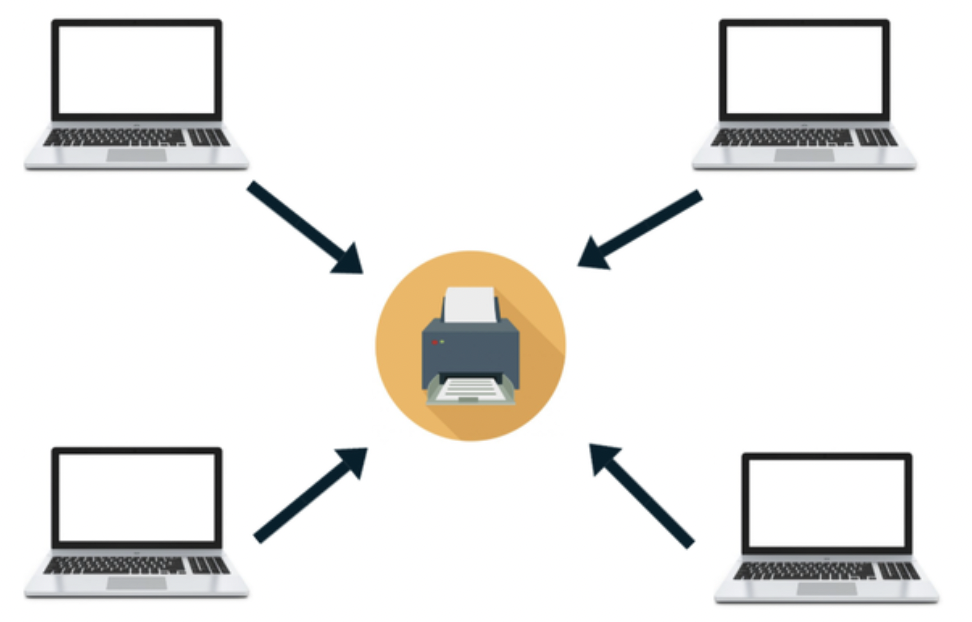
**PrintNightmare**

**Giới thiệu**

Chúng ta sẽ khám phá lỗ hổng PrintNightmare từ khía cạnh tấn công và phòng thủ.

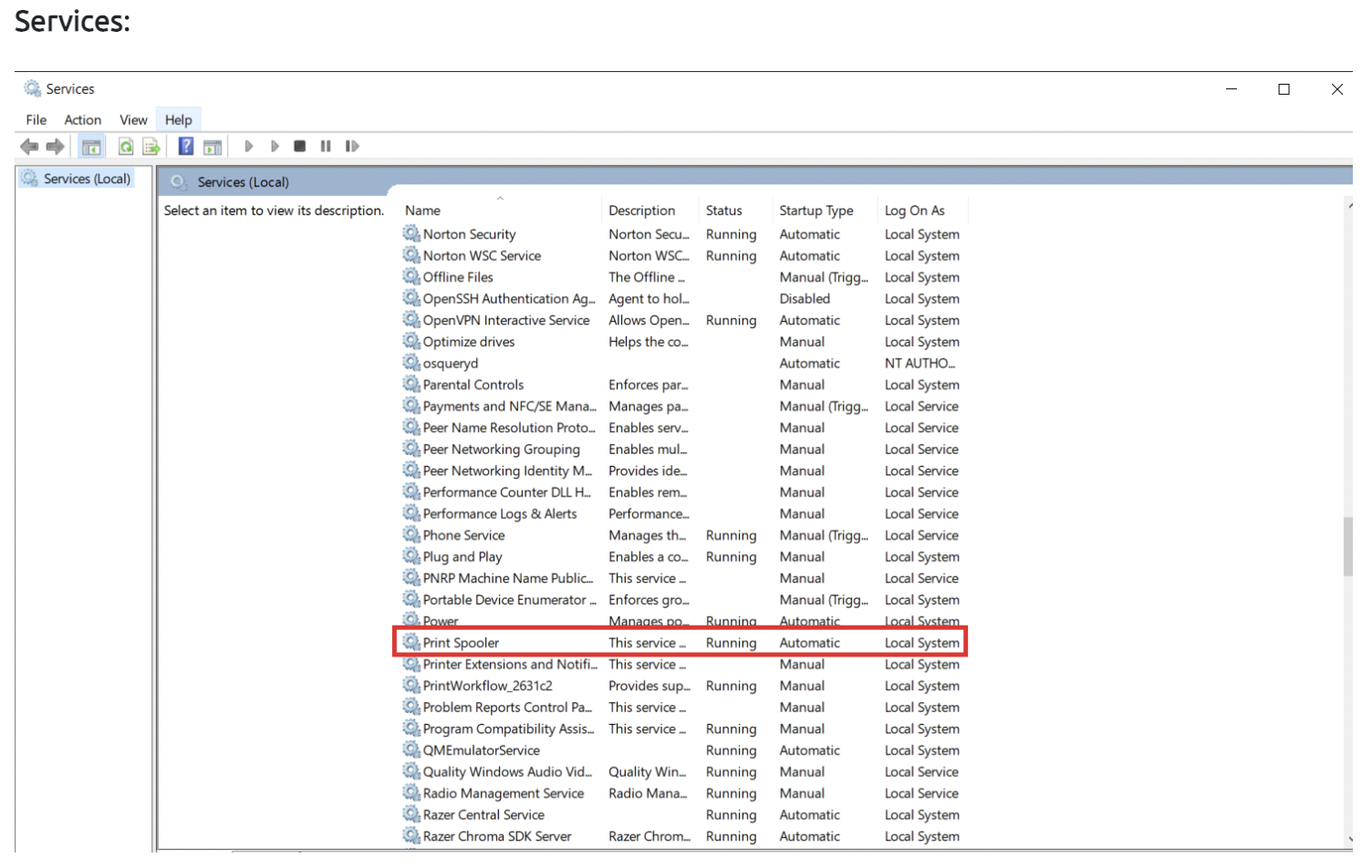
Theo Microsoft, lỗ hổng RCE tồn tại khi dịch vụ Print Spooler thao tác tập tin không đúng cách. Kẻ tấn công khai thác lỗ hổng này có thể chạy bất kỳ lệnh nào với đặc quyền của SYSTEM. Sau đó, họ cài đặt các chương trình; xem, thay đổi hoặc xóa dữ liệu; tạo tài khoản mới.

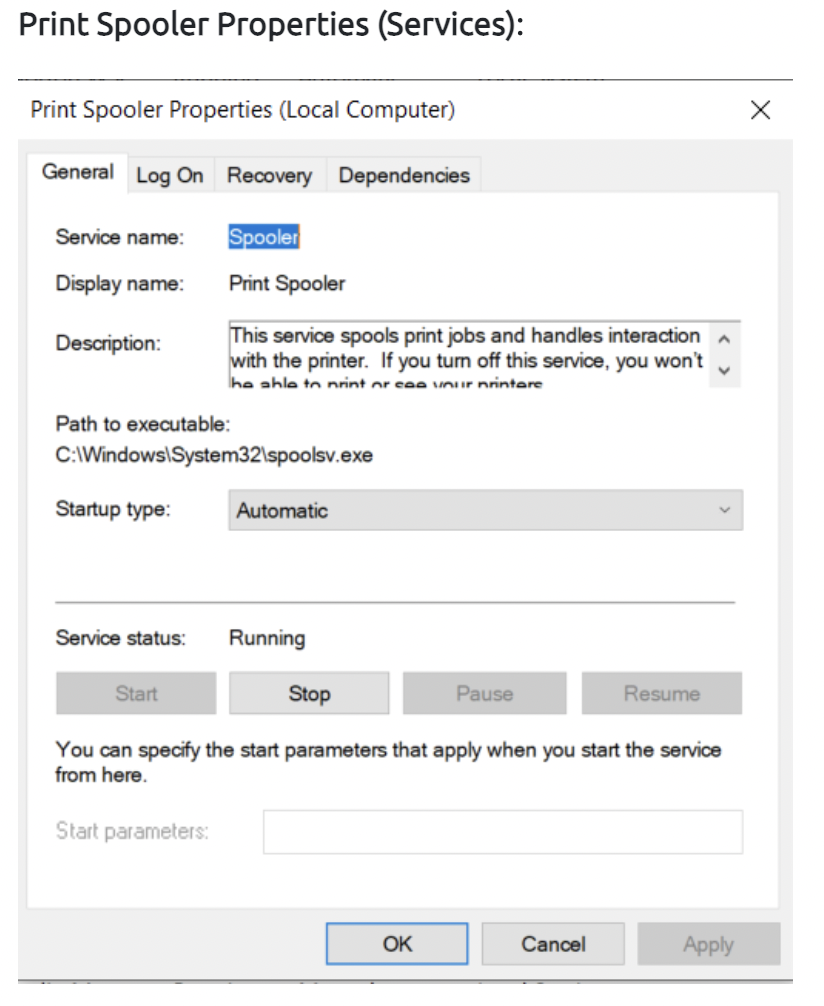
**Windows Print Spooler Service**



Print Spooler service là 1 dịch vụ chạy trên mỗi hệ thống máy tính. Print spooler service quản lý các tiến trình in. Print spooler chịu trách nhiệm quản lý công việc in, nhận các tập tin cần in, sắp xếp và lập lịch cho chúng.

Bạn có thể bắt đầu/kết thúc/dừng Print Spooler Service bằng cách chuyển đến Services trong hệ thống Windows.





Print spooler service đảm bảo cung cấp đủ tài nguyên cho các máy tính gửi công việc in. Nhớ những ngày đầu, khi người dùng phải đợi công việc in hoàn thành để thực hiện các hoạt động khác? Print spooler service giúp chúng ta giải quyết vấn đề trên.

Print spooler service cho phép các hệ thống hoạt động giống như print clients, administrative clients hoặc print servers. Print spooler service được thực thi mặc định trong tất cả máy khách và máy chủ Windows. Có 1 dịch vụ Print spooler trên máy tính để kết nối đến máy in rất cần thiết.. Có 1 phần mềm bên thứ ba hoặc drivers được cung cấp bởi nhà sản xuất máy in sẽ không yêu cầu bạn chạy dịch vụ print spooler. Tuy nhiên, hầu hết các công ty vẫn thích sử dụng Print spooler service.

Domain Controllers dùng print spooler service để bỏ bớt máy in (quá trình xóa các máy in không dùng nữa trên mạng và được thêm làm đối tượng vào Active Directory). Việc cắt bớt máy in sẽ loại bỏ vấn đề người dùng tiếp cận với một máy in không tồn tại. Bạn sẽ sớm biết tại sao chúng tôi đề cập đến Domain Controllers.

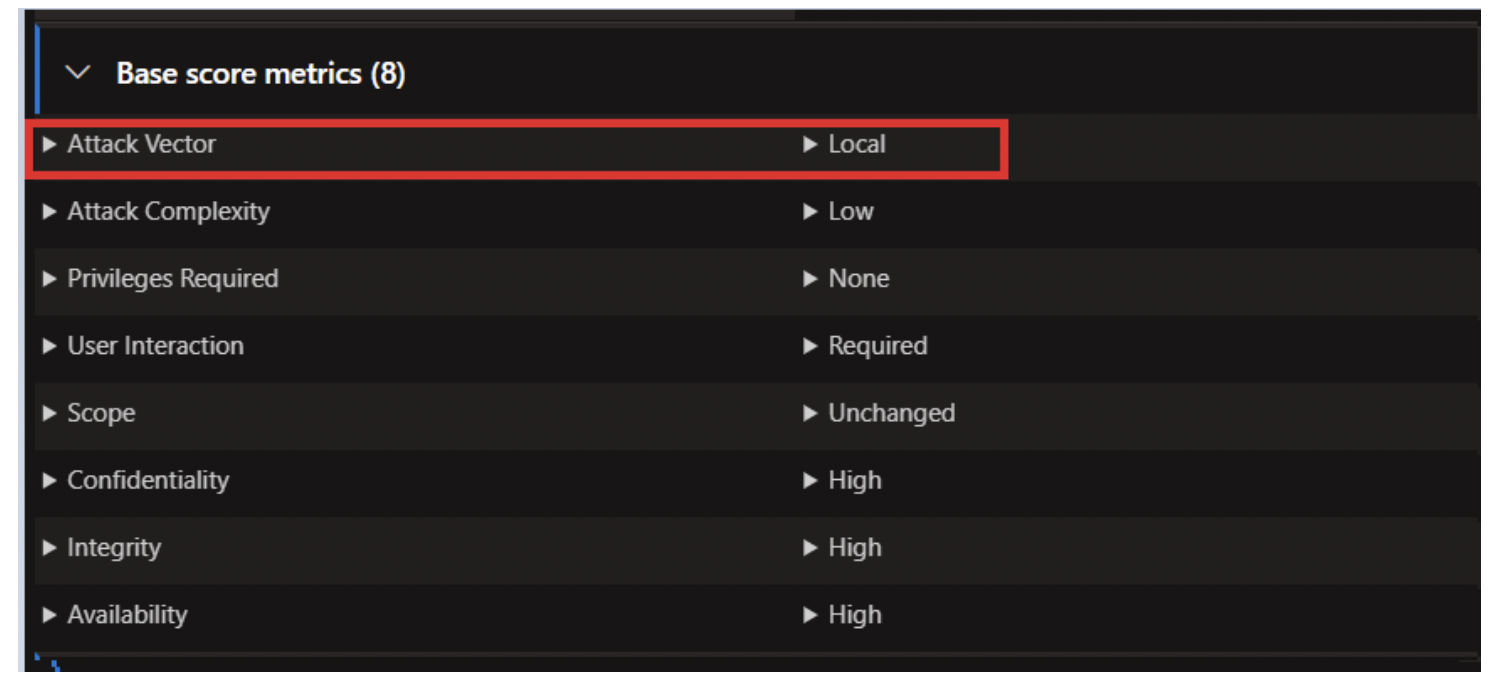
**Lỗ hổng thực thi từ xa**

Để hiểu rõ hơn về lỗ hổng PrintNightmare, bạn nên có thói quen nghiên cứu lỗ hổng bằng cách đọc các bài báo của Microsoft trên bất kỳ CVE nào dành riêng cho Windows hoặc duyệt qua Internet để tìm các bài đăng trên blog của cộng đồng và nhà cung cấp.

Lỗ hổng PrintNightmare (CVE-2021-34527) tương tự nhưng khác với lỗ hổng CVE-2021-1675. Phương pháp tấn công cũng khác nhau.

Để khai thác CVE-2021-1675, kẻ tấn công cần truy cập trực tiếp hoặc cục bộ đến máy ảo để dùng tập tin DLL độc hại. Để khai thác CVE-2021-34527, kẻ tấn công có thể tiêm tập tin DLL độc hại từ xa.

Số liệu về CVE-2021-1675:



Số liệu về CVE-2021-34527



Điều gì làm cho PrintNightmare trở nên đáng sợ?

1. Nó có thể được khai thác qua mạng; kẻ tấn công không cần truy cập đến máy ảo trực tiếp

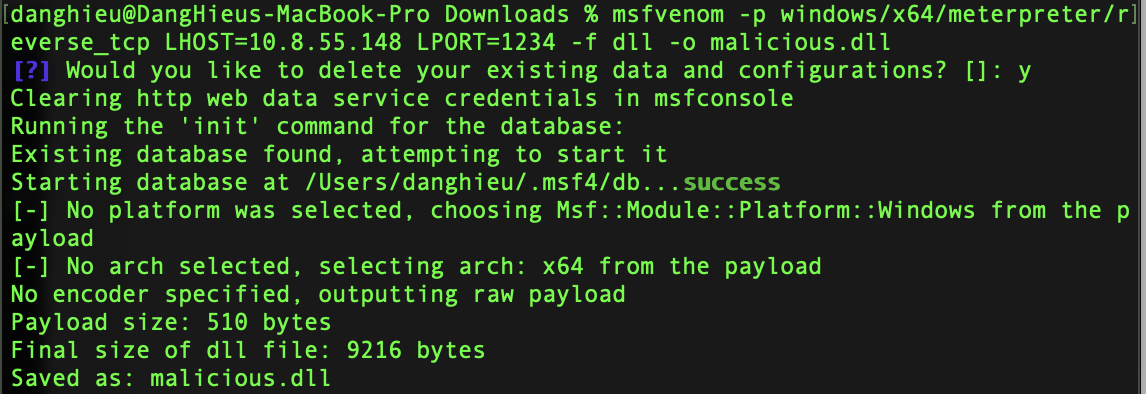
2. POC được public trên Internet

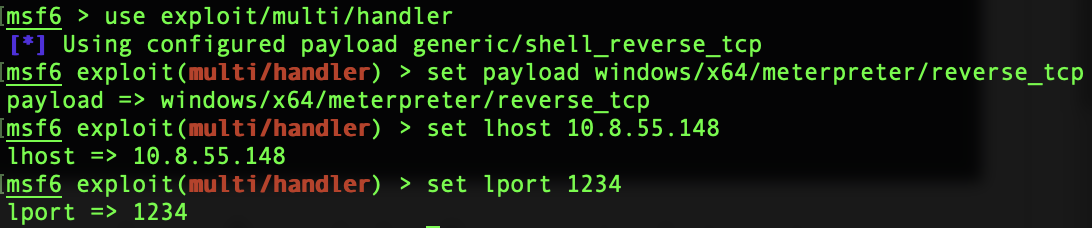
3. Print Spooler service được bật mặc định trên domain controllers và các máy tính với đặc quyền của SYSTEM.

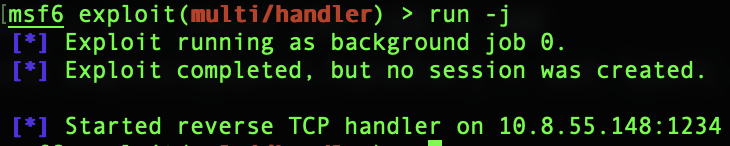
**Try it yourself**

Theo dõi các bước sau để khai thác Domain Controller bằng cách khai thác lỗ hổng PrintNightmare.

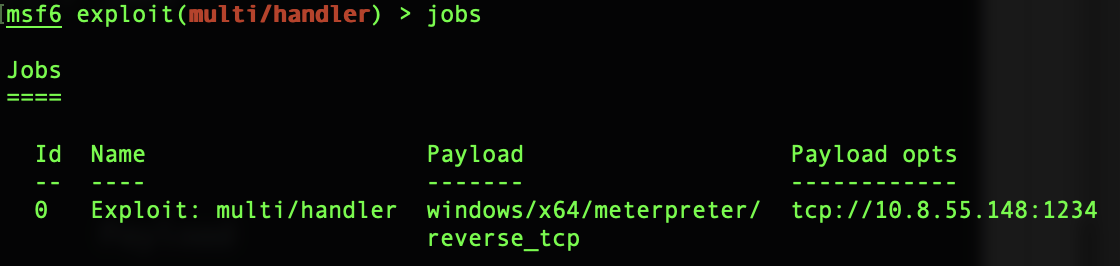
Dùng msfvenom để tạo DLL độc hại:



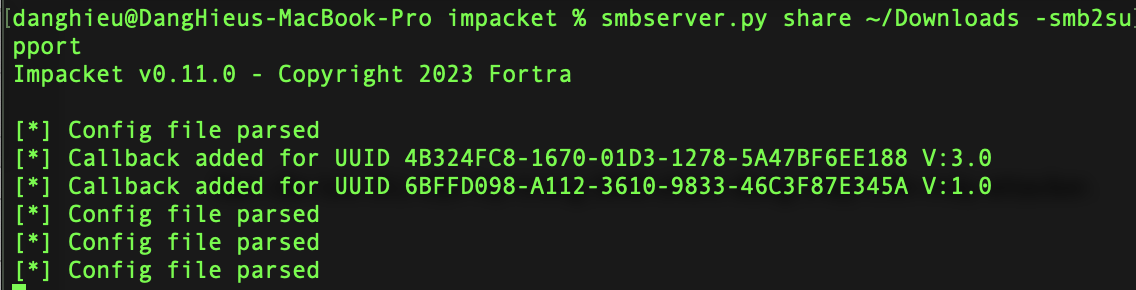




Flag -j: bạn đang chạy nó như 1 job



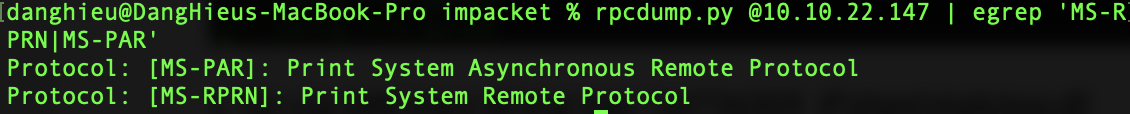
Bạn cần lưu DLL độc hại trong SMB share đang chạy trên máy attacker.



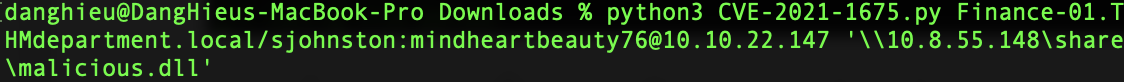
1. Tên của SMB share để khai thác: \\ATTACKER\_IP\share\malicious.dll

2. Thư mục cục bộ sẽ lưu DLL độc hại: ~/Downloads/malicious.dll

Trước khi chúng ta mù quáng khai thác mục tiêu, hãy kiểm tra xem máy nạn nhân có phù hợp với tiêu chí để khai thác không:

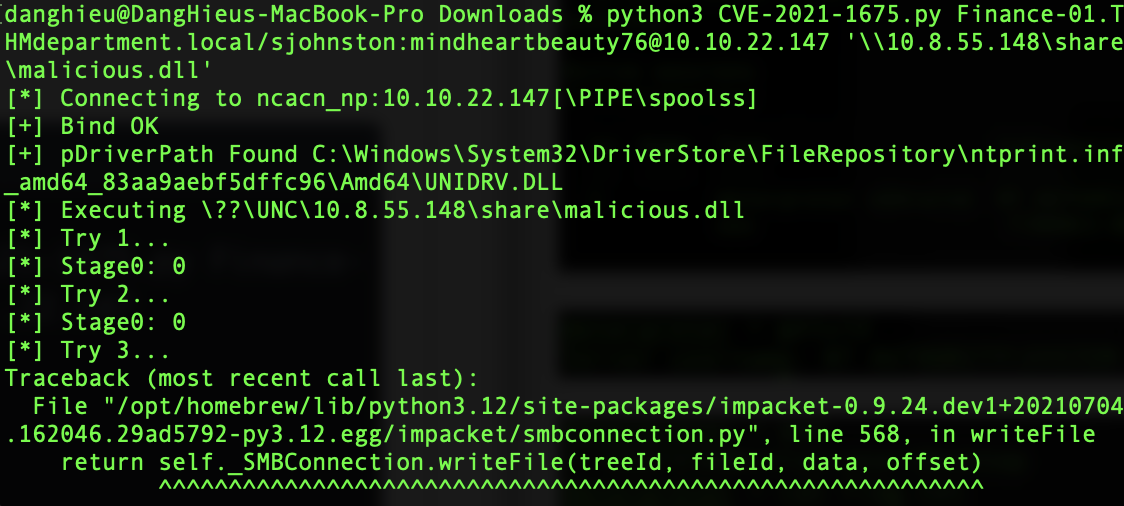


Đúng, có vẻ tốt. Cuối cùng cũng đến lúc chạy khai thác.



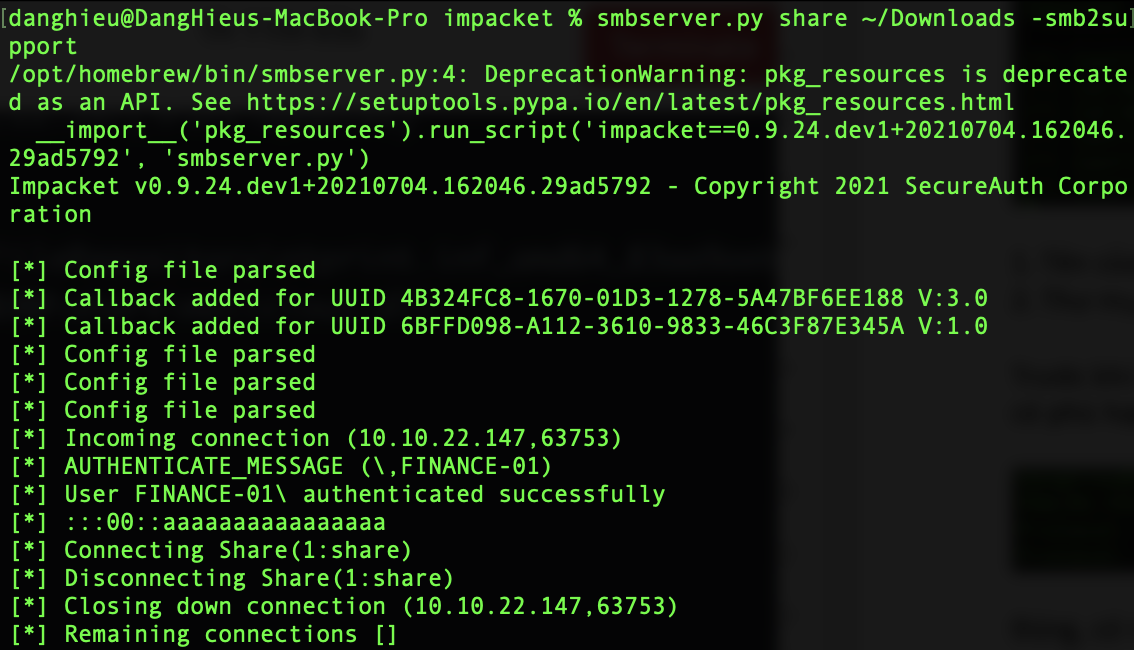
* Finance-01.THMdepartment.local: tên của domain controller (Finance-01) cùng với tên miền (THMdepartment.local)
* sjohnston:mindheartbeauty76@10.10.22.147: username và password cho tài khoản người dùng Windows có đặc quyền thấp
* \\ATTACKER\_IP\_ADDRESS\share\malicious.dll: nơi SMB lưu trữ DLL độc hại

Nếu mọi việc suôn sẻ, bạn sẽ thấy kết quả sau:



Bạn có thể thấy các lỗi Python sau Try 3

Kết nối SMB đang gọi DLL độc hại:



Cuối cùng, bạn có phiên Meterpreter thành công:

