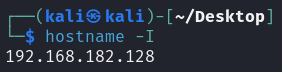
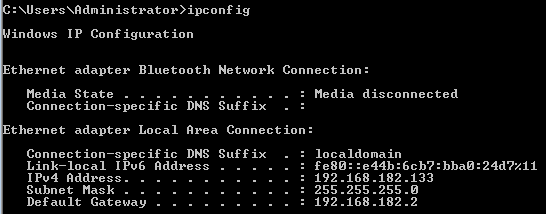
**- Khi bật 2 máy ảo lên thì show IP cả 2 máy:**





=> 2 máy đã cùng mạng Lan với nhau (do cùng xài 1 mạng từ laptop chính)

**- Cách đặt IP của máy Win phòng khi khác IP: (cẩn thận coi chừng ko có connect mạng)**

Click phải biểu tượng Wifi -> Open Network and Sharing Center -> Click phải Local Area Connection -> Properties -> Internet Protocol Version 4 (TCP/Ipv4) -> Properties

----------------------------------------------------------------------------

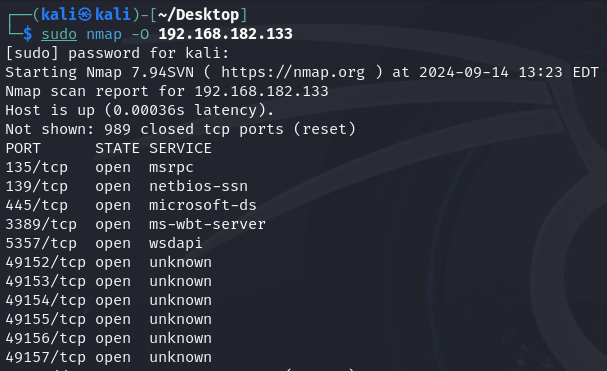
1. **Ms12\_020: Khai thác lỗ hổng về port 3389/tcp về lỗi cho phép từ xa truy cập Remote Desktop: Ms12\_020\_maxchannelids**

**1. Bật chế độ Remote Destop trên Win7 (để mở port 3389)**

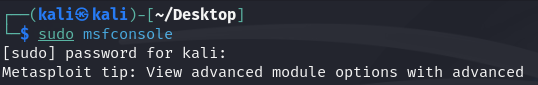
- Vì mặc định remote destop sẽ bị tắt => phải bật thì mới có port 3389 open

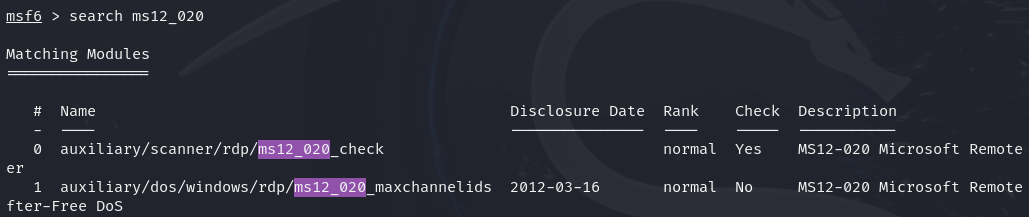
Click phải Computer -> Propeties -> Remote Settings -> Allow connections from computers running any version of Remote Desktop (less secure)

**2. Scan port = Kali**

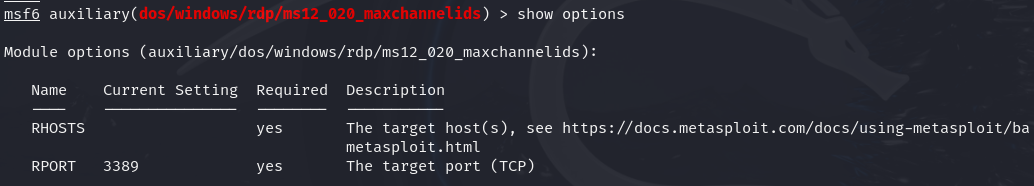


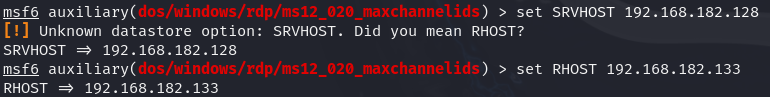
**3. Khởi động Metasploit [Kali]**

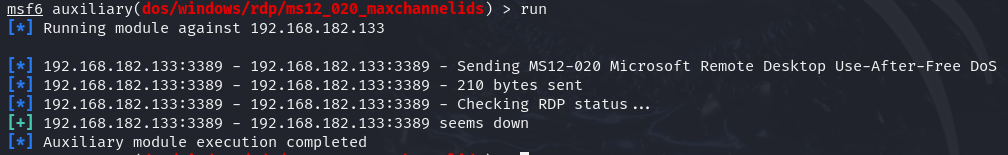




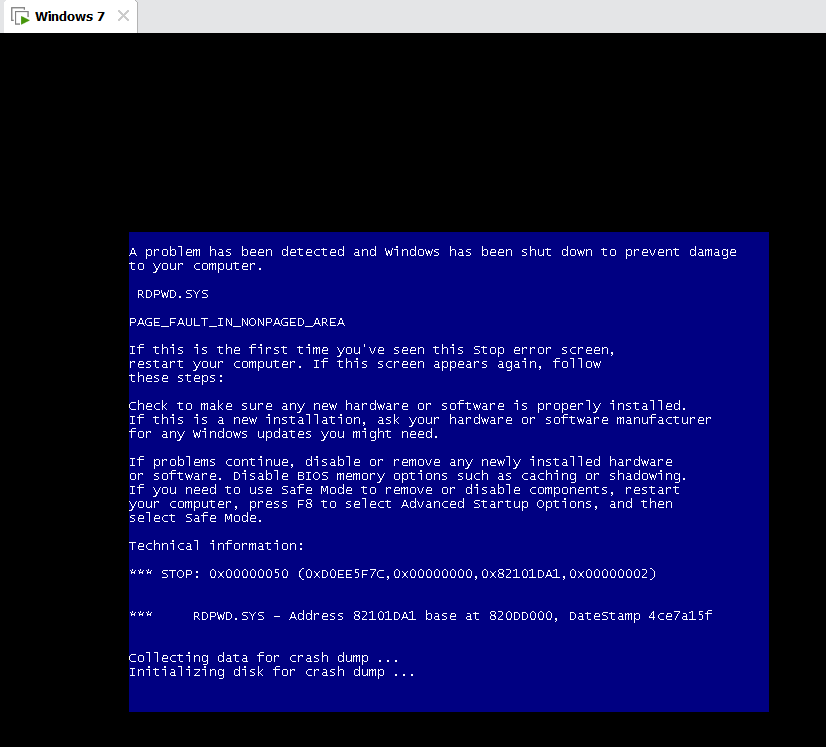








**4. Kết quả**



---------------------------------------------------------------------------------------------------------

1. **MS08-067: port 445 –SMB. (chỉ dành cho WinXP2 or cũ hơn, Win7 ko attack được)**

**• Chiếm quyền truy xuất vào trong máy nạn nhân**

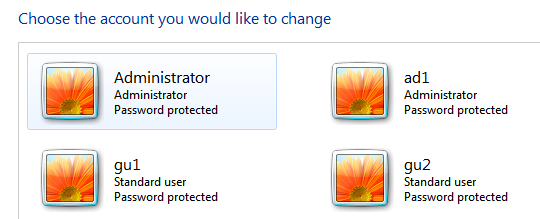
**• Lấy username/ password của các tài khoản trong máy nạn nhân**

**1. Tạo username/pass cho Win7**

- Control Pannel -> Add or Remove User account -> Create a new accout ->

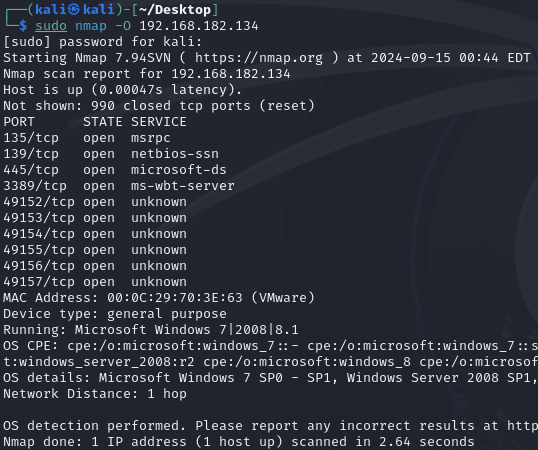
+ Standare: gu1-gu11, gu2-gu22

+ Admin: Administrator-admin, ad1-ad11



**2. Trên Kali**

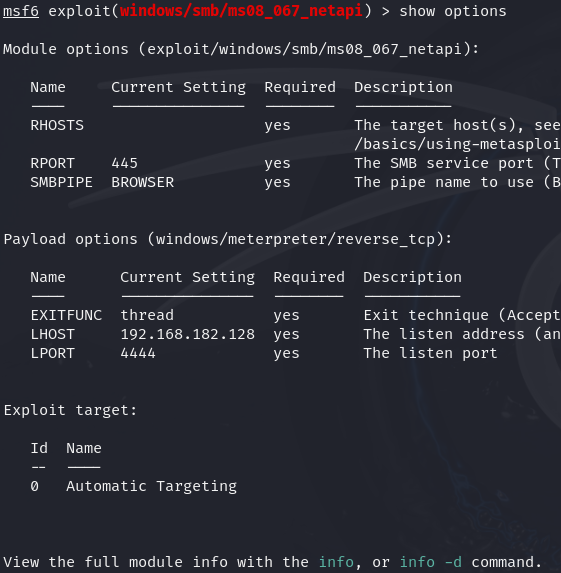
- Do đổi chỗ caphe nên IP của máy win7 bị đổi thành 192.168.182.134









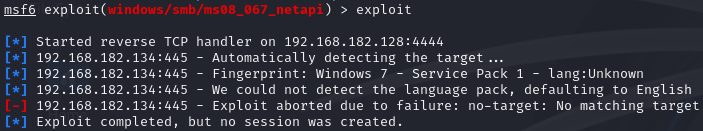


Ở đây đã được set LHOST là IP của máy Kali, nên ở dưới có thể không cần set LHOST lại



(dòng này có thể không cần vì ở trên đã được set rồi)





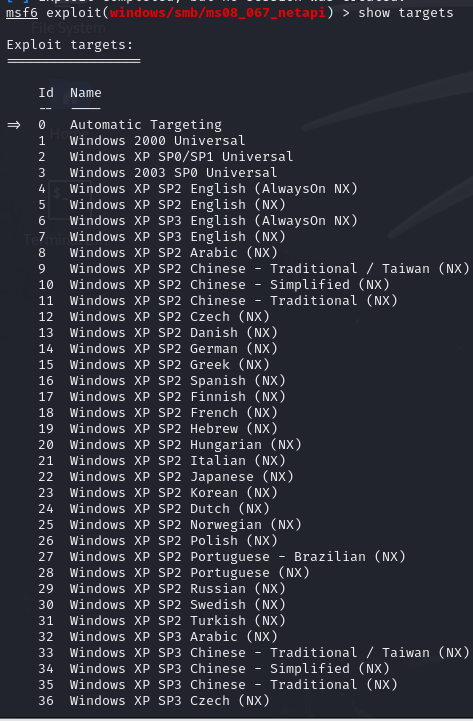
🡪 Lỗi no-target:

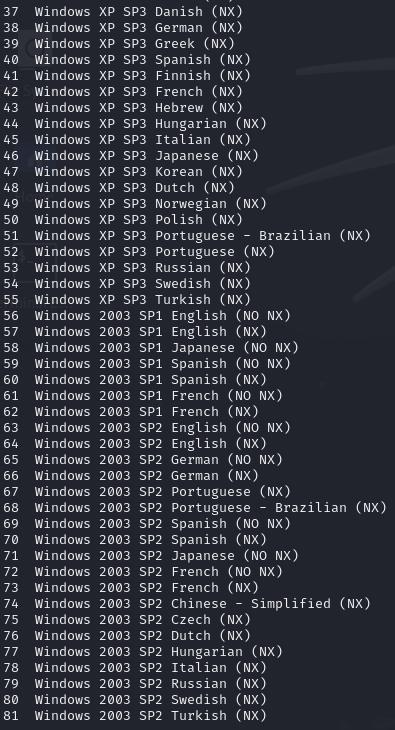
**Hệ điều hành không phù hợp với lỗ hổng MS08-067**:

* Lỗ hổng **MS08-067** nhắm vào các phiên bản Windows cũ hơn, như **Windows XP**, **Windows 2000**, và **Windows Server 2003**.
* **Windows 7** (đặc biệt là Service Pack 1) không bị ảnh hưởng bởi lỗ hổng này. Điều này có nghĩa là hệ điều hành mà bạn đang cố gắng khai thác không dễ bị tổn thương bởi lỗ hổng MS08-067.

**Mục tiêu không tương thích**:

* Thông báo **No matching target** cho biết rằng không có mục tiêu nào tương thích với hệ điều hành và bản vá (Service Pack) của máy đích được phát hiện. Điều này có nghĩa là payload mà bạn chọn không thể khai thác thành công trên mục tiêu hiện tại.





🡺 Win7 không thuộc mục tiêu có thể bị khai thác bởi lỗ hỏng ms08\_067 này

🡺 Tải WinServer 2003 để làm lại LAB

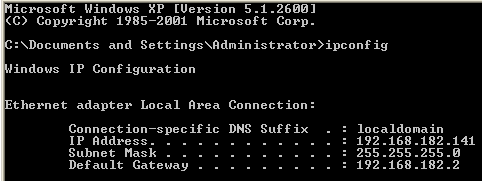
**WinXP2:**

**0. Tắt firewall (remoteDestop không cần bật cx được vì lỗi này ko có tấn công qua port 3389 mà là 445)**

Control Pannel -> Network and Internet Connections -> Windows Firewall -> OFF

*(Phải My Computer -> Properties -> Remote -> Click Allow hết: này là mở Remote Destop)*

**1. IP winxp2 = 192.168.182.141, IP Kali = 192.168.182.128**

****

****

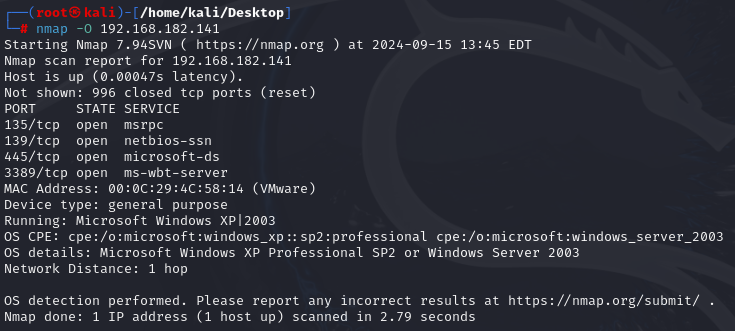
**2. Tạo User-Pass cho winXP**

Control Pannel 🡪 User Accounts 🡪 Create a new acc 🡪

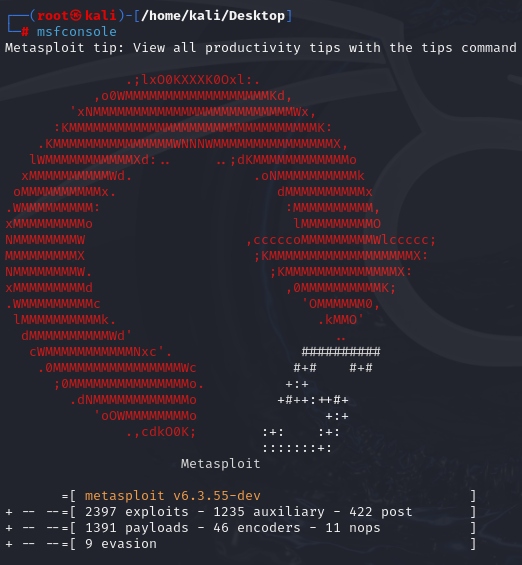
* Administrator: ad1 – ad11

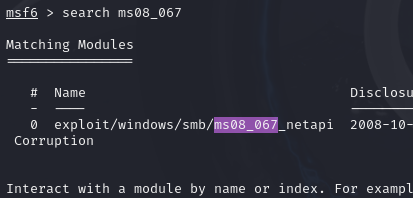
**3. Trên Kali:**

****

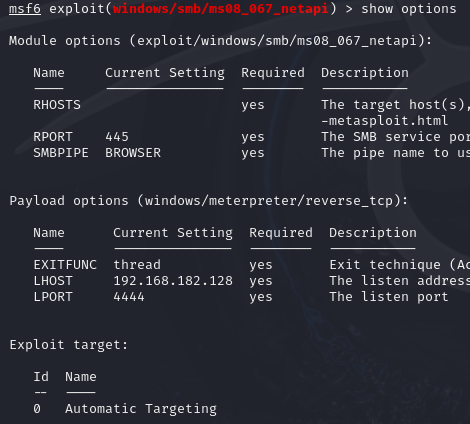
****

- Lỗi tấn công MS08-067 là một lỗ hổng bảo mật nghiêm trọng trong dịch vụ Server của Windows, cụ thể là trong giao thức **Server Message Block (SMB)**. Lỗ hổng này cho phép thực thi mã từ xa mà không cần xác thực. Cuộc tấn công dựa vào việc khai thác lỗ hổng trên **cổng 445**, đây là cổng được sử dụng cho giao thức SMB để chia sẻ tệp, máy in và các dịch vụ mạng khác.

****

****

****

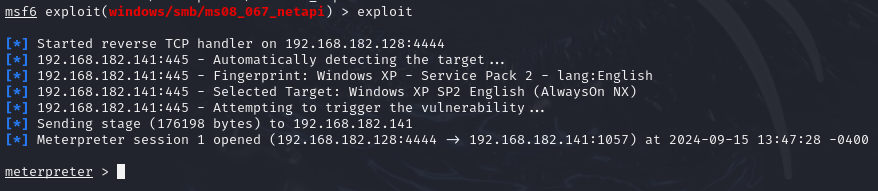
****

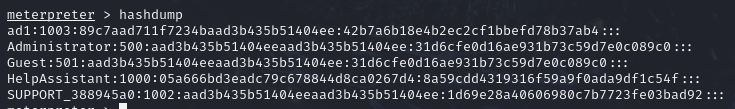
Đã được đặt IP nên ko cần set

Chưa được đặt IP, phải đặt

****

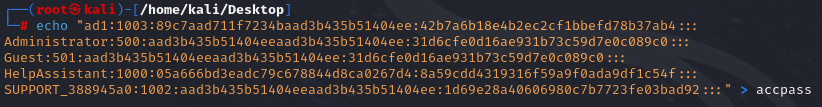
****

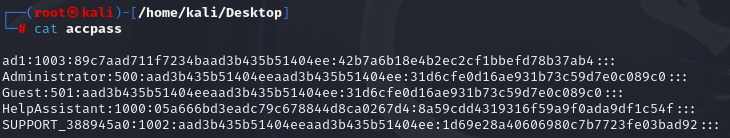
****

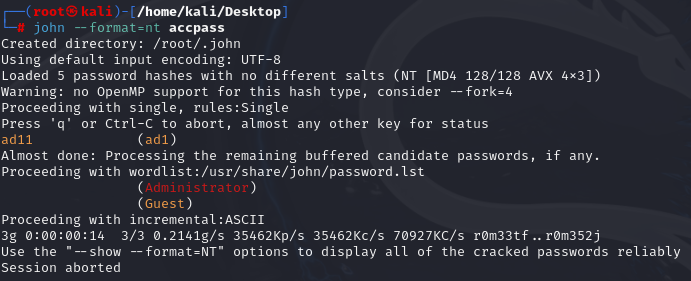
****

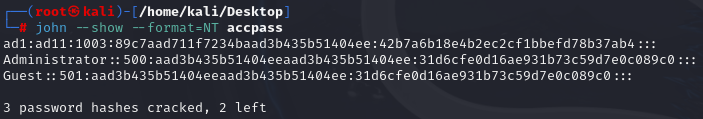
****

****

****

****

****

****

**-----------------------------------------------------------------------**

1. **Khai thác lổ hổng MS17-010 (y như trên, attack port 445, chỉ dùng được win7\_64bit thì mới expoilt được)**

**Các bước ban đầu làm như các mã lỗi MS08-067**

**• Quét cổng**

**• Chạy metasploit**

**• Khai thác**

**• Chiếm quyền truy xuất**

**0. Tắt firewall trên winXP2**

**1. IP\_winXP2 = 192.168.182.141**

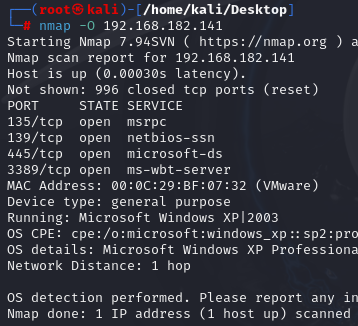
**IP\_Kali = 192.168.182.128**

****

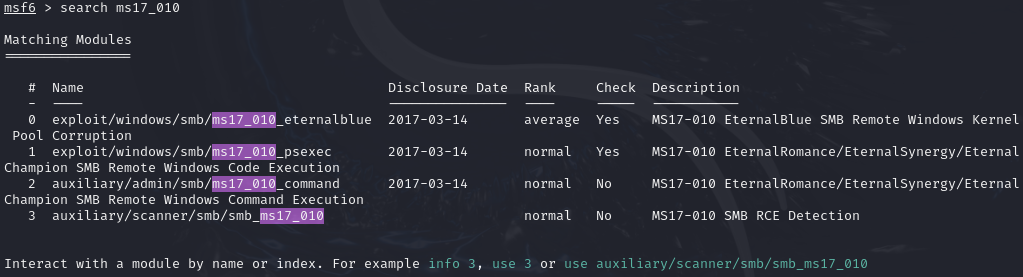
****

**2. Trên Kali**

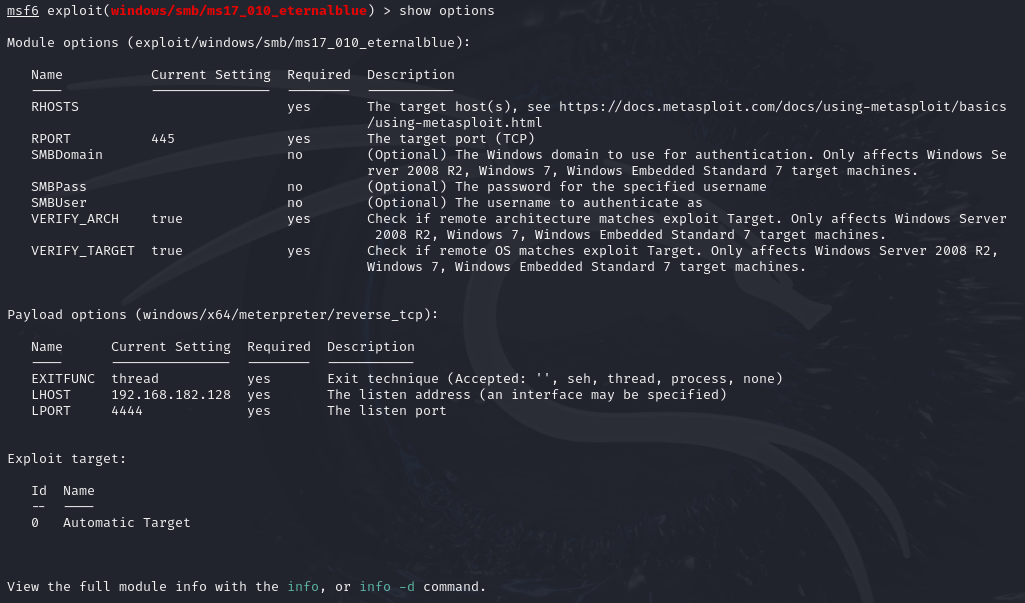


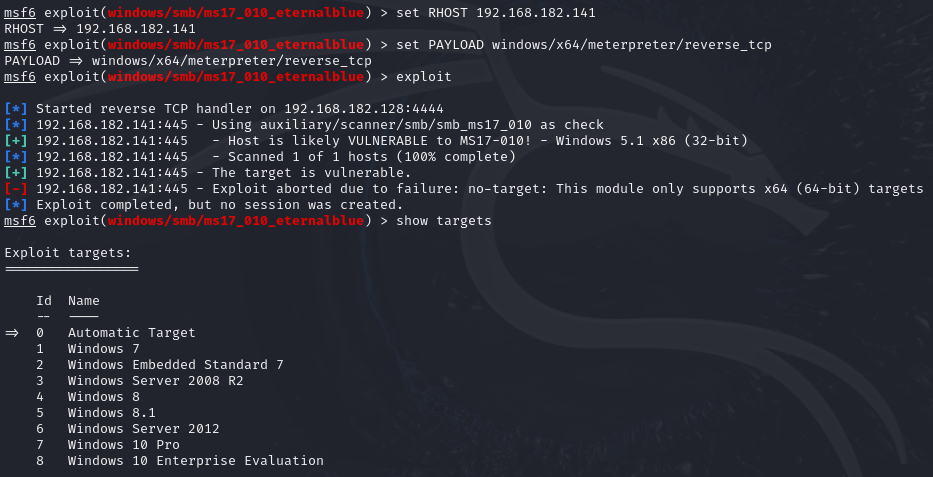












🡺 Winxp2 không khai thác được 🡺 Xài Win7, là phải là 64bits

**Win7-32bits (làm lúc đầu => kết quả là ko attack đc):**

**0. Tắt firewall trên win7**

**1. IP\_win7 = 192.168.182.135**

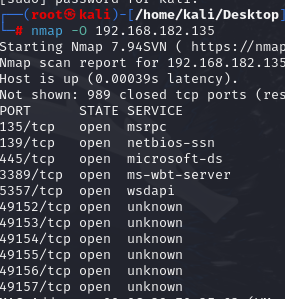
**IP\_Kali = 192.168.182.128**



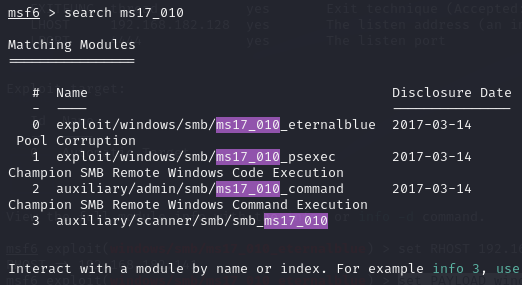
****

**2. Trên Kali**

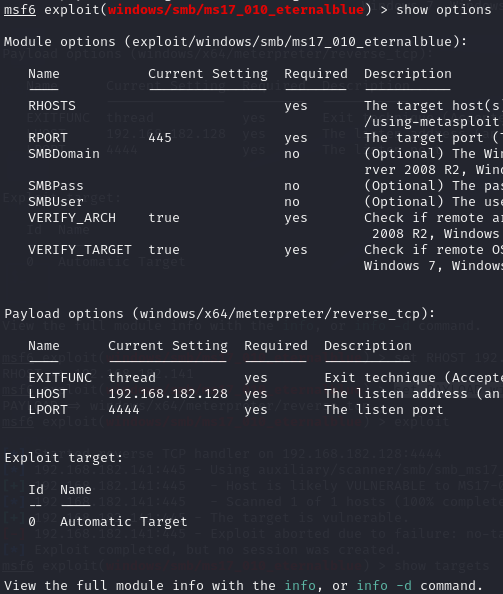






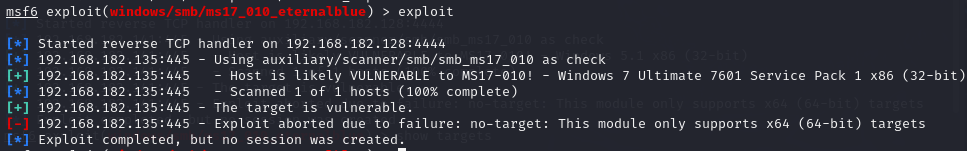












🡺 Bản win7\_32bits này thì không thuộc mục tiêu để khai thác

**Win7\_64bits**

**0. Tắt firewall trên win7\_64bits**

**1. IP\_win7\_64bits = 192.168.182.142**

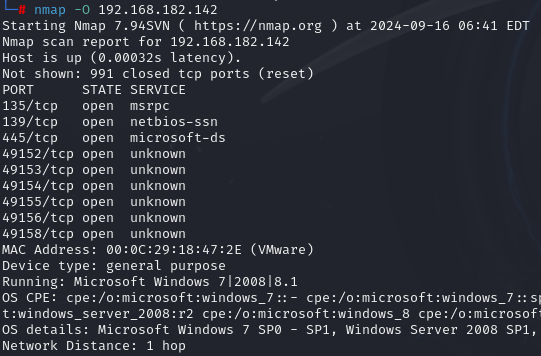
**IP\_Kali = 192.168.182.128**

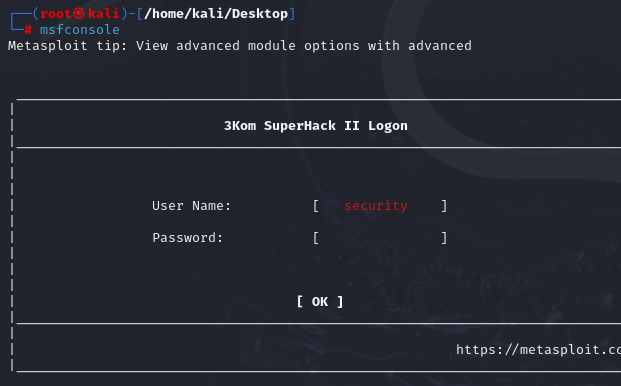
****

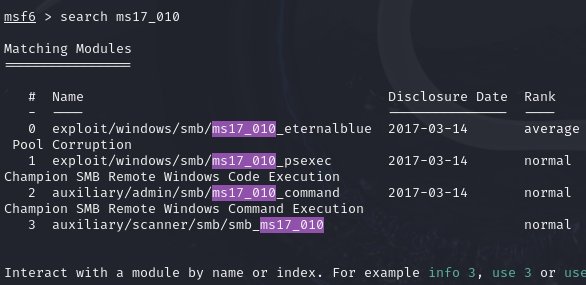
****

**2. Trên Kali**

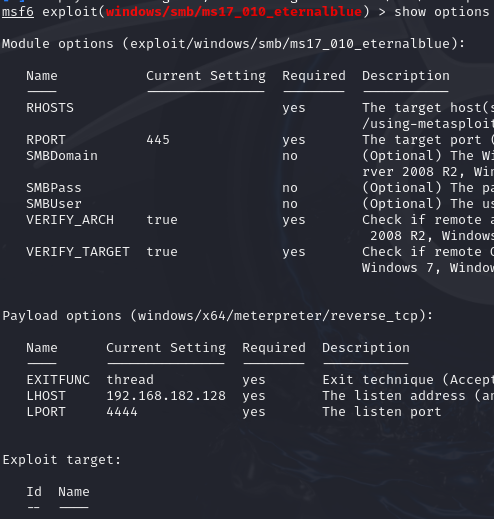






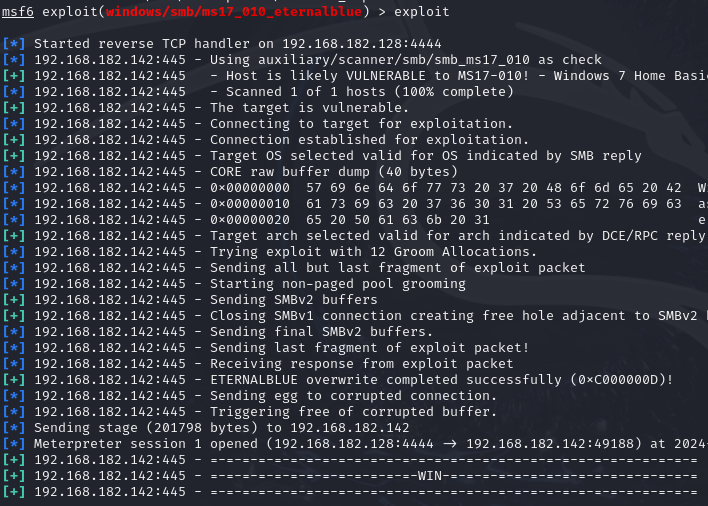


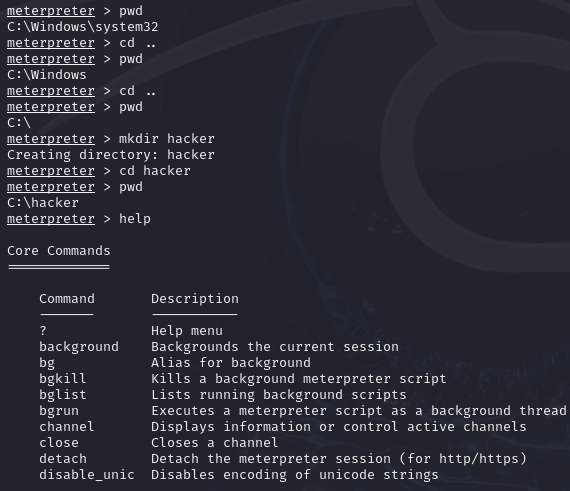






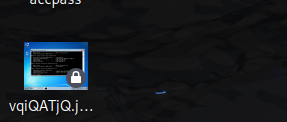






🡺 (chụp ở win7)





🡺



Shutdown ko được vì ko đủ quyền để shutdown