记第一次举办CTF比赛

原创

sjtu_jzh 于 2018-08-30 17:23:15 发布 1834 收藏 3

文章标签： 信息安全 CTF

本文链接：https://blog.csdn.net/sjtu_jzh/article/details/82224899

本次CTF竞赛所使用的平台是Facebook发布的开源CTF平台FBCTF。用户通过浏览器访问FBCTF平台，FBCTF平台支持用户注册、题目装载、积分统计、发布公告等基本功能，配置了优秀的UI和易用的后台；平台也具有高度的可拓展性，用户可以根据自己的需求去自定义游戏流程、规则、代码等等；平台支持数据的导入和导出；平台配置过程简易，并且配备了完整的用户社区，用户可以在社区中和开发者进行有效的互动。

在配置的过程中有两个问题需要留意。一、待配置的ubuntu版本号需与FBCTF支持的ubuntu版本号统一。二、在安装过程中，终端需要从一些外部网站下载数据，请配置socks5、http和https代理，否则安装无法顺利完成。

默认配置下存在测验、夺旗、基地（攻防）三种游戏模式，用户只需要修改文件就可以定制个性化的游戏模式。题目支持挂载网页链接和附件。基地模式下仅有FBCTF平台提供的默认计分代码，用户需要根据实际需求进行相应修改。

本次CTF比赛的攻防战流程如下。主办方给每三支队伍提供了一台预留了漏洞（CVE-2017-16995）的靶机。每支队伍在开始时仅有靶机普通用户的权限，参赛人员需要利用漏洞实现权限提升，随后将自己队伍的名字填入仅有root用户才能修改的文件中并通过修补漏洞等防御手段来保持文件不被修改。配置了FBCTF的主机通过远程访问来检查文件中的名字，并且周期性地给相应队伍加分。

为了保持良好的网络通信环境，请使用有线网络。为了保证比赛顺利进行，请给靶机和配置了FBCTF的主机划出足够多的资源，本次比赛中给靶机和主机都划出了16G内存和单核CPU。

当前版本的FBCTF仅支持Ubuntu 16.04LTS。源码地址：https://github.com/facebook/fbctf

Ok上面都是写给别人的书面语言，用自己的话总结一下吧。

前期学习

学习平台主要使用实验吧 http://www.shiyanbar.com/ ，每道题几乎都有比较详细的write up，非常良心。如果觉得write up不是很明白或者想要知道操作流程，可以看实验吧的免费ctf教学 http://www.shiyanbar.com/courses ，虽然感觉讲的有点慢，但是非常详细。我是先看完了所有教学，然后看的write up，结合一些现学的web知识还是能应付的。如果毫无基础，直接看write up，难度略高。

平台搭建

一开始用的是github下载的简易安装，但是安装的时候报了很多错，当时没管，由于是脚本跑的，所以安装到后面继续不下去了，因为很多后面的依赖包在之前都没有装好，其实报错就是那些包安装失败了。当时不懂事，一个个去找依赖包安装，于是成功陷入无限分支（装A依赖B，装B依赖C……）。Ok，后来一查应该是之前那些包没装上，原因呢，就是相应的源（是第三方源，主要就是hhvm）连不上，后来网上查了一些源作替换，没用。终于在这里，我意识到了是因为网站被墙了，需要翻墙，用已经开过会员的lantern挂socks5代理，失败；改用shadowsocks，我相信可以找到免费账号的，但是花了太多时间不想找了。

最后，网上下了一个别人已经装好的14.04的虚拟机，VMWARE打开就完事了。
见 https://blog.csdn.net/wqh1416814478/article/details/53791485

出题环节

想直接用fbctf自带的extra/score_base.py，然而按照git上的文档操作，只能显示哪个队应该得分，但是分数并没有变化（现在可能已经解决！）。于是自己写了一点python脚本，大致的意思就是读取/tmp/SCORE_POINTS里的队名，拿到数据库里找，没找到返回not_found，找到了就给相应队伍加分，并且返回当前的分数。后来弄了靶机，就写了一个shell脚本，通过scp命令把靶机中的/tmp/xxx文件发到主机的/tmp/中，文件在主机上的路径/tmp/xxx，需要用到expect。

比赛现场

上午因为用的是无线局域网，所以丢包+卡慢，ping巨高。下午遂用交换机+有线网络，很ok。

攻防赛碰到了大问题，两个靶机到后来都炸了。之前测试的时候没有任何问题，但是在实战中，当选手用guest普通用户（ssh）利用CVE-2017-16995进行权限提升之后，我用普通管员账户远程连接这个靶机成功，但是过一段时间就死机了，重启都没用，两个靶机都是这个情况。需要注意的是，从时间的角度上来看是漏洞利用弄坏了靶机？我觉得显然不是。但是背后的真正的原因现在还完全不清楚，有两个考虑，第一是给靶机的内存太少了（2G），第二是选手们在操作的时候对ssh服务进行了一些破坏。不考虑漏洞利用的问题，因为在测试的时候利用guest提权后，管员账户操作没有任何问题。非常欢迎各位大佬就这个问题进行交流，如果需要比赛当日详细信息我会在评论中提供。