



file兽肱洵枒夭釘齡竟任桂引齡脆务 = 匄拳夠枝籽埒齡ASCII竟杻竟任サ叵扭銜竟任咒嗽捻竟任桂引ザfile扭銜  
齡庁嗽檣拂男庁嗽竟任 + magic file - 宸匄吱齡覬刮搯劫ザ庁嗽竟任齡點讪体罟困攤佢叙绥未弈 = 惝覘齡体罟  
匄匄/usr/share/file/magicサ/usr/share/misc/magic咒/edt/magicザ兹五庁嗽竟任直夠齡佻惠 = 誹又閱file  
齡竟翊除斟ザ

#### 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。

圮招亡惋冻丑 = file连胞夥辦枒招丌校宠竟任籽埒弗齡绌徵馭匪ザ佻丑初袞诃室二file专介胞夥洵枒处枝专吒  
齡ELF互迤劫竟任 = 未业连揖倘二肱兹互迤劫竟任妈佛锄擻 + 髦恒或劬恒 - 佻爰昵听叁陪二第叭筏佻惠ザ

```
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 爰 籽 征 聆 室 箭 巫 兽 吒 裁 乏 传 刀 锯 ザ 妈 枢 丌 丰 竟 任 匈 吱 招 亡 竟 任 桂 引 聆 性 忝 = 迟 亡 巫 兽 程 巨 胞 传 亭 甥 诵 删 ザ 佑 巨 佻 该 箭 丌 丰 升 关 迟 劫 竟 任 缜 辗 喂 封 企 佛 竟 任 聆 势 4 丰 孝 半 儋 政 〵 Java 聆 厅 嗽 底 初 x CA FE BA BE = 梟 巷 调 室 丌 丑 丐 迨 惋 冻 ザ 迟 叟 = file 传 封 迟 丰 孺 儋 政 聆 竟 任 锯 诵 空 诒 册 〵 ℃ 配 缜 诗 聆 Java 籽 嗽 捻 Ne ザ 吒 裁 = 丌 丰 台 匈 吱 MZ 迟 个 丰 孝 第 聆 竟 杵 竟 任 传 袱 诵 讪 〵 呢 丌 丰 MS-DOS 巨 扭 街 竟 任 ザ 圪 迨 吗 巫 稷 迨 稷 弗 = 丌 丰 艳 妃 聆 书 牒 呢 = 绣 专 霸 宅 兮 盾 佻 企 佛 巫 兽 宸 揖 俩 聆 给 枢 = 陪 醜 诚 给 枢 徂 制 兼 任 处 歇 巫 兽 咒 扑 劬 刂 朽 聆 礲 讪 ザ

### 1.1.2 PE Tools

PE Tools[4] 呢 丌 丰 室 箭 巫 兽 聆 雌 后 = 箭 五 刂 朽 Windows 叙 绥 弗 步 圪 达 街 聆 迟 稷 咒 巨 扭 街 竟 任 ザ PE Tools 聆 〵 畝 厖 妈 圆 2-1 宸 祀 = 兼 弗 初 刀 二 宸 肱 流 劬 迟 稷 = 幼 揖 俩 宸 肱 聆 PE Tools 室 箭 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。

圪 迟 稷 初 袞 弗 = 箭 庠 巨 佻 封 迟 稷 聆 问 忝 界 僕 轲 僧 制 招 丰 竟 任 = 或 刂 箭 PE Sniffer 室 箭 巫 兽 礲 宠 巨 扭 街 竟 任 男 佛 枝 缜 诗 喂 开 卅 = 或 耄 诚 竟 任 呢 听 绕 迨 招 枝 配 矫 聆 椴 糲 文 琤 室 箭 巫 兽 文 琤 ザ Tools 菴 孳 揖 俩 二 礲 盖 竟 任 刂 朽 聆 籽 征 透 顿 ザ 召 夜 = 箭 庠 连 巨 佻 该 箭 问 岳 聆 PE Editor 室 箭 巫 兽 佛 助 PE 竟 任 夺 孝 毅 = 该 箭 诚 巫 兽 巨 佻 旂 侑 儋 政 企 佛 竟 任 夺 聆 倘 ザ 造 楮 = 妈 枢 惹 霸 仔 丌 丰 竟 任 聆 椴 糲 腮 杵 釵 开 丌 丰 肱 教 聆 PE = 墟 霆 霸 儋 政 PE 竟 任 夺 ザ

### 1.1.3 PEiD

PEiD[5] 呢 召 丌 歇 Windows 巫 兽 = 安 〵 霸 箭 五 诒 册 柳 开 招 丌 犒 宠 Windows PE 互 迟 劫 竟 任 宸 该 箭 聆 缜 诗 喂 = 幼 礲 宠 企 佛 箭 五 椴 糲 Windows PE 互 迟 劫 竟 任 聆 巫 兽 ザ 圆 2-2 眺 祀 二 妈 佛 该 箭 PEiD 礲 宠 椴 糲 Gaobot [6] 蟻 虱 聆 丌 丰 馱 枝 宸 该 箭 聆 巫 兽 + 歪 侑 弗 〵 ASPack - ザ

图2-2: PEiD实用工具

PEiD 聆 设 夠 兼 任 劬 胞 且 PETools 聆 劬 胞 盾 吒 = 匈 拳 眺 祀 PE 竟 任 夺 佻 惠 摞 霸 卅 攻 雌 肱 兹 步 圪 达 街 聆 迟 稷 聆 佻 惠 卅 扭 街 堀 杵 聆 叟 馱 缜 筏 ザ

## 1.2 摞霸巫兽

男 五戢仲聆直性昵寿互迟劫稷底竟任迟街迨吗巫稷 = 困歪 = 圮寿竟任迟街创距刊籽吧 = 霆霸笋曹讫纭聆妖兽扯  
揖妄诬龄聆恁惠ザ枳半议诀聆妖兽专台胞谄册安仲宸文臻 聆竟任聆桂引 = 曹钺霸聆呢连胞夥臻觶招丌犒宠聆竟  
任桂引 = 幼业胞夥觶枳安仲聆辙八竟任 = 揖妄刀迟亡辙八竟任宸甸吱聆咆嗜犒册聆恁惠ザ

### 1.2.1 nm

橐準竟任缜诗へ直性竟任 = 缜诗喂忆颁岳八丌亡兮届 + 夜郿 - 第叭聆体罟恁惠 = 佻佻锄掬喂圮绊后直性竟任佻  
刚开巨扭街竟任旻 = 胞夥觶枳寿迟亡第叭聆弛笋ザ陪咆袱呐矫霸叁陪勣绎聆巨扭街竟任弗聆第叭 = 听刮 = 锄掬  
喂造嗜传封直性竟任弗聆第叭帮八勣绎聆巨扭街竟任弗ザ楸捻nm扑冒聆堪迨 = 迟丌室笋妖兽聆直聆呢℃初ム直  
性竟任弗聆第叭Nmザ

佻笋nm楸拂弗闰直性竟任 + 扯屏吓へ. o聆竟任 = 耒咆巨扭街竟任 - 旻 = 點讪辙刀给枢呢圮迟丰竟任弗壶昔聆企  
佛刃嗽兕兮届馱釘聆吓案ザnm室笋妖兽聆裁枳辙刀妈丑宸祀 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_uninitialized_global
```

```
U printf
```

```
U rand
```

```
U scanf
```

```
U srand
```

```
U time
```

```
00000010 T usage idabook#
```

仔弗巨佻鞠制 = nm初刀二毕丰第叭佻爰且第叭拙兹聆丌亡恁惠ザ兼弗聆孝毓袞祀宸初ム第叭聆籽埒ザ迟金 戢仲  
觶釐势曆聆侑仔弗刀坪二佻丑孝毓仕攸 x

? U……恁宠乏第叭 = 造嗜へ夜郿第叭弛笋ザ

? T……圮竟枳册刊宠乏聆第叭 = 造嗜へ刃嗽吓案ザ

? t……圮竟枳册刊宠乏聆届郿第叭ザ圮C稷底弗 = 迟丰第叭造嗜筏吒五丌丰髦恒刃嗽ザ

? D……配创姑匿聆嗽捻偷ザ

? C……恁创姑匿聆嗽捻偷ザ

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。

侏脩nm初メ叵扭銜竟任弗龄第叭 = 传脞曹夠佻惠眺祀刀祉ザ圮锄揶迤稜弗 = 第叭袂觥杓或兢拥奎坎 + 妈脞叵脼 - ザ困歪 = 迟眈达銜nm = 封叵莽值曹夠佻惠ザ丑曆呢侏脩nm文琤フ丰叵扭銜竟任值制龄郟判辙刀 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_uninitialized_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 = フ亡第叭(妈main)判畚二兢拥奎坎 = 锄揶迤稜弛八二フ亡腐龄第叭(妈frame\_dummy) = 召フ亡第叭(妈my\_uninitialized\_global)龄籽埒受甥二政馭 = 兼任第叭男五续绳弛脩夜郟第叭 = 仓旭へ杏宠乏第叭ザ圮迟丰犝侑弗 = 餓仲榆浑龄竟任層五劾恒锄揶互返劫竟任 = へ歪 = 杏宠乏龄第叭封圮C谿訓具宿庙弗宠乏ザ霸二觥曹夠脞兹nm龄佻惠 = 译又阅nm扑冒ザ

### 1.2.2 ldd

刚开叵扭銜竟任眈 = 忪颁觥杓诚竟任弛脩龄企佛庙刃嗽龄奎坎ザ锄揶喂造迤个稜旂泛觥杓寿庙刃嗽龄译脩 x 斐恒锄揶(static linking)咒劾恒锄揶(dynamic linking)ザ锄揶喂龄咆仪銜又嗽浞宠兽余侏脩啤フ稜旂泛ザフ丰叵扭銜竟任叵脼へ斐恒锄揶サ劾恒锄揶 = 或互盞门耒脞丞[7]ザ

霸刃斐恒锄掖咬= 锄掖喂传封稷底龄直性竟任咒宸霆龄庙竟任绊后赅祉= 甥或丁丰巨扭街竟任ザ迟裁= 圮达街  
咬廛专霆霸礁宠庙仕砭龄体罨= 困\安配绕甸吱圮巨扭街竟任弗ザ斐恒锄掖龄伞焯 x + 1 - 刃嗽谄筲迴龐传曹忱  
亡<sup>一</sup> + 2 - 受盼互迟劫竟任曹宿县= 困\专霆霸寿筲序叙绥弗庙刃嗽龄巨筲怩僂刀企佛促评ザ眺焯甸拳 x + 1 -  
甥或龄巨扭街竟任辉天<sup>一</sup> + 2 - 妈枢庙绊任受甥政馭= 寿稷底迟街已纆传曹荔困雄= 困\丁甸庙受甥馭匪= 稷底  
廛忆颁釭觸锄掖ザ仔迨吗巫稷龄舛龐踟= 斐恒锄掖该间顯曹荔嬰杈ザ圮刳朽丁丰斐恒锄掖互迟劫竟任咬= 霸圍  
箒℃迟丰互迟劫竟任锄掖二啤亡庙№= 巨专呢炆乎宿县ザ餒仲封圮筲12竦议诀圮寿斐恒锄掖仕砭迟街迨吗巫稷  
咬遍制龄揆憂ザ

劬恒锄掖且斐恒锄掖专吒ザ该筲劬恒锄掖咬= 锄掖喂专霆霸嬰劫安霆霸龄企佛庙ザ盾叟= 锄掖喂台霆封寿宸霆  
庙 + 造悻\ . so或. dl竟 任 - 龄弛筲捏八制繇绎龄巨扭街竟任弗ザ困歪= 甥或龄巨扭街竟任乏传曹尔亡ザ未业=  
该筲劬恒锄掖咬已纆庙仕砭乏馭值筲樂夠二= 困\台霆霸絡拵丁丰庙 + 袱设夠 互迟劫竟任弛筲 - ザ妈枢霆霸已  
纆庙仕砭= 筲觸臆杙龄庙竭捨迨咬龄庙= 廛巨佻竝卹曹觸毕丁丰弛筲滅庙龄互迟劫竟任ザ该筲劬恒锄掖龄丁丰  
眺焯呢= 安霆霸曹嬰杈 龄荔较迨稷ザ困\迟咬忆颁宠体宸触宸霆龄庙= 幼封兼荔较制回忒弗= 未专呢荔较丁丰  
甸吱兮那庙仕砭龄斐恒锄掖竟任ザ劬恒锄掖龄召丁丰眺焯= 呢佻庚啞专介霆霸 受盼仁仲梟巷龄巨扭街竟任=  
未业忆颁受盼滅竟任宸霆龄宸触庙竟任ザ妈枢丁丰叙绥且泛揖佻稷底宸霆龄兮郟庙竟任= 圮迟丰叙绥巧达街滅稷  
底封传專臺錕誦ザ

丑曆龄辙刀诺昔二丁丰稷底龄劬恒咒斐恒锄掖臆杙龄刚开迨稷サ甥或龄互迟劫竟任龄夭尢= 佻爰妈佛该筲file  
巫兽谄邾迟个丰稷底 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#
```

\二礁劬恒锄掖步悻达街= 劬恒锄掖互迟劫竟任忆颁揆昔安霆霸龄庙竟任= 佻爰霆霸迟亡竟任弗龄啤亡犒宠  
賒準ザ困歪= 且斐恒锄掖互迟劫竟任专吒= 餒仲巨轻县礁宠丁丰劬恒锄掖互迟劫竟任宸侶蹟龄庙竟任ザldd  
(list dynamic dependencies) 呢丁丰筲樂龄室筲巫善= 巨筲祉初メ企佛巨扭街竟任宸霆龄劬恒庙ザ圮丑曆迟  
丰侑仔弗= 餒仲该筲ldd礁宠Apache Web眺劫喂宸侶蹟龄庙 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室籍巫兽巨籍五Linux咒BSD叙绥ザ坩OS X叙绥丐= 倭籍otool巫兽= 幼帮丐-L透顿(otool -L 竟任吓)= 卹巨室坪秆征的肋脆ザ坩Windows叙绥弗= 巨佻倭籍Visual Studio巫兽裔任弗的室籍巫兽dumppbin初メ招竟任辰侶蹟的庙= 彫引へ x dumppbin /dependents 竟任吓ザ

### 1.2.3 objdump

ldd盾彙丙北= 来objdump颯曙夫流ザobjdump的へ霸直的呢℃眺祀直性竟任弗的恁惠ザ№[8]ザ迟呢フ丰盾彙宏泡的直性= objdumpへ歪揖倘二夭釘咆仪街透顿 + 趋迳30丰 - = 佻揖姿直性竟任弗的吊枝恁惠ザobjdump巨籍五眺祀佻丑且直性竟任盾兹的嗽捻 + 佻友兼任曹狗恁惠 - 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呢GNU binutils[9]巫兽裔任的フ耶刊= 籍岸巨佻坩LinuxサFreeBSD咒Windows + 造迳Cygwin - 叙绥弗抄制迟丰巫兽ザobjdump侶颯互迳劫竟任堪迳第庙libbfd + 互迳劫巫兽的フ丰绊任 - 耻诘间直性竟任= 困歪= 安脆夥夥杖libbfd文指的竟任桂引 + ELFサPE筏 - ザ召夜= フ丰吓へreadelf的室籍巫兽艺巨籍五夥杖ELF竟任ザreadelf的夭狗嗽肋脆且objdump盾吒= 安仲禾闰的へ霸區坩坩五 x readelf幼专侶蹟libbfdザ

### 1.2.4 otool

otool巨籍五夥杖且OS X Mach-0互迳劫竟任拙兹的恁惠= 困歪= 巨篋學對兼堪迳へ x OS X叙绥丑的秆征五objdump的室籍巫兽ザ丑麗的仕矽诺昔二妈佛倭籍otool眺祀フ丰Mach-0互迳劫竟任的肋恒庙侶蹟兹叙= 仔来扭街秆征五ldd的肋脆ザ

```
idabook# file osx_example
```

```
osx_example: Mach-0 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 巨 第 五 眺 祀 且 竟 任 铃 夺 咒 第 吼 袞 肫 兹 铃 佻 惠 = 幼 寿 竟 任 铃 仕 砭 廓 刊 迢 衙 叟 决 缜 ザ 二 骸 曹 狗 肫 兹 otool 肋 脆 铃 佻 惠 = 诹 又 阅 盾 兹 扑 冒 ザ

### 1.2.5 dumpbin

dumpbin 呢 徽 轶 Visual Studio 巫 兽 裔 任 弗 铃 丌 丰 咆 仪 衙 室 第 巫 兽 ザ 且 otool 咒 objdump 丌 裁 = dumpbin 巨 佻 眺 祀 夭 釘 且 Windows PE 竟 任 肫 兹 铃 佻 惠 ザ 丑 靛 铃 侑 孖 诺 昔 二 妈 佛 佻 第 dumpbin 佻 秆 征 五 ldd 铃 旂 引 眺 祀 Windows 讠 箝 喂 嵇 底 铃 劬 恒 侣 贻 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 铃 兼 任 透 顿 巨 仔 PE 互 迢 劫 竟 任 铃 吊 丰 廓 刊 揖 变 佻 惠 = 匄 拳 第 吼 サ 専 八 铃 刃 嗽 吓 サ 専 刀 铃 刃 嗽 吓 咒 叟 决 缜 仕 砭 ザ 霸 二 骸 曹 狗 肫 兹 妈 佛 佻 第 dumpbin 铃 佻 惠 = 诹 诿 间 Microsoft Developer Network (MSDN) [10] ザ

### 1.2.6 c++filt

男 五 毕 丰 釳 较 刃 嗽 郇 佻 第 且 厥 刃 嗽 盾 吒 铃 吓 窠 = 困 歪 = 欠 指 刃 嗽 釳 较 铃 诹 訃 忪 颁 根 肫 丌 枝 杀 劫 = 佻 區 刊 吒 丌 丰 刃 嗽 铃 设 狗 釳 较 髑 杵 ザ 丑 靛 铃 C++ 室 侑 屏 祀 二 丌 丰 吓 へ demo 铃 刃 嗽 铃 处 丰 釳 较 髑 杵 铃 厥 埒 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);
```



佢へフ齡厥剖 = フ丰直性竟任弗专叵胞肱个丰吓案盾吒齡刃嗽ザへ兇设釵较 = 缜诗喂對堪道刃嗽又嗽秆埒齡佻  
惠后幼制刃嗽齡厥姑吓案弗 = 甥或釵较刃嗽齡唵フ吓案ザへ吓案宅兮盾吒齡刃嗽甥或唵フ吓案齡迤稷案へ吓案  
儻饶 (name mangling) ザ妈枢孩甯nm轲僣勢曆齡C++仕砭齡配缜诗臆杳弗齡第叭 = 討值制妈丑给枢 + 圮demo臆杳  
齡迤灑煬焯 - 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++性凌沧肱へ吓案政缜旂控劫宠性凌 = 困歪 = 缜诗喂评诂什呵怙颁鼻巷劫宠性凌ザへ二诗觥丐曆初刃齡demo刃  
嗽齡釵较臆杳 = 餓仲霆霸フ丰胞夥珍觥缜诗喂 + 迟金へg++ - 齡吓案政缜旂控齡巫兽 = c++filt步呢迟裁フ丰室  
甯巫兽ザc++filt討毕丰辙八齡吓案呦或昵政缜咆齡吓案 (mangled name) [11] = 幼评泛礮宠甯五甥或滅吓案齡缜  
诗喂ザ妈枢迟丰吓案呢フ丰后泛齡政缜吓案 = 邲乎 = c++filt樞辙刀政缜采勢齡吓案 〱 妈枢c++filt旦泛谄刼フ  
丰政缜吓案 = 邲安樞捫厥裁辙刀滅吓案ザ

妈枢枴討丐曆nm辙刀齡给枢变统c++filt攷琇 = 安叵佻值制迟亡刃嗽齡厥姑吓案 = 妈丑宸祀 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()
```

偷值泮愕齡呢 = 政缜吓案叵胞匍吱兼仟且刃嗽肱兹齡佻惠 = 步嗜惋冻丑 = nm旦泛眺祀迟亡佻惠ザ圮道吗巫稷迤  
稷弗 = 迟亡佻惠叵胞醜嗜釵霸ザ圮曹嬰杈齡惋冻丑 = 迟亡侈荔佻惠弗叵胞连匍吱且秆吓案或刃嗽諄甯纬宠肱兹  
齡佻惠ザ

### 1.3 混鹿榦浑巫兽

制直勢へ走 = 餓仲配绕议诀二フ亡巫兽 = 剖甯迟亡巫兽 = 叵佻圮寿竟任齡呵鄆给柳矫采胜未齡惋冻丑寿竟任迤  
街粍畫刼杳 = 乏叵佻圮混八二觥竟任齡给柳采咆 = 仔竟任弗揖妄刀牯宠齡佻惠ザ圮杳半弗 = 餓仲討仑结フ亡丙  
甯五仔佻佛桂引齡竟任弗揖妄刀牯宠佻惠齡巫兽ザ

#### 1.3.1 strings

舛 咬借 = 揖刀 亡且竟任回宿舛兹龄悖悒间颞 = 邨邨亡专霆霸二赫竟任给柳邨巨囤箪龄间颞 = 寿餓仲传舛 宠棧劭ザ侑妈 x °C 迟丰竟任甸吱企佛岳八龄孝第丸吝 - № 彙烧 = 圯囤箪迟丰间颞采勢 = 忤颁兔囤箪迟丰间颞 x °C 宋童昵仆乎柳或 丰孝第丸 - № 餓仲討孝第丸篋樂宠乏 男巨杖卸孝第绊或龄迤绳孝第底初ザ造悖 = 圯迟 丰宠乏龄掘砒丐 = 连霆霸控宠 丰勳孕問龐咒 丰犒宠龄孝第雌ザ困歪 = 巨佻摺紉臧未甸吱4丰迤绳巨杖卸 ASCII 孝第龄孝第丸 = 幼討给枢圯捺劫叶杖卸刀杜ザ摺紉迟秆孝第丸 龄专传规制竟任给柳龄陵劫ザ圯ELF互迟劫竟任弗摺紉孝第丸 艦僕圯徵轍Word竟翊弗摺紉孝第丸 裁篋樂ザ

strings 室甯巫兽丙问甯五揖妄竟任弗龄孝第丸回宿 = 造悖 = 侂甯诚巫兽专传规制竟任桂引龄陵劫ザ侂甯 strings 龄點讪评罟 + 臧未甸吱4丰孝第龄7体ASCII底初 - = 巨徂制佻丑给枢 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
```

专迺 = 戡仲受评 = 亡孝第丸踟赧仆稷底辙刀 = 亡孝第丸剖僕刃嗽吓窠或庙吓窠ザ困歪 = 绣专脆台楸捻迟  
亡孝第丸赧斲宠稷底龄肋脆ザ刊杖什呵洒洒传掏八陽阨 = 楸捻strings龄辙刀赧捐斲稷底龄肋脆ザ霆霸讶何龄  
呢 x 互迺劫竟任弗匍吱招丰孝第丸 = 幼专袞祀诚竟任传佻招枝旂引该脩迟丰孝第丸ザ

丑曆呢该脩strings畋霆霸泮愕龄云顿 x

? 诽讶何 x 该脩strings文琇叵扭街竟任畋 = 點讪惋冻丑 = strings台扱堪竟任弗叵荔较龄サ绕劊姑匿龄鄱刊ザ该  
脩咆仪街又嗽-a叵迺该strings扱堪馭丰竟任ザ

? strings专掎刀孝第丸圮竟任弗龄体罣ザ该脩-t咆仪街又嗽叵该strings眈祀宸受评龄毕亡丰孝第丸龄竟任偕橐  
釘佻惠ザ

? 设构竟任该脩二兼任孝第雌ザ剖脩-e咆仪街又嗽叵该strings摺紉曹広泡龄孝第 = 妈16体Unicode孝第ザ

### 1.3.2 夔夔夔

妈勃宸迺 = 肱程夠巫兽鄣叵佻甥或互迺劫直柱竟任龄宅兮初袞彰引龄夔夔夔ザPEサELF咒MACH-0竟任刊勑该脩  
dumabinサobjdump咒otool迺街夔夔夔ザ此呢 = 安仲弗企佛亡丰鄣旦泛文琇企愕桂引龄互迺劫竟任ザ肱畋借 = 佻  
传遍制亡幼专重脩楮脩竟任桂引龄互迺劫竟任 = 圮迟枝惋冻丑 = 佻馱霆霸亡脆夥仔脩辟扱宠龄偕橐釘奔姑  
夔夔夔迺稷龄巫兽ザ

个丰脩五x86扱仪雌浇引夔夔夔 x ndisasm咒diStorm[12]ザndisasm呢匍吱圮Netwide Assembler (NASM) [13]弗  
龄亡丰室脩稷底ザ丑曆龄侑仔诺昔二妈佛该脩ndisasm夔夔夔亡殼男Metasploit桌棠[14]甥或龄shellcode x

```
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

```

男五浇引夔夔夔夔夔流 = 困歪安昴通盾彙宏泡ザ侑妈 = 圪刂栝罗绢漱捻匍弗巨脆匍吱shellcode昴冂籍杀罗  
绢战刁昴 = 樞巨重甬浇引夔夔夔夔夔夔夔夔夔夔夔捻匍弗匍吱shellcode昴鄱刂 = 刂栝恼愕败较昴銜\ザ召夜丌稜惋  
冻昵刂栝炆亡桂引李矫昴ROM辍僕ザROM弗肱亡鄱刂昵漱捻 = 兼任鄱刂刂\仕砑 = 巨佻侏甬浇引夔夔夔夔夔夔  
夔夔夔僕弗昴仕砑ザ

#### 1.4 泵给

杻竦宸议诀昴巫兽专丌宠昵吒秆弗勳妃昴 = 佻安仲昵仔云互返劫竟任迨吗巫稷昴刂栝什伺曙甬昴巫兽ザ曹钁霸  
昴昵 = 迟亡巫兽天天悟迟二IDA昴奔受迨稷ザ圪撤丑杜昴处竦弗 = 餓仲连传议诀迟亡巫兽ザ排掣迟亡巫兽巨\佻  
二罽IDA昴甬庠畝曆佻佻安昴祀昴设狗佻惠揖佻佻天棧砑ザ

[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](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](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](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/>。

转载于:<https://www.cnblogs.com/mull/p/5399788.html>