CTF简介

原创

afei00123 于 2020-02-02 20:04:53 发布 1496 收藏 4
分类专栏： CTF

- ## CTF介绍

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。

其大致流程是，参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而夺得分数。为了方便称呼，我们把这样的内容称之为"Flag"。

CTF比赛中，比赛环境的两种方式：

1. 给予在同一局域网中的攻击机和靶场机器，以web方式可以访问攻击机，通过攻击机来渗透靶场机器，获取对应的flag值; (一般情况下给于kali linux作为攻击机，并且举办方提供计算机)。

2. 给予一个网线接口，用户自备工具，直接连接网线，进行渗透靶场机器，获取对应的flag值。

CTF比赛中涉及内容比较繁杂，我们要利用所有可以利用的方法获得flag。

- ## 解题模式CTF赛题目类别与能力对应

Web——Web应用的漏洞挖掘和利用

PWN——逆向分析、漏洞挖掘、漏洞利用、安全编程

Reverse Engineering——逆向分析、安全编程

Crypto——密码、逆向分析、安全编程

PPC(Professional Programming and Coding)——安全编程

Forensic——网络流量分析、隐写分析、系统取证等

Recon——社工、情报搜集分析