回顾 | 去年爆燃的首届“强网”拟态防御国际精英挑战赛！

转载

李飞cc 于 2019-05-17 11:25:31 发布 153 收藏

文章标签： 拟态防御 信息安全 网络安全

去年5月12日，新华社一篇名为《多国顶尖“白帽黑客”对拟态防御网络设备和系统 发起50余万次攻击测试无一次得手》的消息被广为传播，被数百家媒体转载使用，在网络上红极一时，同时其英文稿件也被多个境外媒体进行了刊发，引起业界普遍关注。

关注新华网

微信

微博

Qzone

0
评论

这一我国独创理论的安全属性得到了充分验证。

记者在现场看到，两天来，来自俄罗斯、乌克兰、日本、波兰和中国等国的２２支参赛战队，针对拟态防御网络设备和系统发起的攻击全部被拟态化的网络设备和系统发现并封堵。赛事主办方还授权俄罗斯、波兰和中国的几支顶尖战队最高管理权限，现场在拟态防御网络设备和系统中植入"后门"，展开注入式攻击。攻击测试结果表明，事先预置的"后门"也无法被有效利用，几支参赛队均未能通过自设"后门"达成完整突破的目的。

据中国工程院院士、拟态防御理论首创者邬江兴介绍，这次邀请顶尖"白帽黑客"开展攻击测试，对进一步验证拟态防御机制的有效性具有十分重要的意义。测试结果表明，拟态防御具有"结构决定安全"的内生安全属性，基于软硬件内部"漏洞""后门"的传统网络攻击方法被彻底颠覆，诸如"挖漏洞""设后门""植病毒"和"藏木马"等经典攻击套路在机理上不再有效，网络安全有了抓手级落地技术。

邬江兴表示，网络空间拟态防御技术历经我国专家团队和国际顶级战队的多轮众测，其先进性与可信性、安全性与开放性的统一得到了充分验证，完全达到理论预期效果，将为维护国家网络空间安全，构建全球网络空间命运共同体提供"改变游戏规则"的核心技术。作为信息技术领域的后来者，中国在网络安全领域完全可以在"换道超车"中实现自主可控与并跑领跑的目标。

炫圈 | 视频

First "Qiangwang" International Elite Challenge on Cyber Mimic Defense attracts "white hat hackers"

0

2018-05-11 13:02 By: GMW.cn

Update of the challenge score of The First "Qiangwang" (Cyberspace power) International Elite Challenge on Cyber Mimic Defense in Nanjiang, capital of east China's Jiangsu Province, May 10, 2018. (Photo provided to Guangming Online)

NANJING, May 11 (Guangming Online)——The First "Qiangwang" (Cyberspace power) International Elite Challenge on Cyber Mimic Defense, which kicked off on Thursday, has attracted almost 30 teams of Chinese and foreign "white hat hackers", including four top foreign teams: dcua from Ukraine, P4 from Poland, TokyoWesterns from Japan and LC⚡BC from Russia,

全篇不过700多字的文字里，流淌的是我国科学家十年磨一剑的心血，跳动的是我国网信技术领域从跟跑、并跑向领跑跃进的脉动，彰显的是我国在网络安全领域的高度技术自信，体现的是我国推动网络空间命运共同体建设的落地举措。

今年又逢5月，让我们对去年已经令人惊愕的首届赛事进行一次简要回顾。

首届“强网”拟态防御国际精英挑战赛于2018年5月10日在南京正式开始，该赛事之所以从发布之初就备受瞩目，是因为它创造了国内外同类赛事多个“第一”、“首次”。

具体来看有如下几个方面

规则首次

据不完全统计，90%以上的网络空间安全赛事都采用CTF（Capture The Flag，夺旗赛）模式，通常设置解题、闯关、攻防对抗等环节。

该赛事对规则进行了全面创新，一是充分“集中火力”，队伍之间不再相互对抗，而是将互联网关键基础设施设备作为所有参赛队伍的“靶机”，且网络环境与实际相差无几；二是充分“自信开放”，在附加赛中设置攻坚闯关赛和后门注入攻击两个阶段，开创了网络安全领域“白盒与黑盒对比测试、外部突破与注入组合实施”比赛机制的先河。

选手第一

该赛事共邀请国内外22支顶尖战队共同参赛，是国内同类赛事队伍实力最强的一次竞赛。

其中，国内战队全部来自去年第二届“强网杯”全国网络安全挑战赛前20强队伍；国际战队是在2018年度CTFTIME全球排行榜中，排名位居首位的乌克兰dcua战队、第二位的波兰P4战队、第三位的日本TokyoWesterns战队，2017年度第六位俄罗斯LC↯BC战队等4支队伍，堪称全明星阵容。

靶机第一

该赛事将基于网络空间拟态防御理论开发的网络设备和系统作为“靶机”，在世界范围内尚属首次。

据赛后统计，所有参赛队伍对其展开了50余万次全方位、高强度的攻击测试，无一次成功得手。拟态防御这一我国独创理论的安全属性得到了充分验证。

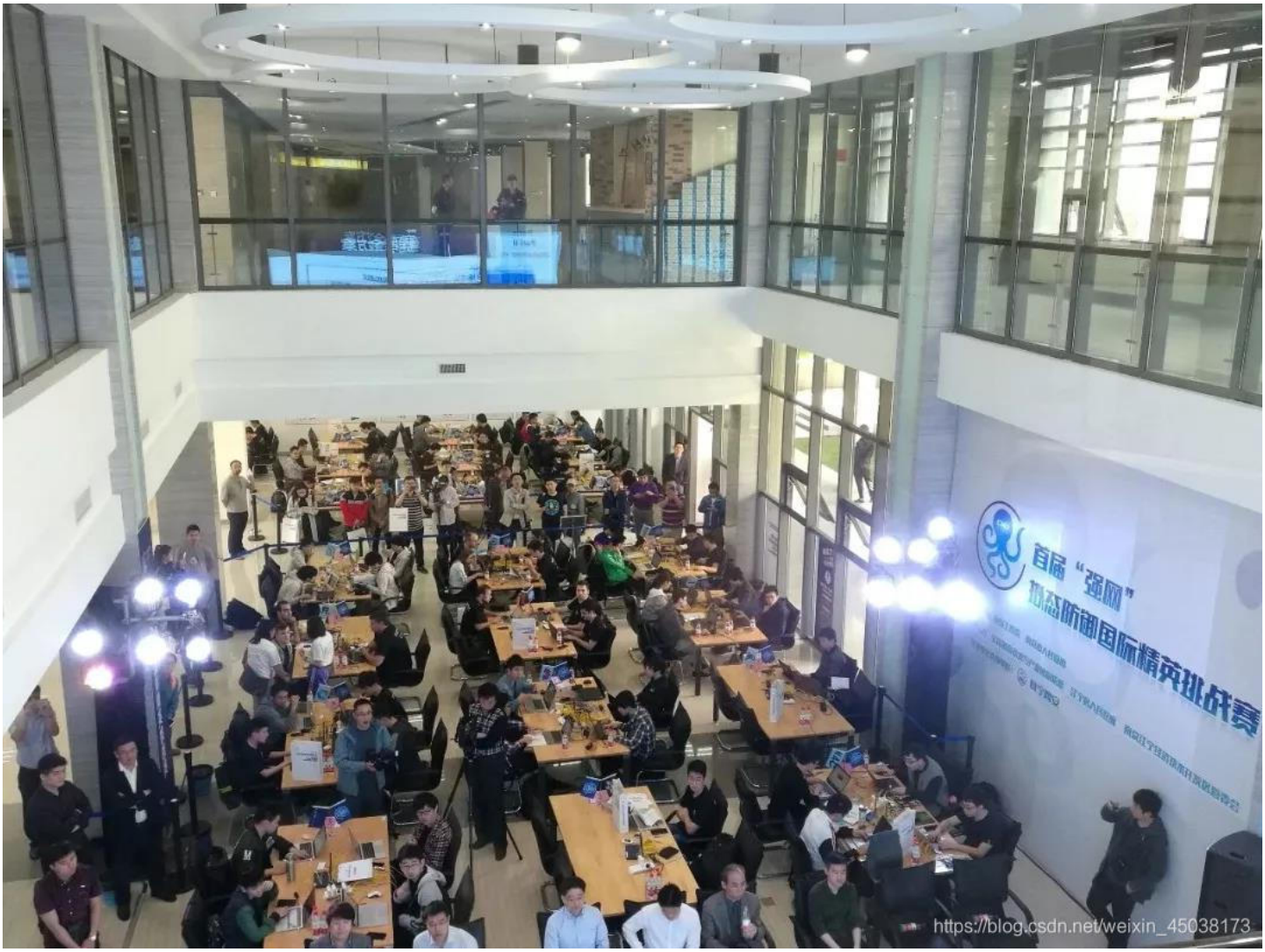
奖金丰厚

该赛事总奖金高达200万元人民币，其中基础奖金100万元，特别奖金100万元。

经过鏖战，据新华社消息权威发布，“来自俄罗斯、乌克兰、日本、波兰和中国等国的22支参赛战队，针对拟态防御网络设备和系统发起的攻击全部被拟态化的网络设备和系统发现并封堵。

赛事主办方还授权俄罗斯、波兰和中国的几支顶尖战队最高管理权限，现场在拟态防御网络设备和系统中植入‘后门’，展开注入式攻击。攻击测试结果表明，事先预置的‘后门’也无法被有效利用，几支参赛队均未能通过自设‘后门’达成完整突破的目的。

纵观首届“强网”拟态防御国际精英挑战赛过程，高强度、高烈度、高亮度！首届即成功驰名中外，吸引眼球！但最基础的、最核心的是我国科学家自主创新的网络空间拟态防御机制！



纵观首届“强网”拟态防御国际精英挑战赛，

“暮色苍茫看劲松，乱云飞渡仍从容。”

这是底气与信心；

“实践是检验真理的唯一标准。”

这是方法与路径；

“和平、安全、开放、合作”，

这是目标与宗旨。

期待网络空间拟态防御

未来有更加精彩的表现！