**Metasploit - Meterpreter**

**Giới thiệu**

Meterpreter là 1 payload của Metasploit hỗ trợ quá trình kiểm thử thâm nhập. Meterpreter sẽ chạy trên hệ thống đích và hoạt động như 1 tác nhân trong cấu trúc command and control (C2). Bạn sẽ tương tác với hệ thống và tập tin và dùng các lệnh riêng biệt của Meterpreter.

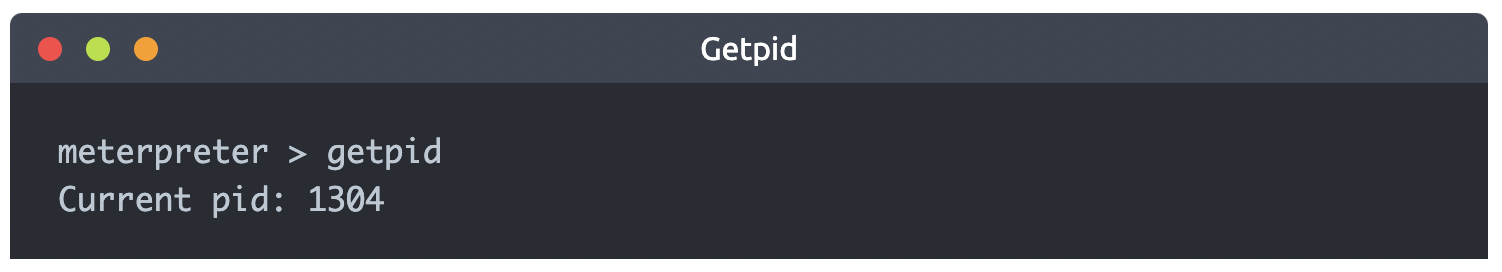
**Cách Metepreter hoạt động?**

Meterpreter chạy trên hệ thống đích nhưng không được cài đặt trên đó. Nó chạy trong bộ nhớ và không ghi đè ổ đĩa. Tính năng này mục đích tránh bị phát hiện trong quá trình quét của antivirus. Mặc định, các phần mềm chống virus sẽ quét những tập tin mới trong ổ đĩa (khi bạn tải 1 file từ internet). Meterpreter chạy trong bộ nhớ RAM để tránh có 1 file bị ghi đè vào ổ đĩa như meterpreter.exe Như vậy, meterpreter sẽ được xem là 1 tiến trình và không có tập tin trên máy mục tiêu.

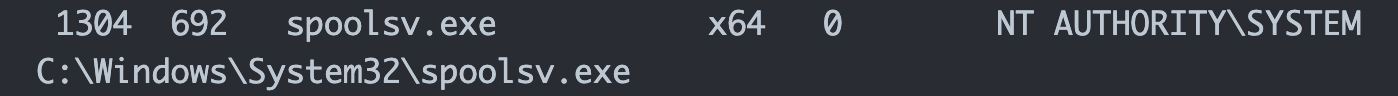
Meterpreter mục đích là tránh bị phát hiện bởi network-based IPS (hệ thống ngăn chặn thâm nhập) và IDS (hệ thống phát hiện thâm nhập) bằng cách giao tiếp với máy chủ có mã hóa trong khi metasploit đang chạy. Nếu máy nạn nhân không giải mã và điều tra lưu lượng được mã hóa ( như https) vào ra mạng nội bộ, IPS và IDS sẽ không thể phát hiện.

Trong khi meterpreter bị phát hiện bởi đa số các phần mềm chống virus, tính năng này cung cấp thêm khả năng tàng hình.

Ví dụ dưới cho thấy 1 máy ảo Windows bị khai thác bằng lỗ hổng MS17-010. Bạn sẽ thấy Meterpreter chạy với id của tiến trình (pid) là 1304; pid này sẽ khác với trường hợp của bạn.



Nếu ta liệt kê các quá trình trên hệ thống đích bằng lệnh ps, ta sẽ thấy pid 1304 là spoolsv.exe và không phải là meterpreter.exe



Thậm chí nếu ta đi sâu hơn và tìm kiếm DDLs (Dynamic-Link Libraries) được dùng bởi tiến trình meterpreter, chúng ta sẽ không tìm thấy bất cứ điều gì liên quan đến nó.

Các kĩ thuật và công cụ có thể được dùng để phát hiện meterpreter nằm ngoài phạm vi của phòng này. Bài này cho bạn thấy cách meterpreter tàng hình, đa số phần mềm antivirus sẽ phát hiện ra nó.

Điều đáng lưu ý là meterpreter sẽ thiết lập 1 kênh giao tiếp được mã hóa TLS với hệ thống của kẻ tấn công.

**Meterpreter Flavors**

Các payloads của Metasploit có thể được chia thành hai loại: inline (single) và staged.

Bạn phải nhớ là staged payloads sẽ gửi đến mục tiêu trong hai bước. Phần đầu là được cài đặt (stager) và yêu cầu phần còn lại của payload. Điều này cho phép payload ban đầu nhỏ hơn. Các payload inline được gửi trong 1 bước duy nhất. Tuy nhiên, meterpreter có rất nhiều phiên bản khác nhau bạn có thể chọn dựa vào hệ thống đích.

Cách dễ nhất là liệt kê bằng msfvenom.

msfvenom --list payloads | grep meterpreter

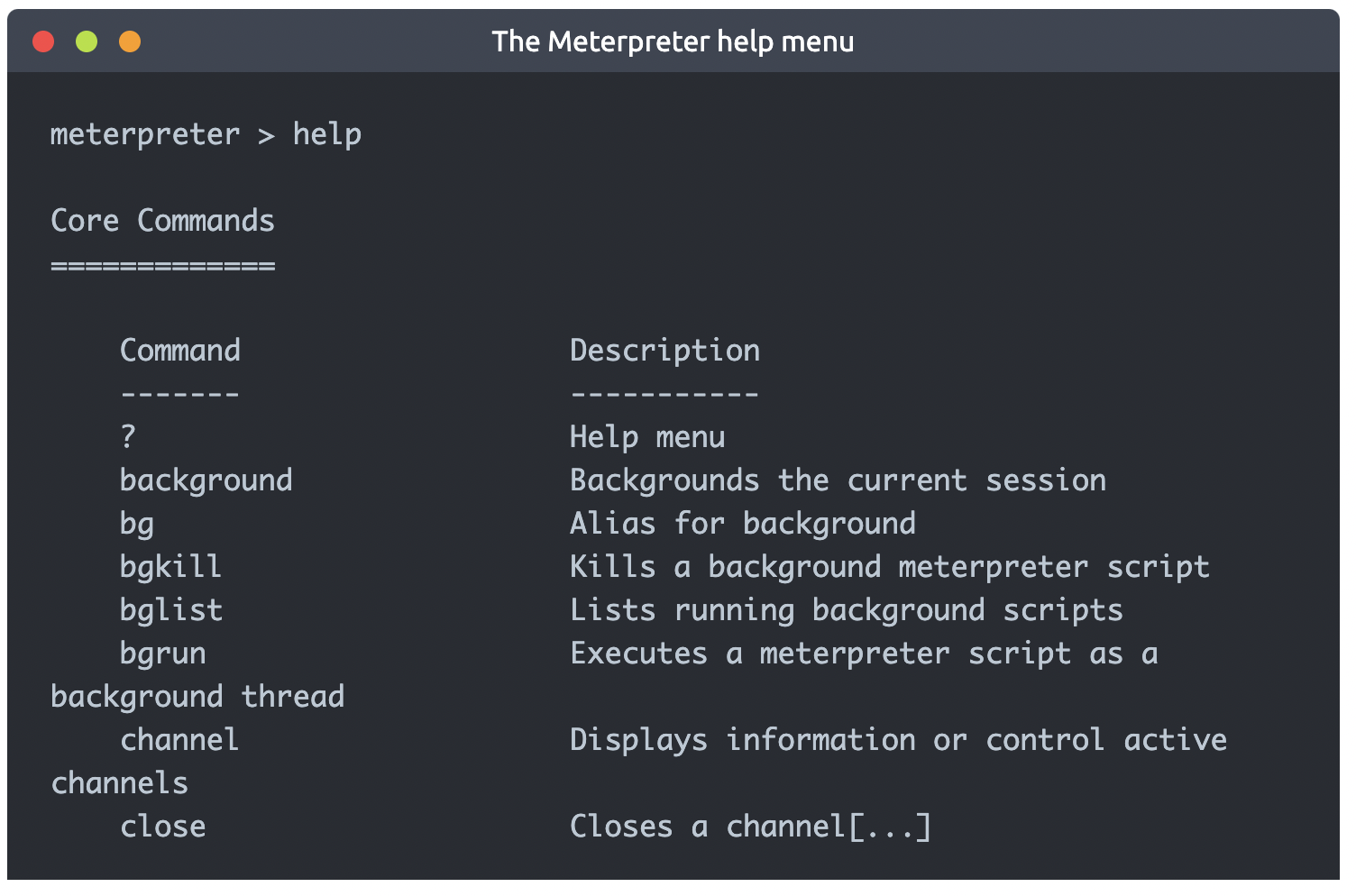
Các phiên bản của meterpreter phù hợp cho những nền tảng sau:

* Android
* Apple iOS
* Java
* Linux
* OSX
* PHP
* Python
* Windows

Nếu bạn không dùng meterpreter làm payload được tạo bởi msfvenom, bạn có thể bị giới hạn trong việc khai thác. Bạn sẽ để ý thấy một vài khai thác dùng meterpreter payload làm mặc định.

**Meterpreter Commands**

Nhập help trong phiên của meterpreter sẽ liệt kê các lệnh khả thi



Mỗi phiên bản của meterpreter sẽ có những lệnh khác nhau. Các lệnh là những công cụ được dựng sẵn trên meterpreter. Chúng sẽ chạy trên hệ thống đích mà không cần tải thêm bất cứ tập lệnh hay file thực thi nào.

Meterpreter sẽ cung cấp cho chúng ta 3 loại công cụ chính:

* Những lệnh được dựng sẵn
* Meterpreter tools
* Meterpreter scripting

Nếu bạn chạy lệnh help, bạn sẽ thấy các lệnh của meterpreter được liệt kê như sau:

* Core commands
* File system commands
* Networking commands
* System commands
* User interface commands
* Webcam commands
* Audio output commands
* Elevate commands
* Password database commands
* Timestomp commands

Các lệnh trên được lấy từ đầu ra của lệnh help trong meterpreter phiên bản windows.

**Meterpreter command**

Các lệnh chính sau sẽ rất có ích để chuyển hướng và tương tác với hệ thống đích.

**Core commands:**

* background: Backgrounds the current session
* exit: Terminate the Meterpreter session
* guid: Get the session GUID (Globally Unique Identifier)
* help: Displays the help menu
* info: Displays information about a Post module
* irb: Opens an interactive Ruby shell on the current session
* load: Loads one or more Meterpreter extensions
* migrate: Allows you to migrate Meterpreter to another process
* run: Executes a Meterpreter script or Post module
* sessions: Quickly switch to another session

**File system commands**

* cd: Will change directory
* ls: Will list files in the current directory (dir will also work)
* pwd: Prints the current working directory
* edit: will allow you to edit a file
* cat: Will show the contents of a file to the screen
* rm: Will delete the specified file
* search: Will search for files
* upload: Will upload a file or directory
* download: Will download a file or directory

**Networking commands**

* arp: Displays the host ARP (Address Resolution Protocol) cache
* ifconfig: Displays network interfaces available on the target system
* netstat: Displays the network connections
* portfwd: Forwards a local port to a remote service
* route: Allows you to view and modify the routing table

**System commands**

* clearev: Clears the event logs
* execute: Executes a command
* getpid: Shows the current process identifier
* getuid: Shows the user that Meterpreter is running as
* kill: Terminates a process
* pkill: Terminates processes by name
* ps: Lists running processes
* reboot: Reboots the remote computer
* shell: Drops into a system command shell
* shutdown: Shuts down the remote computer
* sysinfo: Gets information about the remote system, such as OS

**Others Commands (these will be listed under different menu categories in the help menu)**

* idletime: Returns the number of seconds the remote user has been idle
* keyscan\_dump: Dumps the keystroke buffer
* keyscan\_start: Starts capturing keystrokes
* keyscan\_stop: Stops capturing keystrokes
* screenshare: Allows you to watch the remote user's desktop in real time
* screenshot: Grabs a screenshot of the interactive desktop
* record\_mic: Records audio from the default microphone for X seconds
* webcam\_chat: Starts a video chat
* webcam\_list: Lists webcams
* webcam\_snap: Takes a snapshot from the specified webcam
* webcam\_stream: Plays a video stream from the specified webcam
* getsystem: Attempts to elevate your privilege to that of local system
* hashdump: Dumps the contents of the SAM database

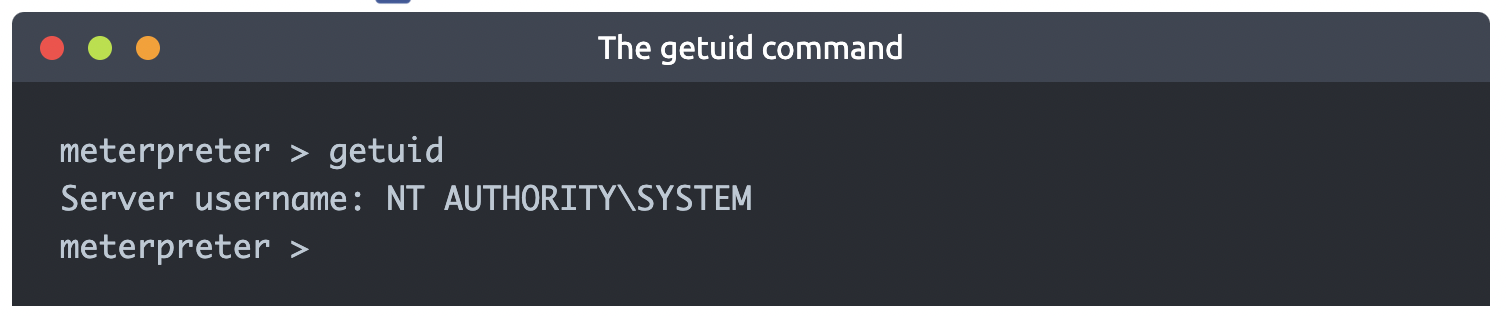
**Post-Exploitation with Meterpreter**

Meterpreter cung cấp cho bạn rất nhiều lệnh để post-exploitation

**Các lệnh Meterpreter**

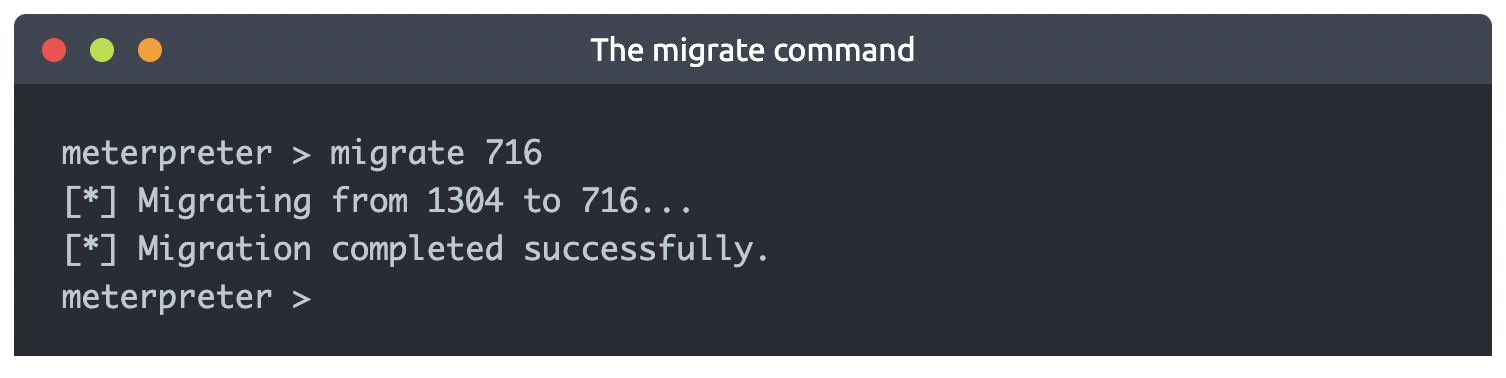
**getuid** hiển thị người dùng mà meterpreter đang chạy. Nó sẽ cho bạn biết mức độ đặc quyền của bạn trên hệ thống đích.

Ví dụ: Bạn là admin user như NTAUTHORITY\SYSTEM hay regular user



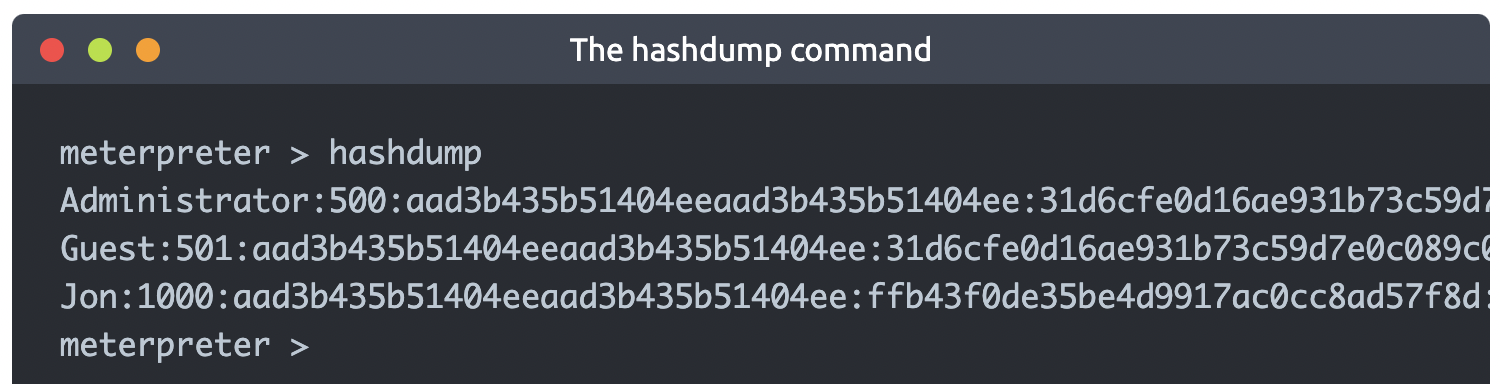
Lệnh **ps** sẽ liệt kê các tiến trình đang chạy. Cột pid sẽ cho bạn biết thông tin về pid mà bạn cần migrate meterpreter đến 1 tiến trình khác.

**Migrate**: chuyển đến 1 quá trình khác sẽ giúp meterpreter tương tác với nó. Ví dụ, nếu bạn thấy 1 word processor đang chạy trên đối tượng như word.exe, notepad.exe, bạn có thể chuyển đến nó và bắt đầu ghi lại các lần nhấn phím do người dùng gửi đến quá trình này. Một vài phiên bản meterpreter sẽ cung cấp cho bạn các lệnh như keyscan\_start, keyscan\_stop và keyscan\_dump để làm cho meterpreter hoạt động như 1 key logger. Di chuyển đến 1 tiến trình khác có thể giúp bạn có 1 phiên meterpreter ổn định hơn.



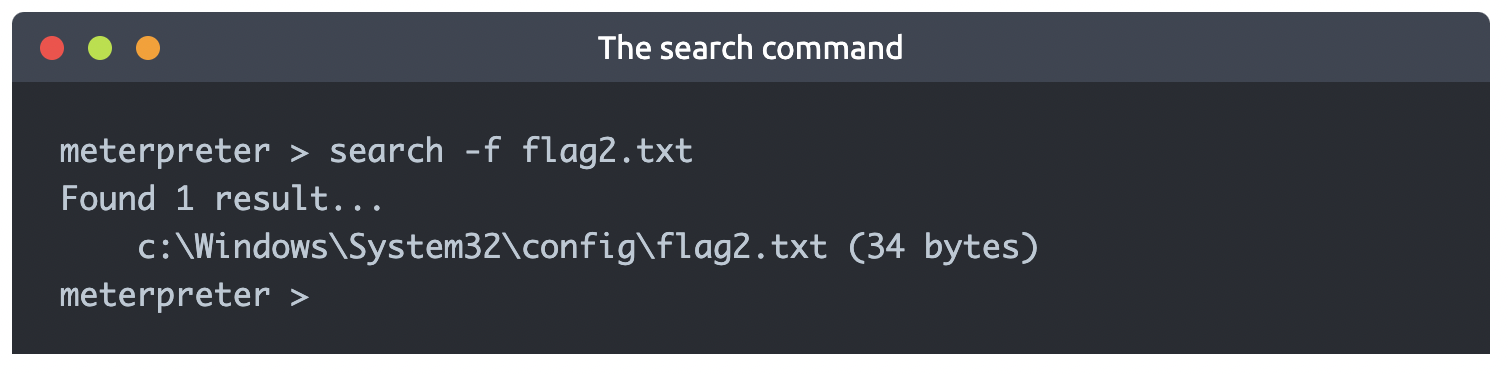
Hãy cẩn thận, bạn có thể mất đặc quyền cao (system) nếu chuyển đến tiến trình có đặc quyền thấp hơn (web server).

**Hashdump** sẽ liệt kê cơ sở dữ liệu SAM. SAM (Security Account Manager) lưu trữ mật khẩu của người dùng trên hệ thống ở định dạng NTLM (New Technology LAN Manager)



Nó không thể crack được hash nhưng bạn có thể khám phá được mật khẩu ở dạng rõ ràng bằng NTLM databases hay rainbow table attack. Những hash này có thể được dùng trong Pass-the-Hash attack để xác thực đến hệ thống khác trong cùng 1 mạng.

**Search** rất hữu ích để tìm kiếm file. Trong CTF, nó có thể được dùng để tìm flag, trong pentest, bạn có thể tìm những tập tin cấu hình hoặc do người dùng tạo ra chứa thông tin đăng nhập.



**Shell** sẽ khởi tạo 1 shell thông thường trên hệ thống đích. Nhấn Ctrl+Z sẽ giúp bạn quay lại với meterpreter shell.

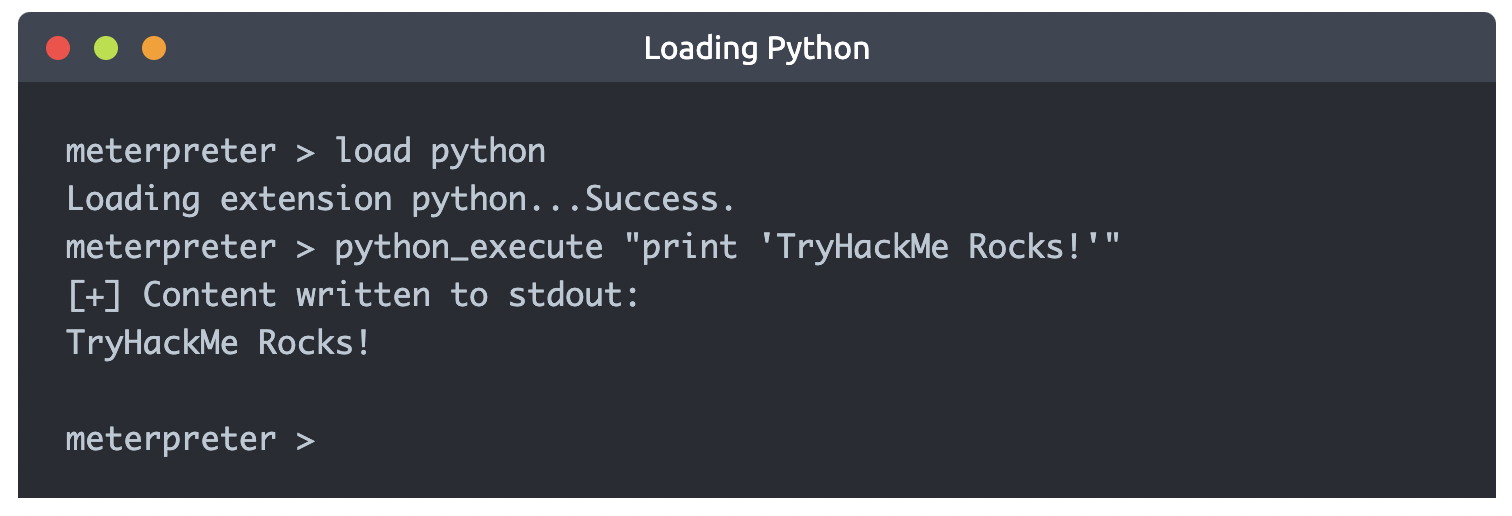


**Post-Exploitation Challenge**

Meterpreter cung cấp 1 vài công cụ quan trọng để post-exploitation.

Các lệnh đã được đề cập trước đây như getsystem và hashdump sẽ cung cấp đòn bẩy và thông tin quan trọng cho việc leo thang đặc quyền và lateral movement.

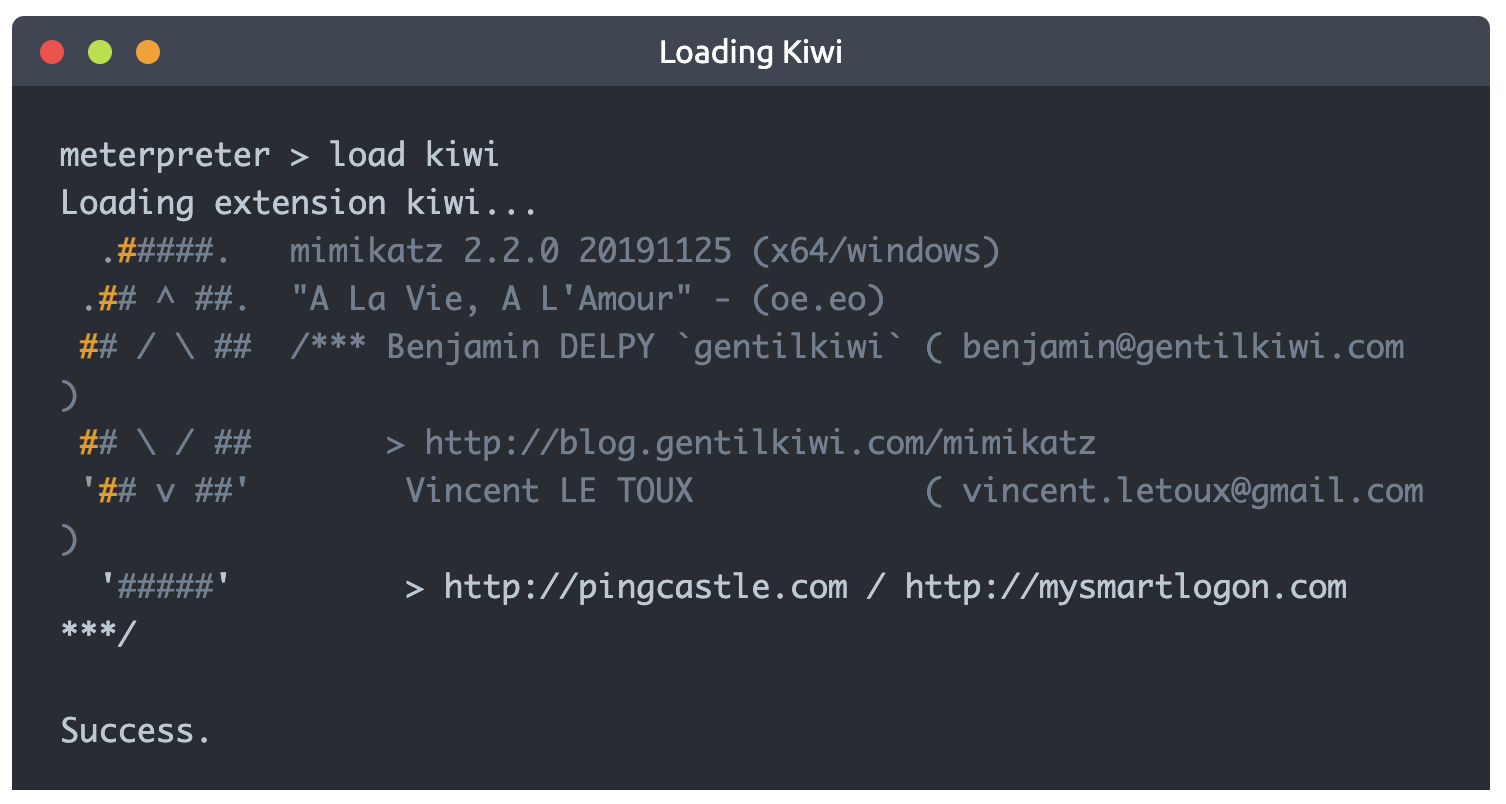
Meterpreter cũng là 1 nền tảng tốt bạn có thể dùng để chạy các module post-exploitation trên thư viện Metasploit. Cuối cùng, bạn có thể dùng lệnh load để tận dụng thêm các công cụ như Kiwi hay thậm chí là Python.

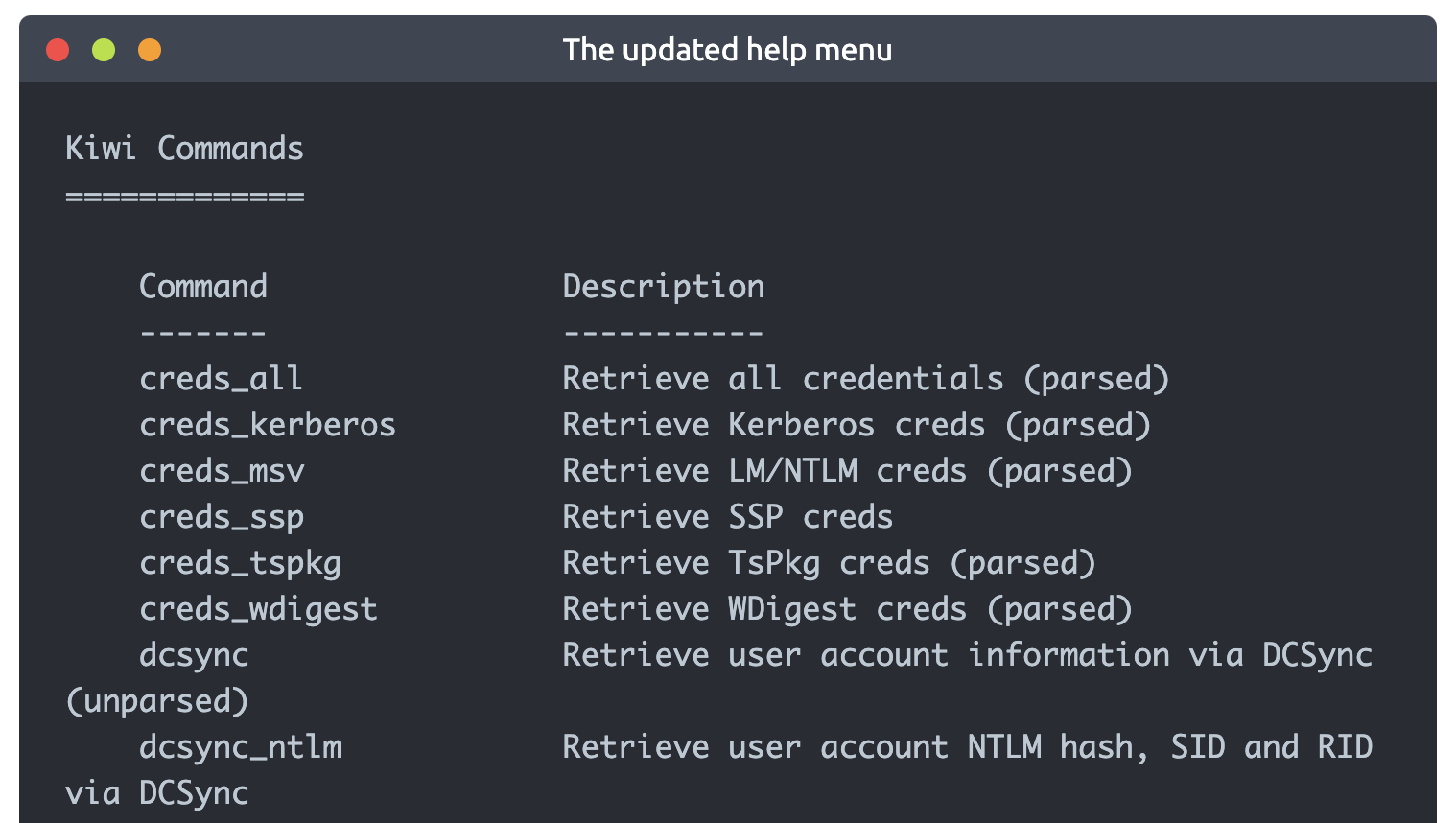


Các bước post-exploitation:

* Thu thập thêm thông tin về hệ thống đích
* Tìm kiếm các tập tin thú vị, thông tin đăng nhập, giao diện mạng
* Leo thang đặc quyền
* Lateral movement (đánh lan sang các mạng khác)

Khi một công cụ mới được thêm vào bằng lệnh load, bạn sẽ thấy thêm các options mới trên menu help.



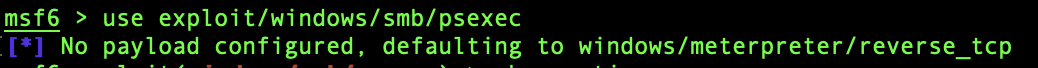


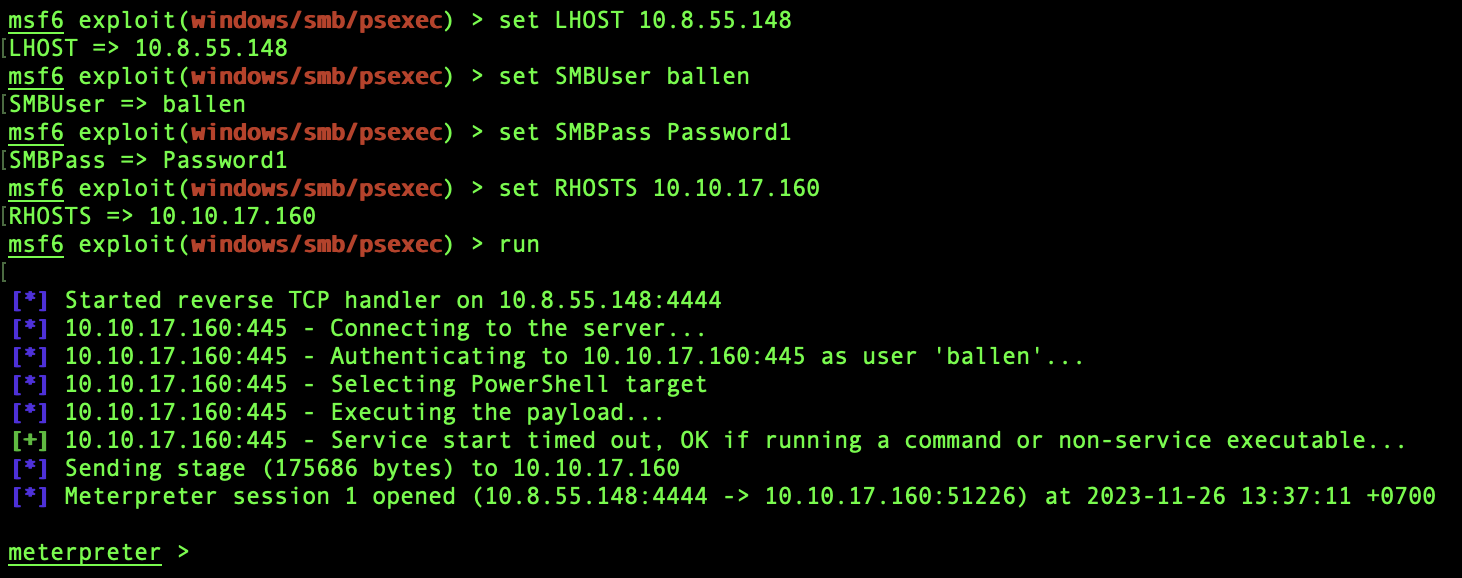
Cùng làm thử 1 challenge để xem meterpreter post exploitation như thế nào?

Giả sử bạn có thông tin đăng nhập dịch vụ SMB (dùng exploit/windows/smb/psexec):

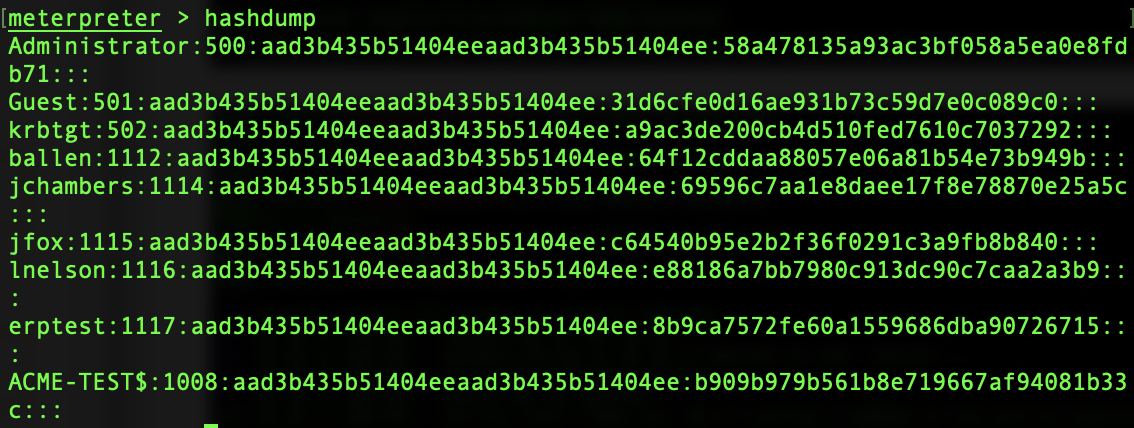
username: ballen

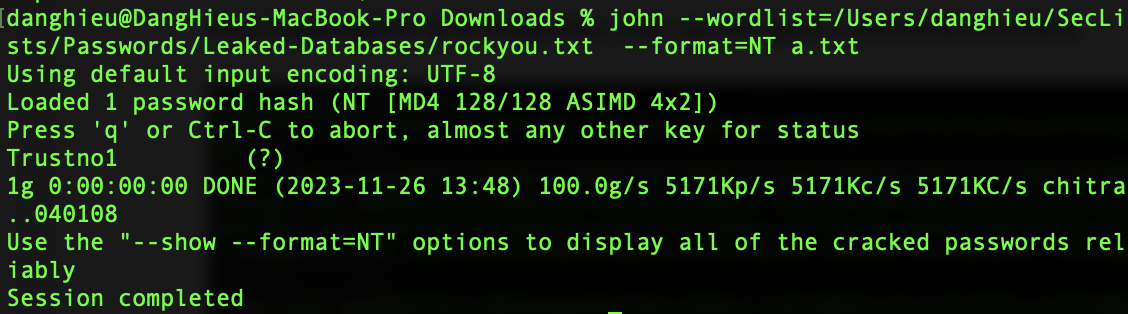
password: Password1

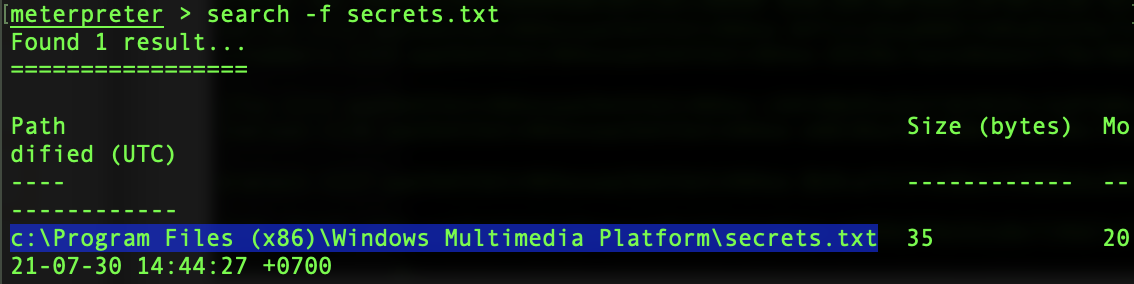


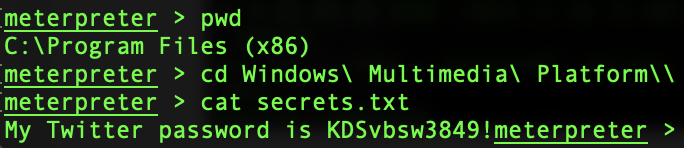


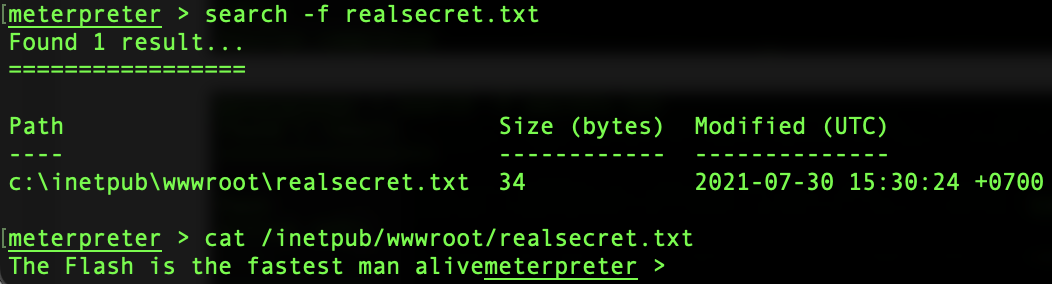
Post Exploitation là kĩ thuật khai thác sau khi gain a foothold (có shell)



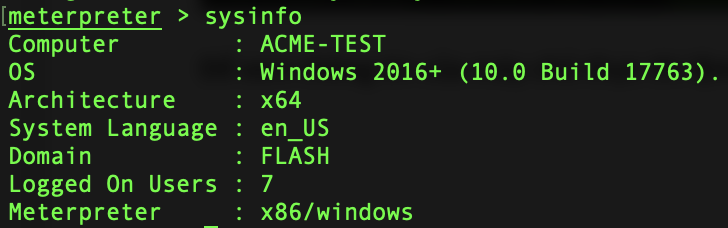




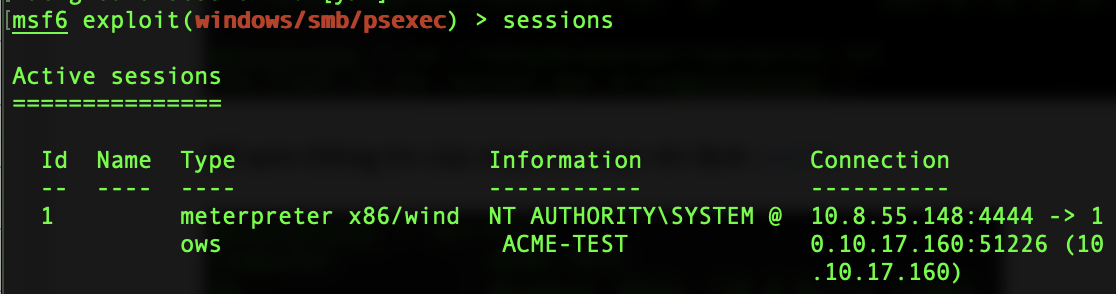




Để xem thông tin của máy chủ thực thi lệnh sysinfo



Background phiên meterpreter:



Để xem được shares tạo bởi người dùng:



