Report: Security Hardening

1. Introduction

LDAP (Lightweight Directory Access Protocol) is a critical component in Active Directory environments for querying and authenticating directory data. However, standard LDAP binds are unencrypted by default, making them susceptible to interception and credential theft, especially during man-in-the-middle (MitM) attacks. LDAP Signing and Channel Binding are security features that enforce data integrity and session binding between the LDAP client and server, ensuring the client is authenticated using trusted mechanisms.

LDAP Signing ensures that LDAP communication between clients and domain controllers uses message integrity checks, while Channel Binding Tokens (CBT) tie the outer TLS channel to the inner authentication attempt, preventing credential forwarding and session hijacking attacks.

2. Objective

The objective of enabling LDAP Signing and Channel Binding is to enhance the security of directory service communications in Active Directory environments. By enforcing LDAP Signing, we ensure that all LDAP traffic is cryptographically signed to prevent tampering and man-in-the-middle attacks. Channel Binding further strengthens this by linking the authentication layer with the underlying secure channel (such as TLS), which helps prevent session hijacking and credential replay attacks. Together, these measures protect against unauthorized data access and ensure that only secure, trusted clients can communicate with domain controllers, aligning the system with modern security best practices and compliance requirements.

Key goals include:

- **Enhance Authentication Security**
  Replace insecure or legacy protocols (like NTLM) with stronger alternatives (like Kerberos) to protect authentication processes from credential theft and replay attacks.

- **Prevent Unauthorized Access**
  Enforce LDAP Signing and Channel Binding to ensure all directory communications are secure, signed, and resistant to tampering or man-in-the-middle attacks.

- **Reduce Lateral Movement Risk**
  By implementing LAPS, ensure each system has a unique, managed local admin password to block attackers from pivoting across machines using shared credentials.

- **Ensure Compliance with Security Standards**
  Align Active Directory configurations with industry best practices and compliance frameworks like CIS Benchmarks, NIST, and Microsoft Security Baselines.

- **Centralize and Automate Credential Management**
  Automate password management for local administrator accounts through LAPS, reducing administrative overhead while improving auditability and control.

3. Methodology

Active Directory (AD) environments often face security risks due to legacy protocols, unmanaged local admin accounts, and weak configurations. This methodology focuses on strengthening AD security by:

1. Enforcing LDAP signing and channel binding
2. Disabling NTLM in favor of Kerberos
3. Deploying Microsoft's Local Administrator Password Solution (LAPS)

These tasks reduce attack surfaces, prevent credential theft, and enforce secure authentication and administration practices.

3.1 Enable LDAP Signing & Channel Binding

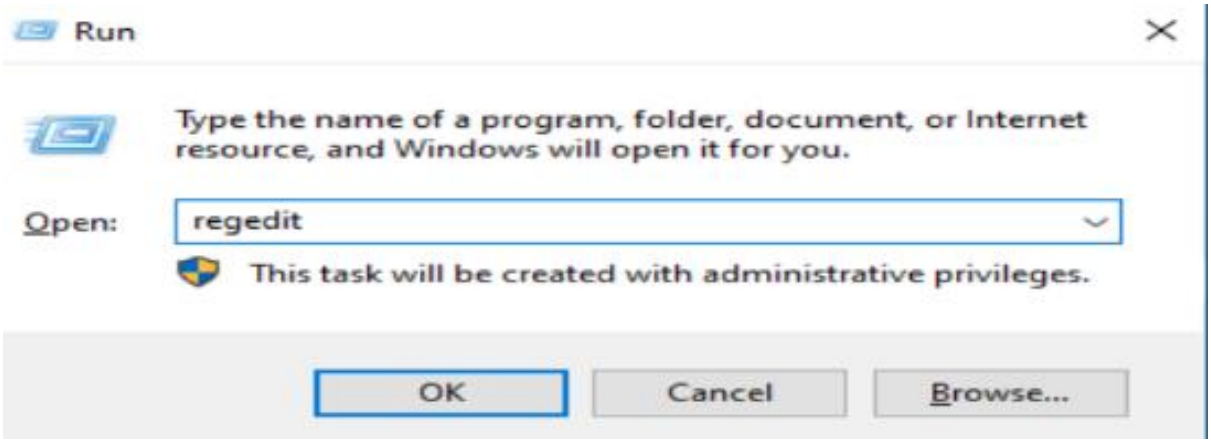
LDAP (Lightweight Directory Access Protocol) is used for querying and modifying directory services. However, unencrypted LDAP is vulnerable to interception and tampering. Enabling signing and channel binding ensures integrity and security of LDAP communications between clients and Domain Controllers (DCs).

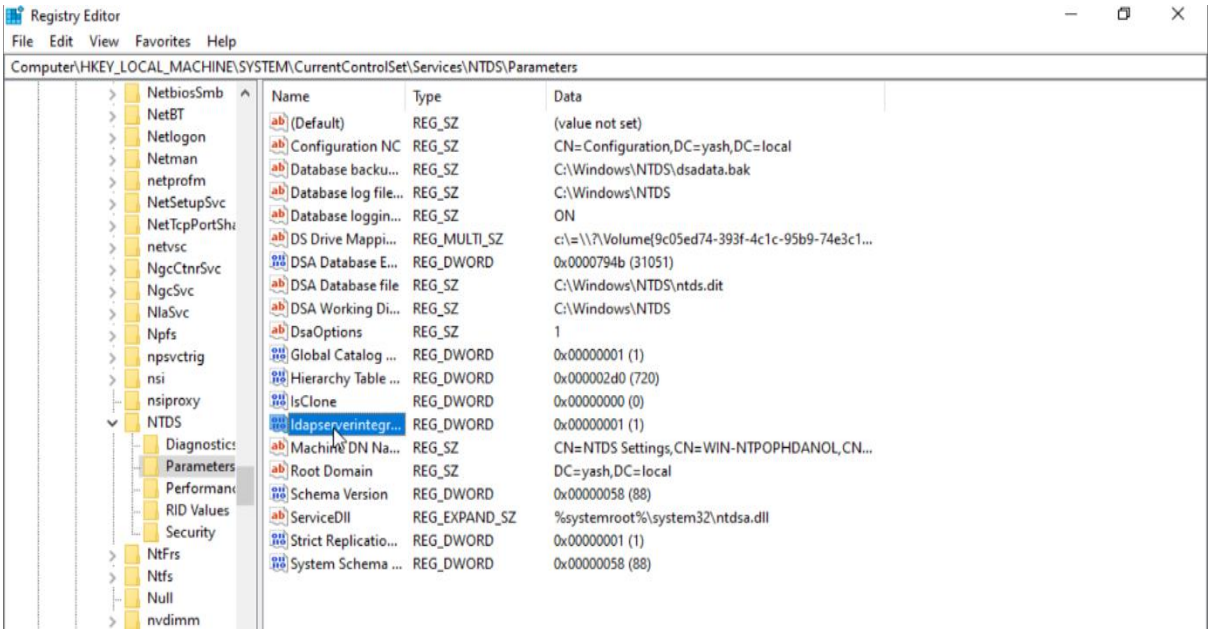
- **Enable LDAP Signing**

  LDAP signing was configured by updating the registry key located at: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters.

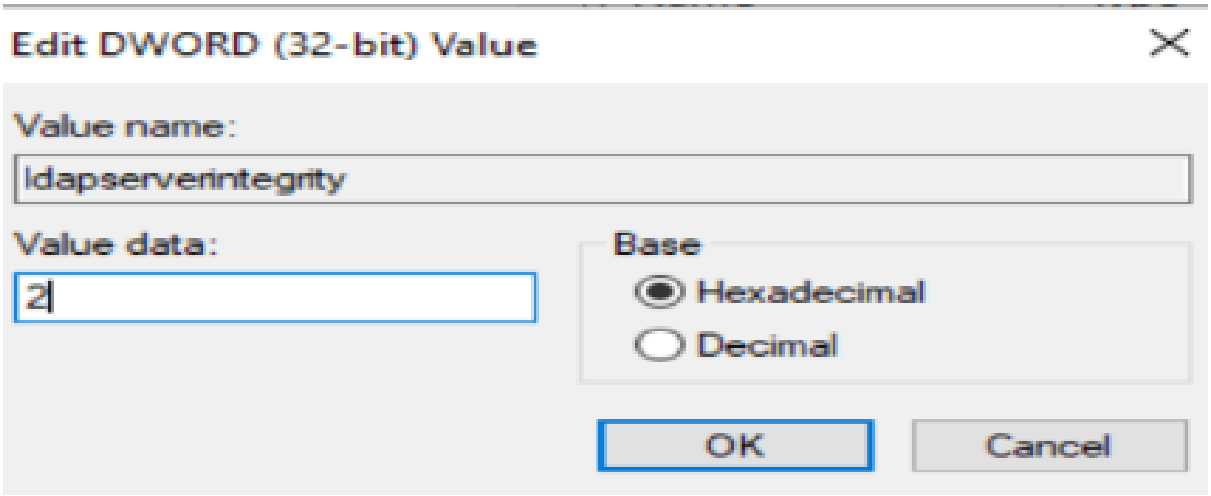
  The ldapserverintegrity setting was modified from a value of 1 to 2, making LDAP signing mandatory. Furthermore, a new DWORD entry called LdapEnforceChannelBinding was added and assigned a value of 2 to activate strict channel binding enforcement.

  (Navigate to NDTS parameters in Registry Editor)





(Registry Editor showing LDAPServerIntegrity = 2)



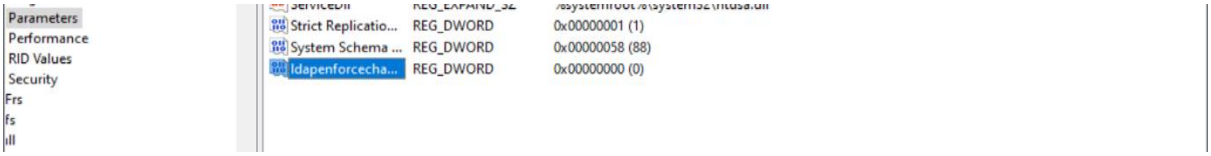
1 = Sign if the client supports it.

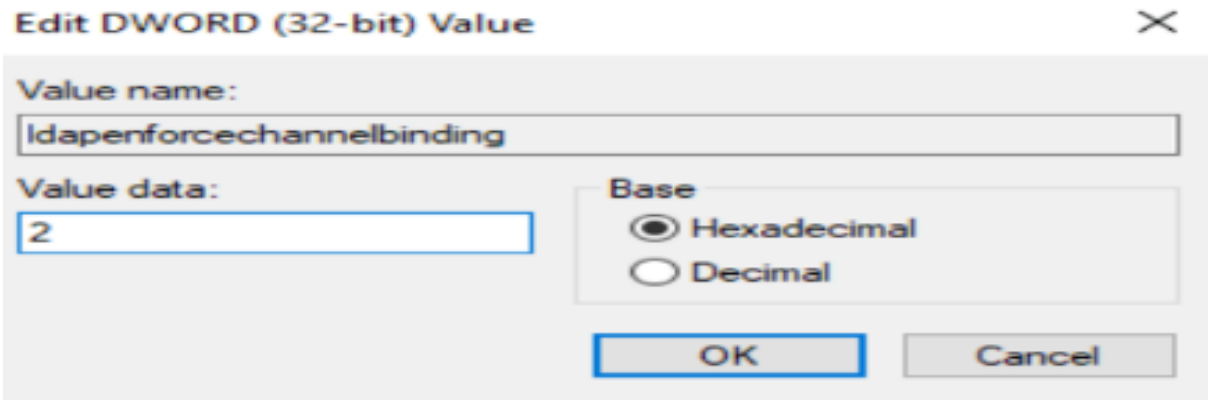
2 = **Require** LDAP signing — secure option.

- **Enable LDAP Channel Binding**

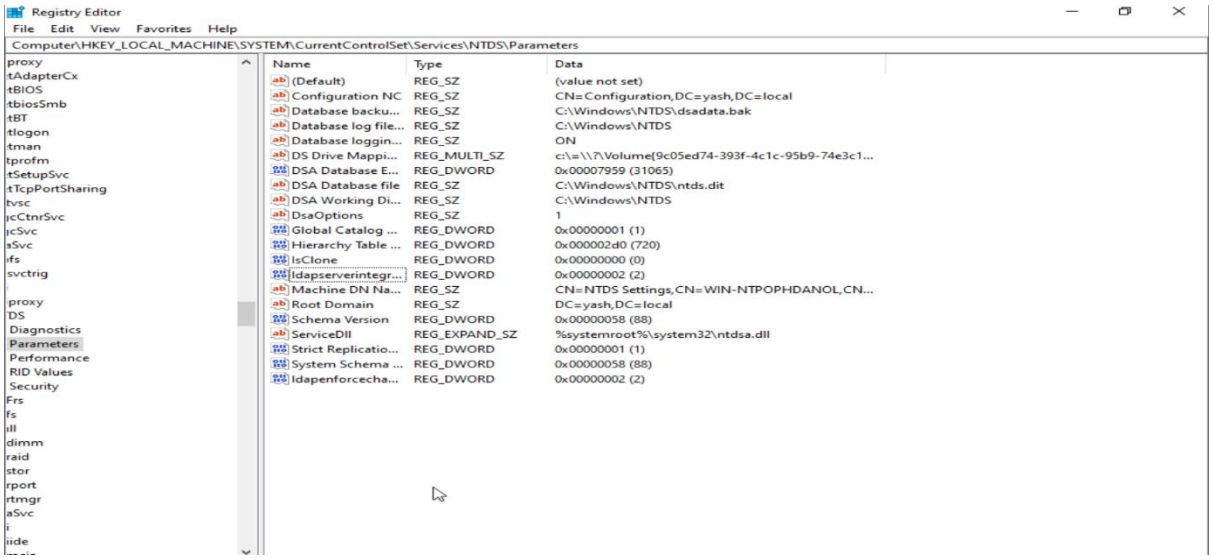
  Channel Binding ties LDAP sessions to the underlying TLS connection. Prevents NTLM relay attacks where an attacker reuses valid credentials in a new session. Essential when clients use LDAP over TLS (LDAPS).

(Add one DWORD LdapEnforceChannelBinding)





(Final ldap values)



3.2 Disable NTLM Authentication

NTLM (NT LAN Manager) is an outdated authentication protocol that is highly vulnerable to relay attacks, hash dumping, and credential forwarding. Disabling it and using Kerberos, which is stronger and more secure, is a critical AD hardening step.

- **Disable NTLM**

  A new Group Policy Object called **Disable_NTLM** was created and configured at the following path:

  Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options.

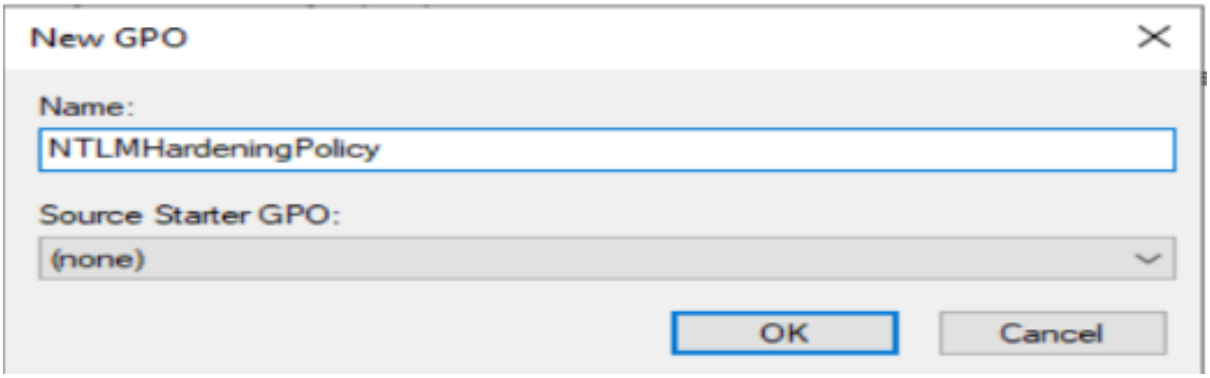
  The settings applied were:

  Network security: Restrict NTLM: Incoming NTLM traffic set to Deny all accounts

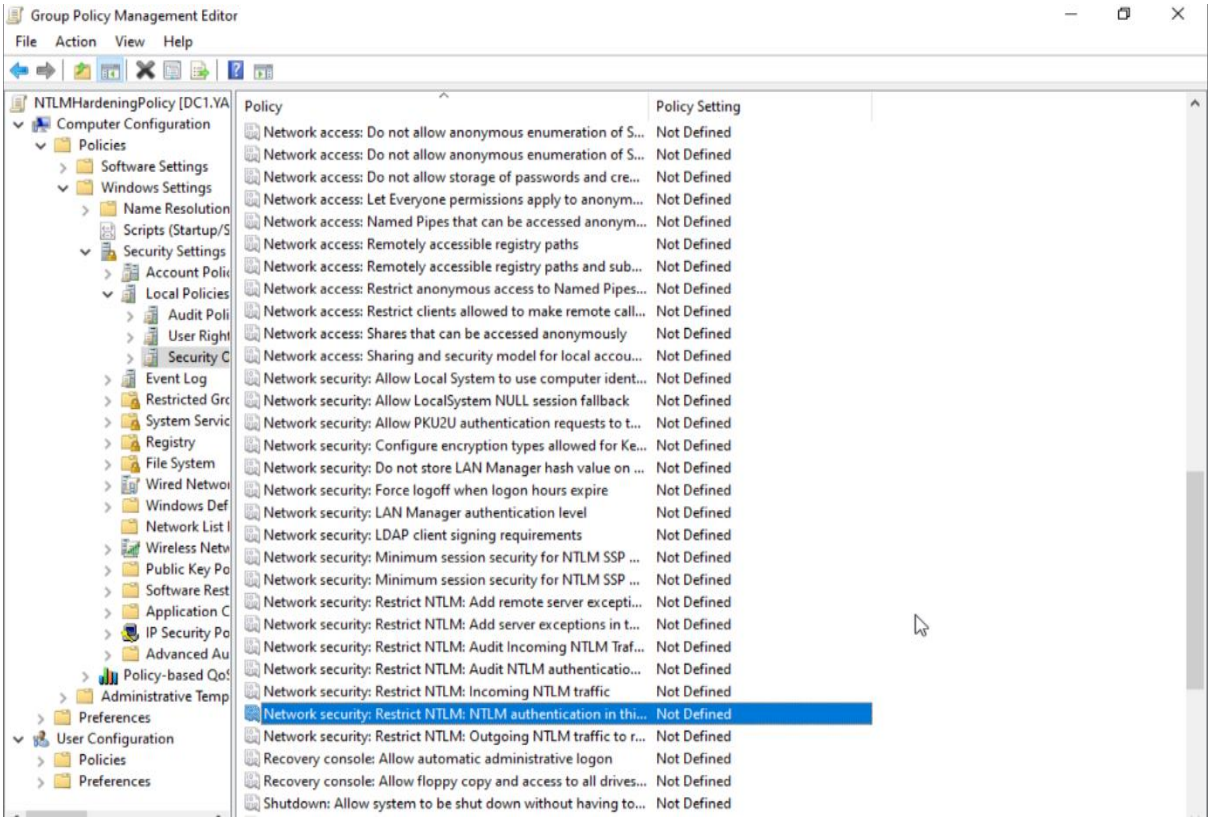
  Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers set to Deny all

This GPO was then linked to the Domain Controllers Organizational Unit (OU) to enforce these NTLM restrictions specifically on authentication processes involving domain controllers.

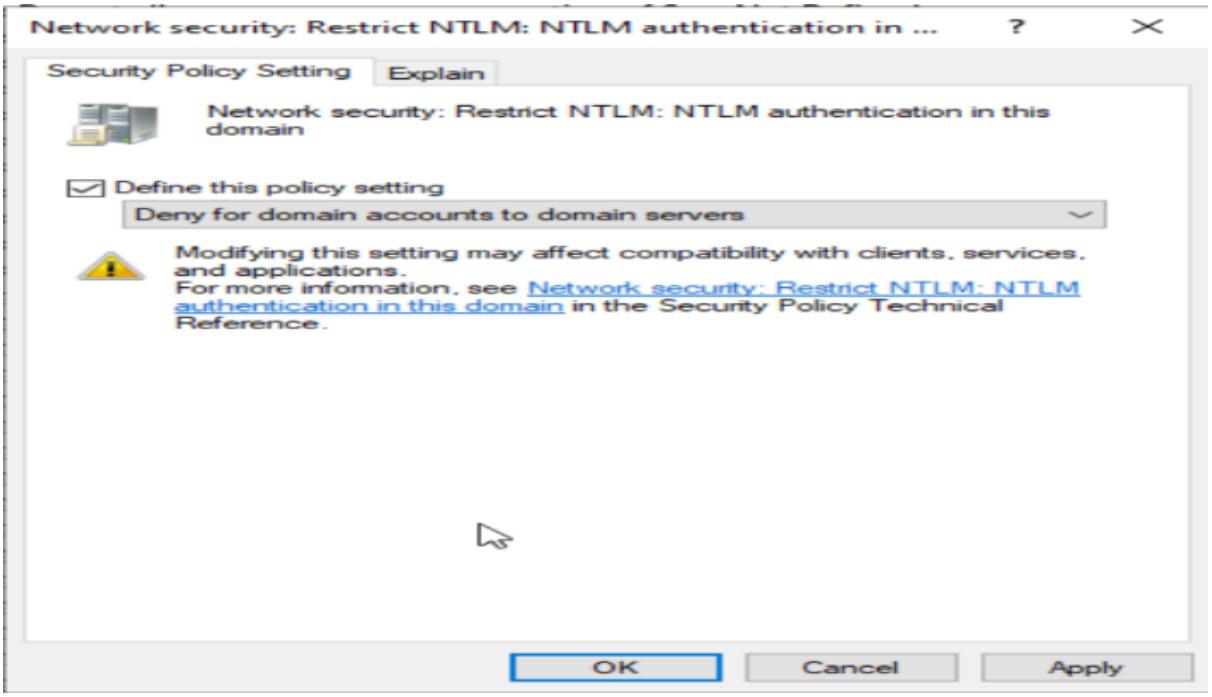
(A new GPO is created.)

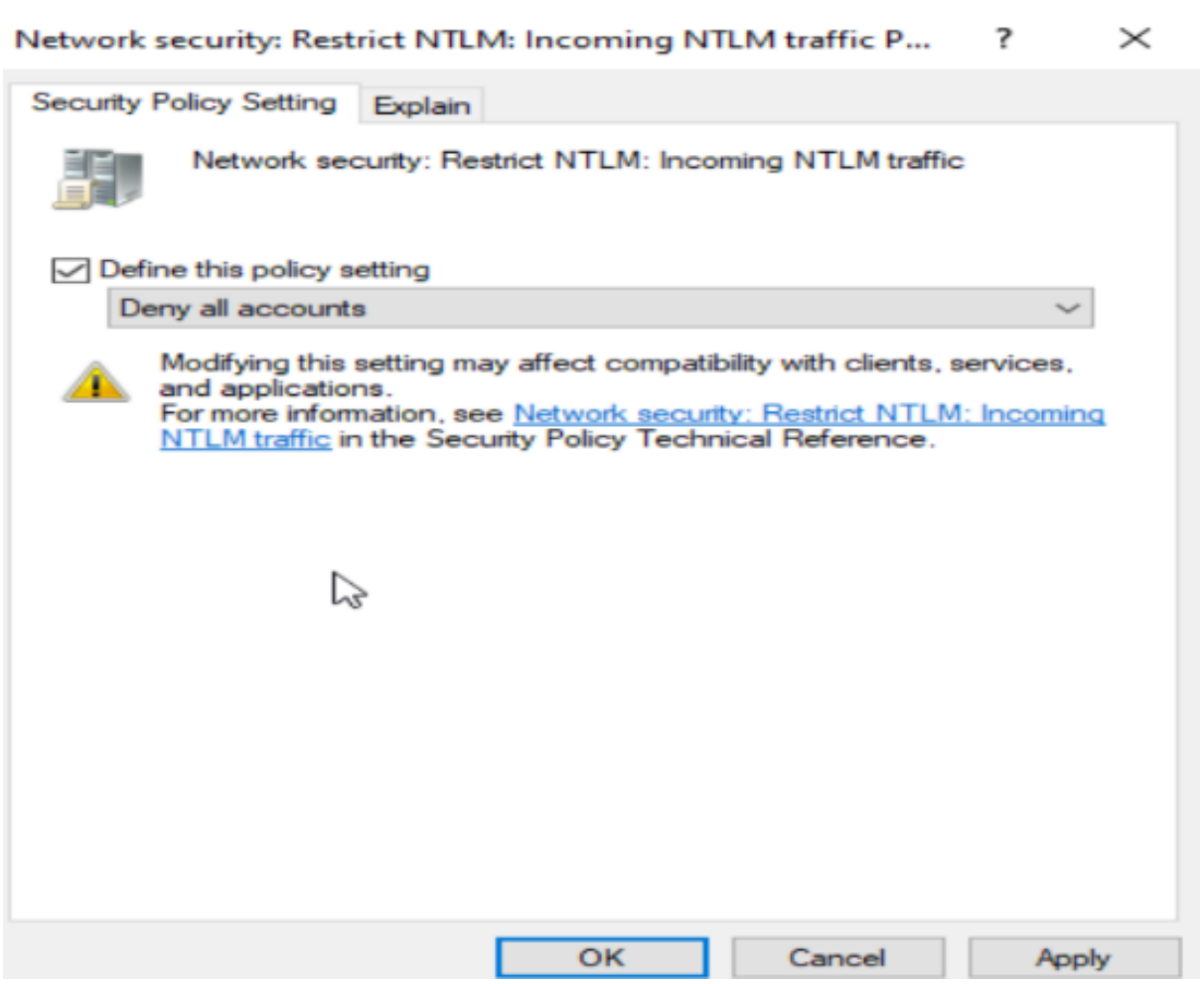


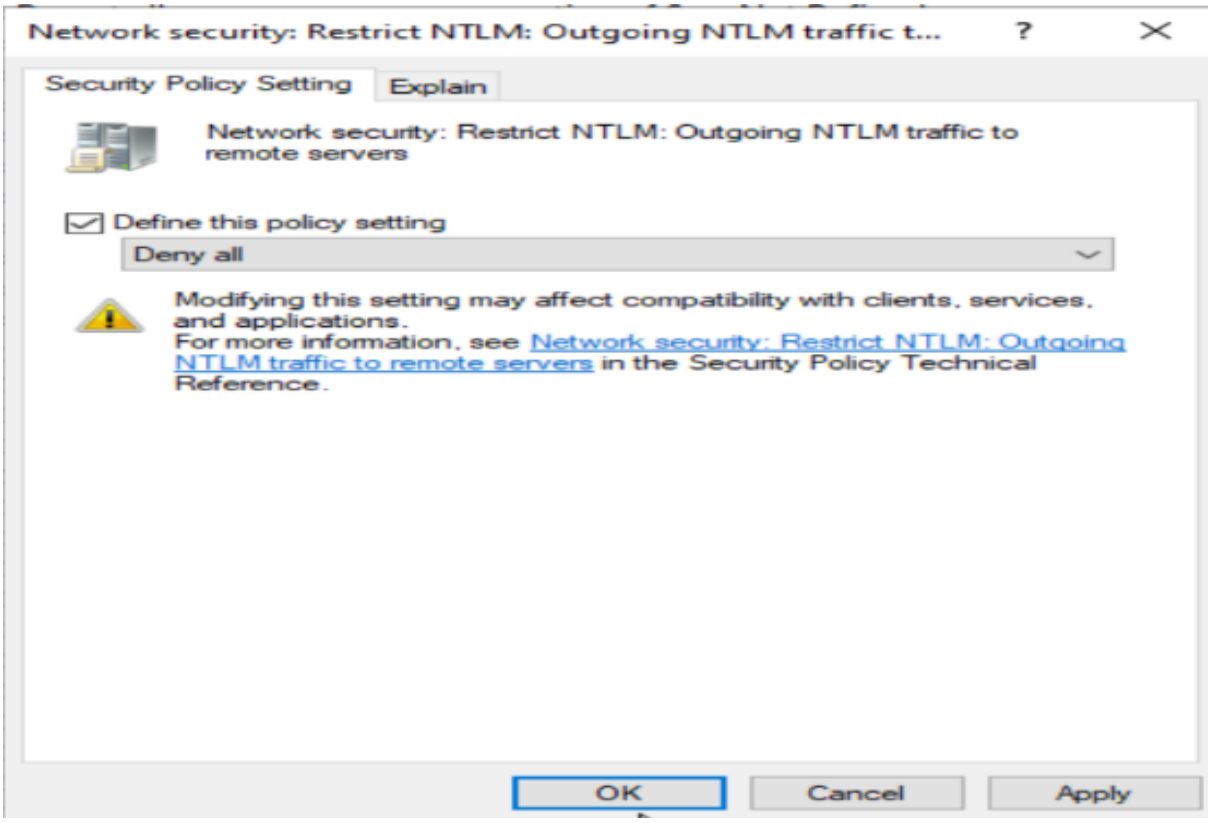
(Edit it.)



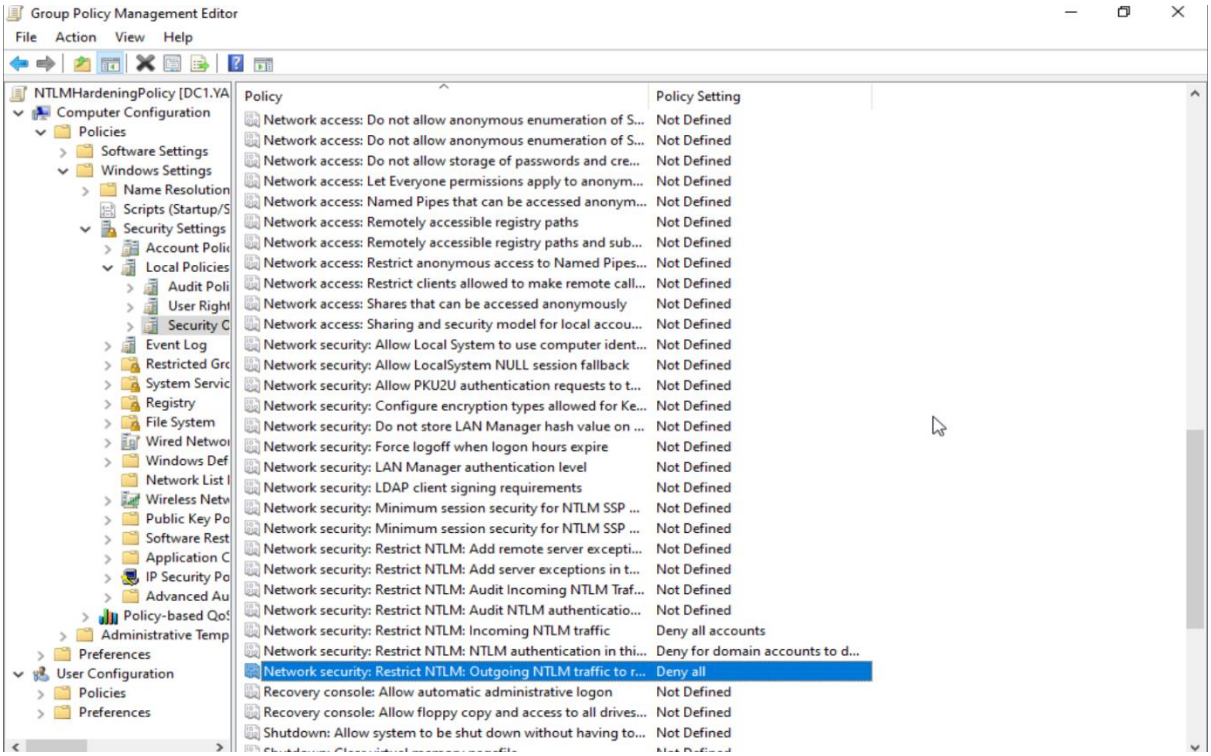
(Edit policies.)







(Final edited policy.)



(Policy is updated.)

```
PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
```

(We can see the policy is updated successfully.)

```
PS C:\Users\Administrator> gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on  5/ 16/ 2025 at 12:02:42 AM


RSOP data for YASH\Administrator on DC1 : Logging Mode
-----------------------------------------------------

OS Configuration:            Primary Domain Controller
OS Version:                  10.0.20348
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\Administrator
Connected over a slow link?: No


COMPUTER SETTINGS
------------------
    CN=DC1,OU=Domain Controllers,DC=yash,DC=local
    Last time Group Policy was applied: 5/16/2025 at 12:01:14 AM
    Group Policy was applied from:      DC1.yash.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        YASH
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    ----------------------------
        Default Domain Controllers Policy
        Windows Server 2019 Security Baseline
        Harden NSA
        Default Domain Policy
        Password Policy
        DisableSMBv1
        NTLMHardeningPolicy
        AutoEnrollment
        Local Group Policy
```

3.3 Implement LAPS (Local Administrator Password Solution)

A cumulative security update was installed to activate the built-in Windows LAPS (Local Administrator Password Solution) functionality. The LAPS PowerShell module was loaded, and the Active Directory schema was extended using the Update-LapsADSchema command. This successfully added all required attributes such as ms-LAPS-Password, ms-LAPS-PasswordExpirationTime, and others.

A new Group Policy Object was then created and configured under: Computer Configuration → Administrative Templates → System → LAPS with the following settings enabled:

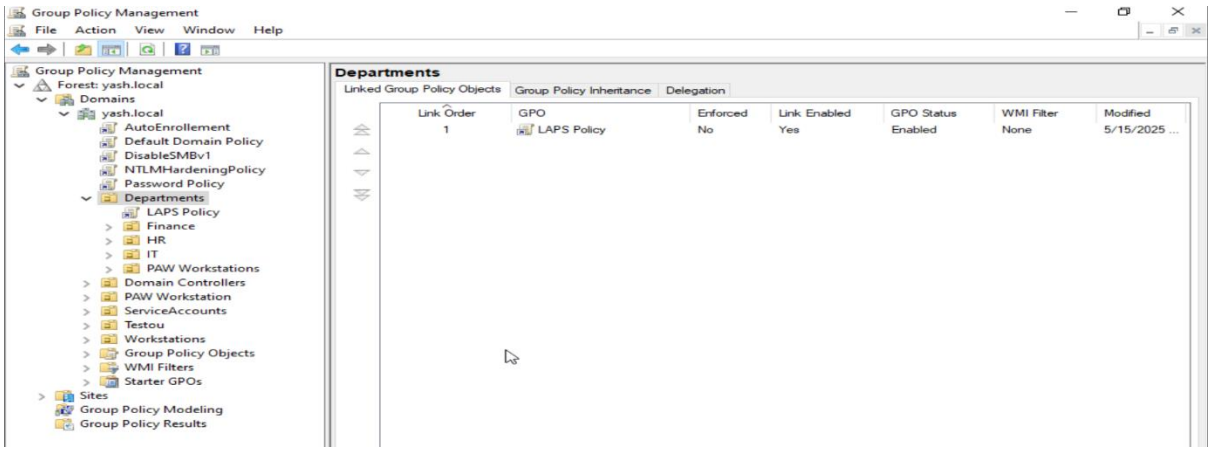
- Backup passwords for DSRM accounts
- Enable password encryption

- Define authorized password decryptors
- Specify the administrator account to be managed
- Set the password backup location
- Configure password complexity and expiration settings

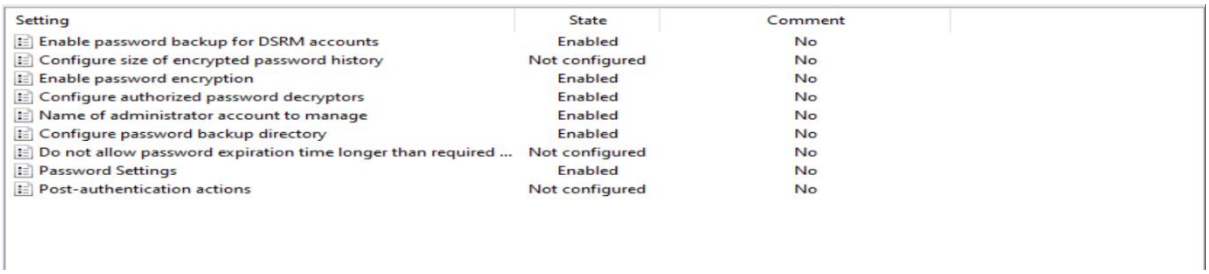
This GPO was linked to the Departments Organizational Unit, and the policy was enforced on client machines using the gpupdate /force command.

(Import and updat LAPS module.)

(Create a new policy.)



(Policy Edited)



(After updating we saw LAS Policy)

```
Applied Group Policy Objects
----------------------------
    LAPS Policy
    Default Domain Policy
    Password Policy
    DisableSMBv1
    NTLMHardeningPolicy
    AutoEnrollement
```

(The Get-LapsADPassword -Identity PC1 command works, means LAPS setup is fully functional)

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-LapsADPassword -Identity PC1


ComputerName        : PC1
DistinguishedName   : CN=PC1,OU=Finance,OU=Departments,DC=task,DC=local
Account             : Administrator
Password            : System.Security.SecureString
PasswordUpdateTime  : 5/13/2025 5:14:06 PM
ExpirationTimestamp : 6/12/2025 5:14:06 PM
Source              : EncryptedPassword
DecryptionStatus    : Success
AuthorizedDecryptor : TASK\Administrator
```

4. Results And Findings

After successfully implementing LDAP signing, disabling NTLM, and deploying LAPS, several technical and security observations were made across the Active Directory environment. These findings reflect the improved hardening status, visibility into legacy protocols, and enhanced local credential security.

4.1 LDAP Signing and Channel Binding Enforced Successfully

LDAP signing and channel binding were enabled through registry changes on the Domain Controller. These settings were applied without disrupting existing services or authentication mechanisms. Testing from client machines confirmed that all LDAP queries were being signed and securely bound to TLS sessions. This proved that critical security features could be implemented without impacting domain functionality.

4.2 NTLM Usage Was Identified and Mapped During Auditing

When auditing was enabled for NTLM through Group Policy, several logs indicated continued use of NTLM from legacy systems and services. These included certain internal applications and unmanaged endpoints. This insight was vital to safely transitioning the domain to a Kerberos-only model, by identifying and documenting components that required updates or exceptions.

4.3 Domain Successfully Transitioned to Kerberos Authentication

Once NTLM was blocked through policy, all standard domain-joined systems continued functioning normally. Authentication logs showed Kerberos ticket requests (Event ID 4768/4769), verifying that Kerberos was now the default and exclusive authentication method. This confirmed a clean transition and significantly reduced risks associated with NTLM, such as relay and hash theft attacks.

4.4 LAPS Functioned Properly and Stored Passwords Securely

Windows LAPS was installed and verified on multiple workstations. After group policies were applied, LAPS rotated the built-in Administrator passwords and stored them in Active Directory attributes. Each password was unique per machine, met complexity requirements, and was set with a secure expiration interval. Retrieval tests confirmed that only machines managed under policy were affected and functioning as expected.

4.5 Delegated Access to LAPS Was Properly Enforced

Read access to LAPS-managed passwords was restricted using Active Directory delegation. Only designated security groups, such as Helpdesk Admins, could retrieve passwords using tools like Get-AdmPwdPassword. Unauthorized users received access denied errors. This demonstrated that sensitive credential information was being protected and that delegation and RBAC (Role-Based Access Control) were correctly implemented.

5. Recommendations

To maintain and expand the gains achieved through LDAP hardening, NTLM removal, and LAPS implementation, several operational and strategic recommendations are proposed. These

recommendations ensure continued protection against credential abuse and enhance resilience in Active Directory environments.

5.1 Continuously Monitor LDAP and Authentication Traffic

It is recommended to implement continuous monitoring of LDAP and authentication traffic using tools such as Zeek, Microsoft Defender for Identity, or SIEM platforms like Splunk. These tools can detect the reintroduction of insecure protocols, misconfigured clients, or attacker activity. Regular alerts and reporting should be configured for any unsigned LDAP or NTLM authentication attempts.

5.2 Replace or Upgrade NTLM-Dependent Systems

All systems or services still relying on NTLM should be prioritized for upgrade, reconfiguration, or decommissioning. Legacy applications that cannot be updated should be isolated using firewall rules, service accounts, or segmentation to reduce exposure. Documenting and minimizing NTLM usage ensures long-term compatibility with secure authentication models.

5.3 Enable NTLM and LDAP-Related Alerts in SIEM

Configure log forwarding and alert rules in your SIEM to notify security teams when NTLM or unsigned LDAP traffic is detected. Use Event IDs such as 4624, 4768, 4771, and LDAP diagnostic events to build detection logic. These alerts help track misconfigurations, policy bypasses, or malicious behavior in real-time.

5.4 Audit LAPS Usage and Rotate Access Periodically

Regularly review audit logs that record which users or systems access LAPS-managed passwords. Rotate access control groups on a scheduled basis to minimize privilege buildup. Ensure temporary admin or Helpdesk roles are granted only for the duration of their operational need, following the principle of least privilege.

5.5 Incorporate Controls Into Baseline Build Policies

LDAP hardening, NTLM blocking, and LAPS deployment should be embedded in baseline server/workstation build processes. Update organizational hardening guides and checklist templates to reflect these configurations as mandatory. This ensures consistent application of security measures across future deployments and avoids gaps in control.

6. Conclusion

The implementation of LDAP signing and channel binding, the deprecation of NTLM authentication, and the deployment of Windows LAPS have significantly strengthened the security posture of the Active Directory environment. By enforcing secure LDAP communication, the risk of credential interception and directory-level manipulation has been mitigated. Eliminating NTLM has closed a critical legacy authentication vector that attackers commonly exploit for lateral movement and privilege escalation. The adoption of Windows LAPS ensures that every workstation now maintains a unique, automatically rotated local administrator password, reducing the chances of credential reuse across machines. All configurations were applied without service disruption, demonstrating that these hardening measures are both practical and production-safe when applied through a structured, phased approach. Overall, these controls have laid a strong security foundation aligned with NSA, CIS, and Microsoft best practices, and they prepare the environment for further enhancements such as Privileged Access Management, Just-in-Time access, and Zero Trust implementation.