研究生创新联盟高校网安大赛经历分享

主讲人：齐划一
计算机学院 2020 级研究生

qi@huayi.email

目录

01

竞赛简介

三省教育厅联合举办的 CTF 比赛

CTF

CTF：夺旗赛，Capture The Flag。

1. 解题模式 - Jeopardy
根据题目提供的可执行文件、资源文件或沙盒环境，通过各种手段，获取形如 flag{xxxxxxxxx} 的秘密字符串。前三名解题成功的小组将得到额外加分。为防止作弊，解题成功后，必须在截止时间之前编写解题步骤（write-up），否则成绩无效。
比赛时不能联网，需提前自行在电脑里准备各种各样的工具。
题型包括：Windows/Linux/Android 程序逆向、Web 漏洞、密码算法、隐写等。

2. 攻防赛 - Attack With Defense
每组拥有一个沙盒环境，需保证环境中的服务保持正常运行，并同时防止敌手骇入环境取得秘密值。比赛时不能联网，需提前自行在电脑里准备各种各样的工具。
在本次竞赛中，AWD 环境运行了一个具有多个漏洞的 PHP 网站。攻防赛持续约 3 小时左右，初始分数为 700 分左右，每 10 分钟检查一次服务状态并更新各个沙盒的秘密值。若某组的秘密值遭到泄露，扣 10 分，提交该秘密值的攻击者加 10 分。若某组的网站宕机，扣 100 分，这 100 分将平均分给在场的所有存活网站。

另请参阅
https://ctf-wiki.org/en/introduction/mode/

研究生创新联盟高校
研究生网络与信息安全技术大赛

分为初赛和决赛。

报名：学校网站通知，辅导员转发。每支队伍最多 3 名同学，另需 1 名指导教师。
https://www.ygb.sdu.edu.cn/info/1011/7994.htm

初赛：本次为线上举行。分为河北、天津、山东赛区，每个省份取前 12 支队伍晋级。内容为网络安全基础知识选择题 + 解题模式。

决赛：线(gong)下(fei)举(lv)行(you)。两整天，上午开幕式，下午解题模式，上午攻防赛，下午颁奖典礼。主办方只管午饭，但会帮助各参赛队伍协助预订酒店，住宿费和交通费由参赛学校自行解决。

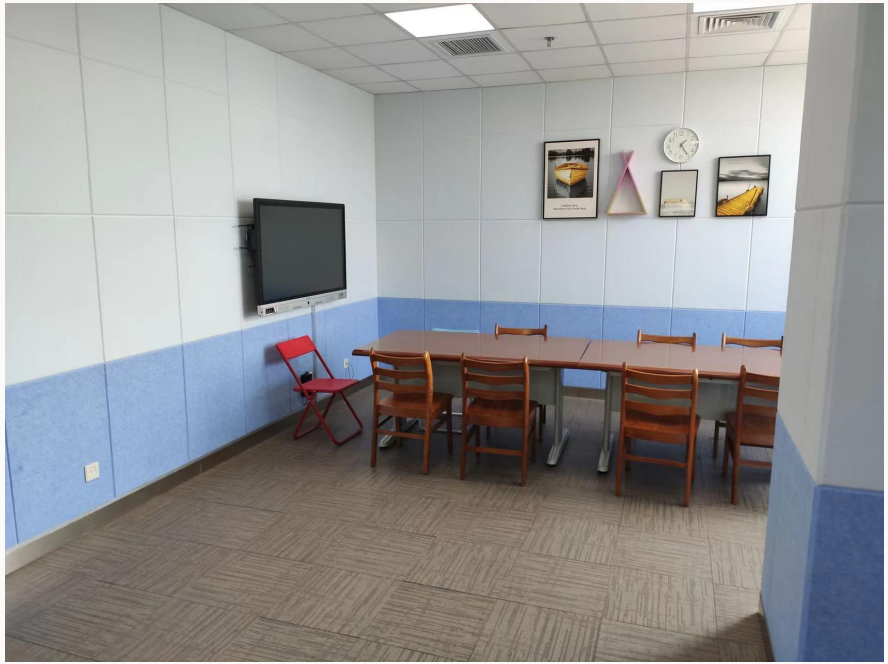
注：通常而言，主办单位只要比省级大，就算做全国级竞赛。

02

比赛经历

简单准备 + 随机应变

线上初赛



预约了青岛校区图书馆的研讨室。

整个下午一直处于紧张状态，晚上吃饭时直接吐了出来（似乎是饭馆不太卫生）。

自带电脑、插线板、纸笔等。对于网络，通常而言学校无线网络已经可以满足要求，但也要自备流量热点以防万一。

准备决赛

正常情况下，初赛结束后一个月左右即进行决赛。
我们队伍**此前从未参加过** CTF 竞赛，因此进行了如下的准备工作：

7月4日 新开这本日记，也为了督促自己下个学期多下些苦功。先要读完手边的莎士比亚的《亨利八世》。
7月13日 打牌。
7月14日 打牌。
7月15日 打牌。
7月16日 胡适之啊胡适之！你怎么能如此堕落！先前订下的学习计划你都忘了吗？子曰：“吾日三省吾身。”不能再这样下去了！
7月17日 打牌。
7月18日 打牌。

由于疫情原因，决赛推迟到了下个学期，此时已经有一些队伍无法重新集结，缺员参赛。

决赛前夕

本次决赛地点在河北大学举行。火车站周围有很多黑车，被宰了一笔。

山大的报销标准：学生人均住宿不超过 300 元一日，非常宽松了。
主办方提供了两种酒店房型：双人间和单人间，价格相同，含早晚餐。
作为男生，果断选择了单人间，同组的两个女生选择了双人间。
到了现场才发现，双人间的设施豪华一些，有额外的沙发、茶具等，适合团队活动。

周围有一些小公园和商场，比较有生活气息，许多居民在散步、跳舞、打太极。

决赛第一天

解题模式。

有两道题属于入门难度，其他题目难度不尽相同。由于各个队伍准备都不太充分，比赛进行到一定时间时，主办方对入门难度的题目进行了比较细致的提示。

工具还是带得不全，有一道题目的第一步需要解析二维码，而这个……谁会想到准备这个玩意儿？许多队伍没有二维码的解码工具，主办方直接提供了二维码的解析结果。

随手编写 Python 代码进行各种计算，解决 Textbook RSA 算法解密以及解多元方程组的需求。

不太擅长逆向题目，直接跳过。

我们队伍在解题模式的总体成绩一般，大约只能在三等奖的程度。此时队伍信心已经降低，不过好在没有放弃第二天的比赛。

决赛第一天

01
02
03
04
05
06

决赛第二天

攻防赛。

从未接触过攻防赛，现场摸索。好在对于 Linux 服务器有一定的管理经验，能够编写简单的 bash 脚本做一些基础的自动化工作。沙箱环境不提供 root 权限，因此一些防御手段无法使用。

比赛刚刚开始的一两分钟时间内，就有几支队伍使用了预先准备好的脚本对所有队伍的沙箱环境展开攻击。而超过一半的队伍还处于完全蒙逼状态，包括我们。每 10 分钟，这些被攻击的沙箱环境就会泄露秘密值并扣 10 分，但没有任何一个环境被攻击到宕机。

正面打不过，只用计谋：

- 哪怕 3 小时内产生的秘密值全部遭泄露，也只不过扣 180 分，而一旦沙箱被攻击到宕机，每次都会扣 100 分。因此把目标放在防止宕机上。
- 没有队伍宕机，**不是因为敌手做不到**，而是因为暂时不想做。窃取秘密值是利己行为，宕机则利好所有存活队伍，因此敌手**应当会在比赛的后半阶段**展开宕机攻击。

决赛第二天

正面打不过，只用计谋：

- 哪怕 3 小时内产生的秘密值全部遭泄露，也只不过扣 180 分，而一旦沙箱被攻击到宕机，每次都会扣 100 分。因此把目标放在防止宕机上。
- 没有队伍宕机，**不是因为敌手做不到**，而是因为暂时不想做。窃取秘密值是利己行为，宕机则利好所有存活队伍，因此敌手**应当会在比赛的后半阶段**展开宕机攻击。
- 敌手已经在我方沙箱环境中植入木马，但我方技术手段有限无法彻底清除。PHP 漏洞亦无能力修复。但**还是有一件事情是可以做的**，编写脚本，每 0.1 秒搜索并结束可疑进程，赌敌手木马无法在 0.1 秒内接收并执行宕机命令。
- 借力打力，最后一个小时，敌手果然展开攻击，大量服务器宕机，我方幸免，因此平分了受攻击服务器的分数，排名不低。

比赛结果

二等奖：每人一个联想移动固态 128 GB，TU100 Pro

没有一张正经的

03

感想寄语

正确对待竞赛

不要将重心放在竞赛上

- CTF 竞赛考察的往往是成熟的（过时的、陈旧的）知识，与研究生阶段的科研工作不符，例：
  - 加密算法考察 Textbook RSA 等简单算法，而不是椭圆曲线等更先进的算法。像属性加密、可搜索加密等科研相关的内容不可能也**不适合**出现在竞赛中。有时候需要被迫关注古典密码等无任何实际研究价值的算法。
  - 选手需掌握一些过时漏洞，并花费时间在旧版本 PHP、一些过时组件上。具体要研究哪些内容，**跟着考题走**，通常不是最前沿的技术，可能能够弱化主观能动性。
- CTF 竞赛要求选手准备很多专用工具，**比赛经验决定了成绩**，需要通过不断刷比赛积累比赛经验。这会消耗大量时间用于学习“套路”。
- 注：参与 CTF 竞赛也会带来很多积极方面的影响，此处未列举。

- 如果你的目标不在于科研或编程，有没有证书对你很重要，则可无视以上内容。

Thanks!

Do you have any questions?

Contact me at: qi@huayi.email （齐划一）