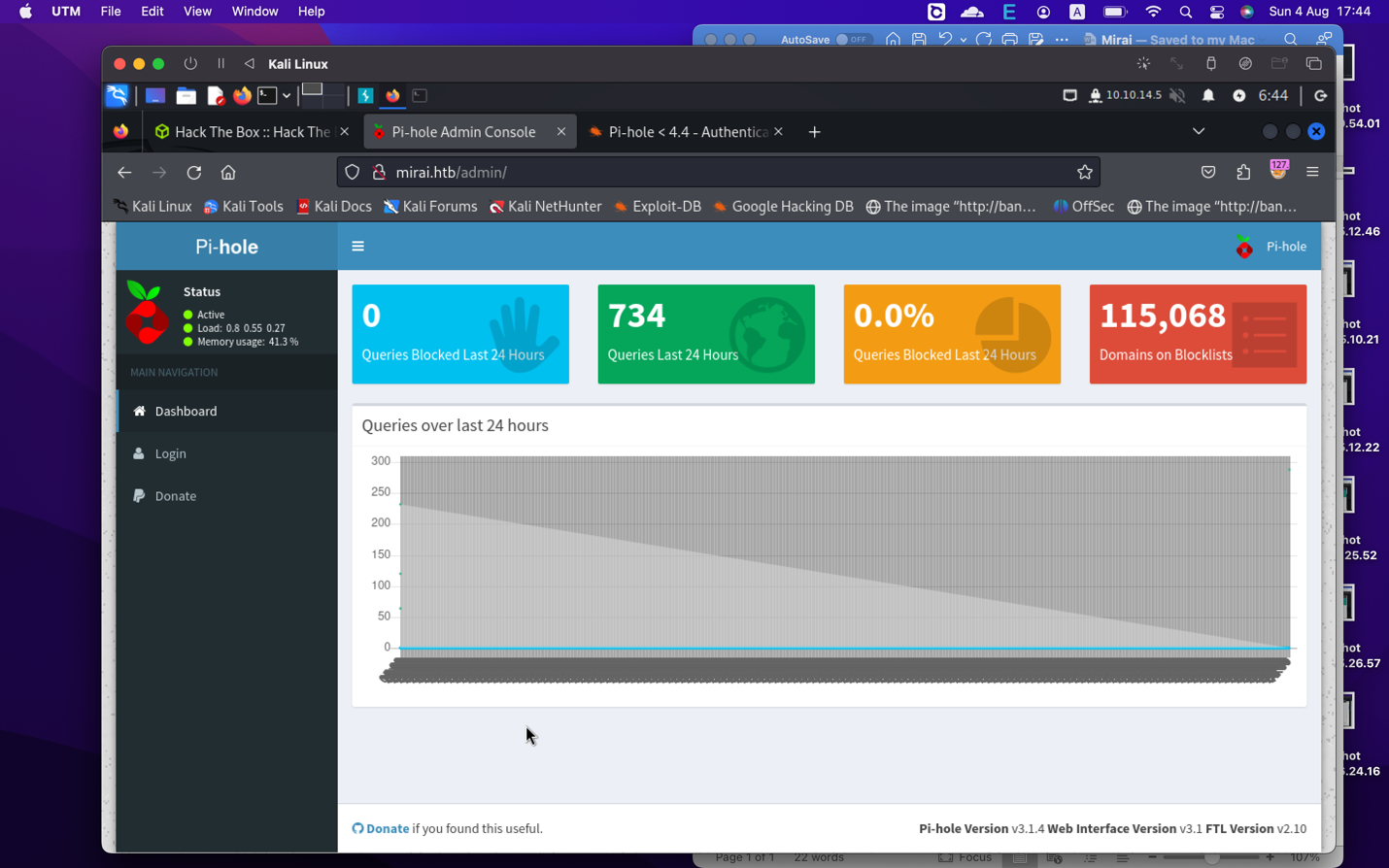


Mình sẽ đi brute force thư mục bị ẩn, tìm được điểm vào admin:

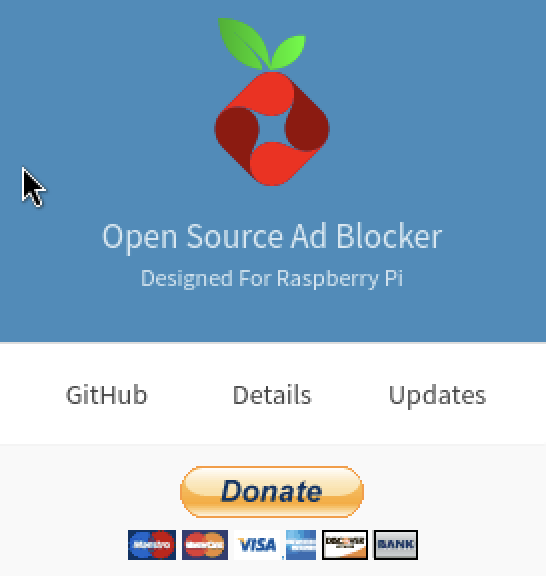
ffuf -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -u http://mirai.htb/FUZZ -c -fw 400

http://mirai.htb/admin/

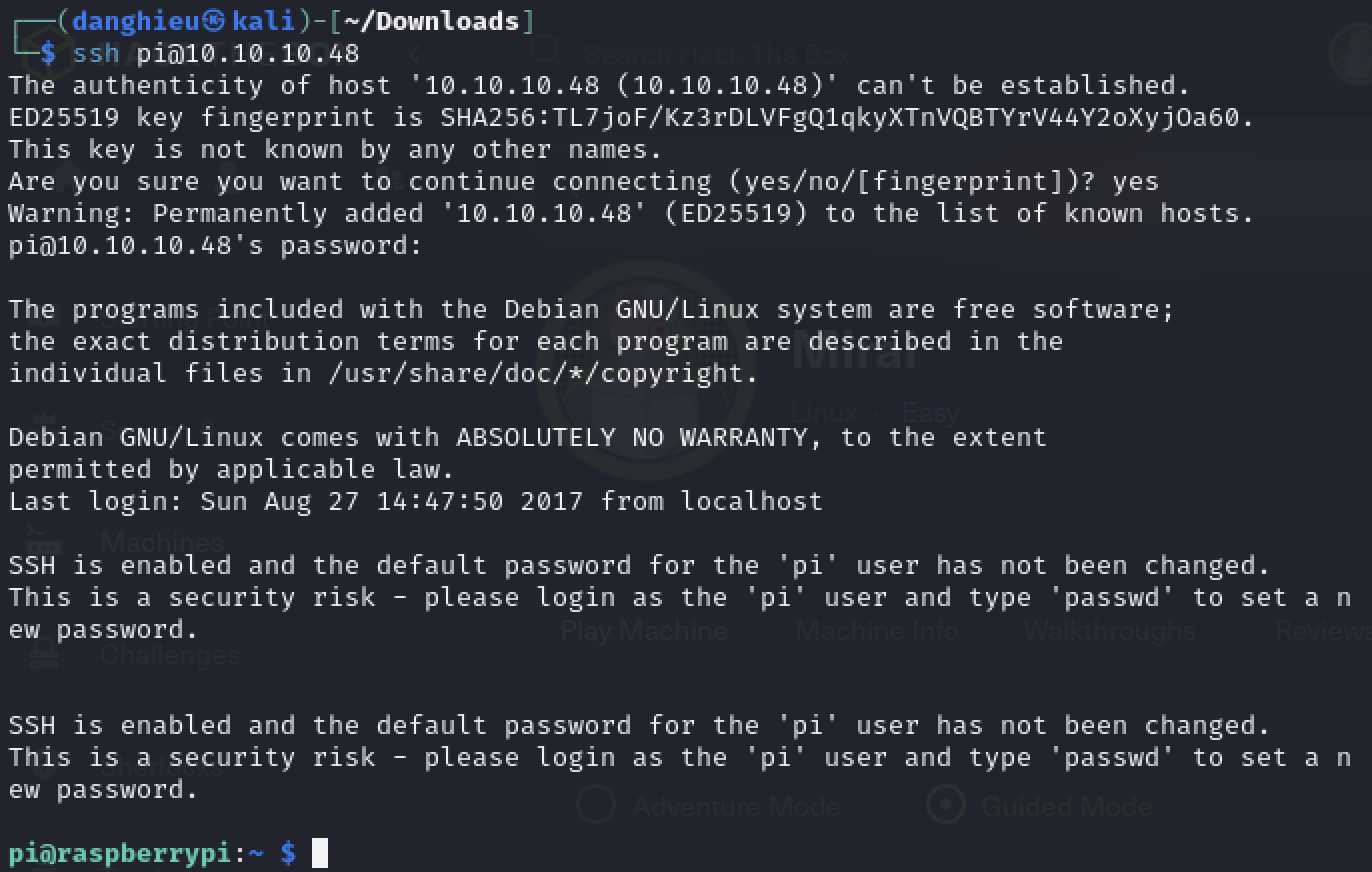


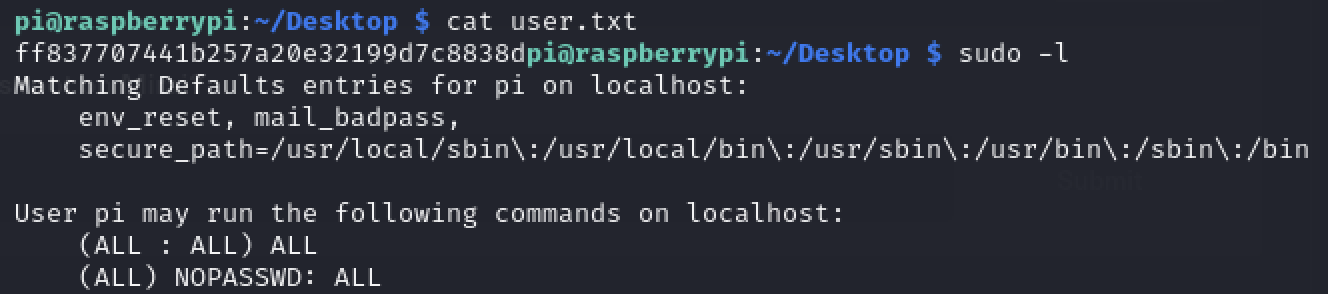
Mới là giao diện trang chủ thôi, mình cần phải tìm thông tin đăng nhập của admin

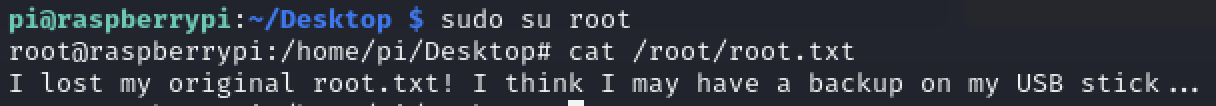
Máy chủ đang chạy dịch vụ web là Raspberry Pi

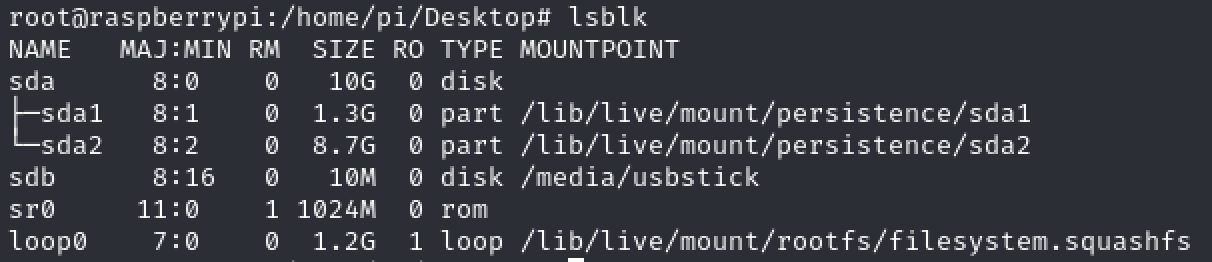


Tài khoản mặc định của Raspberry Pi là pi:raspberry



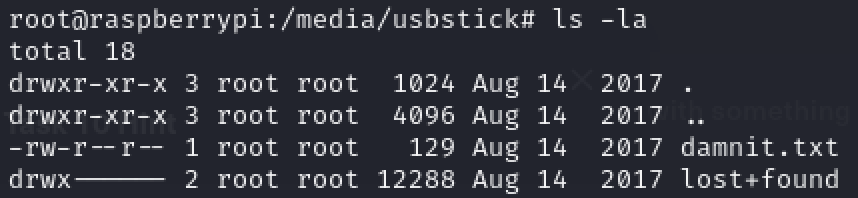


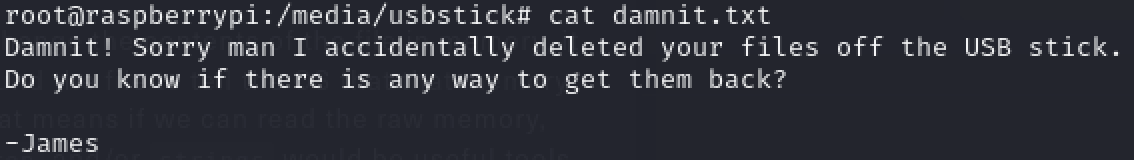




Thư mục /media/usbstick đang mount đến /dev/sdb

Thư mục gốc của USB media là /dev/sdb





Các tập tin đã bị xóa khỏi USB stick, mình phải tìm cách khôi phục

Lệnh strings sẽ lập tức tiết lộ flag nếu chạy trên /dev/sdb:

