2021 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 1

- **赛项时间**

共计 X 小时。

- **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		
	任务 2	网络安全设备配置与防护		
第二阶段 系统安全攻防及运维安全管控	任务 1	PWN：Linux 系统渗透测试		
	任务 2	Web 安全测试：代码审计		
	任务 3	逆向工程：Windows PE		
	任务 4	PWN：Windows 系统渗透测试		
	任务 5	逆向工程：Linux ELF		
	任务 6	大数据与机器学习应用：Web 安全测试		
第三阶段 分组对抗	系统加固			
	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。

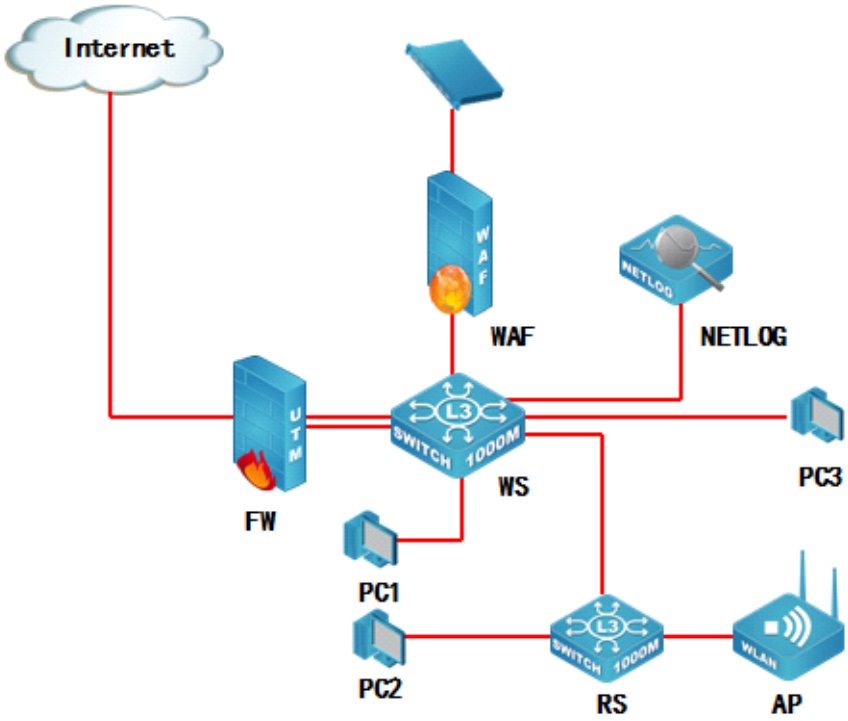
选手首先需要在 U 盘的根目录下建立一个名为“GWxx”的文件夹（xx 用具体的工位号替代），赛题第一阶段所完成的“XXX-答题模板”放置在文件夹中。

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。

- 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 FW	ETH0/1	9.0.0.1/30 （Trust 安全域）	WS
	ETH0/2	10.0.0.1/30 （untrust 安全域）	
	ETH0/3	11.0.0.1/30 （Trust 安全域）	WS
	ETH0/4	12.0.0.1/30 （Trust 安全域）	WS
	ETH0/5	218.5.18.1/27 （untrust 安全域）	INTERNET
	SSL Pool	192.168.10.1/24 可用 IP 数量为 20	SSL VPN 地址池

三层无线交换机 WS	ETH1/0/1-2	10.0.0.2/30	FW
	VLAN 51 ETH1/0/3	10.0.0.10/30	NETLOG
	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 ETH1/0/3	172.16.30.1/26	PC1
	VLAN 50 ETH1/0/5	172.16.50.1/26	PC3
	ETH1/0/20 VLAN 100	192.168.100.1/24	RS
三层交换机 RS	ETH1/0/1 VLAN 100	192.168.100.254/24	WS
	无线管理 VLAN VLAN 101 ETH1/0/2	192.168.101.1/24	AP
	VLAN 40 ETH1/0/4	172.16.40.1/26	PC2
日志服务器 NETLOG	ETH2	10.0.0.9/30	WS
WEB 应用防火墙 WAF	ETH2	172.16.100.2/24	
	ETH3		WS
堡垒服务器	-	-	WAF

- 设备初始化信息

设备名称	管理地址	默认管理接	用户名	密码

		口		
防火墙 FW	http://192.168.1.1	ETH0	admin	admin
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
三层交换机 RS	-	Console	-	-
无线交换机 WS	-	Console	-	-
堡垒服务器	-	-	-	
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。			

- **第一阶段任务书**

任务 1：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 FW 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 RS 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 RS 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 WS 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 NETLOG 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

- RS 和 WS 开启 telnet 登录功能，配置使用 telnet 方式登录终端界面前显示如下授权信息：“WARNING!!! Authorised access only, all of your done will be recorded! Disconnected IMMEDIATELY if you are not an authorised user! Otherwise, we retain the right to pursue the legal responsibility”。
- 总部部署了一套网管系统实现对核心 RS 进行管理，网管系统 IP 为：172.16.100.21，读团体值为：ABC2021，版本为 V2C， RS 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；
- RS 出口往返流量发送给 NETLOG，由 NETLOG 对收到的数据进行用户所要求的分析;
- 对 RS 上 VLAN40 开启以下安全机制：

  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； 如私设 DHCP 服务器关闭该端口;防止 ARP 欺骗攻击；

- 配置使总部 VLAN10，30，40 业务的用户访问 INTERNET 往返数据流都经过 FW 进行最严格的安全防护; RS 使用相关 VPN 技术，模拟 INTERNET ,VPN 名称为 INTERNET 地址为 218.5.18.2；
- WS 与 RS 之间配置 RIPng， 是 VLAN30 与 VLAN50 可以通过 IPv6 通信；

  IPv6 业务地址规划如下，其它 IPv6 地址自行规划：

业务	IPV6 地址
VLAN30	2001:30::254/64
VLAN50	2001:50::254/64

- FW、RS、WS 之间配置 OSPF area 0 开启基于链路的 MD5 认证，密钥自定义；
- 为了有效减低能耗，要求每天晚上 20:00 到早上 07:00 把 RS 端口指示灯全部关闭；如果 RS 的 11 端口的收包速率超过 30000 则关闭此端口，恢复时间 5 分钟，并每隔 10 分钟对端口的速率进行统计；为了更好地提高数据转发的性能，RS 交换中的数据包大小指定为 1600 字节；
- 为实现对防火墙的安全管理，在防火墙 FW 的 Trust 安全域开启 PING,HTTP，SNMP 功能，Untrust 安全域开启 SSH、HTTPS 功能;
- 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；

- 远程移动办公用户通过专线方式接入总部网络，在防火墙 FW 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 ABC2021，地址池参见地址表；
- 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;为净化上网环境，要求在防火墙 FW 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；
- 在公司总部的 NETLOG 上配置，设备部署方式为旁路模式，并配置监控接口与管理接口。增加非 admin 账户 ABC2021，密码 ABC2021，该账户仅用于用户查询设备的日志信息和统计信息。使 NETLOG 能够通过邮件方式发送告警信息，邮件服务器在服务器区，IP 地址是 172.16.10.200，端口号 25，账号 test，密码 test;NETLOG 上配置 SNMPv3，用户名 admin，MD5 秘钥 adminABC，配置日志服务器与 NTP 服务器，两台服务器地址：172.16.10.200；
- 在公司总部的 NETLOG 上配置，监控工作日（每周一到周五）期间 PC1 网段访问的 URL 中包含 xunlei 的 HTTP 访问记录，并且邮

件发送告警。监控 PC2 网段所在网段用户的即时聊天记录。监控内网所有用户的邮件收发访问记录。

- NETLOG 配置应用及应用组“P2P 视频下载”，UDP 协议端口号范围 65521-65621，在周一至周五 8：00-20：00 监控内网中所有用户的“P2P 视频下载”访问记录；
- NETLOG 配置对内网 ARP 数量进行统计，要求 30 分钟为一个周期；NETLOG 配置开启用户识别功能,对内网所有 MAC 地址进行身份识别；
- NETLOG 配置统计出用户请求站点最多前 20 排名信息，发送到邮箱为 bn2021@chinaskills.com；

- 公司内部有一台网站服务器直连到 WAF，地址是 RS 上 VLAN10 网段内的第五个可用地址，端口是 8080，配置将服务访问日志、WEB 防护日志、服务监控日志信息发送 syslog 日志服务器， IP 地址是服务器区内第六个可用地址，UDP 的 514 端口;

172.16.10.1/24

- 在公司总部的 WAF 上配置，阻止常见的 WEB 攻击数据包访问到公司内网服务器，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;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;
- 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；WAF 上配置阻止用户上传 ZIP、DOC、JPG、RAR 格式文件;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;
- WAF 上配置，使用 WAF 的漏洞立即扫描功能检测服务器（172.16.10.100）的安全漏洞情况，要求包括信息泄露、SQL 注入、跨站脚本编制;
- 在公司总部的 WAF 上配置， WAF 设备的内存使用率超过 50%每隔 5 分钟发送邮件和短信给管理，邮箱 bn2021 HYPERLINK "mailto:admin@digitalchina.com"@digitalchina.com，手机 13912345678；在公司总部的 WAF 上配置，将设备状态告警、服务状态告警信息通过邮件（发送到 bn2021@digitalchina.com）及短信方式(发送到 13812345678)发送给管理员;
- WS 上配置 DHCP，管理 VLAN 为 VLAN101,为 AP 下发管理地址，保

证完成 AP 注册； 为无线用户 VLAN10,20, 有线用户 VLAN 30,40 下发 IP 地址；

- 在 NETWORK 下配置 SSID，需求如下：

  1、NETWORK 1 下设置 SSID ABC2021，VLAN10，加密模式为 wpa-personal,其口令为 ABCE2021；

  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；

- NETWORK 1 开启内置 portal+本地认证的认证方式，账号为 ABC 密码为 ABCE2021；
- 配置 SSID GUEST 每天早上 0 点到 6 点禁止终端接入; GUSET 最多接入 10 个用户，并对 GUEST 网络进行流控，上行 1M，下行 2M；配置所有无线接入用户相互隔离；
- 配置当 AP 上线，如果 AC 中储存的 Image 版本和 AP 的 Image 版本号不同时，会触发 AP 自动升级；配置 AP 发送向无线终端表明 AP 存在的帧时间间隔为 1 秒；配置 AP 失败状态超时时间及探测到的客户端状态超时时间都为 2 小时；配置 AP 在脱离 AC 管理时依然可以正常工作；
- 为防止外部人员蹭网，现需在设置信号值低于 50%的终端禁止连接无线信号；为防止非法 AP 假冒合法 SSID，开启 AP 威胁检测

功能；

- RS、WS 运行静态组播路由和因特网组管理协议第二版本；PC1 启用组播，使用 VLC 工具串流播放视频文件 1.mpg，组地址 228.10.10.10，端口：1234，实现 PC2 可以通过组播查看视频播放。

第二阶段任务书

任务 1：PWN：Linux 系统渗透测试

任务环境说明：

攻击机：

物理机：Windows

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具：Python/Python3/GDB

虚拟机 1 用户名：root，密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具：GDB

虚拟机 2 用户名：root，密码：123456

虚拟机操作系统 3：Windows

虚拟机 3 安装工具：OllyICE

虚拟机 3 用户名：administrator，密码：123456

靶机：

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 服务账号：匿名

服务器场景 2：LinuxServer

任务内容：

- 从靶机服务器场景 1 的 FTP 服务中下载文件 Exploit_Linux01.c，编辑该 C 程序源文件，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）；
- 继续编辑该任务题目 1 中的 C 程序文件 Exploit_Linux01.c，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）；
- 继续编辑该任务题目 1 中的 C 程序文件 Exploit_Linux01.c，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）；

- 继续编辑该任务题目 1 中的 C 程序文件 Exploit_Linux01.c，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）；
- 继续编辑该任务题目 1 中的 C 程序文件 Exploit_Linux01.c，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）；
- 对题目 1-5 中编辑的 Exploit_Linux01.c 源文件进行编译、链接，使程序运行，获得服务器场景 2 的 root 权限，并将服务器场景 2 磁盘中根路径下的文件 FLAG 中的完整字符串通过 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 2：Web 安全测试：代码审计

任务环境说明：

攻击机：

物理机：Windows

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具：Python/Python3/GDB

虚拟机 1 用户名：root，密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具：GDB

虚拟机 2 用户名：root，密码：123456

虚拟机操作系统 3：Windows

虚拟机 3 安装工具：OllyICE

虚拟机 3 用户名：administrator，密码：123456

靶机：

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 服务账号：匿名

服务器场景 2：WebSecServer

服务器场景 2 的 FTP 服务账号：匿名

任务内容：

- 以浏览器方式打开网站主页，继续点击超链接进入页面，以 Web 安全测试方法获得服务器场景 2 根路径下的文件

flaginfo 中的完整字符串，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）；

- 从靶机服务器场景 FTP 服务器中下载文件 websec01.php，编辑该 PHP 程序文件，使该程序实现能够对本任务第 1 题中的 Web 应用程序渗透测试过程进行安全防护，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）；
- 继续编辑本任务第 2 题中的 PHP 程序文件，使该程序实现能够对本任务第 1 题中的 Web 应用程序渗透测试过程进行安全防护，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）；
- 继续编辑本任务第 2 题中的 PHP 程序文件，使该程序实现能够对本任务第 1 题中的 Web 应用程序渗透测试过程进行安全防护，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）；

- 继续编辑本任务第 2 题中的 PHP 程序文件，使该程序实现能够对本任务第 1 题中的 Web 应用程序渗透测试过程进行安全防护，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）；
- 继续编辑本任务第 2 题中的 PHP 程序文件，使该程序实现能够对本任务第 1 题中的 Web 应用程序渗透测试过程进行安全防护，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）；
- 将编辑好后的 PHP 程序文件上传至服务器场景 2 的 FTP 服务目录，并在攻击机端通过本任务第 1 题中使用的 Web 安全测试方法对服务器场景 2 进行渗透测试，将此时 Web 页面弹出的字符串通过 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：逆向工程：Windows PE

任务环境说明：

攻击机：

物理机：Windows

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具：Python/Python3/GDB

虚拟机 1 用户名：root，密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具：GDB

虚拟机 2 用户名：root，密码：123456

虚拟机操作系统 3：Windows

虚拟机 3 安装工具：OllyICE

虚拟机 3 用户名：administrator，密码：123456

靶机：

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 服务访问方式：匿名

服务器场景 2：Windows1

任务内容：

- 从靶机服务器场景 1 的 FTP 服务器中下载可执行文件 windows_pe_01 以及渗透测试脚本 windows_pe_01，通过攻击机调试工具，对以上可执行文件 windows_pe_01 进行逆向分析，并利用逆向分析的结果，完善渗透测试脚本

windows_pe_01，补充该脚本当中空缺的 FLAG01 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）；

- 继续完善本任务第 1 题中的渗透测试脚本，补充该脚本当中空缺的 FLAG02 字符串，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）；
- 继续完善本任务第 1 题中的渗透测试脚本，补充该脚本当中空缺的 FLAG03 字符串，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）；
- 继续完善本任务第 1 题中的渗透测试脚本，补充该脚本当中空缺的 FLAG04 字符串，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）；
- 继续完善本任务第 1 题中的渗透测试脚本，补充该脚本当中空缺的 FLAG05 字符串，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）；

- 通过 Python 或 Ruby 解释器执行程序文件 windows_pe_01，获得靶机服务器场景 2 的最高权限，并打印根路径下的文件 FLAG 当中完整的字符串的内容，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 4：PWN：Windows 系统渗透测试

任务环境说明：

攻击机：

物理机：Windows

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具：Python/Python3/GDB

虚拟机 1 用户名：root，密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具：GDB

虚拟机 2 用户名：root，密码：123456

虚拟机操作系统 3：Windows

虚拟机 3 安装工具：OllyICE

虚拟机 3 用户名：administrator，密码：123456

靶机：

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 服务访问方式：匿名

服务器场景 2：Windows2

任务内容：

- 从靶机服务器场景 1 的 FTP 服务器中下载渗透测试脚本 windows_exploit_01，补充该脚本当中空缺的 FLAG01 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）；
- 继续完善本任务第 1 题中的渗透测试脚本，补充该脚本当中空缺的 FLAG02 字符串，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）
- 继续完善本任务第 1 题中的渗透测试脚本，补充该脚本当中空缺的 FLAG03 字符串，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）；
- 继续完善本任务第 1 题中的渗透测试脚本，补充该脚本当中空缺的 FLAG04 字符串，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）；

- 继续完善本任务第 1 题中的渗透测试脚本，补充该脚本当中空缺的 FLAG05 字符串，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）；
- 通过 Python 或 Ruby 解释器执行程序文件 windows_exploit_01，获得靶机服务器场景 2 的最高权限，并打印根路径下的文件 FLAG 当中完整的字符串的内容，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 5：逆向工程：Linux ELF

任务环境说明：

攻击机：

物理机：Windows

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具：Python/Python3/GDB

虚拟机 1 用户名：root，密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具：GDB

虚拟机 2 用户名：root，密码：123456

虚拟机操作系统 3：Windows

虚拟机 3 安装工具：OllyICE

虚拟机 3 用户名：administrator，密码：123456

靶机：

服务器场景 1：WindowsServer

服务器场景 1 的 FTP 服务账号：匿名

服务器场景 2：LinuxServer

任务内容：

- 从靶机服务器场景 1 的 FTP 服务器中下载可执行文件 linux_elf_01 以及 C 程序源文件 linux_elf_01.c，通过攻击机调试工具，对以上可执行文件 linux_elf_01 进行逆向分析，并利用逆向分析的结果，完善 C 程序源文件 linux_elf_01.c，补充该 C 程序源文件当中空缺的 FLAG01 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）；
- 继续完善本任务第 1 题中的 C 程序源文件，补充该 C 程序源文件当中空缺的 FLAG02 字符串，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）；

- 继续完善本任务第 1 题中的 C 程序源文件，补充该 C 程序源文件当中空缺的 FLAG03 字符串，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）；
- 继续完善本任务第 1 题中的 C 程序源文件，补充该 C 程序源文件当中空缺的 FLAG04 字符串，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）；
- 继续完善本任务第 1 题中的 C 程序源文件，补充该 C 程序源文件当中空缺的 FLAG05 字符串，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）；
- 对题目 1-5 中编辑的 linux_elf_01.c 源文件进行编译、链接，使程序运行，获得服务器场景 2 的 root 权限，并将服务器场景 2 磁盘中根路径下的文件 FLAG 中的完整字符串通过 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：大数据与机器学习应用：Web 安全测试

任务环境说明：

攻击机：

物理机：Windows

虚拟机 1：Ubuntu_Linux

虚拟机 1 安装工具：Python/Python3/GDB

虚拟机 1 用户名：root，密码：123456

虚拟机操作系统 2：CentOS_Linux

虚拟机 2 安装工具：GDB

虚拟机 2 用户名：root，密码：123456

虚拟机操作系统 3：Windows

虚拟机 3 安装工具：OllyICE

虚拟机 3 用户名：administrator，密码：123456

靶机：

服务器场景：WindowsServer

服务器场景的 FTP 服务账号：匿名

任务内容：

- 从靶机服务器场景的 FTP 服务器中下载数据集 DS01、DS02，以及 WebSec01.py 脚本，并对该脚本进行完善，实现如下任

务（ABC）：A、对数据集进行特征向量表示得到特征矩阵；B、利用特征矩阵训练 Web 安全异常检测模型；C、使用 Web 安全异常检测模型判断列表中的 URL 请求是否存在异常。补充该脚本当中空缺的 FLAG01 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）；

- 继续完善本任务第 1 题中的 WebSec01.py 脚本，补充该脚本当中空缺的 FLAG02 字符串，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）
- 继续完善本任务第 1 题中的 WebSec01.py 脚本，补充该脚本当中空缺的 FLAG03 字符串，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）
- 继续完善本任务第 1 题中的 WebSec01.py 脚本，补充该脚本当中空缺的 FLAG04 字符串，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）
- 继续完善本任务第 1 题中的 WebSec01.py 脚本，补充该脚本

当中空缺的 FLAG05 字符串，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）

- 继续完善本任务第 1 题中的 WebSec01.py 脚本，补充该脚本当中空缺的 FLAG06 字符串，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）
- 继续完善本任务第 1 题中的 WebSec01.py 脚本，补充该脚本当中空缺的 FLAG07 字符串，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）
- 继续完善本任务第 1 题中的 WebSec01.py 脚本，补充该脚本当中空缺的 FLAG08 字符串，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）
- 继续完善本任务第 1 题中的 WebSec01.py 脚本，补充该脚本当中空缺的 FLAG09 字符串，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）

- 继续完善本任务第 1 题中的 WebSec01.py 脚本，补充该脚本当中空缺的 FLAG10 字符串，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）
- 通过 Python 解释器执行程序文件 WebSec01.py，使用 Web 安全异常检测模型判断列表中的 URL 请求是否存在异常，并将检测结果返回的字符串通过 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）；

第三阶段任务书

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 80、5555，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。每提交 1 次对手靶机的 Flag 值增加 1 分，每当被对手提交 1 次自身靶机的 Flag 值扣除 1 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。

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

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。