长亭科技
CHAITIN.CN

CTF与安全人才培养

陈宇森
北京长亭科技有限公司

长亭科技
CHAITIN.CN

WHO AM I

- 陈宇森 D3AdCa7 / ADoG
- 毕业于浙江大学竺可桢荣誉学院
- 长亭科技联合创始人，blue-lotus 成员
- 国内大量 CTF 冠军
  - 最近的有ZCTF线下决赛冠军
- DEFCON CTF FINALS 全球第五
- 擅长 Web安全 与 渗透

长亭科技
CHAITIN.CN

“

如何借助 CTF 中学到的知识在信息安全领域中探索前行

— 从自身经历说起

”

长亭科技
CHAITIN.CN

大家的心得体会

- 你最早接触CTF是在什么时候，觉得CTF对自己在安全方面的学习有怎样的帮助？
- 为什么CTF能给你带来这么大帮助？
- 什么样的CTF是有价值的，可以帮助学习信息安全知识的？
- 给现在的高校信息安全课程提一些建议。

长亭科技
CHAITIN.CN

受访对象1

- 杨坤
- 清华大学网络与信息安全实验室博士生，北京长亭科技有限公司首席安全研究员及联合创始人，美国加州大学伯克利分校访问学者
- 带领长亭科技的研究团队在硬件破解大赛GeekPwn上攻破多款设备，获得一等奖，入选GeekPwn名人堂
- 作为蓝莲花战队队长，带领战队连续三年闯入DEFCON CTF全球总决赛，成为中国历史上的首次突破
- 主要研究软件漏洞挖掘和利用技术

长亭科技
CHAITIN.CN

受访对象1

- 我是从**4年前**开始打CTF，当时我在读研究生一年级。我在本科阶段学习的是电子和通信方向的专业，没有接触过信息安全，完全不了解什么是漏洞和攻防，完全是怀着好奇心选报了安全方向的研究生，而且清华的信息安全课程非常少。**打了几次CTF后，我很快就理解了信息安全领域中漏洞是怎么一回事，漏洞是怎么产生又是怎么被利用的，并一下子被攻防技术中的趣味和魅力所吸引。**

- 后面的事情大家都知道了，我跟着蓝莲花打了4年CTF，也取得了一些成绩。可以说**CTF为我打开了信息安全领域的大门**，培养了我的兴趣，锻炼了我的技术能力。

长亭科技
CHAITIN.CN

受访对象1

- 首先，**CTF题是信息安全基本概念、攻防技术、技巧的浓缩和提炼**。通过解题，你会快速掌握题目中所包含的概念和技术点，而这些知识在真实环境中可能比较分散、难以学习。高水平CTF都是由业内专家命题，往往凝聚着他们多年积累出来的技能。

- 其次，**CTF题注重实际操作，并与基础理论知识相结合**。每道CTF都需要实际动手才能找到答案，而且在比赛中经常要拼速度，这对攻防实操的能力会有极高的锻炼。除此以外，高质量的CTF题都没法直接使用现成工具解出，一般需要在理解基本原理的基础上，自己编写代码来求解，这个过程会加深和巩固计算机基础知识的理解。

- 最后，**CTF是在不断变化进步的**。计算机技术日新月异，攻防技术也会随之不断升级，高质量的CTF往往会跟进这些变化，在赛题中融入新的领域、新的技巧，让参赛者每次都能学到新东西。

长亭科技
CHAITIN.CN

受访对象1

- 首先要**参加符合自身技术水平的CTF**，不能参加难度过高或者过低的比赛。目前CTF水平差异较大，直接参加高于自身技术过多的竞赛犹如空中楼阁，不仅很难学到东西，也可能会打击自信；参加过于简单的CTF会浪费时间。

- 其次，**有趣**的题目会激发大家的积极性，带动大家的兴趣，尤其对于刚入门的参赛选手。乏味的题目会起到副作用，例如包含过多的猜谜语或者暴力破解的题。

- 再补充一点，题目所**考察的技术具有一定通用性和代表性**的题会对选手提高非常有帮助。如果能通过一个CTF题，学到一个很广泛使用的技术，那这个题的价值就会非常高。

长亭科技
CHAITIN.CN

受访对象1

- 建议老师在讲授信息安全课程理论知识的同时，也**采纳CTF形式的实验来给学生练习**，这样就可以充分地把CTF的优势发挥到常规教学中来。

- 另外，在课程的班上可以**组织大家组队参加CTF竞赛**，让学生吸取课堂以外的知识，这些学生成长起来后，又可以帮助老师改进课程的实验，形成良性循环。

长亭科技 CHAITIN.CN

受访对象2

- 何淇丹(Flanker)
- 毕业于浙江大学和香港科技大学，腾讯科恩实验室(原KeenTeam)高级安全研究员，主要研究方向为*nix(Android, iOS, OSX)平台Sandbox Bypass和内核安全
- 曾在BlackHat, CanSecWest, HITCON, QCon, xKungfoo等安全会议上做技术演讲
- 2016年Pwn2Own OSX项目冠军，2015年GeekPwn攻破奇酷手机，谷歌Android安全名人堂俱乐部成员
- 在学生时代也是CTF爱好者，蓝莲花战队早期成员，随队打入2013年DefCon全球总决赛

长亭科技
CHAITIN.CN

受访对象2

- 我在2011年就接触了CTF这种比赛形式，那时候国内比赛很少，题型比较狭窄，也远远没有现在这么火爆。
- 后来随着蓝莲花的成立，我加入蓝莲花接触到了国际比赛，才认识到了applied security的真正形式。
- 相对于传统的学科书本教学形式，CTF能很好地寓教于练，一场好的比赛、好的对手、好的题目令人受益匪浅。

长亭科技
CHAITIN.CN

受访对象2

- 通过CTF能锻练头脑，磨砺基础，快意人生，认识了很多志同道合的朋友和同学，在成为专业安全研究从业人员的道路上助力颇多。

受访对象2

- 必须要指出的是CTF作为竞赛的一种形式，**除了DEFCON等顶级赛事之外，离工业界实际的攻防研究还是有一定差距。**一个明显的问题是以二进制安全研究为例，**实际的安全研究**需要对目标系统或应用（例如各大浏览器、操作系统）**长年累月的积累和耐心**，而这些因为门槛过高很难在目前这种短期限的CTF中表现为明确的题目形式，这需要出题者有高超的水准。

- 不过竞赛也自有竞赛的魅力。从我个人角度来讲，我觉得好的CTF是既能让参与者学到新知识，又在一定程度上贴近实战，深入考察计算机科学的相关知识而不流于偏门的屠龙之技或雕虫小技，同时又不失竞赛本身的难度和思维挑战的乐趣，能让人有恍然大悟相见恨晚之感。要给目前火热的行业泼一盆冷水的是，**忘为赛而赛。**

受访对象2

- 高校的信息安全课程应注重学生**计算机科学基础的扎实培养**，例如操作系统、编译原理、计算机组成、汇编语言和各门基础编程语言的学习。在此基础之上开设相关系统安全和应用安全的课程。

- **同时避免走过于理论和过于实践两个极端**。高校课程应培养安全研究员而不是安全民工。过于理论的代表案例就是只知密码学（不是说密码学不重要，而是说不能只学密码学）、合规条例而不了解真正的工业界安全内容。过于实践的代表就是让学生过早接触一些渗透案例，结果基础不扎实的情况下只知其然而不知其所以然，沦为安全民工。

- **一个合格的安全研究员应首先是一个合格的计算机科学工程师。**

受访对象3

- 许文

- 上海交大ACM班大四学生，交大LoCCS实验室成员，CTF战队0ops的创始人之一

- 平日里热衷于和队友们参与各类CTF比赛，并组织一年一度的OCTF大赛

- 同时承蒙KeenLab(前KeenTeam)各位前辈的厚爱有幸跟随做了近两年的实习研究，接触到了前沿的二进制漏洞研究技术并积累了一些经验和成果

- 毕业后选择前往佐治亚理工学院攻读博士学位，继续从事二进制安全领域的研究工作

长亭科技
CHAITIN.CN

受访对象3

- 3年前
- CTF带我入门安全领域，激励我在安全研究的道路上不断前进
- 更重要的是，让我有机会去结识、请教许许多多安全领域的大牛们甚至能够与他们共事。

长亭科技
CHAITIN.CN

受访对象3

- 中低难度的CTF比赛帮助我较为平缓入门安全研究领域
- 高难度的CTF比赛时间短、节奏快、涉猎广的特点非常好地磨练了我的安全技术水平。
- 通过CTF比赛更是帮助培养了团队协作意识，丰富了知识面的同时也扩展了朋友圈。

长亭科技
CHAITIN.CN

受访对象3

- CTF比赛的**目的**决定了它的游戏形式、题目难度与整体导向。
- 在我看来，目前所有的CTF比赛都有其受众的群体。
- **各个水平、以及行业层次**的安全研究人员都可以找到能够帮助他们学习信息安全知识的CTF比赛。
- 为了能够有更强的竞技性以及趣味性，no guessing是非常重要的一点；与此同时，**跟进最先进的安全攻防技术**也必不可少。

长亭科技
CHAITIN.CN

受访对象3

- 高校信息安全课程需要开设一些更为贴近实际攻防应用的课程，这方面国外的信息安全强校给出了很好的示范案例。

- 与此同时，高校的信息安全学院要花更多的时间培养院系学生在CS领域的基本功，从长远来看，学生本身扎实的学科基本功才是奠定未来成功的基础。

一些现状

- 我国高校信息安全课程和工业界的需要有一定的脱节。
- 相较于3年前，目前主流CTF的难度越来越高，特别是对于刚刚入门的选手而言，很容易让人望而却步。

长亭科技
CHAITIN.CN

一点想法

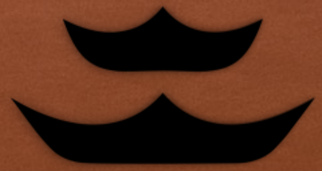
- 公司与高校的课程合作
  - 介绍业界前沿信息
  - 设计贴近实战、更加有趣的实验课程

长亭科技
CHAITIN.CN

一点想法

- 「Wait To Be Named CTF」for beginners
  - 对标CSAW
  - 有趣
  - 难度不高
  - no guessing

THANKS



长亭科技
CHAITIN.CN