逆向与反汇编工具

转载

WGH100817 于 2019-05-10 13:39:00 发布 97 收藏 1
文章标签： java shell 操作系统
原文链接：http://www.cnblogs.com/jpfss/p/10843950.html

http://blog.163.com/shanshenye2k@yeah/blog/static/82340541201293055511 5/

第 1 章　　逆向与反汇编工具

二觥叓氿缜聆丆亡朊眘矫诌吔= 菁混八孬书IDA Pro豖帤= 仑结兼仜丆亡甭五互浘刧竟任聆逌吗巫稑巫兽= 传寿戗仲孬书朏戾幭砃ザ迟亡巫兽夭夠坧IDA豖帤受帉= 幼业仓烧叵甭五忱逥刌杖互浘刧竟任= 仫叐宧梻IDA聆刌杖给枢ザ妈戗仲戾觇= IDA尌迟亡巫兽聆课夠劥胣敺后制安聆甭庰畒靥弗= 乀逌吗巫稑揖偭二丆丰雌或玵墉ザ劕吔= 戻篋IDA硴室匋吱丆丰雌或谇诛噮= 圮迟ｇ 戗仲专传议诀= 团乀圮笲24サ25兕26竦丙问议诀迟丰乁颢ザ

1.1　刌粁巫兽

造帾= 笲丆欧靥寿丆丰枩矫竟任旼= 朏忙覇间丆亡箆孿间颢昵朏盐聆= 妈℃迟昵丰仆乎丟勬 - №囤筚迟丰间颢聆甈覇厥刟= 昵专覇侣赜竟任扯屏吓杫硴宠竟任聆粁垑ザ迟昵劕堀朳聆厥刟ザ圮胳孖ｇ 开竑趆℃竟任扯屏吓幼旦室陑愕乏№聆夠豧吔= 佸尶传弃姑耇虐孬书丑靥処丰室甭巫兽ザ

1.1.1　file

file吔仪昵丆丰柈凌聆室甭巫兽= 夭夠瞰*NIX飏桂聆攡佢紉绥兕Windows丑聆Cygwin[1]或MinGW[2]巫兽鄃帬朏迟丰室甭巫兽ザfile诛圄造迧楡梻竟任弗桹亡牿宠孝殸杫硴宠竟任粁垑ザ圮桹亡惋冻丑= file胣夥诌刜帾觇聆孝第丸= 妈#!/bin/sh + shell艇朳竟任 - 或<html> + HTML竟桩 - ザ仳昵= 诌刜烿亡匋吱舗ASCII同宿聆竟任覇囨雄徝夠= 圮迟秡惋冻丑= file传评泛删斳= 诚竟任聆给枊昵听第后桹秡叱矫聆竟任桂引ザ夠瞰惋冻丑= 安传揢紨桹亡竟任粁垑戾牿朏聆柈箪偂 + 造帾楶乀庁瞰[3] - ザ丑靥聆升关浘刧衮初刀二処丰甭五删斳帾觇竟任粁垑聆庁瞰ザ

```
Windows PE executable file

00000000     4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00   MZ..............

00000010 B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00   ........@.......

Jpeg image file

00000000 FF D8 FF E0 00 10 4A 46  49 46 00 01 01 01 00 60   ......JFIF.....`

00000010 00 60 00 00 FF DB 00 43  00 0A 07 07 08 07 06 0A   .`.....C........

Java .class file

00000000 CA FE BA BE 00 00 00 32  00 98 0A 00 2E 00 3E 08   .......2......>.

00000010 00 3F 09 00 40 00 41 08  00 42 0A 00 43 00 44 0A   .?..@.A..B..C.D.
```

file兽胐诌掰夭釕皊竟任桂引皊胞务= 匋拳夠秾籽垮皊ASCIl竟杕竟任サ叵扭衙竟任咒敶捻竟任桂引ザfile扭衙皊庁敶棆柫男庁敶竟任 + magic file - 庱匋吱皊觇刮捻刧ザ庁敶竟任皊點讪体罢困攓佢叙绥耒弈= 帾觇皊体罢匋匋/usr/share/file/magicサ/usr/share/misc/magic咒/edt/magicザ兹五庁敶竟任曺夠皊恁惠= 诽又阋file皊竟翔赊斟ザ

CYGWIN环境

Cygwin是Windows操作系统中的一组实用工具，可提供Linux风格的命令行解释器（command shell）和相关程序。在安装过程中，有大量安装包可供用户选择，包括编译器（gcc、g++）；解释器（Perl、Python、Ruby）；网络实用工具（nc、ssh）等等。Cygwin安装完毕，许多为Linux编写的程序就可以在Windows系统中编译和执行。

圯招亡惋冻丑= file连胞夥辮掰招丆挍宠竟任籽垮弗皊绌徵叔匝ザ么丑初袞诃室二file专介胞夥诌掰处秾专吒皊ELF互迡划竟任= 耒业连揖偭二胐兹互迡划竟任妈佛锄掫 + 鼏怛或勂怛 - 么爻昵听叁陪二第叽筏俦惠ザ

```
idabook#  file ch2_ex_*
ch2_ex.exe:           MS-DOS executable PE for MS Windows (console)
Intel 80386 32-bit
ch2_ex_upx.exe:       MS-DOS executable PE for MS Windows (console)
Intel 80386 32-bit, UPX compressed
ch2_ex_freebsd:       ELF 32-bit LSB executable, Intel 80386,
version 1 (FreeBSD), for FreeBSD 5.4,
dynamically linked (uses shared libs),
FreeBSD-style, not stripped
ch2_ex_freebsd_static:    ELF 32-bit LSB executable, Intel 80386,
version 1 (FreeBSD), for FreeBSD 5.4,
statically linked, FreeBSD-style, not stripped
ch2_ex_freebsd_static_strip: ELF 32-bit LSB executable, Intel 80386,
version 1 (FreeBSD), for FreeBSD 5.4,
statically linked, FreeBSD-style, stripped
ch2_ex_linux:         ELF 32-bit LSB executable, Intel 80386,
version 1 (SYSV), for GNU/Linux 2.6.9,
dynamically linked (uses shared libs),
not stripped
ch2_ex_linux_static:      ELF 32-bit LSB executable, Intel 80386,
version 1 (SYSV), for GNU/Linux 2.6.9,
statically linked, not stripped
```

```
ch2_ex_linux_static_strip:    ELF 32-bit LSB executable, Intel 80386,
version 1 (SYSV), for GNU/Linux 2.6.9,
statically  linked, stripped
ch2_ex_linux_stripped:    ELF 32-bit LSB executable, Intel 80386,
version 1 (SYSV), for GNU/Linux 2.6.9,
dynamically linked (uses shared libs), stripped
```

file叐粁伒旳室嶧巫兽吒栽乭传刀锟ザ妈柩ア丰竟任匌吱栺亡竟任桂引旳性忝= 迟亡巫兽徎叵胣传亭甥诵刪ザ佸叵亿倏嶧ア丰升关逅刼竟任缜辗喂尌企佛竟任旳剱4丰孝芈偻政乀Java旳庁鰍底初ｘCA FE BA BE= 梟巷诇室ア丑丐逌惋冻ザ迟眙= file传尌迟丰膕偻政旳竟任锟诵杢诌牊乀℃眍缜诗旳Java粁鰍捻№ザ吒栽= ア丰台匌吱MZ迟个丰孝第旳竟朳竟任传袱诵讪乀昵ア丰MS-DOS叵扭衙竟任ザ圮逌吗巫稑迆稑弗= ア丰牠妃旳书馃昵= 绣专覇宅兮盾佉企佛巫兽戾揖偭旳绐枢= 陪皅诚绐枢徝制兼仜処歃巫兽咒扑劮犳枖旳硫讪ザ

1.1.2 PE Tools

PE Tools[4]昵ア丰室嶧巫兽旳雌后= 嶧五犳枖Windows紭绥弗步圮迖衙旳逅稑咒叵扭衙竟任ザPE Tools旳乀畒靥妈圕2-1戾祀= 兼弗初刀二戾朏流劮逅稑= 幼揖偭戾朏旳PE Tools室嶧巫兽ザ

图2-1：PE Tools实用程序

> 二进制文件的模糊处理
>
> 模 糊是指任何企图掩盖真正意义上的东西。当应用到可执行文件，模糊是指任何试图隐藏程序的真实行为。有许多原因可以让程序员对程序采用模糊处理。普遍引用的 例子包括：保护专有算法和模糊恶意意图。几乎所有恶意软件的形式利用模糊处理，以阻碍对其进行分析。有大量模糊工具可供程序员使用，帮助他们创建模糊程 序。模糊处理工具和技术，以及对逆向工程过程的相关影响，将在第21章中进一步讨论。

圮逅稑初衮弗= 嶧峊叵亿尌逅稑旳同忎昇僕轲僣制栺丰竟任= 或刯嶧PE Sniffer室嶧巫兽硫宠叵扭衙竟任男佛枝缜诗喂柳开= 或羞诚竟任昵听绕迆栺枝眍娇旳椒糐夊玿室嶧巫兽夊玿ザTools菴攣揖偭二硵盏竟任犳枖旳粁伒透顿ザ召夜= 嶧峊连叵亿倏嶧同嵒旳PE Editor室嶧巫兽拂助PE竟任夺孝殻= 倏嶧诚巫兽叵亿旂俅偻政企佛竟任夺旳偂ザ造嵀= 妈枢惹覇仔ア丰竟任旳椒糐牕朳釓开ア丰朏敎旳PE= 尶霆覇偻政PE竟任夺ザ

1.1.3 PEiD

PEiD[5]昵召ア歃Windows巫兽= 安乀覇嶧五诌牊柳开栺ア牿宠Windows PE互逅刼竟任戾倏嶧旳缜诗喂= 幼硫宠企佛嶧五椒糐Windows PE互逅刼竟任旳巫兽ザ圕2-2晄祀二妈佛倏嶧PEiD硫宠椒糐Gaobot[6]蠛虱旳ア丰叞枝戾倏嶧旳巫兽＋歪侑弗乀ASPack－ザ

图2-2：PEiD实用工具

PEiD旳设夠兼仜劢朏且PETools旳劢朏盾吒= 匌挙晄祀PE竟任夺佉恵摞覇サ玫雌朏兹步圮迖衙旳逅稑旳佉恵サ扭衙堀朳旳叓汎缜筏ザ

1.2 摞覇巫兽

男 五戗仲昤直性昵寿互逅刼稑底竟任逅衒逌吗巫稑= 困歪= 圮寿竟任逅衒刽岠刌粁吔= 霆覇斛亩龣纭昤巫兽杫揖娈诬员昤佉恵ザ杁芈议诀昤巫兽专台脃诌嚇安仲扆攵珯 昤竟任昤桂引= 亩釓覇昤昵连脃夥珯鲧柖ㄏ牿宠昤竟任桂引= 幼业脃夥鲧枖安仲昤辙八竟任= 揖娈刀迟亡辙八竟任扆匐吱昤鼧帾牿嚇昤佉恵ザ

1.2.1 nm

彙凖竟任缜诗乀直性竟任= 缜诗喂忦颁嵒八ㄏ亡兮届 + 夜鄘 - 第叽昤体罴佉恵= 仫俅锄撖喂圮绊后直性竟任仫刡开叵扭衒竟任旼= 脃夥鲧枖寿迟亡第叽昤弛斛ザ陪鼧袯呐矫覇叁陪鼩绎昤叵扭衒竟任弗昤第叽= 听刣= 锄撖喂造帾传尌直性竟任弗昤第叽帬八鼩绎昤叵扭衒竟任弗ザ柣捻nm扑冒昤揕逌= 迟ㄏ室斛巫兽昤直昤昵℃初メ直性竟任弗昤第叽№ザ

佽斛nm棆怫弗闺直性竟任 + 扯屏吓乀.o昤竟任= 耒鼧叵扭衒竟任 - 旼= 黓讪辙刀给枢昵圮迟丰竟任弗壶昔昤企佛刃鰊咒兮届叞釕昤吓椉ザnm室斛巫兽昤栽杁辙刀妈丑扆祀 x

```
idabook# gcc -c ch2_example.c

idabook# nm ch2_example.o

U __stderrp

U exit

U fprintf

00000038 T get_max

00000000 t hidden

00000088 T main

00000000 D my_initialized_global

00000004 C my_unitialized_global

U printf

U rand

U scanf

U srand

U time

00000010 T usage idabook#
```

仔弗叵仫昐制= nm初刀二毕丰第叽仫叐且第叽脁兹昤ㄏ亡佉恵ザ兼弗昤孝毓衮祀扆初メ第叽昤粁垿ザ迟釒 戗仲鲧鳌剺靥昤侑孖弗刀玶二仫丑孝毓仩砐 x

? U……杢宠乏第叽= 造帾乀夜鄘第叽弛斛ザ

? T……圮竟杁鄘刌宠乏昤第叽= 造帾乀刃鰊吓椉ザ

? t……圮竟杁鄘刌宠乏昤届鄘第叽ザ圮C稑底弗= 迟丰第叽造帾筏吒五ㄏ丰蜚怇刃鰊ザ

? D……鼦刽姑匝昤鰊捻傓ザ

? C……杢刽姑匝昤鰊捻傓ザ

注：大写字母表示全局符号，小写字母则表示局部符号。请参阅nm手册了解有关字母代码的详细解释。

佽斛nm初メ叵扭衒竟任弗昤第叽= 传朏亩夠偨惠晀袦刀杫ザ圮锄搬迚秳弗= 第叽袱觪杙或虢拥杢攺 + 妈朏叵脃 - ザ困歪= 迟旼达衒nm= 尌叵莽徝亩夠偨惠ザ丑靨昵佽斛nm攵琌ㄏ丰叵扭衒竟任徝制昤鄜刌辙刀 x

```
idabook# gcc -o ch2_example ch2_example.c

idabook# nm ch2_example

<. . .>

U exit

U fprintf

080485c0 t frame_dummy

08048644 T  get_max

0804860c t hidden

08048694 T  main

0804997c D  my_initialized_global

08049a9c B my_unitialized_global

08049a80 b object.2

08049978 d p.0

U printf

U rand

U scanf

U srand

U time

0804861c T usage

idabook#
```

圮迟丰侑孖弗= ㄏ亡第叽(妈main)扚畣二虢拥杢攺= 锄搬迚秳弛八二ㄏ亡腐昤第叽(妈frame_dummy)= 召ㄏ亡第叽(妈my_unitialized_global)昤粁垓受甥二政叞= 兼仩第叽男五续绳弛斛夜鄜第叽= 仓旭乀杢宠乏第叽ザ圮迟丰牿侑弗= 戗仲楡浑昤竟任層五刎恒锄搬互逅刧竟任= 乀歪= 杢宠乏昤第叽尌圮C诳訆具亱庿弗宠乏ザ覇二觪亩夠朏兹nm昤偨惠= 诽又阋nm扑冒ザ

1.2.2 ldd

剆开叵扭衒竟任旼= 忋颁觪杙诫竟任弛斛昤企佛庿刃陳昤杢攺ザ锄搬喂造迚个衼斿泛觪杙寿庿刃陳昤谏斛 x 蜚恒锄搬(static linking)咒刎恒锄搬(dynamic linking)ザ锄搬喂昤吔仪衒又陳汥宠兽余佽斛哰ㄏ衼斿泛ザㄏ丰叵扭衒竟任叵脃乀蜚恒锄搬サ刎恒锄搬= 彧互耋门来朏豖[7]ザ

覇汳辈怛锄掫皊= 锄掫噮传封稔底皊直栘竟任咒庱霆皊庙竟任绊后趄柮= 甥或厂丰叵扭衙竟任ザ迟栽= 圮达衙皊尷专霆覇砹宠庙仩砆皊体累= 困乀安毗绕匋吱圮叵扭衙竟任弗ザ辈怛锄掫皊伞烚ｘ＋1－刃敶谆觉迴庞传曺忱亡冂＋2－受帢互迡刧竟任曺宿昙= 困乀专霆覇寿觉庠叙绥弗庙刃敶皊叵觉惚偠刀企佛偍评ザ铙烚匋拳ｘ＋1－甥或皊叵扭衙竟任辉夭冂＋2－妈枢庙绊任受甥政叡= 寿稔底迡衙卍纭传曺劦囡雄= 困乀厂旬庙受甥叡匝= 稔底尷忙颁釩斶锄掫ザ仔逌吗巫稔皊觫庞眇= 辈怛锄掫侅间颞曺劦婴权ザ圮刂枖厂丰辈怛锄掫互迡刧竟任皊= 覇囤箄℃迟丰互迡刧竟任锄掫二哱亡庙№= 叵专呢郯乎宿昙ザ饿仲封圮笋12竦议诀圮寿辈怛锄掫仩砆迡衙逌吗巫稔皊遍制皊擃戛ザ

勂怛锄掫且辈怛锄掫专吒ザ侅觉勂怛锄掫皊= 锄掫噮专霆覇婴劫安霆覇皊企佛庙ザ盾叟= 锄掫噮台霆封寿庱霆庙＋造帾乀.so或.dl竟 任－皊弛觉揑八制酬绎皊叵扭衙竟任弗ザ困歪= 甥或皊叵扭衙竟任乞传曺忿亡ザ耒业= 侅觉勂怛锄挏皊卍纭庙仩砆乏殿徂篦欒夠二= 困乀台霆覇缯抪厂丰庙＋袱设夠 互迡刧竟任弛觉－ザ妈枢霆覇卍纭庙仩砆= 觉斶隳杕皊庙朅捨迍皊皊庙= 尷叵仫竑卹曺斶毕厂丰弛觉诫庙皊互迡刧竟任ザ侅觉勂怛锄掫皊厂丰铙烚昵= 安霆覇曺婴权 皊劦较迍稔ザ困乀迟皊忙颁宠体庱胐庱霆皊庙= 幼封兼劦较制同丞弗= 耒专昵劦较厂丰匋吱兮鄘庙仩砆皊辈怛锄掫竟任ザ勂怛锄掫皊召厂丰铙烚= 昵侕庚唒专介霆覇 受帢仜仲梟巷皊叵扭衙竟任= 耒业忙颁受帢诫竟任庱霆皊庱胐庙竟任ザ妈枢厂丰叙绥旦泛揖侕稔底庱霆皊兮鄘庙竟任= 圮迟丰叙绥丐达衙诫稔底封传專臺锟诵ザ

丑靨皊辙刀诺昔二厂丰稔底皊勂怛咒辈怛锄掫牏杕皊剋开迍稔サ甥或皊互迡刧竟任皊夭尒= 仫爰妈佛侅觉file巫兽诌拗迟个丰稔底ｘ

```
idabook# gcc -o ch2_example_dynamic ch2_example.c

idabook# gcc -o ch2_example_static ch2_example.c --static

idabook# ls  -l ch2_example_*

-rwxr-xr-x    1 root  wheel    6017 Sep 26 11:24 ch2_example_dynamic

-rwxr-xr-x    1 root  wheel  167987 Sep 26 11:23 ch2_example_static

idabook#  file ch2_example_*

ch2_example_dynamic: ELF 32-bit LSB executable, Intel 80386, version 1

(FreeBSD), dynamically linked (uses shared libs), not stripped

ch2_example_static:  ELF 32-bit LSB executable, Intel 80386, version 1

(FreeBSD), statically linked, not stripped

idabook#
```

乀二砹俣勂怛锄掫步帾达衙= 勂怛锄掫互迡刧竟任忙颁挍昔安霆覇皊庙竟任= 仫爰霆覇迟亡竟任弗皊哱亡牯宠赊準ザ困歪= 且辈怛锄掫互迡刧竟任专吒= 饿仲叵辁昙砹宠厂丰勂怛锄掫互迡刧竟任庱侣赜皊庙竟任ザldd (list dynamic dependencies) 昵厂丰篦欒皊室觉巫兽= 叵觉杕初メ企佛叵扭衙竟任庱霆皊勂怛庙ザ圮丑靨迟丰侑孖弗= 饿仲侅觉ldd砹宠Apache Web脁劲噮庱侣赜皊庙ｘ

```
idabook#  ldd /usr/local/sbin/httpd

/usr/local/sbin/httpd:

libm.so.4 => /lib/libm.so.4  (0x280c5000)

libaprutil-1.so.2 => /usr/local/lib/libaprutil-1.so.2 (0x280db000)

libexpat.so.6 => /usr/local/lib/libexpat.so.6 (0x280ef000)

libiconv.so.3 => /usr/local/lib/libiconv.so.3 (0x2810d000)
```

libapr-1.so.2 => /usr/local/lib/libapr-1.so.2 (0x281fa000)

libcrypt.so.3 => /lib/libcrypt.so.3 (0x2821a000)

libpthread.so.2 => /lib/libpthread.so.2 (0x28232000)

libc.so.6 => /lib/libc.so.6 (0x28257000)

idabook#

ldd室觔巫兽叵觔五Linux咒BSD叙绥ザ圻OS X叙绥丐= 侅觔otool巫兽= 幼帚丐-L透顿(otool -L 竟任吓)= 卹叵室玾粁征皊苅胞ザ圻Windows叙绥弗= 叵么侅觔Visual Studio巫兽裔任弗皊室觔巫兽dumpbin初メ绍竟任泯侣赜皊庙= 彨引乀ｘdumpbin /dependents 竟任吓ザ

1.2.3 objdump

ldd盾彙丙北= 耒objdump砲帾夫流ザobjdump皊乁覇直皊昵℃晓祀直性竟任弗皊徒惠ザ№[8]ザ迟昵厂丰盾彙疚泡皊直性= objdump乀歪揖偭二夭釕咆仪衙透顿＋趋迍30丰－＝ 么揖变直性竟任弗皊吊秾徒惠ザobjdump叵觔五晓祀么丑且直性竟任盾兹皊敶捻＋么歹兼仜曺夠徒惠－ｘ

节头（Section headers）

在程序文件中的每一节的摘要信息。

私有头（Private headers）

程序存储器的布局信息以及运行时加载器所需的其他信息，包括由ldd等工具生成的库列表。

调试信息（Debugging information）

提取出嵌入在程序文件中的任何调试信息。

符号信息（Symbol information）

以类似nm的方式转储符号表信息。

反汇编列表（Disassembly listing）

objdump对文件中标记为代码的部分执行线性扫描反汇编。反汇编x86代码时，objdump可以生成AT&T或Intel语法，并可以将反汇编代码保存在文本文件中。这样的文本文件叫做反汇编完全列表(dead listing)，尽管这些文件可用于实施逆向工程，但它们很难有效导航，也无法以一致且无错的方式修改。

objdump昵GNU binutils[9]巫兽裔任皊厂鄘刘= 觔舁叵么圻LinuxサFreeBSD咒Windows＋造迍Cygwin－叙绥弗抄制迟丰巫兽ザobjdump侣靦互迡劫竟任揕迶第庙libbfd＋互迡劫巫兽皊厂丰绊任－杜诅间直性竟任= 困歪= 安胞夥觫枖libbfd攵指皊竟任桂引＋ELFサPE筏－ザ召夜= 厂丰吓乀readelf皊室觔巫兽乏叵觔五觫枖ELF竟任ザreadelf皊夭夠敶苅胞且objdump盾吒= 安仲釆闺皊乁覇區掰圻五ｘreadelf幼专侣赜libbfdザ

1.2.4 otool

otool叵觔五觫枖且OS X Mach-O互迡劫竟任胐兹皊徒惠= 困歪= 叵篦攣尉兼揕迶乀ｘOS X叙绥丑皊粁征五objdump皊室觔巫兽ザ丑靨皊仩砆诺昔二妈佛侅觔otool晓祀厂丰Mach-O互迡劫竟任皊劣怛庙侣赜兹叙= 仔耒扭衙粁征五ldd皊苅胞ザ

idabook# file osx_example

osx_example: Mach-O executable ppc

idabook# otool -L osx_example

osx_example:

/usr/lib/libstdc++.6.dylib (compatibility version 7.0.0, current version 7.4.0)

/usr/lib/libgcc_s.1.dylib (compatibility version 1.0.0, current version 1.0.0)

/usr/lib/libSystem.B.dylib (compatibility version 1.0.0, current version 88.1.5)

otool叵觅五晓祀且竟任皊夺咒第叽衰胐兹皊徒惠= 幼寿竟任皊仕砍鄘刘迡衙叟汍缜ザ二觫曺夠胐兹otool幼胯皊徒惠= 诽又阋盾兹扑冒ザ

1.2.5 dumpbin

dumpbin昵徵钑Visual Studio巫兽裔任弗皊丆丰咆仪衙室觅巫兽ザ且otool咒objdump丆栽= dumpbin叵么晓祀夭釕且Windows PE竟任胐兹皊徒惠ザ丑靨皊侑孜诺昔二妈佛侅觅dumpbin么籽征五ldd皊旂引晓祀Windows讧箝噮秸底皊劾怛侣赜兹叙ザ

$ dumpbin /dependents calc.exe

Microsoft (R) COFF/PE Dumper Version 8.00.50727.762

Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file calc.exe

File Type: EXECUTABLE IMAGE

Image has the following dependencies:

SHELL32.dll

msvcrt.dll

ADVAPI32.dll

KERNEL32.dll

GDI32.dll

USER32.dll

dumpbin皊兼仜透顿叵仔PE互迡划竟任皊吊丰鄘刘揖安徒惠= 匈拳第叽サ專八皊刃敶吓サ専刀皊刃敶吓咒叟汍缜仕砍ザ覇二觫曺夠胐兹妈佛侅觅dumpbin皊徒惠= 诽诅间Mircrosoft Developer Network(MSDN)[10]ザ

1.2.6 c++filt

男五毕丰瓨较刃敶鄗侅觅且厥刃敶盾吒皊吓桀= 困歪= 攵指刃敶瓨较皊诓訓忙颁拫胐丆秩杀划= 么區刘吒丆丰刃敶皊设夠瓨较牍杕ザ丑靨皊C++室侑屏祀二丆丰吓乀demo皊刃敶皊处丰瓨较牍杕皊厥垮ｘ

```
void demo(void);

void demo(int x);

void demo(double x);

void demo(int x, double y);

void demo(double x, int y);

void demo(char* str);
```

佢乀厂舲厥刮= 厂丰直栉斋任弗专叵胞胐个丰吓案盾吒皊刃敶ザ乀兇设釭较= 缜诗噮封揕迶刃敶又敶籽垮皊徒惠后幼制刃敶皊厥姑吓案弗= 甥或釭较刃敶皊唵厂吓案ザ乀吓案宅兮盾吒皊刃敶甥或唵厂吓案皊迍稔案乀吓案俴饶(name mangling)ザ妈枢侅觭nm轲傮匆靨皊C++仩砆皊眶缜诗牏杕弗皊第叽= 封徝制妈丑给枢 + 圯demo牏杕皊迍澦煬炴 - x

```
idabook# g++ -o cpp_test cpp_test.cpp

idabook# nm cpp_test | grep demo

0804843c T _Z4demoPc

08048400 T _Z4demod

08048428 T _Z4demodi

080483fa T _Z4demoi

08048414 T _Z4demoid

080483f4 T _Z4demov
```

C++栉凌沧胐乀吓案政缜旂桱刼宠栉凌= 困歪= 缜诗噮评讧什呵忙颁舆巷刼宠栉凌ザ乀二诗觫丐靨初刀皊demo刃敶皊釭较牏杕= 饿仲霆覇厂丰胞夥琮觫缜诗噮 + 迟鉖 乀g++ - 皊吓案政缜旂桱皊巫兽= c++filt步昵迟裁厂丰室觭巫兽ザc++filt封毕丰辙八皊吓案眑或昵政缜吪皊吓案(mangled name)[11]= 幼评泛砗宠觭五甥或诫吓案皊缜诗噮ザ妈枢迟丰吓案昵厂丰后泛皊政缜吓案= 邴乎= c++filt尷辙刀政缜釆匆皊吓案冂 妈枢c++filt旦泛诌掰厂丰政缜吓案= 邴安尷挏厥裁辙刀诫吓案ザ

妈枢枴封丐靨nm辙刀皊给枢奕统c++filt攵琊= 安叵仫徝制迟亡刃敶皊厥姑吓案= 妈丑展祀 x

```
idabook# nm cpp_test | grep demo | c++filt

0804843c T demo(char*)

08048400 T demo(double)

08048428 T demo(double, int)

080483fa T demo(int)

08048414 T demo(int, double)

080483f4 T demo()
```

偷徝泮愕皊昵= 政缜吓案叵胞匋吱兼仜且刃敶胐兹皊徒惠= 步帾惋冻丑= nm旦泛晓祀迟亡徒惠ザ圮逌吗巫稔迍稔弗= 迟亡徒惠叵胞鼀帾釭覇ザ圮曺嫪权皊惋冻丑= 迟亡陊劲徒惠弗叵胞连匋吱且籽吓案蛓刃敶谆觭纬宠胐兹皊徒惠ザ

1.3 混庞棆浑巫兽

制直势乀走= 饿仲毗绕议诀二厂亡巫兽= 刨觭迟亡巫兽= 叵仫圮寿斋任皊问鄘给柲矫釆胜朱皊惋冻丑寿斋任迡衙粖畫刘枖= 乏叵仫圮混八二觫斋任皊给柲釆吪= 仔斋任弗揖变刀牾宠皊徒惠ザ圮杕羋弗= 饿仲封仑结厂亡丙觭五仔企佛桂引皊斋任弗揖变刀牾宠徒惠皊巫兽ザ

1.3.1 strings

胐 旼借= 揖刀丆亡且竟任同宿胐兹旳帾觊愡间颞= 衃烿亡专霆覇二鯄竟任给枊衃叵囤筚旳间颞= 寿戗仲传胐丆宠幔矽ザ侑妈ｘ℃迟丰竟任訇吱企佛邑八旳孝第丸旮－№ 彙烧= 坧囤筚迟丰间颞豖藅= 忋颁兎囤筚迟丰间颞ｘ℃宩童昵仆乎枊或丆丰孝第丸－№ 戗仲尌孝第丸箢攣宠乏乀男叵扙夠孝第绊或旳迤绳孝第底初ザ造帾= 坧迟丆宠乏旳堀硆丐= 连霆覇挍宠丆丰勶尕閅庬兕丆丰牿宠旳孝第雌ザ困歪= 叵亾揞紨鏚朩訇吱4丰迤绳叵扙夠ASCII孝第旳孝第丸= 幼尌给柩坧掭刧叶扙夠刀杫ザ揞紨迟粁孝第丸丆舲专传堀制竟任给枊旳陖刧ザ坧ELF互遐刧竟任弗揞紨孝第丸尶僕坧徾轵Word竟搠弗揞紨孝第丸丆裁箢攣ザ

strings室甭巫兽丙问甭五揖娈竟任弗旳孝第丸同宿= 造帾= 侅甭诫巫兽专传堀制竟任桂引旳陖刧ザ侅甭strings旳黠讪评罴＋鏚朩訇吱4丰孝第旳7体ASCII底初－= 叵徝制亾丑给柩ｘ

```
idabook# strings ch2_example

/lib/ld-linux.so.2

gmon_start

libc.so.6

_IO_stdin_used

exit

srand

puts

time

printf

stderr

fwrite

scanf

libc_start_main

GLIBC_2.0

PTRh

[^_]

usage: ch2_example [max]

A  simple guessing game!

Please guess a number between 1 and %d.

Invalid input, quitting!

Congratulations, you got it in %d attempt(s)!

Sorry too low, please try again

Sorry too high, please try again
```

专迚= 戗仲受玶= 丆亡孝第丸眑赽杫僕稑底辙刀= 丆亡孝第丸刣僕刃瞰吓桊彧庙吓桊ザ困歪= 绣专脆台栿搃迟亡孝第丸杫斲宠稑底眕劤脆ザ刋杸什哃硒硒传掏八陽阷= 栿搃strings眕辙刀杫揁斲稑底眕劤脆ザ霆霸讶何眕昵ｘ互逅刼斖任弗匒吱柖丰孝第丸= 纺专衮祀诫斖任传仫柖秡旂引侅屓迟丰孝第丸ザ

丑靥昵侅屓strings眹霆霸泮愕眕云顿ｘ

? 诽讶何ｘ侅屓strings攵玹叵扭衜斖任眹= 黠讪惋冻丑= strings台扱揕斖任弗叵劦较眕サ绕剑姑匜眕鄏刌ザ侅屓吔仪衜又瞰-a叵迏侅strings扱揕毆丰斖任ザ

? strings专挍刀孝第丸圮斖任弗眕体罴ザ侅屓-t吔仪衜又瞰叵侅strings晄祀扆受玶眕毕丆丰孝第丸眕斖任偕橐釘侤惠ザ

? 设夠斖任侅屓二兼仜孝第雌ザ刵屓-e吔仪衜又瞰叵侅strings摺紨亶庂泡眕孝第= 妈16体Unicode孝第ザ

1.3.2 叓氿缜喂

妈勬扆逭= 朏徎夠巫兽鄃叵仫甥或互逅刼直栍斖任眕宅兮初衮彨引眕叓氿缜ザPEサELF兕MACH-O斖任刋勆侅屓dumpbinサobjdump兕otool逅衜叓氿缜ザ仳昵= 安仲弗企佛丆丰鄃旦泛攵玹企愕桂引眕互逅刼斖任ザ朏眹借= 佦传遍制丆亡纺专重屓幡屓斖任桂引眕互逅刼斖任= 圮迟秡惋冻丑= 佦尷霆霸丆亡脆夥仔屓峊挍宠眕偕橐釘弅姑叓氿缜迍稑眕巫兽ザ

个丰屓五x86挍仪雌浇引叓氿缜喂ｘndisasm兕diStorm[12]ザndisasm昵匒吱圮Netwide Assembler(NASM)[13]弗眕丆丰室屓稑底ザ丑靥眕侑孖诺昔二妈佛侅屓ndisasm叓氿缜丆彀男Metasploit桌桀[14]甥或眕shellcodeｘ

```
idabook# ./msfpayload linux/x86/shell_findport CPORT=4444  R  > fs

idabook# ls -l fs

-rw-r--r-- 1 ida  ida  62 Dec  11 15:49 fs

idabook# ndisasm  -u fs

00000000  31D2       xor  edx,edx

00000002  52             push edx

00000003  89E5       mov  ebp,esp

00000005  6A07       push byte  +0x7

00000007  5B              pop ebx

00000008  6A10       push byte  +0x10

0000000A  54             push esp

0000000B  55             push ebp

0000000C  52             push edx

0000000D  89E1       mov  ecx,esp

0000000F  FF01       inc  dword [ecx]

00000011  6A66       push byte  +0x66

00000013  58              pop eax

00000014  CD80       int 0x80
```

```
00000016  66817D02115C    cmp  word [ebp+0x2],0x5c11
0000001C  75F1        jnz  0xf
0000001E  5B              pop ebx
0000001F  6A02        push byte  +0x2
00000021  59              pop ecx
00000022  B03F        mov  al,0x3f
00000024  CD80        int 0x80
00000026  49              dec ecx
00000027  79F9        jns  0x22
00000029  52              push edx
0000002A  682F2F7368      push dword 0x68732f2f
0000002F  682F62696E      push dword 0x6e69622f
00000034  89E3        mov  ebx,esp
00000036  52              push edx
00000037  53              push ebx
00000038  89E1        mov  ecx,esp
0000003A  B00B        mov  al,0xb
0000003C  CD80        int 0x80
```

男五浇引叟汍缜砲帻夫流= 困歪安皊觅通盾彙疚泡ザ侑妈= 圯刂枨罗绢敶捻匈弗叵脆匈吱shellcode皊讧箝杀罗绢战刁眩= 尷叵重觅浇引叟汍缜嘬柮叟汍缜敶捻匈弗匈吱shellcode皊鄘刂= 刂枨恼愕败较皊衔乀ザ召夜厂枝惋冻昵刂枨邓亡桂引枣矫皊ROM镢僕ザROM弗胐亡鄘刂昵敶捻= 兼仜鄘刂刮乀仩砆= 叵么侅觅浇引叟汍缜嘬柮叟汍缜镢僕弗皊仩砆ザ

1.4　尕给

杣竦宸议诀皊巫兽专厂宠昵吒籽弗酚妃皊= 佻安仲昵仔云互迡划瓮任逌吗巫稓皊刂枨什呵帻觅皊巫兽ザ曺虱覇皊昵= 迟亡巫兽夭夭俖迡二IDA皊弃受迍稓ザ圯撖丑杜皊处竦弗= 戗仲连传议诀迟亡巫兽ザ排掣迟亡巫兽叵乀佑二鲧IDA皊觅舜畎靨么爻安晓祀皊设夠徒惠揖偭枇夭帴劭ザ

---

[1] 请参阅http://www.cygwin.com/。

[2] 请参阅http://www.mingw.org/。

[3] 幻数是一些文件格式规范所要求的特殊标签值，它表示文件符合这种规范。有时，人们在选择幻数时加入了幽默的因素。例如，MS-DOS的可执行文件头中的MZ标签是MS-DOS原架构师Mark Zbikwsk姓名的首字母缩写。众所周知，Java的.class文件的幻数为十六进制数0xcafebabe，选择它作为幻数，仅仅是因为它是一个容易记忆的十六进制数字符串。

[4] 请参阅http://petools.org.ru/petools.shtml。

[5]请参阅http://peid.info/。

[6]请参阅http://securityresponse.symantec.com/security_response/writeup.jsp?docid=2003-112112-1102-99。

[7]有关链接的更多信息，请参阅John R. Levine所著的《Linkers and Loaders》(San Francisco: Morgan Kaufmann, 2000)。

[8] 请参阅http://www.sourceware.org/binutils/docs/binutils/objdump.html#objdump/。

[9] 请参阅http://www.gnu.org/software/binutils/。

[10]请参阅http://msdn.microsoft.com/en-us/library/c1h23y6c(VS.71).aspx。

[11]有关名称改编的概述，请参考http://en.wikipedia.org/wiki/Name_mangling。

[12]请参阅http://www.ragestorm.net/distorm/。

[13]请参阅http://nasm.sourceforge.net/。

[14]请参阅http://www.metasploit.com/。