2023年度湖南省“楚怡杯”职业院校技能竞赛

赛项规程

一、赛项名称

1. 赛项名称：信息安全管理与评估
2. 赛项组别：高职高专组
3. 赛项归属：电子信息大类

二、竞赛内容

重点考核参赛选手网络组建和安全运维、安全审计、网络安全应急响应、数字取证调查、应用程序安全和网络攻防渗透等综合实践能力，具体包括：

（一）参赛选手能够根据大赛提供的赛项要求，设计信息安全防护方案，并且能够提供详细的信息安全防护设备拓扑图。

（二）参赛选手能够根据业务需求和实际的工程应用环境，实现网络设备、安全设备、服务器的连接，通过调试，实现设备互联互通。

（三）参赛选手能够在赛项提供的网络设备及服务器上配置各种协议和服务，实现网络系统的运行，并根据网络业务需求配置各种安全策略，组建网络以满足应用需求。

（四）参赛选手能够根据企业所发现的安全事件，展开网络安全事件的调查、分析和取证工作，收集、保存、处理、分析和提供与计算机相关的证据，审计黑客的入侵行为，恢复被黑客破坏的文件。

（五）参赛选手可以利用一系列网络安全攻击渗透工具对所提供的网络安全攻击靶场环境进行综合分析、挖掘和渗透。

竞赛分值权重和时间分布如下表所示：

序号	内容模块	竞赛时间
第一阶段 权重 40%	网络平台搭建（权重 5%）	240 分钟
	网络安全设备配置与防护（权重 35%）	
第二阶段 权重 20%	网络安全事件响应、数字取证调查、应用程序安全（权重 20%）	
第三阶段 权重 40%	网络安全渗透（权重 40%）	

三、竞赛方式

本赛项为3人团体赛。

四、竞赛时量

竞赛时量为 240 分钟包括网络平台搭建、网络安全设备配置与防护、网络安全事件响应、数字取证调查、应用程序和网络安全渗透。

五、名次确定办法

选手竞赛成绩按照评分标准计分，根据参赛队成绩从高到低排序确定名次。不设并列名次，总成绩相同时以时间较短者名次列前。总成绩和完成时间都相同时，以网络安全渗透成绩高者名次列前。

六、评分标准与评分细则

1.评分标准及权重

竞赛阶段	竞赛任务	考核内容	分值	评分方式
第一阶段 权重 40%	网络平台搭建 权重 5%	网络规划文档 按照要求进行网络设备配置,提交相关配置文件或截图文件	5	结果评分-客观
	网络安全设备配置与防护 权重 35%	防火墙相关配置	35	结果评分-客观
		网络日志系统相关配置		结果评分-客观
		web 应用防火墙相关配置		结果评分-客观
		无线控制器相关配置		结果评分-客观
		三层交换机相关配置		结果评分-客观
第二阶段 权重 20%	网络安全事件响应、数字取证调查、应用程序安全 权重 20%	操作系统日志 应用系统/中间件日志系统进程分析 系统安全漏洞及加固	20	结果评分-客观
		内存镜像分析 编码转换、加解密、数据隐写文件分析取证 网络流量包分析		结果评分-客观
		程序逆向分析 移动应用程序代码分析恶意脚本代码分析		结果评分-客观
第三阶段 权重 40%	网络安全渗透 40%	SQL 注入文件上传 命令执行 缓冲区溢出信息收集 逆向文件分析 二进制漏洞利用 应用服务漏洞利用 操作系统漏洞利用密码学分析	40	结果评分-客观

2．评分细则

（1）根据竞赛任务和评分标准确定评分细则，设计评分表。

（2）所有参赛队成绩由裁判组统一评定。

（3）比赛采取分步得分、错误不传递、累计总分的计分方式。分别计算环节得分，按规定比例计入选手总分。

（4）竞赛过程中，参赛选手如有不服从裁判判决、扰乱赛场秩序、舞弊等不文明行为，由裁判组按照规定扣减相应分数，情节严重的取消竞赛资格。

具体情况与处理方式如下：

①违反比赛规定，提前进行操作或比赛终止后仍继续操作的，由现场裁判负责记录并酌情扣1-5分。

②在竞赛过程中，违反操作规程，影响其他选手比赛的，未造成设备损坏的参赛队，扣5-10分。

③在竞赛过程中，造成设备损坏或影响他人比赛、情节严重的报竞赛执委会批准，终止该参赛队的比赛，竞赛成绩以 0 分计算。

七、赛点提供的设施设备仪器清单

1. 竞赛软件

个人计算机安装Windows操作系统，用以组建竞赛操作环境，并安装Office等常用应用软件。

序号	软件	介绍
1	Windows	操作系统
2	Microsoft Office	文档编辑工具
3	VMware	虚拟机运行环境
4	Secure CRT	设备调试连接工具

渗透测试机和靶机虚拟机环境。

序号	软件	介绍
1	Windows 10	Windows 客户机操作系统
2	Windows Server 2003\2008\2012\2016	Windows 服务器操作系统
3	kali	渗透测试机操作系统
4	Linux CentOS	Linux 服务器操作系统

2. 竞赛设备清单

序号	设备名称	设备型号	数量	技术参数
1	三层虚拟化交换机	神州数码 CS6200-28X-Pro	1	路由交换机(24 个千兆以太网电口+4 个复用千兆 SFP 光口+4 个 10G SFP+光口），主机内置双 AC 电源。
2	防火墙	神州数码 DCFW-1800E-N3002-Pro	1	中小型企业级安全网关 物理参数：9 个 10/100/1000M 以太网电口；1U 标准机箱。
3	堡垒服务器	神州数码 DCST-6000B-Pro	1	1U 虚拟化平台,固化业务背板,固化千兆网络接口≥2 个，Console 口 1 个；平台满足大于 300 个实训场景，包含不限于密码学与应用、信息系统安全、操作系统安全，网

				络安全、数字内容安全、软件安全、漏洞渗透，信息安全工程实践、协议分析、数据库安全等；单台设备虚拟机并发数量≥10 个，单台虚拟机的启动速度小于 20 秒；支持基于 WEB 的用户注册功能，支持用户自己修改用户信息；支持虚拟化管理，支持集群管理，支持实时当前云平台自动调用的虚拟化资源情况；设备提供 SSH、串口管理方式，支持恢复出厂设置；提供用户课件的上传，提供用户上传课件内容后在线浏览功能，支持 HTML、PPT、WORD、PDF、SWF、scom 等格式。
4	WEB 应用防火墙	神州数码 DCFW-1800-WAF-P	1	6 个千兆电口，1 个扩展插槽，1 个 Console ，存储 1T 硬盘，机箱 1U。支持 web 安全扫描，web 安全防护，安全情报分析，DDOS 防护，网页防篡改，包过滤等功能，有效保障 web 应用服务资源安全。
5	网络日志系统	神州数码 DCBC-NetLog	1	6 个千兆电口，1 个扩展插槽，1 个 Console ，存储 1T 硬盘，机箱 1U。内置常用的攻击工具库，重点针对网络层；能够详细识别、记录所有的用户数据，有详细的日志信息。
6	无线交换机	神州数码 DCWS-6028-Pro	1	无线控制器，4 个万兆 SFP 光口，24 个千兆电口，支持 CLI 配置，串口波特率 9600，支持双交流供电接口，不支持 PoE 供电，连接 AP 时需要单独选购供电模块；默认含 8 台 AP 管理许可，最多可支持 72 台 AP。
7	无线接入点	神州数码 WL8200-I2	1	802.11ac wave2 室内放装型无线 AP，内置天线，整机 5 条空间流，整机最大速率 1.317Gbps，支持 802.11a/n/ac wave2 和 802.11b/g/n 同时工作，支持 1 个千兆电口，1 个 USB 接口；支持本地 12V 直流供电和 802.3af/at PoE 供电。
8	PC 机	国产品牌	3	多核 CPU，CPU 主频>=3.5GHZ，>=四核心八线程，内存>=8G，具有串口或者配置 USB 转串口的配置线，支持硬件虚拟化。

八、选手须知

1. 选手自带工具清单

本赛项所有工具由举办方提供，选手无需自带工具。

2. 主要技术规程及要求

该赛项涉及的信息网络安全工程在设计、组建过程中，主要有以下15项国家标准，参赛队在实施竞赛项目中要求遵循如下规范：

序号	标准号	中文标准名称
1	GB 17859-1999	《计算机信息系统安全保护等级划分准则》
2	GB/T 20271-2006	《信息安全技术信息系统通用安全技术要求》
3	GB/T 20270-2006	《信息安全技术网络基础安全技术要求》
4	GB/T 20272-2006	《信息安全技术操作系统安全技术要求》
5	GB/T 20273-2006	《信息安全技术数据库管理系统安全技术要求》

6	GA/T 671-2006	《信息安全技术终端计算机系统安全等级技术要求》
7	GB/T 20269-2006	《信息安全技术信息系统安全管理要求》
8	ISO OSI	OSI 开放系统互连参考模型
9	IEEE 802.1	局域网概述，体系结构，网络管理和性能测量
10	IEEE 802.2	逻辑链路控制 LLC
11	IEEE 802.3	总线网介质访问控制协议 CSMA/CD 及物理层技术规范
12	IEEE 802.6	城域网（Metropolitan Area Networks)MAC 介质访问控制协议 DQDB 及其物理层技术规范
13	IEEE 802.10	局域网安全技术标准
14	IEEE 802.11	无线局域网的介质访问控制协议 CSMA/CA 及其物理层技术规范
15	BG/T 22239-2008	信息安全技术信息系统安全等级保护基本要求

3.选手注意事项

（1）各参赛队应在竞赛开始前一天规定的时间段进入赛场熟悉环境。

（2）每个参赛队指定一名选手在选手会议上抽取场次签。

（3）参赛选手按场次提前 30 分钟达到赛场检录地点。

（4）参赛选手不得穿戴有学校标志的工作服或校服进入赛场，也不得以任何方式透露参赛学校和个人信息，如有违反则取消参赛资格。

（5）参赛选手不允许携带任何书籍和其他纸质资料（相关技术资料的电子文档由组委会提供），不允许携带通讯工具和存储设备（如 U 盘）。竞赛委员会统一提供计算机以及应用软件。

（6）比赛期间，不允许指导教师现场指导。

（7）参赛选手入场后，应与赛场工作人员共同确认操作条件及设备状况，确认材料、工具等。竞赛期间参赛选手原则上不得离开比赛场地。凡在竞赛期间提前离开的选手，当天不得返回赛场。

（8）竞赛时，各参赛队自行决定分工、工作程序和时间安排。选手在接到开赛信号后才能启动操作设备。在指定工位上完成竞赛项目，严禁作弊行为。

（9）竞赛期间，选手饮水等由赛场统一提供，不得自带。选手休息、饮食或如厕时间均计算在比赛时间内。

（10）参赛选手应严格遵守赛场规章、操作规程和工艺准则，保证人身及设备安全，接受裁判员的监督和警示，文明竞赛。

（11）竞赛过程中，因操作失误或安全事故不能进行比赛的（例如因线缆连接发生短路导致赛场断电、造成设备不能正常工作），现场裁判员有权中止该队比赛。由于选手错误操作造成的设备损坏故障，需要承担赔偿。

（12）在竞赛中如遇非人为因素造成的设备故障，经裁判员确认后，可向裁判长申请补足排除故障的时间。

（13）参赛队如欲提前结束比赛，应向现场裁判员举手示意，由裁判员记录竞赛终止时间。竞赛终止后，不得再进行任何与竞赛有关的操作。

（14）竞赛时间到，参赛队选手应立即结束操作，按照大赛要求和赛题要求提交竞赛成果，禁止在竞赛成果上做任何与竞赛无关的记号。

（15）竞赛操作结束后，参赛队要确认成功提交竞赛要求的文件，裁判员在比赛结果的规定位置做标记，并与参赛队一起签字确认。

（16）在竞赛过程中，选手如有不服从裁判判决、扰乱赛场秩序、舞弊等不文明行为，由裁判按照规定扣减相应分数并且给予警告，情节严重的取消竞赛资格，竞赛成绩记 0 分，选手退出比赛现场。

（17）在竞赛期间，未经组委会批准，参赛选手不得接受其他单位和个人进行的与竞赛内容相关的采访。参赛选手不得将竞赛的相关信息私自公布。

（18）所有选手在赛后必须参加闭幕式，如有特殊情况确实无法参加，应向领队说明情况，由领队向赛点学校提出书面申请，并报竞赛组委会办公室备案。

4. 竞赛直播

（1）赛场内部设置无盲点监控设备，能实时录制并播放赛场情况。

（2）在赛点指定的区域，通过监控系统观摩竞赛。

九、样题（竞赛任务书）

样题见附件

2023 年度湖南省“楚怡杯”职业院校技能竞赛

高职电子信息类信息安全管理与评估赛项

［时量：240 分钟，试卷号：1 ］

（样卷）

竞赛任务书

场次号：

机位号（工位号）：

2022 年 12 月

注意事项

一、竞赛任务概述

本赛项包括平台搭建与配置、系统安全攻防及运维安全管控和分组对抗等 3 个竞赛阶段，各阶段分值分别为 40、20、40 分，本赛项满分为 100 分。

二、注意事项

1.竞赛任务书共 31 页。

2．选手进入赛场后，请参赛选手按照赛场提供的“2023 年度湖南省职业院校技能竞赛高职电子信息类信息安全管理与评估项目竞赛软件与硬件设备确认单”，认真检查、核对本场竞赛所需的软、硬件环境，并在确认单上签字确认。

3．参赛选手不允许携带任何书籍、纸质资料、通讯工具、智能终端和存储设备进入赛场，如有发现做舞弊处理，竞赛成绩记 0 分。

4．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。

5．参赛选手应严格遵守赛场规章、操作规程和工艺准则，保证人身及设备安全，接受裁判员的监督和警示，文明竞赛。

6．竞赛过程中，因操作失误或安全事故不能进行比赛的（例如因线缆连接发生短路导致赛场断电、造成设备不能正常工作），现场裁判员有权中止该队比赛。由于选手错误操作造成的设备损坏故障，需要承担赔偿。

7．在竞赛中如遇非人为因素造成的设备故障，经裁判员确认后，可向裁判长申请补足排除故障的时间。

8．参赛队如欲提前结束比赛，应向现场裁判员举手示意，由裁判员记录竞赛终止时间。竞赛终止后，不得再进行任何与竞赛有关的操作。

9．竞赛时间到，参赛队选手应立即结束操作，按照大赛要求和赛题要求提交竞赛成果，禁止在竞赛成果上做任何与竞赛无关的记号。

10．竞赛操作结束后，参赛队要确认成功提交竞赛要求的文件，裁判员在比赛结果的规定位置做标记，并与参赛队一起签字确认。

11．在竞赛过程中，选手如有不服从裁判判决、扰乱赛场秩序、舞弊等不文明行为，由裁判按照规定扣减相应分数并且给予警告，情节严重的取消竞赛资格，竞赛成绩记 0 分，选手退出比赛现场。

2023 年度湖南省“楚怡杯”职业院校技能竞赛
高职电子信息类信息安全管理与评估赛项
竞赛样题

“信息安全管理与评估”样题

第一阶段竞赛项目试题

本文件为信息安全管理与评估项目竞赛第一阶段试题，第一阶段内容包括：网络平台搭建、网络安全设备配置与防护。

介绍

竞赛阶段	任务阶段	竞赛任务
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

所需的设备、机械、装置和材料

所有测试项目都可以由参赛选手根据基础设施列表中指定的设备和软件完成。

评分方案

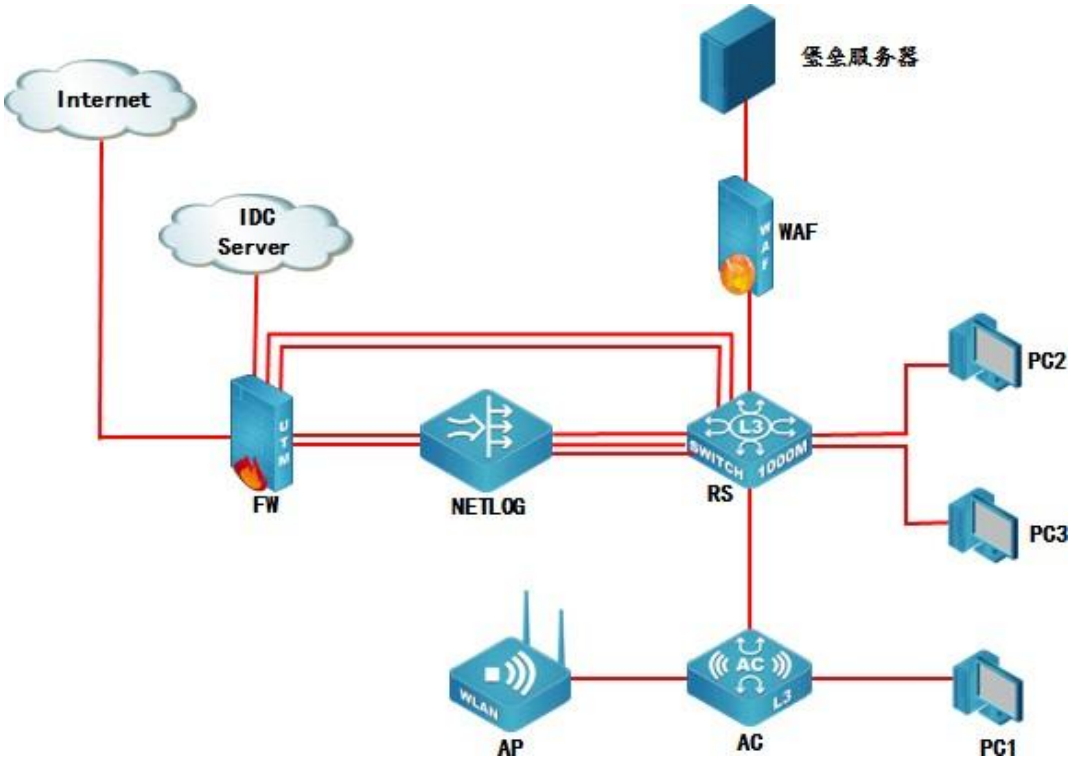
本项目阶段分数为 40 分。

注意事项

赛题第一阶段请按裁判组专门提供的 U 盘中的“XXX-答题模板”中的要求提交答案。选手需要在 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），所完成的 “XXX-答题模板”放置在文件夹中作为比赛结果提交。

项目和任务描述

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FW	ETH0/1-2 （AG1）	AG1.113 10.1.0.254/30 （Trust 安全域）	CS ETH1/0/1CS ETH1/0/2
		AG1.114 10.2.0.254/30 （Trust 安全域）	
	ETH0/3	10.3.0.254/30（Trust 安全域）	BC ETH3

	ETH0/4	10.4.0.254/30（Trust 安全域）	BC ETH4
	ETH0/5	10.100.18.1/27（untrust 安全域）	IDC SERVER 10.100.18.2
	ETH0/6	200.1.1.1/28（untrust 安全域）	INTERNET
	Loopback1	10.11.0.1/24（Trust 安全域）	-
	Loopback2	10.12.0.1/24（Trust 安全域）	
	Loopback3	10.13.0.1/24（Trust 安全域）	
	Loopback4	10.14.0.1/24（Trust 安全域）	
路由交换机CS	VLAN 40 ETH1/0/4-8	172.16.40.62/26	PC2
	VLAN 50 ETH1/0/3	172.16.50.62/26	PC3
	VLAN 51 ETH1/0/23	10.51.0.254/30	BC ETH5
	VLAN 52 ETH1/0/24	10.52.0.254/24	WAF ETH3

	VLAN 113ETH1/0/1	VLAN113 OSPF10.1.0.253/30	FW ETH0/1
	VLAN 114ETH1/0/2	VLAN114 OSPF10.2.0.253/30	FW ETH0/2
	VLAN 117 ETH E1/0/17	10.3.0.253/30	BC ETH1
	VLAN 118CS ETH E1/0/18	10.4.0.253/30	BC ETH2
	ETH1/0/20	VLAN 100 192.168.100.1/302001::192:168:100:1/112VLAN115 OSPF	WS ETH1/0/20
		10.5.0.254/30VLAN116 OSPF 10.6.0.254/30	
无线控制器 WS	ETH1/0/20	VLAN 100 192.168.100.2/302001::192:168:100:2/112VLAN 115 10.5.0.253/30VLAN 116 10.6.0.253/30	CS ETH1/0/20
	VLAN 30ETH1/0/3	172.16.30.62/26	PC1

	无线管理 VLANVLAN 101 ETH1/0/21	需配置	AP
	VLAN 10	需配置	无线 1
	VLAN 20	需配置	无线 2
网络日志系统 BC	ETH1	网桥	FW
	ETH3		CS ETH E1/0/17
	ETH2	网桥	FW
	ETH4		CS ETH E1/0/18
	ETH5	10.51.0.253/30	CS ETH E1/0/23
WEB 应用防火墙WAF	ETH3	10.52.0.253/30	CS ETH E1/0/24
	ETH4		堡垒服务器

工作任务

任务 1：网络平台搭建

题号	网络需求
1	按照 IP 地址规划表，对防火墙的名称、各接口 IP 地址进行配置。
2	按照 IP 地址规划表，对三层交换机的名称进行配置，创建 VLAN 并将相应接口划入VLAN, 对各接口 IP 地址进行配置。
3	按照 IP 地址规划表，对无线交换机的名称进行配置，创建 VLAN 并将相应接口划入VLAN,对接口 IP 地址进行配置。
4	按照 IP 地址规划表，对网络日志系统的名称、各接口 IP 地址进行配置。
5	按照 IP 地址规划表，对 WEB 应用防火墙的名称、各接口 IP 地址进行配置。

任务 2：网络安全设备配置与防护

1. CS 开启telnet 登录功能，用户名 skills01，密码 skills01，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 authoriseduser! Otherwise, we retain the right to pursue the legal responsibility”；
2. 总部交换机 SW 配置简单网络管理协议，计划启用 V3 版本，V3 版本在安全性方面做了极大的扩充。配置引擎号分别为 62001；创建认证用户为 skills01,采用 3des 算法进行加密，密钥为：skills01,哈希算法为 SHA，密钥为：skills01；加入组 ABC，采用最高安全级别；配置组的读、写视图分别为：2022_R、2022_W；当设备有异常时，需要使用本地的 VLAN100 地址发送 Trap 消息至网管服务器 10.51.0.203，采用最高安全级别；
3. 对CS 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；如发现私设 DHCP 服务器则关闭该端口，配置防止 ARP 欺骗攻击；

4. 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CS 所有业务 VLAN 下配置访问控制策略实现双向安全防护；

5. CS 配置 IPv6 地址，使用相关特性实现 VLAN50 的IPv6 终端可自动从网关处获得 IPv6有状态地址；

   WS 配置IPv6 地址，开启路由公告功能，路由器公告的生存期为 2 小时，确保 VLAN30的IPv6 终端可以获得 IPv6 无状态地址。

   WS 与CS 之间配置 RIPng， 使 PC1 与PC3 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

6. 尽可能加大 CS 与防火墙 FW 之间的带宽;配置使总部 VLAN40 业务的用户访问 IDC SERVER的数据流经过 FW 10.1.0.254，IDC SERVER 返回数据流经过 FW 10.2.0.254，且对双向数据流开启所有安全防护，参数和行为为默认；

7. FWCSWS 之间配置OSPF area 0 开启基于链路的MD5 认证，密钥自定义,传播访问 INTERNET默认路由；

8. FW 与CS 建立两对 IBGP 邻居关系，使用 AS 65500，FW 上loopback1-4 为模拟AS 65500中网络，为保证数据通信的可靠性和负载，完成以下配置，要求如下：

   - CS 通过 BGP 到达 loopback1,2 网路下一跳为 10.3.0.254；
   - CS 通过 BGP 到达 loopback3,4 网络下一跳为 10.4.0.254；
   - 通过 BGP 实现到达 loopback1,2,3,4 的网络冗余；
   - 使用 IP 前缀列表匹配上述业务数据流；
   - 使用LP 属性进行业务选路，只允许使用 route-map 来改变LP 属性、实现路由控制，AS PATH 属性可配置的参数数值为：65509

9. 如果CS E1/0/3 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，CS 交换中的数据包大小指定为1600 字节；

10. 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（loopback 接口除外）Untrust 安全域开启 SSH、HTTPS 功能;

11. 总部 VLAN 业务用户通过防火墙访问 Internet 时，复用公网 IP：200.1.1.28/28，保证每一个源 IP 产生的所有会话将被映射到同一个固定的 IP 地址，当有流量匹配本地址转换规则时产生日志信息，将匹配的日志发送至 10.51.0.253 的UDP 2000 端口；

12. 配置L2TP VPN，名称为VPN，满足远程办公用户通过拨号登陆访问内网，创建隧道接口为tunnel 1、并加入 untrust 安全域，地址池名称为 AddressPool，LNS 地址池为10.100.253.1/24-10.100.253.100/24，网关为最大可用地址，认证账号 skills01,密码skills01；

13. FW 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；

14. 在FW 开启安全网关的 TCP SYN 包检查功能，只有检查收到的包为 TCP SYN 包后，才建立连接；配置所有的 TCP 数据包每次能够传输的最大数据分段为 1460，尽力减少网络分片；配置对 TCP 三次握手建立的时间进行检查，如果在 1 分钟内未完成三次握手，则断掉该连接；

15. 为保证总部 Internet 出口线路，在 FW 上使用相关技术，通过 ping 监控外网网关地址，监控对象名称为 Track，每隔5S 发送探测报文，连续 10 次收不到监测报文，就认为线路故障，直接关闭外网接口。FW 要求内网每个 IP 限制会话数量为 300；

16. Internet 端有一分支结构路由器，需要在总部防火墙 FW 上完成以下预配，保证总部与分支机构的安全连接：

防火墙FW 与Internet 端路由器202.5.17.2 建立GRE 隧道，并使用IPSec 保护GRE 隧道，保证分支结构中 2.2.2.2 与总部VLAN40 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:　skills01

17. 已知原 AP 管理地址为 10.81.0.0/15，为了避免地址浪费请重新规划和配置 IP 地址段，要求如下：
    - 使用原 AP 所在网络进行地址划分；
    - 现无线用户 VLAN 10 中需要 127 个终端，无线用户 VLAN 20 需要 50 个终端；
    - WS 上配置DHCP，管理 VLAN 为VLAN101,为AP 下发管理地址，网段中第一个可用地址为AP 管理地址，最后一个可用地址为 WS 管理地址，保证完成 AP 二层注册；为无线用户 VLAN10,20 下发IP 地址，最后一个可用地址为网关；
18. 在NETWORK 下配置SSID，需求如下：
    - NETWORK 1 下设置 SSID 2022skills-2.4G，VLAN10，加密模式为 wpa-personal,其口令为 skills01；
    - NETWORK 20 下设置SSID 2022skills-5G，VLAN20 不进行认证加密，做相应配置隐藏该SSID，只使用倒数第一个可用 VAP 发送5.0G 信号；
19. 配置一个 SSID2022skills_IPv6，属于 VLAN21 用于IPv6 无线测试，用户接入无线网络时需要采用基于 WPA-personal 加密方式,其口令为“skills01”，该网络中的用户从WS DHCP获取 IPv6 地址，地址范围为：2001:10:81::/112；
20. NETWORK 1 开启内置 portal+本地认证的认证方式，账号为 GUEST 密码为 123456,保障无线信息的覆盖性,无线 AP 的发射功率设置为 90%。禁止 MAC 地址为80-45-DD-77-CC-48 的无线终端连接；
21. 通过配置防止多 AP 和WS 相连时过多的安全认证连接而消耗 CPU 资源，检测到 AP 与WS 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；
22. 为方便合理使用带宽，要求针对 SSID 为“2022skills-2.4”下的用户进行带宽控制。对用户上行速率没有限制，但是针对下行速率要求用户的带宽为 2Mbps，在最大带宽可以达到4Mbps；
23. 配置所有 Radio 接口：AP 在收到错误帧时，将不再发送 ACK 帧；打开 AP 组播广播突发限制功能；开启 Radio 的自动信道调整，每天上午 10:00 触发信道调整功能；

24. 配置所有无线接入用户相互隔离，Network 模式下限制每天早上 0 点到4 点禁止终端接入，开启 ARP 抑制功能；
25. 配置当 AP 上线，如果 WS 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；
26. 在公司总部的 BC 上配置，设备部署方式为透明模式。增加非 admin 账户 skills01，密码skills01，该账户仅用于用户查询设备的日志信息和统计信息；要求对内网访问 Internet全部应用进行日志记录。
27. 为日志查询的时间准确性，要求在 BC 上配置NTP 服务，NTP 服务器设定为中国科学院国家授时中心(ntp.ntsc.ac.cn)。
28. 在公司总部的 BC 上配置，在工作日（每周一到周五上班）期间针对所有无线网段访问互联网进行审计，如果发现访问互联网的无线用户就断网 20 分钟，不限制其他用户在工作日（每周一到周五上班）期间访问互联网。
29. BC 配置应用“即时聊天”，在周一至周五 8：00-20：00 监控内网中所有用户的 QQ 账号使用记录，并保存 QQ 聊天记录数据包；
30. BC 配置内容管理，对邮件内容包含“协议”、“投诉”字样的邮件，记录且邮件报警。
31. BC 上配置报警邮箱，邮件服务器 IP 为172.16.10.33，端口号为 25，账号为:skills01，密码: skills01，最大记录数量为 50，同时把报警邮件抄送给 Manager@ chinaskills.com；
32. 使用 BC 对内网所有上网用户进行上网本地认证，要求认证后得用户 4 小时候重新认证，并且对 HTTP 服务器 172.16.10.45 的80 端口进行免认证；
33. BC 上配置用户识别功能,对内网所有 IP 地址进行身份识别；
34. 在公司总部的 WAF 上配置，设备部署方式为透明模式。要求对内网 HTTP 服务器172.16.10.45/32 进行安全防护；
35. 为更好对服务器 172.16.10.45 进行防护，我们定期对服务器进行 Web 漏洞扫描，来及时修改我们的防护规则。
36. 方便日志的保存和查看，需要在把 WAF 上攻击日志、访问日志、DDoS 日志以 JSON 格式发给IP 地址为172.16.10.200 的日志服务器上；

37. 在WAF 上配置基础防御功能，开启 SQL 注入、XXS 攻击、信息泄露等防御功能，要求针对这些攻击阻断并发送邮件告警；
38. 在WAF 上针对HTTP 服务器进行 URL 最大个数为 10，Cookies 最大个数为 30，Host 最大长度为 1024，Accept 最大长度 64 等参数校验设置，设置严重级别为中级，超出校验数值阻断并发送邮件告警；
39. 在 WAF 上保护 HTTP 服务器上的 www.2022skills.com 网站爬虫攻击，从而影响服务器性能，设置严重级别为高级，一经发现攻击阻断并发送邮件告警；
40. 为防止 www.2022skills.com网站资源被其他网站利用，通过 WAF 对资源链接进行保护，通过 Referer 方式检测，设置严重级别为中级，一经发现阻断并发送邮件告警。

第二阶段竞赛项目试题

本文件为信息安全管理与评估项目竞赛第二阶段试题，第二阶段内容包括：网络安全事件响应、数字取证调查和应用程序安全。

介绍

竞赛有固定的开始和结束时间，参赛队伍必须决定如何有效的分配时间。请认真阅读以下指引。

（1） 当竞赛结束，离开时请不要关机；

（2） 所有配置应当在重启后有效；

（3） 除了 CD-ROM/HDD/NET 驱动器，请不要修改实体机的配置和虚拟机本身的硬件设置。

所需的设备、机械、装置和材料

所有测试项目都可以由参赛选手根据基础设施列表中指定的设备和软件完成。

评分方案

本项目模块分数为 20 分。

项目和任务描述

随着网络和信息化水平的不断发展，网络安全事件也层出不穷，网络恶意代码传播、信息窃取、信息篡改、远程控制等各种网络攻击行为已严重威胁到信息系统的机密性、完整性和可用性。因此，对抗网络攻击，组织安全事件应急响应，采集电子证据等技术工作是网络安全防护的重要部分。现在，A 集团已遭受来自不明组织的非法恶意攻击,您的团队需要帮助 A 集团追踪此网络攻击来源，分析恶意攻击攻击行为的证据线索，找出操作系统和应用程序中的漏洞或者恶意代码，帮助其巩固网络安全防线。

本模块主要分为以下几个部分：

- 网络安全事件响应
- 数字取证调查
- 应用程序安全

本部分的所有工作任务素材或环境均已放置在指定的计算机上，参赛选手完成后，填写在电脑桌面上“信息安全管理与评估竞赛-第二阶段答题卷”中。选手的电脑中已经安装好 Office软件并提供必要的软件工具 （Tools 工具包）。

工作任务

第一部分 网络安全事件响应

任务 1：应急响应

A 集团的 Windows 服务器被黑客入侵，该服务器的系统目录被上传恶意软件，域用户凭证被读取，您的团队需要帮助该公司追踪此网络攻击的来源，

在服务器上进行全面的检查，包括日志信息、进程信息、系统文件、恶意文件等，从而分析黑客的攻击行为，发现系统中的漏洞，并对发现的漏洞进行修复。

本任务素材清单：Server 服务器虚拟机。

受攻击的 Windows 服务器已整体打包成虚拟机文件保存，请选手自行导入分析。

注意：Windows 服务器的基本配置参见附录，若题目中未明确规定，请使用默认配置。请根据赛题环境及任务要求提交正确答案。

任务 1：应急响应		
序号	**任务要求**	**答案**
1	任务要求 1	
2	任务要求 2	
3	任务要求 3	
4	.....	

第二部分 数字取证调查

任务 2 ：操作系统取证

A 集团某Windows 服务器系统感染恶意程序，导致系统被远程监听，请分析 A 集团提供的系统镜像和内存镜像，找到系统镜像中的恶意软件，分析恶意软件行为。

本任务素材清单：操作系统镜像、内存镜像。

请根据赛题环境及任务要求提交正确答案。

任务 2：操作系统取证		
序号	**任务要求**	**答案**
1	任务要求 1	
2	任务要求 2	
3	任务要求 3	
4	.....	

任务 3： 网络数据包分析

A 集团的网络安全监控系统发现有恶意攻击者对集团官方网站进行攻击，并抓取了部分可疑流量包。请您根据捕捉到的流量包，搜寻出网络攻击线索，并分析黑客的恶意行为。

本任务素材清单：捕获的网络数据包文件。

请根据赛题环境及任务要求提交正确答案。

任务 3：网络数据包分析		
序号	**任务要求**	**答案**
1	任务要求 1	
2	任务要求 2	
3	任务要求 3	
4	.....	

任务 4： 计算机单机取证

对给定取证镜像文件进行分析，搜寻证据关键字（线索关键字为“evidence 1”、“evidence 2”、……、“evidence 10”，有文本形式也有图片形式，不区分大小写），请提取和固定比赛要求的标的证据文件，并按样例的格式要求填写相关信息，证据文件在总文件数中所占比例不低于15%。取证的信息可能隐藏在正常的、已删除的或受损的文件中，您可能需要运用编码转换

技术、加解密技术、隐写技术、数据恢复技术，还需要熟悉常用的文件格式（如办公文档、压缩文档、图片等）

本任务素材清单：取证镜像文件。

请按要求完成该部分的工作任务。

任务 4： 计算机单机取证		
证据编号	**在取证镜像中的文件名**	**镜像中原文件Hash 码（MD5，不区分大小写）**
evidence 1		
evidence 2		
evidence 3		
evidence 4		
evidence 5		
evidence 6		

evidence 7		
evidence 8		
evidence 9		
evidence 10		

第三部分 应用程序安全

任务 5：代码审计

A 集团发现其发布的 Web 应用程序遭到了恶意攻击，A 集团提供了 Web 应用程序的主要代码，您的团队需要协助 A 集团对该应用程序代码进行分析，找出存在的脆弱点。

本任务素材清单：Web 程序文件。

请根据赛题环境及任务要求提交正确答案。

任务 5：代码审计		
序号	**任务要求**	**答案**
1	任务要求 1	
2	任务要求 2	
3	任务要求 3	
4	.....	

任务 6：Windows 系统恶意程序分析

A 集团发现其网络中蔓延了一种恶意程序，现在已采集到恶意程序的样本，您的团队需要协助 A 集团对该恶意程序样本进行逆向分析、对其攻击/破坏的行为进行调查取证。

本任务素材清单：恶意程序文件。

请根据赛题环境及任务要求提交正确答案。

任务 6：Windows 系统恶意程序分析		
序号	**任务要求**	**答案**
1	任务要求 1	
2	任务要求 2	
3	任务要求 3	
4	……	

第三阶段竞赛项目试题

本文件为信息安全管理与评估项目竞赛-第三阶段试题。根据信息安全管理与评估项目技术文件要求，第三阶段为夺旗挑战 CTF（网络安全渗透）。

本次比赛时间为 180 分钟。

介绍

夺旗挑战赛（CTF）的目标是作为一名网络安全专业人员在一个模拟的网络环境中实现网络安全渗透测试工作。

本模块要求参赛者作为攻击方，运用所学的信息收集、漏洞发现、漏洞利用等渗透测试技术完成对网络的渗透测试;并且能够通过各种信息安全相关技术分析获取存在的 flag 值。

所需的设备、机械、装置和材料

所有测试项目都可以由参赛选手根据基础设施列表中指定的设备和软件完成。

评分方案

本项目阶段分数为 40 分。

注意事项

通过找到正确的 flag 值来获取得分，它的格式如下

所示：flag{<flag 值 >}

这种格式在某些环境中可能被隐藏甚至混淆。所以，注意一些敏感信息并利用工具把它找出来。

项目和任务描述

在A 集团的网络中存在几台服务器，各服务器存在着不同业务服务。在网络中存在着一定网络安全隐患，请利用你所掌握的渗透测试技术，通过信息收集、漏洞挖掘等渗透测试技术，完成指定项目的渗透测试，在测试中获取 flag 值。

网络环境参考样例请查看附录 A。

本模块所使用到的渗透测试技术包含但不限于如下技术领域：

- 信息收集
- 逆向文件分析
- 二进制漏洞利用
- 应用服务漏洞利用
- 杂项与密码学分析

所有设备和服务器的 IP 地址请查看现场提供的设备列表。

工作任务

一、Web1 服务器

任务编号	任务描述	答案	分值
任务一	Web1 系统存在隐藏信息，请找出隐藏信息，并将flag 提交。 flag 格式 flag{<flag 值>}		
任务二	Web1 系统存在漏洞，请利用漏洞并找到flag，并将 flag提交。flag 格式flag{<flag 值>}		
任务三	Web1 系统后台存在漏洞，请利用漏洞并找到 flag，并将		

	flag 提交。flag 格式 flag{<flag 值>}		

二、Web2 服务器

任务编号	任务描述	答案	分值
任务四	Web2 系统存在漏洞，请利用漏洞并找到flag，并将flag提交。flag 格式flag{<flag 值>}		
任务五	Web2 系统后台存在漏洞，请利用漏洞并找到 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		

三、FTP 服务器

任务编号	任务描述	答案	分值
任务六	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将flag提交。flag格式 flag{<flag 值>}		

任务七	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将flag 提交。flag 格式 flag{<flag 值>}		
任务八	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将flag 提交。flag 格式 flag{<flag 值>}		
任务九	请获取 FTP 服务器上对应的流量包进行分析，找出其中隐藏的 flag，并将 flag 提交。flag 格式flag{<flag 值>}		
任务十	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将flag 提交。flag 格式 flag{<flag 值>}		
任务十一	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将flag 提交。flag 格式 flag{<flag 值>}		
任务十二	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将flag 提交。flag 格式 flag{<flag 值>}		
任务十三	请获取 FTP 服务器上对应的文件进行分析，找出其中隐藏的 flag，并将flag 提交。flag 格式 flag{<flag 值>}		

四、应用程序 1 服务器

任务编号	任务描述	答案	分值

任务十四	应用程序1 服务器10000 端口存在漏洞，找出其中隐藏的flag， 并将flag 提交。flag格式flag{<flag 值>}		

五、应用程序 2 服务器

任务编号	任务描述	答案	分值
任务十五	应用程序2 服务器10001 端口存在漏洞，找出其中隐藏的flag， 并将flag 提交。flag格式flag{<flag 值>}		

分值分布表

表1 第三阶段分值分布

序号	描述	分值
C	夺旗(攻击)	
C1	信息收集	
C2	逆向文件分析	
C3	二进制漏洞利用	
C4	应用服务漏洞利用	
C5	杂项与密码学分析	