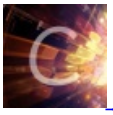
如何开始CTF

转载

千尺浪 于 2017-10-18 18:06:45 发布 834 收藏 3
分类专栏： CTF竞赛 文章标签： 经验 CTF


CTF竞赛 专栏收录该内容
3 篇文章 0 订阅
订阅专栏

如何开始CTF比赛之旅
作者：赵阳
在过去的两个星期里，我已经在DEFCON 22 CTF里检测出了两个不同的问题：“shitsco”和“nonameyet”。感谢所有的意见和评论，我遇到的最常见的问题是：“我怎么才能在CTFs里开始？”在不久前我问过自己一样的问题，所以我想要给出些对你追求CTFs的建议和资源。最简单的方法就是注册一个介绍CTF的帐号，如CSAW, Pico CTF, Microcorruption或是其他的。通过实践、耐心和奉献精神，你的技能会随着时间而提高。
如果你对CTF竞争环境之外的问题有兴趣，这里有一些CTF比赛问题的集锦。挑战往往也是有多种不同的难度级别，注意解决最简单的问题。难易程度是根据你的个人技能的程度决定的，如果你的长处是取证，但是你对加密不在行，取证问题将会成为得分点而相比之下加密问题就会拖后腿。CTF组织者对此有同样的感知，这是为什么对于CTF比赛的评价是很大的挑战性。
如果你已经亲自尝试过几个基础问题且仍然苦恼，现在有很多自学的机会！CTF比赛主要表现以下几个技能上：逆向工程、密码学、ACM编程、web漏洞、二进制练习、网络和取证。可以从中选择并关注一个你已经上手的技能方向。
1、逆向工程。我强烈建议你得到一个IDAPro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。这是我个人的爱好，我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。
最后，Dan Guido和公司最近推出了CTF领域指南，会对以上几个主题的介绍有很好的帮助。

0ops团队向对安全技术感兴趣的小伙伴们，推荐了一些高质量的书籍：《程序员的自我修养》、《深入理解计算机系统》、《算法导论》、《密码学应用》、《编译原理(龙书)》、《鸟哥的私房菜》、《白帽子讲Web安全》等。

此外，还有一些在互联网上具有代表性的关于CTF竞赛相关的练习资源：

逆向工程：bbs.pediy.com，www.52pojie.cn，crackmes.de，reversing.kr

漏洞挖掘与漏洞利用：smashthestack.org，pwnable.kr，overthewire.org/wargames/vortex/

网络渗透：www.wechall.net，pentesterlab.com

CTF竞赛题目汇编：github.com/ctfs，shell-storm.org/repo/CTF/

https://github.com/ctfs

http://www.wechall.net/en/news

http://blog.sina.com.cn/s/blog_9cd8465f0102v6ok.html图片分析题

http://www.e365.org/?p=15541选手心得

http://www.secpulse.com/archives/1112.html通关攻略

http://drops.wooyun.org/tips/3170 14通关攻略

http://www.secpulse.com/archives/39058.html 2015通过攻略

http://bobao.360.cn/learning/detail/129.html通关攻略

http://bobao.360.cn/news/detail/734.html通关2015

http://wenku.baidu.com/link?url=Kk7PDF57WZDQTR9X61FUHUYy_MBSGRZA3v2ruCb9HxvbGJCQa8e-kNiM-aZpJZA-a1u_vafcWSvp2HW5EL8tu4MwH7BjdXewJkv3YXO2OMm###

http://t.qq.com/TXCISG信安微博

http://www.secbox.cn/hacker/ctf/8078.html密码

http://www.freebuf.com/articles/others-articles/79737.htmlCTFwriteup：CSAW CTF 2015 Web200解题过程

http://www.secbox.cn/hacker/tools/8646.html[CTFWRITEUP] 《三个白帽》某题的writeup

http://drops.wooyun.org/tips/4862?utm_source=tuicool隐写术总结

http://www.2cto.com/Article/201406/310858.html**ISCC2014writeup**

http://www.secbox.cn/hacker/ctf可点开认真查看

http://www.tuicool.com/articles/MrmM3uR