RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CRWD-R04

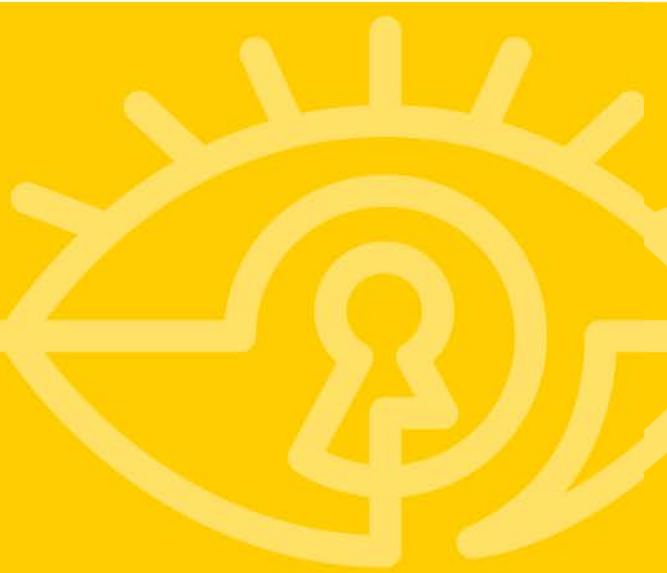
Top 10 Security Hardening Settings for Windows Servers and Active Directory

Derek Melber
Technical Evangelist – ADSolutions
ManageEngine
@derekmelber

#RSAC

Agenda

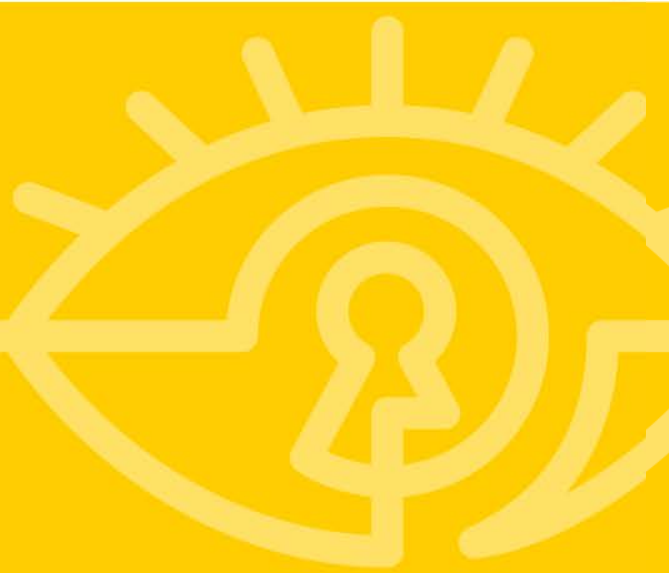
- Traditional security hardening
- Top 10 security settings
- Next-gen security hardening
- Security hardening resources



Traditional security hardening

Traditional security hardening

- Goal is to get all servers to a secure state.
- Typically use Microsoft or other industry “best practice.”
- Often Group Policy is used to configure security.
- Once configurations are complete, task is considered complete, too.



Top 10 security settings

1. User accounts with non-expiring passwords

- Issues
  - Infinite time to be hacked.
  - All internal users can determine these accounts.
  - Resetting passwords at scheduled intervals improves security.
    - Forces attackers to have time limit to break into account.
    - Compromised accounts need to be re-compromised.

1. User accounts with non-expiring passwords

- Solutions
  - All user accounts need to have expiring passwords:
    - IT
    - Developers
    - Help desk
    - Executives
  - Service accounts...more later.

2. User accounts that never logged in

- Issues
  - Accounts have “new user password.”
  - All employees know “new user password.”
  - Any employee could log on to these accounts.
  - Access and privileges are already granted at time of creation.

2. User accounts that never logged in

- Solutions
  - Delete user accounts that will never be used.
  - Report on all user accounts that are not logged into regularly.
  - Do not use same “new user password” for all new user accounts.
  - Implement a random password generator for new user accounts.

3. Default privileged groups need evaluation

- Issues
  - Domain level groups:
    - Domain Admins
    - Administrators
    - DNSAdmins
    - Etc.
  - Forest level groups:
    - Enterprise Admins
    - Schema Admins

3. Default privileged groups need evaluation

- Solutions
  - Verify group membership regularly.
  - Use tool that can get group members recursively.
  - Use least privilege concepts.

4. Application and custom privileged groups need evaluation

- Issues
  - Microsoft applications:
    - SQL
    - Exchange
    - Sharepoint
    - Etc.
  - Third party applications

4. Application and custom privileged groups need evaluation

- Solutions
  - Document all privileged groups.
  - Verify group membership regularly.
  - Use tool that can get group members recursively.
  - Use least privilege concepts.

5. Server-based user rights

- Issues
  - Provide privileges over computer where user rights are assigned.
  - User rights supercede resource access.
  - User rights can allow inappropriate access.
  - User rights can allow denial of service attacks.

5. Server-based user rights

- Solutions
  - Verify user rights using appropriate tool – secpol.msc.
  - Use Group Policy to standardize and deploy user rights settings.
  - Use least privilege concepts.

6. Active Directory delegations

- Issues
  - Delegations provide privileged access to AD objects:
    - Resetting user passwords
    - Creating groups
    - Modifying group membership
  - Delegations are difficult to report.
  - Delegations can be difficult to remove.

6. Active Directory delegations

- Solutions
  - Verify delegations on all OUs and domain – dsacls.
  - Use least privilege concepts.
  - Use third party tool for delegations:
    - Proxy user
    - Easier and increased delegations
    - Track all activity and actions

7. Group Policy delegations

- Issues
  - Group Policy is integral to Active Directory.
  - Group Policy can decrease security providing access.
  - Group Policy can cause significant issues and consequences.
  - Delegations provide access over GPOs:
    - Creating for domain
    - Linking to domain, OU, site
    - Modifying GPO settings

7. Group Policy delegations

- Solutions
  - Use least privilege concepts.
  - User GPMC, GPMC scripts, or PowerShell to obtain delegations.

8. Service accounts

- Issues
  - Service accounts are granted privileges at install or configuration.
  - Service accounts often have non-expiring passwords.
  - Service accounts often have original passwords.
  - Service accounts are rarely monitored for access.

8. Service accounts

- Solutions
  - Associate all service accounts to servers where configured.
  - User long and strong passwords.
  - Configure accounts to only be able to log on to specified computers.
  - Configure accounts to not be able to change own password.

9. Password policy

- Issues
  - Controls domain and local user password parameters.
  - Most password policy settings are weak.
  - Password policy changes are difficult to “see.”
  - Password policy is misunderstood in GPOs.
  - Fine-grained password policies are rarely used.

9. Password policy

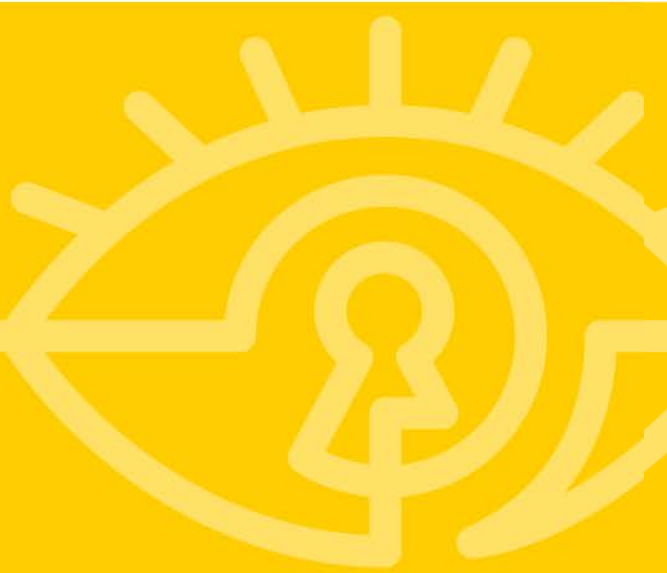
- Solutions
  - Use correct tool(s) to report on current password policy – secpol.msc.
  - Ensure password policies in GPOs linked to OUs are not considered for domain users.
  - User fine-grained password policies or third party tool to have multiple password policies in same domain.
  - Use security concepts to set password parameters, not compliance.

10. Real-time monitoring of Active Directory changes

- Issues
  - Security settings change over time.
  - Security settings are hard to “see” and report.
  - Privileged accounts can alter security settings.
  - Security settings change to solve problems.
  - Without change monitoring of security settings, actual settings are unknown until manually checked.

10. Real-time monitoring of Active Directory changes

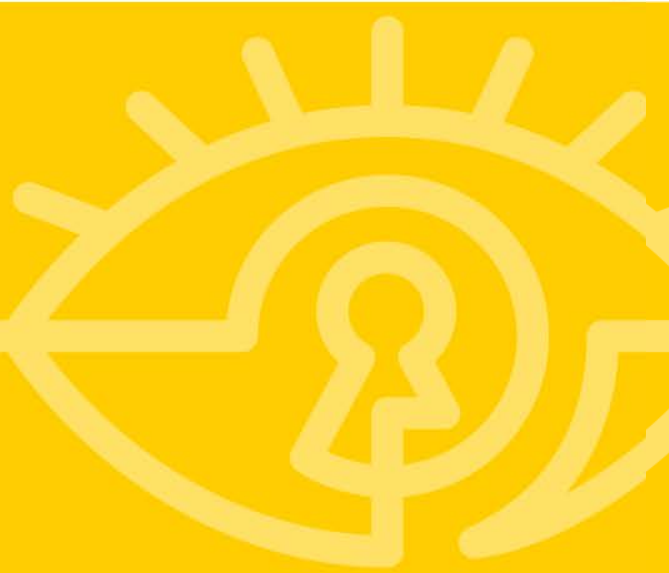
- Solutions
  - Establish a real-time change monitoring tool to track all Active Directory changes.
  - Generate reports to see “drift” of security settings.
  - Review reports often to ensure security is still in tact.



Next-gen security hardening

Next-gen security hardening

- Do not stop at traditional security hardening.
- “Security drift” can occur even within seconds of traditional security hardening.
- Establishing security is only good for that point in time.
- Monitoring changes ensures security is maintained.
- Alerting on security changes provides immediate notice of security changes.



Security hardening resources

After Conference Resources

- derek@manageengine.com
- ManageEngine Security Hardening web site
- Active Directory blog on www.manageengine.com
- Microsoft Security Compliance Manager

Apply security hardening concepts

- Immediately:
  - Ensure security for Active Directory is correct.
  - Determine which security settings should be improved.
  - Configure Active Directory, domain controllers, and Windows servers securely.
- After Active Directory is securely hardened:
  - Implement monitoring to track when any security change occurs.
  - Establish alerts so notifications are sent immediately when key settings change.

RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CRWD-R04

Top 10 Security Hardening Settings for Windows Servers and Active Directory

THANK YOU!

Derek Melber
Technical Evangelist – ADSolutions
ManageEngine
derek@manageengine.com