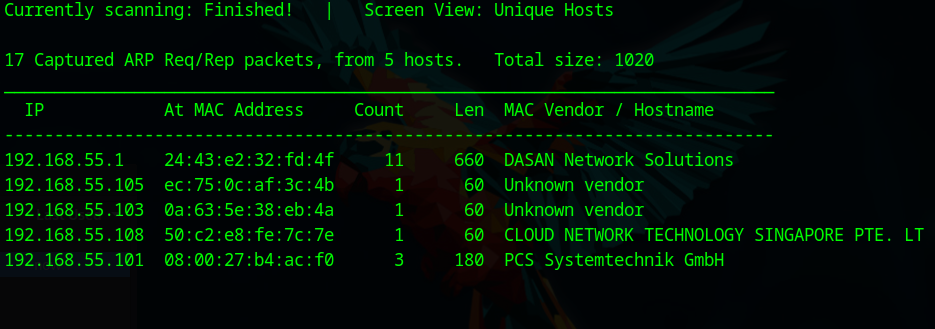
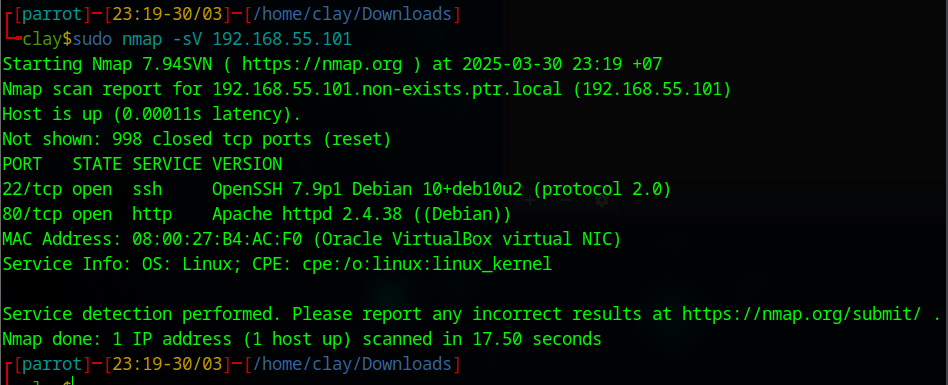
B1:



Netdiscover –r địa chỉ ip để tìm thấy địa chỉ của máy tấn công là.101

B2:

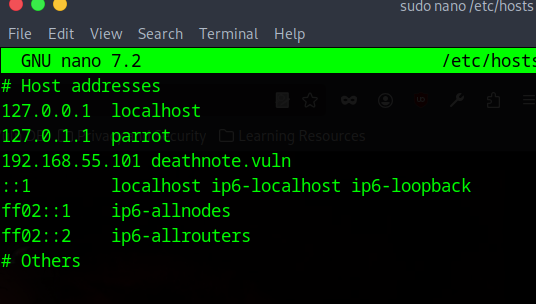
Dùng smap –sV để xem các dịch vụ đang chạy



Ở đây có cổng 80 nên truy cập web browser vào

B3: truy cập website

Trước tiên cần sửa lại file /etc/host bằng thêm địa chỉ ip và tên miền vào thì mới truy cập được

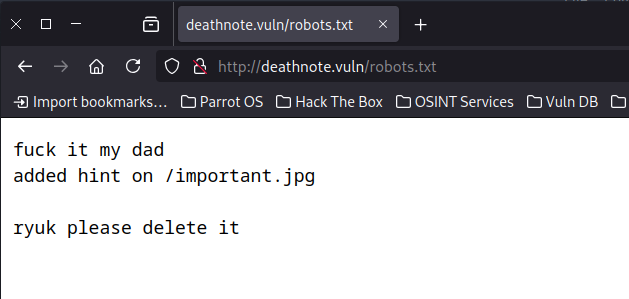


B4: Xem 1 vòng quanh page



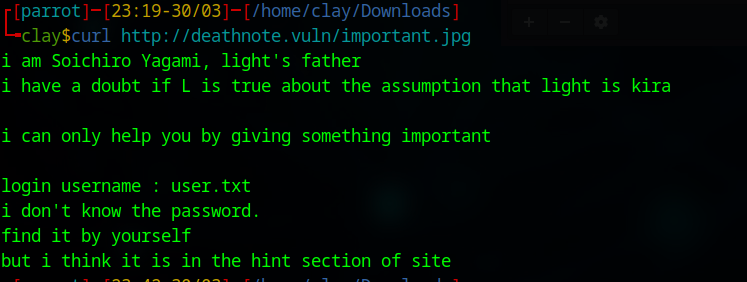
Thông tin đầu tiên

Thử tìm trong file robots.txt (robots.txt là một tệp văn bản được đặt trong thư mục gốc của một trang web để hướng dẫn các công cụ tìm kiếm (search engine bots) như Googlebot, Bingbot)



-> có thông báo sẽ có 1 hint ở ảnh nào đó, giờ sẽ curl nó về và phân tích

B5: Curl ảnh về phân tích



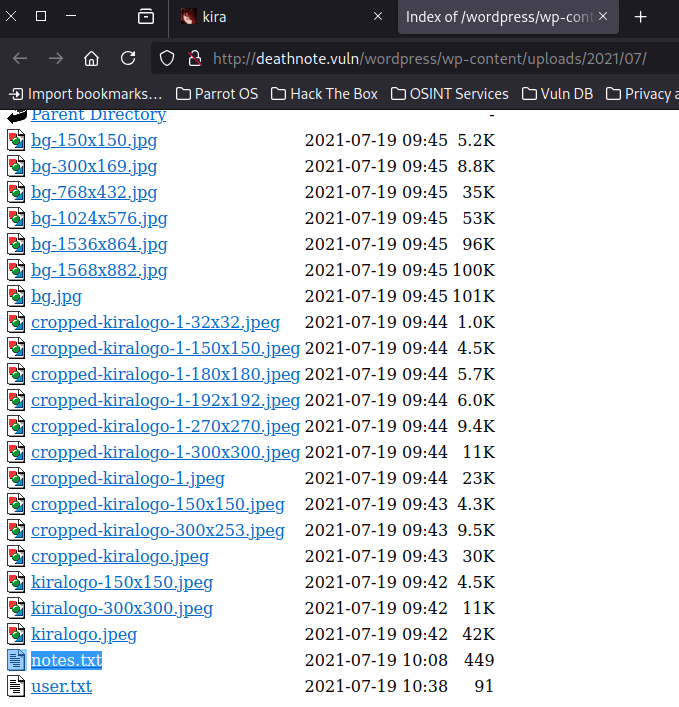
-> ta đã có thông tin là username sẽ có thể nằm trong file user.txt, giờ ta lấy file đó về

B6: curl trang wordpress về

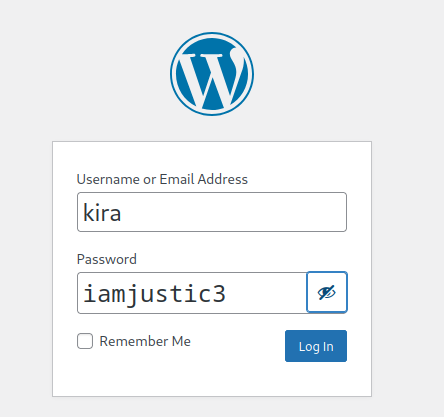
Ta nhận thấp wp có 1 đường dẫn có thể tận dụng



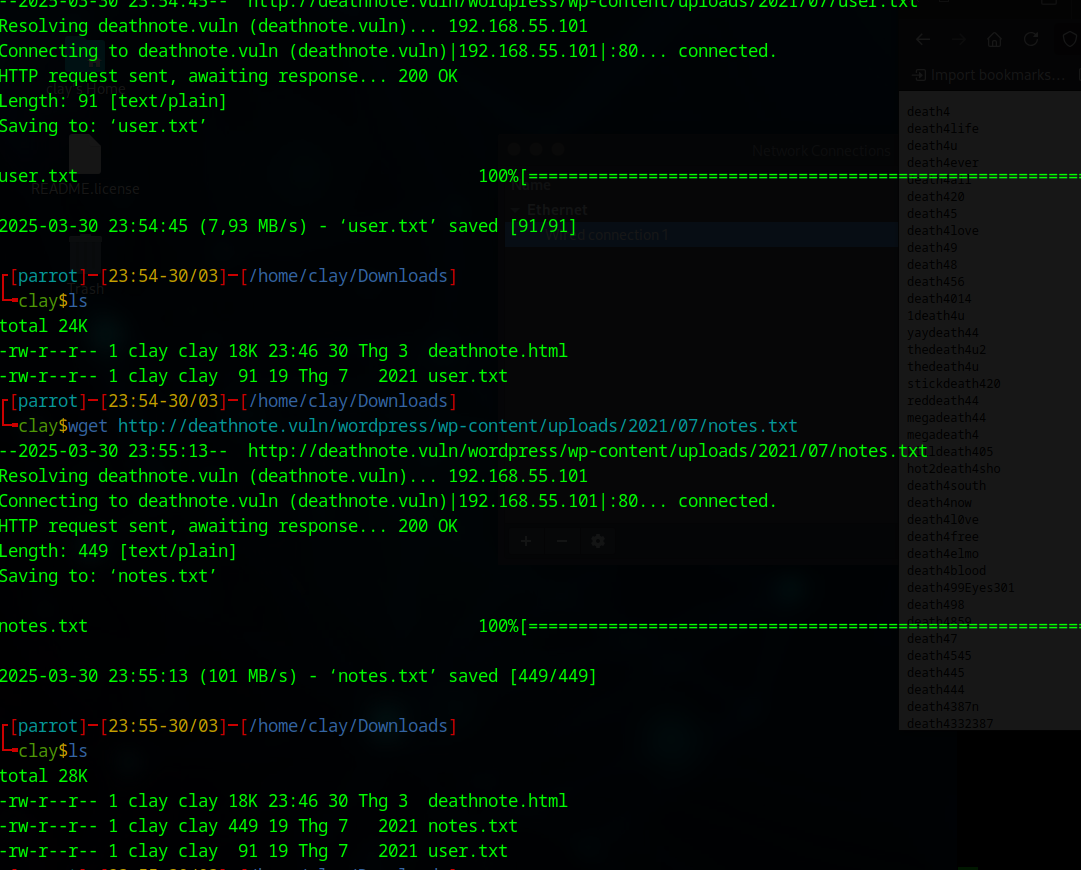
Sau khi truy cập vào 2 trang đó ta thấy được có 2 file cần tìm



Cách 2: từ những thông tin của trang hint, ta đăng nhập vào wp-admin và có thông tin admin là kira và mk là iamjustic3

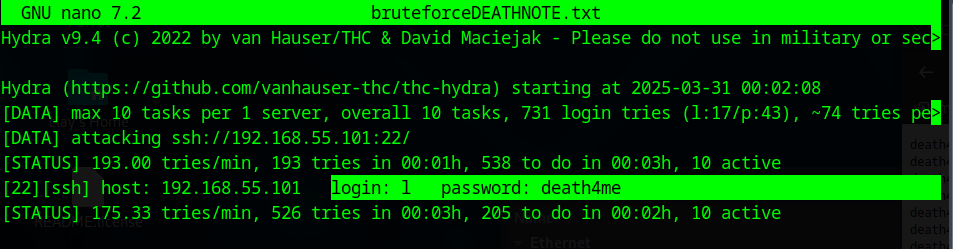


B7: ta thực hiện tải 2 file về -> tk và mk để tấn công bruteforce

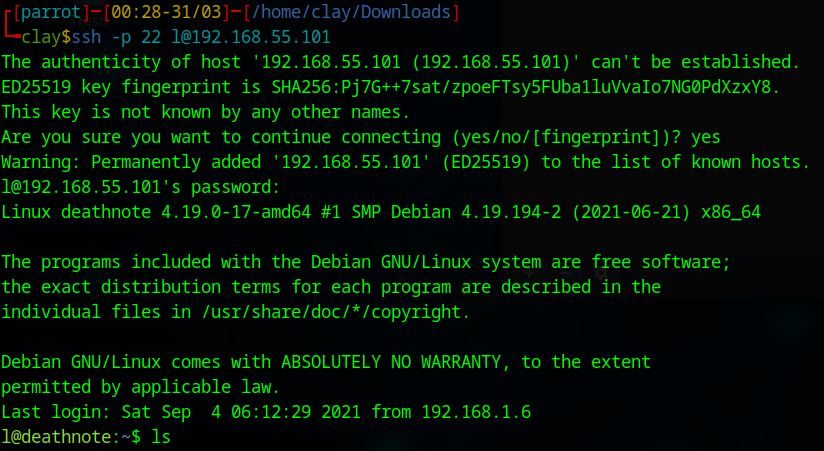


Sử dụng hydra hoặc medusa

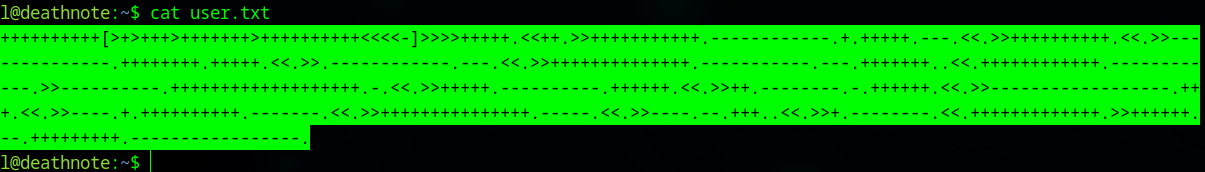
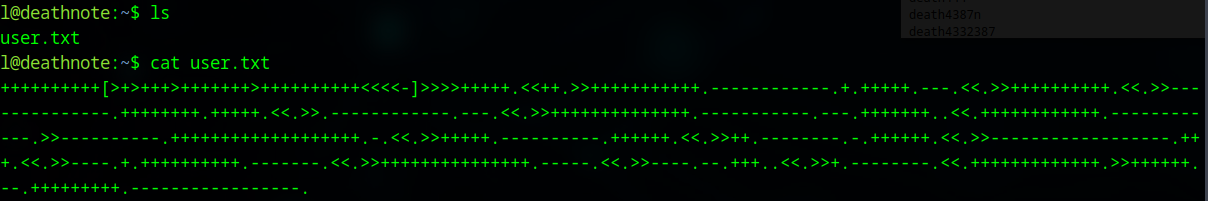
Ta đã thấy dc tk là l và mk là death4me



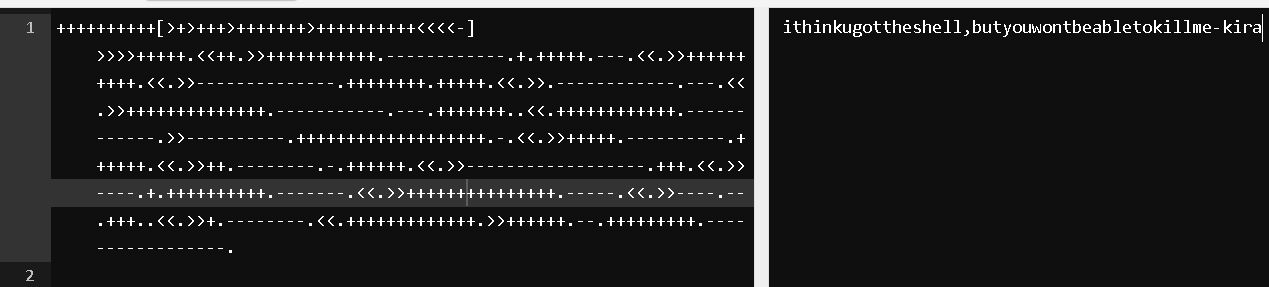
B6: đăng nhập vào qua ssh



Ta xem qua file user.txt )(đây là ngôn ngữ brain fuck :))))

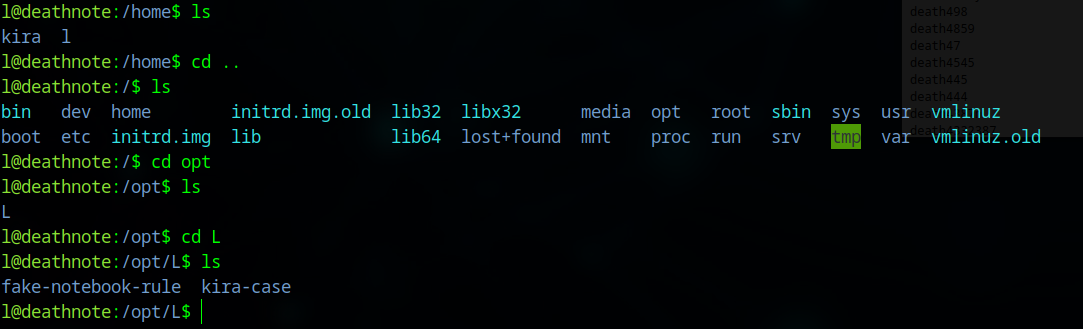


Decode ta được lời nhắn

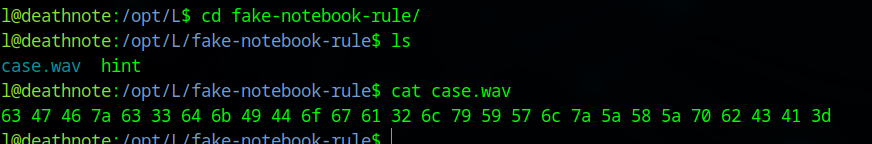


-> k có gì dbiet

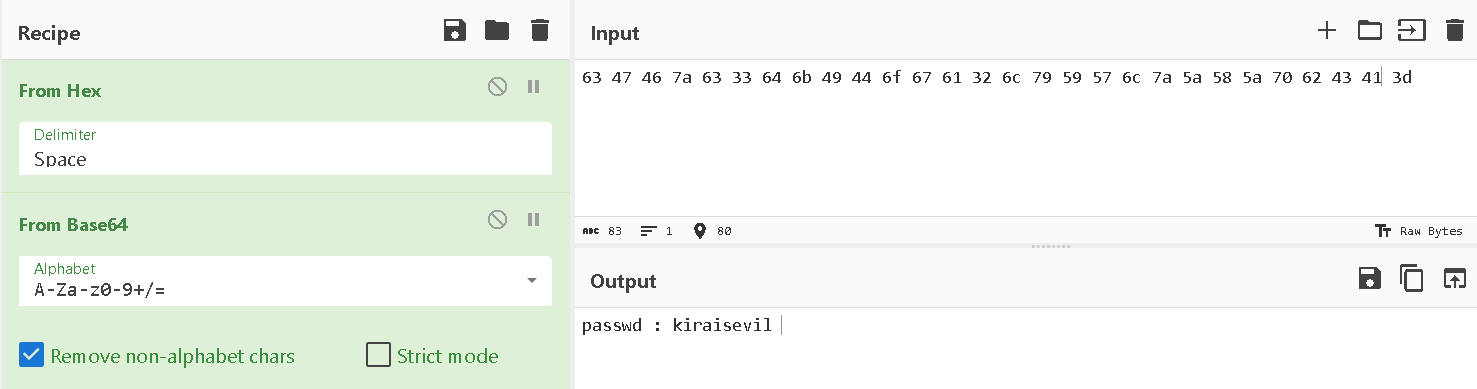
B7: ta thực hiện tìm trong directory



Trong file fake notebook ta thấy có được file hexa như sau

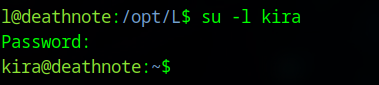


Dùng cyberchef ta giải mã ra được

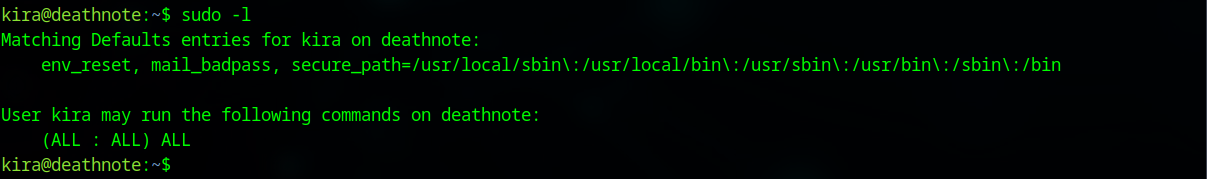


Mật khẩu là kiraisevil

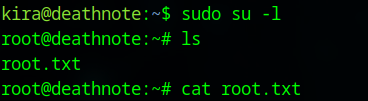
Từ 2 thông tin đó ta đăng nhập vào dc tài khoản kira



Ta nhận thấy tài khoản kira có tất cả các quyền và có thể lên được root -> k cần leo thang đặc quyền



Ta thấy có file root.txt



Thành công

