CTF竞赛所需要的能力

原创

料理码王 于 2019-10-20 16:02:10 发布 1130 收藏 12
分类专栏： 计算机网络 生涯规划 文章标签： ctf

本文链接：https://blog.csdn.net/qq_37150711/article/details/102649894


计算机网络 同时被 2 个专栏收录
2 篇文章 0 订阅
订阅专栏


生涯规划
4 篇文章 0 订阅
订阅专栏

CTF中试题主要包括以下几类：
MISC：取证分析 内网安全 之类
PPC&CRYPTO：事件分析与解决方案 密码学原理应用
PWN：后门分析 移动终端
REVERSE：逆向工程类
WEB：网络攻防

由此可知你需要具备以下能力：

```
Web漏洞与渗透(Web)
```

操作系统和网站应用服务器安全，
网站多种语言源代码阅读分析（特别是php和java），
数据库管理和SQL语句查询，
Web漏洞挖掘和利用（SQL注入和XSS等），
各种服务器提权，
编写补丁并修复网站漏洞。

```
软件逆向 (Reverse Engineering)
```

Windows / Linux / Android 在 x86 / x86_64 / ARM平台多种编程语言的熟练掌握，
对源代码及二进制文件的分析和理解，
对多种反编译乃至反汇编逆向工具和脱壳，调试技巧的熟练掌握，
Android移动应用APK文件的逆向分析，
掌握加解密，内核编程，算法，反调试和代码混淆技术。

漏洞挖掘和利用 (Exploit)

Windows / Linux 在 x86 / x86_64 平台的二进制程序漏洞挖掘
掌握C / C++ / Python / PHP / Java / Ruby / 汇编 等语言，
掌握缓冲区溢出和格式化字符串攻击，
编写shellcode进行利用。

密码学原理及应用 (Crypto)

掌握古典密码学和现代密码学，
分析密码算法和协议，
计算密钥和进行加解密操作。

安全杂项 (Misc)

信息搜集能力，
编程能力考察，
移动（Mobile）应用安全，
隐写术和信息隐藏，
计算机取证 (Forensics) 技术和文件恢复，
网络基础以及对网络流量的分析能力。