CTF基本赛制与题型

原创

彬彬有礼am_03 于 2021-08-23 10:50:22 发布 708 收藏 3

分类专栏： CTF基础

本文链接：https://blog.csdn.net/am_03/article/details/119864475

CTF简介

CTF的全称为Capture The Flag,即夺旗赛。CTF竞赛活动蓬勃发展，已成为了锻炼信息安全技术，展现安全能力和水平的绝佳平台。

CTF号称计算机界的奥林匹克。

CTF目标：

CTF参赛队伍的目标为获取尽可能多的flag。参赛队伍需要通过解决信息安全的技术问题来获取flag。

flag可能来自于一台远端的服务器，一个复杂的软件，也可能隐藏在一段通过密码算法或者协议加密的数据，或一个网络流量及音频视频文件里。选手需要结合利用自己掌握的安全技术，并辅以快速掌握新知识，通过获取服务器权限，分析并破解软件或设计解密算法等不限定途径来获取flag。

CTF的比赛形式

1.解题模式：通常为在线比赛，目前大多数CTF比赛的主流形式，选手自由组队参赛（在线比赛人数一般不做限制）。题目通常在比赛过程里陆续放出。接触一道题目后，提交题目对应的flag即可得分，比赛结束后分高者胜。

2.攻防模式：通常为现场比赛，多数CTF决赛的比赛形式，选手自由组队参赛，但通常队伍人数会受到限制（3～8不等）。相比于解题模式，时间更短，比赛里更关注临场反应和解题速度，需要能够快速攻击目标主机并获取主机的权限，考察团队多方面的整合安全能力。

CTF解题模式的题目类型：

1.web安全：

通过浏览器访问题目服务器上的网站，寻找网站漏洞(sql注入,xss,文件上传,包含漏洞,xxe,ssrf,命令执行,代码审计等)，利用网站漏洞获得服务器的部分或全部权限，拿到flag，通常包含分值最大的web渗透题；

2.逆向工程(Reverse):

题目就是一个软件，但通常没有软件的源代码；需要利用工具对软件进行反编译甚至反汇编，从而理解软件内部逻辑和原理，找出与flag计算相关的算法并破解这个算法，获取flag；

3.漏洞挖掘与漏洞利用(PWN,EXPLOIT)(最难):

访问一个本地或远程的二进制服务程序，通过逆向工程找出程序里存在的漏洞，并利用程序里的漏洞获取远程服务器的部分或者全部权限，拿到flag；

4.密码学(Crypto):

分析题目里的密码算法与协议，利用算法或者协议的弱点来计算密钥或对密文进行解密，从而获取flag。

5.调查取证(Misc)(题目简单):

利用隐写术等保护技术将信息隐藏在图像,音频,视频,压缩包里，或者信息就在一段内存镜像或者网络流量里，尝试将隐藏的信息回复出来即可获得flag。

6.移动安全(Mobile)(题目少):

对安卓和IOS几个系统的理解，逆向工程等知识。

各题型排序(从简到难):

1.Misc->杂项
2.Crypto->密码学
3.Web->Web安全
4.Reverse->逆向工程
5.PWN->二进制

CTF 方向都玩一遍，选1个你最喜欢的、编程基础非常重要，选1个你最喜欢的。

应届生招聘需求：

安全服务工程师，安全工程师，渗透测试工程师

安全岗位核心技能需求：

熟悉Web渗透测试方法和攻防技术，包括SQL注入，XSS跨站，CSRF伪造请求，命令执行等OWSP TOP10安全漏洞与防御，有一些程度上的漏洞分析和挖掘能力；
熟悉Linux，Windows不同平台的渗透测试，了解常用Web框架，数据库，之间件和操作系统的弱点以及相关攻防技术；
熟悉主流安全工具，包括Kali linux,Metasploit,Nessus,Nmap,AWVS,Burp,Appscan等；
熟悉一门编程语言：如C/Python/PHP/Java等，有一些程度上的代码编写能力