网安学院 2021 级分级通关第四级操作说明

1 课程简介

1.1 课程目标和任务

网络安全综合实践分级通关第四级场景包括系统渗透测试训练和网络安全攻防对抗实践。具体课程内容包括 CTF 实训和 CTF 比赛以及 AWD 分组对抗，课程目标是锻炼同学们运用安全攻防技术进行综合分析和解决网络安全问题的能力。

课程第一阶段任务需要每个同学独立完成，主要内容有两项：第一项是针对 CTF 进行专题训练，学生攻克专题内的靶机或题目，解出 flag；第二项是参与 CTF 比赛。

课程第二阶段任务：学生们自由选择组成小组，班级内两个人一组，最后剩余的单数可以跨班级组队，分组进行 AWD 攻防对抗，对自己小组内靶机进行安全防护，防止其他小组进行攻击；同时可以攻击其他小组的靶机，拿到靶机内 flag，获得攻击分数。

1.2 成绩计算方法

第一周总共有四次课程，学院分级通关实训平台会开放四个时间段做 CTF 专题训练，分别对应周二（6.11）晚上 WEB 攻防靶机，周四（6.13）晚上逆向题目，周六（6.15）下午密码题目，周六（6.15）晚上限时开放学生补做前面三次的题目。周日（6.16）下午开放一次 AWD 模拟练手。第二周的周一（6.17）晚上杂项题目，周二（6.18）晚上 CTF 比赛，周四（6.20）晚上和周六（6.22）下午 AWD 分组对抗比赛。周六（6.22）晚上限时开放补做杂项题目、CTF 比赛题目。AWD 分组对抗比赛不提供补做的机会。

WEB、逆向、密码、杂项四个专题，每个专题 5 个题目，总计 20 个题目。每个题目提供 flag 成功得到 2 分，最高得 40 分。如果在课程开放时间内，没有攻破靶机或题目，可以把攻击的具体结题思路和过程写下来，在平台提交，指导老师会根据学生提交的结题思路和过程适当给与一定的分数。

CTF 比赛共计 10 分。按照个人得分占总体分的比例进行归一化处理计算个人 CTF 比赛总分，最高得分为 10 分。

分组 AWD 对抗成绩攻击 30 分。具体每个小组得分会根据最终 AWD 分组对抗平台的计分综合分布情况，进行统一归一化处理，最高可得 30 分。

每个同学最后都需要提交一份课程报告，报告内容包括描述攻 CTF 专题训练解题过程、参加 CTF 比赛解题情况和过程以及参加小组 AWD 对抗的具体工作内容以及相关思政题目。课程报告总计 20 分。

1.3 指导老师

各班指导教师情况说明，网安专业 2021 级：汤学明（202101 班）、骆婷（202102 班）、路松峰（202103 班）、崔永泉（202104 班）。

信安专业 2021 级:王美珍(202101 班)、鲁宏伟(202102 班)、陈凯(202103 班)、董枫（202104 班）。

2 具体操作过程

2.1 登录平台

浏览器访问学院分级通关实训平台：https://222.20.126.111/login，用户名和密码与其他分级通关平台内课程一致，如下图 2.1 所示。

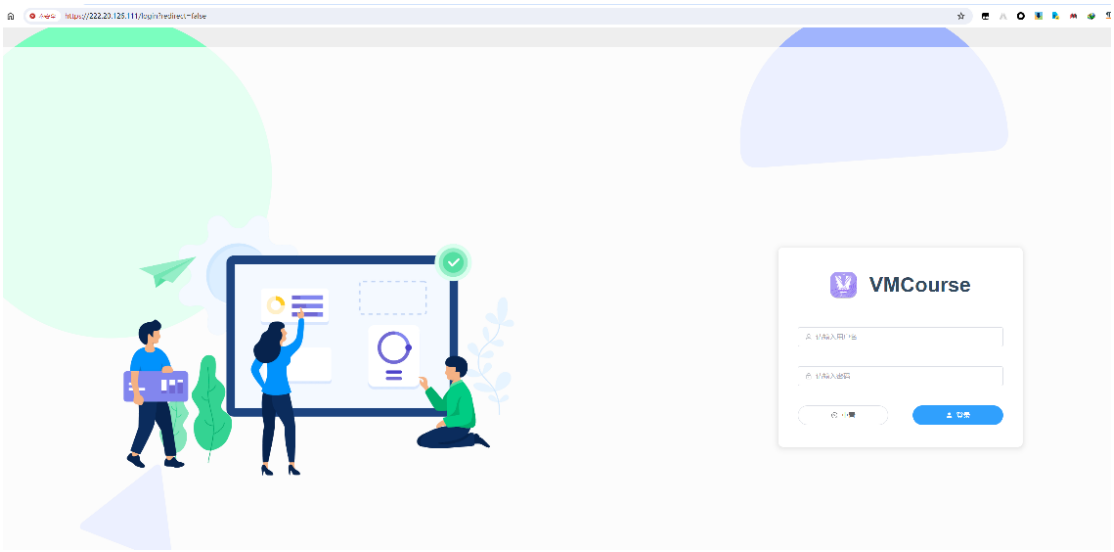

图 2.1 学院分级通关实训平台登录页面

2.2 下载内容

登录平台成功后，选择我的课程，进入“2024 年春季-CTF 实训”课程。如图 2.2 所示。

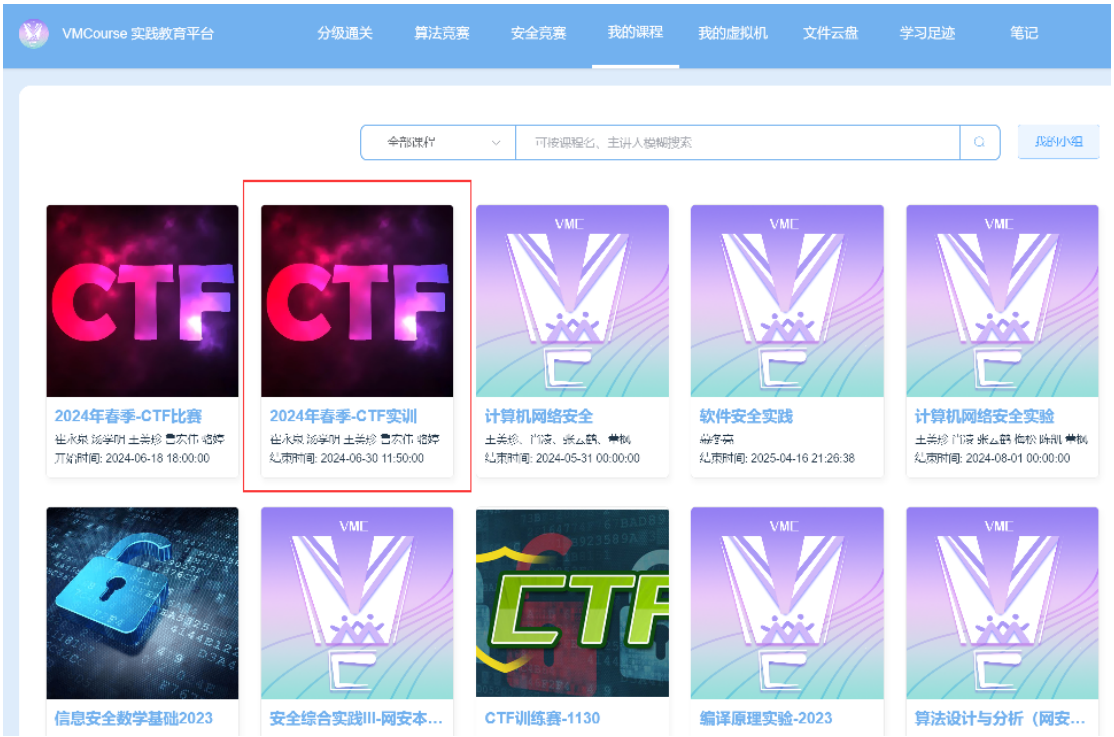

图 2.2 “2024 年春季-CTF 实训”课程页面

点击进入该课程，显示课程详细信息，如图 2.3 所示。

图 2.3 “2024 年春季-CTF 实训”课程资源页面

点击开始学习，可以看到课程资源具体内容，如图 2.4 所示。在左侧栏目中选择“分级通关第四级 vpn 及配置.zip”，右面页面内会显示下载链接，点击“下载”操作可以下载压缩包。

图 2.4 课程资源下载页面

压缩包“分级通关第四级 vpn 及配置.zip”还可以在 2021 级信息安全数据基础 QQ 群内或学院分级通关教学平台公有云盘中下载。

2.3 安装 vpn 并建立连接

解压以后得到安装文件 openvpn-install-2.4.8-I601-Win10，其他版本的 openvpn 同学们可以自行在网上下载、安装。

安装以后，将配置文件 vmcourse.ovpn 拷贝到安装目录的 config 目录下，以管理员权限启动 openvpn，在桌面右下角系统托盘内会出现 openvpn 图标，用鼠标右键点击“openvpn 图标”，出现 openvpn 菜单，选择“vmcourse”选项，在右边选择“连接”功能（如图 2.5），开启 openvpn 连接。**无需用户名和密码。连接成功后，将成功建立一个 10.8.x.x 的虚拟网络。**

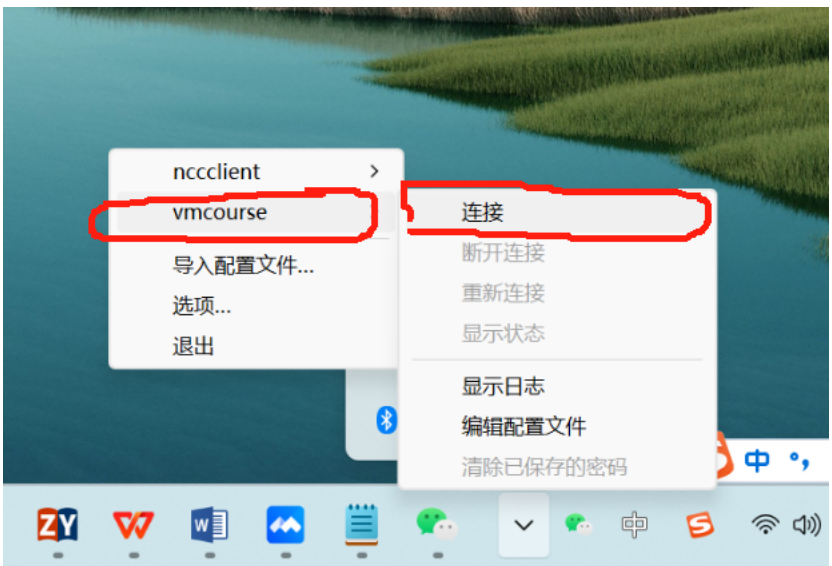

图 2.5 开启 openvpn 连接

3.获取任务

3.1 CTF 实训

登录进入学院分级通关实训平台，如图 3.1 所示，选择“我的课程”页面的“2024 年春季-CTF 实训”课程。

图 3.1 选择“我的课程”的 2024 年春季-CTF 实训课程

可以看到该课程下的所有章节，除了“0.课程资源”以外，其他每个章节下面是一道 CTF 题目，点击章节右侧的开始学习按钮，进入学习页面，该页面提供相应题目的学习资料（**注：当未到题目作答时间时按钮无法点击**）。

图 3.2 课程章节

点击开始学习按钮，进入学习资料页面。

图 3.3 开始学习页面

点击每个章节的习题按钮即可进入 CTF 题目作答页面。

举例说明，如图 3.4 所示，选择第一题“Web-SQL 注入漏洞”，点击“习题”，会看到靶机的具体内容（**注：当未到题目作答时间时按钮无法点击**）。

图 3.4 选择“Web-SQL 注入漏洞”题目

如图 3.5 所示，点击左侧红色的“靶机”图标，显示靶机对应的具体 docker 信息，初始靶机状态是“尚未申请”。

图 3.5 “Web-SQL 注入漏洞”靶机的 docker 环境

点击“申请”按钮，会启动 docker 环境，鼠标在“端口映射+2”功能界面上停留，系统会提示 docker 启动成功以后，对外提供服务的 IP 和端口信息，如图 3.6 所示。（**注：CTF 题目中的 22 端口仅用于管理员生成 Flag 使用，题目位于 80 端口**）

图 3.6 “Web-SQL 注入漏洞”靶机的 IP 和端口信息

在图中展示的 ip：10.12.153.8，开放 80 端口信息：30314。可以在正常浏览器中访问 http://10.12.153.8:30314 服务，靶机展示的 web 服务页面如图 3.7 所示。

图 3.7 “Web-SQL 注入漏洞”靶机提供的 web 服务

剩余的操作就是，想办法攻破靶机的 web 服务，获取 flag。然后提交 flag 获取对应的分数。点击左侧提交图标，出现提交 flag 的界面，flag 格式是 vmc 开头，后面大括号内***一长串 flag 值，如图 3.8 所示。（注：容器题目中的 Flag

为动态生成，每次启动容器 Flag 都不相同）

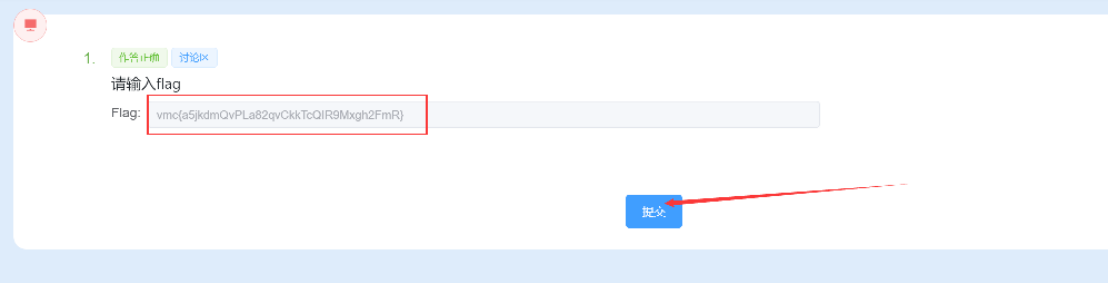

图 3.8 提交 flag 页面

对于非靶机题目（即不需要申请 docker 容器），只需在课程章节页面点击开始学习，如图 3.9，图 3.10 所示，进入学习资料页面，下载题目附件在本机解题即可（后面专题的题目将会陆续加入）。

图 3.9 非靶机题目

图 3.10 开始学习页面

解出题目后，点击相应题目的习题按钮提交 Flag，如图 3.11 所示。

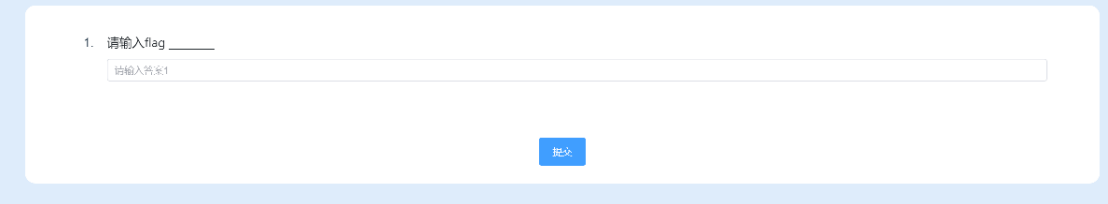

图 3.11 提交静态 Flag 页面

3.2 CTF 比赛

CTF 比赛形式与 CTF 实训类似，主要区别是课程内的题目不同，待 CTF 比赛课程开始后，点击我的课程，进入“2024 年春季-CTF 比赛”课程即可开始比赛。

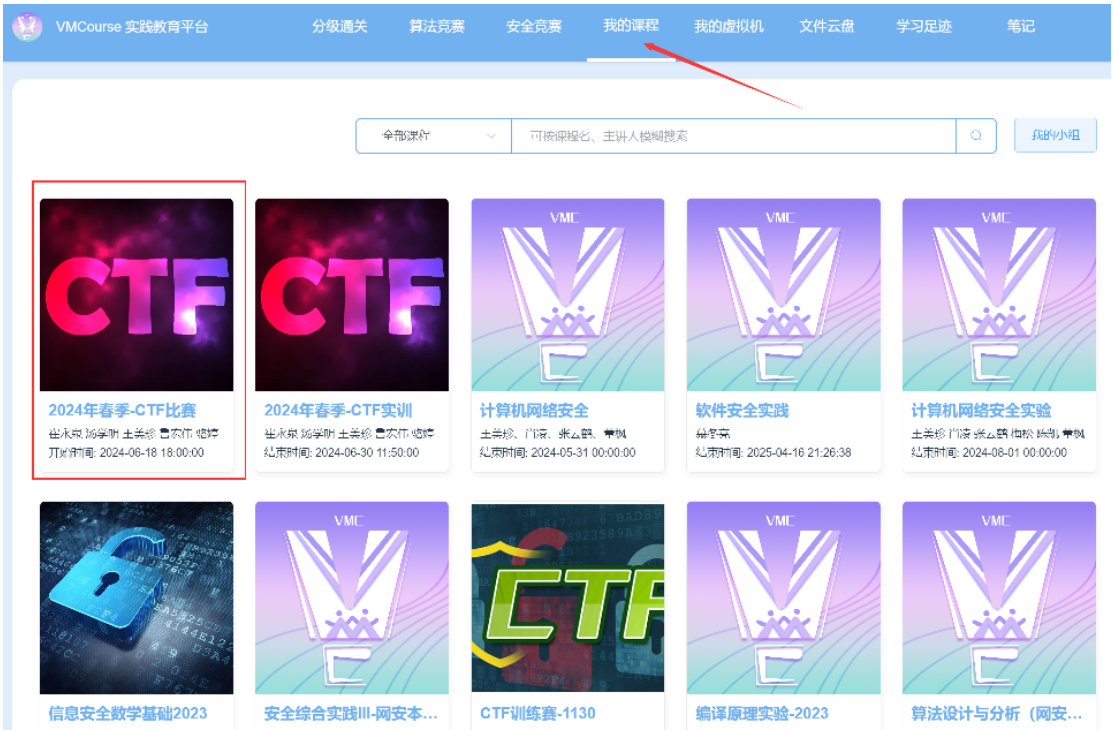

图 3.12 2024 年春季-CTF 比赛页面

3.3 AWD 攻防对抗任务

AWD 任务需要以小组为单位完成的实验场景，需要按照要求进行组队操作。

3.3.1 AWD 赛制介绍

AWD 比赛中每个队伍维护一台（或多台）靶机服务器，靶机中存在若干漏洞，利用漏洞攻击其他队伍的靶机可以进行得分，修复漏洞可以避免被其他队伍攻击失分。

AWD 任务需要以小组为单位完成的实验场景，需要按照要求进行组队操作。回到初始登录平台页面，点击“安全竞赛”(图 3.13)，找到属于 2024 年春季-AWD 模拟专用的 AWD 竞赛（**赛题一和赛题二将于上课时间开放**）。点击 AWD 模拟专用，输入密码 2024 即可进入。

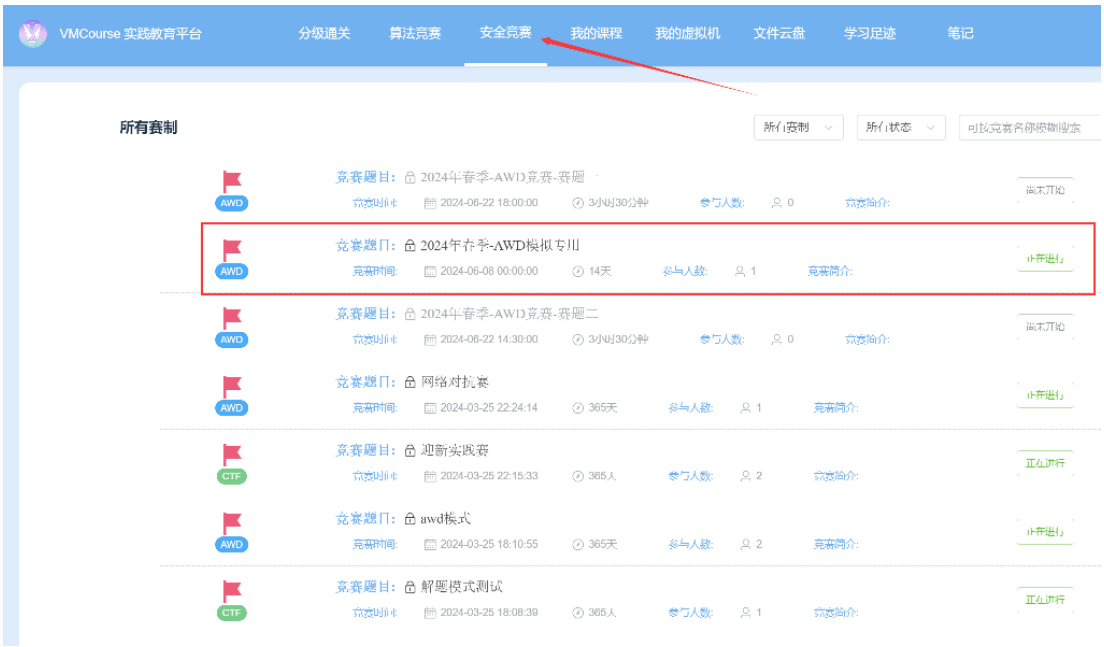

图 3.13 安全竞赛

图 3.14 竞赛页面

进入竞赛页面，点击页面右下角的创建小组按钮，即可创建该比赛的队伍；创建小队后可邀请同学加入小队，通过小队信息可查看已创建、已加入小组的详细信息。

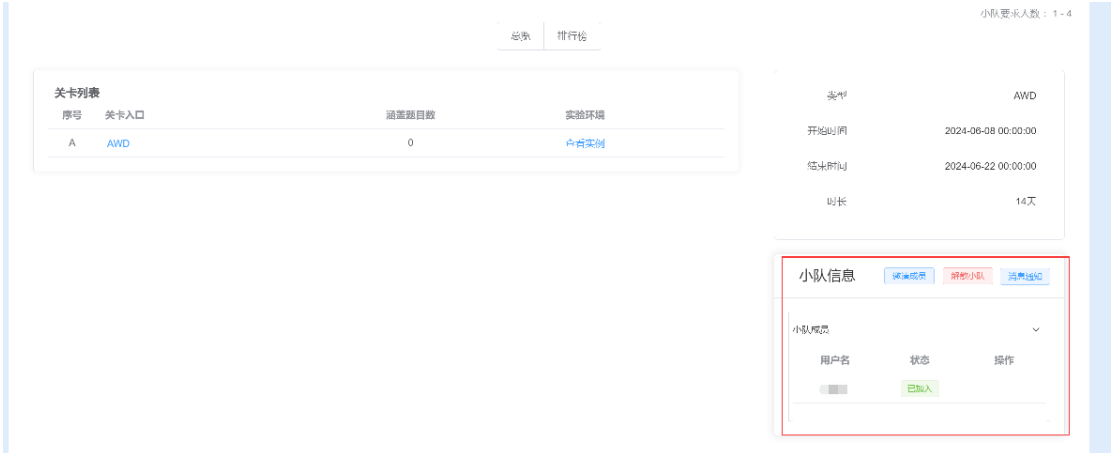

图 3.15 组队功能

对于自己创建的小组，可以进行邀请同学、踢出成员、解散小组等操作；对

于自己加入的小组，则可以选择退出小组。

点击邀请成员按钮，弹出成员邀请界面，可通过**学号、姓名**搜索同学并发送组队邀请。如图 3.16 所示。

图 3.16 邀请成员页面

点击页面上的**消息通知**按钮，可以查看其它小组向自己发送的组队邀请，并选择接受/拒绝邀请。如图 3.17 所示。

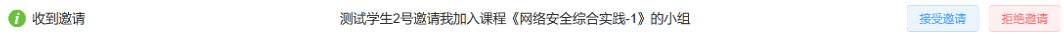

图 3.17 邀请消息通知

1. 比赛积分规则

每个队伍可以申请 1 台靶机服务器，总分 20000 分，被攻陷扣除 50 分，宕机扣除 50 分。采用零和积分制。

2. 攻击得分

在该轮中成功攻击该靶机的所有队伍，一起平分该靶机扣分时失去的的分数。得分加到各自相应题目的靶机上。

例如：John 攻击了 Alice 的 Web1 靶机；Mashiro 攻击了 Alice 的 Web1 靶机。则 Alice 的 Web1 靶机 -50 分。John 和 Mashiro 各自的 Web1 靶机平分这减去的 50 分。即 John 和 Mashiro 每队 +25 分。此时全部队伍的加分与扣分之和，依然为零。

3. 宕机失分

被比赛平台的 Check 功能检测到**服务宕机（不能正常对外提供服务）**的靶机，将减去 50 分。在该轮中题目服务正常的靶机，平分该题目下，所有宕机靶机失去的分数。

例如：John、Alice、Mashiro 的 Pwn2 靶机被检测判定为服务宕机，Asuna、Emiria 的 Pwn2 靶机一直服务正常。则 John、Alice、Mashiro 的 Pwn2 靶机各 -50 分。Asuna 和 Emiria 的队伍平分这减去的 150 分。即 Asuna 和 Emiria 每队各 +75 分。此时全部队伍的加分与扣分之和，依然为零。

3.3.2 参加比赛

1. AWD 竞赛中，每个关卡都是一个攻防场景。请首先按照竞赛人数要求，邀

请您的队友并创建队伍。完成队伍的组建之后，每个队伍可以申请相应题目的一台靶机，队伍中所有人都可以获取该靶机的 SSH 账号密码并连接。如图 3.18 所示。

图 3.18 队伍实例列表

2. 比赛分成若干轮，**每轮时长 30 分钟**。每一轮各队伍都可以发起攻击，挖掘其它队伍靶机中的网络服务漏洞，并利用漏洞攻击对手服务以挖掘 Flag 并提交 Flag 得分，如图 3.19 所示，但一台靶机在一轮中只会被攻陷一次（即被攻陷最多只会被扣一次分）。

图 3.19 提交 Flag 和排行榜入口

3. 平台每轮会对相应的靶机进行服务 Check，宕机的靶机将会扣除相应分数。

4. 每一轮结束时，结算上一轮各队伍得失分数，并更新排行榜，**同时平台将更新各队伍靶机的 Flag**。

5. 新的一轮开始后，上一轮被攻陷的靶机如果没有防护，本轮仍然可以被攻击。

3.3.3 比赛排名

比赛进行中可以在排行榜中查看各个队伍的实时分数和排名，如图 3.20 所示。

图 3.20 排行榜页面

3.3.4 比赛违规操作

违反以下规则一旦被系统检测到，将视同为“宕机”，具体规则包括但不限于下列各个方面：

（1）修改应用程序导致 WEB 服务不能正常服务；

（2）修改或者删除机器中设置的 Flag 文件或者记录，或者恶意阻止平台对 Flag 更新，妨碍比赛公平性；

（3）恶意消耗宿主机磁盘空间导致系统故障。