Scanning for Active Directory Privileges & Privileged Accounts

adsecurity.org

Sean Metcalf June 14, 2017

Active Directory Recon is the new hotness since attackers, Red Teamers, and penetration testers have realized that control of Active Directory provides power over the organization.

I covered ways to enumerate permissions in AD using PowerView (written by Will @harmj0y) during my Black Hat & DEF CON talks in 2016 from both a Blue Team and Red Team perspective.

This post details how privileged access is delegated in Active Directory and how best to discover who has what rights and permissions in AD. When we perform an Active Directory Security Assessment for customers, we review all of the data points listed in this post, including the privileged groups and the rights associated with them by fully interrogating Active Directory and mapping the associated permissions to rights and associating these rights to the appropriate groups (or accounts).

I have had this post in draft for a while and with Bloodhound now supporting AD ACLs (nice work Will @harmj0y & Andy @_Wald0!), it's time to get more information out about AD permissions. Examples in this post use the PowerView PowerShell cmdlets.

Active Directory Privileged Access

The challenge is often determining what access each group actually has. Often the full impact of what access a group actually has is not fully understood by the organization. Attackers leverage access (though not always privileged access) to compromise Active Directory.

The key point often missed is that rights to Active Directory and key resources is more than just group membership, it is the combined rights the user has which is made up of:

- Active Directory group membership.
- AD groups with privileged rights on computers
- Delegated rights to AD objects by modifying the default permissions (for security principals, both direct and indirect).
- Rights assigned to SIDs in SIDHistory to AD objects.
- Delegated rights to Group Policy Objects.
- User Rights Assignments configured on workstations, servers, and Domain Controllers via Group Policy (or Local Policy) defines elevated rights and permissions on these systems.
- Local group membership on a computer or computers (similar to GPO assigned settings).

- Delegated rights to shared folders.

Group Membership

Enumerating group membership is the easy way to discovering privileged accounts in Active Directory, though it often doesn't tell the full story. Membership in Domain Admins, Administrators, and Enterprise Admins obviously provides full domain/forest admin rights. Custom groups are created and delegated access to resources.

This screenshot shows using PowerView to find VMWare groups and list the members.

```
PS C:\Users\joeuser> get-netgroup "*VMWare*" | Get-NetGroupMember


GroupDomain  : lab.adsecurity.org
GroupName    : VMWare Admins
MemberDomain : lab.adsecurity.org
MemberName   : JangoFett
MemberSID    : S-1-5-21-1581655573-3923512380-696647894-4116
IsGroup      : False
MemberDN     : CN=Jango Fett,OU=Accounts,DC=lab,DC=adsecurity,DC=org
```

Interesting Groups with default elevated rights:

Account Operators: Active Directory group with default privileged rights on domain users and groups, plus the ability to logon to Domain Controllers
Well-Known SID/RID: S-1-5-32-548
The Account Operators group grants limited account creation privileges to a user. Members of this group can create and modify most types of accounts, including those of users, local groups, and global groups, and members can log in locally to domain controllers.
Members of the Account Operators group cannot manage the Administrator user account, the user accounts of administrators, or the Administrators, Server Operators, Account Operators, Backup Operators, or Print Operators groups. Members of this group cannot modify user rights.
The Account Operators group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.

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.

Administrators: Local or Active Directory group. The AD group has full admin rights to the Active Directory domain and Domain Controllers
Well-Known SID/RID: S-1-5-32-544
Members of the Administrators group have complete and unrestricted access to the computer, or if the computer is promoted to a domain controller, members have

unrestricted access to the domain.
The Administrators group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.

The Administrators group has built-in capabilities that give its members full control over the system. This group cannot be renamed, deleted, or moved. This built-in group controls access to all the domain controllers in its domain, and it can change the membership of all administrative groups.
Membership can be modified by members of the following groups: the default service Administrators, Domain Admins in the domain, or Enterprise Admins. This group has the special privilege to take ownership of any object in the directory or any resource on a domain controller. This account is considered a service administrator group because its members have full access to the domain controllers in the domain.

This security group includes the following changes since Windows Server 2008:
Default user rights changes: Allow log on through Terminal Services existed in Windows Server 2008, and it was replaced by Allow log on through Remote Desktop Services. Remove computer from docking station was removed in Windows Server 2012 R2.

Allowed RODC Password Replication Group: Active Directory group where members can have their domain password cached on a RODC after successfully authenticating (includes user and computer accounts).
Well-Known SID/RID: S-1-5-21-<domain>-571
The purpose of this security group is to manage a RODC password replication policy. This group has no members by default, and it results in the condition that new Read-only domain controllers do not cache user credentials. The Denied RODC Password Replication Group group contains a variety of high-privilege accounts and security groups. The Denied RODC Password Replication group supersedes the Allowed RODC Password Replication group.
The Allowed RODC Password Replication group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This security group has not changed since Windows Server 2008.

Backup Operators: Local or Active Directory group. AD group members can backup or restore Active Directory and have logon rights to Domain Controllers (default).
Well-Known SID/RID: S-1-5-32-551
Members of the Backup Operators group can back up and restore all files on a computer, regardless of the permissions that protect those files. Backup Operators also can log on to and shut down the computer. This group cannot be renamed, deleted, or moved. By default, this built-in group has no members, and it can perform backup and restore operations on domain controllers. Its membership can be modified by the following groups: default service Administrators, Domain Admins in the domain, or Enterprise Admins. It cannot modify the membership of any administrative groups. While members of this group cannot change server settings or modify the configuration of the directory, they do have the permissions needed to replace files (including operating system files) on

domain controllers. Because of this, members of this group are considered service administrators.
The Backup Operators group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This security group has not changed since Windows Server 2008.

Certificate Service DCOM Access: Active Directory group.
Well-Known SID/RID: S-1-5-32-<domain>-574
Members of this group are allowed to connect to certification authorities in the enterprise.
The Certificate Service DCOM Access group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This security group has not changed since Windows Server 2008.

Cert Publishers: Active Directory group.
Well-Known SID/RID: S-1-5-<domain>-517
Members of the Cert Publishers group are authorized to publish certificates for User objects in Active Directory.
The Cert Publishers group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This security group has not changed since Windows Server 2008.

Distributed COM Users
Well-Known SID/RID: S-1-5-32-562
Members of the Distributed COM Users group are allowed to launch, activate, and use Distributed COM objects on the computer. Microsoft Component Object Model (COM) is a platform-independent, distributed, object-oriented system for creating binary software components that can interact. Distributed Component Object Model (DCOM) allows applications to be distributed across locations that make the most sense to you and to the application. This group appears as a SID until the domain controller is made the primary domain controller and it holds the operations master role (also known as flexible single master operations or FSMO).
The Distributed COM Users group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This security group has not changed since Windows Server 2008.

DnsAdmins: Local or Active Directory group. Members of this group have admin rights to AD DNS and **can run code via DLL on a Domain Controller operating as a DNS server.**
Well-Known SID/RID: S-1-5-21-<domain>-1102
Members of DNSAdmins group have access to network DNS information. The default permissions are as follows: Allow: Read, Write, Create All Child objects, Delete Child objects, Special Permissions.
For information about other means to secure the DNS server service, see Securing the DNS Server Service.
This security group has not changed since Windows Server 2008.

Domain Admins: Active Directory group with full admin rights to the Active Directory domain and all computers (default), including all workstations, servers, and Domain Controllers. Gains this right through automatic membership in the Administrators group for the domain as well as all computers when they are joined to the domain.
Well-Known SID/RID: S-1-5-<domain>-512
Members of the Domain Admins security group are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. The Domain Admins group is the default owner of any object that is created in Active Directory for the domain by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.
The Domain Admins group controls access to all domain controllers in a domain, and it can modify the membership of all administrative accounts in the domain. Membership can be modified by members of the service administrator groups in its domain (Administrators and Domain Admins), and by members of the Enterprise Admins group. This is considered a service administrator account because its members have full access to the domain controllers in a domain.
The Domain Admins group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This security group has not changed since Windows Server 2008.

Enterprise Admins: Active Directory group with full admin rights to all Active Directory domains in the AD forest and gains this right through automatic membership in the Administrators group in every domain in the forest.
Well-Known SID/RID: S-1-5-21-<root domain>-519
The Enterprise Admins group exists only in the root domain of an Active Directory forest of domains. It is a Universal group if the domain is in native mode; it is a Global group if the domain is in mixed mode. Members of this group are authorized to make forest-wide changes in Active Directory, such as adding child domains.
By default, the only member of the group is the Administrator account for the forest root domain. This group is automatically added to the Administrators group in every domain in the forest, and it provides complete access for configuring all domain controllers.
Members in this group can modify the membership of all administrative groups. Membership can be modified only by the default service administrator groups in the root domain. This is considered a service administrator account.
The Enterprise Admins group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This security group has not changed since Windows Server 2008.

Event Log Readers
Well-Known SID/RID: S-1-5-32-573
Members of this group can read event logs from local computers. The group is created when the server is promoted to a domain controller.

The Event Log Readers group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This security group has not changed since Windows Server 2008.

Group Policy Creators Owners: Active Directory group with the ability to create Group Policies in the domain.
Well-Known SID/RID: S-1-5-<domain>-520
This group is authorized to create, edit, or delete Group Policy Objects in the domain. By default, the only member of the group is Administrator.
The Group Policy Creators Owners group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This security group has not changed since Windows Server 2008.

Hyper-V Administrators
Well-Known SID/RID: S-1-5-32-578
Members of the Hyper-V Administrators group have complete and unrestricted access to all the features in Hyper-V. Adding members to this group helps reduce the number of members required in the Administrators group, and further separates access.
System_CAPS_noteNote
Prior to Windows Server 2012, access to features in Hyper-V was controlled in part by membership in the Administrators group.
This security group was introduced in Windows Server 2012, and it has not changed in subsequent versions.

Pre–Windows 2000 Compatible Access
Well-Known SID/RID: S-1-5-32-554
Members of the Pre–Windows 2000 Compatible Access group have Read access for all users and groups in the domain. This group is provided for backward compatibility for computers running Windows NT 4.0 and earlier. By default, the special identity group, Everyone, is a member of this group. Add users to this group only if they are running Windows NT 4.0 or earlier.
System_CAPS_warningWarning
This group appears as a SID until the domain controller is made the primary domain controller and it holds the operations master role (also known as flexible single master operations or FSMO).
The Pre–Windows 2000 Compatible Access group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This security group has not changed since Windows Server 2008.

Print Operators
Well-Known SID/RID: S-1-5-32-550
Members of this group can manage, create, share, and delete printers that are connected to domain controllers in the domain. They can also manage Active Directory printer objects in the domain. Members of this group can locally sign in to and shut down domain

controllers in the domain.
This group has no default members. Because members of this group can load and unload device drivers on all domain controllers in the domain, add users with caution. This group cannot be renamed, deleted, or moved.
The Print Operators group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This security group has not changed since Windows Server 2008. However, in Windows Server 2008 R2, functionality was added to manage print administration. For more information, see Assigning Delegated Print Administrator and Printer Permission Settings in Windows Server 2008 R2.

Protected Users
Well-known SID/RID: S-1-5-21-<domain>-525
Members of the Protected Users group are afforded additional protection against the compromise of credentials during authentication processes.
This security group is designed as part of a strategy to effectively protect and manage credentials within the enterprise. Members of this group automatically have non-configurable protection applied to their accounts. Membership in the Protected Users group is meant to be restrictive and proactively secure by default. The only method to modify the protection for an account is to remove the account from the security group.
This domain-related, global group triggers non-configurable protection on devices and host computers running Windows Server 2012 R2 and Windows 8.1, and on domain controllers in domains with a primary domain controller running Windows Server 2012 R2. This greatly reduces the memory footprint of credentials when users sign in to computers on the network from a non-compromised computer.

Depending on the account's domain functional level, members of the Protected Users group are further protected due to behavior changes in the authentication methods that are supported in Windows.
Members of the Protected Users group cannot authenticate by using the following Security Support Providers (SSPs): NTLM, Digest Authentication, or CredSSP.
Passwords are not cached on a device running Windows 8.1, so the device fails to authenticate to a domain when the account is a member of the Protected User group.

The Kerberos protocol will not use the weaker DES or RC4 encryption types in the preauthentication process. This means that the domain must be configured to support at least the AES cipher suite.

The user's account cannot be delegated with Kerberos constrained or unconstrained delegation. This means that former connections to other systems may fail if the user is a member of the Protected Users group.
The default Kerberos ticket-granting tickets (TGTs) lifetime setting of four hours is configurable by using Authentication Policies and Silos, which can be accessed through the Active Directory Administrative Center. This means that when four hours has passed, the user must authenticate again.

The Protected Users group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This group was introduced in Windows Server 2012 R2. For more information about how this group works, see Protected Users Security Group.
The following table specifies the properties of the Protected Users group.

Remote Desktop Users
Well-Known SID/RID: S-1-5-32-555
The Remote Desktop Users group on an RD Session Host server is used to grant users and groups permissions to remotely connect to an RD Session Host server. This group cannot be renamed, deleted, or moved. It appears as a SID until the domain controller is made the primary domain controller and it holds the operations master role (also known as flexible single master operations or FSMO).
The Remote Desktop Users group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This security group has not changed since Windows Server 2008.

Schema Admins
Well-Known SID/RID: S-1-5-<root domain>-518
Members of the Schema Admins group can modify the Active Directory schema. This group exists only in the root domain of an Active Directory forest of domains. It is a Universal group if the domain is in native mode; it is a Global group if the domain is in mixed mode.
The group is authorized to make schema changes in Active Directory. By default, the only member of the group is the Administrator account for the forest root domain. This group has full administrative access to the schema.
The membership of this group can be modified by any of the service administrator groups in the root domain. This is considered a service administrator account because its members can modify the schema, which governs the structure and content of the entire directory.
For more information, see What Is the Active Directory Schema?: Active Directory.
The Schema Admins group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This security group has not changed since Windows Server 2008.

Server Operators
Well-Known SID/RID: S-1-5-32-549
Members in the Server Operators group can administer domain servers. This group exists only on domain controllers. By default, the group has no members. Memebers of the Server Operators group can sign in to a server interactively, create and delete network shared resources, start and stop services, back up and restore files, format the hard disk drive of the computer, and shut down the computer. This group cannot be renamed, deleted, or moved.
By default, this built-in group has no members, and it has access to server configuration options on domain controllers. Its membership is controlled by the service administrator

groups, Administrators and Domain Admins, in the domain, and the Enterprise Admins group. Members in this group cannot change any administrative group memberships. This is considered a service administrator account because its members have physical access to domain controllers, they can perform maintenance tasks (such as backup and restore), and they have the ability to change binaries that are installed on the domain controllers. Note the default user rights in the following table.
The Server Operators group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
This security group has not changed since Windows Server 2008.

WinRMRemoteWMIUsers_
Well-Known SID/RID: S-1-5-21-<domain>-1000
In Windows 8 and in Windows Server 2012, a Share tab was added to the Advanced Security Settings user interface. This tab displays the security properties of a remote file share. To view this information, you must have the following permissions and memberships, as appropriate for the version of Windows Server that the file server is running.

The WinRMRemoteWMIUsers_ group applies to versions of the Windows Server operating system listed in the Active Directory default security groups by operating system version.
If the file share is hosted on a server that is running a supported version of the operating system:

- *You must be a member of the WinRMRemoteWMIUsers__ group or the BUILTIN\Administrators group.*
- *You must have Read permissions to the file share.*

If the file share is hosted on a server that is running a version of Windows Server that is earlier than Windows Server 2012:

- *You must be a member of the BUILTIN\Administrators group.*
- *You must have Read permissions to the file share.*

In Windows Server 2012, the Access Denied Assistance functionality adds the Authenticated Users group to the local WinRMRemoteWMIUsers__ group. Therefore, when the Access Denied Assistance functionality is enabled, all authenticated users who have Read permissions to the file share can view the file share permissions.

The WinRMRemoteWMIUsers_ group allows running Windows PowerShell commands remotely whereas the Remote Management Users group is generally used to allow users to manage servers by using the Server Manager console.
This security group was introduced in Windows Server 2012, and it has not changed in subsequent versions.

Active Directory Groups with Privileged Rights on Computers

Most organizations use Group Policy to add an Active Directory group to a local group on computers (typically the Administrators group). Using PowerView, we can easily discover the AD groups that have admin rights on workstations and servers (which is the typical use case).

In the following screenshot, we see that the organization has configured the following GPOs:

GPO: “Add Server Admins to Local Administrator Group”
Local Group: Administrators
AD Group: Server Admins (SID is shown in the example)

GPO: “Add Workstation Admins to Local Administrator Group”
Local Group: Administrators
AD Group: Workstation Admins (SID is shown in the example)

```
PS C:\Users\joeuser> Get-NetGPOGroup


GPOPath        : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212}\MACHINE\Pref
Filters        :
GroupName      : Administrators (built-in)
GroupSID       : S-1-5-32-544
GroupMemberOf  :
GroupMembers   : {S-1-5-21-1581655573-3923512380-696647894-2628}
GPODisplayName : Add Server Admins to Local Administrator Group
GPOName        : {E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212}
GPOType        : GroupPolicyPreferences

GPODisplayName : Add Workstation Admins to Local Administrators Group
GPOName        : {45556105-EFE6-43D8-A92C-AACB1D3D4DE5}
GPOPath        : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{45556105-EFE6-43D8-A92C-AACB1D3D4DE5}
GPOType        : RestrictedGroups
Filters        :
GroupName      : ADSECLAB\Workstation Admins
GroupSID       : S-1-5-21-1581655573-3923512380-696647894-2627
GroupMemberOf  : {S-1-5-32-544}
GroupMembers   : {}

GPOPath        : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{F481B887-A0BC-4044-9DB2-4979899B0BC5}\MACHINE\Pref
Filters        :
GroupName      : Remote Desktop Users (built-in)
GroupSID       : S-1-5-32-555
GroupMemberOf  :
GroupMembers   : {S-1-5-21-1581655573-3923512380-696647894-513}
GPODisplayName : Set Remote Users
GPOName        : {F481B887-A0BC-4044-9DB2-4979899B0BC5}
GPOType        : GroupPolicyPreferences
```

We can also use PowerView to identify what AD groups have admin rights on computers by OU.

```
PS C:\> Find-GPOComputerAdmin -OUName 'OU=Workstations,DC=lab,DC=adsecurity,DC=org'


ComputerName   :
GPODisplayName : Add Workstation Admins to Local Administrators Group
GPOPath        : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{45556105-EFE6
                 92C-AACB1D3D4DE5}
ObjectName     : Workstation Admins
ObjectDN       : CN=Workstation Admins,OU=AD Management,DC=lab,DC=adsecurity,DC=org
ObjectSID      : S-1-5-21-1581655573-3923512380-696647894-2627
IsGroup        : True



PS C:\> get-NetComputer -ADSpath 'OU=Workstations,DC=lab,DC=adsecurity,DC=org'
ADSWRKWIN7.lab.adsecurity.org
ADSWKWIN7.lab.adsecurity.org
ADSWKWin10.lab.adsecurity.org
```

Active Directory Object Permissions (ACLs)

Similar to file system permissions, Active Directory objects have permissions as well.

These permissions are called Access Control Lists (ACLs). The permissions set on objects use a cryptic format called Security Descriptor Definition Language (SDDL) which looks like this:
D:PAI(D;OICI;FA;;;BG)(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)
(A;OICI;FA;;;BU)

This is translated by the GUI to provide the more user-friendly format we are used to (see screenshot below).

Every Active Directory object has permissions configured on them, either explicitly defined, or inherited from an object above them (typically an OU or the domain) and the permission can be defined to either allow or deny permissions on the object and its properties.

When performing Active Directory security assessments, we scan Active Directory for AD ACLs and identify the accounts/groups with privileged rights based on the delegation on AD objects such as the domain, OUs, security groups, etc.

Every object in Active Directory has default permissions applied to it as well as inherited and any explicit permissions. Given that by default Authenticated Users have read access to objects in AD, most of their properties and the permissions defined on the objects, AD objects, their properties and permissions are easily gathered.

One quick note about AD ACLs. There is an object in the System container called "AdminSDHolder " which only has one purpose: to be the permissions template object for objects (and their members) with high levels of permissions in the domain.

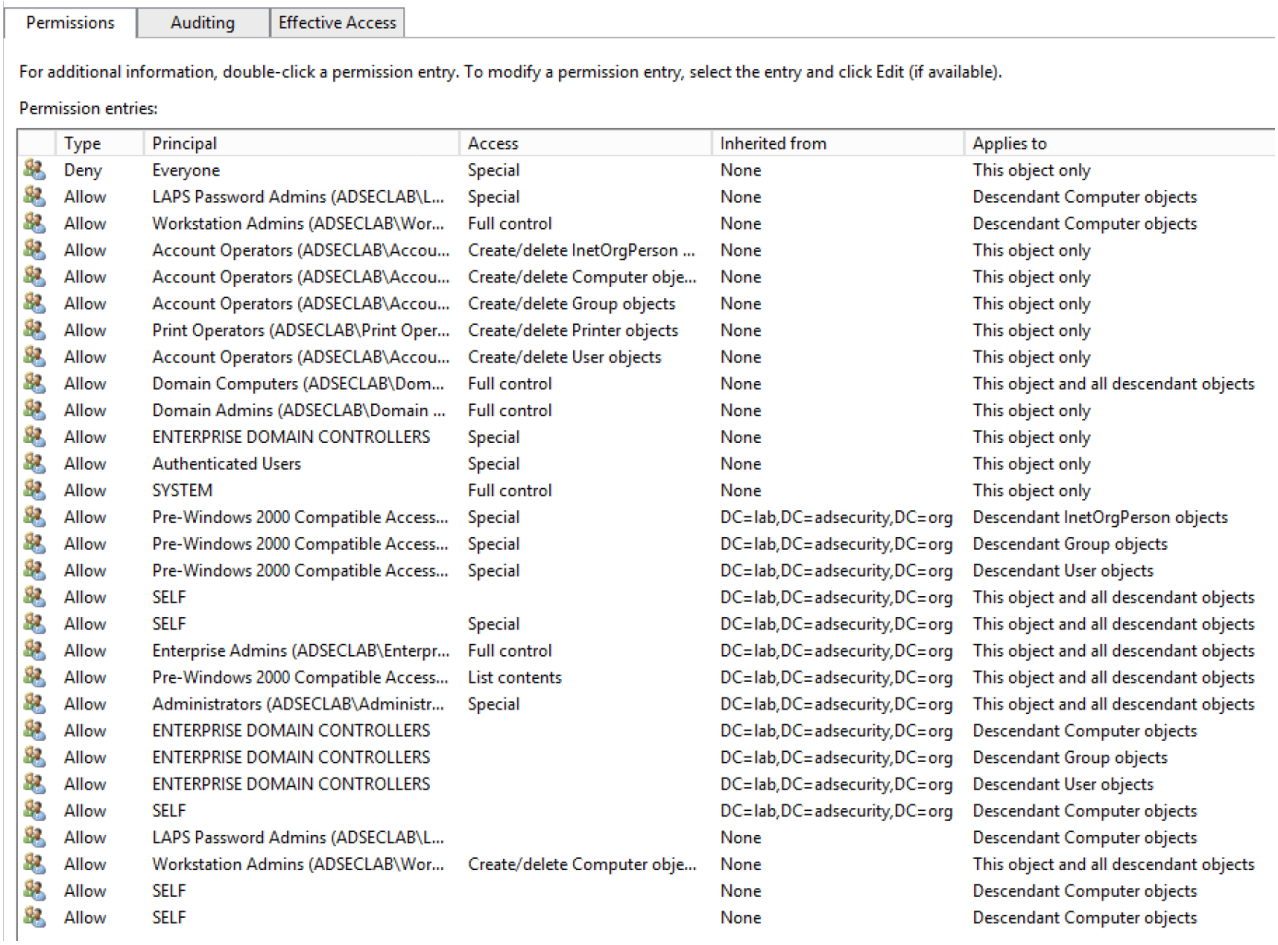
SDProp Protected Objects (Windows Server 2008 & Windows Server 2008 R2):

- Account Operators
- Administrator
- Administrators
- Backup Operators
- Domain Admins
- Domain Controllers
- Enterprise Admins
- Krbtgt
- Print Operators
- Read-only Domain Controllers
- Replicator
- Schema Admins
- Server Operators

About every 60 minutes, the PDC emulator runs a process to enumerate all of these protected objects and their members and then stamps the permissions configured on the AdminSDHolder object (and sets the admin attribute to '1'). This ensures that privileged

groups and accounts are protected from improper AD permission delegation.

It's extremely difficult to stay on top of custom permissions on AD objects. For example, the following graphic shows permissions on an OU.



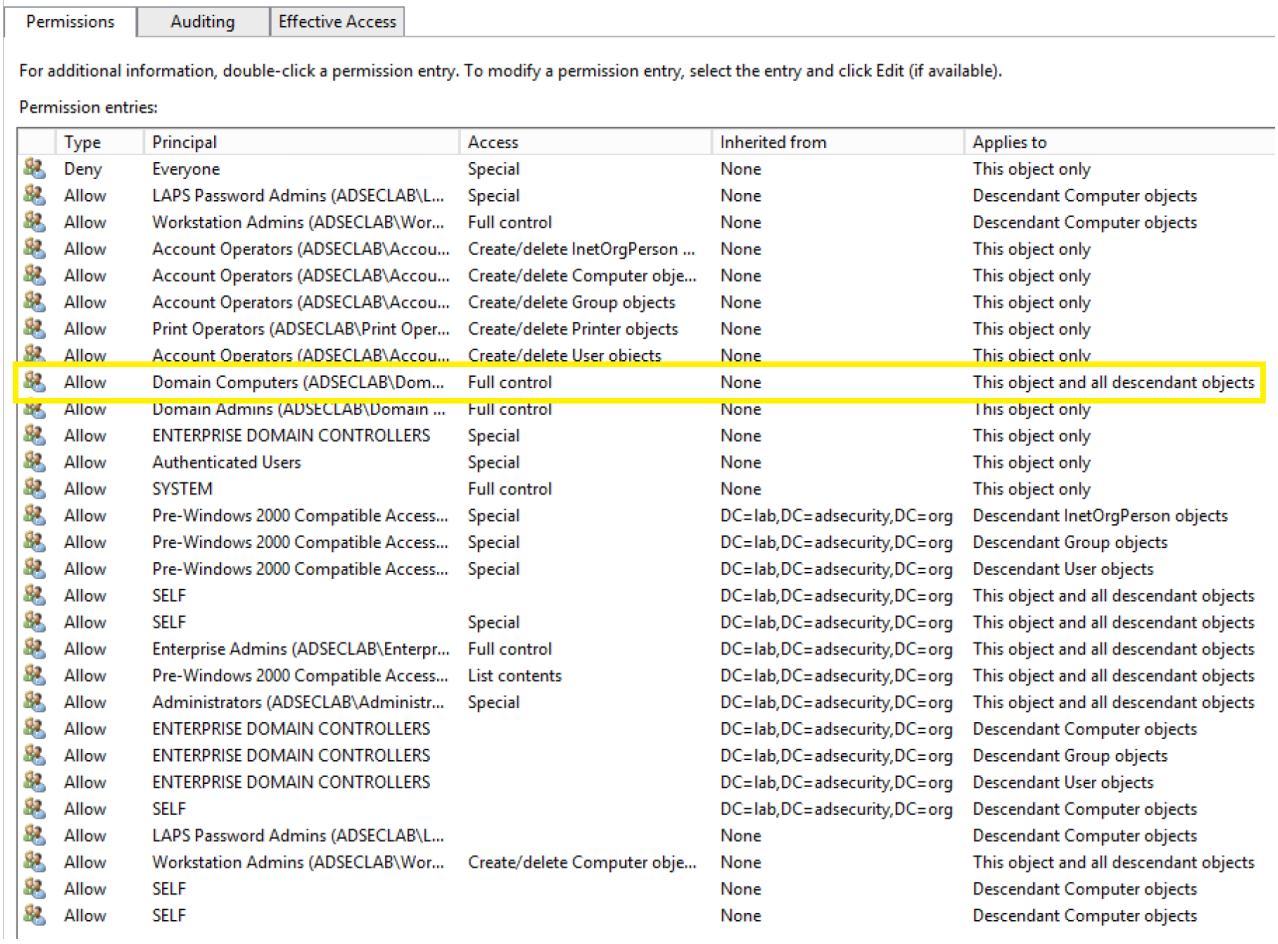
Permissions | Auditing | Effective Access

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

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Deny	Everyone	Special	None	This object only
Allow	LAPS Password Admins (ADSECLAB\L...	Special	None	Descendant Computer objects
Allow	Workstation Admins (ADSECLAB\Wor...	Full control	None	Descendant Computer objects
Allow	Account Operators (ADSECLAB\Accou...	Create/delete InetOrgPerson ...	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete Computer obje...	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete Group objects	None	This object only
Allow	Print Operators (ADSECLAB\Print Oper...	Create/delete Printer objects	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete User objects	None	This object only
Allow	Domain Computers (ADSECLAB\Dom...	Full control	None	This object and all descendant objects
Allow	Domain Admins (ADSECLAB\Domain ...	Full control	None	This object only
Allow	ENTERPRISE DOMAIN CONTROLLERS	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant InetOrgPerson objects
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant Group objects
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant User objects
Allow	SELF		DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	SELF	Special	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	Enterprise Admins (ADSECLAB\Enterpr...	Full control	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	Pre-Windows 2000 Compatible Access...	List contents	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	Administrators (ADSECLAB\Administr...	Special	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	ENTERPRISE DOMAIN CONTROLLERS		DC=lab,DC=adsecurity,DC=org	Descendant Computer objects
Allow	ENTERPRISE DOMAIN CONTROLLERS		DC=lab,DC=adsecurity,DC=org	Descendant Group objects
Allow	ENTERPRISE DOMAIN CONTROLLERS		DC=lab,DC=adsecurity,DC=org	Descendant User objects
Allow	SELF		DC=lab,DC=adsecurity,DC=org	Descendant Computer objects
Allow	LAPS Password Admins (ADSECLAB\L...		None	Descendant Computer objects
Allow	Workstation Admins (ADSECLAB\Wor...	Create/delete Computer obje...	None	This object and all descendant objects
Allow	SELF		None	Descendant Computer objects
Allow	SELF		None	Descendant Computer objects

There's a serious issue with the delegation on this OU which is highlighted below.
This issue is delegation to Domain Controllers with Full Control rights on all objects to this OU and all objects contained in it.



Permissions | Auditing | Effective Access

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

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Deny	Everyone	Special	None	This object only
Allow	LAPS Password Admins (ADSECLAB\L...	Special	None	Descendant Computer objects
Allow	Workstation Admins (ADSECLAB\Wor...	Full control	None	Descendant Computer objects
Allow	Account Operators (ADSECLAB\Accou...	Create/delete InetOrgPerson ...	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete Computer obje...	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete Group objects	None	This object only
Allow	Print Operators (ADSECLAB\Print Oper...	Create/delete Printer objects	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete User objects	None	This object only
Allow	Domain Computers (ADSECLAB\Dom...	Full control	None	This object and all descendant objects
Allow	Domain Admins (ADSECLAB\Domain ...	Full control	None	This object only
Allow	ENTERPRISE DOMAIN CONTROLLERS	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant InetOrgPerson objects
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant Group objects
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant User objects
Allow	SELF		DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	SELF	Special	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	Enterprise Admins (ADSECLAB\Enterpr...	Full control	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	Pre-Windows 2000 Compatible Access...	List contents	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	Administrators (ADSECLAB\Administr...	Special	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	ENTERPRISE DOMAIN CONTROLLERS		DC=lab,DC=adsecurity,DC=org	Descendant Computer objects
Allow	ENTERPRISE DOMAIN CONTROLLERS		DC=lab,DC=adsecurity,DC=org	Descendant Group objects
Allow	ENTERPRISE DOMAIN CONTROLLERS		DC=lab,DC=adsecurity,DC=org	Descendant User objects
Allow	SELF		DC=lab,DC=adsecurity,DC=org	Descendant Computer objects
Allow	LAPS Password Admins (ADSECLAB\L...		None	Descendant Computer objects
Allow	Workstation Admins (ADSECLAB\Wor...	Create/delete Computer obje...	None	This object and all descendant objects
Allow	SELF		None	Descendant Computer objects
Allow	SELF		None	Descendant Computer objects

An attacker is most interested in permissions that provide privileged actions. These ACLs include:

- **Replicating Directory Changes All**
  Extended right needed to replicate only those changes from a given NC that are also replicated to the Global Catalog (which includes secret domain data). This constraint is only meaningful for Domain NCs.
  An Extended Right that provides the ability to replicate all data for an object, including password data (I call this the Domain Controller impersonation right) which when combined with Replicating Directory Changes, provides the ability to "DCSync" the password data for AD users and computers. See my write-up on DCSync usage & detection for more detail.
  Example: FIM, Riverbed, SharePoint, and other applications often have a service account granted this right on the domain root. If an attacker can guess this password (or potentially crack it by Kerberoasting), they now own the domain since they can DCSync password hashes for all AD users and computers (including Domain Admins and Domain Controllers).
- Replicating Directory Changes (DS-Replication-Get-Changes)
  Control access right that allows the replication of all data in a given replication NC, excluding secret domain data.
  This right provides the ability to pull data from Active Directory regardless of configured AD ACLs.

- **GenericAll**: GenericAll = Full Control
  The right to create or delete children, delete a subtree, read and write properties, examine children and the object itself, add and remove the object from the directory, and read or write with an extended right.
  It provides full rights to the object and all properties, including confidential attributes such as LAPS local Administrator passwords, and BitLocker recovery keys. In many cases, Full Control rights aren't required, but it's easier to delegate and get working than determining the actual rights required.
  Example: A Server tier group may be delegated Full Control on all Computer objects in an OU that has the computer objects associated with servers. Another common configuration is delegating Full Control on all Computer objects in the Workstations OU for the Desktop Support group, and delegating Full Control on all user objects in the Users OU for the Help Desk.
- **GenericWrite**: Provides write access to all properties.
  The right to read permissions on this object, write all the properties on this object, and perform all validated writes to this object.
- **WriteDACL**: Provides the ability to modify security on an object which can lead to Full Control of the object.
  The right to modify the DACL in the object security descriptor.
  Example: A service account may be granted this right to perform delegation in AD. If an attacker can guess this password (or potentially crack it by Kerberoasting), they now set their own permissions on associated objects which can lead to Full Control of an object which may involve exposure of a LAPS controlled local Administrator password.
- **Self:** Provides the ability to perform validated writes.
  The right to perform an operation that is controlled by a validated write access right.
  Validated writes include the following attributes:
  - Self-Membership(bf9679c0-0de6-11d0-a285-00aa003049e2 / member attribute)
  - Validated-DNS-Host-Name (72e39547-7b18-11d1-adef-00c04fd8d5cd / dNSHostName attribute)
  - Validated-MS-DS-Additional-DNS-Host-Name (80863791-dbe9-4eb8-837e-7f0ab55d9ac7 / msDS-AdditionalDnsHostName attribute)
  - Validated-MS-DS-Behavior-Version (d31a8757-2447-4545-8081-3bb610cacbf2 / msDS-Behavior-Version attribute)
  - Validated-SPN (f3a64788-5306-11d1-a9c5-0000f80367c1 / servicePrincipalName attribute)
- **WriteOwner:**: Provides the ability to take ownership of an object. The owner of an object can gain full control rights on the object.
  The right to assume ownership of the object. The user must be an object trustee. The user cannot transfer the ownership to other users.

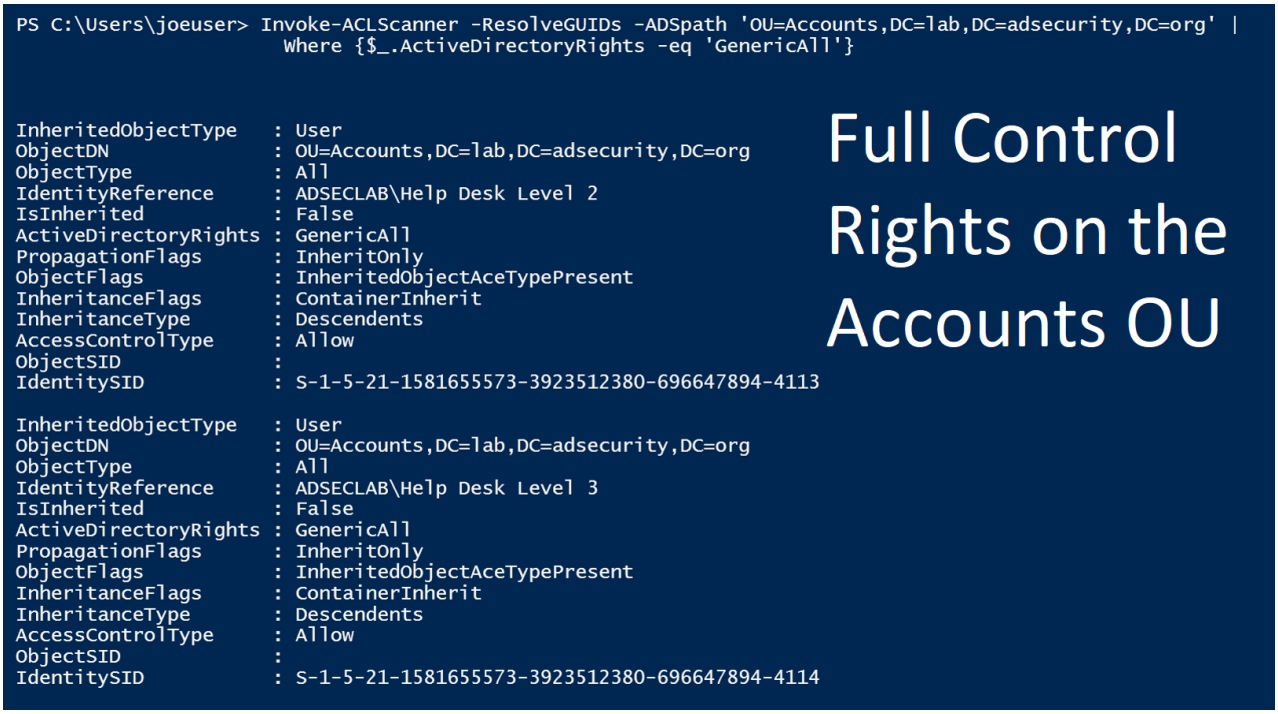
- **WriteProperty**: Typically paired with specific attribute/property information.Example: The help desk group is delegated the ability to modify specific AD object properties like Member (to modify group membership), Display Name, Description, Phone Number, etc.
- **CreateChild**: Provides the ability to create an object of a specified type (or “All”).
- **DeleteChild**: Provides the ability to delete an object of a specified type (or “All”).
- **Extended Right**: This is an interesting one because if provides additional rights beyond the obvious.Example: All Extended Right permissions to a computer object may provide read access to the LAPS Local Administrator password attribute.

Andy Robbin’s (@_Wald0) post covers ways these rights can be abused.

The ability to create and link GPOs in a domain should be seen as effective Domain Admin rights since it provides the ability to modify security settings, install software, configure user and computer logon (and startup/shutdown) scripts, and run commands.

- **Manage Group Policy link (LinkGPO)**: Provides the ability to link an existing Group Policy Object in Active Directory to the domain, OU, and/or site where the right is defined. *By default, GPO Creator Owners has this right.*
- **Create GPOs**: By default, the AD group Group Policy Creator Owners has this right. Can be delegated via the Group Policy Management Console (GPMC).

PowerView provides the ability to to search AD permissions for interesting rights.



SIDHistory

SID History is an attribute that supports migration scenarios. Every user account has an associated Security IDentifier (SID) which is used to track the security principal and the access the account has when connecting to resources. SID History enables access for another account to effectively be cloned to another. This is extremely useful to ensure users retain access when moved (migrated) from one domain to another. Since the user's SID changes when the new account is created, the old SID needs to map to the new one. When a user in Domain A is migrated to Domain B, a new user account is created in DomainB and DomainA user's SID is added to DomainB's user account's SID History attribute. This ensures that DomainB user can still access resources in DomainA.

This means that if an account has privileged accounts or groups in its SIDHistory attribute, the account receives all the rights assigned to those accounts or groups, be they assigned directly or indirectly. If an attacker gains control of this account, they have all of the associated rights. The rights provided via SIDs in SIDHistory are likely not obvious and therefore missed.

Group Policy Permissions

Group Policy Objects (GPOs) are created, configured, and linked in Active Directory. When a GPO is linked to an OU, the settings in the GPO are applied to the appropriate objects (users/computers) in that OU.

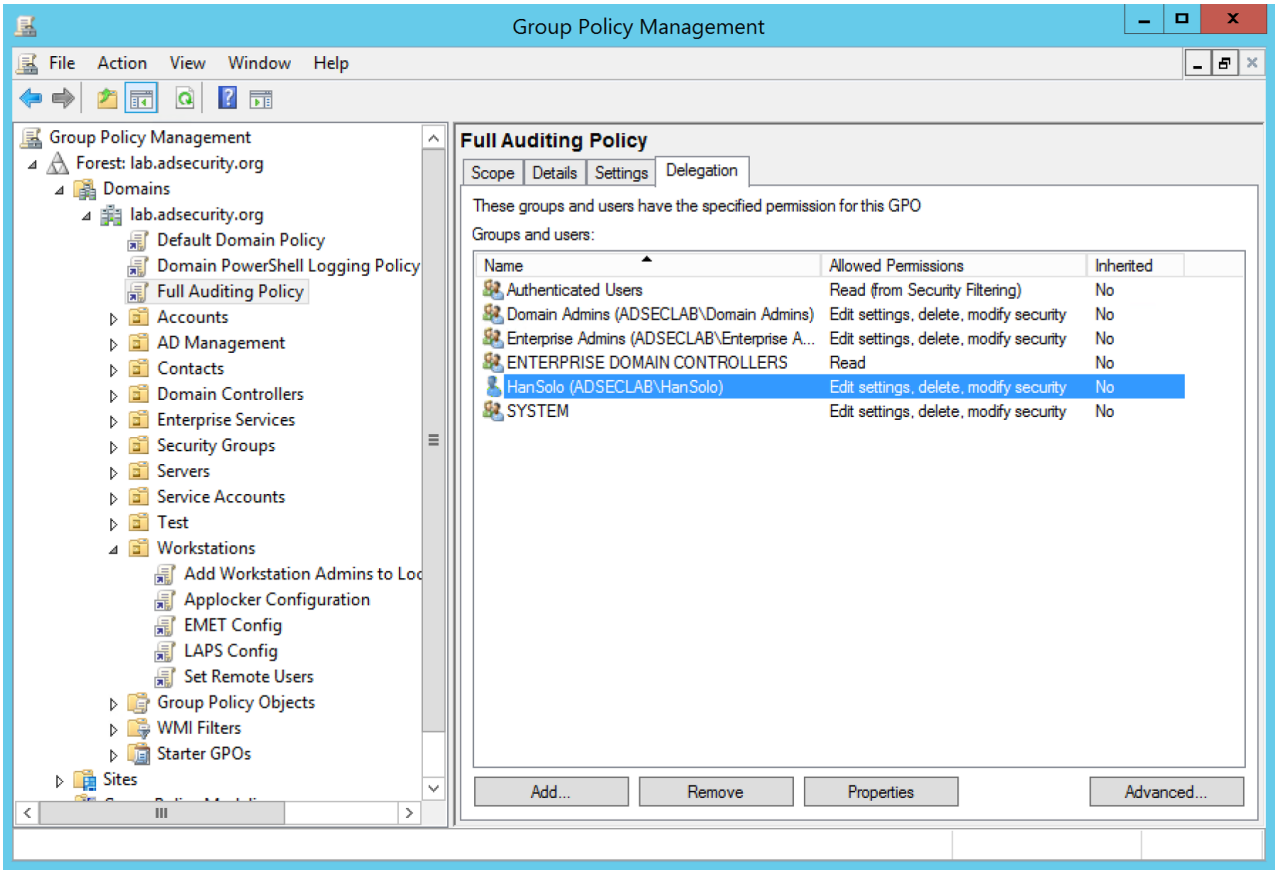
Permissions on GPOs can be configured to delegate GPO modify rights to any security principal.

If there are custom permissions configured on Group Policies linked to the domain and an attacker gains access to an account with modify access, the domain can be compromised. An attacker modifies GPO settings to run code or install malware. The

impact of this level of access depends on where the GPO is linked. If the GPO is linked to the domain or Domain Controllers container, they own the domain. IF the GPO is linked to a workstations or servers OU, the impact may be less somewhat; however, the ability to run code on all workstations or servers, it may be possible to still compromise the domain.

Scanning for GPO permissions identifies which GPOs are improperly permissioned and scanning for where the GPO is linked determines the impact.

Fun fact: The creator of a Group Policy retains modify rights to the GPO. A possible result is that a Domain Admin needs to set an audit policy for the domain, but discovers that an OU admin has already created a GPO with the required settings. So, the Domain Admin links this GPO to the domain root which applies the settings to all computers in the domain. The problem is the OU admin can still modify a GPO that is now linked to the domain root providing an escalation path if this OU admin account is compromised. The following graphic shows the OU Admin “Han Solo” with GPO edit rights.



PowerView provides a quick way to scan all the permissions for all domain GPOs:

```
Get-NetGPO | %{Get-ObjectAcl -ResolveGUIDs -Name $_.Name}
```

Reference: Abusing GPO Permissions

User Rights Assignment

User Rights Assignments are frequently configured in a computer GPO and defines several rights to the computer.

Domain Controllers are often configured with User Rights Assignments in the Default Domain Controllers Policy applied to the Domain Controllers container. Parsing the GPOs linked to Domain Controllers provides useful information about security principals with elevated rights to DCs and the domain.

These assignments include:

- SeTrustedCredManAccessPrivilege: Access Credential Manager as a trusted caller
- SeNetworkLogonRight: Access this computer from the network
- SeTcbPrivilege: Act as part of the operating system
- SeMachineAccountPrivilege: Add workstations to domain
- SeIncreaseQuotaPrivilege: Adjust memory quotas for a process
- SeInteractiveLogonRight: Allow log on locally
- SeRemoteInteractiveLogonRight: Allow log on through Remote Desktop Services
- SeBackupPrivilege: Back up files and directories
- SeChangeNotifyPrivilege: Bypass traverse checking
- SeSystemtimePrivilege: Change the system time
- SeTimeZonePrivilege: Change the time zone
- SeCreatePagefilePrivilege: Create a pagefile
- SeCreateTokenPrivilege: Create a token object
- SeCreateGlobalPrivilege: Create global objects
- SeCreatePermanentPrivilege: Create permanent shared objects
- SeCreateSymbolicLinkPrivilege: Create symbolic links
- SeDebugPrivilege: Debug programs
- SeDenyNetworkLogonRight: Deny access to this computer from the network
- SeDenyBatchLogonRight: Deny log on as a batch job
- SeDenyServiceLogonRight: Deny log on as a service
- SeDenyInteractiveLogonRight: Deny log on locally
- SeDenyRemoteInteractiveLogonRight: Deny log on through Remote Desktop Services
- SeEnableDelegationPrivilege: Enable computer and user accounts to be trusted for delegation
- SeRemoteShutdownPrivilege: Force shutdown from a remote system
- SeAuditPrivilege: Generate security audits
- SeImpersonatePrivilege: Impersonate a client after authentication
- SeIncreaseWorkingSetPrivilege: Increase a process working set
- SeIncreaseBasePriorityPrivilege: Increase scheduling priority
- SeLoadDriverPrivilege: Load and unload device drivers
- SeLockMemoryPrivilege: Lock pages in memory
- SeBatchLogonRight: Log on as a batch job
- SeServiceLogonRight: Log on as a service
- SeSecurityPrivilege: Manage auditing and security log
- SeRelabelPrivilege: Modify an object label
- SeSystemEnvironmentPrivilege: Modify firmware environment values
- SeManageVolumePrivilege: Perform volume maintenance tasks

- SeProfileSingleProcessPrivilege: Profile single process
- SeSystemProfilePrivilege: Profile system performance
- SeUndockPrivilege: Remove computer from docking station
- SeAssignPrimaryTokenPrivilege: Replace a process level token
- SeRestorePrivilege: Restore files and directories
- SeShutdownPrivilege: Shut down the system
- SeSyncAgentPrivilege: Synchronize directory service data
- SeTakeOwnershipPrivilege: Take ownership of files or other objects

The interesting ones in this list (especially in GPOs that apply to Domain Controllers):

- Manage auditing and security log: Provides the ability to view all events in the event logs, including security events, and clear the event log.
  Fun Fact: Exchange Servers require this right, which means that if an attacker gains System rights on an Exchange server, they can clear Domain Controller security logs.
- Synchronize directory service data: *"This policy setting determines which users and groups have authority to synchronize all directory service data, regardless of the protection for objects and properties. This privilege is required to use LDAP directory synchronization (dirsync) services. Domain controllers have this user right inherently because the synchronization process runs in the context of the* ***System*** *account on domain controllers."*
  This means that an acocunt with this user right on a Domain Controller may be able to run DCSync.
- Enable computer and user accounts to be trusted for delegation: Provides the ability to configure delegation on computers and users in the domain.
  Fun Fact: This provides the ability to set Kerberos delegation on a computer or user account.
- Impersonate a client after authentication: This one looks like some fun could be had with it…
- Take ownership of files or other objects: Administrators only. *"Any users with the* ***Take ownership of files or other objects user right*** *can take control of any object, regardless of the permissions on that object, and then make any changes that they want to make to that object. Such changes could result in exposure of data, corruption of data, or a denial-of-service condition."*
- Load and Unload Device Drivers: *"Device drivers run as highly privileged code. A user who has the Load and unload device drivers user right could unintentionally install malware that masquerades as a device driver. Administrators should exercise care and install only drivers with verified digital signatures."*

Putting it all together

In order to effectively identify all accounts with privileged access, it's important to ensure that all avenues are explored to effectively identify the rights. This means that defenders need to check the permission on AD objects, starting with Organizational Units (OUs) and then branching out to security groups.

Things to check:

- Enumerate group membership of default groups (including sub-groups). Identify what rights are required and remove the others.
- Scan Active Directory (specifically OUs & security groups) for custom delegation.
- Scan for accounts with SIDHistory (should only be required during an active migration from one domain to another).
- Review User Rights Assignments in GPOs that apply to Domain Controllers, Servers, and Workstations.
- Review GPOs that add AD groups to local groups and ensure these are still required and the level of rights are appropriate.

Tools for Checking Active Directory Permissions:

- Bloodhound
- PowerView (modules used in Bloodhound)
- AD ACL Scanner

Confused by this and want some help unraveling the AD permissions in your organization?
Contact Trimarc, we love this stuff!

References

- BloodHound 1.3 – The ACL Attack Path Update
  https://wald0.com/?p=112
- Abusing Active Directory Permissions with PowerView
  http://www.harmj0y.net/blog/redteaming/abusing-active-directory-permissions-with-powerview/
- Abusing GPO Permissions
  http://www.harmj0y.net/blog/redteaming/abusing-gpo-permissions/
- AD DS Owner Rights
  https://technet.microsoft.com/en-us/library/dd125370(v=ws.10).aspx
- Security Descriptor Definition Language for Conditional ACEs
  https://msdn.microsoft.com/en-us/library/windows/desktop/dd981030(v=vs.85).aspx
- Sneaky Active Directory Persistence #15: Leverage AdminSDHolder & SDProp to (Re)Gain Domain Admin Rights
  https://adsecurity.org/?p=1906
- The Security Descriptor Definition Language of Love (Part 1)
  https://blogs.technet.microsoft.com/askds/2008/04/18/the-security-descriptor-definition-language-of-love-part-1/
- ActiveDirectoryRights Enumeration
  https://msdn.microsoft.com/en-us/library/system.directoryservices.activedirectoryrights(v=vs.110).aspx
- Bloodhound
- PowerView

- AD ACL Scanner
- AD Security: SIDHistory
- User Rights Assignments
- Active Directory Security Groups
- ActiveDirectoryRights Enumeration

(Visited 156,178 times, 20 visits today)