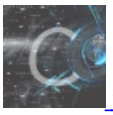
CTF 简介 竞赛流程 知识点 学习攻略

原创

SK Primin 于 2021-08-05 12:04:14 发布 589 收藏 6

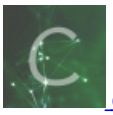
分类专栏： 笔记 ctf 文章标签： 信息安全

SKPrimn


笔记 同时被 2 个专栏收录

116 篇文章 0 订阅

订阅专栏


ctf

2 篇文章 0 订阅

订阅专栏

CTF 简介

CTF竞赛流程

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”。

单兵作战

- 理论、杂项、 web、pwn、逆向等各种题目

综合靶场

- 团队形式，攻击相同环境的靶机
- 主要是web题型
- 只需攻击不用防御针对同一个环境，越早拿到flag，获取的分数越高一台靶机通常会有多个flag flag通常放在web根目录、桌面、C盘根目录、C:\windows\system32、/、/tmp/./home等

混战模式

- 参赛团队既是攻击者也是防御者
- 通常团队通过ssh管理靶机、只有web权限 flag每隔几分钟一轮，各队有自己的初始分数，flag被其他队拿到会被扣分，拿到其他队的flag会加分主办方会队每个队伍的服务进行check , check不过会被扣分，扣除的分数由服务check正常的队伍均分。

CTF知识点

- Web
  - sql注入、xSs、文件上传、包含漏洞、xxe、ssrf、命令执行、代码审计等等
- 破解题（ Pwn ）
  - 攻击远程服务器的服务
  - 会提供服务程序的二进制文件
  - 分析漏洞并写出exp
  - 栈溢出、堆溢出
  - 绕过保护机制(ASLR,NX等)
- 逆向(Reverse)
  - 逆向，破解程序的算法来得到程序中的flag
  - 对抗反调试、代码混淆等等
- 移动安全（Mobile)
  - 主要考察选手对安卓和ios系统的理解
- 杂项(Misc)
  - 不属于上述类别或组合类别的题目统称为杂项
  - 取证（wireshark）、编解码、加解密、隐写、图片处理、压缩包、编程、…

学习攻略

资讯

- XCTF社区 | XCTF联赛对外发布及交流平台
- CTFtime.org / All about CTF (Capture The Flag)

练习平台

- GitHub - Audi-1/sqli-labs: SQLI labs to test error based, Blind boolean based, Time based.
- prompt(1) to win - 0x0
- XSS Challenges (by yamagata21)
- Hacking-Lab Cyber Range
- SegmentFault 思否
- http://captf.com/
- PentesterLab: Learn Web Penetration Testing: The Right Way

CTF-Writeup

- CTFs · GitHub
- GitHub - VulnHub/ctf-writeups: CTF write-ups from the VulnHub CTF Team
- 安全客 - 安全资讯平台 (anquanke.com)