- Sử dụng MSBuild như một phương tiện bypass cho kiểm soát ứng dụng

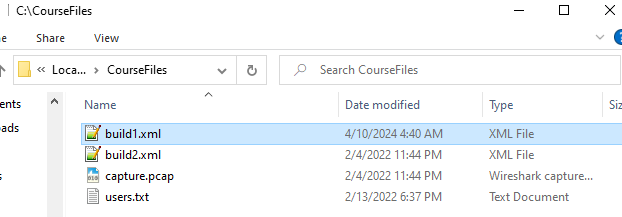
- Sử dụng một tệp XML thử nghiệm để xuất ra văn bản đơn giản

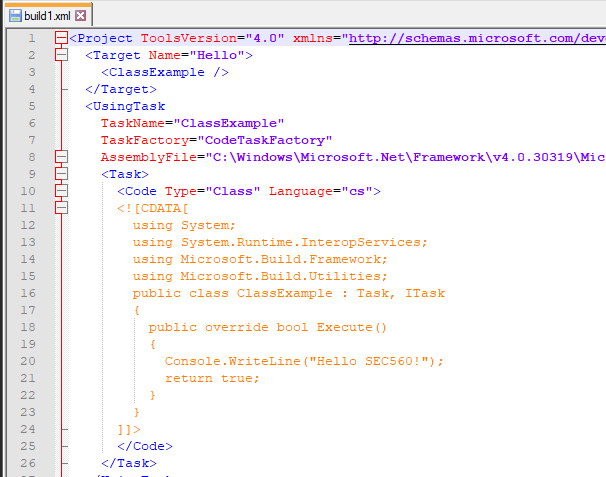
- Sử dụng MSBuild với Metasploit/Meterpreter

- Sử dụng MSBuild với Empire

# 1. Setup

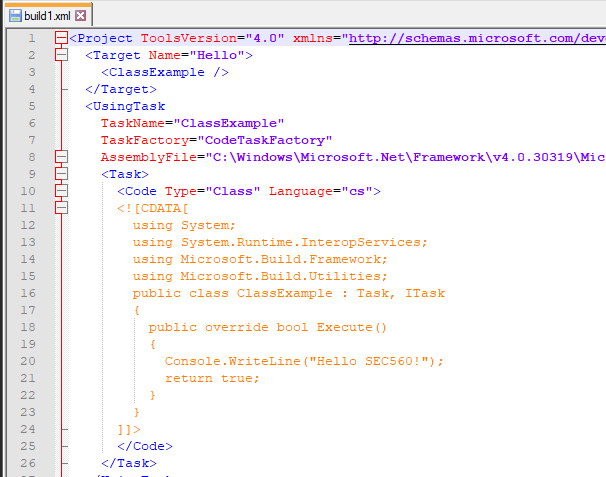
Mở file build1.xml





# 2. initial testing

-Điển đoạn code { Console.WriteLine(“Hello SEC560!”); }



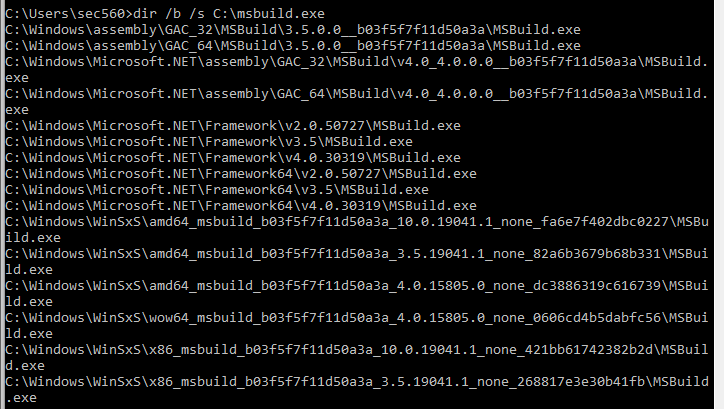
C:\Users\sec500> dir /b /s C:\msbuild.exe: tìm kiếm tất cả các tệp có tên là "msbuild.exe" trên ổ đĩa C và hiển thị kết quả dưới dạng danh sách ngắn với đường dẫn đầy đủ.

dir: Đây là lệnh trong Command Prompt để hiển thị danh sách các tệp và thư mục trong một thư mục cụ thể hoặc trên toàn bộ ổ đĩa.

/b: Đây là một tùy chọn của lệnh dir, chỉ định rằng chỉ tên tệp (không bao gồm thông tin bổ sung như kích thước và ngày tạo) sẽ được hiển thị.

/s: Đây là một tùy chọn khác của lệnh dir, chỉ định rằng tìm kiếm sẽ được thực hiện trên toàn bộ cây thư mục, bao gồm cả thư mục con và tệp con của thư mục hiện tại.

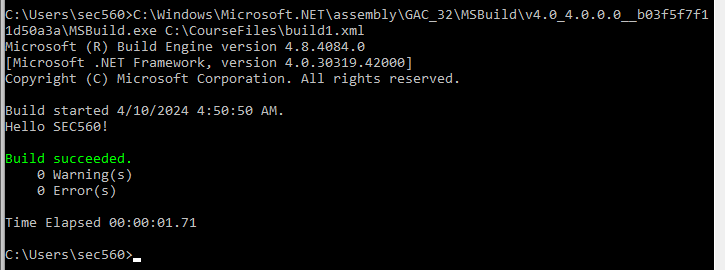
C:\msbuild.exe: Đây là đường dẫn của tệp cần tìm kiếm. Trong trường hợp này, tệp "msbuild.exe" được tìm kiếm trên ổ đĩa C.



C:\Windows\Microsoft.NET\assembly\GAC\_32\MSBuild\v4.0\_4.0.0.0\_\_b03f5f7f11d50a3a\MSBuild.exe

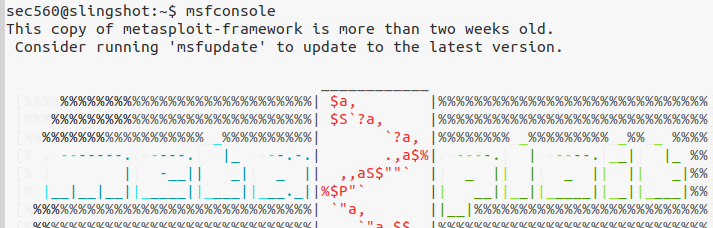
Đây là phiên bản 32-bit, vì vậy shellcode của chúng ta cũng cần là 32-bit

Lệnh này dùng để chạy file build1.xml



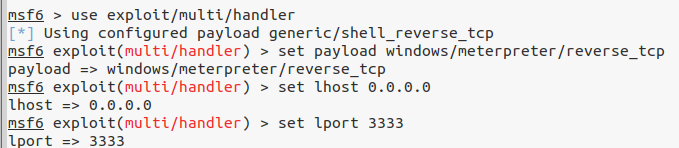
# 3. Meterpreter shellcode

-Chạy Metasploit



-Sử dụng module handler

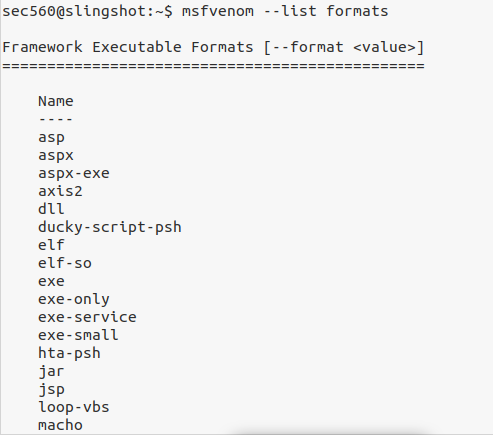
module exploit/multi/handler được sử dụng để tạo một máy chủ lắng nghe (listener) để chờ đợi các kết nối từ các payload tấn công. Khi một payload kết nối thành công đến máy chủ lắng nghe này, module exploit/multi/handler sẽ giúp quản lý kết nối và cung cấp quyền điều khiển đối với máy mục tiêu.

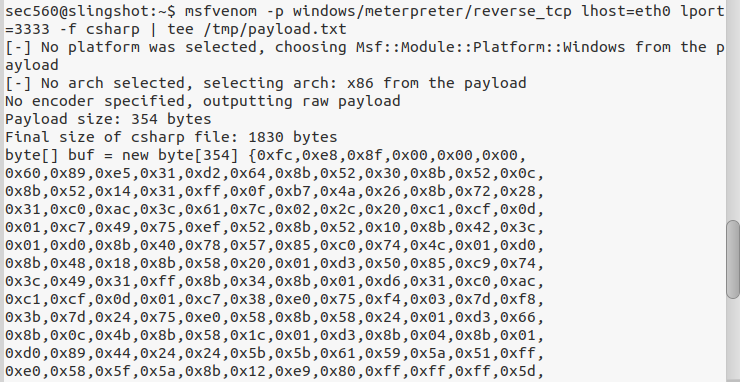




msfvenom là một công cụ trong Metasploit Framework được sử dụng để tạo ra các payload tấn công. Payload là mã thực thi hoặc dữ liệu có chứa các lệnh độc hại được gửi đến máy mục tiêu trong quá trình khai thác lỗ hổng bảo mật.

msfvenom có thể tạo ra nhiều loại payload khác nhau, bao gồm các shellcode, mã thực thi, tập tin tin tức, và nhiều hơn nữa

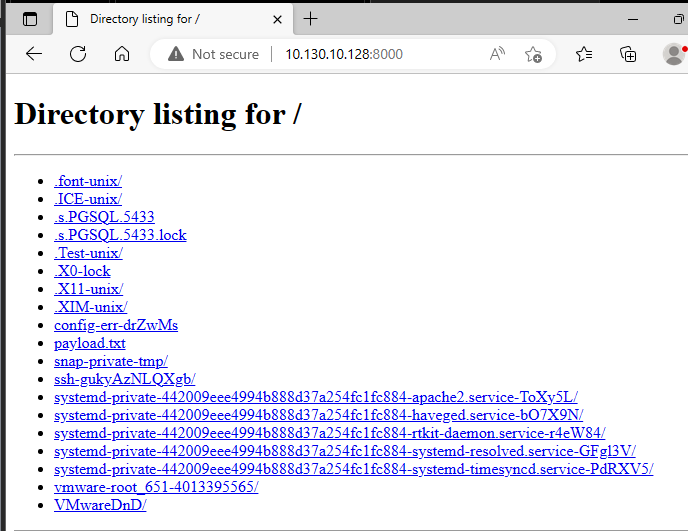




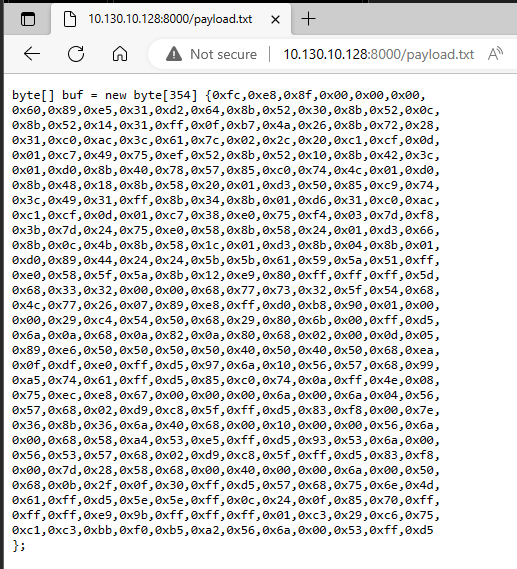
-Chạy dịch vụ http



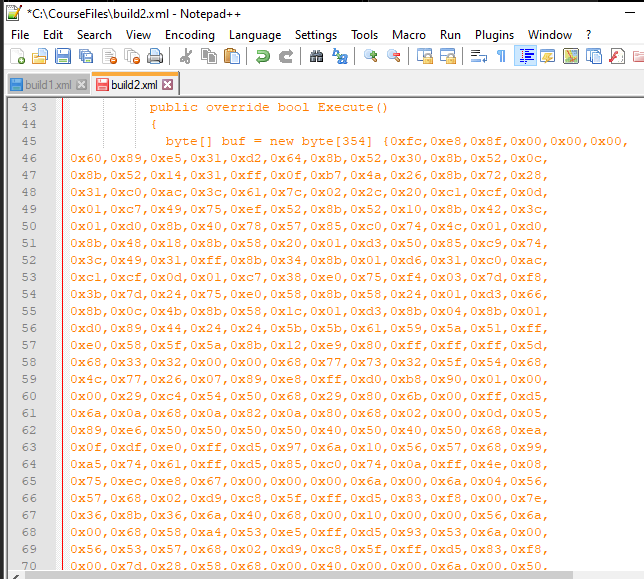
-Máy windows truy cập vào server



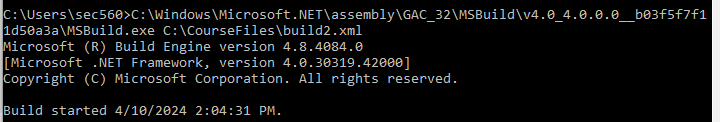
-Xem file payload.txt



-Copy nội dung file trên vào phần nhập code trong file build2.xml

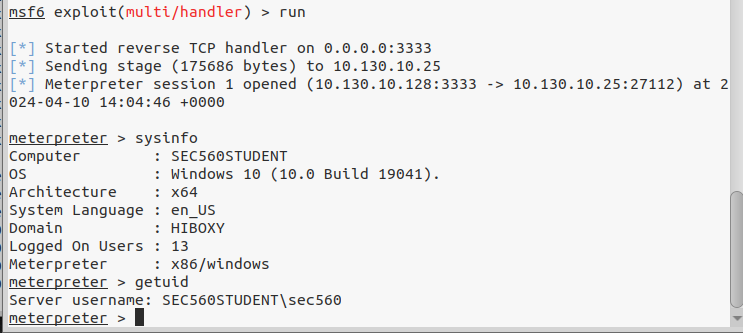


-Máy windows chạy file build2.xml



-Máy tấn công thiết lập đc phiên kết nối

-Kiểm tra thông tin



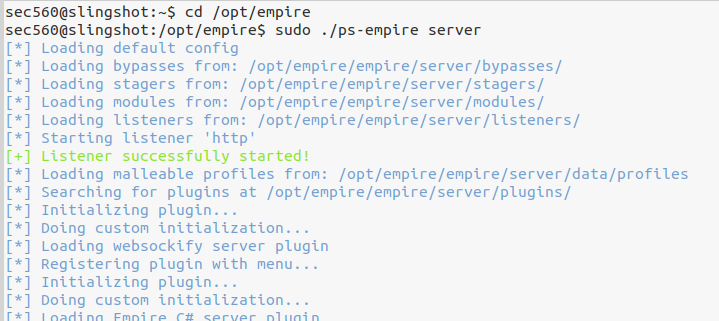
# 4. empire

Empire là một công cụ kiểm thử thâm nhập và quản lý hệ thống từ xa mã nguồn mở, được phát triển bởi PowerShellEmpire. Nó cung cấp một nền tảng đa nền tảng cho việc triển khai các công cụ tấn công, thu thập thông tin, và duy trì truy cập không ủy quyền trên một mạng hoặc máy tính mục tiêu.

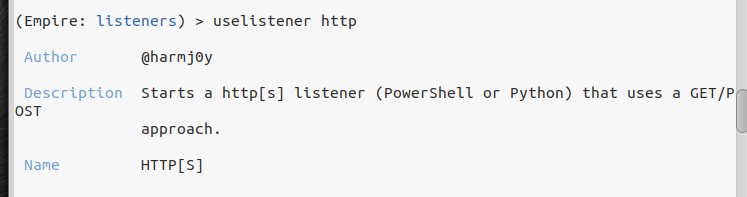
Stagers: Các stagers là các tệp PowerShell hoặc Python nhỏ được sử dụng để khởi động kết nối giữa máy mục tiêu và máy chủ kiểm soát Empire.

Listeners: Các listeners là các máy chủ lắng nghe trên máy chủ kiểm soát Empire, chờ đợi các kết nối từ các stagers.

Modules: Empire cung cấp một loạt các modules cho các chức năng khác nhau như lấy dữ liệu, tạo và thực thi mã độc, thu thập thông tin, và nhiều hơn nữa.

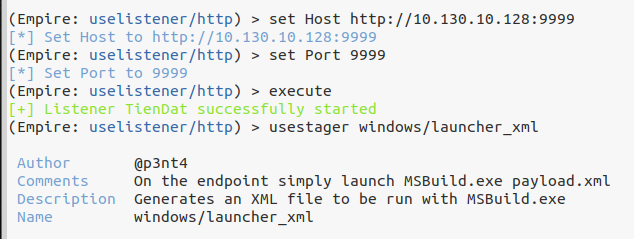


Cài đặt tên máy chủ lắng nghe là http



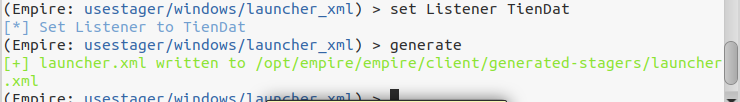
-Cài đặt server

-Tạo file launcher\_xml



-Cài đặt tên máy client lắng nghe là TienDat

-Tạo file launcher.xml thành công



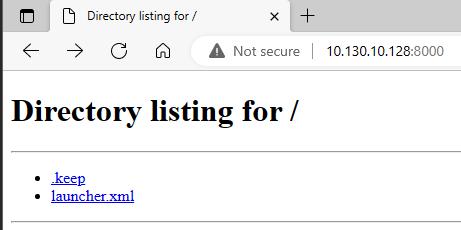
Mở terminal mới, chuyển đến địa chỉ chứa stager (tệp chạy powershell)



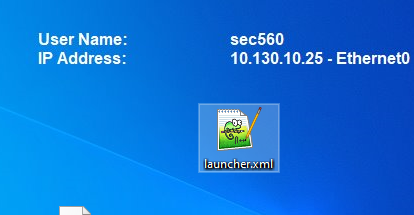
Thiết lập dịch vụ http mới



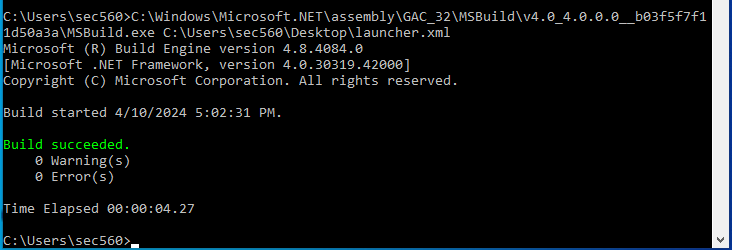
-Windows vào server



-Tải file launcher.xml về



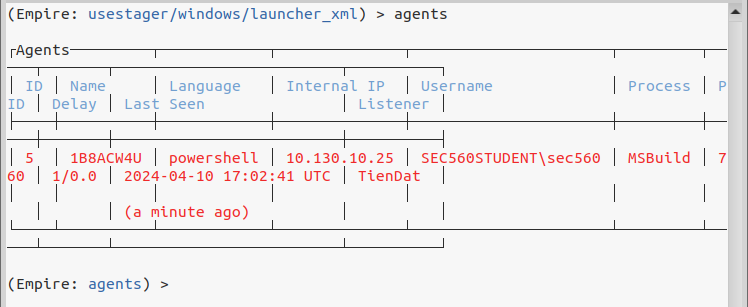
-Chạy file launcher



Bên server thiết lập kết nối thành công



-Kiểm tra thông tin



5.Bonus

6.Cleanup