**SOCIAL ENGINEERING ATTACK**

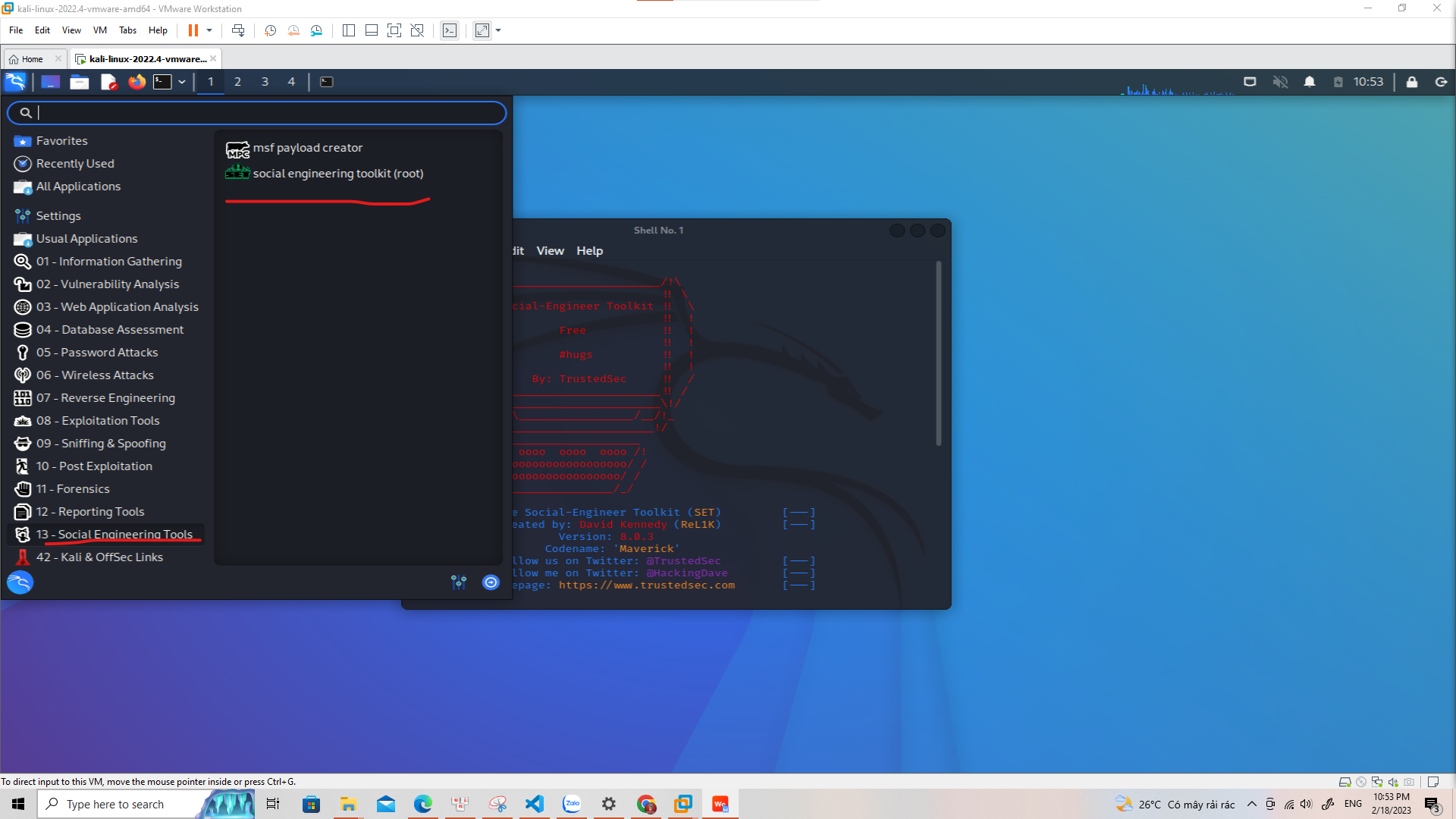
Social Engineering (hay tấn công phi kỹ thuật) là thuật ngữ phổ biến trong lĩnh vực bảo mật thông tin, mô tả kiểu tấn công sử dụng các hình thức thao túng hành vi của con người thay vì tập trung khai thác các lỗ hổng bảo mật của máy móc, thiết bị. Qua đó, kẻ tấn công có thể đạt được các mục đích của mình như xâm nhập vào hệ thống, truy cập thông tin quan trọng,… mà không cần phải thực hiện những kỹ thuật tấn công quá phức tạp.

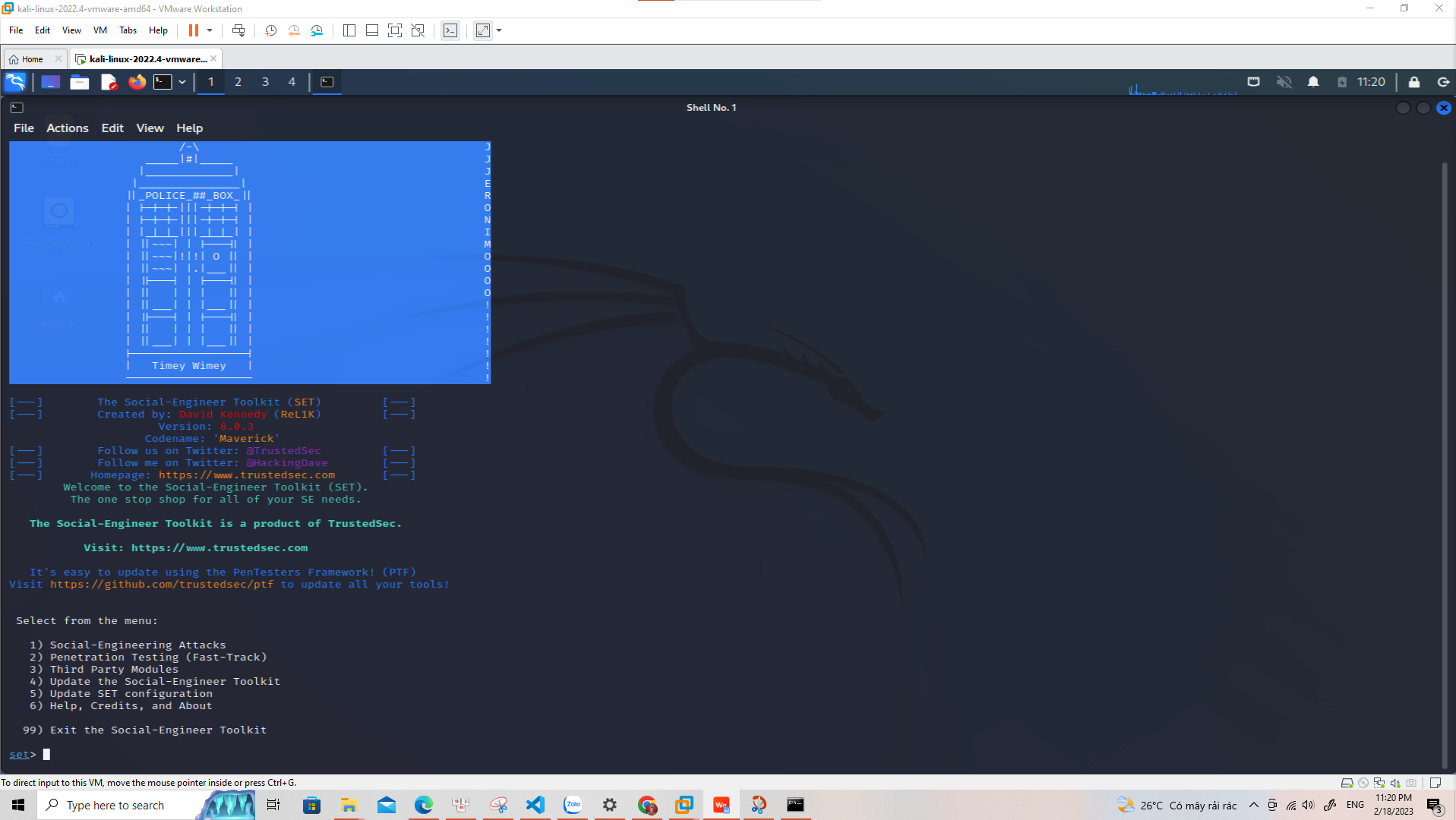
**B1**: Tạo một trang lừa đảo: Ở ví dụ này ta tạo một trang đăng nhập google giả trong môi trường chung mạng LAN. Khi nạn nhân đăng nhập chúng ta biết được username và password của nạn nhân.

- Vào kali - linux trong VMWare

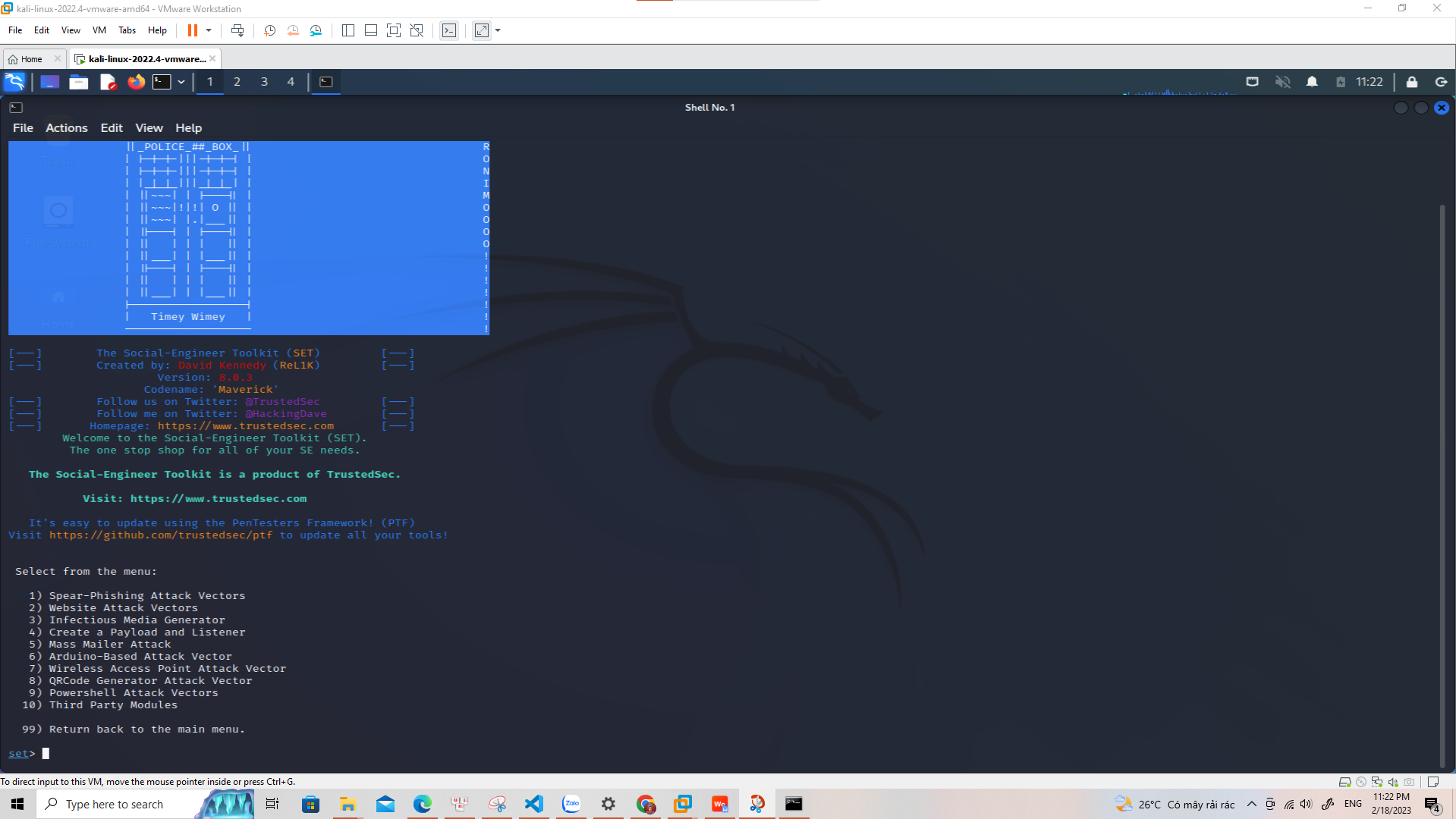
- Vào phần applications chọn Social Engineering tools hoặc gõ setoolkit trong terminal.

- Chọn số 1 và nhấn ENTER





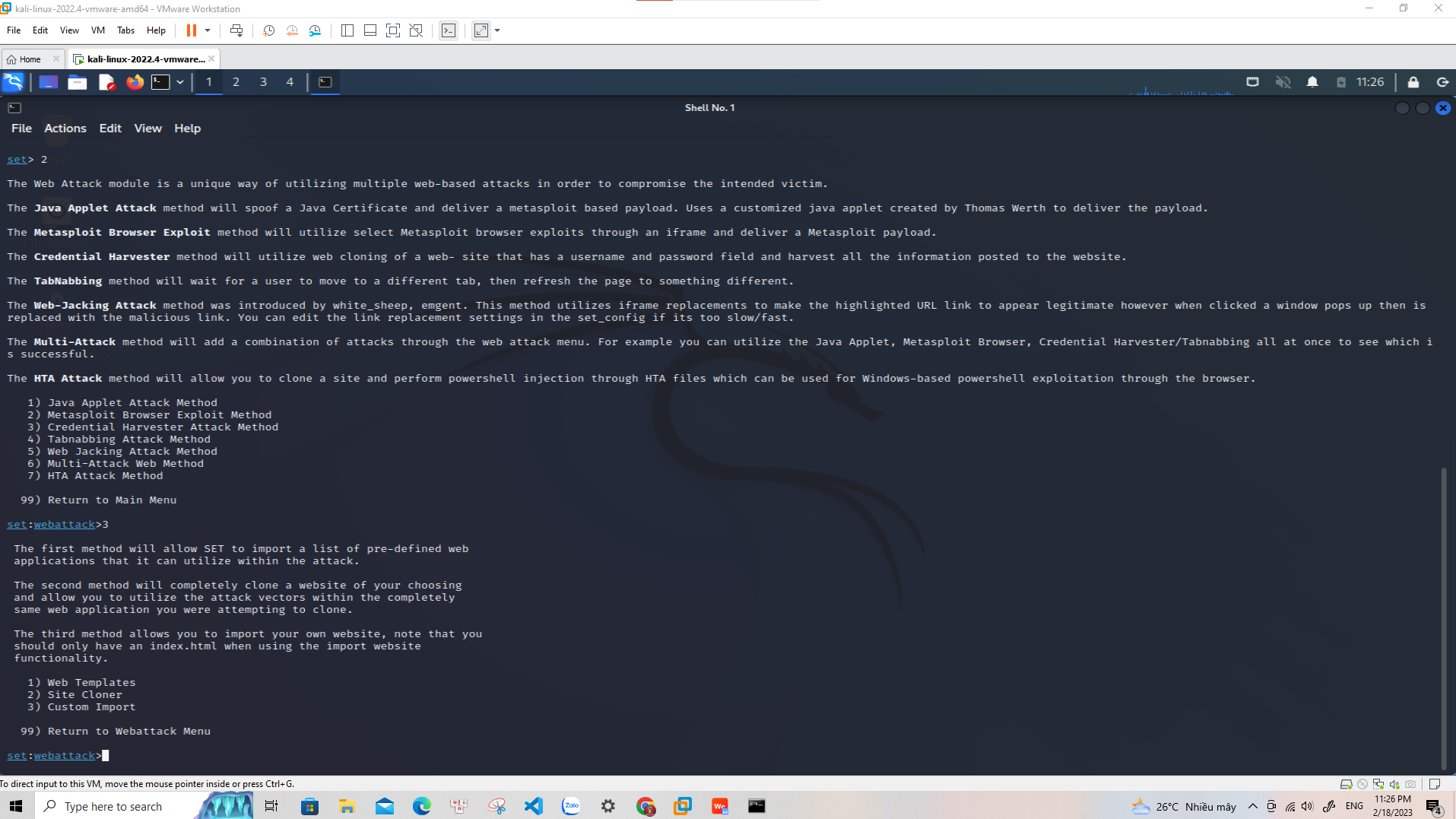
- Tiếp tục số 2 Website Attack Vectors



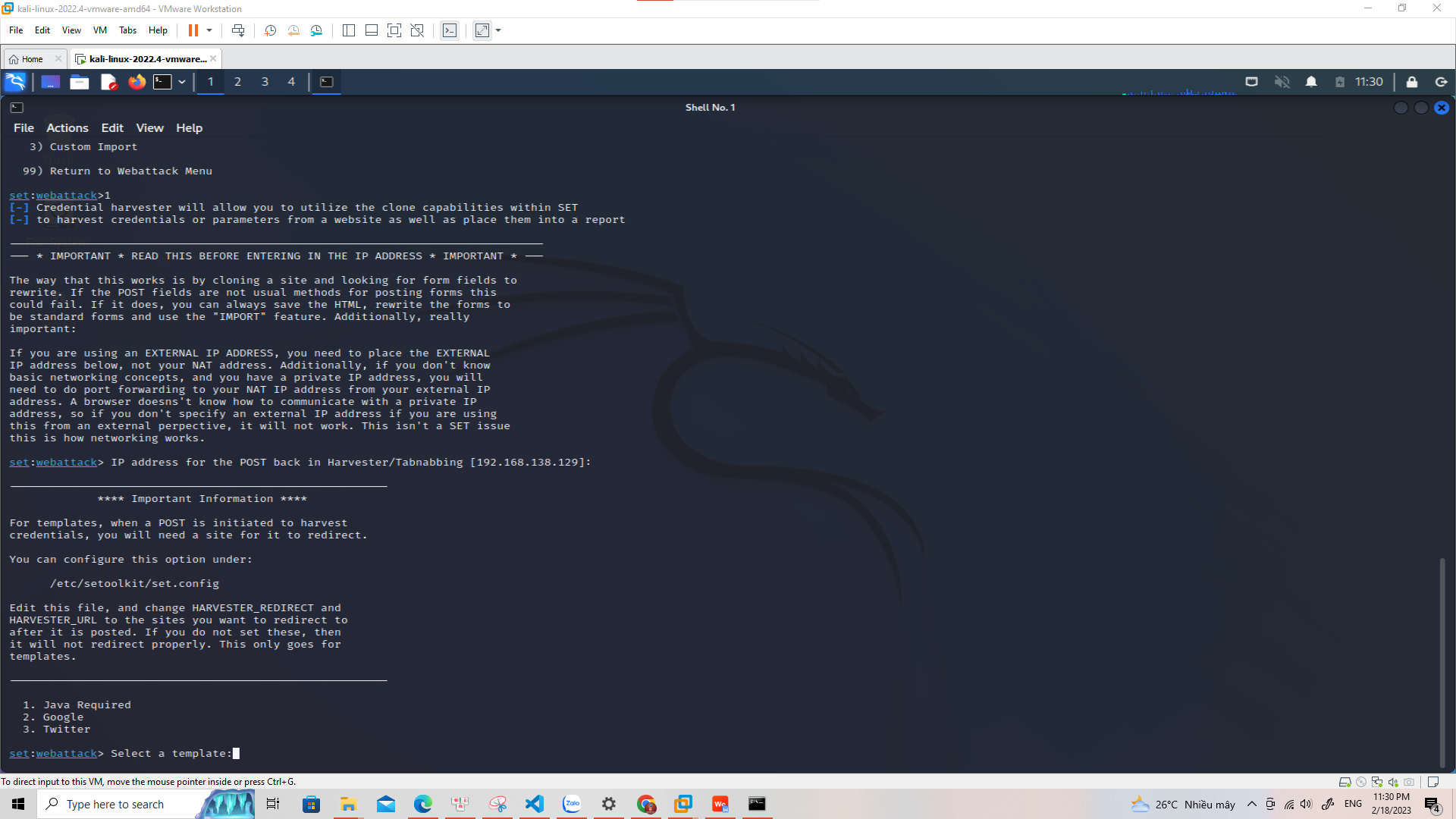
- Chọn số 3 Credential Harvester Attack Method



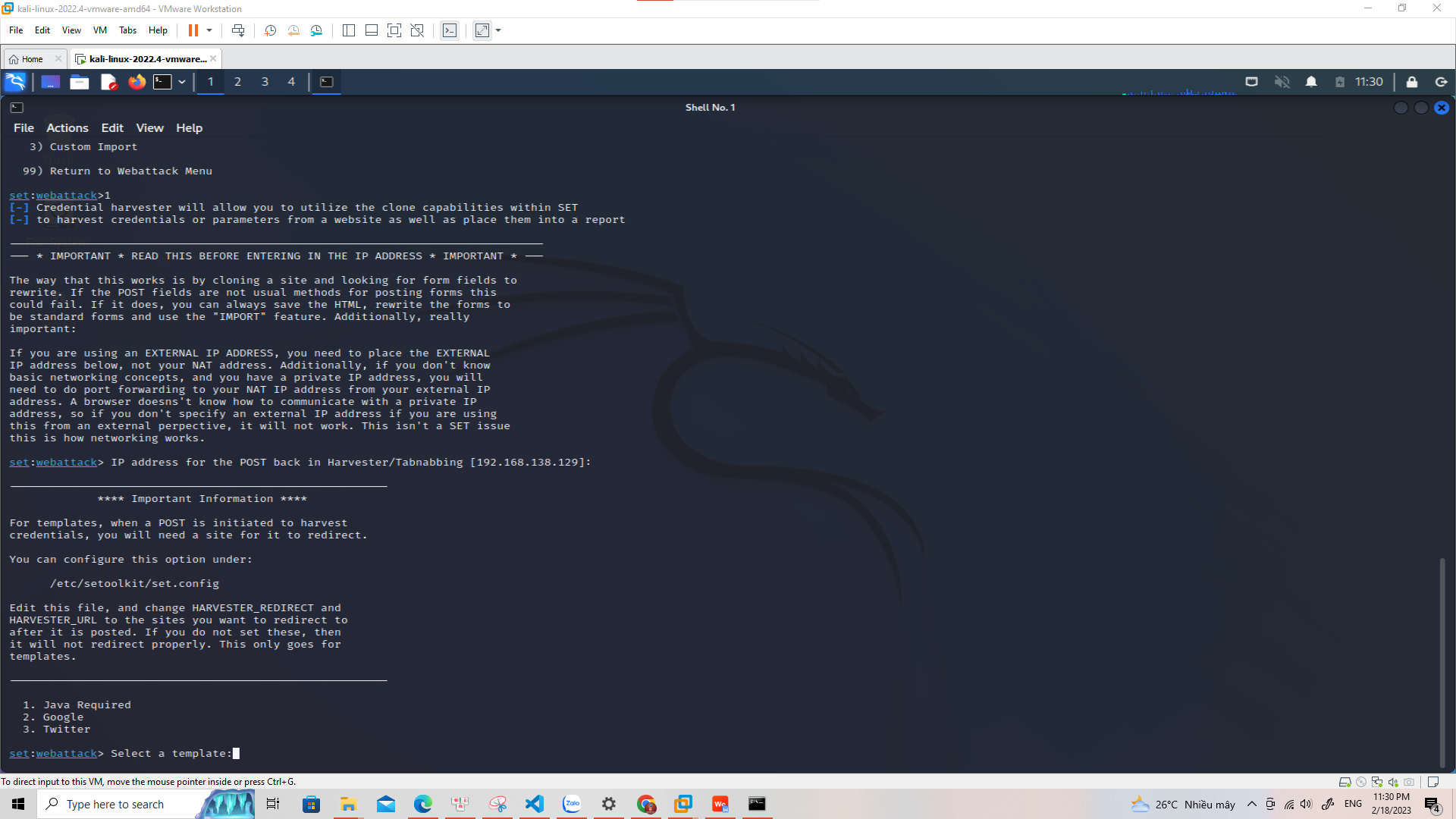
- Chọn số 1 Web Templates



- Vì máy mục tiêu và máy chúng ta chung môi trường mạng. Nên ta nhấn Enter luôn để lấy local IP đó là 192.168.138.129 làm IP cho trang web giả mạo.



- Chọn mục số 2 Google

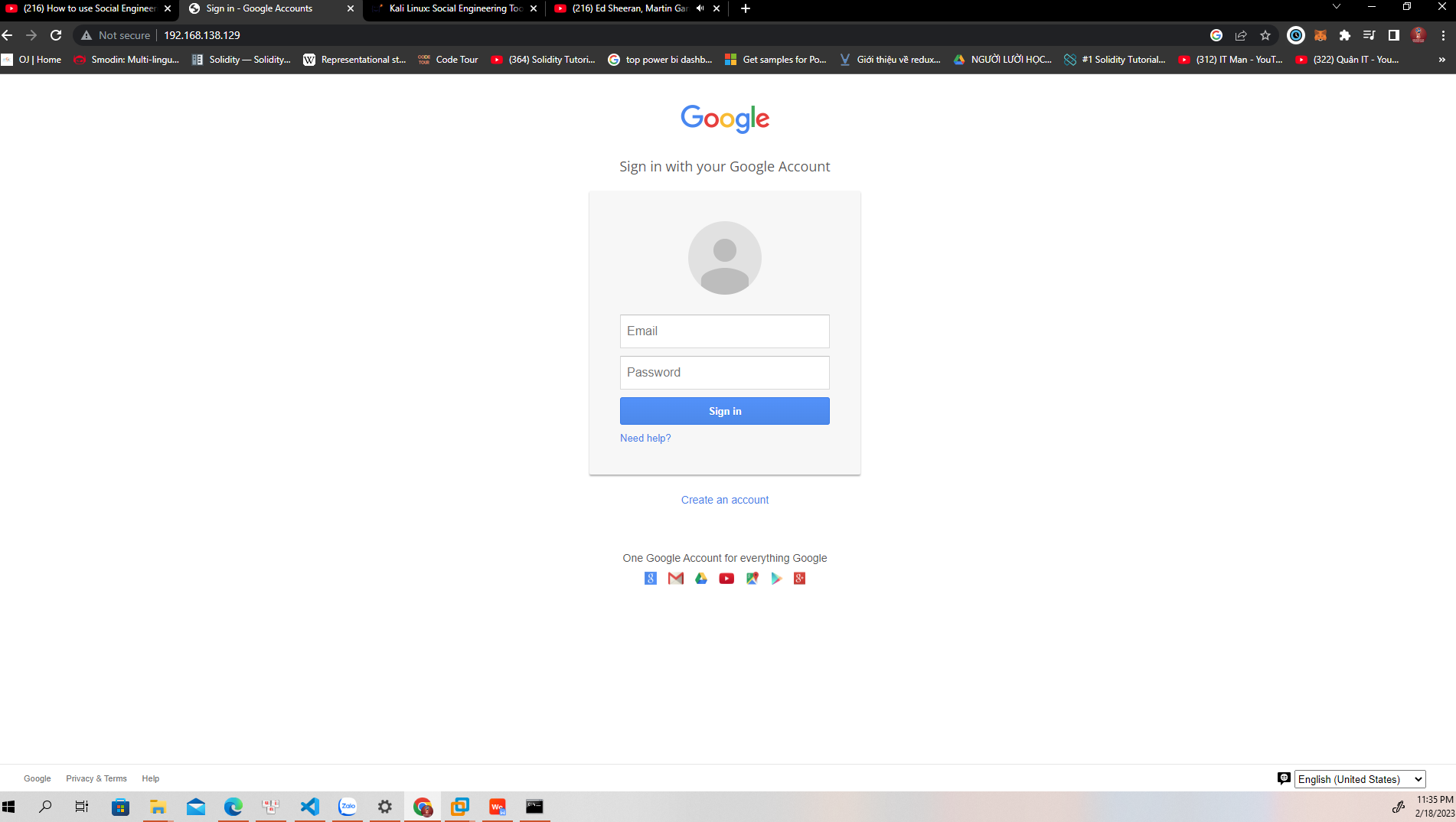


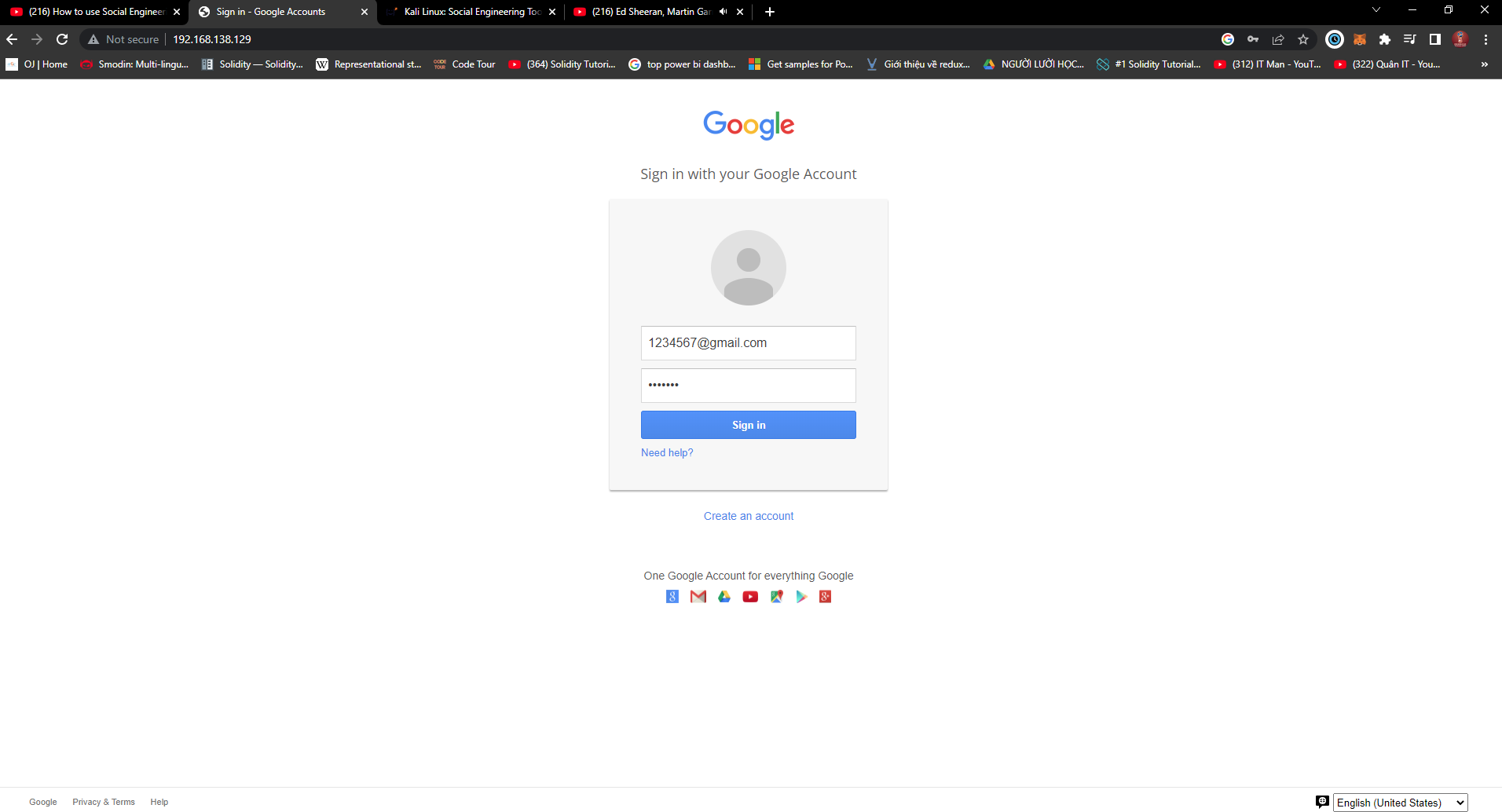
- Như vậy đã tạo xong một trang google giả trên máy chúng ta và lắng nghe thông tin từ những nạn nhân.

- link giả chúng ta có địa chỉ 192.168.138.129

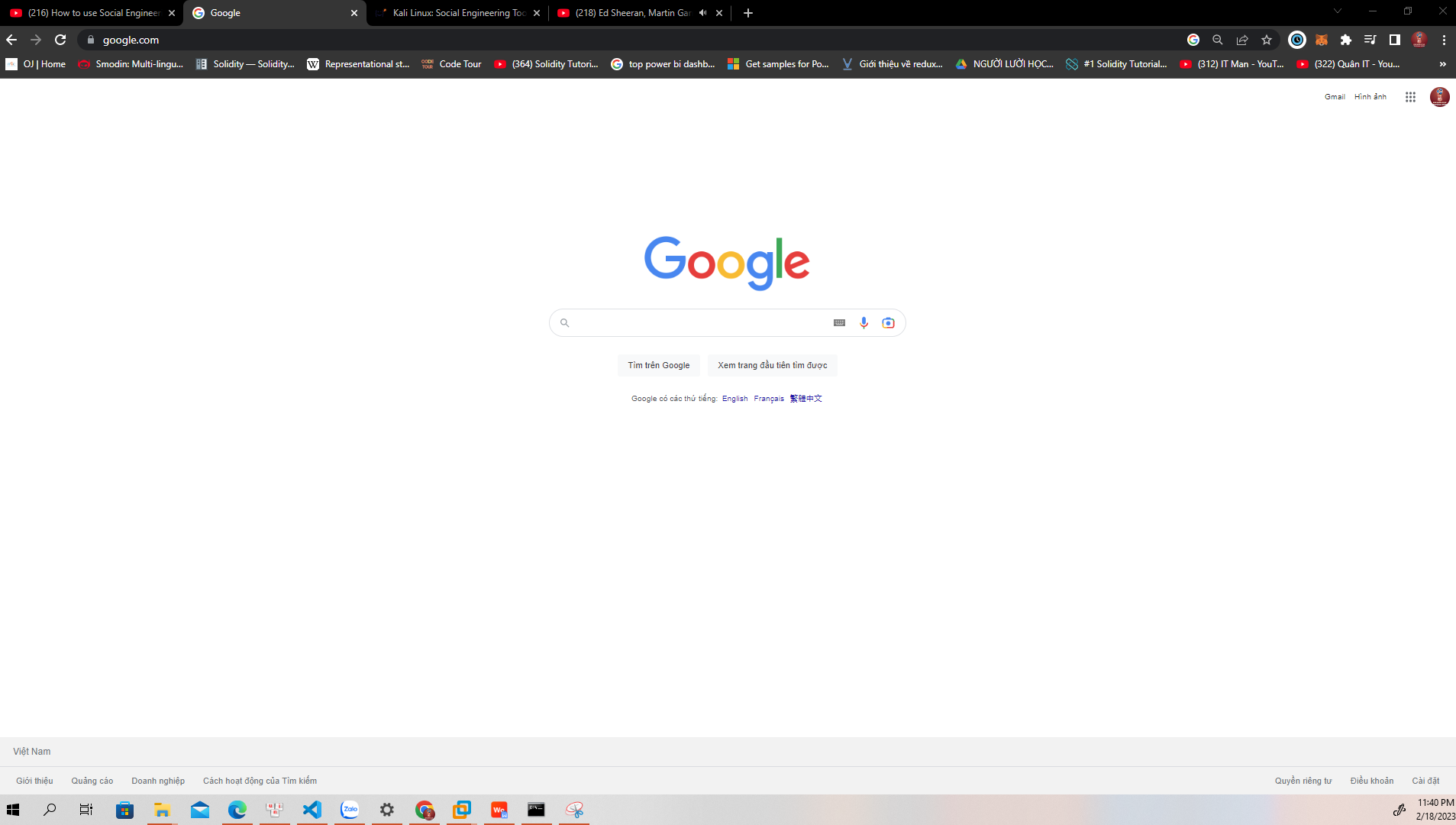
**B2**: Tấn công

- Giả sử nạn nhân nhấn vào link giả của chúng ta và tưởng rằng là trang đăng nhập từ Google





- Tự động chuyển sang trang Google khi nhấn đăng nhập.



- Khi nạn nhân nhấn đăng nhập thì máy chúng ta sẽ lắng nghe được thông tin của nạn nhân bao gồm cả username và password vừa nhập -> lấy thành công thông tin nạn nhân.

