首届世界职业院校技能大赛

信息技术应用创新赛项

赛　题

竞赛说明

一、竞赛内容发布

“网络搭建与应用”赛项竞赛共分三个部分，其中：

第一部分：信创服务运维（600 分），比赛时间：240 分钟；

第二部分：信创 CTF（200 分），比赛时间：120 分钟；

第三部分：信创安全对抗（200 分）比赛时间：60 分钟；

二、竞赛注意事项

1. 禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

2. 请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

3. 请选手仔细阅读比赛试卷，按照试卷要求完成各项操作。

4. 操作过程中，需要及时保存设备配置。

5. 比赛结束后，所有设备保持运行状态，评判以最后的硬件连接和配置为最终结果。

6. 比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。

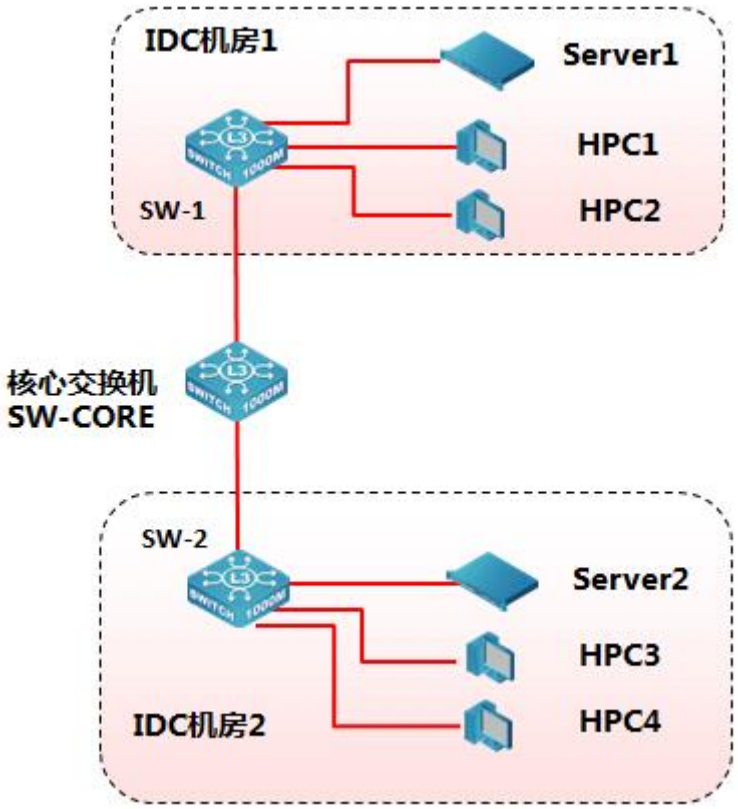
7. 禁止在纸质资料、比赛设备、上填写任何与竞赛无关的标记，如违反规定，可视为 0 分。

8. 与比赛相关的工具软件放置在每台主机的 D:\soft 文件夹中。

项目简介:

2021 年疫情过后，公司计划继续开展之前定下的战略规划。在集团高层领导下，下半年公司规模恢复快速发展，业务数据量和公司访问量增长巨大。为了更好管理数据，提供服务，集团决定将公司两个 IDC 机房增加两台信创服务器和 PC，部署部分应用进行测试。

拓扑:



网络设备链接表:

A 设备连接至 B 设备			
设备名称	接口	设备名称	接口
SW-1			
SW-2			
SW-CORE			
Server1			
Server2			
HPC1			
HPC2			
HPC3			
HPC4			

虚拟机名称	域名信息	服务角色	IPv4 信息
Server1			
Linux-1	cs1.skills.com	DNS 服务 CA 服务 chrony 服务	10.10.70.11
Linux-2	cs2.skills.com	DNS 服务 mail 服务 docker 服务	10.10.70.12
Linux-3	cs3.skills.com	apache2 服务 Mariadb 服务 PHP 服务 rsyslog 服务	10.10.70.13
Linux-4	cs4.skills.com	Mariadb 客户端 rsyslog 客户端	10.10.70.14
Server2			
Linux-5	cs5.skills.com	iSCSI 服务	10.10.70.15 10.10.80.16
Linux-6	cs6.skills.com	keepalive 集群	10.10.70.16 10.10.80.17
Linux-7	cs7.skills.com	keepalive 集群	10.10.70.17 10.10.80.18

信创网络运维（600 分）

比赛时间 240 分钟

一、信创服务器组建及上架（50 分）

右侧布线面板立面示意图　　左侧布线面板立面示意图

【说明】

1. 机柜左侧布线面板编号 101；机柜右侧布线面板编号 102。
2. 面对信息底盒方向左侧为 1 端口、右侧为 2 端口。所有配线架、模块按照 568B 标准端接。
3. 主配线区配线点与工作区配线点连线对应关系如下表所示。
4. PC1、PC2 配线点连线对应关系表

序号	信息点编号	配线架编号	底盒编号	信息点编号	配线架端口编号
1	W1-02-101-1	W1	101	1	02
2	W1-06-102-1	W1	102	1	06

一、铺设线缆并端接

1. 截取 2 根适当长度的双绞线，两端制作标签，穿过 PVC 线槽或线管。双绞线在机柜内部进行合理布线，并且通过扎带合理固定;
2. 将 2 根双绞线的一端，根据“PC1、PC2 配线点连线对应关系表“的要求，端接在配线架的相应端口上;
3. 将 2 根双绞线的另一端，根据“PC1、PC2 配线点连线对应关系表”的要求，端接上 RJ45 模块，并且安装上信息点面板，并标注标签。

二、跳线制作与测试

1. 再截取 2 根当长度的双绞线，两端制作标签，根据“PC1、PC2 配线点连线对应关系表”的要求，链接网络信息点和相应计算机，端接水晶头，制作网络跳线，所有网络跳线要求按 568B 标准制作;
2. 根据网络拓扑要求，截取适当长度和数量的双绞线，端接水晶头，制作网络跳线， 根据题目要求，插入相应设备的相关端口上;（包括设备与设备之间、设备与配线架之间）;
3. 实现 PC、信息点面板、配线架、设备之间的连通;（提示：可利用机柜上自带的设备进行通断测试）;

PC1 连接 102 底盒 1 端口、PC2 连接 101 底盒 1 端口。

三、信创服务器上架

1. 信创服务器需按综合布线标准上架;
2. 信创服务器，HPC 使用双绞线或光纤与交换机正确连接;

二、信创网络搭建（100分）

1. 为了减少广播，需要根据题目要求规划并配置VLAN。要求配置合理，所有链路上不允许不必要VLAN的数据流通过，包括VLAN 1。根据下述信息及表，在交换机上完成VLAN配置和端口分配。

设备	VLAN编号	端口	说明
SW-1	VLAN10	E1/0/1-4	营销1段
	VLAN20	E1/0/5-7	产品1段
	VLAN30	E1/0/8-10	法务1段
	VLAN40	E1/0/11-12	财务1段
	VLAN50	E1/0/13-14	人力1段
SW-2	VLAN10	E1/0/1-4	营销2段
	VLAN20	E1/0/5-7	产品2段
	VLAN30	E1/0/8-10	法务2段
	VLAN40	E1/0/11-12	财务2段
	VLAN50	E1/0/13-14	人力2段
SW-3	VLAN20	E1/0/1-6	产品3段
	VLAN30	E1/0/7-11	法务3段
	VLAN50	E1/0/12-15	人力3段

2. 集团核心交换机SW-1和SW-2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”。
3. 集团核心交换机SW-1、 SW-2与SW-CORE间租用运营商三条裸光缆通道实现两个DC之间互通，一条裸光缆通道实现三层IP业务承载、一条裸光缆通道实现VPN业务承载、一条裸光缆通道实现二层业务承载。具体要求如下:
4. 为了节约集团成本，设计实现VPN业务承载的裸光缆通道带宽只有10Mbps，后续再根据业务使用情况再考虑是否扩容；使用相关技术分别实现集团财务1段、财务2段业务路由表与其它业务网段路由表隔离；

5. 目前设计实现二层业务承载的只有一条裸光缆通道，随着集团 IDC 服务器数量快速扩容，预计未来 2-3 年集团 DC 间服务器大二层流量会呈现爆发式增长，配置相关技术，方便后续链路扩容与冗余备份。
6. SW-CORE 既作为集团核心交换机实现与集团财务业务路由表、其它业务网段路由表隔离，Internet 路由表位于 VPN 实例名称 Internet 内。
7. 配置相关功能，使集团核心交换机 SW-1、 SW-2 、SW-CORE 设备能够在网络中相互发现并交互各自的系统及配置信息，以供管理员查询两端接口对应关系及判断链路的通信状况。

三、信创系统运维（400分）

1. DNS服务

1. 设置所有Linux服务器的时区设为“上海”，本地时间调整为实际时间。
2. 启动所有Linux服务器的防火墙，并添加相应端口（不允许添加服务）放行相关服务。
3. 利用chrony配置Linux-1为其他Linux主机提供时间同步服务。
4. 利用bind9软件，配置Linux-1为主DNS服务器，采用rndc技术提供不间断的DNS服务；配置Linux-2为备用DNS服务器，为所有Linux主机提供冗余DNS正反向解析服务。
5. 所有Linux主机root用户使用完全合格域名免密码ssh登录到其他Linux主机。
6. 配置Linux-1为CA服务器,为所有Linux主机颁发证书，不允许修改/etc/pki/tls/openssl.conf。CA证书有效期20年，CA颁发证书有效期均为10年,证书信息:国家=“CN”,省=“Beijing”,城市=“Beijing”,组织=“skills”,组织单位=“system”。chrome浏览器访问https网站时，不出现证书警告提示信息。

2. mail服务

1. 配置Linux-2为mail服务器，安装postfix和dovecot。
2. 仅支持smtps和pop3s连接，证书路径为/etc/ssl/mail.crt，私钥路径为/etc/ssl/mail.key。
3. 创建用户mail1和mail2,向all@skills.com发送的邮件,每个用户都会收到。
4. root用户使用mail工具向all@skills.com发送一封邮件,邮件主题为“Hello”，内容为“Welcome”。

3. apache2 服务

1. 配置 Linux-2 为 httpd 服务器，安装 apache2，http 访问时自动跳转到 https 安全连接。
2. 采用 LDAP 认证用户，只有认证的账户 user1 和 user2 才能访问网站。
3. 使用 skills.com 或 any.skills.com（any 代表任意网址前缀）访问时，自动跳转到 www.skills.com。
4. 关闭不安全的服务器信息，在任何页面不会出现系统和 WEB 服务器版本信息。
5. 客户端访问时，必须有 SSL 证书。

4. rsyslog 服务

配置 Linux-3 为远程日志服务器，为 Linux-4 提供日志服务。

5. Mariadb 服务

1. 配置 Linux-3 为 Mariadb 服务器，安装 Mariadb-server，创建数据库用户 jack，在任意机器上对所有数据库有完全权限；允许 root 远程登陆。
2. 配置 Linux-4 为 Mariadb 客户端，在/app 目录中设计并编写 Python 程序 mariadb2.py，创建数据库 userdb；在库中创建表 userinfo，在表中插入 2 条记录，分别为(1,user1,1995-7-1,男)，(2,user2,1995-9-1,女)，口令与用户名相同，password 字段用 password 函数加密，表结构如下：

字段名	数据类型	主键	自增
id	int	是	是
name	varchar(10)	否	否
birthday	datetime	否	否
sex	char(5)	否	否
password	char(200)	否	否

3. 在/app 目录中设计并编写 Python 程序 mariadb3.py，修改表 userinfo 的结构，在 name 字段后添加新字段 height(数据类型为 float)，更新

user1 和 user2 的 height 字段内容为 1.61 和 1.62。

4. 把物理机/soft/mysql.txt 中的内容导入到 userinfo 表中，password 字段用 password 函数加密。
5. 将表 userinfo 中的记录导出，并存放到/var/databak/mysql.sql 文件中。

6. PHP 服务

1. 在 Linux-3 上安装 php，搭建 PHP 网站。

7. keepalive 服务

1. 为 Linux-5 添加 4 块硬盘，每块硬盘大小为 5G，创建 lvm 卷，卷组名称为 vg1，逻辑卷名称为 lv1，容量为全部空间，格式化为 ext4 格式。使用/dev/vg1/lv1 配置为 iSCSI 目标服务器，为 Linux-6 和 Linux-7 提供 iSCSI 服务。iSCSI 目标端的 wwn 为 iqn.2021-05.com.skills:server,iSCSI 发起端的 wwn 为 iqn.2021-05.com.skills:client.
2. 配置 Linux-6 和 Linux7 为 iSCSI 客户端。
3. 配置 Linux-6 和 Linux-7 为集群服务器，安装 keepalive，Linux-6 为主服务器，Linux-7 为备份服务器，虚拟 IP 地址为 10.10.70.90。提供 apache 服务，域名为 www2.skills.com,，网站主页 index.html 内容为“HelloLinuxCluster”。

8. 虚拟化

1. 在 Linux-2 上安装 docker-ce，导入 centos 镜像。软件包和镜像存放在物理机/soft/DockerLinux。

创建名称为 skills 的容器，映射 Linux-2 的 80 端口到容器的 80 端口，在容器内安装 apache2，默认网页内容为“HelloContainer”。

四、职业素养（50分）

信创 CTF（200 分）
比赛时间 120 分钟

在 集团IDC网络中存在几台信创服务器，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。

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

任务一、WEB 服务器

1. Web 服务器系统存在隐藏信息，请找出隐藏信息，并将 flag 提交。flag 格式 flag{<flag 值>}

2. Web 服务器系统存在漏洞,请利用漏洞并找到 flag,并将 flag 提交。flag 格式 flag{<flag 值>}

3. Web 服务器系统后台存在漏洞,请利用漏洞并找到 flag,并将 flag 提交。flag 格式 flag{<flag 值>}

任务二、FTP 服务器

1. 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>}

2. 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>}

3. 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>}

4. 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>}

5. 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>}

6. 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>}

任务三、应用服务器

1. 应用服务器 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>}

2. 应用服务器 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>}

3. 应用服务器 10002 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>}

4. 应用服务器 10003 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>}

5. 应用服务器 10004 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>}

任务四、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:

虚拟机 1:

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:

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:

服务器场景的 FTP 服务账号：匿名

任务内容:

1. 从靶机服务器场景的 FTP 服务器中下载数据集文件：DS01、DS02，以及机器学习算法脚本：WebSec.py，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）；
2. 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）

3. 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）
4. 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）
5. 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）
6. 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）
7. 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）
8. 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）
9. 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）
10. 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）

11. 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）；

信创分组对抗（200 分）
比赛时间 60 分钟

假定各位选手是集团的信息安全工程师，负责服务器的维护，该信创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、3306、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。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。