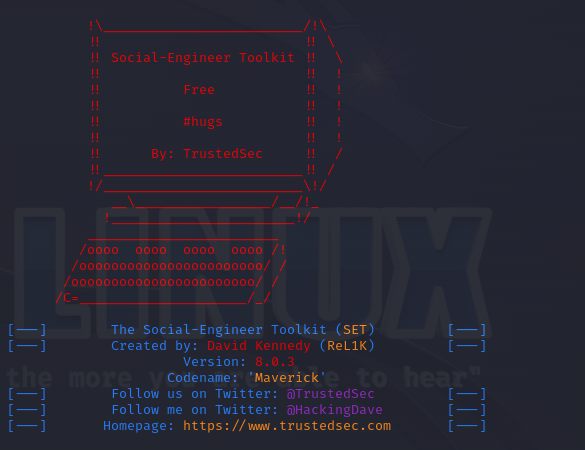
**BÀI TẬP CÁ NHÂN 2**

Bài 1: Tìm hiểu SET toolkit và Zphisher:

1. SET tool kit:

* SET toolkit, hay còn được gọi là Social Engineering Toolkit, là một bộ công cụ mạnh mẽ được phát triển để thực hiện các cuộc tấn công mạng thông qua kỹ thuật xâm nhập xã hội. Được thiết kế đặc biệt để hỗ trợ các chuyên gia an ninh và penetration testers trong việc thực hiện các cuộc kiểm tra an ninh bằng cách mô phỏng các kỹ thuật lừa đảo và xâm nhập xã hội, SET toolkit cho phép người dùng tạo ra các cuộc tấn công mô phỏng như lừa đảo qua email, trang web giả mạo và các kỹ thuật xâm nhập xã hội khác. Mục tiêu của việc sử dụng SET toolkit là kiểm tra độ bảo mật của một hệ thống hoặc tổ chức bằng cách đánh giá khả năng phòng ngừa và phản ứng của họ trước mối đe dọa từ các tình huống xâm nhập xã hội.

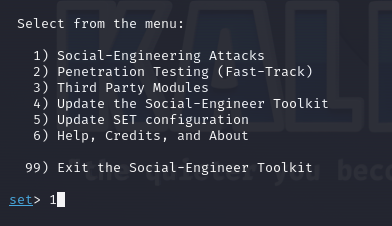


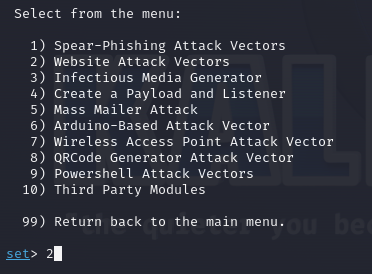
1. Zphisher:

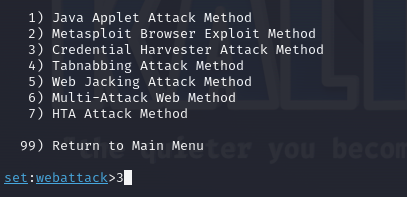
-Zphisher là một công cụ phishing, tức là một phần mềm được phát triển để thực hiện các cuộc tấn công lừa đảo thông tin cá nhân và đăng nhập. Chức năng chính của Zphisher là mô phỏng giao diện đăng nhập của các trang web phổ biến như Facebook, Instagram, Gmail và nhiều dịch vụ khác. Điều này cho phép người sử dụng tạo ra các trang đăng nhập giả mạo nhằm lừa dối người dùng và thu thập thông tin cá nhân hoặc thông tin đăng nhập của họ.

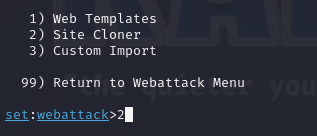
Bài 2: demo SET toolkit phishing website

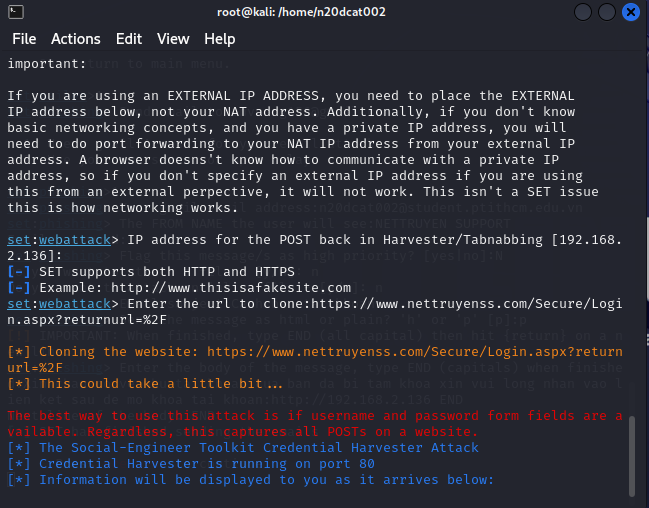
* Tạo web phishing bằng SET toolkit





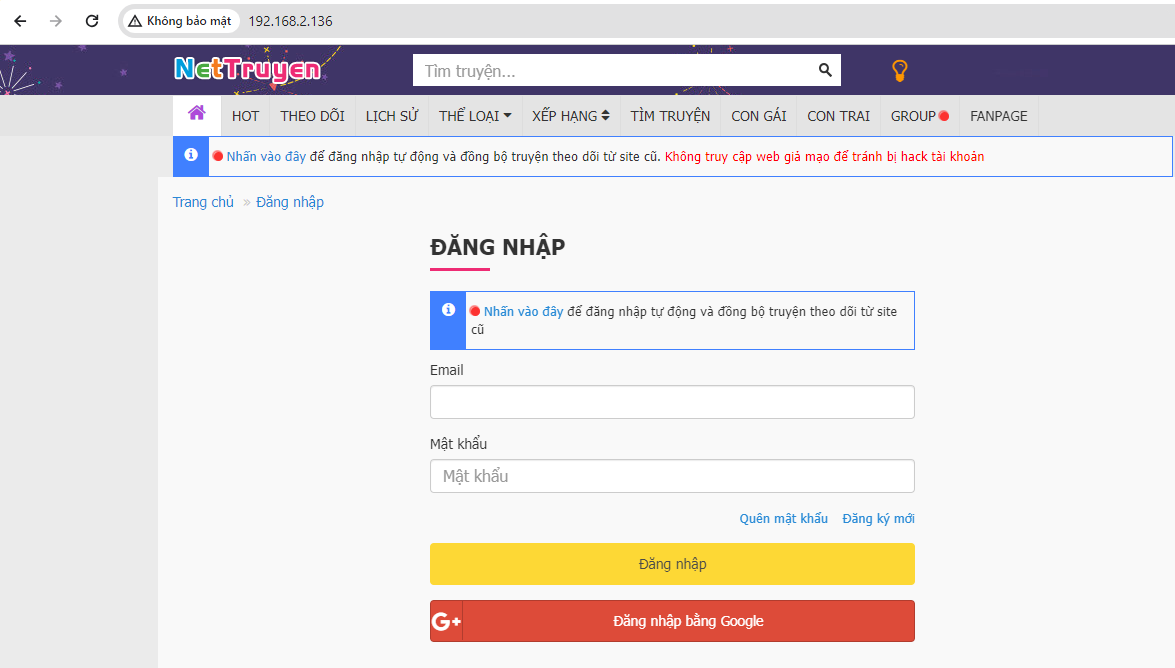




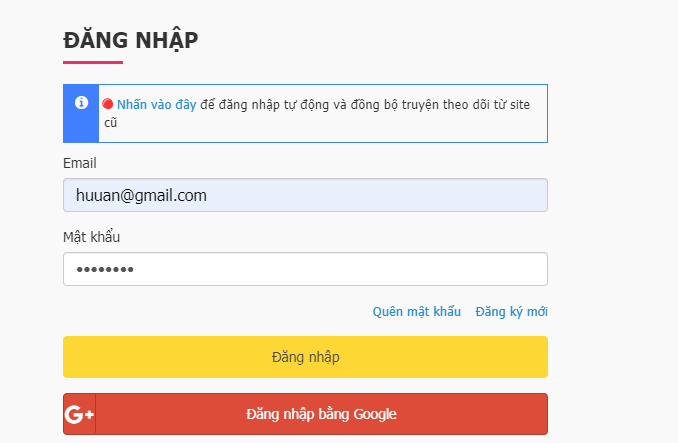


* Kiểm tra web phishing

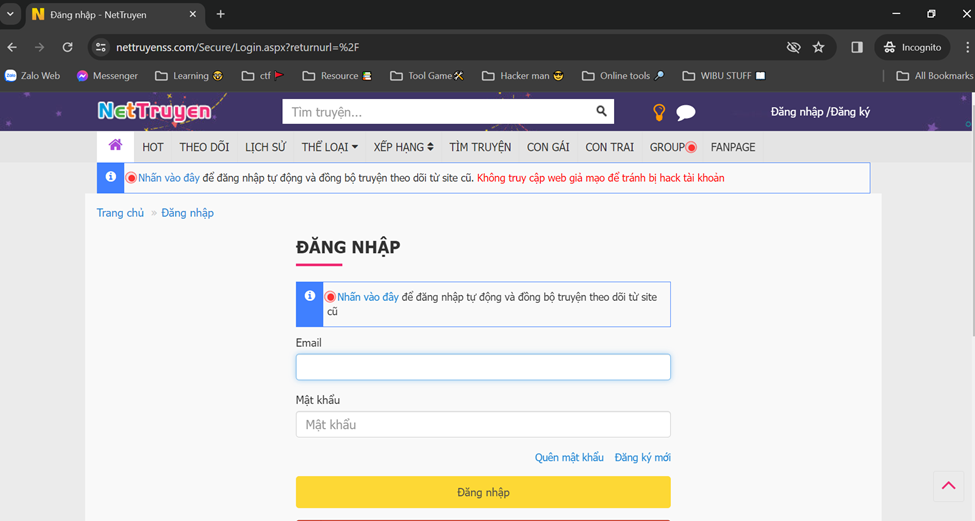
+ Web phishing có giao diện đăng nhập giống như web gốc chỉ có khác địa chỉ tên miền



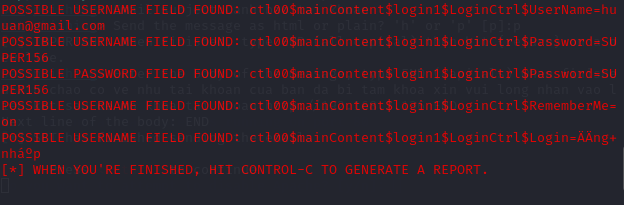
* Thử đăng nhập



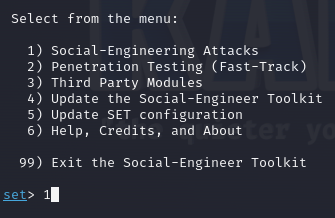
* Sau khi đăng nhập trên web phishing sẽ tự động chuyển về trang web gốc

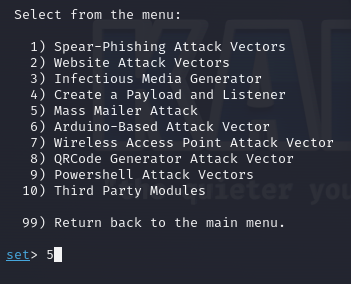


* Trên máy kali đã lấy được email và mật khẩu mà người dùng đã nhập

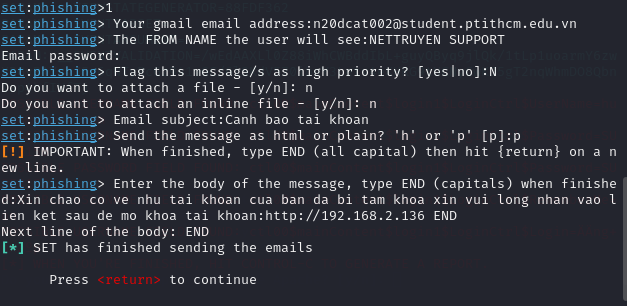


* Gửi mass email chưa link web phishing cho victim bằng SET toolkit

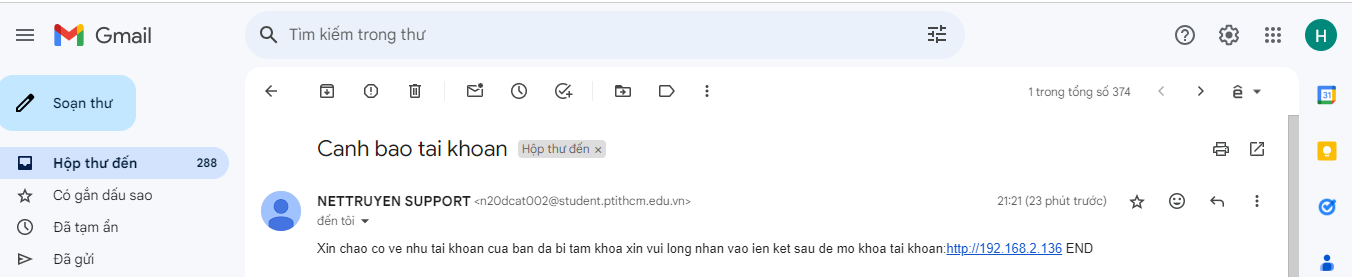








* Trên email của victim đã nhận được Mass email



* Khi nhấn vào đường link sẽ chuyển đến trang web phishing

