
ManageEngine
IT Management, Simplified
Real-time IT management solutions for the new speed of business

# Security Hardening:

# Passwords and Authentication

Derek Melber, MVP

derek@manageengine.com

# About Your Speaker

# Derek Melber, MCSE & MVP (Active Directory and GP)

**derek@manageengine.com**

- **www.manageengine.com resources**
  - ManageEngine “Active Directory” Blog
  - Security Hardening Website
- Other useful resources
  - Twitter: @derekmelber
  - www.windowsecurity.com
  - www.derekmelber.com
  - Group Policy Resource Kit – MSPress

# Agenda

- Password Policy
- Authentication Protocols
- Anonymous Authentication

# Password Policy

# Password Policy Defined

- Default Domain Policy contains default Password Policy
  - Password Policy
  - Account Lockout Policy
  - Kerberos Policy
- Password Policy for domain users must be in GPO linked to domain
  - Can only be one Password Policy per domain using GP
- Password Policy in GPO linked to OU only effects local users

# Reporting on Current Password Policy

- GPO reports fail to give current Password Policy
- Tools to report on current Password Policy
  - Secpol.msc
  - GPMC – Group Policy Results
  - Dumpsec (portion)
  - Net accounts (portion)
  - ADManager Plus

# Configuring Appropriate Password Policy

- Need to defend against attacks
  - Dictionary
  - Brute force
  - Rainbow table
- Length is most important factor for secure password!
  - Ideally password length should be over 20 characters
  - Use passphrases to help generate long passwords

# More Than One Password Policy For the Domain?

- Fine Grained Password Policies
  - Windows Server 2008 and greater
  - Configure using ADSIEdit
  - Still limited to options contained in GP

# Reporting Fine Grained Password Policy

- Tools
  - Manually using ADSIEdit
  - PowerShell

# Monitoring Password Policy Changes

- ADMP
  - Report
    - Advanced GPO Reports – Password Policy Changes
  - Alert
    - GPO Alert
    - Specify associated GPOs from current Password Policy GPOs

# Monitoring Fine Grained Password Policy Changes

- ADMP
  - Report
    - Profile Based Reports – Advanced AD Object Audit – Password Settings Object Changes
  - Alert
    - Password Settings Object Changes Report

# Authentication Protocols

# Available Authentication Protocols

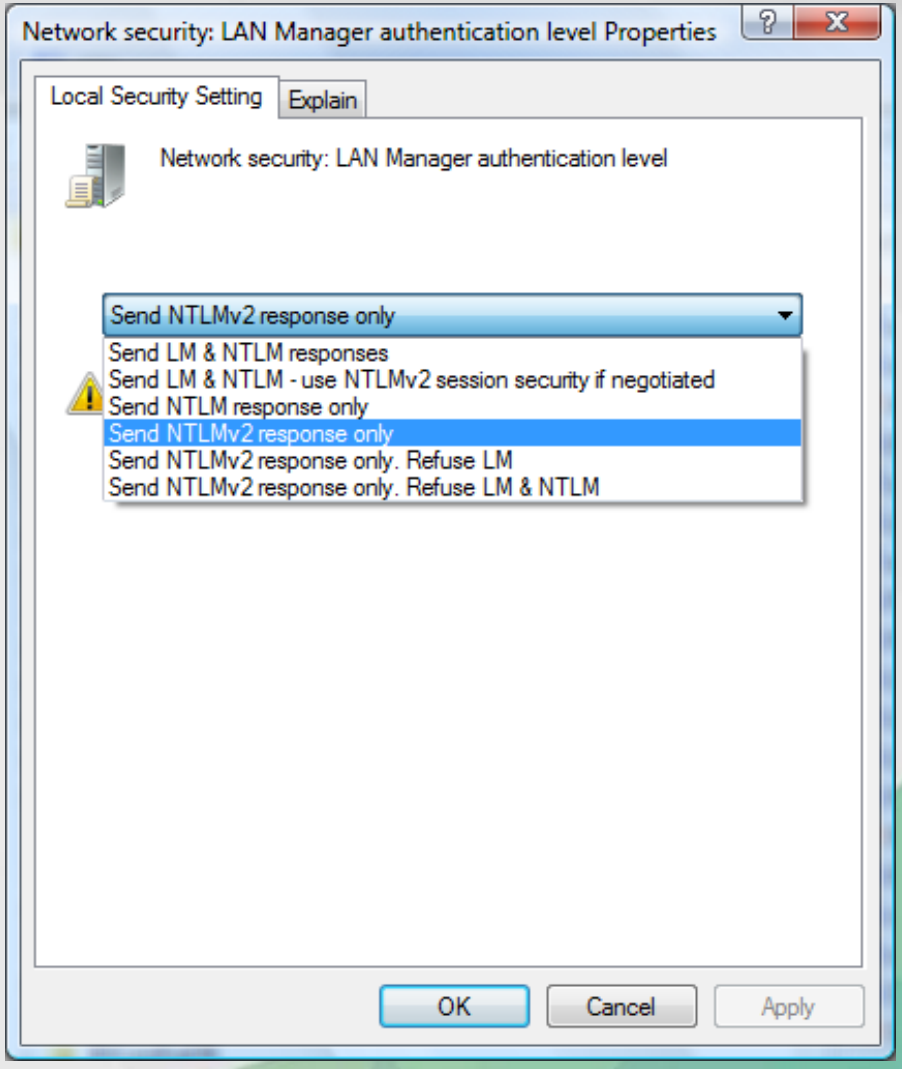
- Kerberos
  - Mutual authentication
  - Domain controllers authenticate using Kerberos Distribution Centers
  - No portion of the password is ever transmitted over the network
  - Attackers are prevented from capturing and replaying packets
- NTLMv2
  - Mutual authentication
  - No portion of the password is even transmitted over the network
  - Allowed 128 character length passwords

# Available Authentication Protocols

- NTLM
  - Introduced with Windows 3.1
  - Same as LM
- LM
  - First introduced in Windows 3.11
  - Only upper case alphas supported
  - Character set is limited to 142 characters
  - Maximum length of password is 14 characters
  - Algorithm breaks password into two 7 character chunks
  - Algorithm uses a cryptographic one-way function

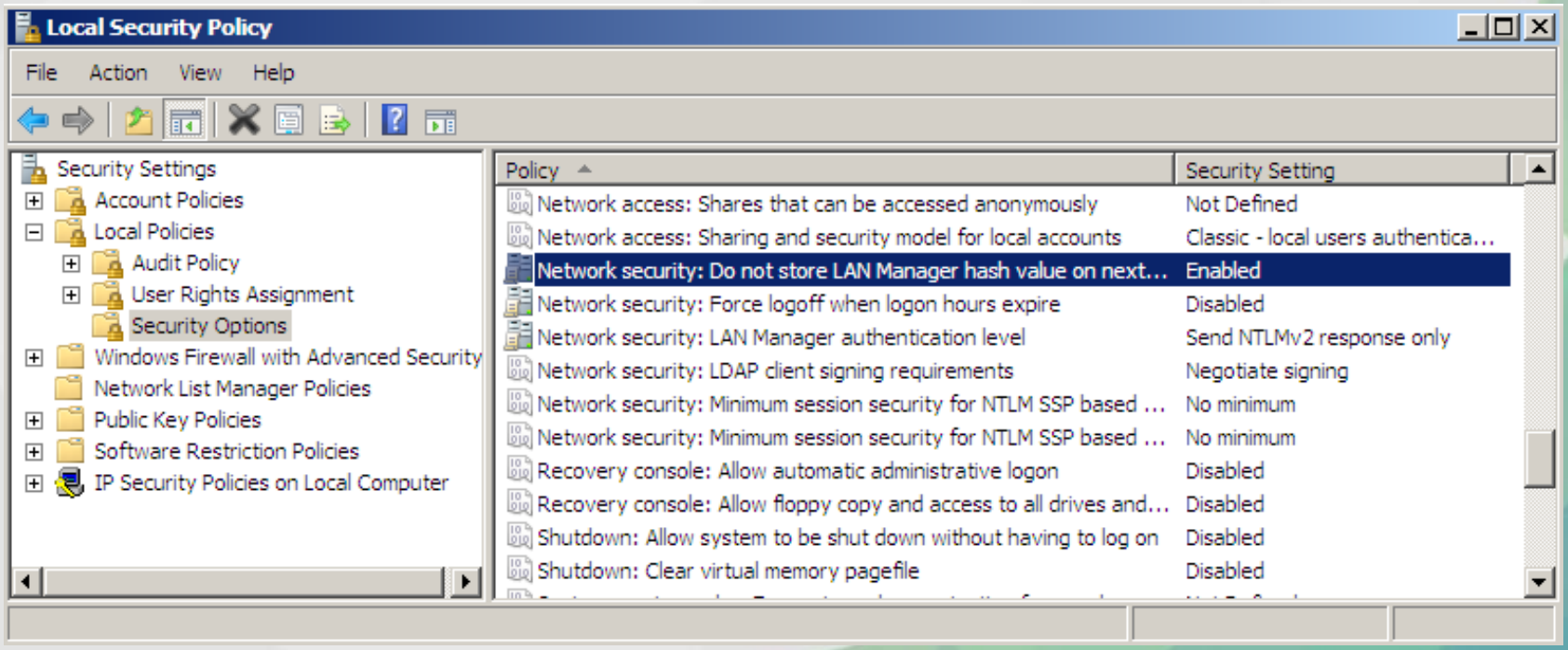
# LANManager Authentication Protocols

- Allow LM Authentications
- Configured using Group Policy
  - Registry modification
  - LMCompatibilityLevel
  - Only “Refuse LM” options are secure



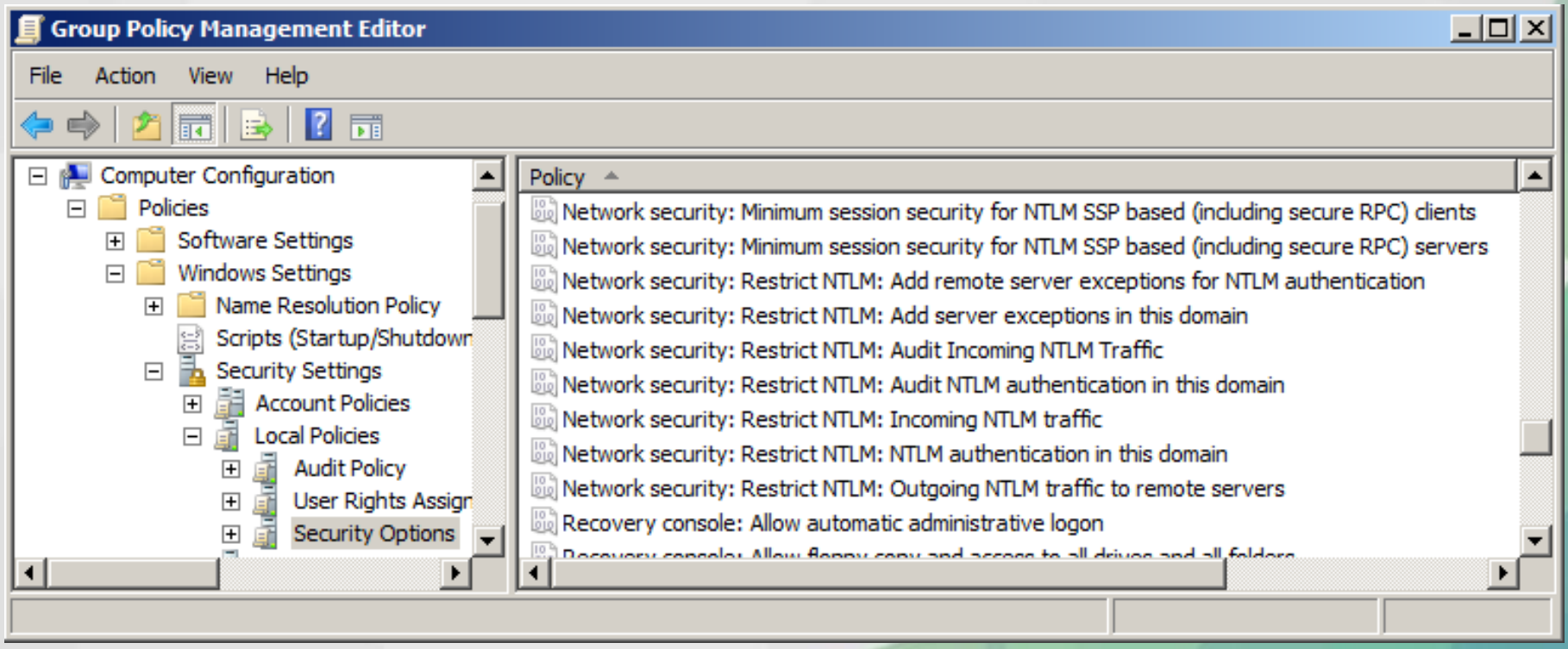
# LANManager Authentication Protocols

- Storage of LM Hashes
- Configured using Group Policy



# NTLM Authentication Protocol Controls

- Updated for Windows 7/Windows Server 2008 R2



# Restricting LM Authentication Protocol

- Deny 100% with Group Policy
  - Causes issues with user accounts that require LM/NTLM
  - Typically include legacy services
- Deny all but services and service accounts
  - Enforce minimum password length for domain users to above 14 characters
  - Allow service accounts to use password less than 14 characters

# Reporting LM Authentication Protocol

- Tools
  - Regedit (manually on each and every computer)
  - Secpol.msc

# Monitoring Use of LM Authentication Protocol

- Tools
  - Group Policy w/ Event Viewer (NTLM Log)
  - ADAP (Report and Alert)
  - Event Log Analyzer

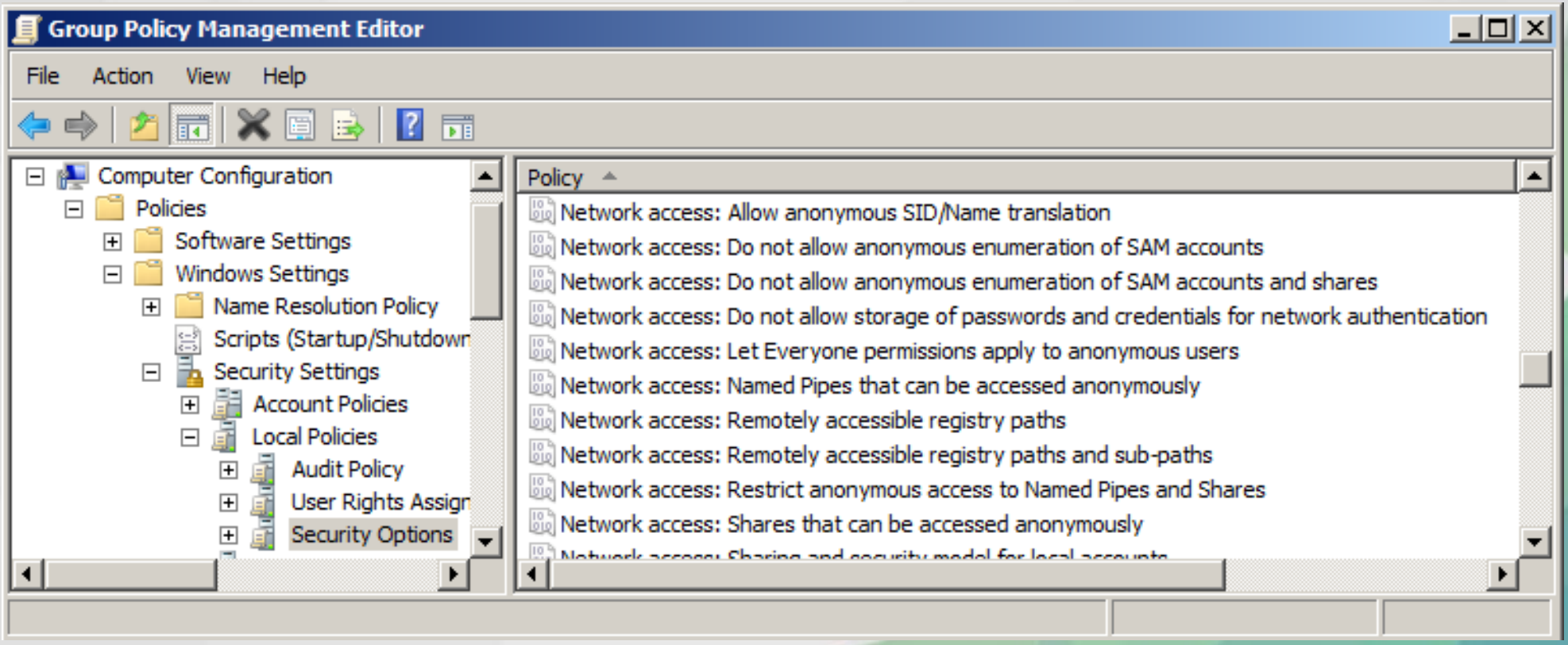
# Anonymous Authentication

# Anonymous Authentication Basics

- Designed to allow computer to computer communication
- IPC$ share on each computer is communication gateway
  - Net use \\computername\ipc$ “” /user:””
- Anonymous connections allow for “null user” access
  - Object properties
  - List shares

# Anonymous Authentication Controls

- Anonymous access is controlled using Group Policy



# Reporting on Anonymous Authentication

- Tools
  - Manually using Regedit
  - Secpol.msc

# Summary

# Summary

- Password Policy
- Authentication Protocols
- Anonymous Authentication

Thank you!

# Questions?

Derek Melber
derek@manageengine.com