

# CAPSTONE CASE STUDY- PROSPERITY BANK BREACH INVESTIGATION

BY

STANLEY EKECHUKWU

# SOC Incident Report



Organisation: Prosperity Bank

Prepared by: Stanley Ekechukwu

Date: 5<sup>th</sup> 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

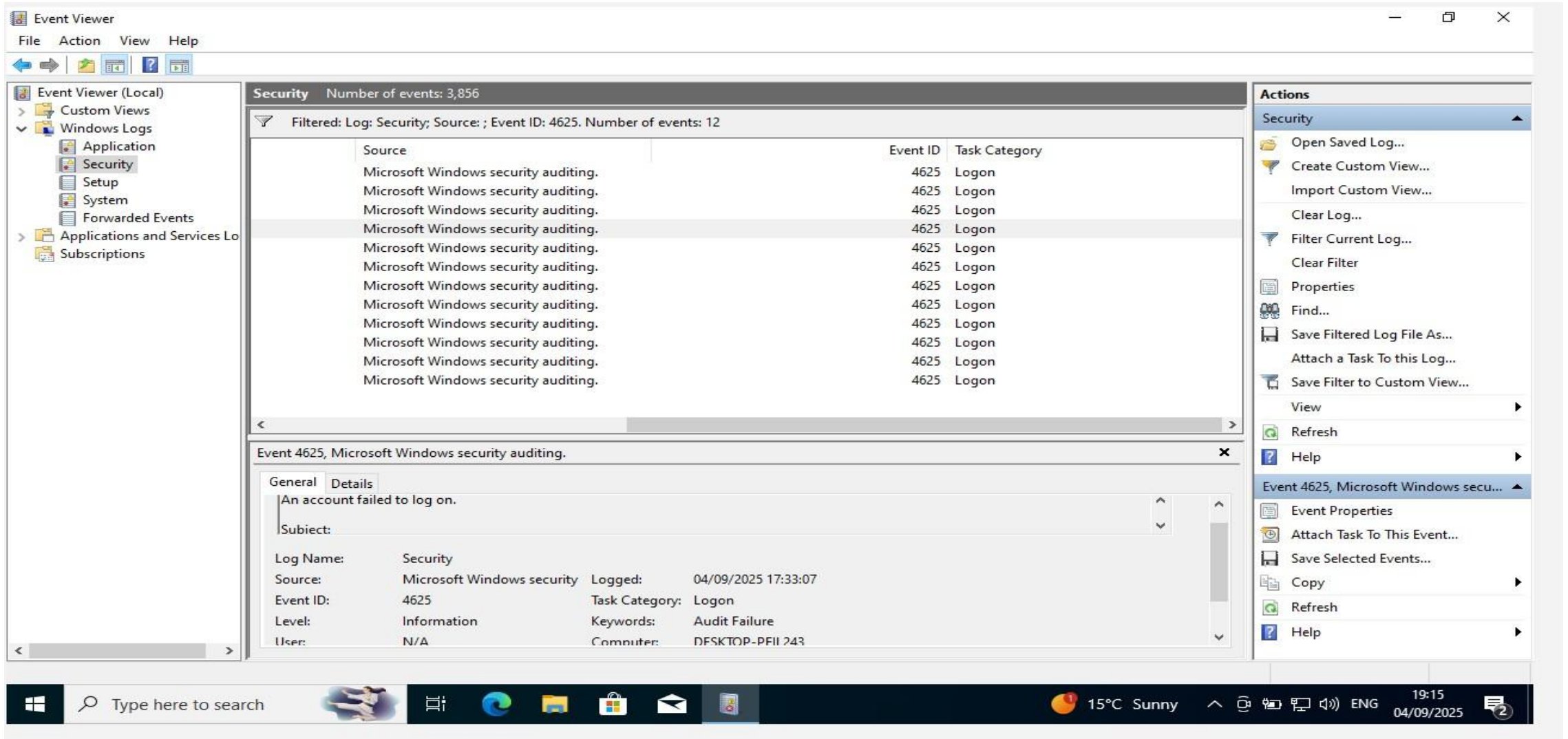
INCIDENT TYPE: UNAUTHORISED LOGIN ATTEMPTS, PRIVILEGE ESCALATION, RECONNAISSANCE

SEVERITY LEVEL: HIGH

AFFECTED SYSTEMS:

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

# Win10 Failed Login Attempts-Event Viewer Logs



The screenshot displays the Windows Event Viewer application. The left-hand pane shows the tree structure with 'Security' selected under 'Windows Logs'. The main pane is titled 'Security' and shows a list of 12 filtered events (Log: Security; Source: ; Event ID: 4625). The events are all 'Logon' tasks from 'Microsoft Windows security auditing'. The right-hand pane shows the 'Actions' menu for the selected event, with 'Event Properties' highlighted.

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

- 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

# Win10 Failed Login Attempts-Wazuh Capture

W. Threat Hunting windows-1 a ?					
Sep 4, 2025 @ 10:40:34.497 - Sep 5, 2025 @ 10:40:34.497					
Export Formatted 743 available fields Columns 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

0000 08 00 27 d3 ed 4d 08 00 27 d1 f8 5d 08 00 45 00 ..'.M..']..E.  
0010 00 54 1b 18 40 00 40 01 2d 71 c0 a8 38 65 c0 a8 .T..@.-q..8e..  
0020 38 6a 08 00 82 28 00 02 00 c2 be ca ba 68 00 00 8j...(.h..  
0030 00 00 38 0d 05 00 00 00 00 00 10 11 12 13 14 15 ..8.....  
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 &'()\*+,-./012345  
0060 36 37 67



# Win10 Port Scan-Wireshark Capture

The image shows a Wireshark capture of network traffic on interface eth0 (udp). The capture is filtered for 'udp'. The packet list shows a series of DNS queries and responses, followed by a DHCP Discover and Offer sequence, and then a series of DNS queries and responses. The packet details pane shows the structure of the selected packet (Frame 15: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0). The packet structure is as follows:

- Ethernet II, Src: PCSSystemtec d3:ed:4d (08:00:27:d3:ed:4d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 192.168.56.106, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 68, Dst Port: 67
- Dynamic Host Configuration Protocol (Inform)

The packet bytes pane shows the raw data of the selected packet, including the Ethernet II header, IP header, UDP header, and DHCP packet structure.



# 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

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

File Machine View Input Devices Help

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=257/257, ttl=64 (reply in 2)
2	0.000452016	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=257/257, ttl=64 (request in 1)
3	1.005797524	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=258/513, ttl=64 (reply in 4)
4	1.011981972	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=258/513, ttl=64 (request in 3)
5	2.007938803	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=259/769, ttl=64 (reply in 6)
6	2.010178170	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=259/769, ttl=64 (request in 5)
7	3.009502560	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=260/1025, ttl=64 (reply in 8)
8	3.012013253	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=260/1025, ttl=64 (request in 7)
9	4.011524436	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=261/1281, ttl=64 (reply in 10)
10	4.012614808	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=261/1281, ttl=64 (request in 9)
11	5.012796299	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=262/1537, ttl=64 (reply in 12)
12	5.014126538	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=262/1537, ttl=64 (request in 11)
13	6.016863885	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=263/1793, ttl=64 (reply in 14)
14	6.018115019	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=263/1793, ttl=64 (request in 13)
15	7.021751777	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=264/2049, ttl=64 (reply in 16)
16	7.023876003	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=264/2049, ttl=64 (request in 15)
17	8.023426155	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=265/2305, ttl=64 (reply in 18)
18	8.024782089	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=265/2305, ttl=64 (request in 17)
19	9.027084410	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=266/2561, ttl=64 (reply in 20)
20	9.028039261	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=266/2561, ttl=64 (request in 19)
21	10.029324124	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=267/2817, ttl=64 (reply in 22)
22	10.030723588	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=267/2817, ttl=64 (request in 21)
23	11.032649363	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=268/3073, ttl=64 (reply in 24)
24	11.034610006	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=268/3073, ttl=64 (request in 23)
25	12.034134860	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=269/3329, ttl=64 (reply in 26)
26	12.035123686	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=269/3329, ttl=64 (request in 25)
27	13.037294331	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=270/3585, ttl=64 (reply in 28)
28	13.039880196	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=270/3585, ttl=64 (request in 27)
29	14.039710419	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=271/3841, ttl=64 (reply in 30)
30	14.040221208	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=271/3841, ttl=64 (request in 29)
31	15.050279114	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=272/4097, ttl=64 (reply in 32)
32	15.051943758	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=272/4097, ttl=64 (request in 31)

Frame 33: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0

Ethernet II, Src: PCSSystemtec\_d1:f8:5d (08:00:27:d1:f8:5d), Dst: PCSSystemtec\_84:09:22 (08:00:27:84:09:22)

Address Resolution Protocol (request)

eth0: <live capture in progress>

Packets: 458

Profile: Default

# Ubuntu Network Scan-Wireshark Capture2

The image shows a Wireshark network capture of ICMP Echo (ping) traffic. The packet list pane displays 60 packets, alternating between requests and replies. The packet details pane for packet 33 shows the Ethernet II header and the ARP request details. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
28	13.039880196	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=270/3585, ttl=64 (request in 27)
29	14.039710419	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=271/3841, ttl=64 (reply in 30)
30	14.040221208	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=271/3841, ttl=64 (request in 29)
31	15.050279114	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=272/4097, ttl=64 (reply in 32)
32	15.051943758	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=272/4097, ttl=64 (request in 31)
33	15.177599043	PCSSystemtec_d1:f8:5d	PCSSystemtec_84:09:22	ARP	42	Who has 192.168.56.102? Tell 192.168.56.101
34	15.179520228	PCSSystemtec_84:09:22	PCSSystemtec_d1:f8:5d	ARP	60	192.168.56.102 is at 08:00:27:84:09:22
35	16.052371682	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=273/4353, ttl=64 (reply in 36)
36	16.052769365	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=273/4353, ttl=64 (request in 35)
37	16.288552287	PCSSystemtec_84:09:22	PCSSystemtec_d1:f8:5d	ARP	60	Who has 192.168.56.101? Tell 192.168.56.102
38	16.288563523	PCSSystemtec_d1:f8:5d	PCSSystemtec_84:09:22	ARP	42	192.168.56.101 is at 08:00:27:d1:f8:5d
39	17.065643725	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=274/4609, ttl=64 (reply in 40)
40	17.066618069	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=274/4609, ttl=64 (request in 39)
41	18.066757562	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=275/4865, ttl=64 (reply in 42)
42	18.067962832	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=275/4865, ttl=64 (request in 41)
43	19.071583316	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=276/5121, ttl=64 (reply in 44)
44	19.082222924	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=276/5121, ttl=64 (request in 43)
45	20.072891995	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=277/5377, ttl=64 (reply in 46)
46	20.075780546	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=277/5377, ttl=64 (request in 45)
47	21.074124366	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=278/5633, ttl=64 (reply in 48)
48	21.075795225	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=278/5633, ttl=64 (request in 47)
49	22.075787790	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=279/5889, ttl=64 (reply in 50)
50	22.077664616	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=279/5889, ttl=64 (request in 49)
51	23.076370415	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=280/6145, ttl=64 (reply in 52)
52	23.078603404	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=280/6145, ttl=64 (request in 51)
53	24.077845421	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=281/6401, ttl=64 (reply in 54)
54	24.081778166	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=281/6401, ttl=64 (request in 53)
55	25.078318988	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=282/6657, ttl=64 (reply in 56)
56	25.080658078	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=282/6657, ttl=64 (request in 55)
57	26.080162321	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=283/6913, ttl=64 (reply in 58)
58	26.080995849	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=283/6913, ttl=64 (request in 57)
59	27.082654676	192.168.56.101	192.168.56.102	ICMP	98	Echo (ping) request id=0x0003, seq=284/7169, ttl=64 (reply in 60)
60	27.083070750	192.168.56.102	192.168.56.101	ICMP	98	Echo (ping) reply id=0x0003, seq=284/7169, ttl=64 (request in 59)

Frame 33: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0  
Ethernet II, Src: PCSSystemtec\_d1:f8:5d (08:00:27:d1:f8:5d), Dst: PCSSystemtec\_84:09:22 (08:00:27:84:09:22)  
Address Resolution Protocol (request)

0000 08 00 27 84 09 22 08 00 27 d1 f8 5d 08 06 00 01 ..... "8f" .....  
0010 08 00 06 04 00 01 08 00 27 d1 f8 5d c0 a3 38 65 ..... 8e  
0020 00 00 00 00 00 00 c0 a3 38 66 ..... 8f



# Ubuntu Port Scan-Wireshark Capture

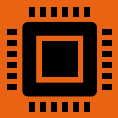
Wireshark packet capture showing a port scan on 192.168.56.102. The capture is filtered by 'tcp' and shows packets captured on interface 'eth0'.

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	110 → 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

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 employee 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.

