# Mục tiêu:

PowerShell Empire là một framework post-exploitation (sau khi khai thác thành công) cho phép tin tặc triển khai các payloads và thực hiện các tác vụ post-exploitation khác trên một hệ thống đã bị tấn công. Nó cung cấp một loạt các tính năng như keylogging, privilege escalation, persistence và nhiều tính năng khác

+ Sử dụng powershell tạo 1 trình lắng nghe (listener) trên Slingshot linux và các agent (tác nhân) trên máy Window, 1 agent với đặc quyền thấp và cao.

+ các tính năng OpSec Safe của Empire

+ Sử dụng các module của Empire để thu thập thông tin từ máy mục tiêu

+ Sử dụng privesc/powerup/allchecks của Empire để tìm kiếm các lỗ hổng leo thang đặc quyền trên máy nạn nhân (local priviledge).

+ Sử dụng Empire để lừa người dùng vượt qua UAC (User Account Control - module 5 slide 19) để có đặc quyền nâng cao hơn.

+ Sử dụng module của Empire để trích xuất các giá trị băm từ mục tiêu

+ Tiến hành quét cổng từ một agent của Empire.

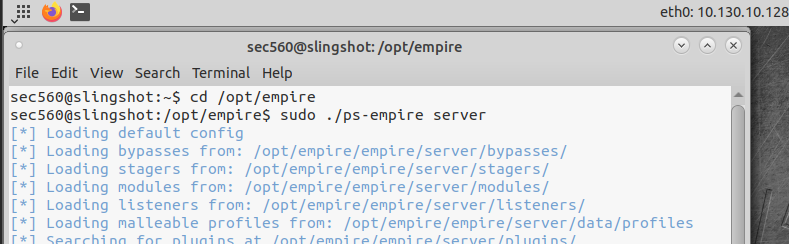
Sử dụng empire để tạo 1 người nghe trên linux và agents trên windows, 1 ng đặc quyền thấp, 1 người đặc quyền cao

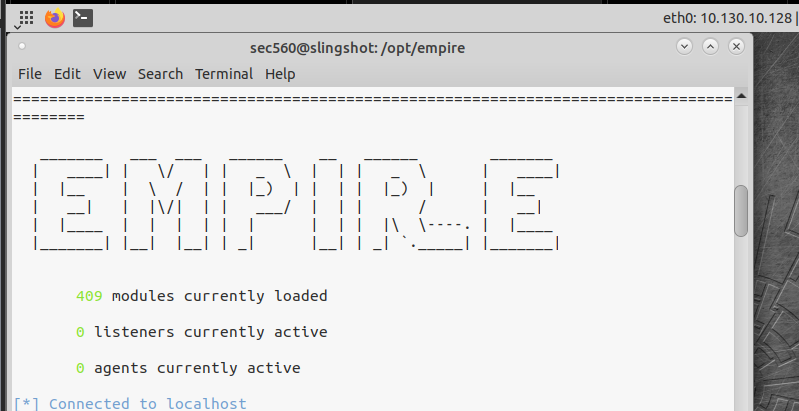
Sau khi thiết lập kết nối giữa listener và agent trên windows, mk sử dụng empire để kiểm tra, tìm kiếm các cơ hội leo thang đặc quyền=> bypass UAC

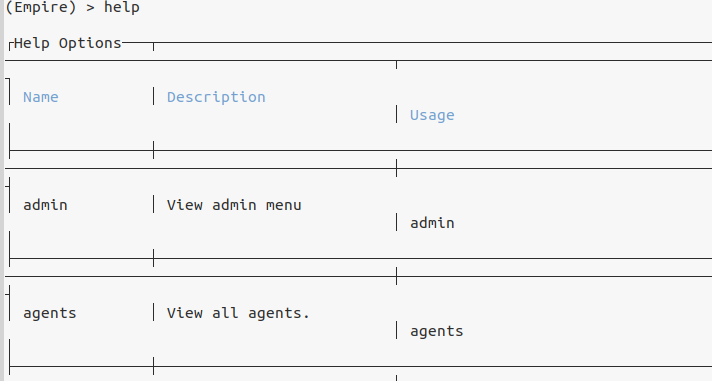
Empire sử dụng privesc /ask để hiện lên lời nhắc UAC, yêu cầu user đăng nhập vào windows cho phép thực thi lệnh bypass UAC. Thông thường user sẽ bấm “yes” khi hiện thông báo nên thực thi đc

Lừa người dùng bỏ qua kiểm soát tài khoản người dùng

# 1. Starting empire

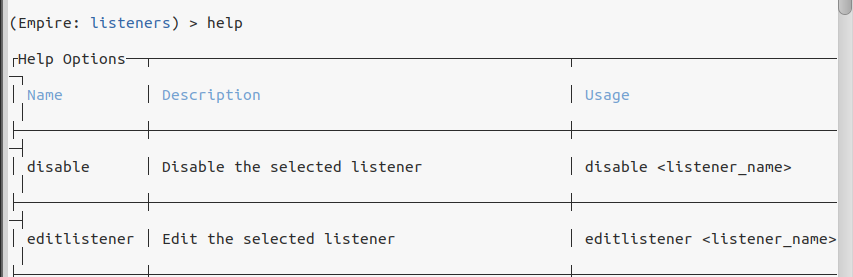


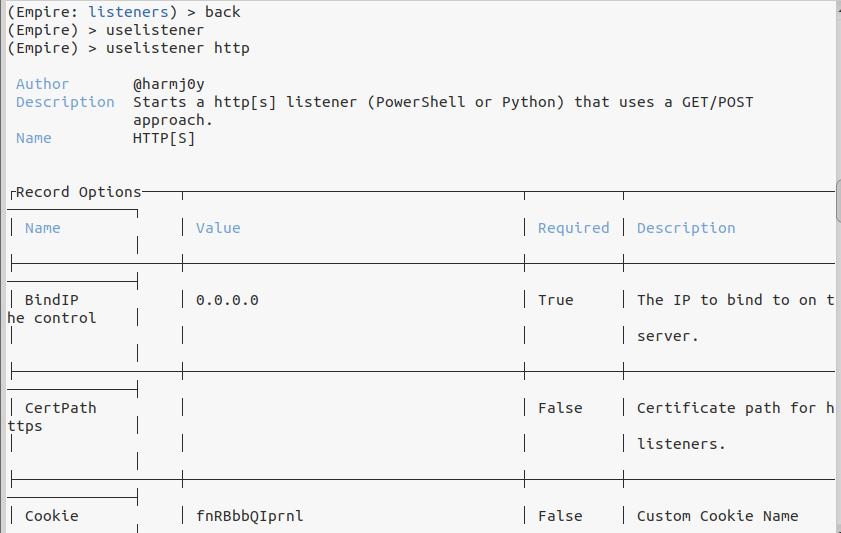


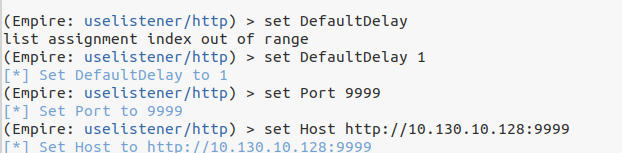


# 2.Configure a listener

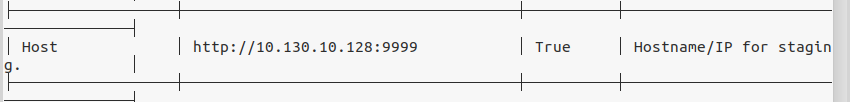


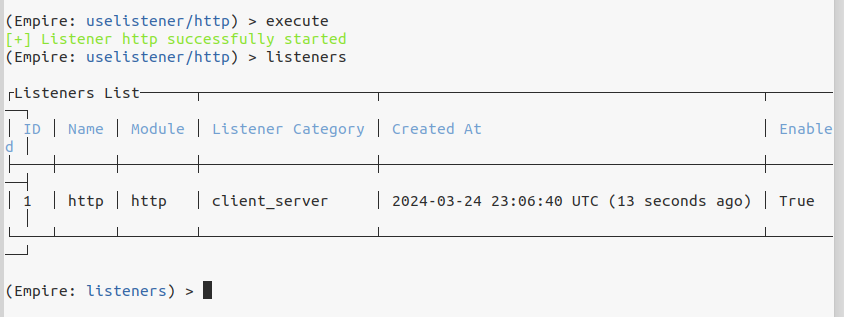




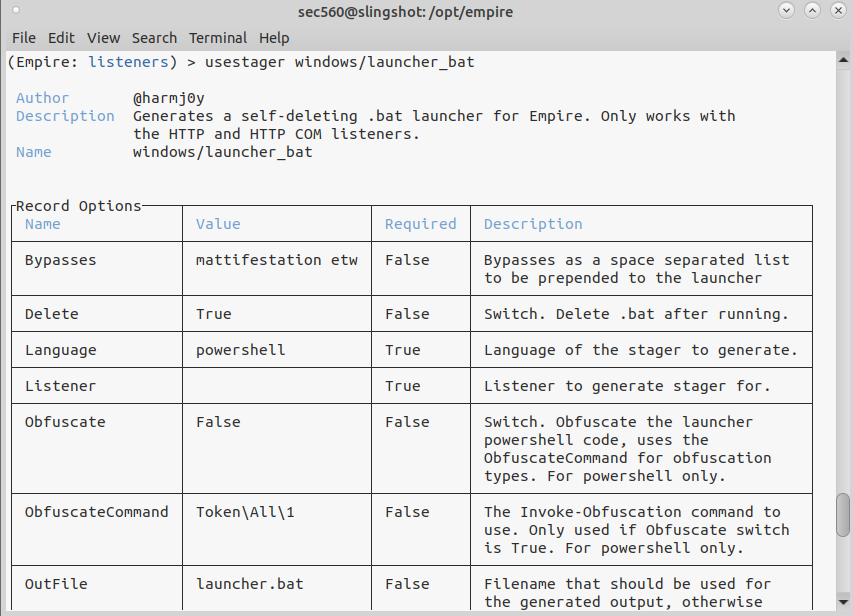


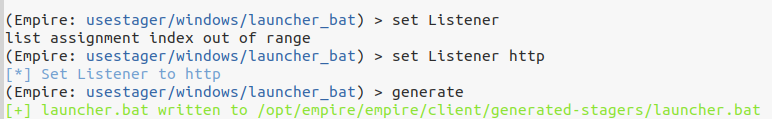






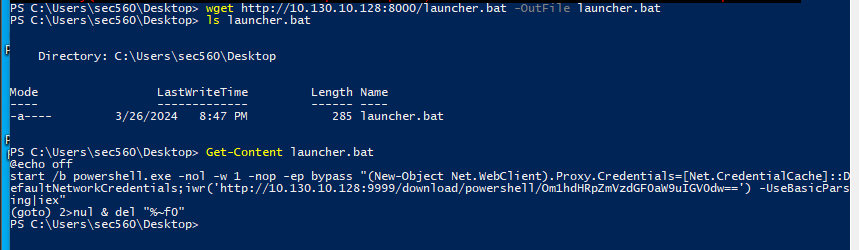
# 3. Deploy an agent

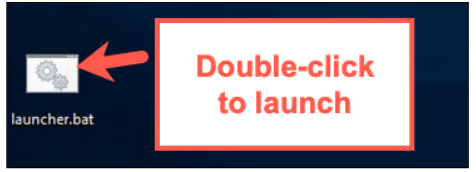






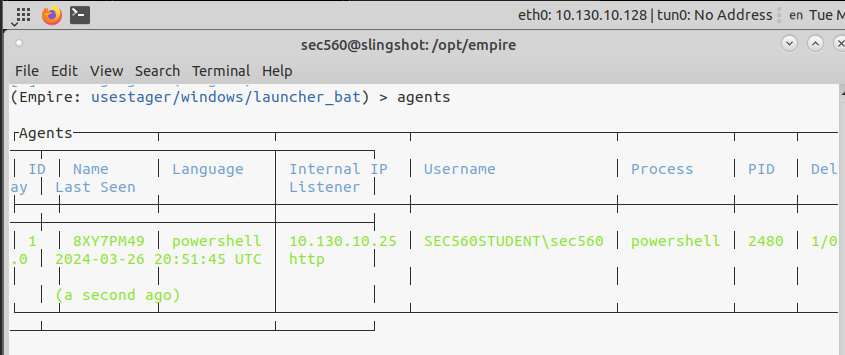
# 4. Deploy the stager

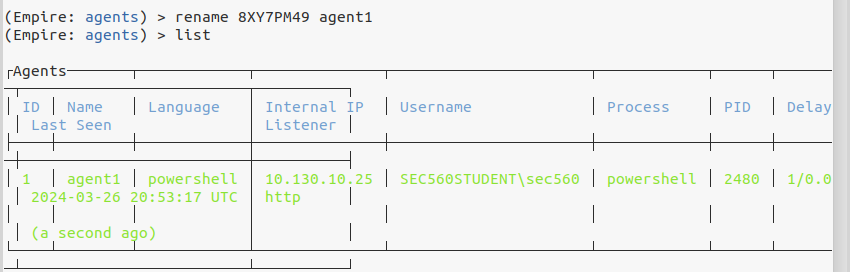


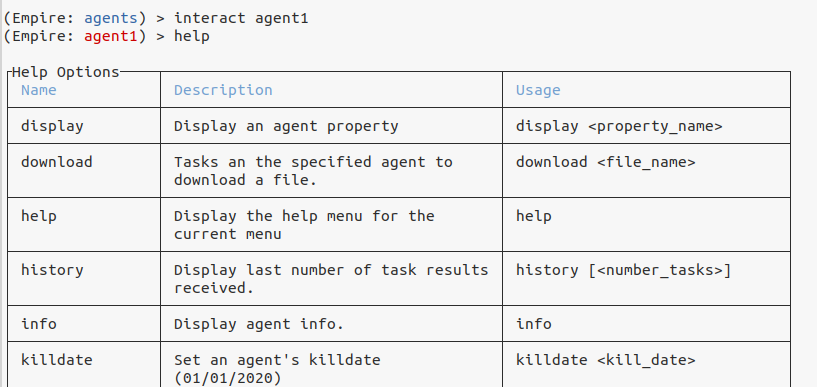


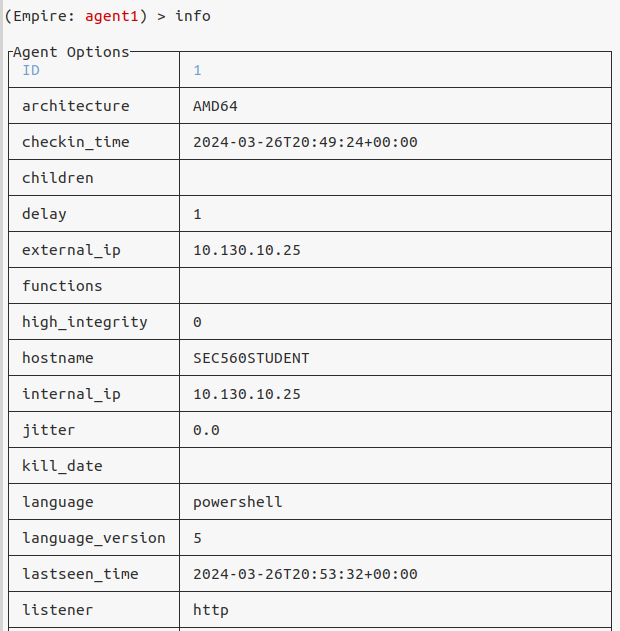


# 5. Active agent

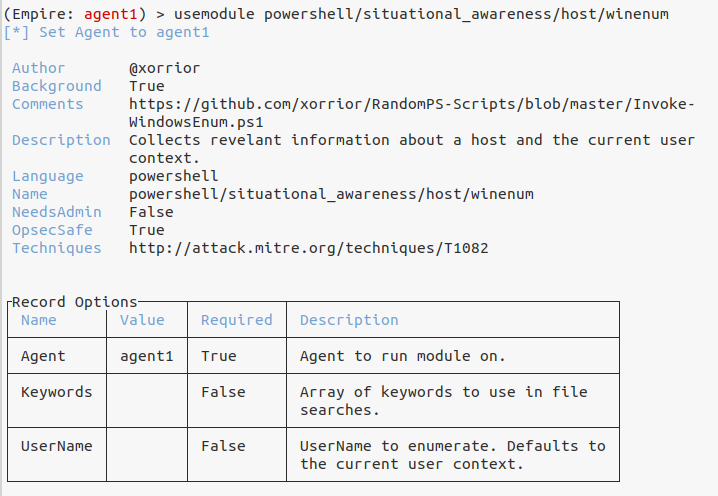




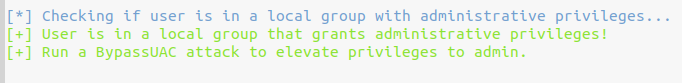


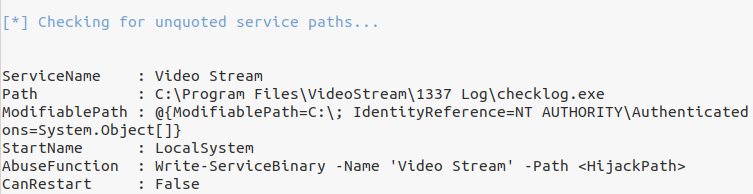


# 6. Modules

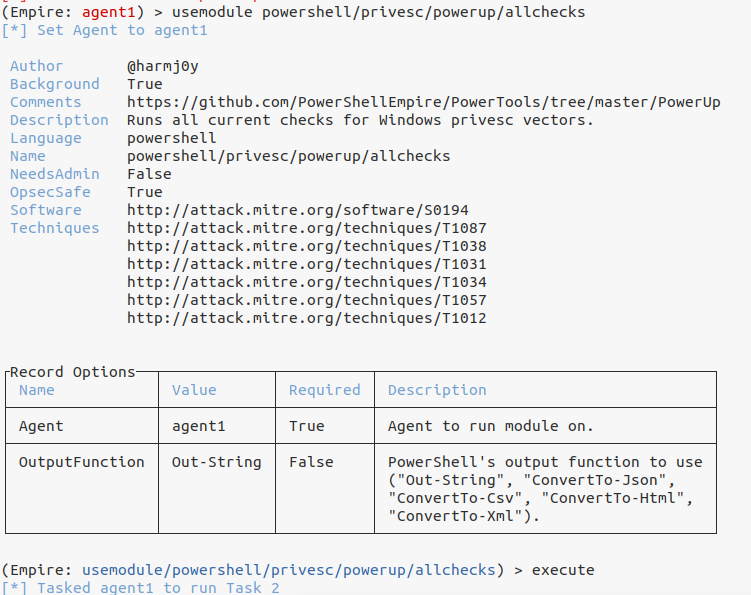


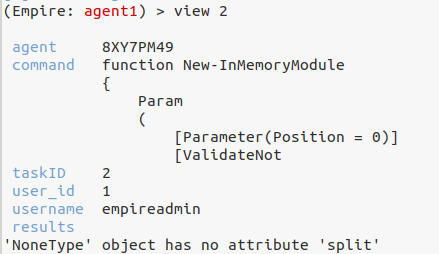


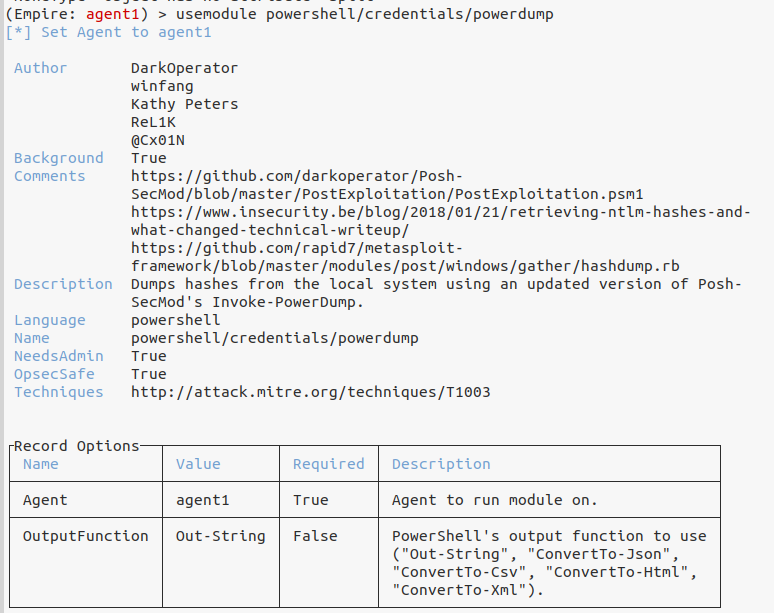




# 7. Looking for privilege escalation

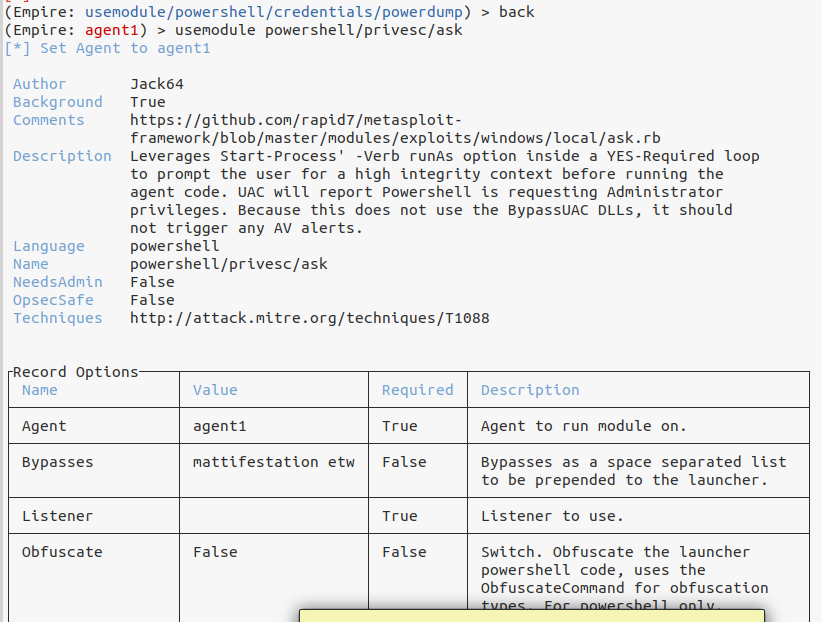




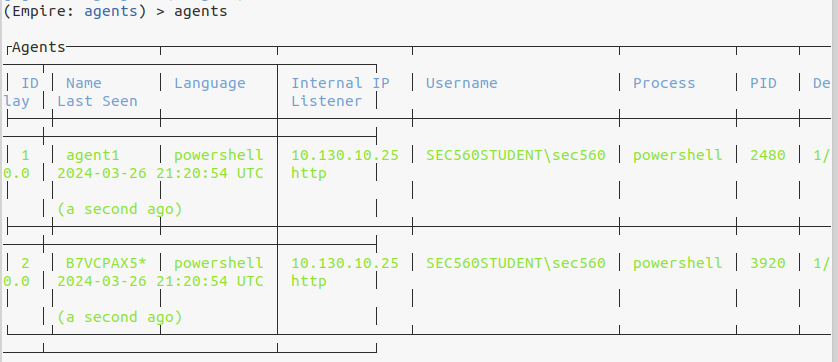


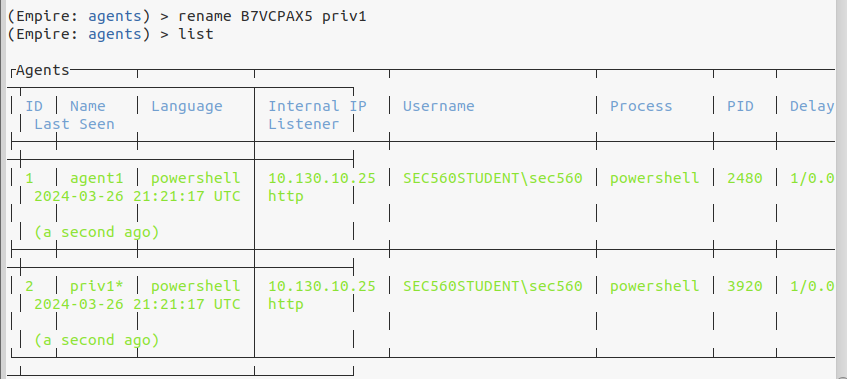


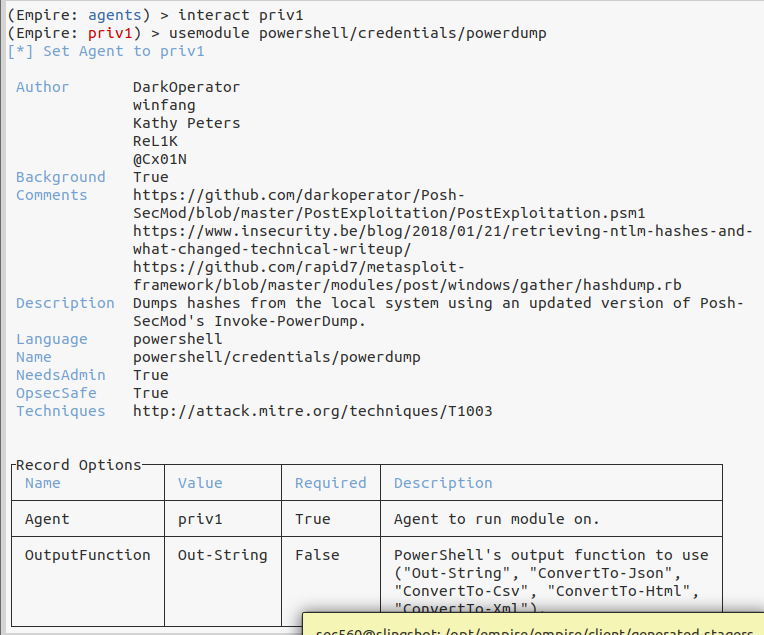
# 8. UAC bypass

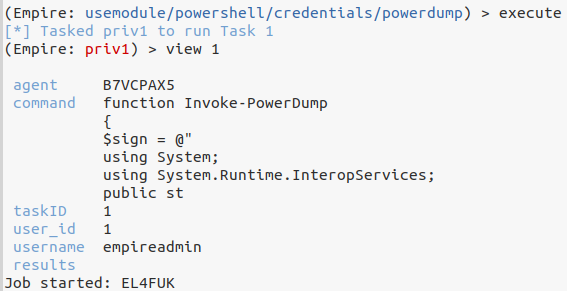


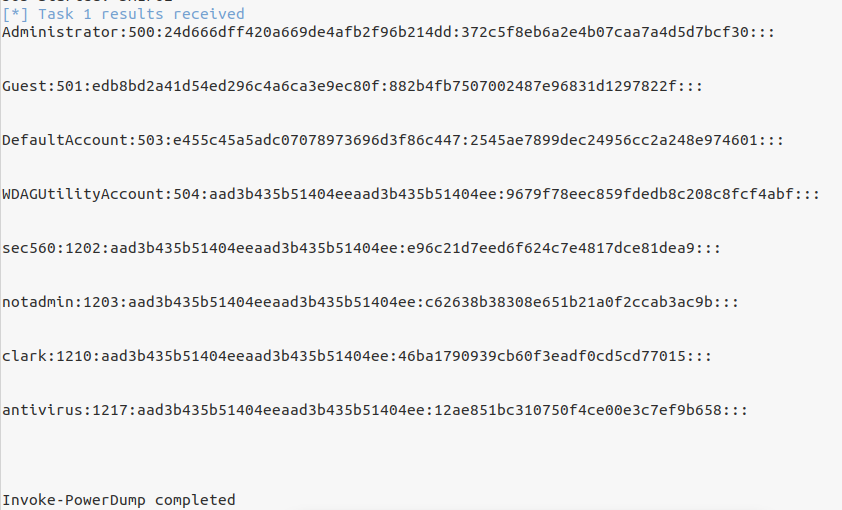


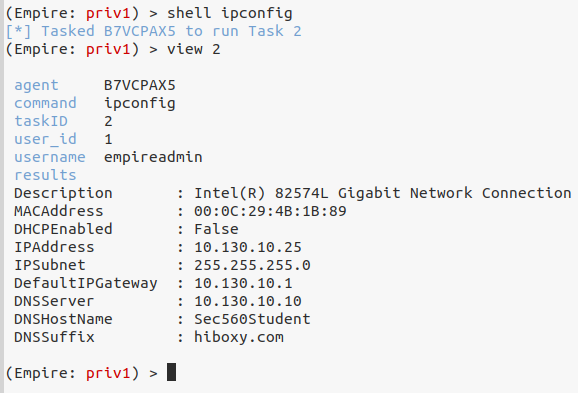




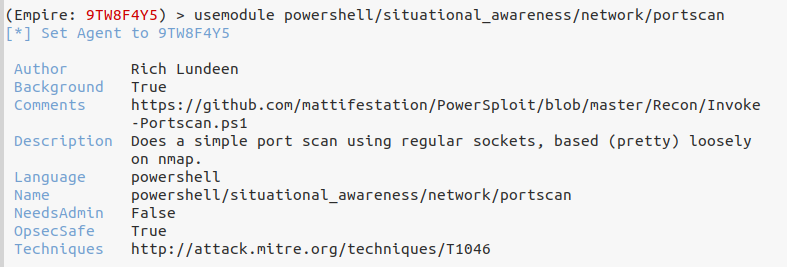


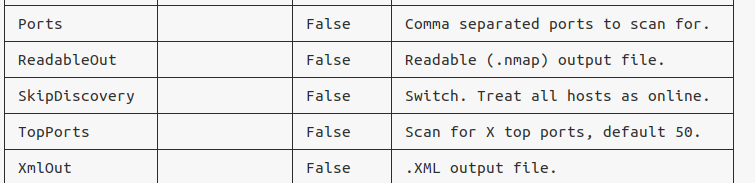


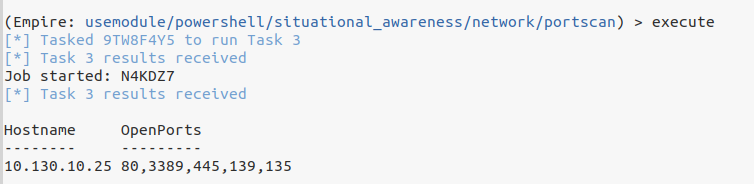




# 9.Port scan







# 10. Wrap up

