

第六届蓝盾杯山东赛区省赛-比赛反思

原创

怀揣梦想的大鸡腿 于 2018-02-28 09:58:12 发布 371 收藏 2

分类专栏: [日记](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/dajitui2024/article/details/79396663>

版权



[日记](#) 专栏收录该内容

48 篇文章 0 订阅

订阅专栏

本来是确定好三个人去参赛的, 其中一个web主力因为私事, 没能去, 我只好顶替。没想到, 居然有我会做的题, 下半场的防守, 虽然不算得心应手, 但是相比较一些简单的攻击, 还是可以有效处理和面对的。只是, 有的选手过于执着, 浪费时间在我们身上太久。比如过于执着的暴力破解跑我们锁定禁止登录的用户, 以及删除了的用户。

上半场CTF答题部分:

- 1、web题很多, 破解和密码题, 隐写题。别卡在题上, 不会的赶紧下一个, 别浪费时间。
- 2、可以在实验吧刷题, 多一些思路, 基础操作可以借助合天lab操作。多练题, 以题促学, 没有别的好办法, 也没有速成的路径。

下半场AWD部分:

- 1、ssh配置文件里配置限制访问ip。防火墙可能是失效的。
- 2、一个强力防守, 随时踢掉其他登录进来的用户。
- 3、两个攻击, 一个打web攻击, 一个暴力破解和其他破解等攻击。
- 4、nfs, ssh, ftp等服务的攻击。shellcode攻击。
- 5、如果防守做的不好, 两个防守, 一个攻击。必须有一个监控的, 及时交流攻击和访问记录。
- 6、别在一个目标身上浪费太多时间, 如果对一个目标实现了一种攻击, 立刻对其他目标做一样的攻击测试。
- 7、可以访问目标目录的时候, 先遍历目录是否有flag这个关键词。