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:

B22DCAT251 Đặng Đức Tài

Giảng viên hướng dẫn: TS. Phạm Hoàng Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

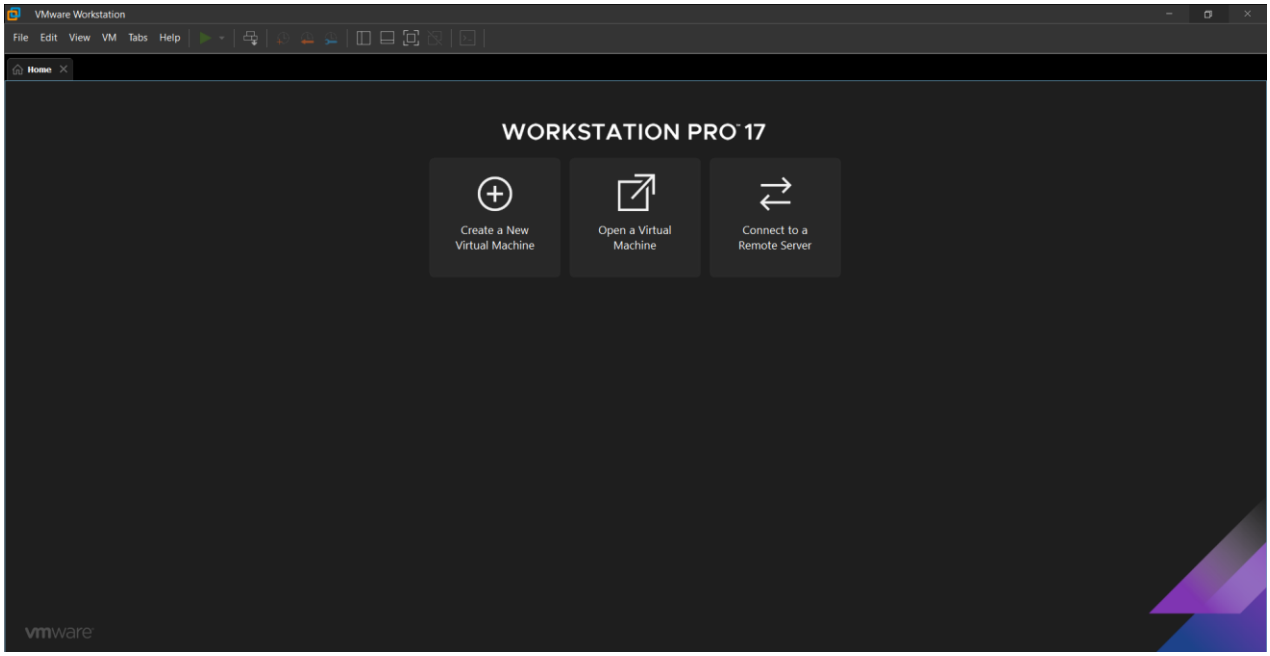
- Rèn luyện kỹ năng cài đặt và quản trị hệ điều hành máy trạm Windows cho người dùng với các dịch vụ cơ bản.

1.2 Tìm hiểu lý thuyết

1.2.1 Tìm hiểu về các phần mềm ảo hóa

1.2.1.1 VMWare Workstation

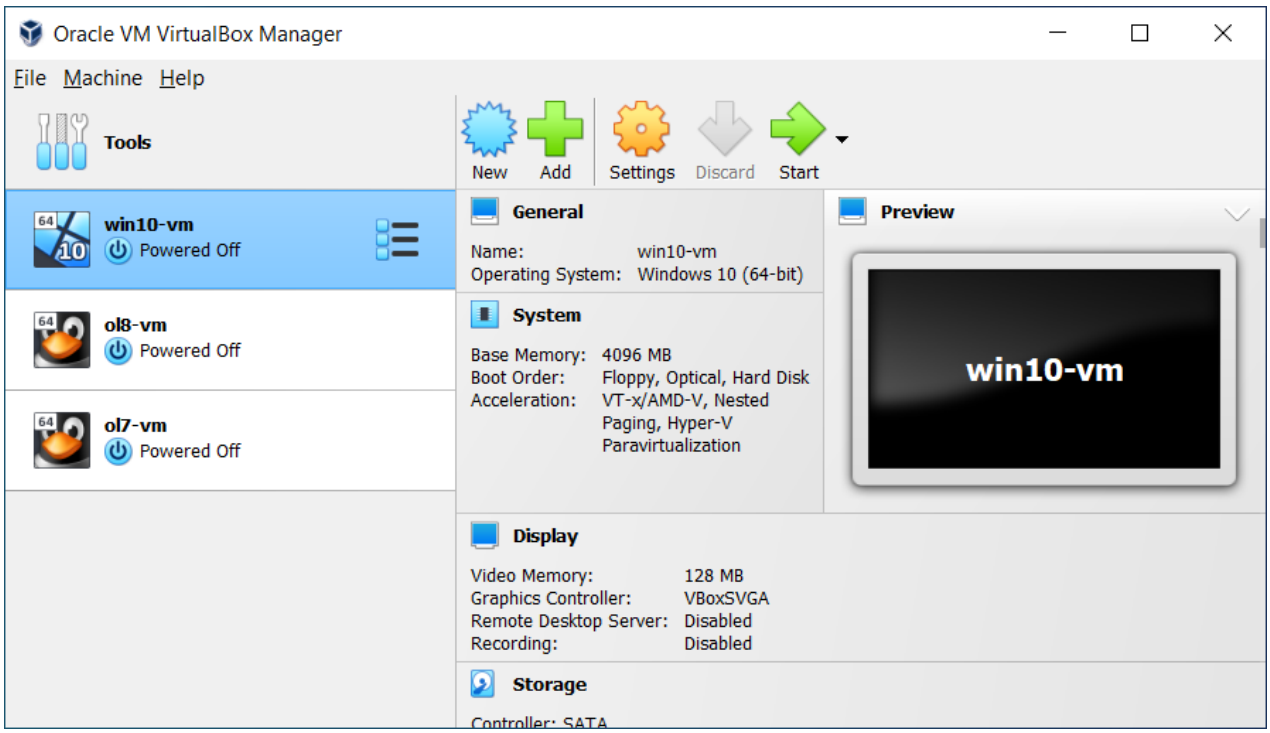
- VMWare Workstation là một trong những phần mềm ảo hóa mạnh mẽ và phổ biến nhất hiện nay. Phần mềm này cho phép người dùng chạy nhiều hệ điều hành trên một máy tính vật lý, giúp dễ dàng kiểm thử, phát triển phần mềm hoặc mô phỏng môi trường làm việc. Một số tính năng nổi bật của VMWare Workstation bao gồm *snapshot* (lưu trạng thái máy ảo để có thể khôi phục nhanh khi cần), *clone* (sao chép máy ảo), và khả năng chia sẻ máy ảo giữa các hệ thống khác nhau. Ngoài ra, VMWare Workstation hỗ trợ tối ưu hóa hiệu suất phần cứng, giúp hệ điều hành khách chạy mượt mà hơn.



Hình 1 Giao diện đồ họa của VMWare Workstation

1.2.1.2 Oracle VirtualBox

- Bên cạnh đó, VirtualBox là một lựa chọn ảo hóa miễn phí, mã nguồn mở do Oracle phát triển. VirtualBox cũng hỗ trợ nhiều hệ điều hành như Windows, Linux, macOS, nhưng có ưu điểm là nhẹ, dễ sử dụng và tương thích với nhiều định dạng ổ đĩa ảo. Tuy nhiên, so với VMWare Workstation, VirtualBox có hiệu suất thấp hơn và không tối ưu phần cứng bằng, nhưng vẫn là một công cụ hữu ích cho những ai muốn sử dụng ảo hóa mà không tốn phí.

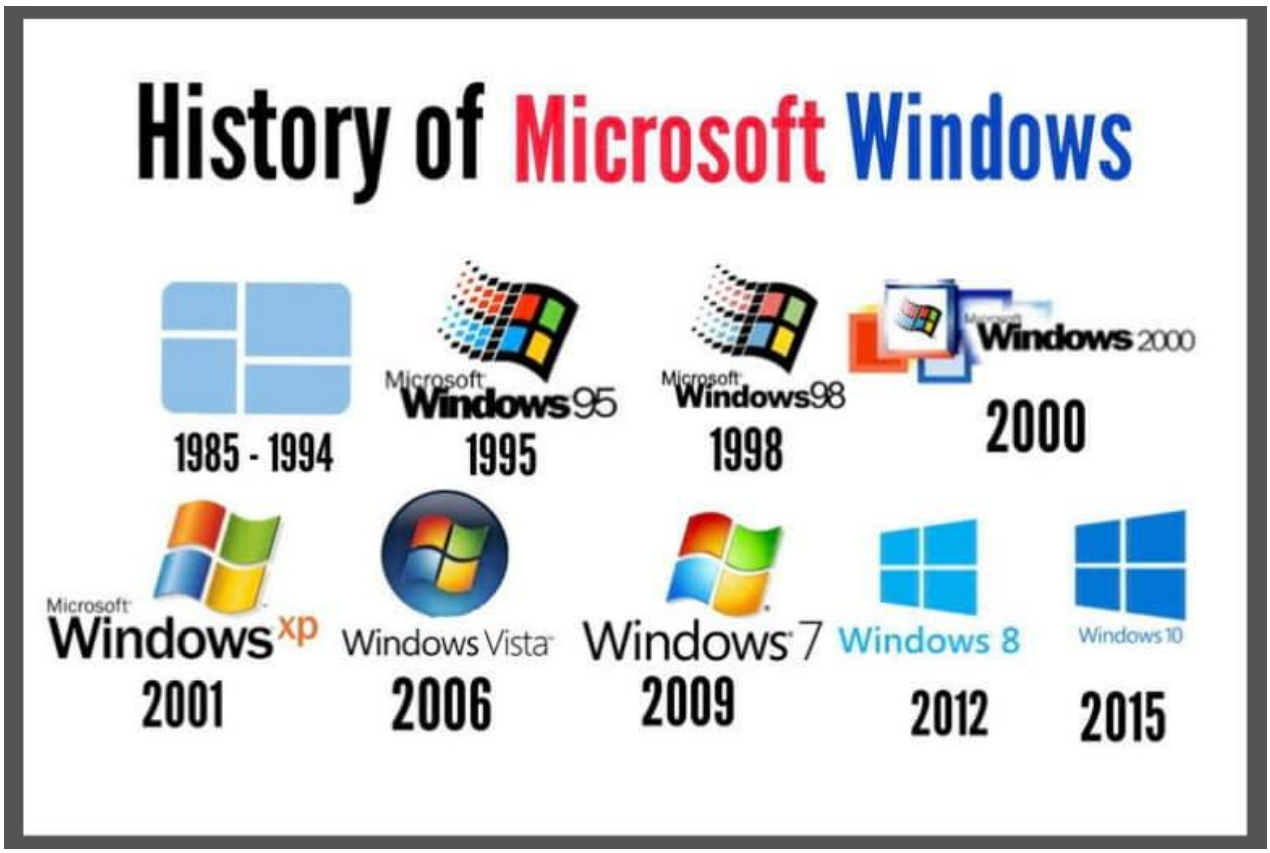


Hình 2 Giao diện đồ họa của VirtualBox

1.2.2 Tìm hiểu về hệ điều hành Windows

1.2.2.1 Lịch sử

- Windows là hệ điều hành do Microsoft phát triển, lần đầu tiên ra mắt vào năm 1985 với phiên bản Windows 1.0. Trải qua nhiều phiên bản quan trọng như Windows 95, Windows XP, Windows 7, Windows 10 và mới nhất là Windows 11, hệ điều hành này đã trở thành nền tảng phổ biến nhất trên máy tính cá nhân và doanh nghiệp.



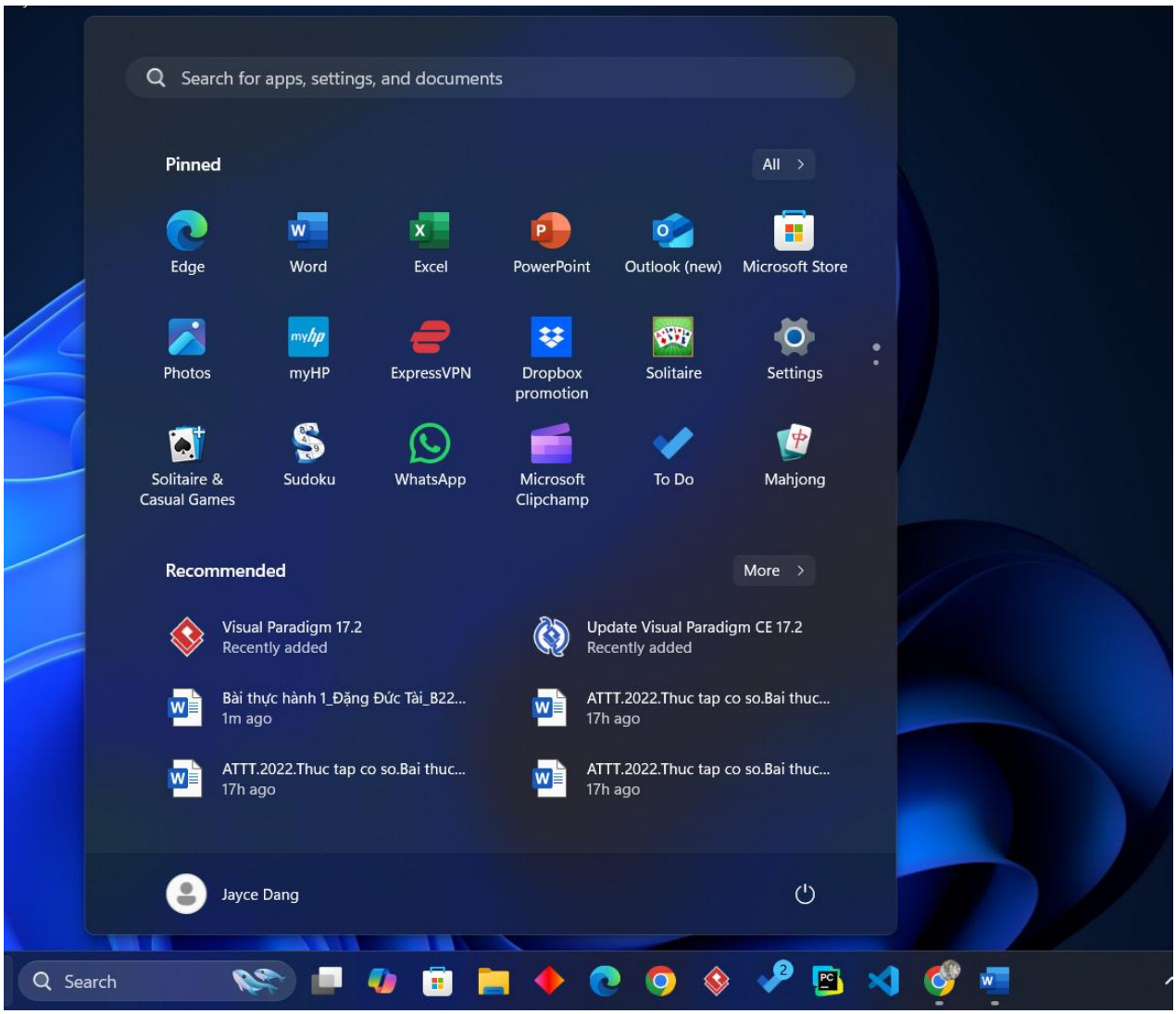
Hình 3 Lịch sử phát triển của hệ điều hành Windows

1.2.2.2 Kiến trúc

- Về mặt kiến trúc, Windows được thiết kế theo bốn tầng chính: *Kernel* (Nhân hệ điều hành) chịu trách nhiệm quản lý tài nguyên hệ thống; *HAL* (Hardware Abstraction Layer) hoạt động như một tầng trung gian giữa phần cứng và hệ điều hành; *User Mode* là nơi các ứng dụng và giao diện người dùng hoạt động; và *Driver* giúp hệ điều hành giao tiếp với các thiết bị phần cứng. Hệ thống tập tin phổ biến mà Windows hỗ trợ bao gồm NTFS, FAT32 và exFAT.

1.2.2.3 Giao diện

- Giao diện của Windows được thiết kế thân thiện với người dùng, với Start Menu, Taskbar và File Explorer giúp thao tác nhanh chóng. Windows 11 còn được cải tiến với thiết kế bo tròn các góc, hiệu ứng mượt mà và hỗ trợ chế độ Dark Mode giúp giảm mỏi mắt.



Hình 4 Giao diện của hệ điều hành Windows

1.2.2.4 Đặc điểm

- Những đặc điểm nổi bật của Windows bao gồm tính đa nhiệm, hỗ trợ mạnh mẽ cho DirectX giúp tối ưu hóa trải nghiệm chơi game và xử lý đồ họa, cũng như tính bảo mật được nâng cao với Windows Defender và BitLocker. Ngoài ra, hệ điều hành này có độ tương thích cao với hầu hết các phần mềm phổ biến hiện nay.

1.3 Tìm hiểu về các phần mềm

1.3.1 Phần mềm diệt virus

- Một trong những phần mềm quan trọng nhất trên máy tính là phần mềm diệt virus, giúp bảo vệ hệ thống khỏi các mối đe dọa như virus, mã độc và ransomware. Một số phần mềm phổ biến có thể kể đến như Windows Defender, Kaspersky, Avast, Bitdefender. Các phần mềm này cung cấp tính năng quét virus theo thời gian thực, bảo vệ email, tường lửa nâng cao và quét định kỳ để phát hiện các mối nguy hại tiềm ẩn.

Hình 5 Các phần mềm diệt virus phổ biến

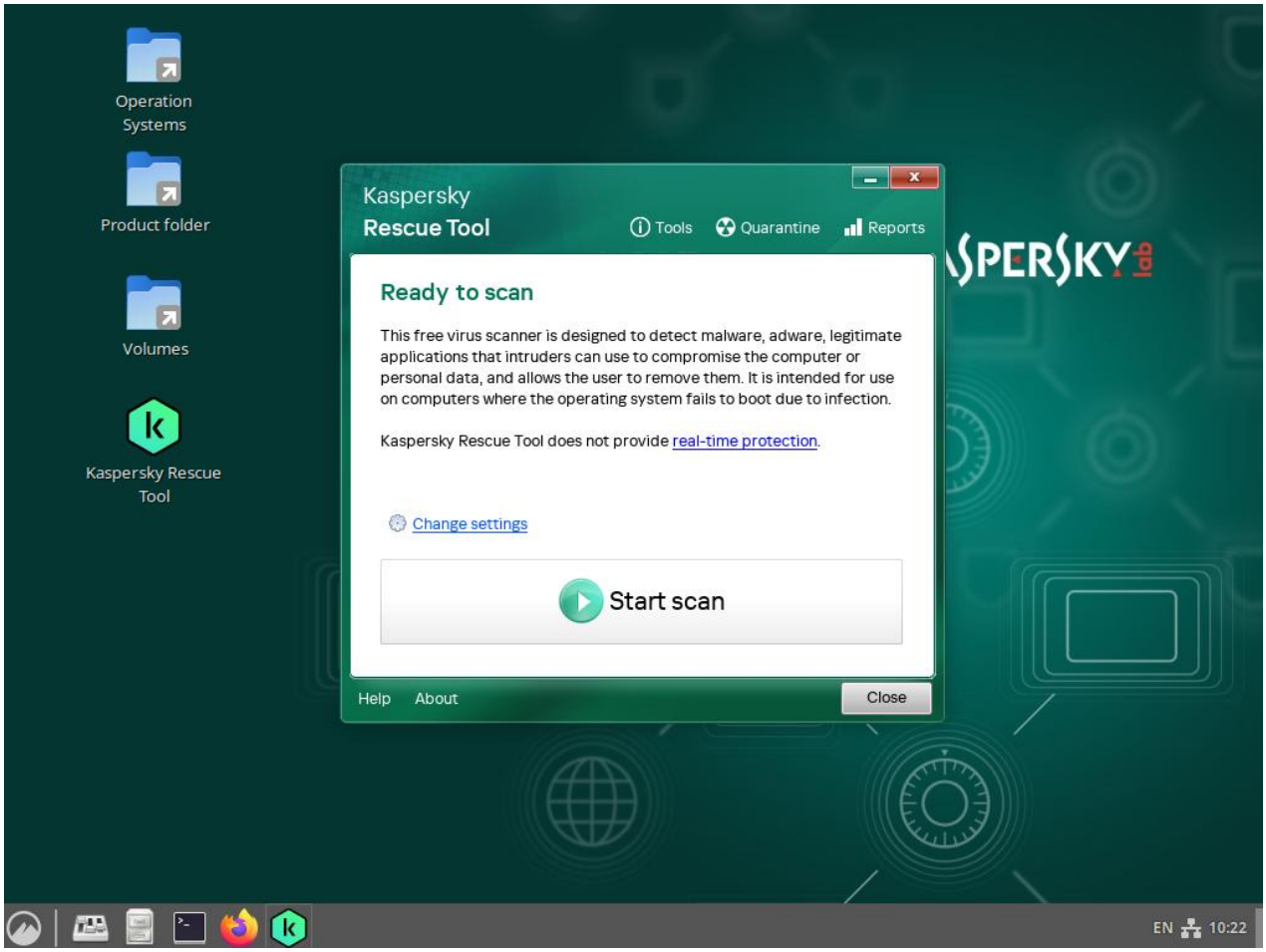
1.3.2 Phần mềm chống phần mềm gián điệp

- Bên cạnh đó, phần mềm chống phần mềm gián điệp giúp bảo vệ dữ liệu cá nhân và thông tin nhạy cảm khỏi bị theo dõi trái phép. Một số công cụ như Malwarebytes, Spybot Search & Destroy, SUPERAntiSpyware có thể phát hiện và loại bỏ các phần mềm gián điệp, bảo vệ quyền riêng tư của người dùng.

Hình 6 Giao diện của phần mềm Spybot Search & Destroy

1.3.3 Phần mềm cứu hộ

- Phần mềm cứu hộ đóng vai trò quan trọng khi hệ thống gặp sự cố. Các công cụ như Kaspersky Rescue Disk (KRD), Hiren's BootCD, MiniTool Partition Wizard, EaseUS Data Recovery giúp khôi phục dữ liệu bị mất, sửa lỗi hệ thống, thậm chí có thể khởi động từ USB để xử lý sự cố khi Windows không hoạt động bình thường.



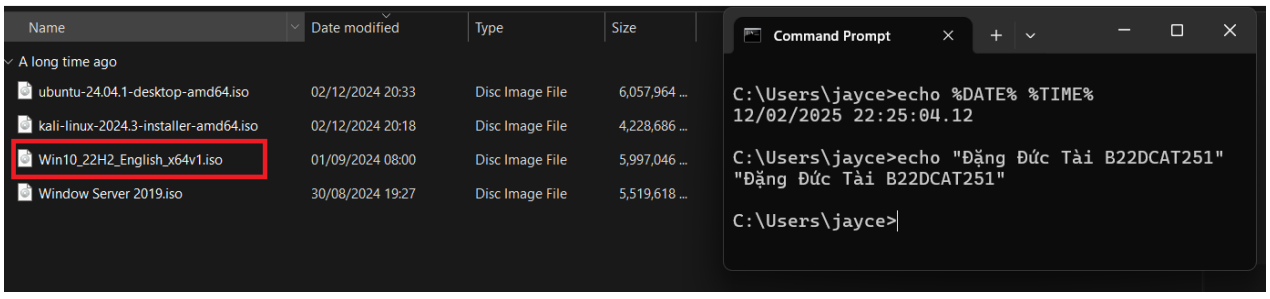
Hình 7 Giao diện của phần mềm cứu hộ Kaspersky Rescue Disk

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

- File cài đặt Windows 7/8/10/11 định dạng iso.

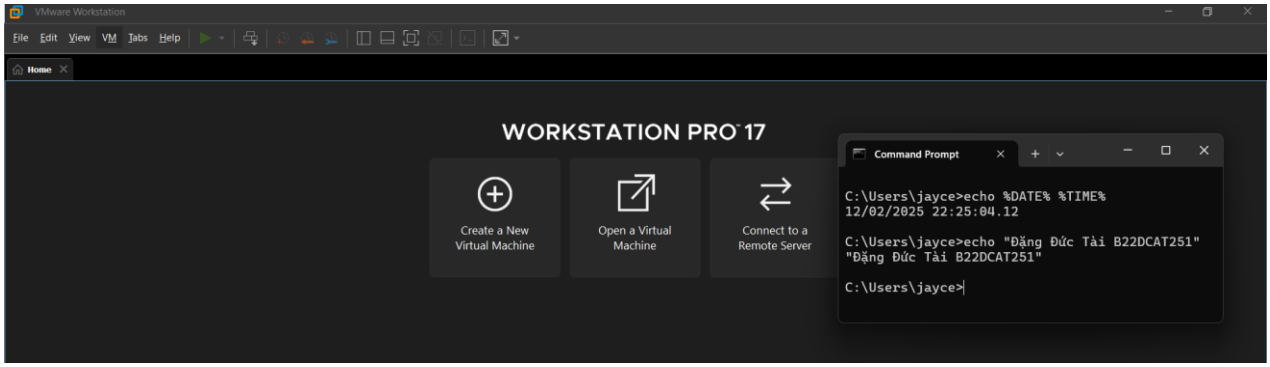
→ Trong bài thực hành này sử dụng máy ảo Windows 10 22H2 iso.



Hình 8 Chuẩn bị máy ảo windows 10

- Phần mềm ảo hóa, chẳng hạn: VMWare Workstation.

→ Trong bài thực hành này sử dụng phần mềm ảo hóa VMWare Workstation Pro 17.



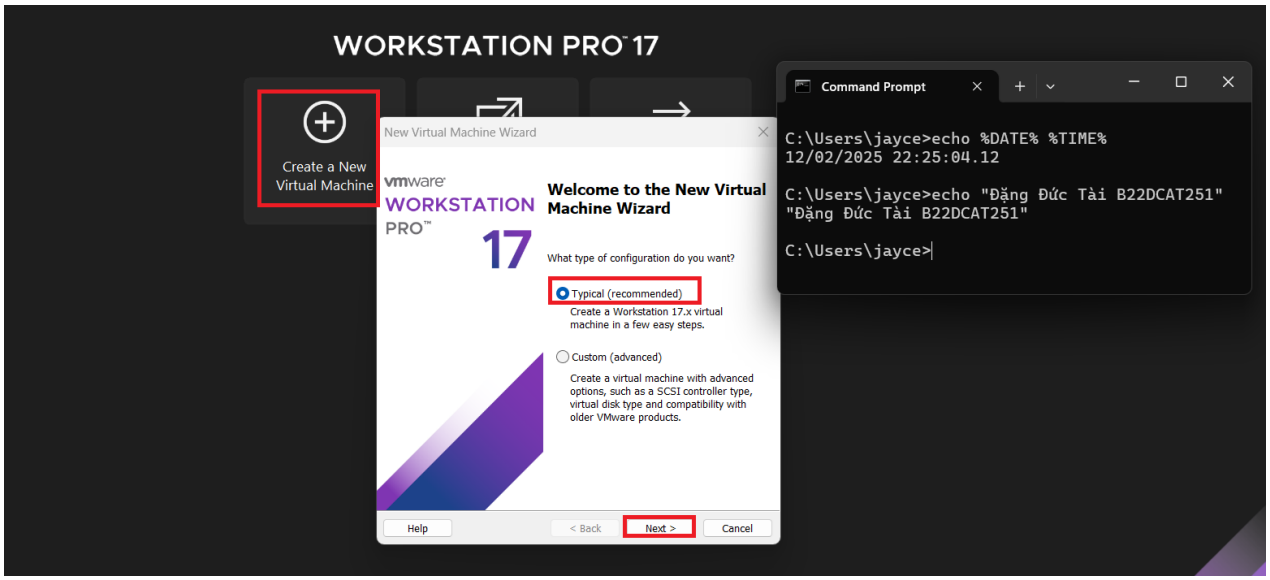
Hình 9 Chuẩn bị phần mềm VMWare Workstation Pro 17

2.2 Các bước thực hiện

2.2.1 Cài đặt máy ảo

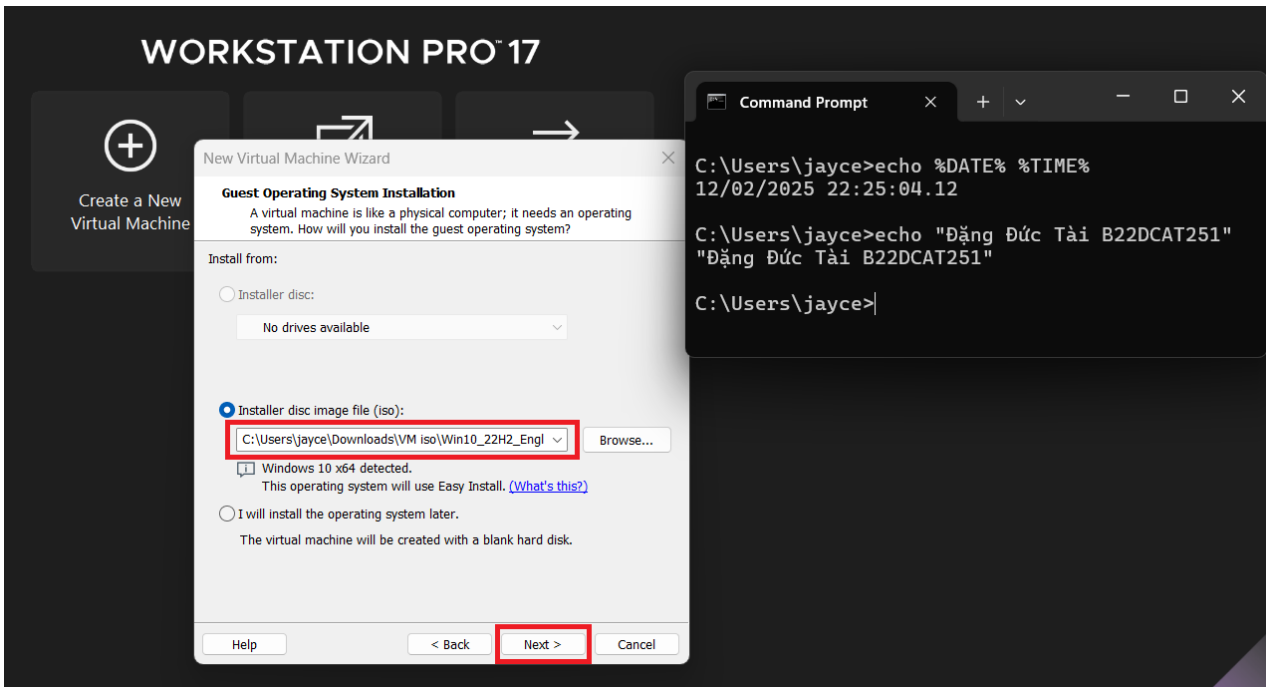
- Khởi động chương trình máy ảo, thực hiện cài đặt theo các bước dưới đây:

- Bước 1: Bấm vào Create a New Vitual Machine → Typical → Next



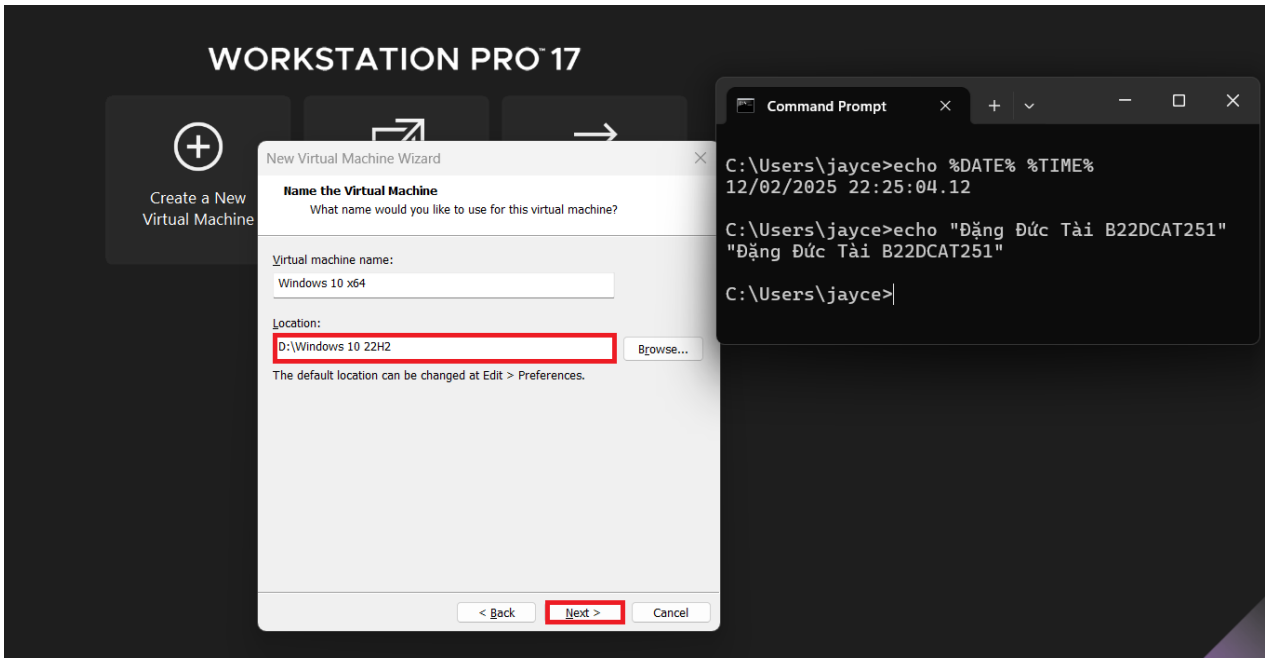
Hình 10 Cài đặt máy ảo

- Bước 2: Load file iso → Next



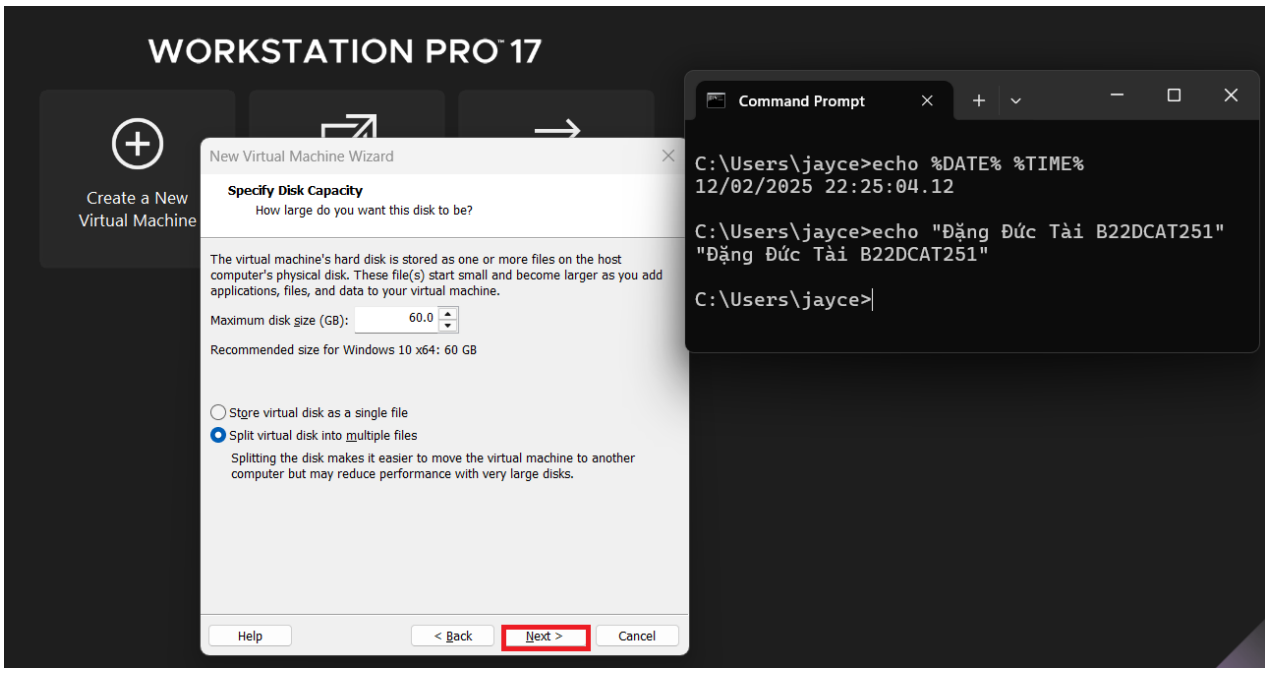
Hình 11 Chọn đường dẫn đến file chứa máy ảo

- Bước 3: Set đường dẫn để lưu máy trạm → Next



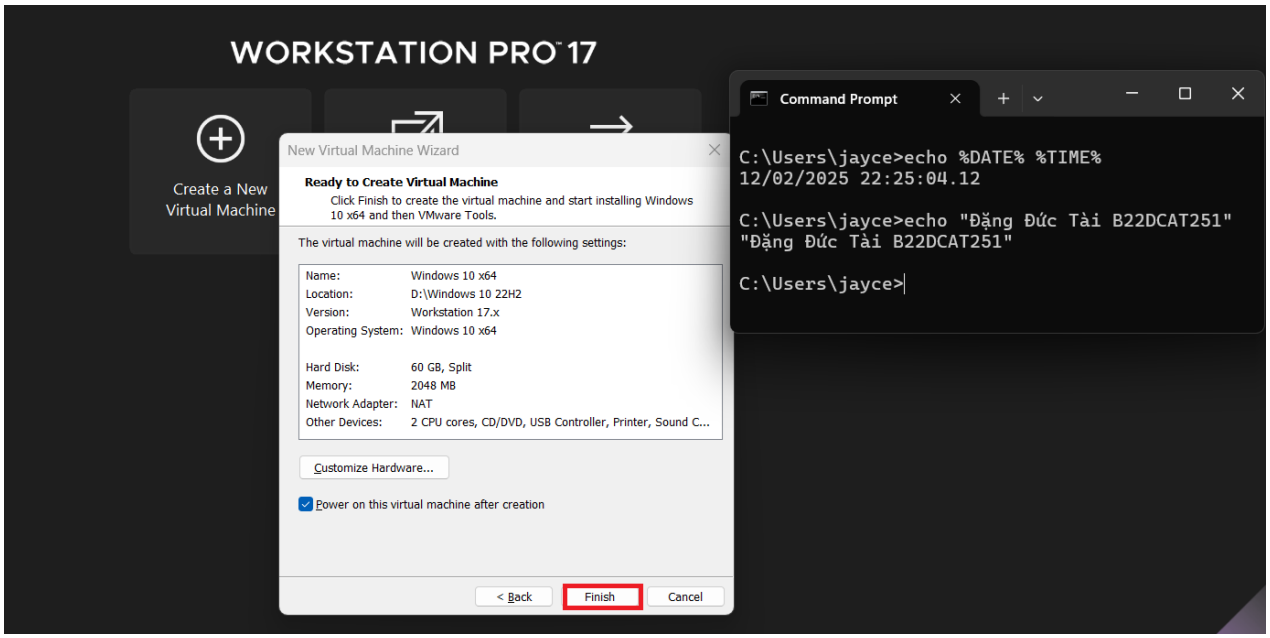
Hình 12 Cài đặt đường dẫn

- Bước 4: Có thể tùy chỉnh bộ nhớ ổ đĩa (disk) của máy trạm → Next



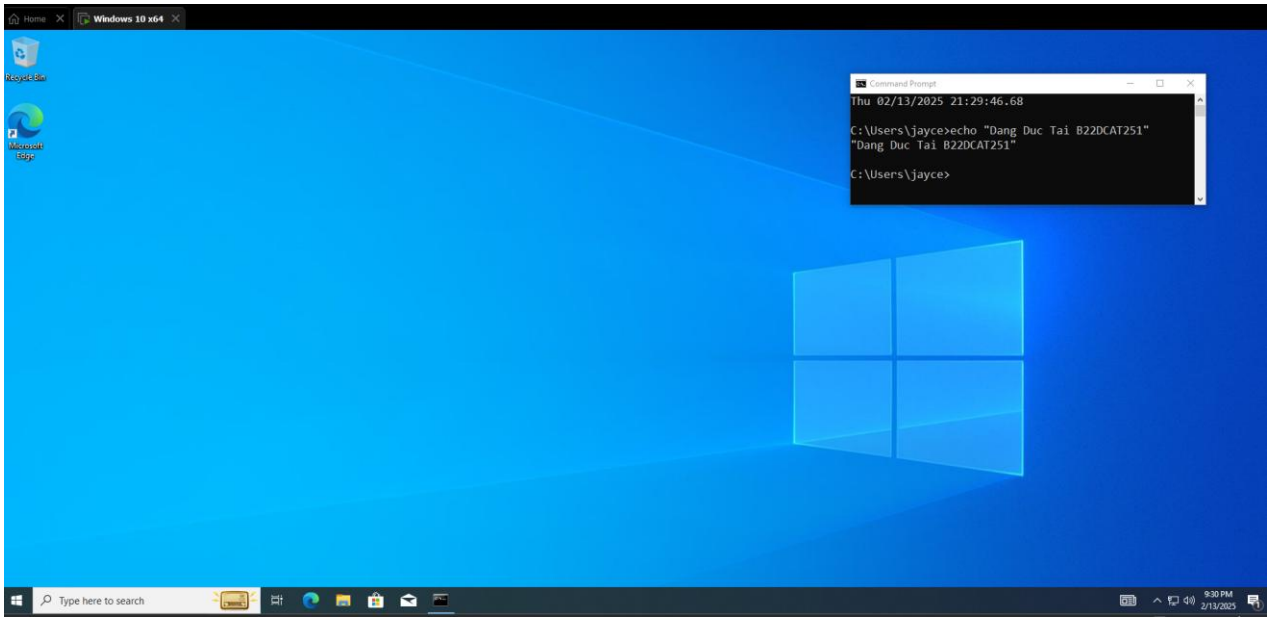
Hình 13 Cấu hình ổ đĩa cho máy ảo

- Bước 5: Có thể chỉnh lại cấu hình bằng cách Customize Hardware → Finish



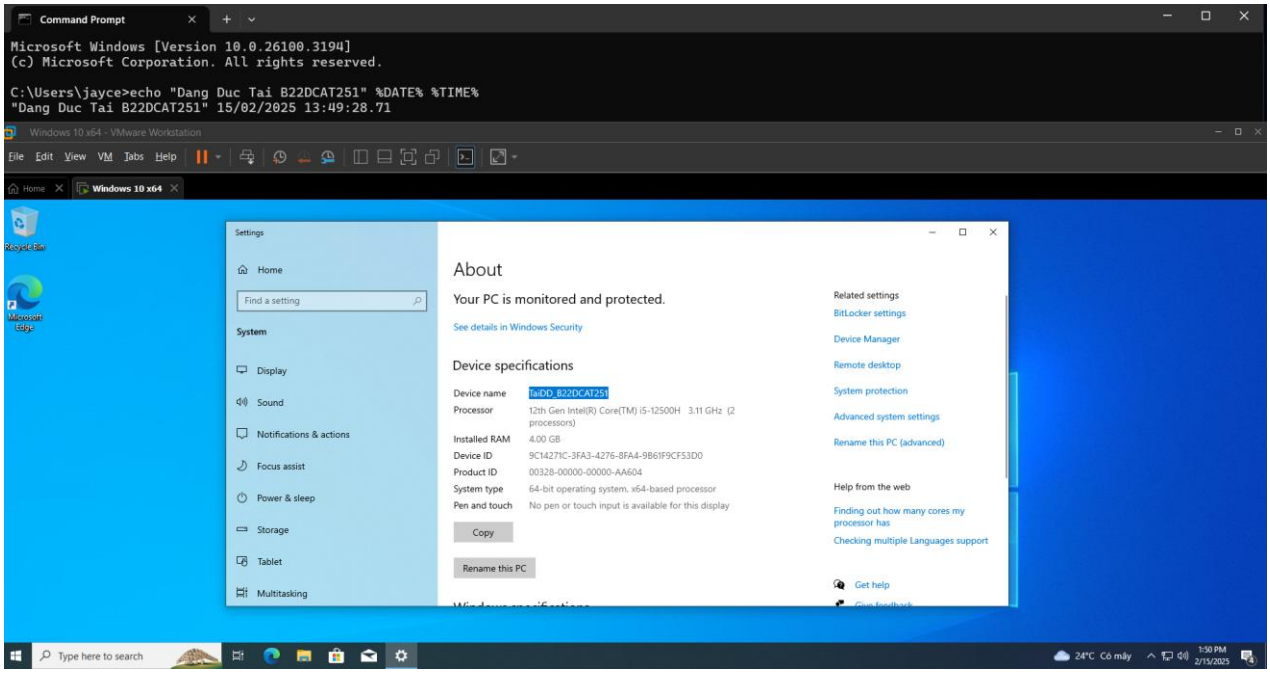
Hình 14 Kiểm tra & kết thúc cài đặt

- Bước 6: Cài đặt thành công



Hình 15 Giao diện của máy ảo Windows 10

- Bước 7: Thực hiện đổi tên



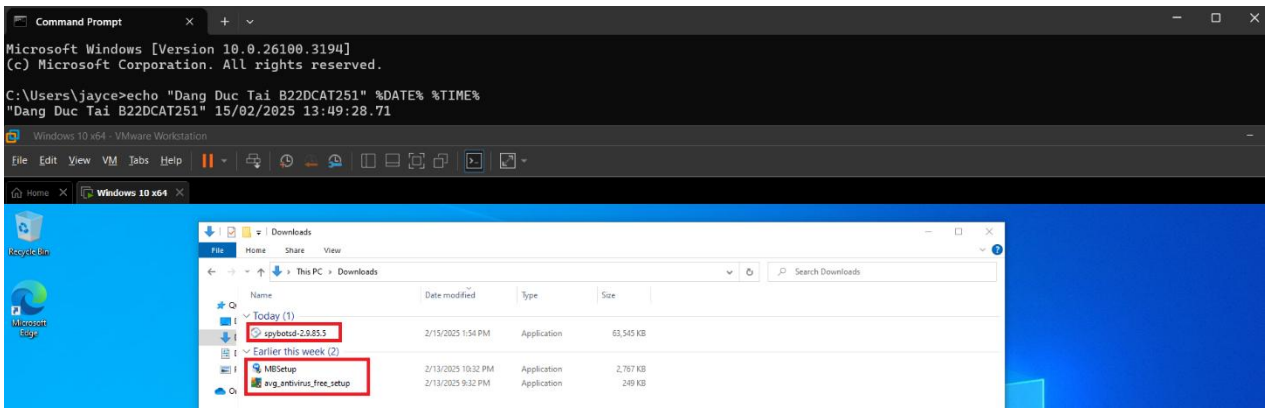
Hình 16 Đổi tên người dùng

2.2.2 Cài đặt các chương trình phần mềm

2.2.2.1 Chuẩn bị

- Trên máy trạm windows 10:

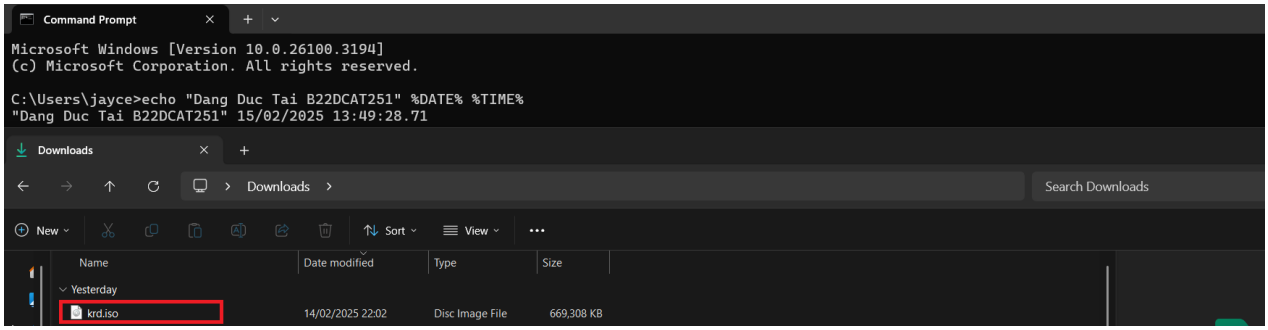
- Phần mềm diệt virut: AVG AntiVirus
- Phần mềm chống phần mềm gián điệp Spybot S&D
- Phần mềm chống các phần mềm độc hại: Malwarebytes Anti-Malware



Hình 17 Chuẩn bị các phần mềm trên máy ảo

- Trên máy thật

- Phần mềm cứu hộ: Kaspersky Rescue Disk (KRD)



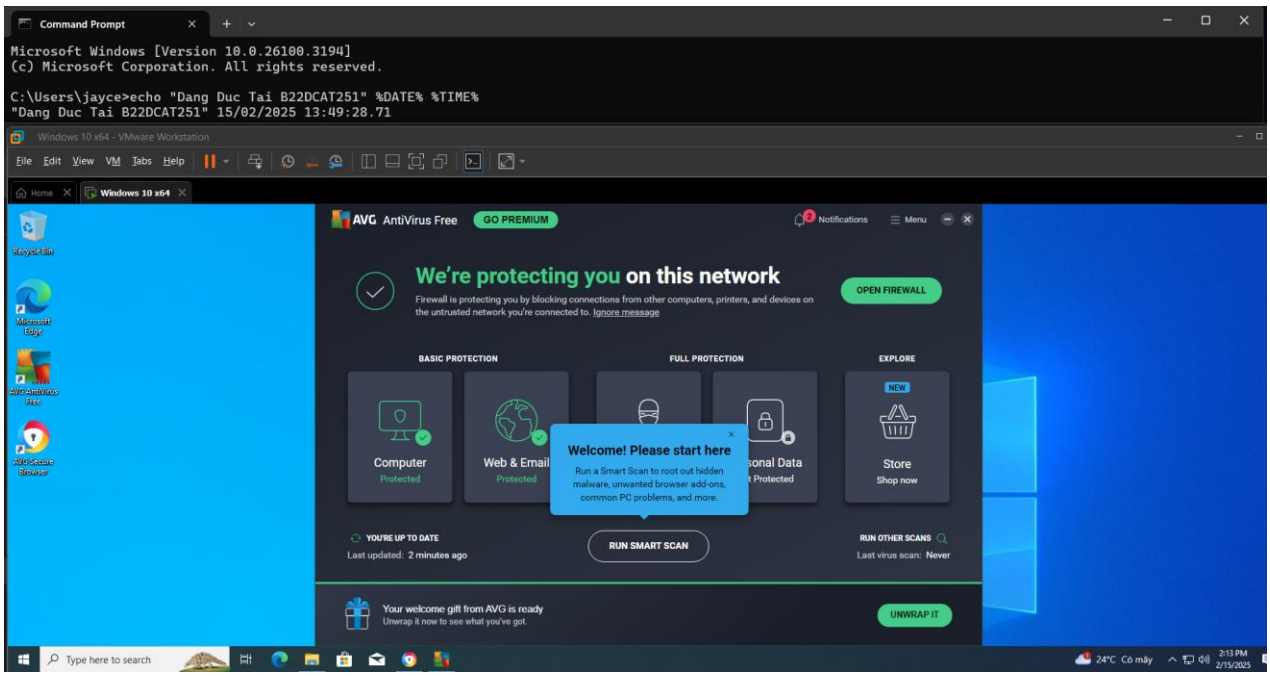
Hình 18 Chuẩn bị phần mềm cứu hộ trên máy thật

2.2.2.2 Cài đặt

- Cài đặt trên trang web của AVG AntiVirus, với link sau:

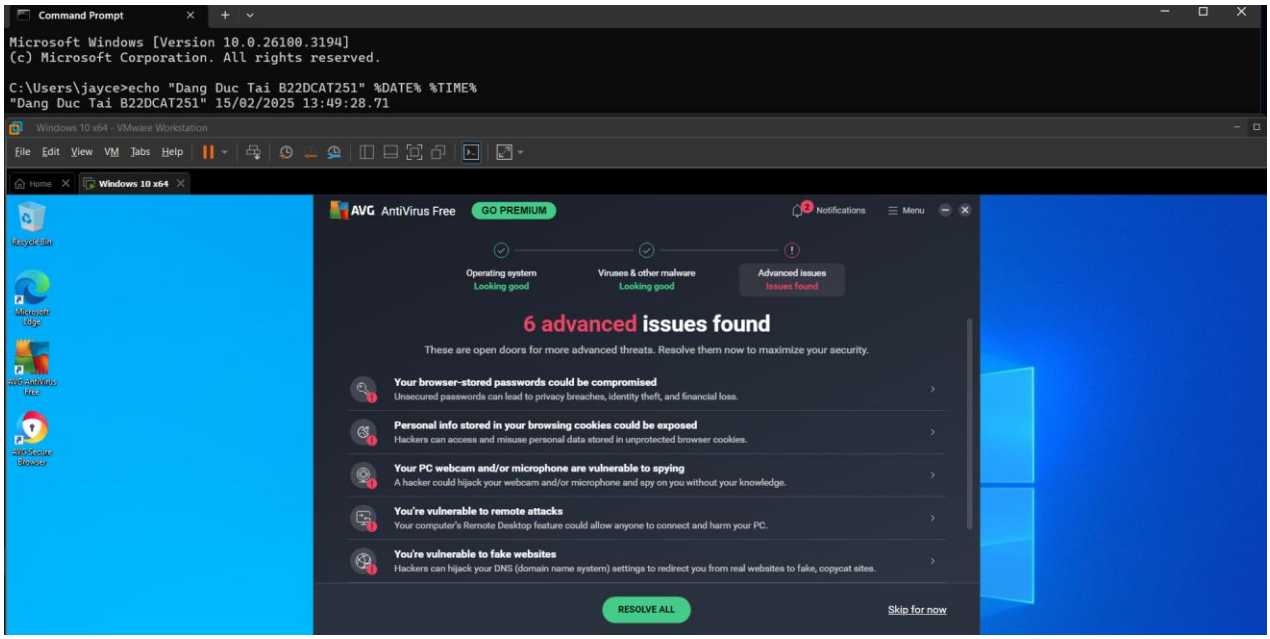
  https://www.avg.com/download-thank-you.php?product=FREEGSR

- Cài đặt phần mềm AVG AntiVirus thành công.



Hình 19 Giao diện phần mềm AVG Anti Virus

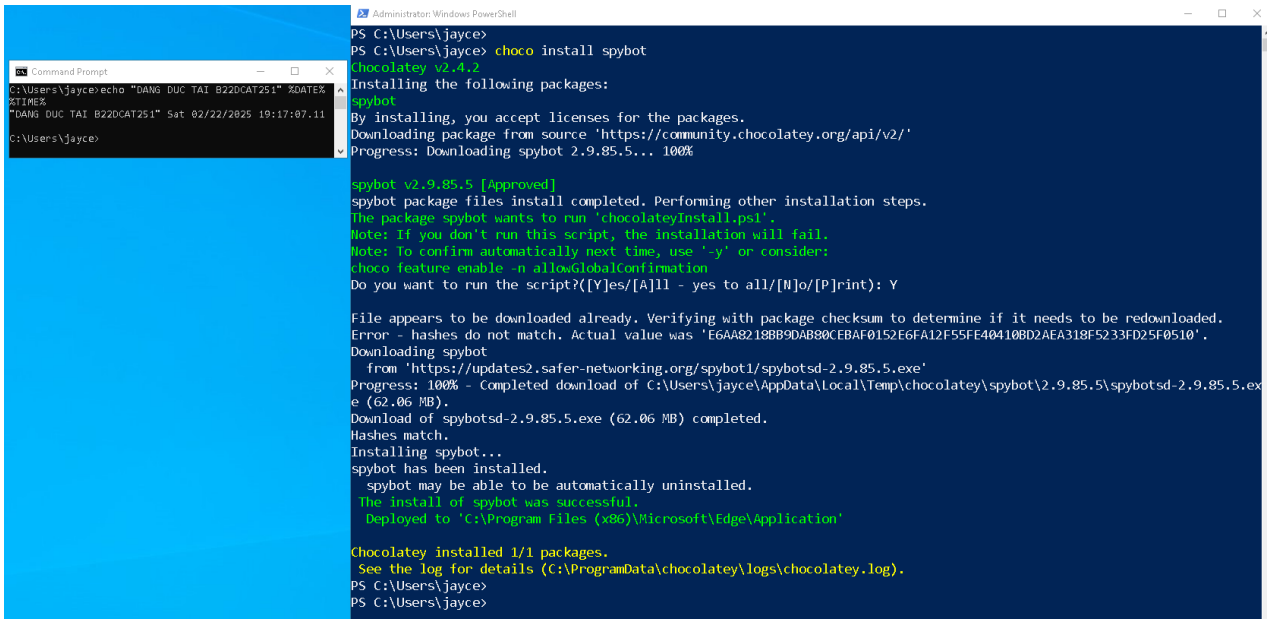
- Chạy và sử dụng phần mềm AVG thành công.



Hình 20 Kết quả sau khi sử dụng phần mềm AVG

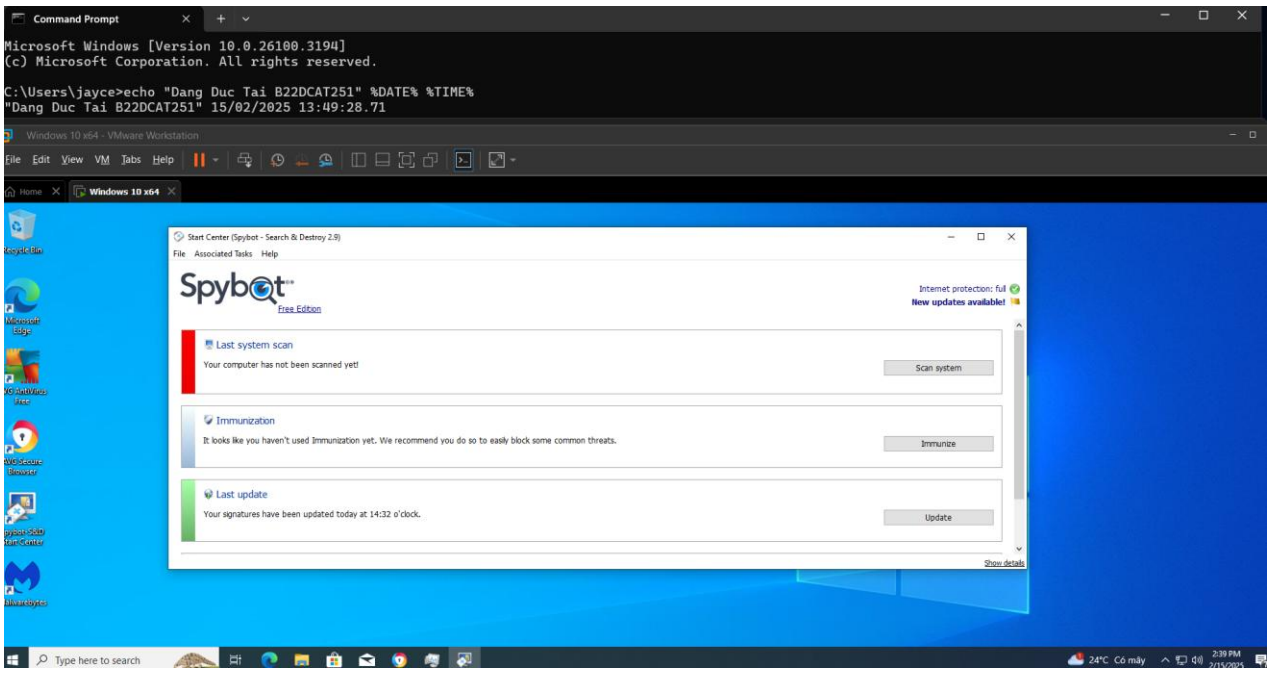
- Sử dụng chocolatey để cài đặt phần mềm Spybot

  choco install spybot -Y



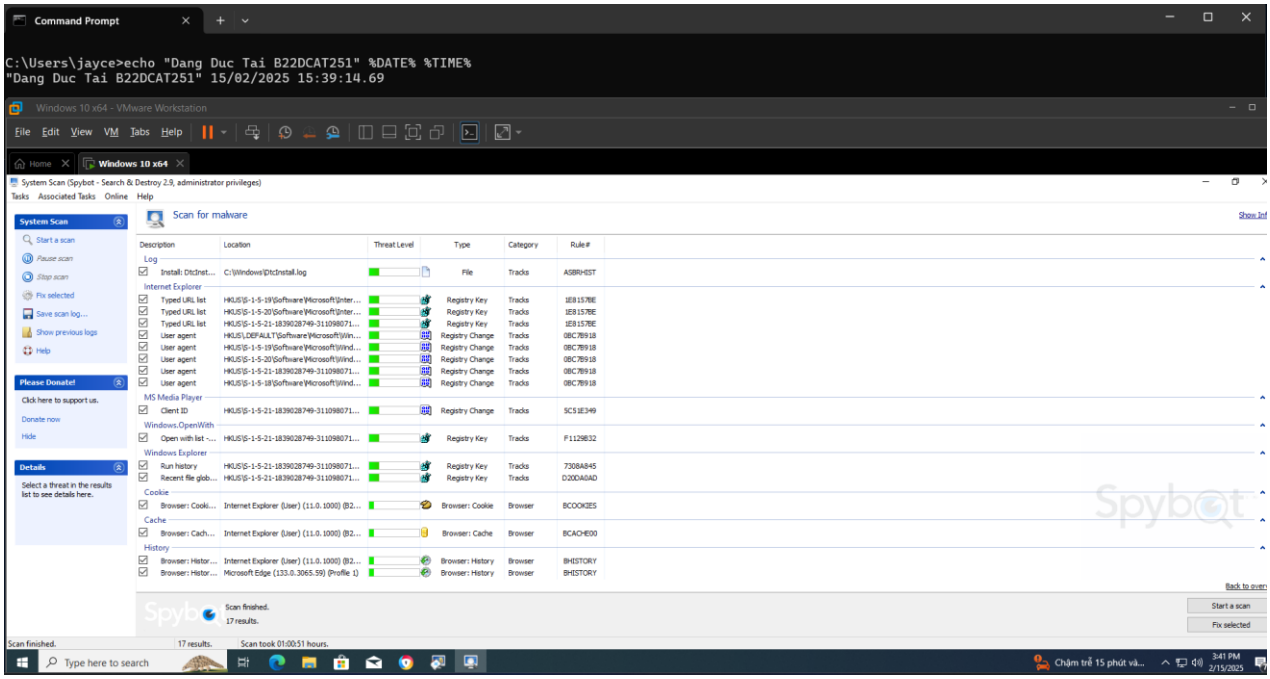
Hình 21 Cài đặt Spybot bằng choco

- Cài đặt phần mềm Spybot thành công.



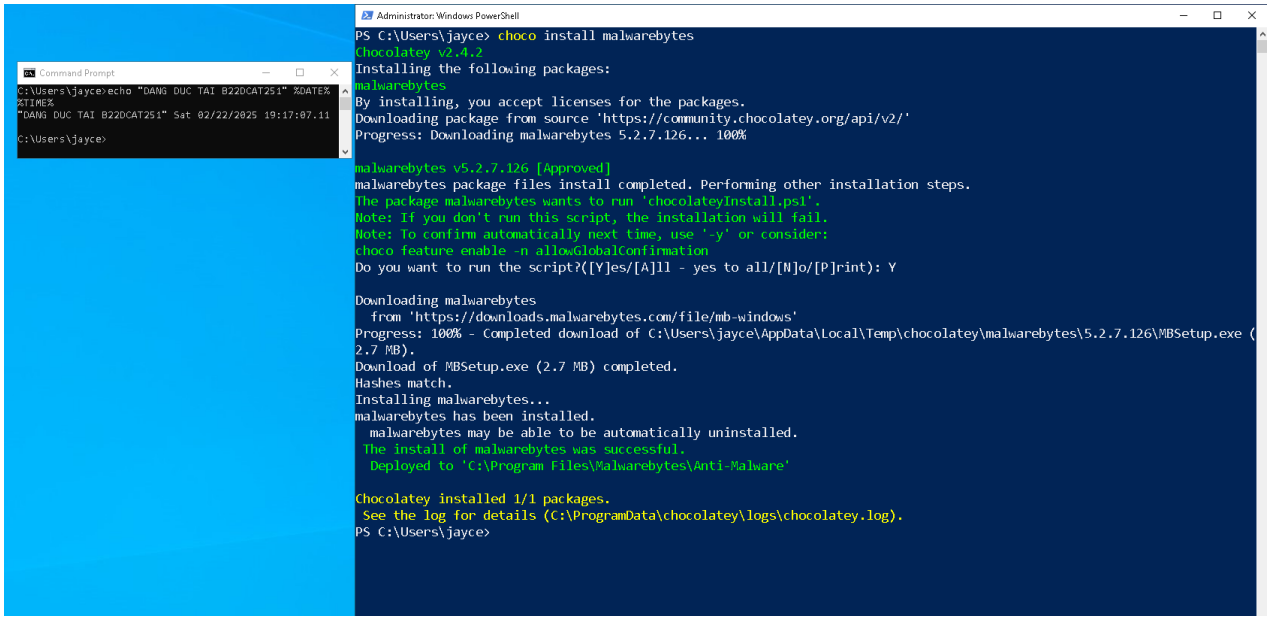
Hình 22 Giao diện phần mềm Spybot

- Chạy và sử dụng phần mềm Spybot thành công.



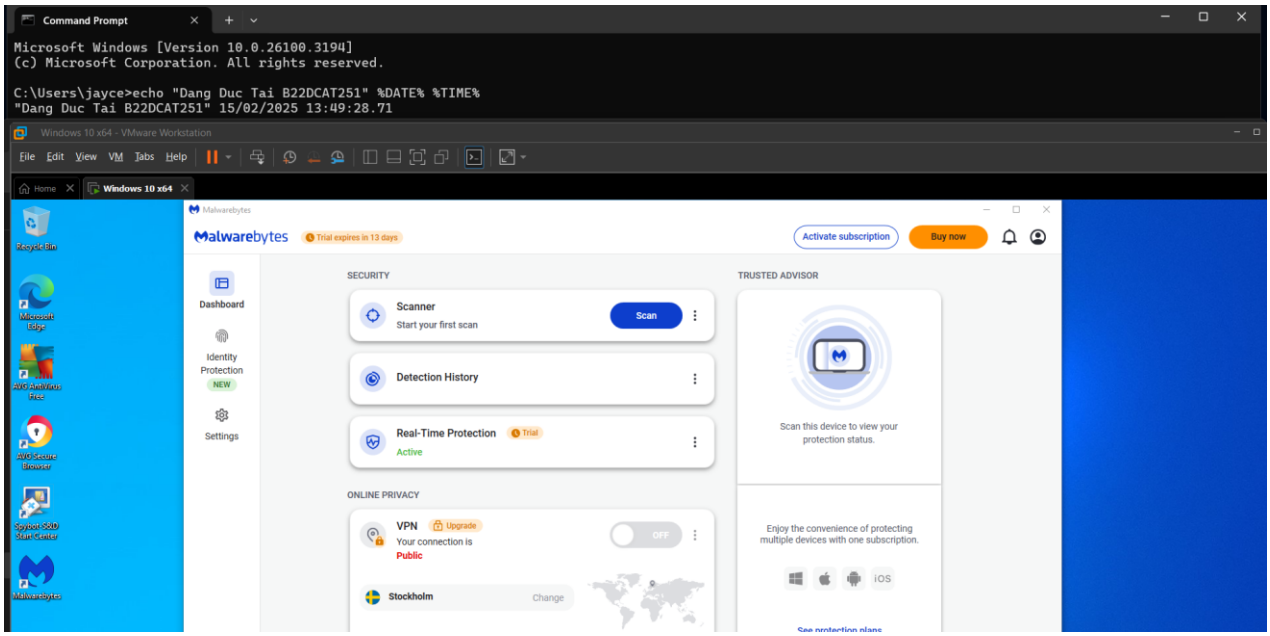
Hình 23 Kết quả sau khi chạy phần mềm Spybot

- Cài đặt phần mềm Malwarebytes Anti-Malware bằng choco.



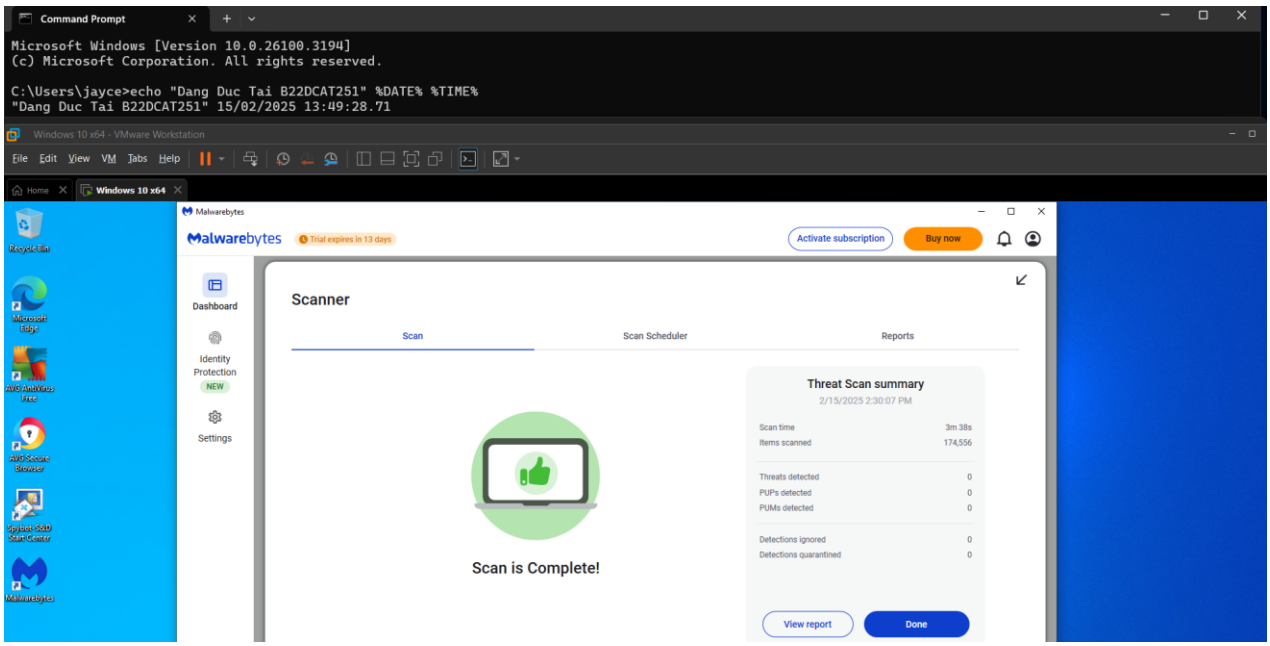
Hình 24 Cài đặt Malwarebytes Anti-Malware bằng choco

- Cài đặt phần mềm Malwarebytes Anti-Malware thành công.



Hình 25 Giao diện phần mềm Malwarebytes Anti-Malware

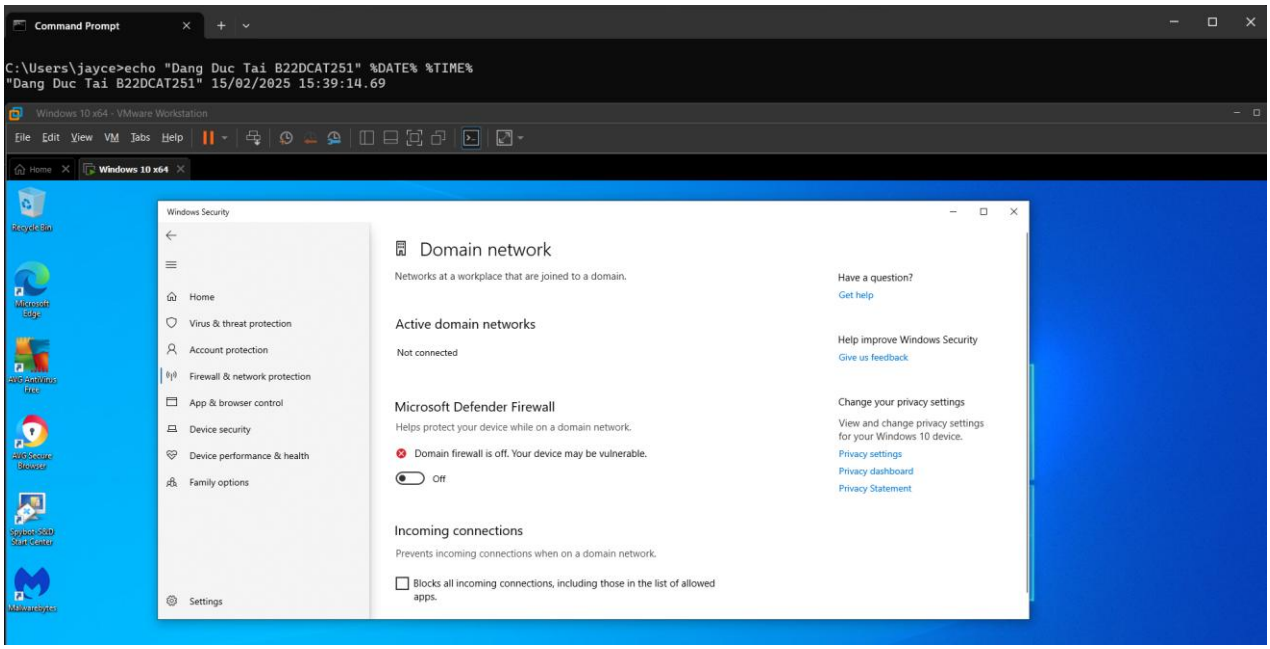
- Chạy và sử dụng phần mềm Malwarebytes Anti-Malware thành công.



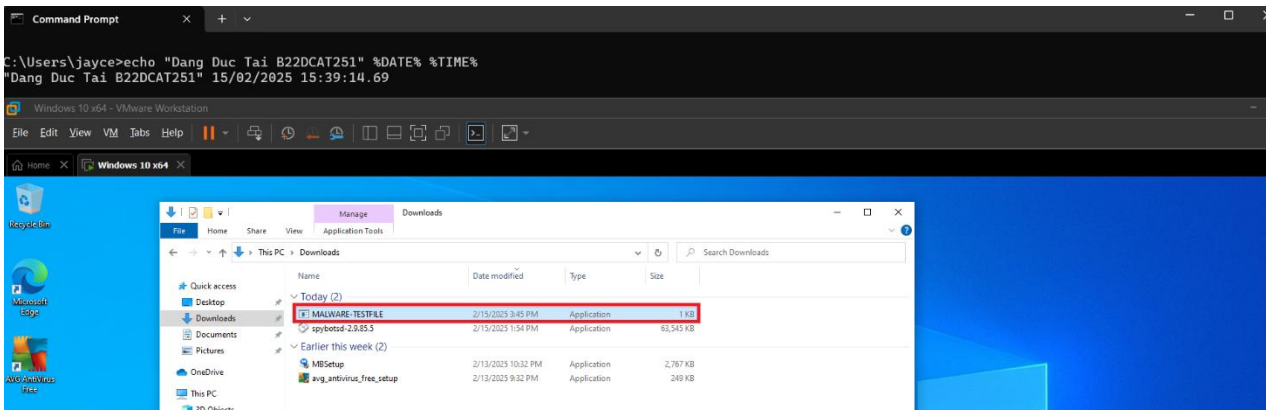
Hình 26 Kết quả sau khi chạy phần mềm Malwarebytes Anti-Malware

- Thực hiện cài mã độc theo đường link bên dưới (**Lưu ý**: tắt Firewall trước khi cài). File mã độc sẽ được lưu tại C:\Users\jayce\Downloads

- http://www.computersecuritystudent.com/WINDOWS/W7/lesson7/MALWARE-TESTFILE.exe



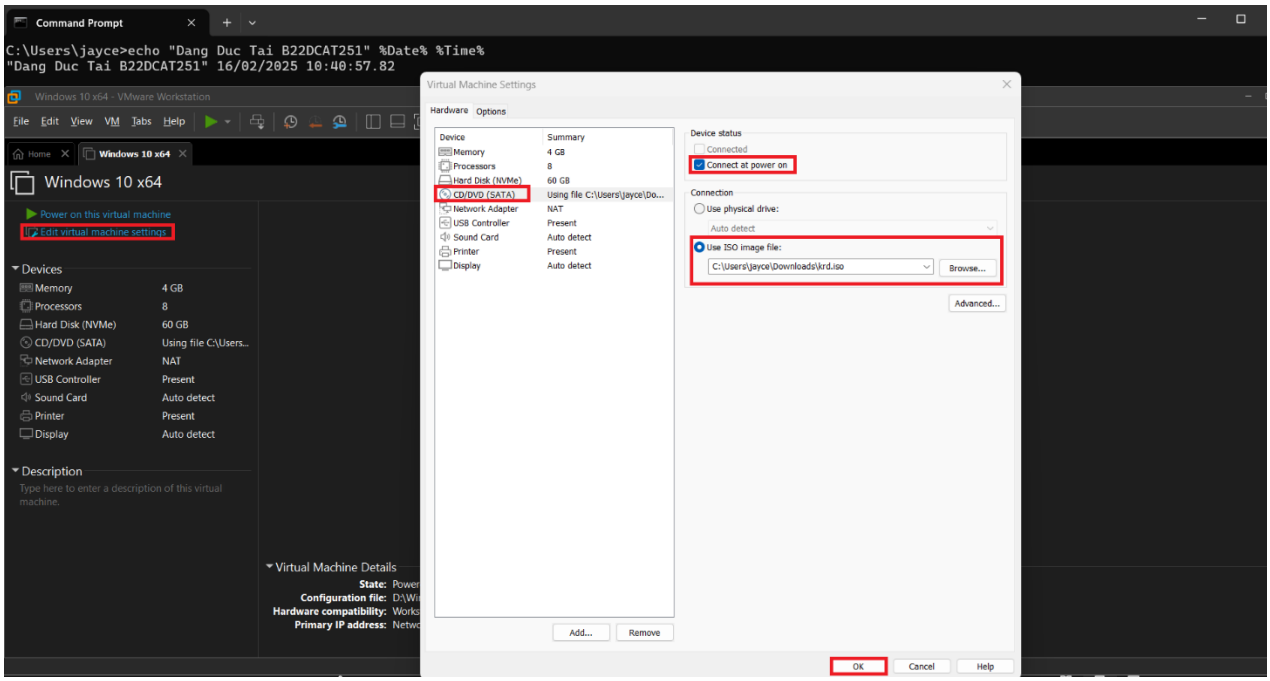
Hình 27 Cấu hình tắt tường lửa



Hình 28 Tải thành công file có chứa mã độc

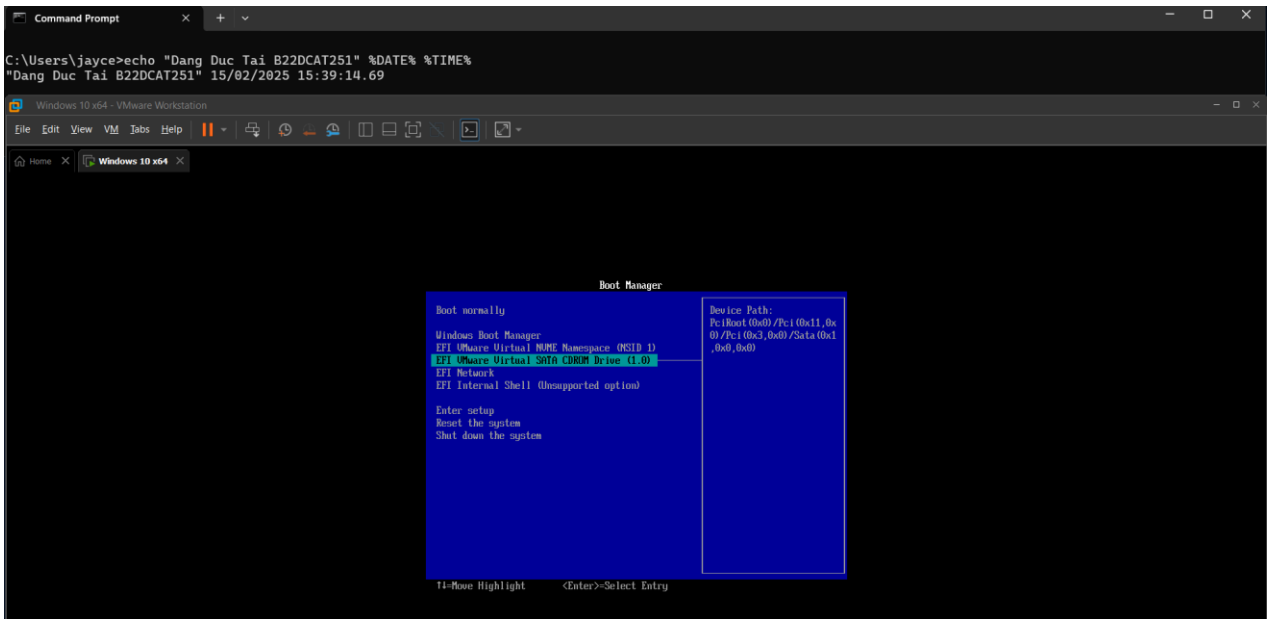
- Tiến hành cấu hình phần mềm cứu hộ KRD vào ổ đĩa chứa file máy ảo windows 10:

- Edit virtual machine settings → CD/DVD (SATA) → Use ISO image file → Chọn đường dẫn chứa phần mềm cứu hộ KRD → OK



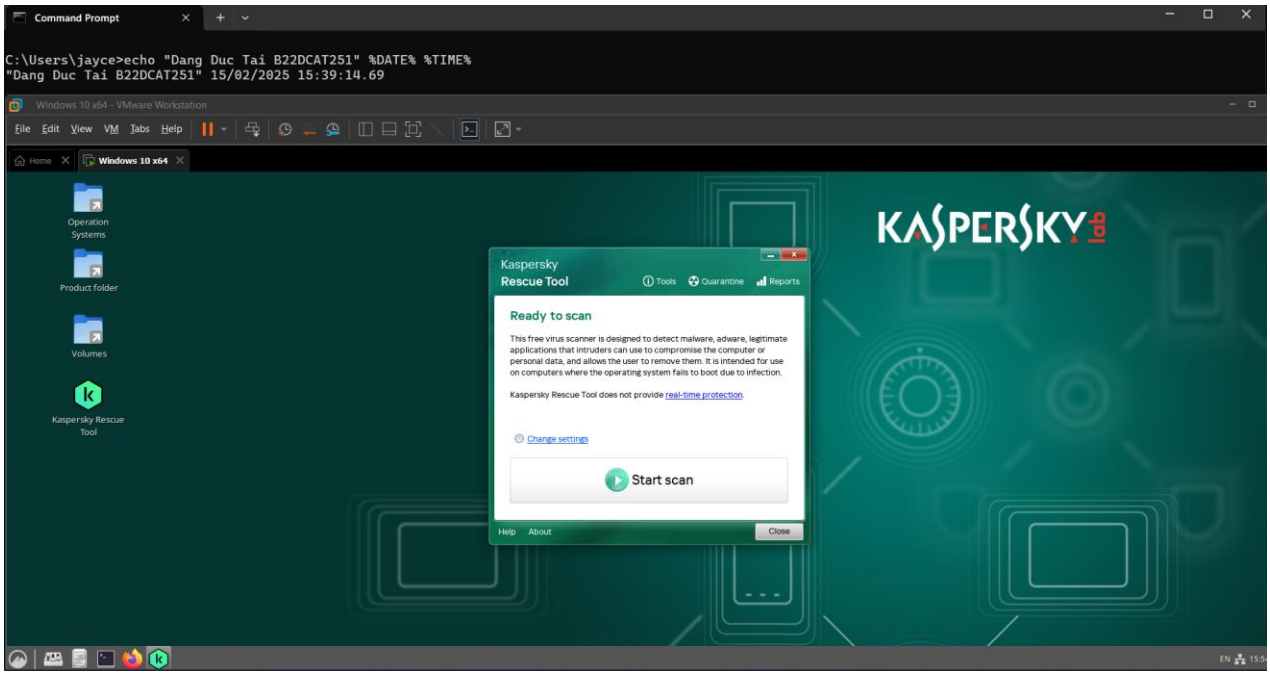
Hình 29 Cấu hình phần mềm cứu hộ KRD

- Boot phần mềm KRD bằng cách restart máy ảo, sau đó bấm phím **esc** ngay lúc khởi động lại để hiển thị **Boot Manager** → Chọn SATA CDROM Drive



Hình 30 Boot phần mềm cứu hộ KRD

- Boot phần mềm cứu hộ KRD thành công.

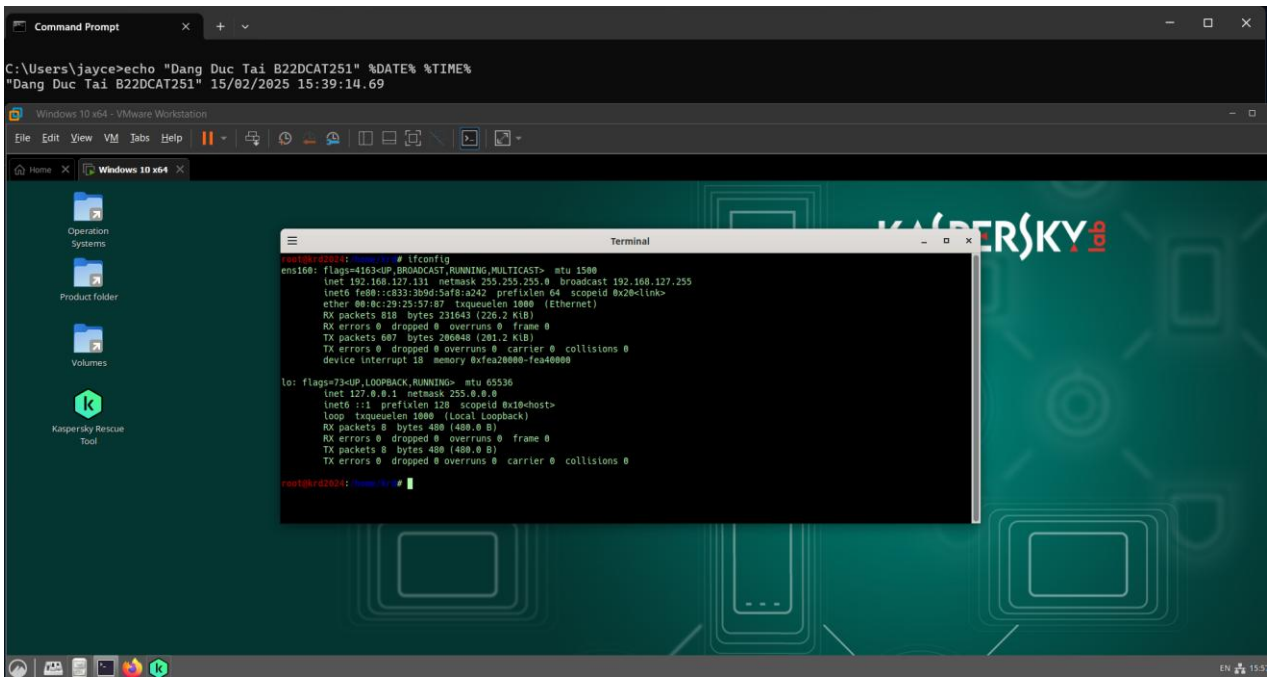


Hình 31 Giao diện của phần mềm cứu hộ KRD

- Kiểm tra ip của máy ảo.

- Mở cmd → gõ câu lệnh *ifconfig*

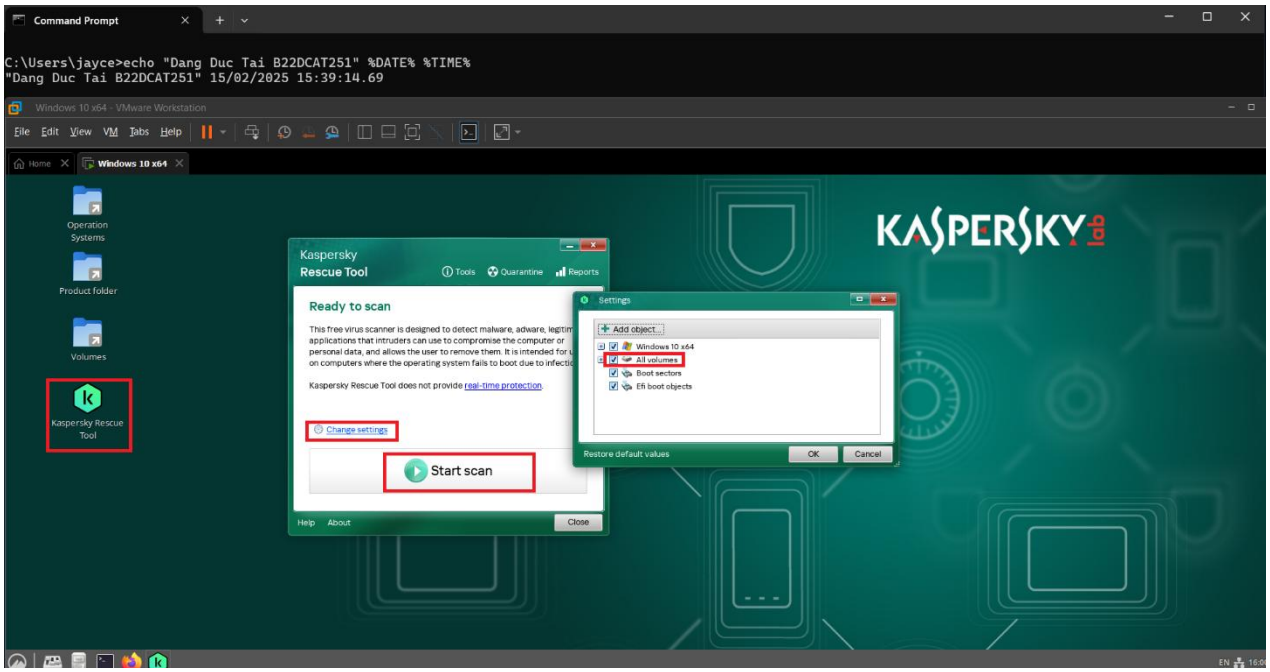
  → Địa chỉ ip của máy trạm là *192.168.127.131*



Hình 32 Kiểm tra ip của máy ảo

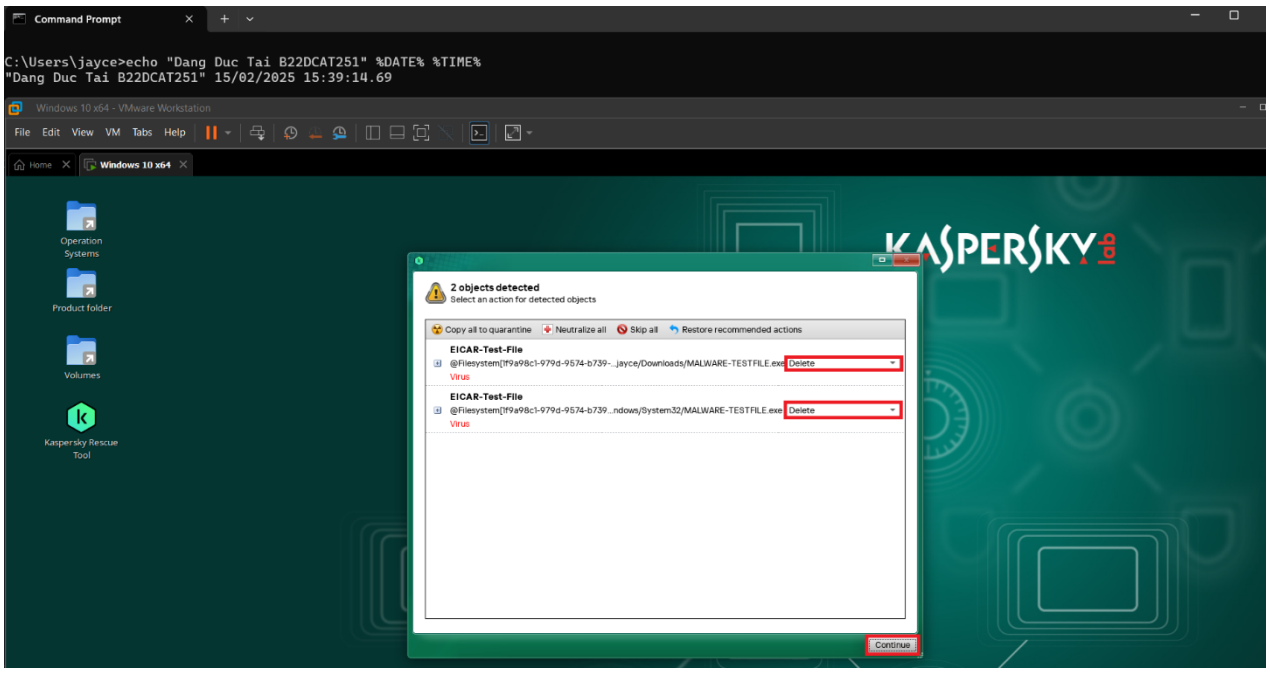
- Thực hiện quét trên phần mềm KDR

- Chọn change settings → All volumes → Start scan



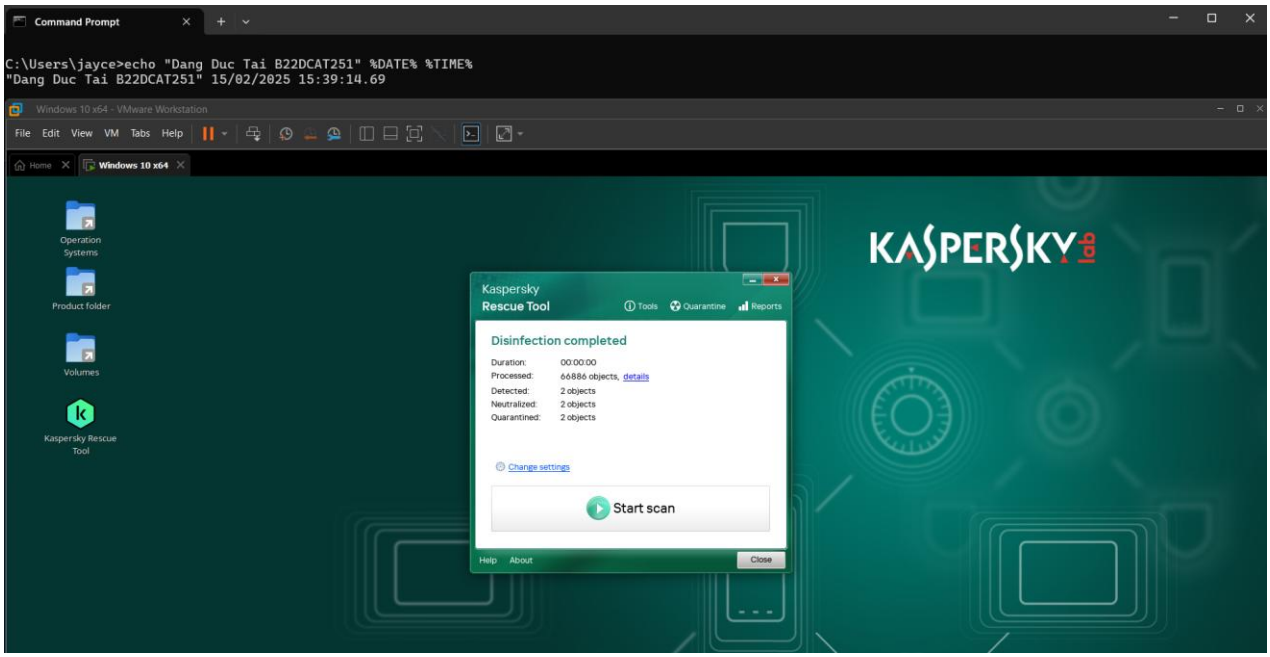
Hình 33 Quét virus trên phần mềm KRD

- Quét thành công, phần mềm KRD đã phát hiện được virus có trong đường dẫn tại C:\Users\jayce\Downloads\MALWARE-TESTFILE.exe
  C:\Windows\System32\MALWARE-TESTFILE.exe



Hình 34 Quét thành công mã độc

- Tiến hành xóa mã độc



Hình 35 Loại bỏ mã độc

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.