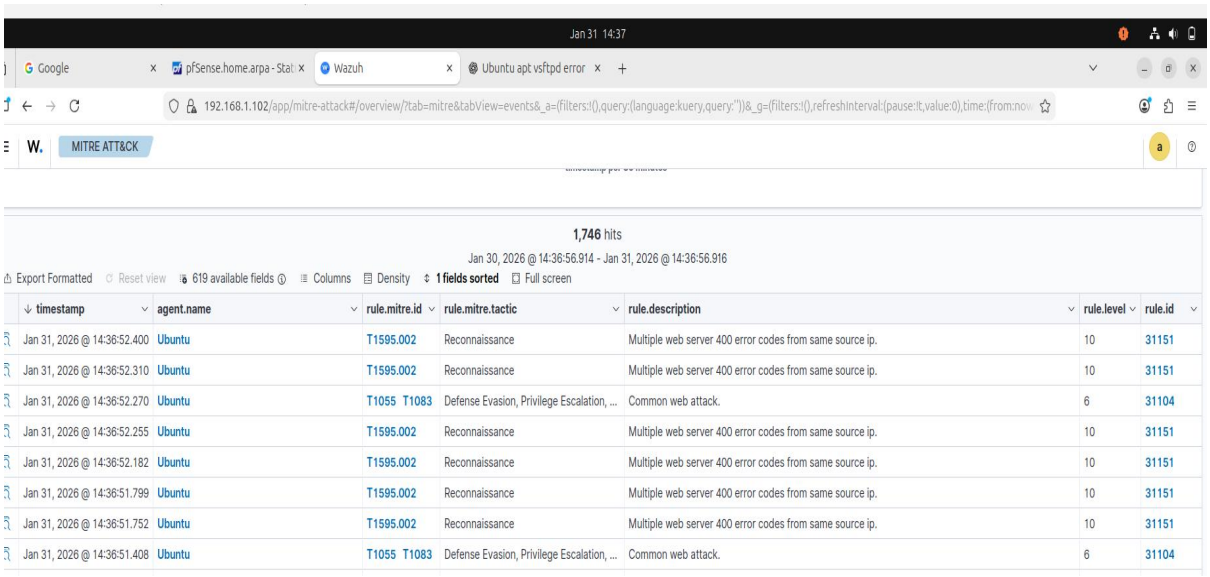
4.4 Reconnaissance activities.

Evidence: Wazuh alerts generated from numerous web vulnerability scans:

Severity Level: High

Classification: True Positive

Impact: Risk of unauthorized access.



timestamp	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
Jan 31, 2026 @ 14:36:52.400	Ubuntu	T1595.002	Reconnaissance	Multiple web server 400 error codes from same source ip.	10	31151
Jan 31, 2026 @ 14:36:52.310	Ubuntu	T1595.002	Reconnaissance	Multiple web server 400 error codes from same source ip.	10	31151
Jan 31, 2026 @ 14:36:52.270	Ubuntu	T1055 T1083	Defense Evasion, Privilege Escalation, ...	Common web attack.	6	31104
Jan 31, 2026 @ 14:36:52.255	Ubuntu	T1595.002	Reconnaissance	Multiple web server 400 error codes from same source ip.	10	31151
Jan 31, 2026 @ 14:36:52.182	Ubuntu	T1595.002	Reconnaissance	Multiple web server 400 error codes from same source ip.	10	31151
Jan 31, 2026 @ 14:36:51.799	Ubuntu	T1595.002	Reconnaissance	Multiple web server 400 error codes from same source ip.	10	31151
Jan 31, 2026 @ 14:36:51.752	Ubuntu	T1595.002	Reconnaissance	Multiple web server 400 error codes from same source ip.	10	31151
Jan 31, 2026 @ 14:36:51.408	Ubuntu	T1055 T1083	Defense Evasion, Privilege Escalation, ...	Common web attack.	6	31104

4.5 Net discover wrshark captures for number of hosts on the network

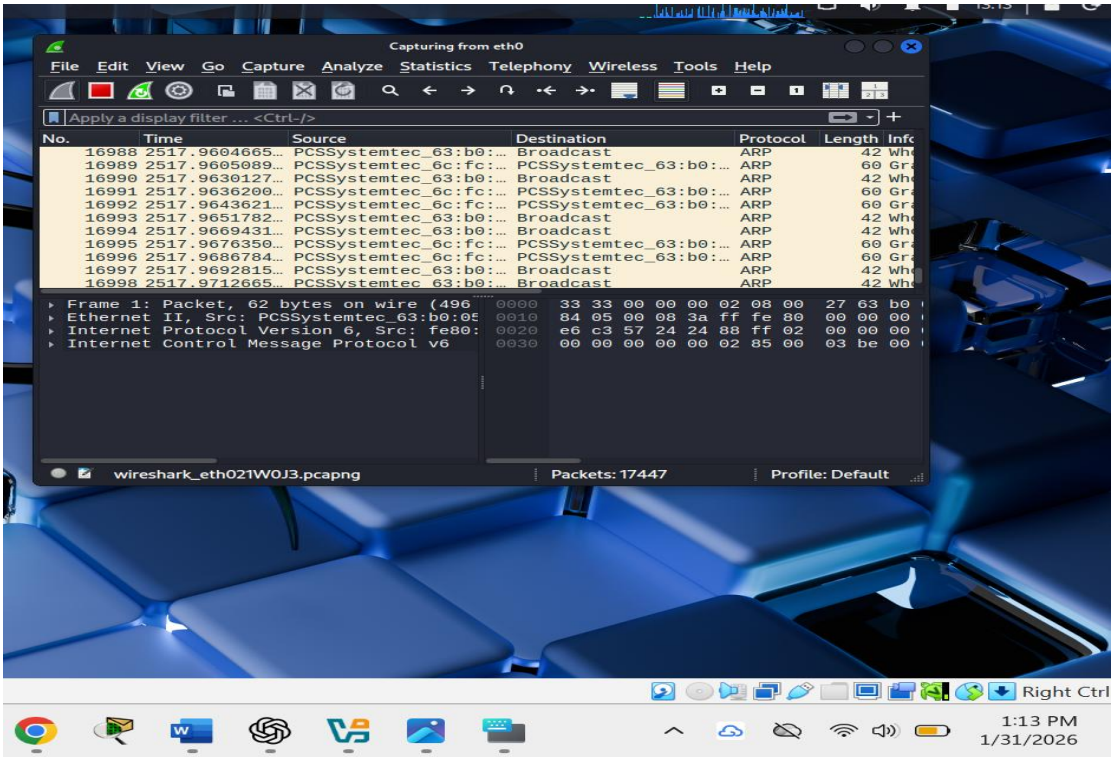
Description: Port scanning from Kali to Ubuntu VM to identify open services.

Evidence: Wireshark captures showing imminent network scanning

Severity Level: High

Classification: True Positive

Impact: Risk of unauthorized access



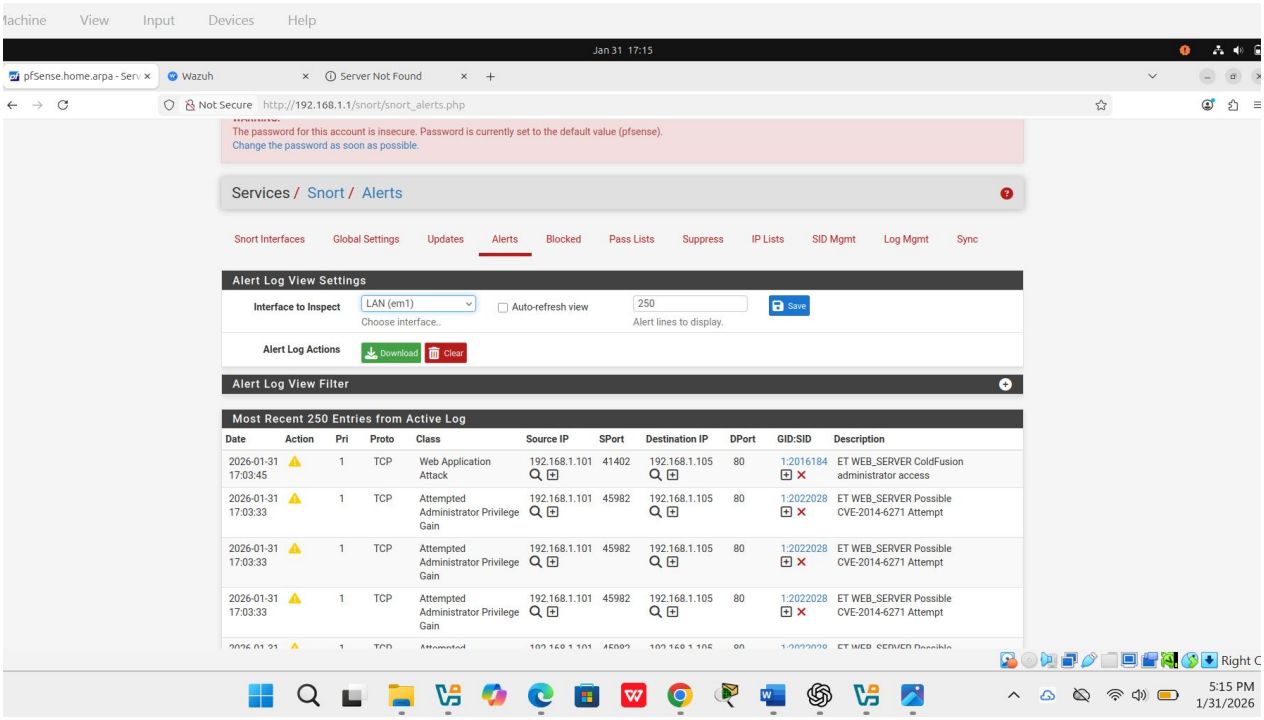
4.6 Description: Web vulnerability scan on HTTP port 80

Evidence: Alert generated by Snort IDS

Severity Level: (10) High

Classification: True Positive

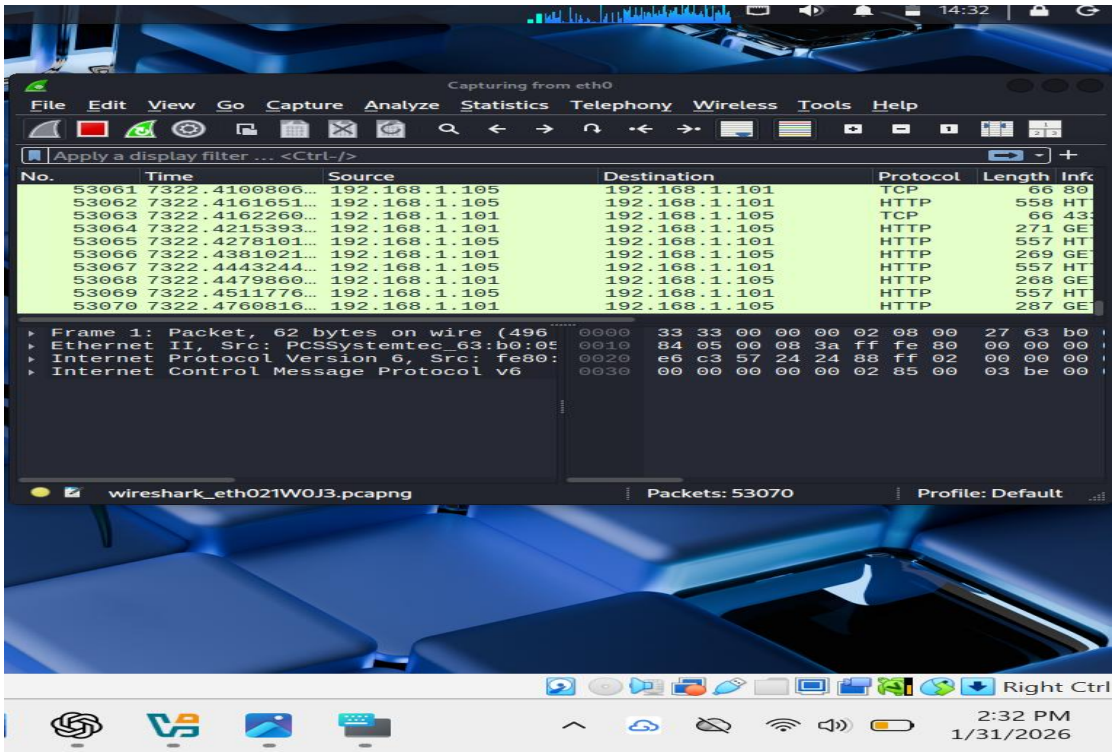
Impact: Risk of unauthorized access



4.7 **. Real-time Wire-shark capture screenshot of HTTP port 80.**

Severity Level:(10) High

Evidence:



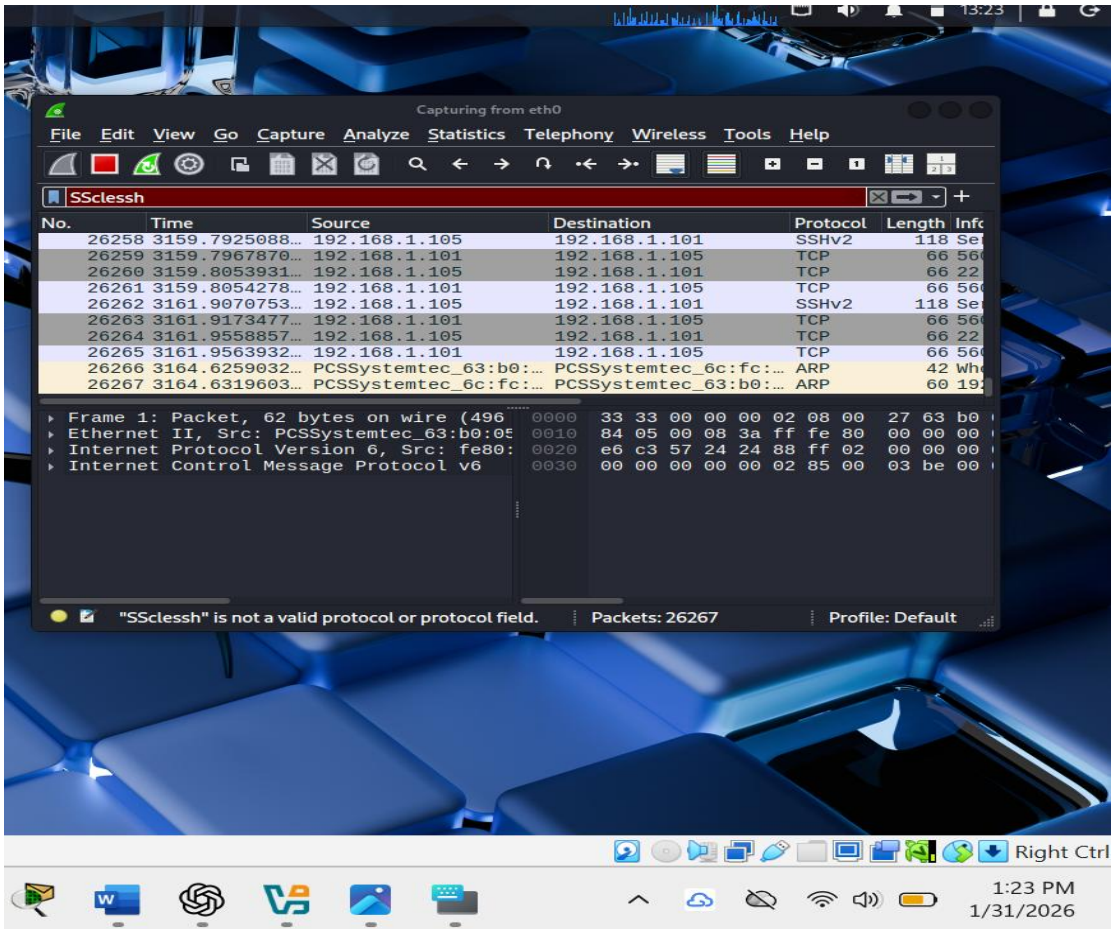
4.8 Nmap scan for open ports on Ubuntu VM

Evidence: Wireshark real-time capture

Severity Level:(10)High

Classification: True Positive

Impact: Risk of unauthorized access



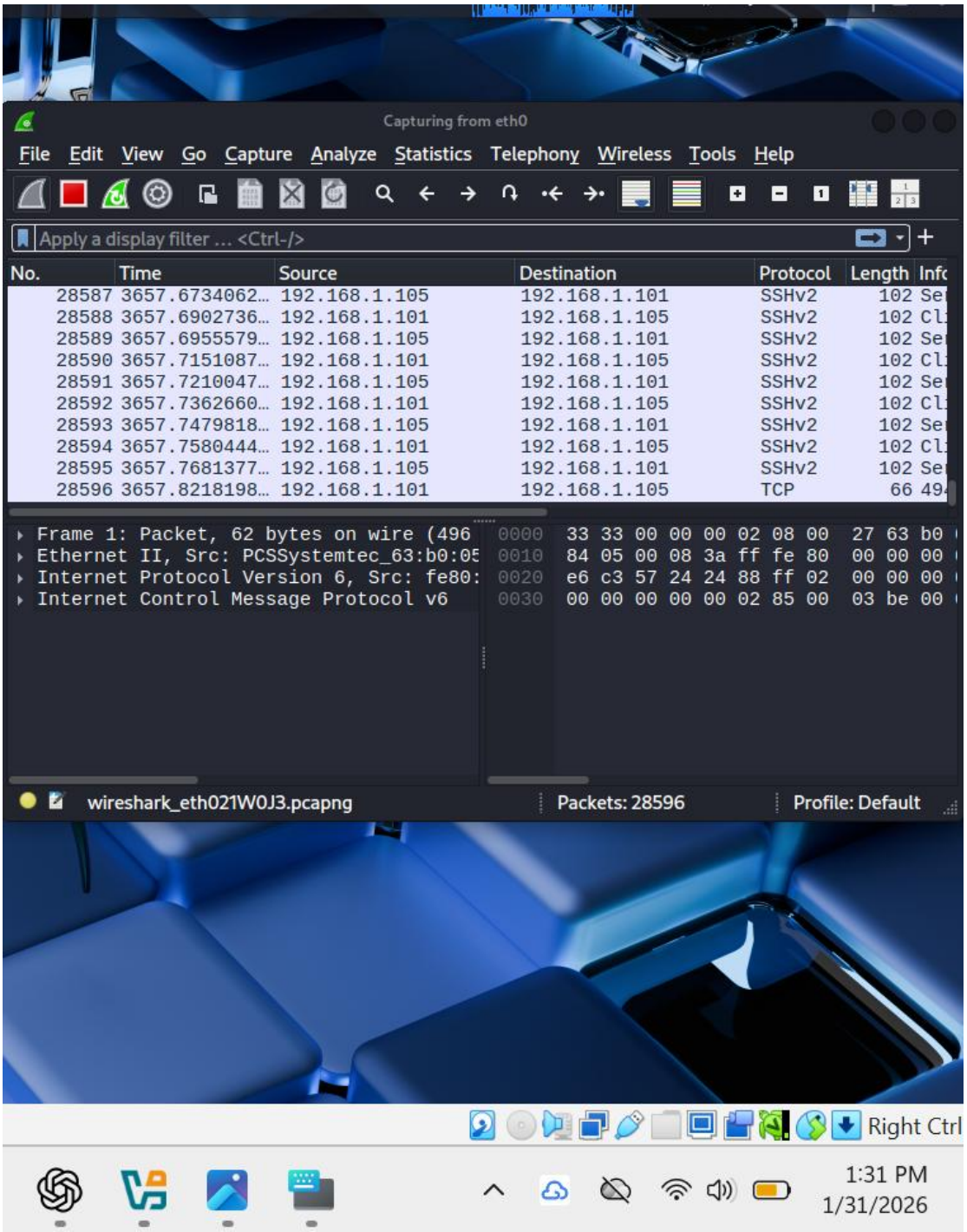
4.9 Real-time Wire-shark capture of Brute-force attack on SSH Port 22.

Evidence: Wireshark real-time capture

Severity Level:(12) Crictical

Classification: True Positive

Impact: Potential lateral movement



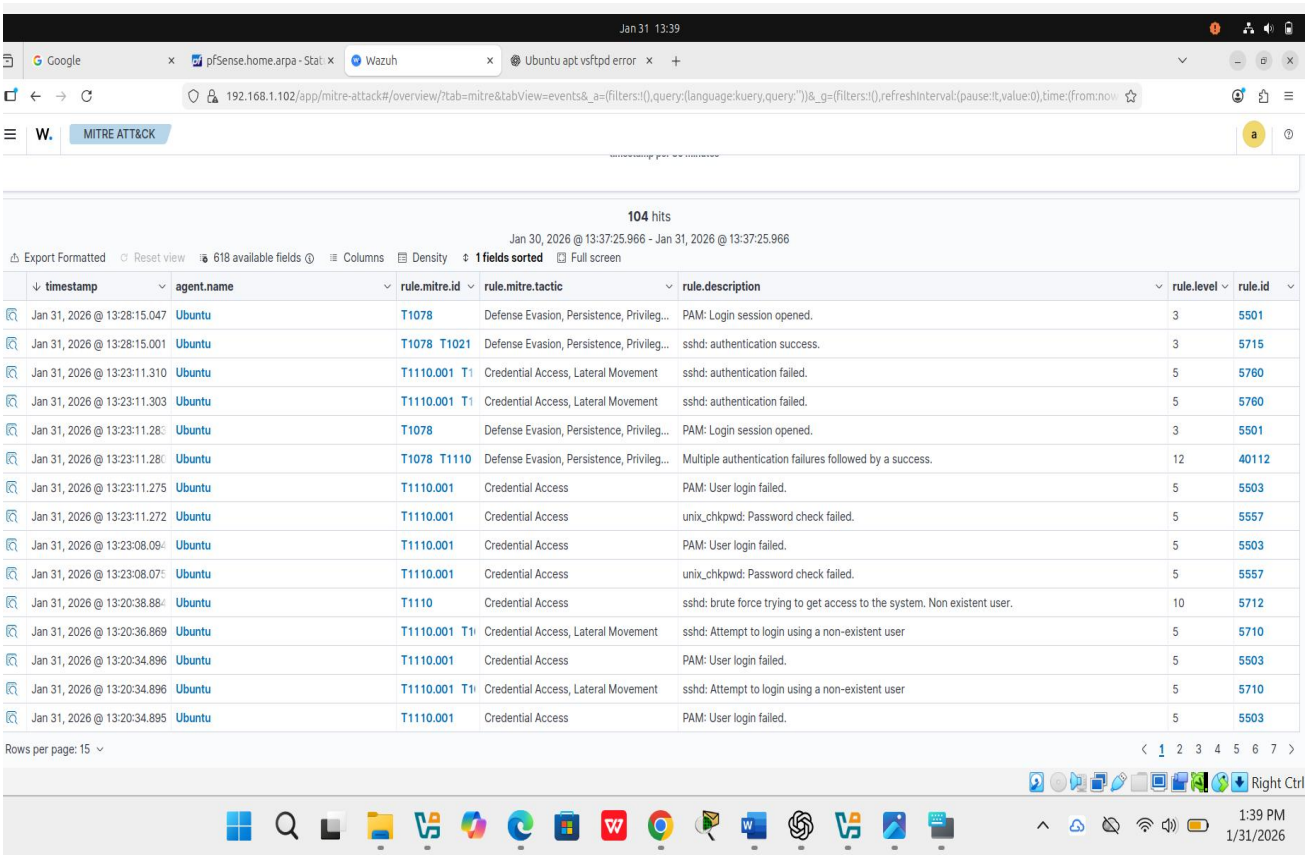
5.0 Brute-force and other forms of attack from an attacker.

Evidence: Wazuh logs showing series of attack including privilege escalation

Severity Level: (12) Crictical

Classification: True Positive

Impact: Potential lateral movement



5. 1 Remediation & Recommendations

Immediate Actions:

1. Immediate system isolation to counter SSH successful access and lateral movement, the system should be put on DMZ to stop the risk of a spread.
2. Disable or restrict FTP access; consider SFTP for secure file transfers.
3. Set up SSH Public/private key pair or create a STRONG login username and password.
4. Implement firewall rules to limit access to HTTP and FTP to trusted IPs.
5. Configure Snort rules to block suspicious traffic if required (IPS mode).

Long-term Improvements:

1. Enable SSL/TLS for web services to protect data in transit.
2. Harden Apache and vsftpd configurations (disable anonymous login, restrict directories)
3. Integrate regular vulnerability scanning and Wazuh alert tuning.

5.2 Conclusion

The lab exercise demonstrated the SOC's ability to detect and report network reconnaissance and web scanning activities. ICMP pings, open FTP/HTTP ports and web vulnerability scans were all captured and recorded, validating the effectiveness of the deployed security controls. Recommendations include hardening services, restricting access, and continuous monitoring