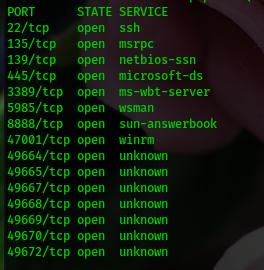


Hôm nay mk trở lại với 1 bài mới được ra mắt trên Tryhackme có tên là Weasel. Trước khi vào bài này thì mk xin nói 1 chút về bài Busqueda – HTB. Thì ở bài đó, khi leo thang lên root thì hướng SUID trong bài mk làm là không chuẩn, tệp /usr/local/bin/bash do 1 người dùng khác họ đã leo thang thành công nên họ đã set SUID cho tệp đó =)).

1. **Dò quét**

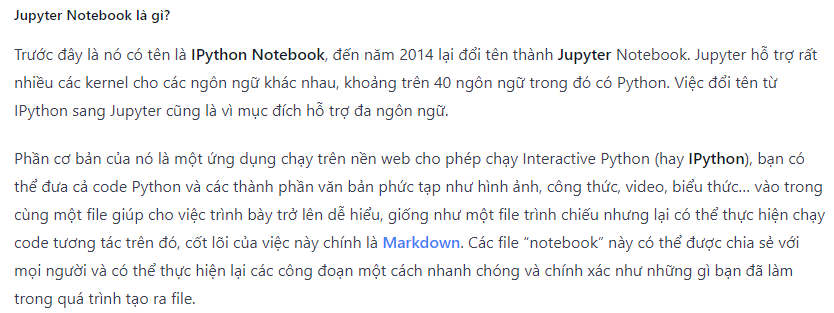
nmap -p- --min-rate=2500 -v 10.10.154.246 -Pn



Với kết quả này chúng ta biết được OS là Windows. Trong trường hợp này thì những port 22, 3389, 5985 mk sẽ động đến nó sau. Dịch vụ SMB và Web, mk sẽ ktra trước.

1. **Enum**

Ở cổng 8888, đang chạy Jupyter Notebook. Ngày trc khi báo cáo bài tập lớn trên trường, mk thấy các bạn trong lớp cũng hay dùng cái Jupyter này để làm project.

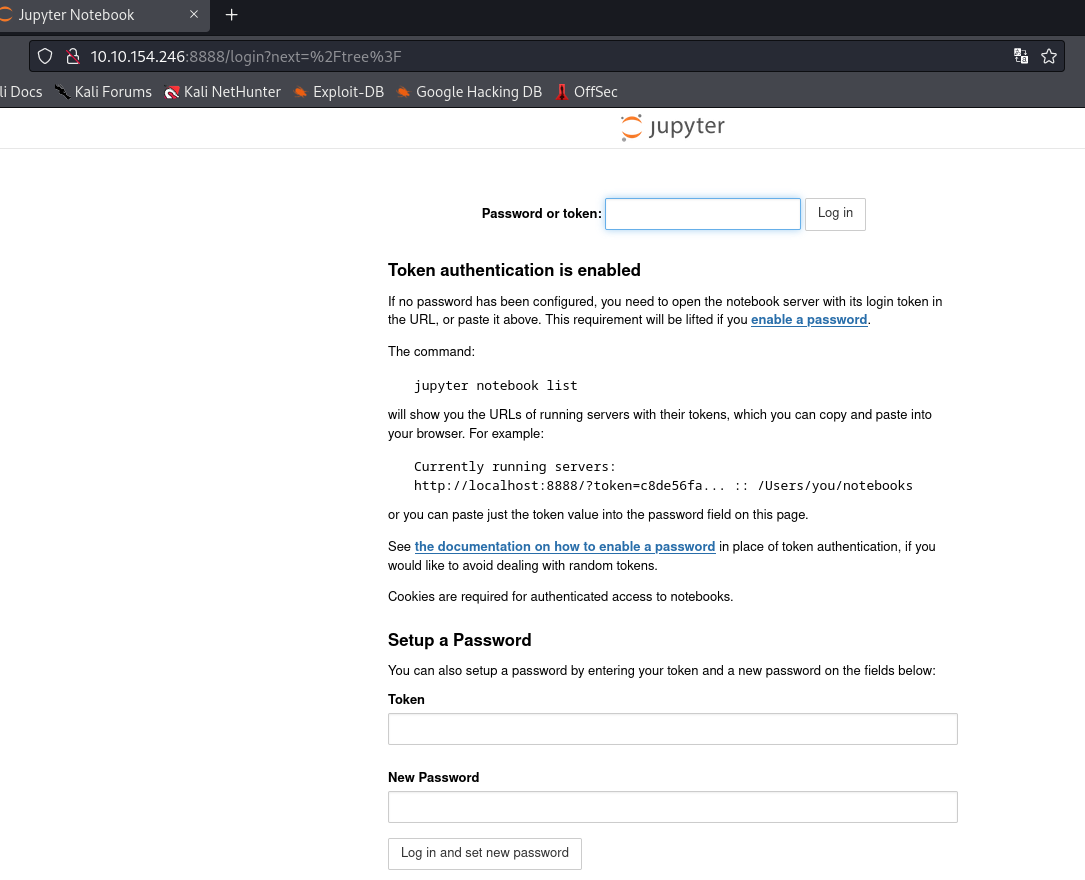


Đó là giới thiệu, còn điều mk quan tâm là cái Jupyter Notebook này cho phép chúng ta chạy code trên đó và nó sẽ trả lại kết quả cho chúng ta. Đây là ví dụ minh họa:

A screenshot of a computer

Description automatically generated with medium confidence

Từ ví dụ trên thì attacker có thể thực thi code => RCE để chiếm quyền kiểm soát máy. Đương nhiên, để vào được giao diện này thì chúng ta cần phải có user/pass.

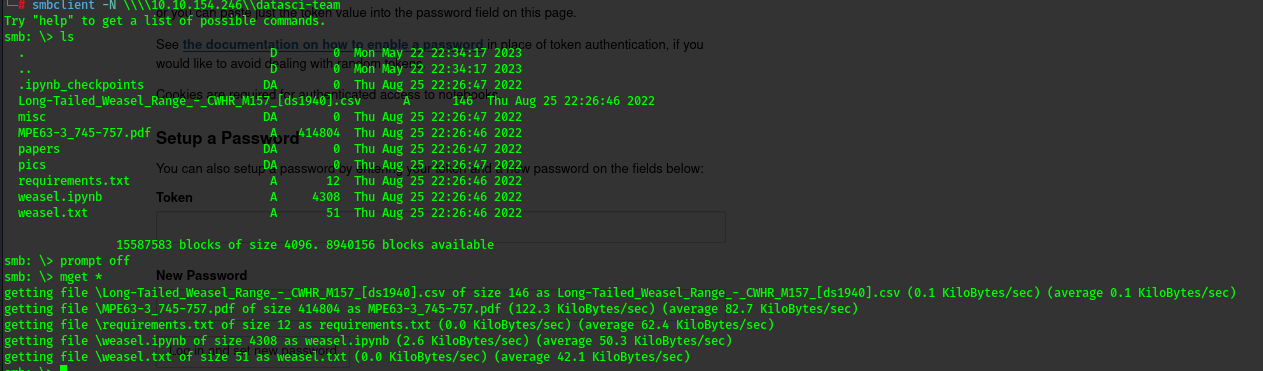


Ở đây nó bắt nhập token/password. Thử 1 vài weak password xem sao: admin, password, root, toor,……Fail.

Nhiệm vụ bây giờ phải đi kiếm token/password để login vào giao diện chính. Vậy token/password nằm ở đâu? Mk quyết định check thử xem ở dv SMB có anonymous share folder nào không, nhiều trường hợp quản trị viên họ lộ file password ở đây. Và kết quả là:

A screen shot of a computer program

Description automatically generated with low confidence



Đọc mấy file tải về này cũng ko tận gì được gì mấy. Mk thử vào mấy folder misc, papers, pics xem có gì ở đó không.

A screenshot of a computer

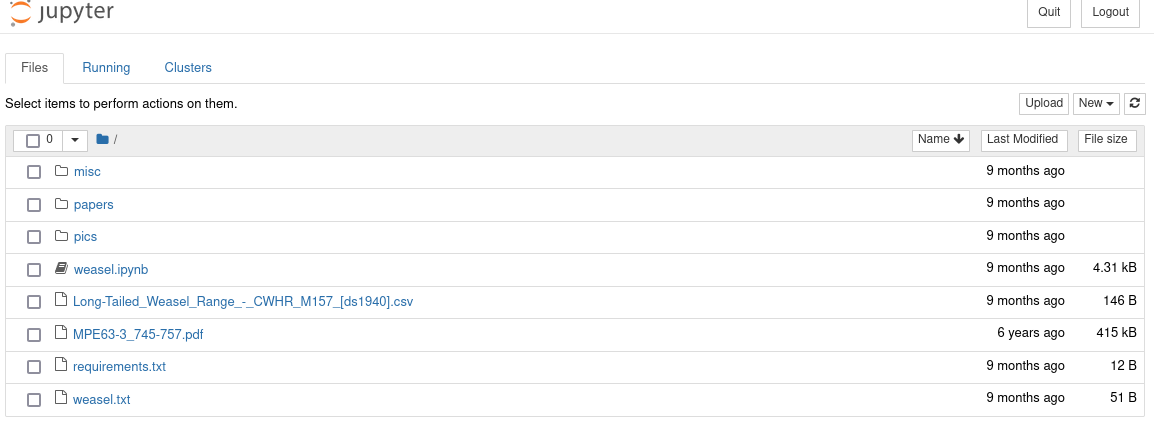
Description automatically generated with medium confidence

Token đây rồi.

A screenshot of a computer

Description automatically generated with medium confidence

Dùng nó để login và đây là giao diện sau khi đã login thành công



File thực thi code là file .ipynb. Khi xem file weasel.ipynb thì có mk phát hiện ra 1 username.

A screenshot of a computer

Description automatically generated with medium confidence

Mà thôi, cái username này để sau đi, RCE cái đã rồi tính tiếp =)).

1. **Exploitation**

Do OS là windows và backend sử dụng python => cần tìm reverse shell cho phù hợp

A screenshot of a computer

Description automatically generated

Tiến hành chạy code trên Jupyter

A screenshot of a computer program

Description automatically generated with medium confidence

Sau khi chạy thì get được shell nhưng lạ ở chỗ shell này ko phải của Windows

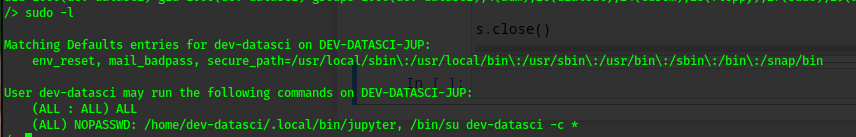
A screenshot of a computer program

Description automatically generated with medium confidence

Phán đoán: liệu đây có phải là 1 docker container ? hay trong dải mạng còn các machine khác? Thì ở đây mk tiến hành enum trên local thì đều không phải 2 trường hợp đã nêu trên. Vấn đề này mk sẽ giải quyết ở phần sau.

1. **Leo thang**

Trước tiên, mk sẽ leo từ dev-datasci lên root trước đã.

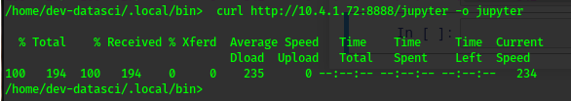


Tận dụng /home/dev-datasci/.local/bin/jupyter để leo lên root user

Vì file jupyter nằm ở thư mục của dev-datasci và chúng ta có quyền sửa/xóa nó => tạo file jupyter mới để get shell.

A screenshot of a computer program

Description automatically generated with medium confidence



A picture containing screenshot, green

Description automatically generated

Và đây là kết quả:

A picture containing text, screenshot, font

Description automatically generated

Quay trở lại vấn đề vừa nêu ở trên, thì để giải quyết nó mk thử hướng là: tìm tất cả các password trên shell của linux này rồi dùng nó login thử vào các dv SMB, RDP, WinRM. Sau khi ngồi khá lâu để tìm password, crack cả hash trong file /etc/shadow,…. Nhưng đều không thu được cái password nào. Mất nhiều thời gian mà không có kết quả và cũng ko có hướng giải quyết mới nào nên mk đành phải xem writeup phần này. Thì ra nó dùng WSL và c/ta sẽ theo hướng đó để leo lên “administrator” trên Windows

**Bài học rút ra:** trong quá trình leo thang mk đã quên một bước rất quan trọng, ấy là Research => chính vì thiếu bước đó nên dẫn tới việc phán đoán của mk bị thiếu xót các trường hợp khác. Những điều mà c/ta biết thường sẽ nhỏ hơn nhiều so với những công nghệ hiện có (vì công nghệ liên tục thay đổi và update không ngừng). Buồn hơn nữa là bản thân mk cũng đã dùng WSL =)) thế mà lại không nhớ ra.