绿盟信息安全攻防竞技平台

产品白皮书

■ 文档编号	NSF-PROD-ISTS-产品白皮书	■ 密级	完全公开
■ 版本编号	V2.0	■ 日期	2019-05-06
■ 撰 写 人		■ 批准人	

目录

一. 产品背景

随着信息化的快速发展，网络安全问题更加突出，对网络安全人才建设不断提出新的要求。2014 年 2 月 27 日，中央网络安全和信息化领导小组成立，习近平亲自担任组长。在第一次会议上习近平明确指出，没有网络安全就没有国家安全。建设网络强国要有高素质的网络安全和信息化人才队伍。网络空间的竞争，归根结底是人才竞争。

近期关于网络安全人才培养的相关政策法规先后出台，截取相关内容如下：

- 2017 年 6 月 1 日施行的《网络安全法》首次以法律条款的形式对网络空间安全领域的人才问题进行规定，不仅体现出国家对网络人才的重视，更是为国务院以及各地方出台网络安全人才培养的细则提供了最高位阶的法律依据。
- 2016 年 6 月 6 日，中央网络安全和信息化领导小组办公室、国家发展和改革委员会、教育部、科学技术部 、工业和信息化部、人力资源和社会保障部等部委联合发文《关于加强网络安全学科建设和人才培养的意见》。
- 《工业和信息化部关于加强电信和互联网行业网络安全工作的指导意见》（国家工信部保 [2014] 368 号）明确提出基础电信企业要积极开展网络安全专业岗位职业技能鉴定工作，建立健全网络安全专业岗位持证上岗制度；加强网络安全培训，把相关培训纳入员工培训计划；积极组织和参与网络安全知识技能竞赛，形成培养、选拔、吸引和使用网络安全人才的良性机制。
- 《中国金融业信息技术“十三五”发展规划》中明确提出，开展信息技术研究。密切跟踪信息技术发展方向及金融业应用情况，持续对信息安全等领域及金融业信息技术基础理论开展前瞻性专题研究；加强人才队伍建设。适应“互联网+”时代需要，积极开展新技术领域人才培训，重点加强复合型技术、分布式架构技术人才的培养，优化金融信息技术人才结构。
- 为了规范电力行业网络与信息安全的监督管理，国家能源局制定了《电力行业网络与信息安全管理办法》中规定：组织开展电力行业网络与信息安全信息通报、从业人员技能培训考核等工作；组织开展电力行业网络与信息安全的技术研发工作；电力企业应当加强信息安全从业人员考核和管理。从业人员应当定期接受相应的政策规范和专业技能培训，并经培训合格后上岗等。

2015 年年底，工信部中国电子信息产业发展研究院（赛迪）发布中国当前对网络安全人才的需求大约为 50 万人，但目前国内国家安全厂商的安全类工程师加在一起也不过 5 万人上

下，人才缺口高达 45 万，到 2020 年缺口将达到 140 万。供求比为 1:10，是目前互联网人才供求差距最大的市场领域。

在上述背景下，绿盟科技将自己在网络安全领域的多年技术积累转换成网络安全人才培养能力，研发出信息安全攻防竞技平台，满足用户的考核评比、竞赛演练等需求。

二. 产品介绍

2.1 产品概述

绿盟信息安全攻防竞技平台通过虚拟化技术创建各类网络安全对抗场景，集单兵挑战、综合靶场、网络混战等比赛模式于一体，为用户开展网络安全人才竞赛演练提供有力支撑。并可依托此平台举办网络安全攻防大赛，通过以赛促学、以赛促练的方式选拔和培育信息安全人才，创新网络安全人才培养机制。下图为信息安全攻防竞技平台的产品框架图：

绿盟信息安全攻防竞技平台框架图

2.2 硬件平台

信息安全攻防竞技平台根据单台设备支持虚拟机并发数量分成 4 种不同的型号，用户可

根据实验室规模选配合适的型号。另外攻防竞技平台支持集群部署功能，可通过集联多台设备开展大规模的竞赛实训。

	ISCSNX3-1000A	ISCSNX3-2000A	ISCSNX3-3000A	ISCSNX5-5000A
平台配置及性能	1U 机架式设备，单台设备支持虚拟机（windows2003 512M 内存）并发数量 20 个，虚拟机启动速度小于 15 秒，支持 10 名学生开展竞赛演练（具体人数与竞赛题目所需虚拟机数量有关）。	2U 机架式设备，单台设备支持虚拟机（windows2003 512M 内存）并发数量 30 个，虚拟机启动速度小于 15 秒，约支持 15 名学生开展竞赛演练（具体人数与竞赛题目所需虚拟机数量有关）。	2U 机架式设备，单台设备支持虚拟机（windows2003 512M 内存）并发数量 60 个，虚拟机启动速度小于 15 秒，支持 30 名学生开展竞赛演练（具体人数与竞赛题目所需虚拟机数量有关）。	2U 机架式设备，单台设备支持虚拟机（windows2003 512M 内存)并发数量 100 个，虚拟机启动速度小于 15 秒，支持 50 名学习开展竞赛演练（具体人数与竞赛题目所需虚拟机数量有关）。

2.3 竞赛模式

信息安全攻防竞技平台涵盖单人、团队、人机对抗、人人对抗等多种竞赛形式，主要分为单兵挑战、综合靶场和网络混战等模式。

2.3.1 单兵挑战

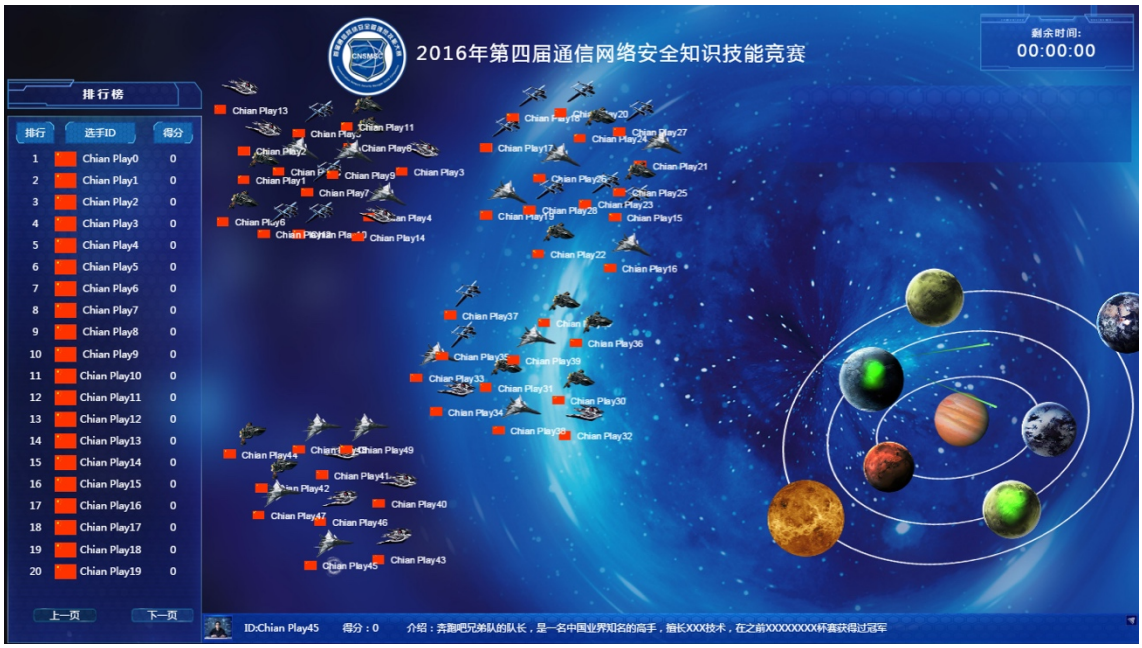
单兵挑战模式以闯关的方式进行挑战，参赛人员需在规定的时间内容通过完成关卡。关卡涉及 WEB、密码学、隐写、溢出、逆向、编程、综合等内容。单兵挑战提供在线部署模式，靶机共享模式，靶机独享模式三种模式。

单兵挑战态势展示以星座图方式显示题目关卡，能够实时展示每名参赛人员的得分情况并进行排名。在此界面不仅可以查看每名竞赛人员的答题情况，而且可以查看每道题目的过关率。

2.3.2 综合靶场

综合靶场模式为每个参赛队提供相同的模拟真实企业内部架构的实训环境。环境由若干存在漏洞的靶机组成，在靶机的关键位置存有 Flag 文件。参数队伍需要按照网络拓扑情况对此环境进行逐层渗透得到 Flag 文件并提交。

综合靶场态势展示以外太空为背景，通过星球大战的方式形象展示比赛情况，主要包括参赛队伍答题状况、得分排行、比赛时间等内容。



2.3.3 网络混战

网络混战模式为每个参赛队伍提供具有相同漏洞的网络靶机。每个队伍在加固自己网络靶机的同时，要攻击其它队伍的网络靶机。攻击成功后，攻击方得分，防守方减分。

网络混战态势展示以中国地图为背景，通过区域混战的方式展示比赛情况，主要包括参赛队伍的攻击类型、得分排行、比赛时间等内容。

2.4 平台功能

平台提供便捷的管理功能，支持管理员对不同比赛模式的信息等进行设置。管理员可以对单兵挑战的比赛信息、场景、靶机部署、题库、态势展示等内容进行管理，并可实时查看比赛成绩。

管理员可以对综合靶场的比赛信息、场景、靶机部署、态势展示等内容进行管理，并可实时查看比赛成绩。

管理员可以对混战模式的比赛信息、场景、混战部署、态势展示等内容进行管理，并可实时查看比赛成绩。

平台支持管理员上传工具并进行分类，方便参赛队员下载使用。

管理员能够根据不同比赛模式为参赛队员创建不同的比赛账号。

管理员能够对平台使用的虚拟化资源进行统一管理，以便平台在最佳性能下稳定运行。

在比赛过程中，管理员可以实时查看靶机、攻击机及资源，方便管理员掌握竞赛进度。

2.5 竞赛内容

信息安全攻防竞技平台默认提供 29 道单兵挑战、1 道综合靶场和 1 道网络混战；并提供题目升级授权，每年新增 20 道单兵挑战、1 道综合靶场和 1 道网络混战。

单兵挑战部分题目信息如下：

序号	实验名称	序号	实验名称	过关文档
1	FTP 服务器漏洞	16	利用系统漏洞对目标主机植入远程控制后门	提供
2	获取 windows 本地密码	17	万网购物网站渗透测试	提供
3	通过网络嗅探获取 Password	18	电气公司网站漏洞利用	提供
4	通过系统漏洞获取敏感文件内容	19	网站漏洞攻击之新闻发布系统	提供
5	服务器木马查杀	20	网站漏洞攻击之旅游网站	提供
6	针对东方科技的渗透测试	21	网站漏洞攻击之 XYCMS 企业建站系统	提供
7	针对社交博文系统的渗透测试	22	网站漏洞攻击之国际环保	提供

8	SQL-server 提权	23	网络攻击之编辑器漏洞攻击	提供
9	SQL 注入	24	数据包分析	提供
10	cookie 注入	25	crackme1	提供
11	IIS write 漏洞利用	26	crackme2	提供
12	表单欺骗	27	天下咨讯网站入侵测试	提供
13	数据恢复	28	大海科技网站渗透测试	提供
14	MS08_067 漏洞利用	29	MS04_007 漏洞利用	提供
15	Tomcat 服务器漏洞利用			

除了平台中已经提供的竞赛题目外，绿盟科技也可根据客户的实际需求进行题目定制，并针对客户举办相关竞赛提供竞赛运维服务。

三. 产品价值及优势

3.1 产品价值

绿盟信息安全攻防竞技平台能够为用户开展网络安全人才培养提供以下帮助：

1. 以赛促学、以赛促练创新网络安全人才培养模式；

2. 通过竞赛的方式，激发学员学习网络安全的兴趣，提升网络安全防护能力；

3. 通过真实网络环境下的网络对抗考察学员的攻击和防御水平，提高学员的实际动手能力。

3.2 产品优势

1. 竞赛环境极速部署

信息安全攻防竞技平台三种模式均支持一键部署方式，管理员选择竞赛题目、关联参赛队后点击“一键部署”，本场竞赛的竞赛环境和策略就自动下发。使用此部署模式能大幅度地减少网络安全竞赛的配置时间，方便用户开展竞赛实训。

2. 动态 FLAG，预防作弊

为防止不同队伍间共享答案信息等违规行为，平台采用动态 Flag 机制来实时更改比赛答案。Flag 动态变化的时间可以在后台人工设置。动态变化的 Flag 通过两次动态变化和加密等措施来保证 Flag 机制的安全性。

3. 完备的竞赛模式

平台涵盖单人、团队、人机对抗、人人对抗等多种竞赛形式，可帮助用户面向不同群体开展不同规模的竞赛演练。