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 1

Cài Đặt Hệ Điều Hành Máy Trạm Windows

Họ và tên: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Nhóm môn học: 04

Giảng viên: Đinh Trường Duy

Hà Nội, 1/2024

Mục lục

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. Cơ sở lý thuyết

2.1.1. Phần mềm ảo hóa

2.1.1.1. VMWare Workstation

VMware workStation là một phần mềm chạy trên máy tính cho phép thiết lập một hay nhiều máy ảo trên một máy tính duy nhất và sử dụng đồng thời cùng với máy tính thực tế.

VMware Workstation dựa trên các phần cứng có thể tái tạo các server, destop và máy tính bảng trong một môi trường máy ảo. Người dùng có thể sử dụng VMware Workstation chạy các ứng dụng trên các hệ để hành bao gồm cả Linux, Windows và nhiều máy tính cùng một lúc.

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

- Có thể chạy nhiều hệ điều hành trên một máy vật lý
- Cung cấp báo lỗi và cách ly an toàn với phần cứng
- Tính sẵn sàng cao
- Phần cứng linh hoạt
- Tiết kiệm năng lượng vì tất cả chỉ chạy trên một máy vật lý duy nhất

Bên cạnh những lợi ích thì cũng có một số nhược điểm như:

- Nếu hacker nắm quyền điều khiển máy tính chứa các máy ảo thìhacker có thể kiểm soát được tất cả các máy ảo trong nó.
- Máy tính có cấu hình phần cứng thấp cài nhiều chương trình máy ảo thì dẫn tới máy chậm và ảnh hưởng đến các chương trình khác.
- Nếu máy ảo dùng các tập tin để lưu những gì diễn ra, nên nếu bị mất những tập tin này thì xem như mất máy ảo.

2.1.1.2. Vitual Box

VirtualBox là phần mềm tạo máy ảo miễn phí chuyên nghiệp. Người dùng có thể sử dụng VirtualBox để cài nhiều hệ điều hành trên một máy tính. VirtualBox có sẵn để cài đặt trên Windows, Linux Ubuntu, Mac OS X và Solaris. Vì VirtualBox là một phần mềm ảo hóa 2 các nền tảng, nên bạn có thể trải nghiệm những hệ điều hành

mới, phần mềm mới một cách nhanh chóng và an toàn mà không lo bị nhiễm virus, không lo làm rác máy tính, không phải cài lại hệ điều hành,…

Lợi ích khi sử dụng phần mềm Vitual Box:

- Khả năng tương thích
- Không yêu cầu phần cứng ảo hóa
- Hỗ trợ phần cứng tuyệt vời: đa xử lý, hỗ trợ USB
- Tương thích phần cứng…

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

- Hiệu suất không cao so với một số giải pháp ảo hóa khác.
- Ổn định có thể không đảm bảo, đặc biệt trên môi trường sản xuất.
- Khả năng tương thích không đầy đủ với một số hệ điều hành và ứng dụng.
- Hiệu suất đồ họa có thể kém.
- Hỗ trợ USB có thể gặp vấn đề.
- Quản lý tài nguyên không linh hoạt so với giải pháp ảo hóa chuyên nghiệp.
- Cập nhật và tính năng mới có thể ra mắt chậm.

2.1.2. Hệ điều hành Windows

2.1.2.1. Lịch sử phát triển

Hệ điều hành Windows là một hệ điều hành do Microsoft phát triển, được ra mắt lần đầu vào năm 1985. Dưới đây là một giới thiệu về lịch sử phát triển của từng phiên bản hệ điều hành Windows:

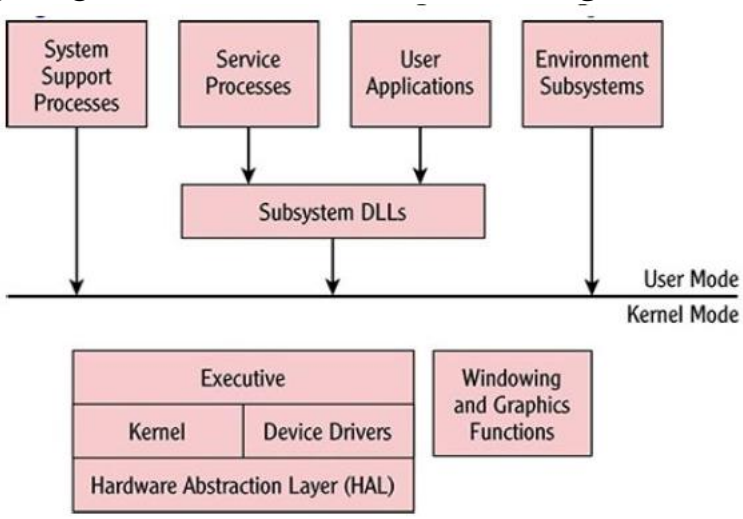
- MS-DoS (1981):
  - Ưu điểm: đơn giản và nhẹ nhàng, làm việc trực tiếp với phần cứng và tập trung vào quản lý tệp tin và lệnh dòng lênh, tương thích với nhiều loại phần cứng và ứng dung, khởi động nhanh.
  - Nhược điểm: giao diện dòng lệnh khó sử dụng, hạn chế về đồ họa và đa nhiệm, quản lý bộ nhớ hạn chế
- Windows 1.0 (1985):
  - Ưu điểm: Đánh dấu sự xuất hiện của giao diện đồ họa đơn giản, tạo ra trải nghiệm người dùng mới.
  - Nhược điểm: Hạn chế tính năng và ổn định, chỉ hỗ trợ một số ứng dụng cơ bản.
- Windows 3.0 (1990):
  - Ưu điểm: Giao diện màu sắc, tăng cường hiệu suất, hỗ trợ ứng dụng đa nhiệm.
  - Nhược điểm: Vẫn còn hạn chế về tính năng và bảo mật.

- Windows 95 (1995):
  - Ưu điểm: Giao diện Start menu và taskbar mới, tích hợp Internet Explorer, tăng cường đáng kể về hiệu suất.
  - Nhược điểm: Ẩn chứa nhiều lỗ hổng bảo mật và có thể gặp vấn đề về ổn định.
- Windows 98 (1998):
  - Ưu điểm: Cải thiện ổn định, hỗ trợ USB, tích hợp nhiều ứng dụng tiện ích.
  - Nhược điểm: Vẫn tồn tại vấn đề về bảo mật và hiệu suất.
- Windows 2000 (2000):
  - Ưu điểm: Dựa trên nền tảng NT, cung cấp tính năng và bảo mật cao, ổn định cho môi trường doanh nghiệp.
  - Nhược điểm: Giao diện người dùng không thay đổi nhiều, không dành cho người dùng cá nhân.
- Windows XP (2001):
  - Ưu điểm: Giao diện đẹp, ổn định và linh hoạt, hỗ trợ nhiều ứng dụng và phần cứng.
  - Nhược điểm: Gặp vấn đề bảo mật, đặc biệt sau sự kiện WannaCry năm 2017.
- Windows Vista (2007):
  - Ưu điểm: Cải thiện đồ họa và bảo mật, giới thiệu Windows Aero.
  - Nhược điểm: Tính năng cao cấp yêu cầu phần cứng mạnh mẽ, gặp vấn đề hiệu suất và tương thích.
- Windows 7 (2009):
  - Ưu điểm: Giao diện Aero, cải thiện hiệu suất so với Vista, tích hợp các tính năng tiện ích.
  - Nhược điểm: Vẫn tồn đọng một số vấn đề bảo mật.
- Windows 8 (2012):
  - Ưu điểm: Giao diện mới, tích hợp tính năng cảm ứng, khả năng đồng bộ đám mây.
  - Nhược điểm: Gây tranh cãi về giao diện đối với người dùng máy tính để bàn truyền thống.
- Windows 10 (2015):
  - Ưu điểm: Trở lại với giao diện truyền thống, tích hợp nhiều dịch vụ đám mây, cải thiện bảo mật.
  - Nhược điểm: Gặp vấn đề về quyền riêng tư và cập nhật bắt buộc.
- Windows 11 (2021):

- Ưu điểm: Giao diện người dùng mới, cải tiến về hiệu suất và trải nghiệm người dùng.
- Nhược điểm: Yêu cầu cấu hình phần cứng cao, có thể gặp khó khăn với một số ứng dụng và trò chơi.

2.1.2.2. 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. 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.



Hình 1 – Kiến trúc cơ bản của 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.

Các khối chức năng cơ bản của chế độ người quản trị như sau:

- Chương trình hỗ trợ hệ thống (System Support Processes): chứa các chương trình thực hiện các chức năng hệ thống như đăng nhập, quản lý phiên làm việc.
- Các chương trình dịch vụ (Service Processes): cung cấp dịch vụ của hệ điều hành như quản lý máy in, tác vụ. Chúng cũng có thể là các dịch vụ như cơ sở dữ liệu hay cung cấp chức năng cho chương trình khác.
- Ứng dụng người dùng (User Applications): Các chương trình thực hiện theo yêu cầu của người quản trị.

- Hệ thống con (Environment Sussystems) và hệ thống liên kết động (Subsystem DLL) kết hợp với nhau cho phép các kiểu ứng dụng khác nhau hoạt động được như môi trường Win32, Win64 hay DOS 32. Trong đó, hệ thống liên kết động chuyển các hàm ứng dụng thành các hàm dịch vụ hệ thống trực tiếp.

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

- Thực thi (Executive) thực hiện việc quản lý các tiến trình và luồng, quản lý bộ nhớ, vào/ra …
- Nhân (Kernel) chịu trách nhiệm điều độ luồng, đồng bộ giữa các tiến trình, xử lý ngắt.
- Các trình điều khiển thiết bị (Device Drivers) làm nhiệm vụ giao tiếp giữa quản lý vào/ra của phần thực thi và phần cứng cụ thể. Các trình điều khiển này cũng có thể liên lạc với hệ thống file, mạng hay giao thức khác.
- Lớp phần cứng trừu tượng (Hardware Abstraction Layer - HAL) giấu đi các chi tiết phần cứng giúp cho hệ điều hành có thể hoạt động trên nhiều phần cứng khác nhau với giao tiếp không đổi.
- Các chức năng cửa sổ và đồ họa (Windowing and Graphics Functions) cung cấp giao diện đồ họa cho người dùng như vẽ các cửa sổ các đối tượng đồ họa.
- Kiến trúc của Windows rất giống với các hệ điều hành khác như Linux hay Mac OS X. Điểm khác biệt căn bản là việc xử lý đồ họa. Windows nhúng chức năng này vào phần nhân để nhằm tăng hiệu năng đồ họa. Linux thì loại bỏ chức năng này ra khỏi phần nhân để tăng độ tin cậy.

2.1.2.3. 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.

- 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). Phần quan trọng khác, đó là màn hình làm việc (desktop).
- Giao diện dòng lệnh: Giao diện này là giao diện xưa nhất của Microsoft đó chính là dòng lệnh DOS 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. 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.

2.1.2.4. Đặc điểm, đặc trưng

❖ Đặc điểm:

- Giao diện thân thiện, đơn giản
- Tương tác với người dùng thông qua các dòng lệnh 5
- Với các phiên bản hệ điều hành Windows mới nhất hiện nay thì giao diện đã có phần cải thiện theo hướng tương tác người dùng đồ họa.

❖ Đặc trưng:

- Chế độ đa nhiệm
- Có một hệ thống giao diện dựa trên cơ sở bảng chọn với các biểu tượng kết hợp giữa đồ họa và văn bản giải thích
- Cung cấp nhiều công cụ xử lí đồ hoạ và đa phương tiện (Multimedia)
- Đảm bảo khai thác có hiệu quả nẳhiều loại dữ liệu khác nhau như âm thanh, hình ảnh
- Đảm bảo các khả năng làm việc trong 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 diệt virus và bảo mật dữ liệu được phát triển bởi AVG Technologies. Phần mềm này giúp bảo vệ máy tính của bạn khỏi các mối đe dọa trực tuyến, bao gồm phần mềm độc hại, virus, phần mềm gián điệp, rootkit, mã độc, các tập tin có chứa mã độc và các tập tin độc hại khác.

AVG AntiVirus cung cấp nhiều tính năng bảo vệ, bao gồm quét virus và phát hiện các tập tin độc hại, tường lửa để ngăn chặn truy cập trái phép, chế độ bảo vệ chống thư rác và bảo vệ đám mây để ngăn chặn các tập tin độc hại được tải xuống từ Internet.

Phần mềm này được cung cấp dưới dạng miễn phí và có thể được nâng cấp lên phiên bản trả phí với nhiều tính năng bảo vệ cao cấp hơn. AVG AntiVirus được hỗ trợ trên nhiều nền tảng, bao gồm hệ điều hành Windows, macOS và Android.

❖ Tính năng:

- Bảo vệ máy tính trong thời gian thực, chống lại các mối đe dọa về an ninh và bảo mật với công cụ quét virus CyberCapture mạnh mẽ.
- Chế độ thụ động (Passive) cho phép chạy 2 công cụ bảo vệ trong cùng 1 thời điểm.
- Cải tiến khả năng bảo vệ online bằng cách quét website, link và dữ liệu tải về để bảo vệ người dùng.
- Quét virus miễn phí và kiểm tra hiệu năng máy với AVG TuneUp.
- Giao diện được thiết kế mới mẻ, trực quan.
- Khắc phục hiện tượng BSOD (màn hình xanh) trong khi quét Anti-Rootkit.
- Bổ sung thêm tính năng hỗ trợ white/black list của AntiSpam dưới dạng địa chỉ email và cả domain.
- Sửa lỗi hệ thống hay bị treo khi thực hiện chức năng giả lập Script.
- Tối ưu hóa hiệu suất để rút ngắn thời gian quét Mass Mailing đối với **Microsoft Office 2010.**
- Sửa lỗi thông tin xác thực hiển thị không chuẩn xác sau khi cập nhật **AVG**.

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

❖ Khái niệm:

Spybot S&D là phần mềm chống phần mềm gián điệp tuyệt vời, miễn phí bởi PepiMK Software phát triển. Phiển bản ổn định phải kể đến là Spybot S&D 1.4. 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, gửi thông tin từ máy của bản về cho hacker. Nếu tìm thấy đối tượng, Spybot S&D sẽ gỡ bỏ và thay thế chúng bằng những adware giả, rỗng.

❖ Phạm vi hoạt động:

Trong số các mục tiêu mà Spybot Search and Destroy xử lý có Aureate, CLPRS, Comet Cursors, eZula HotText, Gator, GoHip, Radiate, WebHancer và WildTangent. Chương trình an ninh này còn loại bỏ phần lưu hồ sơ sử dụng (track) chẳng hạn như các trang web mới truy cập, những file đã mở, các chương trình đã kích hoạt hoặc cookies. Vì thế, ngay cả những loại spyware mà chương trình chưa biết cũng không thể khai thác và truyền đi thông tin cá nhân được.

❖ Tính năng:

- Tính năng tìm & diệt virus (trong bản Home Edition hoặc cao hơn): được cải thiện đáng kể phụ thuộc vào cở sở dữ liệu nhận diện virus tự động cập nhật nhiều lần trong ngày.
- Thông tin cụ thể khi người dùng cập nhật được hiển thị nhất định, đa dạng dưới dạng đồ thị.
- Giao diện chính cũng như thành phần được cải thiện đáng kể, thân thiện hơn rất nhiều với người dùng.
- Dễ dàng hơn trong việc chọn thể loại malware nào bạn mong muốn xóa bỏ, bên cạnh đấy là thông tin chi tiết như những file nào bị lây nhiễm, có nên giữ lại tệp đó hay không...
- Hỗ trợ nhiều ngôn ngữ. Chúng ta có thể dễ dàng thay đổi ngôn ngữ hiển thị trong phần Start Center.
- **MRU (Most Recently Used) Scan:** nếu bạn chỉ muốn quét một số file nhất định nào đó thì có thể thiết lập để Spybot để scan những file được sử dụng gần đây nhất.
- Chức năng **Rootkit Scan** cũng đã được cải thiện đáng kể.
- **Live Protection**: có thể kích hoạt hay không tùy thuộc vào nhu cầu của người dùng.
- **Internet Protection**: được tích hợp với proxy server có khả năng ngăn chặn nhiều domain độc hại, có chứa mã độc và cookies nguy hiểm trong hệ thống.
- **Protected Repair Environment**: chức năng khá mới mẻ này đã dễ sử dụng hơn rất nhiều đối với người dùng.
- Bên cạnh đó là công cụ hỗ trợ **Boot CD Creator** - giúp chúng ta thuận tiện hơn trong việc tạo đĩa boot nhằm khắc phục những máy tính đã bị ảnh hưởng bởi malware

2.1.3.3. 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

- Phát hiện và loại bỏ các phần mềm độc hại, phần mềm gián điệp mà phần mềm diệt virus của bạn có thể bỏ lỡ.
- Loại bỏ rootkit và sửa chữa các tập tin mà chúng làm hỏng.
- Sử dụng công nghệ hàng đầu để loại bỏ hoàn toàn mã phần mềm độc hại.
- Khả năng tương thích với các phần mềm diệt virus khác.
- Quét nhanh với tốc độ cực đại.
- Khả năng quét toàn bộ cho các ổ đĩa.
- Cập nhập dữ liệu hàng ngày.
- Kiểm tra các mối nguy hiểm và khôi phục chúng một cách thuận tiện.
- Danh sách bỏ qua cho cả trình quét và Module bảo vệ.
- Các cài đặt giúp nâng cao hiệu suất cho Malwarebytes Anti-Malware.
- Danh sách nhỏ các tiện ích phụ giúp xóa các malware thủ công.
- **Hỗ trợ đa ngôn ngữ trong đó có cả tiếng Việt.**
- Hoạt động cùng các tiện ích chống malware khác.
- Hỗ trợ dòng lệnh để quét nhanh.
- Menu nội dung được tích hợp để quét file theo yêu cầu.

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

❖ Khái niệm:

Kaspersky Rescue Disk là một công cụ khẩn cấp mà khi máy tính của người dùng bị nhiễm virus nhưng không còn cho phép nó được sửa chữa thông qua chế độ xem phía trước của cửa sổ. Với điều đó, người dùng chỉ cần tạo một đĩa có thể khởi động bằng Kaspersky Rescue Disk, sau đó khởi động qua đĩa để thực hiện cứu hộ khẩn cấp.

Không chỉ có sẵn dưới dạng Kaspersky Rescue Disk, còn có tính năng Kaspersky USB Rescue. Trường hợp người dùng thay đổi phương tiện khởi động từ Đĩa (DVD / CD) thành ổ đĩa flash.

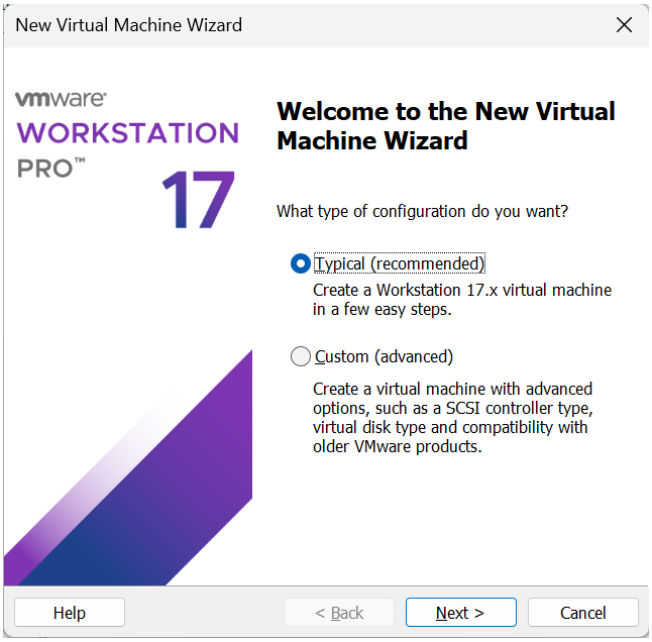
❖ Tính năng:

- Công cụ này rất dễ sử dụng, và có giao diện tiêu chuẩn và trực quan hấp dẫn.
- Thật dễ dàng để quét.
- Đĩa cứu hộ sẽ lập báo cáo kết quả quét 8
- Bất kỳ tệp bị nhiễm nào cũng có thể được cách ly, khử trùng hoặc xóa.
- Có một tùy chọn bỏ qua tệp định dạng nhất định, vì vậy không cần phải quét tất cả các loại tệp.

2.2. Nội dung thực hành

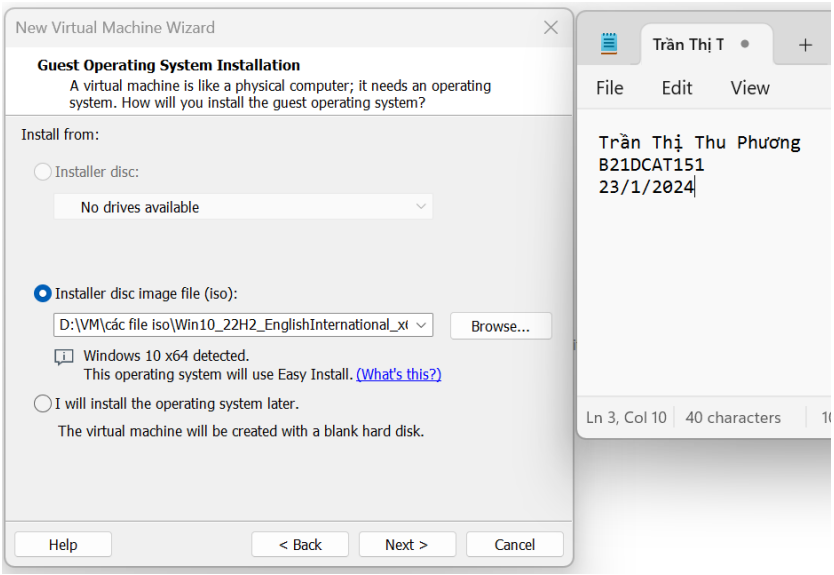
2.2.1. Cài đặt thành công Windows 10 trên VMWare Workstation

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



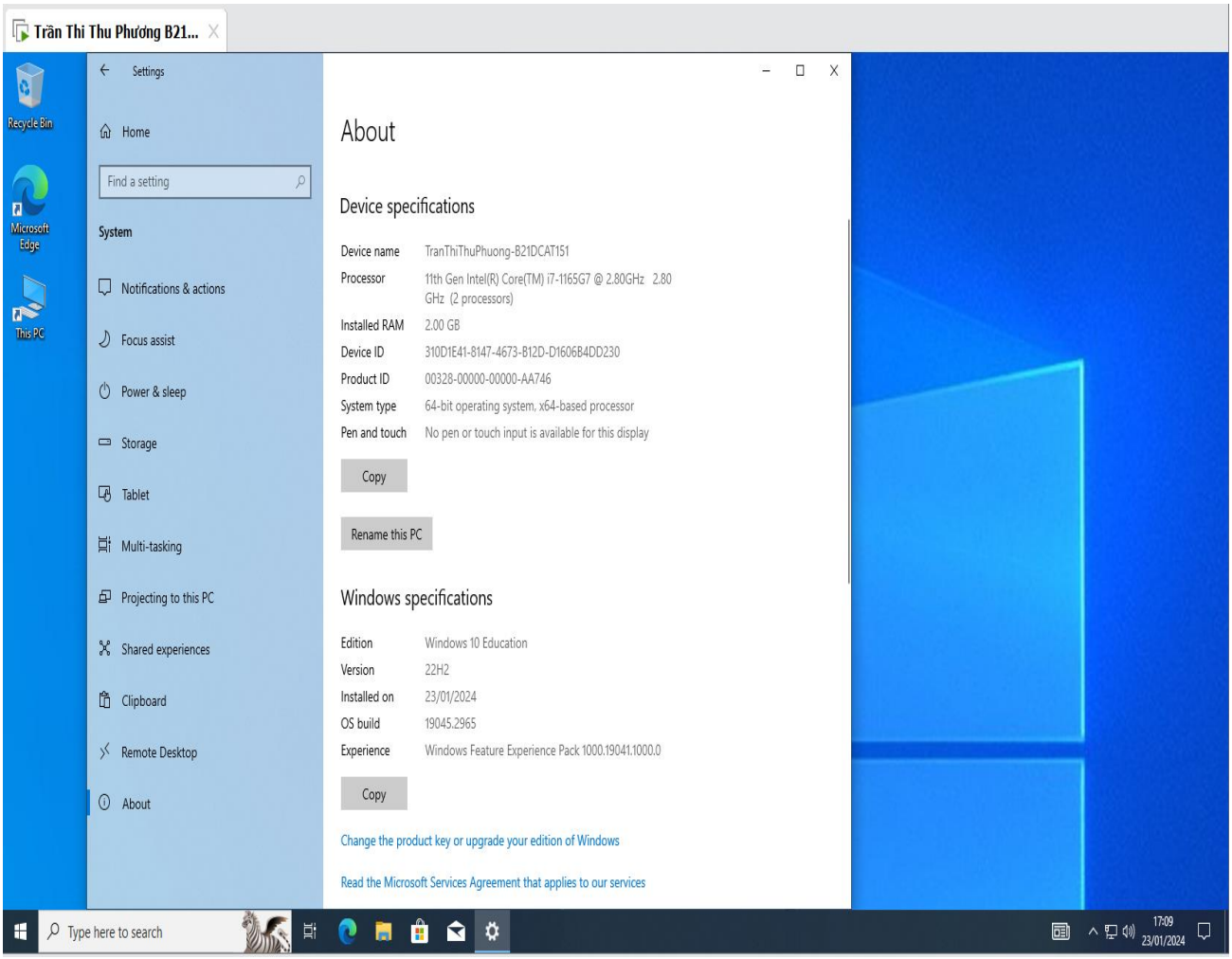
Hình 2 – cửa sổ New Vitual Machine Wizard

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



Hình 3 – Chọn file iso

Bước 3: Đã cài đặt thành công



Hình 4 – 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

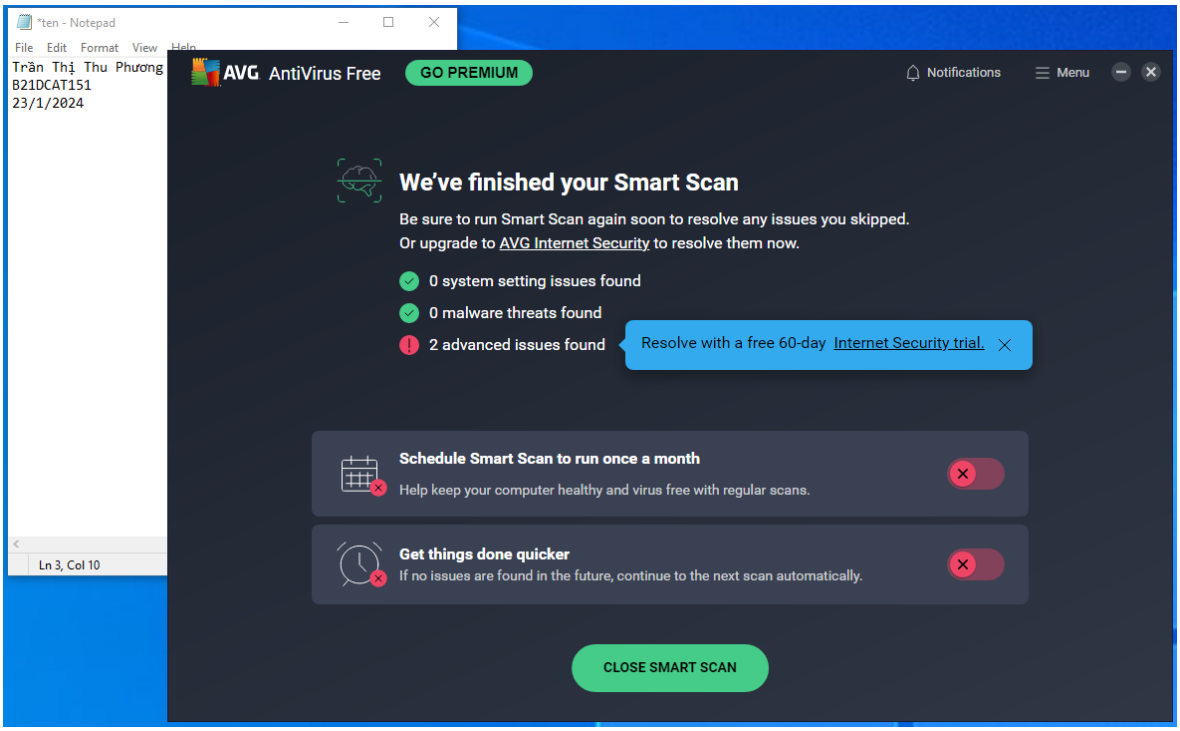
Bước 1: Kích hoạt file cài đặt đã tải về và tiến hành cài đặt

Hình 5 – Phần mềm AVG AntiVirus

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

Hình 6 – Giao diện của phần mềm AVG AntiVirus sau khi cài đặt thành công

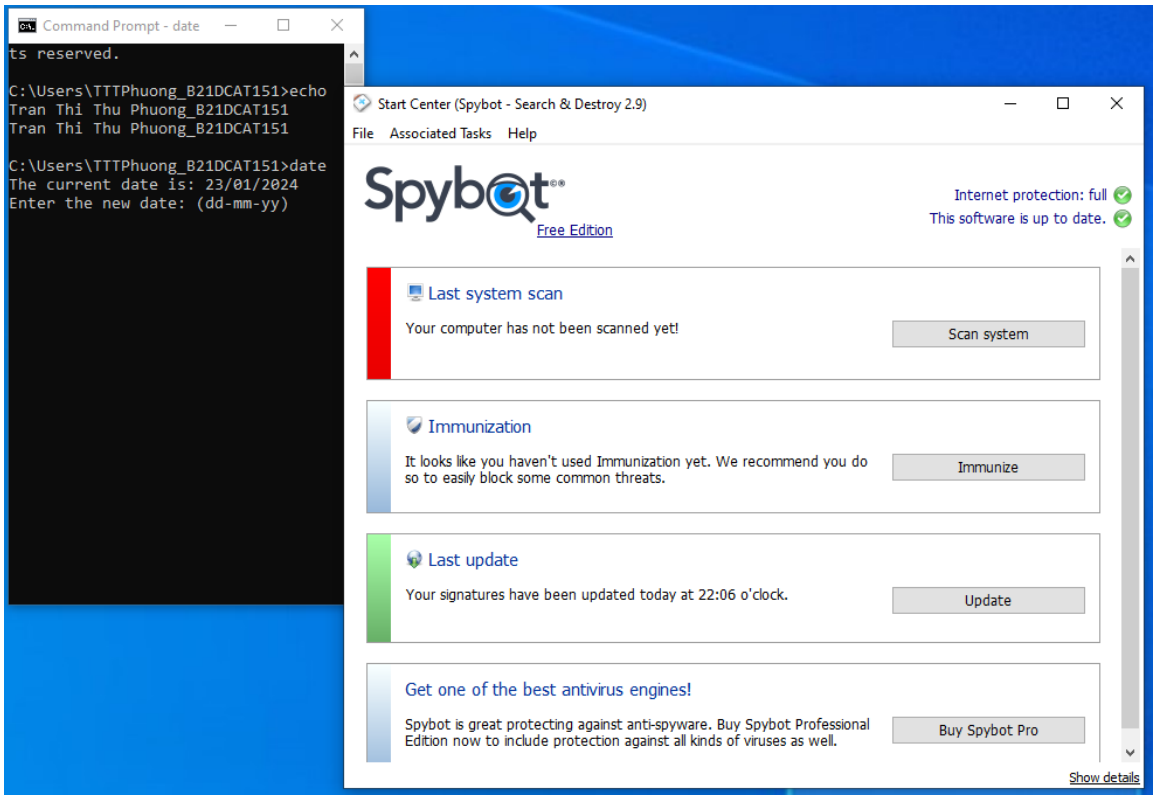
Bước 3: Click *Run Smart Scan* → Kết quả thu được



Hình 7 – Chạy thử AVG AntiVirus

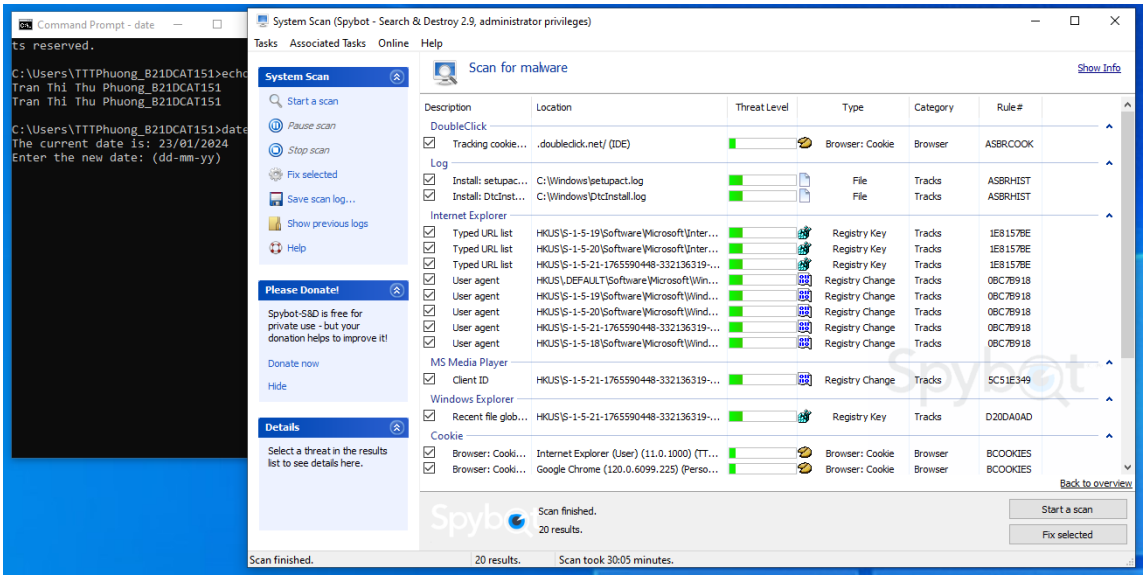
2.2.2.2. Phần mềm chống gián điệp Spybot S&D (Spybot – Search & Destroy)

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



Hình 8 – Giao diện của Spybot S&D sau khi đã cài đặt thành công

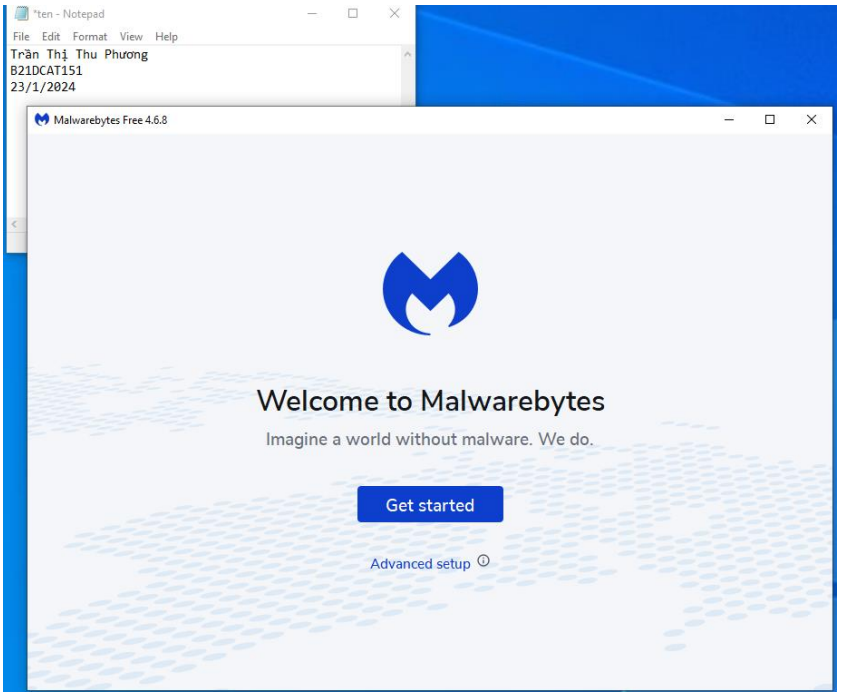
Bước 2: Chạy thử phần mềm



Hình 9 – Chạy thử Spybot S&D

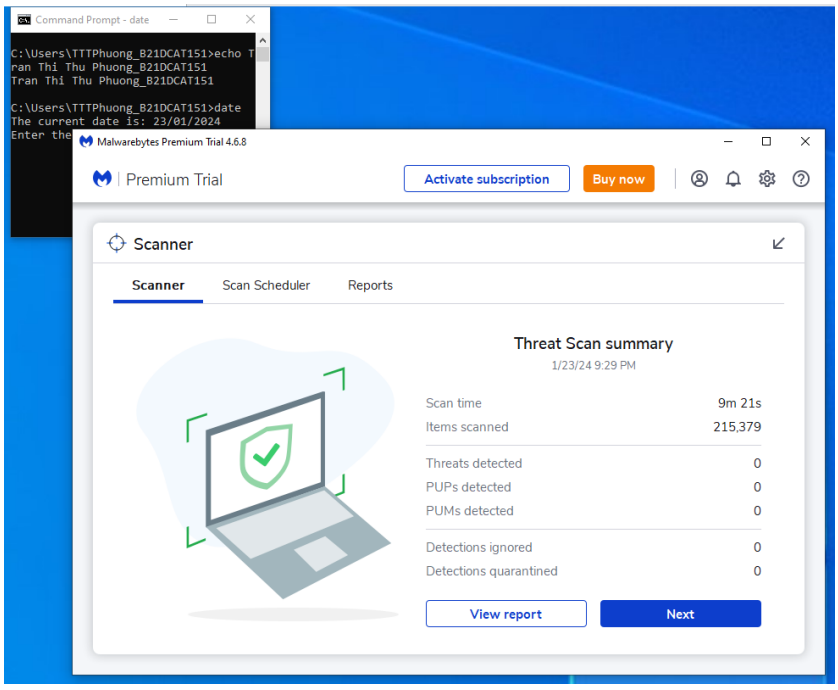
2.2.2.3. Phần mềm chống các phần mềm độc hại: Malwarebytes Anti-Malware

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 10 – Malwarebytes Anti-Malware sau khi đã cài đặt thành công

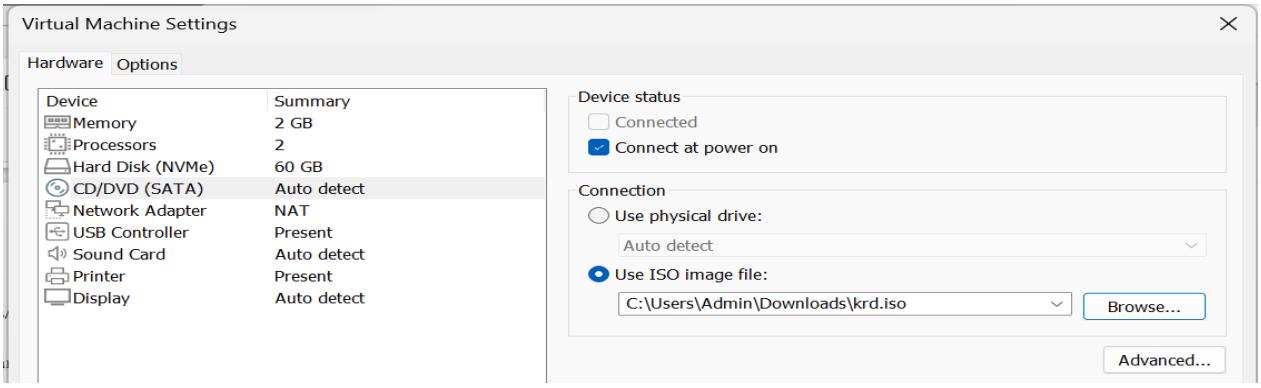
Bước 2: Chọn Get started → Scan để bắt đầu quét. Kết quả sau khi quét thành công.



Hình 11 – Chạy thử Malwarebytes Anti-Malware

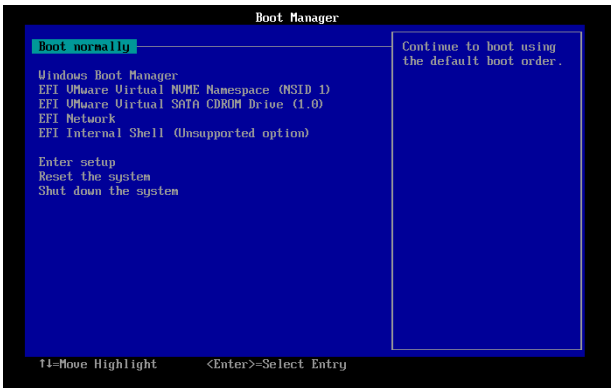
2.2.2.4. Phần mềm cứu hộ: Kaspersky Rescue Disk (KRD)

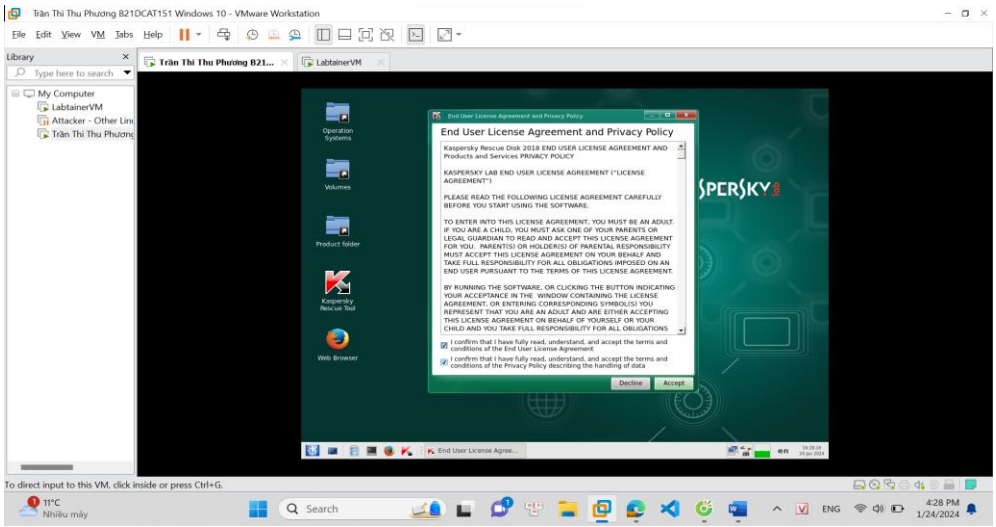
Bước 1: Load file iso KRD vào trong mục CD/DVD của máy trạm ảo



Hình 12 - Load file iso KRD vào trong mục CD/DVD của máy trạm ảo

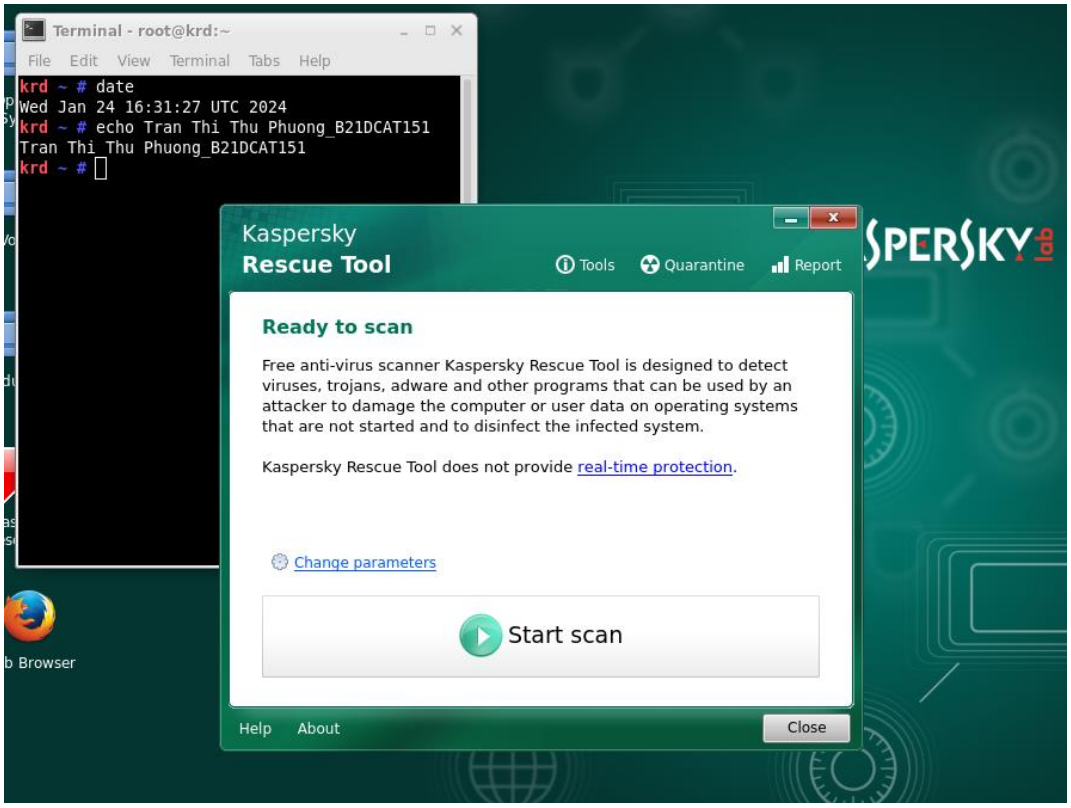
Bước 2: Chạy máy trạm ảo, sử dụng phím "esc" để chọn boot từ CD-ROM drive để cài đặt KRD





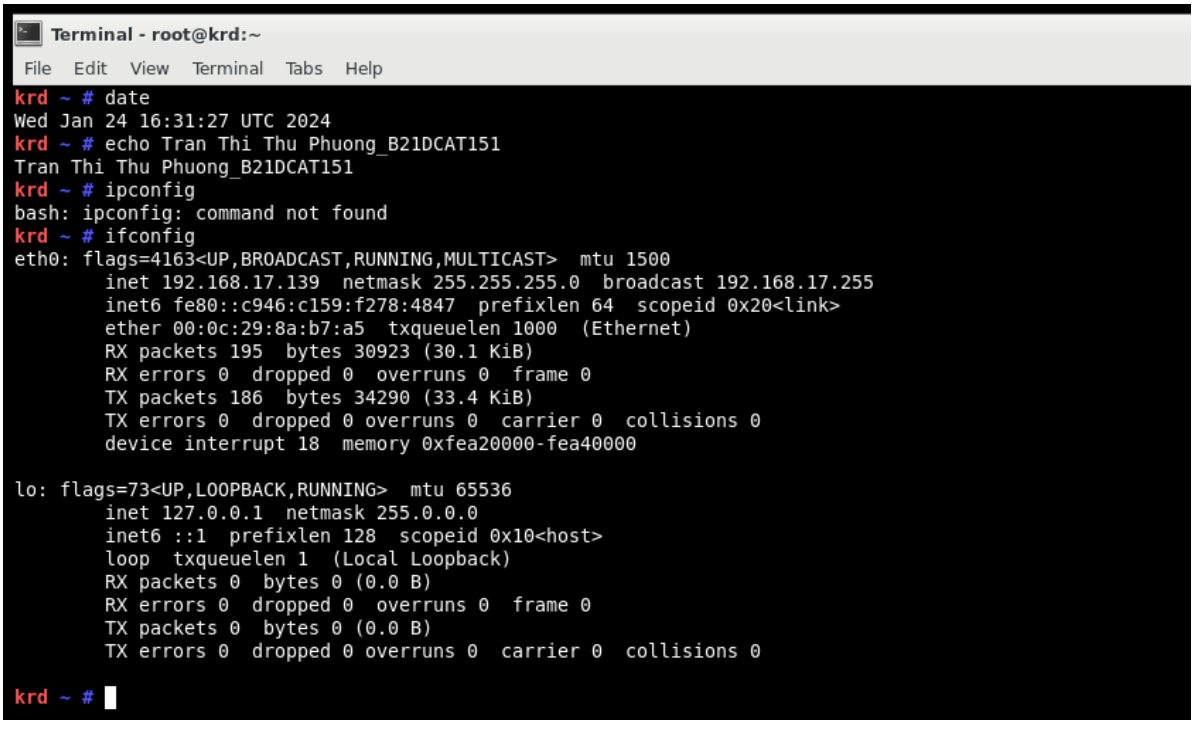
Hình 13 – Một số bước tiêu biểu khi cài đặt phần mềm Kaspersky Rescue Disk (KRD)

Bài 1: Cài đặt hệ điều hành máy trạm Windows



Hình 14 - Giao diện sau khi đã cài đặt thành công.

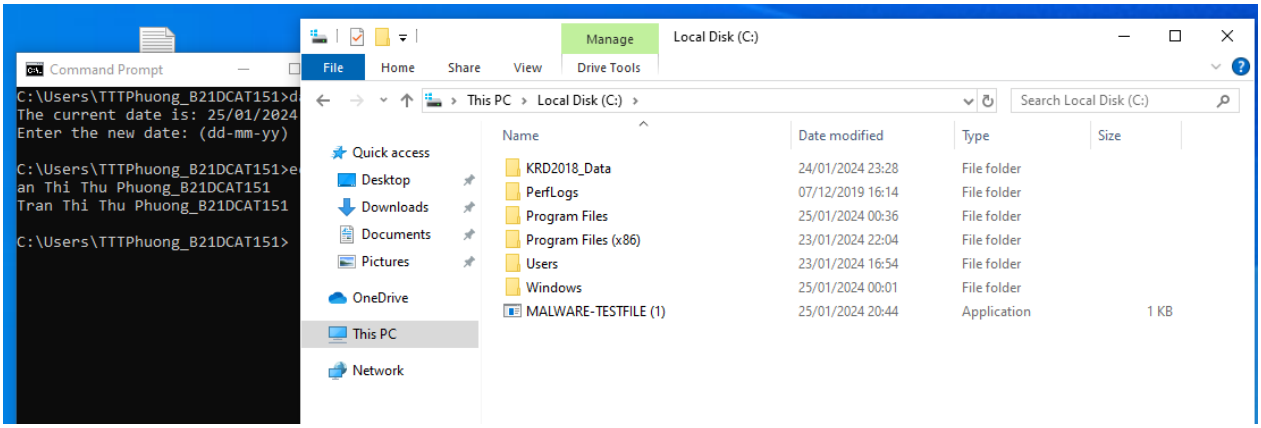
Bước 3: Mở cmd để kiểm tra IP của máy trạm bằng câu lệnh: ipconfig



Hình 15 – Kiểm tra IP của máy trạm

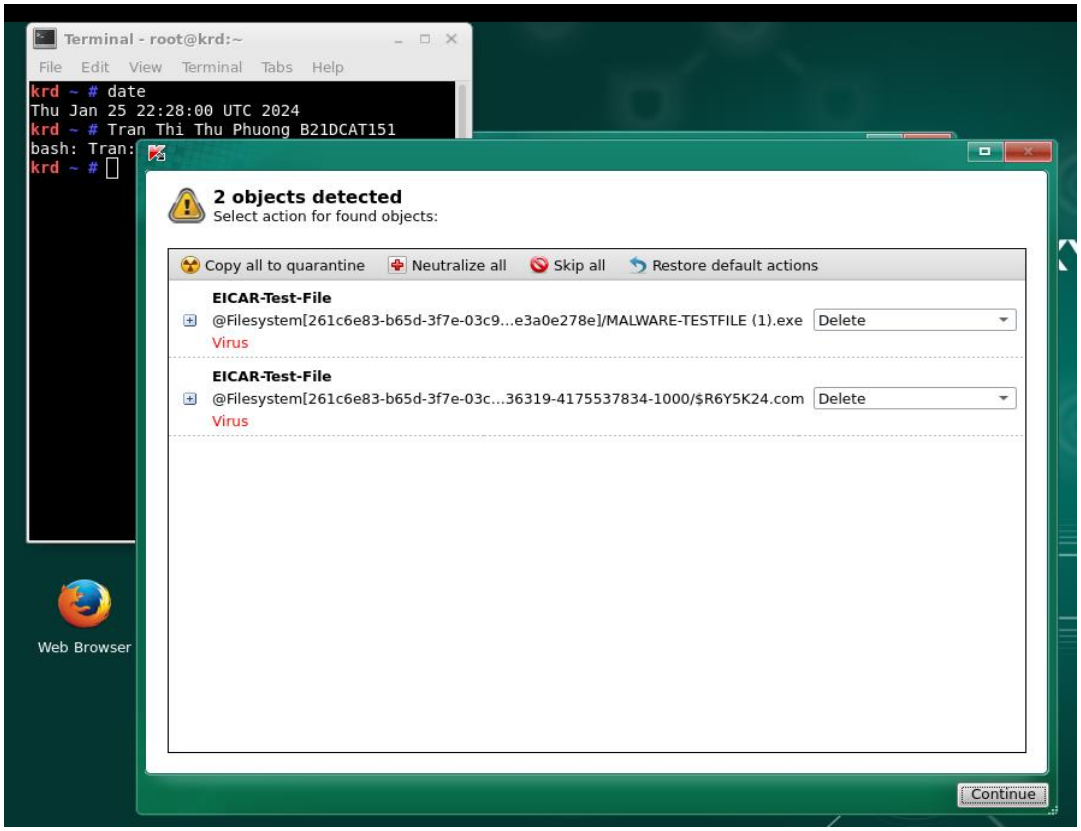
Bước 4: Tải file mã độc từ đường link dưới đây. Lưu file test mã độc vào ổ C của máy trạm

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



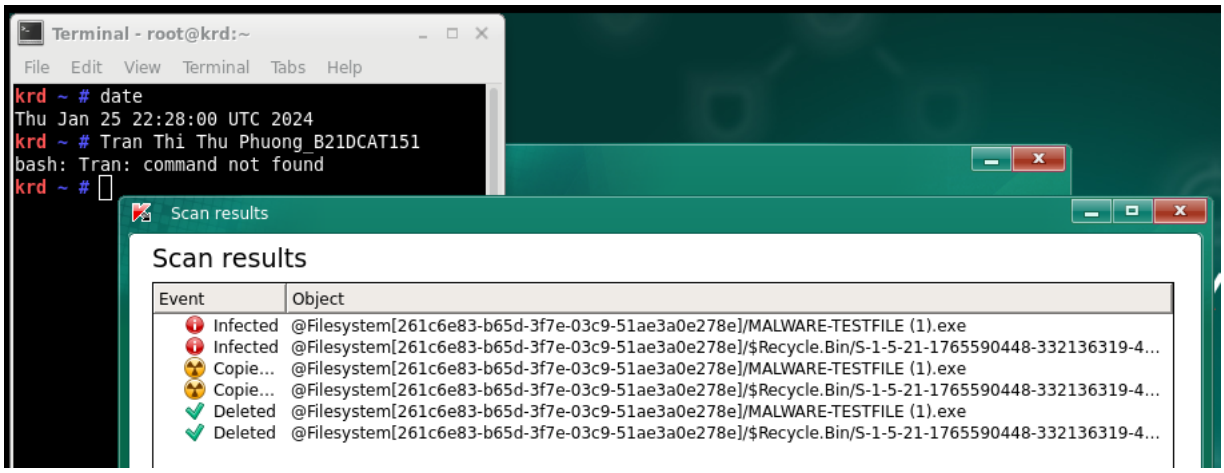
Hình 16 – File mã độc được đặt trong ổ C của máy

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



Hình 17 – Sử dụng KDR phát hiện ra file mã độc vừa tải

Bước 6: Chọn Continue để xóa file mã độc



Hình 18 – 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.
- Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.