# Mục tiêu:

Persistence đảm bảo việc pentester vẫn có quyền truy cập vào hệ thống mục tiêu ngay cả khi hệ thống khởi động lại hoặc các hoạt động khác từ phía người phòng thủ.

Tạo nhiều loại tệp để duy trì persistence với Sliver

Tạo một dịch vụ persistence sẽ tạo session Sliver

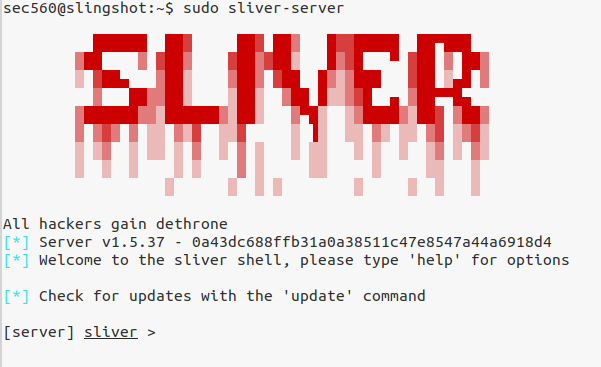
Tạo khóa đăng ký người dùng để persistence

Sử dụng bộ lọc WMI để phát hiện các lần đăng nhập thất bại nhằm kích hoạt persistence

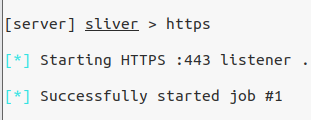
Sliver là một công cụ kiểm thử thâm nhập và quản lý hệ thống từ xa mã nguồn mở, được thiết kế để cung cấp quyền kiểm soát hoàn toàn trên máy tính mục tiêu. Nó cho phép người dùng tạo ra các payload độc lập và linh hoạt, cung cấp một loạt các chức năng như mở một phiên dòng lệnh đầu vào từ xa (reverse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

**Cài đặt Sliver để nhận được kết nối**

Đầu tiên khởi động Sliver:



Sau đó cài đặt listener trên port 443 chạy bằng https để khởi động listener:



Vậy ta đã cài đặt Sliver để nhận kết nối thành công. Giờ sẽ bắt đầu tạo payload:

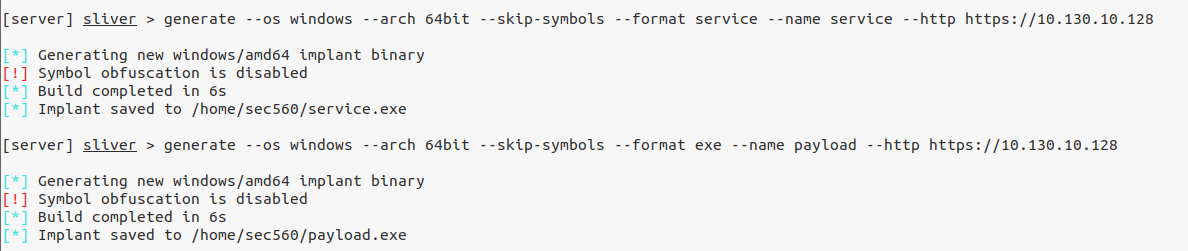
# 1. Tạo Payloads Sliver để persistence

Trước tiên sẽ xem các option của generate bằng lệnh generate -h



Nhận thấy có thể tạo format service. Format này sẽ phản hồi chính xác với service controller và không die sau 30s.

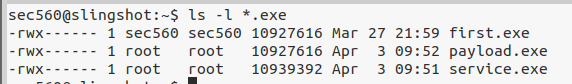
Giờ tạo 2 payloads, một cho service và một cho tệp thực thi tiêu chuẩn



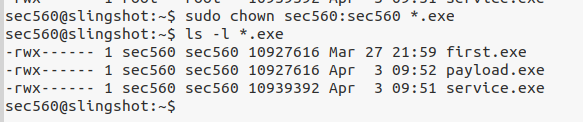
Tiếp theo, chuyển những tệp này sang windows

# 2. Chuyển các tệp sang máy Windows

Mở terminal mới, xem quyền sở hữu của hai file trên:



Thấy cả 2 đang thuộc quyền sở hữu của root, thực hiện chuyển quyền sang sec560:



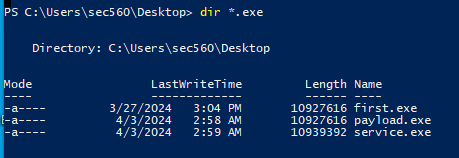
Giờ mình sẽ run python web server để có thể chuyển file sang win:



Sau đó mở PowerShell (bình thường) trong win lên:



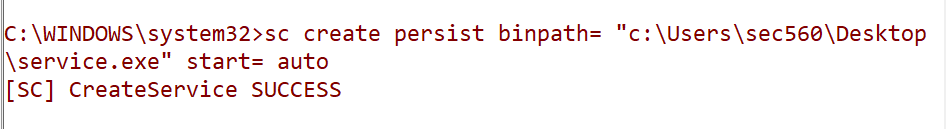
Confirm download thành công:



# 3. Service Persistence

Đầu tiên chúng ta sẽ tạo một service bằng cách thủ công, để thực hiện thì cần Administrator level prompt trên win, mình sẽ mở command prompt – run as administrator lên.

Dùng lệnh sc để tạo một dịch vụ có tên là Persist:

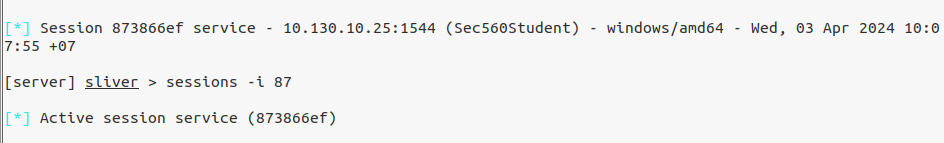


Kiểm tra cơ chế persistence. Khởi động lại máy chủ Windows và sẽ thấy session Sliver mới trên máy Slingshot Linux

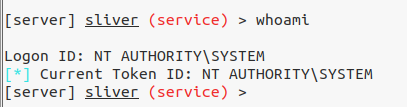


Tương tác với sesion này:

Sessions -i + 2 chữ cái đầu id session, ở đây là 87

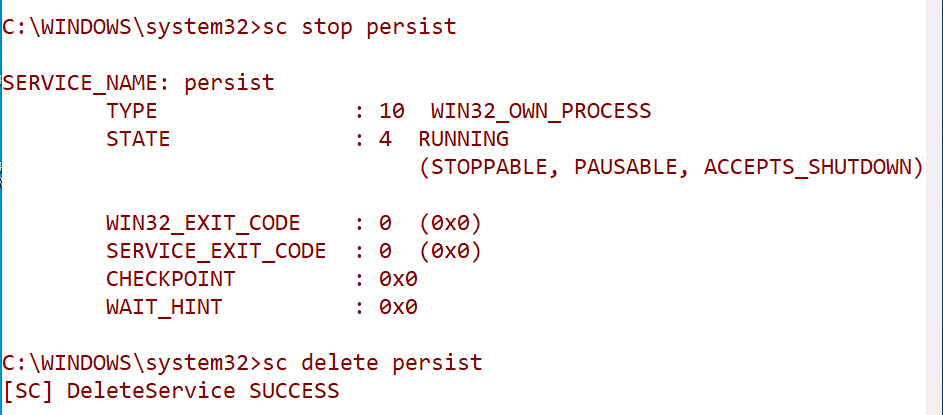


Giờ thử xem mức truy cập ta có với whoami:



Như trên hình, service chạy dưới form system cho phép ta sở hữu mức độ truy cập cao với cơ chế persistence. Dọn dẹp Windows bằng cách kill và xóa service.

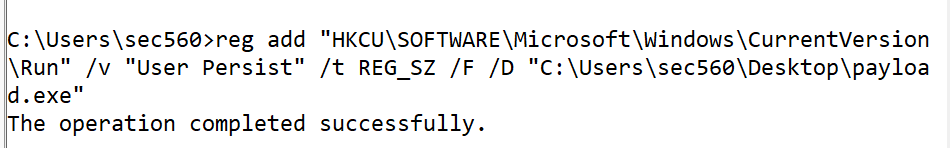
Chuyển sang CMD nâng cao trên windows, hủy process và service bằng lệnh:



# 4. HKCU run Persistence

Trên máy chủ Win, mở CMD thường.

Chạy lệnh reg để tạo registry key (khóa đăng ký) của user gần đây:



Command: reg add “HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run” /v “User Persist” /t REG\_SZ /F /D “C:\Users\sec560\Desktop\payload.exe"

Trong đó:

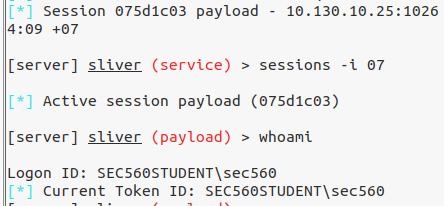
* reg: Câu lệnh để chạy
* add: Thêm key
* “HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”: Location thêm key
* /v “User Persist”: Tên của key (giá trị)
* /t REG\_SZ: kiểu String
* /F: ghi đè nếu đã tồn tại (?)
* /D “C:\Users\sec560\Desktop\payload.exe": tệp thực thi để chạy

Cũng có thể sử dụng HKLM (HKEY Local Machine) và cách này hiệu quả hơn với bất kỳ người dùng nào đăng nhập vào hệ thống, nhưng yêu cầu quyền truy cập nâng cao mới dùng được key này nên mình đang dùng HKCU (HKEY Current User), không cần quyền truy cập nâng cao.

Để check thì chỉ cần restart lại win, sẽ thấy sessions mới trên sliver

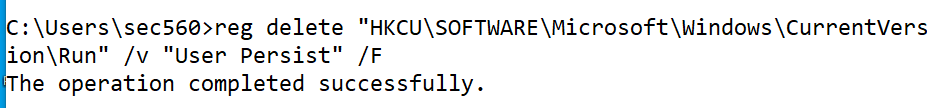


Tương tác với session:



Chạy whoami, ta thấy truy cập gần đây là sec560!

Giờ mình sẽ quay về win để xóa key này. Mở cmd thường lần nữa:



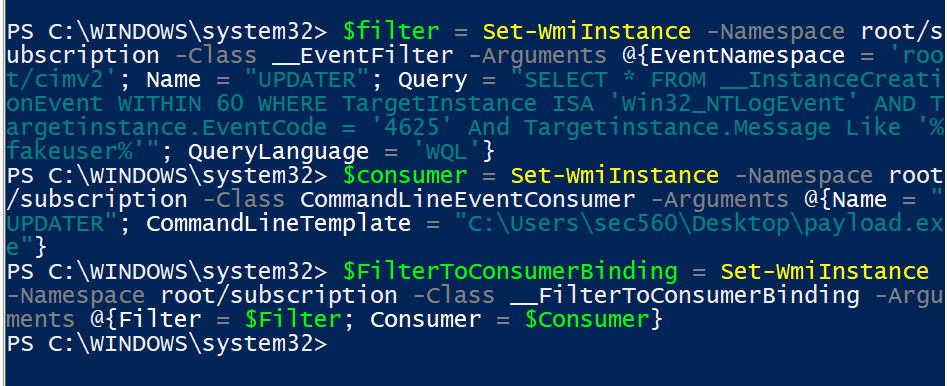
# 6. WMI Event Persistence:

WMI event cho phép cách kích hoạt tải trọng rất linh hoạt. Thiết lập event listener cho lần đăng nhập không thành công (event ID: 4625) đối với fakeuser. Cho phép attacker kích hoạt payload khi đăng nhập thất bại với người dùng không tồn tại.

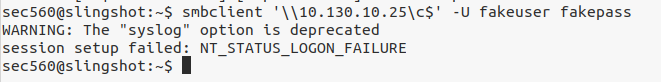
Sử dụng các lệnh PowerShell (PowerShell run as admin) để thiết lập bộ lọc.

Có 3 phần thiết lập:

1. Lệnh đầu tiên ta sẽ sử dụng thiết lập Event Filter -Class \_\_EventFilter với tên UPDATER. Sau đó, truy vấn sẽ tìm kiếm các thông tin đăng nhập không thành công (Event ID 4625) trong đó thông tin đăng nhập khớp với fakeuser
2. Phần 2 thiết lập consumer hoặc việc cần làm khi khớp với filter. Ở đây sẽ khớp với filter UPDATER chạy payload tại C:\Users\sec560\Desktop\payload.exe
3. Cuối cùng thiết lập liên kết để tìm kiếm trigger và run consumer (payload)



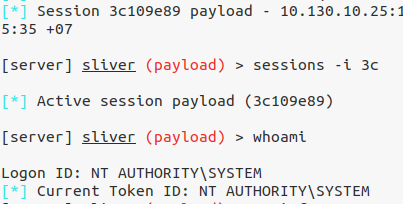
Đã thiết lập bộ lọc, chuyển sang Linux mở terminal mới thử đăng nhập bằng smbclient và fakeuser.

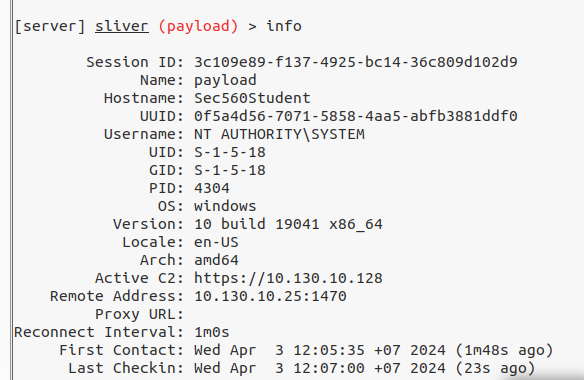


Chú ý trên Sliver, thấy session mới xuất hiện:



Tương tác với session





Thấy rằng có quyền truy cập ở cấp độ hệ thống trên Windows. Nếu mất quyền truy cập thì phải làm lại.

Ngoại trừ phương pháp thủ công dưới đây thì có thể sử dụng Metasploit: module windows/local/wmi\_persistence hoặc Empire: module persistence/elevated/wmi

Xóa filter này ở Powershell đang bật trên máy win:

