HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

Môn: THỰC TẬP CƠ SỞ

BÁO CÁO BÀI THỰC HÀNH SỐ 1

Họ và tên sinh viên:
Trần Đức Minh
Mã số sinh viên:
B20DCAT127

Họ và tên giảng viên:
TS. Đinh Trường Duy

I. Tìm hiểu lý thuyết:

1. Tìm hiểu về các phần mềm ảo hóa:

- Ảo hóa là công nghệ cho phép khai thác triệt để khả năng hoạt động của các phần cứng trong hệ thống máy chủ bằng cách chạy đồng thời nhiều OS trên cùng lớp vật lý, cùng chia sẻ tài nguyên phần cứng và được quản lý bởi lớp ảo hóa (Hypervisor). Lớp ảo hóa nằm giữa như một tầng trung gian giữa phần cứng (hardware) và phần mềm hệ điều hành (OS) giúp quản lý, phân phát tài nguyên phần cứng cho lớp OS ảo hoạt động ở trên

- VirtualBox là một chương trình ảo hóa đầy đủ cho mục đích chung dành cho phần cứng x86 và AMD64/Intel64 được thiết kế để sử dụng cho doanh nghiệp cũng như người dùng chạy trên Linux, Windows, Solaris, macOS, FreeBSD, có mã nguồn mở, miễn phí.

- VMware Workstation Pro là một phần mềm được phát triển bởi VMware, một công ty hàng đầu trong lĩnh vực ảo hóa, chạy trên Linux, Windows, macOS. Với sự trợ giúp của phần mềm này, người dùng có thể sao chép môi trường desktop, server, điện thoại thông minh trên một máy ảo tồn tại trên máy tính của người dùng. Với phiên bản trả phí Pro, người dùng sẽ có thêm một số tính năng như kết nối với vSphere, ESXi và các máy chủ Workstation khác để quản lý các máy ảo và máy chủ.

2. Tìm hiểu về hệ điều hành Windows:

a. Lịch sử ra đời:

- Windows được phát triển từ hệ điều hành DOS ban đầu của Microsoft, đây là hệ điều hành được phát hành năm 1981. Phiên bản khiến cho Windows trở nên phổ biến là Windows 3.1 xuất hiện vào giữa những năm 1990 và thiết lập nền móng cho các các phiên bản Windows khác đến tận ngày nay. Hệ thống Windows 3.1 bao gồm các menu lựa chọn, các cửa sổ có thể thay đổi kích thước và hệ thống chạy chương trình gọi là quản lý chương trình – Program Manager. Cùng thời điểm với Windows 3.1, Microsoft tung ra hệ điều hành Windows NT được thiết kế lại và là hệ điều hành mạng, chạy trên nền 32 bit và sử dụng GUI. Hệ điều hành mới mạnh hơn và sử dụng các nhân và phần nạp khởi động riêng chứ không dựa trên DOS.

- Vào 2001, Microsoft đưa ra Windows 2000 hướng tới môi trường máy chủ và máy trạm nhằm thay thế cho sản phẩm Windows NT trước đó.

Một trong những tính năng quan trọng đó là thư mục động (Active Directory) và dịch vụ đầu cuối (Terminal Service). Cùng năm, Microsoft kết hợp các dòng sản phẩm Windows NT/2000 (dành cho đối tượng công ty và doanh nghiệp) và Windows 95/98/Me (người quản trị thông thường) tạo nên Windows XP. Windows Vista và Windows 7 được Microsoft đưa ra nhằm thay thế cho bản Windows XP.

- Windows 8 và đặc biệt là Windows 10 thể hiện sự thay đổi mạnh mẽ về việcsử dụng các thiết bị tính toán cá nhân mà máy tính PC là một đại diện. Mục tiêu của hệ điều hành mới là hợp nhất các nền tảng Windows cho các thiết bị di động như điện thoại, máy tính bảng. Như vậy, các ứng dụng có thể được tải về và chạy trên tất cả các thiết bị Windows.

- Với sản phẩm dành cho môi trường chuyên nghiệp, Windows Server 2003 đưa ra các khái niệm về chức năng máy chủ như Web, file, ứng dụng hay cơ sở dữ liệu và công cụ hỗ trợ cài đặt các chức năng một cách thuận tiện. Các phiên sau gồm có Server 2008, 2012 tăng cường khả năng kết nối mạng, các hệ thống file phân tán, các tính năng bảo mật, ảo hóa và hướng tới tính toán đám mây (cloud computing).

b. Kiến trúc của hệ điều hành:

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.

c. 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.

3. Tìm hiểu về các phần mềm diệt virus, phần mềm chống phần mềm gián điệp, phần mềm cứu hộ:

a. 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 thông dụng:

- Kaspersky Anti-Virus: Phần mềm mới được phát triển vài năm gần đây, tuy không có lịch sử như các đại gia khác nhưng cũng đã vươn lên đứng trong danh sách các phần mềm diệt virus loại tốt, thuộc hãng Kaspersky. Phần mềm không miễn phí, tuy nhiên cũng có phần cho phép quét virus trực tuyến.

- McAfee: Phần mềm diệt virus và các phần mềm độc hại Của hãng McAfee, phát triển khá lâu và có uy tín. Đây là phần mềm thương mại.

- Norton AntiVirus: Phần mềm diệt virus và các phần mềm độc hại của hãng Symantec, được phát triển từ khá lâu, và được đánh giá tốt. Đây là phần mềm thương mại.

- Symantec Antivirus: Một phần mềm diệt virus khác cũng của hãng Symantec, được đánh giá là "nhẹ", ít chiếm tài nguyên hơn so với Norton Antivirus. Phần mềm này thường thích hợp với mạng nội bộ (các máy trạm cài bản client) với sự quản lý của một máy chủ (được cài bản server). Phần mềm này có phiên bản miễn phí.

b. Phần mềm chống gián điệp:

- Phần mềm gián điệp là phần mềm không mong muốn xâm nhập vào máy tính của bạn mà bạn thường không nhận ra, để theo dõi, giám sát và nắm bắt thông tin cá nhân của bạn.

- Những phần mềm này có thể tích hợp vào hệ điều hành của bạn để theo dõi tổ hợp phím, chỉnh sửa cài đặt và giảm hiệu suất thiết bị của bạn để có thể thu thập dữ liệu nhạy cảm như chi tiết đăng nhập, email và lịch sử duyệt web và chi tiết thẻ tín dụng.

c. Phần mềm cứu hộ (USB Boot):

- Khác với những USB thông thường, USB Boot có chứa bộ cài đặt hệ điều hành dùng để sửa lỗi và cài đặt hệ điều hành Windows, hoặc chứa các công cụ, lệnh và chương trình để khắc phục các sự cố máy tính.

- Phân loại USB Boot:

+ USB DOS: Là USB được tạo để tương thích với các chương trình DOS, ví dụ Flash FW BIOS, chương trình Ghost, Partition Wizard,… chạy trên nền DOS.

+ USB HĐH: Là USB dùng để xử lí các files ISO của các hệ điều hành (Windows, Linux, MacOS) và cài đặt lại hệ điều hành mới, hoặc Boot Live Distro, hoặc để đưa máy tính vào chế độ Recovery của hệ điều hành,…

+ USB Cứu Hộ: Là USB bên trong có tích hợp các công cụ có thể chạy trên nền DOS và thường có một vài môi trường cứu hộ ảo (WinPE), tích hợp nhiều công cụ cứu hộ dạng Portable (chạy ngay) trên môi trường này nhằm mục đích khắc phục sửa chữa, khắc phục sự cố, cài mới hệ điều hành trực tiếp trên môi trường ảo mà không cần vào hệ điều hành thật.

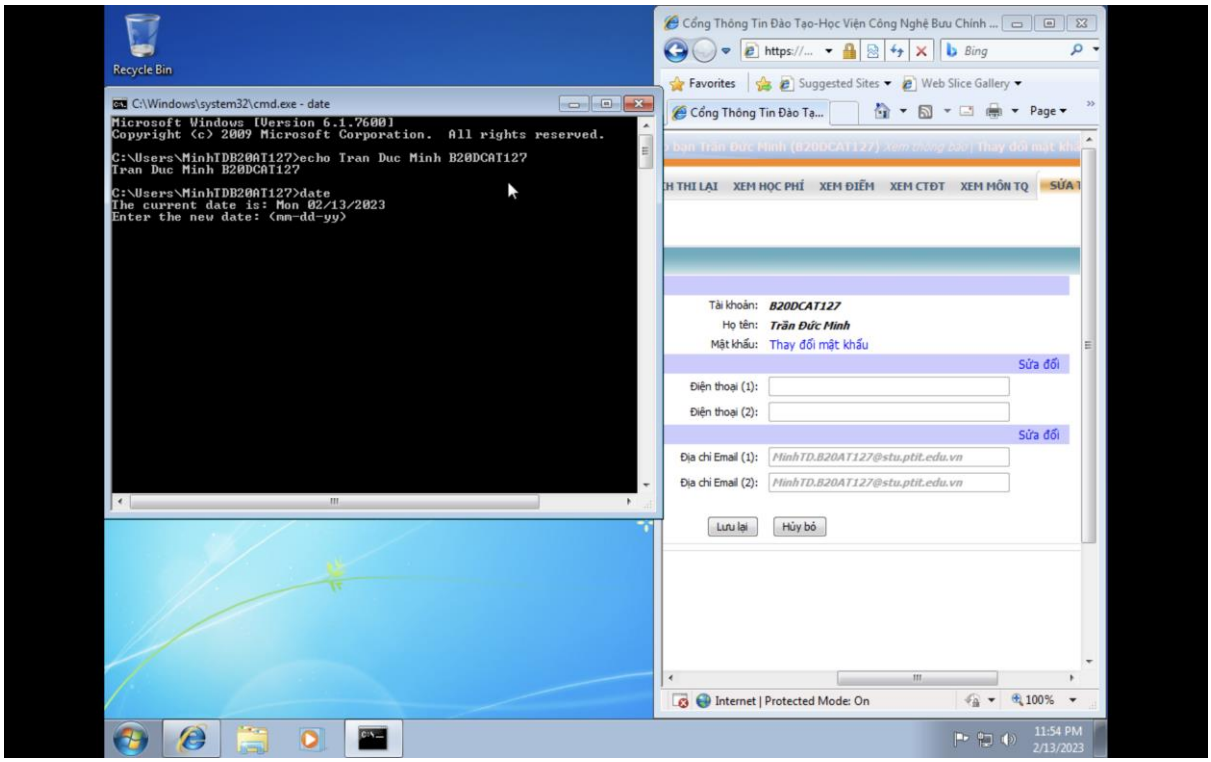
+ USB Đa Năng: Là USB được tích hợp tất cả các chương trình DOS, môi trường cứu hộ, cài đặt hệ điều hành. Có thể tích hợp rất nhiều hệ điều hành từ Linux đến Windows, các chương trình DOS cứu hộ, hỗ trợ chạy Live các Distro Linux, các công cụ chuẩn đoán,…

II. Các bước thực hiện:

- Khởi động chương trình máy ảo

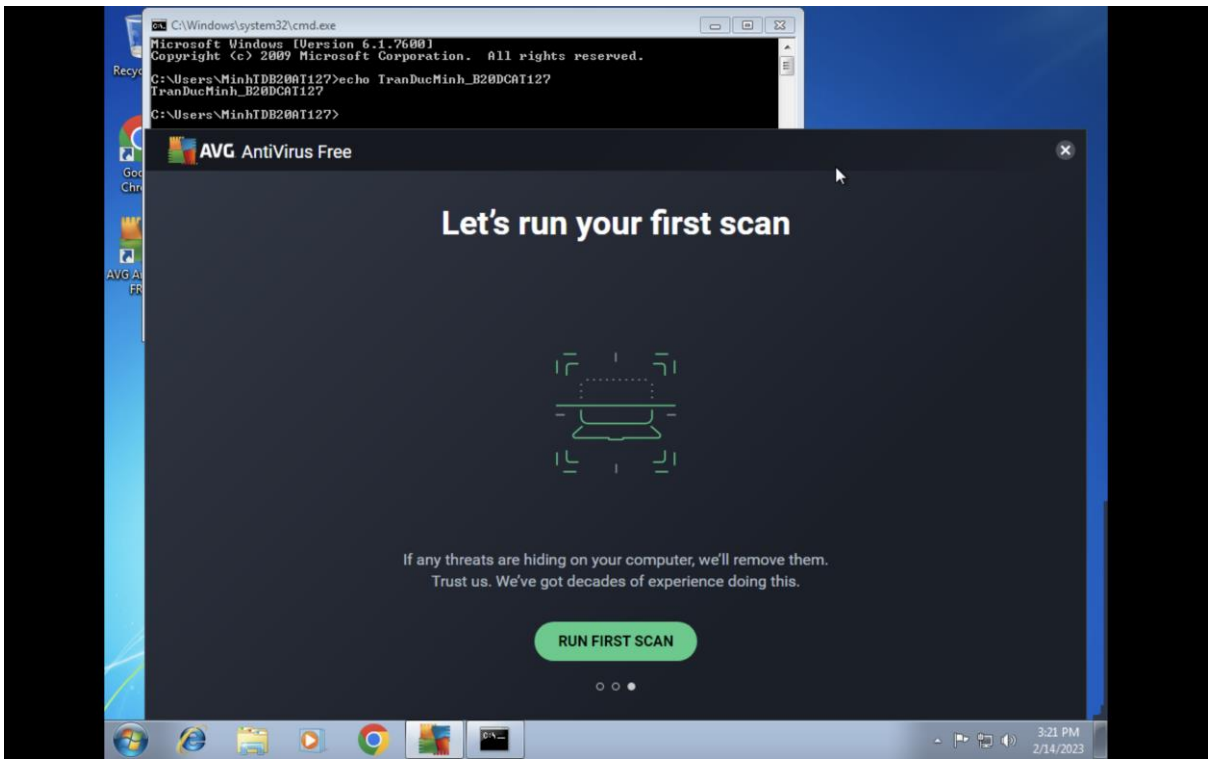
- Cài đặt Windows 7/10/11 từ file đã chuẩn bị.

- Trong mục “System Properties” đổi tên máy trạm Windows thành “họ tên SV_mã SV”.



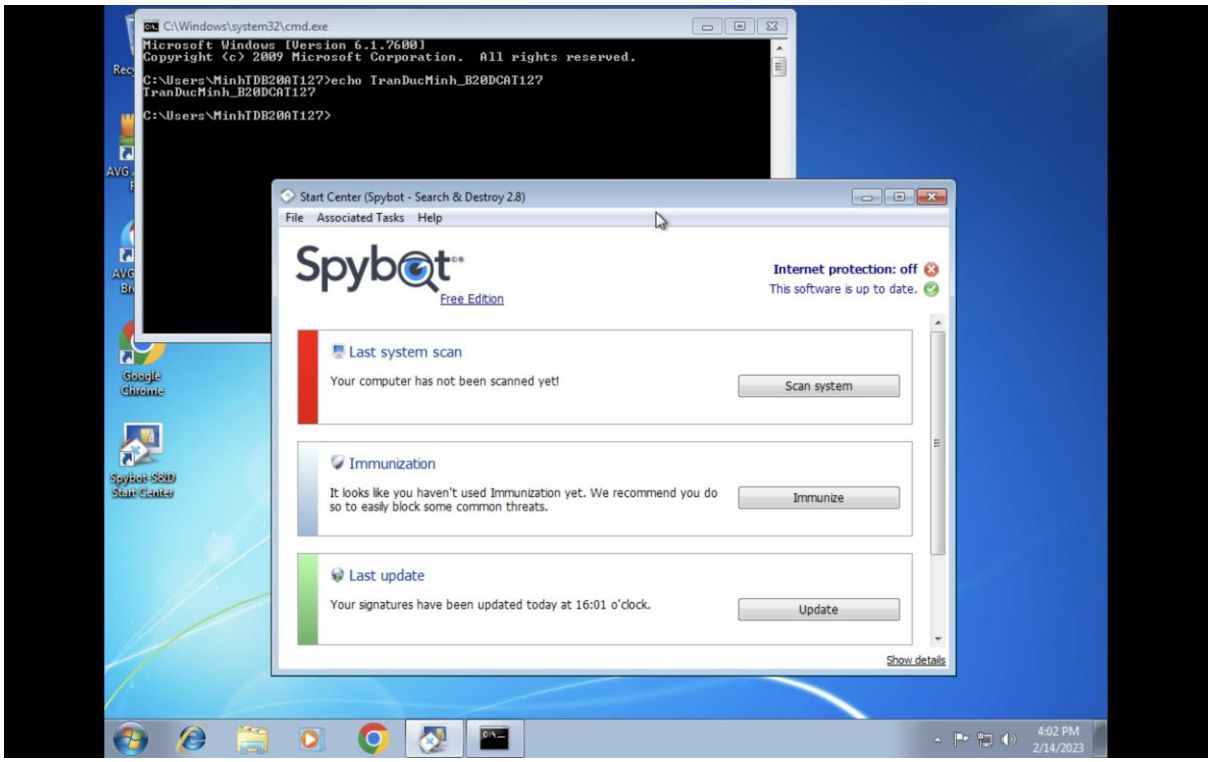
a) Phần mềm diệt virus: AVG AntiVirus.

- Cài đặt thành công.



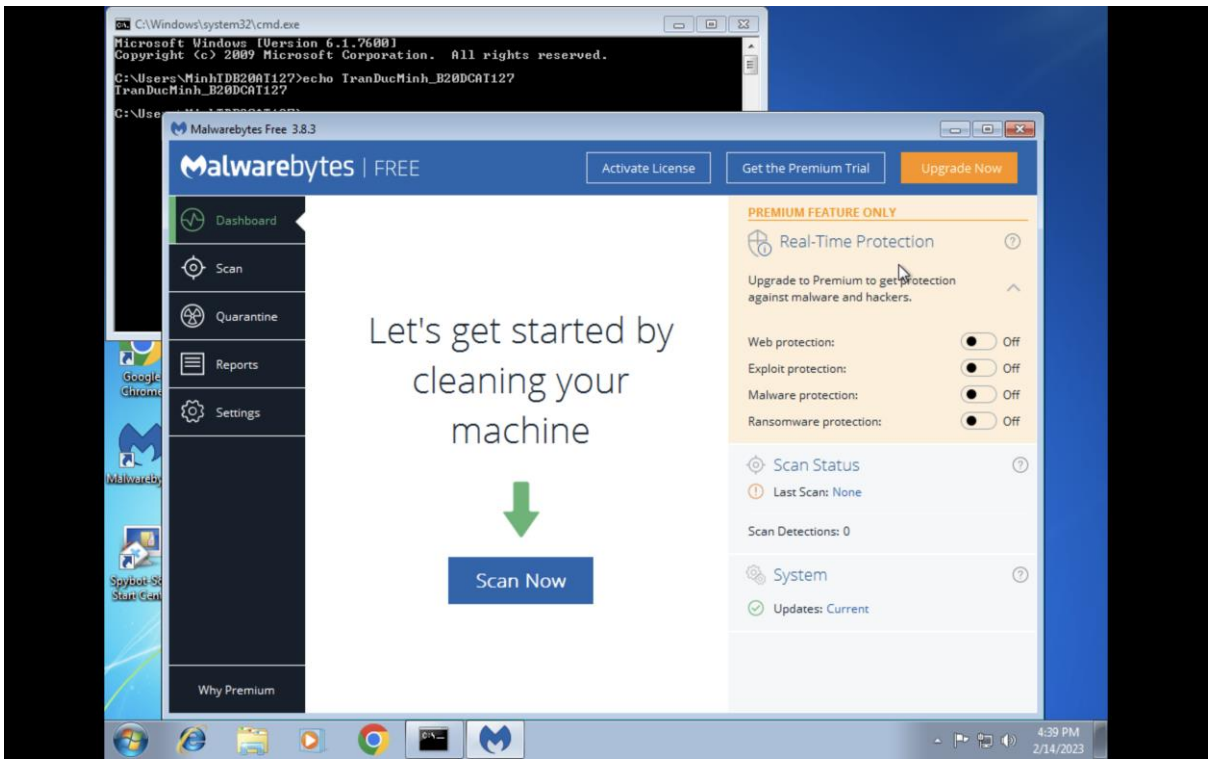
b) Phần mềm chống phần mềm gián điệp Spybot S&D (Spybot – Search & Destroy)

- Cài đặt thành công.



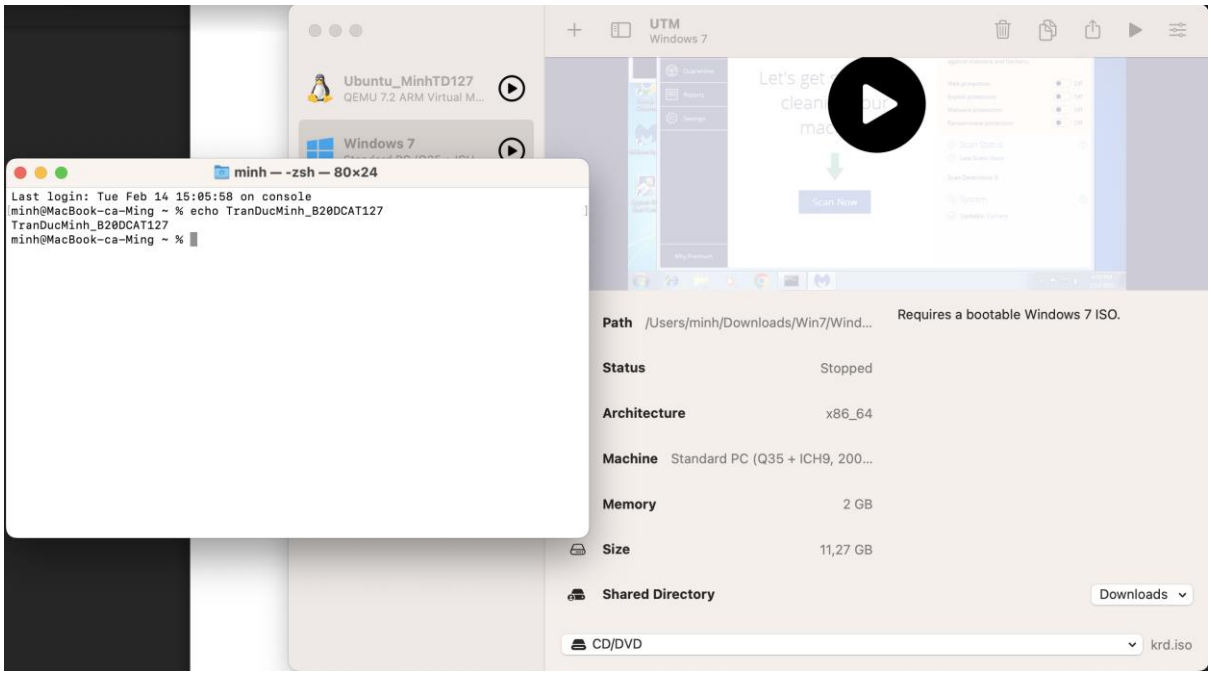
c) Phần mềm chống các phần mềm độc hại: Malwarebytes Anti-Malware

- Cài đặt thành công.

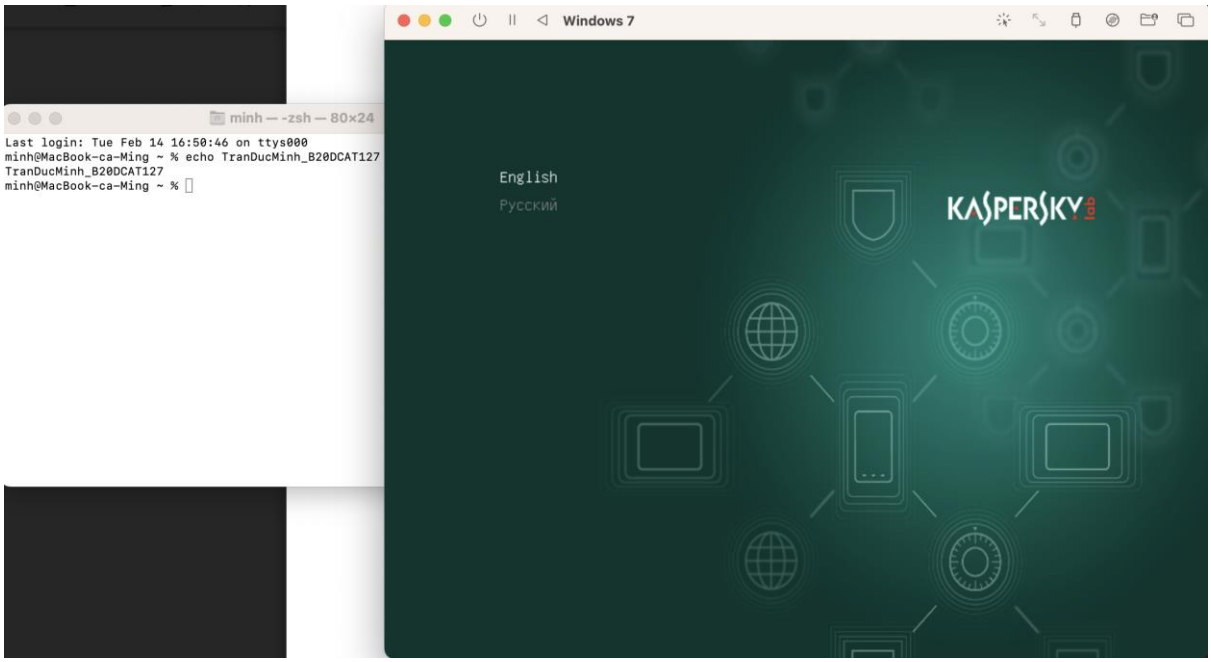


d) Phần mềm cứu hộ: Kaspersky Rescue Disk (KRD)

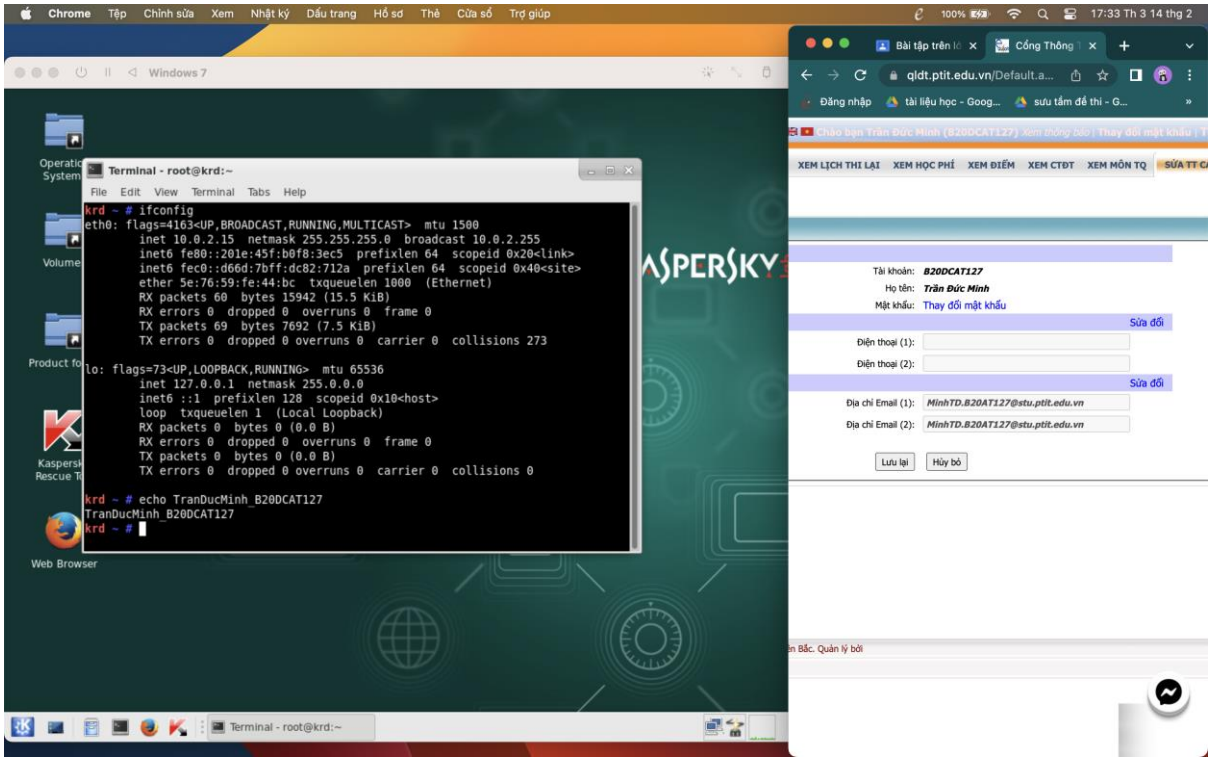
- Load vào trong mục CD/DVD của máy trạm ảo để có thể khởi động máy trạm ảo dùng đĩa KRD



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



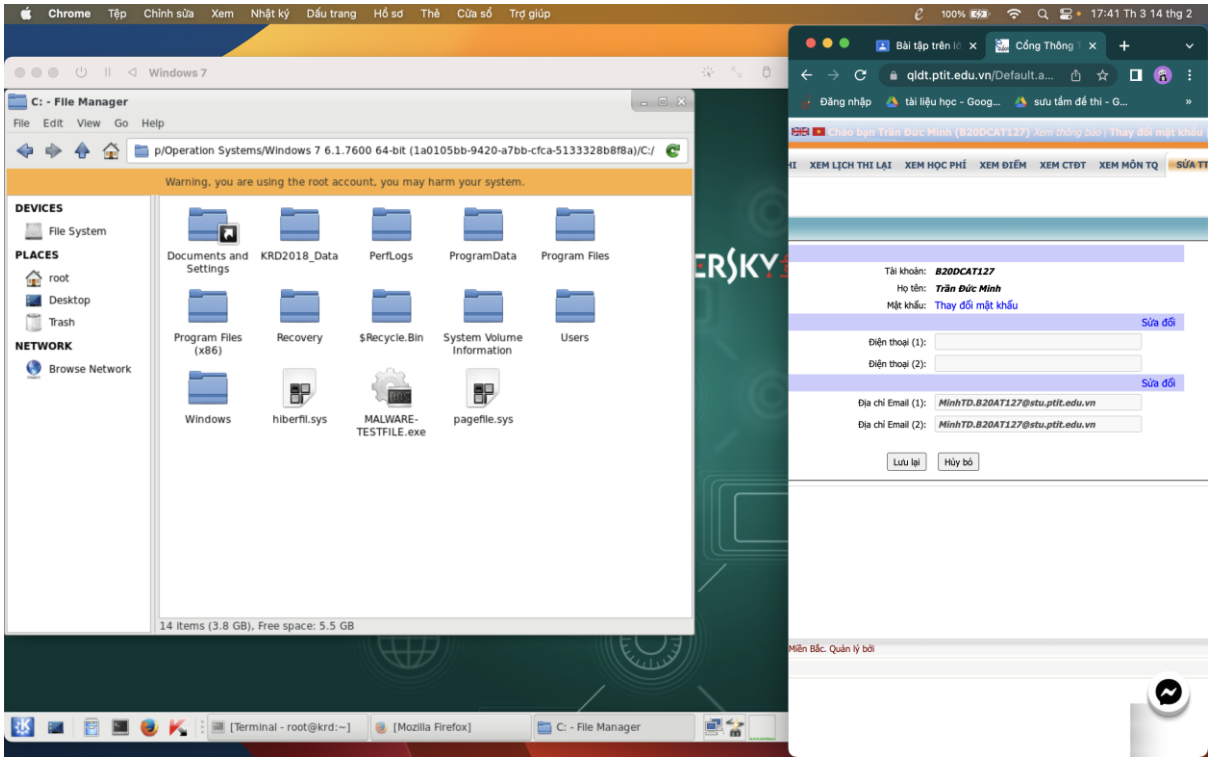
- Mở cmd kiểm tra IP của máy trạm bằng câu lệnh: ifconfig



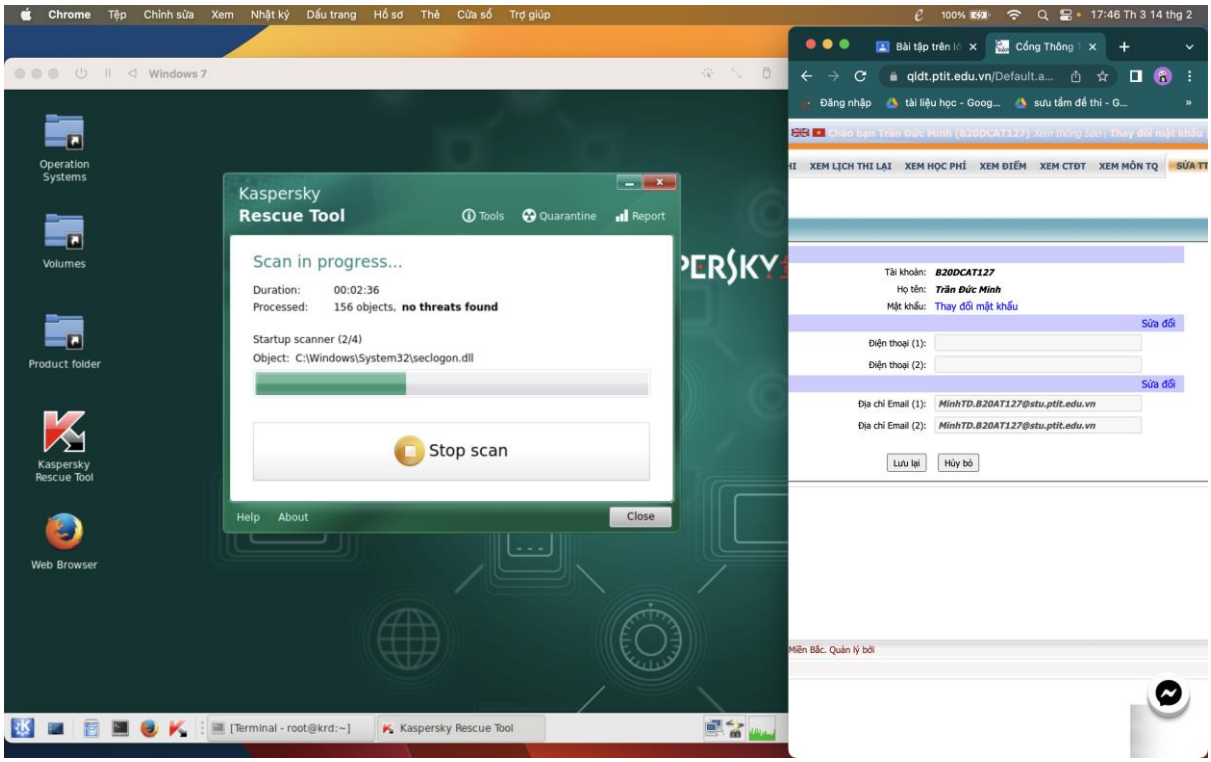
- Dùng Web browser tải file test mã độc từ đường link :

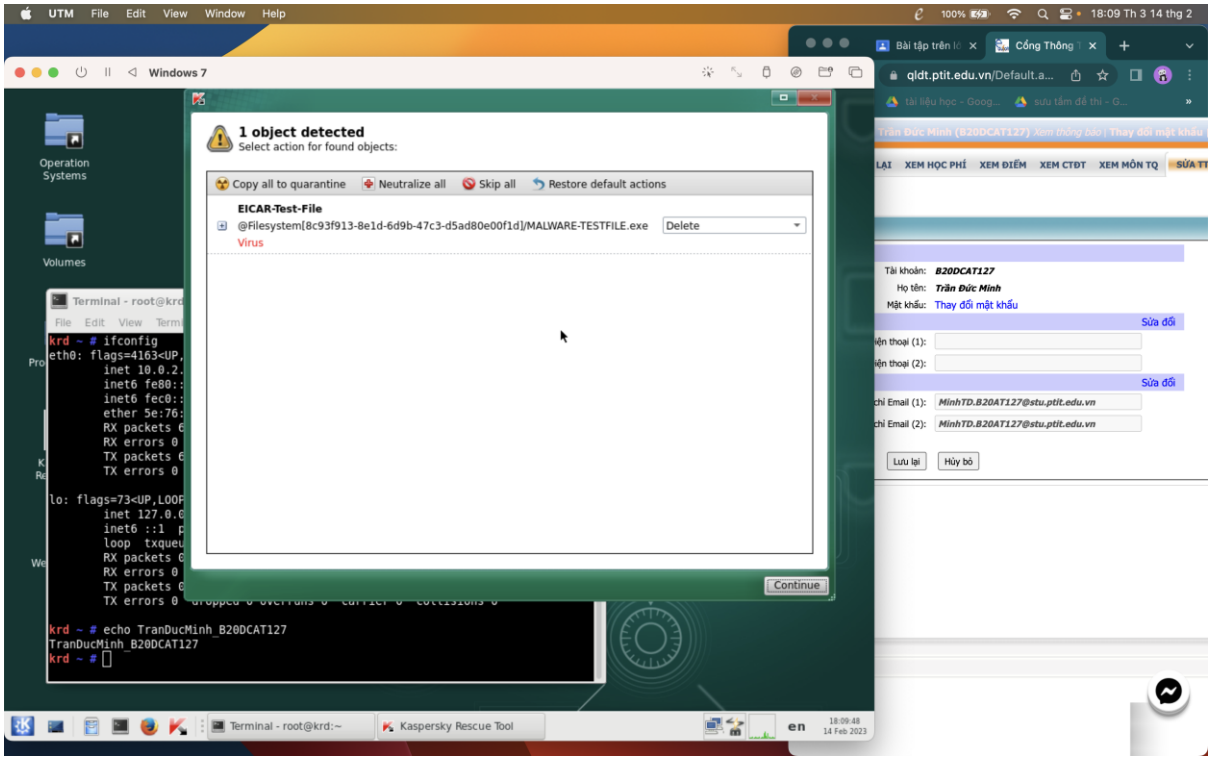
http://www.computersecuritystudent.com/WINDOWS/W7/lesson7/MALWARE-TESTFILE.exe

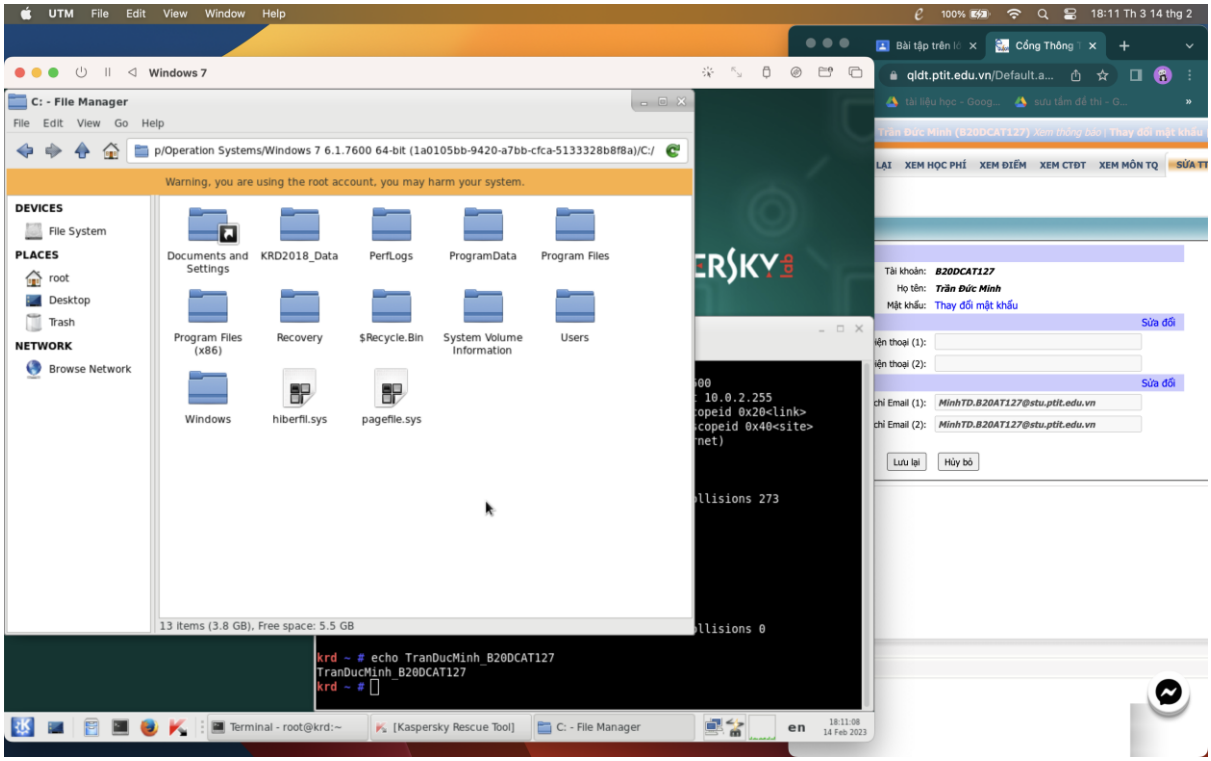
- Lưu file test mã độc vào ổ C của máy trạm



- 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.




1 object detected
Select action for found objects:
Copy all to quarantine
Neutralize all
Skip all
Restore default actions
EICAR-Test-File
@Filesystem[8c93f913-8e1d-6d9b-47c3-d5ad80e00f1d]/MALWARE-TESTFILE.exe
Delete
Virus
Continue
krd ~ # ifconfig
krd ~ # echo TranDucMinh_B20DCAT127
TranDucMinh_B20DCAT127
krd ~ #


C: - File Manager
Warning, you are using the root account, you may harm your system.
DEVICES
File System
PLACES
root
Desktop
Trash
NETWORK
Browse Network
Documents and Settings
KRD2018_Data
PerfLogs
ProgramData
Program Files
Program Files (x86)
Recovery
$Recycle.Bin
System Volume Information
Users
Windows
hiberfil.sys
pagefile.sys
13 items (3.8 GB), Free space: 5.5 GB
krd ~ # echo TranDucMinh_B20DCAT127
TranDucMinh_B20DCAT127
krd ~ #