Secure Configuration Basics Guide

Default configurations are designed for ease of use, not security. Default passwords, open ports, unnecessary services, and verbose error messages all create attack surface. Hardening systems by applying secure configuration baselines is a foundational security control.

Key Points

- ✓ Never use default credentials — change all default passwords before deployment
- ✓ Disable unnecessary services, ports, and protocols on all systems
- ✓ Follow CIS Benchmarks or vendor hardening guides for baseline configurations
- ✓ Enable logging and auditing on all critical systems
- ✓ Remove sample applications, test accounts, and development tools from production
- ✓ Implement network segmentation to limit blast radius of compromises
- ✓ Document all configuration changes and maintain a golden image library

Action Items

1. Run a CIS benchmark scan against your primary systems this week
2. Audit and disable any services you do not actively use
3. Verify that default credentials have been changed on all network devices
4. Enable audit logging on critical servers and forward logs to SIEM
5. Create or update your secure baseline documentation

Quick Reference

Hardening Priorities: 1) Change defaults 2) Disable unused services 3) Enable logging 4) Apply least privilege 5) Enable encryption 6) Update firmware
Key Standards: CIS Benchmarks, NIST SP 800-123, DISA STIGs, vendor security guides
Common Misconfigurations: Default admin/admin, open RDP, world-readable S3 buckets, verbose error pages, unnecessary ports (Telnet, FTP)