Active Directory Recon 是一个新的热点，因为攻击者，Red Teamers 和渗透测试人员已经意识到 Active Directory 的控制可以为组织提供动力。
在 Blue Hat 和 Red Team 的 Black Hat 和 DEF CON 会谈中，我介绍了使用 PowerView（由 Will @ harmj0y 编写）在 AD 中枚举权限的方法。

本文详细介绍了如何在 Active Directory 中委派特权访问，以及如何最好地发现谁在 AD 中拥有哪些权限。

Active Directory Privileged Access

挑战通常是确定每个组实际拥有的访问权限。组织通常不会完全理解组访问实际所具有的全部影响。攻击者利用访问权限（虽然并非总是特权访问）来破坏 Active Directory。

经常遗漏的关键点是 Active Directory 和关键资源的权限不仅仅是组成员身份，而是用户拥有的组合权限由以下组成：

Active Directory 组成员身份。
AD 组在计算机上具有特权
通过修改默认权限（对于直接和间接的安全主体）委派 AD 对象的权限。
分配给 SIDHistory 中的 SID 到 AD 对象的权限。
委派组策略对象的权限。
通过组策略（或本地策略）在工作站，服务器和域控制器上配置的用户权限分配定义了对这些系统的提升权限。
计算机或计算机上的本地组成员身份（类似于 GPO 分配的设置）。
委派共享文件夹的权限。

Group Membership

枚举组成员身份是在 Active Directory 中发现特权帐户的简便方法，尽管它通常不能说明完整的故事。Domain Admins，Administrators 和 Enterprise Admins 中的成员资格显然提供完整的域/林管理员权限。创建自定义组并委派对资源的访问权限。
比如通过 powerview.ps1 的 get-Netgroup 功能查看组内所有名称中带有 admin 的组

```
PS C:\Users\administrator.YUNYING\Desktop> get-netgroup "*admin*" | Get-NetGroupMember


GroupDomain             : yunying.lab
GroupName               : Administrators
GroupDistinguishedName  : CN=Administrators,CN=Builtin,DC=yunying,DC=lab
MemberDomain            : yunying.lab
MemberName              : Domain Admins
MemberDistinguishedName : CN=Domain Admins,CN=Users,DC=yunying,DC=lab
MemberObjectClass       : group
MemberSID               : S-1-5-21-4054579877-26337388-655639334-512

GroupDomain             : yunying.lab
GroupName               : Administrators
GroupDistinguishedName  : CN=Administrators,CN=Builtin,DC=yunying,DC=lab
MemberDomain            : yunying.lab
MemberName              : Enterprise Admins
MemberDistinguishedName : CN=Enterprise Admins,CN=Users,DC=yunying,DC=lab
MemberObjectClass       : group
MemberSID               : S-1-5-21-4054579877-26337388-655639334-519

GroupDomain             : yunying.lab
GroupName               : Administrators
GroupDistinguishedName  : CN=Administrators,CN=Builtin,DC=yunying,DC=lab
MemberDomain            : yunying.lab
MemberName              : Administrator
MemberDistinguishedName : CN=Administrator,CN=Users,DC=yunying,DC=lab
MemberObjectClass       : user
```

默认情况下能够提升权限的组 Account Operators：

Account Operators 具有域用户和组的默认权限的 Active Directory 组，以及登录到域控制器的功能，已知的 SID/RID：S-1-5-32-548

```
PS C:\Users\administrator.YUNYING\Desktop> get-netgroup "Account Operators"


usncreated             : 12363
admincount             : 1
iscriticalsystemobject : True
grouptype              : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY
samaccountname         : Account Operators
whenchanged            : 2019/7/10 4:56:55
objectsid              : S-1-5-32-548
objectclass            : {top, group}
cn                     : Account Operators
usnchanged             : 28416
dscorepropagationdata  : {2019/7/11 0:09:32, 2019/7/10 4:56:55, 2019/7/10 4:28:12, 2019/7/10 4:28:12...}
name                   : Account Operators
description            : 成员可以管理域用户和组帐户
distinguishedname      : CN=Account Operators,CN=Builtin,DC=yunying,DC=lab
samaccounttype         : ALIAS_OBJECT
systemflags            : -1946157056
whencreated            : 2019/7/10 2:38:22
instancetype           : 4
objectguid             : 4b3377ec-40a4-4b0f-aab1-272e238ef296
objectcategory         : CN=Group,CN=Schema,CN=Configuration,DC=yunying,DC=lab
```

Account Operators 组授予有限的帐户创建权限一个用户。该组的成员可以创建和修改大多数类型的帐户，包括用户，本地组和全局组，并且成员可以本地登录到域控制器。

Account Operators 组的成员无法管理 Administrator 用户帐户，管理员的用户帐户或 Administrators，Server Operators，Account Operators，Backup Operators 或 Print Operators 组。该组的成员无法修改用户权限。

Account Operators 组适用于按操作系统版本在 Active Directory 默认安全组中列出的 Windows Server 操作系统版本。

默认情况下，此内置组没有成员，它可以创建和管理域中的用户和组，包括其自己的成员身份和 Server Operators 组的成员身份。该组被视为服务管理员组，因为它可以修改服务器操作员，而操作员操作员又可以修改域控制器设置。作为最佳实践，请将此组的成员身份留空，并且不要将其用于任何委派管理。无法重命名，删除或移动此组。

Administrators:

本地或 Active Directory 组。AD 组具有 Active Directory 域和域控制器的完全管理权限。
已知的 SID / RID：S-1-5-32-544
Administrators 组的成员具有对计算机的完全且不受限制的访问权限，或者如果计算机是提升为域控制器，成员可以无限制地访问域。
Administrators 组按操作系统版本应用于 Active Directory 默认安全组中列出的 Windows Server 操作系统版本。

Administrators 组具有内置功能，可使其成员完全控制系统。无法重命名，删除或移动此组。此内置组控制对其域中所有域控制器的访问，并且可以更改所有管理组的成员身份。
成员身份可由以下组的成员修改：默认服务管理员，域中的域管理员或企业管理员。该组具有获取目录中任何对象或域控制器上任何资源的所有权的特殊权限。此帐户被视为服务管理员组，因为其成员对域中的域控制器具有完全访问权限。

此安全组包括自 Windows Server 2008 以来的以下更改：
默认用户权限更改：允许通过 Windows Server 2008 中存在的终端服务登录，并且已由“允许通过远程桌面服务登录”替换。

PowerView 提供的搜索 AD 权限的功能

```
PS C:\Users\administrator.YUNYING\Desktop> Invoke-ACLScanner


ObjectDN                : DC=yunying,DC=lab
AceQualifier            : AccessAllowed
ActiveDirectoryRights   : ExtendedRight
ObjectAceType           : ab721a53-1e2f-11d0-9819-00aa0040529b
AceFlags                : ContainerInherit
AceType                 : AccessAllowedObject
InheritanceFlags        : ContainerInherit
SecurityIdentifier      : S-1-5-21-4054579877-26337388-655639334-1120
IdentityReferenceName   : Exchange Windows Permissions
IdentityReferenceDomain : yunying.lab
IdentityReferenceDN     : CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=yunying,DC=lab
IdentityReferenceClass  : group

ObjectDN                : DC=yunying,DC=lab
AceQualifier            : AccessAllowed
ActiveDirectoryRights   : ExtendedRight
ObjectAceType           : 00299570-246d-11d0-a768-00aa006e0529
AceFlags                : ContainerInherit
AceType                 : AccessAllowedObject
InheritanceFlags        : ContainerInherit
```

直接运行会显示所有的 ACE