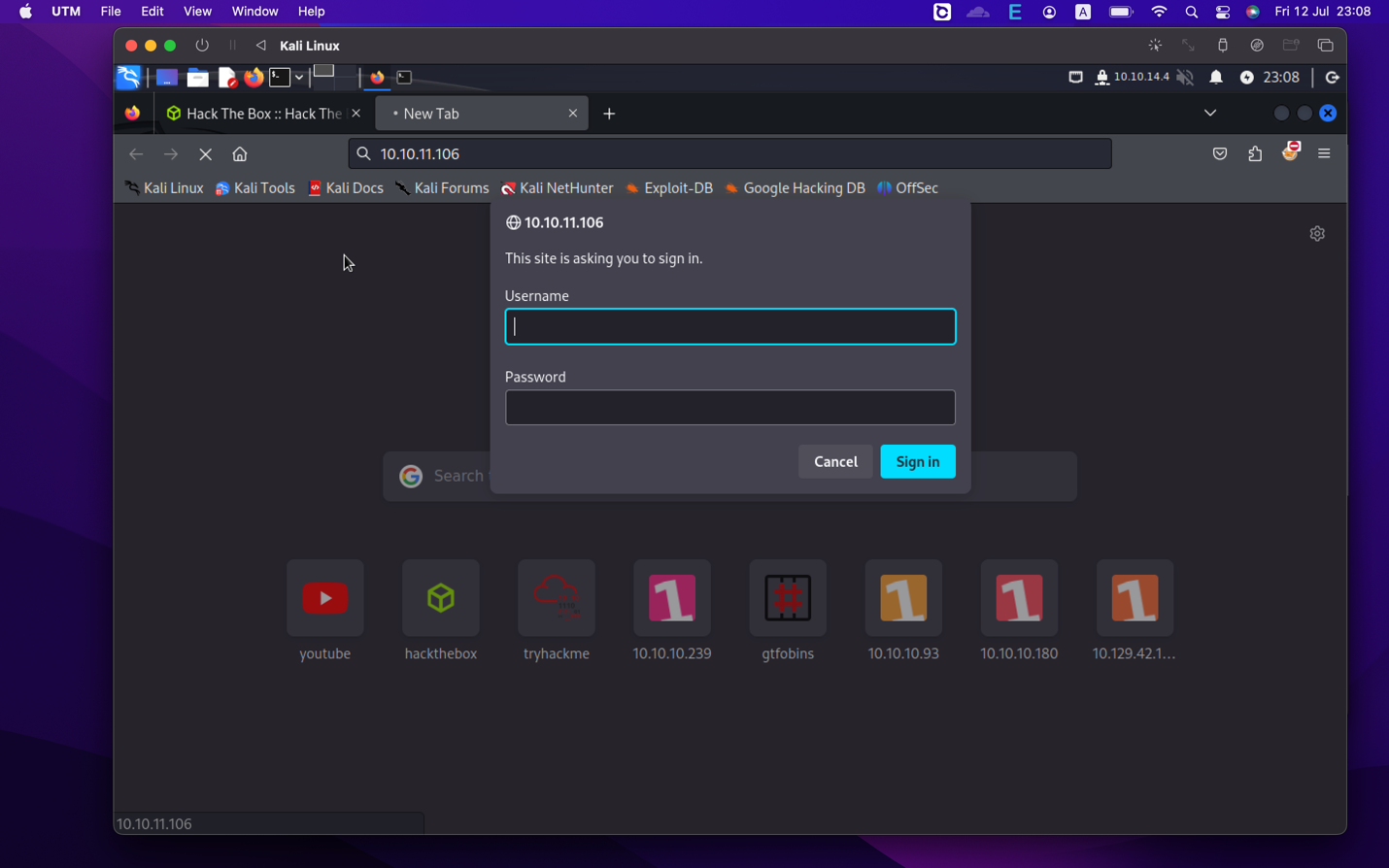
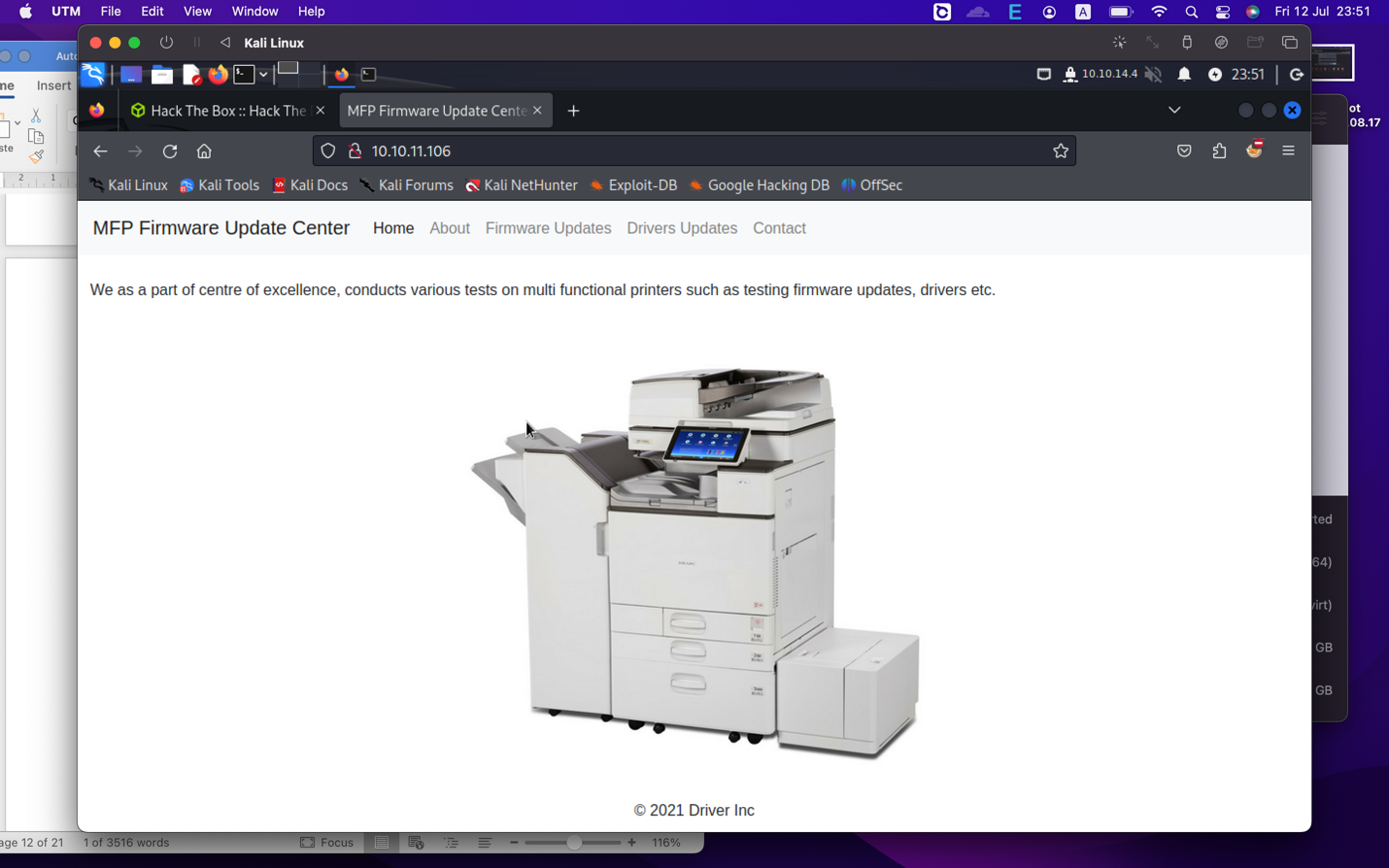


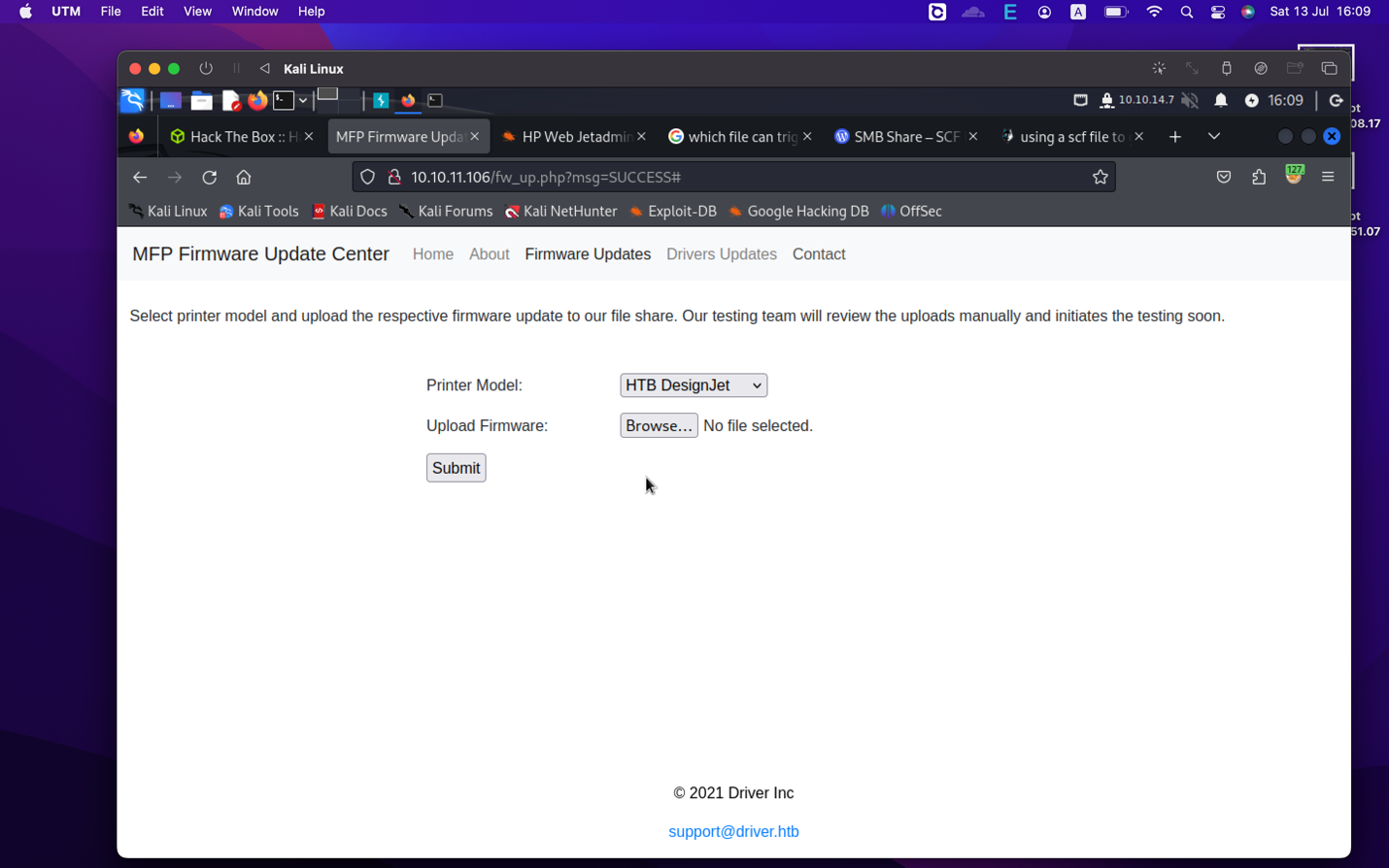
Trang web yêu cầu đăng nhập:



admin:admin

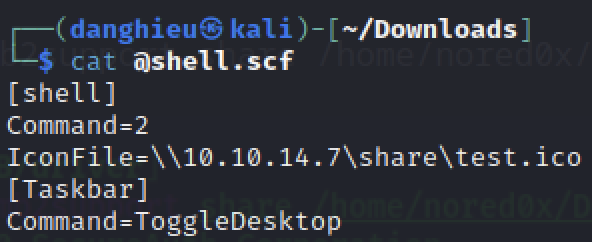


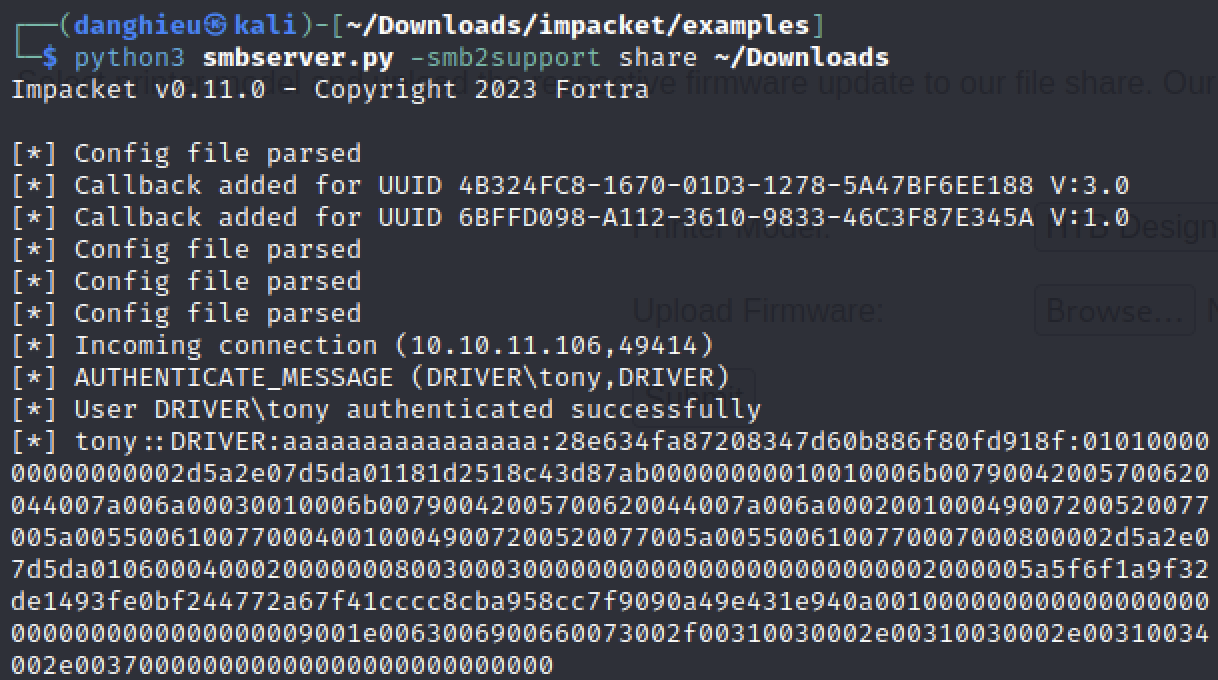
Trang web cho mình upload tập tin. Nó bảo upload firmware nhưng mình tìm hết trên mạng không thấy cách nào để tạo firmware mà reverse shell được cả.

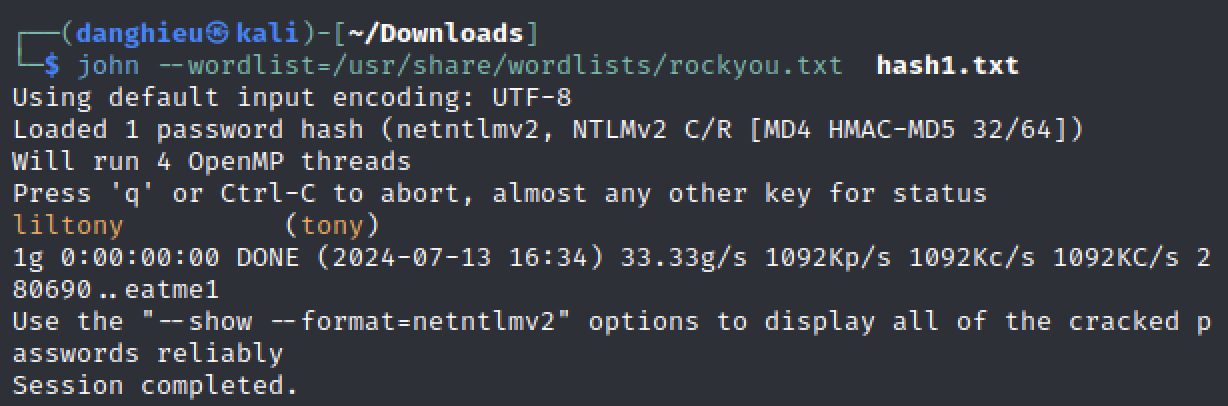


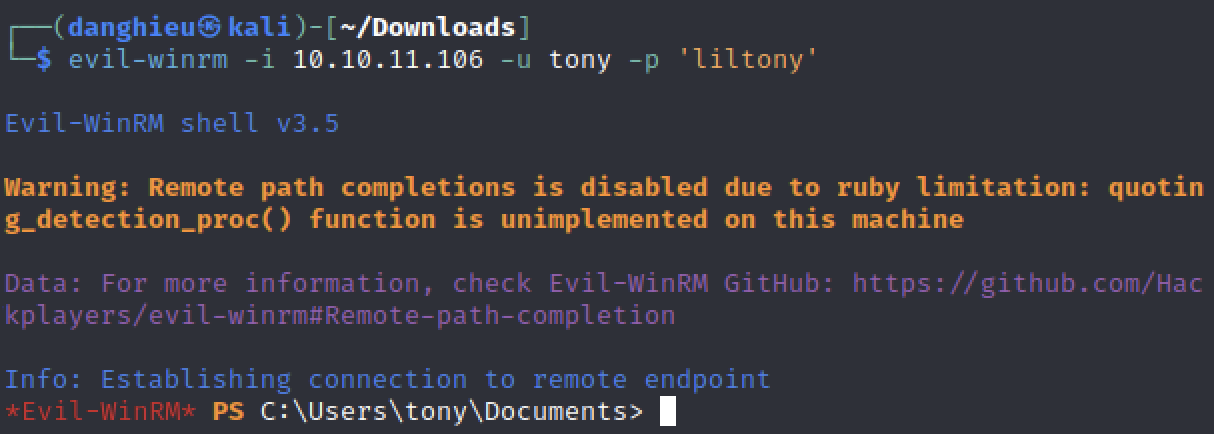
Firmware có liên quan gì đến Driver, máy chủ đang chạy dịch vụ SMB, cho chúng ta tải tập tin 🡪 Mình tìm 1 bài viết nói về tải tập tin lên smb share.

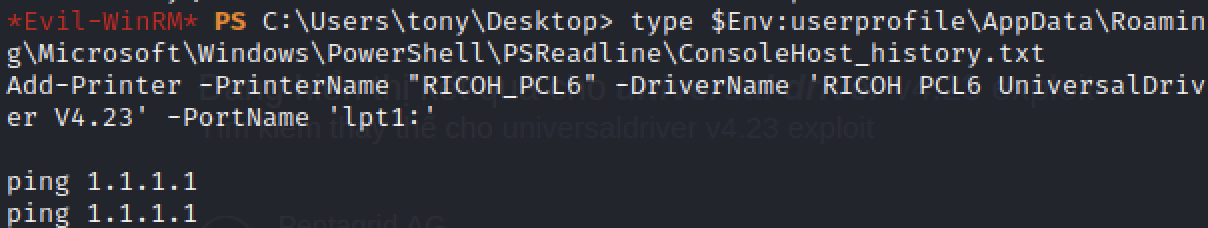
Tập tin chúng ta sẽ tải lên smb share là scf (Shell Command Files). Khi người dùng duyệt qua tập tin sẽ được thực thi.

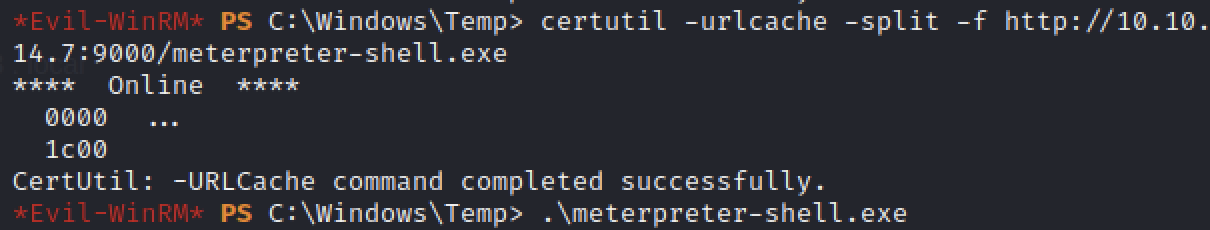


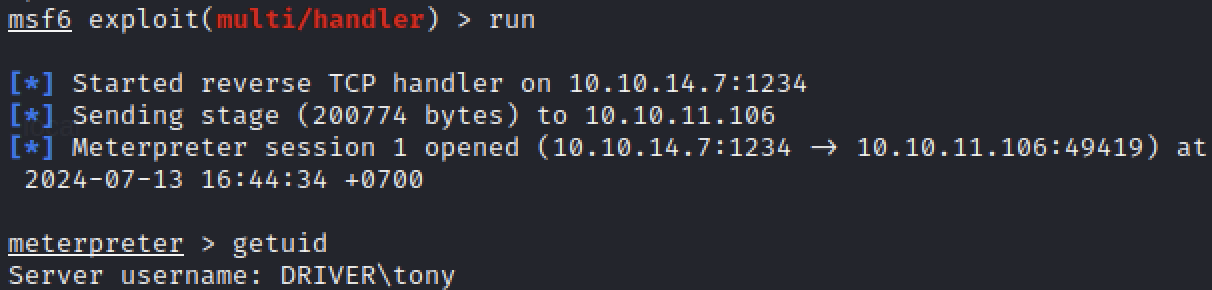












Tiến trình của mình có đặc quyền là 0, mình sẽ di chuyển đến 1 tiến trình có đặc quyền cao hơn





