CTF概述

原创

3o3o 于 2019-11-10 09:53:43 发布

CTF介绍：

CTF（Capture The Flag）中文译作夺旗赛，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 为团队赛，通常以三人为限，要想在比赛中取得胜利，要求团队中每个人在各种类别的题目中至少精通一类，三人优势互补，取得团队的胜利。同时，准备和参与 CTF 比赛是一种有效将计算机科学的离散面、聚焦于计算机安全领域的方法。

赛事介绍：

CTF是一种流行的信息安全竞赛形式，其英文名可直译为“夺得Flag”，也可意译
为“夺旗赛”。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，内容称之为“Flag”。

CTF竞赛模式：

1. 解题模式（Jeopardy） 在解题模式CTF赛制中，参赛队伍可以通过互联网或者现场网络参与，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程
   等类别。
2. 攻防模式（Attack-Defense） 在攻防模式CTF赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。攻防模式CTF赛制可以实时通过得分反映出比赛情况，最终也以得分直接分出胜负，。
3. 混合模式（Mix） 结合了解题模式与攻防模式的CTF赛制，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。

题目类别

Reverse：
题目涉及到软件逆向、破解技术等，要求有较强的反汇编、反编译功底。
主要考查参赛选手的逆向分析能力。
所需知识：汇编语言、加密与解密、常见反编译工具
Pwn：
Pwn 在黑客俚语中代表着攻破，获取权限，在 CTF 比赛中它代表着溢出类的题目，其中常见类型溢出漏洞有整数溢出、栈溢出、堆溢出等。主要考查参赛选手对漏洞的利用能力。
所需知识：C，OD+IDA，数据结构，操作系统
Web：
Web 是 CTF 的主要题型，题目涉及到许多常见的 Web 漏洞，如 XSS、文件包含、代码执行、上传漏洞、SQL 注入等。也有一些简单的关于网络基础知识的考察，如返回包、TCP/IP、数据包内容和构造。
所需知识：PHP、Python、TCP/IP、SQL
Crypto：
题目考察各种加解密技术，包括古典加密技术、现代加密技术甚至出题者自创加密技术，以及一些常见编码解码。
所需知识：矩阵、数论、密码学
Misc：
Misc 即安全杂项，题目涉及隐写术、流量分析、电子取证、人肉搜索、数据分析、大数据统计等，覆盖面比较广。
所需知识：常见隐写术工具、Wireshark 等流量审查工具、编码知识
Mobile：
主要分为 Android 和 iOS 两个平台，以 Android 逆向为主，破解 APK 并提交正确答案。
所需知识：Java，Android 开发，常见工具等。

竞赛须知：

> web 主要是向目标服务器发送 http 请求，返回 flag
>
> bin 主要是通过 exploit 脚本读取 /home/username 下某个文件夹下的 flag 文件。
>
> 出题人自己写的 CMS 或者魔改后的 CMS(注意最新漏洞、1day 漏洞等)。
>
> 框架型漏洞(CI等)。

AWD 模式生存技巧：

1.漏洞反应能力。
2.快速编写脚本。
3.web代码审计。
3. web 比较容易抓取流量，所以即使被打，我们也可以及时通过分析流量去查看别的队伍的 payload，从而进行反打。
4. 脚本准备：一句话，文件包含，不死马、禁止文件上传等。
5. 警惕 web 弱口令，用最快的速度去补。

Bin 题目类型：

1.大部分是 PWN，题目类型包括栈、堆、格式化字符串等等。
竞赛能力：
2.迅速找到二进制文件的漏洞，迅速打 patch 的能力。
3.全场打 pwn 的 exp 脚本编写。
4.熟悉服务器运维，尽快摸清楚比赛的 check 机制。
5.如果二进制分析遇到障碍难以进行，那就去帮帮 web 选手运维。
看看现场环境是否可以提权，这样可以方便我们操作（如魔改 libc 等等）。

小技巧：
1.如果自己拿到 FB， 先用 NPC 服务器或者自己服务器测试，防止自己的 payload 被抓取到, 写打全场的 exp（漏洞利用程序） 时，一定要加入混淆流量。
2.提前准备好 PHP （提示文件不存在）一句话木马等等脚本。
3.小心其他队伍恶意攻击使我们队伍机器的服务不能正常运行，因此一定要备份服务器的配置。
4.尽可能在不搞崩服务和绕过 check 的情况下，上 WAF，注意分析别人打过来的流量，如果没有混淆，可以大大加快我们的漏洞分析速度。
5.工具准备: 中国菜刀、 Nmap、Xshell、 合适的扫描器等。
6.关注 Github 等平台，可能会有写好的 exp 可以用。
7.将 flag 的提交自动化。
8.平衡心态。