

2024 年甘肃省职业院校技能大赛中职组电子与信息类

“网络安全”赛项竞赛规程

（一）赛项名称

赛项名称：网络安全

英文名称：Cyber Security

赛项组别：中职组

专业大类：信息技术类

（二）竞赛目的

网络空间已经成为陆、海、空、天之后的第五大主权领域空间，习近平总书记强调：没有网络安全就没有国家安全。为引领全国中职学校紧跟网络安全技术和产业的发展，为国家和社会培养急需的网络安全技能型人才，国家教育部联合多部委特举办本赛项，将网络安全行业新业态、新技术、新标准等纳入比赛内容，以赛促教，以赛促学，以赛促改，发挥示范引领作用，推进“岗课赛证”综合育人。

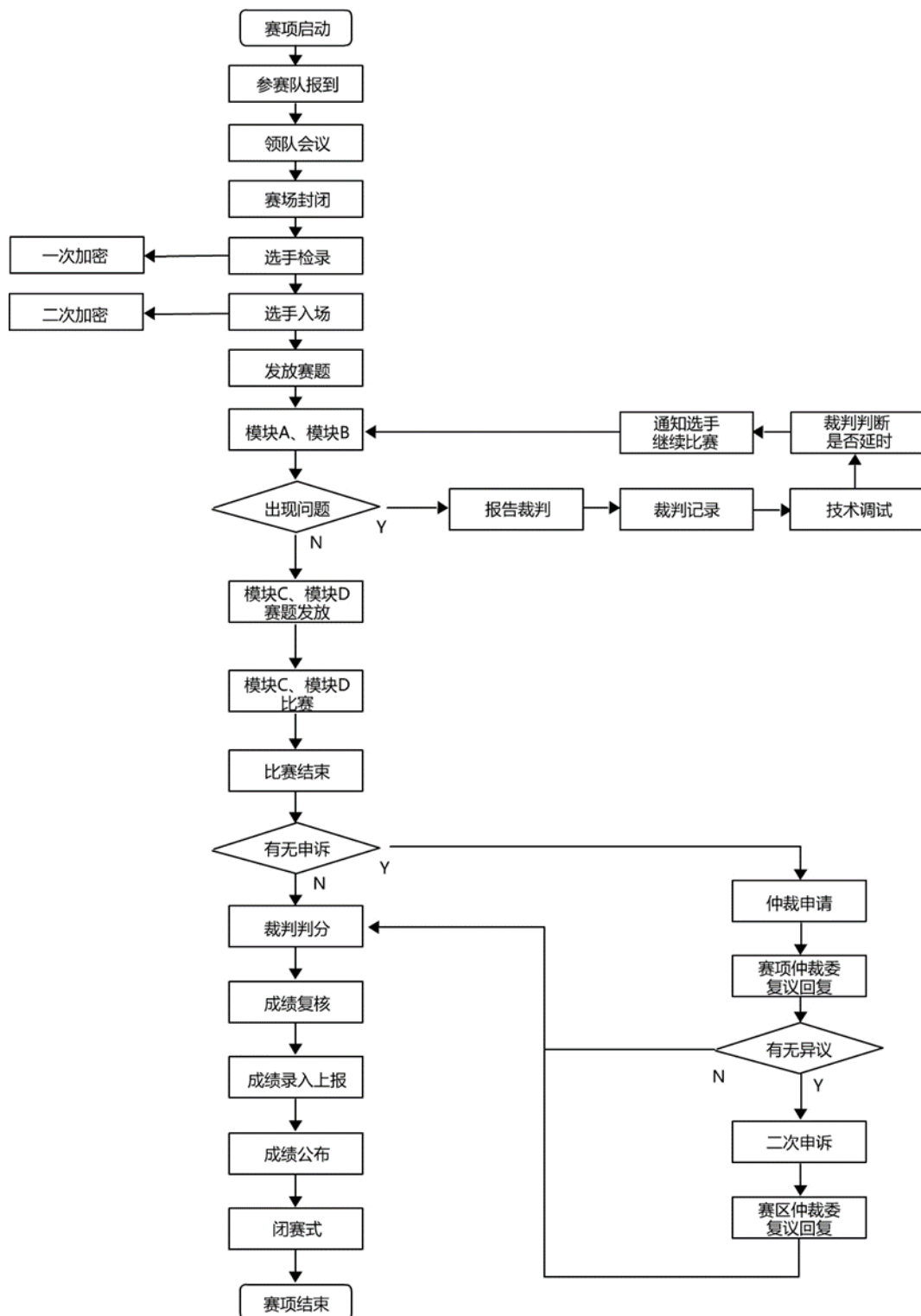
（三）竞赛时间及流程

1. 竞赛时间、地点

竞赛时间：待定根据甘肃省教育厅下发文件为准

竞赛地点：兰州石化职业技术大学新区校区（重技楼）

2. 竞赛流程图



3. 竞赛场次

竞赛限定在 1 天内进行，竞赛场次为 1 场，竞赛时间为 3 小时。

模块编号	模块名称	竞赛时间（小时）	权值
A	基础设施设置与安全加固	1.5	20%
B	网络安全事件响应、数字取证调查和应用安全		40%
C	CTF 夺旗-攻击	1.5	20%
D	CTF 夺旗-防御		20%
总计		3	100%

（四）竞赛内容

1. 竞赛内容

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，具体包括：

竞赛阶段	竞赛任务	竞赛内容
A 模块	基础设施设置与安全加固	登录安全加固、数据库加固（Data）、Web 安全加固（Web）、流量完整性保护（Web,Data）、事件监控、服务加固、防火墙策略等；
B 模块	网络安全事件响应、数字取证调查和应用安全	网络安全事件、数字取证调查和应用安全” 内容主要包括：数据分析、数字取证、内存取证、漏洞扫描与利用、操作系统渗透测试、应急响应等；
C 模块	CTF 夺旗-攻击	假定你是某企业的网络安全渗透测试工程师，负责企业某些服务器的安全防护，为了更好的寻找企业网络中可能存在的各种问题和漏洞。你尝试利用各种攻击手段，攻击特定靶机，了解网络黑客的心态，

		从而改善您的防御策略；
D 模块	CTF 夺旗-防御	假定各位选手是某安全企业的网络安全工程师，负责若干服务器的渗透测试与安全防护，这些服务器可能存在着各种问题和漏洞。你需要尽快对这些服务器进行渗透测试与安全防护。每个参赛队拥有专属的堡垒机服务器，参赛选手通过扫描、渗透测试等手段检测自己堡垒服务器中存在的安全缺陷，进行针对性加固，从而提升系统的安全防御性能。

2. 竞赛分值权重和时间安排

模块编号	模块名称	竞赛时间（小时）	权值
A	基础设施设置与安全加固	1.5	20%
B	网络安全事件响应、数字取证调查和应用安全		40%
C	CTF 夺旗-攻击	1.5	20%
D	CTF 夺旗-防御		20%
总计		3	100%

（五）竞赛方式

本赛项为团体赛，以院校为单位组队参赛，不得跨校组队。每个参赛队由 2 名选手组成，同一学校报名参赛队不超过 1 支。指导教师须为本校专任教师，每个参赛队限报 2 名指导教师。

1. 报名资格

参赛选手须为 2023 年度在籍全日制中等职业学校学生；五年制全日制高职一至三年级（含三年级）在籍学生可参加竞赛。参赛选手不限性别，年龄须不超过 21 周岁，年龄计算的截止时间以 2023 年 10 月 30 日为准。

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. 参赛选手在赛前 20 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。

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。

（六）竞赛环境

1. 竞赛场地。竞赛场地需保证良好的采光、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。同时提供所有指导教师休息室 1 间。

2. 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。

3. 竞赛工位。工位间距和场地空间必须符合竞赛要求，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）。

4. 服务区提供医疗等服务保障，并用隔离带隔离。

（七）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 20271-2006	《信息安全技术信息系统通用安全技术要求》
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》

（八）技术平台

1. 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>磐云网络安全实战平台</p> <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</p>

			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。
2	PC 机	2	CPU 主频>=2.8GHZ,>=四核四线程；内存>=8G；硬盘>=500G；支持硬件虚拟化。

2. 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

Chrome 浏览器 62.0 及以上版本

RealVNC 客户端 4.6 及以上版本

（九）成绩评定

1. 评分说明

在规定时间内完成规定的任务，以质量高低（正确率）完成评分。

2. 裁判评分方法

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。

3. 成绩产生办法

(1) 评分阶段：

竞赛阶段	阶段名称	任务阶段	评分方式
模块 A 权重 40%	基础设施设置、安全加固	任务 1...N	裁判客观评分
模块 B 权重 60%	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
模块 C 权重 20%	CTF 夺旗攻击	系统攻防演练	机考评分
模块 D 权重 20%	CTF 夺旗防御	系统攻防演练	裁判客观评分

(2) 模块 A、模块 B 评分规则

模块 A 与模块 B 总分为 600 分，分为 N 个任务，每道题的具体分值在赛题中标明；模块 A 基础设施设置、安全加固部分评分由评分裁判客观评分；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。

(3) 模块 C、模块 D 评分规则

模块 C 总分为 200 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。

模块 D 总分为 200 分，按照选手答题内容，由评分裁判进行客观评分。

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。

（十）奖项说明

按实际参赛人(队)数的 10%、20%、30%（小数点后一位四舍五入）分设一、二、三等奖。

（十一）申诉与总裁

1. 各参赛队对不符合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、竞赛成绩，以及工作人员的不规范行为等，可向赛项仲裁组提出申诉，申诉主体为参赛队领队。

2. 申诉启动时，参赛队向赛项仲裁组递交领队亲笔签字的书面报告。书面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

3. 提出申诉的时间应在比赛结束后(选手赛场比赛内容全部完成)2 小时内。超过时效不予受理

4. 赛项仲裁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，可由领队向比赛监督员提出申诉，由监督员传达最终仲裁结果。

5. 申诉方不得以任何理由拒绝接收仲裁结果，不得以任何理由采取过激行为扰乱赛场秩序。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。

6. 申诉方可随时提出放弃申诉。

（十二）安全预案

为保障赛项顺利进行，避免竞赛过程中出现可能的不可控的紧急情况，赛项预案由赛项可靠性设计、故障的应急处理方案两部分组成。

1. 赛项可靠性设计

（1）电力系统可靠性设计 供电负荷匹配电力要求，防止电子设备运行过程中过载导致火灾隐患或电力中断；提供三项电源接地保证，杜绝运行过程中静电可能导致设备重启、短路、漏电等安全威胁；布线强弱电分离，防止发生干扰；各区域供电保障独立，相互不干扰。

（2）弱电系统可靠性设计 弱电系统必须保证良好的运行状态，系统应具备长期和稳定的工作能力，遇到突发状况时应存在快速解决方法，保证系统可靠运行。弱电系统应与电力系统隔离部署，防止干扰造成故障。

（3）网络设备可靠性设计 网络设备必须要运行稳定，满足带宽要求，预留端口备份，通信 线缆、设备预留备份，具备故障快速恢复机制，提供必要的冗余备份设计。

(4) 攻防平台可靠性设计平台必须支持集群功能，在大规模流量下支持负载分担，同时可为竞赛数据提供备份、回退机制。具备冗余备份机制，在最短时间内恢复故障问题。平台应提供访问控制机制，具备防攻击手段，保障平台运行稳定。

(5) PC 可靠性设计 PC 的部署必须保证良好的运行状态，遇到突发状况时应存在快速解决方法，保证系统可靠运行。系统规格必须满足要求，保证良好的性能和稳定的运行。

2. 故障的应急处理方案

(1) 参赛选手 PC 故障

如参赛选手 PC 遇到故障，先判断其为硬件故障还是软件故障。软件故障或出现卡顿现象则对 PC 进行重启，因 PC 配备还原卡，可将系统恢复至初始状态，故障恢复时间约 30 秒；硬件故障经过现场裁判允许后更换备用机，故障恢复时间约 1 分钟。键盘、鼠标故障及时更换，恢复时间约 1-3 分钟。不会对学生成绩产生影响。

(2) 竞赛工位线缆连接故障

竞赛工位如遇到网络连接问题，现场裁判判定线缆物理连接问题，非选手设置操作导致，应及时更换备用线缆，故障恢复时间约 30 秒；竞赛工位两条以上网线物理故障，经现场裁判允许为其更换竞赛工位，故障恢复时间约 3-5 分钟。

(3) 竞赛工位电力故障

如遇竞赛工位电力故障,经裁判长允许更换备用工位。故障恢复时间 3-5 分钟。

(4) 网络设备交换机故障

更换备用交换机,故障恢复时间约 5-10 分钟;跳线线缆故障及时更换备用线缆(光纤及网线),故障恢复时间约 3-5 分钟。

(5) 攻防平台集群故障

服务器集群主设备故障,启用备用集群设备,数据互备份,集群恢复时间约 5-10 分钟。服务器集群从设备故障,更换备用设备,恢复时间约 5-10 分钟。成绩实时保存,不会对学生成绩产生影响。

(6) WEB 应用防火墙故障

如遇 WAF 设备故障,影响访问,取消防护策略或取消 WAF 设备连接,故障恢复时间约 1-3 分钟。

(7) 服务器区供电问题

若服务器区发生供电问题,UPS 电源可支持 20-30 分钟。

(十三) 竞赛须知

1. 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) 对于有碍竞赛公正和竞赛正常进行的参赛队，视其情节轻重，按照相关管理办法给予警告、取消竞赛成绩、通报批评等处理。

2. 参赛领队须知

(1) 领队应按时参加赛前领队会议，不得无故缺席。

(2) 领队负责组织本参赛队参加各项赛事活动。

(3) 领队应积极做好本参赛队的服务工作，协调各参赛队与赛项组织机构、承办院校的对接，按照防疫要求做好团队各项防疫工作。

(4) 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。

3. 参赛选手须知

(1) 各参赛选手要按照防疫要求做好个人和团队防疫工作，发扬良好道德风尚，听从指挥，服从裁判，不弄虚作假。如发现弄虚作假者，取消参赛资格，名次无效。

(2) 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。

(3) 参赛选手应按照规定时间抵达赛场，凭统一印制的参赛证、有效身份证件检录，按要求入场，不得迟到早退。请勿携带任何电子设备及其他资料、用品进入赛场。

(4) 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。

(5) 参赛选手应增强角色意识，科学合理做好时间分配。

(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) 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。

(9) 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。

(10) 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。

(11) 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。

4. 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，在赛项组织部门的领导下，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。

(十四) 其他规定

1. 食宿酒店（暂定）：兰州新区翰东酒店（原兰州新区博华酒店）。

2. 有关食宿的其他服务需求，请提前与赛务组联系。

2024 年甘肃省职业院校技能大赛中职组“网络安全”赛
项
比赛任务书（样题）

一、竞赛时间

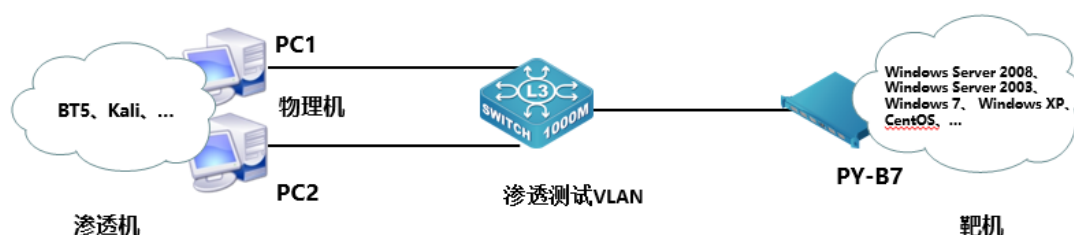
总计：180 分钟

二、竞赛阶段

竞赛阶段	任务阶段	竞赛任务	竞赛时间	分值
A 模块	A-1	登录安全加固	90 分钟	200 分
	A-2	本地安全策略配置		
	A-3	流量完整性保护		
	A-4	事件监控		
	A-5	服务加固		
	A-6	防火墙策略		
B 模块	B-1	Windows 操作系统渗透测试	90 分钟	400 分
	B-2	Linux 操作系统渗透测试		
	B-3	数字调查取证		
	B-4	网络安全事件响应		
	B-5	Web 安全绕过		
C、D 模块	C 模块	CTF 夺旗-攻击	90 分钟	200 分
	D 模块	CTF 夺旗-防御		200 分

三、竞赛任务书内容

(一) 拓扑图



(二) A 模块基础设施设置/安全加固 (200 分)

一、项目和任务描述:

假定你是某企业的网络安全工程师，对于企业的服务器系统，根据任务要求确保各服务正常运行，并通过综合运用登录和密码策略、流量完整性保护策略、事件监控策略、防火墙策略等多种安全策略来提升服务器系统的网络安全防御能力。

二、服务器环境说明

AServer06(Windows)系统：用户名 administrator 密码 P@ssw0rd

AServer07(Linux)系统：用户名 root 密码 123456

三、说明:

1. 所有截图要求截图界面、字体清晰，并粘贴于相应题目要求的位置；
2. 文件名命名及保存：网络安全模块 A-XX (XX 为工位号)，PDF 格式保存；
3. 文件保存到 U 盘提交。

A-1: 登录安全加固 (Windows, Linux)

请对服务器 Windows、Linux 按要求进行相应的设置，提高服务器的安全性。

1. 密码策略 (Windows, Linux)

- a) 密码策略必须同时满足大小写字母、数字、特殊字符 (Windows)，将密码必

须符合复杂性要求的属性配置界面截图：

- b) 密码策略必须同时满足大小写字母、数字、特殊字符（Linux），将
/etc/pam.d/system-auth 配置文件中对应的部分截图：
- c) 最小密码长度不少于 8 个字符（Windows），将密码长度最小值的属性配置界面截图：
- d) 最小密码长度不少于 8 个字符（Linux），将/etc/login.defs 配置文件中对应的部分截图：

2. 登录策略

- a) 设置账户锁定阈值为 6 次错误锁定账户，锁定时间为 1 分钟，复位账户锁定计数器为 1 分钟之后（Windows），将账户锁定策略配置界面截图：
- b) 一分钟内仅允许 5 次登录失败，超过 5 次，登录帐号锁定 1 分钟（Linux），将/etc/pam.d/login 配置文件中对应的部分截图：

3. 用户安全管理 (Windows)

- a) 禁止发送未加密的密码到第三方 SMB 服务器，将 Microsoft 网络客户端：将未加密的密码发送到第三方 SMB 服务器的属性配置界面截图：
- b) 禁用来宾账户，禁止来宾用户访问计算机或访问域的内置账户，将账户：来宾账户状态的属性配置界面截图：

A-2：本地安全策略设置（Windows）

- 1. 关闭系统时清除虚拟内存页面文件，将关机：清除虚拟内存页面文件的属性配置界面截图：
- 2. 禁止系统在未登录的情况下关闭，将关机：允许系统在未登录的情况下关闭的属性配置界面截图：
- 3. 禁止软盘复制并访问所有驱动器和所有文件夹，将恢复控制台：允许软盘复制并访问所有驱动器和所有文件夹的属性配置界面截图：
- 4. 禁止显示上次登录的用户名，将交互式登录：不显示最后的用户名的属性配置界面截图：

A-3: 流量完整性保护 (Windows, Linux)

1. 创建 `www.chinaskills.com` 站点，在 `C:\web` 文件夹内中创建名称为 `chinaskills.html` 的主页，主页显示内容“热烈庆祝 2022 年职业院校技能大赛开幕”，同时只允许使用 SSL 且只能采用域名（域名为 `www.test.com`）方式进行访问，将网站绑定的配置界面截图：
2. 为了防止密码在登录或者传输信息中被窃取，仅使用证书登录 SSH (Linux)，将 `/etc/ssh/sshd_config` 配置文件中对应的部分截图：

A-4: 事件监控 (Windows)

1. 应用程序日志文件最大大小达到 65M 时将其存档，不覆盖事件，将日志属性-应用程序（类型：管理的）配置界面截图：

A-5: 服务加固 SSH\VSFTPD\IIS (Windows, Linux)

1. SSH 服务加固 (Linux)
 - a) SSH 禁止 root 用户远程登录，将 `/etc/ssh/sshd_config` 配置文件中对应的部分截图：
 - b) 设置 root 用户的计划任务。每天早上 7:50 自动开启 SSH 服务，22:50 关闭；每周六的 7:30 重新启动 SSH 服务，使用命令 `crontab -l`，将回显结果截图；
 - c) 修改 SSH 服务端口为 2222，使用命令 `netstat -anltp | grep sshd` 查看 SSH 服务端口信息，将回显结果截图；
2. VSFTPD 服务加固 (Linux)
 - a) 设置数据连接的超时时间为 2 分钟，将 `/etc/vsftpd/vsftpd.conf` 配置文件中对应的部分截图：
 - b) 设置站点本地用户访问的最大传输速率为 1M，将 `/etc/vsftpd/vsftpd.conf` 配置文件中对应的部分截图：
3. IIS 加固 (Windows)

- a) 防止文件枚举漏洞枚举网络服务器根目录文件，禁止 IIS 短文件名泄露，将配置命令截图：
- b) 关闭 IIS 的 WebDAV 功能增强网站的安全性，将警报提示信息截图：

A-6: 防火墙策略 (Linux)

- 1. 只允许转发来自 172.16.0.0/24 局域网段的 DNS 解析请求数据包，将 iptables 配置命令截图：
- 2. 禁止任何机器 ping 本机，将 iptables 配置命令截图：
- 3. 禁止本机 ping 任何机器，将 iptables 配置命令截图：
- 4. 禁用 23 端口，将 iptables 配置命令截图：
- 5. 禁止转发来自 MAC 地址为 29:0E:29:27:65:EF 主机的数据包，将 iptables 配置命令截图：
- 6. 为防御 IP 碎片攻击，设置 iptables 防火墙策略限制 IP 碎片的数量，仅允许每秒处理 1000 个，将 iptables 配置命令截图：
- 7. 为防止 SSH 服务被暴力枚举，设置 iptables 防火墙策略仅允许 172.16.10.0/24 网段内的主机通过 SSH 连接本机，将 iptables 配置命令截图：

(三) B 模块安全事件响应/网络安全数据取证/应用安全 (400 分)

B-1: Windows 操作系统渗透测试

任务环境说明：

- ✓ 服务器场景：Server2003
 - ✓ 服务器场景操作系统：Windows7
- 1. 通过本地 PC 中渗透测试平台 Kali 对服务器场景 Windows 进行系统服务及版本扫描渗透测试，并将该操作显示结果中 Telnet 服务对应的端口号作为 FLAG 提交；
 - 2. 通过本地 PC 中渗透测试平台 Kali 对服务器场景 Windows 进行渗透测试，使用

- kali 中 hydra 对服务器 Telnet 服务进行暴力破解（用户名为 teltest），将 hydra 使用的必要参数当做 FLAG 进行提交（例：nmap -s -p 22）；（字典路径 /usr/share/wordlists/dirb/small.txt）
3. 通过本地 PC 中渗透测试平台 Kali 对服务器场景 Windows 进行渗透测试，使用 kali 中 hydra 对服务器 Telnet 服务进行暴力破解（用户名为 teltest），将破解成功的密码当做 FLAG 进行提交；（字典路径 /usr/share/wordlists/dirb/small.txt）
 4. 通过本地 PC 中渗透测试平台 win7 对服务器场景 Windows 进行渗透测试，取得的账户密码有远程桌面权限，将该场景系统中 sam 文件使用 reg 相关命令提取，将完整命令作为 FLAG 提交；
 5. 通过本地 PC 中渗透测试平台 win7 对服务器场景 Windows 进行渗透测试，取得的账户密码有远程桌面权限，将该场景系统中 system 文件使用 reg 相关命令提取，将完整命令作为 FLAG 提交；
 6. 通过本地 PC 中渗透测试平台 win7 对服务器场景 Windows 进行渗透测试，将 sam 文件与 system 文件提取到本地，使用桌面 mimikatz 工具提取 teltest 密码信息，将提取信息的命令作为 FLAG 提交；
 7. 通过本地 PC 中渗透测试平台 win7 对服务器场景 Windows 进行渗透测试，将 sam 文件与 system 文件提取到本地，使用桌面 mimikatz 工具提取 administrators 密码信息，将提取到的 hash 值作为 FLAG 提交；

B-2: Linux 操作系统渗透测试

任务环境说明：

- ✓ 服务器场景：Server2106（[关闭链接](#)）
 - ✓ 服务器场景操作系统：Linux（版本不详）
1. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景 /var/www 目录中唯一一个后缀为.bmp 文件的文件名称作为 Flag 值提交；

2. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景 /var/www 目录中唯一一个后缀为.bmp 的图片文件中的英文单词作为 Flag 值提交；
3. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景 /var/vsftpd 目录中唯一一个后缀为.docx 文件的文件名称作为 Flag 值提交；
4. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景 /var/vsftpd 目录中唯一一个后缀为.docx 文件的文件内容作为 Flag 值提交；
5. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景 /home/guest 目录中唯一一个后缀为.pdf 文件的文件名称作为 Flag 值提交；
6. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景 /home/guest 目录中唯一一个后缀为.pdf 文件的文件内容作为 Flag 值提交；
7. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景/root 目录中唯一一个后缀为.txt 文件的文件名称作为 Flag 值提交；
8. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景/root 目录中唯一一个后缀为.txt 文件的文件内容作为 Flag 值提交。

B-3: 数字取证调查

任务环境说明：

- ✓ 服务器场景：FTPServer220817
 - ✓ 服务器场景操作系统：未知（封闭靶机）
 - ✓ FTP 用户名:attack817 密码：attack817
1. 分析 attack.pcapng 数据包文件，通过分析数据包 attack.pcapng 找出恶意用户第一次访问 HTTP 服务的数据包是第几号，将该号数作为 Flag 值提交；
 2. 继续查看数据包文件 attack.pcapng，分析出恶意用户扫描了哪些端口，将全部的端口号从小到大作为 Flag 值（形式：端口 1, 端口 2, 端口 3..., 端口 n）提交；
 3. 继续查看数据包文件 attack.pcapng 分析出恶意用户登录后台所用的密码是什

么，将后台密码作为 Flag 值提交；

4. 继续查看数据包文件 `attack.pcapng` 分析出恶意用户写入的一句话木马的密码是什么，将一句话密码作为 Flag 值提交；
5. 继续查看数据包文件 `attack.pcapng` 分析出恶意用户下载了什么文件，将该文件内容作为 Flag 值提交。

B-4：网络安全事件响应

任务环境说明：

- ✓ 服务器场景：Server2216（[开放链接](#)）
- ✓ 用户名:root 密码：123456

1. 黑客通过网络攻入本地服务器，通过特殊手段在系统中建立了多个异常进程，找出启动异常进程的脚本，并将其绝对路径作为 Flag 值提交；
2. 黑客通过网络攻入本地服务器，通过特殊手段在系统中建立了多个异常进程，将恶意脚本的源文件所在的绝对路径作为 Flag 值提交；（多个路径之间以英文逗号分割，如： `/etc/proc, /etc/my.cnf`）
3. 黑客在服务器某处存放了多个木马程序，请你找到此木马程序并清除木马，将木马建立连接所使用的端口号作为 Flag 值提交；
4. 黑客通过网络攻入本地服务器，将黑客暴力破解服务器的次数作为 Flag 值提交；
5. 黑客攻入本地服务器，请你找出黑客成功暴力破解服务器的具体时间，将暴力破解的时间范围作为 Flag 值（提交的时间格式为：20220112 08:08:18-08:09:24）提交；
6. 黑客攻入本地服务器，请你找出黑客入侵服务器时所使用的 IP 地址，将 IP 地址作为 Flag 值（若存在多个 IP，IP 地址之间以英文逗号分割，如：10.1.1.1, 20.1.1.2）提交。

B-5: Web 安全绕过

任务环境说明:

- ✓ 服务器场景名称: Server2201 (关闭链接)
- ✓ 服务器场景操作系统: centos5.5

1. 使用渗透机场景 kali 中工具扫描服务器, 将服务器上 apache 版本号作为 flag 提交;
2. 使用渗透机场景 windows7 访问服务其场景中的网站 (网站路径为 IP/javascript), 找到网站首页中 flag 并提交;
3. 使用渗透机场景 windows7 根据第二题的入口继续访问服务器本题场景, 通过提示得到 flag 并提交;
4. 使用渗透机场景 windows7 根据第三题入口继续访问服务器的本题场景, 通过提示得到 flag 并提交;
5. 使用渗透机场景 windows7 根据第四题入口继续访问服务器的本题场景, 通过提示得到 flag 并提交;
6. 使用渗透机场景 windows7 根据第五题入口继续访问服务器的本题场景, 通过提示得到 flag 并提交;

(四) 模块 C CTF 夺旗-攻击

(本模块 200 分)

一、项目和任务描述:

假定你是某企业的网络安全渗透测试工程师, 负责企业某些服务器的安全防护, 为了更好的寻找企业网络中可能存在的各种问题和漏洞。你尝试利用各种攻击手段, 攻击特定靶机, 以便了解最新的攻击手段和技术, 了解网络黑客的心态, 从而改善您的防御策略。

请根据《赛场参数表》提供的信息, 在客户端使用谷歌浏览器登录答题平台。

二、操作系统环境说明：

客户机操作系统：Windows 10/Windows7

靶机服务器操作系统：Linux/Windows

三、漏洞情况说明：

1. 服务器中的漏洞可能是常规漏洞也可能是系统漏洞；
2. 靶机服务器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；
3. 靶机服务器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；
4. 靶机服务器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；
5. 操作系统提供的服务可能包含了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；
6. 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；
7. 操作系统中可能存在一些系统后门，选手可以找到此后门，并利用预留的后门直接获取到系统权限。

四、注意事项：

1. 不能对裁判服务器进行攻击，警告一次后若继续攻击将判令该参赛队离场；
2. flag 值为每台靶机服务器的唯一性标识，每台靶机服务器仅有 1 个；
3. 选手攻入靶机后不得对靶机进行关闭端口、修改密码、重启或者关闭靶机、删除或者修改 flag、建立不必要的文件等操作；
4. 在登录自动评分系统后，提交靶机服务器的 flag 值，同时需要指定靶机服务器的 IP 地址；
5. 赛场根据难度不同设有不同基础分值的靶机，对于每个靶机服务器，前三个获得 flag 值的参赛队在基础分上进行加分，本阶段每个队伍的总分均计入阶段得分，具体加分规则参照赛场评分标准；

6. 本环节不予补时。

（五）模块 D CTF 夺旗-防御

（本模块 200 分）

一、项目和任务描述：

假定各位选手是某安全企业的网络安全工程师，负责若干服务器的渗透测试与安全防护，这些服务器可能存在着各种问题和漏洞。你需要尽快对这些服务器进行渗透测试与安全防护。每个参赛队拥有专属的堡垒机服务器，其他队不能访问。参赛选手通过扫描、渗透测试等手段检测自己堡垒服务器中存在的安全缺陷，进行针对性加固，从而提升系统的安全防御性能。

请根据《赛场参数表》提供的信息，在客户端使用谷歌浏览器登录答题平台。

二、操作系统环境说明：

客户机操作系统：Windows 10/Windows7

堡垒服务器操作系统：Linux/Windows

三、漏洞情况说明：

1. 堡垒服务器中的漏洞可能是常规漏洞也可能是系统漏洞；
2. 堡垒服务器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；
3. 堡垒服务器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；
4. 堡垒服务器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；
5. 操作系统提供的服务可能包含了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；
6. 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；
7. 操作系统中可能存在一些系统后门，选手可以找到此后门，并利用预留的后门直

接获取到系统权限。

四、注意事项：

1. 每位选手需要对加固点和加固过程截图，并自行制作系统防御实施报告，最终评分以实施报告为准；

2. 系统加固时需要保证堡垒服务器对外提供服务的可用性；

3. 不能对裁判服务器进行攻击，警告一次后若继续攻击将判令该参赛队离场；

4. 本环节不予补时。

二、说明：

1. 所有截图要求截图界面、字体清晰；

2. 文件名命名及保存：网络安全模块 D-XX（XX 为工位号），PDF 格式保存；

3. 文件保存到 U 盘提交。