第一次参加CTF线下比赛的三剑客，都经历了....

原创

破壳野生喵 于 2019-10-08 03:28:06 发布

> **前言**
> 赛事名称：第三届广东省强网杯
> 参赛人员：破壳学员-罗（我）、破壳学员-香、破壳学员-白
> 单纯给大家分享第一次参加ctf线下比赛的过程以及总结的经验

启程：深圳-广州

21日的下午2点，因为日常拖延症，不到最后一刻绝不妥协的我匆忙装好我的小电脑和一套换洗衣服就往火车站冲，地铁上给破壳随同的兄弟发微信问他啥时候到火车站集合，结果这位大兄弟说**俺受伤了去不得**，当时我立马就不乐意辽，不过我也不是什么小心眼的人，**只要带着小小的诚意道歉，并发出红包领取邀请，就能缓解我心头的怒气。**（钱能解决的事咱就学会不逼逼，何况旁边的位置上还变成了一位小姐姐）

深圳到广州的车时也就1小时左右，四点半就到广州东站了，手机电量仅剩20%的情况下不慌不忙的**荡**到酒店，期间，等公交时候因为手机没电不敢多玩，只能**尽情的欣赏大学城附近的风景**小姐姐，终于历经3个小时的折腾，在晚上6.30左右抵达酒店，躺在床上那一刻，手机刚好就“睡着”罢工辽！

赛前准备：三剑客汇合

我和阿里大佬-香在酒店提前面基成功，不适南方气候的**小白被导航骗去乘船**，所以到酒店的时间有点儿晚，与小白成功汇合之后，就在酒店附近吃了个便饭就回房间商量准备明天比赛的事情了，由于我和阿里大佬-香是**第一次参与CTF的线下比赛**，完全莫得经验，跟其他人比起来我俩碎的掉渣，只能乖巧的在赛场当**吉祥物**，不过，临时抱佛脚的态度还是要有的，之后便在**酒店抱着电脑，冲着50K/S的浪，疯狂的找资料学习**

比赛过程：应急响应-WAF

早上天还没亮，公鸡的鸣叫声还被掐在喉咙里，我们三剑客就起身前往比赛现在-广州大学城体育馆，进场后第一件事就是**签到领队服**，队服是蓝色的，嗯，很符合安全的调调。随后仔细一看场内的比赛场地，瞬间**感受到了电视剧&现实的差距**，没有电竞椅，没有360°全损音效的大耳机，只有一排排冷冰冰并且让我仿佛回到**高中时代的学生课桌椅**，不过丝毫不影响我们的心情，毕竟**技术才是硬核**...

过了一会儿，比赛总算开始啦，上半场比赛内容是关于应急响应的，事中题是有两道选择题，事后题是九道实操题，凭我的好记性，依稀还记得些许题目， ①判断黑客正在用什么手法攻击 ②怎么样防御 (大概这意思)，由于我们经验不足查日志查了几条看到都是正常的百度访问就没有看下去了，然后就**随便蒙了个文件上传漏洞，结果出错了**，心里想着那就在蒙一个，结果提示一**道题只能提交一次答案！！！**

至于第二题我们寻思**万事上waf应该没毛病，结果又悲催了**(泪了.jpg)。由于前面太浮躁丢了很多分，不过没关系，再经过总结&深呼吸缓解情绪之后，我们逐渐变得**越来越稳**，开始对题目细究，发现有几题还是相对比较简单的，打算从查找黑客webshell的文件名和黑客放的挖矿程序目录和挖矿的钱包地址这两题入手，比赛过程中有个**比较刁钻**的题是让我们找到黑客创建的一个root权限的用户，我们cat /etc/passwd文件，发现有个叫demo0的用户，觉得就是它了！**demo0这个臭弟弟**，没想到提交后，发现不对，我们带着不甘的心情一遍遍的尝试，结果把五次提交机会给用完辽，事后总结才发现有两个mysql用户，细看才发现一个是**mysql**一个是**mysq1**(这是数字1！你品，你细品)，总之比赛进行到这里时，我们三还是保持着探索知识的动力。

接下来在做查黑客登录ip和黑客登录时间这一题时，**因为早上没吃早餐就去比赛所以记性有点不好，忘了命令**(借口，还不是因为不会)最后我们以第**名结束了上半场的比赛。（我是不会告诉你们的！）

比赛结束后，终于得到解放了，那一刻只想好好犒劳我饿了一早上**叽里呱啦叫的肚子**，带着这份饥饿感，我终于领到了贴心主办方准备的盒饭（饭量大的我，没饱），一顿乱造之后，趴在专用的学生课桌椅上休息，准备迎接下半场的AWD的比赛

下半场**比赛并没有因为我的困意延迟开始那么几分钟，就这么无情开始了**，我们怀揣着满满的信心，决定采取防守策略，开局30分钟是服务器加固阶段，当然最先想到的是上**waf**，在**check**机制允许下，**waf**无疑是一个大杀器。但是不知道为什么只要**include**，网页就报错。于是就放任不管**waf**了，开始找弱口令这些。这次比赛每支队伍要运维三台服务器，两台**web（PHP，python）**一台**PWN**。

我们没有二进制，果断放弃**PWN**，看了一下**python**站点，觉得没接触过，也没自信就放弃了。主要搞了**PHP**那台服务器，首先需要检查弱口令，**SSH**弱口令和后台弱口令，通过**SSH**弱口令我们控制了两台服务器，并且后期帮他们修复了漏洞，这样这两台机器我们就一直能拿他的分数。

最后通过日志看流量，发现**check**机制其实就是检测网页是否还在，不过中间出现了**system**命令，不知道是不是也是**check**。

在开局我们就上了防护，文件保护功能，这样不会被人上马。但是忽略了隐藏的后门文件**.1ndex.php**，之后看流量发现了这个文件，果断删除。通过流量分析还发现首页报错注入，但是大佬们混淆了流量，再仔细看看了看才发现需要两条**payload**组合才能拿到**flag**，不得不佩服。果断修复这个漏洞。

就这样一轮一轮的分数又加又减的，最后一轮小白提了个好建议就是把手上现有的机子网站或者服务关闭，这样其他队伍就会被裁判组扣分，排名就更稳了，最终以**名结束了第二场的**AWD**比赛。

END：广州-深圳

比赛告一段落了，在广州-深圳的火车上，看着窗外思考，虽然比赛没能拿到满意的成绩，但也是意料之内，我们三个接触网络安全仅仅1年时间，**安全领域还有更多知识需要我们不断去探索学习，保持热情才是关键。**强网杯今年的奖励是第一名CISP-PTE，第二名是CISM，第三名是NISP一级，挺好，心里默念，以后，我一定会带着我并肩作战的兄弟一起把奖品拿回来的，**毕竟，我还小，我年年18岁！**

在这个年纪坚持自己热爱的事物，并且有着一群小伙伴一起做这件事，还有什么比这更美好的呢？

———更多精彩内容回顾———

01 Pockr安全学习地图

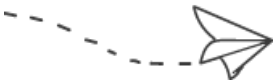
02 Ubuntu内核提权（CVE-2017-16995）漏洞的复现&脏牛漏洞

03 WEB安全-端口转发

04 DVWA SQL Injection分析及刷洞技巧

05 WEB安全——rsync&tomcat漏洞

06 如何挖信息泄密漏洞



破壳学院

个性、有趣、好玩，魔鬼陪伴式的白帽黑客技术在线教学平台