WEBCARE PRO

Enterprise Server Hardening & Security Protocol

Compiled by Mir Alamin | Web Server Expert & Linux System Administrator

PRO TIP FOR SYSTEMS ARCHITECTS

This 25-point list is the baseline standard Mir Alamin deploys on production Linux environments. A fully hardened server repels 99.9% of automated scanners, credential stuffing, and brute force scripts.

1. Access Control & SSH Hardening

- [ ] **Disable Root Login:** Ensure "PermitRootLogin no" is configured in /etc/ssh/sshd_config to prevent direct admin access.
- [ ] **SSH Key-Only Auth:** Enforce passwordless key authentication ("PasswordAuthentication no") to eliminate brute-force risk.
- [ ] **Custom Port Binding:** Move default SSH port from 22 to a non-standard port (e.g., 2200+) to dodge automatic scanners.
- [ ] **Strict Sudo Restrictions:** Avoid shared accounts. Grant specific root command privileges via dedicated sudoers user groups.
- [ ] **Auto-Logout Idle Sessions:** Set SSH "ClientAliveInterval" and "ClientAliveCountMax" to terminate inactive admin logins.

2. Firewall & Network Security

- [ ] **Stateful Firewall Deployment:** Setup UFW (Ubuntu/Debian) or Firewalld (RHEL/AlmaLinux) to block all unsolicited incoming traffic.
- [ ] **Restricted Database Access:** Bind database ports (MySQL 3306, PostgreSQL 5432) strictly to localhost (127.0.0.1) or trusted IPs.
- [ ] **Brute-Force Shield (Fail2Ban):** Monitor auth logs to automatically ban IPs showing repetitive failed login attempts.
- [ ] **Malicious Bot & Geo IP Filtering:** Configure blacklists and IPsets to drop traffic originating from notorious hacking subnets.
- [ ] **Cloudflare Proxy Shield:** Proxy DNS through Cloudflare to mask origin server IPs and filter out Layer 3/4 volumetric DDoS attacks.

3. OS & Package Maintenance

- [ ] **Automated Security Patching:** Install and configure automated unattended security upgrades to patch kernel flaws.
- [ ] **Active Vulnerability Scans:** Run regular scans against installed binaries using specialized vulnerability scanners.
- [ ] **Daemon Service Hardening:** Deactivate and remove unused system packages, legacy tools (rsh, rlogin), and services.
- [ ] **Secure Shared Memory:** Mount the /run/shm segment with strict "noexec, nosuid, nodev" flags to prevent runtime exploits.
- [ ] **File System Integrity (AIDE):** Set up Advanced Intrusion Detection Environment to monitor and alert on unauthorized file changes.

4. Web Server & Application Protection

- [ ] **Suppress Web Server Tokens:** Disable server signature exposure (e.g., "ServerTokens Prod" / "ServerSignature Off").
- [ ] **Modern SSL/TLS Protocols:** Force modern TLS 1.3 encryption, disable legacy suites (SSLv3/TLS1.0), and configure HSTS.
- [ ] **Hardened PHP Execution (php.ini):** Disable dangerous server functions (exec, system, shell_exec) in PHP configuration.
- [ ] **Anti-Malware Automation:** Run automated scans of the public web root using ClamAV and ConfigServer eXploit Scanner (CXS).
- [ ] **Strict File Permissions:** Set directories to 755 and files to 644, owned by non-privileged application owners (www-data).

5. Monitoring, Backups & Disaster Recovery

- [ ] **Encrypted Offsite Backups:** Automate daily encrypted backups to AWS S3, Wasabi, or Google Cloud with a 30-day retention loop.
- [ ] **Central Log Auditing:** Forward system auth logs to a secure, remote location or logging hub to prevent log-tampering by hackers.
- [ ] **Real-Time Health Monitors:** Install monitoring daemons (e.g., Netdata, Prometheus) to check for anomalous CPU or RAM surges.
- [ ] **Instant Slack/Email Alerts:** Set up instant notification triggers for server alerts such as low disk space or service failures.
- [ ] **Disaster Recovery Testing:** Perform periodic recovery dry-runs to verify backup integrity and calculate system restore times.