**Bài Nghiên Cứu Tháng 7**

**Tấn công thông qua Excel 4.0 Macro**

1. **Khái niệm ?**

Excel 4.0 Macro là một chức năng macro được hỗ trợ trong các phiên bản Excel cũ hơn, như Excel 4.0 và Excel 5.0. Nó đã được thay thế bởi VBA (Visual Basic for Applications) trong các phiên bản Excel mới hơn. Tuy nhiên, Excel 4.0 Macro vẫn có thể được sử dụng và vẫn có thể làm cho tệp Excel dễ bị tấn công nếu không cẩn thận.

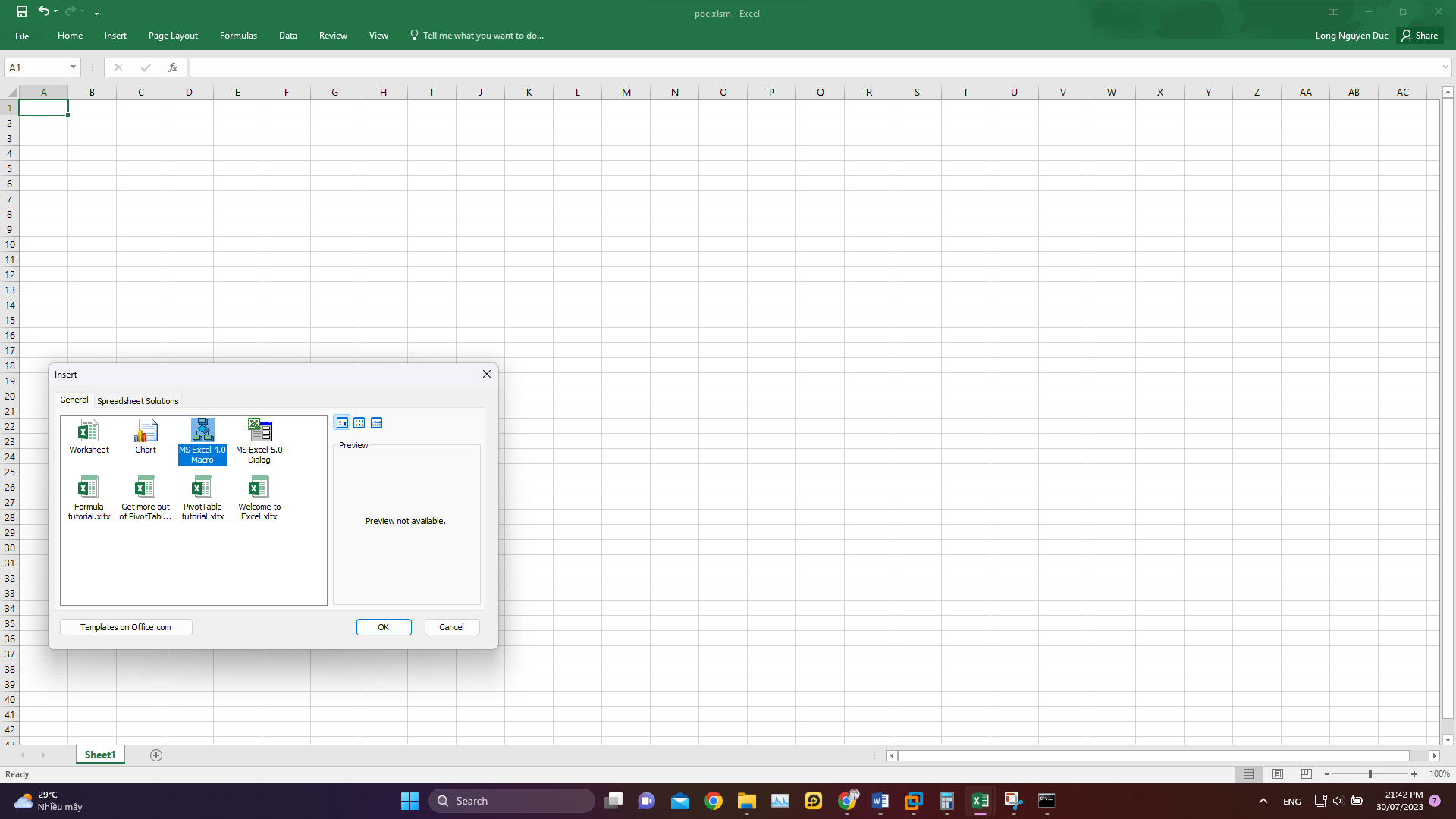
1. **Một số kiểu tấn công phổ biến:**

* Phishing: Kẻ tấn công có thể sử dụng Excel 4.0 Macro để chạy mã độc và thực hiện các cuộc tấn công phishing. Chẳng hạn, họ có thể giả mạo các tệp bảng tính và email giả mạo để lừa người dùng kích hoạt macro, từ đó thực hiện các hành động nguy hiểm.
* Thực thi mã độc: Kẻ tấn công có thể sử dụng Excel 4.0 Macro để thực thi mã độc trên máy tính của người dùng mà không cần sự đồng ý của họ. Điều này có thể dẫn đến mất dữ liệu, ảnh hưởng đến hiệu suất hệ thống hoặc thậm chí lây lan mã độc qua mạng nội bộ.
* Cài đặt Backdoor: Kẻ tấn công có thể sử dụng Excel 4.0 Macro để cài đặt backdoor trên hệ thống của người dùng, cho phép họ tiếp tục tấn công sau này.

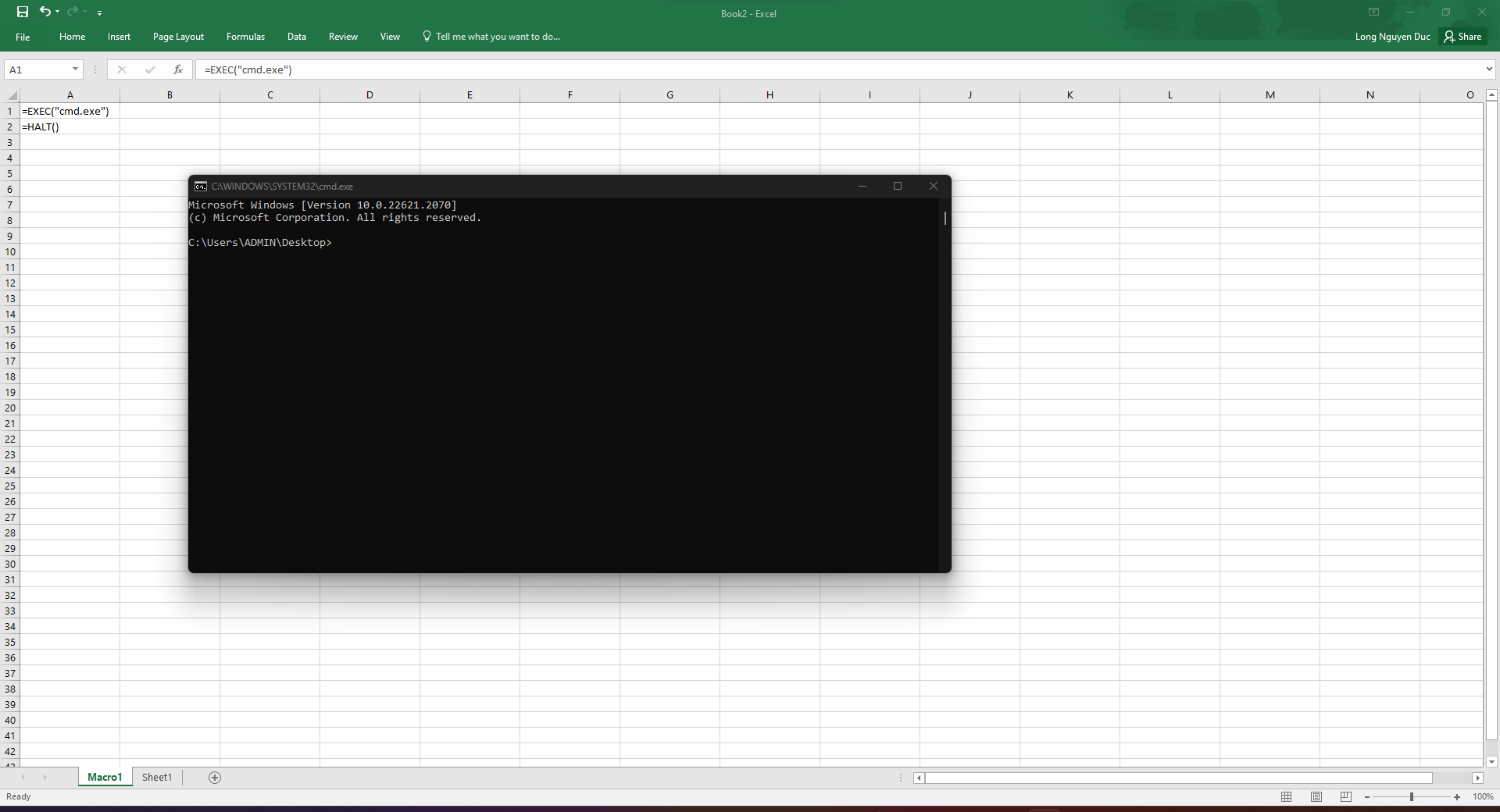
Kịch bản thường thấy khi người dùng bị gửi đến 1 email lừa đảo, sau đó ấn tải về và thực thi file excel có chứa mã độc đó.

1. **Demo tấn công**

* Tạo 1 file excel và sau đó insert Macro 4.0:



* Chạy thử hàm EXEC để mở cmd:



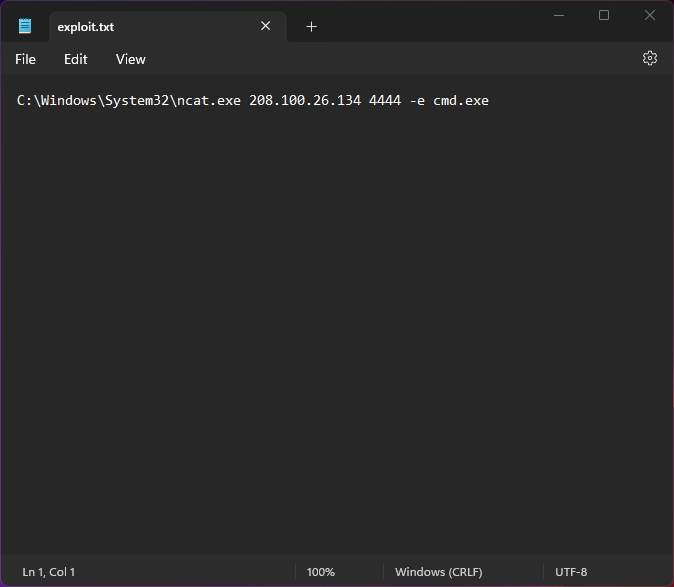
Trong Excel 4.0 Macro (đôi khi được gọi là XLM Macro), "EXEC" là một hàm (function) mà người dùng có thể sử dụng để thực thi các lệnh hoặc công thức tùy chỉnh trong ngôn ngữ Excel 4.0 Macro (XLM).

Excel 4.0 Macro là một phiên bản cũ hơn của ngôn ngữ lập trình macro trong Excel (được sử dụng trước khi VBA - Visual Basic for Applications - được giới thiệu). Điểm đặc biệt của XLM là nó sử dụng các công thức và hàm tùy chỉnh (custom functions) được xác định bằng cách sử dụng các ký tự đặc biệt và mã lệnh (thường là các chữ cái và số).

Trong Excel 4.0 Macro (XLM Macro), "HALT" là một lệnh (command) được sử dụng để dừng thực thi macro và kết thúc chương trình.

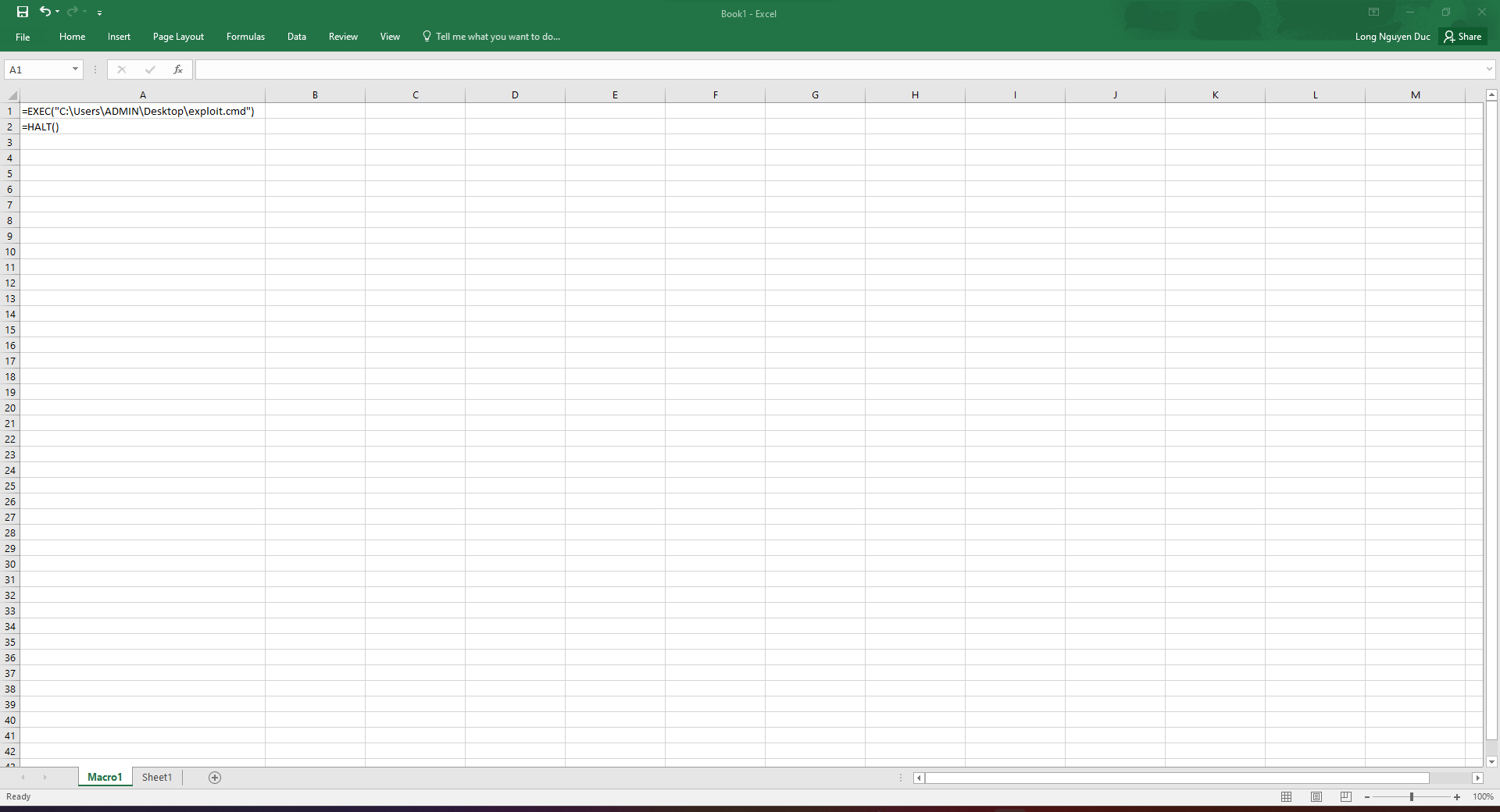
Dựa vào đó ta có thể sử dụng để thực thi 1 số câu lệnh.

* Tạo 1 file cmd có nội dung như sau

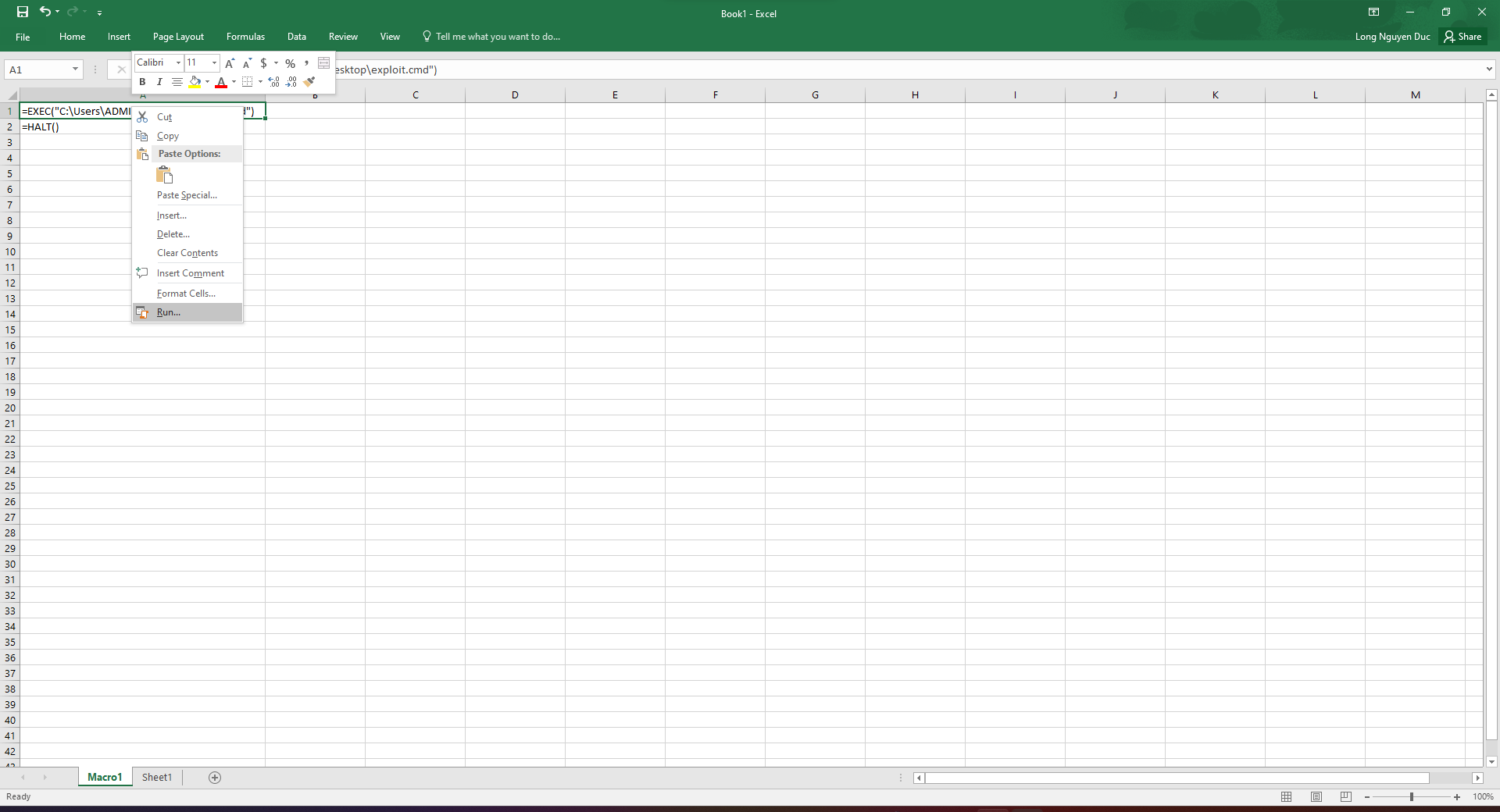


Nội dung file chạy ncat tạo kết nối ra bên ngoài để Hacker từ bên ngoài bắt kết nối đó và xâm nhập vào máy của nạn nhân

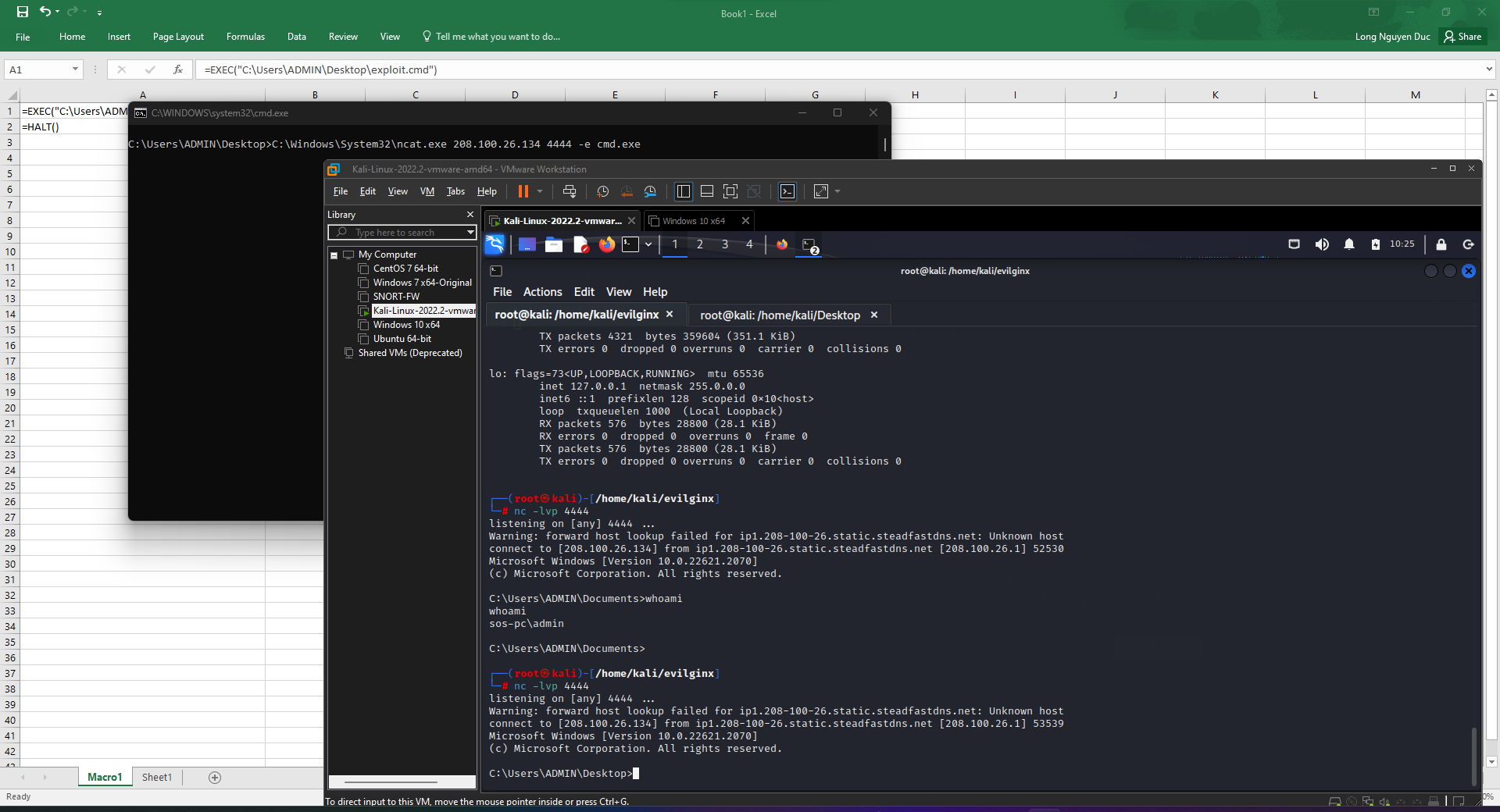
* Chỉnh sửa nội dung file excel để thực thi file exploit.cmd

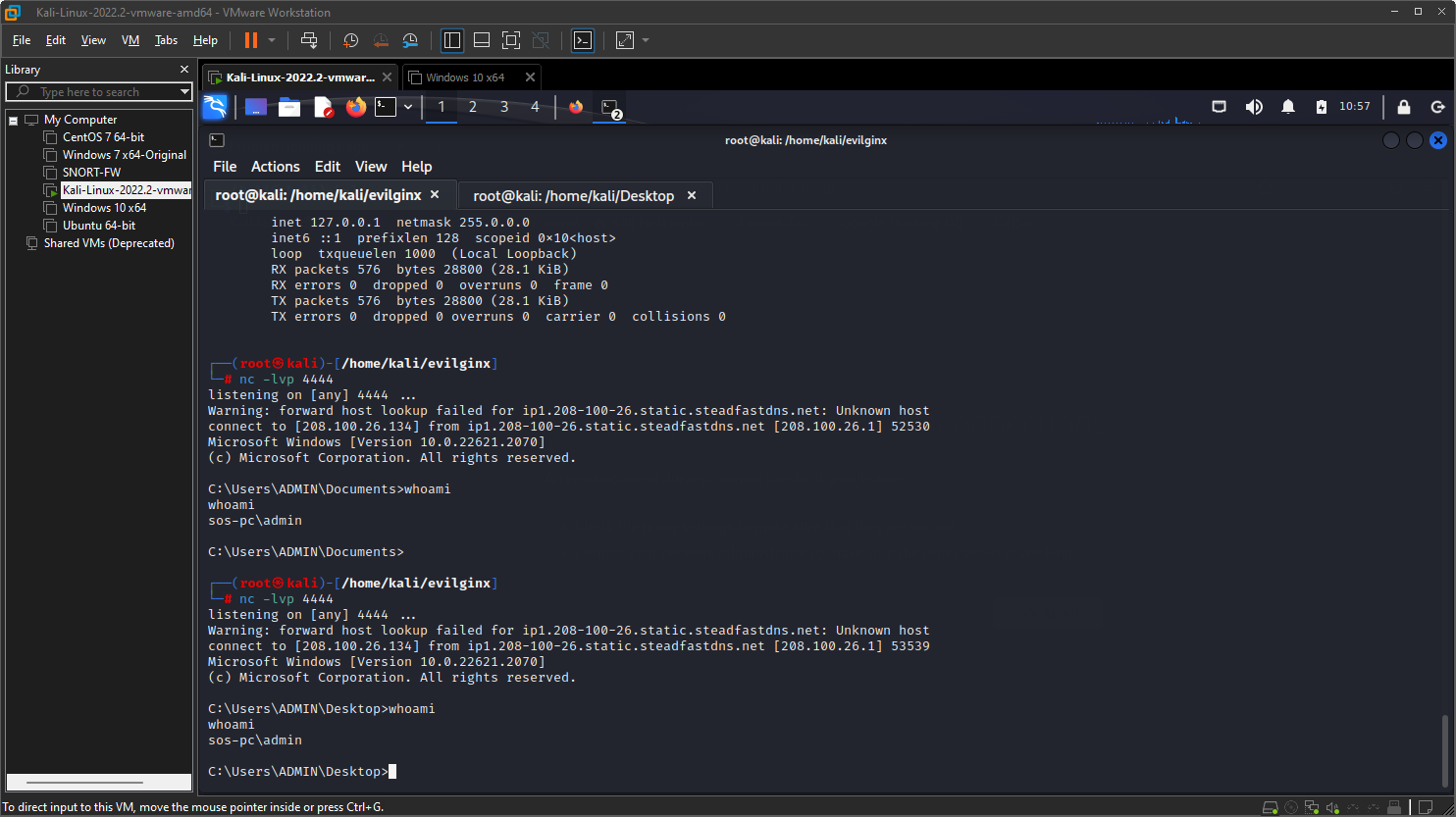


* Sau đó thực thi câu lệnh



* Thu được kết quả như sau: Hacker bắt được kết nối và xâm nhập máy của nạn nhân thành công và tiến hành kiểm tra thông tin





Khi tấn công Hacker có thể ẩn nội dung trong file excel để tránh bị nghi ngờ

1. **Để bảo vệ khỏi các tấn công thông qua Excel 4.0 Macro, bạn có thể thực hiện các biện pháp sau:**

* Tắt macro mặc định: Để ngăn người dùng không có kiến thức về Excel 4.0 Macro, bạn nên tắt macro mặc định trong các tệp bảng tính. Điều này sẽ ngăn chặn các mã độc tự động chạy khi tệp được mở.
* Không tin tưởng tệp không rõ nguồn gốc: Không mở các tệp Excel từ nguồn không rõ hoặc không tin tưởng. Đặc biệt, không nên mở các tệp tài liệu từ email không được xác định hoặc không yêu cầu.
* Cập nhật phần mềm và bảo mật: Luôn duy trì các phần mềm và bảo mật của hệ thống của bạn lên phiên bản mới nhất để tránh bị lợi dụng các lỗ hổng đã biết.
* Sử dụng phiên bản mới hơn của Excel: Hạn chế sử dụng các phiên bản cũ của Excel như Excel 4.0, thay vào đó, nên sử dụng các phiên bản mới hơn có hỗ trợ bảo mật và tích hợp hơn, như Microsoft Excel 365.
* Kích hoạt chế độ bảo mật: Kích hoạt chế độ bảo mật trong Excel để ngăn người dùng chạy các macro không an toàn không được xác nhận.