No.163-HackTheBox-Linux-Writeup-Walkthrough渗透学习

原创

大余xiyou 于 2020-07-17 11:36:04 发布 229 收藏

分类专栏： Hack The box 文章标签： linux python 数据库

本文链接：https://blog.csdn.net/qq_34801745/article/details/107396783

**

HackTheBox-Linux-Writeup-Walkthrough

**

靶机地址：https://www.hackthebox.eu/home/machines/profile/192

靶机难度：初级（4.5/10）

靶机发布日期：2019年6月12日

靶机描述：

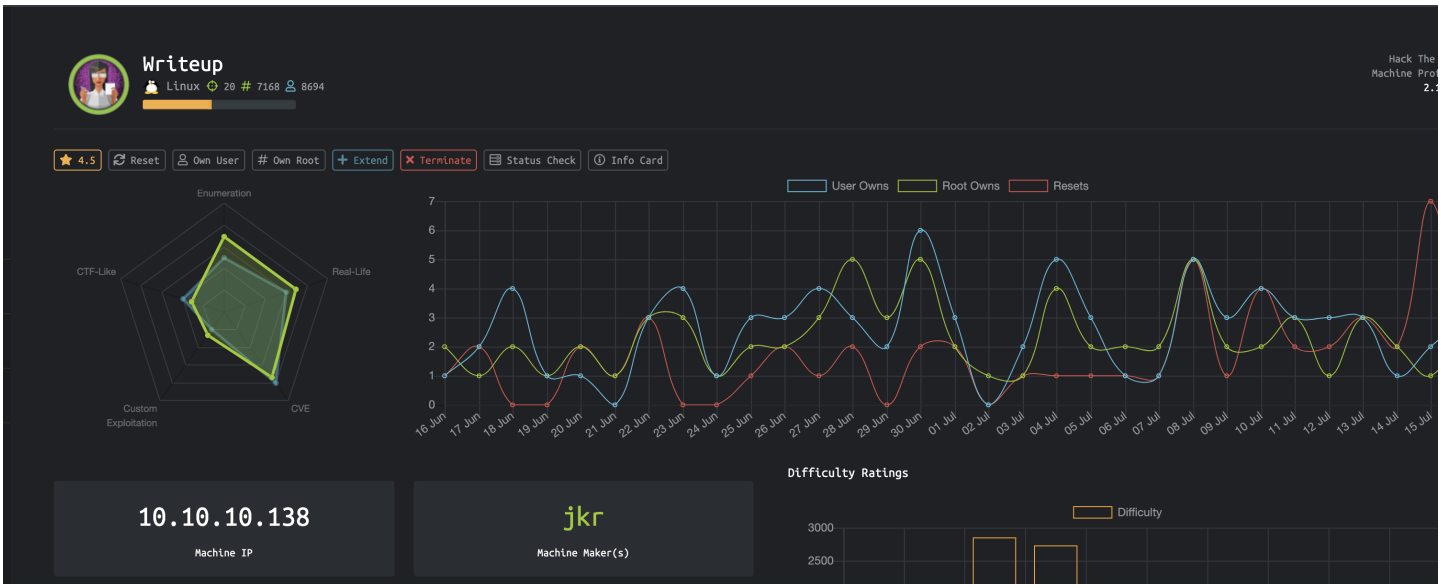
Writeup is an easy difficulty Linux box with DoS protection in place to prevent brute forcing. A CMS is found, and contains a SQL injection vulnerability, which is leveraged to gain user credentials. The user is found to be in a non-default group, which gives him write access to part of the PATH. A path hijacking results in escalation of privileges to root.

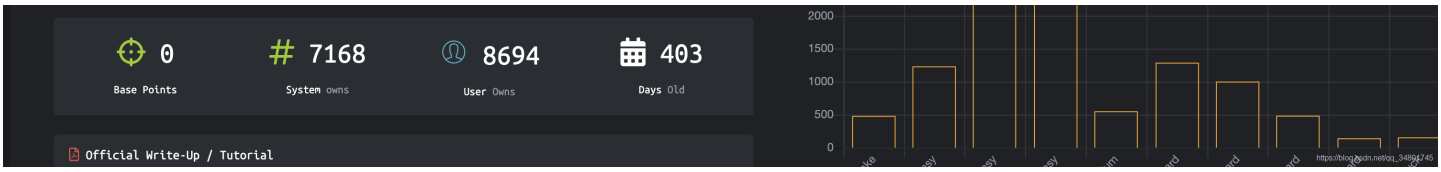
作者：大余

时间：2020-07-17

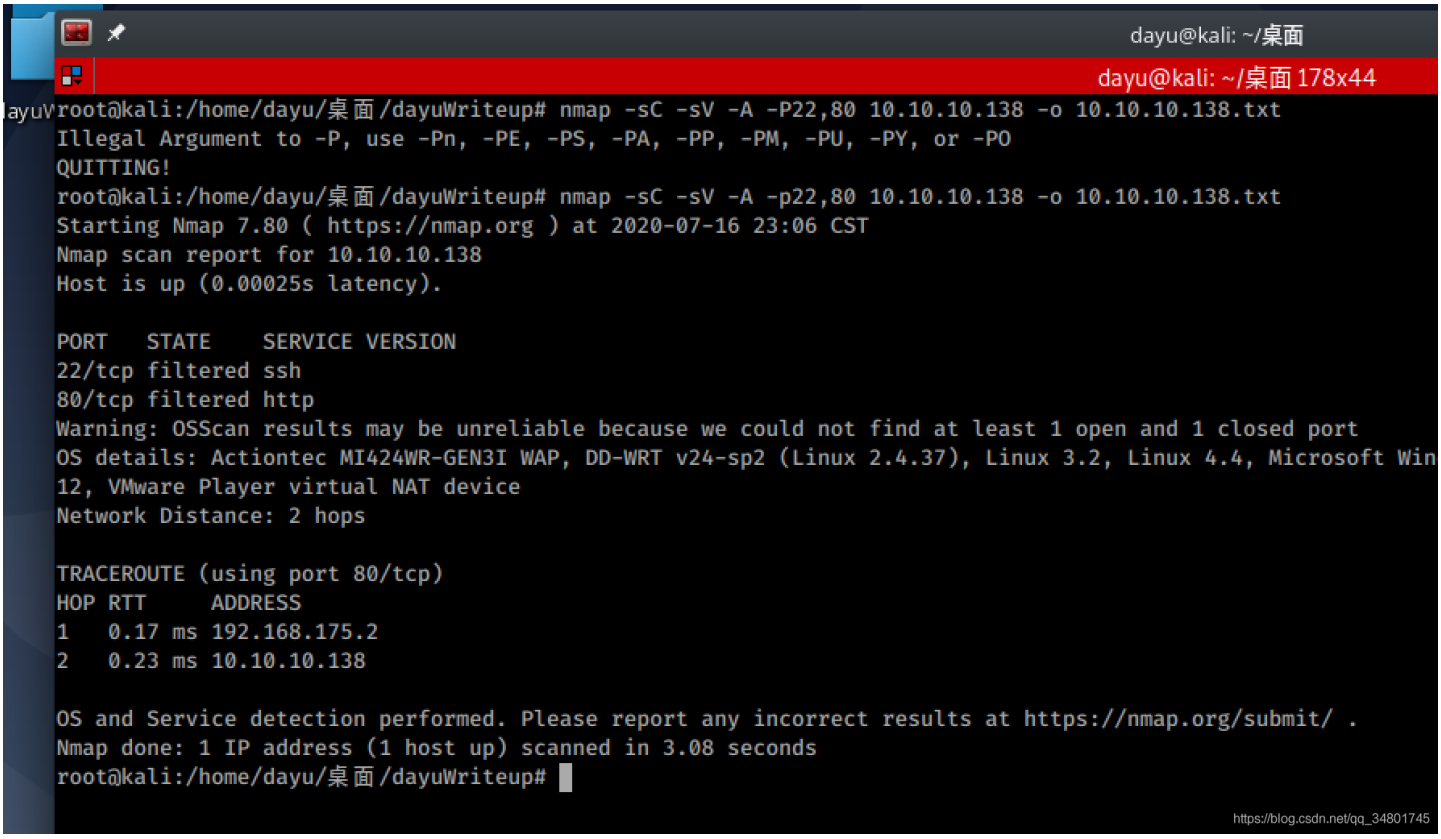
请注意：对于所有这些计算机，我是通过平台授权允许情况进行渗透的。我将使用Kali Linux作为解决该HTB的攻击者机器。这里使用的技术仅用于学习教育目的，如果列出的技术用于其他任何目标，我概不负责。

一、信息收集

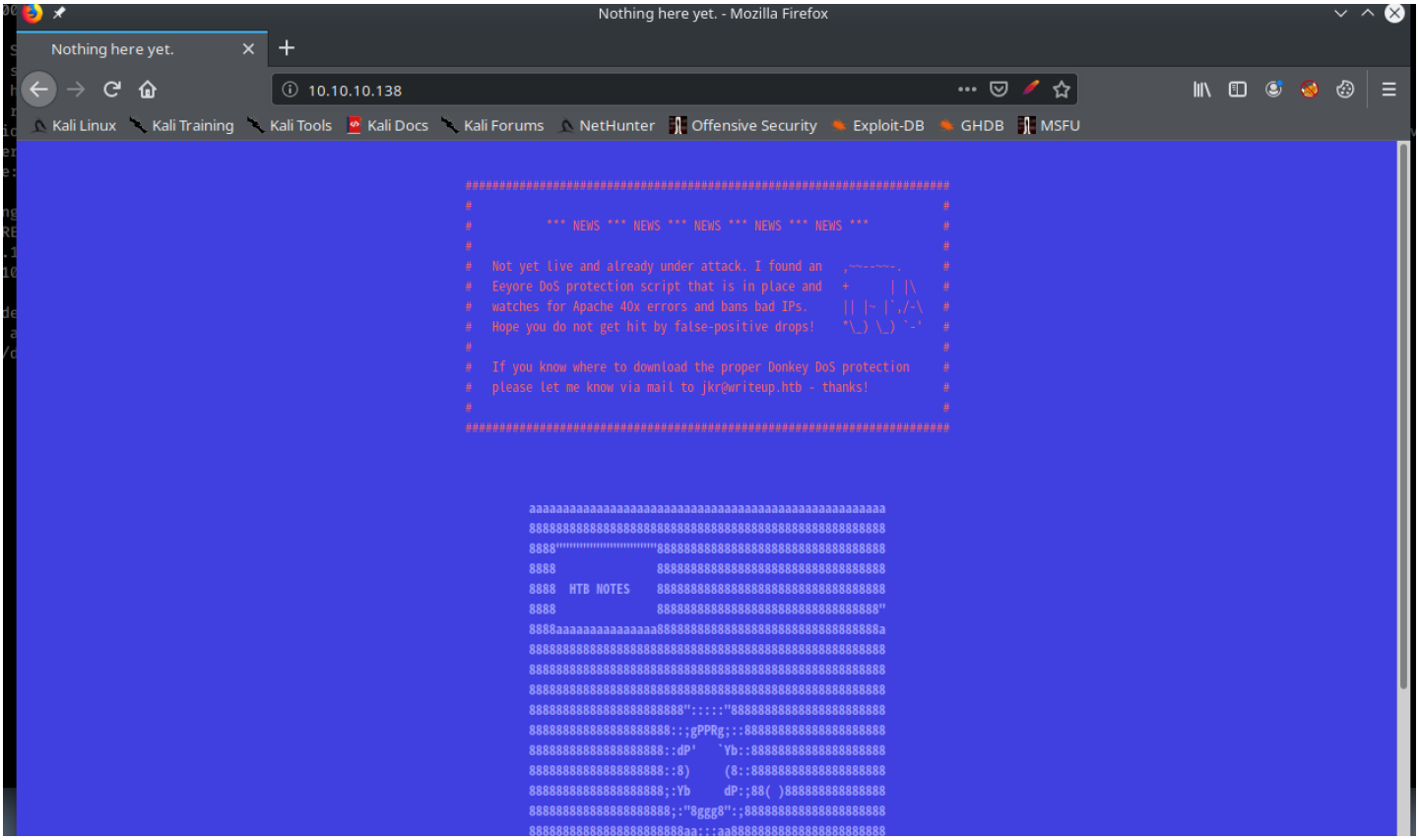


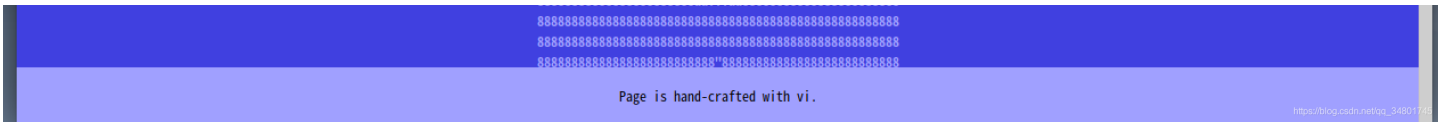


可以看到靶机的IP是10.10.10.138…

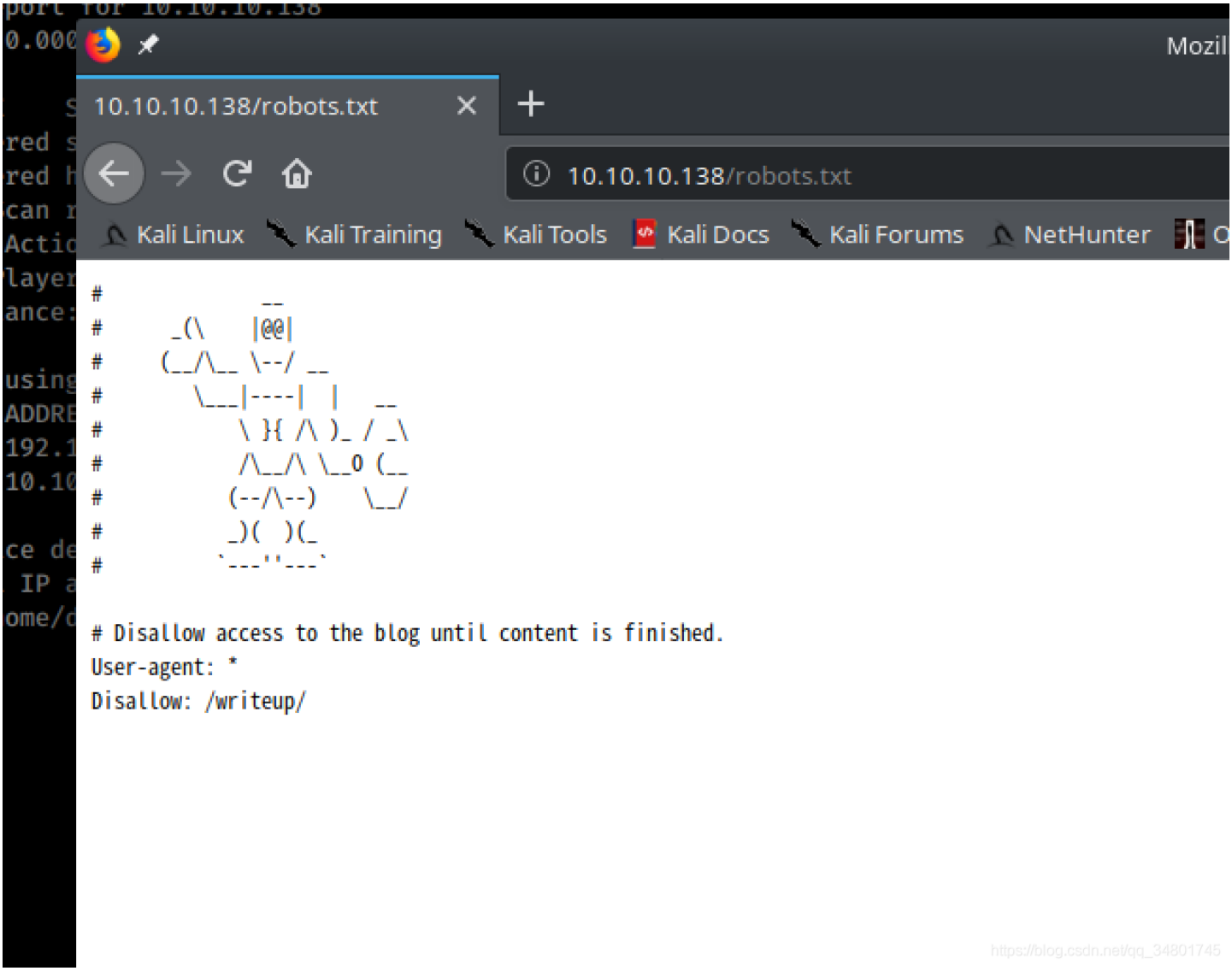


nmap发现开放了apache和SSH服务…

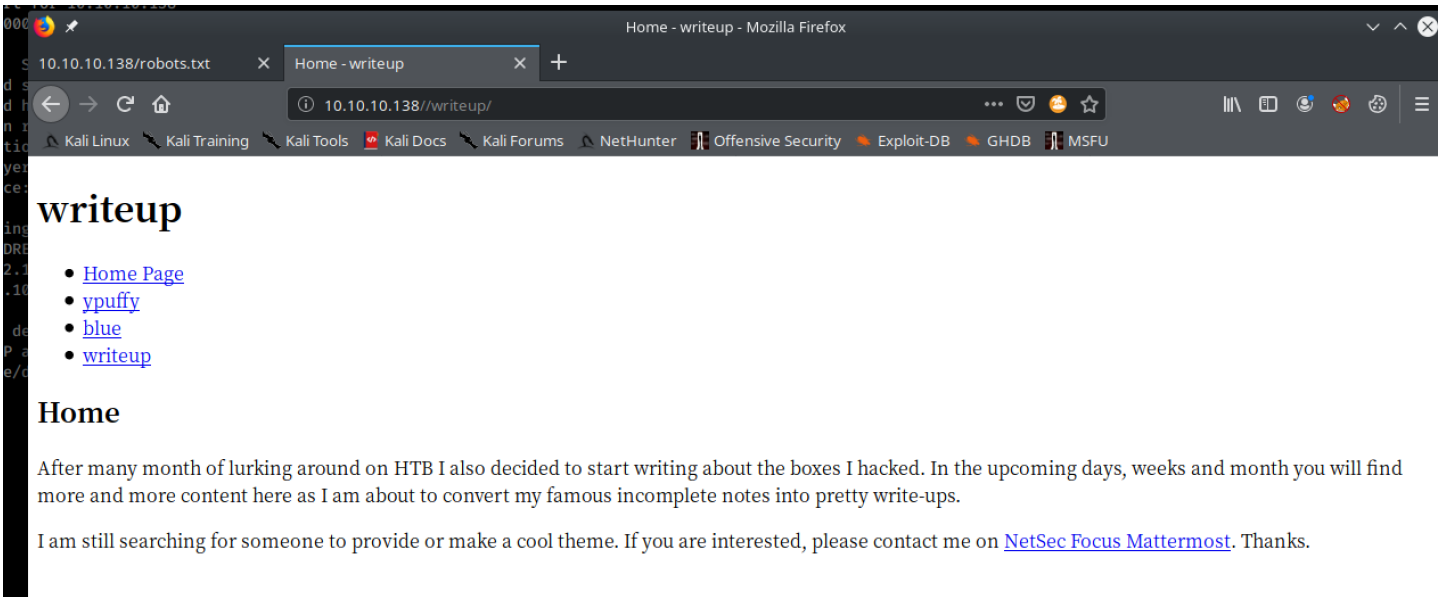




浏览到端口80，可看到一个复古风格的页面…

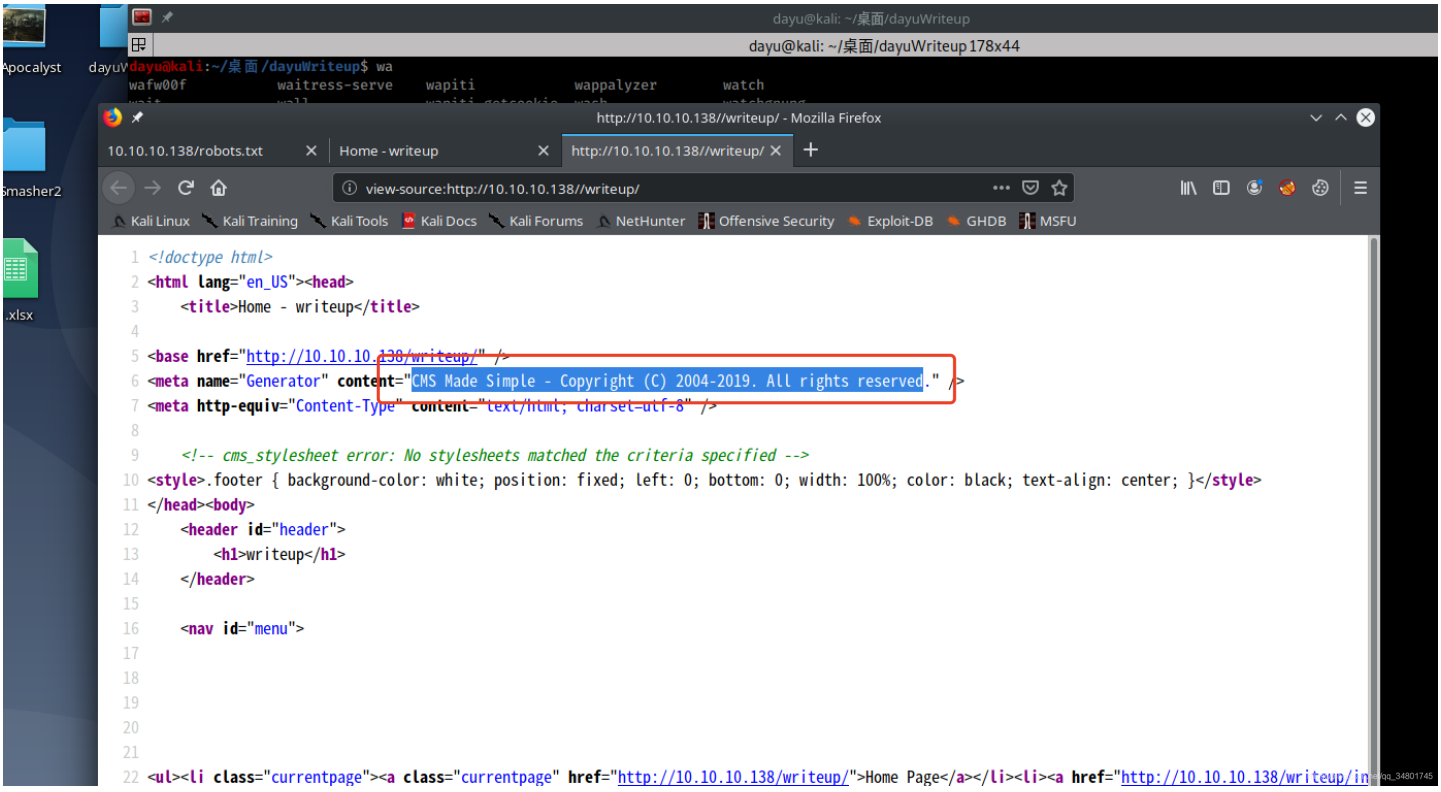


每次apache我都会查看robots文本，提示了writeup目录…

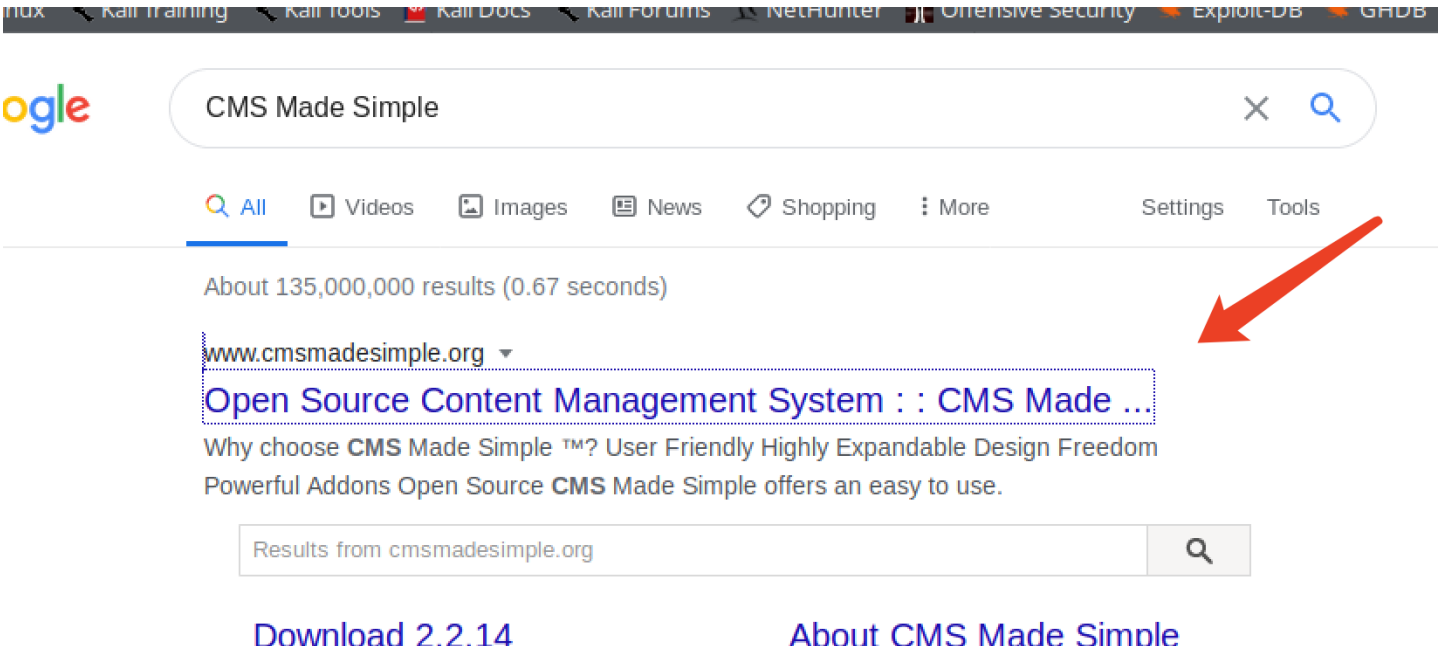


Pages are hand-crafted with vim. NOT.

进入该目录，开始枚举信息...



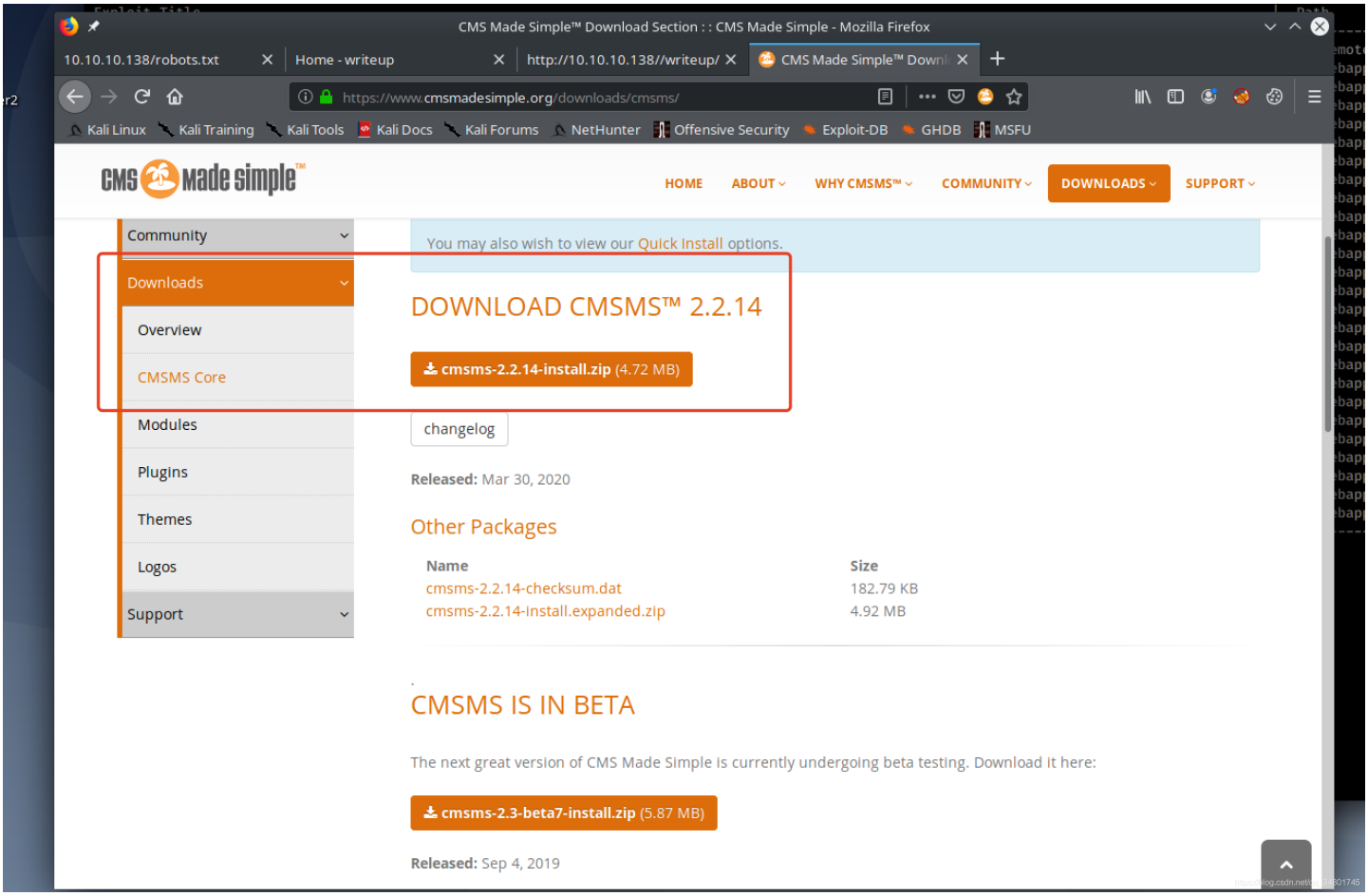
查看前段源码，发现了这是CMS Made Simple框架的服务，版本最新2019年...



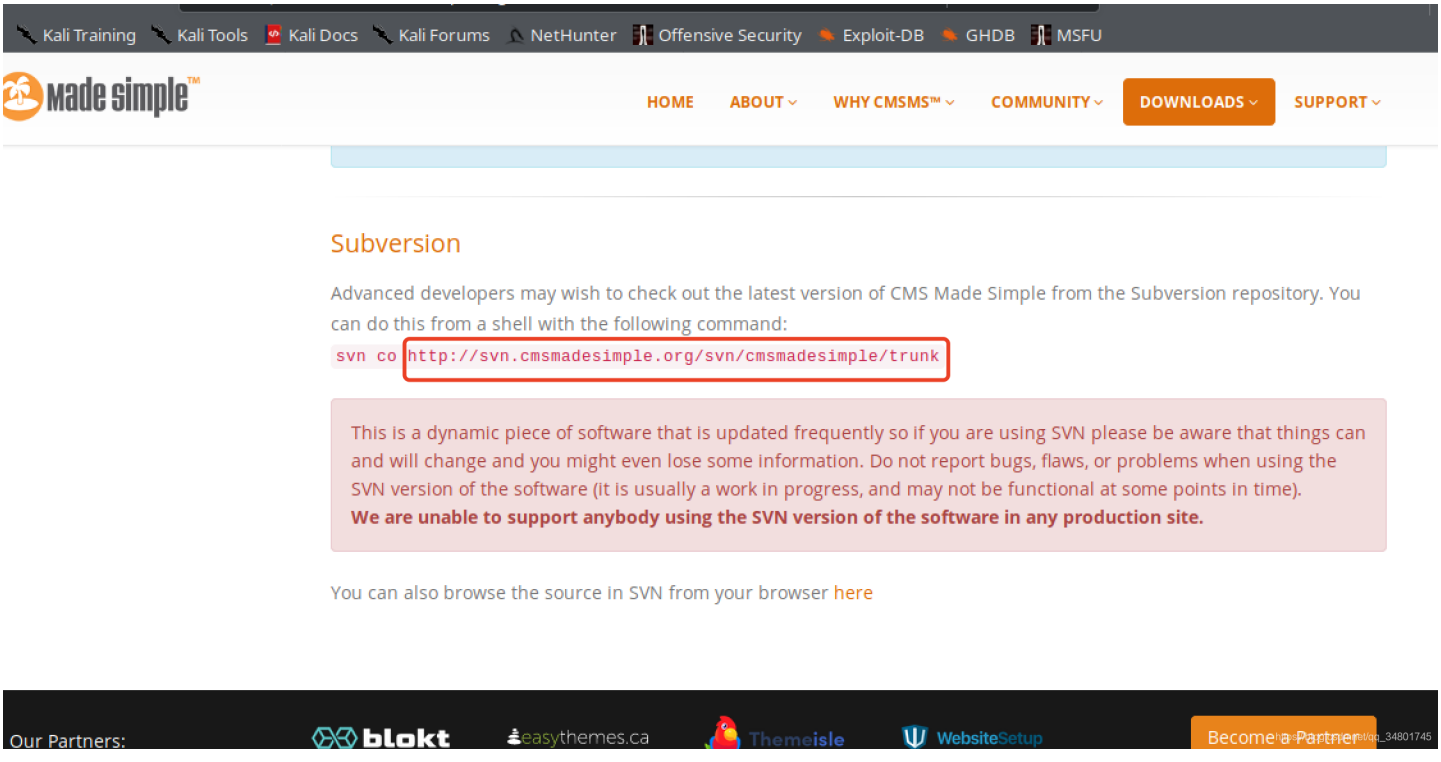
You can download it by clicking on

CMS Made Simple is an Open

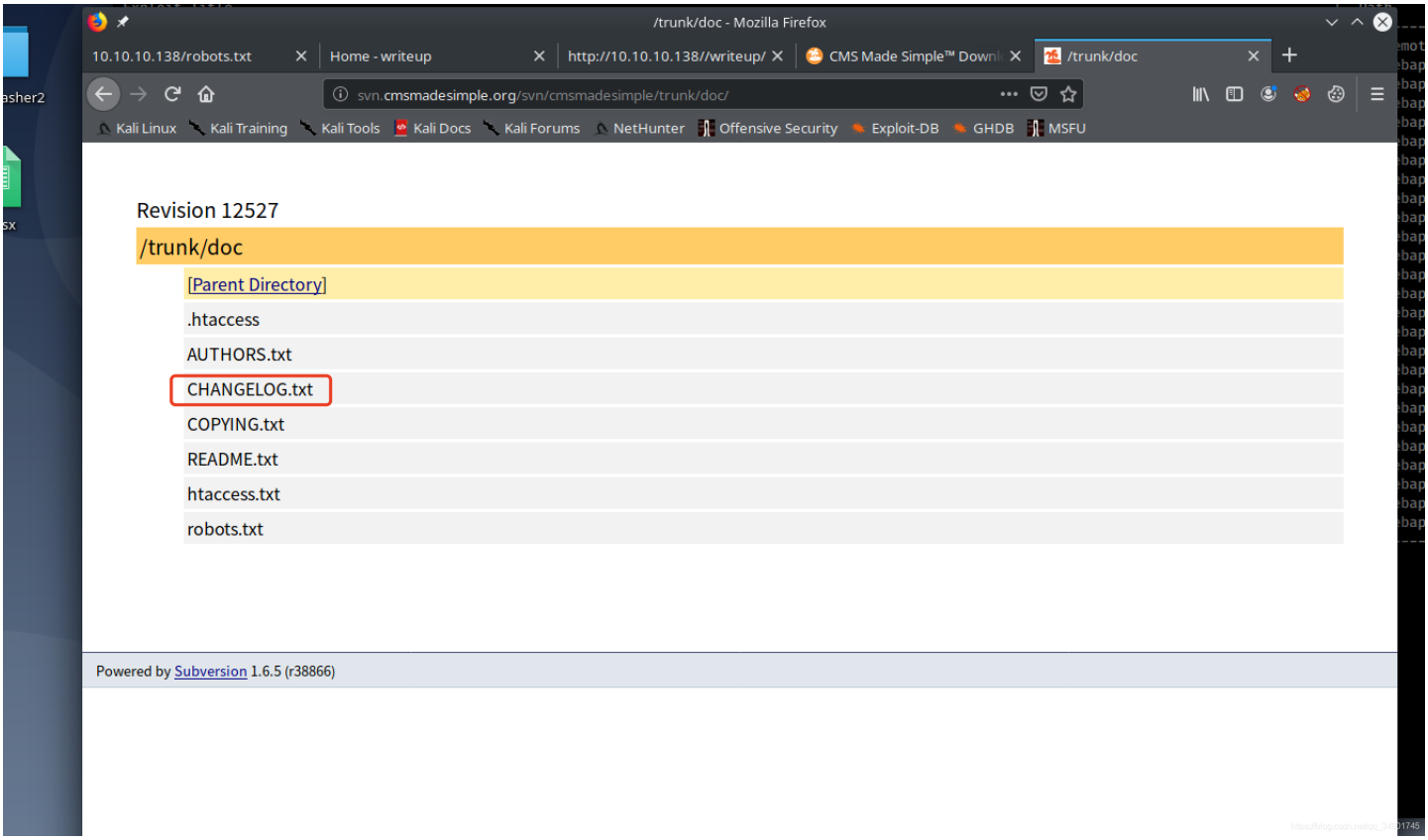
根据提示直接开始google，查找到了相关的源码？



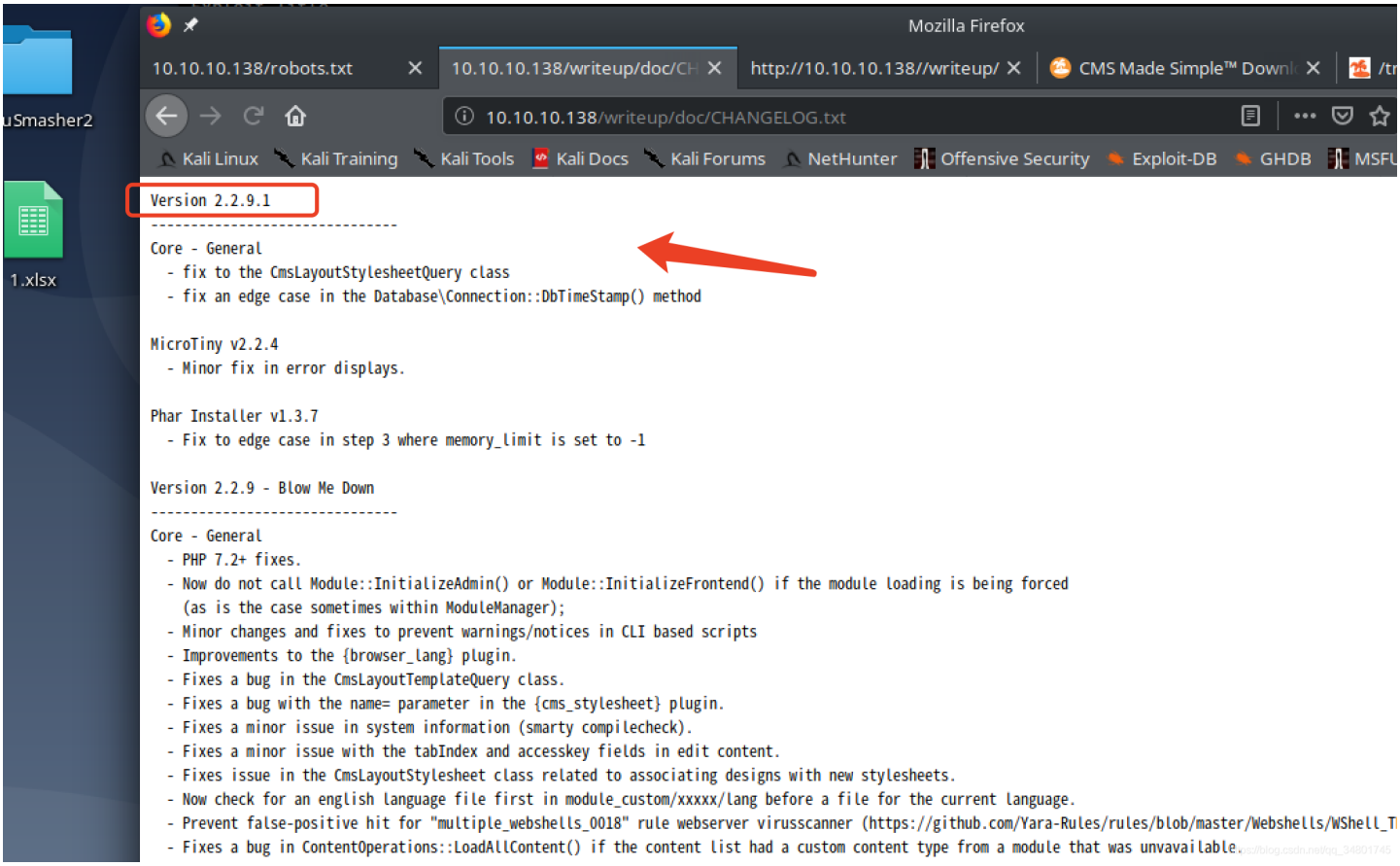
到下载页面，果然有源码包...



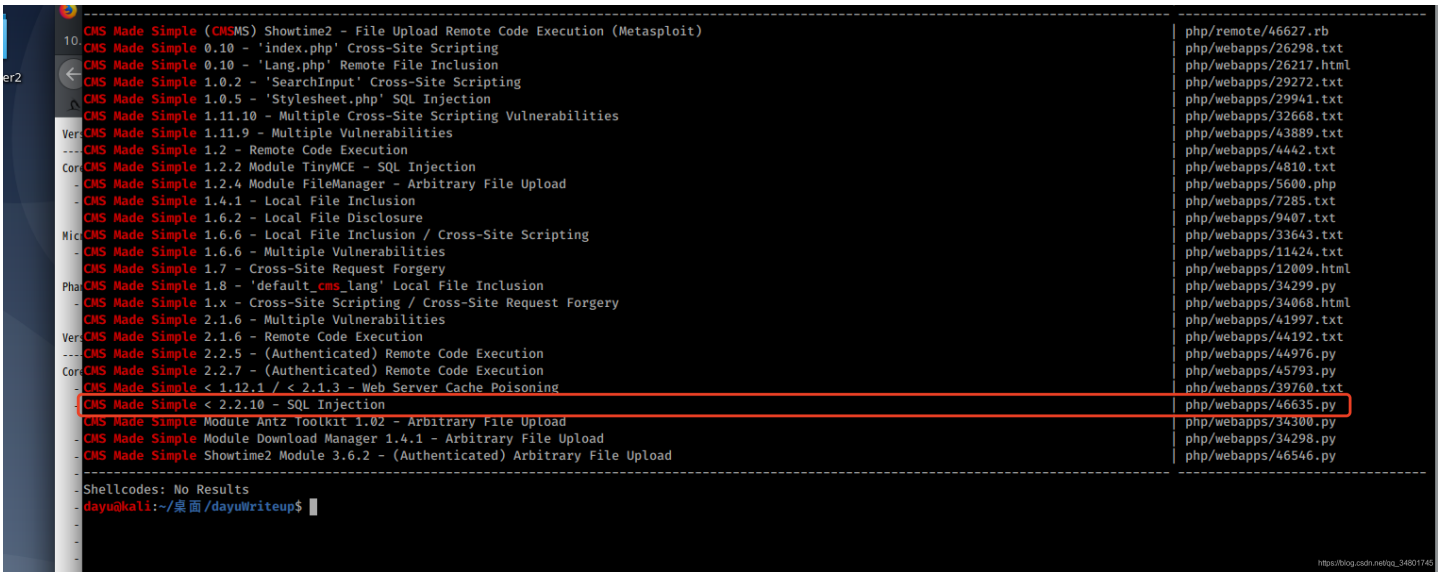
往下滑，有源码包部署好的页面地址，省的我下载包部署，我只需要查看下即可...



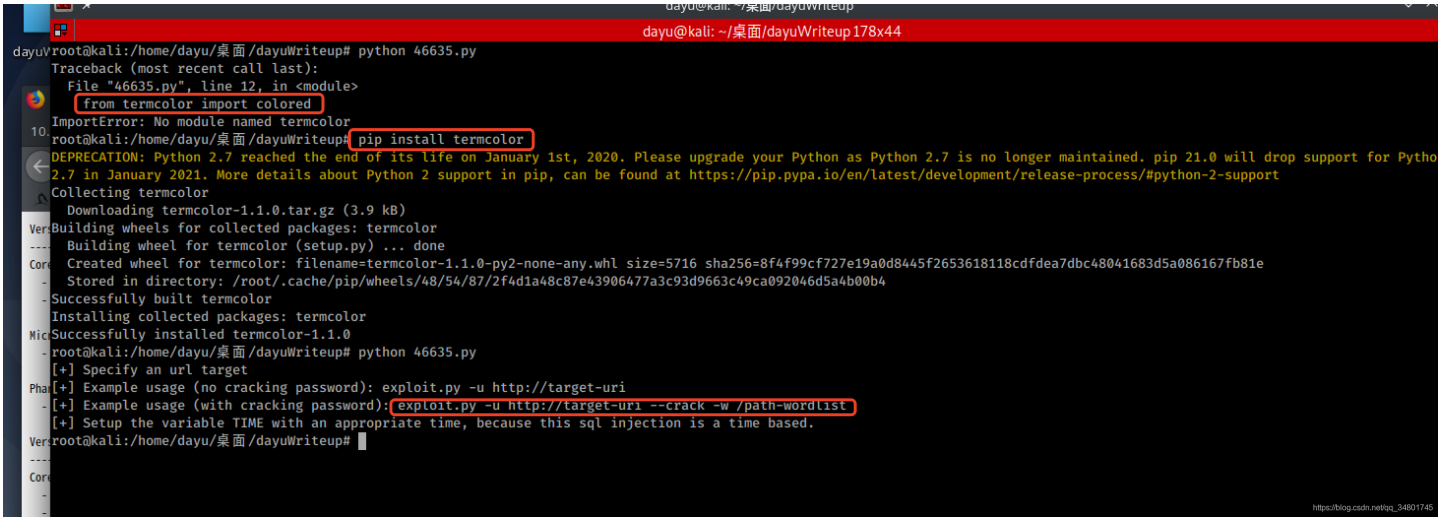
访问后，发现底层存在很多目录，doc中发现了CHANGELOG页面日志信息...



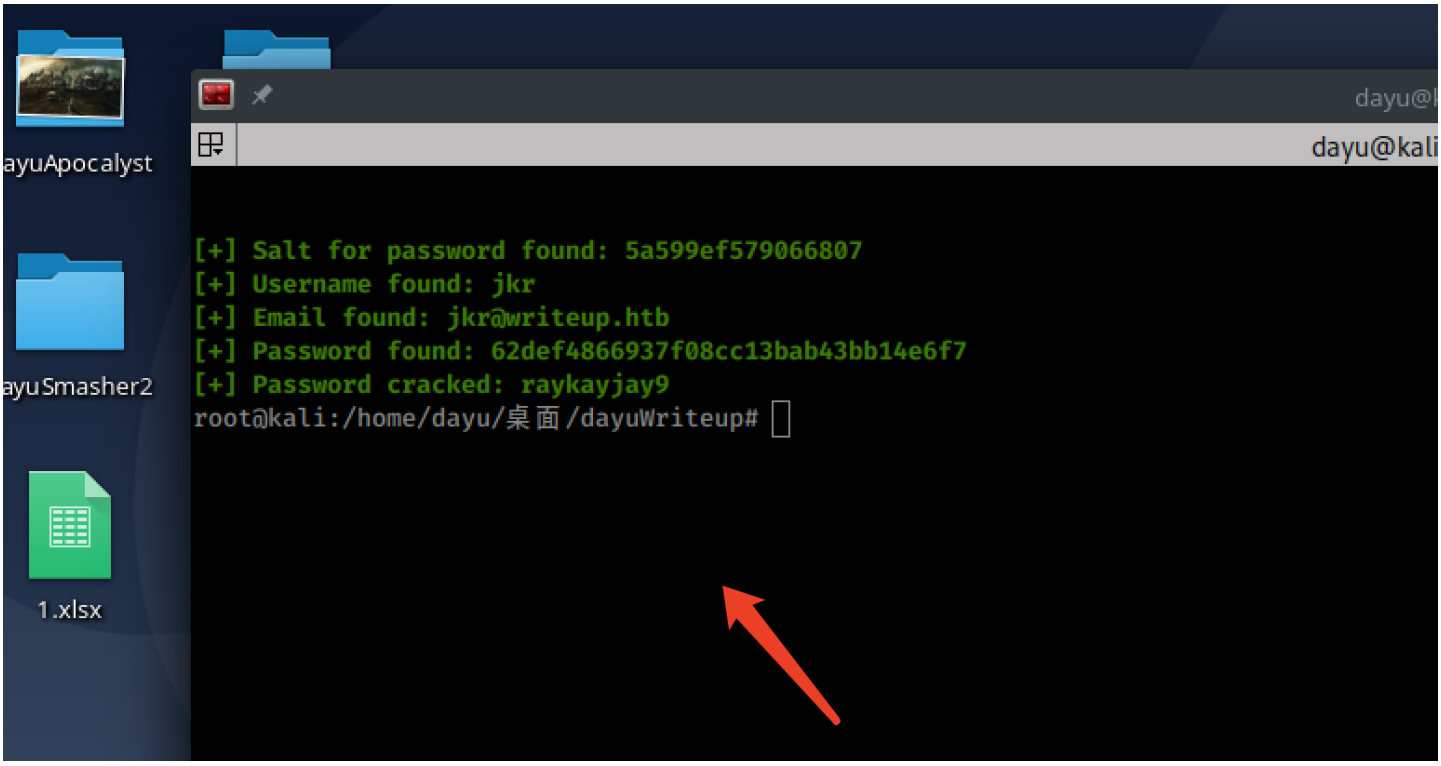
查看到了版本信息...2.2.9.1的



通过本地查找相关的漏洞信息…可利用CVE-2019-9053漏洞46635EXP进行提权…

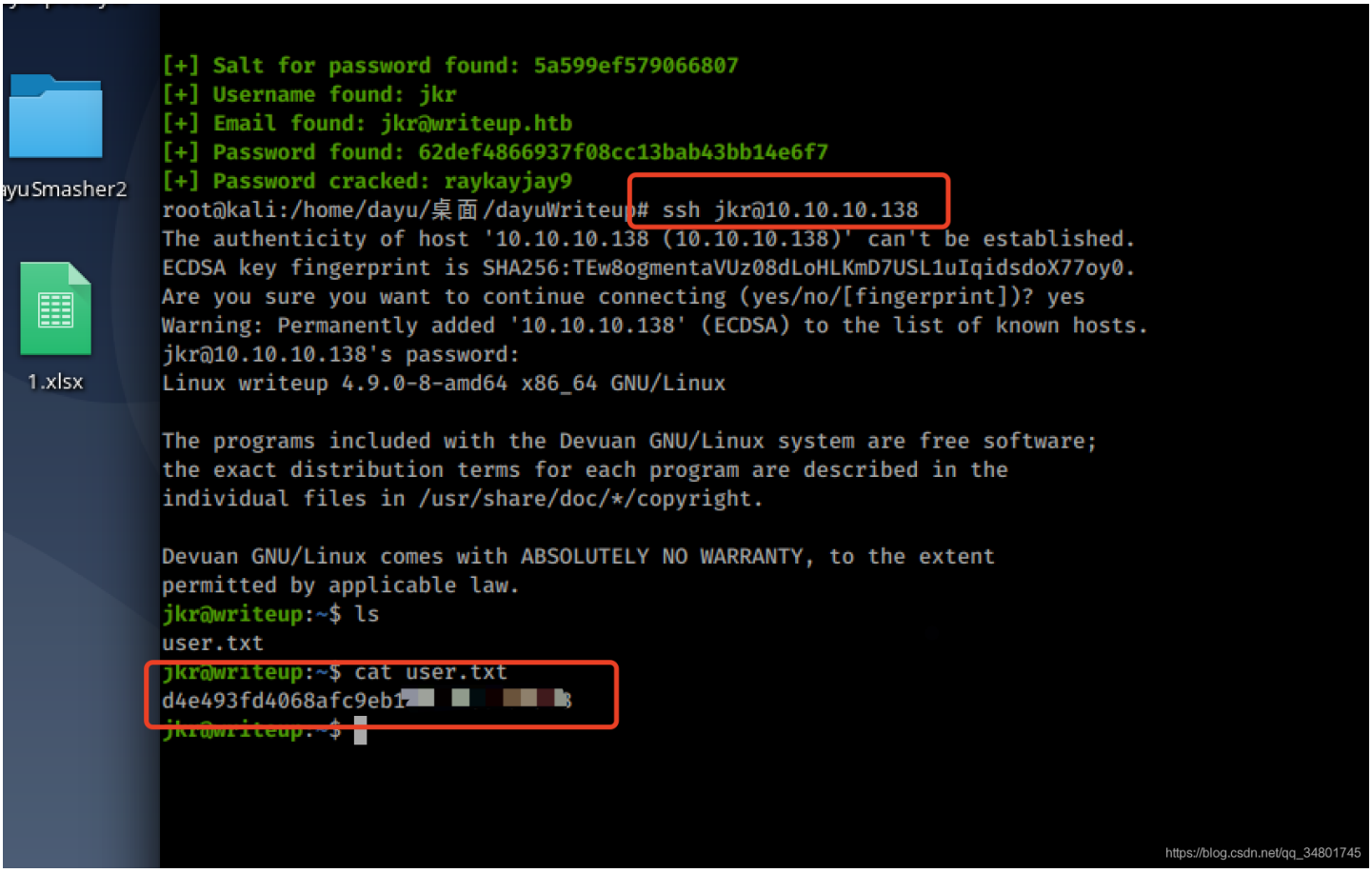


首先放到本地目录下，执行后发现了需要termcolor模块执行…PIP下载即可…

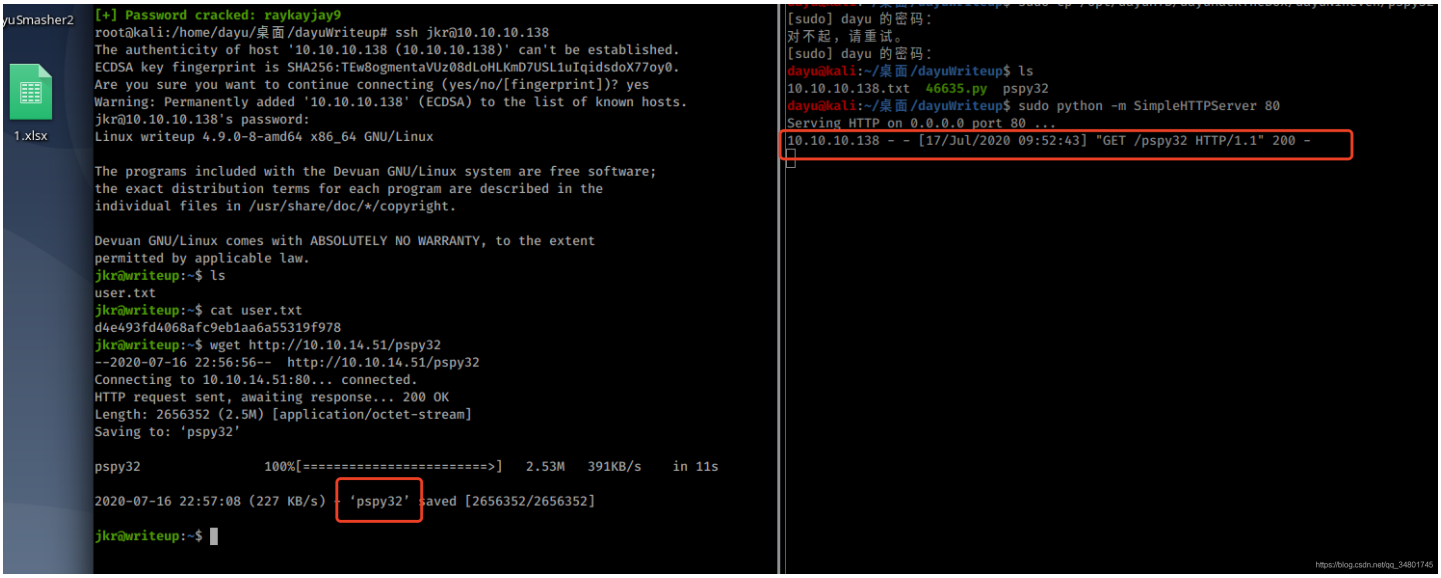


命令：`python 46635.py -u http://10.10.10.138/writeup/ --crack -w /opt/dayuHTB/dayuHackTheBox/dayuAriekei/rockyou.txt`

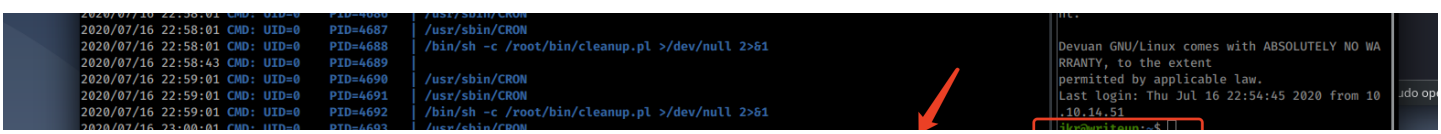
按照脚本执行即可...通过EXP和rockyou密码本，爆破获得了用户名密码...

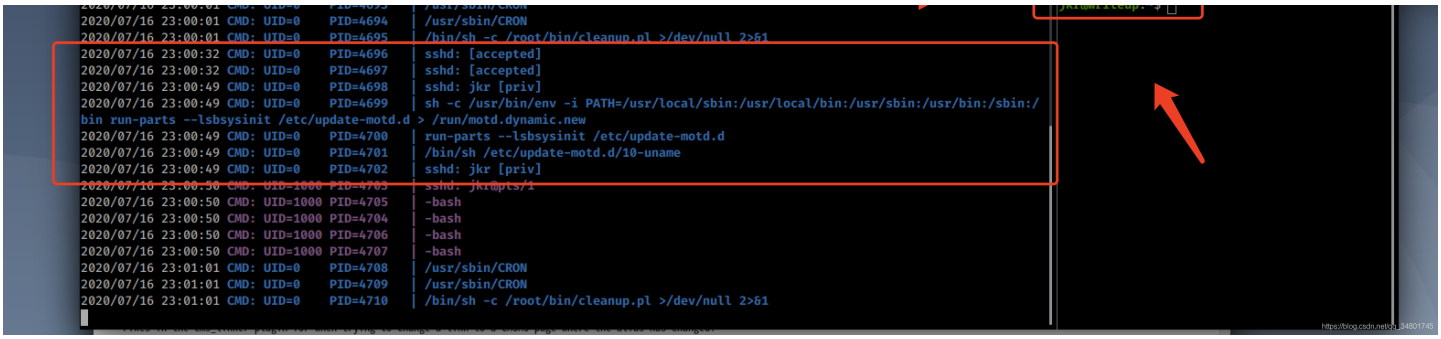


SSH服务成功登录了jkr用户，并获得了user_flag信息...

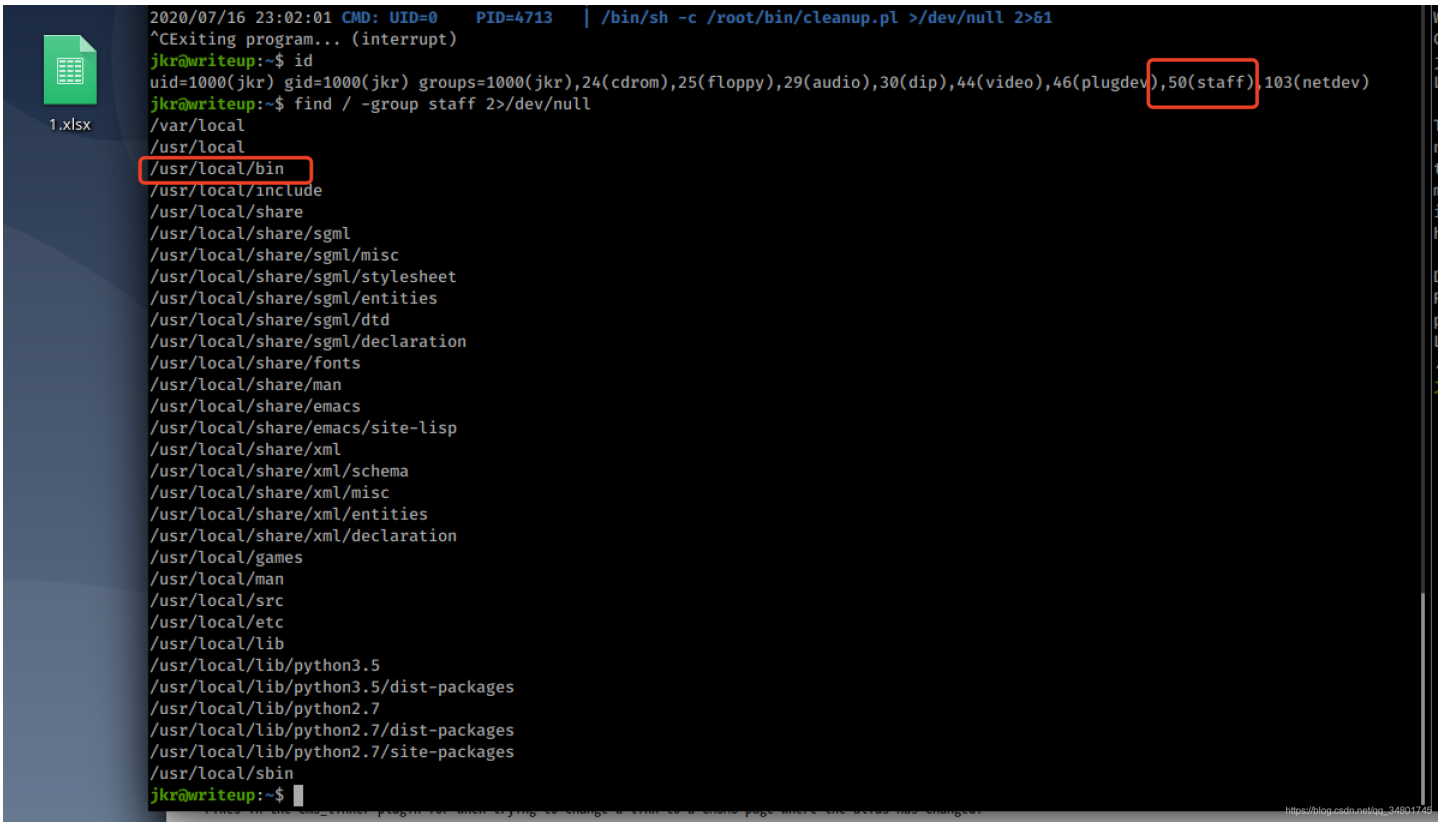


我这里上传了pspy枚举目前靶机进程状态...成功上传

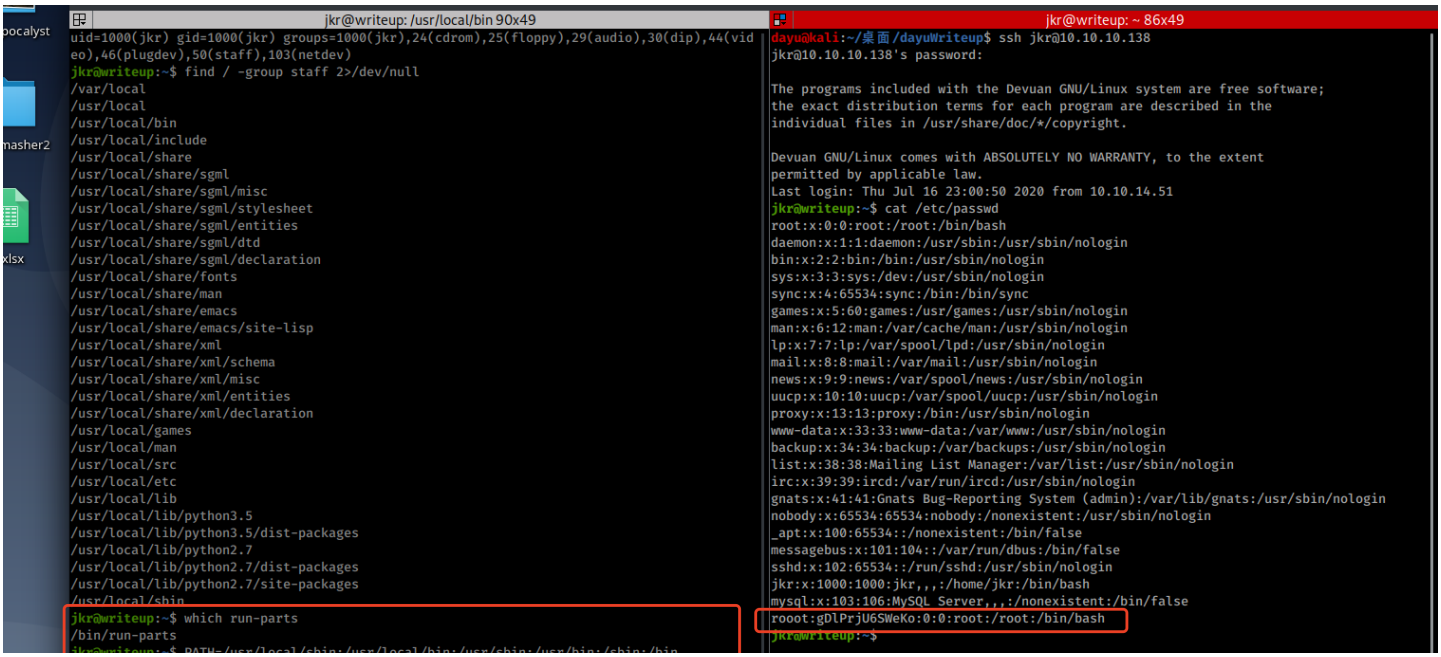




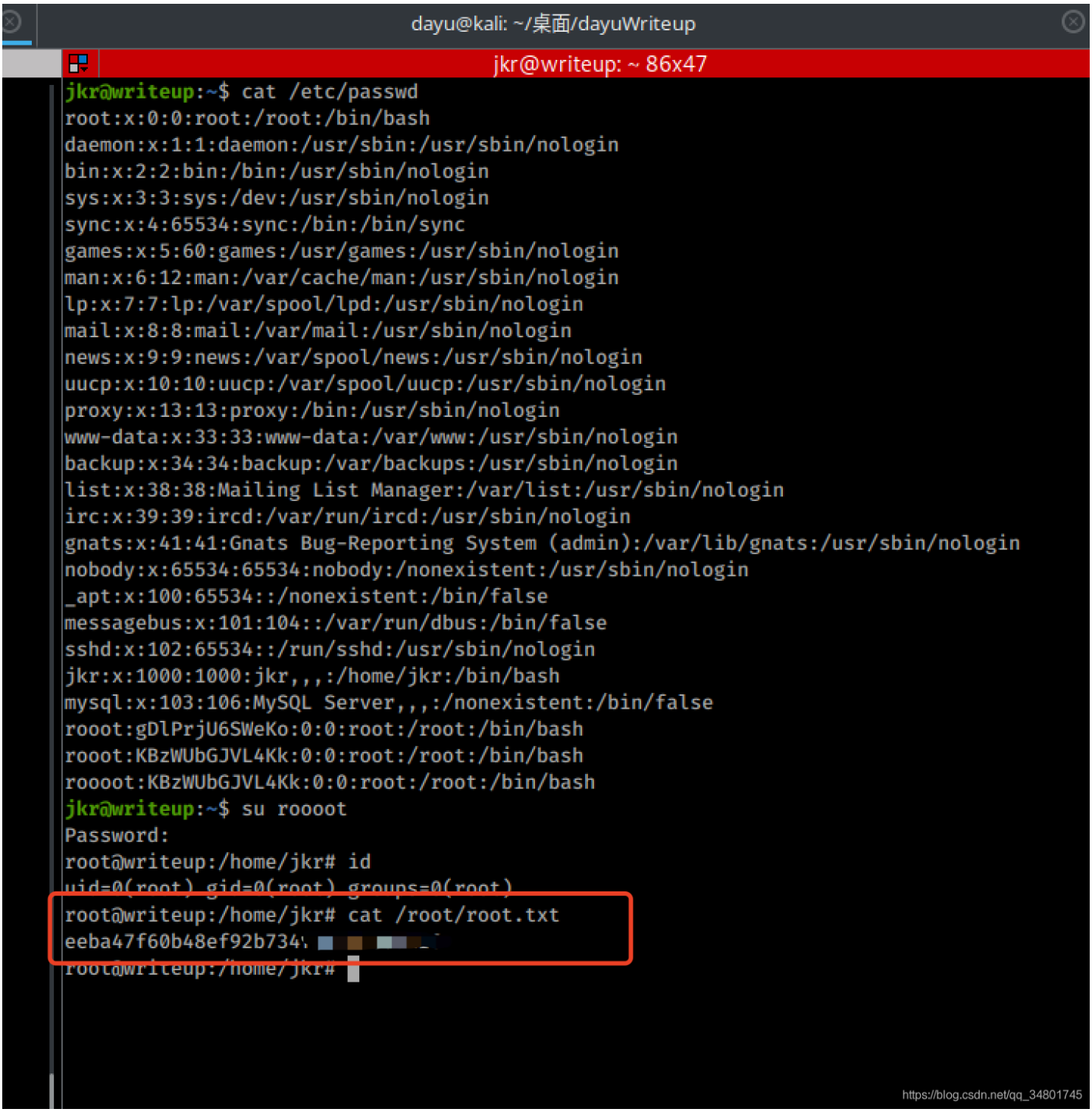
开始查看发现sshd？？，我重新开启另外窗口登录ssh后，发现每次登录都会运行一次bin目录下的run-parts文件…以root权限执行…那就简单了…



可看到jkr在一个名为staff的组中…staff成员可以写/usr/local/bin…



默认情况下run-parts位于/bin中…
创建run-parts，并写入简单的shell，在执行后写入/etc/passwd新的用户名密码具有root权限…



通过成功写入的新用户…直接su成功登录，获得了root权限…
读取到了root_flag信息…

这台靶机简单常规…
获取apache框架信息–寻找相关的EXP–利用EXP获得用户名密码–SSH登录后pspy32枚举进程–最后写shell提权…

由于我们已经成功得到root权限查看user和root.txt，因此完成这台初级的靶机，希望你们喜欢这台机器，请继续关注大余后期会有更多具有挑战性的机器，一起练习学习。

如果你有其他的方法，欢迎留言。要是有写错了的地方，请你一定要告诉我。要是你觉得这篇博客写的还不错，欢迎分享给身边的人。