

# 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

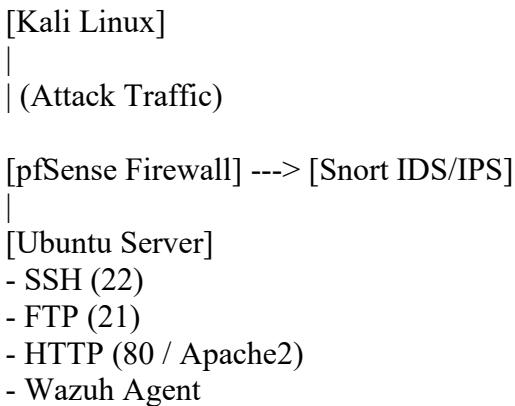
#### **Security Devices:**

pfSense Firewall

Snort IDS/IPS (custom rule)

Wazuh Agent (installed on Ubuntu)

## Monitoring Tool: Wireshark



### 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 critical 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: Critical

## 4. Detailed Technical Findings

### 4.1 ICMP Ping Detection

**Description:** ICMP echo requests sent from Attackr (Kali) to Ubuntu.

**Severity Level:** Low

**Classification:** False positive

The screenshot shows a web browser window titled 'Services / Snort / Alerts' on a pfSense system. A warning message at the top states: 'The password for this account is insecure. Password is currently set to the default value (pfsense). Change the password as soon as possible.' Below this, the 'Alerts' tab is selected in the navigation bar. The 'Alert Log View Settings' section shows 'WAN (em0)' as the interface to inspect, with an 'Auto-refresh view' checkbox and a 'Save' button. The 'Alert Log Actions' section includes 'Download' and 'Clear' buttons. The 'Alert Log View Filter' section has a '+' button. The main table displays 'Most Recent 250 Entries from Active Log' with columns: Date, Action, Pri, Proto, Class, Source IP, SPort, Destination IP, DPort, GID:SID, and Description. Three log entries are listed, all showing ICMP test traffic between LAN and WAN interfaces.

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2026-01-21 18:49:56	⚠️	0			fe80::2 Q +		fe80::a00:27ff:fea:8163 Q +		1:1000002 + ✘	ICMP Test Both LAN and WAN
2026-01-21 18:49:56	⚠️	0			fe80::a00:27ff:fea: 8163 Q +		fe80::2 Q +		1:1000002 + ✘	ICMP Test Both LAN and WAN
2026-01-21 18:49:56	⚠️	0	ICMP		10.0.2.2 Q +		10.0.2.15 Q +		1:1000002 + ✘	ICMP Test Both LAN and WAN

## 4.2 OPEN PORTS ON UBUTU VM (193.168.1.105)

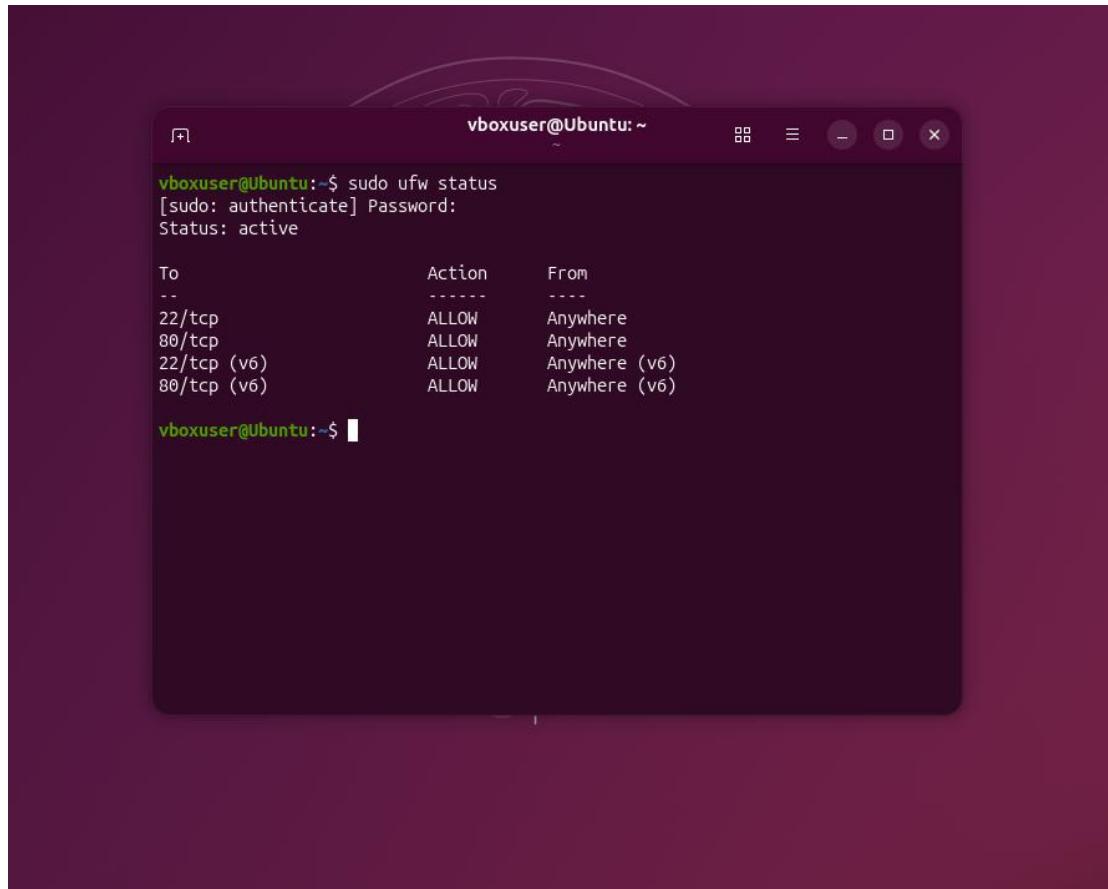
**21/FTP**

**22/SSH**

**80/HTTP**

**Status:** Service running, accessible from attacker VM.

**Evidence**



vboxuser@Ubuntu:~\$ sudo ufw status  
[sudo: authenticate] Password:  
Status: active

To	Action	From
--	-----	----
22/tcp	ALLOW	Anywhere
80/tcp	ALLOW	Anywhere
22/tcp (v6)	ALLOW	Anywhere (v6)
80/tcp (v6)	ALLOW	Anywhere (v6)

vboxuser@Ubuntu:~\$ █

#### 4.3. Description : Two (2) PAM login session from admin

**Evidence:** Wazuh alerts generated from admin login:

**Severity Level:** (3) Low

**Classification:** false Positive

The screenshot shows a Wazuh alert list with the following details:

**Timestamp:** Jan 30, 2026 @ 13:37:25.966 - Jan 31, 2026 @ 13:37:25.966

**Filter:** 104 hits

**Columns:** timestamp, agent.name, rule.mitre.id, rule.mitre.tactic, rule.description, rule.level, rule.id

**Data:** The table lists 104 alerts across various timestamps and agent names (Ubuntu). The alerts are categorized by rule ID and tactic. Key entries include:

- Jan 31, 2026 @ 13:28:15.047 Ubuntu: T1078 Defense Evasion, Persistence, Privileged... PAM: Login session opened.
- Jan 31, 2026 @ 13:28:15.001 Ubuntu: T1078 T1021 Defense Evasion, Persistence, Privileged... sshd: authentication success.
- Jan 31, 2026 @ 13:23:11.310 Ubuntu: T1110.001 T1 Credential Access, Lateral Movement sshd: authentication failed.
- Jan 31, 2026 @ 13:23:11.303 Ubuntu: T1110.001 T1 Credential Access, Lateral Movement sshd: authentication failed.
- Jan 31, 2026 @ 13:23:11.28 Ubuntu: T1078 Defense Evasion, Persistence, Privileged... PAM: Login session opened.
- Jan 31, 2026 @ 13:23:11.28 Ubuntu: T1078 T1110 Defense Evasion, Persistence, Privileged... Multiple authentication failures followed by a success.
- Jan 31, 2026 @ 13:23:11.275 Ubuntu: T1110.001 Credential Access PAM: User login failed.
- Jan 31, 2026 @ 13:23:11.272 Ubuntu: T1110.001 Credential Access unix\_chkpwd: Password check failed.
- Jan 31, 2026 @ 13:23:08.09- Ubuntu: T1110.001 Credential Access PAM: User login failed.
- Jan 31, 2026 @ 13:23:08.07- Ubuntu: T1110.001 Credential Access unix\_chkpwd: Password check failed.
- Jan 31, 2026 @ 13:20:38.88- Ubuntu: T1110 Credential Access sshd: brute force trying to get access to the system. Non-existent user.
- Jan 31, 2026 @ 13:20:36.869 Ubuntu: T1110.001 T1 Credential Access, Lateral Movement sshd: Attempt to login using a non-existent user
- Jan 31, 2026 @ 13:20:34.896 Ubuntu: T1110.001 Credential Access PAM: User login failed.
- Jan 31, 2026 @ 13:20:34.896 Ubuntu: T1110.001 T1 Credential Access, Lateral Movement sshd: Attempt to login using a non-existent user
- Jan 31, 2026 @ 13:20:34.895 Ubuntu: T1110.001 Credential Access PAM: User login failed.

**Bottom of the window:**

- Rows per page: 15
- Navigation icons: back, forward, search, etc.
- Date and time: 1/31/2026, 1:39 PM
- System tray icons: battery, signal, etc.

## 4.4 Reconnaissance activities.

**Evidence:** Wazuh alerts generated from numerous web vulnerability scans:

**Severity Level:** High

**Classification:** True Positive

**Impact:** Risk of unauthorized access.

The screenshot displays a web-based interface for monitoring security alerts. At the top, there are several tabs: 'Google', 'pfSense.home.arpn - Stat', 'Wazuh', and 'Ubuntu apt vsftpd error'. The main content area shows a table of alerts with the following data:

1,746 hits						
Jan 30, 2026 @ 14:36:56.914 - Jan 31, 2026 @ 14:36:56.916						
Export	Formatted	Reset view	619 available fields	Columns	Density	1 fields sorted
🕒	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

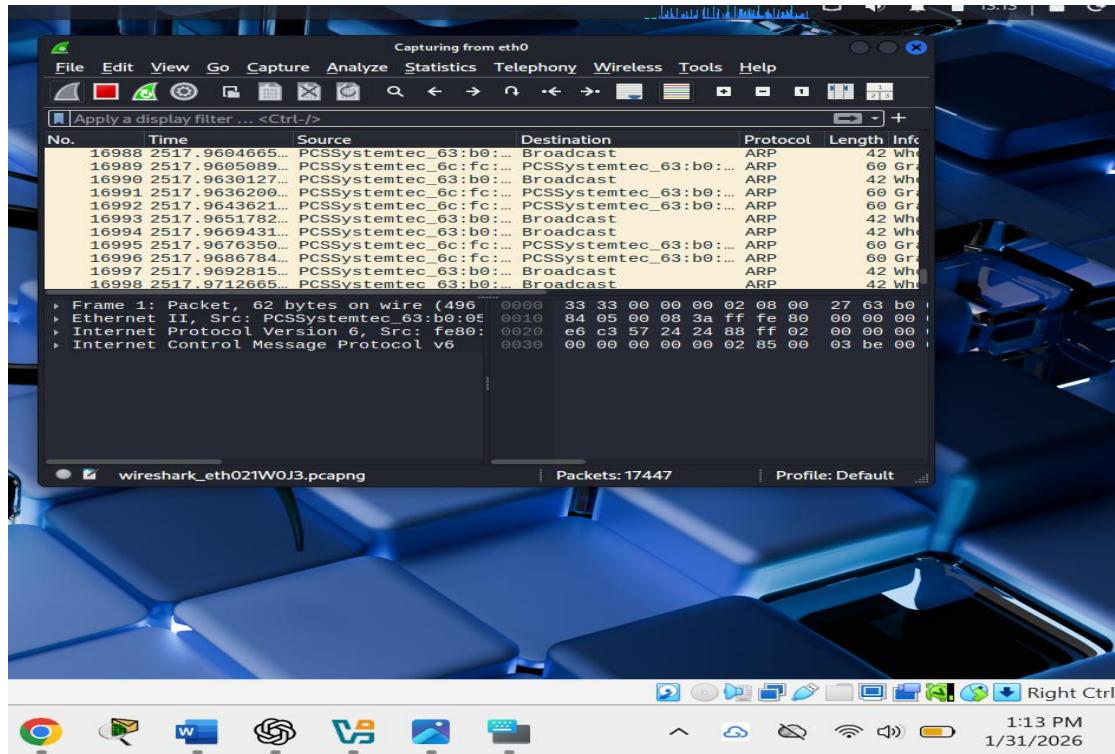
**Description:** Port scanning from Kali to Ubuntu VM to identify open services.

**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**

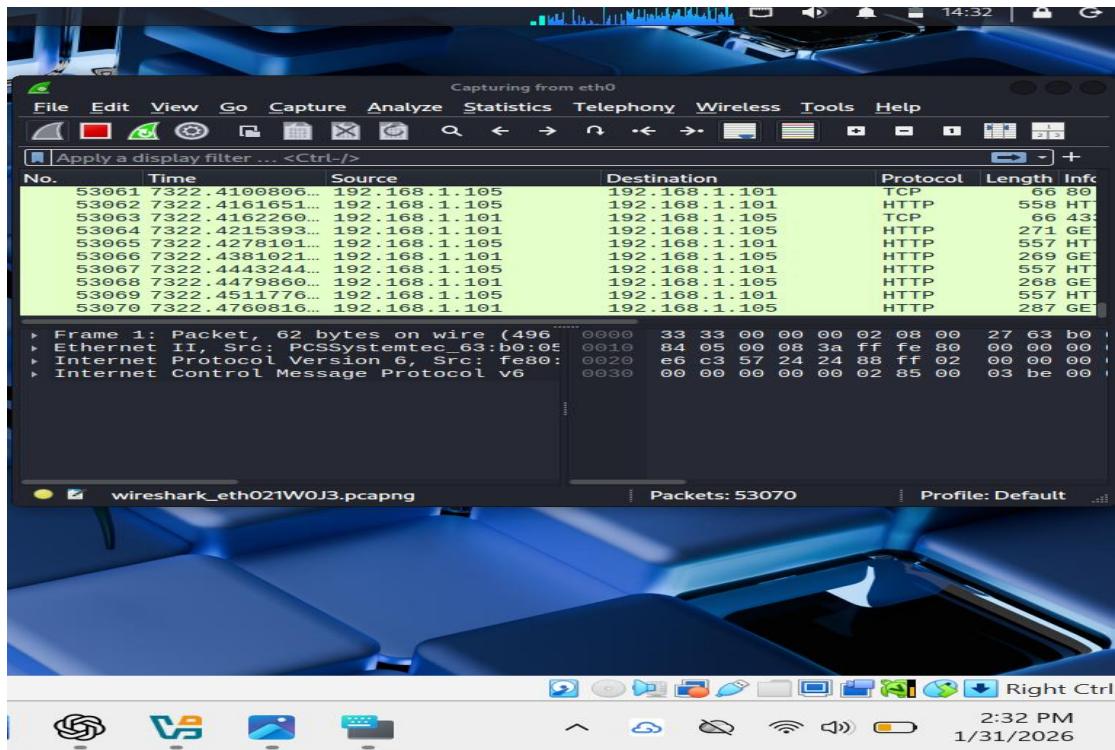
The password for this account is insecure. Password is currently set to the default value (pfSense).  
Change the password as soon as possible.

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2026-01-31 17:03:45	▲	1	TCP	Web Application Attack	192.168.1.101	41402	192.168.1.105	80	1:2016184	ET WEB_SERVER ColdFusion administrator access
2026-01-31 17:03:33	▲	1	TCP	Attempted Administrator Privilege Gain	192.168.1.101	45982	192.168.1.105	80	1:2022028	ET WEB_SERVER Possible CVE-2014-6271 Attempt
2026-01-31 17:03:33	▲	1	TCP	Attempted Administrator Privilege Gain	192.168.1.101	45982	192.168.1.105	80	1:2022028	ET WEB_SERVER Possible CVE-2014-6271 Attempt
2026-01-31 17:03:33	▲	1	TCP	Attempted Administrator Privilege Gain	192.168.1.101	45982	192.168.1.105	80	1:2022028	ET WEB_SERVER Possible CVE-2014-6271 Attempt

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

Severity Level:(10) High

Evidence:



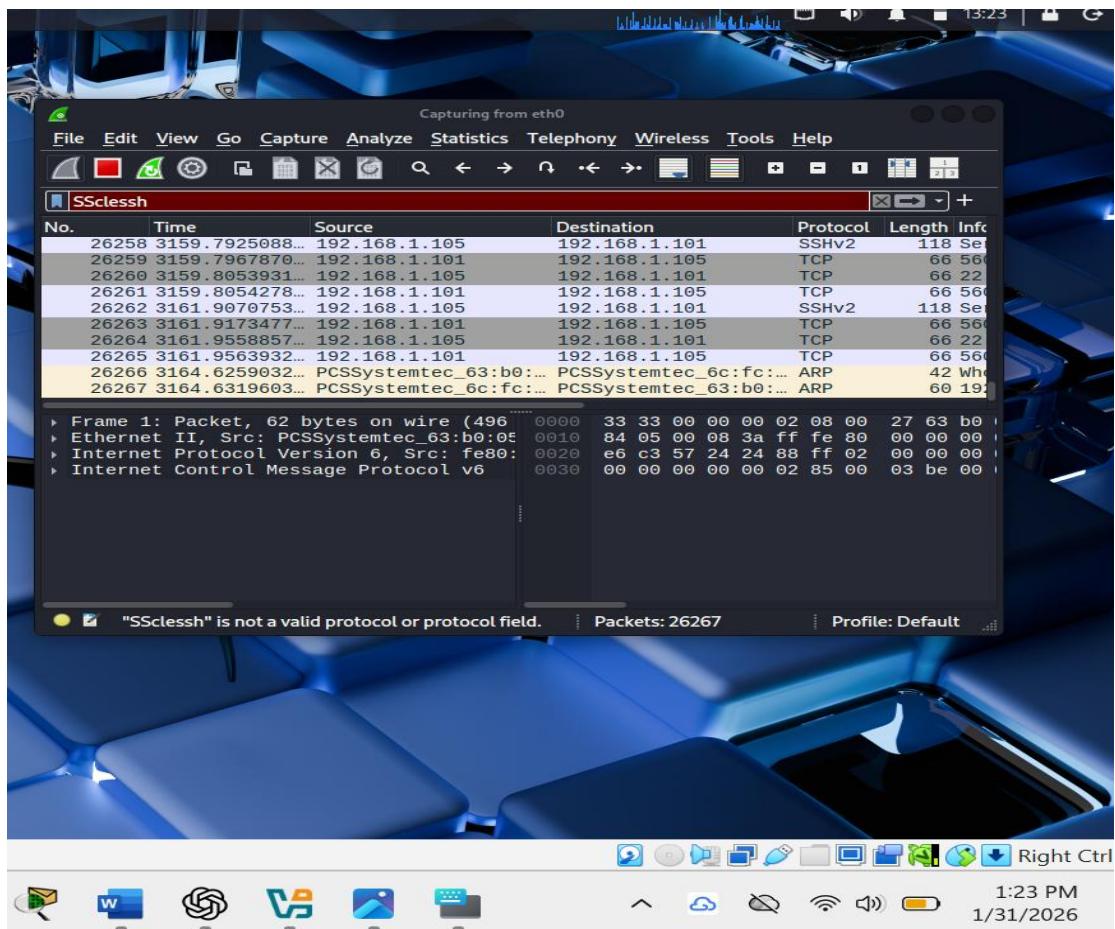
## 4.8 Nmap scan for open ports on Ubuntu VM

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) Critical

**Classification:** True Positive

**Impact:** Potential lateral movement

The screenshot shows the Wireshark interface capturing traffic from the eth0 interface. The packet list pane displays a series of SSHv2 and TCP packets between source IP 192.168.1.105 and destination IP 192.168.1.101. The details pane shows the structure of a selected packet, which is a Frame 1: Packet, 62 bytes on wire (496 bits), starting at offset 0000. The bytes pane shows the raw hex and ASCII data for the selected packet. The bottom status bar indicates the file is named 'wireshark\_eth021W0J3.pcapng', there are 28596 packets, and the profile is 'Default'. The system tray at the bottom right shows the date and time as 1:31 PM on 1/31/2026.

No.	Time	Source	Destination	Protocol	Length	Info
28587	3657.6734062...	192.168.1.105	192.168.1.101	SSHv2	102	Set
28588	3657.6902736...	192.168.1.101	192.168.1.105	SSHv2	102	Cli
28589	3657.6955579...	192.168.1.105	192.168.1.101	SSHv2	102	Set
28590	3657.7151087...	192.168.1.101	192.168.1.105	SSHv2	102	Cli
28591	3657.7210047...	192.168.1.105	192.168.1.101	SSHv2	102	Set
28592	3657.7362660...	192.168.1.101	192.168.1.105	SSHv2	102	Cli
28593	3657.7479818...	192.168.1.105	192.168.1.101	SSHv2	102	Set
28594	3657.7580444...	192.168.1.101	192.168.1.105	SSHv2	102	Cli
28595	3657.7681377...	192.168.1.105	192.168.1.101	SSHv2	102	Set
28596	3657.8218198...	192.168.1.101	192.168.1.105	TCP	66	49

## 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) Critical**

**Classification: True Positive**

**Impact: Potential lateral movement**

104 hits						
Jan 30, 2026 @ 13:37:25.966 - Jan 31, 2026 @ 13:37:25.966						
Export	Formatted	Reset view	618 available fields	Columns	Density	1 fields sorted
↓	timestamp	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level rule.id
	Jan 31, 2026 @ 13:28:15.047	Ubuntu	T1078	Defense Evasion, Persistence, Privileg...	PAM: Login session opened.	3 5501
	Jan 31, 2026 @ 13:28:15.001	Ubuntu	T1078 T1021	Defense Evasion, Persistence, Privileg...	sshd: authentication success.	3 5715
	Jan 31, 2026 @ 13:23:11.310	Ubuntu	T1110.001 T1	Credential Access, Lateral Movement	sshd: authentication failed.	5 5760
	Jan 31, 2026 @ 13:23:11.303	Ubuntu	T1110.001 T1	Credential Access, Lateral Movement	sshd: authentication failed.	5 5760
	Jan 31, 2026 @ 13:23:11.283	Ubuntu	T1078	Defense Evasion, Persistence, Privileg...	PAM: Login session opened.	3 5501
	Jan 31, 2026 @ 13:23:11.280	Ubuntu	T1078 T1110	Defense Evasion, Persistence, Privileg...	Multiple authentication failures followed by a success.	12 40112
	Jan 31, 2026 @ 13:23:11.275	Ubuntu	T1110.001	Credential Access	PAM: User login failed.	5 5503
	Jan 31, 2026 @ 13:23:11.272	Ubuntu	T1110.001	Credential Access	unix_chkpwd: Password check failed.	5 5557
	Jan 31, 2026 @ 13:23:08.094	Ubuntu	T1110.001	Credential Access	PAM: User login failed.	5 5503
	Jan 31, 2026 @ 13:23:08.075	Ubuntu	T1110.001	Credential Access	unix_chkpwd: Password check failed.	5 5557
	Jan 31, 2026 @ 13:20:38.884	Ubuntu	T1110	Credential Access	sshd: brute force trying to get access to the system. Non existent user.	10 5712
	Jan 31, 2026 @ 13:20:36.869	Ubuntu	T1110.001 T1	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5 5710
	Jan 31, 2026 @ 13:20:34.896	Ubuntu	T1110.001	Credential Access	PAM: User login failed.	5 5503
	Jan 31, 2026 @ 13:20:34.896	Ubuntu	T1110.001 T1	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5 5710
	Jan 31, 2026 @ 13:20:34.895	Ubuntu	T1110.001	Credential Access	PAM: User login failed.	5 5503

## 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