**2019年全国职业院校技能大赛**

**赛项规程**

# 一、赛项名称

赛项编号：ZZ-2019024

赛项名称：网络空间安全

英文名称：[Cyberspace Security](http://www.baidu.com/link?url=Ltb-4t1FNAs7ZPE6xtBnVYCgbAb-538XHRCKjaCuJRg5urKbS0R2HQWwtRjzqW6_5TWgxixiDaVIqbwDE2E0OHejjwXEgTCBXWAi_qxQguuYy2FVw5RNy3Pcanpmcg-_)

赛项组别：中职组

赛项归属：信息技术类

# 二、竞赛目的

网络空间安全已经上升到国家安全的战略高度，得到社会各界的广泛重视，信息安全产业发展进入快车道。通过本竞赛，可检验参赛选手对网络、服务器系统等网络空间中各个信息系统的安全防护能力，以及分析、处理现场问题的能力，培养更多学生掌握网络安全知识与技能，发展成为国家信息安全领域的技术技能人才。引导中等职业学校关注网络安全技术发展趋势和产业应用方向，促进网络信息安全专业建设与教学改革。本赛项赛项紧密结合新一代信息产业发展对网络安全应用型人才的需求，促进校企合作、产教融合，增强中职学校学生的新技术学习能力和就业竞争力，助力新一代信息技术产业快速发展，是践行“以赛促学、以赛促教、以赛促改、以赛促创”的成功实践。

# 三、竞赛内容

重点考核参赛选手网络系统安全策略部署、信息保护、网络安全运维管理的综合实践能力，具体包括：

1.参赛选手能够在赛项提供的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，以满足应用需求。

2.参赛选手能够根据赛项要求，实施网络空间安全防护操作。

3.参赛选手能够根据网络实际运行中面临的安全威胁，确定安全策略并部署实施，防范并制止网络恶意入侵和攻击行为。

4.参赛选手通过分组混合对抗的形式，能够实时防护自己服务器，抵御外界的攻击，同时能够对目标进行渗透测试。

5.竞赛总时长为3个小时，各竞赛阶段安排如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容模块** | **具体内容** | **说明** |
| 第一阶段 | 单兵模式系统渗透测试 | 密码学和VPN | 密码学、IPSec VPN、IKE：PreShared Key（预共享密钥认证）、IKE：PKI（公钥架构认证）、SSL VPN等。 |
| 操作系统渗透测试及加固 | Windows操作系统渗透测试及加固、Linux操作系统渗透测试及加固等。 |
| Web应用渗透测试及加固 | SQL Injection（SQL注入）漏洞渗透测试及加固、Command Injection（命令注入）漏洞渗透测试及加固、File Upload（文件上传）漏洞渗透测试及加固、Directory Traversing（目录穿越）漏洞渗透测试及加固、XSS（Cross Site Script）漏洞渗透测试及加固、CSRF（Cross Site Request Forgeries）漏洞渗透测试及加固、Session Hijacking（会话劫持）漏洞渗透测试及加固 |
| 网络安全数据分析 | 能够利用日志收集和分析工具对网络流量收集监控，维护网络安全。 |
| 常用渗透扫描工具使用与脚本语言应用 | 能够利用如Nmap、Nessus、metasploit等常用渗透扫描工具进行信息收集及系统渗透；熟悉shell，Python等脚本语言的应用。 |
| 第二阶段 | 攻防对抗 | 参赛队之间进行对抗演练 | Windows/Linux操作系统安全攻防、Web应用/数据库安全攻防等。 |

6.竞赛分值权重和时间安排

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容模块** | **分值权重** | **阶段时间** |
| 第一阶段 | 单兵模式系统渗透测试 | 70% | 100分钟 |
| 备战阶段 | 攻防对抗准备工作 | 0% | 20分钟 |
| 第二阶段 | 攻防对抗 | 30% | 60分钟 |

# 四、竞赛方式

1.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，每个参赛队限报2名指导教师。

2.本赛项正在与国际参赛队接洽，同时欢迎国内外团队及选手到场观赛。

# 五、竞赛流程

（一）竞赛流程图

（二）竞赛时间表

比赛限定在1天内进行，比赛场次为1场，赛项竞赛时间为3小时，时间为9:00-12:00，具体安排如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **日期** | **时间** | **事项** | **参加人员** | **地点** |
| 赛前2日 | 20:00前 | 裁判、仲裁、监督报到 | 工作人员 | 住宿酒店 |
| 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、监督组 | 竞赛场地 |
| 16:00 | 返回酒店 | 参赛领队 | 竞赛场地 |
| 竞赛当天 | 07:30 | 裁判就位 | 裁判 | 竞赛场地 |
| 07:30-08:00 | 选手抽签，一次加密 | 参赛选手、裁判 | 竞赛场地 |
| 08:00-08:30 | 选手抽签，二次加密及入场 | 参赛选手、裁判 | 竞赛场地 |
| 08:30-08:40 | 参赛选手就位，宣读考场纪律 | 参赛选手、裁判 | 竞赛场地 |
| 08:40-09:00 | 设备检查、第一阶段赛题发放 | 参赛选手、裁判 | 竞赛场地 |
| 09:00-10:40 | 第一阶段比赛时间 | 参赛选手、裁判 | 竞赛场地 |
| 10:40-11:00 | 第二阶段赛题发放、攻防准备 | 参赛选手、裁判 | 竞赛场地 |
| 11:00-12:00 | 第二阶段比赛时间 | 参赛选手、裁判 | 竞赛场地 |
| 12:00 | 比赛正式结束 | 参赛选手、裁判 | 竞赛场地 |
| 12:30-16:30 | 成绩核查、解密、确认 | 裁判长、监督 | 竞赛场地 |
| 16:30-18:30 | 成绩公布，成绩汇总报送 | 裁判长、监督 | 竞赛场地 |
| 赛后1日 | 9：00-11：00 | 闭幕式 | 领导、嘉宾、裁判、各参赛队 | 会议室 |

# 六、竞赛赛卷

（一）赛项执委会专家组下设的命题组负责本赛项命题工作。

（二）本赛项赛卷公开，竞赛赛卷距国赛开始日前一个月公开。

（三）本赛项通过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）公布竞赛赛卷。

赛卷样题见附件。

# 七、竞赛规则

（一）报名资格

参赛选手须为2019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）在籍学生可参加比赛。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2019年5月1日为准。

（二）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。

（三）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。

（四）参赛选手自行决定工作程序和时间安排。

（五）参赛选手在赛前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。

（六）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。

（七）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。

（八）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，以纸质形式向全体参赛队进行公布，并在闭赛式上予以宣布。

（九）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。

（十）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。

（十一）赛项每个比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。

# 八、竞赛环境

1.竞赛场地。竞赛现场设置竞赛区、裁判区、服务区、技术支持区。现场保证良好的采光、照明和通风；提供稳定的水、电和供电应急设备。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比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。竞赛现场各个工作区配备单相220V/3A以上交流电源。每个比赛工位上标明编号。配备2把工作椅（凳）。

4.技术支持区为参赛选手比赛提供网络环境部署和网络安全防范。

5.服务区提供医疗等服务保障。

6.竞赛工位隔离和抗干扰。竞赛工位之间标有隔离线。

# 九、技术规范

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7项国家标准，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》 |

# 十、技术平台

（一）比赛器材

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **设备型号** |
| 1 | 网络空间安全技能评测平台 | 1 | 中科软磐云系列网络空间安全实战平台PY-B7，磐云PY-B7为1U设备，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，支持多用户并发在线比赛，根据不同的实战任务下发进行自动调度靶机虚拟化模板，为学员提供单兵闯关、分组混战等实际对战模式，提供超过20种不同级别70个的攻防题目。整个过程全自动评判，自定义动画态势展示，成绩详细分析，多端口监控，全程加密。包含往年网络空间安全国赛和省赛部分样题场景。 |
| 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。 |

（二）软件技术平台：

比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。

2．虚拟机安装操作系统：

 Windows系统（试用版）：Windows XP、Windows 7、Windows2003 Server、Windows2008 Server（根据命题确定）。

 Linux系统：Ubuntu、Debian、CentOS（根据命题确定）。

3.其他主要应用软件为:

VMware workstation 12 pro 免费版

Putty 0.67

Python 3

Chrome 浏览器 62.0

RealVNC 客户端 4.6

JDK（Java Development Kit）7.0

# 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，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。

本赛项拟设裁判18名。

因为本赛项全部分数由计算机自动评分，因此只需进行两次加密，加密后参赛选手中途不得擅自离开赛场。分别由2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。

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

裁判组监督现场机考评分，由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。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）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** |
| 第一阶段权重70% | 单兵模式系统渗透测试（本阶段由多个任务组成） | 任务1 | 机考评分 |
| 任务2 | 机考评分 |
| …… | 机考评分 |
| 任务N | 机考评分 |
| 第二阶段权重30% | 分组对抗 | 系统攻防演练 | 机考评分 |

选手向考评服务器中提交每道赛题唯一的“KEY”值或“FLAG”值，所有得分由计算机自动评判，参赛队的得分等于队中两位参赛选手的得分总和。

2.第一阶段评分规则

第一阶段总分为700分,分为N个任务，每道题的具体分值在赛题中标明；系统自动评分和排名，公开显示在外接大屏幕上。

3.第二阶段评分规则

第二阶段总分为300分，初始分为100分；每提交1次对手靶机的FLAG值得分，每当被对手提交1次自身靶机的FLAG值扣分，每个对手靶机的FLAG值只能提交一次，得分和扣分的具体分值在赛题中标明。

系统自动启动违规检测和扣分机制，如发现如下违规行为，系统均给予自动扣分，每检测到一次违规行为扣除一次分数，扣分明细显示在扣分榜中，记录在第二阶段总成绩中：

（1）启用FLAG检测机制，如发现FLAG异常（譬如：删除、修改、杀进程），记为一次违规行为；

（2）启用服务端口检测机制，如发现关闭赛题中要求开启的端口，记为一次违规行为；

（3）靶机服务器IP参数为DHCP自动获取，不允许自行修改，如修改触发上述（1）和（2）检测机制；

（4）在加固时间后，选手自己关闭靶机或被他人关闭，触发上述（1）和（2）检测机制，且裁判员不予帮助重启；

（5）违反题目中规定的其他违规操作等（参考赛题）。

# 十二、奖项设定

本赛项为团队赛，依照实际参赛队数量确定奖项：一等奖占参赛队总数的10%，二等奖占参赛队总数的20%，三等奖占参赛队总数的30%。

获得一等奖参赛队的指导教师获“优秀指导教师奖”，授予荣誉证书。

# 十三、赛场预案

为保障赛项顺利进行，避免竞赛过程中不可控但可能出现的紧急情况，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。

1. 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，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电源可支持约20-30分钟。

# 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。

1. 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。制定相应安全管理的规范、流程和突发事件应急预案，及时处置突发事件，全过程保证比赛筹备和实施工作安全。

1. 赛项设计

1.比赛内容涉及的器材、设备应符合国家有关安全规定。赛项专家组应充分考虑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应在赛项技术文件中加以明确。

2.赛项技术文件应包含国家（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.赛项执委会须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。源于实际生产过程的赛项，须根据《中华人民共和国劳动法》等法律法规，建立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.赛项执委会须制定专门方案保证比赛命题、赛题保管和评判过程的安全。

1. 比赛环境

1.环境安全保障

赛场组织与管理员应制定安保须知、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。后备时间：2小时；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，确认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。

参赛选手旅途及竞赛过程中的安全保障由各省市负责。

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。如有必要，也可进行赛场仿真模拟测试，以发现可能出现的问题。承办单位赛前须按照赛项执委会要求排除安全隐患。

5.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。

6.承办单位应提供保证应急预案实施的条件。对于内容涉及高空作业、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。

7.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。

8.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。

9.参赛选手进入赛位、赛事裁判工作人员进入工作场所，严禁携带通讯、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。

1. 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。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.大赛期间组织的参观和观摩活动，由赛区组委会负责。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。

1. 组队责任

1.各省、自治区、直辖市和计划单列市在组织参赛时，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、直辖市和计划单列市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.各参赛选手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。

1. 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。

1. 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.因参赛选手原因造成重大安全事故的，取消其参赛资格。

3.参赛选手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、计划单列市、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.各参赛选手要发扬良好道德风尚，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。

（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）领队向赛区仲裁委员会提出申诉。赛区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，使用大屏幕实时展示网络空间安全竞技过程。

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。竞赛过程采用实况转播的形式，对比赛的开闭幕式、比赛过程全程摄录。

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《2019年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，赛项执委会赛后内向大赛执委会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 | 电子教材 | 赛后180天 |
| 技能训练指导书 | 文本资料 | 1 | 电子教材 | 赛后180天 |
| 大赛作品集 | 文本资料 | 1 | 电子版资料 | 赛后180天 |
| 技能操作规程 | 文本资料 | 1 | 电子版资料 | 赛后180天 |
| 拓展资源 | 案例库 | 文本资料 | 1 | 电子版资料 | 赛后60天 |
| 素材资源库 | 仿真课件 | 1 | 电子版资料 | 赛后180天 |
| 赛题库 | 文本资料 | 1 | 电子版资料 | 赛后60天 |
| 衍生成果 | 文本资料 | 1 | 电子版资料 | 赛后180天 |
| 访谈视频 | 视频 | 1 | 10分钟以上 | 赛后60天 |

赛后还需加强师资队伍建设，促进资源转化成果能够在教学中有效应用。2019年大赛完毕后计划进行9场活动：1期赛项总结会，4期专业建设研讨会，以及4期师资培训。

|  |  |  |
| --- | --- | --- |
| **序号** | **活动名称** | **计划时间** |
| 1 | 赛项总结会和资源转化会议 | 2019年7月 |
| 2 | 专业建设研讨会第1期 | 2019年6月 |
| 3 | 专业建设研讨会第2期 | 2019年9月 |
| 4 | 专业建设研讨会第3期 | 2019年10月 |
| 5 | 专业建设研讨会第4期 | 2019年11月 |
| 6 | 师资培训第1期 | 2019年7月中旬 |
| 7 | 师资培训第2期 | 2019年7月下旬 |
| 8 | 师资培训第3期 | 2019年8月上旬 |
| 9 | 师资培训第4期 | 2019年8月中旬 |

# 附件：样题

**中职组“网络空间安全”赛项样题**

一、竞赛阶段简介

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **竞赛阶段** | **任务阶段** | **竞赛任务** | **竞赛时间** | **分值** |
| 第一阶段单兵模式系统渗透测试 | 任务1 | MSSQL数据库渗透测试 | 100分钟 | 100 |
| 任务2 | 主机发现与信息收集 | 100 |
| 任务3 | SNMP信息收集与利用 | 100 |
| 任务4 | Windows操作系统渗透测试 | 100 |
| 任务5 | Linux操作系统渗透测试 | 100 |
| 任务6 | 网络协议堆栈渗透测试 | 100 |
| 任务7 | Web应用程序渗透测试及安全加固 | 100 |
| 备战阶段 | 攻防对抗准备工作 | 20分钟 | 0 |
| 第二阶段分组对抗 | 系统加固：15分钟 | 60分钟 | 300 |
| 渗透测试：45分钟 |

二、拓扑图

三、竞赛任务书

（一）第一阶段任务书（700分）

**任务1. MSSQL数据库渗透测试（100分）**

**任务环境说明：**

* 服务器场景：server2003（用户名：administrator；密码：空）
* 服务器场景操作系统：Windows server2003

1.在本地PC渗透测试平台BT5中使用zenmap工具扫描服务器场景server2003所在网段(例如：172.16.101.0/24)范围内存活的主机IP地址和指定开放的1433、3306、80端口。并将该操作使用的命令中必须要使用的字符串作为FLAG提交；（10分）

2.通过本地PC中渗透测试平台BT5对服务器场景server2003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数据库服务对应的服务端口信息作为FLAG提交；（10分）

3.在本地PC渗透测试平台BT5中使用MSF中模块对其爆破，使用search命令，并将扫描弱口令模块的名称作为FLAG提交；（10分）

4.在上一题的基础上使用命令调用该模块，并查看需要配置的信息（使用show options命令），将回显中需要配置的目标地址,密码使用的猜解字典,线程,账户配置参数的字段作为FLAG提交（之间以英文逗号分隔，例hello,test，..,..）；（10分）

5.在msf模块中配置目标靶机IP地址，将配置命令中的前两个单词作为FLAG提交；（10分）

6.在msf模块中指定密码字典，字典路径为/root/2.txt爆破获取密码并将得到的密码作为FLAG提交；（14分）

7.在msf模块中切换新的渗透模块，对服务器场景server2003进行数据库服务扩展存储过程进行利用，将调用该模块的命令作为FLAG提交；（14分）

8.在上一题的基础上，使用第6题获取到的密码并进行提权，同时使用show options命令查看需要的配置，并配置CMD参数来查看系统用户，将配置的命令作为FLAG提交；（14分）

9.在利用msf模块获取系统权限并查看目标系统的异常（黑客）用户，并将该用户作为FLAG提交。（8分）

**任务2. 主机发现与信息收集（100分）**

**任务环境说明：**

* 服务器场景：server2003（用户名：administrator；密码：空）
* 服务器场景操作系统：Windows server2003

1.通过本地PC中渗透测试平台BT5使用fping对服务器场景server2003所在网段(例如：172.16.101.0/24)进行主机发现扫描,并将该操作使用的命令中必须要使用的参数作为FLAG提交；（12分）

2.通过本地PC中渗透测试平台BT5使用genlist对服务器场景server2003所在网段进行扫描进行主机存活发现, 并将该操作使用的命令中必须要使用的参数作为FLAG提交；（12分）

3.在通过本地PC中渗透测试平台BT5使用nbtscan对服务器场景server2003所在网段进搜索扫描，获取目标的MAC地址等信息，并将该操作使用的命令中必须要使用的参数作为FLAG提交；（12分）

4.假设服务器场景server2003设置了防火墙无法进行ping检测，通过PC中渗透测试平台BT5使用arping检测主机连通性扫描（发送请求数据包数量为4个），并将该操作使用的命令中固定不变的字符串作为FLAG提交；（12分）

5.通过本地PC中渗透测试平台BT5使用fping对服务器场景server2003所在网段进行存活性扫描，且要把最终扫描的存活主机输出到文件ip.txt中，并将该操作使用的命令中必须要使用的参数作为FLAG提交（各参数之间用英文逗号分割，例a,b）；（12分）

6.通过本地PC中渗透测试平台BT5使用nbtscan从第5题的ip.txt文件中读取IP扫描主机信息MAC地址等信息，并将该操作使用的命令中固定不变的字符串作为FLAG提交；（12分）

7.通过本地PC中渗透测试平台BT5使用xprobe2对服务器场景server2003进行TCP扫描，仅扫描靶机80,3306端口的开放情况(端口之间以英文格式下逗号分隔)，并将该操作使用的命令中固定不变的字符串作为FLAG提交；（12分）

8.通过本地PC中渗透测试平台BT5使用xprobe2对服务器场景server2003进行UDP扫描，仅扫描靶机161,162端口的开放情况(端口之间以英文格式下逗号分隔)，并将该操作使用的命令中固定不变的字符串作为FLAG提交。（16分）

**任务3. SNMP信息收集与利用（100分）**

**任务环境说明：**

* 服务器场景：server2003（用户名：administrator；密码：空）
* 服务器场景操作系统：Windows server2003

1.在本地PC渗透测试平台BT5中使用autoscan工具扫描服务器场景server2003所在网段(例如：172.16.101.0/24)范围内存活的主机地址。判断存活主机是否开放网络管理服务，若开启则以扫描出开启SNMP服务的主机名作为FLAG提交；（11分）

2.在本地PC渗透测试平台BT5中使用nmap工具进行UDP扫描服务器场景server2003所在网段范围内存活的主机地址，判断网络管理服务的开放情况，若开启，则以扫描出SNMP开放的端口号作为FLAG（各端口之间用英文分号分割，例21;23），若未开放则提交none作为FLAG；（11分）

3.在本地PC渗透测试平台BT5中调用snmpwalk工具测试服务器场景server2003是否开启Windows SNMP服务（共同体为默认字符串为public，通过对目标靶机的.1.3.6.1.2.1.25.1.6分支进行snmpwalk来测试服务的开放情况（SNMP 版本为v2c），并将该操作使用的命令中必须要使用的参数作为FLAG提交（各参数之间用英文分号分割，例a;b）；（11分）

4.在本地PC渗透测试平台BT5中使用ADMsnmp工具尝试猜解团体字符串，并将使用的全部命令作为FLAG提交（提交答案时IP以192.168.100.10代替,使用默认字典snmp.passwd）；（11分）

5.更换使用onesixtyone工具执行命令查看帮助选项，并将输入的命令作为FLAG提交；（11分）

6.在本地PC渗透测试平台BT5中使用onesixtyone对靶机SNMP进行团体字符串猜解，并将使用的全部命令作为FLAG提交（提交的命令为忽略IP后必须使用的命令，字典名字为dict.txt）；（11分）

7.在本地PC渗透测试平台BT5中对猜解结果进行查看，将回显中猜解的团体字符串作为FLAG提交；（11分）

8.在本地PC渗透测试平台BT5中选择新的SNMP攻击模块snmpcheck，根据得到的public团体字符串并利用snmpcheck进行对靶机的信息收集，并将该操作使用的命令中必须使用的参数作为FLAG提交；（11分）

9.查看获取的系统信息，将系统管理员用户和异常（黑客）用户作为FLAG提交，（各用户之间用英文分号分割，例root;user）。（12分）

**任务4. Windows操作系统渗透测试（100分）**

**任务环境说明：**

* 服务器场景：PYsystem4
* 服务器场景操作系统：Windows（版本不详）

1.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行操作系统扫描渗透测试，并将该操作显示结果“Running：”之后的字符串作为FLAG提交；（6分）

2.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4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445端口对应的服务版本信息字符串作为FLAG提交；（6分）

3.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行渗透测试，将该场景网络连接信息中的DNS信息作为FLAG提交;(例如114.114.114.114)（13分）

4.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行渗透测试，将该场景桌面上111文件夹中唯一一个后缀为.docx文件的文件名称作为FLAG提交；（14分）

5.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行渗透测试，将该场景桌面上111文件夹中唯一一个后缀为.docx文件的文档内容作为FLAG提交；（16分）

6.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行渗透测试，将该场景桌面上222文件夹中唯一一个图片中的英文单词作为FLAG提交；（15分）

7.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行渗透测试，将该场景中的当前最高账户管理员的密码作为FLAG提交；（10分）

8.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行渗透测试，将该场景中回收站内文件的文档内容作为FLAG提交。（20分）

**任务5. Linux操作系统渗透测试（100分）**

**任务环境说明：**

* 服务器场景：PYsystem5
* 服务器场景操作系统：未知

1.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行操作系统扫描渗透测试，并将该操作显示结果“OS Details：”之后的字符串作为FLAG提交；（6分）

2.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5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MySQL数据库对应的服务版本信息字符串作为FLAG提交；（6分）

3.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行渗透测试，将该场景/var/www/html目录中唯一一个后缀为.html文件的文件名称作为FLAG提交；（12分）

4.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行渗透测试，将该场景/var/www/html目录中唯一一个后缀为.html文件的文件内容作为FLAG提交；（16分）

5.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行渗透测试，将该场景/root目录中唯一一个后缀为.bmp文件的文件名称作为FLAG提交；（27分）

6.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行渗透测试，将该场景/root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提交。（33分）

**任务6. 网络协议堆栈渗透测试（100分）**

**任务环境说明：**

服务器场景：WindowsServer18065

服务器场景操作系统：Windows2003 Server

服务器场景FTP下载服务用户名：anonymous，密码：123456

服务器场景FTP下载服务端口：2121

1.通过物理机的ping程序访问靶机，成功访问后，在攻击机中使用arpspoof程序对物理机进行ARP渗透测试，对物理机进行ARP缓存毒化为：靶机IP地址映射攻击机MAC地址；从靶机服务器场景的FTP服务器中下载文件arpspoof.py，编辑该Python3程序文件，使该程序实现同本任务中arpspoof程序一致的功能，填写该文件当中空缺的F1字符串，将该字符串作为Flag值提交；（9分）

2.继续编辑该Python3程序文件，使该程序实现同本任务题1中arpspoof程序一致的功能，填写该文件当中空缺的F2字符串，将该字符串作为Flag值提交；（9分）

3.继续编辑该Python3程序文件，使该程序实现同本任务题1中arpspoof程序一致的功能，填写该文件当中空缺的F3字符串，将该字符串作为Flag值提交；（9分）

4.继续编辑该Python3程序文件，使该程序实现同本任务题1中arpspoof程序一致的功能，填写该文件当中空缺的F4字符串，将该字符串作为Flag值提交；（9分）

5.继续编辑该Python3程序文件，使该程序实现同本任务题1中arpspoof程序一致的功能，填写该文件当中空缺的F5字符串，将该字符串作为Flag值提交；（9分）

6.继续从靶机服务器场景FTP服务器中下载文件icmpflood.py，编辑该Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F6字符串，将该字符串作为Flag值提交；（9分）

7.继续编辑命名为icmpflood.py的Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F7字符串，将该字符串作为Flag值提交；（9分）

8.继续编辑命名为icmpflood.py的Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F8字符串，将该字符串作为Flag值提交；（9分）

9.继续编辑命名为icmpflood.py的Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F9字符串，将该字符串作为Flag值提交；（9分）

10.继续编辑命名为icmpflood.py的Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F10字符串，将该字符串作为Flag值提交；（9分）

11. 在本地PC渗透测试平台BT5中通过Python3程序解释器执行程序文件icmpflood.py，并打开WireShark监听网络流量，分析通过程序文件icmpflood.py产生的ICMP流量，并将该ICMP数据对象中的Code属性值通过MD5运算后返回的哈希值的十六进制结果的字符串作为Flag值提交。（10分）

**任务7. Web应用程序渗透测试及安全加固（100分）**

**任务环境说明：**

服务器场景：WindowsServer18065

服务器场景操作系统：Windows2003 Server

服务器场景FTP下载服务用户名：anonymous，密码：123456

服务器场景FTP下载服务端口：2121

服务器场景FTP上传服务用户名：anonymous，密码：123456

服务器场景FTP上传服务端口：21

1.在攻击机端通过浏览器访问主页http://靶机IP地址，通过Web应用程序渗透测试方法登陆磐石公司模拟产品网站，成功登陆后，将Web页面弹出的字符串通过SHA256运算后返回哈希值的十六进制结果的字符串作为Flag值提交；（7分）

2.从靶机服务器场景FTP服务器中下载文件loginauthentic.php，编辑该PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F11字符串，将该字符串作为Flag值提交；（7分）

3.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F12字符串，将该字符串作为Flag值提交；（7分）

4.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F13字符串，将该字符串作为Flag值提交；（7分）

5.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F14字符串，将该字符串作为Flag值提交；（7分）

6.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F15字符串，将该字符串作为Flag值提交；（7分）

7.将编辑好后的loginauthentic.php程序文件上传至靶机FTP服务，在攻击机端通过浏览器访问主页http://靶机IP地址，通过本任务第1题所使用的Web应用程序渗透测试方法登陆磐石公司模拟产品网站，将此时Web页面弹出的字符串通过SHA256运算后返回的哈希值的十六进制结果的字符串作为Flag值提交；（7分）

8.成功登陆磐石公司模拟产品网站后，继续点击超链接进入磐石公司产品信息页面，通过Web应用程序渗透测试方法获得靶机根路径下的文件flaginfo中的字符串，并将该字符串通过SHA256运算后返回哈希值的十六进制结果的字符串作为Flag值提交；（8分）

9.从靶机服务器场景FTP服务器中下载文件product.php，编辑该PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F16字符串，将该字符串作为Flag值提交；（7分）

10.继续编辑本任务第9题中的PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F17字符串，将该字符串作为Flag值提交；（7分）

11.继续编辑本任务第9题中的PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F18字符串，将该字符串作为Flag值提交；（7分）

12.继续编辑本任务第9题中的PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F19字符串，将该字符串作为Flag值提交；（7分）

13.继续编辑本任务第9题中的PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F20字符串，将该字符串作为Flag值提交；（7分）

14.将编辑好后的product.php程序文件上传至靶机FTP服务，并在攻击机端通过本任务第8题中使用的Web应用程序渗透测试方法获得靶机根路径下的文件flaginfo中的字符串，将此时Web页面弹出的字符串通过SHA256运算后返回的哈希值的十六进制结果的字符串作为Flag值提交。（8分）

（二）第二阶段任务书（300分）

假定各位选手是某电子商务企业的信息安全工程师，负责企业某些服务器的安全防护，该服务器可能存在着各种问题和漏洞。你需要尽快对该服务器进行安全加固，15分钟之后将会有其它参赛队选手对这些服务器进行渗透。

根据《赛场参数表》提供的第二阶段的信息，请使用PC的谷歌浏览器登录实战平台。

**靶机服务器环境说明：**

场景1：CentOS2018065（用户名：root；密码：123456），服务器操作系统：CentOS（版本不详）；

场景2：Windows2018065（无法打开控制台操作该靶机，只能获取到该靶机的IP，选手需要通过其他方法进入靶机才能进行加固），服务器场景操作系统：Windows（版本不详）。

**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.靶机服务器的FLAG值存放在/root/flagvalue.txt文件或C:\ flagvalue.txt文件中；

4.在登录自动评分系统后，提交对手靶机服务器的FLAG值，同时需要指定对手靶机服务器的IP地址；

5. CentOS2018065靶机服务器如下服务及端口不允许关闭：21、22、23、80、555、3306、7000-8000；Windows2018065靶机服务器如下服务及端口不允许关闭：HTTP 80、FTP 21、Telnet 23、7000-8000；

6.系统加固时需要保证靶机对外提供服务的可用性，服务只能更改配置，不允许更改内容；

7.本环节是对抗环节，不予补时。

**可能的漏洞列表如下：**

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。

**评分说明：**

规则1：每提交1次对手靶机服务器的FLAG值增加2分，每当被对手提交1次自身靶机服务器的FLAG值扣除2分，每个对手靶机服务器的FLAG值只能提交一次；

规则2：系统自动启动违规检测和扣分机制，如发现如下违规行为，系统均给予自动扣分，每检测到一次违规行为扣除一次分数，扣分明细显示在违规记录中，计算在第二阶段总成绩中：

1）攻防阶段启用FLAG检测机制，如发现FLAG异常（譬如：删除、修改、移动、杀进程），记为一次违规行为，每次扣分3分；

2）攻防阶段启用服务端口检测机制，如发现关闭题目要求开启的端口，记为一次违规行为，每端口每次扣分1分；

3）攻防阶段靶机服务器IP地址为DHCP自动获取，不允许修改，如修改触发上述所有检测机制；

4）在加固时间后，选手自己关闭靶机服务器或被他人关闭，触发上述所有检测机制，且裁判员不予帮助重启。

规则3：第二阶段总分为300分，初始分为100分。在实际得分和大屏显示中，某选手得分可能会显示负分或者超过300分；凡是负分的，本阶段评判成绩一律为0分；凡是超过300分的，本阶段评判成绩一律为300分；0-300分的评判成绩保持不变。

（样卷完）