2016年全国职业院校技能大赛高职组“神州数码”杯

“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  平台搭建与配置 | 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 | SQL注入攻防 | 55 |
| 任务2 | XSS和CSRF攻防 | 65 |
| 任务3 | 命令注入与文件包含攻防 | 50 |
| 任务4 | MAC协议安全攻防 | 45 |
| 任务5 | ARP协议安全攻防 | 45 |
| 任务6 | SpanningTree协议安全攻防 | 40 |
| 中场收卷 | | | 13:30-14:00 | |
| 第三阶段  分组对抗 | 系统加固 | | 14:00-14:15 | 100 |
| 系统攻防 | | 14:15-15:00 | 300 |

# 赛项内容

本次大赛，各位选手需要完成三个阶段的任务，其中前两个阶段需要提交任务操作文档留存备案，所有文档需要存放在裁判组专门提供的U盘中。第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），并在“xx工位”文件夹下，建立“第一阶段”、“第二阶段”两个文件夹，赛题两个阶段的文档分别归类放置在对应的文件夹中。

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”文件夹下建立“第一阶段”、“第二阶段”两个文件夹。

**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-2相连 | 见赛场IP参数表 |
| EthX | x.x.x.x/x | 与DCFS相连 | 见赛场IP参数表 |
| 地址池 | x.x.x.x/x | VPN地址池 | 见赛场IP参数表 |
| 网络流控系统DCFS | EthX | 无 | 与DCFW相连 | 见赛场IP参数表 |
| EthX | x.x.x.x/x | 与DCRS相连 | 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 | 无 | 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DCFS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相连 | 见赛场IP参数表 |
| Vlan 30 | x.x.x.x/x | 与PC-3相连 | 见赛场IP参数表 |
| Vlan 40 | x.x.x.x/x | 与NETLOG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 |
| 地址池 | x.x.x.x/x | DHCP地址池 | 见赛场IP参数表 |
| 网络日志系统NETLOG | EthX | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| EthX | 无 | 与DCRS相连 | 见赛场IP参数表 |
| 堡垒服务器DCST | EthX | 无 | 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-3 | 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 |
| 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IP参数表》-“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 |
| 网络流控系统DCFS | https://192.168.1.254:9999 | ETH0 | admin | Admin123 |
| 网络日志系统NETLOG | https://192.168.5.254 | ETH0 | admin | 123456 |
| web应用防火墙WAF | https://192.168.45.1 | ETH5 | admin | admin123 |
| 堡垒服务器DCST | http://192.168.1.100 | Eth0–Eth9 | 参见“DCST登录用户表” | |
| **注意：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）**

提示：该阶段答案文档命名格式为：“第X阶段”-“任务X”-“任务名称”。

例：“第一阶段、任务2、网络安全设备配置与防护”的答案提交文档，文件名称为：第一阶段-任务2-网络安全设备配置与防护.doc或第一阶段-任务2-网络安全设备配置与防护.docx。

### 任务1：网络平台搭建（60分）

提示：需要提交所有设备配置文件，其中DCRS设备要求提供show run配置文件保存到WORD文档，DCFW、DCFS、WAF、NETLOG设备需要提交配置过程截图存入WORD文档，并在截图中加配置说明。提交的答案保存到一个WORD文档中，需标明题号，按顺序答题。

平台搭建要求如下：

|  |  |  |
| --- | --- | --- |
| **题号** | **网络需求** | **分值** |
| 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。 | 5分 |
| 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。 | 5分 |
| 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。 | 5分 |
| 4 | 根据网络拓扑图所示，按照IP地址参数表，对DCFS的各接口IP地址进行配置。 | 5分 |
| 5 | 根据网络拓扑图所示，按照IP地址参数表，对NETLOG的名称、各接口IP地址进行配置。 | 5分 |
| 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。 | 5分 |
| 7 | 采用RIPV2路由协议，全网络互连。 | 6分 |
| 8 | 完整填写“赛场IP参数表”。 | 24分 |

### 任务2：网络安全设备配置与防护（240分）

提示：需要提交所有设备配置文件，其中DCRS设备要求提供show run配置文件保存到WORD文档，DCFW、DCFS、WAF、NETLOG设备需要提交配置过程截图存入WORD文档，并在截图中加以说明。请顺序答题，并标注题号。每个设备提交的答案各自保存到不同的WORD文档中（本任务可以保存5个WORD文档）。

例：“第一阶段、任务2、网络安全设备配置与防护”关于NETLOG设备的答案提交文档，文件名称为：第一阶段-任务2-网络安全设备配置与防护-NETLOG.doc或第一阶段-任务2-网络安全设备配置与防护-NETLOG.docx。

1. 在公司总部的DCFW上配置，连接互联网的接口属于WAN安全域、连接内网的接口属于LAN安全域。（6分）
2. 在公司总部的DCFW上配置，开启DCFW针对以下攻击的防护功能：

ICMP洪水攻击防护、UDP洪水攻击防护、SYN洪水攻击防护、WinNuke攻击防护、IP地址欺骗攻击防护、IP地址扫描攻击防护、端口扫描防护、Ping of Death攻击防护、Teardrop攻击防护、IP分片防护、IP选项、Smurf或者Fraggle攻击防护、Land攻击防护、ICMP大包攻击防护、TCP选项异常、DNS查询洪水攻击防护、DNS递归查询洪水攻击防护。（6分）

1. 在公司总部的DCFW上新增2个用户，用户1（用户名：User1；密码：User1）：只拥有配置查看权限，不能进行任何的配置添加与修改，删除。 用户2（用户名：User2；密码：User2）：拥有所有的查看权限，拥有除“用户升级、应用特征库升级、重启设备、配置 日志”模块以外的所有模块的配置添加与修改，删除权限。（6分）
2. 在公司总部的DCFW上配置，内网可以访问互联网任何服务，互联网不可以访问内网。（6分）
3. 在公司总部的DCFW上配置网页内容过滤：内网用户不能访问互联网网站：www.tudou.com；（6分）
4. 在公司总部的DCFW上配置，使公司总部的DCST服务器可以通过互联网被访问，从互联网访问的地址是公网地址的第三个可用地址（公网IP地址段参考“赛场IP参数表”），且仅允许PC-2通过互联网访问DCST设备。（6分）
5. 在公司总部的DCFW上配置，使内网所有用户网段和服务器区网段都可以通过DCFW外网接口IP地址访问互联网。（6分）
6. 为了保证正常工作，在公司总部的DCFW上配置：对于上班时间（8：00-17：00）公司总部内网浏览Internet网页，连接总数不超过2000；（6分）
7. 在公司总部的DCFW上配置，使内网访问Internet网站时，不允许访问MSI(.msi)、EXE(.exe)、COM(.com)、(.bat)类型的文件。（6分）
8. 在公司总部的DCFW上配置，使内网向Internet发送邮件，或者从Internet接收邮件时，不允许邮件携带附件大于50MB。（6分）
9. 在公司总部的DCFW上启用L2TP VPN，使分支机构通过L2TP VPN拨入公司总部，访问内网的所有信息资源。L2TP VPN地址池x.x.x.x/x（具体IP地址参考“赛场IP参数表”）。（6分）
10. 在公司总部的DCFW上启用SSL VPN，使分支机构通过SSL VPN拨入公司总部，访问内网的所有信息资源。SSL VPN地址池x.x.x.x/x（具体IP地址参考“赛场IP参数表”）。（6分）
11. 在PC-2运行Wireshark分别对L2TP VPN和SSL VPN访问内网的流量进行捕获，并对以上两种流量进行对比分析区别。（6分）
12. 在公司总部的DCFS上配置，使其连接DCFW防火墙和DCRS交换机之间的接口能够实现二层互通。（6分）
13. 在公司总部的DCFS上配置，使DCFS能够对由公司内网发起至Internet的流量实现以下操作：会话保持、应用分析、主机统计、会话限制、会话日志。（6分）
14. 在公司总部的DCFS上配置，使工作日内（每周一至周五），阻止PC-1访问迅雷相关应用，并返回TCP Reset数据包。（6分）
15. 在公司总部的DCFS上配置，实现公司内网每用户访问Internet带宽上限为1Mbps，全部用户访问Internet带宽上限为100Mbps。（6分）
16. 在题目15条件的基础之上，继续在在公司总部的DCFS上配置，实现公司内网每用户访问Internet的FTP服务带宽上限为512Kbps，全部用户访问Internet的FTP服务带宽上限为20Mbps。（6分）
17. 在公司总部的NETLOG上配置，设备部署方式为旁路模式，并配置监控接口。（6分）
18. 在公司总部的DCRS交换机上配置SPAN，使内网经过DCRS交换机的全部流量均交由NETLOG分析。（6分）
19. 在公司总部的NETLOG上配置，监控内网所有用户的即时聊天记录。（6分）
20. 在公司总部的NETLOG上配置，监控内网所有用户的网站访问记录。（6分）
21. 在公司总部的DCRS交换机上运行SSH服务，客户端PC-1运行支持SSH2.0标准的客户端软件如Secure Shell Client或Putty，使用用户名和密码方式登录交换机。（6分）
22. 在公司总部的DCRS交换机上启动SSL功能，客户端PC-1通过浏览器客户端通过https登录交换机时，交换机和浏览器客户端进行SSL握手连接，形成安全的SSL连接通道，从而保证通信的私密性。（6分）
23. 在公司总部的DCRS上配置除内网IP地址段的RFC3330过滤来限制源IP欺骗攻击。（6分）
24. 在公司总部的DCRS上配置，VLAN110用户可通过DHCP的方式获得IP地址，在交换机上配置DHCP Server，地址池名称为pool110，DNS地址为202.106.0.20，租期为8天，VLAN110网段最后20个可用地址（DHCP地址段参考“赛场IP参数表”）不能被动态分配出去。（6分）
25. 配置公司总部的DCRS，防止来自VLAN110接口的DHCP地址池耗尽攻击。（6分）
26. 配置公司总部的DCRS，防止来自VLAN110接口的DHCP服务器假冒攻击。（6分）
27. 在公司总部的DCRS上配置端口环路检测（Loopback Detection），防止来自接口下的单端口环路，并配置存在环路时的检测时间间隔为50秒，不存在环路时的检测时间间隔为20秒（6分）
28. 在公司总部的DCRS上配置，需要在交换机第10个接口上开启基于MAC地址模式的认证，认证通过后才能访问网络，认证服务器连接在服务器区，IP地址是服务器区内第105个可用地址（服务器区IP地址段参考“赛场IP参数表”），radius key是dcn。（6分）
29. 黑客主机接入直连终端用户VLAN110，通过RIPV2路由协议向DCRS注入度量值更低的外网路由，从而代理内网主机访问外网，进而通过Sniffer来分析内网主机访问外网的流量（如账号、密码等敏感信息）。通过在DCRS上配置HMAC，来阻止以上攻击的实现。（认证Key须使用Key Chain实现）（6分）
30. 为方便公司总部网络规模扩展，将公司总部的DCRS交换机的24端口配置为Trunk模式，用于将来继续连接其它的交换机，配置公司总部的DCRS，使其能够防御由此带来VLAN Hopping（VLAN跳跃）攻击。（6分）
31. 配置公司总部的DCRS，通过Gratuitous ARP来抵御来自VLAN110接口的针对网关的ARP欺骗攻击。（6分）
32. 配置公司总部的DCRS，通过ARP Guard来抵御来自VLAN110接口的针对网关的ARP欺骗攻击。（6分）
33. 配置公司总部的DCRS，防止对公司总部服务器的以下3类DOS（Denial Of Service）攻击：ICMP Flood攻击、LAND攻击、SYN Flood攻击。（6分）
34. 配置公司总部的DCRS，通过控制平面（Control Plane）策略，防止DCRS受到来自于VLAN110接口的DOS（Denial Of Service）攻击；其中CIR(Committed Information Rate)定义为128Kbps，TC（Time Commit）定义为8192ms，速率大于CIR的流量将被DCRS丢弃，其余流量将被正常发送。（6分）
35. 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。（6分）
36. 在公司总部的WAF上配置，使用WAF的漏洞扫描功能检测web服务器的安全漏洞情况。（6分）
37. 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128，防止缓冲区溢出攻击。（6分）
38. 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。（6分）
39. **第二阶段：系统安全攻防及运维安全管控（300分）**

提示1：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

提示2：每个任务提交一个word文档，请在文档中标明题号，按顺序答题。将关键步骤和操作结果进行截屏，并辅以文字说明，保存到提交文档中。

提示3：文档命名格式为：“第X阶段”-“任务X”-“任务名称”。

例：“第二阶段、任务2”的答案提交文档，文件名称为：第二阶段-任务2- XSS和CSRF攻防.doc或第二阶段-任务2- XSS和CSRF攻防.docx。

### 任务1：SQL注入攻防（55分）

**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）

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，并截图；（5分）
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站点可通过任意用户名登录，并将测试过程截图；（5分）
3. 进入DCST中的WebServ2003服务器场景的C:\AppServ\www目录，找到loginAuth.php程序，使用EditPlus工具分析并修改PHP源程序，使之可以抵御SQL注入，并将修改后的PHP源程序截图；（10分）
4. 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，并将验证过程截图；（5分）
5. 在PC-1上，Web继续访问DCST中的WebServ2003服务器场景，"/"->"Employee Information Query"，分析该页面源程序，找到提交的变量名，并截图；（5分）
6. 对该任务题目5页面注入点进行渗透测试，根据输入“%”以及“\_”的返回结果确定是注入点，并将测试过程截图；（5分）
7. 通过对该任务题目5页面注入点进行SQL注入渗透测试，删除DCST中的WebServ2003服务器场景的C:\目录下的1.txt文档，并将注入代码及测试过程截图；（5分）
8. 进入DCST中的WebServ2003服务器场景的C:\AppServ\www目录，找到QueryCtrl.php程序，使用EditPlus工具分析并修改PHP源程序，使之可以抵御SQL注入渗透测试，并将修改后的PHP源程序截图；（10分）
9. 再次对该任务题目5页面注入点进行渗透测试，验证此次利用注入点对该WebServ2003服务器场景进行SQL注入渗透测试无效，并将验证过程截图。（5分）

### 任务2：XSS和CSRF攻防（65分）

**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）

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，"/"->" Employee Message Board"，分析该页面源程序，找到提交的变量名，并截图；（5分）
2. 对该任务题目1页面注入点进行XSS渗透测试，并进入"/"->" Employee Message Board"->"Display Message"页面，根据该页面的显示，确定是注入点，并将测试过程截图；（5分）
3. 对该任务题目1页面注入点进行渗透测试，使"/"->" Employee Message Board"->"Display Message"页面的访问者执行网站（http://hacker.org/）中的木马程序：http://hacker.org/TrojanHorse.exe，并将注入代码及测试过程截图；（5分）
4. 通过IIS搭建网站（http://hacker.org/），并通过PC-3生成木马程序TrojanHorse.exe，将该程序复制到网站（http://hacker.org/）的WWW根目录下，并将搭建该网站结果截图；（5分）
5. 当"/"->" Employee Message Board"->"Display Message"页面的访问者执行网站（http://hacker.org/）中的木马程序TrojanHorse.exe以后，访问者主机需要被PC-3远程控制，打开访问者主机的CMD.exe命令行窗口，并将该操作过程截图；（5分）
6. 进入DCST中的WebServ2003服务器场景的C:\AppServ\www目录，找到insert.php程序，使用EditPlus工具分析并修改PHP源程序，使之可以抵御XSS渗透测试，并将修改后的PHP源程序截图；（10分）
7. 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XSS渗透测试无效，并将验证过程截图；（5分）
8. 在PC-1上，Web访问DCST中的WebServ2003服务器场景，"/"->" Shopping Hall"，分析该页面源程序，找到提交的变量名，并截图；（5分）
9. 对该任务题目1页面注入点进行渗透测试，使"/"->" Employee Message Board"->"Display Message"页面的访问者向页面ShoppingProcess.php提交参数goods=cpu&quantity=999999，查看"/"->"PurchasedGoods.php页面，并将注入代码及测试过程截图；（5分）
10. 进入DCST中的WebServ2003服务器场景的C:\AppServ\www目录，找到DisplayMessage.php程序，使用EditPlus工具分析并修改PHP源程序，使之可以抵御CSRF渗透测试，并将修改后的源程序截图；（10分）
11. 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CSRF渗透测试无效，并将验证过程截图；（5分）

### 任务3：命令注入与文件包含攻防（50分）

**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）

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，"/"->" Display Directory"，分析该页面源程序，找到提交的变量名，并截图；（5分）
2. 对该任务题目1页面注入点进行渗透测试，使页面DisplayDirectoryCtrl.php回显C:\Windows目录内容的同时，对WebServ2003服务器场景添加账号“Hacker”，将该账号加入管理员组，并将注入代码及测试过程截图；（5分）
3. 进入DCST中的WebServ2003服务器场景的C:\AppServ\www目录，找到DisplayDirectoryCtrl.php程序，使用EditPlus工具分析并修改PHP源程序，使之可以抵御命令注入渗透测试，并将修改后的源程序截图；（10分）
4. 再次对该任务题目1页面注入点进行渗透测试，验证此次利用注入点对该DCST中的WebServ2003服务器场景进行命令注入渗透测试无效，并将验证过程截图；（5分）
5. 在PC-1上，Web访问DCST中的WebServ2003服务器场景，"/"->" Display Uploaded's File Content"，分析该页面源程序，找到提交的变量名，并截图；（5分）
6. 对该任务题目5页面注入点进行渗透测试，使页面DisplayFileCtrl.php回显DCST中的WebServ2003服务器场景访问日志文件：AppServ/Apache2.2/logs/access.log的内容，并将注入代码及测试过程截图；（5分）
7. 进入DCST中的WebServ2003服务器场景的C:\AppServ\www目录，找到DisplayFileCtrl.php程序，使用EditPlus工具分析并修改PHP源程序，使之可以抵御文件包含渗透测试，并将修改后的源程序截图；（10分）
8. 再次对该任务题目5页面注入点进行渗透测试，验证此次利用注入点对该DCST中的WebServ2003服务器场景进行文件包含渗透测试无效，并将验证过程截图。（5分）

### 任务4：MAC协议安全攻防（45分）

**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1：Metasploit Framework

虚拟机安装服务/工具2：Macof

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；

多层交换机：

交换机操作平台：DCRS-5650-28

1. 将PC-1、PC-3所连接端口划入与WAF同一VLAN（VLAN10），并将PC-1、PC-3分配与DCST服务器相同网段IP地址，使PC-1、PC-3、DCST中的WebServ2003服务器场景能够在同一个网段（VLAN10）内相互Ping通。（2分）
2. 查看DCRS交换机VLAN10的MAC地址表容量信息，并将DCRS交换机配置相关参数、查看命令、查看结果截图。（3分）
3. 从PC-3发起MAC Flooding渗透测试，使DCRS交换机的MAC地址表溢出，使其在MAC地址表溢出的条件下，无法学习到PC-1和DCST中的WebServ2003服务器场景的MAC地址表信息，查看DCRS交换机的MAC地址表信息，并将渗透测试过程截图。（5分）
4. PC-3打开wireshark，验证在DCRS交换机MAC地址表溢出的条件下，可以监听到PC-1访问DCST中的WebServ2003服务器场景的HTTP流量，并将该验证过程截图。（5分）
5. 在DCRS交换机的PC-3所连接端口配置Port Security特性，阻止PC-3发起MAC Flooding渗透测试，验证此时DCRS交换机MAC地址表能够学习到PC-1、DCST中的WebServ2003服务器场景的MAC地址，并将DCRS交换机相关配置信息以及验证信息截图。（8分）
6. 在DCRS交换机配置Port Security特性的条件下，PC-3再次打开wireshark，监听PC-1访问DCST中的WebServ2003服务器场景流量，验证此时PC-3无法监听到PC-1访问DCST中的WebServ2003服务器场景的HTTP流量，并将验证过程截图。（7分）
7. 将DCRS交换机Port Security配置删除，配置DCRS交换机Access Management特性来阻止PC-3发起MAC Flooding渗透测试，验证此时DCRS交换机MAC地址表能够学习到PC-1、DCST中的WebServ2003服务器场景的MAC地址，并将DCRS交换机相关配置信息以及验证信息截图。（8分）
8. 在DCRS交换机配置Access Management特性的条件下，PC-3再次打开wireshark，监听PC-1访问DCST中的WebServ2003服务器场景流量，验证此时PC-3无法监听到PC-1访问DCST中的WebServ2003服务器场景的HTTP流量，并将验证过程截图。（7分）

### 任务5：ARP协议安全攻防（45分）

**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1：Metasploit Framework

虚拟机安装服务/工具2：Arpspoof

虚拟机安装服务/工具3：Ettercap

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；

多层交换机：

交换机操作平台：DCRS-5650-28

1. 在PC-1访问DCST中的WebServ2003服务器场景时，查看PC-1和DCST中的WebServ2003服务器场景的ARP缓存信息，并将PC-1和DCST中的WebServ2003服务器场景的ARP缓存信息截图。（5分）
2. 在PC-3对PC-1进行ARP Spoofing渗透测试，使PC-1无法访问DCST中的WebServ2003服务器场景，PC-1的ARP缓存为：DCST中的WebServ2003服务器场景IP->PC-3的MAC地址，在PC-1查看被PC-3毒化后的ARP缓存信息，并将该信息截图。（5分）
3. 在PC-3对PC-1和DCST中的WebServ2003服务器场景进行ARP中间人渗透测试，使PC-3能够使用wireshark监听到PC-1向DCST中的WebServ2003服务器场景的LoginAuth.php页面提交的登录网站用户名、密码参数，并将该渗透测试过程截图。（7分）
4. 在DCRS交换机上配置Access Management特性阻止PC-3发起ARP Spoofing渗透测试，并将DCRS交换机该配置信息截图。（5分）
5. 在DCRS交换机上配置Access Management特性的条件下，再次在PC-3对PC-1和DCST中的WebServ2003服务器场景进行ARP Spoofing渗透测试，此时DCRS交换机的Access Management特性能够阻止PC-3对PC-1和DCST中的WebServ2003服务器场景进行ARP Spoofing渗透测试，再次查看PC-1和DCST中的WebServ2003服务器场景的ARP缓存信息，并将该信息截图。（8分）
6. 在DCRS交换机上删除Access Management技术配置，通过IP DHCP Snooping Bind特性来阻止PC-3发起ARP Spoofing渗透测试，并将DCRS交换机相关配置信息截图。（7分）
7. 在DCRS交换机上配置IP DHCP Snooping Bind特性的条件下，再次在PC-3对PC-1和DCST中的WebServ2003服务器场景进行ARP Spoofing渗透测试，此时DCRS交换机的IP DHCP Snooping Bind特性能够阻止PC-3对PC-1和DCST中的WebServ2003服务器场景进行ARP Spoofing渗透测试，再次查看PC-1和DCST中的WebServ2003服务器场景的ARP缓存信息，并将该信息截图。（8分）

### 任务6：Spanning Tree协议安全攻防（40分）

**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1：Metasploit Framework

虚拟机安装服务/工具2：Yersinia

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；

多层交换机：

交换机操作平台：DCRS-5650-28

1. 在DCRS交换机开启生成树协议，生成树协议模式为STP，DCRS交换机优先级为0，防止网络出现物理环路，显示DCRS交换机生成树协议的状态，并将该信息截屏；（5分）
2. 在PC-3向DCRS交换机发起Take Over The Root Bridge渗透测试，使DCRS交换机认为PC-3为Root Bridge，显示DCRS交换机生成树协议的状态，并将该信息截屏；（5分）
3. 配置DCRS交换机生成树协议安全特性，阻止Take Over The Root Bridge渗透测试，并将DCRS交换机相关配置信息截屏；（7分）
4. 在DCRS交换机配置生成树协议安全特性的条件下，DCRS交换机不会认为渗透测试平台为Root Bridge，由PC-3再次向DCRS交换机发起Take Over The Root Bridge渗透测试，再次显示DCRS交换机生成树协议的状态，并将以上验证过程截屏；（8分）
5. 由PC-3向DCRS交换机发起BPDU DOS渗透测试，提高DCRS交换机CPU的利用率为50%以上，显示DCRS交换机CPU的利用率，并将该信息截屏；（5分）
6. 配置DCRS交换机生成树协议安全特性，阻止BPDU DOS渗透测试，并将配置信息截屏；（5分）
7. 在DCRS交换机配置生成树协议安全特性的条件下，DCRS交换机不会受PC-3的BPDU DOS渗透测试影响，此时由PC-3再次向DCRS交换机发起BPDU DOS渗透测试，显示DCRS交换机CPU的利用率，并将该验证截屏；（5分）

**备注：提交文档数量与命名**

|  |  |  |  |
| --- | --- | --- | --- |
| **阶段** | **任务** | **序号** | **文档名称** |
| 第一阶段 | 任务1 | 1 | 第一阶段-任务1-网络平台搭建 |
| 2 | 赛场IP参数表 |
| 任务2 | 3 | 第一阶段-任务2-网络安全设备配置与防护-DCFW |
| 4 | 第一阶段-任务2-网络安全设备配置与防护-DCFS |
| 5 | 第一阶段-任务2-网络安全设备配置与防护-NETLOG |
| 6 | 第一阶段-任务2-网络安全设备配置与防护-DCRS |
| 7 | 第一阶段-任务2-网络安全设备配置与防护-WAF |
| 第二阶段 | 任务1 | 8 | 第二阶段-任务1-SQL注入攻防 |
| 任务2 | 9 | 第二阶段-任务2-XSS和CSRF攻防 |
| 任务3 | 10 | 第二阶段-任务3-命令注入与文件包含攻防 |
| 任务4 | 11 | 第二阶段-任务4-Ethernet协议安全攻防 |
| 任务5 | 12 | 第二阶段-任务5-ARP协议安全攻防 |
| 任务6 | 13 | 第二阶段-任务6- Spanning Tree协议安全攻防 |

1. **第三阶段：分组对抗（400分）**

假定各位选手是某公司的系统管理员，负责服务器（受保护服务器IP、管理员账号见现场发放的参数表）的维护，该服务器可能存在着各种问题和漏洞（见漏洞列表）。你需要尽快对服务器进行加固，十五分钟之后将会有很多黑客对这台服务器进行猛烈地攻击。

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：加固常规漏洞取得KEY值并提交到裁判服务器中（裁判服务器网址见现场发放的参数表）；

提示4：加固系统漏洞取得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80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：KEY值为漏洞点的特征值，有多个；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：运行flagsubmit程序将提取服务器的硬件及相关信息作为标识，可以通过在靶机上运行命令‘flagsubmit–h’来查看帮助。因此，请注意如果在本机找到的KEY或者FLAG请在本机运行，如果在其他机器找到的KEY或者FLAG请在其他机器系统内运行。

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（其他服务器网段见现场发放的参数表）。

**漏洞列表：**

1. 选手需要提前加固靶机漏洞，在一些加固点存在KEY值，获取KEY值并提交。
2. 系统提供弱口令用户，要求用户能够检出弱口令用户，并根据描述提供相关的KEY。
3. 靶机上的网站存在SQL注入的漏洞，要求选手找到SQL注入的相关漏洞，获取到靶机的数据库，在数据库中获取到相关KEY值进行提交。
4. 靶机上的网站上存在COOKIE漏洞，要求选手找到COOKIE注入的漏洞并获取KEY值进行提交。
5. 靶机上的一些端口上存在敏感信息，要求选手找到存在敏感信息的端口，并获取KEY值进行提交。
6. 靶机上可以提供用户下载加密文件，要求选手通过破解文件来获取KEY值进行提交。
7. 靶机上的网站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。
8. 靶机中存在服务端请求伪造攻击漏洞，要求选手找到相关漏洞，并利用此漏洞获取一定权限。
9. 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
10. 靶机上的网站存在文件包含漏洞，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
11. 操作系统提供的服务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。
12. 操作系统提供的服务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。
13. 系统环境搭建了存在Java反序列化漏洞的服务，要求选手找到此漏洞并利用此漏洞获取一定权限。
14. 靶机中存在一些系统后门，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。
15. 靶机中搭建了Redis数据库并存在未授权访问漏洞，要求选手找到此漏洞并利用此漏洞获取一定权限。
16. 靶机中搭建了Rsync的数据镜像备份工具并存在Rsync未授权访问漏洞，要求选手找到此漏洞并利用此漏洞获取一定权限。
17. 系统提供mysql服务，要求用户能够对root口令进行暴力破解获取弱口令，并获取权限。
18. 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。