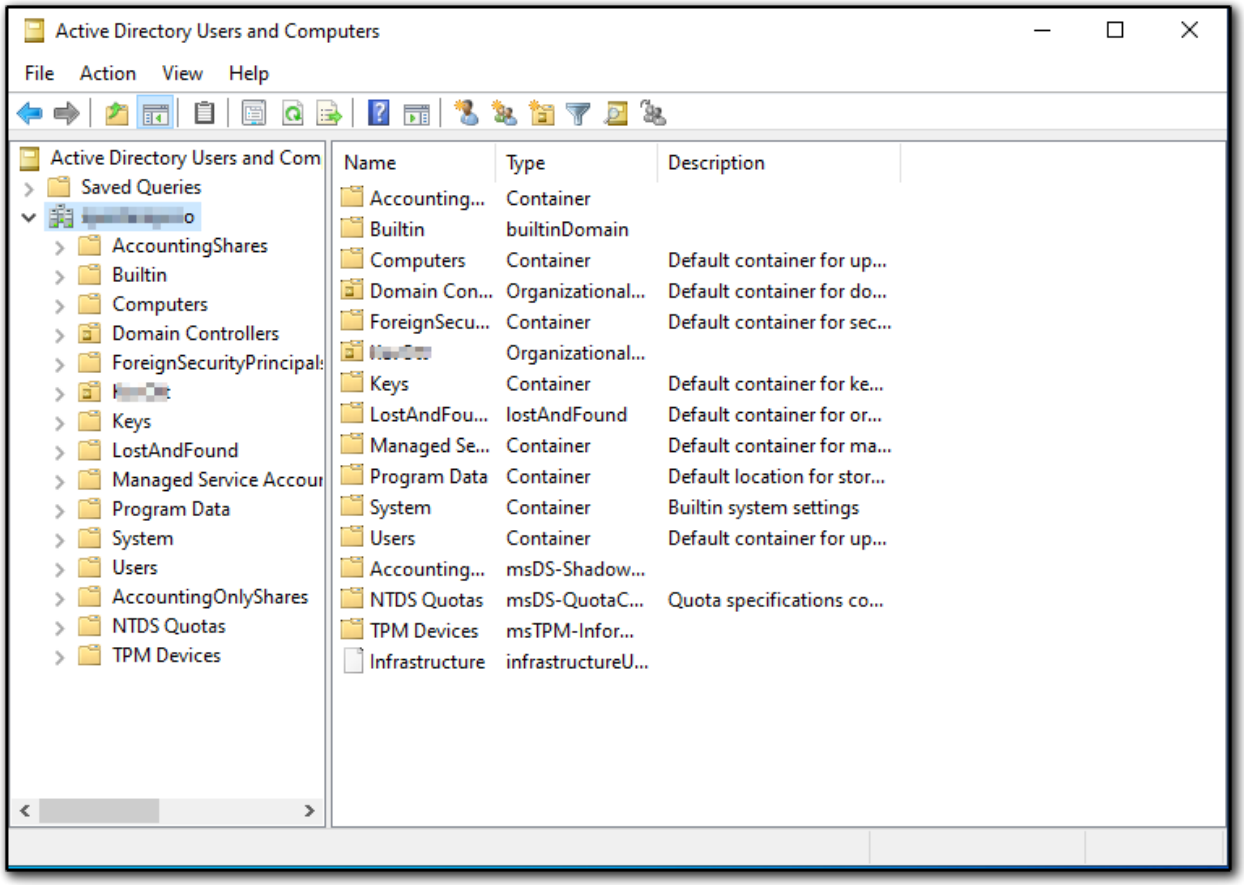
LDAP Queries for Offensive and Defensive Operations

politoinc.com/post/ldap-queries-for-offensive-and-defensive-operations

Erica Zelickowski July 5, 2023



In the age of BloodHound, many consultants have become accustomed to let this very powerful tool do much of the heavy lifting in domain enumeration. BloodHound integrates a strong visual perspective, security descriptors, inbound and outbound object controls, exploit information, OPSEC considerations, and so much more. It's as much a defensive tool as it is an offensive tool. However, some engagements may prefer consultants to take a “low and slow” approach to see what useful information can be acquired about the directory and its objects without BloodHound.

None of the queries outlined here are new or late breaking information. With the exception of a few, they’ve been acquired from multiple resources around the web as referenced below. In fact, the first LDAP RFCs date back to at least 1997 for LDAP version 3. There are numerous blogs, RFCs, and technical specifications; all explaining how to gather information from AD DS with LDAP queries.

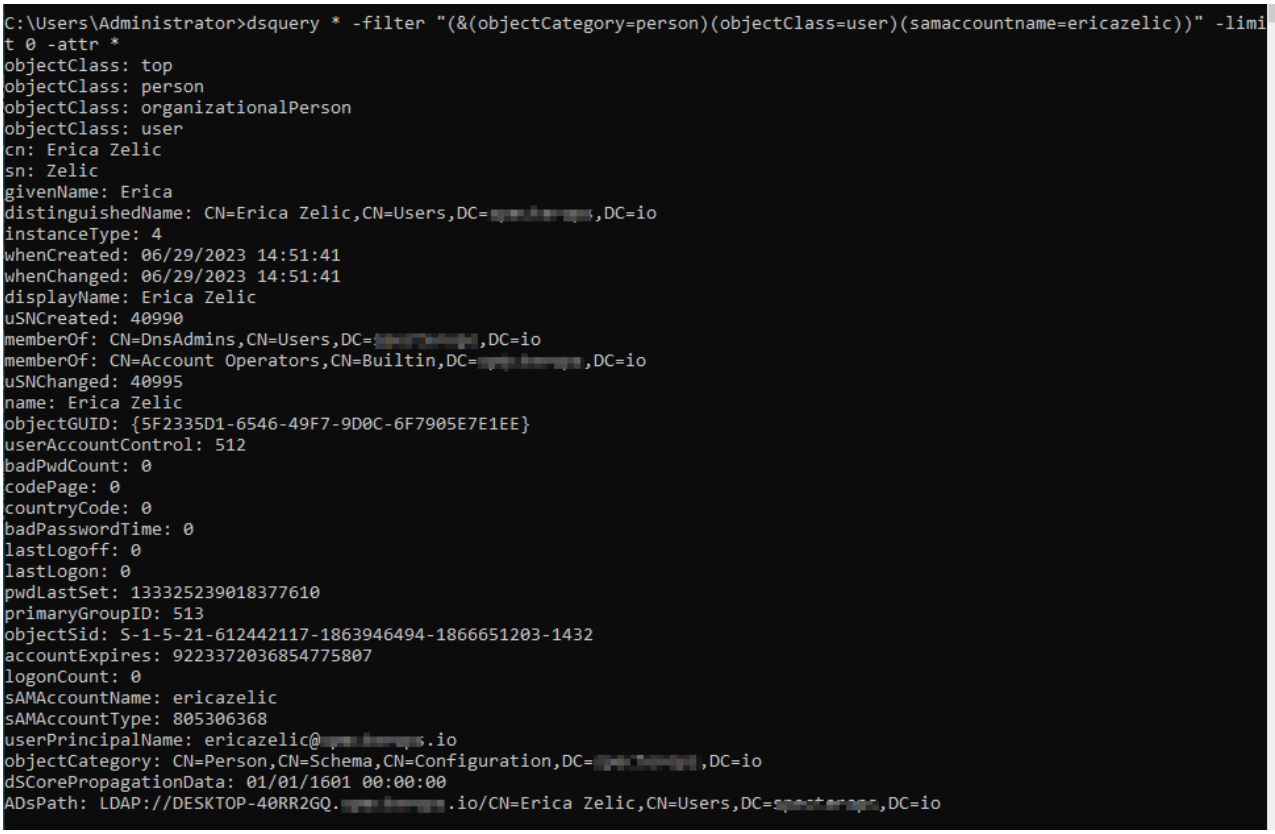
The intention of this post is to provide basic queries for targeted AD DS information gathering used in penetration testing. The reader can pick their poison when deciding how to deliver them. Some delivery method examples include vbscript, powershell (i.e. adsi and adsisearcher type accelerators), dsquery, ADExplorer, AdsiEdit, javascript, win32API, .NET languages, ldapsearch, adfind, adsearch, and likely many others.

Equally, defenders can use these queries to test their detection capabilities when large traffic spikes may not be produced, see what attackers will see from various perspectives within their environment, and aid to remediate domain privilege escalation and lateral movement opportunities from breach hosts.

1. Find directory information about my current user.

For example: let's assume my user's samaccountname is ericazelic

```
dsquery * -filter "(&(objectCategory=person)(objectClass=user)
(samaccountname=ericazelic))" -limit 0 -attr *
```



2. Find all Domain Controllers (DC):

Some tests may require two domain controllers (i.e. zerologon, NTLM downgrade relay over LDAP with authentication on second DC). Other places this information may be available is the DNS Client Cache, or klist. However, having a list of all of them may be useful.

```
(&(objectCategory=Computer)(userAccountControl:1.2.840.113556.1.4.803:=8192))
```

3. Look for places (servers) to move laterally.

Traditional penetration tests often rely on Nessus and/or nmap scans. With LDAP enumeration, you can find all servers in the directory that are not DCs to look for information gathering, and lateral movement opportunities:

```
(&(objectCategory=computer)(operatingSystem=*server*)(!
(userAccountControl:1.2.840.113556.1.4.803:=8192)))
```

```
C:\Users\Administrator>dsquery * -filter "(&(objectCategory=computer)(operatingSystem=*server*)(!(userAccountControl:1.2
.840.113556.1.4.803:=8192)))" -limit 0 -attr samaccountname
  samaccountname
  APPSRV01$
  APPSRV02$
  APPSRV03$
  APPSRV04$
  APPSRV05$
  SQLSRV01$
  SQLSRV02$
  SQLSRV03$
  SQLSRV04$
  SQLSRV05$
  VNCSRV01$
  VNCSRV02$
  VNCSRV03$
  VNCSRV04$
  VNCSRV05$
  WEBSRV01$
  WEBSRV02$
  WEBSRV03$
  WEBSRV04$
  WEBSRV05$
  BCKUPSRV01$
  BCKUPSRV02$
  BCKUPSRV03$
  BCKUPSRV04$
  BCKUPSRV05$
```

4. Find certificate authorities and publishers:

```
(CN="Cert Publishers"*)
```

5. Find all organizational units (OU):

Different OUs may have different group policies, targeted configurations, and administrators:

```
(objectCategory=organizationalUnit)
```

VBScript example:

```
On Error Resume Next

Const ADS_SCOPE_SUBTREE = 2

Set objConnection = CreateObject("ADODB.Connection")
Set objCommand = CreateObject("ADODB.Command")
objConnection.Provider = "ADsDSOObject"
objConnection.Open "Active Directory Provider"
Set objCommand.ActiveConnection = objConnection

objCommand.Properties("Page Size") = 1000
objCommand.Properties("Searchscope") = 2
objCmd.Properties("Timeout") = 30
objCmd.Properties("Cache Results") = False

objCommand.CommandText = _
"SELECT Name FROM 'LDAP://DC=ad,DC=yummy,DC=tacos' WHERE
objectCategory='organizationalUnit'"
Set objRecordSet = objCommand.Execute

objRecordSet.MoveFirst
Do Until objRecordSet.EOF
Wscript.Echo objRecordSet.Fields("Name").Value
objRecordSet.MoveNext
Loop
```

6. Find all Containers:

Look for non-default AD containers. Sometimes organizations will have containers for shares, authentication, and other uses.

```
(objectCategory=container)
```

```
C:\Users\Administrator\Desktop>dsquery * -filter "(&(objectcategory=container)(cn=AccountingShares))" -limit 0 -attr nam
e
  name
  AccountingShares

C:\Users\Administrator\Desktop>
```

7. Find accounts with a serviceprincipalname (SPN):

Finding accounts with SPNs helps us identify kerberoastable accounts as well as helps us understand what services are running where in the environment. In some cases, if we have the ability to write to an object in the directory, we could add a serviceprincipalname to the object to make it kerberoastable. This query could also be used to help us confirm the serviceprincipalname was added:

DSQuery:

```
* -filter "(&(objectClass=User)(serviceprincipalname=*)(samaccountname=*))" -limit
0 -attr samaccountname serviceprincipalname
```

```
C:\Users\Administrator\Downloads\Powermad-master\Powermad-master>dsquery * -filter "(&(objectClass=User)(serviceprincipalname
=*)(samaccountname=*))" -limit 0 -attr samaccountname serviceprincipalname
  samaccountname      serviceprincipalname
  DESKTOP-40RR2GQ$    Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/DESKTOP-40RR2GQ.[redacted].io;ldap/DESKTOP-40RR2GQ.[redacted]
.io/ForestDnsZones.[redacted].io;ldap/DESKTOP-40RR2GQ.[redacted].io/DomainDnsZones.[redacted].io;DNS/DESKTOP-40RR2GQ.[redacted]
[redacted].io;GC/DESKTOP-40RR2GQ.[redacted].io/[redacted].io;RestrictedKrbHost/DESKTOP-40RR2GQ.[redacted].io;RestrictedKrbHost/DESKTO
P-40RR2GQ;RPC/daa8bc4f-b3eb-4829-9b15-7c457c3f3315._msdcs.[redacted].io;HOST/DESKTOP-40RR2GQ/[redacted];HOST/DESKTOP-40RR2GQ.
[redacted].io/[redacted];HOST/DESKTOP-40RR2GQ;HOST/DESKTOP-40RR2GQ.[redacted].io;HOST/DESKTOP-40RR2GQ.[redacted].io/[redacted]
[redacted].io;E3514235-4B06-11D1-AB04-00C04FC2DCD2/daa8bc4f-b3eb-4829-9b15-7c457c3f3315/[redacted].io;ldap/DESKTOP-40RR2GQ/[redacted];
ldap/daa8bc4f-b3eb-4829-9b15-7c457c3f3315._msdcs.[redacted].io;ldap/DESKTOP-40RR2GQ.[redacted].io/[redacted];ldap/DESKTOP-40R
R2GQ;ldap/DESKTOP-40RR2GQ.[redacted].io;ldap/DESKTOP-40RR2GQ.[redacted].io/[redacted].io;
  exchange_svc$       exchange_svc/exserver.[redacted].io

  MyRBCD$             RestrictedKrbHost/MyRBCD;HOST/MyRBCD;RestrictedKrbHost/MyRBCD.[redacted].io;HOST/MyRBCD.[redacted] io;

  IISAdmin            http/iLikeSilverTicketsToo

  http_svc$           http_svc/httpserver.[redacted].io

  krbtgt              kadmin/changepw
  mssql_svc           mssql/kerberoasting_is_fun

  mssql_svc$          mssql_svc/mssqlserver.[redacted].io
```

Powershell:

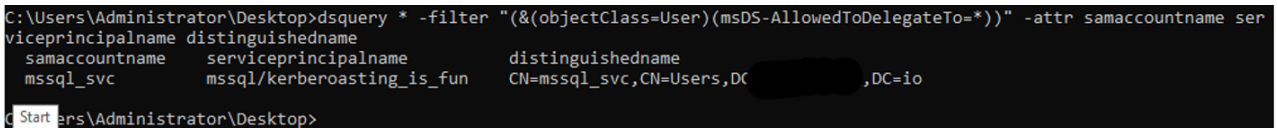
```
([adsisearcher]'(servicePrincipalName=*)').FindAll()
```

```
PS C:\Users\Administrator\Desktop> ([adsisearcher]'(servicePrincipalName=*)').FindAll()

Path                                                                Properties
----                                                                ----------
LDAP://CN=DESKTOP-[redacted],OU=Domain Controllers,DC=[redacted],DC=io    {ridsetreferences, logoncount, codepage, objectcat...
LDAP://CN=exchange_svc,CN=Managed Service Accounts,DC=[redacted],DC=io    {logoncount, codepage, objectcategory, iscriticals...
LDAP://CN=http_svc,CN=Managed Service Accounts,DC=[redacted],DC=io        {logoncount, codepage, objectcategory, iscriticals...
LDAP://CN=krbtgt,CN=Users,DC=[redacted],DC=io                             {logoncount, codepage, objectcategory, description...
LDAP://CN=mssql_svc,CN=Managed Service Accounts,DC=[redacted],DC=io       {logoncount, codepage, objectcategory, iscriticals...
```

8. Constrained Delegation:

Accounts with constrained delegation allow you to impersonate any domain user account as long as it's not flagged with "Account is sensitive and cannot be delegated" or a member of the Protected Users group:

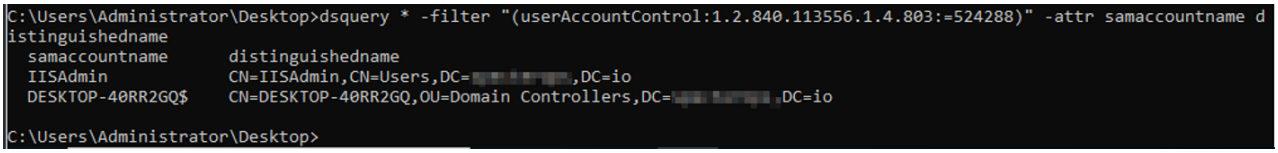
```
(&(objectClass=User)(msDS-AllowedToDelegateTo=*))
```



9. Unconstrained Delegation (will include DCs):

Unless an account is marked "Account is sensitive and cannot be delegated" or a member of Protected Users group, you can coerce authentications and dump the TGT which is stored in memory and can be extracted:

```
(userAccountControl:1.2.840.113556.1.4.803:=524288)
```

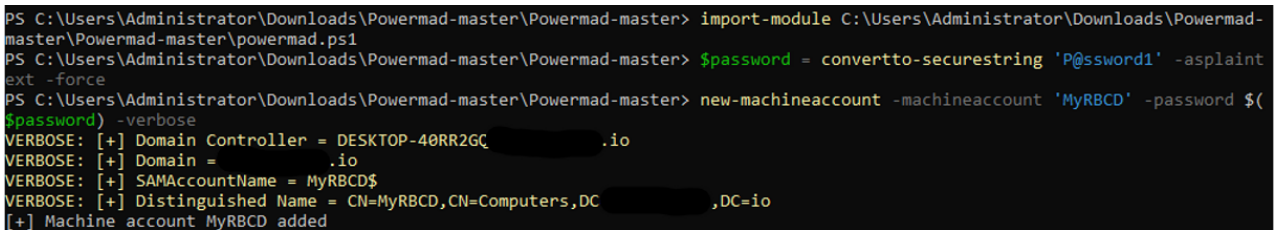


10. Resource Based Constrained Delegation (RBCD):

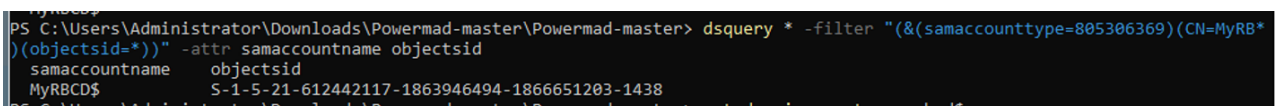
Looking for RBCD helps us to identify targets in potential attack paths as well as allows us to check the object attribute when setting it ourselves. A discussion of RBCD is beyond the scope of this post, however, a great reference is Elad Shamir's Wagging the Dog blog post.

```
(msDS-AllowedToActOnBehalfOfOtherIdentity=*)
```

For example, if machineaccountquota is > 0, we can use powermad to add a machine account:



Using dsquery to check if the machine account was created and list the SID:



Add a raw security descriptor to the msds-allowedtoactonbehalfofotheridentity and check it was successfully added with dsquery:

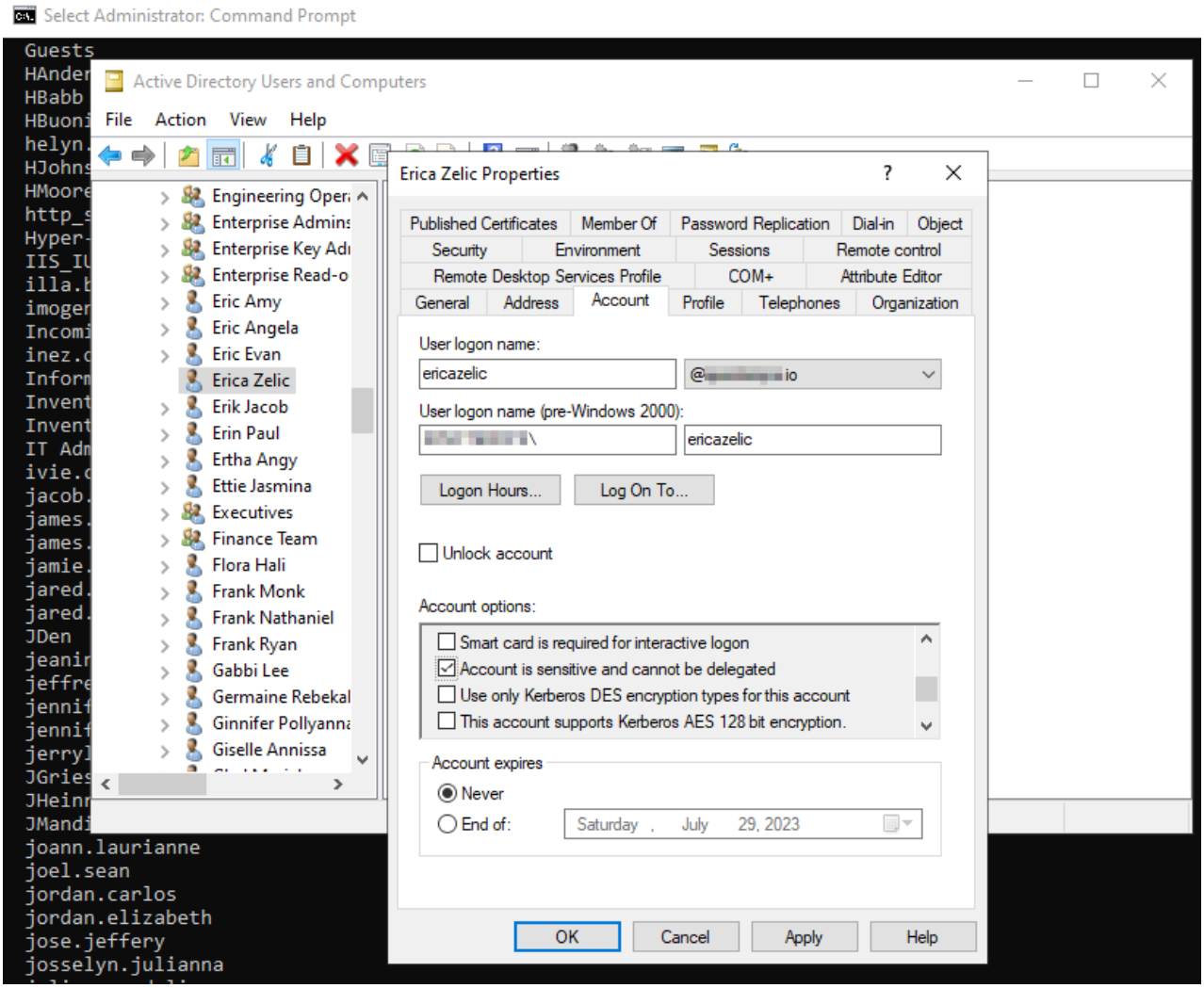
```
PS C:\Users\Administrator\Downloads\Powermad-master\Powermad-master> $SD = New-Object Security.AccessControl.RawSecurityDescr
iptor -ArgumentList "O:BAD:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-21-612442117-1863946494-1866651203-1438)"
>> $SDBytes = New-Object byte[] ($SD.BinaryLength)
>> $SD.GetBinaryForm($SDBytes, 0)
PS C:\Users\Administrator\Downloads\Powermad-master\Powermad-master> Get-DomainComputer myrbcd | Set-DomainObject -Set @{'msd
s-allowedtoactonbehalfofotheridentity'=$SDBytes} -Verbose
VERBOSE: [Get-DomainSearcher] search base: LDAP://DESKTOP-40RR2GQ.[redacted].IO/DC=[redacted],DC=IO
VERBOSE: [Get-DomainObject] Extracted domain '[redacted].io' from 'CN=MyRBCD,CN=Computers,DC=[redacted],DC=io'
VERBOSE: [Get-DomainSearcher] search base: LDAP://DESKTOP-40RR2GQ.[redacted].IO/DC=[redacted],DC=io
VERBOSE: [Get-DomainObject] Get-DomainObject filter string:
(&(|(distinguishedname=CN=MyRBCD,CN=Computers,DC=[redacted],DC=io)))
VERBOSE: [Set-DomainObject] Setting 'msds-allowedtoactonbehalfofotheridentity' to '1 0 4 128 20 0 0 0 0 0 0 0 0 0 0 0 36 0 0
 0 1 2 0 0 0 0 0 5 32 0 0 0 32 2 0 0 2 0 44 0 1 0 0 0 0 0 36 0 255 1 15 0 1 5 0 0 0 0 0 5 21 0 0 0 5 32 129 36 254 144 25
111 67 214 66 111 158 5 0 0' for object 'MyRBCD$'
PS C:\Users\Administrator\Downloads\Powermad-master\Powermad-master> cmd
Microsoft Windows [Version 10.0.20348.1787]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads\Powermad-master\Powermad-master>dsquery * -filter "(&(msDS-AllowedToActOnBehalfOfOtherIdenti
ty=*)(samaccountname=*))" -attr samaccountname msds-allowedtoactonbehalfofotheridentity
  samaccountname    msds-allowedtoactonbehalfofotheridentity
  MyRBCD$           O:BAD:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-21-612442117-1863946494-1866651203-1438)

C:\Users\Administrator\Downloads\Powermad-master\Powermad-master>
```

Now we can use the NT hash as the RC4 key to get a Kerberos ticket and impersonate other domain users to complete the attack.

11. Accounts Not Trusted for Delegation:

If this attribute is set, accounts cannot be used in delegations discussed above.

```
(&(samaccountname=*)(userAccountControl:1.2.840.113556.1.4.803:=1048576))
```



```
C:\Users\Administrator\Desktop>dsquery * -filter "(&(samaccountname=*)(userAccountControl:1.2.840.113556.1.4.803:=104857
6))" -limit 0 -attr samaccountname
  samaccountname
  ericazelic

C:\Users\Administrator\Desktop>_
```

12. Shadow Credentials:

In domains using Active Directory Certificate Service (AD CS) and a domain controller (DC) with PKINIT enabled that's 2016 or later, we may be able to modify this attribute to take over user and computer accounts. Once we have generated a certificate and written to the attribute, we can confirm the modification with this LDAP query. More about Shadow Credentials can be found here.

```
(msDS-KeyCredentialLink=*)
```

13. Kerberos Pre-Authentication Disabled:

Although rare, an account with this attribute means it is AS-REP roastable.

```
(&(objectCategory=person)(objectClass=user)
(userAccountControl:1.2.840.113556.1.4.803:=4194304))
```

```
C:\Users\Administrator\Desktop>dsquery * -filter "(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.1135
56.1.4.803:=4194304))" -attr samaccountname distinguishedname
  samaccountname      distinguishedname
  miof mela.allx      CN=Miof Mela Allx,CN=Users,DC=[redacted]DC=io
  emmalynn.jill       CN=Emmalynn Jill,CN=Users,DC=[redacted]=io
  aurelea.fernanda    CN=Aurelea Fernanda,CN=Users,[redacted],DC=io
  catlaina.enrica     CN=Catlaina Enrica,CN=Users,D[redacted]DC=io
  s.monk              CN=Scarred Monk,CN=Users,DC=[redacted]io
  sharepoint_proxy    CN=sharepoint_proxy,CN=Users[redacted],DC=io

C:\Users\Administrator\Desktop>_
```

14. Kerberoastable Users:

This query will help us find user accounts that are kerberoastable. This means we may be able to crack the password offline and forge a silver ticket, or use the credentials alone to move laterally.

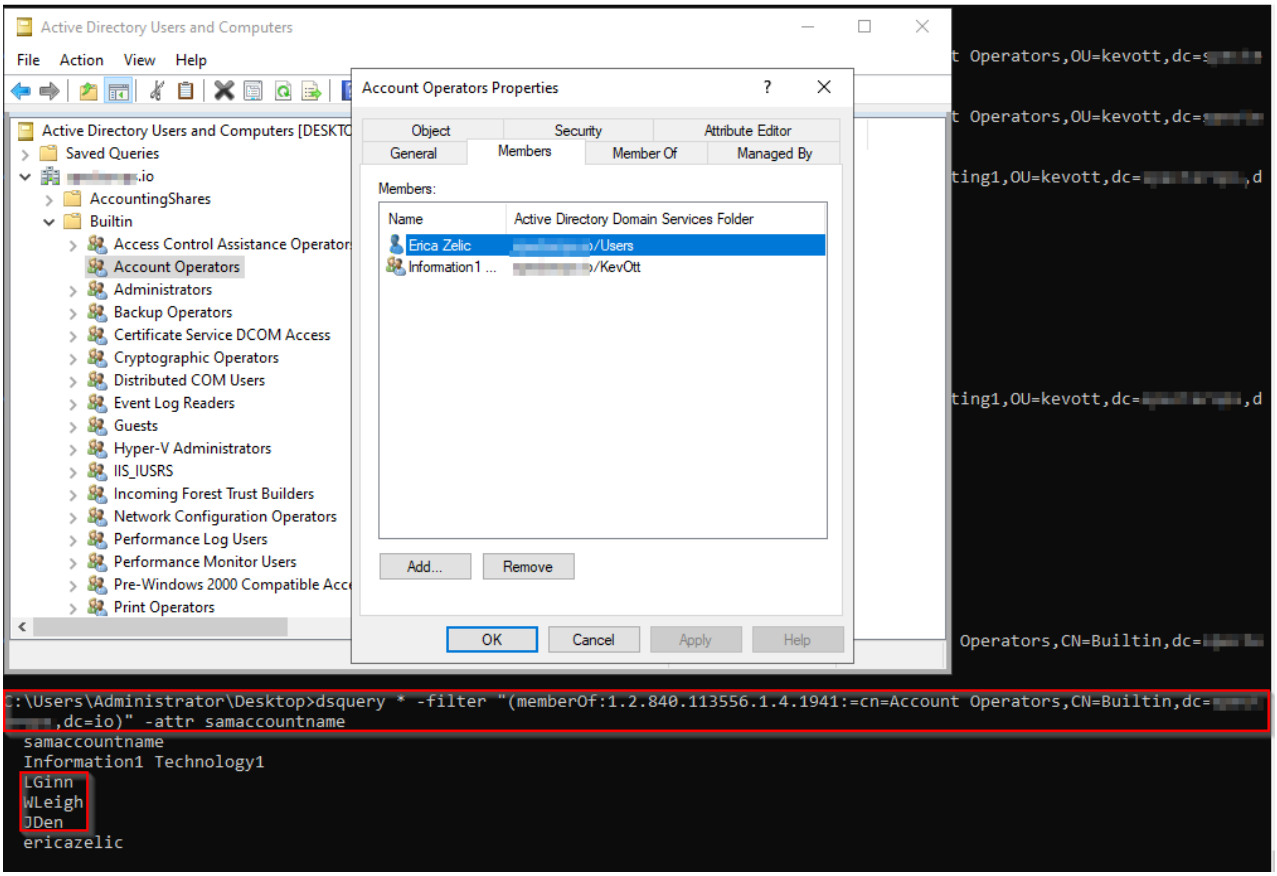
```
(&(objectClass=user)(servicePrincipalName=*)(!(cn=krbtgt))(!
(samaccounttype=805306369)))
```

```
C:\Users\Administrator\Desktop>dsquery * -filter "(&(objectClass=user)(servicePrincipalName=*)(!(cn=krbtgt))(!(samaccounttype
=805306369)))" -attr samaccountname serviceprincipalname
  samaccountname    serviceprincipalname
  IISAdmin          http/iLikeSilverTicketsToo
  mssql_svc         mssql/kerberoasting_is_fun

C:\Users\Administrator\Desktop>
```

15. Members of a group through nesting:

Many directories will have users that are not direct members of a group but have the group's privileges due to nesting.

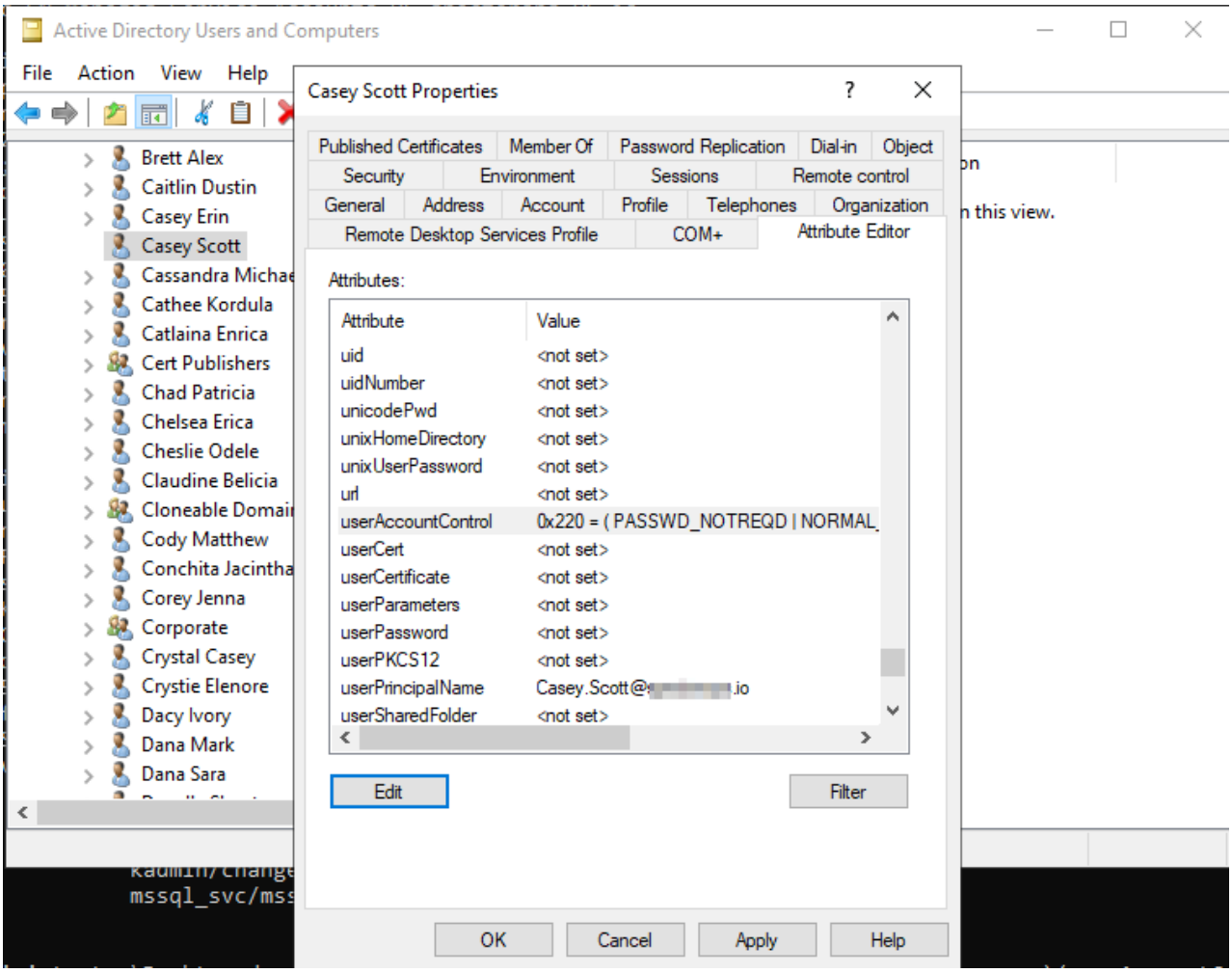
```
(memberOf:1.2.840.113556.1.4.1941:=cn=Test,ou=East,dc=Domain,dc=com)
```



16. Users Not Required to Have a Password:

This helps us find opportunities for lateral movement. [According to Microsoft](), even if a password is required by group policy (GP), this setting will override the GP.

```
(&(objectCategory=person)(objectClass=user)
(userAccountControl:1.2.840.113556.1.4.803:=32))
```

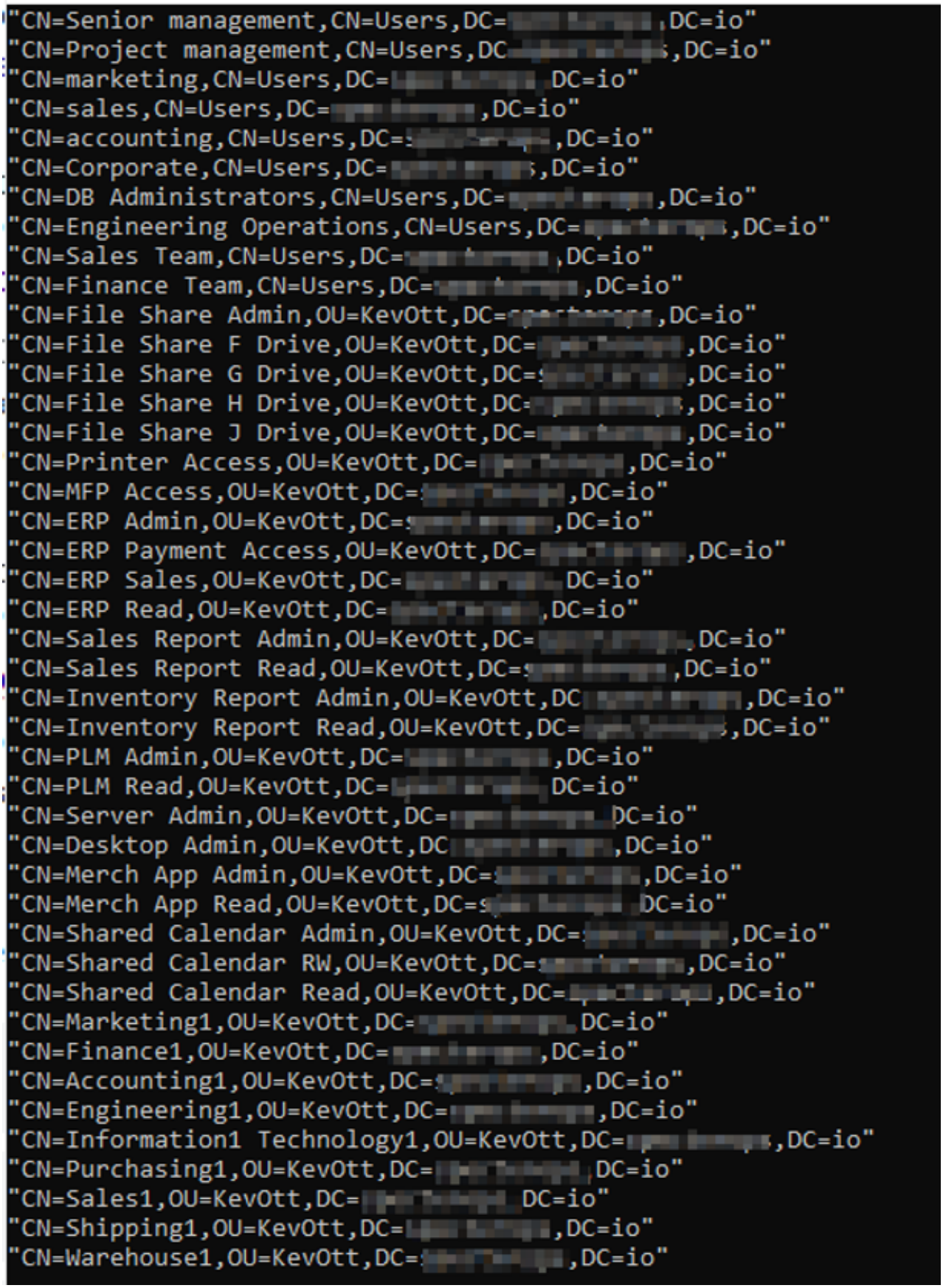



```
C:\Users\Administrator\Desktop>dsquery * -filter "(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=32))" -limit 0 -attr samaccountname
  samaccountname
  Guest
  casey.scott
```

17. Groups:

This enables you to view all the groups in the directory and identify groups that may have administrative permissions as possible targets, additional information about the technology stack, and other useful information about the environment.

```
(objectCategory=group)
```

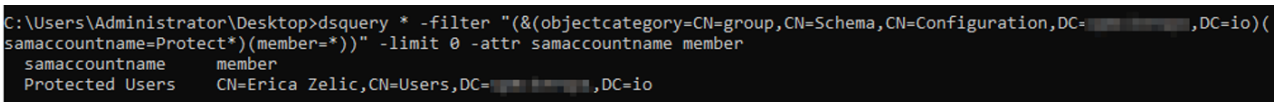


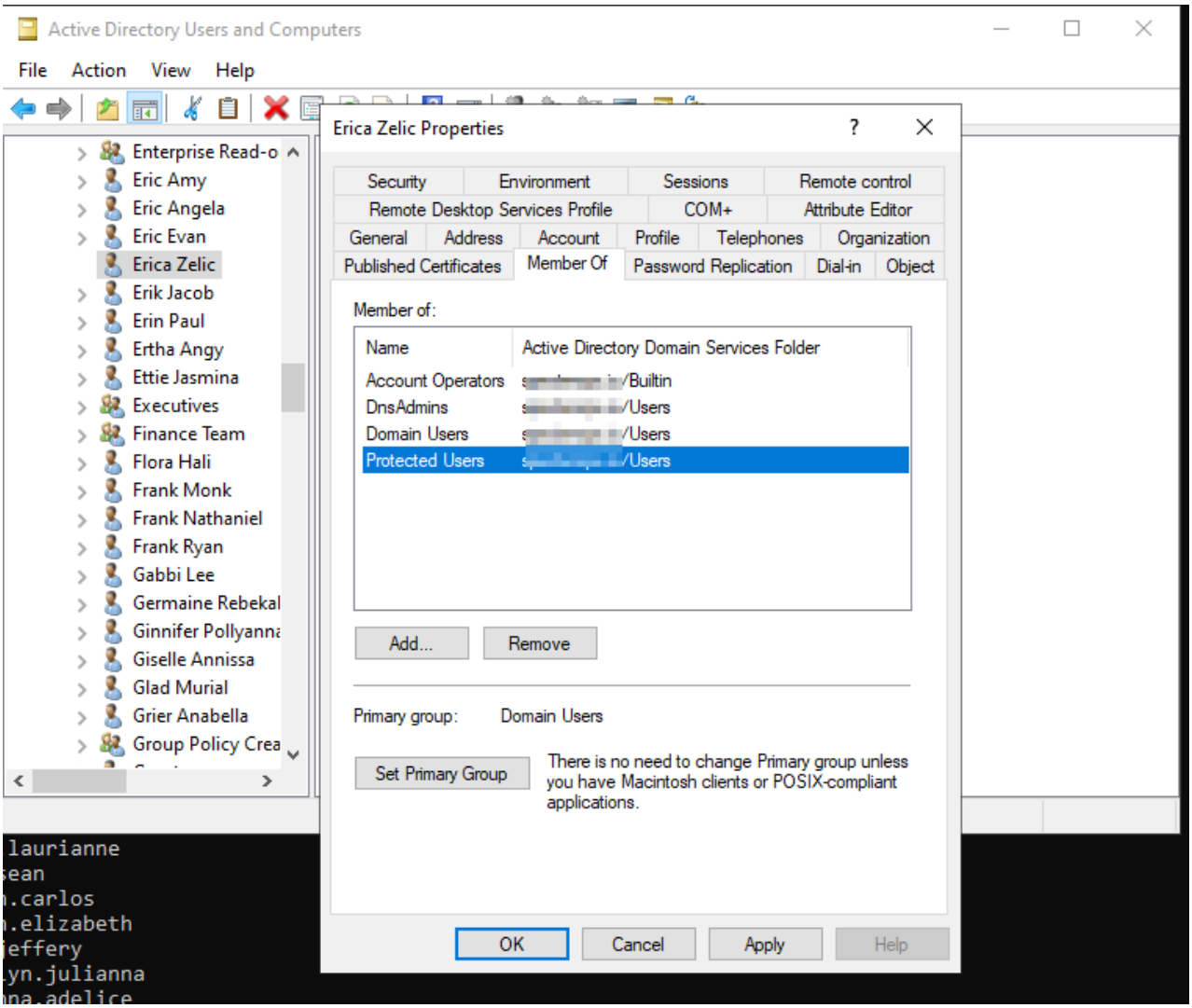
18. Protected Users Group:

Members of this group can only sign on using Kerberos. If an account is in the Protected Users group, delegations and NTLM pass-the-hash attacks will not work. Also, DES or RC4 encryption types in Kerberos pre-authentication will fail, Kerberos TGTs cannot be

renewed beyond their initial 4 hour period, and passwords will not be cached.

```
(&
(objectCategory=CN=group,CN=Schema,CN=configuration,DC=yourDomainName,DC=yourDomain
(samaccountname=Protect*)(member=*))
```





19. User Objects With Description:

The description attributes of user directory objects sometimes contain passwords or additional useful information about users.

```
(&(objectCategory=user)(description=*))
```

20. Computer Objects With Description:

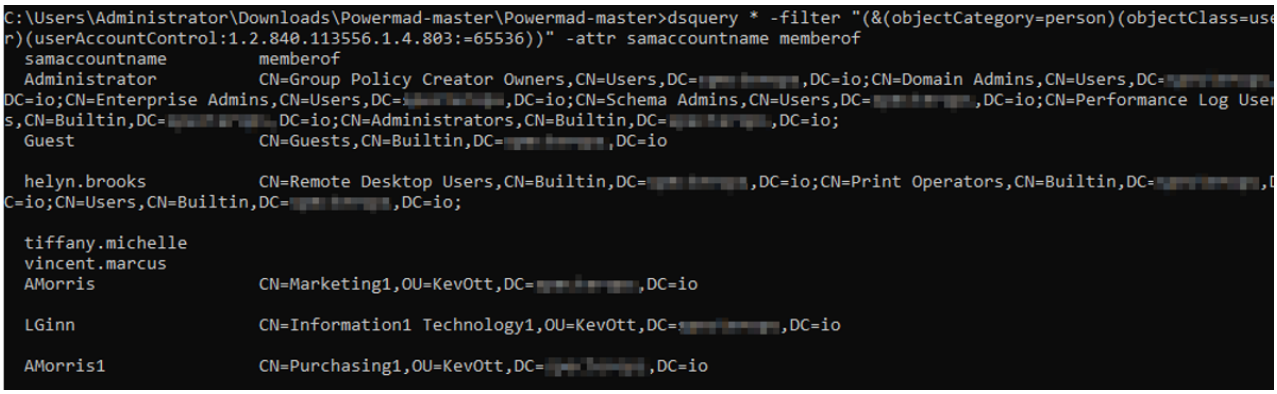
The description attribute of computer objects sometimes reveals additional information about the system and its purpose that may not be derived from the NetBIOS name.

```
(&(objectCategory=computer)(description=*))
```

21. Passwords Don’t Expire:

Accounts with old passwords may be more vulnerable. For example, we could look at breach information and create more precise lists for low and slow brute force attacks (not ideal) ensuring we don't lockout users.

```
(&(objectCategory=person)(objectClass=user)
(userAccountControl:1.2.840.113556.1.4.803:=65536))
```



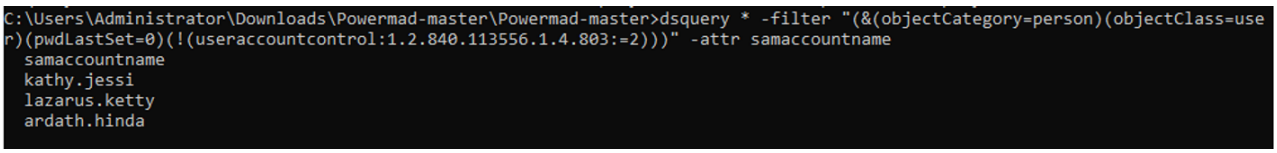
22. User Must Change Password on Next Login:

Some organizations may use a scripted password when doing password changes. Suppose we find that password on a share with Snaffler. We may be able to use tools like smbpasswd or rpcclient to change it from Linux. This is probably a bad idea to do on a penetration test without asking the client first. It's generally a bad idea to change users' passwords unless you have the ability to change them back before they notice and have permission from the client when consulting.

As for the pwdlastset=0 attribute, according to Microsoft, there are 3 occurrences you may see this attribute set to zero:

- Where an account has been created but a password has not been assigned.
- Where an account has been created and the administrator has assigned a password but selected the option to change password at next logon.
- Where the administrator has selected the option to require a user to change their password at the next logon as part of managing that user’s account, such as after a password reset.

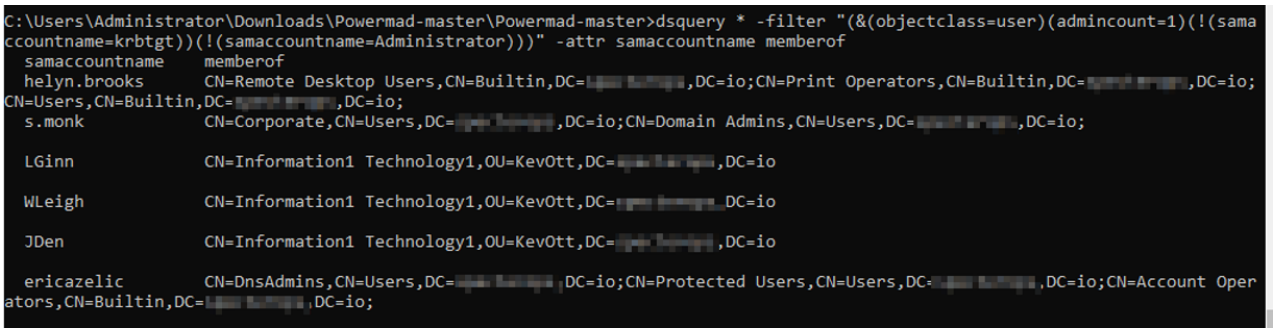
```
(&(objectCategory=person)(objectClass=user)(pwdLastSet=0)(!
(useraccountcontrol:1.2.840.113556.1.4.803:=2)))
```



23. User Objects with Elevated Domain Rights:

Usually, if an object has this attribute set, it is part of a protected group with elevated domain privileges, or once was. Examples of security groups where this attribute is known to enable domain privilege escalation include backup operators, account operators, server operators, print operators, domain admins, enterprise admins, schema admins, dnsadmins, and sometimes read-only domain controllers. If an account is a member of one of these groups, either directly or indirectly, we can gain control of the domain. Knowing which directory objects have this attribute set helps us create a list of targets. It's not unusual to see kerberoastable service accounts with this attribute value although passwords for service accounts have become harder to crack offline in recent years due to stronger passwords on high value service accounts.

```
(&(objectClass=user)(admincount=1)(!(samaccountname=krbtgt))(!
(samaccountname=administrator)))
```



24. User Accounts with SID History:

Accounts with SIDHistory may have access in other domains.

```
(&(objectCategory=Person)(objectClass=User)(sidHistory=*))
```

25. Generate a List of User Accounts samaccountname:

```
(&(objectCategory=Person)(objectClass=User)(samaccountname=*))
```

26. Generate a list of computer object names:

```
(&(objectClass=Computer)(samaccountname=*))
```

Polito Inc. offers a wide range of security consulting services including threat hunting, penetration testing, vulnerability assessments, red teaming engagements, incident response, digital forensics, and more. If your business or your clients have any cyber security needs, contact our experts and experience what Masterful Cyber Security is all about.

Phone: 571-969-7039

E-mail:info@politoinc.com

Website:politoinc.com

CHANGELOG:

Updated #26 from NetBIOS to computer object: 07/06/2023

REFERENCES:

https://qa.social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx

https://ldap.com/ldap-related-rfcs/

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/d2435927-0999-4c62-8c6d-13ba31a52e1a

https://blogs.uw.edu/kool/2016/10/26/kerberos-delegation-in-active-directory/

https://rootdse.org/posts/active-directory-security-2/

https://learn.microsoft.com/en-us/windows/win32/adsi/active-directory-service-interfaces-adsi

https://www.ired.team/

https://book.hacktricks.xyz/welcome/readme

https://www.thehacker.recipes/

https://learn.microsoft.com/en-us/azure/active-directory-domain-services/create-ou

https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group

https://posts.specterops.io/shadow-credentials-abusing-key-trust-account-mapping-for-takeover-8ee1a53566ab

https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html

https://snovvcrash.rocks/2020/10/31/pretending-to-be-smbpasswd-with-impacket.html

https://www.youtube.com/watch?v=IfCysW0Od8w

https://github.com/SnaffCon/Snaffler

https://learn.microsoft.com/en-us/services-hub/health/remediation-steps-ad/review-accounts-whose-attribute-pwdlastset-has-a-zero-value

https://www.youtube.com/watch?v=VxbC03xmS60&t=1080s