2023 年度“楚怡杯”湖南省职业院校技能竞赛
赛项规程

一、赛项名称

1. 赛项名称：网络安全

2. 赛项组别：中职组

3. 赛项归属：信息技术类

二、竞赛内容

1. 竞赛任务

本赛项由四个模块组成，每个模块根据赛题设有多个子任务。

模块 A: 基础设施设置与安全加固；

模块 B: 网络安全事件响应、数字取证调查和应用安全；

模块 C: CTF 夺旗-攻击；

模块 D: CTF 夺旗-防御。

2. 技术要求

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，具体考核的能力点如下：

1. 操作、维护、监督和管理
• 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。
2.保护和防御

• 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。
3.分析
• 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。
4.收集与操作
• 收集策略、技术及工具应用。 • 网络信息情报收集能力和资源库的利用。 • 信息需求和收集需求的转换、跟踪、优先排序。 • 网络运营计划方案、策略和有关资源。 • 网络运营策略、资源和工具。 • 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。
5.调查
• 威胁调查、报告、调查工具和法律、法规。 • 恶意软件分析的概念和方法。 • 收集、打包、传输和储存电子证据的过程，同时并维持监管链。 • 司法流程，包括事实陈述和证据。 • 持久性数据的类型和集合。 • 数字取证数据的类型和识别方法。 • 网络安全漏洞的具体操作性影响。

三、竞赛方式

2 人小组赛。

四、竞赛时量

竞赛时长为 180 分钟。竞赛时间安排：

模块编号	模块名称	竞赛时间（分钟）
A	基础设施设置与安全加固	90
B	网络安全事件响应、数字取证调查和应用安全	
C	CTF 夺旗-攻击	90
D	CTF 夺旗-防御	
总计		180

五、名次确定办法

按照总分从高至低排名，不设并列名次。如果总分相同，以模块 B 评判成绩高低排序;如果模块B评判成绩也相同,以模块B提交最后一个正确的 FALG 时间排序，先完成者排名靠前。

六、评分标准与评分细则

1. 评分标准（总分100分，各模块分值如下）

模块编号	模块名称	分值
A	基础设施设置与安全加固	20
B	网络安全事件响应、数字取证调查和应用安全	40
阶段切换		
C	CTF 夺旗-攻击	20
D	CTF 夺旗-防御	20
总计		100

2. 评分细则

模块编号	模块名称	模块任务	分值	评分方式
A	基础设施设置与安全加固	任务 1…N	20	根据每道题的具体分值客观评分。
B	网络安全事件响应、数字取证调查和应用安全	任务 1…N	40	机考评分。
C	CTF 夺旗-攻击	系统攻防演练	20	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。
D	CTF 夺旗-防御	系统攻防演练	20	根据选手答题内容，由评分裁判进行客观评分。

注意：选手严格按要求答题，不得以违规方式获取得分，不得攻击裁判服务器、网关、系统服务器等非靶机目标，如系统检测到选手有违规攻击行为，警告一次后，若该选手继续攻击，判令该队终止竞赛，清离赛场。

七、竞赛相关设施设备仪器清单

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	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 夺旗防御等知识和技能竞赛环境实现，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。 2. 标配 2 个千兆以太口，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 20 种以上不同级别的 70 个攻防场景；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。
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

（1）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：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（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

八、选手须知

1.选手自带工具及材料清单

选手无需自带工具

2.主要技术规范及要求

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》

3. 选手注意事项

（1）各选手要按照疫情防控要求做好个人和团队的防疫工作。

（2）各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。

（3）各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）各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。

（5）各选手须按要求规范操作竞赛设备。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。

（6）各选手须详细阅读赛题中文档命名的要求，不得在提交的文档中标识任何关于选手地名、校名、姓名、参赛编号等信息，否则取消竞赛成绩。

（7）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，经工作人员清点后方可离开赛场且不得带走任何资料。

（8）在竞赛期间，未经执委会批准，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。各选手不得将竞赛的相关信息私自公布。

（9）选手若对竞赛过程有异议，在规定的时间内经由领队向赛项仲裁工作组提出书面报告。

4. 竞赛直播

赛点全程无死角监控记录比赛情况，并可在指定区域通过监控观看比赛实况。

九、样题（竞赛任务书）

2023 年度湖南省职业院校技能大赛（中职组）
网络安全竞赛样题
（总分 100 分）

赛题说明

一、竞赛项目简介

“网络安全”竞赛共分 A、B、C、D 四个模块。根据比赛实际情况，竞赛赛场实际使用赛题参数、表述及环境可能有适当修改，具体情况以实际比赛发放赛题为准。竞赛时间安排和分值权重见表。

竞赛时间安排与分值权重表

模块编号	模块名称	竞赛时间（分钟）	分值
A	基础设施设置与安全加固	90	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	90	20
D	CTF 夺旗-防御		20
总计		180	100

二、竞赛注意事项

1.比赛期间禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

2.请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

3.在进行任何操作之前，请阅读每个部分的所有任务。各任务之间可能存在一定关联。

4.操作过程中需要及时按照答题要求保存相关结果。比赛结束后，所有设备

保持运行状态，评判以最后提交的成果为最终依据。

5.比赛完成后，比赛设备、软件和赛题请保留在座位上。禁止将比赛所用的所有物品（包括试卷）带离赛场。

6.禁止在提交资料上填写与竞赛无关的标记。如违反规定，可视为0分。

7.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。

竞赛内容

模块A 基础设施设置与安全加固

（本模块20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、数据库安全策略、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

Windows　用户名：administrator，密码：123456

Linux　　用户名：root，密码：123456

三、提交任务说明

本模块要求对具体任务的操作截图并加以相应的文字说明,以word文档的形式书写,以PDF格式保存,以网络安全模块A-XX（XX为工位号）作为文件名。

四、具体任务

A-1任务一 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.最小密码长度不少于16个字符。

2.登录策略（Windows, Linux）

a.在用户登录系统时，应该有“For authorized users only”提示信息；

b.远程用户非活动会话连接超时应小于等于5分钟。

3.用户安全管理(Windows)

a.设置user1用户只能在上班时间(周一至周五的9:00~18:00)可以登录，将user1的登录时间配置界面截图；

b.在组策略中只允许管理员账号从网络访问本机。

A-2 任务二 数据库加固（Linux）

4.以普通帐户mysql安全运行mysql服务，禁止mysql以管理员帐号权限运行

5.删除默认数据库(test)

6.改变默认mysql管理员用户为:SuperRoot

7.使用mysql内置MD5加密函数加密用户user1的密码为(P@sswOrd1!)

8.赋予user1用户对数据库所有表只有select,insert,delete,update权限

A-3 任务三 流量完整性保护（Windows）

9.对 Web 网站进行 HTTP 重定向 HTTPS 设置，仅使用 HTTPS 协议访问网站（Windows）(注：证书颁发给 test.com 并通过 https://www.test.com 访问 Web 网站)

模块 B 网络安全事件响应、数字取证调查和应用安全

（本模块 40 分，每个任务 8 分）

一、项目和任务描述：

假定你是某网络安全技术支持团队成员，某企业的服务器系统被黑客攻击，你的团队前来帮助企业进行调查并追踪本次网络攻击的源头，分析黑客的攻击方式，发现系统漏洞，提交网络安全事件响应报告，修复系统漏洞，删除黑客在系统中创建的后门，并帮助系统恢复正常运行。

二、服务器环境参考（以实际赛题为准）

操作系统：Windows/Linux。

三、PC 机环境参考（以实际赛题为准）

物理机：Windows7 或 Windows10

虚拟机 1：Kali（用户名：root；密码：toor）

虚拟机 2：Windows7（用户名：administrator；密码：123456）

四、具体任务

B-1 任务一 流量分析

任务说明：仅能获取 Server2 的 IP 地址

1.使用 Wireshark 查看并分析 Server2 桌面下的 capture.pcapng 数据包文件，找出黑客获取到的可成功登录目标服务器 FTP 服务的账号密码，并将黑客获取到的账号密码作为 Flag 值（用户名与密码之间以英文逗号分隔，例如：root,toor）提交；

2.继续分析 capture.pcapng 数据包文件，找出黑客使用获取到的账号密码登录 FTP 服务的时间，并将黑客登录 FTP 的时间作为 Flag 值（例如：14:22:08）提交；

3.继续分析 capture.pcapng 数据包文件，找出黑客成功登录 FTP 服务后执行的第一条命令，并将执行的命令作为 Flag 值提交;

4.继续分析 capture.pcapng 数据包文件，找出黑客成功登录 FTP 服务后下载的关键文件，并将下载的文件名称作为 Flag 值提交；

5.继续分析 capture.pcapng 数据包文件，找出黑客成功登录 FTP 服务后下载的关键文件，并将下载的文件内容作为 Flag 值提交。

B-2 任务二 渗透测试

任务说明：仅能获取 Server3 的 IP 地址

1.通过本地 PC 中渗透测试平台 Kali 对靶机场景 Server3 进行系统服务及版本扫描渗透测试，以 xml 格式向指定文件输出信息（使用工具 Nmap），将以 xml 格式向指定文件输出信息必须要使用的参数作为 Flag 值提交；

2.在本地 PC 的渗透测试平台 Kali 中，使用命令初始化 MSF 数据库并将此命令作为 Flag 值提交；

3.在本地 PC 的渗透测试平台 Kali 中，打开 MSF，使用 db_import 将扫描结果导入到数据库中，并查看导入的数据，将查看该数据要使用的命令作为 Flag 值提交；

4.在 MSF 工具中用 search 命令搜索 CVE-2019-0708 漏洞利用模块，将回显结果中的漏洞公开时间作为 Flag 值（如：2017-10-16）提交；

5.在 MSF 工具中调用 CVE-2019-0708 漏洞攻击模块，并检测靶机是否存在漏洞，将回显结果中最后一个单词作为 Flag 值提交。

B-3 任务三 Python 代码分析

任务说明：仅能获取 Server4 的 IP 地址,Server4 FTP 服务用户名：user，密码：123456

1.完善 Flag1.py 文件，填写该文件当中空缺的 Flag1 字符串，并将该字符串作为 Flag 值提交；

2.完善 Flag1.py 文件，填写该文件当中空缺的 Flag2 字符串，并将该字符串作为 Flag 值提交；

3.完善 Flag1.py 文件，填写该文件当中空缺的 Flag3 字符串，并将该字符串作为 Flag 值提交；

4.完善 Flag1.py 文件，填写该文件当中空缺的 Flag4 字符串，并将该字符串作为 Flag 值提交；

5.将完善好的脚本文件执行，将执行成功后的回显内容作为 Flag 值提交。

B-4 任务四 隐写术应用

任务说明：Server5 用户名：administrator，密码：123456

1.找出文件夹 1 中的文件，将文件中的隐藏信息作为 Flag 值提交；

2.找出文件夹 2 中的文件，将文件中的隐藏信息作为 Flag 值提交；

3.找出文件夹 3 中的文件，将文件中的隐藏信息作为 Flag 值提交；

4.找出文件夹 4 中的文件，将文件中的隐藏信息作为 Flag 值提交；

5.找出文件夹 5 中的文件，将文件中的隐藏信息作为 Flag 值提交。

B-5 任务五 Web 安全应用

任务说明：仅能获取 Server6 的 IP 地址

1.通过 URL 访问 http://靶机 IP/1，对该页面进行渗透测试,找到 Flag1 作为 Flag 值提交；

2.通过 URL 访问 http://靶机 IP/2，对该页面进行渗透测试，找到 Flag2 作为 Flag 值提交；

3.通过 URL 访问 http://靶机 IP/3，对该页面进行渗透测试，找到 Flag3 作为 Flag 值提交；

4.通过 URL 访问 http://靶机 IP/4，对该页面进行渗透测试，找到 Flag4 作为 Flag 值提交；

5.通过 URL 访问 http://靶机 IP/5，对该页面进行渗透测试，找到 Flag5 作为 Flag 值提交。

模块 C CTF 夺旗-攻击

（本模块 20 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、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。

模块 D　CTF 夺旗-防御

（本模块 20 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需要答题平台。

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、注意事项

1.每位选手需要对加固点和加固过程截图，所有截图要求截图界面、字体清晰，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；

5.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；

6.文件保存到 U 盘提交。