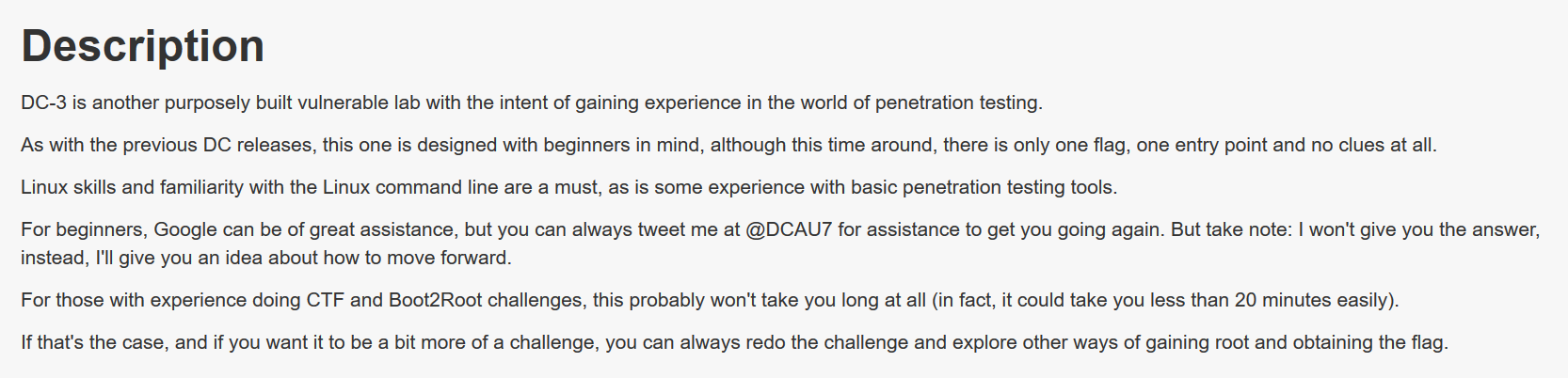
# 0x00: 下载链接

下载链接: <https://www.vulnhub.com/entry/dc-32,312/>

看了一下描述，本次靶机只有一个flag



解压完后有个.ova文件



点击选择一个合理的位置进行安装

A screenshot of a cell phone

Description automatically generated

记得改为NAT模式

A screenshot of a cell phone

Description automatically generated

同时调一下IDE变成0:0设置完成开机即可

A screenshot of a cell phone

Description automatically generated

# 0x01: 探测靶机

先用netdiscover,确认靶机IP排除.1,.2默认网关可以确认靶机IP为192.168.204.133

命令:netdiscover -r 192.168.204.0/16

A close up of a sign

Description automatically generated

然后开始用nmap扫描端口，这次开放的端口比较少，只有一个80端口。不过在http-generator那里显示Joomla，这是一个CMS来着

命令:nmap -A -sS -sV -v -p- 192.168.204.133

A screenshot of a cell phone screen with text

Description automatically generated

再用whatweb探测，确认了是Joomla CMS来的



既然是个Joomla的网站可以访问默认的/README.txt来查看版本信息，可以知道版本为3.7

A screenshot of a cell phone

Description automatically generated

# 0x02: 挖掘漏洞

启动一下MSF，搜索一下Joomla 3.7可以找到一些SQL的漏洞

A screenshot of a computer

Description automatically generated

打开其中的一个已经有SQLMAP的使用方法了

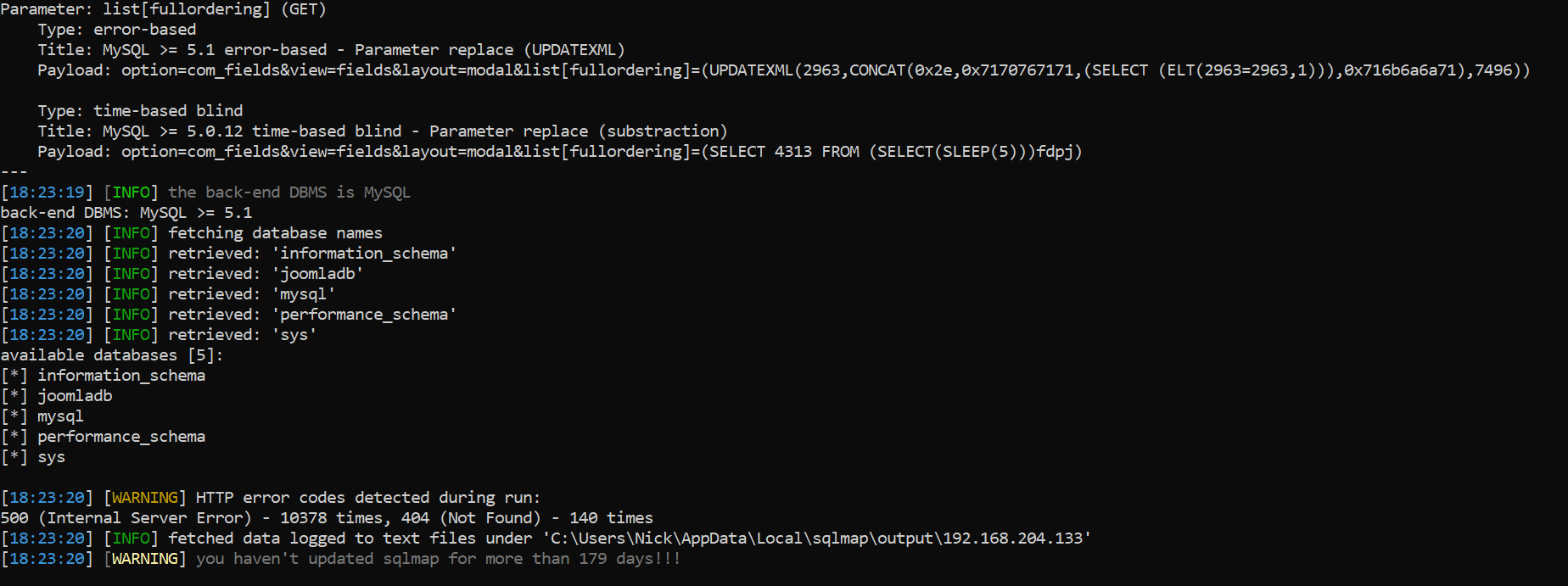
A screenshot of a cell phone

Description automatically generated

直接修改IP地址放到SQLMAP里面跑就行了，然而还是推荐大家在主机跑吧。测试了一下主机跑要10分钟，而kali要跑15分钟。。。。。。。

命令: sqlmap -u "http://192.168.204.133/index.php?option=com\_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent --dbs –batch

Python sqlmap.py -u "http://192.168.204.133/index.php?option=com\_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent --dbs –batch



开始逛该选中joomladb库里面有个users表

A screenshot of a cell phone

Description automatically generated

选中user表里面之后有关键词,username和Password

A screenshot of text

Description automatically generated

直接—dump提取数据除了有点不是很美观之外。。。。

A picture containing table

Description automatically generated

尝试过用在线MD5然而解不出来，最后保存成文本直接跑出密码出来

Admin:snoopy

A screen shot of a computer

Description automatically generated

# 0x03: 上传反弹shell

这里输完刚才得到的账号密码以后成功进入后台接下来就寻找可以修改源码的地方

A screenshot of a computer

Description automatically generated

最后在Extensions/template/template下发现可以更改代码

A screenshot of a social media post

Description automatically generated

然后去到kali目录下/usr/share/webshells/php/的反弹shell复制里面的代码

A screenshot of a cell phone

Description automatically generated

然后把代码贴上去，修改IP地址和端口

A screenshot of a social media post

Description automatically generated

然后点SAVE，在访问一下主页，再次之前记得得提前开启netcat，成功反弹

A screen shot of a computer

Description automatically generated

# 0x04:提权

由于是反弹shell不知道密码所以先放弃sudo -l，改为uname -a 和 cat/etc/issue查看内核和版本号，得到2个关键信息 Ubuntu 16.04 和 4.40-21-generic

A picture containing monitor

Description automatically generated

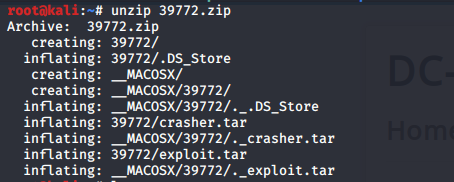
然后在必应搜索到该payload

注:该payload仅仅只是介绍，真正下载的是https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/39772.zip

A screenshot of a social media post

Description automatically generated

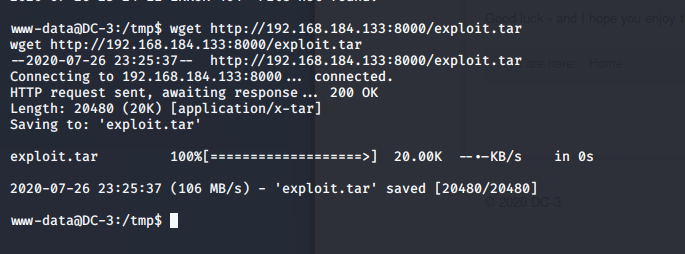
下载完以后解压一下我们的目标是exploit.tar



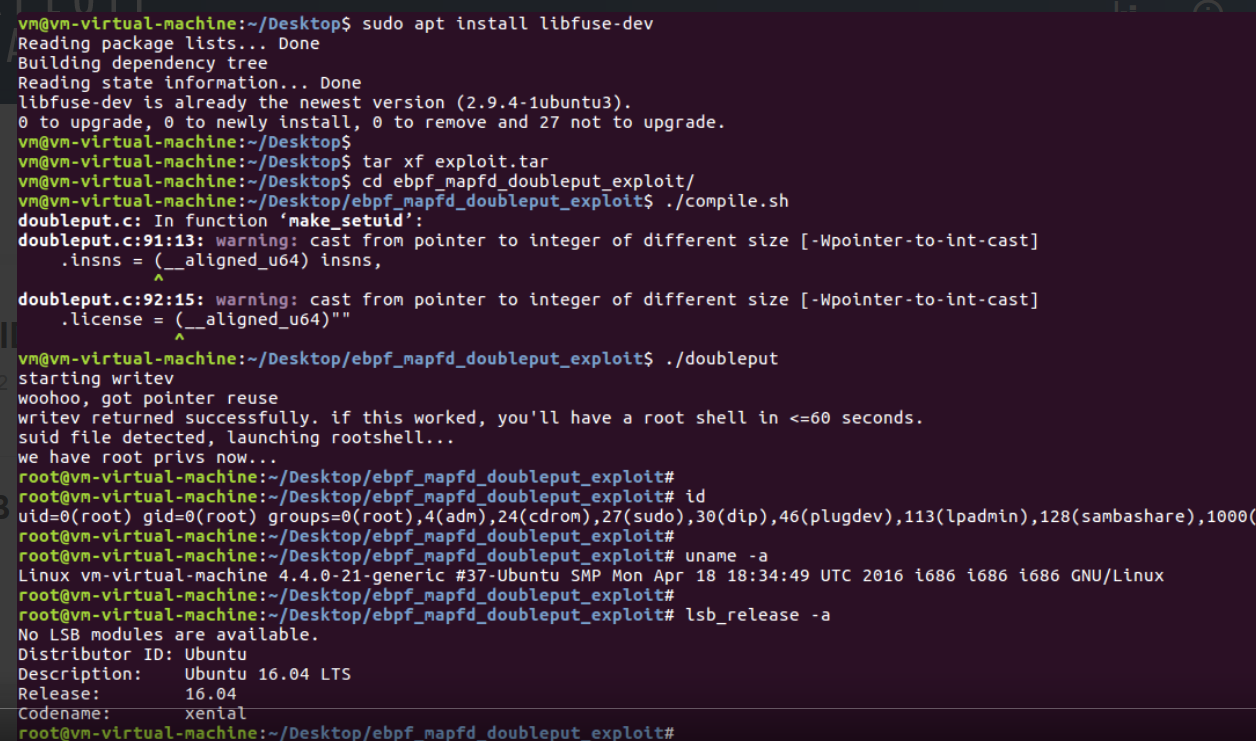
然后复制我们的目标exploit.tar到我们的根目录下方便操作，利用python开启共享模式



然后再目标服务器上用wget命令下载下来



运行方法在<https://www.exploit-db.com/exploits/39772>底下有张图有介绍如何运行



按照步骤成功得到root权限并且得到flag

