

关于CTF的简介及赛题模式

原创

格子小七  于 2018-04-27 16:53:32 发布  16345  收藏 27

分类专栏: [小记](#) 文章标签: [CTF](#) [信息安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/lanyandong/article/details/80110363>

版权



[小记](#) 专栏收录该内容

20 篇文章 0 订阅

订阅专栏

关于CTF

1、CTF简介

CTF (Capture The Flag) 中文一般译作夺旗赛, 在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。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。发展至今, 已经成为全球范围网络安全圈流行的竞赛形式。

CTF竞赛模式具体分为以下三类: (解题模式 (Jeopardy)、攻防模式 (Attack-Defense)、混合模式 (Mix))

2、CTF赛题

一般CTF比赛中, 会涉及MISC, PPC, CRYPTO, PWN, REVERSE, WEB, STEGA这几种题目。

MISC 的全称是 miscellaneous 杂乱无章的意思, 其中的题目可能涉及, 流量分析, 取证, 人肉, 大数据统计等等。

PPC 是 Professionally Program Coder 的意思, 会涉及到一些简单的算法知识, 不过比ACM要简单的多。

CRYPTO 是密码学的缩写, 这一类的题目通常以破解密文为主, 加密算法有可能是古典加密算法, 也有可能是现代的加密算法, 甚至有些是出题者杜撰的加密算法。

PWN 在黑客俚语中代表着, 攻破, 取得权限, 在CTF中它代表着溢出类的题目。

REVERSE 就是逆向工程, 这个大家应该很熟悉的。破解crackme.exe就是这类题的主旋律。

STEGA是Steganography的缩写, 隐写术的意思, 这类题很有意思, flag被藏在一段视频, 一张图片, 一首音乐, 或者任何你意想不到的载体中, 也是CTF比赛中最有挑战和乐趣的一类题。

WEB 题型就是最大众化的WEB漏洞的考察了, 他会涉及到注入, 代码执行, 文件包含等常见的WEB漏洞。

3、如何开启你的CTF之旅?

CTF比赛主要表现以下几个技能上: 逆向工程、密码学、ACM编程、web漏洞、二进制练习、网络和取证。可以从中选择并关注一个你已经上手的技能方向。(Web、Pwn、RE、Mobile、Crypto)

[1]<http://www.freebuf.com/articles/others-articles/36927.html>

4、相关网站及论坛

[1] 实验吧（自己有账号）

<http://www.shiyanbar.com/>

[2] 看雪学院

<https://www.kanxue.com/>

[3] CTF社区：

<http://www.bugku.com/>

[4] 知乎帖

<https://www.zhihu.com/question/47498673>

(针对CTF，大家都是怎么训练的?)

<https://www.zhihu.com/question/3050559>

5、常用网址与比赛工具

[1] 破解密码的所有工具

<https://bbs.ichunqiu.com/forum.php?mod=viewthread&tid=32105>

[2] 编码解码常用网址

<http://web.chacuo.net/charseturlencode>

【注】个人对于CTF比赛只是一个了解性学习，目的是扩宽对信息安全方面的知识的认识与了解。