

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



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 1.1
CÀI ĐẶT HỆ ĐIỀU HÀNH MÁY TRẠM WINDOWS**

Sinh viên thực hiện:

B22DCAT018 – Nguyễn Hoàng Anh

Giảng viên hướng dẫn: ThS. Ninh Thị Thu Trang

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

Mục Lục	2
Danh Mục Các Hình Vẽ	3
Danh Mục Các Bảng Biểu	4
Danh Mục Các Từ Viết Tắt	5
Chương 1. Giới Thiệu Chung Về Bài Thực Hành.....	6
1.1 Mục Đích	6
1.2 Tìm Hiểu Lý Thuyết	6
1.2.1 Phần Mềm Ảo Hoá Vmware Workstation	6
1.2.2 Hệ Điều Hành Windows	6
1.2.2.1 Lịch Sử Hệ Điều Hành Windows	6
1.2.2.2 Kiến Trúc Của Hệ Điều Hành Windows	9
1.2.2.3 Giao Diện Của Hệ Điều Hành Windows	10
1.2.2.4 Hệ Thống File Của Hệ Điều Hành Windows	11
1.2.3 Các Phần Mềm Diệt Virut, Phần Mềm Chống Phần Mềm Gián Điệp, Phần Mềm Cứu Hộ	12
1.2.3.1 Phần Mềm Diệt Virut	12
1.2.3.2 Phần Mềm Chống Phần Mềm Gián Điệp	12
1.2.3.3 Phần Mềm Cứu Hộ	12
Chương 2. Nội Dung Thực Hành	13
2.1 Chuẩn Bị Môi Trường	13
2.2 Các Bước Thực Hiện	13
2.2.1 Cài Đặt Windows	13
2.2.2 Cài Đặt Phần Mềm Diệt Virus	13
2.2.2.1 Phần Mềm Diệt Virut Avg Antivirus	13
2.2.2.2 Phần Mềm Chống Phần Mềm Gián Điệp Spybot S&D	14
2.2.2.3 Phần Mềm Chống Các Phần Mềm Độc Hại Malwarebytes Anti-Malware	15
2.2.2.3 Phần Mềm Cứu Hộ Kaspersky Rescue Disk (Krd)	16
Tổng Kết	22
Tài Liệu Tham Khảo	23

DANH MỤC CÁC HÌNH VẼ

Hình 1 - Giao diện dòng lệnh của MS-DOS	7
Hình 2 - Giao diện menu và đồ hoạ Windows 3.1	8
Hình 3 - Kiến trúc cơ bản của hệ điều hành Windows.....	9
Hình 4 - File Windows 10 định dạng iso	13
Hình 5 - Màn hình máy ảo Windows 10	13
Hình 6 - Cài đặt thành công phần mềm AVG AntiVirus	14
Hình 7 - Quét máy tính thành công với phần mềm AVG AntiVirus	14
Hình 8 - Cài đặt thành công Spybot S&D	15
Hình 9 - Quét máy bằng Spybot S&D.....	15
Hình 10 - Cài đặt thành công Malwarebytes Anti-Malware	16
Hình 11 - Quét máy tính bằng Malwarebytes Anti-Malware.....	16
Hình 12 - File định dạng iso của KRD	17
Hình 13 - Load vào mục CD/DVD của máy ảo	17
Hình 14 - Ấn esc để vào boot manager	18
Hình 15 - Giao diện KRD	19
Hình 16 - File mã độc.....	19
Hình 17 - Kiểm tra ip	20
Hình 18 - Quét phát hiện mã độc thành công.....	21
Hình 19 - Thông tin sinh viên thực hiện	22

DANH MỤC CÁC BẢNG BIỂU

Bảng 1. Tương quan các hệ thống file Windows	11
--	----

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
MS-DOS	Microsoft Disk Operating System	Hệ điều hành đĩa từ Microsoft
HAL	Hardware Abstraction Layer	Lớp phần cứng trừu tượng
GUI	Graphical User Interface	Giao diện đồ họa người dùng

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

Rèn luyện kỹ năng cài đặt và quản trị hệ điều hành máy trạm Windows cho người dùng với các dịch vụ cơ bản.

1.2 Tìm hiểu lý thuyết

1.2.1 Phần mềm ảo hoá VMWARE Workstation

VMWare Workstation là phần mềm máy chủ ảo giúp tạo ra các máy ảo với CPU, bộ nhớ, mạng và bộ lưu trữ riêng. Các máy ảo này được tạo ra từ phần cứng vật lý thông qua phần mềm hypervisor và hoạt động như hệ thống máy tính độc lập. Đồng thời chia sẻ tài nguyên từ máy chủ để có thể sử dụng.

VMware Workstation được sử dụng để tạo và quản lý các máy ảo trên một máy tính, nên tầm quan trọng của nó bao gồm:

- Cho phép bạn tạo nhiều hệ điều hành khác nhau trên cùng một máy tính mà không làm ảnh hưởng tới hiệu suất cũng như tính năng của toàn hệ thống.
- Tạo điều kiện cho nhà phát triển phần mềm kiểm tra và phát triển được các ứng dụng trên nhiều hệ điều hành.
- Cung cấp một môi trường ảo hóa an toàn với người dùng và để thử nghiệm các ứng dụng mới hoặc hệ thống cập nhật mà không làm ảnh hưởng và làm hỏng tới hệ thống hiện tại đang chạy.
- Tiết kiệm chi phí phát triển các phần mềm mới bởi sử dụng các máy ảo thay vì phải mua nhiều máy tính mới để kiểm tra.

1.2.2 Hệ điều hành Windows

1.2.2.1 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. MS-DOS không tích hợp giao diện người dùng đồ họa và hoạt

động qua các câu lệnh như trong Hình 1-1. Hệ điều hành này đã rất phổ biến từ năm 1981 đến năm 1999.

```
C:\DOS>chkdsk c:

Volume DOS622      created 08-22-2011 3:45p
Volume Serial Number is 1228-1708

 535,396,352 bytes total disk space
 155,648 bytes in 3 hidden files
   8,192 bytes in 1 directories
 3,178,496 bytes in 82 user files
532,854,816 bytes available on disk

   8,192 bytes in each allocation unit
 65,356 total allocation units on disk
64,948 available allocation units on disk

655,360 total bytes memory
624,688 bytes free

Instead of using CHKDSK, try using SCANDISK.  SCANDISK can reliably detect
and fix a much wider range of disk problems.  For more information,
type HELP SCANDISK from the command prompt.

C:\DOS>_
```

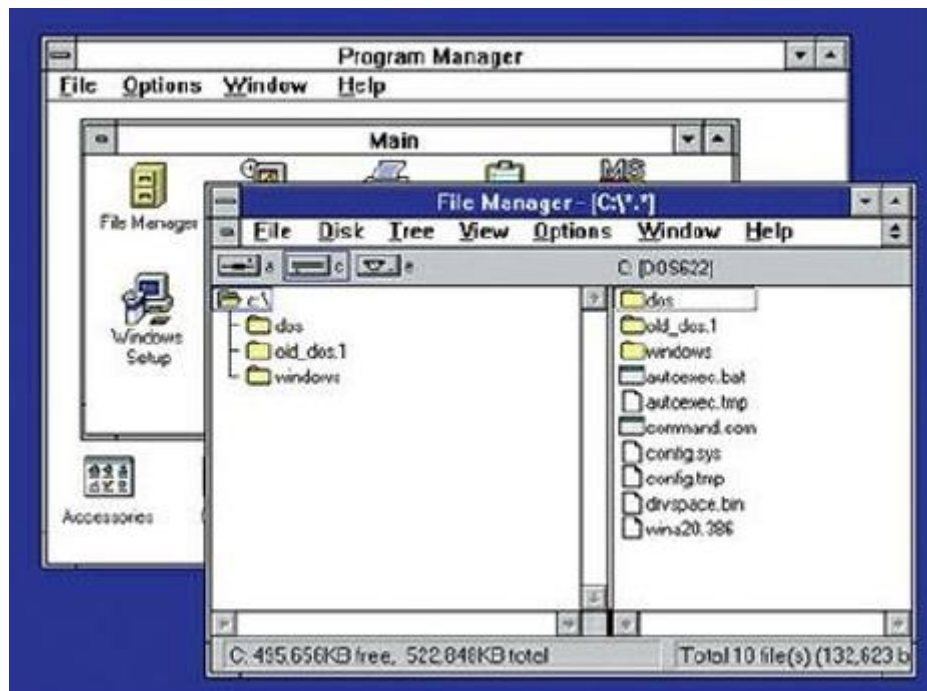
Hình 1 - Giao diện dòng lệnh của MS-DOS

Cấu hình máy tính tiêu biểu cho hệ điều hành này là bộ xử lý tốc độ cỡ khoảng 10-40Mhz, bộ nhớ chính 1MB, màn hình độ phân giải 640x480 điểm ảnh, ổ đĩa mềm dung lượng 1,44MB, và ổ cứng dung lượng cỡ 100MB.

Tuy có nhiều công ty cung cấp giao diện đồ họa như Apple, Xerox, hay IBM song Windows đã thành công hơn tất cả sản phẩm của công ty khác thể hiện qua số lượng các bản được bán ra ngoài thị trường. Việc phổ biến này không có nghĩa là Windows ưu việt hơn các sản phẩm khác mà đơn giản là mọi người sẽ hay bắt gặp sản phẩm này hơn.

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 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 – ProgramManager. Chương trình đặc biệt này cho phép nhóm các chương trình lại và dùng biểu tượng đại diện cho chương trình. Rất nhiều các khái niệm của Windows 3.1 đã được sử dụng cho đến các hệ điều hành ngày nay. Windows 3.1 và hệ thống tương tự vẫn dựa trên DOS để hoạt động.

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. Windows NT được thiết kế lại và là hệ điều hành mạng, chạy trên nền 32 bit song sử dụng GUI như Windows 3.1. Hệ điều hành mới mạnh hơn và sử dụng các nhân và phần nạp khởi động riêng chứ không dựa trên DOS. Windows NT hướng tới môi trường làm việc cộng tác và tính toán hiệu năng cao. Các hệ thống Windows sau này vẫn dựa trên kiến trúc của Windows NT.



Hình 2 - Giao diện menu và đồ họa Windows 3.1

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. Một trong những tính năng quan trọng đó là thư mục động (*Active Directory*) dựa trên các chuẩn công nghiệp về tên miền, giao thức truy nhập thư mục và xác thực để kết nối và chia sẻ dữ liệu giữa các máy tính với nhau. Dịch vụ đầu cuối (Terminal Service) cho phép kết nối từ xa được tích hợp và mở rộng cho tất cả các phiên bản dùng cho máy chủ.

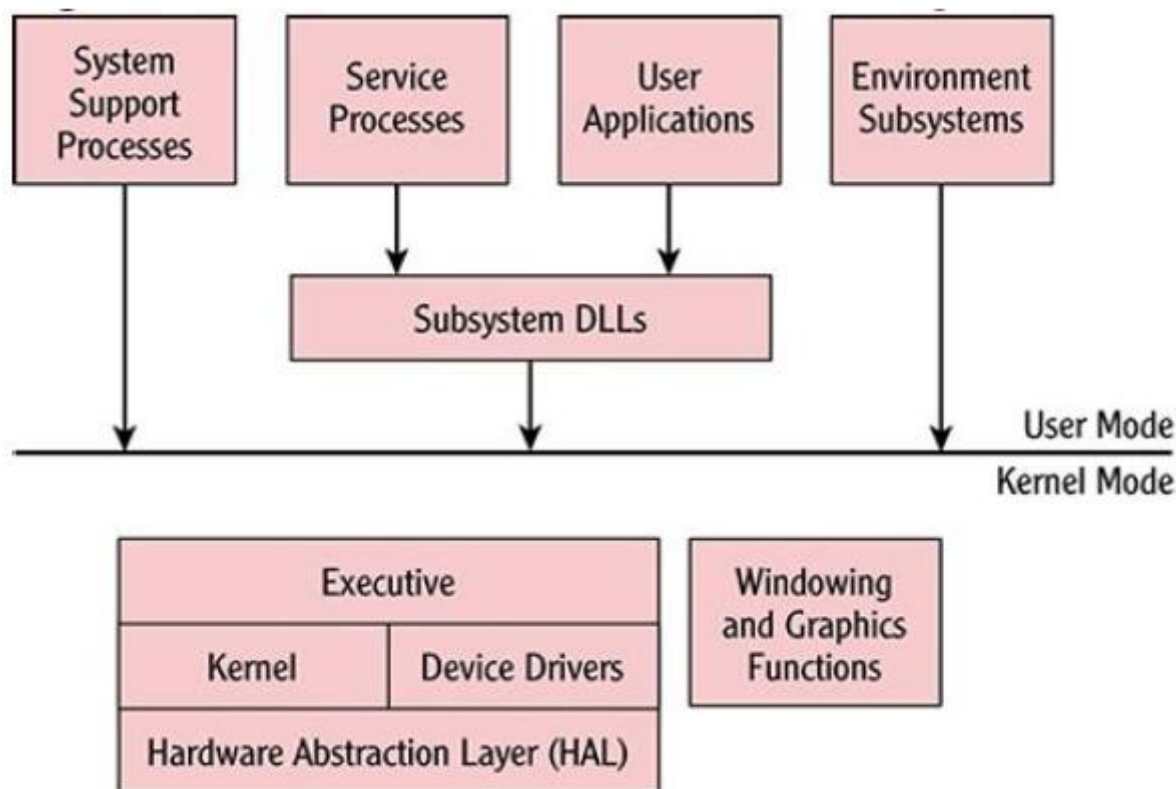
Vào năm 2001, Microsoft kết hợp các dòng sản phẩm Windows NT/2000 (dành cho đối tượng công ty và doanh nghiệp) và Windows 95/98/Me (người quản trị thông thường) tạo nên Windows XP. Kể từ phiên bản này các sản phẩm của Microsoft cần phải qua thủ tục kích hoạt để được sử dụng hợp lệ. Đây có lẽ là một trong những phiên bản Windows tốt nhất và là hệ thống chạy lâu nhất (gần 13 năm tính từ lúc ra đời) cho dù ban đầu hệ thống có nhiều vấn đề về tính an toàn và hiệu năng. 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. 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. Phiên bản nâng cấp Server 2003 R2 hỗ trợ tính toán 64 bit và các công cụ quản lý tập trung, các chức năng ảo hóa. Các phiên bản 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*).

1.2.2.2 Kiến trúc của 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 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.

Kiến trúc của Windows rất giống với các hệ điều hành khác như Linux hay Mac OS. 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.

1.2.2.3 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.

- 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*) 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.

- 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 có nhiều câu lệnh DOS vẫn còn dùng được và 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. Thực tế, Microsoft hỗ trợ tập các lệnh trong môi trường PowerShell được gọi là *cmdlet* để thực hiện các tác vụ quản trị mong muốn.

Một trong những tính năng quan trọng của PowerShell là khả năng lập trình đơn giản (*scripting*). Với các hàm logic 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.

1.2.2.4 Hệ thống File 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.

Bảng cấp phát chứa mảng các mô tả khối cấp phát. Mỗi phần tử trong mảng này tương ứng với một phần tử cấp phát. Số thứ tự của phần tử mảng giúp tương ứng với vị trí của khối cấp phát trong không gian lưu trữ. Giá trị không của phần tử trong mảng cho biết khối cấp phát tương ứng chưa được sử dụng. Giá trị khác không cho biết vị trí của phần tử mảng cũng chính là khối lưu trữ kế tiếp.

Trong hệ thống file FAT gồm có FAT12, FAT16 và FAT32 tương ứng với của số lượng tối đa các khối cấp phát là 2^{12} , 2^{16} và 2^{32} . Đến nay hệ thống FAT chủ yếu dùng cho các thiết bị lưu trữ ngoài như thẻ nhớ hay USB.

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.

Bảng dưới đây cho thấy khả năng của từng hệ thống file.

Bảng 1. Tương quan các hệ thống file Windows

	FAT16	FAT32	NTFS
Tương thích	DOS, Windows	Windows 95 và mới hơn	Windows NT 4.0 và mới hơn
Kích cỡ	4GB	32GB	2TB hay lớn hơn
Số file	~65.000	~4.000.000	~4.000.000.000

Kích cỡ file tối đa	4GB	4GB	16TB
---------------------	-----	-----	------

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

1.2.3.1 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.

Một số phần mềm diệt virus phổ biến: Windows Defender, Kaspersky Antivirus, Avast Antivirus, AVG Antivirus, ...

1.2.3.2 Phần mềm chống phần mềm gián điệp

Phần mềm chống phần mềm gián điệp là chương trình được thiết kế để phát hiện, ngăn chặn và loại bỏ phần mềm gián điệp - những phần mềm có thể thu thập dữ liệu cá nhân, theo dõi hoạt động người dùng hoặc chiếm quyền điều khiển thiết bị mà không được sự cho phép.

Một số phần mềm chống phần mềm gián điệp phổ biến: Malwarebytes Anti – Malware, Spybot – Search & Destroy, SuperAntiSpyware, Window Defender, ...

1.2.3.3 Phần mềm cứu hộ

Phần mềm cứu hộ là các công cụ được thiết kế để khôi phục hệ thống, sửa lỗi phần mềm, cứu dữ liệu hoặc diệt virus khi hệ điều hành không thể hoạt động bình thường. Những phần mềm này thường được khởi động từ USB boot, CD/DVD hoặc môi trường bên ngoài để khắc phục sự cố mà hệ điều hành không thể tự sửa chữa.

Một số phần mềm cứu hộ phổ biến: Kaspersky Rescue Disk, DLC Boot, Hiren's BootCD, ...

CHƯƠNG 2. NỘI DUNG THỰC HÀNH



2.1 Chuẩn bị môi trường

- File cài đặt Windows 7/8/10/11 định dạng iso.
- Phần mềm ảo hóa: VMWare Workstation.

2.2 Các bước thực hiện

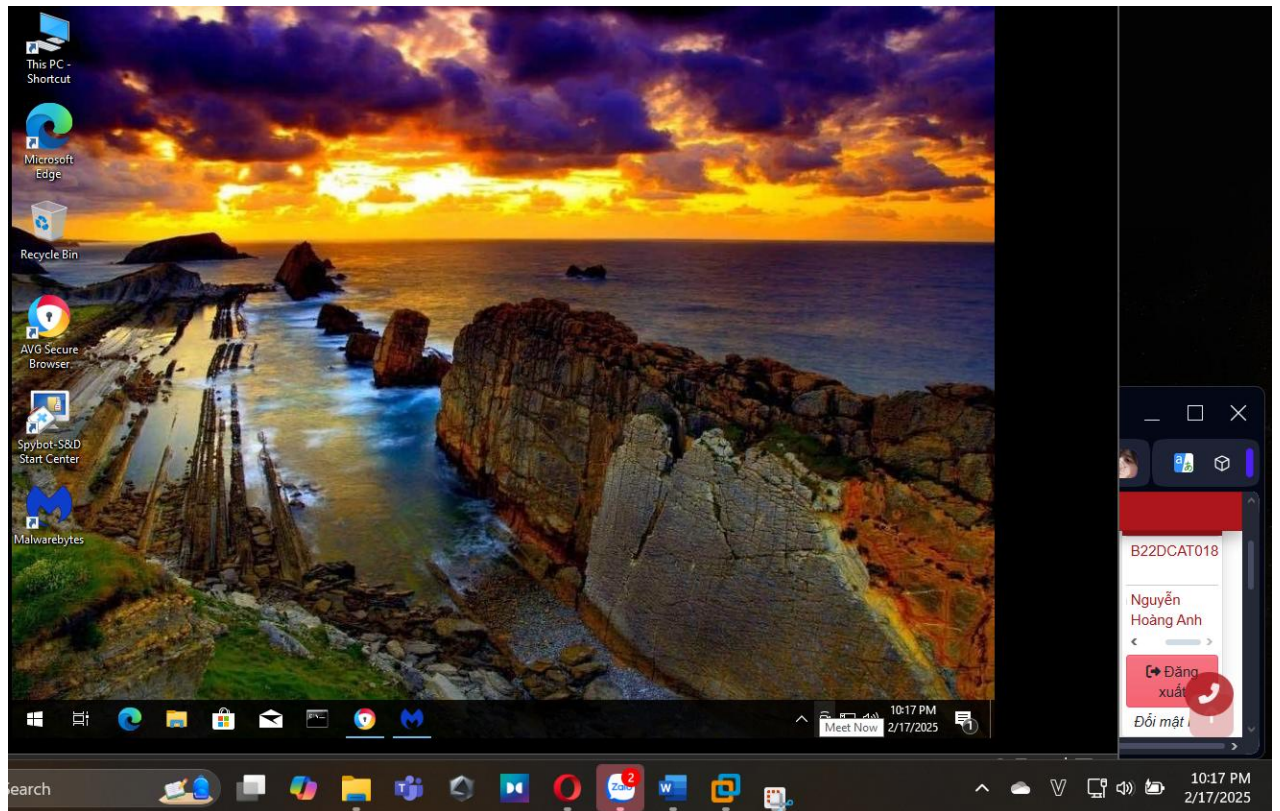
2.2.1 Cài đặt Windows

Chuẩn bị file cài đặt Windows 10 định dạng iso:

 MediaCreationTool_22H2.exe	2/13/2025 1:58 PM	Application	19,008 KB
 Windows.iso	2/13/2025 2:03 PM	Disc Image File	4,779,200 ...

Hình 4 - File Windows 10 định dạng iso

Cài đặt thành công máy ảo Windows 10:

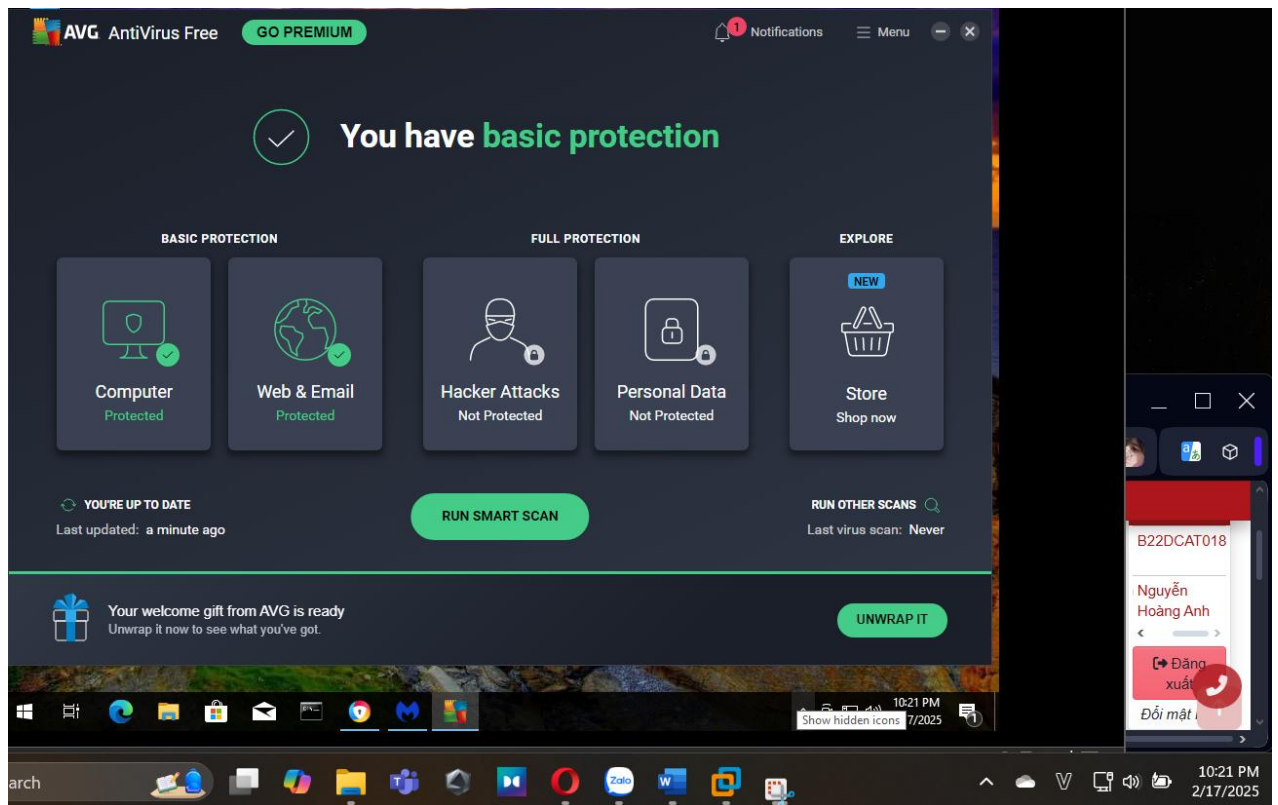


Hình 5 - Màn hình máy ảo Windows 10

2.2.2 Cài đặt phần mềm diệt virus

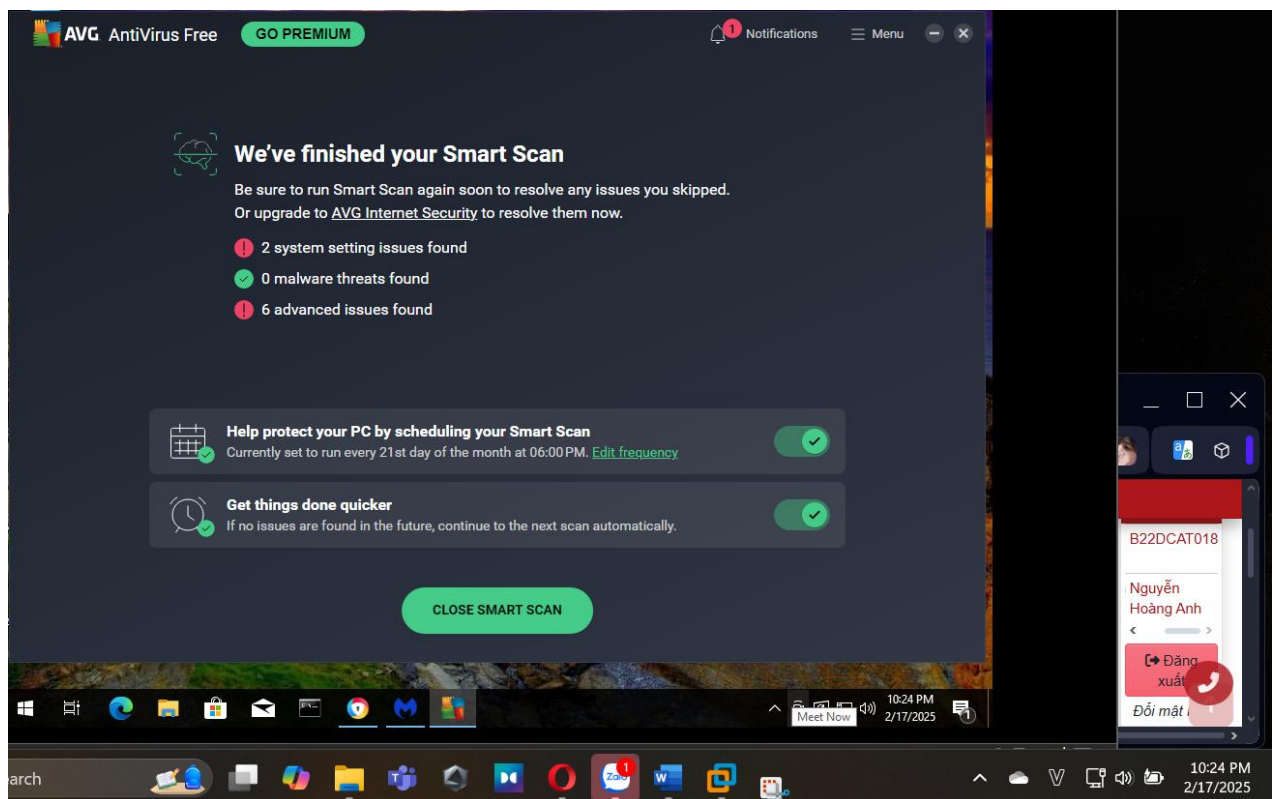
2.2.2.1 Phần mềm diệt virut AVG AntiVirus

Cài đặt thành công phần mềm:



Hình 6 - Cài đặt thành công phần mềm AVG AntiVirus

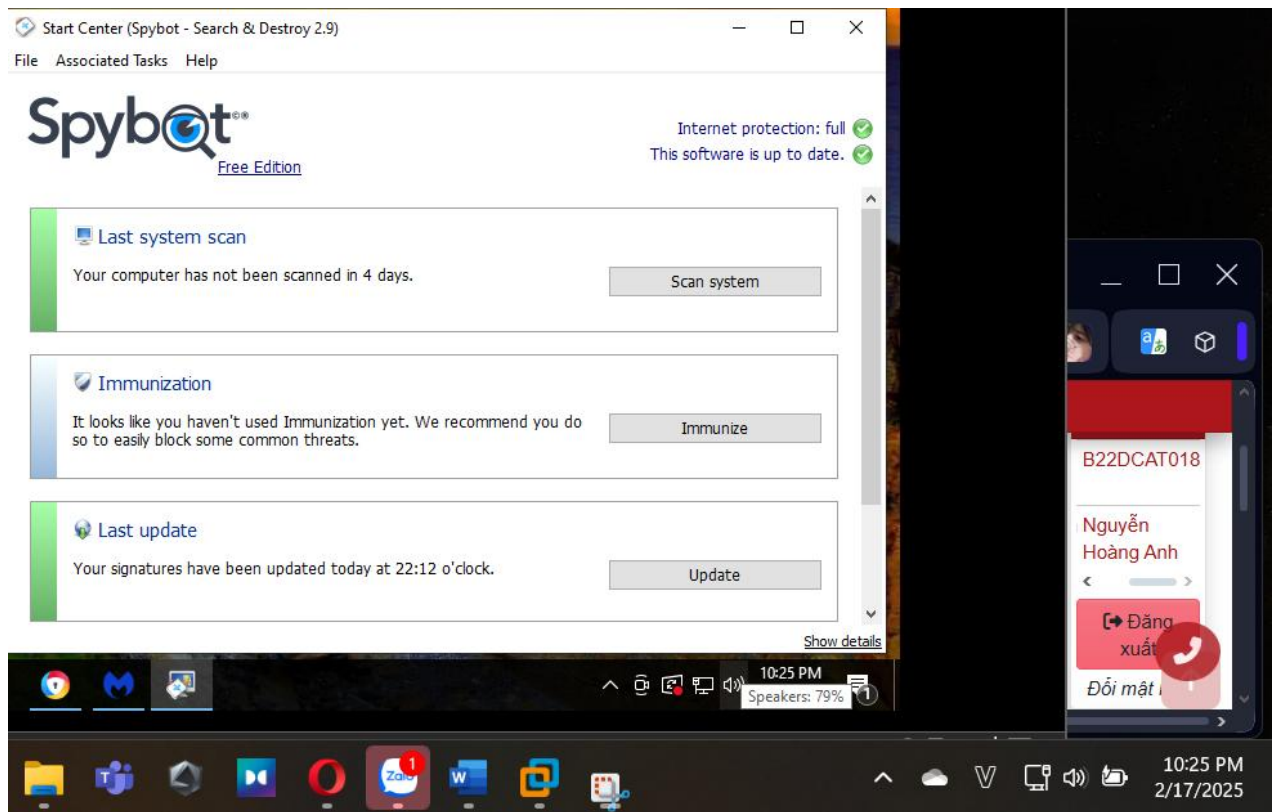
Chạy phần mềm AVG AntiVirus thành công:



Hình 7 - Quét máy tính thành công với phần mềm AVG AntiVirus

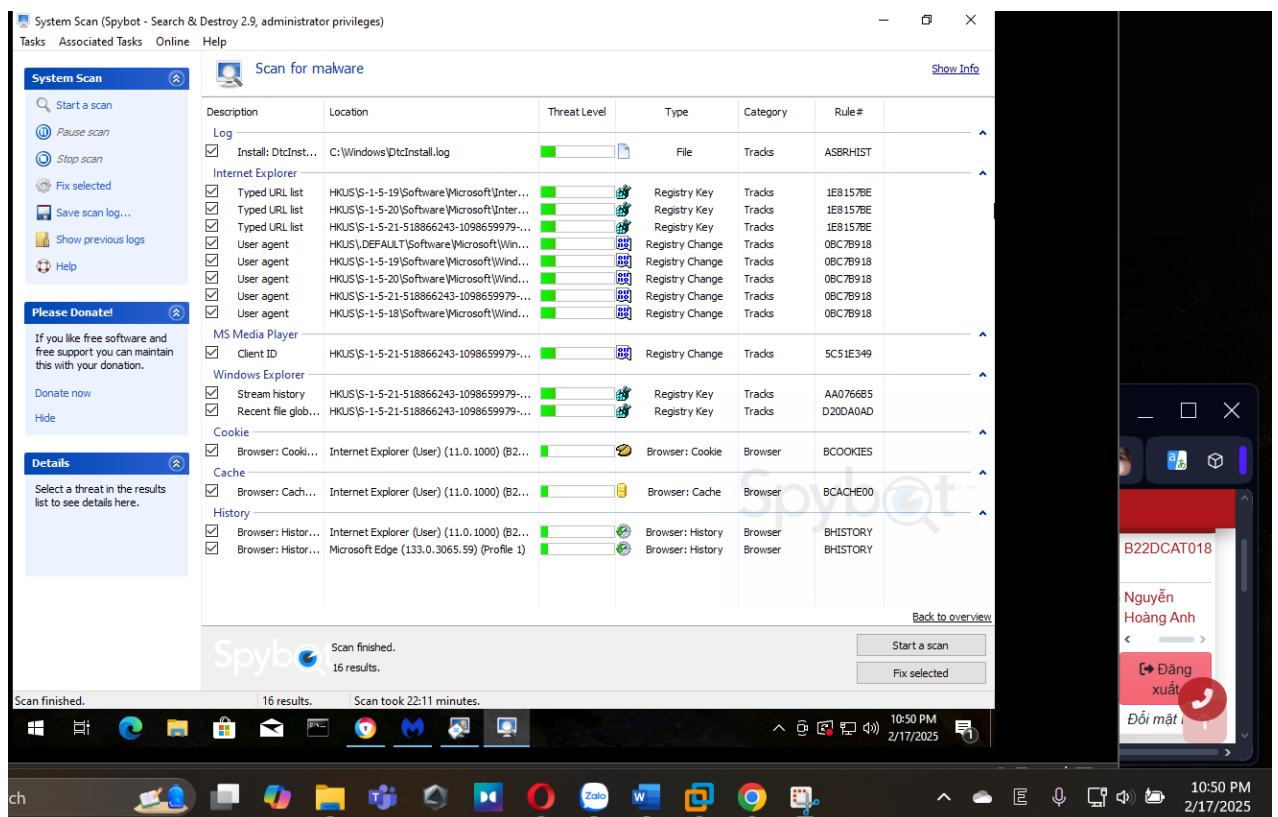
2.2.2.2 Phần mềm chống phần mềm gián điệp Spybot S&D

Cài đặt thành công Spybot S&D



Hình 8 - Cài đặt thành công Spybot S&D

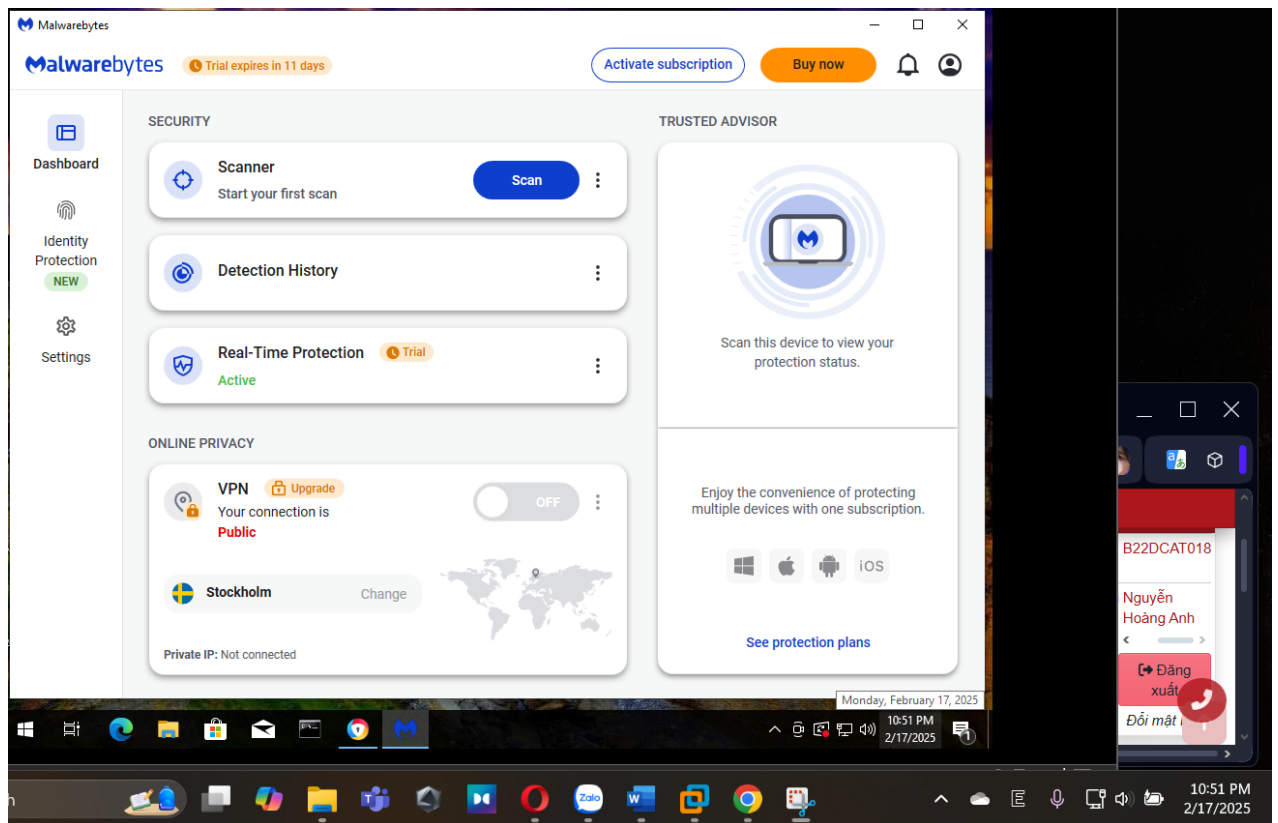
Quét máy bằng phần mềm Spybot S&D:



Hình 9 - Quét máy bằng Spybot S&D

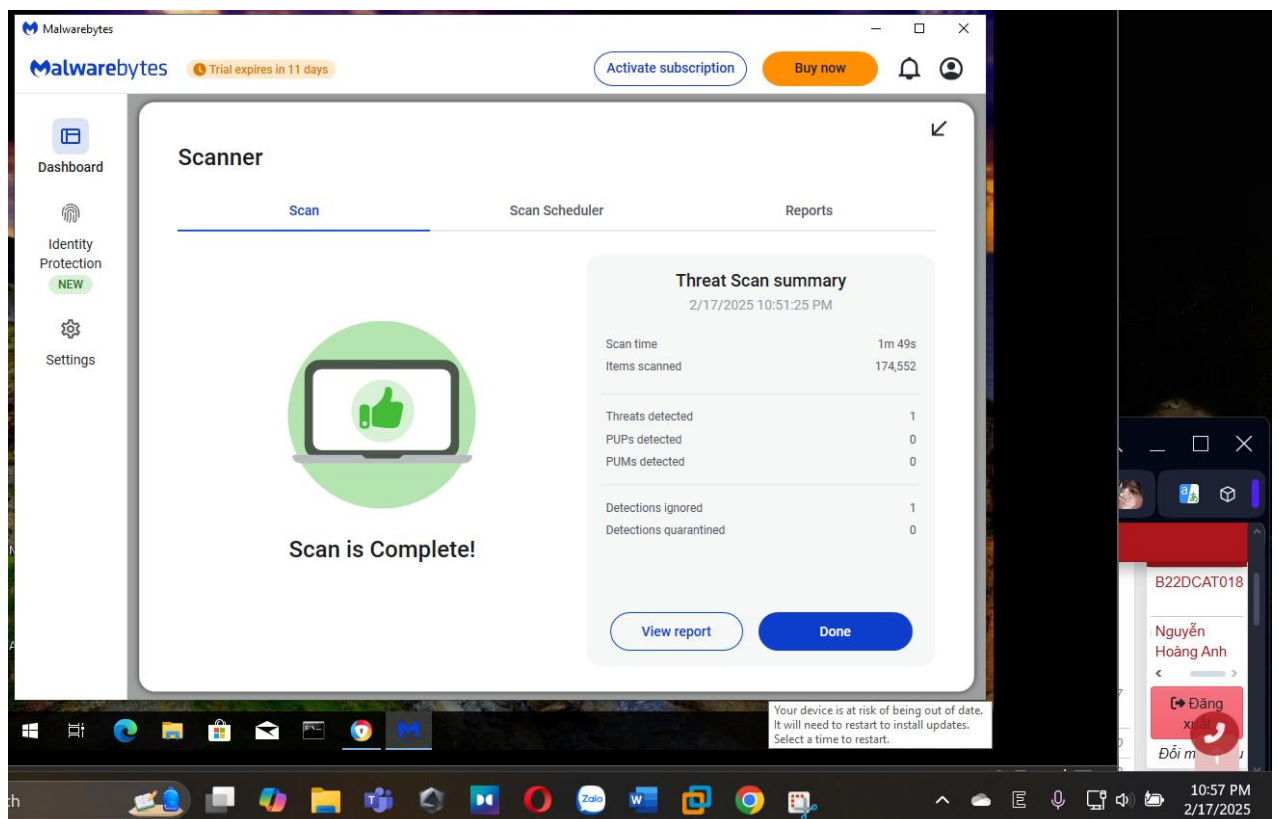
2.2.2.3 Phần mềm chống các phần mềm độc hại Malwarebytes Anti-Malware

Cài đặt thành công phần mềm Malwarebytes Anti-Malware:



Hình 10 - Cài đặt thành công Malwarebytes Anti-Malware

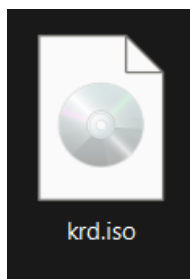
Quét máy tính thành công với Malwarebytes Anti-Malware:



Hình 11 - Quét máy tính bằng Malwarebytes Anti-Malware

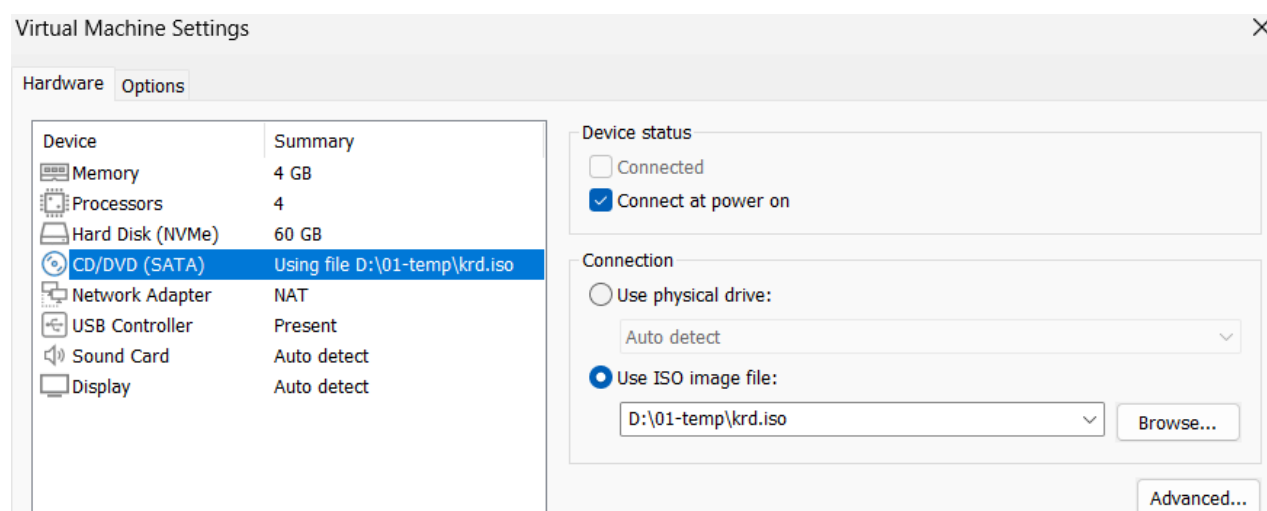
2.2.2.3 Phần mềm cứu hộ Kaspersky Rescue Disk (KRD)

Tải file iso của Kaspersky Rescue Disk:



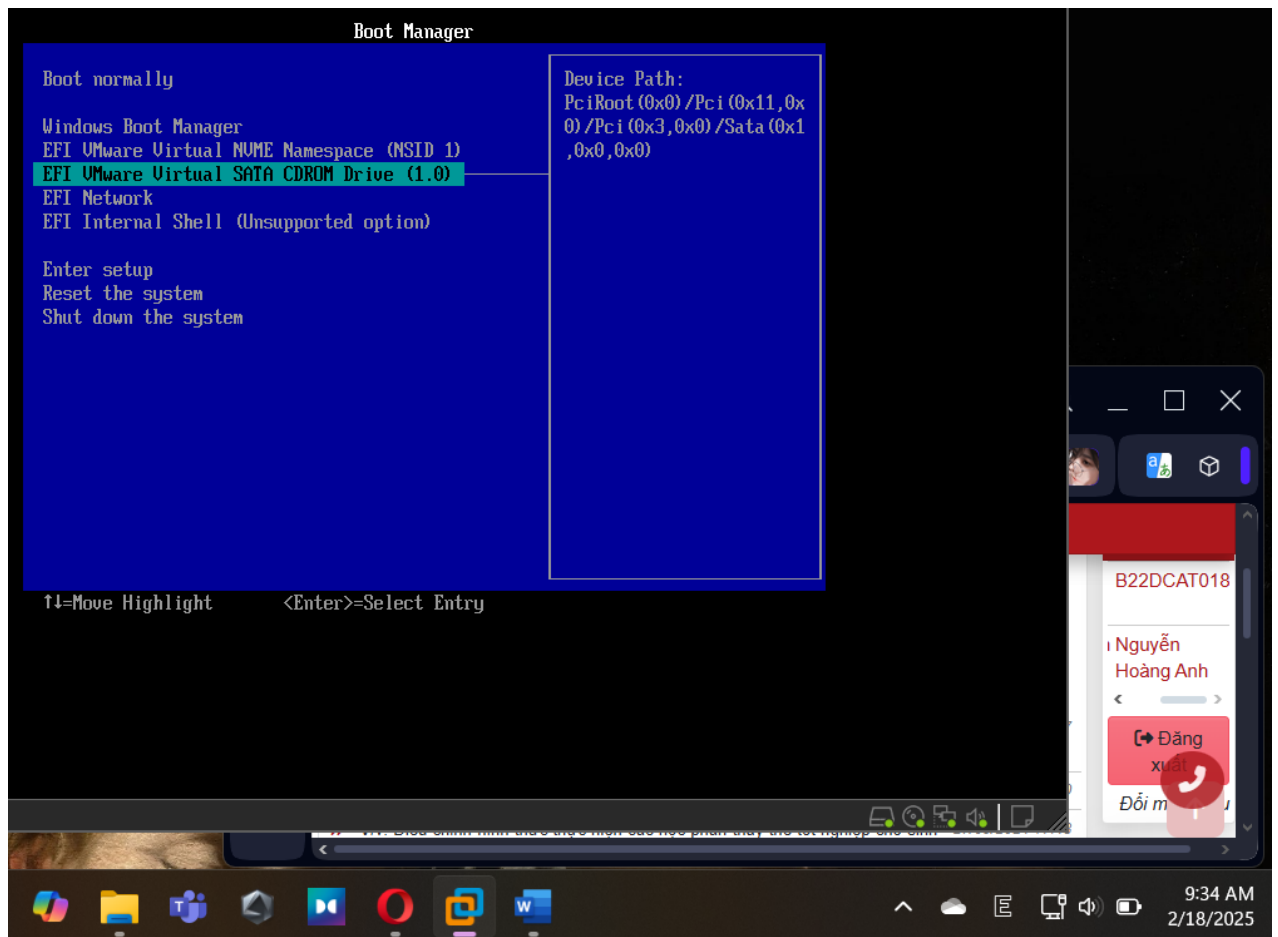
Hình 12 - File định dạng iso của KRD

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



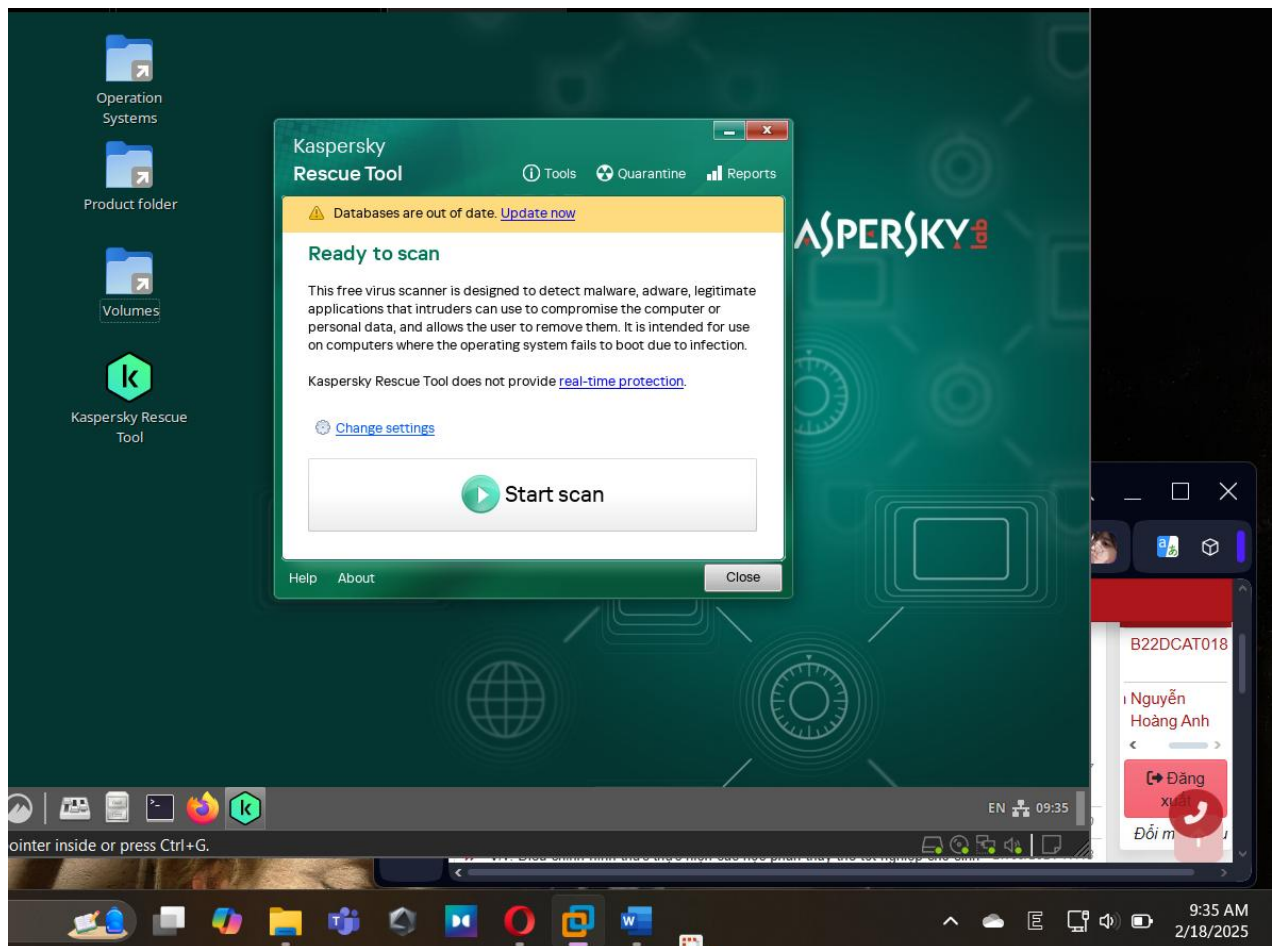
Hình 13 - Load vào mục CD/DVD của máy ảo

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



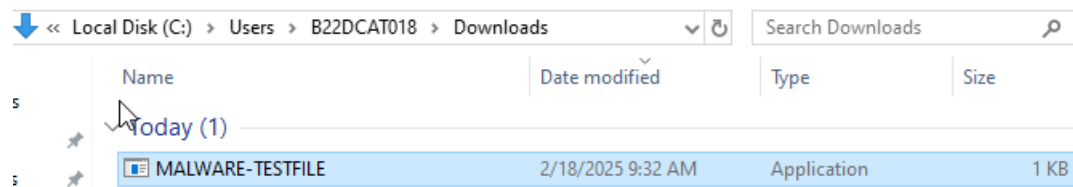
Hình 14 - Ấn esc để vào boot manager

Giao diện Kaspersky Rescue Disk:



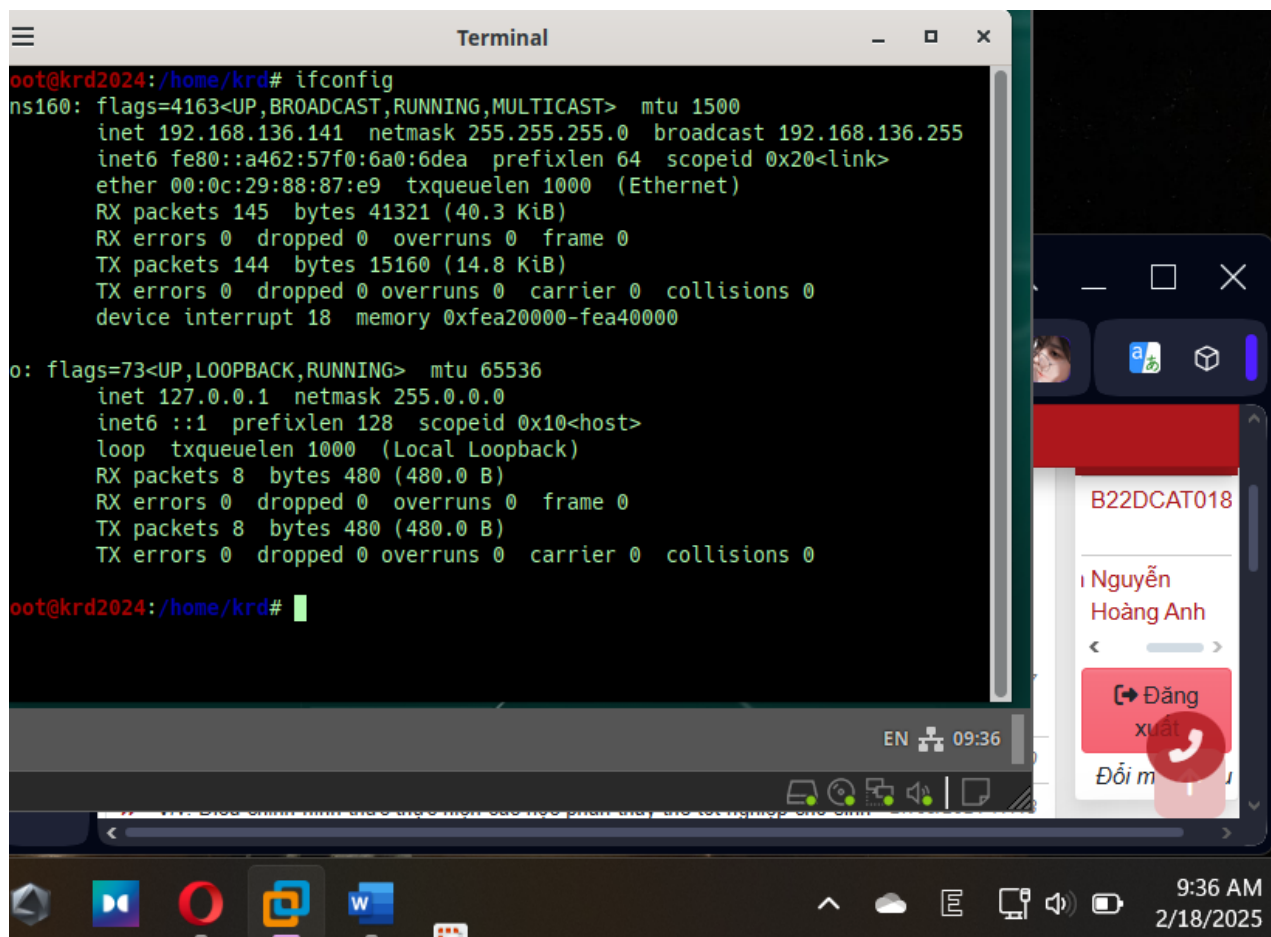
Hình 15 - Giao diện KRD

File mã độc tải từ đường link của đề bài, lưu file mã độc vào ổ C:



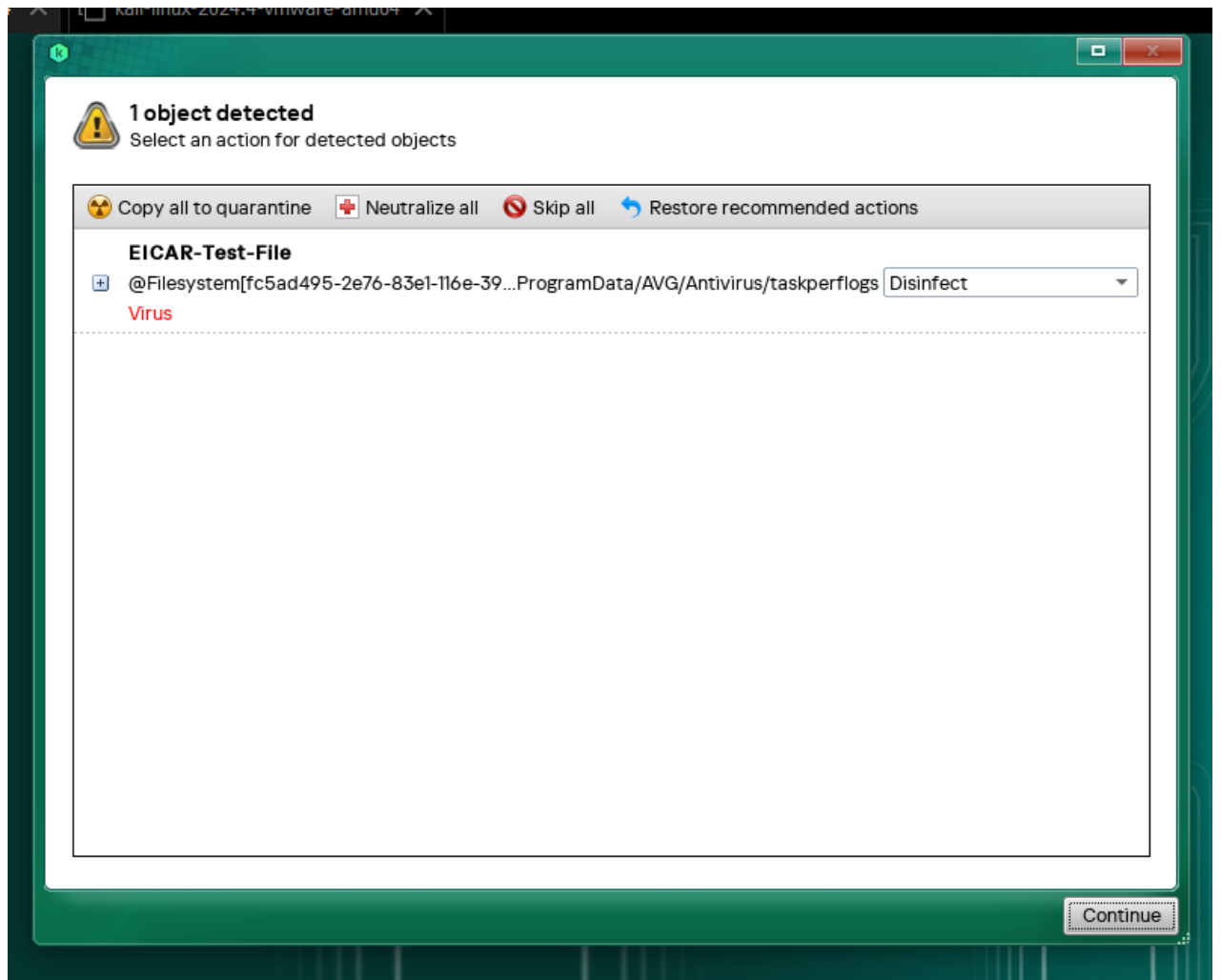
Hình 16 - File mã độc

Kiểm tra ip máy trạm bằng lệnh: *ifconfig*:



Hình 17 - Kiểm tra ip

Chạy Kaspersky Rescue Tool để quét, phát hiện mã độc và xóa bỏ nó:



Hình 18 - Quét phát hiện mã độc thành công

TỔNG KẾT

Trong bài học này, em đã được tìm hiểu về phần mềm ảo hoá VMWARE, hệ điều hành Windows, các phần mềm diệt virus AVG Antivirus, phần mềm chống phần mềm gián điệp Malwarebytes Anti – Malware, phần mềm cứu hộ Kaspersky Rescue Disk và thực hành cài đặt máy ảo Windows 10 trên VMWARE, cài đặt các phần mềm trên và thực hiện loại bỏ file nhiễm virus khỏi máy bằng Kaspersky Rescue Disk mà không cần khởi động vào hệ điều hành chính.

Qua bài báo cáo đã giúp em hiểu rõ hơn về hệ điều hành Windows và tầm quan trọng của các phần mềm bảo mật. Thông qua việc nghiên cứu lý thuyết và thực hành, em có thể áp dụng những kiến thức này vào thực tế, góp phần nâng cao khả năng bảo vệ hệ thống và dữ liệu cá nhân khỏi các mối đe dọa trên không gian mạng.

```
C:\Users\B22DCAT018>whoami
nguyenhoanganh-\b22dcat018

C:\Users\B22DCAT018>time
The current time is: 21:10:57.64
Enter the new time:

C:\Users\B22DCAT018>date
The current date is: Fri 02/14/2025
Enter the new date: (mm-dd-yy)

C:\Users\B22DCAT018>echo Nguyen Hoang Anh-B22DCAT018
Nguyen Hoang Anh-B22DCAT018

C:\Users\B22DCAT018>_
```

Hình 19 - Thông tin sinh viên thực hiện

TÀI LIỆU THAM KHẢO

- [1] Đinh Trường Duy, Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022.
- [2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.