Active Directory Security Checks (by Sean Metcalf - @Pyrotek3)

General Recommendations

- Manage local Administrator passwords (LAPS).
- Implement RDP Restricted Admin mode (as needed).
- Remove unsupported OSs from the network.
- Monitor scheduled tasks on sensitive systems (DCs, etc.).
- Ensure that OOB management passwords (DSRM) are changed regularly & securely stored.
- Use SMB v2/v3+
- Default domain Administrator & KRBTGT password should be changed every year & when an AD admin leaves.
- Remove trusts that are no longer necessary & enable SID filtering as appropriate.
- All domain authentications should be set (when possible) to: "Send NTLMv2 response onlyrefuse LM & NTLM."
- Block internet access for DCs, servers, & all administration systems.

Protect Admin Credentials

- No "user" or computer accounts in admin groups.
- Ensure all admin accounts are "sensitive & cannot be delegated".
- Add admin accounts to "Protected Users" group (requires Windows Server 2012 R2 Domain Controllers, 2012R2 DFL for domain protection).
- Disable all inactive admin accounts and remove from privileged groups.

Protect AD Admin Credentials

- Limit AD admin membership (DA, EA, Schema Admins, etc.) & only use custom delegation groups.
- ‘Tiered’ Administration mitigating credential theft impact.
- Ensure admins only logon to approved admin workstations & servers.
- Leverage time-based, temporary group membership for all admin accounts

Protect Service Account Credentials

- Limit to systems of the same security level.
- Leverage “(Group) Managed Service Accounts” (or PW >20 characters) to mitigate credential theft (kerberoast).
- Implement FGPP (DFL =>2008) to increase PW requirements for SAs and administrators.
- Logon restrictions – prevent interactive logon & limit logon capability to specific computers.
- Disable inactive SAs & remove from privileged groups.

Protect Resources

- Segment network to protect admin & critical systems.
- Deploy IDS to monitor the internal corporate network.
- Network device & OOB management on separate network.

Protect Domain Controllers

- Only run software & services to support AD.
- Minimal groups (& users) with DC admin/logon rights.
- Ensure patches are applied before running DCPromo (especially MS14-068 and other critical patches).
- Validate scheduled tasks & scripts.

Protect Workstations (& Servers)

- Patch quickly, especially privilege escalation vulnerabilities.
- Deploy security back-port patch (KB2871997).
- Set Wdigest reg key to 0 (KB2871997/Windows 8.1/2012R2+): HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlSecurityProvidersWdigest
- Deploy workstation whitelisting (Microsoft AppLocker) to block code exec in user folders – home dir & profile path.
- Deploy workstation app sandboxing technology (EMET) to mitigate application memory exploits (0-days).

Logging

- Enable enhanced auditing
- “Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings”
- Enable PowerShell module logging (“*”) & forward logs to central log server (WEF or other method).
- Enable CMD Process logging & enhancement (KB3004375) and forward logs to central log server.
- SIEM or equivalent to centralize as much log data as possible.
- User Behavioural Analysis system for enhanced knowledge of user activity (such as Microsoft ATA).

Security Pro’s Checks

- Identify who has AD admin rights (domain/forest).
- Identify who can logon to Domain Controllers (& admin rights to virtual environment hosting virtual DCs).
- Scan Active Directory Domains, OUs, AdminSDHolder, & GPOs for inappropriate custom permissions.
- Ensure AD admins (aka Domain Admins) protect their credentials by not logging into untrusted systems (workstations).
- Limit service account rights that are currently DA (or equivalent).