2019 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

一、 赛项时间

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	270 分钟	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	Linux Kernel 提权		50
	任务 2	扫描渗透测试		50
	任务 3	Linux/x86 系统漏洞挖掘与利用		50
	任务 4	Windows/x86 系统漏洞挖掘与利用		50
	任务 5	逆向分析和缓冲区溢出渗透测试		50
	任务 6	云服务安全渗透测试		50
	任务 7	二进制漏洞挖掘与利用		50
	任务 8	操作系统安全渗透测试		50
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。

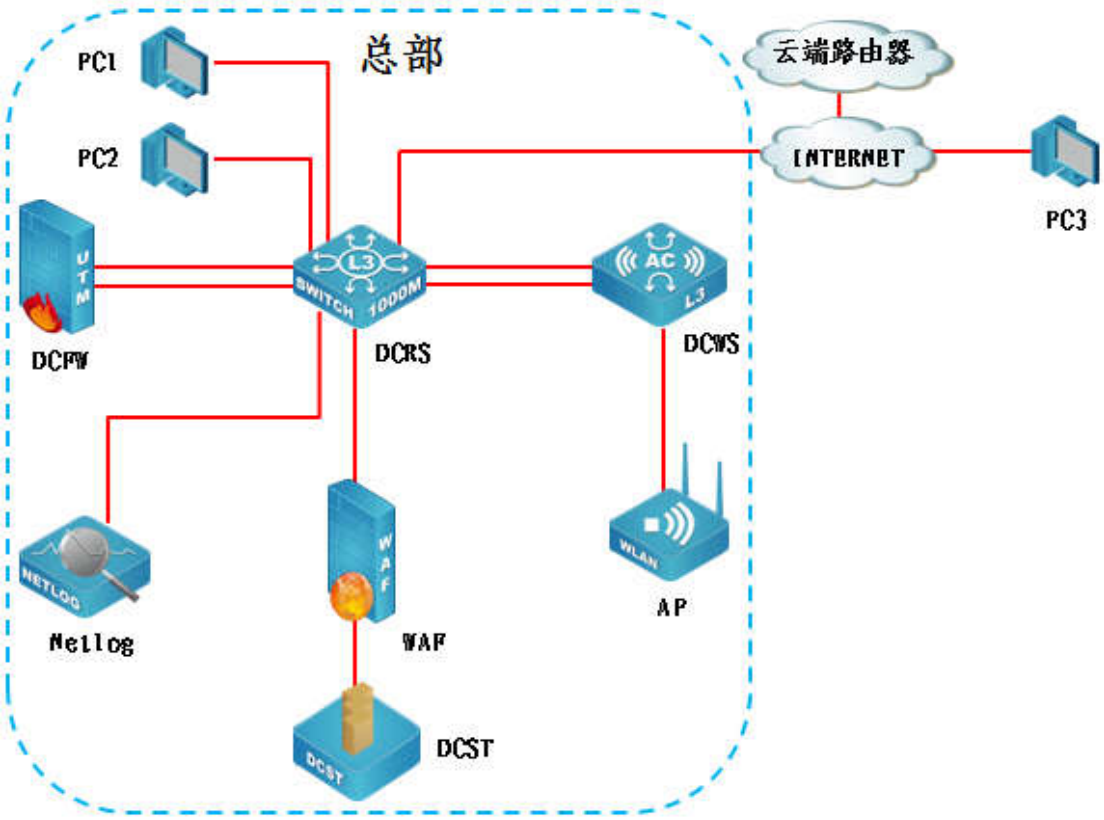
选手首先需要在U盘的根目录下建立一个名为“GWxx”的文件夹（xx用具体的工位号替代),赛题第一阶段所完成的“XXX-答题模板”放置在文件夹中。

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“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。

(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	ETH0/1-2	10.0.0.1/30（Trust 安全域）	DCRS
		218.5.18.1/27（untrust 安全域）	DCRS
		172.16.200.1/24	DCRS
	Tunnel 1	12.12.12.1/24	云端路由器
	SSL Pool	192.168.10.1/24 可用 IP 数量为 20	SSL VPN 地址池
三层交换机 DCRS	ETH1/0/4	-	DCWS ETH1/0/4
	ETH1/0/5	-	DCWS ETH1/0/5

	VLAN49 ETH1/0/1	10.0.0.2/30	DCFW
	VLAN50 ETH1/0/2	218.5.18.2/27	DCFW
	VLAN 51 ETH1/0/3	10.0.0.10/30	DCBI
	VLAN 52 ETH1/0/22	172.16.100.1/24	WAF
	VLAN 10	172.16.10.1/24	无线 1
	VLAN 20	172.16.20.1/25	无线 2
	VLAN 30 ETH1/0/7-9	172.16.30.1/26	PC1
	VLAN 40 ETH1/0/10-12	192.168.40.1/24	PC2
	VLAN 100	192.168.100.1/24	DCWS
	VLAN 200	172.16.200.2/24	DCFW
	ETH1/0/24	-	INTERNET
无线控制器 DCWS	VLAN 100	192.168.100.254/24	DCRS
	无线管理 VLAN VLAN 101 ETH1/0/3	192.168.101.1/24	AP
日志服务器 DCBI	ETH2	10.0.0.9/30	DCRS
WEB 应用防火墙 WAF	ETH2	172.16.100.2/24	DCST
	ETH3		DCRS
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	-	-	-	
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）

任务 1：网络平台搭建（60 分）

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 DCFW 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 的名称进行配置，创建 VLAN 并将相应接口划入 VLAN。
3	根据网络拓扑图所示，按照 IP 地址参数表，对 DCRS 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，对 WAF 的名称、各接口 IP 地址进行配置。

任务 2：网络安全设备配置与防护（240 分）

1. 总部核心交换机 DCRS 上开启 SSH 远程管理功能，本地认证用户名:2019DCN,密码：DCN2014;
2. 总部启用 MSTP 协议，NAME 为 DCN2014、 Revision-level 1，实例 1 中包括 VLAN10；实例 2 中包括 VLAN20、要求两条链路负载分担,其中 VLAN10 业务数据在 E1/0/4 进行数据转发，要求 VLAN20 业务数据在 E1/0/5 进行数据转发,通过在 DCWS 两个端口设置 COST 值 2000000 实现;配置 DCRS 连接终端接口立即进入转发模式且在收到 BPDU 时自动关闭端口;防止从 DCWS 方向的根桥抢占攻击;
3. 尽可能加大总部核心交换机 DCRS 与防火墙 DCFW 之间的带宽;
4. 配置使总部 VLAN10，30，40 业务的用户访问 INTERNET 往返数据流都经过 DCFW 进行最严格的安全防护;
5. 总部核心交换机 DCRS 上实现 VLAN40 业务内部终端相互二层隔离，启用环路检测，环路检测的时间间隔为 10s，发现环路以后关闭该端口，恢复时间为 30 分钟;
6. 总部核心交换机 DCRS 检测到 VLAN40 中私设 DHCP 服务器关闭该端口;

7. 总部核心交换机 DCRS 开启某项功能,防止 VLAN40 下 ARP 欺骗攻击;
8. 总部核心交换机 DCRS 上实现访问控制，在 E1/0/14 端口上配置 MAC 地址为 00-03-0f-00-00-04 的主机不能访问 MAC 地址为 00-00-00-00-00-ff 的主机;
9. 2017 年勒索蠕虫病毒席卷全球，爆发了堪称史上最大规模的网络攻击，通过对总部核心交换机 DCRS 所有业务 VLAN 下配置访问控制策略实现双向安全防护;
10. 总部部署了一套网管系统实现对核心 DCRS 交换机进行管理,网管系统 IP 为: 172.16.100.21,读团体值为: DCN2014,版本为 V2C,交换机 DCRS Trap 信息实时上报网管，当 MAC 地址发生变化时,也要立即通知网管发生的变化，每 35s 发送一次;
11. 总部核心交换机 DCRS 出口往返流量发送给 DCBI，由 DCBI 对收到的数据进行用户所要求的分析;
12. 为实现对防火墙的安全管理,在防火墙 DCFW 的 Trust 安全域开启 PING,HTTP，SNMP 功能，Untrust 安全域开启 SSH、HTTPS 功能;
13. 总部 VLAN 业务用户通过防火墙访问 Internet 时，复用公网 IP: 218.5.18.9、218.5.18.10;
14. 项目二期要启用云端路由器，需要在总部防火墙DCFW上完成以下预配:

    防火墙DCFW与云端路由器220.5.22.3建立GRE隧道，并使用IPSec保护GRE隧道，保证隧道两端2.2.2.2与VLAN20安全通信。

    第一阶段　采用pre-share认证 加密算法: 3DES;

    第二阶段　采用ESP协议，　加密算法: 3DES，预设共享秘钥

:DCN2014

15. 配置RIP完成云端路由器2.2.2.2、DCFW、总部核心交换机VLAN20的连通性，使用MD5认证，密钥为DCN2014;
16. 总部核心交换机 DCRS 上使用某种技术，将 VLAN20 通过 RIP 连接云端路由器路由与本地其它用户访问 INTERNET 路由隔离;
17. 远程移动办公用户通过专线方式接入总部网络，在防火墙 DCFW 上配置，采用 SSL 方式实现仅允许对内网 VLAN 30 的访问，用户名密码均为 DCN2014，地址池参见地址表;
18. 出于安全考虑，无线用户移动性较强，无线用户访问 INTERNET 时需要采用认证，在防火墙上开启 WEB 认证，账号密码为 DCN2014;
19. 为了保证带宽的合理使用，通过流量管理功能将引流组应用数据流，上行最小带宽设置为 2M，下行最大带宽设置为 4M;
20. 为净化上网环境，要求在防火墙DCFW做相关配置，禁止无线用户周一至周五工作时间9：00-18：00的邮件内容中含有“病毒”、“赌博”的内容，且记录日志;
21. DCBI 配置应用及应用组“流媒体”，UDP 协议端口号范围 10847-10848，

    在周一至周五 8：00-20：00 监控内网中所有用户的“流媒体”访问记录;
22. DCBI 配置对内网 ARP 数量进行统计，要求 30 分钟为一个周期;
23. DCBI 配置内网用户并发会话超过 1000，60 秒报警一次;
24. DCBI 配置监测到内网使用 RDP、Telnet 协议时，进行网页报警;
25. DCBI 配置开启用户识别功能,对内网所有 MAC 地址进行身份识别;

26. DCBI 配置统计出用户请求站点最多前 100 排名信息，发送到邮箱为 DCN2014@chinaskills.com;
27. DCBI 配置创建一个检查 2019-05-01 至 2019-05-05 这个时间段邮箱内容包含“密码”的关键字的任务;
28. WAF 上配置开启爬虫防护功能，当爬虫标识为 360Spider，自动阻止该行为;
29. WAF 上配置开启防护策略，将请求报头 DATA 自动重写为 DATE;
30. WAF 上配置开启盗链防护功能，User-Agent 参数为 PPC Mac OS X 访问 www.DCN2014.com/index.php 时不进行检查;
31. WAF 上配置开启错误代码屏蔽功能，屏蔽 404 错误代码;
32. WAF 上配置阻止用户上传 ZIP、DOC、JPG、RAR 格式文件;
33. WAF 上配置开启基本防护功能，阻止 SQL 注入、跨站脚本攻击;
34. WAF 上配置编辑防护策略，要求客户机访问内部网站时，禁止访问*.bat 的文件;
35. 无线控制器 DCWS 上配置管理 VLAN 为 VLAN101,第二个地址作为 AP 的管理地址,配置 AP 二层手工注册并启用序列号认证，要求连接 AP 的接口禁止使用 TRUNK;
36. 无线控制器 DCWS 上配置 DHCP 服务，前十个地址为保留地址，无线用户 VLAN10,20，有线用户 VLAN 30,40 从 DCWS 上动态获取 IP 地址;
37. 在 NETWORK 下配置 SSID，需求如下:

    1、NETWORK 1 下设置 SSID DCN2019，VLAN10，加密模式为 wpa-personal,其口令为 DCNE2014;

2、NETWORK 2 下设置 SSID GUEST，VLAN20 不进行认证加密,做相应配置隐藏该 SSID;

38. 配置 SSID GUEST 每天早上 0 点到 6 点禁止终端接入;

39. 在 SSID DCN2019 下启动组播转单播功能，当某一组播组的成员个数超过 8 个时组播 M2U 功能就会关闭;

40. 开启 ARP 抑制功能，开启自动强制漫游功能、动态黑名单功能;

(三) 第二阶段任务书（400分）

任务1: Linux Kernel提权（50分）

任务环境说明:

攻击机:

物理机: Windows10

物理机安装工具1: Microsoft Visual Studio 2008

物理机安装工具2: OllyICE

物理机安装工具3: 木马连接工具

虚拟机1: Ubuntu_Linux

虚拟机1安装工具1: Python3/Python2

虚拟机1安装工具2: GCC

虚拟机1安装工具3: GDB

虚拟机1安装工具4: NetCat

虚拟机1用户名: root，虚拟机1密码: 123456

虚拟机操作系统2: CentOS_Linux

虚拟机2安装工具1: GCC

虚拟机2安装工具2: GDB

虚拟机2用户名: root，虚拟机2密码: 123456

虚拟机操作系统3: Windows7

虚拟机3用户名: administrator，虚拟机3密码: 123456

虚拟机操作系统4: WindowsXP

靶机:

服务器场景1: WindowsServer

服务器场景 1 的 FTP 下载服务用户名：anonymous

服务器场景 2：Windows（版本不详）

靶机环境中已经上传了 WebShell 访问 http://ip/shell.php/(登陆密码为 admin)

任务内容:

1. 登录服务器场景 2 的 WebShell，通过相关手段打印当前系统相关信息（内核版本号、硬件架构、主机名称和操作系统类型等，命令并非查看文件），将操作命令作为 FLAG 值提交;
2. 根据操作命令回显将内核版本信息作为 FLAG 值提交;
3. 通过相关手段对服务器场景 2 上传提权文件，将上传成功提示单词全部作为 FLAG 值提交;
4. 在攻击机虚拟机 1 通过 NC 进行监听模式，输出交互信息或报错信息，并且监听 8081 端口，将命令作为 FLAG 值提交;
5. 从攻击机虚拟机 1 对服务器场景 2 通过相关手段进行 NC 连接，将成功回显后结果的正数第三排第四个单词作为 FLAG 值提交;
6. 从攻击机虚拟机 1 对服务器场景 2 通过相关手段进行 NC 成功连接后，通过相关命令修改 root 密码，将回显最后一行后三个单词作为 FLAG 值提交;
7. 修改密码后，查看/root/flag.txt 文件，将回显最后一行最后两个单词作为 FLAG 值提交;
8. 对当前用户进行提权，提权成功后，再次查看/root/flag.txt，将回显内容后两个单词作为 FLAG 值提交;

任务 2：扫描渗透测试（50 分）

任务环境说明:

攻击机:

物理机: Windows10

物理机安装工具 1: Microsoft Visual Studio 2008

物理机安装工具 2: OllyICE

物理机安装工具 3: 木马连接工具

虚拟机 1: Ubuntu_Linux

虚拟机 1 安装工具 1: Python3/Python2

虚拟机 1 安装工具 2: GCC

虚拟机 1 安装工具 3: GDB

虚拟机 1 安装工具 4: NetCat

虚拟机 1 用户名：root，虚拟机 1 密码：123456

虚拟机操作系统 2: CentOS_Linux

虚拟机 2 安装工具 1: GCC

虚拟机 2 安装工具 2: GDB

虚拟机 2 用户名：root，虚拟机 2 密码：123456

虚拟机操作系统 3: Windows7

虚拟机 3 用户名：administrator，虚拟机 3 密码：123456

虚拟机操作系统 4: WindowsXP

靶机:

服务器场景 1: WindowsServer

服务器场景 1 的 FTP 下载服务用户名：anonymous

服务器场景 2: Windows（不详）

该环境存在上传、包含、截断漏洞（js 目录下的 calendar.php 网页中的 lang 参数存在包含漏洞）

http://ip/shop/ 注册任意用户

任务内容:

1. 针对服务器场景 2 上传一句话木马，使用文件包含将 URL 中有关文件包含的目录、网页、参数字符串作为参数，通过 MD5 函数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. 在服务器场景 2 的磁盘 C:\Windows 下找到 ABC_04.py 文件，将其上传到攻击机虚拟机 1 中，根据文件内注释要求的功能完善脚本，在完善脚本代码中，将 FLAG1 对应需要完善的内容字符串作为参数，通过 MD5 函数运算后，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 ABC_04.py 文件，在完善脚本代码中，将 FLAG2 对应需要完善的内容字符串作为参数，通过 MD5 函数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 ABC_04.py 文件，在完善脚本代码中，将 FLAG3 对应需要完善的内容字符串作为参数，通过 MD5 函数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 ABC_04.py 文件，在完善脚本代码中，将 FLAG4 对应需要完善的内容字符串作为参数，通过 MD5 函数运算后返回的

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. 继续编辑 ABC_04.py 文件，在完善脚本代码中，将 FLAG5 对应需要完善的内容字符串作为参数，通过 MD5 函数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）；
7. 继续编辑 ABC_04.py 文件，在完善脚本代码中，将 FLAG6 对应需要完善的内容字符串作为参数，通过 MD5 函数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）；
8. 继续编辑 ABC_04.py 文件，在完善脚本代码中，将 FLAG7 对应需要完善的内容字符串作为参数，通过 MD5 函数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）；
9. 继续编辑 ABC_04.py 文件，在完善脚本代码中，将 FLAG8 对应需要完善的内容字符串作为参数，通过 MD5 函数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）；
10. 在攻击机虚拟机 1 当中执行脚本 ABC_04.py，根据回显将扫描到的服务器场景 2 的端口输出信息字符串作为参数，通过 MD5 函数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: Linux/x86 系统漏洞挖掘与利用（50 分）

任务环境说明:

攻击机:

物理机: Windows10

物理机安装工具 1: Microsoft Visual Studio 2008

物理机安装工具 2: OllyICE

物理机安装工具 3: 木马连接工具

虚拟机 1: Ubuntu_Linux

虚拟机 1 安装工具 1: Python3/Python2

虚拟机 1 安装工具 2: GCC

虚拟机 1 安装工具 3: GDB

虚拟机 1 安装工具 4: NetCat

虚拟机 1 用户名: root，虚拟机 1 密码: 123456

虚拟机操作系统 2: CentOS_Linux

虚拟机 2 安装工具 1: GCC

虚拟机 2 安装工具 2: GDB

虚拟机 2 用户名: root，虚拟机 2 密码: 123456

虚拟机操作系统 3: Windows7

虚拟机 3 用户名: administrator，虚拟机 3 密码: 123456

虚拟机操作系统 4: WindowsXP

靶机:

服务器场景 1: WindowsServer

服务器场景 1 的 FTP 下载服务用户名: anonymous

服务器场景 2: LinuxServer

任务内容:

1. 在攻击机端通过渗透测试方法登陆靶机服务器场景;
2. 使服务器场景 2 从服务器场景 1 的 FTP 服务器中下载文件 Exploit_Linux04.c，编辑该 C 程序文件，对 Linux/x86 系统下 Exploit 源程序进行完善，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）;
3. 继续编辑该任务题目 1 中的 C 程序文件 Exploit_Linux04.c，对 Linux/x86 系统下 Exploit 源程序进行完善，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）;
4. 继续编辑该任务题目 1 中的 C 程序文件 Exploit_Linux04.c，对 Linux/x86 系统下 Exploit 源程序进行完善，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）;
5. 继续编辑该任务题目 1 中的 C 程序文件 Exploit_Linux04.c，对 Linux/x86 系统下 Exploit 源程序进行完善，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）;
6. 继续编辑该任务题目 1 中的 C 程序文件 Exploit_Linux04.c，对 Linux/x86 系统下 Exploit 源程序进行完善，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）；

7. 对以上题目中编辑的 Exploit_Linux04.c 源文件进行编译、链接，使程序运行，将程序运行后，服务器场景 2 增加的服务端口号以字符串的形式作为参数，通过 MD5 函数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：Windows/x86 系统漏洞挖掘与利用（50 分）

任务环境说明:

攻击机:

物理机：Windows10

物理机安装工具 1：Microsoft Visual Studio 2008

物理机安装工具 2：OllyICE

物理机安装工具 3：木马连接工具

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具 1：Python3/Python2

虚拟机 1 安装工具 2：GCC

虚拟机 1 安装工具 3：GDB

虚拟机 1 安装工具 4：NetCat

虚拟机 1 用户名：root，虚拟机 1 密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具 1：GCC

虚拟机 2 安装工具 2：GDB

虚拟机 2 用户名：root，虚拟机 2 密码：123456

虚拟机操作系统 3：Windows7

虚拟机 3 用户名：administrator，虚拟机 3 密码：123456

虚拟机操作系统 4：WindowsXP

靶机:

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 下载服务用户名：anonymous

服务器场景 2：Windows 7

任务内容:

1. 在攻击机端通过渗透测试方法登陆靶机服务器场景;
2. 使服务器场景 2 从服务器场景 1 的 FTP 服务器中下载文件 Exploit_Windows04.c，编辑该 C 程序文件，对 Windows/x86 系统下 Exploit 源程序进行完善，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）;
3. 继续编辑该任务题目 1 中的 C 程序文件 Exploit_Windows04.c，对 Windows/x86 系统下 Exploit 源程序进行完善，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）;
4. 继续编辑该任务题目 1 中的 C 程序文件 Exploit_Windows04.c，对 Windows/x86 系统下 Exploit 源程序进行完善，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）；

5. 继续编辑该任务题目 1 中的 C 程序文件 Exploit_Windows04.c，对 Windows/x86 系统下 Exploit 源程序进行完善，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）；
6. 继续编辑该任务题目 1 中的 C 程序文件 Exploit_Windows04.c，对 Windows/x86 系统下 Exploit 源程序进行完善，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）；
7. 对以上题目中编辑的 Exploit_Windows04.c 源文件进行编译、链接，使程序运行，将程序运行后，服务器场景 2 增加的服务端口号以字符串的形式作为参数，通过 MD5 函数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 5：逆向分析和缓冲区溢出渗透测试（50 分）

任务环境说明：

攻击机：

物理机：Windows10

物理机安装工具 1：Microsoft Visual Studio 2008

物理机安装工具 2：OllyICE

物理机安装工具 3：木马连接工具

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具 1：Python3/Python2

虚拟机 1 安装工具 2：GCC

虚拟机 1 安装工具 3：GDB

虚拟机 1 安装工具 4：NetCat

虚拟机 1 用户名：root，虚拟机 1 密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具 1：GCC

虚拟机 2 安装工具 2：GDB

虚拟机 2 用户名：root，虚拟机 2 密码：123456

虚拟机操作系统 3：Windows7

虚拟机 3 用户名：administrator，虚拟机 3 密码：123456

虚拟机操作系统 4：WindowsXP

靶机：

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 下载服务用户名：anonymous

服务器场景 2：LinuxServer

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 OverFlow04，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 OverFlow04，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 OverFlow04，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 OverFlow04，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 OverFlow04，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 OverFlow04，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 OverFlow04，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 OverFlow04，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 OverFlow04，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 OverFlow04，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）；

任务 6：云服务安全渗透测试（50 分）

攻击机:

物理机：Windows10

物理机安装工具 1：Microsoft Visual Studio 2008

物理机安装工具 2：OllyICE

物理机安装工具 3：木马连接工具

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具 1：Python3/Python2

虚拟机 1 安装工具 2：GCC

虚拟机 1 安装工具 3：GDB

虚拟机 1 安装工具 4：NetCat

虚拟机 1 用户名：root，虚拟机 1 密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具 1：GCC

虚拟机 2 安装工具 2：GDB

虚拟机 2 用户名：root，虚拟机 2 密码：123456

虚拟机操作系统 3：Windows7

虚拟机 3 用户名：administrator，虚拟机 3 密码：123456

虚拟机操作系统 4：WindowsXP

靶机:

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 下载服务用户名：anonymous

服务器场景 2：Windows 7

任务内容:

1. 从靶机服务器场景 1 的 FTP 服务器中下载文件 pwn04.py，编辑该 Python 程序文件，使该程序实现通过靶机服务器场景 2 中某具有 0day 漏洞的云服务来获得该云服务器的最高权限；完善 pwn04.py 程序文件，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 1 中的 Python 程序文件 pwn04.py，使该程序实现通过靶机服务器场景 2 中某具有 0day 漏洞的云服务来获得该云服务器的最高权限，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 1 中的 Python 程序文件 pwn04.py，使该程序实现通过靶机服务器场景 2 中某具有 0day 漏洞的云服务来获得该云服务器的最高权限，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 1 中的 Python 程序文件 pwn04.py，使该程序实现通过靶机服务器场景 2 中某具有 0day 漏洞的云服务来获得该云服务器的最高权限，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 1 中的 Python 程序文件 pwn04.py，使该程序实现通过靶机服务器场景 2 中某具有 0day 漏洞的云服务来获得该云服务器的最高权限，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 Python 程序解释器执行程序文件 pwn04.py，获得靶机服务器场景 2 中云服务器的最高权限，并打印云服务器根路径下的文件 FLAG 当中的字符串的内容，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）；

任务 7：二进制漏洞挖掘与利用（50 分）

任务环境说明：

攻击机：

物理机：Windows10

物理机安装工具 1：Microsoft Visual Studio 2008

物理机安装工具 2：OllyICE

物理机安装工具 3：木马连接工具

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具 1：Python3/Python2

虚拟机 1 安装工具 2：GCC

虚拟机 1 安装工具 3：GDB

虚拟机 1 安装工具 4：NetCat

虚拟机 1 用户名：root，虚拟机 1 密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具 1：GCC

虚拟机 2 安装工具 2：GDB

虚拟机 2 用户名：root，虚拟机 2 密码：123456

虚拟机操作系统 3：Windows7

虚拟机 3 用户名：administrator，虚拟机 3 密码：123456

虚拟机操作系统 4：WindowsXP

靶机：

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 下载服务用户名：anonymous

服务器场景 2：LinuxServer

任务内容：

1. 对靶机进行端口扫描探测，获取靶机开放的端口号，并将此端口号作为 FLAG1 的值进行提交（Flag 形式：flag{端口号}）
2. 通过 Netcat 对探测到的端口号进行监听并调试，在调试过程中获得 FLAG2 的值进行提交（Flag 形式：flag{xxxxxxxx}）

3. 通过浏览器直接访问 http://靶机 ip/pwn 即可下载到可执行文件 pwn，通过攻击机调试工具，对 pwn 文件进行调试分析，根据程序存在的漏洞编写攻击脚本，并利用此攻击脚本对服务器进行攻击，在服务器根目录下获取到 FLAG3 的值进行提交（Flag 形式：flag{xxxxxxxx}）

任务 8：操作系统安全渗透测试（50 分）

攻击机：

物理机：Windows10

物理机安装工具 1：Microsoft Visual Studio 2008

物理机安装工具 2：OllyICE

物理机安装工具 3：木马连接工具

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具 1：Python3/Python2

虚拟机 1 安装工具 2：GCC

虚拟机 1 安装工具 3：GDB

虚拟机 1 安装工具 4：NetCat

虚拟机 1 用户名：root，虚拟机 1 密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具 1：GCC

虚拟机 2 安装工具 2：GDB

虚拟机 2 用户名：root，虚拟机 2 密码：123456

虚拟机操作系统 3：Windows7

虚拟机 3 用户名：administrator，虚拟机 3 密码：123456

虚拟机操作系统 4：WindowsXP

靶机:

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 下载服务用户名：anonymous

服务器场景 2：操作系统类型及版本均未知

任务内容:

1. 从靶机服务器场景 1 的 FTP 服务器中下载文件 scan04.py，编辑该程序文件，使该程序实现从攻击机对靶机进行的 ARP 类型的主机在线探测渗透测试;
2. 从靶机服务器场景 1 的 FTP 服务器中下载文件 scan044.py，编辑该程序文件，使该程序实现从攻击机对靶机进行的操作系统类型探测渗透测试;
3. 从靶机服务器场景 1 的 FTP 服务器中下载文件 Exploit04.py 或 Exploit04.rb，编辑该程序文件，使该程序实现通过靶机服务器场景 2 的最高权限;完善 Exploit04.py 或 Exploit04.rb 程序文件，填写该文件当中空缺的 FLAG01 字符串，将该字符串作为 MD5 函数参数，经计算函数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 1 中的程序文件 Exploit04.py 或 Exploit04.rb，使该程序实现通过靶机服务器场景 2 的最高权限；完善 Exploit04.py 或 Exploit04.rb 程序文件，填写该文件当中空缺的 FLAG02 字符串，将该字符串作为 MD5 函数参数，经计算函数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 1 中的程序文件 Exploit04.py 或 Exploit04.rb，使该程序实现通过靶机服务器场景 2 的最高权限；完善 Exploit04.py 或 Exploit04.rb 程序文件，填写该文件当中空缺的 FLAG03 字符串，将该字符串作为 MD5 函数参数，经计算函数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. 继续编辑该任务题目 1 中的程序文件 Exploit04.py 或 Exploit04.rb，使该程序实现通过靶机服务器场景 2 的最高权限；完善 Exploit04.py 或 Exploit04.rb 程序文件，填写该文件当中空缺的 FLAG04 字符串，将该字符串作为 MD5 函数参数，经计算函数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）；
7. 继续编辑该任务题目 1 中的程序文件 Exploit04.py 或 Exploit04.rb，使该程序实现通过靶机服务器场景 2 的最高权限；完善 Exploit04.py 或 Exploit04.rb 程序文件，填写该文件当中空缺的 FLAG05 字符串，将该字符串作为 MD5 函数参数，经计算函数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）；
8. 继续编辑该任务题目 1 中的程序文件 Exploit04.py 或 Exploit04.rb，使该程序实现通过靶机服务器场景 2 的最高权限；完善 Exploit04.py 或 Exploit04.rb 程序文件，填写该文件当中空缺的 FLAG06 字符串，将该字符串作为 MD5 函数参数，经计算函数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）；

9. 通过 Python 或 Ruby 程序解释器执行程序文件 Exploit04.py 或 Exploit04.rb，获得靶机服务器场景 2 的最高权限，并打印靶机服务器场景 2 磁盘根路径下的文件 FLAG 当中的字符串的内容，将该字符串作为 MD5 函数参数，经计算函数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）；

（四） 第三阶段任务书（300 分）

假定各位选手是某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 92、4308、6557，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。靶机的 Flag 值存放在./root/flaginfoxxxx.xxx.txt 文件内容当中。基础分 100 分,每提交 1 次对手靶机的 Flag 值增加 2 分，每当被对手提交 1 次自身靶机的 Flag 值扣除 2 分,每个对手靶机的 Flag 值只能被自己提交一次,得分低于 0 分计为 0 分，得分高于 300 分计为 300 分。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。

注意 5：不得人为恶意破坏自己服务器的 Flag 值，否则将判令停止比赛，第三阶段分数为 0 分；

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。