Creative Education Studies 创新教育研究, 2023, 11(9), 2578-2584
Published Online September 2023 in Hans. https://www.hanspub.org/journal/ces
https://doi.org/10.12677/ces.2023.119380

基于CTF赛题分析的网络安全学科知识体系研究

吴　昊

西安邮电大学网络空间安全学院，陕西　西安

收稿日期：2023年7月14日；录用日期：2023年8月28日；发布日期：2023年9月6日

摘　要

学科竞赛是实践教学的有效载体，对培养网络安全人才具有重要意义。参赛者通过竞赛的实践可以巩固和应用所学的知识，解决实际问题，提升自身的专业技能水平和创新实践能力。通过对近年各项CTF竞赛赛题的收集、处理与统计，深入地剖析了信息安全竞赛所考查的知识体系，挖掘CTF竞赛的潜力，探索更好的方法来培养网络安全人才的技能，以满足不断增长的网络安全人才需求。

关键词

CTF，网络安全学科，知识体系，知识领域

Research on the Knowledge System of Network Security Subject Based on CTF Question Analysis

Hao Wu

School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an Shaanxi

Received: Jul. 14th, 2023; accepted: Aug. 28th, 2023; published: Sep. 6th, 2023

Abstract

Subject competitions are an effective carrier of practical teaching and are of great significance for cultivating network security talents. Participants can consolidate and apply their learned knowledge, solve practical problems, and enhance their professional skills and innovative practical abilities through competition practice. Through the collection, processing, and statistics of various CTF competition questions in recent years, this paper deeply analyzes the knowledge system ex-

文章引用: 吴昊. 基于 CTF 赛题分析的网络安全学科知识体系研究[J]. 创新教育研究, 2023, 11(9): 2578-2584.
DOI: 10.12677/ces.2023.119380

amined in information security competitions, explores the potential of CTF competitions, and explores better methods to cultivate the skills of network security talents to meet the growing demand for network security talents.

Keywords

CTF, Network Security Discipline, Knowledge System, Knowledge Domain

1. 引言

网络安全作为一门新兴专业，新概念层出不穷、新技术发展迅速、新需求不断涌现，对抗性特别突出，网络安全人才培养更需要紧跟技术前沿，更需要高水平对抗实践训练[1]。在网络人才培养过程中，如何提高学生实战对抗能力一直是各方关注的重点。近年来，CTF (Capture The Flag)竞赛成为培养学生网络实战对抗能力的重要载体，其特点是多种多样的任务，从利用网站、破解密码到破坏不安全的网络。这些高水平 CTF 竞赛活动给学生提供了难得的网络实战对抗训练机会，可以帮助学生了解技术发展前沿，提高实战对抗能力。

ACM 和 IEEE 发布的 CSEC2017 [2]，是国际上具有较高权威性的网络安全学科知识体，具有比较悠久的历史渊源和广泛的代表性。本文旨在研究将各类 CTF 竞赛赛题映射到 CSEC2017 课程指南课程的不同知识领域和知识单元中去，以更好地在今后的课程和实践教学中积极融入 CTF 元素，以 CTF 竞赛促进网络安全人才培养质量提升。

2. CTF 竞赛简介

2.1. CTF 竞赛模式

CTF 一词最初指的是一种两支队伍参加的户外比赛，每个队必须保护自己所在的基地一面(物理)旗帜，同时设法夺取对方的旗帜[3]。自 20 世纪 90 年代以来，这个比赛转移到了网络空间上。CTF 可以在各种技术平台上举办，既可以线上，也可以线下进行比赛。CTF 最常见的形式是解题模式和攻防模式。

在解题模式 CTF 中，参与者从不同类别的挑战中选择题目作答，如密码学、逆向工程或获得服务的所有权(即 PWN)，每项挑战通常都有不同的得分。参与者在自己的计算机上本地解决挑战或与远程服务器交互。例如，参与者收到一个包含加密标志的二进制文件，他们必须设法解密得到该标志。

在攻防模式 CTF 中，每个参与者团队控制并维护一个相同的计算机网络。网络中的主机运行着各种易受攻击的服务，每个团队的目标是在利用其他团队服务中的漏洞的同时，设法修补自身网络服务以保护网络资产。最后根据漏洞利用情况和防御对策效果进行综合评分。

2.2. CTF 竞赛的意义

CTF 竞赛是将网络安全学科知识应用于实践的平台[4]。参赛者需要运用密码学、漏洞分析、逆向工程、网络协议等各个方面的知识来解决比赛中的各种问题和挑战。通过参加 CTF 竞赛，学习者能够巩固理论知识，并将其应用于实际的场景中，提升对网络安全领域的认识和理解。

其次，CTF 竞赛对于网络安全学科知识的学习提供了实践的方向。网络安全学科庞杂且涵盖面广，学习者在面对大量的理论知识时，可能感到困惑和无从下手。通过网络安全课程和 CTF 竞赛在形式和内容上进行结合，以实践的方式引导学习者深入学习和理解各个知识点，建立一套侧重于实践的教学体系，从教学计划、教学方法、考核形式、师资队伍、配套平台等方面进行改革，有助于培养学生既具有扎实理论基础，又能通过解决实际问题来增强技能[5]。

此外，CTF 竞赛还可以推动网络安全学科的发展和创新。竞赛中的问题和挑战通常都是实际场景中的真实问题，参赛者需要发挥创造力和创新能力来解决这些问题。通过比赛中的实践和反思，参赛者可以发现新的漏洞、提出新的攻击和防御方法，为网络安全学科的发展做出贡献。

3. 网络安全课程体系 CSEC2017 简介

CSEC2017 是由美国计算机学会(ACM)、电子电器工程师协会、计算机学会(IEEE-CS)、信息系统协会安全专业工作组(AIS SIGSEC)、国际信息处理联合会信息安全教育技术委员会(IFIP WG 11.8)等机构组成的国际联合工作组经过两年多的努力开发而成，是一套面向本科教育的网络空间安全学科知识体系。CSEC2017 将网络空间安全分为数据、软件、组件、连接、系统、人、组织、社会安全共八大知识领域，每个知识领域包含不同的技能和知识。具体包括：

1) 数据安全：重点是数据存储和传输过程中的安全保护及其支撑的相关基础理论，关键知识包括密码学、端到端安全通信、数字取证、数据完整性与认证、信息存储安全等。

2) 软件安全：重点是从软件的开发与使用的角度，保证相关的信息和系统的安全，关键知识包括基本设计原则、安全需求及其在设计中的作用、实现问题、静态与动态分析、配置与打补丁、伦理(尤其是开发、测试和漏洞披露方面)等。

3) 组件安全：重点是系统中的组件在设计、制造、采购、测试、分析与维护等方面的安全问题，关键知识包括系统组件的漏洞、组件生命周期、安全组件设计原则、供应链管理、安全测试、逆向工程等。

4). 网络连接安全：重点是组件之间连接时的安全问题(物理连接与逻辑连接的安全问题)，关键知识包括系统及体系结构及模型及标准、物理组件接口、软件组件接口、连接攻击、传输攻击等。

5) 系统安全：重点是由组件连接构成的系统整体安全问题，关键知识包括整体方法论、安全策略、身份认证、访问控制、系统监测、系统恢复、系统测试、文档支持等。

6) 人员安全：重点是用户的个人数据隐私保护和安全威胁化解及用户的行为、知识和隐私对网络空间安全的影响，关键知识包括身份管理、社会工程、意识与常识、社交行为的隐私与安全、个人数据相关的隐私与安全等。

7) 组织安全：重点是各种组织在网络空间安全威胁面前的保护问题及组织的任务所要进行的风险管理，关键知识包括风险管理、安全治理与策略、法律和伦理及合规性、安全战略与规划等。

8) 社会安全：重点是网络空间安全问题对整个社会产生的广泛影响，关键知识包括网络犯罪、网络法律、网络伦理、网络政策、隐私权等。

以上每个知识领域又由若干知识单元组成，每个知识单元又包含一系列知识主题。总体上来说，8 个知识领域共有 55 个知识单元和 287 知识主题。

4. 近年 CTF 竞赛赛题相关知识领域分析

4.1. 赛题知识领域分析方法

文献[6]通过对 CTF 的题解的分析，研究 CTF 竞赛时需要学习的各种基本技能和知识。我们借鉴该研究方法，对 2016~2022 年国内进行的各项 CTF 竞赛的共 23,632 道赛题题解进行分析，将每道赛题考察

的知识点映射到 CSEC2017 课程指南的不同知识领域和知识单元，对 CTF 竞赛涉及的相关知识领域进行了统计。图 1 显示了数据分析的整体流程：

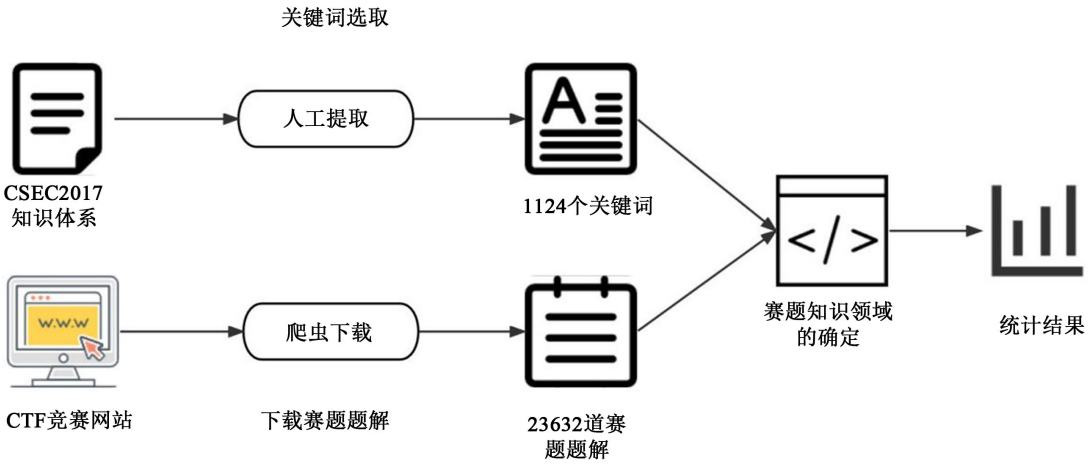

Figure 1. Analysis process of knowledge domain in competition questions
图 1. 赛题知识领域分析流程

1) 关键词选取：我们从 CSEC2017 的 8 个知识领域分别选取了一定数量的中英文关键词，总计 1124 个，包括日志、加密、解密、漏洞、逆向、exploit、pwn、http 等。为了避免重复，我们将每个关键字单独归属于一个知识领域的一个知识单元的一个主题，并建立了类似图 2 的关键词与知识领域的对应关系。知识领域 KA_1 由 3 个知识单元 KU_1、KU_2 和 KU_3 组成，KU_1 下设 KT_1 和 KT_2 两个主题，KU_2 和 KU_3 分别只有 KT_3 和 KT_4 一个主题。和 KT_1 相关联的两个关键字是 k_1 和 k_2，和 KT_2 相关联的关键字为 k_3，和 KT_3 相关联的两个关键字是 k_4 和 k_5，和 KT_4 相关联的关键字是 k_6、k_7 和 k_8。

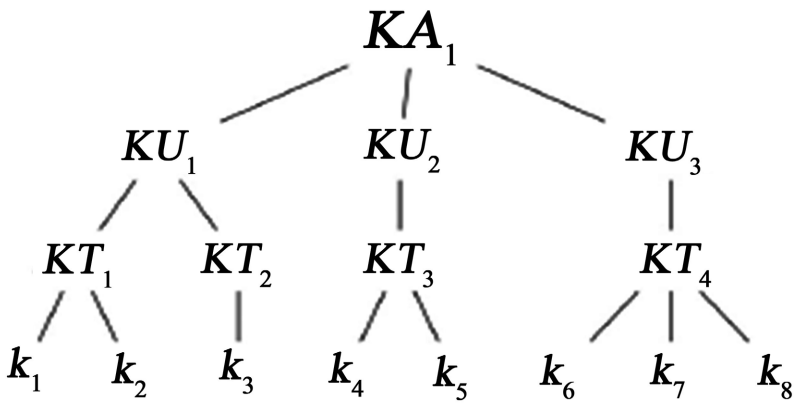

Figure 2. Correspondence between keywords and knowledge domains
图 2. 关键词与知识领域的对应关系

2) 下载赛题题解：我们了下载 2016~2022 年国内进行的各项 CTF 竞赛的共 23,632 道赛题题解，并在当中查找相应的关键字。

3) 赛题知识领域确定：将每个赛题详解的关键词进行归类，确定赛道涉及的知识领域、知识单元和知识主题，最终得到整体分析报告。例如，一篇赛题详解包含了关键词 k_2，k_3，k_7，表明该题目涉及知识领域 KA_1 的知识单元 KU_1 的主题 KT_1 和 KT_2，及 KU_3 的主题 KT_4。

4.2. 赛题分析结果

4.2.1. 知识领域的总体分布

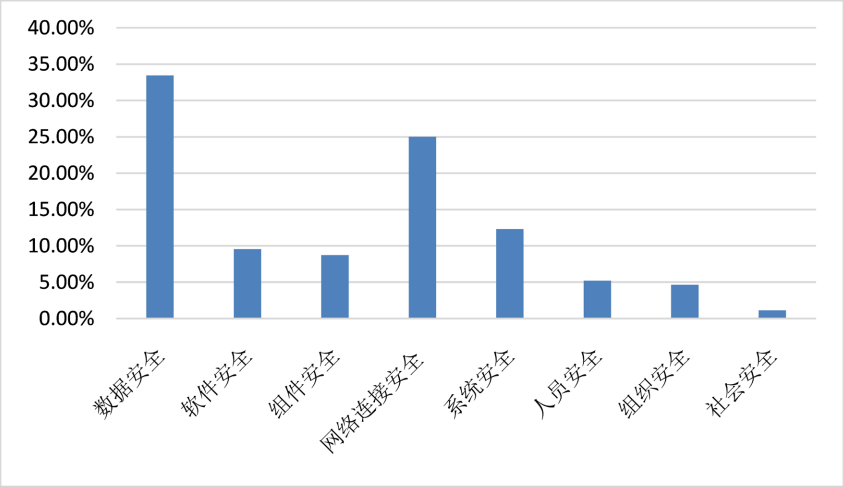

Figure 3. Distribution of network security knowledge fields
图 3. 网络安全知识领域的分布

图 3 显示了分析报告中赛题知识领域的分布。可以看到：

1) 这些赛题基本上包含了所有知识领域。排在第一名的是数据安全，有超过 30%的赛题与领域有关。第二名是网络连接安全，约 25%，第三名是系统安全，约 13%，说明它们在 CTF 竞赛中是最常考察的知识领域。数据安全包括关于加密、身份验证和安全通信的知识。网络连接安全包括网络服务的攻击和防御。系统安全涉及渗透测试和多级攻击。这些都是最适合在 CTF 竞赛中考查的技能和知识。

2) 软件、组织、组件和人员安全的值相似，约为 5~10%，低于平均水平。这些方面的考察通常要涉及到额外的物理设备和人员管理，会增加 CTF 竞赛的复杂性，同时也增加了昂贵的成本投入。

3) 最不常见的知识领域是社会安全，只有约 3%。因为网络安全的社会方面，如隐私或网络法律，涉及技术层面知识较少，通常在 CTF 竞赛中不常出现。

4.2.2. 知识单元的整体分布

Table 1. Top 10 knowledge unit distribution
表 1. 排名前十的知识单元分布

知识单元	主题	涉及知识领域	百分比
密码学	加密解密	数据安全	12.43%
组件设计	逆向工程	组件安全	8.14%
漏洞利用	安全编程	软件安全	7.88%
系统控制	渗透测试	系统安全	7.86%
Web 系统安全	Web 攻击	网络连接安全	7.23%
网络服务	网络协议安全	网络连接安全	7.18%
网络应用安全	网络攻防	网络连接安全	6.64%
数字取证	流量分析	数据安全	3.74%
安全认证管理	身份认证	人员安全	3.12%
业务安全和容灾	应急响应	组织安全	2.23%

表 1 列出了我们统计得出的排名前十的知识单元，以及它们涉及的主题和知识领域。

1) 密码学是排名第一的知识单元，解题模式下的 Crypto (密码学)题目都属于这个领域。此外，密码学相关知识也可以用解决其他更大任务的子任务。比如，往往许多 Web 题目要得到最后的 flag 往往要用到各种解密算法。

2) 组件设计、漏洞利用、系统控制通常在逆向和 PWN 题中出现。参与者需要将二进制码通过逆向分析还原源代码中缺失的符号和数据结构等信息，进而寻找程序中的漏洞，并通过漏洞利用到最终的 flag。

3) Web 系统安全、网络服务、网络应用安全主要体现在 Web 类赛题中。尤其是在攻防模式的竞赛中，要求参与者利用网络服务、分析流量或建立远程连接，还需要借助一些犀利的工具和脚本，对目标网络进行相应的攻击和防御，获取最终的 flag。因此，网路连接安全是攻防竞赛模式下最重要的知识领域。

此外，55 个知识单元中“物理接口和连接”在所有赛题中均未出现。这是因为目前绝大多数 CTF 竞赛都是虚拟仿真环境下进行的，很少涉及到针对物理设备的黑客攻击。

5. 对 CTF 竞赛促进网络安全人才技能培养的建议

通过前面的统计分析，我们不难发现，尽管 CTF 比赛在国内外开展得如火如荼，对网安人才的培养和选拔无疑具有积极的推动作用。但是，目前 CTF 竞赛在网安人才的知识体系培养中仍存在诸多不足。针对 CTF 竞赛存在的局限性，我们提出相应建议：

1) 网络安全的基础知识与技能培养应该理论与实践的结合，理论课程应侧重于 CTF 未涵盖的领域。

尽管 CTF 竞赛在网络安全领域涉及广泛，但仍有一些领域未被充分覆盖，如安全管理、社会工程、物理安全、云安全等。因此，还需要关注和学习这些未覆盖的领域，通过理论知识帮助学习者建立一个坚实的基础，从而获得全面的网络安全知识和技能，并为实践应用提供指导。理论和实践相结合可以帮助学习者理解网络安全的战术和策略，从而更好地理解如何应用不同的安全解决方案，制定有效的网络安全策略，应对网络安全中不同类型的挑战和问题。

2) 赛题知识点高度集中，需要不断引入网络安全新领域和知识前沿，增加跨学科的知识以吸引更广泛的非技术受众。

网络安全的各个知识领域在 CTF 竞赛赛题中的表现很不均衡。像密码学、网络攻防或逆向工程，多年来一直是 CTF 竞赛的主要内容。这是因为 CTF 竞赛的组织者和出题人通常均为专业技术人员或熟练的网络安全从业者。一些 CTF 竞赛的题目设置非常困难，需要深入的专业知识和高超的技术能力。对于初学者来说，可能需要更多的基础知识和技能才能有效参与竞赛，而对于广大非专业网络安全爱好者的参与产生了困难。

CSEC2017 将网络安全定义为“一门基于计算的学科，涉及技术、人员、信息和流程，以确保运营”，但 CTF 竞赛目前 CTF 竞赛通常不涉及非技术层面的安全问题，缺少跨学科“人”的方面。诸如网络钓鱼和网络安全意识之类的主题，对于减少当前的网络威胁又至关重要。引入跨学科的网络安全新领域和知识前沿可以为 CTF 竞赛提供了一个新的契机，吸引更广泛的非技术受众进入网络安全领域，使 CTF 竞赛更具挑战性和创新性，同时也能够推动参与者不断学习和探索。

3) 目前的大多数 CTF 竞赛缺乏核心对抗能力的考查，与真实的攻防场景还有很大差距，因此，催生了一批新型安全竞赛的诞生。

尽管 CTF 竞赛模拟了一些真实的网络安全挑战，但并不总是能够反映真实世界中的安全问题和应用场景[7]。参与者在竞赛中获得的技能和经验可能在实际工作中并不完全适用。随着大数据、物联网、云计算、人工智能的飞速发展，传统企业进行数字化赋能的同时，网络环境变得更加错综复杂，网络攻击不断，国家关键信息基础设施建设面临着持续的威胁。安全技术的应用场景日趋广泛并逐步扩大，同时

也诞生了一批新型网络安全竞赛。

全国工控系统信息安全攻防竞赛[8]通过真实还原了工业生产环境，针对不同的行业对象关键信息基础设施的安全风险漏洞挖掘与防护技术的交流与研究，准确把握工控安全风险发生的规律、动向、趋势，积极探索工控安全防护技术、促进安全产品和服务模式创新。

ISCC(信息安全与对抗技术竞赛)中数据思维赛[9]主要面向具备基础数据挖掘知识和实践创新能力的选手，意在激发选手对网络安全数据挖掘的兴趣，培养数据分析综合能力。选手根据赛题要求使用机器学习方法对题目中描述的应用问题进行建模，并提交对测试数据集的预测结果。

2022 年举办的全国人工智能安全大赛[10]，针对人脸识别安全、深度伪造内容治理、自动驾驶安全等领域设置赛题，将产业应用中的实际需求与最前沿的安全问题融合，为人工智能的能力演进提供重要参考，强化人工智能治理体系与安全评估能力建设，助力人工智能产业高质量发展，培育高水平的人工智能安全团队。

这些专题竞赛引入了多样性的题目和挑战，涵盖了网络安全领域的更多方面。结合实际应用场景，使竞赛更加贴近实际工作和需求，可以更好地满足各种参与者的需求，推动网络安全教育和培训的发展。

6. 结束语

CTF 竞赛使学生通过在线练习，学习和锻炼各种各样的网络安全技能，有效地弥补了目前大学传统教育形式下网络安全教育的不足。我们分析了近年来举行的 CTF 竞赛的 23,632 道赛题题解，以确定 CSEC2017 网络安全课程指南中定义的各类网络安全主题在 CTF 竞赛中的体现，希望对未来参加此 CTF 竞赛的院校和同学提供理论借鉴和数据参考。分析表明，密码学和网络安全等主题在 CTF 竞赛中目前仍占主导地位。在此，我们建议在 CTF 竞赛中引入多样性的题目和挑战，涵盖不同网络安全领域的知识和技能，吸引越来越多的跨学科的非技术受众进入网络安全领域，使 CTF 竞赛可以为网络安全人才的培养提供更全面和有针对性的支持，帮助参与者广泛接触各种安全挑战，培养全面的技能，不断学习和成长，从而更好地适应网络安全领域的需求，应对不断变化的网络安全挑战。

基金项目

西安邮电大学教学改革项目(JGB201904)。

参考文献

[1] 宋晓锋, 倪林, 韩鹃, 等. CTF 竞赛融入网络安全人才培养过程的探索与实践[J]. 计算机教育, 2021(11): 1-5.

[2] 王星. 美国高等教育网络安全知识体系规范综述[J]. 中国信息安全, 2018(4): 100-103.

[3] 葛昕, 马立新. 基于 CTF 竞赛的网络安全课程教学研究[J]. 教育教学论坛, 2020(46): 268-270.

[4] 宋超, 吴明. CTF 赛题在“1 + X”证书制度下的教学实践[J]. 网络安全技术与应用, 2021(10): 104-105.

[5] 秦金. 基于知识图谱的网络安全教学知识库构建探究[J]. 网络安全技术与应用, 2023(5): 92-94.

[6] Burns, T.J., Rios, S.C., Jordan, T.K., *et al.* (2017) Analysis and Exercises for Engaging Beginners in Online CTF Competitions for Security Education. 2017 *USENIX Workshop on Advances in Security Education*, Vancouver.

[7] 杨志增, 肖锋, 董婷, 等. 基于专业技能竞赛平台的网络空间安全类人才实践育人培养模式探索[J]. 高教学刊, 2020(10): 121-124.

[8] 第七届全国工控系统信息安全攻防竞赛(决赛) [EB/OL]. https://www.ichunqiu.com/competition/detail/300, 2022-12-27.

[9] 第 20 届信息安全与对抗技术竞赛(ISCC2023)个人挑战赛、无限擂台赛、数据思维赛简况[EB/OL]. https://www.isclab.org.cn/2023/06/13/iscc2023-online-summarize/, 2023-06-13.

[10] 大赛介绍[Z]. https://www.zgc-aisc.com/#page-3