HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BỘ MÔN THỰC TẬP CƠ SỞ

BÀI 1:
CÀI ĐẶT HỆ ĐIỀU HÀNH MÁY TRẠM WINDOWS

Giảng viên : Nguyễn Ngọc Điệp
Sinh viên : Nguyễn Đức Anh
Mã sinh viên : B21DCAT031
Hệ : Đại học chính quy

Hà Nội, 2/2024

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 Tìm hiểu lý thuyết

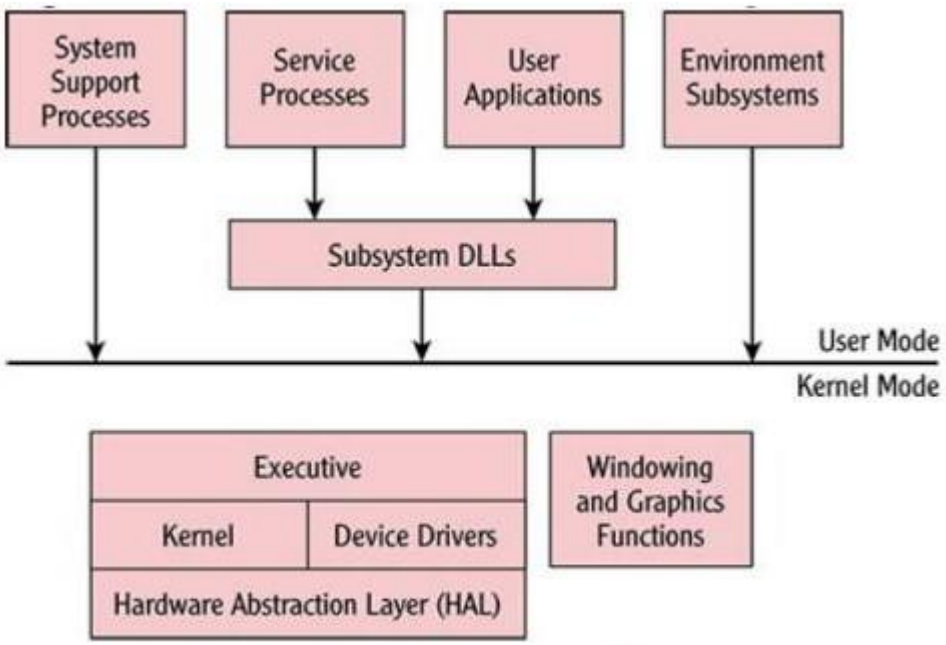
- **Tìm hiểu về hệ điều hành Windows: lịch sử, kiến trúc, giao diện, đặc điểm đặc trưng.**

Lịch sử hệ điều hành Windows

Hệ điều hành Windows ban đầu không sử dụng giao diện đồ họa như hiện nay mà có nguồn gốc từ hệ thống dựa trên ký tự và giao diện đồ họa đơn giản. Phiên bản đầu tiên của hệ điều hành Microsoft là MS-DOS (Disk Operating System – Hệ thống điều khiển đĩa) ra đời vào năm 1981. Tại thời điểm đó, chức năng chủ yếu của hệ điều hành là nạp các chương trình và quản lý các ổ đĩa. Sau hơn 30 năm phát triển, Mircrosoft đã liên tục cập nhật những phiên bản mới cho hệ điều hành Windows và mới đây nhất là hệ điều hành Windows 11.

Kiến trúc hệ điều hành Windows

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 1-3. 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.

Giao diện của hệ điều hành 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. Song đối với bài thực hành này ta chủ yếu tập trung đến giao diện đồ họa.

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) 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.

Hình 1-4. Giao diện GUI Windows

Đặc trưng của hệ điều hành Windows

Hệ điều hành Windows sử dụng chủ yếu 2 hệ thống file: FAT* thừa hưởng từ DOS, và NTFS được sử dụng rộng rãi.

Hệ thống file FAT là một kiểu hệ thống file đơn giản nhất. Nó bao gồm một cung mô tả hệ thống file (cung khởi động-boot sector), bảng cấp phát các khối cấp phát và không gian lưu trữ file và thư mục. Các file được lưu vào thư mục và mỗi thư mục là một mảng gồm các bản ghi 32 byte dùng để mô tả các file hay thuộc tính mở rộng như tên file dài. Bản ghi file trỏ tới khối lưu trữ đầu tiên của file. Các khối lưu trữ tiếp theo được tìm bằng cách truy theo liên kết trong bảng cấp phát.

Hệ thống file NTFS được đưa ra cùng với Windows NT. Đến nay là hệ thống file chủ yếu của hệ điều hành Windows. Hệ thống file này mềm dẻo và hỗ trợ nhiều kiểu thuộc tính file bao gồm kiểm soát truy nhập, mã hóa, nén... Mỗi file trong hệ thống NTFS được lưu bằng một mô tả file trong bảng file chính (master file table) và nội dung của file. Bảng file chính chứa toàn bộ thông tin về file như kích cỡ, cấp phát, tên... Các khối cấp phát đầu tiên và cuối cùng của hệ thống file chứa các cài đặt của hệ thống file. Hệ thống file này sử dụng các giá trị 48 hay 64 bit để tham chiếu file nên hỗ trợ các thiết bị lưu trữ cỡ lớn.

2.2 Tài liệu tham khảo

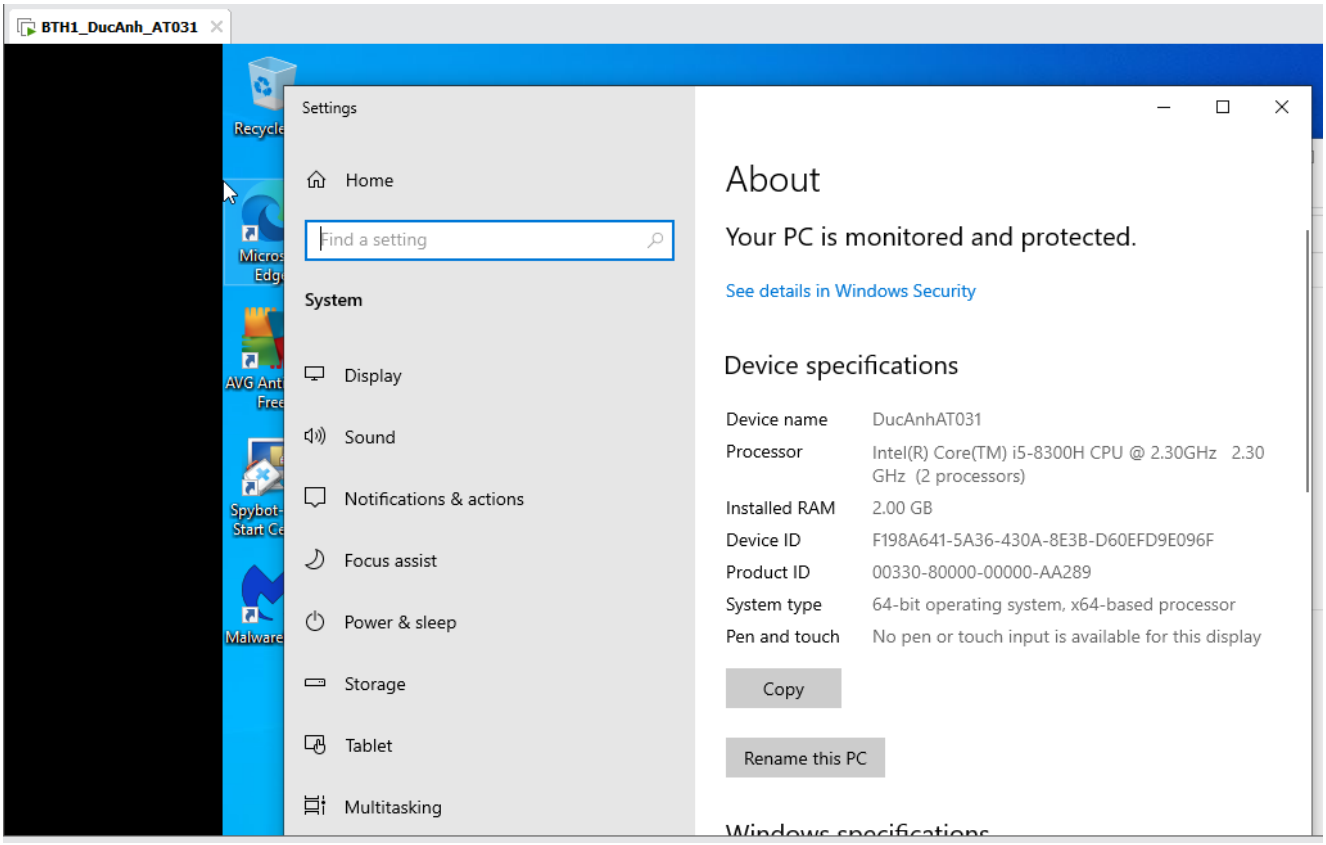
- Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.

2.3 Chuẩn bị môi trường

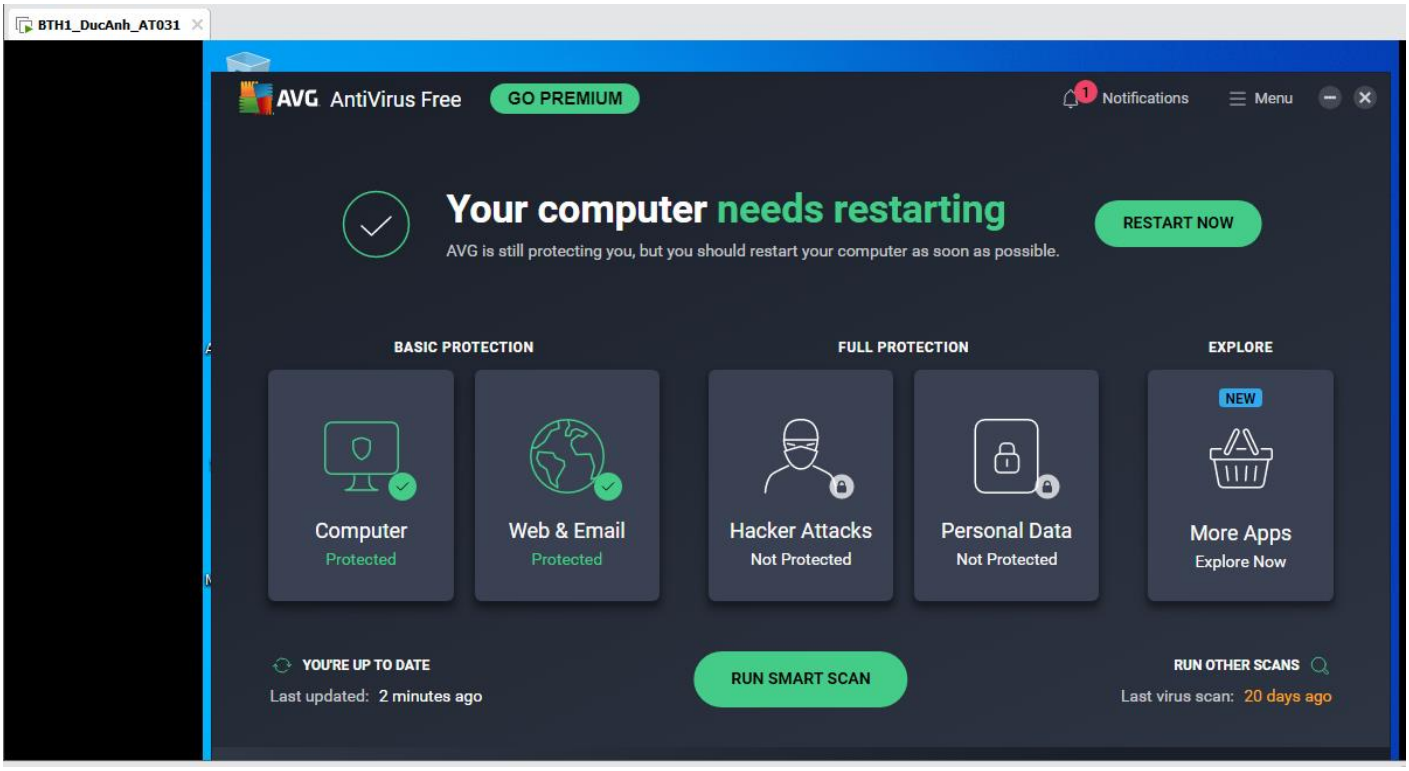
- File cài đặt Windows định dạng ISO.
- Phần mềm ảo hóa: VMWare Workstation.

2.4 Các bước thực hiện

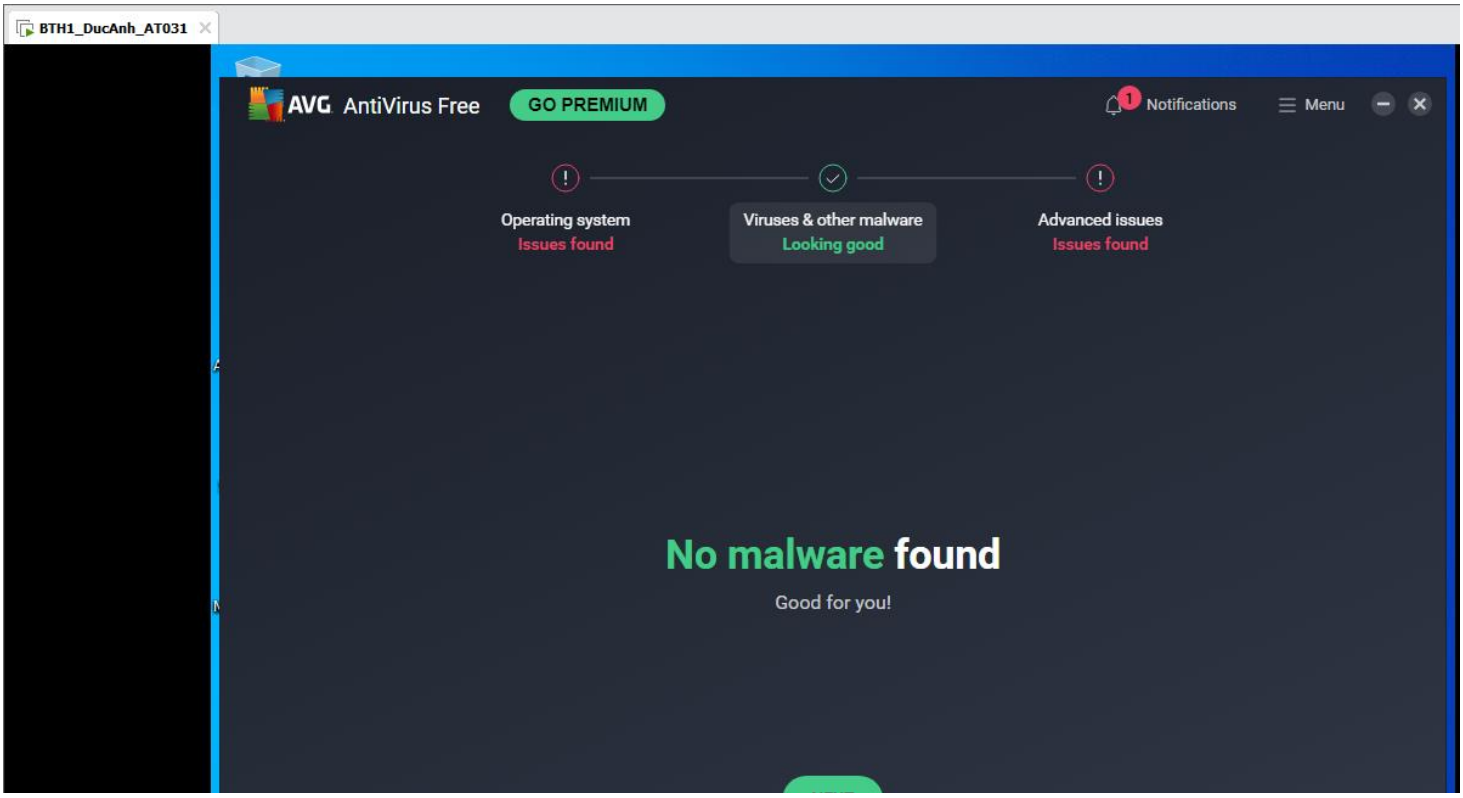
- Khởi động chương trình máy ảo, cài đặt Windows từ file đã chuẩn bị.



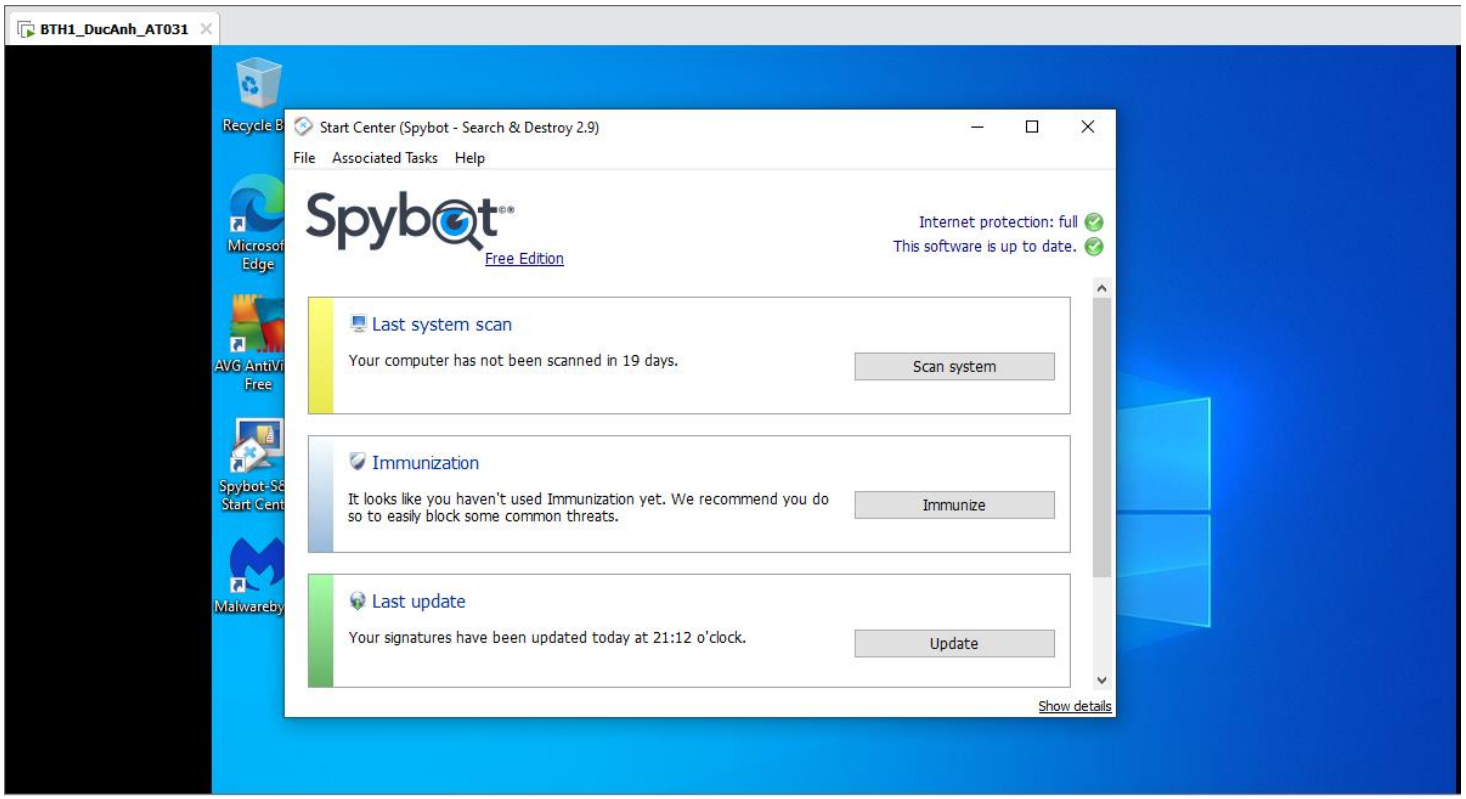
- Cài đặt phần mềm diệt virus AVG AntiVirus



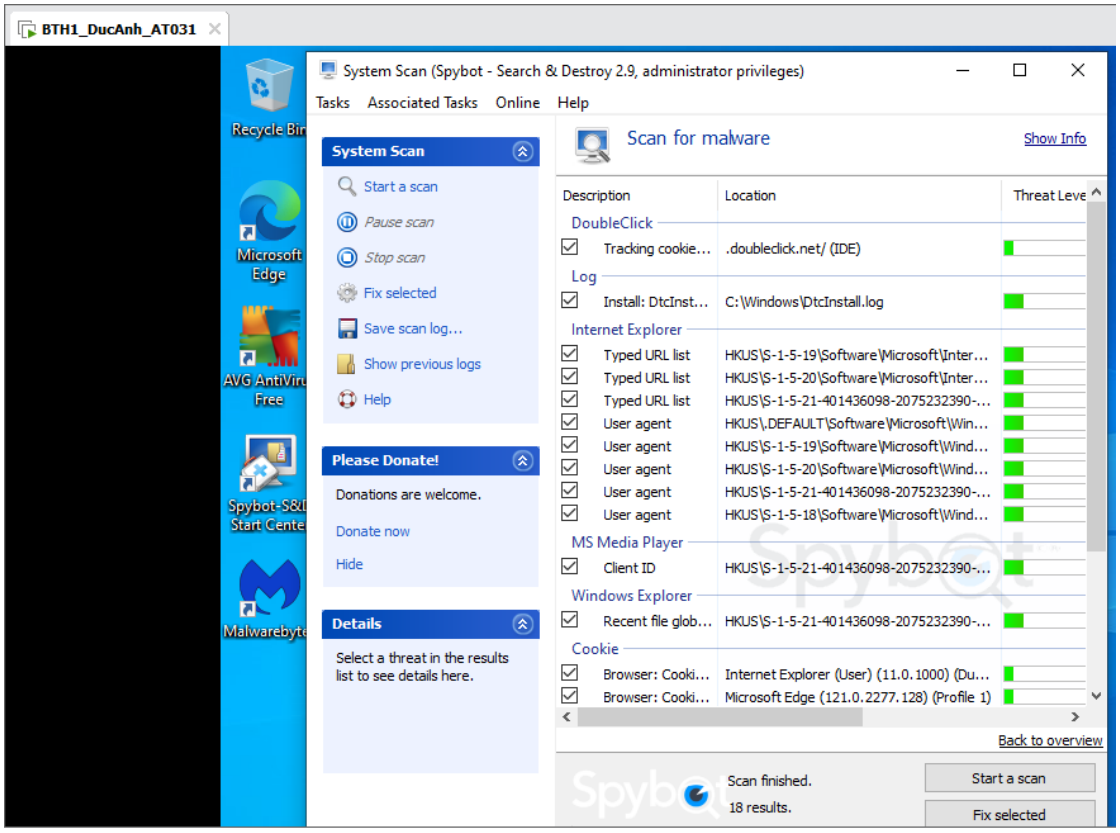
Cài đặt thành công. Tiến hành scan máy ảo



- Cài đặt Spybot S&D(Spybot – Search & Destroy)

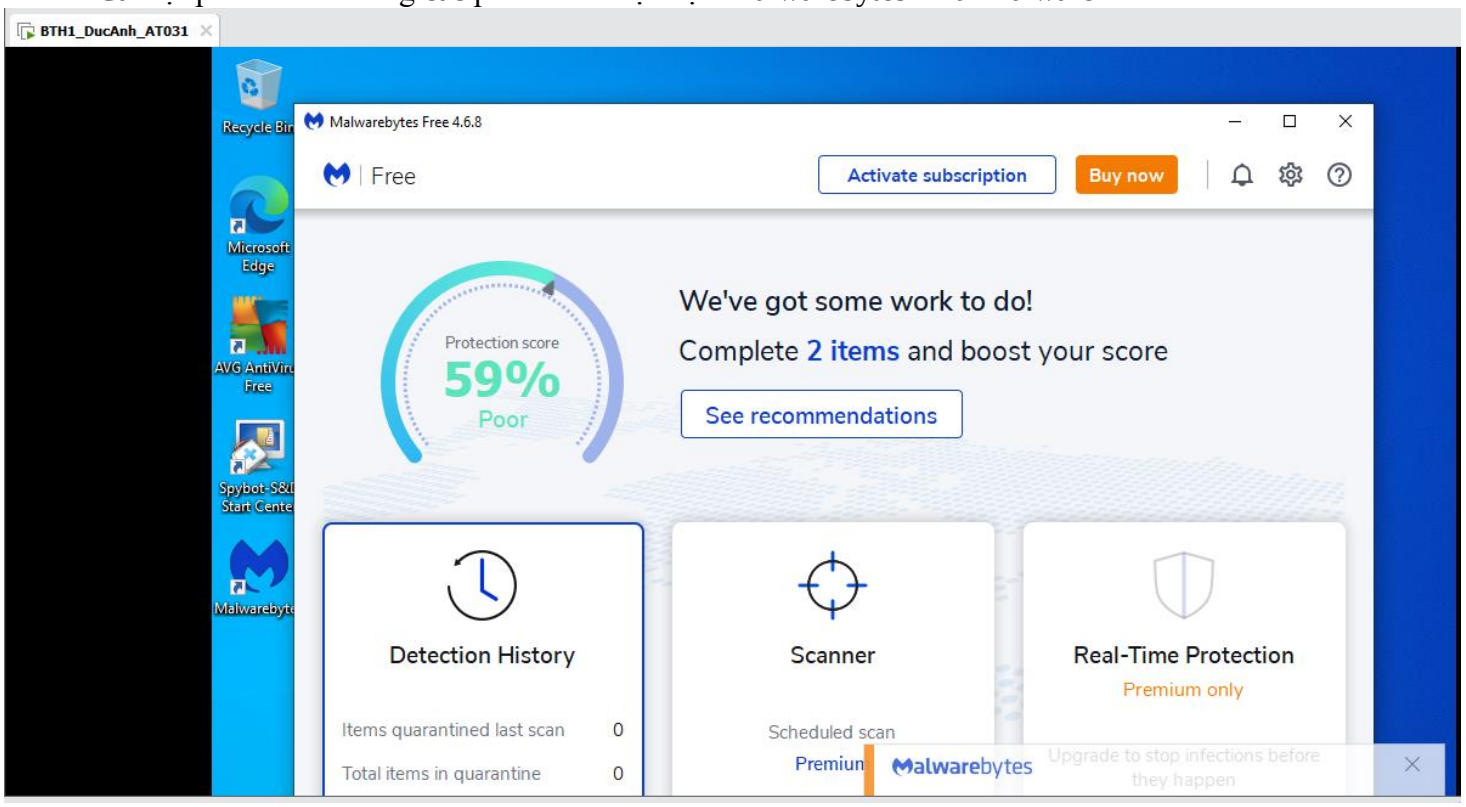


Cài đặt thành công. Tiến hành scan



Scan thành công.

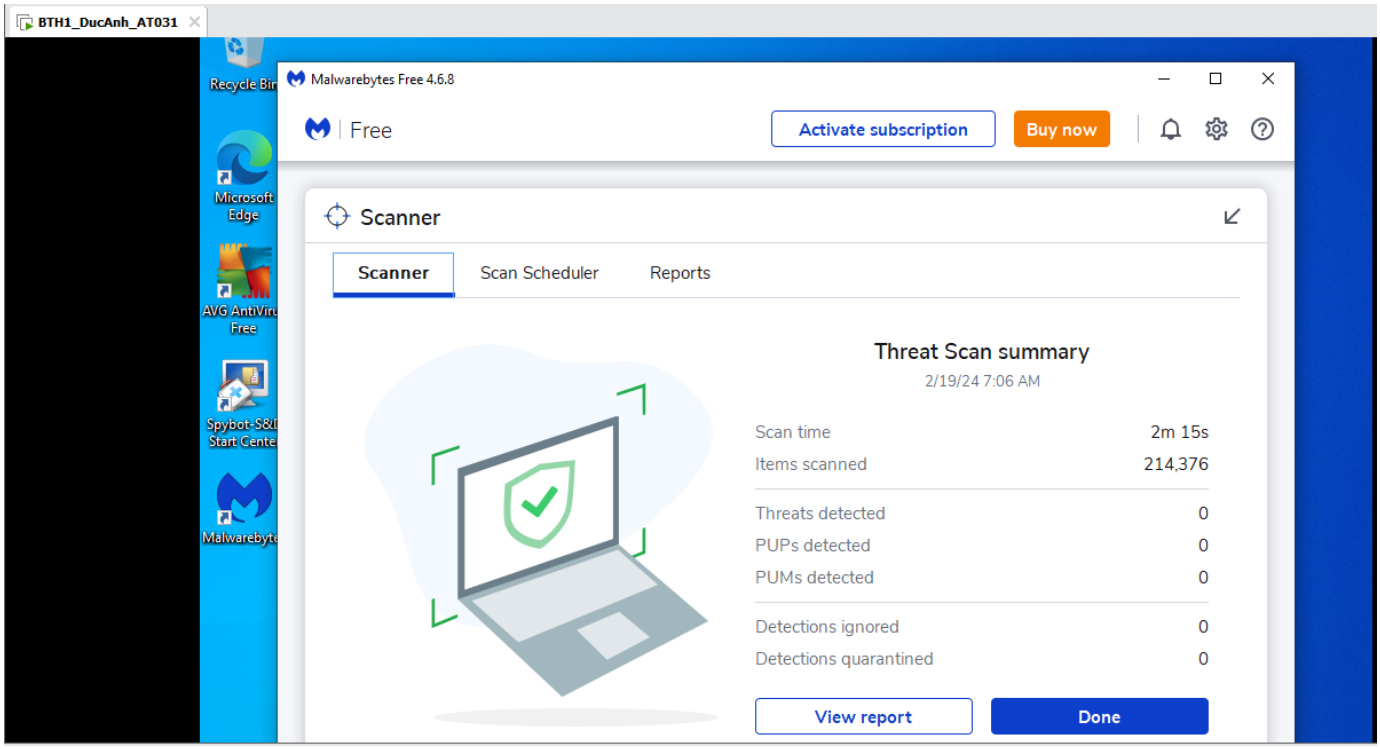
- Cài đặt phần mềm chống các phần mềm độc hại: Malwarebytes Anti-Malware



Cài đạt thành công. Tiến hành scan.

- Cài phần mềm cứu hộ: Kaspersky Rescue Disk (KRD)

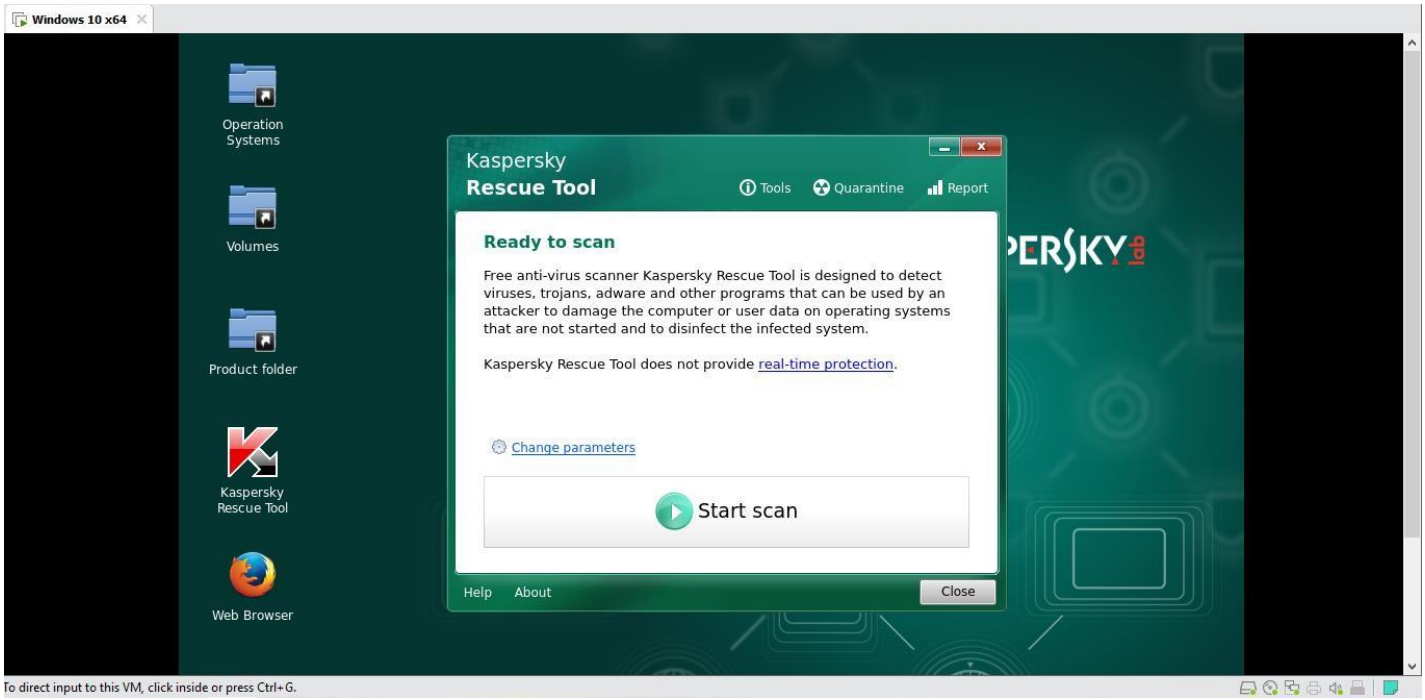
Load vào mục CD/DVD của máy ảo, sau đó chạy máy ảo dạng safe mode rồi chọn boot từ CD-ROM để cài KRD



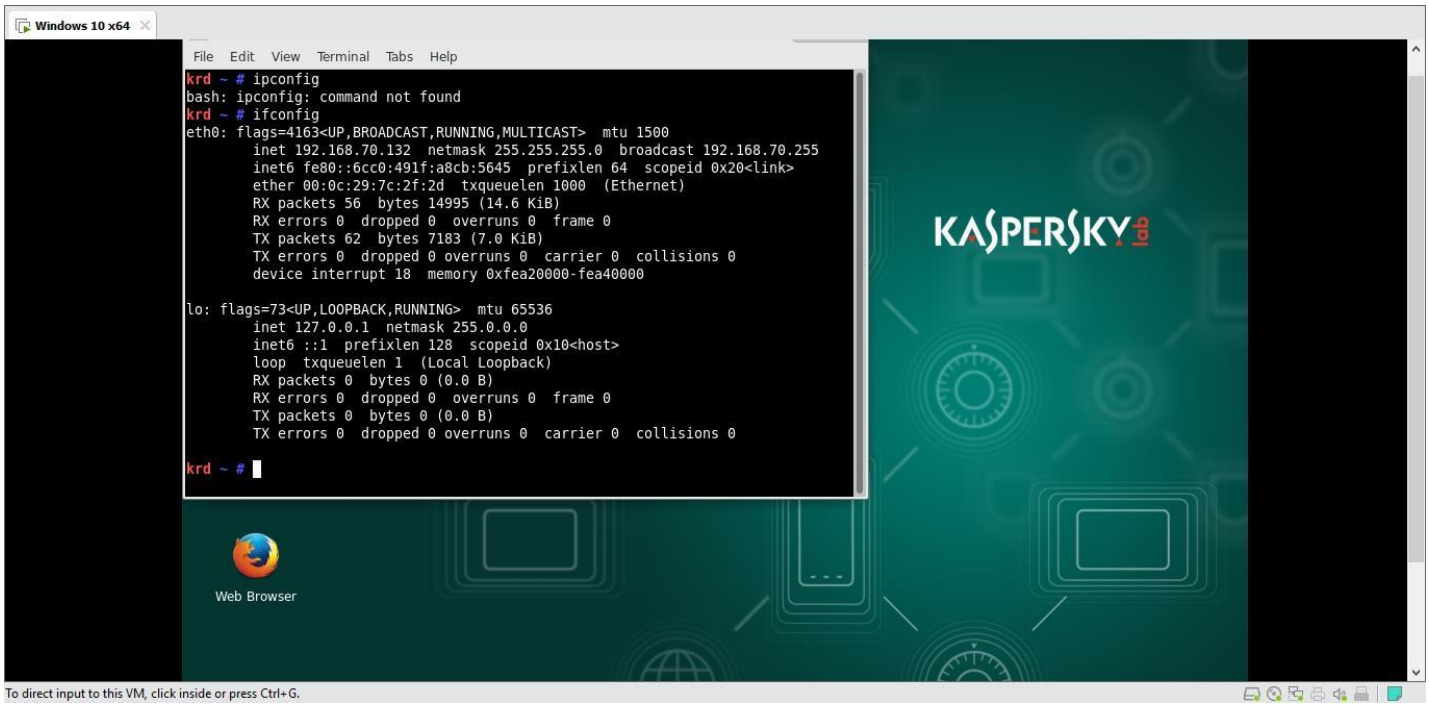
Scan thành công.

- Cài đặt phần mềm cứu hộ: Kaspersky Rescue Disk (KRD). Sau đó mount ra dạng đĩa ảo.

Load vào mục CD/DVD của máy ảo, sau đó chạy máy ảo dạng safe mode rồi chọn boot từ CD-ROM để cài KRD

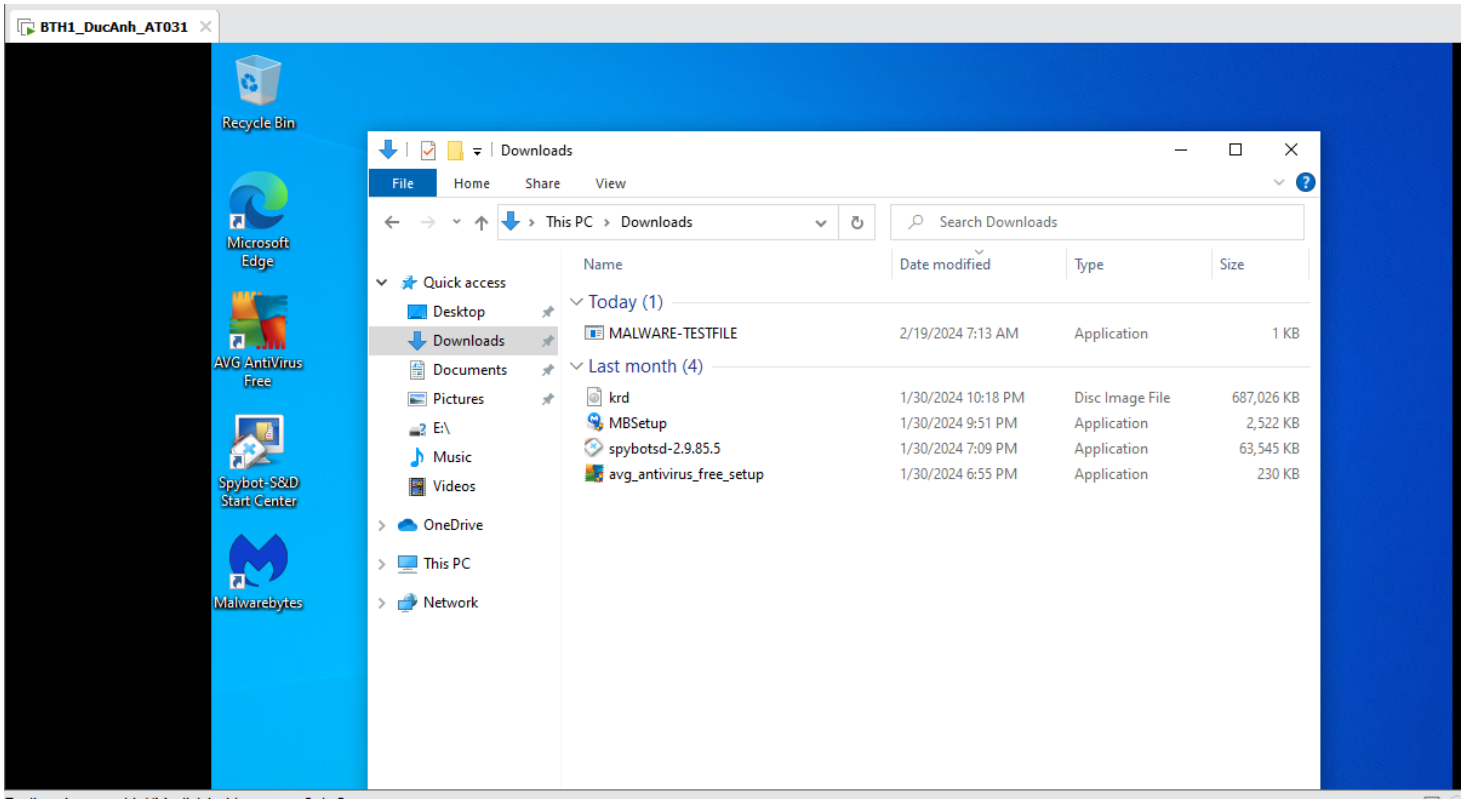


Chạy lệnh ifconfig trên cmd

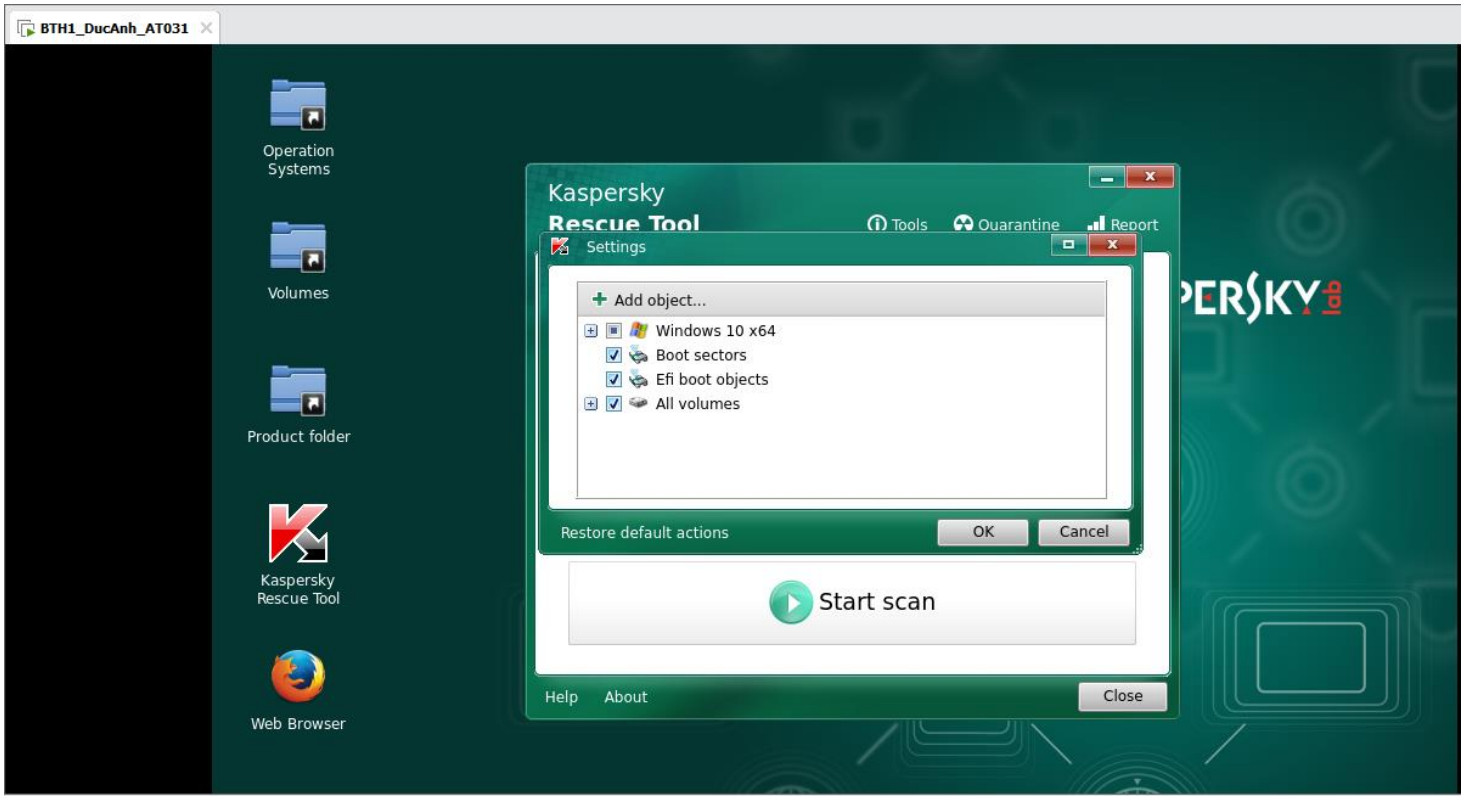


Tiến hành cài file mã độc theo đường link:

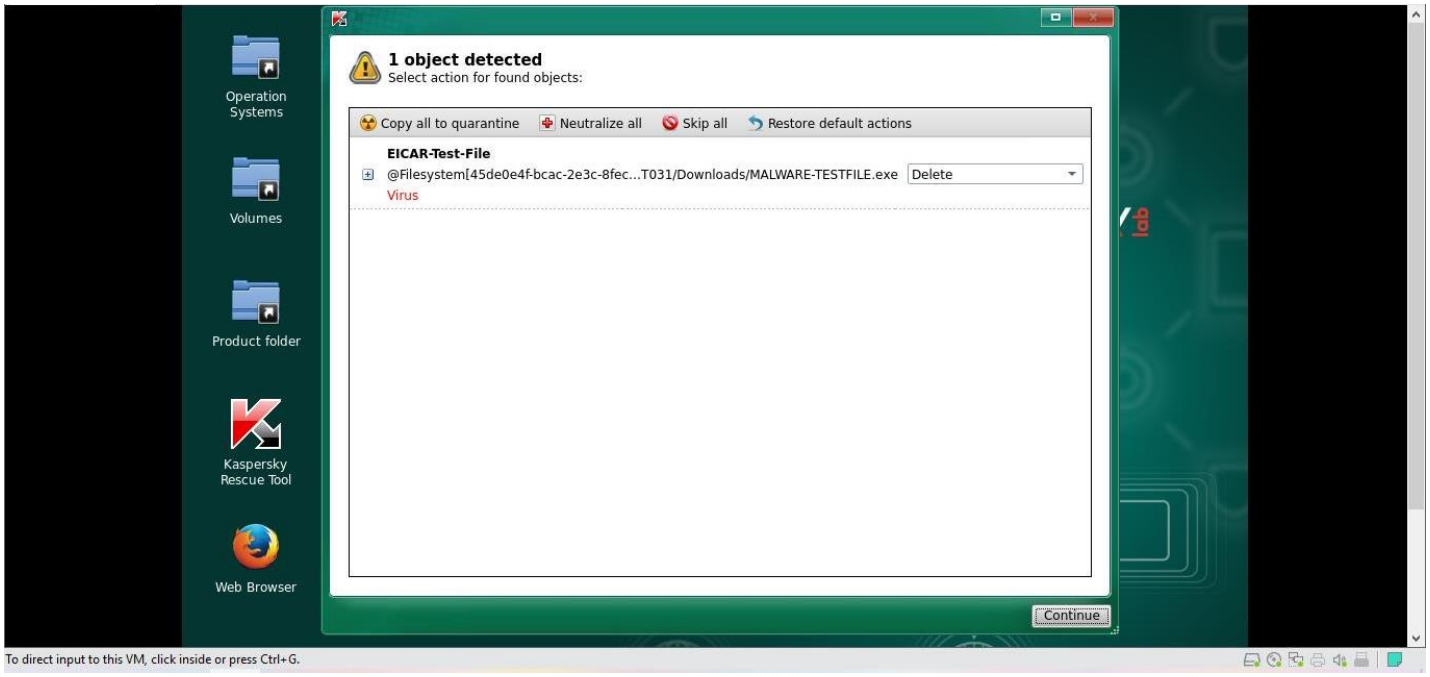
http://www.computersecuritystudent.com/WINDOWS/W7/lesson7/M ALWARE-TESTFILE.exe



Dùng KRD Security tool để quét.



Phát hiện file mã độc đã lưu, chuyển tùy chọn từ Cure thành Delete. Chọn Continue.



Kiểm tra lại vị trí lưu file trong ổ C phát hiện file mã độc đã bị xóa thành công.