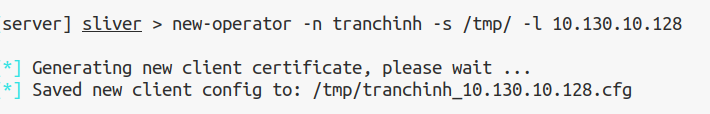
1. **Starting sliver**

Khởi động sliver server và bật chế độ muiltiplayer



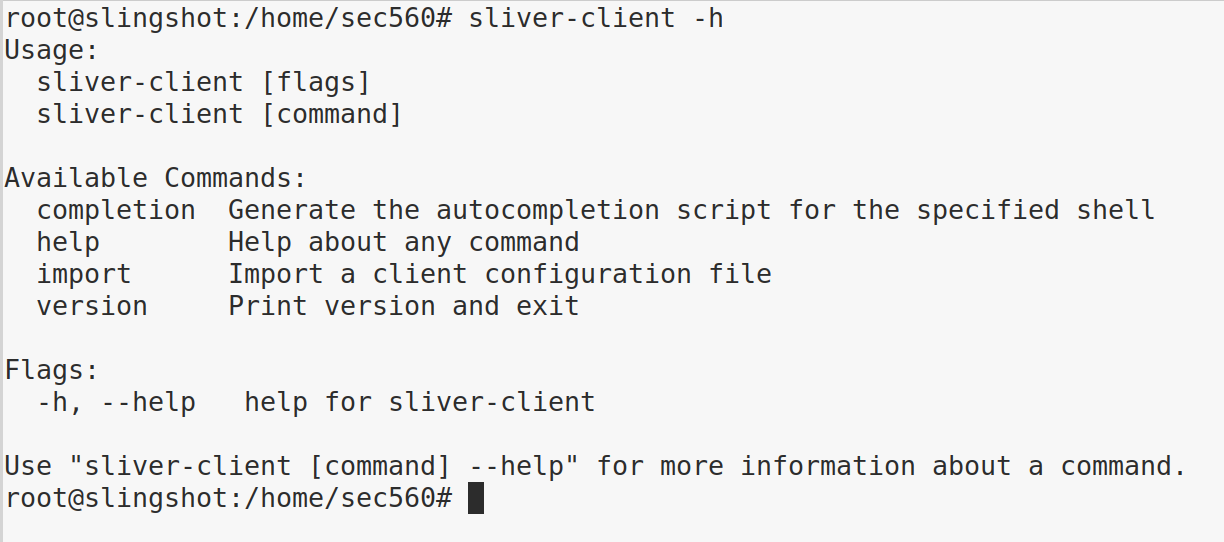
Tạo người dung mới tranchinh từ phía client. Cách này sẽ giúp chúng ta tạo 1 operator offline và kết nối sau

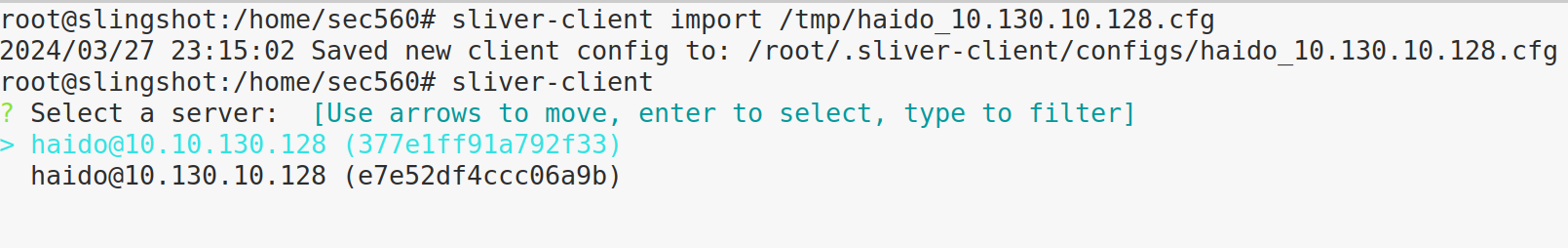


Xem quyền của file cấu hình của người dung mà mình vừa tạo. Có thể thấy file được tạo có quyền sở hữu của root và chỉ những root mới đọc được. Vậy nên ta hãy chuyển quyền đó thành của nguiowf dung sec560



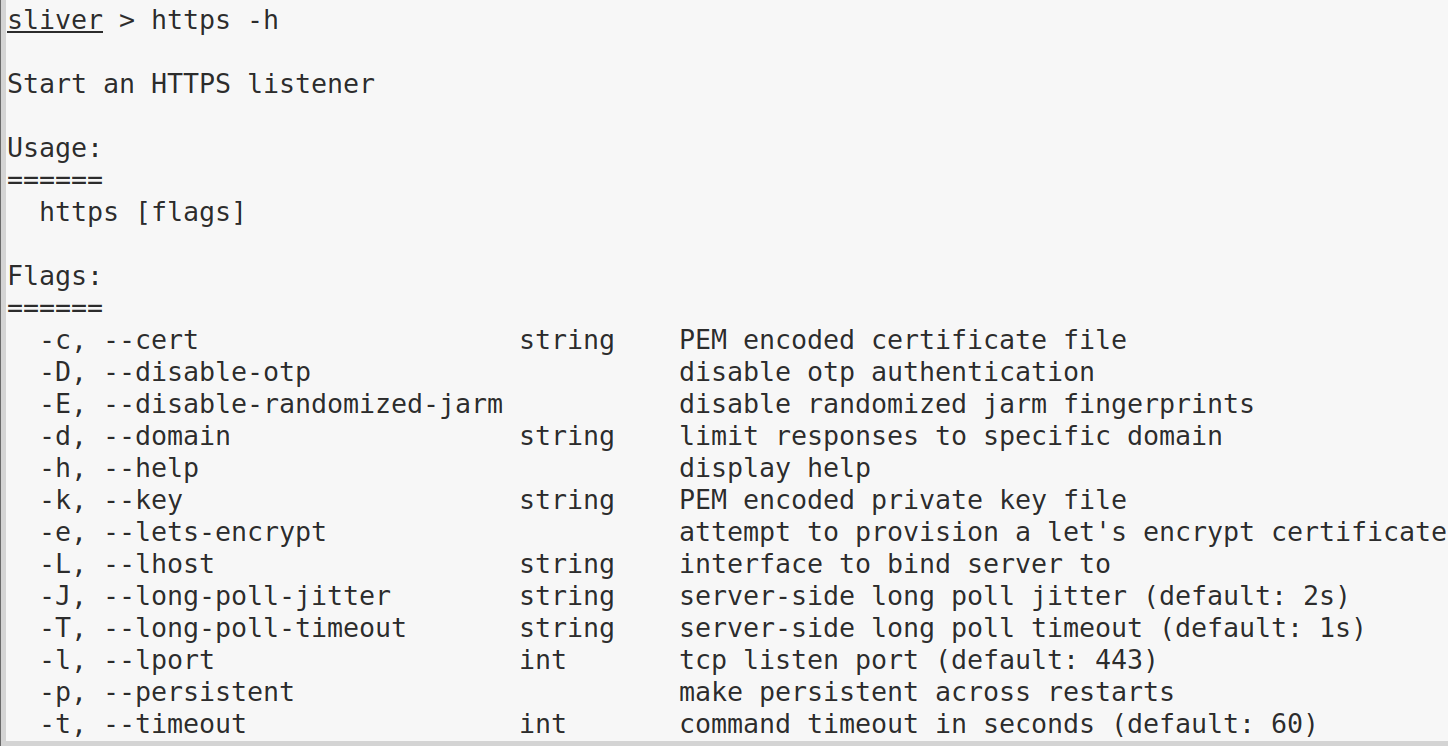
Chạy sliver-client và import file cấu hình vừa tạo

****

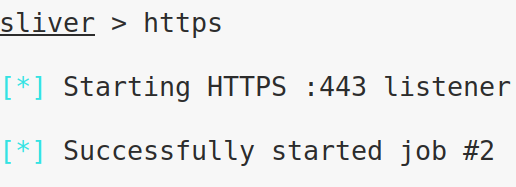
****

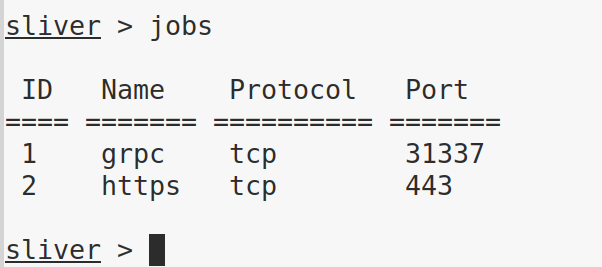
Như thế là ta có thể thành công kết nối tới sliver server

**2. Creating a listener and an implant payload**

****

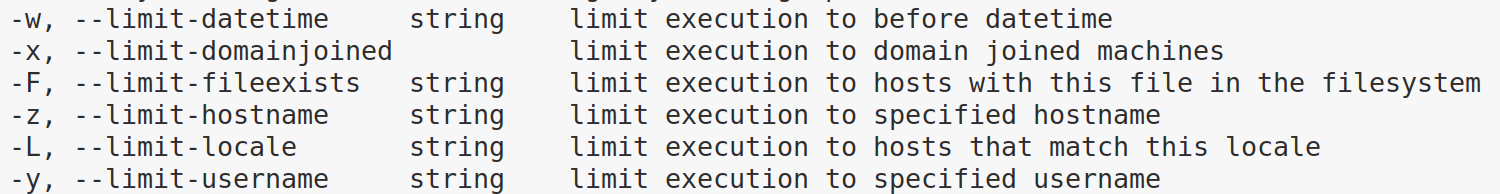
Use https listener

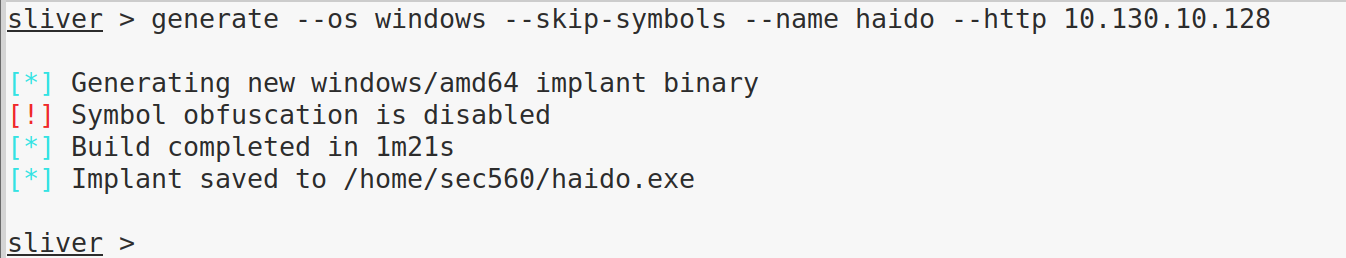
****

****

Có 2 job ở đây với job thứ nhất là sử dụng cho remote user(multiplayer)

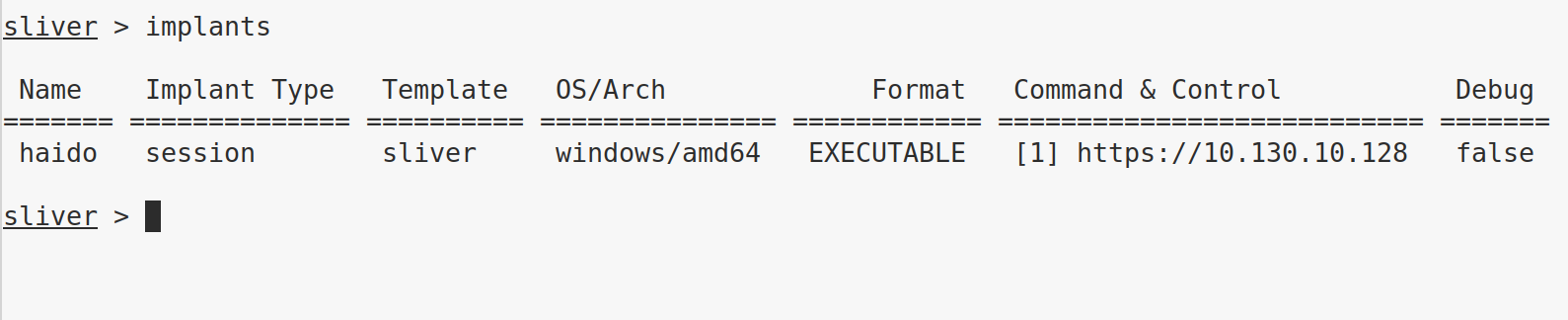
**Generate -h**

****

****

--os windows

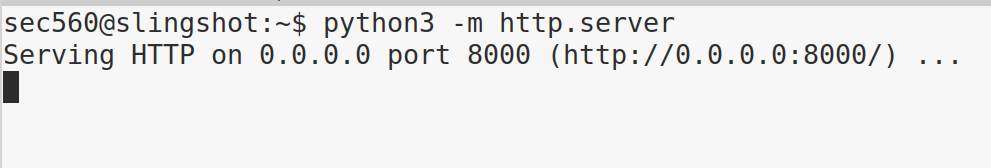
--skip-sym `bols: bỏ qua việc mã hóa hay che giấu payload để tang tốc độ

****

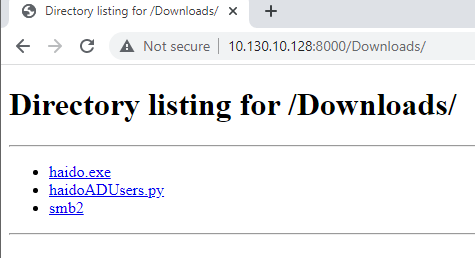
Thành công tạo ra 1 implant

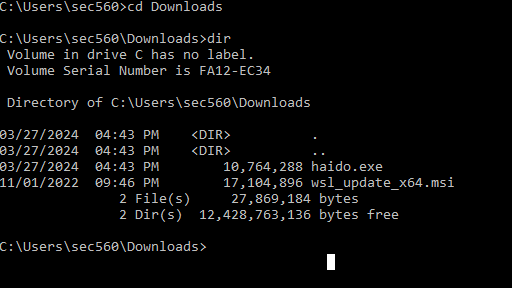
**3. Sending the Payload to the Windows system**

Dùng python3 để mở 1 http server với port mặc định 8000

****

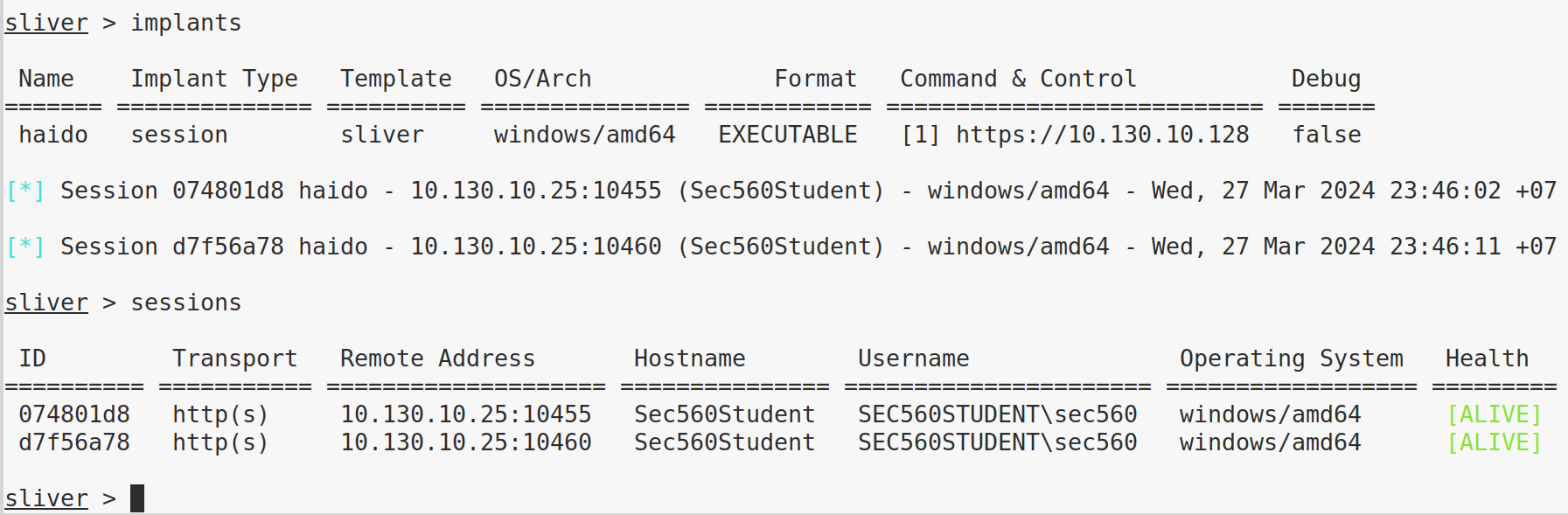
Tải file về máy window

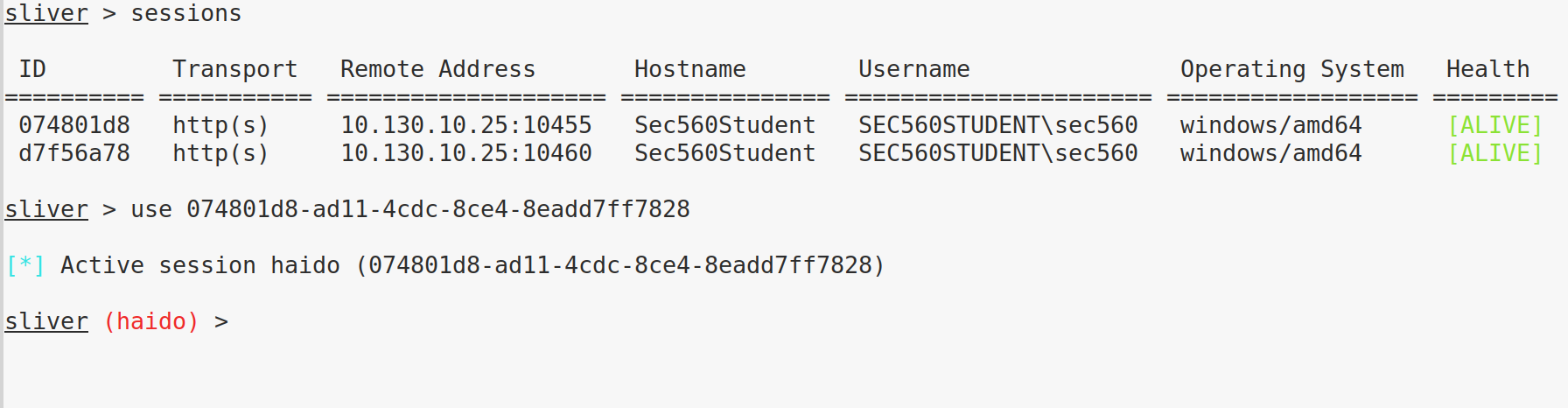
****

****

**4. Executing the Payload**

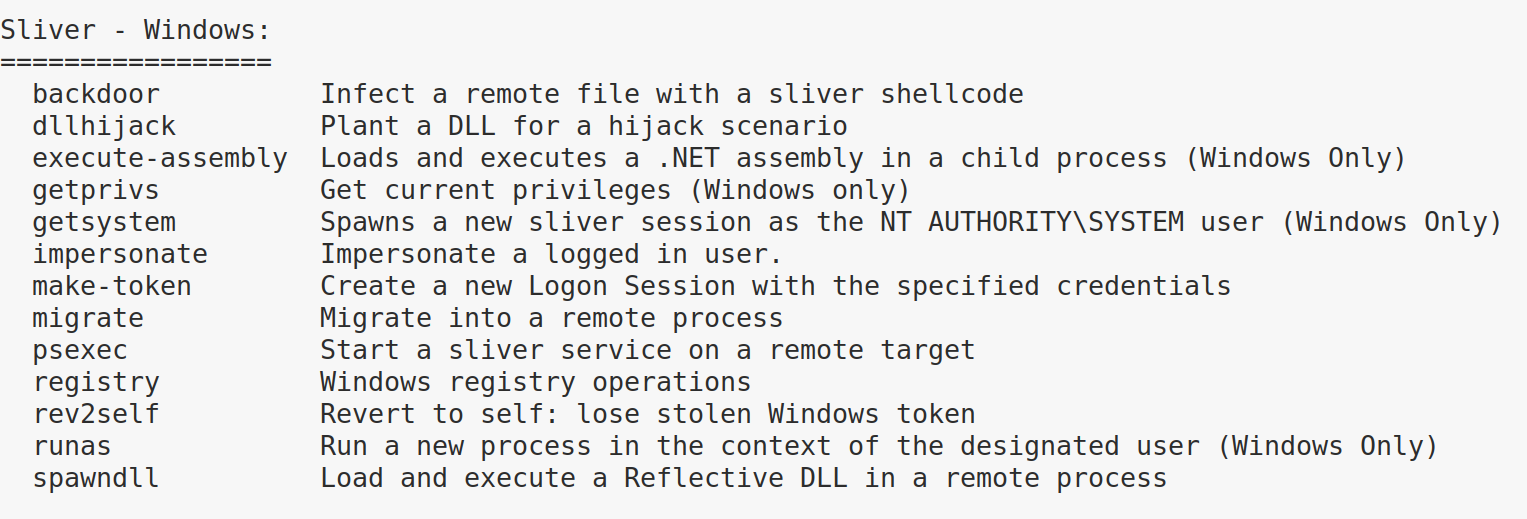
Tại máy window thực hiện chạy file vừa tạo

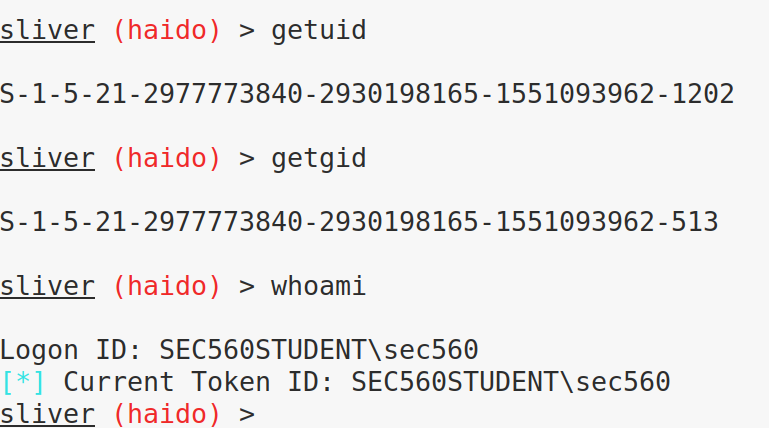
****

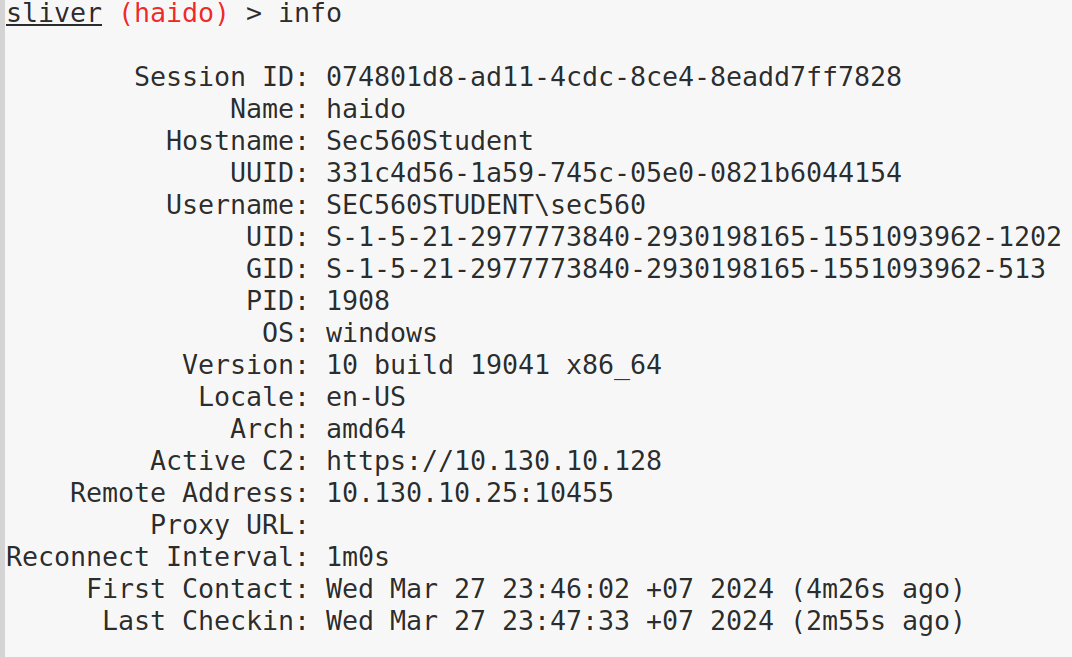
****

Thành công tạo 1 session

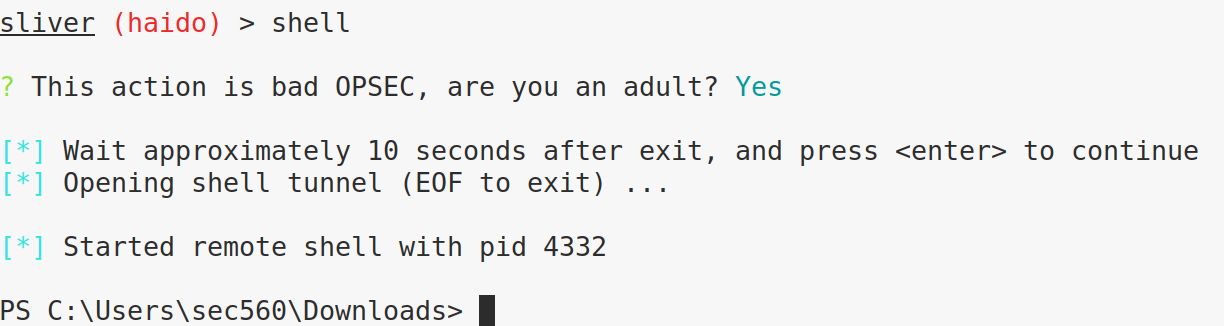
**5. Interacting with the session**

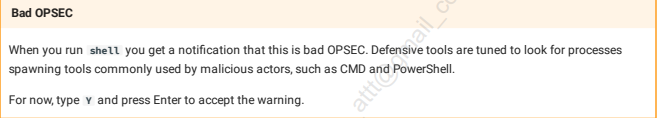
****

****

****

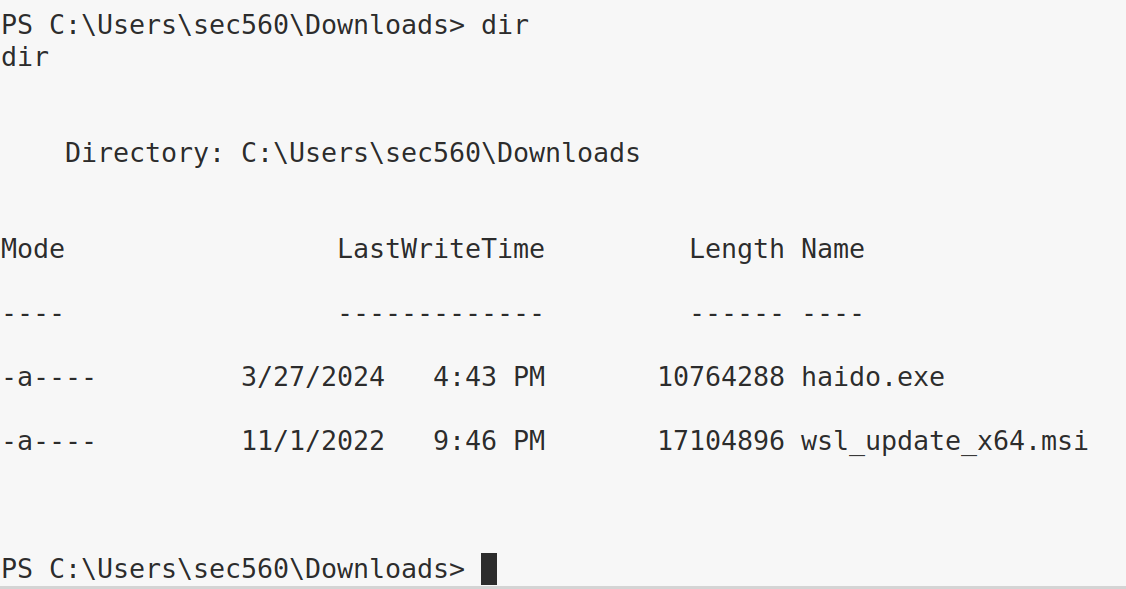
**6. Shell**

****

****

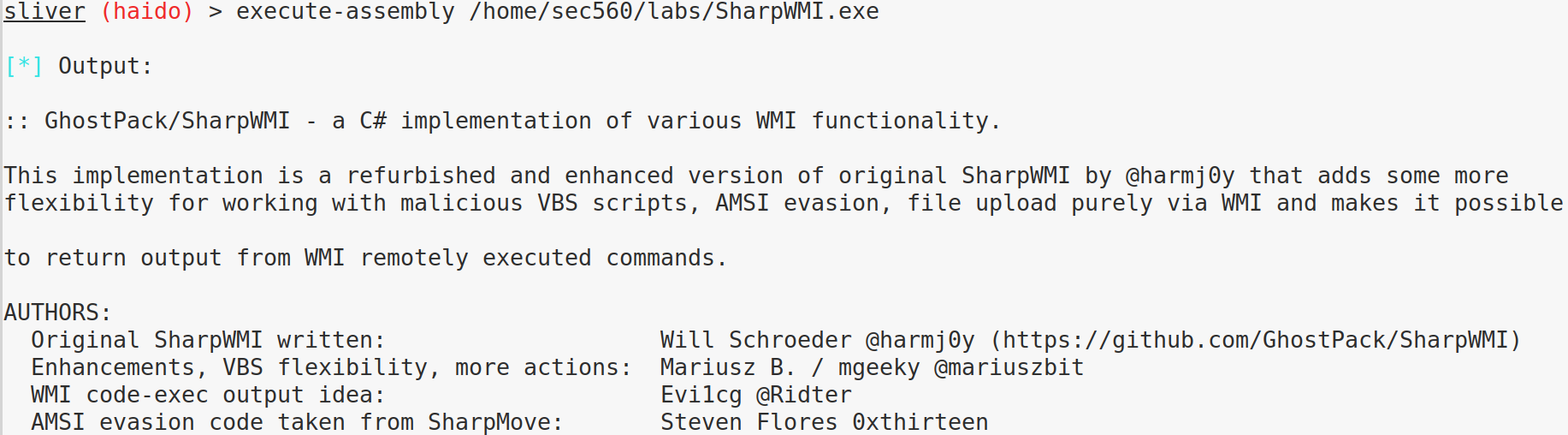
Khi chạy shell, bạn nhận được thông báo rằng đây là OPSEC không tốt. Các công cụ phòng thủ được điều chỉnh để tìm kiếm các côngcụ tạo quy trình thường được các tác nhân độc hại sử dụng, chẳng hạn như CMD và PowerShell.

**Bây giờ, gõ y và nhấn Enter để chấp nhận cảnh báo.**

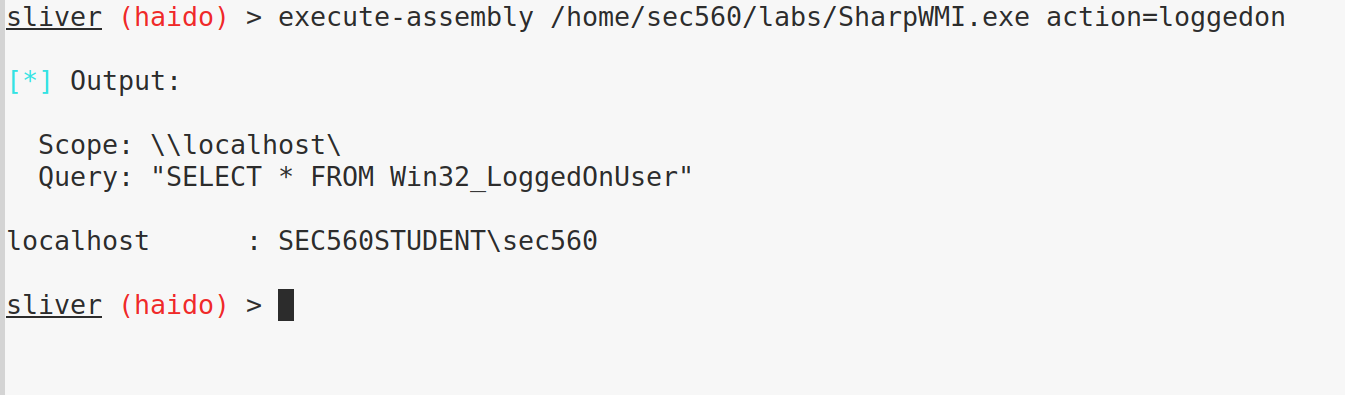
****

**7. Execute Assembly – SharpVMI**

**SharpWMI là 1 tính năng cực mạnh của GhostPack trong Sliver. Nó sẽ gửi file và thực thi trên memory. Vì file này sẽ ko ghi trên đĩa nên sẽ rất khó để phòng thủ và ngăn nhặn nó**

****

****

****

**Liệt kê các user đang đăng nhập trên máy**