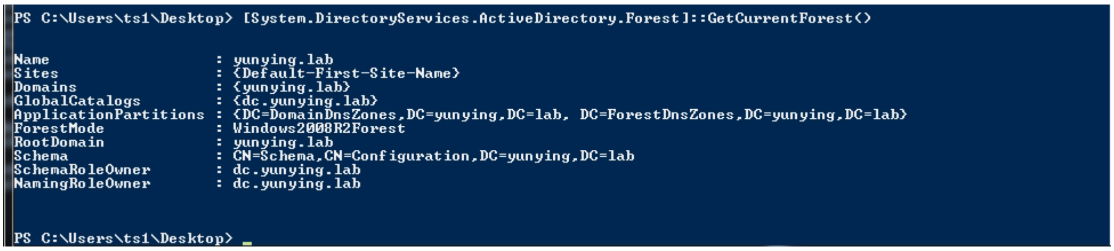
本文主要说明在普通域用户权限下如何进行 AD 域的信息收集。在收集域信息时一个很好的脚本就是 PowerView，就是 harmj0y 写的那个，这里介绍的均来自 windows 原生的命令。

获取 AD 信息

1、获取当前域林的信息

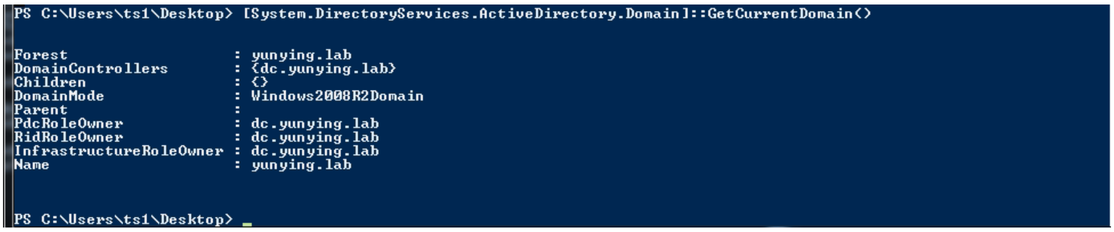
[System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest()



```
PS C:\Users\ts1\Desktop> [System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest()


Name                  : yunying.lab
Sites                 : {Default-First-Site-Name}
Domains               : {yunying.lab}
GlobalCatalogs        : {dc.yunying.lab}
ApplicationPartitions : {DC=DomainDnsZones,DC=yunying,DC=lab, DC=ForestDnsZones,DC=yunying,DC=lab}
ForestMode            : Windows2008R2Forest
RootDomain            : yunying.lab
Schema                : CN=Schema,CN=Configuration,DC=yunying,DC=lab
SchemaRoleOwner       : dc.yunying.lab
NamingRoleOwner       : dc.yunying.lab



PS C:\Users\ts1\Desktop> _
```

2、查看当前域信息

[System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()

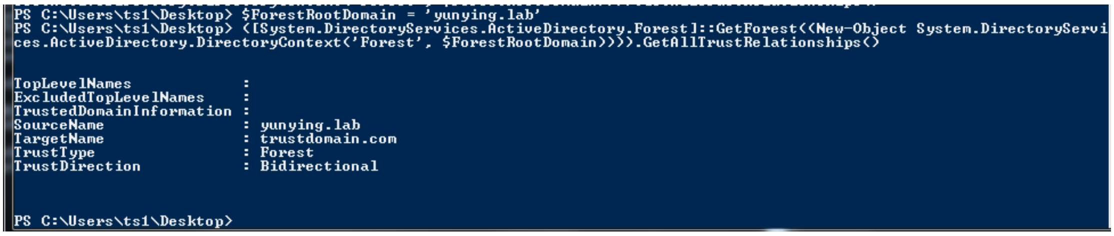


```
PS C:\Users\ts1\Desktop> [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()


Forest                  : yunying.lab
DomainControllers       : {dc.yunying.lab}
Children                : {}
DomainMode              : Windows2008R2Domain
Parent                  :
PdcRoleOwner            : dc.yunying.lab
RidRoleOwner            : dc.yunying.lab
InfrastructureRoleOwner : dc.yunying.lab
Name                    : yunying.lab



PS C:\Users\ts1\Desktop> _
```

3、查看域林信任

$ForestRootDomain = ‘lab.adsecurity.org’

([System.DirectoryServices.ActiveDirectory.Forest]::GetForest((New-Object System.DirectoryServices.ActiveDirectory.DirectoryContext(‘Forest’, $ForestRootDomain)))).GetAllTrustRelationships()

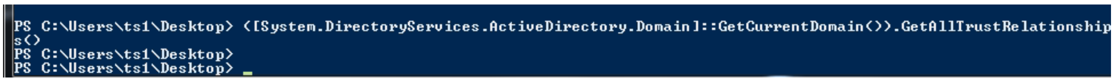


```
PS C:\Users\ts1\Desktop> $ForestRootDomain = 'yunying.lab'
PS C:\Users\ts1\Desktop> ([System.DirectoryServices.ActiveDirectory.Forest]::GetForest((New-Object System.DirectoryServi
ces.ActiveDirectory.DirectoryContext('Forest', $ForestRootDomain)))).GetAllTrustRelationships()


TopLevelNames             :
ExcludedTopLevelNames     :
TrustedDomainInformation  :
SourceName                : yunying.lab
TargetName                : trustdomain.com
TrustType                 : Forest
TrustDirection            : Bidirectional



PS C:\Users\ts1\Desktop>
```

4、域信任

没有配置域信任，结果为空白

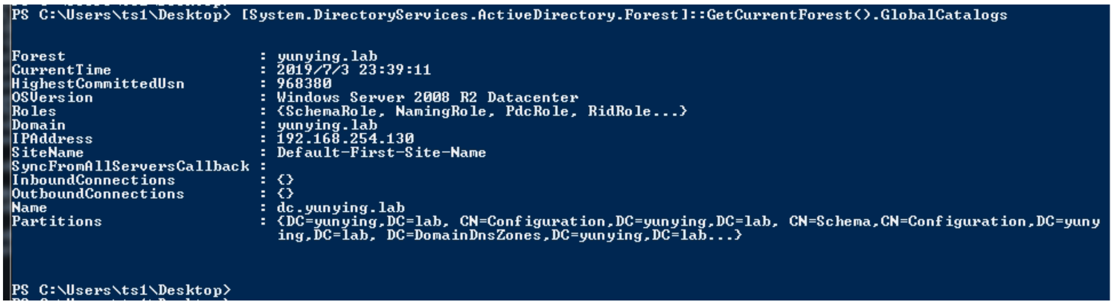
([System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()).GetAllTrustRelationships()



```
PS C:\Users\ts1\Desktop> ([System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()).GetAllTrustRelationship
s()
PS C:\Users\ts1\Desktop>
PS C:\Users\ts1\Desktop> _
```

5、查看域林的全局目录

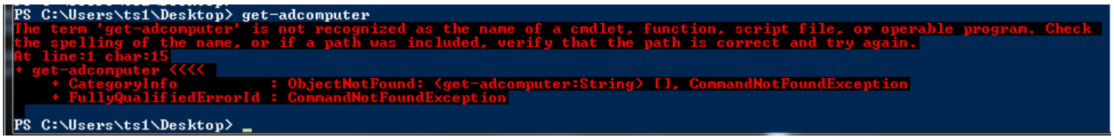
[System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest().GlobalCatalogs



```
PS C:\Users\ts1\Desktop> [System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest().GlobalCatalogs


Forest                     : yunying.lab
CurrentTime                : 2019/7/3 23:39:11
HighestCommittedUsn        : 968380
OSVersion                  : Windows Server 2008 R2 Datacenter
Roles                      : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain                     : yunying.lab
IPAddress                  : 192.168.254.130
SiteName                   : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections         : {}
OutboundConnections        : {}
Name                       : dc.yunying.lab
Partitions                 : {DC=yunying,DC=lab, CN=Configuration,DC=yunying,DC=lab, CN=Schema,CN=Configuration,DC=yuny
                             ing,DC=lab, DC=DomainDnsZones,DC=yunying,DC=lab...}



PS C:\Users\ts1\Desktop>
```

不通过网络扫描而发现企业服务

这里说的主要是通过 SPN 能够发现内网中所有使用 kerberos 协议认证的服务的主机或者账户。比如 TERMSRV（RDP 服务）、WSMAN（WinRM）还有一些比如 MSSQL。下面的命令在 windows 8 和 windows server 2012 R2 及以上版本才能使用（或者是 powershell4.0），在 win7 或者是 win2008 是不行的。

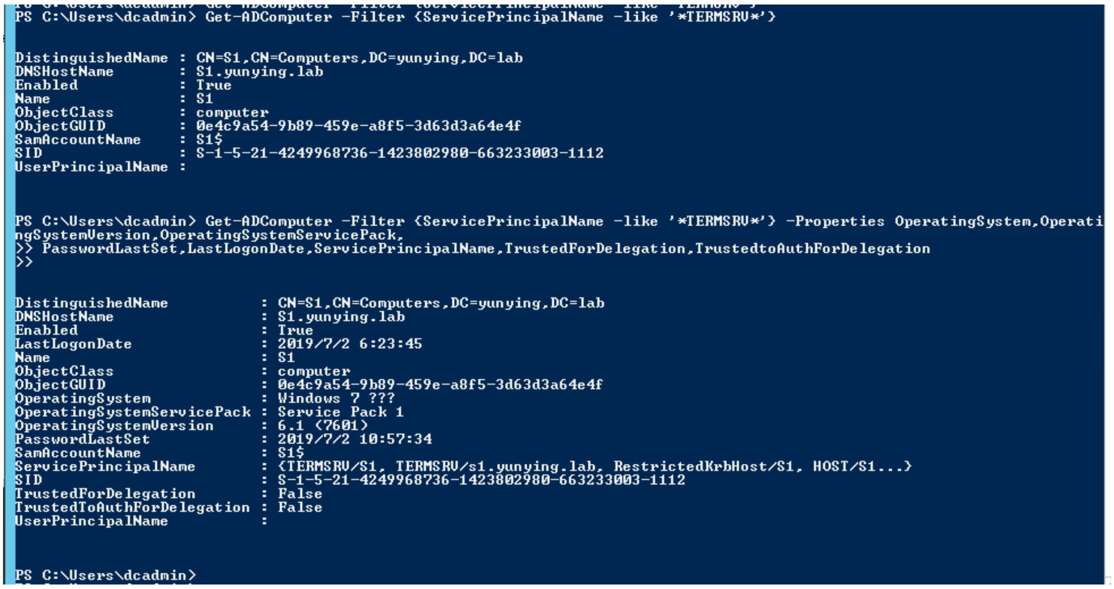


```
PS C:\Users\ts1\Desktop> get-adcomputer
The term 'get-adcomputer' is not recognized as the name of a cmdlet, function, script file, or operable program. Check
the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:15
+ get-adcomputer <<<<
    + CategoryInfo          : ObjectNotFound: (get-adcomputer:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\ts1\Desktop> _
```

通过主机的 SPN 查找

get-adcomputer -filter {ServicePrincipalName -like ‘*TERMSRV*’}

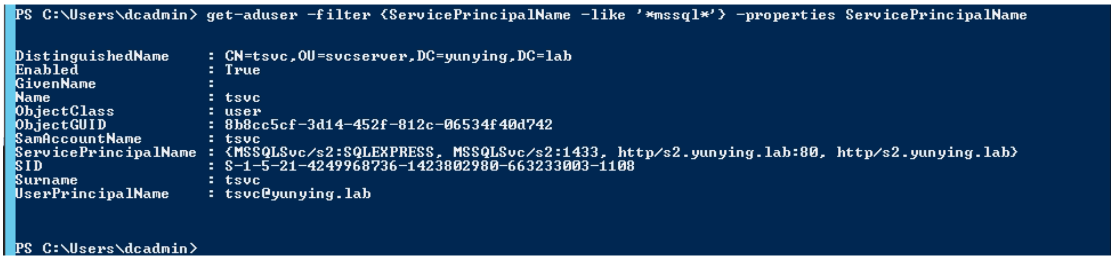
这里必须用单引号，不然会提示语法错误，-Filter 加过滤信息，-Properties 加想看的其他值



```
PS C:\Users\dcadmin> Get-ADComputer -Filter {ServicePrincipalName -like '*TERMSRV*'}


DistinguishedName : CN=S1,CN=Computers,DC=yunying,DC=lab
DNSHostName       : S1.yunying.lab
Enabled           : True
Name              : S1
ObjectClass       : computer
ObjectGUID        : 0e4c9a54-9b89-459e-a8f5-3d63d3a64e4f
SamAccountName    : S1$
SID               : S-1-5-21-4249968736-1423802980-663233003-1112
UserPrincipalName :



PS C:\Users\dcadmin> Get-ADComputer -Filter {ServicePrincipalName -like '*TERMSRV*'} -Properties OperatingSystem,Operati
ngSystemVersion,OperatingSystemServicePack,
>> PasswordLastSet,LastLogonDate,ServicePrincipalName,TrustedForDelegation,TrustedtoAuthForDelegation
>>


DistinguishedName          : CN=S1,CN=Computers,DC=yunying,DC=lab
DNSHostName                : S1.yunying.lab
Enabled                    : True
LastLogonDate              : 2019/7/2 6:23:45
Name                       : S1
ObjectClass                : computer
ObjectGUID                 : 0e4c9a54-9b89-459e-a8f5-3d63d3a64e4f
OperatingSystem            : Windows 7 ???
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion     : 6.1 (7601)
PasswordLastSet            : 2019/7/2 10:57:34
SamAccountName             : S1$
ServicePrincipalName       : {TERMSRV/S1, TERMSRV/s1.yunying.lab, RestrictedKrbHost/S1, HOST/S1...}
SID                        : S-1-5-21-4249968736-1423802980-663233003-1112
TrustedForDelegation       : False
TrustedToAuthForDelegation : False
UserPrincipalName          :


PS C:\Users\dcadmin>
```

查找用户的 SPN 包含 mssql 服务的

get-aduser -filter {ServicePrincipalName -like '*mssql*'} -properties ServicePrincipalName

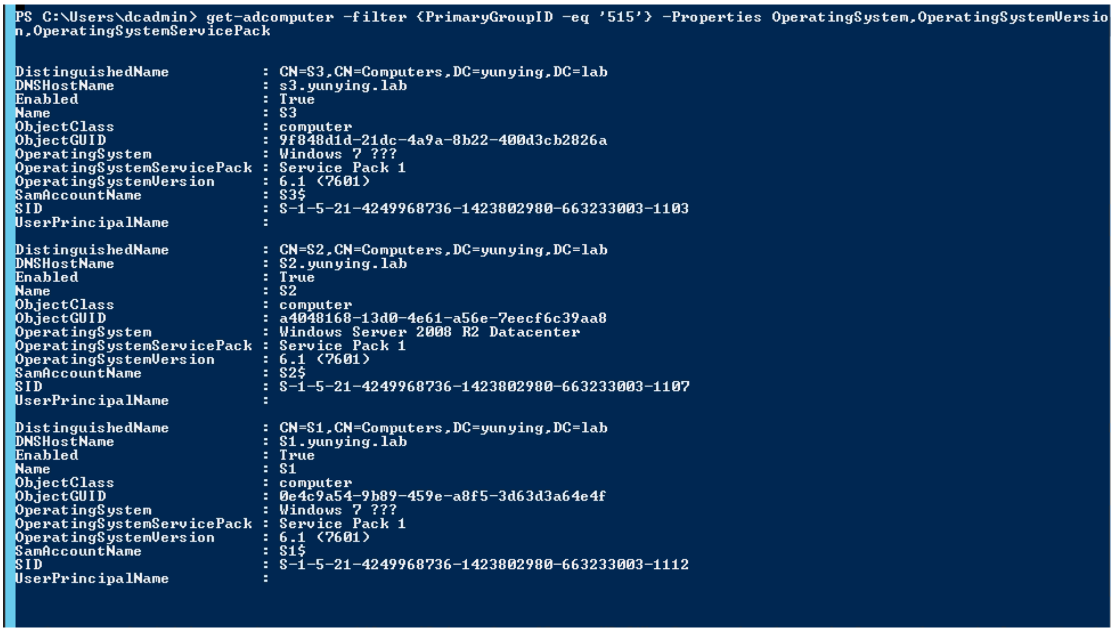


```
PS C:\Users\dcadmin> get-aduser -filter {ServicePrincipalName -like '*mssql*'} -properties ServicePrincipalName

DistinguishedName     : CN=tsvc,OU=svcserver,DC=yunying,DC=lab
Enabled               : True
GivenName             :
Name                  : tsvc
ObjectClass           : user
ObjectGUID            : 8b8cc5cf-3d14-452f-812c-06534f40d742
SamAccountName        : tsvc
ServicePrincipalName : {MSSQLSvc/s2:SQLEXPRESS, MSSQLSvc/s2:1433, http/s2.yunying.lab:80, http/s2.yunying.lab}
SID                   : S-1-5-21-4249968736-1423802980-663233003-1108
Surname               : tsvc
UserPrincipalName     : tsvc@yunying.lab


PS C:\Users\dcadmin>
```

域控和域内主机发现

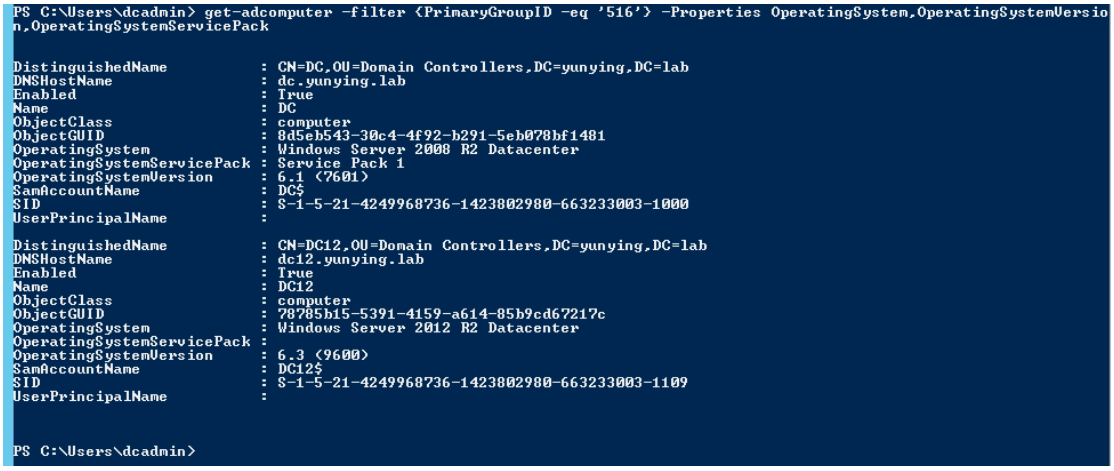
不通过网络扫描发现域控和域内主机

get-adcomputer -filter {PrimaryGroupID -eq ‘515’} -Properties OperatingSystem,OperatingSystemVersion,OperatingSystemServicePack,Passwot,LastLogonDate, ServicePrincipalName,TrustedForDelegation,TrustedtoAuthForDelegation



```
PS C:\Users\dcadmin> get-adcomputer -filter {PrimaryGroupID -eq '515'} -Properties OperatingSystem,OperatingSystemVersio
n,OperatingSystemServicePack


DistinguishedName          : CN=S3,CN=Computers,DC=yunying,DC=lab
DNSHostName                : s3.yunying.lab
Enabled                    : True
Name                       : S3
ObjectClass                : computer
ObjectGUID                 : 9f848d1d-21dc-4a9a-8b22-400d3cb2826a
OperatingSystem            : Windows 7 ???
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion     : 6.1 (7601)
SamAccountName             : S3$
SID                        : S-1-5-21-4249968736-1423802980-663233003-1103
UserPrincipalName          :

DistinguishedName          : CN=S2,CN=Computers,DC=yunying,DC=lab
DNSHostName                : S2.yunying.lab
Enabled                    : True
Name                       : S2
ObjectClass                : computer
ObjectGUID                 : a4048168-13d0-4e61-a56e-7eecf6c39aa8
OperatingSystem            : Windows Server 2008 R2 Datacenter
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion     : 6.1 (7601)
SamAccountName             : S2$
SID                        : S-1-5-21-4249968736-1423802980-663233003-1107
UserPrincipalName          :

DistinguishedName          : CN=S1,CN=Computers,DC=yunying,DC=lab
DNSHostName                : S1.yunying.lab
Enabled                    : True
Name                       : S1
ObjectClass                : computer
ObjectGUID                 : 0e4c9a54-9b89-459e-a8f5-3d63d3a64e4f
OperatingSystem            : Windows 7 ???
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion     : 6.1 (7601)
SamAccountName             : S1$
SID                        : S-1-5-21-4249968736-1423802980-663233003-1112
UserPrincipalName          :
```

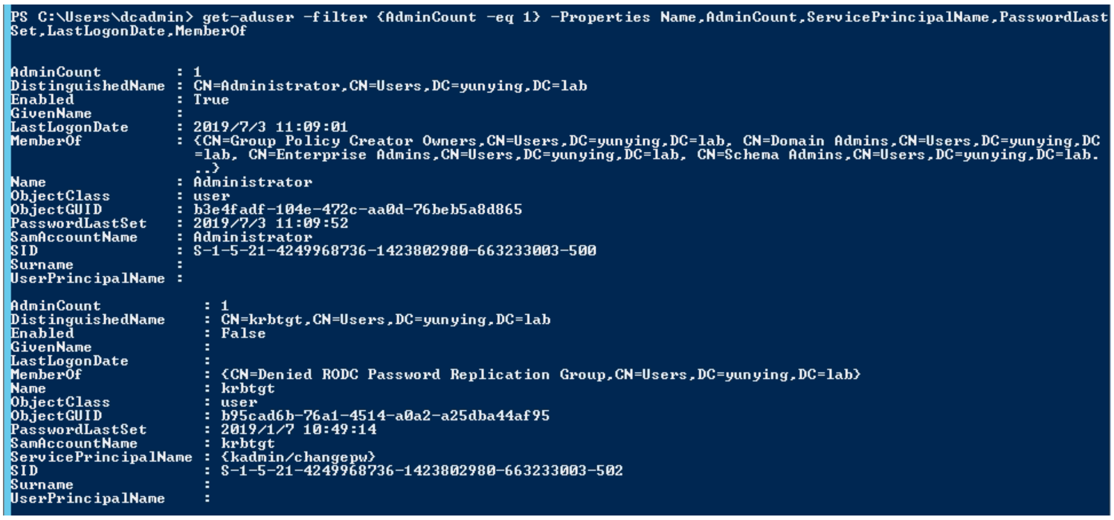
PrimaryGroupID515 为域内主机，516 为域控



```
PS C:\Users\dcadmin> get-adcomputer -filter {PrimaryGroupID -eq '516'} -Properties OperatingSystem,OperatingSystemVersio
n,OperatingSystemServicePack


DistinguishedName          : CN=DC,OU=Domain Controllers,DC=yunying,DC=lab
DNSHostName                : dc.yunying.lab
Enabled                    : True
Name                       : DC
ObjectClass                : computer
ObjectGUID                 : 8d5eb543-30c4-4f92-b291-5eb078bf1481
OperatingSystem            : Windows Server 2008 R2 Datacenter
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion     : 6.1 (7601)
SamAccountName             : DC$
SID                        : S-1-5-21-4249968736-1423802980-663233003-1000
UserPrincipalName          :

DistinguishedName          : CN=DC12,OU=Domain Controllers,DC=yunying,DC=lab
DNSHostName                : dc12.yunying.lab
Enabled                    : True
Name                       : DC12
ObjectClass                : computer
ObjectGUID                 : 78785b15-5391-4159-a614-85b9cd67217c
OperatingSystem            : Windows Server 2012 R2 Datacenter
OperatingSystemServicePack :
OperatingSystemVersion     : 6.3 (9600)
SamAccountName             : DC12$
SID                        : S-1-5-21-4249968736-1423802980-663233003-1109
UserPrincipalName          :


PS C:\Users\dcadmin>
```

识别域内管理员（组）

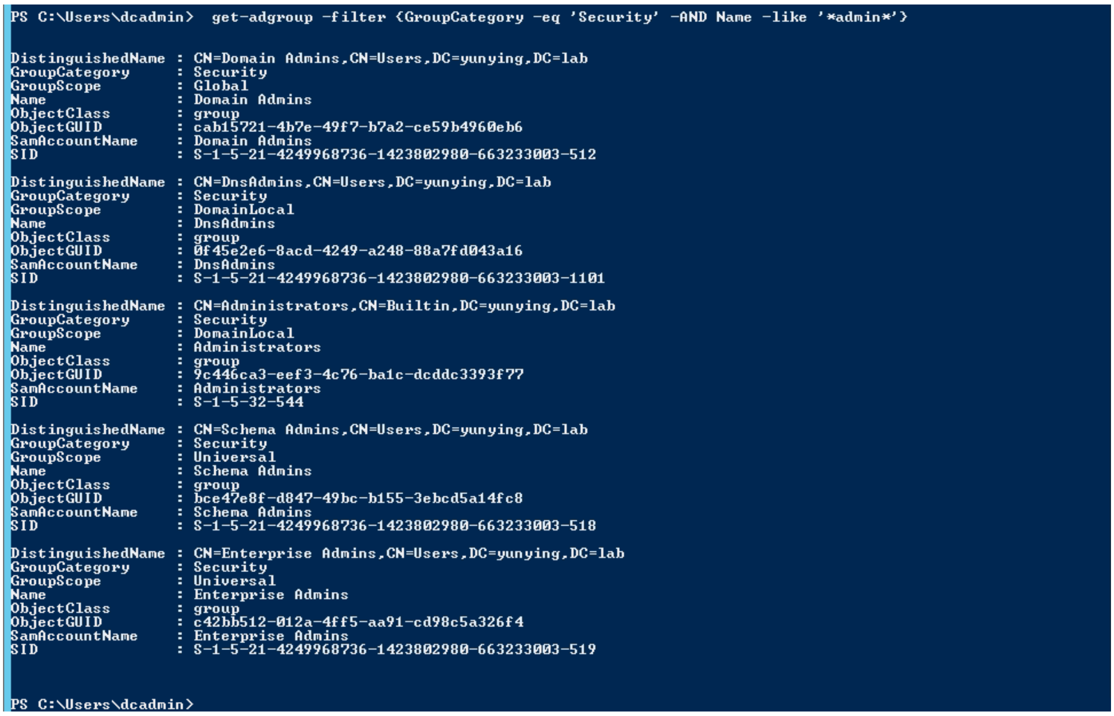
识别管理员账户



```
PS C:\Users\dcadmin> get-aduser -filter {AdminCount -eq 1} -Properties Name,AdminCount,ServicePrincipalName,PasswordLast
Set,LastLogonDate,MemberOf


AdminCount        : 1
DistinguishedName : CN=Administrator,CN=Users,DC=yunying,DC=lab
Enabled           : True
GivenName         :
LastLogonDate     : 2019/7/3 11:09:01
MemberOf          : {CN=Group Policy Creator Owners,CN=Users,DC=yunying,DC=lab, CN=Domain Admins,CN=Users,DC=yunying,DC
                    =lab, CN=Enterprise Admins,CN=Users,DC=yunying,DC=lab, CN=Schema Admins,CN=Users,DC=yunying,DC=lab.
                    ..}
Name              : Administrator
ObjectClass       : user
ObjectGUID        : b3e4fadf-104e-472c-aa0d-76beb5a8d865
PasswordLastSet   : 2019/7/3 11:09:52
SamAccountName    : Administrator
SID               : S-1-5-21-4249968736-1423802980-663233003-500
Surname           :
UserPrincipalName :

AdminCount           : 1
DistinguishedName    : CN=krbtgt,CN=Users,DC=yunying,DC=lab
Enabled              : False
GivenName            :
LastLogonDate        :
MemberOf             : {CN=Denied RODC Password Replication Group,CN=Users,DC=yunying,DC=lab}
Name                 : krbtgt
ObjectClass          : user
ObjectGUID           : b95cad6b-76a1-4514-a0a2-a25dba44af95
PasswordLastSet      : 2019/1/7 10:49:14
SamAccountName       : krbtgt
ServicePrincipalName : {kadmin/changepw}
SID                  : S-1-5-21-4249968736-1423802980-663233003-502
Surname              :
UserPrincipalName    :
```

查看所有的管理员组

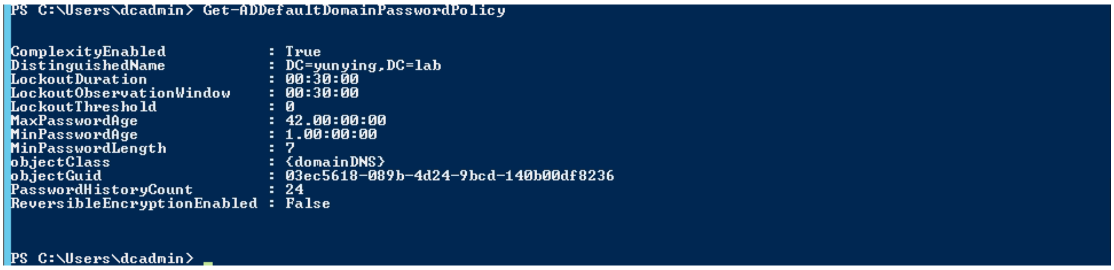
get-adgroup -filter {GroupCategory -eq 'Security' -AND Name -like '*admin*'}



```
PS C:\Users\dcadmin>  get-adgroup -filter {GroupCategory -eq 'Security' -AND Name -like '*admin*'}


DistinguishedName : CN=Domain Admins,CN=Users,DC=yunying,DC=lab
GroupCategory     : Security
GroupScope        : Global
Name              : Domain Admins
ObjectClass       : group
ObjectGUID        : cab15721-4b7e-49f7-b7a2-ce59b4960eb6
SamAccountName    : Domain Admins
SID               : S-1-5-21-4249968736-1423802980-663233003-512

DistinguishedName : CN=DnsAdmins,CN=Users,DC=yunying,DC=lab
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : DnsAdmins
ObjectClass       : group
ObjectGUID        : 0f45e2e6-8acd-4249-a248-88a7fd043a16
SamAccountName    : DnsAdmins
SID               : S-1-5-21-4249968736-1423802980-663233003-1101

DistinguishedName : CN=Administrators,CN=Builtin,DC=yunying,DC=lab
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Administrators
ObjectClass       : group
ObjectGUID        : 9c446ca3-eef3-4c76-ba1c-dcddc3393f77
SamAccountName    : Administrators
SID               : S-1-5-32-544

DistinguishedName : CN=Schema Admins,CN=Users,DC=yunying,DC=lab
GroupCategory     : Security
GroupScope        : Universal
Name              : Schema Admins
ObjectClass       : group
ObjectGUID        : bce47e8f-d847-49bc-b155-3ebcd5a14fc8
SamAccountName    : Schema Admins
SID               : S-1-5-21-4249968736-1423802980-663233003-518

DistinguishedName : CN=Enterprise Admins,CN=Users,DC=yunying,DC=lab
GroupCategory     : Security
GroupScope        : Universal
Name              : Enterprise Admins
ObjectClass       : group
ObjectGUID        : c42bb512-012a-4ff5-aa91-cd98c5a326f4
SamAccountName    : Enterprise Admins
SID               : S-1-5-21-4249968736-1423802980-663233003-519



PS C:\Users\dcadmin>
```

确定域密码策略

Get-ADDefaultDomainPasswordPolicy



```
PS C:\Users\dcadmin> Get-ADDefaultDomainPasswordPolicy


ComplexityEnabled           : True
DistinguishedName           : DC=yunying,DC=lab
LockoutDuration             : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold            : 0
MaxPasswordAge              : 42.00:00:00
MinPasswordAge              : 1.00:00:00
MinPasswordLength           : 7
objectClass                 : {domainDNS}
objectGuid                  : 03ec5618-089b-4d24-9bcd-140b00df8236
PasswordHistoryCount        : 24
ReversibleEncryptionEnabled : False



PS C:\Users\dcadmin>
```

识别细粒度密码策略

Get-ADFineGrainedPasswordPolicy -Filter *

实验环境未配置，所以无图片