Proxmox Security Assessment Notes

Server version and system details

```
root@cyberlab:~# pveversion -v
proxmox-ve: 8.4.0 (running kernel: 6.8.12-9-pve)
pve-manager: 8.4.0 (running version: 8.4.0/ec58e45e1bcdf2ac)
proxmox-kernel-helper: 8.1.1
proxmox-kernel-6.8: 6.8.12-9
proxmox-kernel-6.8.12-9-pve-signed: 6.8.12-9
ceph-fuse: 17.2.8-pve2
corosync: 3.1.9-pve1
criu: 3.17.1-2+deb12u1
frr-pythontools: 10.2.1-1+pve2
glusterfs-client: 10.3-5
ifupdown2: 3.2.0-1+pmx11
ksm-control-daemon: 1.5-1
libjs-extjs: 7.0.0-5
libknet1: 1.30-pve2
libproxmox-acme-perl: 1.6.0
libproxmox-backup-qemu0: 1.5.1
libproxmox-rs-perl: 0.3.5
libpve-access-control: 8.2.2
libpve-apiclient-perl: 3.3.2
libpve-cluster-api-perl: 8.1.0
libpve-cluster-perl: 8.1.0
libpve-common-perl: 8.3.1
libpve-guest-common-perl: 5.2.2
libpve-http-server-perl: 5.2.2
libpve-network-perl: 0.11.2
libpve-rs-perl: 0.9.4
libpve-storage-perl: 8.3.6
```

```
libspice-server1: 0.15.1-1
lvm2: 2.03.16-2
lxc-pve: 6.0.0-1
lxcfs: 6.0.0-pve2
novnc-pve: 1.6.0-2
proxmox-backup-client: 3.3.7-1
proxmox-backup-file-restore: 3.3.7-1
proxmox-firewall: 0.7.1
proxmox-kernel-helper: 8.1.1
proxmox-mail-forward: 0.3.2
proxmox-mini-journalreader: 1.4.0
proxmox-offline-mirror-helper: 0.6.7
proxmox-widget-toolkit: 4.3.10
pve-cluster: 8.1.0
pve-container: 5.2.6
pve-docs: 8.4.0
pve-edk2-firmware: 4.2025.02-3
pve-esxi-import-tools: 0.7.3
pve-firewall: 5.1.1
pve-firmware: 3.15-3
pve-ha-manager: 4.0.7
pve-i18n: 3.4.2
pve-qemu-kvm: 9.2.0-5
pve-xtermjs: 5.5.0-2
qemu-server: 8.3.12
smartmontools: 7.3-pve1
spiceterm: 3.3.0
swtpm: 0.8.0+pve1
vncterm: 1.8.0
zfsutils-linux: 2.2.7-pve2
```

```
root@cyberlab:~# uname -a
Linux cyberlab 6.8.12-9-pve #1 SMP PREEMPT_DYNAMIC PMX 6.8.12-9 (2025-03
```

Running Services

Open TCP/UDP Ports

```
root@cyberlab:~# ss -tuln
Netid      State       Recv-Q      Send-Q           Local Address:Port           Peer Add
udp        UNCONN      0           0                  0.0.0.0:111                 0.0.0.0:*
udp        UNCONN      0           0                127.0.0.1:323                 0.0.0.0:*
udp        UNCONN      0           0                  [::]:111                    [::]:*
udp        UNCONN      0           0                  [::1]:323                   [::]:*
tcp        LISTEN      0           4096               0.0.0.0:111                 0.0.0.0:*
tcp        LISTEN      0           128                0.0.0.0:22                  0.0.0.0:*
tcp        LISTEN      0           4096             127.0.0.1:85                  0.0.0.0:*
tcp        LISTEN      0           100              127.0.0.1:25                  0.0.0.0:*
tcp        LISTEN      0           4096               [::]:111                    [::]:*
tcp        LISTEN      0           128                [::]:22                     [::]:*
tcp        LISTEN      0           100                [::1]:25                    [::]:*
tcp        LISTEN      0           4096                  *:3128                      *:*
tcp        LISTEN      0           4096                  *:8006                      *:*
```

Top processes by memory use

```
root@cyberlab:~# ps aux --sort=-%mem | head -n 15
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMANI
www-data    1133  0.0  1.0 260968 163844 ?        S    13:08   0:00 pveproxy worker
www-data    1132  0.0  0.9 257880 161660 ?        S    13:08   0:01 pveproxy worker
www-data    1134  0.0  0.9 256840 159272 ?        S    13:08   0:01 pveproxy worker
root        1125  0.0  0.9 250872 150996 ?        S    13:08   0:00 pvedaemon worker
root        1123  0.0  0.9 251004 150484 ?        S    13:08   0:00 pvedaemon worker
root        1124  0.0  0.9 250312 149588 ?        S    13:08   0:00 pvedaemon worker
root        1223  0.0  0.9 250872 146788 ?        Ss   13:08   0:00 task UPID:cyberlab:
www-data    1131  0.0  0.8 243824 146556 ?        Ss   13:08   0:00 pveproxy
root        1122  0.0  0.8 242408 145232 ?        Ss   13:08   0:00 pvedaemon
root        1144  0.0  0.7 225344 121376 ?        Ss   13:08   0:00 pvescheduler
root        1130  0.0  0.7 229100 118956 ?        Ss   13:08   0:00 pve-ha-crm
root        1139  0.0  0.7 228536 118252 ?        Ss   13:08   0:00 pve-ha-lrm
```

```
root        1112  0.1  0.6 205668 113612 ?       Ss   13:08   0:02 pvestatd
root        1096  0.1  0.6 201052 105572 ?       Ss   13:08   0:02 pve-firewall
```

Nmap Port Scan

```
PS C:\Users\karan> nmap -sV -O 192.168.2.103
Starting Nmap 7.97 ( https://nmap.org ) at 2025-05-30 13:43 -0400
Nmap scan report for cyberlab.local (192.168.2.103)
Host is up (0.013s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.2p1 Debian 2+deb12u6 (protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
3128/tcp open  http    Proxmox Virtual Environment REST API 3.0
MAC Address: 3C:58:C2:2B:C9:A6 (Intel Corporate)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:rou
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https
Nmap done: 1 IP address (1 host up) scanned in 18.85 seconds
```

Web UI Security

Is HTTPS enabled with trusted Cert ?

HTTPS is enabled but certificate is not verified.

Can you login without 2FA?

Yes

Is the username *root@pam* used?

Yes

Outdated Packages

```
root@cyberlab:~# apt update
Hit:1 http://security.debian.org/debian-security bookworm-security InRelease
Hit:2 http://deb.debian.org/debian bookworm InRelease
Hit:3 http://deb.debian.org/debian bookworm-updates InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
root@cyberlab:~# apt list --upgradeable
Listing... Done
```

Account and SSH Security

Users that can log in

```
root@cyberlab:~# cat /etc/passwd | grep '/bin/bash'
root:x:0:0:root:/root:/bin/bash
```

if root login is allowed with SSH

```
root@cyberlab:~# cat /etc/ssh/sshd_config | grep PermitRootLogin
PermitRootLogin yes
# the setting of "PermitRootLogin prohibit-password".
```