2019—2020年度广东省职业院校学生专业技能大赛

高职组“信息安全管理与评估”赛项任务书

样题

# 赛项时间

XX:XX- XX:XX，含赛题发放、收卷及午餐时间。

# 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 | XX:XX |  |
|  | 任务2 | 网络安全设备配置与防护 |  |  |
| 第二阶段  系统安全攻防及运维安全管控 | 任务1 | Web渗透测试 |  |  |
|  | 任务2 | mysql数据库攻防与加固 |  |  |
|  | 任务3 | 文件包含漏洞攻防 |  |  |

# 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、二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。

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。

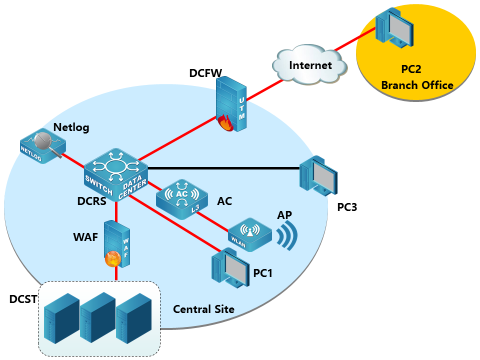
例如：08工位，则需要在U盘根目录下建立“GW08”文件夹，并在“GW08”文件夹下直接放置第一个阶段的所有“XXX-答题模板”文件。

**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。**

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。

### 网络拓扑图



### 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 | Eth1 | 200.1.1.1/24 | 与PC-2相连 | - |
| 地址池 | 172.16.10.1 | SSL VPN地址池 | 10,网关为254 |
| Eth2 | 192.168.2.2/24 | 与DCRS相连 | - |
| 无线交换机DCWS | Eth24 | 192.168.66.253/24 | 与DCRS相连 | - |
| Eth23 | - | AP | - |
| WEB应用防火墙WAF | Eth2 | - | 与DCRS相连 | - |
| Eth3 | - | 与DCST相连 | - |
| 三层交换机DCRS | Vlan1 Eth1 | 192.168.1.254/24 | 与DCBI相连 | - |
| Vlan2 Eth2 | 192.168.2.1/24 | 与DCFW相连 | - |
| Vlan 10 Eth3 | 192.168.10.254/24 | 与WAF相连 | - |
| Vlan 20 Eth4 | 192.168.20.254/24 | 与PC-1所在用户区相连 | - |
| Vlan 30 Eth5 | 192.168.30.254/24 | 与PC-3所在用户区相连 | - |
| Vlan 66 Eth6 | 192.168.66.254/24 | DCWS | - |
| 网络日志系统DCBI | Eth1 | 192.168.40.253/24 | 与DCRS相连 | - |
| 堡垒服务器DCST | Eth1 | 192.168.1.100/24 | 与WAF相连 | - |
| PC-1 | 无 | 192.168.20.1/24 | 与DCRS相连 | - |
| PC-2 | 无 | 200.1.1.2/24 | 与DCFW相连 | - |
| PC-3 | 无 | 192.168.30.1/24 | 与DCFW相连 | - |
| 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。） | | | |

### 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 | - | Console | - | - |
| 无线交换机DCWS | - | Console | - | - |
| 堡垒服务器DCST | http://192.168.1.100 | Eth1 | 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（400分）**

该阶段需要提交配置或截图文档，命名如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| **阶段** | **任务** | **序号** | **文档名称** |
| 第一阶段 | 任务1 | 1 | 任务1 |
| 2 | 赛场IP参数表 |
| 任务2 | 3 | 任务2-DCFW |
| 4 | 任务2-DCBI |
| 5 | 任务2-WAF |
| 6 | 任务2-DCRS |
| 7 | 任务2-DCWS |

### 任务1：网络平台搭建（100分）

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，在DCWS上创建相应的VLAN，并将相应接口划入VLAN,对DCWS的管理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。 |

### 任务2：网络安全设备配置与防护（300分）

#### DCFW:

1. 在总公司的DCFW根据题意配置Trust,Untruct,VPNhub区域，并配置区域之间的放行策略；
2. 配置路由，通往internet的方向配置默认路由，使用下一跳IP为PC2,通往内部路由配置静态主类汇总路由；
3. 配置动态NAT，对应关系如下：

VLAN20用户映射为200.1.1.20；

VLAN30用户映射为200.1.1.30；

1. DCFW连接Internet的区域上配置以下攻击防护：

启以下Flood防护：

ICMP洪水攻击防护，警戒值2000，动作丢弃；

UDP供水攻击防护，警戒值1500，动作丢弃；

SYN洪水攻击防护，源警戒值5000，目的警戒值基于IP 2000，动作丢弃；

开启以下DOS防护：

Ping of Death攻击防护；

Teardrop攻击防护；

IP选项，动作丢弃；

ICMP大包攻击防护，警戒值2048，动作丢弃；

1. 总公司DCFW配置SSLVPN，建立用户dcn01，密码dcn01，要求连接Internet PC2可以拨入，服务端口为9998，SSLVPN地址池参见地址表；

#### DCBI:

1. 在公司总部的DCBI上配置，设备部署方式为旁路模式，增加管理员账户dcn2018，密码dcn2018；
2. 公司总部LAN中用户访问网页URL中带有“MP3”、“MKV” 、“RMVB”需要被DCBI记录；
3. 添加内容规则，对于网站访问关键字包含“暴力”的，记录并邮件报警；

#### WAF:

1. 配置WAF为透明模式，按题意完成接口桥接；
2. 创建审计管理员帐户，用户名：dcn2018,密码：201810dcn
3. 配置WAF当发现恶意扫描网站时，将HTTP重定向到http://www.dcn.com/alarm.html，警告攻击者；
4. 配置WAF防当IP请求数超过500个线程阻止该IP继续访问；

#### DCRS:

1. 配置默认路由,使内网用户可以访问Internet;
2. 将连接DCFW的双向流量镜像至Netlog进行监控和分析；
3. 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，Eth5的端口最多学习到5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；
4. 接入DCRS Eth4，仅允许IP地址192.168.20.1-10为源的数据包为合法包，以其它IP地址为源地址，交换机直接丢弃；
5. 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；

#### DCWS：

1. DCWS配置VLAN110为管理VLAN, AP动态方式注册到AC，AC管理IP为192.168.110.254； 数据VLAN为111和222，分别下发网段192.168.111.0/24，192.168.222.0/24，网关为最后一个可用IP，DNS:8.8.8.8，需要排除网关，地址租约为2天； AP静态方式注册到AC；
2. 配置默认路由，使无线用户可以访问Internet;
3. 配置2.4G频段下工作，使用802.11g协议；
4. **第二阶段任务书（600分）**

### 任务1：Web渗透测试

**任务环境说明：**

DCST:

攻击机场景：hackerpc

攻击机场景操作系统：WindowsXP

攻击机场景安装服务/工具1：sqlmap

攻击机场景安装服务/工具2：burpsuite

攻击机场景安装服务/工具3：firefox浏览器及hackbar插件

攻击机场景安装服务/工具4：中国菜刀

服务器场景：WEB2017

服务器场景操作系统：Microsoft Windows Server 2003

服务器场景安装服务：apache2.4+php5.4+mysql集成环境

**任务内容：**

1. 从hackerpc访问DCST中的WEB2017服务器的web页面（访问靶机，在登录界面连按五次shift可获取靶机IP），找到注入点并进行sql注入攻击，获取藏在数据库中的flag，并对结果进行截图。
2. 尝试找到网站的后台并进行登录，获取放在后台页面中的flag值，并对结果进行截图。
3. 寻找后台存在漏洞的上传点，编写一句话木马并绕过上传，利用一句话木马查看上传目录下的flag文件，并对结果进行截图。
4. 利用一句话木马进入服务器后，尝试找到藏在管理员用户开机自启文件夹中的flag文件，并对结果进行截图。
5. 该服务器上存在一隐藏用户，尝试从注册表中找到这个隐藏用户，flag值为此用户的用户名，flag格式为flag{隐藏用户的用户名},并对结果进行截图。

### 任务2：Mysql数据库攻防与加固

**任务环境说明：**

DCST：

服务器场景：MYSQLserver

服务器场景操作系统：Centos 6.5

服务器场景安装服务：mysql服务

**任务内容：**

1. 访问DCST中的MYSQLserver，在/var/log目录下创建access.log文件，并修改mysql服务配置文件，使其能够记录所有的访问记录，对操作步骤进行截图。
2. 进入mysql数据库，找到可以从任何IP地址进行访问的用户，对操作过程进行截图。
3. 对题号2中的漏洞进行加固，删除可从任意IP地址进行登录的用户，对操作步骤进行截图。
4. 改变默认mysql管理员的名称，将默认管理员root改为admin，并将操作过程进行截图。
5. 禁止mysql对本地文件进行存取，对mysql的配置文件进行修改，将修改部分进行截图。

### 任务3：文件包含漏洞攻防

**任务环境说明：**

DCST：

攻击机场景：fipc

攻击机场景操作系统：WindowsXP

攻击机场景安装服务/工具1：apache2.4+php5.4+mysql集成环境（phpstudy）

攻击机场景安装服务/工具2：firefox浏览器及hackbar插件

服务器场景：fiserver

服务器场景操作系统：Microsoft Windows Server 2003

服务器场景安装服务：apache2.4+php5.4+mysql集成环境

**任务内容：**

1. 用fipc访问DCST中的fiserver，验证其存在本地文件包含漏洞，使页面包含C盘里面的flag.txt文件，并对页面回显内容截图。
2. 查看页面代码，找到存在文件包含漏洞的代码，标记并截图。
3. 在fipc上然后利用远程文件包含漏洞，向windows服务器上写入文件名为exp.php的一句话木马，将fipc上创建的文件内容及结果进行截图。
4. 利用php输入流，执行系统命令，查看服务器开放的端口，对url及页面回显内容进行截图。
5. 对上述题目中的漏洞进行加固，对php的配置文件进行配置，使其无法对远程文件进行包含，对修改部分进行截图。