CTF基础知识

原创

EV-Ain285 已于 2022-04-26 16:58:05 修改 18 收藏

文章标签： 其他

于 2022-04-26 16:55:04 首次发布

本文链接：https://blog.csdn.net/weixin_67901533/article/details/124431358

文章目录

CTF基础知识

一、简介

二、竞赛

1.解题模式

2.攻防模式

3.混合模式（Mix）

三、比赛形式

四、题目

CTF基础知识

一、简介

CTF（Capture The Flag）中文一般译作夺旗赛(不要小看这夺旗，这可不是魔兽！)，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、竞赛

1.解题模式

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。所以你要学习的东西有很多，比如Python，C，密码学等。这是考验团队，能力的综合比赛！

2.攻防模式

参赛队伍在网络内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。（有很多选手会努力让对手当机，伤敌一千，自损八百！提前建立自己的优势）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。比起之前说的解题模式，它更加考验团队与硬实力，每时每刻的攻击与防守。

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、比赛形式

CTF比赛一般分为线上赛和线下赛。通常来说，线上赛多为初赛, 线下赛多为决赛, 但是也不排除直接进行
线上：
选手通过主办方搭建的比赛平台在线注册，在线做题并提交flag，线上比赛多为解题模式，攻防模式较为少见。通常来说对于长时间未解出的题目，主办方会酌情给出提示(Hint)来帮助选手做题。
线下：
选手前往比赛所在地，现场接入比赛网络进行比赛，线下多为AWD模式，近年来随着比赛赛制的不断革新，线下赛也会出现多种模式混合进行，例如结合解题+AWD ，解题+RW 等等。

四、题目

在CTF中主要包含以下5个大类的题目，有些比赛会根据自己的侧重点单独添加某个分类，例如移动设备(Mobile), 电子取证(Forensics)等，近年来也会出来混合类型的题目，例如在Web中存在一个二进制程序，需要选手先利用Web的漏洞获取到二进制程序，之后通过逆向或是Pwn等方式获得最终flag

Web：
Web类题目大部分情况下和网、Web、HTTP等相关技能有关。主要考察选手对于Web攻防的一些知识技巧。诸如SQL注入、XSS、代码执行、代码审计等等都是很常见的考点。一般情况下Web题目只会给出一个能够访问的URL。部分题目会给出附件

Pwn：
Pwn类题目重点考察选手对于二进制漏洞的挖掘和利用能力，其考点也通常在堆栈溢出、格式化漏洞、UAF、Double Free等常见二进制漏洞上。选手需要根据题目中给出的二进制可执行文件进行逆向分析，找出其中的漏洞并进行利用，编写对应的漏洞攻击脚本(Exploit)，进而对主办方给出的远程服务器进行攻击并获取flag通常来说Pwn类题目给出的远程服务器信息为nc IP_ADDRESS PORT

Reverse：
Re类题目考察选手逆向工程能力。题目会给出一个可执行二进制文件，有些时候也可能是Android的APK安装包。选手需要逆向给出的程序，分析其程序工作原理。最终根据程序行为等获得flag

Crypto：
Crypto类题目考察选手对密码学相关知识的了解程度，诸如RSA、AES、DES等都是密码学题目的常客。有些时候也会给出一个加密脚本和密文，根据加密流程逆推出明文。

Misc：
Misc意为杂项，即不包含在以上分类的题目都会放到这个分类。题目会给出一个附件。选手下载该附件进行分析，最终得出flag
常见的题型有图片隐写、视频隐写、文档隐写、流量分析、协议分析、游戏、IoT相关等等。