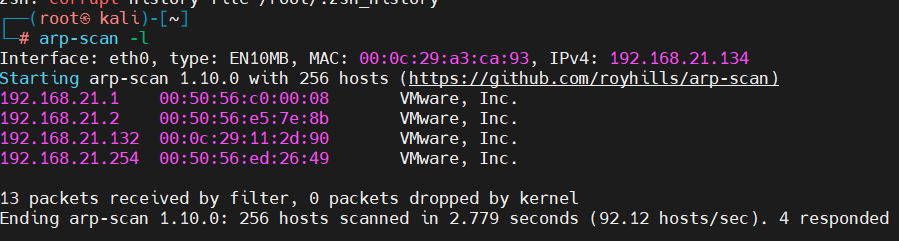
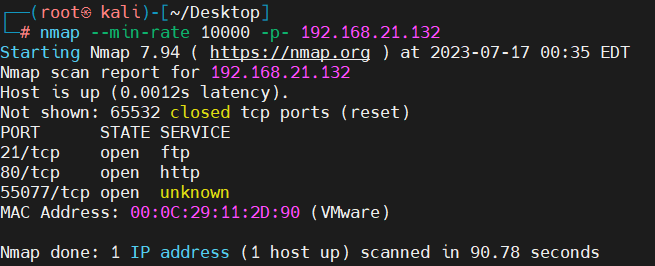
Arp发现主机

arp-scan -l



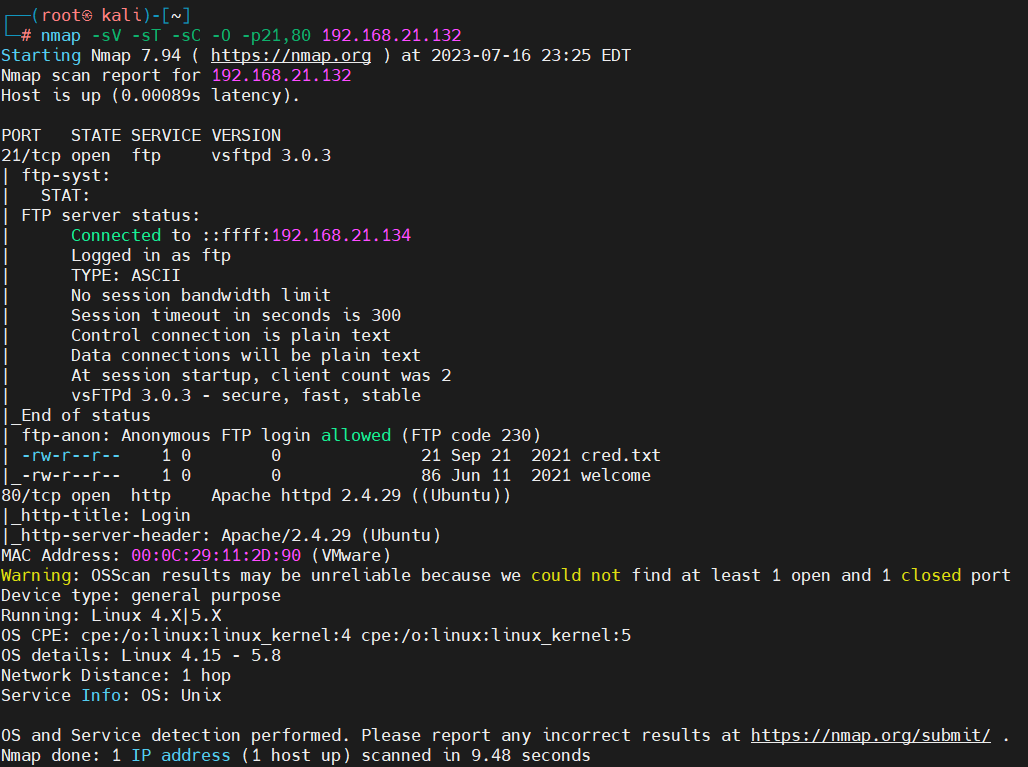
扫描端口

nmap --min-rate 10000 -p- 192.168.21.132



扫描端口的服务版本号以及操作系统

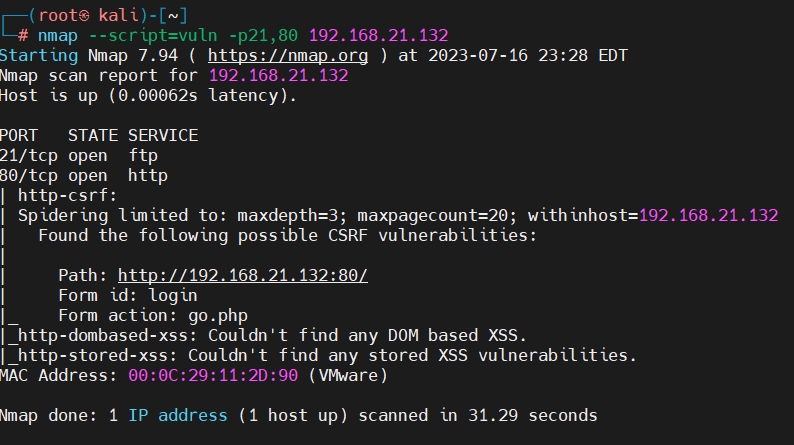
nmap -sV -sT -sC -O -p21,80 192.168.21.132



可以看到ftp里面有文件，web是php

扫描基础漏洞

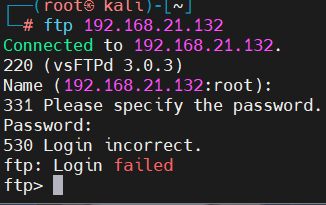
nmap --script=vuln -p21,80 192.168.21.132



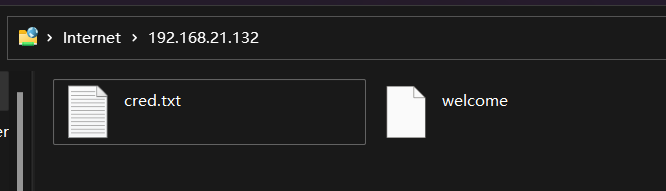
有scrf（基本没用）

先看一下ftp的文件

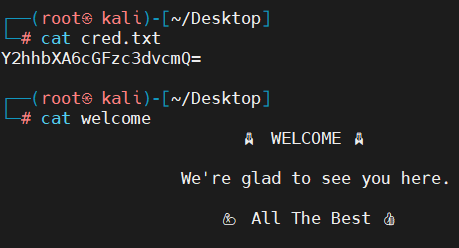
ftp 192.168.21.132



不知道密码就不输入（但是必须要登入那就去页面看一下）

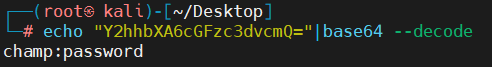


下载下来进行分析



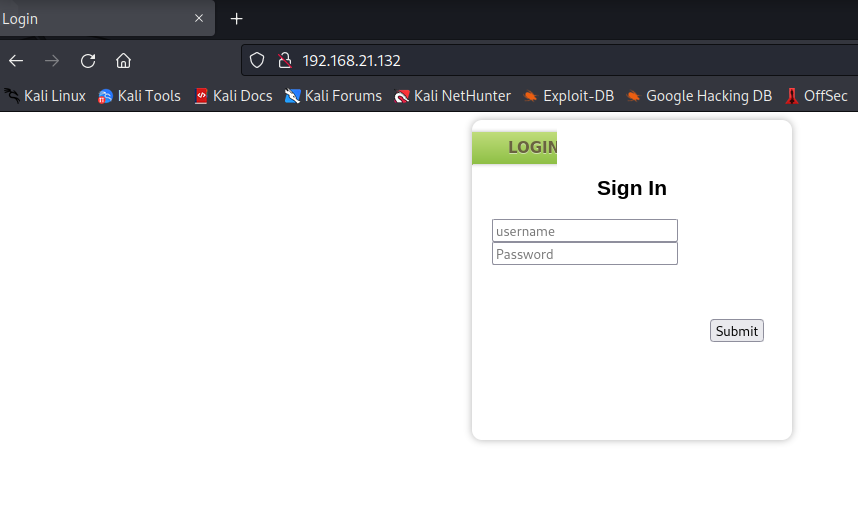
有等号大概是base64

echo "Y2hhbXA6cGFzc3dvcmQ="|base64 –decode



ftp是不能登入的

现在看看80端口的东西

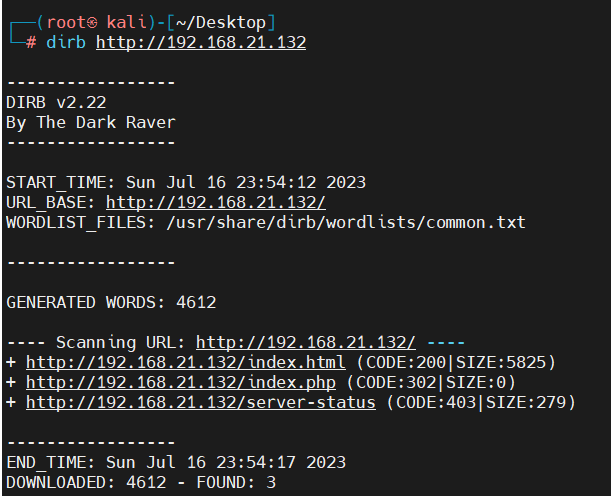


拿到的密码试一下，ok成功进入



发现点about us的时候有文件下载，保险起见直接整点目录扫描

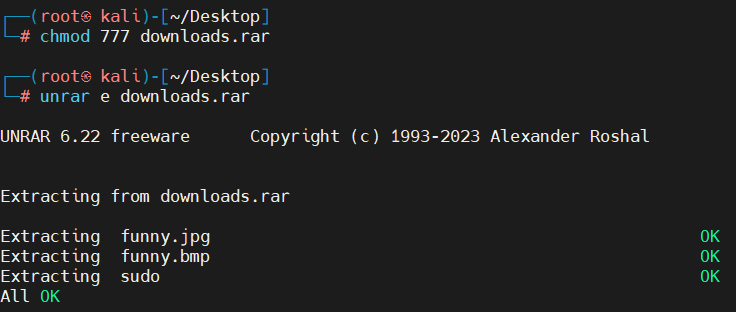
dirb <http://192.168.21.132>



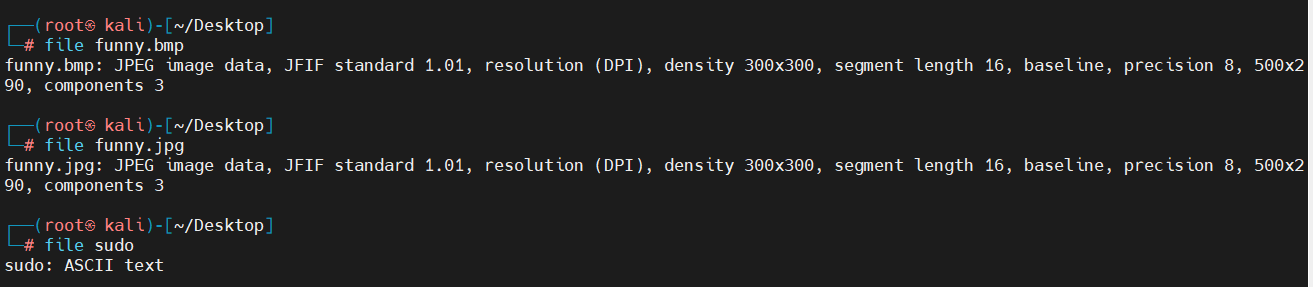
此时文件没有权限给个权限就能解压

chmod 777 downloads.rar

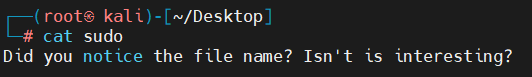
unrar e downloads.rar



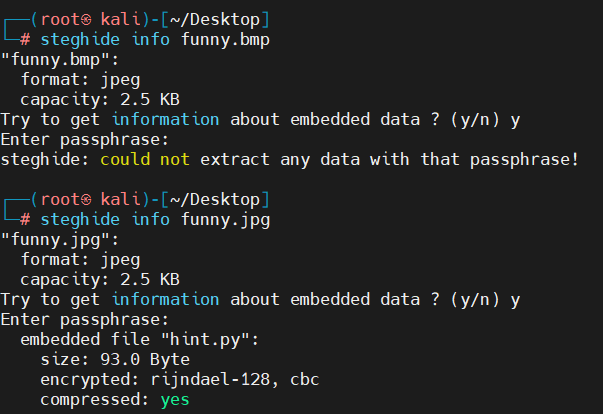
看一下这三个文件



先看ascii文件

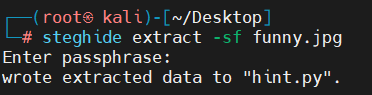


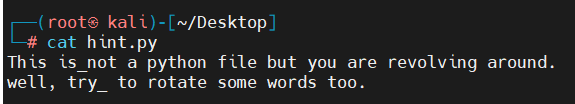
从侧面来说这两图片可能有隐写



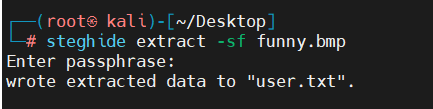
发现python文件

steghide extract -sf funny.jpg



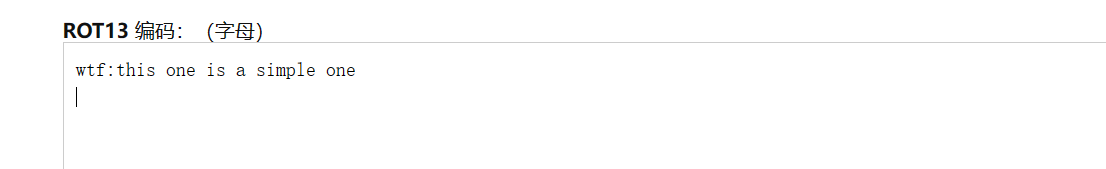


steghide extract -sf funny.bmp



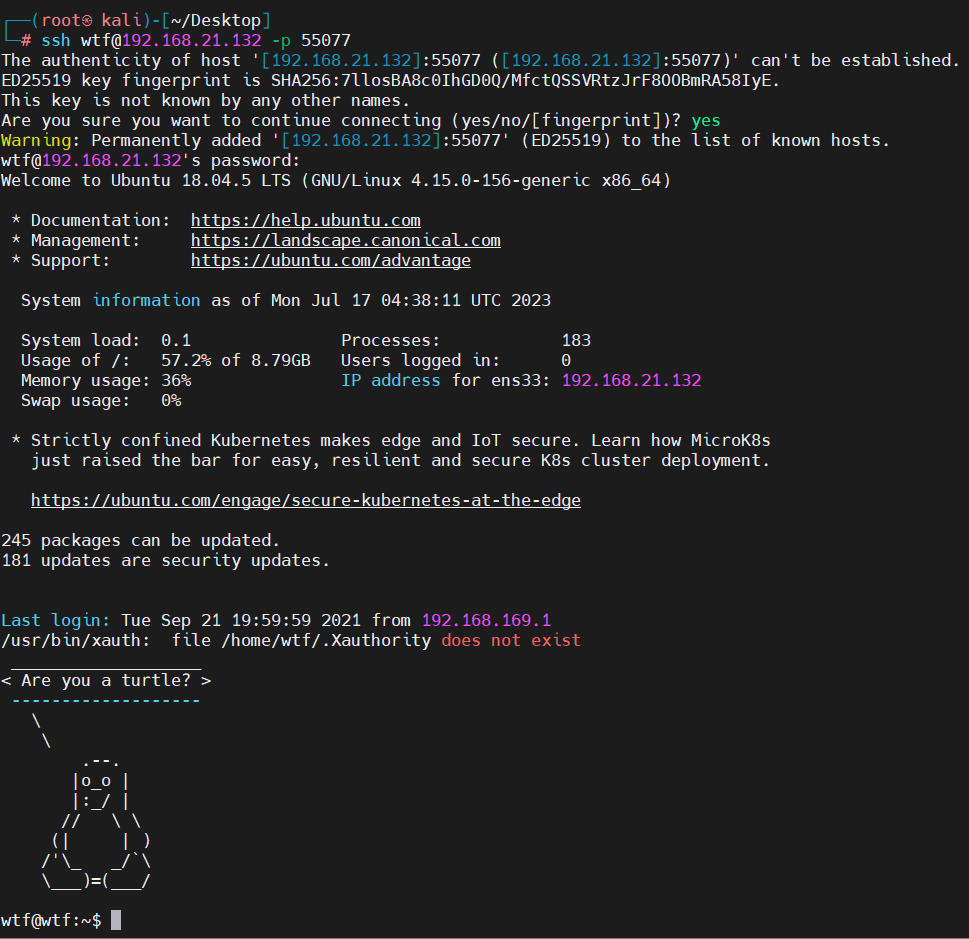
密码sudo，才出来的

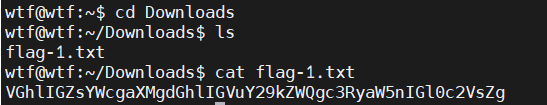
提示我们要吧文件rotate，那就因该是加解密了，随手一搜[CTF在线工具-在线Rot13密码加密|在线Rot13密码解密|Rot13密码算法|Rot13 Cipher (hiencode.com)](http://www.hiencode.com/rot13.html)



这个有点像账号和密码，那应该是ssh的密码了

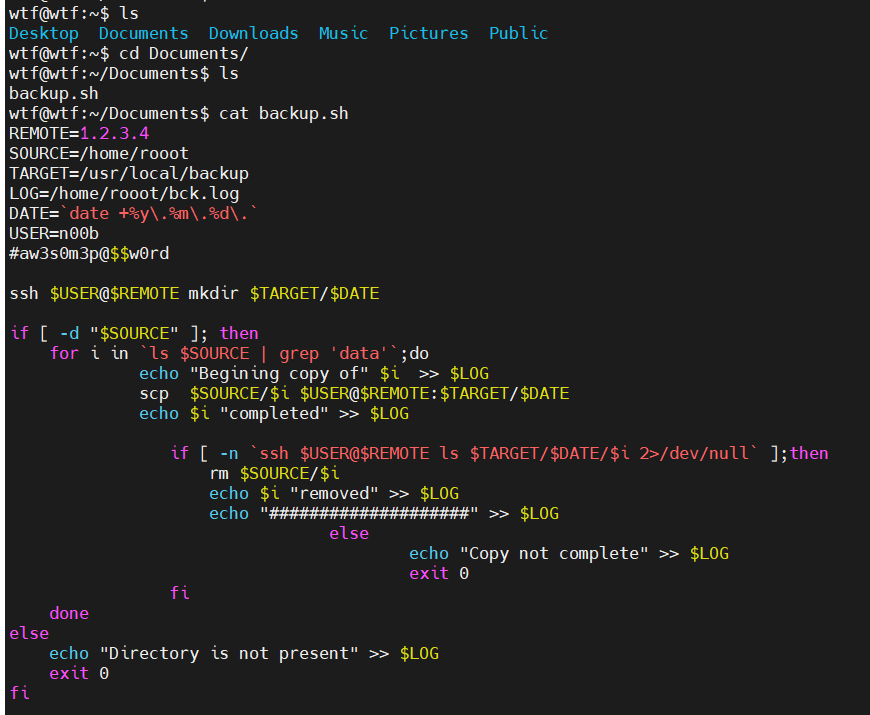
ssh wtf@192.168.21.132 -p 55077





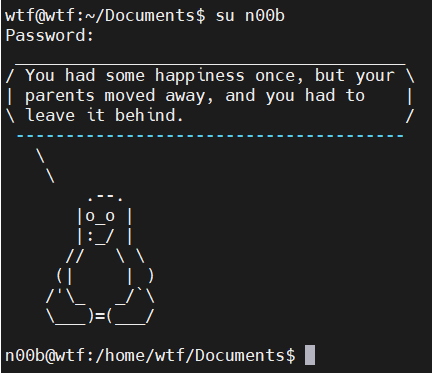
找到flag

又来一个脚本，看到user和密码

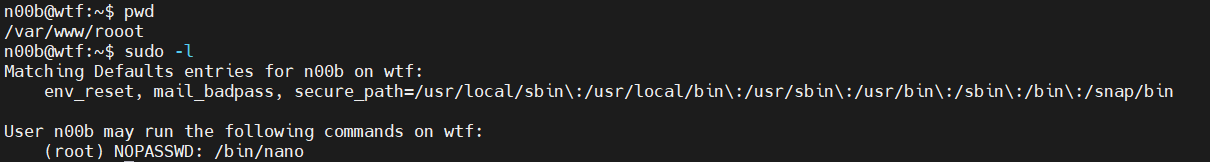


注意#是注释

切换账号



查看权限



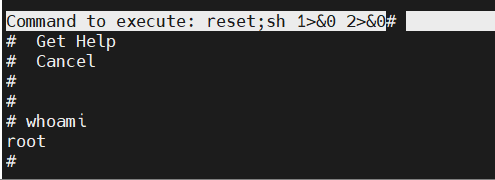
发现可以用 nano 编辑器，nano 编辑器允许二进制文件以超级用户身份运行sudo，它不会放弃提升的权限，并可用于访问文件系统、升级或维护特权访问。 <https://gtfobins.github.io/gtfobins/nano/#sudo>

sudo nano

ctrl+r ，Ctrl+x

输入 reset; sh 1>&0 2>&0

会搞定



得到 root 权限，查看flag，在 /root 目录下

