

# 解决pwn题目加载指定libc版本的问题

---

不会修电脑 2021-03-16 原文

因为本地和远程的libc版本不同，pwn题目调试起来会有影响，所以来记录一下用patchelf和glibc-all-in-one来解决这个问题过程。

## 下载工具

---

下载patchelf

git clone <https://github.com/NixOS/patchelf>

下载glibc-all-in\_one

git clone <https://github.com/matrix1001/glibc-all-in-one>

[glibc-all-in\\_one](#)

```
1. $ ./update_list #更新最新版本的glibc
2. $ cat list #查看可下载的glibc
3. $ ./download glibc #glibc为你想要下载glibc的名字
```

更多说明请进入github查看: <https://github.com/matrix1001/glibc-all-in-one>

## 生成所需的符号链接

```
1. $ cd /lib64 #进入64位的目录    glibc 32位就 cd /lib
2. $ sudo su    #进入root态
3. $ ln -s /home/bhxdn/glibc-all-in-one/libs/2.32-0ubuntu3_amd64/ld-2.32.so ./32_3-linux.so.2
4.   #32代表glibc版本,3代表ubuntu后面的数字 (单纯为了好记)
5. $ ls -l #可以看到生成的符号链接
```

第三步链接的时候, 按照自己安装的目录填写。

## 更改elf文件的ld和libc

```
1. $ patchelf --set-interpreter /lib64/32_3-linux.so.2 ./pwn
2. $ patchelf --replace-needed libc.so.6 /home/bhxdn/glibc-all-in-one/libs/2.32-0ubuntu3_amd64/libc-2.32.so ./pwn#libc.so.6为需要替换的libc路径 第二个参数是需要加载的glibc的目录    pwn 是二进制文件
3. $ ldd ./bin #查看elf的ld和libc
```

找个题目实践一下

```
bhxdn@ubuntu: ~/桌面/第三赛区/fake(复件)

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

bhxdn@ubuntu:~/桌面/第三赛区/fake(复件)$ ldd fake
linux-vdso.so.1 (0x00007fffc8983000)
libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f35d8257000)
/lib64/ld-linux-x86-64.so.2 (0x00007f35d8648000)
```

```
bhxdn@ubuntu: ~/桌面/第三赛区/fake(复件)

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

bhxdn@ubuntu:~/桌面/第三赛区/fake(复件)$ ldd fake
linux-vdso.so.1 (0x00007fffc8983000)
libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f35d8257000)
/lib64/ld-linux-x86-64.so.2 (0x00007f35d8648000)
bhxdn@ubuntu:~/桌面/第三赛区/fake(复件)$ $ patchelf --set-interpreter /lib64/32_3-linux.so.2 ./pwn
$: 未找到命令
bhxdn@ubuntu:~/桌面/第三赛区/fake(复件)$ patchelf --set-interpreter /lib64/32_3-linux.so.2 ./fake
bhxdn@ubuntu:~/桌面/第三赛区/fake(复件)$ patchelf --replace-needed libc.so.6 /home/bhxdn/glibc-all-in-one
/libs/2.32-0ubuntu3_amd64/libc-2.32.so ./fake
bhxdn@ubuntu:~/桌面/第三赛区/fake(复件)$ ldd fake
linux-vdso.so.1 (0x00007ffd38d58000)
/home/bhxdn/glibc-all-in-one/libs/2.32-0ubuntu3_amd64/libc-2.32.so (0x00007f7a72bca000)
/lib64/ld-linux-x86-64.so.2 (0x00007f7a72b8f000)
bhxdn@ubuntu:~/桌面/第三赛区/fake(复件)$
```

写命令的时候，目录要根据自己的电脑是实际目录进行改写。

参考文章：

[https://blog.csdn.net/qq\\_41560595/article/details/114597342](https://blog.csdn.net/qq_41560595/article/details/114597342)

<https://www.cnblogs.com/z2yh/p/13881605.html>

<https://github.com/matrix1001/glibc-all-in-one>