**2017年全国职业院校技能大赛高职组**

**“信息安全管理与评估”赛项规程**

#  一、赛项名称

赛项编号：GZ-2017028

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

赛项归属产业：电子信息产业

#  二、竞赛目的

通过赛项检验参赛选手网络组建、安全架构和网络安全运维管控等方面的技术技能，检验参赛队组织和团队协作等综合职业素养，培养学生创新能力和实践动手能力，提升学生职业能力和就业竞争力。通过大赛引领专业教学改革，丰富完善学习领域课程建设，使人才培养更贴近岗位实际，实现以赛促教、以赛促学、以赛促改的产教结合格局，提升专业培养服务社会和行业发展的能力，为国家信息安全行业培养选拔技术技能型人才。

#  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、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，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，指定安全策略并部署实施，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立即下线，该参赛队比赛结束，选手出场。比赛结果通过大屏幕等形式在休息区实时展示。
7. 各竞赛阶段重点内容如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **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； |

8.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30% | 系统安全攻防及运维安全管控权重30% |
| 第三阶段权重40% | 分组对抗权重40% | 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

（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 |
| 竞赛后1日 | 13：30-14：00 | 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、竞赛试题

（一）赛项执委会下设的命题专家组负责本赛项命题工作。

（二）本赛项为公开赛题，竞赛试题距国赛开始日1月之前公开。

（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）公布竞赛试题库。

样题见附件。

# 七、竞赛规则

（一）报名资格

参赛选手须为3名2017年度高等职业学校全日制在籍学生。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2017年5月1日为准。凡在往届本赛项全国大赛中获一等奖的学生，不再参加该赛项的比赛。

（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。

（四）参赛队自行决定选手分工、工作程序和时间安排。

（五）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。

（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。

# 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》 |

# 十、技术平台

（一）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 |

（二）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

 （一）裁判工作原则

按照《2017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。

 （二）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。

 （三）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 |
| 三层交换机配置文件 | 7% | 结果评分-客观 |
| 网络安全设备配置与防护权重21% | 防火墙配置截图文件 | 7% | 结果评分-客观 |
| 网络流控系统配置截图文件 | 7% | 结果评分-客观 |
| 网络日志系统配置截图文件 | 7% | 结果评分-客观 |
| 第二阶段权重30% | 系统安全攻防及运维安全管控权重30% | 服务器加固配置 | 10% | 机考评分 |
| 服务器渗透配置 | 10% | 机考评分 |
| web应用防火墙配置 | 10% | 机考评分 |
| 第三阶段权重40% | 分组对抗权重40% | 防守成功，坚持到竞赛结束 | 10% | 机考评分 |
| 渗透成功（每渗透成功1队得2分） | 30% | 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。

（四）成绩复核与公布

1. 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。

2．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。竞赛成绩通过赛场显示屏和网络直播等方式进行实时公布。同时，在赛场及赛场外张贴纸质成绩。若有异议，经过规定程序仲裁后，按照仲裁结果公布比赛成绩。

# 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，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。

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。

参赛队由各省市负责参赛选手旅途及竞赛过程中的安全保障。

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。

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、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

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。

4. 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。

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。

2. 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。

3. 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。

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. 因参赛队伍原因造成重大安全事故的，取消其参赛资格。

3. 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。

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。

# 十四、竞赛须知

（一）参赛队须知

1. 各参赛队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. 各参赛队领队要坚决执行竞赛的各项规定，加强对参赛人员的管理，做好赛前准备工作，督促选手带好证件等竞赛相关材料。

3. 竞赛过程中，除参加当场次竞赛的选手、执行裁判员、现场工作人员和经批准的人员外，领队、指导教师及其他人员一律不得进入竞赛现场。

4. 参赛队若对竞赛过程有异议，在规定的时间内由领队向赛项仲裁工作组提出书面报告。

5. 对申诉的仲裁结果，领队要带头服从和执行，并做好选手工作。参赛选手不得因申诉或处理意见不服而停止竞赛，否则以弃权处理。

6. 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。

7. 参赛队领队应对本队参赛队员和指导教师的参赛期间安全负责，参赛学校须为参赛选手和指导教师购买意外保险。

8. 领队和指导教师应在赛后做好赛事总结和工作总结。

（二）指导教师须知

1.各参赛代表队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.各代表队领队要坚决执行竞赛的各项规定，加强对参赛人员的管理，做好赛前准备工作，督促选手带好证件等竞赛相关材料。

3.竞赛过程中，除参加当场次竞赛的选手、执行裁判员、现场工作人员和经批准的人员外，领队、指导教师及其他人员一律不得进入竞赛现场。

4.参赛代表队若对竞赛过程有异议，在规定的时间内由领队向赛项仲裁工作组提出书面报告。

5.对申诉的仲裁结果，领队要带头服从和执行，并做好选手工作。参赛选手不得因申诉或对处理意见不服而停止竞赛，否则以弃权处理。

6.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。

（三）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。

（四）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

本赛项在比赛过程中若出现有失公正或有关人员违规等现象，参赛队领队可在比赛结束后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。

# 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

赛项全程录像。

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、手工评卷等过程进行全程实况转播。

本赛况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

在大赛执委会的领导与监督下，赛后60日内向大赛执委会办公室提交资源转化方案，半年内完成资源转化工作。

（一）竞赛过程中获得的主要资源

1.竞赛样题、试题库；

2.竞赛技能考核评分案例；

3.考核环境描述；

4.竞赛过程音视频记录；

5.评委、裁判、专家点评；

6.优秀选手、指导教师访谈。

（二）资源转化基本方案与呈现形式

资源转化成果遵循行业标准,契合课程标准,突出技能特色,展现竞赛优势，形成满足职业教育教学需求、体现先进教学模式、反映职业教育先进水平的共享性职业教育教学资源。资源转化成果包含基本资源和拓展资源，充分体现本赛项技能考核特点：

1.基本资源：

基本资源按照技能概要、训练单元、训练资源三大模块设置：

（1）技能概要包括技能介绍、训练大纲、技能要点、评价指标等。

（2）训练单元按任务模块或技能模块组织设置，可包括演示文稿、操作流程演示视频/动画等。

（3）训练资源可包括教学方案、训练指导、作业/任务、实验/实训/实习资源等。训练资源模块可单独列出，也可融入各训练单元。

2.拓展资源：

拓展资源以反映技能特色为主，应用于各教学与训练环节，支持技能教学和学习过程，较为成熟的多样性辅助资源。例如：点评视频、访谈视频、试题库、案例库、素材资源库等。

（三）资源的技术标准

资源转化成果以文本文档、演示文稿、视频文件、Flash文件、图形/图像素材和网页型资源等：

1.文本文档：采用DOC或DOCX格式。文件制作所使用的软件版本不低于Microsoft Office 2003。

2.演示文稿：采用PPT或PPTX格式。文件制作所使用的软件版本不低于Microsoft Office 2003。尽可能少用宏，播放时不要出现宏脚本提示。

3.视频文件：采用MP4格式。录像环境光线充足、安静，衣着得体，语音清晰。

（1）视频压缩采用H.264(MPEG-4 Part10：profile=main, level=3.0)编码方式，码流率256 Kbps以上，帧率不低于25 fps，分辨率不低于720×576（4:3）或1024×576（16:9）。

（2）声音和画面要求同步，无交流声或其他杂音等缺陷，无明显失真、放音过冲、过弱。伴音清晰、饱满、圆润，无失真、噪声杂音干扰、音量忽大忽小现象。解说声与现场声、背景音乐无明显比例失调。音频信噪比不低于48 dB。

（3）字幕要使用符合国家标准的规范字，不出现繁体字、异体字(国家规定的除外)、错别字；字幕的字体、大小、色彩搭配、摆放位置、停留时间、出入屏方式力求与其他要素（画面、解说词、音乐）配合适当，不能破坏原有画面。

（4）Flash文件：文件制作所使用的软件版本不低于Flash 6.0。

（5）图形/图像素材：采用常见存储格式，如GIF、PNG、JPG等。彩色图像颜色数不低于真彩（24位色），灰度图像的灰度级不低于256级，屏幕分辨率不低于1024×768时，扫描图像的扫描分辨率不低于72 dpi。

（6）网页型资源：交互式仿真实训资源。兼容Microsoft IE、Google Chrome、Mozilla Firefox浏览器。避免出现大量的垃圾代码，使用网页编辑工具编辑网页，不可直接将Microsoft Word、WPS等文件内容粘贴到网页文件中。

（四）资源的提交方式与版权

赛项资源转化成果的版权由技能大赛执委会和赛项执委会共享。

（五）资源的使用与管理

资源转化成果的使用与管理由大赛执委会统一使用与管理，会同赛项承办单位、赛项有关专家，联系出版社编辑出版有关赛项试题库、岗位典型操作流程等精品资源。

（六）资源转化项的工作进程表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **一级资源项** | **二级资源项** | **内容简述** | **转化方式** | **进度安排** | **备注** |
| 风采展示 | 赛项宣传片 | 介绍大赛主题、目的、意义以及实施过程，突出展现参赛选手同台竞技的风采。 | 15分钟视频 | 赛后5天内完成 | 1.承办校比赛当天全程摄像，拍摄比赛各个阶段2. 承办校拍摄教师休息区和大屏展示区采集素材 |
| 获奖选手风采展示片 | 介绍选手日常学习、备赛、参赛、获奖等环节的感受。 | 10分钟视频 | 赛后5天内完成 | 1. 承办校9号闭幕式之后，访谈拍摄大赛一等奖参赛选手2.赛项执委会通知各个参赛选手留存日常训练视频，比赛当天提供给承办校用于剪辑 |
| 技能概要 | 技能介绍 | 介绍大赛相关技能 | 编写相关文本资料 | 赛后60天内完成 | 赛项专家组完成 |
| 训练大纲 | 介绍大赛训练过程要点 | 编写相关文本资料 | 赛后60天内完成 | 赛项专家组完成 |
| 评价指标 | 介绍大赛评价指标 | 编写相关文本资料 | 赛后60天内完成 | 赛项专家组完成 |
| 教学资源 | 网络空间安全基础 | 该门课程可作为中职网络与安全专业的基础入门课程，适合本专业全体学生学习 | 教材、文档、图片、视频、仿真课件等 | 赛后60天内完成 | 包括教学方案、训练指导、作业/任务、实验/实训/实习资源等。教学单元按任务模块或技能模块组织设置， 包括演示文稿、图片、操作流程演示视频、提供交互式仿真实训课件。 |
| 网络空间安全进阶 | 该门课程可作为中职信息安全的进阶课程，适合学有余力的本专业学生进一步加深学习 | 教材、文档、图片、视频、仿真课件等 | 赛后60天内完成 | 包括教学方案、训练指导、作业/任务、实验/实训/实习资源等。教学单元按任务模块或技能模块组织设置， 包括演示文稿、图片、操作流程演示视频、提供交互式仿真实训课件。 |
| 网络空间安全大赛项目解析 | 对2017年该赛项赛题进行解析，分析重点、难点。可供中职信息安全专业学校进行综合项目实训以及技能大赛训练使用 | 教材、文档、图片、视频、仿真课件等 | 赛后60天内完成 | 包括教学方案、训练指导、作业/任务、实验/实训/实习资源等。教学单元按任务模块或技能模块组织设置， 包括演示文稿、图片、操作流程演示视频、提供交互式仿真实训课件。 |

# 附件：样题

2017年全国职业院校技能大赛高职组

信息安全管理与评估赛项任务书（样题）

一、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。

二、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配置 | 任务一 | 网络平台搭建 | 9:00-13:30 | 60 |
| 任务二 | 网络安全设备配置与防护 | 240 |
| 第二阶段系统安全攻防及运维安全管控 | 任务一 | IIS安全加固与证书签发 | 30 |
| 任务二 | 数据库攻防与加固 | 40 |
| 任务三 | CSRF攻击 | 40 |
| 任务四 | XSS攻击 | 40 |
| 任务五 | 密码嗅探 | 40 |
| 任务六 | 文件包含攻击 | 40 |
| 任务七 | SQL注入攻击 | 40 |
| 任务八 | linux操作系统安全防护 | 30 |
| 中场收卷 | 13:30-14:00 |
| 第三阶段分组对抗 | 系统加固 | 14:00-14:15 | 100 |
| 系统攻防 | 14:15-15:00 | 300 |

三、赛项内容

假定各位选手是某公司的信息安全工程师，负责维护公司信息系统安全。你们需要完成三个阶段的任务，其中前两个阶段需要提交任务操作文档留存备案，所有文档需要存放在裁判组专门提供的U盘中。第三阶段是否提交文档，请根据现场具体题目要求。

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，并在“xx工位”文件夹下，建立“第一阶段”、“第二阶段”两个文件夹，赛题两个阶段的文档分别归类放置在对应的文件夹中。

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”文件夹下建立“第一阶段”、“第二阶段”两个文件夹。

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。

1.网络拓扑图



2.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-3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 |
| 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-2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 100 | x.x.x.x/x | 直连服务器区 | 见赛场IP参数表 |
| Vlan 110 | x.x.x.x/x | 直连用户区 | 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 |
| 网络日志系统DCBI | EthX | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| EthX | 无 | 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DCRS相连 | 见赛场IP参数表 |
| PC-3 | 无 | x.x.x.x/x | 与DCFW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 |  |
| 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。） |

3.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 |
| 无线交换机DCWS | https://192.168.1.254 | ETH0 | admin | Admin123 |
| 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 | ETH5 | admin | admin123 |
| 堡垒服务器DCST | http://192.168.1.100 | Eth0–Eth9 | 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）

提示：该阶段答案文档命名格式为：“第X阶段”-“任务X”-“任务名称”。

例：“第一阶段、任务二、网络安全设备配置与防护”的答案提交文档，文件名称为：第一阶段-任务二-网络安全设备配置与防护.doc或第一阶段-任务二-网络安全设备配置与防护.docx。

任务一：网络平台搭建（60分）

提示：需要提交所有设备配置文件，其中DCRS设备要求提供show run配置文件保存到WORD文档，DCFW、DCWS、WAF、DCBI设备需要提交配置过程截图存入WORD文档，并在截图中加配置说明。提交的答案保存到一个WORD文档中，标明题号，按顺序答题。

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”。 |

任务二：网络安全设备配置与防护（240分）

提示：需要提交所有设备配置文件，其中DCRS设备要求提供show run配置文件保存到WORD文档，DCFW、DCWS、WAF、DCBI设备需要提交配置过程截图存入WORD文档，并在截图中加以说明。请顺序答题，并标注题号。每个设备提交的答案各自保存到不同的WORD文档中（本任务可以保存5个WORD文档）。

例：“第一阶段、任务二、网络安全设备配置与防护”关于DCBI设备的答案提交文档，文件名称为：第一阶段-任务二-网络安全设备配置与防护-DCBI.doc或第一阶段-任务二-网络安全设备配置与防护-DCBI.docx。

1. 在公司总部的DCFW上配置，开启网络管理功能（SNMP），网管服务器连接在服务器区，IP地址是服务器区内第二个可用地址（服务器区IP地址段参考“赛场IP参数表”），community名字为public，网管软件对DCFW没有写权限。（6分）
2. 在公司总部的DCFW上配置，连接互联网的接口属于WAN安全域、连接内网的接口属于LAN安全域，开启DCFW的DDoS防护。（6分）
3. 在公司总部的DCFW上配置，仅允许通过HTTP方式访问DCFW，并且新增一个用户，用户名dcfw1234，密码dcfw1234，该用户只有查看配置权限，不具有添加配置或修改配置的权限。（6分）
4. 在公司总部的DCFW上配置，在上班时间（工作日的9:00-17:00）只允许公司员工访问内网资源。（6分）
5. 在公司总部的DCFW上配置，在上班时间如有事情需要访问网络，限制只有通过DCFW的WEB认证后才能访问互联网，且在连接网络一个小时后如果不重新认证则断开网络访问。（6分）
6. 在公司总部的DCFW上配置，使公司总部的DCST设备可以通过互联网被访问，从互联网访问的地址是公网地址的第三个可用地址（公网IP地址段参考“赛场IP参数表”），且仅允许PC-3通过互联网访问DCST设备。（6分）
7. 在公司总部的DCFW上配置，使内网所有用户网段和服务器区网段都可以通过DCFW外网接口IP地址访问互联网，但要求公司PC-1只能通过固定的公网地址的第四个可用地址（公网IP地址段参考“赛场IP参数表”）访问互联网。（6分）
8. 在公司总部的DCFW上配置，在内网接口上开启防护功能，每秒钟最大接收1000个ARP包，超过的将被丢弃。（6分）
9. 在公司总部的DCFW上配置，限制每个用户访问互联网时最大的会话数是1000，上网带宽最大是5M。（6分）
10. 在公司总部的DCFW上启用SSL VPN，使分支机构通过VPN拨入公司总部，访问内部的所有服务器资源。SSL VPN地址池x.x.x.x/x（具体IP地址参考“赛场IP参数表”）。（6分）
11. 在公司总部的DCBI上配置，增加非admin账户dcbi1234，密码dcbi1234，该账户仅用于用户查询设备的日志信息和统计信息。（6分）
12. 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。（6分）
13. 在公司总部的DCBI上配置，使DCBI能够通过邮件方式发送告警信息，邮件服务器在服务器区，IP地址是服务器区内第三个可用地址（服务器区IP地址段参考“赛场IP参数表”），端口号25，账号test，密码test。（6分）
14. 在公司总部的DCBI上配置，将DCBI的日志信息发送到日志服务器，日志服务器在服务器区，IP地址是服务器区内第四个可用地址（服务器区IP地址段参考“赛场IP参数表”），community名字public。（6分）
15. 在公司总部的DCBI上配置，监控工作日（每周一到周五）期间PC-1访问的URL中包含xunlei的HTTP访问记录，并且邮件发送告警。（6分）
16. 在公司总部的DCBI上配置，监控PC-2所在网段用户的即时聊天记录。（6分）
17. 在公司总部的DCBI上配置，监控内网所有用户的邮件收发访问记录。（6分）
18. 在公司总部的DCBI上配置，使DCBI可以通过交换机（DCRS）获得内网PC的MAC地址，并在记录日志时显示内网PC的MAC地址。（6分）
19. 在公司总部的DCRS上配置，配置设备enable密码，并且在登录设备时必须正确输入enable密码才能进入交换机的配置模式。（6分）
20. 在公司总部的DCRS上配置，在交换设备上开启SSH管理功能，用户名和密码都是DCN，并关闭设备的web管理方式，仅允许使用console、ssh和telnet方式管理设备。（6分）
21. 在公司总部的DCRS上配置，VLAN20的成员接口开启广播风暴抑制功能，参数设置为400pps。（6分）
22. 在公司总部的DCRS上配置，公司为了统一管理，通过SNMP技术使用网管软件对DCRS进行管理，配置只读字串为public , 读写字串为private，网管服务器连接在服务器区，IP地址是服务器区内第二个可用地址（服务器区IP地址段参考“赛场IP参数表”）。（6分）
23. 在公司总部的DCRS上配置，在DCRS上的Ethernet1/15-17端口开启ARP保护功能，防止PC发出网关欺骗报文。并在Ethernet1/19接口上配置，使MAC为00-FF-51-BE-AD-32的主机不能访问MAC地址为E1-B6-4C-25-6A-13的主机，其他主机访问正常。（6分）
24. 在公司总部的DCRS上配置，需要在交换机10接口上开启基于用户模式的认证，认证通过后才能访问网络，认证服务器连接在服务器区，IP地址是服务器区内第五个可用地址（服务器区IP地址段参考“赛场IP参数表”），radius key是123456。（6分）
25. 在公司总部的DCRS上配置，VLAN110用户可通过DHCP的方式获得IP地址，在交换机上配置DHCP Server，地址池名称为pool-vlan110，DNS地址为114.114.114.114和8.8.8.8，租期为2天，VLAN110网段最后20个可用地址（DHCP地址段参考“赛场IP参数表”）不能被动态分配出去。（6分）
26. 在公司总部的WAF上配置，公司内部有一台网站服务器直连到WAF，地址是DCRS上VLAN10网段内的第五个可用地址（VLAN10地址段参考“赛场IP参数表”），端口是8080，并将服务访问日志、WEB防护日志、服务监控日志信息发送syslog日志服务器，syslog日志服务器在服务器区，IP地址是服务器区内第六个可用地址（服务器区IP地址段参考“赛场IP参数表”），UDP的514端口。（6分）
27. 在公司总部的WAF上配置，将设备状态告警、服务状态告警信息通过邮件（发送到jiankongceshi@digitalchina.com）及短信方式(发送到13812345678)发送给管理员。（6分）
28. 在公司总部的WAF上配置，阻止常见的WEB攻击数据包访问到公司内网服务器。（6分）
29. 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：10秒钟超过3000次请求。（6分）
30. 在公司总部的WAF上配置，禁止公网IP地址（218.240.143.219）访问网站服务器，网站服务器地址是DCRS上VLAN10网段内的第五个可用地址（VLAN10地址段参考“赛场IP参数表”）。（6分）
31. 在公司总部的WAF上配置，对公司网站（服务器地址是DCRS上VLAN10网段内的第五个可用地址，VLAN10地址段参考“赛场IP参数表”）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。
32. 在公司总部的WAF上配置，禁止HTTP请求和应答中包含敏感字段“赛题”的报文经过WAF设备。（6分）
33. 使用无线控制器提供DHCP服务，动态分配IP地址和网关。（6分）
34. DCWS配置VLAN100为管理和通信VLAN, DHCP下发192.168.100.0/24地址，DNS:8.8.8.8，需要排除网关，地址租约为2天；网关使用最后一个可用IP地址，DCWS使用第一个地址作为管理地址,AC使用DHCP功能下发管理地址。（6分）
35. 设置协议802.11n 2.4G频段。（6分）
36. 设置SSID DCN，加密模式为wpa-personal,其口令为：chinaskill。（6分）
37. 设置SSID GUEST 不进行认证加密。（6分）
38. 配置所有无线接入用户相互隔离。（6分）
39. GUSET最多接入10个用户，并对GUEST网络进行流控，每用户上行1M，下行2M。（6分）
40. 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。（6分）
41. 第二阶段：系统安全攻防及运维安全管控（300分）

提示1：本阶段用到堡垒服务器DCST中的服务器场景，获得服务器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123456
* 执行ipconfig /all，即可获得服务器IP地址

Linux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root，密码是123456
* 执行ifconfig即可获得服务器IP地址

提示2：每个任务提交一个word文档，请在文档中标明题号，按顺序答题。将关键步骤和操作结果进行截屏，并辅以文字说明，保存到提交文档中。

提示3：文档命名格式为：“第X阶段”-“任务X”-“任务名称”。

例：“第二阶段、任务二”的答案提交文档，文件名称为：第二阶段-任务二-数据库攻防与加固.doc或第二阶段-任务二-数据库攻防与加固.docx

任务一：IIS安全加固与证书签发（30分）

任务描述：贵公司的IIS服务器并不是那么安全，很有可能会被境外黑客攻击，并且可以作为跳板攻入贵公司的内网，所以需要对IIS服务器进行加固，尤其是安全证书的签发是安全管理员必不可少的工作。

任务环境说明：

•Web服务器操作系统：windows2003 server；

•安装服务/工具1：Web服务，版本是IIS-6.0；

•安装服务/工具2：FTP服务，版本是IIS-6.0；

•win-wireshark操作系统：windows2003 server；

•安装服务/工具1：抓包工具，wireshark；

1. 配置Windows 防火墙，使IIS Web服务能够被访问，对配置进行截屏。（3分）
2. 使用windows 自带的防火墙加固IIS Web服务器的安全配置，使得Web服务只能被内网用户所在的网段访问，对加固配置进行截屏。（3分）
3. 为IIS Web服务器申请服务器证书，对申请摘要进行截屏。（3分）
4. 为IIS Web服务器颁发一年期服务器证书，对颁发过程进行截屏。（3分）
5. 将IIS服务器启动SSL安全通信，并安装服务器证书。使用win-wireshark虚拟机中的浏览器访问该Web服务进行测试。由于cn和IIS 的域名不一致，所以一定有警报弹出窗，请将该窗口截屏。（3分）
6. 将IIS 服务器启用客户端证书设置。使用win-wireshark虚拟机自带的浏览器访问该Web服务进行测试。将要求客户端提供证书的弹出页面截屏。（6分）
7. 为win-wireshark虚拟机申请CA证书。颁发该证书。对申请和颁发过程截屏。（6分）
8. 在win-wireshark虚拟机上安装CA证书。使用PC浏览器访问该Web服务进行测试，对操作过程截屏。（3分）

任务二：数据库攻防与加固 （40分）

任务描述：贵公司的很多服务都是用了MySQL服务器，但是MySQL服务器是个开源的服务器，有很多已知的漏洞，如果没有很好的进行补丁和安全配置，将会带来很大的灾难。

任务环境说明：

•xserver-mysql服务器操作系统：Redhat Linux AS5；

•安装服务/工具1：Web服务，版本Apache 2.2.23；

•安装服务/工具2：MySQL服务，版本5.0.22；

•安装服务/工具3：PHP服务，版本5.0.48；

•安装服务/工具4：Nmap服务，版本4.11；

1. 进入xserver-mysql, 加固MySQL服务器，使所有的访问能被审计，要求通过对mysqld 的启动项进行加固，对加固操作进行截屏。（4分）
2. 配置Linux 防火墙，允许MySQL服务能够被访问，要求规则中只包含端口项，对防火墙规则列表进行截屏。（4分）
3. 进入xserver-mysql，查看所有用户及权限，找到可以从任何IP地址访问的用户，对操作过程进行截屏。（8分）
4. 对题号3中的漏洞进行加固，设定该用户只能从公司PC-1访问，用grants 命令进行管理，并将加固过程截屏。（8分）
5. 检查xserver-mysql中的是否存在数据库匿名用户，如果存在数据库匿名用户，则删除该用户，将发现的数据库匿名用户信息以及删除过程进行截屏。（4分）
6. 改变默认MySQL管理员的名称，将系统的默认管理员root 改为admin，防止被列举，将执行过程进行截屏。（4分）
7. 禁止MySQL对本地文件进行存取，对mysqld 的启动项进行加固，将加固部分截屏。（4分）
8. 限制一般用户浏览其他用户数据库，对mysqld 的启动项进行加固，将加固部分截屏。（4分）

任务三：CSRF攻击（40分）

任务描述：贵公司的网站漏洞多多，CSRF（Cross-site request forgery跨站请求伪造）通过伪装来自受信任用户的请求来利用受信任的网站。这是黑客常用的手段之一，你需要了解他。

任务环境说明：

•xserver操作系统：Redhat Linux AS5；

•安装服务/工具1：Web服务，版本Apache 2.2.23；

•安装服务/工具2：MySQL服务，版本5.0.22；

•安装服务/工具3：PHP服务，版本5.0.48；

•安装服务/工具4：Nmap服务，版本4.11；

•metas2-lab-1操作系统：Redhat Linux AS5；

•安装服务/工具1：Web服务，版本Apache 2.2.23；

•安装服务/工具2：MySQL服务，版本5.0.22；

•安装服务/工具3：PHP服务，版本5.0.48；

•安装服务/工具4：Nmap服务，版本4.11；

•安装服务/工具5：telnet服务端，版本0.17-39-el5;

•安装服务/工具6：telnet客户端，版本0.17-39-el5；

•win-wireshark操作系统：windows2003 server；

•安装服务/工具1：抓包工具，wireshark；

1. 访问metas2-lab-1 "/"->"csrf"，分析登录的页面源程序，找到提交的变量名，并截屏。（4分）
2. 启动win-wireshark，启动桌面程序csrfp，设置完成后，启动wireshark设定过滤条件包含WEB协议和端口，并对抓取的数据包信息进行截屏。（8分）
3. 在监听数据中分析得到用户名和密码，并截屏。（8分）
4. 根据用户名和密码，登录进入“csrf”页面，进入"csrf攻防"页面，点击“源程序”，分析需要提交的引用变量名称，并截屏。（4分）
5. 在xserver中存在csrf恶意攻击程序test.php，请修改该恶意程序，使得登录用户密码为12erfgbn，对test.php修改过程进行截屏。（8分）
6. 在PC上执行csrf攻击，并截屏。（4分）
7. 在win-wireshark中启动csrpcheck程序，输入metas2-lab-1的地址，点击“测试”将返回结果截屏。（4分）

任务四：XSS攻击（40分）

任务描述：贵公司的网站漏洞多多，XSS漏洞是Web应用程序中最常见的漏洞之一。如果您的站点没有预防XSS漏洞的固定方法，那么就存在XSS漏洞。利用XSS漏洞的病毒在黑客圈里是最喜欢使用的手段之一，如果你不防备，你的网站将成为黑客的游乐场。

任务环境说明：

•xserver操作系统：Redhat Linux AS5；

•安装服务/工具1：Web服务，版本Apache 2.2.23；

•安装服务/工具2：MySQL服务，版本5.0.22；

•安装服务/工具3：PHP服务，版本5.0.48；

•安装服务/工具4：Nmap服务，版本4.11；

•metas2-lab-1操作系统：Redhat Linux AS5；

•安装服务/工具1：Web服务，版本Apache 2.2.23；

•安装服务/工具2：MySQL服务，版本5.0.22；

•安装服务/工具3：PHP服务，版本5.0.48；

•安装服务/工具4：Nmap服务，版本4.11；

•安装服务/工具5：telnet服务端，版本0.17-39-el5;

•安装服务/工具6：telnet客户端，版本0.17-39-el5；

•win-wireshark操作系统：windows2003 server；

•安装服务/工具1：抓包工具，wireshark；

1. 使用PC访问metas2-lab-1，"/"->"xss注入"，然后利用用户名"admin"、密码"password"登录。点击xxs存储，进入注入页面，然后做简单注入，使得能够弹出js对话框"444"，确认存在xss漏洞，并截屏。（4分）
2. 在xserver上有一段简单的php程序，名字为accept\_cookie.php，接受cookie，请读懂并找到存放接收cookie的文件，并用ls –l列出存放Cookie文件的全路径，如[ls –l /xx/xx/yy，xx是路径，yy是存放Cookie的文件名]，并截屏。（12分）
3. 对metas2-lab-1进行xss注入，注入可以窃取cookie的代码，该代码将所有浏览“xss存储”的用户访问cookie上传到xserver，由accept\_cookie.php 负责接收，将导入代码及反馈信息截屏。（8分）
4. 启动win-wireshark,启动桌面程序是xssp,输入metas2-lab-1 的IP地址，进入每隔6秒钟的一次访问，该访问其实就是先登录后浏览metas2-lab-1 的“xss存储”页面。通过xserver的accept\_cookie 程序，得到自动页面访问的cookie。将过程及结果进行截屏。（8分）
5. 通过修改PC的cookie，不输入用户名和密码直接进入<http://x.x.x.x/dcn/vulnerabilities/xss_s/?mpage=xss>，然后并截屏。要求本题截屏中包括自动浏览程序的用户名，否则无效，x.x.x.x是metas2-lab-1的IP地址。（8分）

任务五：密码嗅探（40分）

任务描述：你以为自己的密码很安全么？有一种局域网密码嗅探器，在你的电脑上运行便可获取局域网中任意一台电脑的账号密码，你的POP3、FTP、SMTP、NNTP、IMAP、TELNET、HTTP、IRC协议中的密码，都将公开于天下，你的秘密都会被别人发现。尽快解决它吧。

任务环境说明：

•虚拟机metas2-lab操作系统：Redhat Linux AS5；

•安装服务/工具1：Web服务，版本Apache 2.2.23；

•安装服务/工具2：MySQL服务，版本5.0.22；

•安装服务/工具3：PHP服务，版本5.0.48；

•安装服务/工具4：Nmap服务，版本4.11；

•安装服务/工具5：telnet服务端，版本0.17-39-el5;

•安装服务/工具6：telnet客户端，版本0.17-39-el5；

•安装服务/工具7：Vsftpd，版本2.0.5；

•虚拟机win-wireshark操作系统：windows2003 server；

•安装服务/工具1：抓包工具，wireshark；

1. 在win-wireshark启动wireshark，并且设定过滤条件为telnet，并启动telnetp程序，每1分钟访问1次metas2-lab的telnet 服务器，将过程进行截屏。（4分）
2. 在win-wireshark 用抓包工具捕获自动连接软件使用的telnet 用户和密码，然后退出telnetp程序，对整个执行过程进行截图。（8分）
3. 在win-wireshark 设定wireshark 的过滤条件是ftp。（4分）
4. 运行win-wireshark桌面上的ftp自动连接软件ftpp，在win-wireshark中用抓包工具捕获ftp 的用户名和密码并截图。（8分）
5. 在win-wireshark用浏览器访问80服务，访问“漏洞发现”,分析该页面的源码,指出用户名数据和密码数据提交的方法以及相应的变量名。（4分）
6. 在win-wireshar设定wireshark的过滤条件，包括WEB服务的协议和目标地址，截屏。（4分）
7. 运行在win-wireshar桌面上的Web自动连接软件httpp，用抓包工具捕获输入的管理用户名和密码并截图。（8分）

任务六：文件包含攻击（40分）

任务描述：你是不是经常从陌生文件中打开附件？那么你就可能会遭遇文件包含攻击。远程文件包含攻击Remote File Include，属于“代码注入”的一种，其原理就是注入一段用户能控制的脚本或代码，并让服务端执行。文件包含漏洞可能出现在JSP、PHP、ASP等语言中，原理都是一样的，你要解决它。

任务环境说明：

•xserver操作系统：Redhat Linux AS5；

•安装服务/工具1：Web服务，版本Apache 2.2.23；

•安装服务/工具2：MySQL服务，版本5.0.22；

•安装服务/工具3：PHP服务，版本5.0.48；

•安装服务/工具4：Nmap服务，版本4.11；

•虚拟机metas2-lab-1操作系统：Redhat Linux AS5；

•安装服务/工具1：Web服务，版本Apache 2.2.23；

•安装服务/工具2：MySQL服务，版本5.0.22；

•安装服务/工具3：PHP服务，版本5.0.48；

•安装服务/工具4：Nmap服务，版本4.11；

•安装服务/工具5：telnet服务端，版本0.17-39-el5;

•安装服务/工具6：telnet客户端，版本0.17-39-el5；

•虚拟机win-wireshark操作系统：windows2003 server；

•安装服务/工具1：抓包工具，wireshark；

1. Web访问metas2-lab-1，"/"->"文件包含"，进入登录页面，分析登录的页面源程序，找到提交的变量名，并截屏。（4分）
2. 在winxp-wireshark，启动桌面程序fileip，输入metas2-lab-1 的IP地址，点击“访问”，每隔6秒钟的一次访问登录，启动Wireshark，设定过滤条件包含Web协议和端口，并截屏。（8分）
3. 在监听数据中分析得到用户名和密码，并截屏。（4分）
4. 根据用户名密码，登录进入“文件包含”页面，通过文件包含漏洞获得metas2-lab-1的用户文件passwd，截屏必须包含URL。（8分）
5. 根据获得的用户名列表，从社会工程学密码破解原理，破解test1，test2，test3的密码，请写出这三个用户的SSH的登陆密码，都能通过SSH方式成功登陆，并截屏。（8分）
6. 进入“命令执行”攻击页，获得当前的网络连接信息并截屏。（8分）

任务七：SQL注入攻击（40分）

任务描述：SQL注入是从正常的WWW端口访问，而且表面看起来跟一般的Web页面访问没什么区别，所以市面的[防火墙](http://baike.baidu.com/view/3067.htm)都不会对SQL注入发出警报，如果你没查看ⅡS日志的习惯，可能被入侵很长时间都不会发觉。SQL注入的手法相当灵活，在注入的时候会碰到很多意外的情况，需要构造巧妙的SQL语句，从而成功获取想要的数据。你是猎人，他是狐狸，你们谁更厉害？

任务环境说明：

•操作系统：Windows 2003 Server；

•安装服务/工具1：Web网站；

•安装服务/工具2：数据库，版本SQL Server 2005；

1. 访问网站，并通过Acunetix Web Vulnerability Scanner 扫描器对其进行扫描，识别存在SQL注入风险以及注入点的URL，并截图。（4分）
2. 通过对注入点手工判断，根据报错信息或者输入’and 1=1 以及’and 1=2 比对返回不同结果确定是注入点 并截图。（4分）
3. Get型注入，使用sqlmap对注入点的URL进行注入测试，获得当前的数据库名称，并截图。（8分）
4. POST型注入，使用sqlmap对注入点的URL以及POST数据进行注入测试，获得所有数据库的名称及个数，并截图。（8分）
5. 登录认证型，在网站注册任意帐号，对后台指定的URL进行SQL注入测试，通过SQLMAP工具dump到管理员帐号admin的加密密码并截图 。（12分）
6. 对第五步获取的加密密码进行md5破解，破解成功后的使用admin 帐号进行登录，并截图。（4分）

任务八：Linux操作系统安全防护 （30分）

任务描述：贵公司的服务器以Linux居多，你不要说自己是Windows专家，Linux操作系统的安全防护是基本功，如果不会，那么请学好再来上班吧。

任务环境说明：

•操作系统：Redhat Linux AS5；

1. 修改ssh的配置文件，禁止root直接登录，退出所有账号，使用root直接ssh登录操作系统，将提示信息截图。（3分）
2. 修改密码策略配置文件，确保密码最小长度为8位，然后创建新账号，并赋予密码低于8位，将错误提示信息截图。（3分）
3. 修改/etc/pam.d/ system-auth文件，确保错误登录10次，锁定此账户10分钟，将配置截图。（3分）
4. 配置至少三个配置文件的umask值为027，将配置截图并说明是哪个配置文件。（3分）
5. 自编脚本，查找本机存在SUID与SGID的文件，并截图。（3分）
6. 自编脚本，查找本机存在的所有人均有写权限的目录，并截图。（3分）
7. 修改配置文件，将登录超时设置为10分钟，并截图。（3分）
8. 修改syslog.conf配置文件，将认证日志、邮件日志，备份存储到指定服务器，并截图。（3分）
9. 使用root帐号登录系统，创建一个UID为0的帐号，然后使用一行命令查找本系统UID为0的帐号有哪些，并截图。（6分）
10. 第三阶段：分组对抗（400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猛烈地攻击。

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：加固常规漏洞取得KEY值并提交到裁判服务器中（裁判服务器网址见现场发放的参数表）；

提示4：加固系统漏洞取得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。

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）。如果你的服务器FLAG被他人取得并提交到裁判服务器，那么只能马上结束比赛，离开赛场。

注意1：不允许关闭80端口，否则将判令停止比赛，第三阶段分数为0分；在系统加固时，可以根据需要重启服务；

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：不允许更改syslog的配置，不允许停止syslog服务，不允许关闭514端口。

注意4：仔细阅读裁判服务器登录界面的大赛规则。

漏洞列表

1. Web服务器包含SQL注入的漏洞，用户通过SQL注入的漏洞获取数据库表单KEY的内容。
2. Web服务器包含跨站的漏洞，用户通过跨站漏洞获取KEY的内容。
3. Web服务器包含表单提权漏洞，用户通过表单提权的漏洞进行获取KEY并进行提权。
4. Web服务器包含COOKIE漏洞，用户通过COOKIE的漏洞进行获取KEY并进行提权。
5. Web服务器包含文件上传漏洞，用户通过文件上传进行获取KEY并进行提权。
6. Web服务器包含文件包含漏洞，用户通过文件包含进行获取KEY并进行提权。
7. Web服务器提供用户下载相关已经抓获的数据包，要求攻击者通过分析获取KEY。
8. Web服务器提供用户下载相关加密文件，要求攻击者通过破解文件来获取KEY的内容。
9. Web服务器包含BASH漏洞，通过BASH漏洞进行提权获取KEY。
10. 操作系统提供的服务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。
11. 操作系统提供的服务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。
12. 操作系统提供SAMBA服务，要求用户找到服务的远程溢出的漏洞。
13. 操作系统提供VSFTPD服务，要求用户找到服务的远程溢出的漏洞。
14. AS5的ROOTKIT查杀，用户可以通过预留的rootkit远程渗透。
15. SSHD的后门，用户可以通过预留的SSH后门进行远程渗透。
16. 系统提供mysql服务，要求用户能够对root口令进行暴力破解获取弱口令，并进行提权。
17. 系统提供弱口令用户，要求用户能够检出弱口令用户，并根据描述提供相关的KEY。

（样题完）