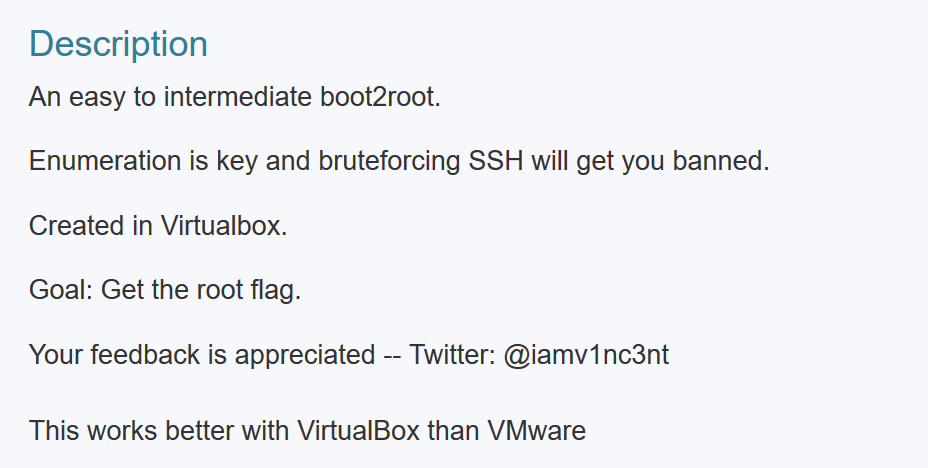
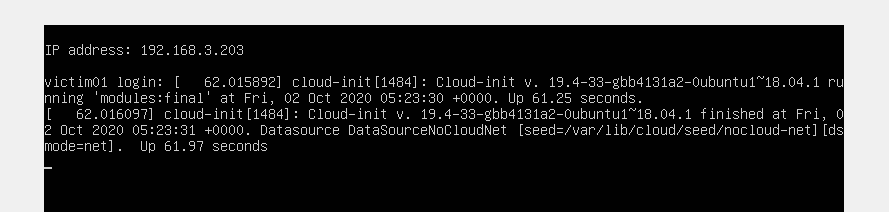
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/victim-1,469/>

简单级别，目标是得到root的flag，枚举是关键，强行爆破SSH端口会翻车。建议在virutalbox下运行



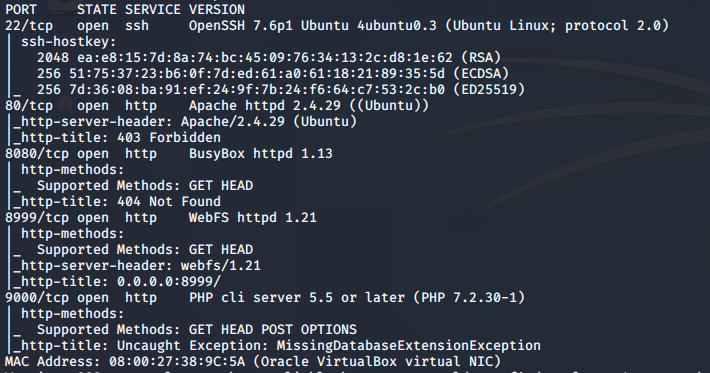
由于之前有些过如何在virtualbox下安装这里就忽略了，运行靶机以后会自动回显IP出来



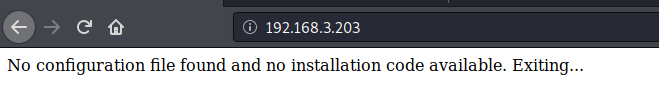
# 0x01:探测靶机

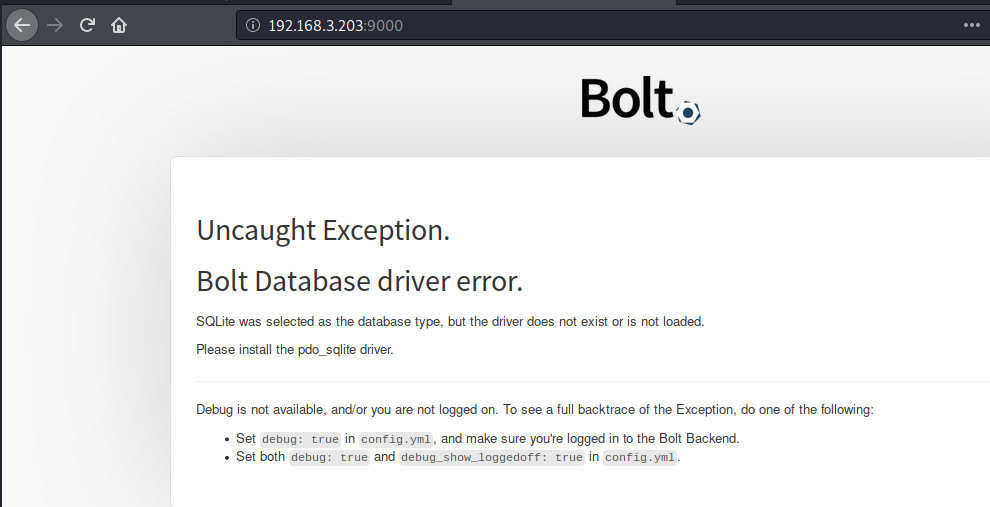
由于知道了IP为192.168.3.203直接上nmap探测波端口

命令:nmap -A -sS -sV -v -p- 192.168.3.203

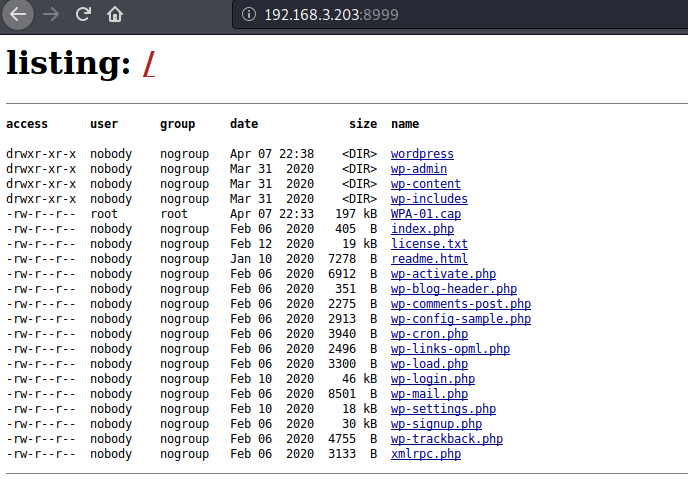


扫完以后发现有点奇怪，80端口会回显403，8080会回显404，先输入波IP跟进会发现没有配置文件，然后9000端口也是提示配置错误





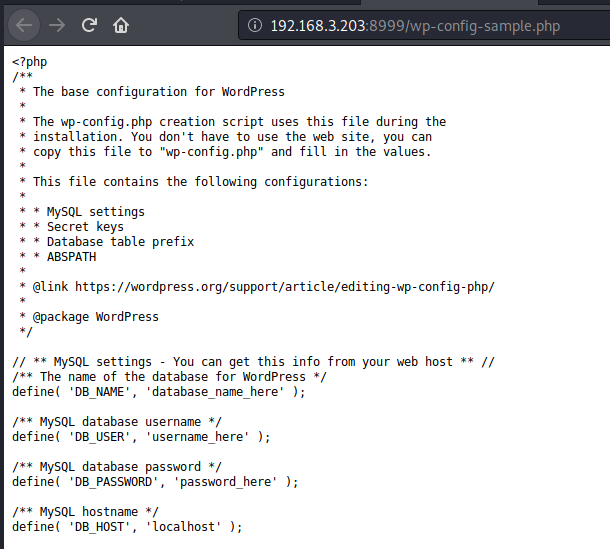
然而突破口是在8999端口，可以正常访问开始挖掘8999端口



# 0x02:挖掘信息

这里先思考一个问题，正常来讲访问靶机的80端口或者HTTP服务都会回显正常页面或者其它信息，而这里却提示配置文件出了点问题。而且从这个8999端口的文件信息可以判断出这是一个wordpress的CMS站点。可能是数据库账号密码出错导致这种情况发生。

点开wp-config-sample.php看到里面的数据库账号密码好像是有点奇怪还是没填?

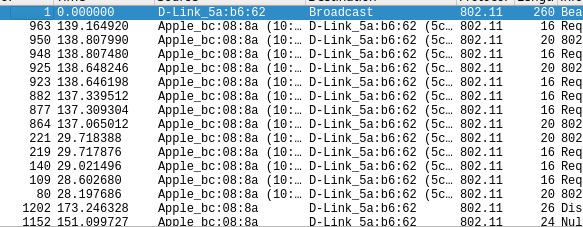


同时在8099端口有一个奇怪的文件WPA-01.cap，得用wireshark打开才行，可能是个流量文件

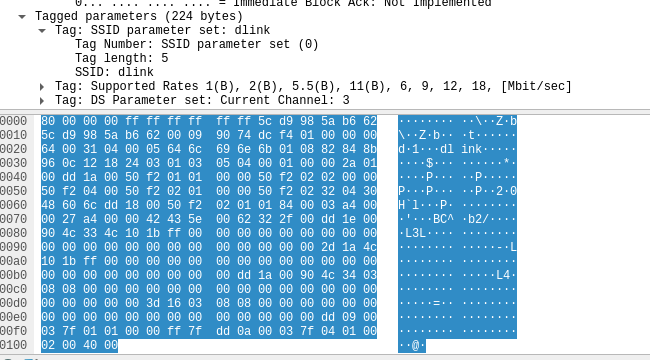


# 0x03:分析流量包

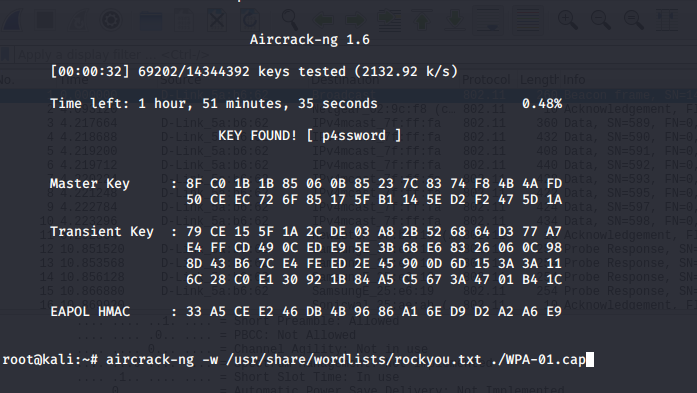
打开以后看了下source address主要有D-Link和Apple，都很好理解D-Link就是路由器的意思可能是一个WIFI浏览过这个网站，Apple就是iphone嘛。可能就是有苹果设备用户和一个路由器用户访问过这个网站(网站配置正常的情况下猜测)



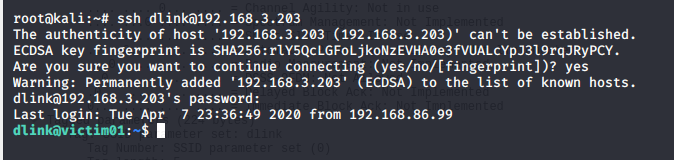
继续分析在点开一堆折叠发现一个东西SSID，简单的来讲就是WIFI名字叫dlink。然后最下面就是一堆间间断断的明文信息



为了看看这个流量包里面可不可能会包含密码之类的东西可以用aircrack-ng的-w功能加载字典匹配一波，-w其实也可以用来爆破WIFI密码一波最后找到密码为p4ssword

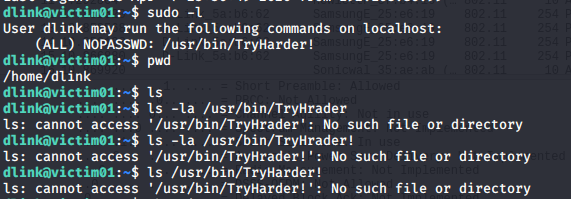


总结一下就是WIFI名称为dlink,密码是p4ssword,有点像账号密码一样，尝试登录一波22端口成功了

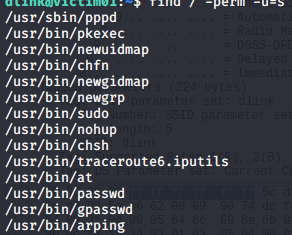


# 0x04:提权

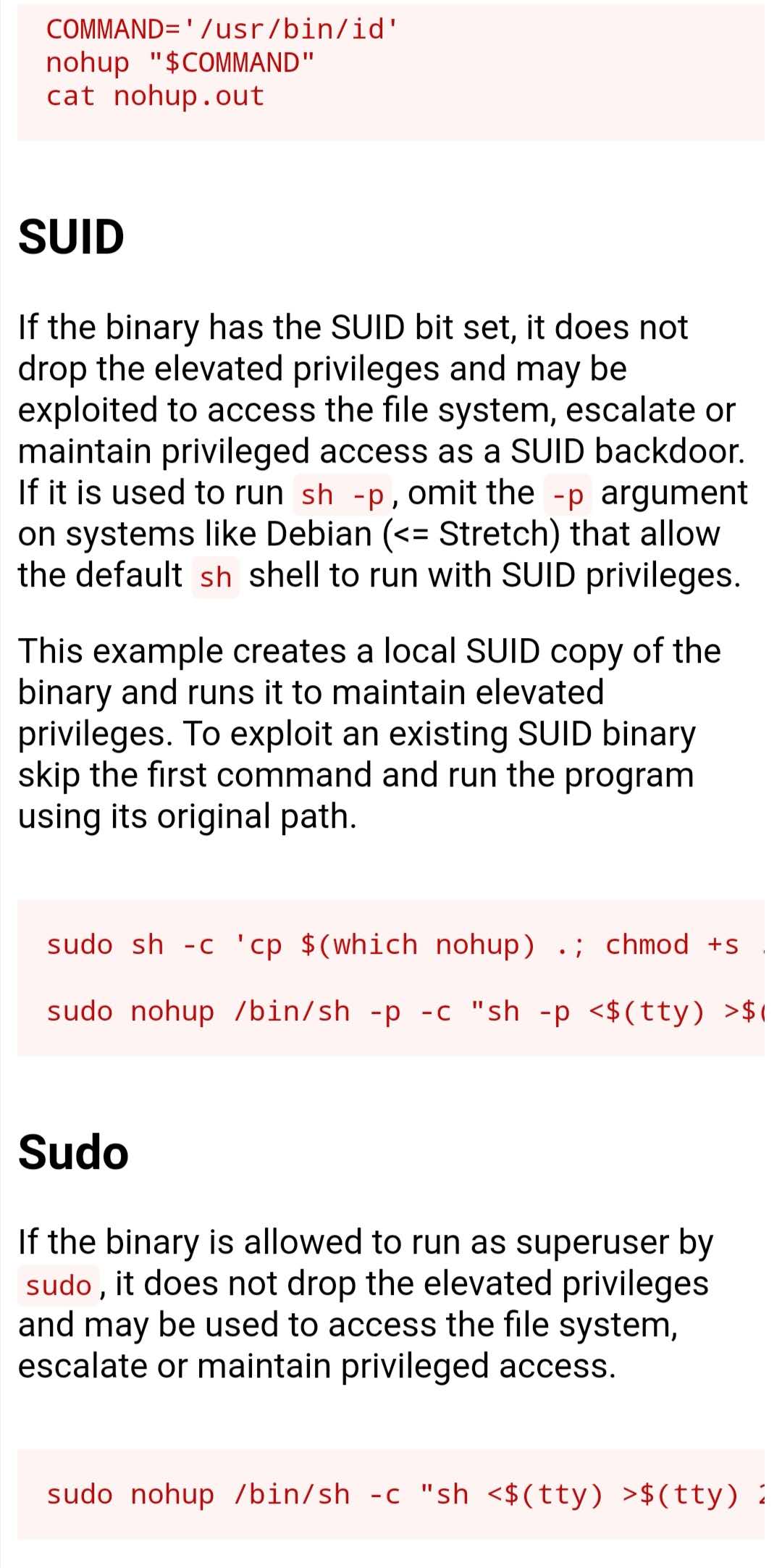
一开始我是想用sudo -l来看看有没有什么特殊权限结果出来个TryHrader我以为是个文件结果。。。。。。不存在



换成find找到一些，然后去找那些奇奇怪怪的命令，比如说pppd,nohup



然后到<https://gtfobins.github.io/gtfobins>这个网站找对应的命令，这里一直到nohup发现一个对应的SUID



只不过最后是要忽略sudo才能执行成功

