

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH  
HỌC PHẦN: THỰC TẬP CƠ SỞ  
MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 1.1  
CÀI ĐẶT HỆ ĐIỀU HÀNH MÁY TRẠM WINDOWS**

Sinh viên thực hiện: B22DCAT176 Nguyễn Thị Thùy Linh

Giảng viên hướng dẫn: PGS.TS Hoàng Xuân Dậu

**HỌC KỲ 2 NĂM HỌC 2024-2025**

# MỤC LỤC

MỤC LỤC .....	2
DANH MỤC CÁC HÌNH VẼ.....	3
DANH MỤC CÁC BẢNG BIỂU .....	<b>Error! Bookmark not defined.</b>
DANH MỤC CÁC TỪ VIẾT TẮT.....	4
<b>CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH</b> .....	<b>5</b>
I. Mục đích .....	<b>Error! Bookmark not defined.</b>
II. Tìm hiểu lý thuyết.....	<b>Error! Bookmark not defined.</b>
<b>CHƯƠNG 2. NỘI DUNG THỰC HÀNH</b> .....	<b>11</b>
I. Chuẩn bị môi trường .....	<b>11</b>
II. Các bước thực hiện .....	<b>11</b>
<b>1</b> Cài đặt Windows .....	<b>11</b>
<b>2</b> Cài đặt phần mềm diệt virus.....	<b>12</b>
<b>TÀI LIỆU THAM KHẢO</b> .....	<b>20</b>

## DANH MỤC CÁC HÌNH ẢNH

Hình 1 – Kiến trúc của Hệ điều hành Windows.....	<b>Error! Bookmark not defined.</b>
<a href="#">Hình 2 – Giao diện GUI của Hệ điều hành Windows.....</a>	8
<a href="#">Hình 3 – Giao diện dòng lệnh của Hệ điều hành Windows.....</a>	8
<a href="#">Hình 4 – Giao diện PowerShell của Hệ điều hành Windows.....</a>	9
<a href="#">Hình 5 – Ảnh cài đặt Hệ điều hành Windows 10 thành công trên VMWare.....</a>	11
<a href="#">Hình 6 – Đổi tên thành công máy ảo.....</a>	12
<a href="#">Hình 7 – Cài đặt thành công AVG Antivirus.....</a>	12
<a href="#">Hình 8 – Chạy thử phần mềm AVG Antivirus.....</a>	13
<a href="#">Hình 9 - Màn hình giao diện phần mềm Spybot.....</a>	14
<a href="#">Hình 10 – Chạy thử phần mềm Spybot.....</a>	15
<a href="#">Hình 11 – Tải thành công phần mềm Malwarebytes.....</a>	<b>1Error! Bookmark not defined.</b>
<a href="#">Hình 12 – Scanner trong Malwarebytes hoàn thành.....</a>	<b>1Error! Bookmark not defined.</b>
<a href="#">Hình 13 – Thông tin về các lần quét trong Malwarebytes.....</a>	17
<a href="#">Hình 14 – Load Iso vào máy trạm.....</a>	18
<a href="#">Hình 15 – Giao diện của phần mềm Kaspersky Rescue Disk.....</a>	19
<a href="#">Hình 16– Check IP của máy trạm.....</a>	19
<a href="#">Hình 17 – Mã độc đã được tải xuống.....</a>	20
<a href="#">Hình 18– Kết quả sau khi quét.....</a>	20
<a href="#">Hình 19 – Quá trình quét kết thúc.....</a>	21

## DANH MỤC CÁC TỪ VIẾT TẮT

<b>Từ viết tắt</b>	<b>Thuật ngữ tiếng Anh/Giải thích</b>	<b>Thuật ngữ tiếng Việt/Giải thích</b>
HAL	Hardware Abstraction Layer	Lớp phần cứng trừu tượng
DLL	Dynamic Link Library	Thư viện liên kết động
GUI	Graphical User Interface	Giao diện đồ họa
Spybot S&D	Spybot – Search & Destroy	Tên 1 phần mềm chống các phần mềm độc hại
KRD	Kaspersky Rescue Disk	Tên 1 phần mềm cứu hộ

# CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

## I. Mục đích

Rèn luyện kỹ năng cài đặt và quản trị Hệ điều hành máy trạm Windows cho người dùng với các dịch vụ cơ bản.

## II. Tìm hiểu lý thuyết

### 1.1 Tìm hiểu về phần mềm VMWare Workstation

**VMWare Workstation** là một phần mềm cho phép người dung chạy máy ảo trên máy tính vật lý. Người dung có thể thiết lập, hủy bỏ một hay nhiều máy ảo một cách dễ dàng trên phần mềm này.

- VMWare có một số ưu điểm :
  - + Cho phép người dung tạo nhiều hệ điều hành khác nhau trên cùng một máy tính mà không làm ảnh hưởng đến hiệu suất cũng như tính năng của toàn hệ thống.
  - + Cung cấp môi trường ảo hóa an toàn với người dung và để thử nghiệm các ứng dụng mới hoặc hệ thống cập nhật mà không làm ảnh hưởng và làm hỏng tới hệ thống hiện tại đang chạy.
  - + Tiết kiệm chi phí phát triển các phần mềm mới mà không cần mua nhiều máy tính mới để kiểm tra.
- Tuy nhiên, VMWare cũng có những nhược điểm sau :
  - + Nếu để vào tay kẻ xấu nắm quyền kiểm soát máy tính vật lý chứa các máy ảo thì hẳn có thể kiểm soát được tất cả các máy ảo trong nó.
  - + Khi cài nhiều chương trình máy ảo thì máy tính sẽ chậm và ảnh hưởng đến các chương trình khác.

### 1.2 Tìm hiểu về phần mềm Virtual Box

**Virtual Box** là một phần mềm giả lập hệ điều hành cho phép bạn chạy nhiều hệ điều hành trên một máy tính duy nhất. Đây cũng là công cụ cho những người sử dụng máy tính cá nhân muốn có thể sử dụng nhiều hệ điều hành khác nhau mà không cần phải tắt máy hoặc cài đặt một máy ảo.

- Một số tính năng của Virtual Box:
  - + Là một công cụ đa nền tảng tương thích với mọi hệ thống máy tính hỗ trợ intel/AMD và các hệ điều hành: macOS, Windows, Linux, Oracle Solaris.
  - + Virtual Box cho phép nhiều hệ điều hành chạy trên các máy ảo cùng một lúc.  
Ví dụ như MacBook Air có thể chạy Windows 11 và Ubuntu.
  - + Cho phép mọi hệ thống có thể cài đặt và vận hành tối đa máy ảo của bộ nhớ và dung lượng đĩa. Điều này giúp cho việc triển khai công việc trên máy tính và máy ảo dễ dàng hơn.

## 2. Hệ điều hành Windows

### 2.1. Lịch sử phát triển

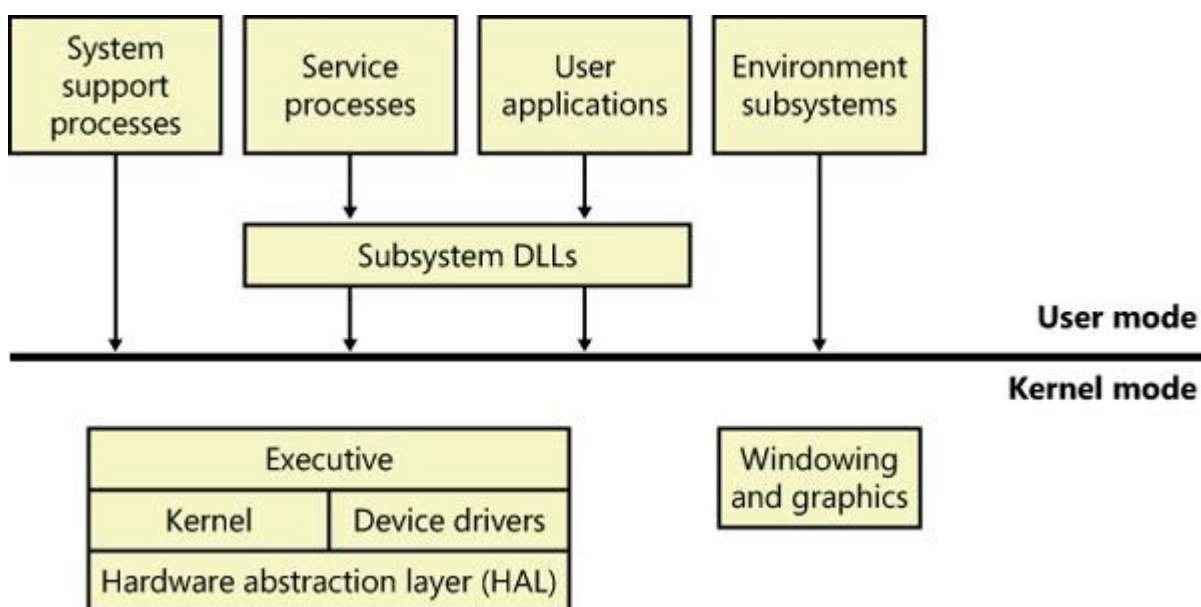
Phiên bản đầu tiên của hệ điều hành Windows được nghiên cứu từ năm 1981 dựa trên nền tảng MS-DOS và được Microsoft ra mắt vào năm 1985, là hệ điều hành đầu tiên có giao diện đồ họa của hãng này.

Nối tiếp sự thành công của phiên bản đầu tiên, Microsoft tiếp tục cho ra đời các phiên bản tiếp theo như: Windows 1.0( 1985), Windows 3.0 & 3.1( 1990 - 1992), Windows 95( 1995), Windows 98( 1998), Windows XP( 2001), Windows Vista( 2006), Windows 7( 2009), Windows 8 & 8.1( 2012 - 2013), Windows 10( 2015), Windows 11( 2021 - nay).

Windows 7, Windows 8, Windows 10, Windows 11 thể hiện sự thay đổi mạnh mẽ về việc sử dụng các thiết bị tính toán cá nhân mà máy tính PC là một đại diện. Mục tiêu của hệ điều hành mới là hợp nhất các nền tảng Windows cho các thiết bị di động như : điện thoại, máy tính bảng. Nhờ vậy mà các ứng dụng có thể được tải về và chạy trên tất cả các thiết bị Windows.

### 2.2 Kiến trúc hệ điều hành Windows

Kiến trúc của hệ điều hành Windows hiện thời dựa trên kiến trúc Windows NT. Về cơ bản, kiến trúc này được chia thành hai lớp tương ứng với hai chế độ hoạt động: Chế độ nhân và Chế độ người dùng.



Hình ảnh 1 : Kiến trúc của Hệ điều hành Windows

**Chế độ nhân (Kernel mode) :** Có quyền kiểm soát toàn bộ tài nguyên phần cứng. Nếu một lỗi xảy ra ở Kernel mode, có thể “crash toàn bộ hệ thống” (khiến toàn bộ hệ thống bị sập). Các chức năng cơ bản gồm :

+ *Executive (Thực thi)* : thực hiện quản lý các tiến trình và luồng, quản lý bộ nhớ,..

- + *Kernel (Nhân)* : chịu trách nhiệm điều độ luồng, đồng bộ giữa các tiến trình, xử lý ngắt.
- + *Device Drivers (Các trình điều khiển thiết bị)* : nhiệm vụ giao tiếp giữa quản lý vào/ra của phần thực thi và phần cứng cụ thể. Các trình điều khiển này cũng có thể liên lạc với hệ thống file, mạng hay giao thức khác.
- + *Hardware Abstraction Layer – HAL (Lớp phần cứng trừu tượng)*: giấu đi các chi tiết phần cứng giúp hệ điều hành có thể hoạt động trên nhiều phần cứng khác nhau với giao tiếp không đổi.
- + *Windowing and Graphics Functions (Các chức năng cửa sổ và đồ họa)*: cung cấp giao diện đồ họa cho người dùng.

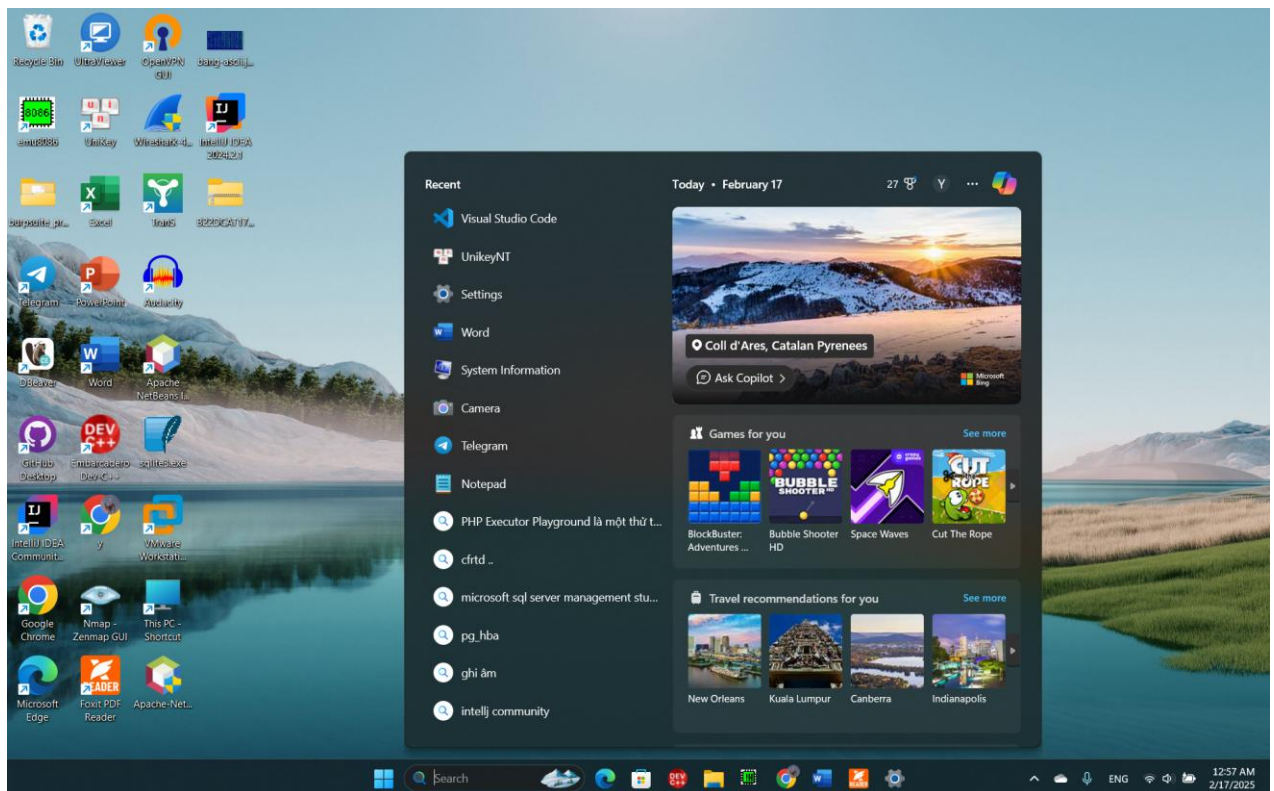
**Chế độ người dùng (User mode):** Là nơi ứng dụng chạy, có quyền truy cập giới hạn vào hệ thống. Nếu một ứng dụng lỗi, nó không ảnh hưởng đến toàn bộ hệ thống. Các chức năng cơ bản gồm:

- + *System Support Processes (Chương trình hỗ trợ hệ thống)*: chứa các chương trình thực hiện các chức năng hệ thống: đăng nhập, quản lý phiên làm việc.
- + *Service Processes (Các chương trình dịch vụ)*: cung cấp các dịch vụ: quản lý máy in, tác vụ, cơ sở dữ liệu,...
- + *User Applications (Ứng dụng người dùng)*: các chương trình thực hiện theo yêu cầu của người quản trị.
- + *Environment Subsystem (Hệ thống con)* và *Subsystem DLL (Hệ thống liên kết động)*: kết hợp với nhau cho phép các kiểu ứng dụng khác nhau hoạt động được trên các môi trường: Win32, Win64 hay DOS32.

### **2.3 Giao diện của hệ điều hành Windows**

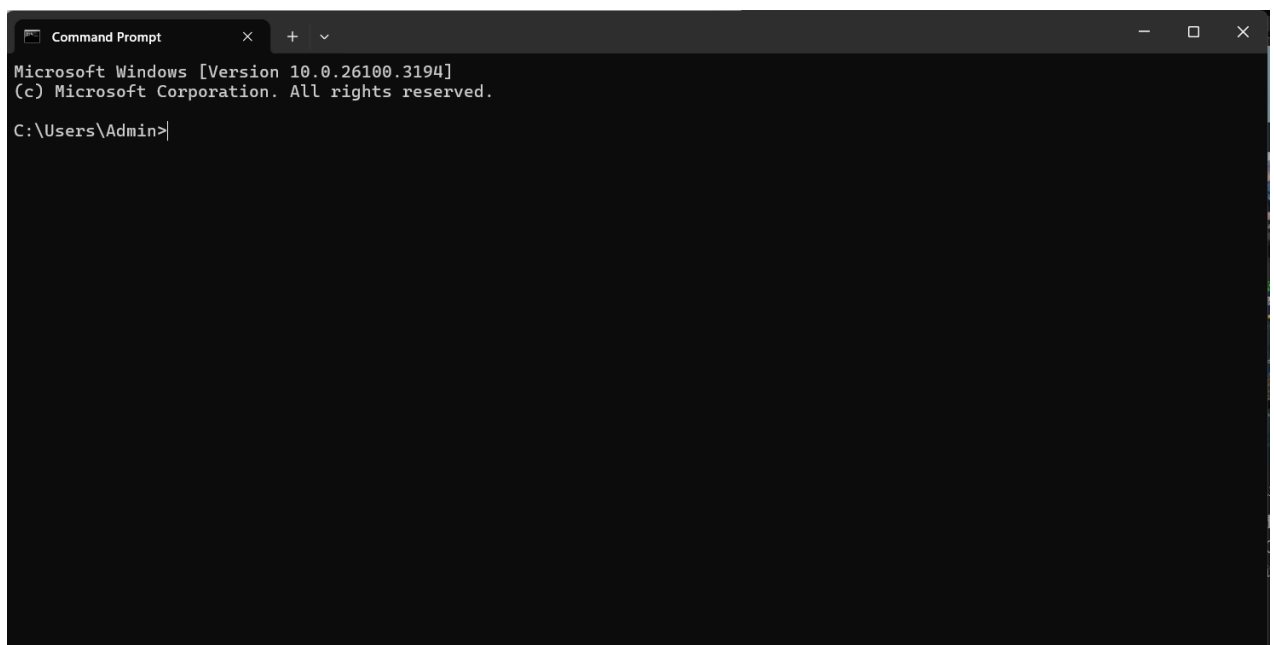
Hệ điều hành Windows gồm 3 giao diện chính giúp hệ điều hành làm việc với các ứng dụng và thực hiện các công việc quản trị.

- *Giao diện đồ họa (GUI)*: bao gồm các cửa sổ, nút bấm, menu khởi động (Start), thanh tác vụ (Taskbar). Start cho phép người quản trị truy nhập vào tất cả các chức năng của hệ điều hành cũng như các chương trình quản trị. Thanh Taskbar cho phép truy nhập nhanh đến các ứng dụng và cho biết tính trạng của các chương trình người quản trị. Màn hình làm việc (Desktop) chứa các biểu tượng chương trình người dùng và sẽ hiển thị thông tin cho người dùng khi các chương trình người dùng chạy.



Hình ảnh 2 : Giao diện GUI của Hệ điều hành Windows

- *Giao diện dòng lệnh (dòng lệnh DOS):* Giao diện dùng để thực thi các thao tác cầu hình cho hệ điều hành hay chạy các chương trình DOS cũ. Trong môi trường Windows, nó không còn thực sự là DOS dù có nhiều câu lệnh DOS vẫn còn dùng được và được kích hoạt thông qua chương trình cmd.exe.

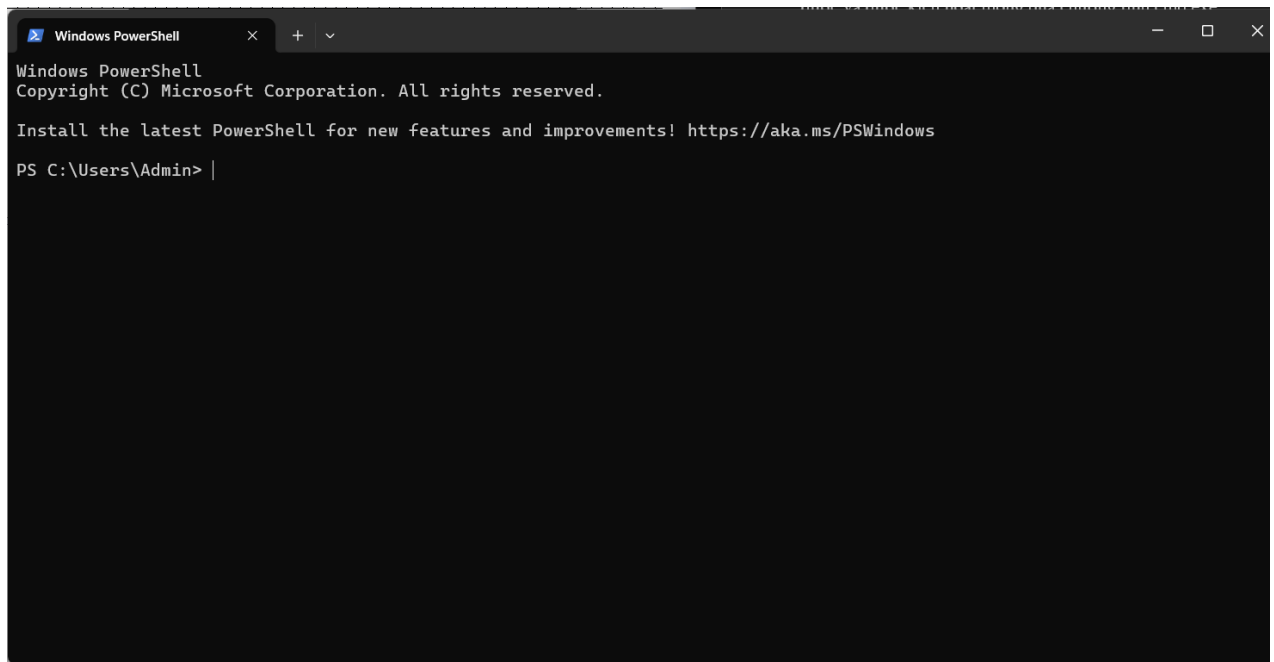


Hình ảnh 3 : Giao diện dòng lệnh trong Hệ điều hành Windows

- *Giao diện PowerShell:* Đây là giao diện dòng lệnh mới của Windows thường dùng cho các tác vụ quản trị. Cung cấp tính năng lập trình đơn giản (Scripting) cùng với các hàm logic và các biến, người quản trị có thể tự động hóa các tác vụ thuận tiện



hơn rất nhiều so với giao diện DOS cũ. Ngoài ra nó còn cho phép thực thi các lệnh từ xa nhờ hỗ trợ từ hệ điều hành. Microsoft đã hỗ trợ tập các lệnh cmdlet trong môi trường PowerShell để thực hiện các tác vụ mong muốn.



Hình ảnh 4: Giao diện PowerShell trong Hệ điều hành Windows

#### **2.4 Đặc điểm đặc trưng:**

- Windows có chế độ đa nhiệm cùng với một hệ thống giao diện dựa trên cơ sở bảng chọn với các biểu tượng kết hợp giữa đồ họa và văn bản giải thích.
- Cung cấp nhiều công cụ xử lý đồ họa và đa phương tiện (Multimedia)
- Người dùng có thể mở cùng lúc nhiều chương trình nhưng không nên mở quá nhiều chương trình vì nếu mở quá nhiều chương trình có thể khiến máy tính bị quá tải hoặc gặp phải tình trạng treo máy.

### **3. Các phần mềm diệt Virus, phần mềm chống gián điệp, phần mềm cứu hộ**

#### **3.1 Phần mềm diệt virus AVG AntiVirus**

**AVG Antivirus Free** là phần mềm diệt virus cho máy tính với cơ chế hoạt động thông minh, tiện lợi, có thể ngăn chặn, phát hiện và loại bỏ virus, chặn quảng cáo một cách nhanh chóng và hiệu quả.

- + Với sự trợ giúp của AVG Antivirus Free, máy tính, dữ liệu web và email của bạn sẽ luôn được bảo vệ trong một môi trường an toàn.
- + Phần mềm được miễn phí những được tích hợp đầy đủ các tính năng phong phú hơn các công cụ trả phí khác, mang đến cho hệ thống của người dùng khả năng quét và tìm nhiều loại virus với phần mềm độc hại khác.

- + AVG Antivirus Free sở hữu giao diện làm việc trực quan tạo sự dễ dàng cho người mới bắt đầu.
- + Nổi bật chế độ quét virus khác nhau để người dùng lựa chọn tùy theo tình trạng hệ thống của mình, bảo vệ tốt nhất.
- + AVG Antivirus Free sẽ thực hiện quét máy tính trong thời gian nhanh nhất, phát hiện và tạo báo cáo quét virus chi tiết cho người dùng.

### 3.2 Phần mềm gián điệp Spybot S&D (Spybot – Search & Destroy)

*Spybot S&D* là phần mềm chuyên thu thập các thông tin từ các máy chủ (thông thường vì mục đích thương mại) qua mạng Internet mà không có sự nhận biết và cho phép của chủ máy (Spyware)

- + Spybot S&D là phần mềm cho hệ điều hành Windows. Chương trình này sẽ quét ổ cứng để xác định những phần mềm do thám hoặc những module phần mềm chuyên làm hiển thị các mục quảng cáo hoặc gửi thông tin từ máy của bạn về cho chủ của nó. Nếu tìm được những đối tượng này, Spybot Search and Destroy sẽ gỡ bỏ và thay thế chúng bằng những adware giả, trống rỗng vì thông thường, phần mềm chủ của chúng vẫn sẽ hoạt động sau khi adware đã bị gỡ đi.

### 3.3 Phần mềm chống các phần mềm độc hại Malwarebytes Anti-Malware

Là một phần mềm chống, tìm và xóa phần mềm độc hại được phát triển bởi Malwarebytes Corporation. Các tính năng của Malwarebytes bao gồm cả diệt virus và phát hiện, ngăn chặn các mã độc, virus theo dõi, malware, trojan, worm để tránh gián điệp, đánh cắp thông tin hay khóa file trái phép.

### 3.4 Phần mềm cứu hộ Kaspersky Rescue Disk (KRD)

Phần mềm cứu hộ được sử dụng để làm sạch một PC không thể khởi động và có thể tìm thấy phần mềm độc hại ẩn khi hệ điều hành của máy chủ đang hoạt động.

**Kaspersky Rescue Disk** là một bộ phần mềm với các công cụ như chương trình chống virus có khả năng khởi động miễn phí, trình duyệt web và trình chỉnh sửa Windows Registry. Trình quét virus cho phép bạn quét bất kỳ tệp hoặc thư mục nào trên máy tính mà không yêu cầu bạn quét toàn bộ ổ cứng, đây là một tính năng hữu ích.

## CHƯƠNG 2 : NỘI DUNG THỰC HÀNH

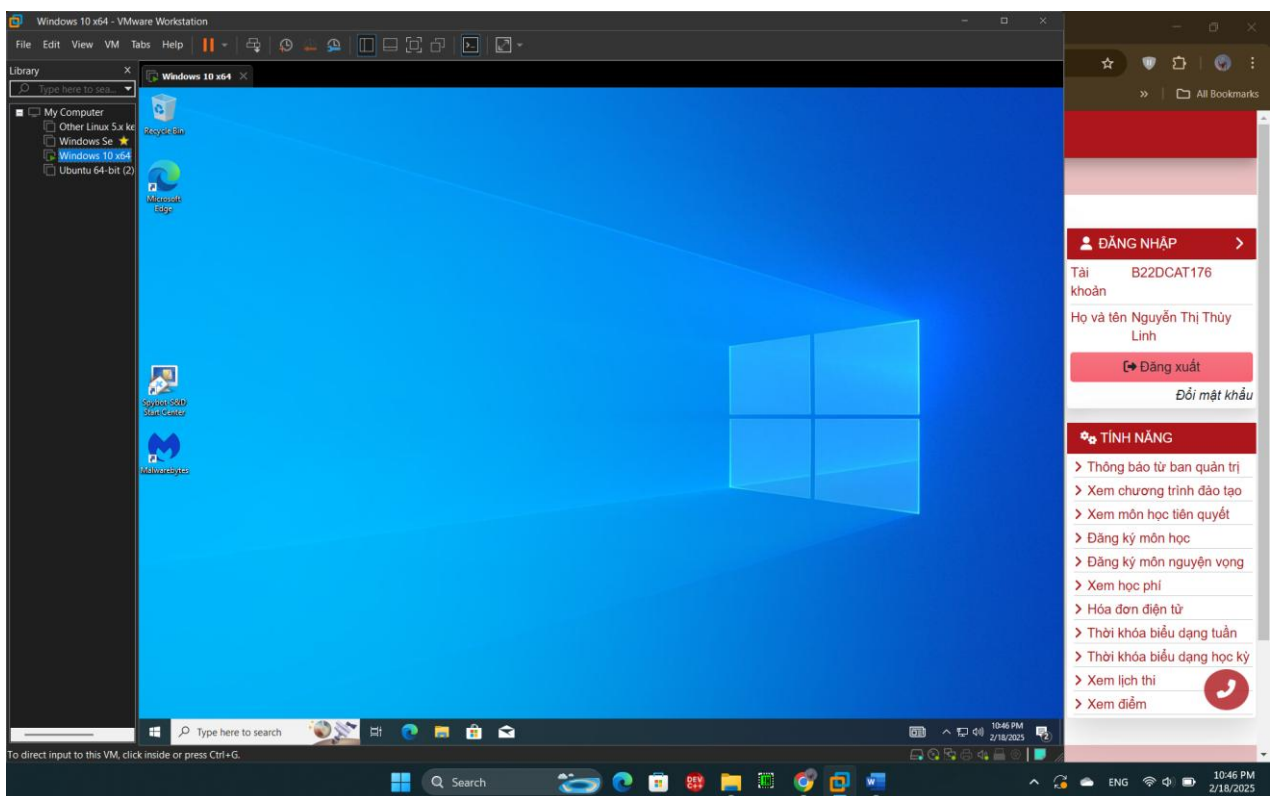
### I. Chuẩn bị môi trường

- Download file đĩa của phần mềm Windows 10 (iso)
- Download phần mềm ảo hóa VMWare Workstation
- Download phần mềm cứu hộ (iso)

### II. Các bước thực hiện

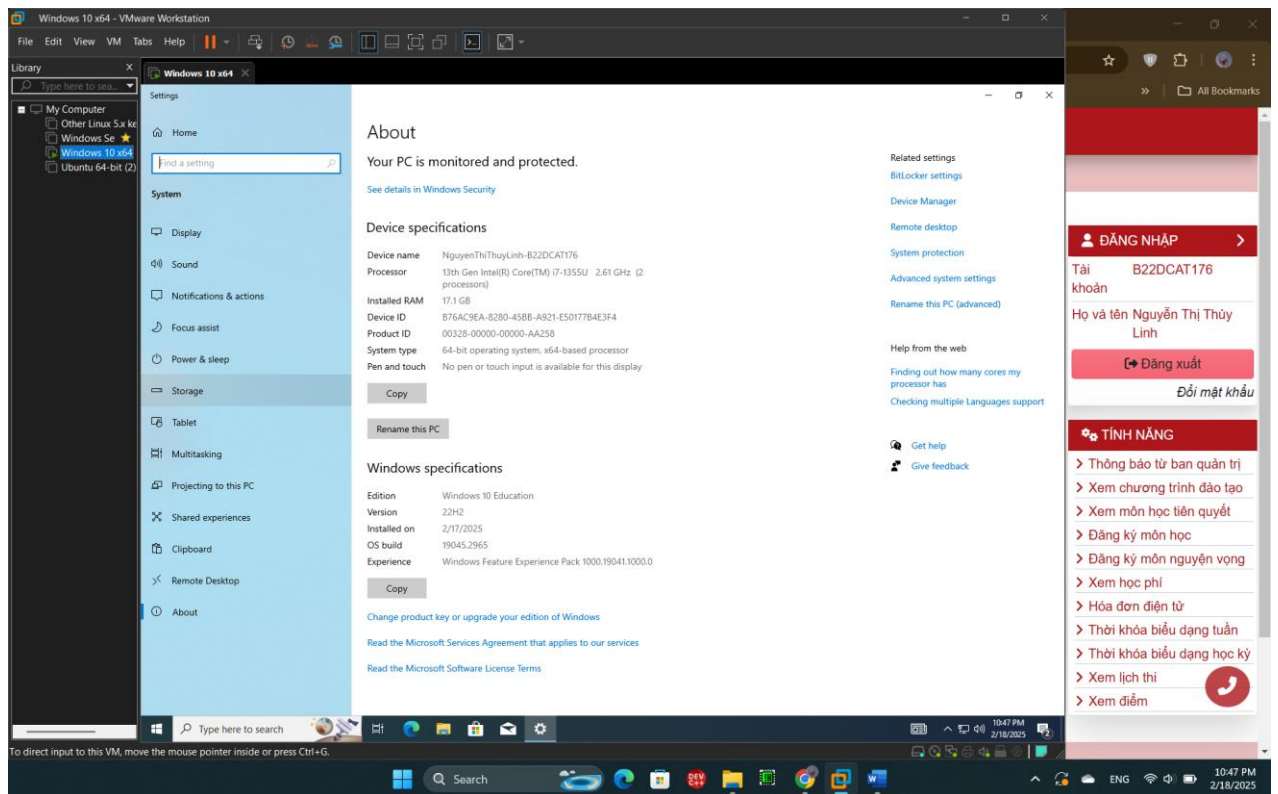
#### 1. Cài đặt Windows

- Cài đặt VMWare Workstation và máy ảo Windows 10



Hình ảnh 5 : Ảnh cài đặt hệ điều hành Windows 10 thành công trên VMWare

- Đổi tên của máy ảo

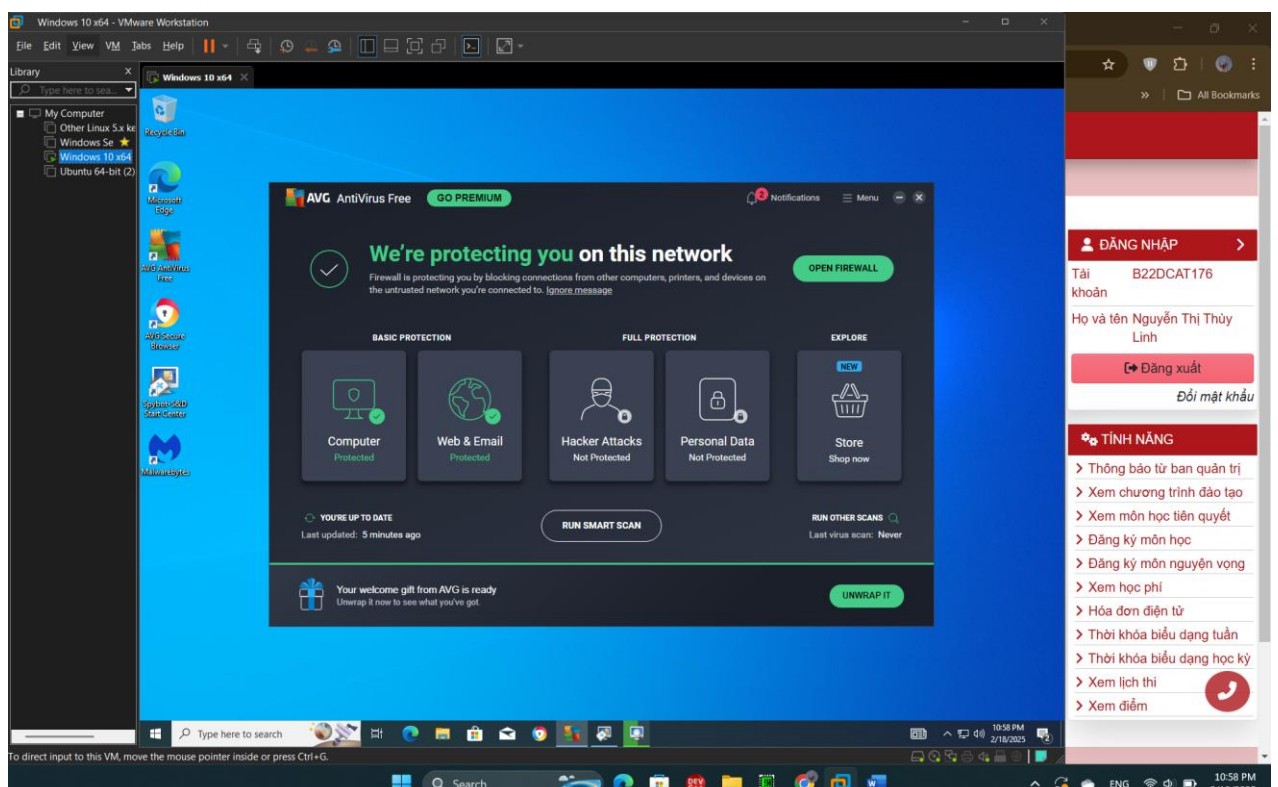


Hình ảnh 6 : Đổi tên thành công máy ảo

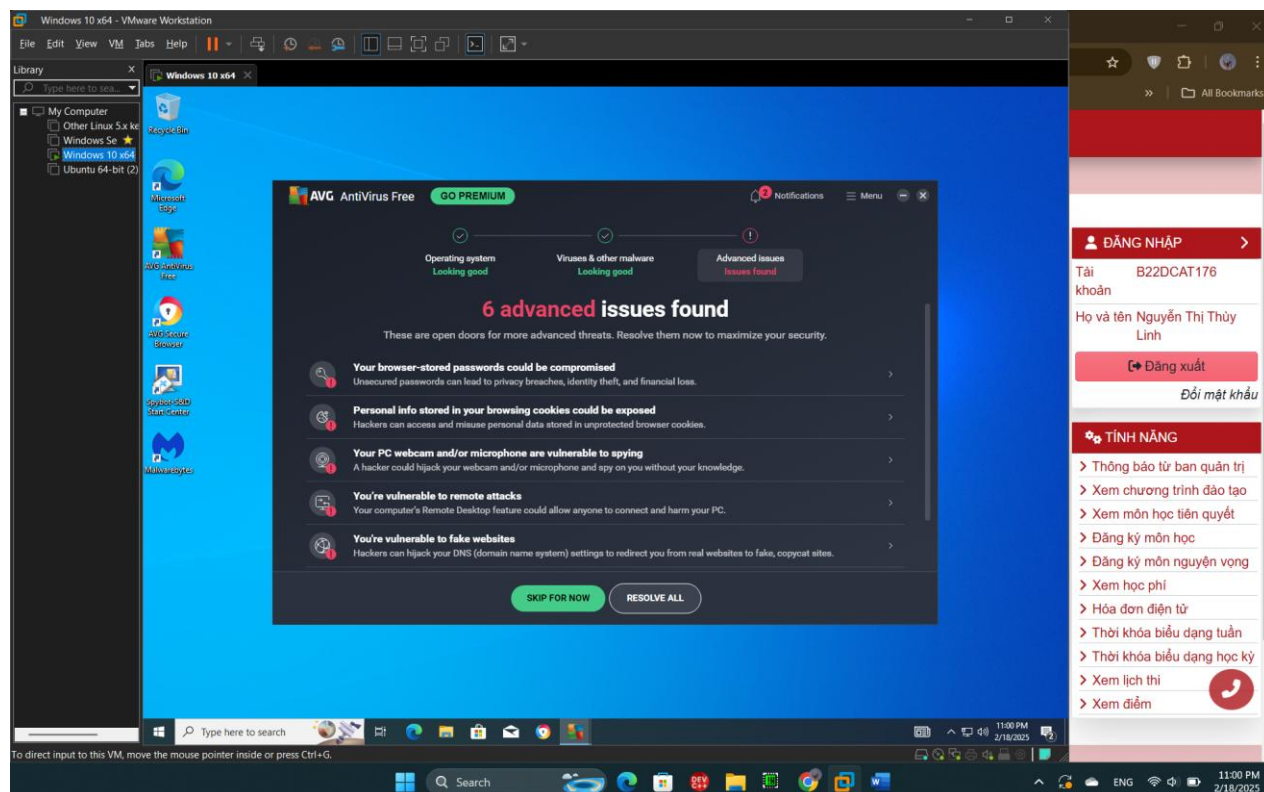
## 2) Cài đặt phần mềm diệt virus

\* Cài đặt phần mềm diệt virus AVG Antivirus.

- Chạy và sử dụng phần mềm



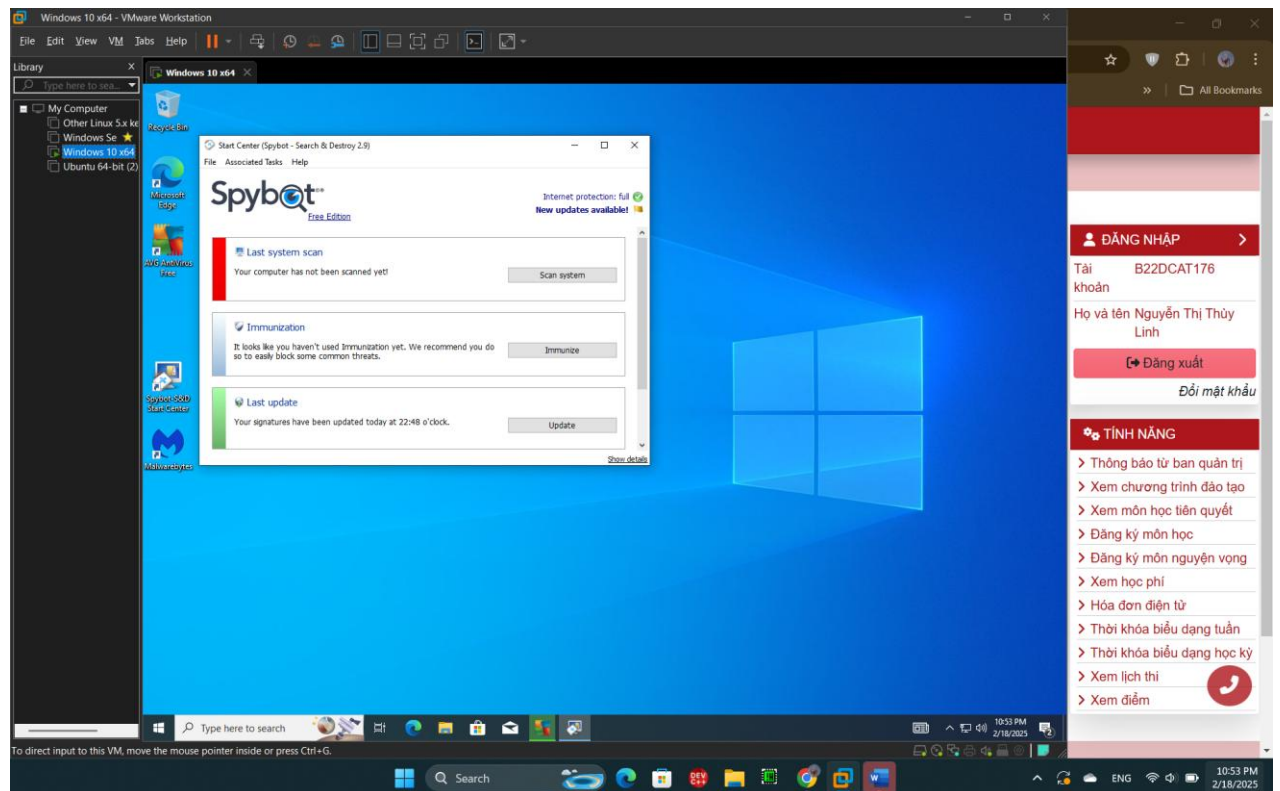
*Hình ảnh 7 : Cài đặt thành công AVG Antivirus*



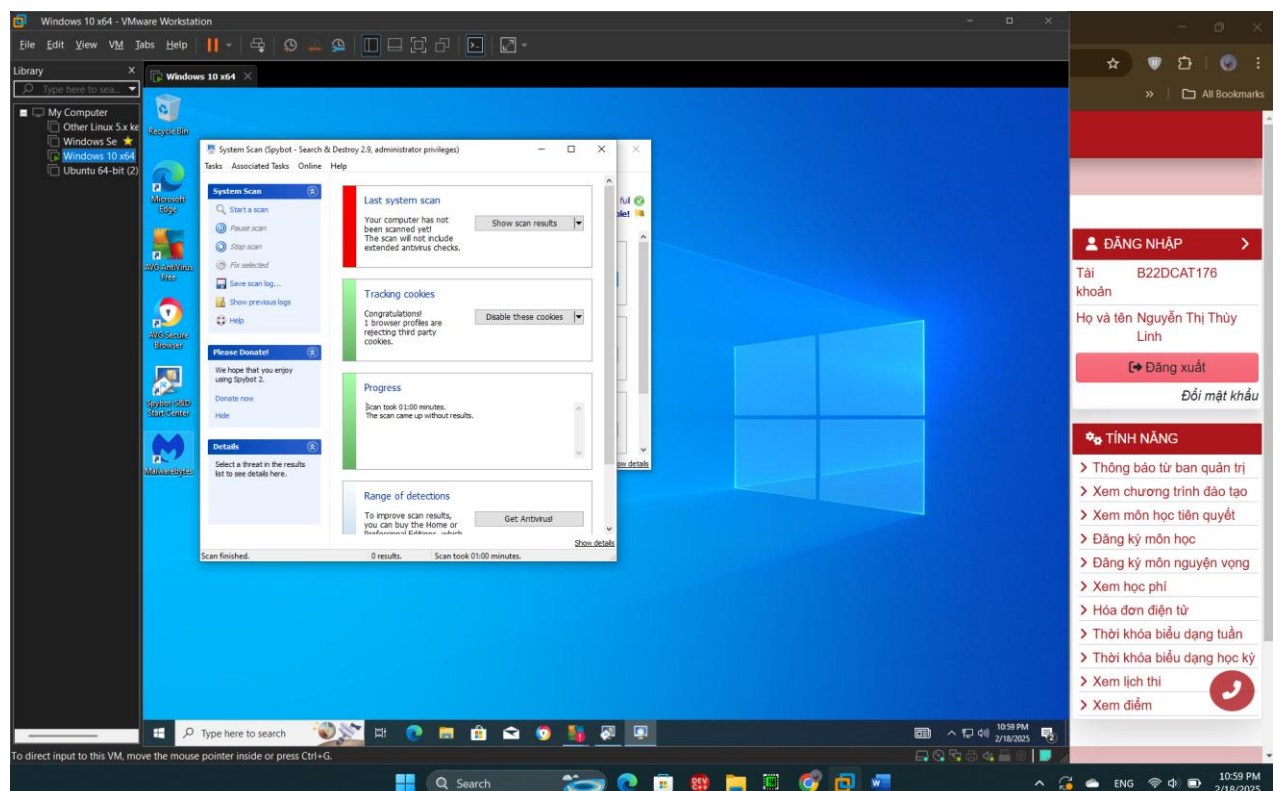
*Hình ảnh 8 : Chạy thử phần mềm AVG Antivirus*

- Cài đặt phần mềm chống phần mềm gián điệp Spybot S&D (Spybot – Search & Destroy)
  - Tải và chạy thử phần mềm



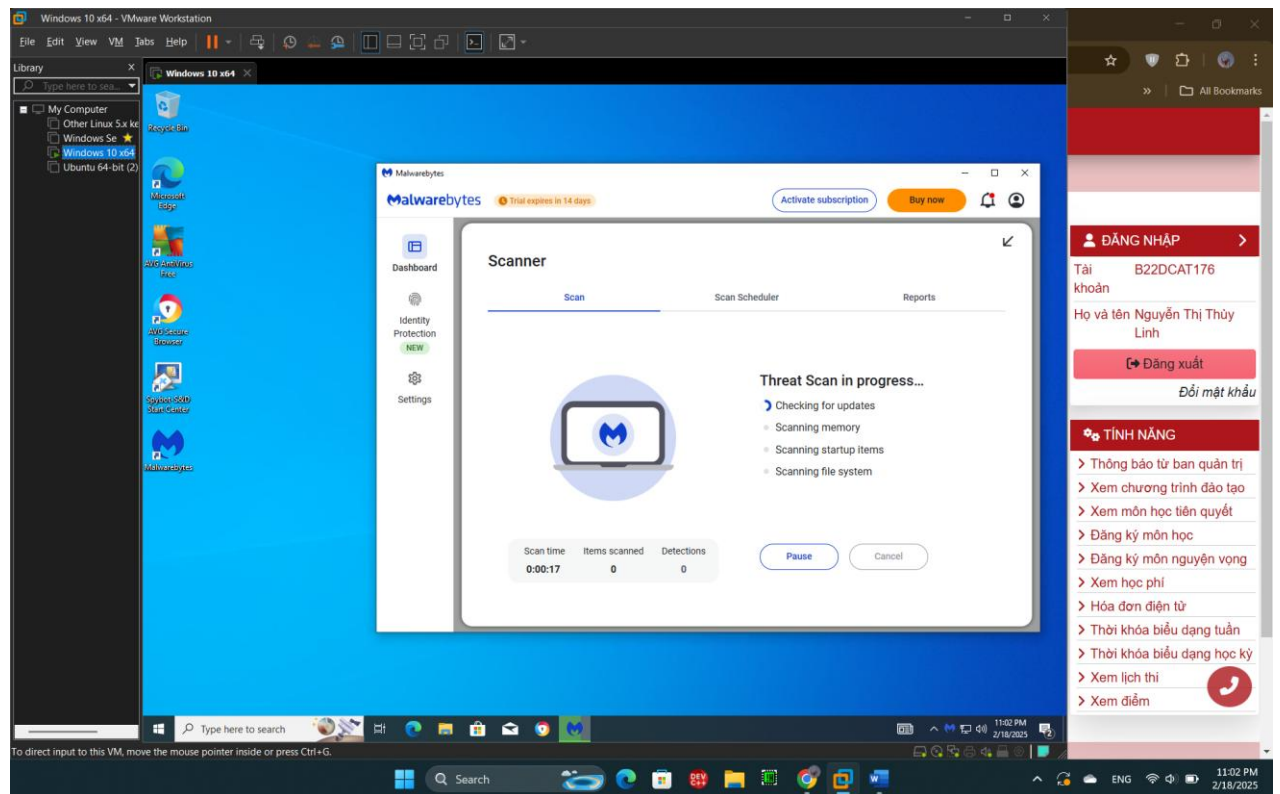


Hình ảnh 9 : Màn hình giao diện phần mềm Spybot

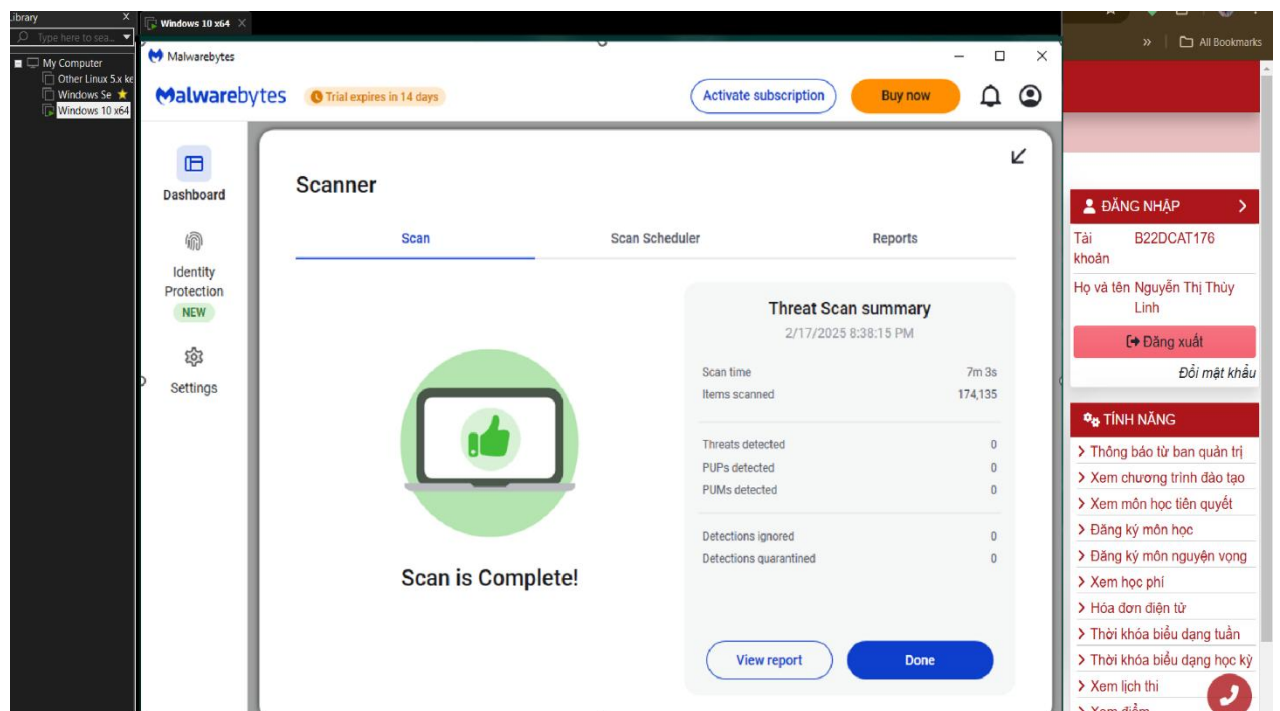


Hình ảnh 10 : Chạy thử phần mềm Spybot

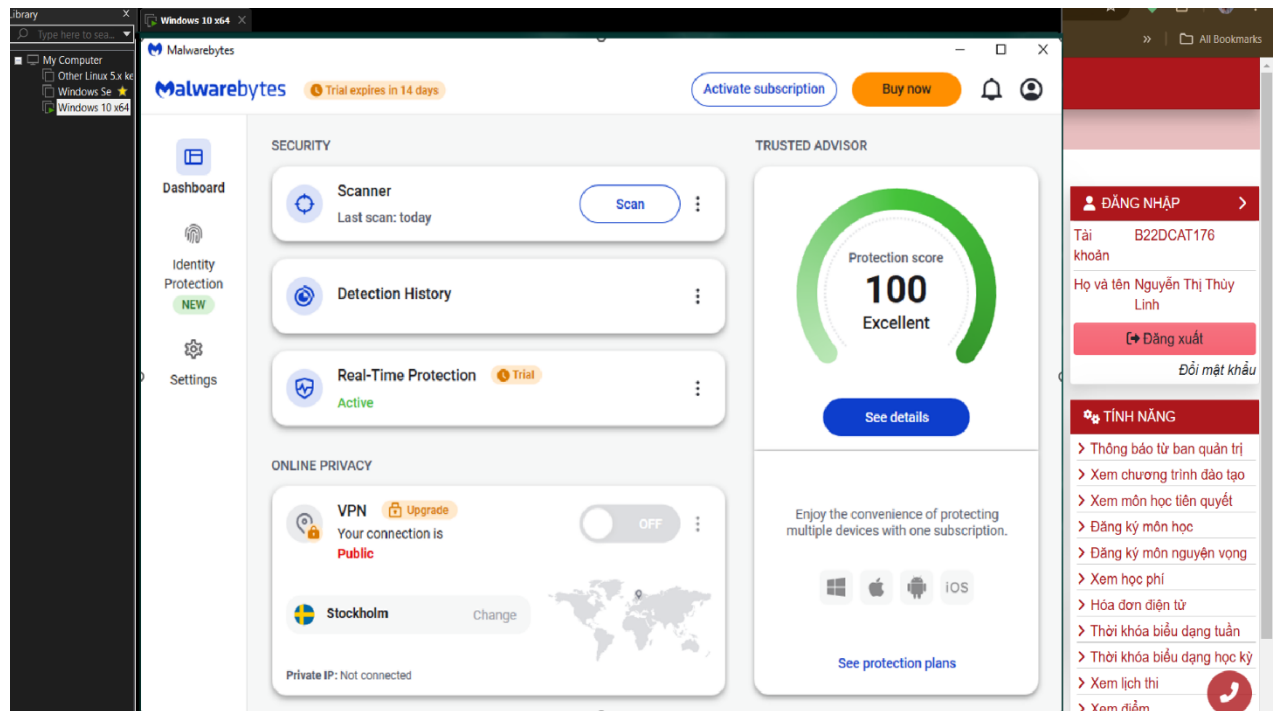
- Phần mềm chống các phần mềm độc hại Malwarebytes Anti-Malware
- Tải và sử dụng phần mềm chống các phần mềm độc hại



Hình ảnh 11 : Tải thành công phần mềm Malwarebytes

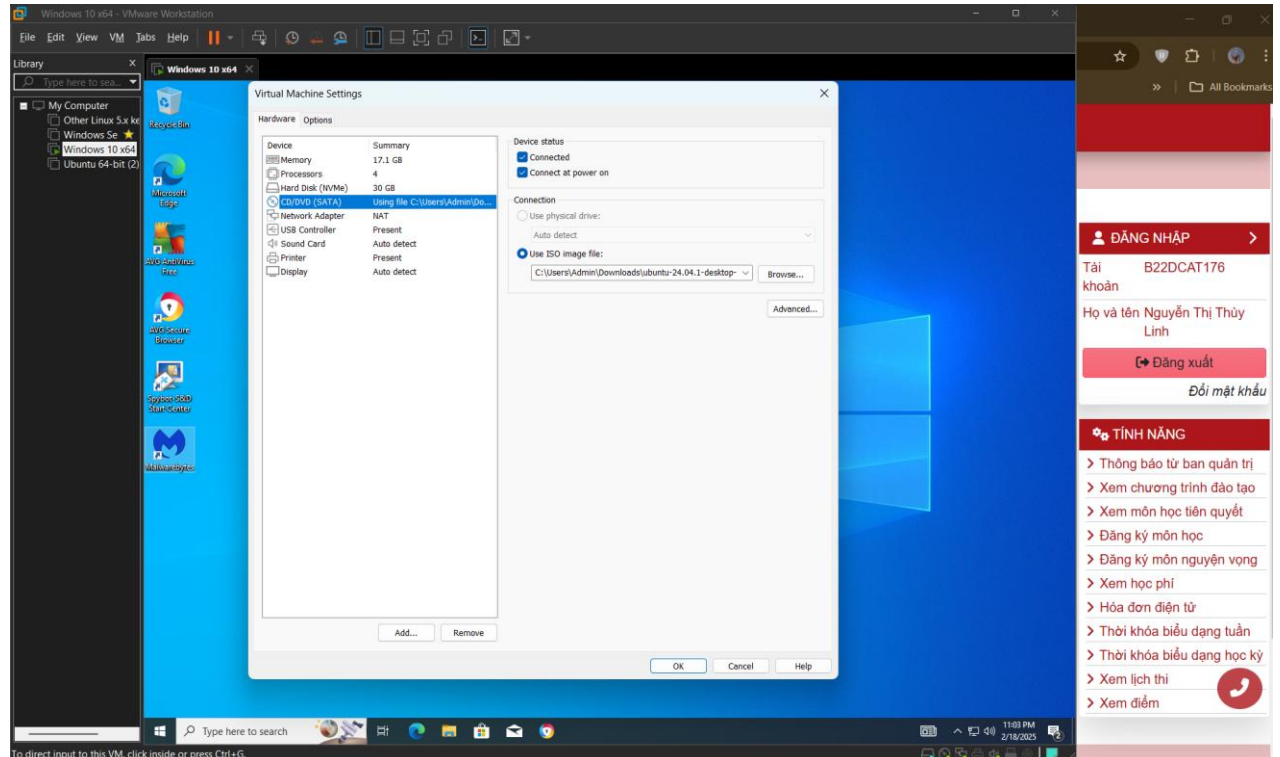


Hình ảnh 12 : Scanner trong Malwarebytes hoàn thành



Hình ảnh 13 : Thông tin về các lần quét trong Malwarebytes

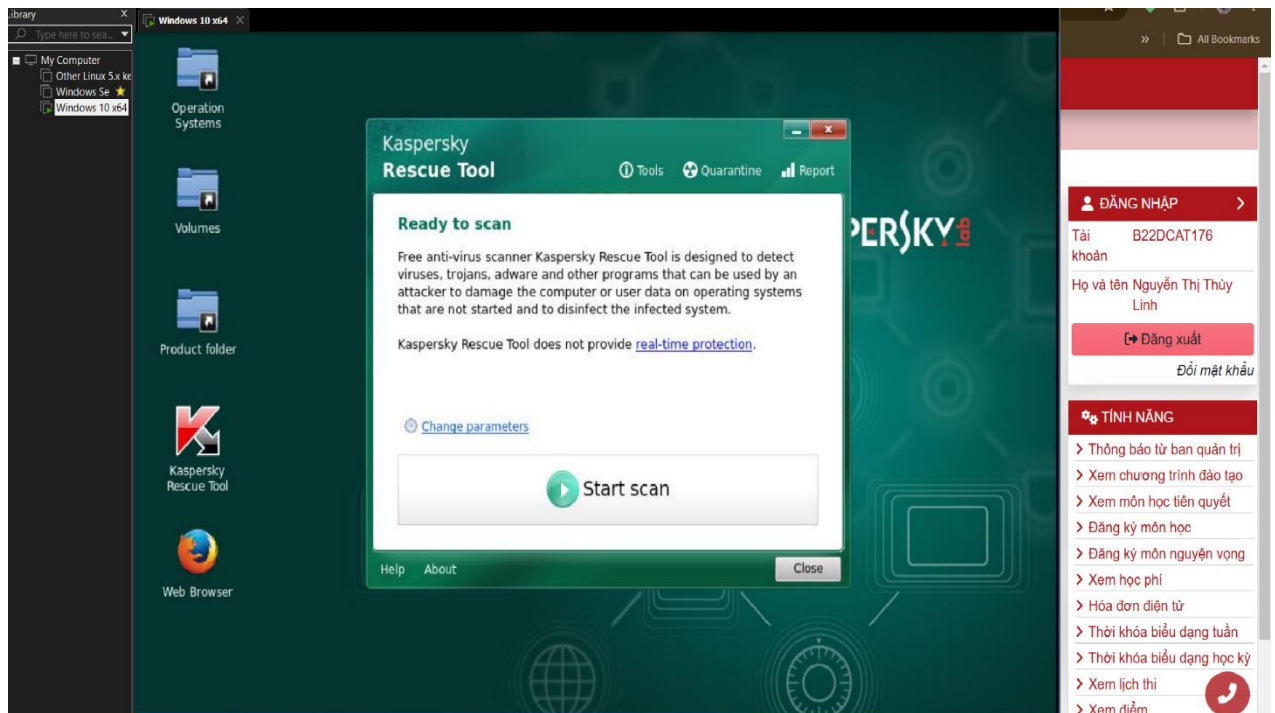
- Cài đặt Phần mềm cứu hộ: Kaspersky Rescue Disk (KRD)
  - Load phần mềm KRD dạng iso vào máy trạm



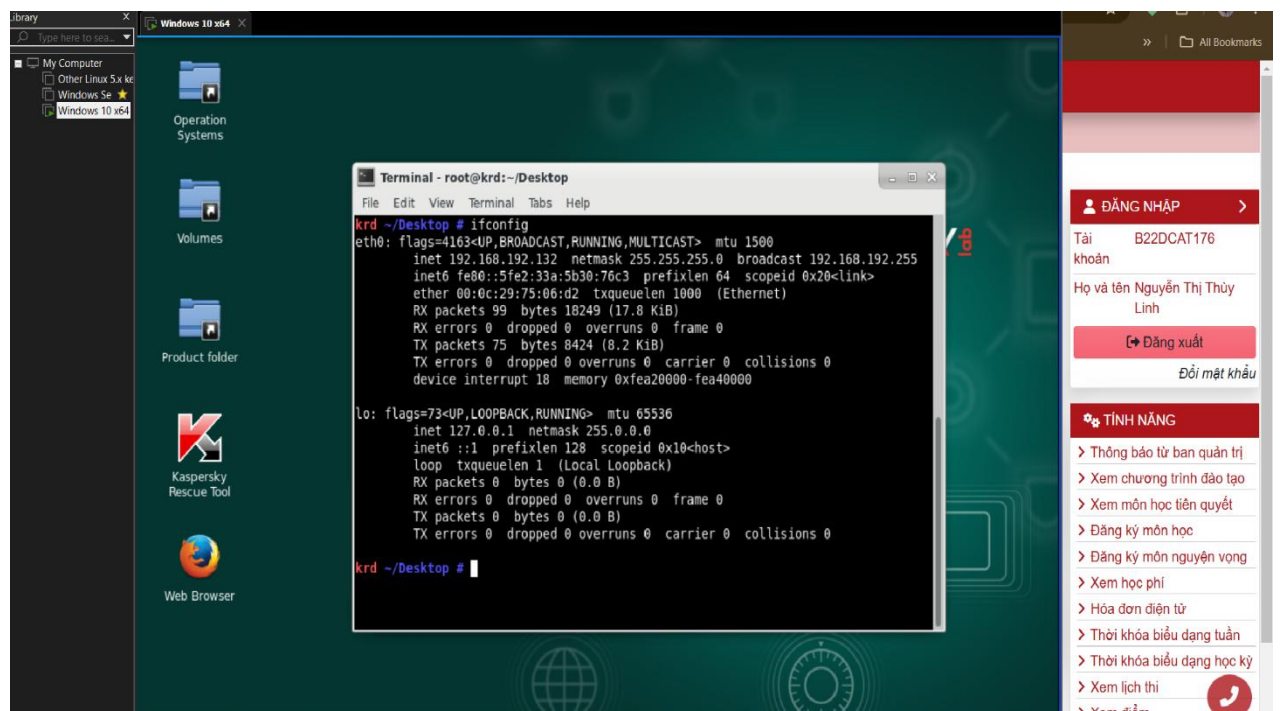
Hình ảnh 14 : Load iso vào máy trạm

- Giao diện của phần mềm

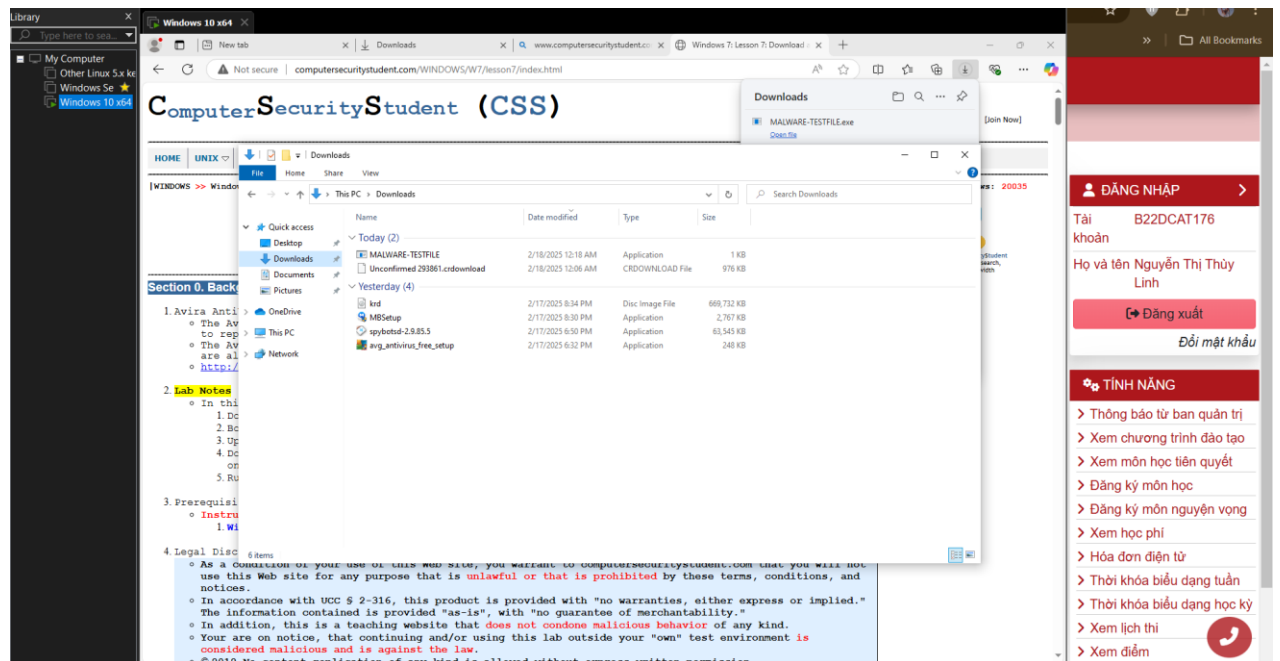




Hình ảnh 15 : Giao diện của phần mềm

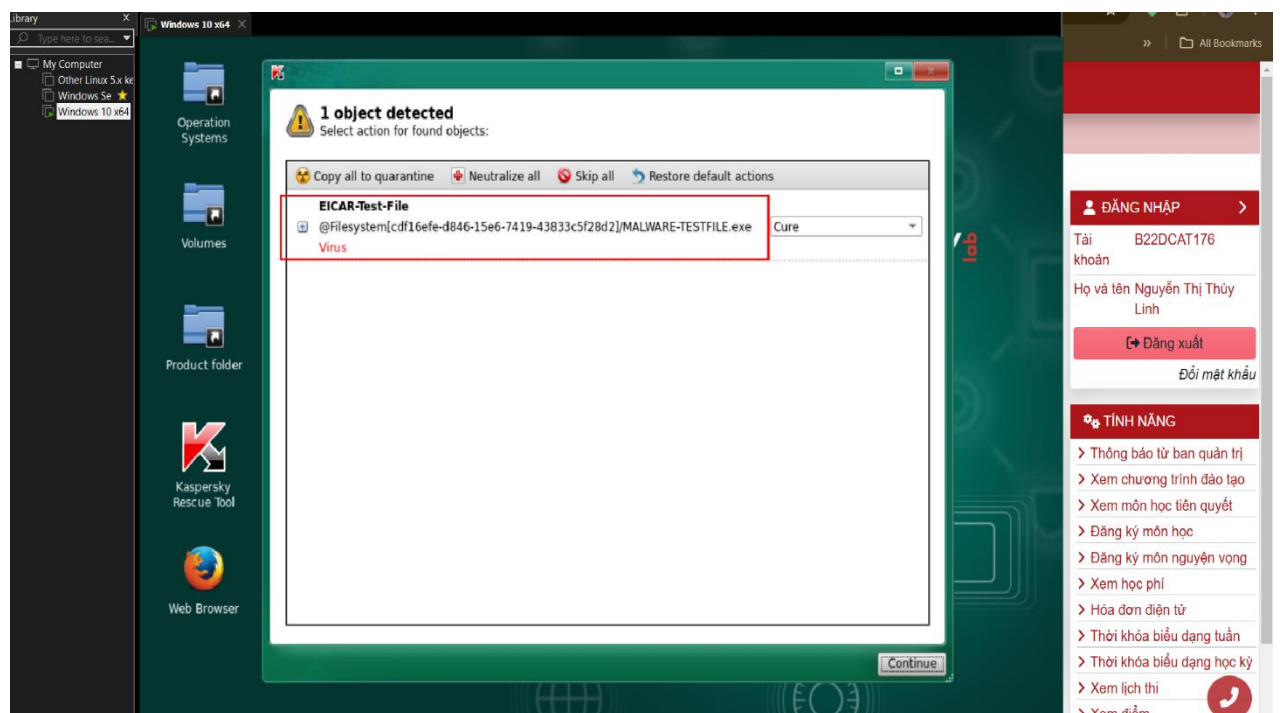


Hình ảnh 16 : Check ip của máy trạm



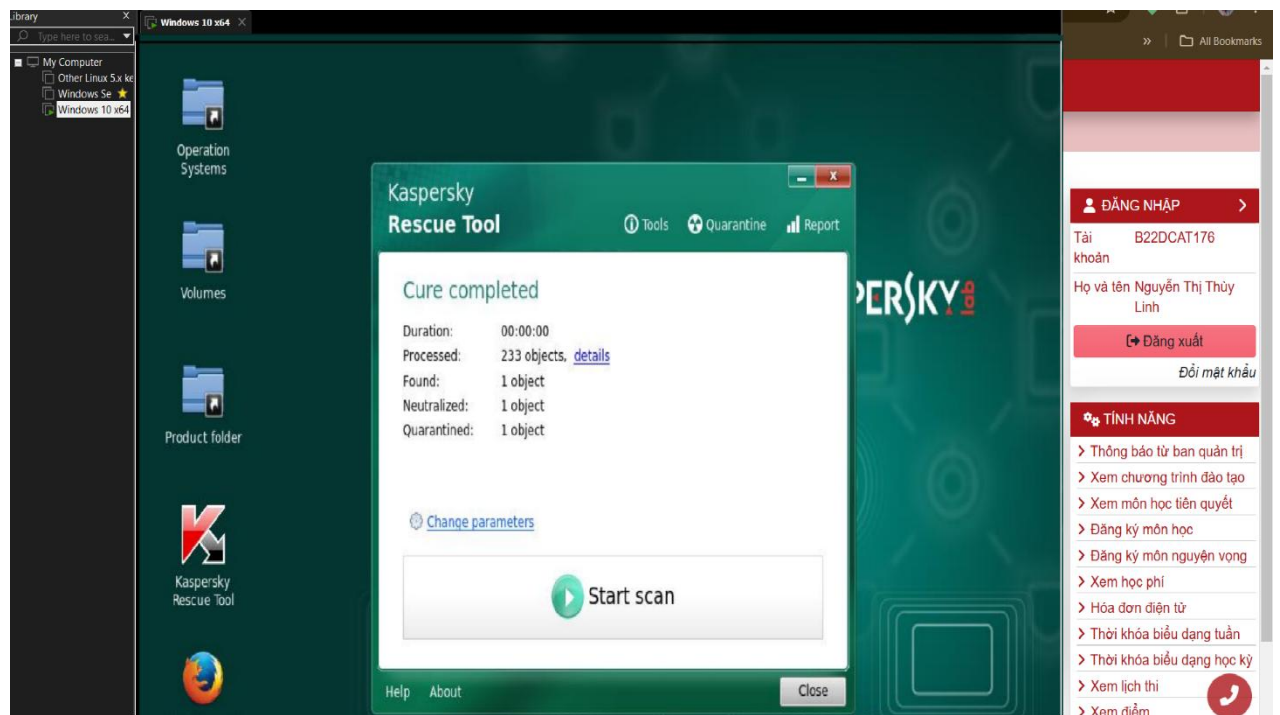
Hình ảnh 17 : Mã độc đã được tải xuống

- Chạy Kaspersky Rescue Tool, quét tất cả các thư mục, phát hiện file test mã độc và thực hiện xóa nó.



Hình ảnh 18 : Kết quả sau khi quét

- Quá trình quét kết thúc :



Hình ảnh 19 : Quá trình quét kết thúc

## **TÀI LIỆU THAM KHẢO**

- [1] Đinh Trường Duy, Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022.
- [2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.
- [3] Giáo trình Hệ điều hành