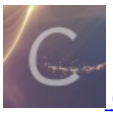
CTF介绍

原创

ST0new 于 2019-05-16 23:22:39 发布 8213 收藏 24
分类专栏： CTF 文章标签： 基础 题目类型

本文链接：https://blog.csdn.net/wang_624/article/details/90274338



前言

刚开始接触CTF,对于misc，reverse等等都傻傻分不清，所以专门去查了下这些名词，给没有接触CTF的童鞋一点入门基础。如果有不对的地方，欢迎大佬指点。

CTF是什么

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。
附上参考链接：CTF

CTF 介绍

赛事介绍

我们把CTF简称为夺旗赛，是因为出题的人把答案都放一个叫flag的文件下或者用flag{}形式展示给我们。一般是我们在某个站点或者某个文件下去寻找或分析得到的

模式介绍

一般分为三类：`解题模式`、`攻防模式`,`混合模式`

1. 解题模式

> 通过解决主办方出的题目得到相应的分数，从而获得排名。参赛有个人和团队之分。
> 赛题主要分为以下几个方向：CHOICE(比较少，适合初学者)、BASIC(这个也不多见，适合刚入门的童鞋)、WEB、REVERSE、PWN、MISC等
> 以上名词等下会有介绍

2. 攻防模式

> 一般我们叫AWD,这个模式不仅看眼技术还考验手速，参赛队伍在网络空间中互相攻击和防守，挖掘漏洞并攻击对手来得分。并防御其他对手攻击自己。攻防很考验技术和应急。也考研团队的合作能力

3. 混合模式

> 将上述的两个模式结合起来。就是两个都玩，最后用分数一较高下
> 一般更多的是国际赛的比赛方式

题型介绍

没错，这就是我刚接触最头疼的了，我内个去，这是啥啊！ 这就给你介绍介绍

1. CHOICE:选择题包含关于信息安全的各类知识点，难度系数偏低，适合刚接触信息安全的人士来全面的了解安全行业的情况
2. BASIC: 主要考察基础的计算机与网络安全知识，涉及信息发掘、搜索、嗅探、无线安全、正则表达式、SQL、脚本语言、汇编、C语言以及简单的破解、溢出等知识。旨在普及信息安全知识，引领信息安全爱好者入门
3. WEB: 考察脚本注入、欺骗和跨站等脚本攻击技术
4. REVERSE: 考察逆向破解的相关技术，要求有较高的汇编语言读写能力，以及对操作系统原理的认识
5. PWN: 考察软件漏洞挖掘、分析及利用技术，探索二进制代码背后的秘密，要求对漏洞有一定理解，掌握操作系统原理的相关知识(自我感觉最有难度的)
6. MOBILE: 考察移动终端安全相关知识
7. MISC: 即杂项，考察各种计算机系统与网络安全知识，涉及隐写术、流量分析、内核安全等信息安全的各个领域。
8. PPC:即编程类题目，题目涉及到编程算法
9. CRYPTO:即密码学，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。

> 对AWD等不过多介绍，因为我好菜啊，还没玩过，不敢发言

总结

看了这么多，大家应该知道ctf是什么了吧！那么开始起航吧，之后我会一步一脚印的更新。形成一个完整的体系。