Active Directory Hardening

# Securing Authentication Methods:

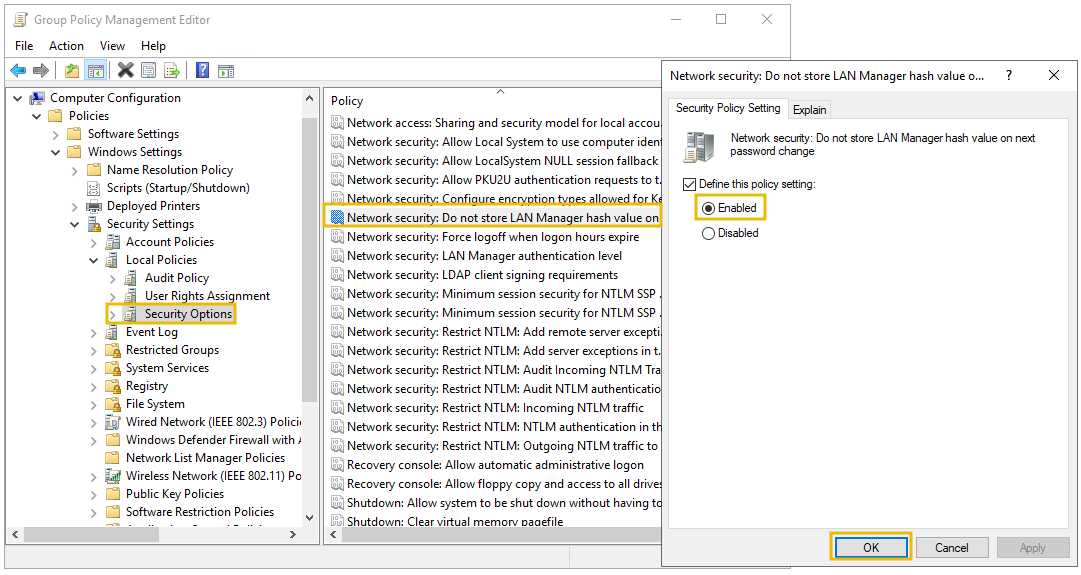
## LAN Manager Hash:

User Password Hashes, LAN Manager hash (LAM) and Windows NT hash are stored in AD. The LM hash is relatively weaker than the NT hash and prone to Brute force attack.

Recommendation: Prevent Windows from storing the password’s LM hash.

### Action:

|  |
| --- |
| Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > double click Network security - Do not store LM hash value on next password change policy > select "Define policy setting" |



* Check!

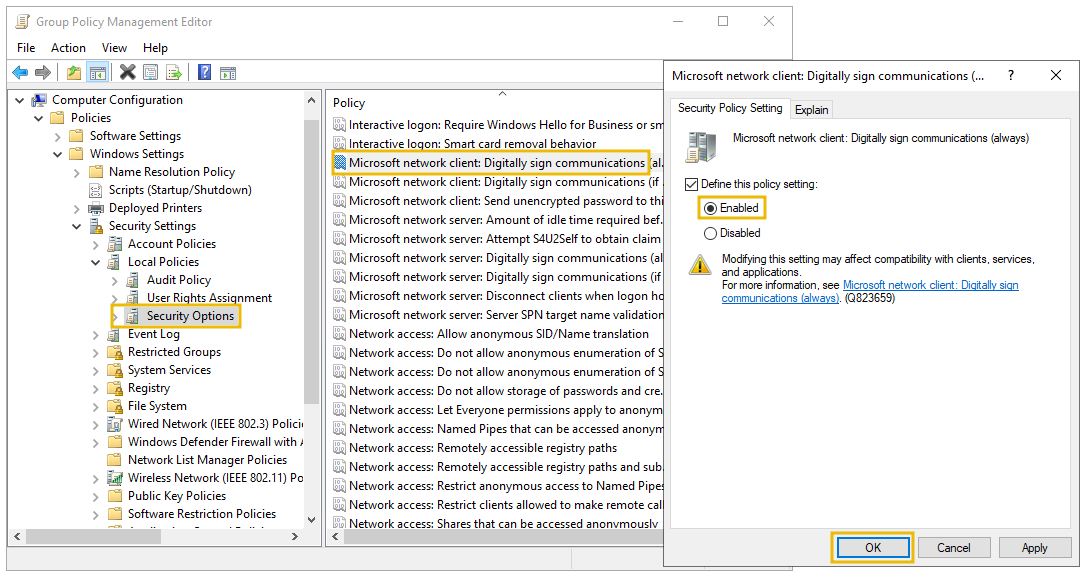
## SMB Signing:

SMB is a Microsoft-based file and printer communication protocol. It is prone to MiTM attack, that may result in modification of SMB traffic in transit, if not the signing is enabled. SMB packet signing ensures the integrity of data for both client and server.

Recommendation: Enable SMB packet signing.

Action:

|  |
| --- |
| Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > double click Microsoft network server: Digitally sign communication (always) > select Enable Digitally Sign Communications |



* Check!

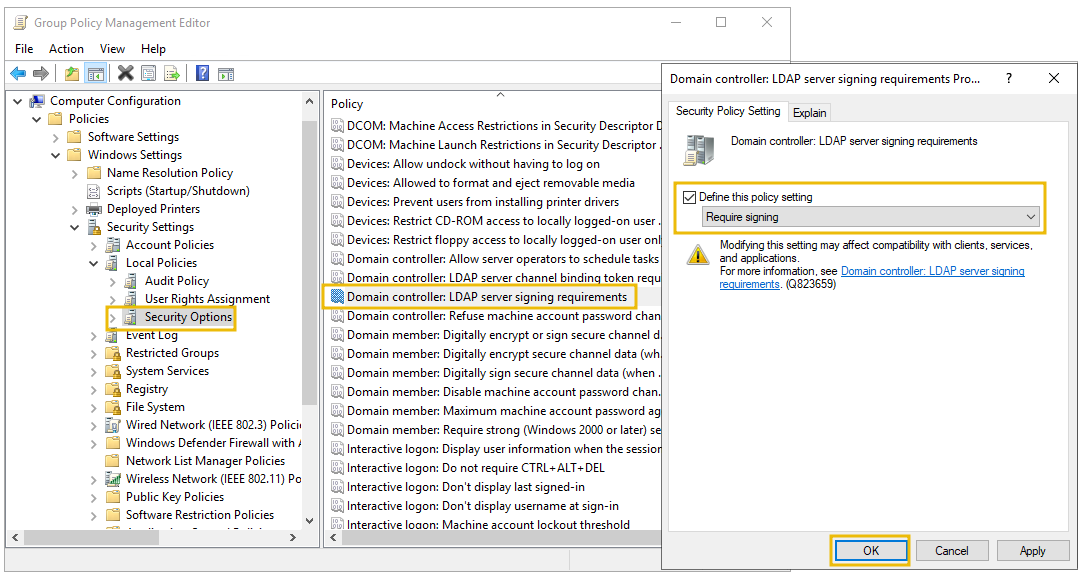
## LDAP Signing:

LDAP is used to locate and authenticate resources on the Network. LDAP is targeted with MiTM and replay attack using custom LDAP request. LDAP Signing is a Simple Authentication and Security Layer (SASL) property that allows only signed LDAP requests and reject plain text or non SASL requests.

Recommendation: Enable LDAP Signing

Action:

|  |
| --- |
| Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Domain controller: LDAP server signing requirements > select Require signing from the dropdown |



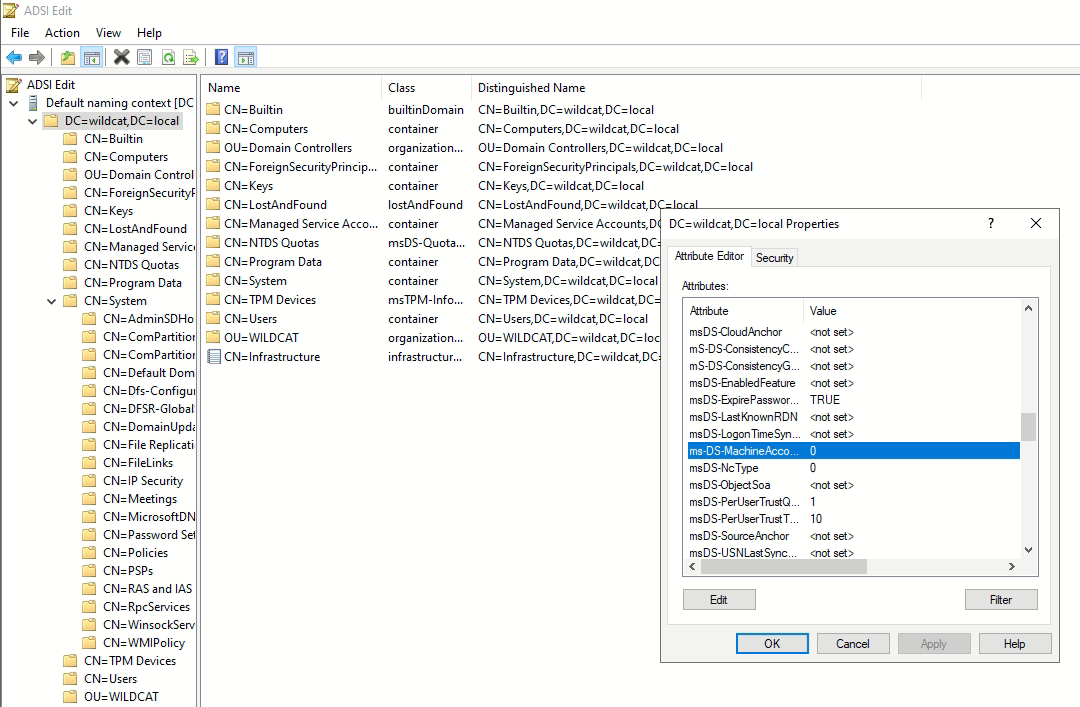
* Check!

Password Rotation:

Password Policies:

## Unprivileged users can add computer accounts to the domain:

Disable “ms-DS-Machine-Account Quota” accesing the ADSI Edit tool. First connect to the Domain from the ADSI tool > right click on the “DC=…, DC=local” and find the attribute and set it to 0.

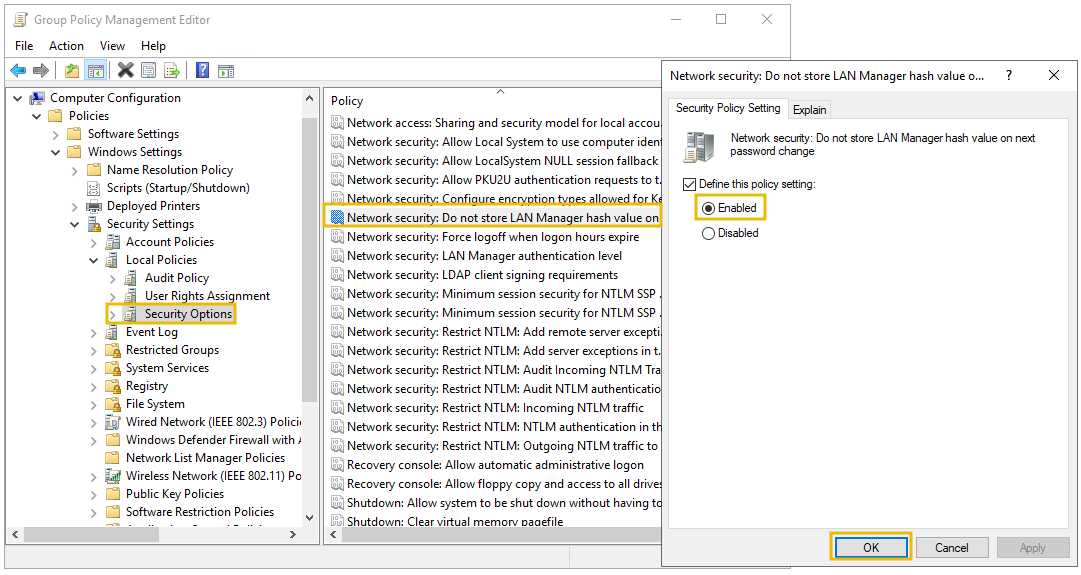


## LAN Manager Hash

The user account password for Windows isn't stored in clear text; instead, it stores passwords with two types of hash representation. When the password for any user account is changed or set with fewer than 15 characters, both LM hash (LAN Manager hash) and NT hash (Windows NT hash) are generated by Windows and can be stored in AD. The LM hash is relatively weaker than the NT and is prone to a fast brute-force attack. The best recommendation is to prevent Windows from storing the password's LM hash. You can access it through the following:

### Action:

Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > double click Network security - Do not store LM hash value on next password change policy > select "Define policy setting"



REF:

https://tryhackme.com/room/activedirectoryhardening

https://book.hacktricks.xyz/windows-hardening/active-directory-methodology