CTF学习

转载

CN_CodeLab 于 2016-12-19 19:51:38 发布 3417 收藏 4

分类专栏： CTF


CTF 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

> 转载于百度贴吧http://tieba.baidu.com/p/3933947157?see_lz=1&pn=1

CTF（Capture The Flag）中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF起源于1996年DEFCON全球黑客大会，以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式，2013年全球举办了超过五十场国际性CTF赛事。而DEFCON作为CTF赛制的发源地，DEFCON CTF也成为了目前全球最高技术水平和影响力的CTF竞赛，类似于CTF赛场中的“世界杯”。

1. 赛事介绍

CTF竞赛模式分为以下三类：

- 解题模式（Jeopardy）在解题模式CTF赛制中，参赛队伍可以通过互联网或者现场网络参与，这种模式的CTF竞赛与ACM编程竞赛、信息学奥赛比较类似，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别。
- 攻防模式（Attack-Defense）在攻防模式CTF赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。攻防模式CTF赛制可以实时通过得分反映出比赛情况，最终也以得分直接分出胜负，是一种竞争激烈，具有很强观赏性和高度透明性的网络安全赛制。在这种赛制中，不仅仅是比参赛队员的智力和技术，也比体力（因为比赛一般都会持续48小时及以上），同时也比团队之间的分工配合与合作。
- 混合模式（Mix）结合了解题模式与攻防模式的CTF赛制，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。采用混合模式CTF赛制的典型代表如iCTF国际CTF竞赛。

2.如何开始CTF比赛之旅

“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。

- 逆向工程。我强烈建议你得到一个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》

- 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》

- 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。

- 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。

- 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》

- 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。

3.安全团队的 CTF 得分能代表哪方面的实力水平？

ctf的类型还是挺多的，大概可以分为三类：脑洞类，学术类，实战类。不同风格队伍会适应不同类型的题目，然后比赛中题目类型的占比也会影响到最后的成绩排名，所以体现的实力水平也是不一样的。还有队友分布要均衡，对于不同方向的题目都能有人做有人出力，不然就会出现一堆web汪盯着pwn漏洞利用和re逆向之类的二进制题目干瞪眼的情况~ㄟ(￣▽￣")ㄏ队伍的合作也要愉快，能互相鼓励一起前进，心态也要好一些。

第一类的话，是脑洞类的题目，脑洞要大，要能联想，看到一个细节不要放过都要好好利用起来，这种的ctf比赛的代表貌似就是以360的比赛比较出名（俗称360脑洞大赛=.=），附带上几篇writeup吧，可以参考参考。360hackgame writeup、第三届-360信息安全大赛 WriteUP、AppLeU0’s Blog。有一些是比较莫名奇妙的联系，有的会很牵强，所以感觉做起来不是很爽。甚至最后看到writeup都会出现（ノ’-‘)ノ （┻━┻还能这样子做题的感慨。至于做好这类题目代表了什么实力水平？可能就是要见多识广，联想能力好，能头脑风暴，脑洞够大吧~＞▽＜

2.第二类的话，是比较常规的题目，其实有挺多的比赛都是这样子的，有点点偏学术。它会抽象出一个一个知识点，然后分别考察，一道题一道题来，这样子解题之类的。考察的方面可能都会比较全面，web渗透、pwn漏洞利用、re逆向工程、code编程、misc杂项。可能都会被涵盖到的。

比如之前刚刚举行的强网杯的比赛，附两个writeup。、AppLeU0’s Blog、“强网杯”网络安全挑战赛writeup。

这种类型的比赛，一个人要搞定是几乎不可能的，必须要找到合适的队友，合理分配战力。队友也要给力，对于这些考察的知识自己平时也有研究与积累。还有就是和时间的战斗吧，很多时候比赛都是24小时48小时连续的，一般都是留在实验室通宵熬夜的做题，所以肾要好(严肃脸)，要能熬夜。

这种比赛，其实还是考验一个队伍的知识全面与否，最弱的方向不能太弱，比较平均，各方面都能出的上力，可能是获得这种比赛好成绩的一个条件吧。

3.第三类的话，可能都是一些偏实战的题目的，这种类型的题目一般比较少见，因为环境搭建、权限控制什么的，还有一些时候会涉及到一些选手之间的对抗，所以一般是在ctf的决赛中比较多吧。因为选手少，好控制，网络环境也好配置。

这种偏实战的很多都是从真正的实战环境来的，很多是去模拟一个实战的环境，所以需要有丰富的渗透经验啊，平时多搞搞站，多实战，才能提高这方面的能力吧。还有一些是选手互相进攻的，占领彼此的服务器，可能就是要看经验了吧，很多时候一个猥琐的直到比赛结束都没法被发现的后门就是致胜的关键。

也发几个这种类型的writeup吧，这种比赛还是挺好的，做出来题目就种渗透成功了的感觉，还提高了姿势，特别nice~ o((>ω<))o。AppLeU0’s Blog、ALICTF Quals 2015 [Pentest]、AppLeU0’s Blog。