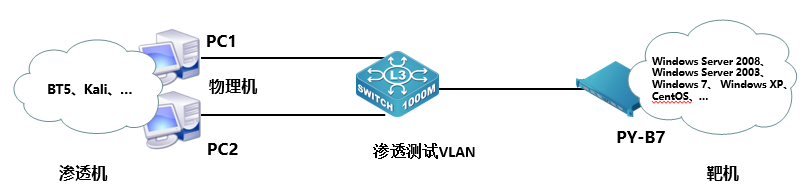
# 2021年河北省职业院校技能大赛（高职）网络安全赛项样题

# 一、竞赛阶段简介

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **竞赛阶段** | **任务阶段** | **竞赛任务** | **竞赛时间** | **分值** |
| 第一阶段 |  | 基础设置和安全强化 | 60分钟 | 300 |
| 第二阶段  单兵模式系统渗透测试 | 任务1 | 根据赛题确定任务 | 120分钟 | 100 |
| 任务2 | 根据赛题确定任务 | 100 |
| 任务3 | 根据赛题确定任务 | 200 |
| 第三阶段  分组对抗 | 系统加固：15分钟 | | 60分钟 | 300 |
| 渗透测试：45分钟 | |

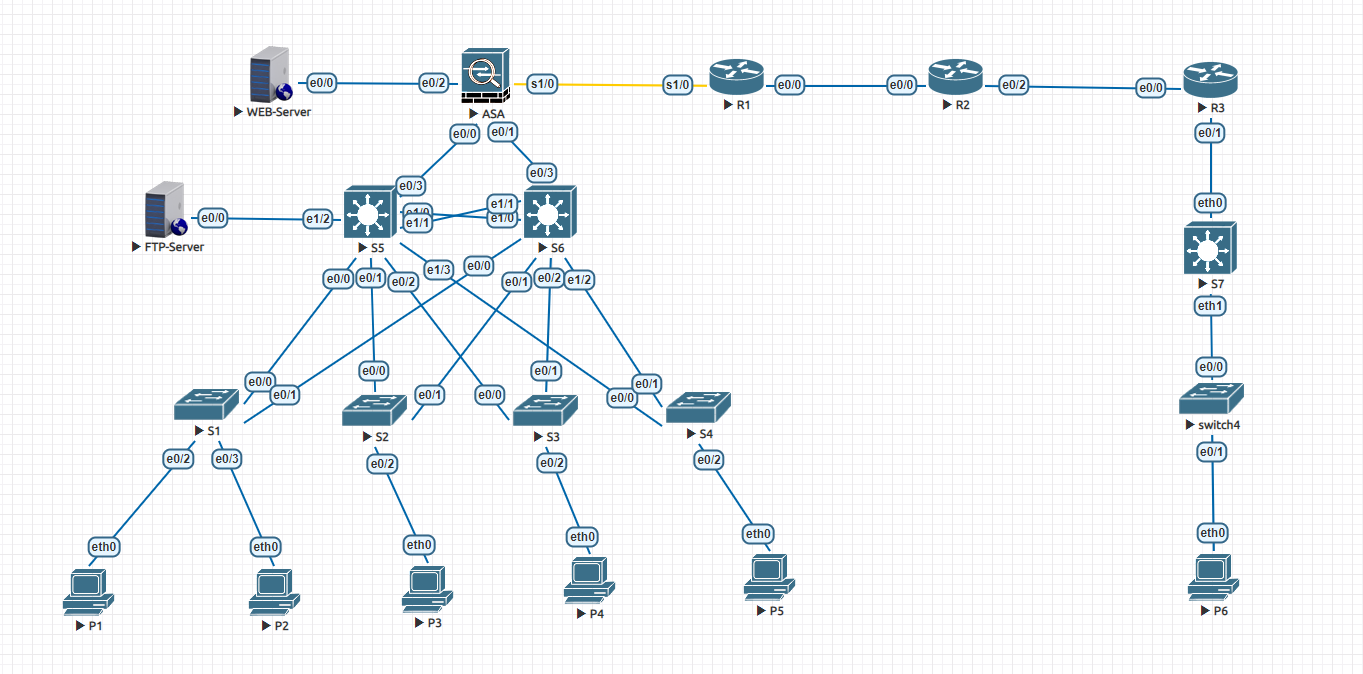
# 二、拓扑图



# 三、竞赛任务书

## （一）第一阶段任务书（300分）

根据拓扑图和下述题义要求，完成相应配置填写答题卡。



1、某公司分为总部和分部，总部分为ABCD四个区域，如图所示，S1、S2、S3、S4为接入层交换机，S5、S6为汇聚层交换机；为了方便对总公司网络的管理，减少广播风暴的影响，部门ABCD分别设置为VLAN 10、VLAN 20、VLAN 30、VLAN 40，限制不必要的vlan通过。（30分）

2、配置S5作为DHCP服务器为VLAN20内用户提供服务。（30分）

3、汇聚层要求使用VRRP技术进行网关冗余。（30分）

4、核心层和汇聚层使用OSPF传递路由，实现校园网内的互联互通。（30分）

5、防火墙FW1作为公司内网的出口网关，在核心层防火墙划分安全区域。（30分）

6、在防火墙FW1指定安全策略对网络进行访问控制，Server0作为公司内部ftp服务器，可以供公司内部访问，但外网无法访问。（30分）

7、Server1作为总公司内部www服务器，要求内外网均可访问。（30分）

8、核心层防火墙使用PAT技术实现公司内部可以访问Internet。（30分）

9、总公司内部出口网关设备R1与分公司出口网关设备R3之间配置GRE VPN保证私网之间的互通。（30）

10、通过配置实现全网互通。（30分）

## （一）第二阶段任务书（400分）

### 任务一：Web安全渗透测试

任务环境说明：

服务器场景：server1

服务器场景用户名、密码：未知（关闭链接）

1.通过URL访问http://靶机IP/1，对该页面进行渗透测试,将完成后返回的结果内容作为flag值提交；

2.通过URL访问http://靶机IP/2，对该页面进行渗透测试,将完成后返回的结果内容作为flag值提交；

3.通过URL访问http://靶机IP/3，对该页面进行渗透测试,将完成后返回的结果内容作为flag值提交；

4.通过URL访问http://靶机IP/4，对该页面进行渗透测试,将完成后返回的结果内容作为flag值提交；

5.通过URL访问http://靶机IP/5，对该页面进行渗透测试,将完成后返回的结果内容作为flag值提交。

### 任务二：数据分析

\*任务说明：仅能获取Server2的IP地址

1.使用Wireshark查看并分析Server2桌面下的capture.pcapng数据包文件，找出telnet服务器的用户名和密码，并将密码作为flag值提交；

2.使用Wireshark查看并分析Server2桌面下的capture.pcapng数据包文件，FTP服务器已经传输文件结束，将登陆服务器后的第一条指令作为flag值提交；

3.使用Wireshark查看并分析Server2桌面下的capture.pcapng数据包文件，web服务器地址是192.168.181.250， 其使用的脚本语言为php，将服务器使用php的版本号作为flag值提交；

4.使用Wireshark查看并分析Server2桌面下的capture.pcapng数据包文件，这些数据中有非常多的ICMP报文，其中有一个设备是路由器，IP地址为192.168.181.25，将路由器上主动发出的ping请求的数量作为flag值提交；

5.使用Wireshark查看并分析Server2桌面下的capture.pcapng数据包文件，这些数据中有ssh报文，由于ssh有加密功能，现需要将这些加密报文的算法分析出来，将ssh客户端支持的第一个算法的名称作为flag值提交。

任务三：数字取证

\*任务说明：仅能获取Server3的IP地址

1.黑客是通过上传页面进行上传木马，将上传页面找到，上传页面文件名作为flag值提交；

2.找到对应的木马后门，将木马文件名作为flag值提交；

3.查看木马文件，将木马文件的登录密码进行提交；

4.在任务计划中找到黑客所创建的任务计划（具有危险操作的任务计划），任务计划名为flag值提交；

5.找到任务计划所对应执行程序将分析代码将密码处作为flag值提交。

### 任务四：Web渗透测试

\*任务说明：仅能获取Server4的IP地址

1.获取PHP的版本号作为flag值提交；（例如：5.2.14）

2.获取MySQL数据库的版本号作为flag值提交；（例如：5.0.22）

3.获取系统的内核版本号作为flag值提交；（例如：2.6.18）

4.获取网站后台管理员admin用户的密码作为flag值提交；

5.找到/root目录中的txt文件，将文件内容作为flag值提交。

## （三）第二阶段任务书（300分）

各位选手是某公司的系统安全管理员，负责服务器（受保护服务器IP、管理员账号见现场发放的参数表）的维护，该服务器可能存在着各种问题和漏洞（见漏洞列表）。你需要尽快对服务器进行加固，十五分钟之后将会有很多黑客对这台服务器进行攻击。

提示：服务器中的漏洞可能是常规漏洞也可能是系统漏洞；需要加固常规漏洞；并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。

十五分钟之后，各位选手将真正进入分组对抗环节。

**注意事项：**

注意1：任何时候不能人为关闭服务器常用服务端口（21、22、23、80），否则将判令停止比赛，第二阶段分数为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，第二阶段分数为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，第二阶段分数为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。

在渗透测试环节里，各位选手需要继续保护你的服务器免受各类黑客的攻击，你可以继续加固你的服务器，你也可以选择攻击其他组的保护服务器。

漏洞列表如下：

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。

7. 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。