初学pwn-攻防世界(get_shell)

原创

天柱是真天柱 于 2021-08-26 15:34:03 发布 536 收藏

分类专栏： pwn 文章标签： pwn

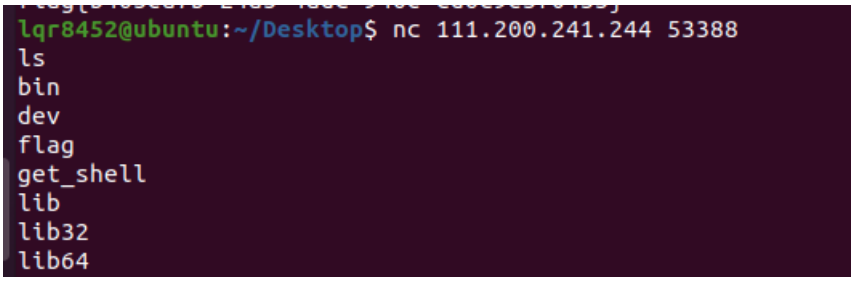
初学pwn - writeUp

从攻防世界新手区的第一道题目开始，首先是get_shell，题目上说这道题很贱单，运行就可以获取shell。这里首先使用到的工具是nc(netcat)。
Netcat 是一款简单的Unix工具，使用UDP和TCP协议。使用它你可以轻易的建立任何连接。内建有很多实用的工具。功能非常强大，这里列举一下百度到的内容，这里就算了，之后再专门介绍一下。

- telnet / 获取系统 banner 信息
- 传输文本信息
- 传输文件和目录
- 加密传输文件
- 端口扫描
- 远程控制 / 正方向 shell
- 流媒体服务器
- 远程克隆硬盘

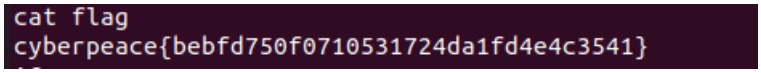
首先创建一个场景，创建之后，首先使用nc链接到对应的端口。

链接之后，输入ls命令，查看到了远端的文件，说明链接成功了。



在这里发现了flag文件，这就是我们的目标文件，直接使用命令

```
cat flag
```



这样就得到了我们这个题目的flag，完成。