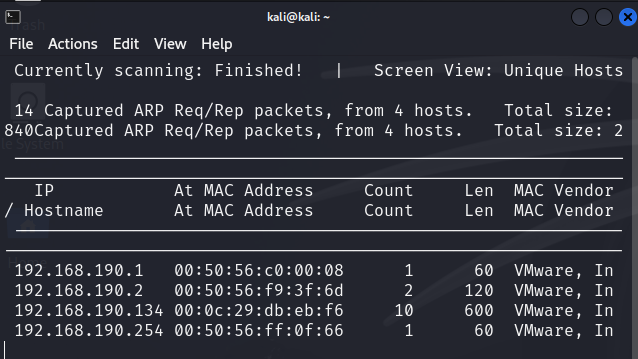
## Quét địa chỉ IP

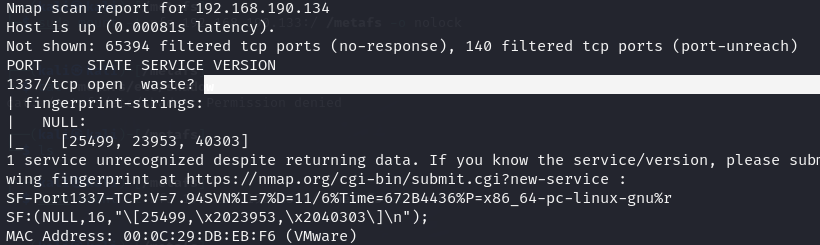
netdiscover –r 192.168.190.134



=> Địa chỉ máy victim là 192.168.190.134

Quét cổng hoạt động

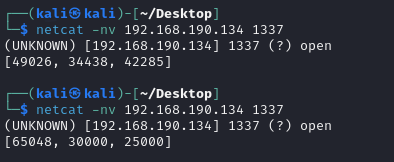
nmap -v -sV -A -O -T4 -p- 192.168.190.134



=> Chỉ thấy cổng 1337 hđ

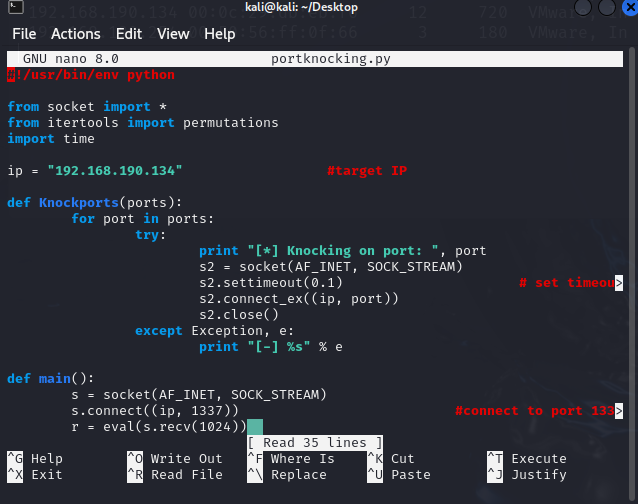
## Sử dụng portknocking

Portknocking là 1 cách thức bảo vệ các dịch vụ của 1 máy chủ. Nó sẽ che dấu khỏi quét nhg để mở ra sẽ cần phải mở kết nối tới 3 port theo 1 thứ tự chính xác đã dc admin cài đặt trong 1 khoảng thời gian chính xác thì port mới mở. -> Phải dùng script để tự động thao tác thử tất cả những cái có thể.

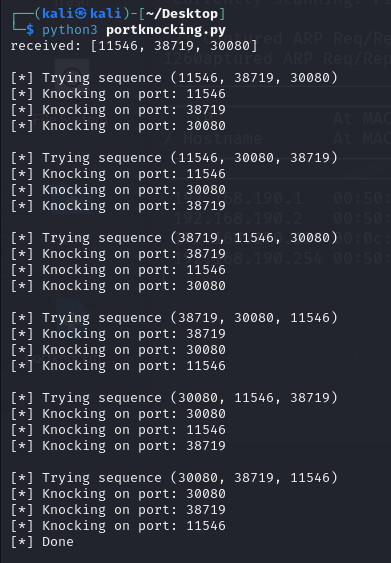


Dùng netcat để thử thì mỗi lần sẽ 1 thứ tự khác -> rất khó. Ở đây cổng k mở

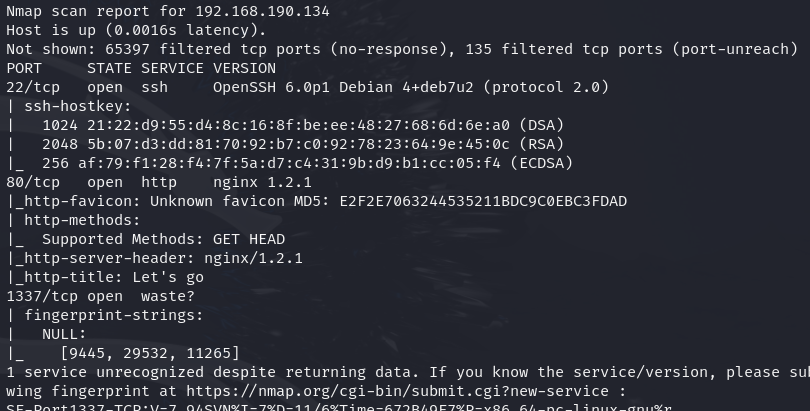
Thực hiện dùng script



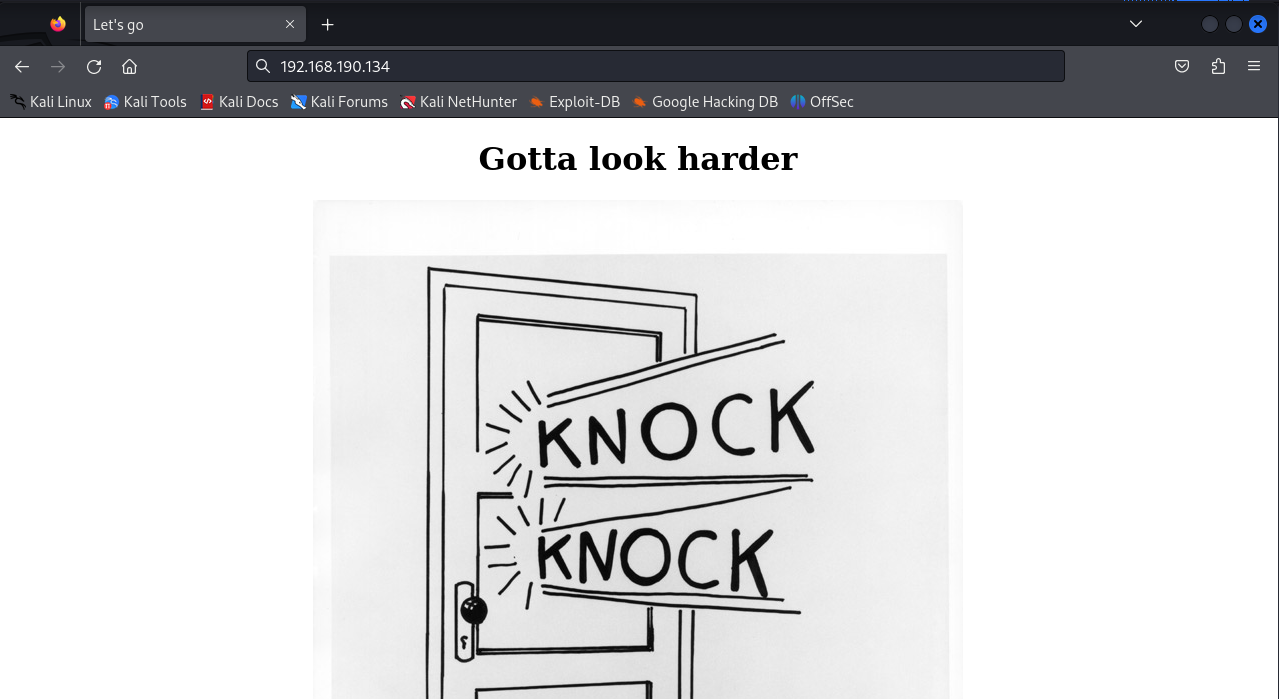
* Nhớ đổi ip target.
* Đổi cú pháp thành python3 nhé, đây đang dùng python2
* Chạy script và gõ cửa thành công



* Quét lại với namp thấy cổng đã mở

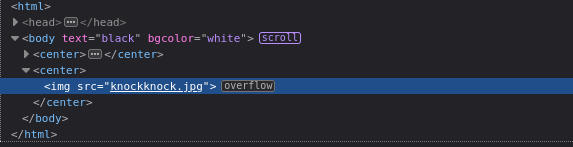


* Truy cập tới web vì cổng 80 mở

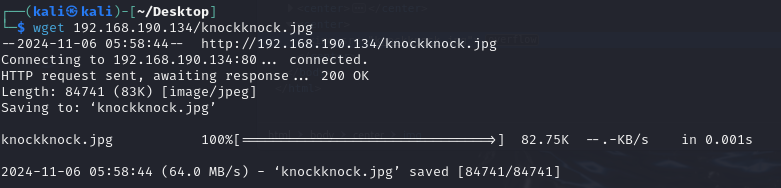


=> Mấy thằng làm ác vcl :)))

Xem mã nguôn của trang



Thử tải ái ảnh về nghịch



Biến ảnh thành strings để xem có thông tin gì ẩn giấu k

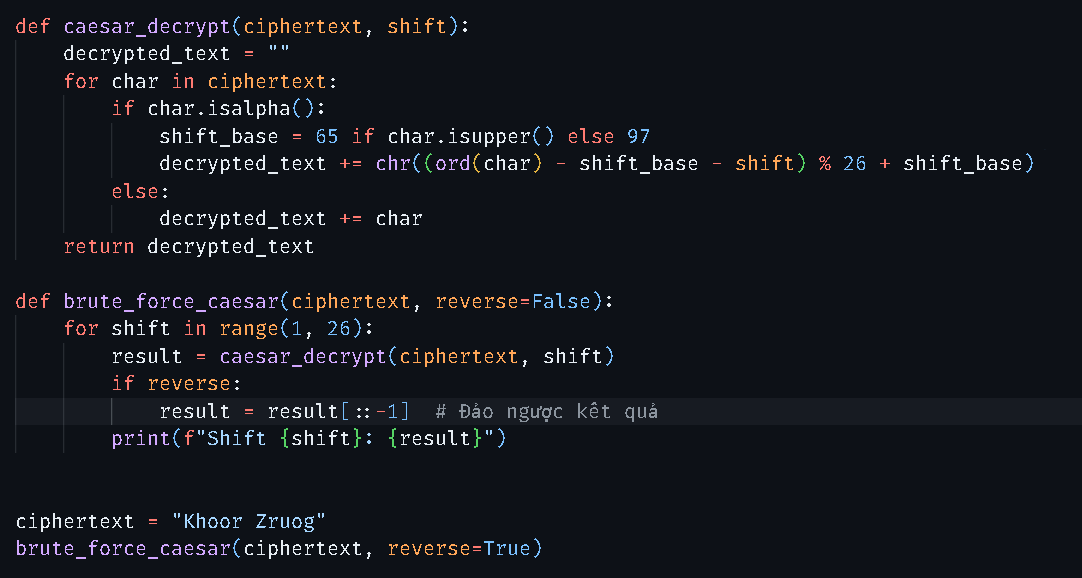


* KQ là đc thông tin đăng nhập được dấu ở ảnh :)))

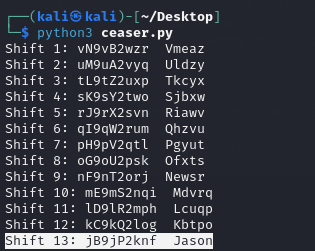


Trông vô nghĩa nên chắc bị mã hóa, thử với mã hóa đơn giản nhất là Ceaser dịch vòng

Viết 1 script python dịch mã



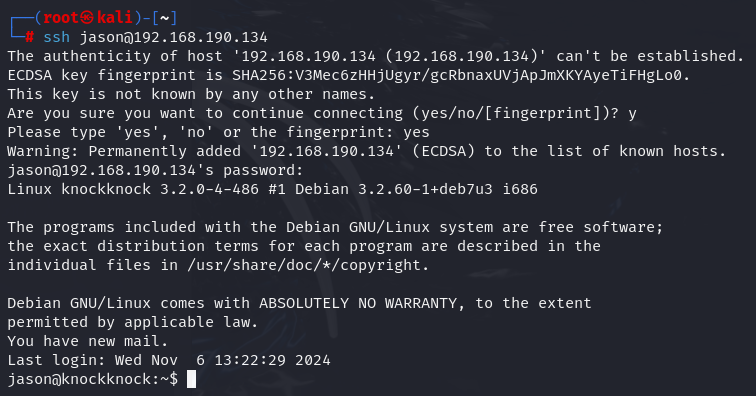
Kq



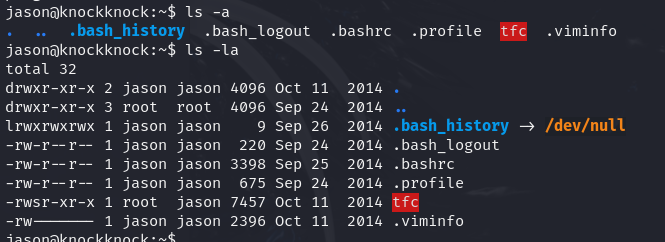
Username là jason pass là cái đống kia

## Truy cập SSH

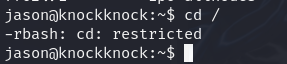
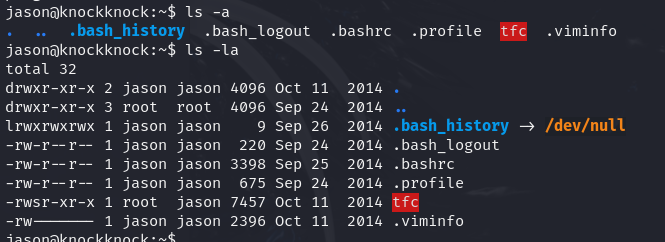
Dùng mk và tên vừa nãy



Thông tin tên đăng nhập



Xem các file và các quyền



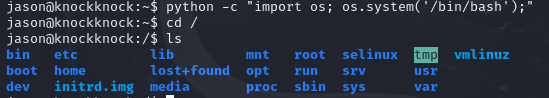
Bị dính shell giới hạn nên cần tim cách leo thang đặc quyền

## Shell Unlock

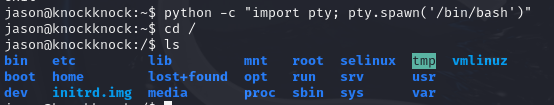
Có rất nh cách để shell unlock trong đó sử dụng Vim hoặc python

* Nhập câu lệnh python: python -c "import pty; pty.spawn('/bin/bash')" hoặc python -c "import os; os.system('/bin/bash');". Do 2 thư viện và hàm này excute bất cứ câu lệnh nào

\*\*\*Với os

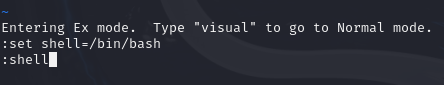


\*\*\* với pty

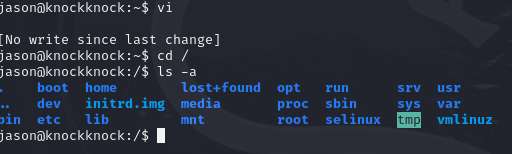


Câu lệnh này tạo 1 pseudo terminal, 1 terminal ảo, chạy shell bash

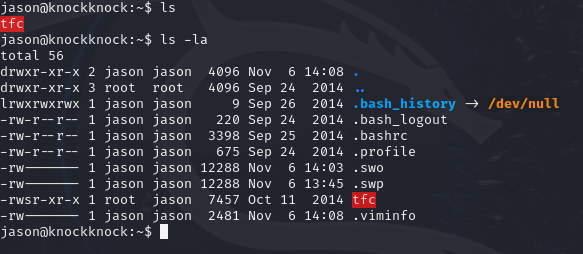
* Bật vim và trước khi thoát(dùng shift Q) thực hiện câu lệnh nhập



Kết quả



* Kiểm tra và khám phá ra 1 tệp có thể tấn công



\*\*\* ở đây có thể thấy là tệp này có quyền S: Setuid => mượng được quyền root => là có thể leo thang đặc quyền

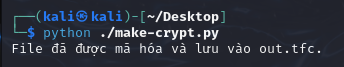
........check cái tfc đọc hiểu là dc.

B?: TÌm eip

* Tạo 1 pattern 6000 bytes với msf (nhớ đúng tên file là in.tfc)



* Tạo file mã hóa từ in.tfc (để sau chạy ./tfc mã hóa ngc 1 lần nữa là ra bản gốc)có code

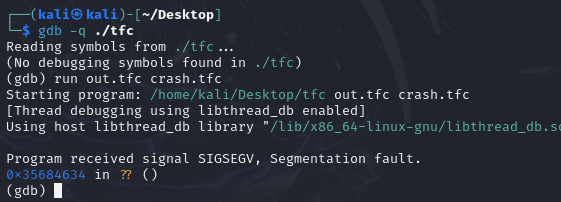


Dùng gdb để xem segnmaint fault và đấy offset

Dùng 2 cái này để có thể ghi core dump

ulimit -s unlimited

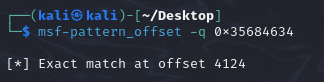
ulimit -c unlimited



Ktra thấy là nó đây



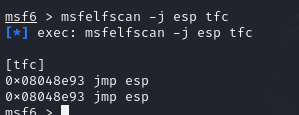
Kq offset khiến nó tràn là đây :VVVVV dcm 4h của bố



=> từ offset thứ 4124 sẽ là lúc con trỏ EIP bị tràn

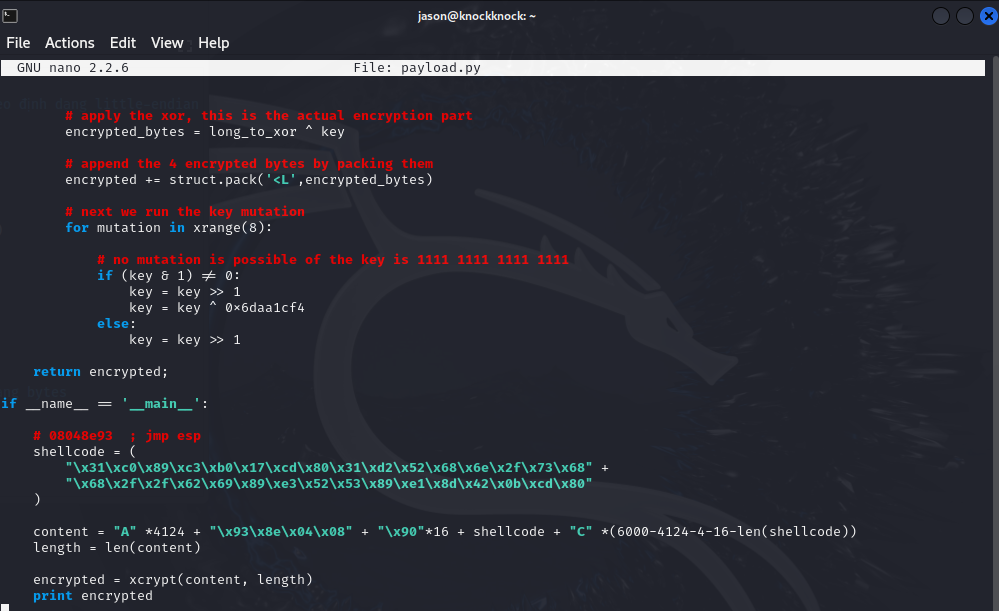
=> tiêm vào vị trí đấy câu lệnh chỉ tới shell có payload là ok

=> tìm địa chỉ của câu lệnh jmp esp nữa là ok (vào msfcosole: msfelfscan -j esp tfc) )



B?: Giờ viết code để tạo ra 1 file có chứa shell code để tiêm vào bộ đệm tràn(có file code)

-> rồi ném lên máy nạn nhân cho nó mã hóa ./tfc là xong



BÙM xong cmnr :)))))))))



Lấy đc flag va quyền -> xong dcm 4 ngày cuộc đời bố.