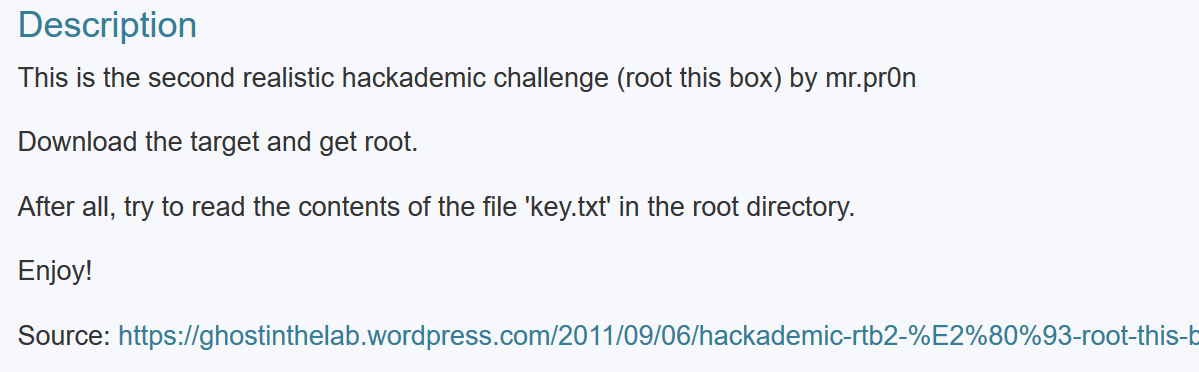
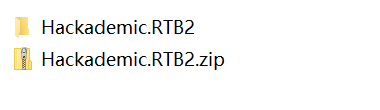
# 0x00:下载靶机

下载链接: <https://www.vulnhub.com/entry/hackademic-rtb2,18/>

目标是得到root权限，顺便读取里面的Key.txt文件



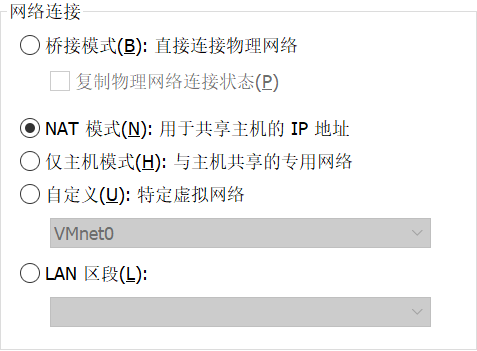
下载以后有个文件夹跟进



点击其中的.vmx会自动打开VM顺便安装好



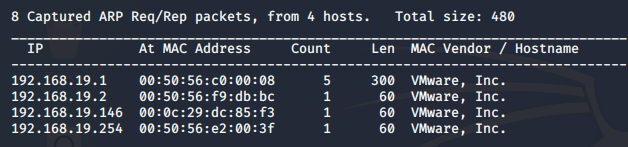
不过要记得改为NAT模式就可以运行了



# 0x01:探测靶机

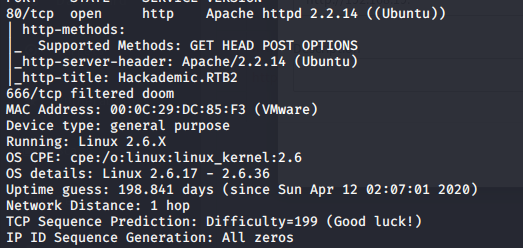
还是先用netdiscover探测一波,排除.1,.2和.254可以确定靶机IP为192.168.19.146

命令:netdiscover -r 192.168.19.0/16

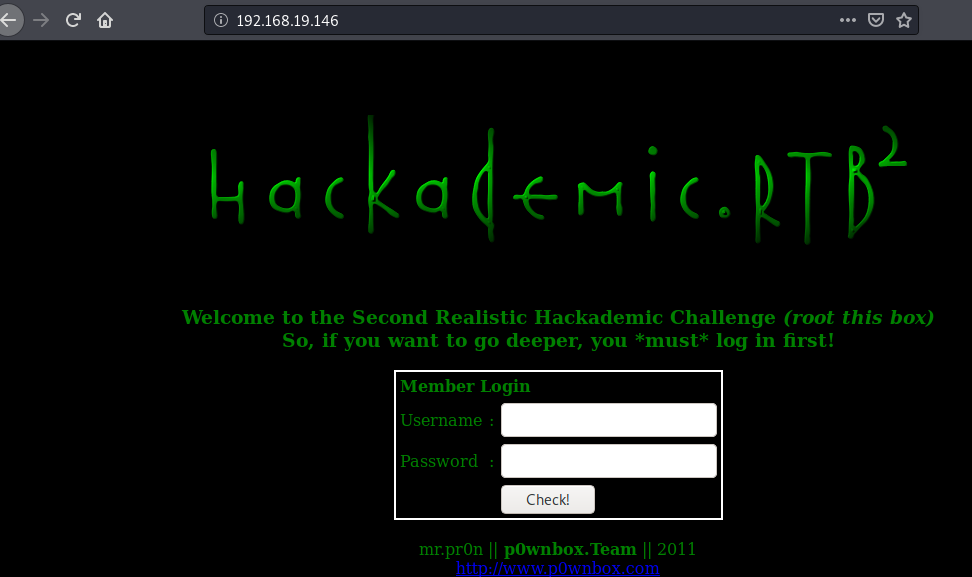


开始用nmap探测一波，这次没开22，只有80，和一个过滤的666端口

命令:nmap -A -sS -sV -v -p- 192.168.19.146



在浏览器输入IP，可以正常访问开搞



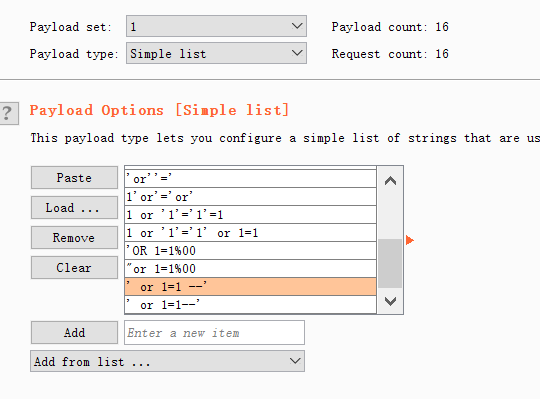
# 0x02:挖掘漏洞

又到了喜闻乐见的登录框了，这里兵分两路，一路用BURP抓包放SQLMAP跑，另一边启动一波万能密码注入一波

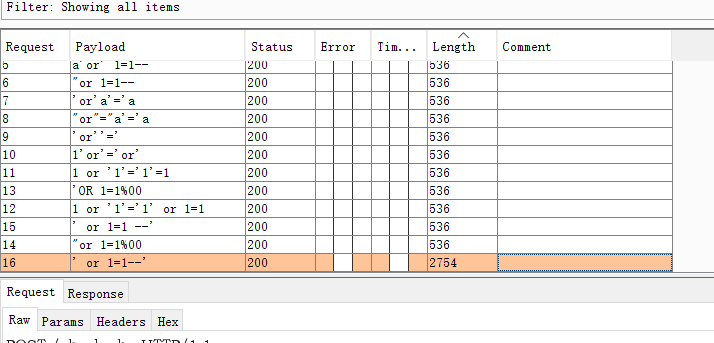
先用BURP抓包然后发到Intruder,我们的目标是在password那里



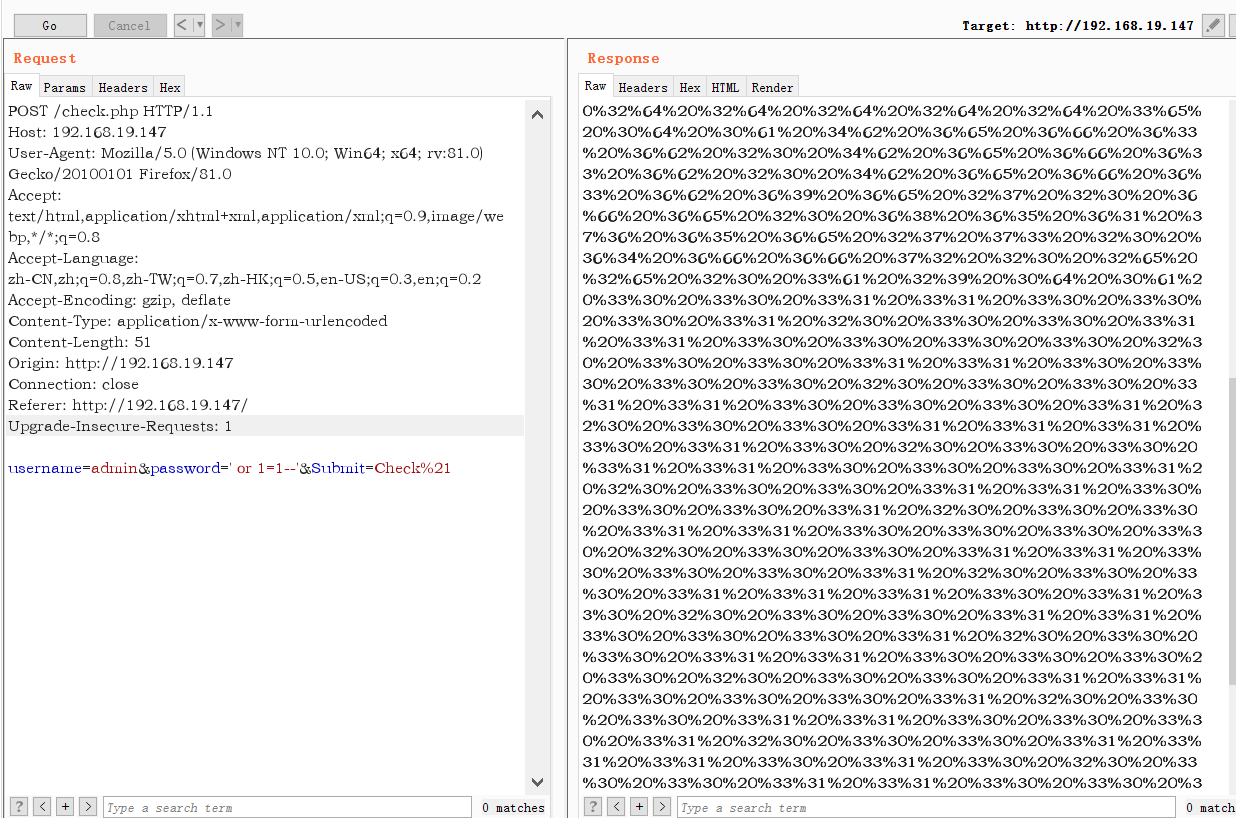
然后点击payloads,从网上收集了一波常见的万能密码



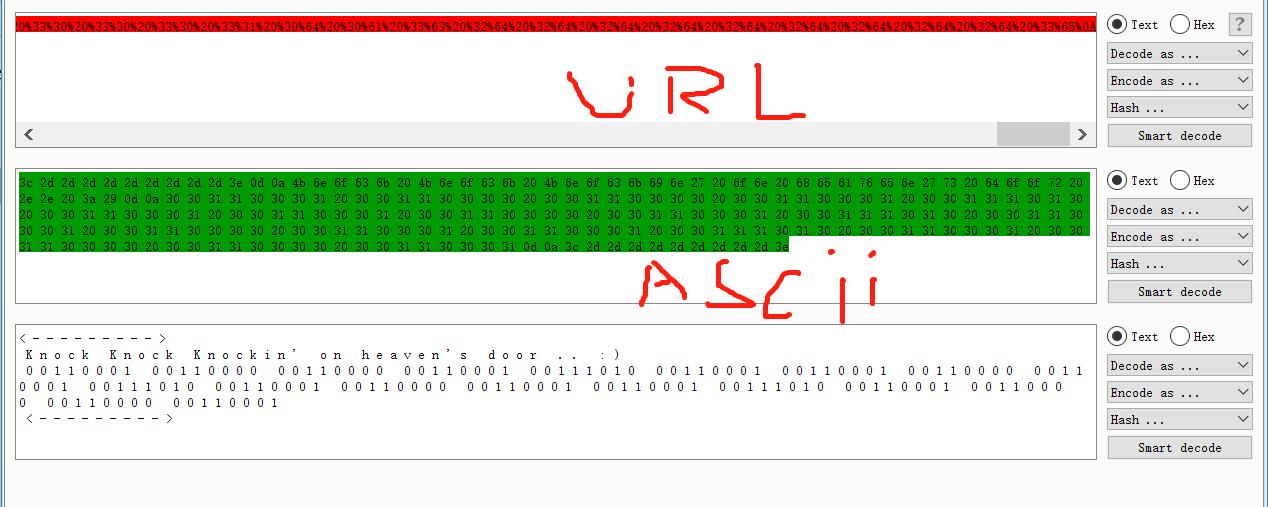
然后点击 start attack选项，注入开始。发现了个长度与众不同的。有可能登录成功了。



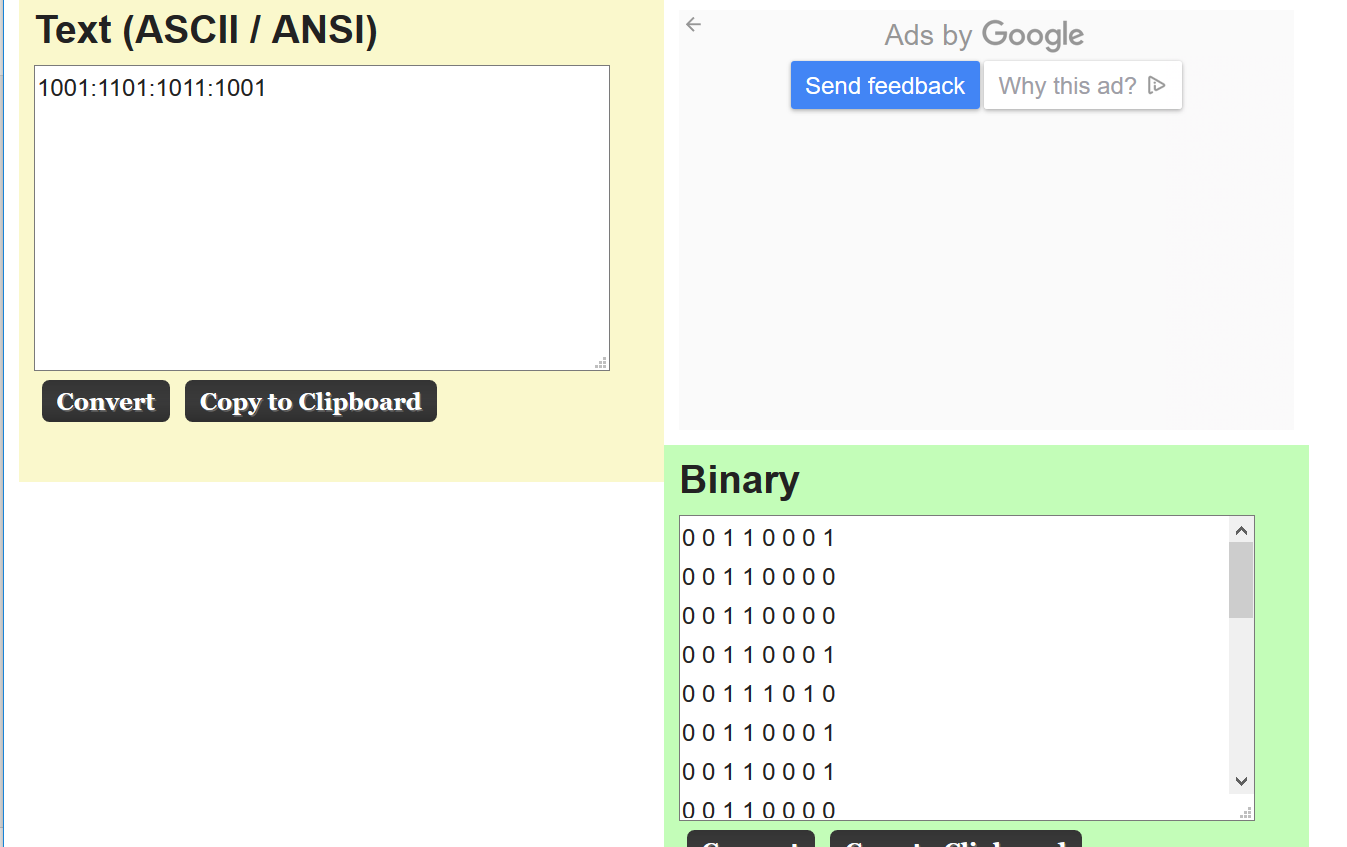
发到REPEATER，发现了一堆又臭又长的不知道什么鬼加密



经过不断尝试，首先先来波URL解码，然后在来波ASCII解码，终于看到点文字，虽然下面是0和1

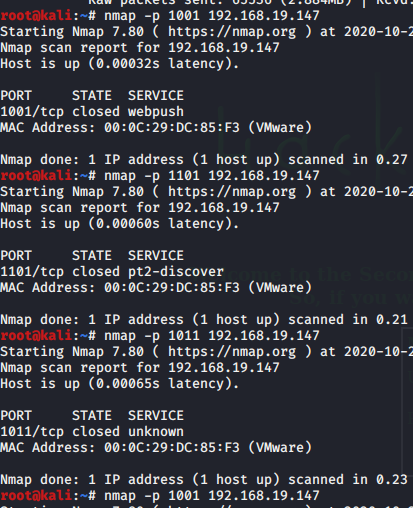


解到这里，有点懵逼，因为直接转换二进制你是不明白啥意思的，<https://www.asciitohex.com/>，我用这个网站在把二进制往回转你才能得到点正常答案。结合答案那就是需要敲1001，1101，1011，1001端口才能解封666端口

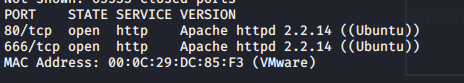


# 0x03:探索666端口

这里用nmap把这四个端口先敲一遍



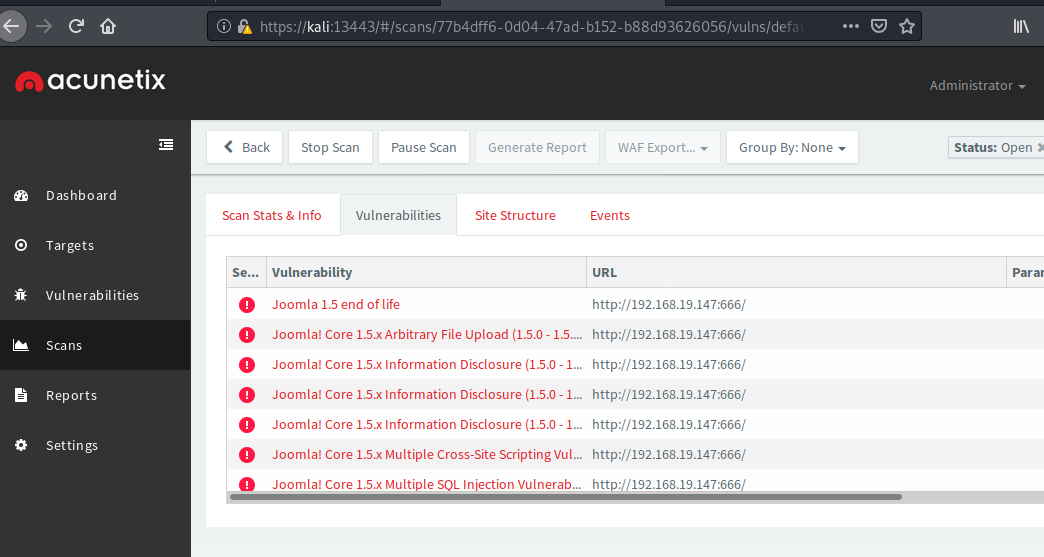
然后用nmap重新扫描一波，发现666端口重开了



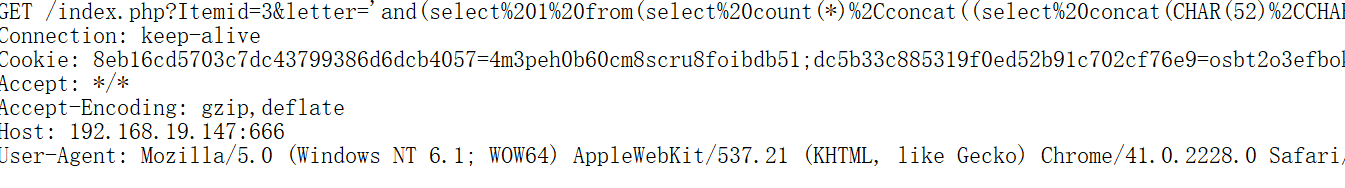
输入IP这次页面有回显



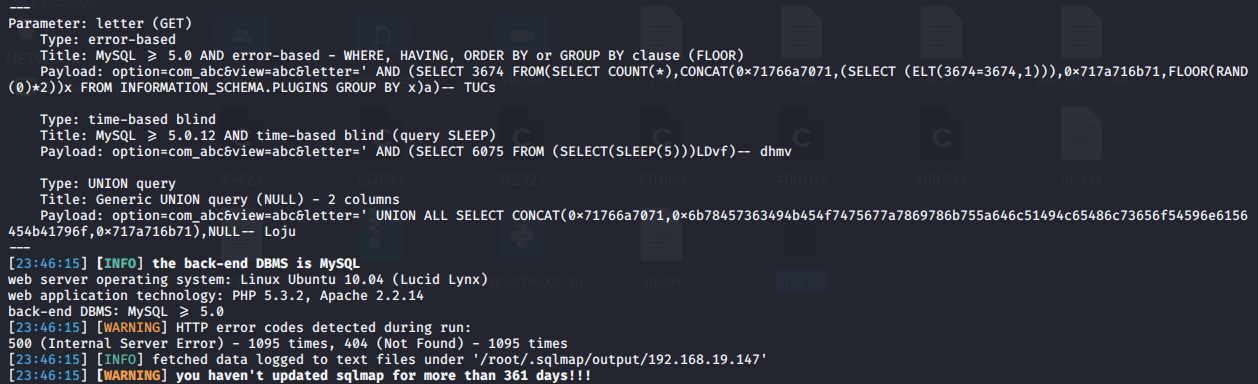
最近在Kali上装了AWVS12，测试了一下可以跑出很多漏洞出来，这里选择SQL注入一波



这里我直接复制一波AWVS扫描出来的payload然后保存为txt丢给sqlmap

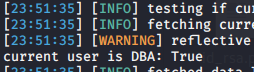


然而AWVS给的payload跑不出来。。。。还不如自己用burp抓个包能跑出来

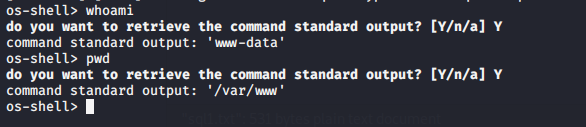


# 0x04:利用sqlmap 获取shell

Sqlmap也可以直接getshell,首先先用—is-dba判断是否为TRUE，如果判断为TRUE，则可以进行下一步—os-shell

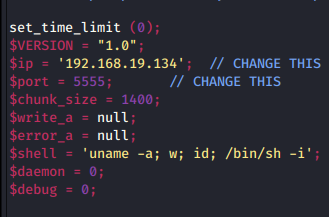


然后直接输入—os-shell, 直接获得一个shell了。

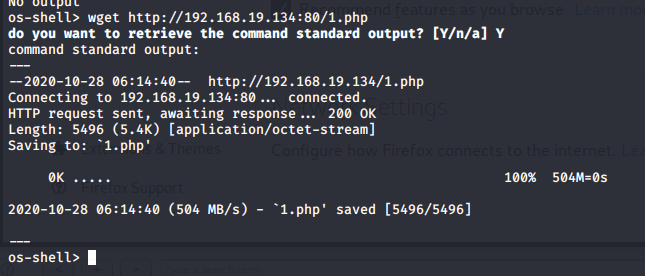


# 0x05:反弹shell

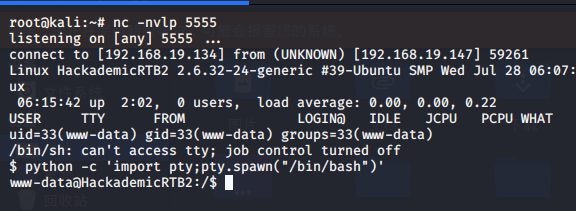
由于sqlmap的shell有点笨所以这里计划改一改，在kali上传一个php反弹shell到sqlmap的shell里面，然后在访问弹回来一个正常点的shell，先把shell改为kali的



然后开启python共享模式，让sqlmap把它下载下来，当前sqlmap的shell的目录是在/var/www/目录下建议不要乱走动把反弹shell放错地方

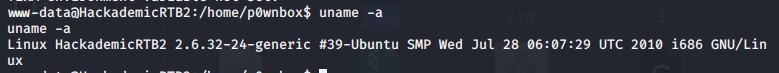


记得提前开启netcat,然后访问192.168.19.147:666/1.php,就能得到一个正常点的shell了



# 0x06:提权

放弃sudo -l因为是反弹shell没得密码不行唉所以Uname -a以下，原来是2.6.32的直接脏牛打死



直接传一个15285.c过来，用gcc编译运行就可以是root权限了

