信息安全管理与评估赛项规程

一、赛项名称

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）检验教学成果

通过赛项检验参赛选手安全网络组建、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

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：

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。

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。

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。

参赛选手能够按照要求准确撰写工作总结。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	网络平台搭建，权重40%	3小时
第二阶段	网络安全设备配置，权重60%	

四、竞赛方式

本赛项为团体赛，可跨班级组队，每支队由 2 名选手（队长 1 名）

五、竞赛流程

根据学院下发通知，组织报名，两人一队，报名后根据赛程塞规进行备赛复习，按照参赛时间进行比赛。

六、竞赛时间

预定比赛时间：4 月 18 日，9:00-13:00

比赛限定在 1 天内进行，比赛场次根据报名情况而定，每场比赛 15 支队，赛项竞赛时间为 3 小时，时间为 9:00-12:00，参赛队小于 10 支队在 B111，大于 10 支队在 B313，具体安排如下：

日期	时间	事项	参加人员	地点
前一天	当天	安装软件布置赛场	裁判	B111/B313
竞赛当天	8:00	裁判进入比赛实训室	裁判	B111/B313
	8:20-8:30	选手抽签比赛场次	参赛选手、裁判	B111/B313
	8:30-8:40	选手抽签比赛工位	参赛选手、裁判	B111/B313
	8:40-8:50	参赛代表队就位，宣读考场纪律,抽取赛题参数表	参赛选手、裁判	B111/B313
	8:50-9:00	第一阶段和第二阶段赛题发放时间	参赛选手、裁判	B111/B313
	9:00-12:00	第一阶段和第二阶段正式比赛时间	参赛选手、裁判	B111/B313
	12:00-12:30	第一阶段与第二阶段比赛结果提交时间	参赛选手、裁判	B111/B313
	12:40	比赛正式结束	参赛选手、裁判	B111/B313
	13:00-评判完	成绩汇总报送，成绩公布	评分裁判	B111/B313

七、竞赛规则

（一）报名资格

参赛选手须为 2 名，三年制 2021 级、五年制 2019 级、三年制 2022 级、五年制 2020 级，计算机网络技术、移动通信技术、大数据技术等专业，符合以上条件即可报名。

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。

竞赛所需的硬件设备、系统软件和辅助工具由实训室统一安排，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。

参赛队自行决定选手分工、工作程序和时间安排。

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。

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。

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。

最终竞赛成绩经复核无误及裁判、教研室主任签字确认后，在指定地点，以纸质形式向全体参赛队进行公布。

本赛项分初赛和决赛，按30%比例进入决赛。

（二）参加竞赛的选手要求

1. 参赛选手必须遵守赛项规程和相关要求。

2. 领队代表参赛应当严格遵守大赛制度的有关规定。

3. 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

竞赛工位内设有一台台式电脑，软件为 eNSP 华为虚拟机、office 软件，截图软件。

九、赛项知识点

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等；
第二阶段	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；

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	eNSP	华为虚拟机

（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	华为CS6200交换机
2	防火墙	1	华为DCFW-1800E-N3002
3	堡垒服务器	1	华为DCST-6000B
4	WEB应用防火墙	1	华为DCFW-1800-WAF-LAB
5	网络日志系统	1	华为DCBI-NetLog-LAB
6	无线交换机	1	华为DCWS-6028
7	无线接入点	1	华为WL8200-I2

十一、成绩评定

（一）裁判评分方法

裁判组负责竞赛机考评分和结果性评分，由裁判负责竞赛全过程；

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	网络平台搭建 权重40%	网络规划文档	12%	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	28%	结果评分-客观
第二阶段	网络安全设备配置与防护 权重60%	防火墙相关配置截图文件	60%	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

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：

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。

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。

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。

系统自动启动违规检测，如有如下违规行为，给予扣分：

发现 FLAG 异常（譬如：删除、修改、杀进程等）；

关闭赛卷中要求开启的端口；

（二）成绩公布

竞赛成绩以复核无误后，经项目裁判、教研室主任审核签字后确定，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，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。

云南工程职业学院第五届“铭鼎杯”

大学生职业技能大赛组委会

2023年3月28日

附件

“信息安全管理与评估”样题

一、赛项时间

9:00-12:00，共计 3 小时，含赛题发放、收卷时间。

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	任务1	网络平台搭建	14:00-17:00	60
第二阶段 全设备配置防护	任务2	网络安全设备配置与防护		240

三、赛项内容

本次大赛，各位选手需要完成两个阶段的任务，其中第一个阶段需要按给定模板“XXX-答题模板”提交答案。第二阶段请根据现场具体题目要求操作。

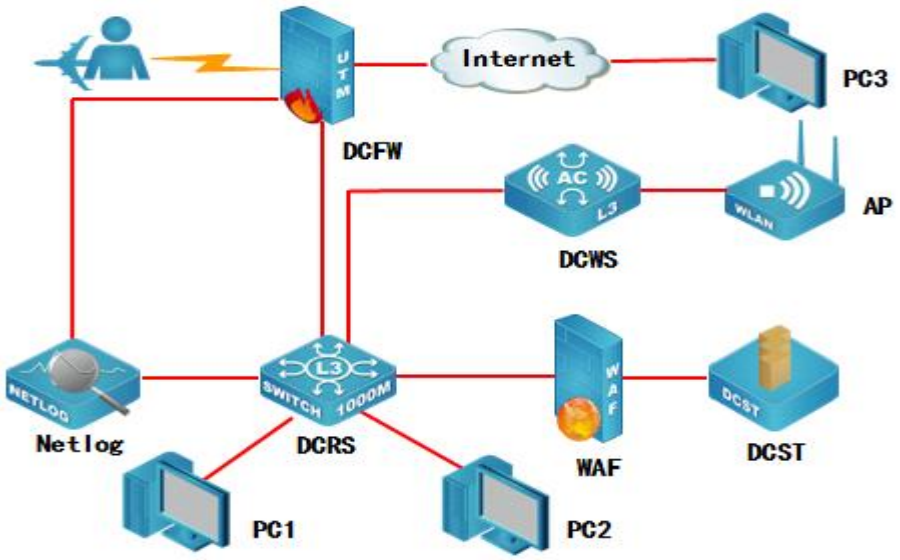
选手首先需要在桌面目录下建立一个名为“GWxx”的文件夹（xx 用具体的工位号替代），赛题第一阶段所完成的“XXX-答题模板”放置在文件夹中。

例如:08 工位,则需要在桌面目录下建立“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：只允许在桌面目录下的“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。

赛项环境设置网络拓扑图



IP地址规划表

设备名称	接口	IP地址	对端设备
防火墙DCFW	ETH0/2	10.0.0.1/30	DCRS
	ETH0/1	218.5.18.1/27	PC（218.5.18.2）
	L2TP	192.168.10.1/24 可用IP数量为20	L2TP地址池
	ETH0/3	10.0.0.10/30	Netlog
无线控制器DCWS	VLAN 1002 ETH1/0/1	10.0.0.6/30	DCRS
	ETH1/0/2		AP
	管理VLAN VLAN 100	192.168.100.254/24	
	VLAN 101 ETH1/0/11-24	192.168.101.1/24	
WEB应用防火墙 WAF	ETH2	172.16.100.2/24	DCST
	ETH3		DCRS
三层交换机DCRS	VLAN 1001 ETH1/0/2	10.0.0.2/30	DCFW
	VLAN 1002 ETH1/0/1	10.0.0.5/30	DCWS

	VLAN 10	172.16.10.1/24	无线2
	VLAN 20	172.16.20.1/25	无线1
	无线管理 VLAN VLAN 30	172.16.30.1/26	
	VLAN 40 ETH1/0/6-9	192.168.40.1/24	PC1
	管理VLAN VLAN 100	192.168.100.1/24	
	VLAN 200 ETH1/0/10-24	172.16.100.1/24	WAF、PC2
日志服务器Netlog	ETH2	10.0.0.9/30	DCFW
	ETH3		DCRS(ETH1/0/4)
堡垒服务器DCST	-	-	WAF

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	ETH5	admin	admin123
三层交换机DCRS	-	Console	-	-
无线交换机 DCWS	-	Console	-	-
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。			

四、竞赛题目

（一）任务1：网络平台搭建（60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	防火墙做必要配置实现内网对外网访问

（二）任务2：网络安全设备配置与防护（240分）

在 DCFW 上配置，连接 LAN 接口开启 PING,HTTP,HTTPS，telnet 功能,连接 Internet 接口开启 PING、HTTPS 功能;连接 netlog 接口为 DMZ 区域，合理配置策略，让内网用户能通过网络管理 netlog;

DCFW 配置 LOG，记录 NAT 会话， Server IP 为 172.16.100.10.开启 DCFW 上 snmp 服务，Server IP 172.16.100.10 团体字符为 public5;

DCFW 做相应配置,使用 L2TP 方式让外网移动办公用户能够实现对内网的访问，用户名密码为 dcn2015， VPN 地址池参见地址表；合理配置安全策略。

出于安全考虑，无线用户移动性较强，无线用户访问 Internet 是需要采用实名认证，在防火墙上开启 Web 认证，账号密码为 2015web;

为了合理利用网络出口带宽，需要对内网用户访问 Internet 进行流量控制，园区总出口带宽为 200M，对除无线用户以外的用户限制带宽，每天上午 9:00 到下午 6:00 每个 IP 最大下载速率为 2Mbps，上传速率为 1Mbps；

DCFW 上配置 NAT 功能，使 PC3 能够通过 Web 方式正常管理到 AC，端口号使用 6665;）合理配置安全策略;

在 DCFW 做相关配置要求防火墙能够记录每天 9:00-18:00 内网用户访问外网的 URL，保存在日志服务器；

配置防火墙 Web 外发信息控制策略，禁止内网无线用户到所有网站的 Web 外发信息控制；内网有线用户到外网网站 Web 外发信息控制，禁止外发关键字“攻击”“病毒”，信任值为 1，并记录相关日志。

DCFW 做相关配置要求内网用户不能登录 QQ 和 MSN；

DCFW 上配置限制内网用户访问 www.sohu.com 限制内网用户访问 URL 中带有 sohu 关键字的所有网站;

在 DCBI-netlog 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;要求对内网访问 Internet 全部应用进行记录日志;

在 DCBI-netlog 上配置，监控周一至周五 9：00-18：00 无线用户所在网段访问的 URL 中包含 sohu 的 HTTP 访问记录，并且邮件发送告警;

在 DCBI 上配置，添加内容规则，对于网站访问关键字包含“搜狐”的，记录并邮件报警；

在 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 IP 172.16.100.20，端口号 25，账号 test5dcn，密码 test5，当 DCBI 磁盘使用率超过 90%时发送一次报警；

在 DCBI 上配置，将 DCBI 的日志信息发送到日志服务器，日志服务器 IP 172.16.100.10，community 名字 public3；

在 DCBI 上配置，增加非 admin 账户 DCN2015，密码 dcbi5555，该账户仅用于用户查询设备的日志信息和统计信息；

DCBI 配置应用及应用组“P2P 下载”，UDP 协议端口号范围 40500-42000，在周一至周五 9：00-18：00 监控 LAN 中所有用户的“P2P 下载”访问记录并告警；

在 WAF 上配置，公司内部有一台网站服务器直连到 WAF，IP 地址是 172.16.100.30，端口是 8080，并将服务访问日志、Web 防护日志、服务监控日志发送至 syslog 日志服务器，syslog 日志服务器 IP 地址是 172.16.100.10，UDP 的 514 端口；

在公司总部的 WAF 上配置，将攻击告警、设备状态告警信息通过邮件（发送到 DCN@digitalchina.com）及短信方式(发送到 13913814949)发送给管理员；

在公司总部的 WAF 上配置，禁止公网 IP 地址（218.5.18.2）访问网站服务器，网站服务器 IP 地址是 172.16.100.30；

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；

在 WAF 上配置，开启基于 session cookie 的 CC 防护，最大请求数为 3000，超过进行阻止;

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 25 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;连接 PC1 的接口为专用接口，限定只允许 PC1 的 MAC 地址可以连接；

将连接 DCFW 的双向流量镜像至 Netlog 进行监控和分析；

开启防 ARP 扫描功能，单位时间内端口收到 ARP 数量超过 50 便认定是攻击，DOWN 掉此端口；

在公司总部的 DCRS 上配置端口环路检测（Loopback Detection），防止来自 VLAN200 接口下的单端口环路，并配置存在环路时的检测时间间隔为 30 秒，不存在环路时的检测时间间隔为 10 秒;

为了控制接入网络 PC，需要在交换 ETH1/0/10 口开启 DOT1X 认证，配置认证服务器，IP 地址是 172.16.100.40，radius key 是 dcn2015;

交换机开启远程管理，使用 SSH 方式账号为 DCN2015，密码为 555555;

VLAN20、VLAN30、VLAN10 用户采用动态获取 IP 地址方式，DHCP 服务器在 AC 上配置，前十个地址为保留地址，VLAN40 用户也动态获取 IP，DHCP server 为 DCFW;

在交换机上配置，在只允 VLAN200 用户在上班时间（周-到周五 8:00

到 18:00）内访问 VLAN100 段 IP;

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，VLAN30 用户的 ARP 阀值为 50;

为了防止 VLAN40 网段 arp 欺骗，需要在交换机上开启 ip dhcp snooping 并在接口下绑定用户;

在 DCRS 上配置，配置设备 enable 密码，密码为 dcn2015，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;

DCRS 上配置，VLAN40 的成员接口开启广播风暴抑制功能，参数设置为 2500pps;

AP 通过 option43 方式进行正常注册上线,hwtype 值为 59,AC 地址为管理 VLANIP;

设置 SSID DCN2015，VLAN10，加密模式为 wpa-personal,其口令为 GSdcn2015 的；设置 SSID dcntest ，VLAN20 不进行认证加密,做相应配置隐藏该 ssid;

dcntest 最多接入 20 个用户，用户间相互隔离，并对 dcntest 网络进行流控，上行速率 1Mbps，下行速率 2Mbps；

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;

通过配置防止多 AP 和 AC 相连时过多的安全认证连接而消耗 CPU 资源，检测到 AP 与 AC 在 10 分钟内建立连接 5 次就不再允许继续连接，两小时后恢复正常;

AC 开启 Web 管理，账号密码为 DCN2015；