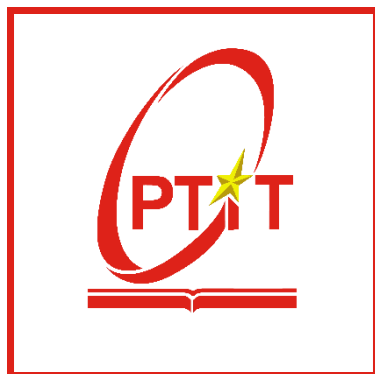


**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA AN TOÀN THÔNG TIN**

---



**THỰC TẬP CƠ SỞ**  
**Cài đặt hệ điều hành máy trạm Windows**

Sinh viên	Nguyễn Duy Đạt
MSV	B21DCAT056
Giảng viên	Vũ Minh Mạnh

**Hà Nội – 2024**

## Môn học Thực tập cơ sở

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

#### I. Lý thuyết

a) *Tìm hiểu về phần mềm ảo hóa VMWare Workstation, VirtualBox*

##### 1. VMWare Workstation

VMware Workstation là một ứng dụng phần mềm ảo hóa mạnh mẽ được VMware, một trong những nhà cung cấp hàng đầu về giải pháp ảo hóa, phát triển. Được thiết kế cho cả người dùng cá nhân và doanh nghiệp, VMware Workstation cho phép bạn tạo và quản lý các máy ảo trên một máy tính vật lý.

Dưới đây là một số điểm quan trọng về VMware Workstation:

- **Tính Năng Ảo Hóa:**  
VMware Workstation hỗ trợ nhiều loại ảo hóa, bao gồm ảo hóa phần cứng và ảo hóa phần mềm. Điều này cho phép bạn chạy nhiều hệ điều hành và ứng dụng trên cùng một máy tính.
- **Hỗ Trợ Hệ Điều Hành Rộng Rãi:**  
VMware Workstation hỗ trợ nhiều hệ điều hành khác nhau, bao gồm Windows, Linux, macOS, và nhiều phiên bản khác của chúng.
- **Chia Sẻ Dữ Liệu Dễ Dàng:**  
VMware Workstation cung cấp các công cụ để chia sẻ dữ liệu giữa máy chủ vật lý và các máy ảo, tạo điều kiện thuận lợi cho việc phát triển và kiểm thử ứng dụng.
- **Snapshot và Clone:**  
Snapshot cho phép bạn lưu trạng thái của máy ảo tại một thời điểm cụ thể, giúp dễ dàng quay trở lại trạng thái trước đó nếu cần. Clone giúp bạn tạo bản sao của máy ảo một cách nhanh chóng.
- **Chạy Máy Ảo Đa Nhiệm:**  
Bạn có thể chạy nhiều máy ảo cùng một lúc trên một máy tính vật lý, giúp bạn kiểm thử và phát triển ứng dụng hiệu quả hơn.

➤ **Tính Tương Thích:**

VMware Workstation tương thích tốt với nhiều công nghệ và tiêu chuẩn ảo hóa, đảm bảo tính tương thích cao với nhiều môi trường và ứng dụng.

➤ **Hỗ Trợ Đồ Họa và Hiệu Suất Cao:**

Hỗ trợ đồ họa 3D và khả năng tối ưu hiệu suất giúp VMware Workstation chạy mượt mà ngay cả khi chạy các ứng dụng đòi hỏi nhiều tài nguyên đồ họa.

➤ **Cộng Đồng Lớn:**

VMware Workstation có một cộng đồng người dùng lớn, nơi bạn có thể tìm kiếm hỗ trợ, chia sẻ kinh nghiệm và kiến thức về việc sử dụng phần mềm này.

VMware Workstation là một công cụ mạnh mẽ cho việc phát triển, kiểm thử ứng dụng và quản lý môi trường máy ảo trên máy tính cá nhân hoặc máy chủ.

## 2. VirtualBox

Oracle VM VirtualBox là một phần mềm ảo hóa miễn phí và mã nguồn mở, phát triển bởi Oracle Corporation. Nó cho phép người dùng tạo và quản lý máy ảo trên một máy tính vật lý. Dưới đây là một số điểm quan trọng về VirtualBox:

➤ **Tính Năng Ảo Hóa:**

VirtualBox hỗ trợ ảo hóa phần cứng và phần mềm, cho phép bạn chạy nhiều hệ điều hành và ứng dụng trên cùng một máy tính.

➤ **Hỗ Trợ Hệ Điều Hành Rộng Rãi:**

VirtualBox có khả năng hỗ trợ nhiều hệ điều hành khác nhau, bao gồm Windows, Linux, macOS, BSD, Solaris, và nhiều hệ điều hành khác.

➤ **Tính Linh Hoạt:**

VirtualBox cung cấp khả năng tùy chỉnh linh hoạt, giúp bạn điều chỉnh cấu hình máy ảo theo nhu cầu cụ thể.

➤ **Snapshot và Clone:**

Snapshot cho phép bạn lưu trạng thái của máy ảo tại một thời điểm cụ thể. Clone giúp bạn tạo bản sao của máy ảo một cách nhanh chóng.

- Chia Sẻ Dữ Liệu:  
VirtualBox cung cấp các tính năng giúp bạn chia sẻ dữ liệu giữa máy chủ vật lý và máy ảo.
- Hỗ Trợ USB và Thiết Bị Ngoại Vi:  
VirtualBox có khả năng hỗ trợ các thiết bị USB và thiết bị ngoại vi, giúp bạn kết nối và sử dụng chúng trong máy ảo.
- Hiệu Suất Tốt:  
Mặc dù là một phần mềm miễn phí, VirtualBox vẫn cung cấp hiệu suất tốt, đặc biệt là trong việc chạy các hệ điều hành và ứng dụng đơn giản.
- Cộng Đồng Hỗ Trợ:  
VirtualBox có một cộng đồng sử dụng lớn, nơi người dùng có thể tìm kiếm hỗ trợ, chia sẻ thông tin và giải quyết vấn đề.
- Dễ Cài Đặt và Sử Dụng:  
VirtualBox có giao diện người dùng thân thiện và dễ sử dụng, giúp người dùng mới nhanh chóng làm quen và tận dụng được tính năng của phần mềm.

Oracle VM VirtualBox là một giải pháp ảo hóa linh hoạt và mạnh mẽ, thích hợp cho cả người dùng cá nhân và doanh nghiệp. Nó cung cấp một lựa chọn tốt để tạo và quản lý các môi trường máy ảo trên một máy tính.

## *b) Tìm hiểu về HĐH Windows*

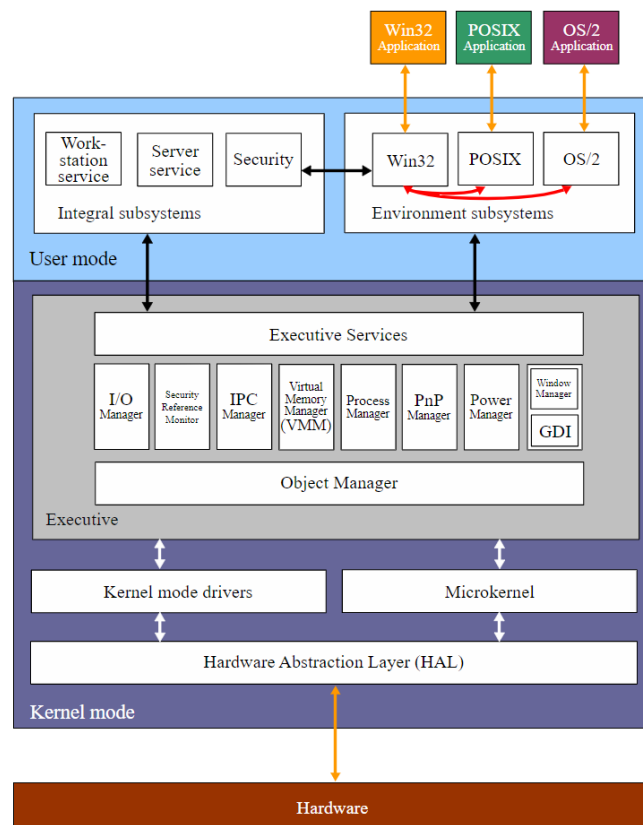
### 1. Lịch sử phát triển

Hệ điều hành Windows, phát triển bởi Microsoft Corporation, có một lịch sử đa dạng và tiến triển qua nhiều phiên bản. Bắt đầu từ Windows 1.0 vào năm 1985, với giao diện đơn giản và hỗ trợ đa nhiệm cơ bản, hệ điều hành này đã trải qua nhiều bước tiến quan trọng. Windows 95 đánh dấu sự chuyển đổi từ MS-DOS sang hệ điều hành độc lập, mang theo thanh Start và menu Start. Các phiên bản

như Windows XP (ổn định và đa nhiệm tốt) và Windows 7 (giao diện cải tiến) đã đạt được sự phổ biến lớn. Tuy nhiên, Windows Vista gặp khó khăn với vấn đề hiệu suất, trong khi Windows 8, thiết kế cho màn hình cảm ứng, nhận phản ứng tiêu cực. Windows 10, ra mắt vào năm 2015, là một hệ điều hành dịch vụ với giao diện mới, tính năng hiện đại và chuyển sang mô hình dịch vụ liên tục thông qua Windows Update.

## 2. Kiến trúc của hệ điều hành

Kiến trúc của hệ điều hành Windows là một hệ thống phức tạp và linh hoạt. Trái tim của nó là Kernel, chịu trách nhiệm quản lý bộ nhớ, tương tác với phần cứng và xử lý yêu cầu hệ thống. Chia chế độ người dùng và chế độ kernel giúp cách ly quyền truy cập và tác vụ giữa ứng dụng và hạ tầng hệ thống. Win32 API là giao diện lập trình quan trọng, cung cấp các hàm để tương tác với hệ điều hành. Hardware Abstraction Layer (HAL) giúp tương tác với nhiều loại phần cứng khác nhau mà không cần sửa đổi nhiều. Hệ thống tệp, Registry và các dịch vụ hệ thống quản lý cấu hình, lưu trữ dữ liệu và chạy các dịch vụ nền. Giao diện người dùng đồ họa được quản lý bởi Desktop Window Manager (DWM), còn subsystem hỗ trợ nhiều môi trường để chạy ứng dụng đa dạng. Tóm lại, kiến trúc của Windows tạo ra một hệ điều hành linh hoạt, tương thích và mạnh mẽ, đáp ứng đa dạng nhu cầu của người dùng.



### 3. Giao diện của Windows

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**

Giao diện người dùng đồ họa trong Windows bao gồm các cửa sổ, nút bấm, hộp văn bản và các phần tử định hướng khác. Phần tử quan trọng trong GUI đó chính là menu khởi động (Start) và thanh tác vụ (Taskbar). Menu khởi động 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 cho phép truy nhập nhanh đến các ứng dụng và cho biết tình trạng của các chương trình người quản trị. Phần quan trọng khác, đó là màn hình làm việc (desktop). Đây 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**

Đây là giao diện dòng lệnh mới của Windows và là môi trường nên dùng cho các tác vụ quản trị. Thực tế, Microsoft hỗ trợ tập các lệnh trong môi trường PowerShell được gọi là cmdlet để thực hiện các tác vụ quản trị mong muốn.

Một trong những tính năng quan trọng của PowerShell là khả năng lập trình đơn giản (scripting). Với các hàm lô-gíc 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. Hơn thế, PowerShell còn cho phép thực thi các lệnh từ xa nhờ hỗ trợ từ hệ điều hành.

*c) Tìm hiểu về một số phần mềm bảo vệ máy trạm*

1. Phần mềm diệt virus: AVG AntiVirus



AVG AntiVirus là một ứng dụng diệt virus và bảo mật máy tính được phát triển bởi AVG Technologies. Với hơn 25 năm kinh nghiệm trong lĩnh vực an ninh mạng, AVG AntiVirus được thiết kế để bảo vệ người dùng khỏi các mối đe dọa trực tuyến đa dạng. Phần mềm này cung cấp nhiều tính năng chính để đảm bảo sự an toàn và ổn định của hệ thống.

AVG AntiVirus có khả năng phát hiện và loại bỏ virus, malware, spyware và các loại phần mềm độc hại khác một cách hiệu quả. Chế độ quét thông minh cho phép người dùng kiểm tra toàn bộ hệ thống hoặc chọn lựa quét các khu vực cụ thể, giúp ngăn chặn mối đe dọa trước khi chúng có cơ hội gây hại.

Tính năng tường lửa của AVG giúp ngăn chặn các mối đe dọa mạng và bảo vệ quyền riêng tư trong quá trình sử dụng Internet. Bảo vệ email và web giúp ngăn chặn các đính kèm độc hại và truy cập vào các trang web có thể đe dọa an toàn trực tuyến.

AVG AntiVirus thường xuyên cập nhật cơ sở dữ liệu virus để đối mặt với các mối đe dọa mới xuất hiện, đảm bảo rằng người dùng luôn được bảo vệ với thông tin mới nhất về an ninh.

Giao diện người dùng của AVG thường được thiết kế dễ sử dụng, với các tính năng và tùy chọn được sắp xếp một cách rõ ràng. Bạn có thể tận hưởng sự bảo vệ cơ bản thông qua phiên bản miễn phí hoặc trải nghiệm những tính năng nâng cao hơn với các phiên bản trả phí của phần mềm.

## 2. Phần mềm chống phần mềm gián điệp Spybot S&D



Spybot - Search & Destroy (Spybot S&D) là một phần mềm chống phần mềm gián điệp và bảo vệ máy tính khỏi các mối đe dọa an ninh trực tuyến. Được phát triển bởi Safer-Networking Ltd., Spybot S&D là một trong những ứng dụng chống spyware phổ biến từ thập kỷ trước.

Phần mềm này có khả năng quét và loại bỏ spyware, adware, trojan, keylogger và các phần mềm độc hại khác một cách hiệu quả. Nó sử dụng một cơ sở dữ liệu độc lập để nhận diện các mối đe dọa và cung cấp khả năng bảo vệ thời gian thực để ngăn chặn sự xâm nhập của phần mềm gián điệp trước khi chúng gây hại.

Tính năng Immunization của Spybot S&D giúp người dùng ngăn chặn truy cập của các trang web độc hại và nguy hiểm. Ngoài ra, Spybot S&D còn cung cấp công cụ System Startup để quản lý các ứng dụng khởi động cùng hệ thống, giúp người dùng kiểm soát và tối ưu hóa hiệu suất máy tính.

Một trong những đặc điểm độc đáo của Spybot S&D là tính năng TeaTimer, một ứng dụng giám sát thời gian thực giúp theo dõi và ngăn chặn các thay đổi không mong muốn trong hệ thống.

Được cập nhật đều đặn, Spybot S&D là một công cụ đáng tin cậy cho việc bảo vệ máy tính cá nhân khỏi các mối đe dọa an ninh trực tuyến và giữ cho thông tin cá nhân người dùng an toàn. Tính linh hoạt và tính năng mạnh mẽ của nó giúp người dùng duyệt web và thực hiện các hoạt động trực tuyến một cách an toàn.



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



## Malwarebytes®

Malwarebytes Anti-Malware là một phần mềm chống phần mềm độc hại hàng đầu được thiết kế để bảo vệ máy tính khỏi các mối đe dọa an ninh trực tuyến. Phần mềm này, phát triển bởi Malwarebytes Corporation, đã nhanh chóng trở thành một trong những công cụ quét và diệt malware phổ biến nhất trên thị trường.

Malwarebytes Anti-Malware sử dụng công nghệ tiên tiến để phát hiện và loại bỏ nhiều loại phần mềm độc hại, bao gồm virus, trojan, spyware, rootkit và adware. Chương trình này tập trung vào việc tìm kiếm các mối đe dọa mới và chưa được xác định, cung cấp một lớp bảo vệ mạnh mẽ cho người dùng.

Với giao diện người dùng thân thiện và dễ sử dụng, Malwarebytes Anti-Malware cung cấp khả năng quét nhanh chóng và hiệu quả, giúp người dùng kiểm tra toàn bộ hệ thống hoặc các khu vực cụ thể một cách thuận tiện. Chế độ quét đầy đủ hệ thống hoặc chế độ quét tùy chỉnh giúp tối ưu hóa trải nghiệm người dùng.

Malwarebytes Anti-Malware không chỉ giới hạn việc diệt malware mà còn cung cấp các tính năng bảo vệ an ninh, bao gồm chức năng ngăn chặn các trang web độc hại và tự động cập nhật định kỳ để đối mặt với các mối đe dọa mới.

Phiên bản cơ bản của Malwarebytes Anti-Malware thường là miễn phí và có thể được sử dụng để quét và loại bỏ malware cơ bản. Phiên bản Premium cung cấp các tính năng bảo vệ nâng cao, bao gồm bảo vệ thời gian thực và chế độ tự động quét để duy trì một hệ thống an toàn và ổn định trong thời gian dài. Malwarebytes Anti-Malware là

một công cụ quan trọng để giúp người dùng duy trì sự an toàn và bảo vệ trong môi trường trực tuyến ngày càng nguy hiểm.

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

Kaspersky Rescue Disk (KRD) là một công cụ cứu hộ chống malware và diệt virus, được phát triển bởi Kaspersky Lab, một công ty nổi tiếng trong lĩnh vực an ninh mạng. Được thiết kế để hoạt động độc lập và không cần cài đặt trực tiếp trên hệ thống, Kaspersky Rescue Disk chủ yếu được sử dụng khi máy tính bị nhiễm malware mà không thể quét và loại bỏ bằng phần mềm antivirus truyền thống.

Kaspersky Rescue Disk hoạt động dựa trên môi trường Linux và sử dụng công nghệ quét mạnh mẽ để phát hiện và diệt các mối đe dọa an ninh, bao gồm virus, trojan, spyware và rootkit. Người dùng chỉ cần tạo một đĩa hoặc USB bootable từ tệp ISO của Kaspersky Rescue Disk, sau đó khởi động máy tính từ đĩa hoặc USB này để bắt đầu quá trình quét và làm sạch hệ thống.

Một trong những đặc điểm quan trọng của Kaspersky Rescue Disk là khả năng quét và làm sạch máy tính khi hệ điều hành chưa được tải, giúp loại bỏ các mối đe dọa trước khi chúng kích hoạt trong quá trình khởi động của hệ điều hành chính. Ngoài ra, Kaspersky Rescue Disk cung cấp giao diện dòng lệnh đơn giản nhưng mạnh mẽ, cho phép người dùng tùy chỉnh các tùy chọn quét và xử lý mối đe dọa.

Với tính năng cập nhật định kỳ, Kaspersky Rescue Disk đảm bảo rằng cơ sở dữ liệu virus luôn được cập nhật để nhận diện các mối đe dọa mới. Điều này làm cho nó trở thành một công cụ hiệu quả để khắc phục và làm sạch máy tính khi hệ thống chính không thể hoạt động đúng cách do tác động của malware.

## II. Thực hành

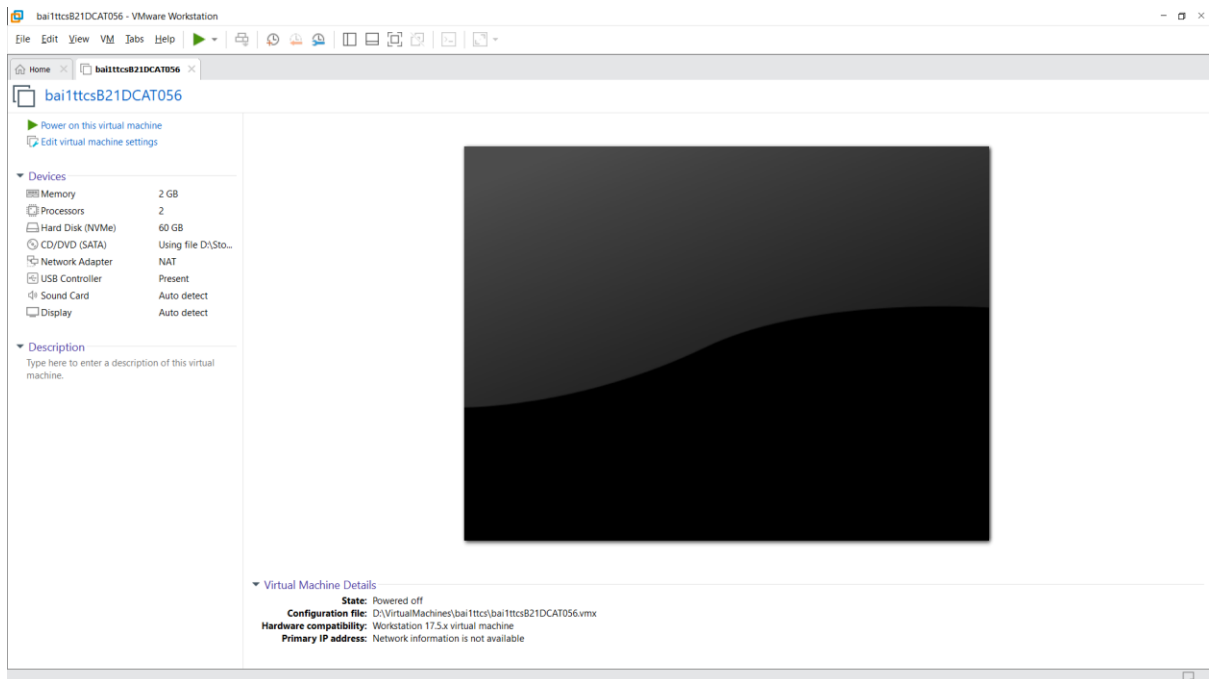
*Chuẩn bị môi trường:*

- File cài đặt Windows 10 định dạng iso
- Phần mềm ảo hóa: VMWare Workstation

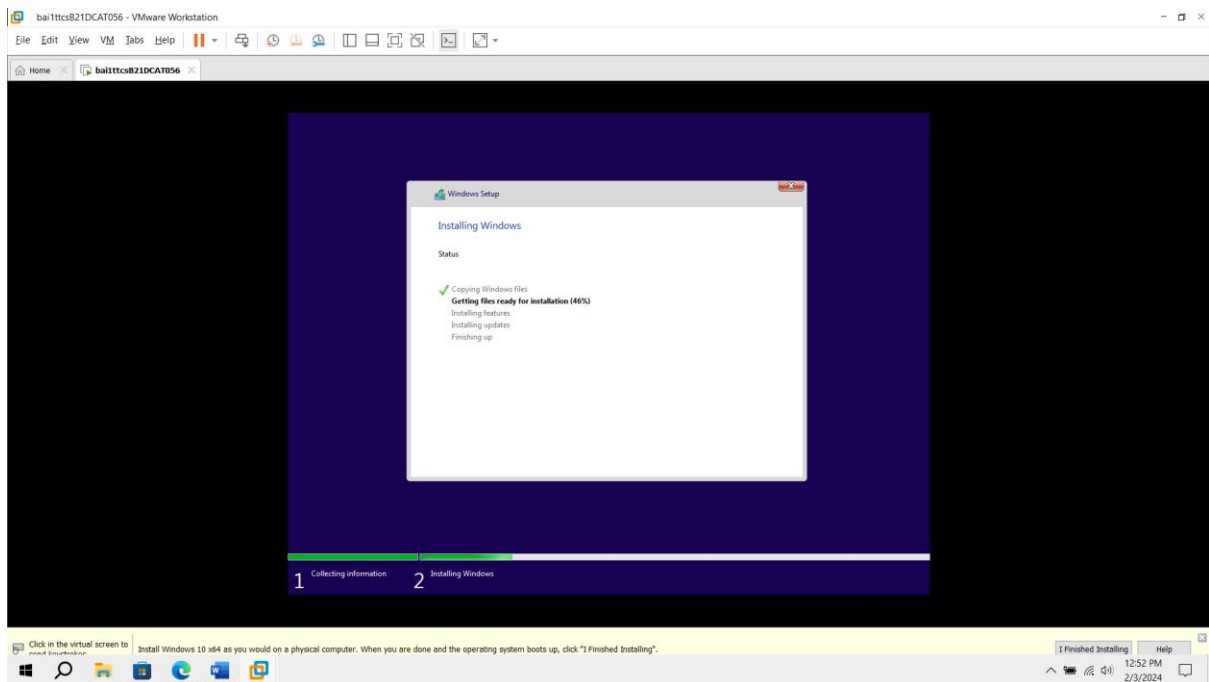
*Các bước thực hiện:*

a) Cài đặt Windows 10

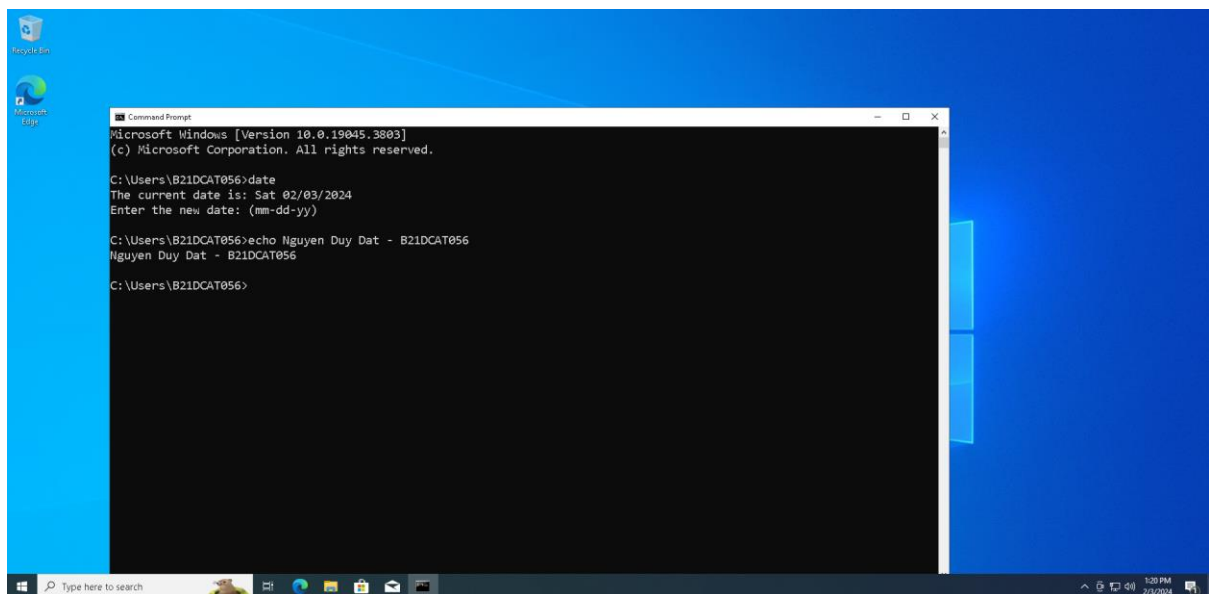
- Khởi động chương trình máy ảo



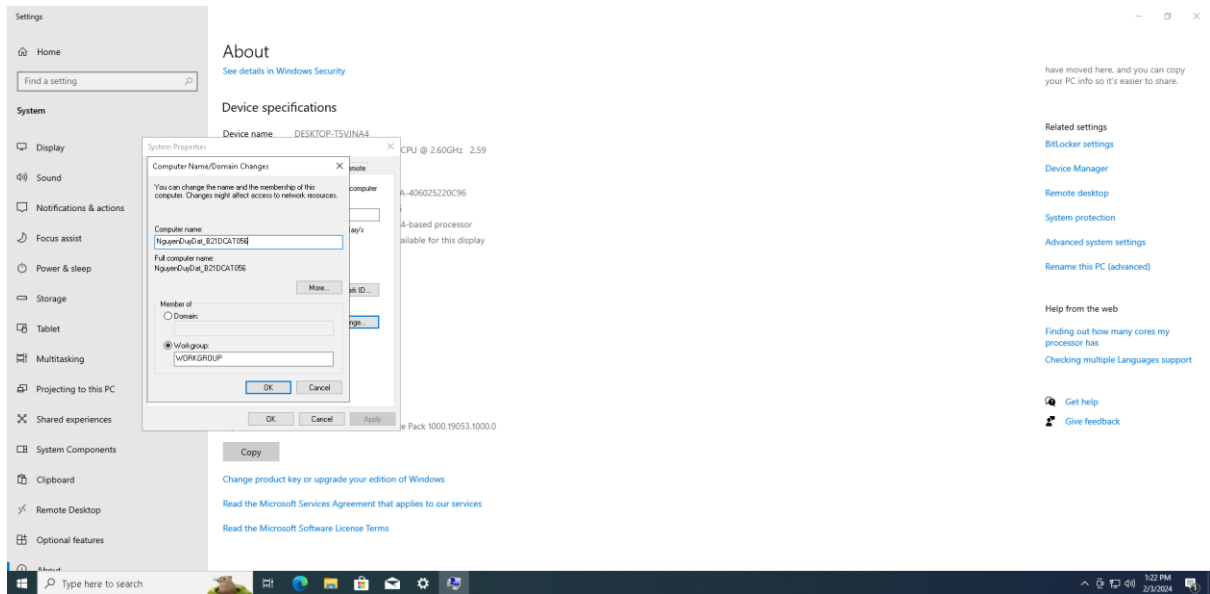
## - Tiến hành cài đặt Windows 10



## - Giao diện Windows sau khi đã cài đặt xong

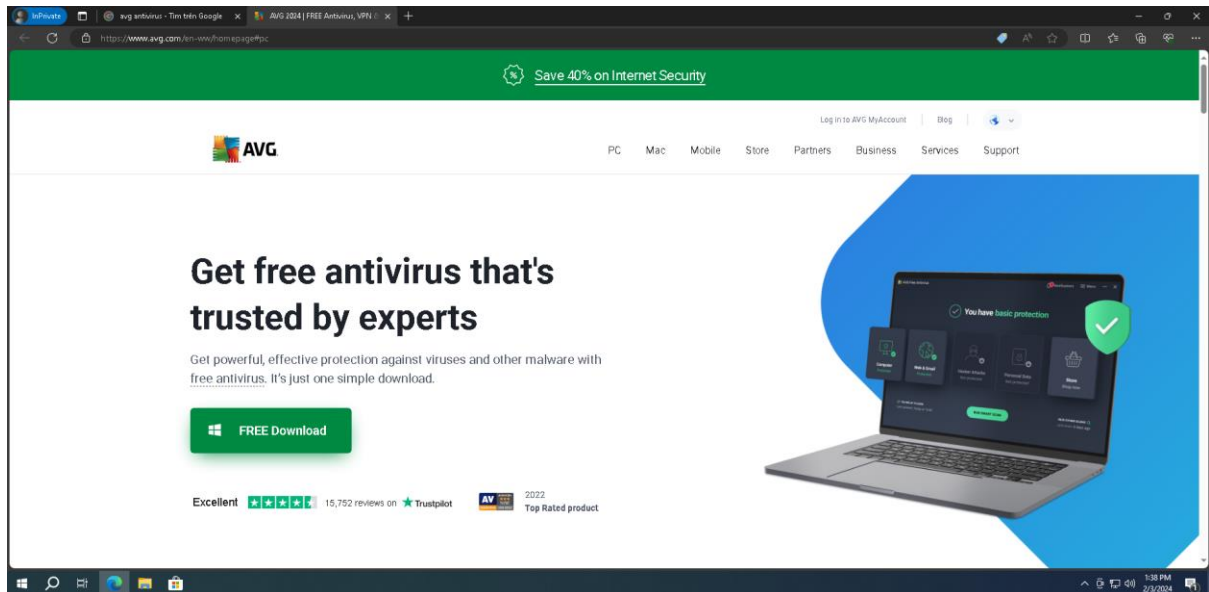


- Trong mục “System Properties”, đổi tên máy thành NguyenDuyDat\_B21DCAT056

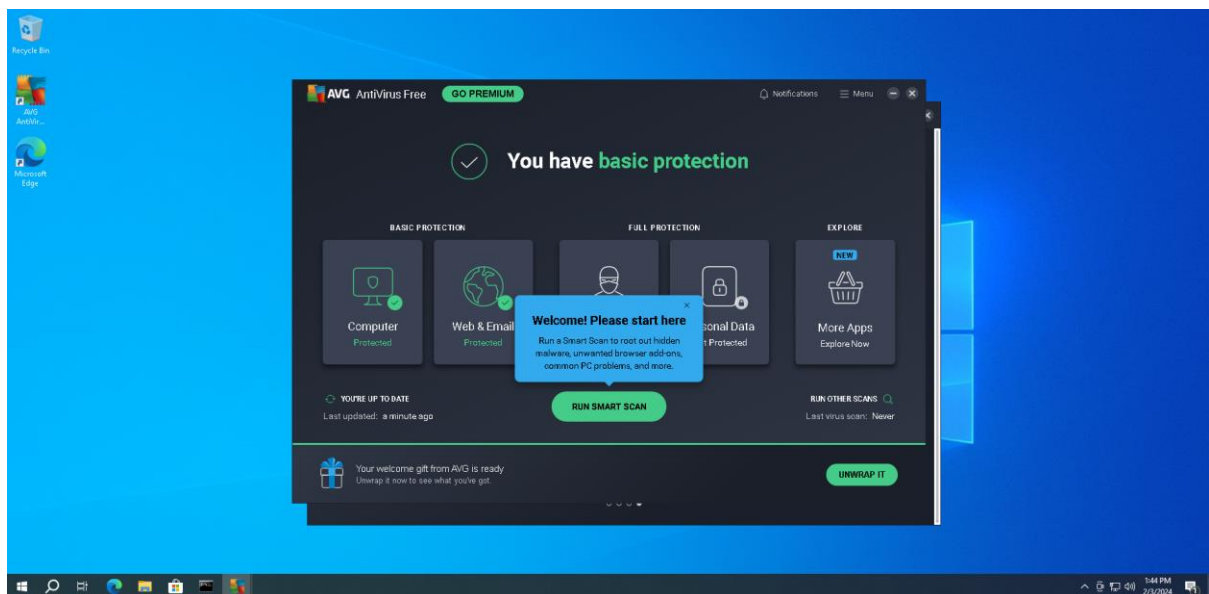


## b) Phần mềm diệt virus: AVG AntiVirus

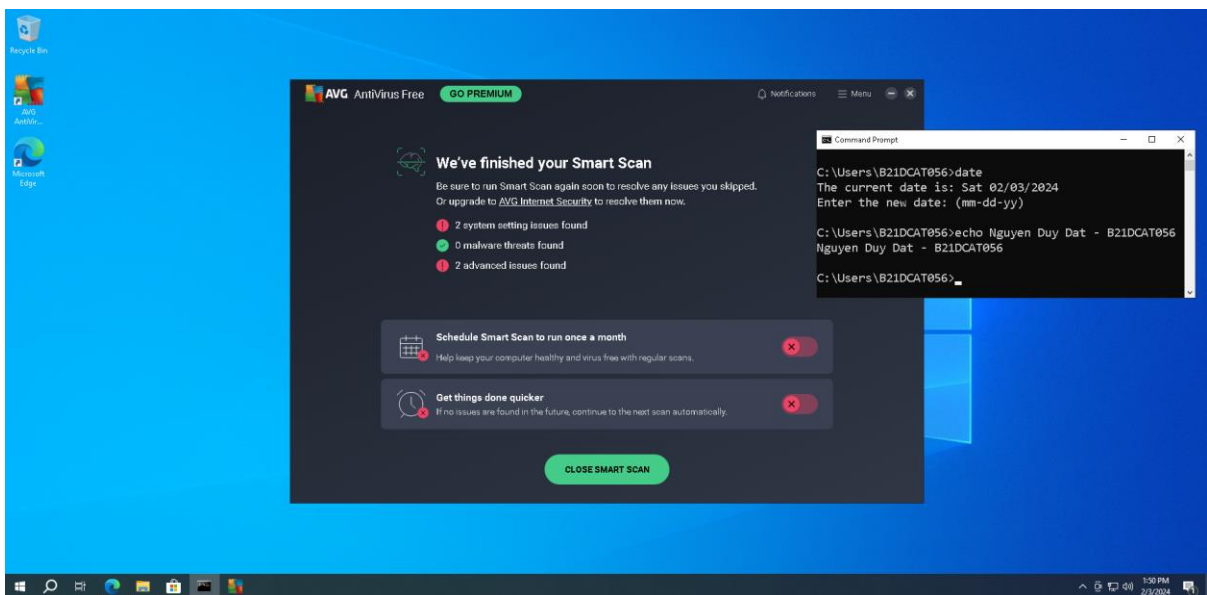
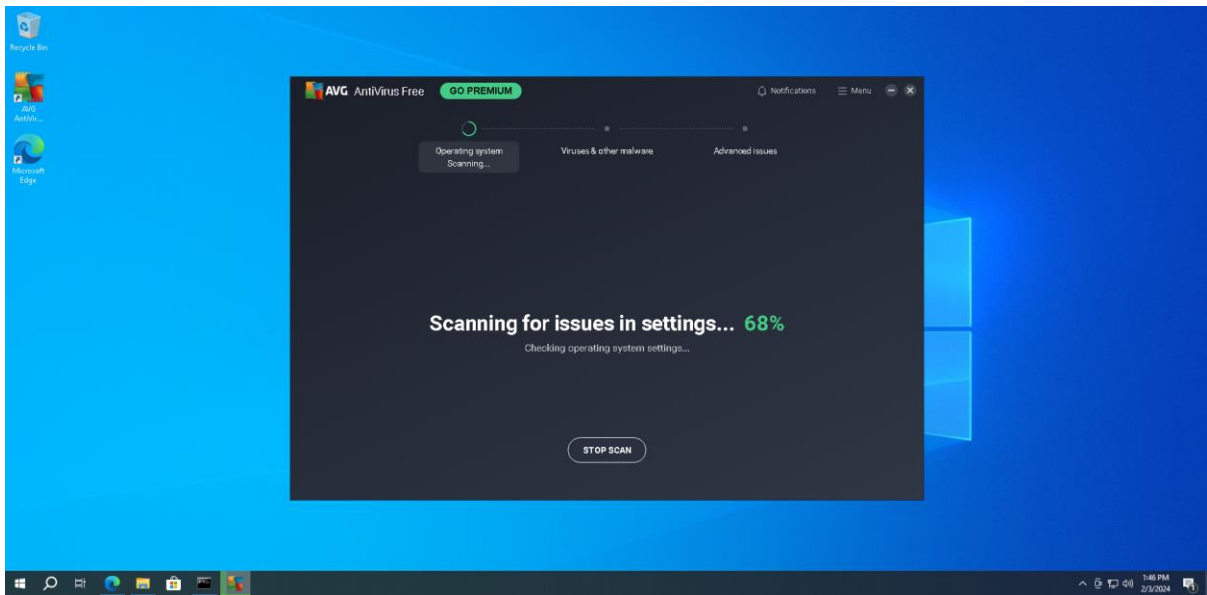
- Vào trang web tải phần mềm AVG AntiVirus



- Tiến hành cài đặt phần mềm AVG AntiVirus thành công

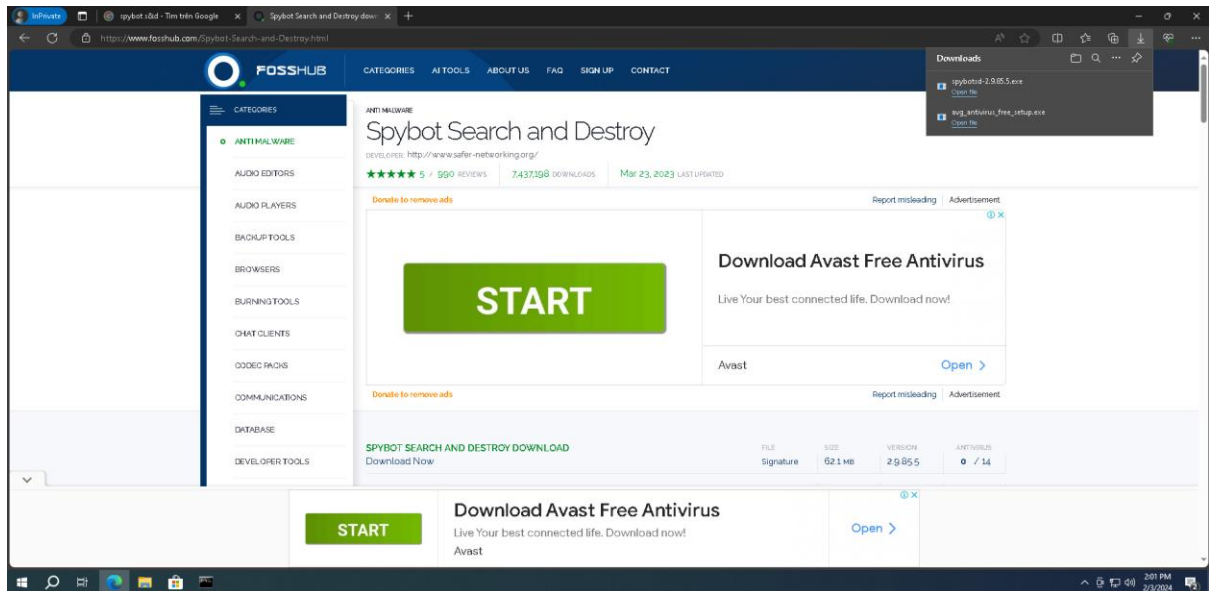


- Sau khi cài xong thì bắt đầu quét máy

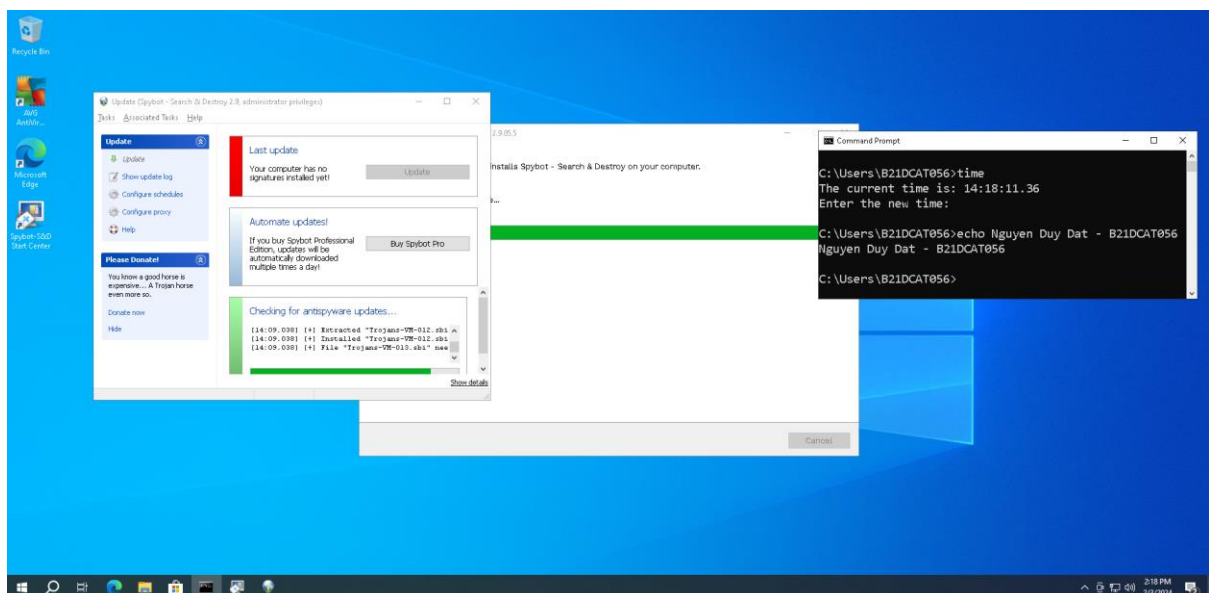


## c) Phần mềm chống phần mềm gián điệp Spybot S&D

### - Tải phần mềm

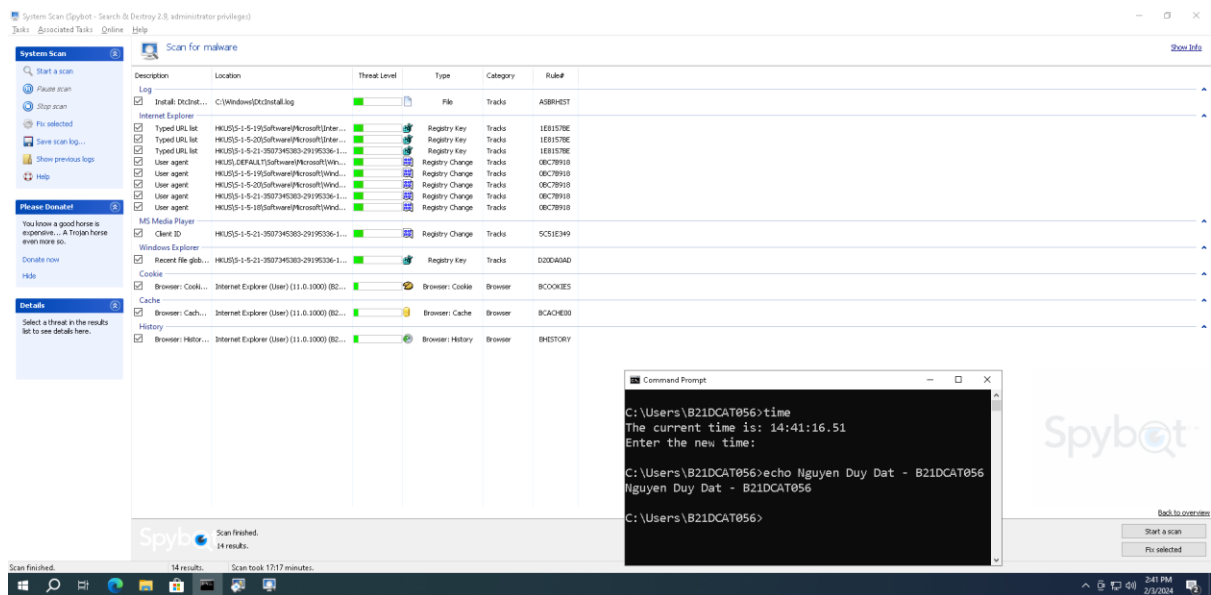
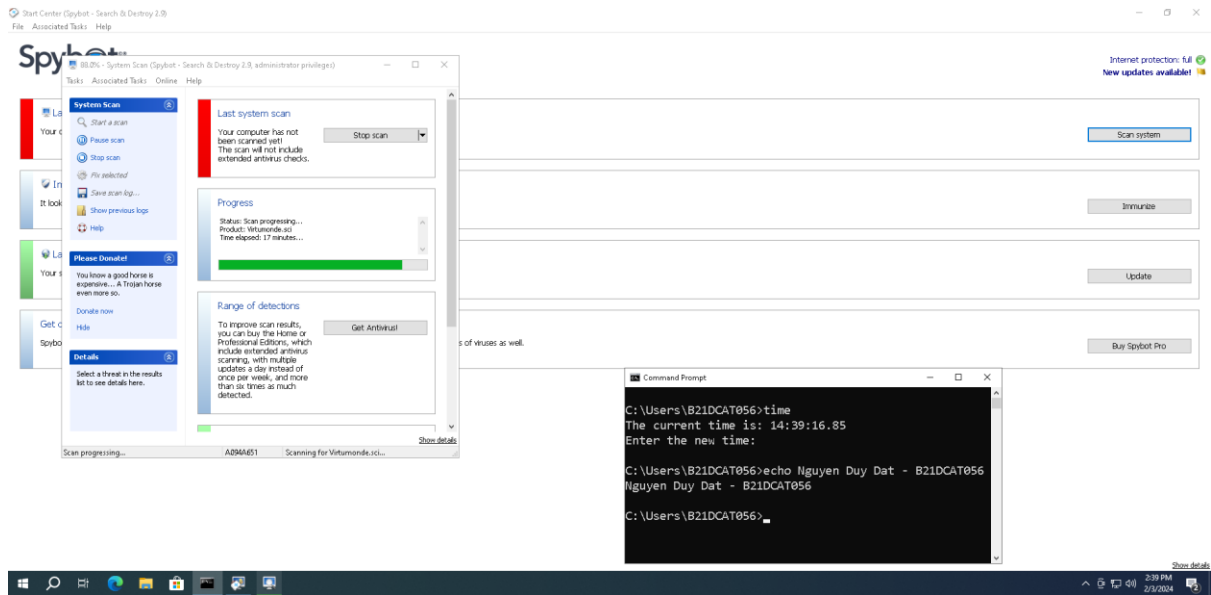


### - Tiến hành cài đặt



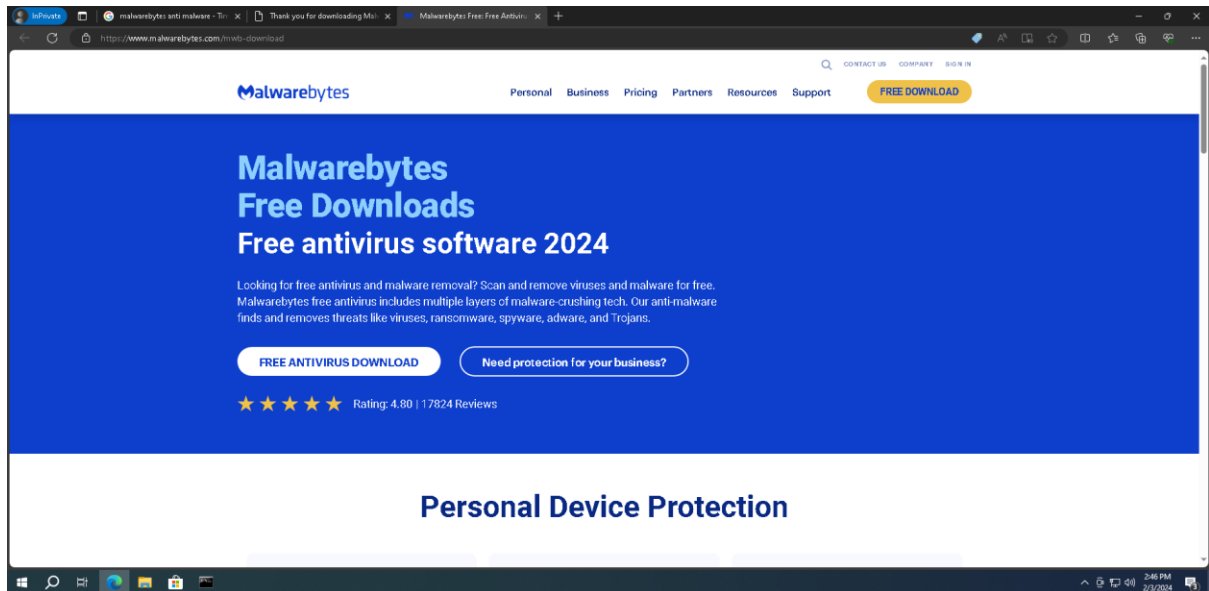


- Sau khi cài xong thực hiện quét máy

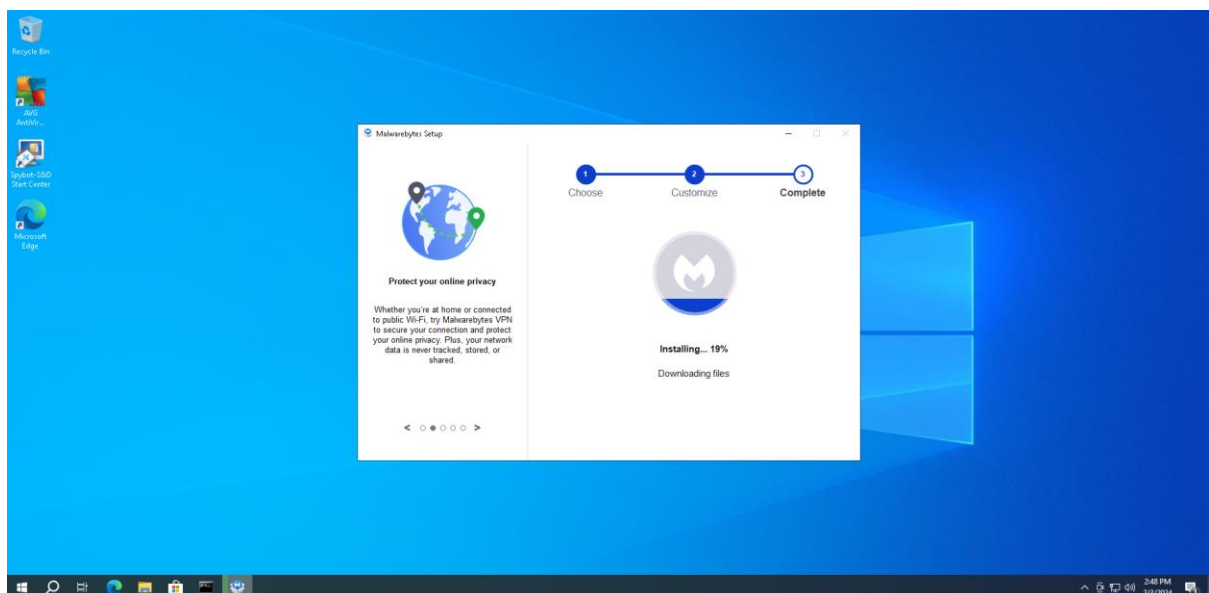


d) Phần mềm chống các phần mềm độc hại: Malwarebytes Anti-Malware

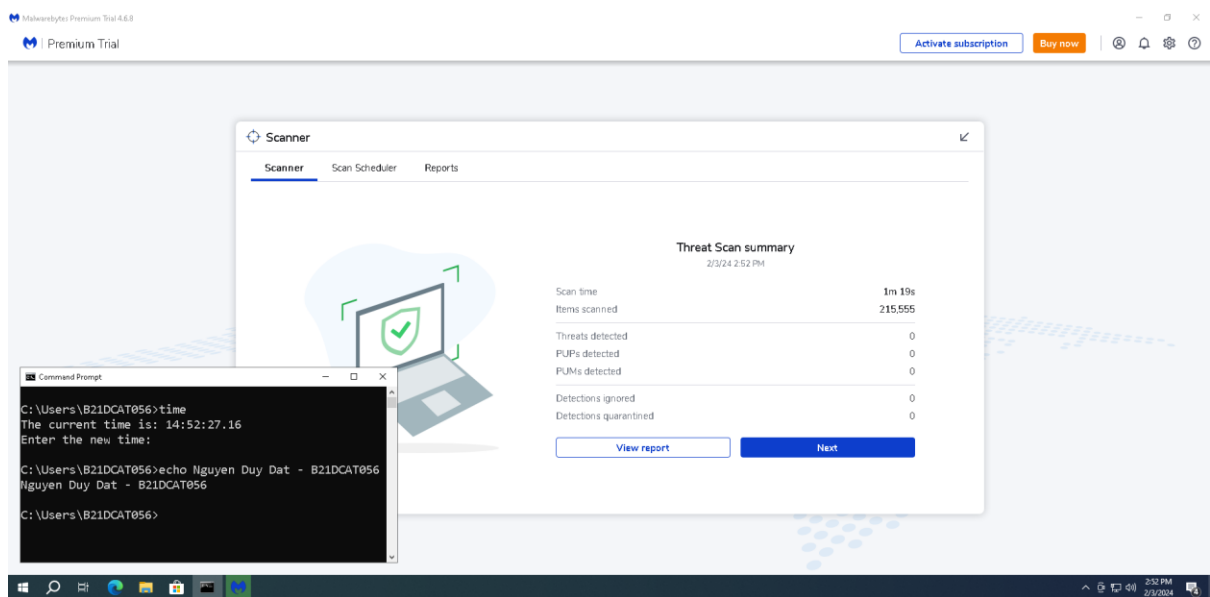
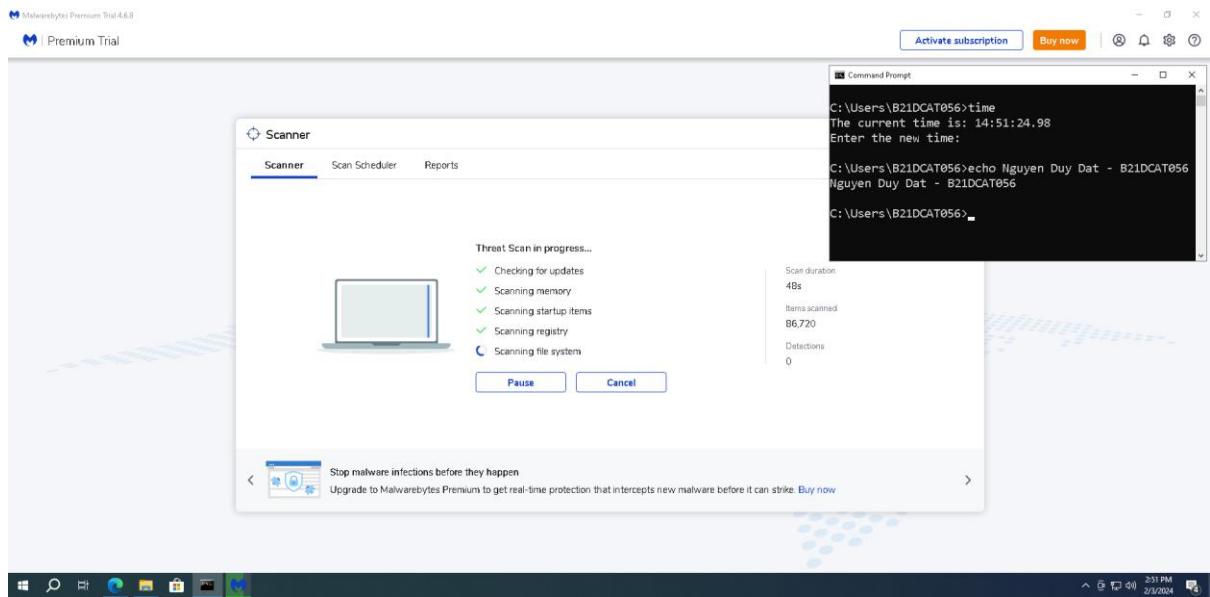
- Tải phần mềm trên trang chủ



- Tiến hành cài đặt

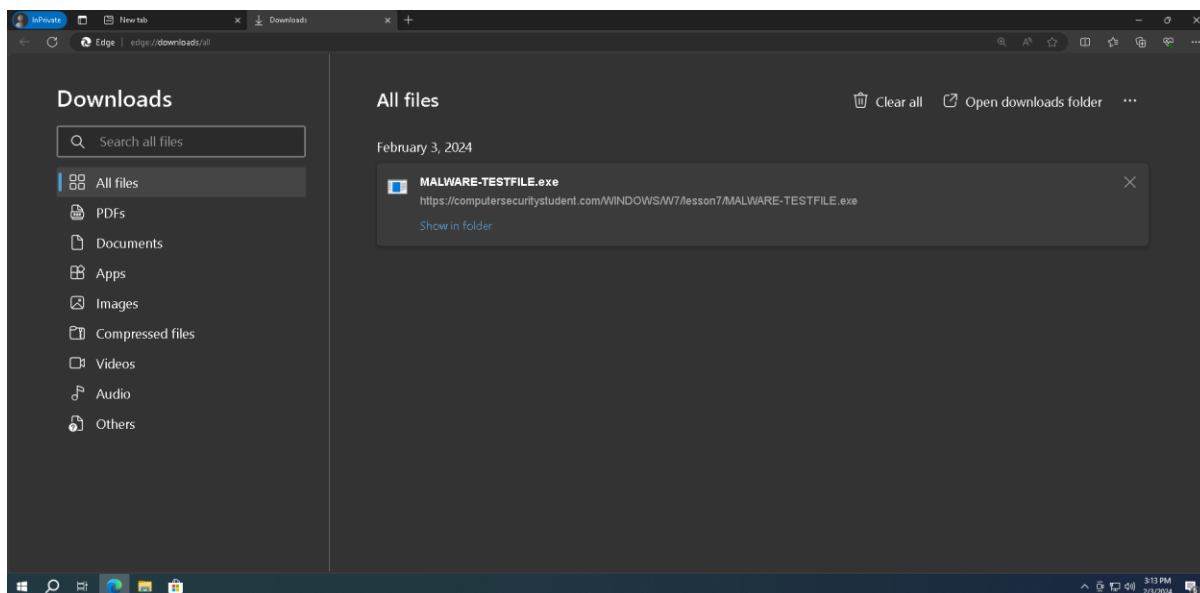


- Sau khi cài xong, bắt đầu quét máy

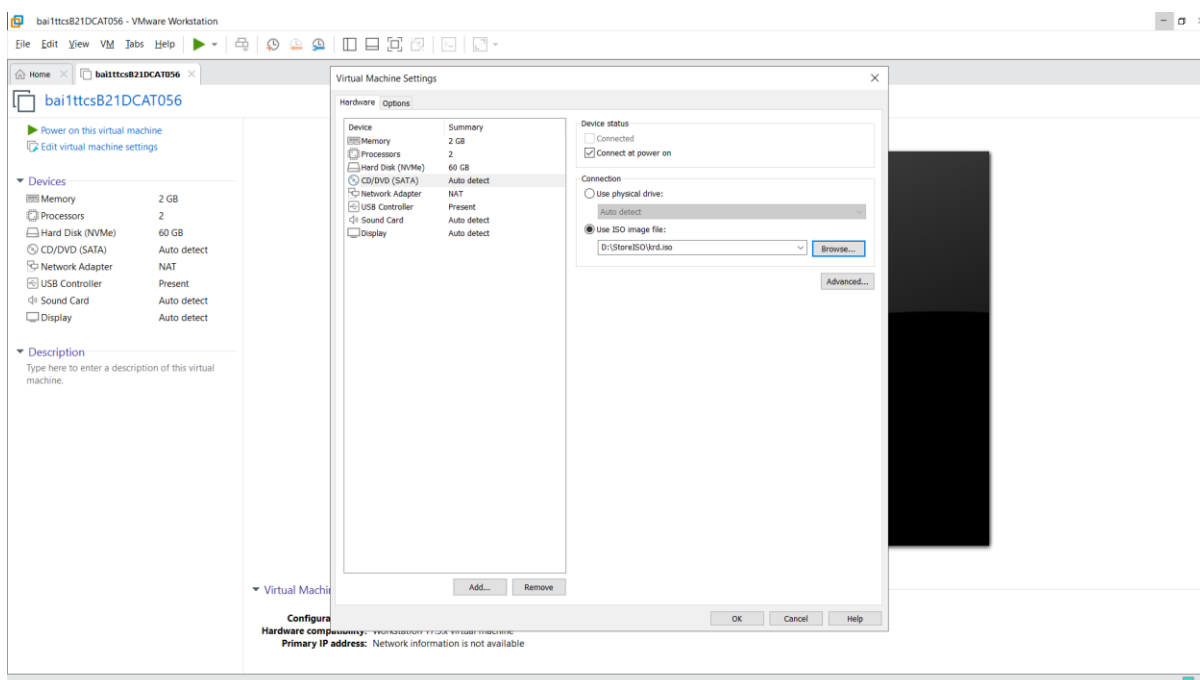


## e) Phần mềm cứu hộ: Kaspersky Rescue Disk (KRD)

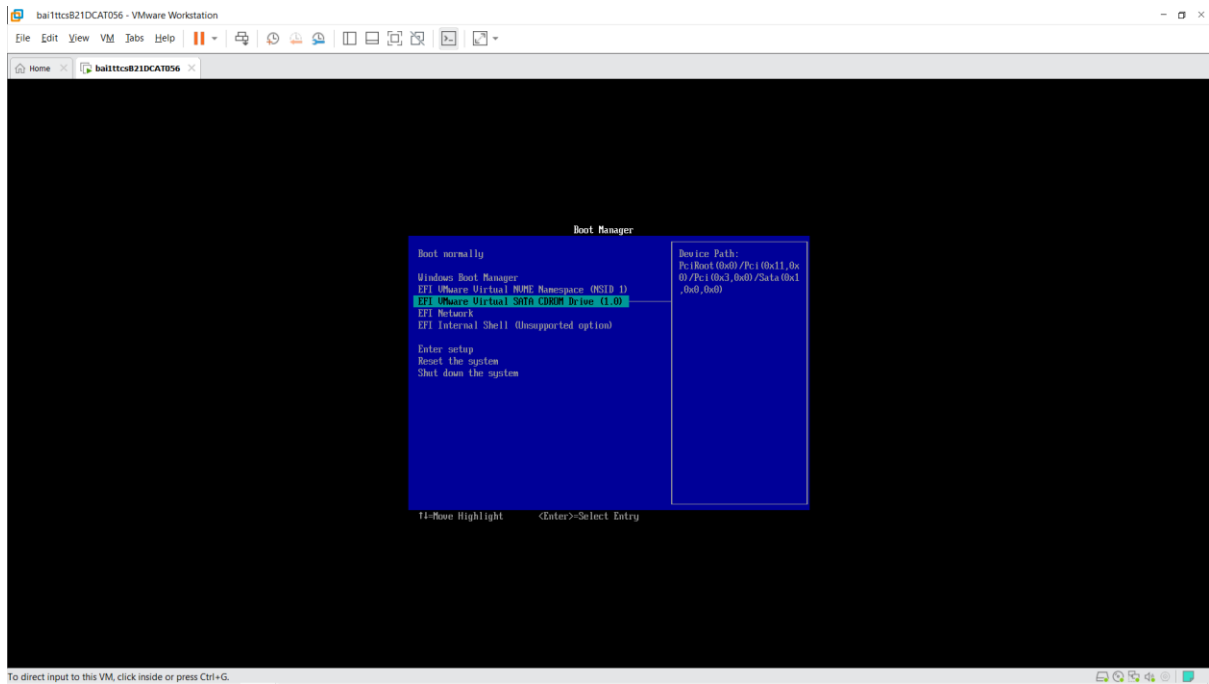
- Tải phần mềm độc hại về máy trạm trước



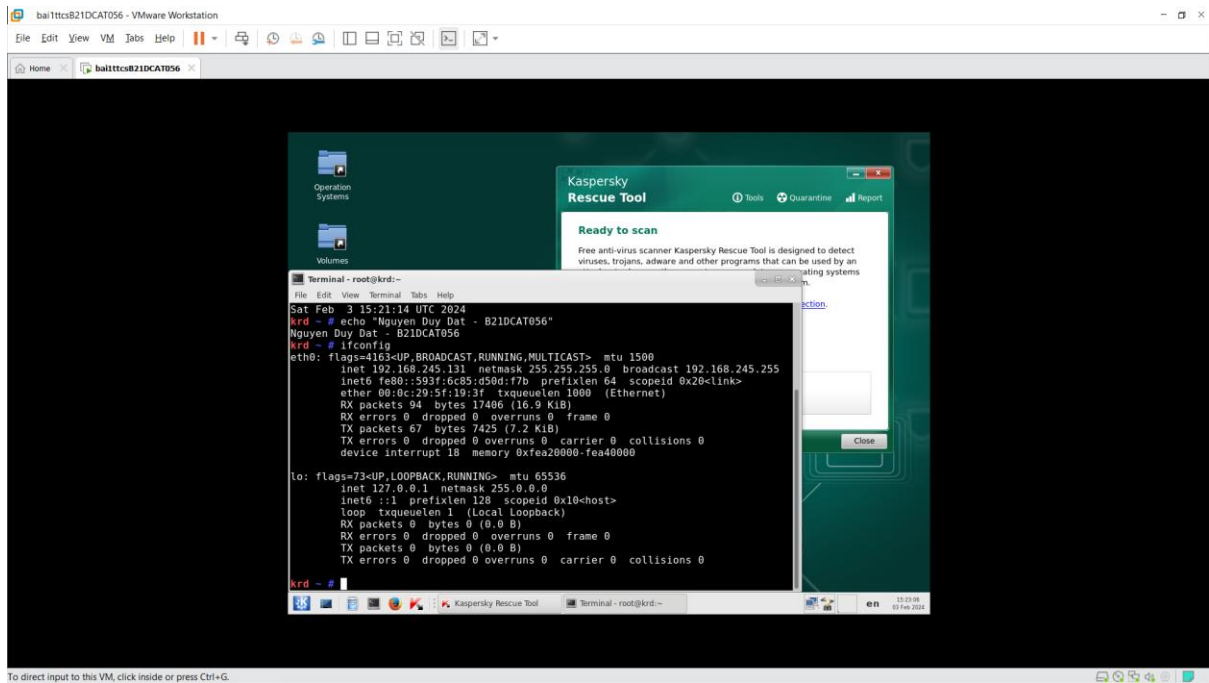
- Load file rkd.iso vào mục CD/DVD của máy trạm



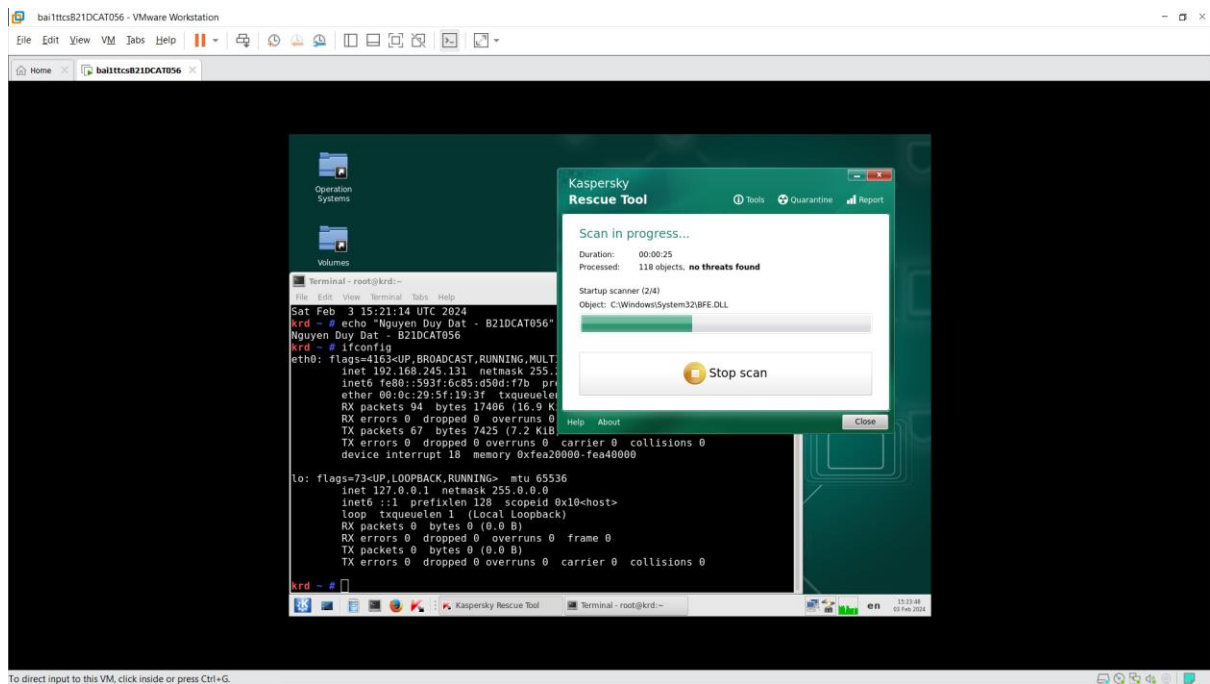
- Boot từ CDROM drive để cài đặt KRD



- Mở terminal kiểm tra IP bằng câu lệnh: ifconfig



- Tiến hành quét các thư mục



- Phát hiện file mã độc -> Xóa

