CTF 基本知识

原创

Strawberry. 于 2021-11-07 14:49:41 发布 2806 收藏

分类专栏： ctf试题 文章标签： 安全 web安全

本文链接：https://blog.csdn.net/qq_43754288/article/details/121191242

CTF简介

- 中文译为夺旗赛
- 竞赛模式
    1. 解题模式：类似于ACM编程竞赛、信息学奥数，以解决网络安全技术挑战题目的分值和时间排名，通常用于线上选拔赛，题目包括逆向、漏洞挖掘与利用、web渗透、密码、取证、隐写、安全编程等
    2. 攻防模式：参赛队伍在网络空间互相进行攻击与防守，挖掘网络服务漏洞并攻击对手来得分，修补自身服务漏洞进行防御来避免丢分
    3. 混合模式：解题模式与攻防模式相结合的赛制。

题目类型

1. Web

- web是ctf竞赛中主要题型之一，题目设计许多常见web漏洞，如sql注入、xss、文件包含、上传漏洞等，也有简单的网络基础知识的考察，如返回包、TCP-IP数据包内容和构建
- 所需知识：PHP，Python，sql(以mysql为主)，TCP-IP，Linux，HTML，JavaScript

2. Crypto(密码学)

- 包括古典密码学和现代密码学，古典密码学趣味性强，种类多，现代密码学安全性高，对算法理解的要求较高
- 所需知识：古典密码学、矩阵、数论、算法等。

3. Reverse(逆向)

- 题目涉及到软件逆向、破解技术等，要求有较强的反汇编、反编译功底。主要考察选手逆向分析能力
- 所需知识：汇编语言、加密与解密、常见反编译工具

4. PWN(二进制安全)

- 在CTF中代表溢出类的题目，常见类型有栈溢出、堆溢出。主要考察选手对漏洞的利用能力。
- 所需知识：C、OD+IDA、数据结构、操作系统

5. MISC(安全杂项)

- MISC涉及到隐写术、流量分析、电子取证、人肉搜索、数据分析、大数据统计等，覆盖面广，主要考查选手的各种基础综合知识
- 所需知识：熟悉使用众多隐写工具、流量审查工具、了解编码等
- MISC所有人均可进行，因为它涉及面较广，主要以刷题为主，没有具体的学习流程，但需对所有基本知识进行了解。

学习方法

1. 确定方向

- 每人可选自己感兴趣的一到两个方向进行具体学习(杂项除外)

2. 入门知识：WIndows基础，Linux基础，计算机组成原理，操作系统，网络协议分析
3. 刷题

- bugku：https://ctf.bugku.com/
- 攻防世界：https://adworld.xctf.org.cn/
- 推荐先在bugku进行练习，然后再做攻防世界。

4. 工具

- 先不要下载别人推荐的工具，在学习和解题过程中遇到问题进行寻找，可以让你对工具的使用更加熟练。

编程

- 编程不必太深入学习，但基础知识都要掌握，对照文档可以写出程序，看得懂别人的程序，PHP是必学语言，若可以把这门语言学透，那代码审计一点压力也没有，python，java根据情况掌握

多做题是最重要的！！！

这是我做的一道bugku里的一道题，可进行参考，看一下题目类型和解题方法。
https://blog.csdn.net/qq_43754288/article/details/120827659?spm=1001.2014.3001.5501