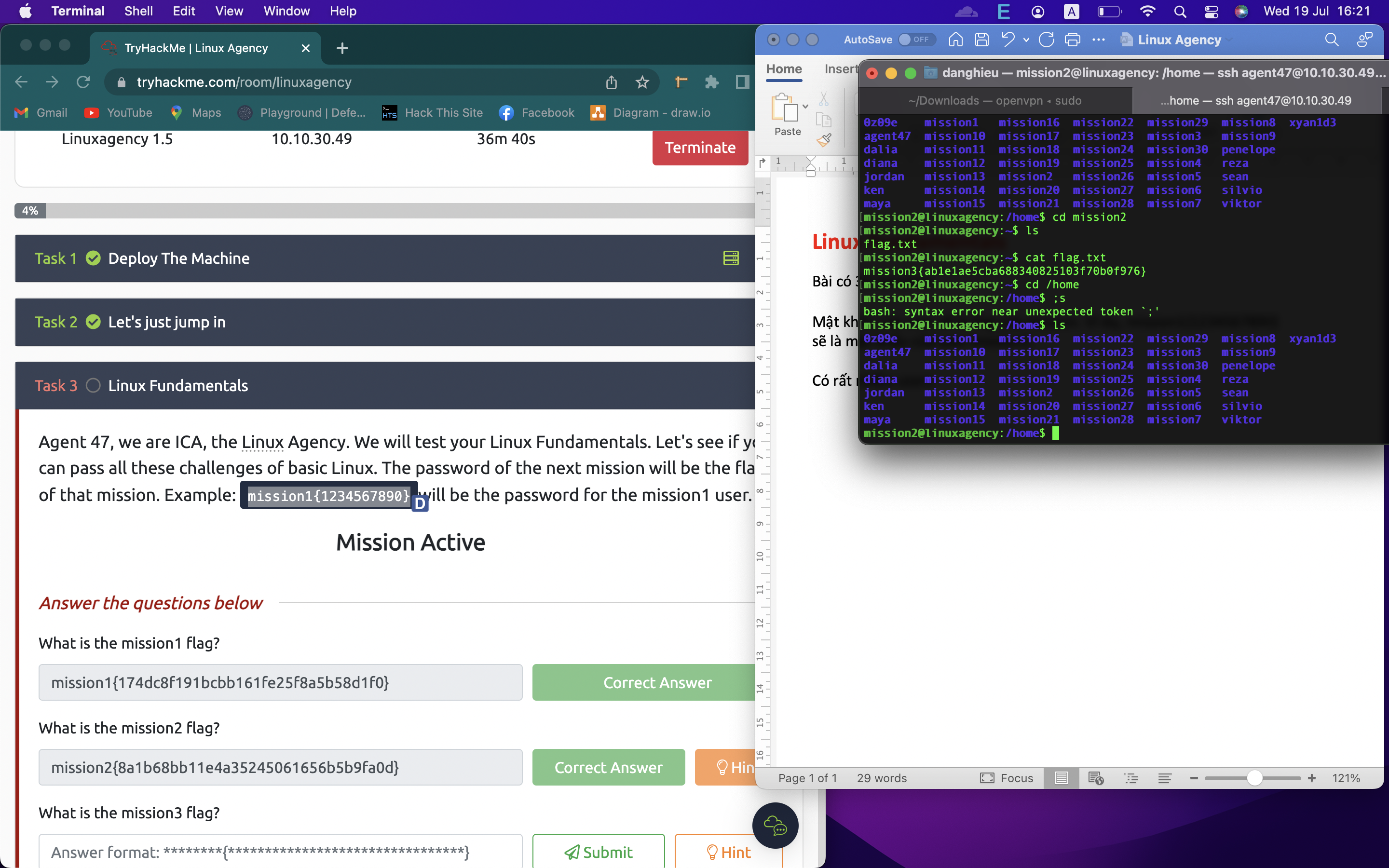
**Linux Fundamentals**

Bài có 30 missions.

Mật khẩu của user sẽ là flag của mission. Ví dụ, mission1{1234567890}

sẽ là mật khẩu của user mission1.

Có rất nhiều users.



Muốn vào thư mục của mission2 phải đăng nhập user mission2.

su mission2

pass: mission2{8a1b68bb11e4a35245061656b5b9fa0d}

Muốn lấy được flag của mission 4 bạn phải là user mission3.

**Mission 4:**

Mình vào thư mục của mission3 thấy file flag.txt

cat flag.txt thì nó báo lỗi: I am really sorry man the flag is stolen by some thief's.

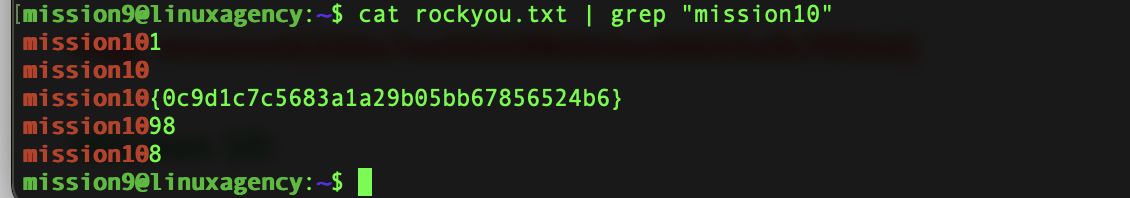
Không hiểu sao vim thì được

**Flag: mission4{264a7eeb920f80b3ee9665fafb7ff92d}**

**Mission 10:**

Khi mình liệt kê thư mục của mission9 thì thấy file rockyou.txt

Mở file thì thấy rất nhiều chữ, không biết flag nằm ở đâu nên mình dùng grep.



**Mission 17:**

Liệt kê thư mục mission16 thì thấy file flag. Chúng ta kiểm tra loại file:



ELF 64 bit là file thực thi của linux. Mình phải cấp quyền thực thi cho nó.

chmod+x flag

./flag

**Mission 23:**

Mở đầu là 1 trình biên dịch python. Khi chúng ta exit() thì nó lại quay lại user mission21.

Cách làm: spawning tty shell giúp shell có nhiều tính năng hơn

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

**Mission 24:**

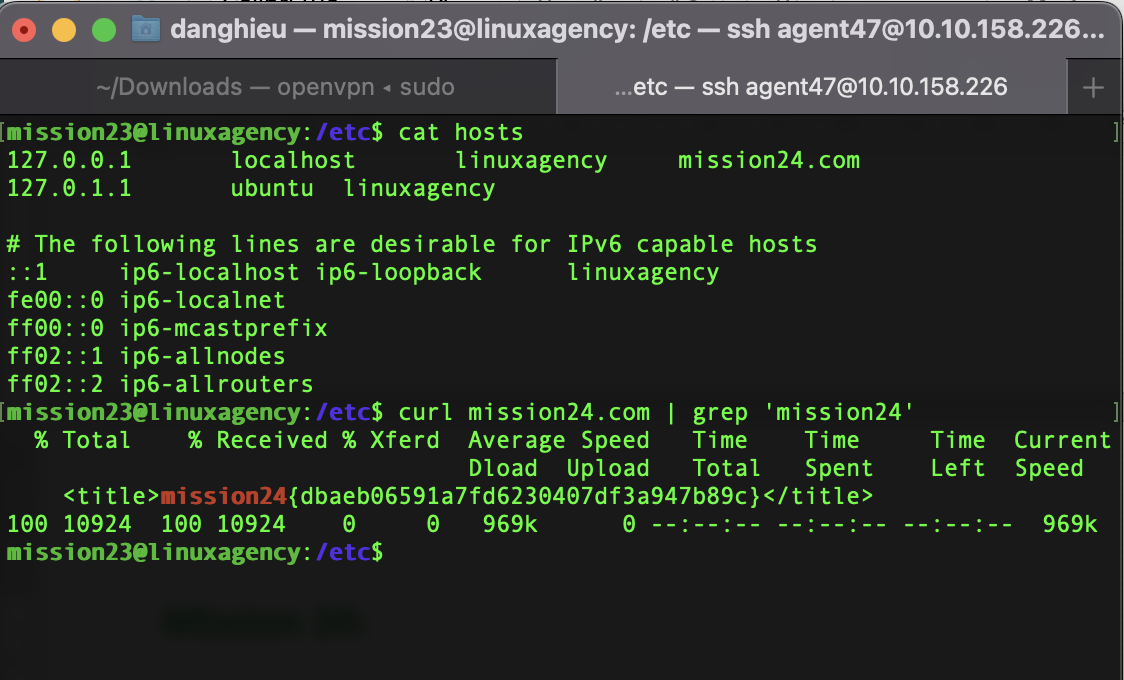
Mình liệt kê các thư mục thì thấy tệp message.txt có nội dung như sau:

The hosts will help you.

[OPTIONAL] Maybe you will need curly hairs.

Mình vẫn chưa hiểu làm sao để lấy được flag. Các mission đã ngày càng khó hơn.

Khi ta kiểm tra file /etc/hosts sẽ thấy tên miền mission24.com



**Mission 25:**

Nó cho 1 file .viminfo và bribe.

Thực thi file bribe:

There is a guy who is smuggling flags

Bribe this guy to get the flag

Put some money in his pocket to get the flag

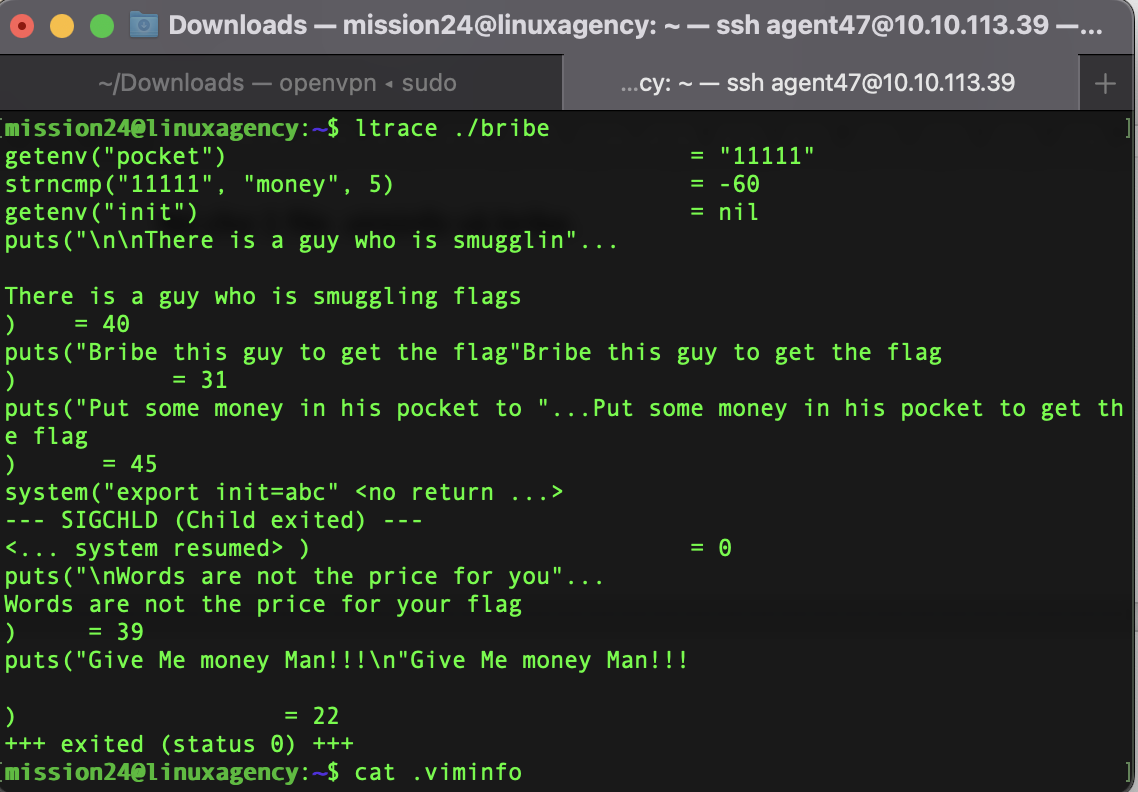
Words are not the price for your flag

Give Me money Man!!!

Bài này rất hay nhưng khó giải thích, chỉ có làm thử mới hiểu.

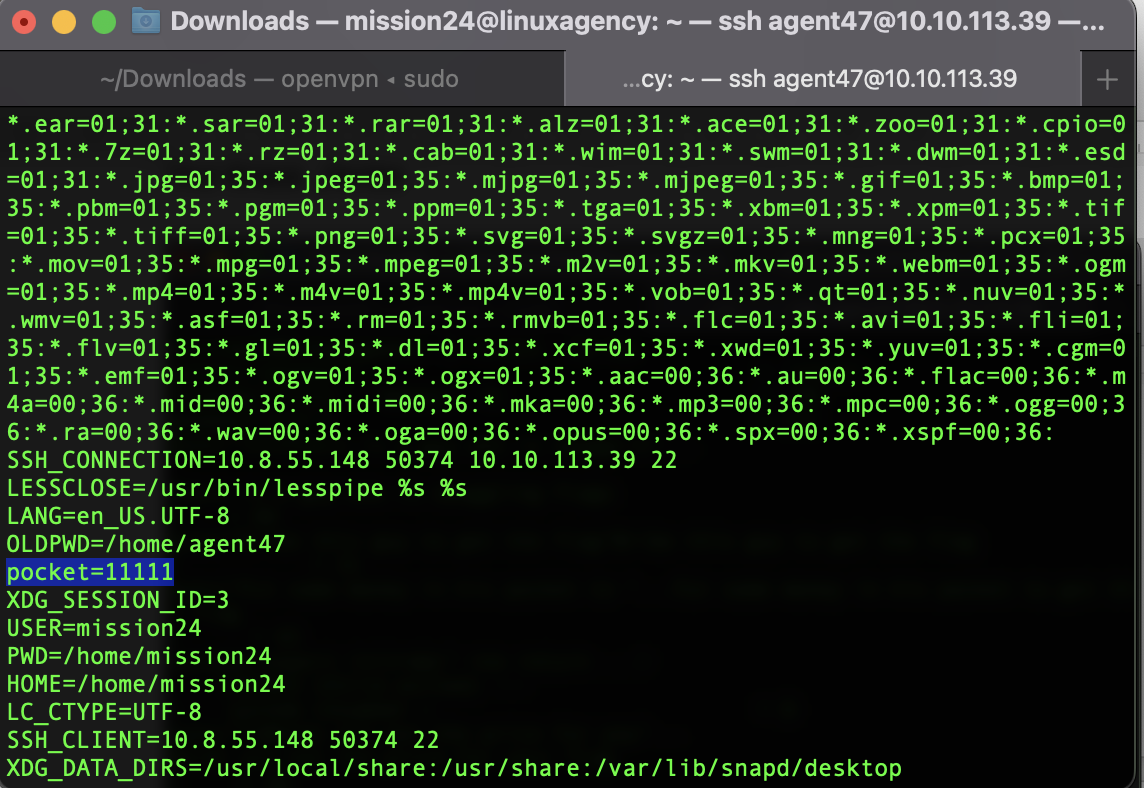
ltrace command là theo dõi quá trình thực thi diễn ra như thế nào.

Thử ltrace ./bribe

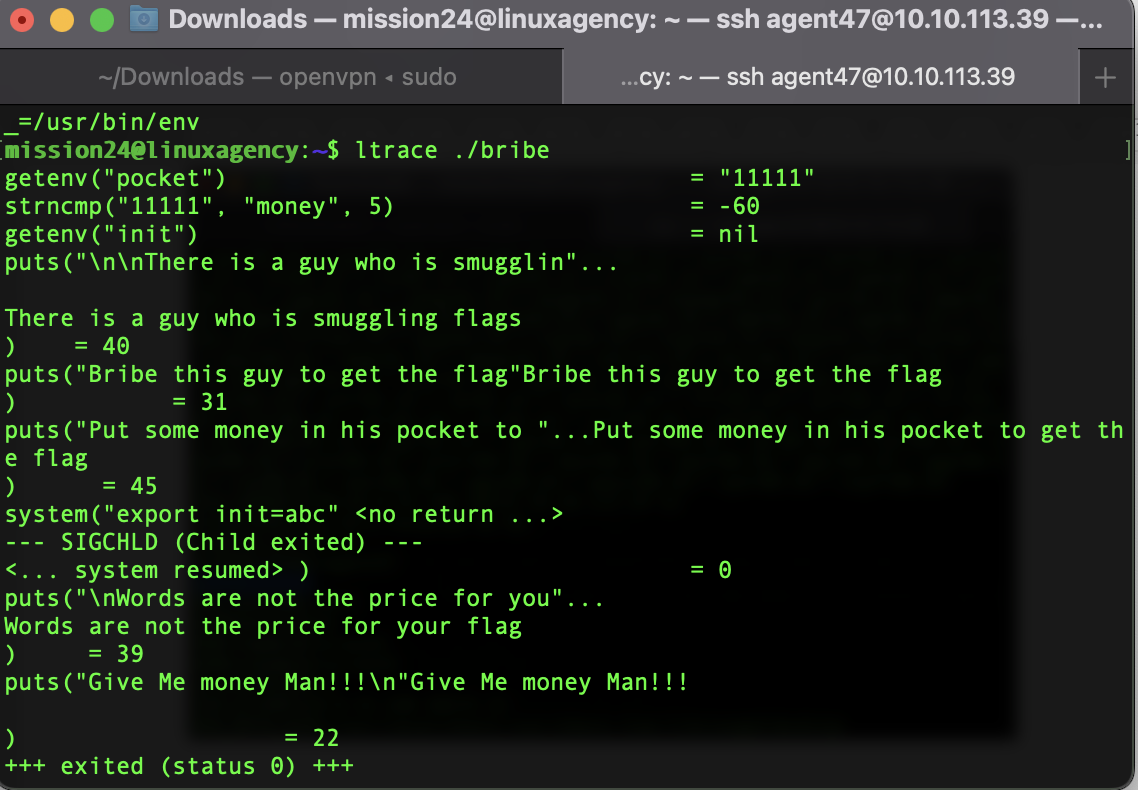


Bạn thấy nó getenv(“pocket”).

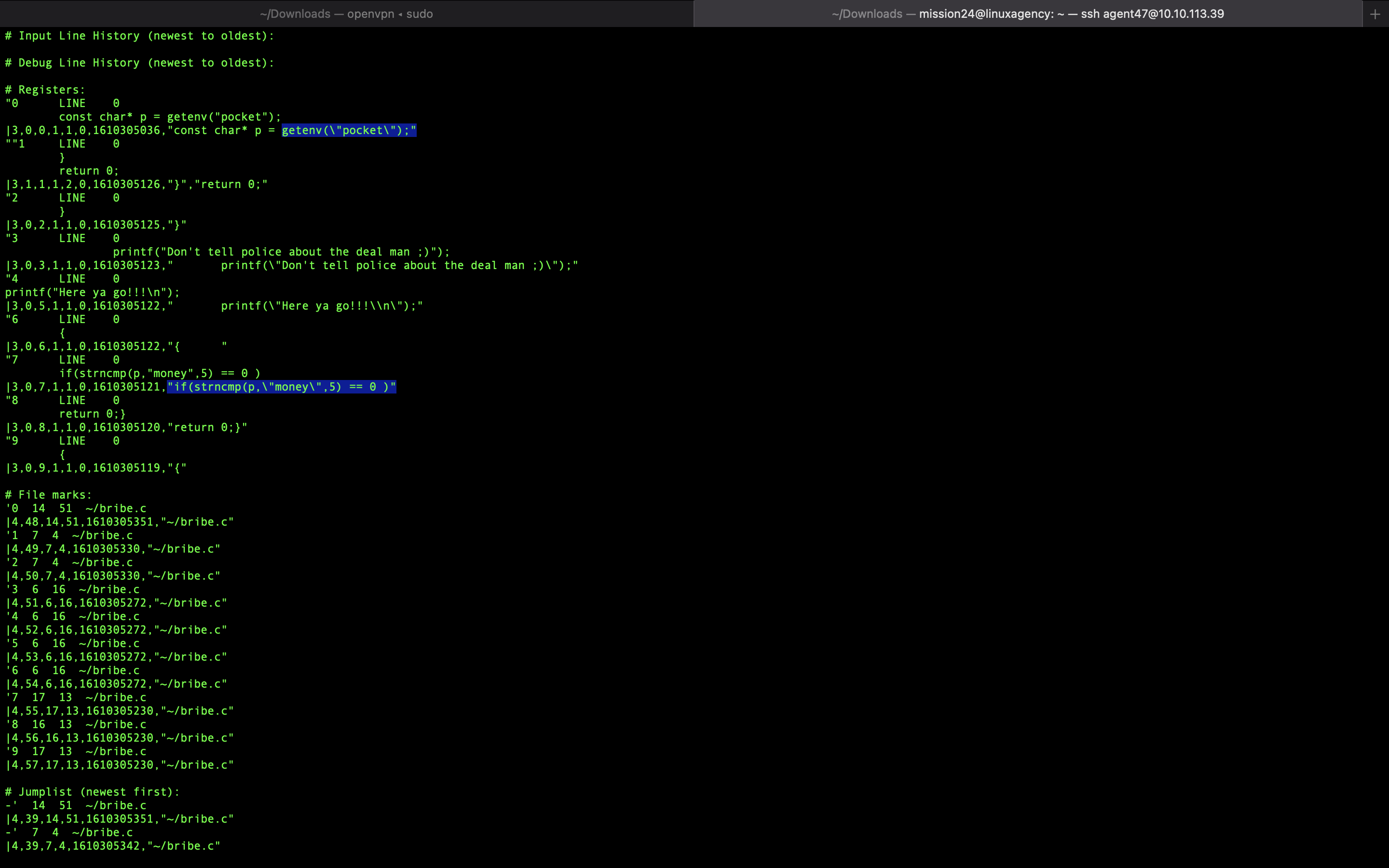
Mình thử export pocket=11111. Check biến môi trường:



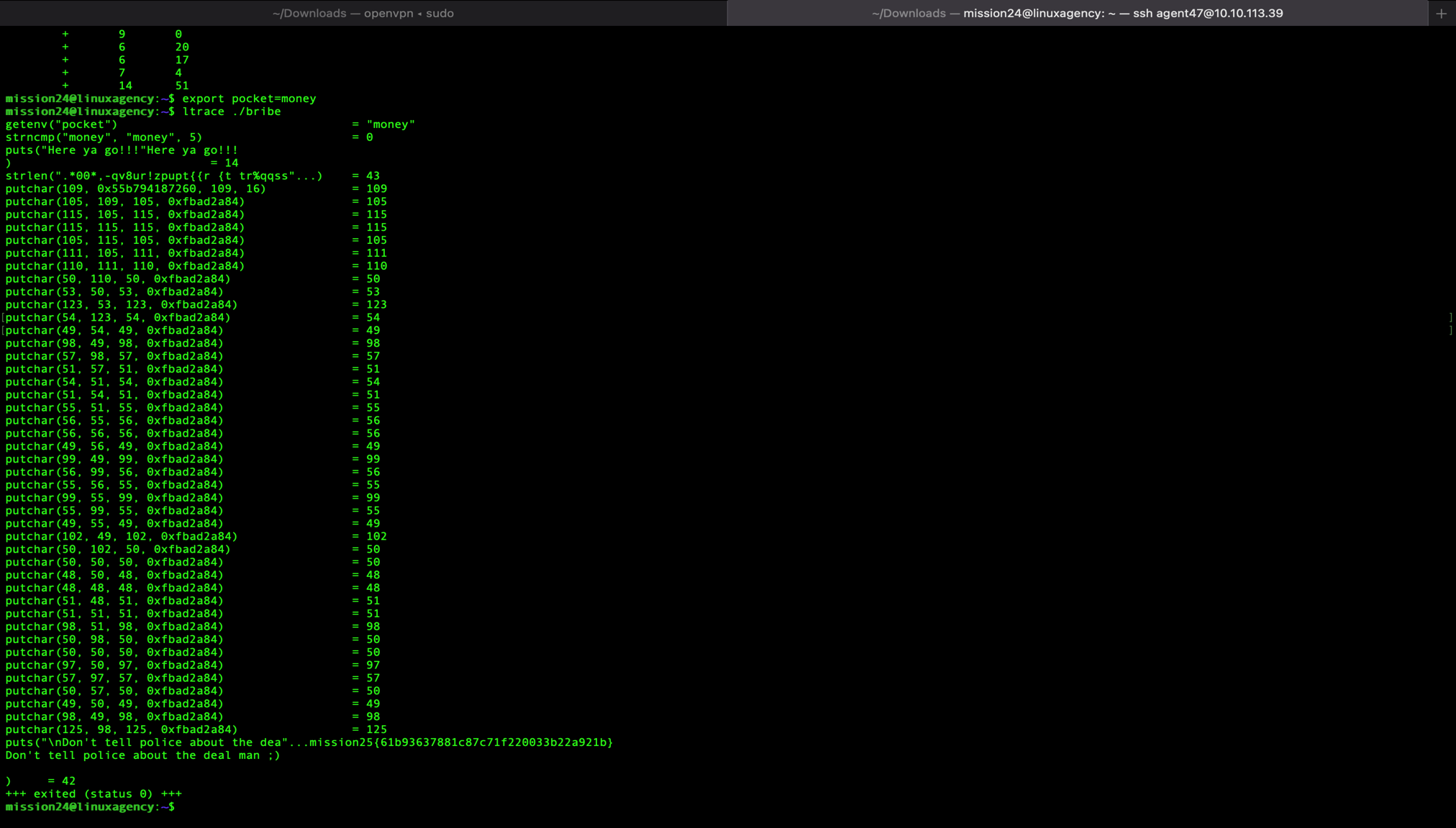
Theo dõi lại quá trình thực thi ./bribe



Mình thấy hàm strncmp() giống trong file .viminfo. Chắc nó đang thực thi file ấy.



Thử cho p là money: export pocket=money



**Mission 26:**

Thật sự đến mission này mình không biết làm gì cả nên phải đọc hướng dẫn.

Khi liệt kê thư mục nó báo lỗi: ls: No such file or directory

Lúc đầu mình cứ tưởng không có file nào trong thư mục của mission25 nhưng đọc lại lỗi mới thấy không có file hay thư mục ls nào như thế.

Ủa ls là câu lệnh mà. Vậy để làm được bài này phải thực thi được những lệnh cơ bản đã.

Mình đọc trên mạng thì thấy phải set lại $path.

echo $path thì thấy rỗng 🡪 Hèn chi không thực thi được lệnh ☺

export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

Thực hiện lệnh ls lại thì thấy flag.txt 🡪Done