Proxmox Security Audit Report

# 1. Executive Summary

This report provides a basic security assessment of the Proxmox VE 8.4.0 server (cyberlab.local). It evaluates the system for insecure configurations, exposed services, account policies, and update status. The goal is to identify potential vulnerabilities and provide hardening recommendations to reduce risk.

# 2. Scope & Objectives

- Assess externally accessible services and attack surface  
- Identify insecure configurations  
- Review account & SSH access controls  
- Provide actionable hardening steps

# 3. System Overview

Hostname: cyberlab  
Proxmox Version: 8.4.0  
Kernel: 6.8.12-9-pve  
Architecture: x86\_64  
System IP: 192.168.2.103

# 4. Findings

## A. Exposed Services (Nmap)

|  |  |  |  |
| --- | --- | --- | --- |
| Port | Service | Version | Risk Level |
| 22 | SSH | OpenSSH 9.2p1 | Medium |
| 111 | RPCbind | v2–4 | Medium |
| 3128 | HTTP (API) | Proxmox REST API 3.0 | High |
| 8006 | Web UI | Self-signed HTTPS | Medium |

## B. Web UI Security

- HTTPS Enabled: Yes (self-signed cert) [Medium Risk]  
- 2FA Enabled: No [High Risk]  
- Username used: root@pam [Medium Risk]

## C. SSH & Account Security

- Root login via SSH: Enabled [High Risk]  
- Additional shell users: None [Safe]

## D. Running Services (SS + ps)

Open services include Web UI, SSH, and RPC. Core Proxmox daemons such as pveproxy, pvedaemon, and pvescheduler are active with no suspicious processes observed.

## E. Patch Status

System is up to date. No pending package upgrades.

# 5. Risk Summary Table

|  |  |  |
| --- | --- | --- |
| Risk Level | Count | Examples |
| High | 3 | Root SSH login, No 2FA, Port 3128 open |
| Medium | 3 | Self-signed cert, RPCbind, root GUI access |
| Low | 2 | No non-root users, System patched |

# 6. Recommendations

1. Disable root SSH login (edit /etc/ssh/sshd\_config and set PermitRootLogin to no)  
2. Enable Two-Factor Authentication (TOTP/WebAuthn via Proxmox GUI)  
3. Investigate and close unexpected port 3128  
4. Set up “Let's Encrypt” SSL for Web GUI  
5. Add IP allowlists via Proxmox firewall or CLI  
6. Install and configure fail2ban to prevent brute-force

# 7. Conclusion

The Proxmox VE server 'cyberlab.local' is functional and up-to-date, but has critical services exposed. By applying the recommendations, risk can be significantly reduced.