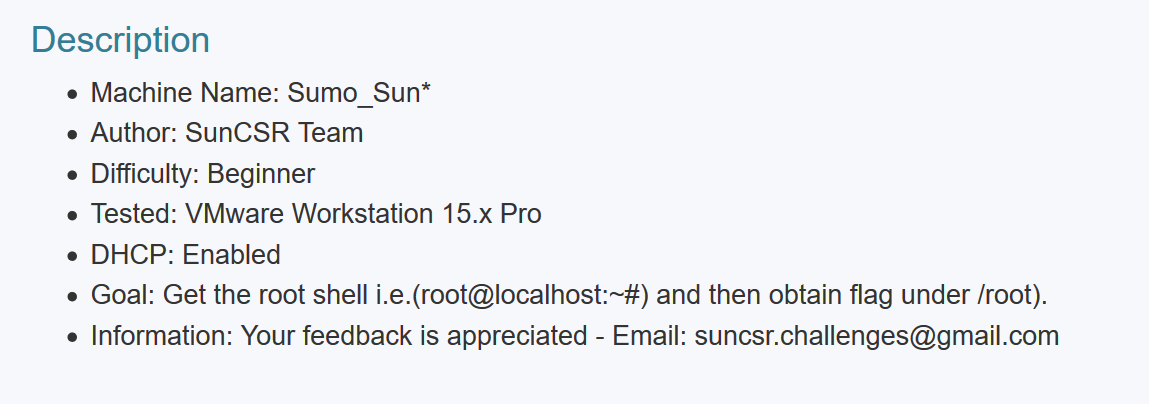
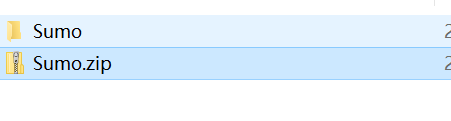
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/sumo-1,480/>

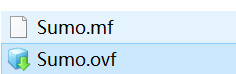
新手级别，VM下做目标是获得root的权限



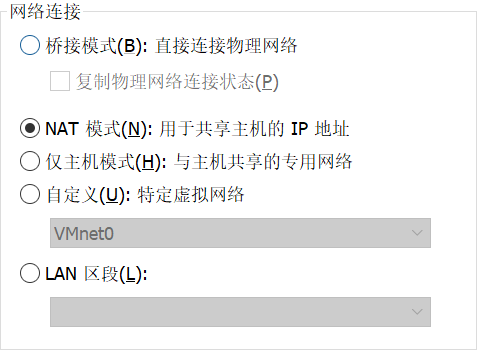
下载完解压跟进sumo



点击.ovf然后选一个地方存放



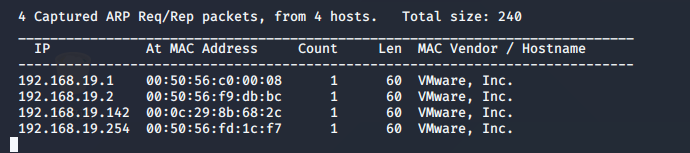
记得调回NAT模式



# 0x01:靶机探测

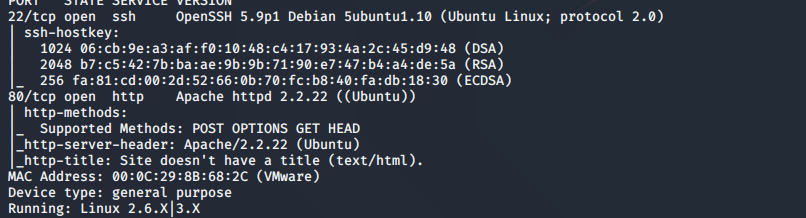
先用Netdiscover探测一波,排除.1,.2可以确定靶机IP为192.168.19.142

命令:netdiscover -r 192.168.19.0/16

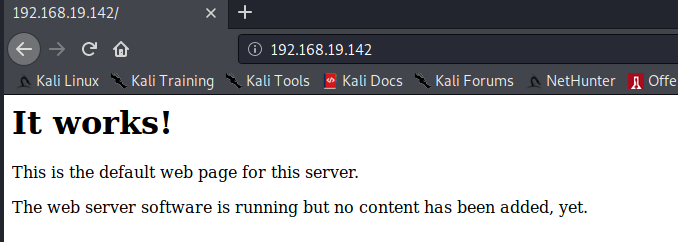


开始用nmap探测波端口，不过只开了22和80

命令:nmap -A -sS -sV -v -p- 192.168.19.142

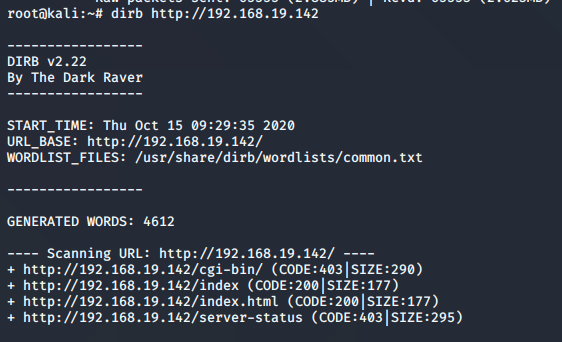


访问波IP，页面回显正常

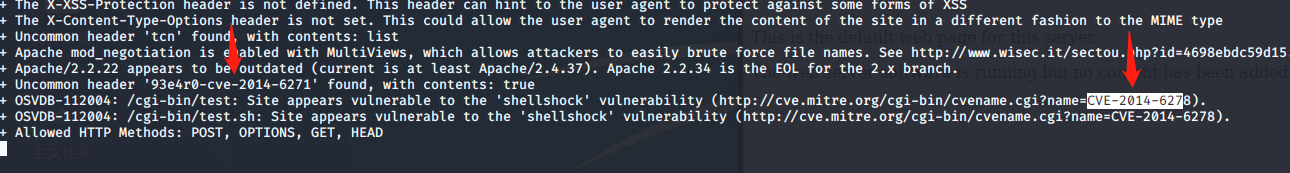


# 0x02:挖掘漏洞

先用dirb探探路，然而东西太少了

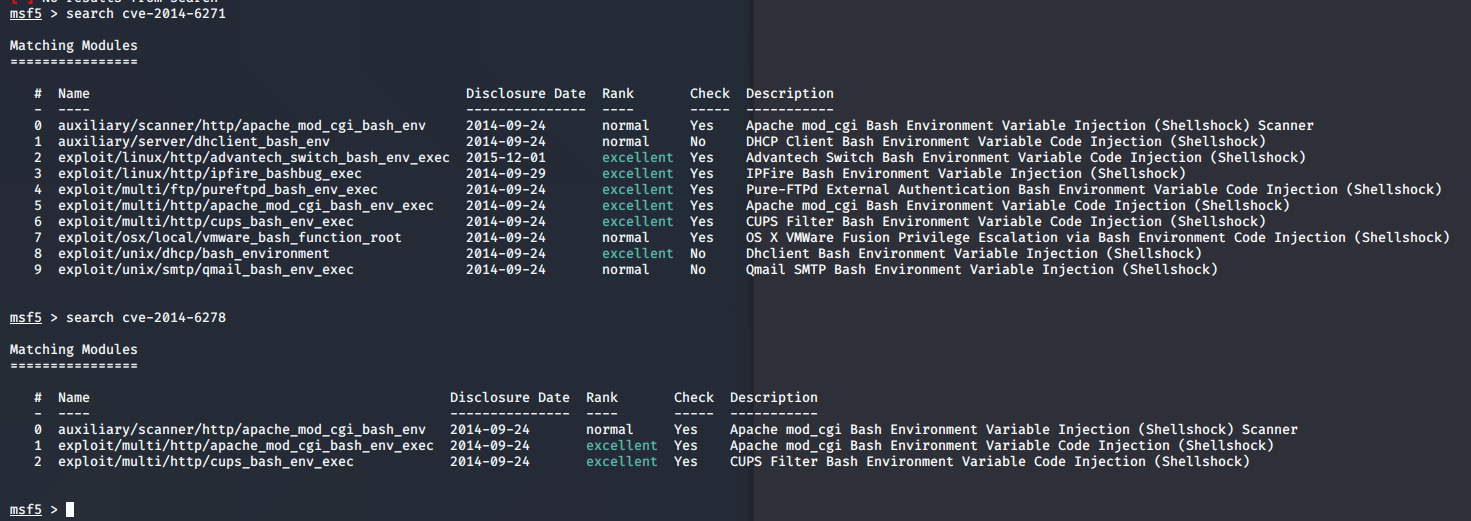


在用dirb扫的时候也用了nikto,扫出点东西，可能存在CVE-2014-6271和CVE-2014-6278漏洞



# 0x03:利用MSF寻找payload

那么MSF启动然后也用search找到了对应的payload



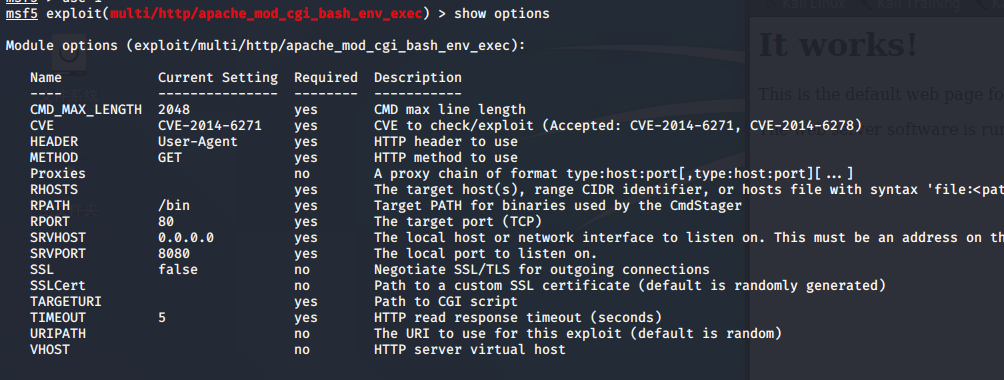
这里比如说用下面的第一个

命令: use 1

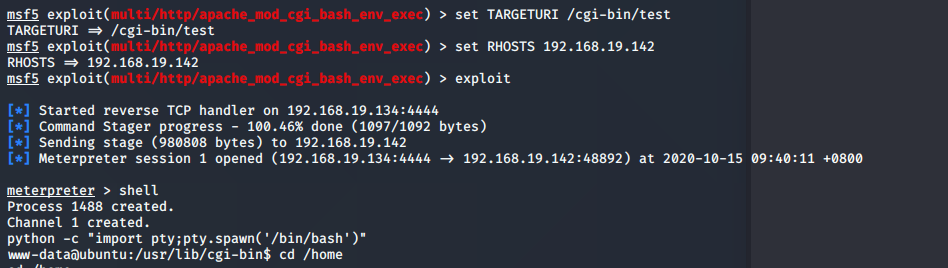
Set rhosts 192.168.19.142

Set TARGETURI /cgi-bin/test

exploit

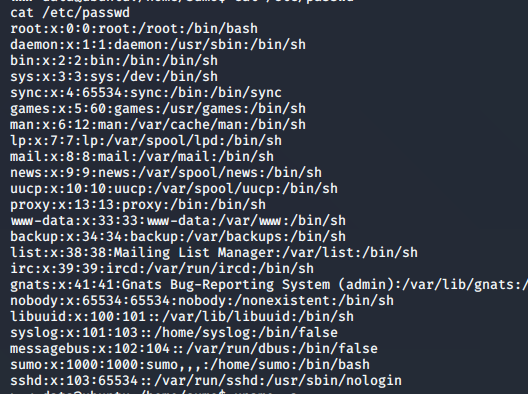


Exploit完出现个meterpreter就是代表成功了然后进入shell模式打一个python的shell进去

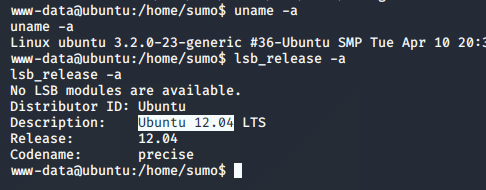


# 0x04:提权

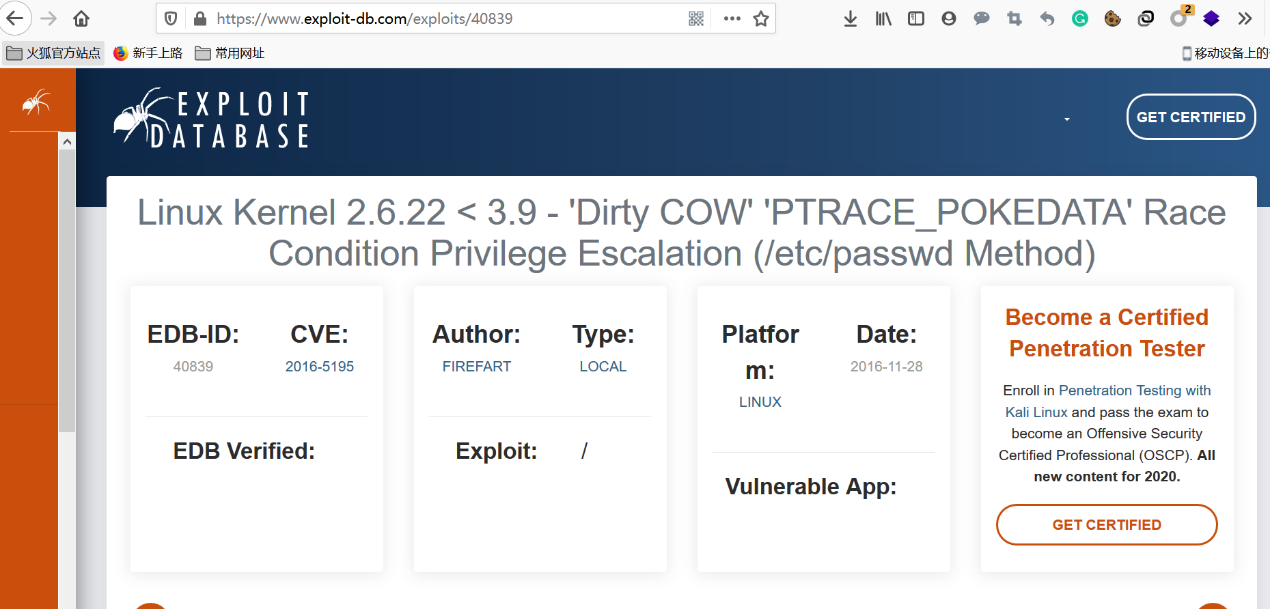
拿到www-data的权限以后想去/home目录下发现sumo但是里面没信息，所以找一波用户名，有个正常点的是sumo让hydra跑一跑



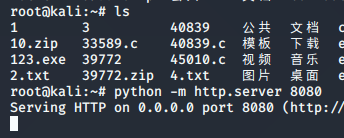
在跑的时候顺便用uname -a 和 lsb\_release -a提取内核和版本信息



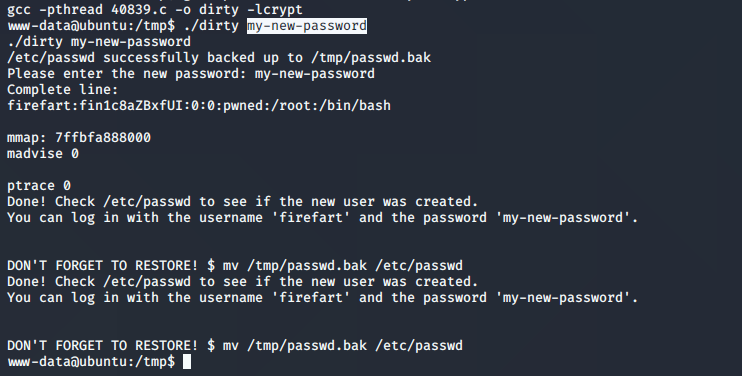
在exploitdb上找到这个<https://www.exploit-db.com/exploits/40839>



下载到kali里面然后开启共享



然后在靶机那里下下来，运行方法很简单gcc编译一波然后按照<https://www.exploit-db.com/exploits/40839>这里教的步骤和方法进行运行，等待一波提示可以用firefart 和my-new-password出现为止



因为之前探测端口的时候已经知道开了22端口所以直连，登录以后已经是root权限了可以读到flag,然而强行爆破sumo到现在还没成功。。。。。。

