# Lab 2.1: Password guessing

Trong lab này ta sẽ lấy danh sách người dùng từ domain controller rồi thực hiện spray password

Địa chỉ IP slingshot linux: 10.130.10.128

Kiểm tra kết nối từ máy Slingshot Linux đến địa chỉ 10.130.10.10 của máy Hiboxy DC

A screen shot of a computer code

Description automatically generated

1. Password spray (SMB)

Hiển thị 20 dòng đầu tiên trong danh sách tên người dùng

A screenshot of a computer

Description automatically generated

Ta thấy cái tên Smith khá là phổ thông, ta sẽ dùng danh sách này dể đóa mật khẩu ban đầu và một số mật khẩu phổ biến

Ta sử dụng hydra để tấn công vét cạn, với danh sách username và mật khẩu ở đây ta sử dụng là Spring2024

A screenshot of a computer

Description automatically generated

Tương tự với các mật khẩu được gợi ý trong workbook

A screenshot of a computer

Description automatically generated

1. The dictionary

Sử dụng list mật khẩu chứa các mùa, năm và mật khẩu phố biến là Password1

A screenshot of a computer

Description automatically generated

Dùng lệnh đếm số dòng trong file simple.txt, ta thấy có 26 mật khẩu trong file này



1. Password guessing

Ta biết một trong như QTV của Linux tên là Bruce Green, nên ta sẽ sử dụng bgreen để đoán mật khẩu

A screenshot of a computer screen

Description automatically generated

1. Verifying access

Trước tiên ta lấy list các system đang listen trên port 445 (SMB). Ta sẽ chỉ chạy nằm mục tiêu nmap cổng 445 và lưu kết quả đầu ra vào /tmp

A screen shot of a computer

Description automatically generated

Sử dụng grep để lọc ra các dòng trong tệp /tmp/smb.gnmap mà chứa chuỗi "445/open", sau đó sử dụng cut để tách các trường từ các dòng tìm thấy bằng dấu cách và lấy ra trường thứ hai từ mỗi dòng. Cuối cùng, kết quả được ghi vào tệp /tmp/smbservers.txt và cũng được hiển thị trên màn hình

Sử dụng hydra test xem tài khoản bgreen có đăng nhập được vào các địa chỉ hệ thống trên hay không

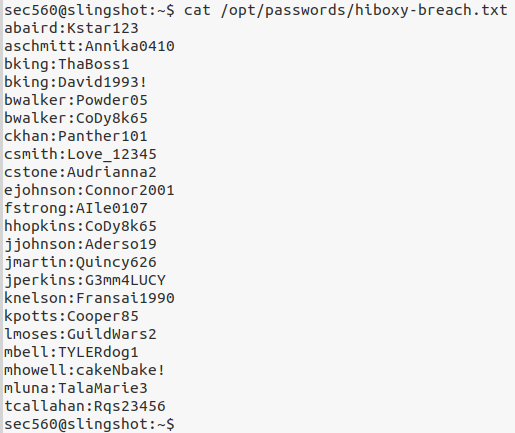
A screenshot of a computer screen

Description automatically generated

Có vẻ tài khoản này có quyền truy cập vào tất cả các hệ thống. Nếu tùy ý đăng nhập từ xa sử dụng tài khoản này có thể dẫn đến khóa máy.

1. Thông tin xác thực bị vi phạm

Xem thử list trong /opt/passwords/hiboxy-breach.txt được cung cấp.



Username & password được tách ra bởi dấu : nên ta có thể dùng hydra

Option -C chỉ định tệp tin danh sách tài khoản để sử dụng. Trong trường hợp này, danh sách được lưu trữ trong tệp /opt/passwords/hiboxy-breach.txt.

A screen shot of a computer

Description automatically generated

Ta tìm thấy 2 trong số các thông tin đăng nhập bị vi phạm vẫn đang hoạt động trong domain

1. Password spraying all domain users

Sử dụng script GetADUsers.py để truy vấn thông tin người dùng từ một máy chủ Active Directory với thông tin đăng nhập bgreen:Password1 trên miền hiboxy.com, sử dụng máy chủ điều khiển miền có địa chỉ IP là 10.130.10.10. Kết quả của truy vấn sẽ được ghi vào tệp /tmp/adusers.txt.

We also need to specify the IP address of the domain controller ( -dc-ip ) and tell the tool to get a list of all users with -all . We'll display the output on the screen and save the output with tee . A screenshot of a computer

Description automatically generated

Trích xuất danh sách người dùng. Nhìn vào kết quả hình trên ta bỏ qua 6 dòng đầu tiên rồi lấy mục đầu tiên trên mỗi dòng, dùng tail -n +6 để bỏ qua 6 dòng đầu tiên rồi cut để lấy cột đầu tiên, lưu vào /tmp/domainusers.txt

A screen shot of a computer

Description automatically generated

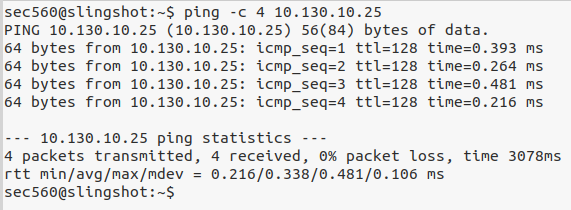
Thử spraying bằng Password1

A screenshot of a computer screen

Description automatically generated

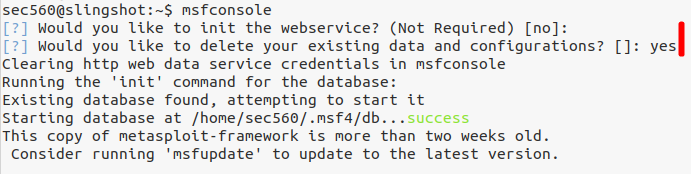
# Lab 2.2: Metasploit & Meterpreter

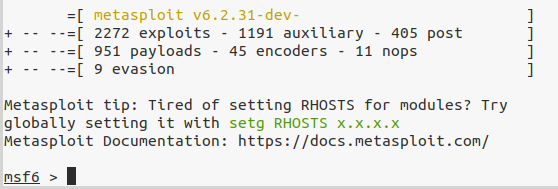
Kiểm tra kết nối từ slingshot linux đến win10



1. Metasploit on Linux

Mở metasploit bằng lệnh msfconsole



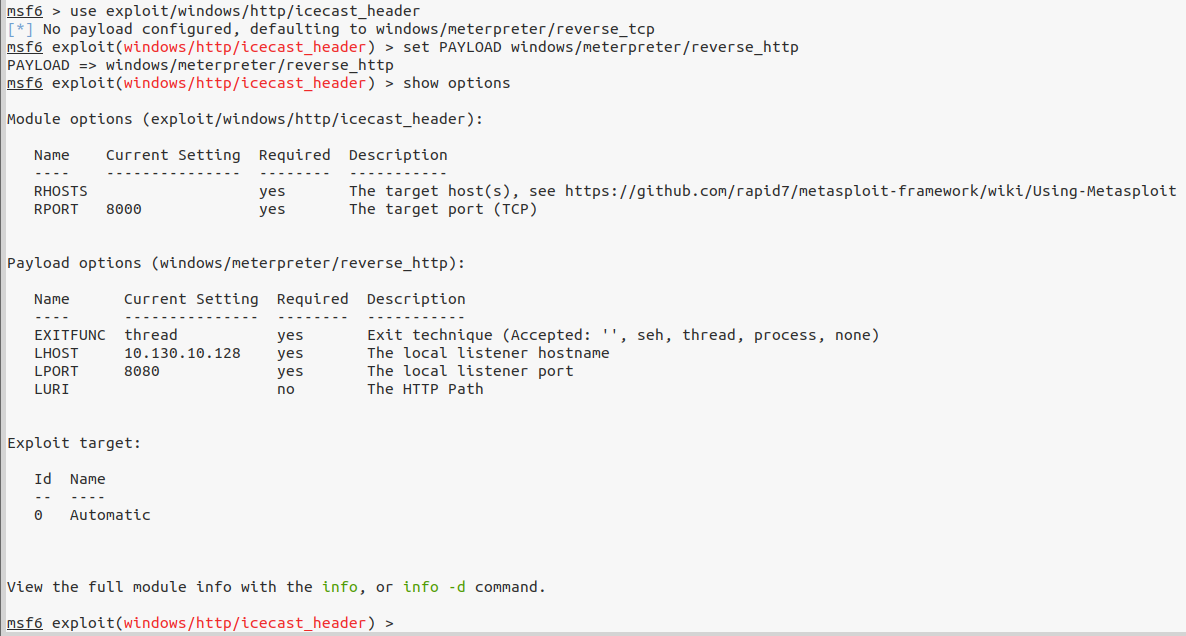


Tìm icecast. Icecast là một phần mềm máy chủ truyền phát media và mã nguồn mở, miễn phí được dùng để phát trực tiếp âm thanh video qua internet.



Ta tìm thấy module exploit window có tên là icecast\_header với ranking great. Ta sẽ khai thác sử dụng khai thác tràn bộ đệm Icecast Header

Ta sẽ chọn payload reversehttp. Reverse\_http sẽ gửi http request đến máy chủ tấn công, sau đó thiết lập kết nối TCP ngược từ máy nạn nhân về máy attacker



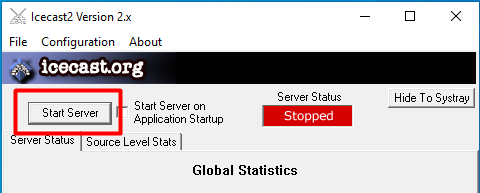
Ta sẽ set RHOSTS – địa chỉ mà ta muốn metasploit tấn công - bằng IP của win10

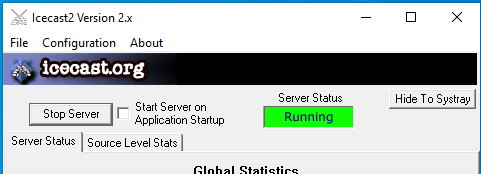
Set LHOST là địa chỉ ip của máy attacker để reverse shell kết nối đến



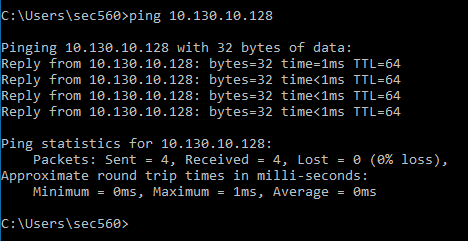
1. Setting window

Trước khi exploit bên Linux ta sẽ chuyển sang máy win 10, chạy icecast với quyền admin và click vào start server cho đến khi server status chuyển sang running

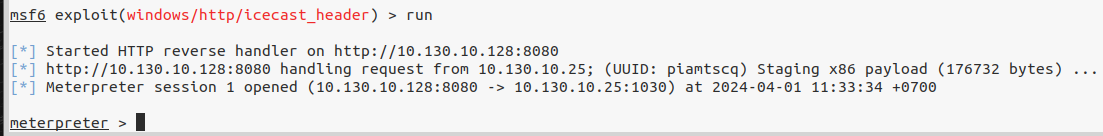




Mở cmd, ping thử sang ip của máy slingshot Linux, ở đây là 10.130.10.128

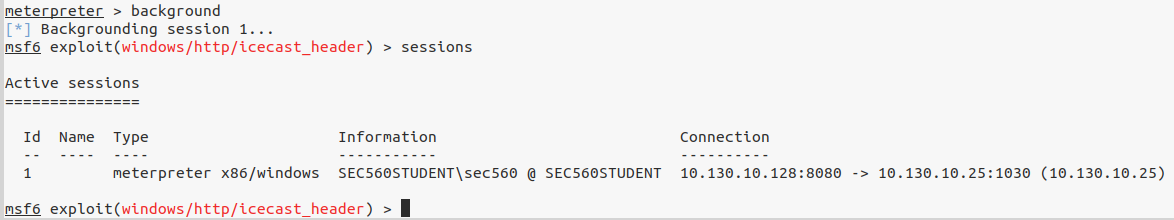


1. Launch the attack

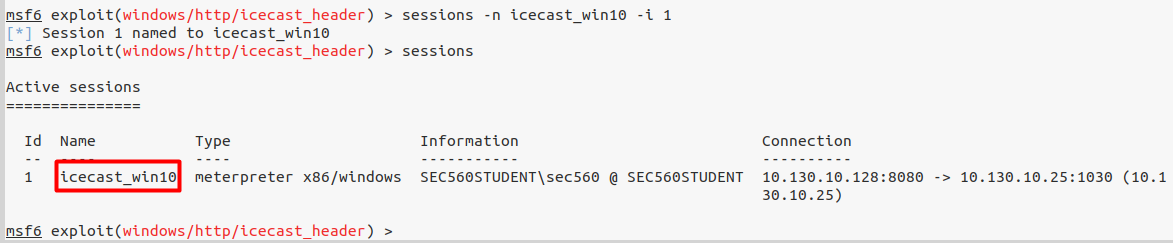


1. Sessions

Sau khi run ta sẽ được chuyển vào meterpreter. Nếu muốn thực hiện các hành động khác trong metasploit thì cần chạy session làm việc ở chế độ nền bằng lệnh background hoặc nhấn ctrl Z

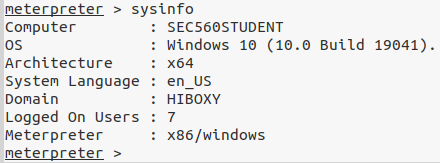


Để tránh nhầm tên phiên thì ta có thể dùng lệnh -n (newname) và -i (id) để đổi tên phiên có id 1 sang icecast\_win10



1. Meterpreter

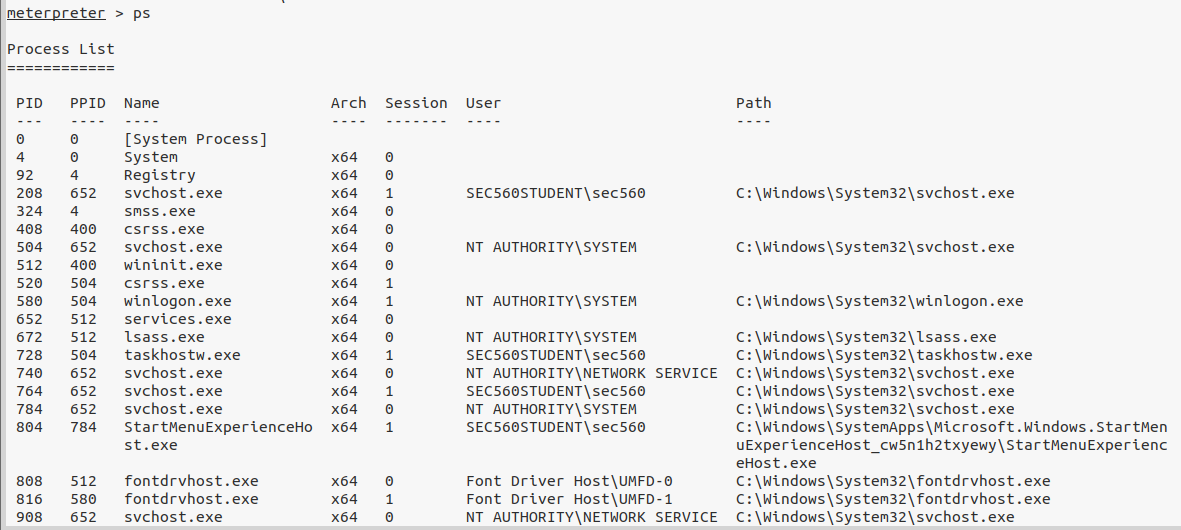
Dùng lệnh sysinfo để xem thông tin về hệ điều hành vừa bị ta xâm nhập vào.



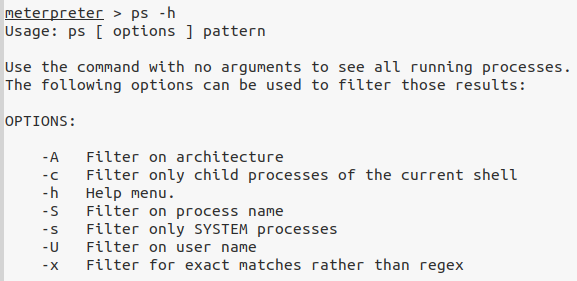
Getuid để biết username nạn nhân. Cần phải có cùng tên với username được dùng để gọi máy chủ icecaset vì đang chạy trong không gian bộ nhớ của nó.



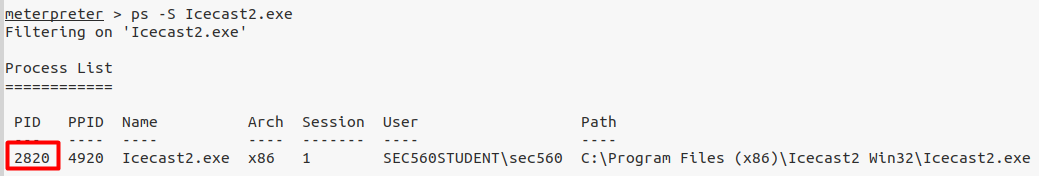
Chạy xem process



Thử xem có những câu lệnh gì có thể sử dụng với ps



Tìm process icecast của mình bằng -S



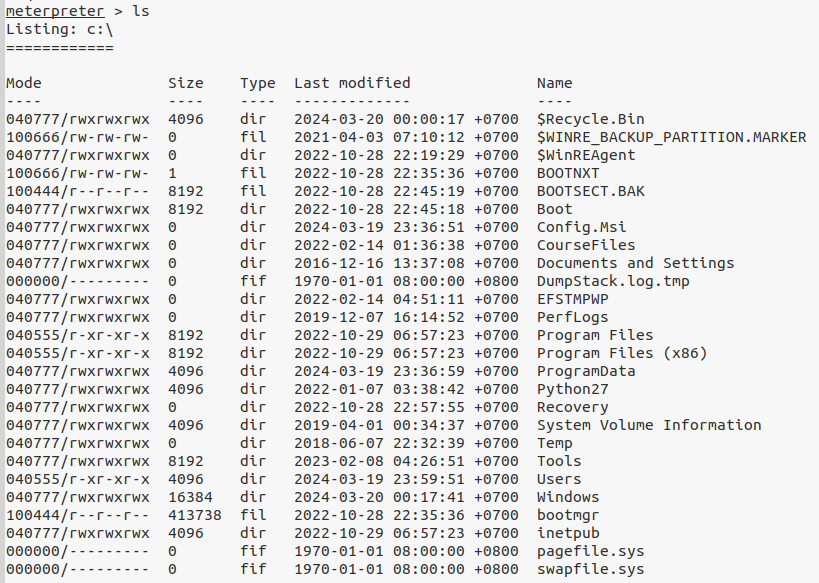
Process ID của Icecast2.exe là 2820

Chuyển sang ổ C

Pwd để xem đang ở đâu trong cấu trúc thư mục

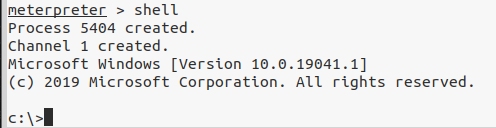


ls xem danh sách thư mục

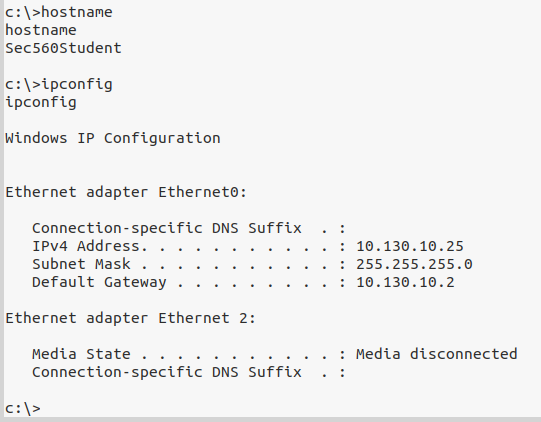


1. Shell

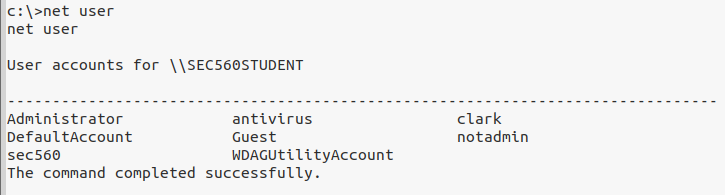
Chúng ta sẽ thử dùng lệnh shell mà meterpreter hỗ trợ



Giờ thì có thể gõ bất kỳ lệnh gì tùy thích như sử dụng cmd



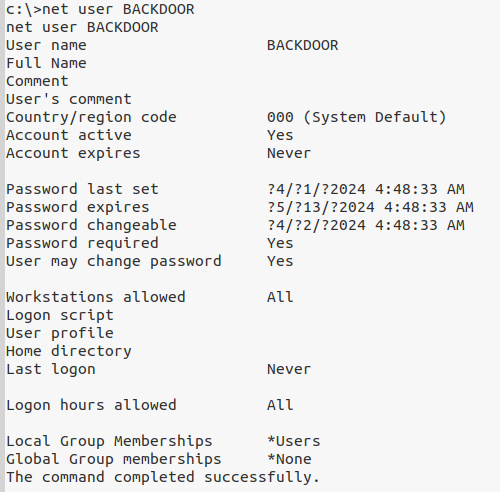
Xem các users trong hệ thống:

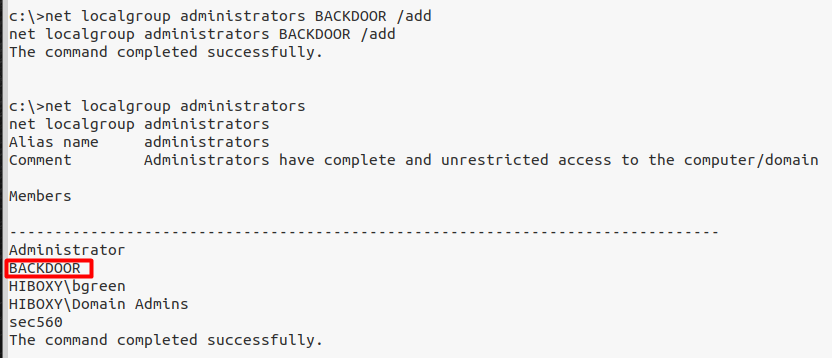


Tạo một account backdoor tên là BACKDOOR ở bước trên rồi xem xem user BACKDOOR có tồn tại chưa:

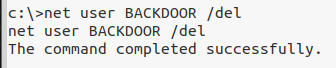


Tài khoản BACKDOOR vừa tạo là tài khoản thường, để khai thác nhiều hơn mình sẽ đặt tài khoản này làm QTV. Rồi xem các thành viên của nhóm QTV để confirm tài khoản BACKDOOR đã là QTV





Remove account và exit

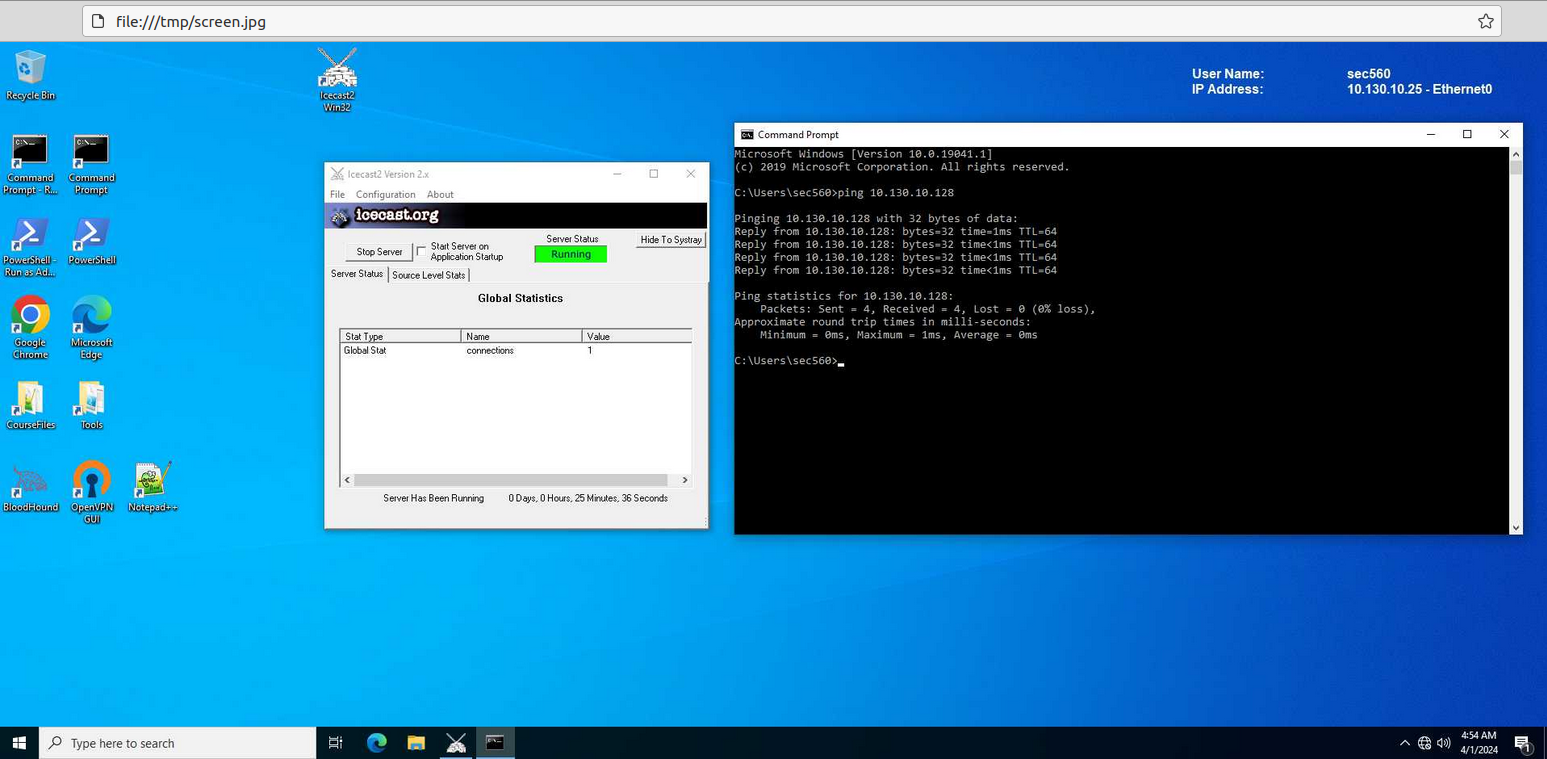
 

1. More meterpreter features

Thử chụp màn hình của system bị khai thác và lưu nó vào:

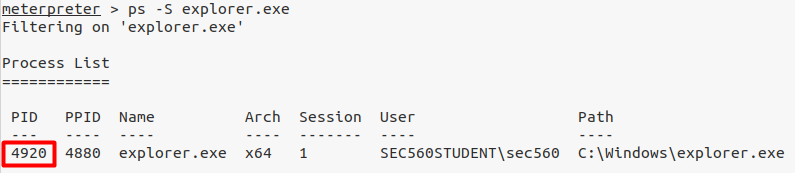


Sau đó mở Firefox rồi tới location, sẽ thấy hình sau:

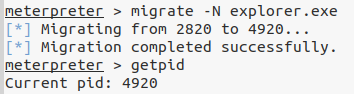


Tiếp theo sẽ di chuyển Meterpreter DLL trên máy bị khai thác từ tiến trình này sang tiến trình khác. Sẽ chuyền từ Icecast2.exe sang explorer.exe trên máy win. Dùng Explorer vì nó vẫn sẽ tiếp tục chạy miễn là user đăng nhập vào

Quay lại Meterpreter và lấy số ID tiến trình hiện tại, tìm PID của explorer.exe



Nhảy sang explorer.exe bằng lệnh migrate, chỉ định bằng tùy chọn -N

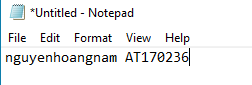


1. Keystroke logging

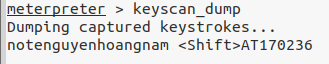
Sử dụng keyscan\_start. Đây là một tệp thực thi dùng để khởi động trình quét bàn phím đầu vào

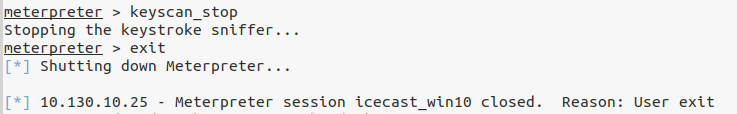


Mở win10, mở notepad, gõ vài dòng vào trong đó



Quay lại meterpreter và chuyển các lần nhấn phím đã quét được lên màn hình

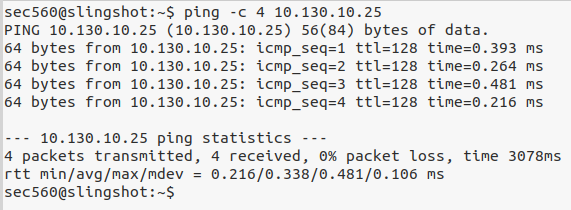




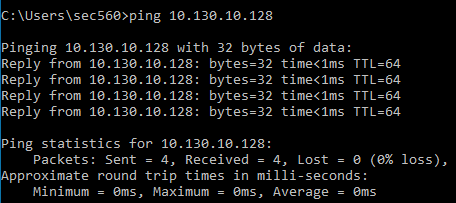
# Lab 2.3: Sliver

Để tạo một listener và tạo ra một payload để kết nối với listener

Ping sang IP của Win 10



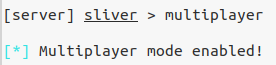
Ping IP của Linux



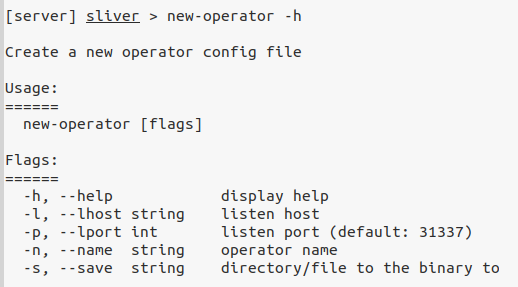
1. Starting sliver

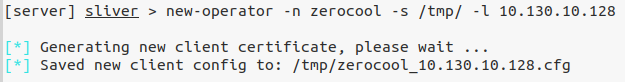


Multiplayer trên server cho phép ta cấu hình và thêm user mới để có thể hoạt động như một nhóm.



Tạo user mới





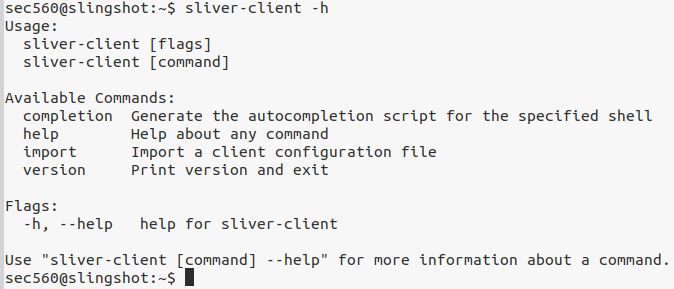
Kiểm tra file cfg



Như ta thấy file cfg trên chỉ cấp quyền rw cho user root, ta cần đổi qua user sec560



Kiểm tra option với client

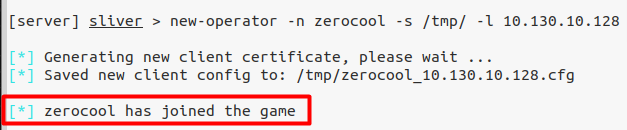


Import cfg file

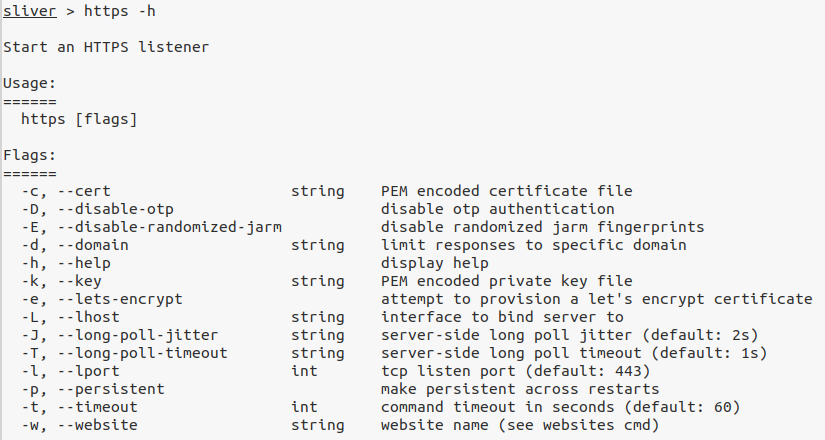


Dùng lệnh sau để kết nối đến server

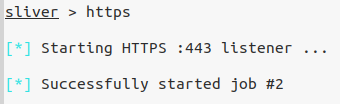




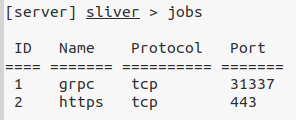
1. Creating a listener and an implant payload



Khởi động một listener

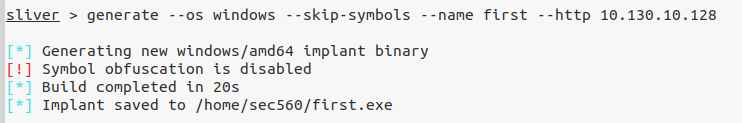


Kiểm tra jobs

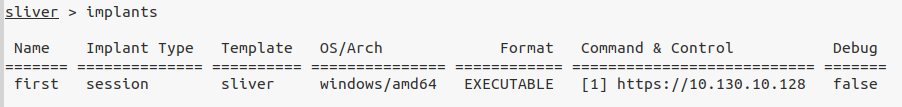


Remote user chạy trên cổng 31337, https listener p443

Tao payload để gửi đến window



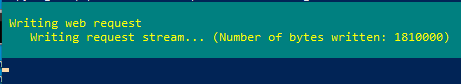
Kiểm tra payload

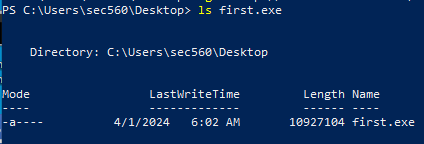


1. Sending the Payload to the Windows system





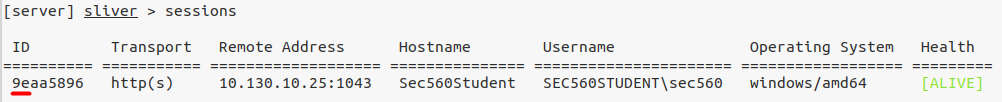




1. Executing the Payload





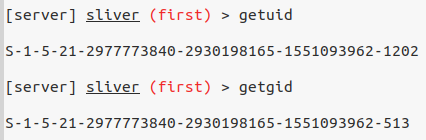


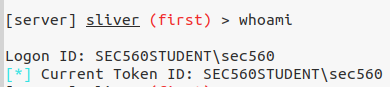
Thực hiện tương tác với session bằng cách sử dụng use + 2 chữ cái đầu của ID session

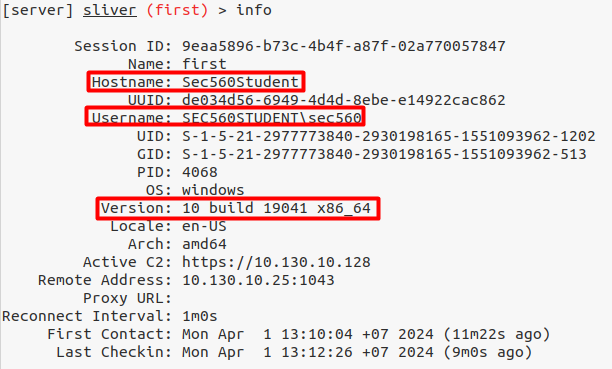


1. Interacting with the session

Tìm kiếm thông tin về hệ thống mới bị xâm nhập

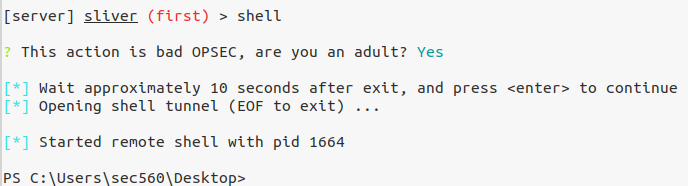


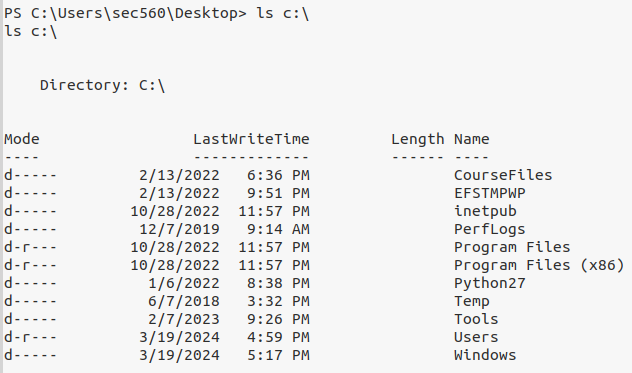


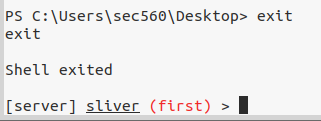


1. Shell

Tương tự như Metasploit, chúng ta có thể thả một shell lệnh bằng câu lệnh shell:

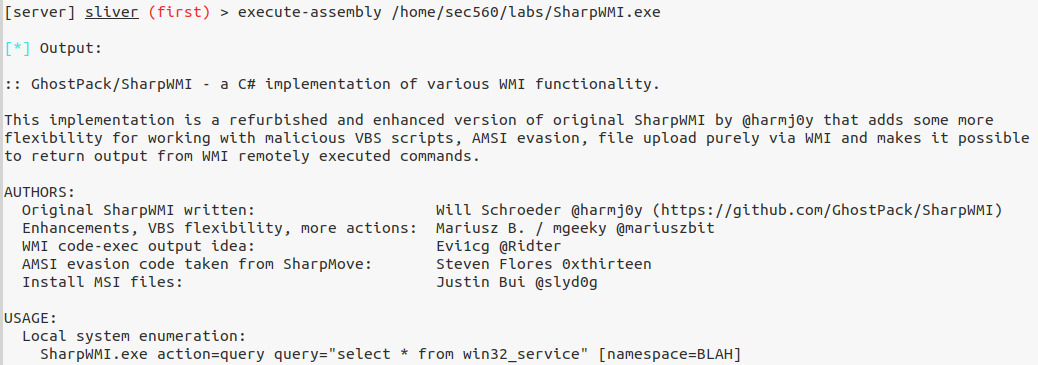


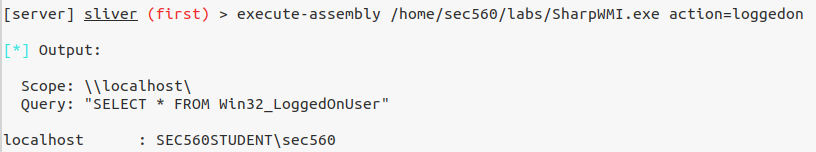




1. Execute Assembly – SharpWMI

ta cần sử dụng lệnh execute-assembly và cung cấp cho nó đường dẫn đến SharpWMI.exe





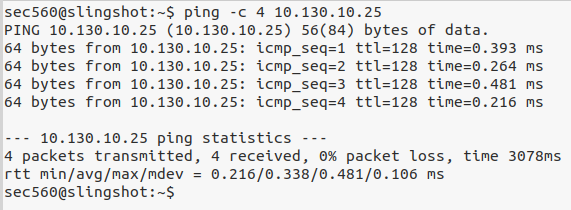
# Lab 2.4: Empire

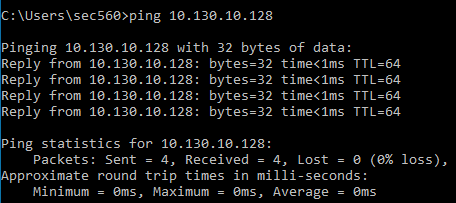
Dùng empire để tạo listener trên linux và agent trên máy windows.

Sau đó dùng empire để tìm kiếm lỗ hổng leo thang đặc quyền

Bypass để leo lên đặc quyền cao hơn

Dùng module powerdump để dump hash từ máy mục tiêu





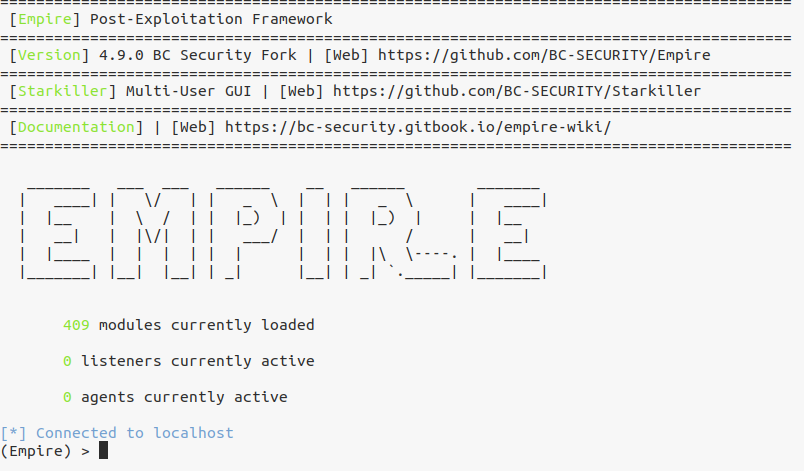
1. Starting Empire

Khởi động Empire server



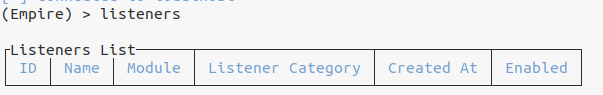
sudo ./ps-empire client

Sau đó mở một cửa sổ terminal mới để kết nối với server bằng lệnh sudo ./ps-empire client



1. Configure a listener

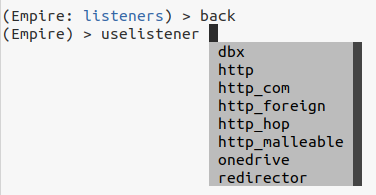
Để cấu hình một listener và triển khai tác nhân ta sẽ bắt đầu bằng viết lấy một danh sách các listeners:

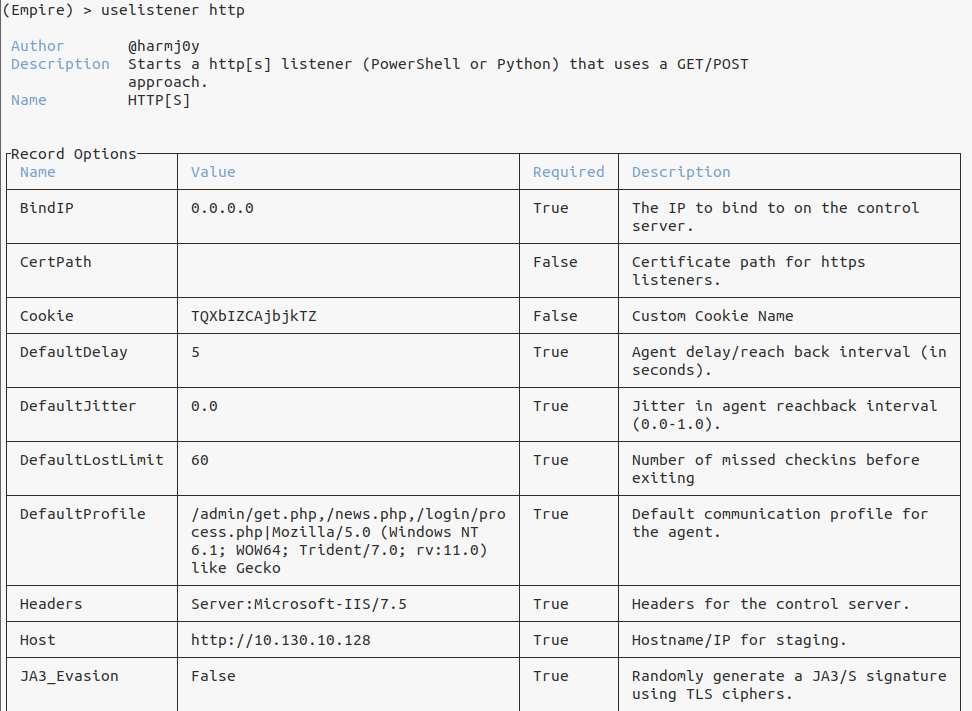


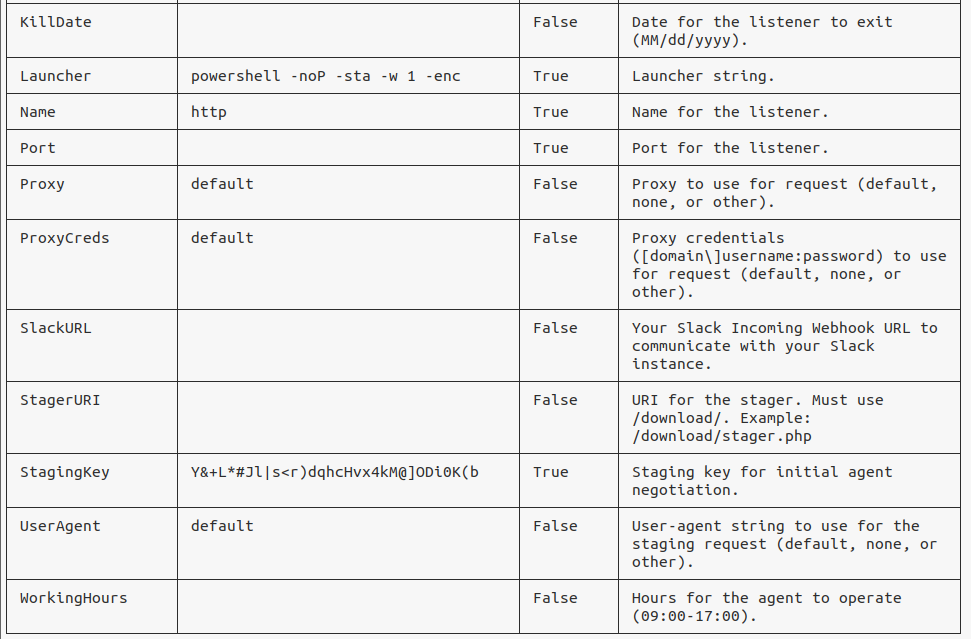
Từ bảng trên ta thấy chúng ta chưa cấu hình được listener nào. Nhưng chúng ta được phép cấu hình và khởi động một listener có thể chờ được gọi ngược lại từ agent Empire dùng lệnh help để biết một vài options có ích cho chúng ta. Sau đó quay lại bằng lệnh back và cấu hình listener.

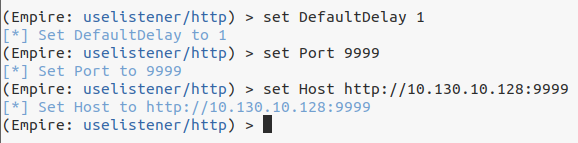
Để bắt đầu một listener, ta dùng câu lệnh uselistener

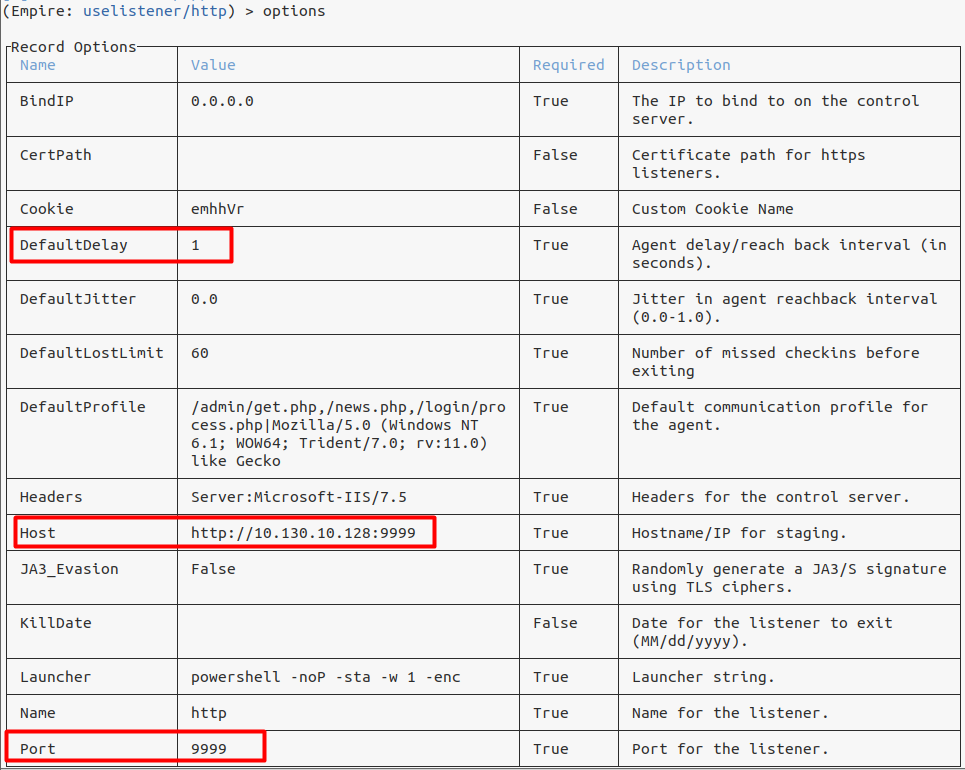
Với lab này ta sẽ dùng kiểu listener http, nó hỗ trợ cả HTTP và HTTPS và nếu ta dùng HTTP thì giao thức cũng sẽ được mã hóa bằng khóa mã hóa của Empire. Ta sẽ cấu hình listener HTTP.



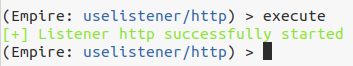




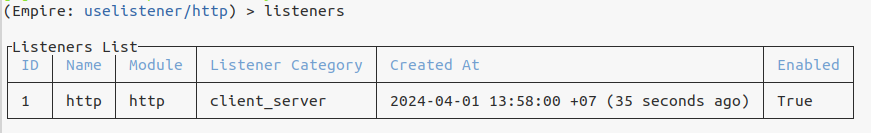




Dùng lệnh execute để khởi động listener:

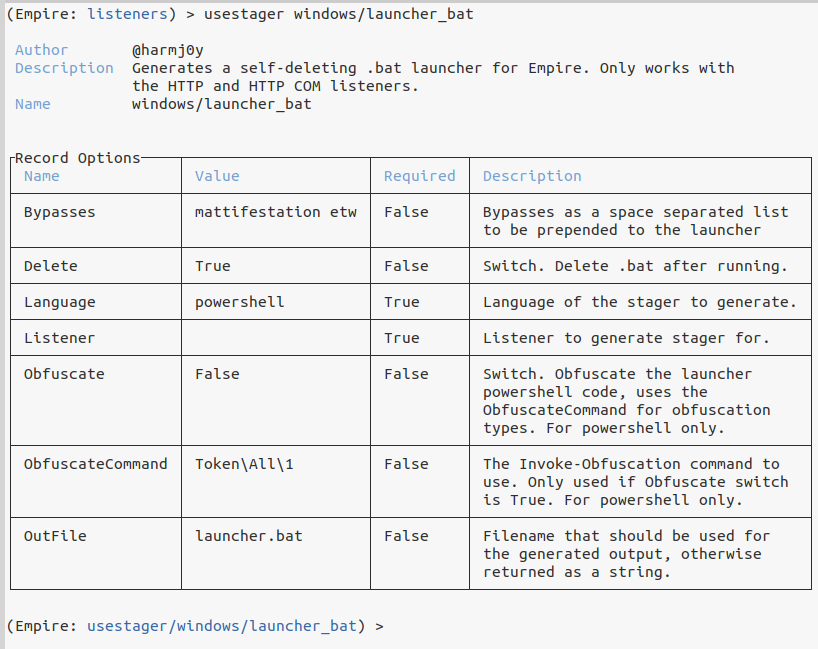


Kiểm tra listener

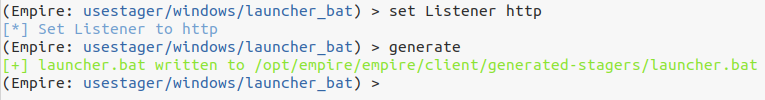


1. Deploy an agent

Với lab này ta sẽ tạo một stager chạy agent (tác nhân) thông qua Powershell từ tệp .bat của Windows rồi xóa tệp .bat đó.



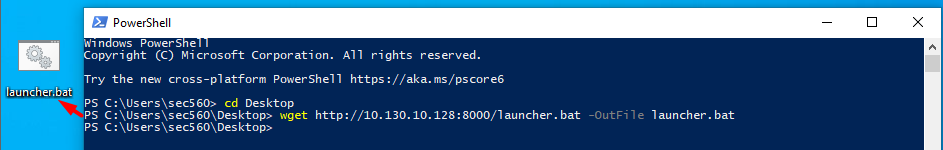
Lưu ý rằng agent có khả năng xác thực để ủy quyền thông qua biến ProxyCreds. Ở lab này ta sẽ giữ nguyên các giá trị mặc định. Cần cho stager biết sẽ callback tới listener nào & tạo ra file stager:

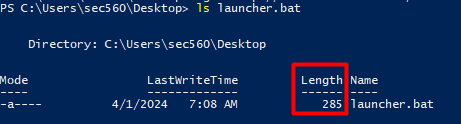


Tiếp theo, mở terminal mới trên linux, chuyển sang /opt/empire/empire/client/generated-stagers/ và phân phát tệp stager của mình thông qua http.server Python, listen trên cổng TCP mặc định là 8000. Tạo một máy chủ web python server /opt/empire/empire/client/generated-stagers/launcher.bat

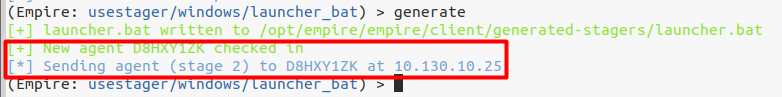


1. Deploying the stager

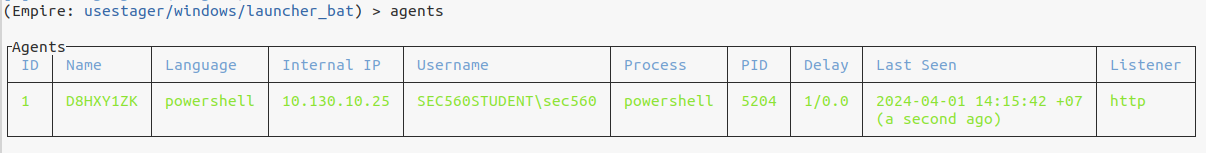




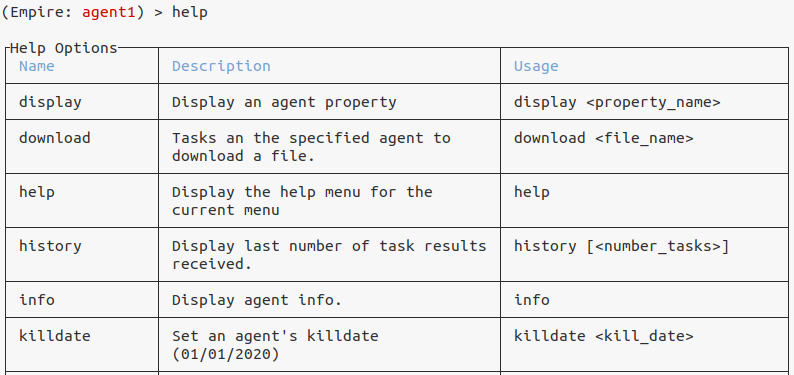


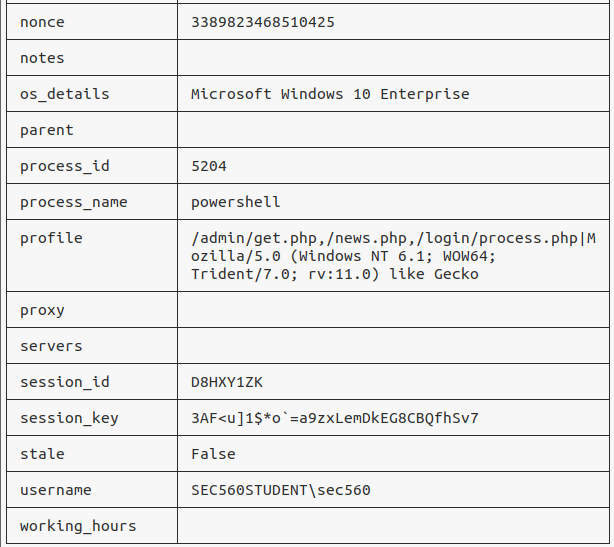
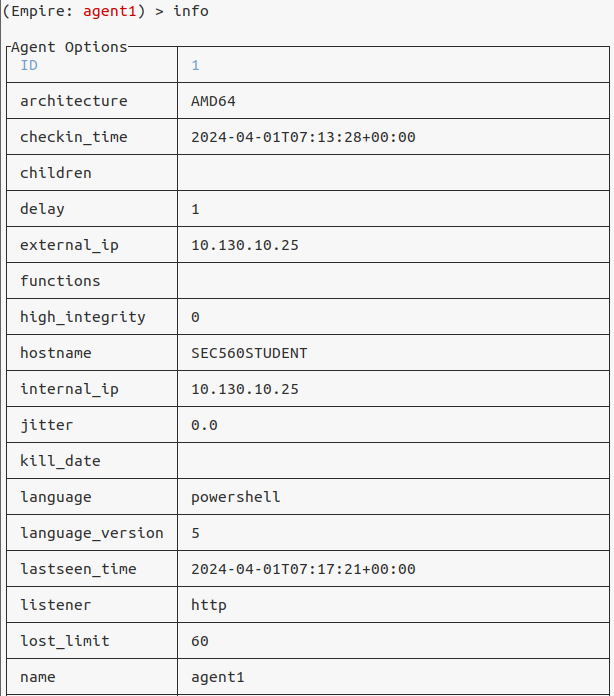


1. Active agent











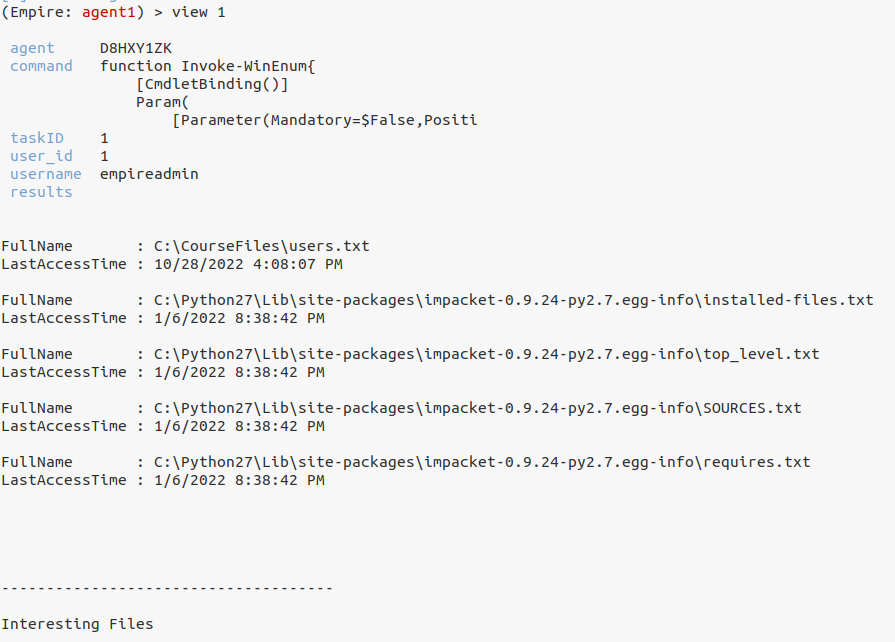
1. Module

Giò ta đã có một agent được triển khai và giao tiếp ngược lại với listeners. Cùng chú ý đến các module khả dụng để thực thi agent. Ta dùng lệnh usemodule và xem danh sách bằng cách không bấm enter. Chúng ta thấy rất nhiều module. Nhưng sẽ chạy một module là usemodule powershell/situational\_awareness/host/winenum:



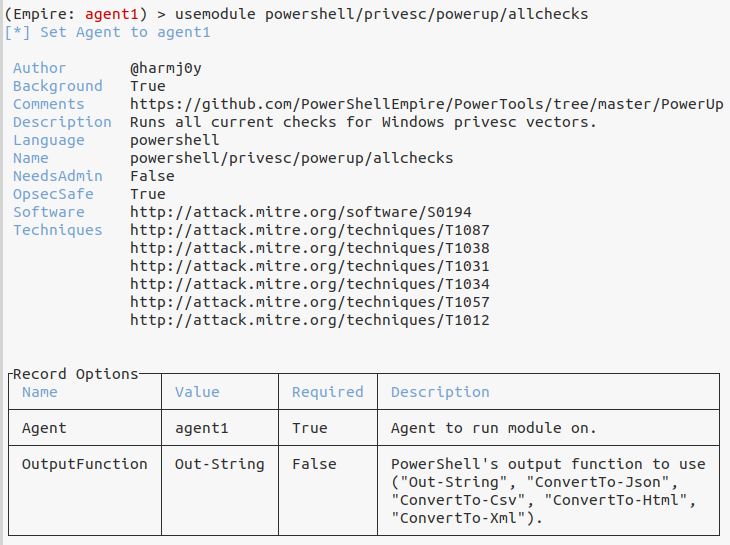
Chú ý thấy Empire tự động đặt Agent có value là agent1. Module này lấy cắp thông tin hữu ích từ máy mục tiêu, bao gồm thông tin về phần mềm và file được lưu trữ

Chạy module winenum bằng lệnh execute: Dùng lệnh view để job chạy trong khoảng 30s, sau đó kiểm tra kết quả:



1. Looking for privilege escalation

PowerUp có tính năng chạy tất cả các bước kiểm tra để leo thang đặc quyền trong powershell/privesc/powerup/allchecks

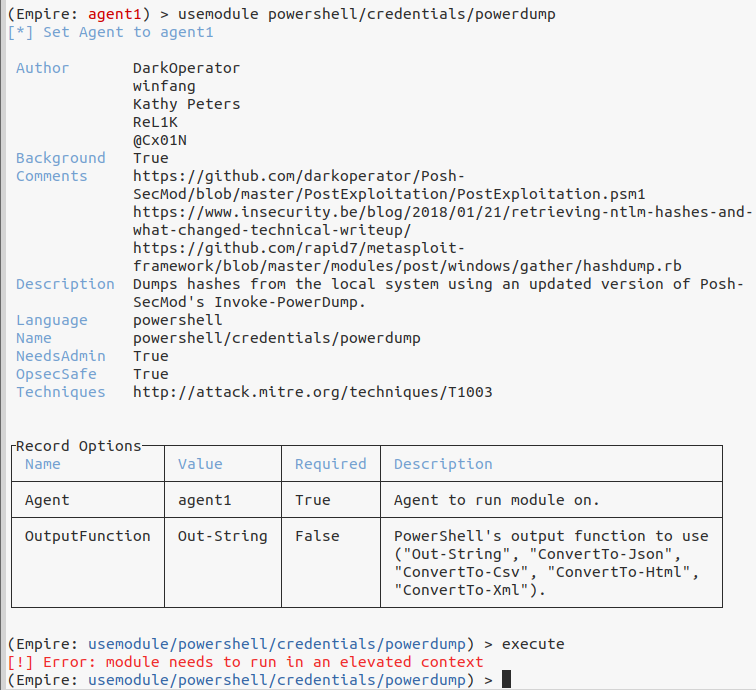


Thực thi, dùng lệnh view 2 để xem





Trước khi nâng quyền nên xem thử ta có bị giới hạn nếu không đủ quyền QTV trong agent hay không. Ta sẽ thử module powerdump:



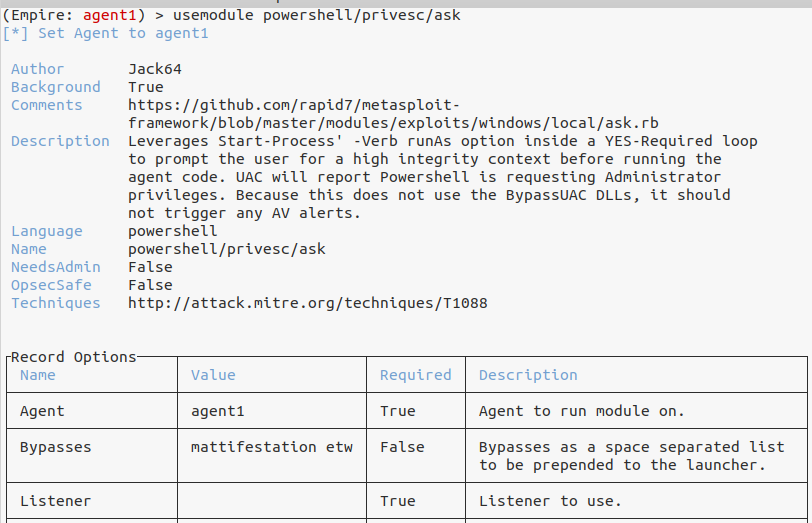
Từ đây có thể thấy rằng nếu agent không chạy với đủ quyền thì sẽ thất bại

1. UAC bypass

Ta thử vượt qua UAC để có những đặc quyền nâng cao cần thiết để kết xuất ra hàm băm. Đầu tiên ta sẽ quay về agent1



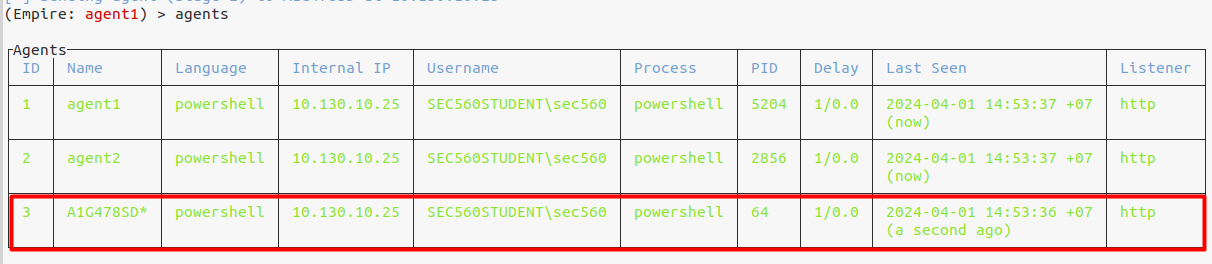
Giờ ta sẽ chạy một module tấn công tên là prives/ask. Module này chỉ đơn giản bật lên lời nhắc UAC, yêu cầu người dùng đăng nhập vào Windows cho phép thực thi một số chương trình. Mặc dù có thể người dùng cẩn thận sẽ kiểm tra nhưng hầu như bình thường sẽ click Yes. Mặc dù có những cách khác để khai thác việc vượt qua UAC nhưng Microsoft vá khá thường xuyên. Chỉ riêng cú click của user là vẫn hoạt động tốt ngay trên tệp Windows đã được debbug đầy đủ.

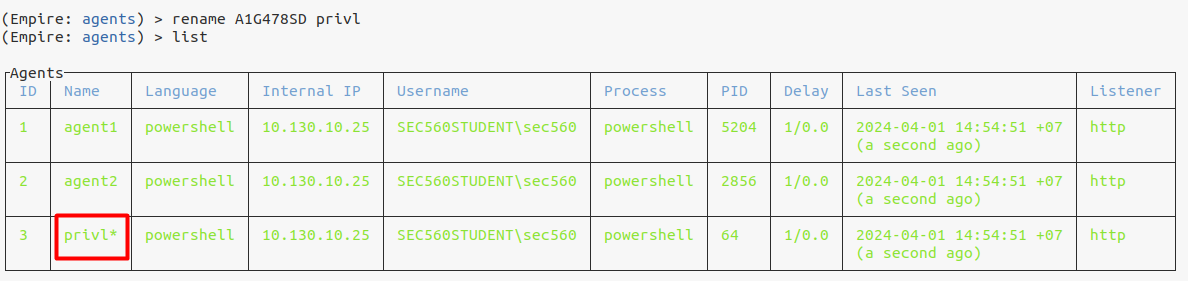


Giờ chỉ cần để Empire biết nếu module thành công thì nó sẽ kết nối lại với listener, ta sẽ chỉ định tên của listener http và thực thi module này bằng execute:



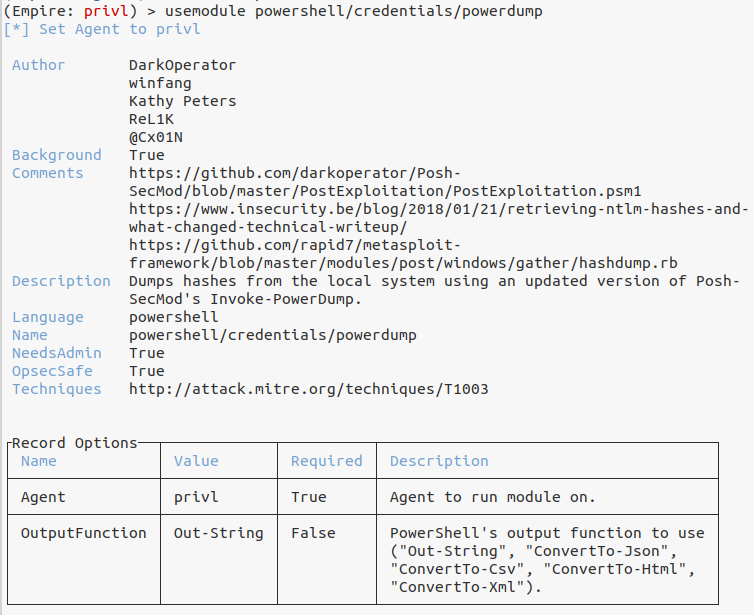








thử chạy powerdump để lấy hàm băm

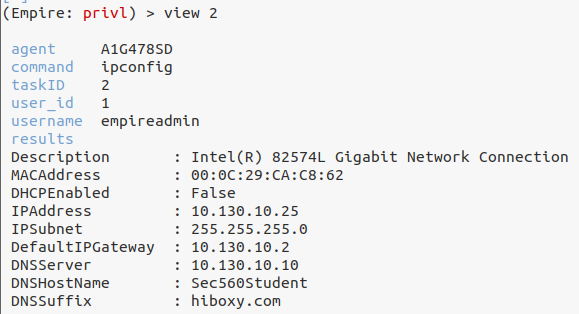




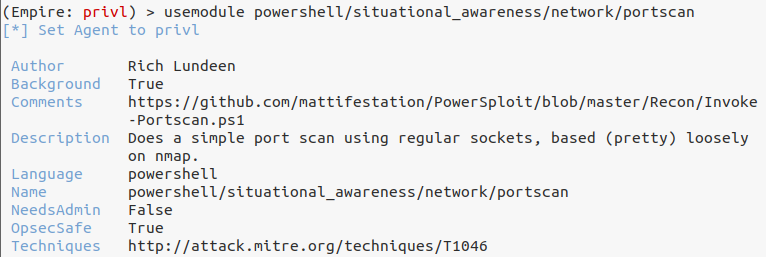


Ta chạy lệnh shell, view để xem chi tiết



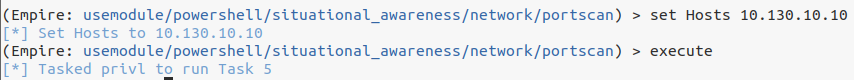


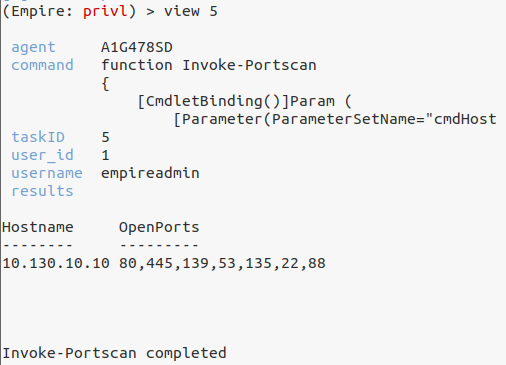
1. Port scan



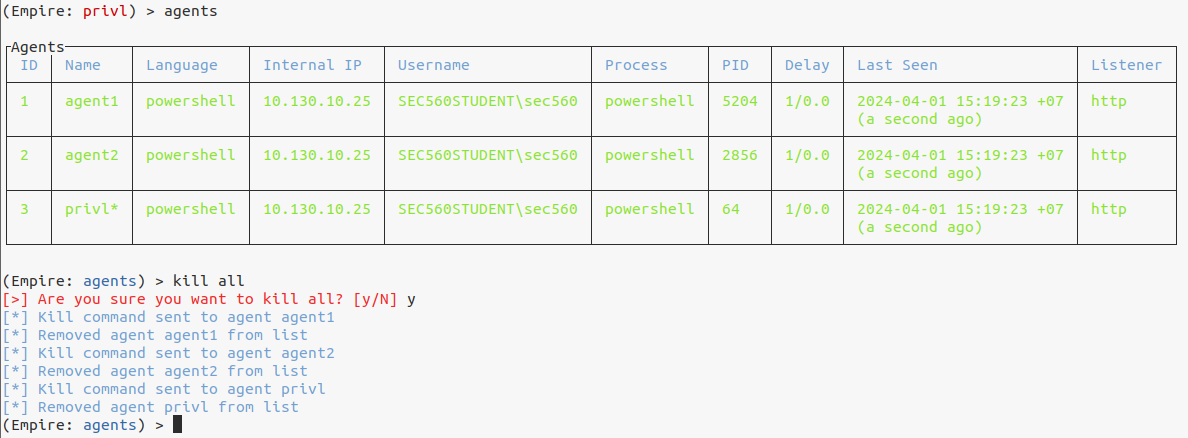


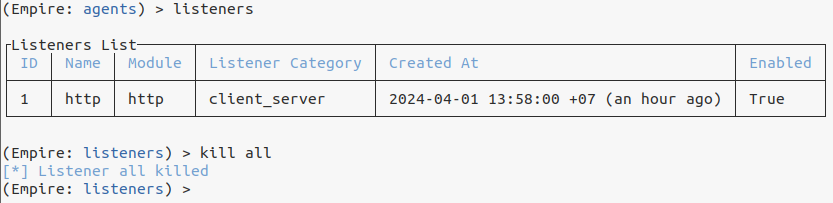


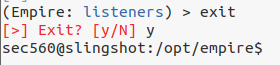




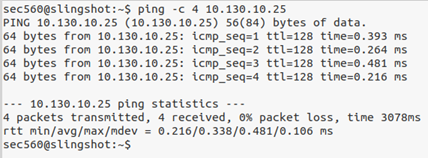
1. Wrap up



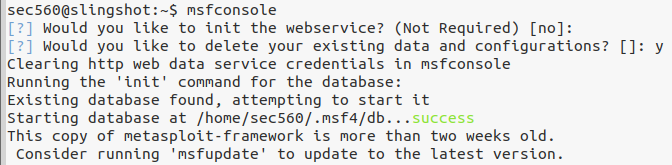




# Lab 2.5: Payloads



1. Setup Metasploit to receive a connection

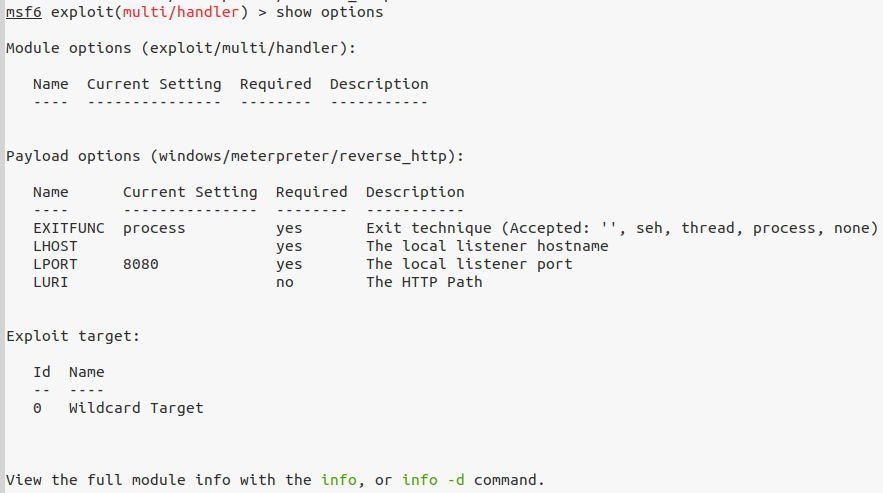


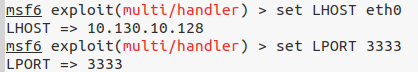


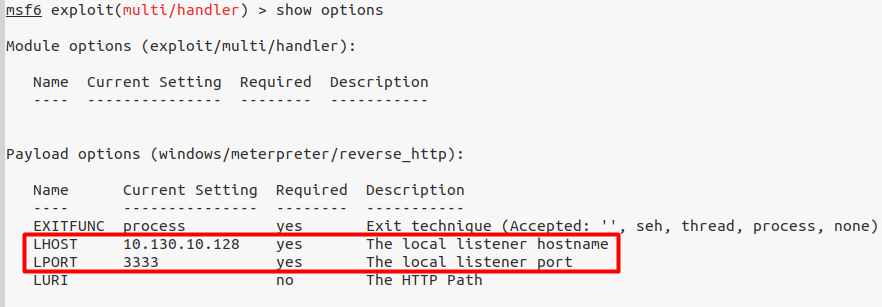
Dùng multi/hander khai thác để có kết nối. Multi Hander không phải một trình khai thác mà nó chỉ đơn giản là cho metasploit biết rằng ta đang chuẩn bị khởi chạy payload bên ngoài Metasploit và Metasploit nên sẵn sàng nhận kết nối.





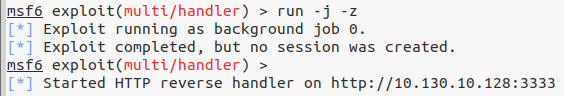






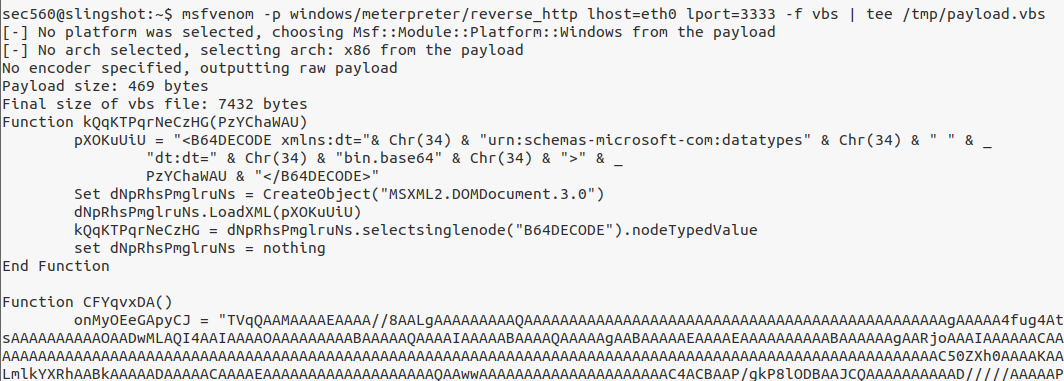


Khởi động listener bằng cách chạy nó như một job (-j) và không tương tác với các kết nối mới (-z):



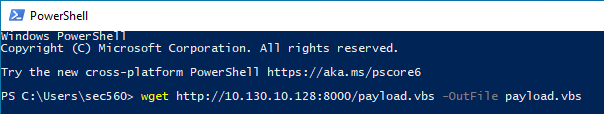
1. Metasploit Payloads with MSFVenom

Mở một cửa sổ terminal mới. Để cho Metasploit chạy, ta sẽ dùng lệnh msfvenom để tạo ra vài payloads sẽ được dùng để thực thi trên win10:

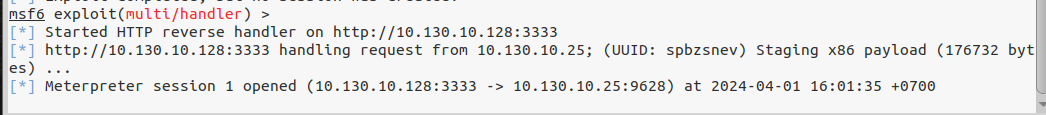


1. Copying the VBS payload to Windows and execute it

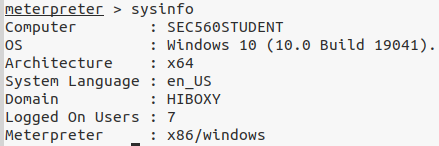


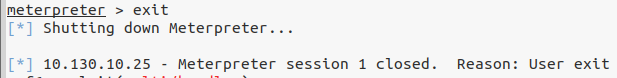




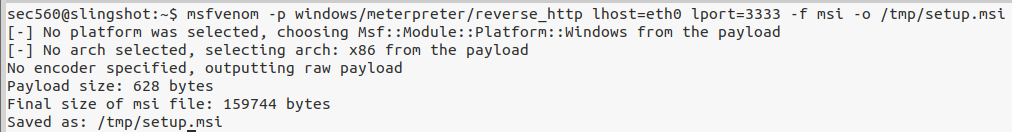


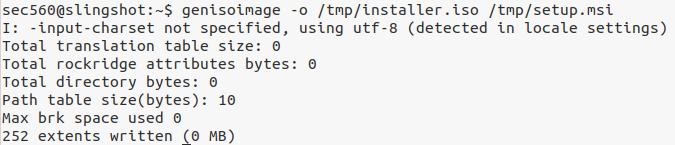




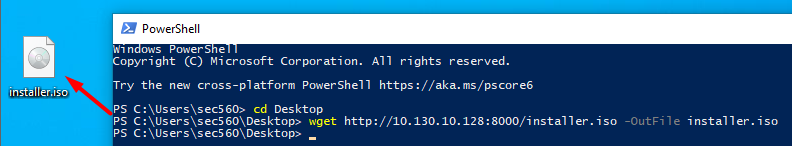


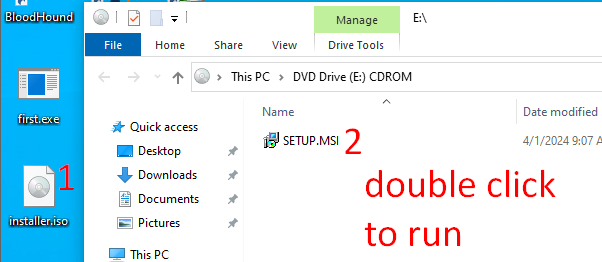
1. Creating an MSI payload in an ISO file

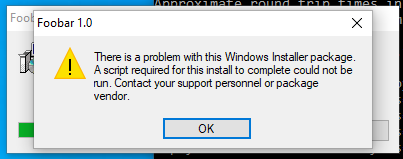


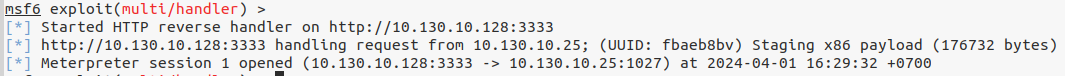


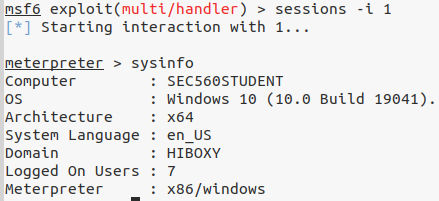
1. Download and open ISO and MSI files

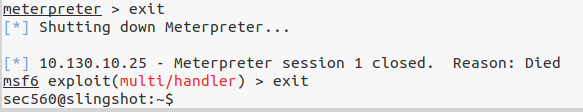




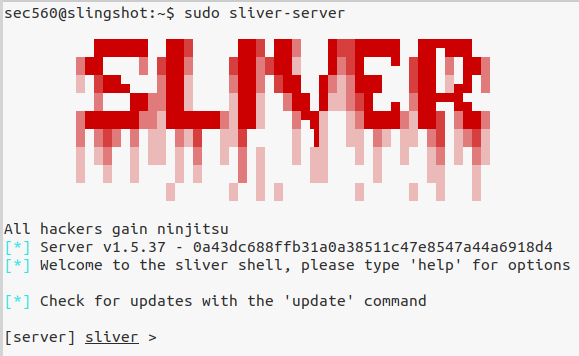




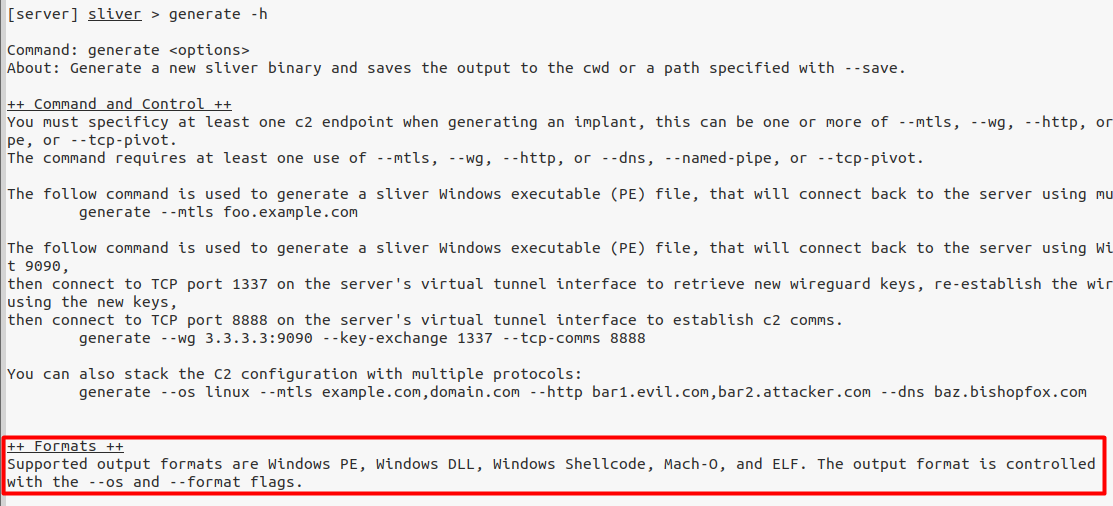


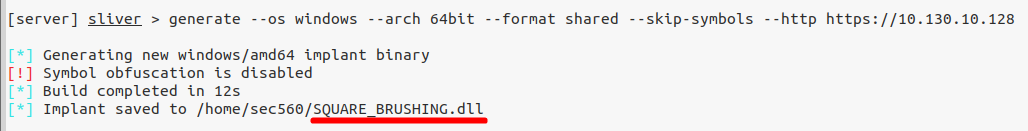


1. Sliver and Payloads



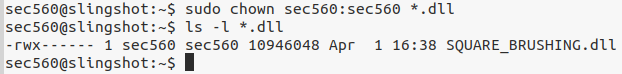


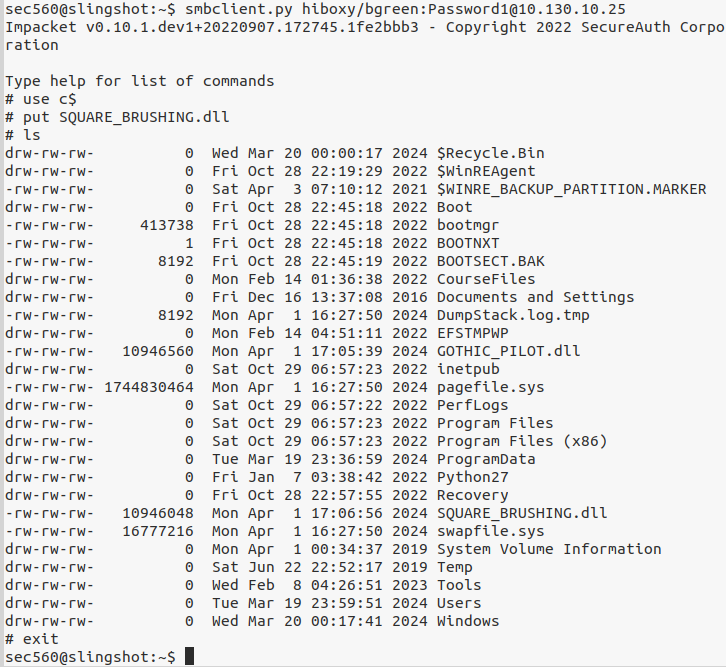


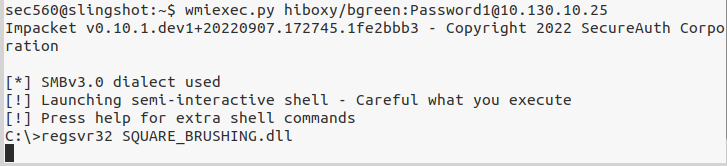


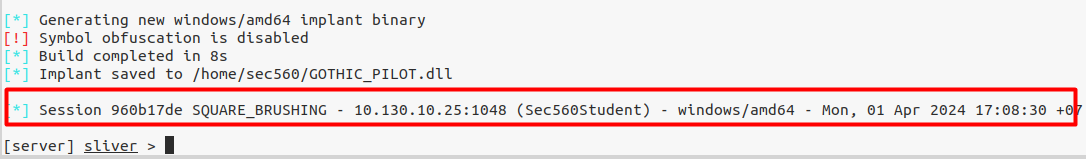
1. Copying and executing the DLL

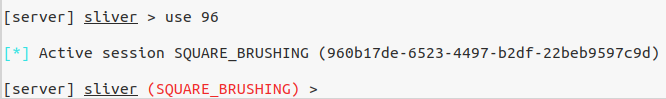


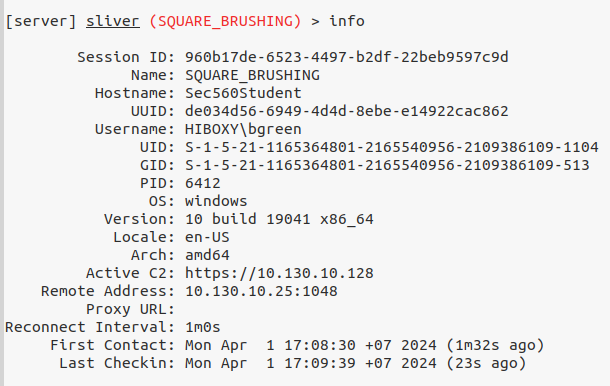




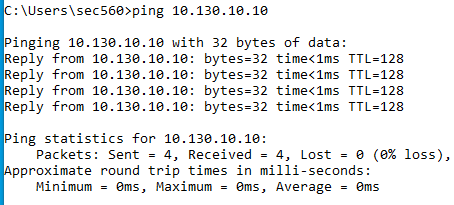






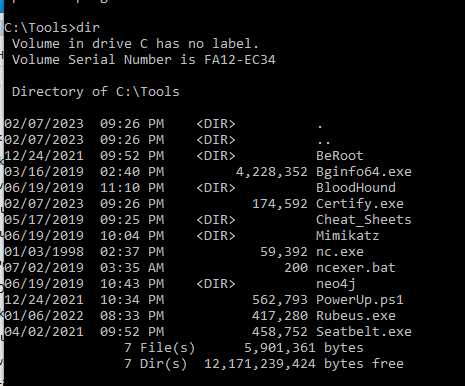


# Lab 2.6: Seatbelt



1. Launching Seatbelt

Mở CMD, chuyển qua kiểm tra thu mục \Tools





Khi ta chạy seatbell, nó sẽ hiển thị một hình ASCII lên màn hành và hiển thị kết quả. Để tắt việc này ta sử dụng option quiet -q

1. Single checks

Chạy các bước kiểm tra riêng lẻ bằng cách dùng lệnh cụ thể. Ở đây thử kiếm tra và lấy thông tin hiện tại:

A screenshot of a computer program

Description automatically generated

Thử kiểm tra xem có những gì đã được cài đặt trên hệ thống của chúng ta. Chúng ta có thể sử dụng các lỗ hổng trong phần mềm để switch giữa các hệ thống

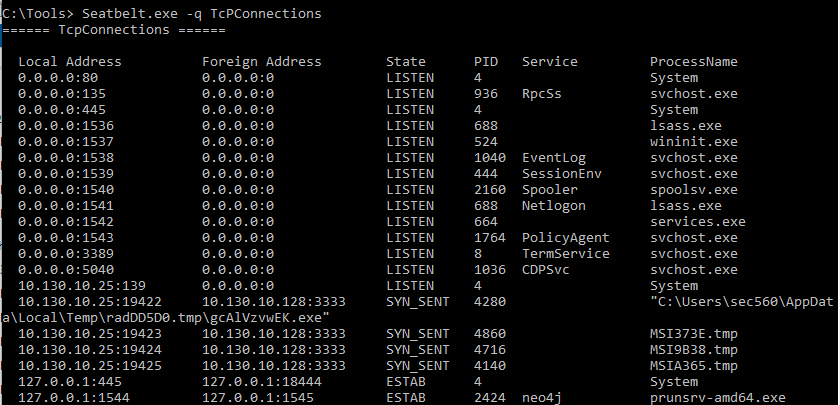
A screenshot of a computer

Description automatically generated

Ở đây ta thấy phần mềm Icecast mà ta đã khai thác từ lab 2.2 trước đó.

Một số chức năng của Seatbelt khá giống các lệnh đã được cài đặt sẵn. Chúng ta có thể tải .NET assembly (exe) này vào bộ nhớ hệ thống đích và truy vấn những thứ như netstat mà không cần dùng cmd, powershell or các tệp thực thi netstat vốn có thể bị giám sát quyền truy cập.

Thử kiểm tra TcpConnections

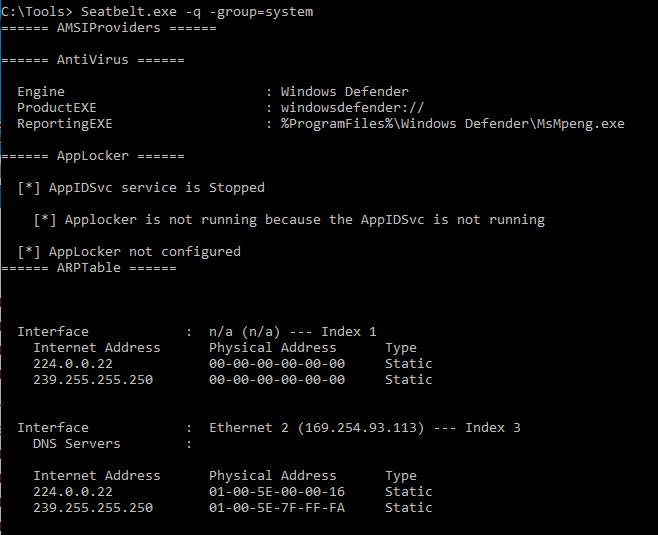


1. Groups

Thay vì chạy các câu lệnh riêng lẻ, ta có thể chạy một nhóm các lệnh mà seatbell hỗ trợ:

* All: tất cả lệnh.
* User: Người dùng hiện tại/tất cả người dùng nếu đăng nhập vào với quyền cao hơn
* System: Khai thác những data thú vị về hệ thống mục tiêu
* Slack: Các module được thiết kế để trích xuất thông tin về slack (nó đã được cài đặt, tải về, và workspaces
* Chrome: TRích xuất thông tin trên trình duyệt Chrome (nó đã được cài đặt chưa, dấu trang, lịch sử\_)
* Remote: Kiểm tra hoạt động trên các hệ thống từ xa (khá thú vị trước khi tấn công ngang (?)
* Misc: Một vài kiểm tra khác

Thử kiểm tra group system:



Ta thấy được lệnh này chạy gần 40 câu lệnh khác nhau.

Đây là cách nhanh để có được dữ liệu về hệ thống mục tiêu bằng việc phân tích ngoại tuyến.

1. Sử dụng từ xa

Chúng ta có thể dùng công cụ này để tìm hiểu về mục tiêu trước khi thai thác nó. Windows sẽ tự động chuyển token người dùng hiện tại của mình hoặc mình có thể chỉ định tên người dùng và mật khẩu bằng -username và -password.

Ở đây ta sẽ dùng bgreen/Password1 để truy vấn nhằm lấy thông tin trên hệ thống

