2023-2024 年重庆市职业院校技能大赛

信息安全管理与评估（CQGZ032）赛项规程

一、赛项信息

<table>
<tr><td colspan="4">赛项组别</td></tr>
<tr><td colspan="4">☐中等职业教育　☑高等职业教育</td></tr>
<tr><td colspan="4">☑学生赛（☐个人/☑团体）　☐师生同赛　☐教师赛（☐个人/☐团体）</td></tr>
<tr><td colspan="4">涉及专业大类、专业类、专业及核心课程</td></tr>
<tr><td>专业大类</td><td>专业类</td><td>专业名称</td><td>核心课程
（对应每个专业，明确涉及的专业核心课程）</td></tr>
<tr><td rowspan="12">31 电子与信息大类</td><td rowspan="12">3102
计算机类</td><td rowspan="10">310207
信息安全与管理</td><td>操作系统原理及安全</td></tr>
<tr><td>数据库原理及安全</td></tr>
<tr><td>Web 应用安全审计</td></tr>
<tr><td>密码技术应用</td></tr>
<tr><td>网络安全系统集成</td></tr>
<tr><td>数字取证与司法鉴定</td></tr>
<tr><td>数据灾备技术</td></tr>
<tr><td>信息安全测评与风险评估</td></tr>
<tr><td>软件逆向技术</td></tr>
<tr><td>信息安全工程管理</td></tr>
<tr><td rowspan="3">310202
网络工程技术</td><td>路由交换技术</td></tr>
<tr><td>网络安全技术</td></tr>
<tr><td>无线网络技术</td></tr>
</table>

			网络规划与系统集成
			Linux 操作系统
		310201 计算机应用工程	软件工程
			服务器管理与配置
			信息系统安全
			网络系统集成
			Web 开发技术
38 公安与司法大类	3802 公安技术类	380202 网络安全与执法	计算机网络
			操作系统
			计算机犯罪侦查
			网络信息监控技术
			信息安全体系结构
51 电子与信息大类	5102 计算机类	510207 信息安全技术应用	操作系统安全
			网络安全设备配置与安全
			电子数据取证技术应用
			信息安全产品配置与应用
			信息安全风险评估
			数据存储与容灾
			Web 应用安全与防护
		510216 密码技术应用	信息安全技术与实施
			商用密码产品部署
			公钥基础设施应用
			电子商务安全应用
			密码应用安全测评

			信息安全工程与管理
		510202 计算机网络技术	路由交换技术与应用
			Linux 操作系统管理
			网络系统集成
			网络安全设备配置与管理
		510201 计算机应用技术	数据库技术及应用
			系统部署与运维
			前端设计与开发
			交换路由技术
58 公安与司法	5802 公安技术类	580202K 安全与执法	网络安全设备配置
			电子数据勘查取证技术
			信息系统安全监察
			网络安全管理
			网络犯罪侦查

二、竞赛目标

为全面贯彻落实国家网络强国战略，对接新一代信息技术产业，助推我国信息安全产业链发展，促进职普融通、产教融合、科教融汇，产教协同培养信息安全领域高素质、专业化、创新型人才。

本赛项根据国家职业技能标准和行业从业人员能力要求，通过竞赛促进参赛选手熟悉信息安全行业标准规范和信息安全测试员新职业要求，考查参赛选手网络和信息安全相关的理论知识，重点考查参赛选手信息安全产品配置与应用、网络设备配置与管理、电子

数据分析与取证、系统安全评估、网络安全渗透测试等能力，校验参赛队计划组织和团队协作等综合职业素养，强调学生创新能力和实践能力培养，提升学生职业能力和就业质量。

本赛项衔接国家信息安全技术应用等高等职业教育专业标准，内容覆盖“信息安全技术与实施”“网络安全设备配置与管理”“信息安全风险评估”“操作系统安全”“Web 应用安全与防护”等专业核心课程内容。

赛项基于信息安全领域主流技术和现行业务流程设计，信息安全行业专家与院校教育专家紧密合作，赛前完成竞赛内容向教学改革的成果转化，实现以赛促教、以赛促学、以赛促改、以赛促建的教产融合的赛事创新。推动提升高等职业院校的人才培养水平，解决信息安全产业规模增长迅速与专业人才严重短缺的矛盾，实现人才到岗即用。

三、竞赛内容

根据《网络与信息安全管理员》国家职业技能标准、《信息安全测试员》国家职业技能标准、《信息安全技术 网络安全从业人员能力基本要求》（GB/T 42446-2023）等标准要求，结合企业实际岗位能力需求和具体工作任务，主要考查参赛选手网络和信息安全相关的理论知识掌握程度，重点考查参赛选手网络和信息安全相关的理论知识，以及信息安全产品配置与应用、网络设备配置与管理、电子数据分析与取证、系统安全评估、网络安全渗透测试等综合实践能力，要求参赛选手能够根据赛项要求，设计信息安全防护方案，实现设备互联互通。

本赛项为团队赛，竞赛分为操作和理论两个部分。理论部分主要考查参赛选手的网络与信息安全知识掌握情况和职业素养。操作部分考查参赛选手的综合实践能力，让选手尝试解决实际问题并不断优化自己的信息安全防护方案，同时根据网络业务需求配置各种安全策略，防范并解决网络恶意入侵和攻击行为，考查参赛选手的网络规划能力、实践操作能力和临场应变能力，检验参赛队的团队协作、质量意识、效益意识和创新意识等。

（一）竞赛具体内容

竞赛内容具体包括以下六个部分:

1.根据大赛提供的赛项要求，设计信息安全防护方案，并且能够提供详细的信息安全防护设备拓扑图。

2.根据业务需求和实际的工程应用环境，实现网络设备、安全设备、服务器的连接，通过调试，实现设备互联互通。

3.在赛项提供的网络设备及服务器上配置各种协议和服务，实现网络系统的运行，并根据网络业务需求配置各种安全策略，组建网络以满足应用需求。

4.根据企业所发现的安全事件，展开网络安全事件的调查、分析和取证工作，收集、保存、处理、分析和提供与计算机相关的证据，审计黑客的入侵行为，恢复被黑客破坏的文件。

5.利用一系列网络安全攻击渗透工具对所提供的网络安全攻击靶场环境进行综合分析、挖掘和渗透。

6.网络和信息安全相关的理论技能与职业素养。

（二）竞赛模块及分值

表 1 竞赛模块、时长及分值一览表

模块名称	主要内容	竞赛时长	分值
模块一	网络平台搭建与设备安全防护	180 分钟	300
模块二	网络安全事件响应、数字取证调查、应用程序安全	180 分钟	300
模块三	网络安全渗透、理论技能与职业素养	180 分钟	400

四、竞赛方式

竞赛以团体赛方式进行，为线下比赛。

每支参赛队由 3 名选手（设队长 1 名）组成，不得跨校组队，同一学校参赛队不超过 2 队，参赛选手必须是高等职业学校专科、高等职业学校本科全日制在籍学生或五年制高职中四至五年级（含四年级）的全日制在籍学生，凡在往届全国职业院校技能大赛中获一等奖的选手，不能再参加同一项目同一组别的比赛。

指导教师须为本校专职教师，每队不超过 2 名指导教师。

五、竞赛流程

（一）竞赛流程图

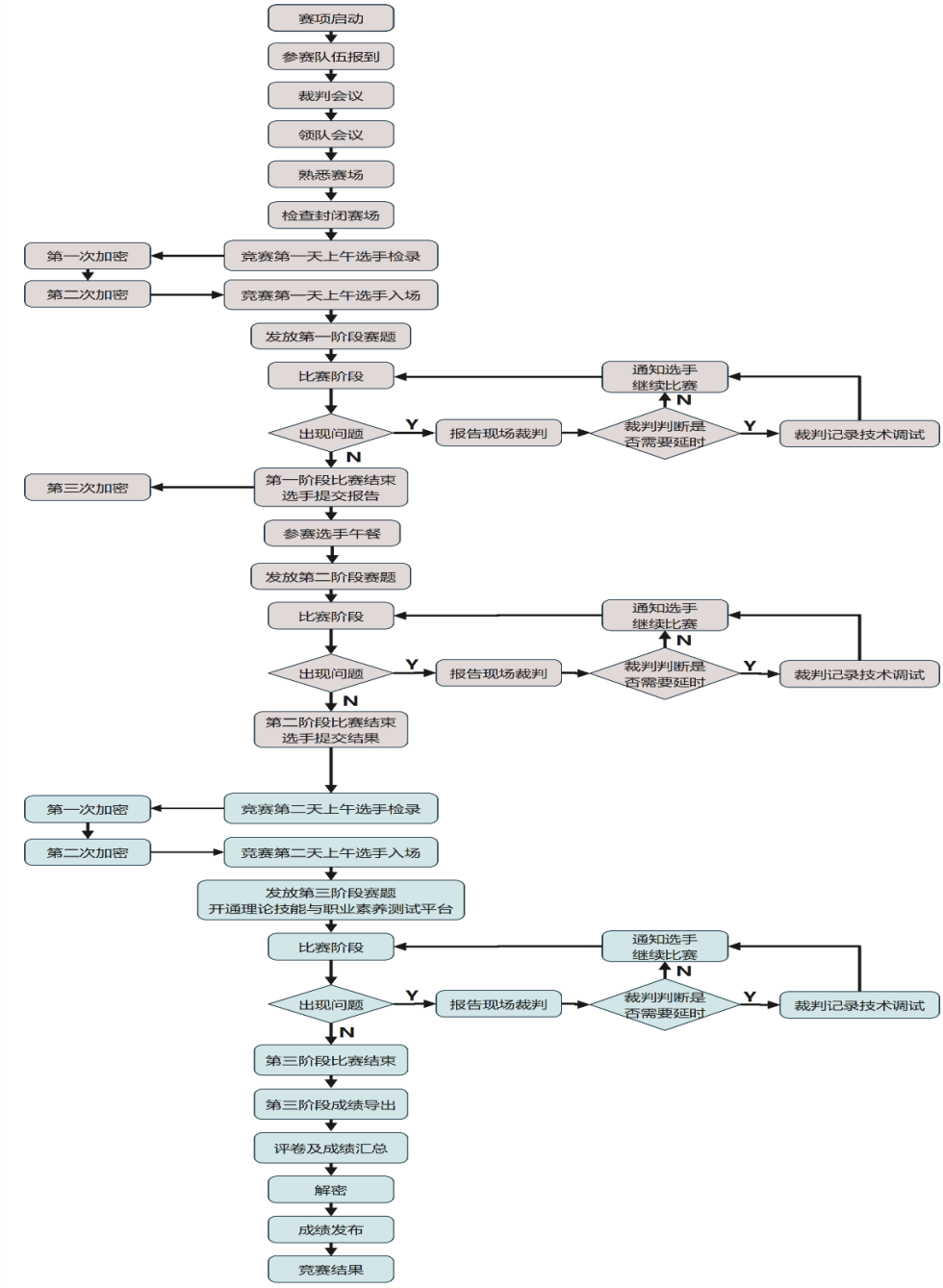

图 1 竞赛流程图

（二）竞赛时间表

竞赛限定在 2 天内进行，竞赛场次为 3 场，赛项竞赛时间为 9 小时，具体安排如下。

表 2 竞赛时间一览表

日期	时间	事项	参加人员	地点
竞赛	20:00 前	裁判、监督仲裁报到	工作人员	住宿酒店

日期	时间	事项	参加人员	地点
前 2 日				
	09:00-12:00	裁判工作会议	裁判长、裁判员、监督仲裁组	会议室
	12:00-15:00	参赛队报到，领取资料	工作人员、参赛队	竞赛场地
	13:00-14:30	领队工作会议	各参赛队领队、裁判长	会议室
	15:00-16:00	参观赛场	各参赛队领队	竞赛场地
	16:00-20:00	检查封闭赛场	裁判长、监督仲裁组	竞赛场地
竞赛 第 1 天	07:00-08:00	参赛选手检录	参赛选手、现场裁判	竞赛场地
	08:00-08:50	选手抽签第一次加密 选手抽签第二次加密 参赛代表队入场	参赛选手、加密裁判	竞赛场地
	08:50-09:00	宣读考场纪律 发放第一阶段赛题	参赛选手、现场裁判	竞赛场地
	09:00-12:00	第一阶段正式比赛	参赛选手、现场裁判	竞赛场地
	12:00-12:30	第一阶段结果提交 第三次加密	参赛选手、现场裁判	竞赛场地
	12:30-13:50	参赛选手午餐	参赛选手、现场裁判	竞赛场地
	13:50-14:00	参赛代表队就位 发放第二阶段赛题	参赛选手、现场裁判	竞赛场地
	14:00-17:00	第二阶段正式比赛	参赛选手、现场裁判	竞赛场地
	17:00-17:30	第二阶段结果提交	参赛选手、现场裁判	竞赛场地
	17:30-19:30	申诉受理	参赛选手、现场裁判、监督仲裁员	监督 仲裁室
竞赛 第 2 天	07:00-08:00	参赛选手检录	参赛选手、现场裁判	竞赛场地
	08:00-08:50	选手抽签第一次加密 选手抽签第二次加密 参赛代表队入场	参赛选手、加密裁判	竞赛场地
	08:50-09:00	宣读考场纪律 发放第三阶段赛题和理论测试系统使用说明	参赛选手、现场裁判	竞赛场地
	09:00-12:00	第三阶段正式比赛	参赛选手、现场裁判	竞赛场地
	12:00-12:30	第三阶段结果提交	参赛选手、现场裁判	竞赛场地
	12:30-14:30	申诉受理	参赛选手、现场裁判、监督仲裁员	监督 仲裁室
	12:30-21:00	评分核分	裁判长、评分裁判、监督仲裁员	裁判评分室
	21:00-21:30	抽检复核	裁判长、评分裁判、监督仲裁员	裁判评分室
	21:30-22:00	解密	裁判长、加密裁判、监督仲裁员	裁判评分室

日期	时间	事项	参加人员	地点
	22:00-24:00	成绩汇总报送，成绩公布	评分裁判、裁判长、专家、监督仲裁	竞赛场地和参赛队住宿酒店

（注：时间安排以比赛通知为准）

六、 竞赛规则

（一）选手报名

大赛报名方式和时间等要求，根据大赛办具体通知为准。

（二）熟悉场地

参赛选手报到后，根据大赛指南中规定的时间安排，前往竞赛场地，在指定区域熟悉场地情况。

（三）入场规则

参赛选手根据检录号，进行一次加密顺序号及二次加密工位号的抽取，入场时工位号进行检录查询赛场的位置，并按照工位位置就位等候竞赛开始。

（四）赛场规则

1.竞赛工位通过抽签决定，竞赛期间参赛选手不得离开竞赛工位。

2.竞赛所需的硬件设备、系统软件和辅助工具由承办单位统一安排，参赛选手不得自带硬件设备、软件、移动存储、辅助工具、移动通信等进入竞赛现场。

3.参赛队在赛前 10 分钟进入竞赛工位，并确认设备是否正常，竞赛正式开始后方可展开相关工作。

4.竞赛过程中，选手须严格遵守操作规程，确保人身及设备安全，并接受裁判员的监督和警示。若因选手造成设备故障或损坏，无法继续竞赛，裁判长有权决定终止该队竞赛；若因非参赛人员造成设备故障，由裁判长视具体情况做出裁决。

5.竞赛结束后，参赛队要确认已成功提交所有竞赛文档，裁判员与参赛队队长一起签字确认，参赛队在确认后不得再进行任何操作。

（五）离场规则

竞赛结束，参赛选手必须清洁桌面，扫除垃圾，整理工作现场，所有移动过的仪器、设备都必须恢复原状。参赛选手与裁判办理终结手续后，裁判统一宣布离场后，所有选手方可离场。

（六）成绩评定与结果公布

1. 结果评分

由评分裁判依据评分表，对参赛队所提交的答案（结果性评分）和系统自动统计的数据（机考评分）进行评分（总分为 1000 分）。

2. 解密

裁判长正式提交工位号评分结果并复核无误后，加密裁判在监督人员监督下对加密结果进行逐层解密，形成成绩表，并由裁判长、监督员签字确认。

3. 成绩公布

将解密后的各参赛队得分结果汇总，经裁判长、监督员和专家组长及巡视员签字后，在指定地点，以纸质形式向全体参赛队进行公布，并在成绩发布会上予以宣布。

七、技术规范

（一）标准与规范

本赛项涉及的信息网络安全工程在设计、组建过程中，主要有以下 9 项国家或国际标准，参赛队在实施竞赛项目中要求遵循如下规范。

表 3 标准和技术规范一览表

序号	标准号	中文标准名称
1	WSC2022_WSO554_Cyber_Security	《世界技能大赛网络安全项目职业标准》
2	4-04-04-02	《网络与信息安全管理员》
3	4-04-04-04	《信息安全测试员》
4	GB/T 22239-2019	《信息安全技术网络安全等级保护基本要求》
5	GB/T 28448-2019	《信息安全技术网络安全等级保护测评要求》
6	GB/T 36627-2018	《信息安全技术网络安全等级保护测试评估技术指南》
7	GB／T 31509-2015	《信息安全技术信息安全风险评估实施指南》
8	ISO17799	《信息安全管理实施细则》
9	ISO/IEC 27001	《信息安全管理体系》

（二）知识点和技能点

本赛项涉及的知识点与技能点如下。

表 4 知识点和技能点一览表

序号	内容模块	具体内容	知识点或技能点
第一阶段	网络平台搭建	网络规划	VLSM、CIDR 等
		基础网络	VLAN、WLAN、STP、SVI、RIPV2、OSPF、BGP、IPv6、组播等

序号	内容模块	具体内容	知识点或技能点
	网络安全设备配置与防护	访问控制	保护网络应用安全；实现防 DOS、DDOS 攻击；实现包过滤、应用层代理、状态化包过滤、URL 过滤；基于 IP、协议、应用、用户角色、自定义数据流和时间等方式的带宽控制、QoS 策略等
		密码学和 VPN	密码学基本理论、L2L IPSec VPN、GRE Over IPSec、L2TP Over IPSec、IKE: PSK、IKE: PKI、SSL VPN 等
		数据分析	利用日志系统对网络内的数据进行分析、安全管理等
第二阶段	网络安全事件响应、数字取证调查、应用程序安全	网络安全事件响应	操作系统日志、应用系统/中间件日志、系统进程分析、系统安全漏洞及加固等
		数字取证调查	内存镜像分析、编码转换、加解密、数据隐写、文件分析取证、网络流量包分析等
		应用程序安全	程序逆向分析、移动应用程序代码分析、恶意脚本代码分析等
第三阶段	网络安全渗透	针对预设的环境进行渗透测试	SQL 注入、文件上传、命令执行、缓冲区溢出、信息收集、逆向文件分析、二进制漏洞利用、应用服务漏洞利用、操作系统漏洞利用、密码学分析等
	理论技能与职业素养	网络与信息安全理论知识和职业素养	信息安全与网络基础、操作系统安全、网络协议安全、网络设备安全、网络数据安全、程序代码安全、网络安全渗透、安全运维与应急服务、密码技术、网络安全法律法规和职业素养等

八、技术环境

（一）竞赛环境

竞赛场地配置：保证良好的采光、照明和通风。提供稳定的水、电、网络和供电应急设备。竞赛场地面积需≥参赛队伍数量*10 m^2。

竞赛工位配置：每个操作平台面积≥8m²、工位间隔＞1.5m，需注明工位号并配备符合安全标准的 220V 电源。

赛场区域配置：选手竞赛区、裁判工作区、技术支持区、裁判评分区、观摩区、仲裁室等。

（二）竞赛设备

表 5 竞赛设备一览表

序号	设备名称	数量	参考型号
1	PC 机	3 台/组	CPU：I5 及以上，主频≥2.3GHZ; 硬盘：SSD 1TB 及以上; 内存：16GB 及以上
2	三层交换机	1 台/组	神州数码 CS6200-28X-Pro
3	防火墙	1 台/组	神州数码 DCFW-1800E-N3002-Pro
4	Web 应用防火墙	1 台/组	神州数码 DCFW-1800-WAF-P
5	网络日志系统	1 台/组	神州数码 DCBC-NetLog
6	无线交换机	1 台/组	神州数码 DCWS-6028-Pro
7	无线接入点	1 台/组	神州数码 WL8200-I2
8	服务器	1 台/组	神州数码 DCST-6000B-Pro

（三）竞赛软件

表 6 竞赛软件一览表

序号	软件	版本
1	Windows 操作系统	Windows 10 及以上版本
2	Microsoft Office	Microsoft Office 2010 及以上版本
4	VMware Workstation	Version 12 及以上版本
5	Windows Server DataCenter	2016 及以上版本
6	Linux(CentOS)	Version 7.6.1810
7	Ubuntu	20.04
8	Wireshark	3.4.9
9	bind	9.11.4

序号	软件	版本
10	Kali	Version2021.3
11	IDA free	7.0
12	OllyDbg	Version1.10 及以上版本
13	PDF Reader	
14	Volatility	Version2.6 及以上版本
15	Autopsy	Version4.0 及以上版本
16	WinDbg	Version4.0 及以上版本
17	Jadx-gui	1.2.0
18	apktool	2.6.1
19	Android Studio	2021.3.1
20	HxD Hex Editor	Version 2.X 及以上版本
21	Android Emulator	API27
22	StegSolve	1.4
23	audacity	3.1.0
24	Parrot-security	4.11.2
25	gdb-pwndbg	2021.06.22
26	sagemath	9.2
27	pwntools	4.5.0
28	pycryptodome	3.14.1
29	frida-server	15.1.10
30	frida-tools	10.4.1
31	VsCode	X64-1.6.1
32	Frp	0.38.0
33	Neo-reGeorg	v3.7.0
34	EmEditor Free	V21.5.2
35	Putty	0.68 及以上版本
36	VNC viewer	1.2.1.2
37	Virtual Box	6.1.28
38	CaptfEncoder	2.1.0
39	BeautifulSoup4	4.9.3
40	one_gadget	1.7.4
41	超级终端	设备调试连接工具

九、竞赛样卷

2023—2024 年重庆市职业院校技能大赛（高等职业教育）

“信息安全管理与评估”样题

竞赛需要完成三个阶段的任务,分别完成三个模块,总分共计 1000 分。三个模块内容和分值分别是:

1.第一阶段：模块一 网络平台搭建与设备安全防护（180 分钟，300 分）。

2.第二阶段：模块二 网络安全事件响应、数字取证调查、应用程序安全（180 分钟，300 分）。

3.第三阶段：模块三 网络安全渗透、理论技能与职业素养（180 分钟，400 分）。

【注意事项】

1.第一个阶段需要按裁判组专门提供的 U 盘中的“XXX-答题模板”提交答案。

第二阶段请根据现场具体题目要求操作。

第三阶段网络安全渗透部分请根据现场具体题目要求操作，理论测试部分根据测试系统说明进行登录测试。

2.所有竞赛任务都可以由参赛选手根据基础设施列表中指定的设备和软件完成。

第一阶段

模块一 网络平台搭建与设备安全防护

一、竞赛内容

第一阶段竞赛内容包括：网络平台搭建、网络安全设备配置与防护，共 2 个子任务。

竞赛阶段	任务阶段	竞赛任务	竞赛时间	分值
第一阶段 网络平台搭建与 设备安全防护	任务 1	网络平台搭建	XX:XX- XX:XX	50
	任务 2	网络安全设备配置与防护		250
总分				**300**

二、竞赛时长

本阶段竞赛时长为 180 分钟，共 300 分。

三、注意事项

第一阶段请按裁判组专门提供的 U 盘中的“XXX-答题模板”中的要求提交答案。

选手需要在 U 盘的根目录下建立一个名为“GWxx”的文件夹（xx 用具体的工位号替代），所完成的“XXX-答题模板”放置在文件夹中作为竞赛结果提交。

例如：08 工位，则需要在 U 盘根目录下建立“GW08”文件夹，并在“GW08”文件夹下直接放置第一个阶段的所有“XXX-答题模板”文件。

【特别提醒】

只允许在根目录下的“GWxx”文件夹中体现一次工位信息，不允许在其它文件夹名称或文件名称中再次体现工位信息，否则按作弊处理。

五、赛项环境设置

1.网络拓扑图

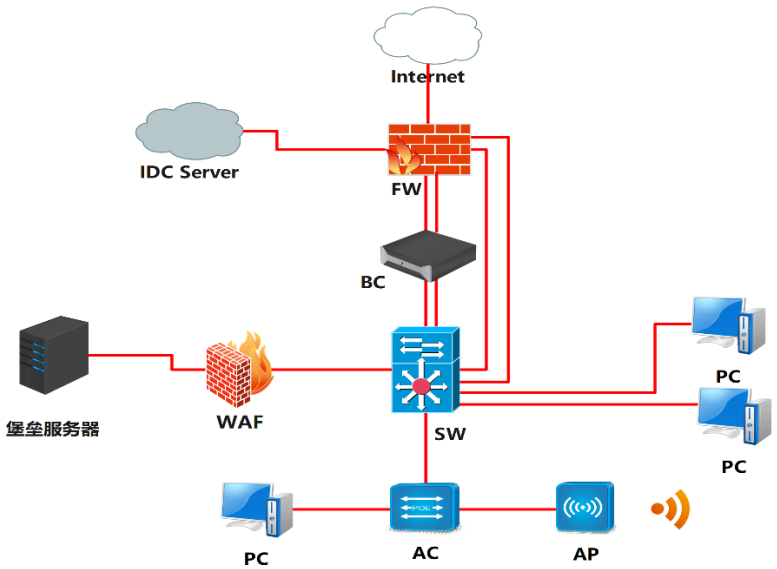

图 1 网络拓扑图

2.IP 地址规划表

设备名称	接口	IP 地址	对端设备
防火墙 FW	ETH0/1-2（AG1）	AG1.113 10.1.0.254/30 （Trust 安全域）	SW ETH1/0/1 SW ETH1/0/2
		AG1.114 10.2.0.254/30 （Trust 安全域）	
	ETH0/3	10.3.0.254/30 （Trust 安全域）	BC ETH3
	ETH0/4	10.4.0.254/30 （Trust 安全域）	BC ETH4
	ETH0/5	10.100.18.1/27 （untrust 安全域）	IDC SERVER 10.100.18.2
	ETH0/6	200.1.1.1/28 （untrust 安全域）	INTERNET
	Loopback1	10.11.0.1/24 （Trust 安全域）	-
	Loopback2	10.12.0.1/24 （Trust 安全域）	
	Loopback3	10.13.0.1/24 （Trust 安全域）	
	Loopback4	10.14.0.1/24 （Trust 安全域）	
路由交换机 SW	VLAN 40 ETH1/0/4-8	172.16.40.62/26	PC2
	VLAN 50	172.16.50.62/26	PC3

设备名称	接口	IP 地址	对端设备
	ETH1/0/3		
	VLAN 51 ETH1/0/23	10.51.0.254/30	BC ETH5
	VLAN 52 ETH1/0/24	10.52.0.254/24	WAF ETH3
	VLAN 113 ETH1/0/1	VLAN113 OSPF 10.1.0.253/30	FW ETH0/1
	VLAN 114 ETH1/0/2	VLAN114 OSPF 10.2.0.253/30	FW ETH0/2
	VLAN 117 ETH E1/0/17	10.3.0.253/30	BC ETH1
	VLAN 118 SW ETH E1/0/18	10.4.0.253/30	BC ETH2
	ETH1/0/20	VLAN 100 192.168.100.1/30 2001::192:168:100:1/112 VLAN115 OSPF 10.5.0.254/30 VLAN116 OSPF 10.6.0.254/30	AC ETH1/0/20
无线控制器 AC	ETH1/0/20	VLAN 100 192.168.100.2/30 2001::192:168:100:2/112 VLAN 115 10.5.0.253/30 VLAN 116 10.6.0.253/30	SW ETH1/0/20
	VLAN 30 ETH1/0/3	172.16.30.62/26	PC1
	无线管理 VLAN VLAN 101 ETH1/0/21	需配置	AP
	VLAN 10	需配置	无线 1
	VLAN 20	需配置	无线 2
网络日志系统 BC	ETH1	网桥	FW
	ETH3		SW ETH E1/0/17
	ETH2	网桥	FW
	ETH4		SW ETH E1/0/18
	ETH5	10.51.0.253/30	SW ETH E1/0/23
Web 应用 防火墙 WAF	ETH3	10.52.0.253/30	SW ETH E1/0/24
	ETH4		堡垒服务器

第一阶段 任务书

任务 1 网络平台搭建（50 分）

题号	网络需求
1	按照 IP 地址规划表，对防火墙的名称、各接口 IP 地址进行配置
2	按照 IP 地址规划表，对三层交换机的名称进行配置，创建 VLAN 并将相应接口划入 VLAN, 对各接口 IP 地址进行配置
3	按照 IP 地址规划表，对无线交换机的名称进行配置，创建 VLAN 并将相应接口划入 VLAN,对接口 IP 地址进行配置
4	按照 IP 地址规划表，对网络日志系统的名称、各接口 IP 地址进行配置
5	按照 IP 地址规划表，对 Web 应用防火墙的名称、各接口 IP 地址进行配置

任务 2 网络安全设备配置与防护（250 分）

1.SW 开启 telnet 登录功能，用户名 skills01，密码 skills01，密码呈现需加密。

2.总部交换机 SW 配置简单网络管理协议，计划启用 V3 版本，V3 版本在安全性方面做了极大的扩充。配置引擎号分别为 62001；创建认证用户为 skills01，采用 3des 算法进行加密，密钥为：skills01，哈希算法为 SHA，密钥为：skills01；加入组 ABC，采用最高安全级别；配置组的读、写视图分别为：2023_R、2023_W；当设备有异常时，需要使用本地的 VLAN100 地址发送 Trap 消息至网管服务器 10.51.0.203，采用最高安全级别。

3.接入 SW Eth4，仅允许 IP 地址 172.16.40.62-80 为源的数据包为合法包，以其它 IP 地址为源地址，交换机直接丢弃。

4.为减少内部 ARP 广播询问 VLAN 网关地址，在全局下配置 SW 每隔 300S 发送免费 ARP。

5.勒索蠕虫病毒席卷全球，爆发了堪称史上最大规模的网络攻击，通过对总部核心交换机 SW 所有业务 VLAN 下配置访问控制策略实现双向安全防护。

6.SW 配置 IPv6 地址，使用相关特性实现 VLAN50 的 IPv6 终端可自动从网关处获得 IPv6 有状态地址。

7.AC 配置 IPv6 地址，开启路由公告功能，路由器公告的生存期为 2 小时，确保 VLAN30 的 IPv6 终端可以获得 IPv6 无状态地址。

8.AC 与 SW 之间配置 RIPng，使 PC1 与 PC3 可以通过 IPv6 通信。

9.IPv6 业务地址规划如下，其它 IPv6 地址自行规划:

业务	**IPV6 地址**
VLAN30	2001:30::254/64
VLAN50	2001:50::254/64

10.FW、SW、AC 之间配置 OSPF area 0 开启基于链路的 MD5 认证，密钥自定义,传播访问 INTERNET 默认路由。

11.FW 与 SW 建立两对 IBGP 邻居关系，使用 AS 65500，FW 上 loopback1-4 为模拟 AS 65500 中网络，为保证数据通信的可靠性和负载，完成以下配置，要求如下:

- SW 通过 BGP 到达 loopback1,2 网路下一跳为 10.3.0.254;
- SW 通过 BGP 到达 loopback3,4 网络下一跳为 10.4.0.254。

12.FW 与 SW 建立两对 IBGP 邻居关系，使用 AS 65500，FW 上 loopback1-4 为模拟 AS 65500 中网络，为保证数据通信的可靠性和负载，通过 BGP 实现到达 loopback1,2,3,4 的网络冗余，请完成配置。

13.FW 与 SW 建立两对 IBGP 邻居关系，使用 AS 65500，FW 上 loopback1-4 为模拟 AS 65500 中网络，为保证数据通信的可靠性和负载，使用 IP 前缀列表匹配上述业务数据流，请完成配置。

14.FW 与 SW 建立两对 IBGP 邻居关系，使用 AS 65500，FW 上 loopback1-4 为模拟 AS 65500 中网络，为保证数据通信的可靠性和负载，完成以下配置，使用 LP 属性进行业务选路，只允许使用 route-map 来改变 LP 属性、实现路由控制，LP 属性可配置的参数数值为：200。

15.配置使总部 VLAN50 业务的用户访问 IDC SERVER 的数据流经过 FW 10.1.0.254, IDC SERVER 返回数据流经过 FW 10.2.0.254，且对双向数据流开启所有安全防护，参数和行为为默认。

16.在端口 ethernet1/0/7 上，将属于网段 172.16.40.62/26 内的报文带宽限制为 10M 比特/秒，突发 4M 字节，超过带宽的该网段内的报文一律丢弃。

17.在 FW 上配置，连接 LAN 接口开启 PING 等所有管理方式，连接 Internet 接口关闭所有管理方式，配置 trust 区域与 Untrust 之间的安全策略且禁止从外网访问内网的任何设备。

18.总部 VLAN 业务用户通过防火墙访问 Internet 时，复用公网 IP: 200.1.1.28/28，保证每一个源 IP 产生的所有会话将被映射到同一个固定的 IP 地址，当有流量匹配本地址转换规则时产生日志信息，将匹配的日志发送至 10.51.0.253 的 UDP 2000 端口。

19.为了合理利用网络出口带宽，需要对内网用户访问 Internet 进行流量控制，园区总出口带宽为 200M，对除无线用户以外的用户

限制带宽，每天上午 9:00 到下午 6:00 每个 IP 最大下载速率为 2Mbps，上传速率为 1Mbps。

20.配置 L2TP VPN，名称为 VPN，满足远程办公用户通过拨号登陆访问内网，创建隧道接口为 tunnel 1、并加入 untrust 安全域，地址池名称为 AddressPool，LNS 地址池为 10.100.253.1/24-10.100.253.100/24，网关为最大可用地址，认证账号 skills01,密码 skills01。

21.Internet 端有一分支结构路由器，需要在总部防火墙 FW 上完成以下预配，保证总部与分支机构的安全连接：防火墙 FW 与 Internet 端路由器 202.5.17.2 建立 GRE 隧道，并使用 IPSec 保护 GRE 隧道，保证分支结构中 2.2.2.2 与总部 VLAN40 安全通信。
16.Internet 端有一分支结构路由器，需要在总部防火墙 FW 上完成以下预配，保证总部与分支机构的安全连接:

- 第一阶段　采用 pre-share 认证 加密算法:3DES;
- 第二阶段　采用 ESP 协议，　加密算法:3DES，预设共享秘钥: skills01。

22.Vlan30 内的工作人员涉及到商业机密，因此在 FW 上配置不允许 vlan30 内所有用户访问外网。

23.配置出于安全考虑，无线用户访问因特网需要采用认证，在防火墙上配置 Web 认证，采用本地认证，用户名为 test，test1，test2，密码为 123456。

24.已知原 AP 管理地址为 10.81.0.0/15，为了避免地址浪费请重新规划和配置 IP 地址段，使用原 AP 所在网络进行地址划分，请完成配置。

25.已知原 AP 管理地址为 10.81.0.0/15，为了避免地址浪费请重新规划和配置 IP 地址段，现无线用户 VLAN 10 中需要 127 个终端，无线用户 VLAN 20 需要 50 个终端，请完成配置。

26.已知原 AP 管理地址为 10.81.0.0/15，为了避免地址浪费请重新规划和配置 IP 地址段，要求完成在 AC 上配置 DHCP，管理 VLAN 为 VLAN101,为 AP 下发管理地址，网段中第一个可用地址为 AP 管理地址，最后一个可用地址为 AC 管理地址，保证完成 AP 二层注册；为无线用户 VLAN10,20 下发 IP 地址，最后一个可用地址为网关。

27.在 NETWORK 下配置 SSID，需求如下:

● NETWORK 1 下设置 SSID 2023skills-2.4G，VLAN10，加密模式为 wpa-personal,其口令为 skills01;

● NETWORK 20 下设置 SSID 2023skills-5G，VLAN20 不进行认证加密,做相应配置隐藏该 SSID。

28.配置一个 SSID 2023skills_IPv6，属于 VLAN21 用于 IPv6 无线测试，用户接入无线网络时需要采用基于 WPA-personal 加密方式，其口令为“skills01”，该网络中的用户从 AC DHCP 获取 IPv6 地址，地址范围为：2001:10:81::/112。

29.NETWORK 1 开启内置 portal+本地认证的认证方式，账号为 GUEST 密码为 123456,保障无线信息的覆盖性，无线 AP 的发射功率设置为 90%。禁止 MAC 地址为 80-45-DD-77-CC-48 的无线终端连接。

30.2023skills-5G 最多接入 20 个用户，用户间相互隔离，并对 2023skills-5G 网络进行流控，上行速率 1Mbps，下行速率 2Mbps。

31.在 AC 上配置使 radio 1 的射频类型为 IEEE 802.11b/g,并且设置 RTS 的门限值为 256 字节，当 MPDU 的长度超过该值时，802.11MAC 启动 RTS/CTS 交互机制。

32.在 AC 上配置一条基于 SSID 时间点时周一 0 点到 6 点的禁止用户接入的策略（限时策略）。

33.通过配置防止多 AP 和 AC 相连时过多的安全认证连接而消耗 CPU 资源，检测到 AP 与 AC 在 10 分钟内建立连接 5 次就不再允许继续连接，两小时后恢复正常。

34.配置所有无线接入用户相互隔离，Network 模式下限制每天 0 点到 6 点禁止终端接入，开启 ARP 抑制功能。

35.在公司总部的 BC 上配置，设备部署方式为透明模式。增加非 admin 账户 skills01，密码 skills01，该账户仅用于用户查询设备的日志信息和统计信息；要求对内网访问 Internet 全部应用进行日志记录。

36.BC 上配置用户认证识别功能。

37.在公司总部的 BC 上配置，在工作日（每周一到周五上班）期间针对所有无线网段访问互联网进行审计，如果发现访问互联网的无线用户就断网，不限制其他用户在工作日（每周一到周五上班）期间访问互联网。

38.使用 BC 对内网所有上网用户进行上网本地认证，要求认证后得用户 3 小时候重新认证，并且对 HTTP 服务器 172.16.10.45 的 80 端口进行免认证。

39. BC 配置应用“即时聊天”，在周一至周五 9：00-21：00 监控内网中所有用户的微信账号使用记录，并记录数据。

40.在 BC 上配置激活 NTP，本地时区+8:00，并添加 NTP 服务器名称清华大学，域名为 s1b.time.edu.cn。

41. BC 配置内容管理，对邮件内容包含“比赛答案”字样的邮件，记录且邮件报警。

42.BI 监控周一至周五工作时间 VLAN40 用户使用“迅雷”的记录，每天工作时间为 9:00-18:00。

43.在公司总部的 WAF 上配置，设备部署方式为透明模式。要求对内网 HTTP 服务器 172.16.10.45/32 进行安全防护。

44.方便日志的保存和查看，需要在把 WAF 上攻击日志、访问日志、DDoS 日志以 JSON 格式发给 IP 地址为 172.16.10.200 的日志服务器上。

45.在 WAF 上配置基础防御功能，开启 SQL 注入、XXS 攻击、信息泄露等防御功能，要求针对这些攻击阻断并发送邮件告警。

46.为防止 www.2023skills.com 网站资源被其他网站利用，通过 WAF 对资源链接进行保护，通过 Referer 方式检测，设置严重级别为中级，一经发现阻断并发送邮件告警。

47.在公司总部的 WAF 上配置，编辑防护策略，定义 HTTP 请求体的最大长度为 256，防止缓冲区溢出攻击。

48.对公司内网用户访问外网进行网页关键字过滤，网页内容包含“暴力”“赌博”的禁止访问。

49.为了安全考虑，无线用户移动性较强，访问因特网时需要实名认证，在 BC 上开启 web 认证使用 http 方式，采用本地认证，密码账号都为 web2023。

50.在 WAF 上保护 HTTP 服务器上的 www.2023skills.com 网站爬虫攻击，从而影响服务器性能，设置严重级别为高级，一经发现攻击阻断并发送邮件告警。

第二阶段

模块二 网络安全事件响应、数字取证调查、应用程序安全

一、竞赛内容

第二阶段竞赛内容包括：网络安全事件响应、数字取证调查和应用程序安全。

竞赛阶段	任务阶段		竞赛任务	竞赛时间	分值
第二阶段 网络安全事件响应、数字取证调查和应用程序安全	网络安全事件响应	任务 1	应用响应	XX:XX-XX:XX	70
	数字取证调查	任务 2	操作系统取证		40
		任务 3	网络数据包分析		50
		任务 4	计算机单机取证		60
	应用程序安全	任务 5	恶意代码分析		50
		任务 6	代码审计		30
总分					**300**

二、竞赛时长

本阶段竞赛时长为 180 分钟，共 300 分。

三、注意事项

1.本部分的所有工作任务素材或环境均已放置在指定的计算机上，参赛选手完成后，填写在电脑桌面上“信息安全管理与评估竞赛-第二阶段答题卷”中。

2.选手的电脑中已经安装好 Office 软件并提供必要的软件工具（Tools 工具包）。

【特别提醒】

竞赛有固定的开始和结束时间，选手必须决定如何有效的分配时间。请阅读以下指引！

1.当竞赛结束，**离开时请不要关机**;

2.所有配置应当在重启后有效;

3.除了 CD-ROM/HDD/NET 驱动器，请不要修改实体机的配置和虚拟机本身的硬件设置。

第二阶段 任务书

任务描述

随着网络和信息化水平的不断发展，网络安全事件也层出不穷，网络恶意代码传播、信息窃取、信息篡改、远程控制等各种网络攻击行为已严重威胁到信息系统的机密性、完整性和可用性。因此，对抗网络攻击，组织安全事件应急响应，采集电子证据等技术工作是网络安全防护的重要部分。现在，A 集团已遭受来自不明组织的非法恶意攻击，您的团队需要帮助 A 集团追踪此网络攻击来源，分析恶意攻击行为的证据线索，找出操作系统和应用程序中的漏洞或者恶意代码，帮助其巩固网络安全防线。

本模块主要分为以下几个部分:

- 网络安全事件响应;
- 数字取证调查;
- 应用程序安全。

第一部分 网络安全事件响应

任务 1 应急响应（70 分）

A 集团的 WebServer 服务器被黑客入侵，该服务器的 Web 应用系统被上传恶意软件，系统文件被恶意软件破坏，您的团队需要帮助该公司追踪此网络攻击的来源，在服务器上进行全面的检查，包括日志信息、进程信息、系统文件、恶意文件等，从而分析黑客的攻击行为，和残留的关键证据信息。

本任务素材清单：Server 服务器虚拟机

受攻击的 Server 服务器已整体打包成虚拟机文件保存，请选手自行导入分析。

虚拟机用户名：root，密码：123456，若题目中未明确规定，请使用默认配置。

请按要求完成该部分工作任务，答案有多项内容的请用换行分隔。

任务 1 应急响应		
序号	任务要求	答案
1	提交攻击者的两个内网 IP 地址	
2	提交网站管理员用户的用户名与密码	
3	提交黑客得到 MySQL 服务的 root 账号密码的时间（格式：dd/MM/yyyy:hh:mm:ss）	
4	查找黑客在 Web 应用文件中写入的恶意代码，提交文件绝对路径	
5	查找黑客在 Web 应用文件中写入的恶意代码，提交代码的最简形式（格式：<?php xxxx?>）	
6	分析攻击者的提权手法，提交攻击者通过哪一个指令成功提权	
7	服务器内与动态恶意程序相关的三个文件绝对路径	
8	恶意程序对外连接的目的 ip 地址	

第二部分 数字取证调查

任务 2　操作系统取证（40 分）

A 集团某电脑系统感染恶意程序，导致系统关键文件被破坏，请分析 A 集团提供的系统镜像和内存镜像，找到系统镜像中的恶意软件，分析恶意软件行为。

本任务素材清单：操作系统镜像、内存镜像（*.dump、*.img）

请按要求完成该部分的工作任务。

任务 2 操作系统取证		
序号	任务要求	答案
1	提交恶意进程名称（两个）	
2	被破坏的文件位置	
3	加密数据的内存地址	
4	原文件内容	
5	分析恶意程序行为	

任务 3 网络数据包分析（50 分）

A 集团的网络安全监控系统发现有恶意攻击者对集团官方网站进行攻击，并抓取了部分可疑流量包。请您根据捕捉到的流量包，搜寻出网络攻击线索，并分析黑客的恶意行为。

本任务素材清单：捕获的网络数据包文件（*.pcapng）

请按要求完成该部分的工作任务，答案有多项内容的请用换行分隔。

任务 3 网络数据包分析		
序号	任务要求	答案
1	提交恶意程序传输协议 （只提交一个协议，两个以上视为无效）	
2	恶意程序对外连接目标 IP	
3	恶意程序加载的 dll 文件名称	

4	解密恶意程序传输内容	
5	分析恶意程序行为	

任务 4 计算机单机取证（60 分）

对给定取证镜像文件进行分析，搜寻证据关键字（线索关键字为“evidence 1”“evidence 2”……“evidence 10”，有文本形式也有图片形式，不区分大小写），请提取和固定比赛要求的标的证据文件，并按样例的格式要求填写相关信息，证据文件在总文件数中所占比例不低于15%。取证的信息可能隐藏在正常的、已删除的或受损的文件中，您可能需要运用编码转换技术、加解密技术、隐写技术、数据恢复技术，还需要熟悉常用的文件格式（如办公文档、压缩文档、图片等）。

本任务素材清单：取证镜像文件

请根据赛题环境及现场答题卡任务要求提交正确答案。

任务 4 计算机单机取证		
证据编号	**原始文件名 （不包含路径）**	**镜像中原文件 Hash 码 （MD5，不区分大小写）**
evidence 1		
evidence 2		
evidence 3		
evidence 4		
evidence 5		
evidence 6		
evidence 7		
evidence 8		
evidence 9		
evidence 10		

第三部分 应用程序安全

任务 5 恶意程序分析（50 分）

A 集团发现其发布的应用程序文件遭到非法篡改，您的团队需要协助 A 集团对该恶意程序样本进行逆向分析、对其攻击/破坏的行为进行调查取证。

本任务素材清单：恶意程序代码

请按要求完成该部分的工作任务。

任务 5 恶意程序分析		
序号	任务内容	答案
1	请提交素材中的恶意应用回传数据的 url 地址	
2	请提交素材中的恶意代码保存数据文件名称（含路径）	
3	请描述素材中恶意代码的行为	
4	.....	

任务 6 代码审计（30 分）

代码审计是指对源代码进行检查，寻找代码存在的脆弱性，这是一项需要多方面技能的技术。作为一项软件安全检查工作，代码安全审查是非常重要的一部分，因为大部分代码从语法和语义上来说是正确的，但存在着可能被利用的安全漏洞，你必须依赖你的知识和经验来完成这项工作。

本任务素材清单：源文件

请按要求完成该部分的工作任务。

任务 6 代码审计		
序号	任务内容	答案
1	请指出存在安全漏洞的代码行	

2	请指出可能利用该漏洞的威胁名称	
3	请提出加固修改建议	
4	.....	

第三阶段

模块三 网络安全渗透、理论技能与职业素养

一、竞赛内容

第三阶段竞赛内容是：网络安全渗透、理论技能与职业素养。

本阶段分为两个部分。第一部分主要是在一个模拟的网络环境中实现网络安全渗透测试工作，要求参赛选手作为攻击方，运用所学的信息收集、漏洞发现、漏洞利用等渗透测试技术完成对网络的渗透测试；并且能够通过各种信息安全相关技术分析获取存在的 flag 值。第二部分是在理论测试系统中进行考核。

竞赛阶段	任务阶段		竞赛任务	竞赛时间	分值
第三阶段网络安全渗透、理论技能与职业素养	网络安全渗透	第一部分：网站	任务 1～任务 3	XX:XX-XX:XX	45
		第二部分：应用系统	任务 4～任务 5		30
		第三部分：应用服务器 1	任务 6～任务 13		165
		第四部分：应用服务器 2	任务 14		30
		第五部分：应用服务器 2	任务 15		30
	第六部分：理论技能与职业素养				100
总分					**400**

二、竞赛时长

本阶段竞赛时长为 180 分钟，其中网络安全渗透 300 分，理论技能与职业素养 100 分，共 400 分。

三、注意事项

通过找到正确的 flag 值来获取得分，flag 统一格式如下所示:

flag{<flag 值 >}

这种格式在某些环境中可能被隐藏甚至混淆。所以，注意一些敏感信息并利用工具把它找出来。

【特别提醒】部分 flag 可能非统一格式，若存在此情况将会在题目描述中明确指出 flag 格式，请注意审题。

第三阶段 任务书

任务描述

在 A 集团的网络中存在几台服务器，各服务器存在着不同业务服务。在网络中存在着一定网络安全隐患，请利用您所掌握的渗透测试技术，通过信息收集、漏洞挖掘等渗透测试技术，完成指定项目的渗透测试，在测试中获取 flag 值。网络环境参考样例请查看附录 A。

本模块所使用到的渗透测试技术包含但不限于如下技术领域:

- 数据库攻击;
- 枚举攻击;
- 权限提升攻击;
- 基于应用系统的攻击;
- 基于操作系统的攻击;
- 逆向分析;
- 密码学分析;
- 隐写分析。

所有设备和服务器的 IP 地址请查看现场提供的设备列表，请根据赛题环境及现场答题卡任务要求提交正确答案。

第一部分 网站（45 分）

任务编号	任务描述	答案	分值
任务 1	门户网站存在漏洞，请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 2	门户网站存在漏洞，请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 3	门户网站存在漏洞，请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

第二部分 应用系统（30 分）

任务编号	任务描述	答案	分值
任务 4	应用系统存在漏洞，请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 5	应用系统存在漏洞，请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

第三部分 应用服务器 1（165 分）

任务编号	任务描述	答案	分值
任务 6	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 7	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 8	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 9	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

任务 10	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 11	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 12	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 13	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

第四部分 应用服务器 2（30 分）

任务编号	任务描述	答案	分值
任务 14	应用系统服务器 10000 端口存在漏洞，获取 FTP 服务器上对应的文件进行分析，请利用漏洞找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

第五部分 应用服务器 3（30 分）

任务编号	任务描述	答案	分值
任务 15	应用系统服务器 10001 端口存在漏洞，获取 FTP 服务器上对应的文件进行分析，请利用漏洞找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

附录 A

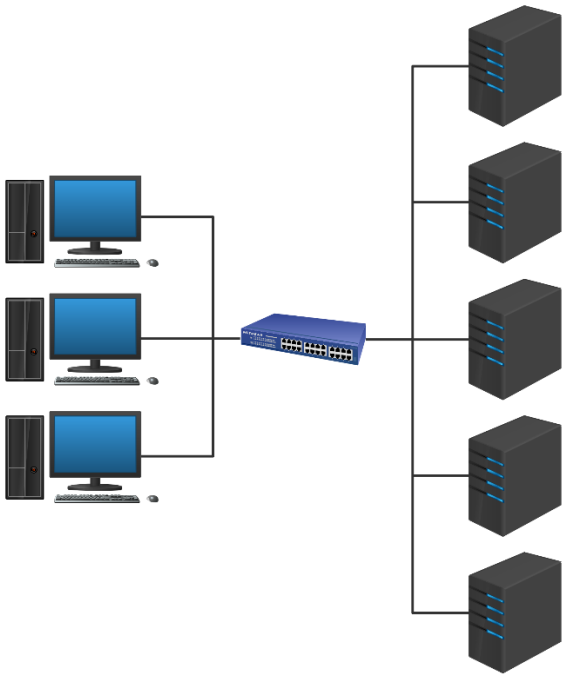

图 2 网络拓扑结构图

第六部分 理论技能与职业素养（100 分）

2023—2024 年重庆市职业院校技能大赛（高等职业教育）

“信息安全管理与评估”测试题（样题）

【注意事项】

1.理论测试前请仔细阅读提供的测试系统使用说明书，按提供的账号和密码登录测试系统进行测试，账号只限 1 人登录。

2.该部分答题时长包含在第三阶段竞赛时长内，请在临近竞赛结束前提交。

3.参赛团队可根据自身情况，可选择 1-3 名参赛选手进行作答，参赛队内部可以进行交流，但不得影响其他团队。

一、 单选题（每题 2 分，共 35 题，共 70 分）

1.将用户 user123 修改为管理员权限命令是（ ）。

A. net user localgroup administrators user123 /add

B. net use localgroup administrators user123 /add

C. net localgroup administrators user123 /add

D. net localgroup administrator user123 /add

2. SQL 注入出 password 的字段值为“YWRtaw44ODg=”，这是采用了哪种加密方式？（　　）

A. md5

B. base64

C. AES

D. DES

3.下列哪个工具可以进行 Web 程序指纹识别？（　　）

A. Nmap

B. OpenVAS

C. 御剑

D. WhatWeb

4.ELK 日志解决方案中，Elasticsearch 的作用是？（　　）

A. 收集日志并分析

B. 保存日志并搜索日志

C. 收集日志并保存

D. 保存日志并展示日志

5.RIP 路由协议有 RIP v1 和 RIP v2 两个版本，下面关于这两个版本的说法错误的是（　　）。

A.RIP v1 和 RIP v2 都具有水平分割功能

B.RIP v1 是有类路由协议，RIP v2 是无类路由协议

C.RIP v1 和 RIP v2 都是以跳数作为度量值

D.RIP v1 规定跳数的最大值为 15，16 跳视为不可达，而 RIP v2 无此限制

6.如果明文为 abc，经凯撒密码-加密后，密文 bcd，则密钥是（　　）。

A.1

B.2

C.3

D.4

7.哪个关键词可以在 Python 中进行处理错误操作？（　　）

A.try

B.catch

C.finderror

D.error

8.关闭默认共享 C$的命令是（　　）。

A.net share C$ /del

B.net share C$ /close

C.net use C$ /del

D.net user C$ /del

9.DNS 服务器根据查询方式可以分为多种，以下（　　）方式可以通过 IP 查找域名。

A.递归查询

B.迭代查询

C.正向查询

D.反向查询

10.域完整性指特定列的项的有效性。那么通过（　　）可以强制域完整性限制格式。

A.UNIQUE 约束

B.CHECK 约束和规则

C.PRIMARY KEY 约束

D.FOREIGN KEY 约束

11.客户机从 DHCP 服务器获得 IP 地址的过程称为 DHCP 的租约过程，在服务器发送 DHCP Offer 广播包时，DHCP Offer 中的目的地址是（　　）。

A.255.0.0.0

B.255.255.0.0

C.255.255.255.0

D.255.255.255.255

12.通过使用下列（　　）方式，无法获取对方密码。

A.DDOS 攻击

B.字典攻击

C.网络钓鱼

D.暴力破解

13.在常见的安全扫描工具中，以下（　　）主要用来分析 Web 站点的漏洞，可以针对数千种常见的网页漏洞或安全风险进行检测。

A.SuperScan

B.Fluxay（流光）

C.Wikto

D.MBSA

14.在 PKI 公钥体系应用中，数据机密性指的是（　　）。

A.确认用户的身份标识

B.保证数据在传送过程中没有被修改

C.防止非授权的用户获取数据

D.确保用户不能冒充其他用户的身份

15.AES 结构由以下四个不同的模块组成，其中(　　)是非线性模块。

A.字节代换

B.行位移

C.列混淆

D.轮密钥加

16.Skipjack 是一个密钥长度为（　　）位。

A.56

B.64

C.80

D.128

17.现今非常流行的 SQL（数据库语言）注入攻击属于下列哪一项漏洞的利用？（　　）

A.域名服务的欺骗漏洞

B.邮件服务器的编程漏洞

C.WWW 服务的编程漏洞

D.FTP 服务的编程漏洞

18.ARP 欺骗的实质是（　　）。

A.提供虚拟的 MAC 与 IP 地址的组合

B.让其他计算机知道自己的存在

C.窃取用户在网络中的传输的数据

D.扰乱网络的正常运行

19.下列哪一种网络欺骗技术是实施交换式（基于交换机的网络环境）嗅探攻击的前提（　　）。

A.IP 欺骗

B.DNS 欺骗

C.ARP 欺骗

D.路由欺骗

20.目标计算机与网关通信失败，更会导致通信重定向的攻击形式是？（　　）

A.病毒

B.木马

C.DOS

D.ARP 欺骗

21.IP 数据报分片后的重组通常发生在？（　　）

A.源主机和数据报经过的路由器上

B.源主机上

C.数据报经过的路由器上

D.目的主机上

22.以下关于 VPN 说法正确的是（　　）。

A.VPN 指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路

B.VPN 指的是用户通过公用网络建立的临时的、安全的连接

C.VPN 不能做到信息验证和身份认证

D.VPN 只能提供身份认证、不能提供加密数据的功能

23.Linux 系统中，关于 uname 命令说法错误的是？（　　）

A.-a: 显示所有信息

B.-v: 详细显示信息

C.-r: 内核的 release 发行号

D.-n: 主机名

24.IPSec 包括报文验证头协议 AH 协议号（　　）和封装安全载荷协议 ESP 协议号（　　）。

A.51 50

B.50 51

C.47 48

D.48 47

25.利用虚假 IP 地址进行 ICMP 报文传输的攻击方法称为？（　　）

A.ICMP 泛洪

B.死亡之 ping

C.LAND 攻击

D.Smurf 攻击

26.MD5 散列算法具有（　　）位摘要值。

A.56

B.128

C.160

D.168

27.AH 协议报文头中，32bit 的（　　）结合防重放窗口和报文验证来防御重放攻击。

A.安全参数索引 SPI

B.序列号

C.验证数据

D.填充字段

28.下列不属于信息完整性破坏的是哪一项？（　　）

A.篡改

B.删除

C.复制

D.在信息插入其他信息

29.下列选项哪列不属于网络安全机制？（　　）

A.加密机制

B.数据签名机制

C.解密机制

D.认证机制

30.下列关于网络嗅探技术说明错误的是？（　　）

A.嗅探技术对于已加密的数据无能为力

B.将网卡设置为混杂模式来进行嗅探对于使用交换机且进行了端口和 MAC 绑定的局域网无能为力

C.将网卡设置为混杂模式可以对任意局域网内的数据包进行窃听

D.可以通过配置交换机端口镜像来实现对镜像端口的数据包进行窃听

31.下面不是计算机网络面临的主要威胁的是?（　　）

A.恶意程序威胁

B.计算机软件面临威胁

C.计算机网络实体面临威胁

D.计算机网络系统面临威胁

32. AH 协议报文头中，32bit 的（　　）结合防重放窗口和报文验证来防御重放攻击。

A.安全参数索引 SPI

B.序列号

C.验证数据

D.填充字段

33.Linux 中，通过 chmod 修改权限设置，正确的是？（　　）

A.chmod test.jpg +x

B.chmod u+8 test.jpg

C.chmod 777 test.jpg

D.chmod 888 test.jpg

34.小李在使用 nmap 对目标网络进行扫描时发现，某一个主机开放了 25 和 110 端口，此主机最有可能是什么？（　　）

A.文件服务器

B.邮件服务器

C.WEB 服务器

D.DNS 服务器

35.《中华人民共和国网络安全法》于（　　）起正式施行。

A.2019 年 6 月 1 日

B.2018 年 6 月 1 日

C.2017 年 6 月 1 日

D.2016 年 6 月 1 日

二、 多选题（每题 3 分，共 10 题，共 30 分）

1.下列哪些选项属于误用入侵检测技术？（　　）

A.统计检测

B.基于状态转移的入侵检测

C.基于专家系统的入侵检测

D.基于神经网络的入侵检测

2.利用 Metasploit 进行缓冲区溢出渗透的基本步骤包括（　　）。

A.选择利用的漏洞类型

B.选择 meterpreter 或者 shell 类型的 payload

C.设置渗透目标 IP、本机 IP 地址和监听端口号

D.选择合适的目标类型

3.分组密码常用的算法设计方法包括（　　）。

A.代换

B.扩散和混淆

C.线性反馈移位寄存器

D.J-K 触发器

4.VPN 设计中常用于提供用户识别功能的是（　　）。

A.RADIUS

B.TOKEN 卡

C.数字证书

D.8O2.1

5.在反杀伤链中，情报可以分为那几个层次？（　　）

A.战斗

B.战略

C.战区

D.战术

6.防火墙的主要技术有哪些？（　　）

A.简单包过滤技术

B.网络技术地址转换技术

C.应用代理技术

D.复合技术

7.安全业务指安全防护措施，包括（　　）。

A.保密业务

B.认证业务

C.完整性业务

D.不可否认业务

8.安全的网络通信必须考虑以下哪些方面？（　　）

A.加密算法

B.用于加密算法的秘密信息

C.秘密信息的分布和共享

D.使用加密算法和秘密信息以获得安全服务所需的协议

9.信息道德包括（　　）。

A.网络信息道德

B.学术性信息道德

C.思想品德

D.社会公德

10.我国现行的信息安全法律体系框架分为哪三个层面？（　　）

A.信息安全相关的国家法律

B.信息安全相关的行政法规和部分规章

C.信息安全相关的地方法规/规章和行业规定

D.信息安全相关的个人职业素养

十、赛项安全

（一）组织保障

1. 大赛办组织专门机构负责赛区内赛项的安全工作，建立公安、消防、司法行政、交通、卫生、食品、质检等相关部门协调机制保证比赛安全，制定应急预案，及时处置突发事件。制定相应安全管理的规范、流程和突发事件应急预案，全过程保证比赛筹备和实施工作安全。

2.与地方相关部门建立协调机制，制定应急预案，及时处置突发事件，保证比赛安全进行。

（二）赛项安全管理要求

1.赛场布置，赛场内的器材、设备，应符合国家有关安全规定，并在竞赛现场安排技术支持人员，保障赛项设备安全稳定。

2.竞赛工位张贴安全操作说明。

3.赛前大赛办对全体裁判和工作人员进行安全培训，裁判员要严防选手出现具有危险性的操作。

（三）竞赛环境安全要求

1.承办单位赛前须按照大赛办要求进行现场考察，排除安全隐患。

2.承办单位制定安全制度和应急预案，并配备急救人员与设施。

3.制定人员疏导方案。赛场环境中存在人员密集、车流人流交错的区域，除了设置齐全的指示标志外，须增加引导人员，并开辟备用通道。

4.竞赛现场需要进行网络安全控制，同时严禁易燃易爆以及各类危险品进入。

（四）参赛队伍安全责任

1.各参赛单位须为参赛选手购买大赛期间的人身意外伤害保险。

2.各参赛单位须制定相关管理制度，并对所有选手、指导教师进行安全教育。

3.各参赛单位须加强对参与竞赛人员的安全管理，实现与赛场安全管理的对接。

十一、成绩评定

（一）裁判工作原则

按照《全国职业院校技能大赛专家和裁判工作管理办法》建立重庆职业院校技能大赛赛项裁判库，裁判长由大赛办聘任。赛前建立健全裁判组。裁判组为裁判长负责制，划分裁判小组（2 人为一组），并设有专职督导仲裁员 1-2 名，负责竞赛过程全程监督，防止营私舞弊。本赛项计划需要裁判 7 名，现场裁判 2 名，评分裁判 3 名，加密裁判 3 名。

表 7 裁判建议一览表

序号	专业技术方向	知识能力要求	执裁、教学、工作经历	专业技术职称	人数
1	网络与信息	全面掌握网络平台搭建	省级以上执裁和组织	专业相关高级职	1

序号	专业技术方向	知识能力要求	执裁、教学、工作经历	专业技术职称	人数
	安全（裁判长）	与设备安全防护、网络安全事件响应、数字取证调查、应用程序安全、网络安全渗透等信息安全技术。	执裁经验；具有领导能力，组织协调能力；5年以上相关专业教学经验或相关行业工作经验。	称（高级职业资格证书/技能等级）	
2	网络与信息安全（现场裁判、评分裁判）	至少掌握三个竞赛模块中的一个。	省级以上执裁经验；5年以上相关专业教学经验或相关行业工作经验。	原则上应具有副高级以上专业技术职称或高级技师职业资格	3
3	理工类（加密裁判）	能熟练运用电脑办公软件，认真细致负责完成加密工作。	有责任心，与参赛队无利益关系。	中级以上职称	3

赛项需进行三次加密，加密后参赛选手中途不得擅自离开赛场。分别由3组加密裁判组织实施加密工作，管理加密结果。监督仲裁员全程监督加密过程。

第一组加密裁判，组织参赛选手进行第一次抽签，产生参赛编号，替换选手参赛证等个人身份信息，填写一次加密记录表连同选手参赛证等个人身份信息证件，装入一次加密结果密封袋中单独保管。

第二组加密裁判，组织参赛选手进行第二次抽签，确定赛位号，替换选手参赛编号，填写二次加密记录表连同选手参赛编号，装入二次加密结果密封袋中单独保管。

第三组加密裁判对提交的竞赛文档进行加密。确定竞赛文档号，替换赛位号，填写三次加密记录表，装入三次加密结果密封袋中单独保管。

所有加密结果密封袋的封条均需相应加密裁判和监督仲裁员签字。密封袋在监督仲裁员监督下，由加密裁判放置于保密室的保险柜中保存。

（二）裁判评分方法

裁判组负责竞赛机考评分和结果性评分，由裁判长负责竞赛全过程。裁判员提前报到，报到后所有裁判的手机等通信设备全部上缴并统一保管，评分结束后返还，保证竞赛的公平与公正。

竞赛现场有监督仲裁员、现场裁判员、技术支持队伍等组成，分工明确。根据现场环境，每位现场裁判负责一定数量的参赛队，由多名技术支持人员负责所有工位的设备应急。现场裁判负责与参赛队伍的交流沟通及试卷等材料的收发，以及设备问题确认和现场执裁，技术支持人员负责执行现场裁判员确认后的设备应急处理。

（三）成绩产生办法

评分裁判执裁过程中，各模块由分组评分裁判进行独立评分，由评分裁判负责裁定成绩一致后，提交到成绩统计组，统计组再次核对每小题的得分，并汇总产生每套竞赛文档号的对应成绩。

裁判长正式提交竞赛文档号对应的评分结果并复核无误后，加密裁判在监督仲裁员的监督下，对加密结果进行逐层解密，形成成绩一览表，成绩表由裁判长、监督仲裁员签字确认。

竞赛评分严格按照公平、公正、公开的原则，评分标准注重考查参赛选手以下各方面的能力和水平。

表 8　评分细则和评分方式一览表

竞赛阶段	具体内容及占比	评分细则和评分方式
第一阶段 权重 30%	网络平台搭建 权重 5%	防火墙、网络日志系统、Web 应用防火墙、无线控制器、三层交换机，物理连接，命名、IP 地址等配置。 满分 50 分。 结果评分-客观。
	网络安全设备配置与防护 权重 25%	防火墙路由、安全策略、NAT、VPN 等配置和测试；网络日志系统网络检测、统计、告警等配置；Web 应用防火墙防护策略、过滤策略、告警等配置；无线管理、无线网络设置、安全策略等配置和测试；三层交换机路由、二层安全等配置和测试。 满分 250 分；结果评分-客观。
第二阶段 权重 30%	网络安全事件响应、数字取证调查和应用安全 权重 30%	操作系统和应用系统的日志分析，漏洞分析，系统进程分析，内存分析，系统安全加固，程序逆向分析，编码转换，加解密技术，数据隐写，文件分析取证，网络流量包分析，移动应用程序分析，代码审计。 满分 300 分；结果评分-客观及主观。
第三阶段 权重 40%	网络安全渗透 权重 30%	使用渗透测试技术利用 SQL 注入、文件上传、命令执行、栈溢出、缓冲区溢出等漏洞对目标靶机进行渗透测试；通过信息收集、逆向文件分析、二进制漏洞利用、应用服务漏洞利用、操作系统漏洞利用、密码学分析及一些杂项信息分析等信息安全技术获取靶机内的关键内容。 满分 300 分；结果评分-客观。
	理论技能与职业素养 权重 10%	通过理论测试系统进行理论技能与职业素养考核，主要考查信息安全与网络基础、操作系统安全、网络协议安全、网络设备安全、网络数据安全、程序代码安全、网络安全渗透、安全运维与应急服务、密码技术、网络安全法律法规及职业素养等职业素养。 满分 100 分；结果评分-客观。

十二、奖项设置

（一）奖项设置

本赛项奖项设团体奖。以赛项实际参赛队总数为基础，一等奖占比 10%，二等奖占比 20%，三等奖占比 30%。

获得一等奖的参赛队指导教师获“优秀指导教师奖”，授予荣誉证书。

（二）排序办法

按照总分进行名次排序，如出现参赛队总分相同情况，按模块三得分排序，如模块三得分相同，再以模块二得分进行排序，以此类推。

十三、赛项预案

（一）设备问题

1.为避免突发停电引起竞赛设备关机，应提供 UPS 保电，确保停电后赛事有效进行。

2.预留充足备用 PC 和交换机等竞赛设备，当出现设备掉电、故障等意外时经现场裁判确认后由赛场技术支持人员予以更换。

3.竞赛过程中出现设备掉电、故障等意外时，现场裁判需及时确认情况，安排技术支持人员进行处理，现场裁判登记细情况，填写补时登记表，报裁判长批准后，可安排延长补足相应选手的竞赛时间。

（二）题目问题

1.若发现题目无法正常访问，在 5 分钟内无法正常恢复，即开启同题型备用题目，并及时通告选手。

2.若发现题目被恶意修改，应在 2 分钟内重启题目宿主机或恢复宿主机镜像。

（三）平台问题

1.当发现平台访问缓慢，即部分选手可正常访问，部分选手访问异常或访问平台响应时间过长，应首先排查交换机、平台网络负载情况，然后建议参赛选手更换网络。

2.当发现平台无法正常访问，即所有选手访问平台异常，平台保障人员应在1分钟内做出响应，及时排查故障，应在5分钟内恢复平台的正常运行。

3.若排除故障时间超过5分钟，应及时上报，裁判长根据修复时间可适当延长竞赛时长。

（四）其他突发性事件预案

1.若出现重大突发事件和重大安全问题，经大赛办和专家组同意，暂停竞赛，由涉及人员有关领导，如裁判长、领队、技术支持公司负责人、大赛办领导和承办校负责人协调处理解决；如若不能处理，中止竞赛，是否停赛由大赛办决定。

2.竞赛期间发生意外伤害、意外疾病等重大事故，裁判长立即中止相关人员竞赛，第一时间由应急医疗组负责抢救，严重时送往医院。

十四、竞赛须知

（一）参赛队须知

1.参赛队名称统一使用规定的代表队名称。

2.各参赛队需为参赛选手购买交通意外保险以及人身安全保险。

3.各参赛队要注意饮食卫生，防止食物中毒。

4.各参赛队应该参加赛项承办单位组织的闭赛式等各项赛事活动。

5.在赛事期间，领队及参赛队其他成员不得私自接触裁判，凡发现有弄虚作假者，取消其参赛资格，成绩无效。

6.所有参赛人员须按照赛项规程要求完成赛项评价工作。

7.对于有碍比赛公正和比赛正常进行的参赛队，视其情节轻重，按照《全国职业院校技能大赛奖惩办法》给予警告、取消比赛成绩、通报批评等处理。

（二）参赛领队须知

1. 由拟参赛高校领队 1 人，赛项领队应该由参赛院校中层以上管理人员或教育行政部门人员担任，熟悉赛项流程，具备管理与组织协调能力。

2.领队应按时参加赛前领队会议，不得无故缺席。

3.领队负责组织本省参赛队参加各项赛事活动。

4.领队应积极做好本省参赛队的服务工作，协调各参赛队与赛项组织机构、承办院校的对接。

5.参赛队认为存在不符合竞赛规定的设备、工具、软件，有失公正的评判、奖励，以及工作人员的违规行为等情况时，须由领队向赛项监督仲裁组提交书面申诉材料。各参赛队领队应带头服从和执行申诉的最终仲裁结果，并要求指导教师、选手服从和执行。

（三）指导教师须知

1.指导教师应根据专业教学计划和赛项规程合理制定训练方案，认真指导选手训练，培养选手的综合职业能力和良好的职业素养，克服功利化思想，避免为赛而学、以赛代学。

2.指导老师应认真研究和掌握本赛项规程、技术规范和赛场要求，指导选手做好赛前的一切技术准备和竞赛准备。

3.指导教师应根据赛项规程要求做好参赛选手保险办理工作，并积极做好选手的安全教育。

4.指导教师参加赛项观摩等活动，不得违反赛项规定进入赛场，干扰比赛正常进行。

5.指导教师必须是参赛选手所在学校的在职专任教师，每个团队不超过 2 名指导教师，指导教师一经确定不得随意变更。

6.指导老师要发扬道德风尚，听从指挥，服从裁判，不弄虚作假。

7.对申诉的仲裁结果，领队和指导老师应带头服从和执行，还应说服参赛选手服从和执行。

（四）参赛选手须知

1.参赛选手应按有关要求如实填报个人信息，否则取消竞赛资格。

2.参赛选手应持统一印制的参赛证，带齐身份证、注册的学生证。在赛场的着装，应符合职业要求。在赛场的表现，应体现自己良好的职业习惯和职业素养。

3.参赛选手应遵守比赛规则，尊重裁判和赛场工作人员，自觉遵守赛场秩序，服从裁判的管理。

4.参赛选手应按照规定时间抵达赛场，凭参赛证、身份证件检录，按要求入场，不得迟到早退。

5.参加选手请勿携带任何电子设备及其他资料、用品进入赛场。

6.参赛选手应按有关要求在指定位置就坐。

7.参赛选手须在确认竞赛内容和现场设备等无误后开始竞赛。在竞赛过程中，确因计算机软件或硬件故障，致使操作无法继续的，经项目裁判长确认，予以启用备用计算机。

8.竞赛过程中不准互相交谈，不得大声喧哗；不得有影响其他选手比赛的行为，不准有旁窥、夹带等作弊行为。

9.竞赛过程中需要去洗手间，应报告现场裁判，由裁判或赛场工作人员陪同离开赛场。

10.各参赛选手必须按规范要求操作竞赛设备。一旦出现较严重的安全事故，经裁判长批准后将立即取消其参赛资格。

11.参赛选手需详细阅读赛题中竞赛文档命名的要求，不得在提交的竞赛文档中标识出任何关于参赛选手地名、校名、姓名、参赛编号等信息，否则取消竞赛成绩。

12.完成竞赛任务后，需要在竞赛结束前离开赛场，应向现场裁判示意，在赛场记录上填写离场时间并签工位号确认后，方可离开赛场到指定区域，离开赛场后不可再次进入。未完成竞赛任务，因病或其他原因需要终止竞赛离开赛场，需经裁判长同意，在赛场记录表的相应栏目填写离场原因、离场时间并签工位号确认后，方可离开；离开后，不能再次进入赛场，离开赛场时不得带走任何资料。

13.裁判长发出停止竞赛的指令，选手（包括需要补时的选手）应立即停止操作，在现场裁判的指挥下离开赛场到达指定的区域等候评分。需要补时的选手在离场后，由现场裁判召唤进场补时。

14.遇突发事件，立即报告裁判和赛场工作人员，按赛场裁判和工作人员的指令行动。

15.在竞赛期间，未经大赛办批准，参赛选手不得接受其他单位和个人进行的与竞赛内容相关的采访。参赛选手不得将竞赛的相关信息私自公布。

（五）工作人员须知

1.工作人员必须服从赛项组委会统一指挥，佩戴工作人员标识，认真履行职责，忠于职守，秉公办理，保守秘密，做好服务赛场、服务选手的工作。

2.工作人员按照分工准时上岗，不得擅自离岗，应认真履行各自的工作职责，保证竞赛工作的顺利进行。

3.注意文明礼貌，保持良好形象，熟悉赛项指南。

4.提前 30 分钟到达赛场，严守工作岗位，不迟到，不早退，不得无故离岗，特殊情况需向工作组组长请假。

5.熟悉竞赛规程，严格按照工作程序和有关规定办事，如遇突发事件，按照应急预案，组织指挥人员疏散，确保人员安全。

6.工作人员在竞赛中若有舞弊行为，立即撤销其工作资格，并严肃处理。

7.保持通讯畅通，服从统一领导，严格遵守竞赛纪律，加强协作配合，提高工作效率。

十五、申诉与仲裁

各参赛队对不符合大赛和赛项规程规定的设备、工具、材料、计

算机软硬件，竞赛执裁、赛场管理以及工作人员的不规范行为等持有异议时，可向赛项监督仲裁工作组提出书面申诉。

（一）申诉主体为参赛队领队。

（二）监督仲裁员的姓名、联系方式应该在竞赛期间向参赛队和工作人员公示，确保信息畅通并同时接受大众监督。

（三）申诉启动时，应以参赛队领队签字同意的书面报告形式递交赛项监督仲裁工作组。报告应对申诉事件的现象、发生时间、涉及人员、申诉依据等进行充分、实事求是的叙述。非书面申诉不予受理。

（四）提出申诉应在成绩公示后 2 小时内提出，超过时效不予受理。

（五）赛项监督仲裁工作组在接到申诉报告后的 2 小时内组织复议，并及时将复议结果以书面形式告知申诉方。申诉方对复议结果仍有异议，可由领队向赛区仲裁委员会提出申诉。赛区仲裁委员会的仲裁结果为最终结果。

（六）仲裁结果由申诉人签收，不能代收。如在约定时间和地点申诉人离开，视为自行放弃申诉。

（七）申诉方可随时提出放弃申诉。

（八）申诉方必须提供真实的申诉信息并严格遵守申诉程序，提出无理申诉或采取过激行为扰乱赛场秩序的应给予取消参赛成绩等处罚。