中国信息安全测评中心

教育部高等学校网络空间安全专业教学指导委员会

第十八届全国大学生信息安全竞赛（创新实践能力赛）暨第二届“长城杯”铁人三项赛（防护赛）初赛技术文件

初赛技术文件主要由初赛考核大纲、赛题说明和答题要求三部分组成，具体内容如下。

一、考核大纲

考核大纲主要包括理论知识考核和实操技能解题，包含信息安全基础知识、安全法律法规及标准规范、密码学、WEB安全等7部分内容。明确参赛选手应具备的知识与技能，是大赛命题及参赛队伍训练准备的参考资料。

（一）信息安全基础知识

考查选手对信息安全保障、信息安全管理、信息安全支撑技术、物理与网络通信安全、计算环境安全、软件安全开发等信息安全基础知识的掌握情况。

（二）安全法律法规及标准规范

考查选手对《网络安全法》《个人信息安全保护法》《数据安全法》《关键信息基础设施保护条例》等法律法规的了解程度。

考查选手对《信息安全风险评估规范》《网络安全等级保护基本要求》《个人信息安全规范》《关键信息基础设施安全保护要求》等网络安全标准的了解程度。

（三）密码学

考查选手对密码学相关知识的掌握情况，包括编码解码、古典密码学、RSA、AES、DES、SM2、SM4现代密码学算法、量子密码学等。

（四）WEB安全

考查选手对WEB应用常见安全风险和网络攻击的掌握程度，包括通用框架和中间件漏洞、反序列化、SQL注入、文件包含、文件上传、命令执行、权限绕过、弱口令等常见安全问题，及常用WEB安全检测及对抗技术、漏洞挖掘与利用技术手段等。

（五）逆向工程

考查选手对Windows/Linux/Android等平台的二进制代码的逆向分析和理解能力，主要包括多种反汇编、反编译逆向工具的使用，脱壳、调试技巧，加解密、反调试和代码混淆，恶意样本分析等技术。

（六）PWN

考查选手对于二进制漏洞的挖掘和利用能力，包括堆栈溢出、格式化漏洞等常见二进制漏洞，选手需要分析并发现程序漏洞，并进行利用。

（七）威胁检测与网络流量分析

考查选手对恶意代码、程序、流量的识别、检测分析和还原能力，包括网络流量行为分析、流量还原解密、Web日志分析、恶意代码痕迹检测，及恶意活动进程行为分析和数据恢复等。

二、赛题说明

初赛赛题数量及难度等级如下表所示。

表：初赛赛题数量及难度说明

赛项	考核阶段	考核内容	题目数量	难度等级
初赛	理论知识	信息安全基础知识	20 道	初级
		法律法规及安全标准	10 道	初级
	实操技能	威胁检测与网络流量分析	4 道	中高级
		密码学	4 道	中高级
		WEB 安全	8 道	中高级
		逆向工程	4 道	高级
		PWN	4 道	高级

命题组负责赛题的罐装测试，并交由裁判组进行审核确认。赛题一经确认，任何单位和个人不得再做修改。

三、参赛队伍答题要求

初赛参赛队伍答题要求如下：

（一）同一队伍的参赛人员应集中参赛，赛前开启视频摄像头，手持身份证和学生证原件完成身份确认;

（二）比赛期间，参赛队伍全程开启房间摄像头和个人计算机视频摄像头，非参赛人员（指导老师、领队老师和非报名学生等）严禁出现在比赛场地;

（三）参赛队伍严禁使用双屏幕答题，严禁使用大模型等智能平台辅助答题;

（四）参赛队伍在参赛过程中不得对比赛平台、系统和第三方服务进行攻击，所有比赛个人行为不得与国家法律、法规、公序良俗相违背;

（五）参赛选手应全程开启电脑录屏，每小时保存1份视频文件，比赛结束后4小时内须将录屏视频文件和CTF解题思路上传网盘并提交赛务组存档。