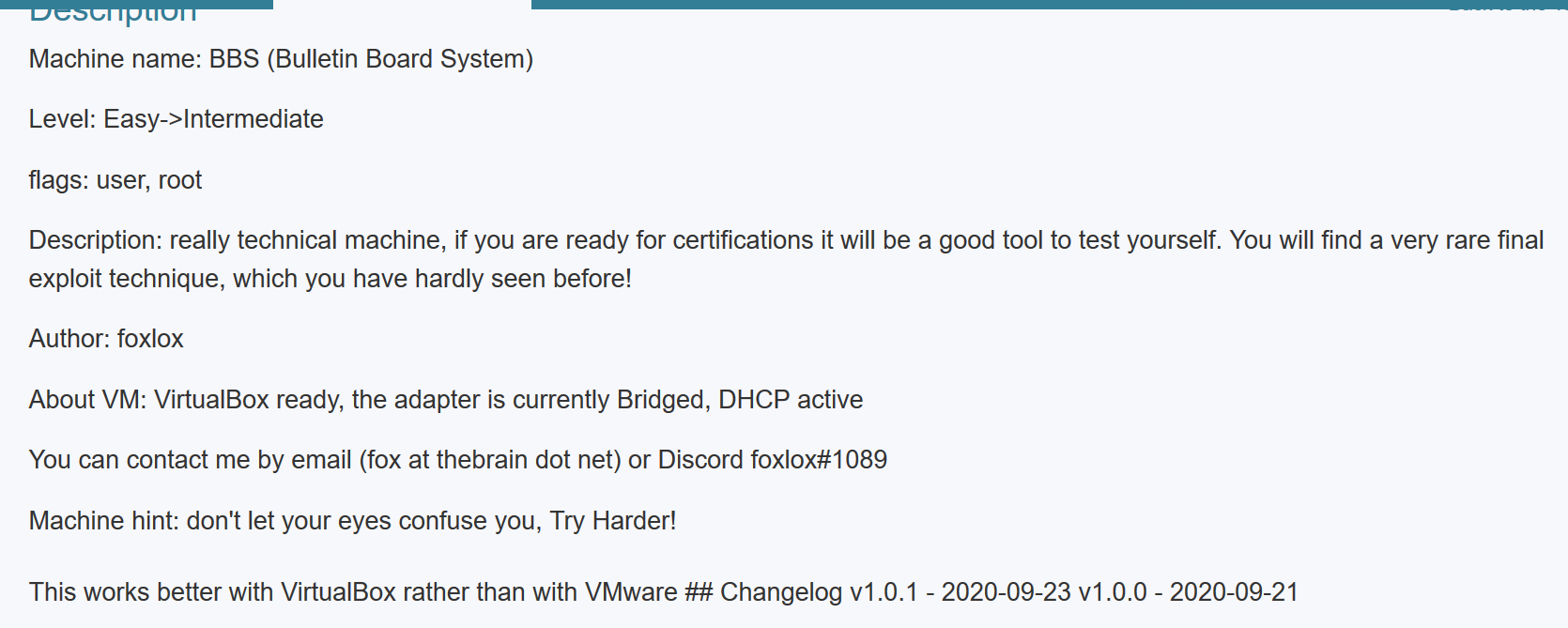
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/bbs-cute-101,567/>

难度简单到中等，2个flag，建议用virtualbox安装

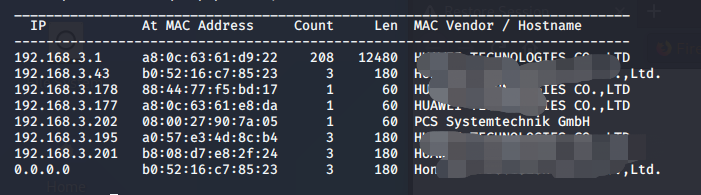


今天就偷懒写安装方法了直接开始探测靶机

# 0x01:探测靶机

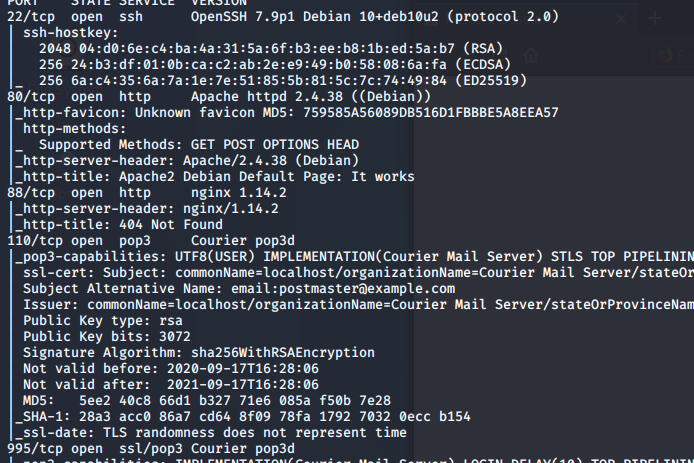
先用netdiscover探测波靶机，直接找PCS可以确定靶机IP为192.168.3.202

命令:netdiscover -r 192.168.3.0/16

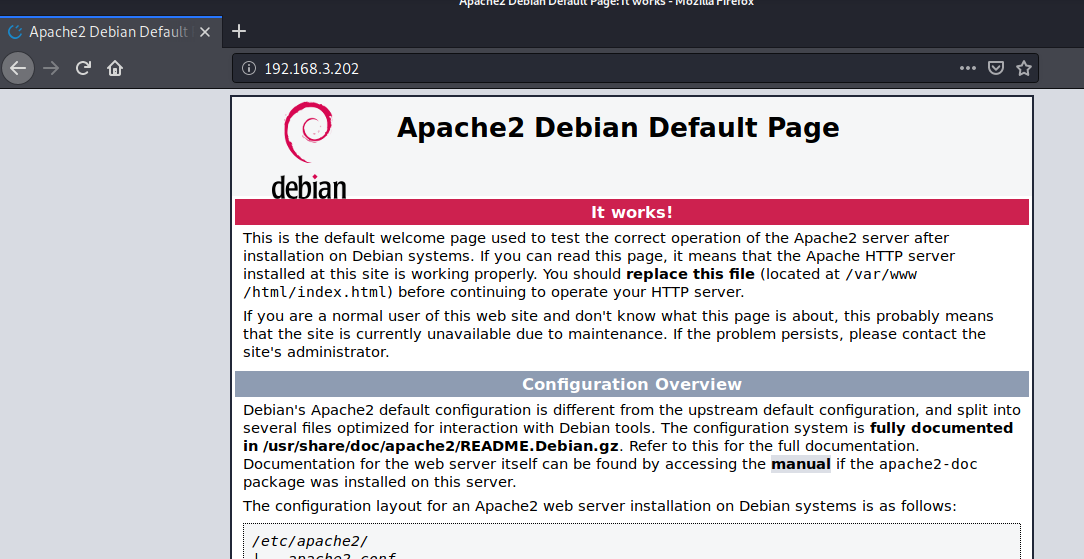


然后开始用nmap探测波端口,这次开了22，80，88，110，995端口

命令:nmap -A -sS -sV -v -p- 192.168.3.202

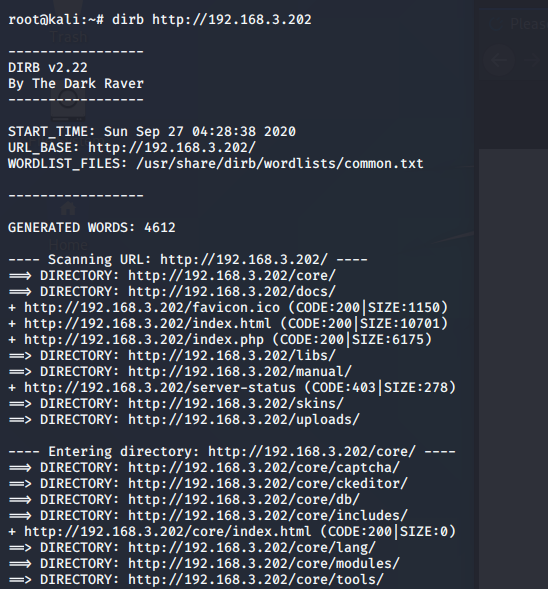


访问波IP可以正常回显，开始挖掘

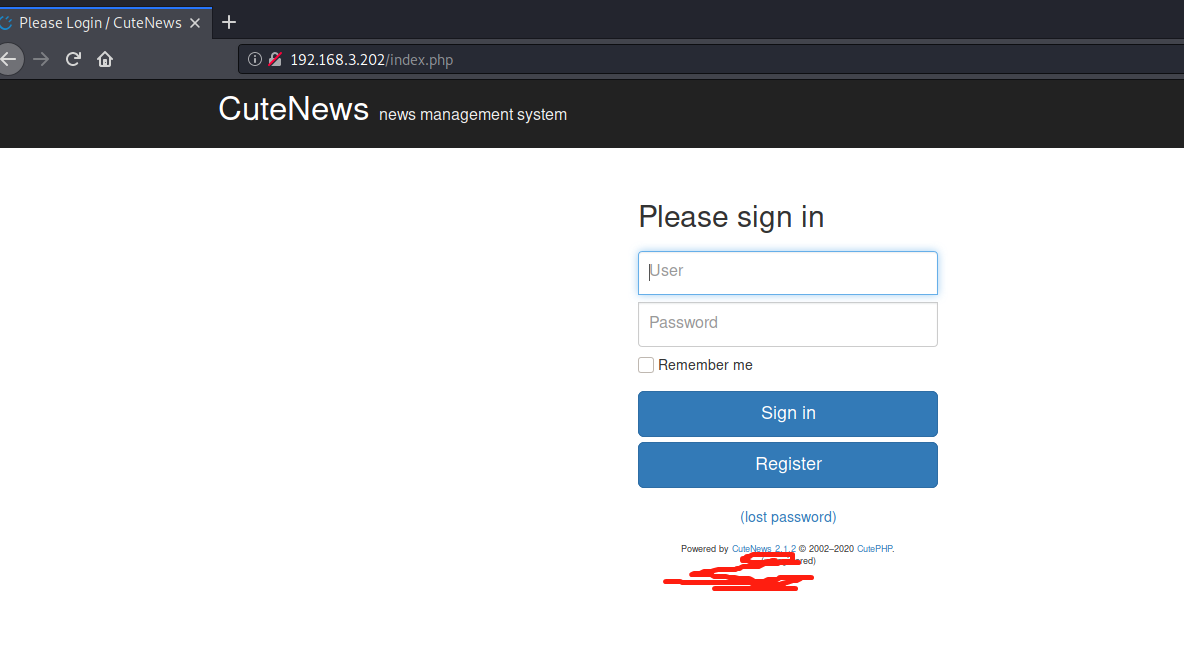


# 0x02:漏洞挖掘

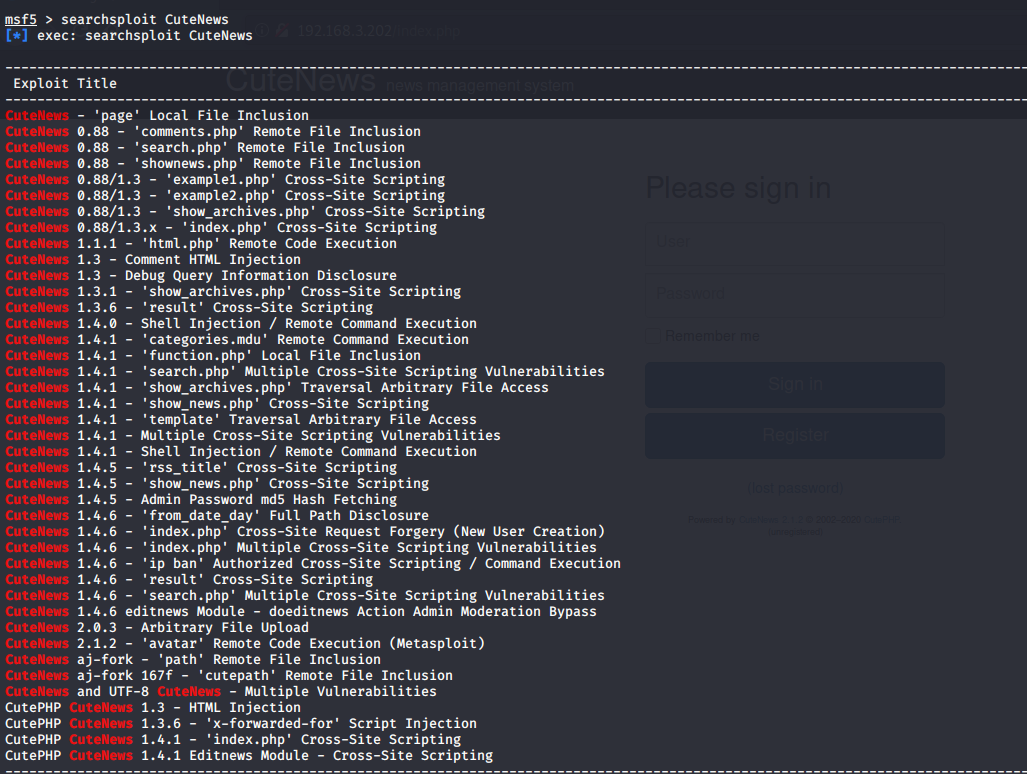
由于不是正常的HTTP服务页面先用dirb探探路，挖到一些好东西



逐一跟进，跟进到index.php的时候是个登录界面而且底下有个大大的powered by CuteNews这个字样可以确认这是个CMS

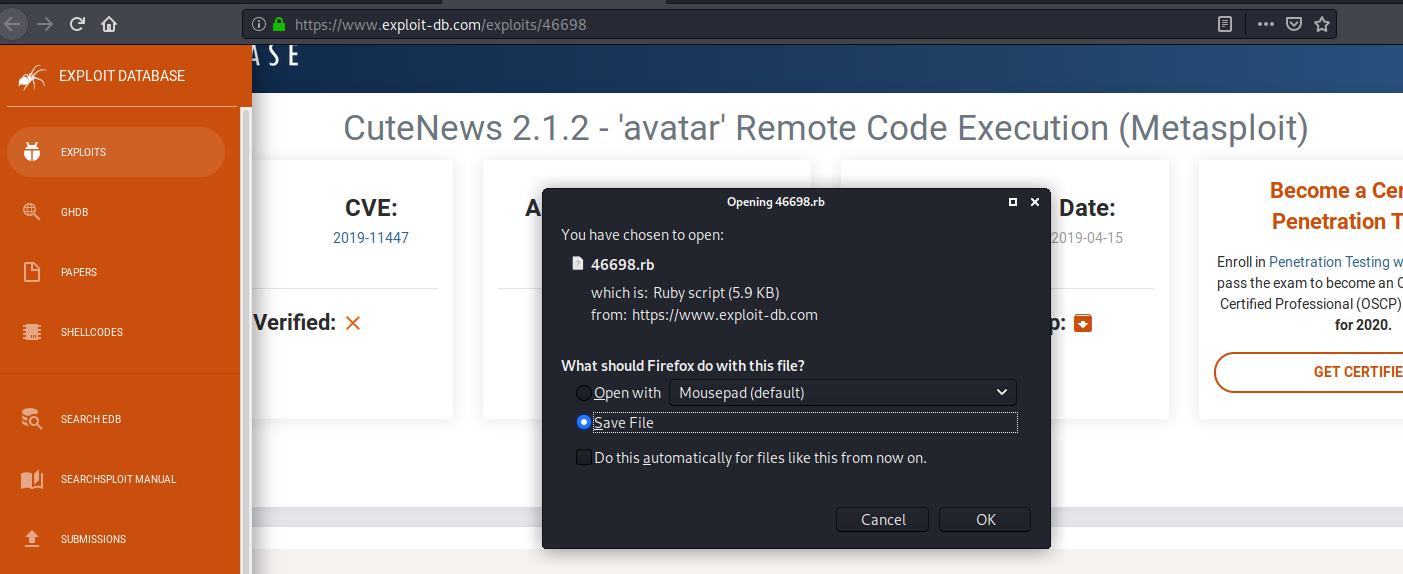


这里启动MSF搜索了一下有关于这个CMS的payload，但是本地没有。。。。。

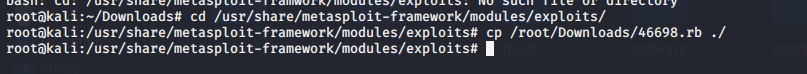


# 0x03:下载payload

所以先去exploitdb下载下来先

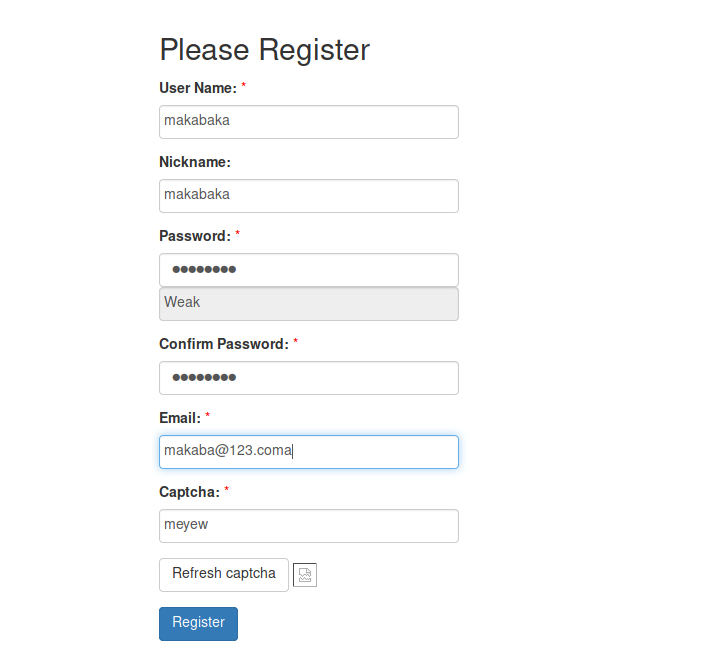


默认下载保存的地方是在/root/Downloads下，然后要把该文件复制到MSF的保存地方让它下次运行的时候可以加载出来。MSF默认存储payload位置是在/usr/share/metasploit-framwork/modules/exploits(这里我用的方法是先去到目标目录然后复制/Downloads的文件过来，也可以直接在/Downloads下直接复制也可以，多种方法仅供参考)



用了show options以后才发现首先需要一个账号先。。。。。所以返回注册一波

账号密码均为makabaka



最后这是需要设置好的参数

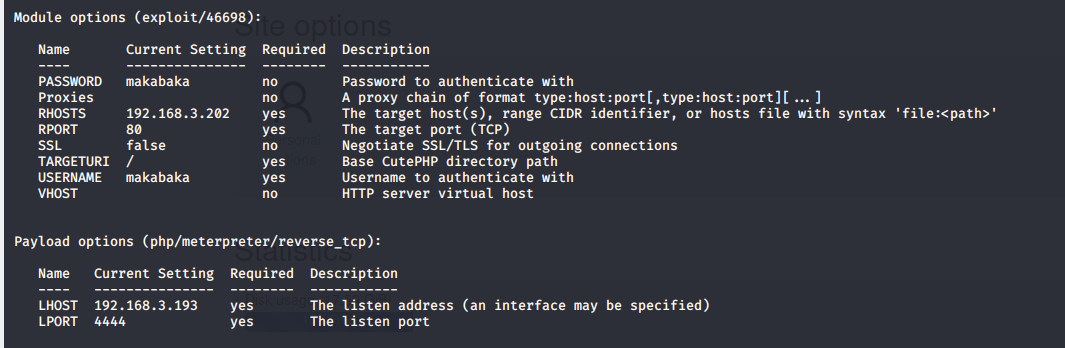
命令:use 46698.rb

Set USERNAME makabaka

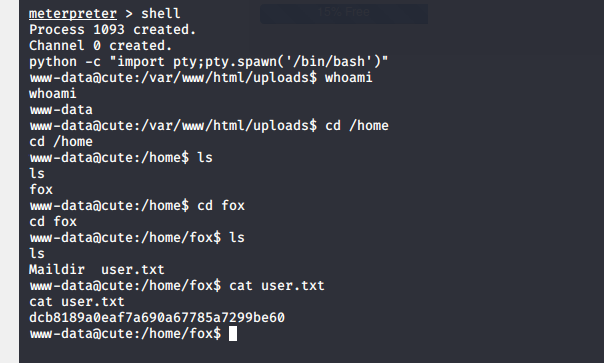
Set Password makabaka

Set RHOSTS 192.168.3.202

Set TARGETURI /

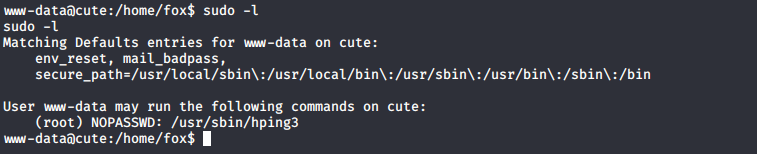


然后等待一下，出现meterpreter就是代表成功了，然后进入shell模式打一个python交互式shell进去顺便得到第一个user的flag

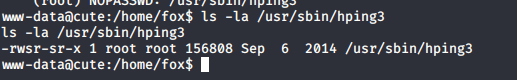


# 0x04:提权

害，sudo -l终于又可以正常运行了，发现有个hping3,只不过又陷入迷茫了，hping3又是啥玩意



查了一下，hping3似乎是一个DDOS工具，然后再看了一下是个二进制文件



尝试一波运行，emmmm咋说了挺意外的。直接一头撞过去就行了，还不如给我整个无密码切换root

