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

Báo cáo thực tập cơ sở

Bài 1: Cài đặt hệ điều hành máy trạm Windows

Giảng viên: Phạm Hoàng Duy
Sinh viên: Nguyễn Kim Bảo
Mã sinh viên: B22DCAT031
Hệ: Đại học chính quy

Hà Nội, 2/2025

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

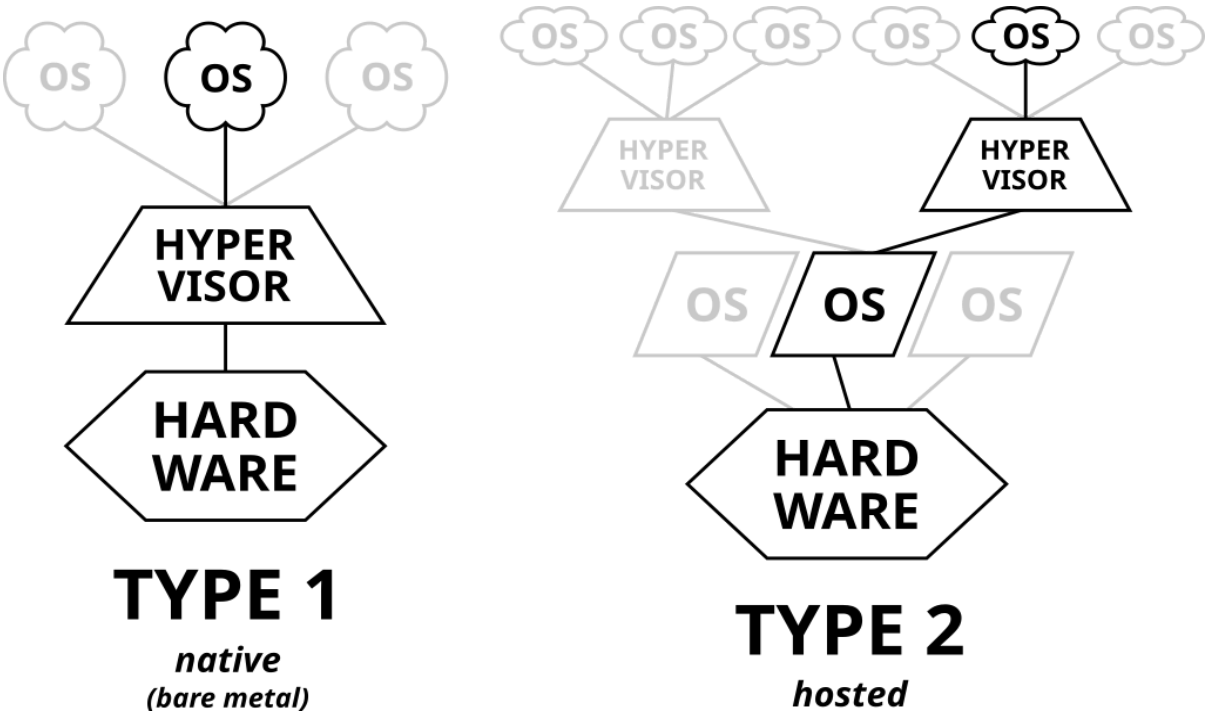
2.1 Tìm hiểu lý thuyết

2.1.1 Phần mềm ảo hóa Hypervisor

- Khái niệm Hypervisor

Hypervisor, còn được biết đến như trình giám sát máy ảo (Virtual Machine Monitor - VMM) hay bộ ảo hóa (Virtualizer), là một loại phần mềm, firmware hay phần cứng tạo và chạy các máy ảo. Một máy tính sử dụng hypervisor để chạy một hay nhiều máy ảo gọi là máy chủ (host machine), và mỗi máy ảo được gọi là một máy khách (guest machine). Hypervisor cung cấp cho hệ điều hành của máy khách một nền tảng hệ điều hành ảo để quản lý việc thực thi của chúng. Không giống với một trình giả lập (emulator), máy khách thực thi phần lớn câu lệnh trên phần cứng quản lý.
Phân loại

- Phân loại Hypervisor:
    - Hypervisor Loại 1 (Type-1) - Native hoặc Bare-Metal
        - Chạy trực tiếp trên phần cứng của máy chủ để kiểm soát và quản lý các hệ điều hành khách. Vì lý do này chúng thường được gọi là bare-metal hypervisors.
        - Một số có thể kể đến như : HyperV, VMware ESXi
    - Hypervisor Loại 2 (Type-2) - Hosted hypervisors
        - Chạy trên một hệ điều hành thông thường như một ứng dụng bình thường.
        - Một trình giám sát ảo hóa chạy như một tiến trình trên máy chủ
        - Loại 2 trừu tượng hóa hệ điều hành của máy khách khỏi máy chủ, tạo ra một hệ thống cô lập có thể tương tác qua máy chủ
        - Một số có thể kể đến như: Virtual Box, Vmware Workstation



- Một số phần mềm ảo hóa phổ biến
    - VirtualBox

VirtualBox là một phần mềm ảo hóa mã nguồn mở do Oracle phát triển, cho phép chạy nhiều hệ điều hành trên cùng một máy tính. Nó hỗ trợ nhiều hệ điều hành như Windows, Linux, macOS. VirtualBox có giao diện thân thiện, dễ sử dụng và miễn phí. Tuy nhiên, hiệu suất có thể kém hơn so với VMware khi chạy các máy ảo nặng.

    - VMware Workstation

VMware Workstation là một phần mềm ảo hóa mạnh mẽ do VMware phát triển, chuyên dụng cho doanh nghiệp và người dùng chuyên nghiệp. Nó hỗ trợ nhiều hệ điều hành, tối ưu hóa hiệu suất tốt hơn VirtualBox. VMware Workstation có bản miễn phí (VMware Workstation Player) và bản trả phí (VMware Workstation Pro) với nhiều tính năng nâng cao.

2.1.2 Tìm hiểu về hệ điều hành Windows

- **Lịch sử**

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. 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. Cùng thời điểm với Windows 3.1, Microsoft tung ra hệ điều hành khác gọi là Windows NT với nghĩa là hệ thống Windows công nghệ mới. Vào năm đầu của thế kỷ 21, Microsoft đưa ra Windows 2000 hướng tới môi trường máy chủ và máy trạm nhằm thay thế cho sản phẩm Windows NT trước đó. Vào năm 2001, 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 song không được người dùng chấp nhận rộng rãi như bản Windows XP. Windows 8 và đặc biệt là Windows 10 thể hiện sự thay đổi mạnh mẽ về việc sử dụng các thiết bị tính toán cá nhân mà máy tính PC là một đại diện. Và đến mới nhất hiện nay là Window 11 với nhiều cải tiến và tính năng mới so với Window 10.

- **Kiến trúc**

Kiến trúc của hệ điều hành Window về cơ bản được chia thành hai lớp tương ứng với hai chế độ hoạt động: chế độ nhân và chế độ người dùng. 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. Các chức năng cơ bản của chế độ người quản trị: Chương trình hỗ trợ hệ thống, các chương trình dịch vụ, ứng dụng người dùng, hệ thống con. Các chức năng cơ bản của chế độ nhân: Thực thi, nhân, các trình điều khiển thiết bị, lớp phần cứng trừu tượng, các chức năng cửa sổ và đồ họa

- **Giao diện**

Hệ điều hành Windows có ba cách giao tiếp chính giúp làm việc với các ứng dụng và 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 quang trọng trong GUI là menu khởi động, thanh tác vụ và màn hình làm việc.

  - **Giao diện dòng lệnh**

    Giao diện này là giao diện xưa nhất của Microsoft đó chính là dòng lệnh DOS. Trong môi trường Windows nó không còn thực sự là DOS dù nhiều lệnh DOS vẫn còn dùng được. Thông qua giao diện này người dùng có thể thực thi các thao tác cấu hình cho hệ điều hành.

  - **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 quang trọng của PowerShell là khả năng lập trình đơn giản và thực thi các lệnh từ xa.

- **Đặc điểm đặc trưng**

Khả năng tương thích cao do đây vẫn là hệ điều hành có tỷ lệ người dùng cao nhất trên toàn cầu. Tuy nhiên, đây cũng là lý do mà hệ điều hành này là mục tiêu hàng đầu của các hacker, tin tắc nhắm đến. Dễ sử dụng do Windows ngày càng được cải tiến về tính năng và giao diện theo hướng đơn giản hóa tối đa.

2.1.3 Tìm hiểu phần mềm diệt virus, phần mềm chống phần mềm gián điệp, phần mềm cứu hộ.

- **Phần mềm diệt virus**

Phần mềm diệt virus là một chương trình được tạo ra để tìm kiếm, phát hiện và ngăn chặn hoặc loại bỏ phần mềm virus ra khỏi thiết bị. Các phần mềm gây hại khác như sâu, phần mềm quảng cáo, hoặc các mối đe dọa cũng có thể được phát hiện và loại bỏ qua phần mềm diệt virus

- **Phần mềm chống phần mềm gián điệp**

Phần mềm chống phần mềm gián điệp phát hiện, chặn và loại bỏ các phần mềm gián điệp, bảo vệ quyền riêng tư của người dùng và tính an toàn thông tin. Nó sử dụng phương pháp phát hiện dựa theo đặc trưng và dựa theo luật để định danh và tiêu diệt mối nguy gián điệp

- **Phần mềm cứu hộ**

Phần mềm cứu hộ là một công cụ được thiết kế đặc biệt để khôi phục các dữ liệu bị mất, xóa, hỏng và không thể truy cập từ kho lưu trữ của các thiết bị như ổ cứng, SSDs, USB, thẻ nhớ,.... Công cụ này rất lý tưởng trong việc khôi phục dữ liệu bị mất do vấn đề về logic, thao tác xóa ngoài ý muốn, và các lỗi định dạng, nhưng không thể khôi phục dữ liệu mất do viruses hay các phần mềm độc hại cũng như các tổn thương vật lý tới các thiết bị.

2.2 Tài liệu tham khảo

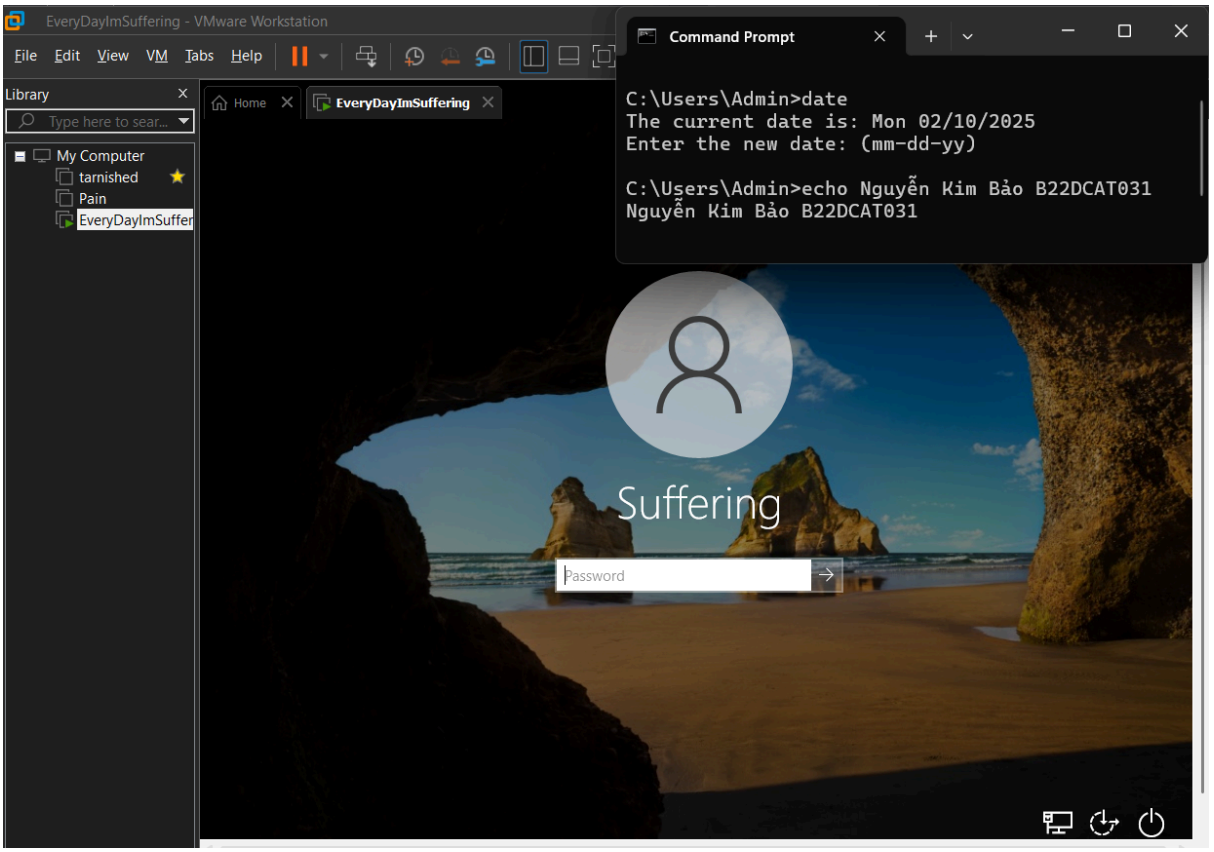
- Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.
- Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.

2.3 Chuẩn bị môi trường

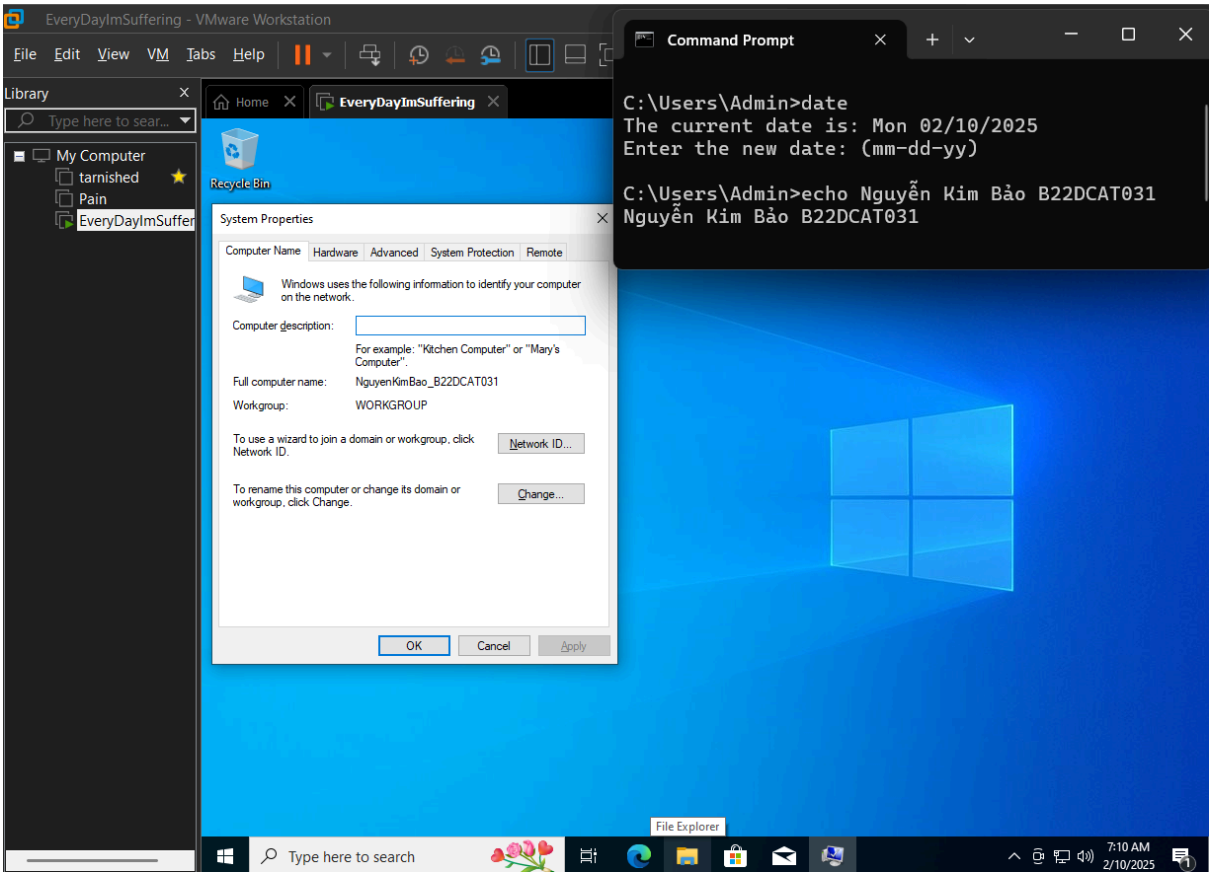
- File cài đặt Windows 7 (hoặc Windows 10/11) định dạng iso.
- Phần mềm ảo hóa ví dụ: VMWare Workstation.

2.4 Các bước thực hiện

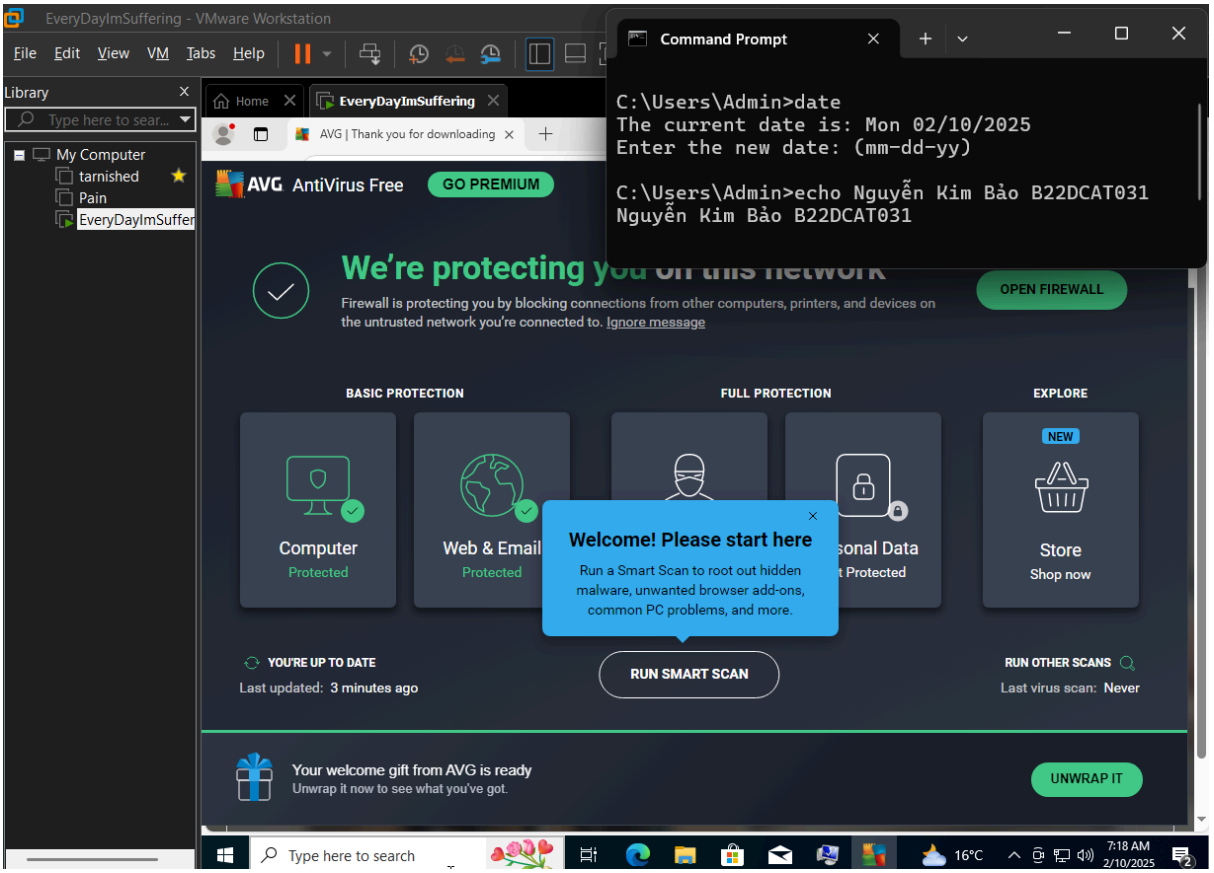
- Khởi động chương trình máy ảo, cài đặt Windows 7/10/11 từ file đã chuẩn bị.



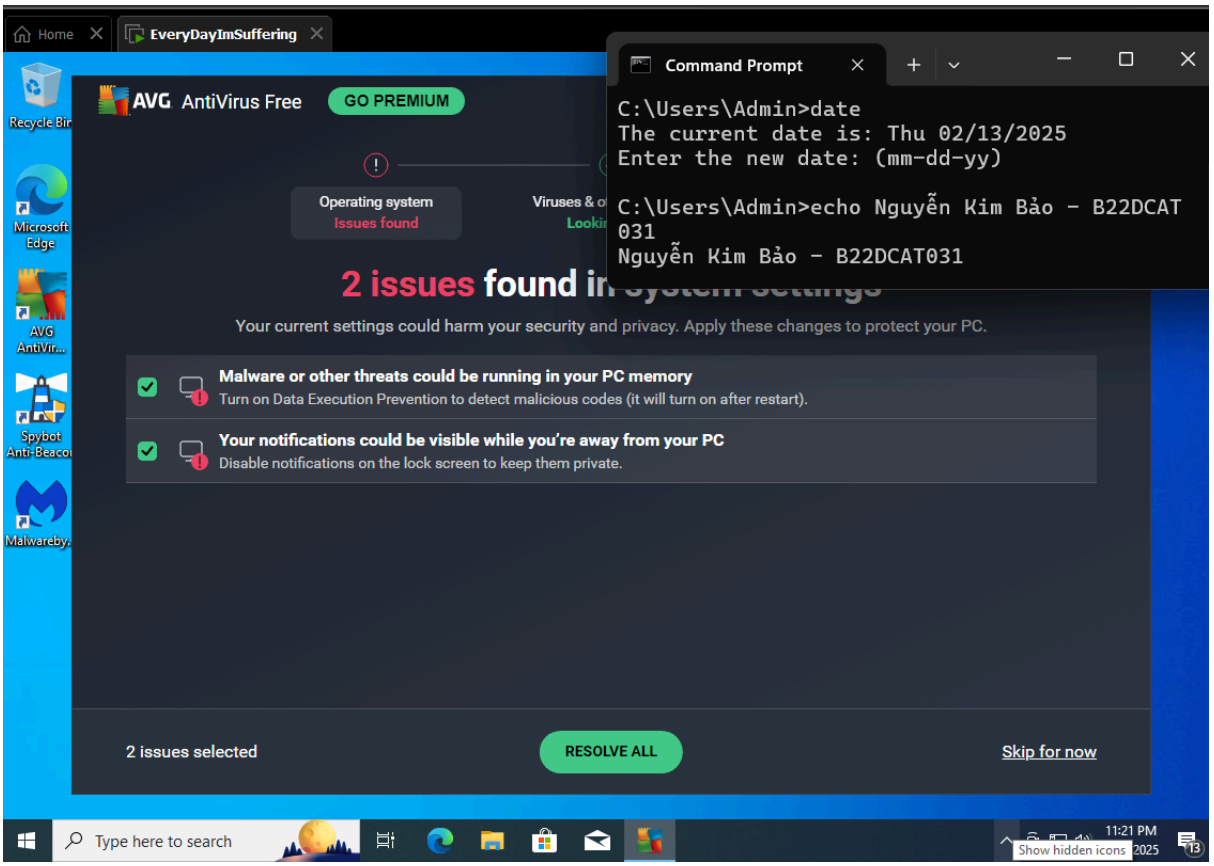
- Trong mục “System Properties” đổi tên máy trạm Windows thành “họ tên SV_mã SV”.



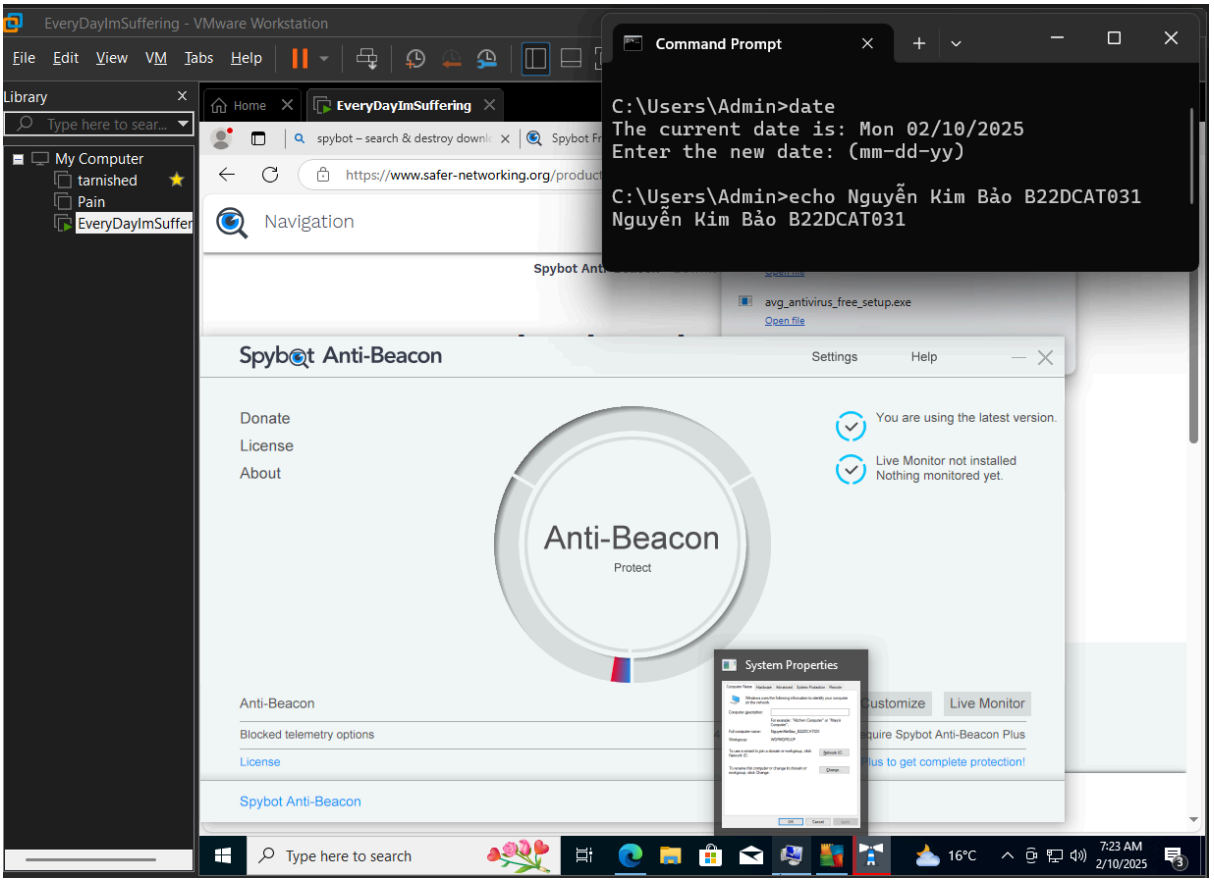
- Thực hiện cài đặt và chạy một số phần mềm bảo vệ máy trạm sau:
  - Phần mềm diệt virut: AVG AntiVirus.
    - Cài đặt thành công



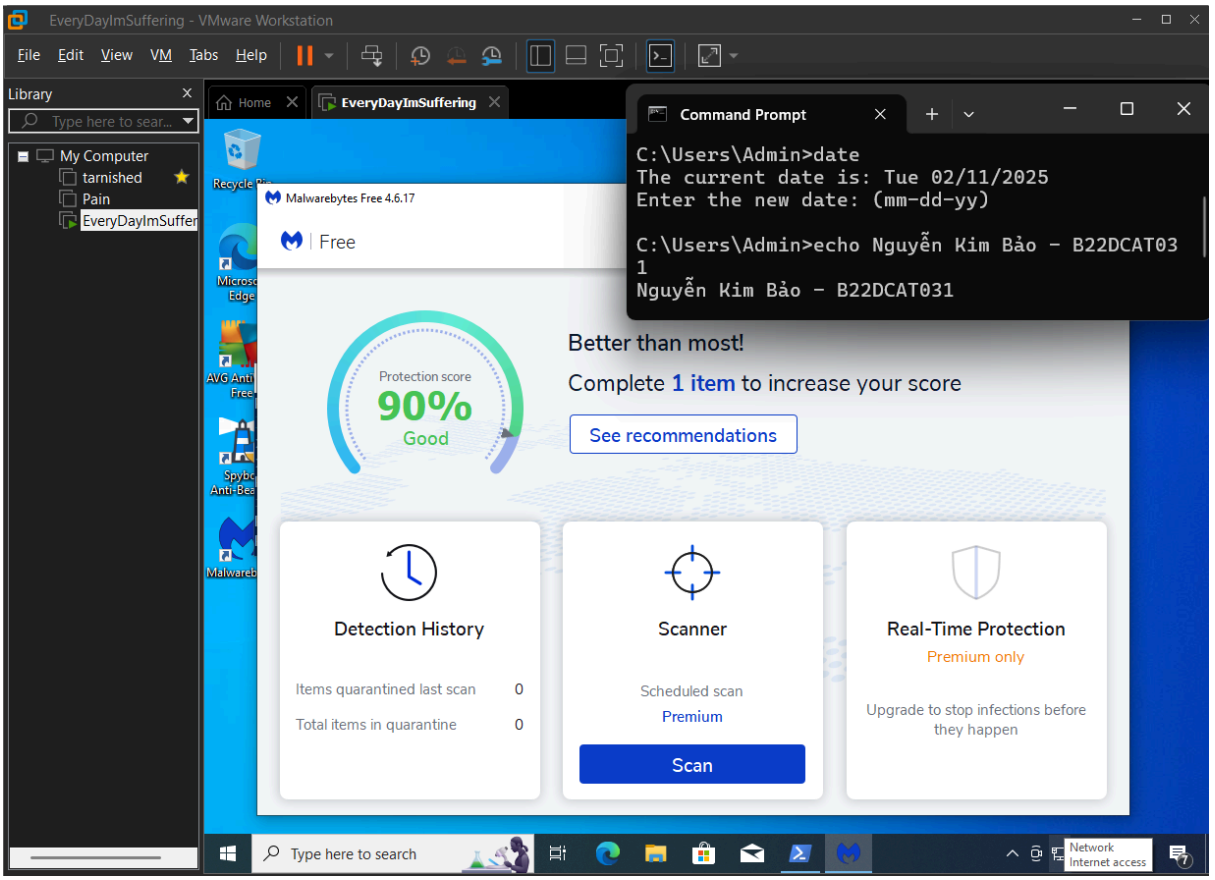
    - Chạy và sử dụng phần mềm thành công.



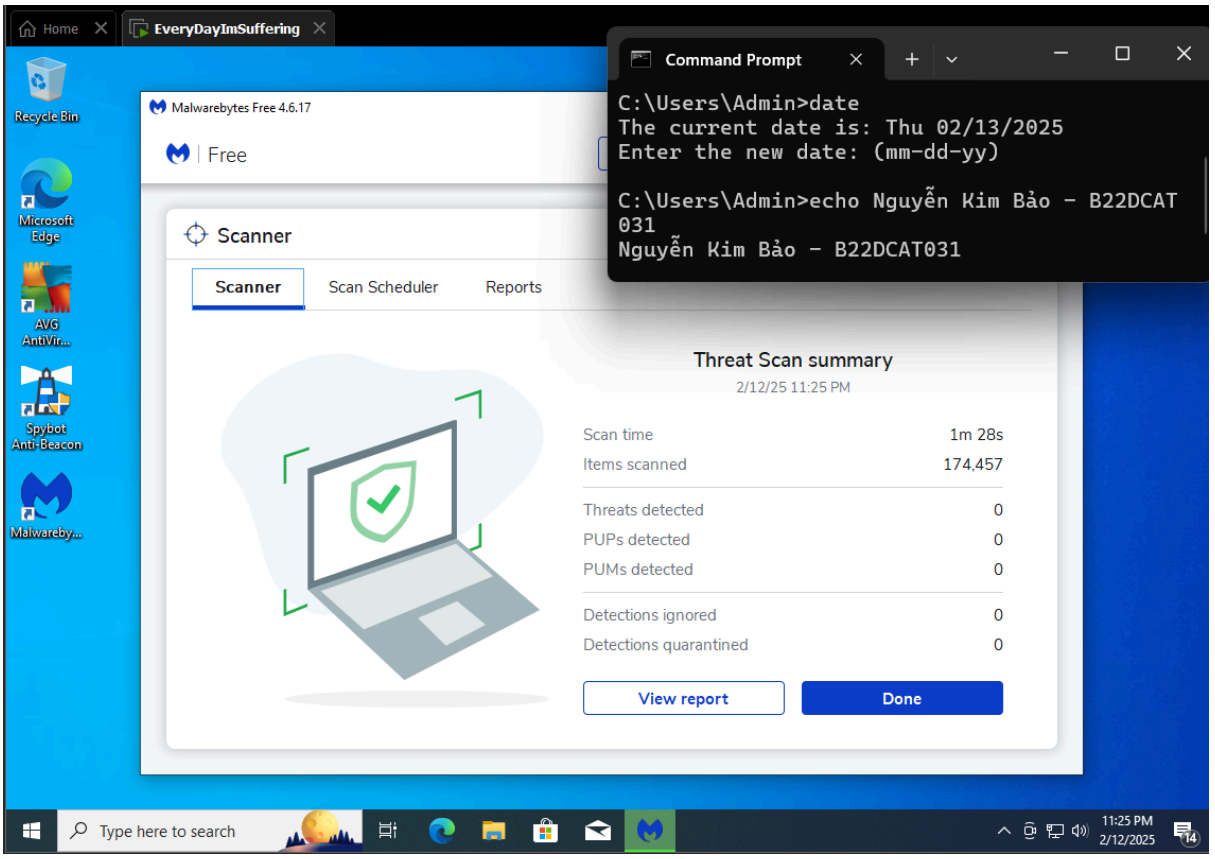
- 1
  - Phần mềm chống phần mềm gián điệp Spybot S&D (Spybot – Search & Destroy)
    - Cài đặt thành công, chạy và sử dụng phần mềm thành công.



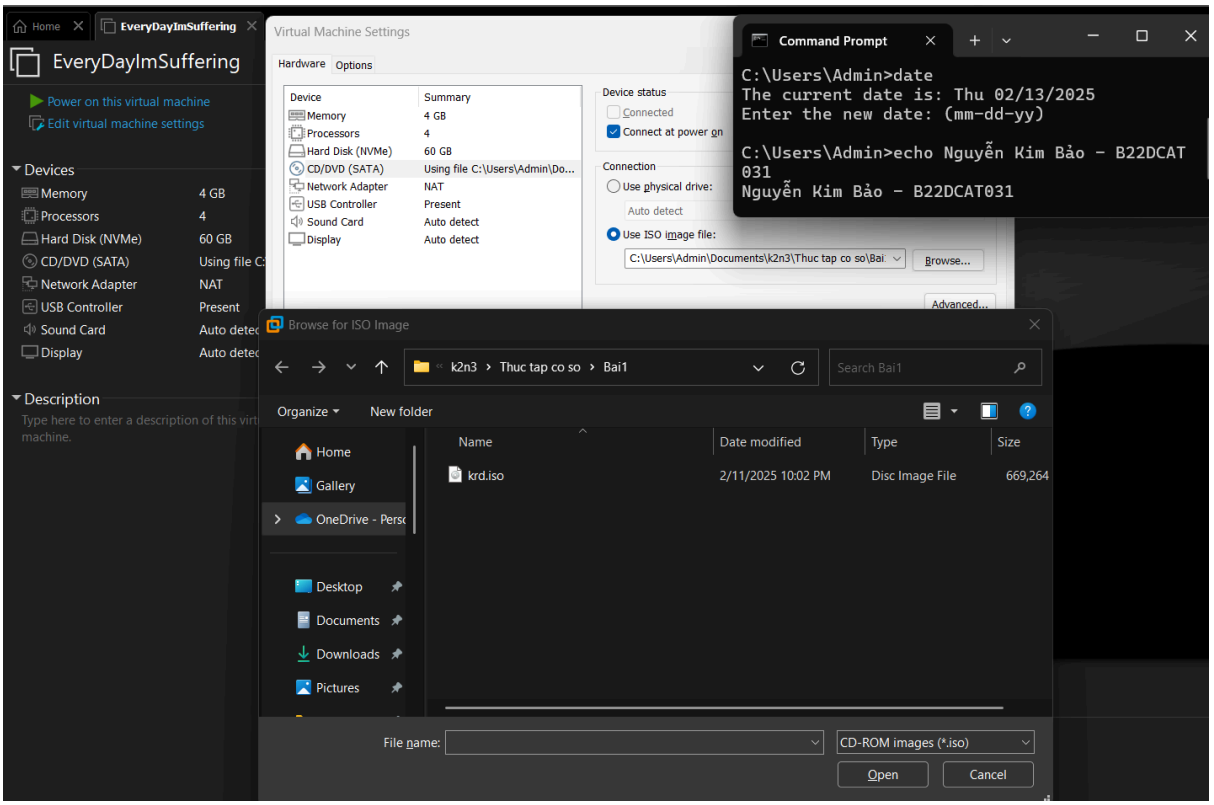
- Phần mềm chống các phần mềm độc hại: Malwarebytes Anti-Malware
  - Cài đặt thành công.



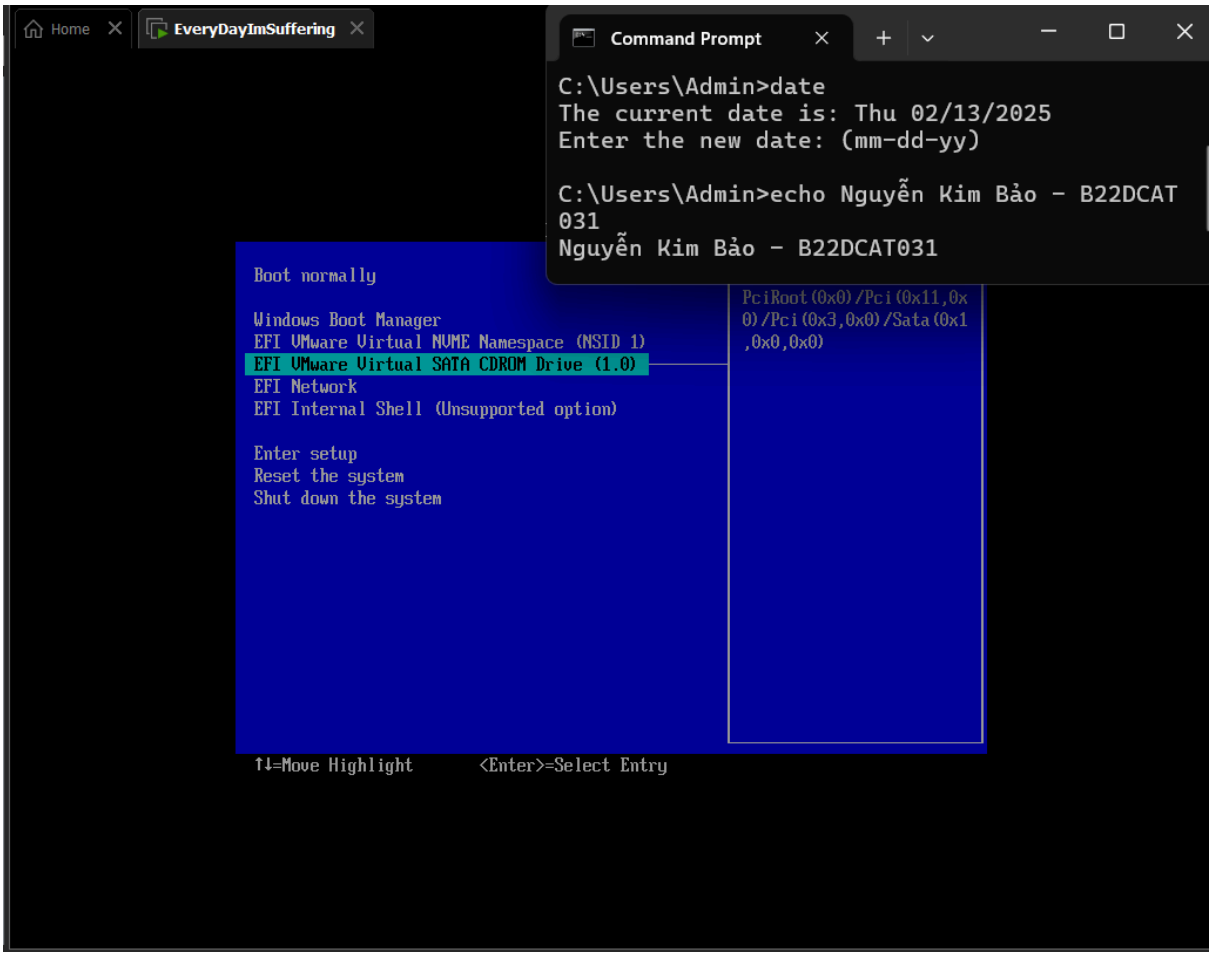
  - Chạy và sử dụng phần mềm thành công.

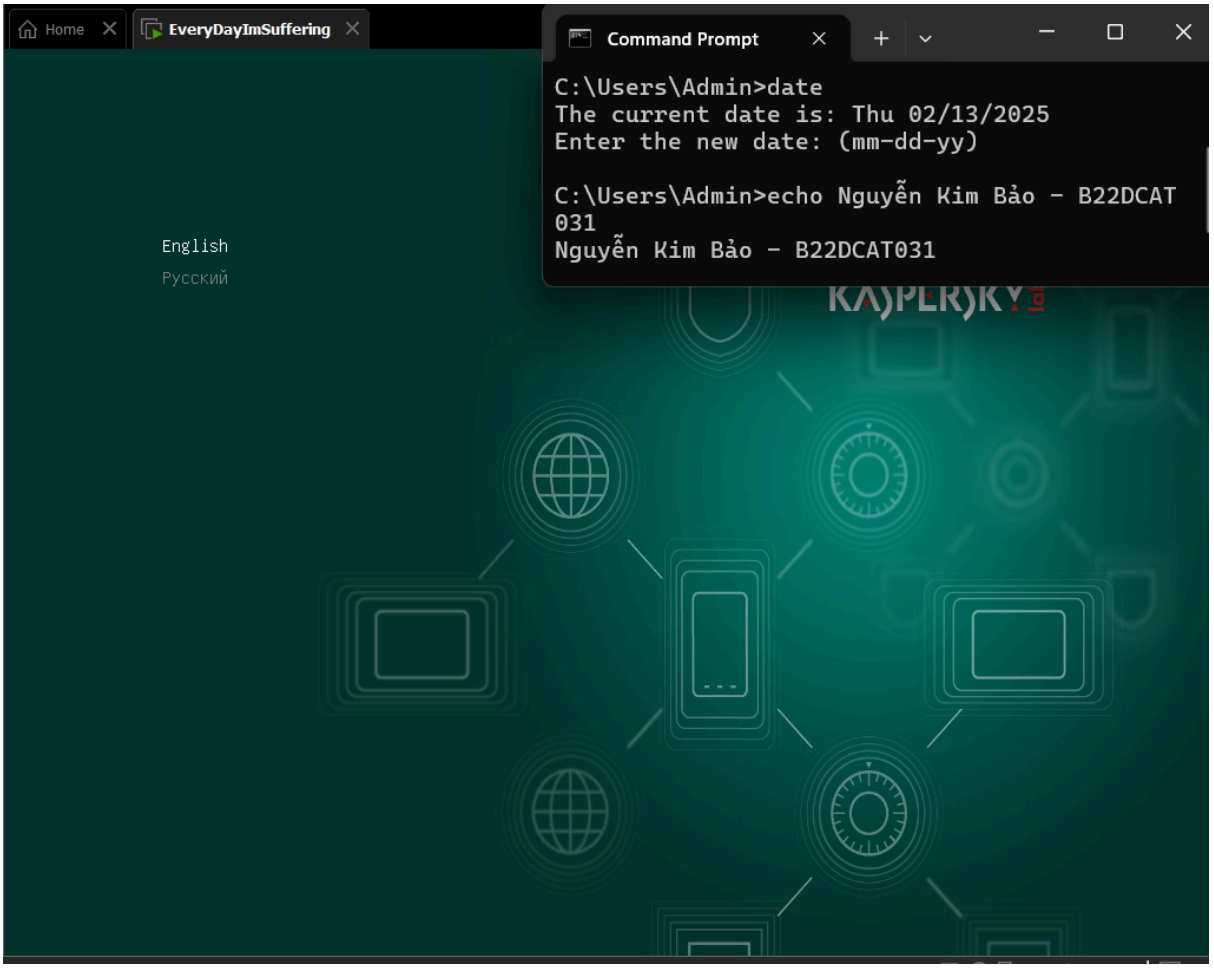


- Phần mềm cứu hộ: Kaspersky Rescue Disk (KRD)
  - ▪ Tải phần mềm cứu hộ dạng iso: https://www.kaspersky.com/downloads/free-rescue-disk. Load vào trong mục CD/DVD của máy trạm ảo để có thể khởi động máy trạm ảo dùng đĩa KRD

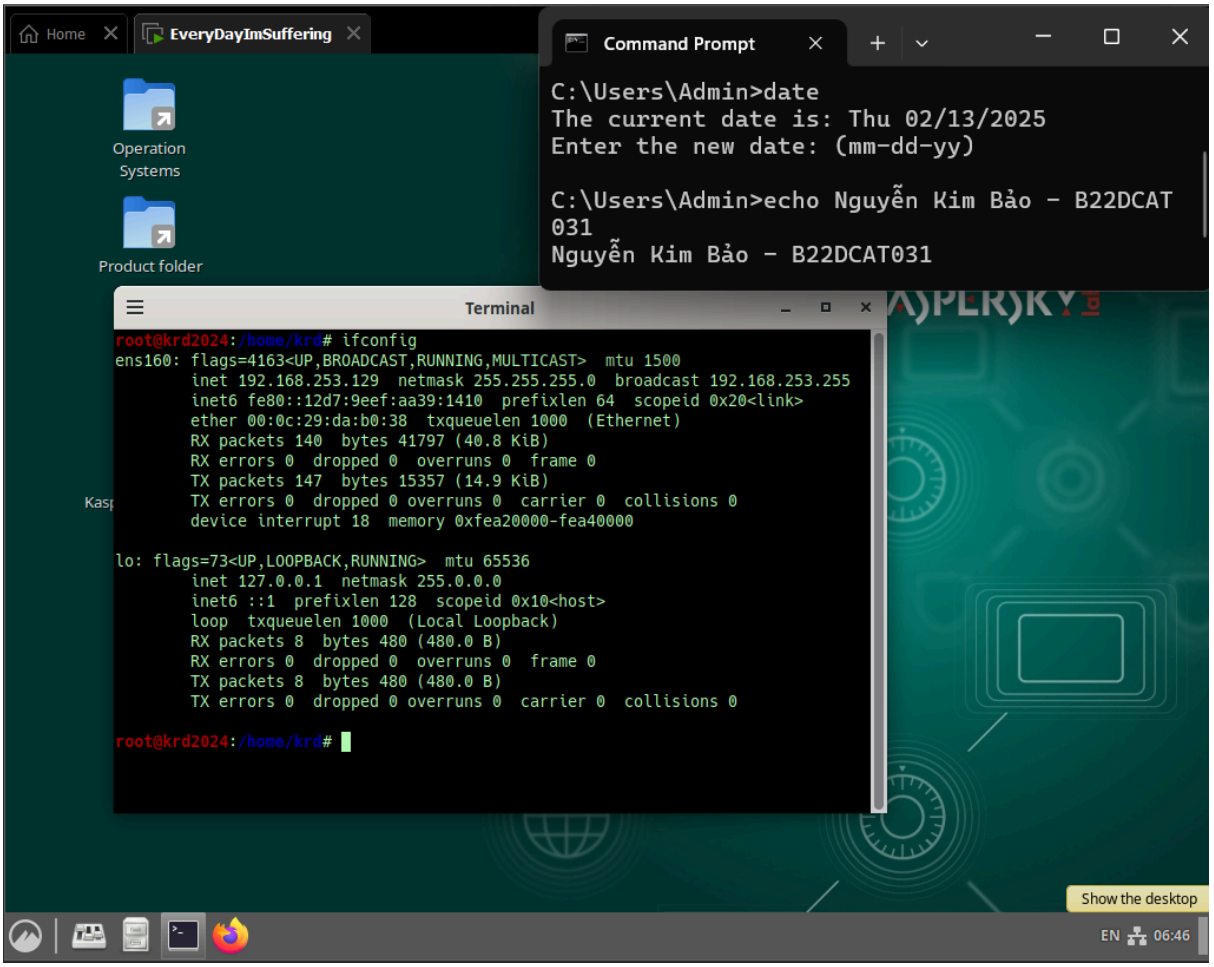


  - Chạy máy trạm ảo, sử dụng phím “esc” để chọn boot từ CD-ROM drive để cài đặt KRD.

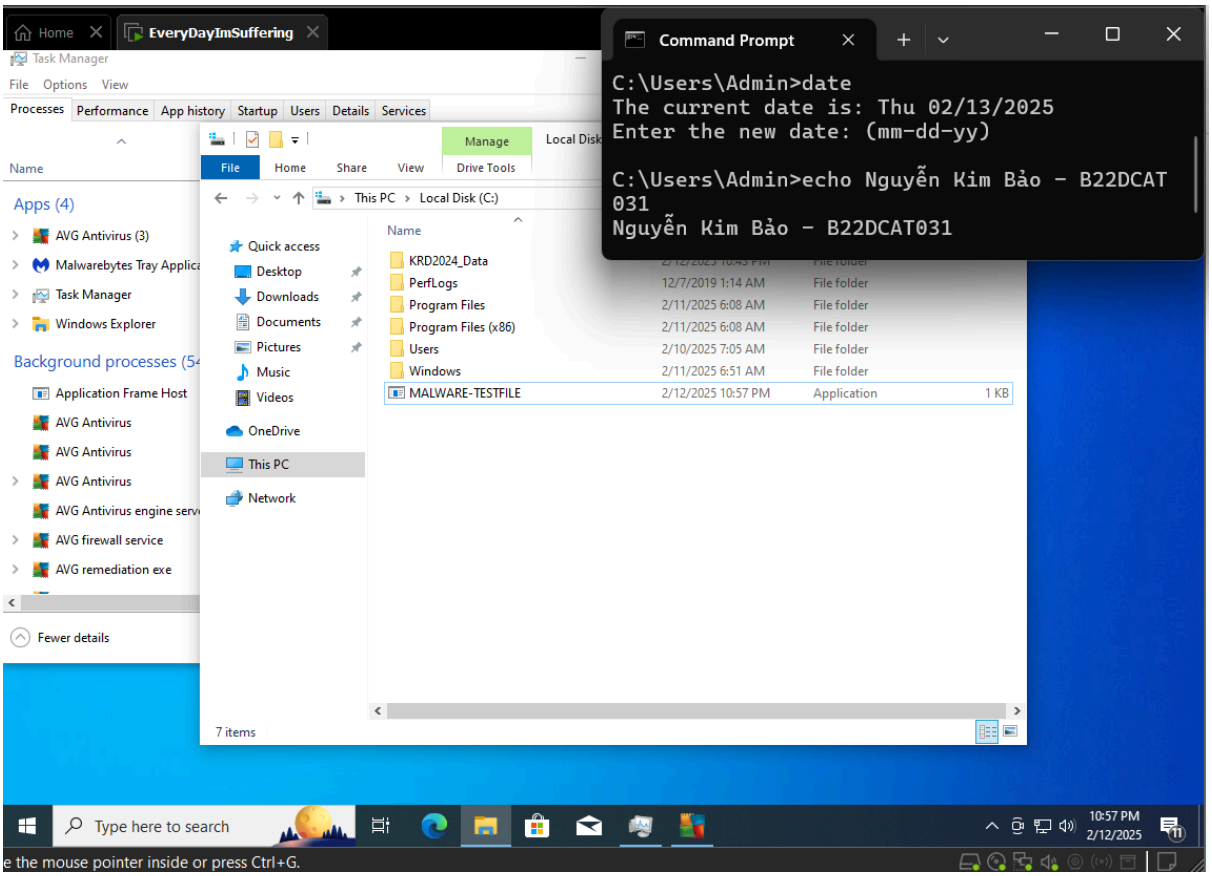

Home
EveryDayImSuffering
Command Prompt
C:\Users\Admin>date
The current date is: Thu 02/13/2025
Enter the new date: (mm-dd-yy)
C:\Users\Admin>echo Nguyễn Kim Bảo - B22DCAT031
031
Nguyễn Kim Bảo - B22DCAT031
Boot normally
Windows Boot Manager
EFI VMware Virtual NVME Namespace (NSID 1)
EFI VMware Virtual SATA CDROM Drive (1.0)
EFI Network
EFI Internal Shell (Unsupported option)
Enter setup
Reset the system
Shut down the system
PciRoot(0x0)/Pci(0x11,0x0)/Pci(0x3,0x0)/Sata(0x1,0x0,0x0)
↑↓=Move Highlight
<Enter>=Select Entry


Home
EveryDayImSuffering
Command Prompt
C:\Users\Admin>date
The current date is: Thu 02/13/2025
Enter the new date: (mm-dd-yy)
C:\Users\Admin>echo Nguyễn Kim Bảo - B22DCAT031
031
Nguyễn Kim Bảo - B22DCAT031
English
Русский

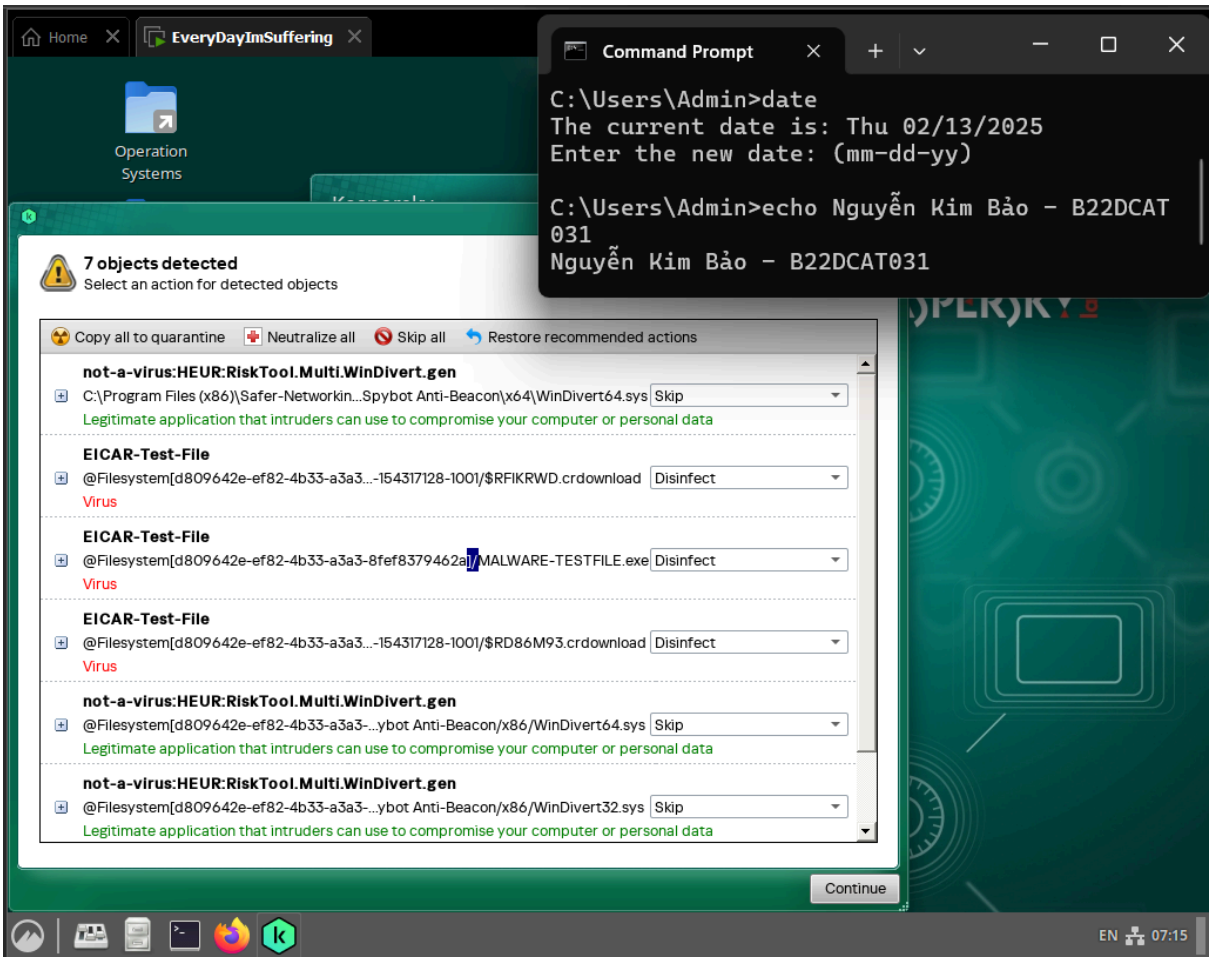
- Mở cmd kiểm tra IP của máy trạm bằng câu lệnh: ifconfig

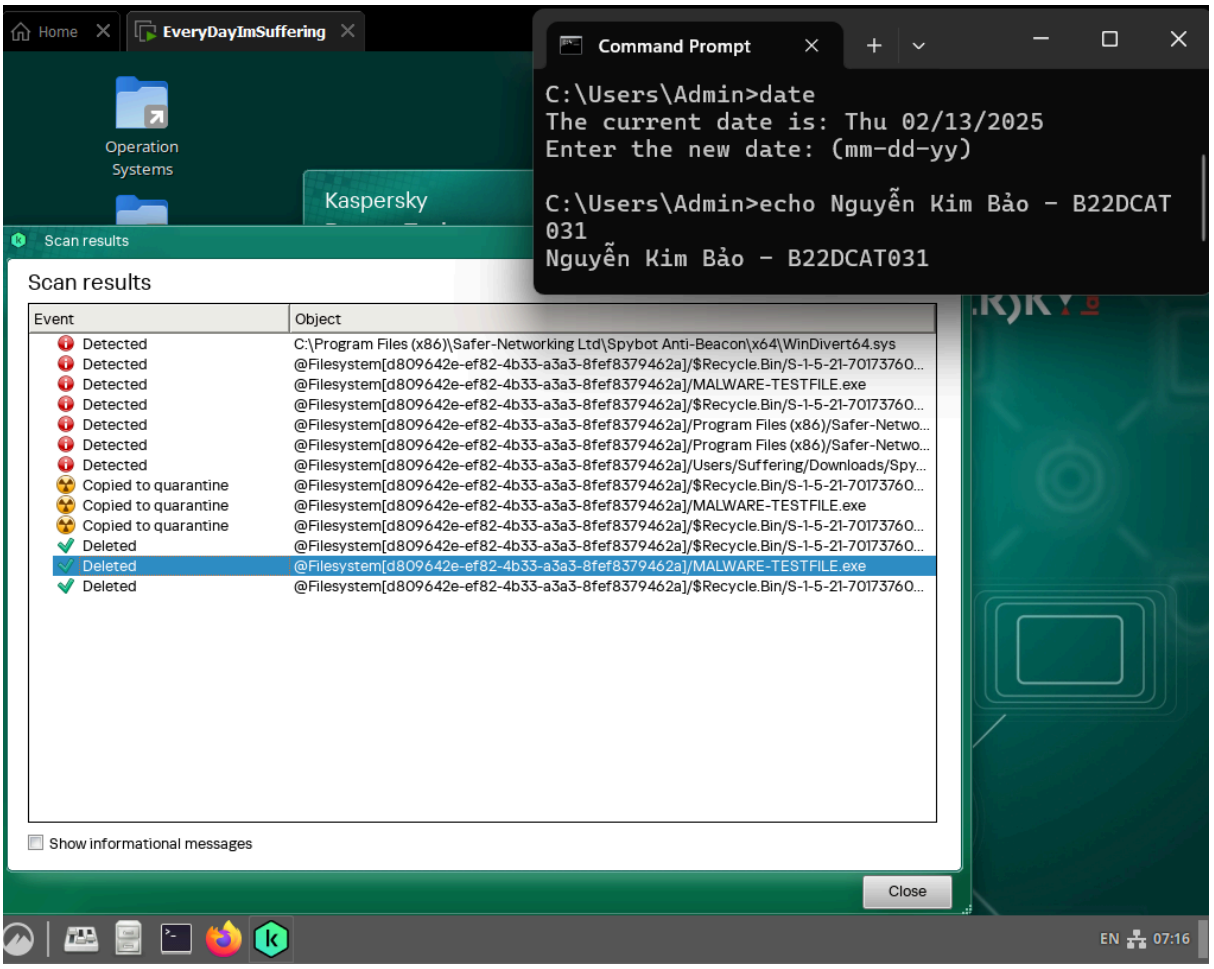


- Dùng Web browser tải file test mã độc từ đường link : http://www.computersecuritystudent.com/WINDOWS/W7/lesson7/MALWARE-TESTFILE.exe. Lưu file test mã độc vào ổ C của máy trạm



- 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.




Home
EveryDayImSuffering
Operation Systems
Kaspersky
Command Prompt
C:\Users\Admin>date
The current date is: Thu 02/13/2025
Enter the new date: (mm-dd-yy)
C:\Users\Admin>echo Nguyễn Kim Bảo - B22DCAT031
Nguyễn Kim Bảo - B22DCAT031
Scan results
Scan results
Event
Object
Detected C:\Program Files (x86)\Safer-Networking Ltd\Spybot Anti-Beacon\x64\WinDivert64.sys
Detected @Filesystem[d809642e-ef82-4b33-a3a3-8fef8379462a]/$Recycle.Bin/S-1-5-21-70173760...
Detected @Filesystem[d809642e-ef82-4b33-a3a3-8fef8379462a]/MALWARE-TESTFILE.exe
Detected @Filesystem[d809642e-ef82-4b33-a3a3-8fef8379462a]/$Recycle.Bin/S-1-5-21-70173760...
Detected @Filesystem[d809642e-ef82-4b33-a3a3-8fef8379462a]/Program Files (x86)/Safer-Netwo...
Detected @Filesystem[d809642e-ef82-4b33-a3a3-8fef8379462a]/Program Files (x86)/Safer-Netwo...
Detected @Filesystem[d809642e-ef82-4b33-a3a3-8fef8379462a]/Users/Suffering/Downloads/Spy...
Copied to quarantine @Filesystem[d809642e-ef82-4b33-a3a3-8fef8379462a]/$Recycle.Bin/S-1-5-21-70173760...
Copied to quarantine @Filesystem[d809642e-ef82-4b33-a3a3-8fef8379462a]/MALWARE-TESTFILE.exe
Copied to quarantine @Filesystem[d809642e-ef82-4b33-a3a3-8fef8379462a]/$Recycle.Bin/S-1-5-21-70173760...
Deleted @Filesystem[d809642e-ef82-4b33-a3a3-8fef8379462a]/$Recycle.Bin/S-1-5-21-70173760...
Deleted @Filesystem[d809642e-ef82-4b33-a3a3-8fef8379462a]/MALWARE-TESTFILE.exe
Deleted @Filesystem[d809642e-ef82-4b33-a3a3-8fef8379462a]/$Recycle.Bin/S-1-5-21-70173760...
Show informational messages
Close
EN 07:16