CTF如何入门

转载

Sandra_93 于 2018-09-25 10:52:45 发布 4442 收藏 48

分类专栏： CTF理论 文章标签： CTF

 CTF理论 专栏收录该内容

3 篇文章 1 订阅

订阅专栏

不知道从哪里找来的，可能是知乎吧，放在这里。

感谢编辑内容的大佬，此为转载。

最近有些人问关于ctf怎么入门的问题，大家先不要急着一步登天，也不要把ctf想的很复杂，其实入门还是很简单的，然后就是不断的自学阅读并坚持下来（各种书籍与大牛的博客，网站，wp），还有就是我再说下关于不同方向怎么入门的问题：

web：

1：先去大概了解一下html，php和sql的相关知识，熟悉一下语言。推荐W3cschool

2：了解http包的组成部分

2：接着你需要一个可以抓包的工具（Burpsuite）工具自行百度，需要JAVA环境。

3：当然，浏览器也很重要，这里推荐web狗专用firefox浏览器，保证你用了之后题题出flag！（火狐需要自行下载插件，这五个插件用的比较多可以自己去下载1.Firebug

2.Hackbar 3.HostAdmin 4.UserAgent Switcher 5.Modify Headers（工具使用方法可以先自己百度下）

4：现在就需要一个可以编辑和看代码的软件,一个是Notpad,一个是Sublime,根据喜好自行选择。

逆向： 逆向我也懂的不多，说说我觉得重要的吧，仅供参考：

1.首先的首先必须得掌握基本的编程能力，之后就是学习相对底层的【汇编语言】

2.对不同的调试工具例如windbg，ollydbg，ida熟练的调试与使用（逻辑思维能力要强）

3.掌握外壳原理和技巧，遇到加密程序时能进行脱壳与解密处理（学长讲的的汇编题就属于解密）

4.经常逛各大论坛：吾爱破解，看雪论坛，发现新姿势

这里推荐吾爱破解的入门教程：https://www.52pojie.cn/thread-349073-1-1.html

pwn（最难的部分）：

1.shell的基本语法

2.kali下各种渗透工具的使用

3.熟练掌握逆向方面的知识

4.不断的摸索…（我也不知道接下来该怎么办…）

misc： 无限的脑洞！分为很多类隐写：

1.图片隐写：stegsolve对图片进行分析，winhex找隐藏信息，lsb隐写，ntfs文件流，图种，二维码等等等等…

2.音频隐写：mp3stego分离MP3中的隐藏文件，audacity分析等等等等…

3.压缩包隐写：伪加密，明文攻击，暴力破解等等等等…

4…等等…

密码学（其实并不难）：

1.阅读各种加密模式，查阅资料，掌握加密原理

2.能快速识别各种加密的特征

我能想到的也就这么多，大概都写出来了，只要萌新掌握基本知识，熟练使用各种工具，相信会提升的很快。最后，祝各位同学们玩的开心，希望与各位学弟学妹学长学姐16级的同学们一同学习和进步！

ps：关于上节课第二题讲的sql注入的知识，大家如果有不懂的地方可以看下这篇基础文章：http://blog.csdn.net/stilling2006/article/details/8526458/ 结合wp食用效果更佳~
不懂的多多百度~ 百度是最好的老师~

以上