Sliver là một công cụ kiểm thử thâm nhập và quản lý hệ thống từ xa mã nguồn mở, được thiết kế để cung cấp quyền kiểm soát hoàn toàn trên máy tính mục tiêu. Nó cho phép người dùng tạo ra các payload độc lập và linh hoạt, cung cấp một loạt các chức năng như mở một phiên dòng lệnh đầu vào từ xa (reverse shell), thu thập thông tin hệ thống, và triển khai mã độc hại.

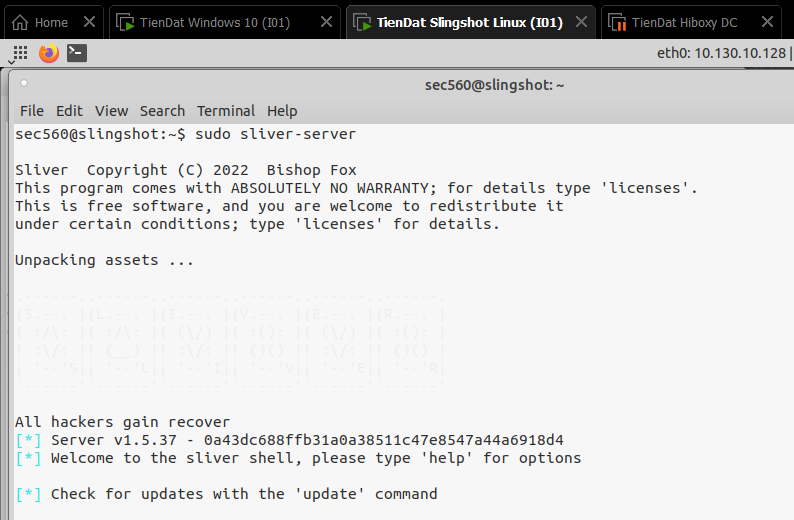
# Mục tiêu Lab 2.3:

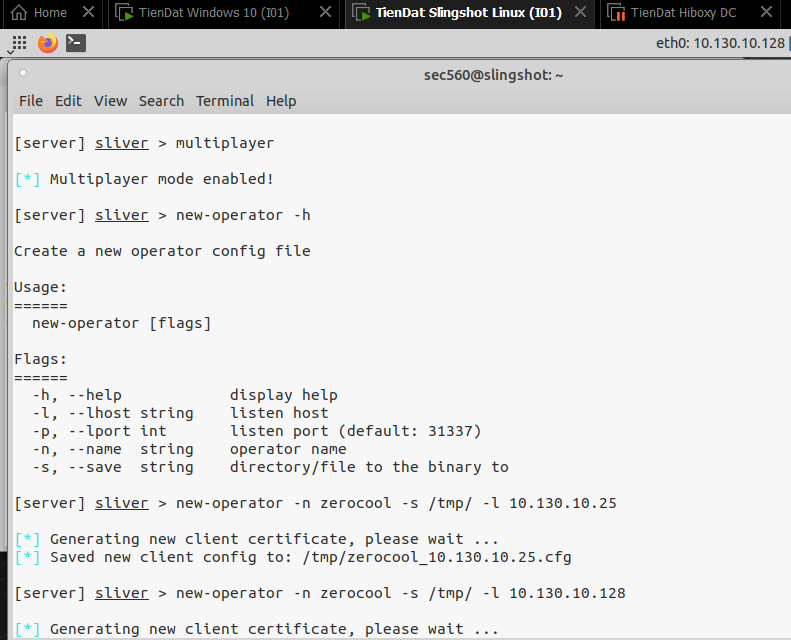
Làm quen với công cụ Sliver

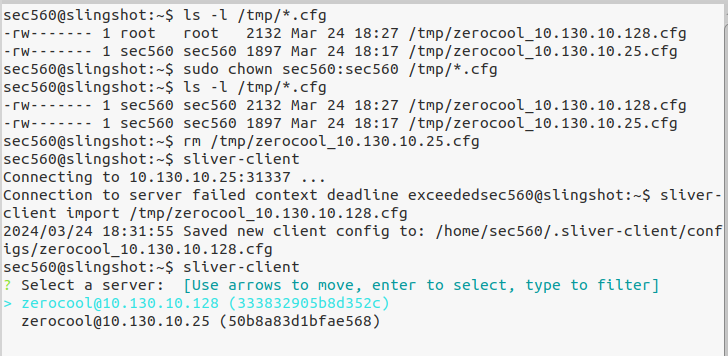
Tạo một trình nghe (listener) và payload để kết nối với trình nghe.

Sử dụng một số phần mềm của Sliver, cụ thể là execute-assembly

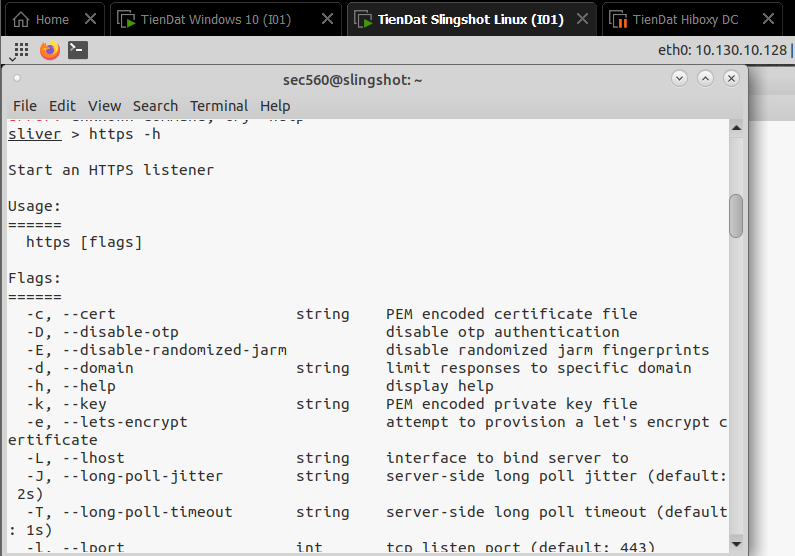
# 1. Start Sliver

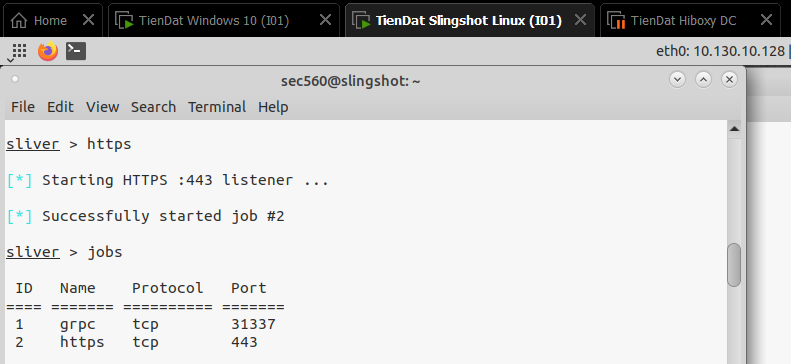


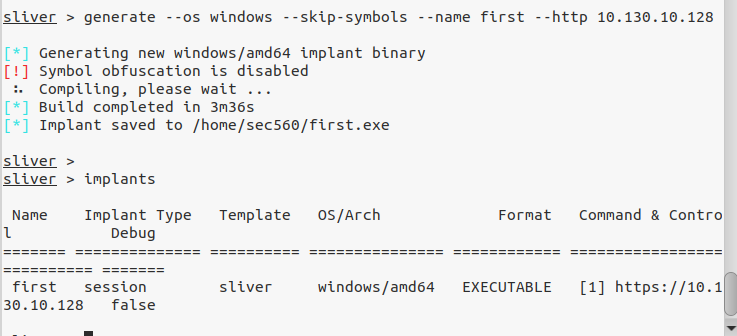




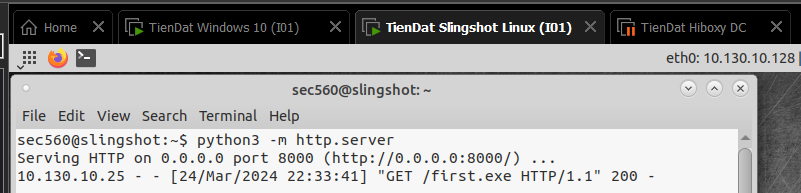
# 2. Creating a listener and an implant payload

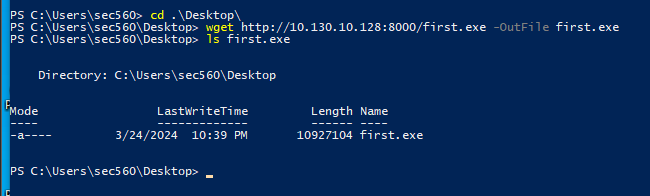




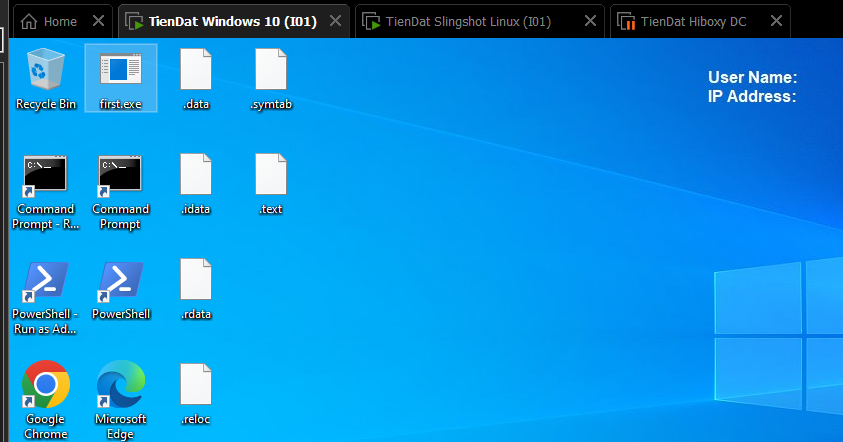


# 3. Sending the Payload to the Windows system

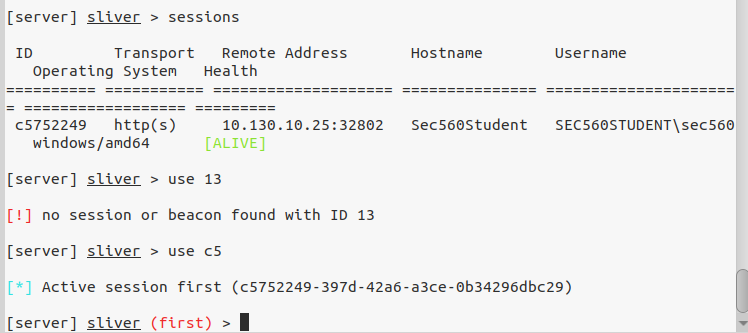




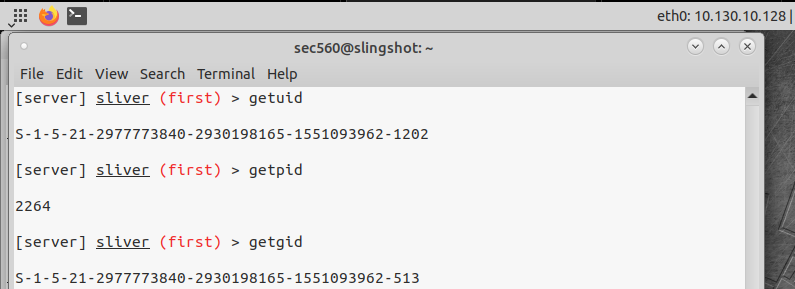
# 4. Executing the Payload

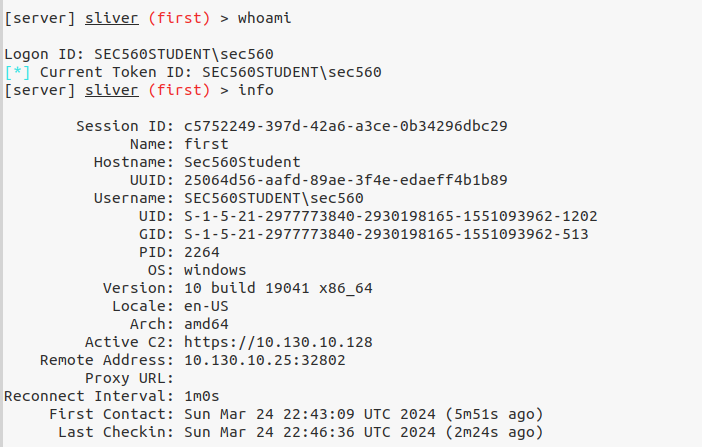




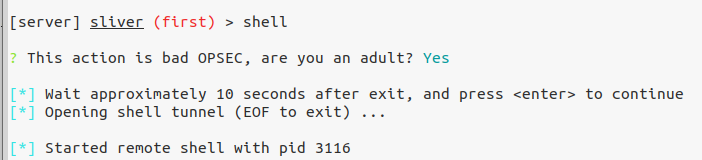


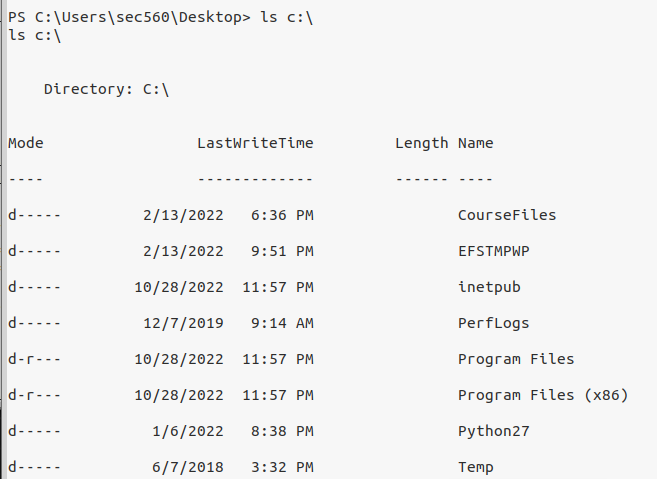
# 5. Interacting with the session

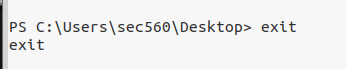




# 6. shell







# 7. Execute Assembly – SharpWMI

