2018年山东省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

一、 赛项时间

8:30-13:00，共计4小时30分钟，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	8:30-11:30	60
	任务2	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1	代码审计		100
	任务2	恶意代码分析及利用		150
	任务3	web渗透		150
中场收卷			30分钟	
第三阶段 分组对抗	系统加固		15分钟	300
	系统攻防		45分钟	

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。

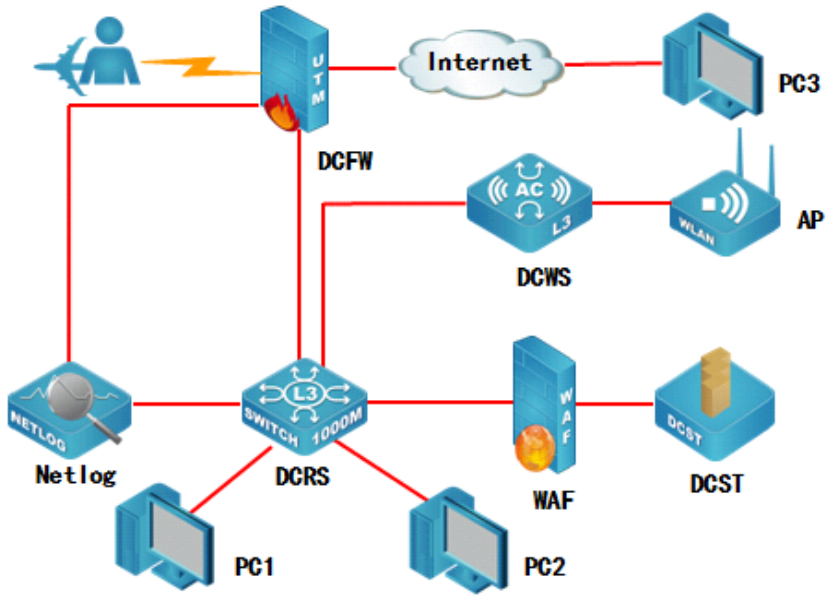
选手首先需要在U盘的根目录下建立一个名为“GWxx”的文件夹(xx用具体的工位号替代)，赛题第一阶段所完成的“XXX-答题模板”放置在文件夹中。

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 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（300 分）

任务一：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

任务 2：网络安全设备配置与防护（240 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 dcn2018， 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 2018web；
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；

Netlog：

6. 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；
7. DCBI 监控 LAN 中 VLAN20 所有用户的聊天信息并做记录；
8. DCBI 监控周一至周五工作时间 VLAN20 用户使用“迅雷”的记录，每天工作时间为 9:00-18:00；

WAF：

9. 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。
10. 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。

11. 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：

12. 配置认证服务器，IP 地址是 192.168.2.100，radius key 是 dcn2018；
13. 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；
14. 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；
15. 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；

DCWS：

16. 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；
17. 设置 SSID DCN2011,VLAN10,加密模式为 wpa-personal,其口令为 GSdcn2011 的;设置 SSID dcntest ,VLAN20 不进行认证加密,做相应配置隐藏该 ssid；
18. 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；
19. 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；
20. AC 开启 Web 管理，账号密码为 DCN2011；

（三） 第二阶段任务书（400 分）

任务 1：代码审计（100 分）

任务环境说明：

SDC：
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,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：

SDC:
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. 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（150 分）

任务环境说明：

SDC:
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,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。

（四） 第三阶段任务书（300 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。

十五分钟之后，各位选手将真正进入分组对抗环节。

注意事项：

注意 1：任何时候不能关闭服务器 80 端口，要求站点能够被正常访问，网站正常业务不能受到影响，否则后台强制重置靶机并扣 50 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。

注意 5：靶机的 Flag 值存放在/flag 文件内容当中。

注意 6：每队初始分 100 分，每提交 1 次对手靶机的 Flag 值增加 10 分，每当被对手提交 1 次自身靶机的 Flag 值扣除 10 分，每个对手靶机的 Flag 值只能提交一次。

注意 7：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 8：本阶段最高得分为 300 分，如得分高于 300 分，则取 300 分作为最终成绩；最低分不低于 0 分，若得分低于 0 分，则取 0 分作为最终成绩。

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。

漏洞列表：

1. 靶机上的网站存在后门，要求选手进行代码审计，找到的相关漏洞，利用此漏洞获取一定权限。
2. 靶机上的网站存在文件上传漏洞，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. 操作系统提供的服务存在未授权访问，要求选手利用相关漏洞，获取一定权限。
4. 靶机中存在一些后门，选手可以找到此后门，并利用预留的后门直接获取 flag。

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。