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: B22DCAT206 - PHẠM ĐỨC NAM

Giảng viên hướng dẫn: Đỗ Xuân Chợ

HỌC KỲ 2 NĂM HỌC 2024-2025

Mục lục

Danh mục hình ảnh

1. Mục đích

Nâng cao kỹ năng cài đặt, cấu hình và quản lý hệ điều hành Windows trên máy trạm, đồng thời làm quen với các dịch vụ cơ bản phục vụ người dùng.

2. Nội dung thực hành

2.1. Cơ sở lý thuyết

2.1.1. Phần mềm ảo hóa

2.1.1.1. VMWare Workstation

VMware Workstation là một phần mềm ảo hóa mạnh mẽ, cho phép tạo và vận hành nhiều máy ảo trên một máy tính vật lý. Nó hỗ trợ chạy đồng thời các hệ điều hành khác nhau, như Windows, Linux, và nhiều nền tảng khác, trên cùng một thiết bị.

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

✓ Hỗ trợ chạy nhiều hệ điều hành trên một máy tính duy nhất.Cung cấp báo lỗi và cách ly an toàn với phần cứng

✓ Đảm bảo cách ly an toàn giữa máy ảo và phần cứng vật lý.

✓ Tăng tính sẵn sàng và linh hoạt trong việc sử dụng phần cứng.

✓ Tiết kiệm tài nguyên nhờ chỉ sử dụng một máy vật lý.

Hạn chế:

➢ Hiệu suất không bằng các giải pháp ảo hóa chuyên nghiệp.

➢ Có thể thiếu ổn định trong môi trường sản xuất.

➢ Hỗ trợ đồ họa hạn chế.

➢ Quản lý tài nguyên không linh hoạt.

2.1.1.2. Vitual Box

VirtualBox là một phần mềm ảo hóa miễn phí, chuyên nghiệp, cho phép người dùng thiết lập nhiều hệ điều hành trên cùng một máy tính. Phần mềm này tương thích với các nền tảng như Windows, Linux Ubuntu, macOS và Solaris. Là một giải pháp ảo hóa đa nền tảng, VirtualBox giúp người dùng dễ dàng thử nghiệm các hệ điều hành và ứng dụng mới một cách an toàn,

không lo ngại về virus, không gây lộn xộn cho hệ thống chính, và không cần phải cài đặt lại hệ điều hành.

Lợi ích khi sử dụng phần mềm Vitual Box:

- ✓ Tương thích với nhiều hệ điều hành.
- ✓ Không đòi hỏi phần cứng hỗ trợ ảo hóa.
- ✓ Hỗ trợ tốt các tính năng phần cứng như xử lý đa nhân và kết nối USB.
- ✓ Cung cấp môi trường an toàn để thử nghiệm phần mềm.

Bên cạnh đó, Vitual Box vẫn còn một số mặt hạn chế như:

- ➢ Hiệu suất thấp hơn so với một số công cụ ảo hóa chuyên biệt.
- ➢ Độ ổn định có thể không đảm bảo trong các môi trường sản xuất.
- ➢ Không hỗ trợ đầy đủ một số hệ điều hành hoặc ứng dụng.
- ➢ Hiệu năng đồ họa hạn chế.
- ➢ Gặp một số vấn đề khi sử dụng thiết bị USB.
- ➢ Quản lý tài nguyên kém linh hoạt so với các giải pháp ảo hóa cao

2.1.2. Hệ điều hành Windows

2.1.2.1. Lịch sử phát triển

Hệ điều hành Windows, do Microsoft phát triển, ra mắt lần đầu vào năm 1985. Dưới đây là tóm tắt về các phiên bản chính:

- ❖ MS-DOS (1981): Giao diện dòng lệnh đơn giản, tương thích nhiều phần cứng, nhưng thiếu hỗ trợ đa nhiệm và đồ họa.
- ❖ Windows 1.0 (1985): Giới thiệu giao diện đồ họa cơ bản, nhưng hạn chế về tính năng.
- ❖ Windows 3.0 (1990): Cải tiến giao diện, hỗ trợ đa nhiệm, nhưng bảo mật còn yếu.
- ❖ Windows 95 (1995): Ra mắt Start Menu, tích hợp Internet Explorer, cải thiện hiệu suất.
- ❖ Windows 98 (1998): Hỗ trợ USB, tăng độ ổn định, nhưng vẫn có vấn đề bảo mật.

❖ Windows 2000 (2000): Dựa trên nền tảng NT, phù hợp cho doanh nghiệp, nhưng giao diện ít thay đổi.

❖ Windows XP (2001): Giao diện thân thiện, ổn định, nhưng dễ bị tấn công (ví dụ: WannaCry).

❖ Windows Vista (2007): Cải tiến bảo mật và đồ họa (Aero), nhưng yêu cầu phần cứng cao.

❖ Windows 7 (2009): Tối ưu hiệu suất, cải thiện giao diện, nhưng vẫn có lỗ hổng bảo mật.

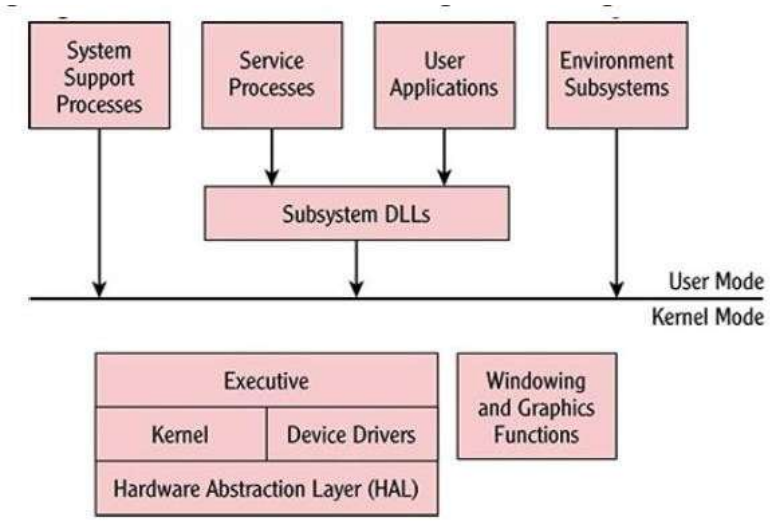
❖ Windows 8 (2012): Giao diện cảm ứng, đồng bộ đám mây, nhưng không phù hợp với PC truyền thống.

❖ Windows 10 (2015): Kết hợp giao diện truyền thống và hiện đại, cải thiện bảo mật, nhưng có vấn đề về quyền riêng tư.

❖ Windows 11 (2021): Giao diện mới, hiệu suất cao, nhưng yêu cầu phần cứng mạnh.

2.1.2.2. Kiến trúc

Kiến trúc của các hệ điều hành Windows hiện đại được xây dựng dựa trên nền tảng Windows NT. Về cơ bản, kiến trúc này được chia thành hai lớp chính, tương ứng với hai chế độ hoạt động: **chế độ nhân** và **chế độ người dùng**. Chế độ nhân được dành cho lõi của hệ điều hành và các chương trình cấp thấp, trong khi chế độ người dùng hỗ trợ các ứng dụng như Microsoft Word, Excel và các hệ thống con.



Hình 1 – Kiến trúc cơ bản của hệ điều hành Windows

Về mặt kỹ thuật, các tác vụ trong chế độ nhân được thực thi ở cấp độ thấp nhất, còn gọi là chế độ đặc quyền, cho phép truy cập vào các tài nguyên hệ thống quan trọng. Ngược lại, các tác vụ trong chế độ người dùng được thực hiện ở cấp độ cao nhất, hay chế độ không đặc quyền, giới hạn quyền truy cập vào tài nguyên của các chương trình.

Các thành phần chính của chế độ người dùng bao gồm:

— Quy trình hỗ trợ hệ thống (System Support Processes): Xử lý các chức năng hệ thống thiết yếu như đăng nhập người dùng và quản lý phiên làm việc.

— Quy trình dịch vụ (Service Processes): Cung cấp các dịch vụ của hệ điều hành, chẳng hạn như quản lý máy in hoặc lập lịch tác vụ, đồng thời hỗ trợ các dịch vụ cơ sở dữ liệu hoặc chức năng cho các chương trình khác.

— Ứng dụng người dùng (User Applications): Các chương trình thực hiện nhiệm vụ theo yêu cầu của người dùng hoặc quản trị viên.

— Hệ thống con (Environment Subsystems) và Thư viện liên kết động (Subsystem DLLs): Kết hợp để hỗ trợ các loại ứng dụng khác nhau như môi trường Win32, Win64 hoặc DOS 32. Thư viện liên kết động chuyển đổi các hàm ứng dụng thành các lệnh gọi dịch vụ hệ thống trực tiếp.

Các chức năng cơ bản của chế độ nhân gồm có:

— Thực thi (Executive): Quản lý tiến trình, luồng, bộ nhớ và hoạt động vào/ra.

— Nhân (Kernel): Đảm nhiệm việc điều phối luồng, đồng bộ hóa tiến trình và xử lý các ngắt.

— Trình điều khiển thiết bị (Device Drivers): Kết nối giữa hệ thống quản lý vào/ra của phần thực thi và phần cứng cụ thể, đồng thời hỗ trợ giao tiếp với hệ thống tệp, mạng hoặc giao thức.

— Lớp trừu tượng phần cứng (Hardware Abstraction Layer - HAL): Che giấu chi tiết phần cứng, giúp hệ điều hành hoạt động nhất quán trên nhiều nền tảng phần cứng khác nhau.

— Chức năng cửa sổ và đồ họa (Windowing and Graphics Functions): Cung cấp giao diện đồ họa cho người dùng, bao gồm hiển thị cửa sổ và các đối tượng đồ họa.

2.1.2.3. Giao diện

Hệ điều hành Windows cung cấp ba phương thức giao tiếp chính, hỗ trợ người dùng tương tác với các ứng dụng và thực hiện các tác vụ quản trị hệ thống:

— Giao diện đồ họa (GUI): Giao diện người dùng đồ họa của Windows bao gồm các thành phần như cửa sổ, nút bấm, ô nhập liệu và các yếu tố điều hướng khác. Hai thành phần cốt lõi của GUI là menu Bắt đầu (Start Menu) và thanh tác vụ (Taskbar), cùng với màn hình nền (Desktop), đóng vai trò quan trọng trong trải nghiệm người dùng.

— Giao diện dòng lệnh (Command Line): Đây là phương thức giao tiếp lâu đời nhất của Microsoft, dựa trên hệ thống lệnh DOS, được truy cập thông qua chương trình cmd.exe. Giao diện này cho phép người dùng thực hiện các thao tác cấu hình hệ thống hoặc chạy các ứng dụng DOS truyền thống.

— Giao diện PowerShell: Là một giao diện dòng lệnh hiện đại, PowerShell được thiết kế đặc biệt cho các tác vụ quản trị. Tính năng nổi bật của PowerShell là khả năng lập trình (scripting), cho phép sử dụng các hàm logic và biến để tự động hóa các tác vụ một cách hiệu quả hơn nhiều so với giao diện DOS. Ngoài ra, PowerShell hỗ trợ thực thi lệnh từ xa, nhờ vào sự tích hợp với hệ điều hành.

2.1.2.4. Đặc điểm, đặc trưng

- Đặc điểm:

— Giao diện thân thiện, dễ sử dụng cho người dùng.

— Hỗ trợ tương tác thông qua các lệnh văn bản.

— Các phiên bản Windows mới nhất đã cải tiến giao diện, tập trung vào trải nghiệm đồ họa trực quan hơn.

- Đặc trưng:

— Hỗ trợ chế độ đa nhiệm, cho phép chạy nhiều ứng dụng cùng lúc.

— Sử dụng giao diện dựa trên menu với các biểu tượng kết hợp giữa hình ảnh và chú thích văn bản.

— Cung cấp các công cụ mạnh mẽ để xử lý đồ họa và đa phương tiện (âm thanh, video).

— Tối ưu hóa việc xử lý nhiều loại dữ liệu như hình ảnh, âm thanh.

— Đảm bảo khả năng hoạt động hiệu quả trong các môi trường mạng.

2.1.3. Phần mềm diệt Virut, chống phần mềm gián điệp, chống các phần mềm độc hại, cứu hộ

2.1.3.1. Phần mềm diệt virus: AVG AntiVirus

❖ Khái niệm:

AVG AntiVirus là một phần mềm bảo mật do AVG Technologies phát triển, được thiết kế để bảo vệ máy tính khỏi các mối đe dọa trực tuyến như virus, phần mềm gián điệp, rootkit, mã độc và các tệp nguy hiểm khác. Phần mềm này cung cấp các tính năng như quét virus, tường lửa ngăn chặn truy cập trái phép, bảo vệ chống thư rác và bảo vệ đám mây để chặn các tệp độc hại tải xuống từ internet. AVG AntiVirus có phiên bản miễn phí và phiên bản trả phí với các tính năng nâng cao, hỗ trợ trên nhiều nền tảng bao gồm Windows, macOS và Android.

❖ Tính năng:

— Bảo vệ thời gian thực với công nghệ CyberCapture mạnh mẽ, ngăn chặn các mối đe dọa bảo mật.

— Chế độ thụ động cho phép chạy đồng thời với các công cụ bảo mật khác.

— Tăng cường bảo vệ trực tuyến bằng cách kiểm tra các liên kết, trang web và dữ liệu tải về.

— Hỗ trợ quét virus miễn phí và tối ưu hiệu suất máy tính với AVG TuneUp.

— Giao diện trực quan, dễ sử dụng với thiết kế hiện đại.

— Khắc phục lỗi màn hình xanh (BSOD) khi sử dụng chức năng Anti-Rootkit.

— Hỗ trợ danh sách trắng/đen cho AntiSpam, áp dụng cho cả email và tên miền.

— Sửa lỗi treo hệ thống khi thực hiện mô phỏng script.

— Tối ưu thời gian quét email hàng loạt trên Microsoft Office 2010.

2.1.3.2. Phần mềm chống gián điệp: Spybot S&D (Spybot – Search & Destroy)

❖ Khái niệm:

Spybot S&D là một công cụ miễn phí do PepiMK Software phát triển, chuyên phát hiện và loại bỏ phần mềm gián điệp và quảng cáo độc hại. Phiên bản ổn định nổi bật là Spybot S&D 1.4. Phần mềm quét ổ cứng để tìm các phần mềm do thám hoặc mô-đun quảng cáo gửi dữ liệu người dùng về cho tin tặc. Khi phát hiện, Spybot S&D sẽ xóa chúng và thay thế bằng các tệp quảng cáo giả, không gây hại.

❖ Phạm vi hoạt động:

Spybot S&D xử lý các mối đe dọa như Aureate, CLPRS, Comet Cursors, eZula HotText, Gator, GoHip, Radiate, WebHancer và WildTangent. Ngoài ra, phần mềm loại bỏ các dấu vết sử dụng như lịch sử duyệt web, tệp đã mở, chương trình đã kích hoạt hoặc cookie, đảm bảo thông tin cá nhân không bị khai thác bởi các phần mềm gián điệp chưa được nhận diện.

❖ Tính năng

— Tính năng tìm và diệt virus (trong phiên bản Home Edition trở lên) được cải tiến, sử dụng cơ sở dữ liệu virus cập nhật liên tục trong ngày.

— Hiển thị thông tin cập nhật chi tiết dưới dạng biểu đồ trực quan.

— Giao diện thân thiện, dễ sử dụng hơn với người dùng.

— Cho phép chọn loại phần mềm độc hại cần xóa và cung cấp thông tin chi tiết về tệp bị nhiễm.

— Hỗ trợ đa ngôn ngữ, dễ dàng thay đổi ngôn ngữ tại Start Center.

— Chức năng quét MRU (Most Recently Used) giúp quét các tệp được sử dụng gần đây.

— Cải thiện khả năng quét rootkit.

— Live Protection có thể bật/tắt theo nhu cầu người dùng.

— Internet Protection tích hợp proxy server để chặn các tên miền độc hại và cookie nguy hiểm.

— Protected Repair Environment dễ sử dụng, hỗ trợ sửa chữa hệ thống bị nhiễm độc.

— Công cụ Boot CD Creator giúp tạo đĩa khởi động để khắc phục máy tính bị ảnh hưởng bởi phần mềm độc hại.

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

❖ Khái niệm

Malwarebytes là một công cụ miễn phí (với phiên bản cao cấp bổ sung thêm tính năng) chuyên phát hiện và loại bỏ các loại phần mềm độc hại như gián điệp, trojan, worm và ransomware. Phiên bản cao cấp cung cấp bảo vệ thời gian thực, phát hiện mối đe dọa ngay khi chúng xuất hiện.

❖ Tính năng

— Phát hiện và xóa bỏ các phần mềm độc hại mà các chương trình diệt virus thông thường có thể bỏ sót.

— Loại bỏ rootkit và khôi phục các tệp bị hỏng do chúng gây ra.

— Ứng dụng công nghệ tiên tiến để tiêu diệt triệt để mã độc.

— Tương thích tốt với các phần mềm diệt virus khác.

— Thực hiện quét

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

❖ Khái niệm:

Kaspersky Rescue Disk là một công cụ cứu hộ khẩn cấp dành cho các máy tính bị nhiễm virus nghiêm trọng, không thể khắc phục thông qua giao diện Windows thông thường. Người dùng có thể tạo một đĩa khởi động bằng Kaspersky Rescue Disk và sử dụng nó để khởi động máy tính, thực hiện quá trình cứu hộ. Ngoài ra, công cụ còn hỗ trợ tính năng Kaspersky USB Rescue, cho phép sử dụng ổ USB thay vì đĩa CD/DVD làm phương tiện khởi động.

❖ Tính năng:

— Giao diện thân thiện, trực quan và dễ sử dụng.

— Quá trình quét đơn giản, hiệu quả.

— Tạo báo cáo chi tiết về kết quả quét.

— Cho phép cách ly, khử trùng hoặc xóa các tệp bị nhiễm virus.

— Hỗ trợ tùy chọn bỏ qua các loại tệp cụ thể để tối ưu hóa quá trình quét.

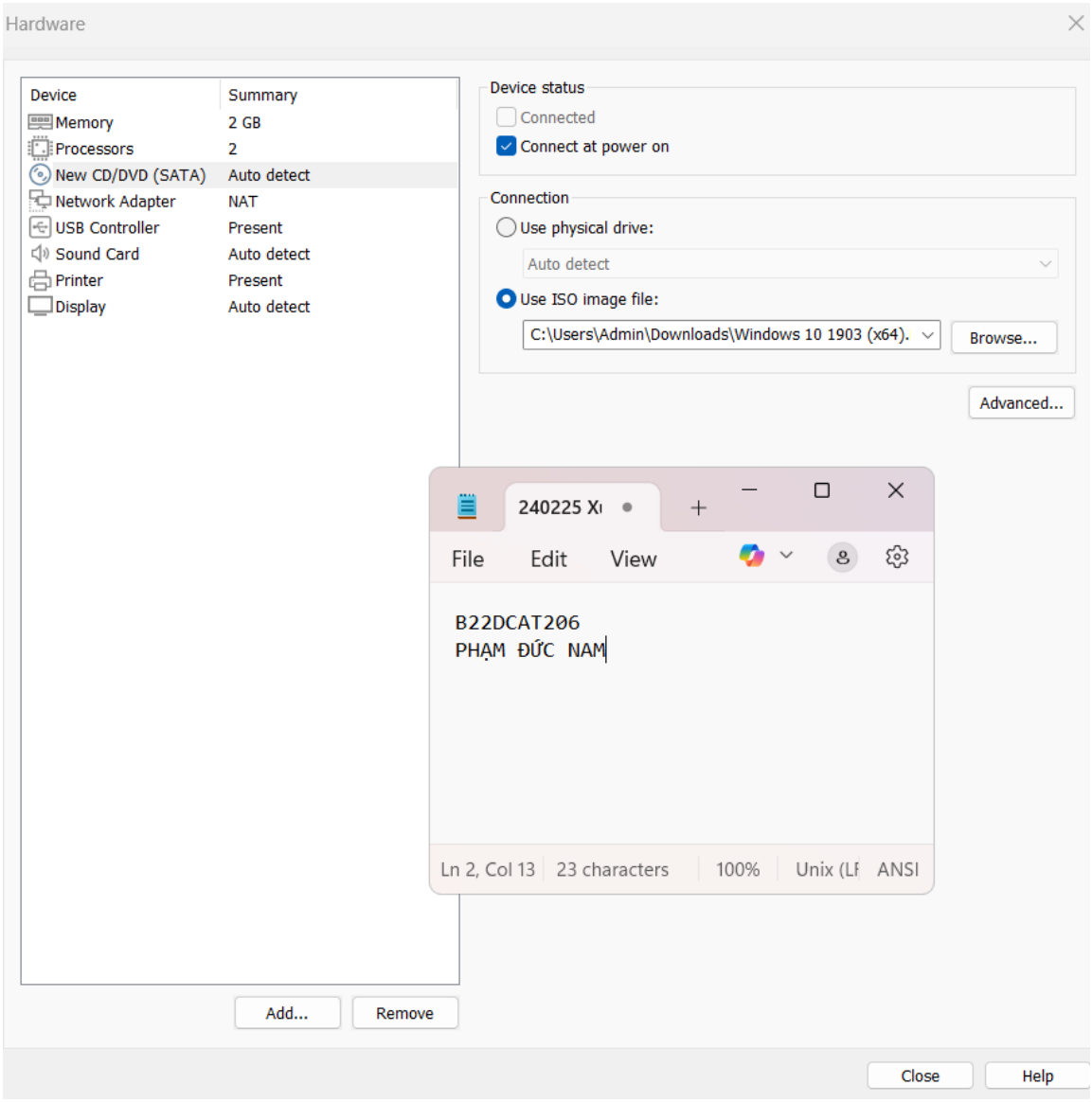
2.2. Nội dung thực hành

2.2.1. Cài đặt thành công Windows 10 trên VMWare Workstation

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

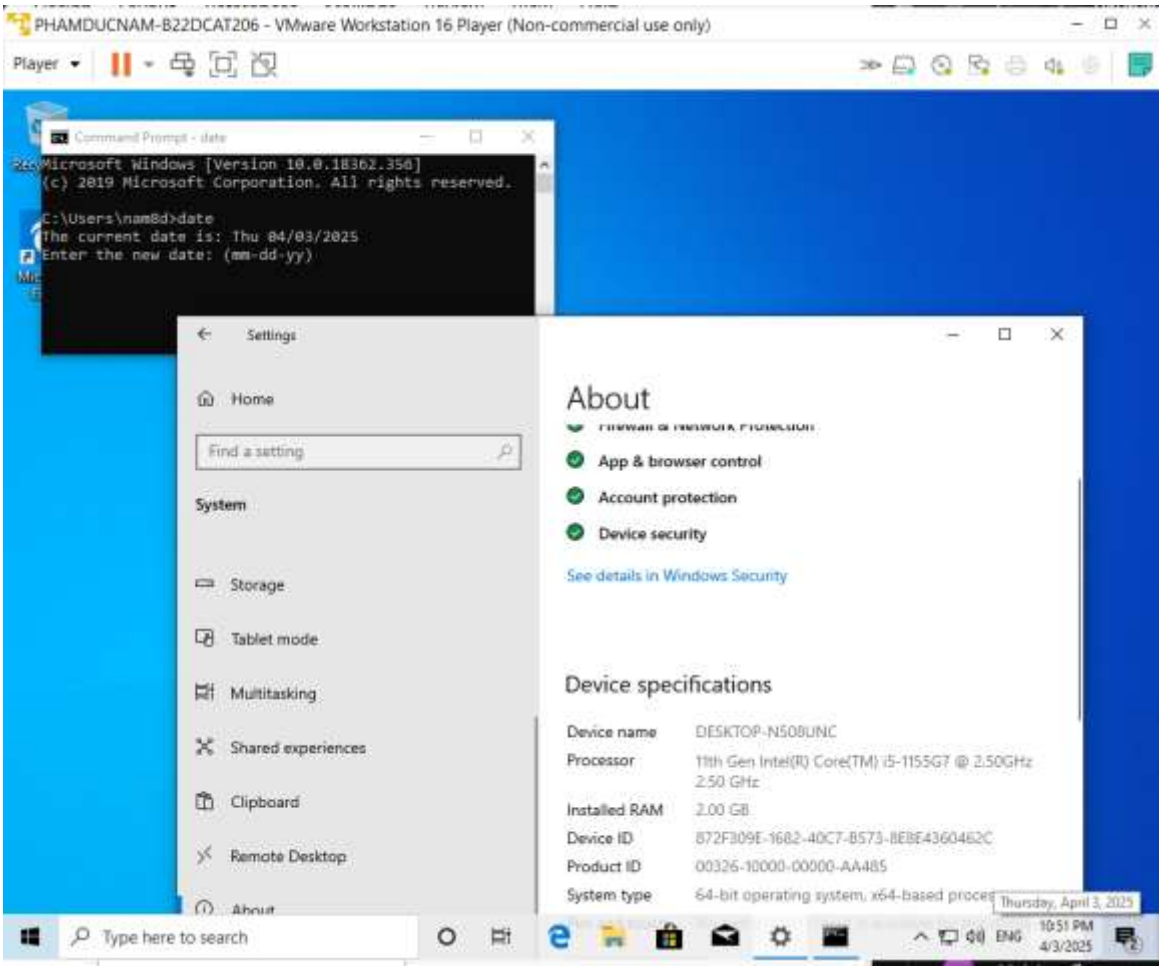
Hình 1 cửa sổ New Vitual Machine Wizard

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



Hình 2 Chọn file iso

Bước 3: Đã cài đặt thành công



Hình 3 Giao diện Windows 10 sau khi đã được cài đặt thành công và đổi tên máy

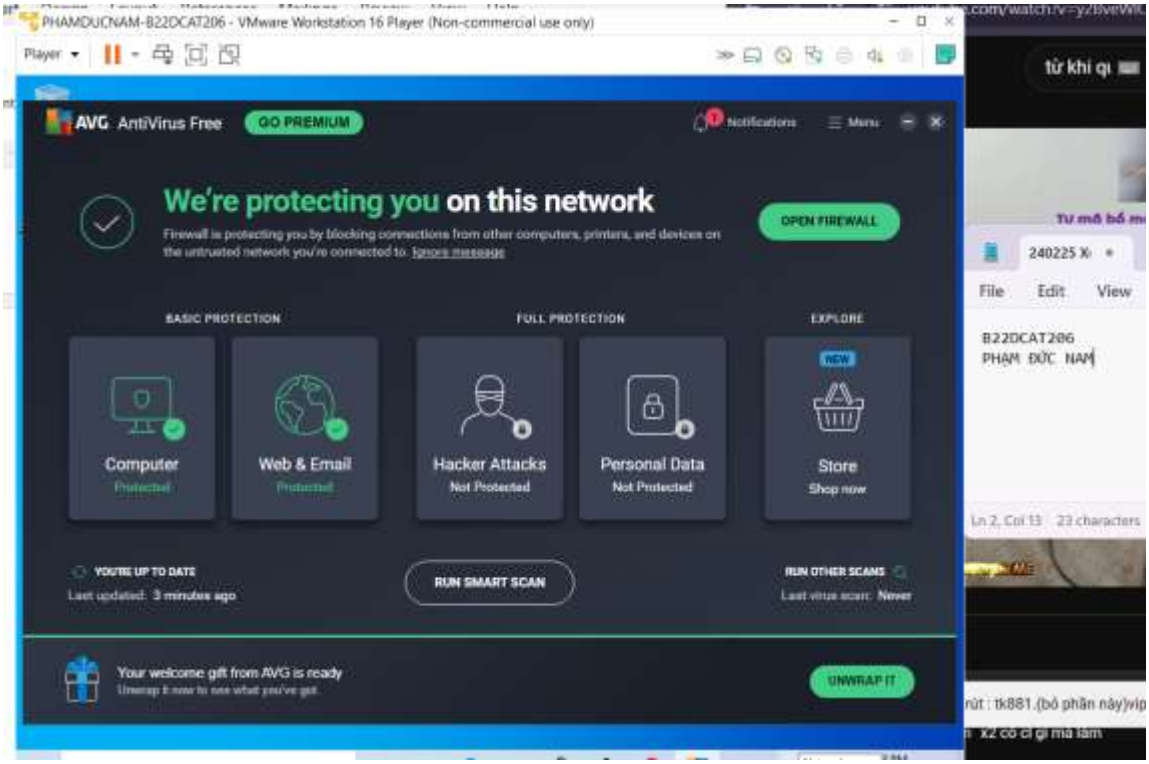
2.2.2. Thực hiện cài đặt và chạy một số phần mềm bảo vệ máy trạm

2.2.2.1. Phần mềm diệt virut: AVG AntiVirus

Hình 4 Phần mềm AVG AntiVirus

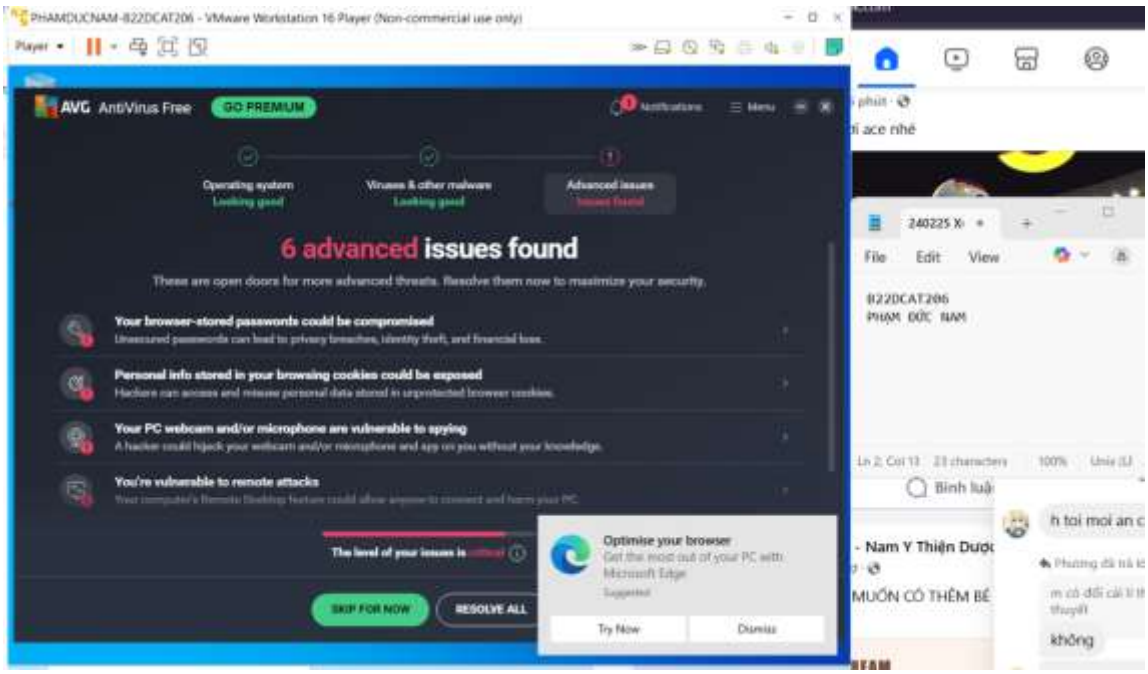
Bước 1: Kích hoạt file cài đặt đã tải về và tiến hành cài đặt

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



Hình 5 Giao diện AVG

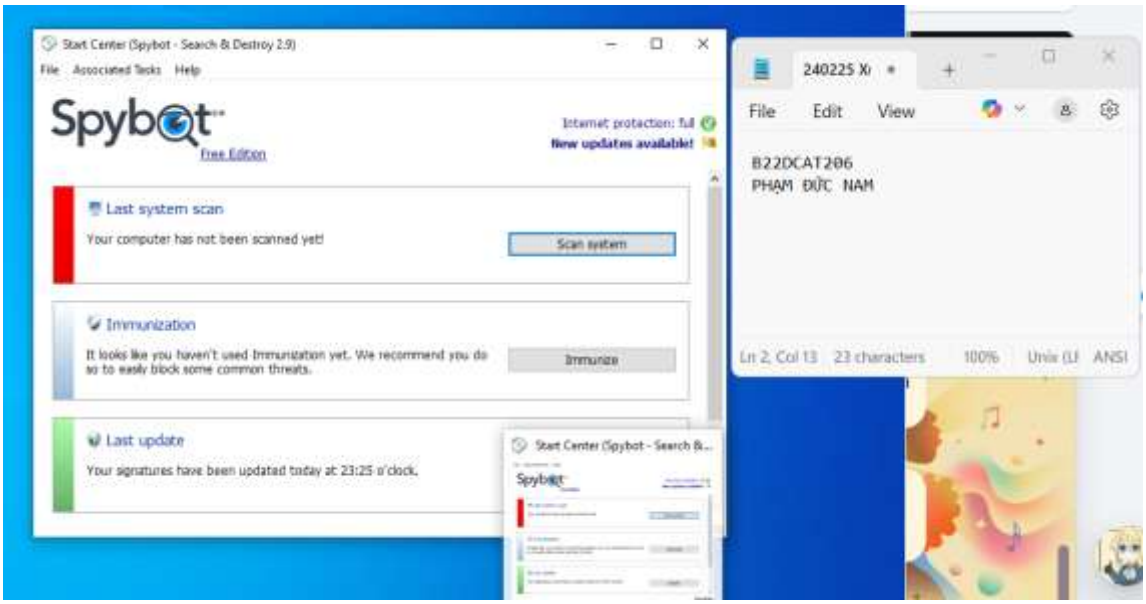
Bước 3: Click *Run Smart Scan* à Kết quả thu được



Hình 6 Chạy thử AVG AntiVirus

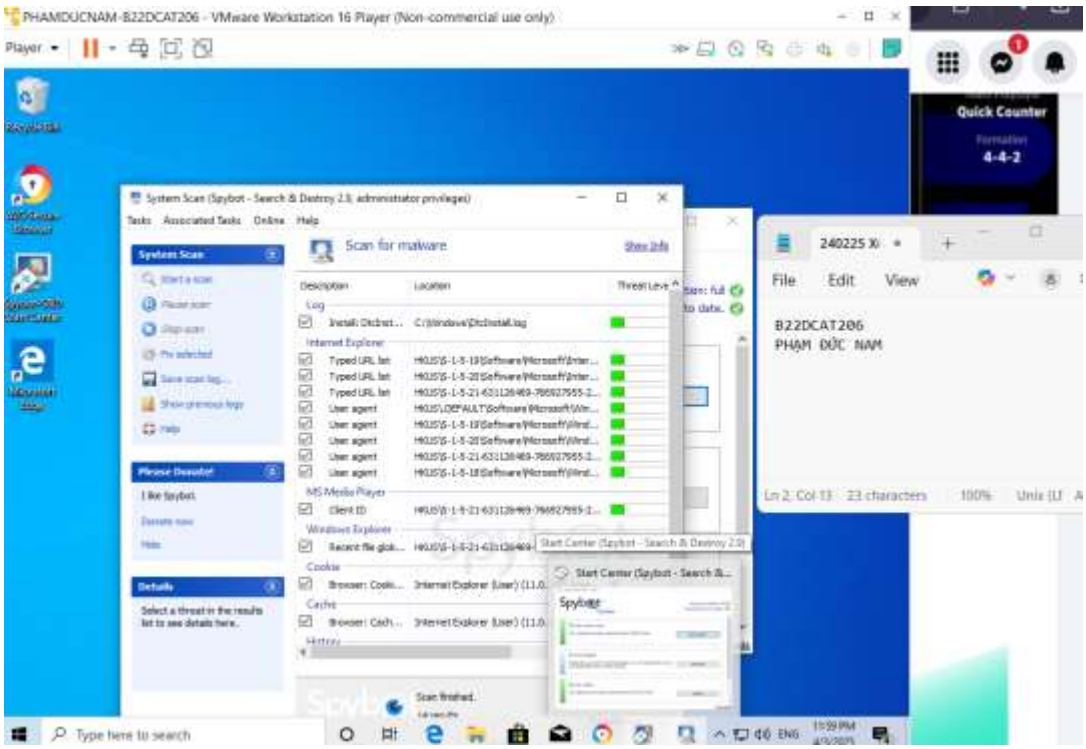
2.2.2.2. Phần mềm chống gián điệp Spybot S&D (Spybot – Search & Destroy)

Bước 1: Khởi chạy file đã cài đặt và tiến hành cài đặt. Giao diện sau khi đã cài đặt thành công.



Hình 7 Giao diện của Spybot S&D sau khi đã cài đặt thành công

Bước 2: Chạy thử phần mềm



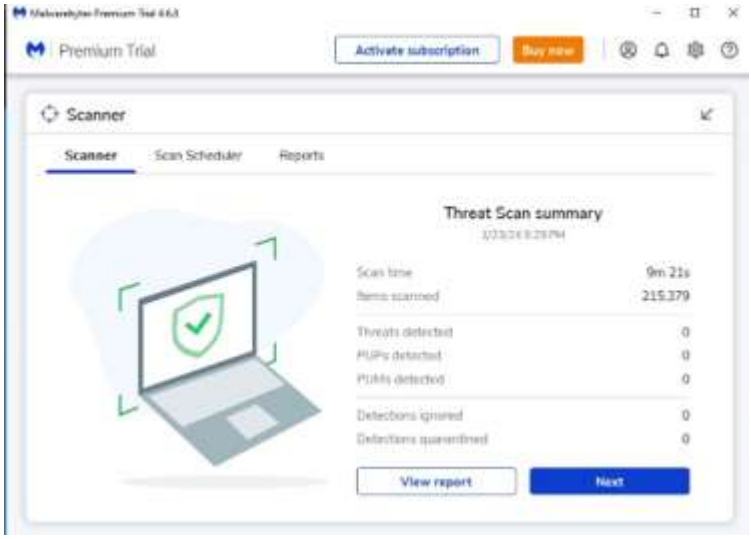
Hình 8 Chạy thử Spybot S&D

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

Bước 1: Khởi chạy file đã cài đặt và tiến hành cài đặt. Chọn bản Personal. Giao diện sau khi đã cài đặt thành công

Hình 9 Malwarebytes Anti-Malware sau khi đã cài đặt thành công

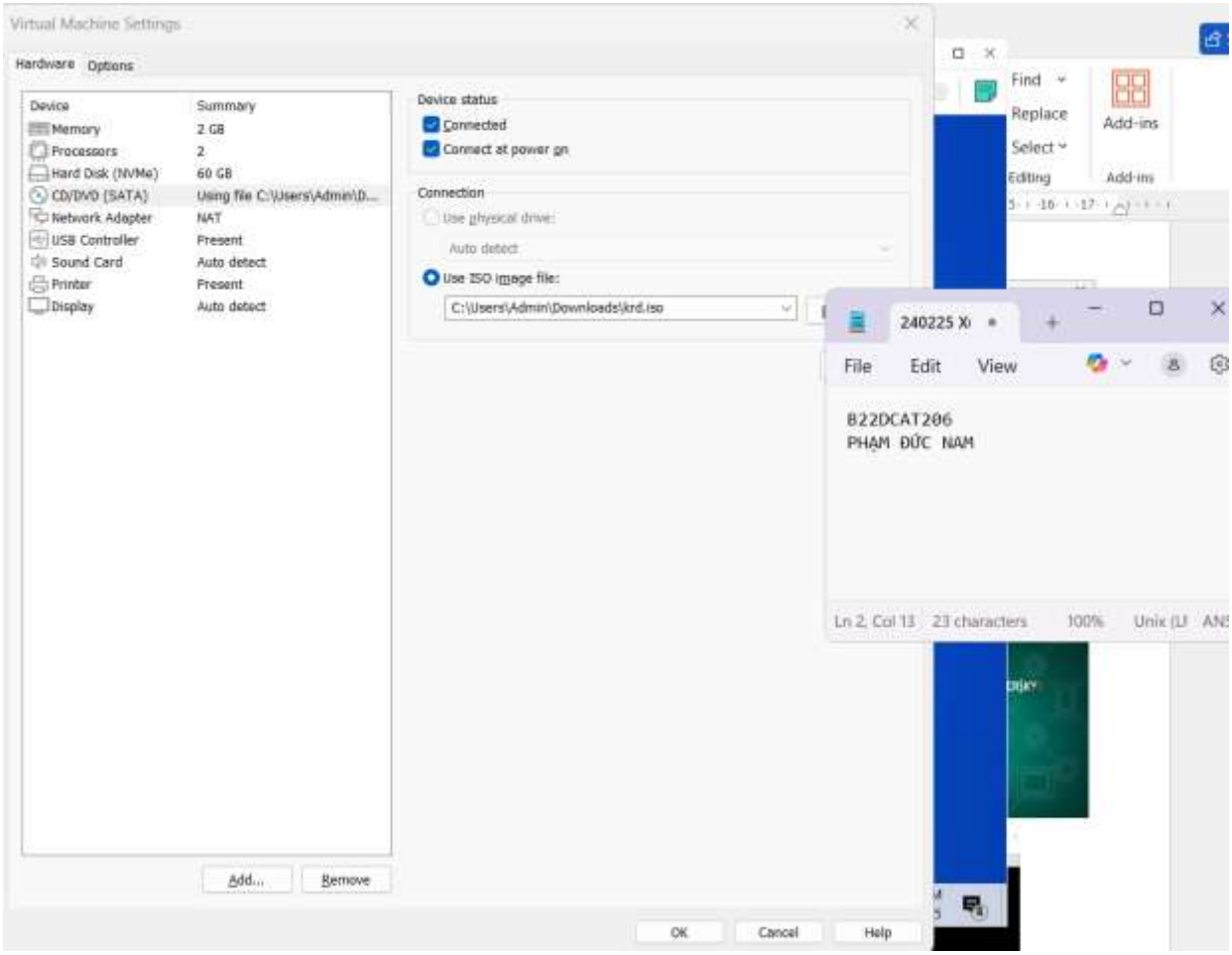
Bước 2: Chọn Get started à Scan để bắt đầu quét. Kết quả sau khi quét thành công.



Hình 10 Chạy thử Malwarebytes Anti-Malware

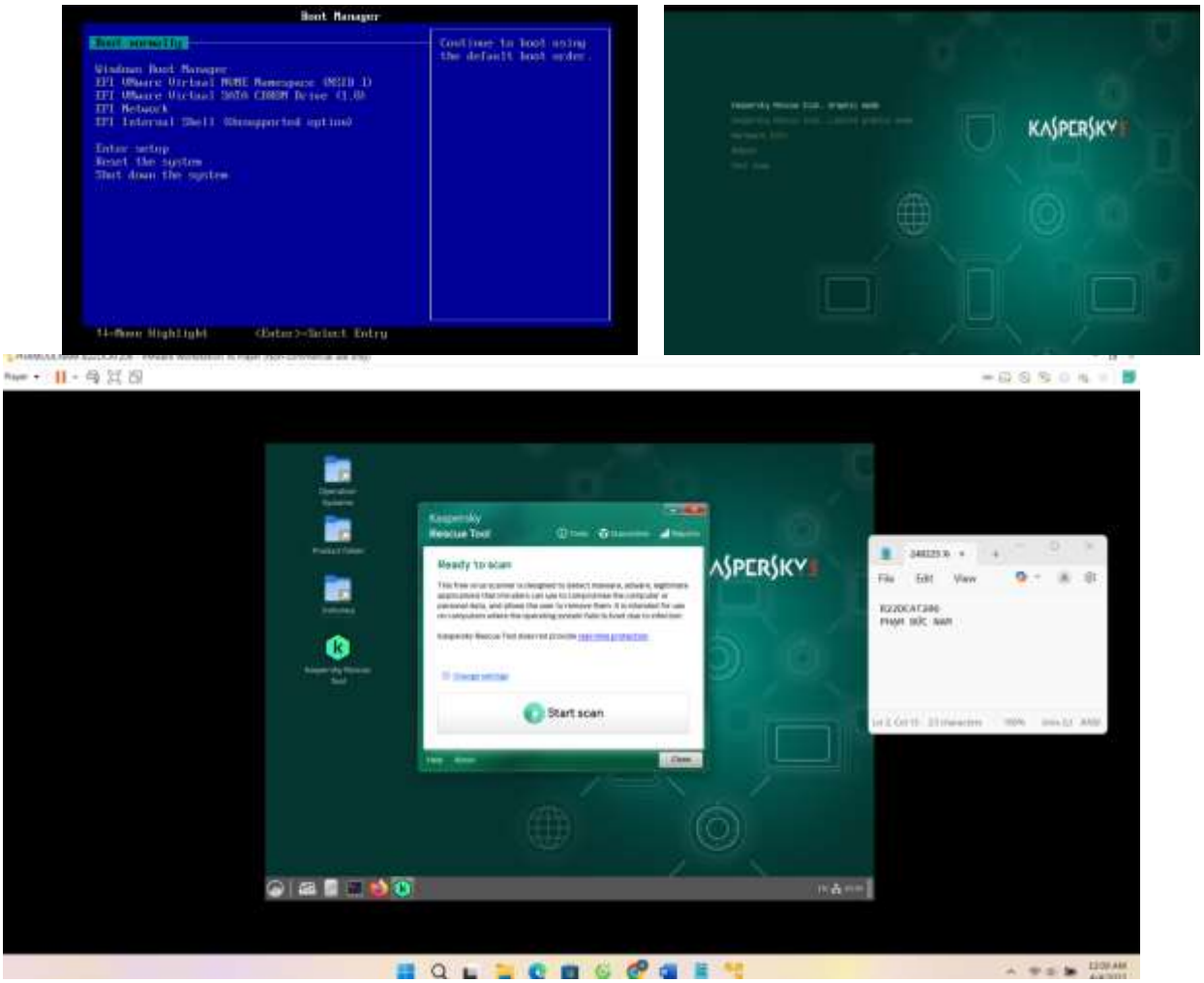
2.2.2.4. Phần mềm cứu hộ: Kaspersky Rescue Disk (KRD)

Bước 1: Load file iso KRD vào trong mục CD/DVD của máy trạm ảo

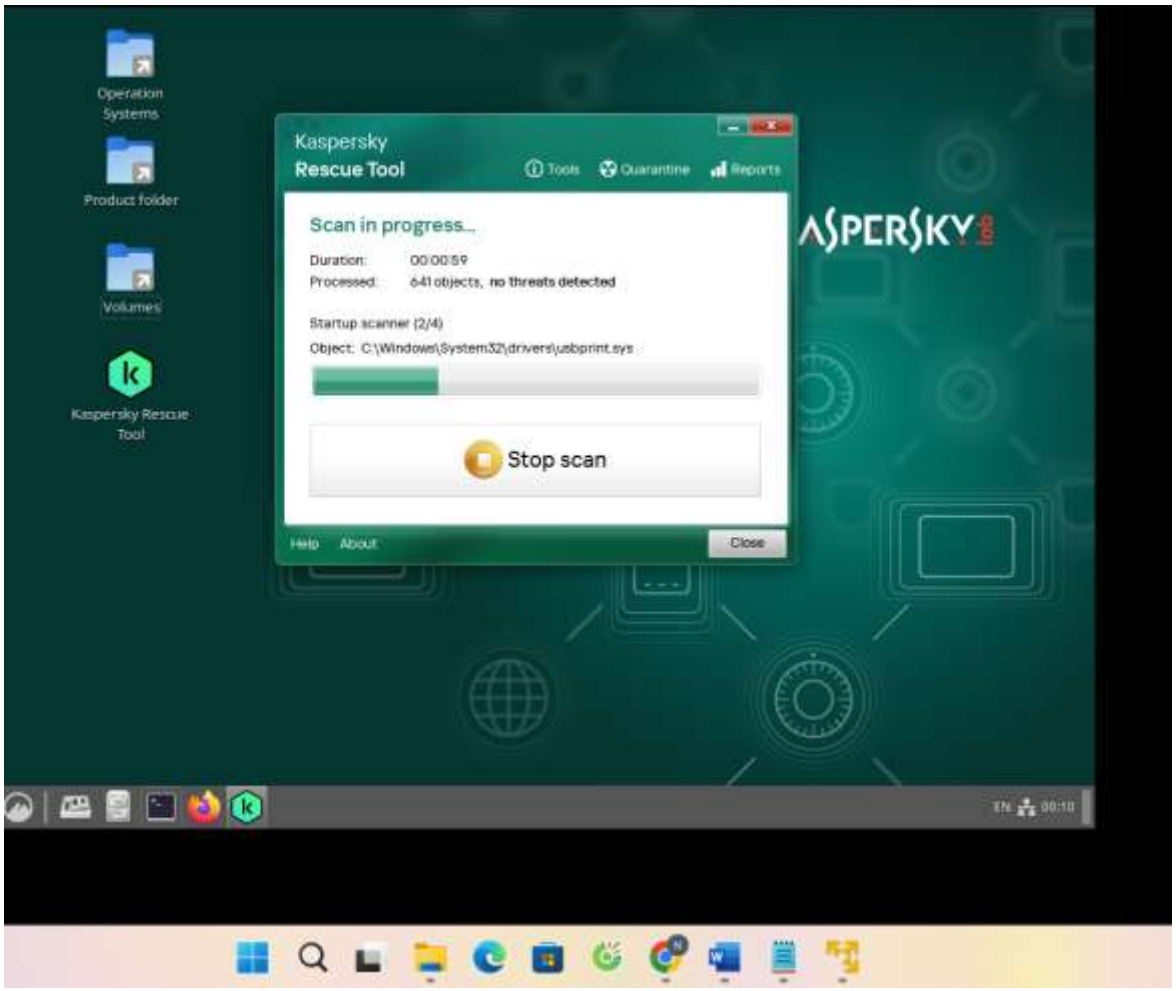


Hình 11 Load file iso KRD vào trong mục CD/DVD của máy trạm ảo

Bước 2: Chạy máy trạm ảo, sử dụng phím “esc” để chọn boot từ CD-ROM drive để cài đặt KRD

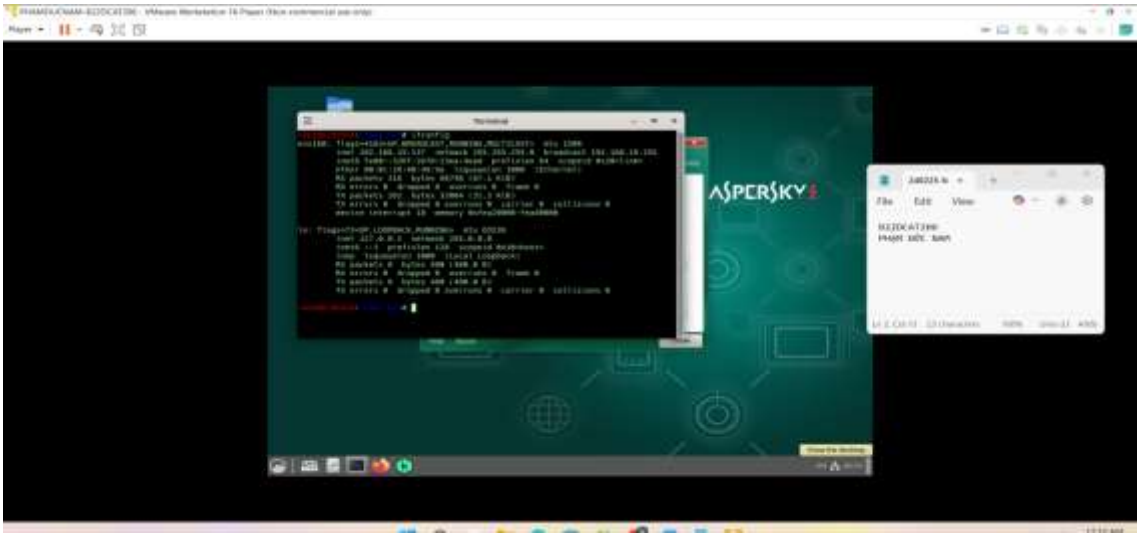


Hình 12 Một số bước tiêu biểu khi cài đặt phần mềm Kaspersky Rescue Disk (KRD)



Hình 13 Giao diện sau khi đã cài đặt thành công.

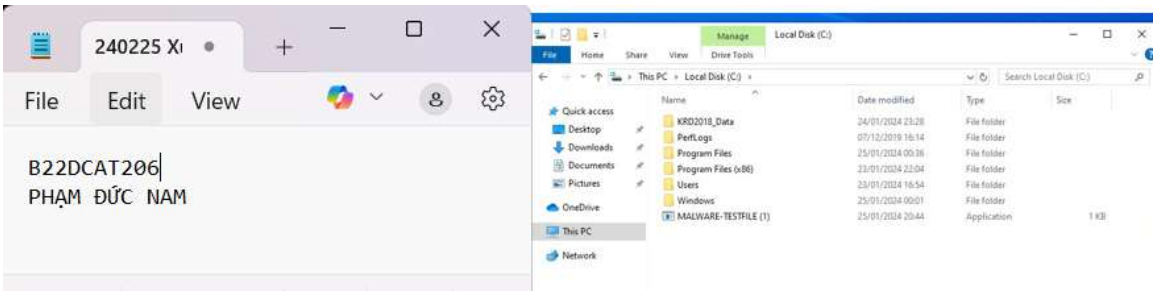
Bước 3: Mở cmd để kiểm tra IP của máy trạm bằng câu lệnh: ipconfig



Hình 14 Kiểm tra IP của máy trạm

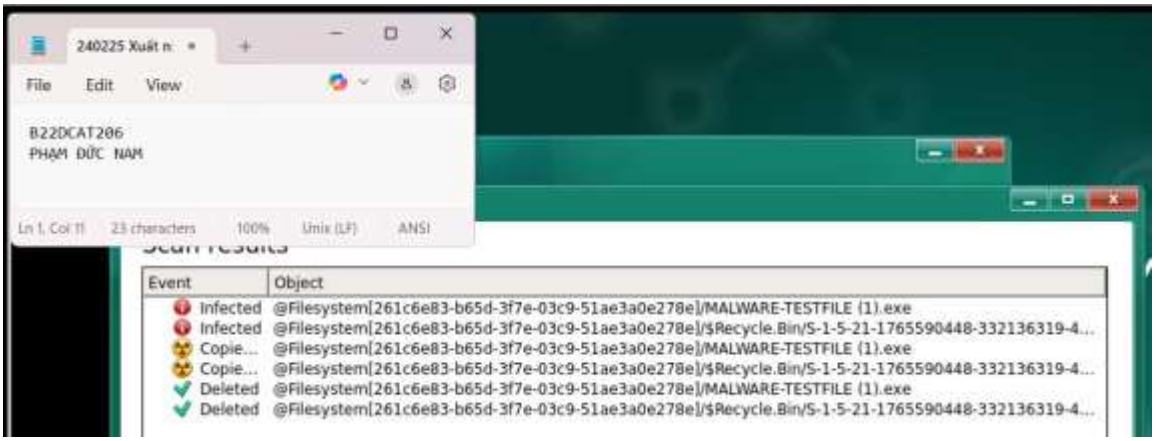
Bước 4: Tải file mã độc từ đường link dưới đây. Lưu file test mã độc vào ổ C của máy trạm

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



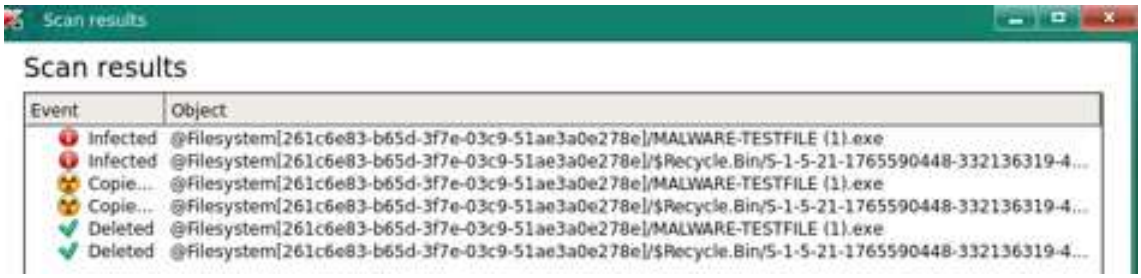
Hình 15 File mã độc được đặt trong ổ C của máy

Bước 5: Sau đó chạy Kaspersky Rescue Tool, vào setting chọn quét tất các các thư mục à phát hiện ra file test mã độc và thực hiện xóa nó.



Hình 16 Sử dụng KDR phát hiện ra file mã độc vừa tải

Bước 6: Chọn Continue để xóa file mã độc



Hình 17 Xóa file mã độc

3. Kết luận

– Cài đặt thành công Windows 10 trên VMWare Workstation

– Thực hiện cài đặt và chạy thành công các phần mềm:

+ Phần mềm diệt virut: AVG AntiVirus.

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

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

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

4. Tài liệu tham khảo

– Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.