Security Control Implementation

Prepared by: Leo D. Dorsey

Objective

Deploy and validate critical security controls to align with security frameworks and reduce exposure across systems and users.

Tools & Methods

Tools Used: Group Policy Editor, Active Directory Users & Computers, Firewalld/iptables, CIS Benchmarks

Controls Implemented:

- Strong password enforcement
- Multi-Factor Authentication (MFA)
- Local firewall rules and configurations
- Role-based access control (RBAC)
- System hardening: disable guest accounts, remove unused services

Implementation Steps

1. Assessed current system configuration and identified gaps
2. Mapped required controls against NIST and CIS benchmarks
3. Configured Group Policy and local policies to enforce password and access controls
4. Deployed MFA using built-in AD and third-party integrations
5. Verified controls with test users and logging tools
6. Documented all changes and created rollback plans

Results

- Achieved 90% alignment with CIS Level 1 benchmark
- Reduced local admin accounts by 75%

- MFA enforced across remote user logins

- Developed SOP for deploying baseline controls on new systems

Conclusion

This project significantly reduced common risk vectors by implementing tested and repeatable security controls. It established a standard security baseline, strengthened user account management, and improved audit readiness.