CTF网络安全比赛介绍

原创

山里来的Dark杰瑞 于 2021-11-16 10:53:52 发布 2043 收藏 1
文章标签： web安全 安全

本文链接：https://blog.csdn.net/Dark0518/article/details/121350871

2019年，电视剧《亲爱的，热爱的》的一经播出，而一直稳占热搜，该剧主线讲述的是韩商言与佟年青春言情故事，而副线则是讲述了以韩商言为代表的一群职业CTF选手共同努力为国争光的故事。剧中韩商言是CTF圈子里的大佬，也是中国CTF大赛的领头羊。那问题来了，这CTF是个什么东西？

一、CTF简介

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”。

二、CTF竞赛模式

（1）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。
（2）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。
（3）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。

三、CTF各大题型简介

MISC（安全杂项）：全称Miscellaneous。题目涉及流量分析、电子取证、人肉搜索、数据分析、大数据统计等等，覆盖面比较广。我们平时看到的社工类题目；给你一个流量包让你分析的题目；取证分析题目，都属于这类题目。主要考查参赛选手的各种基础综合知识，考察范围比较广。

PPC（编程类）：全称Professionally Program Coder。题目涉及到程序编写、编程算法实现。算法的逆向编写，批量处理等，有时候用编程去处理问题，会方便的多。当然PPC相比ACM来说，还是较为容易的。至于编程语言嘛，推荐使用Python来尝试。这部分主要考察选手的快速编程能力。

CRYPTO（密码学）：全称Cryptography。题目考察各种加解密技术，包括古典加密技术、现代加密技术甚至出题者自创加密技术。实验吧“角斗场”中，这样的题目汇集的最多。这部分主要考查参赛选手密码学相关知识点。

REVERSE（逆向）：全称reverse。题目涉及到软件逆向、破解技术等，要求有较强的反汇编、反编译扎实功底。需要掌握汇编，堆栈、寄存器方面的知识。有好的逻辑思维能力。主要考查参赛选手的逆向分析能力。此类题目也是线下比赛的考察重点。

STEGA（隐写）：全称Steganography。隐写术是我开始接触CTF觉得比较神奇的一类，知道这个东西的时候感觉好神奇啊，黑客们真是聪明。题目的Flag会隐藏到图片、音频、视频等各类数据载体中供参赛选手获取。载体就是图片、音频、视频等，可能是修改了这些载体来隐藏flag，也可能将flag隐藏在这些载体的二进制空白位置。有时候需要你侦探精神足够的强，才能发现。此类题目主要考查参赛选手的对各种隐写工具、隐写算法的熟悉程度。实验吧“角斗场”的隐写题目在我看来是比较全的，以上说到的都有涵盖。新手盆友们可以去了解下。

PWN（溢出）：PWN在黑客俚语中代表着攻破，取得权限，在CTF比赛中它代表着溢出类的题目，其中常见类型溢出漏洞有栈溢出、堆溢出。在CTF比赛中，线上比赛会有，但是比例不会太重，进入线下比赛，逆向和溢出则是战队实力的关键。主要考察参数选手漏洞挖掘和利用能力。

WEB（web类）：WEB应用在今天越来越广泛，也是CTF夺旗竞赛中的主要题型，题目涉及到常见的Web漏洞，诸如注入、XSS、文件包含、代码审计、上传等漏洞。这些题目都不是简单的注入、上传题目，至少会有一层的安全过滤，需要选手想办法绕过。且Web题目是国内比较多也是大家比较喜欢的题目。因为大多数人开始安全都是从web日站开始的。

四、ctf新手要具备什么知识？

（1）语言运用，编程技术

首先第一步要掌握的知识就是计算机相应的的语言，计算机语言可以分为：机器语言、汇编语言、高级语言，为什么要掌握这些语言呢？如果你都不懂计算机的每一个动作都是由语言编写的程序而来，你都看不懂这些语言又怎么可能看的懂程序呢？

（2）Web安全

ctf比赛大部分都是以web安全为主要的杯赛内容，所以学习web安全也是很有必要的。而Web安全所涉及的内容是非常广泛的，包含了：服务器、数据库、程序以及开发语言等，所以需要学习者花费更多的时间与精力去学习与掌握。

（3）安全加固

ctf比赛的核心是什么？是在于攻防，而如何防止他人轻易攻防呢？安全加固显得很有必要，如果能在长时间抵御对手的攻击，那么取得胜利的概率也就会越高。那么怎么样的加固是有效的呢？了解漏洞产生的原因，减少漏洞产生是安全加固的有效办法。

（4）密码算法

密码算法的多种多样的，那么参赛者该如何进行选择呢？参赛者可以选择一些主流的密码算法进行学习，例如：对称密码、公钥密码、流密码等。那么密码算法有什么什么样呢？在实际对战中可以用着这些算法对一些突破口与关键信息进行加密，这样对手就更难进行破解了，增加自己的赢面。

（5）网络取证

什么是网络取证呢？简单来说就是通过对面的攻击来进行分析，挖掘其中的漏洞从而打响反攻战。这一知识点说起容易做起来却要难得多。能够在越短的时间抓到线索就越能取得胜利的关键。

相信聊到这里，很多朋友都有一定的了解了吧，喜欢的朋友可以点个赞吗，感谢各位朋友的阅读，如果你有任何的建议和想法，也可以留言，我会去看每一条评论！小白在这里先感谢大家了。Respect!