Vulnhub Target

1. MoneyBox: 1
2. Hackademic: RTB1
3. Me and My Girlfriend: 1

WriteUp For MoneyBox

About Release

(https://www.vulnhub.com/entry/moneybox-1,653/#top)

- **Name**: MoneyBox: 1
- **Date release**: 27 Feb 2021
- **Author**: Kirthik_T
- **Series**: MoneyBox

  Description

Back to the Top

Difficulty : Easy

Goal : 3 flags

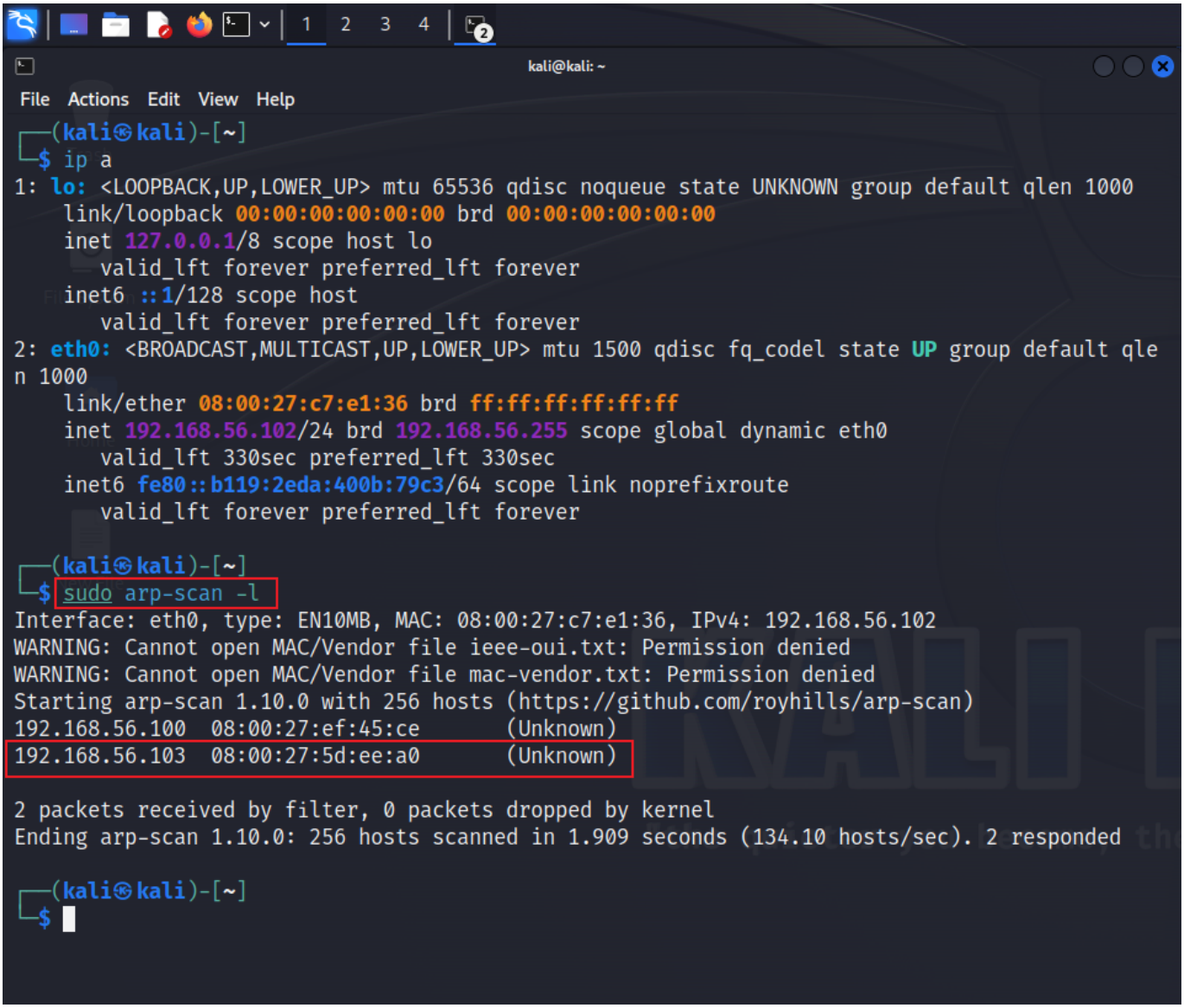
This works better with VirtualBox rather than VMware

主要渗透过程：

信息收集

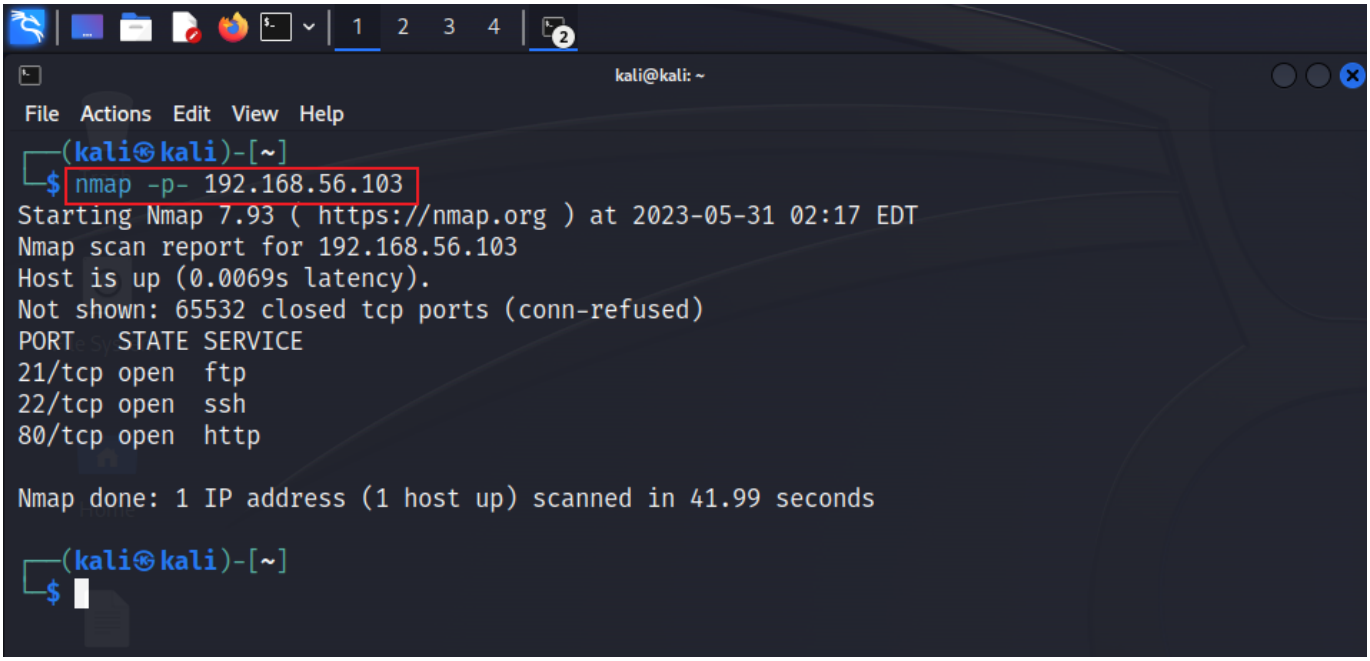
1.靶机发现

```
sudo arp-scan -l
```

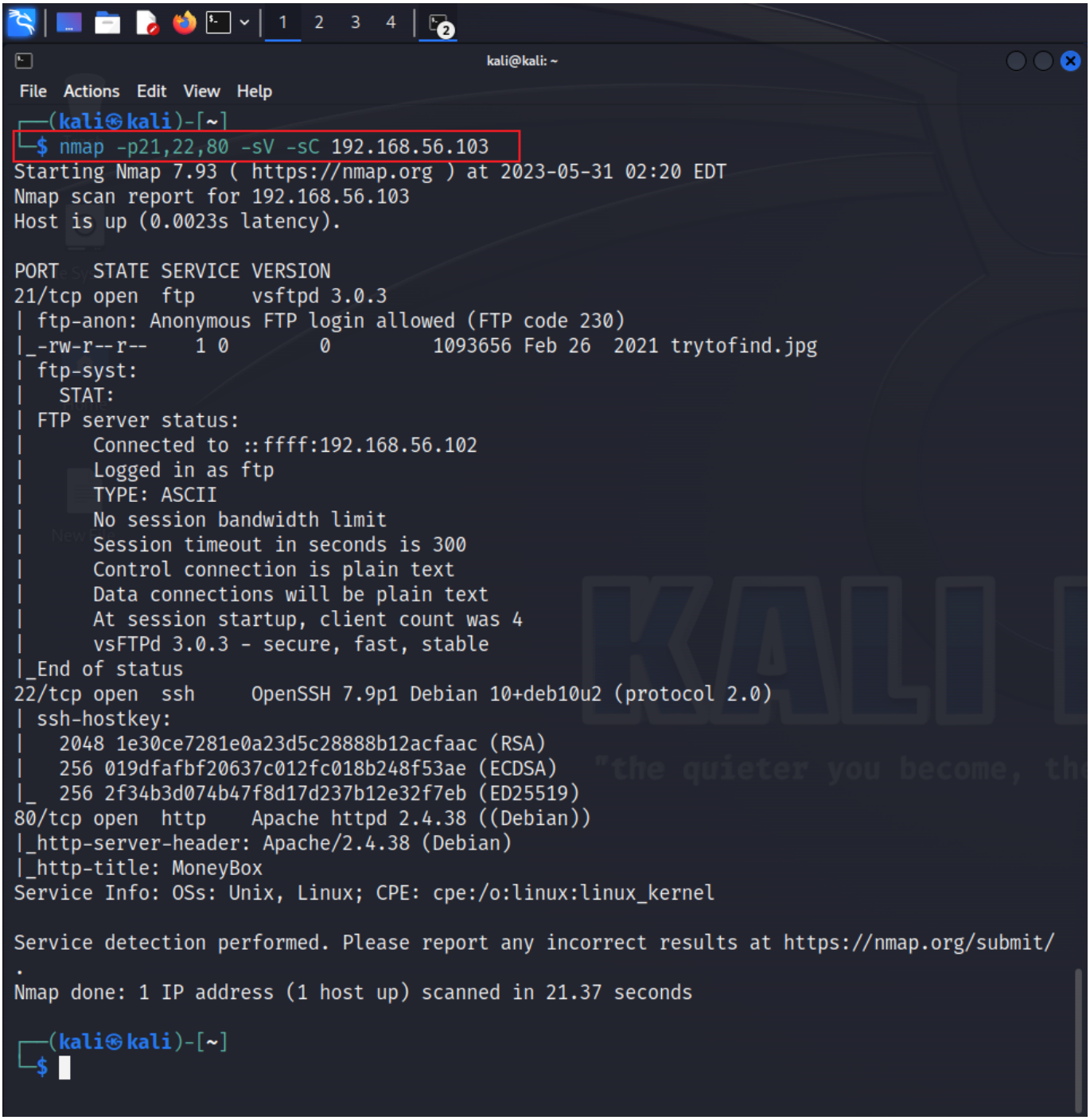


2.靶机全端口扫描

```
nmap -p- 192.168.56.
```



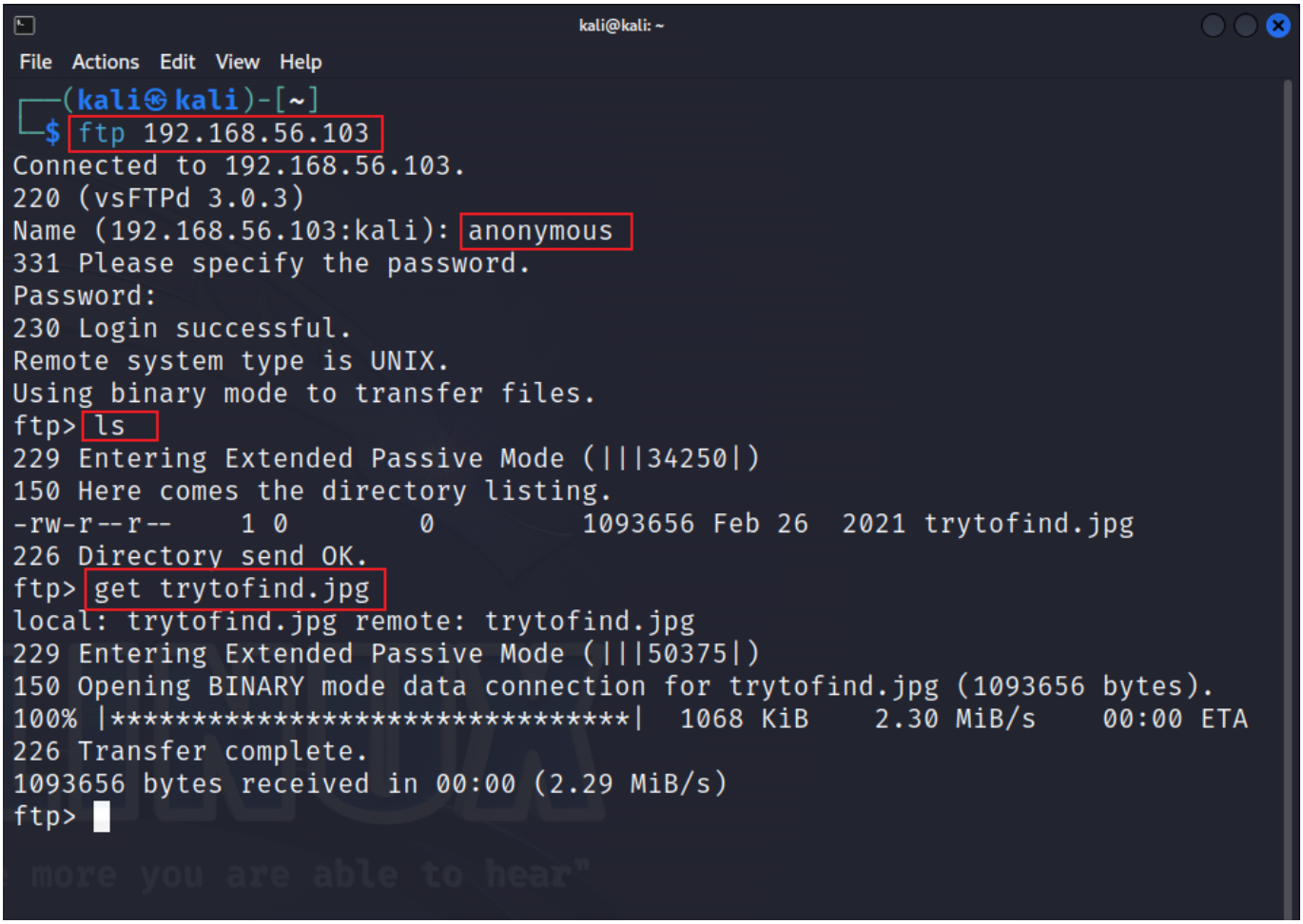
3.靶机所有开放的端口对应服务版本号、漏洞探测



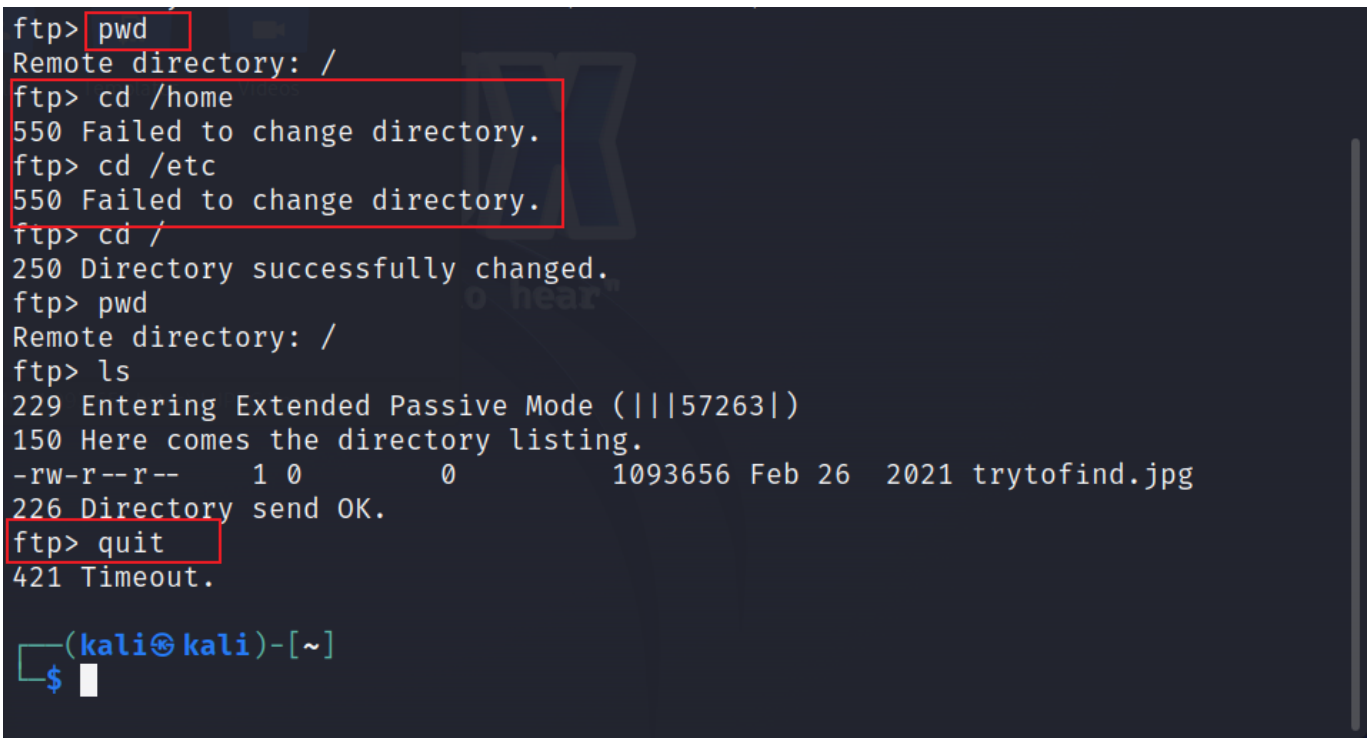
4.漏洞利用

根据前3步探测的信息，访问靶机开放的服务，尝试渗透

1）先是21端口，根据探测的信息判断为FTP服务，且存在匿名访问，FTP主目录下还有一个图片文件；

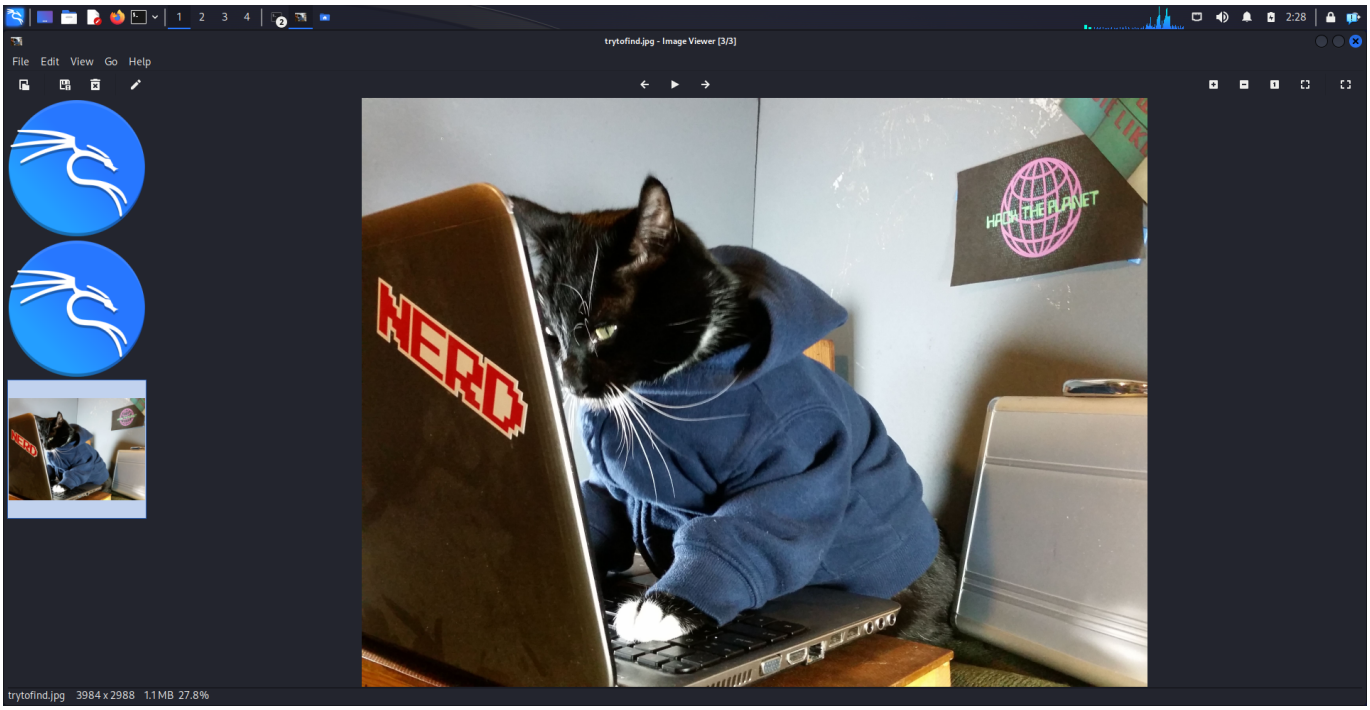


有些FTP服务配置不当允许匿名用户在FTP服务器上切换目录，我们尝试能不能跳出FTP主目录；



经过尝试，发现不能跳出FTP主目录，于是先使用quit命令退出FTP服务。

那我们对下载的图片文件进行查看。

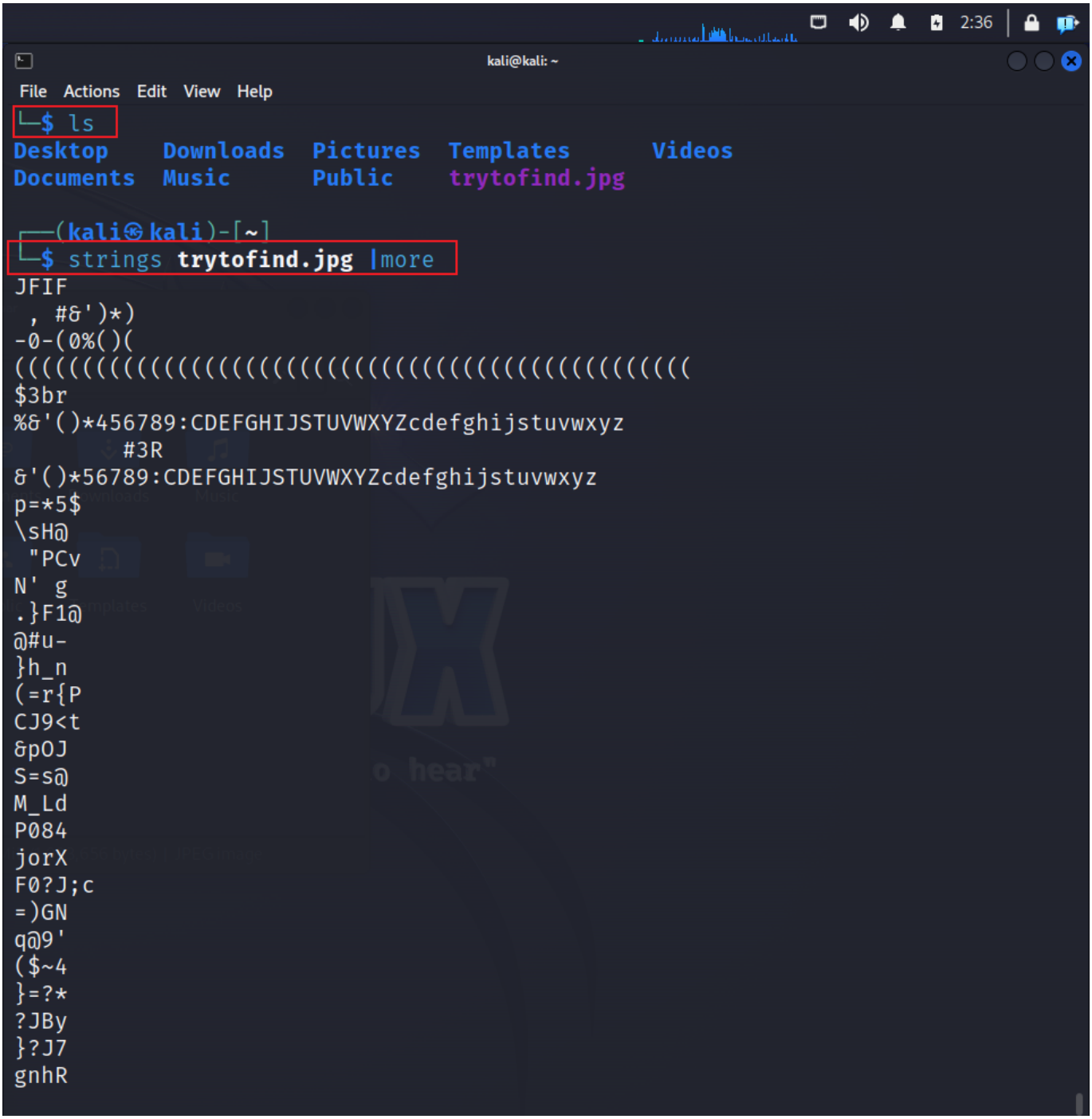


这是一张滑稽的猫照，似乎也没有什么有用的信息。

这条线索似乎到这里就进行不下去了....

联想到在CTF夺旗赛中经常会在图片中隐藏一些信息，那这张图片中是否有隐藏一些重要信息呢?

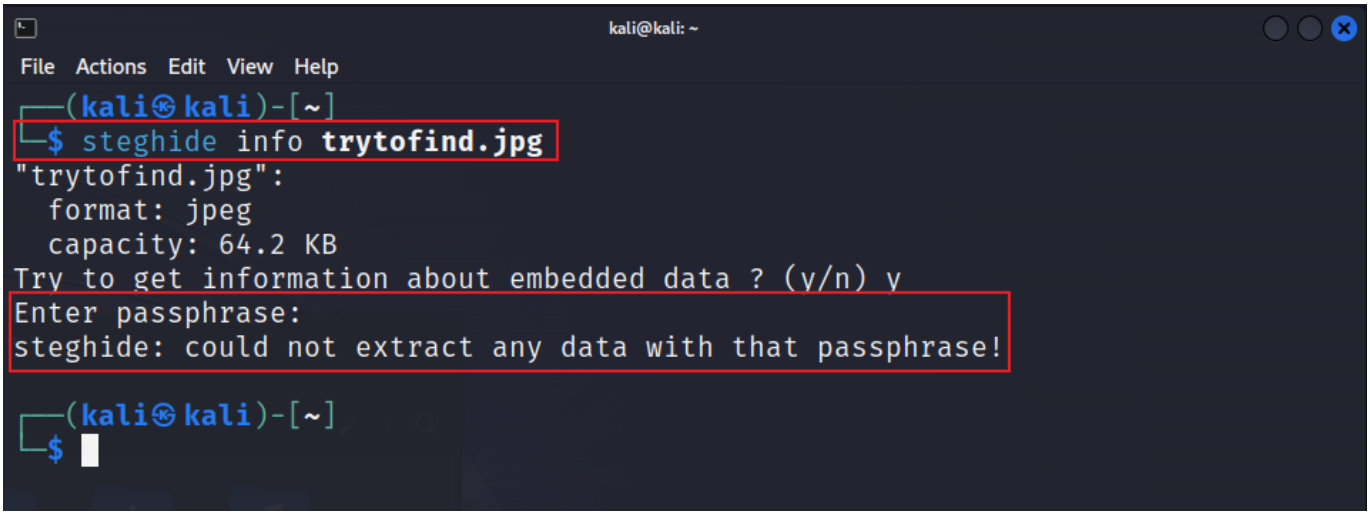
先用kali自带的strings工具查看一下该图片中的可打印字符。



发现文件前面有一些异常，出现大量左括弧和英文字母，不同于普通图片文件。

接下来进一步借助steghide命令进一步探测

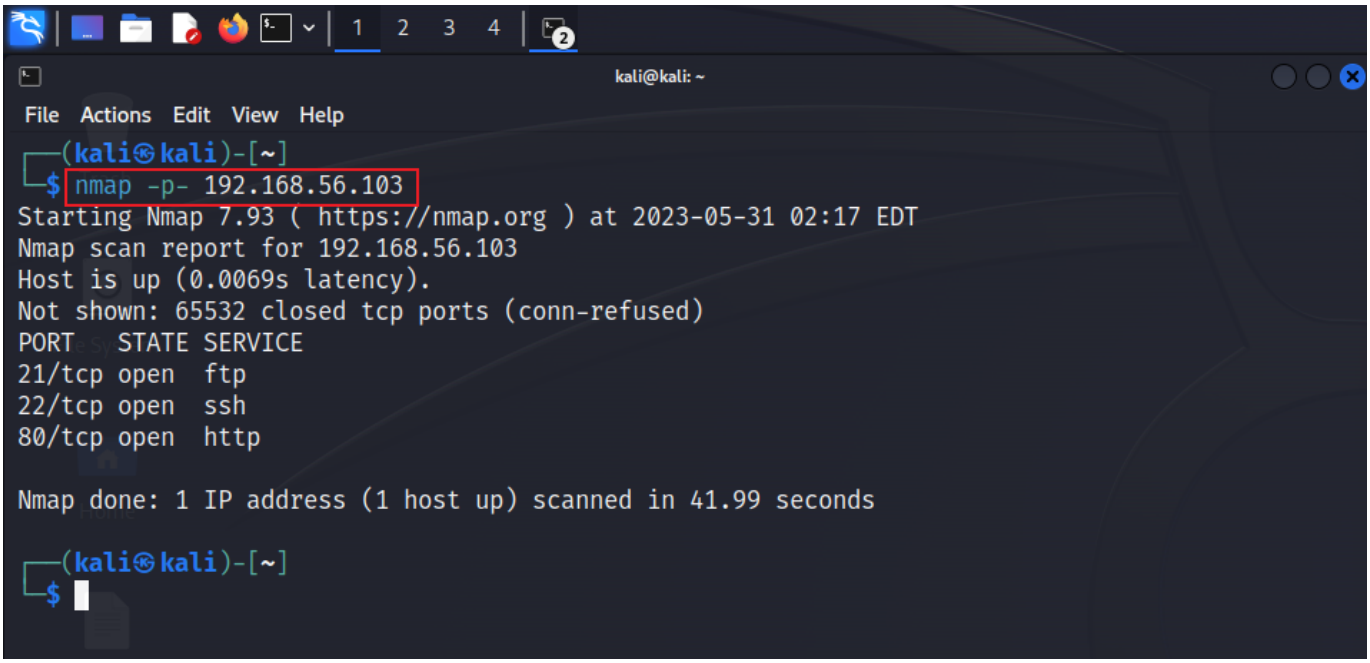
```
steghide info trytofind.jpg
```



图片文件确实嵌入了其它数据，但是被加密了，查看需要密码....!?????/

渗透工作再次陷入被动.....

FTP服务我们获得一些信息和数据，但是目前进行不下去，根据渗透回溯思想，我们再次回到粗发的地方....



不是还有22和80端口吗，嘻嘻

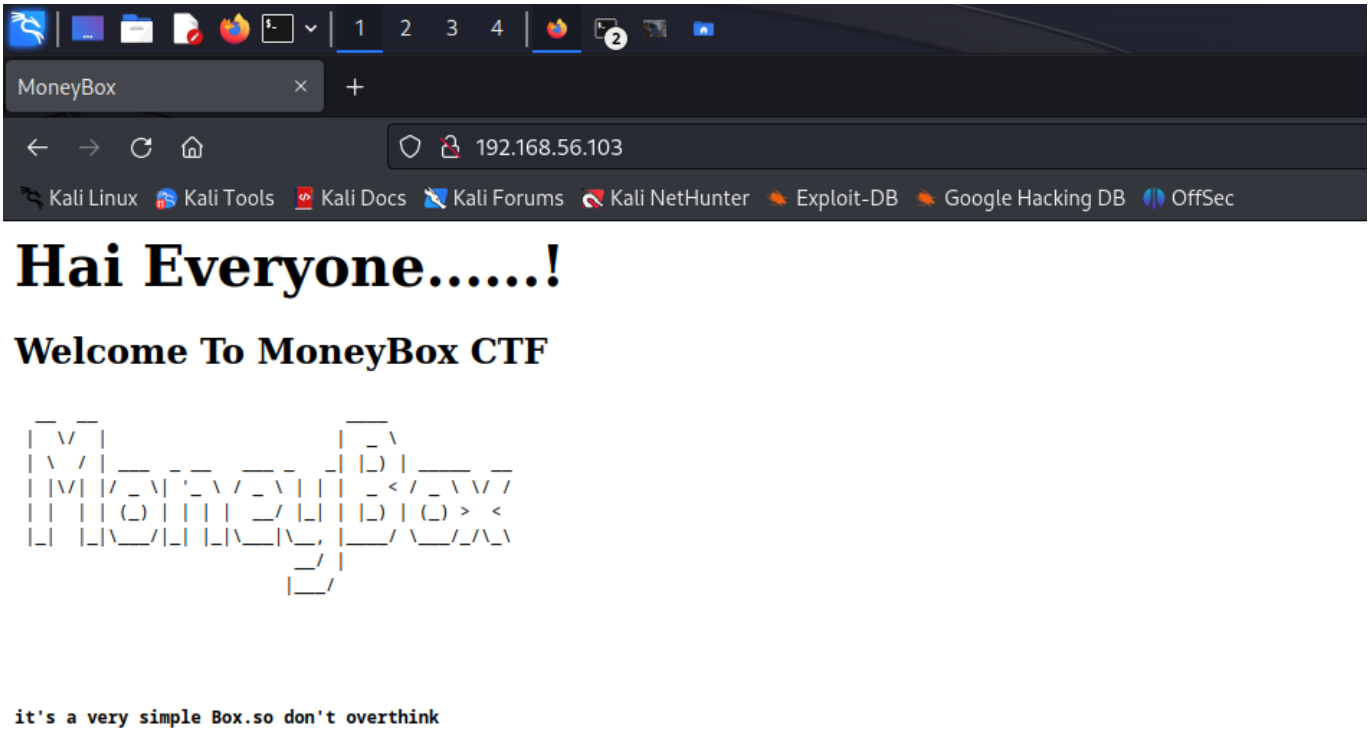
你倾向于先从哪个端口突破呢，有同学说是22端口，那22端口有哪些漏洞利用方法呢?

讨论一下吧

老师说一下自己的想法:

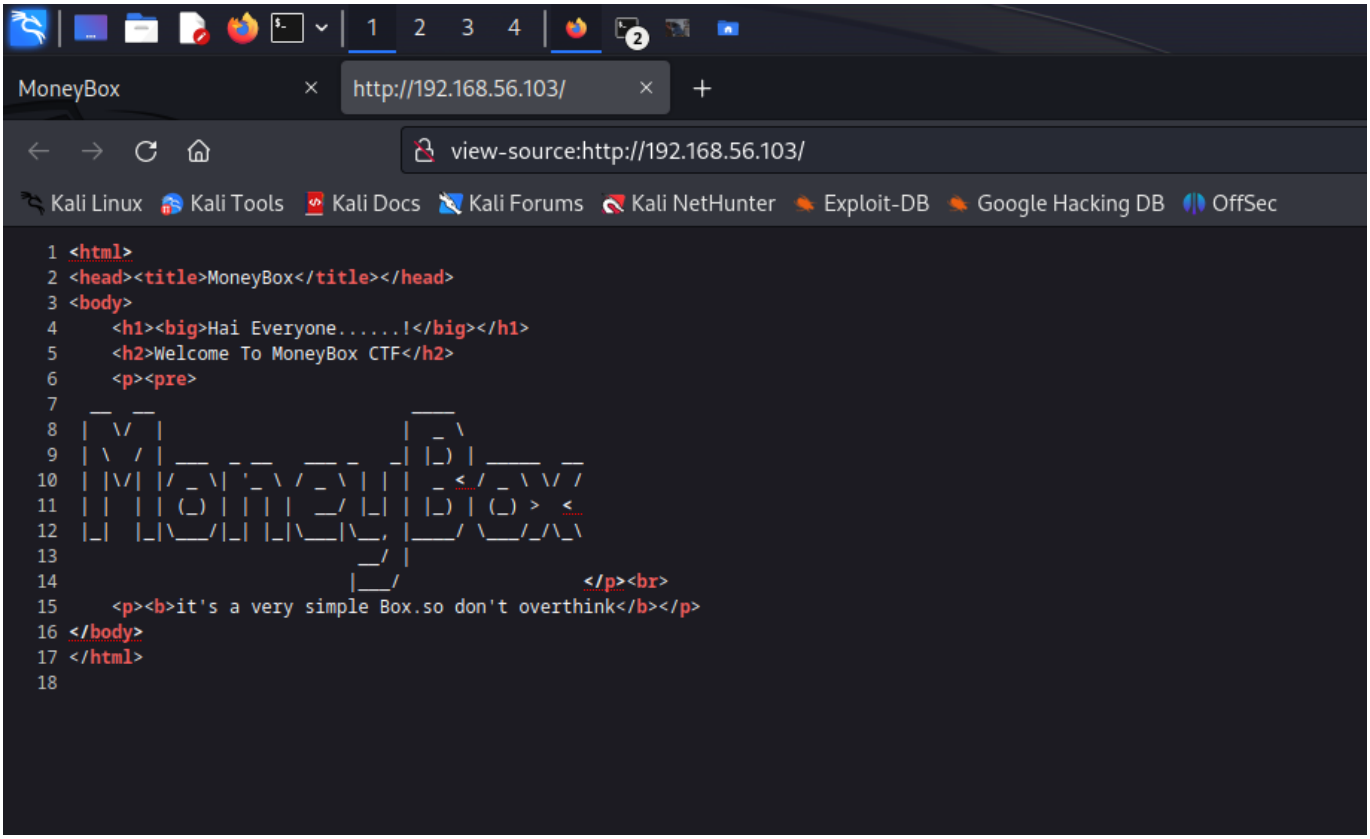
22端口，对应的是ssh远程登录服务，一般利用的方法是用户名和密码的爆破，但当前靶机提示信息既没有给到用户名，也么有给到密码，虽然可以使用字典，但排列组合数量太大，还不一定能成功，可以做为最后沉底节目，因此我们先从80端口开始。

2）访问靶机80端口



比较简单的网页，页面有一行提示：这是一个简单的盒子，不需要想的特别复杂。

于是查看网页源文件：

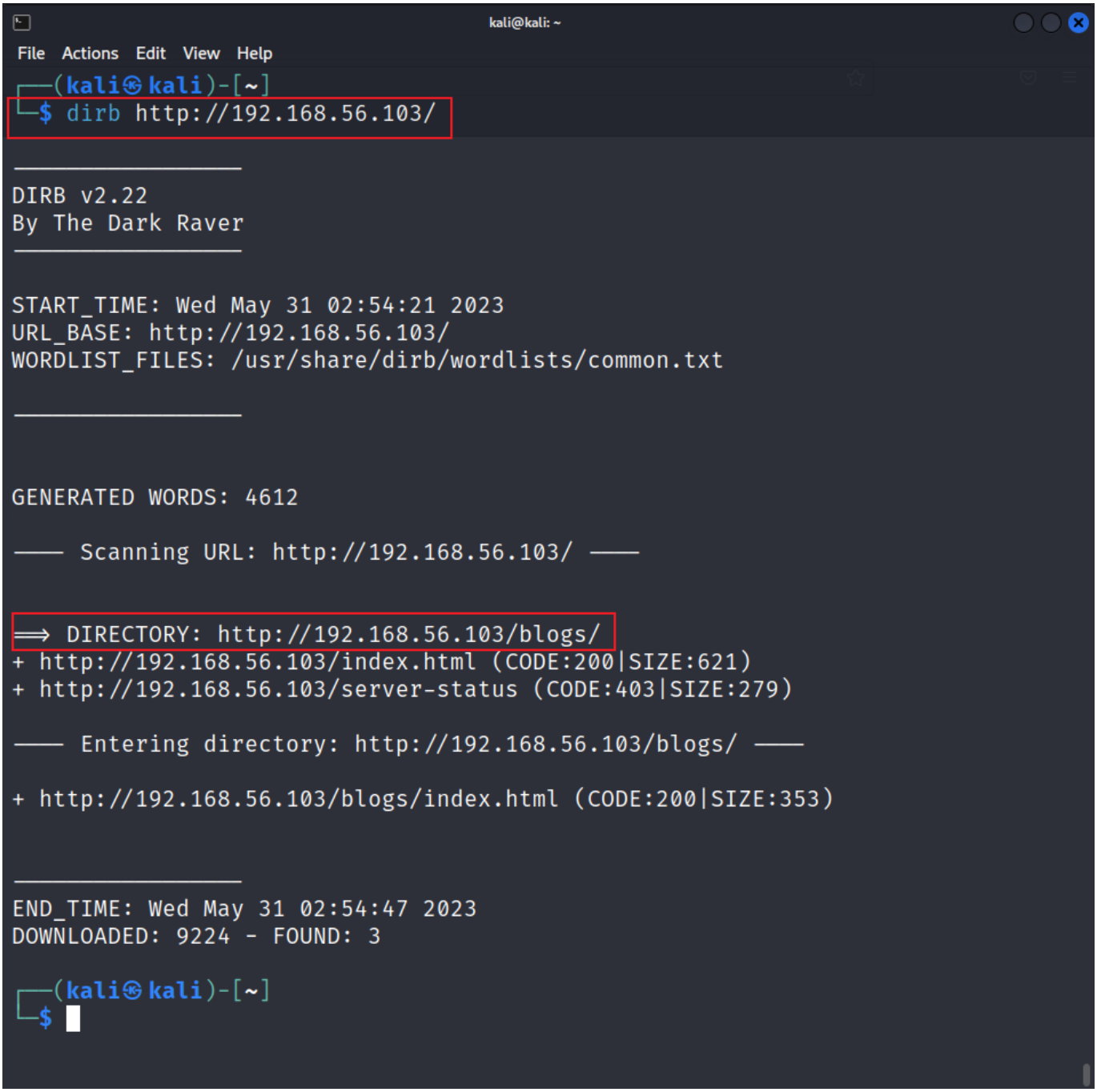


也是毫无收获！

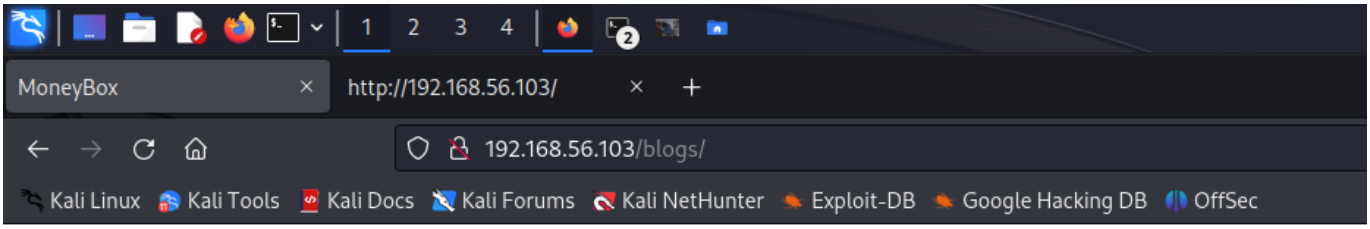
对于这个网站我们还能做点什么？同学讨论

没错，就是网站目录枚举！

```
dirb http://192.168.56.103
```



目录字典跑完，发现3个文件和目录，其中有一个目录是blogs，尝试访问一下



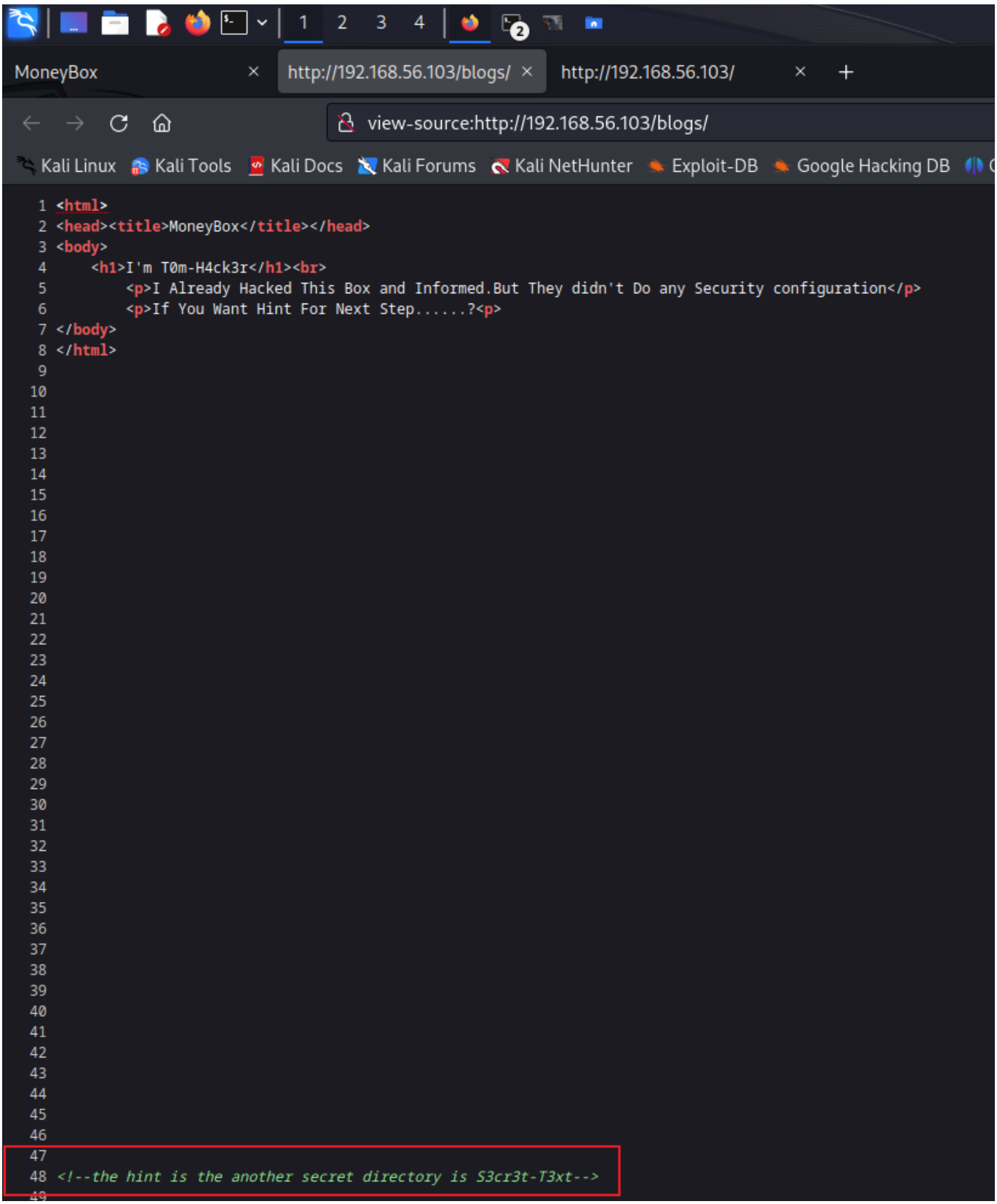
I'm T0m-H4ck3r

I Already Hacked This Box and Informed.But They didn't Do any Security configuration

If You Want Hint For Next Step.....?

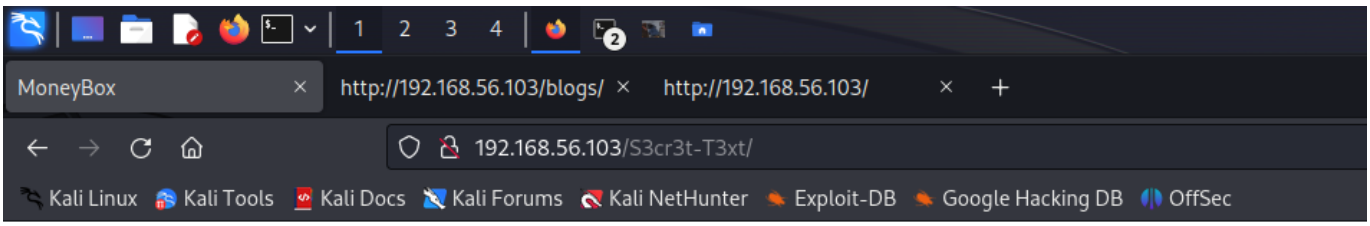
这段话提示我们有人已经成功渗透这台靶机了且通知管理者了，但他们依然没有做任何的加固措施...

查看网页源代码



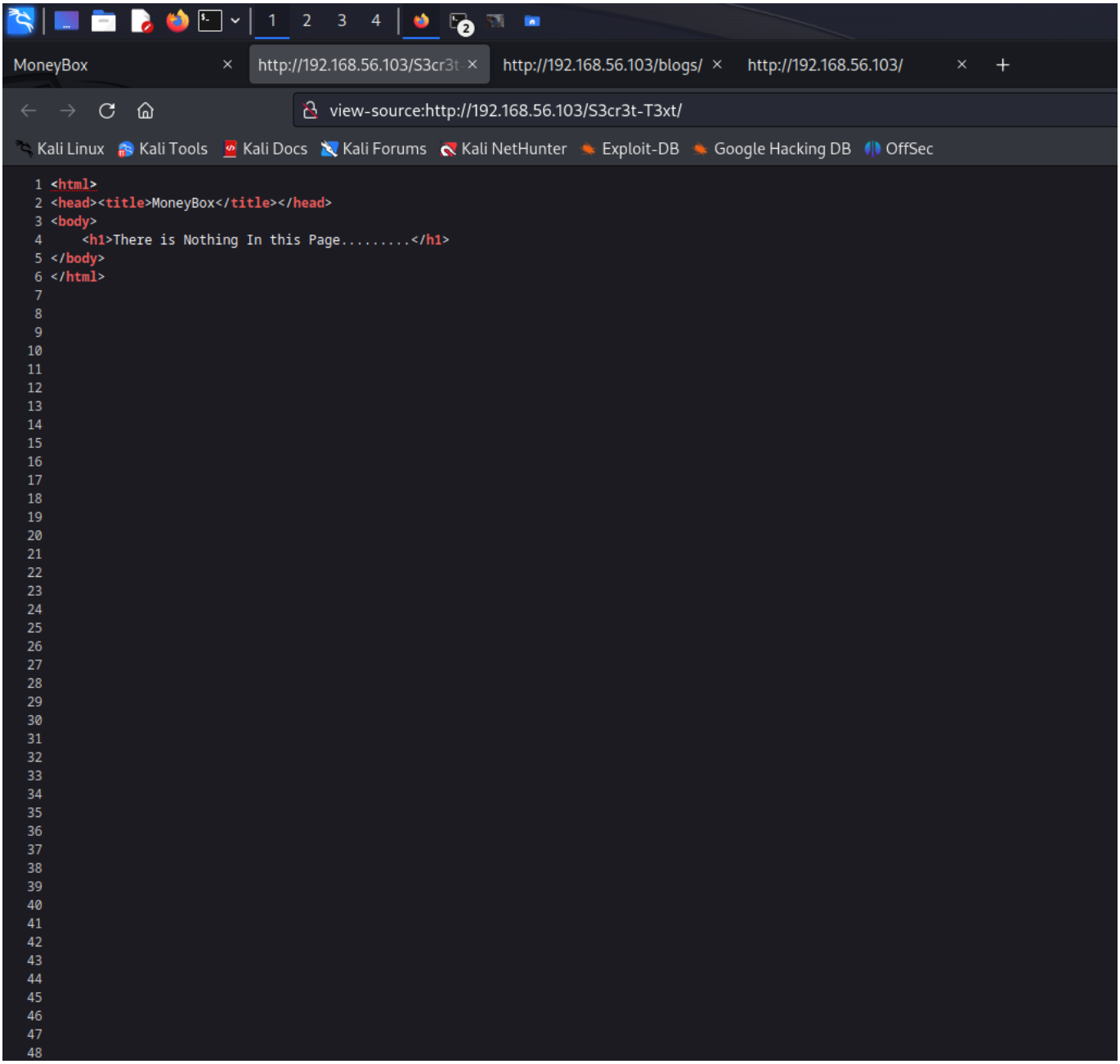
似乎没什么，但在源代码的下方有一行HTML注释

告诉我们有一个隐藏目录S3cr3t-T3xt，尝试访问一下

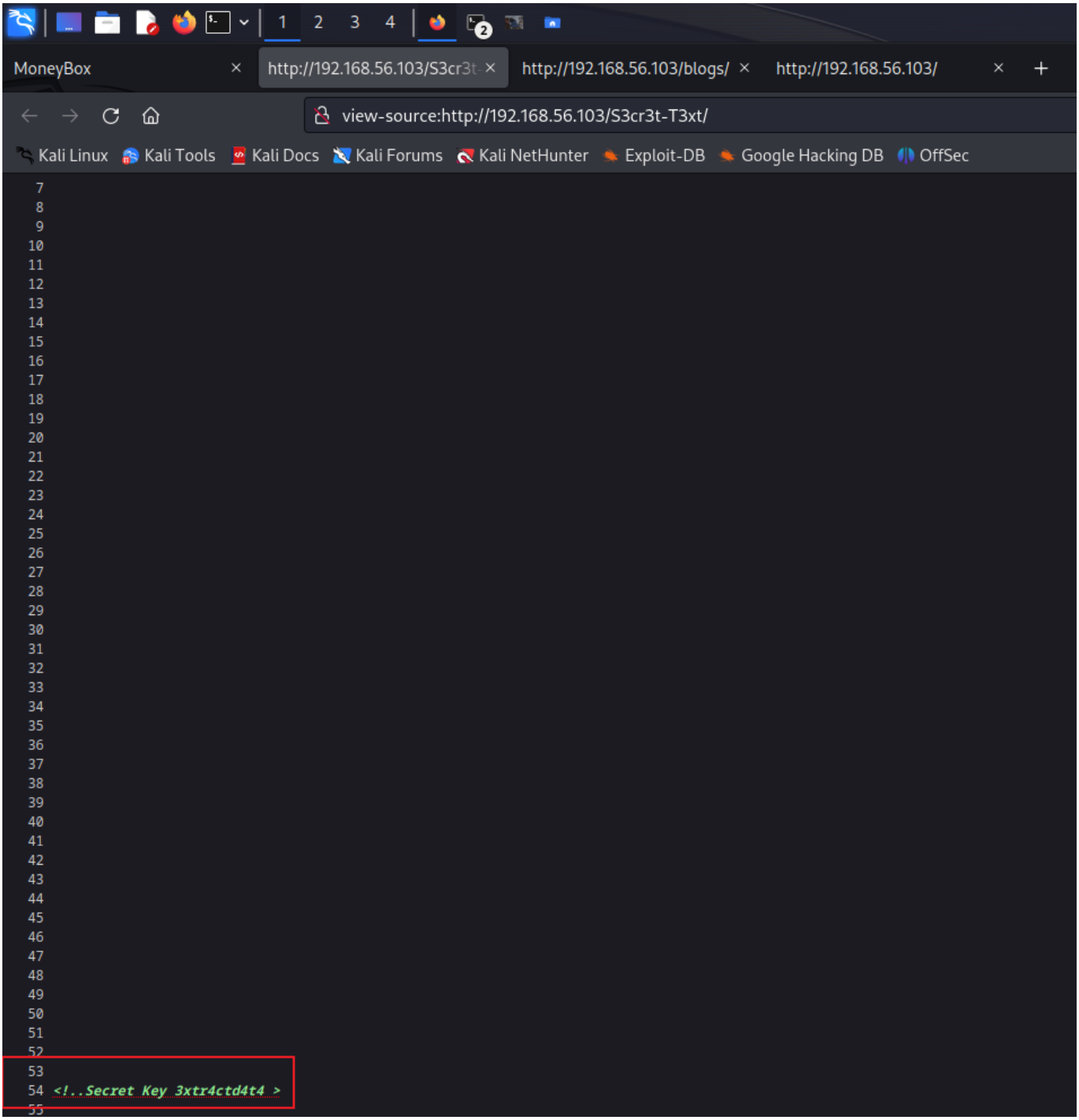


There is Nothing In this Page.....

又是一片干净的网页，继续查看源代码



乍一看，也没什么，但这一溜行号暴露的作者的意图，滚动条继续往下拉

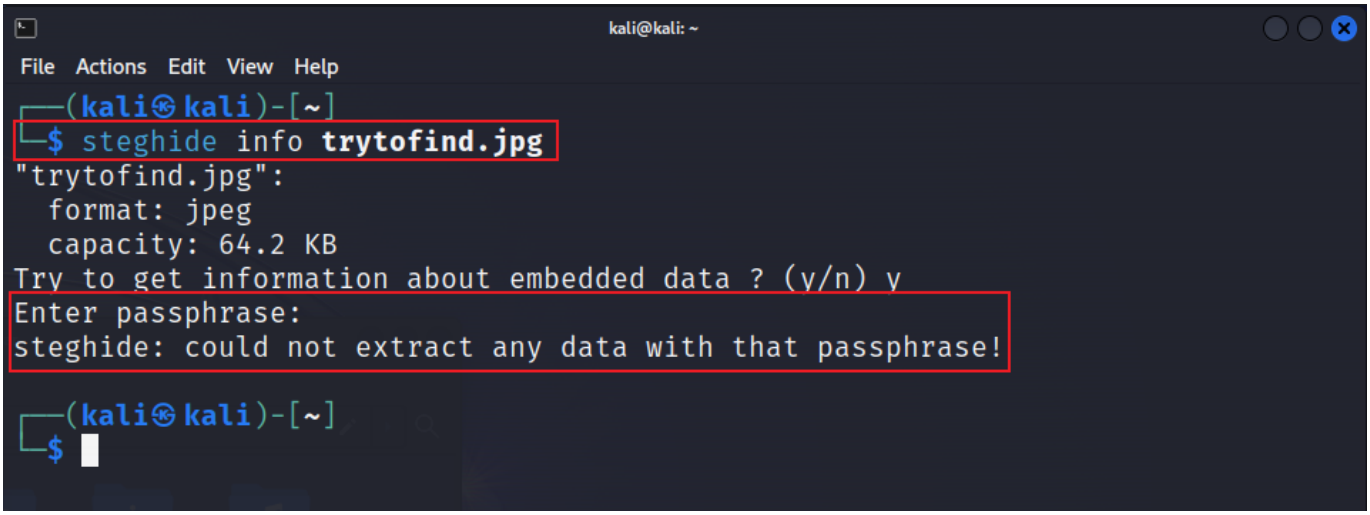


又是相同的配方，熟悉的味道

一把钥匙，做什么用途的?先保存下来再说

讨论：这把钥匙有什么用?

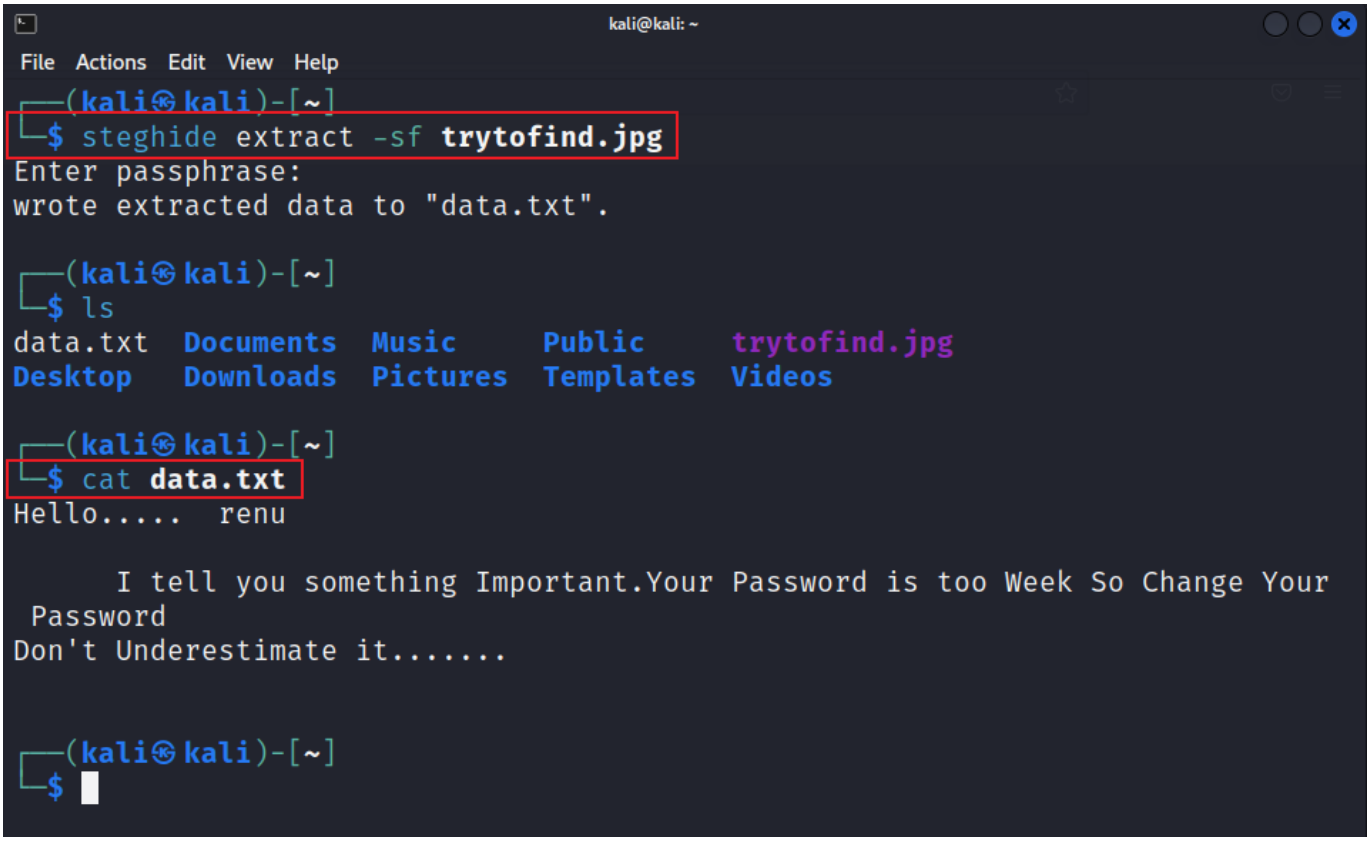
还记得这张滑稽猫图片吗？里面藏了点东西，但是设置了密码



下面利用得到的密码解密图片信息

密码核验通过，里面果真藏了个data.txt。下面继续使用steghide分离出data.txt文件

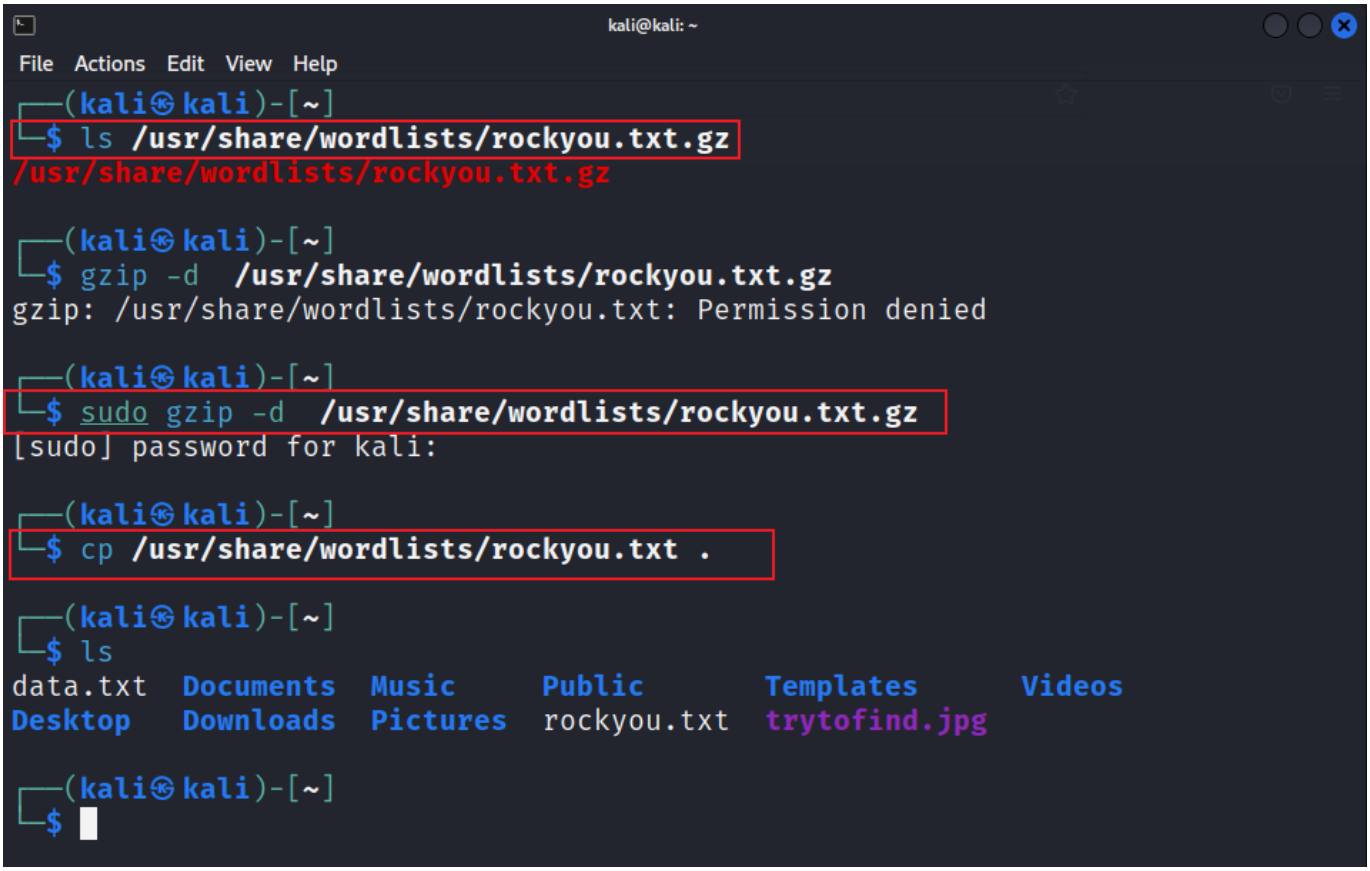
```
steghide extract -sf trytofind.jpg
```



成功分离出data.txt，查看文件内容，得知系统中可能存在renu用户，且其密码为弱密码。

那自然想到了基于renu用户名的密码爆破。

密码字典呢？既然是弱密码，那一般的密码字典应该就可以，请出kali linux自带rockyou.txt.gz

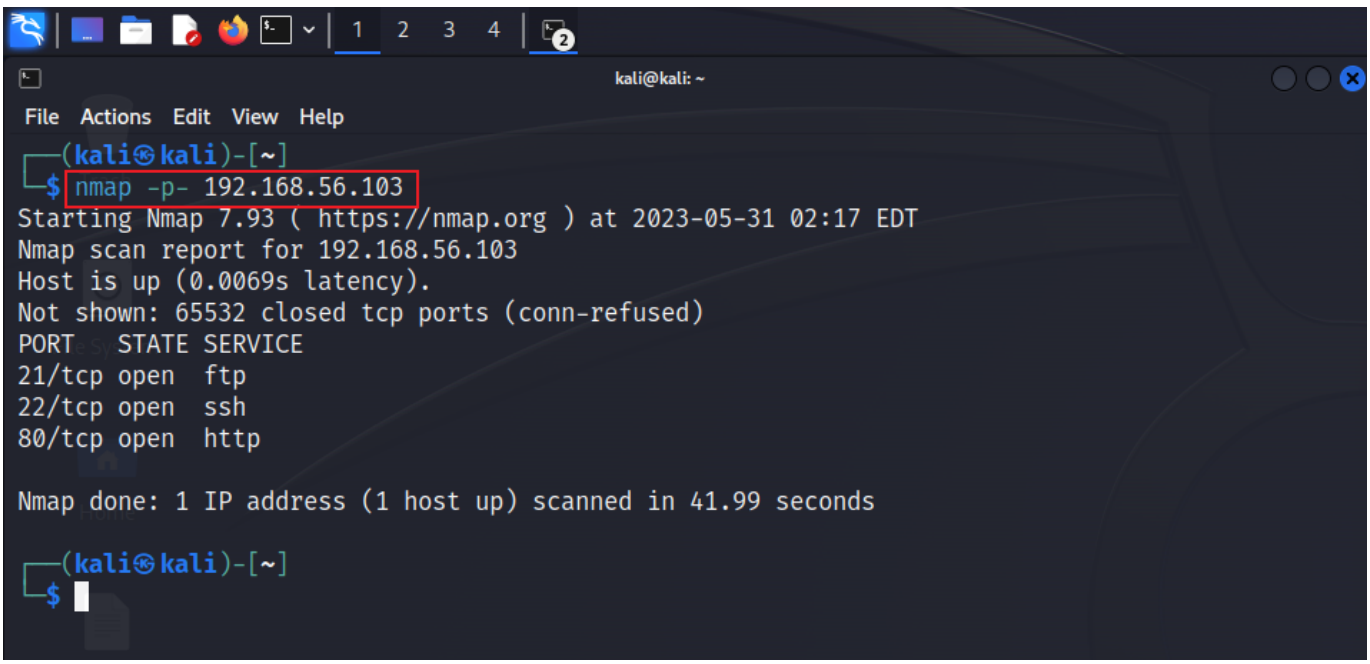


将rockyou.txt.gz密码字典解压，然后拷贝到当前目录

讨论：有了用户名和密码字典后，如何爆破呢?

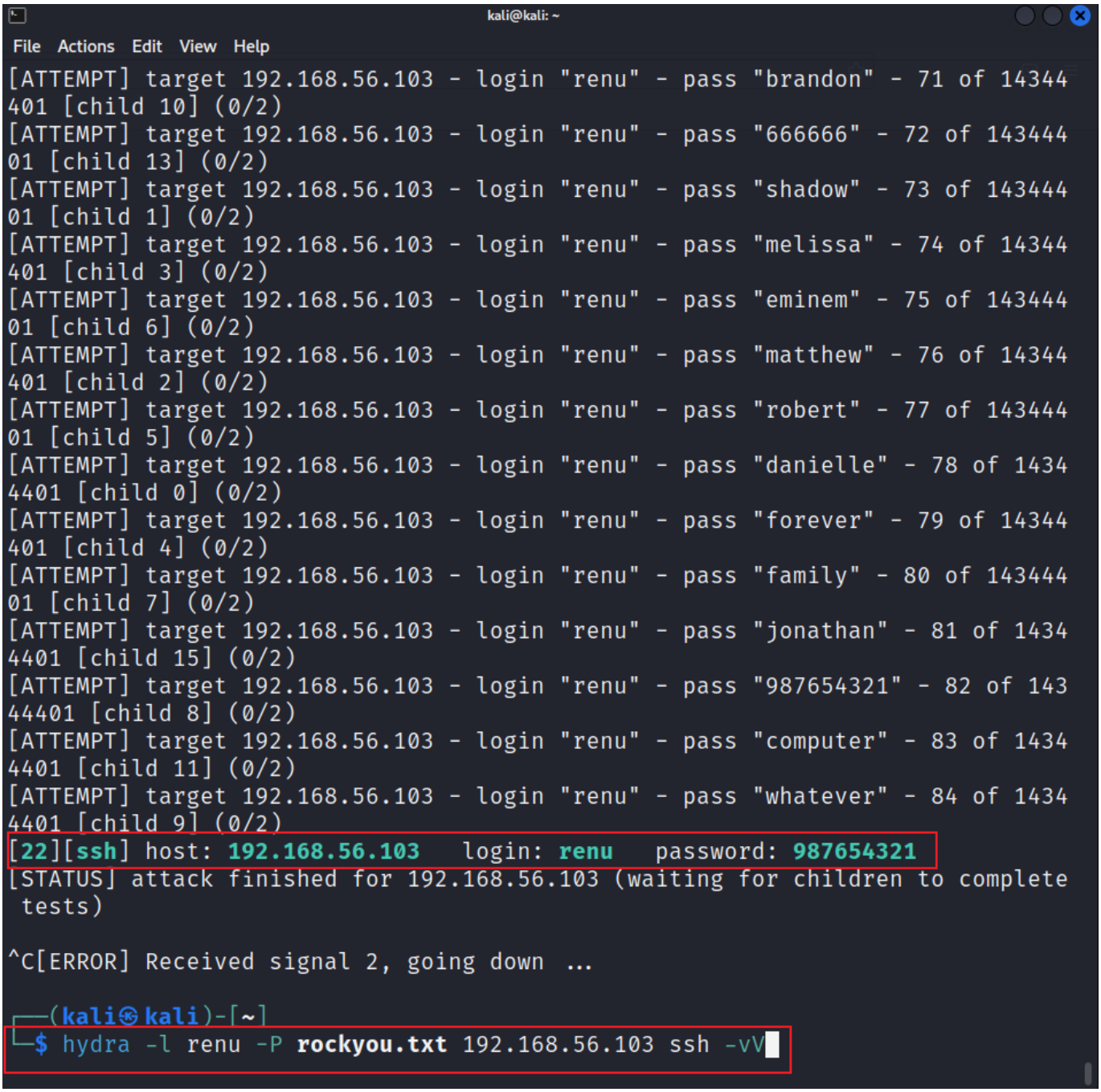
总结：用户名密码爆破的前提是靶机系统有一个开放的服务，访问它时需要身份验证，这样我们结合爆破工具和字典文件才有爆破成功的可能性。

3）是不是靶机还开有22端口



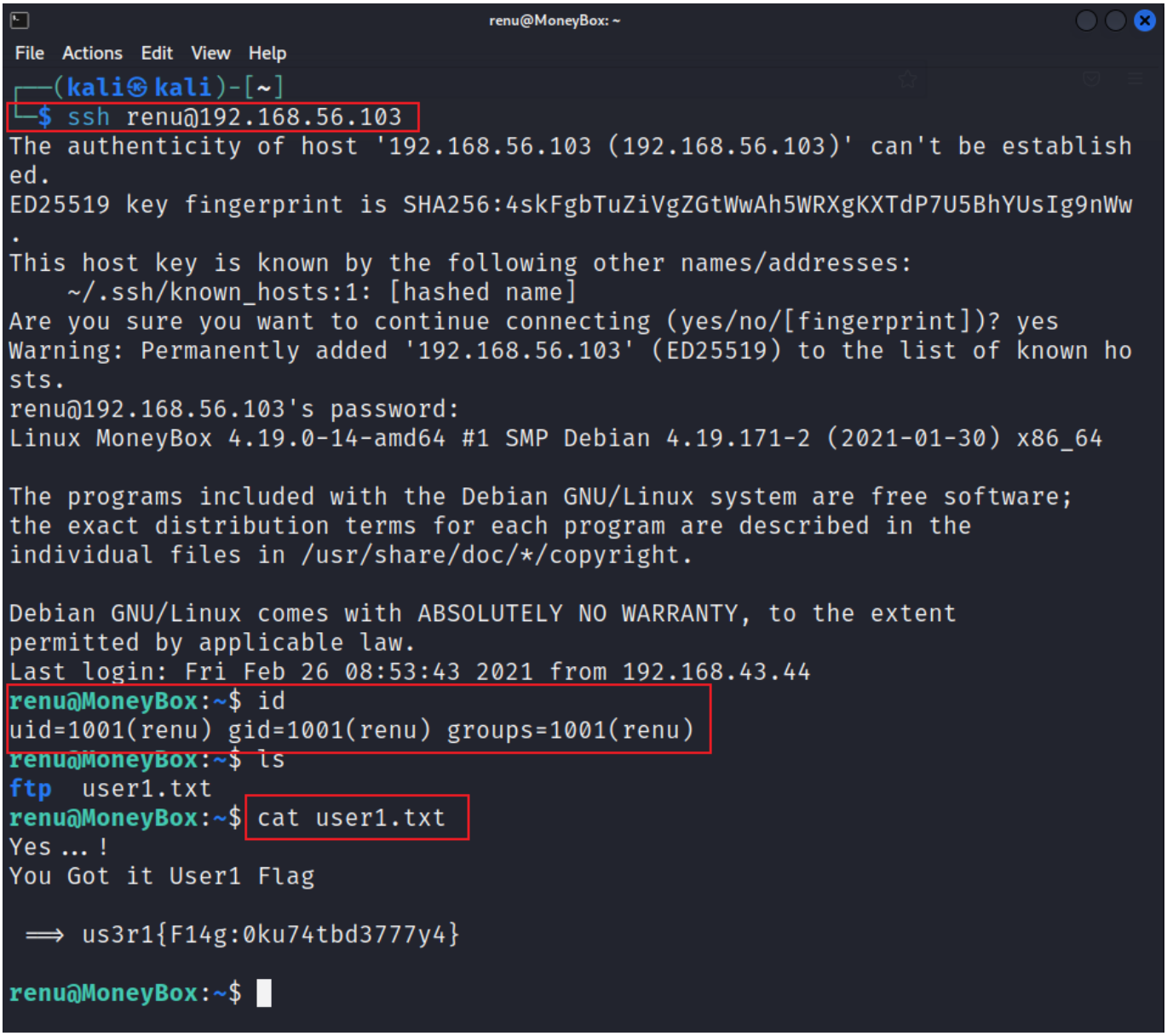
下面我们使用hydra工具开始爆破

```
hydra -l 用户名 -P 密码字典文件 靶机IP 协议 -vV
```



爆破成功，得到renu用户的密码为987654321。

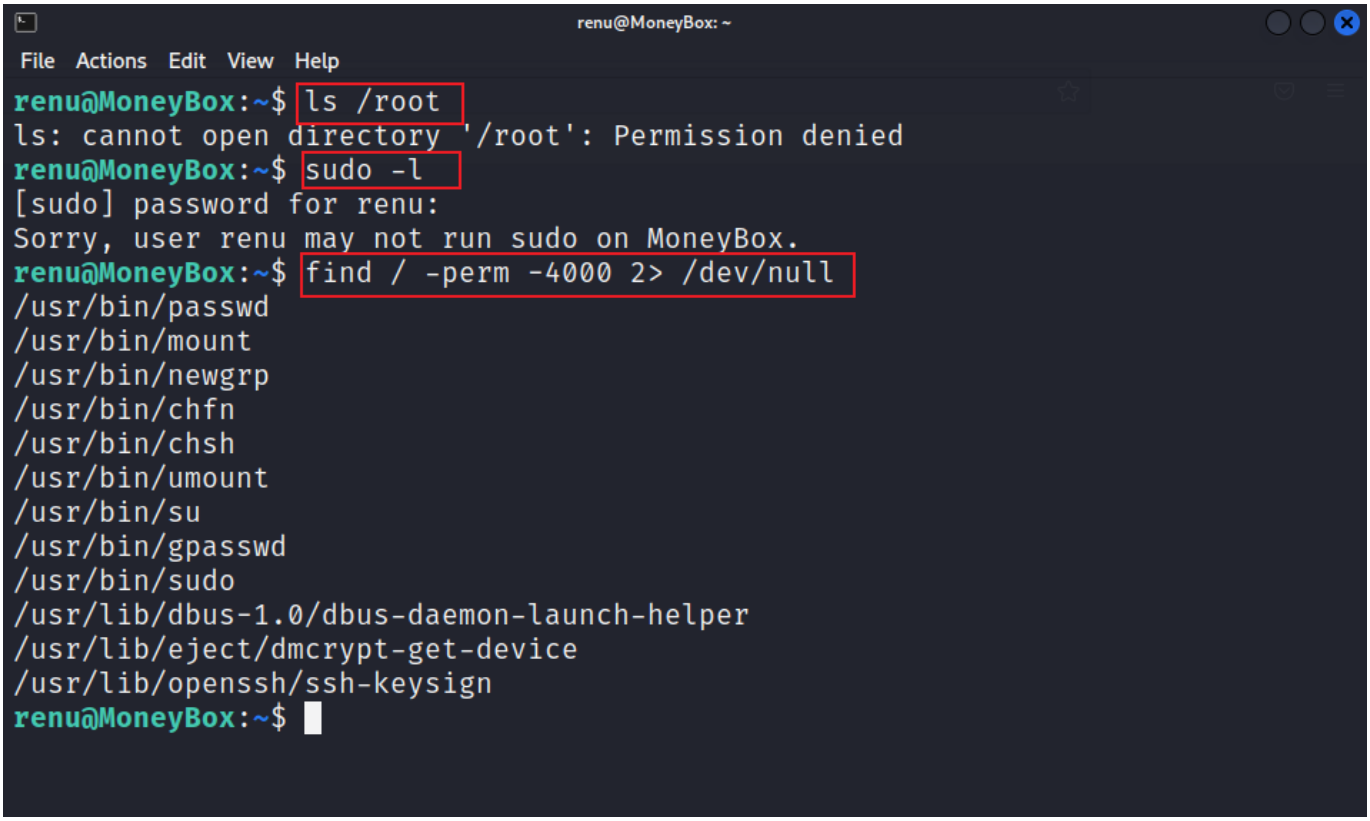
接下来就通过SSH服务用renu用户及其密码登录靶机。



renu用户能够登录，至此，我们已经突破了靶机的边界，拿到了靶机的Shell控制权。

前面提到这台靶机有3个FLAG，那么还有2个FLAG。

5、漏洞提权

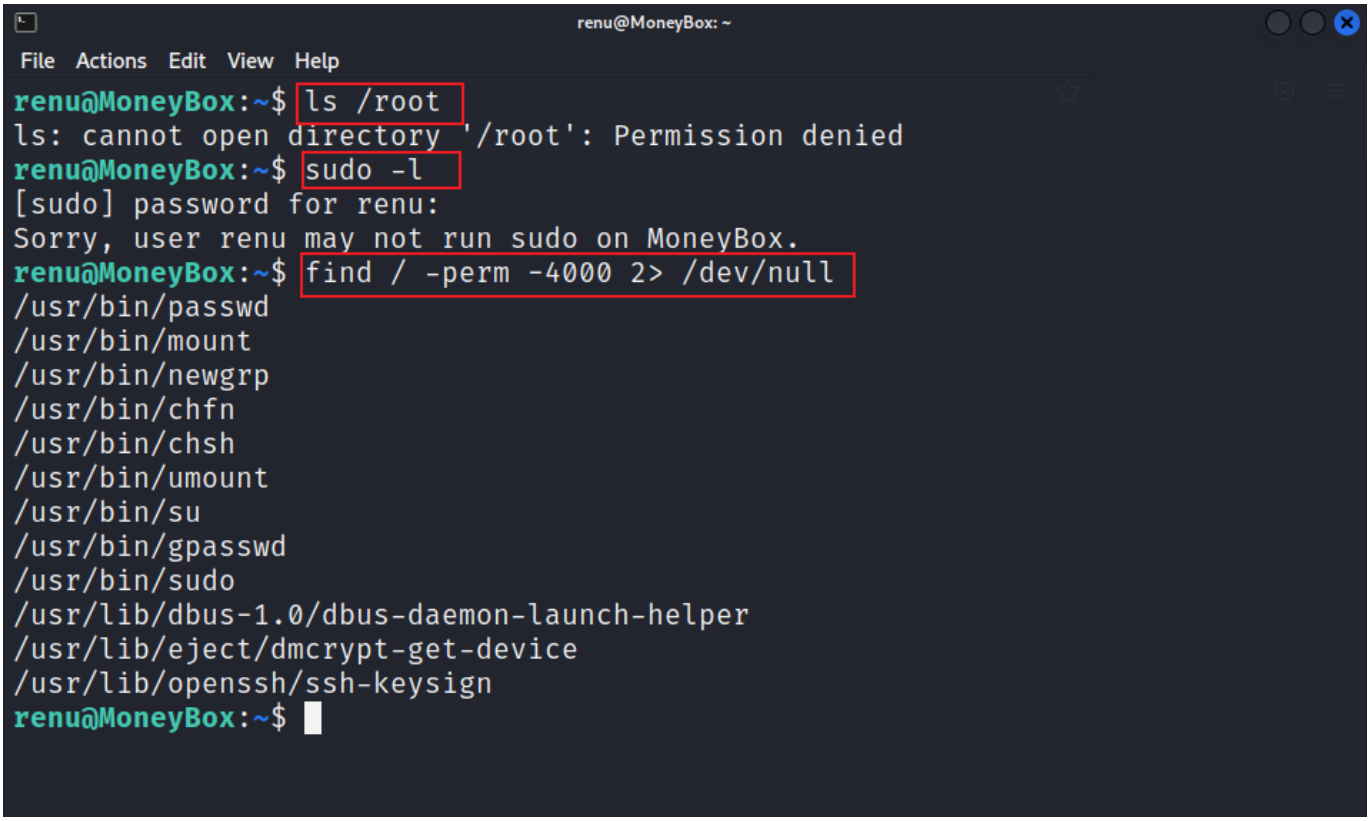


尝试访问root家目录，提示权限不足。

讨论：

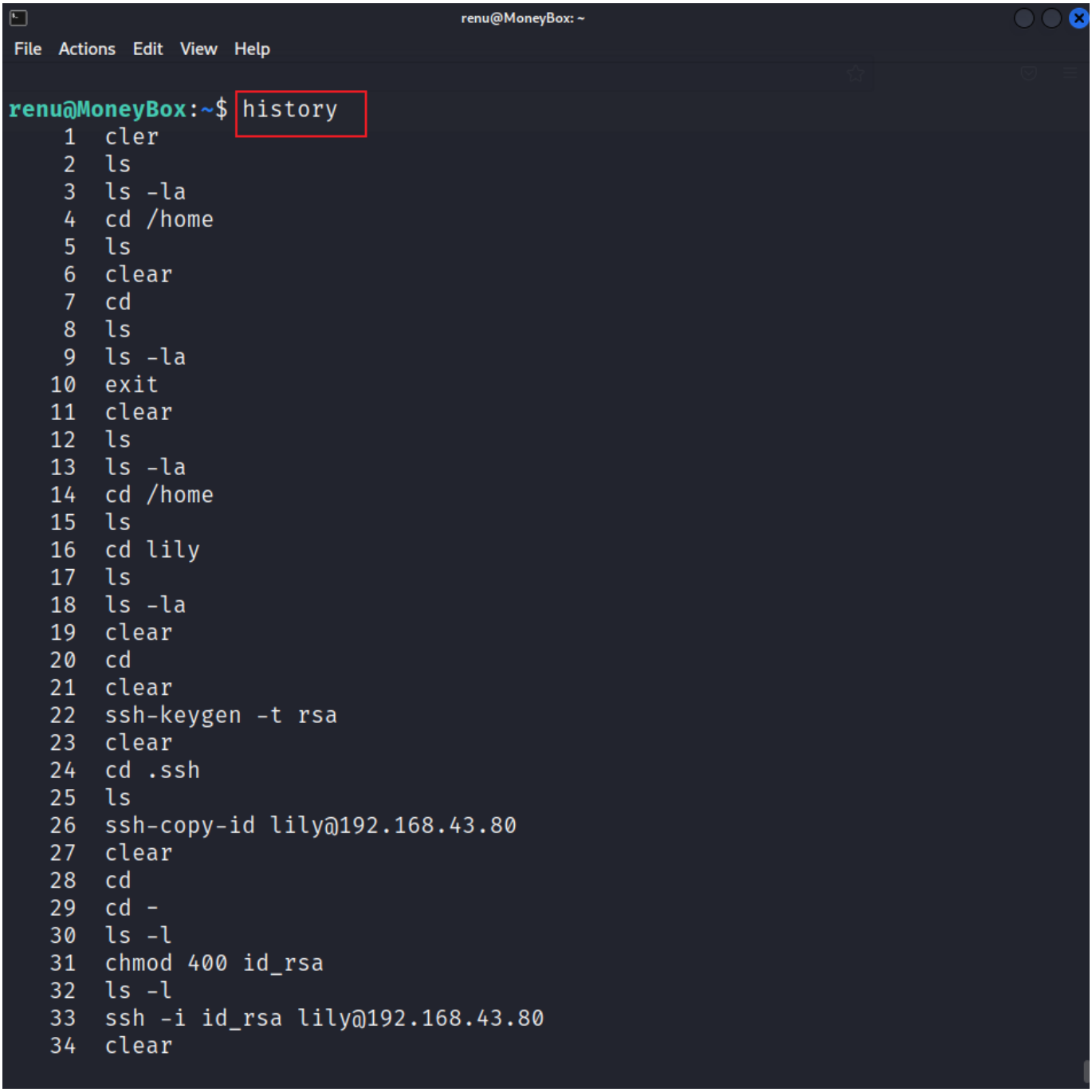
linux系统一般有哪些提权方式呢?

总结：Linux系统提权可能通过以下方式：sudo权限提权，suid提权



发现靶机这2种提权方式都行不通。

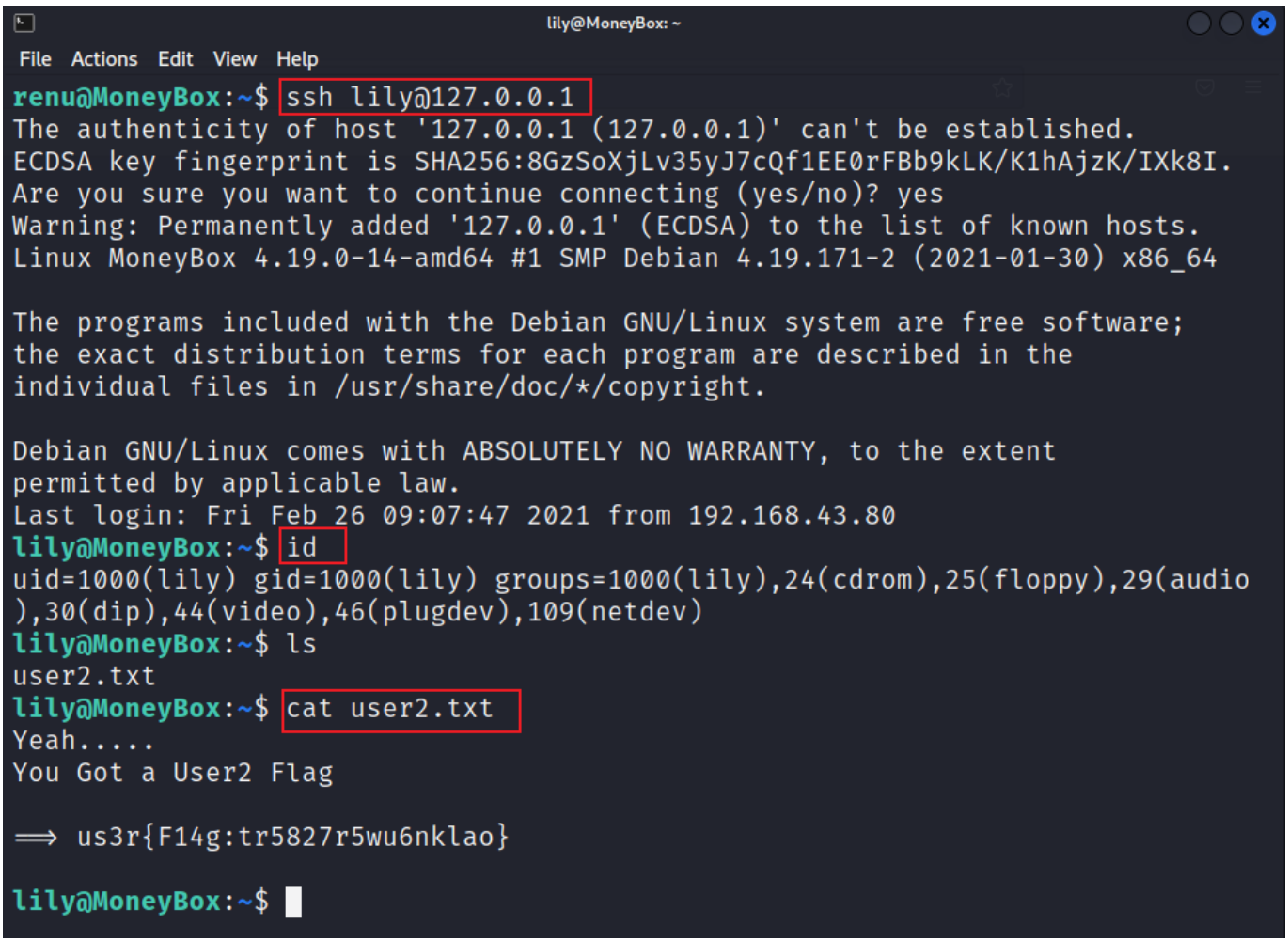
经过一番摸索和实验，发现renu用户的命令历史记录存在SSH免密登录，这似乎有突破的可能。



也就是说renu用户将自己的公钥拷贝到了靶机系统上的lily用户家目录的authorized_keys文件，从而可以不用密码就以lily身份登录到靶机上。

发现确实renu用户的公钥已经拷贝到lily用户家目录的ssh免密授权文件authorized_keys中。

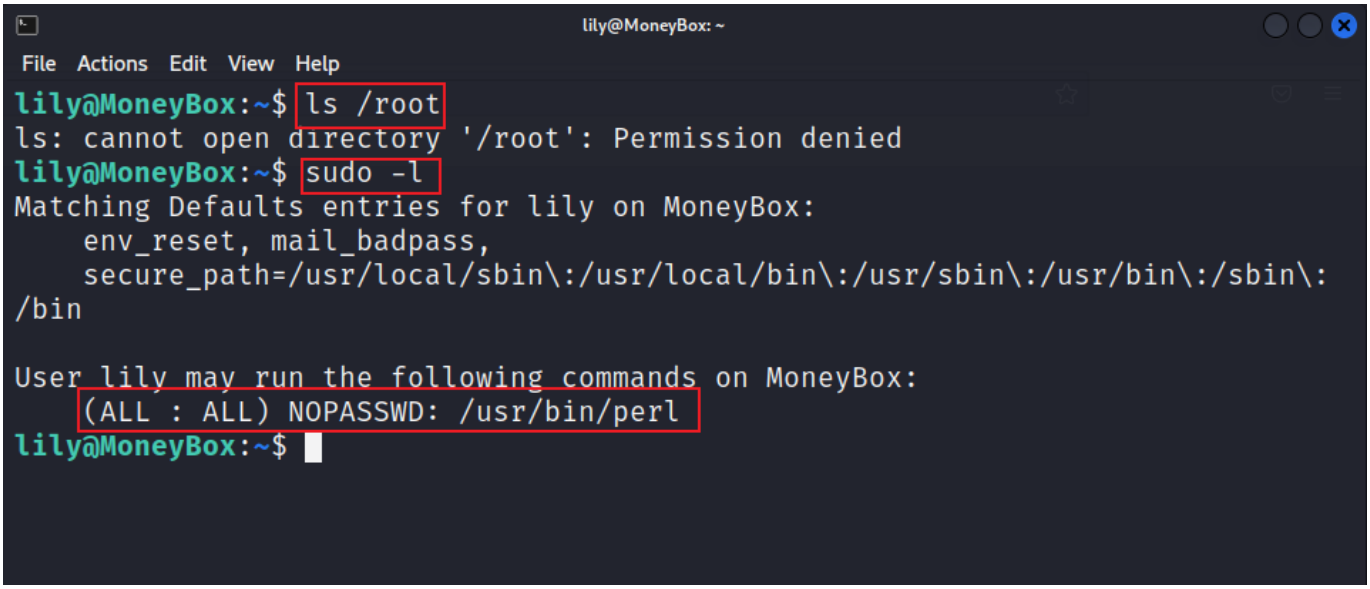
接下来思路就清晰了



renu用户成功以lily身份免密登录靶机，拿到Flag2。

还差最后一个FLAG，那应该是在root家目录了。

访问/root家目录，任然是权限不足，还需要提权到root身份。



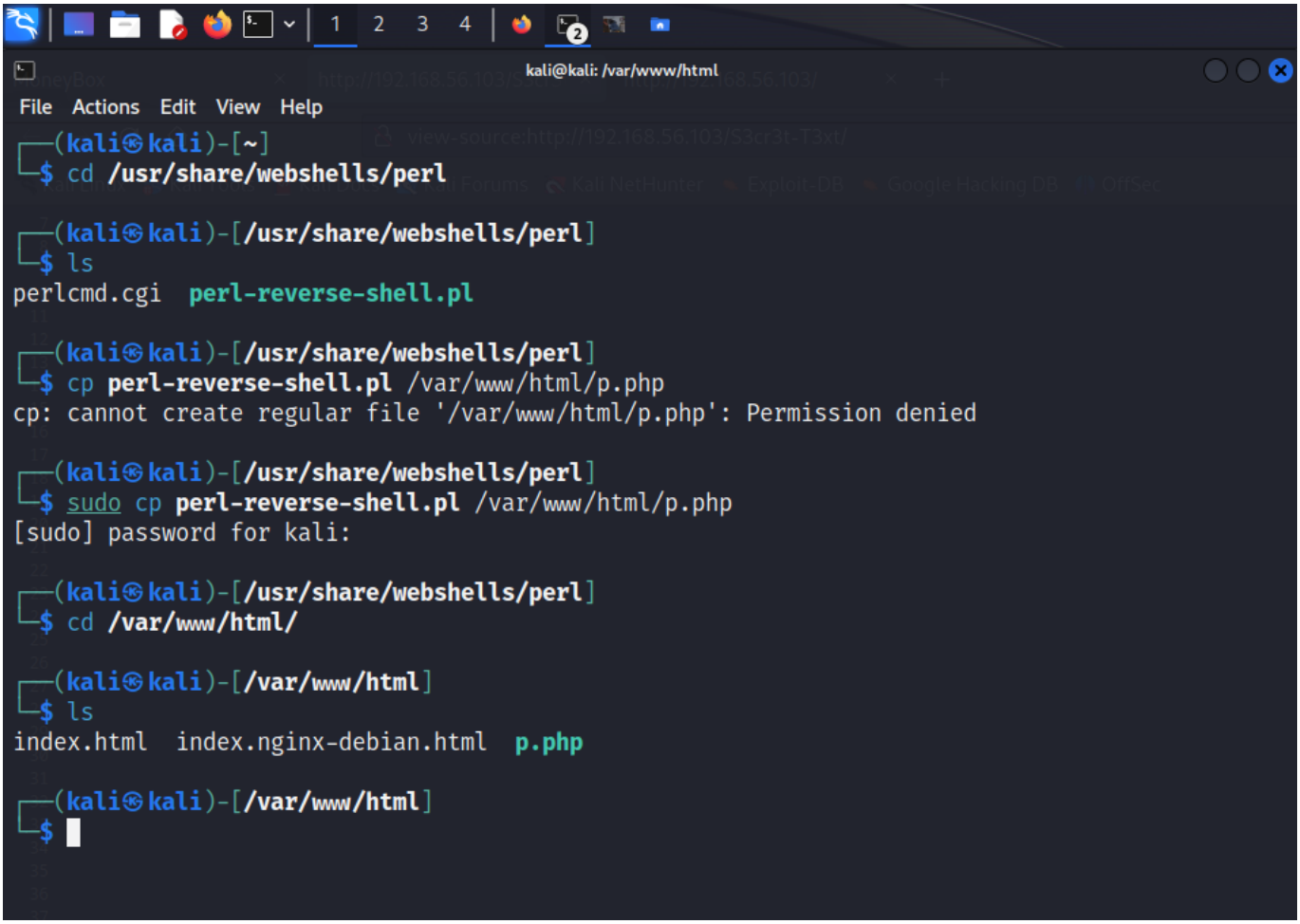
执行sudo -l发现该用户存在sudo赋权，程序为/usr/bin/perl，perl同python类似，也是一门解释型语言，推测靶机应该有perl运行环境。

下面是如何通过Perl程序提权的实现过程。

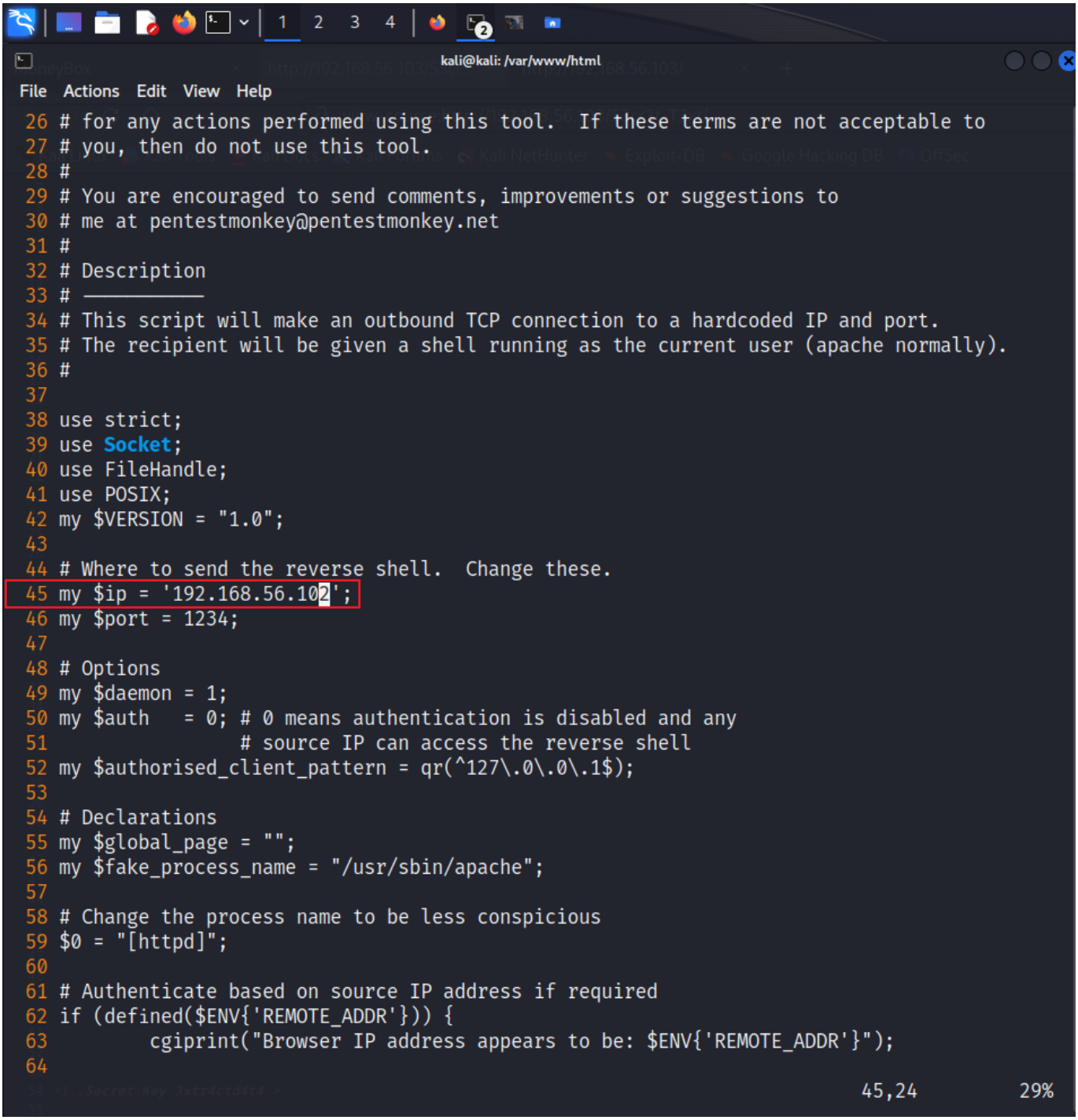
思路：kali中自带perl脚本反弹shell，将其略加修改拷贝到靶机上；该脚本需要在渗透机监听一个端口(默认为1234)，然后在靶机上运行perl脚本，靶机会自动反弹一个shell到渗透机，从而通过运行perl程序获得一个管理员的Shell。

实现步骤：

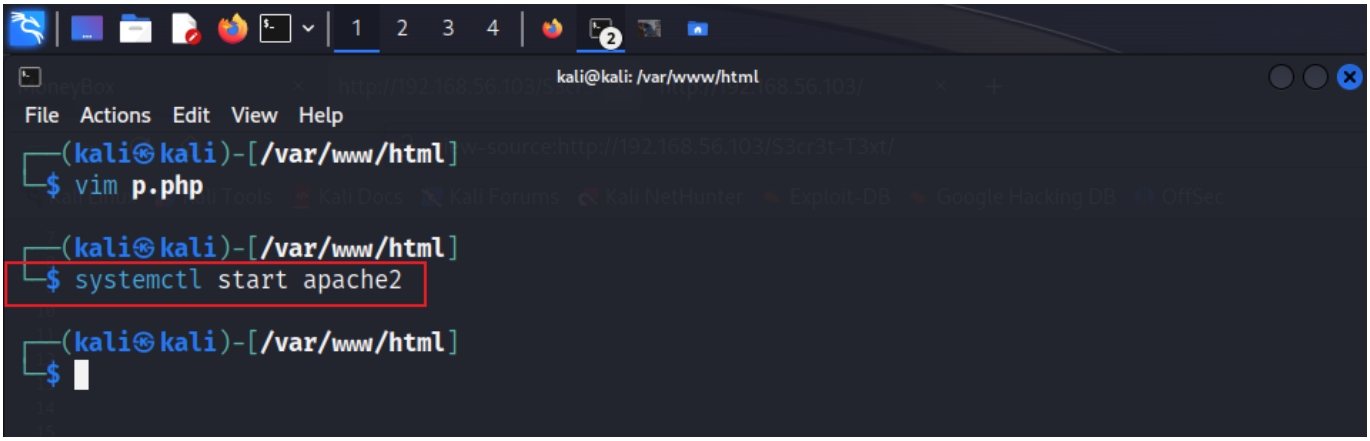
1）定位kali中的perl脚本反弹shell，将其拷贝到kali的/var/www/html下，重命名为p.php；



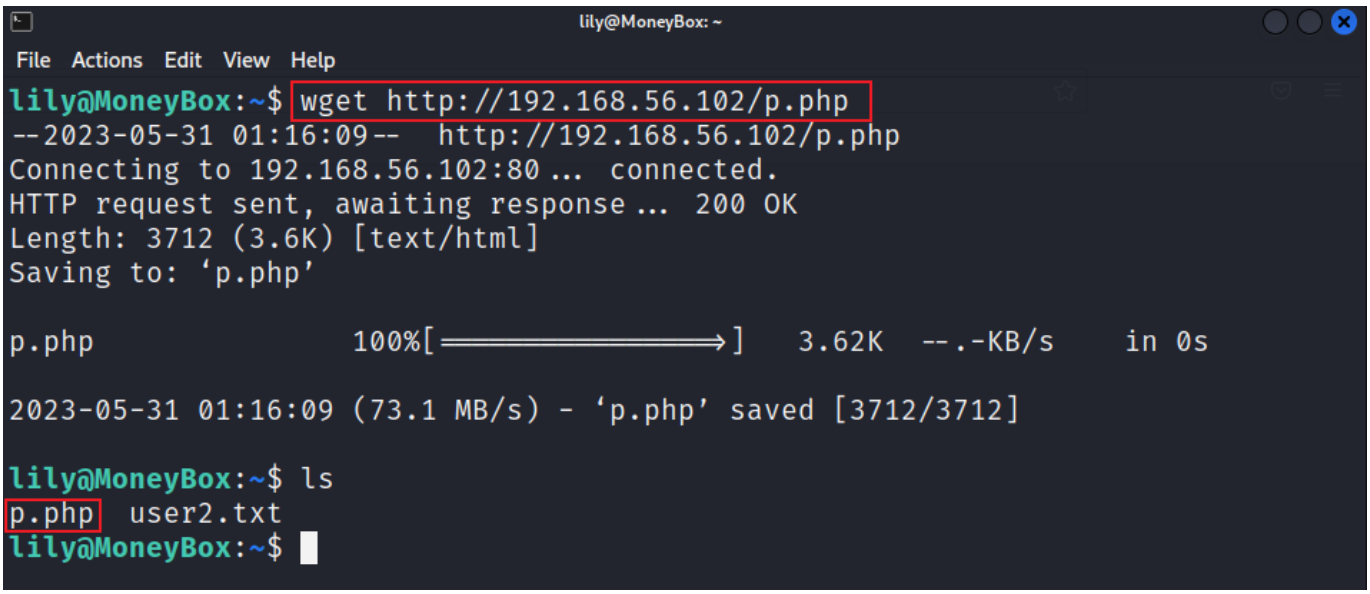
2）修改p.php文件内容，将反弹连接的Ip地址改为kali的IP；



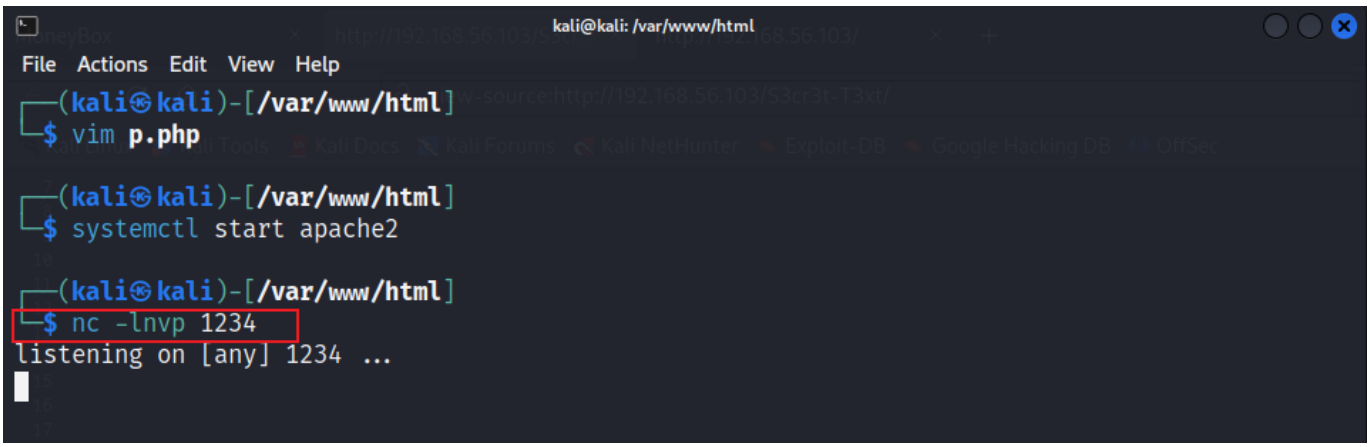
3）开启kali的网站服务；



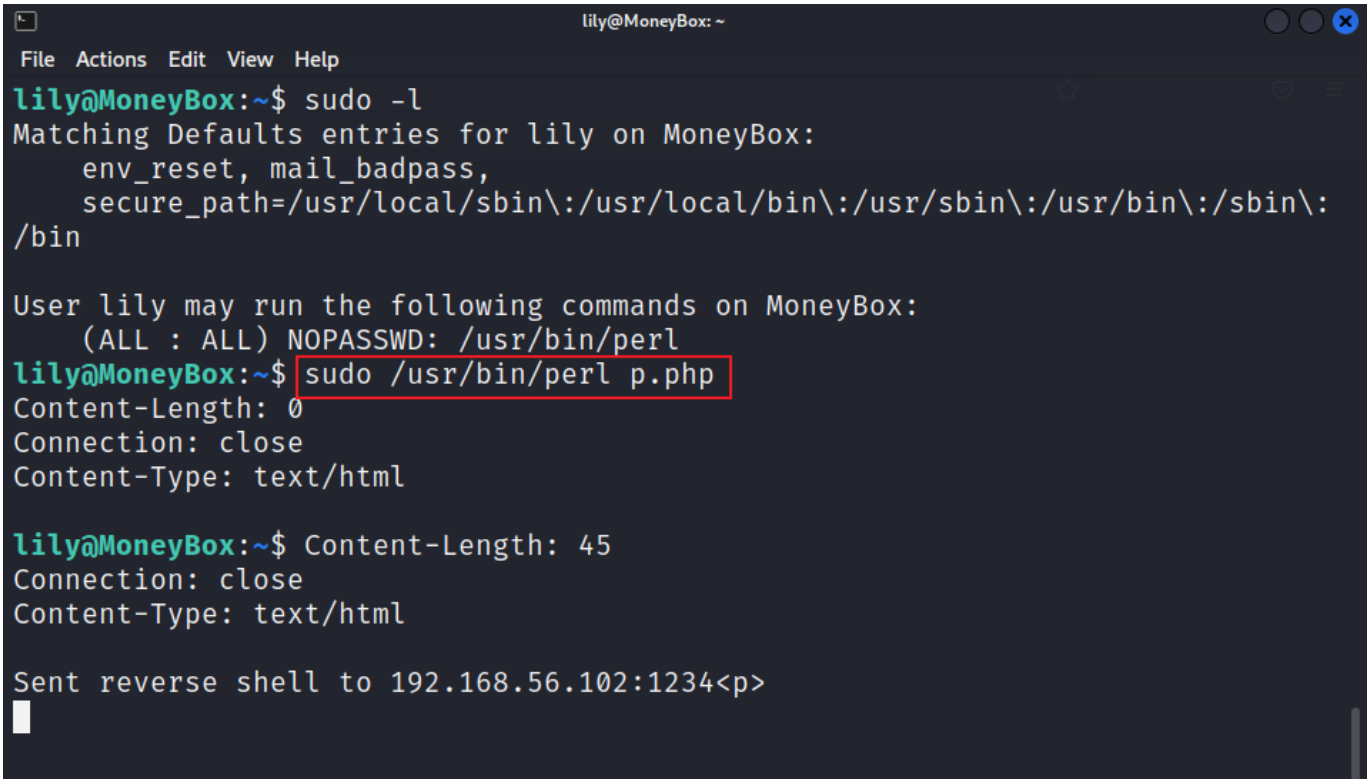
4）切换到靶机lily会话，通过http协议下载p.php



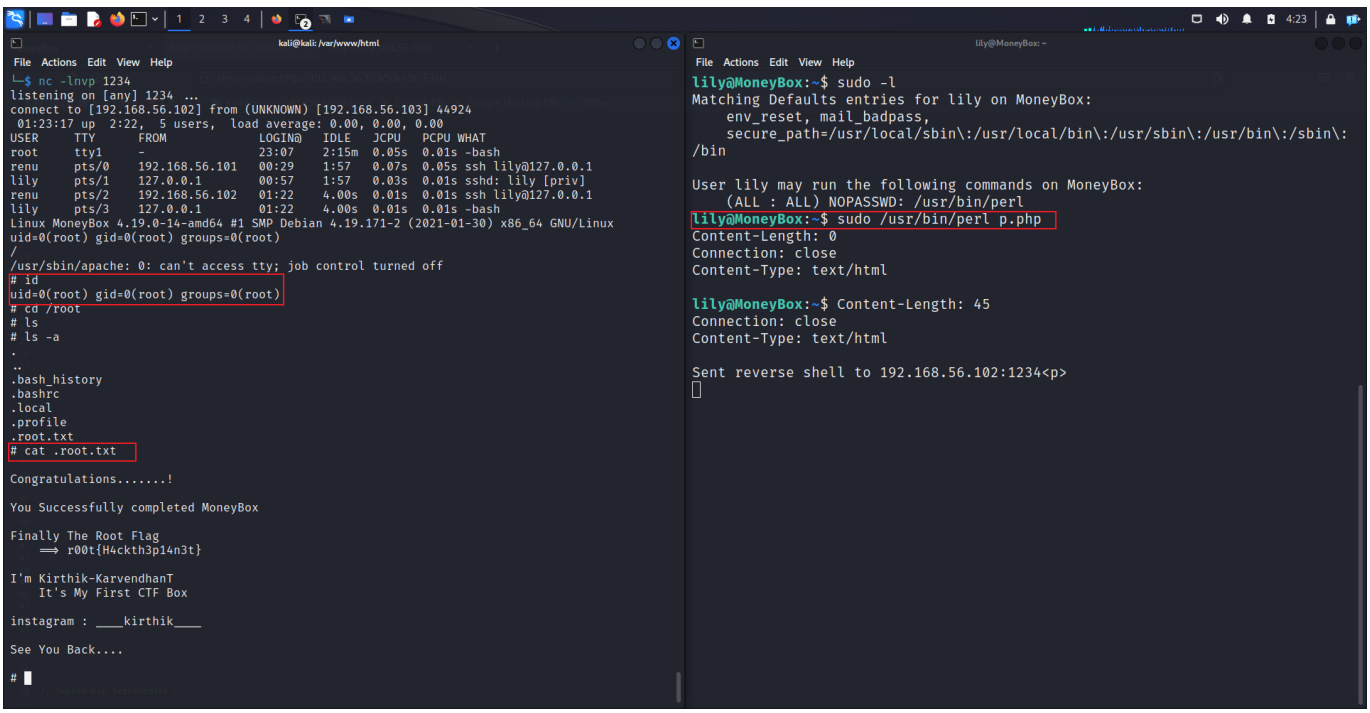
5）kali 通过nc命令监听1234端口



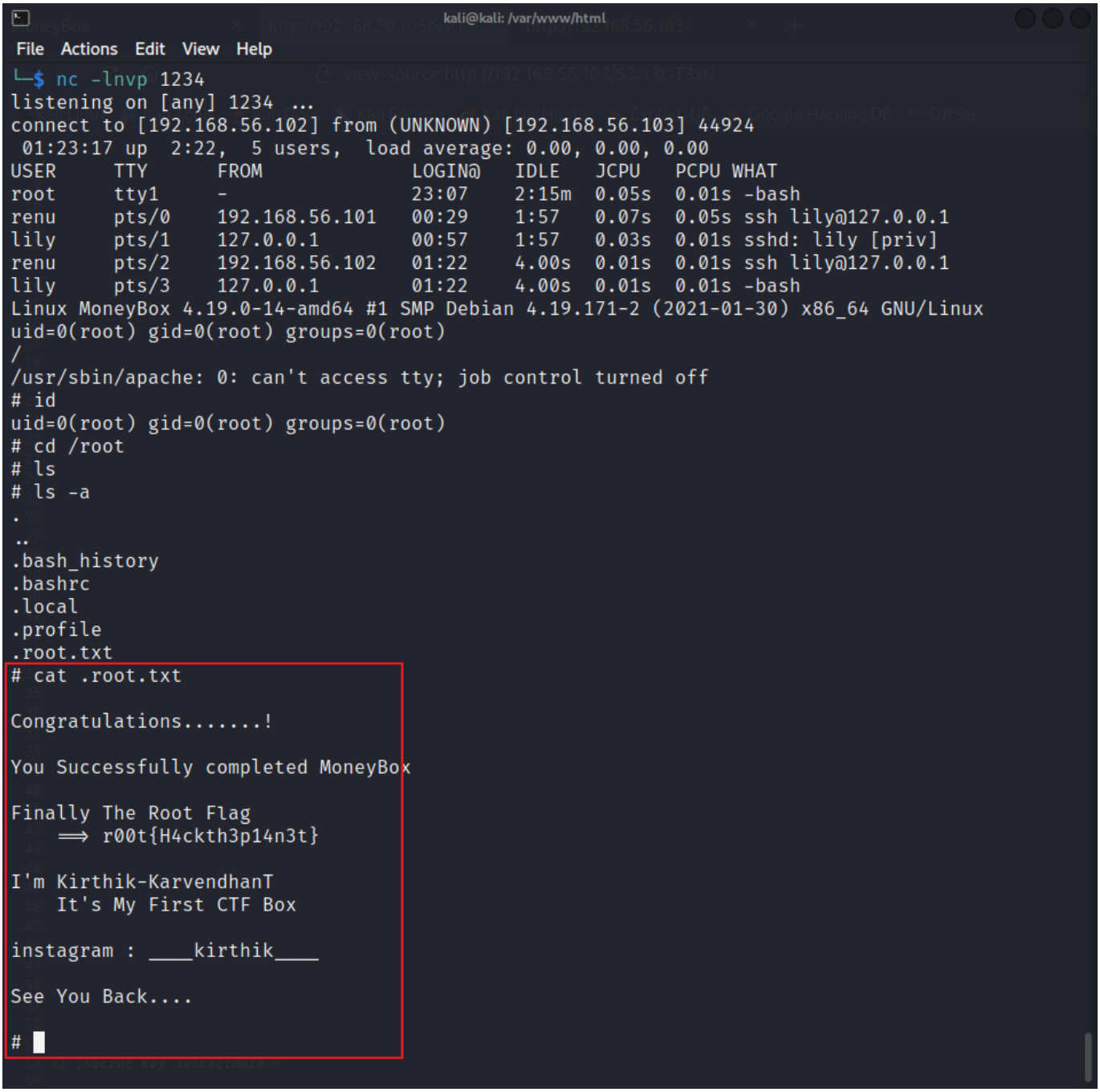
6）靶机上通过sudo 运行p.php程序



7）切换到渗透机kali，成功反弹管理员权限shell



8）提权成功，拿到最终Flag!



至此，moneybox靶场渗透工作完成！

该靶场难度并不高，但其中的知识点并不少，同学们须要独立完成该实验，并在实验后梳理一下整个渗透过程，好好揣摩一下渗透过程中用到的技术和知识。再见！