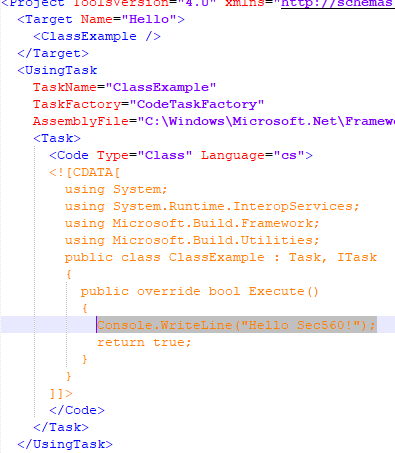
MsBuild

1. Setup

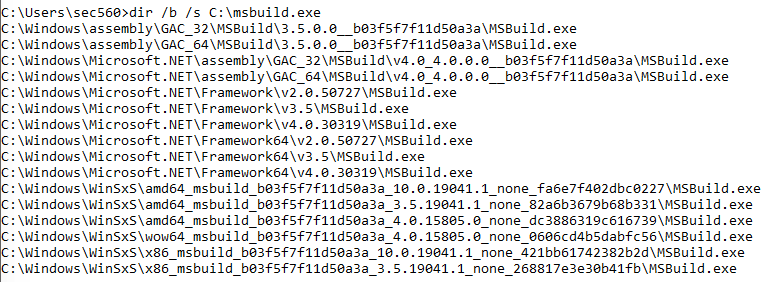
Mở file build1.xml, chèn đoạn code mới



1. Initial Testing

Lưu file build1.xml

Tìm file MsBuild.exe



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

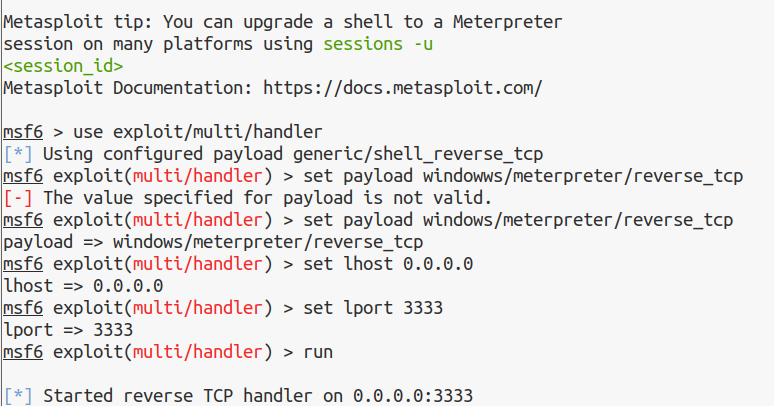
Công cụ này là 32 bit nên shellcode ta cũng cần 32bit

Run file build1.xml

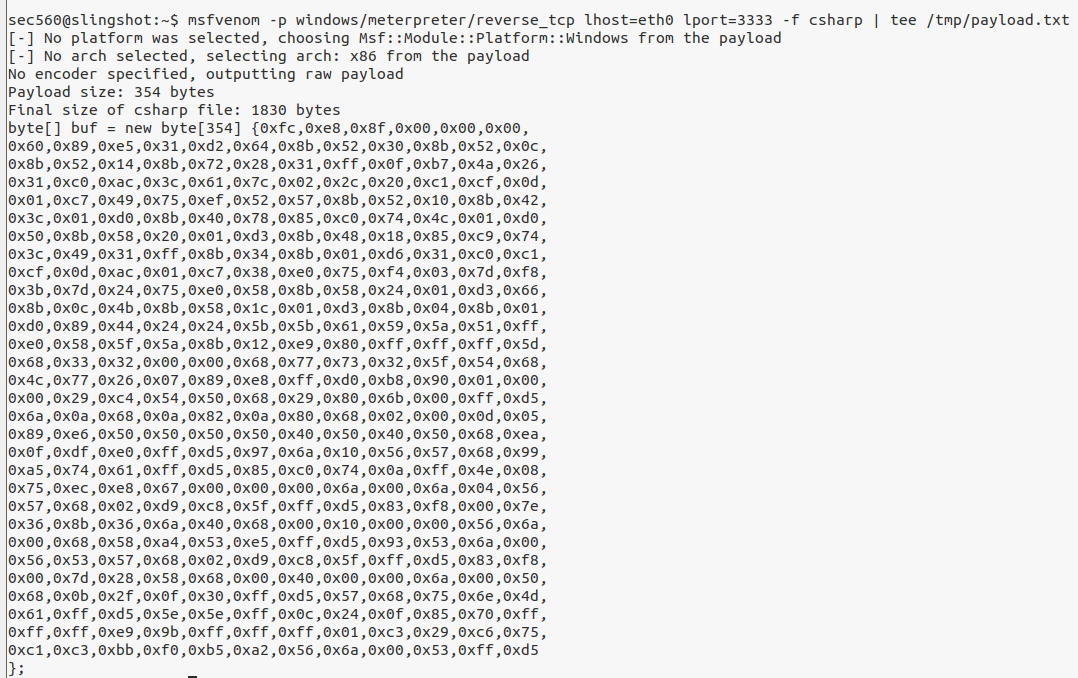


1. Meterpreter shellcode

Tạo 1 listener ở máy linux bằng Metasploit.

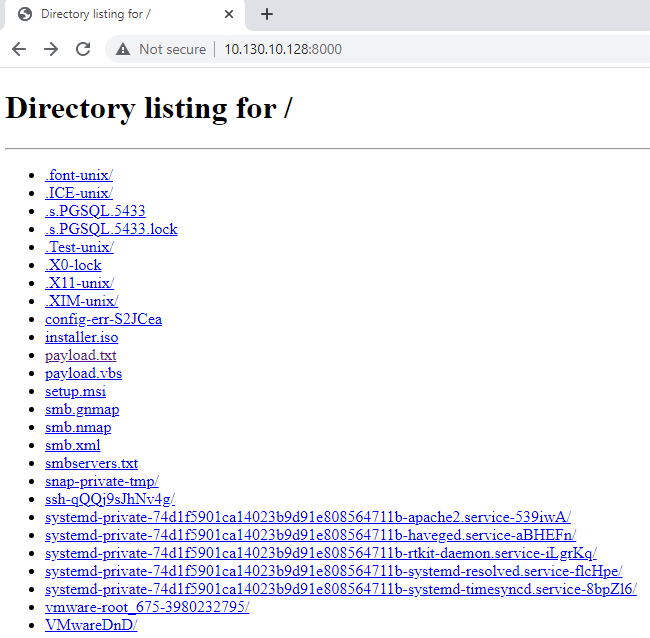


Tạo payload bằng msfvenom với format=csharp

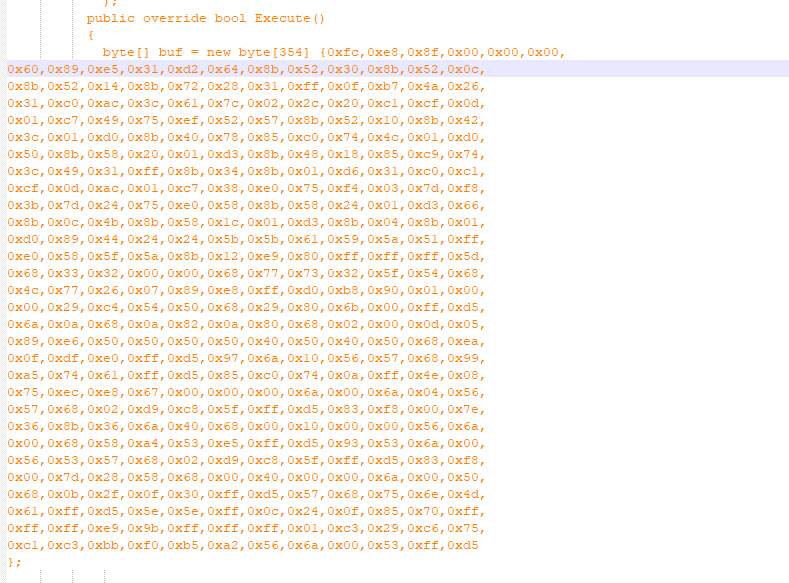


Khởi tạo http server để tải file payload về máy window



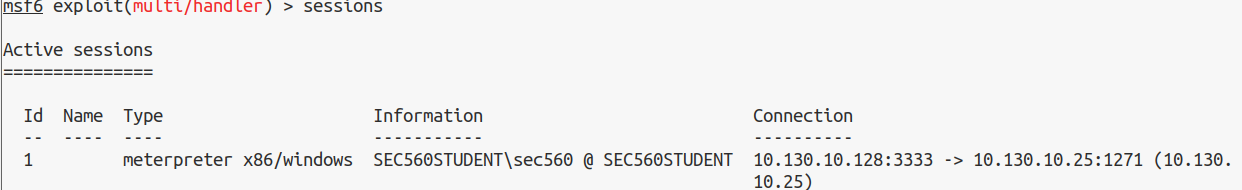


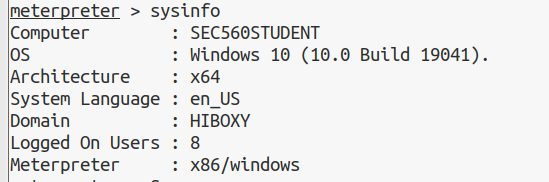
Mở file payload.exe và copy payload cho vào file bulid2.xml



Chạy file build2.xml bằng msbuild

* Thành công có được 1 session trên Metasploit





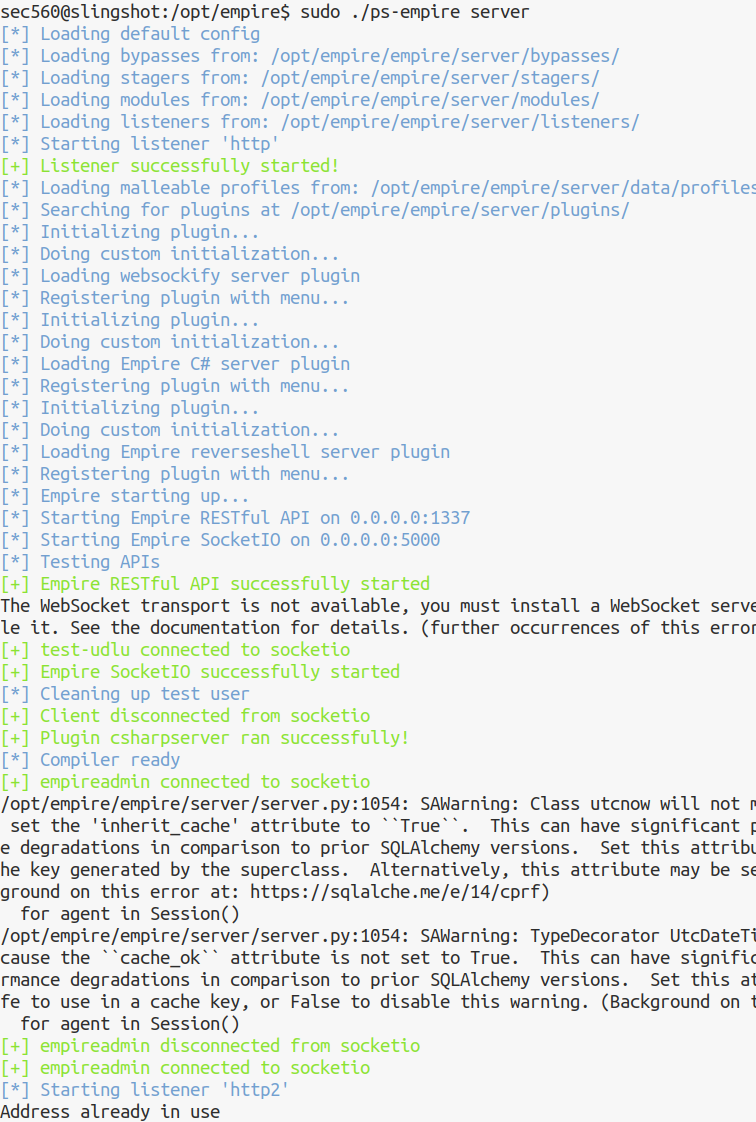
Có quyền admin

1. Empire

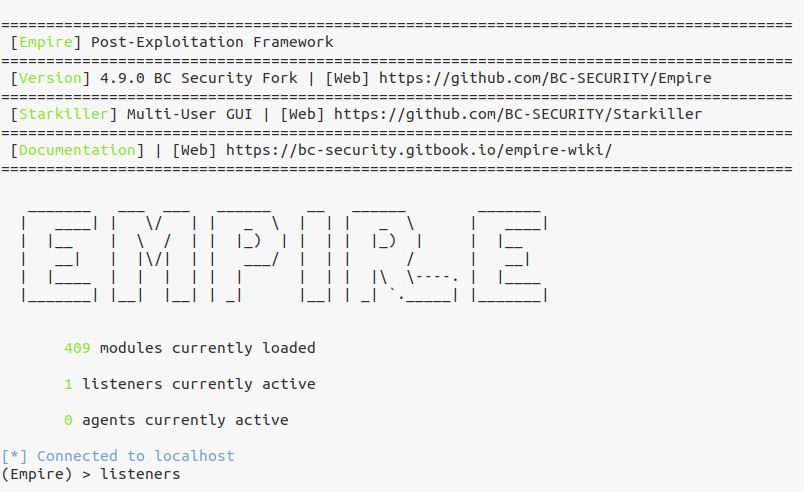
Tạo payload với Empire

Khởi động

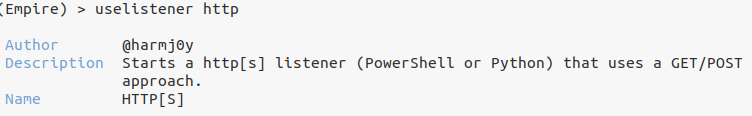
Khởi động server

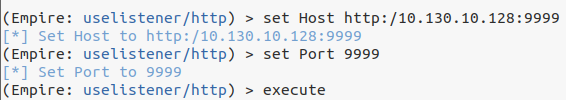


Khởi động client

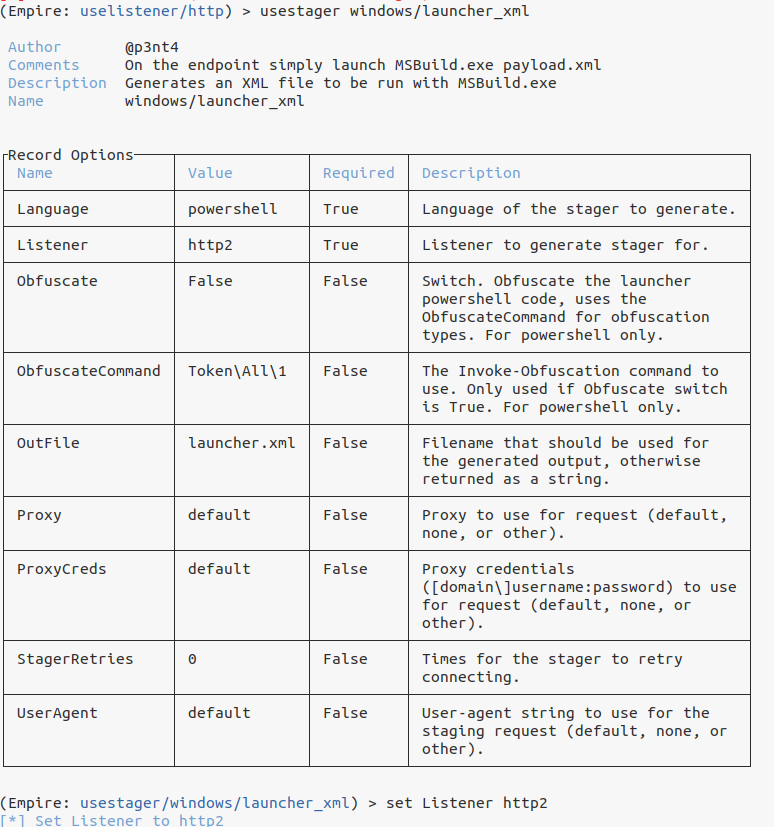


Cấu hình 1 listener





Build 1 file XML launcher



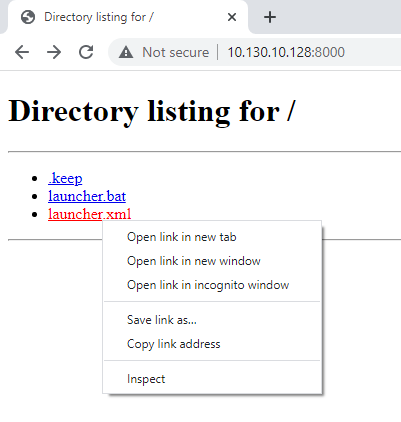
Generate file và được lưu vào đường dẫn



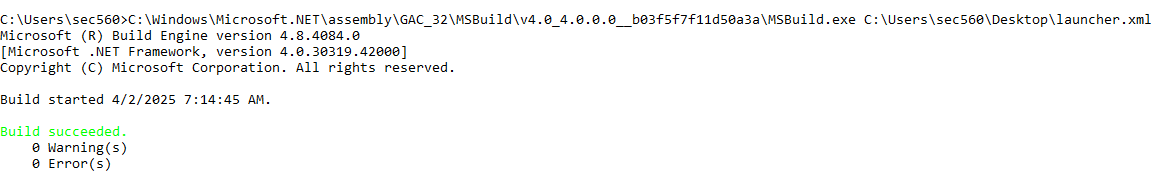
Tạo lại 1 web server



Sang máy window và lưu file vừa tạo ra Desktop



Chạy file với MSbuild



Thành công tạo 1 Empire agent

