CTF介绍

转载

lixue20141529 于 2017-09-09 17:52:49 发布 2124 收藏 4
分类专栏： 网络安全 文章标签： 安全


网络安全 专栏收录该内容
12 篇文章 1 订阅
订阅专栏

转自：http://tieba.baidu.com/p/3933947157

CTF（Capture The Flag）中文一般译作夺旗赛，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起源于1996年DEFCON全球黑客大会，以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式，2013年全球举办了超过五十场国际性CTF赛事。而DEFCON作为CTF赛制的发源地，DEFCON CTF也成为了目前全球最高技术水平和影响力的CTF竞赛，类似于CTF赛场中的“世界杯”。

1赛事介绍

CTF竞赛模式分为以下三类：

一、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，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。

二、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，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，不仅仅是比参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。

三、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。采用混合模式CTF赛制的典型代表如iCTF国际CTF竞赛。

2国际知名CTF赛事

根据CTFTIME提供的国际CTF赛事列表，包括已完成的赛事和即将开赛的赛事。此外也根据社区反馈为每个国际CTF赛事评定了权重级别，权重级别大于或等于50的重要国际CTF赛事包括：

· 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Men in 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
· 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

3国内知名CTF赛事

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、KEEN TEAM协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联赛提供100万元奖励池，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

4国内外知名CTF战队

PPP –近几年崛起的超神明星战队，来自美国CMU，队内有Geohot神奇小子和Ricky两位国际最高水平黑客作为双子领军，2014年PPP包揽了GitS和CodeGate冠军，CTFTIME全球排名仅次于Dragon Sector排名第二，Geohot神奇小子的单人队tomcr00se（没错，他就自称网络空间的汤姆克鲁斯）在大满贯赛Boston Key Party和大奖赛Secuinside，击败其他多人战队拔得头筹。由Geohot神奇小子加盟2013年DEFCON CTF总决赛冠军阵容，PPP战队再度卫冕2014年总决赛冠军。

Blue-Lotus –来自中国大陆的安全宝·蓝莲花战队。2013年历史性地作为华人世界首次入围DEFCON CTF总决赛的队伍，并在决赛获得第11名，八支首次入围决赛战队中名次仅次于澳大利亚9447的较好成绩。2014年 在成功举办首届BCTF全国网络安全技术对抗赛后，连续第二次闯入DEFCON总决赛，并获得第五名的优秀成绩。2014年国际CTF战绩包括ASIS CTF资格赛第3名、PlaidCTF/CodeGate八强，在CTFTIME全球排名第16位，亚洲战队第2（仅次于韩国penthackon）。

Men in the Blackhats – 来自美国传统强队Hates Irony分拆的战队，Hates Irony战队先前在2011年和2012年资格赛中都位居第一，并在2011年总决赛中获得季军，2013年DEFCON总决赛亚军队伍，2014年DEFCON总决赛第六名，实力和经验都不容小觑的一支战队。

More Smoked Leet Chicken – 简称MSLC，俄罗斯的传统强队，由两支队伍Leet More和Smoked Chicken合并而成。2014年DEFCON以RuCTFe大满贯赛冠军入围总决赛，在已获得入围资格时也参加了资格赛，获得第7名。MSLC战队在2012年曾狂揽七项CTF赛冠军，但近两年被美国PPP和波兰Dragon Sector等强队压制，少有冠军战绩，2013年DEFCON总决赛获得第4名，2014年DEFCON总决赛下滑至第12名。2014年CTFTIME全球排名第3位。

Dragon Sector – 来自波兰Google Security Team的强队，今年狂揽六项CTF赛冠军，CTFTIME全球排名力压PPP（但是积分和没有PPP+Tomc00se高），占据积分榜首位。2014年DEFCON CTF总决赛获得季军。

StratumAuhuur – 来自德国的战队，由Stratum0和CCCAC联盟组成，以大满贯赛Boston Key Party亚军（冠军被神奇小子Geohot单人队Tomc00rse摘走）获得总决赛入场券。今年国际CTF赛事多次屈居亚军，全球CTFTIME排名第4位，首次入围DEFCON总决赛，并获得第8名的较好名次。

HITCON – 来自中国宝岛台湾的队伍，主力为台湾大学学生，在蓝莲花战队组织的首届BCTF全国网络安全技术对抗赛获得冠军，之后在DEFCON CTF资格赛最后时刻逆袭得分，突入DEFCON总决赛，成为台湾地区首次入围决赛的队伍。2014年获得ASIS CTF资格赛第一名，并在DEFCON总决赛中以大黑马姿态获得亚军。

Shellphish– 来自美国UCSB大学的传统强队，也是历史最悠久的全球高校CTF夺旗赛iCTF的组织者，曾于2005年在DEFCON CTF总决赛夺冠，2011年和2012年在CTF总决赛排名都是第9位，2013年第7名。

raon_ASRT – 2013年DEFCON CTF总决赛的季军队伍，来自韩国RAON公司安全研究院的团队，其中两位核心人员是由韩国Best of Best白帽计划培养的天才少年。2013年Codegate决赛冠军队，Secuinside决赛亚军，2014年Nuit du Hack CTF季军。Raon_ASRT也是今年Secuinside大奖赛的组织者。2014年DEFCON CTF总决赛第7名。

9447– DEFCON CTF总决赛唯一一支来自南半球的队伍，源自澳大利亚UNSW大学，由IT安全讲师Fionnbharr Davies以一门课程9447为基础发展起来的新锐战队，2013年刚一成立便晋级DEFCON总决赛，并在总决赛中获得第10名的好成绩。今年更是以资格赛第3名的好成绩入围总决赛，并获得第9名。

KAIST GoN – 韩国传统的CTF强队，以韩国科学技术院（KAIST）学生为主力，在2013年缺席总决赛之后，2014以资格赛第8名回归。
，DEFCON CTF总决赛获得第10名。

[SEWorks]penthackon – 以大满贯赛Olympic CTF亚军（冠军是Dragon Sector）身份获得2014年DEFCON CTF总决赛入场券，获得。目前CTFTIME全球排名第7位。SEWorks是韩国一家Mobile Security的公司，公司创始人也是五届入围DEFCON总决赛WOWHackers战队的创始人。Binja – 队名含义为“二进制忍者”，以日本传统CTF强队Sutegoma2为班底，加上katagaitai和EpsilonDelta组建的一支新战队，2014年以大奖赛Secuinside第4名成绩（前三名分别为TomC00se单人队、CodeRed和MSLC）抓住了进军DEFCON总决赛最后的救命稻草，在总决赛排名第13名。Sutegoma2的队名含义为日本“将棋”中的一种常见手筋“退路舍驹”，成员也以安全公司技术人员为主，2011年DEFCON 19首次打入总决赛，已经是连续第四届入围总决赛，2013年总决赛排名第6名。

0ops – 上海交通大学信息网络安全协会组织的CTF战队，姜开达老师作为领队。队长Slipper、副队长Lovelydream曾是蓝莲花战队队员。2013年9月成立后即积极参与国际知名CTF赛事，曾在Hack.Lu在线夺旗赛中获得季军，成功组织过0CTF、ISG等国内知名的CTF赛事。

针对CTF，大家都是怎么训练的？
作者：4ido10n
1.CTF起步指南：如何开始CTF比赛之旅http://blog.idf.cn/2014/06/how-to-get-started-in-ctf/
2.网站：FreeBuf、 乌云 等等
3.逆向：看雪学院 CrackMe(http://www.crackmes.de/)、BLACKBOX、reversing.kr （下面会放两张图更多说明）
4.Web：web安全入门 http://blog.sycsec.com/?p=166
4.杂志《安全参考》《乌云月报》《黑客防线》《黑客x档案》.....
5.博客 一蓑烟雨等各安全大牛博客，暂时不一一列举。切题相关，217's Blog(http://217.logdown.com/)、0ops's Blog(http://blog.0ops.net/).....
6.writeup参考 CTF Writeup Summary [CTF Writeup Summary](http://sec.yka.me/)、writeup">//**/(http://www.hackdog.me/writeup/).....
7.题库：下面又会“有一些可以去玩的地方CTF”更详细说明

一些可以去玩的地方CTF
作者：L3m0n 0xmuhe 4ido10n
综合：
http://wargame.kr/
西普学院
http://www.simplexue.com/CTF.html
http://canyouhack.it/
http://fun.coolshell.cn/
网络信息安全攻防学习平台 http://hackinglab.cn/
idf实验室
http://ctf.idf.cn/
wechall

http://www.wechall.net/
合天
http://erange.heetian.com/
jctf
http://ctf.3sec.cn/
http://oj.xctf.org.cn/
补：i春秋中也有CTF
http://www.ichunqiu.com/

渗透:
米安网
http://ctf.moonsos.com/pentest/index.php
http://webhacking.kr/
四叔叔写的一个
http://hackit.sinaapp.com/

xss:
http://prompt.ml/0
http://xss.pkav.net/xss/

sql:
http://redtiger.labs.overthewire.org/

逆向:

http://reversing.kr/
http://pwnable.kr/
http://exploit-exercises.com/
http://overthewire.org/

各种writeup
https://github.com/ctfs/
bin干货区
http://security.cs.rpi.edu/courses/binexp-spring2015/

各种赛事预告
https://ctftime.org/event/list/upcoming

来自：http://bbs.secbox.cn/thread-38-1-1.html

http://overthewire.org
都是Bin http://pwnable.kr
还是Bin http://exploit-exercises.com
都是re，http://reversing.kr
bin干货区
http://security.cs.rpi.edu/courses/binexp-spring2015/
XCTF的OJ平台也可以玩玩 http://oj.xctf.org.cn/

乌云XSS互动学习平台 http://xss.pkav.net/xss/
补：脑洞题，严格上不算CTF，但是可以玩玩
http://cafebabe.cc/nazo/
暂时就这些了，想到在补充...