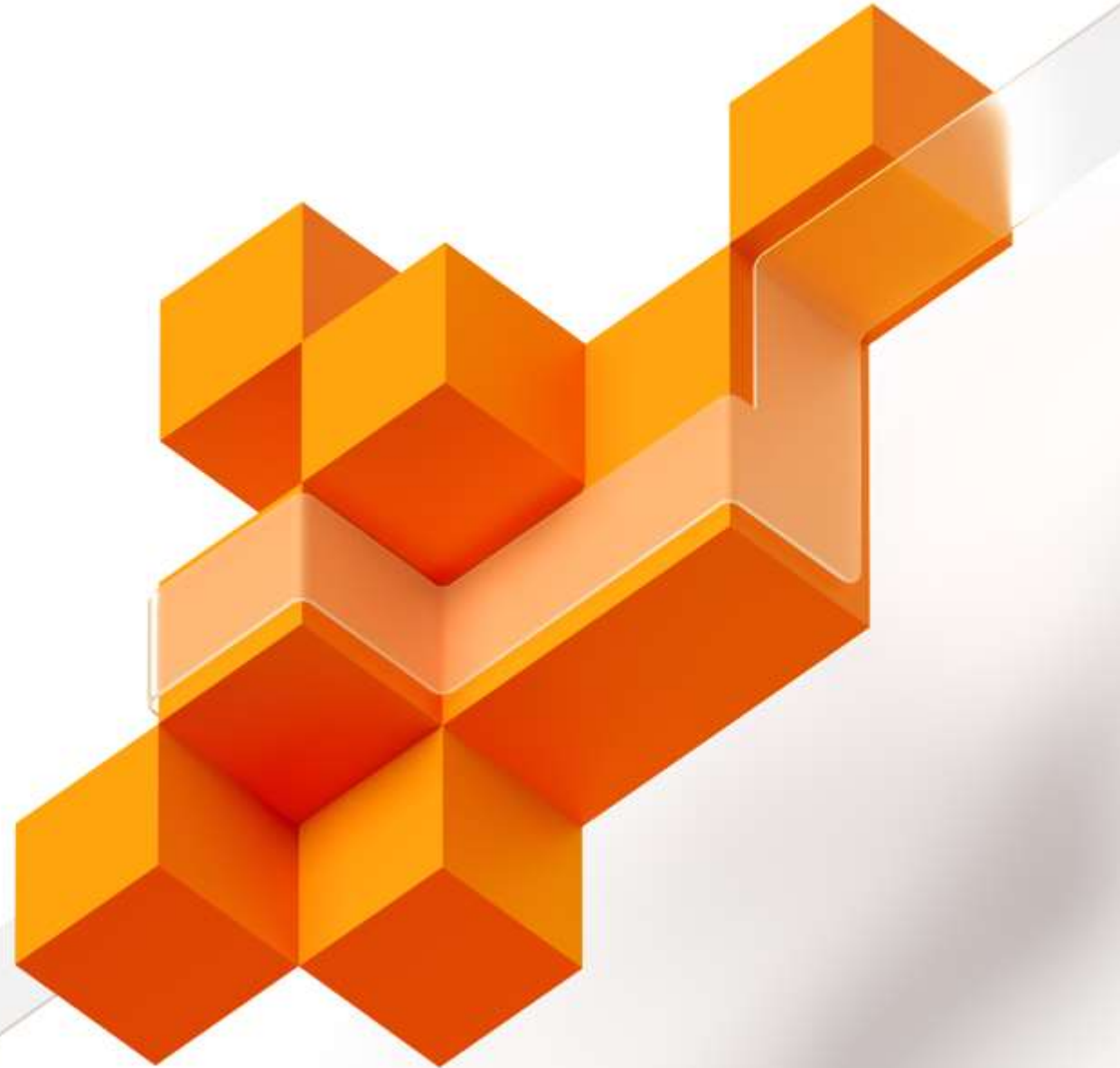




Microsoft Ignite





Top 10 Active Directory Security Issues, Impact, & Remediation

Sean Metcalf
CTO, Trimarc



About

- Founder Trimarc ([Trimarc.io](https://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 DC, BSides Charm, BSides PR, DEF CON, DerbyCon
- Security Consultant / Researcher
- AD Enthusiast - Own & Operate ADSecurity.org
(Microsoft platform security info)

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
 - Management issues (user accounts with admin rights, improper protection of server, ...)
- 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.

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

Common AD Security Issues

We find really interesting things...



1. 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

Mitigation:

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

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

SAMKey : 364d77a8399af95033658c1498e09bf2

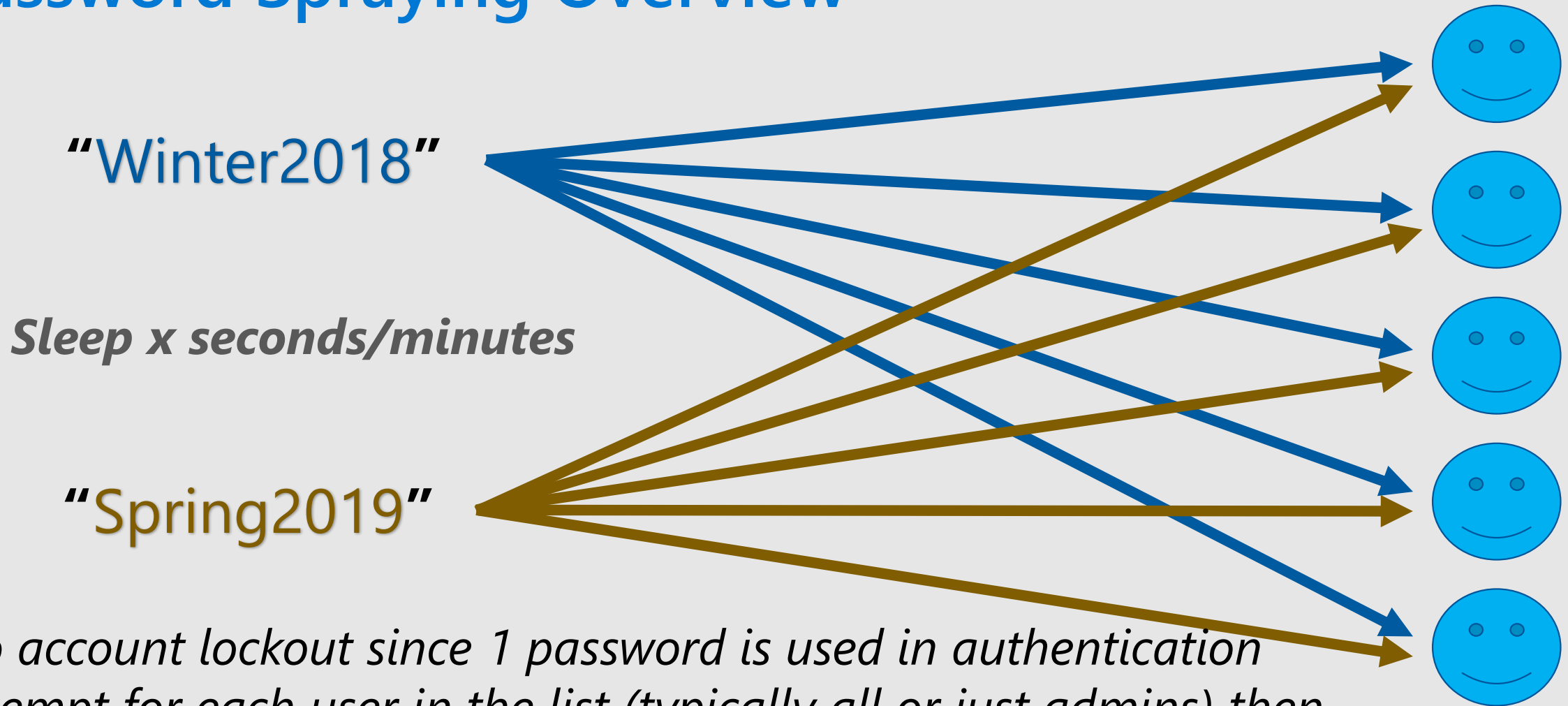
RID : 000001f4 (500)
User : Administrator
LM :
NTLM : 4771c80c83293beb882cb621a6a063fe

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

2. 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 (AD Default)
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Password Spraying Overview



No account lockout since 1 password is used in authentication attempt for each user in the list (typically all or just admins) then the password spray tool pauses before moving onto the next password.

Password Spraying Overview

"Winter2018!"

Sleep x seconds/minutes

"Spring2019!"

No account lockout since 1 password is used in authentication attempt for each user in the list (typically all or just admins) then the password spray tool pauses before moving onto the next password.









2. Domain Password Policy

Shorter passwords = more effective password spraying

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


2. Domain Password Policy (improvement?)

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

Set to at least 12 characters, preferably 15.

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

Also review Azure AD Password Protection for (on-prem) AD

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises>

3. 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
}
```

Kerberoast:

Offline password attack using a Kerberos service ticket requested as a user.

trimarcadmin Properties

Organization	Published Certificates	Member Of	Password Replication
Dial-in	Object	Security	Environment
General	Address	Account	Profile
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 Tim
whenCreated	5/16/2018 9:20:16 PM Eastern Daylight Tim

Edit Filter

4. AD Admin Accounts: Old Passwords

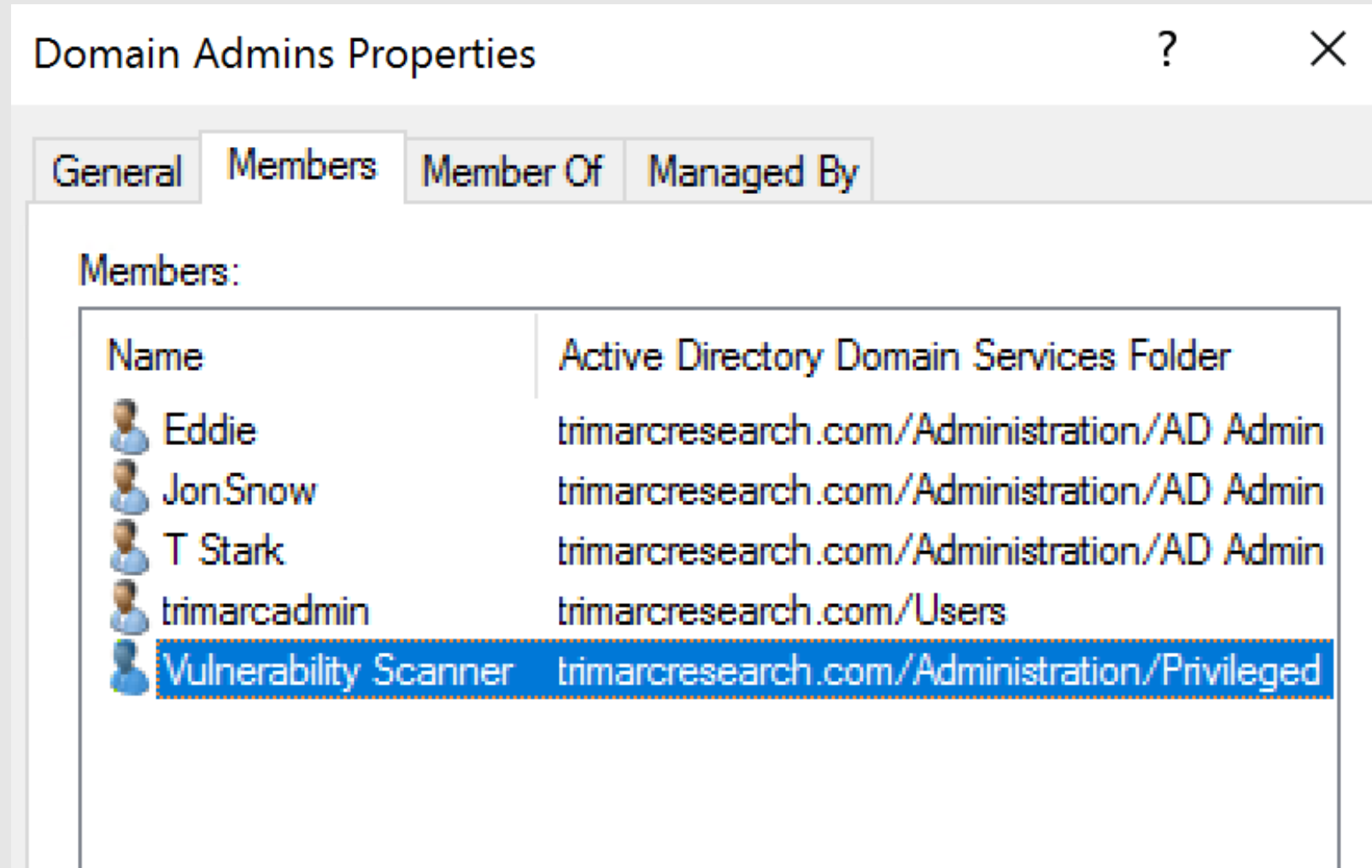
SamAccountName	Enabled	PasswordLastSet	Password Age (years)
Administrator	Yes	1/9/2005 10:58:24 AM	14.5
AGPMService	Yes	5/3/2009 3:17:32 PM	10.5
SCCMsvc	Yes	11/14/2011 5:23:12 PM	7.9
VMWareAdmin	Yes	8/28/2012 10:23:41 AM	7.0
admAEdwards	Yes	1/12/2013 2:20:06 PM	6.5
VulnerabilityScanner	Yes	9/19/2015 4:43:19 PM	4.2
admBWalker	No	6/11/2017 10:14:08 AM	2.2
admCGriffin	Yes	3/1/2019 12:41:18 PM	0.5

4. Admin Accounts: Service Accounts in Domain Admins

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

Mitigation:

- Determine rights actually required.
- Delegate these rights.
- Remove from Domain Admins.



4. Admin Accounts: Old KRBtgt Account Password

- KRBtgt account is disabled but used for Kerberos Tickets.
- Password set when created & practically never changes.
- If an attacker gains knowledge of pw, Golden Tickets!!!

```
PS C:\> Get-ADUser -filter {SamAccountName -like "krbtgt*"} -Prop *,msds-keyversionnumber |
```

```
DistinguishedName      : CN=krbtgt,CN=Users,DC=lab,DC=trimarcresearch,DC=com
Created                 : 1/9/2019 11:31:12 AM
PasswordLastSet        : 1/9/2019 11:31:12 AM
msds-keyversionnumber  :
```



Matt Nelson @enigma0x3 · 14h

I've cracked the krbtgt in an environment, in which it was set to a 3 character password. Talk about terrifying.

Mitigation:

- Change this password 2x every year
(DoD STIG requirement)










```
mimikatz # sekurlsa::krbtgt
```

```
Current krbtgt: 6 credentials
```

```
* rc4_hmac_nt       : 8b4e3f3c8e5e18ce5fb124ea9d7ac65f
* rc4_hmac_old      : 8b4e3f3c8e5e18ce5fb124ea9d7ac65f
* rc4_md4           : 8b4e3f3c8e5e18ce5fb124ea9d7ac65f
* aes256_hmac       : 8846a887883334322e0820bdd64c0f8e99a71147ae7f81310aa257bcfeeb3bcf
* aes128_hmac       : 17d63df4e26dde3e926e266f08a5d6cc
* rc4_plain         : 8b4e3f3c8e5e18ce5fb124ea9d7ac65f
```

5. DC GPOs: Domain Controllers with minimal event auditing

If Advanced Auditing is not configured on DCs, you are missing events required to potentially detect malicious activity.

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

5. DC GPOs: 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

GPOs provide the capability to change security settings, update Administrators group membership, and install/run code.

5. DC GPOs: 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

Computer Configuration

Policies

Windows Settings

Security Settings

Restricted Groups

Group

ADSECLAB\Se

Administrators Properties

Object Security Attribute Editor

General Members Member Of Managed By

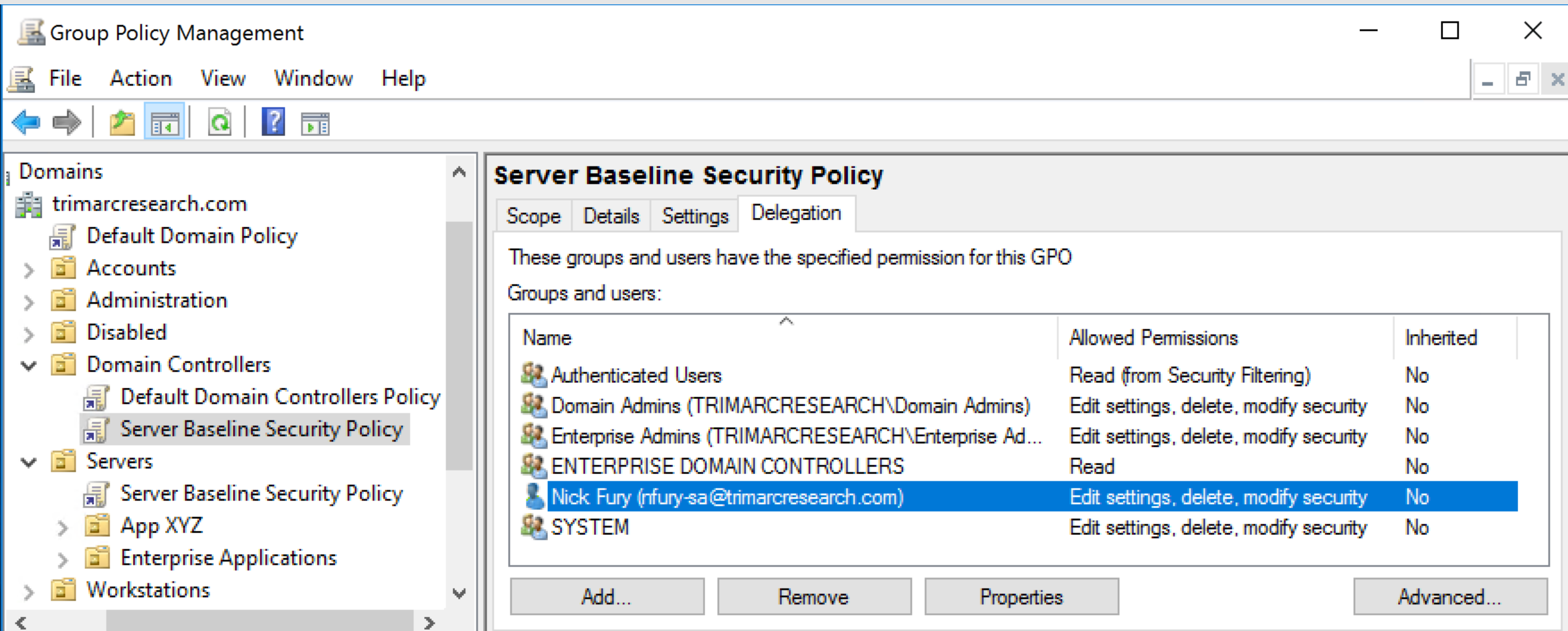
Members:

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.

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

6. GPOs: Modify Rights to GPOs at Domain /DC Level



The screenshot shows the Group Policy Management console for the domain trimarcresearch.com. The left pane shows the hierarchy: Domains > trimarcresearch.com > Servers > Server Baseline Security Policy. The right pane shows the 'Delegation' tab for this GPO. It lists groups and users with their allowed permissions and whether they are inherited.

Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (TRIMARCRESEARCH\Domain Admins)	Edit settings, delete, modify security	No
Enterprise Admins (TRIMARCRESEARCH\Enterprise Ad...	Edit settings, delete, modify security	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
Nick Fury (nfury-sa@trimarcresearch.com)	Edit settings, delete, modify security	No
SYSTEM	Edit settings, delete, modify security	No

Buttons at the bottom: Add..., Remove, Properties, Advanced...

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

7. Permissions: 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
```

7. Permissions: 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
```

8. Admins Use Regular Workstations for AD Administration

1 workstation

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?



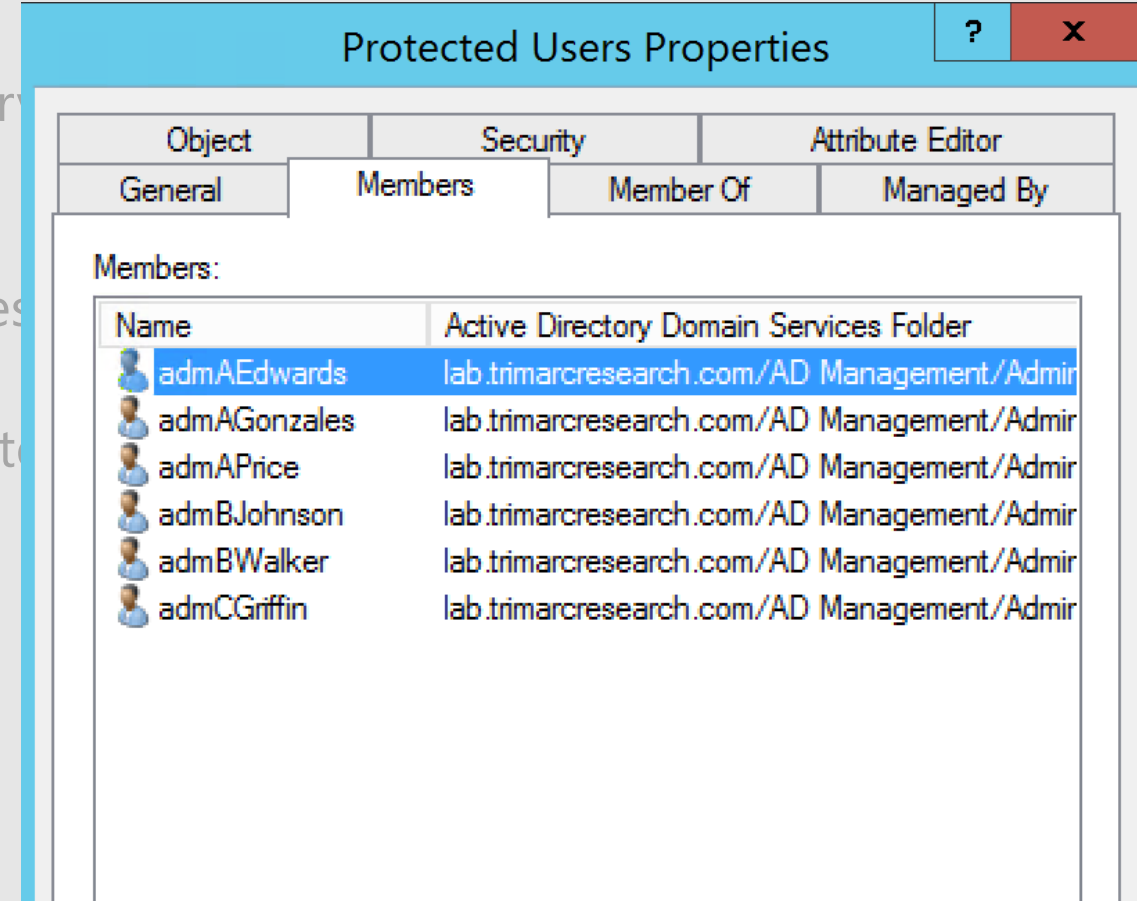
9. Kerberos Delegation

- Delegation = Impersonation
- Kerberos Delegation:
 - **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.

9. Kerberos Delegation

- Delegation = Impersonation
- Kerberos Delegation:
 - **Unconstrained:**
Impersonate users connecting to service to ANY Kerberos service.
 - **Constrained:**
Impersonate authenticated users connecting to service to specific servers.
 - **Constrained with Protocol Transition:**
Impersonate any user to SPECIFIC Kerberos services
 - **Resource-based Constrained Delegation:**
Enables delegation configured on the resource instance

☒ Account is sensitive and cannot be delegated



10. 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:

DEF CON 25 (July 2017)

Permission	Used for
<ul style="list-style-type: none">• 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

10. 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:

DEF CON 25 (July 2017)

Permission	Used for
<ul style="list-style-type: none">• Replicate Directory Changes• Replicate Directory Changes All	Password sync



Protect your Azure AD Connect Server like a Domain Controller

BONUS: 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

Thanks Quest!

Q&A at the Quest booth 2149
right after this

Stop by and ask me anything
(Active Directory & Azure AD security)



Sean Metcalf (@Pyrotek3)
s e a n @ t r i m a r c s e c u r i t y . c o m
TrimarcSecurity.com
www.ADSecurity.org

