CTF学习指南

原创

书一文，解一惑 于 2020-04-18 14:12:43 发布 383 收藏 17

分类专栏： 笔记

本文链接：https://blog.csdn.net/weixin_44350891/article/details/105597921

文章目录

类型

Web：网络安全

Crypto：密码学（凯撒密码、栅栏密码等）

PWN：程序的逻辑分析漏洞，利用Windows、Linux、还有小型机等

- Mist：杂项，包括数据还原、脑洞推理、大数据等

Reverse：逆向分析，逆向类的破解分析漏洞

PPC：编程类，不是常规CTF的类型，是掺杂在以上五种中。

比赛

国际比赛：DEFCON资格赛

国内比赛：XCTF联赛（0CTF较为值得关注）

基础篇

编程语言基础（C、汇编、脚本等）

数学基础（算法、密码学）

脑洞（想象力，推理解密）

体力耐力（各种通宵熬夜不睡觉）

入门进阶之路

恶补基础

尝试从脑洞开始（hackgame）

基础题目出发

学习信息安全专业知识

锻炼体力耐力

赛题学习

分析赛题情况

分析自身能力，选择更适合的入手

赛题分析
PWN、RE更偏重于汇编、逆向思维代码理解

Crypto偏重数学、算法理解

Web偏重技巧沉淀、快速搜索，更偏向于发散思维，对底层要求不是特别深

mist所有与计算机安全挑战有关

路线选择

常规的有以下两种，可以分析自身情况，选择一条路线，其实5条选一两个方向即可。

A路线：PWN+Reverse+Crypto随机搭配

B路线：Web+Mist，Web其实和另三种都可以搭配，但web对底层不够了解，更偏向于发散思维，所以选择了Mist，Web安全为主，Mist类为辅。

需恶补的知识点
常规学习：Linux基础、计算机组成原理、操作系统原理、网络协议分析、C语言、汇编等

A：IDA工具使用（最重要）、逆向工程、密码学、缓冲区溢出等

B：数据库安全、网络安全、内网渗透等，如果可以的话要对安全认证中对前十的安全漏洞进行了解

书籍推荐

A路线
《RE for Beginners》（逆向工程入门，乌云里应该有翻译，去找找乌云的数据库，看官方英文也行）

《IDA Pro权威指南》（最推荐，学A路线最好都买这本）

《揭秘家庭路由器0day漏洞挖掘技术》（对mist漏洞分析和利用，对逆向分析有基础了解，但对小型机不了解，可以看这本）

《 自己动手写操作系统》（初级不需要，中级可以尝试分析）

《黑客攻防宝典：系统实战篇》（推荐，Windows、Linux等逆向基本讲解）

B路线
《web应用安全权威指南》（最推荐，纯小白看这本，从宏观的角度告诉你信息安全中的Web安全是什么）

《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》（web安全所有的大况，所有的核心技术和最常规技术都有了，对Web安全前进方向很有用）

《代码审计：企业级Web代码安全架构》

赛棍之路(推荐的都是基础题篇）

IDF实验室:有些题目偏脑洞，超基础,每道题基本只考一个点,题目非常基
础

i春秋的在线挑战,去i春秋的官网那里有在线挑战，有线下决赛和线上题目题目复现，对于不懂的可以论坛提问

http://oj.xctf.cn/xctf ，xctf的部分历年题库题库网站，题目较难

www.wechall.net/challs ,，很推荐，非常入门的国外ctf题库，很多大牛都从这里出来，第一步从这里刷题

http://canyouhack.it/也是非常入门的国外ctf题库，比上面那个弱一些，有移动安全类题目，可对移动安全有所了解

https://microcorruption.com/login,关于A方向的，很酷炫，有很多友好提示

http://smashthestack.org比较简洁，SSH连入即可开始玩，国外的wargame，从初级开始，蛮好玩

http://overthewire.org/wargame/，比较老牌的wargame，国内资料比较多，一些writeup[http://drops.wooyun.org/author/litao3rd乌云上有

http://exploit-exercise.com/，也是一个比较老的Wargame，国内资料较多，新的资料比较少

http://pwnable.kr/play.phpPWN类题目的游乐场。大概不到100题，刷简单题目

http://ctf.moonsoc.com/pentest/index.php,米安的Web漏洞靶场，web安全的核心技术点

http://prompt.ml/0,国外的xss测试，没有具体考核对错的过程，可构建各种xss

http://redtiger.labs.overthewire.rog/国外的SQL注入挑战网站，10关，比较初级，对SQL注入来说会比较简单，6-10关没有提示

入门工具
ctf比赛一般都是网络安全常用工具，比如burp、IDA等，但是也有大家不怎么常见的工具。
还有看雪、吾爱推出的工具库，这里就不放链接了，自己搜索一下就有了。

CTF选手整理的工具库：

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

https://github.com/Plkachu/v0lt

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

https://github.com/TUCTF/Tools

入门与比赛
以练促赛：选择已经存在的Writeup比赛，在writeup把多个队伍的的解题方式结合，怎么要这样做，如果他们失败了，分析他们之前失败的原因

以赛养练：参加最新CTF比赛，不要在意名次， https://ctftime.org国际比赛（比较基础） https://www.xctf.org.cn/国内比赛（国内主流，较强，较难）

强力队员画像
思维跳跃：灵活性、不会钻墙角

专注：遇到问题不放弃直到解决

耐力：可以一天一夜不睡觉的研究技术

团队精神：责任、凝聚、分享

以上三条为强力成员，以上四条会成为强力队长

团队组建
新人招募：如何评判新人潜力（基于强力成员来看）

队员培养：如何快速培养队伍能力（看上面的进阶之路）

梯队有序：如何建立阶梯层级

纪律严格：如何拒绝无团队精神队员

点点吐槽
CTF之路真是道阻且长啊。。。但是总算有了方向不是么？