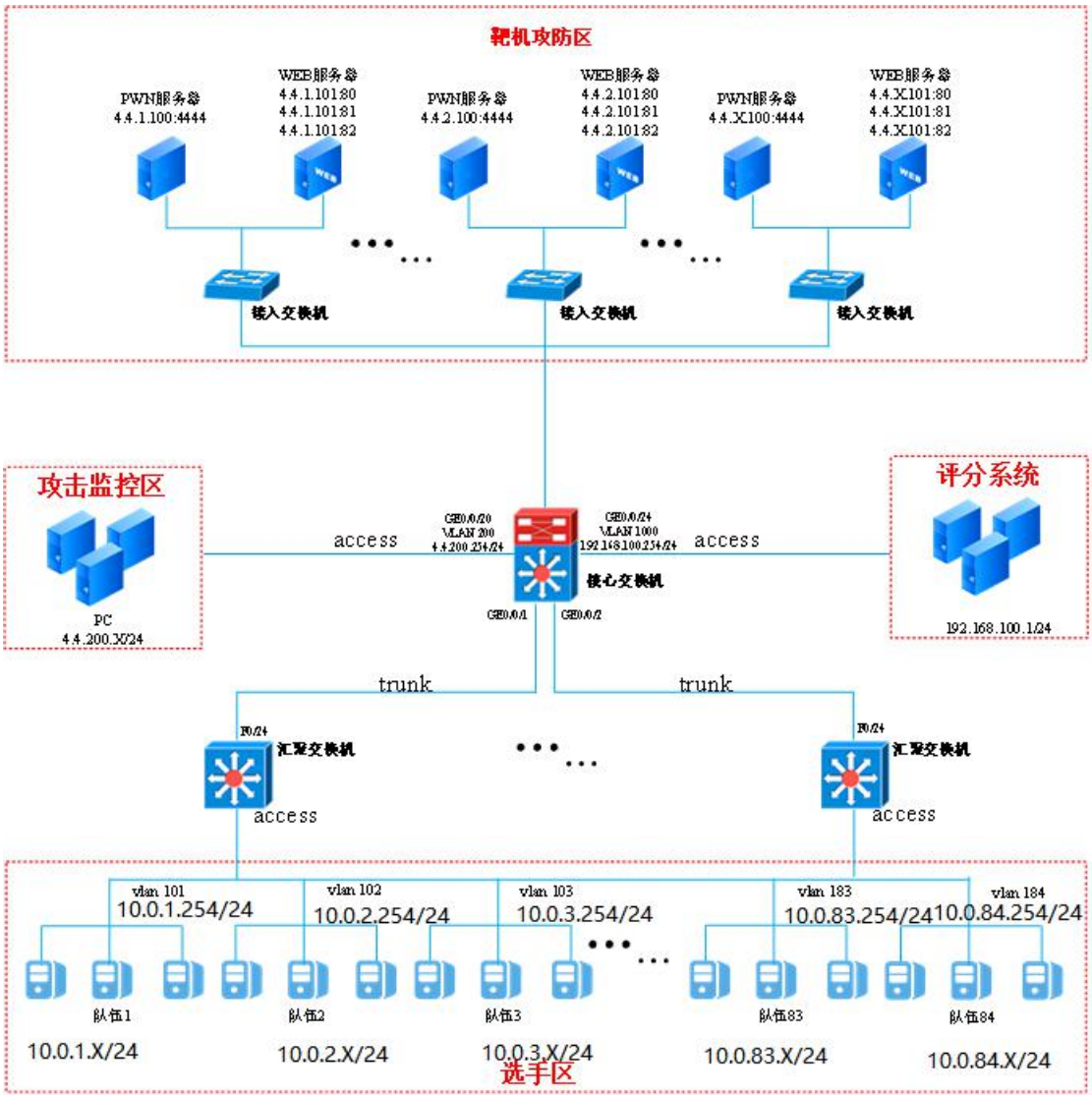
第三届“蓝帽杯”全国大学生网络安全技能·总决赛竞赛规则

（一）赛制和时长

竞赛为混战模式，3 人为 1 队。每个队伍环境靶机 2 个，一个靶机为 PWN 考察点，一个靶机含有多个 web 考察点，每 20 分钟为 1 阶段，共 9 个阶段，第 1 阶段为准备及加固阶段，第 2 至第 9 阶段为渗透混战阶段。比赛总时长为 3 小时。

1、物理拓扑



攻防对抗混战比赛环境部署示意

2、配置说明

1）队伍 A、B、C 的 IP 地址分别为 10.0.1.X、10.0.2.X、10.0.3.X…，

掩码为 255.255.255.0，网关为分别为 10.0.1.254、10.0.2.254……、10.0.X.254.。每个队伍有 2 个防守机，防守机分别部署 pwn 类型、web 类型漏洞考察点，3 个 web 服务对应端口 80、81、82.pwn 类型靶机服务端口为 4444,2 台靶机都为 linux 服务器,ssh 连接端口为 22,防守队伍可通过 xshell 等工具远程连接防守机进行加固。Flag 机为 192.168.100.1。

2)获得 flag 的方式为,拿下其他队伍的防守机的 shell 权限,执行 curl http://192.168.100.1/Getkey.

3）攻击范围:4.4.1.100/101-4.4.x.100/101 之间。x 为队伍数量。

4）准备阶段无法对其他选手的靶机进行访问，但可对自己的靶机进行操作。

5）比赛过程中若发现任何问题，请示意裁判组，由裁判组进行解答。

（二）竞赛规则

1、参赛选手于比赛正式开始前凭有效证件签到。

2、比赛正式开始后迟到 30 分钟者不得进入比赛场地。

3、竞赛期间参赛选手不得随意离开竞赛工位。

4、参赛选手自带笔记本电脑（自带 RJ45 网口或 USB-RJ45 转接头）、资料(包括书籍、电子资料)及移动存储工具。

5、比赛过程中发现问题，应当示意裁判组，由裁判组进行解答。

6、比赛过程中不允许任何参数选手携带通讯设备，需统一上交进行管理，不允许任何人通过任何形式进行上网。

7、参赛队伍必须保证防守机持续正常运行，保持特定服务或端口处于持续正常服务状态，对漏洞的修复不得影响服务的正常功能。

8、禁止任何对比赛相关平台的暴力破解和攻击，禁止对本平台进行重放数据包攻击，限制频率为 10 次/1 秒，禁止 DDOS、ARP 等干扰比赛正常进行的攻击，禁止任何针对参赛对手的网络攻击行为，违规者一律取消参赛资格并进行公示。

9、除参赛选手及大赛赛场工作人员外，其余人员一律不得进入赛场。

10、禁止进行限制其他队伍攻击己方防守机的配置，或者限制访问 FLAG 服务器（例如，修改防守机到 FLAG 服务器的路由等），违规者一律取消参赛

资格并进行公示。

11、比赛过程中不能相互交流，禁止参赛队伍之间分享任何解题思路及 FLAG，违规者一律取消参赛资格并进行公示。

12、比赛中裁判有可能抽查获取得分点的方法，如果发现回答有误，疑似非法渠道获取答案的，取消其该项得分，严重者取消比赛资格并进行公示。

13、公平起见，只有当没有任何参赛队伍解出某题的时候，裁判组才可能发放相关提示，解题提示信息请关注竞赛公告。

14、竞赛结束（或提前完成）后，参赛选手不得进行任何操作。

15、比赛过程中，请服从和配合裁判和现场工作人员的相关安排。

16、如有其它违规行为，组委会及裁判组将酌情进行相应的处罚措施。

17、其他事项由组委会裁判组在比赛前一天进行公告及通知。

（三）注意事项

- 竞赛组委会为每个队伍分配一个账号，比赛当天下发，队伍通过账号密码进入比赛系统，以团队形式进行比赛，可以多个人共用一个账号，所有得分均以团队形式呈现，成绩会进行实时排名。
- 比赛开始之后，第一阶段为准备加固阶段，不得对其他参赛队伍、比赛平台进行任何攻击行为。
- 参赛队伍请自备至少三台笔记本电脑用于答题，并确保笔记本能正常使用网线，推荐安装 Chrome 浏览器的最新版，版本号高于 64；
- 请团队提前准备渗透工具及防守技术文档；
- 一旦团队的竞赛主机环境出现异常，请举手示意竞赛现场人员，由工作人员进行问题排查和解决；
- 请各参赛队伍严格遵守比赛规章制度，不要进行违规操作，一经发现，将会严格按照比赛规则进行处理；

（四）攻防对抗赛评分规则

攻防对抗题总得分=初始分值+攻击得分-被攻击失分-服务异常扣分-重置防守机扣分

1、攻防对抗题初始分值为 8000 分。

2、参赛队伍攻击其他队伍防守机并获得权限后，可访问平台 flag 生成地址

（curl http://192.168.100.1/Getkey）获得 flag。

3、比赛每 20 分钟为一个阶段，同一阶段内只能提交同一队伍的 flag1 次。

4、flag 有效期为 60s，获取后尽快提交。

5、flag 提交成功后，渗透成功 1 个靶机得分 5 分，2 个靶机得分 10 分。

6、check 机制定时对所有防守机进行探测，探测业务可用性，服务可用性。每轮次比赛，最多扣 400 分（防守机任意应用服务异常，则触发扣分机制，比赛平台答题页面会实时提醒防守机异常状态）

7、参赛队伍可请求裁判重置本方防守机，每重置一个虚拟机，扣除 50 分（注意：重置后，之前所有的加固策略及攻击方的后门皆失效，所以防守机恢复到初始状态）。