CTF比赛总结

原创

苦行僧(csdn) 于 2021-10-16 16:16:46 发布 2800 收藏 8
分类专栏： 信息安全 文章标签： CTF

本文链接：https://blog.csdn.net/qpeity/article/details/120797861

目录

2021年10月14日，山东·青岛，中国工业互联网安全大赛核能行业赛道，上午9:00开始，下午5:30结束。本人与另外2名同事组队参加比赛，经过8个半小时的角逐，最终获得三等奖。这个系列是本次CTF比赛复盘。

一、CTF准备工作

CTF比赛时间长、无间歇、题量大、难度大。参赛选手应提前准备好常用的CTF工具，应具备快速编写脚本的能力，应做好分工配合。

二、CTF类型、工具和应对策略

CTF题目常见类别有：流量分析、逆向工程、Web漏洞、其他类型。

2.1、流量分析类

重点就是要提前准备好工具和脚本。

应关注常见协议，使用 wireshark 工具全局搜索flag，注意观察包中特别的数据。比如

{ 这类Unicode编码

http.request.method == POST ， 常见 Webshell

http.response.code == 200 ， 第一次尝试成功的访问

2.2、逆向工程类

重点就是要提前准备好工具和脚本。

1. 用ExeinfoPE、PEID、DIE等工具查壳，有壳就用工具UPX等脱壳
2. 用IDA等工具，静态分析、反编译，找flag
3. 必要时动态调试，常用工具ollydbg、x32dbg、x64dbg等

如果发现exe文件过大，那么极有可能是用 pyinstaller 打包的，用工具 pyinstxtractor.py 逆向代码。

2.3、Web漏洞

重点就是要提前准备好工具和脚本。

熟练使用 Kali 里面的工具集。

2.4、其他类型

重点就是要提前准备好工具和脚本。

图片隐写，使用binwalk或foremost工具分离。使用stegsolve工具分离图层直接找到flag。

修复文件头部信息。

使用john工具暴力破解。

三、靶场

CTF-wiki（https://ctf-wiki.github.io/ctf-wiki/）是一个关于CTF的社区项目，上面有着各个方向的学习路线与讲解。只是部分讲解并不是很清楚，需要自己多想多动手。

pwnable.tw（pwnable.tw）是一个著名的刷题网站，网站上的题目都十分有意思，可以学到许多新的东西。只是后面部分的题目并没有writeup。

Buuoj（https://buuoj.cn/challenges）是北京联合大学的CTF题目平台，上面有着各种比赛的题目环境，适合大家复现比赛的题目。

墨者学院（https://www.mozhe.cn/bug）

BugKu（https://ctf.bugku.com/）