CAPSTONE CASE STUDY- PROSPERITY BANK BREACH INVESTIGATION

BY

STANLEY EKECHUKWU

SOC Incident Report

Organisation: Prosperity Bank

Prepared by: Stanley Ekechukwu

Date: 5th September, 2025.

Executive Summary

On 01/09/2025, the Security Operations Centre detected suspicious activities across multiple devices and networks at Prosperity Bank.

A Windows 10 workstation recorded repeated failed login attempts, including a possible brute-force attack.

An Ubuntu server showed attempts at privilege escalation, unauthorised access to protected files, and the creation of a suspicious user account.

Network reconnaissance was observed, which suggests possible lateral movements by the threat actor.

These incidents could lead to insider threat, lateral movement by an attacker across multiple systems, identity theft, credential compromise, data theft, denial of service, financial loss and reputational damage if left unattended.

Mitigation measures, including pfSense VLAN segmentation with access control lists, strict firewall rules, effective monitoring policies, and trainings have been recommended to strengthen Prosperity Bank's security posture.

INCIDENT OVERVIEW

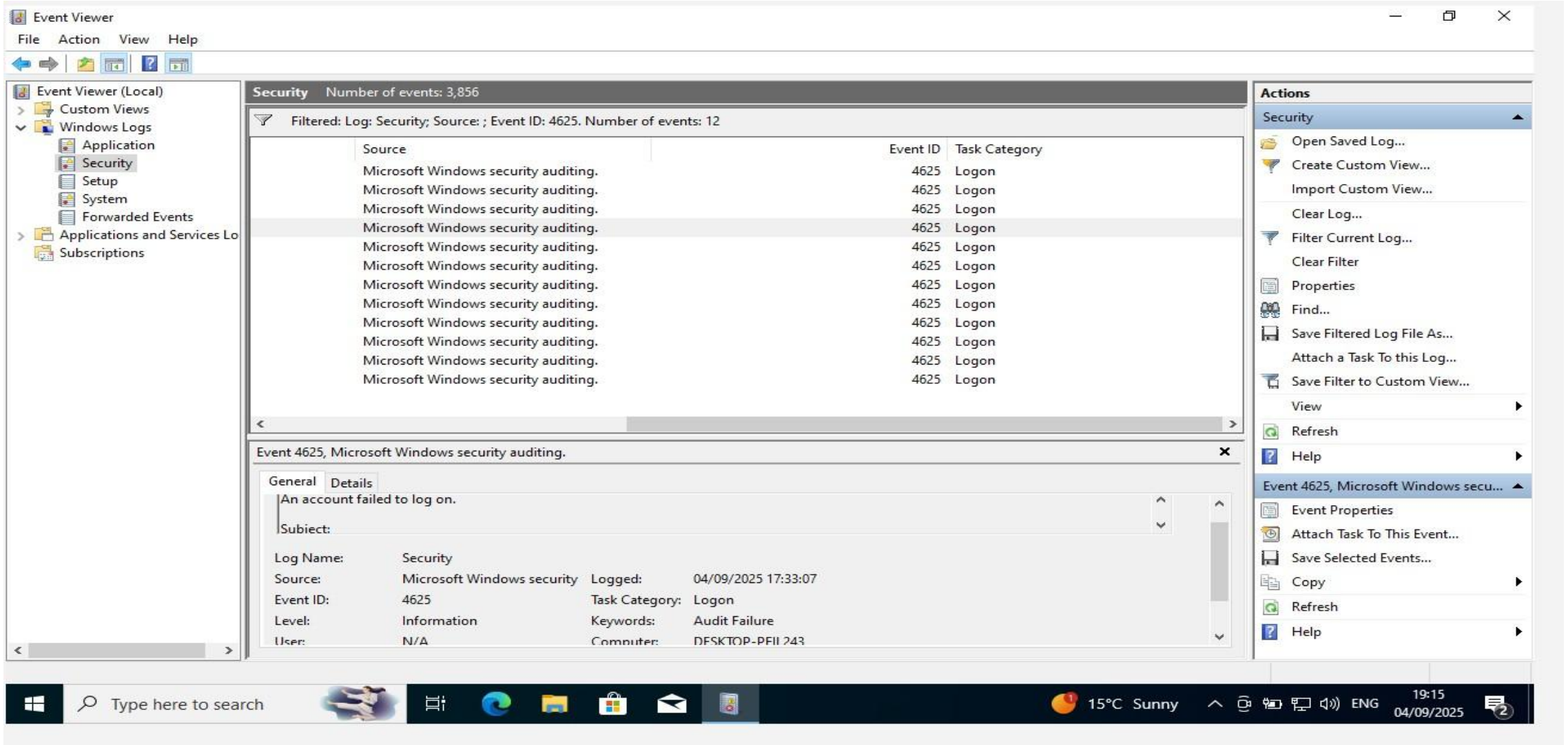
INCIDENT TYPE: UNAUTHORISED LOGIN ATTEMPTS, PRIVILEGE ESCALATION, RECONNAISSANCE

SEVERITY LEVEL: HIGH

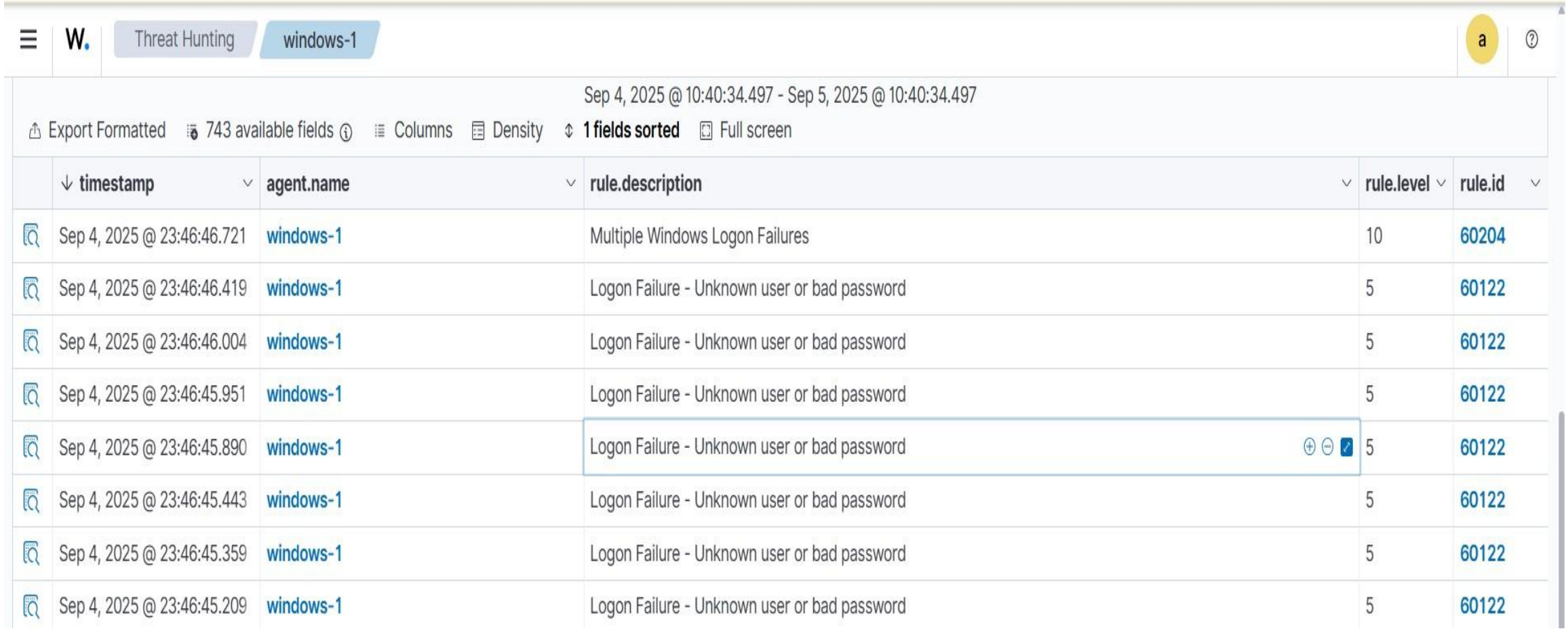
AFFECTED SYSTEMS:

- WINDOWS 10 WORKSTATION (EMPLOYEE ENDPOINT)
- UBUNTU SERVER (BACKEND SYSTEM)

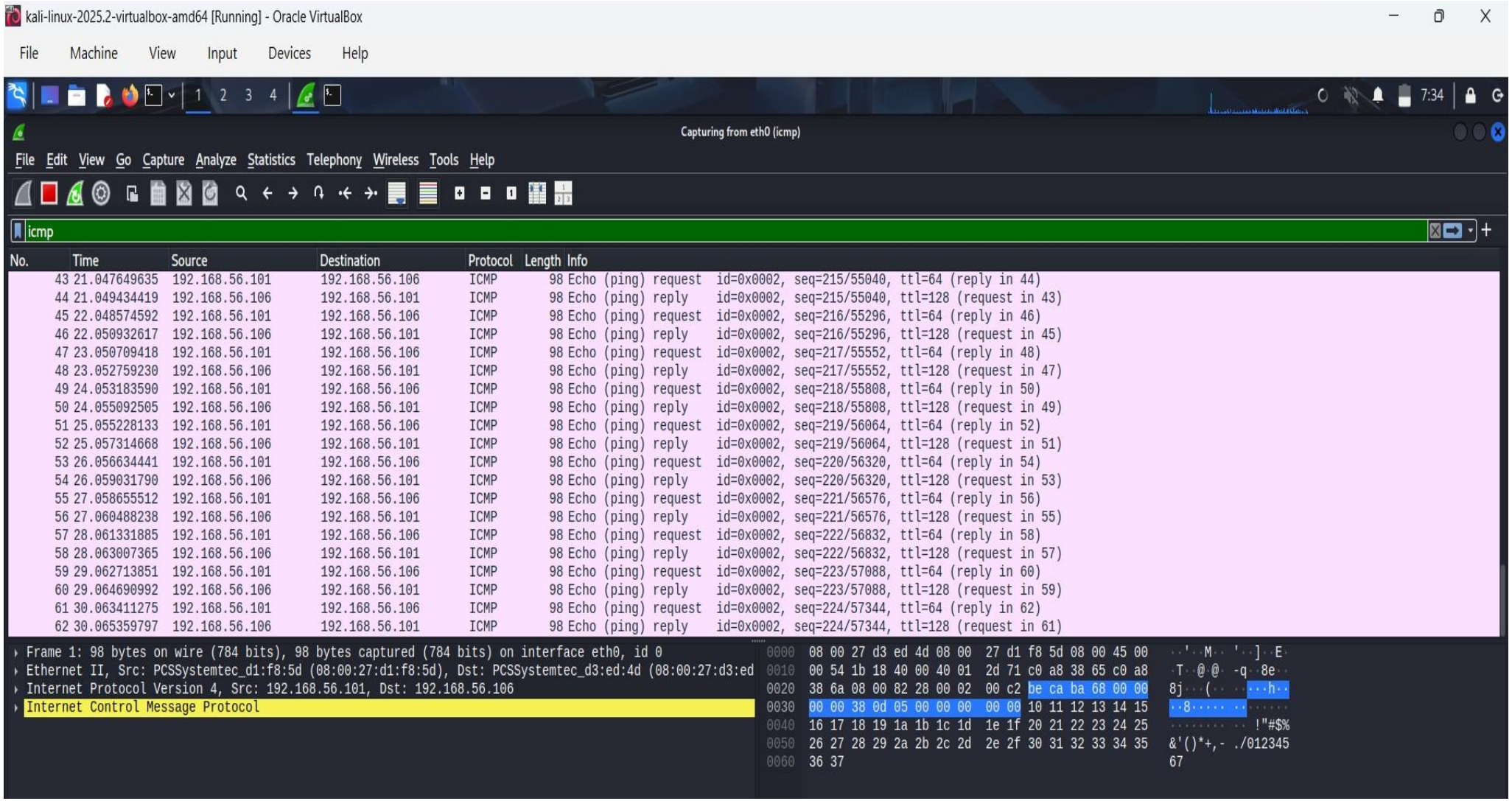
Win10 Failed Login Attempts-Event Viewer Logs



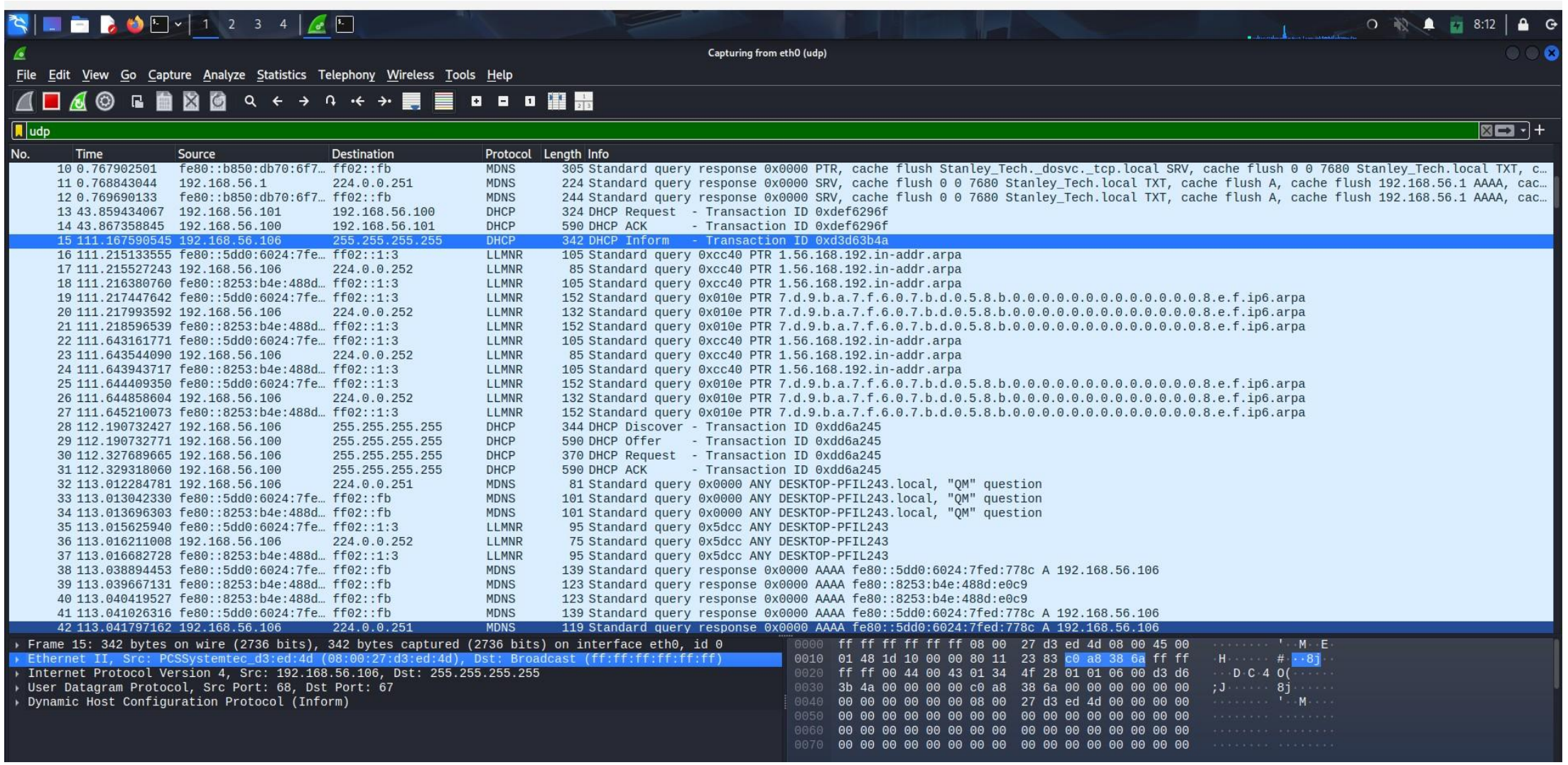
Win10 Failed Login Attempts-Wazuh Capture



Win10 Network Scan-Wireshark Capture



Win10 Port Scan-Wireshark Capture



Ubuntu Privilege Escalation-Wazuh Capture

>	Sep 4, 2025 @ 23:40:09.195	001	ubuntu-1	PAM: Login session opened.	5501	3
>	Sep 4, 2025 @ 23:40:09.190	001	ubuntu-1	Successful sudo to ROOT executed.	5402	3
>	Sep 4, 2025 @ 23:40:09.129	001	ubuntu-1	PAM: Login session opened.	5501	3
>	Sep 4, 2025 @ 23:40:09.124	001	ubuntu-1	Successful sudo to ROOT executed.	5402	3
>	Sep 4, 2025 @ 23:40:08.581	001	ubuntu-1	PAM: Login session closed.	5502	3
>	Sep 4, 2025 @ 23:40:08.568	001	ubuntu-1	PAM: Login session opened.	5501	3
>	Sep 4, 2025 @ 23:40:08.564	001	ubuntu-1	Successful sudo to ROOT executed.	5402	3

Ubuntu Privilege Escalation-Wazuh Capture2

t	rule.groups	pam, syslog, authentication_success
t	rule.hipaa	164.312.b
t	rule.id	5501
#	rule.level	3
◔	rule.mail	false
t	rule.mitre.id	T1078
t	rule.mitre.tactic	Defense Evasion, Persistence, Privilege Escalation, Initial Access
t	rule.mitre.technique	Valid Accounts

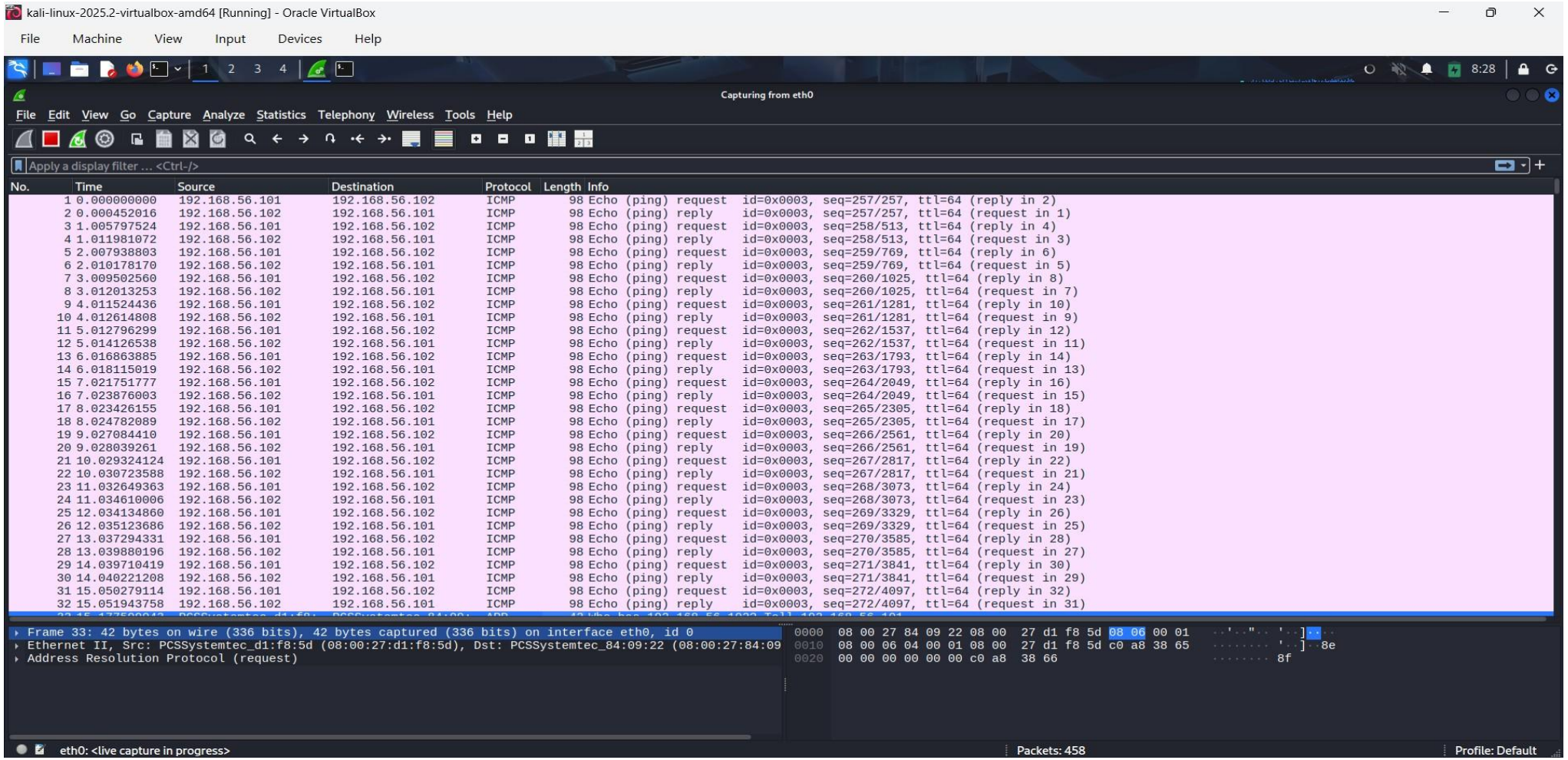
Ubuntu Unauthorised File Access- Wazuh Capture

t	data.audit.type	AVC
t	decoder.name	auditd
t	full_log	type=AVC msg=audit(1757026808.652:472): apparmor="DENIED" operation="capable" class="cap" profile="/usr/sbin/cupsd" pid =6212 comm="cupsd" capability=12 capname="net_admin"
t	id	1757026809.1685898
t	input.type	log
t	location	/var/log/audit/audit.log
t	manager.name	wazuh-server

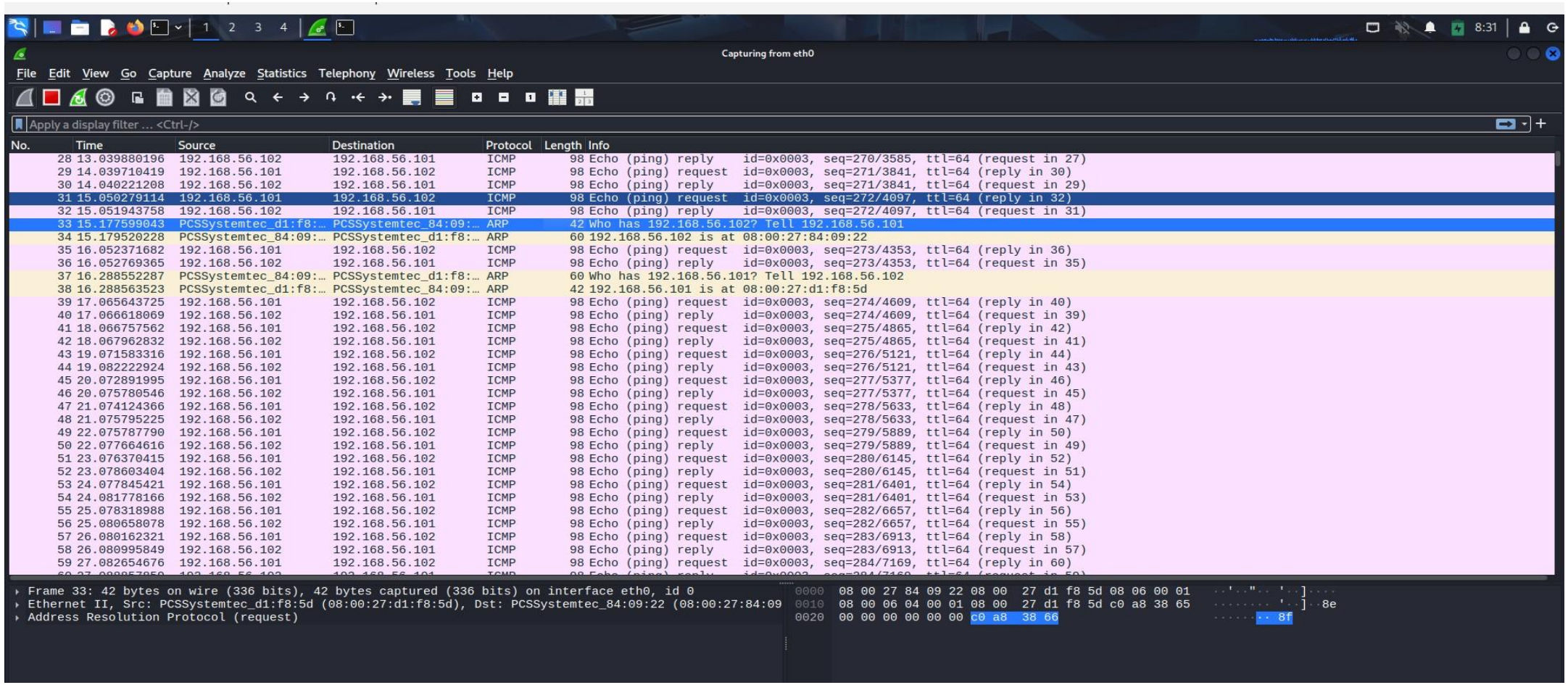
Ubuntu Suspicious User Addition-Wazuh Capture

›	Sep 4, 2025 @ 23:40:09.706	001	ubuntu-1	New user added to the system.	5902	8
›	Sep 4, 2025 @ 23:40:09.699	001	ubuntu-1	New group added to the system.	5901	8

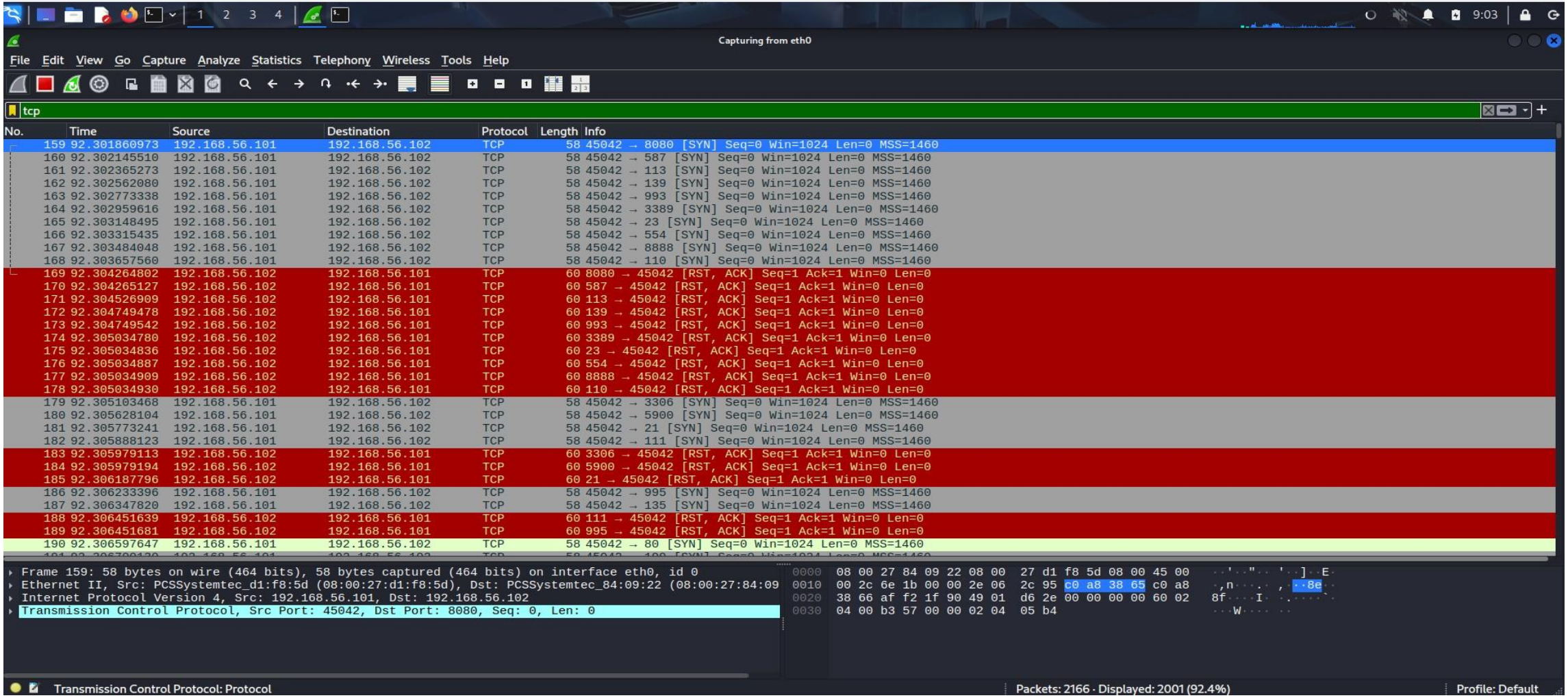
Ubuntu Network Scan-Wireshark Capture



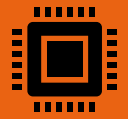
Ubuntu Network Scan-Wireshark Capture2



Ubuntu Port Scan-Wireshark Capture



Investigation Analysis



Multiple failed login attempts on Windows 10 workstation as captured by Windows event viewer and Wazuh indicates potential brute-force attack leading to data theft, identity theft, and other attacks.

Privilege escalation attempts, unauthorised file access, and suspicious user creation on Ubuntu server as captured by Wazuh indicates a possible insider attack or an external cyber criminal trying to gain initial foothold and remain undetected to launch major attacks in future.

ICMP and TCP traffic between attacker and target systems, as captured by Wireshark simply suggests preparation for lateral movement across networks, devices, and various departments to launch attacks.

ROOT CAUSE ANALYSIS

- Poor network segmentation enabled the attacker to communicate with workstations and servers across the network
- Weak endpoint (workstations and servers) security configurations enabled the attacker to gain root/privilege access in the first place that further enabled access to confidential data and creating a new user.
- Poor access controls may have enabled a malicious employee within the organisation to perform such activities.
- Lack of awareness/training could have made an unsuspecting employer to click a phishing link or reveal login details without knowing.
- Poor security culture/policies such as password policies could have led to this security breach.

Recommendations

Endpoint Security Configurations:

- Enforce account lockout after 4 failed login attempts
- Enable Multi-Factor authentication (MFA) for all employees
- Restrict sudo/privilege access to essential administrators only
- Enforce least privilege access across all devices and systems

Network Security:

- Implement proper network segmentation by separating various departments such as employee and backend server
- Configure strict firewall rules that block unauthorised inter-vlan traffic
- Allow only SOC/admin access where required

Awareness and Policies:

- Conduct regular security awareness and attack simulations such as phishing and password hygiene
- Implement healthy security policies across the organisation such as routine password change and use of strong passwords

CONCLUSION

The security breach at Prosperity Bank highlights the severe risks posed by brute-force attacks, privilege escalation, and network reconnaissance.

These risks can be mitigated by implementing active monitoring using SIEM tools, endpoint configuration, proper network segmentation, stricter access controls, and employee training among others. These measures will reduce the risk of lateral movement, unauthorised access, and insider threats.

An efficient and effective security culture and posture can mitigate reputational damage, unauthorised data access/theft, data manipulation, and possible denial of service, thereby upholding a healthy CIA Triad – Confidentiality, Integrity, and Availability.