信息安全竞赛入门

AssassinQ

课时安排

- 信息安全竞赛入门+CTF比赛进阶（共30课时）
  - 星期二下午1:40～4:15
  - ？ 星期六or星期天 上午or下午or晚上

课程要求

- 每节课自己带电脑来
- 课后写博客记录所学的知识
- 每三个人组成一支队伍（四个也可以）

考核标准

- 每节课结束后签到
- 第五次课和第十次课进行考核，考核形式是打比赛，比完赛之后每个人写下解题报告，以队伍的形式发给我

- 关于信息安全竞赛
  - 作品赛：比如密码学竞赛，之后的课会有学姐给大家分享一些比赛经历
  - 实践赛：比如CTF，信息安全小组主要参加的比赛，国内比较正式的有XCTF、国赛、西湖论剑等，省内有省赛


WHAT IS A CTF?

CTF 的起源

- CTF（Capture The Flag，夺旗赛）起源于 1996 年 DEFCON 全球黑客大会，是网络安全爱好者之间的竞技游戏。
- CTF 的前身是传统黑客之间网络技术比拼的游戏，起源于 1996 年第四届 DEFCON。

DEF CON × 百度安全

DEFCON β

CHINA

DEFCON CHINA 发布会

DEFCON CHINA RELEASE CONFERENCE

时间：2018 年 2 月 12 日　地点：中国 · 北京

早期 CTF 竞赛

- 最开始的 CTF 比赛（1996 年 - 2001 年），没有明确的比赛规则，没有专业搭建的比赛平台与环境。由参数队伍各自准备比赛目标（自己准备的比赛目标自己防守并要尝试攻破对方提供的比赛目标）。而组织者大都只是一些非专业的志愿者，接受参赛队伍请求手工计分。

- 没有后台自动系统支持和裁判技术能力认定，计分延迟和误差以及不可靠的网络和不当的配置，导致比赛带来了极大的争论与不满。

「现代」CTF 竞赛

- 由专业队伍承担比赛平台、命题、赛事组织以及自动化积分系统。参赛队伍需提交参赛申请，由 DEFCON 会议组织者们进行评选。
- 就 LegitBS 组织的三年 DEFCON CTF 比赛而言，有以下突出特点：
  - 比赛侧重于对计算机底层和系统安全核心能力，Web 漏洞攻防技巧完全不受重视。
  - 竞赛环境趋向多 CPU 指令架构集，多操作系统，多编程语言。
  - 采用「零和」计分规则。
  - 团队综合能力考研：逆向分析、漏洞挖掘、漏洞利用、漏洞修补加固、网络流量分析、系统安全运维以及面向安全的编程调试。


SmokedChicken

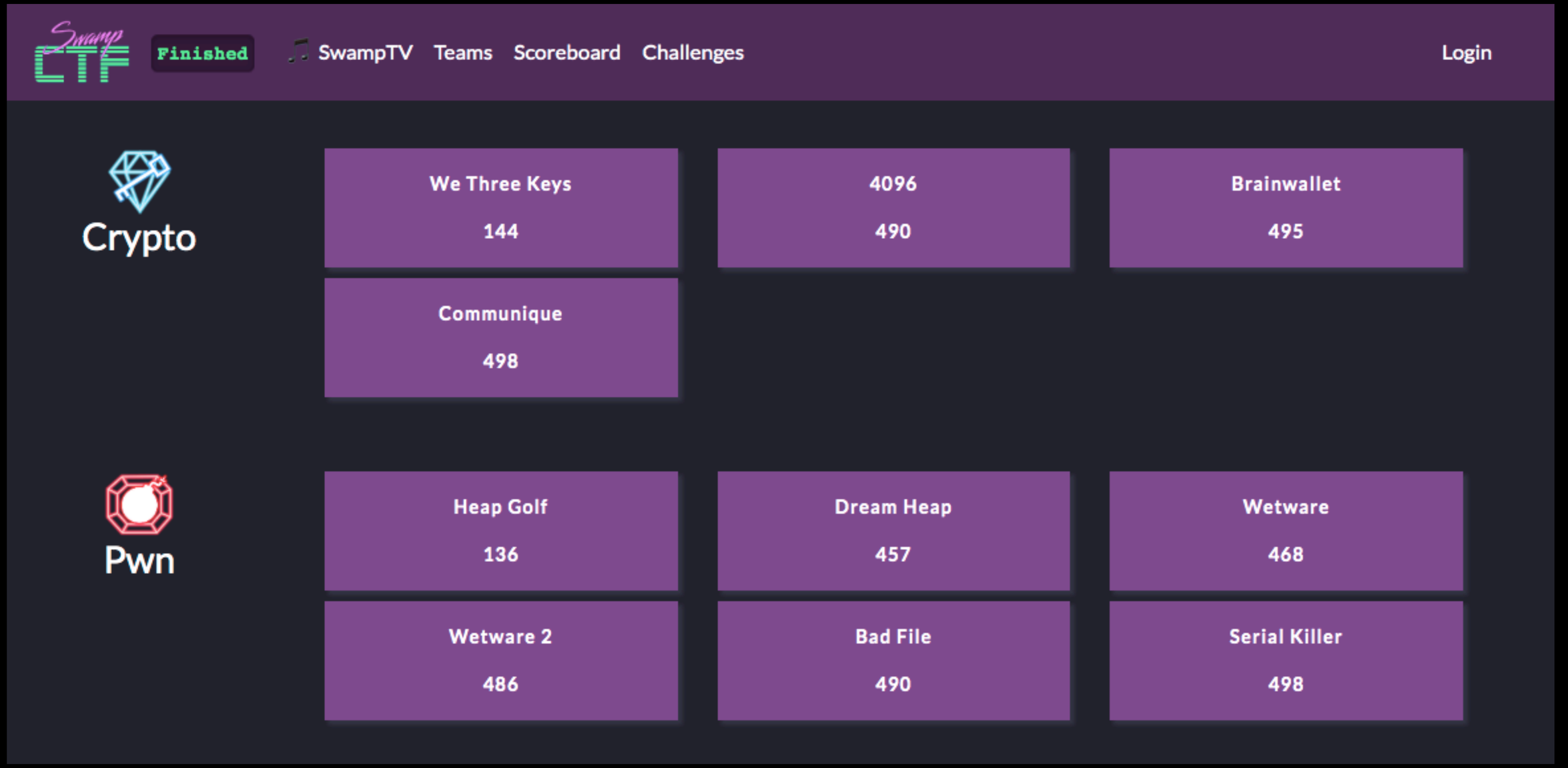
- 解题模式 - Jeopardy
- 战争分享模式 - Belluminar
- 攻防模式 - Attack With Defense（AWD）

解题模式 - Jeopardy

- 常见于线上选拔比赛。在解题模式 CTF 赛制中，参赛队伍可以通过互联网或者现场网络参与，参数队伍通过与在线环境交互或文件离线分析，解决网络安全技术挑战获取相应分值，与 ACM 编程竞赛、信息学奥赛比较类似，根据总分和时间来排名。

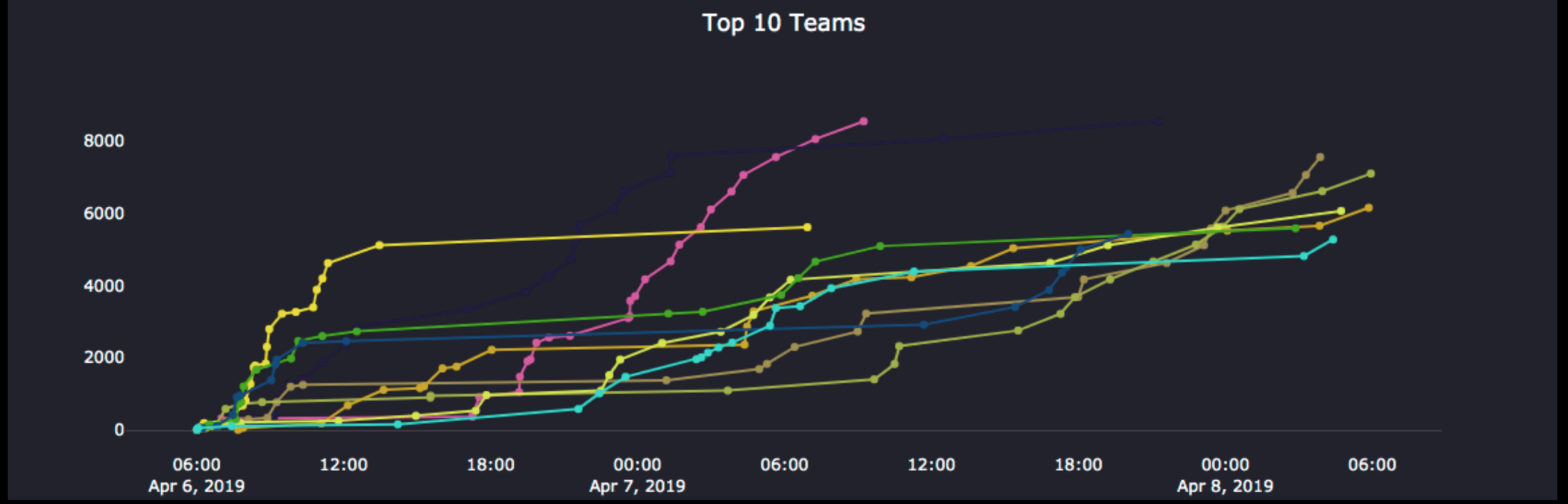
- 相不同的是解题模式一般会设置 一血 、 二血 、 三血 ，也即最先完成的前三支队伍会获得额外分值，所以这不仅是对首先解出题目的队伍的分值鼓励，也是一种团队能力的间接体现。

- 题目类型主要包含 Web 网络攻防 、 RE 逆向工程 、 Pwn 二进制漏洞利用 、 Crypto 密码攻击、 Mobile 移动安全 以及 Misc 安全杂项 这六个类别。


SwampCTF
Finished
SwampTV
Teams
Scoreboard
Challenges
Login
Crypto
We Three Keys
144
4096
490
Brainwallet
495
Communique
498
Pwn
Heap Golf
136
Dream Heap
457
Wetware
468
Wetware 2
486
Bad File
490
Serial Killer
498

SwampCTF Finished SwampTV Teams Scoreboard Challenges Login

Scoreboard



战争分享模式 - Belluminar

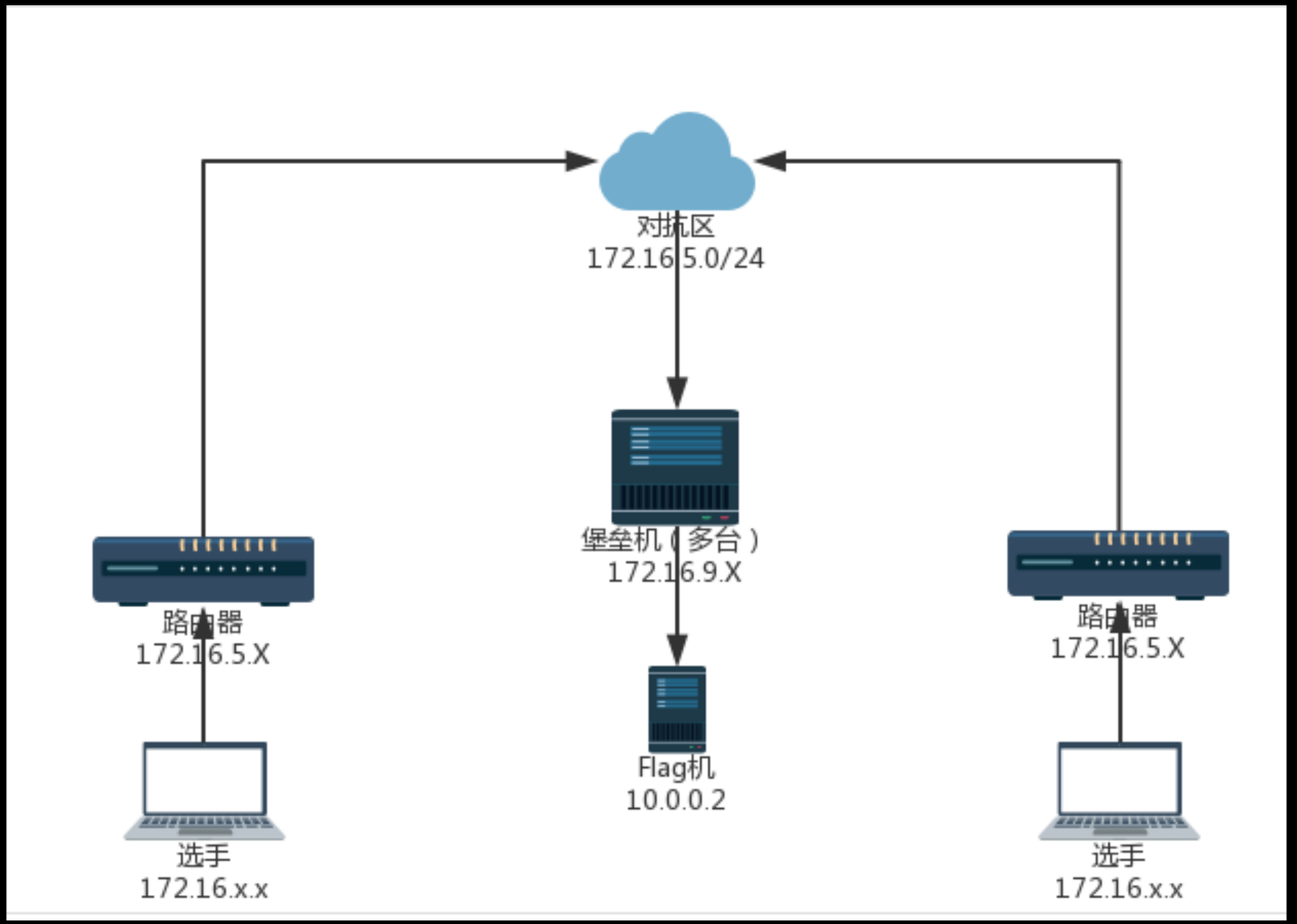
- BELLUMINAR CTF 赛制由受邀参赛队伍相互出题挑战，并在比赛结束后进行赛题的出题思路，学习过程以及解题思路等进行分享。战队评分依据出题得分，解题得分和分享得分进行综合评价并得出最终的排名。

- 比如国赛半决赛，需要各支队伍出题，不同赛区的题目打乱后分散给其他赛区的队伍做。

攻防模式 - Attack With Defense

- 攻防模式常见于线下决赛。在攻防模式中，初始时刻，所有参赛队伍拥有相同的系统环境（包含若干服务，可能位于不同的机器上），常称为 gamebox，参赛队伍挖掘网络服务漏洞并攻击对手服务获取 flag 来得分，修补自身服务漏洞进行防御从而防止扣分。

- 攻防模式可以实时通过得分反映出比赛情况，最终也以得分直接分出胜负，是一种竞争激烈，具有很强观赏性和高度透明性的网络安全赛制。在这种赛制中，不仅仅是比参赛队员的智力和技术，也比体力（因为比赛一般都会持续 48 小时），同时也比团队之间的分工配合与合作。


对抗区
172.16.5.0/24
堡垒机（多台）
172.16.9.X
路由器
172.16.5.X
路由器
172.16.5.X
Flag机
10.0.0.2
选手
172.16.x.x
选手
172.16.x.x


FIRST BLOOD
DEFKOR against 9447
rxc
DEF CON CTF 2015

环境搭建

- 浏览器：**Chrome/Firefox**
- 插件：**Hackbar/FoxyProxy**/SwitchyOmega
- Java环境配置：**Java SE Development Kit 8 Downloads**
- BurpSuite：**Burp_Suite_Pro_v1.7.37_Loader_Keygen.zip**
- PHP Study：**phpstudy2018**
- VMware Workstation/VirtualBox
- Kali Linux/Ubuntu Linux

- ctf-wiki: https://ctf-wiki.github.io/ctf-wiki/
- 实验吧: http://www.shiyanbar.com/ctf/practice
- BugkuCTF: https://ctf.bugku.com/challenges
- hackerfire: https://ctf.hackerfire.com/challenges
- 安恒月赛平台: https://www.linkedbyx.com/home
- 南京邮电大学网络攻防训练平台: http://ctf.nuptsast.com/challenges
- 东南大学SUS: http://sus.njnet6.edu.cn/challenges
- 浙江JarvisOJ: https://www.jarvisoj.com/challenges
- XCTF攻防世界: https://adworld.xctf.org.cn/

References

- https://ctf-wiki.github.io/ctf-wiki/
- https://neversec.top/20190407/%E5%95%A5%E6%98%AFCTF%EF%BC%9F%E6%96%B0%E6%89%8B%E5%A6%82%E4%BD%95%E5%85%A5%E9%97%A8CTF%EF%BC%9F.html