全国职业院校技能大赛
赛项规程

一、赛项名称

赛项编号：GZ-2021038

赛项名称：信息安全管理与评估

英文名称：Information Security Management and Evaluation

赛项组别：高职组

赛项归属：电子信息大类

二、竞赛目的

（一）引领教学改革

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多万，2021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:

(一)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。

(二)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。

(三)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。

(四)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。

(五)参赛选手能够按照要求准确撰写工作总结。

(六)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。

(七)竞赛分值权重和时间分布

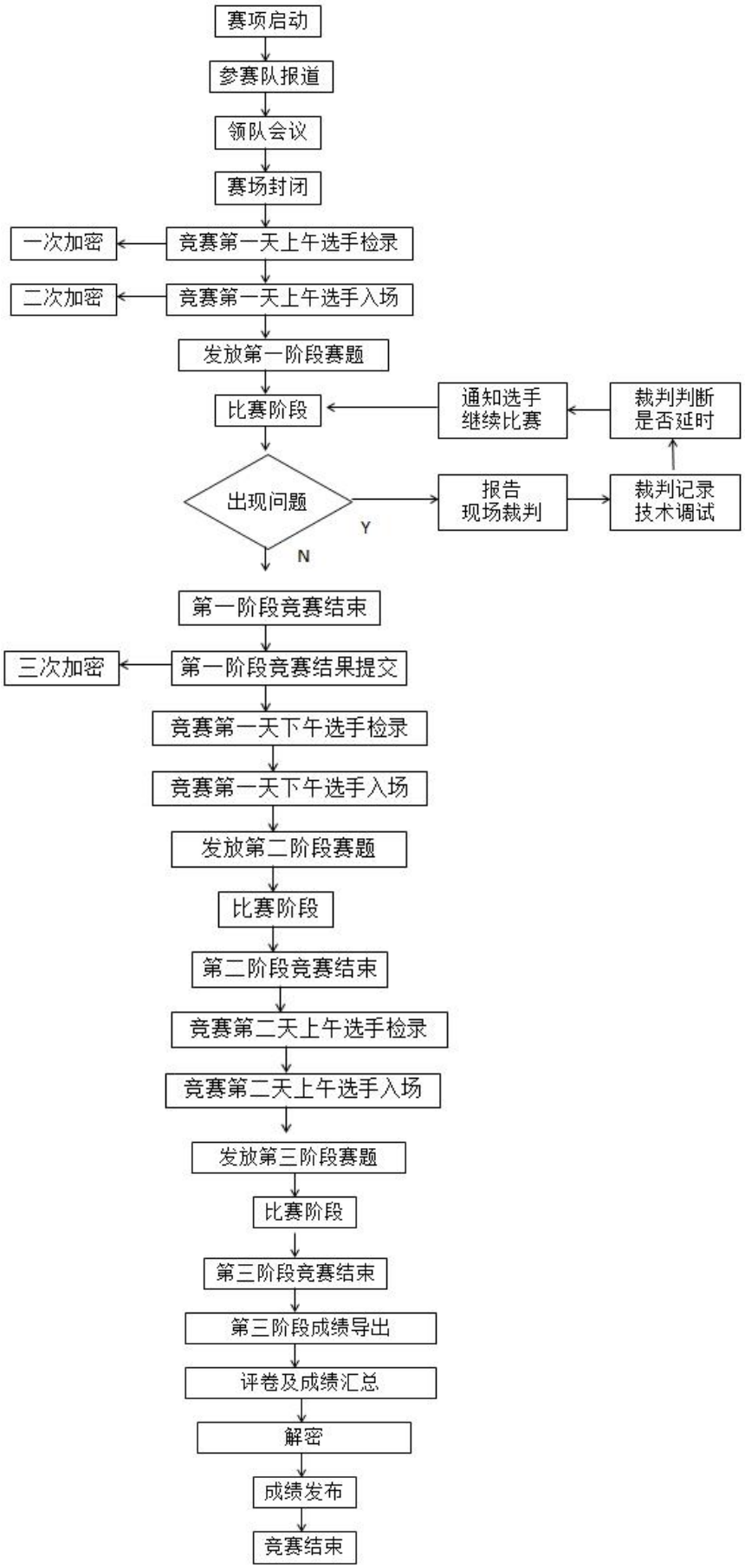
序号	内容模块	竞赛时间
第一阶段 权重 30%	网络平台搭建 权重 5%	竞赛第一天上午 150 分钟
	网络安全设备配置与防护 权重 25%	
第二阶段 权重 45%	系统安全攻防及运维安全管控 权重 45%	竞赛第一天下午 180 分钟
第三阶段 权重 25%	分组对抗 权重 25%	竞赛第二天上午 90 分钟

四、竞赛方式

本赛项为团体赛，以院校为单位组队参赛，不得跨校组队。每支参赛队由 3 名选手（设队长 1 名）和不超过 2 名指导教师组成。

五、竞赛流程

(一) 竞赛流程图


赛项启动
参赛队报道
领队会议
赛场封闭
竞赛第一天上午选手检录
一次加密
竞赛第一天上午选手入场
二次加密
发放第一阶段赛题
比赛阶段
通知选手
继续比赛
裁判判断
是否延时
出现问题
Y
报告
现场裁判
裁判记录
技术调试
N
第一阶段竞赛结束
第一阶段竞赛结果提交
三次加密
竞赛第一天下午选手检录
竞赛第一天下午选手入场
发放第二阶段赛题
比赛阶段
第二阶段竞赛结束
竞赛第二天上午选手检录
竞赛第二天上午选手入场
发放第三阶段赛题
比赛阶段
第三阶段竞赛结束
第三阶段成绩导出
评卷及成绩汇总
解密
成绩发布
竞赛结束

(二) 竞赛时间表

比赛限定在 2 天内进行，比赛场次为 3 场，赛项竞赛时间为 7 小时，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、监督仲裁报到	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、监督仲裁组	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、监督仲裁组	竞赛场地
	16: 00	返回酒店	参赛领队	竞赛场地
竞赛第 1 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，第一阶段赛题发放时间	参赛选手、现场裁判	竞赛场地
	09: 00-11: 30	第一阶段比赛时间	参赛选手、现场裁判	竞赛场地
	11: 30-12: 00	第一阶段结果提交时间，三次加密	参赛选手、现场裁判	竞赛场地
	13: 50-14: 00	第二阶段赛题发放时间	参赛选手、现场裁判	竞赛场地

	14:00-17:00	第二阶段正式比赛时间	参赛选手、现场裁判	竞赛场地
	17:00-17:30	第二阶段结果提交时间，三次加密	参赛选手、现场裁判	竞赛场地
竞赛第2天	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	第三阶段赛题发放时间	参赛选手、现场裁判	竞赛场地
	09:00-10:30	第三阶段比赛时间	参赛选手、现场裁判	竞赛场地
	10:30	比赛正式结束	参赛选手、现场裁判	竞赛场地
	10:30-评判完毕后	成绩汇总报送，成绩公布	评分裁判、裁判长、专家、监督仲裁	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

六、竞赛赛卷

(一)赛项执委会下设的命题专家组负责本赛项命题工作。

(二)本赛项为公开赛卷，竞赛赛卷距国赛开始日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）公布竞赛赛卷。

七、竞赛规则

(一)报名资格

参赛选手须为3名2021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2021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。

(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) 最终竞赛成绩经复核无误及裁判长、监督仲裁长签字确认后，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判分的原始材料和最终成绩等结果性材料经监督仲裁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。

(十二)赛事规定

1. 参赛选手和指导教师必须遵守赛项规程和相关要求。

2. 领队代表参赛省市负责管理参赛选手和指导教师，应当严格遵守大赛制度的有关规定，有效管理参赛选手和指导教师，遵守申诉与监督仲裁程序。

3. 专家、裁判、监督仲裁人员必须遵守《全国职业院校技能大赛制度汇编》，按制度规定履行职责，严格执行保密制度、遵守竞赛规程，公平公正履职。

4. 赛务工作人员必须遵守规章制度，认真负责履行有关赛务岗位职责。

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

（一）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15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

（二）赛项涉及知识点与技能点如下:

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、BGP、IPv6、组播等;
	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 VPN GRE Over IPSec L2TP Over IPSec IKE: PSK IKE: PKI SSL 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 人工智能在信息安全中的应用
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;

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	备注
1	三层虚拟化交换机	1	厂家提供
2	防火墙	1	厂家提供
3	堡垒服务器	1	厂家提供
4	WEB 应用防火墙	1	厂家提供
5	网络日志系统	1	厂家提供
6	无线交换机	1	厂家提供
7	无线接入点	1	厂家提供
8	PC 机 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	3	厂家提供

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，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18名，现场裁判5名，打分裁判10名，加密裁判3名。

序号	专业技术方向	知识能力要求	执裁、教学、工作经历	专业技术职称（职业资格等级）	人数
1	信息安全、网络安全、计算机网络、计算机应用方向	熟悉网络基础以及Windows和Linux操作系统，熟悉信息安全类别和主要攻防手段	具有相关专业教学工作经验或电子信息类省级或国家级执裁经验	工程师、高级工程师、副教授、教授	9
2	信息安全、计算机网络方向	熟悉网络基础以及Windows和Linux操作系统，熟悉系统加固及安全评估流程，熟悉信	具有相关专业教学工作经验或电子信息类省级或国家级执裁经验	工程师、高级工程师、副教授、教授	9

		息安全主要类别和主要攻防手段，熟练调试主流网络设备			
裁判总人数	18 名，现场裁判 5 名，打分裁判 10 名，加密裁判 3 名。				

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、监督仲裁员签字确认。

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	具体内容分值	评分细则和评分方式
第一阶段 权重 30%	网络平台搭建 权重 5%	防火墙、网络日志系统、web 应用防火墙、无线控制器、三层交换机，物理连接，命名、IP 地址等配置，满分 5 分；结果评分-客观；
	网络安全设备配置与防护 权重 25%	防火墙路由、安全策略、NAT、VPN 等配置和测试；网络日志系统网络检测、统计、告警等配置；web 应用防火墙防护策略、过滤策略、告警等配置；无线管理、无线网络设置、安全策略等配置和测试；三层交换机路由、二层安全等配置和测试；满分 25 分；结果评分-客观；

第二阶段 权重 45%	系统安全攻防及运维安全管控 权重 45%	MAC、DHCP、ARP、STP 等渗透测试及其加固; Windows、Linux 操作系统服务缓冲区溢出渗透测试及其加固; SQL 注入、命令注入、文件上传、目录穿越、XSS、CSRF、Cookie 盗用、会话劫持等漏洞渗透测试及其安全编程，人工智能在信息安全中的应用; 满分 45 分; 结果评分-客观/机考评分;
第三阶段 权重 25%	分组对抗 权重 25%	使用命令注入、文件上传、文件包含、远程代码执行、缓冲区溢出、系统后门等漏洞加固或渗透靶机，满分 25 分; 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。

比赛过程中禁止攻击裁判服务器和网络连接设备，按照现场 WAF（或网络设备）告警记录一经发现攻击行为根据《全国职业院校技能大赛制度汇编》奖惩办法中大赛惩处参赛选手部分，按扰乱赛场秩序处理，立即停止比赛，并给予选手取消成绩的处分，同时，责成所在学校按照学生违纪违规处分规定作出处理;

攻防阶段参赛选手需保护自己的靶机不被其他参赛选手攻击或入侵;

(四) 成绩复核与公布

1. 为保障成绩评判的准确性，监督仲裁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、监督仲裁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布。

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、赛场预案

1.竞赛过程中出现设备掉电、故障等意外时，现场裁判需及时确认情况，安排技术支持人员进行处理，现场裁判登记细情况，填写补时登记表，报裁判长批准后，可安排延长补足相应选手的比赛时间。

2.预留充足备用 PC 和设备，当出现设备掉电、故障等意外时经现场裁判确认后由赛场技术支持人员予以更换。

3.赛项出现重大突发事件和重大安全问题，经赛项执委会和专家组同意，暂停比赛，由涉及人员有关领导，如裁判长、领队、技术支持公司负责人、执委会领导和承办校负责人协调处理解决；如若不能处理，中止比赛，是否停赛由赛区执委会决定。事后，赛区执委会应向大赛执委会报告详细情况。

4.比赛期间发生意外伤害、意外疾病等重大事故，裁判长立即中止相关人员比赛，第一时间由承办校医疗站校医抢救，严重呼叫 120 送往医院。

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。

(一)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。

(二)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。

(三)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。

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。

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。承办单位赛前须按照赛项执委会要求排除安全隐患。

5．根据大赛组委会和当地教育厅要求做好疫情防控工作。

6．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。

7．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。

8．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。

9．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。

10．参赛选手进入赛位、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。

(四)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（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。

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。

(五)组队责任

1．各省、自治区、直辖市在组织参赛队时，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。

(六)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。

(七)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、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，可向赛项监督仲裁组提出申诉。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 小时之内向监督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。

赛项监督仲裁组在接到申诉报告后的 2 小时内组织复议，并及时将复议结果以书面形式告知申诉方。申诉方对复议结果仍有异议，可由省（市）领队向赛区监督仲裁委员会提出申诉。赛区监督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。

十九、资源转化

依照《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，赛后赛项执委会向大赛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	补充完善定期再版	赛后 90 天
拓展资源	案例库		文本资料	1	电子版资料	赛后 60 天
	试题库		文本资料	1	电子版资料	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。2021 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	2021 年 7 月	
2	师资培训第 1 期	2021 年 7 月	
3	师资培训第 2 期	2021 年 10 月	
4	研讨会第 2 期	2021 年 12 月	

2021 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

一、赛项时间

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 平台搭建与安全设备配置防护	任务 1	网络平台搭建	150 分钟	50
	任务 2	网络安全设备配置与防护		250
第二阶段 系统安全攻防及运维安全管控	任务 1	Linux Kernel 提权	180 分钟	30
	任务 2	扫描渗透测试		60
	任务 3	Linux/x86 系统 ShellCode 编程		60
	任务 4	Windows/x86 系统 ShellCode 编程		60
	任务 5	逆向分析和缓冲区溢出渗透测试		60
	任务 6	云服务安全渗透测试		60
	任务 7	二进制漏洞挖掘与利用		60
	任务 8	操作系统安全渗透测试		60
第三阶段 分组对抗	系统加固		90 分钟	250
	系统攻防			

三、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按裁判组专门提供的 U 盘中的“XXX-答题模板”提交答案。第二、三阶段请根据现场具体题目要求操作。

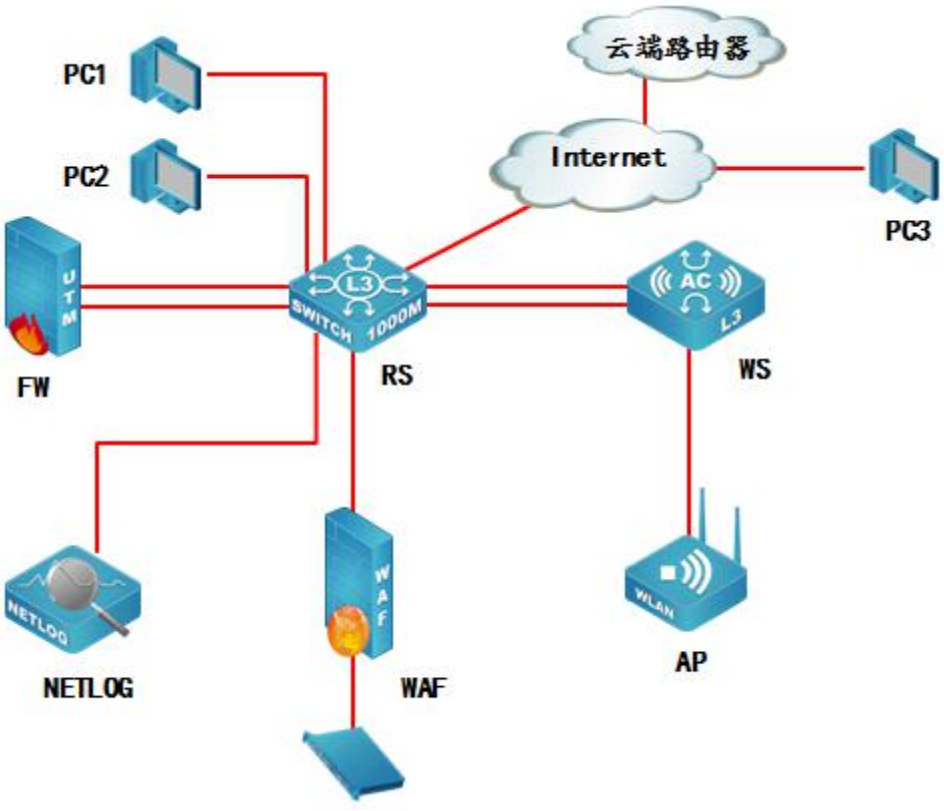
选手首先需要在U盘的根目录下建立一个名为“GWxx”的文件夹（xx用具体的工位号替代），赛题第一阶段所完成的“XXX-答题模板”放置在文件夹中。

例如：08工位，则需要在U盘根目录下建立“GW08”文件夹，并在“GW08”文件夹下直接放置第一个阶段的所有“XXX-答题模板”文件。

特别说明：只允许在根目录下的“GWxx”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。

(一)赛项环境设置

1. 网络拓扑图



2. IP 地址规划表

设备名称	接口	IP 地址	对端设备
防火墙 FW	ETH0/1-2	10.0.0.1/30（Trust 安全域）	RS
		218.5.18.1/27（untrust 安全域）	RS
		172.16.200.1/24	RS
	Tunnel 1	12.12.12.1/24	云端路由器
	SSL Pool	192.168.10.1/24 可用 IP 数量为 20	SSL VPN 地址池
三层交换机 RS	ETH1/0/4	-	WS ETH1/0/4
	ETH1/0/5	-	WS ETH1/0/5
	VLAN49 ETH1/0/1	10.0.0.2/30	FW
	VLAN50 ETH1/0/2	218.5.18.2/27	FW
	VLAN 51 ETH1/0/3	10.0.0.10/30	NETLOG
	VLAN 52 ETH1/0/22	172.16.100.1/24	WAF
	VLAN 10	172.16.10.1/24	无线 1
	VLAN 20	172.16.20.1/25	无线 2
	VLAN 30 ETH1/0/7-9	172.16.30.1/26	PC1
	VLAN 40 ETH1/0/10-12	192.168.40.1/24	PC2
	VLAN 100	192.168.100.1/24	WS
	VLAN 200	172.16.200.2/24	FW

	ETH1/0/24	-	INTERNET
无线控制器 WS	VLAN 100	192.168.100.254/24	RS
	无线管理 VLAN VLAN 101 ETH1/0/3	192.168.101.1/24	AP
日志服务器 NETLOG	ETH2	10.0.0.9/30	RS
WEB 应用防火墙 WAF	ETH2	172.16.100.2/24	
	ETH3		RS
堡垒服务器	-	-	WAF

（二） 第一阶段任务书（竞赛时间 150 分钟，共 300 分）

任务 1：网络平台搭建（50 分）

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 FW 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 RS 的名称进行配置，创建 VLAN 并将相应接口划入 VLAN。
3	根据网络拓扑图所示，按照 IP 地址参数表，对 RS 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 WS 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 NETLOG 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，对 WAF 的名称、各接口 IP 地址进行配置。

任务 2：网络安全设备配置与防护（250 分）

（1）总部核心交换机 RS 上开启 SSH 远程管理功能，本地认证用户名:2019ABC,密码：ABC2011;

（2）总部启用 MSTP 协议，NAME 为 ABC2011、 Revision-level 1，实例 1 中包括 VLAN10; 实例 2 中包括 VLAN20、要求两条链路负载分担,其中 VLAN10 业务数据在 E1/0/4 进行数据转发,要求 VLAN20 业务数据在 E1/0/5 进行数据转发，通过在 WS 两个端口设置 COST 值 2000000 实现;配置 RS 连接终端接口立即进入转发模式且在收到 BPDU 时自动关闭端口;防止从 WS 方向的根桥抢占攻击;

（3）尽可能加大总部核心交换机 RS 与防火墙 FW 之间的带宽;

（4）配置使总部 VLAN10，30，40 业务的用户访问 INTERNET 往返数据流都经过 FW 进行最严格的安全防护;

（5）总部核心交换机 RS 上实现 VLAN40 业务内部终端相互二层隔离，启用环路检测，环路检测的时间间隔为 10s，发现环路以后关闭该端口，恢复时间为 30 分钟;

（6）总部核心交换机 RS 检测到 VLAN40 中私设 DHCP 服务器关闭该端口;

（7）总部核心交换机 RS 开启某项功能,防止 VLAN40 下 ARP 欺骗攻击;

（8）总部核心交换机 RS 上实现访问控制，在 E1/0/14 端口上配置 MAC 地址为 00-03-0f-00-00-01 的主机不能访问 MAC 地址为 00-00-00-00-00-ff 的主机;

（9）2017 年勒索蠕虫病毒席卷全球，爆发了堪称史上最大规模的网络攻击，通过对总部核心交换机 RS 所有业务 VLAN 下配置访问控制策略实现双向安全防护;

（10）总部部署了一套网管系统实现对核心 RS 交换机进行管理，网管系统 IP 为：172.16.100.21，读团体值为：ABC2011，版本为 V2C，交换机 RS Trap 信息实时上报网管，当 MAC 地址发生变化时，也要立即通知网管发生的变化，每 35s 发送一次;

（11）总部核心交换机 RS 出口往返流量发送给 NETLOG，由 NETLOG 对收到的数据进行用户所要求的分析;

（12）为实现对防火墙的安全管理，在防火墙 FW 的 Trust 安全域开启 PING,HTTP，SNMP 功能，Untrust 安全域开启 SSH、HTTPS 功能;

（13）总部 VLAN 业务用户通过防火墙访问 Internet 时，轮询复用公网 IP:　218.5.18.9、218.5.18.10;

（14）项目二期要启用云端路由器，需要在总部防火墙FW上完成以下预配:

防火墙FW与云端路由器220.5.22.3建立GRE隧道，并使用IPSec保护GRE隧道，保证隧道两端2.2.2.2与VLAN20安全通信。

第一阶段　采用pre-share认证 加密算法:3DES;

第二阶段　采用ESP协议，　加密算法:3DES，预设共享秘钥:ABC2011

（15）配置RIP完成云端路由器2.2.2.2、FW、总部核心交换机VLAN20的连通性，使用MD5认证，密钥为ABC2011;

（16）总部核心交换机 RS 上使用某种技术，将 VLAN20 通过 RIP 连接云端路由器路由与本地其它用户访问 INTERNET 路由隔离;

（17）远程移动办公用户通过专线方式接入总部网络，在防火墙 FW 上配置，采用 SSL 方式实现仅允许对内网 VLAN 30 的访问，用户名密码均为 ABC2011，地址池参见地址表;

（18）出于安全考虑，无线用户移动性较强，无线用户访问 INTERNET 时需要采用认证，在防火墙上开启 WEB 认证，账号密码为 ABC2011;

（19）为了保证带宽的合理使用，通过流量管理功能将引流组应用数据流，上行带宽设置为 2M，下行带宽设置为 4M;

（20）为净化上网环境，要求在防火墙FW做相关配置，禁止无线用户周一至周五工作时间9：00-18：00的邮件内容中含有“病毒”、“赌博”的内容，且记录日志;

（21）NETLOG 配置应用及应用组“流媒体”，UDP 协议端口号范围 10817-10818，

在周一至周五 8：00-20：00 监控内网中所有用户的“流媒体”访问记录;

（22）NETLOG 配置对内网 ARP 数量进行统计，要求 30 分钟为一个周期;

（23）NETLOG 配置内网用户并发会话超过 1000，60 秒报警一次;

（24）NETLOG 配置监测到内网使用 RDP、Telnet 协议时，进行网页报警;

（25）NETLOG 配置开启用户识别功能，对内网所有 MAC 地址进行身份识别;

（26）NETLOG 配置统计出用户请求站点最多前 100 排名信息，发送到邮箱为 ABC2011@chinaskills.com;

（27）NETLOG 配置创建一个检查 2019-05-01 至 2019-05-05 这个时间段邮箱内容包含“密码”的关键字的任务;

（28）WAF 上配置开启爬虫防护功能，当爬虫标识为 360Spider，自动阻止该行为;

（29）WAF 上配置开启防护策略,将请求报头 DATA 自动重写为 DATE;

（30）WAF 上配置开启盗链防护功能，User-Agent 参数为 PPC Mac OS X 访问 www.ABC2011.com/index.php 时不进行检查;

（31）WAF 上配置开启错误代码屏蔽功能，屏蔽 404 错误代码;

（32）WAF 上配置阻止用户上传 ZIP、DOC、JPG、RAR 格式文件;

（33）WAF 上配置开启基本防护功能，阻止 SQL 注入、跨站脚本攻击;

（34）WAF 上配置编辑防护策略，要求客户机访问内部网站时，禁止访问*.bat 的文件;

（35）无线控制器 WS 上配置管理 VLAN 为 VLAN101,第二个地址作为 AP 的管理地址,配置 AP 二层手工注册并启用序列号认证，要求连接 AP 的接口禁止使用 TRUNK;

（36）无线控制器 WS 上配置 DHCP 服务，前十个地址为保留地址，无线用户 VLAN10,20，有线用户 VLAN 30,40 从 WS 上动态获取 IP 地址;

（37）在 NETWORK 下配置 SSID，需求如下:

1、设置 SSID ABC2019，VLAN10，加密模式为 wpa-persona1,其口令为 ABCE2011;

2、设置 SSID GUEST，VLAN20 不进行认证加密,做相应配置隐藏该 SSID;

（38）配置 SSID GUEST 每天早上 0 点到 6 点禁止终端接入;

（39）在 SSID ABC2019 下启动组播转单播功能，当某一组播组的成员个数超过 8 个时组播 M2U 功能就会关闭;

（40）开启 ARP 抑制功能,开启自动强制漫游功能、动态黑名单功能;

(三) 第二阶段任务书（竞赛时间 180 分钟，共 450 分）

任务 1: Linux Kernel 提权（30 分）

任务环境说明:

攻击机:

物理机: Windows7

物理机安装工具 1: Microsoft Visual Studio 2008

物理机安装工具 2: OllyICE

虚拟机 1: Ubuntu_Linux

虚拟机 1 安装工具 1: Python3/Python2

虚拟机 1 安装工具 2: GCC

虚拟机 1 安装工具 3: GDB

虚拟机 1 安装工具 4: Netcat

虚拟机 1 用户名: root，虚拟机 1 密码: 123456

虚拟机操作系统 2: CentOS_Linux

虚拟机 2 安装工具 1: GCC

虚拟机 2 安装工具 2: GDB

虚拟机 2 用户名: root，虚拟机 2 密码: 123456

靶机:

服务器场景 1: WindowsServer

服务器场景 1 的 FTP 下载服务用户名: anonymous

服务器场景 2: LinuxServer_01

任务内容:

1. 登录服务器场景 2 的 WebShell，通过相关手段打印当前系统相关信息（内核版本号、硬件架构、主机名称和操作系统类型等，命令并非查看文件），将操作命令作为 FLAG 值提交;
2. 根据操作命令回显将内核版本信息作为 FLAG 值提交;
3. 通过相关手段对服务器场景 2 上传提权文件，将上传成功提示单词全部作为 FLAG 值提交;
4. 在攻击机虚拟机 1 通过 NC 进行监听模式，输出交互信息或报错信息，并且监听 8081 端口，将命令作为 FLAG 值提交;
5. 从攻击机虚拟机 1 对服务器场景 2 通过相关手段进行 NC 连接，将成功回显后结果的正数第三排第四个单词作为 FLAG 值提交;
6. 从攻击机虚拟机 1 对服务器场景 2 通过相关手段进行 NC 成功连接后，通过相关命令修改 root 密码，将回显最后一行后三个单词作为 FLAG 值提交;
7. 修改密码后，查看/root/flag.txt 文件，将回显最后一行最后两个单词作为 FLAG 值提交;
8. 对当前用户进行提权，提权成功后，再次查看/root/flag.txt，将回显内容后两个单词作为 FLAG 值提交;

任务 2：扫描渗透测试（60 分）

任务环境说明:

攻击机:

物理机：Windows7

物理机安装工具 1：Microsoft Visual Studio 2008

物理机安装工具 2：OllyICE

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具 1：Python3/Python2

虚拟机 1 安装工具 2：GCC

虚拟机 1 安装工具 3：GDB

虚拟机 1 安装工具 4：Netcat

虚拟机 1 用户名：root，虚拟机 1 密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具 1：GCC

虚拟机 2 安装工具 2：GDB

虚拟机 2 用户名：root，虚拟机 2 密码：123456

靶机:

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 下载服务用户名：anonymous

服务器场景 2：Windows（不详）

任务内容:

1. 针对服务器场景 2 上传一句话木马,使用文件包含将 URL 中有关文件包含的目录、网页、参数字符串作为参数，通过 MD5 函数运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
2. 在服务器场景 2 的磁盘 C:\Windows 下找到 ABC_01.py 文件，将其上传到攻击机虚拟机 1 中,根据文件内注释要求的功能完善脚本，在完善脚本代码中，将 FLAG1 对应需要完善的内容字符串作为参数，通过 MD5 函数运算后，返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；

3. 继续编辑 ABC_01.py 文件，在完善脚本代码中，将 FLAG2 对应需要完善的内容字符串作为参数，通过 MD5 函数运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
4. 继续编辑 ABC_01.py 文件，在完善脚本代码中，将 FLAG3 对应需要完善的内容字符串作为参数，通过 MD5 函数运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
5. 继续编辑 ABC_01.py 文件，在完善脚本代码中，将 FLAG4 对应需要完善的内容字符串作为参数，通过 MD5 函数运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
6. 继续编辑 ABC_01.py 文件，在完善脚本代码中，将 FLAG5 对应需要完善的内容字符串作为参数，通过 MD5 函数运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
7. 继续编辑 ABC_01.py 文件，在完善脚本代码中，将 FLAG6 对应需要完善的内容字符串作为参数，通过 MD5 函数运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
8. 继续编辑 ABC_01.py 文件，在完善脚本代码中，将 FLAG7 对应需要完善的内容字符串作为参数，通过 MD5 函数运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；

9. 继续编辑 ABC_01.py 文件，在完善脚本代码中，将 FLAG8 对应需要完善的内容字符串作为参数，通过 MD5 函数运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
10. 在攻击机虚拟机 1 当中执行脚本 ABC_01.py，根据回显将扫描到的服务器场景 2 的端口输出信息字符串作为参数，通过 MD5 函数运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；

任务 3：Linux/x86 系统 ShellCode 编程（60 分）

任务环境说明：

攻击机：

物理机：Windows7

物理机安装工具 1：Microsoft Visual Studio 2008

物理机安装工具 2：OllyICE

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具 1：Python3/Python2

虚拟机 1 安装工具 2：GCC

虚拟机 1 安装工具 3：GDB

虚拟机 1 安装工具 4：Netcat

虚拟机 1 用户名：root，虚拟机 1 密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具 1：GCC

虚拟机 2 安装工具 2：GDB

虚拟机 2 用户名：root，虚拟机 2 密码：123456

靶机:

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 下载服务用户名：anonymous

服务器场景 2：LinuxServer

任务内容:

1. 使服务器场景 2 从服务器场景 1 的 FTP 服务器中下载文件 Shellcode_Linux01.c，编辑该 C 程序文件，对 Linux/x86 系统下 ShellCode 进行完善，填写该文件当中空缺的 FLAG01 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
2. 继续编辑该任务题目 1 中的 C 程序文件 Shellcode_Linux01.c，对 Linux/x86 系统下 ShellCode 进行完善，填写该文件当中空缺的 FLAG02 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交(形式:十六进制字符串);
3. 继续编辑该任务题目 1 中的 C 程序文件 Shellcode_Linux01.c，对 Linux/x86 系统下 ShellCode 进行完善，填写该文件当中空缺的 FLAG03 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交(形式:十六进制字符串);
4. 继续编辑该任务题目 1 中的 C 程序文件 Shellcode_Linux01.c，对 Linux/x86 系统下 ShellCode 进行完善，填写该文件当中空缺的 FLAG04 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交(形式:十六进制字符串);

5. 继续编辑该任务题目1中的C程序文件Shellcode_Linux01.c，对Linux/x86系统下ShellCode进行完善，填写该文件当中空缺的FLAG05字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交(形式:十六进制字符串);
6. 对以上题目中编辑的Shellcode_Linux01.c源文件进行编译、链接，使程序运行，将程序运行后，服务器场景2增加的服务端口号以字符串的形式作为参数，通过MD5函数运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；

任务4：Windows/x86系统ShellCode编程（60分）

任务环境说明:

攻击机:

物理机：Windows7

物理机安装工具1：Microsoft Visual Studio 2008

物理机安装工具2：OllyICE

虚拟机1：Ubuntu_Linux

虚拟机1安装工具1：Python3/Python2

虚拟机1安装工具2：GCC

虚拟机1安装工具3：GDB

虚拟机1安装工具4：Netcat

虚拟机1用户名：root，虚拟机1密码：123456

虚拟机操作系统2：CentOS_Linux

虚拟机2安装工具1：GCC

虚拟机 2 安装工具 2：GDB

虚拟机 2 用户名：root，虚拟机 2 密码：123456

靶机:

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 下载服务用户名：anonymous

服务器场景 2：Windows 7

任务内容:

1. 使服务器场景 2 从服务器场景 1 的 FTP 服务器中下载文件 Shellcode_Windows01.c，编辑该 C 程序文件，对 Windows/x86 系统下 ShellCode 进行完善，填写该文件当中空缺的 FLAG01 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
2. 继续编辑该任务题目 1 中的 C 程序文件 Shellcode_Windows01.c，对 Windows/x86 系统下 ShellCode 进行完善，填写该文件当中空缺的 FLAG02 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
3. 继续编辑该任务题目 1 中的 C 程序文件 Shellcode_Windows01.c，对 Windows/x86 系统下 ShellCode 进行完善，填写该文件当中空缺的 FLAG03 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
4. 继续编辑该任务题目 1 中的 C 程序文件 Shellcode_Windows01.c，对 Windows/x86 系统下 ShellCode

进行完善，填写该文件当中空缺的 FLAG04 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；

5. 继续编辑该任务题目 1 中的 C 程序文件 Shellcode_Windows01.c，对 Windows/x86 系统下 ShellCode 进行完善，填写该文件当中空缺的 FLAG05 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
6. 对以上题目中编辑的 Shellcode_Windows01.c 源文件进行编译、链接，使程序运行，将程序运行后，服务器场景 2 增加的服务端口号以字符串的形式作为参数，通过 MD5 函数运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；

任务 5：逆向分析和缓冲区溢出渗透测试（60 分）

任务环境说明:

攻击机:

物理机：Windows7

物理机安装工具 1：Microsoft Visual Studio 2008

物理机安装工具 2：OllyICE

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具 1：Python3/Python2

虚拟机 1 安装工具 2：GCC

虚拟机 1 安装工具 3：GDB

虚拟机 1 安装工具 4：Netcat

虚拟机 1 用户名：root，虚拟机 1 密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具 1：GCC

虚拟机 2 安装工具 2：GDB

虚拟机 2 用户名：root，虚拟机 2 密码：123456

靶机:

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 下载服务用户名：anonymous

服务器场景 2：LinuxServer

任务内容:

1. 从靶机服务器场景的 FTP 服务器中下载可执行文件 OverFlow01，通过攻击机调试工具，对以上可执行文件进行逆向分析;通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP:4444 端口进行渗透测试，获得靶机根路径下的文件 FLAG01 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）;
2. 从靶机服务器场景的 FTP 服务器中下载可执行文件 OverFlow01，通过攻击机调试工具，对以上可执行文件进行逆向分析;通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP:4444 端口进行渗透测试，获得靶机根路径下的文件 FLAG02 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）;

3. 从靶机服务器场景的 FTP 服务器中下载可执行文件 OverFlow01，通过攻击机调试工具，对以上可执行文件进行逆向分析;通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP: 4444 端口进行渗透测试，获得靶机根路径下的文件 FLAG03 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）;
4. 从靶机服务器场景的 FTP 服务器中下载可执行文件 OverFlow01，通过攻击机调试工具，对以上可执行文件进行逆向分析;通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP: 4444 端口进行渗透测试，获得靶机根路径下的文件 FLAG04 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）;
5. 从靶机服务器场景的 FTP 服务器中下载可执行文件 OverFlow01，通过攻击机调试工具，对以上可执行文件进行逆向分析;通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP: 4444 端口进行渗透测试，获得靶机根路径下的文件 FLAG05 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）;
6. 从靶机服务器场景的 FTP 服务器中下载可执行文件 OverFlow01，通过攻击机调试工具，对以上可执行文件进行逆向分析;通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP: 4444 端口进行渗透测试，获得靶机根路径下的文件 FLAG06 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）;

7. 从靶机服务器场景的 FTP 服务器中下载可执行文件 OverFlow01，通过攻击机调试工具，对以上可执行文件进行逆向分析;通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP:4444 端口进行渗透测试，获得靶机根路径下的文件 FLAG07 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）;
8. 从靶机服务器场景的 FTP 服务器中下载可执行文件 OverFlow01，通过攻击机调试工具，对以上可执行文件进行逆向分析;通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP:4444 端口进行渗透测试，获得靶机根路径下的文件 FLAG08 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）;
9. 从靶机服务器场景的 FTP 服务器中下载可执行文件 OverFlow01，通过攻击机调试工具，对以上可执行文件进行逆向分析;通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP:4444 端口进行渗透测试，获得靶机根路径下的文件 FLAG09 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）;
10. 从靶机服务器场景的 FTP 服务器中下载可执行文件 OverFlow01，通过攻击机调试工具，对以上可执行文件进行逆向分析;通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP:4444 端口进行渗透测试，获得靶机根路径下的文件 FLAG10 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）;

任务 6：云服务安全渗透测试（60 分）

攻击机:

物理机：Windows7

物理机安装工具 1：Microsoft Visual Studio 2008

物理机安装工具 2：OllyICE

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具 1：Python3/Python2

虚拟机 1 安装工具 2：GCC

虚拟机 1 安装工具 3：GDB

虚拟机 1 安装工具 4：Netcat

虚拟机 1 用户名：root，虚拟机 1 密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具 1：GCC

虚拟机 2 安装工具 2：GDB

虚拟机 2 用户名：root，虚拟机 2 密码：123456

靶机:

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 下载服务用户名：anonymous

服务器场景 2：Windows 7

任务内容:

1. 从靶机服务器场景 1 的 FTP 服务器中下载文件 pwn01.py，编辑该 Python 程序文件，使该程序实现通过靶机服务器场景 2 中某具有 0day 漏洞的云服务来获得该云服务器的最高权限；完善 pwn01.py 程序文件，填写该文件当中空缺的 FLAG01 字符

串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；

2. 继续编辑该任务题目 1 中的 Python 程序文件 pwn01.py，使该程序实现通过靶机服务器场景 2 中某具有 0day 漏洞的云服务来获得该云服务器的最高权限，填写该文件当中空缺的 FLAG02 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
3. 继续编辑该任务题目 1 中的 Python 程序文件 pwn01.py，使该程序实现通过靶机服务器场景 2 中某具有 0day 漏洞的云服务来获得该云服务器的最高权限，填写该文件当中空缺的 FLAG03 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
4. 继续编辑该任务题目 1 中的 Python 程序文件 pwn01.py，使该程序实现通过靶机服务器场景 2 中某具有 0day 漏洞的云服务来获得该云服务器的最高权限，填写该文件当中空缺的 FLAG04 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
5. 继续编辑该任务题目 1 中的 Python 程序文件 pwn01.py，使该程序实现通过靶机服务器场景 2 中某具有 0day 漏洞的云服务来获得该云服务器的最高权限，填写该文件当中空缺的 FLAG05 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
6. 通过 Python 程序解释器执行程序文件 pwn01.py，获得靶机服务器场景 2 中云服务器的最高权限，并打印云服务器根路径下

的文件 FLAG 当中的字符串的内容，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；

任务 7：二进制漏洞挖掘与利用

任务环境说明:

攻击机:

物理机：Windows7

物理机安装工具 1：Microsoft Visual Studio 2008

物理机安装工具 2：OllyICE

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具 1：Python3/Python2

虚拟机 1 安装工具 2：GCC

虚拟机 1 安装工具 3：GDB

虚拟机 1 安装工具 4：Netcat

虚拟机 1 用户名：root，虚拟机 1 密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具 1：GCC

虚拟机 2 安装工具 2：GDB

虚拟机 2 用户名：root，虚拟机 2 密码：123456

靶机:

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 下载服务用户名：anonymous

服务器场景 2：LinuxServer

任务内容:

1. 对靶机进行端口扫描探测，获取靶机开放的端口号，并将此端口号作为 FLAG1 的值进行提交（Flag 形式: flag{端口号}）
2. 通过 Netcat 对探测到的端口号进行监听并调试，在调试过程中获得 FLAG2 的值进行提交（Flag 形式: flag{xxxxxxxx}）
3. 通过浏览器直接访问 http://靶机 ip/pwn 即可下载到可执行文件 pwn，通过攻击机调试工具，对 pwn 文件进行调试分析，根据程序存在的漏洞编写攻击脚本,并利用此攻击脚本对服务器进行攻击，在服务器根目录下获取到 FLAG3 的值进行提交（Flag 形式: flag{xxxxxxxx}）

任务 8: 操作系统安全渗透测试

攻击机:

物理机: Windows7

物理机安装工具 1: Microsoft Visual Studio 2008

物理机安装工具 2: OllyICE

虚拟机 1: Ubuntu_Linux

虚拟机 1 安装工具 1: Python3/Python2

虚拟机 1 安装工具 2: GCC

虚拟机 1 安装工具 3: GDB

虚拟机 1 安装工具 4: Netcat

虚拟机 1 用户名: root，虚拟机 1 密码: 123456

虚拟机操作系统 2: CentOS_Linux

虚拟机 2 安装工具 1: GCC

虚拟机 2 安装工具 2：GDB

虚拟机 2 用户名：root，虚拟机 2 密码：123456

靶机:

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 下载服务用户名：anonymous

服务器场景 2：Windows XP

任务内容:

1. 从靶机服务器场景 1 的 FTP 服务器中下载文件 scan01.py，编辑该程序文件，使该程序实现从攻击机对靶机进行的 ARP 类型的主机在线探测渗透测试;
2. 从靶机服务器场景 1 的 FTP 服务器中下载文件 Penetrationtest01.py 或 Penetrationtest01.rb，编辑该程序文件，使该程序实现通过靶机服务器场景 2 的最高权限；完善 Penetrationtest01.py 或 Penetrationtest01.rb 程序文件，填写该文件当中空缺的 FLAG01 字符串，将该字符串作为 MD5 函数参数，经计算函数返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
3. 继续编辑该任务题目 1 中的程序文件 Penetrationtest01.py 或 Penetrationtest01.rb，使该程序实现通过靶机服务器场景 2 的最高权限；完善 Penetrationtest01.py 或 Penetrationtest01.rb 程序文件，填写该文件当中空缺的 FLAG02 字符串，将该字符串作为 MD5 函数参数，经计算函数返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；

4. 继续编辑该任务题目 1 中的程序文件 Penetrationtest01.py 或 Penetrationtest01.rb，使该程序实现通过靶机服务器场景 2 的最高权限；完善 Penetrationtest01.py 或 Penetrationtest01.rb 程序文件，填写该文件当中空缺的 FLAG03 字符串，将该字符串作为 MD5 函数参数，经计算函数返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
5. 继续编辑该任务题目 1 中的程序文件 Penetrationtest01.py 或 Penetrationtest01.rb，使该程序实现通过靶机服务器场景 2 的最高权限；完善 Penetrationtest01.py 或 Penetrationtest01.rb 程序文件，填写该文件当中空缺的 FLAG04 字符串，将该字符串作为 MD5 函数参数，经计算函数返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
6. 继续编辑该任务题目 1 中的程序文件 Penetrationtest01.py 或 Penetrationtest01.rb，使该程序实现通过靶机服务器场景 2 的最高权限；完善 Penetrationtest01.py 或 Penetrationtest01.rb 程序文件，填写该文件当中空缺的 FLAG05 字符串，将该字符串作为 MD5 函数参数，经计算函数返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
7. 继续编辑该任务题目 1 中的程序文件 Penetrationtest01.py 或 Penetrationtest01.rb，使该程序实现通过靶机服务器场景 2 的最高权限；完善 Penetrationtest01.py 或

Penetrationtest01.rb 程序文件，填写该文件当中空缺的 FLAG06 字符串，将该字符串作为 MD5 函数参数，经计算函数返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；

8. 通过 Python 或 Ruby 程序解释器执行程序文件 Penetrationtest01.py 或 Penetrationtest01.rb，获得靶机服务器场景 2 的最高权限，并打印靶机服务器场景 2 磁盘根路径下的文件 FLAG 当中的字符串的内容，将该字符串作为 MD5 函数参数，经计算函数返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；

（四） 第三阶段任务书（竞赛时间 90 分钟，共 250 分）

假定各位选手是某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 80、3306、5555，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 X 分，每当被对手提交 1 次自身靶机的 Flag 值扣除 X 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。