# Mục tiêu:

Sử dụng mô-đun khai thác Metasploit psexec để triển khai một tải trọng Meterpreter đến một máy Windows mục tiêu bằng cách sử dụng phiên SMB được xác thực

Khám phá khả năng của Meterpreter để lấy đặc quyền và dump các băm từ máy mục tiêu

Metasploit là một công cụ kiểm tra và khai thác lỗ hổng bảo mật trong hệ thống máy tính. Nó là một nền tảng kiểm thử thâm nhập được sử dụng rộng rãi bởi các chuyên gia an ninh mạng và các nhà nghiên cứu bảo mật để phát hiện và khai thác lỗ hổng bảo mật trong mạng, ứng dụng, và hệ điều hành.

Metasploit cung cấp một loạt các công cụ và tính năng để thực hiện các hoạt động kiểm thử thâm nhập, bao gồm:

**Kiểm thử lỗ hổng**: Metasploit cho phép bạn tìm kiếm lỗ hổng bảo mật trong hệ thống bằng cách sử dụng các module kiểm thử mà người dùng có thể cài đặt và chạy.

**Khai thác lỗ hổng**: Metasploit cung cấp các công cụ để tự động khai thác các lỗ hổng được tìm thấy. Các kỹ thuật này có thể được sử dụng để kiểm tra tính khả dụng và độ tin cậy của hệ thống.

**Quản lý tác vụ:** Metasploit cung cấp giao diện dòng lệnh và giao diện đồ họa cho việc quản lý các tác vụ kiểm thử thâm nhập, bao gồm việc lưu trữ kết quả, phân tích dữ liệu và tạo báo cáo.

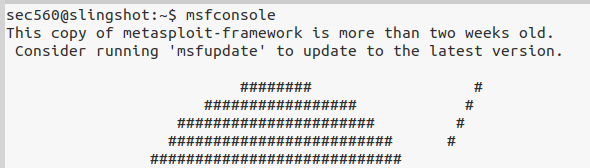
**Meterpreter** là một payload được sử dụng rộng rãi trong tấn công hệ điều hành Windows. Nó thường được áp dụng trên hầu hết các phiên bản của Windows hiện nay. Sau khi khai thác thành công, Meterpreter trở thành một remote shell (chương trình nhập lệnh điều khiển từ xa) cho phép người tấn công thực hiện các thao tác sau:

**Không tạo tệp trên đĩa cứng**: Meterpreter tồn tại trong bộ nhớ và tự gắn vào một tiến trình.

**Giao tiếp máy khách-máy chủ ở dạng TLV (kiểu-độ dài-giá trị**): Điều này cho phép truyền thông tin giữa máy tấn công và máy mục tiêu.

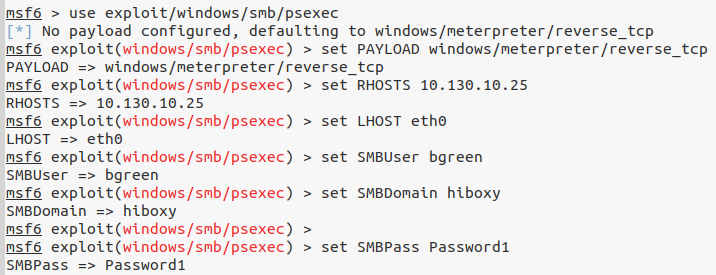
**Thực hiện các hành động trên hệ thống**: Bao gồm thao tác với tệp tin, mạng, và thậm chí chạy các tập lệnh 12.

# 1. Launch Metasploit

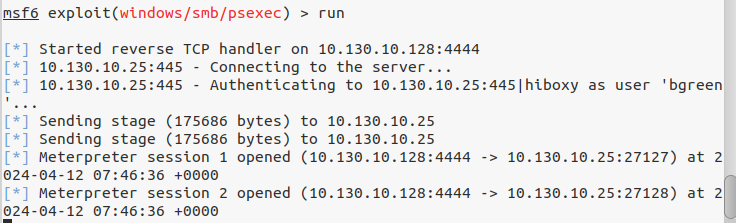


Trong Metasploit, exploit/windows/smb/psexec là một module sử dụng để thực hiện tấn công kiểu "Pass the Hash" trên hệ thống Windows thông qua dịch vụ SMB (Server Message Block).

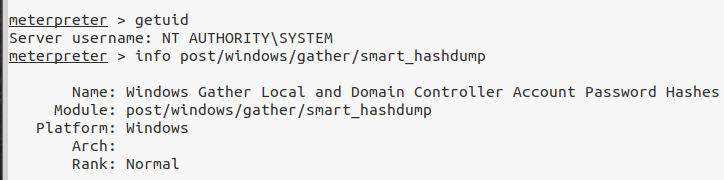
Sử dụng một bản sao của mã hash mật khẩu (password hash) để xác thực mà không cần biết mật khẩu thực sự

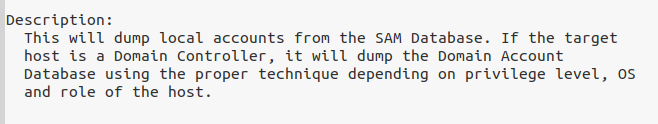


# 2. Launch the attack

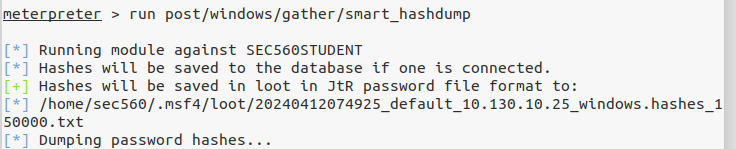


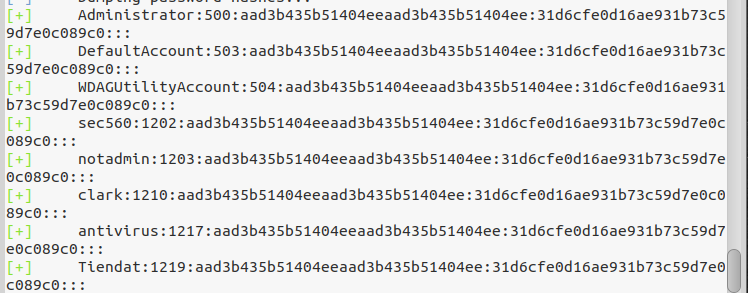
-Xem mk đang chạy ở quyền nào





Sử dụng module post/windows/gather/smart\_hashdump để trích xuất các password hash từ remote system.

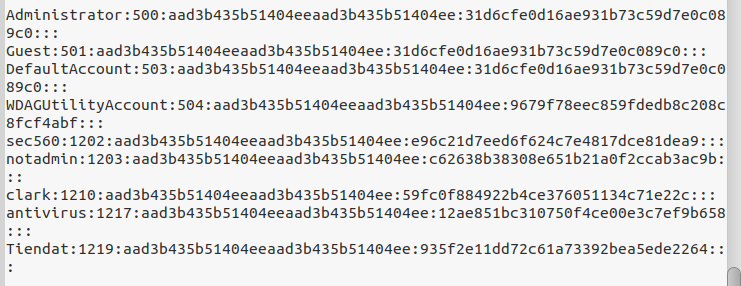




Thấy lệnh này cố gắng lấy gợi ý mật khẩu từ hệ thống nếu bất kỳ người dùng nào đã configure tài khoản bằng gợi ý mật khẩu.

Thấy các giá trị băm NT (phần 2) là 31d6c…: đây là NT hash NULL. Module này không hoạt động ở đây nhưng hoạt động trên domain controller

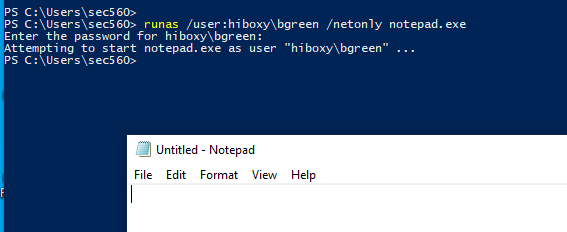




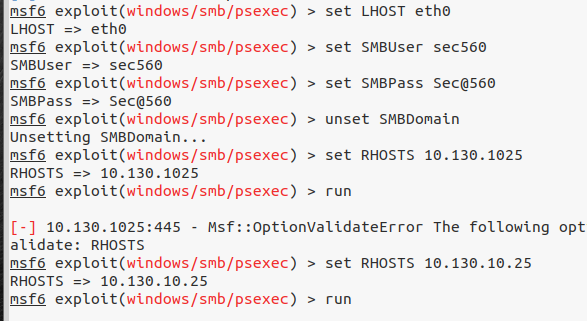
# 4. Mimikatz setup

Mimikatz là một module sau khai thác (post-exploitation) trong Metasploit, thực hiện Tấn công thu thập thông tin đăng nhập, Tấn công Pass-the-Hash, Tấn công Pass-the-Ticket. để dump mật khẩu từ bộ nhớ (có thể ở dạng cleartext).

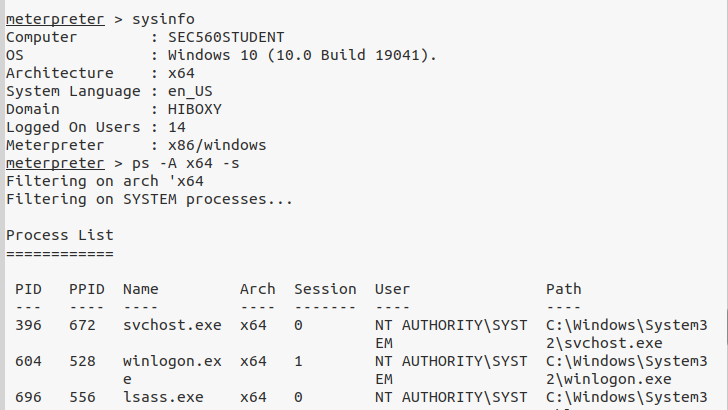
Chuyển sang máy Win, tải một số thông tin xác thực của domain user vào bộ nhớ. Giả vờ như bgreen đã đăng nhập vào hệ thống.



# 5. Running mimikatz

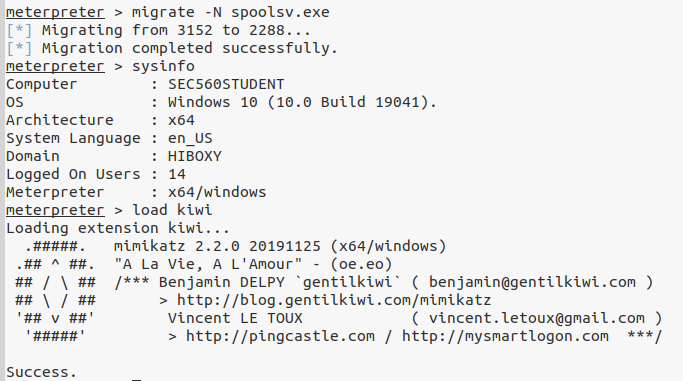


Ta thấy hệ thống mục tiêu có cấu trúc x64 nhưng bản thân process Meterpreter đã là 32-bit. Giờ sẽ tìm các process 64 bit đang chạy với quyền cấp system



Ta thấy hệ thống mục tiêu có cấu trúc x64 nhưng bản thân process Meterpreter đã là 32-bit. Giờ sẽ tìm các process 64 bit đang chạy với quyền cấp system

Sau khi đã khớp nhau, bất đầu chạy kiwi



Giờ thì lấy password từ RAM bằng câu lệnh

