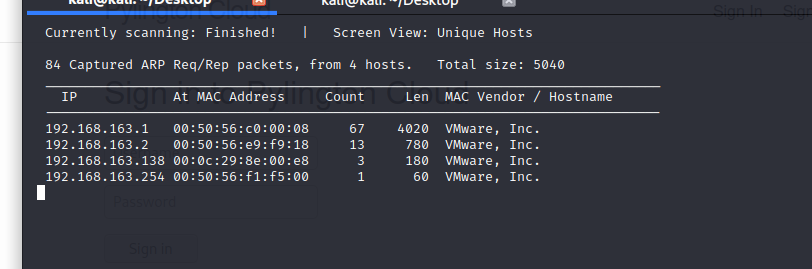
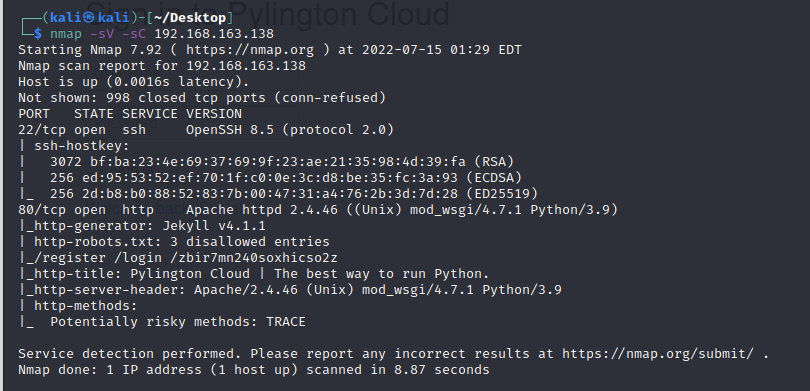
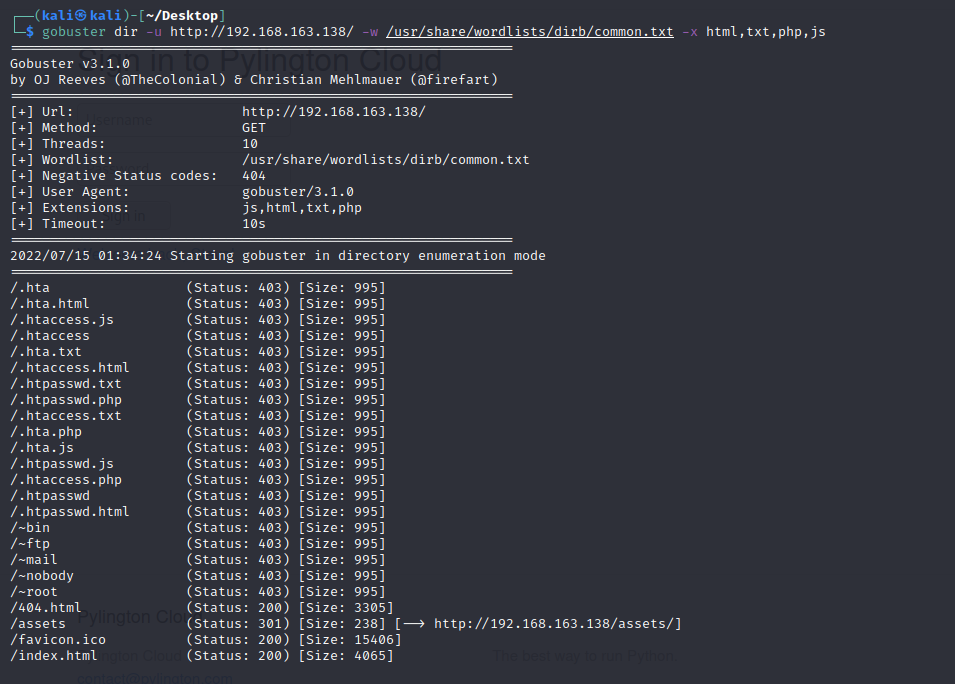
- Dùng netdiscover để tìm ra ip của máy tấn công



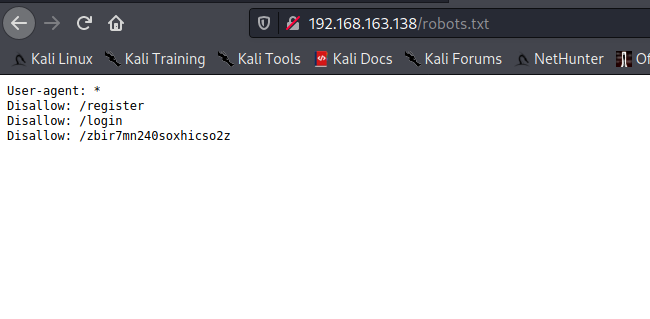
- nmap



- gobuster để tìm các path khả thi

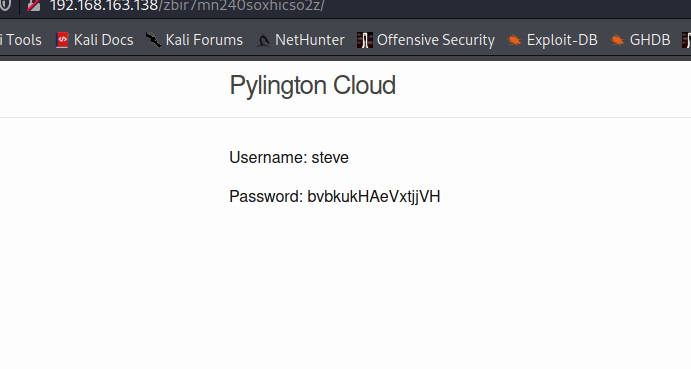


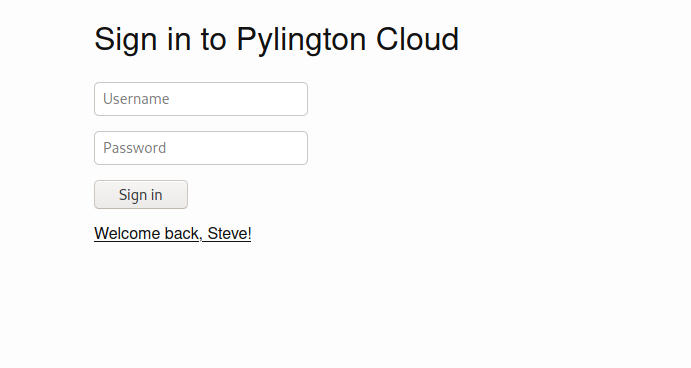
- Vào thử /robots.txt

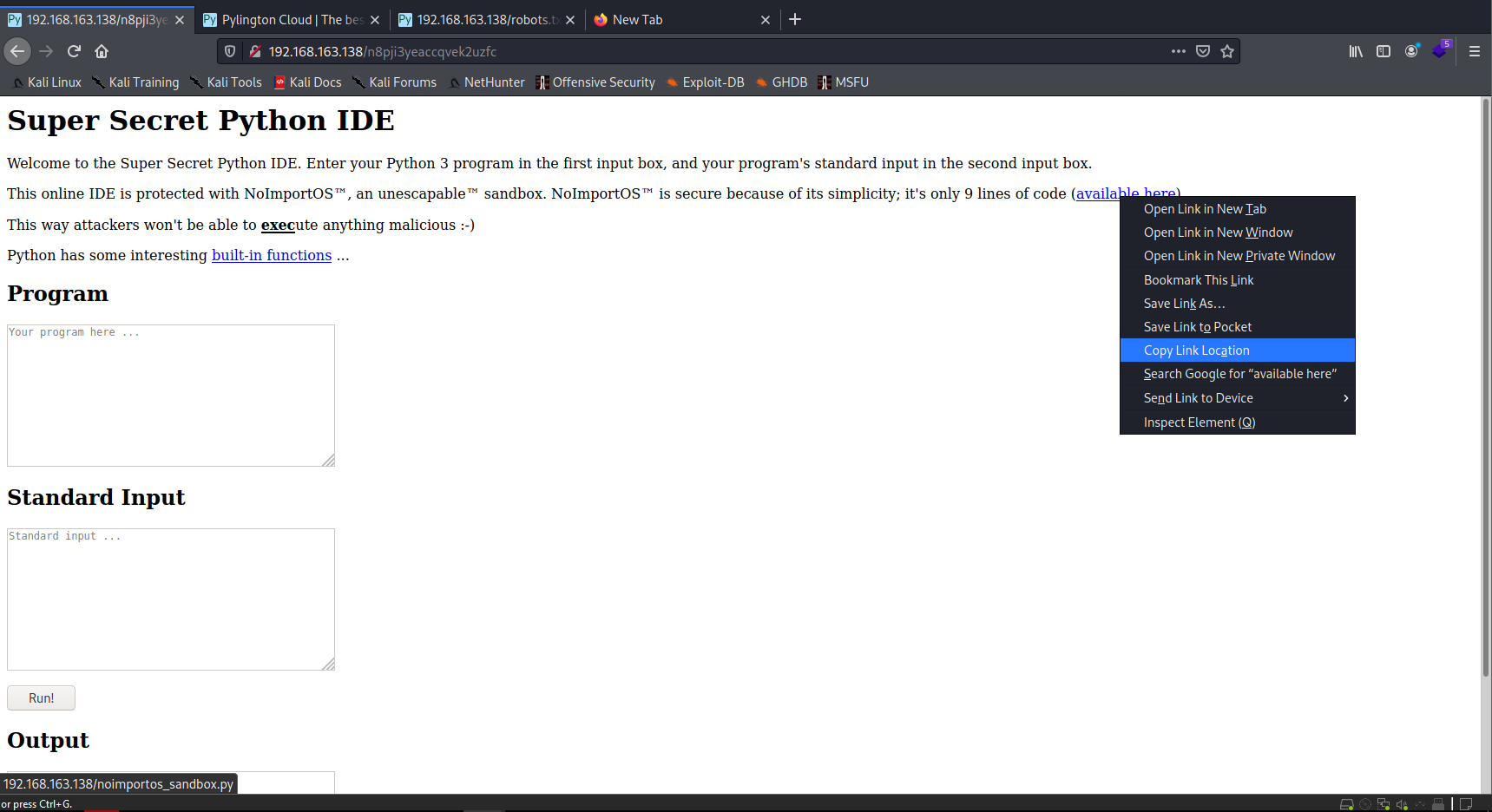


- Vào /zbir7mn240soxhicso2z thì phát hiện username và mật khẩu

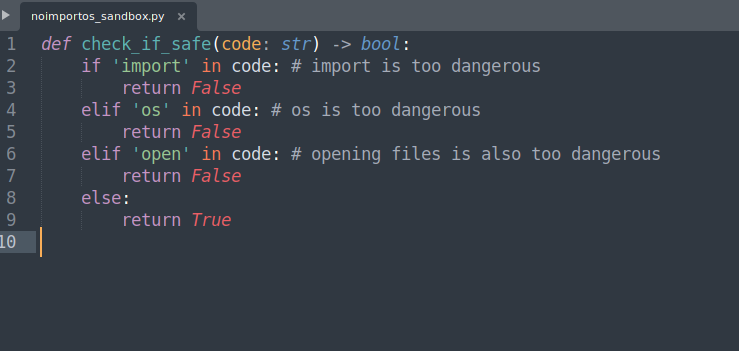
- Dùng username và mật khẩu đó để vào /login đăng nhập



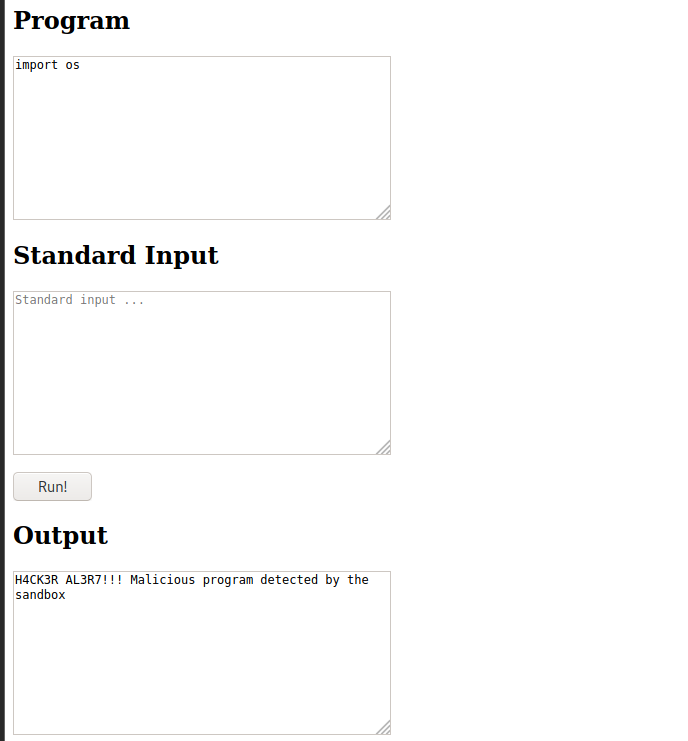


- Đăng nhập thành công sẽ hiện như trên, và lúc đó ta bấm vào Welcome back, Steve!

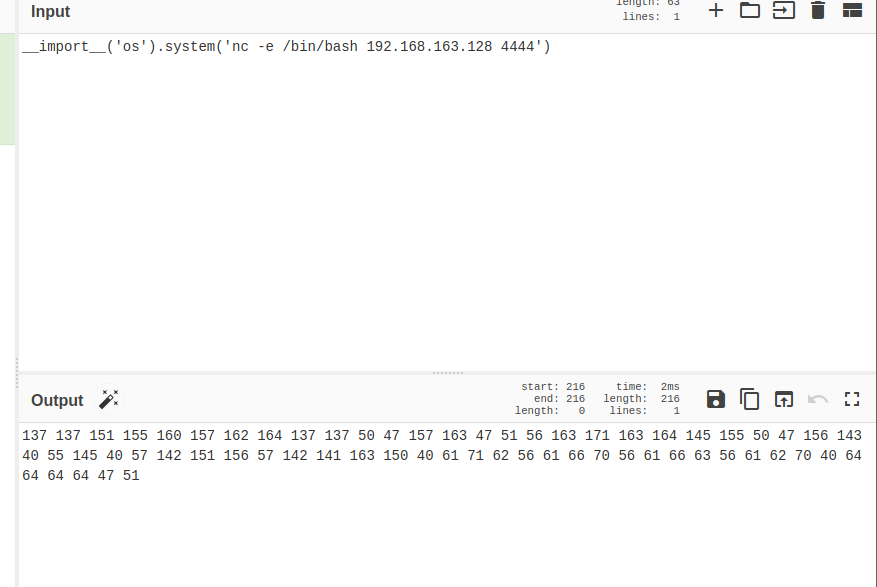
- Tải noimportos\_sandbox.py về và dùng subl hay bất cứ trình chỉnh sửa nào để kiểm tra dòng code bên trong



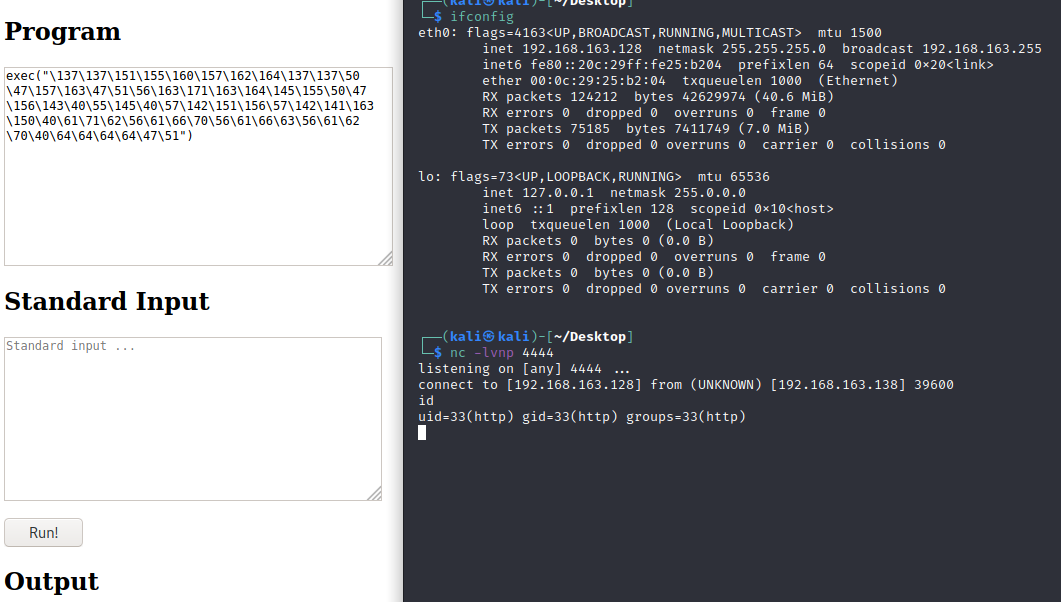
- Thử import os (báo lỗi)



- Thử chạy shell bằng câu lệnh dưới dạng bát phân (dùng cyber chef)

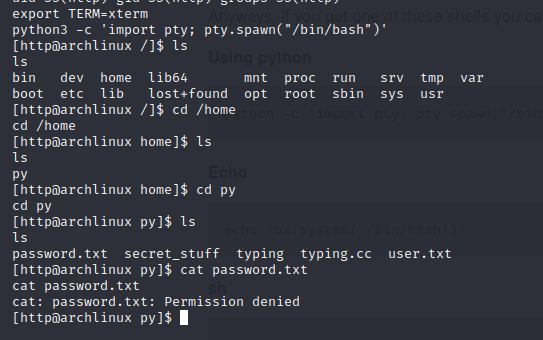


- Nhớ thêm \ giữa mỗi kí tự

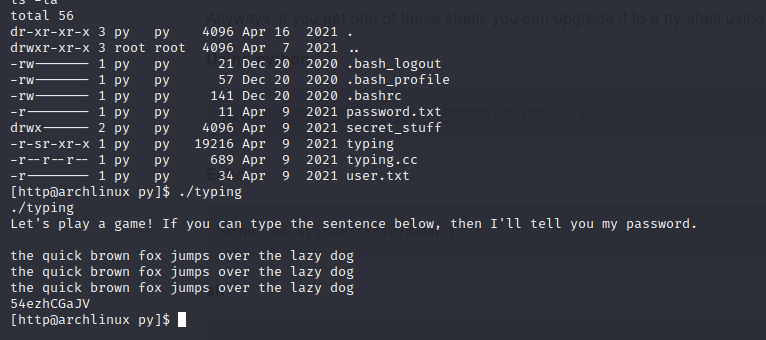


- Thiết lập listener và chạy shell

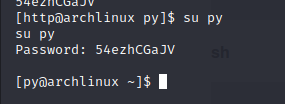
- spawn shell, vào được máy chủ, kiểm tra các file txt, kiếm flag



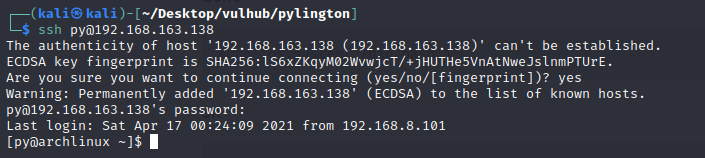
- Chạy file typing, làm theo hướng dẫn, có được mật khẩu



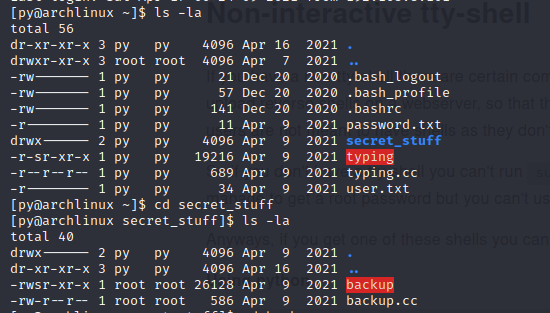
- Đăng nhập vào bằng py

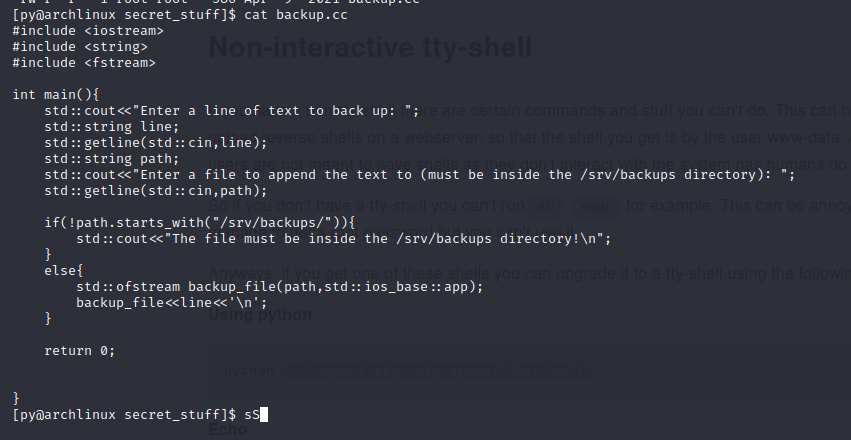


- Thử ssh vào py trên máy chủ của mình



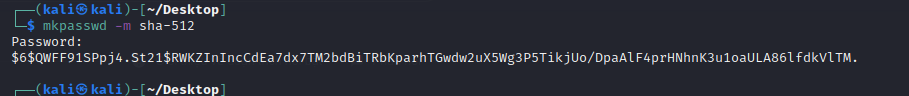
- Vào thành công, tìm kiếm các lỗ hổng (các file backup hay file liên quan tới lịch sử chỉnh sửa hay mật khẩu)





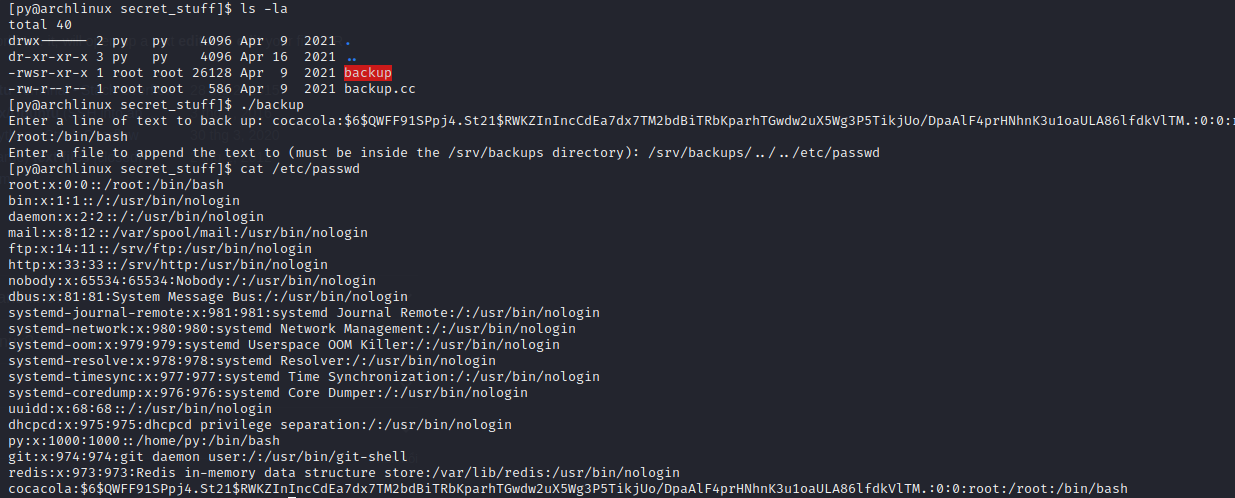
- backup sẽ thay đổi lại mật khẩu và chúng ta có thể dùng nó để leo quyền root

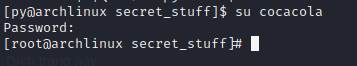
- Tự tạo mật khẩu và thêm user, id, và quyền khởi chạy





- Mở file backup lên và chạy dòng lệnh đó, thêm đường dẫn /etc/passwd, và sau đó đăng nhập vào bằng username của mình và mật khẩu mà ta đã tạo là đã leo được quyền root





- Tìm, mò file root.txt

