**2018年全国职业院校技能大赛**

**拟设赛项规程**

# 一、赛项名称

赛项编号：GZ-2018110

赛项名称：信息安全管理与评估

英语翻译：Information Security Management and Evaluation

赛项组别：高职组

赛项归属产业：第三产业-信息传输、计算机服务和软件业

# 二、竞赛目的

（一）检验教学成果

全国高职高专院校信息安全与管理和计算机网络技术的专业点数已经超过700多个，在校生40多万，2018年信息安全管理与评估大赛是延续历届赛项的竞赛内容，通过赛项检验参赛选手安全网络组建、按照等保要求加固网络系统、安全架构、渗透测试、攻防实战等技术能力，检验参赛队计划组织和团队协作等综合职业素养，强调学生创新能力和实践能力培养，提升学生职业能力和就业质量。

（二）强化专业建设

针对国家“十二五”期间互联网+、电子政务、智慧城镇和教育信息化等领域信息安全岗位人才急需，按照《高等职业教育电子信息类专业指导规范II》的信息安全与管理专业标准建设框架，通过赛项丰富完善信息安全与管理专业课程体系建设，使人才培养更贴近岗位实际，提升专业培养服务社会和行业发展的能力。

该赛项内容覆盖信息安全与管理专业“信息安全技术与实施”、“信息安全产品配置与应用”、“网络设备配置与管理”、“网络攻防实训”、“系统运行安全与维护”、“操作系统安全配置”、“Web渗透测试技术”等专业核心课程内容。

（三）促进产教合作

赛项基于信息安全领域主流技术和现行业务流程设计，信息安全行业专家与院校教育专家紧密合作，赛前完成竞赛内容向教学改革的成果转化，实现以赛促教、以赛促学、以赛促改的教产融合的赛事创新。

# 三、竞赛内容

重点考核参赛选手安全网络组建、网络系统安全策略部署、按照等级保护要求进行系统加固与信息保护、网络安全运维管理等综合实践能力，具体包括：

* + 1. 参赛选手能够根据大赛提供的赛项要求，设计信息安全防护方案，并且能够提供详细的信息安全防护设备拓扑图。
		2. 参赛选手能够根据业务需求和实际的工程应用环境，实现网络设备、安全设备、服务器的连接，通过调试，实现设备互联互通。
		3. 参赛选手能够在赛项提供的网络设备及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，组建网络以满足应用需求。
		4. 参赛选手能够根据网络实际运行中面临的安全威胁，按照等级要求指定安全策略并部署实施，实现系统的加固，防范并解决网络恶意入侵和攻击行为。
		5. 参赛选手能够按照要求准确撰写工作总结。
		6. 以参赛队为单位进行分组对抗，在防护本参赛队服务器的同时，渗透其他参赛队的服务器，服务器被渗透的参赛队将被扣除相应分数。比赛结果通过大屏幕等形式在休息区实时展示。
		7. 竞赛共分三个阶段，各阶段重点内容如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容模块** | **具体内容** | **说明** |
| 第一阶段 | 网络平台搭建 | 网络规划 | VLSM、CIDR等； |
| 基础网络 | VLAN、WLAN、STP、SVI、RIPV2、OSPF等； |
| 网络安全设备配置与防护 | 访问控制 | 保护网络应用安全，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； |
| 密码学和VPN | 密码学基本理论L2L IPSec VPNGRE Over IPSecL2TP Over IPSecIKE：PSKIKE：PKISSL VPN等； |
| 数据分析 | 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； |
| 第二阶段 | 系统安全攻防及运维安全管控 | 网络渗透测试及其加固技术 | MAC渗透测试及其加固DHCP渗透测试及其加固ARP渗透测试及其加固STP渗透测试及其加固VLAN渗透测试及其加固路由协议(RIPV2、OSPF)渗透测试及其加固 |
| 操作系统渗透测试及其加固 | Windows、Linux操作系统服务缓冲区溢出渗透测试及其加固 |
| Web应用和数据库渗透测试及其加固技术 | SQL Injection（SQL注入）漏洞渗透测试及其安全编程Command Injection（命令注入）漏洞渗透测试及其安全编程File Upload（文件上传）漏洞渗透测试及其安全编程Directory Traversing（目录穿越）漏洞渗透测试及其安全编程XSS（Cross Site Script）漏洞渗透测试及其安全编程CSRF（Cross Site Request Forgeries）漏洞渗透测试及其安全编程Cookie Stole（Cookie盗用）漏洞渗透测试及其安全编程Session Hijacking（会话劫持）漏洞渗透测试及其安全编程配置WAF（Web应用防火墙）加固Web应用等； |
| 第三阶段 | 分组对抗 | 参赛队之间进行对抗演练 | 网络协议安全攻防Windows/Linux操作系统安全攻防Web应用/数据库安全攻防等； |

* + 1. 竞赛分值权重和时间分布

|  |  |  |
| --- | --- | --- |
| **序号** | **内容模块** | **竞赛时间** |
| 第一阶段权重30% | 网络平台搭建权重9% | 300分钟 |
| 网络安全设备配置与防护权重21% |
| 第二阶段权重40% | 系统安全攻防及运维安全管控权重40% |
| 第三阶段权重30% | 分组对抗权重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，同一学校相同项目报名参赛队不超过1支。每支参赛队由3名选手（设队长1名）和不超过2名指导教师组成。
2. 赛项拟邀请香港、澳门、台湾等地区和境外代表队参赛或观摩交流，但参赛成绩不计入总体排名。

# 五、竞赛流程

1. 竞赛流程图
2. 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6小时，时间为9:00-15:00，具体安排如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **日期** | **时间** | **事项** | **参加人员** | **地点** |
| 竞赛前2日 | 20:00前 | 裁判、仲裁、监督报到 | 工作人员 | 住宿酒店 |
| 竞赛前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 | 裁判进入裁判室 | 裁判长、现场裁判 | 竞赛场地 |
| 08:00-08:30 | 选手抽签，一次加密 | 参赛选手、现场裁判 | 竞赛场地 |
| 08:30-08:50 | 选手抽签，二次加密及入场 | 参赛选手、现场裁判 | 竞赛场地 |
| 08:50-09:00 | 参赛代表队就位，宣读考场纪律,抽取赛题参数表 | 参赛选手、现场裁判 | 竞赛场地 |
| 09:00-09:15 | 第一阶段和第二阶段赛题发放时间 | 参赛选手、现场裁判 | 竞赛场地 |
| 09:15-13:30 | 第一阶段和第二阶段正式比赛时间 | 参赛选手、现场裁判 | 竞赛场地 |
| 13:30-14:00 | 第一阶段与第二阶段比赛结果提交时间，三次加密 | 参赛选手、现场裁判 | 竞赛场地 |
| 14:00-14:15 | 第三阶段赛题发放时间 | 参赛选手、现场裁判 | 竞赛场地 |
| 14:15-15:00 | 第三阶段正式比赛时间 | 参赛选手、现场裁判 | 竞赛场地 |
| 15:00 | 比赛正式结束 | 参赛选手、现场裁判 | 竞赛场地 |
| 15:00-评判完毕后 | 成绩汇总报送，成绩公示 | 评分裁判、裁判长、专家、监督 | 竞赛场地和参赛队住宿酒店 |
| 竞赛后1日 | 9：30-10：00 | 闭幕式 | 领导、嘉宾、裁判、各参赛队、专家组 | 会议室 |

备注：第一阶段和第二阶段赛题在开始比赛时同时发放，并于13：30统一提交答题成果，交卷完毕后发放第三阶段赛题。

参赛选手午餐时间由赛项执委会统一安排，就餐时间计入比赛时间。

# 六、竞赛赛卷

* + 1. 赛项执委会下设的命题专家组负责本赛项命题工作。
		2. 本赛项为公开赛卷，竞赛赛卷距国赛开始日1月之前公开。
		3. 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。

# 七、竞赛规则

* + 1. 报名资格

参赛选手须为3名2018年度普通高等学校全日制在籍专科学生。本科院校中高职类全日制在籍学生，五年制高职四、五年级学生可报名参加高职组比赛。高职组参赛选手年龄须不超过25周岁（当年），年龄计算的截止时间以2018年5月1日为准。凡在往届本赛项全国职业院校技能大赛中获一等奖的学生，不再参加该赛项的比赛。

* + 1. 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。
		2. 竞赛所需的硬件设备、系统软件和辅助工具由赛项执委会统一安排，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。
		3. 参赛队自行决定选手分工、工作程序和时间安排。
		4. 参赛队在赛前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。
		5. 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。
		6. 竞赛结束（或提前完成）后，参赛队要确认已成功提交所有竞赛文档，裁判员与参赛队队长一起签字确认，参赛队在确认后不得再进行任何操作。
		7. 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示，并在闭赛式上予以公布。
		8. 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。
		9. 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。
		10. 赛项每个比赛环节裁判判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

竞赛工位内设有操作平台，每工位配备220V电源，工位内的电缆线应符合安全要求。每个竞赛工位面积≥6㎡，确保参赛队之间互不干扰。竞赛工位标明工位号，并配备竞赛平台和技术工作要求的软、硬件。环境标准要求保证赛场采光(大于500lux)、照明和通风良好；每支参赛队提供一个垃圾箱。

除了竞赛工位之外，同时设计了成果展示区、体验区、观摩区、服务区等。成果展示区主要展示大赛配套教材、资源包等内容；体验区主要展示竞赛设备以及相关新技术、新产品；观摩区主要展示信息安全攻防对战的实时进度；服务区提供医疗等服务保障。

# 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 | GB 17859-1999 | 《计算机信息系统安全保护等级划分准则》 |
| 2 | GB/T 20271-2006 | 《信息安全技术信息系统通用安全技术要求》 |
| 3 | GB/T 20270-2006 | 《信息安全技术网络基础安全技术要求》 |
| 4 | GB/T 20272-2006 | 《信息安全技术操作系统安全技术要求》 |
| 5 | GB/T 20273-2006 | 《信息安全技术数据库管理系统安全技术要求》 |
| 6 | 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》 |
| 7 | GB/T 20269-2006 | 《信息安全技术信息系统安全管理要求》 |
| 8 | ISO OSI | OSI开放系统互连参考模型 |
| 9 | IEEE 802.1 | 局域网概述，体系结构，网络管理和性能测量 |
| 10 | IEEE 802.2 | 逻辑链路控制LLC |
| 11 | IEEE 802.3 | 总线网介质访问控制协议CSMA/CD及物理层技术规范 |
| 12 | IEEE 802.6 | 城域网（Metropolitan Area Networks)MAC 介质访问控制协议DQDB及其物理层技术规范 |
| 13 | IEEE 802.10 | 局域网安全技术标准 |
| 14 | IEEE 802.11 | 无线局域网的介质访问控制协议CSMA/CA及其物理层技术规范 |
| 15 | BG/T 22239-2008 | 信息安全技术信息系统安全等级保护基本要求 |

# 十、技术平台

1. 竞赛软件

赛项执委会提供个人计算机（安装Windows操作系统），用以组建竞赛操作环境，并安装Office等常用应用软件。

|  |  |  |
| --- | --- | --- |
| **序号** | **软件** | **介绍** |
| 1 | Windows | 操作系统 |
| 2 | Microsoft Office | 文档编辑工具 |
| 3 | VMware | 虚拟机运行环境 |
| 4 | 超级终端 | 设备调试连接工具 |

赛项执委会提供渗透测试机和靶机虚拟机环境。

|  |  |  |
| --- | --- | --- |
| **序号** | **软件** | **介绍** |
| 1 | Windows 7\Windows XP | Windows客户机操作系统 |
| 2 | Windows Server 2003\2008 | Windows服务器操作系统 |
| 3 | Ubuntu\Debian | 渗透测试机操作系统 |
| 4 | Linux CentOS | Linux服务器操作系统 |

1. 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 | 神州数码CS6200交换机 |
| 2 | 防火墙 | 1 | 神州数码DCFW-1800E-N3002 |
| 3 | 堡垒服务器 | 1 | 神州数码DCST-6000B |
| 4 | WEB应用防火墙 | 1 | 神州数码DCFW-1800-WAF-LAB |
| 5 | 网络日志系统 | 1 | 神州数码DCBI-NetLog-LAB |
| 6 | 无线交换机 | 1 | 神州数码DCWS-6028 |
| 7 | 无线接入点 | 1 | 神州数码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 |

# 十一、成绩评定

1. 裁判工作原则

按照《2018年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，划分裁判小组（2人为一组），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。本赛项计划需要裁判14名。分为加密裁判、现场裁判和评分裁判。

赛项需进行三次加密，加密后参赛选手中途不得擅自离开赛场。分别由3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。

第三组加密裁判对提交的竞赛文档进行加密。确定竞赛文档号，替换赛位号，填写三次加密记录表，装入三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。

1. 裁判评分方法

裁判组负责竞赛机考评分和结果性评分，由裁判长负责竞赛全过程；裁判员提前报到，报到后所有裁判的手机全部上缴裁判长统一保管，评分结束返回，保证竞赛的公正与公平。

竞赛现场有监督员、裁判员、监考员、技术支持队伍等组成，分工明确。根据现场环境，每位监考员负责2-3组参赛队，5-6名技术支持工程师负责所有工位设备应急。监考员负责与参赛队伍的交流沟通及试卷等材料的收发，裁判员负责设备问题确认和现场执裁，技术支持负责执行裁判确认后的设备应急处理。

1. 成绩产生办法

裁判员执裁过程中，各模块由分组裁判员进行背对背评分，由小组长负责裁定成绩一致方提交到成绩统计组，统计组再次核对每小题的得分，并汇总产生每套竞赛文档号的对应成绩。

裁判长正式提交竞赛文档号对应的评分结果并复核无误后，加密裁判在监督人员监督下对加密结果进行逐层解密，形成成绩一览表，成绩表由裁判长、监督员签字确认。

竞赛评分严格按照公平、公正、公开的原则，评分标准注重考查参赛选手以下各方面的能力和水平：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **竞赛阶段** | **竞赛任务** | **考核内容** | **分值** | **评分方式** |
| 第一阶段权重30% | 网络平台搭建权重9% | 网络规划文档 | 2% | 结果评分-客观 |
| 按照等保要求进行网络设备配置,提交相关配置文件或截图文件 | 7% | 结果评分-客观 |
| 网络安全设备配置与防护权重21% | 防火墙相关配置截图文件 | 21% | 结果评分-客观 |
| 网络日志系统相关配置截图文件 | 结果评分-客观 |
| web应用防火墙相关配置截图文件 | 结果评分-客观 |
| 无线控制器相关配置文件 | 结果评分-客观 |
| 三层交换机相关配置文件 | 结果评分-客观 |
| 第二阶段权重40% | 系统安全攻防及运维安全管控权重40% | 服务器加固配置 | 20% | 机考评分 |
| 服务器渗透配置 | 20% | 机考评分 |
| 第三阶段权重30% | 分组对抗权重30% | 防守成功，坚持到竞赛结束 | 10% | 机考评分 |
| 渗透成功 | 20% | 机考评分 |

参赛选手应体现团队风貌、团队协作与沟通、组织与管理能力和工作计划能力等，并注意相关文档的准确性与规范性。

竞赛过程中，参赛选手如有不服从裁判判决、扰乱赛场秩序、舞弊等不文明行为，由裁判组按照规定扣减相应分数，情节严重的取消竞赛资格。选手有下列情形，需从比赛成绩中扣分：

1. 违反比赛规定，提前进行操作或比赛终止后仍继续操作的，由现场裁判负责记录并酌情扣1-5分。
2. 在竞赛过程中，违反操作规程，影响其他选手比赛的，未造成设备损坏的参赛队，扣5-10分。
3. 在竞赛过程中，造成设备损坏或影响他人比赛、情节严重的报竞赛执委会批准，终止该参赛队的比赛，竞赛成绩以0分计算。
4. 成绩复核与公布
5. 为保障成绩评判的准确性，监督组将对赛项总成绩排名前30%的所有参赛队伍（选手）的成绩进行复核；对其余成绩进行抽检复核，抽检覆盖率不得低于15%。如发现成绩错误以书面方式及时告知裁判长，由裁判长更正成绩并签字确认。复核、抽检错误率超过5%的，裁判组将对所有成绩进行复核。
6. 竞赛成绩以复核无误后，经项目裁判长、监督人员审核签字后确定，并在赛场及赛场外张贴纸质成绩进行公示。

# 十二、奖项设定

赛项设参赛选手团体奖，以赛项实际参赛队总数为基础，一等奖占比10%，二等奖占比20%，三等奖占比30%，小数点后四舍五入。

获得一等奖的参赛队指导教师获“优秀指导教师奖”，授予荣誉证书。

# 十三、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，制定应急预案，及时处置突发事件。制定相应安全管理的规范、流程和突发事件应急预案，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、设备均符合国家有关安全规定。赛项专家组充分考虑了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将在赛项技术文件中加以明确。

2. 赛项技术文件包含国家（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. 赛项执委会将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。该赛项源于实际安全网络组建与运维的生产过程，根据《中华人民共和国劳动法》等法律法规，建立了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. 赛项执委会将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

赛场组织与管理人员制定安保须知、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。

* 1. 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，额定功率：3KVA，后备时间：2小时，电池类型：输出电压：230V±5%V；市电采用双路供电。

* 1. 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，确保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。

参赛队选手从参赛校到承办校的旅途安全由各省市负责，参赛选手竞赛过程中的安全保障由竞赛组委会负责。

* 1. 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。承办单位赛前须按照赛项执委会要求排除安全隐患。
	2. 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。
	3. 承办单位应提供保证应急预案实施的条件。对于比赛内容涉及高空作业、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。
	4. 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。
	5. 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。
	6. 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、照相摄录设备，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
2. 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（费用自理）。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。
3. 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。
4. 大赛期间有组织的参观和观摩活动的交通安全由赛项执委会负责。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。
5. 各赛项的安全管理，除了可以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。
6. 组队责任
7. 各省、自治区、直辖市和计划单列市在组织参赛队时，须安排为参赛选手购买大赛期间的人身意外伤害保险。
8. 各省、自治区、直辖市和计划单列市参赛队组成后，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。
9. 各参赛队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。
10. 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
2. 赛项出现重大安全事故的，停止承办单位的赛项承办资格。
3. 因参赛队伍原因造成重大安全事故的，取消其参赛资格。
4. 参赛队伍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。
5. 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。

# 十四、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. 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。
2. 参赛选手需持统一印制的参赛证和有效身份证件参加竞赛。
3. 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。
4. 参加选手请勿携带任何电子设备及其他资料、用品进入赛场。
5. 参赛选手应按照规定时间抵达赛场，凭参赛证、身份证件检录，按要求入场，不得迟到早退。
6. 参赛选手应增强角色意识，科学合理分工与合作。
7. 参赛选手应按有关要求在指定位置就坐。
8. 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。
9. 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。
10. 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。
11. 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。
12. 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。

# 十五、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。

# 十六、竞赛观摩

本赛项将会设计观摩区，使用大屏幕实时显示信息安全攻防对战的进度。

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。

# 十七、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。竞赛过程采用全程摄录的形式，对比赛的开闭幕式、比赛过程实况转播、手工评卷过程进行摄录。

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。

# 十八、资源转化

依照《2018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 |
| 试题库 | 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 |
| 优秀选手访谈 | 视频 | 1 | 10分钟以上 | 赛后60天 |

赛后还需加强师资队伍建设，促进资源转化能够在教学中有效应用。2018年大赛完毕后计划进行2期研讨会，以及2期师资培训,培训内容定为信息安全在工作与生活中的应用，系统信息安全实战，网络信息安全实战，数据安全及取证技术，数据中心灾备技术、无线网络安全等内容。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **活动名称** | **计划时间** | **备注** |
| 1 | 研讨会第1期 | 2018年7月 |  |
| 2 | 师资培训第1期 | 2018年7月 |  |
| 3 | 师资培训第2期 | 2018年10月 |  |
| 4 | 研讨会第2期 | 2018年12月 |  |

**2018年全国职业院校技能大赛高职组**

**“信息安全管理与评估”样题**

# 赛项时间

9:00-15:00，共计6小时，含赛题发放、收卷及午餐时间。

# 赛项信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **竞赛阶段** | **任务阶段** | **竞赛任务** | **竞赛时间** | **分值** |
| 第一阶段平台搭建与安全设备配置防护 | 任务1 | 网络平台搭建 | 9:00-13:30 | 300 |
| 任务2 | 网络安全设备配置与防护 |
| 第二阶段系统安全攻防及运维安全管控 | 任务1 | 缓冲区溢出漏洞渗透测试 | 400 |
| 任务2 | Web应用程序安全攻防 |
| 任务3 | ARP扫描渗透测试 |
| 任务4 | 操作系统判断渗透测试 |
| 任务5 | 数据库访问渗透测试及其加固 |
| 任务6 | 网络协议渗透测试及其加固 |
| 中场收卷 | 13:30-14:00 |
| 第三阶段分组对抗 | 系统加固 | 14:00-15:00 | 300 |
| 系统攻防 |

# 赛项内容

本次大赛，各位选手需要完成三个阶段的任务，其中第一个阶段需要提交任务“操作文档”，“操作文档”需要存放在裁判组专门提供的U盘中。第二、三阶段请根据现场具体题目要求操作。

选手首先需要在U盘的根目录下建立一个名为“xx工位”的文件夹（xx用具体的工位号替代），赛题第一阶段完成任务操作的文档放置在文件夹中。

例如：08工位，则需要在U盘根目录下建立“08工位”文件夹，并在“08工位”文件夹下直接放置第一个阶段的操作文档文件。

**特别说明：只允许在根目录下的“08工位”文件夹中体现一次工位信息，不允许在其他文件夹名称或文件名称中再次体现工位信息，否则按作弊处理。**

1. **赛项环境设置**

赛项环境设置包含了三个竞赛阶段的基础信息：网络拓扑图、IP地址规划表、设备初始化信息。

### 网络拓扑图



### IP地址规划表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **设备名称** | **接口** | **IP地址** | **互联** | **可用IP数量** |
| 防火墙DCFW | EthX | x.x.x.x/x | 与PC-2相连 | 见赛场IP参数表 |
| EthX | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| 地址池 | x.x.x.x/x | SSL VPN地址池 | 见赛场IP参数表 |
| 无线交换机DCWS | EthX | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| 地址池 | x.x.x.x/x | DCHP地址池 | 见赛场IP参数表 |
| WEB应用防火墙WAF | EthX | x.x.x.x/x  | 与DCRS相连 | 见赛场IP参数表 |
| EthX |  | 与DCST相连 | 见赛场IP参数表 |
| 三层交换机DCRS | Vlan 2 | x.x.x.x/x | 与DCWS相连 | 见赛场IP参数表 |
| Vlan 10 | x.x.x.x/x | 与WAF相连 | 见赛场IP参数表 |
| Vlan 20 | x.x.x.x/x | 与PC-1所在用户区相连 | 见赛场IP参数表 |
| Vlan 30 | x.x.x.x/x | 与PC-3所在用户区相连 | 见赛场IP参数表 |
| Vlan 40 | x.x.x.x/x | 与DCBI相连 | 见赛场IP参数表 |
| Vlan 50 | x.x.x.x/x | 与DCFW相连 | 见赛场IP参数表 |
| 网络日志系统DCBI | EthX | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| 堡垒服务器DCST | EthX | x.x.x.x/x | 与WAF相连 | 见赛场IP参数表 |
| PC-1 | 无 | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| PC-2 | 无 | x.x.x.x/x | 与DCFW相连 | 见赛场IP参数表 |
| PC-3 | 无 | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| 服务器场景-1 | 无 | 见系统安全攻防加固赛题部分 |  |
| 服务器场景-2 | 无 | 见系统安全攻防加固赛题部分 |  |
| 服务器场景-3 | 无 | 见系统安全攻防加固赛题部分 |  |
| 服务器场景-4 | 无 | 见系统安全攻防加固赛题部分 |  |
| 服务器场景-5 | 无 | 见系统安全攻防加固赛题部分 |  |
| 服务器场景-6 | 无 | 见系统安全攻防加固赛题部分 |  |
| 备注 | 1.赛题可用IP地址范围见“赛场IP参数表”；2.具体网络连接接口见“赛场互联接口参数表”；3.设备互联网段内可用地址数量见“赛场IP参数表”；4.IP地址分配要求，最节省IP地址，子网有效地址规划遵循2n-2的原则；5.参赛选手按照“赛场IP参数表”要求，自行分配IP地址段、设备互联接口；6.将分配的IP地址段和接口填入“赛场IP参数表”中（“赛场IP参数表”电子文件存于U盘“第一阶段”文件夹中，请填写完整后提交。） |

### 设备初始化信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **设备名称** | **管理地址** | **默认管理接口** | **用户名** | **密码** |
| 防火墙DCFW | <http://192.168.1.1> | ETH0 | admin | admin |
| 网络日志系统DCBI | https://192.168.5.254 | ETH0 | admin | 123456 |
| WEB应用防火墙WAF | https://192.168.45.1 | ETH3 | admin | admin123 |
| 三层交换机DCRS | - | Console | - | - |
| 无线交换机DCWS | - | Console | admin | admin |
| 堡垒服务器DCST | - | - | 参见“DCST登录用户表” |
| 备注 | 所有设备的默认管理接口、管理IP地址不允许修改;如果修改对应设备的缺省管理IP及管理端口，涉及此设备的题目按 0 分处理。 |

1. **第一阶段任务书（300分）**

该阶段需要提交配置或截图文档，命名如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| **阶段** | **任务** | **序号** | **文档名称** |
| 第一阶段 | 任务1 | 1 | 任务1  |
| 2 | 赛场IP参数表 |
| 任务2 | 3 | 任务2-DCFW |
| 4 | 任务2-DCBI |
| 5 | 任务2-WAF |
| 6 | 任务2-DCRS |
| 7 | 任务2-DCWS |

### 任务1：网络平台搭建

平台搭建要求如下：

|  |  |
| --- | --- |
| 题号 | 网络需求 |
| 1 | 根据网络拓扑图所示，按照IP地址参数表，对WAF的名称、各接口IP地址进行配置。 |
| 2 | 根据网络拓扑图所示，按照IP地址参数表，对DCRS的名称、各接口IP地址进行配置。 |
| 3 | 根据网络拓扑图所示，按照IP地址参数表，对DCFW的名称、各接口IP地址进行配置。 |
| 4 | 根据网络拓扑图所示，按照IP地址参数表，对DCWS的各接口IP地址进行配置。 |
| 5 | 根据网络拓扑图所示，按照IP地址参数表，对DCBI的名称、各接口IP地址进行配置。 |
| 6 | 根据网络拓扑图所示，按照IP地址参数表，在DCRS交换机上创建相应的VLAN，并将相应接口划入VLAN。 |
| 7 | 采用静态路由的方式，全网络互连。 |
| 8 | 完整填写“赛场IP参数表”。 |

### 任务2：网络安全设备配置与防护

#### DCFW:

1. 在总公司的DCFW上配置，连接LAN接口开启PING,HTTP,HTTPS功能，连接Internet接口开启PING、HTTPS功能；并且新增一个用户，用户名dcn2017，密码dcn2017，该用户只有读-执行权限；
2. DCFW配置NTP 和 LOG， Server IP为X.X.X.X，NTP认证密码为Dcn2017；
3. DCFW配置静态ARP绑定，MAC地址880B.0A0B.0C0D与IP地址X.X.X.X绑定；
4. DCFW连接Internet的区域上配置以下攻击防护：

开启以下Flood防护：

ICMP洪水攻击防护，警戒值2000，动作丢弃；

UDP供水攻击防护，警戒值1500，动作丢弃；

SYN洪水攻击防护，警戒值5000，动作丢弃；

开启以下DOS防护：

Ping of Death攻击防护；

Teardrop攻击防护；

IP选项，动作丢弃；

ICMP大包攻击防护，警戒值2048，动作丢弃；

1. 限制LAN到Internet流媒体RTSP应用会话数，在周一至周五8:00-17:00每5秒钟会话建立不可超过20；
2. DCFW上配置NAT功能，使PC2能够通过WEB方式正常管理到WAF，端口号使用10666;）
3. 总公司DCFW配置SSLVPN，建立用户dcn01，密码dcn01，要求连接Internet PC2可以拨入，配置服务端口为9999， SSLVPN地址池参见地址表；
4. DCFW加强访问Internet安全性，禁止从HTTP打开和下载可执行文件和批处理文件；
5. DCFW配置禁止所有人在周一至周五工作时间9：00-18：00访问京东www.jd.com和淘宝www.taobao.com;相同时间段禁止访问中含有“娱乐”、“新闻”的WEB页面；
6. DCFW上配置ZONE和放行策略，连接Internet接口为“Untrust”区域，连接DCRS接口为“Trust”区域，连接SSL VPN接口为“VPN HUB”区域，要求配置相应的最严格安全策略；）

#### DCBI:

1. 在公司总部的DCBI上配置，设备部署方式为旁路模式，并配置监控接口与管理接口;增加非admin账户DCN2017，密码dcn2017，该账户仅用于用户查询设备的系统状态和统计报表;
2. 在公司总部的DCBI上配置，监控周一至周五9：00-18：00 PC-1所在网段用户访问的URL中包含xunlei的HTTP访问记录，并且邮件发送告警;
3. 在公司总部的DCBI上配置，监控PC-1所在网段用户周一至周五9：00-18：00的即时聊天记录;
4. 公司总部LAN中用户访问网页中带有“MP3”、“MKV” 、“RMVB”需要被DCBI记录；邮件内容中带有“银行账号”记录并发送邮件告警；
5. DCBI监控LAN中用户访问网络游戏，包括“QQ游戏”、“魔兽世界”并作记录；
6. DCBI配置应用及应用组“快播视频”，UDP协议端口号范围23456-23654，在周一至周五9：00-18：00监控LAN中所有用户的“快播视频”访问记录；
7. DCBI上开启邮件告警，邮件服务器地址为X.X.X.X，端口号25,告警所用邮箱用户名dcnadmin,密码Dcn2017;当DCBI磁盘使用率超过75%时发送一次报警；

#### WAF:

1. 在公司总部的WAF上配置，编辑防护策略，定义HTTP请求体的最大长度为512，防止缓冲区溢出攻击；
2. 在公司总部的WAF上配置，防止某源IP地址在短时间内发送大量的恶意请求，影响公司网站正常服务。大量请求的确认值是：并发访问超过3000次请求；
3. 在公司总部的WAF上配置，对公司网站（X.X.X.X）进行安全评估，检查网站是否存在安全漏洞，便于在攻击没有发生的情况下提前做出防护措施；
4. 使用WAF自带标识组配置爬虫防护与扫描防护，通过WAF阻止爬虫探测；
5. 在公司总部的WAF上配置，禁止HTTP应答中包含敏感字段“赛题”和“答案”的报文经过WAF设备;
6. 公司web应用防火墙透明模式部署，为了防止不法人员对公司内的网站(X.X.X.X)进行攻击，在web 应用防火墙上开启“黑名单”策略，禁止公网IP地址（X.X.X.X）访问网站服务器;
7. 公司web应用防火墙透明模式部署，为了防止不法人员对公司内的网站(X.X.X.X)进行攻击，在web 应用防火墙上开启防止“SQL注入”攻击策略阻止攻击流量；
8. 在公司总部的WAF上配置， WAF设备的内存使用率超过75%每隔5分钟发送邮件和短信给管理，邮箱admin@digitalchina.com，手机13912345678；

#### DCRS:

1. DCRS为接入交换机，为终端产生防止MAC地址防洪攻击，请配置端口安全，每个已划分VLAN的端口最多学习到5个MAC地址，发生违规阻止后续违规流量通过，不影响已有流量并产生LOG日志；Ex/x为专用接口，限定MAC地址00-11-11-11-11-11可以连接； 将连接DCFW的双向流量镜像至Netlog进行监控和分析；
2. DCRS配置802.1x认证，Radius服务器IP 地址X.X.X.X,认证密码Dcn2017,

Ex/x号端口开启802.1x功能，接入该端口通过PC上的802.1x软件进行认证；

1. 接入DCRS Ex/x，仅允许IP地址X.X.X.X-X.X.X.X为源的数据包为合法包，以其它IP地址为源地址，交换机直接丢弃；
2. 为拦截，防止非法的MAC地址与IP地址绑定的ARP数据包，配置动态ARP检测功能，AC为DHCP服务器，限制与AC在同一VLAN接口的ARP阀值为50；
3. DCRS上开启以下安全特性，防IP Spoofing攻击、防TCP非法标志攻击、防端口欺骗攻击、防TCP碎片攻击、防ICMP碎片攻击；

#### DCWS：

1. AP通过option43方式进行正常注册上线；
2. 设置AP支持802.11n协议，并兼容802.11b和g协议
3. 设置SSID DCN，加密模式为wpa-personal,其口令为：chinaskill；

设置SSID GUEST 不进行认证加密；

1. GUSET最多接入10个用户，用户间相互隔离，并对GUEST网络进行流控，上行1M，下行2M；
2. 通过配置避免接入终端较多且有大量弱终端时，高速客户端被低速客户端“拖累”，低速客户端不至于长时间得不到传输；
3. 通过使用黑名单技术禁止mac地址为68-a3-c4-e6-a1-be的PC通过无线网络上网；
4. 防止非法AP假冒合法SSID，开启AP威胁检测功能；
5. 通过设置实现在AC断开网络连接时AP还能正常工作；
6. 考虑到无线网络会进一步部署，增加更多的AP，设置已有AP信道和发射功率每隔1小时自动调节；
7. 为防止增多AP后产生过多的ARP数据包，开启ARP抑制功能，要求AP能代为应答其已知的MAC地址；
8. **第二阶段任务书（400分）**

提示：本阶段用到堡垒服务器DCST中的服务器场景，获取服务器IP地址方式如下：

Windows服务器的IP地址可以通过拓扑界面获得，如果获得不了，采用如下方法获得：

* 通过DCST场景里的网络拓扑图，启动连接设备
* 进入服务器，用户名为administrator，密码：空
* 执行ipconfig /all，即可获得服务器IP地址

### 任务1：缓冲区溢出漏洞渗透测试

**任务描述：**

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，在该系统中某程序可能存在缓冲区溢出漏洞；你需要对该程序进行渗透测试，确认程序确实存在该漏洞；

**任务环境说明：**

主机场景：WindowsXP

主机场景操作系统：Microsoft Windows XP Professional

主机场景安装服务/工具1：Visual C++ 6.0；

主机场景安装服务/工具2：OllyICE；

主机场景安装服务/工具3：Findjmp；

**任务内容：**

1. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行分析，找到Main函数中有缓冲区溢出可能的变量名，并将Flag值（形式：有缓冲区溢出可能的变量名）进行提交；
2. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行完善，使用工具findjmp找到Windows内核文件KERNEL32.DLL中的首个“call esp”指令的内存地址，将该内存地址作为函数的返回地址，根据以上信息，填写可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）中的F1字符串，并将Flag值（形式：F1字符串内容）进行提交；
3. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行完善，填写该源代码中join函数中的F2、F3字符串，并将Flag值（形式：F2字符串内容;F3字符串内容）进行提交；
4. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行完善，填写该源代码中repstr函数中的F4、F5字符串，并将Flag值（形式：F4字符串内容;F5字符串内容）进行提交；
5. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行完善，填写该源代码中main函数中的F6、F7、F8字符串，并将Flag值（形式：F6字符串内容;F7字符串内容;F8字符串内容）进行提交；
6. 将完善后的缓冲区溢出渗透测试程序源代码（位置：C:\VC\Source Code\Overflow.c）进行编译、链接、运行，将该程序的运行结果显示的最后1行字符串作为Flag值（形式：程序的运行结果显示的最后1行字符串）提交；

### 任务2：Web应用程序安全攻防

**任务描述：**

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，在该系统中Web应用程序可能存在SQL注入漏洞；首先，你需要对该程序进行渗透测试，确认程序确实存在该漏洞；其次，你需要对该程序打补丁，解决以上漏洞带来的问题；第三，你需要再次对该程序进行渗透测试，验证程序是否还存在漏洞。

**任务环境说明：**

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：Microsoft Internet Explorer 6.0

虚拟机安装服务/工具2：Ethereal 0.10.10.0

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

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. 在PC-1上，Web访问DCST中的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，并将所有提交的变量名作为Flag值（形式：变量名1;变量名2;…;变量名n）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站点可通过万能用户名、数据库users表中当中任意一个密码登录，并将万能用户名字符串当中的固定部分作为Flag值（形式：万能用户名字符串当中的固定部分）提交；
3. 对服务器场景：WebServ2003的Web开发环境进行配置，使其能够支持数据抽象层（PDO）技术，并将配置文件的路径及名称字符串作为Flag值（形式：配置文件的路径及名称字符串）提交；
4. 对服务器场景：WebServ2003的Web开发环境进行配置，使其能够支持数据抽象层技术，并将在上题配置文件中取消注释行内容作为Flag值（形式：按顺序取消注释行1字符串; 按顺序取消注释行1字符串;…; 按顺序取消注释行n字符串）提交；
5. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag1字符串，将该字符串作为Flag值（形式：Flag1字符串）提交；
6. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag2字符串，将该字符串作为Flag值（形式：Flag2字符串）提交；
7. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag3字符串，将该字符串作为Flag值（形式：Flag3字符串）提交；
8. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag4字符串，将该字符串作为Flag值（形式：Flag4字符串）提交；
9. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag5字符串，将该字符串作为Flag值（形式：Flag5字符串）提交；
10. 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该DCST中的WebServ2003服务器场景进行SQL注入渗透测试无效，并将页面回显HTML源文件内容作为Flag值（形式：页面回显HTML源文件内容）提交；

### 任务3：ARP扫描渗透测试

**任务描述：**

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，现欲对该系统中主机进行ARP扫描渗透测试，确认该系统中都有哪些IP主机在线；

**任务环境说明：**

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：EditPlus

虚拟机安装服务/工具2：XFTP

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

服务器场景：CentOS5.5

服务器场景操作系统：CentOS Linux 5.5

1. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_sweep.py文件，填写该文件当中空缺的Flag1字符串，将该字符串作为Flag值（形式：Flag1字符串）提交；（arp\_sweep.py脚本功能见该任务第6题）
2. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_sweep.py文件，填写该文件当中空缺的Flag2字符串，将该字符串作为Flag值（形式：Flag2字符串）提交；（arp\_sweep.py脚本功能见该任务第6题）
3. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_sweep.py文件，填写该文件当中空缺的Flag3字符串，将该字符串作为Flag值（形式：Flag3字符串）提交；（arp\_sweep.py脚本功能见该任务第6题）
4. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_sweep.py文件，填写该文件当中空缺的Flag4字符串，将该字符串作为Flag值（形式：Flag4字符串）提交；（arp\_sweep.py脚本功能见该任务第6题）
5. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_sweep.py文件，填写该文件当中空缺的Flag5字符串，将该字符串作为Flag值（形式：Flag5字符串）提交；（arp\_sweep.py脚本功能见该任务第6题）
6. 在虚拟机操作系统：Ubuntu Linux 32bit下执行arp\_sweep.py文件，对服务器场景进行ARP扫描渗透测试；将该文件执行后的显示结果中，第1行的第1个字符以及第2行的第1个字符作为Flag值（形式：第1行的第1个字符;第2行的第1个字符）提交；

### 任务4：操作系统判断渗透测试

**任务描述：**

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，现欲对该系统中主机进行操作系统扫描渗透测试，确认该系统中主机都运行了哪些操作系统；

**任务环境说明：**

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：EditPlus

虚拟机安装服务/工具2：XFTP

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

服务器场景：CentOS5.5

服务器场景操作系统：CentOS Linux 5.5

1. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的os\_scan.py文件，填写该文件当中空缺的Flag1字符串，将该字符串作为Flag值（形式：Flag1字符串）提交；（os\_scan.py脚本功能见该任务第6题）
2. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的os\_scan.py文件，填写该文件当中空缺的Flag2字符串，将该字符串作为Flag值（形式：Flag2字符串）提交；（os\_scan.py脚本功能见该任务第6题）
3. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的os\_scan.py文件，填写该文件当中空缺的Flag3字符串，将该字符串作为Flag值（形式：Flag3字符串）提交；（os\_scan.py脚本功能见该任务第6题）
4. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的os\_scan.py文件，填写该文件当中空缺的Flag4字符串，将该字符串作为Flag值（形式：Flag4字符串）提交；（os\_scan.py脚本功能见该任务第6题）
5. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的os\_scan.py文件，填写该文件当中空缺的Flag5字符串，将该字符串作为Flag值（形式：Flag5字符串）提交；（os\_scan.py脚本功能见该任务第6题）
6. 在虚拟机操作系统：Ubuntu Linux 32bit下执行os\_scan.py文件，对服务器场景进行操作系统信息判断渗透测试，将该文件执行后的显示结果作为Flag值（形式：文件执行后的显示结果字符串）提交；

### 任务5：数据库访问渗透测试及其加固

**任务描述：**

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，在该系统中Web服务器中的数据库服务可能存在访问漏洞；首先，你需要对该程序进行渗透测试，确认程序确实存在该漏洞；其次，你需要对数据库服务进行安全加固配置，解决以上漏洞带来的问题；第三，你需要再次对该程序进行渗透测试，验证程序是否还存在访问漏洞。

**任务环境说明：**

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：EditPlus

虚拟机安装服务/工具2：XFTP

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

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. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mssql\_brute\_force.py文件，填写该文件当中空缺的Flag1字符串，将该字符串作为Flag值（形式：Flag1字符串）提交；（mssql\_brute\_force.py脚本功能见该任务第6题）
2. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mssql\_brute\_force.py文件，填写该文件当中空缺的Flag2字符串，将该字符串作为Flag值（形式：Flag2字符串）提交；（mssql\_brute\_force.py脚本功能见该任务第6题）
3. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mssql\_brute\_force.py文件，填写该文件当中空缺的Flag3字符串，将该字符串作为Flag值（形式：Flag3字符串）提交；（mssql\_brute\_force.py脚本功能见该任务第6题）
4. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mssql\_brute\_force.py文件，填写该文件当中空缺的Flag4字符串，将该字符串作为Flag值（形式：Flag4字符串）提交；（mssql\_brute\_force.py脚本功能见该任务第6题）
5. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mssql\_brute\_force.py文件，填写该文件当中空缺的Flag5字符串，将该字符串作为Flag值（形式：Flag5字符串）提交；（mssql\_brute\_force.py脚本功能见该任务第6题）
6. 在虚拟机操作系统：Ubuntu Linux 32bit下执行mssql\_brute\_force.py文件，进行数据库超级管理员密码暴力破解渗透测试（使用字典文件./root/superdic.txt），将该文件执行后的显示结果中的最后1行内容作为Flag值（形式：文件执行后的显示结果中的最后1行字符串）提交；
7. 通过对服务器场景WebServ2003的数据库服务进行安全加固，阻止PC-3中渗透测试平台对其进行数据库超级管理员密码暴力破解渗透测试，并将进行安全配置的数据库身份验证选项中的英文单词作为Flag值（形式：进行安全配置的数据库身份验证选项中的唯一一个英文单词字符串）提交；
8. 验证在WebServ2003的数据库服务进行安全加固后，再次在虚拟机操作系统：Ubuntu Linux 32bit下执行mssql\_brute\_force.py文件，进行数据库超级管理员密码暴力破解渗透测试（使用字典文件./root/superdic.txt），将该文件执行后的显示结果中的最后1行内容作为Flag值（形式：文件执行后的显示结果中的最后1行字符串）提交；

### 任务6：网络协议渗透测试及其加固

**任务描述：**

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，在该系统中的网络通讯协议可能存在漏洞；首先，你需要对网络进行渗透测试，确认网络协议确实存在该漏洞；其次，你需要对网络通讯协议进行安全加固配置，解决以上漏洞带来的问题；第三，你需要再次对该网络进行渗透测试，验证网络是否还存在访问漏洞。

**任务环境说明：**

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：EditPlus

虚拟机安装服务/工具2：XFTP

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

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. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mac\_flood.py文件，填写该文件当中空缺的Flag1字符串，将该字符串作为Flag值（形式：Flag1字符串）提交；（mac\_flood.py脚本功能见该任务第6题）
2. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mac\_flood.py文件，填写该文件当中空缺的Flag2字符串，将该字符串作为Flag值（形式：Flag2字符串）提交；（mac\_flood.py脚本功能见该任务第6题）
3. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mac\_flood.py文件，填写该文件当中空缺的Flag3字符串，将该字符串作为Flag值（形式：Flag3字符串）提交；（mac\_flood.py脚本功能见该任务第6题）
4. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mac\_flood.py文件，填写该文件当中空缺的Flag4字符串，将该字符串作为Flag值（形式：Flag4字符串）提交；（mac\_flood.py脚本功能见该任务第6题）
5. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mac\_flood.py文件，填写该文件当中空缺的Flag5字符串，将该字符串作为Flag值（形式：Flag5字符串）提交；（mac\_flood.py脚本功能见该任务第6题）
6. 在虚拟机操作系统：Ubuntu Linux 32bit下执行mac\_flood.py文件，进行MAC Flooding渗透测试；运行DCRS交换机命令（#show mac-address-table count），将该命令执行结果显示的交换机学习到的当前动态MAC地址条目总数作为Flag值（形式：动态MAC地址条目总数）提交；
7. 在DCRS交换机的PC-3所连接端口配置端口安全特性，阻止PC-3发起MAC Flooding渗透测试，将配置的端口模式配置命令字符串作为Flag值（形式：端口模式配置命令字符串）提交；
8. 再次在虚拟机操作系统：Ubuntu Linux 32bit下执行mac\_flood.py文件，进行MAC Flooding渗透测试；运行DCRS交换机命令（#show mac-address-table count），将该命令执行结果显示的交换机学习到的当前动态MAC地址条目总数作为Flag值（形式：动态MAC地址条目总数）提交。
9. **第三阶段任务书（300分）**

假定各位选手是Taojin电子商务企业的信息安全工程师，负责服务器的维护，该服务器可能存在着各种问题和漏洞（见以下漏洞列表）。你需要尽快对服务器进行加固，十五分钟之后将会有很多白帽黑客（其它参赛队选手）对这台服务器进行渗透测试。

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：对其它参赛队系统进行渗透测试，取得FLAG值并提交到裁判服务器。

**注意事项：**

注意1：任何时候不能人为关闭服务器的服务端口，否则将判令停止比赛，第三阶段分数为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，第三阶段分数为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，第三阶段分数为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。靶机的Flag值存放在./root/flaginfoxxxx.xxx.txt文件内容当中。每提交1次对手靶机的Flag值增加20分，每当被对手提交1次自身靶机的Flag值扣除20分，每个对手靶机的Flag值只能被自己提交一次。在登录自动评分系统后，提交对手靶机的Flag值，同时需要指定对手靶机的IP地址。

注意5：不得人为恶意破坏自己服务器的Flag值，否则将判令停止比赛，第三阶段分数为0分；

在这个环节里，各位选手可以继续加固自身的服务器，也可以攻击其他选手的服务器。

**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。

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。

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。