如何入门CTF？

原创

东方与君语 于 2019-06-08 19:59:52 发布 6574 收藏 27

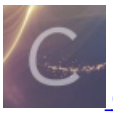
分类专栏： 渗透测试 CTF 文章标签： 安全

本文链接：https://blog.csdn.net/qq_43344642/article/details/91347200


渗透测试 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏


CTF

5 篇文章 0 订阅

订阅专栏

基础

1、编程语言基础（C语言、汇编语言、脚本语言）

2、数学基础（算法、密码学）

3、脑洞大开（天马行空的想象、推理解密）

4、体力耐力（各种通宵熬夜不睡觉）

如何学

1、恶补基础知识（有基础的跳过此步）

2、尝试从脑洞开始（hackgame）

3、从基础题目出发

4、学习信息安全专业知识

5、锻炼体力耐力

赛题情况

PWN、Reverse偏重对汇编、逆向的理解

Crypto偏重对数学、算法的深入学习

Web偏重对技巧沉淀、快速搜索能力的挑战

Misc则更为复杂，所有与计算机安全挑战有关的都算在其中

常规方向：

A方向：PWN+Reverse+Crypto（+ Misc）随机搭配

B方向：Web+ Misc 组合

内容：

Linux基础、计算机组成原理、操作系统原理、网络协议分析

A方向：

IDA工具使用（f5插件）、逆向工程、密码学、缓冲区溢出等

B方向：

网络安全、内网渗透、数据库安全等

推荐图书：

A方向：

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

黑客攻防技术宝典：系统实战篇

B方向：

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

网站：

http://ctf.idf.cn/ 题目基础

www.ichunqiu.com 比赛题目复现

http://oj.xctf.org.cn/ xctf题库网站

www.wechall.net/challs 非常入门的国外ctf题库

http://canyouhack.it/ 非常入门的国外ctf题库

A方向：

https://microcorruption.com/login 很酷炫游戏化

http://smashthestack.org 比较简洁的内容，SSH连入即可开始玩

http://overthewire.org/wargames/ 比较老牌的Wargame ， 国内资料也比较多。一些writeup http://drops.wooyun.org/author/litao3rd

https://exploit-exercises.com/ 也是一个比较老的Wargame，国内资料也比较多。

http://pwnable.kr/play.php PWN类题目的游乐场

B方向：

http://ctf.moonsos.com/pentest/index.php 米安的Web漏洞靶场，还挺好玩

http://prompt.ml/0 国外的xss测试

http://redtiger.labs.overthewire.org/ 国外的SQL注入的挑战网站

常用工具：

比如burp、IDA等，但是会有很多大家不常见的工具。

这里我列举一些聚合：

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

https://github.com/P1kachu/v0lt

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

https://github.com/TUCTF/Tools

进阶

以练促赛：

选择一场已经存在Writeup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/ 国内比赛