1. Setup Sliver

A screenshot of a computer program

AI-generated content may be incorrect.

1. Tạo sliver payloads

A white background with black and blue text

AI-generated content may be incorrect.

Generate: tạo 1 payload, dịch vụ hoặc tệp thực thi

--os windows: xác định hệ điều hành

--arch 64bit: chỉ định kiến trúc hệ điều hành là 64 bit

--skip-symbols: bỏ qua symbols -> giảm kích thước file thực thi

--format service, exe: xác định ra là 1 dạng dịch vụ, thực thi

-- name service: tên là “service”

1. Gửi file payloads sang windows

Chuyển quyền chủ sỡ hữu sang cho người dung sec560

A screenshot of a computer code

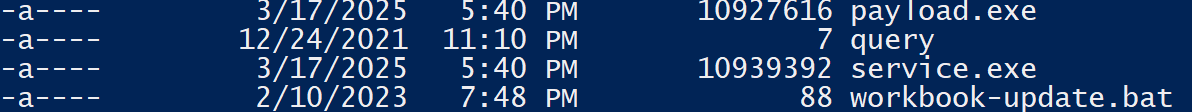
AI-generated content may be incorrect.

Tạo python web server để gửi file



Tải file từ máy Windows





1. **Service persistence**

Tạo 1 service với tên persist khiến cho file service.exe tự động thực thi mỗi khi người dung khởi động máy



Khởi động lại máy window

A screen shot of a computer

AI-generated content may be incorrect.

1 Sliver session mới được tạo. Tương tác với session này và thấy nhận được quyền System – quyền cao cấp nhất trên Windows, mạnh hơn cả Administrators

Xóa service

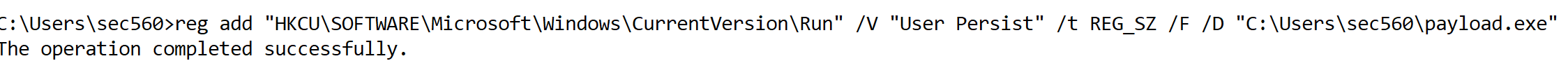
A screenshot of a computer program

AI-generated content may be incorrect.

1. **HKCU Run Persistence**

HKCU(1 user) HKLM(Nhiều user – cần admin)

Tạo 1 registry key cho người dung hiện tại



Reg add: them 1 giá trị vào Windows Registry

HKCU….Run: khóa Registry auto-run khi user đăng nhập

/V “user persist”: tên của khóa

/t REG\_SZ : kiểu dữ liệu

/F: ghi đè nếu giá trị đã tồn tại

/D: đường dẫn đến chương trình cần chạy tự động

Khởi động lại máy windows

A screenshot of a computer

AI-generated content may be incorrect.

Thành công tạo 1 sliver session. Tương tác với session và thấy chỉ nhận được quyền là user sec560 -> cần phải leo thang

Xóa registry vừa tạo



1. **WMI Event Filter Persistence**

WMI event fileter sẽ rất tiện lợi cho việc kích hoạt những payload. Ta sẽ có thể kích hoạt được payload của mình ngay cả khi đăng nhập thất bại với 1 người dung ko tồn tại

Tạo Event Filter

A blue screen with white text

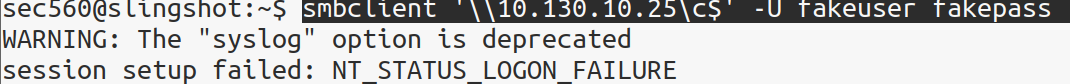
AI-generated content may be incorrect.

Filter: lắng nghe sự kiện 4625 – khi ai đó đăng nhập sai

Consumer: chạy payload ẩn, ko cần thủ công

FilterToConsumerBinding: liên kết filter và consumer -> tự động chạy payload.exe khi đăng nhập sai

Truy cập C$ (là 1 admin share – chia sẻ mặc định ) từ xa với tài khoản fakeuser - fakepass



Thành công tạo 1 sliver session và nhận được quyền system

Đây là phương pháp thủ công ngoài ra có thể sử dụng empire hoặc Metasploit để cso thể thực hiện