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.

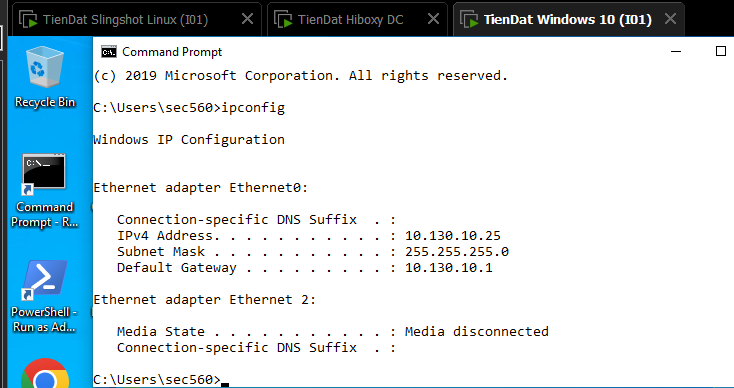
**Giao tiếp máy khách-máy chủ ở dạng TLV (kiểu-độ dài-giá trị**): Điều này cho phép truyền thông tin giữa máy tấn công và máy mục tiêu.

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

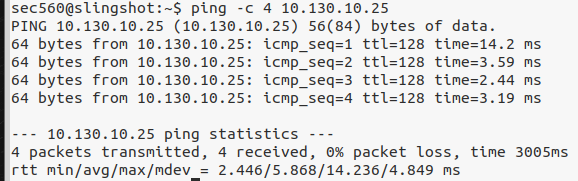
# Mục tiêu Lab 2.2:

Trong lab này, ta tiến hành phân tích Meterpreter và sử dụng Metasploit để triển khai một loại payload vào một lỗ hổng hiện có trên máy window. Cụ thể là dịch vụ Icecast - một máy chủ phát trực tuyến đa phương tiện trên Internet và có một lỗ hổng tràn bộ đệm. Payload trong metasploit sẽ gồm có Meterpreter stage, được truyền qua reverse\_tcp stager, tạo ra một kết nối từ máy bị tấn công đến máy tấn công.

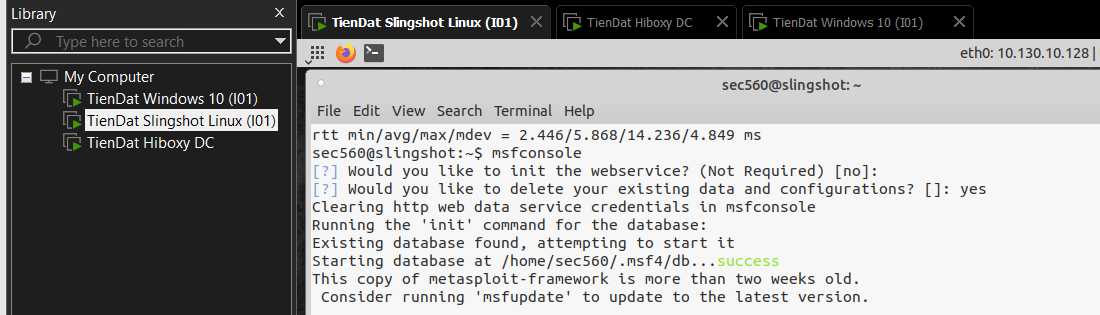
-Địa chỉ Ip của windows 10

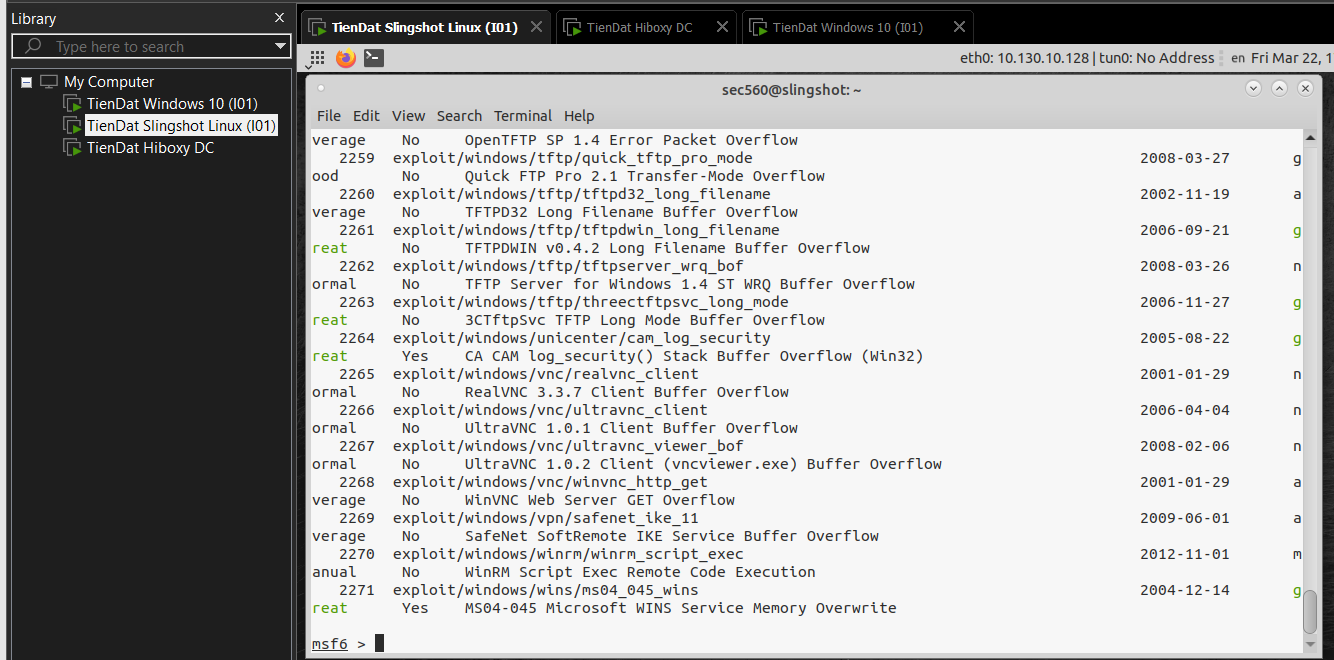


-Ping kiểm tra kết nối từ slingshot đến windows 10



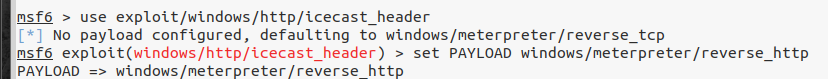
# 1.Metasploit on Linux

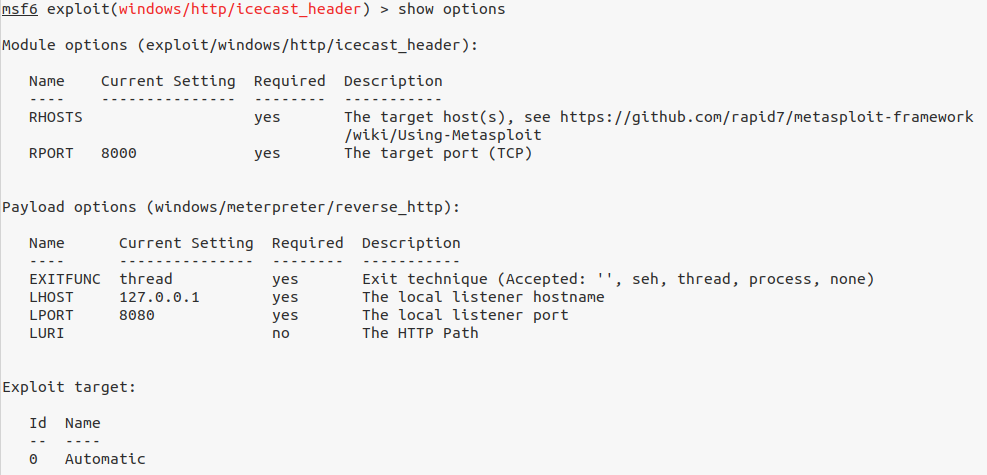


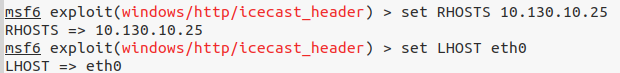


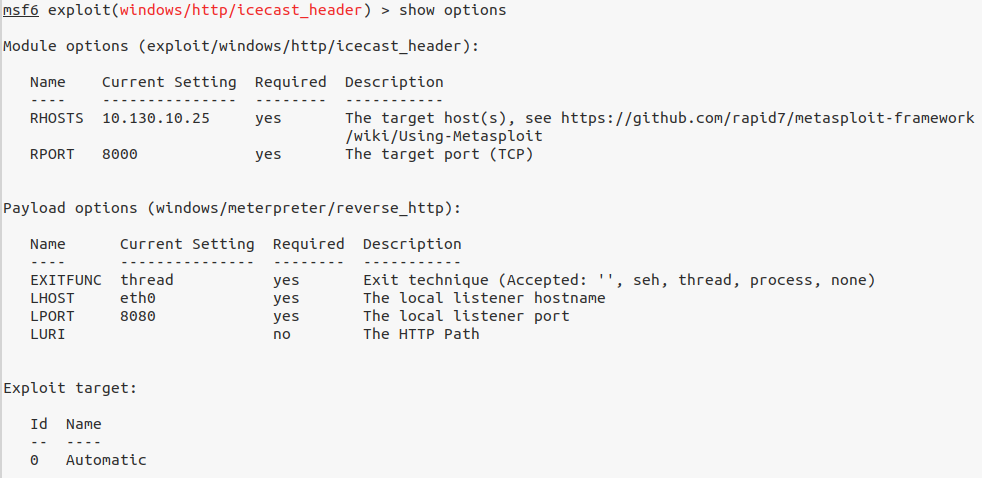


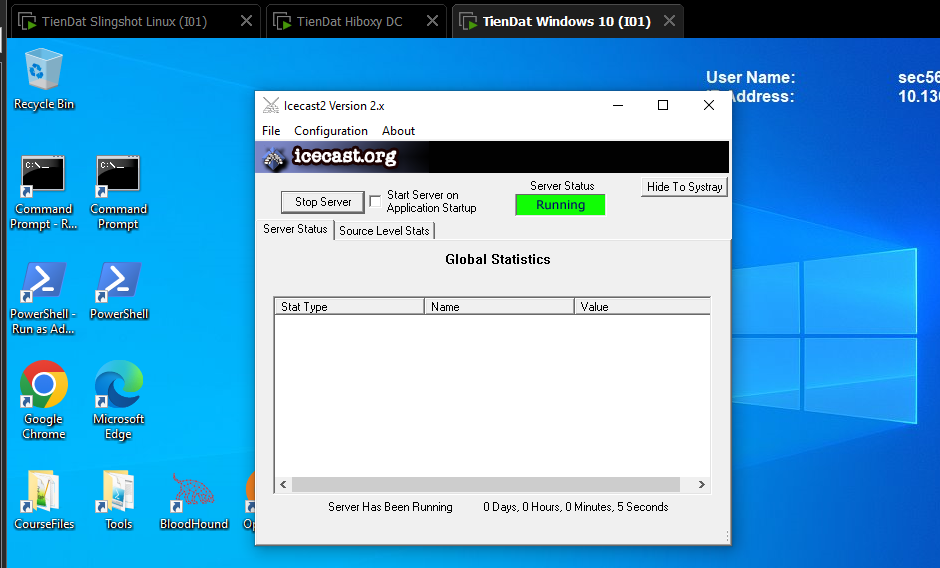
module exploit/windows/http/icecast\_header là một exploit được thiết kế để tận dụng một lỗ hổng trong dịch vụ Icecast trên các hệ thống Windows thông qua HTTP. Icecast là một máy chủ streaming âm nhạc mã nguồn mở, thường được sử dụng để truyền phát các đài phát thanh trực tuyến.

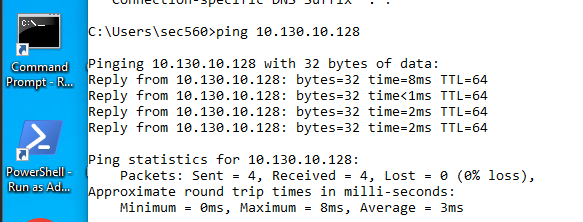




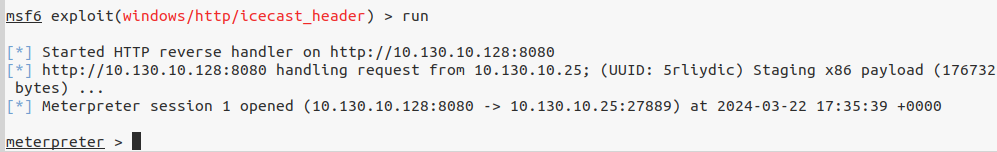








# 2. Launch the attack



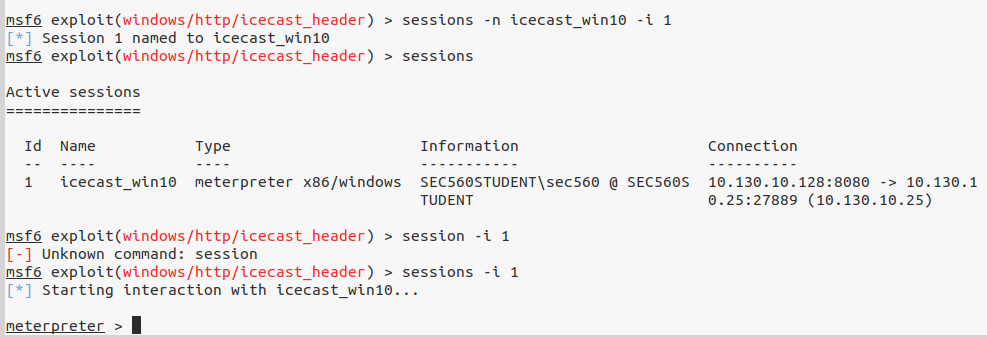
# 3.Sessions



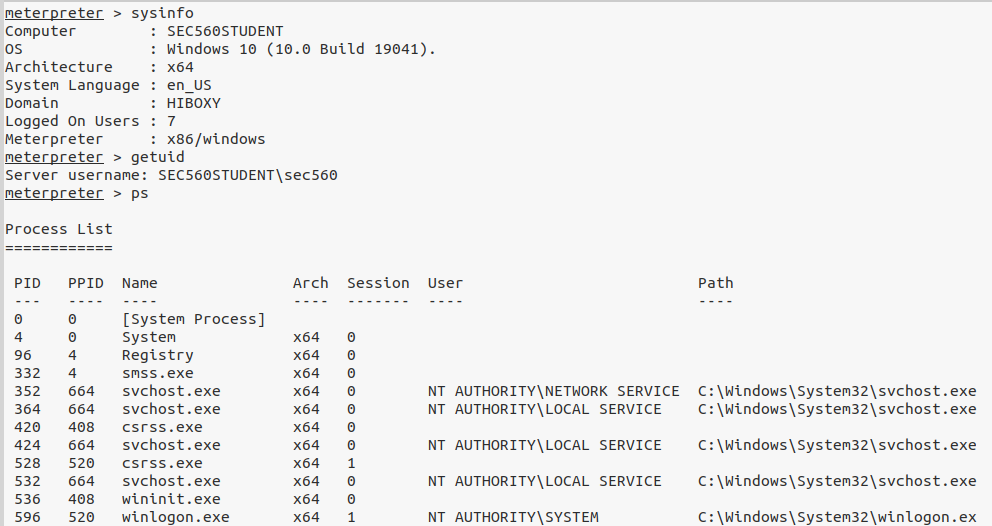
-Đặt tên session là icecast\_win10

-Sessions -i 1: chọn phiên đang chạy trên máy chủ mục tiêu mà bạn đã khai thác thành công.

Ở vd chỉ có 1 session nên số phiên =1

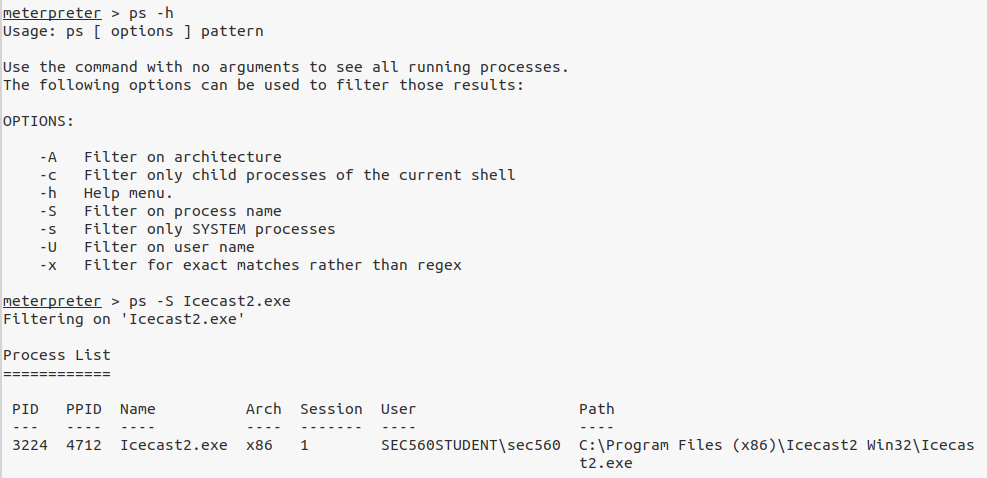


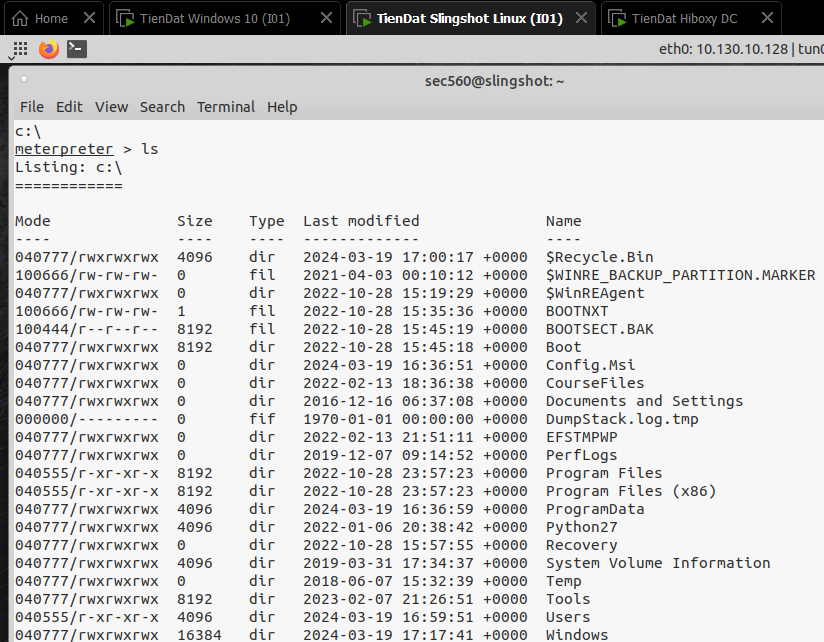
# 4.Metepreter



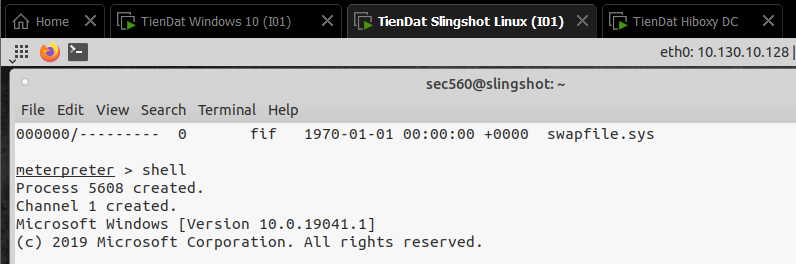
-ps -h: xem các tiến trình đang chạy

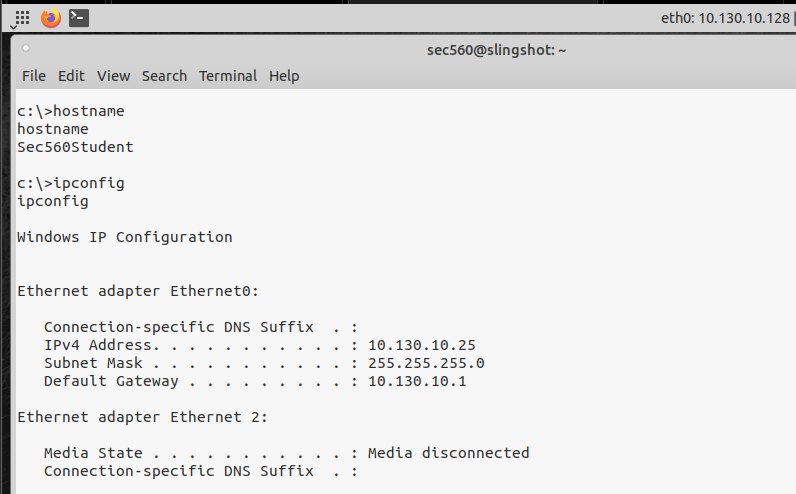
-ps -S Icecast2.exe: xem thông tiến trinh Icecast2.exe

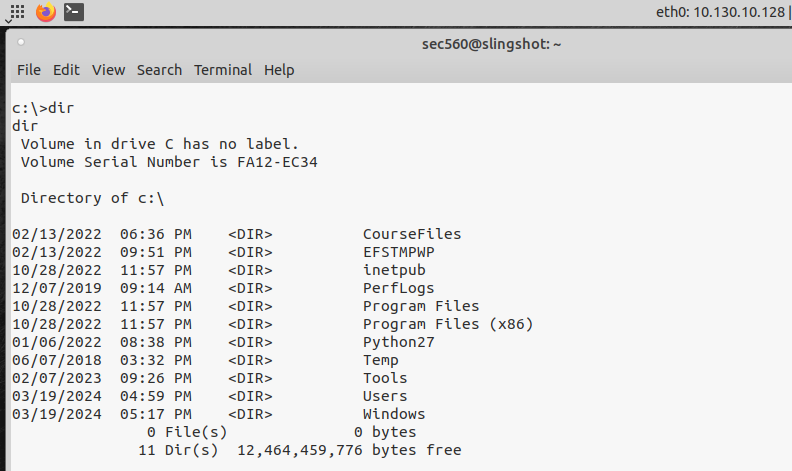




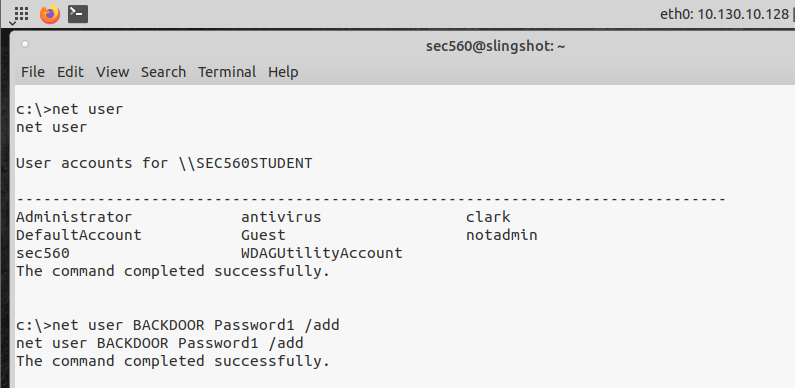
# 5. shell

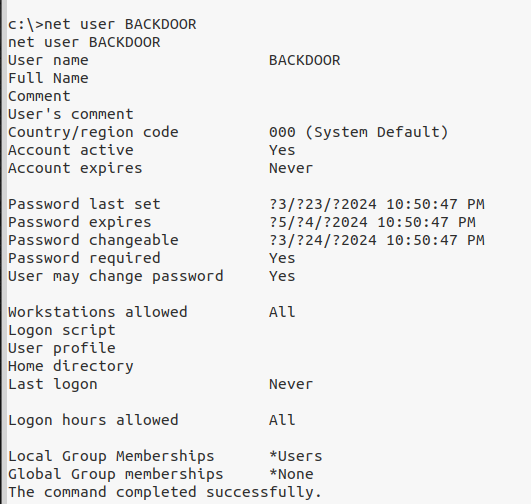


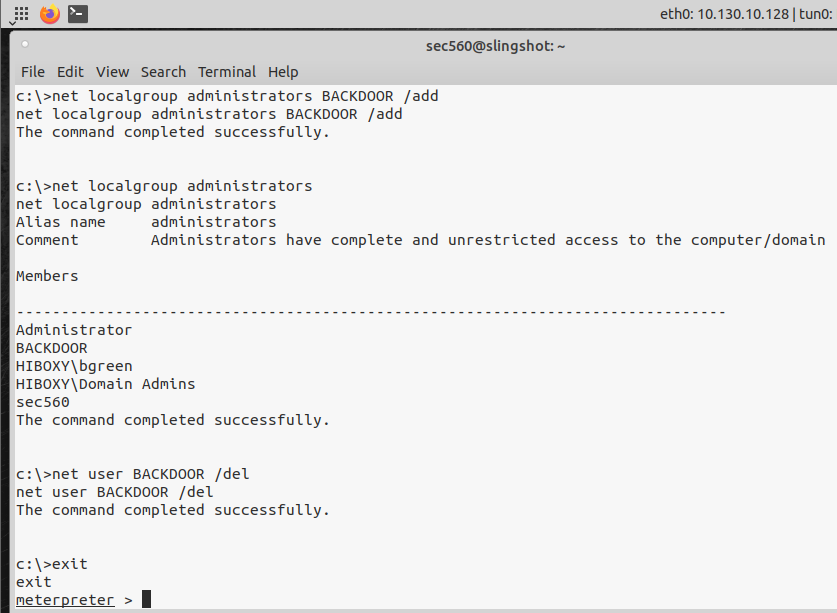




-Net user xem các user trong nhóm admin







# 6. More meterpreter fearture



7.Keystroke Logging

