RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: TECH-F02

Securing Active Directory Correctly

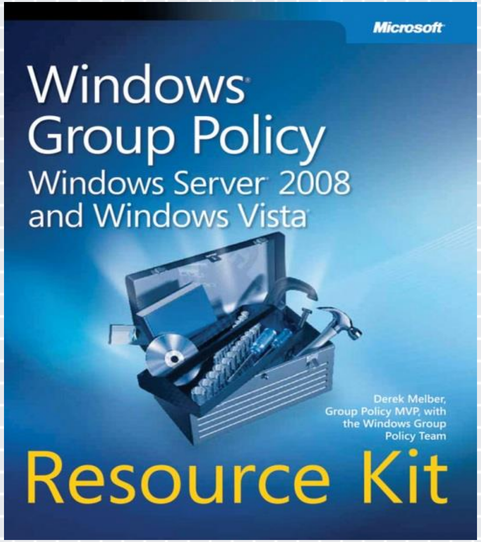
Derek Melber, MVP

Technical Evangelist
ManageEngine
@derekmelber

#RSAC

About Your Speaker

- Derek Melber, MCSE & MVP (Group Policy and AD)
  - derek@manageengine.com
- Global Active Directory Seminars
  - Monitoring and Auditing AD
  - Securing AD Delegations
  - Recovering AD Modifications and Deletions
- Online Resources
  - ManageEngine Active Directory Blog
  - www.auditingwindowsexpert.com
- Publications
  - Group Policy Resource Kit – MSPress


Microsoft
Windows Group Policy
Windows Server 2008 and Windows Vista
Derek Melber, Group Policy MVP, with the Windows Group Policy Team
Resource Kit

Agenda

- Active Directory Delegation is Configured Properly
- Anonymous Connections are Protected
- Authentication is Secured Properly
- Password Policy is Configured Securely

Active Directory Delegation

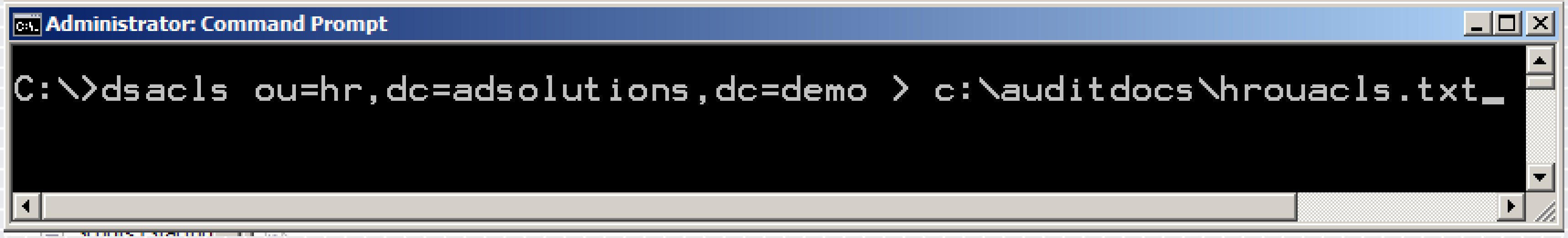
- Ability for AD admin to grant control over AD objects
- Typically done to Jr Admins, managers, etc
- Provides control over AD, but only in limited fashion
- Delegation is not “obvious” using Microsoft tools
- Incorrect delegations could be granted very easily

Active Directory Delegation

- Delegation for administration of AD objects
  - Users
    - Create or delete
    - Modify properties
    - Enable/Disable
    - Reset password
    - Unlock
  - Groups
    - Creation, deletion, modification
    - Group membership
  - Computers
    - Create or delete

Active Directory Delegation

- Verify AD Delegations by using dsacls



```
C:\>dsacls ou=hr,dc=adsolutions,dc=demo > c:\auditdocs\hrouacls.txt
```

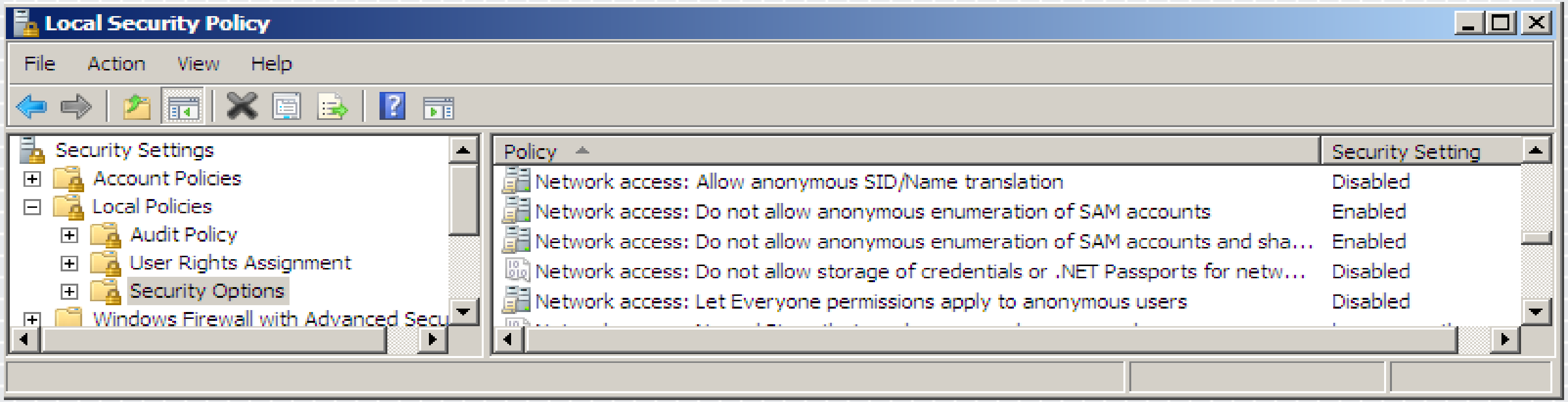
Anonymous Connections

- Anonymous access can grant too much access…
  - To shared folders
  - Users and their properties
- Anonymous access is no longer needed for most apps
- Microsoft provides controls, but not highly noted
- Windows 2000 is still vulnerable!

Anonymous Connections

- Clean out Pre-Windows 2000….. Group
  - At install Everyone “could” be placed into this group
- Ensure all 4 anonymous security settings are correct
  - Network access: Allow anonymous SID/Name translation
  - Network access: Do not allow anonymous enumeration of SAM accounts
  - Network access: Do not allow anonymous enumeration of SAM accounts and shared folders
  - Network access: Let Everyone permissions apply to anonymous users

Anonymous Connections



Policy	Security Setting
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and sha...	Enabled
Network access: Do not allow storage of credentials or .NET Passports for netw...	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled

Use of LAN Manager Authentication

- LAN Manager is a legacy authentication protocol
- LAN Manager (LM) was designed for Windows 3.11
  - (Do you remember what this OS version was called?)
- LM is easily cracked with the correct information exposed
- Eliminating LM can be difficult, but not impossible
  - Could break legacy applications… which is major issue

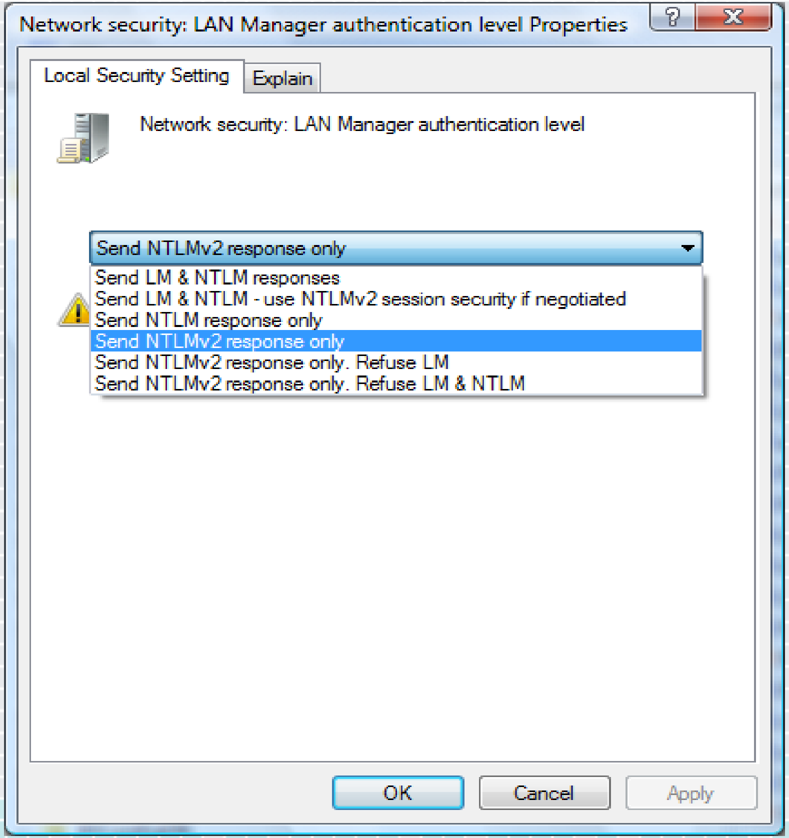
LMCompatibilityLevel

- 0 and 1
  - Clients use LM and NTLM authentication and never use NTLMv2 session security.
  - Domain controllers accept LM, NTLM, and NTLMv2 authentication.
  - Client does not use NTLMv2 auth
- 2
  - Clients use NTLM authentication only and use NTLMv2 session security if the server supports it.
  - Domain controllers accept LM, NTLM, and NTLMv2 authentication.
  - Client refuses to send LM response
- 3
  - Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it
  - Domain controllers accept LM, NTLM, and NTLMv2 authentication.

LMCompatibilityLevel

- 4
  - Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it.
  - Domain controllers refuse LM and accept only NTLM and NTLMv2 authentication.
- 5
  - Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it
  - Domain controllers refuse LM and NTLM (they accept only NTLMv2 authentication).

Use of LAN Manager Authentication



Network security: LAN Manager authentication level Properties

Local Security Setting | Explain

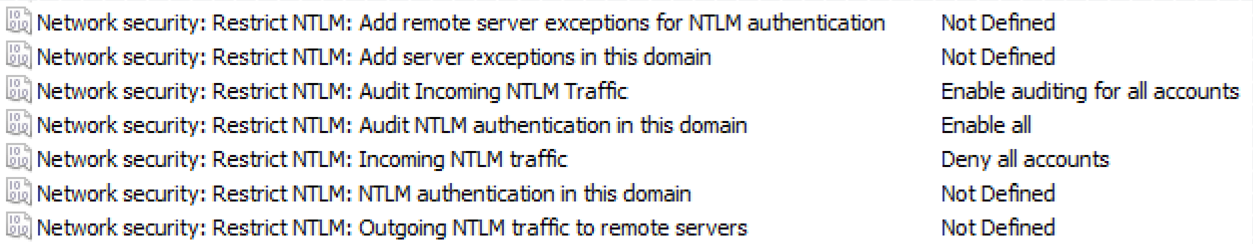
Network security: LAN Manager authentication level

Send NTLMv2 response only

- Send LM & NTLM responses
- Send LM & NTLM - use NTLMv2 session security if negotiated
- Send NTLM response only
- Send NTLMv2 response only
- Send NTLMv2 response only. Refuse LM
- Send NTLMv2 response only. Refuse LM & NTLM

Restricting NTLM Authentication Traffic

- New Group Policy Controls (Server 2003+)
- Detailed control over NTLM
- Audit or restrict
- Incoming or outgoing traffic

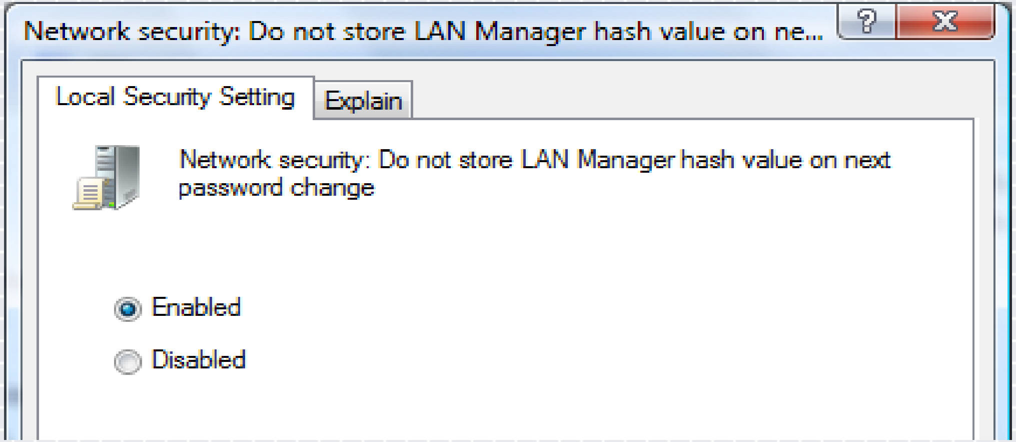


Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Enable auditing for all accounts
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Enable all
Network security: Restrict NTLM: Incoming NTLM traffic	Deny all accounts
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined

Storage of LM Hash

- LM is a very weak authentication protocol
- LM hash is not required
- LM hash can be stored in AD and local SAM
- Obtaining LAN Manager hash is easy way to crack passwords

Storage of LM Hash



Network security: Do not store LAN Manager hash value on ne...

Network security: Do not store LAN Manager hash value on next password change

● Enabled

○ Disabled

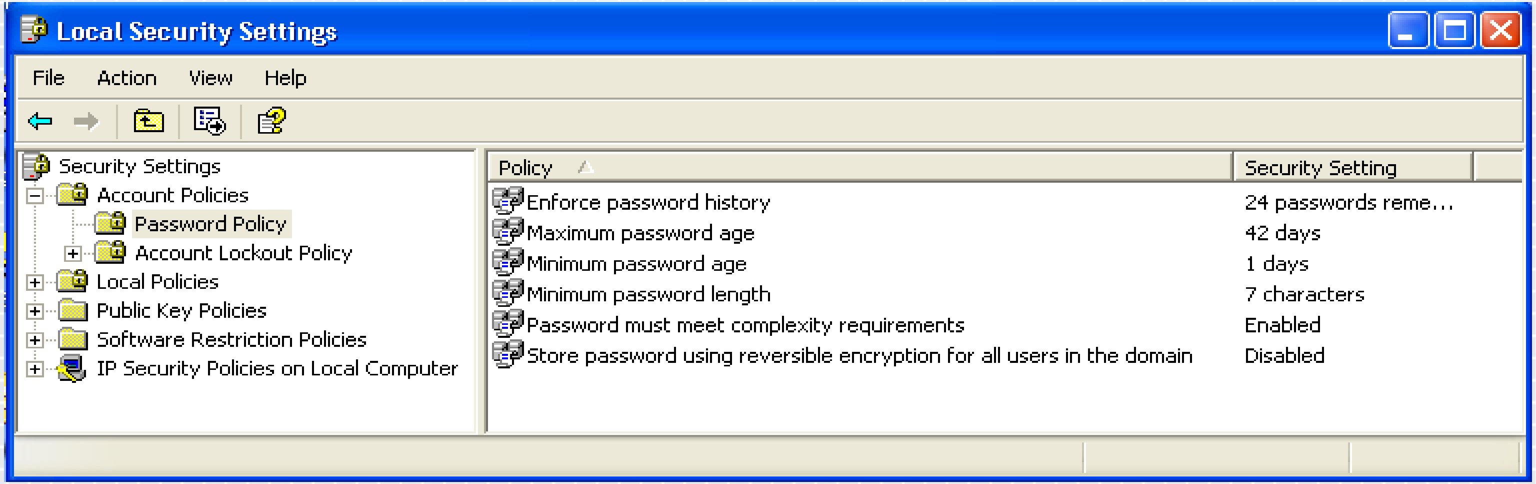
Password Policy

- Password policy controls structure of user password
- Password policy is “rarely” if “ever” understood and configured properly!
- A weak or incorrect password policy could leave your organization completely exposed!
- Approximately 1 out of every 100 auditors correctly analyze these configurations

Password Policy

- Local SAM (Servers and Desktops)
- Active Directory (Domain Controllers)
  - Domain User Accounts
  - Local SAM user accounts
- Fine-Grained Password Policies
  - Provide granular control of passwords to different users
  - Must have the correct environment configured

Password Policy



Policy	Security Setting
Enforce password history	24 passwords reme...
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

Apply What You Learned

- How to Properly Configure Active Directory Delegation
- Ensured Anonymous Connections are Protected
- Properly Secured AD Authentications
- Analyzed and Configured the Password Policy Correctly

Resources

- derek@manageenginecom
- Active Directory blog on www.manageengine.com
- www.auditingwindowsexpert.com
- www.windowsecurity.com
- www.windowsnetworking.com
- The Group Policy Resource Kit (MSPress)

Thank you!

Questions?

Derek Melber

derek@manageengine.com