

# 2018 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-09

## 一、 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。

## 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	9:00-1 3:30	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	XSS 渗透测试与安全开发		60
	任务 2	命令注入渗透测试与安全开发		60
	任务 3	密码学与 IPSec 应用		60
	任务 4	ICMP 扫描渗透测试		60
	任务 5	路由协议安全渗透测试		80
	任务 6	逆向分析和缓冲区溢出渗透测试		80
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。

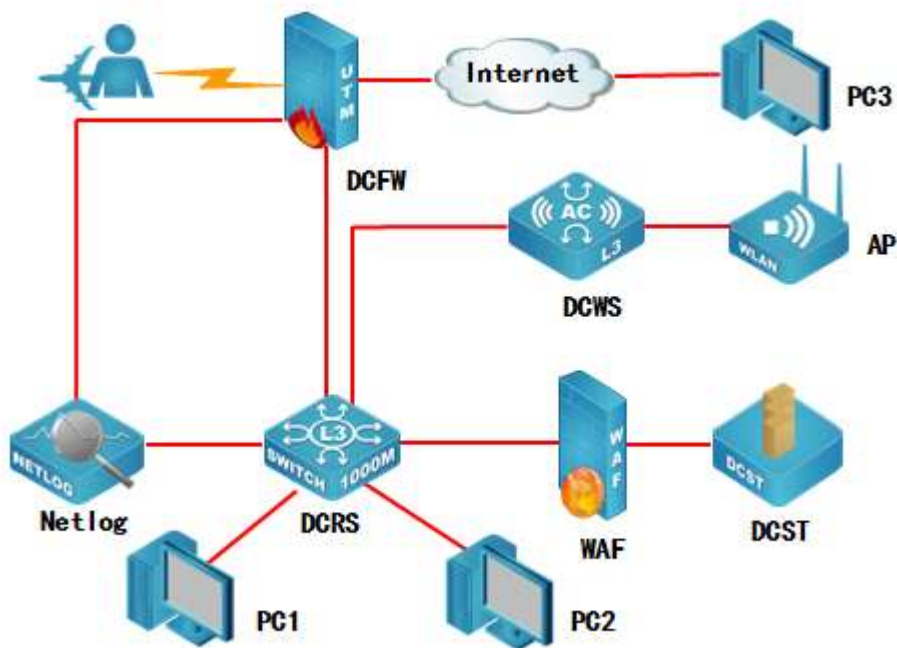
选手首先需要在 U 盘的根目录下建立一个名为“GWxx”的文件夹（xx 用具体的工位号替代），赛题第一阶段所完成的“XXX-答题模板”放置在文件夹中。

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“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。

## （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	10.0.0.2/30	DCFW

	ETH1/0/2		
	VLAN 1002	10.0.0.5/30	DCWS
	ETH1/0/1		
	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		
日志服务器 Netlog	ETH1/0/6-9	192.168.40.1/24	PC1
	管理 VLAN		
	VLAN 100	192.168.100.1/24	
堡垒服务器 DCST	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)

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	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 public9;
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;
6. DCFW 上配置 NAT 功能,使 PC2 能够通过 Web 方式正常管理到 AC,端口号使用 6669;)合理配置安全策略;
7. 在 DCFW 做相关配置要求防火墙能够记录每天 9:00-18:00 内网用户访问外网的 URL,保存在日志服务器;
8. 配置防火墙 Web 外发信息控制策略,禁止内网无线用户到所有网站的 Web 外发信息控制;内网有线用户到外网网站 Web 外发信息控制,禁止外发关键字“攻击”“病毒”,信任值为 1,并记录相关日志。
9. DCFW 做相关配置要求内网用户不能登录 QQ 和 MSN;
10. DCFW 上配置限制内网用户访问 www.google.com 限制内网用户访问 URL 中带有 google 关键字的所有网站;

### Netlog:

11. 在 DCB-netlog 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;要求对内网访问 Internet 全部应用进行记录日志;

12. 在 DCBI-netlog 上配置, 监控周一至周五 9: 00-18: 00 无线用户所在网段访问的 URL 中包含 google 的 HTTP 访问记录, 并且邮件发送告警;
13. 在 DCBI 上配置, 添加内容规则, 对于网站访问关键字包含“谷歌”的, 记录并邮件报警;
14. 在 DCBI 上配置, 使 DCBI 能够通过邮件方式发送告警信息, 邮件服务器 IP 172. 16. 100. 20, 端口号 25, 账号 test9dcn, 密码 test9, 当 DCBI 磁盘使用率超过 85%时发送一次报警;
15. 在 DCBI 上配置, 将 DCBI 的日志信息发送到日志服务器, 日志服务器 IP 172. 16. 100. 10, community 名字 public3;
16. 在 DCBI 上配置, 增加非 admin 账户 DCN2019, 密码 dcbi9999, 该账户仅用于用户查询设备的日志信息和统计信息;
17. DCBI 配置应用及应用组“P2P 下载”, UDP 协议端口号范围 40900-42000, 在周一至周五 9: 00-18: 00 监控 LAN 中所有用户的“P2P 下载”访问记录并告警;

#### WAF:

18. 在 WAF 上配置, 公司内部有一台网站服务器直连到 WAF, IP 地址是 172. 16. 100. 30, 端口是 8080, 并将服务访问日志、Web 防护日志、服务监控日志发送至 syslog 日志服务器, syslog 日志服务器 IP 地址是 172. 16. 100. 10, UDP 的 514 端口;
19. 在公司总部的 WAF 上配置, 将攻击告警、设备状态告警信息通过邮件(发送到 DCN@digitalchina.com)及短信方式(发送到 13913814949)发送给管理员;
20. 在公司总部的 WAF 上配置, 禁止公网 IP 地址 (218. 5. 18. 2) 访问网站服务器, 网站服务器 IP 地址是 172. 16. 100. 30;
21. 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: 并发访问超过 5000 次请求;
22. 在 WAF 上配置, 开启基于 session cookie 的 CC 防护, 最大请求数为 5000, 超过进行阻断;

#### DCRS:

23. 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 45 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; 连接 PC1 的接口为专用接口, 限定只允许 PC1 的 MAC 地址可以连接;
24. 将连接 DCFW 的双向流量镜像至 Netlog 进行监控和分析;
25. 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;

26. 在公司总部的 DCRS 上配置端口环路检测 (Loopback Detection)，防止来自 VLAN200 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 30 秒，不存在环路时的检测时间间隔为 10 秒；
27. 为了控制接入网络 PC，需要在交换 ETH1/0/10 口开启 DOT1X 认证，配置认证服务器，IP 地址是 172.16.100.40，radius key 是 dcn2019；
28. 交换机开启远程管理，使用 SSH 方式账号为 DCN2019，密码为 999999；
29. VLAN20、VLAN30、VLAN10 用户采用动态获取 IP 地址方式，DHCP 服务器在 AC 上配置，前十个地址为保留地址，VLAN40 用户也动态获取 IP，DHCP server 为 DCFW；
30. 在交换机上配置，在只允 VLAN200 用户在上班时间(周一到周五 8:00 到 18:00)内访问 VLAN100 段 IP；
31. 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，VLAN30 用户的 ARP 阈值为 90；
32. 为了防止 VLAN40 网段 arp 欺骗，需要在交换机上开启 ip dhcp snooping 并在接口下绑定用户；
33. 在 DCRS 上配置，配置设备 enable 密码，密码为 dcn2019，并且在登录设备时必须正确输入 enable 密码才能进入交换机的配置模式；
34. DCRS 上配置，VLAN40 的成员接口开启广播风暴抑制功能，参数设置为 2900pps；

#### DCWS:

35. AP 通过 option43 方式进行正常注册上线，AC 地址为管理 VLANIP；
36. 设置 SSID DCN2019，VLAN10，加密模式为 wpa-personal，其口令为 GSdcn2019 的；  
设置 SSID dcntest，VLAN20 不进行认证加密，做相应配置隐藏该 ssid；
37. 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；
38. 通过配置避免接入终端较多且有大量弱终端时，高速客户端被低速客户端“拖累”，低速客户端不至于长时间得不到传输；
39. 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；
40. AC 开启 Web 管理，账号密码为 DCN2019；

### (三) 第二阶段任务书 (400 分)

#### 任务 1: XSS 渗透测试与安全开发 (60 分)

##### 任务环境说明:

攻击机:

注意: 攻击机须使用物理机中的虚拟机



物理机操作系统: Windows7 64 位旗舰版  
虚拟机操作系统 1: Ubuntu Linux 32bit  
虚拟机操作系统 1 安装工具 1: Python3  
虚拟机操作系统 1 安装工具 2: WireShark  
虚拟机操作系统 1 安装工具 3: GCC  
虚拟机网卡与物理机网卡之间的关系: Bridge (桥接)  
用户名: root, 密码: 123456  
虚拟机操作系统 2: CentOS Linux 5.5  
虚拟机操作系统安装工具 1: GCC  
虚拟机操作系统安装工具 2: GDB  
用户名: root, 密码: 123456

靶机:

服务器场景: Web Server

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;

任务内容:

1. Web 访问靶机服务器场景, 完成如下任务: a、进入"/"->"Employee Message Board" 页面, 对该页面进行 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"/"->"Employee Message Board" 页面存在 XSS 注入点; b、进入靶机服务器场景的 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, 填写 insert.php 程序当中空缺的 FLAG01 字符串, 将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交 (形式: 十六进制字符串);
2. 继续修改本任务题目 1 中的 insert.php 源程序, 使之可以抵御 XSS 渗透测试, 填写 insert.php 程序当中空缺的 FLAG02 字符串, 将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交 (形式: 十六进制字符串);
3. 继续修改本任务题目 1 中的 insert.php 源程序, 使之可以抵御 XSS 渗透测试, 填写 insert.php 程序当中空缺的 FLAG03 字符串, 将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交 (形式: 十六进制字符串);
4. 继续修改本任务题目 1 中的 insert.php 源程序, 使之可以抵御 XSS 渗透测试, 填写 insert.php 程序当中空缺的 FLAG04 字符串, 将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交 (形式: 十六进制字符串);
5. 继续修改本任务题目 1 中的 insert.php 源程序, 使之可以抵御 XSS 渗透测试, 填写 insert.php 程序当中空缺的 FLAG05 字符串, 将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交 (形式: 十六进制字符串);

6. 继续修改本任务题目 1 中的 insert.php 源程序,使之可以抵御 XSS 渗透测试,填写 insert.php 程序当中空缺的 FLAG06 字符串,将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交(形式:十六进制字符串);

## 任务 2: 命令注入渗透测试与安全开发 (60 分)

### 任务环境说明:

攻击机:

注意: 攻击机须使用物理机中的虚拟机

物理机操作系统: Windows7 64 位旗舰版

虚拟机操作系统 1: Ubuntu Linux 32bit

虚拟机操作系统 1 安装工具 1: Python3

虚拟机操作系统 1 安装工具 2: WireShark

虚拟机操作系统 1 安装工具 3: GCC

虚拟机网卡与物理机网卡之间的关系: Bridge (桥接)

用户名: root, 密码: 123456

虚拟机操作系统 2: CentOS Linux 5.5

虚拟机操作系统安装工具 1: GCC

虚拟机操作系统安装工具 2: GDB

用户名: root, 密码: 123456

靶机:

服务器场景: Web Server

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;

### 任务内容:

1. Web 访问靶机服务器场景,完成如下任务: a、进入"/"->"Display Directory"页面,对该页面进行渗透测试,使页面 DisplayDirectoryCtrl.php 回显 C:\Windows 目录内容的同时,对靶机服务器场景操作系统添加账号“Hacker”,并将该账号加入管理员组;b、进入靶机服务器场景的 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,使之可以抵御本小题以上渗透测试过程,填写 DisplayDirectoryCtrl.php 程序当中空缺的 FLAG01 字符串,将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交(形式:十六进制字符串);
2. 继续修改本任务题目 1 中的 DisplayDirectoryCtrl.php 源程序,使之可以抵御本任务题目 1 中的渗透测试过程,填写 DisplayDirectoryCtrl.php 程序当中空缺的 FLAG02 字符串,将该字



- 串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交(形式:十六进制字符串) ;
3. 继续修改本任务题目1中的DisplayDirectoryCtrl.php源程序,使之可以抵御本任务题目1中的渗透测试过程,填写DisplayDirectoryCtrl.php程序当中空缺的FLAG03字符串,将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交(形式:十六进制字符串) ;
  4. 继续修改本任务题目1中的DisplayDirectoryCtrl.php源程序,使之可以抵御本任务题目1中的渗透测试过程,填写DisplayDirectoryCtrl.php程序当中空缺的FLAG04字符串,将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交(形式:十六进制字符串) ;
  5. 继续修改本任务题目1中的DisplayDirectoryCtrl.php源程序,使之可以抵御本任务题目1中的渗透测试过程,填写DisplayDirectoryCtrl.php程序当中空缺的FLAG05字符串,将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交(形式:十六进制字符串) ;
  6. 继续修改本任务题目1中的DisplayDirectoryCtrl.php源程序,使之可以抵御本任务题目1中的渗透测试过程,填写DisplayDirectoryCtrl.php程序当中空缺的FLAG06字符串,将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交(形式:十六进制字符串) ;

### 任务3: 密码学与IPSec应用(60分)

#### 任务环境说明:

攻击机:

注意: 攻击机须使用物理机中的虚拟机

物理机操作系统: Windows7 64位旗舰版

虚拟机操作系统: Microsoft Windows2003 Server

虚拟机操作系统安装工具1: Microsoft Windows CA服务

虚拟机操作系统安装工具2: WireShark1.1

虚拟机网卡与物理机网卡之间的关系: Bridge(桥接)

用户名: administrator, 密码: 123456

靶机:

服务器场景: Windows Server

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

#### 任务内容:

1. 通过IPSec传输模式保护保护从攻击机到靶机之间的全部流量(预共享密钥: www.dcn.com), 使用靶机数据库user表中第一条记录中的用户

- 名、密码信息登录靶机网站，打开攻击机工具软件 WireShark 对攻击机和靶机之间的数据对象进行捕获；成功登录靶机服务器场景 Web 页面 login.php 之后，对攻击机登录靶机 Web 站点动作的数据对象进行分析，将 ISAKMP 主模式第 1 个数据对象长度十进制数值通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
2. 通过 IPSec 传输模式保护保护从攻击机到靶机之间的全部流量（预共享密钥：www.dcn.com），使用靶机数据库 user 表中第一条记录中的用户名、密码信息登录靶机网站，打开攻击机工具软件 WireShark 对攻击机和靶机之间的数据对象进行捕获；成功登录靶机服务器场景 Web 页面 login.php 之后，对攻击机登录靶机 Web 站点动作的数据对象进行分析，将 ISAKMP 主模式第 2 个数据对象长度十进制数值通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
  3. 通过 IPSec 传输模式保护保护从攻击机到靶机之间的全部流量（预共享密钥：www.dcn.com），使用靶机数据库 user 表中第一条记录中的用户名、密码信息登录靶机网站，打开攻击机工具软件 WireShark 对攻击机和靶机之间的数据对象进行捕获；成功登录靶机服务器场景 Web 页面 login.php 之后，对攻击机登录靶机 Web 站点动作的数据对象进行分析，将 ISAKMP 快速模式第 1 个数据对象长度十进制数值通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
  4. 通过 IPSec 传输模式保护保护从攻击机到靶机之间的全部流量（预共享密钥：www.dcn.com），使用靶机数据库 user 表中第一条记录中的用户名、密码信息登录靶机网站，打开攻击机工具软件 WireShark 对攻击机和靶机之间的数据对象进行捕获；成功登录靶机服务器场景 Web 页面 login.php 之后，对攻击机登录靶机 Web 站点动作的数据对象进行分析，将 ISAKMP 快速模式第 2 个数据对象长度十进制数值通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
  5. 通过 IPSec 传输模式保护保护从攻击机到靶机之间的全部流量（预共享密钥：www.dcn.com），使用靶机数据库 user 表中第一条记录中的用户名、密码信息登录靶机网站，打开攻击机工具软件 WireShark 对攻击机和靶机之间的数据对象进行捕获；成功登录靶机服务器场景 Web 页面 login.php 之后，对攻击机登录靶机 Web 站点动作的数据对象进行分析，将 ISAKMP 快速模式第 3 个数据对象长度十进制数值通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
  6. 通过 IPSec 传输模式保护保护从攻击机到靶机之间的全部流量（预共享密钥：www.dcn.com），使用靶机数据库 user 表中第一条记录中的用户名、密码信息登录靶机网站，打开攻击机工具软件 WireShark 对攻击机和靶机之间的数据对象进行捕获；成功登录靶机服务器场景 Web 页面 login.php 之后，对攻击机登录靶机 Web 站点动作的数据对象进行分析，将 ISAKMP 快速模式第 4 个数据对象长度十进制数值通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；

## 任务 4: ICMP 扫描渗透测试 (60 分)

### 任务环境说明:

攻击机:

注意: 攻击机须使用物理机中的虚拟机

物理机操作系统: Windows7 64 位旗舰版

虚拟机操作系统: Ubuntu Linux 32bit

虚拟机操作系统安装工具 1: Python3

虚拟机操作系统安装工具 2: WireShark

虚拟机网卡与物理机网卡之间的关系: Bridge (桥接)

用户名: root, 密码: 123456

虚拟机操作系统 2: CentOS Linux 5.5

虚拟机操作系统安装工具 1: GCC

虚拟机操作系统安装工具 2: GDB

用户名: root, 密码: 123456

靶机:

服务器场景: Windows Server

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

服务器场景 FTP 下载服务用户名: anonymous, 密码: 123456

服务器场景 FTP 下载服务端口: 2121

服务器场景 FTP 上传服务用户名: anonymous, 密码: 123456

服务器场景 FTP 上传服务端口: 21

### 任务内容:

1. 从靶机服务器场景的 FTP 服务器中下载文件 scan02.py, 编辑该 Python3 程序文件, 使该程序实现从攻击机对靶机进行的 ICMP 类型的主机在线探测渗透测试, 填写该文件当中空缺的 FLAG01 字符串, 将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交 (形式: 十六进制字符串);
2. 继续编辑该任务题目 7 中的 Python3 程序文件 scan02.py, 使该程序实现从攻击机对靶机进行的 ICMP 类型的主机在线探测渗透测试, 填写该文件当中空缺的 FLAG02 字符串, 将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交 (形式: 十六进制字符串);
3. 继续编辑该任务题目 7 中的 Python3 程序文件 scan02.py, 使该程序实现从攻击机对靶机进行的 ICMP 类型的主机在线探测渗透测试, 填写该文件当中空缺的 FLAG03 字符串, 将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交 (形式: 十六进制字符串);
4. 继续编辑该任务题目 7 中的 Python3 程序文件 scan02.py, 使该程序实现从攻击机对靶机进行的 ICMP 类型的主机在线探测渗透测试, 填写该文件当中空缺的 FLAG04 字符串, 将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交 (形式: 十六进制字符串);
5. 继续编辑该任务题目 7 中的 Python3 程序文件 scan02.py, 使该程序实现从攻击机对靶机进行的 ICMP 类型的主机在线探测渗透测试, 填写该文

件当中空缺的 FLAG05 字符串,将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交(形式:十六进制字符串);

6. 通过 Python3 程序解释器执行程序文件 scan02.py,将该程序文件执行后的显示结果中,找到对应的字符填入以下形式(最后 1 行的第 1 个字符:最后 1 行的最后 1 个字符),并将该形式字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交(形式:十六进制字符串);

## 任务 5: 路由协议安全渗透测试 (80 分)

### 任务环境说明:

攻击机:

注意:攻击机须使用物理机中的虚拟机

物理机操作系统: Windows7 64 位旗舰版

虚拟机操作系统: Ubuntu Linux 32bit

虚拟机操作系统安装工具 1: Python3

虚拟机操作系统安装工具 2: WireShark

虚拟机网卡与物理机网卡之间的关系: Bridge (桥接)

用户名: root, 密码: 123456

虚拟机操作系统 2: CentOS Linux 5.5

虚拟机操作系统安装工具 1: GCC

虚拟机操作系统安装工具 2: GDB

用户名: root, 密码: 123456

靶机:

服务器场景: Windows Server

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

服务器场景 FTP 下载服务用户名: anonymous, 密码: 123456

服务器场景 FTP 下载服务端口: 2121

服务器场景 FTP 上传服务用户名: anonymous, 密码: 123456

服务器场景 FTP 上传服务端口: 21

### 任务内容:

1. 从靶机服务器场景的 FTP 服务器中下载文件 routingattack.py,并完善该 Python3 程序,实现以下功能: a、通过攻击机 WireShark 程序分析靶机发送的动态路由信息; b、通过分析到的该种类型的路由协议,对靶机路由表进行路由毒化,填写 routingattack.py 程序文件当中空缺的 FLAG01 字符串,将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交(形式:十六进制字符串);
2. 继续编辑本任务题目 1 中的 Python3 程序文件,使该程序实现同本任务题目 1 中对靶机路由表进行路由毒化功能,填写该文件当中空缺的 FLAG02 字符串,将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交(形式:十六进制字符串);

3. 继续编辑本任务题目 1 中的 Python3 程序文件，使该程序实现同本任务题目 1 中对靶机路由表进行路由毒化功能，填写该文件当中空缺的 FLAG03 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
4. 继续编辑本任务题目 1 中的 Python3 程序文件，使该程序实现同本任务题目 1 中对靶机路由表进行路由毒化功能，填写该文件当中空缺的 FLAG04 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
5. 继续编辑本任务题目 1 中的 Python3 程序文件，使该程序实现同本任务题目 1 中对靶机路由表进行路由毒化功能，填写该文件当中空缺的 FLAG05 字符串，将该字符串通过 MD5 运算后返回的哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；

## 任务 6：逆向分析和缓冲区溢出渗透测试（80 分）

### 任务环境说明：

攻击机：

注意：攻击机须使用物理机中的虚拟机

物理机操作系统：Windows7 64 位旗舰版

虚拟机操作系统 1：Ubuntu Linux 32bit

虚拟机操作系统 1 安装工具 1：Python3

虚拟机操作系统 1 安装工具 2：WireShark

虚拟机操作系统 1 安装工具 3：GCC

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

用户名：root，密码：123456

虚拟机操作系统 2：CentOS Linux 5.5

虚拟机操作系统安装工具 1：GCC

虚拟机操作系统安装工具 2：GDB

用户名：root，密码：123456

靶机：

服务器场景 1：Windows Server

服务器场景 1 操作系统：Microsoft Windows2003 Server

服务器场景 1 的 FTP 下载服务用户名：anonymous，密码：123456

服务器场景 1 的 FTP 下载服务端口：2121

服务器场景 1 的 FTP 上传服务用户名：anonymous，密码：123456

服务器场景 1 的 FTP 上传服务端口：21

服务器场景 2：LinuxServer

服务器场景 2 操作系统：CentOS Linux 5.5

### 任务内容：



1. 从靶机服务器场景的 FTP 服务器中下载可执行文件 **OverFlow**，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP: 4444 端口进行渗透测试，获得靶机根路径下的文件 **FLAG01** 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 **Flag** 值提交（形式：十六进制字符串）；
2. 从靶机服务器场景的 FTP 服务器中下载可执行文件 **OverFlow**，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP: 4444 端口进行渗透测试，获得靶机根路径下的文件 **FLAG02** 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 **Flag** 值提交（形式：十六进制字符串）；
3. 从靶机服务器场景的 FTP 服务器中下载可执行文件 **OverFlow**，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP: 4444 端口进行渗透测试，获得靶机根路径下的文件 **FLAG03** 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 **Flag** 值提交（形式：十六进制字符串）；
4. 从靶机服务器场景的 FTP 服务器中下载可执行文件 **OverFlow**，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP: 4444 端口进行渗透测试，获得靶机根路径下的文件 **FLAG04** 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 **Flag** 值提交（形式：十六进制字符串）；
5. 从靶机服务器场景的 FTP 服务器中下载可执行文件 **OverFlow**，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP: 4444 端口进行渗透测试，获得靶机根路径下的文件 **FLAG05** 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 **Flag** 值提交（形式：十六进制字符串）；
6. 从靶机服务器场景的 FTP 服务器中下载可执行文件 **OverFlow**，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP: 4444 端口进行渗透测试，获得靶机根路径下的文件 **FLAG06** 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 **Flag** 值提交（形式：十六进制字符串）；
7. 从靶机服务器场景的 FTP 服务器中下载可执行文件 **OverFlow**，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP: 4444 端口进行渗透测试，获得靶机根路径下的文件 **FLAG07** 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 **Flag** 值提交（形式：十六进制字符串）；
8. 从靶机服务器场景的 FTP 服务器中下载可执行文件 **OverFlow**，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP: 4444 端口进行渗透测试，获得靶机根路径下的文件 **FLAG08** 中的字符串，并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 **Flag** 值提交（形式：十六进制字符串）；
9. 从靶机服务器场景的 FTP 服务器中下载可执行文件 **OverFlow**，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP: 4444 端口进行渗透测试，获得靶机根路



径下的文件 FLAG09 中的字符串,并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交(形式:十六进制字符串);

10. 从靶机服务器场景的 FTP 服务器中下载可执行文件 OverFlow,通过攻击机调试工具,对以上可执行文件进行逆向分析;通过缓冲区溢出渗透测试方法对服务器场景 2 的 TCP: 4444 端口进行渗透测试,获得靶机根路径下的文件 FLAG10 中的字符串,并将该字符串通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交(形式:十六进制字符串);

#### (四) 第三阶段任务书 (300 分)

假定各位选手是 DCN 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。

注意事项:

注意 1: 任何时候不能人为关闭服务器的服务端口 1-1024;

注意 2: 不能对裁判服务器进行攻击;

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;

注意 4: 不得人为恶意破坏自己服务器的 Flag 值;

注意 5: 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。靶机的 Flag 值存放在 ./root/flagxxxxx.txt 文件内容当中。每提交 1 次对手靶机的 Flag 值增加 3 分,每当被对手提交 1 次自身靶机的 Flag 值扣除 3 分,每个对手靶机的 Flag 值只能被自己提交一次。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,各位选手可以继续加固自身的服务器,也可以攻击其他选手的服务器。

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。