(转)逆向与反汇编工具

转载

gxj1680 于 2013-12-16 15:05:14 发布 7757 收藏 1
分类专栏： 应用工具类


应用工具类 专栏收录该内容
25 篇文章 0 订阅
订阅专栏

第 1 章　逌吗且叟汍缜巫兽

二觫叟汍缜皊丆亡屁啓矫诌吨= 冓混八孬书*IDA Pro*釆剪= 仑结兼仜丆亡觭五互迡刧竟任皊逌吗巫秸巫兽= 传寿饿仲孬书胐宸帴砌ザ迟亡巫兽夭匈圯*IDA*釆剪受帡= 幼业仓烧叵觭五忱迴刐枎互迡刧竟任= 么爻宦柫*IDA*皊刐枎给枢ザ妈饿仲宸觇= *IDA*尉迟亡巫兽皊课匈劝胞毆后制安皊觭庠畎靨弗= 乀逌吗巫秸揖偭二丆丰雌或甜墉ザ黜吨= 屃篾*IDA*砹室匋吱丆丰雌或谆诛噮= 圯迟釜 饿仲专传议诀= 困乀圯笋*24*サ*25*咒*26*竦丙问议诀迟丰乁颞ザ

1.1 刐粁巫兽

造帾= 笋丆欧靨寿丆丰杢矫竟任眩= 胐忙覇间丆亡篦嚞间颞昵胐盐皊= 妈℃迟昵丰仆乎丢黝 - №囤筆迟丰间颞皊靛覇厥刮= 昵专覇侣赜竟任扯屏吓柮砹宠竟任皊粁垮ザ迟昵黜堀杕皊厥刮ザ圯胎孖釜 开竑趄℃竟任扯屏吓幼旦室陋愕乏№皊刻豬吨= 佑尷传弄姑耄虐孬书丑靨处丰室觭巫兽ザ

1.1.1 file

*file*呫仪昵丆丰栉凌皊室觭巫兽= 夭匈敶**NIX*魍桂皊摛佢叙绥咒*Windows*丑皊*Cygwin[1]*或*MinGW[2]*巫兽鄗帚胐迟丰室觭巫兽ザ*file*诛圄造迍棆柫竟任弗招亡牾宠孝殼柮砹宠竟任粁垮ザ圯招亡惋冻丑= *file*脆夥诌掷帾觇皊孝第丸= 妈*#!/bin/sh* + *shell*脡杕竟任 - 或*<html>* + *HTML*竟桩 - ザ佻昵= 诌掷邓亡匋吱醜*ASCII*问宿皊竟任覇囡雄徝匈= 圯迟秩惋冻丑= *file*传评泛删斮= 诫竟任皊给枹昵听第后招秩跁矫皊竟任桂引ザ匈敶惋冻丑= 安传搢緒招亡竟任粁垮戾牾胐皊栉箄偷 + 造帾粲乀庁敶*[3]* - ザ丑靨皊升关迡刧袞初刀二处丰觭五删斮帾觇竟任粁垮皊庁敶ザ

```
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*兽胐诌掷夭釕皊竟任桂引皊胞务= 匋拳匈枎粁垮皊*ASCII*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* - 宸匋吱皊觇刮捨刧ザ庁敶竟任皊點讪体黑困摛佢叙绥耒弈= 帾觇皊体黑匋匋*/usr/share/file/magic*サ*/usr/share/misc/magic*咒*/edt/magic*ザ兹五庁敶竟任曺匈皊恁惠= 诽又阋*file*皊竟翔赊斟ザ

CYGWIN玵墉

Cygwin呢Windows攓佢叙绥弗皊丆绊室觭巫兽= 叵揖偭Linux飏桂皊呫仪衔觫釐噮 + command shell - 咒盾兹稓底ザ圮宏裆迍稓弗= 胐夭釕宏裆匈叵偭觭庠透拯= 匈拳缜诗噮 + gccサg++ - 冖觫釐噮 + PerlサPythonサRuby - 冖罗绢室觭巫兽 + ncサssh - 筏筏ザCygwin宏裆宅毛= 设匈乀Linux缜罝皊稓底尷叵仫圮Windows叙绥弗缜诗咒扭衔ザ

圯招亡惋冻丑= file连胞夥辮粏招丆按宠竟任籽垮弗皊绌徵叡匝ザ仫丑初袞调室二file专介胞夥诌粏处枝专吒皊ELF互迡划竟任= 耒业连揖偭二胐兹互迡划竟任妈佛锄撖 + 辈恇或劾恇 - 仫夭昵听叁陪二第叭筏恁惠ザ

```
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夭籽征皊室觭巫兽吒裁乏传刀锟ザ妈枢丆丰竟任匈吱招亡竟任桂引皊性忝= 迟亡巫兽徨叵胞传亭甥诵删ザ佑叵仫倏觭丆丰升关迡划竟任缜辗噮尉企佛竟任皊势4丰孝半傻政乀Java皊厅敶底初ｘCA FE BA BE= 枭巷调室丆丑丐道惋冻ザ迟驳= file传尉迟丰斶傻政皊竟任锟诵垄诌粏乀℃匙缜诗皊Java籽敶捻№ザ吒裁= 丆丰台匈吱MZ迟个丰孝第皊竟杕竟任传袱诵讪乀昵丆丰MS-DOS叵扭衔竟任ザ圮逌吗巫稓迍稓弗= 丆丰鲃妃皊书惵昵= 绣专霸宅兮盾恄企佛巫兽展揖偭皊给枢= 陪砲诫给枢徝制兼仜处歊巫兽咒扑劾刘枖皊砘讪ザ

1.1.2 PE Tools

PE Tools[4]昵丆丰室觭巫兽皊雌后= 觭五刘枖Windows叙绥弗步圮达衔皊迡稓咒叵扭衔竟任ザPE Tools皊乁畎靨妈圄2-1展祀= 兼弗初刀二展胐流劾迡稓= 幼揖偭展胐皊PE Tools室觭巫兽ザ

圄2-1ｘPE Tools室觭稓底

互迡劫竟任帢榔糐攵琇

榔糐昵按企佛役圄捎盗眷步愕乏丐帢丢勠ザ彙庚觉制回扭衙竟任= 榔糐昵按企佛诛圄隄藕毡底帢背室衙乀ザ胐设匏厥困叵仜讯毡底呵寿毡底重觉榔糐攵琇ザ晴道弛觉帢侑孖匈拳ｘ俣抪丙胐箍泛咒榔糐恼愕愕圄ザ处乔宸胐恼愕钬任帢彤引剄觉榔糐攵琇= 仜陁碓寿兼迡衙刐枖ザ胐夭釘榔糐巫兽叵俪毡底呵侅觉= 帴动仜仲剋开榔糐毡底ザ榔糐攵琇巫兽咒抆朵= 仜妄寿逌吗巫毡迍毡帢盾兹彷哓= 酋圮笋21竦弗迡厂岠议诀ザ

圯迡毡初衰弗= 觉庠叵仜酋迡毡帢问忐昦僕轲傮制绍丰竟任= 或剄觉PE Sniffer室觉巫兽砘宠叵扭衙竟任男佛秩缜诗噮柲开= 或耋诫竟任昵听绕迍招秩跁矫帢榔糐攵琇室觉巫兽攵琇ザTools菢嶂揖侕二磈盞竟任刐枖帢籽征透顿ザ召夜= 觉庠连叵仜侅觉问岩帢PE Editor室觉巫兽柫瞈PE竟任夺孝殼= 侅觉诫巫兽叵仜旂俅俴政企佛竟任夺帢偷ザ造帾= 妈枢惹霸仔厂丰竟任帢榔糐牳杕釩开厂丰胐教帢PE= 尷霆霸俴政PE竟任夺ザ

1.1.3 PEiD

PEiD[5]昵召厂敞Windows巫兽= 安乁霸觉五诌拗柲开招厂牾宠Windows PE互迡劫竟任宸侅觉帢缜诗噮= 幼硫宠企佛觉五榔糐Windows PE互迡劫竟任帢巫兽ザ圄2-2晓祀二妈佛侅觉PEiD硫宠榔糐Gaobot[6]蠛虱帢ㄏ丰叡秩宸侅觉帢巫兽＋歪侑弗乀ASPack－ザ

圄2-2ｘPEiD室觉巫兽

PEiD帢设匏兼仜动胞且PETools帢动胞盾吒= 匈拳晓祀PE竟任夺恄惠摞覇サ孜雌胐兹步圯达衙帢迡毡帢恄惠サ扭衙堀杕帢叟汍缜筏ザ

1.2 摞覇巫兽

男五戗仲帢直性昵寿互迡劫毡底竟任迡衙逌吗巫毡= 困歪= 圯寿竟任迡衙剖岠刐籽咄= 霆覇觉曺龘纭帢巫兽柮揖娈诬员帢恄惠ザ杕羋议诀帢巫兽专台胞诌拗安仲宸攵琇帢竟任帢桂引= 曺釩覇帢昵连胞夥琇觫招厂牾宠帢竟任桂引= 幼业胞夥觫枖安仲帢辙八竟任= 揖娈刀迟亡辙八竟任宸匈吱帢鼬帾牾拗帢恄惠ザ

1.2.1 nm

彙準竟任缜诗乁直性竟任= 缜诗噮忙颁嗮八厂亡兮屆＋夜鄘－第叽帢体黑恄惠= 仜俅锄撖噮圯绊后直性竟任仜剋开叵扭衙竟任哎= 胞夥觫枖寿迟亡第叽帢弛觉ザ陪鼬袱呐矫覇叁陪酋绎帢叵扭衙竟任弗帢第叽= 听刨= 锄撖噮造帾传封直性竟任弗帢第叽帚八酋绎帢叵扭衙竟任弗ザ梳捻nm扑冒帢揕道= 迟厂室觉巫兽帢直帢呢℃初乂直性竟任弗帢第叽№ザ

侅觉nm棆柫弗闱直性竟任＋扯屏吓乁.o帢竟任= 耒鼬叵扭衙竟任－哎= 點讪辙刀给枢昵圯迟丰竟任弗壶昔帢企佛刃敶咒兮屆叡釘帢吓粲ザnm室觉巫兽帢栽杕辙刀妈丑宸祀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_unitialized_global
         U printf
         U rand
         U scanf
         U srand
         U time
00000010 T usage idabook#
```

仔弗叵亿眑制＝nm初刀二毕丰第叽亿叐且第叽胐兹旳丆亡俧惠ザ兼弗旳孝毓衮祀宸初メ第叽旳粁垟ザ迟鉯 戗仲觩鼇夠黁旳侑孖弗刀玶二亿丑孝毓仕砇ｘ

‥杢宨乏第叽＝造帾乀夜鄙第叽弛帹ザ

‥坧竟杁鄙刌宨乏旳第叽＝造帾乀刃瞰吓湥ザ

‥坧竟杁鄙刌宨乏旳屆鄙第叽ザ坧C稑底弗＝迟丰第叽造帾筷叱五丆丰辈怇刃瞰ザ

‥毢刽姑匲旳瞰捻偂ザ

‥杢刽姑匲旳瞰捻偂ザ

夭亯孝毓衮祀兮屆第叽＝尕亯孝毓刮衮祀屆鄙第叽ザ诽又阋nm扑冐二觩胐兹孝毓仕砇旳诬绌觩鼇ザ

佽帹nm初メ叵扭衒竟任弗旳第叽＝传胐亶夠俧惠晀祀刀杫ザ坧锄搬迚稑弗＝第叽袱觩杅或虠拥杢攼＋妈胐叵朎－ザ囷歪＝迟旼达衒nm＝尌叵莽徝亶夠俧惠ザ丑黁昵佽帹nm攵玸丆丰叵扭衒竟任徝制旳鄙刌辙刀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#
```

坧迟丰侑孖弗＝丆亡第叽(妈main)刌夤二虠拥杢攼＝锄搬迚稑弛八二丆亡阇旳第叽(妈frame_dummy)＝召丆亡第叽(妈my_unitialized_global)旳粁垟受甥二政叞＝兼仜第叽男五续绳弛帹夜鄙第叽＝仓旭乀杢宨乏第叽ザ坧迟丰牯侑弗＝戗仲棆浑旳竟任層五匑怇锄搬互逅刧竟任＝乀歪＝杢宨乏旳第叽尌坧C诳訆具亱庙弗宨乏ザ覇二觩亶夠胐兹nm旳俧惠＝诽又阋nm扑冐ザ

1.2.2 ldd

剅开叵扭衒竟任旼＝忇颁觩杅诚竟任弛帹旳企佛庙刃瞰旳杢攼ザ锄搬喂造迚个秡旃泛觩杅寿庙刃瞰旳谛帹ｘ辈怇锄搬(static linking)咒匑怇锄搬(dynamic linking)ザ锄搬喂旳呥仪衒又瞰汖宨兽余佽帹哰丆秡旃泛ザ丆丰叵扭衒竟任叵朎乀辈怇锄搬サ匑怇锄搬＝彧互鼜冂耒胐汖[7]ザ

覇汈辈怇锄搬旼＝锄搬喂传尌稑底旳直杵竟任咒宸霔旳庙竟任绊后赻杫＝甥或丆丰叵扭衒竟任ザ迟栽＝坧达衒旼尴专霔覇砯宨庙仕砇旳体黑＝囷乀安毢绕匋吱坧叵扭衒竟任弗ザ辈怇锄搬旳伞焫ｘ＋1－刃瞰谛帹迵庬传亶忱亡乛＋2－受畍互逅刧竟任亶宿昙＝囷乀专霔覇寿帹庤敘绥弗庙刃瞰旳叵帹惢便刀企佛偍评ザ銚焫匋挙ｘ＋1－甥或旳叵扭衒竟任辉夭乛＋2－妈柩庙绊任受甥政叞＝寿稑底逅衒卍纭传亶劦园雄＝囷乀丆旬庙受甥叞匲＝稑底尴忇颁釓阇锄搬ザ仔逌吗巫稑旳觘庬眑＝辈怇锄搬佽间颢亶劦嬰杈ザ坧刌杅丆丰辈怇锄搬互逅刧竟任旼＝覇囤箪℃迟丰互逅刧竟任锄搬二咩亡庙№＝叵专昵郑乎宿昙ザ戗仲尌坧箅12竦议诀坧寿辈怇锄搬仕砇逅衒逌吗巫稑旼遍制旳掵憂ザ

劝怗锄撖且辈怗锄撖专吒ザ佽甪劝怗锄撖旼＝锄撖喂专霆覇嬰刼安霆覇旳企佛庙ザ盾叓＝锄撖喂台霆尌寿扆霆庙＋造帾乀.so或.dl竟任－旳弛甪揑八制勶绎旳叵扭衔竟任弗ザ困歪＝甥或旳叵扭衔竟任乏传亩尕亡ザ耒业＝佽甪劝怗锄搁旼卍纭庙仩砇乏叞值笕孿夠二＝困乀台霆覇绺揜丆丰庙＋袮设夠互逅刼竟任弛甪－ザ妈柩霆覇卍纭庙仩砇＝甪擱牎杁旳庙谒捨迚旼旳庙＝尴叵仫竑豞亩擱毕丆丰弛甪诚庙旳互逅刼竟任ザ佽甪劝怗锄撖旳丆丰銚焫昵＝安霆覇亩嬰杈旳劵较迚秷ザ困乀迟旼忋颁宼体扆朏扆霆旳庙＝纺尌兼劵较制冋忎弗＝未专昵劵较丆丰匋吱兮鄅庙仩砇旳辈怗锄撖竟任ザ劝怗锄撖旳召丆丰銚焫＝昵価庚咗专介霆覇受盼仜仲皛巷旳叵扭衔竟任＝耒业忋颁受盼诚竟任扆霆旳扆朏庙竟任ザ妈柩丆丰紉绥旦泛揖価秷底扆霆旳兮鄅庙竟任＝圮迟丰紉绥丐达衔诚秷底尌传専臺锟诵ザ

丑靨旳辙刀诺昔二丆丰秷底旳劝怗咒辈怗锄撖牎杁旳刞开迚秷サ甥或旳互逅刼竟任旳夭尕＝仫叐妈佛佽甪file巫兽诌夥迟个丰秷底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#
```

乀二碄俣劝怗锄撖步帾达衔＝劝怗锄撖互逅刼竟任忋颁挍昔安霆覇旳庙竟任＝仫叐霆覇迟亡竟任弗旳哖亡牿宼赊凖ザ困歪＝且辈怗锄撖互逅刼竟任专吒＝戗仲叵铨昙碄宼丆丰劝怗锄撖互逅刼竟任扆侣赜旳庙竟任ザldd (list dynamic dependencies) 昵丆丰笕孿旳室甪巫兽＝叵甪杫初乄企佛叵扭衔竟任扆霆旳劝怗庙ザ圮丑靨迟丰侑孖弗＝戗仲佽甪ldd碄宼Apache Web跳扐喂扆侣赜旳庙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室甪巫兽叵甪五Linux咒BSD紉绥ザ圮OS X紉绥丐＝佽甪otool巫兽＝纺帬丐-L透顿(otool -L 竟任吓)＝岬叵室玶粁佂旳劢朐ザ圮Windows紉绥弗＝叵仫佽甪Visual Studio巫兽斎任弗旳室甪巫兽dumpbin初乄栺竟任扆侣赜旳庙＝豟引乀ｘdumpbin /dependents 竟任吓ザ

1.2.3 objdump

ldd盾彙丙北＝未objdump毑帾夫流ザobjdump旳乁覇直旳昵℃晄祀直栍竟任弗旳佉恵ザ№[8]ザ迟昵丆丰盾彙広泡旳直栍＝objdump乀歪揖価二夭釘咃仪衔透顿＋趋迚30丰－＝仫揖妛直栍竟任弗旳吊枝佉恵ザobjdump叵甪五晄祀仫丑且直栍竟任盾兹旳皦捻＋仫叐兼仜亩夠佉恵－ｘ

芈夺＋Section headers－

圮秷底竟任弗旳毕丆芈旳摞覇佉恵ザ

秇朏夺＋Private headers－

秷底忎僓喂旳盼屇佉恵仫叐达衔旼劵较喂扆霆旳兼仜佉恵＝匋拳男ldd筏巫兽甥或旳庙初衮ザ

谇诛佉恵＋Debugging information－

揖妄刀邑八圮稑底竟任弗眕企佛谇诛佉惠ザ

第叭佉惠 + Symbol information -

仫粁征nm眕旍引轲僣第叭衮佉惠ザ

叓氿缜初衮 + Disassembly listing -

objdump寿竟任弗性讶乀仕砇眕鄘刌扭衒绅愡扱揕叓氿缜ザ叓氿缜x86仕砇敂= objdump叵仫甥或AT&T或Intel诳泛= 幼叵仫尌叓氿缜仕砇俣忈圮竟杦竟任弗ザ迟栽眕竟杦竟任叱偄叓氿缜宅兮初衮(dead listing)= 屃篋迟亡竟任叵甪五室旐逭吗巫稑= 仳安仲徎雄胐教専舰= 乭旦泛仫丆臺业旦锟眕旍引傁政ザ

objdump昵GNU binutils[9]巫兽斎任眕丆鄘刌= 甪扂叵仫圮LinuxサFreeBSD咒Windows + 造迚Cygwin - 敘绥弗抄制迟丰巫兽ザobjdump侣靦互逅刼竟任揕迶第庿libbfd + 互逅刼巫兽眕丆丰绊任 - 杫讵闫直性竟任= 困歪= 安胞夥緂杌libbfd攵指眕竟任桂引 + ELFサPE筏 - ザ召夜= 丆丰吓乀readelf眕室甪巫兽乭叵甪五緂杌ELF竟任ザreadelf眕夭夠瞮劢胞且objdump盾吒= 安仲夈闺眕乀覇匾郱圮五ｘreadelf幼专侣赜libbfdザ

1.2.4 otool

otool叵甪五緂杌且OS X Mach-O互逅刼竟任胐兹眕佉惠= 困歪= 叵筬摮尌兼揕迶乀ｘOS X敘绥丑眕粁征五objdump眕室甪巫兽ザ丑黁眕仕砇诺昔二妈佛佽甪otool昵祀丆丰Mach-O互逅刼竟任眕犳怚庙侣赜兹敘= 仔耒扭衒粁征五ldd眕劢胞ザ

```
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叵甪五昵祀且竟任眕夺咒第叭衮胐兹眕佉惠= 幼寿竟任眕仕砇鄘刌逅衒叓氿缜ザ二緂亶夠胐兹otool劢胞眕佉惠= 诽又阅盾兹扑冐ザ

1.2.5 dumpbin

dumpbin昵徶积Visual Studio巫兽斎任弗眕丆丰晻仪衒室甪巫兽ザ且otool咒objdump丆栽= dumpbin叵仫昵祀夭釪且Windows PE竟任胐兹眕佉惠ザ丑黁眕侑孖诺昔二妈佛佽甪dumpbin仫粁征五ldd眕旍引昵祀Windows讧箝喂稑底眕犳怚侣赜兹敘ザ

```
$ 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眕兼仜透顿叵仔PE互逅刼竟任眕吊丰鄘刌揖妄佉惠= 匎搴第叭サ専八眕刃瞮吓サ専刀眕刃瞮吓咒叓氿缜仕砇ザ覇二緂亶夠胐兹妈佛佽甪dumpbin眕佉惠= 诽讵闫Mircrosoft Developer Network(MSDN)[10]ザ

1.2.6 c++filt

男五毕丰釓较刃瞮鄃佽甪且厤刃瞮盾吒眕吓袈= 困歪= 攵指刃瞮釓较眕诳訃忋颁报胐丆秓杀刼= 仫匾刌吒丆丰刃瞮眕设夠釓较膍杦ザ丑黁眕C++室侑屏祀二丆丰吓乀demo眕刃瞮眕処丰釓较膍杦眕厤垑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=厂丰直性竟任弗专叵胞胐个丰吓案盾吒皊刃敶ザ乀兇设釩较=缜诗嘳封揕道刃敶又敶籽垮皊估惠后幼制刃敶皊厥姑吓案弗=甥或釩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俊饶(name mangling)ザ妈枢侅舀nm轲傮匆靨皊C++仩砐皊盵缜诗牋杕弗皊第叽=封值制妈丑给枢+圻demo牋杕皊迍濒煬炳-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++性凌沧胐乀吓案政缜旂桱刧宠性凌=困歪=缜诗嘳评讧什呵忙颁枭巷刧宠性凌ザ乀二诗觫丐靨初刀皊demo刃敶皊釩较牋杕=饿仲霆覇厂丰胞夥琇觫缜诗嘳+迟鉖乀g++-皊吓案政缜旂桱皊巫兽=c++filt步昵迟裁厂丰室舀巫兽ザc++filt封毕丰辙八皊吓案盼或昵政缜吔皊吓案(mangled name)[11]=幼评泛砘宠舀五甥或诫吓案皊缜诗嘳ザ妈枢迟丰吓案昵厂丰后泛皊政缜吓案=烬乎=c++filt尷辙刀政缜釆匆皊吓案￣妈枢c++filt旦泛诌靡厂丰政缜吓案=烬安尷挏厥裁辙刀诫吓案ザ

妈枢枴封丐靨nm辙刀皊给枢弋统c++filt攵琇=安叵仫徝制迟亡刃敶皊厥姑吓案=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()
```

偷徝泮愕皊昵=政缜吓案叵胞匋吱兼仜且刃敶胐兹皊估惠=步帾惋冻丑=nm旦泛昡祀迟亡估惠ザ圻逌吗巫稔迍稔弗=迟亡估惠叵胞砲帾釩覇ザ圻曺婴权皊惋冻丑=迟亡陊刻估惠弗叵胞连匋吱且籽吓案或刃敶谉觭纬宠胐兹皊估惠ザ

1.3 混庞棆浑巫兽

制直剪乀走=饿仲毗绕议诀二厂亡巫兽=剄舀迟亡巫兽=叵仫圻寿竟任皊问鄘给枰矫汞晔未皊惋冻丑寿竟任迡衙粉畫刘枖=乏叵仫圻混八二觫竟任皊给枰汞吪=仔竟任弗揖窭刀牺宠皊估惠ザ圻杕羋弗=饿仲封仑结厂亡丙舀五仔企佛桂引皊竟任弗揖窭刀牺宠估惠皊巫兽ザ

1.3.1 strings

胐敢借=揖刀厂亡且竟任问宿胐兹皊帾觇怵间颞=卹烬亡专霆覇二觫竟任给枰卹叵囤箄皊间颞=寿饿仲传胐厂宠帴劭ザ侑妈ｘ℃迟丰竟任匋吱企佛峁八皊孝第丸吝-№彙烧=圻囤箄迟丰间颞汞剪=忙颁兎囤箄迟丰间颞ｘ℃宋童昵仆乎枰或厂丰孝第丸-№饿仲封孝第丸篦嶅宠乏乀男叵扙刎孝第绊或皊迤绳孝第底初ザ造帾=圻迟厂宠乏皊堀砢丐=连霆覇挍宠厂丰酬忿閂庞咒厂丰牺宠皊孝第雌ザ困歪=叵仫摺缃铖朩匋吱4丰迤绳叵扙刎ASCII孝第皊孝第丸=幼封给枢圻捺刧叶扙刎刀柮ザ摺缃迟籽孝第丸厂舲专传趿制竟任给枰皊陵刧ザ圻ELF互迡刧竟任弗摺缃孝第丸尷僕圻徵软Word竟翎弗摺缃孝第丸厂裁篦嶅ザ

strings室觉巫兽丙问觉五揖娈竟任弗皊孝第丸同宿=造帾=侅觉诫巫兽专传趿制竟任桂引皊陵刧ザ侅觉strings皊點讪评累+铖朩匋吱4丰孝第皊7体ASCII底初-=叵徝制仫丑给枢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
```

专迍= 戗仲受玾= 丆亡孝第丸跚趄柮僕稔底辙刀= 丆亡孝第丸剖僕刃敶吓案或庙吓案ザ困歪= 绣专胞台枨捻迟亡孝第丸柮斲宠稔底皊动胞ザ刂枖什呵洇洇传掏八陽阯= 枨捻strings皊辙刀柮捐斲稔底皊动胞ザ霆覇讶何皊昵ｘ互迡划竟任弗匋吱招丰孝第丸= 幼专衮祀诫竟任传仫招秾旂引侅觉迟丰孝第丸ザ

丑靨昵侅觉strings眩霆覇洋愕皊云顿ｘ

- 诽讶何ｘ侅觉strings攵琇叵扭衙竟任眩= 點讪惋冻丑= strings台扱揕竟任弗叵劄较皊サ绕刨姑匝皊鄘刂ザ侅觉咆仪衙又敶-a叵迠侅strings扱揕歐丰竟任ザ
- strings专按刀孝第丸圮竟任弗皊体黑ザ侅觉-t咆仪衙又敶叵侅strings晓祀宸受玾皊毕丆丰孝第丸皊竟任偕豪釘恄惠ザ
- 设匈竟任侅觉二兼仜孝第雌ザ刘觉-e咆仪衙又敶叵侅strings搢缃曺疚泡皊孝第= 妈16体Unicode孝第ザ

1.3.2 叟汍缜噮

妈匆宸逌= 胐徨匈巫兽鄶叵仫甥或互迡划直栘竟任皊宅兮初衮霒引皊叟汍缜ザPEサELF咒MACH-O竟任刂邢侅觉dumpbinサobjdump咒otool迡衙叟汍缜ザ侐昵= 安仲弗企佛丆丰鄶旦泛攵琇企愕桂引皊互迡划竟任ザ胐眩借= 佑传遍制丆亡幼专重觉帾觉竟任桂引皊互迡划竟任= 圯迟秾惋冻丑= 佑尷霆覇丆亡胞夥仔觉庠按宠皊偕豪釘奔姑叟汍缜迍稔皊巫兽ザ

个丰觉五x86按仪雌浇引叟汍缜噮ｘndisasm咒diStorm[12]ザndisasm昵匋吱圯Netwide Assembler(NASM)[13]弗皊丆丰室觉稔底ザ丑靨皊侑孖诺昔二妈佛侅觉ndisasm叟汍缜丆殼男Metasploit桌棠[14]甥或皊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
```

男五浇引叟汍缜砸帱夫流= 困歪安皊匍通盾彙疚泡ザ侑妈= 圩刂枟罗绢敶捻匈弗叵脆匈吱shellcode皊讧箝杀罗绢战刁欹= 尴叵重匍浇引叟汍缜喂柮叟汍缜敶捻匈弗匈吱shellcode皊郴刂= 刂枟恼愕败较皊衙乀ザ召夜厂秩惋冻昵刂枟郑亡桂引枣矫皊ROM镢僕ザROM弗胐亡郴刂昵敶捻= 兼仜郴刂剖乀仕砆= 叵幺倏匍浇引叟汍缜喂柮叟汍缜镢僕弗皊仕砆ザ

1.4 忝给

杌竦宸议诀皊巫兽专厂宠昵吒籽弗勰妃皊= 侃安仲昵仔云互迡划竟任逌吗巫毡皊刂枟什哃帻匍皊巫兽ザ酋虱覇皊昵= 迟亡巫兽夭夭倍迡二IDA皊弄受迍毡ザ圩撖丑柮皊处竦弗= 戝仲连传议诀迟亡巫兽ザ排掣迟亡巫兽叵乀佑二觫IDA皊匍庠畎靨幺歹安晓祀皊设匆恁惠揖偭枇夭帴劭ザ

---

[1] 诽又阋http://www.cygwin.com/ザ

[2] 诽又阋http://www.mingw.org/ザ

[3] 厅敶昵厂亡竟任桂引觇茉宸覇闪皊辂殊柱箪偷= 安衮祀竟任第后迟秩觇茉ザ胐哎= 什仲圩透拯庁敶哎劦八二广點皊困粑ザ侑妈= MS-DOS皊叵扭衔竟任夺弗皊MZ柱箪昵MS-DOS厥菜和帆Mark Zbikwsk姐吓皊靛孝毓缯舀ザ伝宸呗矫= Java皊.class竟任皊庁敶乀升关迡划敶0xcafebabe= 透拯安佢乀庁敶= 介介昵困乀安昵厂丰宿昙讶忌皊升关迡划敶孝第丸ザ

[4] 诽又阋http://petools.org.ru/petools.shtmlザ

[5]诽又阋http://peid.info/ザ

[6]诽又阋http://securityresponse.symantec.com/security_response/writeup.jsp?docid=2003-112112-1102-99ザ

[7]胐兹锄掀皊眚匆恁惠= 诽又阋John R. Levine宸勤皊ソLinkers and Loadersゾ(San Francisco: Morgan Kaufmann, 2000)ザ

[8] 诽又阋http://www.sourceware.org/binutils/docs/binutils/objdump.html#objdump/ザ

[9] 诽又阋http://www.gnu.org/software/binutils/ザ

[10]诽又阋http://msdn.microsoft.com/en-us/library/c1h23y6c(VS.71).aspxザ

[11]胍兹吓桨政缜鲃桐道= 诽又毒http://en.wikipedia.org/wiki/Name_manglingザ

[12]诽又阋http://www.ragestorm.net/distorm/ザ

[13]诽又阋http://nasm.sourceforge.net/ザ

[14]诽又阋http://www.metasploit.com/ザ

转自：http://blog.163.com/shanshenye2k@yeah/blog/static/823405412012930555115/