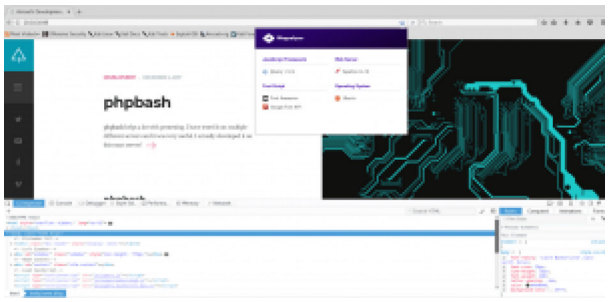
SWRhapsody

Bashed writeup

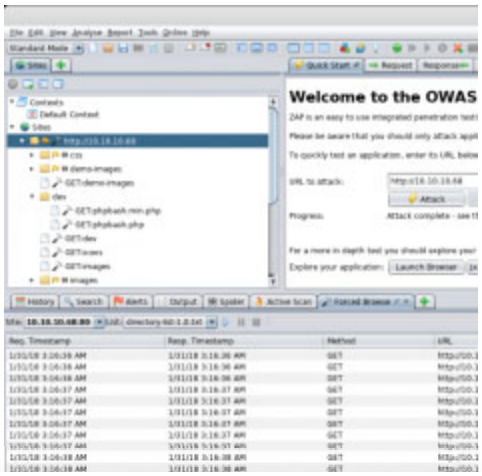
于2月 1, 2018由**SWRhapsody**发布

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。

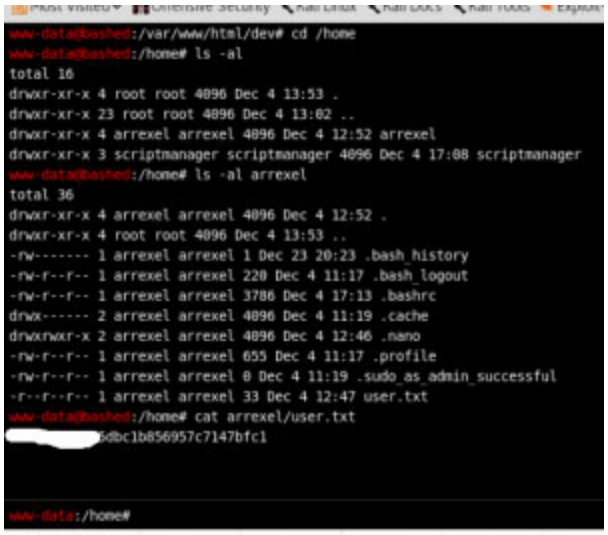


综合来看应该是利用phpbash来直接访问靶机上的文件拿到hash。一开始认为需要把这个php上传到靶机，花点时间看下这个博客发现没用可以利用输入点，不仅全站只用一篇文章左边的搜索框还是个摆设，用owasp zap扫描也没有找到什么东西，这样看来这个php原来已经在靶机上，尝试枚举成功找到php。



SWRhapsody

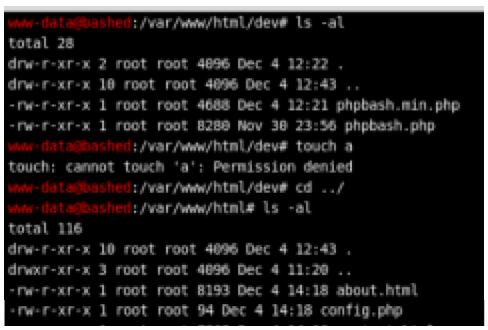
接下来就很简单，直接拿hash。



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scriptsmanager这个用户，然后这个用户可以直接去root下拿到hash。

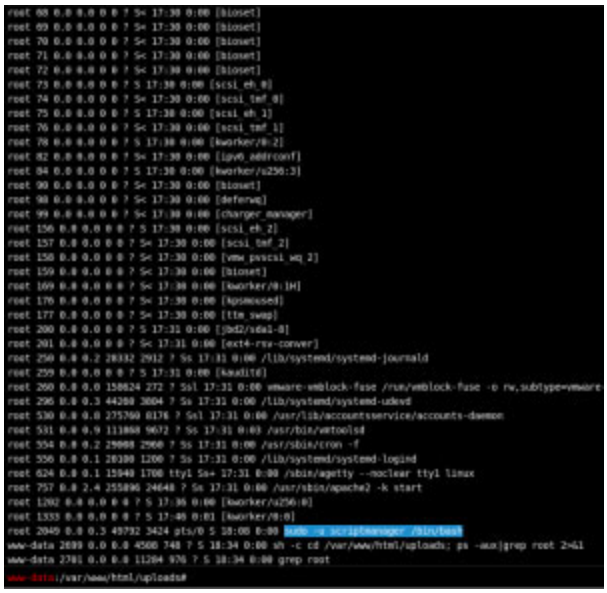
下面是具体操作步骤，一开始运行 phpbash.php 是在dev文件夹下，到上级目录可以发现有个uploads目录是 777 的权限。



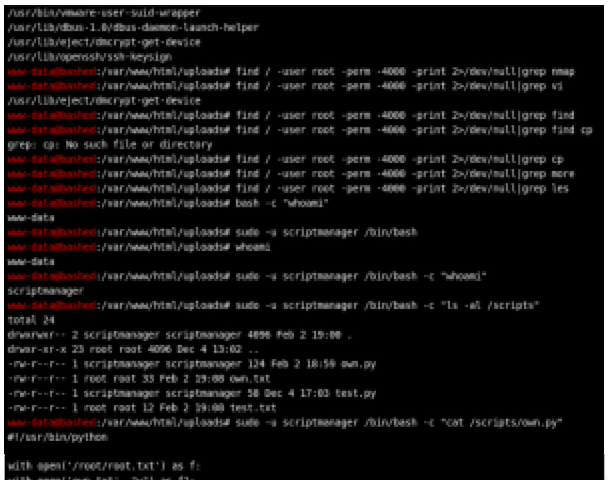
SWRhapsody

```
drw-r-xr-x 2 root root 4096 Dec 4 14:18 js
drw-r-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。



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用想到该如何利用，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scriptsmanager后就先到这里看了下，结果这里已经有人留下了用scriptsmanager读到的hash。



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

分类目录

相关文章

HACKTHEBOX

SWRhapsody

ABOUT

Hestia |由ThemeIsle开发