CTF 简析

原创

rainbowarc 于 2017-03-15 16:06:24 发布 641 收藏 1

本文链接：https://blog.csdn.net/rainbowarc/article/details/62227808

1.方向简析

PWN、Reverse对于汇编、逆向的理解

Crypto偏重对数学、算法的学习深入

Web偏重对技巧沉淀，快速搜索能力的挑战（发散思维）漏洞点的积累

Misc 则更为复杂，所有与计算机安全挑战有关的都算在其中

大体方向分类
A：PWN+Reverse+Crypto随机搭配 选择两个（IDA工具使用,f5插件，逆向工程，密码学，缓冲区溢出等）

推荐书籍
RE for Beginners（逆向工程入门）
IDA Pro权威指南（重要）
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：Web+Misc组合（网络安全，内网渗透，数据库安全等）对于安全认证中前10的安全漏洞进行了解

Web应用安全权威指南（最推荐）
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（第二）
代码审计：企业级Web代码安全架构

2.学习方向

1.）编程语言基础

C++ 汇编语言 脚步语言

2.）Linux基础，计算机组成原理，操作系统原理，网络协议分析

3.）脑洞
hackgame的练习

4.）从基础题目出发

通过国外初中，高中的题目入手

http://ctf.idf.cn/ IDF实验室：题目非常基础

www.ichunqiu.com 线上题目

http://oj.xctf.org.cn/ xctf题库网址（较难）

www.wechall.net/challs(国外ctf入门题目)
http://canyouhack.it/(入门国外)
http://microcorruption.com/login(A方向 炫酷游戏化)

http://smashthestack.org SSH连入就可以开始
http://overthewire.org/wargame/(推荐 难)
http://exploit-excrciscs (wargame)

http://pwnable.kr/play.php(pwn)

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

http://prompt.ml/0(国外的xss测试)

http://redtiger.labs.overthewire.org/(国外的SQL注入挑战网站)

5.）学习信息安全专业知识

3.参赛前如何学习

1.分析赛题的情况
2.分析自身能力
3.选择更适合的入手
4.找一场存在Writeup的比赛

CTF工具下载
http://github.com/truongkma/ctf-tools
http://github.com/Plkachu/v0lt
http://github.com/zardus/ctf-tools
http://github.com/TUCTF/Tools

5.锻炼体力耐力