# CTF如何入门

原创

虎不归 于 2017-04-22 11:34:05 发布 21915 收藏 59

分类专栏： 旧文 文章标签： CTF 学习笔记



本文链接：https://blog.csdn.net/hubuguia/article/details/70399108





## 声明：文字整理自i春秋课程，感谢视频作者幻泉分享。

## 题目类型

- Web
- Crypto
- PWN
- Misc
  - stego
  - forensic
  - …
- Reverse
- PPC(Professonal ProgramCoder)

国际比赛：DEFCON资格赛

国内比赛：XCTF联赛

## 打CTF的意义

- 思维能力
- 快速学习能力
- 技术能力
- 如何入门
- 编程语言基础（C语言、汇编语言、大部分脚本语言）
- 数学基础（算法、密码学）
- 脑洞大开、并落地（天马行空的想象、推理解密）
- 体力耐力（通宵熬夜不睡觉，学习新技术、突破难关，结果不重要，过程很重要）

## 如何学

- 恶补基础知识
- 从脑洞开始
- 从基础题出发
  - 单、双点知识
- 学习信息安全专业知识
- 锻炼体力耐力

  学之前的思考

  分析赛题情况

  - Crypto偏重对数学、算法的学习
  - Web偏重发散思惟、对技巧沉淀、快速搜索能力的挑战，漏洞点几类
  - Misc则更为复杂：隐写类、图片数据分析、数据还原、流量分析、大数据

  分析自身兴趣

  - PWN+Re+Crypto随机搭配
  - Web+Misc组合
  - 精力有限先从一两个方向做起
- 如何恶补知识
  - linux、组原、OS、网络协议分析
  - 二进制：IDA工具使用，f5插件、OD、逆向工程、密码学、缓冲区溢出

  推荐书籍

  - RE for Beginners(逆向工程入门。德国)
  - IDA PRO权威指南
  - 揭秘家用路由器0day漏洞挖掘技术
  - 自己动手写操作系统
  - 黑客攻防技术宝典：系统实战篇
  - web：网络安全、内网渗透、数据库安全、OWASPTOP10
    - 推荐书籍
      - Web应用安全权威指南，日本Lab.Lab.实现

- Web应用安全权威指南。日本！！！宏观
- Web前端黑客技术揭秘——总结、吃透则直线上升、核心技术点都包含
- 黑客秘籍-渗透测试使用指南
- 黑客攻防技术宝典：web实战篇
- 代码审计：企业级web代码安全架构

如何成为一个赛棍

从基础题目出发

- http://ctf.idf.cn idf实验室，非常基础，单点知识，挫败感较小
- www.ichunqiu.com 线下线上题目复现
- http://oj.xctf.org.cn xctf历年题目，较难
- www.wechall.net/challs 非常入门的国外CTF 入门网站 国内安全大牛出发点，可首选
- http://canyouhack.it 非常入门，涉及一些移动安全
- http://microcorruption.com/login 很酷炫，游戏化，二进制方向
- http://smashthestack.org/ war game 非常简洁的内容 ssh连入即玩
- http://overthewire.org/wargames老牌wargame,国内资料较多，WP: http://drops.wooyun.org/author/litao3rd
- http://exploit-exercises.com 老牌wargame，国内资料较多
- http://pwnable.kr/play.php 100题左右，较基础
- http://ctf.moonsos.com/pentest/index.php web安全核心技术点
- http://prompt.ml/0 xss 国外测试平台,不考核对错，自己尝试
- http://redtiger.labs.overthewire.org sql注入挑战赛

工具

- burp、ida
- https://github.com/truongkma/ctf-tools
- https://github.com/P1kachu/v0lt
- https://github.com/zardus/ctf-tools
- https://github.com/TUCTF/Tools

以练促赛、以赛养练：都参与，不在乎名次，看多个WP，对比，重视思路，复现过程，寻找相关题目。

- 以练促赛：选择一场已经存在WP的比赛
- 以赛养练：参加一场最新的CTF，名次不重要，赛后要吃透，猜测作者怎么想，跟着作者想法走
  - https://ctftime.org/ 国际比赛
  - http://www.xctf.org.cn/ 国内比赛

## 如何组建团队

强力成员画像

- 思维跳跃：灵活、不钻牛角尖
- 专注：遇到问题不放弃直到解决
- 耐力：可以一昼夜不睡觉地研究技术
- 团队精神：责任、凝聚（相信将来总会得第一）、分享（先富带动后富）
- 有以上三条为强力成员，四条可为队长

组建团队要解决的问题

- 新人招募：如何评判新人潜力
- 队员培养：如何快速培养队伍能力
- 梯队有序：如何建立梯队层级
- 纪律严格：如何拒绝无团队精神的成员