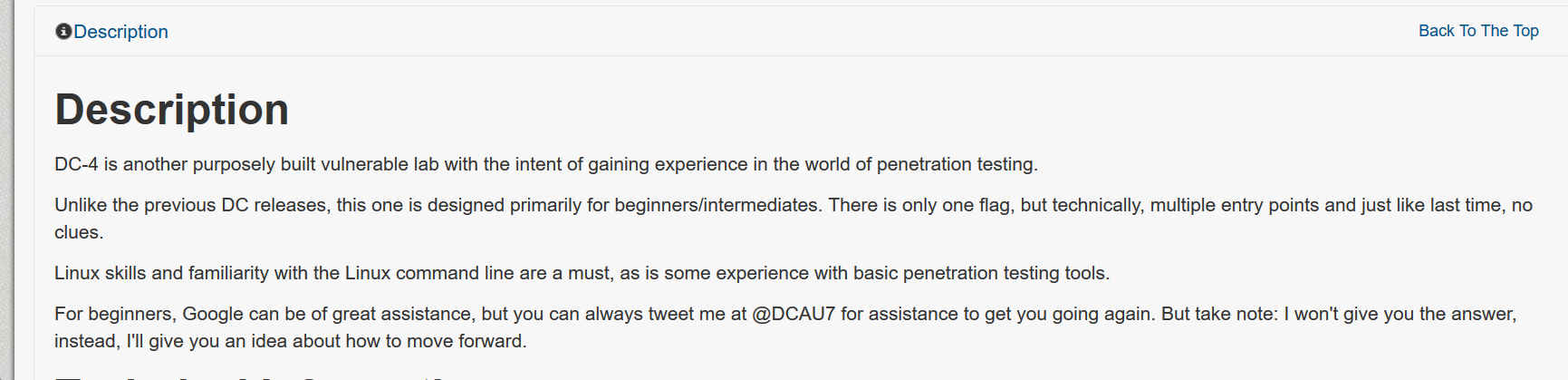
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/dc-4,313/>

看了一下总的来说是新手/中级水平只有一个flag应该就是在root目录下



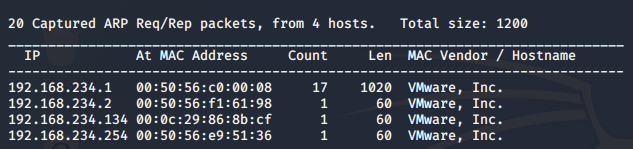
安装的话虽然他建议是用VirtualBox,为了防止中途翻车我还是用VM安装了，直接导入然后调成NAT就可以运行了



# 0x01:探测靶机

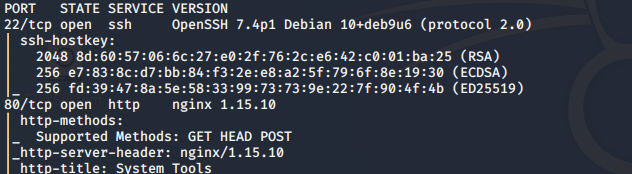
还是先用netdiscover探测一波靶机IP,排除.1,.2和.254可以确定靶机IP为192.168.234.134

命令:netdiscover -r 192.168.234.0/16

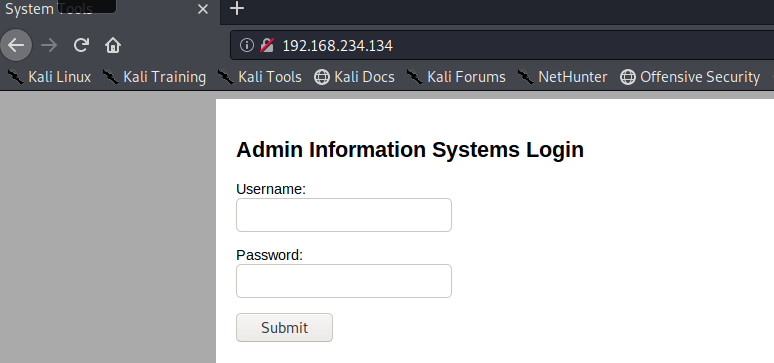


开始用nmap探测波端口,这次只开了22和80

命令:nmap -A -sS -sV -v -p- 192.168.234.134

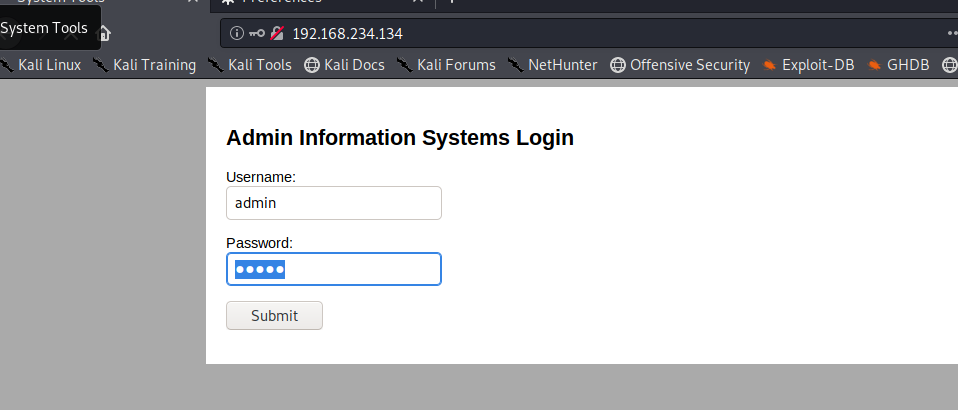


先正常访问一下IP，可以正常回显，可以开搞

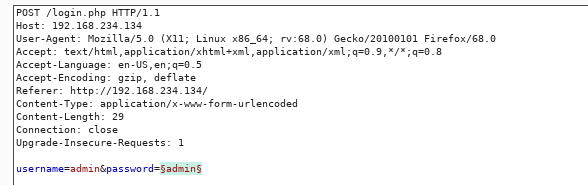


# 0x02:挖掘漏洞

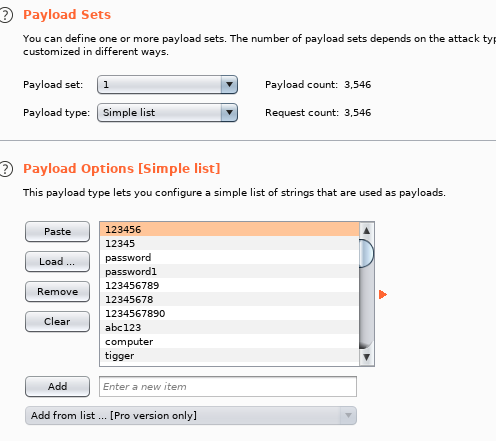
由于是一个登录框能搞的方法是sqlmap和爆破，sqlmap测试了一下没注入，只能尝试Burp爆破了



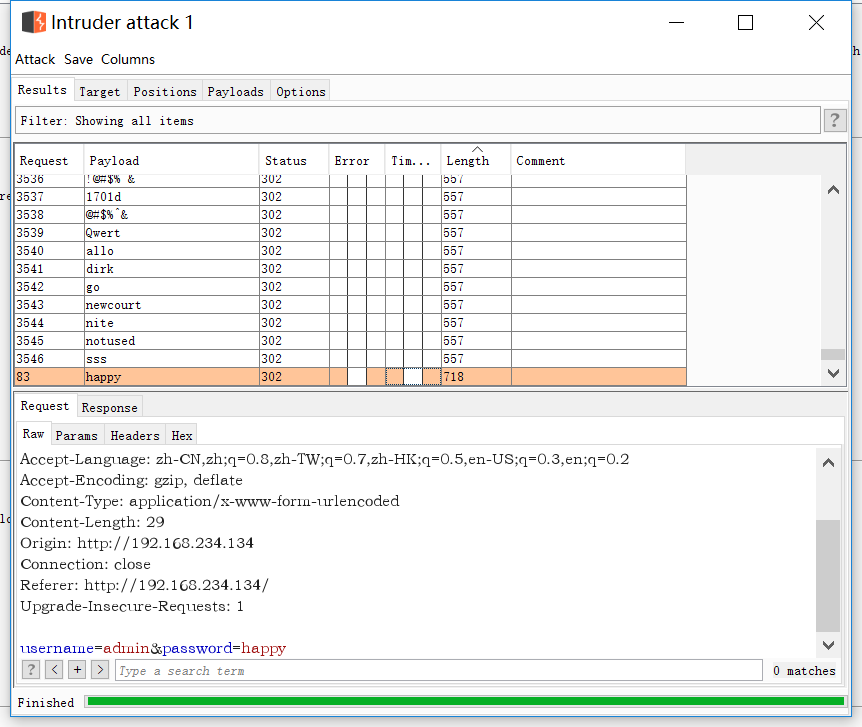
用Burp抓包以后发送到Intruder,假设用户名为admin,爆破其密码



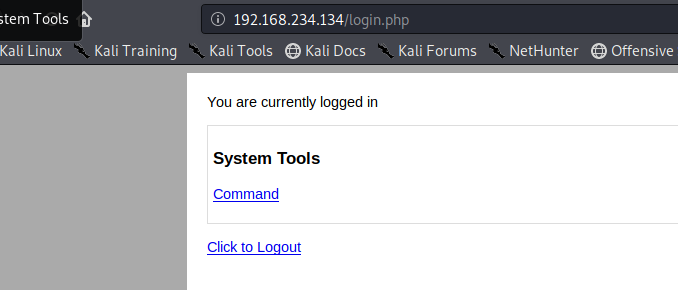
在payload里面加载字典，字典我选择的是john的自带字典位置在/root/john1.80/run/password.lst,然后点击start attack等待一波



等了一会以后，看长度看到happy是最与众不同的仔那密码应该就是它了

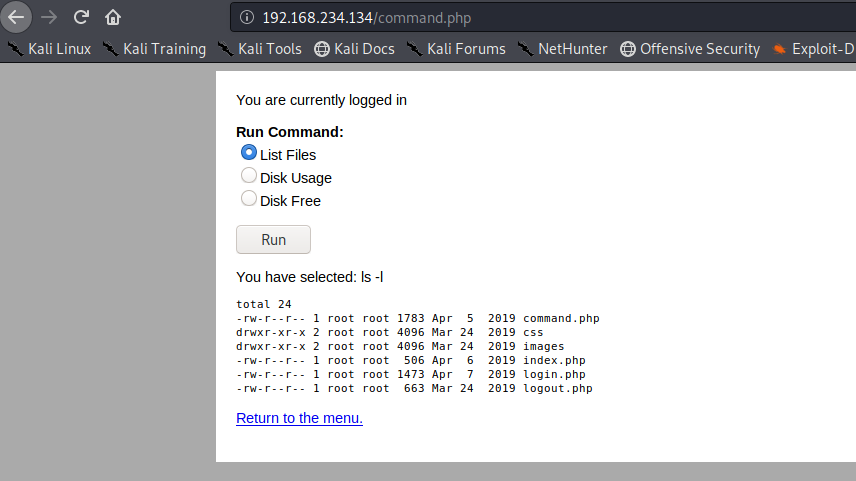


成功登录

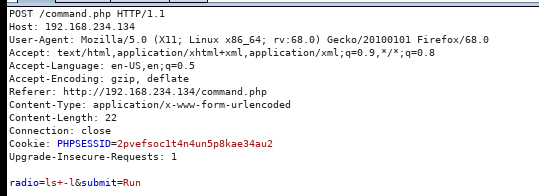


# 0x03:挖掘命令执行漏洞

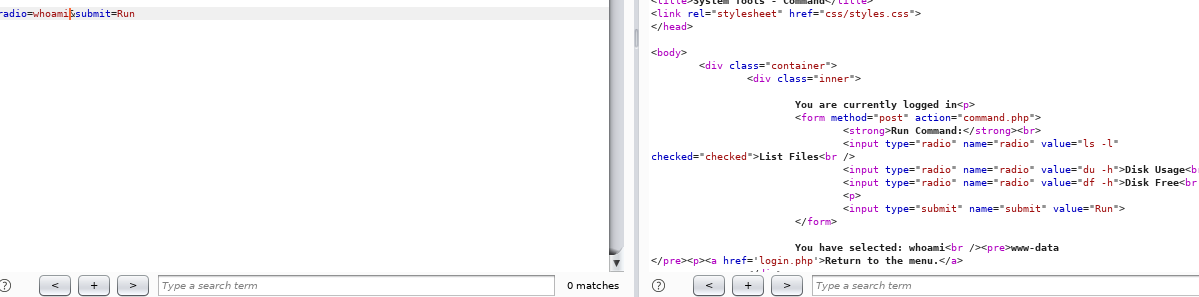
这里点击command以后会有3个选项，这里我选择list files然后点击run以后效果跟ls一样

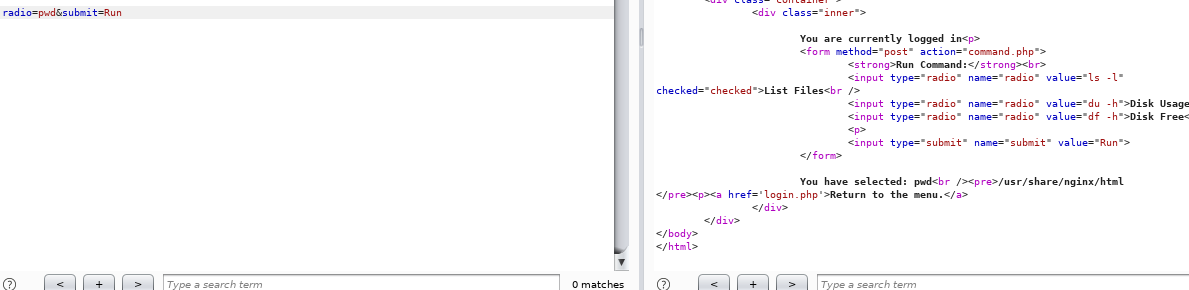


这里用burp抓包然后发送到repeater,可以看到多了个radio=命令

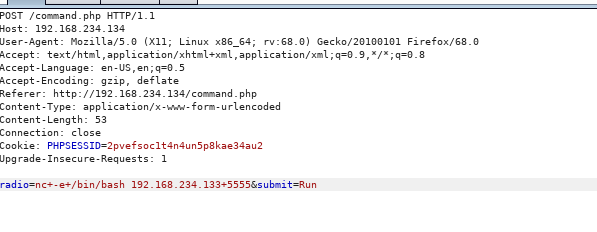


测试了一下whoami,和pwd都可以成功运行，这里确实存在命令执行漏洞

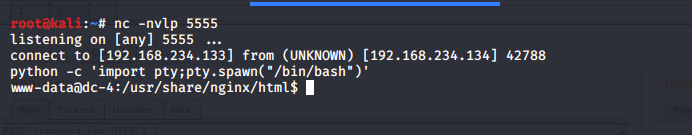




然后插了netcat一句话反弹空格用=表示

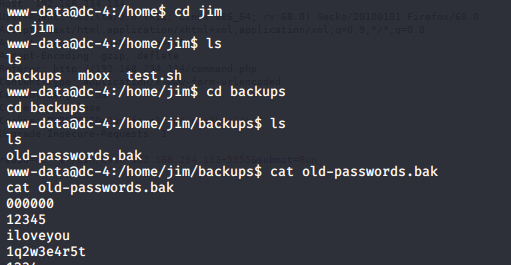


提前开启netcat得到反弹shell

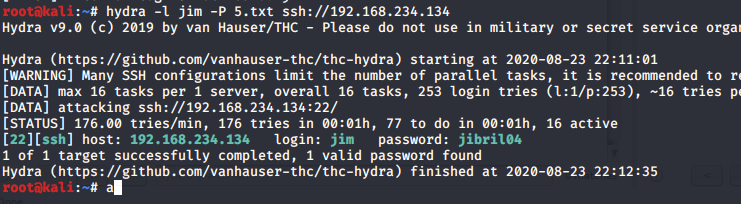


# 0x04:挖掘信息

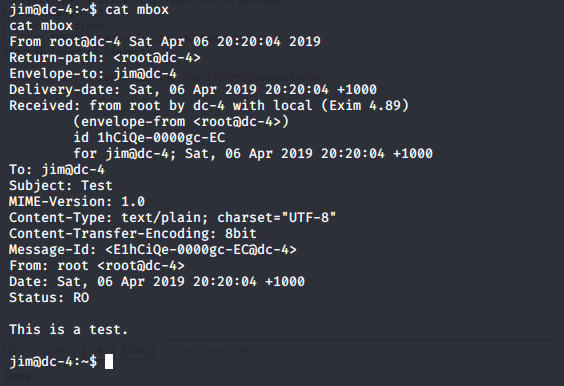
这里来到jim目录下发现一个backups继续跟进以后发现一个Old-passwords里面可能是包含一些密码而用户名就是对应的jim



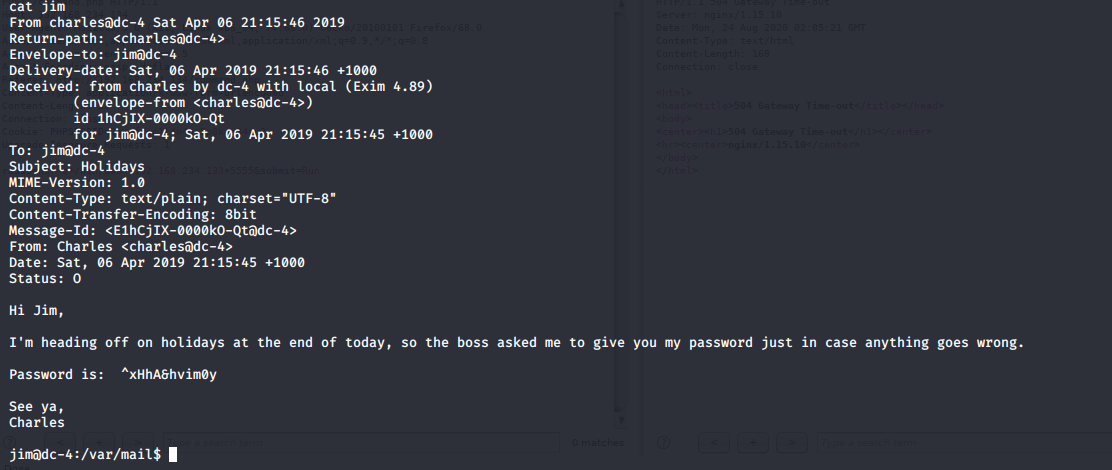
把密码全部保存下来为5.txt利用Hydra爆破，成功跑出来一个



利用su成功切换以后cat一下mbox好像是root给jim的信



这里为了查阅看看还有没有其它的信到/var/mail目录下cat一下jim发现charles的账号密码信息

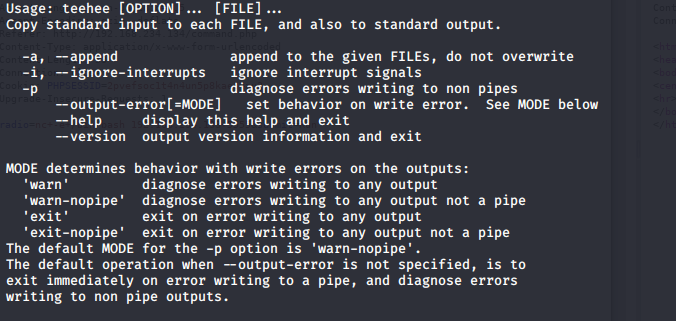


# 0x05:提权

经过多次套娃终于确认不用再切换用户开始提权了，先用sudo -l可以看到一个可以以root运行teehee



用—help可以查看使用命令简单的俩说就是把输入写成文件-a的话加多一个新的

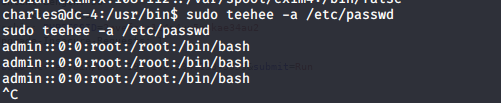


既然可以添加的话我们可以尝试添加一个账号然后设置成root权限就可以了这是cat /etc/passwd的root用户密码格式

root:x:0:0:root:/root:/bin/bash

同理模仿一下设置成这个样子::是代表无密码

语句: admin::0:0:root:/root:/bin/bash



然后直接就su admin无密码登录获得root权限可以读到flag

