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:

B22DCAT034 Trương Quốc Bảo

Giảng viên hướng dẫn: TS. Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
VM	Virtual Machine	Máy ảo
DLL	Dynamic Link Library	Thư viện liên kết động
GUI	Graphical User Interface	Giao diện đồ họa người dùng
WSL	Windows Subsystem for Linux	Hệ thống con Windows cho Linux
KRD	Kaspersky Rescue Disk	Đĩa cứu hộ Kaspersky

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

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

1.2 Tìm hiểu lý thuyết

1.2.1 Phần mềm ảo hóa

Ảo hóa là công nghệ mà bạn có thể sử dụng để tạo các dạng trình bày ảo của máy chủ, kho lưu trữ, mạng và nhiều máy vật lý khác. Phần mềm ảo mô phỏng các chức năng của phần cứng vật lý để chạy đồng thời nhiều máy ảo trên một máy vật lý duy nhất. Các doanh nghiệp ứng dụng công nghệ ảo hóa để sử dụng hiệu quả tài nguyên phần cứng của họ và thu về lợi nhuận trên vốn đầu tư lớn hơn. Công nghệ này cũng hỗ trợ nhiều dịch vụ điện toán đám mây giúp các tổ chức quản lý cơ sở hạ tầng hiệu quả hơn.

Bằng cách sử dụng ảo hóa, bạn có thể tương tác với bất kỳ tài nguyên phần cứng nào với độ linh hoạt cao hơn. Các máy chủ vật lý tiêu thụ điện, chiếm không gian lưu trữ và cần được bảo trì. Bạn thường bị giới hạn về khoảng cách tiếp cận thực tế và thiết kế mạng nếu muốn tiếp cận máy chủ vật lý. Ảo hóa sẽ loại bỏ tất cả những giới hạn này bằng cách trừu tượng hóa chức năng của phần cứng vật lý thành phần mềm. Bạn có thể quản lý, bảo trì và sử dụng cơ sở hạ tầng phần cứng của mình như một ứng dụng trên web.

1.2.2 VMWare Workstation

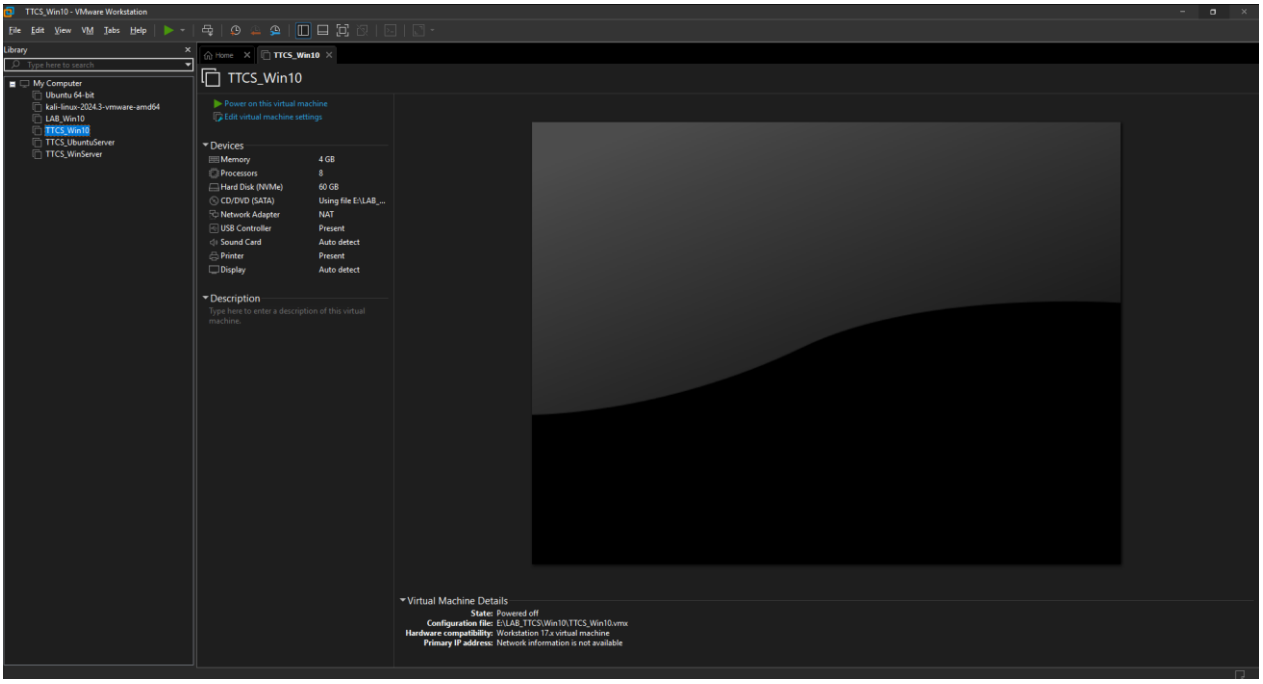
VMware Workstation Pro là một phần mềm ảo hóa (hypervisor loại 2) chạy trên hệ điều hành Windows và Linux (x64). Phần mềm này cho phép người dùng tạo và sử dụng đồng thời nhiều máy ảo (VM) trên cùng một máy tính vật lý, mỗi máy ảo có thể chạy một hệ điều hành riêng như Windows, Linux, BSD hoặc MS-DOS.

VMware Workstation được phát triển và phân phối bởi VMware, công ty thuộc sở hữu của Broadcom từ tháng 11/2023. Vào tháng 5/2024, VMware Workstation Pro được cung cấp miễn phí cho mục đích cá nhân, với tùy chọn đăng ký trả phí dành cho doanh nghiệp. Đến tháng 11/2024, phần mềm này trở thành miễn phí hoàn toàn cho cả mục đích thương mại, và các gói đăng ký trả phí cũng như dịch vụ hỗ trợ không còn được cung cấp.

Phần mềm hỗ trợ kết nối mạng bằng cách sử dụng card mạng của máy chủ, chia sẻ ổ đĩa vật lý và thiết bị USB với máy ảo. Người dùng có thể gắn tập tin ISO làm ổ đĩa quang ảo và sử dụng các ổ đĩa cứng ảo được lưu dưới định dạng .vmdk.

Một tính năng quan trọng của VMware Workstation Pro là khả năng lưu trạng thái của máy ảo bằng snapshot, giúp người dùng khôi phục lại máy ảo về trạng thái trước đó nếu cần. Ngoài ra, phần mềm còn hỗ trợ nhóm nhiều máy ảo vào một thư mục để quản lý dễ dàng, cho phép bật/tắt toàn bộ nhóm cùng lúc, rất hữu ích trong việc kiểm thử môi trường client-server phức tạp.

VMware Workstation giúp người dùng chạy nhiều hệ điều hành khác nhau trên cùng một phần cứng, chẳng hạn như chạy Linux trên máy Mac hoặc Windows. Điều này rất hữu ích cho việc thử nghiệm hệ điều hành, truy cập các trang web không đáng tin cậy hoặc tạo môi trường an toàn cho trẻ em. Phần mềm cũng cho phép chạy nhiều máy ảo đồng thời và có giao diện trực quan, dễ sử dụng.



Hình 1 Giao diện làm việc của VMWare Workstation

1.2.3 Hệ điều dành Windows

1.2.3.1 Lịch sử phát triển

Windows là hệ điều hành do Microsoft phát triển, ra mắt lần đầu vào năm 1985 với Windows 1.0. Kể từ đó, hệ điều hành này đã trải qua nhiều phiên bản quan trọng:

- Windows 3.x (1990-1994): Phiên bản đầu tiên có giao diện đồ họa đáng chú ý.

- Windows 95 (1995): Giới thiệu menu Start, thanh Taskbar, hỗ trợ hệ thống tập tin FAT32 và Plug and Play.

- Windows XP (2001): Giao diện Luna mới, tính ổn định cao hơn và trở thành một trong những phiên bản phổ biến nhất.

- Windows 7 (2009): Cải thiện hiệu năng, giao diện Aero, hỗ trợ DirectX 11.

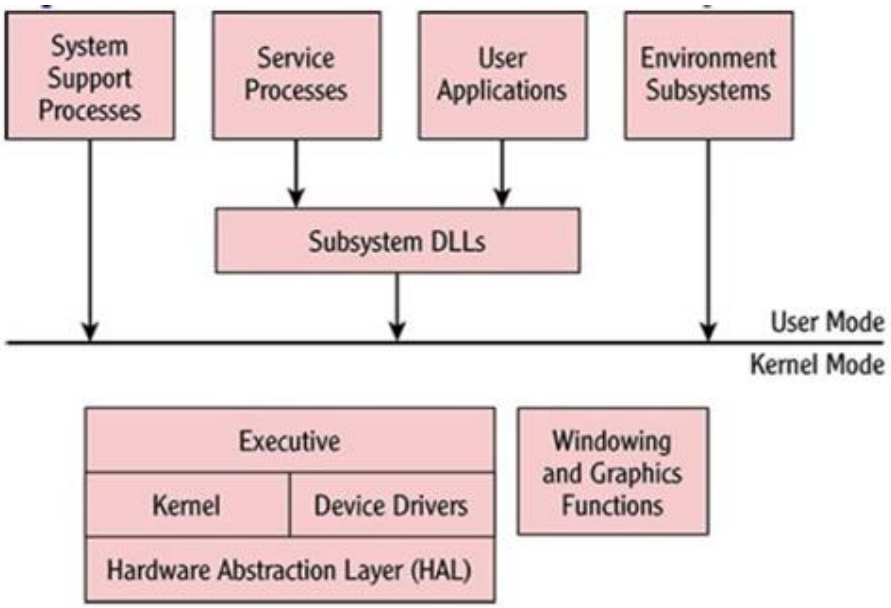
- Windows 10 (2015): Hợp nhất Windows trên nhiều thiết bị, cập nhật liên tục thay vì ra mắt phiên bản mới.

- Windows 11 (2021): Thiết kế hiện đại, hỗ trợ ứng dụng Android, cải thiện hiệu suất.

1.2.3.2 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. Chế độ nhân dành cho nhân của hệ điều hành và các chương trình mức thấp khác hoạt động. Chế độ người dùng dành cho các ứng dụng như Word, Excel và các hệ thống con hoạt động. - Subsystems: Hỗ trợ nhiều môi trường khác nhau như Windows API, POSIX, và Linux Subsystem (WSL).



Hình 2 Kiến trúc hệ điều hành Windows

Về kỹ thuật, các thao tác ở chế độ nhân được thực thi ở cấp độ thấp nhất hay chế độ đặc quyền. Các thao tác ở chế độ người dùng được thực thi ở cấp độ cao nhất hay chế độ không đặc quyền. Nói cách khác, các chế độ này hạn chế các tài nguyên máy tính mà chương trình được phép sử dụng.

1.2.3.3 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 15 khởi động (Start) và thanh tác vụ (Taskbar) như trong hình dưới đây. 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 hiện 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.

1.2.3.4 Đặc trưng cơ bản của Windows

Hệ điều hành windows có những đặc trưng cơ bản như sau:

- Tính phổ biến: Được sử dụng rộng rãi trên PC, laptop và máy chủ.

- Tương thích cao: Hỗ trợ nhiều phần mềm, phần cứng từ nhiều hãng khác nhau.

- Dễ sử dụng: Giao diện trực quan, hỗ trợ nhiều ngôn ngữ.

- Hỗ trợ đa nhiệm: Cho phép chạy nhiều ứng dụng cùng lúc.

- Bảo mật: Tích hợp Windows Defender, BitLocker, Windows Hello.

1.2.4 Phần mềm diệt virus

Phần mềm diệt virus là phần mềm có tính năng phát hiện, loại bỏ các virus máy tính, khắc phục (một phần hoặc hoàn toàn) hậu quả của virus gây ra và có khả năng được nâng cấp để nhận biết các loại virus trong tương lai.

Để đạt được các mục tiêu tối thiểu trên và mở rộng tính năng, phần mềm diệt virus thường hoạt động trên các nguyên lý cơ bản nhất như sau:

- Kiểm tra (quét) các tập tin để phát hiện các virus đã biết trong cơ sở dữ liệu nhận dạng về virus của chúng.

- Phát hiện các hành động của các phần mềm giống như các hành động của virus hoặc các phần mềm độc hại.

Các phần mềm diệt virus nổi tiếng và hiệu quả hiện nay: Kaspersky Anti-Virus, McAfee AntiVirus Plus, Malwarebytes Premium …

1.2.5 Phần mềm chống phần mềm gián điệp

Phần mềm gián điệp (spyware) là một loại phần mềm chuyên thu thập thông tin từ máy tính của người dùng qua mạng Internet mà không có sự nhận biết hoặc cho phép của họ. Thông tin thu thập thường được sử dụng cho mục đích thương mại hoặc có thể bị khai thác bởi tin tặc.

Spyware thường được cài đặt một cách bí mật như một thành phần kèm theo trong các phần mềm miễn phí (freeware) hoặc phần mềm chia sẻ (shareware) mà người dùng tải về từ Internet. Sau khi được cài đặt, spyware sẽ:

- Theo dõi và điều phối các hoạt động trên Internet của máy chủ.

- Lặng lẽ thu thập và gửi dữ liệu đến một máy khác, thường là máy chủ của các công ty quảng cáo hoặc tin tặc.

Phần mềm chống phần mềm gián điệp được phát triển để bảo vệ hệ thống khỏi các mối đe dọa từ spyware. Các tính năng chính bao gồm:

- Quét hệ thống: Phát hiện các chữ ký của spyware đã biết trên toàn bộ hệ thống.

- Theo dõi hành vi: Phát hiện hoạt động đáng ngờ của hệ thống.

- Bảo vệ thời gian thực: Ngăn chặn spyware trước khi nó xâm nhập vào hệ thống.

- Vô hiệu hóa spyware: Sử dụng thuật toán tiên tiến để ngăn chặn và loại bỏ spyware trước khi gây hại.

Việc sử dụng phần mềm chống spyware là một biện pháp quan trọng giúp bảo vệ thông tin cá nhân và duy trì sự an toàn cho hệ thống máy tính.

Các phần mềm chống phần mềm gián điệp hiện nay: SentinelOne, Malwarebytes, Bitdefender, …

1.2.6 Phần mềm cứu hộ

Phần mềm cứu hộ là các công cụ được thiết kế để khắc phục sự cố hệ thống, khôi phục dữ liệu, sửa lỗi ổ cứng, diệt virus hoặc giúp máy tính hoạt động trở lại sau khi gặp sự cố nghiêm trọng. Những phần mềm này thường được sử dụng khi hệ điều hành bị lỗi, không thể khởi động hoặc bị nhiễm mã độc. Phần mềm cứu hộ có thể cung cấp nhiều chức năng quan trọng như:

- Khôi phục dữ liệu: Giúp lấy lại dữ liệu bị xóa, format nhầm hoặc bị mất do lỗi hệ thống.

- Sửa lỗi hệ thống: Sửa lỗi khởi động Windows, lỗi phân vùng, lỗi ổ cứng.

- Diệt virus và phần mềm độc hại: Quét và loại bỏ virus, malware khỏi hệ thống.

- Tạo và phục hồi bản sao lưu: Giúp khôi phục hệ điều hành về trạng thái ổn định trước đó.

- Quản lý phân vùng ổ cứng: Hỗ trợ chia lại ổ đĩa, khôi phục phân vùng bị mất.

Các loại phần mềm cứu hộ phổ biến :

- Hiren’s BootCD: Bộ công cụ cứu hộ toàn diện cho Windows, bao gồm khôi phục dữ liệu, sửa lỗi hệ thống và kiểm tra phần cứng.

- MiniTool Partition Wizard: Quản lý và khôi phục phân vùng ổ cứng.

- Kaspersky Rescue Disk: Diệt virus mạnh mẽ khi Windows không thể khởi động.

CHƯƠNG 2. NỘI DUNG BÀI THỰC HÀNH

2.1 Chuẩn bị môi trường

- File cài đặt Windows 10 định dạng iso.

- Phần mềm ảo hóa VMWare Workstation.

2.2 Các bước thực hiện

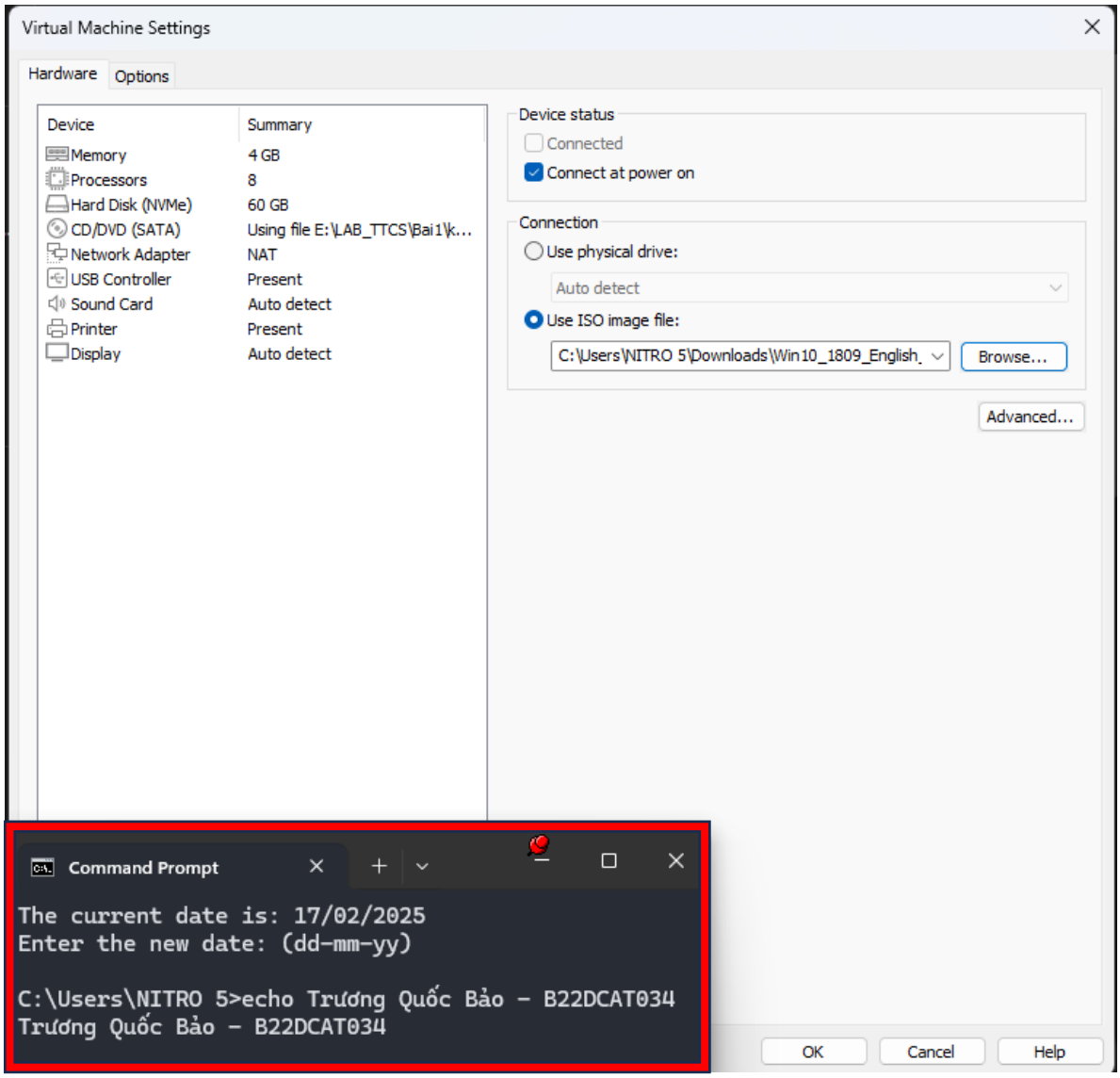
2.2.1 Cài đặt và chuẩn bị máy ảo Windows 10

Tải file iso Windows 10 trên trang chủ của Microsoft và thực hiện các bước để có thể cài đặt và cấu hình cho máy ảo Windows 10.

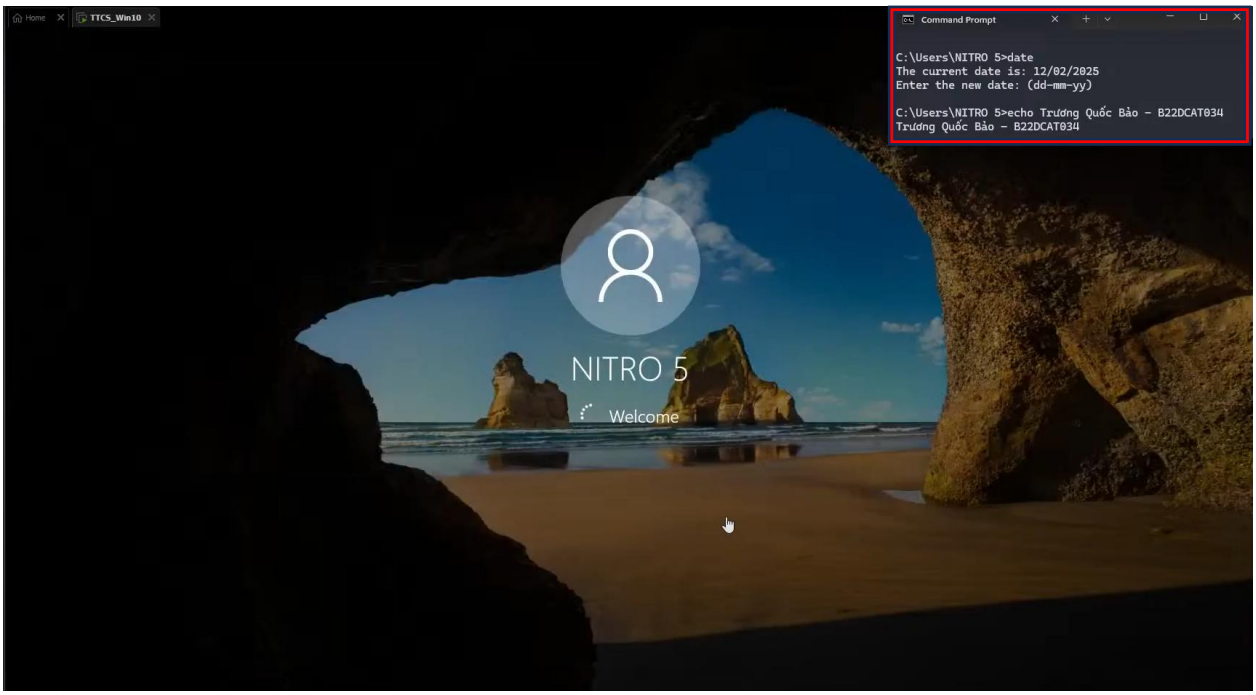
Bước 1: Chọn File → New Vitual Machine để mở cửa sổ New Virtual Wizard → Typical → Next

Bước 2: Chọn file iso Windows 10 đã tải về → Next và tiến hành cài đặt

Bước 3: Cấu hình cho Windows 10 như hình bên dưới

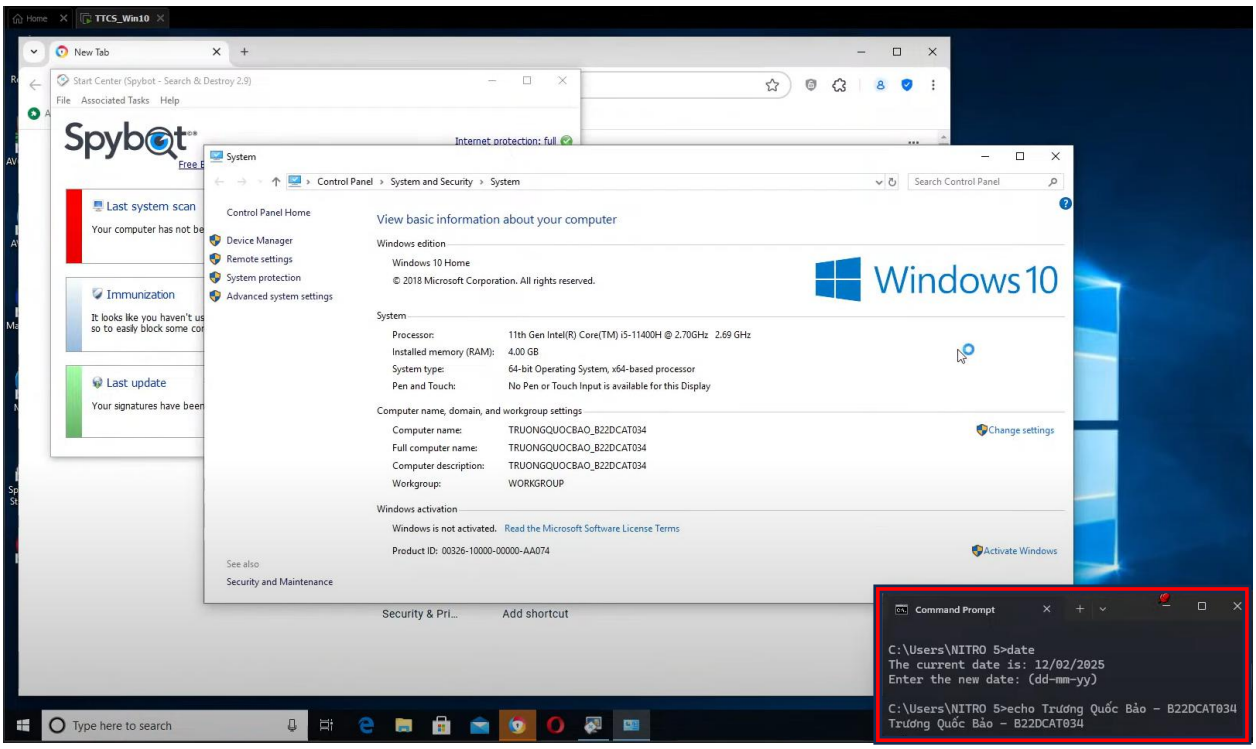


Hình 3 Cấu hình cho file iso của Windows 10



Hình 4 Cài đặt và khởi động Windows 10 thành công

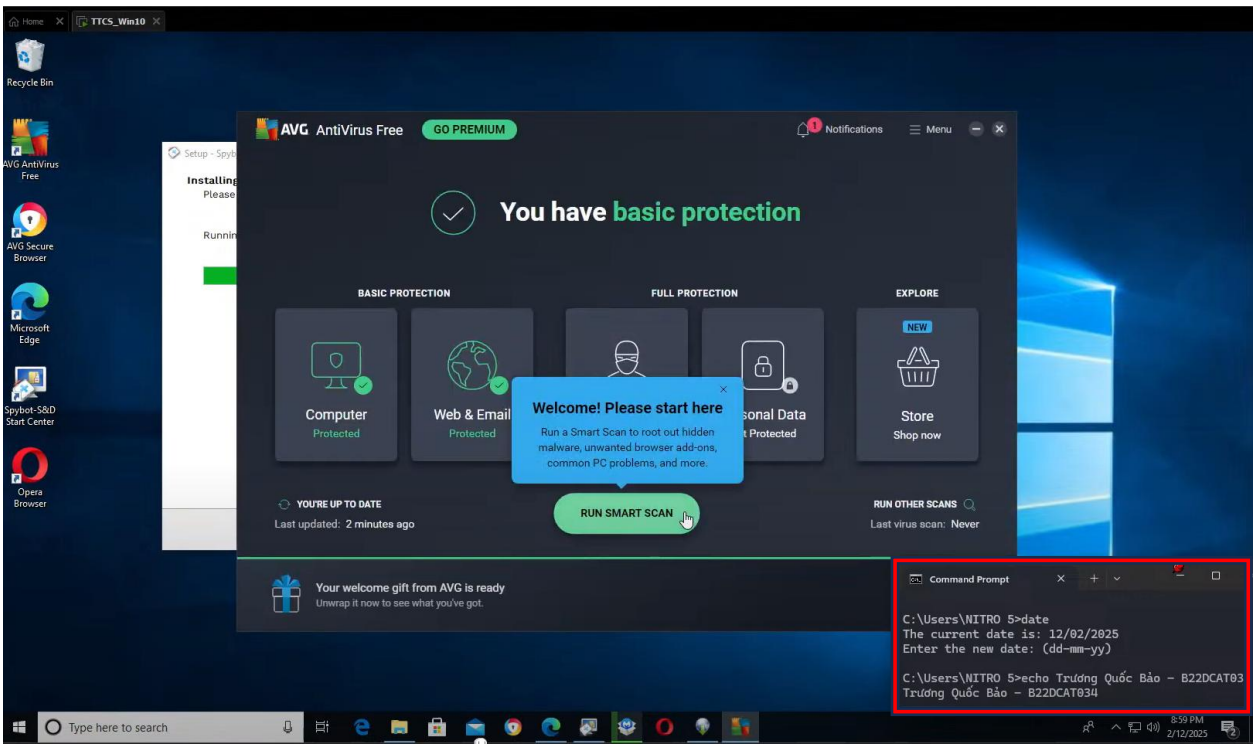
Trong mục "System Properties" đổi tên máy trạm Windows thành "họ tên SV_mã SV".



Hình 5 Đổi tên máy trạm thành tên và MSV tương ứng

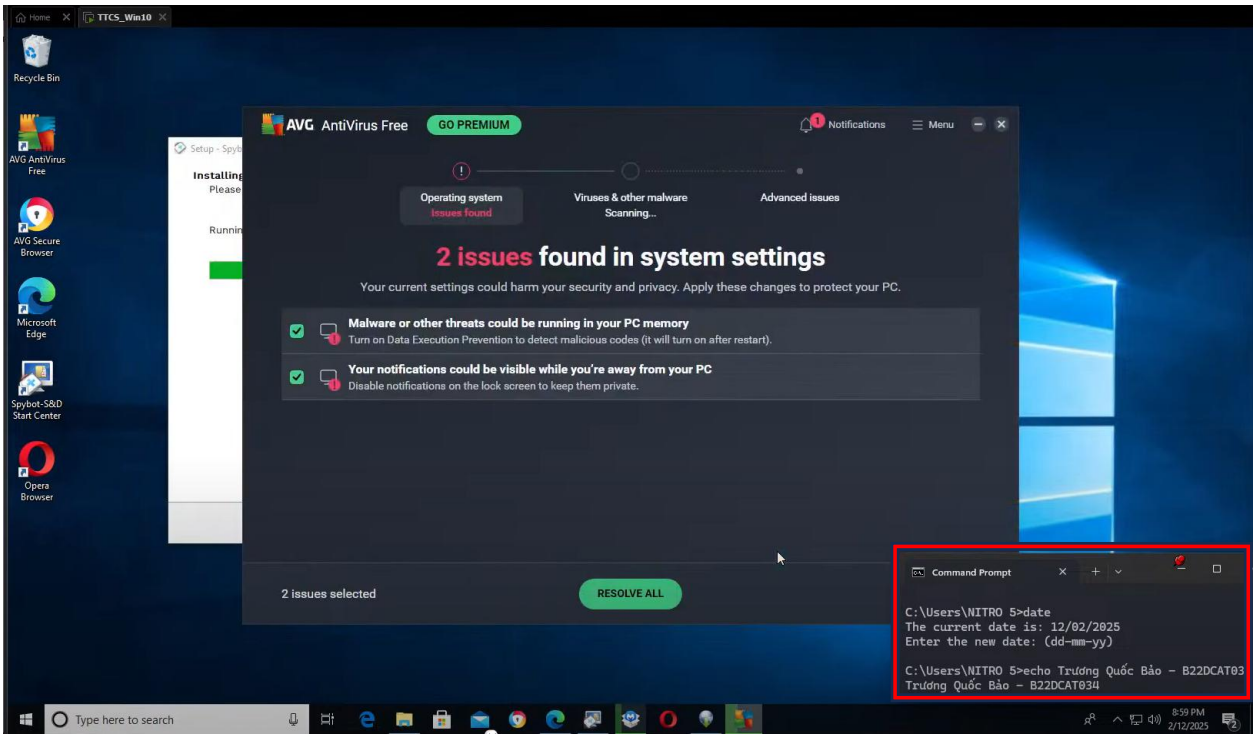
2.2.2 Cài đặt và chạy phần mềm diệt virus AVG Antivirus

Tìm kiếm "AVG Antivirus" trên trình duyệt tìm kiếm, và tiến hành cài đặt về máy trạm. Sau khi cài đặt thành công và chạy phần mềm, giao diện của AVG Antivirus sẽ hiển thị như hình bên dưới.



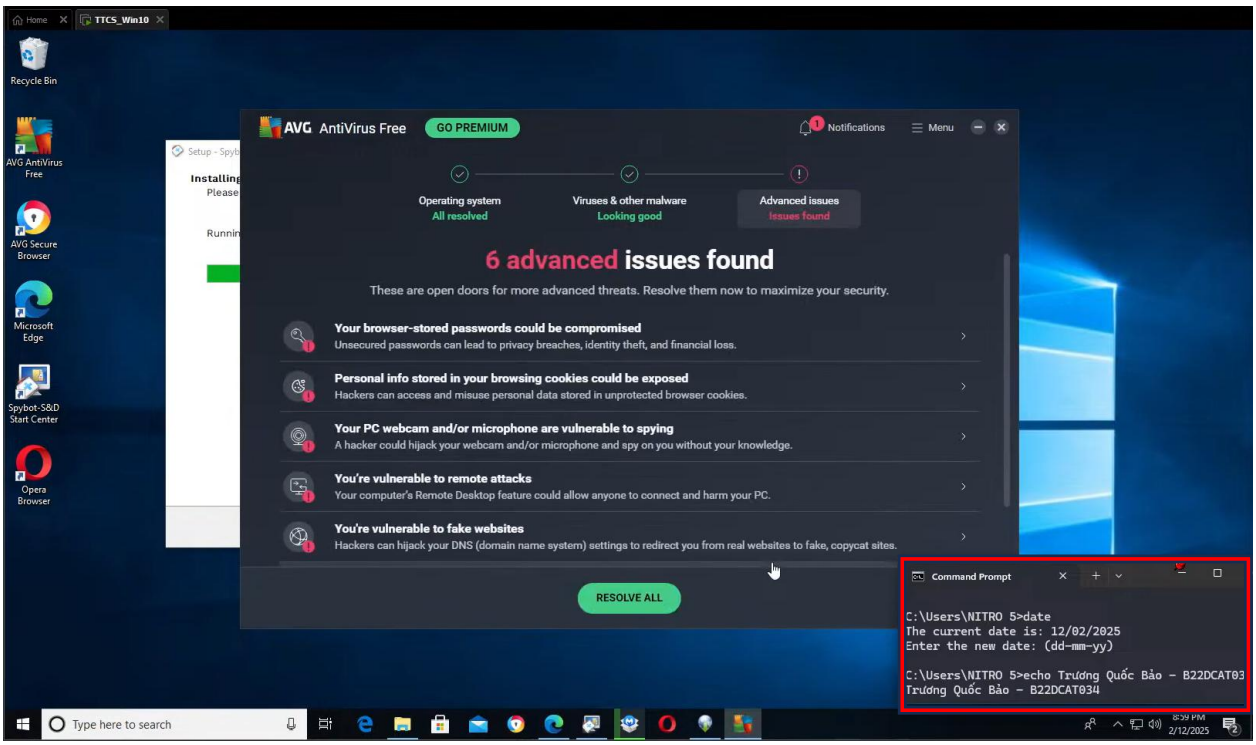
Hình 6 Cài đặt và mở phần mềm AVG Antivirus

Nhấp chọn "RUN SMART SCAN" để tiến hành quét virus



Hình 7 Tiến hành scan virus

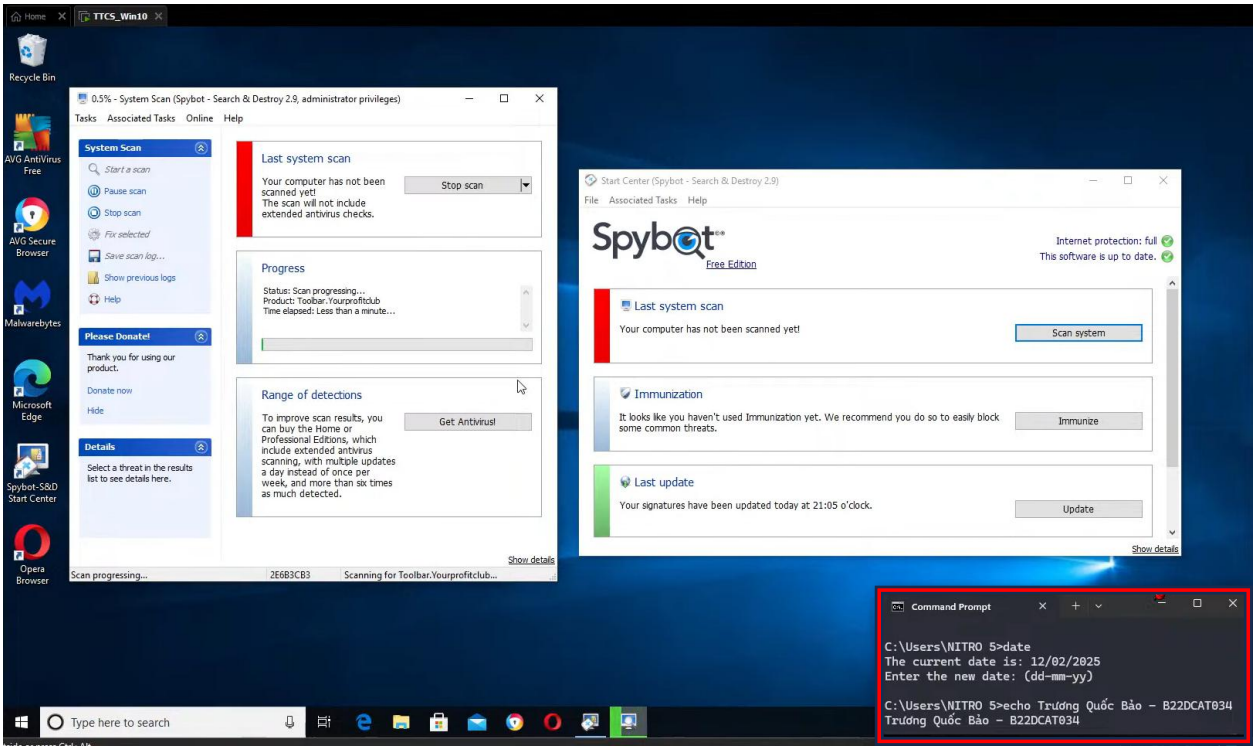
Sau khi hoàn thành, kết quả quét sẽ hiển thị như hình bên dưới:



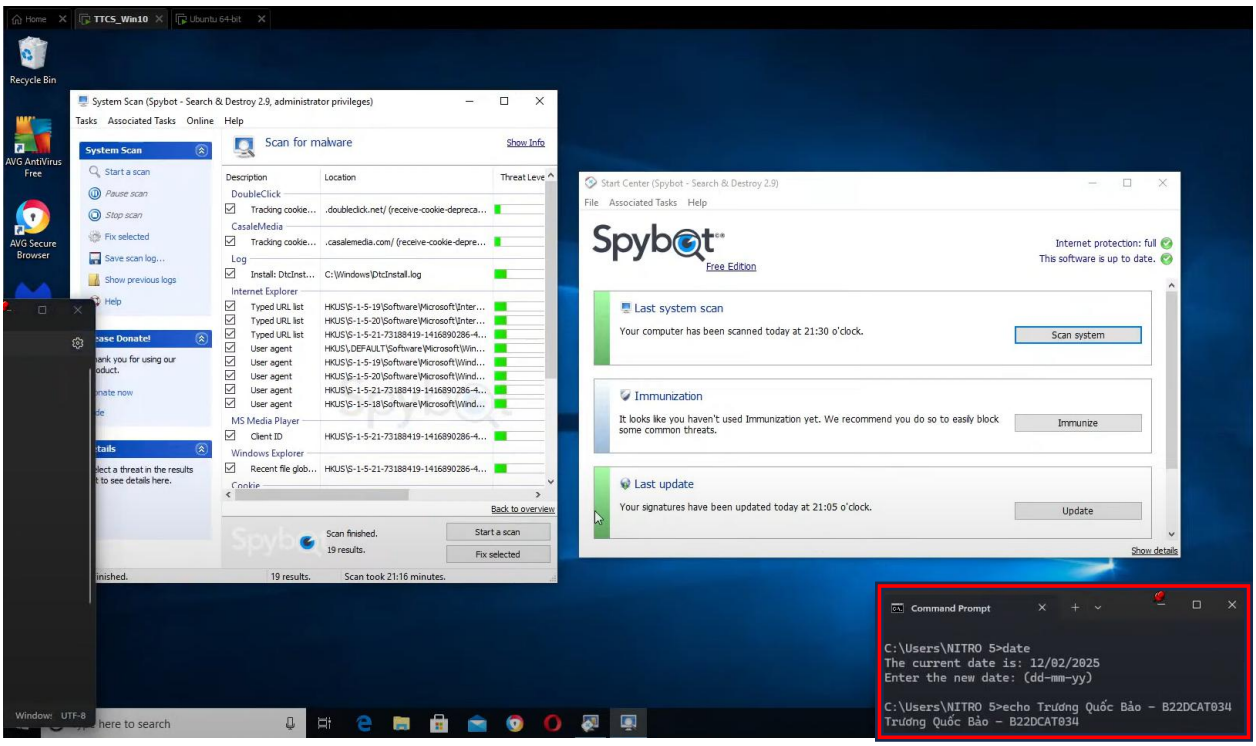
Hình 8 Công cụ AVG Antivirus quét thành công

2.2.3 Phần mềm chống phần mềm gián điệp Spybot S&D

Tìm kiếm "Spybot S&D" trên trình duyệt tìm kiếm, tải xuống và tiến hành cài đặt. Khi chạy phần mềm, giao diện sẽ hiển thị như hình bên dưới. Chọn "Scan system" để tiến hành quét các phần mềm gián điệp.



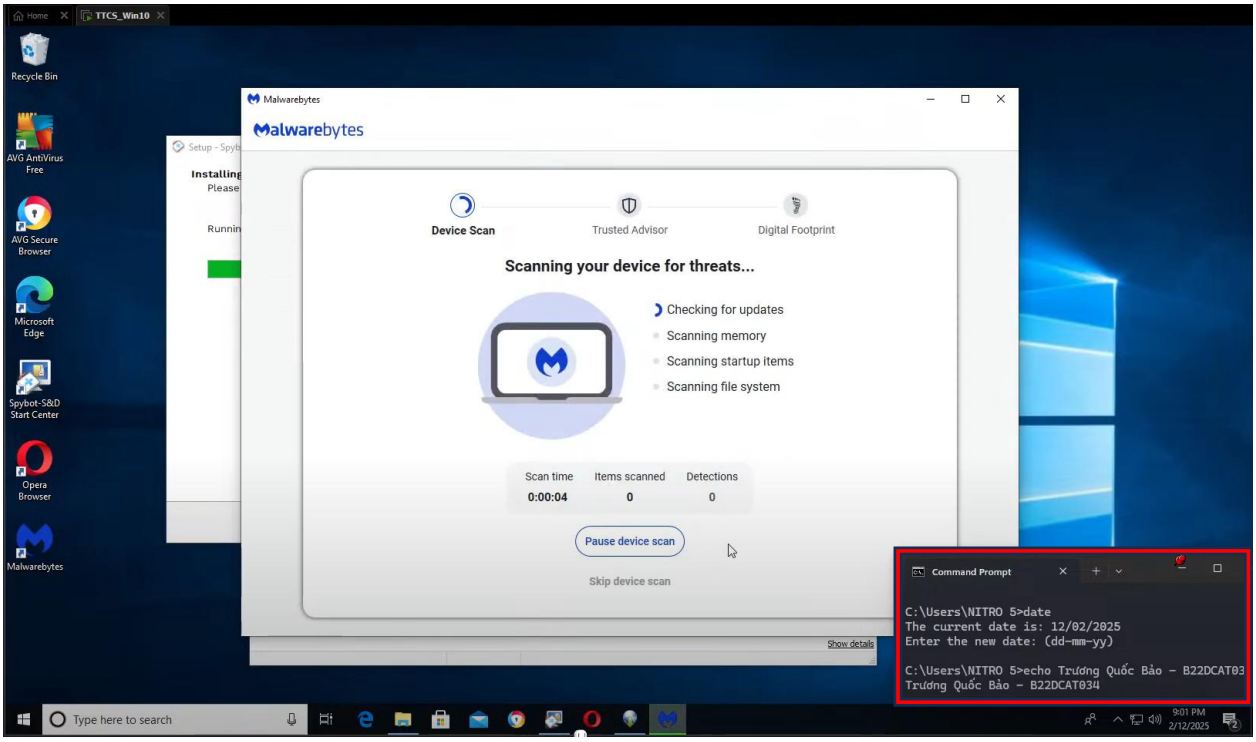
Hình 9 Cài đặt và tiến hành sử dụng phần mềm Spybot S&D



Hình 10 Công cụ Spybot S&D quét thành công

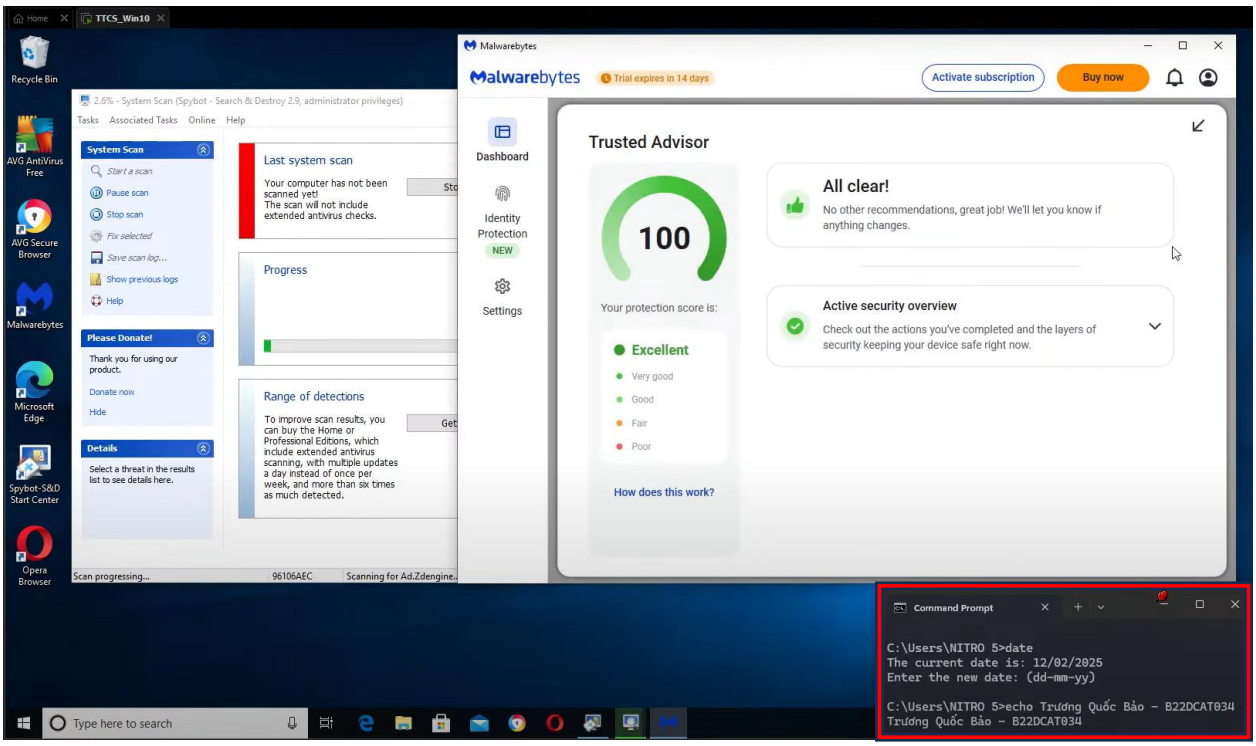
2.2.4 Phần mềm chống các phần mềm độc hại Malwarebytes

Tìm kiếm "Malwarebytes" trên trình duyệt tìm kiếm, cài đặt và tiến hành khởi động ứng dụng. Chọn "Device scan" để quét mã độc trong máy.



Hình 11 Cài đặt và tiến hành sử dụng phần mềm Malwarebytes

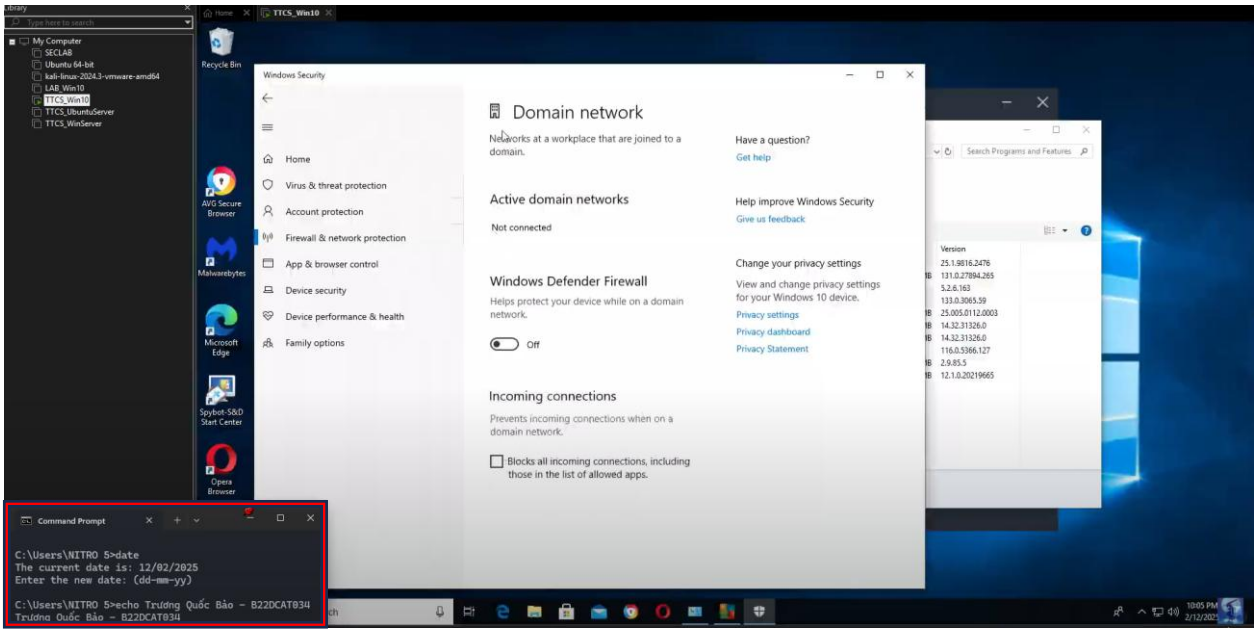
Kết quả sau khi quét sẽ hiển thị, đi kèm điểm tin cậy (Trusted Advisor) của phần mềm đánh giá cho máy trạm.



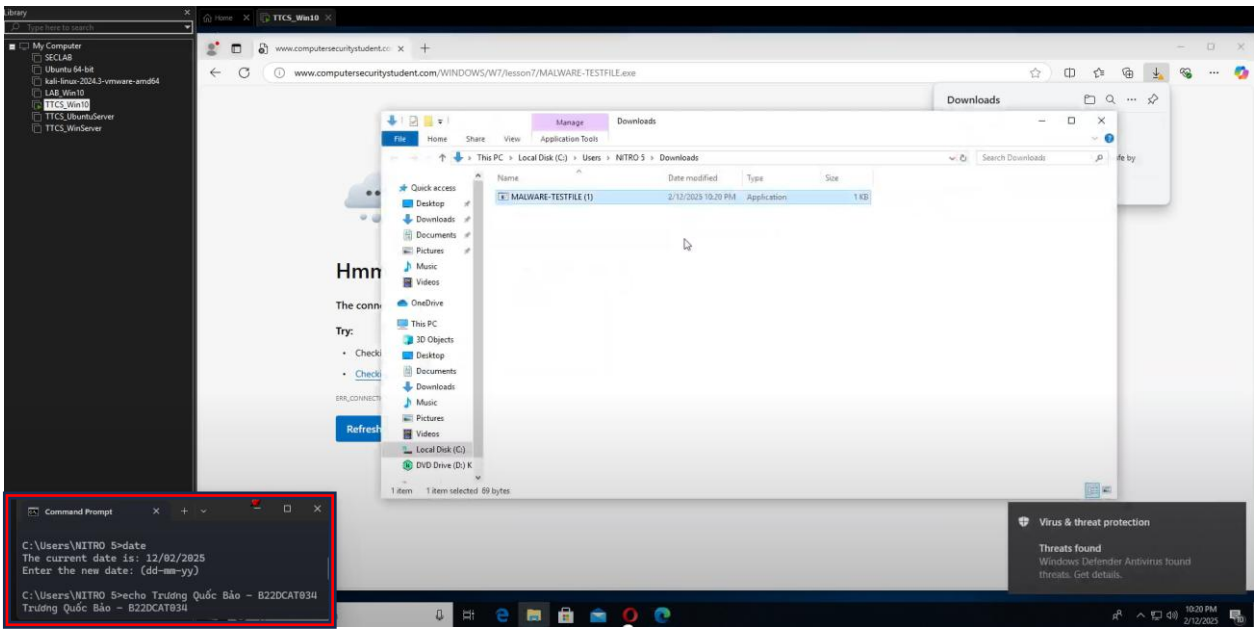
Hình 12 Công cụ Malwarebytes quét thành công

2.2.5 Phần mềm cứu hộ Kaspersky Rescure Disk

Trước khi tiến hành tải file mã độc về máy, phải tắt các hệ thống bảo mật của Windows. Do các phiên bản mới của Windows cung cấp tường lửa và hệ thống tự động scan mã độc mạnh mẽ, các file mã độc dùng để làm mẫu có thể bị chặn.



Hình 13 Tắt tường lửa và hệ thống scan virus tự động của Windows



Hình 14 Lưu file mã độc về ổ C:

Các bước cài đặt và sử dụng phần mềm cứu hộ Kaspersky Rescure Disk:

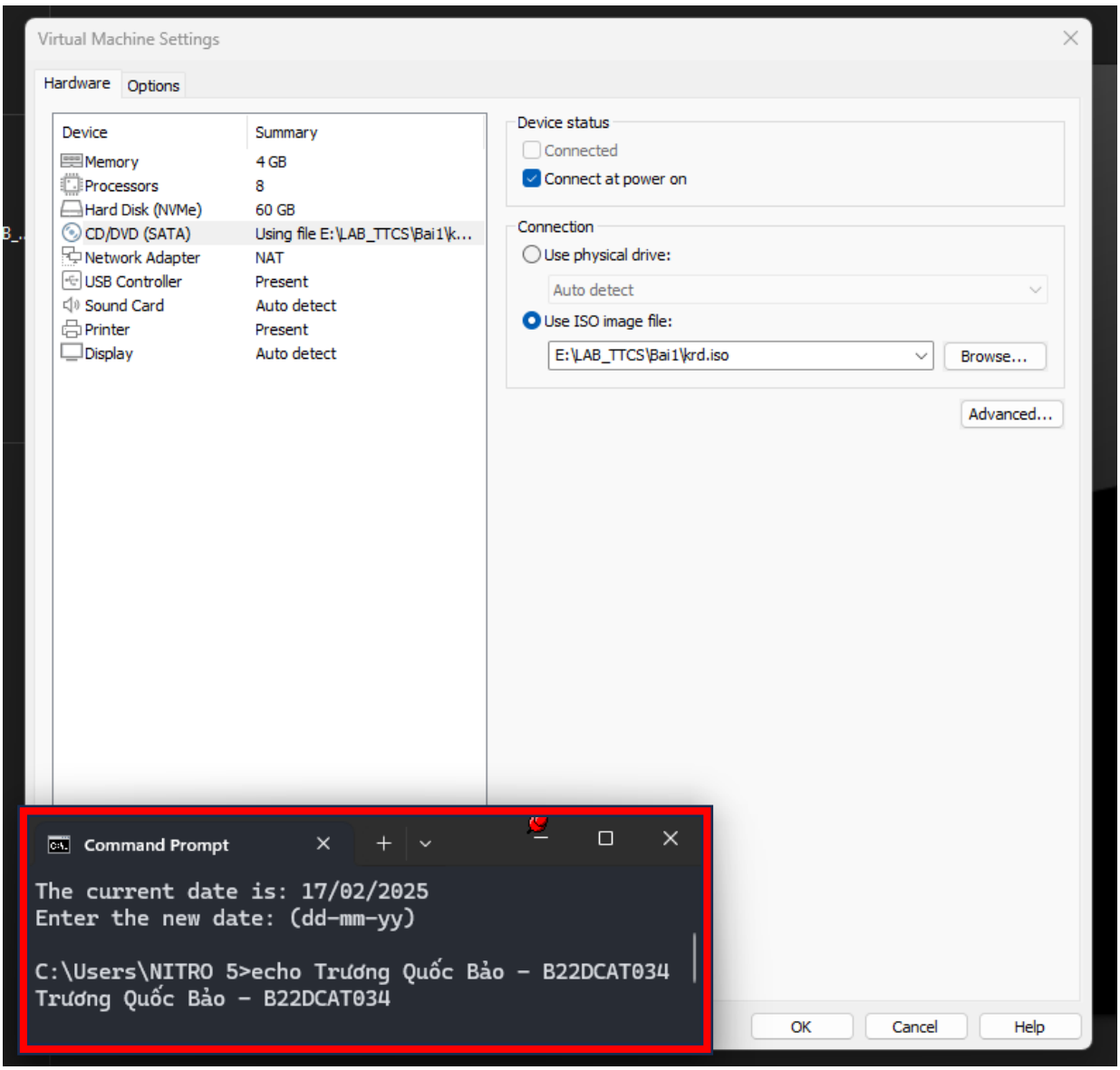
Bước 1: Tải file iso của phần mềm cứu hộ KRD theo đường link có sẵn

Bước 2: Chọn vào phần cấu hình của máy ảo Windows 10, chọn file iso file tương ứng với phần mềm cứu hộ. Chọn OK

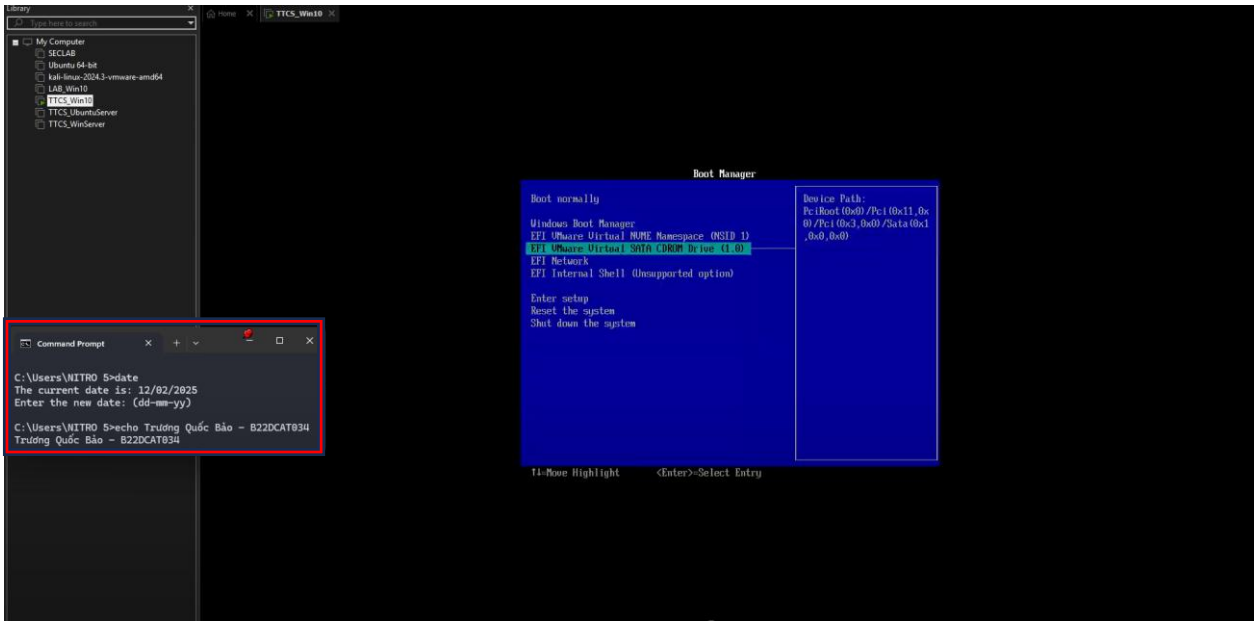
Bước 3: Khởi động máy ảo, nhấn liên tục “ESC” để vào Boot Manager

Bước 4: Dùng mũi tên chọn CD ROM (nơi chứa file phần mềm cứu hộ)

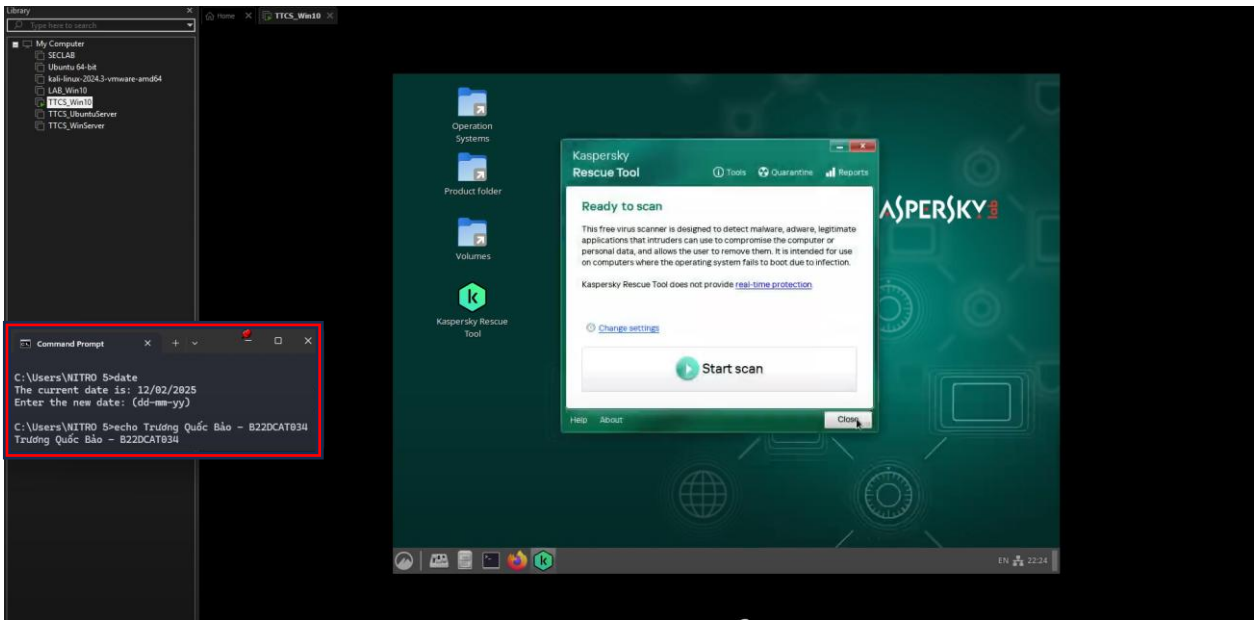
Bước 5: Cài đặt và sử dụng phần mềm KRD



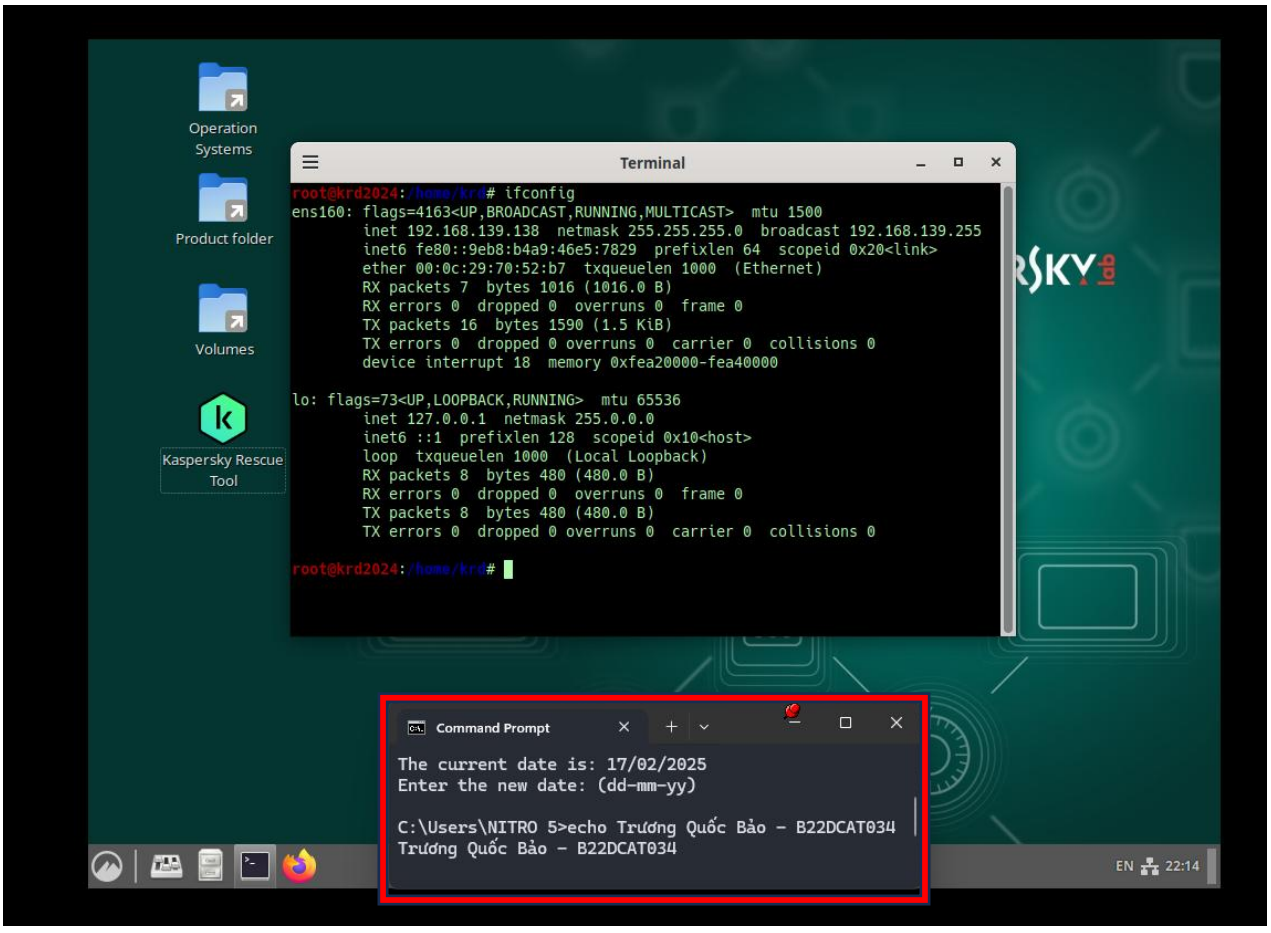
Hình 15 Chọn file iso của phần mềm cứu hộ



Hình 16 Boot vào đĩa CD của file cứu hộ

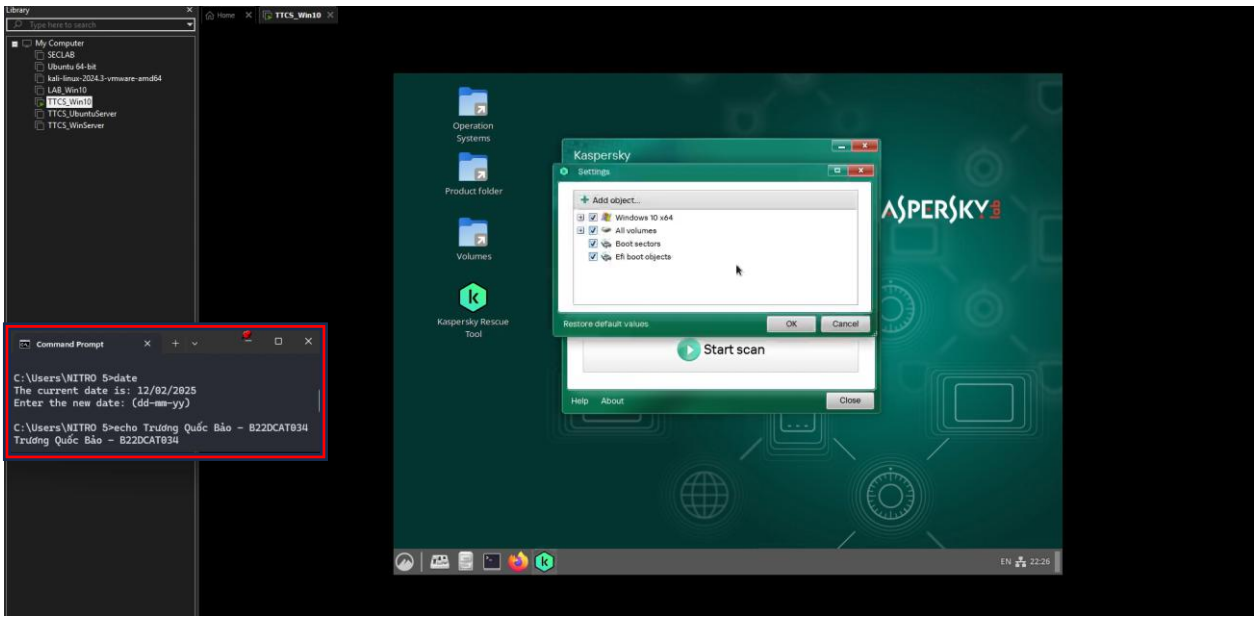


Hình 17 Boot thành công vào phần mềm cứu hộ

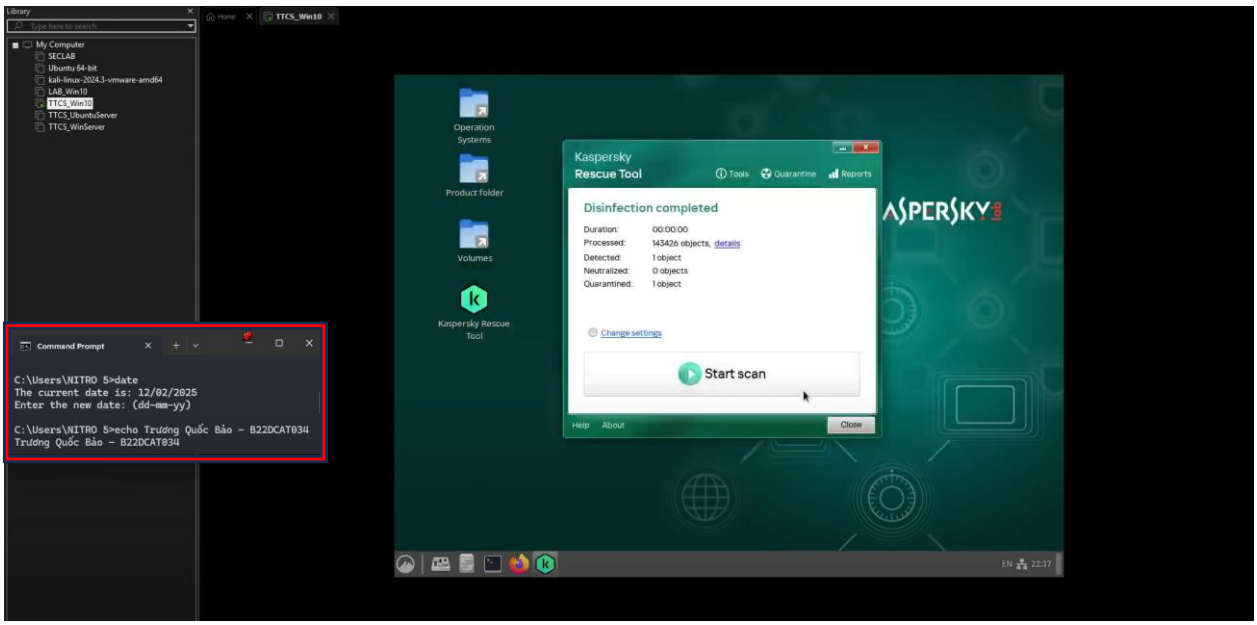


Hình 18 Kiểm tra địa chỉ IP trên máy

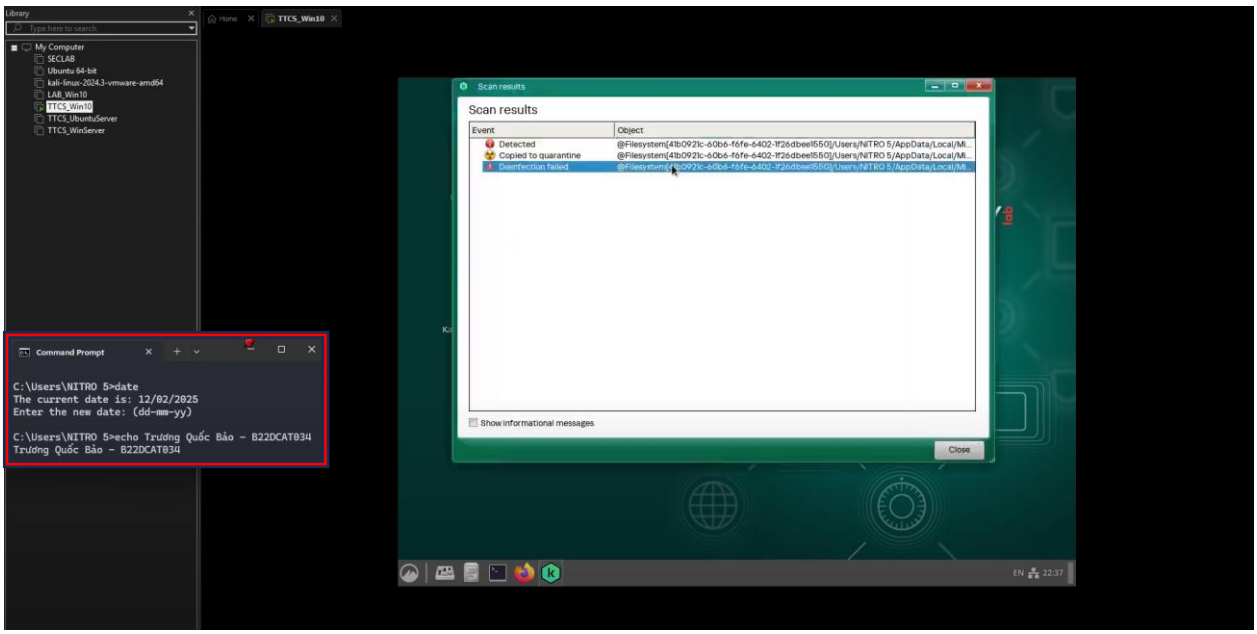
Chú ý: Phải chọn “All volume” trong phần “Setting” của công cụ KRD tools mới có thể phát hiện file mã độc nằm trong máy Windows



Hình 19 Chọn quét tất cả ổ đĩa

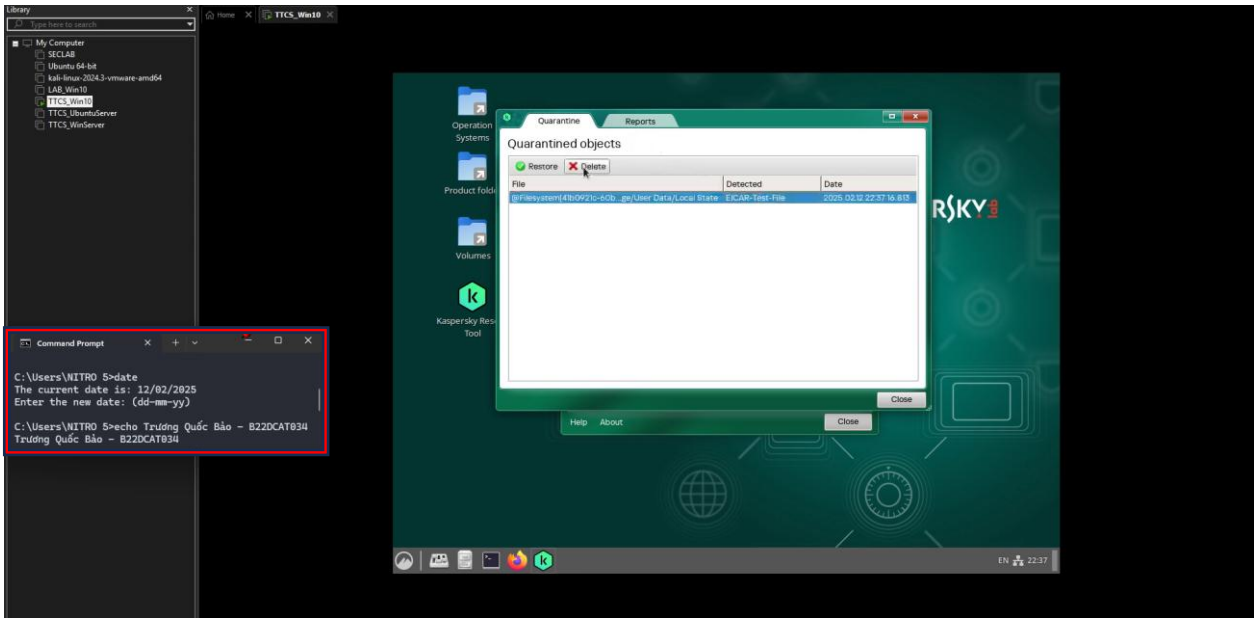


Hình 20 Bắt đầu quét



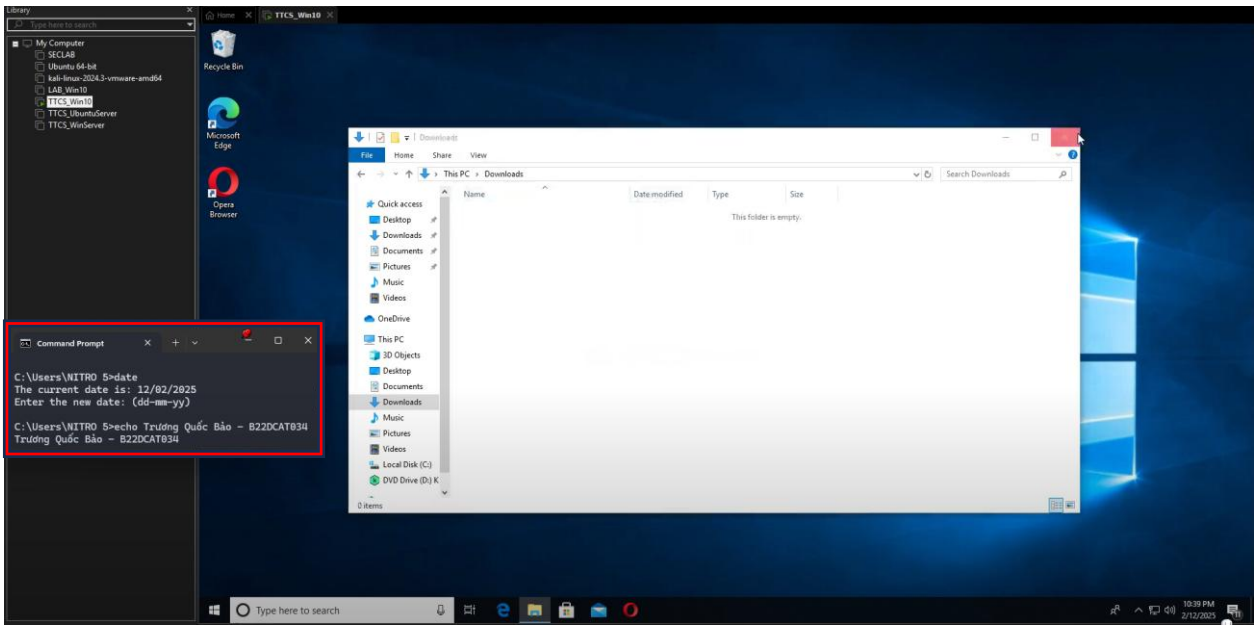
Hình 21 Phát hiện file mã độc

Sau khi phần mềm KRD tools tiến hành quét và phát hiện file mã độc, phần mềm sẽ tự đưa file mã độc sang trạng thái cách ly "Quarantine". Chúng ta có thể xem chi tiết các đối tượng "Object" được cách ly và lựa chọn xóa "Delete".



Hình 22 Tiến hành xóa file mã độc

Sau khi đã xóa thành công file mã độc, tiến hành tắt máy ảo. Trong quá trình bật lại máy ảo, để VMWare tự boot vào Windows 10 bình thường. Mở thư mục đã tải file mã độc trong máy Windows và kiểm tra.



Hình 23 File mã độc đã không còn ở máy Windows

KẾT LUẬN

- Hiểu về lịch sử, kiến trúc, giao diện và các đặc trưng của hệ điều hành Windows

- Nắm được kiến thức về ảo hóa và các phần mềm ảo hóa, cụ thể là phần mềm VMWare Workstation

- HIểu định nghĩa, cách cài đặt, cách sử dụng các phần mềm bảo vệ máy trạm: phần mềm diệt virus – AVG Antivirus, phần mềm chống phần mềm gián điệp – Spybot S&D, phần mềm chống các phần mềm độc hại – Malwarebytes, phần mềm cứu hộ - Kaspersky Rescue Disk.

TÀI LIỆU THAM KHẢO

[1] Thầy Phạm Hoàng Duy, Thầy Đinh Trường 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] Wikipedia.

[5] http://www.computersecuritystudent.com/

[4] https://learn.microsoft.com/