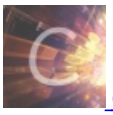
CTF-学习呀

原创

Hacking黑白红 于 2020-06-23 22:20:49 发布 519 收藏 9

分类专栏： CTF 信息安全 文章标签： 安全

本文链接：https://blog.csdn.net/zsw15841822890/article/details/106933301



CTF 同时被 2 个专栏收录

15 篇文章 6 订阅

订阅专栏

信息安全

39 篇文章 8 订阅

订阅专栏

一、CTF概况

CTF的全名是capture the flag 夺旗锦标赛，一般来说分为解题模式，攻防模式和混合模式，其中解题模式比较多。

解题模式：主要以解决网络安全技术问题挑战题目的分值和时间来进行排名，通常是用来在线的选拔，其中题目大概有这么几个 web，misc(杂项），stega(隐写)，crypto(密码学)，reverse(逆向），pwn(综合渗透、溢出）， ppc（编程类）

攻防模式：AWD(Attack With Defense,攻防兼备)，比赛一般就是每一个参赛队伍，在同一个网络中，进行相互攻击和防守，以发现对手服务器的漏洞，修补和防御己方服务器漏洞来的分，一般比赛时间较长。

混合模式:上述两者皆有。

分类知识

1、 **MISC(Miscellaneous)**类型，即安全杂项，题目或涉及流量分析、电子取证、人肉搜索、数据分析等等。所有与计算机安全挑战有关的都算在其中。

2、**PPC(Professionally Program Coder)**类型，即编程类题目，题目涉及到编程算法，相比ACM较为容易。

3、**CRYPTO(Cryptography)**类型，即密码学，题目考察各种加解密技术，包括古典加密技术、现代加密技术甚至出题者自创加密技术。偏重对数学，算法的深入学习。

4、**REVERSE**类型，即逆向工程，题目涉及到软件逆向、破解技术。偏重对汇编，逆向的理解。

5、**PWN类型**，PWN在黑客俚语中代表着攻破、取得权限，多为溢出类题目。同上REVERSE，偏重对汇编，逆向的理解。

6、**STEGA(Steganography)**类型，即隐写术，题目的Flag会隐藏到图片、音频、视频等各类数据载体中供参赛者获取。

7、**WEB**类型，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。偏重对技巧沉淀，快速搜索能力的挑战,**划重点：黑白红客的必备技能。

**

二、CTF学习方向：

方向一：Web；（实战-网站渗透、服务器提权、内网渗透，数据分析）

方向二：Reverse+PWN；（实战-挖洞、软件破解、病毒分析，**划重点-难度五颗星）**

方向三：MISC+STEGA+PPC+CRYPTO（杂项大类）

方向一、二极巨实战价值，学好了可直接进大厂。

都要学的内容：

Linux基础、计算机组成原理，操作系统原理，网络协议分析；

方向一：

网络安全，内网渗透，数据库安全。

书籍推荐：

《Web应用安全权威指南》

《web前端黑客技术揭秘》

《黑客秘籍-渗透测试实用指南》

《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》

《内网安全攻防-渗透测试实战指南》

方向二：

IDA工具使用（f5插件），逆向工程，密码学，缓冲区溢出等

书籍推荐：

《RE for Beginners（逆向工程入门）》；

《IDA Pro权威指南》；

《揭秘家庭路由器0day漏洞挖掘技术》；

《自己动手写操作系统》；

《黑客攻防宝典，系统实战篇》；

从基础题目出发(推荐资源)：

实验吧-CTF题库

i春秋

南邮攻防训练平台

BugKuCTF训练平台

Idf实验室：题目非常基础：ctf.idf.cn

有线下决赛题目复现：www.ichunqiu.com

xctf题库网站：oj.xctf.org.cn/

challs非常入门的国外ctf题库：www.wechall.net/ 很多国内选手都是从这里刷题成长起来

非常入门的国外cif题库：canyouhackit.it

(方向一)

米安的Web漏洞靶场：ctf.moonsos.com/pentest/index.php

国外的XSS测试：prompt.ml/0

国外的sql注入的挑战网站：redtiger.labs.overthewire.org

（方向二）：

吾爱破解论坛

PWN类题目的游乐场：pwnable.kr

三、CTF学习工具和方法

选择什么工具：

CTF比赛一般都是使用网络完全常用工具，比如burp、IDA等，但是会与很多大家不常见的工具。

这里我列举一些聚合：

https://hithub.com/truongkma/ctf-tools

https://hithub.com/Pikachu/v0lt

https://hithub.com/zardus/ctf-tools

https://hithub.com/TUCTF/Tools

以练促赛：

选择一场已经存在writeup(解题思路)的比赛。

以赛养练：

参加一场最新CTF比赛。

https://ctftime.org/国际比赛

http://www.xctf.org.cn/或内比赛

【注】：

1、 参考i春秋网站CTF入门指南系列视频：https://www.ichunqiu.com/course/57519

2、 参考https://www.cnblogs.com/AndyEvans/p/9721272.html