NUIST CTF大赛说明文档

### CTF赛事简介

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” 。

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。为了方便称呼，我们把这样的一定格式的字符串内容称之为“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，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。

* 1. 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。

* 1. 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。

### 国内外知名赛事

* 1. 国外赛事
     + 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
  2. 国内赛事
* 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

2015年之前由西安电子科技大学信息安全协会与西安电子科技大学组织的CTF竞赛，其特点是偏向于渗透实战经验。2016年之后由西安电子科技大学组织举办。

* 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。

* LCTF

由L-Team战队组织的CTF竞赛。

* 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. [3]

* 百度杯CTF夺旗大战

由百度安全应急响应中心和i春秋联合举办的CTF比赛，国内现今为止首次历时最长（半年）、频次最高的CTF大赛。赛题丰富且突破了技术和网络的限制。

* 全国大学生信息安全竞赛创新实践能力赛线上赛

由教育部高等学校信息安全专业教学指导委员会主办，西安电子科技大学、永信至诚、国卫信安等承办;百度安全中心、阿里安全应急响应中心、腾讯安全平台方舟计划、360企业安全集团赞助支持的CTF竞赛，覆盖面广，质量级别最高，被参赛选手称作CTF的国赛。

### 赛事涵盖内容

* 1. MISC（安全杂项）：

全称Miscellaneous。题目涉及流量分析、电子取证、人肉搜索、数据分析、大数据统计等等，覆盖面比较广。列如社工类题目；依据流量包分析的题目；取证分析题目。主要考查参赛选手的各种基础综合知识，考察范围比较广。

* 1. PPC（编程类）：

全称Professionally Program Coder。题目涉及到程序编写、编程算法实现。算法的逆向编写，批量处理等。PPC相比ACM来说，还是较为容易的。但是更多的考验选手的快速编程能力。

* 1. CRYPTO（密码学）：

全称Cryptography。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。列如给选手加密算法的源码，或者可执行文件。要求选手反推出解密算法，对给出的密文进行解密。

* 1. REVERSE（逆向）：

全称reverse。题目涉及到软件逆向、破解技术等，要求有较强的反汇编、反编译扎实功底。需要掌握汇编，堆栈、寄存器方面的知识。有好的逻辑思维能力。主要考查参赛选手的逆向分析能力。此类题目也是线下比赛的考察重点。

* 1. STEGA（隐写）：

全称Steganography。将隐写技术应用到实战的一种方式。题目的Flag会隐藏到图片、音频、视频等各类数据载体中供参赛选手获取。载体就是图片、音频、视频等，此类题目主要考查参赛选手的对各种隐写工具、隐写算法的熟悉程度。

* 1. PWN（溢出）：

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。在CTF比赛中，逆向和溢出则是战队实力的关键。主要考察参数选手漏洞挖掘和利用能力。

* 1. WEB（web类）：

WEB应用在今天越来越广泛，也是CTF夺旗竞赛中的主要题型，题目涉及到常见的Web漏洞，诸如注入、XSS、文件包含、代码审计、上传等漏洞。这些题目要求选手对各类基础web协议有详尽的了解。熟悉各类后端语言，列如PHP，Java，Python，ASP等等。了解网站的基本运作原理，熟悉HTML，JS。以及各类常见漏洞。

* 1. 人工智能方向

随着人工智能的，深度学习技术的兴起。人们对人工智能安全意识的提升。人工智能安全题型也开始逐渐出现在各类大型CTF赛事中。这类赛事通常是以构造合适的攻击样本以达到欺骗人工智能的目的，来最终获取flag。相信未来随着人工智能的越发火热，这类题型将逐渐进入各类CTF赛事中。

### 举办赛事的影响

* 1. 贯彻落实党的十九大和全国网信工作会议精神，为我校网络安全人才展示水平、竞技比拼和交流互动提供舞台，发现、聚集和培养网络安全人才，为加快南京信息工程大学网络安全人才队伍建设作出贡献。
  2. 推广信息安全概念，提升广大学生的信息安全意识。增强信息安全能力。
  3. 让学生学以致用，增强动手实践能力。CTF赛事一向是一个注重动手操作实践能力的比赛。选手需要以灵活的思维多角度思考题目，需要较强的编程能力和理论实践能力来攻破赛题难关。
  4. 通过CTF赛事，提升我校在信息安全专业领域的知名度和影响力，让更多的学生了解信息安全赛事。
  5. 推广信息安全专业在校级层面的认知程度。普及基础的信息安全概念。
  6. 以赛代练，以赛促学。
  7. 增进交流氛围，培养团队意识
  8. 选拔优秀信息安全人才，加入信息安全小组，为今后参加各类其他CTF赛事准备新鲜血液

### 本次大赛筹备计划

* 1. 赛事准备
     1. 成立赛事筹备小组
     2. 确定比赛时间，联系比赛场地
     3. 准备宣传文案
     4. 筹备小组命题，设备调试
  2. 赛事预热
     1. 发布信息公告
     2. 利用校级媒体宣传
     3. 统计报名信息
  3. 比赛期间
     1. 赛前基础知识培训，包括基本赛制讲解，比赛环境使用等等。
     2. 筹备小组负责比赛期间的设备运维，环境运维，以及疑难解答。以及各类突发状况的应对。
  4. 比赛结束
     1. 统计比赛结果，记分排名
     2. 颁奖
     3. 吸纳竞赛成绩优秀者，代表学校参加各类校外赛事。