Impacket cung cấp một loạt các công cụ đã được phát triển sẵn để thực hiện các tấn công và kiểm tra bảo mật trên hệ thống Windows.

# Mục tiêu:

Hiểu về các module trong Impacket (như wmiexec.py, smbexec.py, smbclient.py, và lookupsid.py) và sử dụng Impacket với nhiều phương pháp xác thực, để tác tương với hệ thống từ xa.

# 1. wmiexec.py

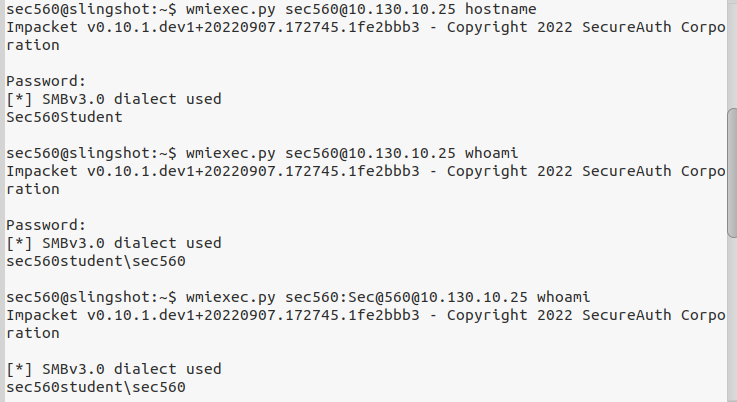
Công cụ cho phép thực thi các lệnh trên các máy chủ Windows từ xa thông qua giao thức WMI

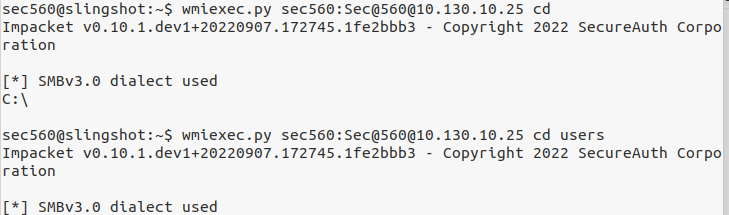
Công cụ này cho phép chúng ta chạy các lệnh trên một dịch vụ từ xa. Điều quan trọng là cần có quyền truy cập cấp quản trị trên máy chủ đích.

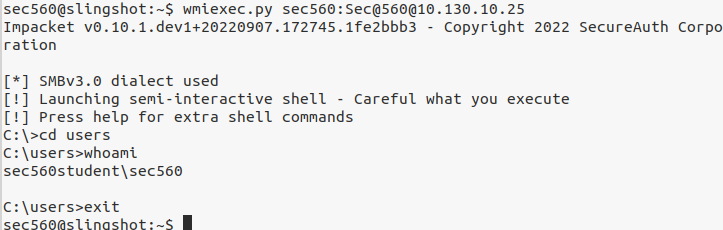
Nhược điểm lớn nhất là nó sử dụng giao thức DCOM (Distributed Component Object Model) và chúng ta cần có khả năng truy cập vào các cổng DCOM trên hệ thống đích.

DCOM là một giao thức mạng được Microsoft phát triển để cho phép các ứng dụng chạy trên các máy tính khác nhau truy cập và tương tác với nhau qua mạng. Tuy nhiên, việc sử dụng DCOM đòi hỏi các cổng DCOM trên hệ thống phải được mở và có sẵn để kết nối từ xa.

Cú pháp: wmiexec.py [[domain/]username[:password]@]<targetName or address> command







# 2. smbexec.py

Hoạt động tương tự như wmicexec, hoạt động trên 2 mode:

-Chế độ chia sẻ (share mode):

Trong chế độ này, người dùng cần chỉ định một thư mục chia sẻ trên máy chủ đích mà họ muốn tương tác.

Các lệnh và hoạt động được thực hiện thông qua thư mục chia sẻ này trên máy chủ đích.

Việc ghi dữ liệu và thực thi các lệnh sẽ diễn ra trên hệ thống của máy chủ đích.

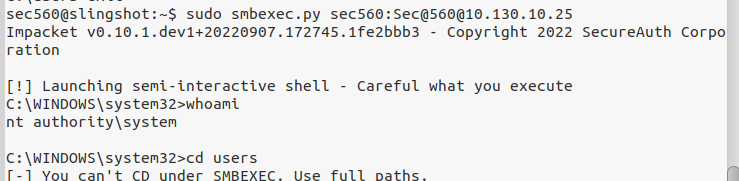
-Chế độ máy chủ (server mode):

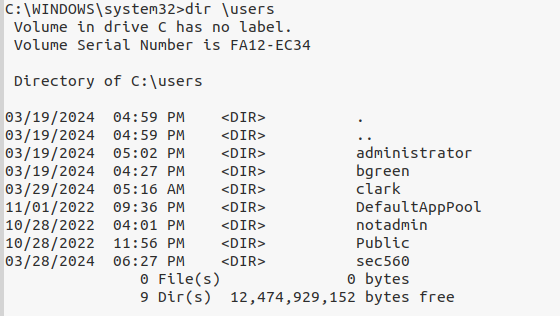
Trong trường hợp không có thư mục chia sẻ sẵn có hoặc nếu không muốn ghi dữ liệu trực tiếp vào hệ thống của máy chủ đích, công cụ sẽ khởi chạy một máy chủ SMB cục bộ trên máy tính tấn công.

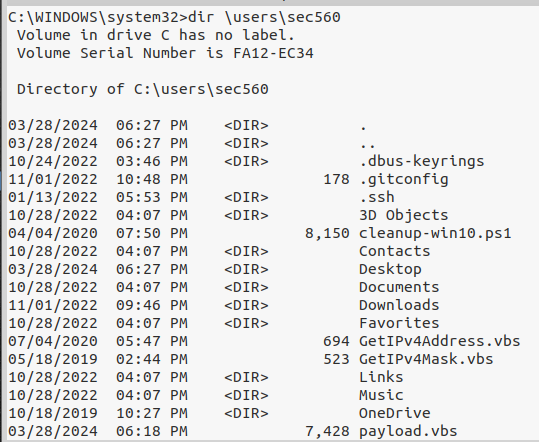
Máy chủ SMB này sẽ lắng nghe trên cổng 445, giao thức mặc định của SMB.

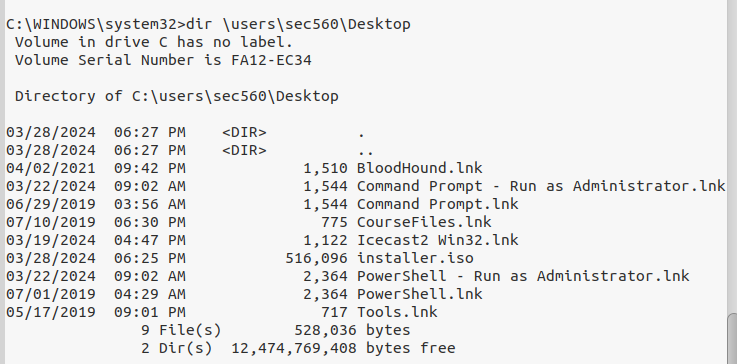
Khi có lệnh được gửi từ máy tính đích, kết quả của lệnh sẽ được trả về và ghi vào một thư mục chia sẻ trên máy tính tấn công.

Điều này giúp tránh việc ghi trực tiếp vào hệ thống của máy chủ đích, giảm nguy cơ để lại các dấu vết trên hệ thống mục tiêu









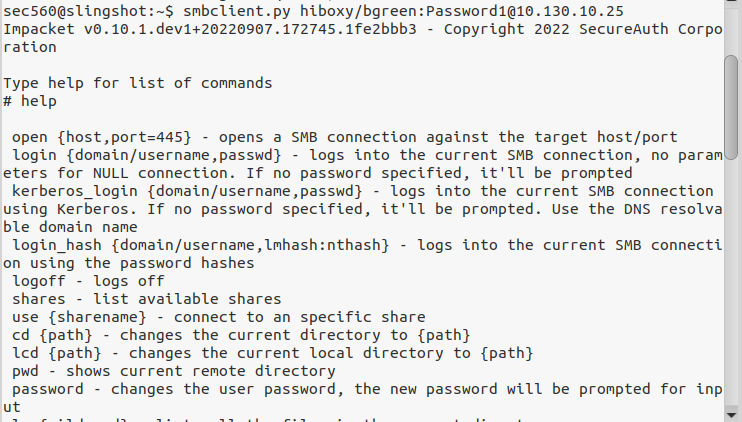
# 3. smbclient.py

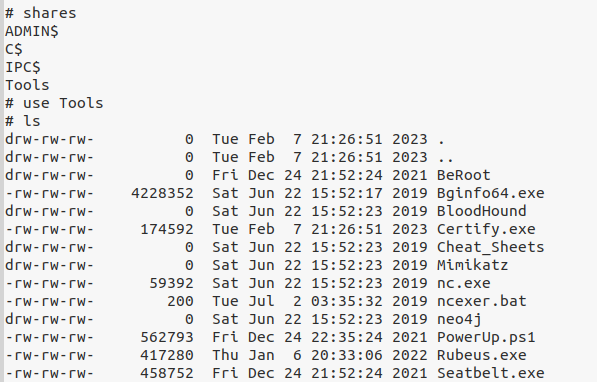
Đăng nhập windows = user bgreen

smbclient.py là một công cụ giống như smbclient trong Linux, cho phép người dùng tương tác với dịch vụ SMB (Server Message Block) trên các máy chủ Windows từ xa.

Chức năng chính của smbclient.py là cho phép người dùng duyệt các thư mục chia sẻ (shares) trên máy chủ, thực hiện các hoạt động như đọc, ghi, xóa và di chuyển các tệp tin giữa các hệ thống.

Nó cung cấp một giao diện dòng lệnh tương tự như smbclient trên Linux, giúp người dùng dễ dàng thao tác với các tài nguyên SMB trên mạng









# 4. lookupsid.py

Là một công cụ trong bộ công cụ Impacket, được thiết kế để thực hiện các thao tác liên quan đến quản lý người dùng và nhóm trên hệ thống Windows.

Công cụ này sẽ tìm kiếm và liệt kê tất cả các người dùng có trong miền (domain) được xác định. Điều này bao gồm cả các tài khoản người dùng chính thức và tài khoản ẩn.

