Nguyễn Hữu Bình

Bài 2 : Thực hiện khai thác lỗ hổng MS17-010 và cài đặt RAT lên máy tính victim

Báo cáo: Quay lại video và trình bày lại cách thức khai thác.

Công cụ sử dụng : máy kali ( attacker); máy win 7(victim) , msfconsole , Rat từ bài 1

Lỗ hổng này là 1 exploit khá nghiêm trọng nó ảnh hưởng từ win server 12 trở xuống , windows 10 trở xuống

Hãy nói về lỗ hổng rất nổi tiếng MS17-010 được gọi phổ biến nhất với một số tên viz. etternalblue, etternalsynergy, etternalromance, etternalchaosystem. Lỗ hổng này có liên quan đến SMB-V1 khá đơn giản khi cung cấp cho kẻ tấn công Đặc quyền quản trị để thực thi mã từ xa (RCE) đặc biệt cho Microsoft Server 2012 R2 và Server 2016 dẫn đến một thỏa hiệp lớn. Ngoài những thứ này, ngay cả Windows 7 và Windows 10 cũng có mặt trong danh sách này, nhưng Server vẫn là Server. Nói tóm lại, kẻ tấn công có thể sở hữu Hệ thống bằng cách gửi các gói được chế tạo đặc biệt đến Máy chủ mà máy chủ không xử lý được các yêu cầu đó một cách chính xác.

Ngoài ra, liên quan đến bản vá cho lỗ hổng này đóng một vai trò quan trọng vì việc vá lỗ hổng này chỉ có sẵn thông qua Windows Updates và không dễ dàng.

Bước đầu tôi kiểm tra ip của máy attacker

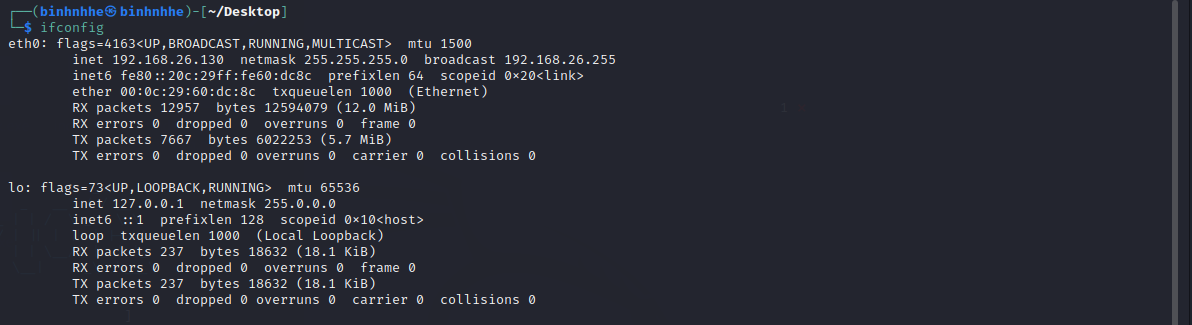
Sau đó tìm địa chỉ ip của máy victims bằng nmap :

Nmap -ss Pn 192.168.26.0/24 ( mô tả rõ nó chức năng )

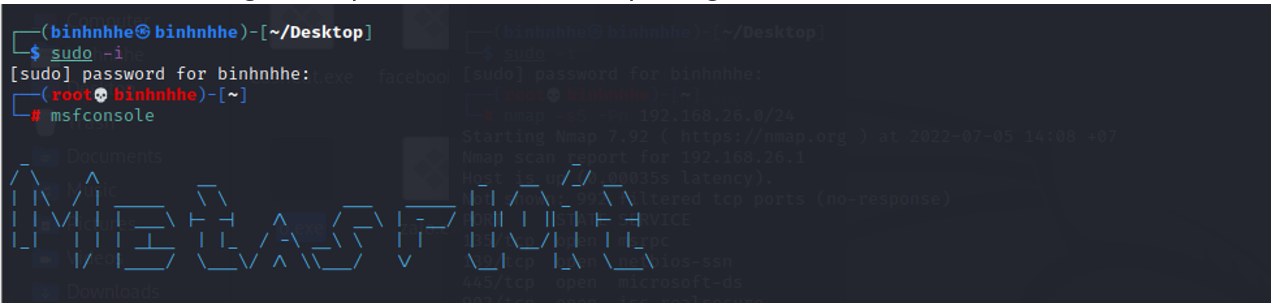
dùng để [quét cổng](https://quantrimang.com/huong-dan-quet-cong-mang-160032) và lỗ hổng bảo mật. Các chuyên gia quản trị mạng sử dụng Nmap để xác định xem thiết bị nào đang chạy trên hệ thống của họ, cũng như tìm kiếm ra các máy chủ có sẵn và các dịch vụ mà các máy chủ này cung cấp, đồng thời dò tìm các cổng mở và phát hiện các nguy cơ về bảo mật.

Về cốt lõi, Nmap là một công cụ quét mạng sử dụng các gói IP để xác định tất cả các thiết bị được kết nối với mạng và cung cấp thông tin về các dịch vụ và hệ điều hành mà chúng đang chạy.

Tìm đc ip máy victims là 192.168.26.147

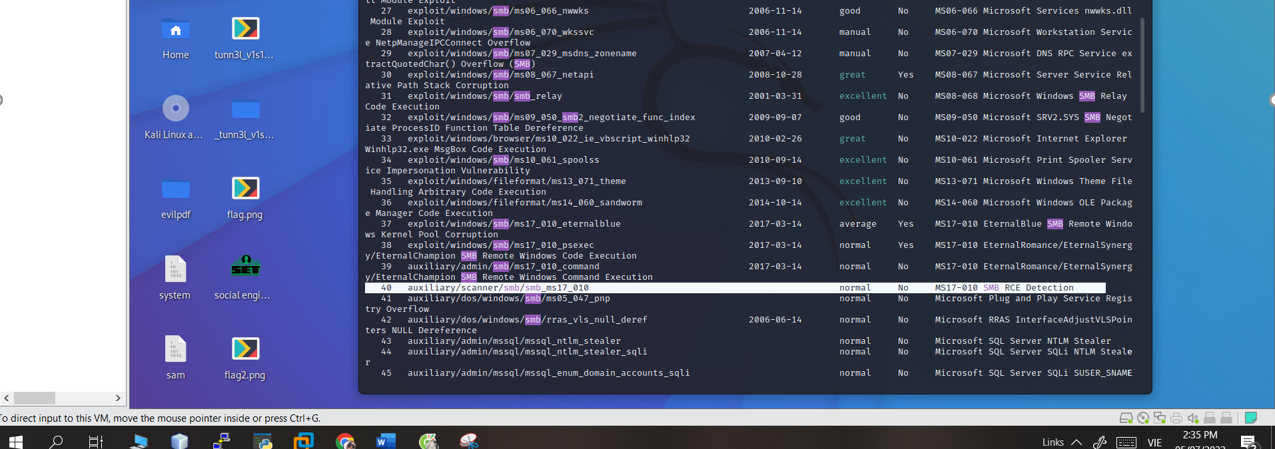




Sau đó tôi sử dụng metasploit để thực hiện tiếp bằng câu lệnh msfconsle : 

Có một payload smb-ms17-010. Payload này được sử dụng để kiểm tra việc thực thi mã từ xa, tức là máy mục tiêu có dễ bị thực thi từ xa hay không . (check lại ) là payload ạ .

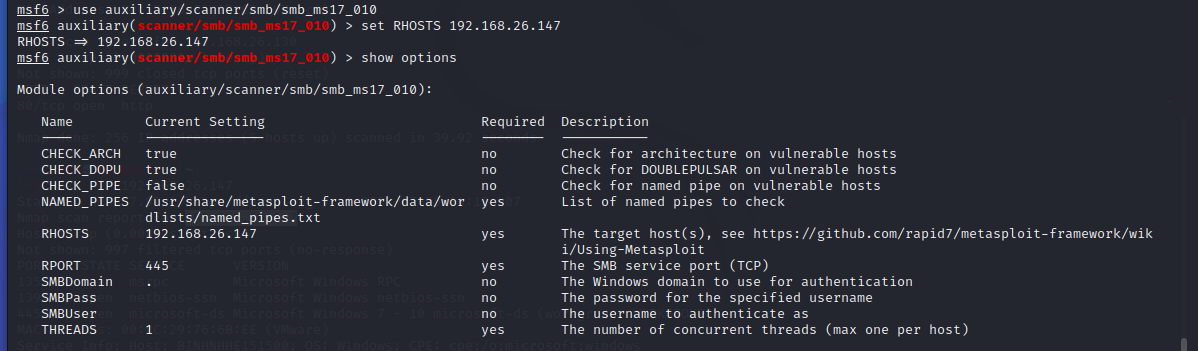




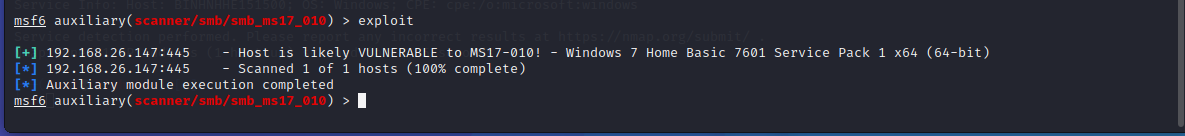
Bây giờ chúng ta tìm thấy cách khai thác phù hợp để chúng ta sẽ sử dụng nó :

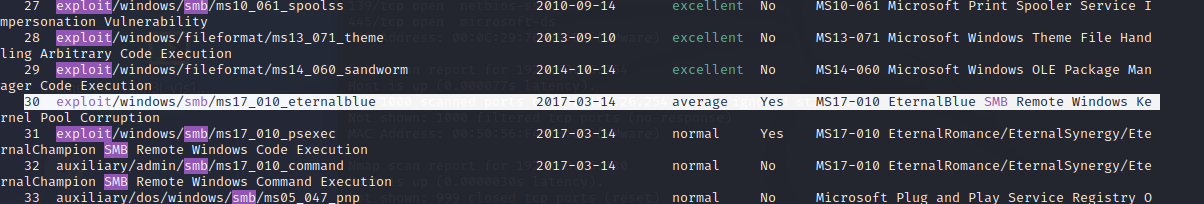
use auxiliary/scanner/smb/smb\_ms17\_010

Thiết lập RHOSTS là id máy victim rồi show option :



Sau đó tiến hành exploit ,có thể thấy đầu ra nơi nó cho thấy máy chủ có khả năng Dễ bị tổn thương đối với MS17-010.

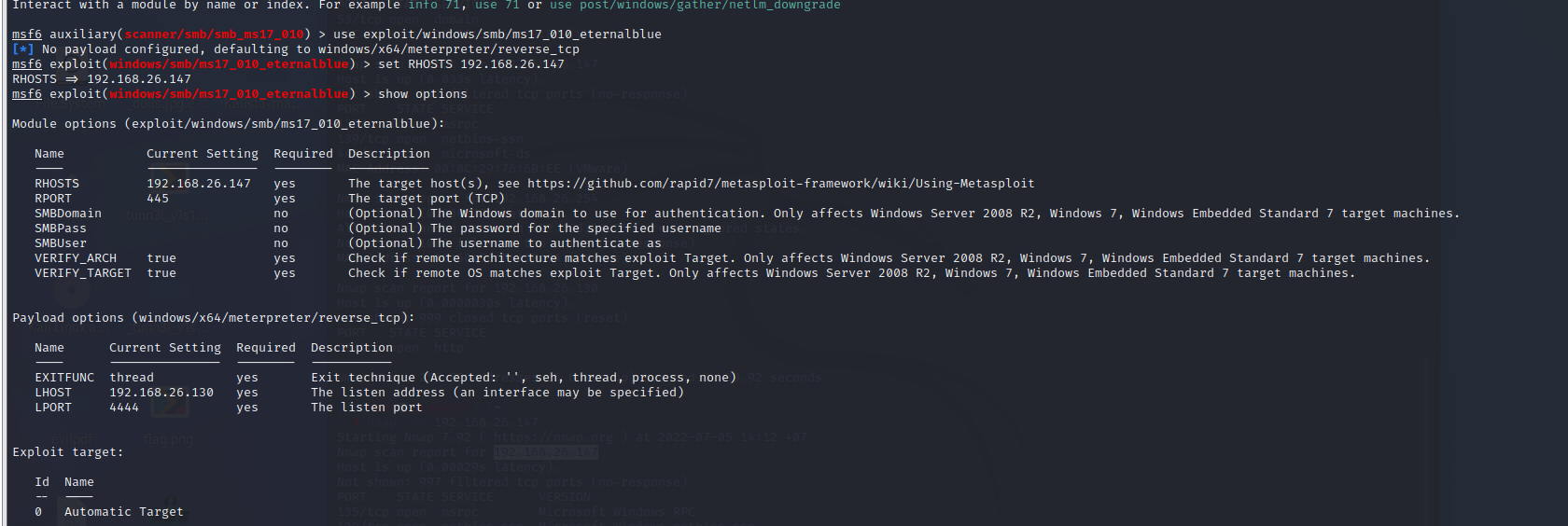


Bây giờ tôi biết máy chủ của victims dễ bị tấn công nên tôi sẽ hack nó, chúng tôi sẽ lại tìm kiếm payload khác sẽ giúp chúng tôi khai thác máy mục tiêu. 

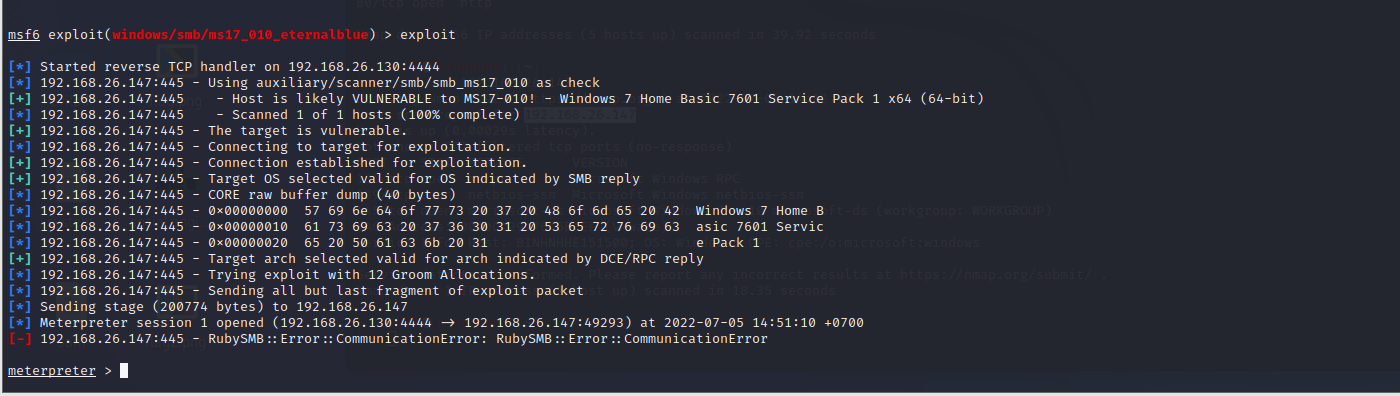
Một lần nữa chúng ta sẽ sử dụng lệnh tương tự để chọn khai thác :

use exploit/windows/smb/ms17\_010\_eternalblue

Thiết lập Rhosts và show option

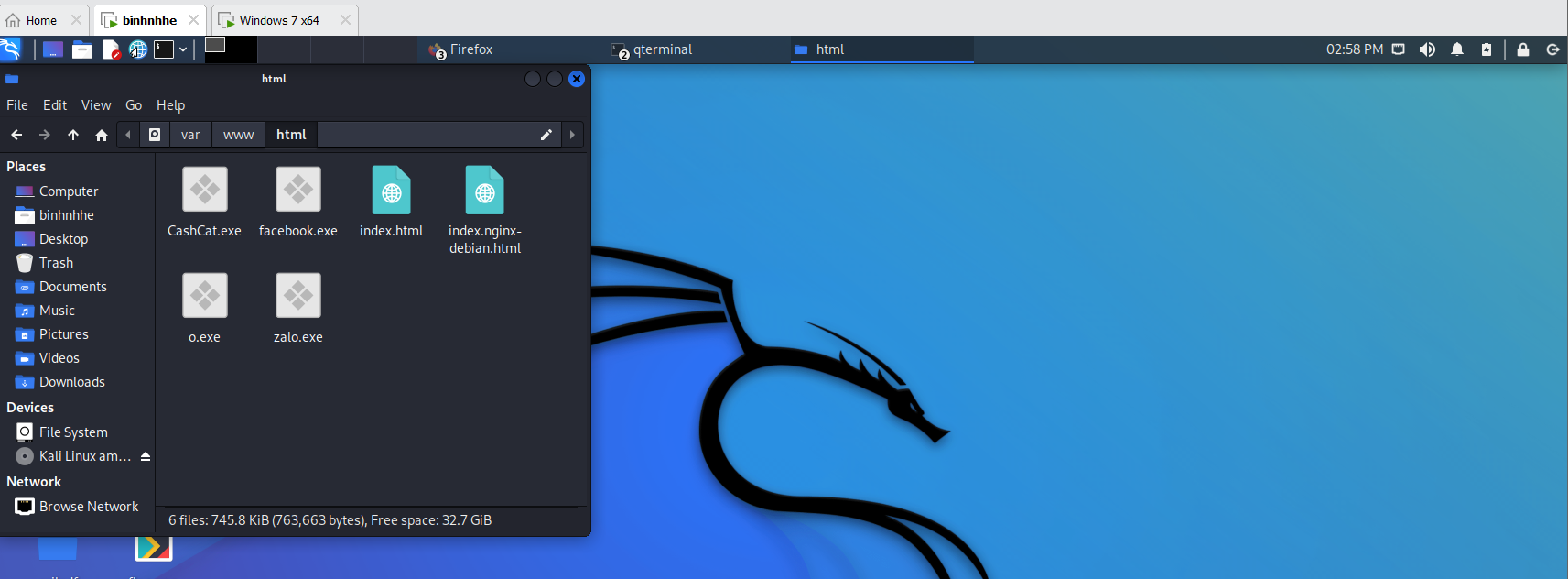


Bây h tôi bắt đầu khai thác lỗ hổng này và đã thành công tấn công vào máy victims

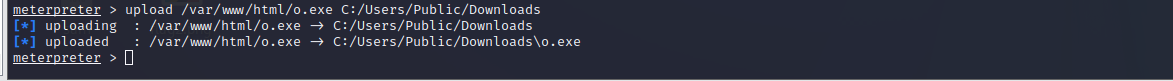


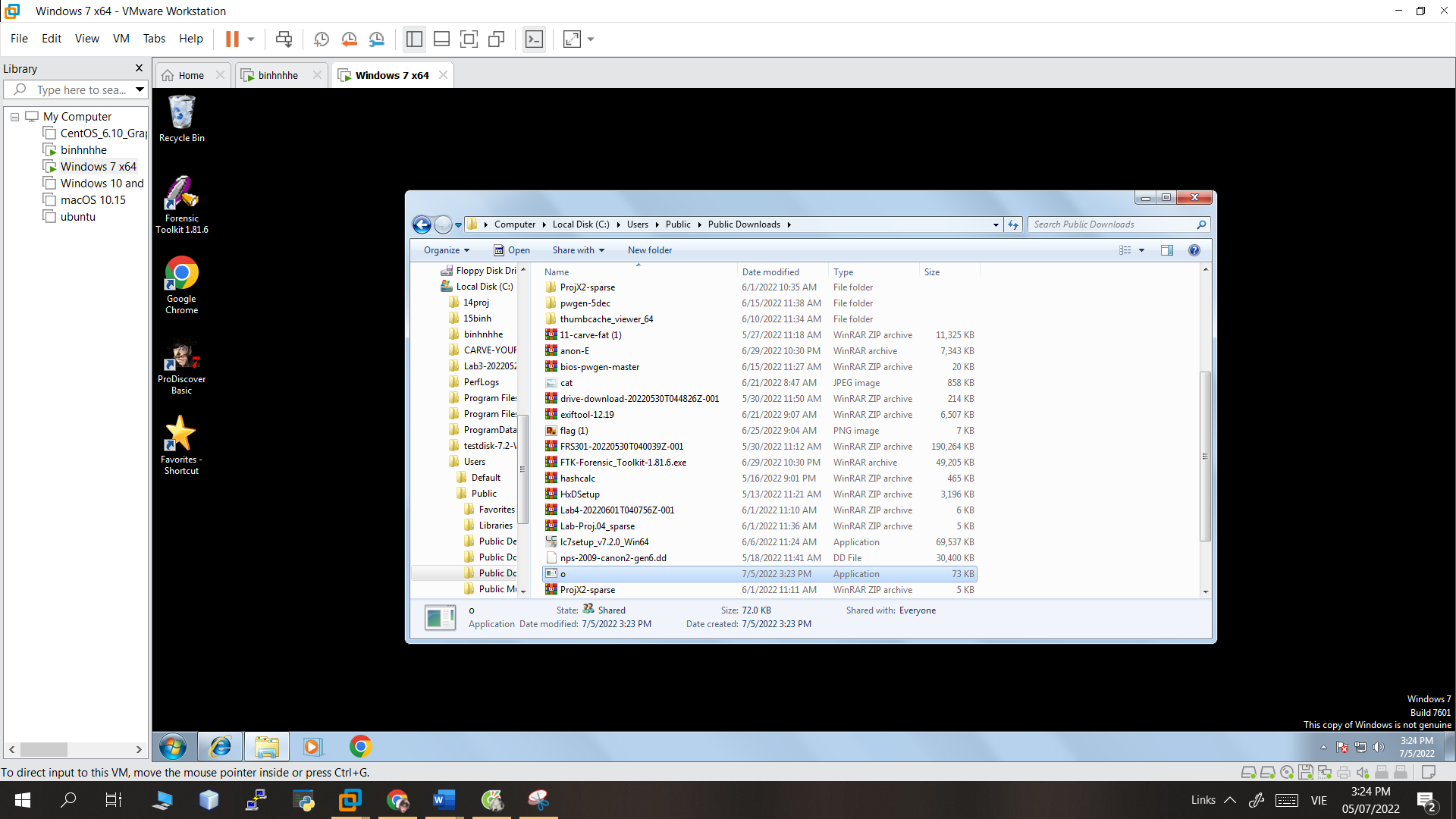
Tiếp theo là cài Rat vào máy victims

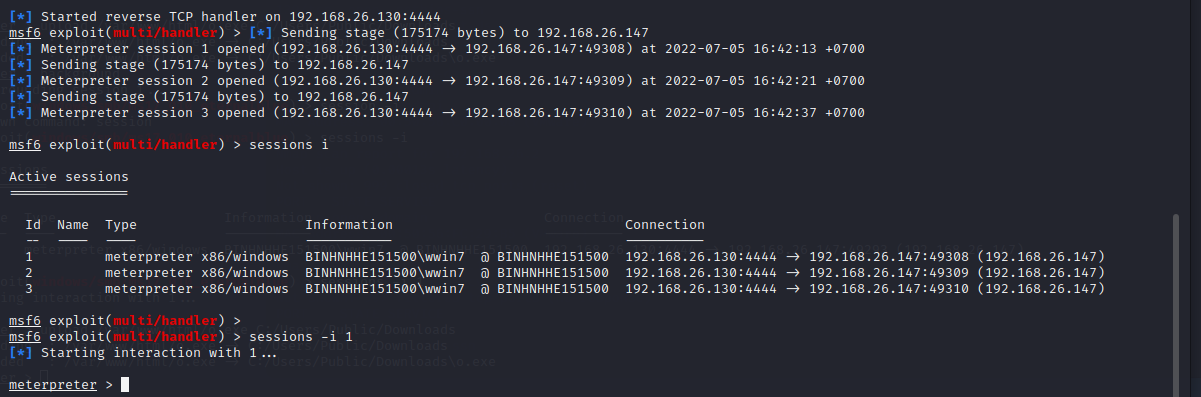
Tôi sẽ sử dụng những con Rat tôi đã tạo hôm trc ở bài 1 :



Upload trực tiếp đến máy victims và xem kết quả :





Sau đó tôi chạy con rat này trên máy victims 

# Và đã thành công xâm nhập vào được máy victims bằng lỗ hổng MS17-010 .

# Hệ điều hành nao bị anh hưởng .

# Windows 7, Windows Server 2008, Windows XP và thậm chí Windows 10(Microsoft Windows Vista SP2; Windows Server 2008 SP2 và R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold và R2; Windows RT 8.1; và Windows 10 Gold, 1511 và 1607; và Windows Server 2016  )

# (tại sao lỗ hổng này lại nguy hiểm)

Khi máy tính bạn bị mắc lỗi này, hệ thống máy chủ dễ tiếp xúc với loại phần mềm độc hại ransomware. Đây là một mô hình tội phạm công nghệ tống tiền nạn nhân tinh vi bằng cách trả phí cho việc yêu cầu khôi phục sau khi mã hóa thành công hoặc làm gián đoạn việc truy cập tìm hiểu dữ liệu của máy chủ.

Đây gọi là EternalBlue - khai thác từ chính bản tin sửa lỗi bảo mật MS17-010 của Microsoft. Các mã độc được kẻ tấn công sử dụng cho mục đích tống tiền là WannaCry, WNCRY, WannaCrypt và NotPetya

# Điều kiện để khai thác lỗ hổng .

# Ip của máy ảo victims , máy ảo có trong nhóm bị ảnh hưởng bởi lỗ hổng (đây là win 7) , sau đó chúng ta sẽ tìm các cổng đang mở, sau đó, chúng ta sẽ khai thác các cổng đó và sử dụng mô-đun Metasploit để hack hệ thống Windows.

# Tham số, điều kiện:

# - Máy window server 2012 R2, window server 2016 r6

# - Giao thức SMP thông qua TCP port 445 / 139

# - anything that uses the SMBv1 (Server Message Block version 1) file-sharing protocol is technically at risk of being targeted for ransomware and other cyberattacks.

# - SMBv1 was first developed in early 1983 as a network communication protocol to enable shared access to files, printers, and ports. It was essentially a way for Windows machines to talk to one another and other devices for remote services.

Nmap -ss Pn 192.168.26.0/24 ( mô tả rõ nó chức năng )

dùng để [quét cổng](https://quantrimang.com/huong-dan-quet-cong-mang-160032) và lỗ hổng bảo mật. Các chuyên gia quản trị mạng sử dụng Nmap để xác định xem thiết bị nào đang chạy trên hệ thống của họ, cũng như tìm kiếm ra các máy chủ có sẵn và các dịch vụ mà các máy chủ này cung cấp, đồng thời dò tìm các cổng mở và phát hiện các nguy cơ về bảo mật.

Về cốt lõi, Nmap là một công cụ quét mạng sử dụng các gói IP để xác định tất cả các thiết bị được kết nối với mạng và cung cấp thông tin về các dịch vụ và hệ điều hành mà chúng đang chạy .

Sử dụng lệnh Nmap để tìm tất cả các cổng đang mở của mục tiêu .tôi phát hiện ra nhiều cổng mở, vì vậy bây giờ chúng tôi sẽ khai thác chúng. Có rất nhiều cổng như 445 mà chúng ta có thể khai thác. Chúng ta biết rằng cổng 445 là một cổng SMB vì ​​vậy chúng ta sẽ bắt đầu tìm kiếm các khai thác .