2022 年全国职业院校技能大赛

赛项规程

一、赛项名称

赛项编号：GZ-2022038

赛项名称：信息安全管理与评估

英文名称：Information Security Management and Evaluation

赛项组别：高职

赛项归属产业：电子信息大类

二、竞赛目的

（一）引领教学改革

本赛项对接世界技能大赛网络安全项目的技术标准，通过竞赛让参赛选手熟悉世界技能大赛网络安全项目的职业标准规范，检验参赛选手网络组建和安全运维、安全审计、网络安全应急响应、数字取证调查、应用程序安全和网络攻防渗透能力，检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。

（二）强化专业建设

该赛项衔接国家信息安全技术应用高职专业标准，竞赛内容覆盖“信息安全技术与实施”、“信息安全产品配置与应用”、“网络安全系统集成”、“网络攻防实训”、“网络安全运行与维护”、“操作系统安全配置”、“Web 渗透测试技术”等专业核心课程内容。

（三）促进产教合作

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。

三、竞赛内容

重点考核参赛选手网络组建和安全运维、安全审计、网络安全应急响应、数字取证调查、应用程序安全和网络攻防渗透等综合实践能力，具体包括：

（一）参赛选手能够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。

（二）参赛选手能够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。

（三）参赛选手能够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。

（四）参赛选手能够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。

（五）参赛选手可以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。

（六）竞赛分值权重和时间分布

序号	内容模块	竞赛时间
第一阶段 权重 30%	网络平台搭建与设备安全防护	竞赛第一天上午（180 分钟）
第二阶段 权重 35%	网络安全事件响应、数字取证调查、应用程序安全	竞赛第一天下午（180 分钟）
第三阶段 权重 35%	夺旗挑战 CTF（网络安全渗透）	竞赛第二天上午（180 分钟）

四、竞赛方式

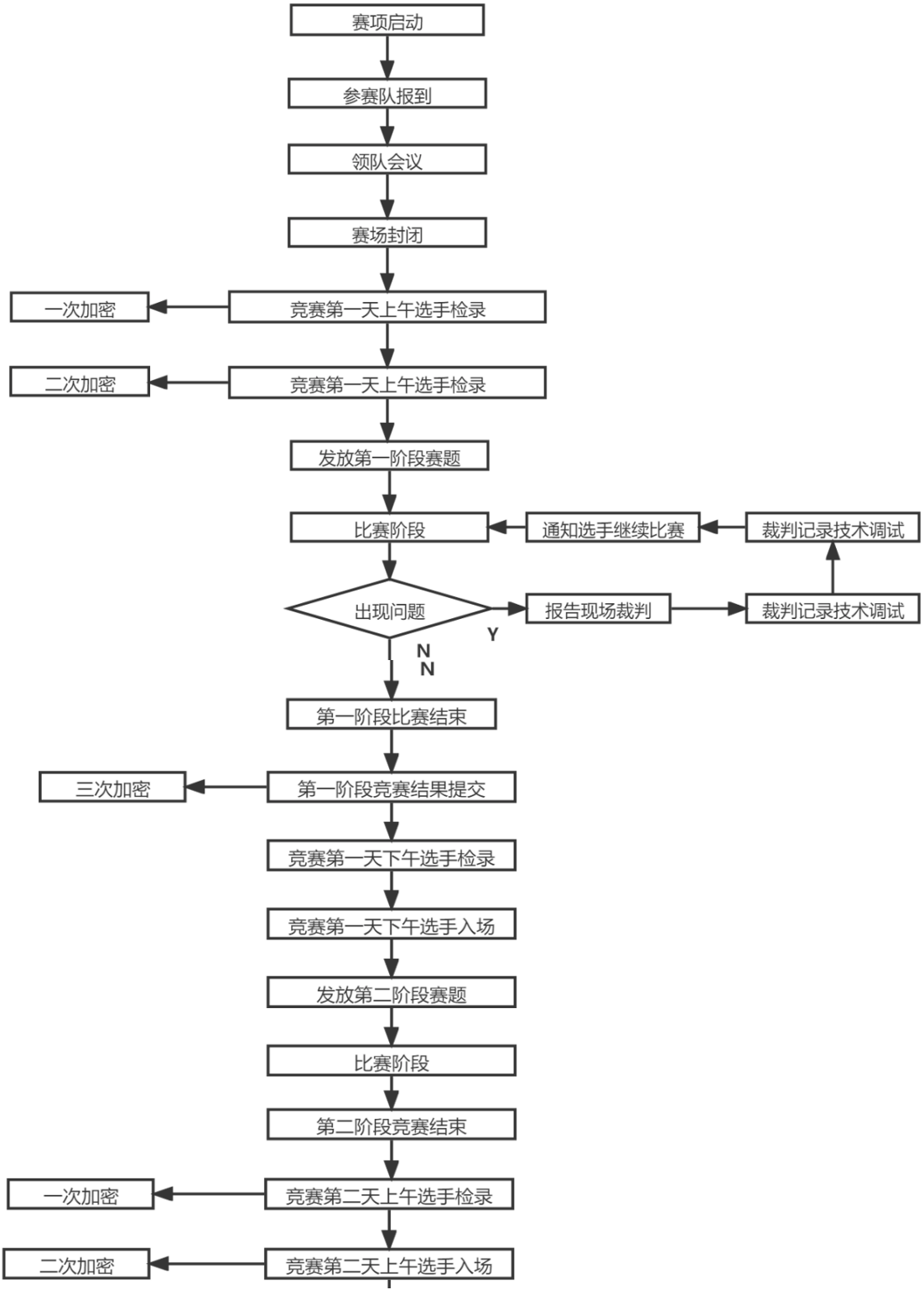
（一）选手构成本赛项为团体赛，每支参赛队由 3 名选手组成，必须为在籍高职院校学生。其中，参赛选手年龄须不超过 25 周岁(年龄计算的截止时间以 2022 年 5 月 1 日为准)，其性别和年级不限。指导教师须为本校专职教师，每参赛队可配置 2 位以内的指导老师。凡在往届全国职业

院校技能大赛中获本赛项高职组一等奖的选手，不能再报名参赛。

五、竞赛流程

（一）竞赛流程图

信息安全管理与评估赛项的竞赛流程如图 1 所示。



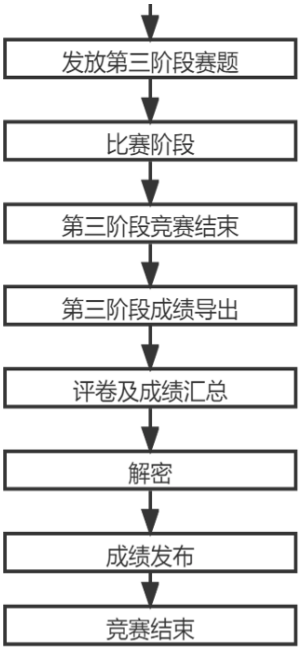


图 1 竞赛流程图

（二）竞赛时间表

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

日期	时间	事项	参加人员	地点
竞赛前 2 日	20:00 前	裁判、监督仲裁报到	工作人员	住宿酒店
竞赛前 1 日	09:00-12:00	参赛队报到，安排住宿，领取资料	工作人员、参赛队	住宿酒店
	09:00-12:00	裁判工作会议	裁判长、裁判员、监督仲裁组	会议室
	13:00-14:30	领队会	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	检查封闭赛场	裁判长、监督仲裁组	竞赛场地
	16:00	返回酒店	参赛领队	竞赛场地
竞赛 第 1 天	07:30	裁判进入裁判室	裁判长、现场裁判	竞赛场地
	08:00-08:30	选手抽签，一次加密	参赛选手、现场裁判	竞赛场地
	08:30-08:50	选手抽签，二次加密及入场	参赛选手、现场裁判	竞赛场地

	08:50-09:00	参赛代表队就位，宣读考场纪律,抽取赛题参数表，第一阶段赛题发放时间	参赛选手、现场裁判	竞赛场地
	09:00-12:00	第一阶段比赛时间	参赛选手、现场裁判	竞赛场地
	12:00-12:30	第一阶段结果提交时间，三次加密	参赛选手、现场裁判	竞赛场地
	14:20-14:30	第二阶段赛题发放时间	参赛选手、现场裁判	竞赛场地
	14:30-17:30	第二阶段正式比赛时间	参赛选手、现场裁判	竞赛场地
	17:30-18:00	第二阶段结果提交时间，三次加密	参赛选手、现场裁判	竞赛场地
竞赛 第 2 天	08:00-08:30	选手抽签，一次加密	参赛选手、现场裁判	竞赛场地
	08:30-08:50	选手抽签，二次加密及入场	参赛选手、现场裁判	竞赛场地
	08:50-09:00	第三阶段赛题发放时间	参赛选手、现场裁判	竞赛场地
	09:00-12:00	第三阶段比赛时间	参赛选手、现场裁判	竞赛场地
	12:00	比赛正式结束	参赛选手、现场裁判	竞赛场地
	12:30-评判完毕后	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
竞赛 后 1 日	9：30-10：00	闭幕式	领导、嘉宾、裁判、各参赛队、专家组	会议室

六、竞赛赛卷

本赛项建立赛题库，赛题库基于样题形式命制。样题由全国职业院校技能大赛执委会组织专家组编制，基于全国职业院校技能大赛相关文件，并参考世界技能大赛相关技术文件要求完成。制作完成的样题于开赛前 1 个月，通过大赛信息发布平台公开。其中，竞赛样题与竞赛规程同步发布，发布方式为全国职业院校技能大赛指定的网络信息发布平台（http://www.chinaskills-jsw.org）。

关于赛题命制事宜，由专家组长会同专家组成员，以教育部颁布的职业院校对应的课程标准和相关行业组织颁布的行业标准为依据，结合信息安全相关专业技能人才培养标准和职业岗位需要，参照行业规范进行设计，形成 3 套赛题。正

式赛题密封存放在大赛组委会指点保密室中。保密室全程监控，并安排专人把守。

正式比赛前 1 小时，由两名裁判及比赛监督员将当阶段的竞赛试卷从保密室监护运往赛场。在监督仲裁组组长的监督下，由裁判长组织裁判从 3 套赛题中随机抽取竞赛正式赛题。

比赛完成后，包括参赛选手在内的任何人，都不得将竞赛试卷带离赛场，由现场裁判对赛卷进行回收，由两名裁判及比赛监督员交由大赛组委会，按照相关要求和规范封存。赛题评分标准不公开，由裁判长在评分阶段公开给裁判。

本竞赛适用于以下专业：

高职专科信息安全技术应用专业（专业代码：510207）；

高职本科信息安全与管理专业（专业代码：310207）；

高职专科区块链技术应用专业（专业代码：510212）；

高职专科密码技术应用专业（专业代码：510216）；

高职专科计算机网络技术专业（专业代码：510202）；

高职专科计算机应用技术专业（专业代码：510201）；

高职专科工业互联网技术专业（专业代码：510211）；

高职本科网络工程技术（专业代码：310202）。

七、竞赛规则

（一）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。

（二）竞赛所需的硬件设备、系统软件和辅助工具由赛项执委会统一安排，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。

（三）参赛队自行决定选手分工、工作程序和时间安排。

（四）参赛队在赛前 10 分钟进入竞赛工位并领取竞赛任务，竞赛正式开始后方可展开相关工作。

（五）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。若因选手因素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；若因非参赛选手个人因素造成设备故障，由裁判长视具体情况做出裁决。

（六）竞赛结束（或提前完成）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。

（七）最终竞赛成绩经复核无误及裁判长、监督仲裁长签字确认后，在指定地点，以纸质形式向全体参赛队进行公布，并在闭赛式上予以宣布。

（八）本赛项各参赛队最终成绩由承办单位信息员录入赛务管理系统。承办单位信息员对成绩数据审核后，将赛务管理系统中录入的成绩导出打印，经赛项裁判长审核无误后签字。承办单位信息员将裁判长确认的电子版赛项成绩信息上传赛务管理系统，同时将裁判长签字的纸质打印成绩单报送大赛执委会。

（九）赛项结束后专家工作组根据裁判判分情况，分析参赛选手在比赛过程中对各个知识点、技术的掌握程度，并将分析报告报备大赛执委会办公室，执委会办公室根据实际情况适时公布。

（十）赛项每个比赛环节裁判判分的原始材料和最终成绩等结果性材料经监督仲裁组人员和裁判长签字后装袋密封留档，并由赛项承办院校封存，委派专人妥善保管。

（十一）赛事规定

1.参赛选手和指导教师必须遵守赛项规程和相关要求。

2.领队代表参赛省市负责管理参赛选手和指导教师，应当严格遵守大赛制度的有关规定，有效管理参赛选手和指导教师，遵守申诉与监督仲裁程序。

3.专家、裁判、监督仲裁人员必须遵守《全国职业院校技能大赛制度汇编》，按制度规定履行职责，严格执行保密制度、遵守竞赛规程，公平公正履职。

4.赛务工作人员必须遵守规章制度，认真负责履行有关赛务岗位职责。

八、竞赛环境

竞赛工位内设有操作平台，每工位配备 220V 电源，工位内的电缆线应符合安全要求。每个竞赛工位面积≥6 ㎡，确保参赛队之间互不干扰。竞赛工位标明

工位号，并配备竞赛平台和技术工作要求的软、硬件。环境标准要求保证赛场采光(大于 500lux)、照明和通风良好；每支参赛队提供一个垃圾箱。

除了竞赛工位之外，同时设计了成果展示区、体验区、观摩区、服务区等。成果展示区主要展示大赛配套教材、资源包等内容；体验区主要展示竞赛设备以及相关新技术、新产品；观摩区主要展示信息安全攻击渗透的实时进度；服务区提供医疗等服务保障。

九、技术规范

（一）该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 15 项国家标准，参赛队在实施竞赛项目中要求遵循如下规范：

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）赛项涉及知识点与技能点如下：

序号	内容模块	具体内容	说明
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
	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	能够利用日志系统对网络内的数据进行日志分析，把控网络安全等
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
		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
		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
第三阶段	夺旗挑战 CTF（网络安全渗透）	参赛队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

十、技术平台

（一）竞赛软件

赛项执委会提供个人计算机（安装 Windows 操作系统），用以组建竞赛操作环境，为参赛选手提供解题过程中的工具软件，并安装 Office 等常用应用软件。

序号	软件	版本
1	Windows 10	professional
2	Microsoft Office	Version 2010 以上
4	VMwareWorkstation	Version 12 以上
5	Windows Server 2016	Datacenter
6	Wireshark	3.4.9
7	bind	9.11.4
8	Kali	Version2021.3
9	IDA free	7.0
10	OllyDbg	Version1.10 以上
11	PDFreader	
12	Volatility	Version2.6 以上

13	Autopsy	Version4.0 以上
14	windbg	Version4.0 以上
15	Jadx-gui	1.2.0
16	apktool	2.6.1
17	Android Studio	2021.3.1
18	HxD Hex Editor	Version 2.X 以上版本
19	Android Emulator	API27
20	StegSolve	1.4
21	audacity	3.1.0
22	Parrot-security	4.11.2
23	gdb-pwndbg	2021.06.22
24	sagemath	9.2
25	pwntools	4.5.0
26	pycryptodome	3.14.1
27	frida-server	15.1.10
28	frida-tools	10.4.1
29	vscode	X64-1.6.1
30	Frp	0.38.0
31	Neo-reGeorg	v3.7.0
32	EmEditor Free	V21.5.2
33	Putty	0.68 以上
34	VNC viewer	1.2.1.2
35	VirtualBox	6.1.28
36	CaptfEncoder	2.1.0
37	BeautifulSoup4	4.9.3
38	one_gadget	1.7.4
38	超级终端	设备调试连接工具

赛项执委会提供渗透测试机和靶机虚拟机环境。

序号	软件	版本
1	Windows Server 2016	Datacenter
2	Windows 10	professional
3	Linux(CentOS)	Version 7.6.1810
4	ubuntu	20.04
5	EVE-NG	v2.0.3-110

（二）竞赛设备清单

序号	设备名称	数量	技术规格	备注
1	三层虚拟化交换机	1 台/组	24 个千兆以太网电口+4 个复用千兆 SFP 光口+4 个 10G SFP+光口	
2	防火墙	1 台/组	9 个 10/100/1000M 以太网电口；1U 标准机箱	
3	WEB 应用防火墙	1 台/组	6 个千兆电口，1 个扩展插槽，1 个	

			Console ，存储 1T 硬盘，机箱 1U	
4	网络日志系统	1 台/组	6 个千兆电口，1 个扩展插槽，1 个 Console ，存储 1T 硬盘，机箱 1U	
5	无线交换机	1 台/组	4 个万兆 SFP 光口，24 个千兆电口，支持 CLI 配置，串口波特率 9600，支持双交流供电接口	
6	无线接入点	1 台/组	802.11ac wave2 室内放装型无线 AP，内置天线，整机 5 条空间流，整机最大速率 1.317Gbps，支持 802.11a/n/ac wave2 和 802.11b/g/n 同时工作，支持 1 个千兆电口，1 个 USB 接口；	
7	POE 模块	1 个/组	10/100/1000Mbps 单端口 802.3at PoE 模块，最高输出功率为 30W	
8	服务器	1 台/组	处理器≥16 核，内存≥64GB，硬盘（SSD）1TB 以上，千兆网口 2 个及以上	

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》建立全国职业院校技能大赛赛项裁判库，裁判长由赛项执委会向大赛执委会推荐，由大赛执委会聘任。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，并设有专职督导人员 1-2 名，负责比赛过程全程监督，防止营私舞弊。本赛项计划需要裁判 18 名，现场裁判 5 名，打分裁判 10 名，加密裁判 3 名。

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人员签字。密封袋在监督人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全部上缴裁判长统一保管，评分结束返回，保证竞赛的公正与公平。

竞赛现场有监督员、裁判员、监考员、技术支持队伍等组成，分工明确。根据现场环境，每位监考员负责 2-3 组参赛队，5-6 名技术支持工程师负责所有工位设备应急。监考员负责与参赛队伍的交流沟通及试卷等材料的收发，裁判员负责设备问题确认和现场执裁，技术支持负责执行裁判确认后的设备应急处理。

（三）成绩产生办法

裁判员执裁过程中，各模块由分组裁判员进行背对背评分，由小组长负责裁定成绩一致方提交到成绩统计组，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，加密裁判在监督人员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。

当出现选手总成绩并列时，本赛项按照第三阶段、第二阶段、第一阶段顺序进行得分排序。首先以第三阶段得分排序，如果第三阶段得分相同，再以第二阶段得分进行排序，以此类推。

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：

竞赛阶段	具体内容分值	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 5 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 25 分；结果评分-客观。
第二阶段 权重 35%	网络安全事件响应、数字取证调查和应用安全 权重 35%	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 35 分；结果评分-客观。
第三阶段 权重 35%	夺旗挑战 CTF（网络安全渗透） 权重 35%	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 35 分；机考评分。

参赛选手应体现团队风貌、团队协作与沟通、组织与管理能力和工作计划能力等，并注意相关文档的准确性与规范性。

比赛过程中禁止攻击裁判服务器和网络连接设备，按照现场 WAF（或网络设备）告警记录一经发现攻击行为根据《全国职业院校技能大赛制度汇编》奖惩办法中大赛惩处参赛选手部分，按扰乱赛场秩序处理，立即停止比赛，并给予选手取消成绩的处分，同时，责成所在学校按照学生违纪违规处分规定做出处理。

（四）成绩复核与公布

为保障成绩评判的准确性，监督仲裁组将对赛项总成绩排名前 30%的所有参赛队伍（选手）的成绩进行复核；对其余成绩进行抽检复核，抽检覆盖率不得低于 15%。如发现成绩错误以书面方式及时告知裁判长，由裁判长更正成绩并签字确认。复核、抽检错误率超过 5%的，裁判组将对所有成绩进行复核。

竞赛成绩以复核无误后，经项目裁判长、监督仲裁人员审核签字后确定，并在赛场及赛场外张贴纸质成绩进行公布。

十二、奖项设定

赛项设参赛选手团体奖，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%，小数点后四舍五入。

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。

十三、赛场预案

1.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比赛时间。

2.预留充足备用 PC 和设备，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.赛项出现重大突发事件和重大安全问题，经赛项执委会和专家组同意，暂停比赛，由涉及人员有关领导，如裁判长、领队、技术支持公司负责人、执委会领导和承办校负责人协调处理解决；如若不能处理，中止比赛，是否停赛由赛区执委会决定。事后，赛区执委会应向大赛执委会报告详细情况。

4.比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比赛，第一时间由承办校医疗站校医抢救，严重呼叫 120 送往医院。

十四、赛项安全

赛事安全是全国职业院校技能大赛一切工作顺利开展的先决条件，是本赛项筹备和运行工作必须考虑的核心问题。

（一）组织机构

赛项执委会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。

（二）赛项设计

1. 比赛内容涉及的器材、设备均符合国家有关安全规定。赛项专家组充分考虑了比赛内容和所用器材、耗材可能存在的危险因素，通过完善设计规避风险，采取有效防范措施保证选手备赛和比赛安全。危险提示和防范措施将在赛项技术文件中加以明确。

2. 赛项技术文件包含国家（或行业）有关职业岗位安全的规范、条例和资格证书要求等内容。

3. 赛项执委会将在赛前对本赛项全体裁判员进行裁判培训和安全培训，对服务人员进行安全培训。该赛项源于实际安全网络组建与运维的生产过程，根据《中华人民共和国劳动法》等法律法规，建立了完善的安全事故防范制度，并在赛前对选手进行培训，避免发生人身伤害事故。

4. 赛项执委会将制定专门方案保证比赛命题、赛题保管和评判过程的安全。

（三）比赛环境

1.环境安全保障

赛场组织与管理人员制定安保须知、安全隐患规避方法及突发事件预案，设立紧急疏散路线及通道等，确保比赛期间所有进入竞赛地点的车辆、人员需凭证入内；严禁携带易燃易爆物、管制刀具等危险品及比赛严令禁止的其他物品进入场地；对于紧急发生的拥挤、踩踏、地震、火灾等进行紧急有效的处置。

2.信息安全保障

安装 UPS：采用 UPS 防止现场因突然断电导致的系统数据丢失，额定功率：3KVA，后备时间：2 小时，电池类型：输出电压：230V±5%V；市电采用双路供电。

3.操作安全保障

赛前要对选手进行计算机、网络设备、工具等操作的安全培训，进行安全操作的宣讲，确保每个队员能够安全操作设备后方可进行比赛。裁判员在比赛前，宣读安全注意事项，强调用火、用电安全规则。

整个大赛过程邀请当地公安系统、卫生系统和保险系统协助支持。

参赛队选手从参赛校到承办校的旅途安全由各省市负责，参赛选手竞赛过程中的安全保障由竞赛组委会负责。

4.赛项执委会须在赛前组织专人对比赛现场、住宿场所和交通保障进行考察，并对安全工作提出明确要求。赛场的布置，赛场内的器材、设备，应符合国家有

关安全规定。承办单位赛前须按照赛项执委会要求排除安全隐患。

5.根据大赛组委会和当地教育厅要求做好疫情防控工作。

6.赛场周围要设立警戒线，防止无关人员进入发生意外事件。比赛现场内应参照相关职业岗位的要求为选手提供必要的劳动保护。在具有危险性的操作环节，裁判员要严防选手出现错误操作。

7.承办单位应提供保证应急预案实施的条件。对于比赛内容涉及高空作业、可能有坠物、大用电量、易发生火灾等情况的赛项，必须明确制度和预案，并配备急救人员与设施。

8.赛项执委会须会同承办单位制定开放赛场和体验区的人员疏导方案。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。

9.大赛期间，赛项承办单位须在赛场管理的关键岗位，增加力量，建立安全管理日志。

10.参赛选手进入赛位、赛事裁判工作人员进入工作场所，严禁携带通讯、照相摄录设备，禁止携带记录用具。如确有需要，由赛场统一配置、统一管理。赛项可根据需要配置安检设备对进入赛场重要部位的人员进行安检。

（四）生活条件

1.比赛期间，原则上由赛事承办单位统一安排参赛选手和指导教师食宿（费用自理）。承办单位须尊重少数民族的信仰及文化，根据国家相关的民族政策，安排好少数民族选手和教师的饮食起居。

2.比赛期间安排的住宿地应具有宾馆/住宿经营许可资质。以学校宿舍作为住宿地的，大赛期间的住宿、卫生、饮食安全等由赛项执委会和提供宿舍的学校共同负责。

3.大赛期间有组织的参观和观摩活动的交通安全由赛项执委会负责。赛项执委会和承办单位须保证比赛期间选手、指导教师和裁判员、工作人员的交通安全。

4.各赛项的安全管理，除了可以采取必要的安全隔离措施外，应严格遵守国

家相关法律法规，保护个人隐私和人身自由。

（五）组队责任

1.各省、自治区、直辖市在组织参赛队时，须安排为参赛选手购买大赛期间的人身意外伤害保险。

2.各省、自治区、直辖市参赛队组成后，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.各参赛队领队须加强参赛人员的安全管理，实现与赛场安全管理的对接。

（六）应急处理

比赛期间发生意外事故，发现者应第一时间报告赛项执委会，同时采取措施避免事态扩大。赛项执委会应立即启动预案予以解决并向赛区执委会报告。出现重大安全问题的赛项可以停赛，是否停赛由赛区组委会决定。事后，赛区执委会应向大赛执委会报告详细情况。

（七）处罚措施

1.赛项出现重大安全事故的，停止承办单位的赛项承办资格。

2.因参赛队伍原因造成重大安全事故的，取消其参赛资格。

3.参赛队伍有发生重大安全事故隐患，经赛场工作人员提示、警告无效的，可取消其继续比赛的资格。

4.赛事工作人员违规的，按照相应的制度追究责任。情节恶劣并造成重大安全事故的，由司法机关追究相应法律责任。

十五、竞赛须知

（一）参赛队须知

1.参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。

2.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。

3.所有参赛人员须按照赛项规程要求按照完成赛项评价工作。

4. 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.由省、自治区、直辖市、新疆生产建设兵团教育行政部门确定赛项领队 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.指导教师应该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.指导老师应及时查看大赛专用网页有关赛项的通知和内容，认真研究和掌握本赛项竞赛的规程、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.指导教师应该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。

（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。

2.参赛选手需持统一印制的参赛证和有效身份证件参加竞赛。

3.参加选手应认真学习领会本次竞赛相关文件，自觉遵守大赛纪律，服从指挥，听从安排，文明参赛。

4.参加选手请勿携带任何电子设备及其他资料、用品进入赛场。

5.参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。

6.参赛选手应增强角色意识，科学合理分工与合作。

7.参赛选手应按有关要求在指定位置就坐。

8.参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。

9.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，经总裁判长批准后将立即取消其参赛资格。

10.参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。

11.竞赛时间终了，选手应全体起立，结束操作。将资料和工具整齐摆放在操作平台上，经工作人员清点后可离开赛场，离开赛场时不得带走任何资料。

12.在竞赛期间，未经执委会批准，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.树立服务观念，一切为选手着想，以高度负责的精神、严肃认真的态度和严谨细致的作风，在赛项执委会的领导下，按照各自职责分工和要求认真做好岗位工作。

2.所有工作人员必须佩带证件，忠于职守，秉公办理，保守秘密。

3.注意文明礼貌，保持良好形象，熟悉赛项指南。

4.自觉遵守赛项纪律和规则，服从调配和分工，确保竞赛工作的顺利进行。

5.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。

6.熟悉竞赛规程，严格按照工作程序和有关规定办事，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。

7.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。

8.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。

十六、申诉与仲裁

各参赛队对不符合大赛和赛项规程规定的仪器、设备、工装、材料、物件、计算机软硬件、竞赛使用工具、用品，竞赛执裁、赛场管理，以及工作人员的不规范行为等，可向赛项监督仲裁组提出申诉。申诉主体为参赛队领队。参赛队领队可在比赛结束后（选手赛场比赛内容全部完成）2小时之内向监督仲裁组提出书面申诉。

书面申诉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，并由领队亲笔签名。非书面申诉不予受理。

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，可由省（市）领队向赛区监督仲裁委员会提出申诉。赛区监督仲裁委员会的仲裁结果为最终结果。

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。

申诉方可随时提出放弃申诉，不得以任何理由采取过激行为扰乱赛场秩序。

十七、竞赛观摩

本赛项将会设计观摩区，使用大屏幕实时显示信息安全攻防对战的进度。

竞赛环境依据竞赛需求和职业特点设计，在竞赛不被干扰的前提下安全开放部分赛场。观摩人员需佩戴观摩证件在工作人员带领下沿指定路线、在指定区域

内到现场观赛。

十八、竞赛直播

本赛项赛前对赛题保密、设备安装调试、软件安装等关键环节进行实况摄录。竞赛过程采用全程摄录的形式，对比赛的开闭幕式、比赛过程实况转播、手工评卷过程进行摄录。

本赛项在赛后将制作大赛制作优秀选手采访、优秀指导教师采访、裁判专家点评和企业人士采访视频资料。

十九、资源转化

依照《全国职业院校技能大赛赛项资源转化工作办法》的有关要求，赛后赛项执委会向大赛办公室提交大赛成果资源转化方案如下表，半年内完成资源转化工作。

资源名称			表现形式	资源数量	资源要求	完成时间
基本资源	风采展示	赛项宣传片	视频	1	15 分钟以上	赛后 30 天
		风采展示片	视频	1	10 分钟以上	赛后 30 天
	技能概要	技能介绍 技能要点 评价指标	文本资料	3	电子版资料	赛后 60 天
	教学资源	专业教材	文本资料	1	补充完善 定期再版	赛后 90 天
拓展资源	案例库		文本资料	1	电子版资料	赛后 60 天
	试题库		文本资料	1	电子版资料	赛后 60 天

赛后还需加强师资队伍建设，促进资源转化能够在教学中有效应用。2022 年大赛完毕后计划进行 2 期研讨会，以及 2 期师资培训,培训内容定为信息安全在工作与生活中的应用，系统信息安全实战，网络信息安全实战，数据安全及取证技术，数据中心灾备技术等内容。

序号	活动名称	计划时间	备注
1	研讨会第 1 期	2022 年 7 月	

2	师资培训第 1 期	2022 年 7 月	
3	师资培训第 2 期	2022 年 10 月	
4	研讨会第 2 期	2022 年 12 月	

2022 年全国职业院校技能大赛高职组

“信息安全管理与评估”样题

第一阶段竞赛项目试题

本文件为信息安全管理与评估项目竞赛-第一阶段试题，第一阶段内容包括：网络平台搭建、网络安全设备配置与防护。

本次比赛时间为 180 分钟。

介绍

竞赛阶段	任务阶段	竞赛任务
第一阶段 平台搭建与安全设备配置防护	任务 1	网络平台搭建
	任务 2	网络安全设备配置与防护

所需的设备、机械、装置和材料

所有测试项目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。

评分方案

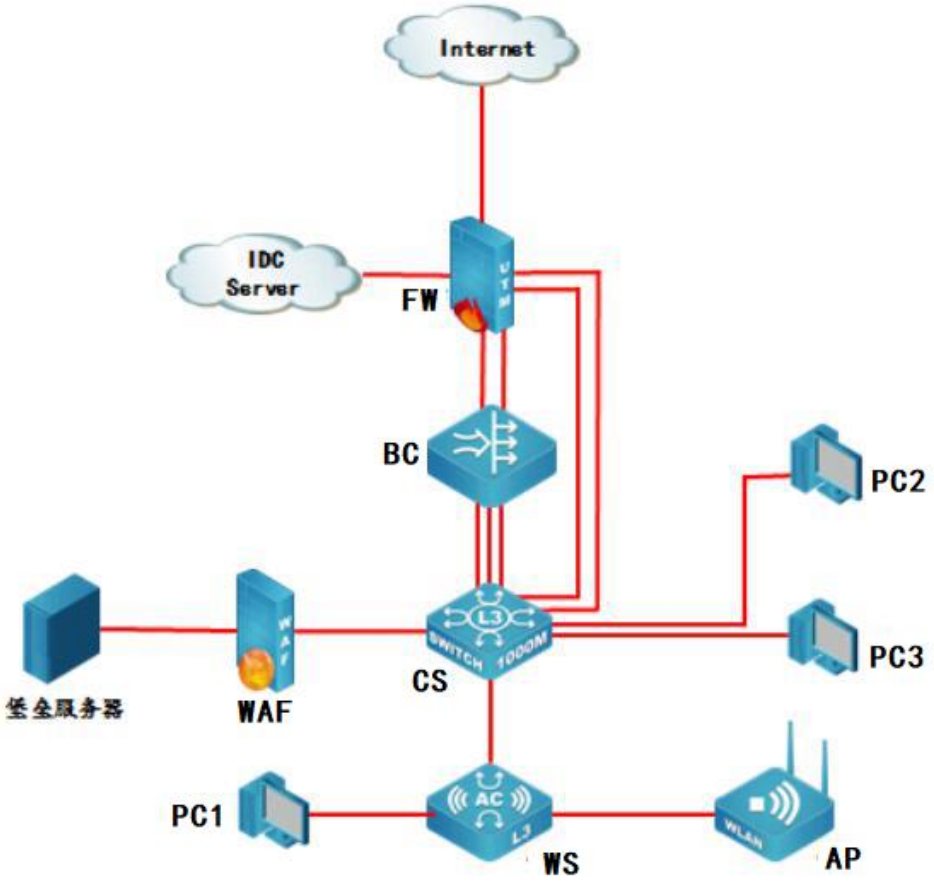
本项目阶段分数为 30 分。

注意事项

赛题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比赛结果提交。

项目和任务描述

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）	CS ETH1/0/1
		AG1.114 10.2.0.254/30 （Trust 安全域）	CS ETH1/0/2
	ETH0/3	10.3.0.254/30	BC ETH3

		（Trust 安全域）	
	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 CS	VLAN 40 ETH1/0/4-8	172.16.40.62/26	PC2
	VLAN 50 ETH1/0/3	172.16.50.62/26	PC3
	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	VLAN113 OSPF	FW ETH0/1

	ETH1/0/1	10.1.0.253/30	
	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 CS 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	WS ETH1/0/20
无线控制器 WS	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	CS 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		CS ETH E1/0/17
	ETH2	网桥	FW
	ETH4		CS ETH E1/0/18
	ETH5	10.51.0.253/30	CS ETH E1/0/23
WEB 应用 防火墙 WAF	ETH3	10.52.0.253/30	CS ETH E1/0/24
	ETH4		堡垒服务器

工作任务

任务 1：网络平台搭建

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

1. CS 开启 telnet 登录功能，用户名 skills01，密码 skills01，配置使用 telnet 方式登录终端界面前显示如下授权信息:“WARNING!!! Authorised access only, all of your done will be recorded! Disconnected IMMEDIATELY if you are not an authorised user! Otherwise, we retain the right to pursue the legal responsibility”;
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：2022_R、2022_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. 对 CS 上 VLAN40 开启以下安全机制：

   业务内部终端相互二层隔离，启用环路检测，环路检测的时间间隔为 10s，发现环路以后关闭该端口，恢复时间为 30 分钟；如发现私设 DHCP 服务器则关闭该端口，配置防止 ARP 欺骗攻击；
4. 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 CS 所有业务 VLAN 下配置访问控制策略实现双向安全防护;
5. CS 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；

   WS 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。

   WS 与 CS 之间配置 RIPng， 使 PC1 与 PC3 可以通过 IPv6 通信；

   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

6. 尽可能加大 CS 与防火墙 FW 之间的带宽;配置使总部 VLAN40 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;

7. FW、CS、WS 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；
8. FW 与 CS 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：
   - CS 通过 BGP 到达 loopback1,2 网路下一跳为 10.3.0.254；
   - CS 通过 BGP 到达 loopback3,4 网络下一跳为 10.4.0.254；
   - 通过 BGP 实现到达 loopback1,2,3,4 的网络冗余；
   - 使用 IP 前缀列表匹配上述业务数据流；
   - 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，AS PATH 属性可配置的参数数值为：65509
9. 如果 CS E1/0/3 端口的收包速率超过 30000 则关闭此端口，恢复时间 5 分钟，并每隔 10 分钟对端口的速率进行统计；为了更好地提高数据转发的性能，CS 交换中的数据包大小指定为 1600 字节；
10. 为实现对防火墙的安全管理，在防火墙 FW 的 Trust 安全域开启 PING,HTTP，SNMP 功能（loopback 接口除外），Untrust 安全域开启 SSH、HTTPS 功能;
11. 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；
12. 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；
13. FW 配置禁止所有人在周一至周五工作时间 9：00-18：00 访问京东 www.jd.com 和淘宝 www.taobao.com;相同时间段禁止访问中含有“娱乐”、“新闻”的 WEB 页面；
14. 在 FW 开启安全网关的 TCP SYN 包检查功能，只有检查收到的包为 TCP SYN 包后，才建立连接；配置所有的 TCP 数据包每次能够传输的最大数据分段为 1460，尽力减少网络分片；配置对 TCP 三次握手建立的时间进行检查，如果在 1 分钟内未完成三次握手，则断掉该连接；

15. 为保证总部 Internet 出口线路，在 FW 上使用相关技术，通过 ping 监控外网网关地址，监控对象名称为 Track，每隔 5S 发送探测报文，连续 10 次收不到监测报文，就认为线路故障，直接关闭外网接口。FW 要求内网每个 IP 限制会话数量为 300；
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：

    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。

    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
17. 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，要求如下：
    - 使用原 AP 所在网络进行地址划分；
    - 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；
    - WS 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 WS 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；
18. 在 NETWORK 下配置 SSID，需求如下：
    - NETWORK 1 下设置 SSID 2022skills-2.4G，VLAN10，加密模式为 wpa-personal,其口令为 skills01；
    - NETWORK 20 下设置 SSID 2022skills-5G，VLAN20 不进行认证加密,做相应配置隐藏该 SSID, 只使用倒数第一个可用 VAP 发送 5.0G 信号；
19. 配置一个 SSID 2022skills_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 WS DHCP 获取 IPv6 地址，地址范围为：2001:10:81::/112;
20. 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;
21. 通过配置防止多 AP 和 WS 相连时过多的安全认证连接而消耗 CPU 资源，检测到 AP 与 WS 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;

22. 为方便合理使用带宽，要求针对 SSID 为“2022skills-2.4”下的用户进行带宽控制。对用户上行速率没有限制，但是针对下行速率要求用户的带宽为 2Mbps，在最大带宽可以达到 4Mbps;
23. 配置所有 Radio 接口：AP 在收到错误帧时，将不再发送 ACK 帧；打开 AP 组播广播突发限制功能；开启 Radio 的自动信道调整，每天上午 10:00 触发信道调整功能;
24. 配置所有无线接入用户相互隔离，Network 模式下限制每天早上 0 点到 4 点禁止终端接入，开启 ARP 抑制功能；
25. 配置当 AP 上线，如果 WS 中储存的 Image 版本和 AP 的 Image 版本号不同时，会触发 AP 自动升级；配置 AP 发送向无线终端表明 AP 存在的帧时间间隔为 1 秒；配置 AP 失败状态超时时间及探测到的客户端状态超时时间都为 2 小时;
26. 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。
27. 为日志查询的时间准确性，要求在 BC 上配置 NTP 服务，NTP 服务器设定为中国科学院国家授时中心(ntp.ntsc.ac.cn)。
28. 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 20 分钟，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。
29. BC 配置应用“即时聊天”，在周一至周五 8：00-20：00 监控内网中所有用户的 QQ 账号使用记录，并保存 QQ 聊天记录数据包；
30. BC 配置内容管理，对邮件内容包含“协议”、“投诉”字样的邮件，记录且邮件报警。
31. BC 上配置报警邮箱，邮件服务器 IP 为 172.16.10.33，端口号为 25，账号为:skills01，密码: skills01，最大记录数量为 50，同时把报警邮件抄送给 Manager@ chinaskills.com;
32. 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 4 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；
33. BC 上配置用户识别功能,对内网所有 IP 地址进行身份识别；
34. 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;

35. 为更好对服务器 172.16.10.45 进行防护，我们定期对服务器进行 Web 漏洞扫描，来及时修改我们的防护规则。
36. 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;
37. 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;
38. 在 WAF 上针对 HTTP 服务器进行 URL 最大个数为 10，Cookies 最大个数为 30，Host 最大长度为 1024，Accept 最大长度 64 等参数校验设置，设置严重级别为中级，超出校验数值阻断并发送邮件告警;
39. 在 WAF 上保护 HTTP 服务器上的 www.2022skills.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;
40. 为防止 www.2022skills.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。

第二阶段竞赛项目试题

本文件为信息安全管理与评估项目竞赛-第二阶段试题，第二阶段内容包括：网络安全事件响应、数字取证调查和应用程序安全。

本次比赛时间为 180 分钟。

介绍

竞赛有固定的开始和结束时间，参赛队伍必须决定如何有效的分配时间。请认真阅读以下指引！

（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。

所需的设备、机械、装置和材料

所有测试项目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。

评分方案

本项目模块分数为 35 分。

项目和任务描述

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

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。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）。

工作任务

第一部分 网络安全事件响应

任务 1：应急响应

A 集团的 Windows 服务器被黑客入侵，该服务器的系统目录被上传恶意软件，域用户凭证被读取，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，发现系统中的漏洞，并对发现的漏洞进行修复。

本任务素材清单：Server 服务器虚拟机。

受攻击的 Windows 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。

注意：Windows 服务器的基本配置参见附录，若题目中未明确规定，请使用默认配置。

请根据赛题环境及任务要求提交正确答案。

任务 1：应急响应		
序号	任务要求	答案
1	任务要求 1	
2	任务要求 2	
3	任务要求 3	
4	.....	

第二部分 数字取证调查

任务 2 ：操作系统取证

A 集团某 Windows 服务器系统感染恶意程序，导致系统被远程监听，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。

请根据赛题环境及任务要求提交正确答案。

任务 2：操作系统取证		
序号	任务要求	答案
1	任务要求 1	
2	任务要求 2	
3	任务要求 3	
4	.....	

任务 3： 网络数据包分析

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。

请根据赛题环境及任务要求提交正确答案。

任务 3：网络数据包分析		
序号	任务要求	答案
1	任务要求 1	
2	任务要求 2	
3	任务要求 3	
4	.....	

任务 4： 计算机单机取证

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。

请按要求完成该部分的工作任务。

任务 4： 计算机单机取证		
证据编号	在取证镜像中的文件名	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：代码审计

A 集团发现其发布的 Web 应用程序遭到了恶意攻击，A 集团提供了 Web 应用程序的主要代码，您的团队需要协助 A 集团对该应用程序代码进行分析，找出存在的脆弱点。

本任务素材清单：Web 程序文件。

请根据赛题环境及任务要求提交正确答案。

任务 5：代码审计		
序号	任务要求	答案
1	任务要求 1	
2	任务要求 2	
3	任务要求 3	
4	.....	

任务 6：Windows 系统恶意程序分析

A 集团发现其网络中蔓延了一种恶意程序，现在已采集到恶意程序的样本，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：恶意程序文件。

请根据赛题环境及任务要求提交正确答案。

任务 6：Windows 系统恶意程序分析		
序号	任务要求	答案
1	任务要求 1	
2	任务要求 2	
3	任务要求 3	
4	.....	

第三阶段竞赛项目试题

本文件为信息安全管理与评估项目竞赛-第三阶段试题。根据信息安全管理与评估项目技术文件要求，第三阶段为夺旗挑战 CTF（网络安全渗透）。

本次比赛时间为 180 分钟。

介绍

夺旗挑战赛（CTF）的目标是作为一名网络安全专业人员在一个模拟的网络环境中实现网络安全渗透测试工作。

本模块要求参赛者作为攻击方，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。

所需的设备、机械、装置和材料

所有测试项目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。

评分方案

本项目阶段分数为 35 分。

注意事项

通过找到正确的 flag 值来获取得分，它的格式如下所示：

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。

项目和任务描述

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，请利用你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：

- 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
- 杂项与密码学分析

所有设备和服务器的 IP 地址请查看现场提供的设备列表。

工作任务

一、Web1 服务器

任务编号	任务描述	答案	分值

任务一	Web1 系统存在隐藏信息，请找出隐藏信息，并将 flag 提交。flag 格式 flag{<flag 值>}		
任务二	Web1 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>}		
任务三	Web1 系统后台存在漏洞，请利用漏洞并找到 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		

二、Web2 服务器

任务编号	任务描述	答案	分值
任务四	Web2 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>}		
任务五	Web2 系统后台存在漏洞,请利用漏洞并找到 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		

三、FTP 服务器

任务编号	任务描述	答案	分值
任务六	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>}		
任务七	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>}		

任务八	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>}		
任务九	请获取 FTP 服务器上对应的流量包进行分析,找出其中隐藏的 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		
任务十	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>}		
任务十一	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>}		
任务十二	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>}		
任务十三	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>}		

四、应用程序 1 服务器

任务编号	任务描述	答案	分值
任务十四	应用程序 1 服务器 10000 端口存在漏洞,找出其中隐藏的 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		

五、应用程序 2 服务器

任务编号	任务描述	答案	分值

任务十五	应用程序 2 服务器 10001 端口存在漏洞,找出其中隐藏的 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		

分值分布表

表 1 第三阶段分值分布

序号	描述	分值
C	夺旗(攻击)	
C1	信息收集	
C2	逆向文件分析	
C3	二进制漏洞利用	
C4	应用服务漏洞利用	
C5	杂项与密码学分析	

附录 A

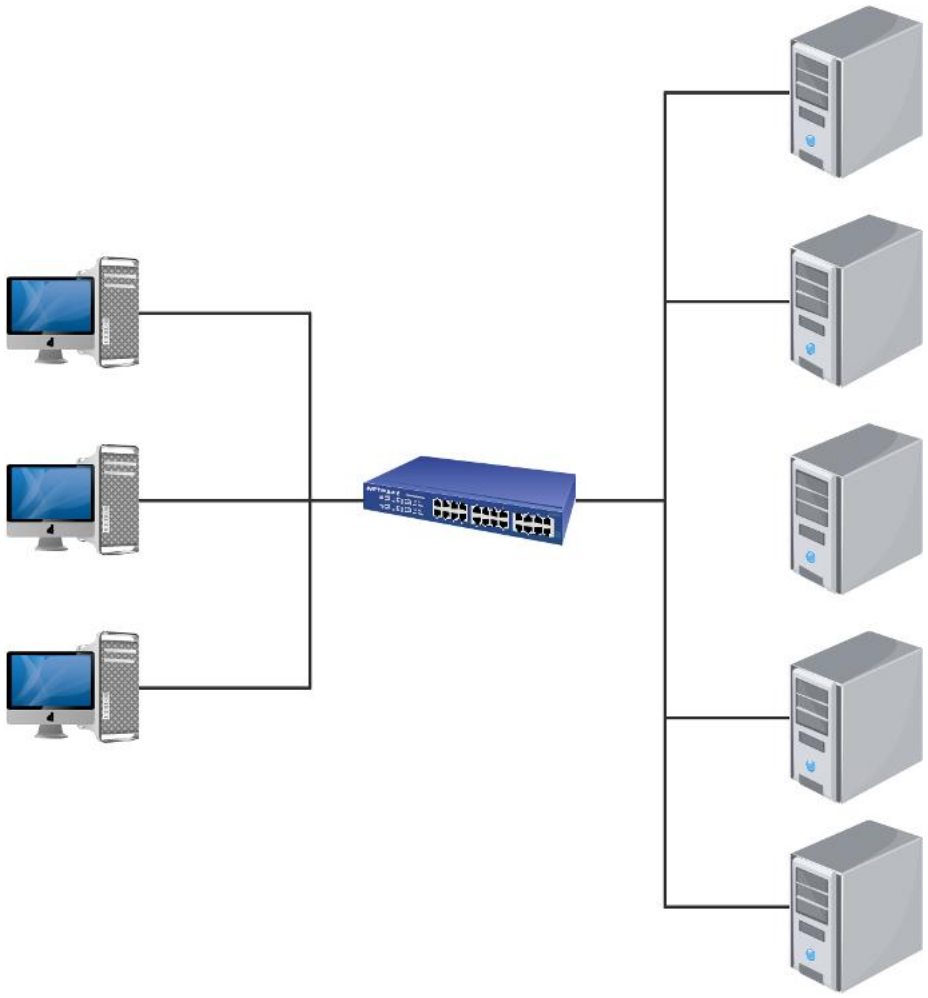


图 1 网络拓扑结构图