Top 10 Active Directory Security Issues, Impact, & Remediation

Sean Metcalf
CTO, Trimarc
About

- Founder Trimarc (Trimarc.io), a professional services company that helps organizations better secure their Microsoft platform, including the Microsoft Cloud.
- Microsoft Certified Master (MCM) Directory Services
- Microsoft MVP
- Speaker: Black Hat, Blue Hat, Bsides DC, BSides Charm, BSides PR, DEF CON, DerbyCon
- Security Consultant / Researcher
- AD Enthusiast - Own & Operate ADSecurity.org (Microsoft platform security info)
Attackers Require...

- Account (credentials)
- Rights (privileges)
- Access (connectivity to resources)

Attacker Capability Depends on the Defender...
As an Attacker, Do I Need Domain Admin?

No.
Avenues to Compromise

- GPO permissions
  - Modify a GPO to own everything that applies it
- AD Permissions
  - Delegation a decade ago is still in place, so are the groups
- Improper group nesting
  - Group inception = innocuous groups with super powers
- Over-permissioned accounts
  - Regular users are admins
- Service account access
  - Domain Admins (of course!)
- Kerberos Delegation
  - Who really knows what this means?
- Password Vaults
  - Management issues (user accounts with admin rights, improper protection of server, ...)
- Backup Process
  - What servers backup Active Directory? How is this backup data protected?
In the Real World, Rights are Everywhere

- Workstation Admins have full control on workstation computer objects and local admin rights.
- Server Admins have full control on server computer objects and local admin rights.
- Often, Server Admins are Exchange Admins.
- Sometimes Server Admins have rights to Domain Controllers.
- Help Desk Admins have local admin rights and remote control on user workstations.
- Local admin accounts & passwords often the same among workstations, and sometimes the same among servers.
- “Temporary” admin group assignments often become permanent.
3rd Party Product Permission Requirements

- Domain user access
- Operations systems access
- Mistaken identity – trust the installer
- AD object rights
- Install permissions on systems
- Needs System rights
- Active Directory privileged rights
- Domain permissions during install
- More access required than often needed.
- Initial start/run permissions
- Needs full AD rights
3rd Party Product Permission Requirements

- Domain user access
- Operations systems access
- Mistaken identity – trust the installer
- AD object rights
- Install permissions on systems
- Needs System rights
- Active Directory privileged rights
- Domain permissions during install
- More access required than often needed.
- Initial start/run permissions
- Needs full AD rights
Common AD Security Issues

We find really interesting things...
1. Local Administrator Passwords Not Managed on Workstations or Servers

- Workstation build usually sets the standard organization Administrator password.
- Compromise one workstation to compromise them all

**Mitigation:**
Ensure local Administrator passwords regularly change on workstations and servers (using something like Microsoft LAPS).
## 2. Domain Password Policy

<table>
<thead>
<tr>
<th>Account Policies/Password Policy</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce password history</td>
<td>24 passwords remembered</td>
</tr>
<tr>
<td>Maximum password age</td>
<td>42 days</td>
</tr>
<tr>
<td>Minimum password age</td>
<td>1 days</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>7 characters (AD Default)</td>
</tr>
<tr>
<td>Password must meet complexity requirements</td>
<td>Enabled</td>
</tr>
<tr>
<td>Store passwords using reversible encryption</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
No account lockout since 1 password is used in authentication attempt for each user in the list (typically all or just admins) then the password spray tool pauses before moving onto the next password.
No account lockout since 1 password is used in authentication attempt for each user in the list (typically all or just admins) then the password spray tool pauses before moving onto the next password.
2. Domain Password Policy

Shorter passwords = more effective password spraying

Password Spraying against 1892 users
User ADSECLAB\Christopher.Kelly has the password Password1
User ADSECLAB\Cameron.Long has the password Password1
User ADSECLAB\Nicholas.Davis has the password Password1
User ADSECLAB\Connor.Moore has the password Password1
User ADSECLAB\Bryce.Torres has the password P@sswOrd
User ADSECLAB\Olivia.Bryant has the password P@sswOrd
User ADSECLAB\Victoria.Young has the password P@sswOrd
User ADSECLAB\Joseph.Rodriguez has the password P@sswOrd
User ADSECLAB\Audrey.Lee has the password Password99!
User ADSECLAB\Landon.Lewis has the password Password99!
User ADSECLAB\Blake.Carter has the password Password1234
User ADSECLAB\Alexis.Phillips has the password Password1
2. Domain Password Policy (improvement?)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Policy Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce password history</td>
<td>24 passwords remembered</td>
</tr>
<tr>
<td>Maximum password age</td>
<td>42 days</td>
</tr>
<tr>
<td>Minimum password age</td>
<td>1 days</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>8 characters</td>
</tr>
<tr>
<td>Password must meet complexity requirements</td>
<td>Enabled</td>
</tr>
<tr>
<td>Store passwords using reversible encryption</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Set to at least 12 characters, preferably 15.
At least use Fine-Grained Password Policies for Admins & Service Accounts

Also review Azure AD Password Protection for (on-prem) AD
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises
3. Default Domain Administrator Account SPN

- There is no good reason for admin accounts to have Kerberos SPNs.
- Attack:
  Kerberoad these accounts to own AD.

Kerberoad:
Offline password attack using a Kerberos service ticket requested as a user.
## 4. AD Admin Accounts: Old Passwords

<table>
<thead>
<tr>
<th>SamAccountName</th>
<th>Enabled</th>
<th>PasswordLastSet</th>
<th>Password Age (years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCCMsvc</td>
<td>Yes</td>
<td>11/14/2011 5:23:12 PM</td>
<td>7.9</td>
</tr>
<tr>
<td>VMWareAdmin</td>
<td>Yes</td>
<td>8/28/2012 10:23:41 AM</td>
<td>7.0</td>
</tr>
<tr>
<td>admAEdwards</td>
<td>Yes</td>
<td>1/12/2013 2:20:06 PM</td>
<td>6.5</td>
</tr>
<tr>
<td>VulnerabilityScanner</td>
<td>Yes</td>
<td>9/19/2015 4:43:19 PM</td>
<td>4.2</td>
</tr>
<tr>
<td>admBWalker</td>
<td>No</td>
<td>6/11/2017 10:14:08 AM</td>
<td>2.2</td>
</tr>
<tr>
<td>admCGriffin</td>
<td>Yes</td>
<td>3/1/2019 12:41:18 PM</td>
<td>0.5</td>
</tr>
</tbody>
</table>
4. Admin Accounts: Service Accounts in Domain Admins

- Service Accounts rarely actually need Domain Admin rights
- Better to delegate the required rights for the accounts.

Mitigation:
- Determine rights actually required.
- Delegate these rights.
- Remove from Domain Admins.
4. Admin Accounts: Old KRBTGT Account Password

- KRBTGT account is disabled but used for Kerberos Tickets.
- Password set when created & practically never changes.
- If an attacker gains knowledge of pw, Golden Tickets!!!

Mitigation:
- Change this password 2x every year (DoD STIG requirement)
5. DC GPOs: Domain Controllers with minimal event auditing

If Advanced Auditing is not configured on DCs, you are missing events required to potentially detect malicious activity.
5. DC GPOs: Server GPOs Linked to Domain Controllers

GPOs provide the capability to change security settings, update Administrators group membership, and install/run code.
5. DC GPOs: Server GPOs Linked to Domain Controllers

Only use GPOs dedicated to Domain Controllers, don’t link GPOs already linked to other OUs.
6. GPOs: Modify Rights to GPOs at Domain / DC Level

Only AD Admins should have modify rights on GPOs linked to the Domain/Domain Controllers.
7. Permissions: Domain Permission Delegation Issues
7. Permissions: AdminSDHolder Permission Delegation Issues

**Domain**: lab.trimarcresearch.com
**ObjectDN**: CN=AdminSDHolder,CN=System,DC=lab,DC=trimarcresearch,DC=com
**ActiveDirectoryRights**: TRDPROD\User Admins
**InheritedObjectClass**: All
**ObjectClass**: All
**AccessControlType**: Allow
**IsInherited**: False
**ObjectFlags**: None
**InheritanceFlags**: None
**PropagationFlags**: None

**Domain**: prod.trimarcresearch.com
**ObjectDN**: CN=AdminSDHolder,CN=System,DC=prod,DC=trimarcresearch,DC=com
**ActiveDirectoryRights**: TRDPROD\User Admins
**InheritedObjectClass**: All
**ObjectClass**: All
**AccessControlType**: Allow
**IsInherited**: False
**ObjectFlags**: None
**InheritanceFlags**: ContainerInherit
**PropagationFlags**: None
8. Admins Use Regular Workstations for AD Administration

1 workstation
30 accounts in the local Administrators group.
50 accounts w/ local admin via software management system.
20 accounts with control of the computer via security agent(s).

~ 100 accounts with effective admin rights on the workstation

How many GPOs apply to the workstation & how many accounts have modify rights?

Who has control of your workstation?
9. Kerberos Delegation

- Delegation = Impersonation
- **Kerberos Delegation:**
  - **Unconstrained:**
    Impersonate users connecting to service to ANY Kerberos service.
  - **Constrained:**
    Impersonate authenticated users connecting to service to SPECIFIC Kerberos services on servers.
  - **Constrained with Protocol Transition:**
    Impersonate any user to SPECIFIC Kerberos services on servers. (aka “Kerberos Magic”) 
  - **Resource-based Constrained Delegation:**
    Enables delegation configured on the resource instead of the account.
9. Kerberos Delegation

- Delegation = Impersonation

- **Kerberos Delegation:**
  - **Unconstrained:**
    Impersonate users connecting to service to ANY Kerberos service.
  - **Constrained:**
    Impersonate authenticated users connecting to service on servers.
  - **Constrained with Protocol Transition:**
    Impersonate any user to SPECIFIC Kerberos services.
  - **Resource-based Constrained Delegation:**
    Enables delegation configured on the resource instead.
10. Azure AD Connect

Permissions for the created AD DS account for express settings

The account created for reading and writing to AD DS have the following permissions when created by express settings:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replicate Directory Changes</td>
<td>Password sync</td>
</tr>
<tr>
<td>Replicate Directory Changes All</td>
<td></td>
</tr>
<tr>
<td>Read/Write all properties User</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties iNetOrgPerson</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Group</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Contact</td>
<td>Import and Exchange hybrid</td>
</tr>
</tbody>
</table>
10. Azure AD Connect

Permissions for the created AD DS account for express settings

The account created for reading and writing to AD DS have the following permissions when created by express settings:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replicate Directory Changes</td>
<td>Password sync</td>
</tr>
<tr>
<td>Replicate Directory Changes All</td>
<td></td>
</tr>
</tbody>
</table>

Protect your Azure AD Connect Server like a Domain Controller
BONUS: Accounts with Delegated Rights to AD

- Group membership
- AD delegated permissions
- Group Policy delegation
- Group Policy User Rights Assignments (DC GPOs)
Thanks Quest!

Q&A at the Quest booth 2149 right after this

Stop by and ask me anything
(Active Directory & Azure AD security)

Sean Metcalf (@Pyrotek3)
sean @ trimarcsecurity. com
TrimarcSecurity.com
www.ADSecurity.org