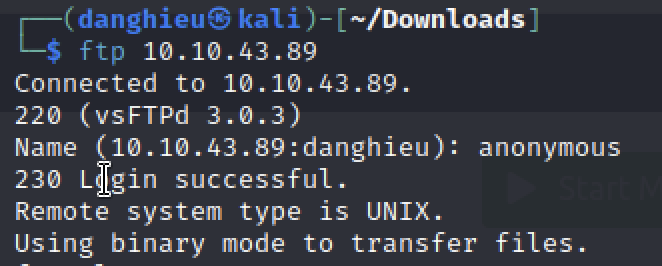


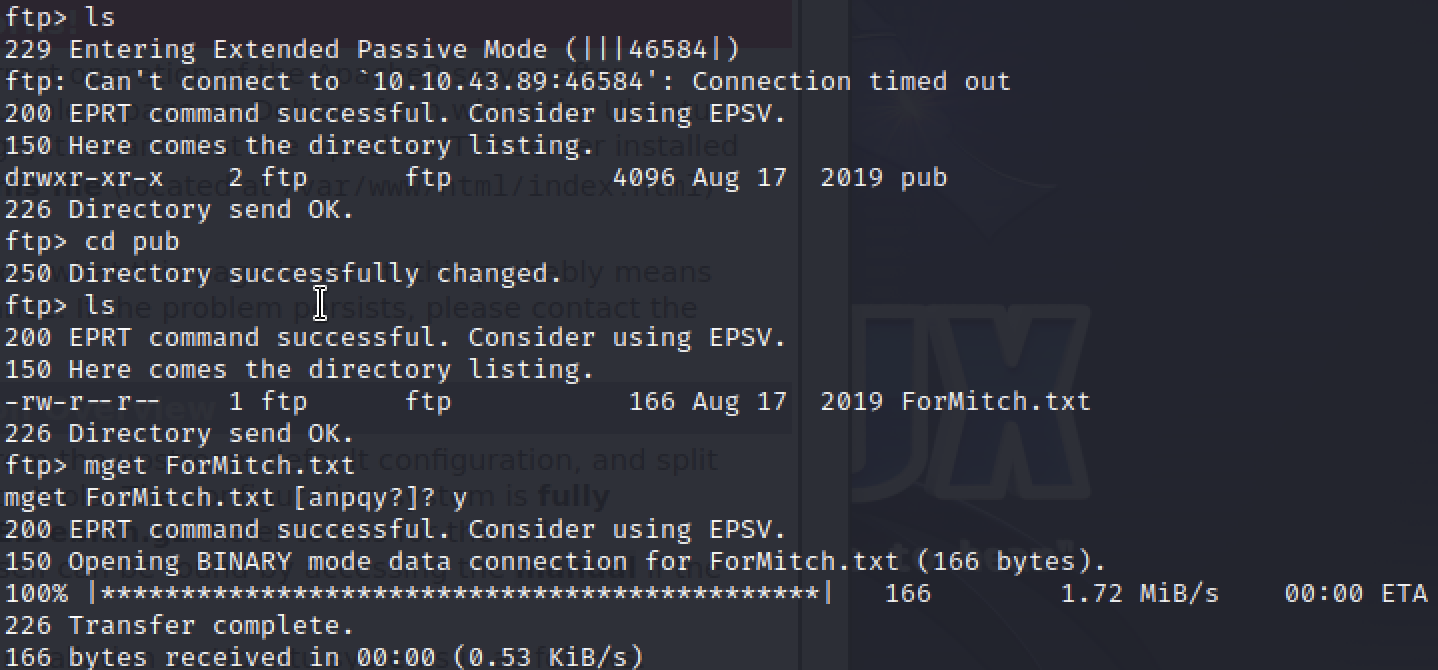
Có 2 cổng dưới 1000 đang mở: ftp(21) và http(80) ; 1 cổng trên 1000: ssh (2222)

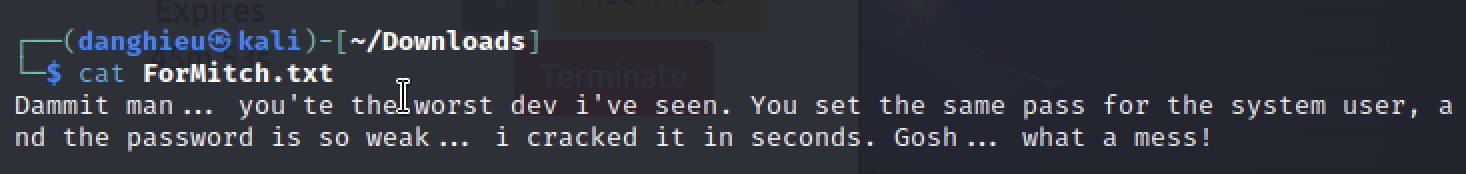
Truy cập vào dịch vụ ftp (được phép đăng nhập anonymous):

ftp 10.10.43.89

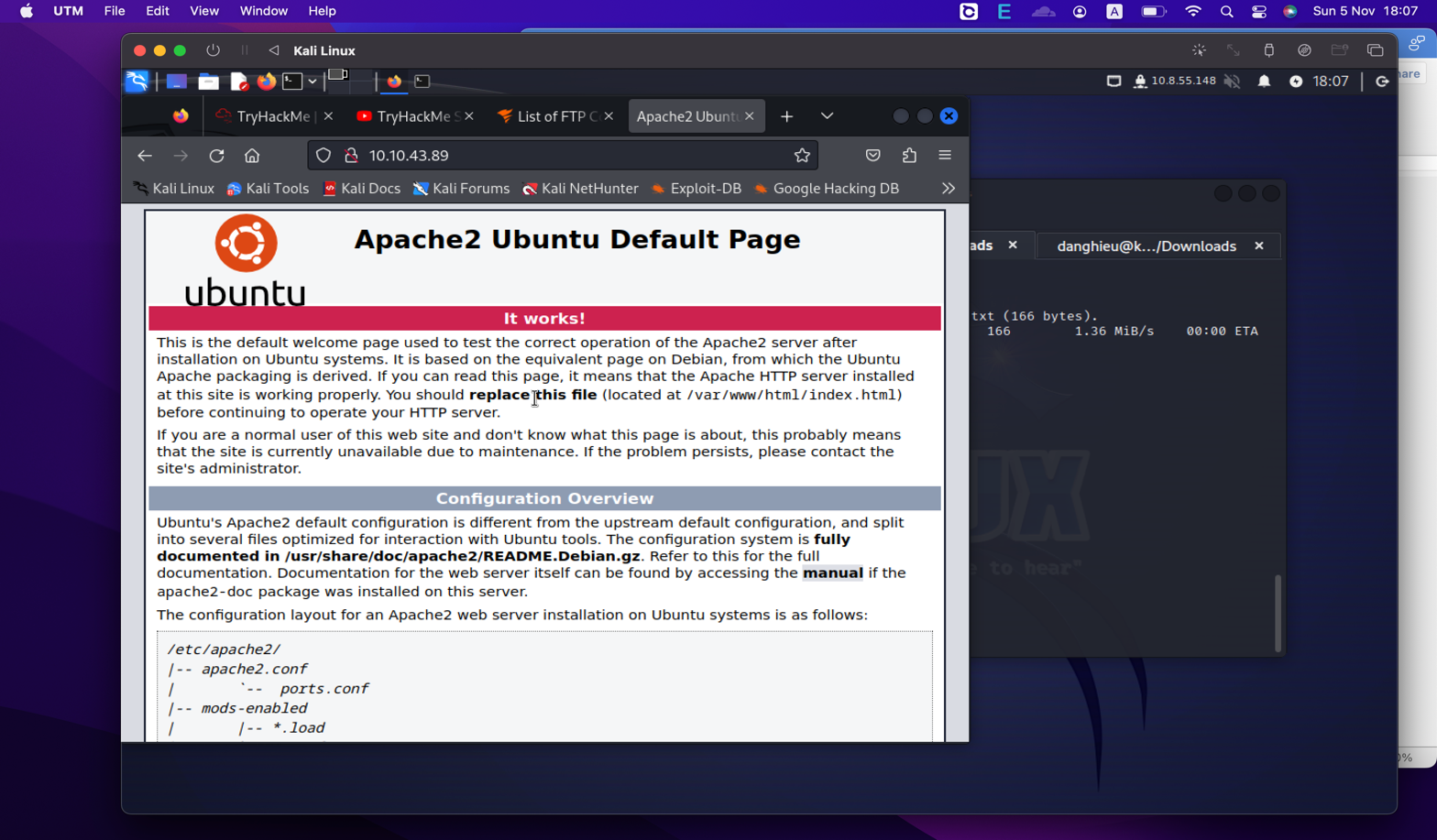


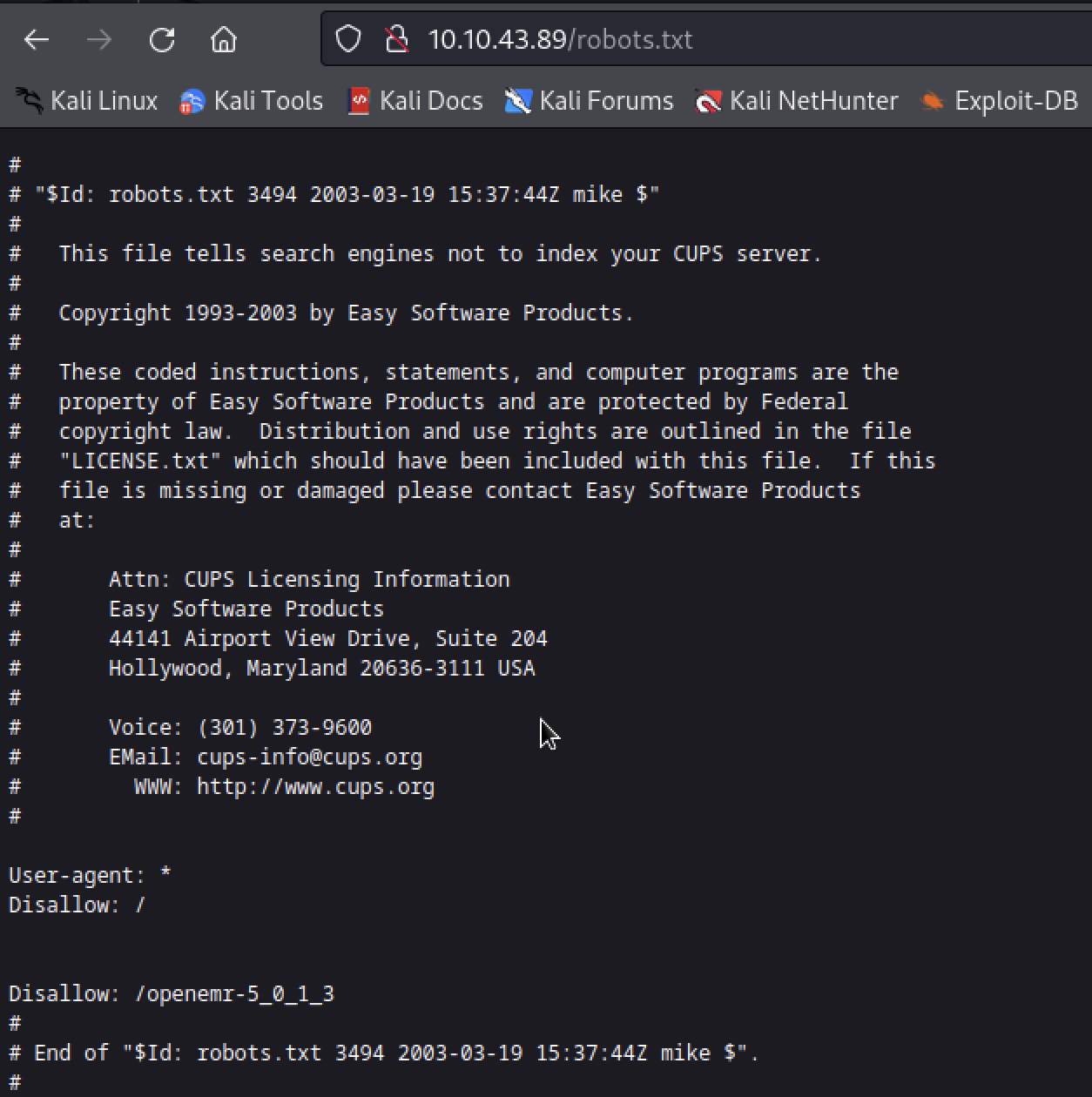
Xem thử ftp có file gì quan trọng không:



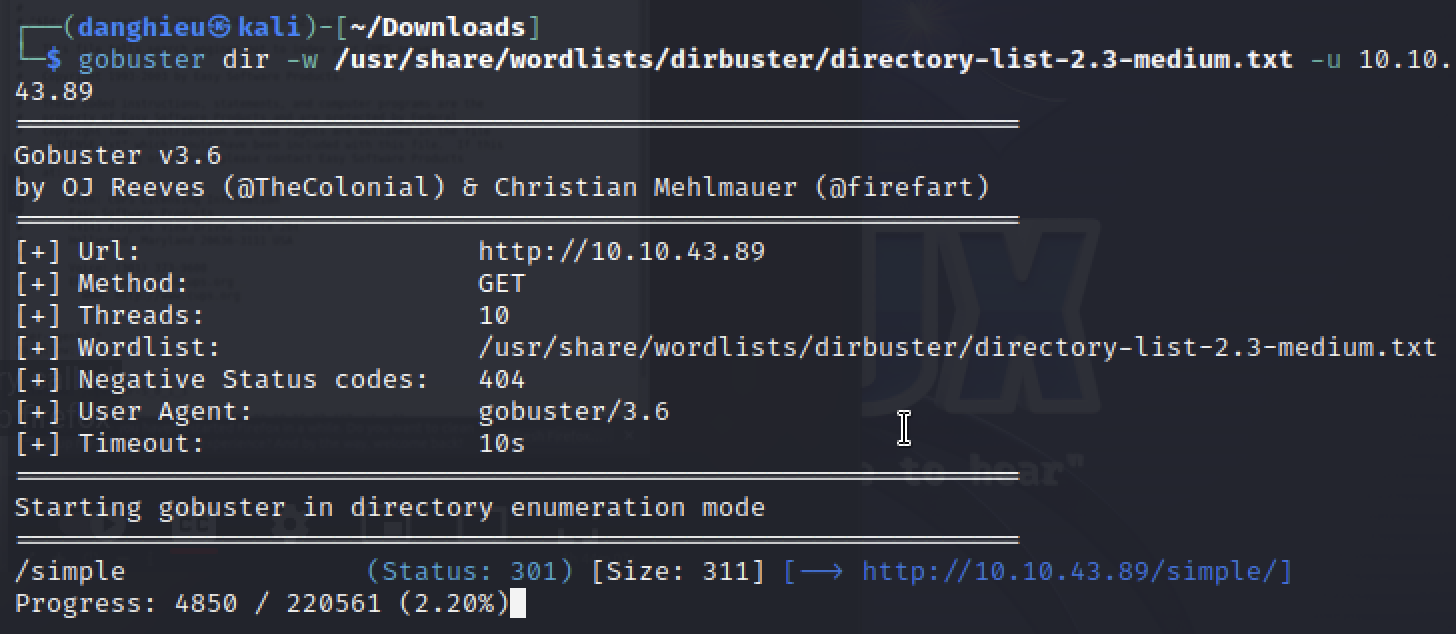


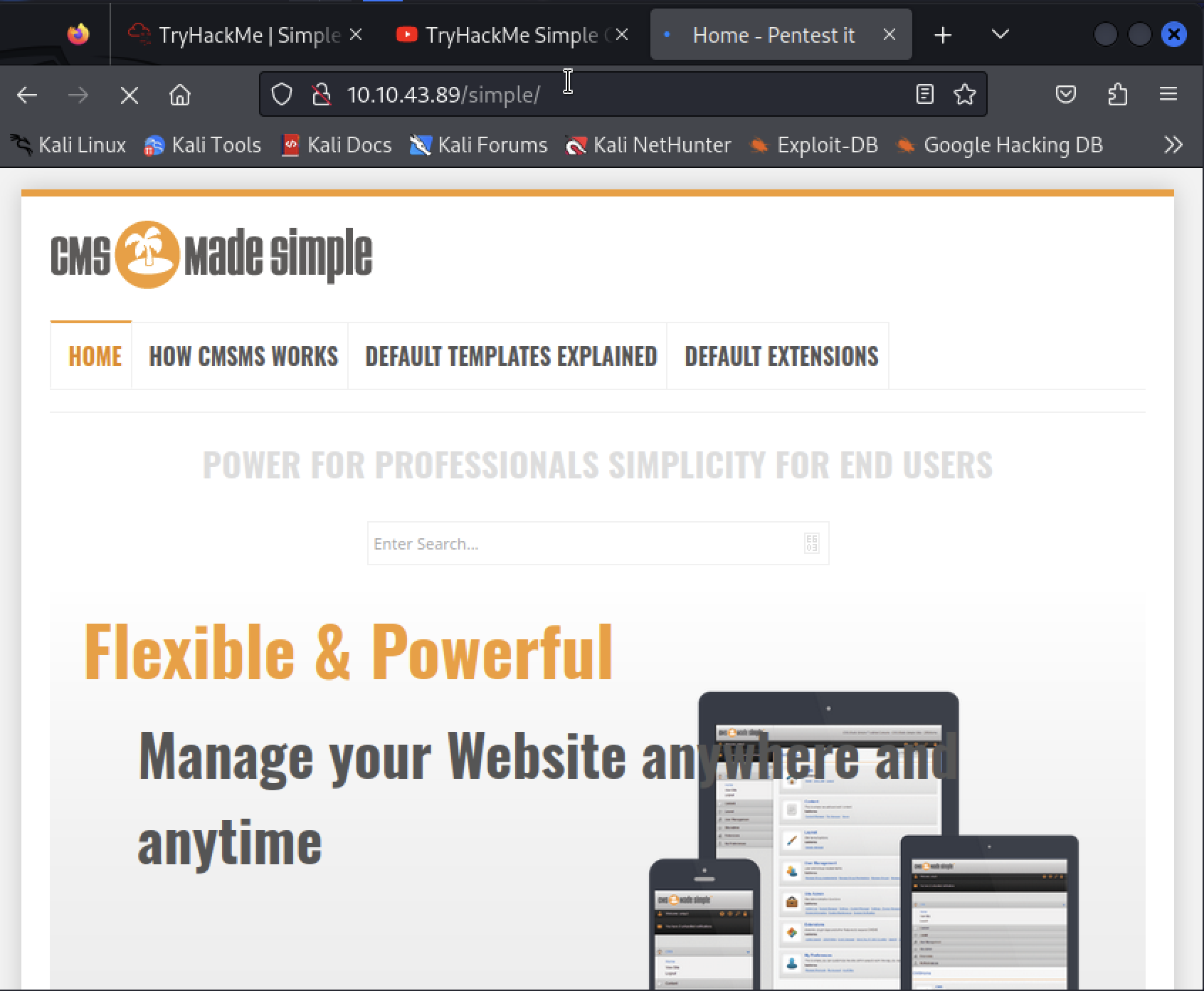
Không có ý nghĩa gì cả

Xem máy chủ web hoạt động ra sao:



Quét xem có thư mục nào bị ẩn không:





Phiên bản CMS của trang web:

This site is powered by CMS Made Simple version 2.2.8



Bạn sẽ tìm thấy CVE cho thư viện ứng dụng đang dùng.

Chạy thử script:

python2 46635.py -u http:// 10.10.43.89/simple



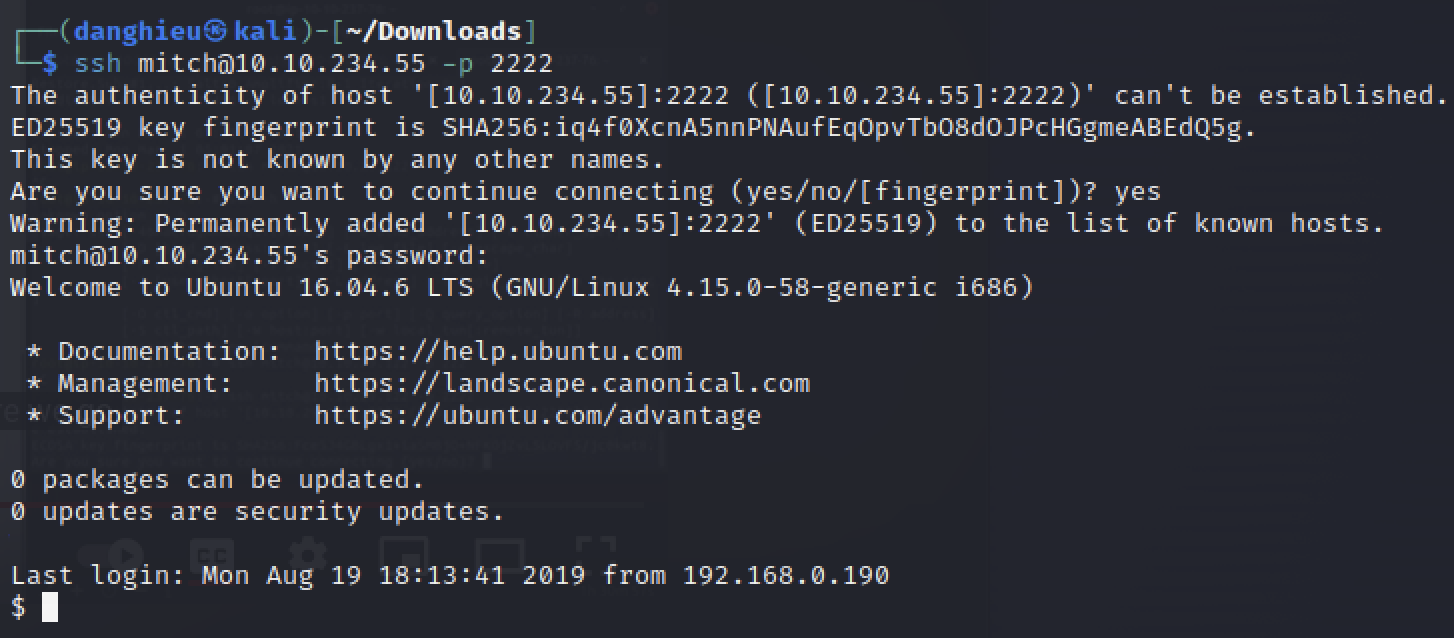
Chạy script không được tối ưu lắm ☺

Mình phải chạy liên tục để tìm được ông admin. Lâu vcl. Làm sao để nhận biết ông admin? Bạn dựa vào cái file mình đọc trên ftp ah.

Mình dùng hashcat để recovery password:

hashcat -a 0 -m 20 pass:salt /usr/share/wordlists/rockyou.txt

ssh đến máy chủ bằng username: password mới tìm được



Bạn sẽ leo thang đặc quyền bằng lệnh sudo -l:

