Privileged Access & Least Privilege Guide

Privileged accounts are the crown jewels for attackers. Administrator, root, and service accounts have broad access that, if compromised, can lead to total system compromise. The principle of least privilege ensures users only have the minimum access needed to perform their job.

Key Points

- ✓ Apply least privilege: grant only the minimum permissions needed for each role
- ✓ Use separate accounts for daily work and administrative tasks
- ✓ Never use admin/root accounts for email, browsing, or non-admin tasks
- ✓ Implement just-in-time (JIT) access — elevate privileges only when needed, for limited time
- ✓ Review access permissions quarterly and revoke unused privileges
- ✓ Require MFA for all privileged account access without exception
- ✓ Monitor and log all privileged account activity for audit purposes

Action Items

1. Audit your current access: do you have permissions you no longer need?
2. Request removal of any unnecessary admin or elevated privileges
3. Enable MFA on all accounts with administrative access
4. Set calendar reminders for quarterly access reviews
5. Document which privileged accounts exist and who owns them

Quick Reference

Least Privilege Checklist: Default deny, role-based access, time-limited elevation, regular reviews, automated deprovisioning.
Privileged Account Types: Domain Admin, Root, Service Accounts, Database Admin, Cloud Admin, API Keys with broad scope.
PAM Tools: CyberArk, BeyondTrust, HashiCorp Vault, Azure PIM — manage, rotate, and audit privileged credentials.