再聊CTF书籍

原创

riusksk 于 2021-03-01 17:00:00 发布 1065 收藏 10
文章标签： 腾讯 编程语言 人工智能 大数据 java
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/riusksk/article/details/114312494
版权

去年7月份，我曾写过一篇关于CTF书籍的文章，里面有一句话：

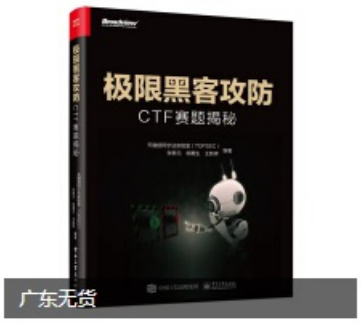
> 相信在未来两三年内，CTF主题的书籍会逐渐出现，正如当年的“企业安全建设”这个话题一样，说不定明年也可能出现“从0到1：CTFxxx"之类的书籍。国内出版社的编辑们也不妨去找找有此话题出书意向的人，或者引进国外的优秀CTF书籍。
>
> riusksk，公众号：漏洞战争「书评」聊聊打CTF的那本书

当时国内只有一本叫《CTF特训营》的书籍，现在你上京东搜索下CTF，可以找到 5 本 CTF 书籍：

¥68.10
CTF竞赛权威指南（Pwn篇）(博文视点出
3万+条评价
电子工业出版社
自营 放心购 新品

¥44.50
CTF特训营:技术详解、解题方法与竞赛技
2万+条评价
机械工业出版社自...
自营 放心购 新品

¥84.80
CTF安全竞赛入门 CTF入门指引类书籍，
7000+条评价
清华大学出版社
自营 放心购 新品



¥78.00
极限黑客攻防：CTF赛题揭秘(博文视点出
3万+条评价
电子工业出版社
自营 放心购 新品

¥99.70
【旧版售罄 新版已上市】从0到1：CTFer
3万+条评价
电子工业出版社
自营 放心购

也没想到，后面真有人出了一本叫“从0到1：CTFxxx"之类的书籍，真被我言中！

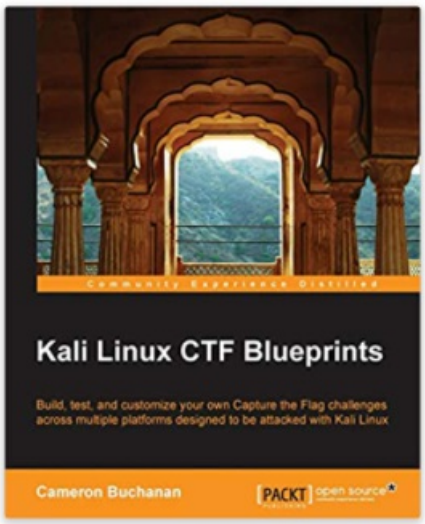
上述5本书，我只看过《CTF竞赛权威指南》与《CTF特训营》，毕竟时间有限，不过有些书籍通过目录就可看出一二。5本书中，除了《CTF竞赛权威指南》专注于Pwn技术外，其余4本都是综合类技术，覆盖面比较广，且多人合著。

之前我也曾说过一个观点：一本技术书籍由3人以内的作者合著会比较合适，少了写得累，多了不利于内容的衔接与系统化知识的构建。

上面4本综合类CTF书籍应该都是超过3人合著的，多多少少会有一些上述问题。

《CTF竞赛权威指南：Pwn篇》是由一人完成，在知识上的衔接和系统化设计上会更好一些。

国外出版的CTF书籍，我只找到下面这一本*"Kali Linux CTF Blueprints"*，2014年出版，网上可以下载到。



全书主要讲Kali在CTF上的应用，更多偏向于安全工具的使用介绍，知识陈旧落后，缺少技术原理的讲解，且CTF讲得也不多，可能书名只是借题发挥下，所以非常不推荐。

去年出版社的编辑找我，让评价下一本新书，个人看了之后觉得挺赞的。后来才知道是科恩的吴老板和腾讯eee战队帮忙审较的，质量还是有保证的。写书不易，一本好书还得值得推荐的，因此后来也帮忙写了个推荐，虽然我也不认识作者  。

> CTF赛题涉及的领域很广，市面上也早有在知识广度上均有所覆盖的CTF书籍，但没有深入单一领域的内容，尤其是Pwn方向的。本书刚好填补了这一空白：它详细介绍了各种内存破坏类型原理与利用技巧。IT行业常说“做开发要刷Leetcode，搞安全要打CTF”——这几乎已是入行的“潜规则”，相信跟随本书动手实践一遍，你的Pwn战斗值会得到较大提升。
>
> —— 泉哥，《漏洞战争：软件漏洞分析精要》作者

个人一直觉得学习过程中，知识体系的构建非常重要，书籍相比文章就应该更加注重知识体系的构建，更加系统化，更加连贯性地介绍相关技术知识，避免知识的跳跃讲解，甚至多处重复的知识点介绍。否则，收集网上的文章看看就好了。在这点上，《CTF竞赛权威指南》确实做到了。

早期CTF刚引入国内的时候，也受到一些挑战，特别是它的对实战的指导价值有多大？

从近几年在国内的推广情况看，效果还是不错的，现在很多企业、机构都搞内部CTF比赛了，我们自己招人也发现打CTF的人动手能力普遍相对会高一些。甚至在一些CTF比赛中，有人还顺手挖到0day，比如之前的ImageMagick 0day。

长亭举办的 Real World CTF 也是为了弥补这种所谓的真实应用场景的限制而举办的，他们的所有赛题全部基于真实世界软件的修改或二次开发来命题，这种模式不仅延续了传统CTF赛事中命题灵活、难度可控的特点，同时也能让参赛者在解题过程中挑战和体验Pwn赛中才会有的真实世界软件攻防技术。

遗憾的是，《CTF竞赛权威指南》书中没有体现出“Real World CTF”这种思想，如果能将一些chrome v8、vmware、qemu等主流软件的CTF赛题，甚至是CVE漏洞，通过整合CTF解题技术来实战讲解，或许可以将书籍的层次再提高一下。

书籍出版后，我也才知道原来此书早在Gitbook上开源，可免费在线阅读，内容上会有所差异：https://firmianay.gitbook.io/ctf-all-in-one/。

在gitbook上可以看到，作者增加了“实战篇”与“学术篇”，补充了CVE漏洞案例分析，以及业界学术研究成果的讲解，也是一种对“Real World CTF”思想的一种补充。

现在微信读书上也可以免费阅读，反正网上都是高清无码的免费版，大家也不用再后台留言找我要PDF了，想支持正版的，可以直接上京东去。

当前的CTF竞赛权威指南只有Pwn篇，期待未来会有Web篇、IoT篇、Reverse篇……

创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖