2021 年职业院校技能大赛高职组
“信息安全管理与评估”赛项样题

一、 赛项时间

9:00-12:00/14:00-17:00，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 平台搭建与安全设备配置防护	任务 1	网络平台搭建	9:00-12:00	140
	任务 2	网络安全设备配置与防护		360
第二阶段 系统安全攻防及运维安全管控	任务 1	代码审计		150
	任务 2	恶意代码分析及利用		150
	任务 3	web 渗透		200

三、 赛项内容

本次大赛，各位选手需要完成两个个阶段的任务，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。

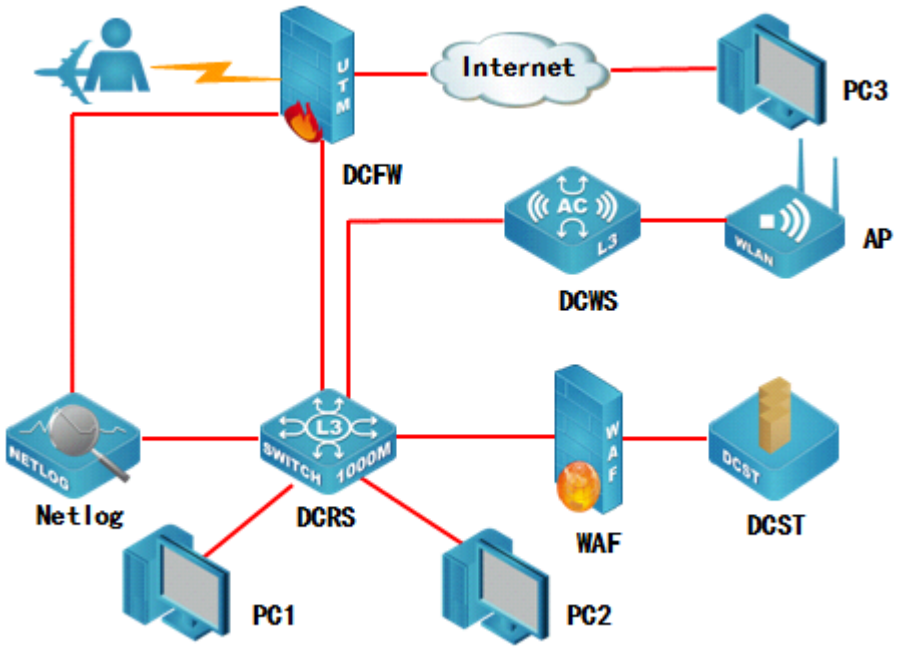
选手首先需要在 U 盘的根目录下建立一个名为“GWxx”的文件夹(xx 用具体的工位号替代)，赛题第一阶段和第二阶段所完成的“XXX-答题模板”放置在文件夹中。

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 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

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
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。			

（二） 第一阶段任务书（500 分）

任务一：网络平台搭建（140 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

任务 2：网络安全设备配置与防护（360 分）

DCFW：

1. 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；
2. 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 public；
3. 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 DCN2019， VPN 地址池参见地址表；合理配置安全策略。
4. 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 2019WEB；
5. 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，对无线用户用户限制带宽，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；
6. 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 5，并记录相关日志。
7. 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 1000；

Netlog：

8. 公司总部 LAN 中用户访问网页中带有“mp3”、“youku”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；
9. DCBI 监控 LAN 中 VLAN20 所有用户的聊天信息并做记录；
10. DCBI 配置相关参数，带宽控制设置成监控和统计；

WAF：

11. 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 256，防止缓冲区溢出攻击。
12. 在公司总部的 WAF 上配置，编辑防护策略，要求客户机访问网站时，禁止访问*.exe 的文件。
13. 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”和“答案”的报文经过 WAF 设备。

DCRS：

14. 配置认证服务器，IP 地址是 192.168.2.100，radius key 是 dcn2018；
15. 在公司总部的 DCRS 上配置，需要在交换机 E1/0/21 接口上开启基于 MAC 地址模式的认证，认证通过后才能访问网络；
16. 配置公司总部的 DCRS，通过 DCP（Dynamic CPU Protection）策略，防止 DCRS 受到来自于全部物理接口的 DOS（Denial Of Service）攻击，每秒最多 30 个包；
17. 为减少内部 ARP 广播询问 VLAN 网关地址，在全局下配置 DCRS 每隔 300S 发送免费 ARP；
18. 要求在公司总部的 DCRS,实现 E1/0/10-13 的业务主机不能相互访问；
19. 要求在公司总部的 DCRS,实现 E1/0/14 口 MAC 为 00-03-0f-00-00-01 不能访问 MAC 00-00-00-00-00-ff；
20. 要求在公司总部的 DCRS 运行 BPDU Guard，防止 E1/0/15 口接入网络设备形成环路影响核心交换机性能。

DCWS：

21. 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；
22. 设置 SSID DCN2019,VLAN10,加密模式为 wpa-personal,其口令为 PASSWORD 的；设置 SSID dcntest ,VLAN20 不进行认证加密,做相应配置隐藏该 ssid；
23. 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；
24. 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；
25. AC 开启 Web 管理，账号密码为 DCN2019；
26. Network 模式下限制 SSID DCN2019 每天早上 8 点到 18 点禁止终端接入；
27. 为了防止 AP 发射功率过大影响其他 AP,把 AP 功率设置 80；
28. 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；
29. 防止非法 AP 假冒合法 SSID，开启 AP 威胁检测功能；

30. 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；

（三） 第二阶段任务书（500 分）

任务 1：代码审计(150 分)

任务环境说明：

DCST：
服务器场景：18web
服务器场景操作系统：Microsoft Windows XP
服务器场景安装服务：apache+php+mysql 集成环境

任务内容：

1. 访问 http://靶机 IP:8000（打开靶机控制台，在登陆界面按 5 次 shift 获取靶机 IP），通过审计第一题的代码并利用获取到隐藏的 flag，并对 flag 进行截图。
2. 访问 http://靶机 IP:8000,通过审计第二题的代码并利用获取到隐藏的 flag，并对 flag 进行截图。
3. 访问 http://靶机 IP:8000,通过审计第三题的代码并利用获取到隐藏的 flag，并对 flag 进行截图。
4. 访问 http://靶机 IP:8000,通过审计第四题的代码并利用获取到隐藏的 flag，并对 flag 进行截图。
5. 访问 http://靶机 IP:8000,通过审计第五题的代码并利用获取到隐藏的 flag，并对 flag 进行截图。

任务 2：恶意代码分析及利用(150 分)

任务环境说明：

DCST：
服务器场景：18shell
服务器场景操作系统：Centos6.5
服务器场景安装服务：apache+php+mysql

任务内容：

1. 通过靶机控制台获取靶机 IP 地址，访问 http://靶机 IP,下载靶机源码并进行代码审计，找到黑客上传的木马，并对木马文件进行截图。
2. 对找到的木马进行利用，查看当前用户权限，并对回显结果进行截图。
3. 通过木马找到 flag 文件的位置(flag 文件名中包含乱码)，并对 flag 文件名进行截图。
4. 通过木马查看 flag 文件内容，并对 flag 值进行截图。
5. 编写脚本对加密的 flag 进行解密(不限制脚本语言)，获得正确的 flag(flag 格式为 flag{*********})，对解密脚本及解密后的 flag 进行截图。

任务 3：web 渗透(200 分)

任务环境说明：

DCST:
服务器场景：18web
服务器场景操作系统：Microsoft Windows XP
服务器场景安装服务：apache+php+mysql 集成环境

任务内容：

1. 访问 http://靶机 IP:8100（打开靶机控制台，在登陆界面按 5 次 shift 获取靶机 IP），绕过限制进行上传，获取到 flag1，并对 flag1 进行截图。
2. 访问 http://靶机 IP:8100，根据题 1 结果给出的提示获取 flag2，并对 flag2 进行截图。
3. 访问 http://靶机 IP:8100，根据题 2 结果给出的提示获取 flag3，并对 flag3 进行截图。
4. 访问 http://靶机 IP:8100，根据题 3 结果给出的提示获取 flag4，并对 flag4 进行截图。
5. 访问 http://靶机 IP:8100，根据题 4 结果给出的提示获取 flag5，并对 flag5 进行截图。