ret2libc

Ret2Text

原理

程序的代码都是存储在二进制文件中的.text段中，代码重用攻击在攻击者劫持了程序的控制流后跳转到程序本来的代码段中执行函数或是有用的指令。

栈保护措施

```
test@2-9:~$ checksec babyrepeater1
[*] Checking for new versions of pwntools
    To disable this functionality, set the contents of /home/test/.cache/.pwntools-cach
    Or add the following lines to ~/.pwn.conf or ~/.config/pwn.conf (or /etc/pwn.conf s
        [update]
        interval=never
[!] An issue occurred while checking PyPI
[*] You have the latest version of Pwntools (4.9.0)
[!] Could not populate PLT: future feature annotations is not defined (unicorn.py, line
[*] '/home/test/babyrepeater1'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

Canary

函数开始执行的时候会先往栈底插入 cookie 信息，当函数真正返回的时候会验证 cookie 信息是否合法 (栈帧销毁前测试该值是否被改变)，如果不合法就停止程序运行 (栈溢出发生)。攻击者在覆盖返回地址的时候往往也会将 cookie 信息给覆盖掉，避免漏洞利用成功。

```
          High
          Address |                 |
                  +-----------------+
                  | args            |
                  +-----------------+
                  | return address  |
                  +-----------------+
          rbp =>  | old ebp         |
                  +-----------------+
        rbp-8 =>  | canary value    |
                  +-----------------+
                  | local variables |
          Low     |                 |
          Address
```

PIE

开启之后在链接器装载程序到内存空间中时，会有一个随机的偏移量，这样攻击者无法预测text段中的代码的虚拟地址，即使攻击者劫持了控制流也无法准确地跳转到目标地址。

Ret2Libc

如果text段中没有攻击者想用的代码，攻击者可以跳转到动态链接库中，使用库函数，如system(”/bin/sh”)，由于动态链接库装载在内存中的地址也有随机化，所以首先需要计算出动态链接库的在内存中的装载地址。装载地址的计算方法一般通过泄露库函数的虚拟地址-库函数在动态链接库中的偏移。

库函数在链接库中的偏移可以通过readelf查看

```
test@2-9:~$ readelf --syms /lib/x86_64-linux-gnu/libc.so.6 | grep system
   233: 0000000000159c50    99 FUNC    GLOBAL DEFAULT   13 svcerr_systemerr@@GLIBC_2.2.5
   609: 000000000004f420    45 FUNC    GLOBAL DEFAULT   13 __libc_system@@GLIBC_PRIVATE
  1406: 000000000004f420    45 FUNC    WEAK   DEFAULT   13 system@@GLIBC_2.2.5
```

库函数中存在的字符串可以通过strings查看

```
pitog teknex binary inex
test@2-9:~$ strings -td /lib/x86_64-linux-gnu/libc.so.6 | grep /bin/sh
1785224 /bin/sh
```