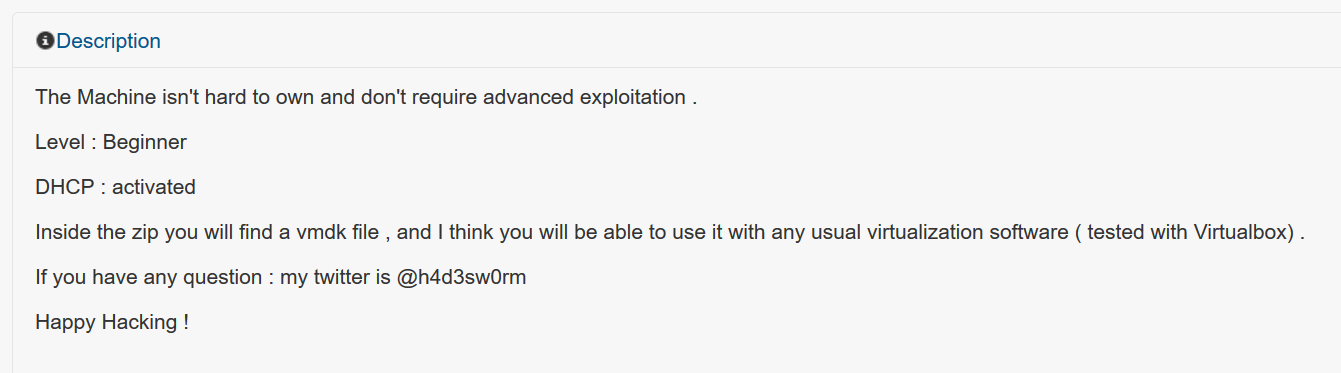
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/toppo-1,245/>

看了一下描述比较适合入门

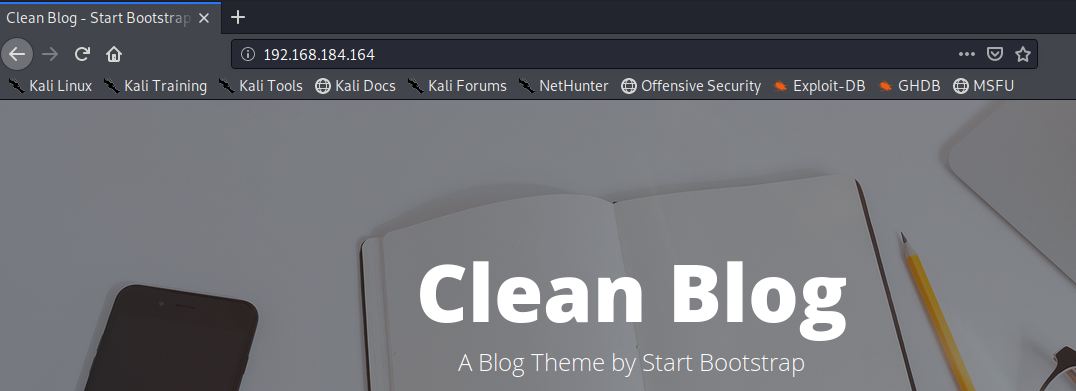


# 0x01:探测靶机

这次启动靶机以后会弹出它的IP出来

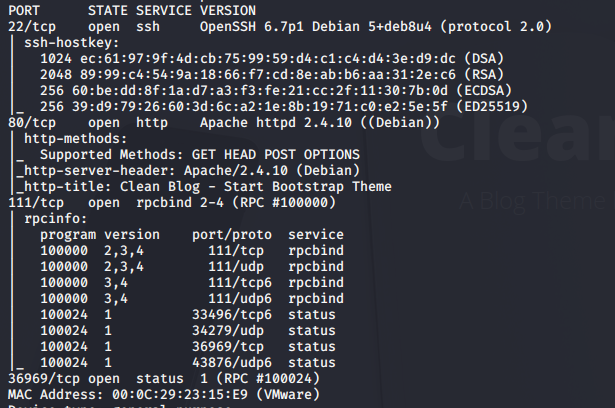


用浏览器输入一下，返回页面正常可以确认是靶机IP



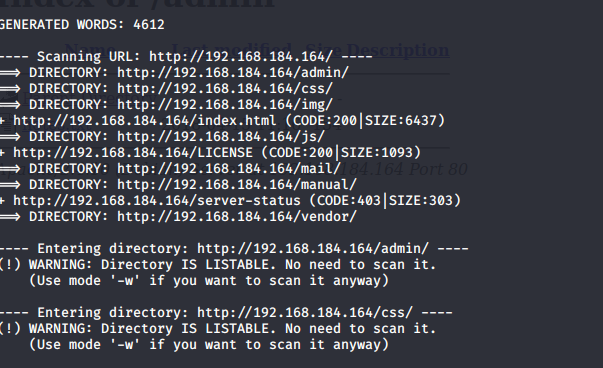
开始用nmap探测一下端口,开了22，80，111和36969端口

命令:nmap -A -sS -sV -v -p- 192.168.184.164

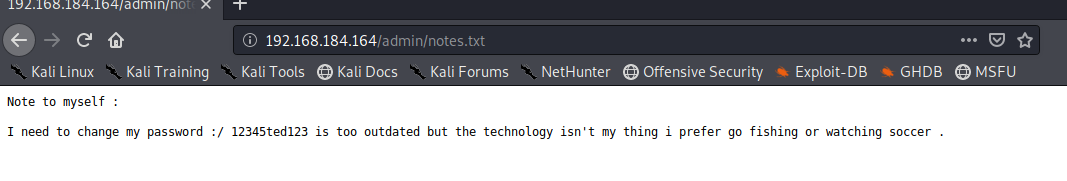


# 0x02:挖掘信息

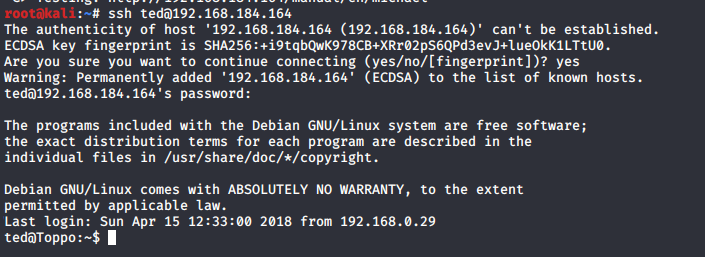
开始用dirb扫目录，扫到很多东西，先跟进/admin/



Admin目录下有个Notes.txt

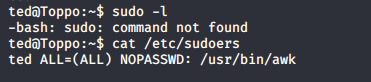


这里有个信息password :12345ted123 划重点，而且刚才开了22 SSH端口，用户名从密码信息中知道可能是ted，尝试一下，成功连接



# 0x03:提权

首先使用sudo -l,发现用不了，用cat /etc/sudoers发现ted 目前可以已root权限运行/usr/bin/awk程序



关于awk 的提权我参考了下这篇文章<https://www.hacknos.com/awk-privilege-escalation/>当然这里要去掉sudo，同时不知道为啥进入不了shell但是可以替换里面的指令,来读取到最后的flag

命令: awk 'BEGIN{system("whoami")}'

awk 'BEGIN{system("ls /root")}'

awk 'BEGIN{system("cat /root/flag.txt")}'

