Active Directory Security Deep-dive Master Class

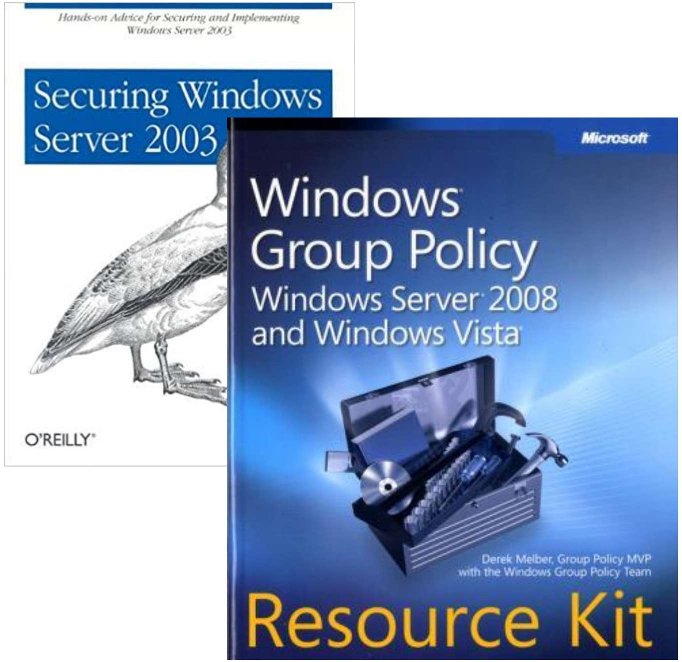
Derek Melber, MVP
Chief Technology and Security Strategist

dmelber@tenable.com
@derekmelber

ABOUT THE SPEAKER

Derek Melber

- Chief Technology and Security Strategist
- 18X Microsoft MVP (AD, GP, Security)
- Speaker in over 35 countries
- Author of 16 books


Hands-on Advice for Securing and Implementing Windows Server 2003
Securing Windows Server 2003
O'REILLY
Microsoft
Windows Group Policy
Windows Server 2008 and Windows Vista
Derek Melber, Group Policy MVP with the Windows Group Policy Team
Resource Kit

dmelber@tenable.com
LinkedIn: @derekmelber

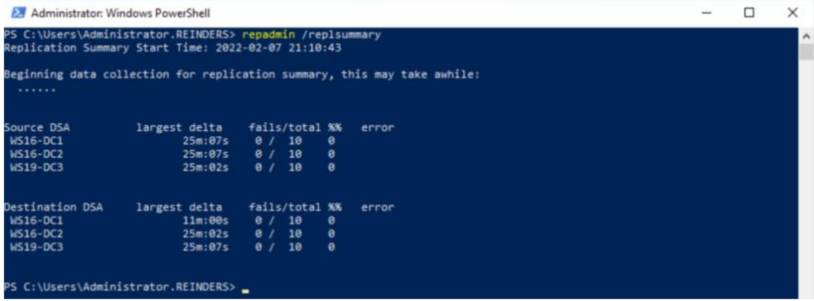
Agenda

- Domain Controllers
- AD Security Overview
- Windows Security Model
- PowerShell and AD
- Privileges in AD
- Stop Thinking Like an Admin to Protect AD!
- Top AD Security Settings

Domain Controllers

Domain Controllers

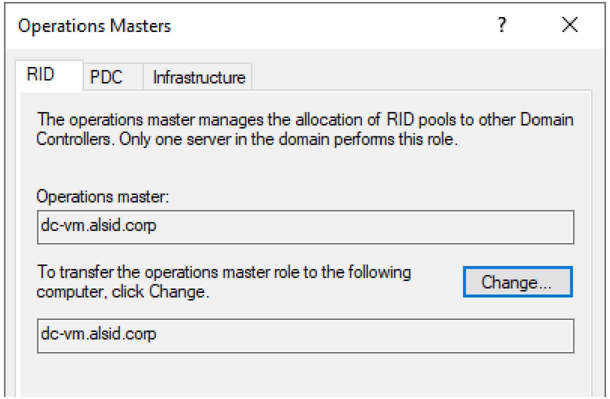
- Main Function
  - Authenticate users and computers
  - Deploy Group Policy and scripts
- Replication and Convergence
  - Intra-site replication
    - Replication between DCs in same site
    - Default is immediate
  - Inter-site replication
    - Replication between DCs in different sites
    - Default is 180 minutes
    - Minimum is 15 minutes
  - Inter-site Change Notification
    - Default is immediate
  - CMD: repadmin /replsummary



```
PS C:\Users\Administrator.REINDERS> repadmin /replsummary
Replication Summary Start Time: 2022-02-07 21:10:43

Beginning data collection for replication summary, this may take awhile:
  ......


Source DSA          largest delta    fails/total %%   error
 WS16-DC1                25m:07s    0 /  10    0
 WS16-DC2                25m:07s    0 /  10    0
 WS19-DC3                25m:02s    0 /  10    0


Destination DSA     largest delta    fails/total %%   error
 WS16-DC1                11m:00s    0 /  10    0
 WS16-DC2                25m:02s    0 /  10    0
 WS19-DC3                25m:07s    0 /  10    0


PS C:\Users\Administrator.REINDERS> _
```

Domain Controllers

- Not all DCs are equal
  - Flexible Single Master Operators
    - Relative ID (RID) Master
    - PDC Emulator
    - Infrastructure Master
    - Domain Naming Master (per forest)
    - Schema Master (per forest)



The operations master manages the allocation of RID pools to other Domain Controllers. Only one server in the domain performs this role.

Operations master:

dc-vm.alsid.corp

To transfer the operations master role to the following computer, click Change.

dc-vm.alsid.corp

Domain Controllers

- PDC Emulator
  - Password changes performed by other DCs in the domain are replicated preferentially to the PDC emulator.
  - If a logon authentication fails at a given DC in a domain due to a bad password, the DC will forward the authentication request to the PDC emulator to validate the request against the most current password. If the PDC reports an invalid password to the DC, the DC will send back a bad password failure message to the user.
  - Account lockout is processed on the PDC emulator.

Domain Controllers

- PDC Emulator
  - Immediate replication to PDC Emulator from another DC
    - Lockout of an account
    - Account is unlocked
    - Password reset on account
    - “User Must Change Password at Next Logon” manually set for user
    - Modification of Local Security Authority (LSA) secret
    - State changes of the RID Manager

tenable®

Active Directory security overview

Active Directory Security Overview

Privileged Accounts

This includes built-in users and groups with privileges, but also newly created users and groups that are granted privileges.

Password Policy

Either via Group Policy or FGPP, the details of the Password Policy need to be configured correctly.

Permissions

Both AD and SYSVOL have permissions that provide granular control, but misconfigured can expose AD to an easy attack.

Service Accounts

These include accounts that are used to support applications, services, scripts, schedule tasks, and more.

Network Protocols

Backward compatible network protocols leave the network and AD open for attack, SMB and NTLM need to be secured.

Trusts

Domain and Forest trusts have many caveats and configurations that often go misconfigured and open to attack.

Active Directory Security Overview

AD Processes

Processes such as SDProp, Kerberos authentication, and Kerberos ticketing need to be secured.

User Attributes

Controls such as SPNs, Kerberos delegation, Primary Group ID, SIDHistory, etc. need to be secured.

Unsecure Users

These accounts are those that have not logged or changed their password in a long time, as well as those with non-expiring passwords.

User Rights

Each Domain Controller has special privileges that can grant power over the server and even AD.

AAD Connections

Settings within the on-prem AD that allow for communications and synchronization with Azure AD need to be secured.

Computer Attributes

Kerberos delegations and group membership can provide an unmonitored attack surface and every attacker looks for these.

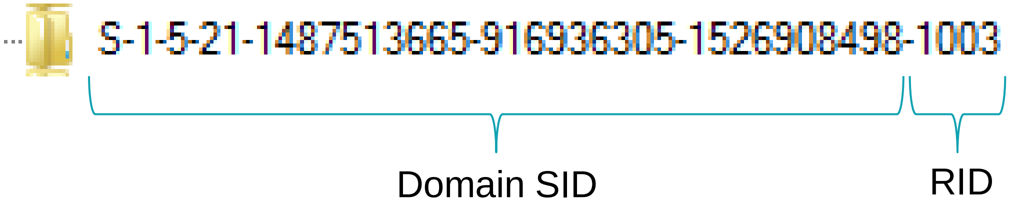
Windows Security Model

The Windows Security Model

- SIDs
- Tokens
- Object-based Access Control
- User Authentication

SIDs

- User and computer account = 1 single object in AD
  - A user/computer account only exists one time in AD
  - User/computer accounts can have membership in many groups
- Security Identifiers (SIDs)
  - Users
  - Groups
  - Computers



S-1-5-21-1487513665-916936305-1526908498-1003

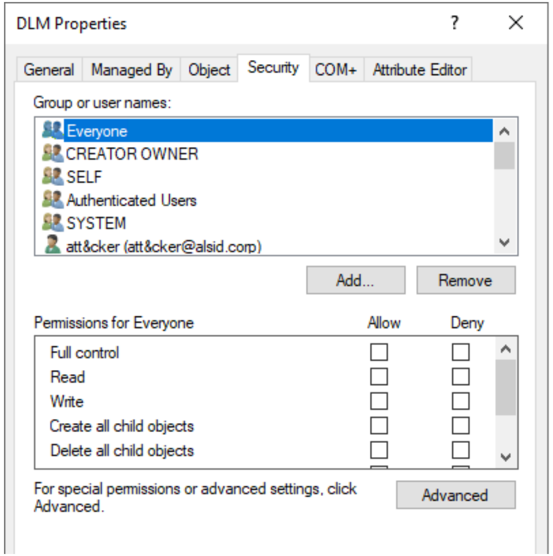
  - PS: Get-aduser derek –properties sid

Authentication Tokens

- Given out by Domain Controller at user logon
- Contents
  - User SID
  - Group SIDs
  - Privileges
  - CMD: whoami /all
- Only refreshed with user logoff/logon or computer restart

Object-based Access Control

- ACL – Access Control List – Security tab
  - Associated with Windows security objects
  - Entries can include: users, groups, computers
  - Defines the access per security principal
  - ACL is list of SIDs
    - GUI translates
    - Orphaned SIDs
- Objects with ACLs
  - Files and Folders
  - Registry keys
  - Printers
  - AD Objects
  - Services



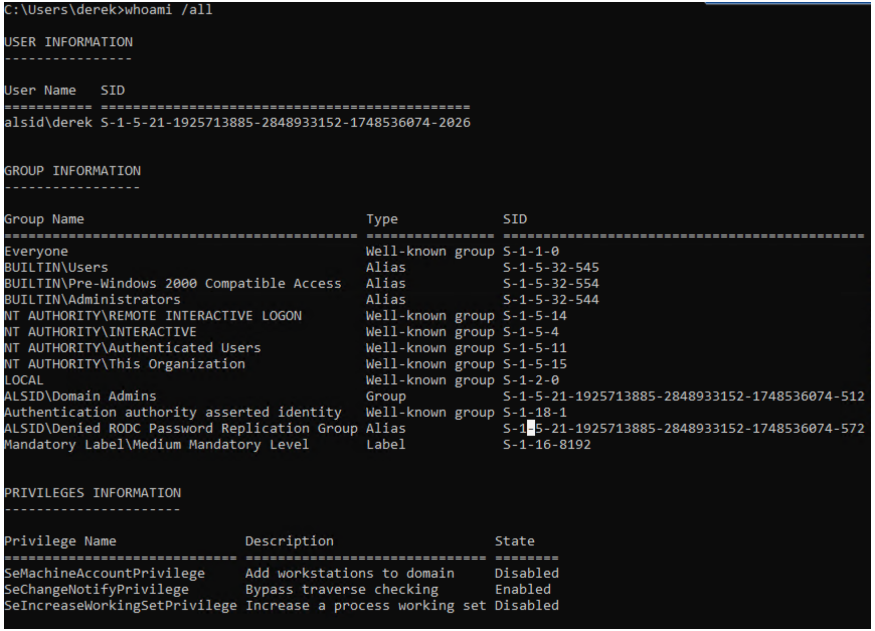
Group or user names:

- Everyone
- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- att&cker (att&cker@alsid.corp)

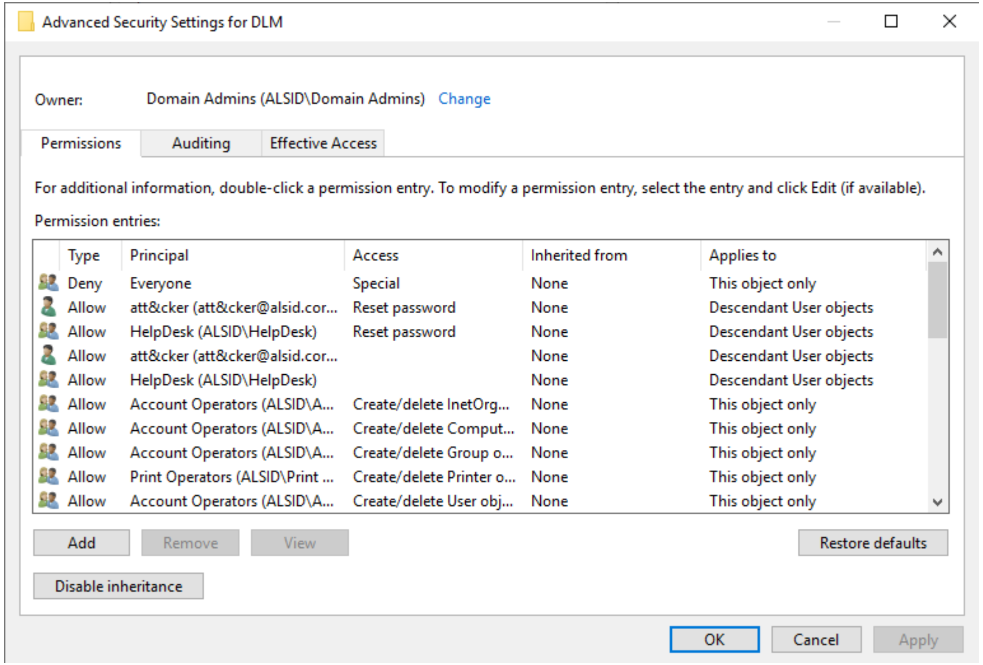
Permissions for Everyone	Allow	Deny
Full control	□	□
Read	□	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□

For special permissions or advanced settings, click Advanced.

User Authentication



```
C:\Users\derek>whoami /all

USER INFORMATION
----------------

User Name   SID
=========== ==============================================
alsid\derek S-1-5-21-1925713885-2848933152-1748536074-2026


GROUP INFORMATION
-----------------

Group Name                                   Type             SID
============================================ ================ =============================================
Everyone                                     Well-known group S-1-1-0
BUILTIN\Users                                Alias            S-1-5-32-545
BUILTIN\Pre-Windows 2000 Compatible Access   Alias            S-1-5-32-554
BUILTIN\Administrators                       Alias            S-1-5-32-544
NT AUTHORITY\REMOTE INTERACTIVE LOGON        Well-known group S-1-5-14
NT AUTHORITY\INTERACTIVE                     Well-known group S-1-5-4
NT AUTHORITY\Authenticated Users             Well-known group S-1-5-11
NT AUTHORITY\This Organization               Well-known group S-1-5-15
LOCAL                                        Well-known group S-1-2-0
ALSID\Domain Admins                          Group            S-1-5-21-1925713885-2848933152-1748536074-512
Authentication authority asserted identity   Well-known group S-1-18-1
ALSID\Denied RODC Password Replication Group Alias            S-1-5-21-1925713885-2848933152-1748536074-572
Mandatory Label\Medium Mandatory Level       Label            S-1-16-8192


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeMachineAccountPrivilege     Add workstations to domain     Disabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
```



Advanced Security Settings for DLM

Owner: Domain Admins (ALSID\Domain Admins) Change

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	att&cker (att&cker@alsid.cor...	Reset password	None	Descendant User objects
Allow	HelpDesk (ALSID\HelpDesk)	Reset password	None	Descendant User objects
Allow	att&cker (att&cker@alsid.cor...		None	Descendant User objects
Allow	HelpDesk (ALSID\HelpDesk)		None	Descendant User objects
Allow	Account Operators (ALSID\A...	Create/delete InetOrg...	None	This object only
Allow	Account Operators (ALSID\A...	Create/delete Comput...	None	This object only
Allow	Account Operators (ALSID\A...	Create/delete Group o...	None	This object only
Allow	Print Operators (ALSID\Print ...	Create/delete Printer o...	None	This object only
Allow	Account Operators (ALSID\A...	Create/delete User obj...	None	This object only

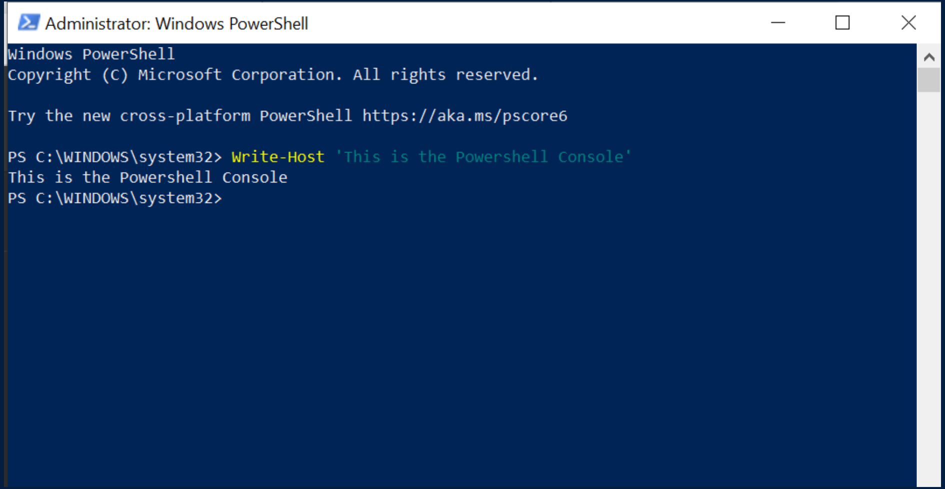
tenable

tenable®

PowerShell and Active Directory

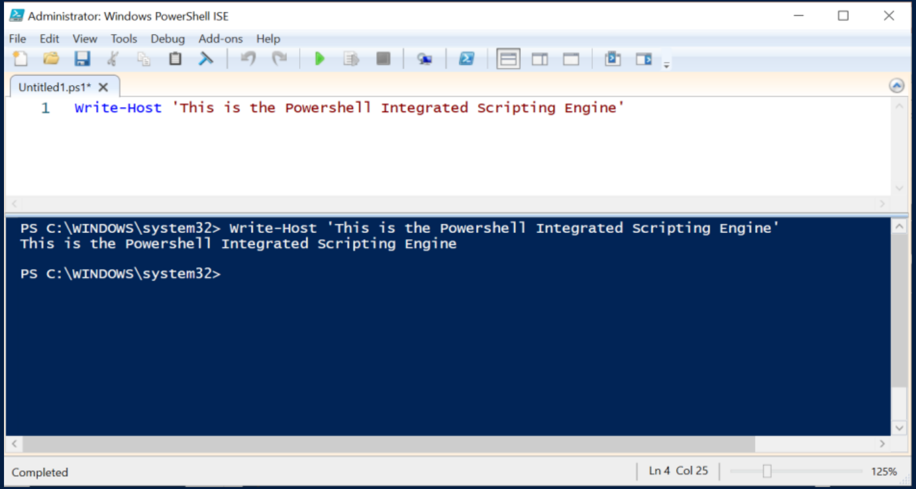
The Powershell Environment

Powershell Console



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> Write-Host 'This is the Powershell Console'
This is the Powershell Console
PS C:\WINDOWS\system32>
```

Powershell ISE



```
Write-Host 'This is the Powershell Integrated Scripting Engine'
```

```
PS C:\WINDOWS\system32> Write-Host 'This is the Powershell Integrated Scripting Engine'
This is the Powershell Integrated Scripting Engine

PS C:\WINDOWS\system32>
```

Useful AD Powershell CMDlets

```
Install-Module NTFSSecurity
```

Installs the NTFS Security Module from the Microsoft Powershell Gallery.

```
Get-ADUser –Filter * -Properties *
```

Retrieves all readable properties of all users in Active Directory

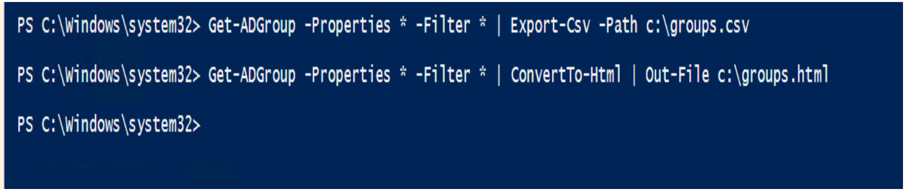
```
Get-ADGroup –Filter * -Properties *
```

Retrieves all readable properties of all groups in Active Directory

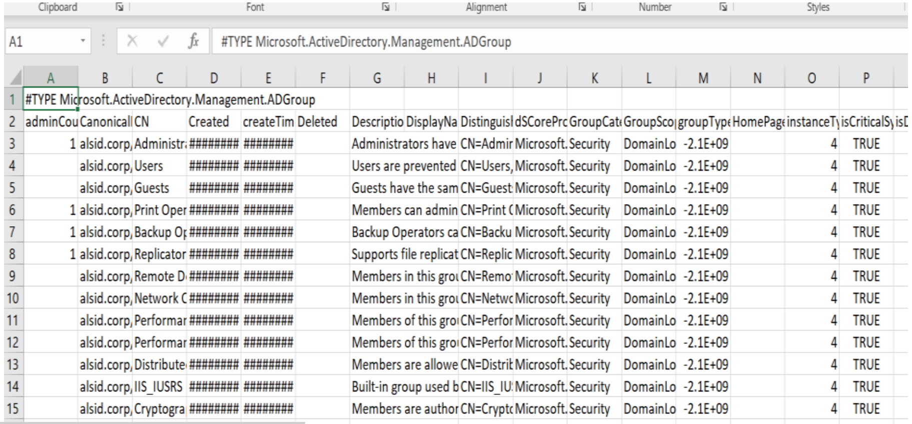
```
Get-ADComputer –Filter “CN=Server,OU=CT,DC=MyCompany,DC=Corp”
```

Retrieves all computers in the Server container of the CT OU in the mycompany.corp domain

Export Info in Multiple Formats

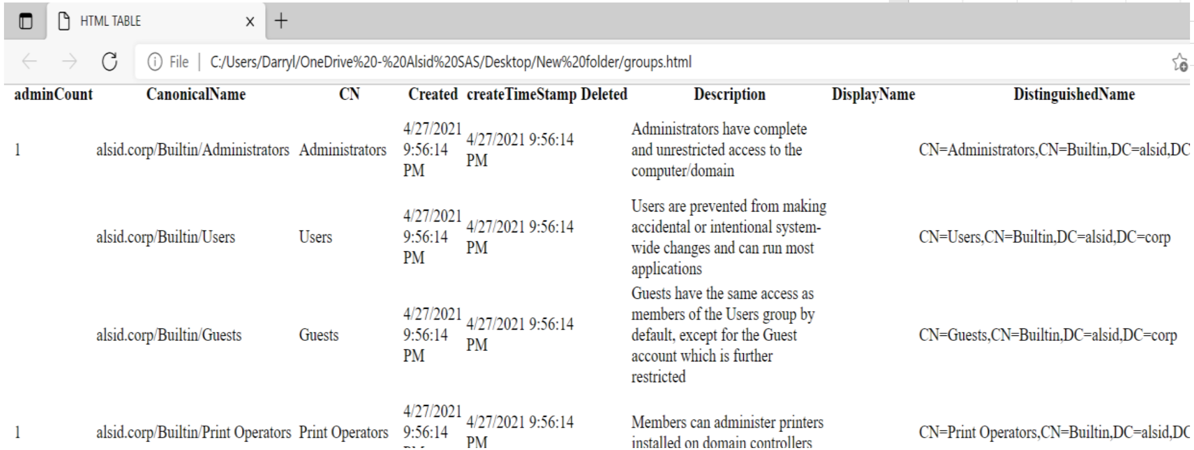


```
PS C:\Windows\system32> Get-ADGroup -Properties * -Filter * | Export-Csv -Path c:\groups.csv

PS C:\Windows\system32> Get-ADGroup -Properties * -Filter * | ConvertTo-Html | Out-File c:\groups.html

PS C:\Windows\system32>
```



#TYPE Microsoft.ActiveDirectory.Management.ADGroup

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
1	#TYPE Microsoft.ActiveDirectory.Management.ADGroup																
2	adminCou	Canonical	CN	Created	createTim	Deleted	Descriptio	DisplayNa	Distinguisl	dSCorePrc	GroupCat	GroupSco	groupType	HomePage	instanceT	isCriticalS	isD
3	1	alsid.corp,	Administr	########	########		Administrators have		CN=Admir	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
4		alsid.corp,	Users	########	########		Users are prevented		CN=Users,	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
5		alsid.corp,	Guests	########	########		Guests have the sam		CN=Guest	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
6	1	alsid.corp,	Print Oper	########	########		Members can admin		CN=Print (	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
7	1	alsid.corp,	Backup Op	########	########		Backup Operators ca		CN=Backu	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
8	1	alsid.corp,	Replicator	########	########		Supports file replicat		CN=Replic	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
9		alsid.corp,	Remote D	########	########		Members in this grou		CN=Remo	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
10		alsid.corp,	Network C	########	########		Members in this grou		CN=Netwc	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
11		alsid.corp,	Performar	########	########		Members of this gro		CN=Perfor	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
12		alsid.corp,	Performar	########	########		Members of this gro		CN=Perfor	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
13		alsid.corp,	Distribute	########	########		Members are allowe		CN=Distrik	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
14		alsid.corp,	IIS_IUSRS	########	########		Built-in group used b		CN=IIS_IU	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
15		alsid.corp,	Cryptogra	########	########		Members are author		CN=Cryptc	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
							Members of this gro		CN=Event	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
							Members of this gro		CN=Certifi	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
							Servers in this group		CN=RDS R	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	
							Servers in this group		CN=RDS E	Microsoft.	Security	DomainLo	-2.1E+09		4	TRUE	



C:/Users/Darryl/OneDrive%20-%20Alsid%20SAS/Desktop/New%20folder/groups.html

adminCount	CanonicalName	CN	Created	createTimeStamp	Deleted	Description	DisplayName	DistinguishedName
1	alsid.corp/Builtin/Administrators	Administrators	4/27/2021 9:56:14 PM	4/27/2021 9:56:14 PM		Administrators have complete and unrestricted access to the computer/domain		CN=Administrators,CN=Builtin,DC=alsid,DC
	alsid.corp/Builtin/Users	Users	4/27/2021 9:56:14 PM	4/27/2021 9:56:14 PM		Users are prevented from making accidental or intentional system-wide changes and can run most applications		CN=Users,CN=Builtin,DC=alsid,DC=corp
	alsid.corp/Builtin/Guests	Guests	4/27/2021 9:56:14 PM	4/27/2021 9:56:14 PM		Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted		CN=Guests,CN=Builtin,DC=alsid,DC=corp
1	alsid.corp/Builtin/Print Operators	Print Operators	4/27/2021 9:56:14	4/27/2021 9:56:14 PM		Members can administer printers installed on domain controllers		CN=Print Operators,CN=Builtin,DC=alsid,DC

Powershell for AD Enumeration

The following are a few examples of Powershell cmds that an authenticated, non-privileged user can easily run and that attackers leverage:

Get-ADUser –Filter {Name –like “*admin*”}

Retrieves all users the admin in the username.

Get-ADUser –Filter {serviceprinciplename –ne “$null”}

Retrieves all users that have an SPN

Get-ADDefaultPasswordPolicy

Retrieves Domain Password Policy located in default domain policy

Get-ADGroup | select name

Retrieves all AD group names

Get-ADDomain

Gets Domain info including DC info

Get-ADDomainControllerReplicationPolicy

Retrieves DC replication info

Get-GPO (or even better Get-GPOReport)

Retrieves all GPOs. Get-GPOReport will even export them as an XML or CSV

tenable®

Privileges in Active Directory

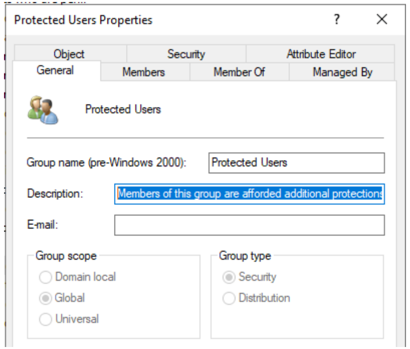
Privileged Groups

Admin/Privileged Domain Groups

- Domain Admins
- Administrators
- Cert Publishers
- DHCP Administrators
- DNSAdmins
- Group Policy Creator Owners
- Account Operators
- Backup Operators
- Protected Users
- Pre-Windows 2000 Compatible Access

Protected Users

- The Protected Users group entails the following restraints on its members:
  - The CredSSP and WDigest security providers will no longer cache, in memory, the passwords in clear text of the logged-on accounts, even if the Allow delegating default credentials strategy is enabled. Accordingly, the accounts will not be allowed to use delegation of authentication to connect to other systems in a transparent way (internal SSO of Windows).
  - The NTLM provider will no longer cache the password's hash of the authenticated accounts in memory.
  - No delegation of authentication will be available anymore for the accounts, neither constrained nor unconstrained delegation.
  - Kerberos pre-authentication usage will be limited to high encryption algorithms such as AES, and the support for DES and RC4 will be disabled.
  - The default lifetime of Kerberos tickets (TGT only) will change from 10h to 4h. Moreover, they will not be automatically renewed.
  - The feature related to the use of the local cache of the domain will be disabled. As a result, if domain controllers are not available to query, accounts will not be able to log into any computers anymore.
  - The NTLM protocol cannot be used anymore for user authentication, limiting the authentication protocol to Kerberos only.



Group name (pre-Windows 2000): Protected Users

Description: Members of this group are afforded additional protections

E-mail:

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

Additional Admin/Privileged Domain Groups

- Service and Application Groups
  - Exchange
  - Sharepoint
  - “Acme” application
- Custom Groups
  - Usually created by admins for ease of naming and used for administration
  - Be sure to document all group names

Admin Forest Groups

- Forest Root Domain
  - Schema Admins
  - Enterprise Admins

Working With Groups

- Group nesting
  - Ideal for organizing “who” can do “what” to an “asset”
  - Horrible when it comes to “Effective permissions/access”
  - Horrible when it comes to “recursive group members”
    - PS: get-adgroupmember administrators -recursive

User Rights

User Rights

- Computer wide configurations that control what users can do to/on that computer
- User rights are unique from computer to computer
- User rights are configured centrally using Group Policy
  - If not centrally, then local policy configures computer user rights
- User rights override security permissions
  - IE. If user has denial permission to a folder, can still back it up with Backup and Restore user right

User Rights

- Domain controllers
  - Obtain more secure configuration at promotion
  - Default Domain Controllers Policy configures user rights
- Server
  - Joining AD domain does not enhance user right security
  - No GPO configures servers user rights by default

User Rights

- Shut down the system
- Force shutdown of remote system
- Log on as a batch job
- Log on as a service
- Log on locally
- Act as part of the OS
- Backup and Restore files and directories

User Rights

- Enable trusted for delegation
- Generate security audits
- Load and unload device drivers
- Manage auditing and security log
- Replace process level token
- Synchronize directory service data
- Take ownership of files and other objects

Stop Thinking Like and Admin to Protect AD!

THE CYBER KILLCHAIN FRAMEWORK

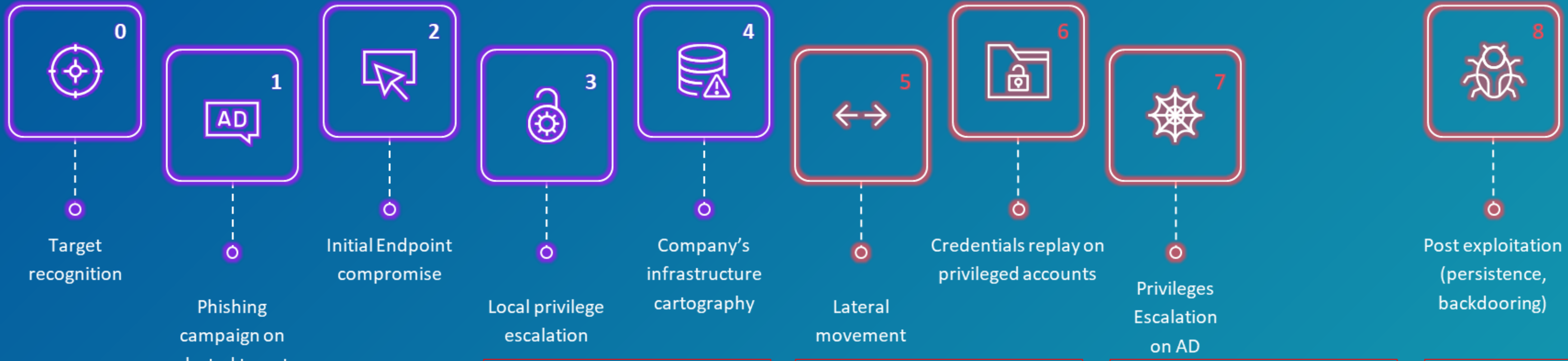
Educate users
Email security

AV
EDR
Least privilege
User is not local Administrator
Application Restriction
UEBA

LAPS
Unique passwords
Common passwords
Change PW often
Strong Password Policy
Password spray detect
Brute force detect
MFA
PAM

Secure privileged users
Secure service accts
Secure computer accts
Clean up old security
Password spray detect
Brute force detect
LSASS detect
DCSync detect
DCShadow detect
SPN modification
Kerberos delegation mod

DCSync detect
DCShadow detect
Golden Ticket detect
LSASS detect
SIDHistory modification
Primary Group ID
modification



0 Target recognition

1 Phishing campaign on selected targets

2 Initial Endpoint compromise

3 Local privilege escalation

4 Company's infrastructure cartography

5 Lateral movement

6 Credentials replay on privileged accounts

7 Privileges Escalation on AD

8 Post exploitation (persistence, backdooring)

Mine credentials
Install enumeration tool
Enumerate AD

Mine credentials
Password spray
Brute force
Cleartext password
No password required

SPN/Kerberoasting
Kerberos delegation
Password spray
Brute force
Cleartext password
LSASS credential dump

Set user attributes
Modify group members
Set user rights
Modify group policy
Create Golden Ticket
adminSDHolder

AD/Windows Issues and Attacks

- Entry Points
  - Too many vulnerabilities and mis-configurations to secure
  - EDR/XDR/…. – too many ways to bypass them
  - Privileged access to easy to obtain
  - Cached credentials easy to obtain
- AD Recon
  - Any user with “read access” can enumerate AD!
  - All (nearly) aspects of AD can be enumerated and analyzed

AD/Windows Issues and Attacks

- Privileged access to easy to obtain
  - With privileges tools can be installed and run
  - Local services and security can be altered
  - Local cache can be accessed
- Cached credentials easy to obtain
  - Usernames and password hashes
    - Crack the hashes
    - Use hashes in Pass-the-hash attacks

Enumeration – Determine Privileged Accounts

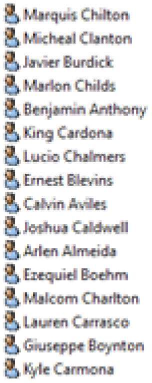
2. Query AD privileges

1. Run installed tools

3. Get users with privileges

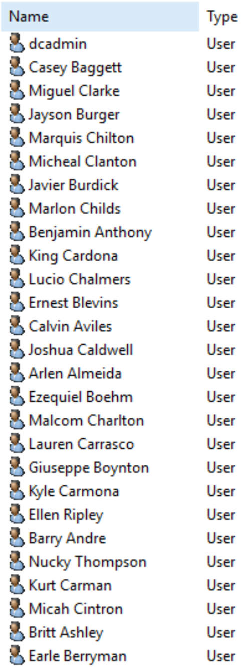
What Attackers Have

- Mined credentials from local cache(s)



Marquis Chilton
Micheal Clanton
Javier Burdick
Marlon Childs
Benjamin Anthony
King Cardona
Lucio Chalmers
Ernest Blevins
Calvin Aviles
Joshua Caldwell
Arlen Almeida
Ezequiel Boehm
Malcom Charlton
Lauren Carrasco
Giuseppe Boynton
Kyle Carmona

4. Compare mined credentials against AD privileged accounts



Name	Type
dcadmin	User
Casey Baggett	User
Miguel Clarke	User
Jayson Burger	User
Marquis Chilton	User
Micheal Clanton	User
Javier Burdick	User
Marlon Childs	User
Benjamin Anthony	User
King Cardona	User
Lucio Chalmers	User
Ernest Blevins	User
Calvin Aviles	User
Joshua Caldwell	User
Arlen Almeida	User
Ezequiel Boehm	User
Malcom Charlton	User
Lauren Carrasco	User
Giuseppe Boynton	User
Kyle Carmona	User
Ellen Ripley	User
Barry Andre	User
Nucky Thompson	User
Kurt Carman	User
Micah Cintron	User
Britt Ashley	User
Earle Berryman	User

What Attackers Obtain

- List of users that have privileges in AD

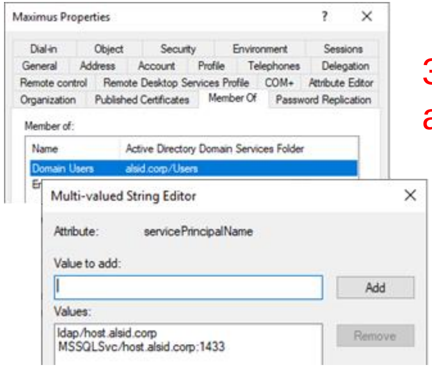
Enumeration – Attack Accounts

What Attackers Have

- Ability to Enumerate AD

1. Run installed tools

2. Query AD accounts



Member of:

Name	Active Directory Domain Services Folder
Domain Users	alsid.corp/Users

Attribute: servicePrincipalName

Value to add:

Values:

ldap/host.alsid.corp
MSSQLSvc/host.alsid.corp:1433

3. Get users with exploitable attributes

4. Attack users/computers to gain privileges

What Attackers Obtain

List of users/computers that have exploitable attributes

tenable®

Top AD Security Settings

Defensive Actions

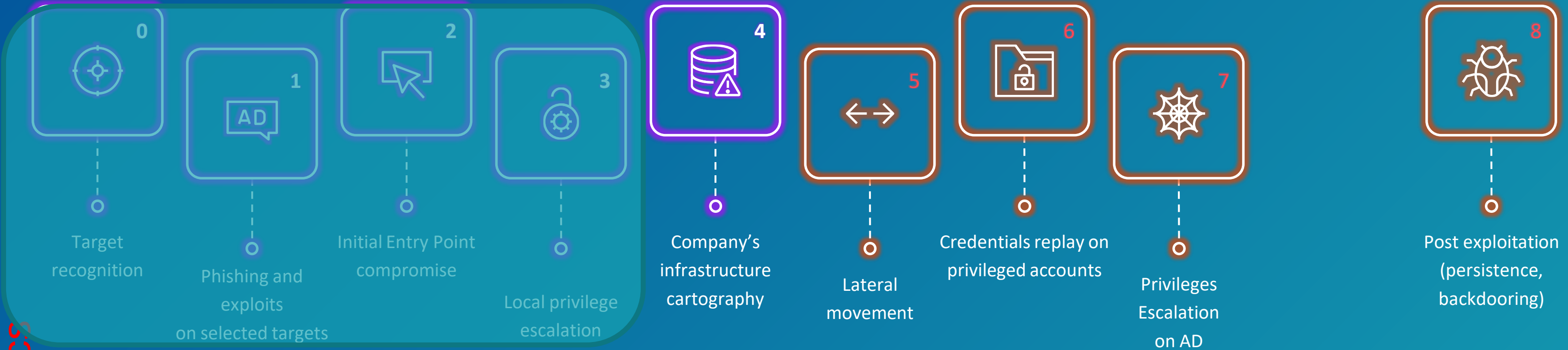
Educate users
Email security

Vulnerability Management
AV
EDR
Least privilege
User is not local Administrator
Application Restriction
UEBA

Vulnerability Management
LAPS
Unique passwords
Common passwords
Change PW often
Strong Password Policy
Password spray detect
Brute force detect
MFA
PAM

Vulnerability Management
Secure privileged users
Secure service accts
Secure computer accts
Clean up old security
Password spray detect
Brute force detect
LSASS detect
DCSync detect
DCShadow detect
SPN modification
Kerberos delegation mod

Vulnerability Management
DCSync detect
DCShadow detect
Golden Ticket detect
LSASS detect
SIDHistory modification
Primary Group ID modification



0 Target recognition

1 Phishing and exploits on selected targets

2 Initial Entry Point compromise

3 Local privilege escalation

4 Company's infrastructure cartography

5 Lateral movement

6 Credentials replay on privileged accounts

7 Privileges Escalation on AD

8 Post exploitation (persistence, backdooring)

Attacker Tactics

Phish users
Exploit Vulnerabilities
Exploit Misconfigurations

Mine credentials
Install enumeration tool
Enumerate AD
Exploit Vulnerabilities

Mine credentials
Password spray
Brute force
Cleartext password
No password required
Exploit Vulnerabilities

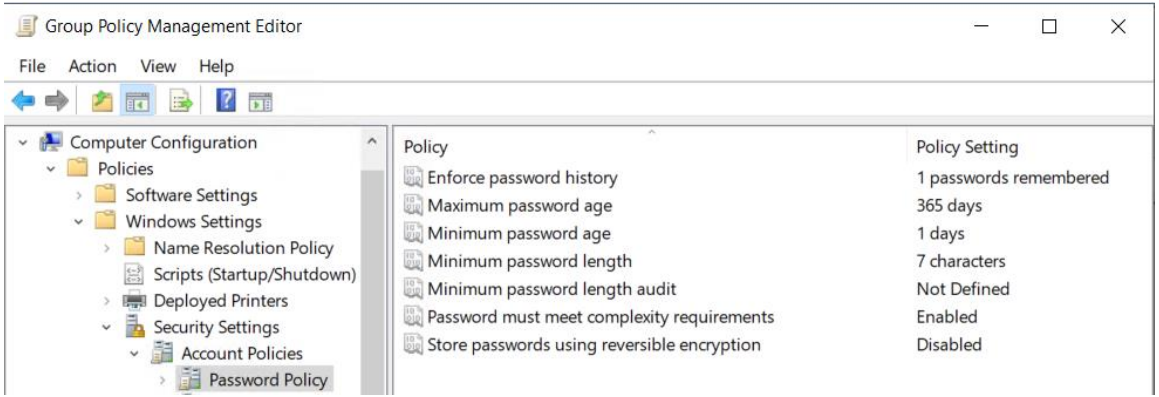
SPN/Kerberoasting
Kerberos delegation
Password spray
Brute force
Cleartext password
LSASS credential dump
Exploit Vulnerabilities

Set user attributes
Modify group members
Set user rights
Modify group policy
Create Golden Ticket
adminSDHolder
Exploit Vulnerabilities

- AD Recon and Lateral Movement

Password Policy(s)

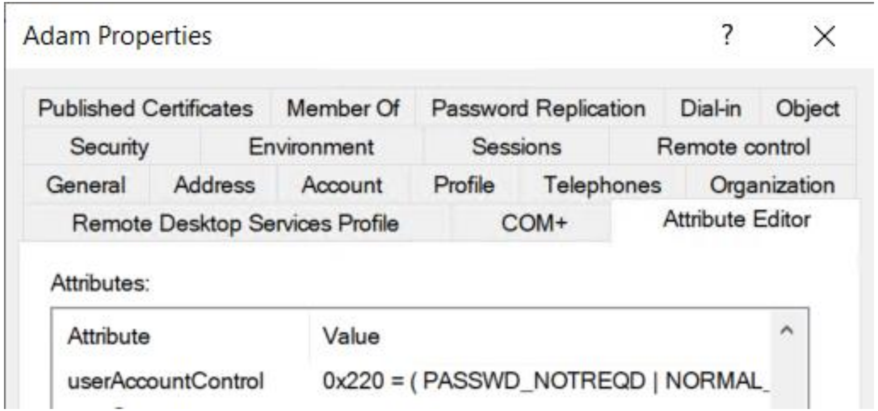
- Availability : In every AD domain
- Level of Threat : Critical
- Attack Method : Spray, Brute force, Kerberoasting
- Commonality of being misconfigured : Near 100%
- Ability to secure : Yes
- How to secure: Solid password policy, FGPP, MFA



Policy	Policy Setting
Enforce password history	1 passwords remembered
Maximum password age	365 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Password Required

- Availability : In every AD domain
- Level of Threat : Critical
- Attack Method : Impersonation, Privilege escalation
- Commonality of being misconfigured : Near 100%
- Ability to secure : Yes
- How to secure: Ensure every user account requires a password



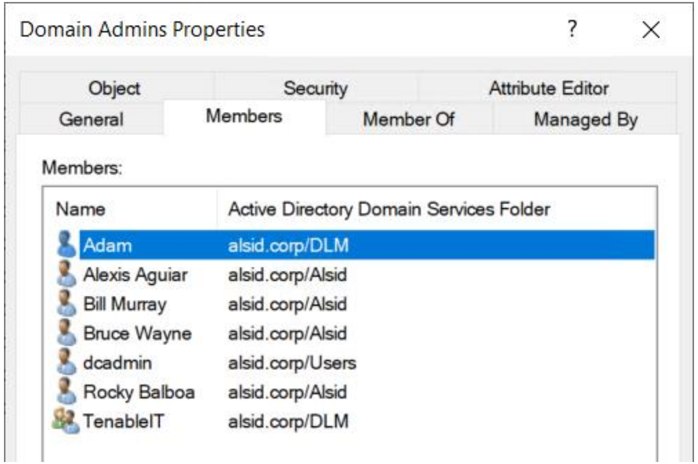
Attribute	Value
userAccountControl	0x220 = (PASSWD_NOTREQD | NORMAL_

```
Net user <username> /passwordreq:no
```

- Immediate Privilege Escalation

Privileged Groups

- Availability : In every AD domain
- Level of Threat : Critical
- Attack Method : Privilege escalation
- Commonality of being misconfigured : Near 100%
- Ability to secure : Yes
- How to secure: Ensure group members are correct

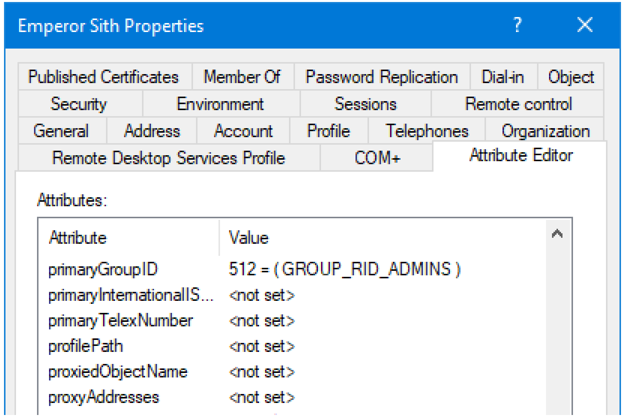


Members:

Name	Active Directory Domain Services Folder
Adam	alsid.corp/DLM
Alexis Aguiar	alsid.corp/Alsid
Bill Murray	alsid.corp/Alsid
Bruce Wayne	alsid.corp/Alsid
dcadmin	alsid.corp/Users
Rocky Balboa	alsid.corp/Alsid
TenableIT	alsid.corp/DLM

Primary Group ID

- Availability : In every AD domain
- Level of Threat : Critical
- Attack Method : Privileged Escalation
- Commonality of being misconfigured : Near 100%
- Ability to secure : Yes
- How to secure: Set primaryGroupID to 513

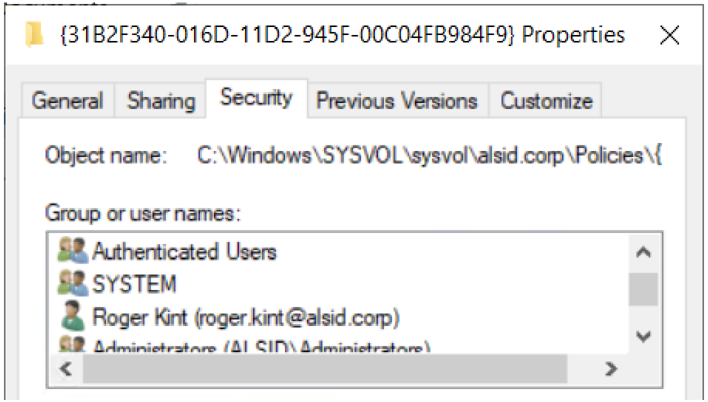


Attributes:

Attribute	Value
primaryGroupID	512 = (GROUP_RID_ADMINS)
primaryInternationalIS...	<not set>
primaryTelexNumber	<not set>
profilePath	<not set>
proxiedObjectName	<not set>
proxyAddresses	<not set>

GPO Permissions

- Availability : In every AD domain
- Level of Threat : Critical
- Attack Method : Privileged Escalation, Ransomware deployment
- Commonality of being misconfigured : Near 100%
- Ability to secure : Yes
- How to secure: Ensure GPO permissions are correct



{31B2F340-016D-11D2-945F-00C04FB984F9} Properties

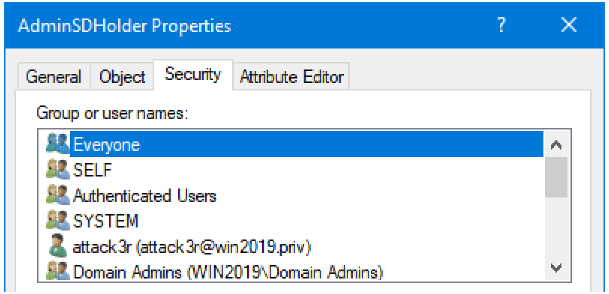
Object name: C:\Windows\SYSVOL\sysvol\alsid.corp\Policies\{

Group or user names:

Authenticated Users
SYSTEM
Roger Kint (roger.kint@alsid.corp)
Administrators (ALSID\Administrators)

adminSDHolder

- Availability : In every AD domain
- Level of Threat : Critical
- Attack Method : Privileged Escalation
- Commonality of being misconfigured : Near 100%
- Ability to secure : Yes
- How to secure: Remove users from AdminSDHolder ACL (via groups too)



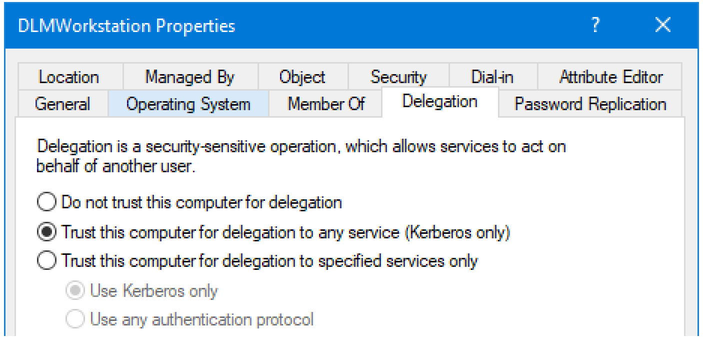
Group or user names:

Everyone
SELF
Authenticated Users
SYSTEM
attack3r (attack3r@win2019.priv)
Domain Admins (WIN2019\Domain Admins)

- Attack to Gain Privileges

Kerberos Delegation

- Availability : In every AD domain
- Level of Threat : Critical
- Attack Method : Impersonation
- Commonality of being misconfigured : Near 100%
- Ability to secure : Yes
- How to secure: Configure contrained delegation



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

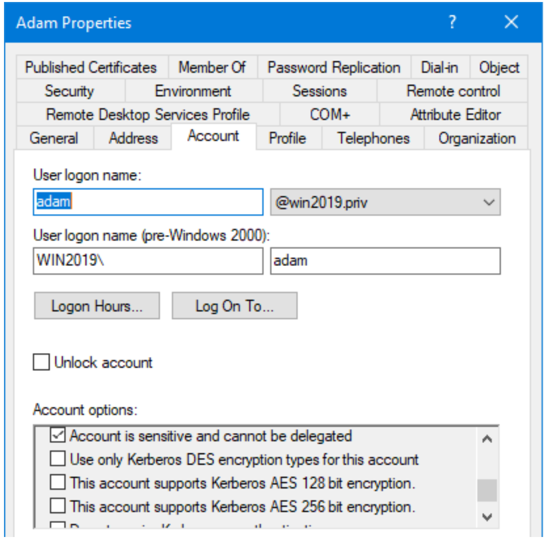
○ Do not trust this computer for delegation

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

○ Trust this computer for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol



User logon name:

adam @win2019.priv

User logon name (pre-Windows 2000):

WIN2019\ adam

□ Unlock account

Account options:

☑ Account is sensitive and cannot be delegated

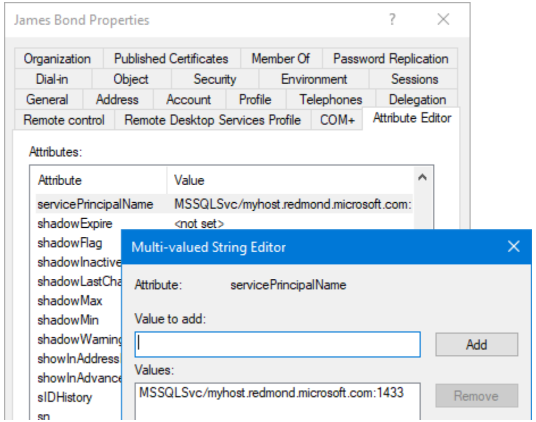
□ Use only Kerberos DES encryption types for this account

□ This account supports Kerberos AES 128 bit encryption.

□ This account supports Kerberos AES 256 bit encryption.

Service Principal Name

- Availability : In every AD domain
- Level of Threat : Critical
- Attack Method : Kerberoasting
- Commonality of being misconfigured : Near 100%
- Ability to secure : Yes
- How to secure: Remove SPN users from privileged groups



Attributes:

Attribute	Value
servicePrincipalName	MSSQLSvc/myhost.redmond.microsoft.com:
shadowExpire	<not set>
shadowFlag	
shadowInactive	
shadowLastCha	
shadowMax	
shadowMin	
shadowWarning	
showInAddress	
showInAdvance	
sIDHistory	
sn	

Attribute: servicePrincipalName

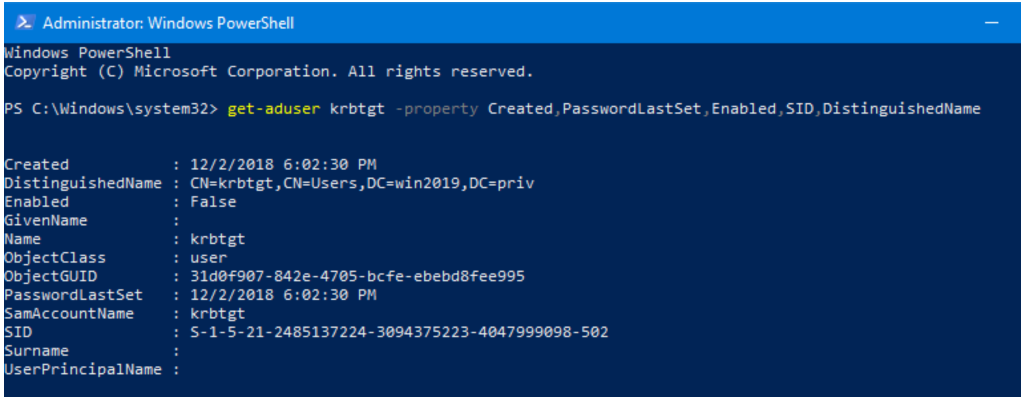
Value to add:

Values:

MSSQLSvc/myhost.redmond.microsoft.com:1433

KRBTGT User Password

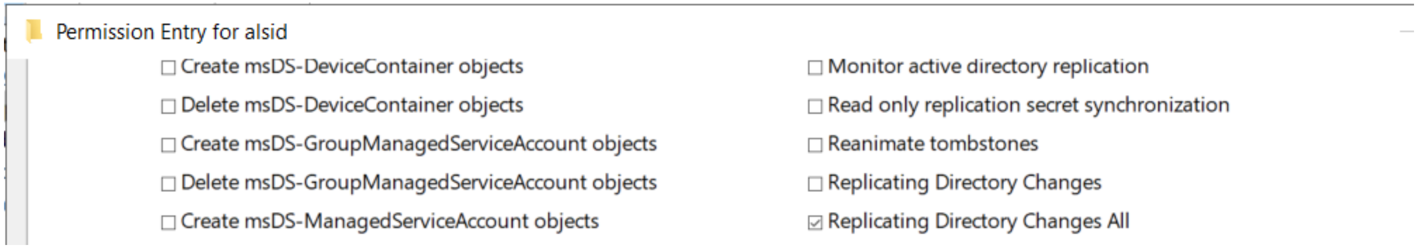
- Availability : In every AD domain
- Level of Threat : Critical
- Attack Method : Kerberoasting, Golden Ticket
- Commonality of being misconfigured : Near 100%
- Ability to secure : Yes
- How to secure: Reset KRBTGT password 2X/year



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> get-aduser krbtgt -property Created,PasswordLastSet,Enabled,SID,DistinguishedName


Created           : 12/2/2018 6:02:30 PM
DistinguishedName : CN=krbtgt,CN=Users,DC=win2019,DC=priv
Enabled           : False
GivenName         :
Name              : krbtgt
ObjectClass       : user
ObjectGUID        : 31d0f907-842e-4705-bcfe-ebebd8fee995
PasswordLastSet   : 12/2/2018 6:02:30 PM
SamAccountName    : krbtgt
SID               : S-1-5-21-2485137224-3094375223-4047999098-502
Surname           :
UserPrincipalName :
```

AD Root Permissions

- Availability : In every AD domain
- Level of Threat : Critical
- Attack Method : DCSync
- Commonality of being misconfigured : Near 100%
- Ability to secure : Yes
- How to secure: Ensure AD root permissions are correct



Permission Entry for alsid

□ Create msDS-DeviceContainer objects
□ Delete msDS-DeviceContainer objects
□ Create msDS-GroupManagedServiceAccount objects
□ Delete msDS-GroupManagedServiceAccount objects
□ Create msDS-ManagedServiceAccount objects

□ Monitor active directory replication
□ Read only replication secret synchronization
□ Reanimate tombstones
□ Replicating Directory Changes
☑ Replicating Directory Changes All

Questions?

Derek Melber, MVP
dmelber@tenable.com

tenable®

Thank You!!!

Derek Melber, MVP
Chief Technology and Security Strategist

dmelber@tenable.com
@derekmelber

tenable®