Top 25 Active Directory Security Best Practices

Provided by - Robert Allen with ActiveDirectoryPro.com

#1 Clean up Domain Admins Group ☐

- Don't login with a day to day account that is a member of the Domain Admins group
- Stop putting so many accounts in this group
- If DA access is needed, temporarily add it then remove from DA group

#2 Use at least Two Accounts ☐

- Use least privilege model, give permissions to only what is needed.
- Create regular account with no admin rights for logging into your computer to check email, surfing internet, etc.
- Create a secondary account for performing administrative tasks

#3 Secure the Domain Admin Account ☐

- Built in domain admins account should only be used for domain setup and recovery
- Set a 20+ character password and lock it in a vault
- No one should no the password or be using this account

#4 Disable Local Admin Account ☐

- Disable the local administrator account on every computers and use your domain individual account instead
- This is a well known account that attackers will try to compromise and often has the same password on every computer

#5 Use LAPS ☐

- If you are unable to disable the local administrator account you should use the Local Administrator Password Solution provided by Microsoft
- This will set a random unique password for every administrator account
- Password can be retrieved with Active Directory Users and Computers

#6 Use a Secure Admin Workstation ☐

- Use a dedicated Secure workstation for performing administrative tasks
- Daily use workstations are more vulnerable to compromise and should be assumed to be breached
- The secure admin workstation should not have internet access or be used for checking email
- Login to the secure admin workstation with your secondary account

#7 Enable Audit Policy Settings ☐

- Use group policy to set an audit policy on all computers
- Malicious activity often starts on end user devices so it is important to apply the audit policy to all computers.
- See full post for audit policy details

#8 Monitor AD Events for Compromise ☐

- Monitor event logs for signs of compromise and abnormal behavior.
- Monitor: changes to privileged groups, spike in bad password attempts, account lockouts, logon/logoff events, use of administrator accounts, disabled or removal of antivirus software

#9 Use Passphrases ☐

#10 Use Descriptive Security Groups ☐

- 8 character passwords with complexity is no longer secure, use passphrases instead
- Longer passwords are better, set a password policy that requires a minimum of 12 characters
- Train staff how to properly use passphrases

- Avoid generic security group names, they will often get used on various resources which lead to out of control permissions
- Create very specific group names, example IT-Helpdesk-ActiveDirectory, this will help prevent permissions from getting out of control

#11 Cleanup Old AD Accounts ☐

- Have a process in place to cleanup old user and computer account from Active Directory
- View step by step guide to identify and remove old accounts

#12 Keep DCs lean and clean ☐

- Domain controllers should have limited software and roles installed on them
- Use server core, it runs with no GUI
- More software and roles you install it increases the security risk, keep DCs lean and clean

#13 Patch & Vulnerability Scanning ☐

- Attackers are quick to exploit known vulnerabilities, you need to continuously scan and patch systems
- Don't forget to patch 3rd party programs
- Upgrade software that is no longer supported
- View the Top 6 Patch Management Software

#14 Use Secure DNS Services ☐

- You can block malicious traffic by using a secure DNS server, this will check the DNS lookup against a known list of BAD domains
- Popular services are: Quad9, OpenDNS and Comodo Secure DNS

#15 Run Latest Operating System ☐

- Each new version of Windows includes built in security features and enhancements
- Staying on the latest OS will help to increase overall security

#16 Use Two Factor Authentication ☐

- It's easy for attackers to compromise accounts, which can allow remote and unauthorized access
- Two factor authentication should be used for all remote access
- Popular two factor solutions: DUO, RSA, Microsoft MFA

#17 Monitor DHCP Logs ☐

- You need to know what is connecting to your network
- A simple way to identify unauthorized devices is by checking the DHCP logs, look for hostnames that you do not recognize. Systems that do not follow you naming convention should be easy to spot

#18 Monitor DNS Logs ☐

- DNS logs can be used to identify malicious DNS lookups
- You will need to enable the Windows DNS debug logs, steps provided in full post
- Look for odd domains that are random in characters, example edsdgjwxngrqw.3fdsco.com

#19 Use ADFS & Azure Security ☐

- Take advantage of latest ADFS & Azure security features

#20 Use Office 365 Secure Score ☐

- Secure score analyzes your office 365 organization security based on activity and security settings

- Microsoft continues to develop and provide security enhancements to both of these services

- It provides a detailed list of what was scored and recommended actions to fix these issues
- Requires a premium or enterprise subscription

#21 Plan for Compromise

- Have a response plan on how to handle a cyber attack
- See the NIST Computer Security Incident Handling Guide for guidelines on incident handling

#22 Document Delegation to AD

- Control access to resources by using Security Groups then delegate rights to those groups
- Document your delegation, know what groups are used on what resources and communicate to IT staff

#23 Lock Down Service Accounts

- Service accounts are used to run executables, tasks, services, authentication and so on
- These accounts often end up with too much permissions and have password that never expire
- See the full post for a complete list of tips for locking down service accounts

#24 Disable SMBv1

- SMBv1 is over 30 years old, Microsoft says stop using it
- Many viruses can spread and exploit flaws in SMBv1
- Beginning with Windows 10 fall creator update, SMBv1 will be disable by default
- Older OS version can disable in registry

#25 Use Security Baselines

- Default installs are not secure, use secure benchmarks and baselines to secure default settings
- These can often be deployed with group policy
- Two good resources for security baselines, Microsoft Security Compliance Toolkit and CIS SecureSuite

Link to full post -> Top 25 Active Directory Security Tips

Send feedback by posting a comment on my site or sending me an email
robert@activedirectorypro.com