

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

The screenshot shows the Windows Event Viewer interface. The left pane displays a navigation tree with 'Event Viewer (Local)', 'Custom Views', 'Windows Logs' (selected), and 'Applications and Services Log'. Under 'Windows Logs', 'Security' is selected. The main pane shows a table of events for 'Log: Security; Source: ; Event ID: 4625. Number of events: 12'. The table has columns for 'Source', 'Event ID', and 'Task Category'. All 12 events are listed with 'Source' as 'Microsoft Windows security auditing.', 'Event ID' as '4625', and 'Task Category' as 'Logon'. Below the table, a specific event is expanded: 'Event 4625, Microsoft Windows security auditing.' The 'Details' tab is active, showing the message 'An account failed to log on.' and various properties: Log Name: Security, Source: Microsoft Windows security, Event ID: 4625, Level: Information, User: N/A, Logged: 04/09/2025 17:33:07, Task Category: Logon, Keywords: Audit Failure, Computer: DESKTOP-PFII 243. The right pane contains an 'Actions' menu with options like 'Open Saved Log...', 'Create Custom View...', 'Import Custom View...', 'Clear Log...', 'Filter Current Log...', 'Properties', 'Find...', 'Save Filtered Log File As...', 'Attach a Task To this Log...', 'Save Filter to Custom View...', 'View', 'Refresh', 'Help', 'Event Properties', 'Attach Task To This Event...', 'Save Selected Events...', 'Copy', 'Refresh', and 'Help'. The taskbar at the bottom includes icons for Start, Search, File Explorer, Edge, File Manager, Mail, and Task View, along with system status indicators for battery, signal, and network.

Event Viewer

File Action View Help

Event Viewer (Local) Custom Views Windows Logs Applications and Services Log Subscriptions

Security Number of events: 3,856

Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 12

Source	Event ID	Task Category
Microsoft Windows security auditing.	4625	Logon
Microsoft Windows security auditing.	4625	Logon
Microsoft Windows security auditing.	4625	Logon
Microsoft Windows security auditing.	4625	Logon
Microsoft Windows security auditing.	4625	Logon
Microsoft Windows security auditing.	4625	Logon
Microsoft Windows security auditing.	4625	Logon
Microsoft Windows security auditing.	4625	Logon
Microsoft Windows security auditing.	4625	Logon
Microsoft Windows security auditing.	4625	Logon
Microsoft Windows security auditing.	4625	Logon
Microsoft Windows security auditing.	4625	Logon

Event 4625, Microsoft Windows security auditing.

General Details

An account failed to log on.

Subject:

Log Name: Security

Source: Microsoft Windows security

Event ID: 4625

Level: Information

User: N/A

Logged: 04/09/2025 17:33:07

Task Category: Logon

Keywords: Audit Failure

Computer: DESKTOP-PFII 243

Actions

Security

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Clear Filter
- Properties
- Find...
- Save Filtered Log File As...
- Attach a Task To this Log...
- Save Filter to Custom View...
- View
- Refresh
- Help

Event 4625, Microsoft Windows secu...

- Event Properties
- Attach Task To This Event...
- Save Selected Events...
- Copy
- Refresh
- Help

Type here to search

15°C Sunny ENG 04/09/2025 19:15

Win10 Failed Login Attempts-Wazuh Capture

The screenshot shows a Wazuh Threat Hunting interface with the following details:

- Filter: windows-1
- Date Range: Sep 4, 2025 @ 10:40:34.497 - Sep 5, 2025 @ 10:40:34.497
- Export Formatted
- 743 available fields
- Columns: timestamp, agent.name, rule.description, rule.level, rule.id
- Density: 1 fields sorted
- Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Sep 4, 2025 @ 23:46:46.721	windows-1	Multiple Windows Logon Failures	10	60204
Sep 4, 2025 @ 23:46:46.419	windows-1	Logon Failure - Unknown user or bad password	5	60122
Sep 4, 2025 @ 23:46:46.004	windows-1	Logon Failure - Unknown user or bad password	5	60122
Sep 4, 2025 @ 23:46:45.951	windows-1	Logon Failure - Unknown user or bad password	5	60122
Sep 4, 2025 @ 23:46:45.890	windows-1	Logon Failure - Unknown user or bad password	5	60122
Sep 4, 2025 @ 23:46:45.443	windows-1	Logon Failure - Unknown user or bad password	5	60122
Sep 4, 2025 @ 23:46:45.359	windows-1	Logon Failure - Unknown user or bad password	5	60122
Sep 4, 2025 @ 23:46:45.209	windows-1	Logon Failure - Unknown user or bad password	5	60122

Win10 Network Scan-Wireshark Capture

kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Capturing from eth0 (icmp)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
43	21.047649635	192.168.56.101	192.168.56.106	ICMP	98	Echo (ping) request id=0x0002, seq=215/55040, ttl=64 (reply in 44)
44	21.049434419	192.168.56.106	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0002, seq=215/55040, ttl=128 (request in 43)
45	22.048574592	192.168.56.101	192.168.56.106	ICMP	98	Echo (ping) request id=0x0002, seq=216/55296, ttl=64 (reply in 46)
46	22.050932617	192.168.56.106	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0002, seq=216/55296, ttl=128 (request in 45)
47	23.050709418	192.168.56.101	192.168.56.106	ICMP	98	Echo (ping) request id=0x0002, seq=217/55552, ttl=64 (reply in 48)
48	23.052759230	192.168.56.106	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0002, seq=217/55552, ttl=128 (request in 47)
49	24.053183590	192.168.56.101	192.168.56.106	ICMP	98	Echo (ping) request id=0x0002, seq=218/55808, ttl=64 (reply in 50)
50	24.055092505	192.168.56.106	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0002, seq=218/55808, ttl=128 (request in 49)
51	25.055228133	192.168.56.101	192.168.56.106	ICMP	98	Echo (ping) request id=0x0002, seq=219/56064, ttl=64 (reply in 52)
52	25.057314668	192.168.56.106	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0002, seq=219/56064, ttl=128 (request in 51)
53	26.056634441	192.168.56.101	192.168.56.106	ICMP	98	Echo (ping) request id=0x0002, seq=220/56320, ttl=64 (reply in 54)
54	26.059031790	192.168.56.106	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0002, seq=220/56320, ttl=128 (request in 53)
55	27.058655512	192.168.56.101	192.168.56.106	ICMP	98	Echo (ping) request id=0x0002, seq=221/56576, ttl=64 (reply in 56)
56	27.060488238	192.168.56.106	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0002, seq=221/56576, ttl=128 (request in 55)
57	28.061331885	192.168.56.101	192.168.56.106	ICMP	98	Echo (ping) request id=0x0002, seq=222/56832, ttl=64 (reply in 58)
58	28.063007365	192.168.56.106	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0002, seq=222/56832, ttl=128 (request in 57)
59	29.062713851	192.168.56.101	192.168.56.106	ICMP	98	Echo (ping) request id=0x0002, seq=223/57088, ttl=64 (reply in 60)
60	29.064690992	192.168.56.106	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0002, seq=223/57088, ttl=128 (request in 59)
61	30.063411275	192.168.56.101	192.168.56.106	ICMP	98	Echo (ping) request id=0x0002, seq=224/57344, ttl=64 (reply in 62)
62	30.065359797	192.168.56.106	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0002, seq=224/57344, ttl=128 (request in 61)

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: PCSSystemtec_d3:ed:4d (08:00:27:d3:ed:
Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.106
Internet Control Message Protocol

Hex	Dec	Text
0000	08 00 27 d3 ed 4d 08 00	27 d1 f8 5d 08 00 45 00
0010	00 54 1b 18 40 00 40 01	2d 71 c0 a8 38 65 c0 a8
0020	38 6a 08 00 82 28 00 02	00 c2 be ca ba 68 00 00
0030	00 00 38 0d 05 00 00 00	00 00 10 11 12 13 14 15
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35
0060	36 37	67

Win10 Port Scan-Wireshark Capture

The screenshot shows a Wireshark capture of a port scan from a Windows 10 host. The interface is set to `eth0 (udp)`. The packet list pane displays a sequence of network frames, primarily DNS (MDNS) and DHCP traffic, indicating a broadcast scan of ports 1-1024. The details pane shows the protocol headers and payload for selected frames, while the bytes pane shows the raw hex and ASCII data.

Key observations from the packet list:

- Frames 10-14 show a series of DNS responses from `fe80::b850:db70:6f7...` to various destinations, including `224.0.0.251`, `192.168.56.106`, and `192.168.56.101`.
- Frame 15 is a `DHCP Inform` frame from `192.168.56.106` to `255.255.255.255`, with Transaction ID `0xd3d63b4a`.
- Frames 16-21 show a series of LLMNR queries from `fe80::5dd0:6024:7fe...` to `224.0.0.252`.
- Frames 22-27 show a series of LLMNR queries from `fe80::5dd0:6024:7fe...` to `224.0.0.252`.
- Frames 28-31 show a sequence of DHCP frames: Discover, Offer, Request, and ACK, all from `192.168.56.106` to `255.255.255.255`.
- Frames 32-35 show a series of DNS queries from `fe80::5dd0:6024:7fe...` to `224.0.0.251`, asking for "QM" records.
- Frames 36-39 show a series of DNS responses from `fe80::5dd0:6024:7fe...` to `224.0.0.251`, containing AAAA records for `192.168.56.106`.
- Frames 40-41 show DNS responses from `fe80::5dd0:6024:7fe...` to `224.0.0.251`, containing AAAA records for `192.168.56.106`.
- Frame 42 is a DNS response from `192.168.56.106` to `224.0.0.251` with Transaction ID `0x041797162`.

The details and bytes panes at the bottom provide a detailed view of the selected frame's structure, including its header fields and the raw data payload.

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
o 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

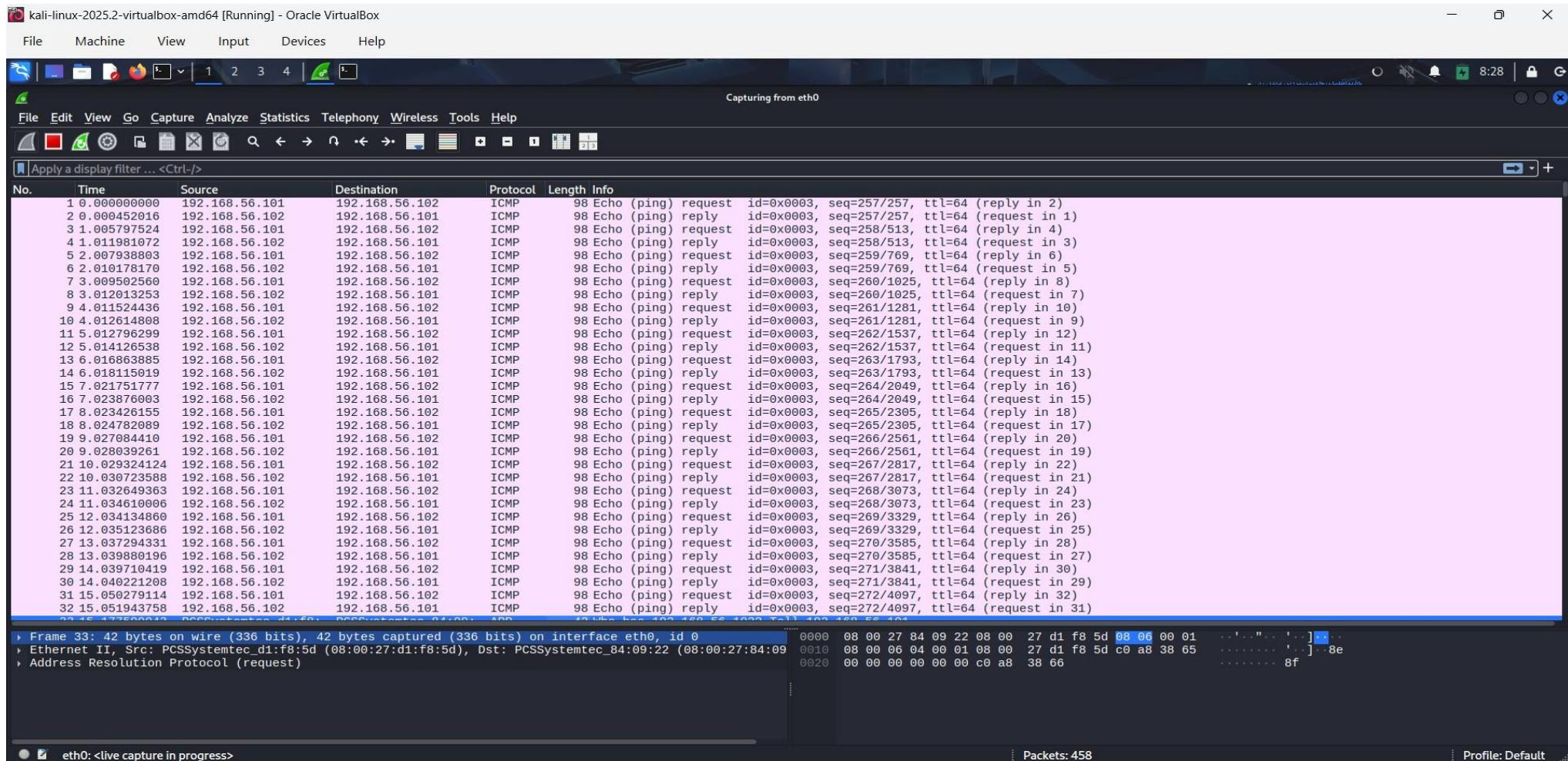
Ubuntu Unauthorised File Access- Wazuh Capture

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

Suspicious User Addition - Wazuh Capture						
Date	Time	User	Action	Severity	Score	Index
> 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

The screenshot shows the Wireshark application window capturing network traffic on interface eth0. The packet list pane displays numerous ICMP Echo (ping) requests and replies between two hosts, 192.168.56.101 and 192.168.56.102. A specific ICMP request from 192.168.56.101 to 192.168.56.102 at timestamp 13.039880196 is highlighted in blue. The packet details and bytes panes show the raw hex and ASCII data for this selected frame.

Packet details for Frame 33:

Field	Value
Frame	33
Length	42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Type	Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: PCSSystemtec_84:09:22 (08:00:27:84:09:22)
Address Resolution Protocol (request)	

Bytes pane for Frame 33:

Hex	Dec	ASCII
0000 08 00 27 84 09 22 08 00	0010 08 00 06 04 00 01 08 00	'.....'.....]
27 d1 f8 5d 08 06 00 01	27 d1 f8 5d c0 a8 38 65'.....]
0000 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00'.....]
0000 00 00 00 00 00 00 00	c0 a8 38 66'.....]
0000 00 00 00 00 00 00 00	8f'.....]

Ubuntu Port Scan-Wireshark Capture

The screenshot shows a Wireshark capture window titled "Capturing from eth0". The packet list is filtered to show only TCP traffic ("tcp"). The list contains 2166 total packets, with 2001 displayed (92.4% of the total). The captured range is from frame 159 to 1904. The packet details pane at the bottom shows a transmission control protocol (TCP) segment with the following hex and ASCII data:

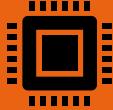
No.	Time	Source	Destination	Protocol	Length	Info
159	92.301860973	192.168.56.101	192.168.56.102	TCP	58	45042 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
160	92.302145510	192.168.56.101	192.168.56.102	TCP	58	45042 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
161	92.302365273	192.168.56.101	192.168.56.102	TCP	58	45042 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
162	92.302562080	192.168.56.101	192.168.56.102	TCP	58	45042 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
163	92.302773338	192.168.56.101	192.168.56.102	TCP	58	45042 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
164	92.302959616	192.168.56.101	192.168.56.102	TCP	58	45042 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
165	92.303148495	192.168.56.101	192.168.56.102	TCP	58	45042 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
166	92.303315435	192.168.56.101	192.168.56.102	TCP	58	45042 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
167	92.303484048	192.168.56.101	192.168.56.102	TCP	58	45042 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
168	92.303657560	192.168.56.101	192.168.56.102	TCP	58	45042 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
169	92.304264802	192.168.56.102	192.168.56.101	TCP	60	8080 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170	92.304265127	192.168.56.102	192.168.56.101	TCP	60	587 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
171	92.304526909	192.168.56.102	192.168.56.101	TCP	60	113 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172	92.304749478	192.168.56.102	192.168.56.101	TCP	60	139 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
173	92.304749542	192.168.56.102	192.168.56.101	TCP	60	993 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
174	92.305034780	192.168.56.102	192.168.56.101	TCP	60	3389 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
175	92.305034836	192.168.56.102	192.168.56.101	TCP	60	23 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
176	92.305034887	192.168.56.102	192.168.56.101	TCP	60	554 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177	92.305034909	192.168.56.102	192.168.56.101	TCP	60	8888 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
178	92.305034930	192.168.56.102	192.168.56.101	TCP	60	119 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
179	92.305103468	192.168.56.101	192.168.56.102	TCP	58	45042 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
180	92.305628104	192.168.56.101	192.168.56.102	TCP	58	45042 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
181	92.305773241	192.168.56.101	192.168.56.102	TCP	58	45042 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
182	92.305888123	192.168.56.101	192.168.56.102	TCP	58	45042 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
183	92.305979113	192.168.56.102	192.168.56.101	TCP	60	3306 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
184	92.305979194	192.168.56.102	192.168.56.101	TCP	60	5900 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
185	92.306187796	192.168.56.102	192.168.56.101	TCP	60	21 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186	92.306233396	192.168.56.101	192.168.56.102	TCP	58	45042 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
187	92.306347820	192.168.56.101	192.168.56.102	TCP	58	45042 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
188	92.306451639	192.168.56.102	192.168.56.101	TCP	60	111 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
189	92.306451681	192.168.56.102	192.168.56.101	TCP	60	995 → 45042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
190	92.306597647	192.168.56.101	192.168.56.102	TCP	58	45042 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
191	92.306700130	192.168.56.101	192.168.56.102	TCP	58	45042 → 100 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Packet details pane:

- Frame 159: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
- Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: PCSSystemtec_84:09:22 (08:00:27:84:09)
- Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.102
- Transmission Control Protocol, Src Port: 45042, Dst Port: 8080, Seq: 0, Len: 0

Packets: 2166 · Displayed: 2001 (92.4%) · Profile: Default

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.

