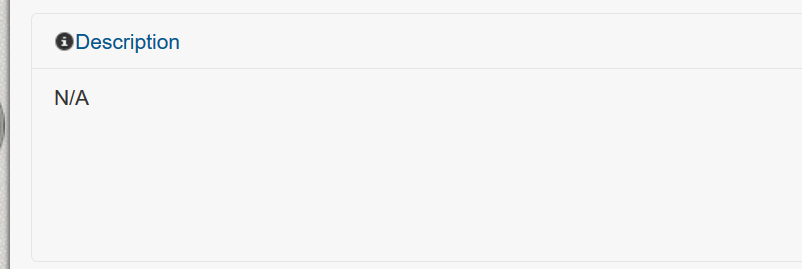
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/my-file-server-1,432/>

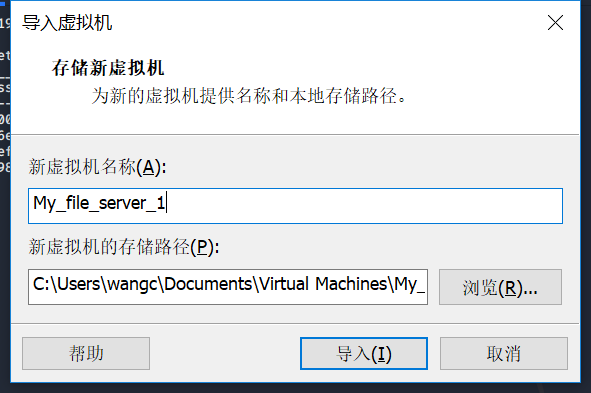
描述无



下载好以后是个.ova文件



点击以后选择一个合适的地方存放



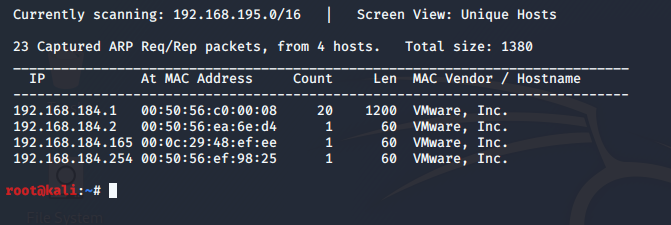
安装好以后把网络调回NAT就可以运行了



# 0x01:探测靶机

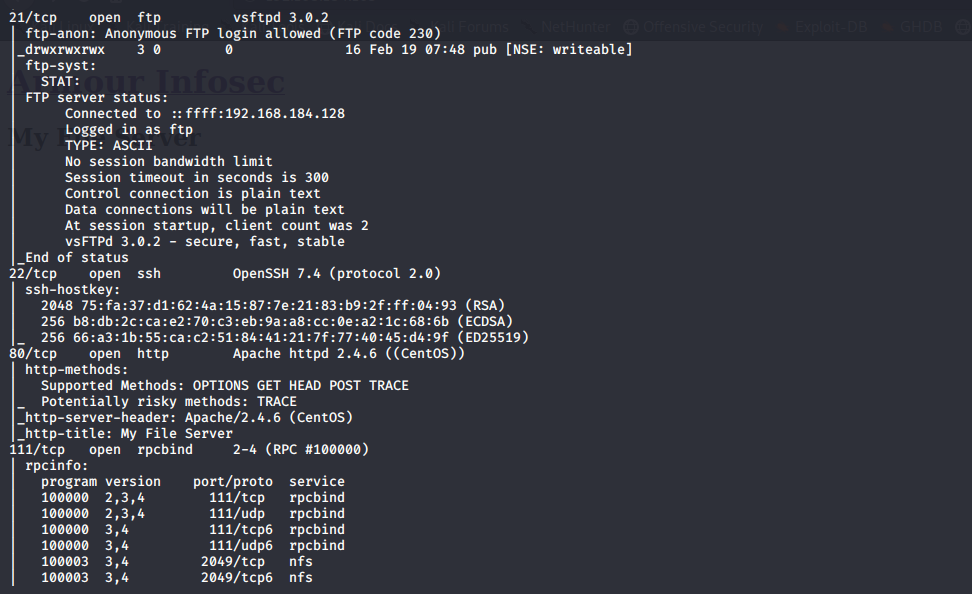
先用netdiscover探测靶机IP,排除.1,.2可以确认靶机IP为192.168.184.165

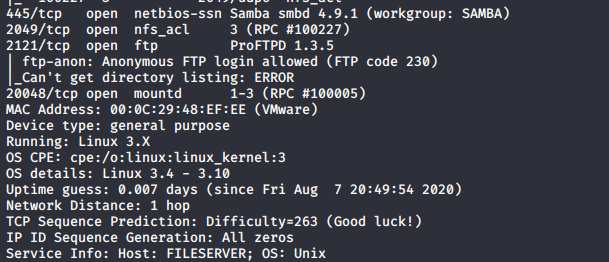
命令:netdiscover -r 192.168.184.0/16



开始用Nmap探测一波端口，这次开放的端口比较多开了，21，22，80，111，445，2049，2121，20048端口

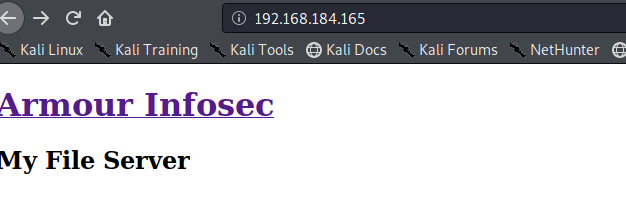
命令:nmap -A -sS -sV -v -p- 192.168.184.165



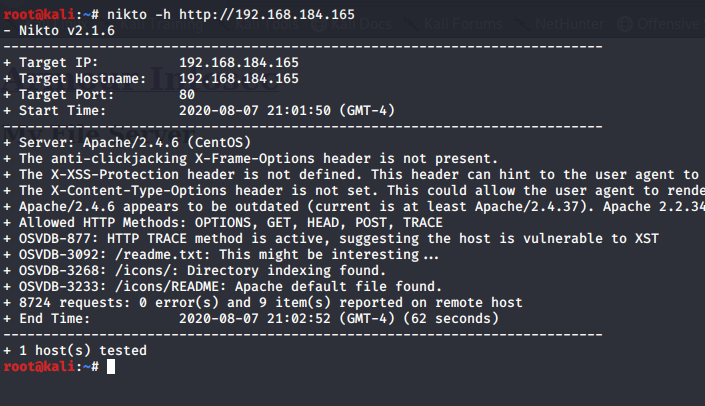
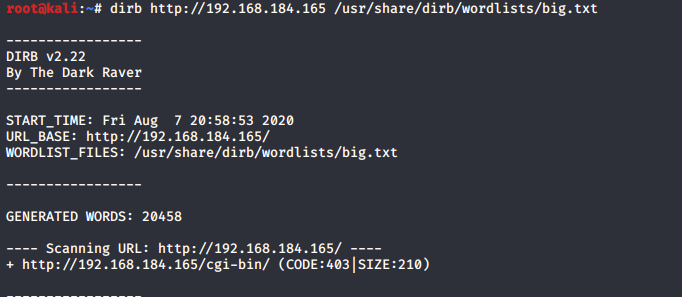


# 0x02:挖掘信息

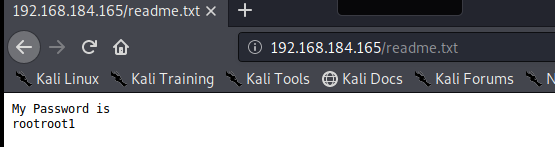
先访问一下主页可以正常回显，只是一个很简单的HTML代码还有一个链接



然后就开始用dirb/nikto扫描目录看看有没有信息，dirb感觉扫不出来然而nikto扫出一个readme.txt出来

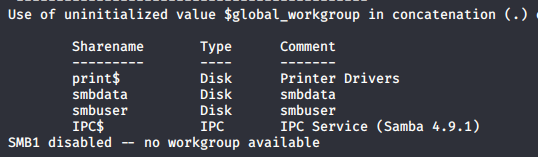


跟进一下发现大宝贝password rootroot1

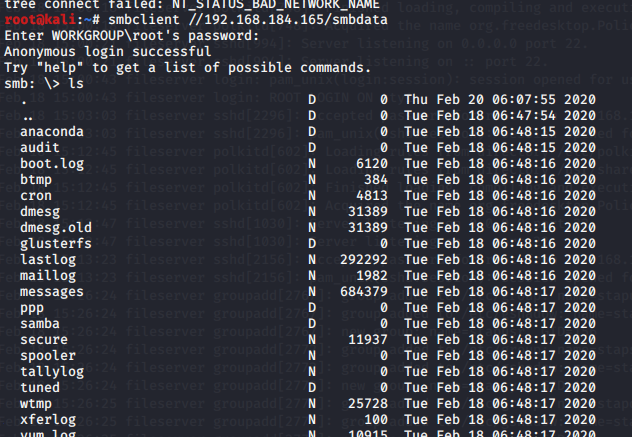


这里先回到445端口是一个Samba服务，所以可以用下enum4linux, enum4linux是一款枚举windows和samba主机的数据的工具，可以发现2个用户名smbdata和smbuser

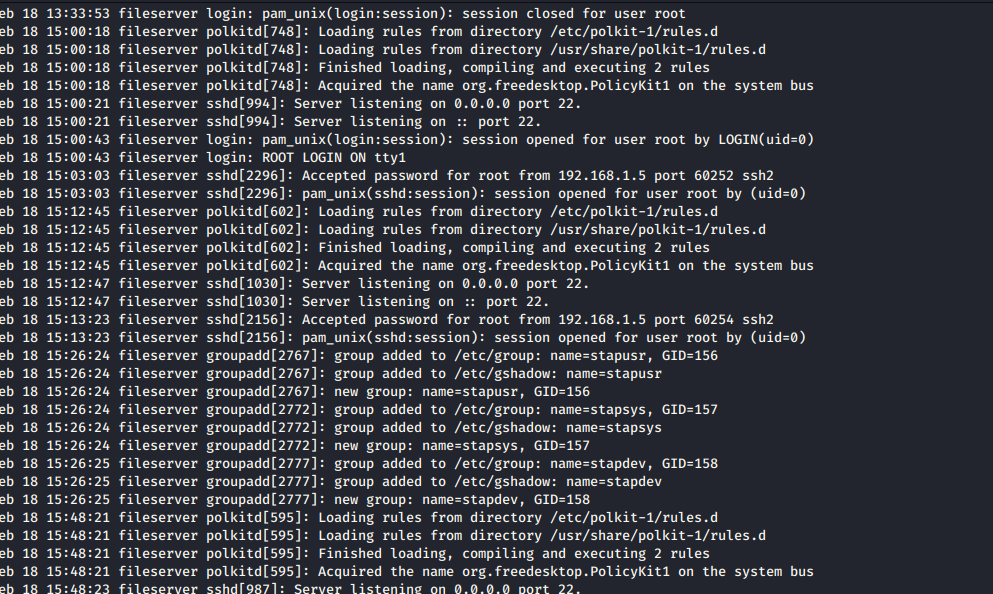
命令:enum4linux <http://192.168.184.165>



然后用smbclient进行连接，然而最后只用smbdata是空密码,smbuser密码不知道卒，不过有比较多的东西



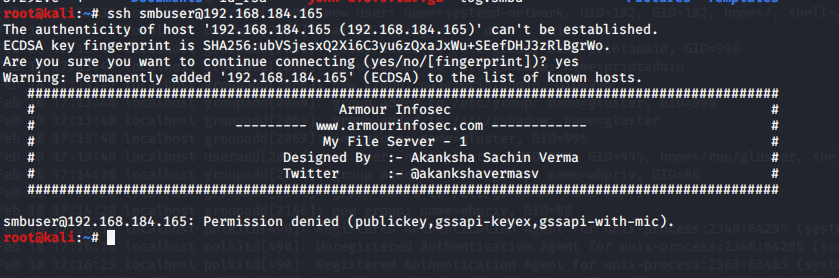
浏览了一下下载了secure，打开了以后是一个日志里面有很多用户



输入name=捕捉后面的关键词，放起来，在浏览的过程中发现一个完整的账号smbuser和密码

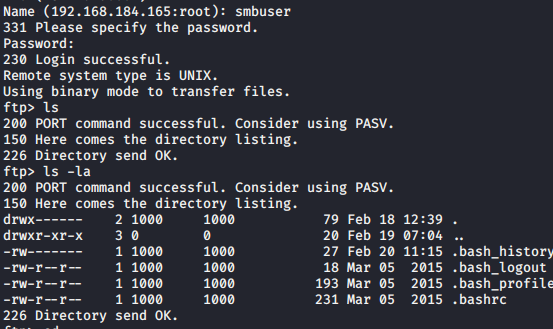


尝试SSH登录然而提示要公钥，行吧这条路走不通了



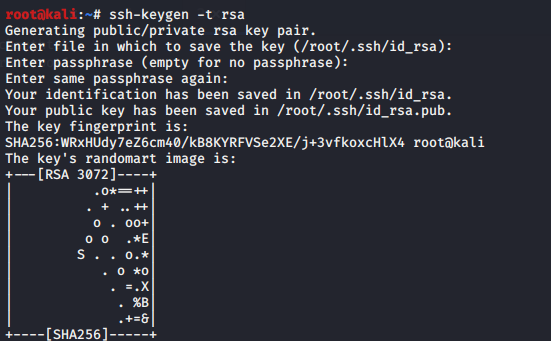
# 0x03:创建SSH公钥

这次换另外一个用户登录21端口 smbuser密码变成rootroot1成功登录

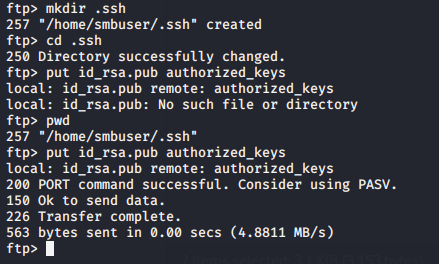


由于缺的是公钥，那么首先在kali建一个然后传到ftp上绕过去

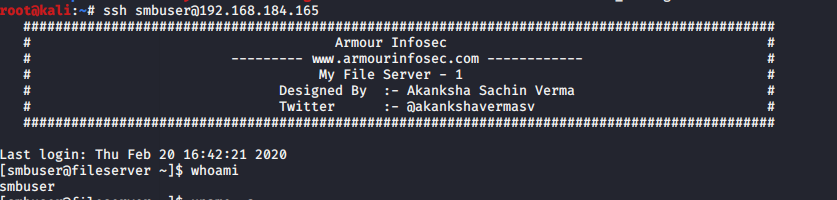
命令:ssh-keygen -t rsa



然后就是在smbuser目录下建立一个.ssh/目录在把刚才生成的钥匙传进去顺便改名达到混淆的效果(注:刚才生成好的文件记得放到/root目录下才能生成),



这次直接ssh不用密码就可以登录成功了



# 0x04:提权

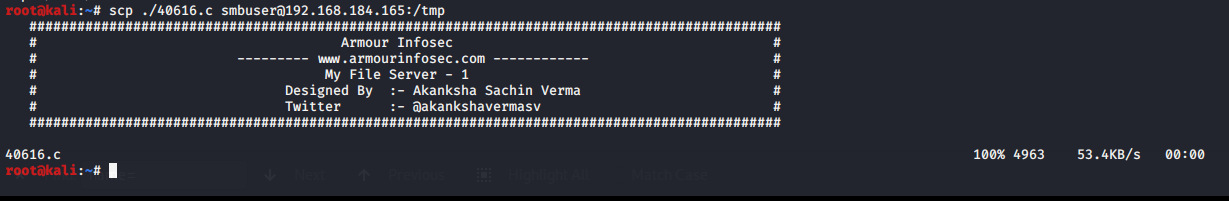
先输入uname -a 得到关键词，内核比较低



在网上找到一个脚本符合版本需求，看了一下脚本其实kali也有就是40616.c



复制到kali/root目录以后用scp命令传上去



使用方法<https://blog.csdn.net/qq_45555226/article/details/102641409>在这里有提到，按照它给的复现步骤成功提权

