Prosperity Bank Breach Investigation

Akin Aremu

1. Executive Summary

Prosperity Bank detected suspicious activity on a critical Ubuntu server during routine security monitoring. I conducted an investigation so that I could analyse authentication and privilege-related events recorded in system logs.

During my investigation, I was able to identify a successful privilege escalation where a standard user account gained root-level access, as well as the creation of an unauthorized local user account. These activities indicated potential insider threat activity or the compromise of valid credentials, which posed a risk of unauthorized system control and persistence within the environment.

Although I was not able to observe any evidence of data exfiltration during this investigation, the detected actions demonstrated weaknesses in access control and monitoring that could be leveraged for lateral movement or further compromise. This report documents the findings, assesses potential impact, and recommends mitigation measures to strengthen Prosperity Bank's security posture.

---

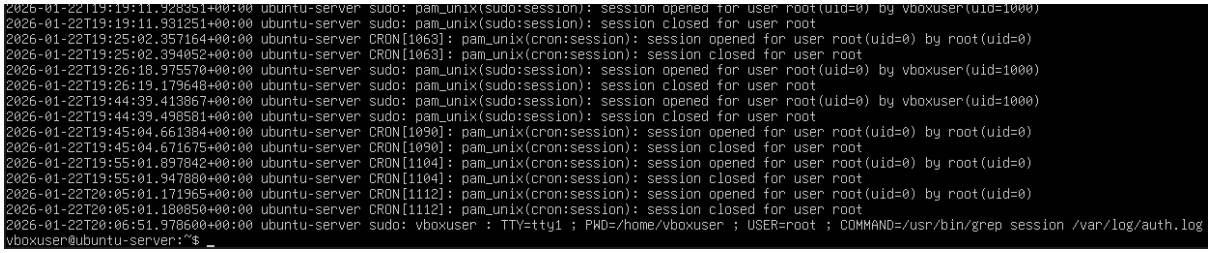
2. Key Detections

Detection 1: Privilege Escalation on Ubuntu Server

Severity: High

Evidence: /var/log/auth.log

```
vboxuser@ubuntu-server:~$ sudo grep useradd /var/log/auth.log
2026-01-22T03:50:42.693524+00:00 ubuntu-server useradd[803]: new group: name=vboxuser, GID=1000
2026-01-22T03:50:42.693555+00:00 ubuntu-server useradd[803]: new user: name=vboxuser, UID=1000, GID=1000, h
2026-01-22T03:50:42.693566+00:00 ubuntu-server useradd[803]: add 'vboxuser' to group 'adm'
2026-01-22T03:50:42.693578+00:00 ubuntu-server useradd[803]: add 'vboxuser' to group 'cdrom'
2026-01-22T03:50:42.693589+00:00 ubuntu-server useradd[803]: add 'vboxuser' to group 'sudo'
2026-01-22T03:50:42.693603+00:00 ubuntu-server useradd[803]: add 'vboxuser' to group 'dip'
2026-01-22T03:50:42.693614+00:00 ubuntu-server useradd[803]: add 'vboxuser' to group 'plugdev'
2026-01-22T03:50:42.693644+00:00 ubuntu-server useradd[803]: add 'vboxuser' to group 'lxd'
2026-01-22T03:50:42.693659+00:00 ubuntu-server useradd[803]: add 'vboxuser' to shadow group 'adm'
2026-01-22T03:50:42.693678+00:00 ubuntu-server useradd[803]: add 'vboxuser' to shadow group 'cdrom'
2026-01-22T03:50:42.693701+00:00 ubuntu-server useradd[803]: add 'vboxuser' to shadow group 'sudo'
2026-01-22T03:50:42.693716+00:00 ubuntu-server useradd[803]: add 'vboxuser' to shadow group 'dip'
2026-01-22T03:50:42.693733+00:00 ubuntu-server useradd[803]: add 'vboxuser' to shadow group 'plugdev'
2026-01-22T03:50:42.693747+00:00 ubuntu-server useradd[803]: add 'vboxuser' to shadow group 'lxd'
```



Non-root user (vboxuser) gained root access.

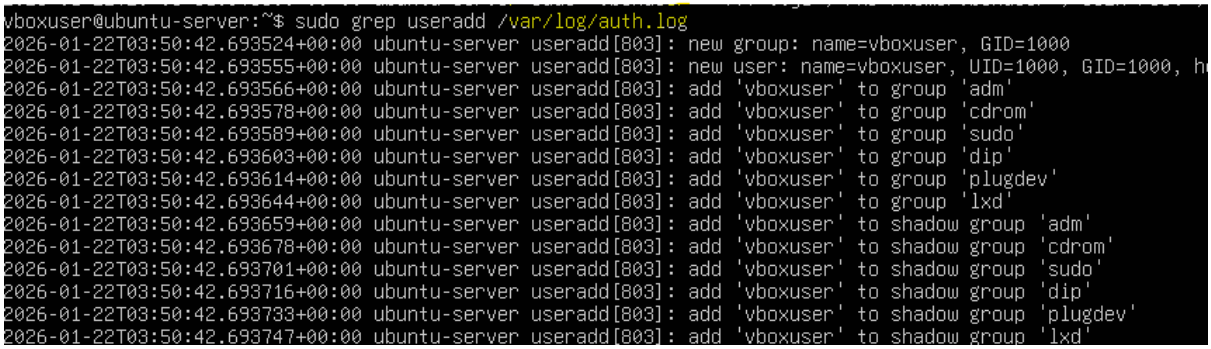
Privilege escalation detected on Ubuntu server via sudo access

---

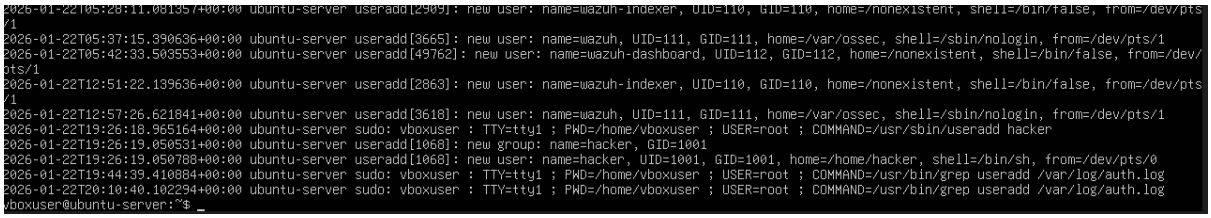
Detection 2: Unauthorized Local User Account Creation

Severity: High

Evidence: /var/log/auth.log,



New local user account hacker created without authorization.



Unauthorized local user account creation detected

---

3. Threat Assessment & Impact

Based on the Ubuntu server logs and the evidence collected:

- **Privilege Escalation**
  - A standard user (vboxuser) gained root access.
  - This represents **high-risk access** that could allow full system control.
  - Potential threats include: disabling security controls, installing backdoors, or accessing sensitive data.
- **Unauthorized User Creation**
  - A new account (hacker) was added without authorization.

- This indicates **persistence**, allowing an attacker to maintain access even if the original account is secured.
- Could be used for lateral movement to other servers or systems.

- **Potential Combined Threats**

- Lateral movement across the network
- Exfiltration of sensitive banking data
- Long-term compromise of server integrity

- **Impact Overview**

- **Confidentiality:** Moderate to High risk. Sensitive system files could be accessed.
- **Integrity:** High risk. Root access allows modification of system configurations and logs.
- **Availability:** Moderate risk. Malicious actions could disrupt server functionality.
- **Business Impact:** If exploited further, could impact customer data and banking operations. Could lead to regulatory or compliance issues if unnoticed.

---

4. *Mitigation: pfSense VLAN Segmentation*

Recommendation

To reduce the risk of lateral movement and limit the impact of future compromise, I would recommend implementing network segmentation using pfSense firewalls with VLANs.

VLAN Design (minimum)

VLAN	Purpose	Example Systems
VLAN 1	Employee Workstations	Windows client machines
VLAN 2	Backend Servers	Ubuntu servers, databases
VLAN 3 (optional)	SOC & Monitoring	Log servers, SIEM agent servers

Explanation:

- By segmenting networks:

- A compromised workstation cannot directly access critical servers.
- Servers are isolated from user endpoints.
- SOC monitoring systems are on their own VLAN, reducing attack exposure.

Additional Security Measures

- **Monitor Privilege Escalation & User Creation**
  - Configure log monitoring (auth.log) or Wazuh Agent alerts
  - Notify SOC when unauthorized sudo or useradd events occur
- **Limit Administrative Access**
  - Only allow root access through SOC-approved accounts
  - Use sudo policies and logging
- **Periodic Review**
  - Check VLAN firewall rules and access lists
  - Audit authentication logs regularly