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

Môn: Thực tập cơ sở

BÀI BÁO THỰC TẬP CƠ SỞ

Bài 1: Cài đặt hệ điều hành máy trạm Windows

Họ và tên giảng viên:	TS.Đinh Trường Duy
Họ và tên:	Nguyễn Quốc Khánh
Mã sinh viên:	B20DCAT103
Lớp:	D20CQAT03-B
Số điện thoại:	0964137761

Hà Nội 2023

1. Tìm hiểu lý thuyết

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.

Các phần mềm ảo hóa thông dụng:

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.

Bảng so sánh:

Tiêu chí so sánh	VirtualBox	VMware
Ảo hóa phần mềm	Có	Không
Ảo hóa phần cứng	Có	Có
Hệ điều hành máy chủ	Linux, Windows, Solaris, macOS, FreeBSD	Linux, Windows + macOS (yêu cầu VMware Fusion)
Hệ điều hành khách	Linux, Windows, Solaris, macOS, FreeBSD	Linux, Windows, Solaris, FreeBSD + MacOS (với VMware Fusion)
Snapshot	Có	Snapshot chỉ được hỗ trợ trên các sản phẩm ảo hóa trả phí, không phải trên VMware Workstation Player
Định dạng ổ đĩa ảo	VDI, VMDK, VHD, HDD	VMDK
Loại cấp phát ổ đĩa ảo	Preallocated: Ổ đĩa cố định Dynamically allocated: Ổ đĩa được cấp phát động.	Preallocated: Ổ đĩa Thin Provisioned Dynamically allocated: Các ổ đĩa Thin Provisioned

Mô hình mạng ảo	Không được đính kèm, NAT, mạng NAT, bridged adapter, mạng nội bộ, adapter chỉ dành cho máy chủ lưu trữ, chung (UDP, VDE)	NAT, bridged adapter, adapter chỉ dành cho máy chủ lưu trữ + Trình chỉnh sửa mạng ảo (trên VMware workstation và Fusion Pro)
Đồ họa 3D	Lên đến OpenGL 3.0 và Direct3D 9 Bộ nhớ video tối đa 128 MB Tăng tốc 3D được kích hoạt theo cách thủ công	Lên đến OpenGL 3.3, DirectX 10 Bộ nhớ video tối đa 2GB Tăng tốc 3D được bật theo mặc định
Tích hợp	VMDK, Microsoft VHD, HDD, QED, Vagrant, Docker	Yêu cầu tiện ích chuyển đổi bổ sung cho nhiều loại VM hơn. VMware VSphere và Cloud Air (trên VMware Workstation)
Chi phí	Miễn phí, theo Giấy phép Công cộng GNU	VMware Workstation Pro cần phải trả phí

Hệ điều hành Windows:

Lịch sử:

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).

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.

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. 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.

Các phần mềm diệt virus, phần mềm chống phần mềm gián điệp, phần mềm cứu hộ:

Avast Free Antivirus: là chương trình bảo vệ hệ thống, quét thiết bị Windows để tìm tất cả các mối đe dọa hiện có như virus, phần mềm gián điệp, phần mềm độc hại. Sau khi quét, chương trình sẽ đặt tất cả các file và thư mục đáng ngờ trong tình trạng cách ly, cho phép người dùng chọn file nào muốn giữ lại và file nào muốn Avast xóa.

Bitdefender Antivirus Free Edition: là phần mềm diệt virus miễn phí tuyệt vời. Bitdefender cũng thường được coi là một trong những công cụ quét virus nhanh nhất hiện có. Điểm trừ lớn nhất là không thể tự lên lịch quét. Thay vào đó, Bitdefender Antivirus Free Edition tự động làm mọi thứ. Đây là một phần mềm chống diệt virus nên được khuyến khích sử dụng. Nó giám sát bất kỳ file nào đến, cũng như trình duyệt và bất kỳ trang web phishing độc hại tiềm ẩn nào. Giao diện của Bitdefender Antivirus đơn giản và được trình bày rõ ràng, với các cài đặt tối thiểu, vì vậy nó hoàn hảo cho những người dùng PC thiếu kinh nghiệm.

Windows Security: Windows 10 bao gồm Windows Security, cung cấp khả

năng bảo vệ chống virus mới nhất. Thiết bị sẽ được bảo vệ tích cực ngay từ khi khởi động Windows 10. Windows Security liên tục quét malware, virus và các mối đe dọa bảo mật. Ngoài tính năng bảo vệ theo thời gian thực này, các bản cập nhật còn được tải xuống tự động để giúp giữ an toàn cho thiết bị và bảo vệ thiết bị khỏi các mối đe dọa.

Đặc điểm:

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

Windows Registry: là một cơ sở dữ liệu của Windows và là nơi lưu các thông tin quan trọng về phần cứng, các chương trình, các cài đặt, và các hồ sơ về tài khoản người dùng trong máy tính. Windows liên tục tham chiếu đến các thông tin trong danh mục này.

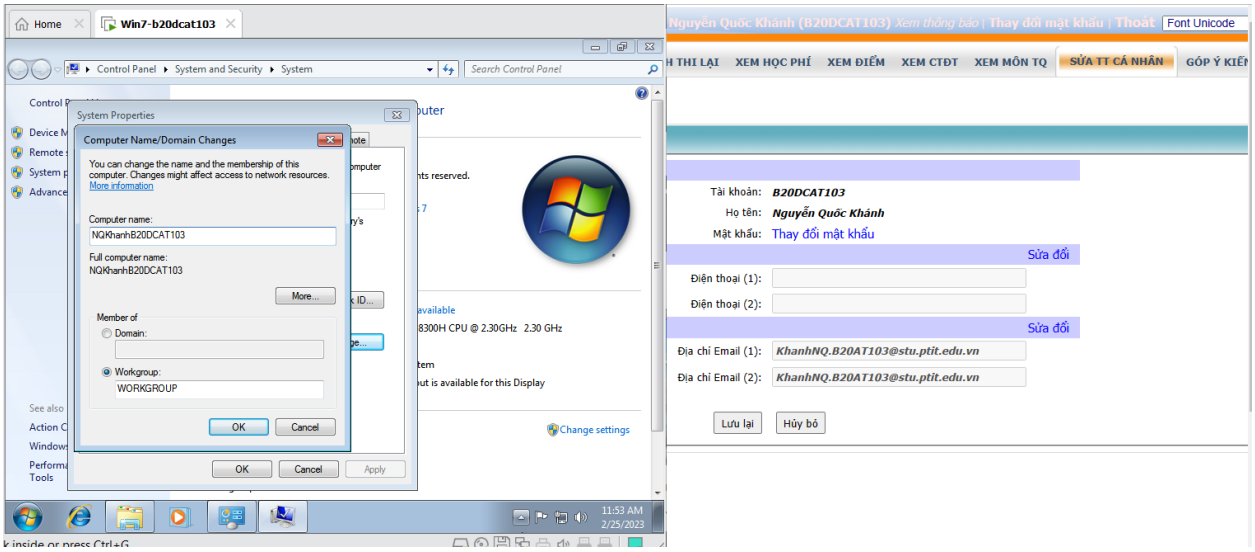
Thư mục động (Active Directory): là công nghệ cung cấp dịch vụ thư mục của Microsoft.

Công cụ quản trị nhóm(Group Policy Management) là tính năng quan trọng với Windows cho phép kiểm soát môi trường làm việc với tài khoản người dùng và máy tính. Ngoài ra, quản trị chính sách nhóm cho phép quản lý và cấu hình tập trung với hệ điều hành, ứng dụng và các cài đặt của người dùng giúp đơn giản hóa công việc quản trị.

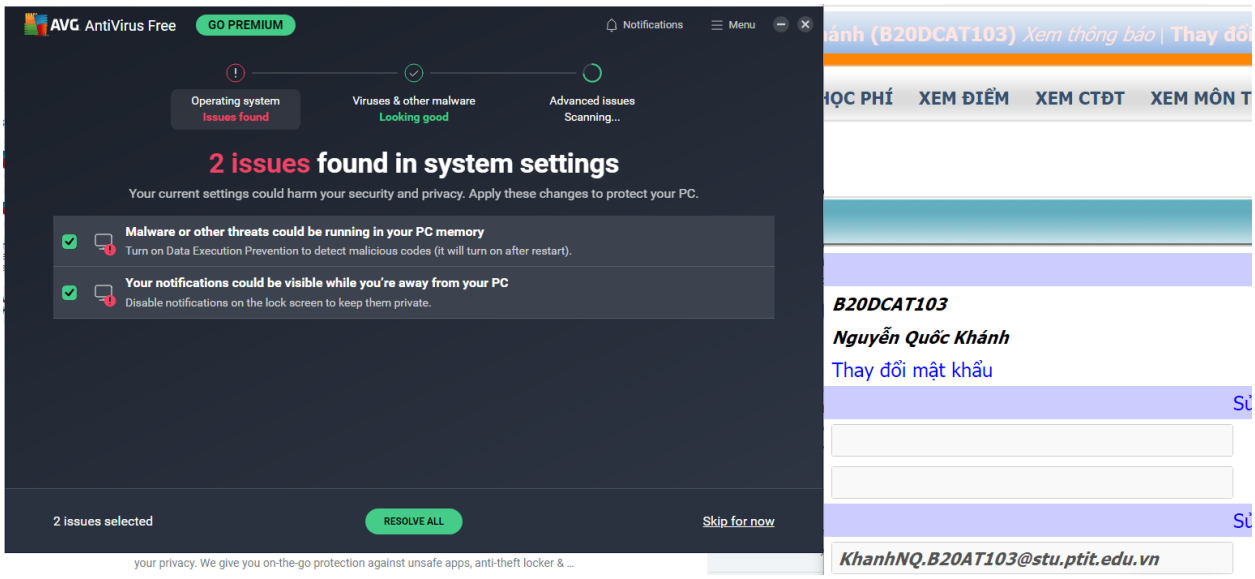
Server Manager là một công cụ cho phép thực hiện hầu hết các thao tác quản trị trên Windows Server,từ các dịch vụ server như Active Directory, DNS, DHCP… đến các thành phần của hệ thống như .NET Framework 3.0, Network Load Balancing, Group Policy Management…

2.4 Các bước thực hiện

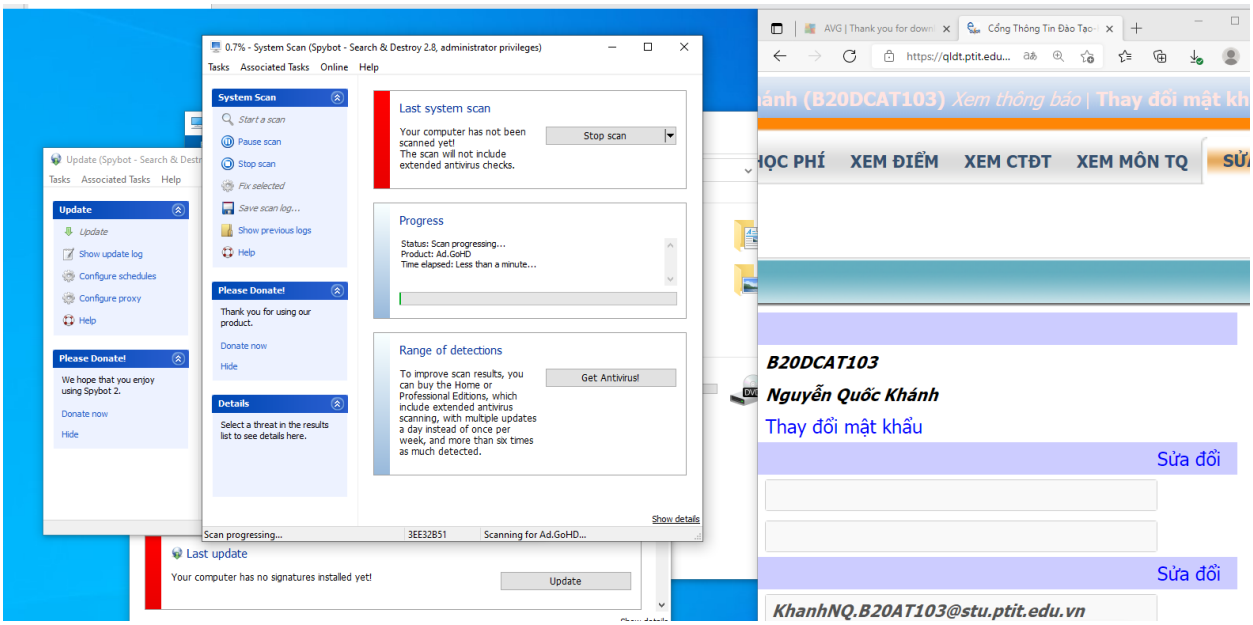
Đổi tên máy trạm:



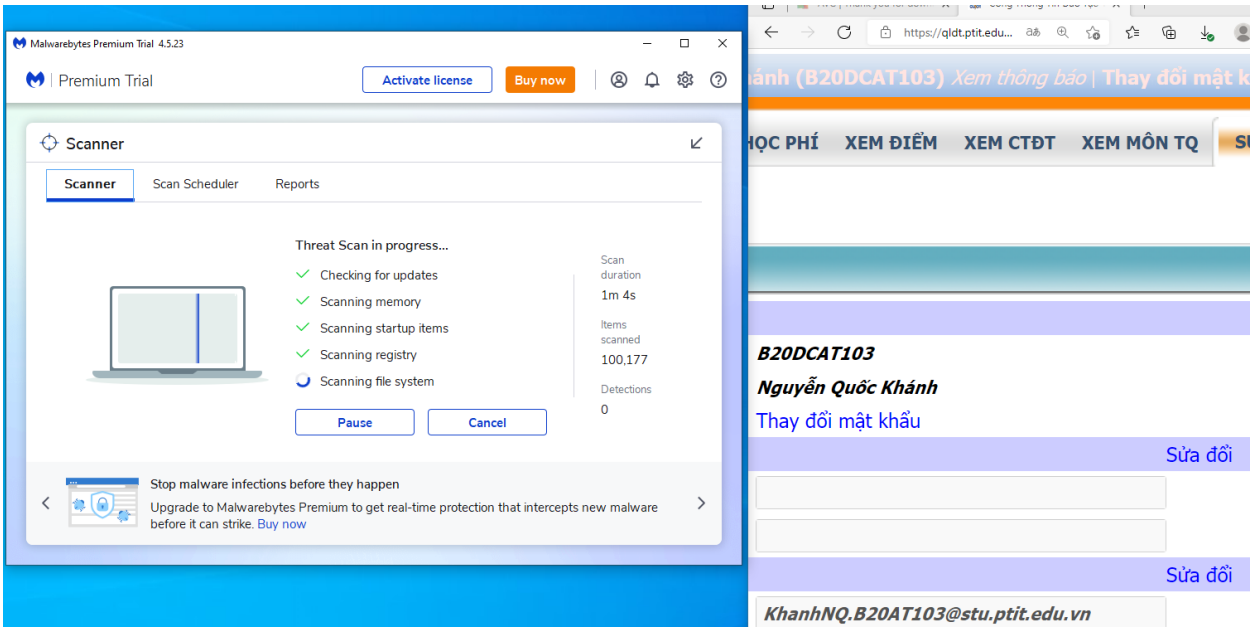
Cài đặt AVG AntiVirus:



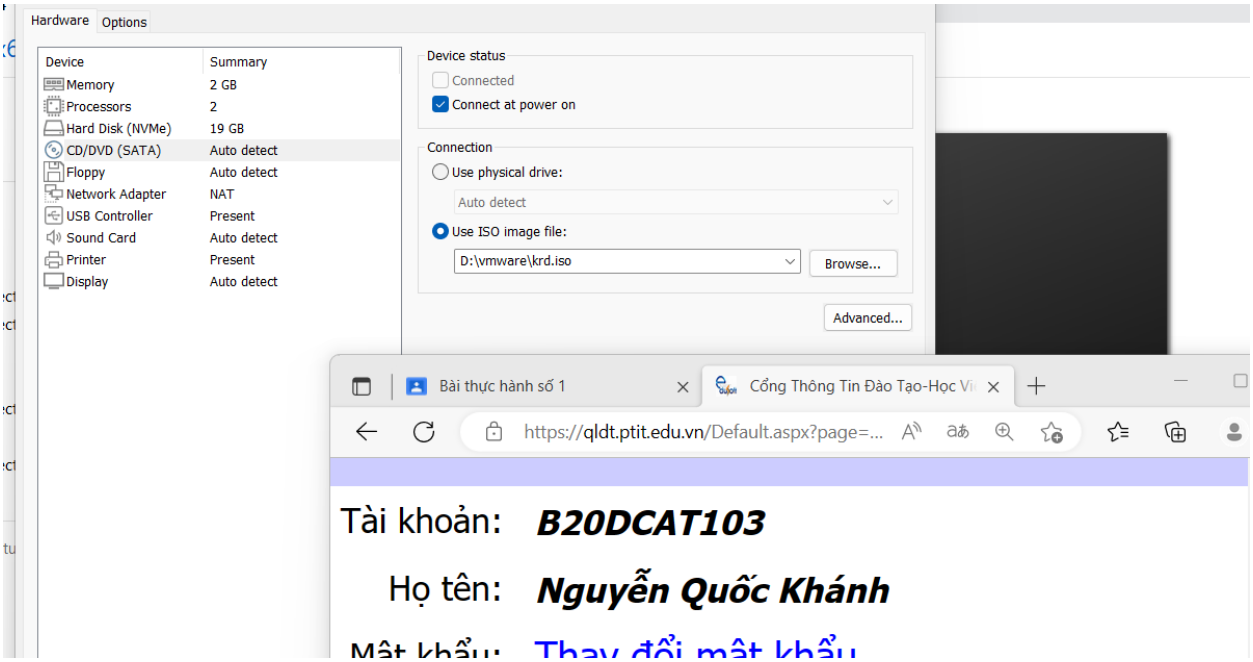
Cài đặt Spybot S&D:



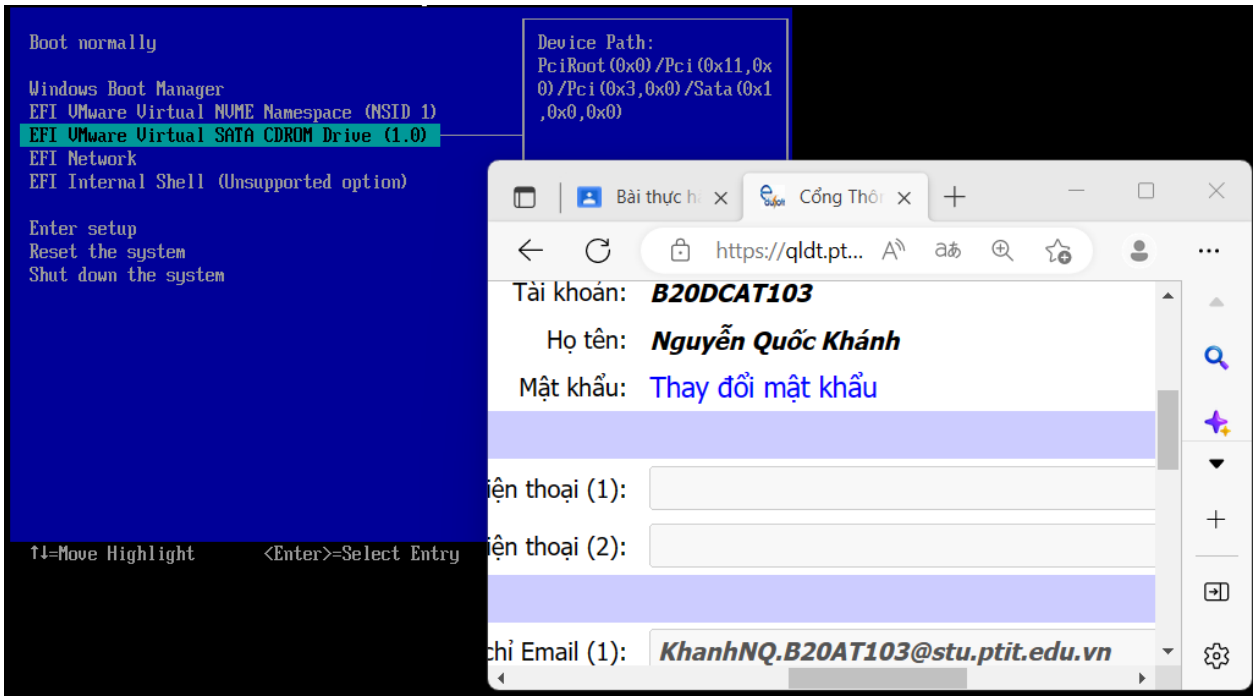
Cài đặt Malwarebytes Anti-Malware:



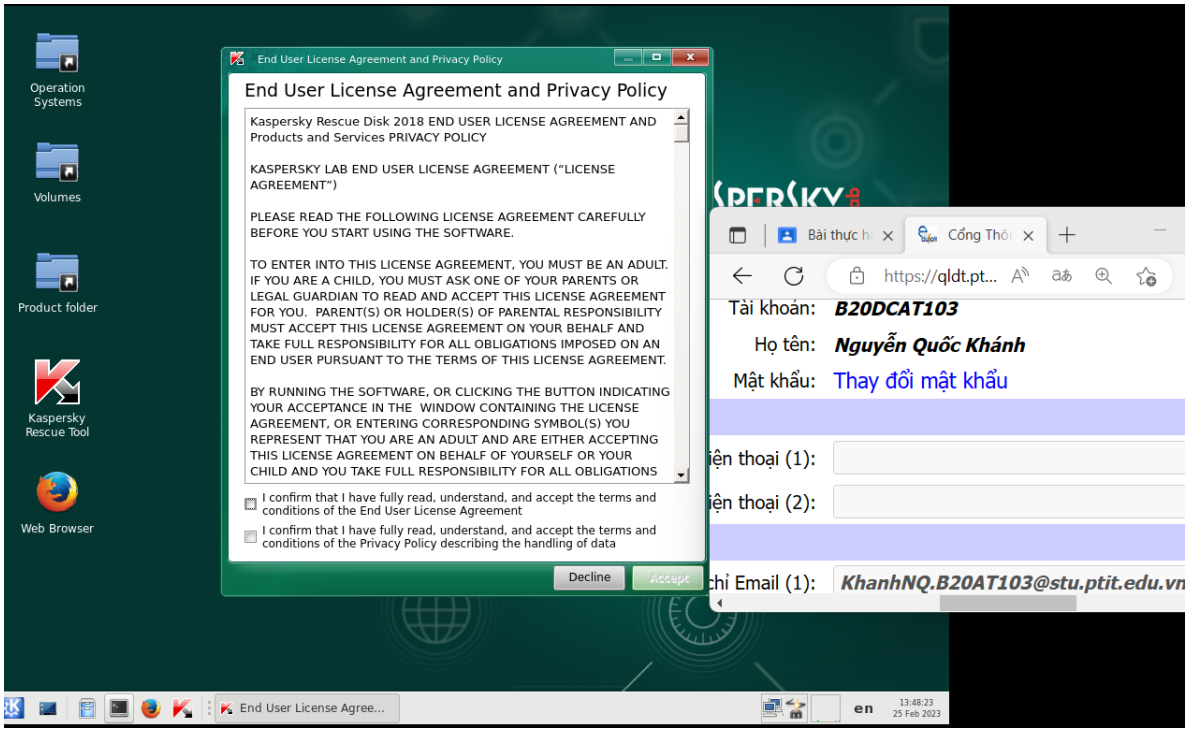
Cài đặt Kaspersky Rescue Disk (KRD):



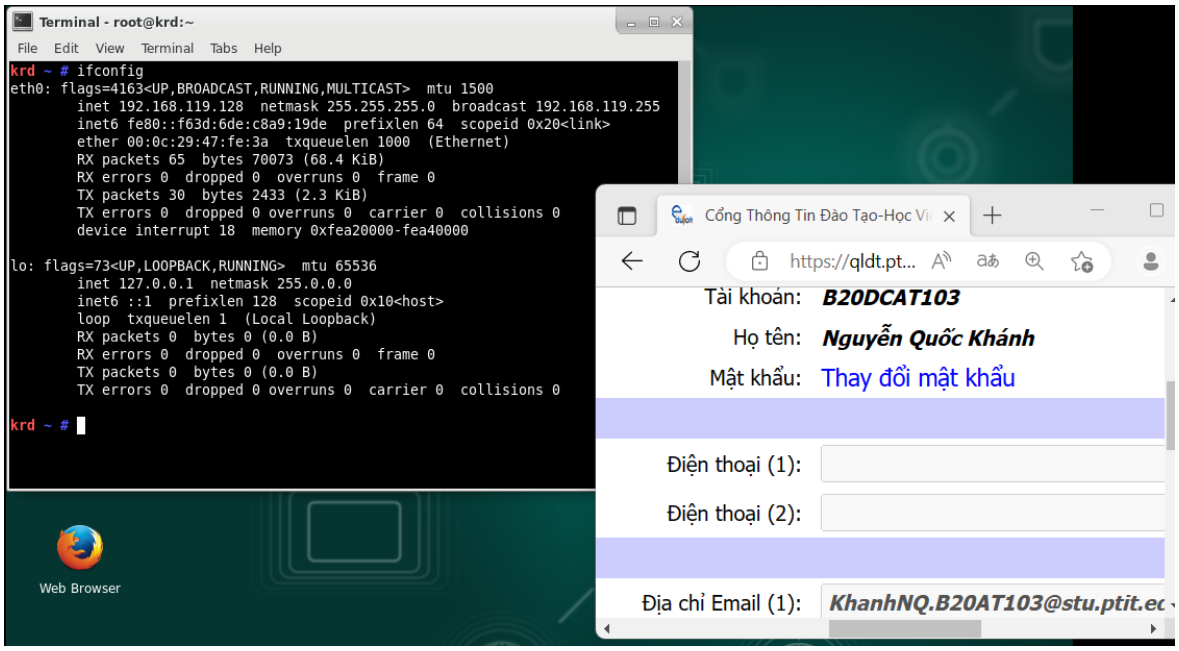
Load vào trong mục CD/DVD của máy trạm ảo để có thể khởi động máy trạm ảo dùng đĩa KRD



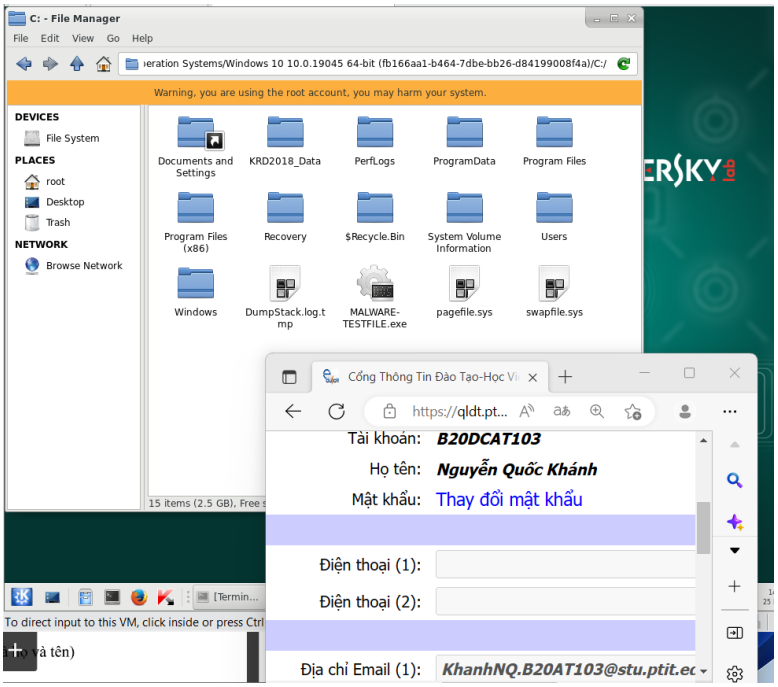
Load vào trong mục CD/DVD của máy trạm ảo để có thể khởi động máy trạm ảo dùng đĩa KRD



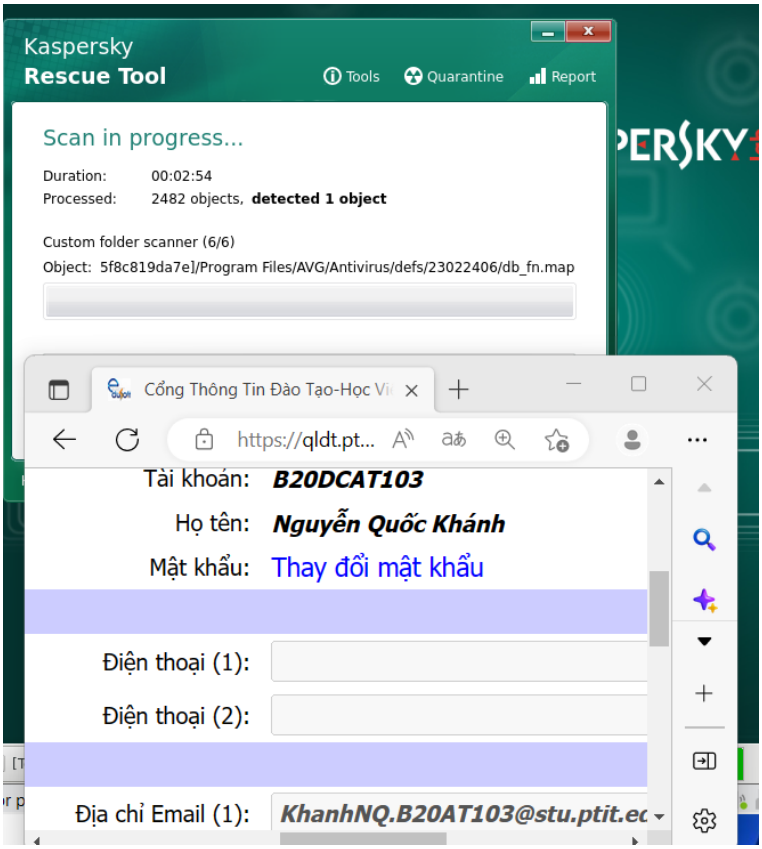
Kiểm tra IP của máy trạm bằng câu lệnh: ifconfig



Lưu file test mã độc vào ổ C của máy trạm



Chạy Kaspersky Rescue Tool:



Phát hiện ra file test mã độc và thực hiện xóa nó: