2017年全国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

# 赛项时间

9:00-15:00，共计6小时，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 | 9:00-13:30 | 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 | 缓冲区溢出漏洞渗透测试 | 50 |
| 任务2 | Web应用程序安全攻防 | 50 |
| 任务3 | ARP扫描渗透测试 | 50 |
| 任务4 | 操作系统判断渗透测试 | 50 |
| 任务5 | 数据库访问渗透测试及其加固 | 50 |
| 任务6 | 网络协议渗透测试及其加固 | 50 |
| 中场收卷 | | | 13:30-14:00 | |
| 第三阶段  分组对抗 | 系统加固 | | 14:00-15:00 | 400 |
| 系统攻防 | |

# 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提交任务“操作文档”，“操作文档”需要存放在裁判组专门提供的U盘中。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“xx工位”的文件夹（xx用具体的工位号替代），赛题第一阶段完成任务操作的文档放置在文件夹中。

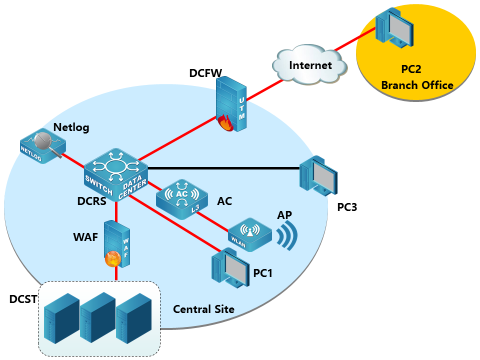
例如：08工位，则需要在U盘根目录下建立“08工位”文件夹，并在“08工位”文件夹下直接放置第一个阶段的操作文档文件。

**特别说明：只允许在根目录下的“08工位”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



**PC环境说明：**

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：Microsoft Internet Explorer 6.0

虚拟机安装服务/工具2：Ethereal 0.10.10.0

虚拟机安装服务/工具3：HttpWatch Professional Edition

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-2（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：Microsoft Internet Explorer 6.0

虚拟机安装服务/工具2：Ethereal 0.10.10.0

虚拟机安装服务/工具3：HttpWatch Professional Edition

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Kali Linux（Debian7 64Bit）

虚拟机安装服务/工具：Metasploit Framework

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

### 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 | EthX | x.x.x.x/x | 与PC-3相连 | 见赛场IP参数表 |
| 地址池 | x.x.x.x/x | SSL VPN地址池 | 见赛场IP参数表 |
| 无线交换机DCWS | EthX | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| 地址池 | x.x.x.x/x | DCHP地址池 | 见赛场IP参数表 |
| WEB应用防火墙WAF | EthX | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| EthX |  | 与DCST相连 | 见赛场IP参数表 |
| 三层交换机DCRS | Vlan 2 | x.x.x.x/x | 与DCWS相连 | 见赛场IP参数表 |
| Vlan 10 | x.x.x.x/x | 与WAF相连 | 见赛场IP参数表 |
| Vlan 20 | x.x.x.x/x | 与PC-1所在用户区相连 | 见赛场IP参数表 |
| Vlan 30 | x.x.x.x/x | 与PC-2所在用户区相连 | 见赛场IP参数表 |
| Vlan 40 | x.x.x.x/x | 与DCBI相连 | 见赛场IP参数表 |
| Vlan 100 | x.x.x.x/x | 直连服务器区 | 见赛场IP参数表 |
| Vlan 110 | x.x.x.x/x | 直连用户区 | 见赛场IP参数表 |
| 网络日志系统DCBI | EthX | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| 堡垒服务器DCST | EthX | x.x.x.x/x | 与WAF相连 | 见赛场IP参数表 |
| PC-1 | 无 | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| PC-2 | 无 | x.x.x.x/x | 与DCFW相连 | 见赛场IP参数表 |
| PC-3 | 无 | x.x.x.x/x | 与DCFW相连 | 见赛场IP参数表 |
| 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 | Eth0–Eth9 | 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（300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（60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，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 | 完整填写“赛场IP参数表”。 |

### 任务2：网络安全设备配置与防护（240分）

#### DCFW:

1. 在总公司的DCFW上配置，连接LAN接口开启PING,HTTP,HTTPS功能，连接Internet接口开启PING、HTTPS功能；并且新增一个用户，用户名dcn2017，密码dcn2017，该用户只有读-执行权限；
2. DCFW配置NTP 和 LOG， Server IP为X.X.X.X，NTP认证密码为Dcn2017；
3. DCFW连接LAN的接口配置二层防护，ARP Flood超过500个每秒时丢弃超出的ARP包，ARP扫描攻击超过300个每秒时弃超出的ARP包；配置静态ARP绑定，MAC地址880B.0A0B.0C0D与IP地址X.X.X.X绑定；
4. DCFW连接Internet的区域上配置以下攻击防护：

FW1，FW2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，警戒值5000，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. 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20；
2. DCFW上配置NAT功能，使PC2能够通过WEB方式正常管理到WAF，端口号使用10666;）
3. 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，配置下载客户端端口为9999，数据连接端口为9998，SSLVPN地址池参见地址表；
4. DCFW加强访问Internet安全性，禁止从HTTP打开和下载可执行文件和批处理文件；
5. DCFW配置禁止所有人在周一至周五工作时间9：00-18：00访问京东www.jd.com和淘宝www.taobao.com;相同时间段禁止访问中含有“娱乐”、“新闻”的WEB页面；
6. DCFW上配置ZONE和放行策略，连接Internet接口为“Untrust”区域，连接DCRS接口为“Trust”区域，连接SSL VPN接口为“VPN HUB”区域，要求配置相应的最严格安全策略；）

#### DCBI:

1. 在公司总部的DCBI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;增加非admin账户DCN2017，密码dcn2017，该账户仅用于用户查询设备的系统状态和统计报表;
2. 在公司总部的DCBI上配置，监控周一至周五9：00-18：00 PC-1所在网段用户访问的URL中包含xunlei的HTTP访问记录，并且邮件发送告警;
3. 在公司总部的DCBI上配置，监控PC-1所在网段用户周一至周五9：00-18：00的即时聊天记录;
4. 公司总部LAN中用户访问网页中带有“MP3”、“MKV” 、“RMVB”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；
5. DCBI监控LAN中用户访问网络游戏，包括“QQ游戏”、“魔兽世界”并作记录；
6. DCBI配置应用及应用组“快播视频”，UDP协议端口号范围23456-23654，在周一至周五9：00-18：00监控LAN中所有用户的“快播视频”访问记录；
7. DCBI上开启邮件告警，邮件服务器地址为X.X.X.X，端口号25,告警所用邮箱用户名dcnadmin,密码Dcn2017;当DCBI磁盘使用率超过75%时发送一次报警；

#### 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512，防止缓冲区溢出攻击；
2. 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：10秒钟超过3000次请求；
3. 在公司总部的WAF上配置，对公司网站（X.X.X.X）进行安全评估，检查网站是否存在安全漏洞，便于在攻击没有发生的情况下提前做出防护措施；
4. 使用WAF自带标识组配置爬虫防护与扫描防护，阻断时间120秒，通过WAF组织爬虫探测和扫描服务器区域；
5. 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。
6. 公司web应用防火墙透明模式部署，为了防止不法人员对公司内的网站(X.X.X.X)进行攻击，在web 应用防火墙上开启“黑名单”策略，禁止公网IP地址（X.X.X.X）访问网站服务器。
7. 公司web应用防火墙透明模式部署，为了防止不法人员对公司内的网站(X.X.X.X)进行攻击，在web 应用防火墙上开启防止“SQL注入”攻击策略阻止攻击流量；
8. 在公司总部的WAF上配置， WAF设备的内存使用率超过75%每隔5分钟发送邮件和短信给管理，邮箱[admin@digitalchina.com](mailto:admin@digitalchina.com)，手机13912345678；

#### DCRS:

1. 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；Ex/x为专用接口，限定MAC地址00-11-11-11-11-11可以连接； 将连接DCFW的双向流量镜像至Netlog进行监控和分析；
2. DCRS配置802.1x认证，Radius服务器IP 地址X.X.X.X,认证密码Dcn2017,

Ex/x号端口开启802.1x功能，接入该端口通过PC上的802.1x软件进行认证；

1. 接入DCRS Ex/x，仅允许IP地址X.X.X.X-X.X.X.X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；
2. 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，AC为DHCP服务器，限制与AC在同一VLAN接口的ARP阀值为50；
3. DCRS上开启以下安全特性，防IP Spoofing攻击、防TCP非法标志攻击、防端口欺骗攻击、防TCP碎片攻击、防ICMP碎片攻击；

#### DCWS：

1. AP通过option43方式进行正常注册上线；
2. 设置AP工作在5G频段；
3. 设置SSID DCN，加密模式为wpa-personal,其口令为：chinaskill；

设置SSID GUEST 不进行认证加密；

1. GUSET最多接入10个用户，用户间相互隔离，并对GUEST网络进行流控，上行1M，下行2M；
2. 通过配置避免接入终端较多且有大量弱终端时，避免高速客户端被低速客户端“拖累”，让低速客户端不至于长时间得不到传输；
3. 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；
4. 防止非法AP假冒合法SSID，开启AP威胁检测功能；
5. 通过设置实现在AC断开网络连接时AP还能正常工作；
6. 考虑到无线网络会进一步部署，增加更多的AP，设置已有AP信道和发射功率每隔1小时自动调节；
7. 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AC能代为应答其已知的MAC地址；
8. **第二阶段任务书（300分）**

提示：本阶段用到堡垒服务器DCST中的服务器场景，获取服务器IP地址方式如下：

Windows服务器的IP地址可以通过拓扑界面获得，如果获得不了，采用如下方法获得：

* 通过DCST场景里的网络拓扑图，启动连接设备
* 进入服务器，用户名为administrator，密码：空
* 执行ipconfig /all，即可获得服务器IP地址

### 任务1：缓冲区溢出漏洞渗透测试（50分）

**任务描述：**

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，在该系统中某程序可能存在缓冲区溢出漏洞；你需要对该程序进行渗透测试，确认程序确实存在该漏洞；

**任务环境说明：**

主机场景：WindowsXP

主机场景操作系统：Microsoft Windows XP Professional

主机场景安装服务/工具1：Visual C++ 6.0；

主机场景安装服务/工具2：OllyICE；

主机场景安装服务/工具3：Findjmp；

主机场景安装服务/工具4：Sublime Text 2.0.2；

**任务内容：**

1. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行分析，找到Main函数中有缓冲区溢出可能的变量名，并将Flag值（形式：有缓冲区溢出可能的变量名）进行提交；
2. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行完善，使用工具findjmp找到Windows内核文件KERNEL32.DLL中的首个“call esp”指令的内存地址，将该内存地址作为函数的返回地址，根据以上信息，填写可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）中的F1字符串，并将Flag值（形式：F1字符串内容）进行提交；
3. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行完善，填写该源代码中join函数中的F2、F3字符串，并将Flag值（形式：F2字符串内容;F3字符串内容）进行提交；
4. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行完善，填写该源代码中repstr函数中的F4、F5字符串，并将Flag值（形式：F4字符串内容;F5字符串内容）进行提交；
5. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行完善，填写该源代码中main函数中的F6、F7、F8字符串，并将Flag值（形式：F6字符串内容;F7字符串内容;F8字符串内容）进行提交；
6. 将完善后的缓冲区溢出渗透测试程序源代码（位置：C:\VC\Source Code\Overflow.c）进行编译、链接、运行，将该程序的运行结果显示的最后1行字符串作为Flag值（形式：程序的运行结果显示的最后1行字符串）提交；

### 任务2：Web应用程序安全攻防（50分）

**任务描述：**

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，在该系统中Web应用程序可能存在SQL注入漏洞；首先，你需要对该程序进行渗透测试，确认程序确实存在该漏洞；其次，你需要对该程序打补丁，解决以上漏洞带来的问题；第三，你需要再次对该程序进行渗透测试，验证程序是否还存在漏洞。

**任务环境说明：**

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：Microsoft Internet Explorer 6.0

虚拟机安装服务/工具2：Ethereal 0.10.10.0

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

服务器场景：WebServ2003

服务器场景操作系统：Microsoft Windows2003 Server

服务器场景安装服务/工具1：Apache2.2；

服务器场景安装服务/工具2：Php6；

服务器场景安装服务/工具3：Microsoft SqlServer2000；

服务器场景安装服务/工具4：EditPlus；

1. 在PC-1上，Web访问DCST中的WebServ2003服务器场景，进入login.php页面，分析该页面源程序，找到提交的变量名，并将所有提交的变量名作为Flag值（形式：变量名1;变量名2;…;变量名n）提交；
2. 对该任务题目1页面注入点进行SQL注入渗透测试，使该Web站点可通过万能用户名、数据库users表中当中任意一个密码登录，并将万能用户名字符串当中的固定部分作为Flag值（形式：万能用户名字符串当中的固定部分）提交；
3. 对服务器场景：WebServ2003的Web开发环境进行配置，使其能够支持数据抽象层（PDO）技术，并将配置文件的路径及名称字符串作为Flag值（形式：配置文件的路径及名称字符串）提交；
4. 对服务器场景：WebServ2003的Web开发环境进行配置，使其能够支持数据抽象层技术，并将在上题配置文件中取消注释行内容作为Flag值（形式：按顺序取消注释行1字符串; 按顺序取消注释行1字符串;…; 按顺序取消注释行n字符串）提交；
5. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag1字符串，将该字符串作为Flag值（形式：Flag1字符串）提交；
6. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag2字符串，将该字符串作为Flag值（形式：Flag2字符串）提交；
7. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag3字符串，将该字符串作为Flag值（形式：Flag3字符串）提交；
8. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag4字符串，将该字符串作为Flag值（形式：Flag4字符串）提交；
9. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag5字符串，将该字符串作为Flag值（形式：Flag5字符串）提交；
10. 再次对该任务题目1页面注入点进行渗透测试，验证此次利用该注入点对该DCST中的WebServ2003服务器场景进行SQL注入渗透测试无效，并将页面回显HTML源文件内容作为Flag值（形式：页面回显HTML源文件内容）提交；

### 任务3：ARP扫描渗透测试（50分）

**任务描述：**

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，现欲对该系统中主机进行ARP扫描渗透测试，确认该系统中都有哪些IP主机在线；

**任务环境说明：**

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：EditPlus

虚拟机安装服务/工具2：XFTP

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

服务器场景：CentOS5.5

服务器场景操作系统：CentOS Linux 5.5

1. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_sweep.py文件，填写该文件当中空缺的Flag1字符串，将该字符串作为Flag值（形式：Flag1字符串）提交；（arp\_sweep.py脚本功能见该任务第6题）
2. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_sweep.py文件，填写该文件当中空缺的Flag2字符串，将该字符串作为Flag值（形式：Flag2字符串）提交；（arp\_sweep.py脚本功能见该任务第6题）
3. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_sweep.py文件，填写该文件当中空缺的Flag3字符串，将该字符串作为Flag值（形式：Flag3字符串）提交；（arp\_sweep.py脚本功能见该任务第6题）
4. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_sweep.py文件，填写该文件当中空缺的Flag4字符串，将该字符串作为Flag值（形式：Flag4字符串）提交；（arp\_sweep.py脚本功能见该任务第6题）
5. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_sweep.py文件，填写该文件当中空缺的Flag5字符串，将该字符串作为Flag值（形式：Flag5字符串）提交；（arp\_sweep.py脚本功能见该任务第6题）
6. 在虚拟机操作系统：Ubuntu Linux 32bit下执行arp\_sweep.py文件，对服务器场景进行ARP扫描渗透测试；将该文件执行后的显示结果中，第1行的第1个字符以及第2行的第1个字符作为Flag值（形式：第1行的第1个字符;第2行的第1个字符）提交；

### 任务4：操作系统判断渗透测试（50分）

**任务描述：**

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，现欲对该系统中主机进行操作系统扫描渗透测试，确认该系统中主机都运行了哪些操作系统；

**任务环境说明：**

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：EditPlus

虚拟机安装服务/工具2：XFTP

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

服务器场景：CentOS5.5

服务器场景操作系统：CentOS Linux 5.5

1. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的os\_scan.py文件，填写该文件当中空缺的Flag1字符串，将该字符串作为Flag值（形式：Flag1字符串）提交；（os\_scan.py脚本功能见该任务第6题）
2. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的os\_scan.py文件，填写该文件当中空缺的Flag2字符串，将该字符串作为Flag值（形式：Flag2字符串）提交；（os\_scan.py脚本功能见该任务第6题）
3. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的os\_scan.py文件，填写该文件当中空缺的Flag3字符串，将该字符串作为Flag值（形式：Flag3字符串）提交；（os\_scan.py脚本功能见该任务第6题）
4. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的os\_scan.py文件，填写该文件当中空缺的Flag4字符串，将该字符串作为Flag值（形式：Flag4字符串）提交；（os\_scan.py脚本功能见该任务第6题）
5. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的os\_scan.py文件，填写该文件当中空缺的Flag5字符串，将该字符串作为Flag值（形式：Flag5字符串）提交；（os\_scan.py脚本功能见该任务第6题）
6. 在虚拟机操作系统：Ubuntu Linux 32bit下执行os\_scan.py文件，对服务器场景进行操作系统信息判断渗透测试，将该文件执行后的显示结果作为Flag值（形式：文件执行后的显示结果字符串）提交；

### 任务5：数据库访问渗透测试及其加固（50分）

**任务描述：**

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，在该系统中Web服务器中的数据库服务可能存在访问漏洞；首先，你需要对该程序进行渗透测试，确认程序确实存在该漏洞；其次，你需要对数据库服务进行安全加固配置，解决以上漏洞带来的问题；第三，你需要再次对该程序进行渗透测试，验证程序是否还存在访问漏洞。

**任务环境说明：**

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：EditPlus

虚拟机安装服务/工具2：XFTP

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

服务器场景：WebServ2003

服务器场景操作系统：Microsoft Windows2003 Server

服务器场景安装服务/工具1：Apache2.2；

服务器场景安装服务/工具2：Php6；

服务器场景安装服务/工具3：Microsoft SqlServer2000；

服务器场景安装服务/工具4：EditPlus；

1. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mssql\_brute\_force.py文件，填写该文件当中空缺的Flag1字符串，将该字符串作为Flag值（形式：Flag1字符串）提交；（mssql\_brute\_force.py脚本功能见该任务第6题）
2. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mssql\_brute\_force.py文件，填写该文件当中空缺的Flag2字符串，将该字符串作为Flag值（形式：Flag2字符串）提交；（mssql\_brute\_force.py脚本功能见该任务第6题）
3. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mssql\_brute\_force.py文件，填写该文件当中空缺的Flag3字符串，将该字符串作为Flag值（形式：Flag3字符串）提交；（mssql\_brute\_force.py脚本功能见该任务第6题）
4. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mssql\_brute\_force.py文件，填写该文件当中空缺的Flag4字符串，将该字符串作为Flag值（形式：Flag4字符串）提交；（mssql\_brute\_force.py脚本功能见该任务第6题）
5. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mssql\_brute\_force.py文件，填写该文件当中空缺的Flag5字符串，将该字符串作为Flag值（形式：Flag5字符串）提交；（mssql\_brute\_force.py脚本功能见该任务第6题）
6. 在虚拟机操作系统：Ubuntu Linux 32bit下执行mssql\_brute\_force.py文件，进行数据库超级管理员密码暴力破解渗透测试（使用字典文件./root/superdic.txt），将该文件执行后的显示结果中的最后1行内容作为Flag值（形式：文件执行后的显示结果中的最后1行字符串）提交；
7. 通过对服务器场景WebServ2003的数据库服务进行安全加固，阻止PC-3中渗透测试平台对其进行数据库超级管理员密码暴力破解渗透测试，并将进行安全配置的数据库身份验证选项中的英文单词作为Flag值（形式：进行安全配置的数据库身份验证选项中的唯一一个英文单词字符串）提交；
8. 验证在WebServ2003的数据库服务进行安全加固后，再次在虚拟机操作系统：Ubuntu Linux 32bit下执行mssql\_brute\_force.py文件，进行数据库超级管理员密码暴力破解渗透测试（使用字典文件./root/superdic.txt），将该文件执行后的显示结果中的最后1行内容作为Flag值（形式：文件执行后的显示结果中的最后1行字符串）提交；

### 任务6：网络协议渗透测试及其加固（50分）

**任务描述：**

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，在该系统中的网络通讯协议可能存在漏洞；首先，你需要对网络进行渗透测试，确认网络协议确实存在该漏洞；其次，你需要对网络通讯协议进行安全加固配置，解决以上漏洞带来的问题；第三，你需要再次对该网络进行渗透测试，验证网络是否还存在访问漏洞。

**任务环境说明：**

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：EditPlus

虚拟机安装服务/工具2：XFTP

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

服务器场景：WebServ2003

服务器场景操作系统：Microsoft Windows2003 Server

服务器场景安装服务/工具1：Apache2.2；

服务器场景安装服务/工具2：Php6；

服务器场景安装服务/工具3：Microsoft SqlServer2000；

服务器场景安装服务/工具4：EditPlus；

1. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mac\_flood.py文件，填写该文件当中空缺的Flag1字符串，将该字符串作为Flag值（形式：Flag1字符串）提交；（mac\_flood.py脚本功能见该任务第6题）
2. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mac\_flood.py文件，填写该文件当中空缺的Flag2字符串，将该字符串作为Flag值（形式：Flag2字符串）提交；（mac\_flood.py脚本功能见该任务第6题）
3. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mac\_flood.py文件，填写该文件当中空缺的Flag3字符串，将该字符串作为Flag值（形式：Flag3字符串）提交；（mac\_flood.py脚本功能见该任务第6题）
4. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mac\_flood.py文件，填写该文件当中空缺的Flag4字符串，将该字符串作为Flag值（形式：Flag4字符串）提交；（mac\_flood.py脚本功能见该任务第6题）
5. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mac\_flood.py文件，填写该文件当中空缺的Flag5字符串，将该字符串作为Flag值（形式：Flag5字符串）提交；（mac\_flood.py脚本功能见该任务第6题）
6. 在虚拟机操作系统：Ubuntu Linux 32bit下执行mac\_flood.py文件，进行MAC Flooding渗透测试；运行DCRS交换机命令（#show mac-address-table count），将该命令执行结果显示的交换机学习到的当前动态MAC地址条目总数作为Flag值（形式：动态MAC地址条目总数）提交；
7. 在DCRS交换机的PC-3所连接端口配置端口安全特性，阻止PC-3发起MAC Flooding渗透测试，将配置的端口模式配置命令字符串作为Flag值（形式：端口模式配置命令字符串）提交；
8. 再次在虚拟机操作系统：Ubuntu Linux 32bit下执行mac\_flood.py文件，进行MAC Flooding渗透测试；运行DCRS交换机命令（#show mac-address-table count），将该命令执行结果显示的交换机学习到的当前动态MAC地址条目总数作为Flag值（形式：动态MAC地址条目总数）提交；
9. **第三阶段任务书（400分）**

假定各位选手是Taojin电子商务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：任何时候不能人为关闭服务器服务端口，否则将判令停止比赛，第三阶段分数为0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./root/flaginfoxxxx.xxx.txt文件内容当中。

注意6：每提交1次对手靶机的Flag值增加4分，每当被对手提交1次自身靶机的Flag值扣除4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。

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. 靶机上的网站可能存在命令注入的漏洞，要求选手找到命令注入的相关漏洞，利用此漏洞获取一定权限。

2. 靶机上的网站可能存在文件上传漏洞，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. 靶机上的网站可能存在文件包含漏洞，要求选手找到文件包含的相关漏洞，与别的漏洞相结合获取一定权限并进行提权

4. 操作系统提供的服务可能包含了远程代码执行的漏洞，要求用户找到远程代码执行的服务，并利用此漏洞获取系统权限。

5. 操作系统提供的服务可能包含了缓冲区溢出漏洞，要求用户找到缓冲区溢出漏洞的服务，并利用此漏洞获取系统权限。

6. 操作系统中可能存在一些系统后门，选手可以找到此后门，并利用预留的后门直接获取到系统权限。

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。