- Sử dụng cuộc tấn công pass-the-hash thông qua mô-đun psexec của Metasploit để tải Meterpreter vào máy mục tiêu

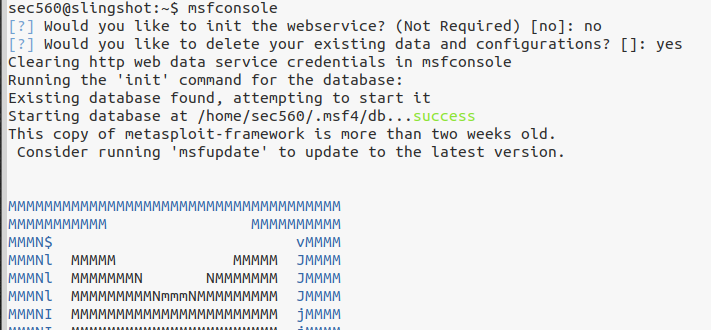
- Xem cách chúng ta có thể xác thực vào một máy Windows mục tiêu chỉ bằng hash, mà không cần sử dụng mật khẩu thực sự hoàn toàn

# Mục tiêu:

Sử dụng kỹ thuật pass-the-hash thông qua module psexec của Metasploit để tải Meterpreter lên máy mục tiêu. Từ đó hiểu được cách hoạt động của Pass the Hash (xác thực bằng bản băm thay vì bản rõ của mật khẩu)

# 1. Obtaining hashes

-Mở metasploit

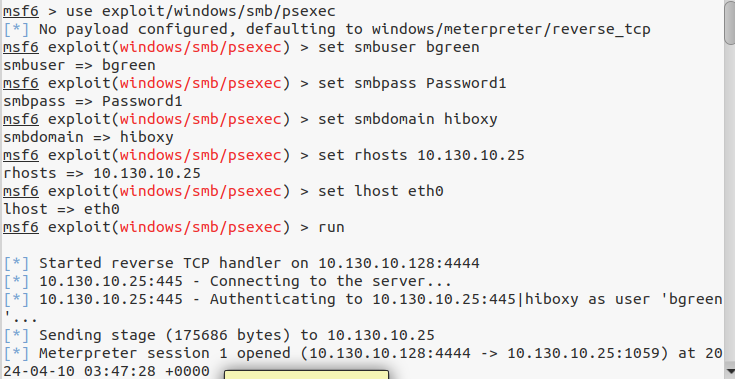


-Sử dụng module psexec

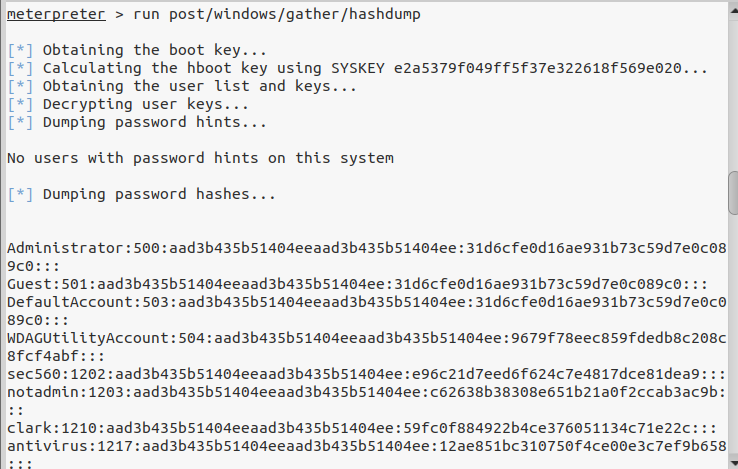
Sử dụng mô-đun khai thác Metasploit psexec để triển khai một tải trọng Meterpreter đến một máy Windows mục tiêu bằng cách sử dụng phiên SMB được xác thực

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

-Cài đặt thông tin máy cần tấn công và chạy

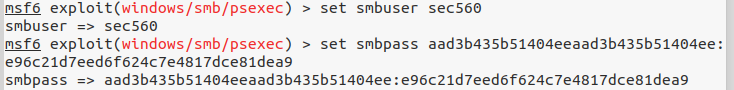


Chạy module để lấy hash



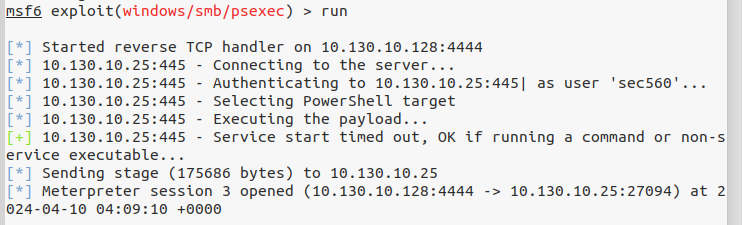
# 2. Using the hashes

-Cài đặt thông tin máy nạn nhân: user sec560 và hash của pass





# 3. Exploit

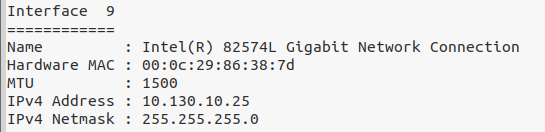


# 4. Meterpreter shell

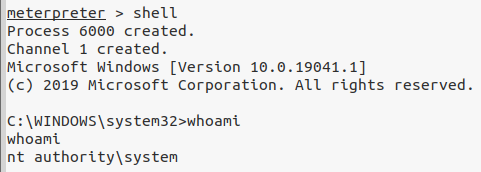
Xem thông tin về máy







Mở shell lên để kiểm tra



-Thêm user thành công

