CTF简介

原创

心酸是我 于 2020-01-15 11:24:52 发布 282 收藏

1、什么是ctf？
CTF（capture the flag）中文一般译为夺旗赛，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。

2、竞赛模式
（1）解题模式
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，这种模式的CTF竞赛与ACM编程竞赛。信息学奥赛比较类似，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在选拔比赛。题目主要包括逆向，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 - Dfense）
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进行攻击对手服务来的分，修补自生服务漏洞进行防御来避免丢分。攻防模式CTF赛制可以实现通过得分反应出比赛情况，最终也以得分直接分出胜负，是一种竞争激烈，具有很强观赏性和高度透明性的网络安全赛制。在这种赛制中，不仅仅是比赛队员的智力和技术，也比体力（因为比赛一般都会持续48小时及以上），同时也比团队之间的分工配合与合作。
（3）混合模式（min）
3、题目类别
（1）WEB(网络安全)
web是CTF竞赛的主要题型，题目涉及到许多常见的WEB漏洞，比如XXS、文件包含、代码执行、上传漏洞、SQL注入。也有一些简单的关于网络基础只是考察，例如返回包、TCP-IP。数据包内容和构造。可以说题目环境比较接近真实环境。
所需要的知识：PHP、Python、TCP-IP、SQL
（2）MISC（安全杂项）
NISC即安全杂项，题目涉及到隐写术、流量分析、电子取证、人肉搜索、数据分析、大数据统计等等、覆盖面比价广，主要考察选手的各种基础综合知识。
所需知识：常见隐写术工具、wireshark等流量审查工具、编码知识。
（3）Crypto(密码学)
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，主要考察选手密码学相关知识点，通常也会和其他题目相结合。
所需知识：矩阵、数论、古典密码学
（4）Reverse(逆向工程)
题目涉及到软件逆向、破解技术等，要求有较强的反汇编，反编译扎实功底。主要考察选手的逆向分析能力。
所需知识：汇编语言、加密解密、常见反编译工具
（5）PPC（编程类题目）
题目涉及到程序编写、编程算法实现，当然PPC相比ACM来说，还是较为容易，至于编程语言：推荐使用Python来尝试。
所需知识：基本编程思路，C、C++、Python、PHP
(6)PWN(二进制安全)
PWN在黑客俚语中代表着攻破，取得权限，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栈溢出、堆溢出。蛀牙考察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
4、国内外赛事
国外：
•DEFCON CTF：CTF赛事中的“世界杯”
•·
UCSB iCTF：来自UCSB的面向世界高校的CTF
•·
Plaid CTF：包揽多项赛事冠军的CMU的PPP团队举办的在线解题赛
•·

Boston Key Party：近年来崛起的在线解题赛

•·

Codegate CTF：韩国首尔“大奖赛”，冠军奖金3000万韩元

•·

Secuinside CTF：韩国首尔“大奖赛”，冠军奖金3000万韩元

•·

XXC3 CTF：欧洲历史最悠久CCC黑客大会举办的CTF

•·

SIGINT CTF：德国CCCAC协会另一场解题模式竞赛

•·

Hack.lu CTF：卢森堡黑客会议同期举办的CTF

•·

EBCTF：荷兰老牌强队Eindbazen组织的在线解题赛

•·

Ghost in the Shellcode：由Marauders和Menin Black Hats共同组织的在线解题赛

•·

RwthCTF：由德国0ldEur0pe组织的在线攻防赛

•·

RuCTF：由俄罗斯Hackerdom组织，解题模式资格赛面向全球参赛，解题攻防混合模式的决赛面向俄罗斯队伍的国家级竞赛[2]

•·

RuCTFe：由俄罗斯Hackerdom组织面向全球参赛队伍的在线攻防赛

•·

PHD CTF：俄罗斯Positive Hacking Day会议同期举办的CTF

国内： •XCTF全国联赛

•中国网络空间安全协会竞评演练工作组主办、南京赛宁承办的全国性网络安全赛事平台，2014-2015赛季五站选拔赛分别由清华、上交、浙大、杭电和成信技术团队组织（包括杭电HCTF、成信SCTF、清华BCTF、上交0CTF和浙大ACTF），XCTF联赛总决赛由蓝莲花战队组织。XCTF联赛是国内最权威、最高技术水平与最大影响力的网络安全CTF赛事平台。

•AliCTF

•由阿里巴巴公司组织，面向在校学生的CTF竞赛，冠军奖金10万元加BlackHat全程费用。

•XDCTF

•由西安电子科技大学信息安全协会组织的CTF竞赛，其特点是偏向于渗透实战经验。

•HCTF

•由杭州电子科技大学信息安全协会承办组织的CTF

•杭州电子科技大学信息安全协会由杭州电子科技大学通信工程学院组织建立，协会已有七年历史，曾经出征DEFCON,BCTF等大型比赛并取得优异成绩，同时协会还有大量有影响力的软件作品。协会内部成员由热爱黑客技术和计算机技术的一些在校大学生组成，有多个研究方向，主要有渗透，逆向，内核，web等多个研究方向。至今已经成功举办6次CTF比赛。

•ISCC

•由北理工组织的传统网络安全竞赛，最近两年逐渐转向CTF赛制。

•TCTF

•TCTF由中国网络空间安全协会竞评演练工作委员会指导、腾讯安全发起、腾讯安全联合实验室主办，0ops战队和北京邮电大学协办的CTF竞赛.