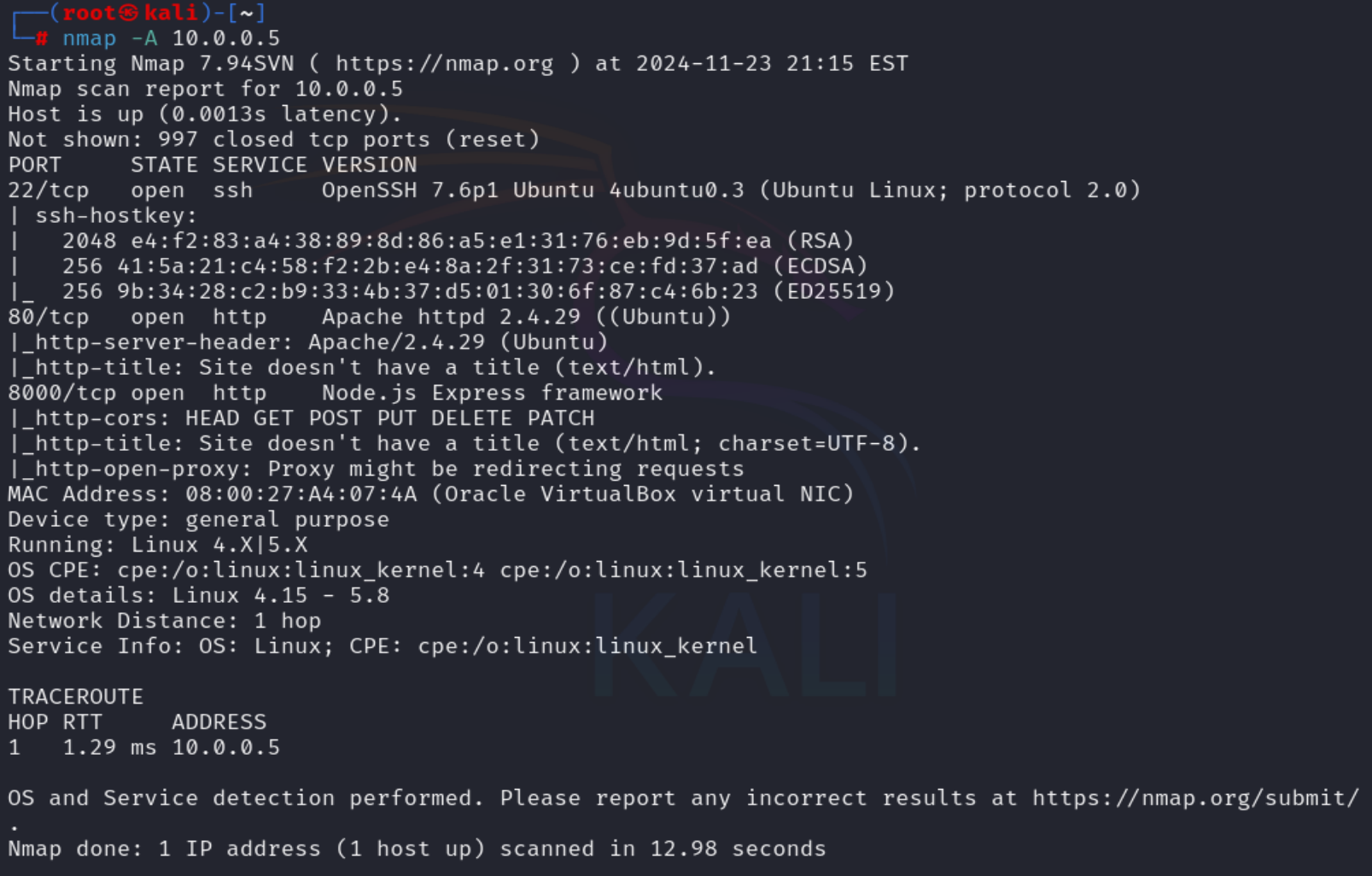
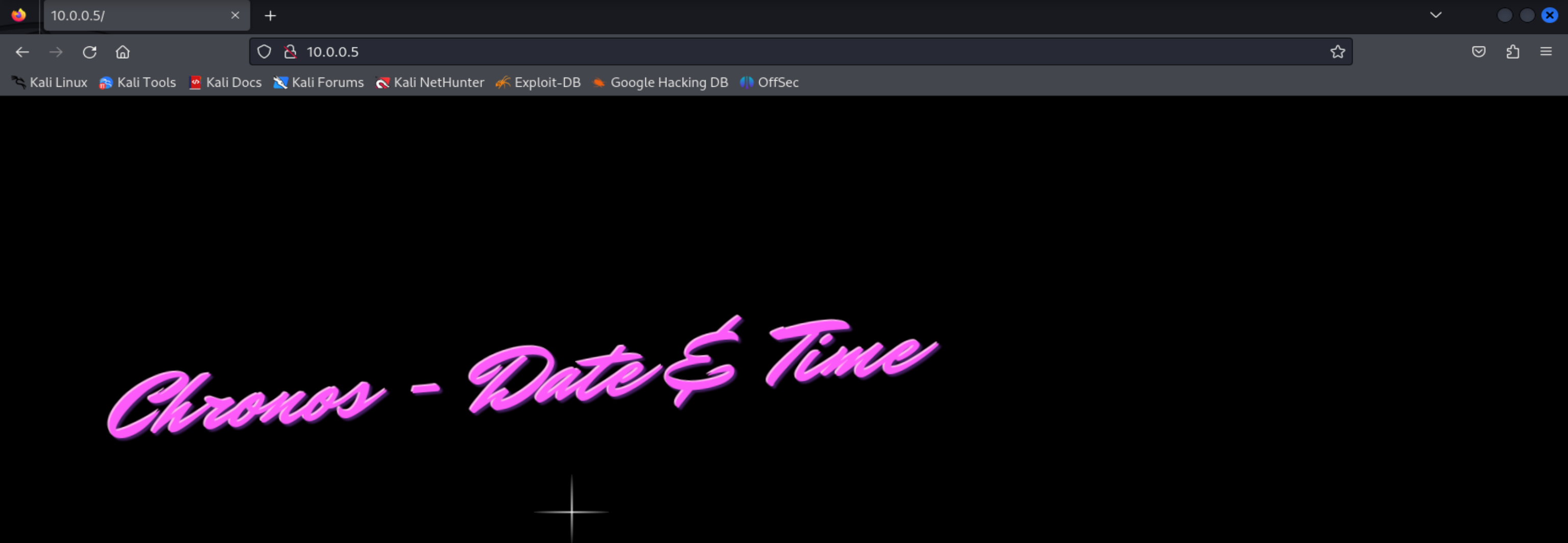
CHUẨN BỊ



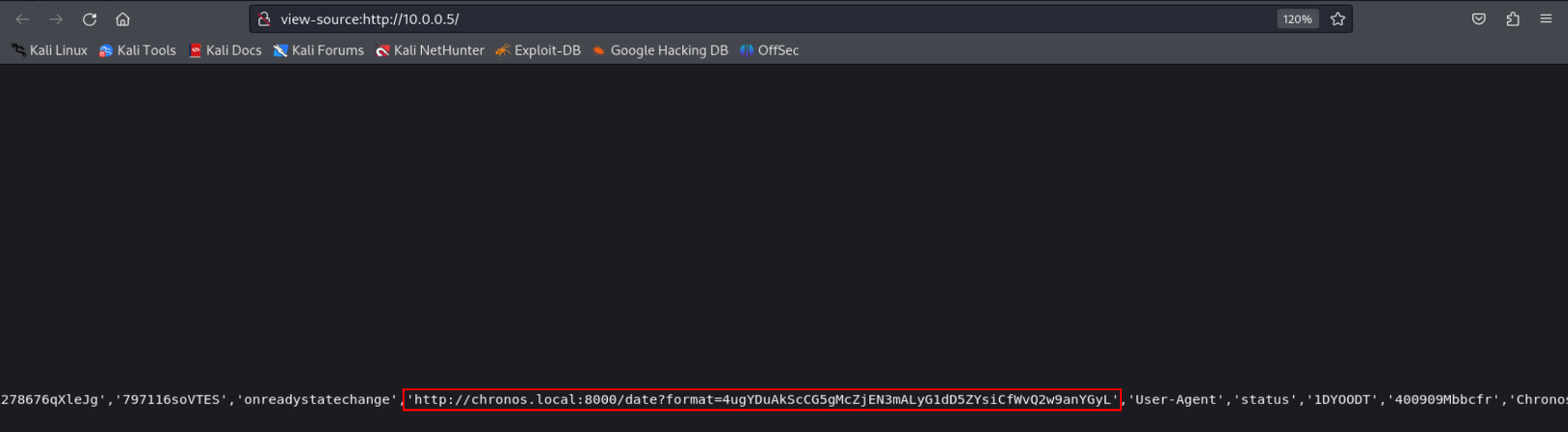
Thấy có cổng 80 mở

TẤN CÔNG

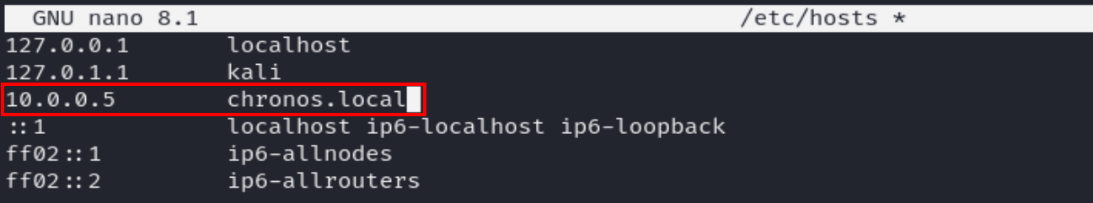
Truy cập qua cổng 80



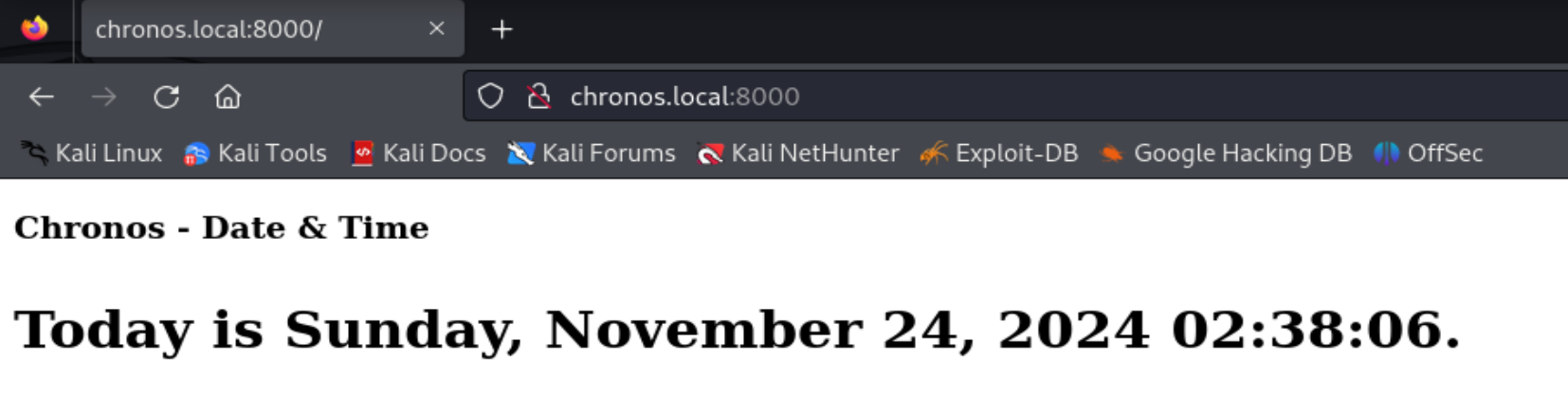
Xem source code thì thấy đc hostname và URL



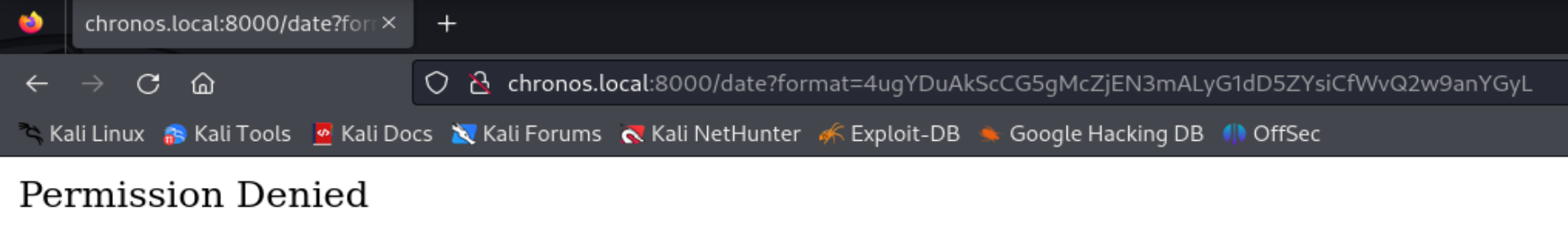
Ta sửa etc/host để thêm cái host mới đó vào



Truy cập vào chronos.local cổng 8000

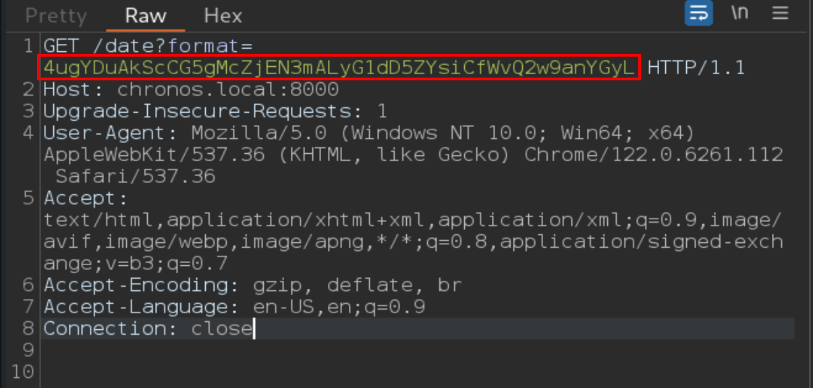


K có gì ngoài hiển thị thời gian



Ta thử vào = URL bắt được ở trên => bị từ chối

Dùng burp suite



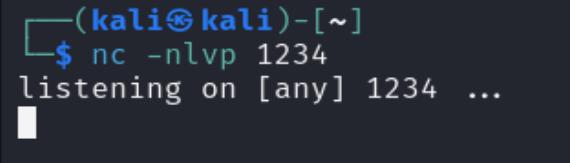
Đây là mã base64 nếu decode thàn base58 trên cyber Chef thì dc kq

4ugYDuAkScCG5gMcZjEN3mALyG1dD5ZYsiCfWvQ2w9anYGyL

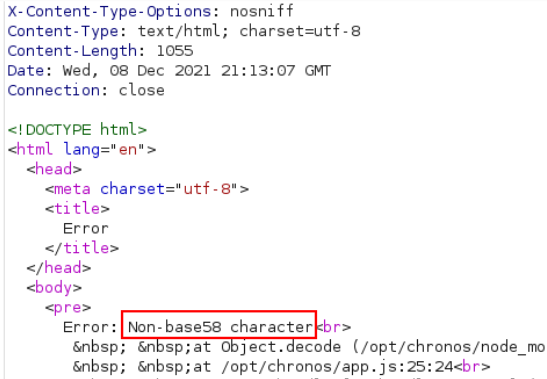
* '+Today is %A, %B %d, %Y %H:%M:%S.'

KHAI THÁC

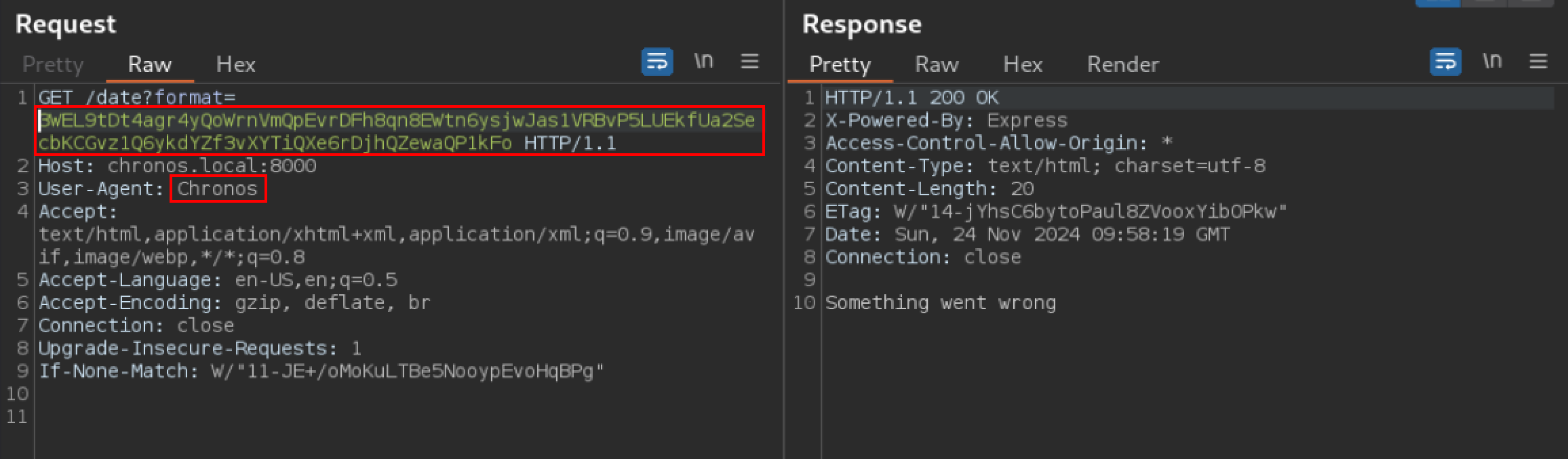
Tạo cổng lắng nghe



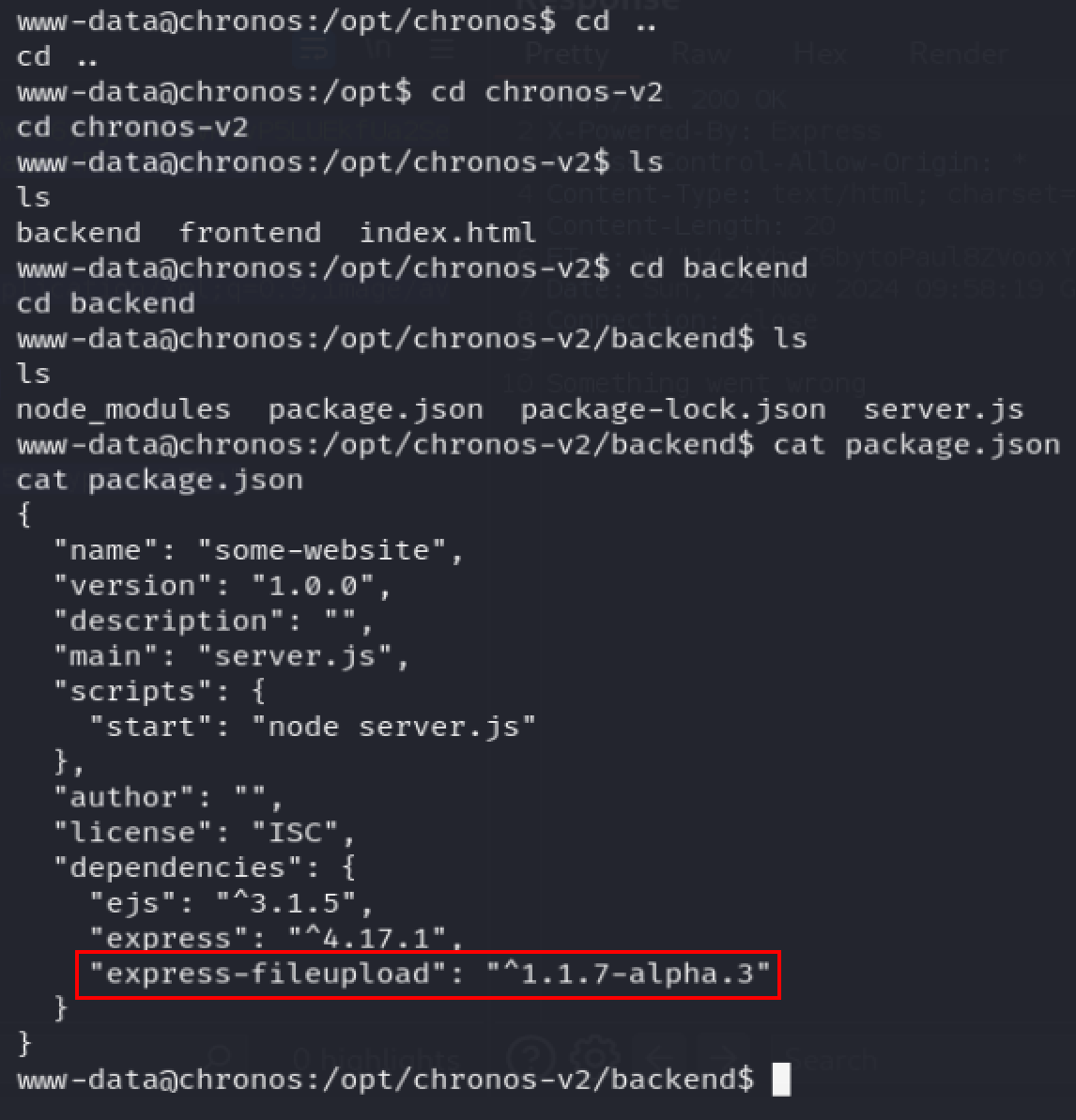
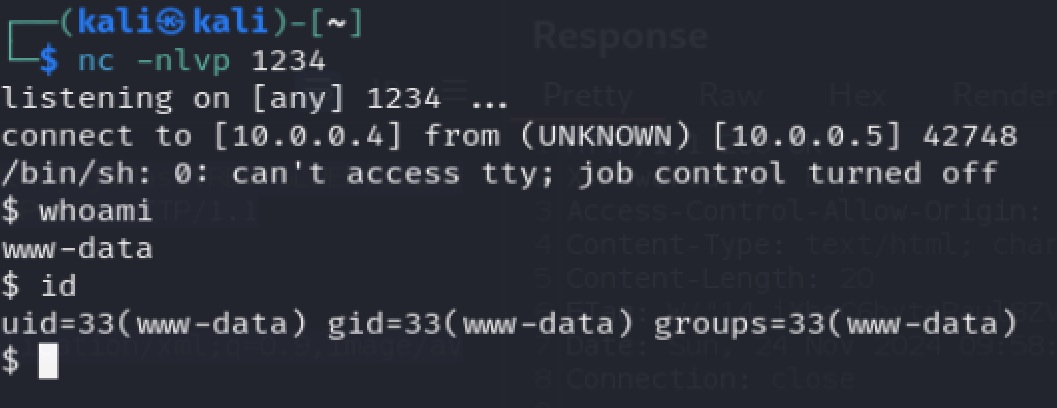
[Reverse Shell Cheat Sheet | pentestmonkey](https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet)  
Vào link này lấy 1 reverseshell rồi encode base58 để tranngg web hiểu, vì nếu đưa vào là base64 sẽ có tbao lỗi chỉ nhận base58



Khi truyền vào thì thành công



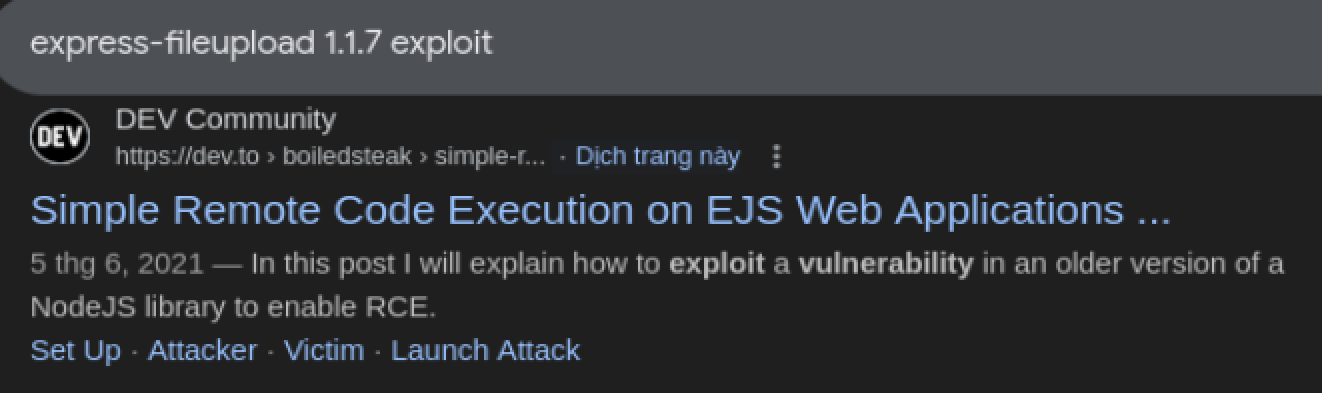
Vào thành công



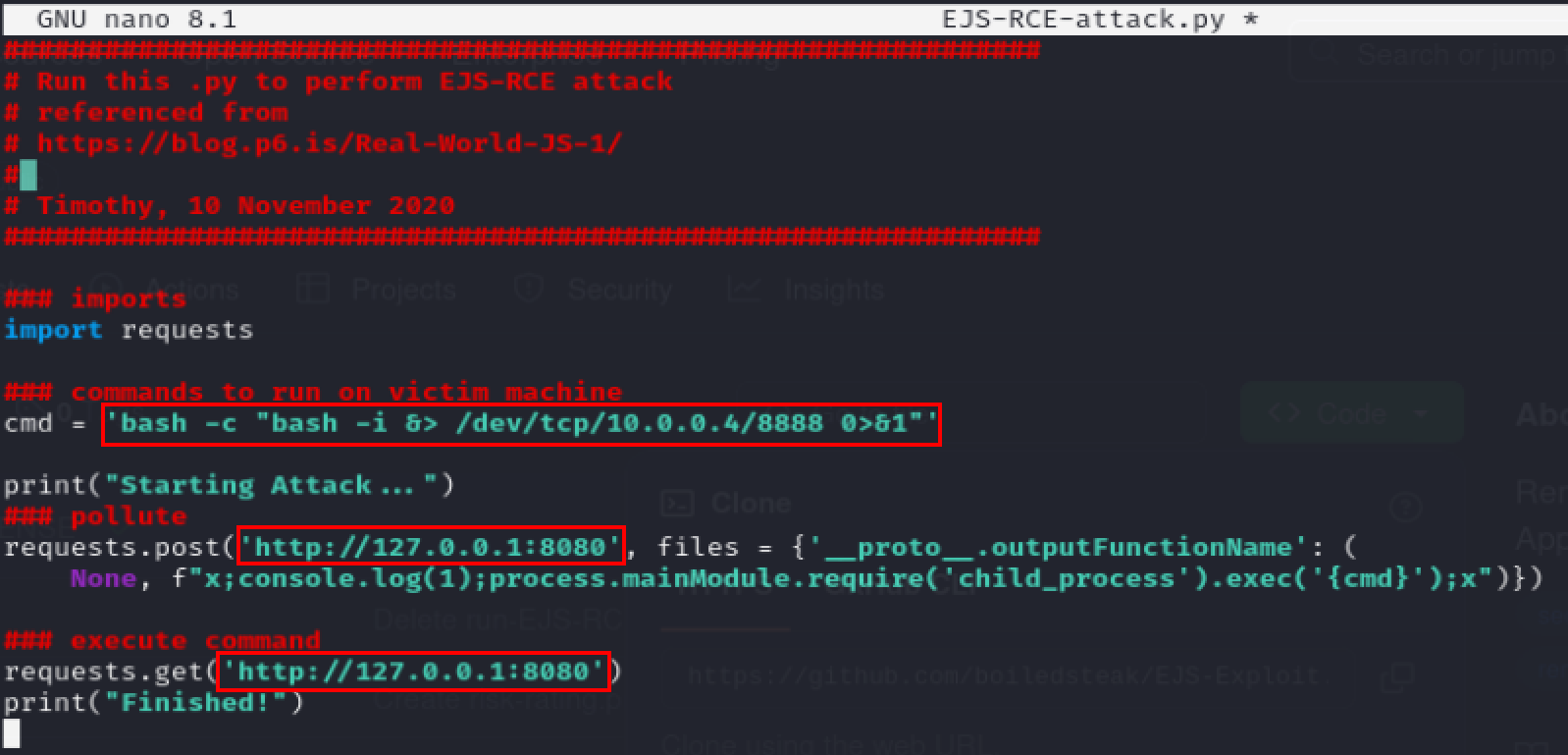
Ta xem fil package.json thì thấy có dịch vụ “**express-fileupload version 1.1.7**”

Leo thang đặc quyền

Tra gg để tìm exploit



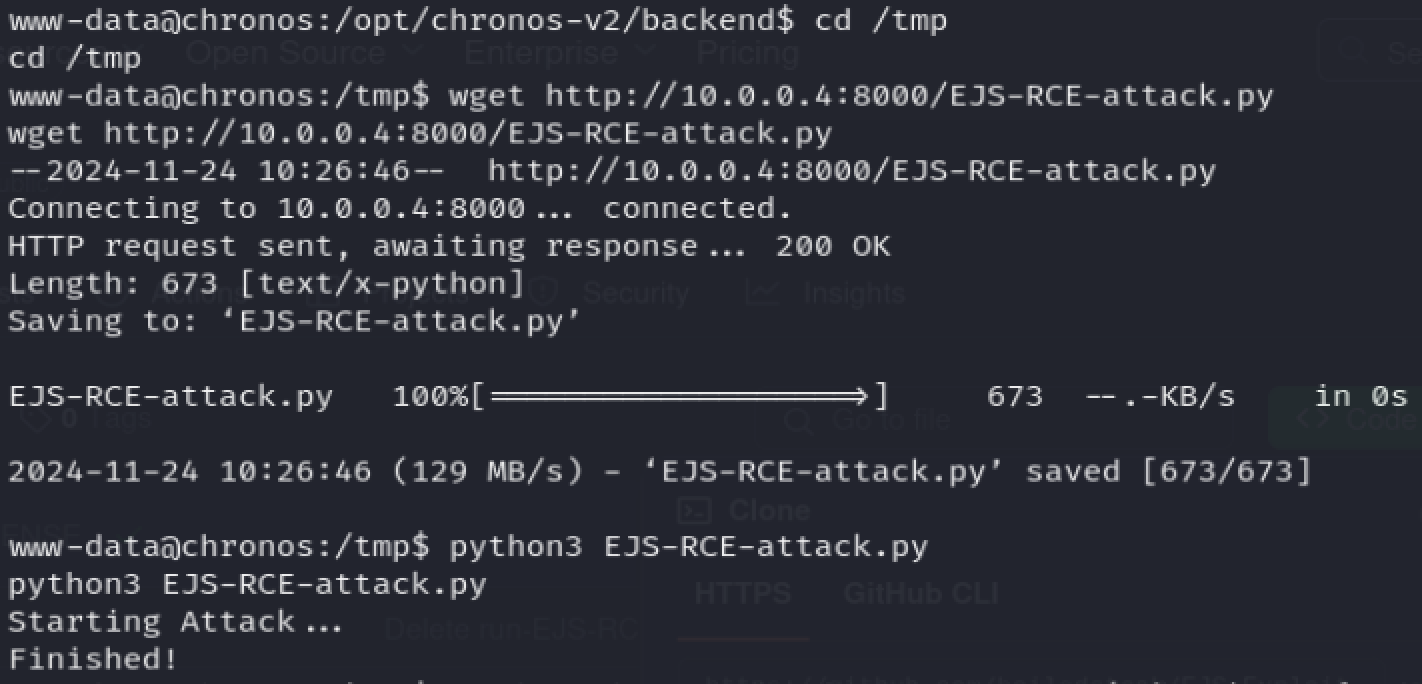
Sửa lại exploit theo địa chỉ ip của mình



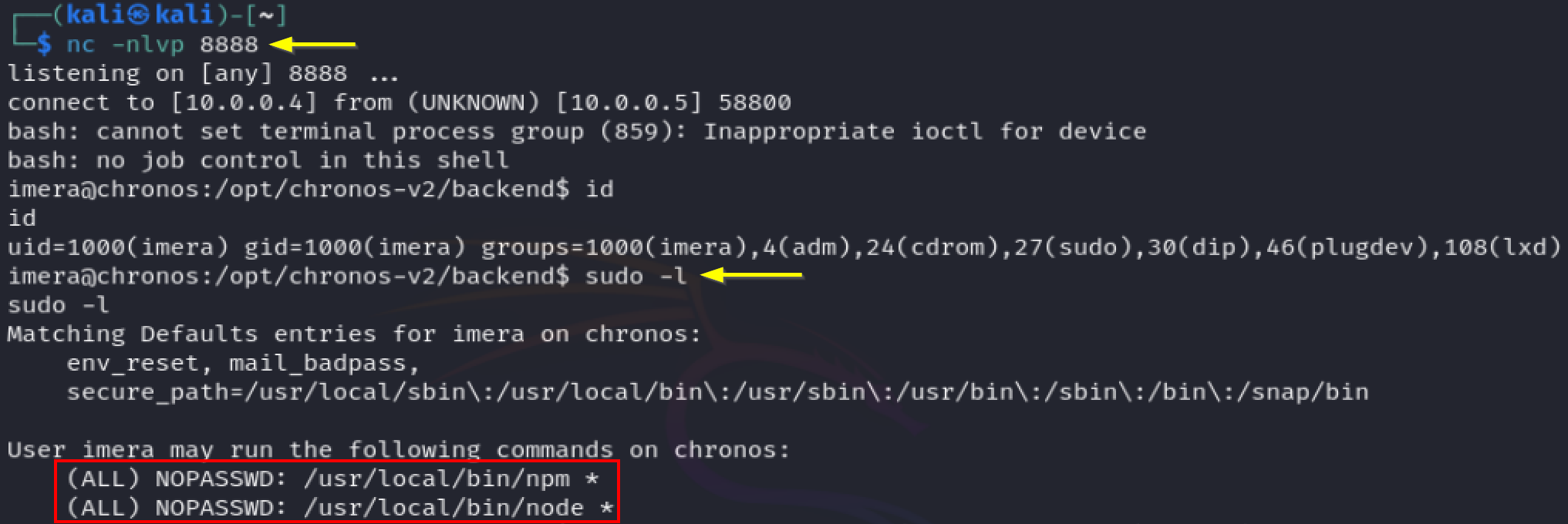
Ta truyền fille này (có thể dùng http sever như các bài trước)



Chạy file exploit

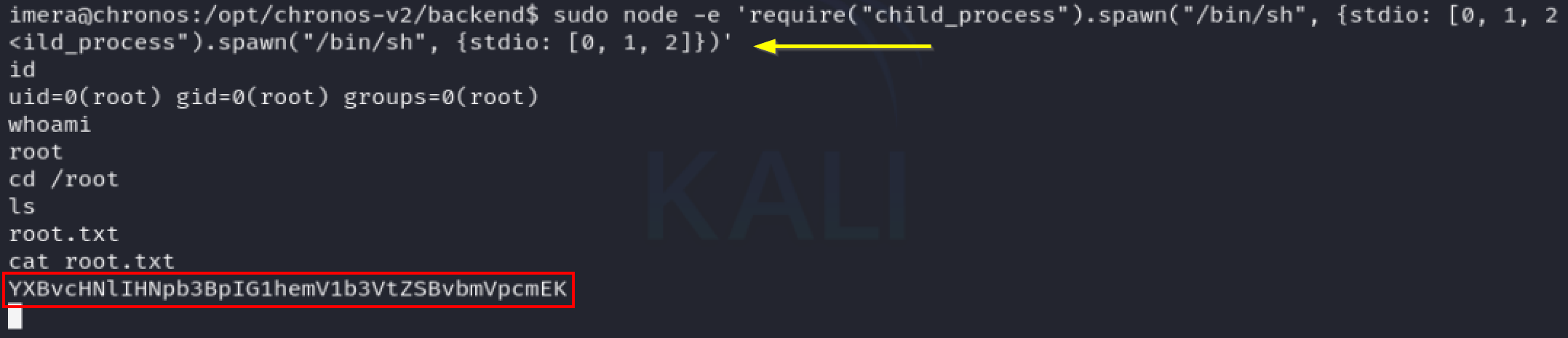
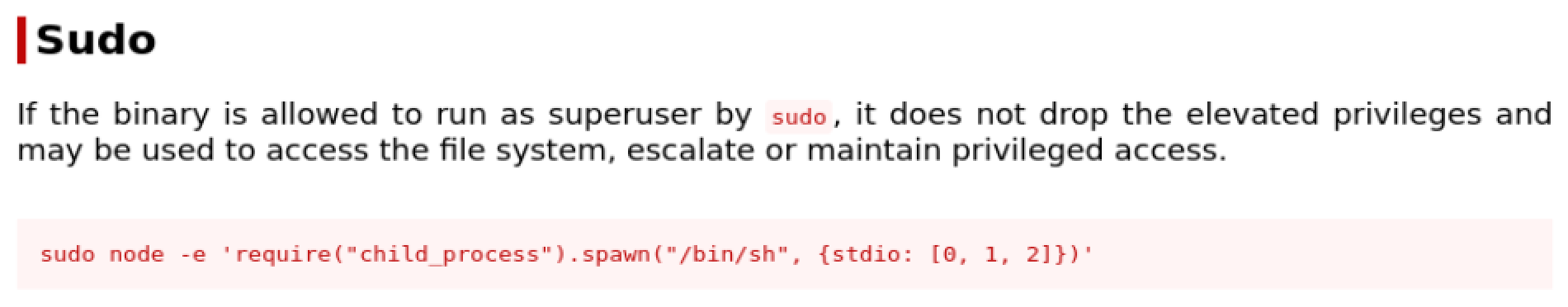


Ở đây sudo –l k dc cho phép



[https://gtfobins.github.io/gtfobins/node/#sudo](https://gtfobins.github.io/gtfobins/node/%23sudo)

Tìm trong tranng này có hd cách để leo thang



Tìm thấy cờ thành công