LDAP SECURITY IMPLEMENTATION CHECKLIST

Active Directory LDAP Signing & Channel Binding

STRAFE CYBERSECURITY

ABOUT THIS CHECKLIST

This comprehensive checklist will guide you through implementing LDAP signing and channel binding to protect your Active Directory environment from relay attacks. Follow each step carefully and check off items as you complete them.

PHASE 1: PRE-IMPLEMENTATION PLANNING

- [ ] **Review Current Environment** CRITICAL
  Document all domain controllers, their locations, and current LDAP configurations.

- [ ] **Identify LDAP Clients** CRITICAL
  Create inventory of all systems that authenticate via LDAP (applications, services, devices).

- [ ] **Check for Legacy Systems** IMPORTANT
  Identify systems older than 10 years that may not support LDAP signing.

- [ ] **Set Up Test Environment** CRITICAL
  Create a non-production environment that mirrors your production setup for testing.

- [ ] **Schedule Maintenance Window** IMPORTANT
  Plan a maintenance window for implementation with rollback procedures ready.

- [ ] **Notify Stakeholders** IMPORTANT

  Inform all relevant teams about the upcoming changes and potential impact.

- [ ] **Backup Current Configuration** CRITICAL

  Document and backup all current GPO settings and registry values.

PHASE 2: TESTING IN NON-PRODUCTION

- [ ] **Enable LDAP Signing in Test** CRITICAL

  Configure LDAP signing requirement to "Require signing" in test environment GPO.

- [ ] **Enable Channel Binding in Test** CRITICAL

  Set channel binding token requirement to "Always" in test environment.

- [ ] **Apply and Verify GPO** CRITICAL

  Run gpupdate /force and verify settings with gpresult /h on test DCs.

- [ ] **Test Application Authentication** CRITICAL

  Verify all identified applications can still authenticate successfully.

- [ ] **Monitor Event Logs** IMPORTANT

  Check for Event IDs 2889, 3039, and 2886 in Directory Services logs.

- [ ] **Test Client Authentication** CRITICAL

  Verify workstations, servers, and services can authenticate properly.

- [ ] **Document Test Results** IMPORTANT

  Record all test outcomes, issues encountered, and resolutions.

PHASE 3: PRODUCTION IMPLEMENTATION

- [ ] **Create Production GPO** CRITICAL

  Create new GPO named "Domain Controller - LDAP Hardening" linked to Domain Controllers OU.

- [ ] **Configure LDAP Server Signing** CRITICAL

  Set "Domain controller: LDAP server signing requirements" to "Require signing".

- [ ] **Configure Channel Binding** CRITICAL

  Set "Domain controller: LDAP server channel binding token requirements" to "Always".

- [ ] **Apply GPO to All DCs** CRITICAL

  Run gpupdate /force on each domain controller in your environment.

- [ ] **Wait for GPO Propagation** CRITICAL

  Wait at least 15 minutes for GPO replication across all domain controllers.

- [ ] **Verify Registry Settings** IMPORTANT

  Confirm LDAPServerIntegrity = 2 and LdapEnforceChannelBinding = 2 on all DCs.

PHASE 4: VERIFICATION & TESTING

- [ ] **Verify with NetExec** IMPORTANT

  Run: netexec ldap [DC_IP] -u user -p pass -M ldap-checker to verify enforcement.

- [ ] **Verify with PowerShell** IMPORTANT

  Check registry values using Get-ItemProperty PowerShell command.

- [ ] **Test User Authentication** CRITICAL

  Verify users can log in successfully across different systems.

- [ ] **Test Application Connectivity** CRITICAL

  Confirm all business-critical applications authenticate properly.

- [ ] **Check Event Logs on All DCs** IMPORTANT

  Review Directory Services logs for unsigned bind attempts (Event ID 2889).

PHASE 5: ONGOING MONITORING

- [ ] **Set Up Event Monitoring** CRITICAL

  Configure alerts for Event IDs: 2889, 3039, 2886, 2887, 3040.

- [ ] **Schedule Daily Monitoring Script** IMPORTANT

  Create scheduled task to run PowerShell monitoring script daily.

- [ ] **Document Baseline Behavior** RECOMMENDED

  Record normal LDAP traffic patterns for comparison.

- [ ] **Review Logs Weekly** IMPORTANT

  Perform weekly review of LDAP-related events and alerts.

- [ ] **Update Documentation** RECOMMENDED

  Keep configuration documentation current with any changes.

PHASE 6: DOCUMENTATION & COMPLIANCE

- [ ] **Document Implementation** IMPORTANT

  Record all configuration changes, dates, and responsible personnel.

- [ ] **Update Security Policies** IMPORTANT

  Reflect LDAP security requirements in organizational security policies.

- [ ] **Train IT Staff** RECOMMENDED

  Educate team members on LDAP security and monitoring procedures.

Create Runbooks RECOMMENDED

Document troubleshooting procedures for LDAP authentication issues.

Schedule Penetration Testing IMPORTANT

Engage professional penetration testers to verify LDAP security and identify any remaining vulnerabilities.

IMPLEMENTATION NOTES & ISSUES:

Use this space to record any issues encountered, systems that needed special configuration, or other important notes.

Implementation Date: _____

Implemented By: _____

Verified By: _____

QUICK REFERENCE

KEY REGISTRY VALUES

Path: HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

- **LDAPServerIntegrity:** 2 (Require signing)
- **LdapEnforceChannelBinding:** 2 (Always enforce)

VERIFICATION COMMANDS

PowerShell Registry Check:

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters"
```

NetExec Verification:

```
netexec ldap <DC_IP> -u user -p pass -M ldap-checker
```