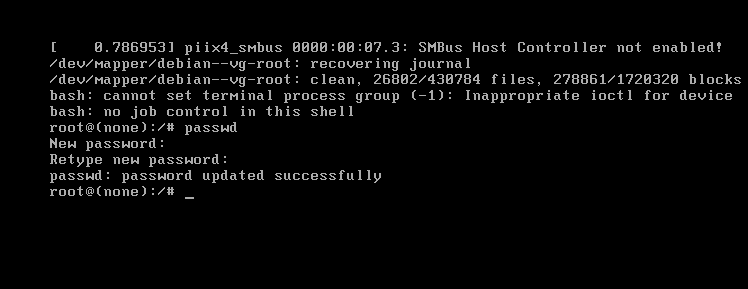
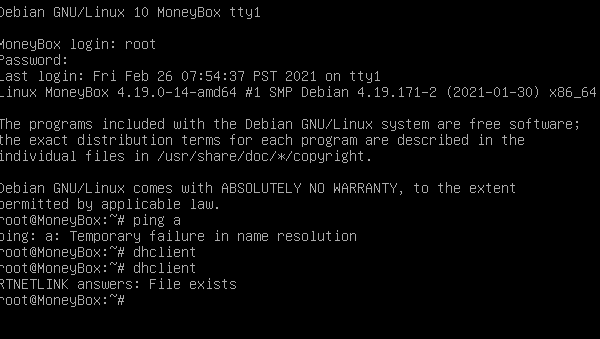
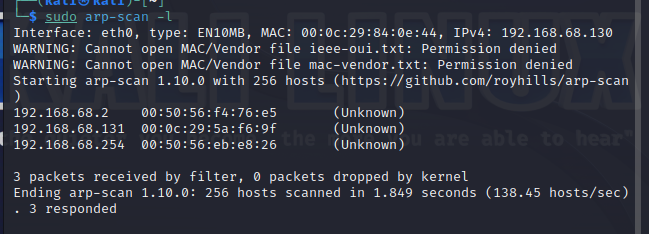
MONEYBOX



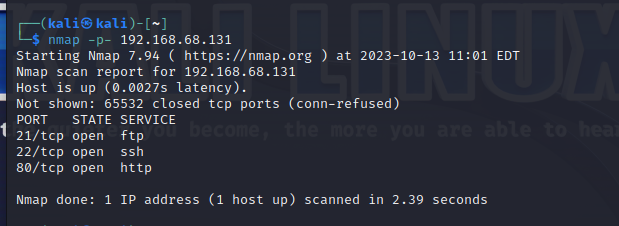
修改密码



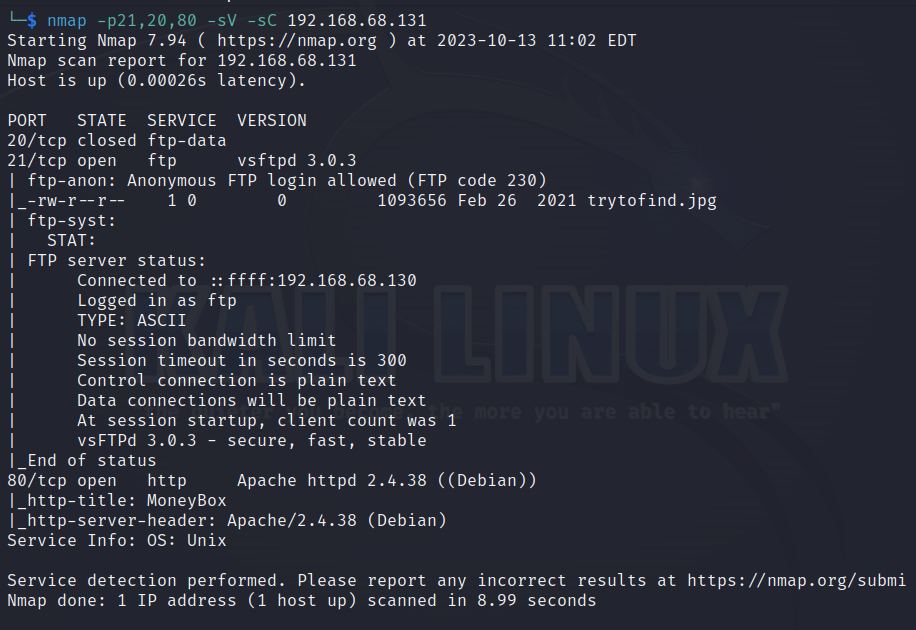
自动获取ip



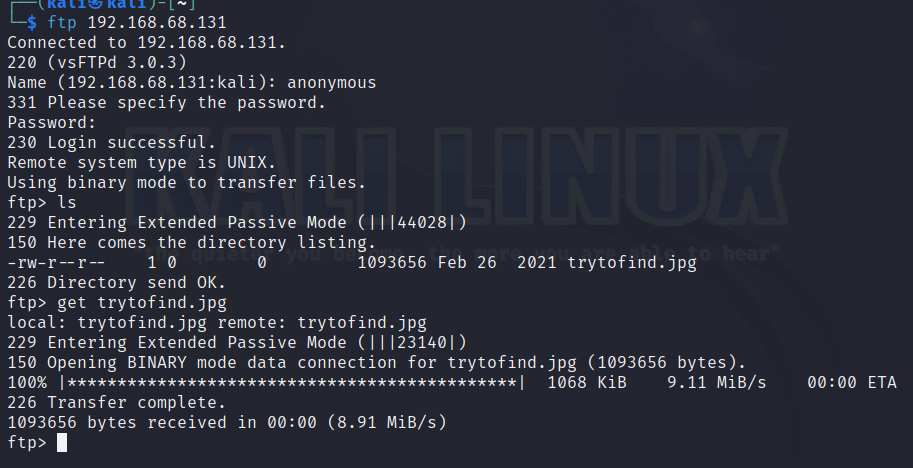
探查靶机



全端口扫描



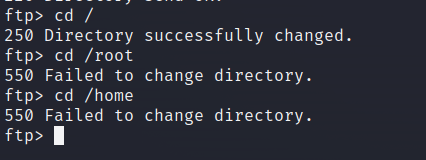
利用kali自带的漏洞探测器进行探测



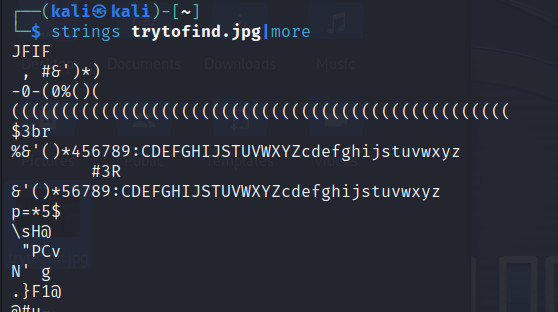
先尝试通过21端口进行渗透，这里利用匿名登陆，查看文件夹后发现一张图片，将其下载至kali目录。



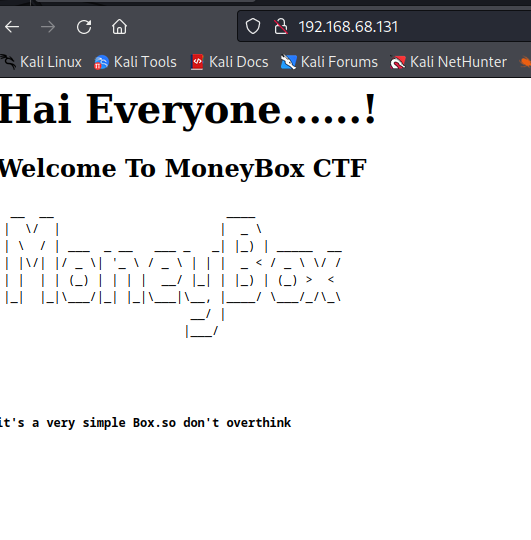
很可惜，我们暂时无法从图片上直接提取到有用的信息。



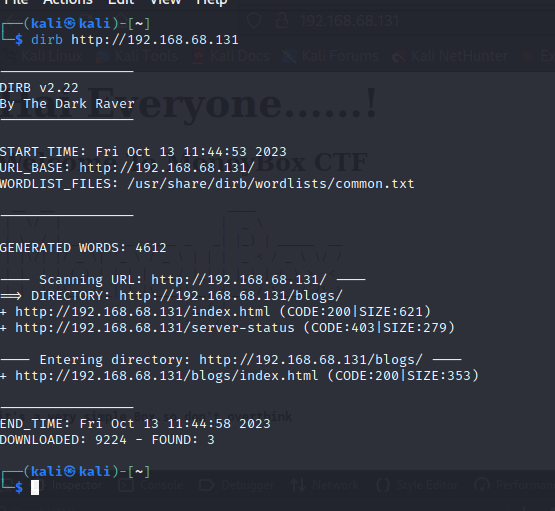
尝试切换至其他目录，可惜被限制无法跳转目录



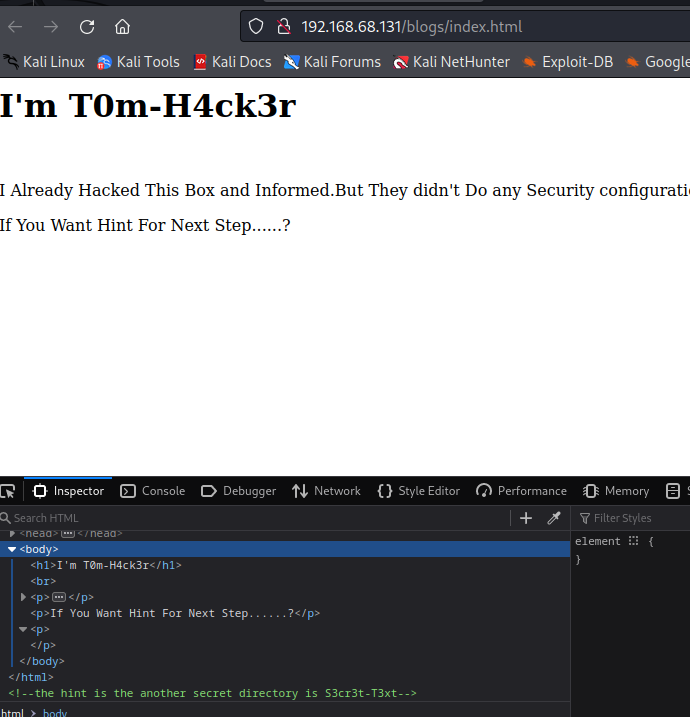
利用strings工具查看该图片中的可打印字符，这里可以看到很多个((((这是不正常现象，因此进行更深入的探测，但很可惜被加密了，暂时无法登入。



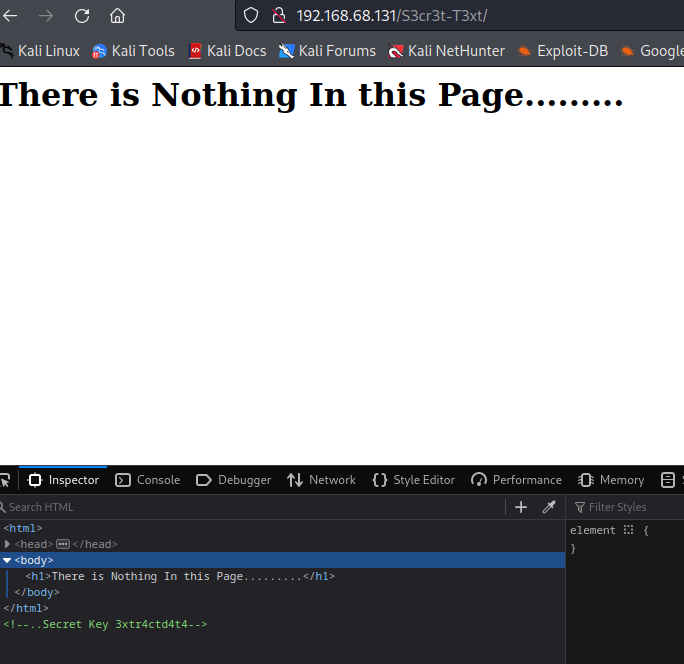
接下来我们来尝试对22端口进行渗透，初步看其没什么东西，这里进行网站目录枚举



这里也是成功枚举出了两个新目录

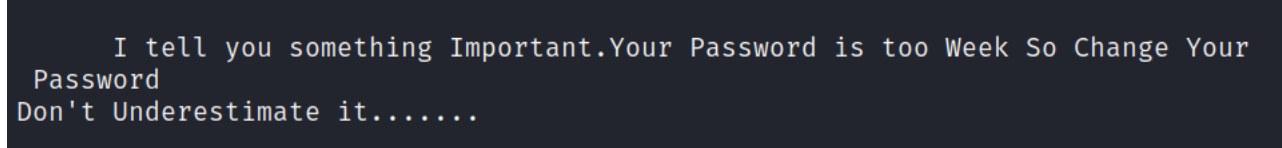


在网页源代码中发现了一个隐藏目录

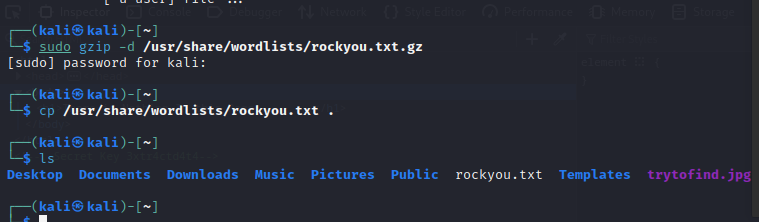


Ok啊，我们也是成功拿到了一个密钥，尝试使用密钥来滑稽猫的图片，发现有一个data.

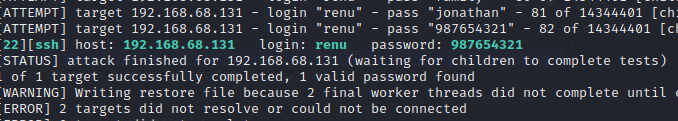
txt的文件，利用steghide分离后，我们得知renu用户为弱密码



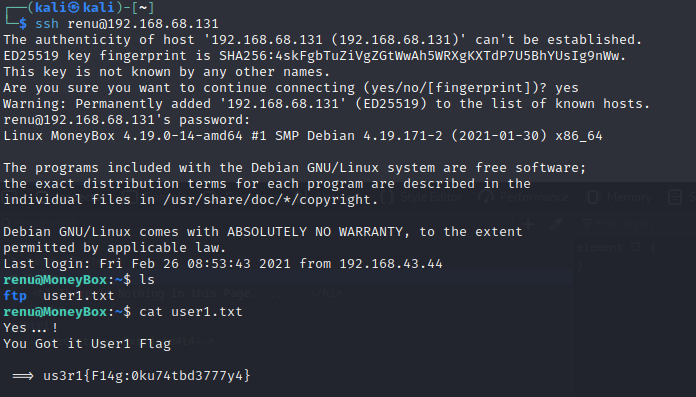
这里也是直接进行kali自带字典爆破，先进行解压



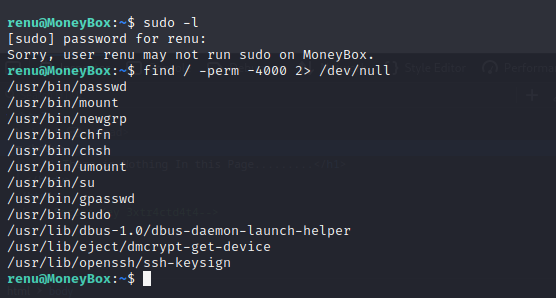
利用hydra进行爆破

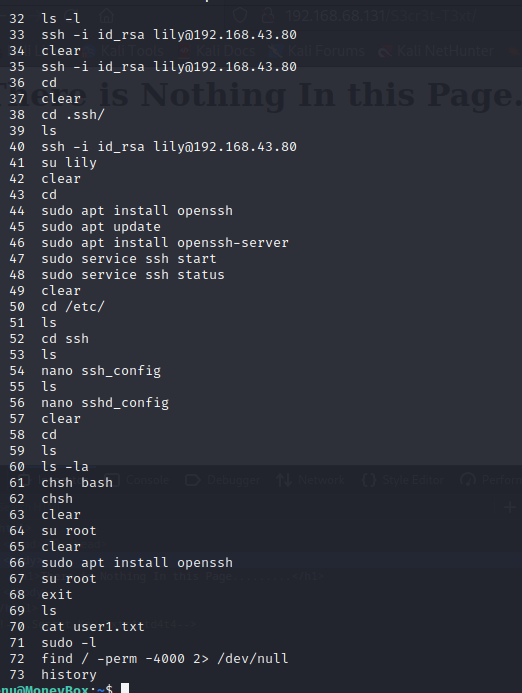


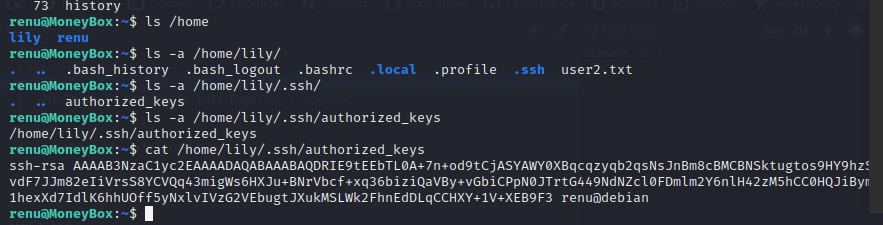
得到renu用户的密码为987654321，接下来利用ssh服务登入



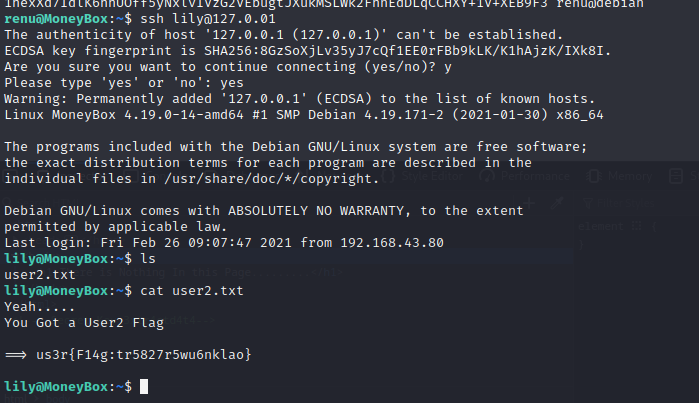
这里也是非常成功的拿下了第一台靶机。



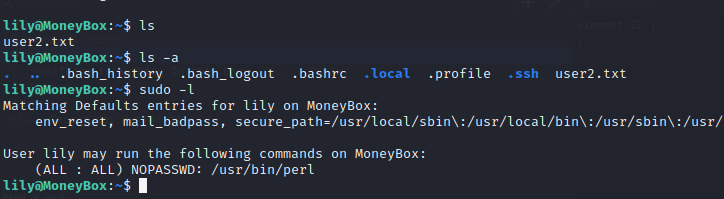




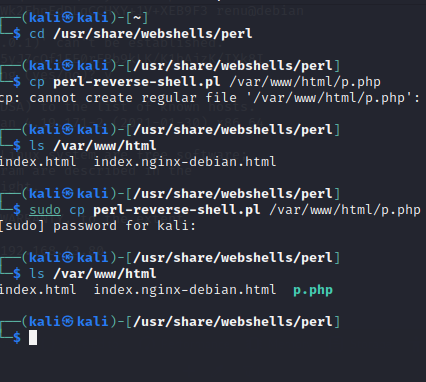
renu用户的命令历史记录存在SSH免密登录，这里可以看到不需要密码就可以以lily的身份登上靶机



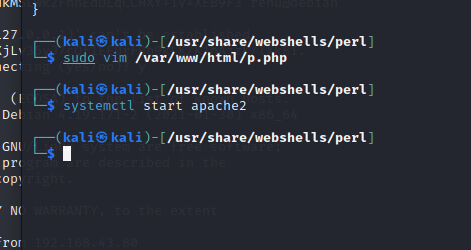
第二个账户也是成功拿下。



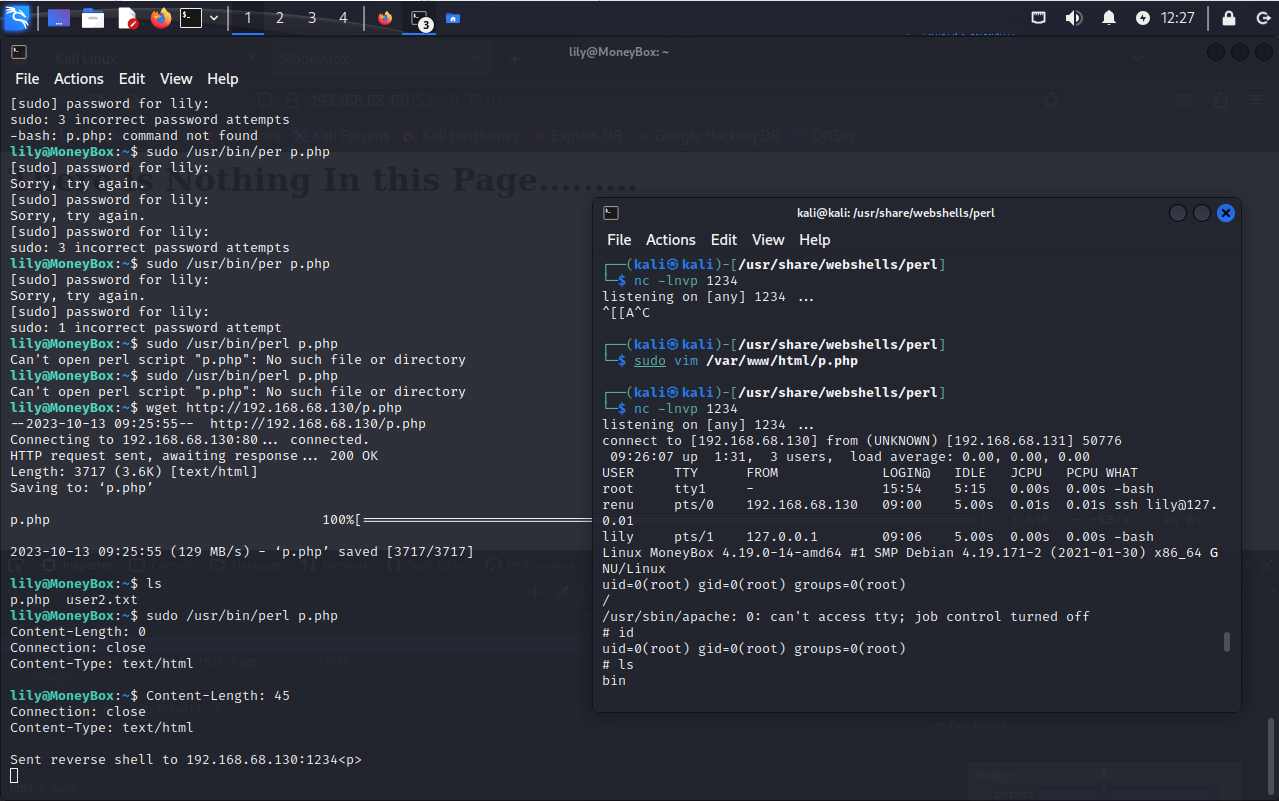
Lily账户存在sudo赋权，程序为usr/bin/perl，这里要利用kali自带的perl脚本反弹shell，从而获得一个管理员shell



反弹shellcopy到www/html目录下



修改反弹ip，开启ssh。



Lily通过http下载p.php,kali通过nc监听，靶机运行p.php，成功反弹权限获取管理员权限shell

