CTF学习资料

转载

臻子007 于 2018-07-04 11:09:10 发布 2294 收藏 2

CTF 竞赛内容

因为 CTF 的考题范围其实比较宽广，目前也没有太明确的规定界限说会考哪些内容。但是就目前的比赛题型而言的话，主要还是依据常见的 Web 网络攻防、RE 逆向工程、Pwn 二进制漏洞利用、Crypto 密码攻击、Mobile 移动安全 以及 Misc 安全杂项 来进行分类。

Web - 网络攻防

主要介绍了 Web 安全中常见的漏洞，如 SQL 注入、XSS、CSRF、文件包含、文件上传、代码审计、PHP 弱类型等，Web 安全中常见的题型及解题思路，提供了一些常用的工具。

Reverse Engineering - 逆向工程

主要介绍了逆向工程中的常见题型、工具平台、解题思路，进阶部分介绍了逆向工程中常见的软件保护、反编译、反调试、加壳脱壳技术。

Pwn - 二进制漏洞利用

Pwn 题目主要考察二进制漏洞的发掘和利用，需要对计算机操作系统底层有一定的了解。在 CTF 竞赛中，PWN 题目主要出现在 Linux 平台上。

Crypto - 密码攻击

主要包括古典密码学和现代密码学两部分内容，古典密码学趣味性强，种类繁多，现代密码学安全性高，对算法理解的要求较高。

Mobile - 移动安全

主要介绍了安卓逆向中的常用工具和主要题型，安卓逆向常常需要一定的安卓开发知识，iOS 逆向题目在 CTF 竞赛中较少出现，因此不作过多介绍。

Misc - 安全杂项

以诸葛建伟翻译的《线上幽灵：世界头号黑客米特尼克自传》和一些典型 MISC 题为切入点，内容主要包括信息搜集、编码分析、取证分析、隐写分析等。