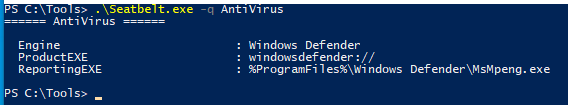
Lab 2.6: Seatbelt

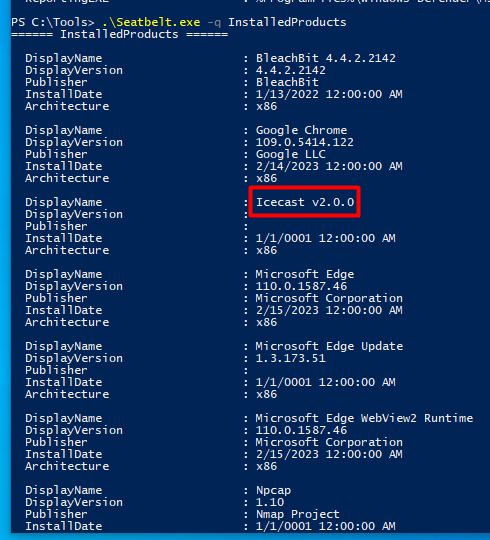
# Launching Seatbelt

**Single Checks**

 Chạy Seatbelt thu thập thông tin về AV (Anti virus)

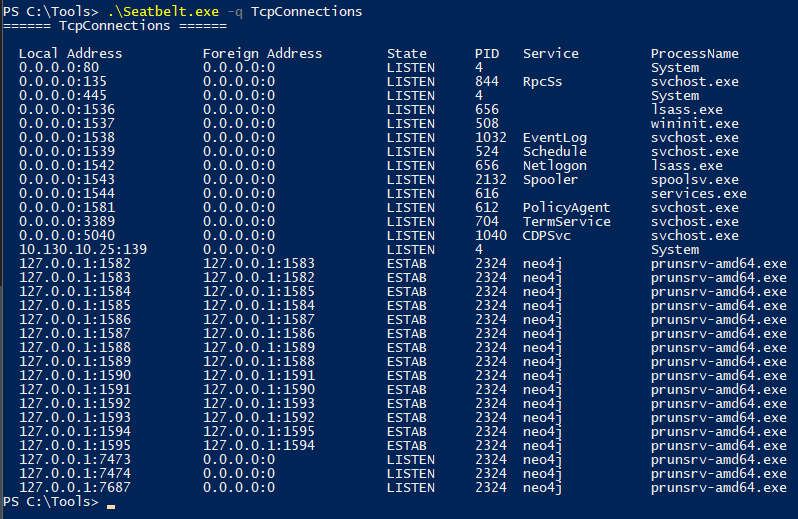


 Hiển thị các phần mềm được cài trên hệ thống:



Chức năng

TcpConnections



# Groups

 Thay vì chạy các command riêng lẻ thì có thể chạy một nhóm các command.

Các command groups được hỗ trợ bởi Seatbelt gồm:

 ALL - tất cả command

 User - User hiện tại hoặc tất cả các user được chạy với các quyền tương ứng

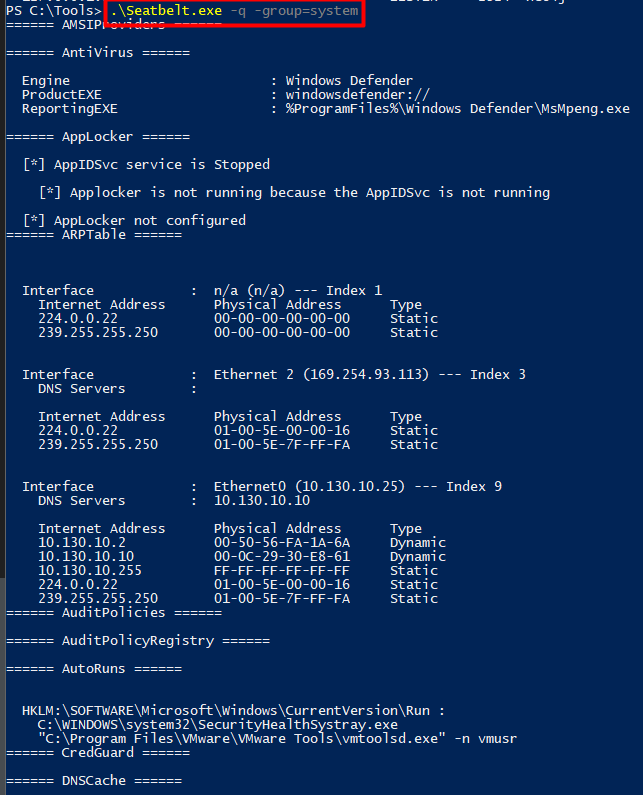
 System - Các dữ liệu thú vị về hệ thống mục tiêu  Cú pháp

**Seatbelt.exe -q -group=group\_name**

# Remote Usage

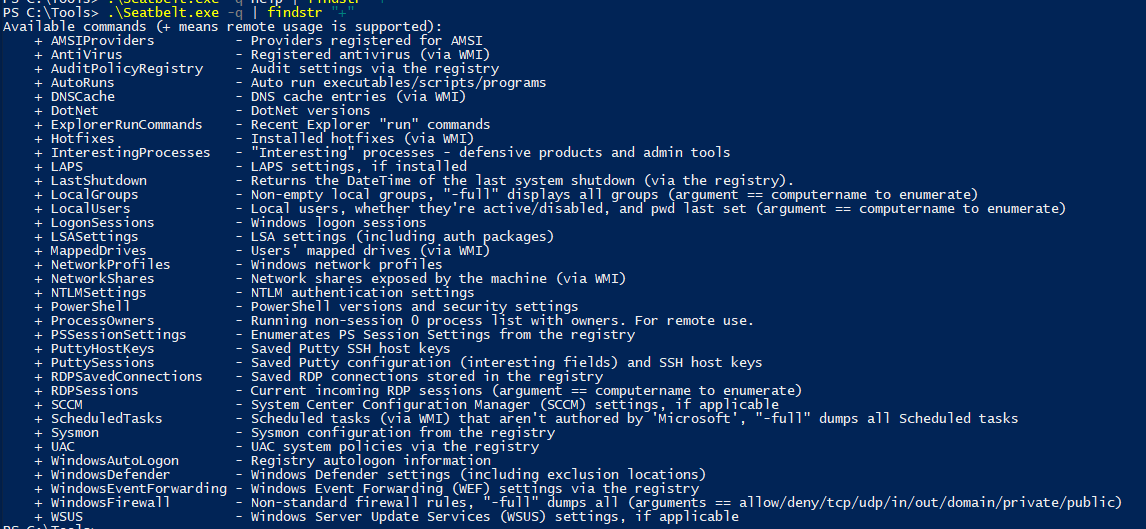
 Command được đánh dấu

trong help menu là các command có thể được

chạy từ xa với các system khác



+



Thử truy vấn UAC tới máy system với credential

10.130.10.25

bgreen:Password1