2019年江西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

A卷

# 赛项时间

9:00-12:00，共计3小时，含赛题发放、收卷时间。

# 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 | 9:00-112:00 | 100 |
| 任务2 | 网络安全设备配置与防护 | 300 |
| 第二阶段系统安全攻防及运维安全管控 | 任务1 | ftp安全配置 | 200 |
| 任务2 | ssh安全配置 | 200 |
| 任务3 | CTF | 200 |

# 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。**

1. **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 1002ETH1/0/1 | 10.0.0.6/30 | DCRS |
| ETH1/0/2  |  | AP |
| 管理VLANVLAN 100 | 192.168.100.254/24 |  |
| VLAN 101ETH1/0/11-24 | 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 1001ETH1/0/2 | 10.0.0.2/30 | DCFW |
| VLAN 1002ETH1/0/1 | 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VLANVLAN 30 | 172.16.30.1/26 |  |
| VLAN 40ETH1/0/6-9 | 192.168.40.1/24 | PC1　 |
| 管理VLANVLAN 100 | 192.168.100.1/24 |  |
| VLAN 200ETH1/0/10-24 | 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。 |

1. **第一阶段任务书**

### 任务一：网络平台搭建

|  |  |
| --- | --- |
| 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

#### 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:

1. 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；
2. DCBI监控LAN中VLAN20所有用户的聊天信息并做记录；
3. 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:

1. 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。
2. 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。
3. 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:

1. 配置认证服务器，IP地址是192.168.2.100，radius key是dcn2019;
2. 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；
3. 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；
4. 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：

1. AP通过option43方式进行正常注册上线,hwtype 值为29,AC地址为管理VLANIP；
2. 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；
3. 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；
4. 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;
5. AC开启Web管理，账号密码为DCN2011；
6. **第二阶段任务书（600分）**

### 任务1：ftp安全配置（200分）

**任务环境说明：**

DCST：

服务器场景：ftp

服务器场景操作系统：centos

服务器场景安装服务：vsftp

**任务内容：**

1. 修改配置文件，将ftp服务预设端口改为2121，并对iptables进行配置，对修改部分及iptables截图并提交
2. 修改配置文件，禁止匿名用户登录，对修改部分进行截图并提交
3. 修改ftp默认主目录为/ftp文件夹，并将用户锁定在主目录内，对修改部分进行截图并提交
4. 修改配置文件，关闭ls -R命令，防止服务器被DoS攻击，对修改部分进行截图并提交
5. 修改配置文件，关闭ascii模式下载，防止被用于DoS攻击，对修改部分进行截图并提交

### 任务2：ssh安全配置（200分）

**任务环境说明：**

DCST：

服务器场景：ssh

服务器场景操作系统：centos

服务器场景安装服务：ssh

**任务内容：**

1. 修改ssh配置文件，禁止root用户通过ssh登录，对修改部分进行截图并提交
2. 配置TCP Wrappers ，对远程主机进行访问控制，仅允许192.168.1.0/24网段使用ssh进行登录,对修改的文件及修改部分进行截图并提交
3. 修改ssh配置文件，控制通过ssh登录的用户，仅允许用户名为dcn的用户进行登录，对修改部分进行截图并提交
4. 修改ssh配置文件，设置每300秒判断一次客户端是否超时,允许超时次数5次，对修改部分进行截图并提交
5. 修改ssh配置文件，禁止使用空密码进行登录，设置最大尝试次数为5次，对修改部分进行截图并提交

### 任务3：CTF（200分）

**任务环境说明：**

DCST：

服务器场景：ctfwin7

服务器场景操作系统：Microsoft Windows 7

服务器场景安装服务：phpstudy集成环境

**任务内容：**

1. 运行桌面上的king.exe，并使用用户名hello登录程序，将“密码正确”弹窗截图。（截图中需要包含用户名和密码，IDA工具在桌面Tools目录中）
2. 打开桌面上的2019dcn.jpg文件，找出文件中的flag字符串，flag格式为flag{xxxx}。（foremost.exe工具在Tools目录中，binwalk可直接在cmd中使用）
3. 开启PhpStudy，打开浏览器访问“http://127.0.0.1/test.php”，使得能够在浏览器中弹出flag内容，将浏览器中弹窗内容截图。（截图中要包含完整的URL地址）