啥是CTF？新手如何入门CTF？

原创

代码熬夜敲 于 2021-08-18 15:34:51 发布 4478 收藏 47

分类专栏： 你永远不了CTF的魅力！ 文章标签： 编程语言 信息安全 百度 安全 java

本文链接：https://blog.csdn.net/MachineGunJoe/article/details/119779592

你永远不了CTF的魅力！ 专栏收录该内容

12 篇文章 3 订阅

订阅专栏

CTF是啥

CTF 是 Capture The Flag 的简称，中文咱们叫夺旗赛，其本意是西方的一种传统运动。在比赛上两军会互相争夺旗帜，当有一方的旗帜已被敌军夺取，就代表了那一方的战败。在信息安全领域的 CTF 是说，通过各种攻击手法，获取服务器后寻找指定的字段，或者文件中某一个固定格式的字段，这个字段叫做 flag，其形式一般为 flag{xxxxxxxx}，提交到裁判机就可以得分。

信息安全的 CTF 的历史可以说很长了，最早起源于 96 年的 DEFCON 全球黑客大会

为啥要参加CTF

入门渗透，那肯定得各种练手对不对？但因为由于 「网络安全法」的颁布，随意扫描他人网站，或非授权渗透测试都有一定的风险。最近也有个新闻：

近日，平罗法院审理了一起利用非法扫描攻击软件侵入政府信息网站的案件，董大风（化名）因犯非法侵入计算机信息系统罪，获刑9个月。

今年3月至4月，董大风通过租赁境外网络虚拟主机，远程运行其在网络上下载的捕获网站域名软件和扫描软件，欲利用扫描到的网站漏洞，对网站进行攻击，在多次对平罗县政府信息网站扫描时，被防火墙拦截。

网站技术人员发现该问题后及时报警，两天后平罗县公安局民警在厦门高崎国际机场将董大风抓获归案。

说实话，这小伙只是在扫描，攻击都被防火墙拦下了，啥都没弄到，结果还是一样被判刑，可谓是偷鸡不成蚀把米了……

所以记住千万不要乱扫国内的网站，尤其是教育、政府类网站。但初入门的同学学习渗透测试没有一个对应的环境也是不行的，而常见的靶机对于小白来说太过复杂，很容易不知如何下手。

这个时候 CTF 就非常适合了，CTF 一般是一个题目有一个或几个知识点相互糅合，相对来说目标性比较强。如果想要体会到安全的成就感和趣味性，促进自己边练边学，CTF 就是一个很好的选择。

CTF 的类型

CTF 题目类型一般分为 Web 渗透、RE 逆向、Misc 杂项、PWN 二进制漏洞利用、Crypto 密码破译，有志于渗透测试的同学一开始建议从 Web 渗透的题目开始，辅以 Misc 杂项和 Crypto 密码学。

CTF 主要分为两种模式，一是解题模式。对于 Web 安全来说，会要求你入侵网站或者靶机，攻击成功后系统会显示flag或者在某个目录 文件 数据库寻找 Flag，提交到答题系统得分。逆向工程题目一般形式是破解注册机、动态调试、dump 内存等等。这些题目可以百度或谷歌别人的解题报告（ 关键字：CTF writeup）来认识一下。

这种模式的缺点是类似于“应试教育”，当前的趋势是注重出题难、出题偏，没有考虑实际，就跟奥数似的。而且这种模式只有攻击，却没有防守，而在企业中工作更多的还是考虑如何防护的问题，这个时候 AWD 攻防赛模式就应运而生了。

二是攻防赛，也叫 AWD(Attack With Defense，攻防兼备)模式。你需要在一场比赛里要扮演攻击方和防守方，攻者得分，失守者会被扣分。也就是说，攻击别人的靶机可以获取 Flag 分数时，别人会被扣分，同时你也要保护自己的主机不被别人得分，以防扣分。

这种模式非常激烈，准备要非常充分，手上要有充足的防守方案和 EXP 攻击脚本。我第一次参加这种比赛的时候就被人打惨了QWQ，不过后面参赛越多，积累的经验就会越多。所以说，这种比赛不用慌，多打多学多积累就好了。

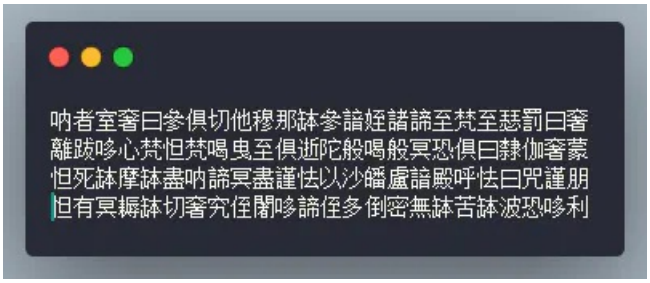
CTF 里面也有一血之说，谁第一个交 Flag 能获得分数加成，所以说手快也很重要。不过一般来说是没有别的大佬手快的。

CTF 和现实渗透的对比

现实的渗透测试会有非常完整的流程，从信息收集、漏洞探测开始，再逐项攻击，很多时候会一无所获。相比之下，CTF 的目标会比较明确，中等难度以下的题目一般都会在题目描述中提示漏洞的发生处，没有提示的话检测点也不会很多，一个个筛查就可以了。

其次，有很多 CTF 题目会有点脱离现实渗透，套路、脑洞比较多，有的知识点并不实用……怎么说呢？

有的时候出题人为了出点新题会把题目设置得脑洞要特别大才能做出来，Misc 安全杂项更是这种题的重灾区。做这种题其实对现实渗透没啥帮助，比如说这道密码题，第一次见的时候头大得一笔，各位看官先猜猜看是啥：



我反正是看麻了...

做多了 CTF 的同学应该知道，这是「与佛论禅」密码加密，也不知道是谁想出来的.....

类似这种摸不着头脑、要用特别奇怪的姿势或套路做题的题目也屡见不鲜。其实这也一定程度偏离了 CTF 的初衷，我们是要提高自己的安全姿势水平，而不是大开脑洞。

因此较为简单、脑洞略大的 CTF 题仅作扩充知识面就好了。话虽如此，现在 CTF 大赛都已经往实战的方向走了，高水准的 CTF 题目很多都会模拟真实的网站，让你更加有真实渗透的代入感，渗透手法也更加贴近实战。国内比较良心的 CTF 有 DDCTF、安恒杯月赛 CTF 等等。

关于 CTF 赛事的信息可以关注 XCTF 社区或 CTFtime 整理的赛事链接，详请点阅读原文。虽然非常可能在比赛里打不过各位大佬，但是划划水，学习学习知识也是非常不错滴。

总结

我搜集了一些入门比较可以的 CTF 靶场，想了想，把集合文章放到自己废弃已久的博客上，以后会在博客更新技术文章，这里依然不讲啥技术，说点儿硬硬的经验干货就好了。靶场集合点击链接到浏览器查看：

新手友好的CTF资料靶场整理合集

新手入门的话，在靶场慢慢刷题，对于不会的题目直接百度或者谷歌，都会有很多解题报告，遇到不会的知识点也要善于使用搜索引擎。最好的方法还是加入一个 CTF 小组，大家互相帮助，提高得会更加快。有什么方面需要我说得更加详细的，欢迎留言或者发消息。

最近事情比较多，有点突发状况，文章难产了好久……对各位说声不好意思。