|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯  logo ATTT-02 |
| HỌC PHẦN  TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG |
| BÁO CÁO THỰC HÀNH  **Mr Robot** |
| |  |  | | --- | --- | | ***Họ tên sinh viên:*** | Nguyễn Hoàng Quân | | ***Lớp:*** | AT18GK | | ***Mã sinh viên:*** | AT180639 | |  |  | | ***Giảng viên:*** | TS. Lại Minh Tuấn | |
| **Hà Nội, 2024** |

MỤC LỤC

[I.Chuẩn bị 3](#_Toc76722270)

[II.Khai thác 6](#_Toc76722271)

[1.Mail Server 6](#_Toc76722272)

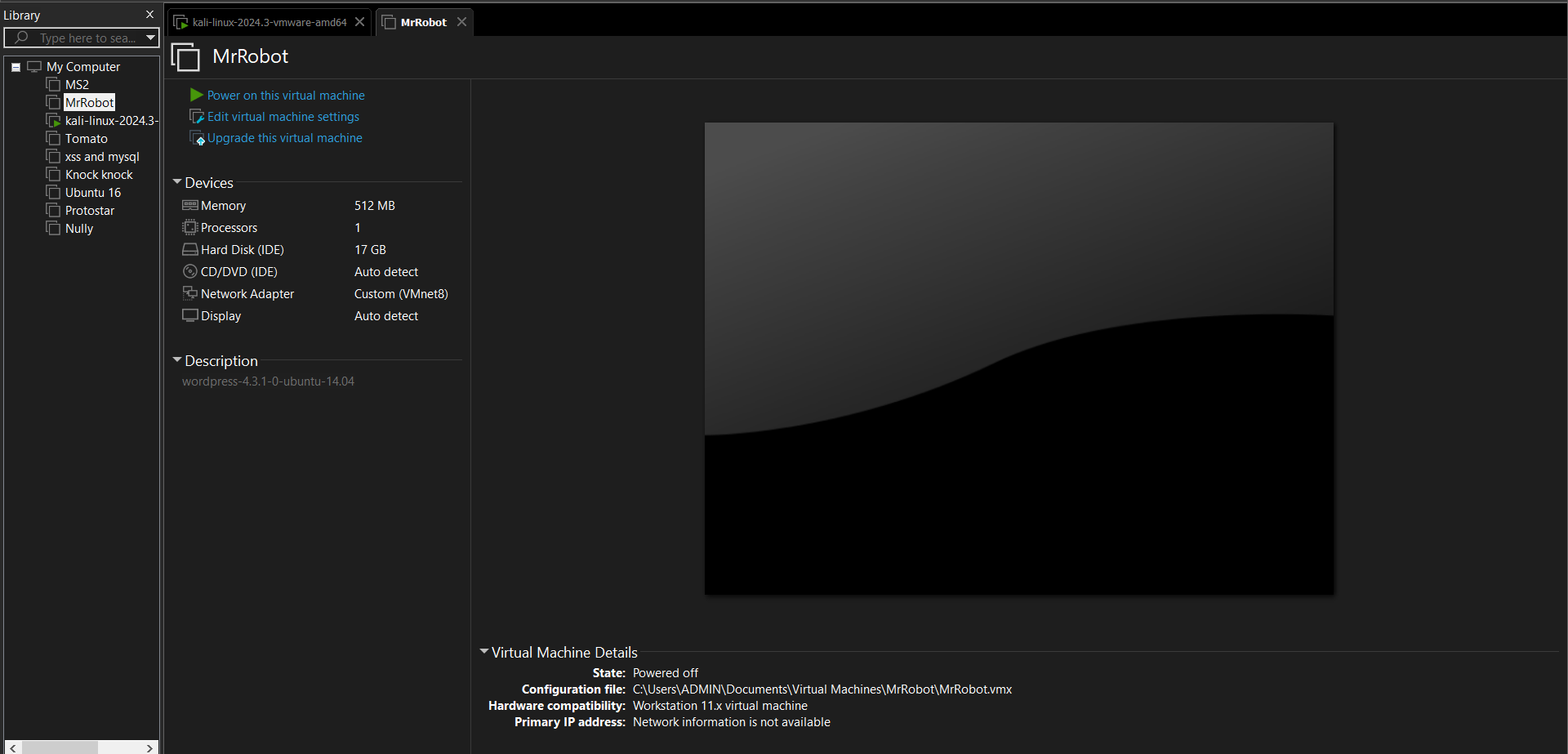
[2.Web Server 18](#_Toc76722273)

[3.Database Server 39](#_Toc76722274)

[III.Kết quả 50](#_Toc76722275)

# Chuẩn bị

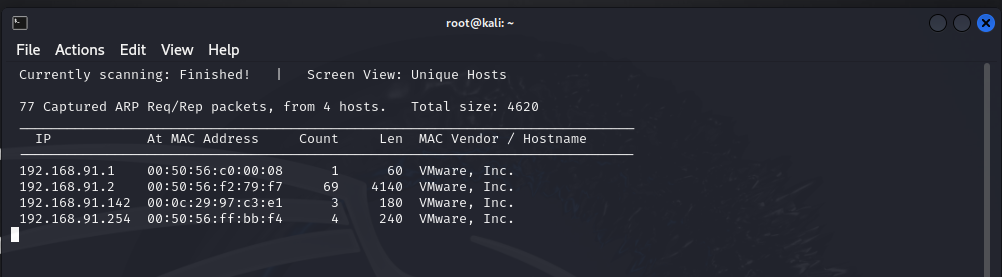
Tải máy ảo về và cài đặt



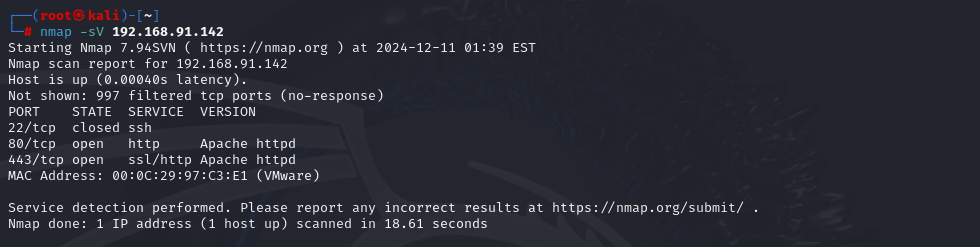
Chạy máy ảo, đợi khoảng 5-8 phút



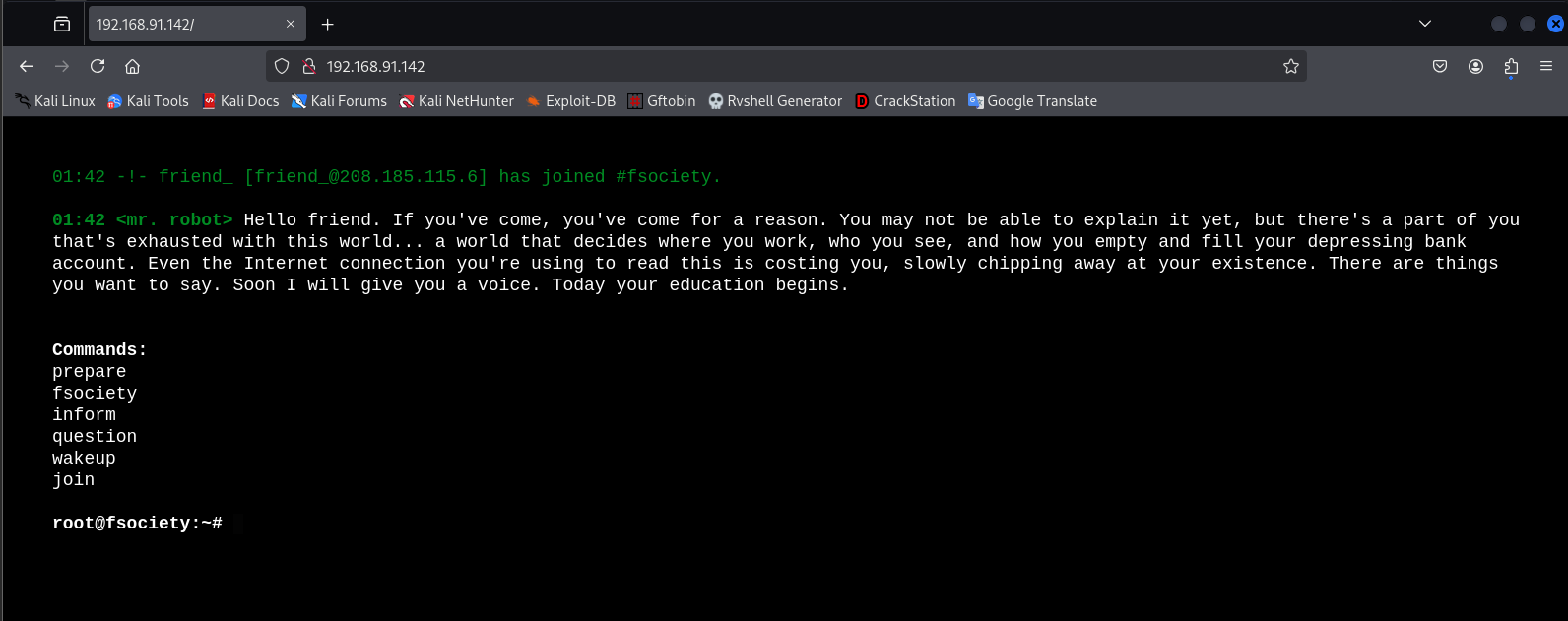
Trên máy tấn công, sử dụng nmap để quét các host đang hoạt động trên dải mạng, tìm ra IP máy ảo là 192.168.91.142



Check nhanh bằng nmap để kiểm tra các dịch vụ đang chạy trên máy ảo (192.168.91.142)



Chạy Web Server trên firefox

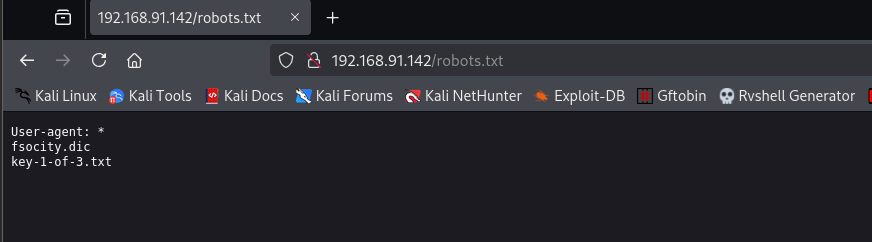


Trang Web cho chúng ta biết một vài thông tin cơ bản và cho phép nhập một số lệnh, sau khi kiểm tra nhanh thì nó có vẻ không có gì đặc biệt.

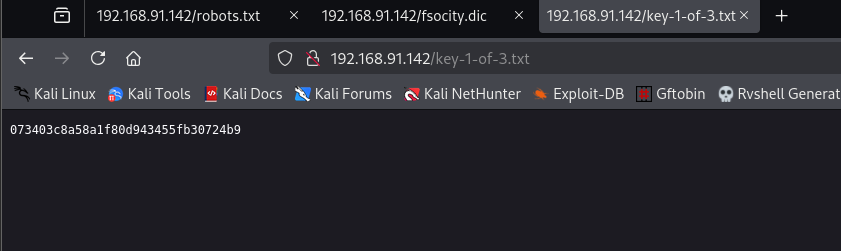
# Khai thác

## Flag 1

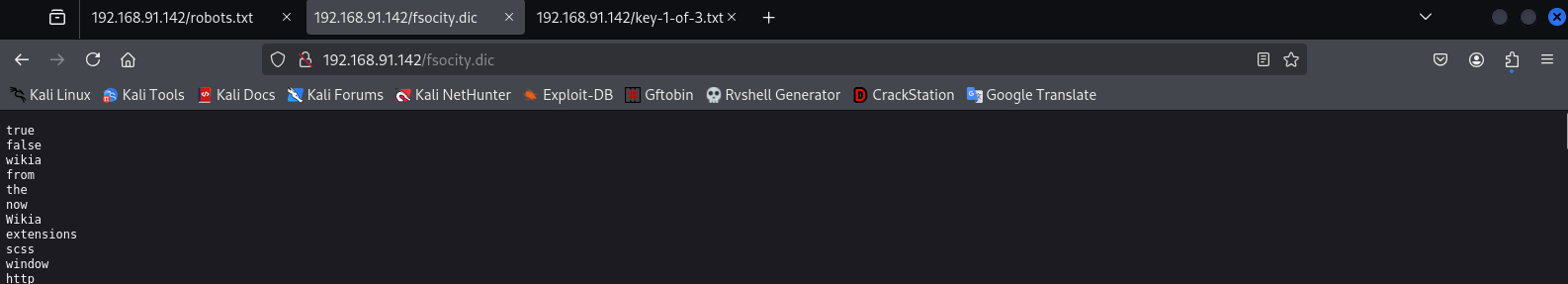
Check qua file robots.txt; là file hướng dẫn các công cụ tìm kiếm biết những phần nào của website được phép hoặc không được phép thu thập dữ liệu.



Ta tìm thấy flag đầu tiên và 1 file fsocity.dic.



## Flag 2



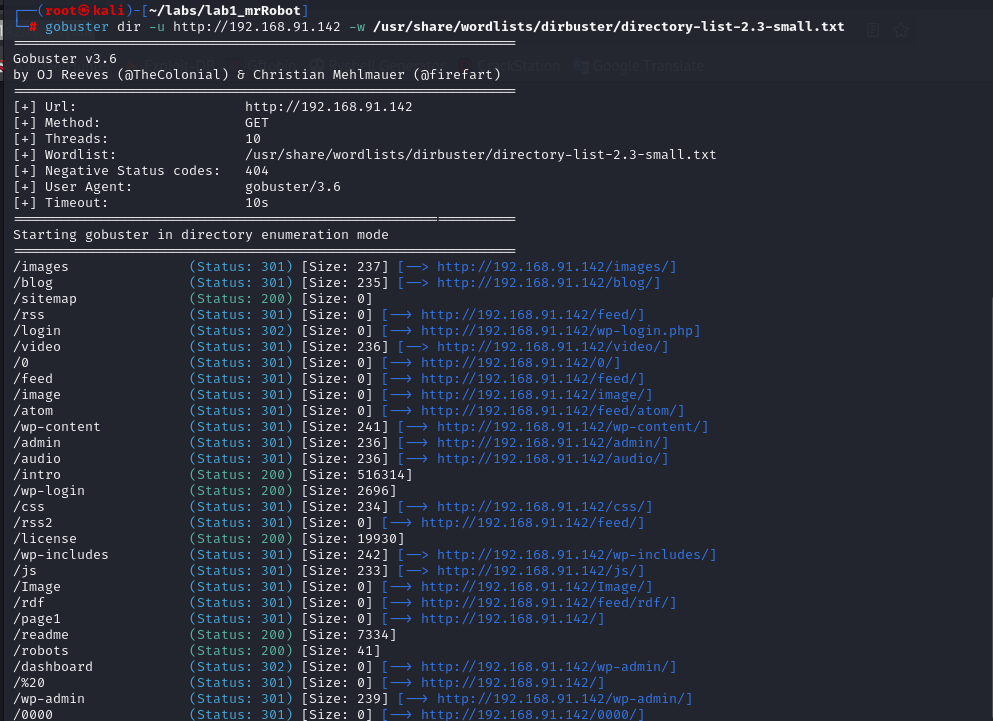
Trong file fsocity.dic chứa danh sách Wordlists, tải nó về và kiểm tra





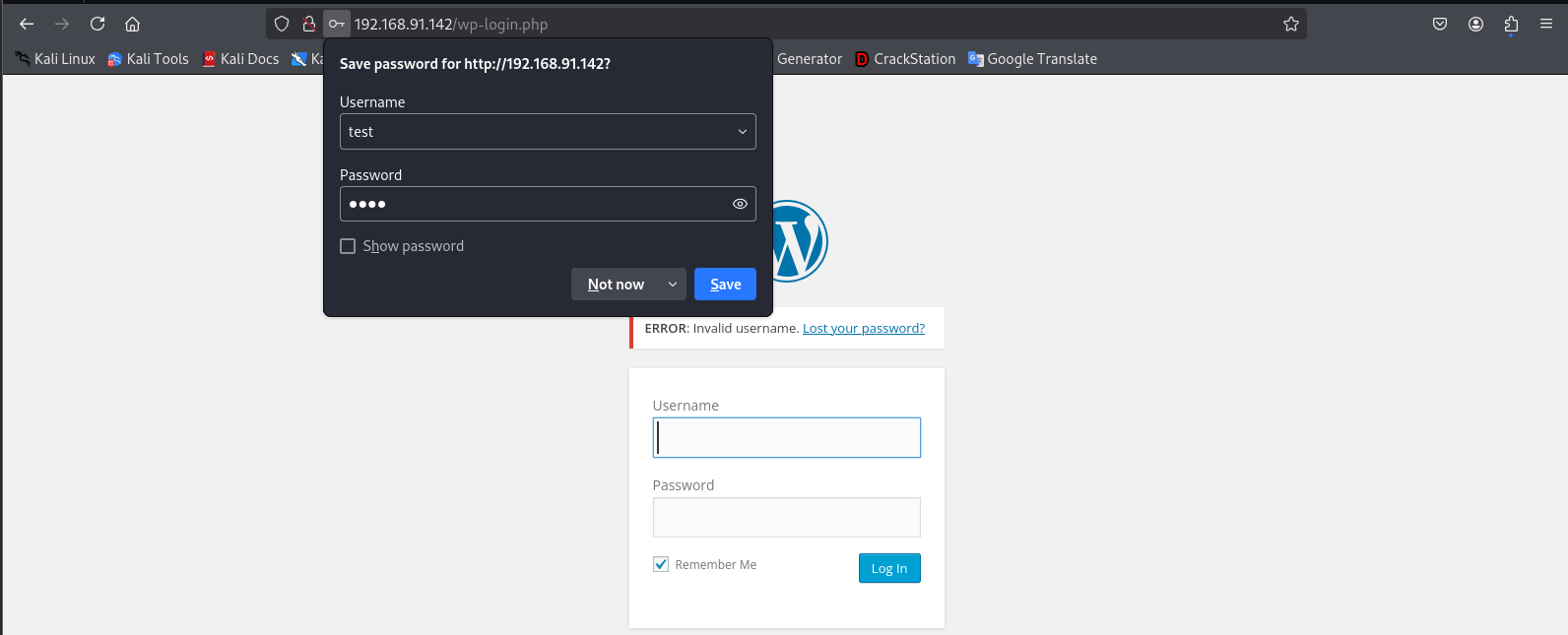
Wordlists có kích thước rất lớn, chúng ta sắp xếp lại, xóa những từ trùng lặp.

Sau đất dùng Gobuster để quét các thư mục ẩn trên máy chủ Web.



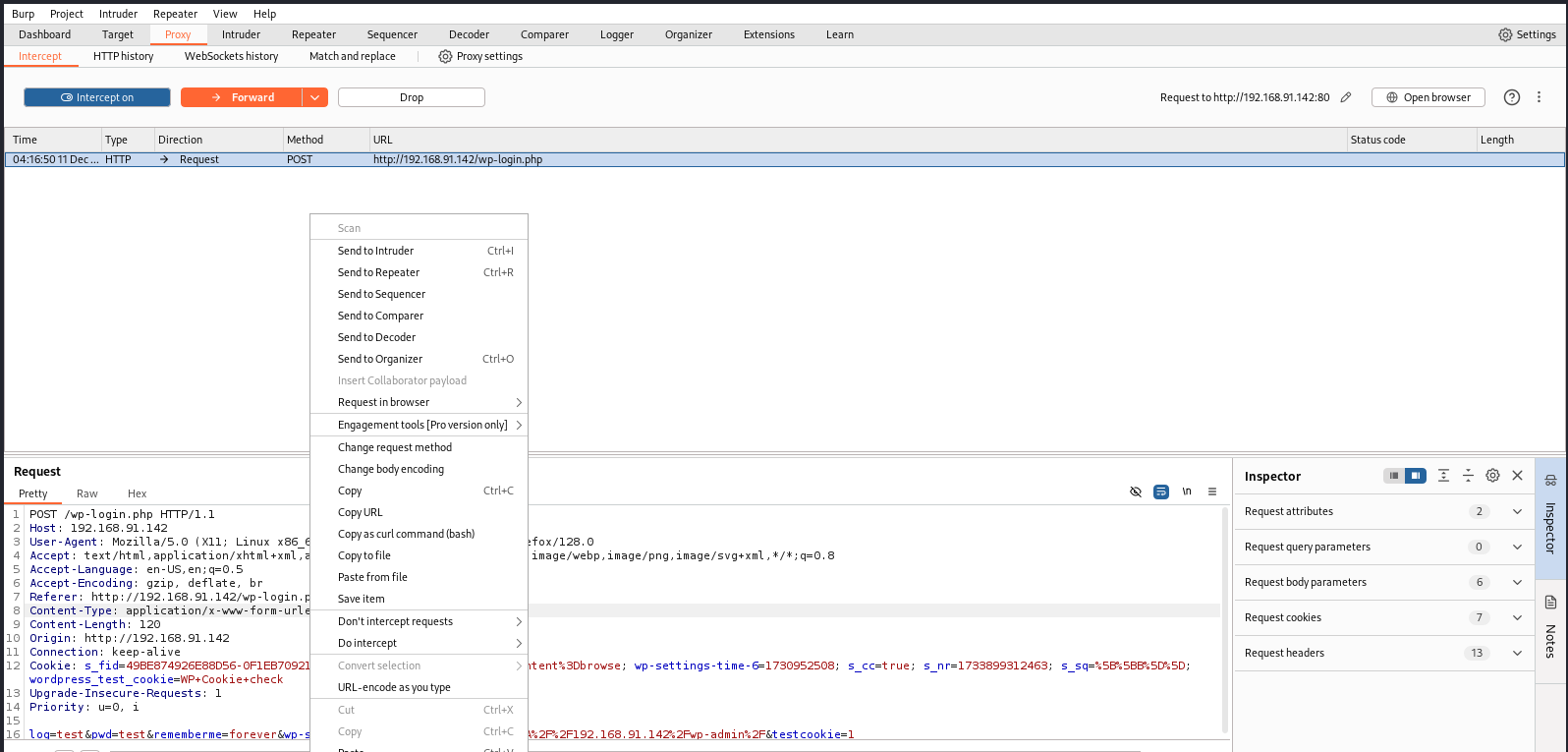
Kết quả ta có thể thấy 2 trang /wp-admin và /wp-login, là dấu hiệu cho thấy Website đang chạy Wordpress.

Ta kiểm tra qua trang wp-login, thử đăng nhập vào thì thấy báo lỗi Invalid Username.

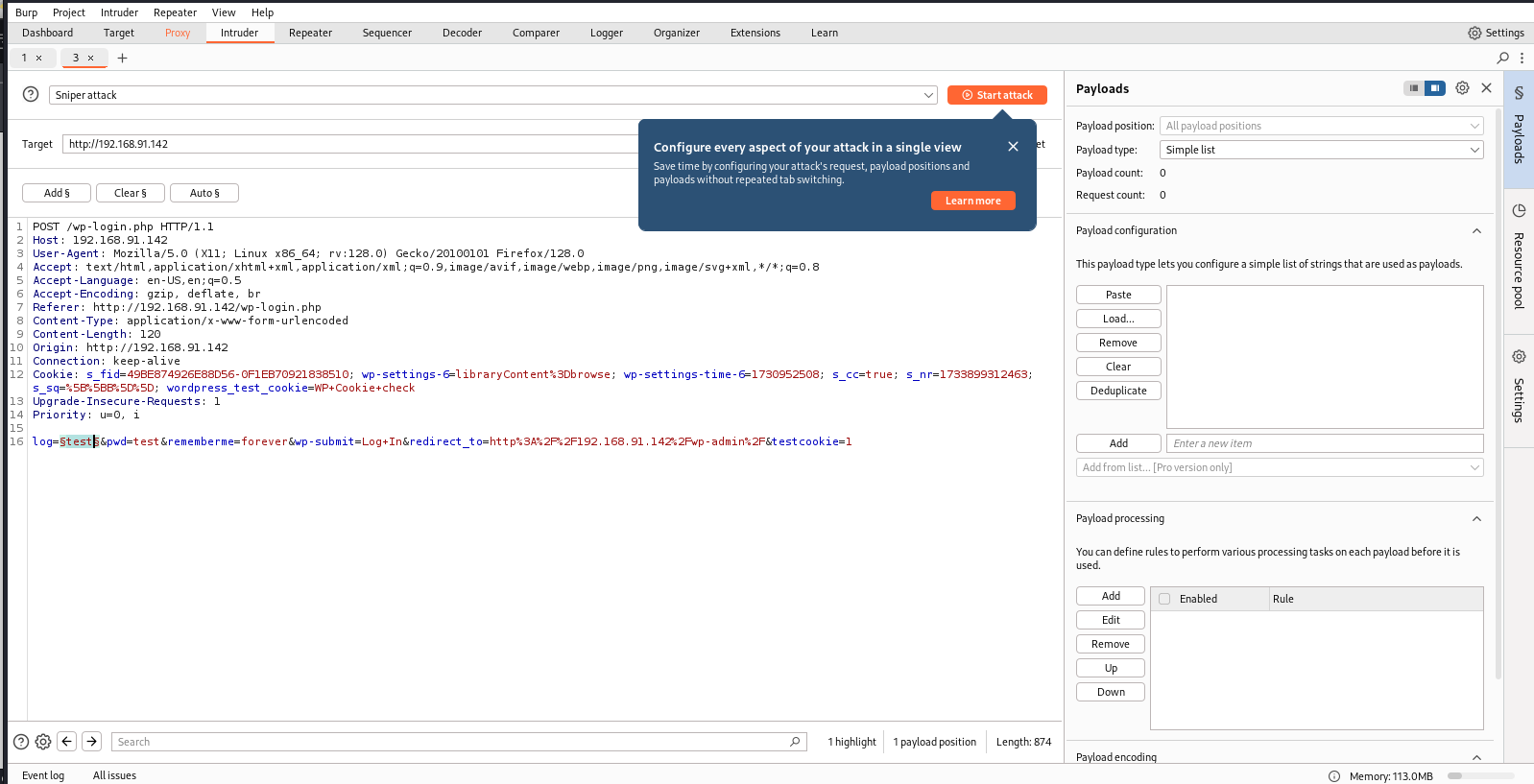


Vì thế ta có thể scan Username bằng cách check message lỗi của trang.

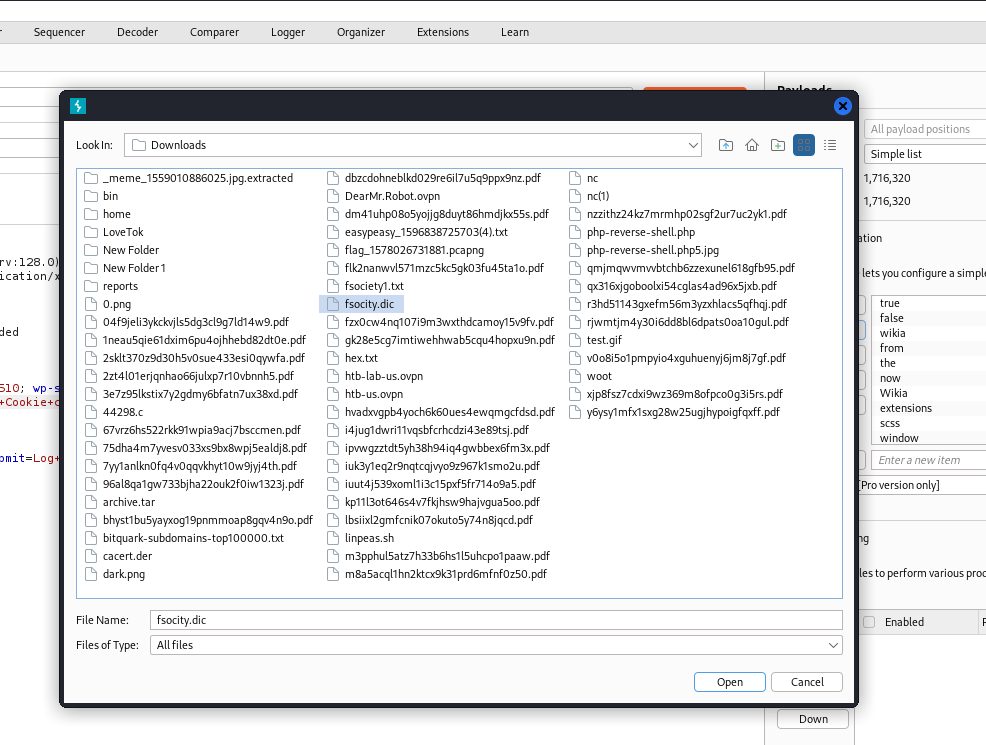
Mở Burpsuite lên, nhập thông tin đăng nhập và chặn Request, sau đó nhấp chuột phải chọn Send to Intruder.

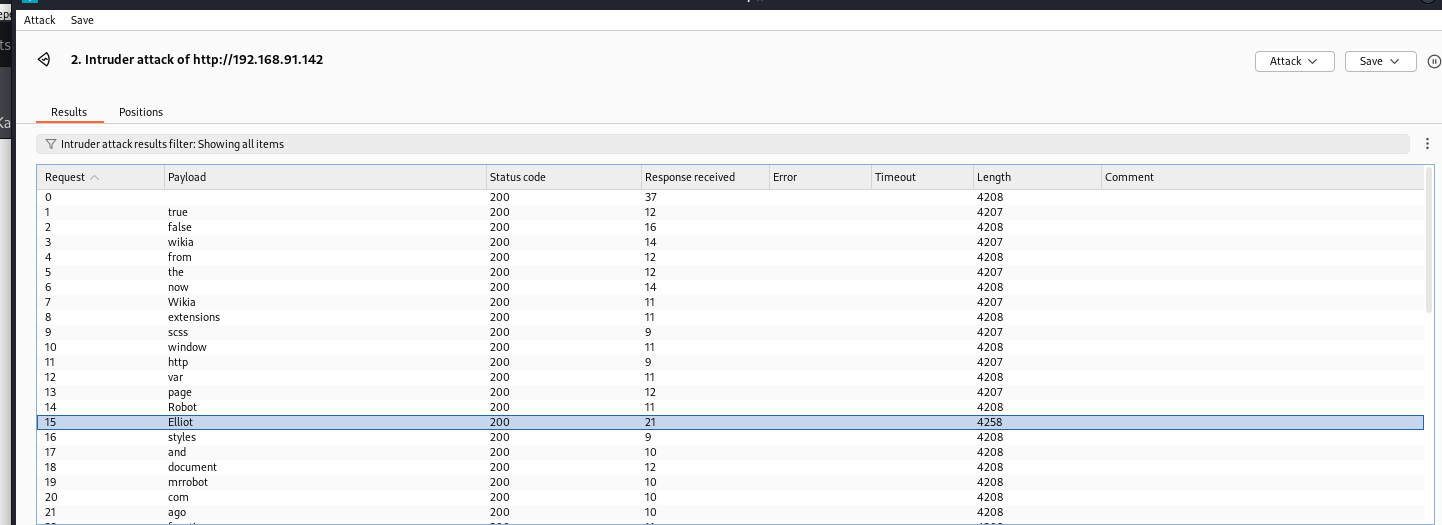


Ở đây chúng ta tô đậm user (“test”) và chọn Add để brute force username.

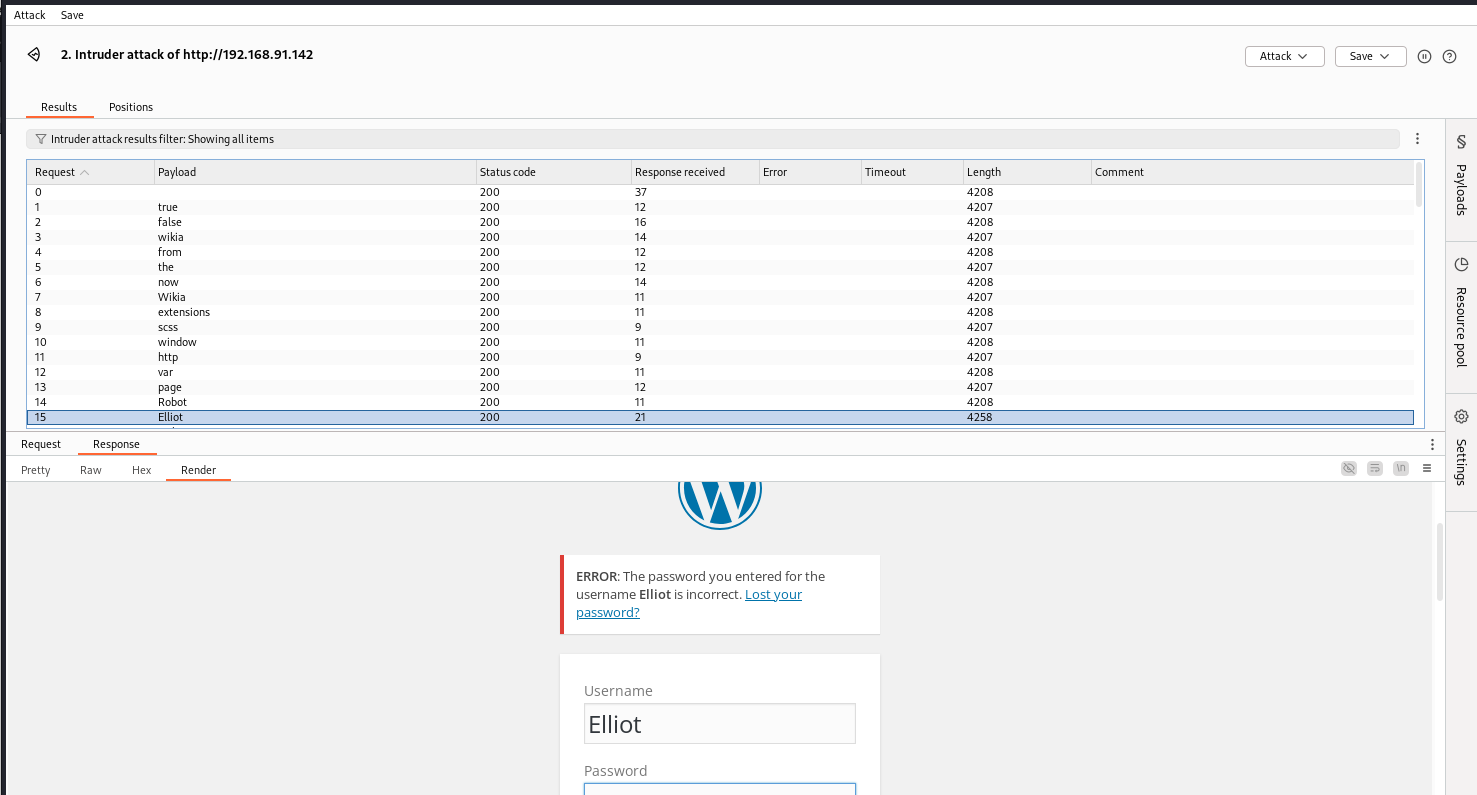


Ở phần Payload, chọn Wordlist mà chúng ta vừa tải về ( Fsocity.dic ) và chọn Start Attack



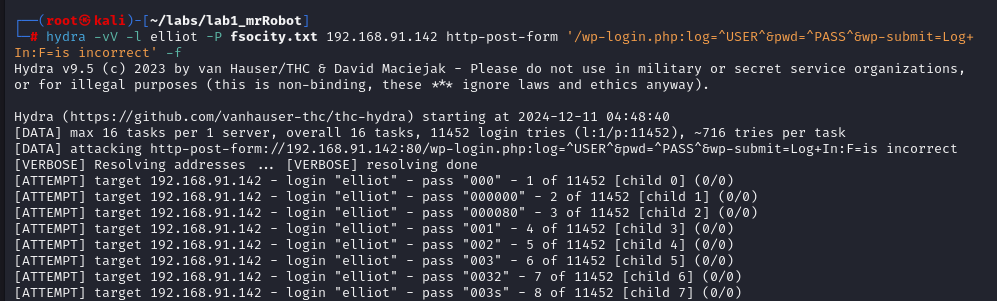


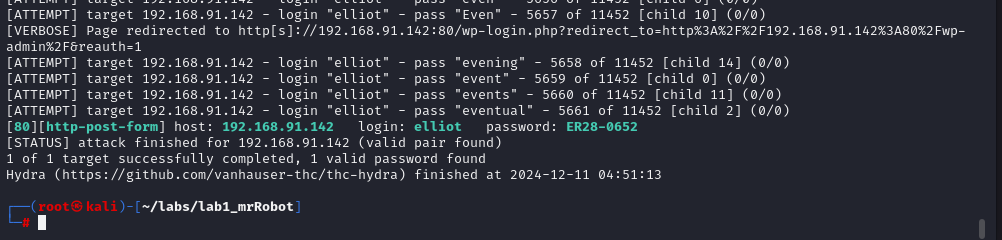
Kết quả nhận thấy rằng user Eliot có kích thước phản hồi khác biệt rõ ràng so với các trường hợp khác, ta thử check chi tiết.



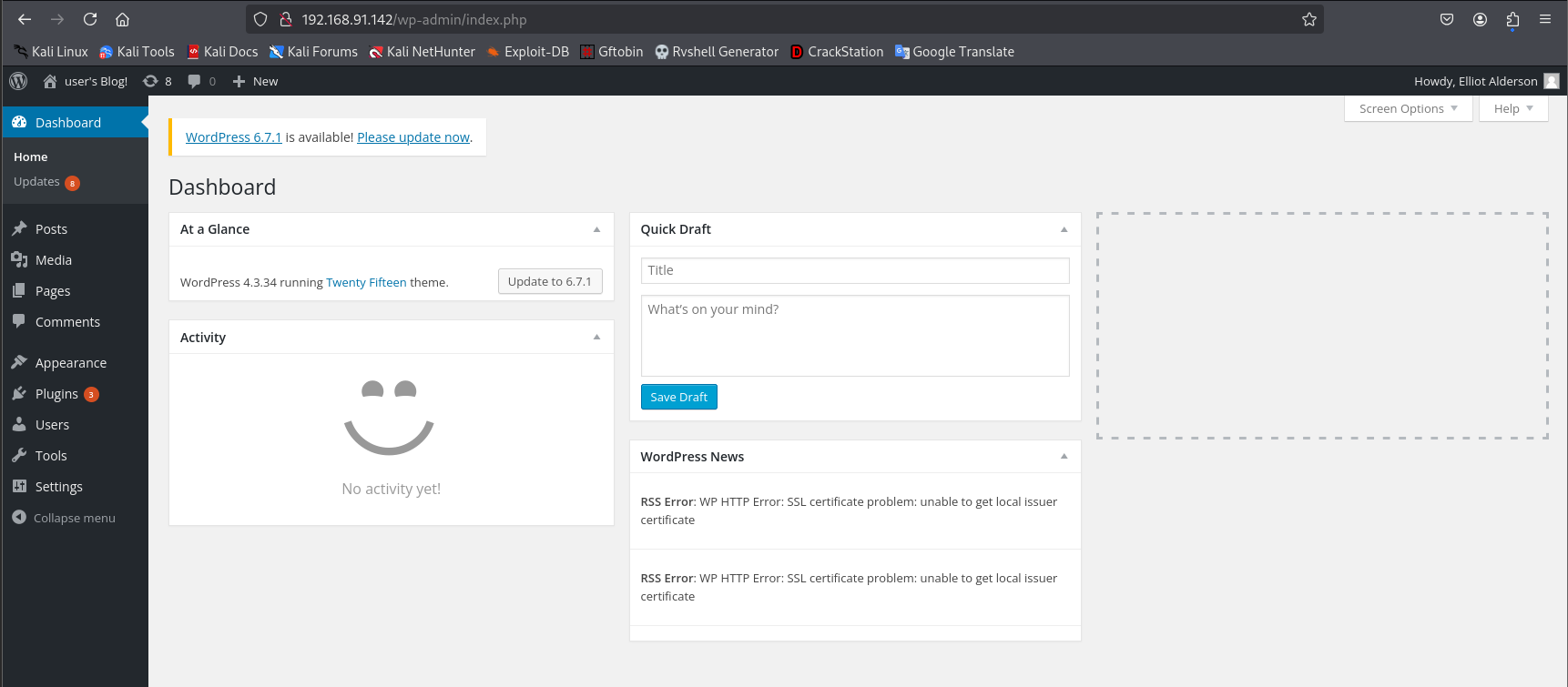
Như vậy, Elliot và một Username đúng.

Sau khi tìm được Username, ta có thể dùng hydra để thử brute force mật khẩu của Elliot.

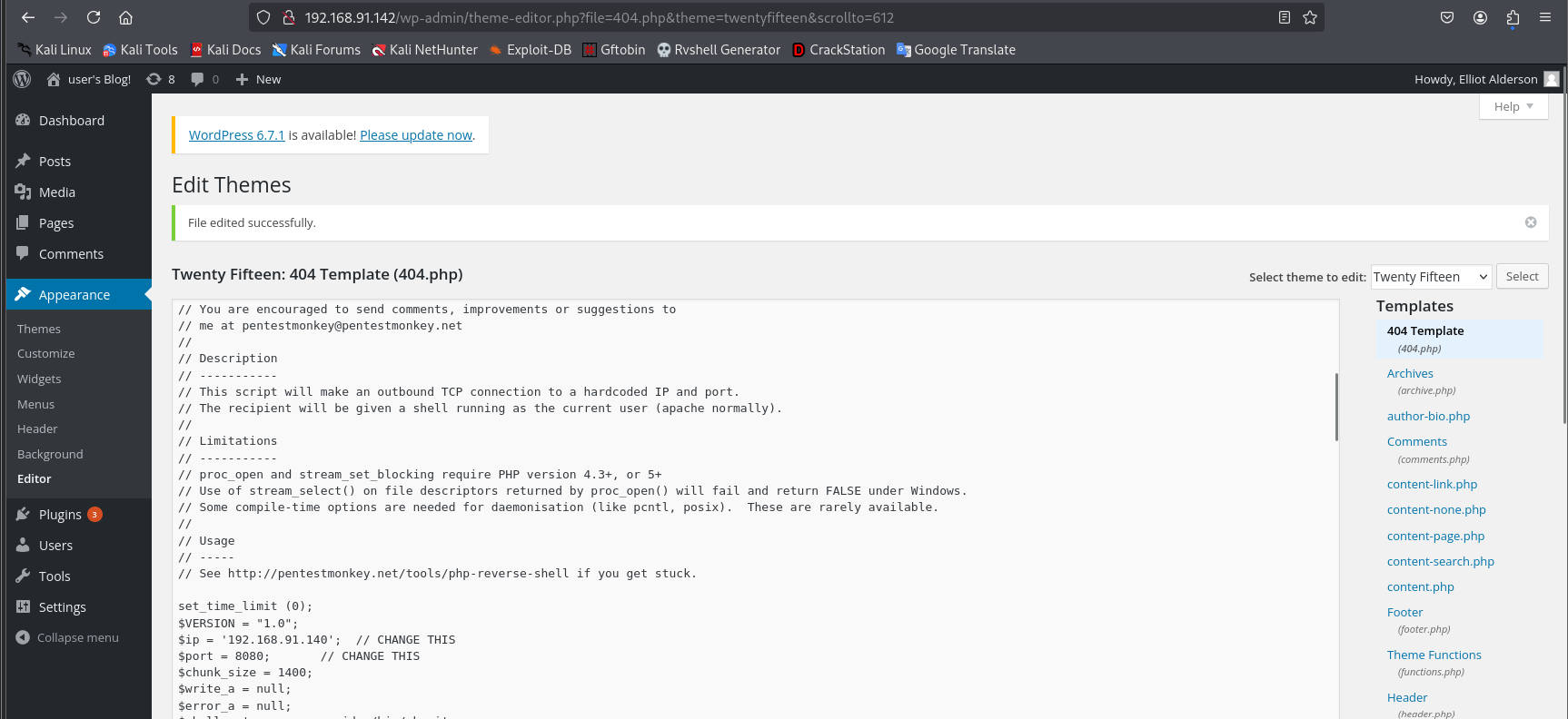




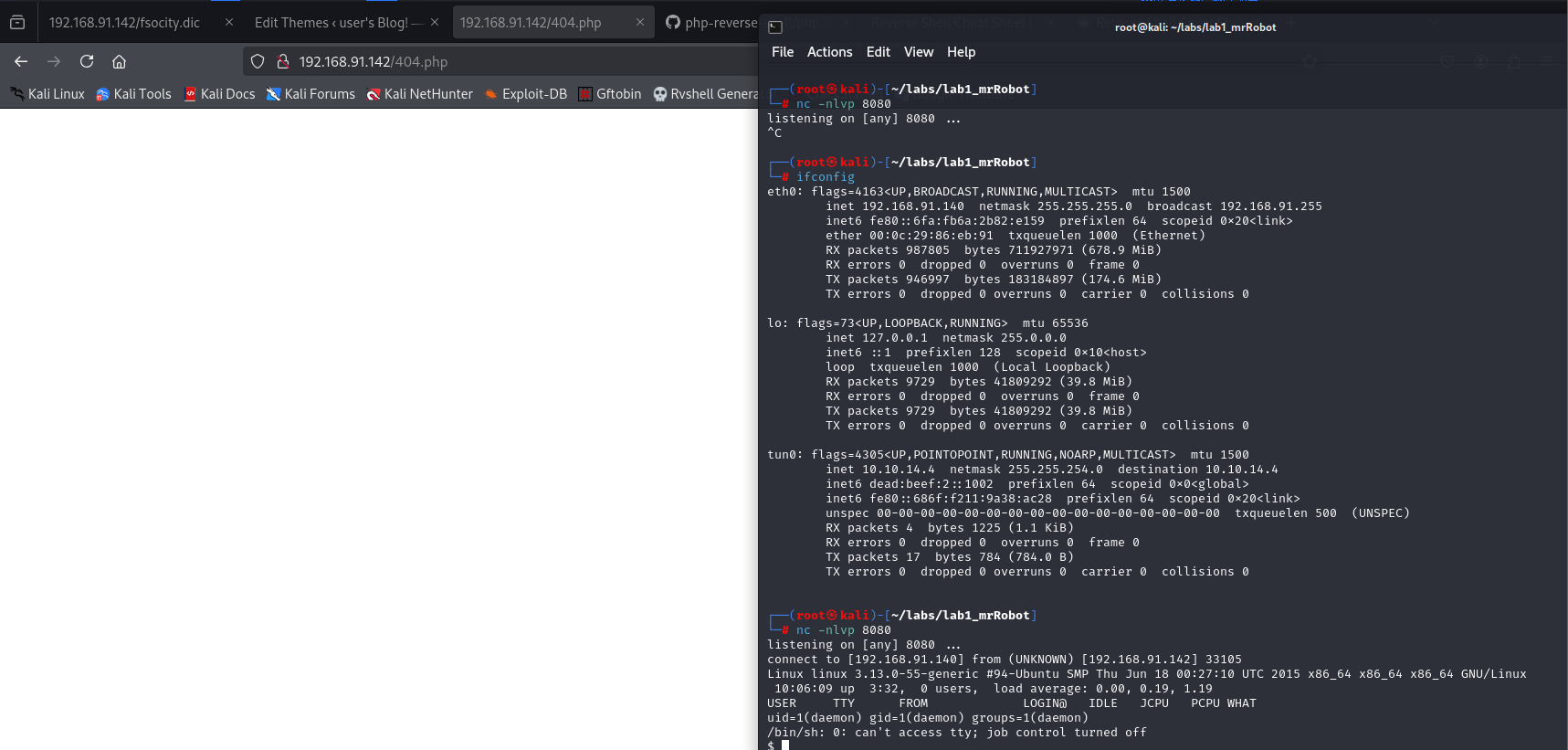
Tìm được mật khẩu cho Elliot:ER28-0652, thử đăng nhập tiếp.



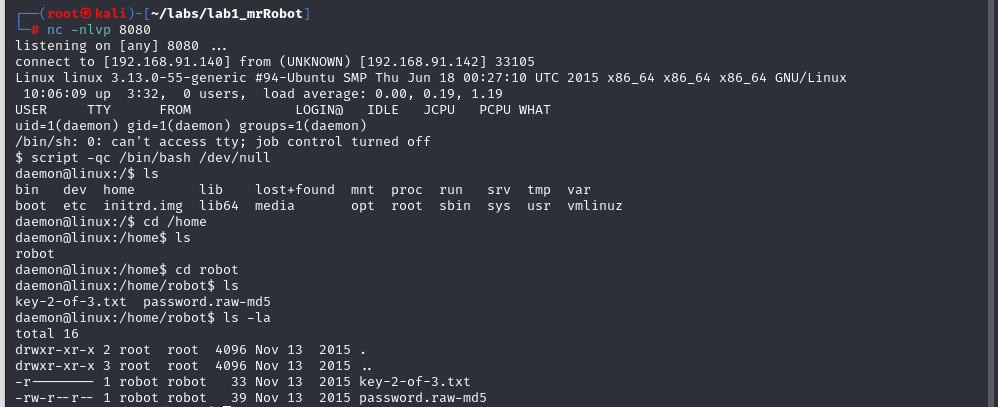
Đăng nhập thành công



Ở đây ta nhận thấy có thể chỉnh sửa các tệp php trên Wp, vì vậy có thể lợi dụng nó để đưa chèn revershell vào.



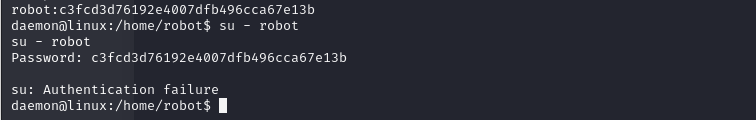
Kết quả ta đã có được shell



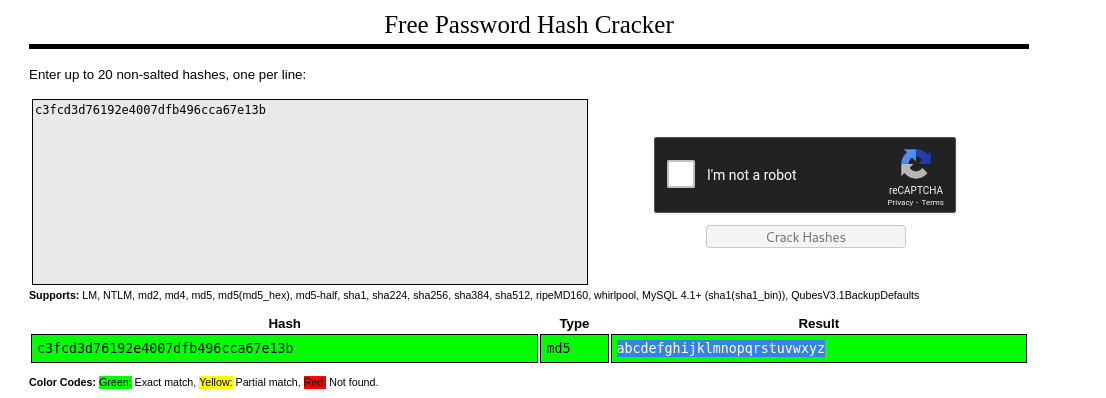
Sau khi kiểm tra chúng ta tìm được flag 2 và tệp password.raw-md5, chúng ta chỉ có thể đọc được tệp password.raw-md5.



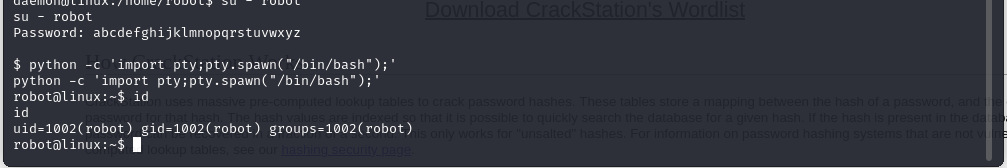
Tìm được chuỗi kí tự có thể là mật khẩu, tuy nhiên khi đăng nhập lại không được.



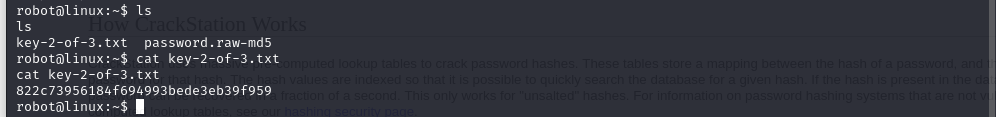
Vì vậy đây có thể là chuỗi hash, ta vào Crackstation để thử crack.



Thu được chuỗi kí tự sau khi crack thành công, thử đăng nhập lại

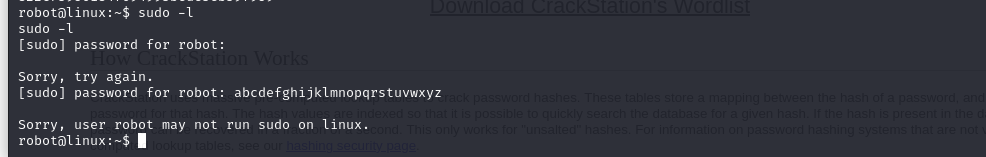


Đăng nhập thành công

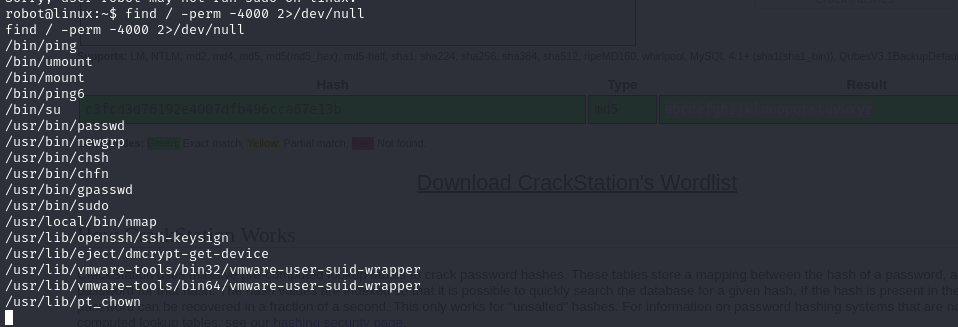


Tìm được flag 2.

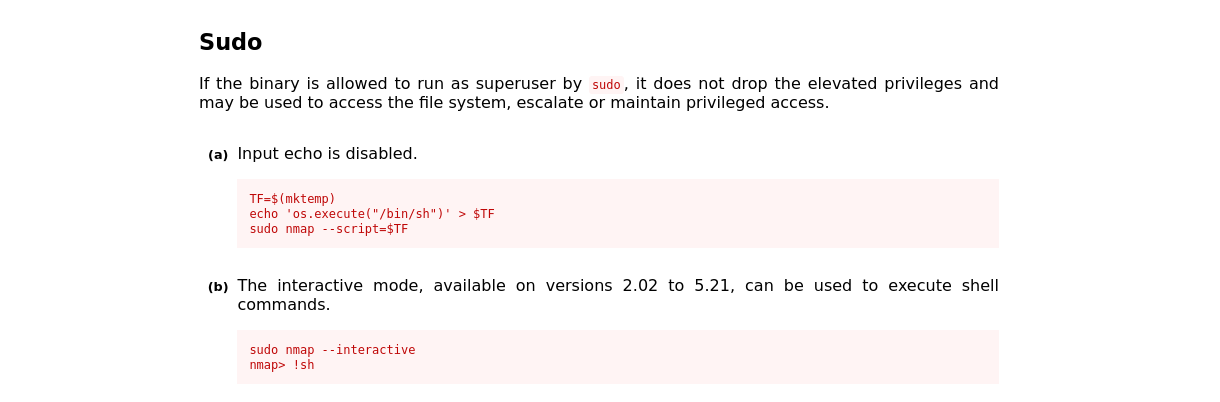
## Flag 3

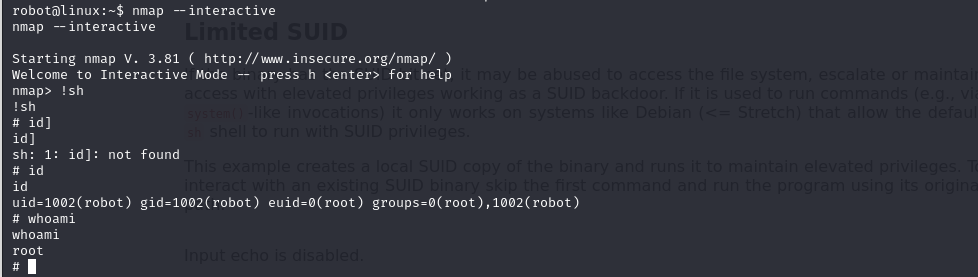


Chạy lệnh sudo –l để kiểm tra Robot có thể thực hiện các lệnh nào với quyền **root. Kết quả không có gì đặc biệt.**

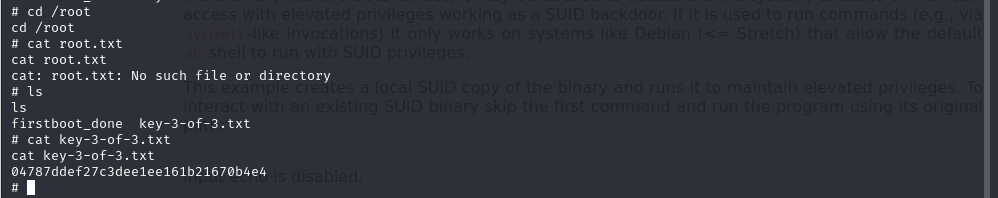
****

**Tìm kiếm các tệp có bit Suid; là các tệp có thể được chạy với quyền của chủ sở hữu. Tìm thấy nmap, kiểm tra trên Gtfobin ta có thể leo thang đặc quyền**

****

****

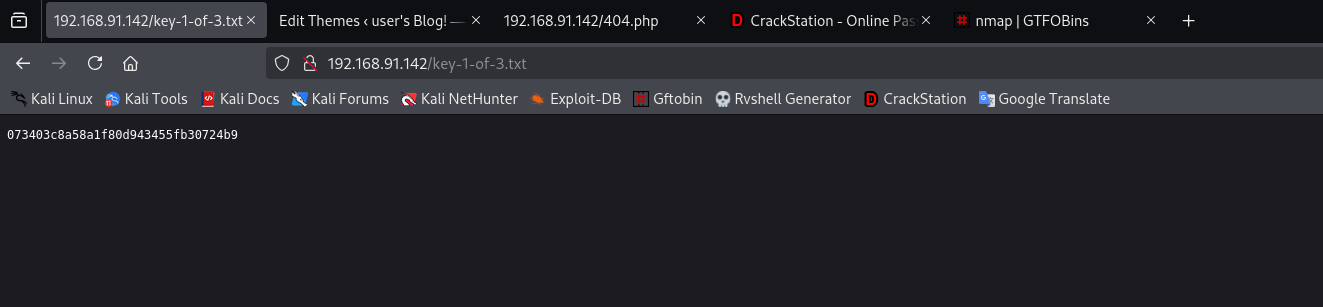
**Đã root thành công.**

****

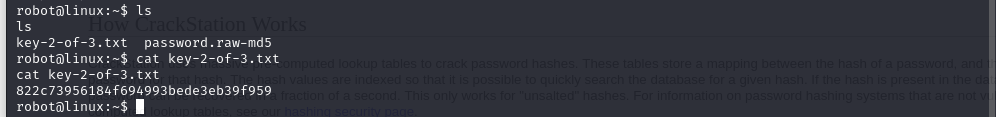
Tìm thấy Flag 3.

# Kết quả

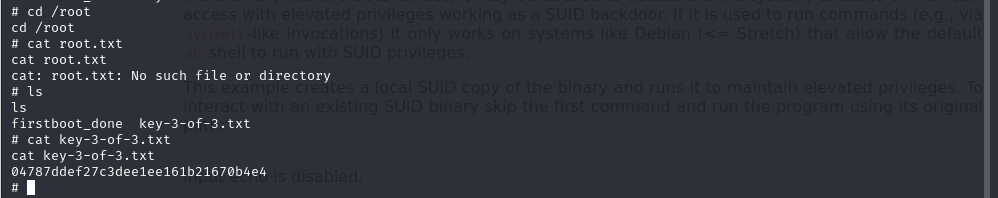
Flag thứ nhất được tìm tại http://192.168.91.142/key-1-of-3.txt



Flag thứ 2 thứ thư mục robot:



Flag cuối cùng trong thư mục root:

****