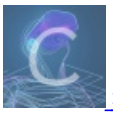
初识CTF

原创

Jensen_79 于 2019-09-13 11:20:45 发布 231 收藏 1

分类专栏： 渗透

本文链接：https://blog.csdn.net/qq_30036471/article/details/100797704



渗透 专栏收录该内容

15 篇文章 0 订阅

订阅专栏

初识CTF

赛事介绍

> 1. CTF(**Capture The Flag**)夺旗锦标赛，网络安全人员之间进行技术竞技一种比赛
> 2. CTF起源于**1996**年DEFCON全球黑客大会，以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。
> 3. 参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而夺得分数。为了方便称呼，我们把这样的内容称之为“**Flag**”。

竞赛模式

CTF竞赛模式具体分为以下三类：

- 解题模式（Jeopardy）

> 这种模式的CTF竞赛与ACM编程竞赛、信息学奥赛比较类似，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别。

- 攻防模式（Attack-Defense）

> 参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。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小时及以上），同时也比团队之间的分工配合与合作

- 混合模式（Mix）

> 结合了解题模式与攻防模式的CTF赛制，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。采用混合模式CTF赛制的典型代表如iCTF国际CTF竞赛。

CTF常见题型

> 1. `MISC(Miscellaneous)` 即为安全杂项如(解题目，流量分析，电子取证，人肉搜索，数据分析等…)
> 2. `PPC(Professionally Program Coder)` 即为算法编程，相比ACM会比较容易些
> 3. `CRYPTO(Cryptography)` 即为密码学 专门研究古典算法，以及题目各种加密算法结构
> 4. `PWN` PWN在黑客俚语中代表着攻破、取得权限，多为溢出类题目。
> 5. `REVERSE` 即逆向工程，题目涉及到软件逆向、破解技术。
> 6. `WEB` 即题目会涉及到常见的Web漏洞，诸如注入、XSS、文件包含、代码执行等漏洞。

赛事级别及练习平台

- DEFCON CTF : CTF 赛事中的 ”世界杯“
- SECCON
- XCTF 全国联赛
- 各种小赛事

> `Website`:
> **ctf赛事平台**
> https://www.xctf.org.cn
> https://ctftime.org
> **练习平台**
> 合天 http://hetianlab.com/
> 实验吧 http://www.shiyanbar.com/ctf
> i春秋 https://www.ichunqiu.com
> Xctf平台 https://adworld.xctf.org.cn/
> 蓝鲸安全 http://whalectf.xin/