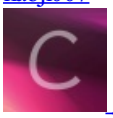
CTF入门指南（Capture the flag）

转载

haoji007 于 2018-10-16 10:34:15 发布 5977 收藏 8



英文教程：*https://trailofbits.github.io/ctf/intro/careers.html*

1、逆向工程

建议你得到一个IDA Pro的副本，这有免费版和学生认证书。尝试下crack me的问题。写出你的C语言代码，然后进行反编译。重复这个过程，同时更改编译器的选项和程序逻辑。在编译的二进制文件中“if”声明和“select”语句有什么不同？我建议你专注于一个单一的原始架构：x86、x86_64或是ARM。在处理器手册中查找你要找的，参考有：

《Practical Reverse Engineering》
《Reversing: Secrets of Reverse Engineering》
《The IDA Pro Book》

2、加密。

虽然这不是我自己的强项，但这里有一些参考还是要看看的：

《Applied Cryptography》
《Practical Cryptography》
Cryptography I

3、ACM编程

选择一个高层次的语言，我推荐使用Python或Ruby。对于Python而言，阅读下《Dive into Python》和找一些你要加入的项目。值得一提的是Metasploit是用Ruby编写的。关于算法和数据结构的计算机科学课也要在此类中要走很长的路。看看来自CTF和其他编程的挑战，战胜他们。专注于创建一个解决方法而不是最快或是最好的方法，特别是在你刚刚开始的时候。

4、web漏洞

有很多的网络编程技术，在CTF中最流行的就是PHP和SQL。php.NET网站（译者注：需翻墙）是一个梦幻的语言参考，只要搜索你好奇的功能。PHP之后，看到网页上存在的挑战的最常见的方法就是使用Python或Ruby脚本。主要到技术有重叠，这有一本关于网络安全漏洞的好书，是《黑客攻防技术宝典：Web实战篇》。除此之外，在学习了一些基本技术之后，你可能也想通过比较流行的免费软件工具来取得一些经验。这些在CTF竞争中也可能会偶尔用到，这些加密会和你凭经验得到的加密重叠。

5、二进制练习

建议你在进入二进制练习前要完成逆向工程的学习。这有几个你可以独立学习的常见类型漏洞：栈溢出，堆溢出，对于初学者的格式字符串漏洞。很多是通过练习思维来辨别漏洞的类型。学习以往的漏洞是进入二进制门槛的最好途径。推荐你可以阅读：

《黑客：漏洞发掘的艺术》
《黑客攻防技术宝典：系统实战篇》
《The Art of Software Security Assessment》

6、取证/网络

大多数的CTF团队往往有“一个”负责取证的人。我不是那种人，但是我建议你学习如何使用010 hex editor，不要怕做出荒谬、疯狂、随机的猜测这些问题运行的结果是怎样。

CTF入门指南-相关靶场平台

标签： ctf竞赛信息安全

2016-08-15 16:09 213人阅读 评论(0) 收藏 举报

分类：

互联网安全（28）

相关靶场平台：

1、IDF实验室：http://ctf.idf.cn/

2、实验吧公司产品：http://www.shiyanbar.com/

3、四叶草安全 这个公司做web比较强：http://www.seclover.com/

4、XCTF_OJ练习平台

XCTF-OJ （X Capture The Flag Online Judge）是由XCTF组委会组织开发并面向XCTF联赛参赛者提供的网络安全技术对抗赛练习平台。
XCTF-OJ平台将汇集国内外CTF网络安全竞赛的真题题库，并支持对部分可获取在线题目交互环境的重现恢复，XCTF联赛后续赛事在赛后也会把赛题离线文件和在线交互环境汇总至XCTF-OJ平台，形成目前全球CTF社区唯一一个提供赛题重现复盘练习环境的站点资源。
地址：http://oj.xctf.org.cn/

5、BCTF比赛平台

BCTF是由蓝莲花战队举办的网络安全夺旗挑战赛，去年只面向国内，从今年开始，向全世界开放。

今年的BCTF也是全国网络安全技术对抗联赛XCTF的分站赛之一，获胜的中国XCTF队伍将直接晋级南京的XCTF总决赛（决赛也由蓝莲花战队命题）。其他参赛的XCTF队伍也将获得积分，来竞争XCTF决赛的其他席位。

地址：http://bctf.cn/#/challenge

6、HacKGame2

HacKGame2是由blackbap论坛开发的一套在线黑客闯关游戏。地址：http://hackgame.blackbap.org/