AWD竞赛规则介绍

比赛积分规则

每个队伍可以申请1台Web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。每一轮分数将在下一轮开始时更新。

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。

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。

如果出现既被攻击又出现宕机的情况，分数按照前序情况计算，即攻击的50分被攻击队伍平分，宕机的50分被服务正常的队伍平分，也即**一个回合每个队伍的每个靶机最多被扣除两次分数**

比赛注意事项

加固阶段

因平台限制，本学期AWD竞赛没有设置加固时间，竞赛开始即可开始攻击。

攻击阶段

尽量以获取flag为目的，禁止对其他队伍的靶机执行破坏性操作，包括但不限于删除网站源码，删除数据库等（俗称删站，删库）。

防护阶段

防护阶段与攻击阶段同步，这里主要说明一下防护操作。AWD靶机提供的ctf账户只对/var/www/html和/tmp有可读可写可执行权限，禁止使用通用防御（WAF），当然权限也不够，可以自己编写小型的waf，文件监控脚本之类进行一定程度的防护。

比赛违规操作

违反以下规则一旦被检测到，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服务不能正常对外提供服务，包括但不限于直接关闭服务，删除网站源码，删除数据库等；

（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；

（4）以任意方式提权至root权限。

（5）对其他队伍的靶机执行破坏性操作，包括但不限于删除网站源码，删除数据库等

Q&A

Q：有哪些文件可以修改，允许安装哪些软件？

A：原则上来说所有的文件都可以修改，但有几个前提：

- 有权限，AWD靶机提供的ctf账户只对部分文件和文件夹有操作权限；
- 保证靶机可以对外提供服务；
- 不违反比赛规则，包括违规操作中提到的；
- 攻击其他队伍靶机时，不得进行破坏性操作，如删站，删库等
- 不允许安装通用防御，如ModSecurity等。

Q：有哪些攻击方式是允许的？哪些不允许？

A：常规的渗透测试中的攻击手段都可以使用，但是不允许进行社工、钓鱼，同时不允许进行任何形式的DoS攻击。

AWD入门指南（供参考

AWD入门指南