1. Starting Empire

Khởi động server:

A close up of a text

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

Khởi động client

A screen shot of a computer

AI-generated content may be incorrect.

1. Configure listener
   1. Uselistener http

Sử dụng http listener cho cả bài

Chú ý đến vài options sau:

Killdate: sau khoảng thời gian này sẽ ngừng theo dõi

StagingKey: 1 stagingkey ngẫu nhiên đễ mã hóa giữa agent và listener

WorkingHours: giới hạn thời gian để agent trả lời listener

DefaultDelay: agent sẽ cho phép listener gửi request sau mỗi 5s

A close-up of a sign

AI-generated content may be incorrect.

A close-up of a white background

AI-generated content may be incorrect.

* 1. Set option

A screenshot of a computer code

AI-generated content may be incorrect.

* 1. Execute



A close-up of a computer screen

AI-generated content may be incorrect.

1. Deploy an agent

Usetager windows/launcher\_bat -> triển khai agent bằng file .bat

A screenshot of a computer

AI-generated content may be incorrect.

Tạo stager file, set Listener http và generate





Tạo file thành công

Kích hoạt module http.server trên cổng 8000 của python3



1. Deploy the stager
   1. Tải file stager về máy window(dựa vào module bên trên) và thực thi

A blue screen with white text

AI-generated content may be incorrect.

Thực thi file launcher.bat và nó sẽ tự xóa ngay lập tức



Thành công tạo 1 agent

1. Active agent

Đổi tên agent

A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

Interact để sử dụng 1 agent

Info để xem thông tin agent

A screenshot of a computer

AI-generated content may be incorrect.

Hãy để ý mỗi lần tương tác với agent và xem thông tin với agent đó. Để ý thông số lastseen\_time. Nết 2 lần đều giống nhau tức là agent đó đã chết và b sẽ phải tạo lại 1 agent mới khác

1. Modules

Usemodule winenum để thu thập thông tin

A screenshot of a computer

AI-generated content may be incorrect.

Excute và xem kết quả

A screenshot of a computer program

AI-generated content may be incorrect.

1. Looking for privilege escalation\

Usemodule powerup/allcheckss để phát hiện tất cả các lỗ hổng mà ta có thể leo thang

A screenshot of a computer

AI-generated content may be incorrect.

Execute và xem kết quả

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Có thể thấy module này đã cho ta thấy user đang trong nhóm cục bộ có quyền admin và cách để leo thang bằng cách sử dụng tấn công BypassUAC

Trước khi leo thang, xem giới hạn quyển admin đối với agent bằng cách sử dụng module powerdump

A screenshot of a computer

AI-generated content may be incorrect.



Cần có quyền admin để dump

1. **UAC bypass**

Use module ask.

Module này sẽ hiển thị hộp thoại UAC prompt lên màn hình nguwiof dung. Nếu nạn nhân đăng nhập với quyền admin và click vào yes thì ta sẽ có shell với quyền cao hơn

**A screenshot of a computer

AI-generated content may be incorrect.**

Set listener http và execute

A screenshot of a computer

AI-generated content may be incorrect.

Thu được agents

Đổi tên agents thành priv1

A screenshot of a computer

AI-generated content may be incorrect.

Dấu \* tức là những agents có full quyền admin

Dump lại bằng priv1 -> thành công(tức là đã thành công có quyền admin)

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer code

AI-generated content may be incorrect.

Run shell ipconfig

A screenshot of a computer program

AI-generated content may be incorrect.

1. **Port scan**

Usemodule

**A screenshot of a computer

AI-generated content may be incorrect.**

set Host và execute

A screenshot of a computer program

AI-generated content may be incorrect.

1. **Wrap up**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**