pwn return-to-dl-resolve (—) 原理分析和认识

0xC4m3l / 2019-05-14 09:16:00 / 浏览数 3959 安全技术 二进制安全 顶(1) 踩(0)

这几天学习了 return-to-dl-resolve 的知识 在这里做一些总结。 看了两个师傅的博客

l1nk3dHouse http://pwn4.fun

首先我们要了解到的是在ELF文件中 存在着一种延时绑定机制 叫做 : lazy binding。这种方式会在第一次调用一个函数时启动。

关于 lazy binding

1. 在第一次调用程序的一个函数时。会去call 一个函数。

```
DISASM
► 0x804859a <main+123>
                           call
                                  write@plt <
```

2. 然而这个call 函数指向的地方(0x80483d0)的代码为

```
► 0x80483d0
             <write@plt>
                                          jmp
                                                 dword ptr [_GLOBAL_OFFSET_TABLE_+28] <0x804a01c>
   0x80483d6
                                                 0x20
             <write@plt+6>
                                          push
                                                                                      ▶ 先知社区
   0x80483db
             <write@plt+11>
这个时候发现在 write@plt 的第一个代码是一个 jmp 跳到 (0x804a01c)保存的指针去。
```

```
x/2wx 0x804a01c
               0x080483d6
0x804a01c:
                                0x00000000
```

但是发现这个 地址并不是我们想要去的 wirte 函数的地址 而是指向了 write@plt 的下一行代

```
dword ptr [_GLOBAL_OFFSET_TABLE_+28] <0x804a01c>
► 0x80483d0 <write@plt>
                                        jmp
 0x80483d6 <write@plt+6>
                                               0x20
                                        push
  0x80483db <write@plt+11>
                                        jmp
                                                                                           光 先知社区
```

3. 接下来 程序进行了 一个 push 和 一个 jmp指令。跳转到(0x8048380)而这个地址可以用 readelf -S 文件名来找到 发现这个 地址是.plt的起始地址也就是PLT[0]

```
c4m3l@c4m3l-virtual-machine:~/Desktop/practise/re2dlresolve$ readelf -S pwn1
  There are 31 section headers, starting at offset 0x18a4:
  Section Headers:
     [Nr] Name
                                                  Addr
                                                            0ff
                                                                     Size
                                                                             ES Flg Lk Inf
                               Type
      0]
                               NULL
                                                  00000000 000000 000000
                                                                                      0
                                                                                              0
                                                                            00
                                                                                           0
      1
          .interp
                                                                                              1
                               PROGBITS
                                                  08048154 000154
                                                                    000013
                                                                             00
                                                                                   Α
                                                                                      0
                                                                                           0
          .note.ABI-tag
                                                  08048168 000168
                                                                    000020
                                                                             00
                                                                                   Α
                                                                                      0
                                                                                           0
                                                                                              4
      21
                               NOTE
                                                                                              4
          .note.gnu.build-i NOTE
                                                  08048188 000188 000024
                                                                            00
                                                                                      0
                                                                                           0
      31
                                                                                   Α
      4
                                                                                      5
                                                                                           0
                                                                                              4
          .gnu.hash
                               GNU HASH
                                                  080481ac 0001ac 00002c 04
                                                                                   Α
       51
                                                  080481d8 0001d8 0000a0 10
                                                                                      б
                                                                                           1
                                                                                              4
          .dynsym
                               DYNSYM
                                                                                   Α
          .dynstr
                                                                                              1
      6]
                                                  08048278 000278 00006b 00
                                                                                   Α
                                                                                      0
                                                                                           0
                               STRTAB
          .gnu.version
                                                                                      5
                               VERSYM
                                                  080482e4 0002e4 000014
                                                                            02
                                                                                   Α
                                                                                           0
                                                                                              2
                                                  080482f8 0002f8 000020
      8]
          .gnu.version_r
                               VERNEED
                                                                            00
                                                                                   Α
                                                                                      б
                                                                                           1
                                                                                              4
                                                                                      5
      9]
          .rel.dyn
                                                  08048318 000318 000018
                                                                                           0
                                                                                              4
                               REL
                                                                             08
                                                                                  Α
     [10]
          .rel.plt
                                                                                      5
                               REL
                                                  08048330 000330
                                                                    000028
                                                                             08
                                                                                 ΑI
                                                                                          24
                                                                                              4
     [11] .init
                               PROGBITS
                                                  08048358 000358
                                                                    000023
                                                                             00
                                                                                 AX
                                                                                      0
                                                                                           0
                                                                                              4
                                                 08048380 000380 000060
                                                                            04
                                                                                 AX
                                                                                      0
                                                                                           0
                                                                                             16
     [12] .plt
                               PROGBITS
                                                                                      0
                                                  080483e0 0003e0 000008
                                                                            00
                                                                                 AX
                                                                                           0
                                                                                              8
                               PROGBITS
          .plt.got
                                                  080483f0 0003f0 000232
                                                                                      0
                                                                                           0
                                                                                             16
     [14]
          .text
                               PROGBITS
                                                                            00
                                                                                 AX
     [15]
          .fini
                                                  08048624 000624 000014
                                                                                 AX
                                                                                      0
                                                                                           0
                                                                                              4
                               PROGBITS
                                                                            00
                                                                                              4
     [16]
          .rodata
                               PROGBITS
                                                  08048638 000638 000008
                                                                            00
                                                                                  Α
                                                                                      0
                                                                                           0
          .eh frame hdr
                               PROGBITS
                                                  08048640 000640 000034
                                                                             00
                                                                                      0
                                                                                           0
                                                                                              4
     [17]
                                                                                   Α
          .eh_frame
                                                  08048674 000674 0000f4
                                                                                      0
                                                                                           0
                                                                                              4
     [18]
                               PROGBITS
                                                                             00
                                                                                  Α
     [19]
          .init_array
                               INIT_ARRAY
                                                  08049f08 000f08
                                                                    000004
                                                                             00
                                                                                 WA
                                                                                      0
                                                                                           0
                                                                                              4
                                                                                           0
                                                                                              4
     [20]
          .fini_array
                               FINI_ARRAY
                                                  08049f0c 000f0c 000004
                                                                             00
                                                                                 WA
                                                                                      0
     [21]
                               PROGBITS
                                                  08049f10 000f10 000004
                                                                            00
                                                                                 WA
                                                                                      0
                                                                                           0
                                                                                              4
          .jcr
                                                  08049f14 000f14 0000e8
                                                                                      б
                                                                                           0
                                                                                              4
     [22]
          .dynamic
                               DYNAMIC
                                                                            08
                                                                                 WA
     [23]
          .got
                               PROGBITS
                                                  08049ffc 000ffc 000004
                                                                            04
                                                                                 WA
                                                                                      0
                                                                                           0
                                                                                              4
          .got.plt
                                                  0804a000 001000 000020
                                                                                      0
                                                                                           0
                                                                                              4
     [24]
                               PROGBITS
                                                                            04
                                                                                 WA
                                                  0804a020 001020 000008
                                                                                      0
                                                                                           0
                                                                                              4
     [25]
          .data
                               PROGBITS
                                                                            00
                                                                                 WA
          .bss
                                                  0804a040 001028 00000c
                                                                                      0
                                                                                           0
                                                                                             32
     [26]
                               NOBITS
                                                                            00
                                                                                 WA
          .comment
                                                                                      0
     27]
                               PROGBITS
                                                  00000000 001028
                                                                    000035
                                                                            01
                                                                                 MS
                                                                                           0
                                                                                              1
          .shstrtab
     [28]
                               STRTAB
                                                  00000000
                                                            001799
                                                                    00010a
                                                                            00
                                                                                      0
                                                                                           0
                                                                                              1
          .symtab
                               SYMTAB
                                                  00000000 001060 0004b0
                                                                             10
                                                                                     30
                                                                                          47
                                                                                              4
     [29]
          .strtab
                                                  00000000 001510 000289
                                                                                              1
     [30]
                               STRTAB
                                                                            00
                                                                                      Θ
                                                                                           0
  Key to Flags:
    W (write), A (alloc), X (execute), M (merge), S (strings)
    I (info), L (link order), G (group), T (TLS), E (exclude), x (unknown) O (extra OS processing required) o (OS specific), p (processor specific
4. 在imp到这个 地址后发现有 push 了一个值然后跳转到了 dl runtime resolve 函数
                                                   dword ptr [_GLOBAL_OFFSET_TABLE_+4] <0x804a004>
dword ptr [0x804a008] <0xf7fee000>
   ► 0x8048380
                                            push
     0x8048386
                                            jmp
     0xf7fee000 < dl runtime resolve>
                                                                                          ▶ 先知社区
                                            push
                                                   eax
  然后 调用这个 函数 实现 延迟绑定。 这个函数的 原型为
  _dl_runtime_resolve(*link_map, rel_offset) rel_offset 是 2.中push的值, link_map为 3.中push的值。
```

从而执行 找到write函数的真实地址 从而在下一次调用的时候直接跳转到 write函数去。

结合 IDA 反编译

```
1. 第一次call 函数会跳转到 .plt
```

.plt:080483D0 ds:off 804A01C imp .plt:080483D0 write endp

2. 然后跳转到 0x804a01c的地址保存的地方 这个地方应该为

.got.plt:0804A01C off 804A01C dd offset write

4. 从而去 push 参数 实现 将 write函数的真实地址保存在 .got.plt(保存函数引用位置) 上方便下次调用这个函数时能直接找到 write函数的地址

上面的就是延迟绑定的基本原理为了更深入了解return-to-dl-resolve 的实现我们还要学习一下 elf 文件。 ELF 可执行文件 由 ELF头部,程序头部表和对应的段,节头部表和其对应的节组成。

• 在程序头部表中会有 一个 PT_DYNAMIC 的段 ,这个段包含 .dynamic 节区 ,这个类型的段的 结构为 (这个 .dynamic 节区也被称为 "重定位节区" 可以用到 readelf -d 查看) :

```
typedef struct {
   Elf32_Sword d_tag;
   union {
        Elf32_Word d_val;
        Elf32_Addr d_ptr;
    } d_un;
} Elf32_Dyn;
```

```
readelf -d
c4m3l@c4m3l-virtual-machine:~/Desktop/practise/re2dlresolve$    readelf -d pwn1
Dynamic section at offset 0xf14 contains 24 entries:
             Type
                                           Name/Value
 Tag
0x00000001 (NEEDED)
                                          Shared library: [libc.so.6]
0x0000000c (INIT)
                                          0x8048358
0x0000000d (FINI)
                                          0x8048624
0x00000019 (INIT ARRAY)
                                          0x8049f08
0x0000001b (INIT ARRAYSZ)
                                          4 (bytes)
0x0000001a (FINI_ARRAY)
                                          0x8049f0c
0x0000001c (FINI ARRAYSZ)
                                          4 (bytes)
0x6ffffef5 (GNU HASH)
                                          0x80481ac
0x00000005 (STRTAB)
                                          0x8048278
0x00000006 (SYMTAB)
                                          0x80481d8
0x00000000a (STRSZ)
                                          107 (bytes)
0x0000000b (SYMENT)
                                          16 (bytes)
0x00000015 (DEBUG)
                                          0x0
0x00000003 (PLTGOT)
                                          0x804a000
0x00000002 (PLTRELSZ)
                                          40 (bytes)
0x00000014 (PLTREL)
                                          REL
0x00000017 (JMPREL)
                                          0x8048330
0x00000011 (REL)
                                          0x8048318
0x00000012 (RELSZ)
                                          24 (bytes)
0x00000013 (RELENT)
                                          8 (bytes)
0x6ffffffe (VERNEED)
                                          0x80482f8
0x6fffffff (VERNEEDNUM)
                                                           ▼ 先知社区
0x6ffffff0 (VERSYM)
                                          0x80482e4
0x000000000 (NULL)
```

```
• 在节区中包含着目标文件的 所有的信息用一个结构保存着。(其中Type为REL的节区包含重定位表项。可以用 readelf -S 查看)
   typedef struct {
                                  // 节头部字符串表节区的索引
       Elf32 Word sh name;
                                  // 节类型
       Elf32 Word sh type;
                                  // 节标志, 用于描述属性
       Elf32 Word sh flags;
                                  // 节的内存映像
       Elf32 Addr sh addr;
                                  // 节的文件偏移
       Elf32 Off sh offset;
                                  // 节的长度
       Elf32 Word sh size;
       Elf32 Word sh link;
                                   // 节头部表索引链接
                                   // 附加信息
       Elf32 Word sh info;
       Elf32_Word sh_addralign; // 节对齐约束
       Elf32_Word sh_entsize; // 固定大小的节表项的长度
   } Elf32 Shdr;
 readelf -S
  c4m3l@c4m3l-virtual-machine:~/Desktop/practise/re2dlresolve$    readelf -S pwn1
  There are 31 section headers, starting at offset 0x18a4:
 Section Headers:
    [Nr] Name
                                                      Off
                                                             Size
                                                                     ES Flg Lk Inf Al
                            Type
                                             Addr
     0]
                            NULL
                                             00000000 000000 000000 00
                                                                             0
                                                                                 0
                                                                                    0
      1]
         .interp
                            PROGBITS
                                             08048154 000154 000013
                                                                     00
                                                                             0
                                                                                 0
                                                                                     1
      2]
         .note.ABI-tag
                            NOTE
                                             08048168 000168 000020 00
                                                                          Α
                                                                             0
                                                                                 0
                                                                                     4
      3] .note.gnu.build-i NOTE
                                             08048188 000188 000024 00
                                                                             0
                                                                                 0
                                                                                    4
                                                                          Α
                                             080481ac 0001ac 00002c 04
                                                                                    4
      4] .gnu.hash
                            GNU HASH
                                                                            5
                                                                                 0
      5]
                            DYNSYM
                                             080481d8 0001d8 0000a0 10
        .dynsym
                                                                          Α
                                                                             б
                                                                                 1
      6]
         .dynstr
                            STRTAB
                                            08048278 000278 00006b 00
                                                                          Α
                                                                             0
                                                                                 0
                                                                                     1
         .gnu.version
                            VERSYM
                                             080482e4 0002e4 000014 02
                                                                             5
                                                                                 0
                                                                                     2
                                                                          Α
      8] .gnu.version r
                            VERNEED
                                            080482f8 0002f8 000020 00
                                                                          Α
                                                                             б
                                                                                 1
     9] .rel.dyn
                            REL
                                            08048318 000318 000018 08
                                                                             5
                                                                                 0
                                                                                    4
                                                                          Α
    [10] .rel.plt
                            REL
                                             08048330 000330 000028 08
                                                                                24
                                                                                    4
                                                                         ΑI
    [11] .init
                            PROGBITS
                                             08048358 000358 000023 00
                                                                         AX
                                                                                 0
                                                                                    4
    [12] .plt
                            PROGBITS
                                             08048380 000380 000060 04
                                                                         AX
                                                                             0
                                                                                 0 16
    [13] .plt.got
                                                                             0
                            PROGBITS
                                             080483e0 0003e0 000008 00
                                                                         AX
                                                                                 0
                                                                                    8
    [14]
                                             080483f0 0003f0 000232 00
                                                                             0
         .text
                            PROGBITS
                                                                         AX
                                                                                 0
                                                                                   16
    [15] .fini
                            PROGBITS
                                             08048624 000624 000014 00
                                                                         AX
                                                                             0
                                                                                 0
                                                                                     4
    [16] .rodata
                            PROGBITS
                                             08048638 000638 000008 00
                                                                          Α
                                                                             0
                                                                                 0
                                                                                    4
                                             08048640 000640 000034 00
    [17] .eh frame hdr
                            PROGBITS
                                                                          Α
                                                                             0
                                                                                 0
                                                                                    4
    [18] .eh frame
                            PROGBITS
                                             08048674 000674 0000f4 00
                                                                             0
                                                                                 0
                                                                          Α
    [19]
        .init array
                            INIT ARRAY
                                             08049f08 000f08 000004 00
                                                                             0
                                                                                 0
                                                                                    4
                                                                         WA
                            FINI ARRAY
    [20]
         .fini_array
                                             08049f0c 000f0c 000004 00
                                                                         WA
                                                                             0
                                                                                 0
                                                                                    4
                                             08049f10 000f10 000004 00
                                                                                     4
    [21] .jcr
                            PROGBITS
                                                                         WA
                                                                             0
                                                                                 0
                                                                                     4
    [22] .dynamic
                            DYNAMIC
                                             08049f14 000f14 0000e8 08
                                                                         WA
                                                                             б
                                                                                 0
                                             08049ffc 000ffc 000004 04
                                                                             0
                                                                                 0
                                                                                    4
    [23] .got
                            PROGBITS
                                                                         WA
    [24] .got.plt
                            PROGBITS
                                             0804a000 001000 000020 04
                                                                         WA
                                                                             0
                                                                                 0
                                                                                    4
                                             0804a020 001020 000008 00
                                                                             0
                                                                                 0
    [25] .data
                            PROGBITS
                                                                         WA
    [26] .bss
                            NOBITS
                                             0804a040 001028 00000c 00
                                                                         WA
                                                                             0
                                                                                 0
                                                                                   32
    [27] .comment
                                             00000000 001028 000035 01
                                                                         MS
                                                                             0
                                                                                 0
                            PROGBITS
                                                                                     1
    [28] .shstrtab
                                             00000000 001799 00010a 00
                                                                             0
                                                                                 0
                                                                                     1
                            STRTAB
    [29] .symtab
                            SYMTAB
                                             00000000 001060 0004b0 10
                                                                            30
                                                                                47
                                                                                     4
    [30] .strtab
                            STRTAB
                                             00000000 001510 000289 00
                                                                             Θ
                                                                                 0
 Key to Flags:
    W (write), A (alloc), X (execute), M (merge), S (strings)
     (info), L (link order), G (group), T (TLS), E (exclude), x (unknown) (extra OS processing required) o (OS specific), p (processor specific)
```

[•] 记录重定位信息的节区中。.rel.plt 用于函数定位 .rel.dyn 用于变量定位。而 REL 类型的节 的结构体为 (可以用 readelf -r 查看着两个节区)注意在 REL 类型的节中 .rel.plt 中的 info 应该如0x607 最后一位为7 而这个7 是为了在 之后找到 对应的 R_386_JUMP_SLOT。

```
typedef struct {
    Elf32_Addr r_offset;  // 对于可执行文件, 此值为虚拟地址
    Elf32_Word r_info;  // 符号表索引
} Elf32_Rel;

#define ELF32_R_SYM(info) ((info)>>8)
#define ELF32_R_TYPE(info) ((unsigned char)(info))
#define ELF32_R_INFO(sym, type) (((sym)<<8)+(unsigned char)(type))
```

c4m3l@c4m3l-virtual-machine:~/Desktop/practise/re2dlresolve\$ readelf -r pwn1 Relocation section '.rel.dyn' at offset 0x318 contains 3 entries: Offset Info Sym.Value Sym. Name Type 08049ffc 00000306 R_386_GLOB_DAT 00000000 _gmon_start_ stdin@GLIBC 2.0 0804a040 00000905 R_386_COPY 0804a040 0804a044 00000705 R_386_COPY 0804a044 stdout@GLIBC_2.0 Relocation section '.rel.plt' at offset 0x330 contains 5 entries: Offset Sym. Value Sym. Name Type 0804a00c 00000107 R_386_JUMP_SLOT 00000000 setbuf@GLIBC_2.0 0804a010 00000207 R_386_JUMP_SLOT read@GLIBC 2.0 00000000 0804a014 00000407 R_386_JUMP_SLOT 00000000 strlen@GLIBC_2.0 0804a018 00000507 R 386 JUMP SLOT 00000000 libc start main@GLIBC 2.0 write@GLIBC 2.0 0804a01c 00000607 R 386 JUMP SLOT 00000000

其中的 .rel.plt 就是 IDA 反编译过后 .got.plt的值

• 查看资料发现 .got节 保存着全局变量偏移表 , .got.plt 节保存全局函数偏移表。也就是 REL 结构体中的

在我们实现 延迟绑定时 还会调用到一个类型为 SYM的节叫做 .dynsym , 这个节的 结构为 (可以用到readelf -s 查看) 主要用于找到REL对应的函数符号表信息。用到 ELF32_R_SYM(Elf32_Rel->r_info)

```
c4m3l@c4m3l-virtual-machine:~/Desktop/practise/re2dlresolve$ readelf -s pwn1
Symbol table '.dynsym' contains 10 entries:
            Value Size Type
   Num:
                                 Bind
                                         Vis
                                                  Ndx Name
     0: 00000000
                      0 NOTYPE
                                 LOCAL
                                        DEFAULT
                                                  UND
     1: 00000000
                      0 FUNC
                                 GLOBAL DEFAULT
                                                  UND setbuf@GLIBC 2.0 (2)
     2: 00000000
                      0 FUNC
                                 GLOBAL DEFAULT
                                                  UND read@GLIBC 2.0 (2)
                      0 NOTYPE
     3: 00000000
                                         DEFAULT
                                 WEAK
                                                  UND
                                                       gmon start
     4: 00000000
                      0 FUNC
                                 GLOBAL DEFAULT
                                                  UND strlen@GLIBC_2.0 (2)
     5: 00000000
                      0 FUNC
                                 GLOBAL DEFAULT
                                                        _libc_start_main@GLIBC_2.0 (2)
                                                  UND
     6: 00000000
                      0 FUNC
                                 GLOBAL DEFAULT
                                                  UND write@GLIBC 2.0 (2)
     7: 0804a044
                      4 OBJECT
                                 GLOBAL DEFAULT
                                                   26 stdout@GLIBC 2.0 (2)
     8: 0804863c
                      4 OBJECT
                                 GLOBAL DEFAULT
                                                   16 _IO_stdin_used
                                                   26 stdin@GLIBC_2.0 (2) 厂 先知社区
     9: 0804a040
                      4 OBJECT
                                 GLOBAL DEFAULT
然后上一个.dynsym 我们得到了 num 然后通过这个 num 在.dynstr中找到对应的函数的字符串。Elf32_Sym[num]->st_name=0x4c■.dynsym +
Elf32_Sym_size■0x10■ * num) 在.dynsym的地址基础上加上 num*0x10 这个地址保存的值 , 这个值是我们需要的 函数字符串保存在
.synstr节上的偏移。比如 这个write 函数的 .rel结构体中 info = 0x607 所以这个num = 6 <-- (0x607>>8)
通过readelf -S得到这两个节的地址
通过偏移找到write函数的字符串在 .dynstr中的偏移
        x/4wx 0x80481d8 + 0x10 * 6
                                    0x00000000
                                                      0x00000000
                                                                       0x00000012±×
0x8048238:
                0x0000004c
用.dynstr基地址+偏移得到函数字符串
  mdbg> x/s 0x8048278+0x4c
                  "write"
0x80482c4:
```

总结return-to-dl-resolve调用步骤:

- 1. 首先找到函数 的reloc entry (reloc 入口) rel.plt结构体offset 和 info。push REL_offset Elf32_Rel * reloc = JMPREL + reloc_offset;
- 2. 然后计算.dynsym中对应的节入口。 Elf32_Sym * sym = &SYMTAB[ELF32_R_SYM (reloc->r_info)];
- 3. 接着验证.rel.plt中 info 的最后一字为 7 assert (ELF32_R_TYPE(reloc->r_info) == R_386_JMP_SLOT);
- 4. 在通过 info 中的 num = (reloc->r_info)>>8; 找到.dynsym 中 存的对应字符串的偏移Elf32_Sym[num]->st_name=0x4c■.dynsym + Elf32_Sym_size■0x10■ * num), 然后在.dynstr 表中找到对应的字符串的位置,然后通过字符串搜索到函数的真实地址。
- 5. 函数地址写入对应got表 , 然后执行函数。

```
// param link_map:■■■■■
// param reloc_offset:
_dl_runtime_resolve(struct link_map *1, ElfW(Word) reloc_offset)
// BEESpltBEESSESS.rel.pltBEESELF_rel
const PLTREL *const reloc = (const void *) (D_PTR (1, l_info[DT_JMPREL]) + reloc_offset);
// ■■■■.dynsym■■Elf_Sym■■
const ElfW(Sym) *sym = &symtab[ELF32_R_SYM(reloc->r_info)];
// Treloc->r_infoTTTRR_386_JUMP_SLOT=7
assert (ELFW(R_TYPE)(reloc->r_info) == ELF_MACHINE_JMP_SLOT);
// BEEstrtabEst_name
result = _dl_lookup_symbol_x (strtab + sym->st_name, 1, &sym, 1->l_scope, version, ELF_RTYPE_CLASS_PLT, flags, NULL);
value = DL_FIXUP_MAKE_VALUE (result, sym ? (LOOKUP_VALUE_ADDRESS (result) + sym->st_value) : 0);
//
return elf_machine_fixup_plt (1, result, reloc, rel_addr, value);
以上就是关于 延迟绑定 和 ELF动态链接文件的学习。
这知识程序的运行方法 想要利用这个 漏洞要 充分理解明白这个 机制的运行。
1.程序找到对应的重定位函数。
```

攻击手段。

修改.dynstr节中的字符串为我们需要的字符串这样就能在绑定是找到我们想利用的函数。

2.通过 num 找到对应函数的 字符串 从而找到函数的真实地址。

修改REL 类型节的 reloc_offset 也就是偏移实现 绑定是 由偏移定位到我们伪造的一个表 从而定位到我们需要的函数。

点击收藏 | 2 关注 | 2

上一篇:某shop API接口前台注入(通... 下一篇:Rabin加密算法和n次同余方程

- 1. 0条回复
 - 动动手指,沙发就是你的了!

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS <u>关于社区</u> 友情链接 社区小黑板