谈谈CTF技能树

原创

banana.us 于 2022-03-17 21:44:51 发布 5229 收藏 1
文章标签： web安全 经验分享

嗨！今天来聊聊CTF中的技能树的五个分支--Web、Pwn、Reverse、Crypto、Misc。博主现在只接触过Web，但相信今后会学习其他四项技能。

一、Web

即万维网，我们日常上网浏览的网页主要由三部分组成--HTML、CSS和Javascrip。Html如同网页的骨干，它编辑了网页的标题、正文等内容；CSS做的是网页的外观，颜色、背景，让网页更加美观。Javascrip是一种脚本语言，可以制作一些动态效果，插入可以播放的视频，让网页更加人性化，易于使用。同时，web安全问题不容忽视，网页作为维系服务端和客户端的纽带，若遭到攻击，可能会导致数据被窃取，网站被挂马等危害。

二、Pwn

主要用于漏洞挖掘、提权从而来实现破解漏洞、攻破服务器。学习pwn需要二进制、汇编语言、C语言、linux等基础。

常见的漏洞有：

缓冲区溢出 比如堆溢出，栈溢出，整数溢出，bss溢出,data溢出。最常见的就是栈溢出吧，还有格式化字符串和逻辑漏洞。

三、Rerverse

即逆向。学习逆向需要C语言、汇编语言、文件格式等基础。逆向工程将低级代码转换到高级代码，方便人的阅读。人编写的高级语言进过汇编成为汇编语言，而将汇编语言转换成高级语言即是逆向工程的目标。逆向工程是一个复杂的过程，需要较好的理论知识基础，并要多实践。

四、Crypto

主要是破解加密的文件，需要了解各种加密方式。可以通过一些工具辅助解密。个人认为crypto和数据安全关系比较大，学习crypto可以更好的认识到数据安全的漏洞从而更好加强维护数据安全。

五、Misc

misc涉及流量分析、电子取证、人肉搜索、数据分析等。用解码工具打开照片可以得到照片的编码方式，通过分析可以找到可能有效的信息。misc要求充分利用各种已知信息，不断地寻找有效信息，或对信息转码得到有用信息。要求有较深的理论知识，分析能力，动手能力和毅力。

总结：博主虽然只接触过web，但我相信兴趣驱动的学习是高效的。我对破解方面感兴趣，我会好好打牢基础知识，多实践操作，不断进步。最终capture the flag。