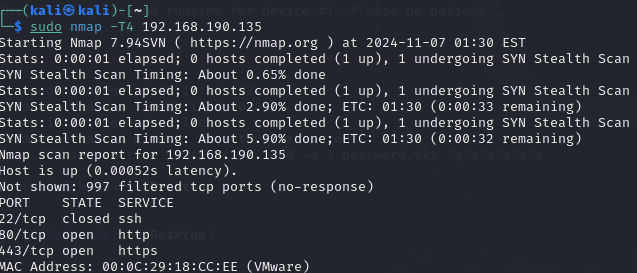
**Chuẩn Bị**

B1 Quét mục tiêu

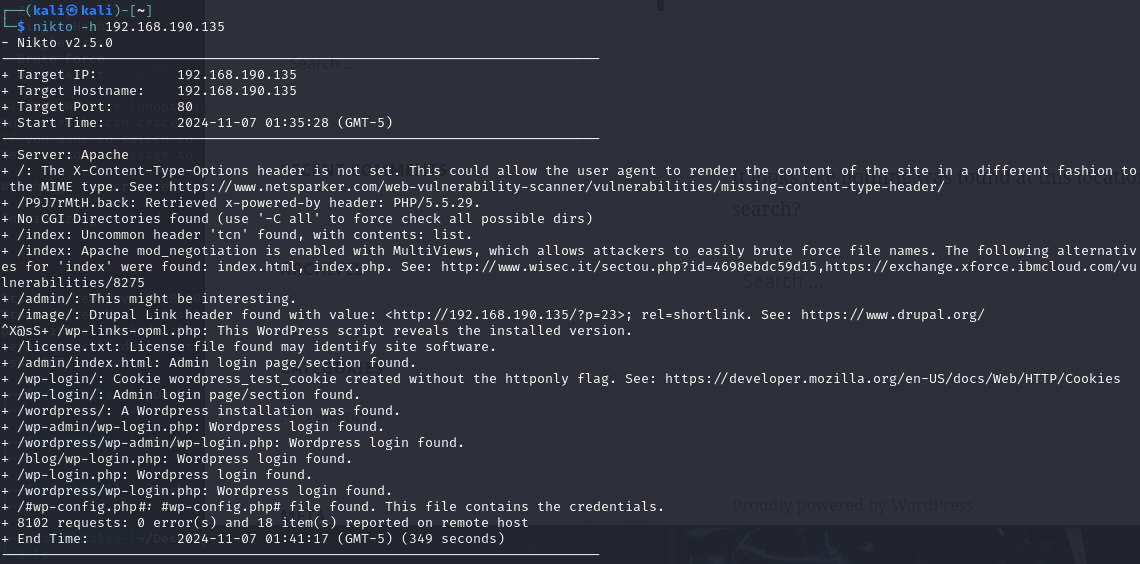


Các cổng mở trên máy victim

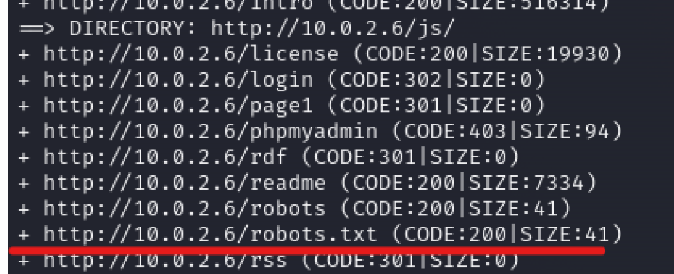
**Tấn công**

=> truy cập vào web

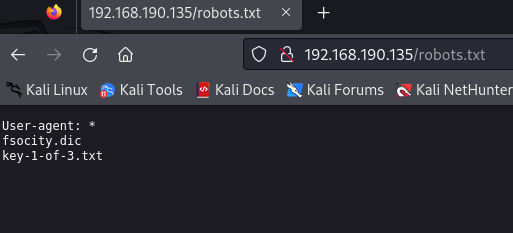
B2 Sử dụng nikto để quét trang web



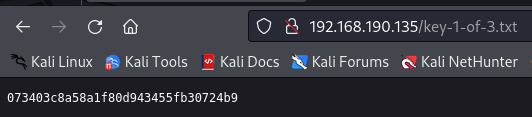
Dùng câu lệnh dirb <http://192.168.190.135> để tìm các file ẩn



B3: Truy cập đường dẫn file robots.txt thấy dc thông tin

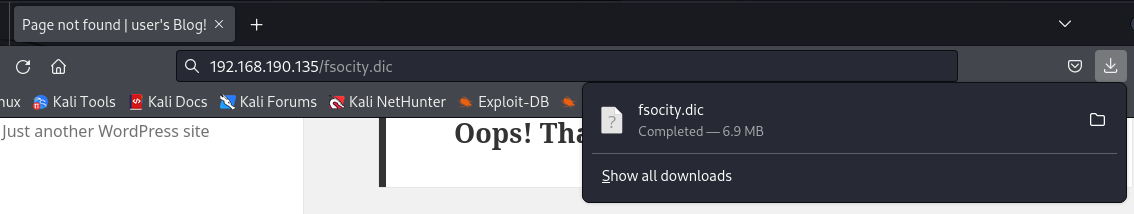


B4: Truy cập vào file ở thông tin trên



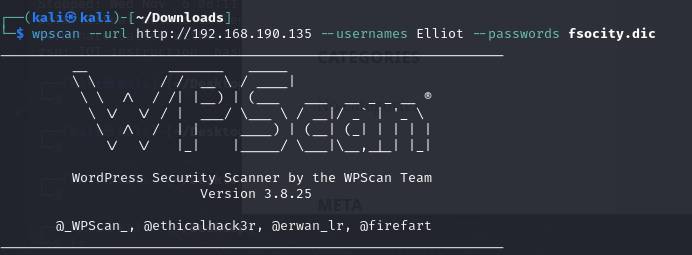
\*Flag đầu tiên

B5: Tải từ điển về qua đường dẫn

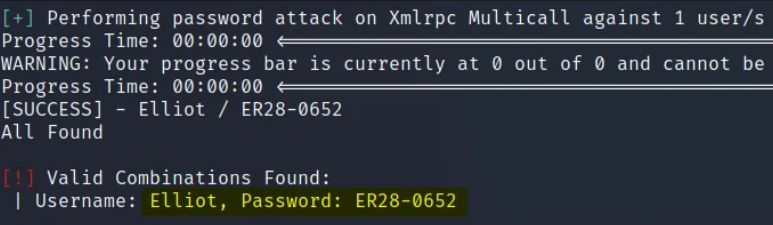


B6: Dùng wps crack mk

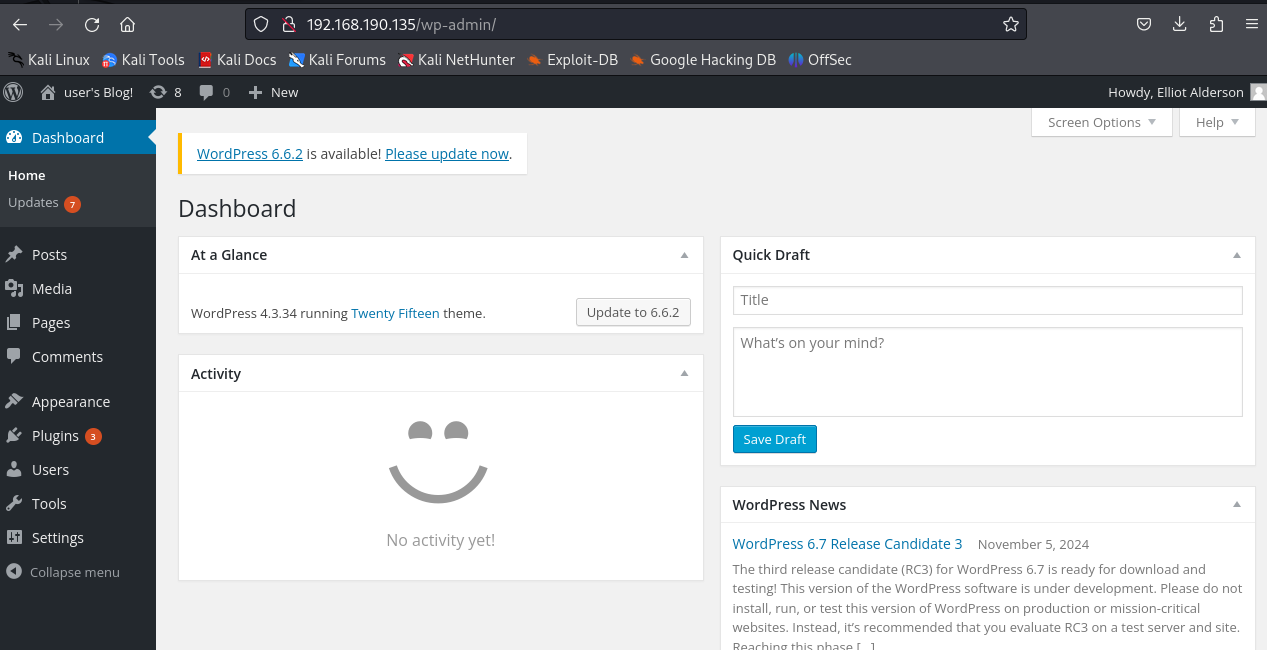
Câu lệnh



Kq

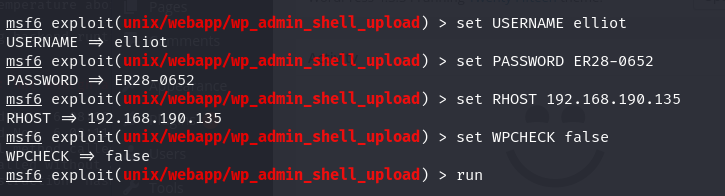


Dùng thông tin đó đăng nhập vào wordpress

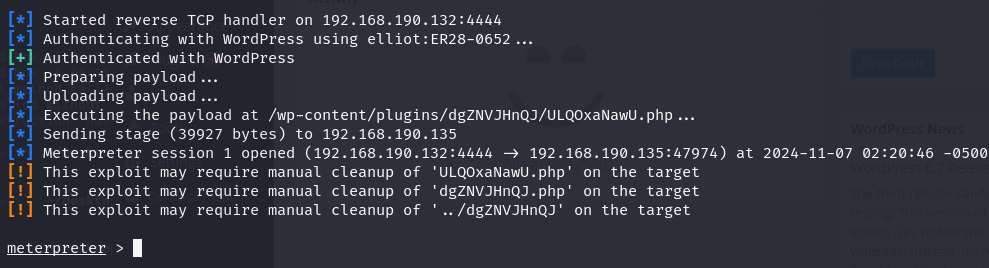


B6: Dùng mfs

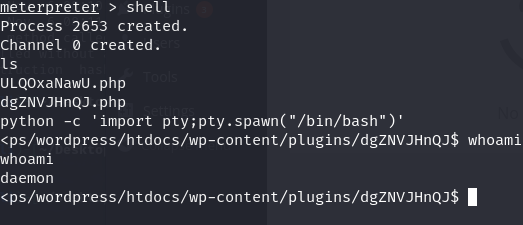
Dùng module sau



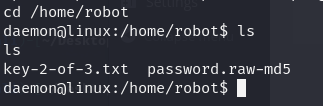
Thành công



Bị shell restricted nên lại unlock shell



Truy cập vào để lấy mã hash của tk root



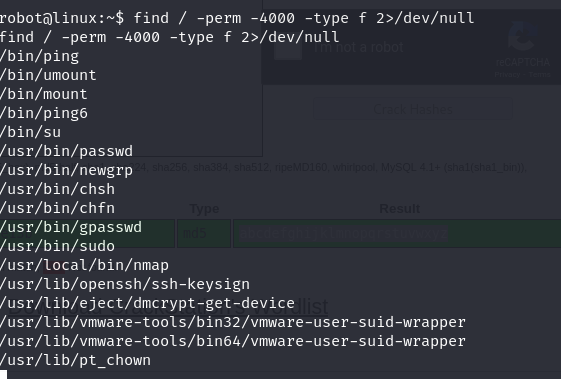
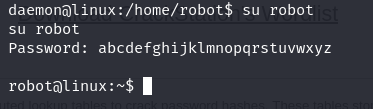
robot:c3fcd3d76192e4007dfb496cca67e13b

Giải mã hash online ta dc



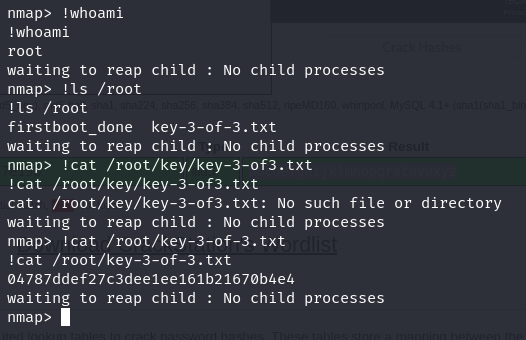
Cờ thứ 2

Đăng nhập thành công



Tìm các câu lệnh có thể chạy dưới quyền của tk này

Ta có thể leo thang đặt quyền thông qua nmap



Tìm ra key cuối