

# 2023 年柳州市职业技能大赛 网络安全项目技术工作文件

2023 年柳州市职业技能大赛执委会赛务保障与技术服务组

2023 年 5 月

# 目录

一、技术描述 .....	3
(一) 项目概要 .....	3
(二) 基本知识与能力要求 .....	3
二、试题与评判标准 .....	10
(一) 试题 (样题) .....	10
(二) 评判标准 .....	18
三、竞赛细则 .....	20
(一) 竞赛实施细则 .....	20
(二) 竞赛方式 .....	201
四、竞赛场地、设施设备等安排 .....	211
五、技术规范 .....	222
六、技术平台 .....	233
(一) 竞赛器材 .....	233
(二) 软件技术平台: .....	244
七、安全、健康要求 .....	255

## 一、技术描述

### （一）项目概要

主要考核参赛选手网络系统安全策略部署、信息保护、网络安全运维管理、网络安全事件应急响应、网络安全数据取证、应用安全、代码审计等综合实践能力。

### （二）基本知识与能力要求

项目	
1	工作组织和管理
	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"><li>• 健康与安全相关法规、义务、规定。</li><li>• 必须使用个人防护用品的场合，如：静电防护、静电放电。</li><li>• 在处理用户设备和信息时的诚信和安全的重要性。</li><li>• 废物回收、安全处置的重要性。</li><li>• 计划、调度和优先处置的方法。</li><li>• 在所有的工作实践过程中，注重准确、检验和细节的重要性。</li><li>• 系统性开展工作的重要性。</li><li>• 工作环境的 6S 管理。</li></ul>
	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"><li>• 遵守健康和标准、规则和规章制度。</li><li>• 保持安全的工作环境。</li><li>• 识别并使用适当的个人静电防护设备。</li><li>• 安全、妥善地选择、使用、清洁、维护和储存工具和设备</li><li>• 遵守相关规定，规划工作区域，维持日常整洁，实现最大化工</li></ul>

	<p>作效率。</p> <ul style="list-style-type: none"> <li>• 有效地工作，并定期检查进度和结果。</li> <li>• 采取全面有效的研究方法，确保知识不断更新。</li> <li>• 主动尝试新方法、新系统和愿意接受变革。</li> </ul>
2	<p>通讯和人际沟通技巧</p>
	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> <li>• 倾听是有效沟通的重要手段。</li> <li>• 团队成员的角色要求和最有效的沟通方式。</li> <li>• 与团队成员和管理人员建立和保持创造性的工作关系的重要性。</li> <li>• 有效的团队合作技巧。</li> <li>• 消除误会和化解冲突的技巧。</li> <li>• 管理紧张和愤怒情绪的能力。</li> <li>• 团队合作的重要性。</li> </ul>
	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> <li>• 运用认真倾听和提问的良好技巧，加深对复杂情境的理解。</li> <li>• 与团队成员进行持续有效的口头和书面沟通。</li> <li>• 认识到并适应团队成员不断变化的需求。</li> <li>• 积极推动，建立强大而有效的团队。</li> <li>• 与团队成员分享知识和专业知识，形成相互支持的学习文化。</li> <li>• 有效管理不良情绪，传递给他人解决问题的信心。</li> <li>• 与工作人员的沟通技巧。</li> </ul>
3	<p>安全规定条款</p>
	<p>个人（选手）需了解和理解：</p>

	<ul style="list-style-type: none"> <li>• 信息技术风险管理标准、政策、要求和过程。</li> <li>• 网络防御和漏洞评估工具的功能和使用方法。</li> <li>• 操作系统的具体功能。</li> <li>• 计算机编程相关概念，包括计算机语言、编程、测试、调试、删除和文件类型。</li> <li>• 应用于软件开发的网络安全和隐私原则和方法。</li> </ul>
	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> <li>• 在设计总体程序测试和记录评估过程时，应将网络安全和隐私原则应用于管理要求（与保密性、完整性、可用性、身份验证、数字签名不可抵赖性相关）。</li> <li>• 对管理、操作和技术安全控制进行独立全面的评估，并对信息技术系统内部或继承的控制改进进行评估，以确定控制的整体有效性。</li> <li>• 开发、创建和维护新的计算机应用程序、软件或专门应用程序。</li> <li>• 修改现有的计算机应用程序、软件或专门应用程序。</li> <li>• 分析新的或者现有计算机应用程序、软件或专业的应用程序的安全状况，提供可用的分析结果。</li> <li>• 进行软件系统研究并开发新功能，确保有网络安全防护功能。</li> <li>• 进行综合技术研究，对网络安全系统中可能存在的薄弱环节进行评估。</li> <li>• 计划、准备和实施系统测试。</li> <li>• 根据技术规范和要求，进行分析、评估并形成报告结果。</li> <li>• 测试和评估信息系统的安全情况，涵盖系统开发生命周期。</li> </ul>
4	操作、维护、监督和管理

	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> <li>• 查询语言，如 SQL (结构化查询语言) 。</li> <li>• 数据备份和恢复，数据标准化策略。</li> <li>• 网络协议，如 TCP/IP、动态主机配置(DHCP)、域名系统 (DNS) 和目录服务。</li> <li>• 防火墙概念和功能。</li> <li>• 网络安全体系结构的概念，包括拓扑、协议、组件和原则。</li> <li>• 系统、网络和操作系统加固技术。</li> <li>• 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）。</li> <li>• 信息技术安全原则和方法。</li> <li>• 身份验证、授权和访问控制方法。</li> <li>• 网络安全、漏洞和隐私原则。</li> <li>• 学习管理系统及其在管理学习中的应用。</li> <li>• 网络安全法与其他相关法规对其网络规划的影响。</li> </ul>
	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> <li>• 管理数据库或数据库管理系统。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul>

	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 管理账户、设置防火墙和安装操作系统补丁程序。</li> <li>• 访问控制、账户和密码的创建和管理。</li> <li>• 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。</li> <li>• 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。</li> </ul>
5	保护和防御
	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> <li>• 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]）。</li> <li>• 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。</li> <li>• 网络安全体系结构的概念，包括拓扑、协议、分层和原理。</li> <li>• 行业技术标准和分析原则、方法和工具。</li> <li>• 威胁调查、报告、调查工具和法律、法规。</li> <li>• 网络安全事件类别、响应和处理方法。</li> <li>• 网络防御和漏洞评估工具及其功能。</li> <li>• 对于已知安全风险的应对措施。</li> <li>• 身份验证、授权和访问方法。</li> </ul>
	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> <li>• 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</li> </ul>

	<p>告发生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。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 监控网络，及时记录未授权的活动。</li> <li>• 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。</li> <li>• 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。</li> <li>• 调查和分析相关网络安全应急响应活动。</li> <li>• 对威胁和漏洞进行评估。</li> <li>• 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。</li> </ul>
6	分析
	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> <li>• 网络威胁行为者的背景和使用的方法。</li> <li>• 用于检测各种可利用的活动的的方法和技术。</li> <li>• 网络情报信息收集能力和资源库。</li> <li>• 网络威胁和漏洞。</li> <li>• 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）。</li> <li>• 漏洞信息传播源（例如，警报、通知、勘误表和公告）。</li> <li>• 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</li> </ul>



	<p>行漏洞分析)。</p> <ul style="list-style-type: none"> <li>• 预测、模拟威胁和应对的内部策略。</li> <li>• 内部和外部协同的网络操作和工具。</li> <li>• 系统伪造和司法用例。</li> </ul>
	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> <li>• 识别和评估网络安全罪犯活动。</li> <li>• 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。</li> <li>• 分析搜集到的信息，找到系统弱点和潜在可被利用的环节。</li> <li>• 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。</li> <li>• 根据背景情况，同步和放置情报信息，找出可能的含义。</li> <li>• 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。</li> <li>• 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。</li> <li>• 识别、保存和使用系统开发过程遗留物并用于分析。</li> </ul>
7	收集与操作
	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> <li>• 收集策略、技术及工具应用。</li> <li>• 网络信息情报收集能力和资源库的利用。</li> <li>• 信息需求和收集需求的转换、跟踪、优先排序。</li> <li>• 网络运营计划方案、策略和有关资源。</li> <li>• 网络运营策略、资源和工具。</li> <li>• 网络运营的概念、网络运营术语、网络运营的原则、功能、边界和效果。</li> </ul>

	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> <li>• 运用适当的策略，通过收集管理的流程建立优先级，从而执行信息收集。</li> <li>• 执行深入的联合目标定位，执行网络安全流程。</li> <li>• 依照需求收集信息，执行详细计划及订单。</li> <li>• 支持收集关于网络威胁的证据，减轻或免受可能的或实时的网络威胁。</li> </ul>
8	调查
	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> <li>• 威胁调查、报告、调查工具和法律、法规。</li> <li>• 恶意软件分析的概念和方法。</li> <li>• 收集、打包、传输和储存电子证据的过程，同时并维持监管链。</li> <li>• 司法流程，包括事实陈述和证据。</li> <li>• 持久性数据的类型和集合。</li> <li>• 数字取证数据的类型和识别方法。</li> <li>• 网络安全漏洞的具体操作性影响。</li> </ul>
	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> <li>• 收集、处理、保存、分析和提供计算机相关的证据，以减轻网络脆弱性，支持犯罪、欺诈、反间谍或执法的调查。</li> </ul>

## 二、试题与评判标准

### （一）试题（样题）

#### 第一阶段任务书（70 分）

##### 任务 1：SQL 注入攻防

任务环境说明：

服务器场景：WebServ2003

服务器场景操作系统：Microsoft Windows2003 Server

服务器场景安装服务/工具 1：Apache2.2；

服务器场景安装服务/工具 2：Php6；

服务器场景安装服务/工具 3：Microsoft SqlServer2000；

服务器场景安装服务/工具 4：EditPlus；

1.访问 WebServ2003 服务器场景，进入 login.php 页面，分析该页面源程序，找到提交的变量名，并将该变量名作为 Flag 提交；

2.对该任务题目 1 页面注入点进行 SQL 注入渗透测试，使该 Web 站点可通过任意用户名登录，并将登录密码作为 Flag 提交；

3.进入 WebServ2003 服务器场景的 C:\AppServ\www 目录，找到 loginAuth.php 程序，使用 EditPlus 工具分析并修改 PHP 源程序，使之可以抵御 SQL 注入，并将修改后的 PHP 源程序中的 Flag 提交；

4.再次对该任务题目 1 页面注入点进行渗透测试，验证此次利用该注入点对 WebServ2003 服务器场景进行 SQL 注入渗透测试无效，并将 Web 页面回显内容作为 Flag 提交；

5.访问 WebServ2003 服务器场景，"/"->"Employee Information Query"，分析该页面源程序，找到提交的变量名，并将该变量名作为 Flag 提交；

6.对该任务题目 5 页面注入点进行渗透测试，根据输入“%”以及“\_”的返回结果确定是注入点，Web 页面回显作为 Flag 提交；

7.通过对该任务题目 5 页面注入点进行 SQL 注入渗透测试，删除 WebServ2003 服务器场景的 C:\目录下的 1.txt 文档，并将注入代码作为 Flag 提交；

8.进入 WebServ2003 服务器场景的 C:\AppServ\www 目录，找到 QueryCtrl.php 程序，使用 EditPlus 工具分析并修改 PHP 源程序，使之可以抵御 SQL 注入渗透测试，并将修改后的 PHP 源程序中的 Flag 提交；

9.再次对该任务题目 5 页面注入点进行渗透测试，验证此次利用注入点对该 WebServ2003 服务器场景进行 SQL 注入渗透测试无效，并将 Web 页面回显内容作为 Flag 提交。

## 任务 2：XSS 和 CSRF 攻防

任务环境说明：

服务器场景：WebServ2003

服务器场景操作系统：Microsoft Windows2003 Server

服务器场景安装服务/工具 1：Apache2.2；

服务器场景安装服务/工具 2：Php6；

服务器场景安装服务/工具 3：Microsoft SqlServer2000；

服务器场景安装服务/工具 4：EditPlus；

1.访问 WebServ2003 服务器场景，“/”->“Employee Message Board”，分析该页面源程序，找到提交的变量名，并将

该变量名作为 Flag 提交；

2.对该任务题目 1 页面注入点进行 XSS 渗透测试，并进入"/"->" Employee Message Board"->"Display Message"页面，根据该页面的显示，确定是注入点，并将 Web 页面回显内容作为 Flag 提交；

3.对该任务题目 1 页面注入点进行渗透测试，使"/"->"Employee Message Board"->"Display Message"页面的访问者执行网站 (<http://hacker.org/>) 中的木马程序：<http://hacker.org/TrojanHorse.exe>，并将注入代码内容作为 Flag 提交；

4.通过 IIS 搭建网站 (<http://hacker.org/>)，并通过 PC2 生成木马程序 TrojanHorse.exe，将该程序复制到网站 (<http://hacker.org/>) 的 WWW 根目录下，并将该网站标题作为 Flag 提交；

5.当"/"->" Employee Message Board"->"Display Message"页面的访问者执行网站 (<http://hacker.org/>) 中的木马程序 TrojanHorse.exe 以后，访问者主机需要被 PC-3 远程控制，打开访问者主机的 CMD.exe 命令行窗口，并将该操作结果回显作为 Flag 提交；

6.进入 WebServ2003 服务器场景的 C:\AppServ\www 目录，找到 insert.php 程序，使用 EditPlus 工具分析并修改 PHP 源程序，使之可以抵御 XSS 渗透测试，并将修改后的 PHP 源程序中的 Flag 提交；

7.再次对该任务题目 1 页面注入点进行渗透测试，验证此次利用该注入点对 WebServ2003 服务器场景进行 XSS 渗

透测试无效，并将 Web 页面回显作为 Flag 提交；

8.访问 WebServ2003 服务器场景，"/"->" Shopping Hall", 分析该页面源程序，找到提交的变量名，并将该变量名作为 Flag 提交；

9.对该任务题目 1 页面注入点进行渗透测试，使"/"->"Employee Message Board"->"Display Message"页面的访问者向页面 ShoppingProcess.php 提交参数 goods=cpu&quantity=999999，查看"/"->"PurchasedGoods.php 页面，并将注入代码作为 Flag 提交；

10.进入 WebServ2003 服务器场景的 C:\AppServ\www 目录，找到 DisplayMessage.php 程序，使用 EditPlus 工具分析并修改 PHP 源程序，使之可以抵御 CSRF 渗透测试，并将修改后的源程序中的 Flag 提交；

11.再次对该任务题目 1 页面注入点进行渗透测试，验证此次利用该注入点对 WebServ2003 服务器场景进行 CSRF 渗透测试无效，并将 Web 页面回显内容作为 Flag 提交；

任务 3：命令注入与文件包含攻防

任务环境说明：

服务器场景：WebServ2003

服务器场景操作系统：Microsoft Windows2003 Server

服务器场景安装服务/工具 1：Apache2.2；

服务器场景安装服务/工具 2：Php6；

服务器场景安装服务/工具 3：Microsoft SqlServer2000；

服务器场景安装服务/工具 4：EditPlus；

1.Web 访问 WebServ2003 服务器场景, "/"->" Display Directory", 分析该页面源程序, 找到提交的变量名, 并将该变量名作为 Flag 提交;

2.对该任务题目 1 页面注入点进行渗透测试, 使页面 DisplayDirectoryCtrl.php 回显 C:\Windows 目录内容的同时, 对 WebServ2003 服务器场景添加账号“Hacker”, 将该账号加入管理员组, 并将注入代码作为 Flag 提交;

3.进入 WebServ2003 服务器场景的 C:\AppServ\www 目录, 找到 DisplayDirectoryCtrl.php 程序, 使用 EditPlus 工具分析并修改 PHP 源程序, 使之可以抵御命令注入渗透测试, 并将修改后的源程序中的 Flag 提交;

4.再次对该任务题目 1 页面注入点进行渗透测试, 验证此次利用注入点对 WebServ2003 服务器场景进行命令注入渗透测试无效, 并将 Web 页面回显作为 Flag 提交;

5.Web 访问 WebServ2003 服务器场景, "/"->" Display Uploaded's File Content", 分析该页面源程序, 找到提交的变量名, 并将该变量名作为 Flag 提交;

6.对该任务题目 5 页面注入点进行渗透测试, 使页面 DisplayFileCtrl.php 回显 WebServ2003 服务器场景访问日志文件: AppServ/Apache2.2/logs/access.log 的内容, 并将注入代码作为 Flag 提交;

7.进入 WebServ2003 服务器场景的 C:\AppServ\www 目录, 找到 DisplayFileCtrl.php 程序, 使用 EditPlus 工具分析并

修改 PHP 源程序，使之可以抵御文件包含渗透测试，并将修改后的源程序中的 Flag 提交；

8.再次对该任务题目 5 页面注入点进行渗透测试，验证此次利用注入点对 WebServ2003 服务器场景进行文件包含渗透测试无效，并将 Web 页面回显作为 Flag 提交。

### **第二阶段任务书：分组对抗（30 分）**

假定各位选手是某公司的系统管理员，负责服务器（受保护服务器 IP、管理员账号见现场发放的参数表）的维护，该服务器可能存在着各种问题和漏洞（见漏洞列表）。你需要尽快对服务器进行加固，十五分钟之后将会有很多黑客对这台服务器进行攻击。

提示 1：该题不需要保存文档；

提示 2：服务器中的漏洞可能是常规漏洞也可能是系统漏洞；

提示 3：加固常规漏洞；

提示 4：对其他参赛队系统进行渗透测试，取得 FLAG 值并提交到裁判服务器。

十五分钟之后，各位选手将真正进入分组对抗环节。

注意事项：

注意 1：任何时候不能关闭 80 端口，否则将判令停止比赛，该阶段分数为 0 分；

注意 2：不能对裁判服务器进行攻击，否则将判令停止比赛，该阶段分数为 0 分。



注意 3：在加固阶段（前十五分钟，具体听现场裁判指令）不得对任何服务器进行攻击，否则将判令攻击者停止比赛，该阶段分数为 0 分。

注意 4：FLAG 值为每台受保护服务器的唯一性标识，每台受保护服务器仅有一个。

在这个环节里，各位选手需要继续保护你的服务器免受各类黑客的攻击，你可以继续加固你的服务器，你也可以选择攻击其他组的保护服务器（其他服务器网段见现场发放的参数表）。

漏洞列表：

1.靶机上的网站可能存在命令注入的漏洞，要求选手找到命令注入的相关漏洞，利用此漏洞获取一定权限。

2.靶机上的网站可能存在文件上传漏洞，要求选手找到文件上传的相关漏洞，利用此漏洞获取一定权限

3.靶机上的网站可能存在文件包含漏洞，要求选手找到文件包含的相关漏洞，与别的漏洞相结合获取一定权限并进行提权

4.操作系统提供的服务可能存在远程代码执行的漏洞，要求用户找到远程代码执行的服务，并利用此漏洞获取系统权限。

5.操作系统提供的服务可能包含了缓冲区溢出漏洞，要求用户找到缓冲区溢出漏洞的服务，并利用此漏洞获取系统权限。

6.操作系统中可能存在系统后门，选手可以找到后门，并利用预留的后门直接获取到系统权限。

选手通过以上的所有漏洞点，最后得到其他选手靶机的最高权限，并获取到其他选手靶机上的 **FLAG** 值进行提交。

## （二）评判标准

### 1.分数权重：

竞赛阶段	阶段名称	任务阶段	评分方式	比赛时长
模块 B 权重 70%	安全事件响应、网络安全数据取证、应用安全	任务 1...N	机考评分	180 分钟
模块 C 权重 30%	CTF 夺旗攻击	系统攻防演练	机考评分	180 分钟

### 2.评判方法：

#### （1）模块 B 评分规则

模块 B 总分为 700 分,分为 N 个任务，每道题的具体分值在赛题中标明；模块 B 安全事件响应、网络安全数据取证、应用安全等部分由系统自动评分和排名，对外公开显示。

#### （2）模块 C 评分规则

模块 C 总分为 300 分，按照选手获得攻击“FLAG”的值得到相应的分数。系统自动评分和排名，对外公开显示。

选手在答题过程中不得违反竞赛试题要求答题，不得以违规形式获取得分，不得违规攻击裁判服务器、网关、系统服务器等非靶机目标，如检测选手有违规攻击行为，警告一次后若继续攻击，判令该队终止竞赛，清离出场。

### （3）裁判组构建

赛前建立健全裁判组。裁判组为裁判长负责制。

本赛项拟设裁判 4 名。其中裁判长 1 名，现场裁判 1 名，评分裁判 1 名，加密裁判 1 名。

因为本赛项模块 B、C 由计算机自动评分，赛场内需进行两次加密，提交作品需进行三次加密。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：对参赛选手提交作品进行第三次加密，将加密后的成果，交由裁判长组织评分裁判进行评分。第三次加密过程文件由加密裁判密封保存，单独保管。

所有加密结果密封袋的封条均需由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。

#### （4）评分流程

现场裁判组监督现场机考评分，评分裁判负责参赛选手提交作品评分，裁判长负责竞赛全过程。

竞赛现场派驻监督员、裁判员、技术支持队伍等，分工明确。现场裁判员负责与参赛选手的交流沟通及试卷等材料的收发，负责设备问题确认和现场执裁；技术支持工程师负责所有工位设备应急，负责执行裁判确认后的设备应急处理。

### 三、竞赛细则

#### （一）竞赛实施细则

##### 1. 报名资格

参赛选手须为 2023 年度企业在职职工或者院校在校学生；参赛选手不限性别。

2. 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。

3. 竞赛所需的硬件设备、系统软件和辅助工具由组委会统一安排，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。

4. 参赛选手自行决定工作程序和时间安排。

5. 参赛选手在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。

6. 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。

7.竞赛结束（或提前完成）后，参赛选手起立，在确认后不得再进行任何操作，按顺序离场。

8.最终竞赛成绩经复核无误及裁判长、监督长签字确认后，在指定地点，以纸质形式在指定点向全体参赛队进行提前公布，各参赛队无异议后在闭赛式上予以宣布。

9.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。

10.赛项结束后专家工作组根据裁判判分情况，分析参赛选手在竞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。

11.赛项每个竞赛环节裁判评分的原始材料和最终成绩等结果性材料经监督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。

## （二）竞赛方式

本赛项为团体赛，以企业或者院校为单位组队参赛，不得跨企业或者跨校组队。每个参赛队由2名选手组成。

## 四、竞赛场地、设施设备安排

（一）竞赛场地。竞赛场地的配备必须符合疫情防控要

求，竞赛现场设置竞赛区、裁判区、技术支持区。现场保证良好的采光、照明和良好通风；提供稳定的水、电和供电应急设备，提供足够的干粉灭火器材。

（二）竞赛设备。竞赛设备由执委会和承办校负责提供和保障，竞赛区按照参赛队数量准备竞赛所需的软硬件平台，为参赛队提供标准竞赛设备。

（三）竞赛工位。工位间距和场地空间必须符合疫情防控要求，竞赛现场各个工作区配备单相 220V/3A 以上交流电源。每个竞赛工位上标明编号并用隔离带隔离，确保参赛队之间互不干扰，每个竞赛工位配备 2 把工作椅（凳）。

（四）技术支持区为技术支持人员的工作场地，为参赛选手竞赛提供网络环境部署和网络安全防范。

（五）竞赛工位隔离和抗干扰。竞赛工位之间标有隔离线。

## 五、技术规范

该赛项结合企业职业岗位对人才培养需求，涉及的信息网络安全工程在设计、组建过程中，主要有以下 8 项国家职业标准，参赛选手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	GA/T 1389-2017	《信息安全技术网络安全等级保护定级指南》
2	GB 17859-1999	《计算机信息系统安全保护等级划分准则》
3	GB/T 20271-2	《信息安全技术信息系统通用安全技术要求》

	006	
4	GB/T 20270-2006	《信息安全技术网络基础安全技术要求》
5	GB/T 20272-2006	《信息安全技术操作系统安全技术要求》
6	GB/T 20273-2006	《信息安全技术数据库管理系统安全技术要求》
7	GA/T 671-2006	《信息安全技术终端计算机系统安全等级技术要求》
8	GB/T 20269-2006	《信息安全技术信息系统安全管理要求》

## 六、技术平台

### （一）竞赛器材

序号	设备名称	数量	设备要求
1	网络安全竞赛平台	1	<p>1. 能完成基础设施设置、安全加固、安全事件响应、网络安全数据取证、应用安全、CTF 夺旗攻击、CTF 夺旗防御等知识、技能内容竞赛环境实现，能有效支持 300 人规模，具备基于本规程竞赛内容同一场景集中答题环境。</p> <p>2. 标配 2 个千兆以太网口，Intel 处理器，大于等于 16G 内存，SSD +SATA 硬盘。可扩展多种虚拟化平台，支持集群</p>

			<p>管理，同步采用增量备份的方式，虚拟化管理采用标准 libvirt 接口；支持多用户并发在线竞赛，根据不同的实战任务下发进行自动调度靶机虚拟化模板，全程无需手工配置地址，VLAN 与 IP 可根据竞赛要求自行设定；提供单兵闯关、分组混战等实际对战模式，阶段间无需人工切换，系统自动处理；提供超过 20 种不同级别 70 个的攻防场景；模块 B、C 全过程自动评判，支持竞赛过程图像元素上传，排名判定策略大于等于 12 种；自定义动画态势展示，成绩详细分析；支持监控异常虚拟机，同时检测 FTP、HTTP、ICMP、SMTP、SSH、TCP 和 UDP 协议，服务端口支持在有效范围内的服务端口；支持全程加密，支持加密文件导入，加密方式为非对称加密，设备能随机生成密码。</p>
2	PC 机	2	<p>CPU 主频<math>\geq 2.8\text{GHZ}</math>,<math>\geq</math>四核四线程；内存<math>\geq 8\text{G}</math>；硬盘<math>\geq 500\text{G}</math>；支持硬件虚拟化。</p>

## （二）软件技术平台：

竞赛的应用系统环境主要以 Windows 和 Linux 系统为主，涉及如下版本：



1. 物理机安装操作系统：微软 Windows 7(64 位)中文试用版或微软 Windows 10(64 位)中文试用版。

2. 虚拟机安装操作系统：

Windows 系统（试用版）：Windows XP、Windows 7、Windows 10、Windows Server2003 及以上版本（根据命题实际确定）。

Linux 系统：Ubuntu、Debian、CentOS（具体版本根据命题实际确定）。

3.其他主要应用软件为（实际竞赛环境可能不仅限于以下软件）：

VMware workstation 12 pro 及以上版本免费版

Putty 0.67 及以上版本

Python 3 及以上版本

Chrome 浏览器 62.0 及以上版本

RealVNC 客户端 4.6 及以上版本

JDK（Java Development Kit）7.0 及以上版本

## 七、安全、健康要求

根据国家相关法规要求，结合本项目实际，提出安全、健康要求及职业操作规范要求，并明确违反后的处理规定。特别是根据本项目具体情况的诸如人身防护，有毒、有害物质携带、存放，防火、防爆等措施。