CTF入门

原创

chaoyueziji123 于 2015-09-28 21:07:25 发布 57180 收藏 501

本文链接：https://blog.csdn.net/chaoyueziji123/article/details/48790331

感谢白帽子ADoG A.K.A D3AdCa7（死猫&霸道总裁）同学的投稿，以下内容供安全爱好者参考学习，本文获得投稿奖励300元，即将打入作者账户，投稿请发送邮件至 huangyuan#360.cn

序

信息安全作为国家越来越重视的领域已经在渐渐起飞，而CTF（Capture the flag）作为信息安全领域选拔人才和互相比拼技能水平的比赛形式，也被越来越多的人所关注，那么作为一个初次接触CTF的新手，你如何在各大赛事中翱翔，在排名榜单的第一页中获取自己的一席之地呢？作为一个在CTF领域中混迹了两年多的老赛棍，来谈谈我自己入门时候的一些经验，以及摸石头过河之后一些过来狗的感慨。

CTF简介

为了方面纯新手了解CTF是个啥，我思考了一下还是在这多写几句。

CTF作为信息安全的一种比赛形式，目前基本有三种形式，解题模式、攻防模式和瞎来模式。

解题模式呢，就是出题者把一些信息安全实战中可能遇到的问题抽象成一个题目，比如一个存在漏洞的网站让你入侵，一个带有解密算法的程序让你逆向来写出注册机，一个有漏洞的程序让你分析来写出漏洞利用程序，一段密文让你解密，一个图片让你从里面找出个种子等等等等。而你在做完这些出题人期望你做的事情之后，你就能获得一串奇怪的字符串，也就是所谓的flag，提交它，就能获得这道题目的分数。

而攻防模式呢，一般出现在线下的CTF中，每个队伍维护自己的服务器，攻击别人的服务器，每个队伍的服务器上一开始拥有相同的设置，比如几个有漏洞的二进制程序、有漏洞的web应用等等，然后大家需要找出这些漏洞，修复自己服务器上的漏洞，且利用这些漏洞来攻击别人的服务器。

瞎来模式呢，可以参见今年年初日本举办的seccon final和每年的ictf等，就是把一些剧情啊设定啊和ctf结合起来搞了一些有趣的比赛。

新手一般所接触的基本都是线上的CTF比赛，大多数都是解题模式。

两年前拿衣服的我

我人生参加的第一个CTF（或者说类似CTF的比赛，因为它当时还不叫CTF），是杭州电子科技大学2012年底举办的信息安全大赛，当时的我只是一个标准的计算机专业的码狗，除了会写点代码之外，了解一些linux的基本使用、一些小技巧以及会一些基本的SQLi和XSS技巧（当时好像还会一点OD，不过现在早已忘光了），我也就是从那时入了CTF的门（入了CTF的坑），所以大家一开始参加CTF的话，了解一些基本的安全技能就可以上战场咯。边参与边学习，不懂就问谷狗，找不到问题的答案就再用英文描述一遍问题，再问谷狗。（小编：原来这就是霸道总裁的第一次）

CTF中含有那些安全知识

CTF中几乎含有所有的信息安全知识，所以CTF来作为一个信息安全爱好者的入门非常棒！

二进制程序的逆向分析，二进制程序的漏洞挖掘与利用，操作系统内和安全，移动安全（安卓逆向与漏洞分析、IOS逆向与漏洞分析），网络协议分析，Web攻击，Web日志审计与分析，隐写术，密码学应用，路由器漏洞利用，ACM编程，各种环境的取证分析等等（可能有遗漏）

你说的我都明白，可是我该如何起飞？

首先是扎实的计算机基础，不能在基本概念上闹笑话，比如：

xx： “我在做题，为啥我搞了个命令执行想反弹shell结果收不到啊，别的啥命令我都能执行！”

我： “你弹到哪个服务器上了？”

xx： “我的虚拟机啊，IP是192.168.1.233”

我： “...”

如果上面那个笑话你看不懂的话，你就需要去补充一下网络方面的基础知识了。

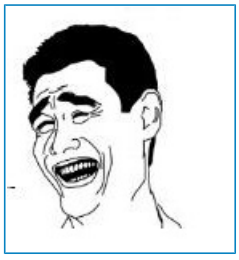
接下来就是各个方面知识的深入理解和应用，安全是个非常应用的学科，很多安全的问题并不是出在理论不健全上，而是在实施的时候出了这样那样的问题。碰到不懂的问题，不能看了别人写的答案或者思路就觉得自己也会了，一定要自己动手做一遍。

赛棍的TIPS

第一，解题型的比赛一定不要在一道题目上卡太久，随时把思路记录下来，不行了就去搞一下别的，然后再回来接着搞。

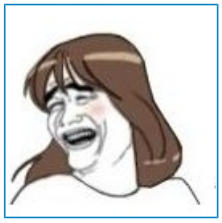
第二，面对国内的比赛时，脑洞一定要大，因为国内很多出题人还控制不好难度高和脑洞大之间的区别，一定要发散思维，像下面这位加特效一样。

第三，长时间比赛一定买好零食，一般做到兴起的时候你是没有心情吃饭的，没有零食你就肚子饿，然后FB就会被别人抢走，然后你的表情会是这样。



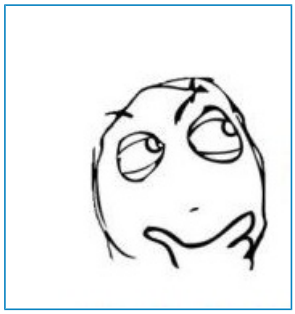
第四，平时见到好的文章技巧，或者自己踩过的坑，一定要全部记在一个小本本上方便查阅，不然很可能有的坑你还要掉第二次。

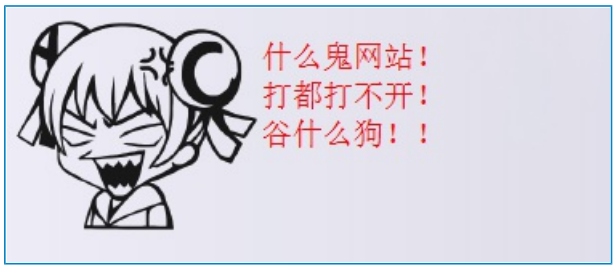
第五，终端一定要美化，不然做题的效率会非常低。



第六，很多web的问题其实想明白之后都是可以在本地搭环境调试或者fuzz的，千万不要不动手。

第七，一定要多多向谷狗请教，一定要多多向谷狗请教，一定要多多向谷狗请教，一定要多多向谷狗请教，一定要多多向谷狗请教，一定要多多向谷狗请教，一定要多多向谷狗请教。（太重要了所以说了7遍）





（搞安全的，一定要学会翻x哦）

接下来推荐一些资源咯~（如果你不想玩CTF，但想尝试进入信息安全领域，以下的很多资源也很好用

Web安全

https://pentesterlab.com/

一个很nice的网站，把一些漏洞打包到一个ISO里面，自己在本地假设好之后，直接从web一路攻入，直到拿到权限，太爽了。

http://www.hackthissite.org/

当年做了很多他们的题，了解了一些奇怪的思路，技术提升到不是很大。

http://www.wechall.net/

之前有刷过一点，能见识到很多的题目，因为站比较久了，所以很多题目如果自己做不出的话在网上找找都能找到一些题解。

http://bobao.360.cn/

（打个软广告咯

二进制安全

http://bbs.pediy.com/

一个圣地，我逆向的启蒙之地，了解了一些基本的东西，不过作为一个web狗，后来基本都荒废了。

https://exploit-exercises.com/

非常酷，一系列的问题打包成一个ISO，下载下来在本地实际操作。

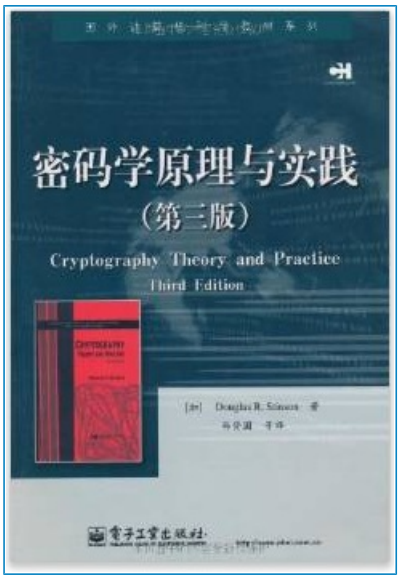
密码学

http://overthewire.org/wargames/

上面有一些wargame是关于密码学的，做过一些。

《密码学原理与实践》

我所了解得密码学的知识都是因为我曾经好好学过这本书（跟着我校数学系的密码学课程去学的



隐写术

http://appleu0.sinaapp.com/?p=501

AppleU0写的一篇很好的总结。

取证分析

一些linux基本命令的巧妙使用，一些取证工具的使用，16进制分析，更多的是经验和积累了，暂时没想到什么比较好的资源。（警察叔叔比较懂这个

王婆卖瓜

http://gou.gg/

我的blog，好久没更新了，懒狗我，新年希望多写一些东西上去。

http://weibo.com/d34dc47