2023

金砖国家职业技能大赛
(金砖国家未来技能挑战赛)

样题 TP(仅供选拔赛参考)

BRICS-FS-27_IT 网络系统管理

2023 年 8 月

模块 A　网络布线与设备配置

分值：100 分

竞赛时间：120 分钟

背景信息：

扬威国际信息有限责任公司 IT 部门的网络工程师们，大家好：我司总部在北京，设有技术研发、产品制造、营销、财务、人力、IT 等部门，在武汉设有办事处。

近年来，随着我国数字经济的高速发展，我司业务范围和经营规模也在快速增长，为满足公司高质量发展需求，同时为员工营造良好的办公环境，急需开拓新的办公地点，准备在上海成立分公司。

从今天起，开始为新成立的分公司搭建网络，并做好网络系统管理工作。

任务 1：网络布线方案设计

任务背景：

工程师们，我司新成立的上海分公司已确认选址，地址为联创 SOHO 七层与八层。我们首先要对新办公地点进行综合布线设计及布线工程实施，然后进行交换机等网络设备安装及配置，最后进行系统测试。

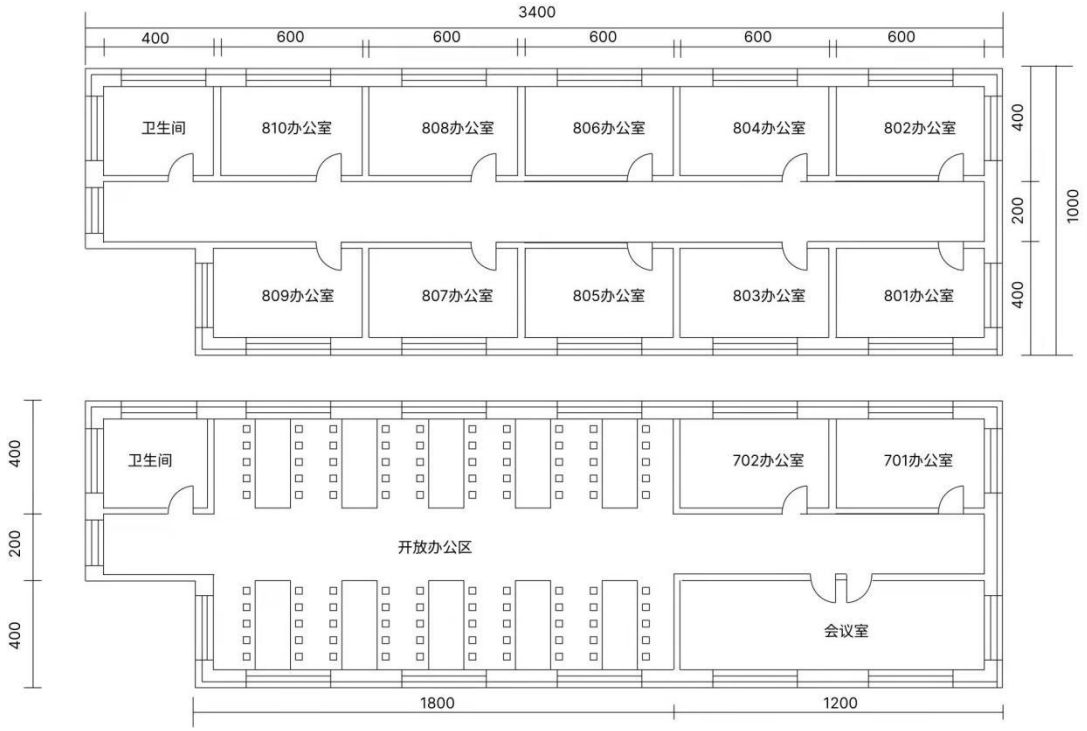
请根据以下提供的资料和数据，在规定的时间内完成有关具体任务。

任务描述：

根据建筑平面设计图和布线需求，对新办公地点进行综合布线设计。

资料：

1. 平面设计图及功能规划



7 层：长约 34 米，宽约 10 米，层高 4 米，有 1 个开放工作区（有 100 个工位）长度约 18 米、1 间会议室（12 人）约 12 米、2 间办公室（每间 4 人）每个 6 米，其中 701 号办公室作为公司网络机房。详见 7 层示意图

8 层：长和宽与 7 层一样，10 间办公室，801-810 室（每间 4 人），每间约 6 米，为公司行政办公室。详见 8 层示意图

2.综合布线需求

（1）分公司采用 1000M 做骨干网络，100M 到桌面，采用超五类双绞线；

（2）分公司采用防火墙结构进行接入，用于同总部业务数据进行同步，网络互联设备（防火墙、路由器、交换机及其设备）；

（3）按分公司部门设置，划分产品(vlan6)、研发(vlan5)、培训(vlan9)、营销(vlan8)、咨询(vlan2)5 个 vlan,服务器组为(vlan7)一个 vlan，vlan 之间不能互访，只有产品和研发部门可以访问服务器组 vlan，服务器组与集团通过 vpn 进行通信；

（4）分公司内具有 www 服务器、财务服务器、公司业务应用服务器，用于公司日常业务需要和网络管理等；

（5）分公司采用基于 MySQL 的数据库做开发平台。

要求：

1.在给定的建筑平面图基础上，进行综合布线设计，使用绘图软件绘制，考虑到网络系统后续的拓展和维护性，采用星形拓扑结构：

（1）每个工位作为 1 个信息点，防火墙和路由器的数量为 1 个，使用 cad 绘制设计方案，保存为 png 格式图片，上传比赛系统；

（2）依据上一个任务的设计方案，对网络耗材进行估算，其中包括：超 5 类双绞线长度、电脑数量、交换机（24 口）数量、防火墙。

2. 使用 visio 画图软件绘制分公司网络拓扑图，保存为 png 格式图片，并上传比赛系统。

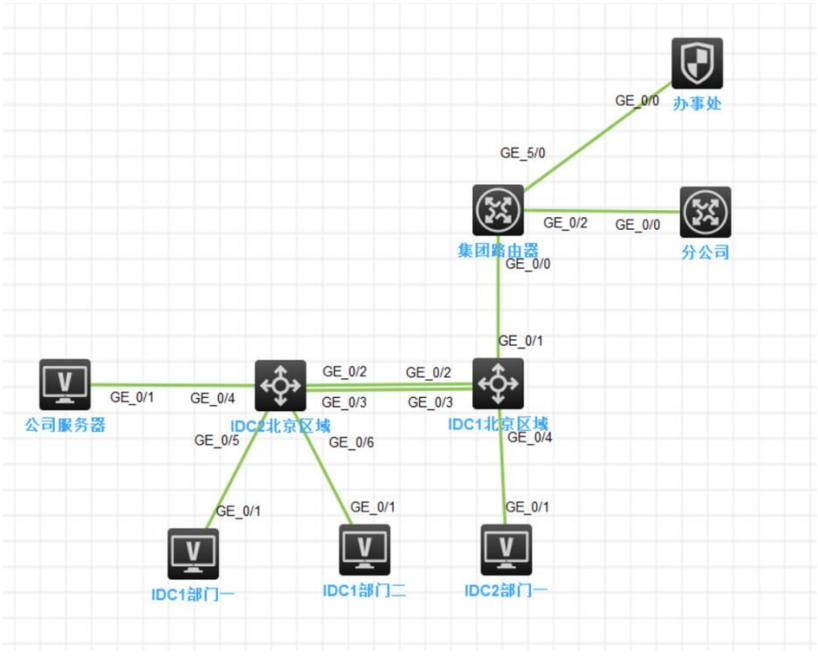
任务 2：网络设备配置及测试

任务描述：

实现集团、北京数据中心、分公司、办事处的网络互连互通。

资料及要求：

1. 网络拓扑图：



IDC1 北京区域、IDC2 北京区域为公司集团核心交换，集团路由

器、分公司路由器、办事处防火墙用于网络互连。

（请注意：在此典型互联网应用网络架构中，作为 IT 网络运维人员，请根据拓扑构建完整的系统环境，使整体网络架构具有良好的稳定性、安全性、可扩展性。请完成所有服务配置后，从客户端进行测试，确保能正常访问到相应应用。）

2.网络连接表：

A 设备连接至 B 设备			
设备名称	接口	设备名称	接口
IDC2 北京区域（SW）	GE1/0/2	IDC1 北京区域（sw）	GE1/0/2
IDC2 北京区域（SW）	GE1/0/3	IDC1 北京区域（sw）	GE1/0/3
IDC2 北京区域（SW）	GE1/0/4	公司服务器（server）	GE1/0/2
IDC2 北京区域（SW）	GE1/0/5	IDC1 部门一	GE1/0/1
IDC2 北京区域（SW）	GE1/0/6	IDC1 部门一	GE1/0/1
IDC1 北京区域（SW）	GE1/0/4	IDC1 部门一	GE1/0/1
IDC1 北京区域（SW）	GE1/0/1	集团路由器	GE1/0/0
集团路由器	GE1/0/2	分公司路由器	GE1/0/0
集团路由器	GE1/0/5	办事处	GE1/0/0

3.网络设备分配表

设备名称	设备接口	IP 地址
IDC2 北京区域	GE1/0/2	10.60.254.11/30

	GE1/0/3 配置 vlan 中继	
	GE1/0/4 服务器网段（vlan30）	172.16.30.1~254/24
	GE1/0/5（vlan10 营销 1）	172.16.10.1~254/24
	GE1/0/6（vlan20 产品 1）	172.16.20.1~254/24
	GE1/0/7（vlan40 法务 1）	172.16.40.1~254/24
	GE1/0/8（vlan50 财务 1）	172.16.50.1~254/24
	GE1/0/9（vlan60 人力 1）	172.16.60.1~254/24
IDC1 北京区域	GE1/0/1	10.60.255.5/30
	GE1/0/2	10.60.254.12/30
	GE1/0/3 配置 vlan 中继	
	GE1/0/5（vlan10 营销 1）	172.16.10.1~254/24
	GE1/0/6（vlan20 产品 1）	172.16.20.1~254/24
	GE1/0/7（vlan40 法务 1）	172.16.40.1~254/24
	GE1/0/8（vlan50 财务 1）	172.16.50.1~254/24
	GE1/0/9（vlan60 人力 1）	172.16.60.1~254/24
集团路由	GE1/0/2	10.60.254.12/30
	GE1/0/5	10.60.253.6/30
	GE1/0/0	10.60.255.6/30
分公司路由	GE1/0/0	10.60.254.14/30
办事处	GE1/0/0	10.60.253.7/30

4.交换机配置

（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，包含 VLAN1。核心交换机 IDC2 北京区域和核心交换机 IDC1 北京区域之间业务承载的裸光缆通道目前暂时只允许 VLAN10、VLAN20、VLAN30、VLAN40、VLAN50 通过，禁止配置 VLAN 及接口的描述信息；

（2）核心交换机 IDC2 和核心交换机 IDC1 之间线路租用运营商 2 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二层业务承载。具体要求如下：

第一：配置实现三层 IP 业务承载的裸光缆通道最大传输单元为 1500bytes；

第二：目前设计实现二层业务承载的只有一条裸光缆通道，为了应对未来二层业务流量的增长，配置相关技术，方便后续链路扩容与冗余备份，编号为 1；

第三：配置核心交换机采用报文的源 MAC 地址和目的 MAC 地址进行负载分担；

第四：使用 CBQ 对“IDC2 北京区域"对营销业务网段的限制收、发数据占用的带宽分别 3096Kbp、1024Kbp；“IDC1 北京区域"对产品网段限制收、发数据占用的带宽分别 2048bps、1024bps；

第五：配置 Server 的 MAC（0014-222c-aa69）为静态 MAC 地址表项，使用户发往服务器的报文只从 GigabitEthernet1/0/4 单播发送出去。丢弃 MAC 地址为 00a0-fc00-583c 的报文。

开启 GigabitEthernet1/0/9 端口的 MAC Information 功能，发送时间间隔为 300 秒， 配置 Device 将 Syslog 信息发送到日志主机（主机地址：192.168.1.10）；

第六：已知 NTP Server 为 109.120.2.191，该服务器时间是国际标准时间，请在所有交换机上配置该功能，保证交换机的时钟和北京时间一致。

5.路由器配置

规划集团内部、集团与广东办事处之间使用 OSPF 协议，集团内使用进程号为 1，集团与成都办事处间使用进程号为 12，具体要求如下：

（1）核心交换机 IDC1 与 IDC2 之间、集团路由器 与 IDC2 之间、集团路由器与 分公司路由器均属于骨干区域；集团路由器与办事处防火墙之间属于普通区域，区域号为 20；

（2）调整 OSPF 进程号 1 所有接口发送 Hello 包的时间间隔为 5 秒，如果接口在 3 倍时间内都没有收到对方的 Hello 报文，则认为对端邻居失效；

（3）IDC1、IDC2 只允许发布营销网段业务路由；办事处防火墙分别发布自身营销、产品网段业务路由。核心交换机 IDC1、IDC2 OSPF 进程 1 的路由表中业务网段路由只允许学习到办事处防火墙通告的 TYPE1 类型的缺省路由、集团营销业务网段路由。

6.防火墙配置：

（1）2022 年护网行动开展在即，调整全网防火墙安全策略缺省

规则为拒绝；在办事处防火墙上限制办事处产品业务网段只可以访问集团产品网段 https、mysql 数据库类型业务，集团营销网段可以访问广东办事处营销业务网段任何端口；

（2）在办事处防火墙配置网络地址转换，NAT 地址转换条件中源、目的 IP 均为 any，公网 NAT 地址池为：202.60.21.0/28；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 100.61.11.122 的 UDP 514 端口；开启相关特性，实现扩展 NAT 转换后的网络地址端口资源；

（3）办事处防火墙开启安全网关的 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；

（4）办事处的出口带宽为 800Mbps，为集团内研发、营销、行政、财务 4 个业务网段更加合理使用出口资源，要求出口带宽小于 480Mbps 时，每 IP 上下行最大 5Mbps 带宽；出口带宽大于 720Mbps 时，每 IP 上下行最大 2Mbps 带宽，规则名称为 JT。同时要求在流量变化期间带宽增长速率为 2 倍，在任何时候都要确保网页访问服务占每 IP 带宽的 40%，FW-1 要求内网每个 IP 限制会话数量为 300。

任务 3：编写 Python 脚本实现网络测试自动化

任务描述：

使用 Python 脚本搜索哪些 IP 地址空闲，完成自动化运维工作。

要求：

1. 根据使用 python 的异或方法编写一段生成 192.168.1.1~192.168.1.254 的代码程序；

2. 使用 python 的 xxx 包对第一题生成的 ip 随机改变颜色，红色代表占用，绿色代表空闲并将 ip 变换成*，输出一个 16*16 的矩阵；

3. 集团网络有多个网络，使用多进程方法，实现同时计算 192.168.1.0/24、192.168.2.0/24,192.168.3.0/24 三个网段的空闲 ip 个数。

模块 B 云网络搭建与运维

分值：100 分

竞赛时间：180 分钟

项目背景：

工程师们，分公司前面完成了网络布线与设备配置。鉴于分公司业务量繁杂，对公司数据中心承载能力和运维服务要求较高。

为节约硬件成本，实现按需调配资源，并能快速回收，故在分公司搭建私有云平台。

请根据下文提供的资料和数据,在规定的时间内完成具体任务。

任务 1 基础运维任务

任务描述

配置 OpenStack 服务器基础环境。

要求：

1.在节点为服务器增加新增 test 用户；

2.在节点上更新镜像源；

3.在节点上配置主机名；

4.在节点上配置 hosts 文件 IP 和主机名的映射关系。

任务 2 OpenStack 搭建任务

任务描述：

部署 OpenStack 云平台虚拟化环境。

要求：

1.OpenStack 平台基础服务（rabbitmq、mariadb、memcache、Apache)；

2.配置 OpenStack keystone 组件；

3.配置 OpenStack Glance 组件；

4.配置 OpenStack Nova 组件；

5.配置 OpenStack Neutron 组件；

6.配置 OpenStack dashboard 组件。

任务 3 OpenStack 云平台运维

任务描述：

通过 OpenStack 配置私网内的 IP 地址段、子网、安全组等子服务。

要求：

1.使用 openstack 命令创建内网（网络名称为 inner）、内网子网（网络名称为 inner-sub），设置内网子网网段 10.0.0.0/24；

2.使用 openstack 命令创建外网（网络名称为 exter）、外网子网（网络名称为 exter-sub），设置外网子网网段 192.168.5.0/24；

3.使用 openstack 命令添加路由（名称为 router），添加内网接口；

4.使用 openstack 命令创建 test 安全组，配置规则打开 ALL ICMP 、 ALL TCP 、 ALL TCP 所有入口方向规则；

5. 使用 openstack 相关命令创建用户，命名格式为例如（姓名：

李四 用户名为 ls，以姓名首字母小写缩写构成）密码：passwd；创建项目 test；绑定 user 角色。

任务 4 OpenStack 云平台运维开发

任务描述：

通过脚本批量安装系统(以 cirros 镜像为例,默认在路径/opt/下）。

要求：

1.用脚本批量创建主机；

2.用脚本批量关闭启动主机；

3.用脚本批量禁用主机安全端口。

模块 C 操作系统网络服务配置

分值：100 分

竞赛时间：120 分钟

项目背景

工程师们，在完成全公司各地办公场所网络综合布线及私有云平台搭建基础上，为提升公司信息网络的整体功效，加强 IT 系统运维管理服务能力。需要设计全网运维架构，公司总部、武汉办

事处、上海分公司网络管理均已进入日常运维。

请根据下文提供的资料和数据,在规定的时间内完成具体任务。

任务 1：系统配置与优化

任务描述：

对 Linux 系统进行网络配置和系统优化，为部署应用程序和中间件做准备。

要求：

1.修改/etc/sysconfig/network-scripts/ifcfg-ens192 网卡配置文件，配置信息为：网关 10.5.5.2，IP 静态地址 10.5.5.10，ONBOOT 设置为 yes，NETMASK 为 255.255.255.0，DNS2 地址设置为 8.8.8.8。(注释：docker 容器中不需要启动网卡)。

2.系统内核优化：请完成以下 13 点内核优化参数，并将参数写入到/etc/sysctl.conf 文件（只配置不需要生效）

（1）NAT 开启 IP 转发支持；

（2）开启 SYN Cookies。（注释：当出现 SYN 等待队列溢出时，启用 cookies 来处理，可防范少量 SYN 攻击，默认为 0，表示关闭，1 表示开启，）；

（3）请开启 TIME-WAIT sockets 重新用于新的 TCP 连接，（默认为 0，表示关闭，1 表示开启）；

（4）开启 TCP 连接中 TIME-WAIT sockets 的快速回收，（默认为 0，表示关闭,1 表示开启）；

（5）FIN-WAIT-2 状态的世界设置为 30s（表示如果套接字由本端要求关闭，这个参数决定了它保持在 FIN-WAIT-2 状态的时间。默认是 60s）；

（6）TCP 发送 keepalive 消息的频度设置为 20 分钟。（表示当 keepalive 起用的时候，TCP 发送 keepalive 消息的频度。缺省是 2 小时）；

（7）外连接的端口范围改为 1024 到 65000。（表示用于向外连接的端口范围。缺省情况下很小：32768 到 61000）；

（8）SYN 队列的长度设置为 8192。（表示 SYN 队列的长度，默认为 1024，增加长度可以容纳更多等待连接的网络连接数。）；

（9）系统同时保持 TIME_WAIT 套接字的最大数量 5000。（表示系统同时保持 TIME_WAIT 套接字的最大数量，如果超过这个数字，TIME_WAIT 套接字将立刻被清除并打印警告信息。默认为 180000）；

（10）关闭 ipv6；

（11）表示每个网络接口接收数据包的速率比内核处理这些包的速率快时，允许送到队列的数据包的最大数目修改为 262144；

（12）请将内核放弃建立连接之前发送 SYNACK 包的数量，设置为 1；

（13）请将内核放弃建立连接之前发送 SYN 包的数量，设置 2。

3.修改/etc/security/limits.conf 文件 将 root 用户句柄数限制设置为 30000。

任务 2：项目实施

任务描述：

在优化过的 Linux 服务器中，安装部署应用程序与中间件，避免网络漏洞入侵要求对安装的 MySQL、Nginx、Redis 安全配置以及参数优化，数据库备份和过期数据清理等。

要求：

注意：系统应用部署程序安装包所在路径/data/package

1. 创建 /data/service/ 目录，安装 jdk，安装目录为 /data/service/jdk 并配置系统环境变量；

2.部署 MySQL：在服务器上部署 MySQL，使用二进制安装方式安装 MySQL，安装目录为 /usr/local/mysql，数据库目录为：/usr/local/mysql/data，登陆并修改 root 密码为：qwe123456，创建账号:jz,jz 账号密码为:qwe123456,创建应用数据库 mock_db，初始化数据，授权 jz 账号对数据库 mock_db 读写权限，导入数据文件 mock_db.sql，创建定任务每天凌晨 1 点全库备份数据库，创建数据库清理脚本并加入定时任务数据备份文件保留 20 天；

3.部署 Redis:服务器上部署 Redis,使用编译安装方式安装 redis，

安装目录为/data/service/redis，修改配置文件：添加密码认证登录,密码：qweiodks569PK。启动并检查是否正常；

4.Java 应用部署：根据提供的 java 应用程序文件，在/data/service/下启动 Java 应用程序、端口；

5.Nginx 服务器搭建：yum 方式部署 Nginx，启动，创建虚拟机配置静态资源目录为 /data/service/nginx/html ，并将/data/package/dist/目录里面的静态资源放入里面。

任务 3：自动化预警

任务描述：

在 Linux 系统部署 Prometheus 监控,对已经运行的应用程序和中间件配置告警规则。

资料：

mysql 默认密码 qwe123456

要求：

1.部署监控服务

使用 /data/package/ 下的 alertmanager-0.24.0.linux-amd64.tar.gz 、node_exporter-1.3.1.linux-amd64.tar.gz 、

prometheus-2.36.2.linux-amd64.tar.gz 安装包搭建 promethues 监控服务

prometheus 安装目录为：/data/service/prometheus

alertmanager 安装目录为：/data/service/alertmanager

node_exporter 安装目录为：/data/service/node_exporter

mysqld_exporter 安装目录为：/data/service/mysqld_exporter

redis_exporter 安装目录为：/data/service/redis_exporter

nginx-vts-exporter 安装目录为：/data/service/nginx-vts-exporter

2.配置报警规则

（1）CPU 使用率达到 80%报警；

（2）内存使用率 80%报警；

（3）磁盘使用率 80%报警；

（4）节点状态；

（5）mysql 存活状态；

（6）redis 存活状态；

（7）nginx 存活状态；

（8）java 应用程序存活状态。

模块 D 网络安全管理

分值：100 分

竞赛时间：180 分钟

项目背景：

工程师们，公司总部、上海分公司以及武汉办事处的网络管理工作均已进入正常运行。

为保障全公司网络链路和设备等网络安全、各种应用系统的信息安全，需要按照国家有关标准制定网络安全实施方案并进行演练，做好网络安全日常监控、预警、处置，根据产生问题的重要程度进行合理加固，提升网络安全突发事件响应能力。

请根据下文提供的资料和数据，在规定的时间内完成具体任务。

任务 1：部署与配置安全设备

任务描述：

确保主机安全，包括账号安全、IP 协议安全和 IPTABLE 配置等。同时根据系统部署并配置相应的防护策略，确保网络配置安全。

要求：

任务 1.1. 主机安全加固

（1）设置密码策略最短密码长度不少于 16 个字符，并将该操作必须使用的参数及参数值作为 Flag 值提交；

（2）设置密码策略必须同时满足大小写字母、数字特殊字符；

（3）密码策略，设置口令定期修改的周期为 30 天，将该操作使用命令中必须要使用的参数及参数值作为 Flag 值提交；

（4）登录策略，设置一分钟内仅允许 3 次登录失败，超过 3 次，登录帐号锁定 1 分钟，并将该操作使用命令必须要使用的参数及参数值作为 Flag 值提交；

（5）设定 bash 历史命令条数，为 5 条，并将该操作使用的命令作为 Flag 值提交；

（6）IPTABLES 设置 Linux 系统禁止别人 ping 通，并将命令作为 flag 值提交；

（7）IPTABLES Linux 设置禁用 23 端口，并将命令作为 flag 值提交；

（8）设置防火墙允许本机转发除 ICMP 协议以外的所有数据包，并将命令作为 flag 值提交。

任务 1.2.配置网络安全防护

（1）防火墙位于企业 Internet 出口，请在防火墙上可以指定规则,允许内网 10.1.1.0/24 网段的 PC 访问 Internet,禁止 Internet 用户访问 IP 地址为 192.168.1.2 的内网主机；

（2）企业内有一台服务器，允许 IP 网段为 10.2.1.0/24 的办公区访问此服务器，配置了安全策略 policy1。运行一段时间后，又要求禁止两台临时办公 PC（10.2.1.1、10.2.1.2）访问服务器；

（3）经常需要远程管理某一个系统内的内网设备，而这些内网设

备又没法直接远程登录，请使用防火墙的 SSL VPN 功能配置完成；

（4）因公司无法访问公网，请给防火墙配置 nat 策略，实现内网用户访问互联网。

任务 2：检测网络安全漏洞

任务描述：

检测网络安全漏洞，包括主机扫描与信息收集、数据分析数字取证、Web 安全应用、渗透测试。

要求：

任务 2.1.主机扫描与信息收集

服务 IP：172.17.224.2

（1）使用 Nmap 工具对靶机场景服务进行 TCP 同步全连接扫描，并将该操作显示结果中从下往上数第 2 行的服务器信息作为 Flag 值提交；

（2）使用 Nmap 工具对设有防火墙禁止 ping 的靶机场服务扫描，将该操作使用的命令中必须要使用的参数作为 Flag 值提交；

（3）使用 Nmap 工具对设有防火墙禁止 ping 的靶机场服务扫描，并将该操作显示结果中的数据库服务信息作为 Flag 值提交；

（4）使用 Nmap 工具探测靶机服务版本信息进行扫描，并将该操作显示结果中从下往上数第 3 行的服务的版本信息作为 Flag 值提

交；

（5)使用 Nmap 工具对靶机场景进行 UDP 扫描渗透测试只扫描 53，111 端口，并将该操作显示结果中 111 端口的状态信息作为 Flag 值提交；

（6）使用 Nmap 工具对靶机场景进行 RPC 扫描渗透测试,并将该操作使用命令中必须要使用的参数作为 Flag 值提交；

（7）使用 Nmap 工具对靶机场景进行 RPC 扫描渗透测试,并将该操作显示结果中从下往上数第 3 行的服务信息作为 Flag 值提交；

（8）使用 Nmap 工具对靶机场景进行服务及版本扫描,并将该操作显示结果中 445 端口对应的服务状态信息作为 flag 值提交；

（9）使用工具 Nmap 对靶机进行系统服务及版本扫描渗透测试，以 xml 格式向指定文件 test.xml 输出信息，将以 xml 格式向指定文件输出信息必须要使用的参数作为 Flag 值提交；

（10）在渗透测试平台中，使用命令初始化 MSF 数据库并将此命令作为 Flag 值提交；

（11）在渗透测试平台中，打开 MSF，使用 db_import 将扫描结果导入到数据库中，并查看导入的数据，将查看该数据要使用的命令作为 Flag 值提交。

任务 2.2.数据分析数字取证

数据包地址：/headless/Desktop/hack.pcapng

（1）使用 Wireshark 查看并分析 hack.pcapng 数据包文件，通过

分析数据包 hack.pcapng 找出首次用户恶意构造的 sqlpayload 语句，该语句证明 sql 注入的存在。将恶意用户的 payload 语句作 Flag 值提交；

（2）使用 Wireshark 查看并分析 hack.pcapn 数据包文件，通过分析数据包 hack.pcapn 在黑客爆破数据名的 sql 语句,将 payload 语句中数据表的完整名字，作为 Flag 值提交；

（3）使用 Wireshark 查看并分析 hack.pcapn 数据包文件，通过分析数据包 hack.pcapn 在黑客爆破数据表的 sql 语句,将 payload 语句中数据表的十六进制的值，作为 Flag 值提交；

（4）使用 Wireshark 查看并分析 hack.pcapn 数据包文件，通过分析数据包 hack.pcapn 在黑客爆破数据表结构的 sql 语句，将 payload 语句中数据表、列相关的十六进制的值，作为 Flag 值提交；

（5）使用 Wireshark 查看并分析 hack.pcapn 数据包文件，通过分析数据包 hack.pcapn 在黑客获取到的系统的账号内容，将账号的用户名、密码作为 Flag 值提交；

（6）使用 Wireshark 查看并分析 hack.pcapn 数据包文件，通过分析数据包 hack.pcapn 在黑客在系统上传木马文件，将木马文件的内容作为 Flag 值提交；

（7）使用 Wireshark 查看并分析 hack.pcapn 数据包文件，通过分析数据包 hack.pcapn 在黑客在通过木马文件执行的内容，将 root 的全部内容为 Flag 值提交。

任务 2.3. Web 安全渗透测试:

服务器场景用户名、密码：未知

HTTP 服务地址:http://172.17.224.2:8080/JSPClassNewsSystem

(1)访问 HTTP 服务地址，通过构造 sql 注入点，构造命令执行，获取系统使用数据库名称，将数据库名称作为 Flag 值提交；例如[数据库名];

(2)访问 HTTP 服务地址，通过构造 sql 注入点，构造命令执行，获取并统计数据库使用表格数量，将统计的表格数量作为 Flag 值提交；例如[6];

(3)访问 HTTP 服务地址，通过构造 sql 注入点，构造命令执行，获取并统计数据库中的表，将表名作为 Flag 值提交；例如[表 1;表 2];

(4)访问 HTTP 服务地址，通过构造 sql 注入点，构造命令执行，获取并统计用户表中字段,将字段名称作为 Flag 值提交;例如[字段 1;字段 2;字段 3];

(5)通过渗透机访问靶机的 HTTP 服务，通过构造 sql 注入点，构造命令执行，获取 admin 用户的密码，将密码作为 Flag 值提交。例如[密码];

(6)通过渗透机访问靶机的 HTTP 服务，通过构造 sql 注入点，构造命令执行，获取 zledu 用户的密码，将密码作为 Flag 值提交。例如[密码]。

任务 3：部署云网络安全防护

任务描述：

完成企业云上资源及常见攻击的防御策略，完成 SQL 注入、XSS 跨站，webshell 上传、命令注入、后门隔离等。

要求：

1.客户 www.test.com 网站被注入漏洞并篡改页面，请使用云 Web 应用防火墙，结合 DNS 解析的配置，帮助网站屏蔽网页漏洞以及篡改的攻击，避免造成经济上的损失；

2.服务器 80 端口是用来提供 web 服务，如果服务器部署了网站，而没有开放 80 端口，这个网站肯定访问不了，请配置规则，使 80 端口开放；

3.某些黑客对业务系统 www.test.com 进行 DDoS 攻击，导致 服务器频繁瘫痪，业务无法正常运作，造成巨大损失。请接入 DDoS 降低网络风险，减少企业损失；

4.客户网站要升级，考虑到数据安全，请通过云数据库做全量份，并且配置使数据备份保留 30 天，备份周期为 1 周。

2023

金砖国家职业技能大赛
（金砖国家未来技能挑战赛）

金砖职赛微信号