CTF入门指南

原创

lcdqqq 于 2018-04-10 17:32:01 发布
分类专栏： CTF

什么是CTF

CTF:Capture The Flag　夺旗赛

分为以下几个方面：

web

Crypto密码学

PWN 程序的逻辑分析 漏洞利用
Misc 杂项：1.stego　forensics　等等
reverse 逆向分析
PPC 编程类（非常规）

CTF==奥数

思维能力、快速学习能力、技术能力

入门需要的基础：
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、推理解秘）
4.体力耐力（通宵不睡觉。。）
但只有这些还是不够的

如何学：
1.恶补基础知识
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

1.分析赛题情况
2.分析自身能力
3.选择更合适的入手

PWN、Reserve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

常规做法：
A：PWN+Reserve+Crypto随机搭配
B：Web+Misc组合

都需要的基础：
Linux基础、计算机组成原理、操作系统原理、网络协议分析
A需要的：IDA工具使用（f5插件）、逆向工程、密码学、缓冲区溢出
B需要的：网络安全、内网渗透、数据库安全

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（一个日本人写的）
Web前端黑客技术揭秘
黑客秘籍-渗透测试使用指南
黑客攻防技术宝典 Web实战篇

从基础题目出发：
http://ctf.idf.cn/ IDF实验室
i春秋
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://canyoihack.it 非常入门的国外ctf题库
https://microcorruption.com/login 很酷炫的游戏化（A方向）
http://smashthestack.org 比较简洁的内容，SSH连入就可以玩
http://overthewire.org/wargames 比较老牌的wargame 很推荐 一些writeup：http://drops.wooyun.org/author/litao3rd
http://exploit-exercises.com 比较老牌的wargame
http://pwnable.kr/play.php PWN类题目
http://ctf.moonsos.com/pentest/index.php 米安得Web漏洞靶场
http://prompt.ml/0 国外的xss测试平台
http://redtiger.labs.overthewire.org/ 国外的SQL注入挑战网站

入门选择的工具：
https://github.com/truongkma/ctf-tools
https://github.com/Plkachu/v0lt
https://github.com/zardus/ctf-tools
https://github.com/TUCTF/Tools

https://ctftime.org/ 国际（有比较基础的比赛 推荐新手）
http://www.xctf.org.cn/ 国内

如何组建团队：
1.思维跳跃：灵活性、不会钻墙角
2.专注：遇到问题不放弃直到解决
3.耐力：可以一天一夜不睡觉研究技术
4.团队精神：责任、凝聚、分享
以上四条达到三条即可强力队员