De-ICE\_S2.100\_(de-ice.net-2.100-1.0)

下载地址：<https://download.vulnhub.com/deice/De-ICE_S2.100_%28de-ice.net-2.100-1.0%29.iso>

靶机搭建

注意下载下来的是iso文件接下来说明系统选择

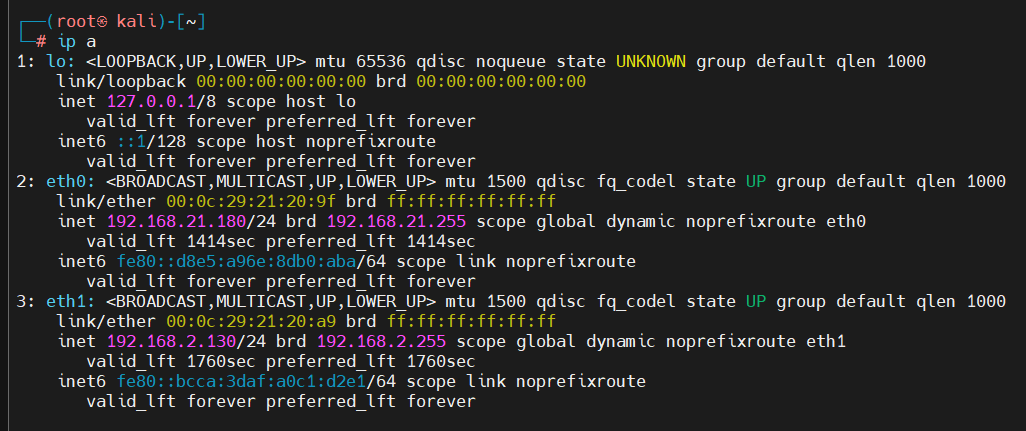
linux的Debian 7.x就可以

然后注意一点我们需要创建一个192.168.2.0/24的网卡进行连接（靶机ip地址默认是192.168.2.100和192.168.2.101）

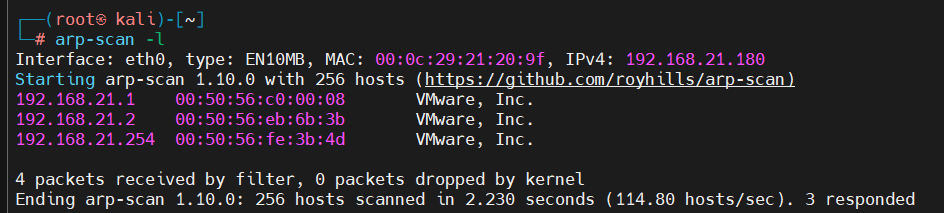
主机发现

注意要kali和靶机在一个内网

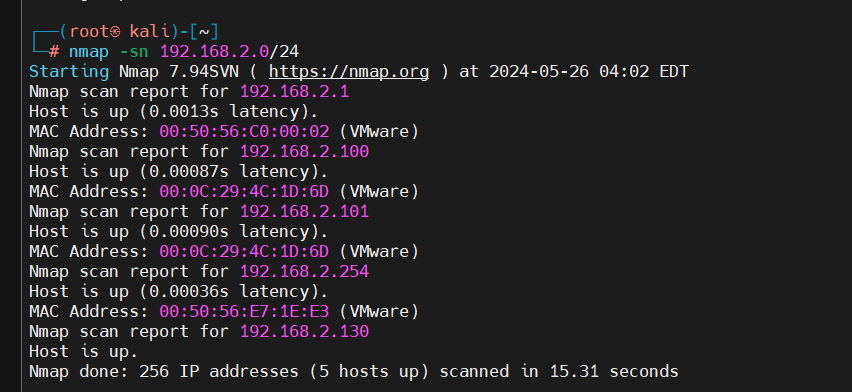
kali靶机



此时arp就不好使了



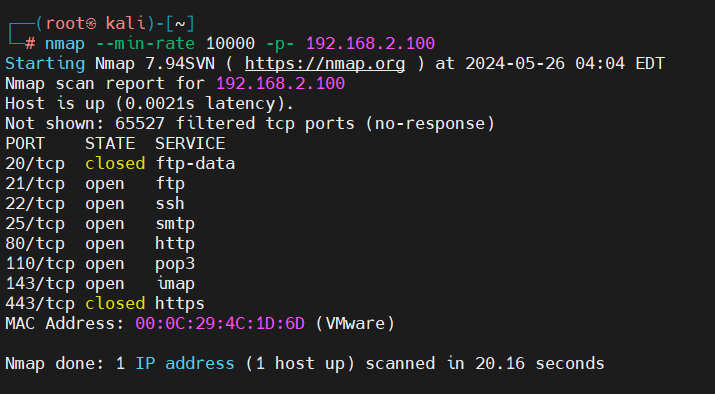
可以使用nmap



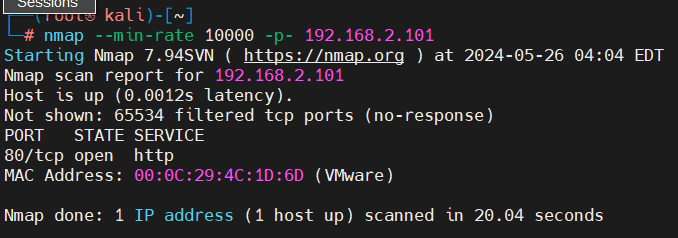
目标是100和101

端口扫描

100

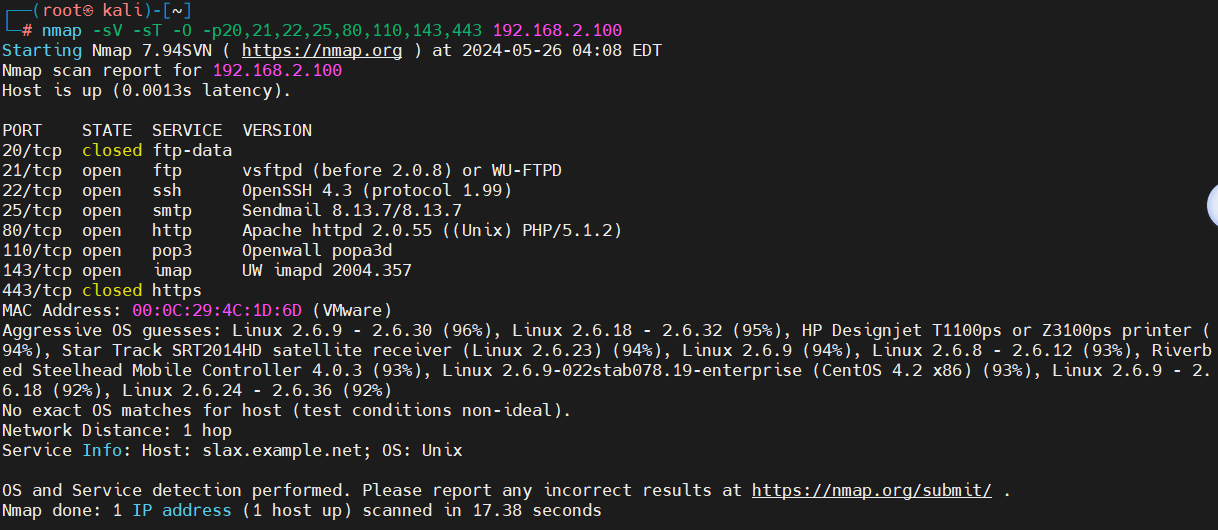


101

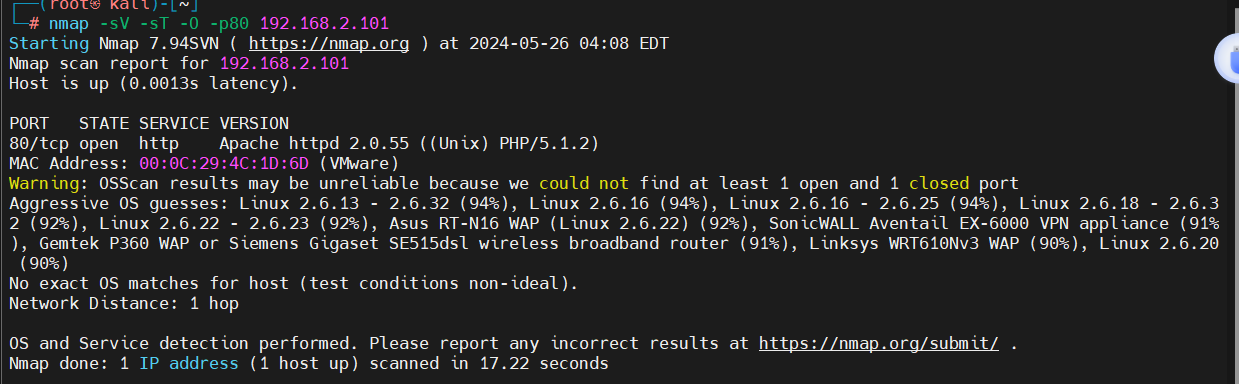


端口服务扫描

100

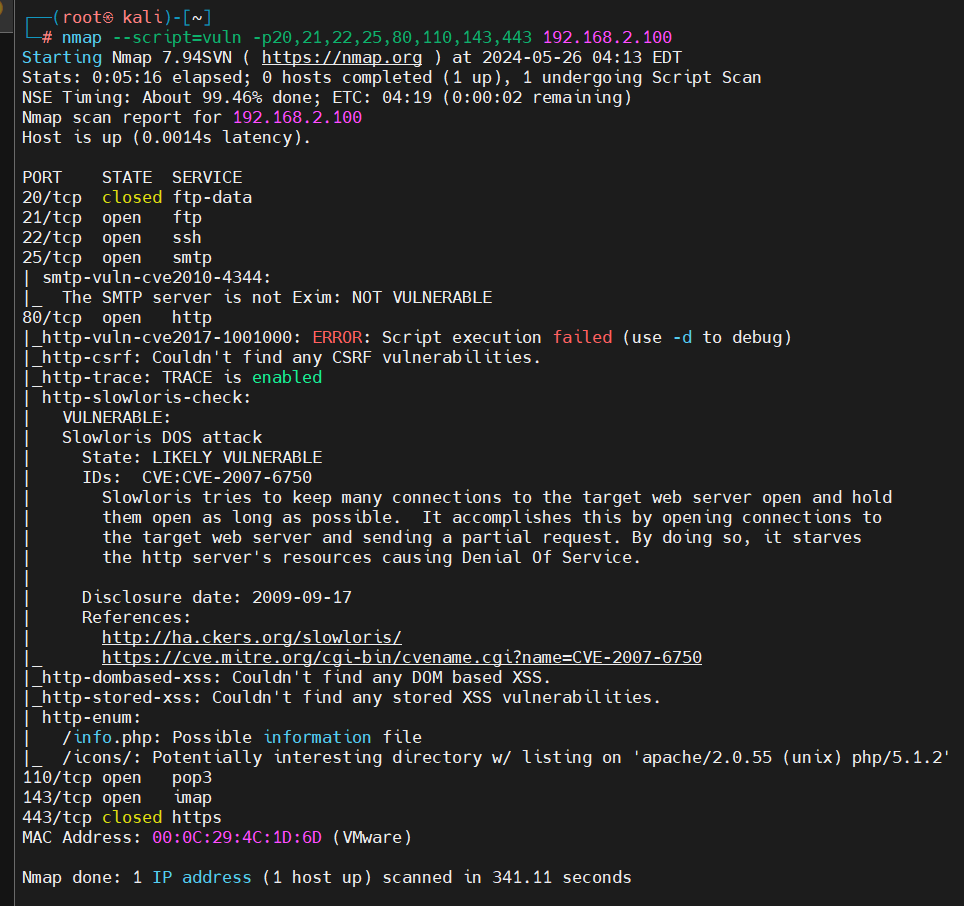


101

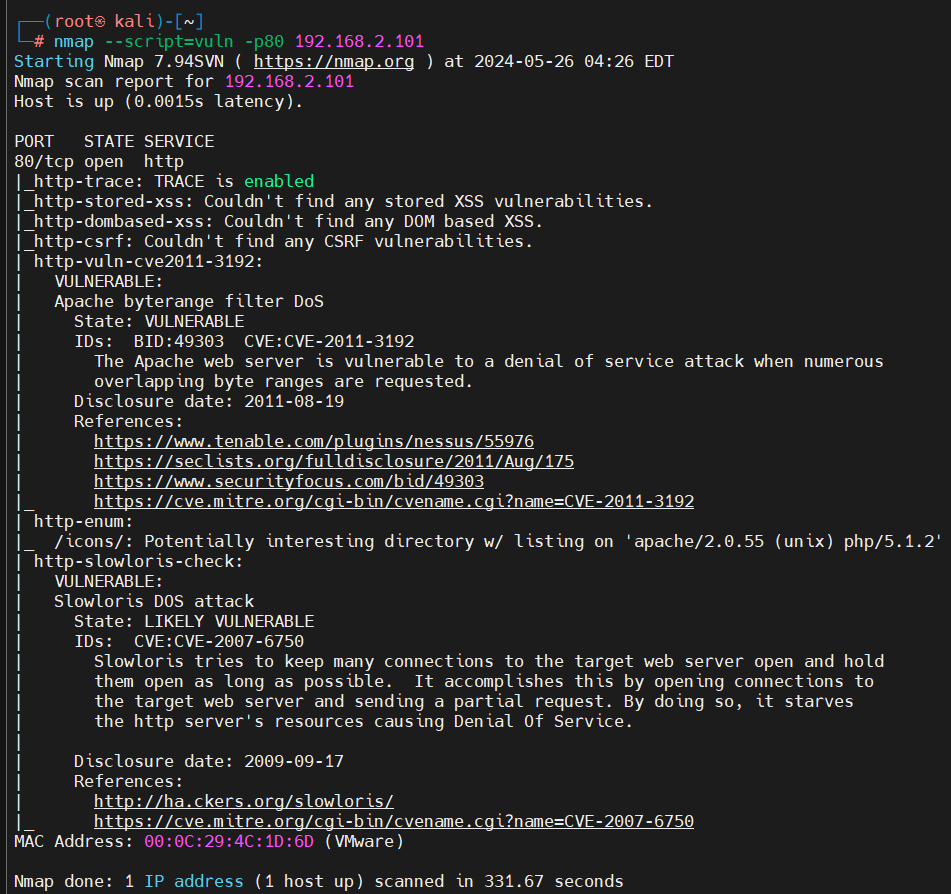


漏洞扫描

100



101



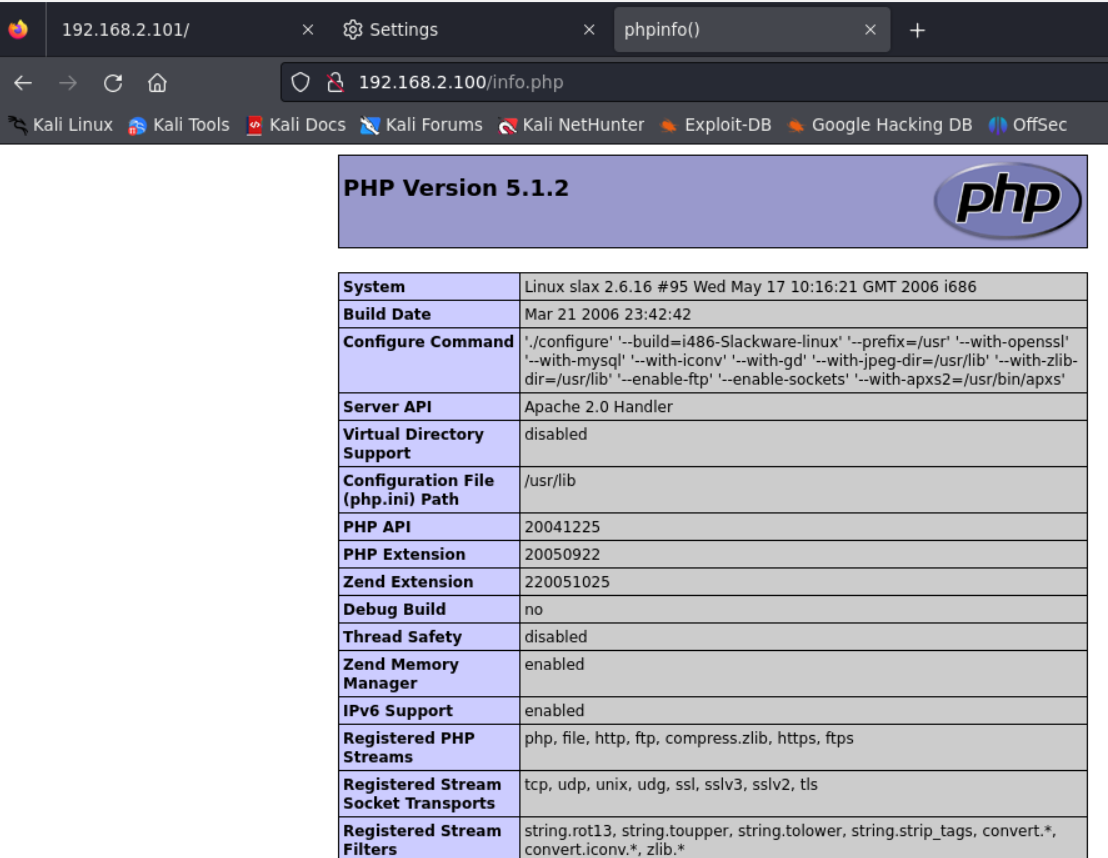
先看一下web

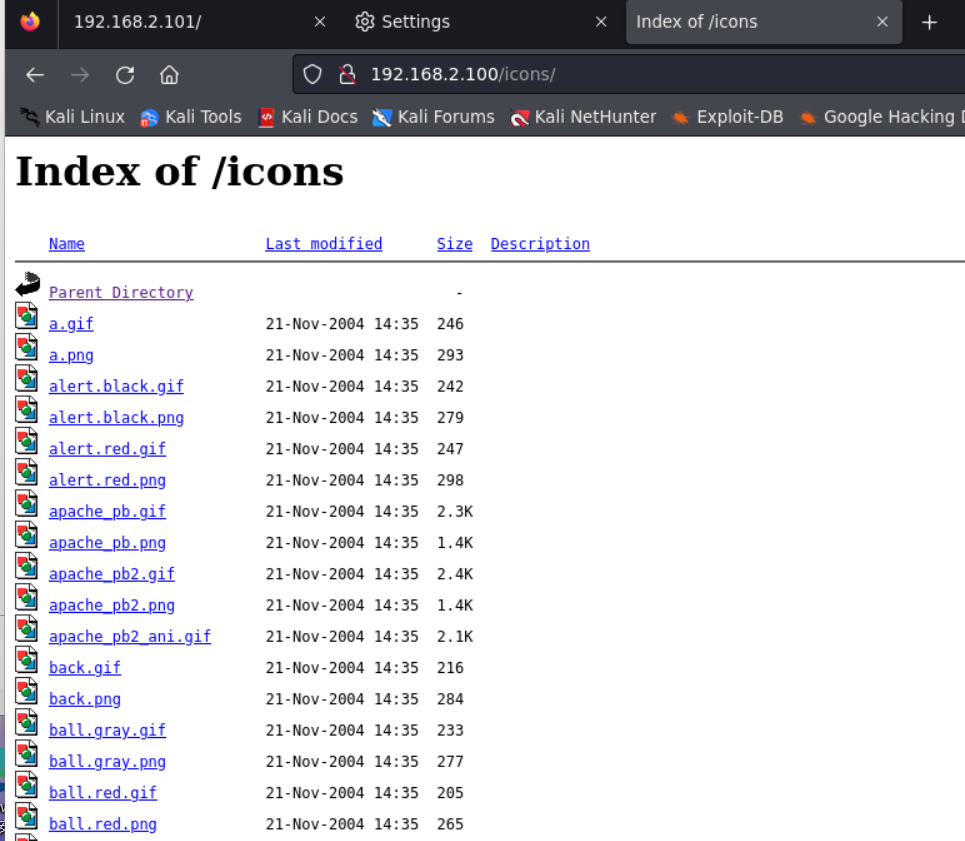
100



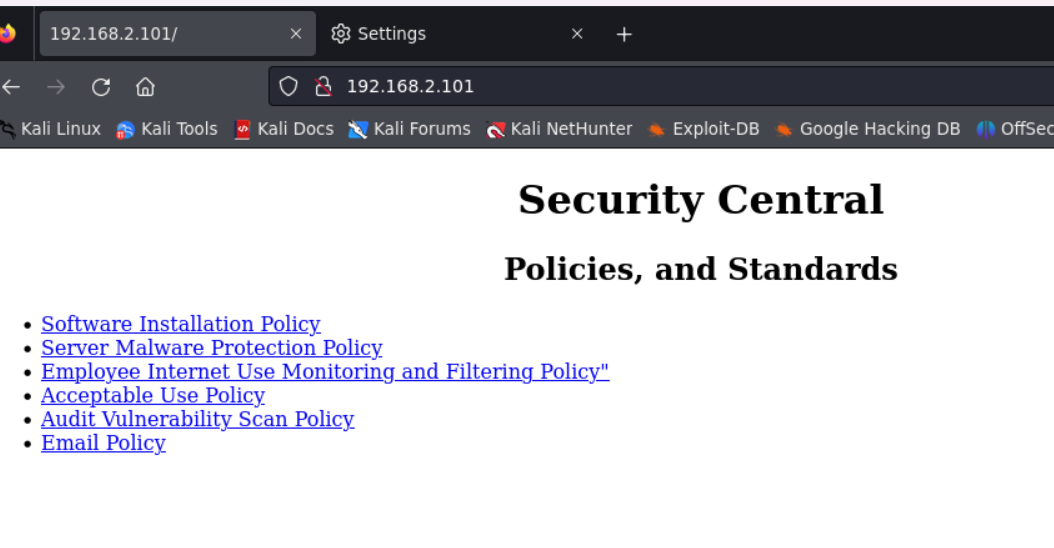
开发人员信息





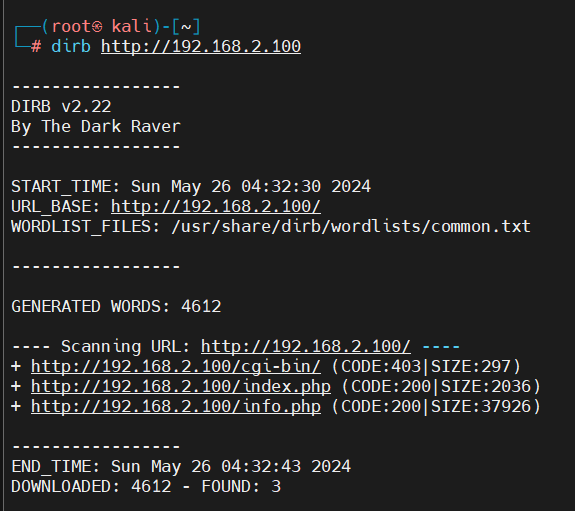


101

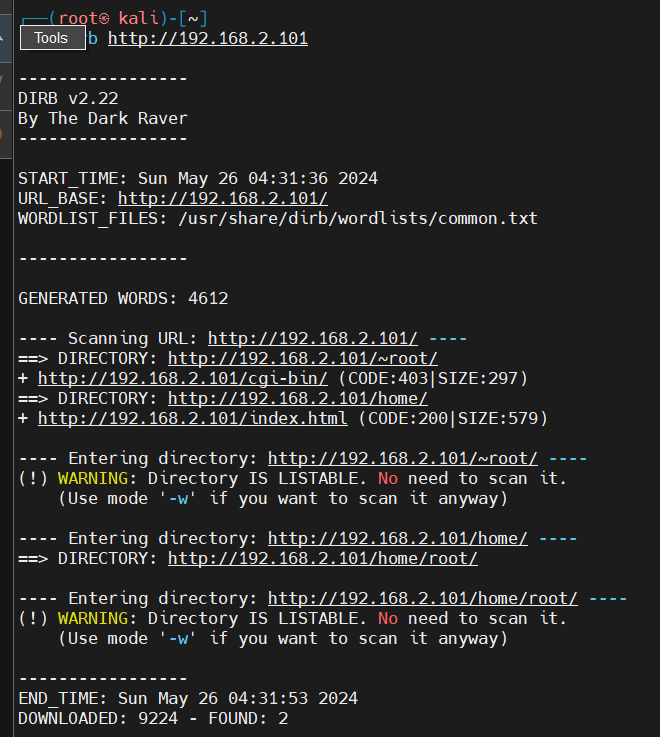


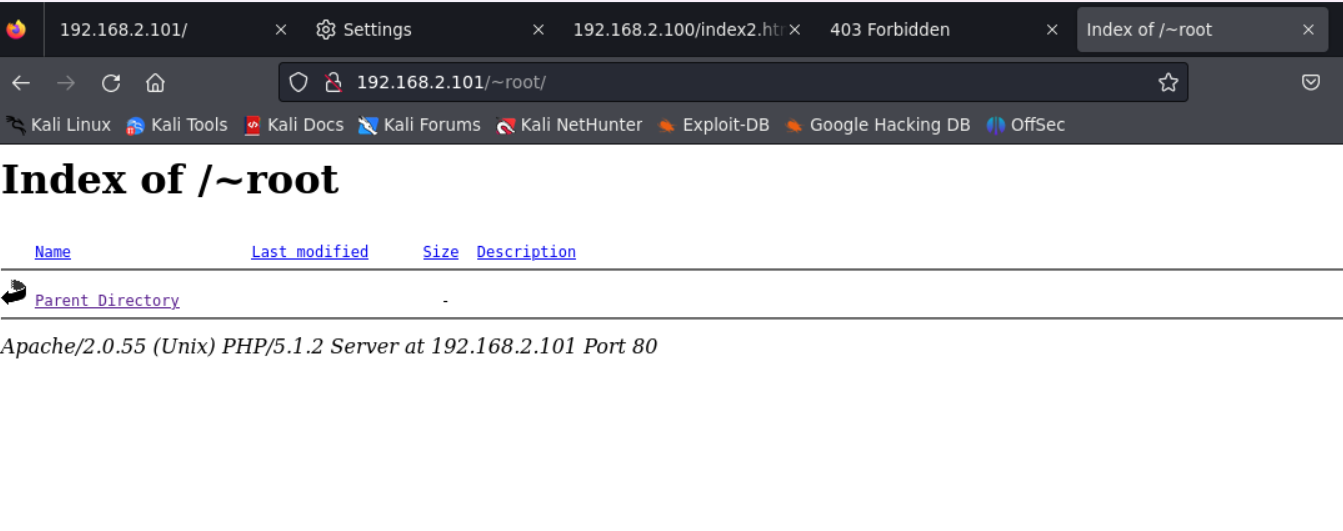
简单扫描一下目录

100

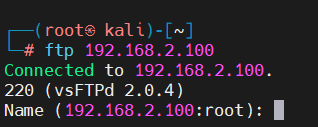


没啥用



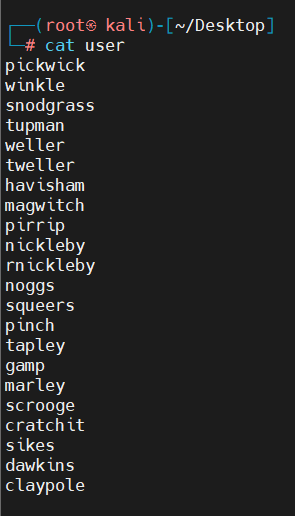


注意这里开放了ftp去看一下



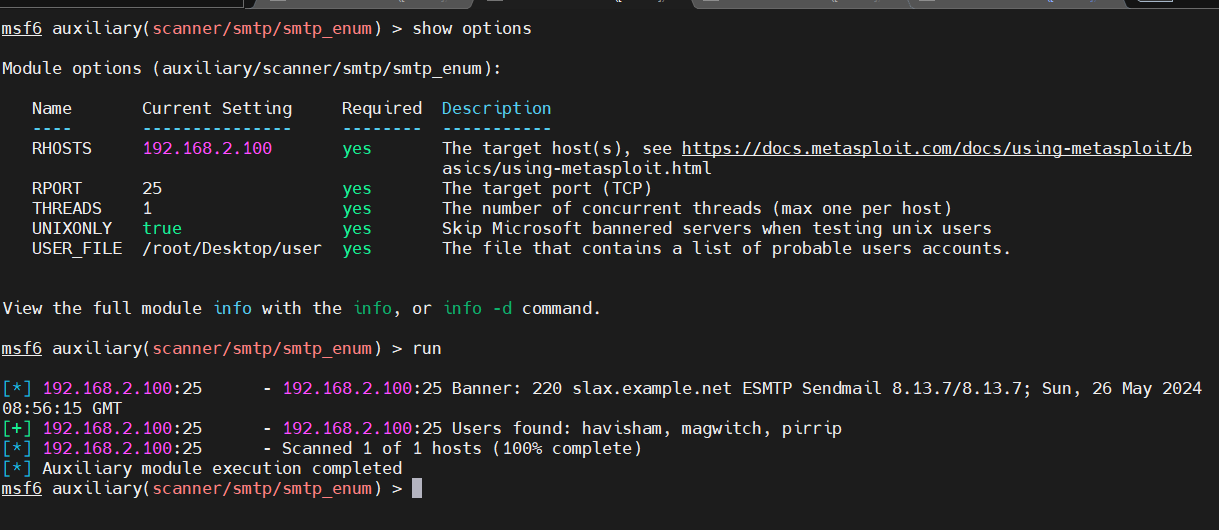
有默认用户那么就不应该能用匿名登入

那么最大的可能是利用100发现的制作人的邮箱去登入smtp



扫描一下

只找到msf有模块可以使用但是别的工具没有找到能使用的

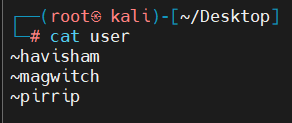


此时有三个用户能用

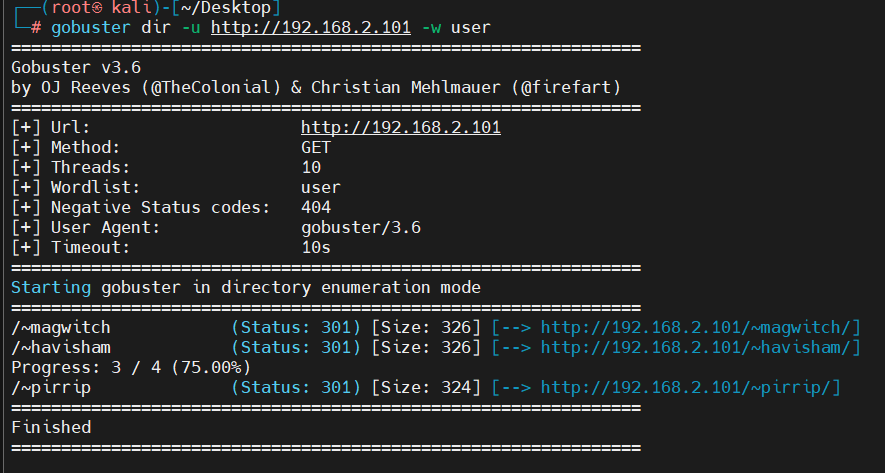
我们注意一下前面扫描web扫描出来的~root

在运维或者开发的过程中常常会根据邮箱来创建远程连接

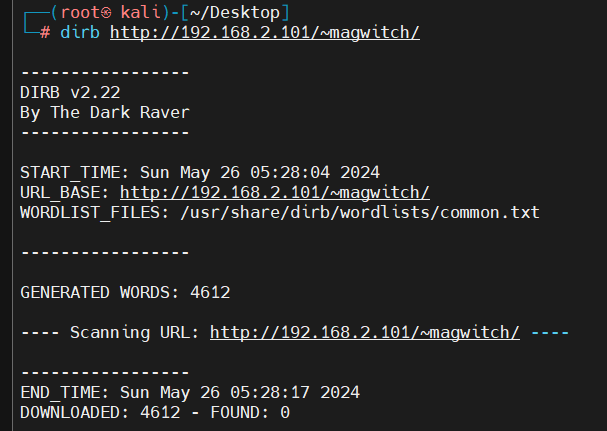
所以我们应该扫一下这三个人的目录（前面加上‘~’）

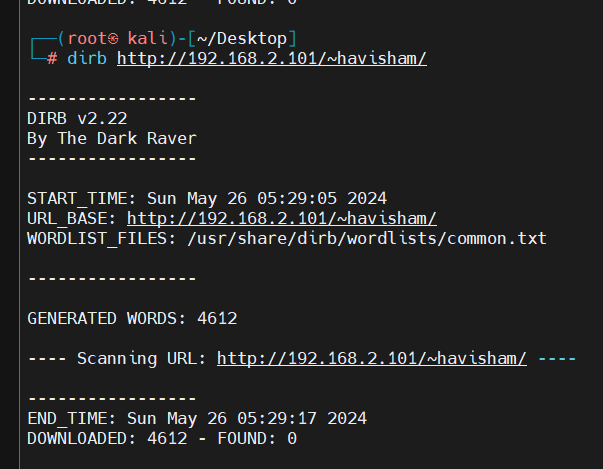


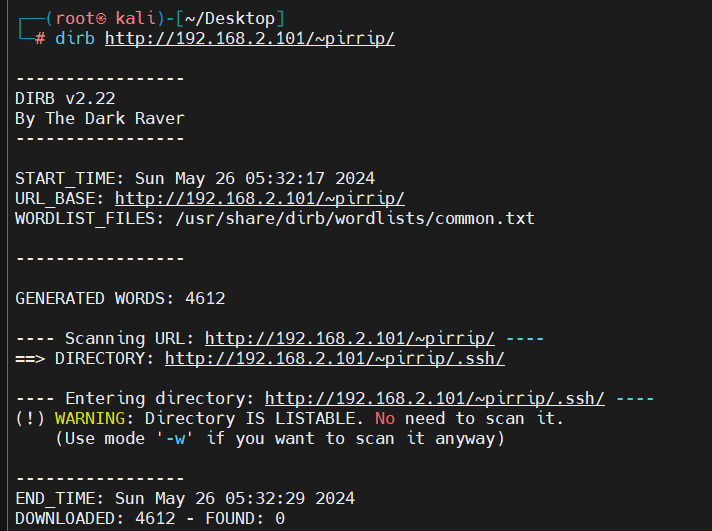
注意目标此时目标因该是101



326可以证明这里面是有东西的



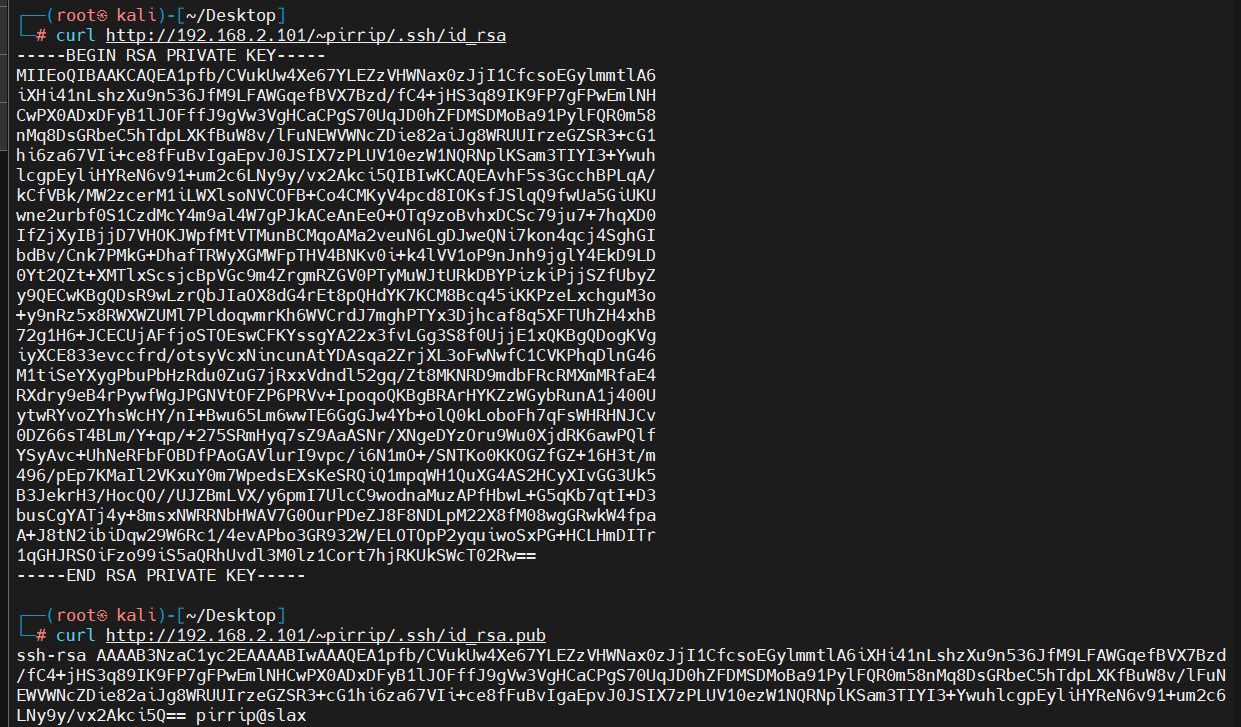




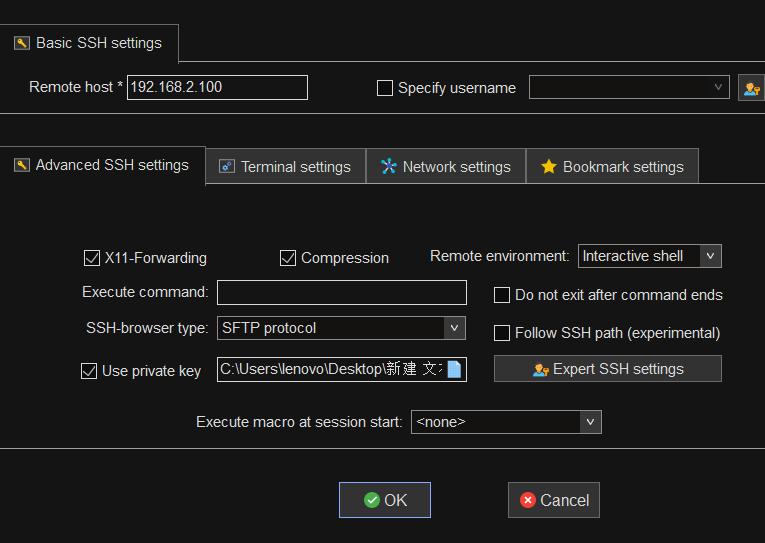
好东西去看看



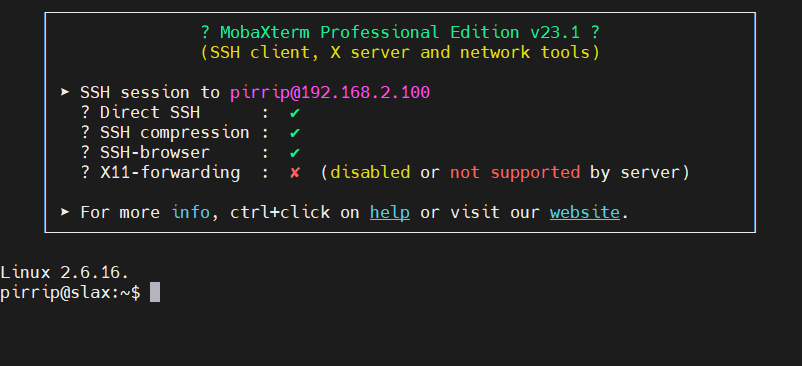
更好了全下载下来



接下来登入

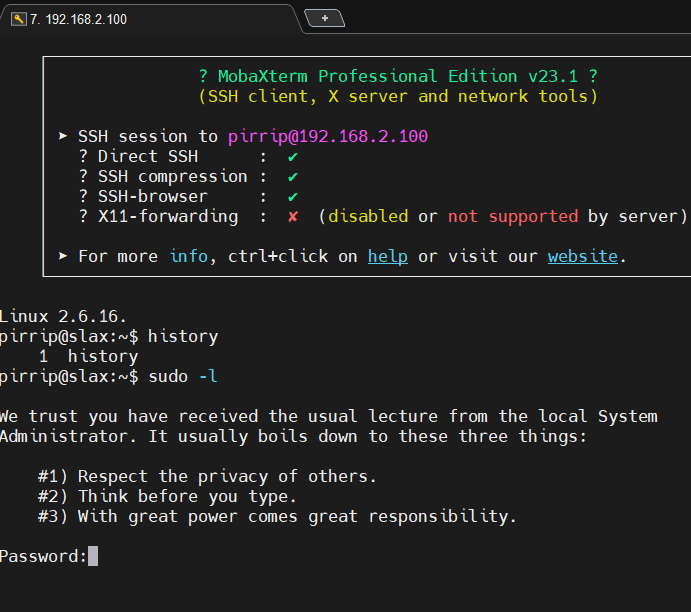


还是要机制操作，不要再一棵树上吊死

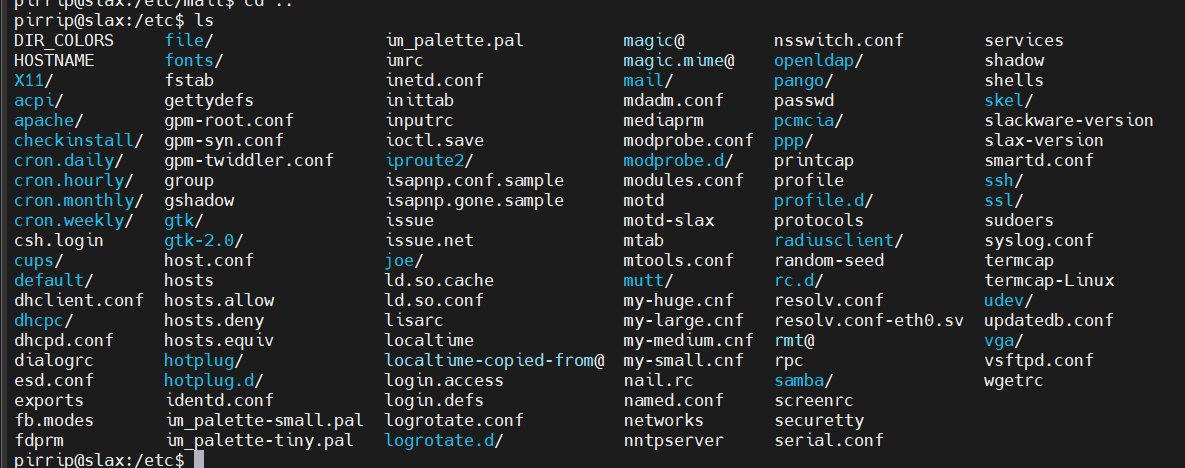


登入成功

信息收集

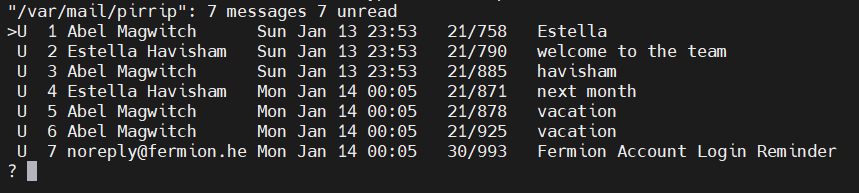


再etc查看后发现

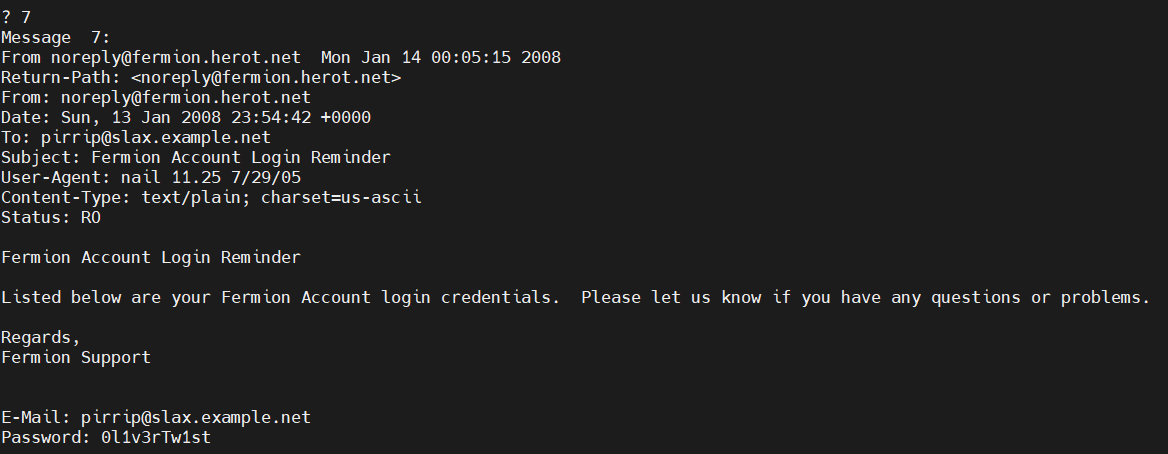


有mail

那就直接运行看看了

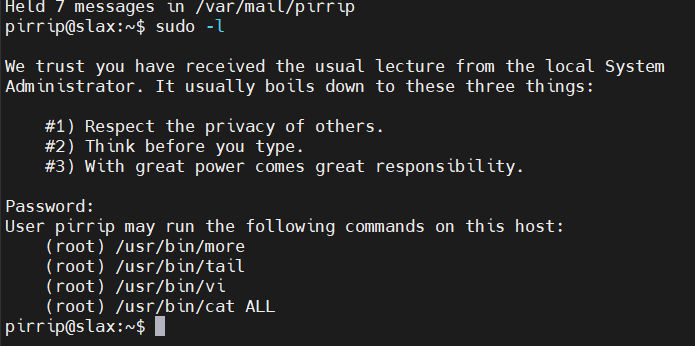
****

邮件都看一下，当然最后一个很有可能是突破点



密码到手了

再次sudo -l



vi提权

