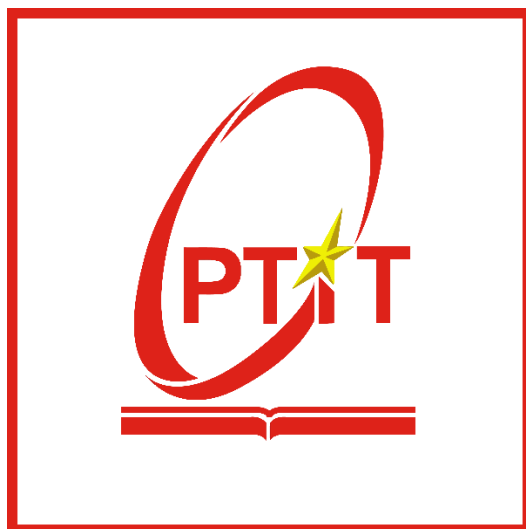


**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA AN TOÀN THÔNG TIN 1**



**Môn học: THỰC TẬP CƠ SỞ**  
**BÁO CÁO BÀI THỰC HÀNH SỐ 1**  
**CÀI ĐẶT HỆ ĐIỀU HÀNH MÁY TRẠM WINDOWS**

Sinh viên thực hiện: Lê Anh Tuấn

Mã sinh viên: B21DCAT205

Giảng viên: Ninh Thị Thu Trang

~ Hà Nội, tháng 1/2024 ~

# Mục Lục

<b>1</b>	<b>Mục đích .....</b>	<b>2</b>
<b>2</b>	<b>Nội dung thực hành .....</b>	<b>2</b>
2.1	Các phần mềm ảo hóa .....	2
2.1.1	VMWare Workstation .....	2
2.1.2	Vitual Box .....	3
2.2	Hệ điều hành Windows .....	4
2.2.1	Lịch sử .....	4
2.2.2	Kiến trúc .....	5
2.2.3	Giao diện .....	6
2.2.4	Đặc điểm, đặc trưng .....	7
2.3	Phần mềm diệt virus, chống phần mềm gián điệp, cứu hộ.....	7
2.3.1	Phần mềm diệt virus: AVG AntiVirus .....	7
2.3.2	Phần mềm chống phần mềm gián điệp Spybot S&D (Spybot – Search & Destroy) .....	8
2.3.3	Phần mềm chống các phần mềm độc hại: Malwarebytes Anti-Malware.....	8
2.3.4	Phần mềm cứu hộ: Kaspersky Rescue Disk (KRD) .....	9
<b>3</b>	<b>Kết quả thực hành .....</b>	<b>10</b>
3.1	Cài đặt thành công Windows 10 trên VMWare Workstation .....	10
3.2	Thực hiện cài đặt và chạy một số phần mềm bảo vệ máy trạm .....	11
3.2.1	Phần mềm diệt virus: AVG AntiVirus .....	11
3.2.2	Phần mềm chống phần mềm gián điệp Spybot S&D (Spybot – Search & Destroy) .....	13
3.2.3	Phần mềm chống các phần mềm độc hại: Malwarebytes Anti-Malware.....	14
3.2.4	Phần mềm cứu hộ: Kaspersky Rescue Disk (KRD) .....	16
<b>4</b>	<b>Kết luận.....</b>	<b>20</b>
<b>5</b>	<b>Tài liệu tham khảo .....</b>	<b>20</b>

# BÀI 1: Cài đặt hệ điều hành máy trạm Windows

## 1 Mục đích

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

## 2 Nội dung thực hành

### 2.1 Các phần mềm ảo hóa

#### 2.1.1 VMWare Workstation

VMware Workstation là phần mềm máy ảo được sử dụng cho máy tính x86 và x86-64 để chạy nhiều hệ điều hành trên một máy chủ vật lý. Mỗi máy ảo có thể chạy đồng thời một phiên bản duy nhất của bất kỳ hệ điều hành nào (Microsoft, Linux, v.v.). VMware Workstation hỗ trợ mạnh mẽ khả năng tương thích phần cứng và hoạt động như cầu nối giữa máy chủ và máy ảo cho tất cả các loại tài nguyên phần cứng bao gồm đĩa cứng, thiết bị USB và CD-ROM. Tất cả các trình điều khiển thiết bị được cài đặt thông qua máy chủ.

VMware Workstation cho phép cài đặt nhiều phiên bản của các hệ điều hành khác nhau, bao gồm cả hệ điều hành máy khách và máy chủ. Nó giúp quản trị viên mạng hoặc hệ thống kiểm tra, kiểm tra và xác minh môi trường máy chủ của khách hàng. Quản trị viên cũng có thể chuyển đổi giữa các máy ảo khác nhau cùng một lúc.

VMware cung cấp cho người dùng rất nhiều lợi ích như:

- **Chi phí (Cost):** VMware là một lựa chọn hiệu quả về mặt giá cả, được khuyến khích nhất cho các giải pháp điện toán đám mây, điều này khiến cho việc mua phần mềm VMware không phải là vấn đề lớn đối với một doanh nghiệp quy mô lớn.
- **Dự phòng (Redundancy):** VMware được sử dụng để thêm và xóa các máy ảo. Có thể đôi khi gặp phải sự cố mất dữ liệu hoặc hỏng tệp. Các phương pháp khôi phục dữ liệu khôi phục nhanh được bao gồm trong VMware cho phép khôi phục các tệp đã sửa đổi hoặc bị xóa.
- **Khả năng mở rộng (Scalability):** Có thể dễ dàng thêm nhiều máy ảo bằng các công cụ VMware. Quá trình triển khai máy ảo cũng trở nên dễ dàng hơn chỉ với vài bước đơn giản.
- **Tính linh hoạt (Flexibility):** VMware có thể được sử dụng để thử nghiệm nhiều mục đích khác nhau. Nó cung cấp một môi trường an toàn để người dùng kiểm tra các bản cập nhật và bản vá trước khi thực sự cài đặt chúng trên máy tính vật lý. Hơn nữa, một phần mềm không đáng tin cậy có thể được sử dụng ở đây để ngăn chặn phần mềm độc hại và các loại mối đe dọa khác.

- **Hỗ trợ nhiều hệ điều hành (Multiple OS Support):** Một máy chủ cụ thể trong VMware có thể được sử dụng để quản lý nhiều hệ điều hành. Kiểu thiết lập này đảm bảo quản lý tài nguyên tốt hơn. Hơn nữa, mỗi hệ điều hành đều được phép truy cập cùng một lúc.

Bên cạnh đó VMware Workstation có những hạn chế, bao gồm hỗ trợ phần cứng, sự cố hệ điều hành và các rào cản về giao thức mạng.

- **Hiệu suất (Performance):** VMware chỉ có thể mang lại hiệu suất tốt nhất cho các hệ thống có thiết bị cao cấp. Vì vậy, không thể đạt được hiệu suất mong muốn đối với các hệ thống có cấu hình thấp hơn. Điều này là do VMware hoàn toàn phụ thuộc vào tài nguyên hệ thống. Trên thực tế, rất khó có thể dự đoán hệ thống sẽ hoạt động như thế nào với các tài nguyên hiện có.
- **Độ tin cậy (Reliability):** Vì việc sử dụng các thiết bị vật lý được bao gồm trong VMware nên luôn có mối lo ngại về độ tin cậy. Các thiết bị vật lý được kết nối cũng phải mang lại hiệu suất như nhau, nếu không có thể xảy ra một số vấn đề khác. Do những vấn đề như thế này mà không thể dự đoán chính xác độ tin cậy của phần mềm VMware.
- **Khả năng tương thích phần cứng (Hardware Compatibility):** Luôn có vấn đề tương thích phần cứng trong VMware. Để triển khai VMware, hệ thống cần đáp ứng các yêu cầu phần cứng nhất định. Nếu không, hệ thống không thể đạt được hiệu suất như mong đợi. Về cơ bản, VMware yêu cầu bộ xử lý 64bit x86, 4GB RAM vật lý (Tùy thuộc vào loại máy ảo), ít nhất 1GB bộ điều khiển Ethernet.
- **Khắc phục sự cố (Troubleshooting):** Một hệ thống ảo hóa hoạt động hoàn toàn khác với một máy trạm thông thường. Khắc phục sự cố trong môi trường ảo hóa như VMware không phải là một quá trình dễ dàng. Ngay cả việc tìm ra nguyên nhân của vấn đề cũng trở nên khó khăn.

### 2.1.2 Virtual Box

VirtualBox là sản phẩm ảo hóa x86 và AMD64/Intel64 mạnh mẽ dành cho doanh nghiệp cũng như gia đình. VirtualBox không chỉ là một sản phẩm cực kỳ giàu tính năng, hiệu suất cao dành cho khách hàng doanh nghiệp mà còn là giải pháp chuyên nghiệp duy nhất được cung cấp miễn phí dưới dạng phần mềm mã nguồn mở.

Hiện tại, VirtualBox chạy trên các máy chủ Windows, Linux, macOS và Solaris và hỗ trợ một số lượng lớn hệ điều hành khách bao gồm nhưng không giới hạn ở Windows (NT 4.0, 2000, XP, Server 2003, Vista, 7, 8, Windows 10 và Windows 11), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x, 4.x, 5.x và 6.x), Solaris và OpenSolaris, OS/2, OpenBSD, NetBSD và FreeBSD.

## Một số ưu điểm của VirtualBox

- **Khả năng tương thích:** VirtualBox tương thích trên hầu hết các hệ điều hành 32 bit và 64 bit hiện nay.
- **Không yêu cầu phần cứng ảo hóa:** có thể chạy phần mềm này trên các phần cứng đời cũ và các phần cứng không hỗ trợ tính năng ảo hóa.
- **Đa xử lý (multiprocessing):** VirtualBox có thể xử lý tối đa 32 CPU cho mỗi máy ảo.
- **Tương thích phần cứng:** VirtualBox hỗ trợ hầu hết các thiết bị, bao gồm trình điều khiển ổ cứng IDE, SCSI và SATA, card mạng ảo, card âm thanh ảo.
- **Khôi phục:** có thể khôi phục hiện trạng của máy ảo về trạng thái trước đó nếu như máy ảo xảy ra lỗi.

## 2.2 Hệ điều hành Windows

### 2.2.1 Lịch sử

- **MS-DOS**
  - Hệ thống điều khiển đĩa
  - Giao diện dòng lệnh
  - Cấu hình tiêu biểu: CPU 286 8MHz, 640KB RAM, 1.44MB ổ đĩa mềm, màn hình VGA (640x480), bàn phím
  - Hệ thống file FAT-12, FAT-16.
- **Windows 3.1**
  - Giao diện đồ họa: Cửa sổ, Menu, Chuột
  - Sử dụng quản lý chương trình (program manager)
  - Hệ thống file FAT 16
  - Chạy trên nền DOS
- **Windows NT**
  - Giao diện đồ họa
  - Sử dụng kiến trúc 32bit
  - Hỗ trợ mạng
  - Hướng tới người dùng chuyên nghiệp
  - Hệ thống file NTFS
  - Không dựa trên DOS
- **Windows XP**
  - Hỗ trợ mạng Wi-Fi và các thiết bị USB
  - Firewall, hỗ trợ truy nhập từ xa, cập nhật qua mạng.
  - Hướng tới người dùng chuyên nghiệp
  - Hệ thống file NTFS

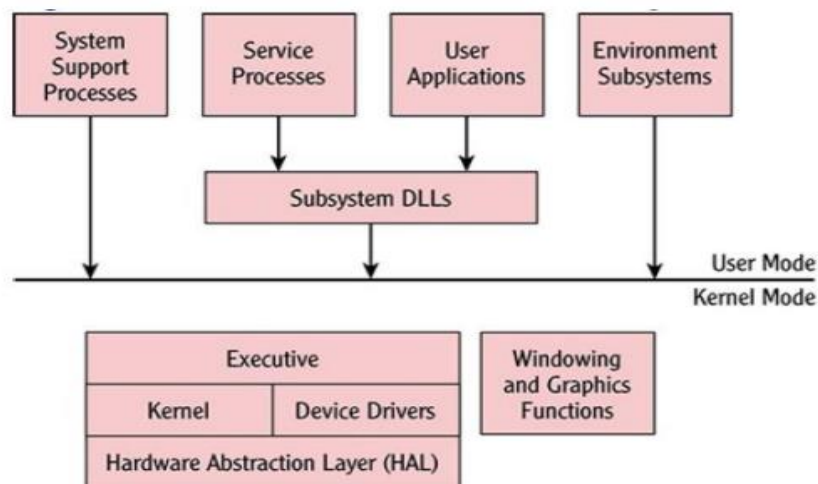
- Kích hoạt trước khi sử dụng
- Hỗ trợ đa phương tiện

### Lịch sử phát triển

1981-1991	1992-1994	2001-2009
DOS	Windows 3.1	Windows XP
<ul style="list-style-type: none"> <li>- Máy PC cơ bản</li> <li>- Bộ nhớ nhỏ KB (640KB)</li> <li>- Ổ đĩa (ổ mềm) nhỏ (KB-MB)</li> </ul>	<ul style="list-style-type: none"> <li>- Máy PC với nhiều thiết bị</li> <li>- Bộ nhớ lớn MB (tối đa 32MB)</li> <li>- Ổ cứng nhỏ (KB-MB)</li> </ul>	<ul style="list-style-type: none"> <li>- Giao diện cải tiến</li> <li>- Bộ nhớ lớn (&gt;512MB)</li> <li>- Các thiết bị USB và kết nối Wi-Fi</li> </ul>

### 2.2.2 Kiến trúc

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



- **User mode:** chế độ người dùng chạy các chương trình của người dùng (như word, excel...).
- *System Support Processes (Chương trình hỗ trợ hệ thống):* Các chương trình thực hiện các chức năng hệ thống như đăng nhập, quản lý phiên làm việc.
- *Service Processes (Các chương trình dịch vụ):* Các chương trình cung cấp dịch vụ của hệ điều hành như quản lý máy in, tác vụ.

- *User Applications (Ứng dụng người dùng)*: Các chương trình thực hiện theo yêu cầu của người dùng.
- *Environment Subsystems (Các hệ thống con)*: Kết hợp với hệ thống liên kết động cho phép các kiểu ứng dụng khác nhau hoạt động được. VD: Win32, Win64, DOS32.
- *Subsystem DLL (hệ thống liên kết động)*: Chuyển các hàm ứng dụng thành các hàm dịch vụ hệ thống trực tiếp.
- **Kernel mode**: chế độ nhân dùng thực hiện các chức năng quản lý truy nhập phần cứng.
- *Executive (Thực thi)*: Thực hiện việc quản lý các tiến trình và luồng, quản lý bộ nhớ, vào/ra ...
- *Kernel (nhân)*: Điều độ luồng, đồng bộ giữa các tiến trình, xử lý ngắt.
- *Device Drivers (các trình điều khiển thiết bị)*: Giao tiếp với quản lý vào/ra.
- *Hardware Abstraction Layer - HAL (Lớp phần cứng trừu tượng)*: Ẩu đi các chi tiết phần cứng giúp cho hệ điều hành có thể hoạt động trên nhiều phần cứng khác nhau.
- *Windowing and Graphics Functions (Các chức năng cửa sổ và đồ họa)*: Cung cấp giao diện đồ họa cho người dùng.

### 2.2.3 Giao diện

Hệ điều hành Windows có ba cách giao tiếp chính giúp làm việc với các ứng dụng và thực hiện các công việc quản trị. Hầu hết người dùng thông thường sử dụng GUI song người quản trị lại được lợi hơn từ giao diện dòng lệnh và Windows PowerShell.

- *Giao diện đồ họa GUI*: Bao gồm các cửa sổ, nút bấm, hộp văn bản và các phần tử định hướng khác. Menu khởi động (Start) cho phép người quản trị truy nhập vào tất cả các chức năng của hệ điều hành cũng như các chương trình người quản trị. Thanh tác vụ (Taskbar) cho phép truy nhập nhanh đến các ứng dụng và cho biết tình trạng của các chương trình người quản trị. Màn hình làm việc (desktop) là nơi chứa các biểu tượng các chương trình người dùng hay hệ thống hoặc các chương trình tiện ích như tra cứu thông tin thời tiết, chứng khoán... Khi các chương trình người dùng chạy, chúng sử dụng không gian này để hiển thị thông tin cho người dùng.
- *Giao diện dòng lệnh*: Giao diện này là giao diện xưa nhất của Microsoft đó chính là dòng lệnh DOS. 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. Thông qua giao diện này người dùng có thể thực thi các thao tác cấu hình cho hệ điều hành hay chạy các chương trình DOS cũ.

- *Giao diện PowerShell*: Giao diện dòng lệnh mới hỗ trợ công việc quản trị. Cung cấp ngôn ngữ lập trình (scripting language). Có thể cung cấp các tập lệnh định trước (cmdlet) để thuận tiện cho việc quản lý. Hỗ trợ xuất dữ liệu trực tiếp (pipeline).

#### 2.2.4 Đặc điểm, đặc trưng

- **Đặc điểm**
  - Khả năng tương thích cao
  - Dễ sử dụng
  - Tính năng bảo mật được nâng cấp thường xuyên
  - Kho ứng dụng phong phú.
  - Hỗ trợ tối đa cho các thiết bị cảm ứng.
- **Đặc trưng**
  - Các chương trình Windows có diện mạo và cách hoạt động giống nhau
  - Các lệnh và hệ thống menu tương tự
  - Chạy nhiều chương trình cùng lúc
  - Chuyển đổi giữa các trình ứng dụng đang mở
  - Windows Clipboard
  - Đa tác vụ: thực hiện nhiều việc cùng lúc

### 2.3 Phần mềm diệt virus, chống phần mềm gián điệp, cứu hộ

#### 2.3.1 Phần mềm diệt virus: AVG AntiVirus

- **Khái niệm**
  - AVG AntiVirus là một phần mềm diệt virus và bảo mật máy tính được phát triển bởi AVG Technologies. Nó cung cấp một tập hợp các tính năng bảo mật và diệt virus để giúp bảo vệ máy tính khỏi các mối đe dọa an toàn và giúp bảo vệ dữ liệu cá nhân. AVG AntiVirus có thể chạy trên nhiều hệ điều hành, bao gồm Windows, MacOS và Android. Nó cung cấp các tính năng như quét virus, diệt spyware, bảo vệ email, chống lạc đường, v.v. để giúp bảo vệ máy tính một cách hiệu quả và an toàn.
- **Các tính năng của AVG Antivirus**
  - Bảo vệ PC trong thời gian thực trước các mối đe dọa về bảo mật và quyền riêng tư với công cụ quét vi rút Cyber Capture mạnh mẽ.
  - Chế độ bị động cho phép chạy 2 công cụ bảo vệ cùng lúc.
  - Cải thiện khả năng bảo vệ trực tuyến bằng cách quét các trang web, liên kết và tải xuống để bảo vệ người dùng.
  - Kiểm tra hiệu suất và quét vi rút miễn phí với AVG TuneUp.
  - Giao diện được thiết kế mới mẻ và trực quan.
  - Khắc phục hiện tượng BSOD (màn hình xanh) trong quá trình quét AntiRootkit.



- Đã thêm hỗ trợ cho danh sách trắng / đen của AntiSpam dưới dạng địa chỉ email và miền.

- Khắc phục sự cố hoặc treo hệ thống khi thực hiện chức năng giả lập Script.

### 2.3.2 Phần mềm chống phần mềm gián điệp Spybot S&D (Spybot – Search & Destroy)

- **Khái niệm**

- SpyBot - Search & Destroy là một công cụ chống phần mềm gián điệp miễn phí và mạnh mẽ, giúp bảo vệ thiết bị khỏi các mối đe dọa trực tuyến.

- **Hoạt động**

- 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 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.

- **Những tính năng của SpyBot - Search & Destroy**

- *Cung cấp nhiều lợi ích* : SpyBot bảo vệ người dùng chống lại nhiều loại phần mềm gián điệp, bao gồm keylogger, phần mềm quảng cáo, cookie theo dõi và các cuộc tấn công phần mềm độc hại. Nó chạy trong nền để bảo vệ chống lại các vi phạm quyền riêng tư và những cuộc tấn công mạng.
- *Giao diện thân thiện với người mới bắt đầu*
- *Vận hành tự động và thủ công*: Với tự động, chương trình sẽ đảm nhận tất cả các chức năng, bao gồm chạy quét nền và xóa phần mềm không mong muốn. Còn nếu như tự động thì có thể tùy chỉnh một loạt các hoạt động của chương trình.
- *Nhiều tùy chọn quét*: quét sâu, quét nhanh.
- *Tính năng quét bổ sung*: là một bản quét định vị rootkit
- *Chặn các trang web nguy hiểm*: chặn quyền truy cập vào các trang web nguy hiểm, cũng như những plugin và cookie lấy cắp thông tin. Một tính năng thiết yếu khác có trong phiên bản miễn phí của ứng dụng là xóa dấu vết trực tuyến, bao gồm lịch sử trình duyệt, ứng dụng, cookie và các file đã mở
- *Kiểm soát khởi động hệ thống*: quản lý các ứng dụng load khi máy tính khởi động

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

- **Khái niệm**

- MalwareBytes là công cụ phát hiện và loại bỏ phần mềm độc hại được cung cấp miễn phí và cũng có phiên bản cao cấp bổ sung một số tính năng quan trọng. Nó có khả năng phát hiện và loại bỏ tất cả các loại phần mềm độc hại, bao gồm phần mềm

gián điệp, trojan, worm và thậm chí cả ransomware. Phiên bản cao cấp bao gồm bảo vệ thời gian thực có thể xác định các mối đe dọa ngay khi chúng xuất hiện.

- **Tính năng**

- *Bảo vệ thời gian thực (Real-Time Protection)*: Phần mềm bảo mật này có tính năng bảo vệ thời gian thực mạnh mẽ, phát hiện các cuộc tấn công zero-day và các thực thể độc hại khác đang bị tội phạm mạng khai thác. Tính năng này tự hào có bốn lớp bảo vệ đồng thời, đó là bảo vệ phần mềm độc hại, bảo vệ ransomware, bảo vệ web và bảo vệ khai thác. Tất cả các lớp này chạy đồng thời và đóng vai trò là nền tảng của phần mềm.
- *Quét nhiều lần (Multiple Scanning)*: Threat Scan giúp kiểm tra các khu vực thường bị nhiễm, chẳng hạn như sổ đăng ký và bộ nhớ. Hyper Scan kiểm tra các đối tượng khởi động và bộ nhớ xem có bất kỳ dấu hiệu lây nhiễm nào không. Custom Scan cho phép chọn các khu vực cụ thể trên hệ thống muốn quét.
- *Cập nhật cơ sở dữ liệu tự động (Automatic Database Update)*: Phần mềm tập hợp các mẫu của bất kỳ thực thể đáng ngờ nào từ hệ thống của người dùng. Các mẫu này sau đó được phân tích và đánh giá để tạo ra các bản cập nhật mới. Phiên bản cao cấp của phần mềm thường được cập nhật hàng giờ. Tuy nhiên có thể điều chỉnh tần suất cập nhật.
- *Hiệu suất nhanh và gọn nhẹ*: Nó có khả năng quét các thông tin cơ bản chỉ trong vài phút và đủ nhẹ để không thấy hệ thống thử nghiệm gặp phải bất kỳ ảnh hưởng nào về hiệu suất. Việc quét nhiều vị trí bổ sung mất nhiều thời gian hơn nhưng vẫn không tiêu tốn tài nguyên hệ thống.

#### 2.3.4 Phần mềm cứu hộ: Kaspersky Rescue Disk (KRD)

- **Khái niệm**

Kaspersky Rescue Disk được thiết kế để quét và khử trùng các máy tính tương thích x86 và x64 đã bị nhiễm virus. Nên sử dụng ứng dụng khi mức độ lây nhiễm ở mức độ không thể khử trùng máy tính bằng các ứng dụng chống vi-rút hoặc tiện ích loại bỏ phần mềm độc hại chạy trong hệ điều hành. Trong trường hợp này, việc khử trùng hiệu quả hơn vì các chương trình phần mềm độc hại không giành được quyền kiểm soát khi hệ điều hành đang được tải.

- **Tính năng**

- Dễ sử dụng, và có giao diện tiêu chuẩn và trực quan hấp dẫn.
- Dễ dàng chạy quét và cập nhật, có thể quét một phần ổ cứng thay vì toàn bộ.
- Có thể sử dụng công cụ này để sao chép các tệp quan trọng ra khỏi ổ đĩa nếu tình trạng nhiễm vi-rút quá nghiêm trọng để khắc phục.
- Đĩa cứu hộ sẽ lập báo cáo kết quả quét
- Bất kỳ tệp bị nhiễm nào cũng có thể được cách ly, khử trùng hoặc xóa.

- Cho phép quét các tập tin/thư mục cụ thể, vì vậy không cần phải quét tất cả các loại tệp, tránh lãng phí thời gian.
- Hỗ trợ các tùy chọn quét nâng cao hơn

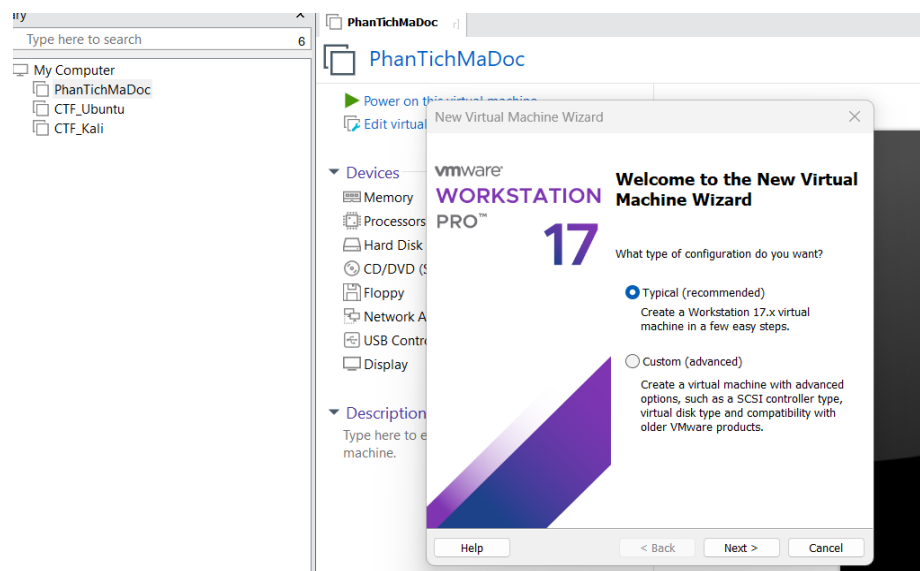
### 3 Kết quả thực hành

#### 3.1 Cài đặt thành công Windows 10 trên VMWare Workstation

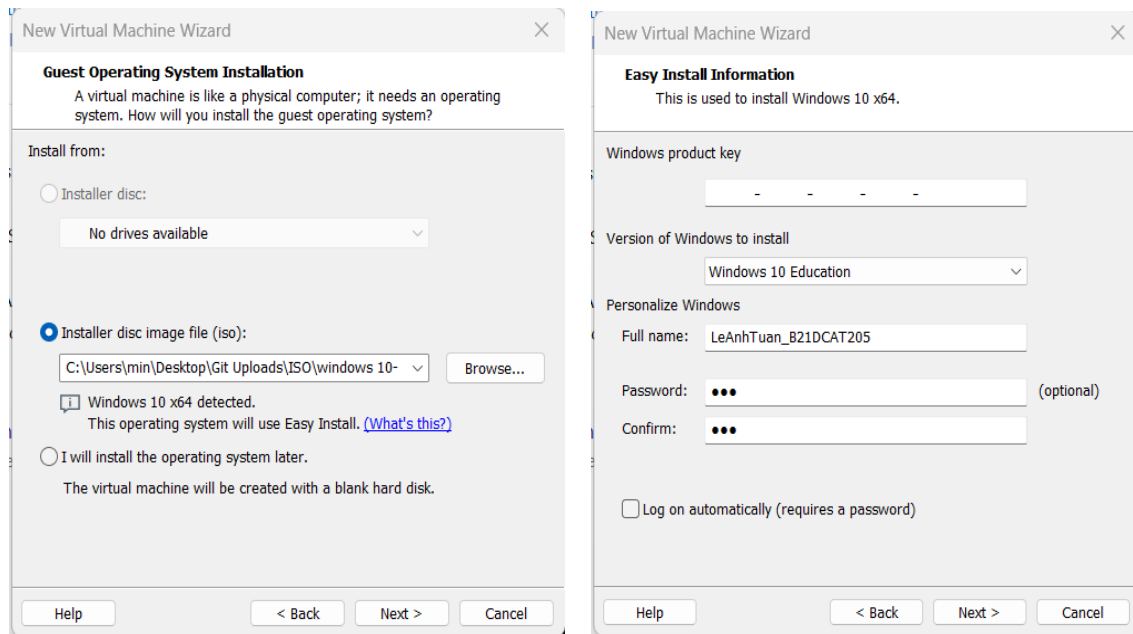
**Bước 1:** Chuẩn bị file ISO.

windows 10- 64bit 21/1/2024 2:22 pm Disc Image File 5,420,408 ...

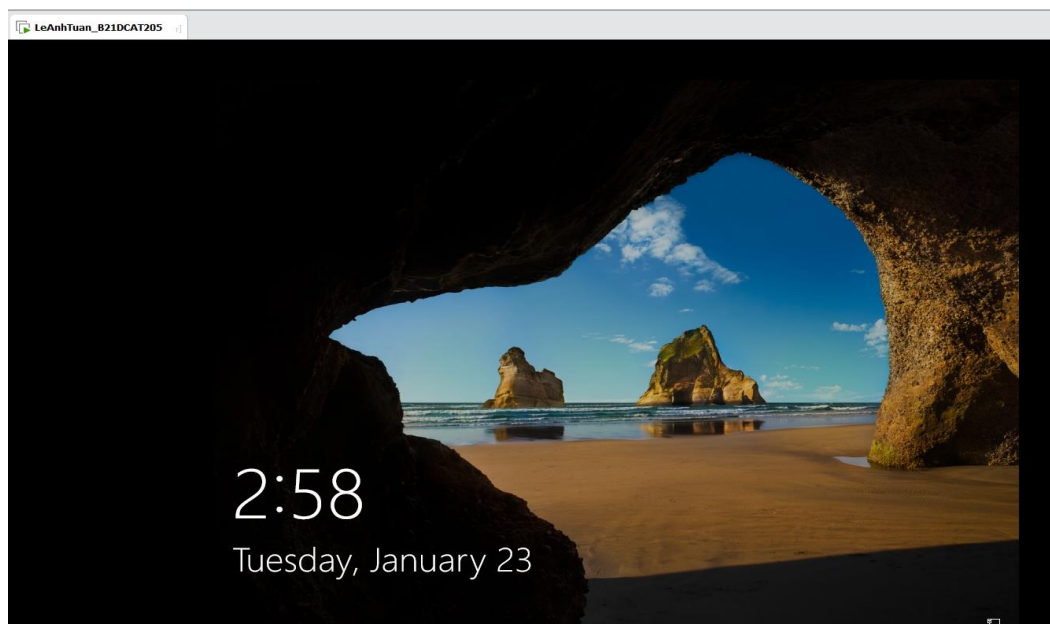
**Bước 2:** Tiến hành tạo máy ảo và sử dụng file ISO đã chuẩn bị



Chọn Typical -> Next, sử dụng file ISO đã chuẩn bị



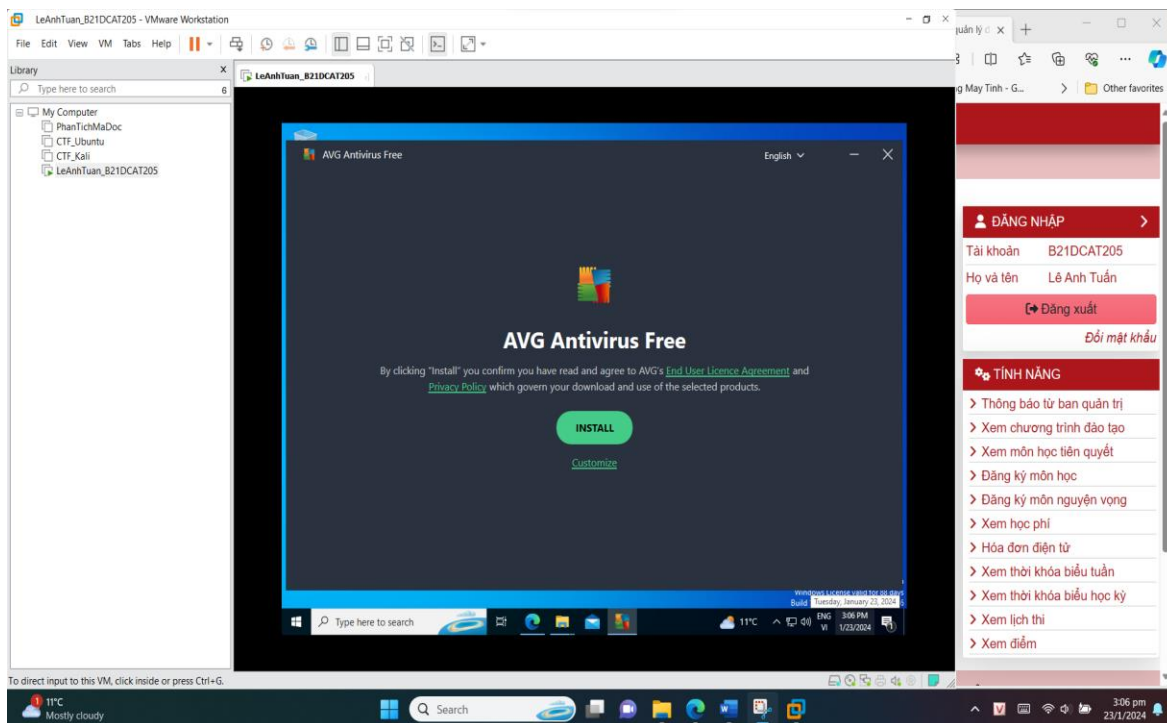
⇒ Cài đặt máy trạm Windows 10 thành công



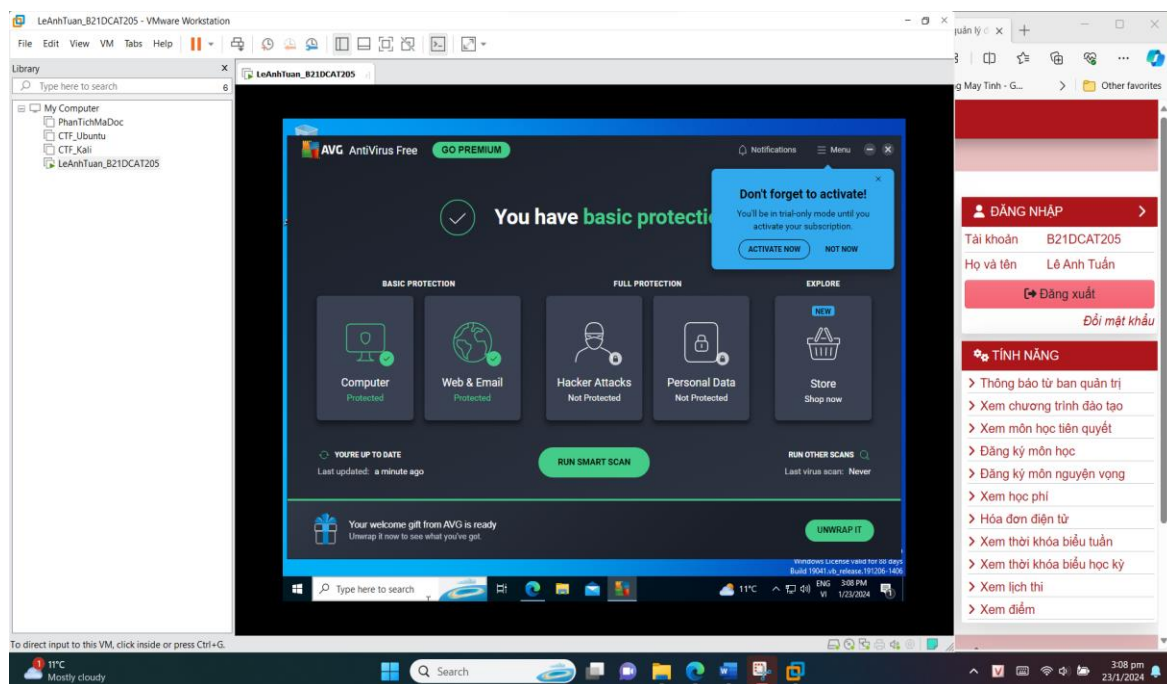
## 3.2 Thực hiện cài đặt và chạy một số phần mềm bảo vệ máy trạm

### 3.2.1 Phần mềm diệt virut: AVG AntiVirus

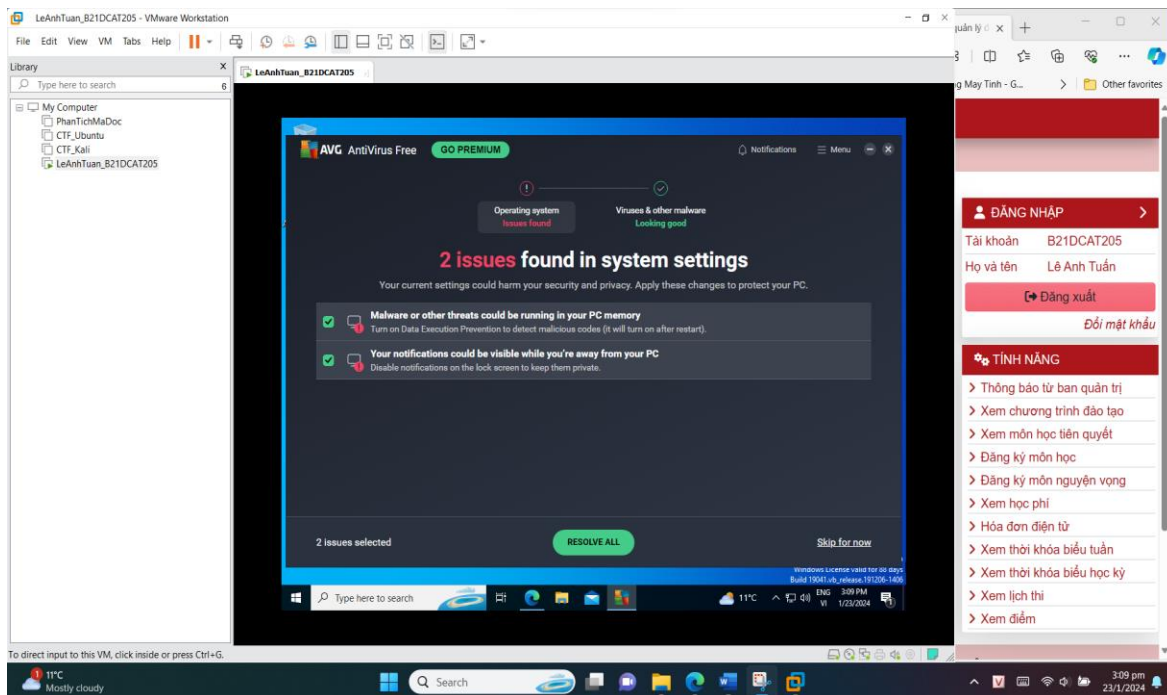
**Bước 1:** Kích hoạt file cài đặt đã tải về và tiến hành cài đặt



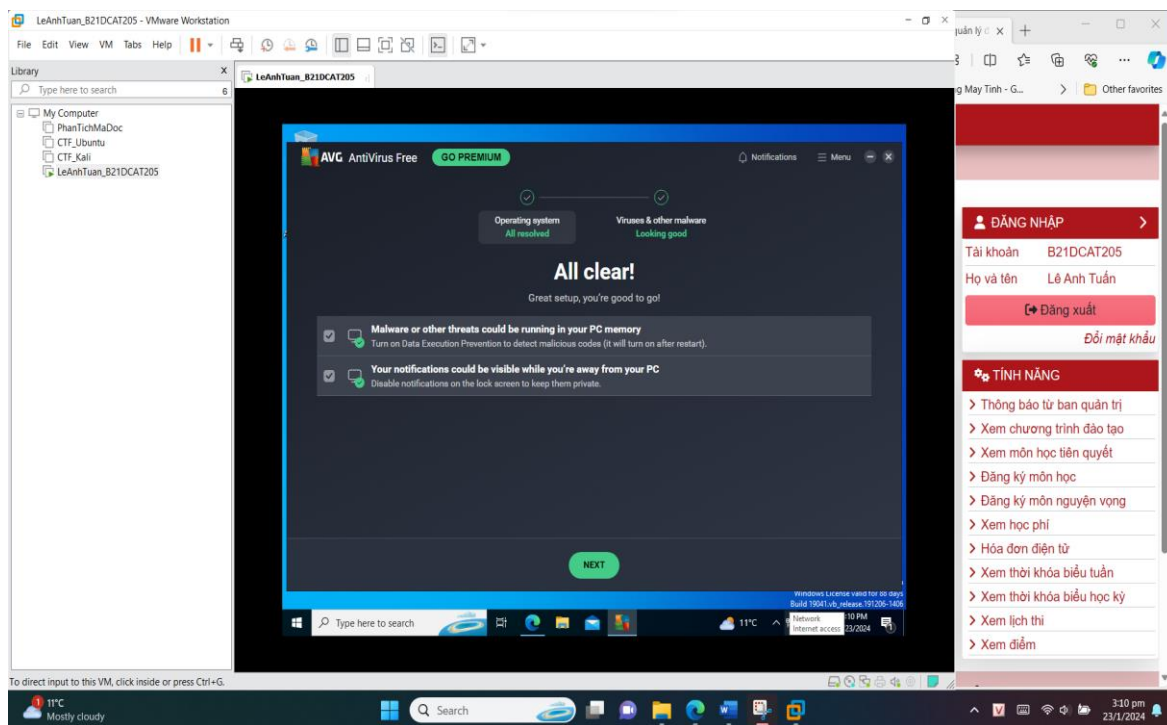
**Bước 2:** Click Install → Hoàn tất cài đặt



**Bước 3:** Click Run Smart Scan → Kết quả thu được



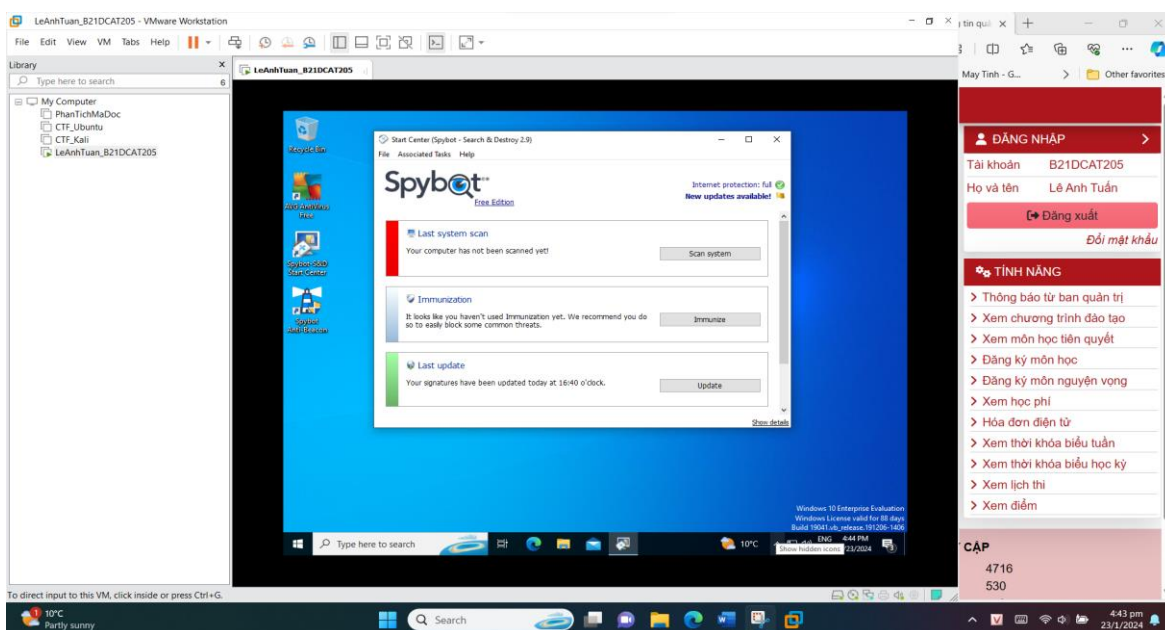
#### Bước 4: Nhấn RESOLVE ALL để giải quyết các vấn đề gặp phải



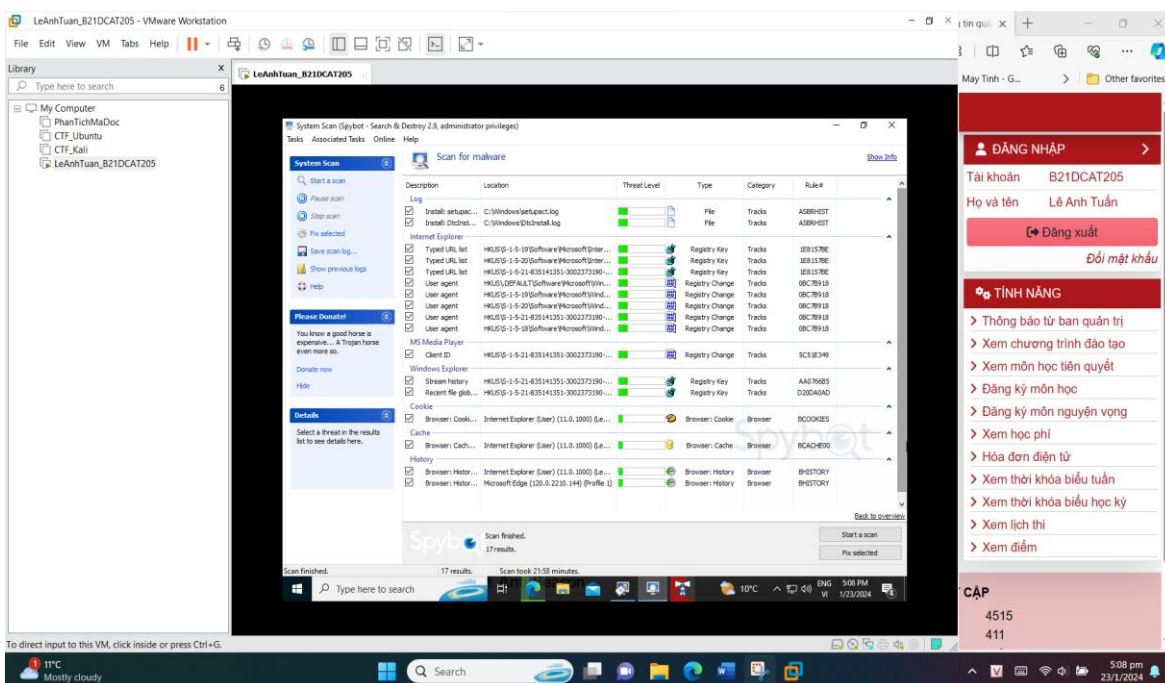
### 3.2.2 Phần mềm chống phần mềm gián điệp Spybot S&D (Spybot – Search & Destroy)



Khởi chạy file cài đặt đã tải, Scan system để bắt đầu quét

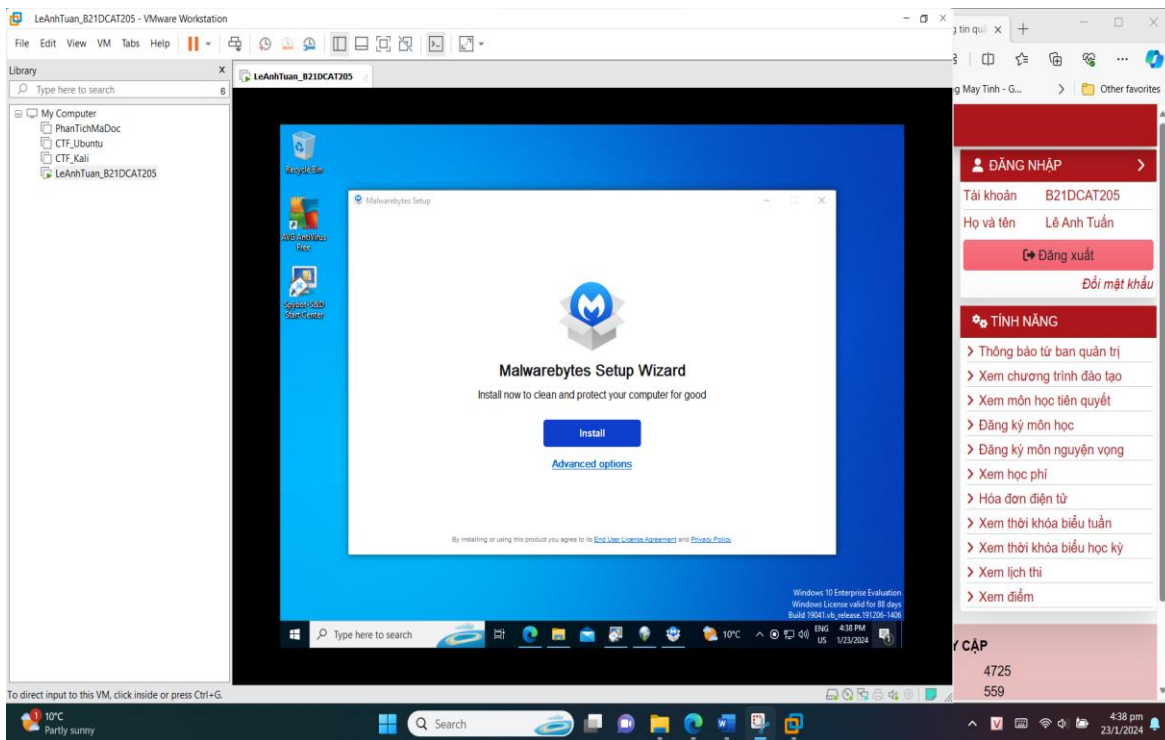


Kết quả sau khi quét

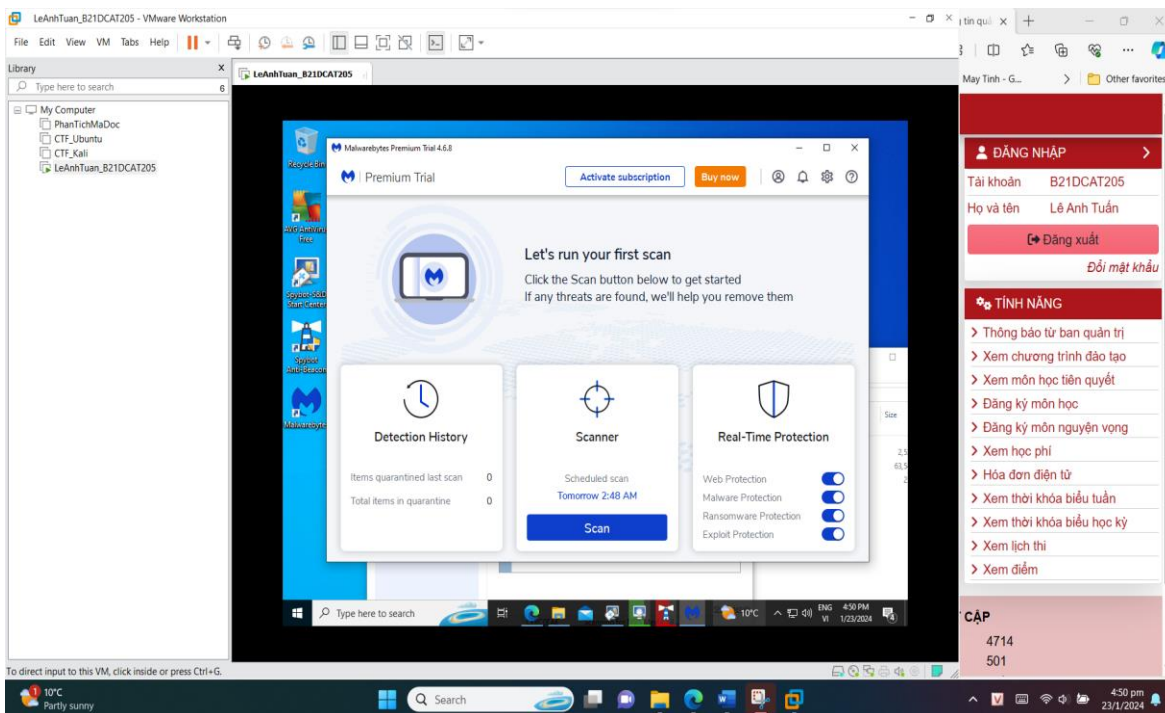


### 3.2.3 Phần mềm chống các phần mềm độc hại: Malwarebytes Anti-Malware

Khởi chạy file cài đặt đã tải, ấn install.

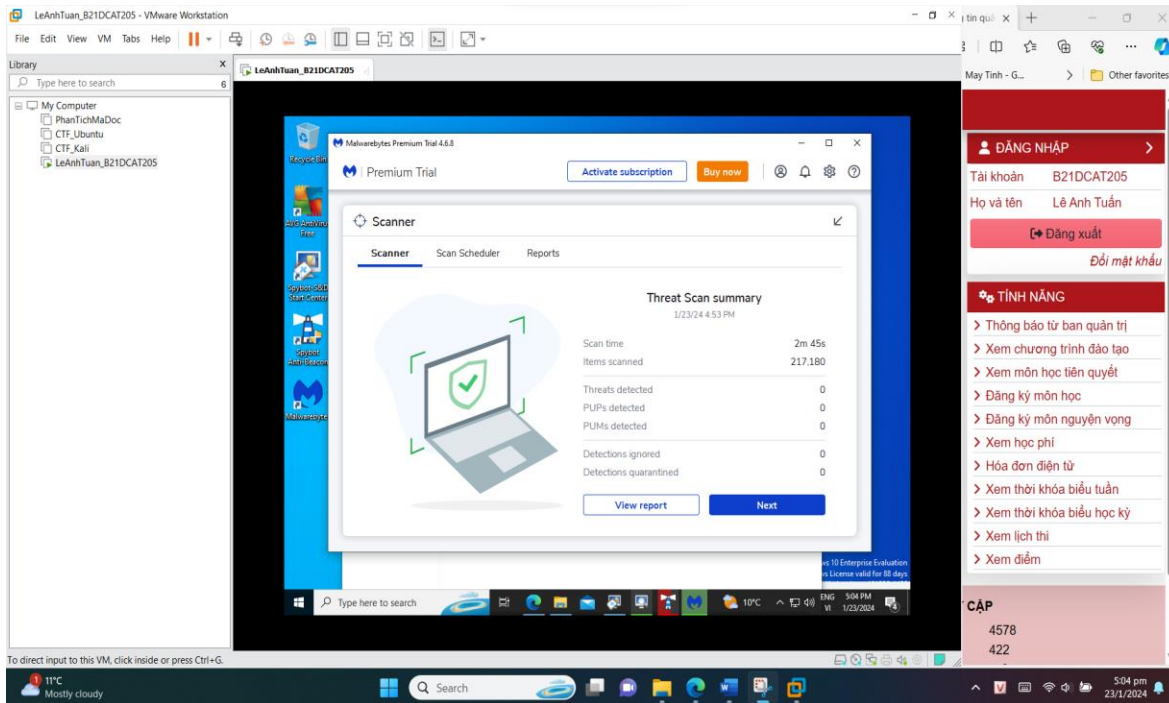


Giao diện sau khi cài đặt thành công, ấn Scan để bắt đầu quá trình rà quét.



Kết quả sau khi quét





### 3.2.4 Phần mềm cứu hộ: Kaspersky Rescue Disk (KRD)

- Tải phần mềm cứu hộ dạng iso: <https://www.kaspersky.com/downloads/free-rescue-disk>



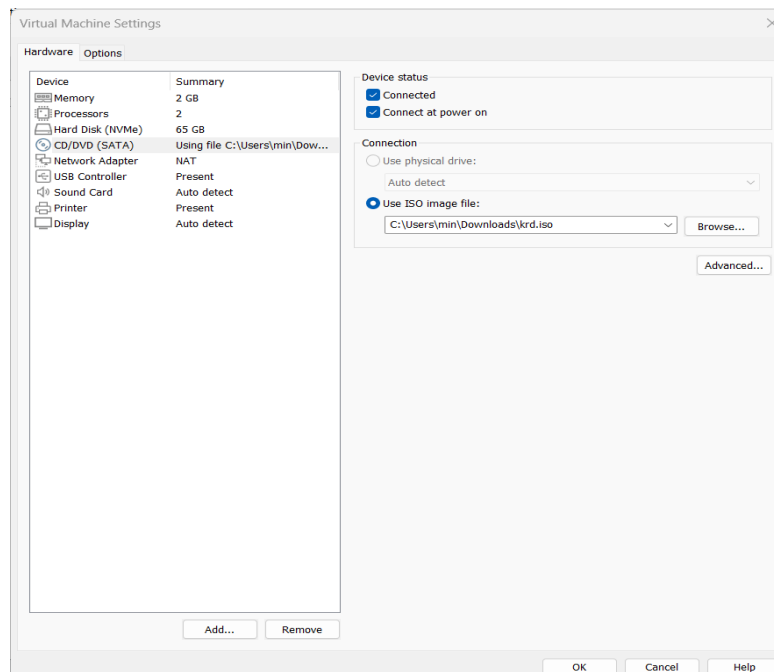
krd

20/1/2024 9:45 pm

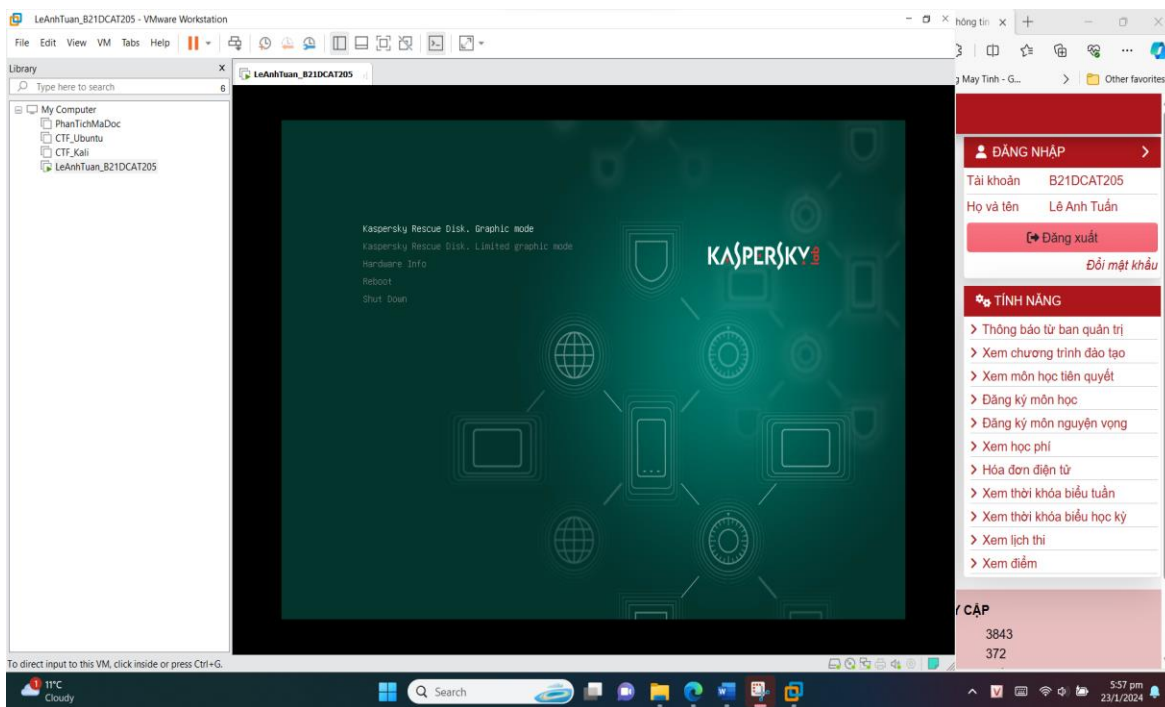
Disc Image File

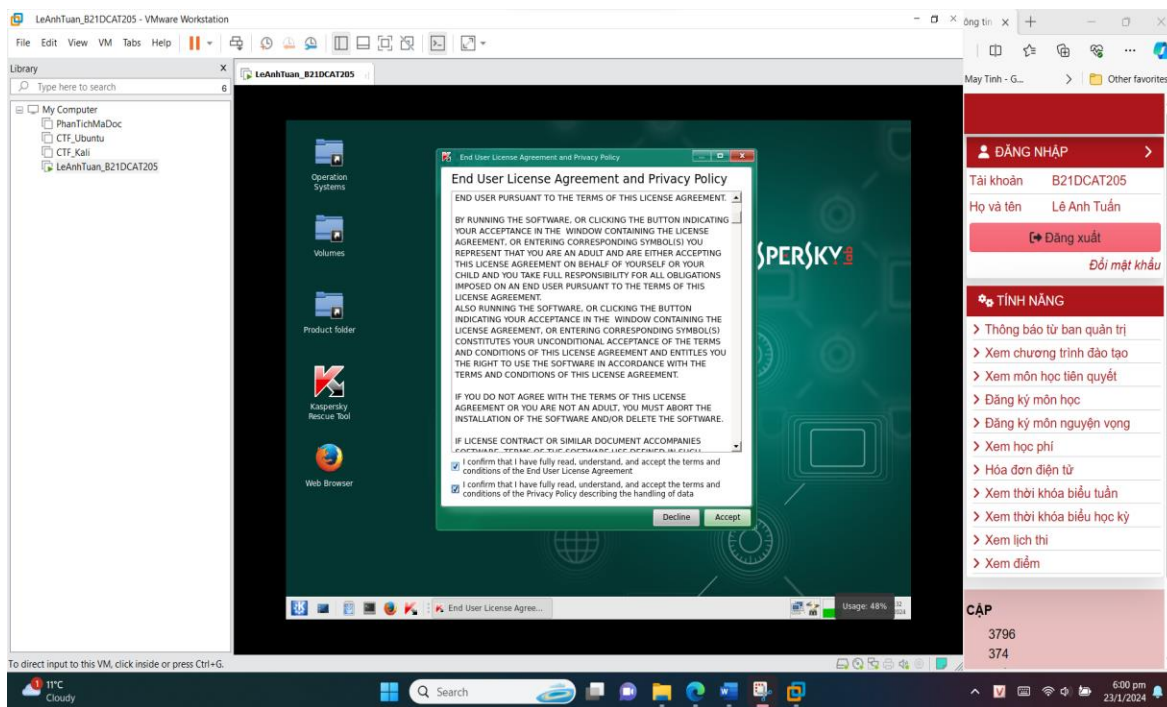
687,698 KB

- Load vào trong mục CD/DVD của máy trạm ảo để có thể khởi động máy trạm ảo dùng đĩa KRD



- Chạy máy trạm ảo, sử dụng phím “esc” để chọn boot từ CD-ROM drive để cài đặt KRD.

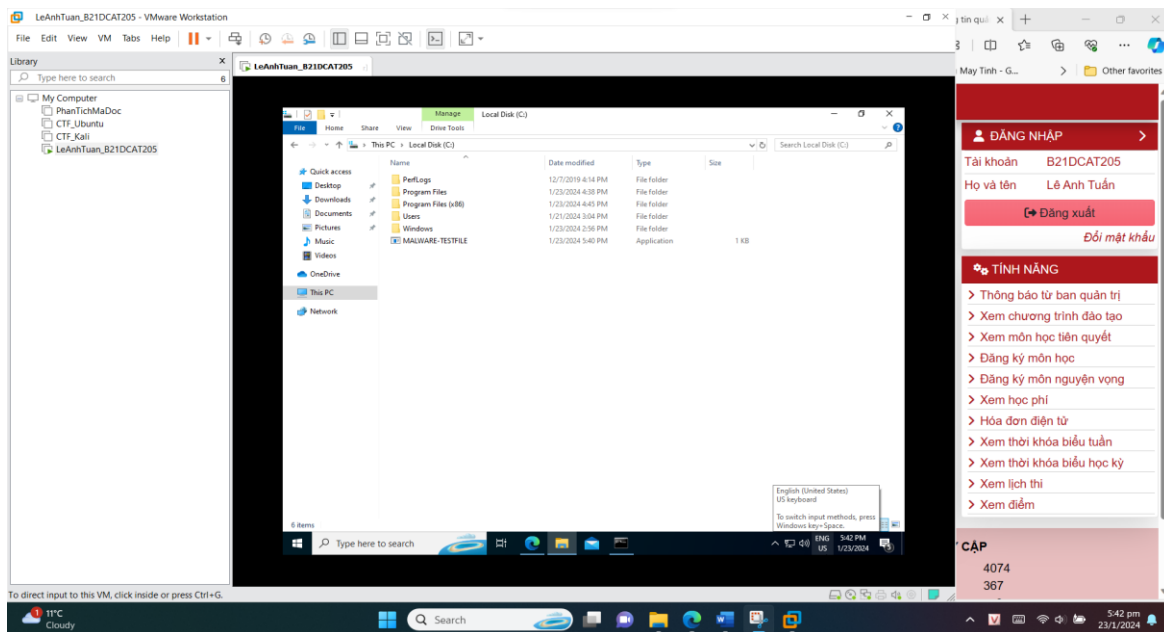




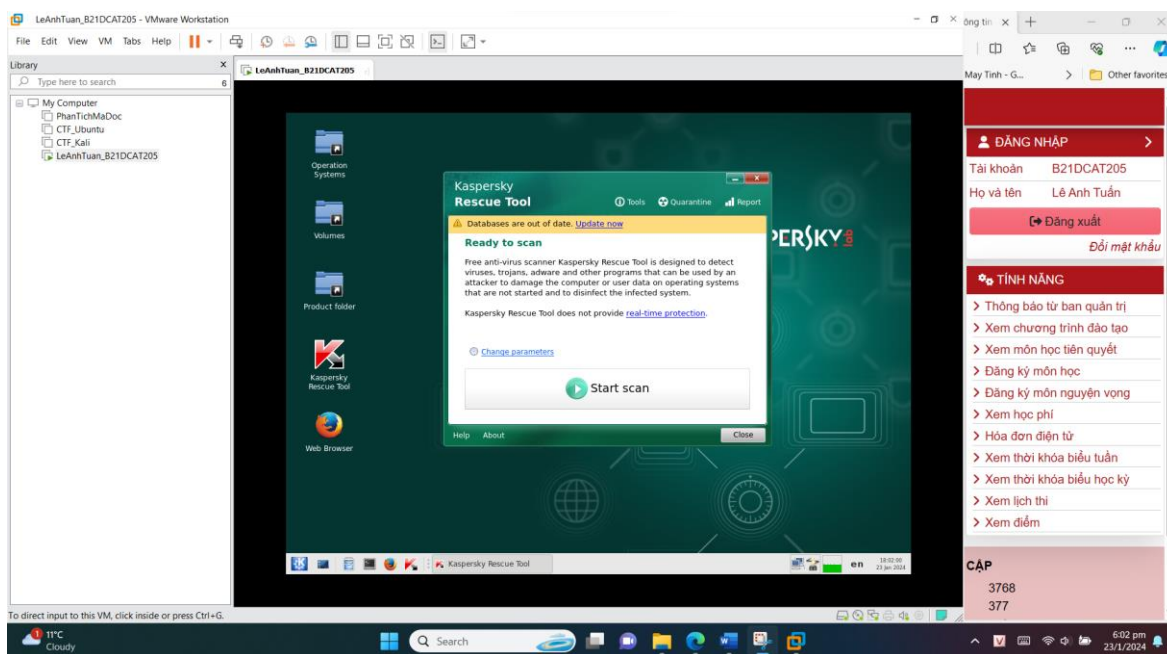
- Mở cmd kiểm tra IP của máy trạm bằng câu lệnh: `ifconfig`
- Dùng Web browser tải file test mã độc từ đường link :  
<http://www.computersecuritystudent.com/WINDOWS/W7/lesson7/M>

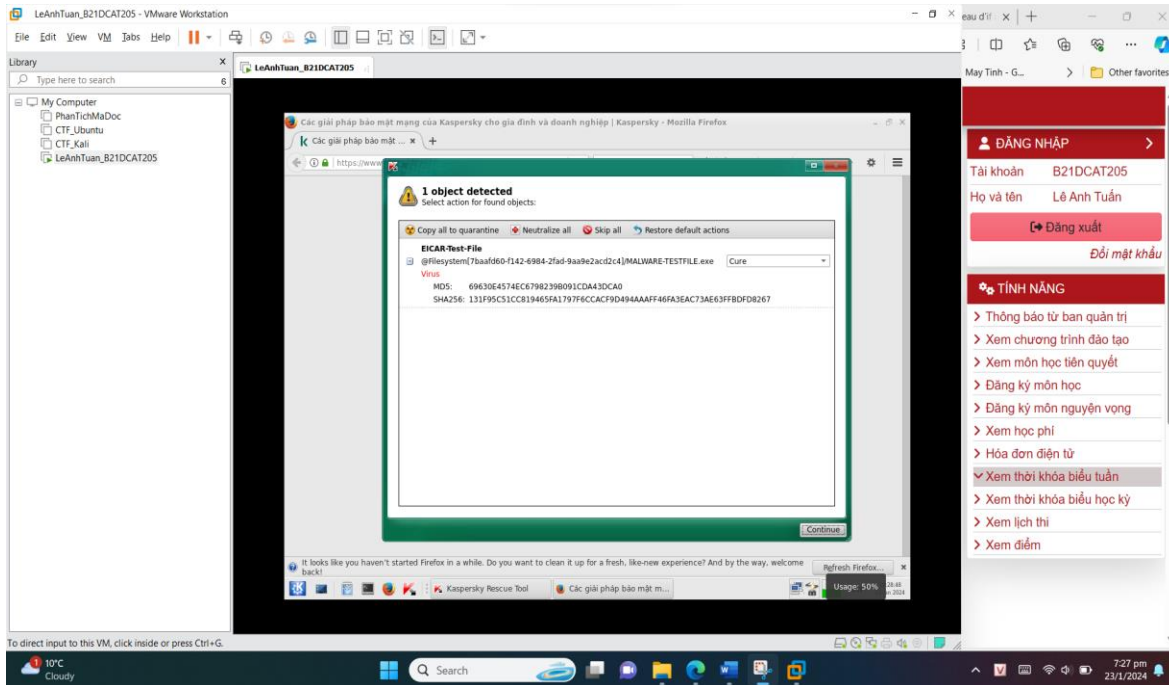
MALWARE-TESTFILE	1/23/2024 5:40 PM	Application	1 KB
------------------	-------------------	-------------	------

- Lưu file test mã độc vào ổ C của máy trạm



- Sau đó chạy Kaspersky Rescue Tool, vào setting chọn quét tất các thư mục -> phát hiện ra file test mã độc và thực hiện xóa nó.





#### 4 Kết luận

- Sinh viên cài đặt và quản trị thành công hệ điều hành máy trạm Windows
- Sinh viên cài đặt thành công và chạy thử một vài phần mềm bảo vệ máy trạm

#### 5 Tài liệu tham khảo

- [What is VMware Workstation? - Definition from Techopedia](#)
- [Advantages and Disadvantages of VMware | Limitations & Benefits of VMware \(hitechwhizz.com\)](#)
- [Oracle VM VirtualBox](#)
- [AVG Antivirus Review 2024 — Should You Download It? \(safetydetectives.com\)](#)
- [Malwarebytes: A Comprehensive Guide \(softwaretested.com\)](#)
- [Kaspersky Rescue Disk](#)
- Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bru Chính Viễn Thông, 2016.
- Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.