2024 上海高职院校学生技能大赛

赛项规程

赛项名称：　　信息安全管理与评估

专业大类：　　电子与信息

赛项编号：　　GZ032

2023 年 12 月

目录

1.项目简介

1.1 项目描述

信息安全管理与评估是指通过对信息系统进行全面、系统的规划、组织、实施、监督、改进和评估，以及对信息系统的各种威胁和风险的预测、预防、控制和处理，确保信息系统的机密性、完整性、可用性和可靠性，从而达到保护信息资产的目的。信息安全评估则是对信息系统进行评估、检测和分析，以发现其中的安全问题和隐患，并提出相应的解决方案。

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，信息安全管理与评估赛项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。

本赛项属于电子与信息类线下比赛，组队方式为**学生团体赛**：

（一）参赛学生必须为高等职业学校专科、高等职业学校本科全日制在籍学生，五年制高职四、五年级学生也可报名参赛。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。

（二）每支参赛队有 3 名选手组成（设 1 名队长），报名获得确认后不得随意更换。必须以院校为单位组队参赛，不得跨校组队。

（三）本赛项为单一场次，所有参赛队在现场根据任务说明，在 4 小时内互相配合，采用小组合作的形式完成任务，最后以提交的结果作为最终评分依据。

1.2 竞赛目的

通过赛项检验参赛选手网络组建、按照等保要求加固网络、安全架构、渗透测试等技术能力，检验参赛队计划组织和团队协作等综合职业素养，培养学生创新能力和实践动手能力，提升学生职业能力和就业竞争力。通过大赛引领专业教学改革，丰富完善学习领域

课程建设，使人才培养更贴近岗位实际，实现以赛促教、以赛促学、以赛促改的产教结合格局，提升专业培养服务社会和行业发展的能力，为国家信息安全行业培养选拔技术技能型人才。

1.3 相关文件

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 9 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_WS0554_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》

2.选手应具备的能力

模块	能力描述
A	**网络平台搭建权重、网络安全设备配置与防护**
	个人需要知道和理解： • 知道和理解网络规划知识，如 VLSM、CIDR 等； • 知道和理解 VLAN、WLAN、STP、SVI、RIPV2、OSPF 等知识； • 知道和理解。L2L IPSec VPN、GRE Over IPSec、L2TP Over IPSec、SSL VPN 等知识。 • 查询语言，如 SQL（结构化查询语言）。 • 数据备份和恢复，数据标准化策略。 • 网络协议，如 TCP/IP、动态主机配置(DHCP)、域名系统(DNS) 和目录服务。 • 防火墙概念和功能。 • 网络安全体系结构的概念，包括拓扑、协议、组件和原则。 • 系统、网络和操作系统加固技术。 • 管理信息技术、用户安全策略(例如：帐户创建、密码规则、访问控制)。 • 信息技术安全原则和方法。 • 身份验证、授权和访问控制方法。 • 网络安全、漏洞和隐私原则。 • 学习管理系统及其在管理学习中的应用。 • 网络安全法与其他相关法规对其网络规划的影响。
	个人应能够： • 能够完成设备连接，保证和测试物理连通性。 • 能够完成指定的交换、路由、防火墙和无线的配置。 • 能够完成企业网的相关策略配置。。 • 能够通过网络设备配置安全防护。 • 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。 • 能够配置网络应用安全，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； • 管理数据库或数据库管理系统。 • 管理并实施流程和工具，确保机构可以识别、存档、获取知识资产和信息内容。 • 处理问题，安装、配置、排除故障，并按照客户需求或咨询提供维护和培训。 • 安装、配置、测试、运行、维护和管理网络和防火墙，包括硬件和软件，确保所有信息的共享、传输，对信息安全和信息系统提供支持。 • 安装、配置、调试和维护服务器（硬件和软件），确保信息保密性、完整性

	和可用性。 • 管理账户、设置防火墙和安装操作系统补丁程序。 • 访问控制、账户和密码的创建和管理。 • 检查机构的现有计算机系统和流程，帮助该机构更安全、更快捷和更高效的运营。 • 协助监督信息系统或网络，管理机构内部的信息安全可能存在的问题或其他需要负责的各方面，包括策略、人员、基础架构、需求、政策执行、应急计划、安全意识和其他资源。
B	**网络安全事件响应、数字取证调查和应用安全**
	个人需要知道和理解： • 文件系统实施(例如，新技术文件系统[NTFS]、文件分配表[FAT]、文件扩展名[EXT])。 • 系统文件(例如：日志文件、注册表文件、配置文件）包含相关信息以及这些系统文件存储位置。 • 网络安全体系结构的概念，包括拓扑、协议、分层和原理。 • 行业技术标准和分析原则、方法和工具。 • 威胁调查、报告、调查工具和法律、法规。 • 网络安全事件类别、响应和处理方法。 • 网络防御和漏洞评估工具及其功能。 • 对于已知安全风险的应对措施。 • 身份验证、授权和访问方法。
	个人应能够： • 使用防护措施和利用不同渠道收集的信息，以识别、分析和报告发生的、或可能发生的网络事件，以保护信息、信息系统和网络免于威胁。 • 测试、实施、部署、维护、检查、管理硬件基础架构和软件，按要求有效管理计算机网络防护服务提供商的网络和资源。 • 监控网络，及时记录未授权的活动。 • 在所属的领域对危机或者紧急状态做出有效响应，在自己的专业领域中降低直接和潜在的威胁。 • 使用缓解措施、准备措施，按照要求做出响应和实施恢复，以最大化存活率保障财产和信息的安全。 • 调查和分析相关网络安全应急响应活动。 • 对威胁和漏洞进行评估。 • 评估风险水平，制定在业务和非运营情况下采取适当的缓解措施。
C	**夺旗挑战 CTF（网络安全渗透）**
	个人需要知道和理解： • 网络威胁行为者的背景和使用的方法。 • 用于检测各种可利用的活动的方法和技术。 • 网络情报信息收集能力和资源库。 • 网络威胁和漏洞。 • 网络安全基础知识(例如，加密、防火墙、认证、诱捕系统、外围保护)。 • 漏洞信息传播源(例如，警报、通知、勘误表和公告)。

	• 开发工具的结构、方法和策略(例如，嗅探、记录键盘）和技术(例如，获取后门访问、收集机密数据、对网络中的其他系统进行漏洞分析)。 • 预测、模拟威胁和应对的内部策略。 • 内部和外部协同的网络操作和工具。 • 系统伪造和司法用例。
	个人应能够： • 识别和评估网络安全罪犯活动。 • 出具调查结果，以帮助初始化或支持执法和反情报调查或活动。 • 分析搜集到的信息，找到系统弱点和潜在可被利用的环节。 • 分析来自情报界的不同渠道、不同学科和不同机构的威胁信息。 • 根据背景情况，同步和放置情报信息，找出可能的含义。 • 应用来自一个或多个不同国家、地区、组织和技术领域的最新知识。 • 应用语言、文化和技术专业知识进行信息收集、分析和其他网络安全活动。 • 识别、保存和使用系统开发过程遗留物并用于分析。

3.竞赛模块及命题方式

3.1 竞赛模块

模块 A、模块 B 与模块 C 同时举行，共计 240 分钟。

模块编号	模块名称	竞赛时间 min	分数		
			评价分	测量分	合计
A	网络平台搭建权重、网络安全设备配置与防护	240	0	30	30
B	网络安全事件响应、数字取证调查和应用安全		0	35	35
C	夺旗挑战 CTF（网络安全渗透）		0	35	35
总计		240	0	100	100

如选手决赛成绩出现同分情况的，按照模块 A 的顺序计算排名顺序。

3.2 模块简述

3.2.1 模块 A：网络平台搭建、网络安全设备配置与防护

本竞赛项目的任务根据实际信息安全服务的工作内容进行设计，以典型的组织机构信息系统网络架构为基础，相关的服务均可以正常运

行，但不满足网络安全行业最佳实践。选手需要使用各种网络安全技术对已有的网络和服务进行配置和加固。一些安全配置比较明确，但另外一些安全配置则为不同的实现选项预留了选择空间，选手需根据行业最佳实践（在安全性、高可用性和可扩展性方面）选择合理安全方案，并尽最大努力实现安全配置。选手应该熟悉cisco、Windows、linux等主流的网络安全设备和产品的安全配置和加固技术。

3.2.2 模块 B：网络安全事件响应、数字取证调查、应用程序安全

本模块包含网络安全事件响应、数字取证调查和应用程序安全。该模块需要选手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，分析黑客的入侵行为，恢复被黑客破坏的文件。

该子项目主要考察选手网络安全事件应急处置能力、网络安全事件取证分析能力、应用程序的代码审计能力以及网络安全风险评估防控能力。

3.2.3 模块 C：夺旗挑战 CTF（网络安全渗透）

模块C为夺旗挑战赛（CTF），改模块目标是在一个有吸引力的环境中展示网络安全，并使安全专业人员能够在模拟的网络安全攻击场景中磨练自己的技能。

本模块参赛选手作为攻击方，综合运用所掌握的网络安全攻击技能和最新的攻击技术的发展趋势，开展网络渗透测试。在比赛期间，参赛队伍可以利用一系列网络安全攻击渗透工具综合分析、挖掘、渗透所提供的网络安全攻击靶场环境。靶场环境中预设了若干Flag，每个Flag 有固定的分值，选手要尽可能多的获取Flag值。

3.3 命题方式

本项目为提前公布试题的项目，于赛前 2 周公布样题。决赛试题在赛前对竞赛样题进行修订，修订比例一般不超过 30%。修订时，裁判长须提供完整的修订方案，裁判组成员均可提出修订意见，最终修改由裁判长确定（或由裁判长发起举手表决通过确定），并由全体裁判签字确认。

3.4 命题方案

项目以全国职业院校技能大赛信息安全管理评估赛项技术文件为参照，并结合国赛标准和国内行业实际来组织命题。重考查参赛选手以下各方面的能力和水平：

竞赛阶	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；结果评分-客观。

4.评分规则

裁判组构成

1. 裁判长：由命题组组长担任，执行裁判长负责制。

2. 裁判员：各参赛学校可选派一名专业教师担任裁判员。

4.1 评价分

打分方式：由裁判长制定执裁规则，裁判长带领所有裁判一起商议，在对该

选手在该项中的实际得分达成一致后最终只给出一个分值。

测量分评分准则样例表：

类型	示例	最高分值	正确分值	不正确分值
满分或零分	分析数据包 capture-z2.pcap，破解文件保护，将文件保护密码作为 FLAG 提交 5 分	5	5	0
从满分中扣除	对 DCRS 的名称进行配置，创建 VLAN 并将相应接口划入 VLAN。10 分（每个 vlan1 分，命名、接口错误扣 1 分）	10	10	0-9
从零分开始加	对 DCFW 的名称、各接口 IP 地址进行配置。8 分，每个 2 分	8	8	0-6

4.3 评分流程说明

所有评分采用事后结果评分，如无特殊情况，当天进行的比赛需当天完成评分并统分。此次技能大赛采用由裁判长组织进行复核后并统分，然后由工作人员提交的方法。裁判长和督考同时对成绩复核，并将参赛选手成绩汇总，各裁判员最终字确认后，成绩经裁判长和督考确认后当场密封公布。具体名次奖项由上海市教委统一发文。

4.4 成绩公布方法

选拔赛现场设立仲裁组，仲裁组由督考、裁判长和场地负责人组成。

裁判长对成绩复核，并将参赛选手成绩汇总，各裁判员最终签字确认后，成绩经裁判长和督考确认后当场公布，无异议后，比赛结果由各参赛院校领队签字确认后报送上海市教委教育技术装备中心，具体名次奖项由教委统一发文。

5.项目特别规定

扰乱赛场秩序，干扰裁判员工作，视情节扣分，情况严重者取消比赛资格。

- 比赛过程中禁止对比赛平台进行攻击，一经发现取消比赛资格。
- 禁止对“规定 iP”以外的地址进行攻击，禁止对比赛平台进行攻击
- 网络设备已配置安全策略及日志记录和告警功能;对网络设备和竞技平台的扫描或渗透都会被记录和告警，一经发现攻击行为，安全策略会阻断流量，上报裁判长按规程处理。

6.竞赛相关设施设备

6.1 场地设备工具：

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	Datacenter
6	Wireshark	3.X.X
7	bind	9.X.X
8	Kali	Version2021.3以上
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.X
24	sagemath	9.2
25	pwntools	4.X
26	pycryptodome	3.X
27	frida-server	15.X
28	frida-tools	10.X
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
39	超级终端	设备调试连接工具

（二）竞赛设备清单

序号	设备名称	数量	参考型号
1	三层虚拟化交换机	1	CS6200-28X-Pro 交换机
2	防火墙	1	DCFW-1800E-N3002-Pro
3	攻防平台	1	CAD 攻防竞技平台
4	WEB 应用防火墙	1	DCFW-1800-WAF-P
5	网络日志系统	1	DCBC-NetLog
6	无线交换机	1	DCWS-6028-pro
7	无线接入点	1	WL8200-I2
8	PC 机	3	多核 CPU，CPU 主频>=3.5GHZ,>=四核心八线程，内存>=8G，具有串口或者配置

			USB 转串口的配置线，支持硬件虚拟化

6.2 决赛选手须自备的设备和工具：

无

6.3 决赛场地禁止自带使用的设备和材料：

序号	设备和材料名称
1	手机
2	光盘
3	U 盘
4	电脑
5	手环

7.健康和安全

（1）赛场人员安全要求

1）现场裁判、选手、工作人员在竞赛期间应该遵守主办方的安全规定和要求。

2）参赛选手进入竞赛场地后，须听从并尊重裁判人员的管理，文明参赛。

3）参赛选手必须在确保人身安全和设备安全的前提下开始竞赛，发现或发生有关安全问题，应立即向裁判报告。

4）参赛选手严禁在赛场区域内吸烟和私自动用明火，严禁携带易燃易爆物品。

（2）场地设备安全要求

1）设施设备安全操作要求

A. 禁止选手及所有参加赛事的人员携带任何有毒有害物品进入竞赛现场。

B. 赛点单位应设置专门的安全防卫组，负责竞赛期间健康和安全事务。主要包括检查竞赛场地、与会人员居住地、车辆交通及其周围环境的安全防卫；制定紧急应对方案；监督与会人员食品安全与卫生；分析和处理安全突发事件等工作。

C. 赛场须配备相应医务人员，并备有相应急救设施。

2）赛场消防安全要求

A. 消防设施、器材和消防安全标志全都在位且功能完整。

B. 消防安全重点部位人员正常在岗工作。

3）安全标识张贴要求

安全出口、疏散通道保证畅通，安全疏散指示标志、应急照明完好无损，竞赛场地安全疏散通道禁止被占用。

4）设备安全操作规程

A. 禁止带电进行线路拆改工作。

B. 所有修改必须在停机状态下进行。

C. 在进行任何安装或维修工作前，必须确认设备处于停止状态。

8.开放赛场

8.1 提供开放式场地

（一）在竞赛过程中，借鉴世界技能大赛组织方式，尝试开放式竞赛方式，广泛宣传，积极组织院校师生、企业员工等人员进行现场观摩，营造参与技能学习、实现技能成才的氛围。

1）赛场内除指定的裁判、工作人员外，其他与会人员须经主办方同意或在主办方负责人陪同下，佩带相应的标志方可进入赛场内；

2）允许进入赛场的人员，只可在参观通道内观摩竞赛，不得使用录像设备长时间拍摄选手工位、屏幕；

3）允许进入赛场的人员应遵守赛场规则，不得与选手交谈，不得妨碍、干扰选手竞赛；

4）允许进入赛场的人员不得在场内吸烟、喧哗；

（二）如疫情防控要求，不能进入赛场进行公开观摩，采用视频观看方式。

1）视频观摩

赛场外设置开放式观摩区，向媒体、企业代表、院校师生等社会公众开放，通过大屏幕对赛场进行直播，同时还可以通过竞赛系统进度监控图实时观看选手答题进度。

2）组织安排

在竞赛开始 1 个小时之后，由承办校组织并派人带领媒体、专家、企业代表、院校师生等进入赛场外的开放式观摩区，按照指定路线进行观摩。

3）纪律要求

为保证大赛顺利进行，在观摩期间应遵循以下纪律要求：

1. 除与竞赛直接有关工作人员、裁判员、参赛选手外，其余人员均为观摩观众。

2. 不得违反职业院校技能大赛规定的各项纪律。

3. 观摩人员需批准，佩戴观摩证件，遵循观摩区的工作人员指挥。

4. 文明观摩，保持观摩区清洁，不得大声喧哗，杜绝各种违反观摩秩序的不文明行为。

9.绿色环保

（一）环境保护

环境整洁卫生，体现绿色环保，严格遵守竞赛规则，提高安全意识和卫生意识，按照要求穿戴工作服装、安全鞋、手套、安全眼镜、耳塞等劳保用品，严格遵守职业规范。

所有竞赛相关人员必须保持场地整洁。交通路线、走廊、楼梯、紧急疏散通道、灭火器及其他救生设备周边必须保持畅通无障碍，竞赛结束后，选手要整理好竞赛工位的卫生，赛场保洁人员要保障赛场整体的环境卫生，体现安全、整洁、有序，将垃圾分类处理。

将废弃物降至最低水平，多余废弃的耗材等要放入到指定垃圾桶内。

（二）可持续性

竞赛项目设计和筹备工作要遵循可持续发展原则，耗材回收有序，设备循环使用。工位将被用于与技能相对应的模块进行测试。

为了减少网络设备的数量，工位设备将用于多个模块的测试环境，使用技术手段进行快速轮替，以免造成浪费。