（笔记）CTF入门指南

转载

weixin_30518397 于 2018-12-13 14:48:00 发布 293 收藏 4
文章标签： 密码学 操作系统 运维
原文链接：http://www.cnblogs.com/xiaomulei/p/10113988.html

【考项分类】
Web: 网页安全
Crypto: 密码学（凯撒密码等）
PWN: 对程序逻辑分析 系统漏洞利用
Misc: 杂项 图片隐写 数据还原 脑洞类 信息安全有关的
Reverse: 逆向工程
PPC: 编程类

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比较复杂，所有与计算机安全挑战有关的都算在其中

【需要的基础知识&信息安全专业知识】
A方向：PWN+Reverse+Crypto随机搭配
IDA工具使用（f5插件）、逆向工程、密码学、缓冲区溢出等

B方向：Web+Misc
网络安全、内网渗透、数据库安全等

公共部分：Linux基础、计算机组成原理、操作系统原理、网络协议分析

【推荐书籍】
A方向：
IDA pro权威指南（重要）
揭秘家庭路由器0day漏洞挖掘技术
RE for Beginners（逆向工程入门）
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（适合小白入门对WEB安全进行宏观的理解）
黑客攻防技术宝典 Web实战篇
Web前端黑客技术揭秘
黑客秘籍-渗透测试实用指南
代码审计：企业级Web代码安全架构

【刷题网站】
http://ctf.idf.cn IDF实验室，题目非常基础（推荐）
http://www.ichunqiu.com i春秋 有线下决赛题目复现（推荐）
http://www.wechall.net/challs 非常入门的国外ctf题库（推荐）
http://canyouhack.it
http://oj.xctf.org.cn/xctf

A方向：
http://microcorruption.com/login 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，国内资料多，writeup 在这里：http://drops.wooyun.org/author/litao3rd

B方向：
http://redtiger.labs.overthewire.org 国外的SQL注入的挑战网站（推荐）
http://ctf.moonsos.com/pentest/index.php 米安的WEB漏洞靶场

【CTF工具】
CTF比赛一般都是使用网络安全常用工具，例如burp、IDA等
这里列举一些聚合：
https://github.com/truongkma/ctf-tools
https://github.com/Plkachu/v0lt
https://github.com/zardus/ctf-tools
https://github.com/TUCTF/Tools

【比赛种类】
国际：DEFCON资格赛
国内：XCTF联赛
（XCTF包括RCTF福州站 ZCTF郑州站 SSCTF西安站 BCTF北京站 0CTF上海站 SCTF成都站 WHCTF

武汉站 ABCTF杭州站 XCTF总决赛）

【学习方法】
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（包含一些比较基础的比赛）
http://www.xctf.org.cn 国内比赛（国内主流，但题目大部分偏难）

转载于:https://www.cnblogs.com/xiaomulei/p/10113988.html