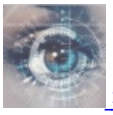
CTF学习路线指南(附刷题练习网址)

转载

Cwhite233 于 2021-02-05 11:20:03 发布 502 收藏 14
分类专栏： 渗透学习 文章标签： 安全 渗透测试
原文链接：https://www.ichunqiu.com/course/57519



PWN,Reverse：偏重对汇编，逆向的理解；

Gypto：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；

Mic：则更为复杂，所有与计算机安全挑战有关的都算在其中

常规做法;

A方向：PWN+Reverse+Gypto,随机搭配；

B方向：Web+Misc组合；

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；

A方向：

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》；

B方向：

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》

从基础题目出发(推荐资源)：

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

（A方向）：

很炫酷游戏化：https://microcorruption.com

比较简洁的内容，ssh连入即可玩：smashthestack.org

比较老牌的Wargame：

overthewire.org

exploit-exercise.com

PWN类题目的游乐场：pwnable.kr

(B方向)

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

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/Plkachu/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

名次不重要，过程很重要！

【注】：

1、writeup指CTF比赛结题思路

2、以上内容来源于i春秋网站CTF入门指南系列视频，原出处：https://www.ichunqiu.com/course/57519