|  |
| --- |
| 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:1** |
| |  |  | | --- | --- | | ***Họ tên sinh viên:*** | Nguyễn Ngọc Anh | | ***Lớp:*** | ATM03 | | ***Mã sinh viên:*** | AT180304 | |  |  | | ***Giảng viên:*** | TS. Lại Minh Tuấn  **Hà Nội, 2024** | |
|  |

MỤC LỤC

[**I)** **Thiết lập Môi trường** 3](#_Toc184490299)

[**II)** **Scanning** 3](#_Toc184490300)

[**III)** **Exploiting** 8](#_Toc184490301)

[**1.** **Password Cracking** 16](#_Toc184490302)

[**2.** **Privilege Escalation (Leo thang đặc quyền)** 17](#_Toc184490303)

1. **Thiết lập Môi trường**

Ở đây tôi giải thích hai cách truy cập máy mục tiêu Mr Robot.

* Sử dụng VulnHub — tải máy MrRobot xuống máy của bạn, cài đặt trên nền tảng ảo hóa như virtualbox, cấu hình mạng ở đó và bắt đầu tấn công. Liên kết ở đây
* Bạn cũng có thể truy cập máy này thông qua TryHackMe. Tải tệp cấu hình vpn xuống máy của bạn và sử dụng openvpn như sau:

**Ở đây tôi chọn cách 2 để thực hiện lab này.**

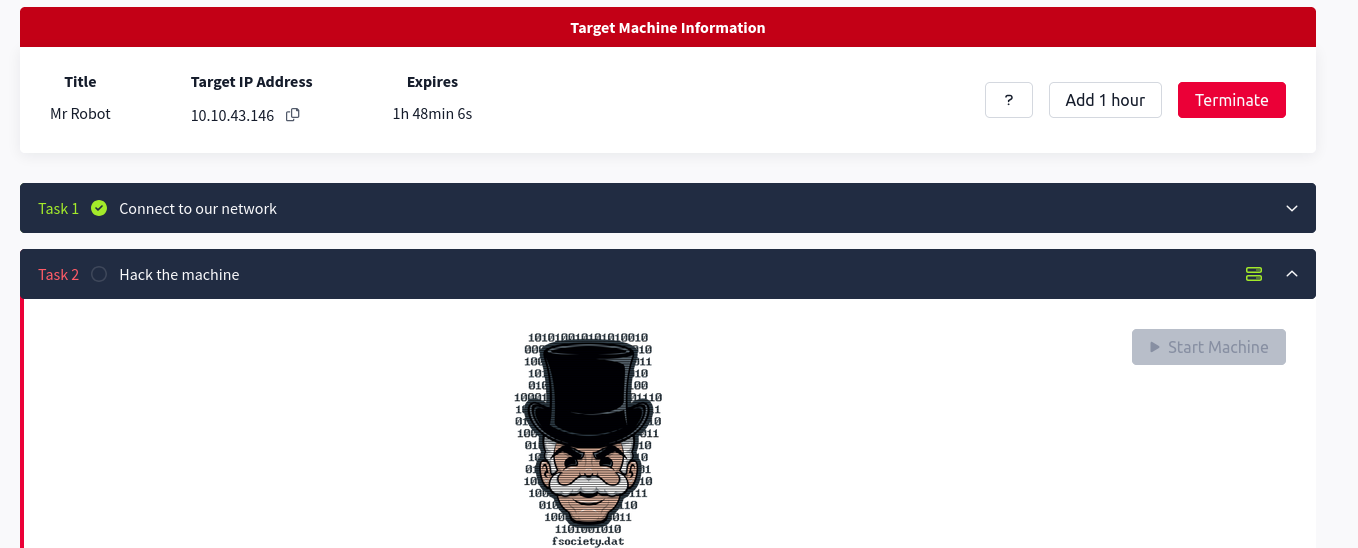
**Link:** [**https://tryhackme.com/r/room/mrrobot**](https://tryhackme.com/r/room/mrrobot)

1. **Scanning**

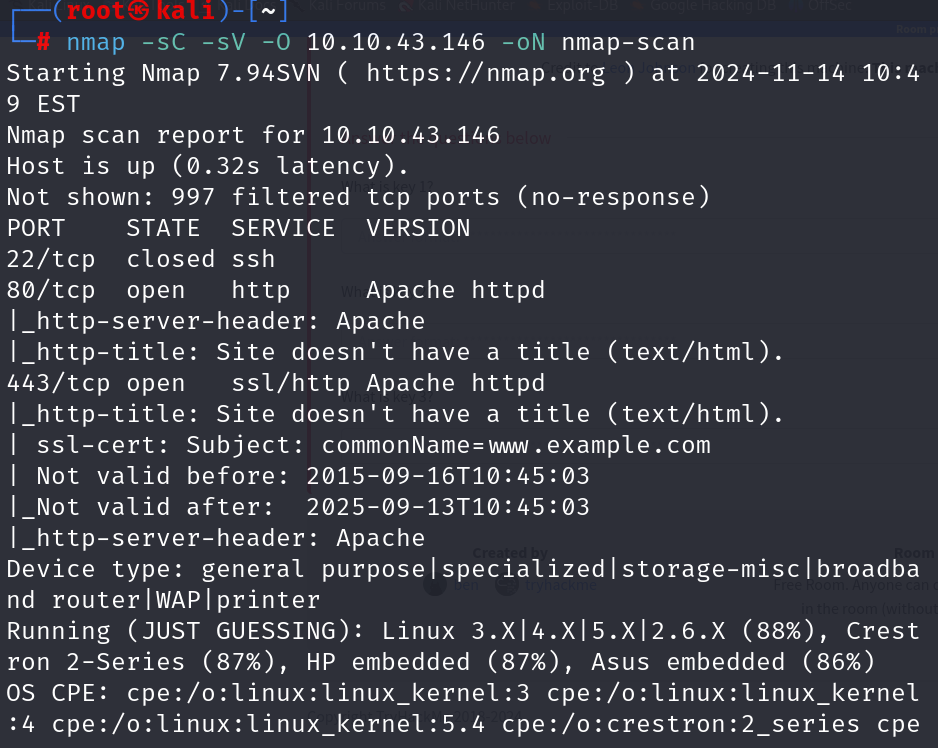
Một điều, đầu tiên chúng ta phải lưu ý ở đây là địa chỉ IP của máy đích. Trong THM, nó hiển thị ở đó nhưng trong trường hợp của virtualbox, bạn phải tìm bằng các công cụ như arp-scan hoặc nmap.

Trong trường hợp của tôi, tôi đã sử dụng máy TryHackMe. Không tập trung vào IP mục tiêu của tôi, do sự cố internet, tôi khởi động lại máy để các IP khác nhau được hiển thị trong hình.

IP mục tiêu: 10.10.43.146



Như bạn đã biết, bước đầu tiên của chúng ta trong CTF như vậy là quét mạng. Tôi cũng làm như vậy ở đây, sử dụng nmap.



Ở đây,

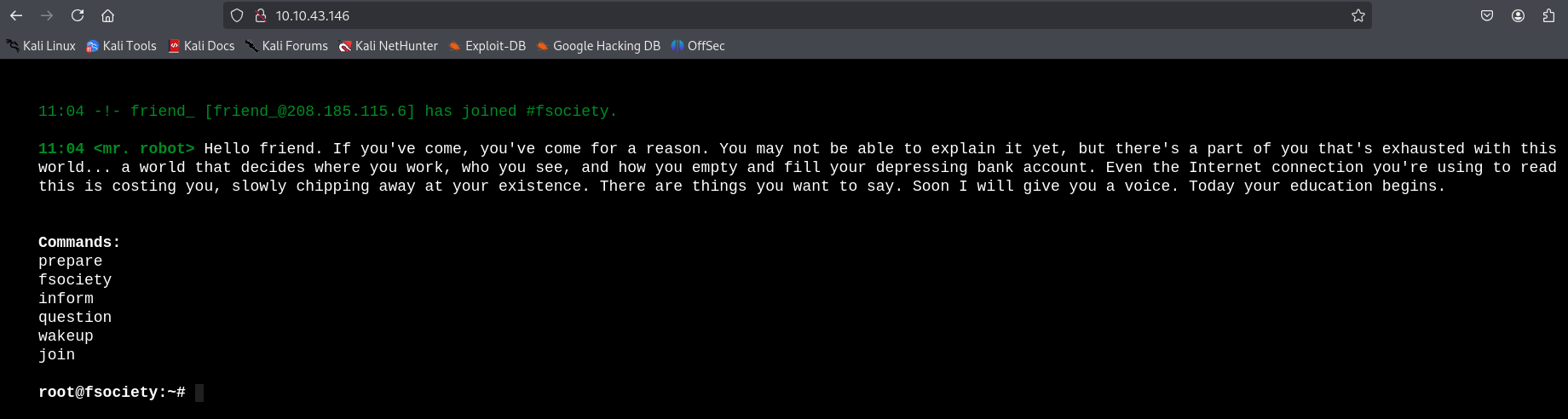
* sC: tương đương với — script=default, tức là chạy mà không có script
* sV: Để xác định thông tin dịch vụ/phiên bản của các cổng mở
* O: cho phép phát hiện hệ điều hành
* oN: để xuất ra bản quét ở dạng bình thường, được lưu trữ trong nmap-scan

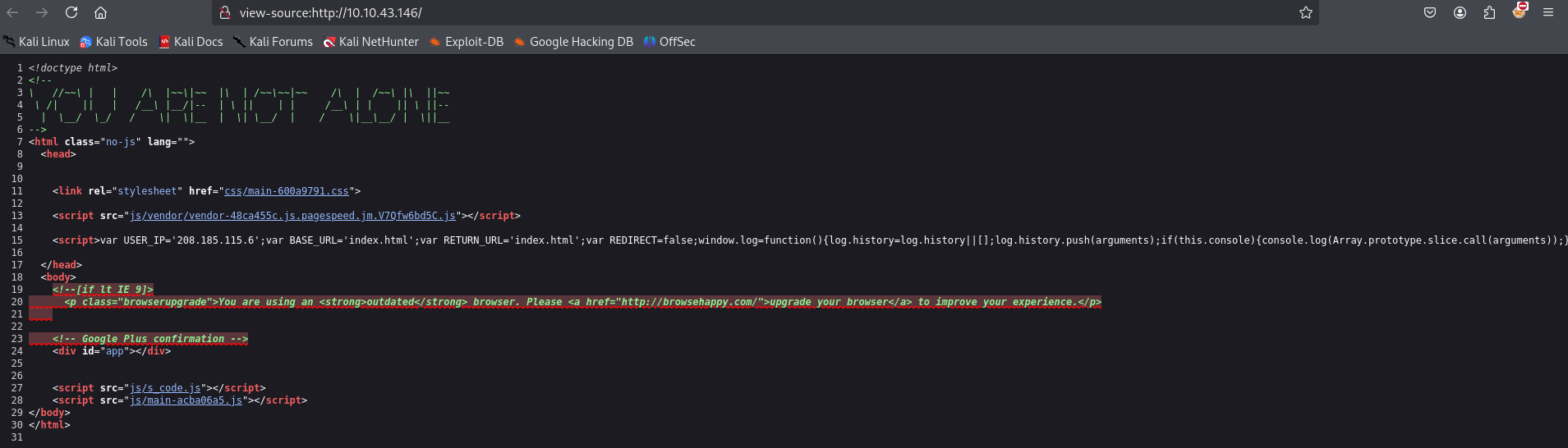
Nó hiển thị một cổng đóng là 22 và hai cổng đang mở là 80,443.

Ta có thể chạy nmap với option khác,

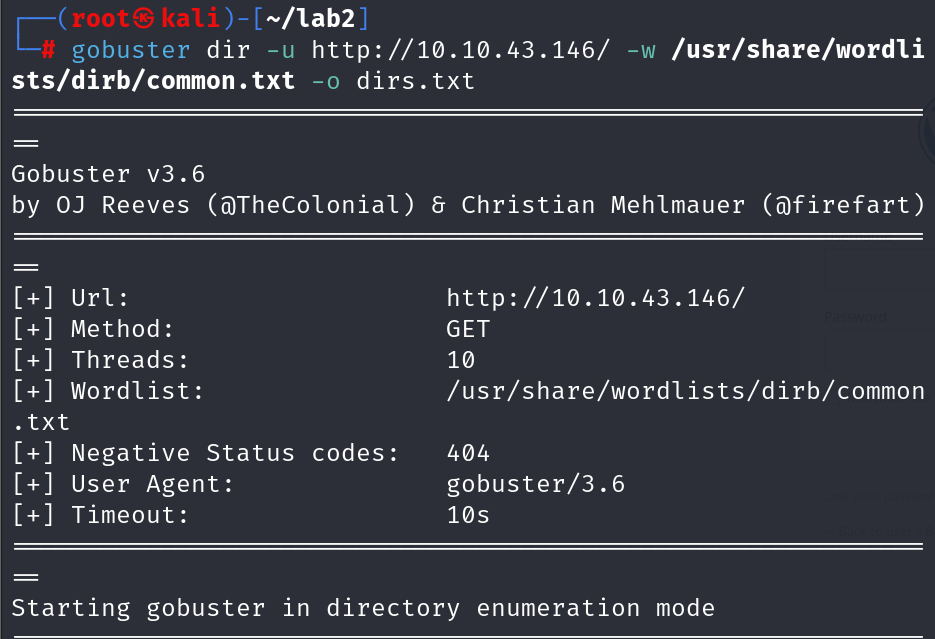
* A: Nó cho phép phát hiện hệ điều hành, phát hiện phiên bản, quét tập lệnh và theo dõi tuyến đường
* oN: để lưu trữ đầu ra

Nó hiển thị port 80 và 443 đang mở, bởi vậy hãy xem website của nó





Không có gì đặc biệt ở đó nhưng bản thân trang web thì đặc biệt. Chúng tôi không biết sitemap của trang web này, có thể có các thư mục đặc biệt nên chúng tôi phải tìm. Ở đây tôi sử dụng gobuster.

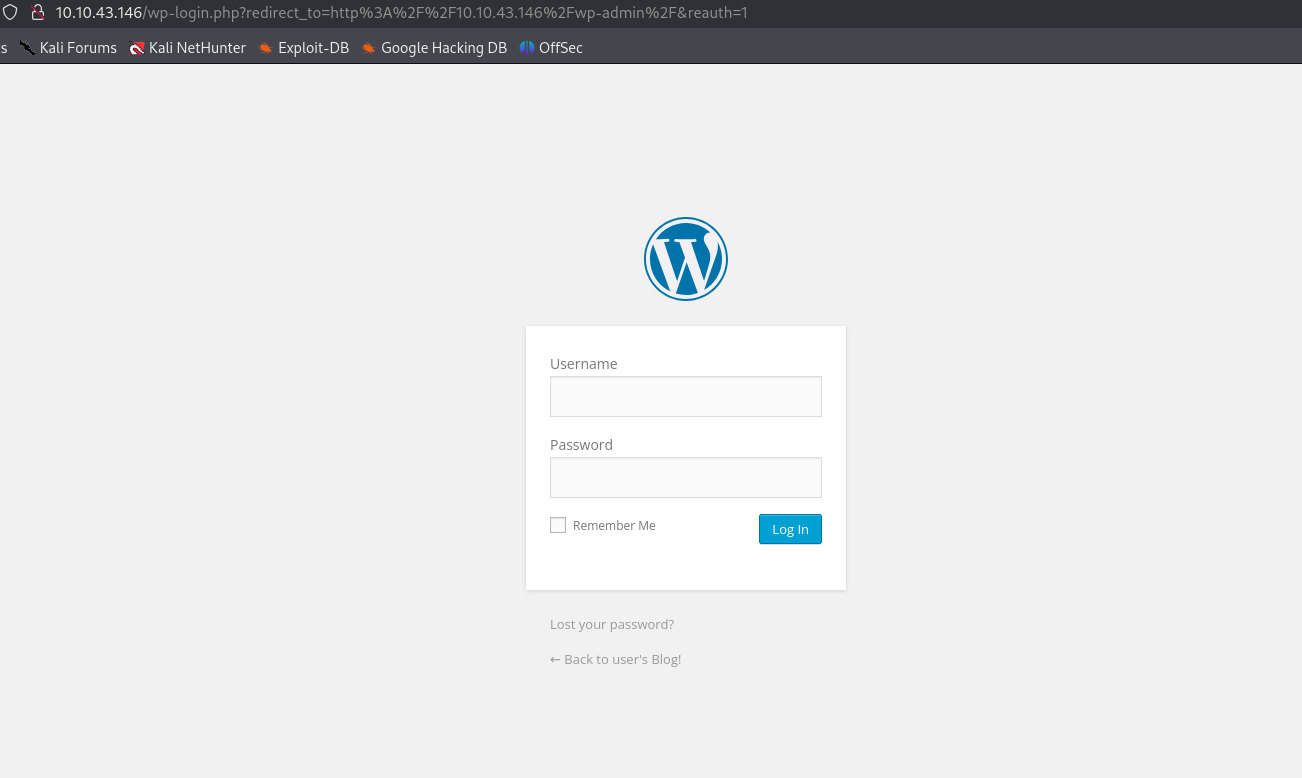


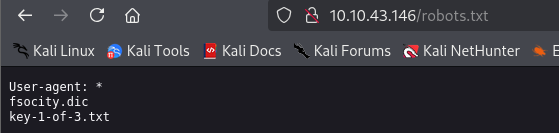
Ở đây,

* u: url của mục tiêu
* w: danh sách từ
* o: xuất kết quả vào một tệp

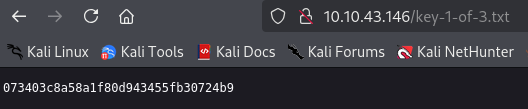
/dashboard đặc biệt vì có giao diện đăng nhập bảng quản trị cho trang web WordPress. Cũng hãy kiểm tra robots.txt, cũng đặc biệt đối với chúng ta.



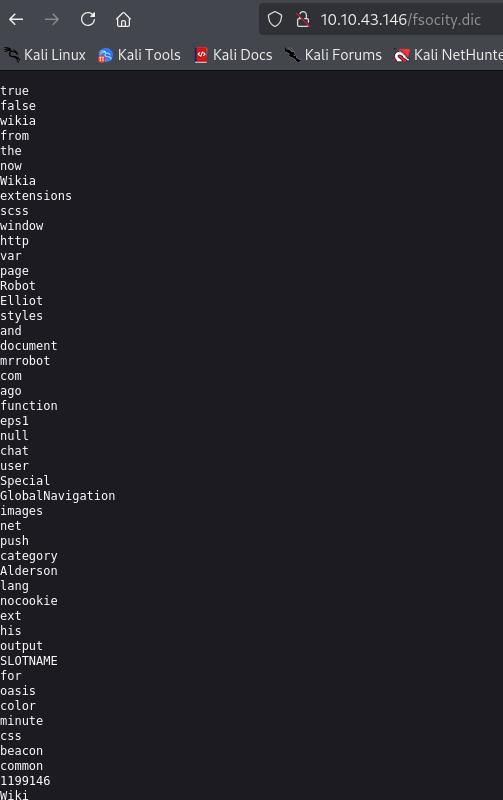




Cái key-1-of-3.txt, chúng ta sẽ truy cập vào đó để xem flag của mình.

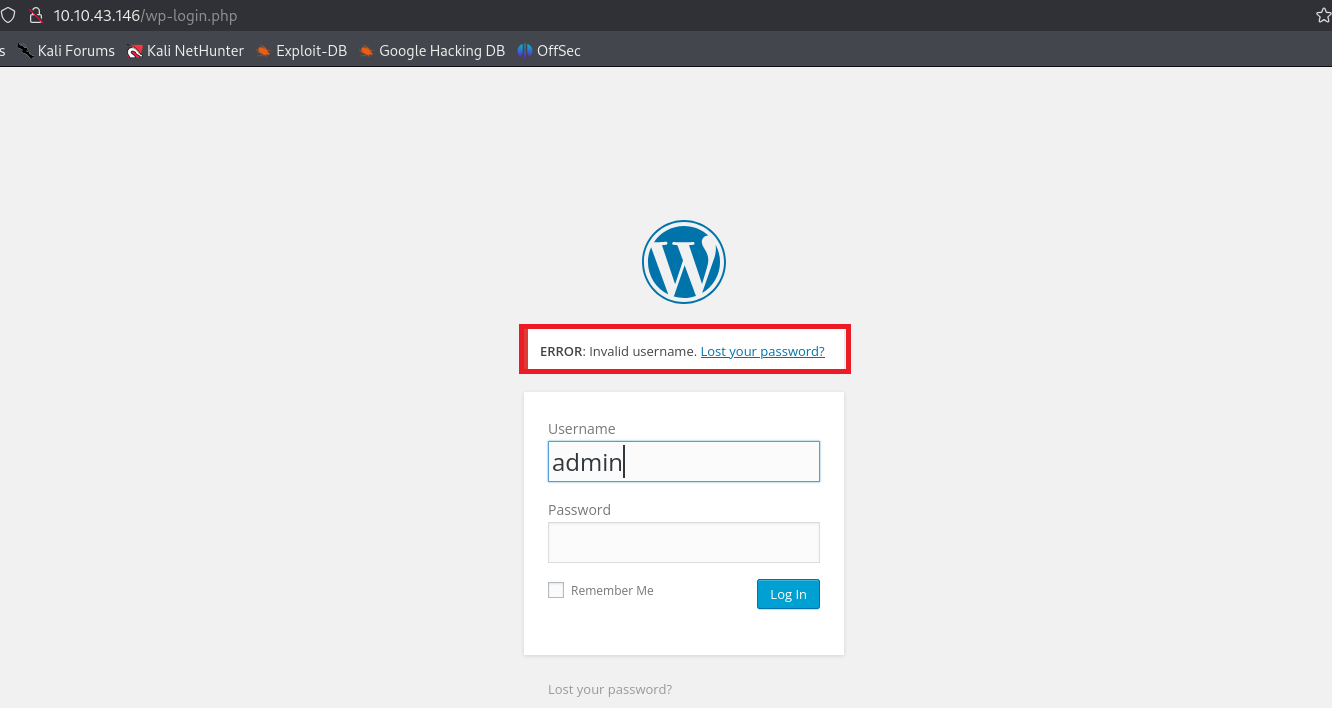


fsociety.dic là một danh sách từ, có thể hữu ích khi đăng nhập vào bảng quản trị hoặc bảng điều khiển của trang web đó. Vì vậy, hãy mở và lưu nó trên máy.

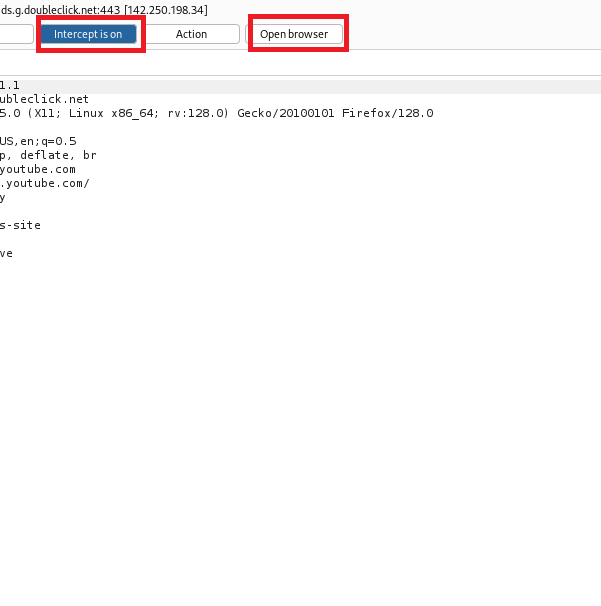


1. **Exploiting**

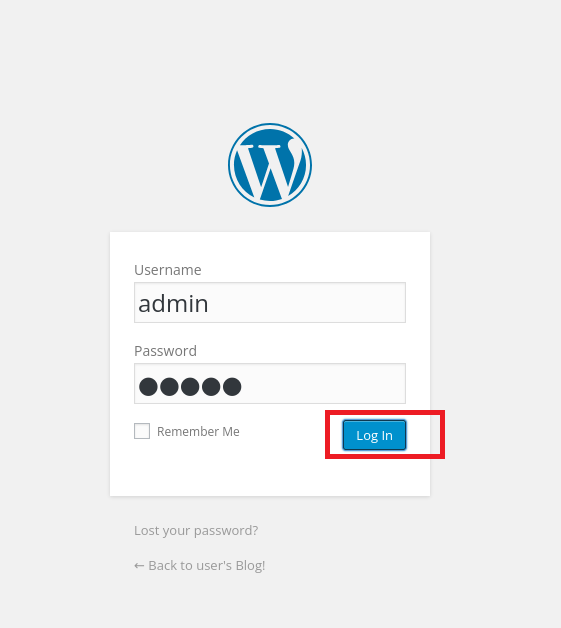
Bây giờ chúng ta vào giao diện trang đăng nhập, ta thử một vài trường hợp random username và password. Nó cho ta thấy



Trường username là không hợp lệ. Bây giờ chúng ta phải tìm tên người dùng hợp lệ trước rồi mới đến mật khẩu. Burp Suite có thể hữu ích trong tình huống này. Mở Burp Suite, trong tab proxy, mở trình duyệt từ đó và đảm bảo trên intercept để tất cả các yêu cầu đều đi qua proxy burp.

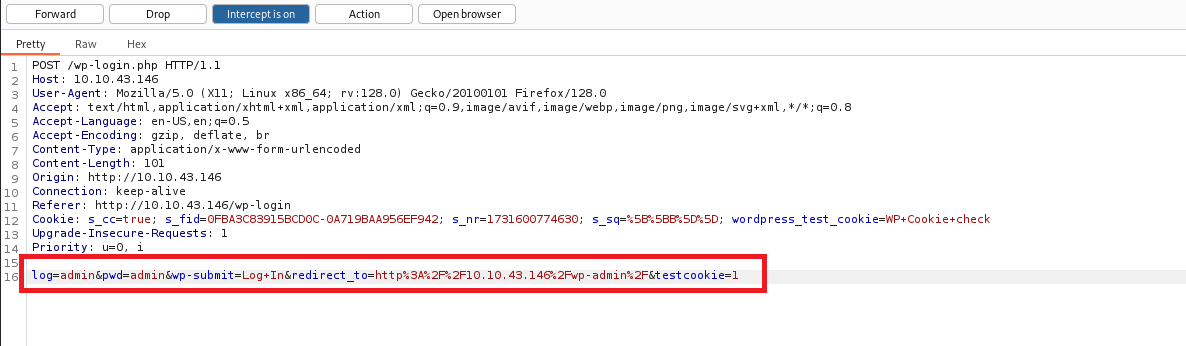


Đăng nhập username và password ngẫu nhiên trên trình duyệt Burp.



Bây giờ hãy nhìn vào Burp, có thứ gì đó trông giống như sau

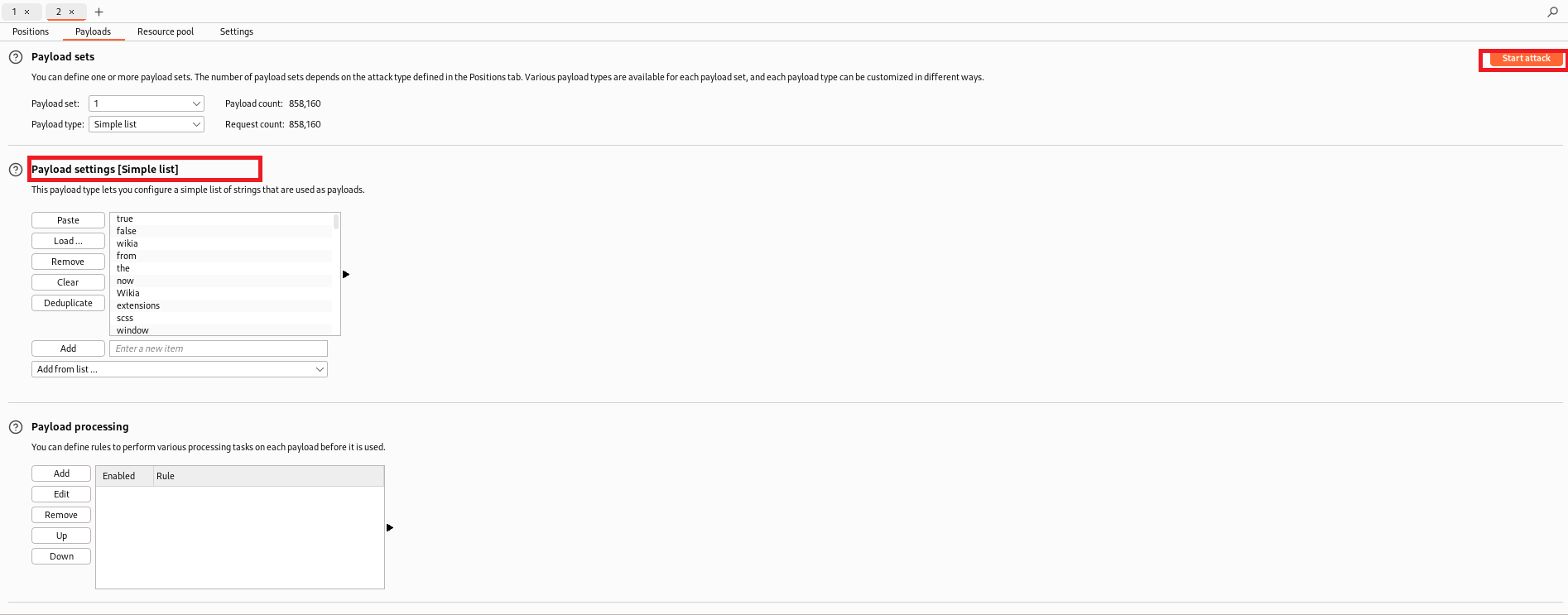
Yêu cầu POST mà chúng ta thực hiện trên trang web sẽ đến được đích bằng đường dẫn proxy đó.



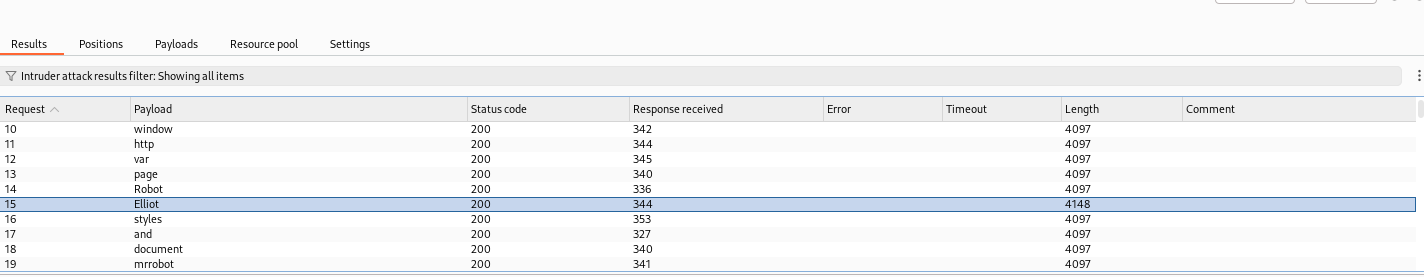
Từ tùy chọn, gửi cái này vào intruder. Ở đây, clear dấu đánh dấu payload trên tất cả và thêm dấu đánh dấu payload lên tên người dùng mà bạn đã nhập để chúng ta có thể áp dụng payload vào username



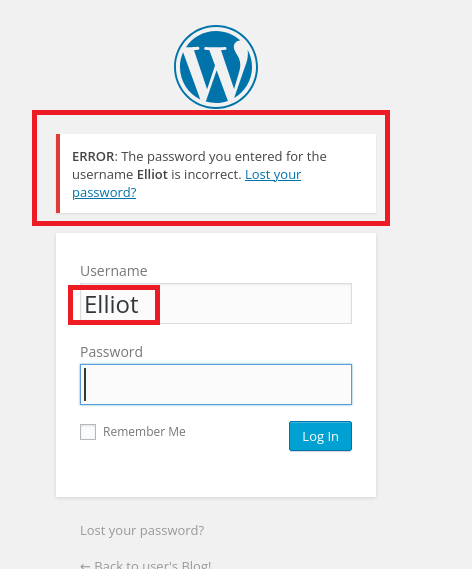
Bây giờ trong payload option hay payload setting(đối với burpsuite pro) dán tất cả các từ tìm thấy trong fsociety.dic và bắt đầu tấn công



Bây giờ, một cửa sổ attacking được mở. Hãy nhìn thật kỹ độ dài của từng gói response. Nếu có một độ dài gói response khác với tất cả gói còn lại thì rất có thể đó là username mà chúng ta cần.



Ở đây,ta tìm thấy username là Elliot. Bây giờ hãy quay lại trình duyệt mặc định, nơi trang web được mở, hãy thử đăng nhập bằng tên người dùng Elliot và mật khẩu ngẫu nhiên. Xem phản hồi, nó hiển thị phản hồi khác với trước đó, điều đó xác nhận rằng tên người dùng là chính xác.



Bây giờ đến lượt tìm mật khẩu đúng. Có thể sử dụng cùng quy trình tìm tên người dùng để tìm mật khẩu. Nhưng có một tùy chọn khác có thể tiết kiệm thời gian.

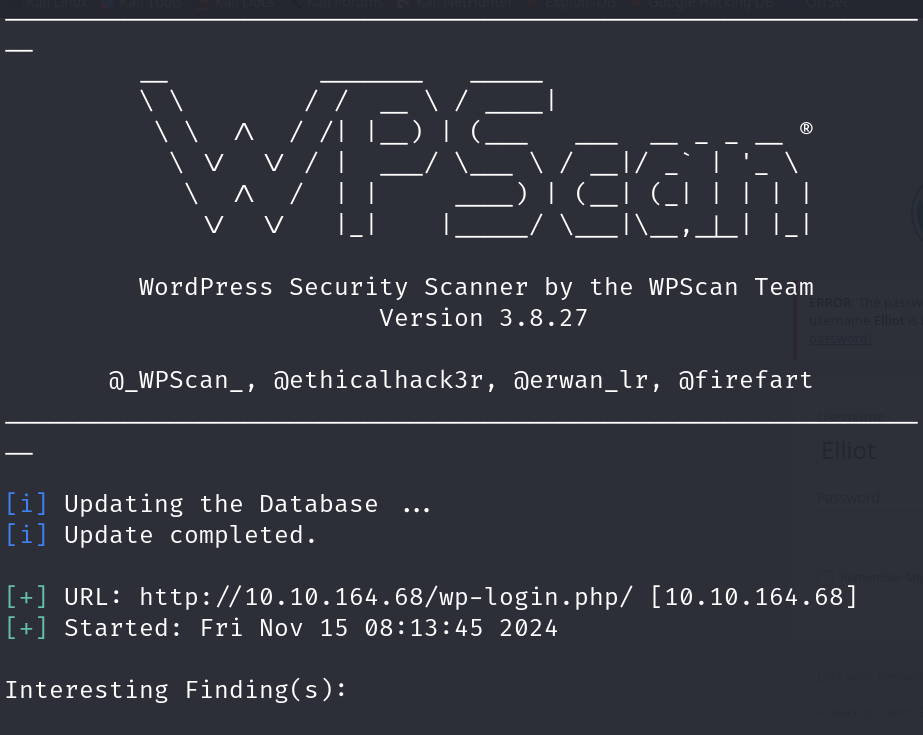
Có một công cụ gọi là Wpscan, rất hữu ích ở đây. Sử dụng nó và áp dụng fsociety.dic làm danh sách mật khẩu thay vì danh sách mật khẩu khác có thể được áp dụng.

$ wpscan --url http://10.10.164.68/wp-login.php -U Elliot -P fsociety.dic

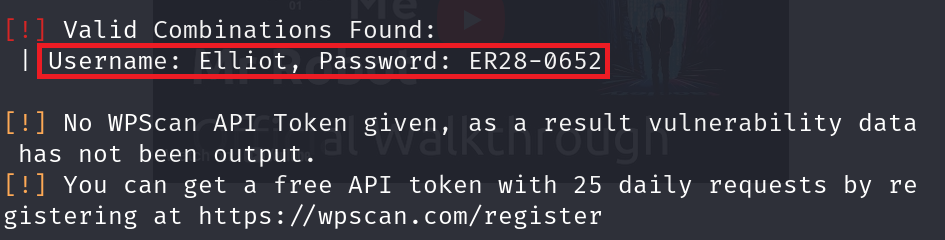
Ở đây,

* url: url của mục tiêu
* U: tên người dùng hoặc danh sách người dùng
* P: danh sách mật khẩu

Quá trình quét trông giống như sau:

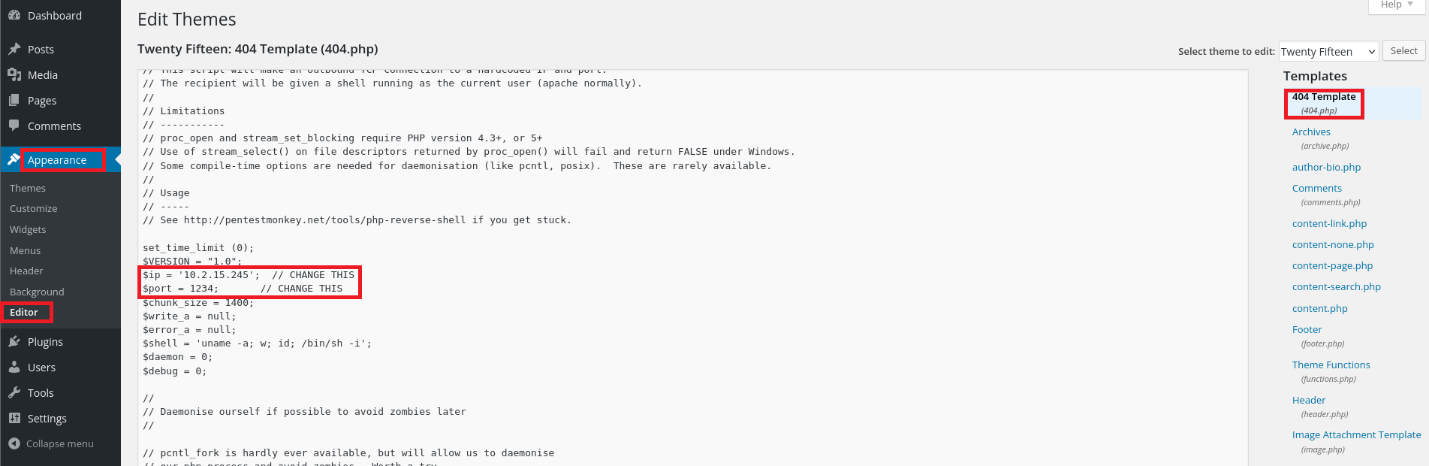


Cuối cùng chúng ta đã tìm ra mật khẩu đăng nhập



Bây giờ, hãy đăng nhập vào bảng điều khiển của trang web. Để truy cập shell, chúng ta phải khởi chạy php reverse shell. Mã cho việc đó có thể được sử dụng từ: <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>

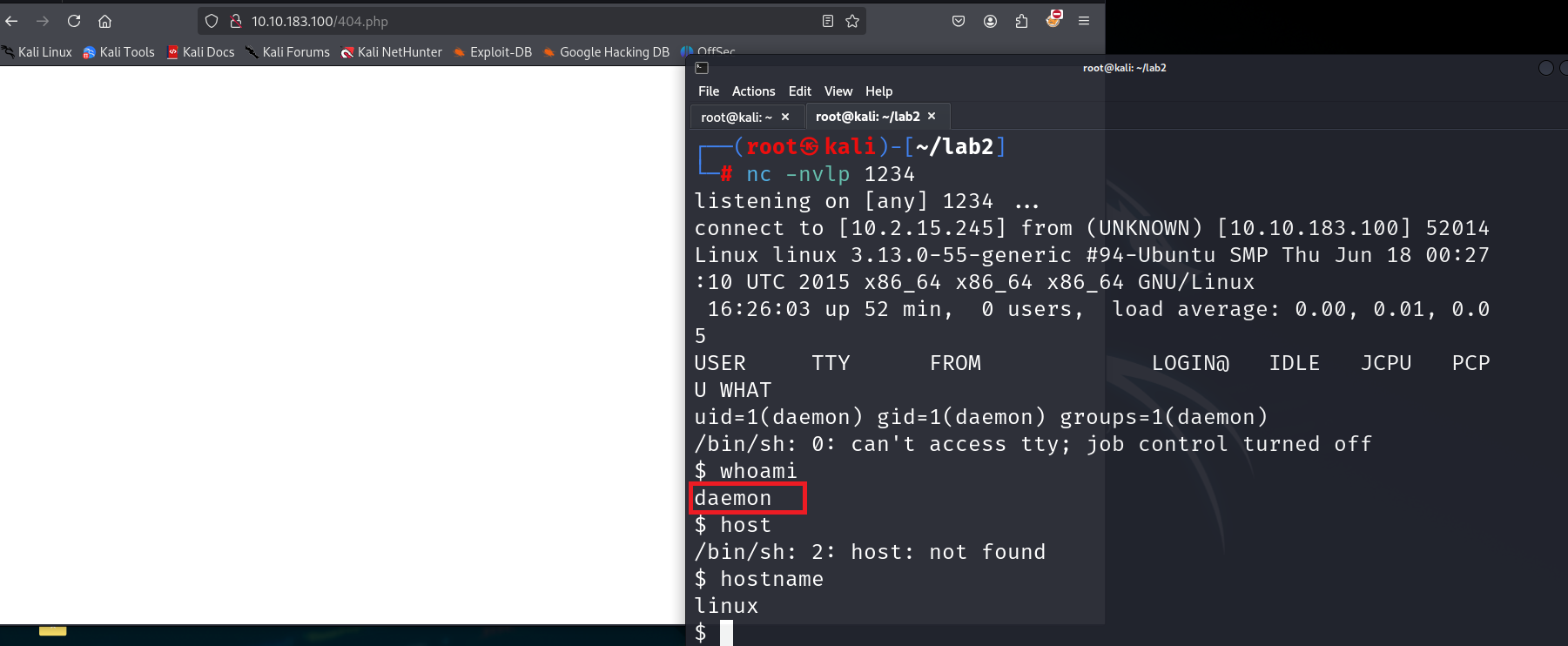
Trong editor, nhấn vào mẫu 404 và dán tất cả mã vào đó



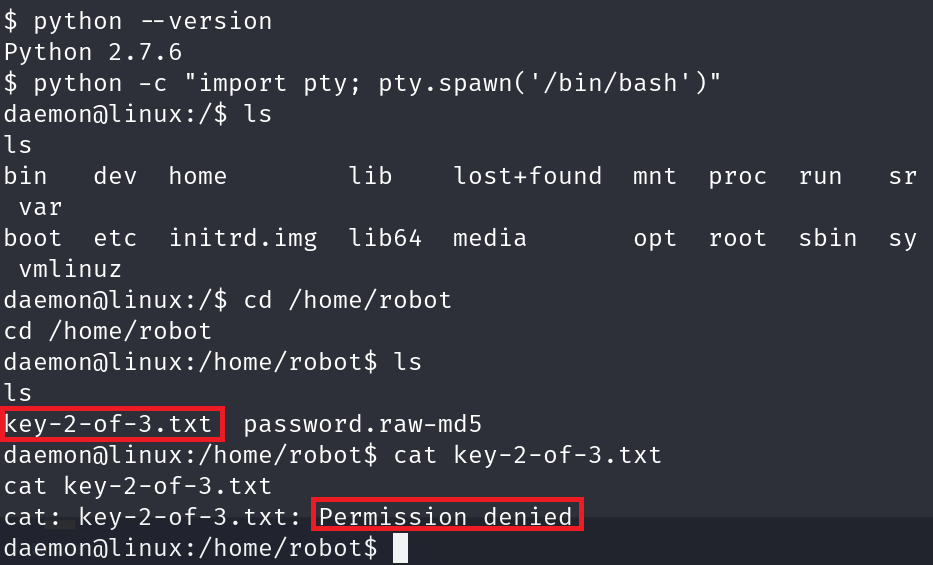
Sau khi lưu, mã độc được thực thi khi chúng ta truy cập trang 404.php. Ngoài ra, chúng ta phải thiết lập trình nghe trong máy chủ hoặc máy riêng. Có hai trường ip và port trong mã, chúng ta phải thay đổi sao cho ip phải là ip của máy nghe và port là số cổng được máy đó sử dụng cho mục đích nghe. Thiết lập trình nghe



Sau khi truy cập 404.php trong trang web đó, mã ngay lập tức được thực thi và chúng ta có được shell.



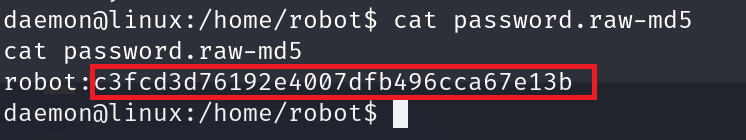
Chúng ta là người dùng daemon trong máy đó. Đối với interactive terminal , chúng ta có thể sử dụng, vì python được cài đặt ở đó



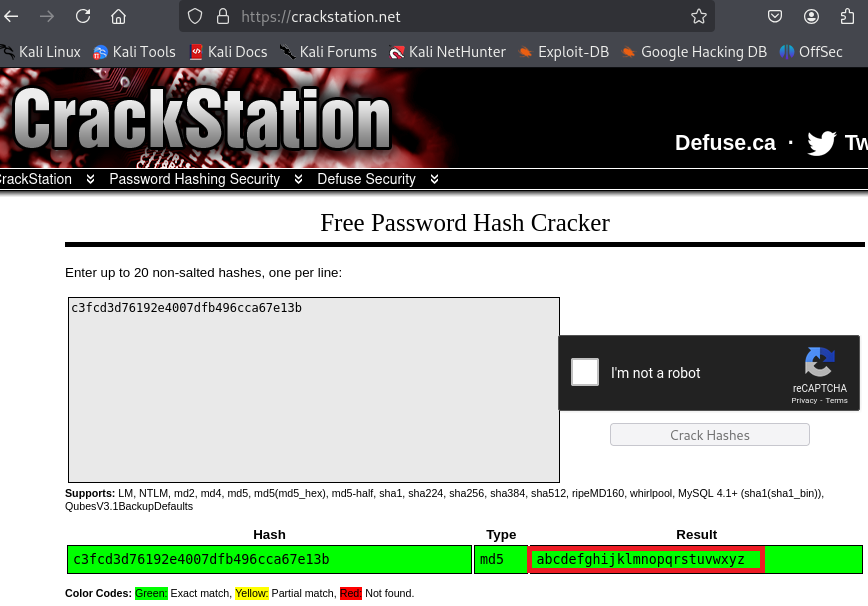
Có một lá cờ khác trong thư mục robot nhưng chúng ta không có quyền truy cập vào nó.

1. **Password Cracking**

Ngoài ra còn có một tệp có hash md5 của mật khẩu của người dùng robot. Bây giờ chúng ta phải bẻ khóa băm đó để trở thành robot. May mắn thay, chúng ta có thể xem băm,

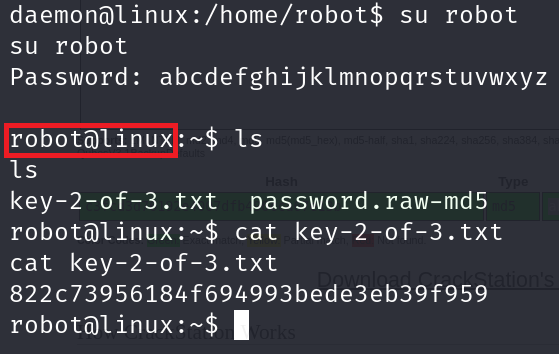


Bạn có thể sử dụng JohnTheRipper, Hashcat hoặc các công cụ trực tuyến để phá mật khẩu. Tôi sử dụng công cụ trực tuyến và tìm ra mật khẩu.

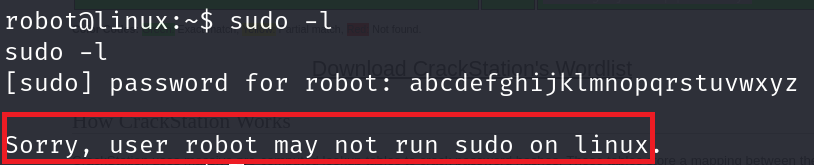


## **Privilege Escalation (Leo thang đặc quyền)**

Bây giờ, sử dụng tên người dùng robot và mật khẩu đó để chuyển sang người dùng robot. Bây giờ chúng ta có lá cờ thứ hai trong số 3 lá cờ.

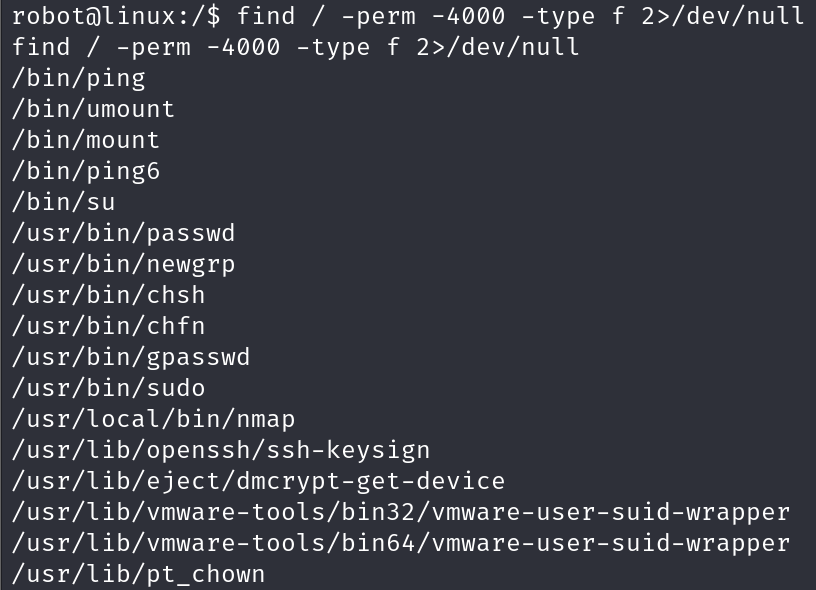


Robot không có quyền chạy lệnh sudo



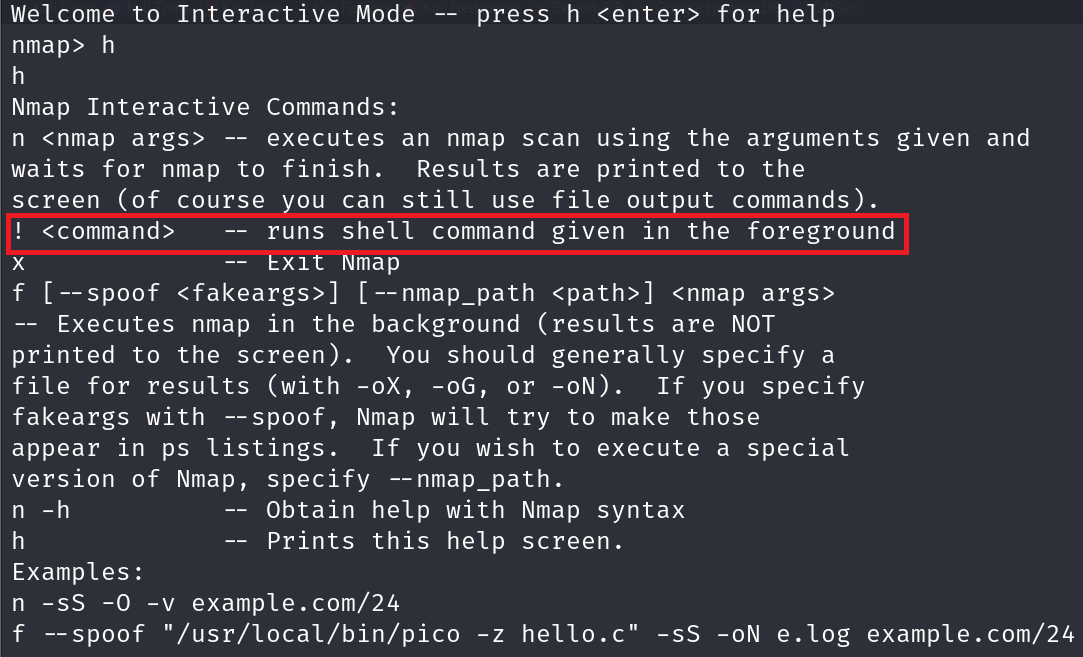
Vì vậy, một lần nữa chúng ta phải tăng đặc quyền để tìm cờ cuối cùng, nằm trong thư mục /root. Vì vậy, chúng ta phải là root. Có một tập lệnh có tên là LinEnum.sh, nó hữu ích cho việc Privilege Escalation để tìm chương trình dễ bị tấn công. Ở đây, ta thiết lập máy chủ trong máy của mình bằng python và sử dụng lệnh curl để truy cập nó từ shell mục tiêu và chạy nó.

Sau một thời gian khám phá hệ thống, tôi tìm thấy một tệp nhị phân thú vị với tập hợp bit SUID:

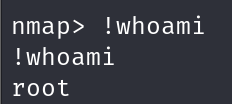


Vâng, đó chính là NMap! Một phiên bản cũ (3.81) của nó, chính xác là như vậy. Thú vị là, tệp thực thi này thuộc sở hữu của root. Vì bit SUID của nó được thiết lập, điều đó có nghĩa là về mặt lý thuyết, nmap có thể thực thi các lệnh dưới dạng root nếu chúng ta quản lý để nó chạy chúng cho chúng ta.

Khi xem kết quả đầu ra của nmap –help, chúng ta thấy rằng nmap có tùy chọn –interactive đưa ra một số loại REPL



Thật tuyệt, hóa ra nmap có thể chạy lệnh shell cho chúng ta!



Do đó, chúng ta có thể yêu cầu nó tạo ra một root shell và lấy cờ cuối cùng nằm trong /root.

