

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 WINDOW

Giáo viên: Nguyễn Hoa Cương

Sinh viên: Nguyễn Huy Quang

Mã Sinh Viên: B20DCAT144

Khóa: D20

Hệ: Chính Quy

Hà Nội – 2023

Nội dung lý thuyết:

- **Tìm hiểu về phần mềm VMWare Workstation:**

- VMWare Workstation là một chương trình quản lý máy ảo được phát triển bởi một nhánh nhỏ của Dell technology là công ty VMWare được ra mắt lần đầu vào năm 1999
- Chương trình này cho phép người dùng thiết lập và cấu hình nhiều máy ảo trên cùng một thiết bị vật lý. Các máy ảo này có thể chạy độc lập và sử dụng các hệ điều hành khác nhau

- **Hệ điều hành Windows**

Lịch sử phát triển

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. MS-DOS không tích hợp giao diện người dùng đồ họa (GUI*) và hoạt động qua các câu lệnh. Hệ điều hành này đã rất phổ biến từ năm 1981 đến 1999.

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. 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. Hệ điều hành mới mạnh hơn và sử dụng các nhân và phần nạp khởi động riêng chứ không dựa trên DOS. Các hệ thống Windows sau này vẫn dựa trên kiến trúc của Windows NT.

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.

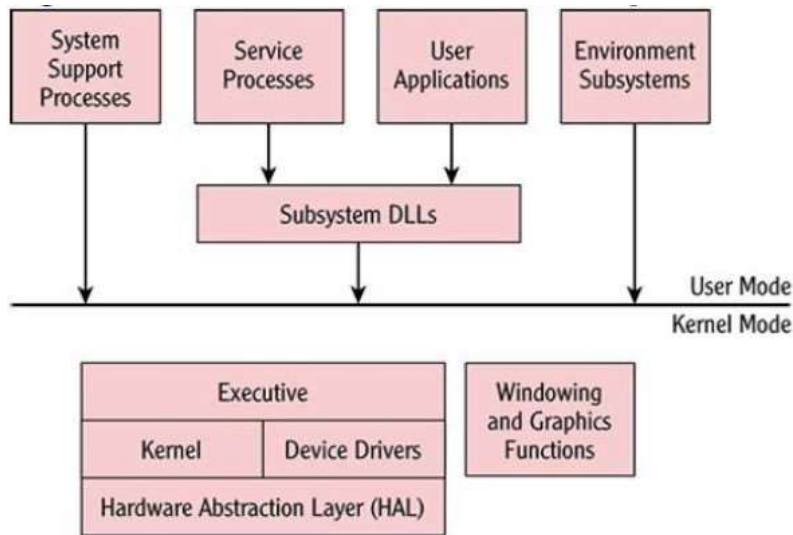
Vào năm 2001, Microsoft kết hợp các dòng sản phẩm Windows NT/2000 (dành cho đối tượng công ty và doanh nghiệp) và Windows 95/98/Me (người quản trị thông thường) tạo nên Windows XP.

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.

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 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



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 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.

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*).

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 dung được và được kích hoạt thông qua chương trình *cmd.exe*

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 lô-gíc 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.

Đặc điểm , đặc trưng

Hệ điều hành Windows có giao diện thân thiện, đơn giản. Nó tương tác với người dùng thông qua các dòng lệnh. Với các phiên bản hệ điều hành Windows mới nhất hiện nay thì giao diện đã có phần cải thiện theo hướng tương tác người dùng đồ họa.

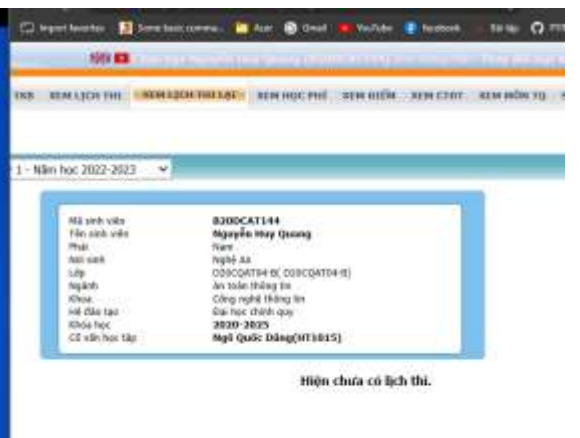
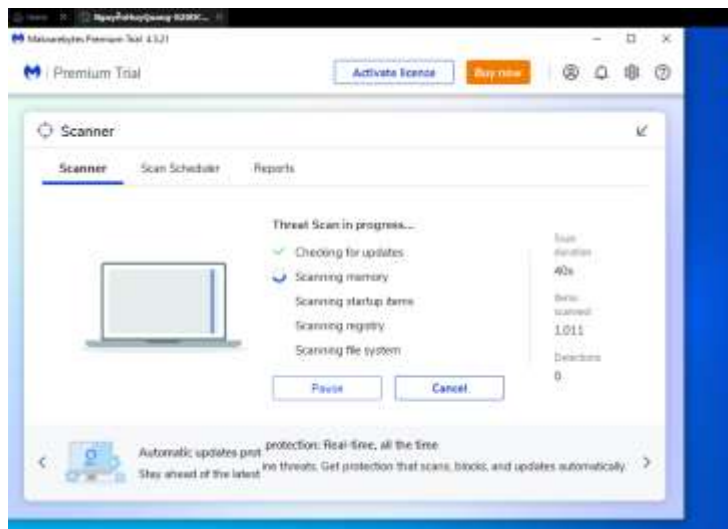
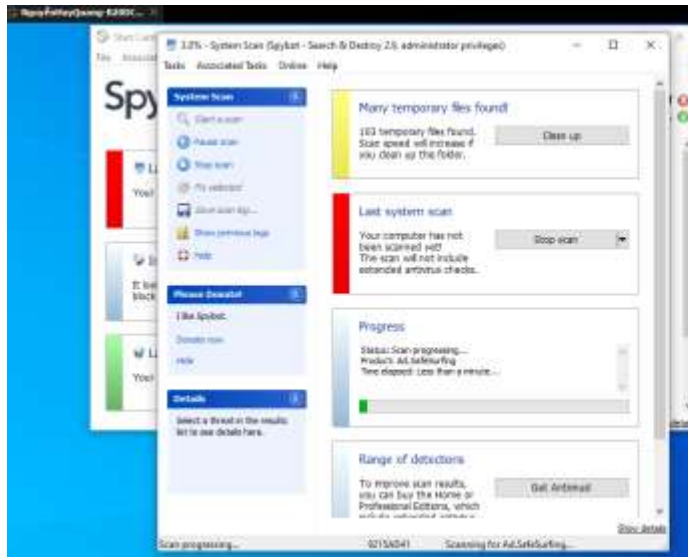
Hệ điều hành Windows rất phổ biến và có khả năng tương thích cao: Vốn là một nền tảng chiếm thị phần sử dụng cao nhất hiện nay nên cũng không có gì khó hiểu khi hầu hết các nhà sản xuất đều đầu tư xây dựng phần mềm cũng như sản xuất phần cứng hỗ trợ cho hệ điều hành Windows.

Dễ sử dụng: Dù cho ra đời nhiều phiên bản nhưng các phiên bản sau luôn có tính kế thừa các phiên bản tiền nhiệm, nên người dùng dễ làm quen khi sử dụng lần đầu.

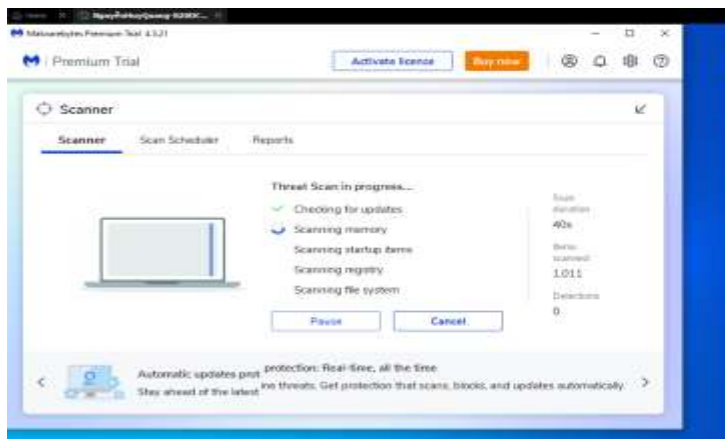
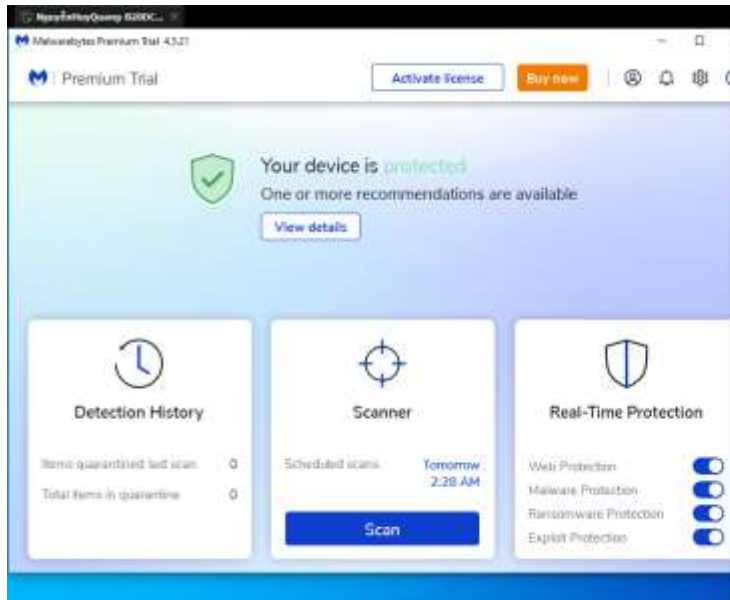
Bảo mật: Nếu so về khả năng bảo mật toàn diện thì Windows vẫn chưa được đánh giá cao bằng các hệ điều hành Linux, Mac OS. Tuy nhiên, nhà phát triển Microsoft luôn có những gói nâng cấp và miễn phí cập nhật, nhằm có thể vá các lỗ hổng bảo mật. Điều này giúp đảm bảo tính ổn định tối ưu cho thiết bị.

Phong phú ứng dụng: Bởi hầu hết các ứng dụng đều viết dựa trên nền tảng tương thích với hệ điều hành Windows, nên ứng dụng của nó phong phú hơn so với các hệ điều hành khác.

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



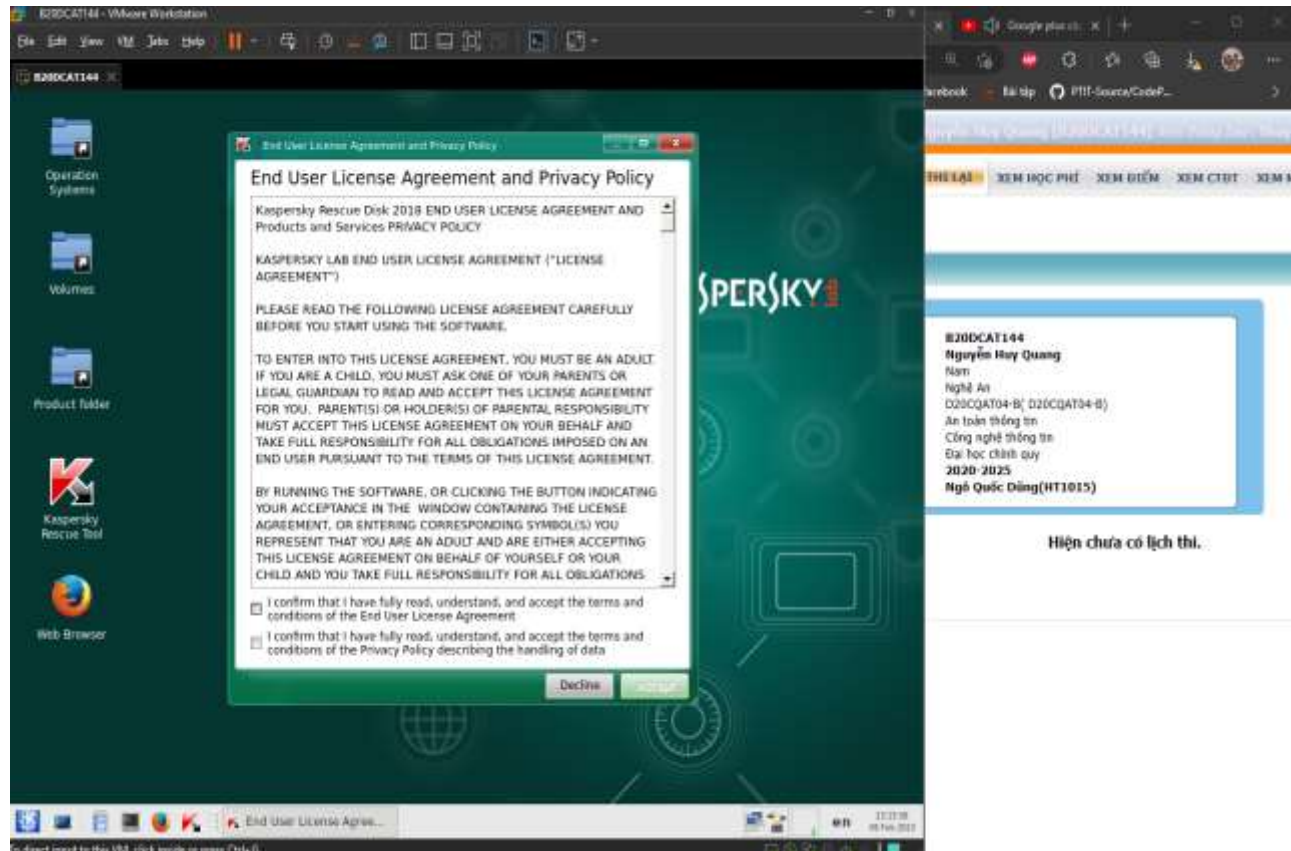
3. Phần mềm chống các phần mềm độc hại: Malwarebytes Anti-Malware



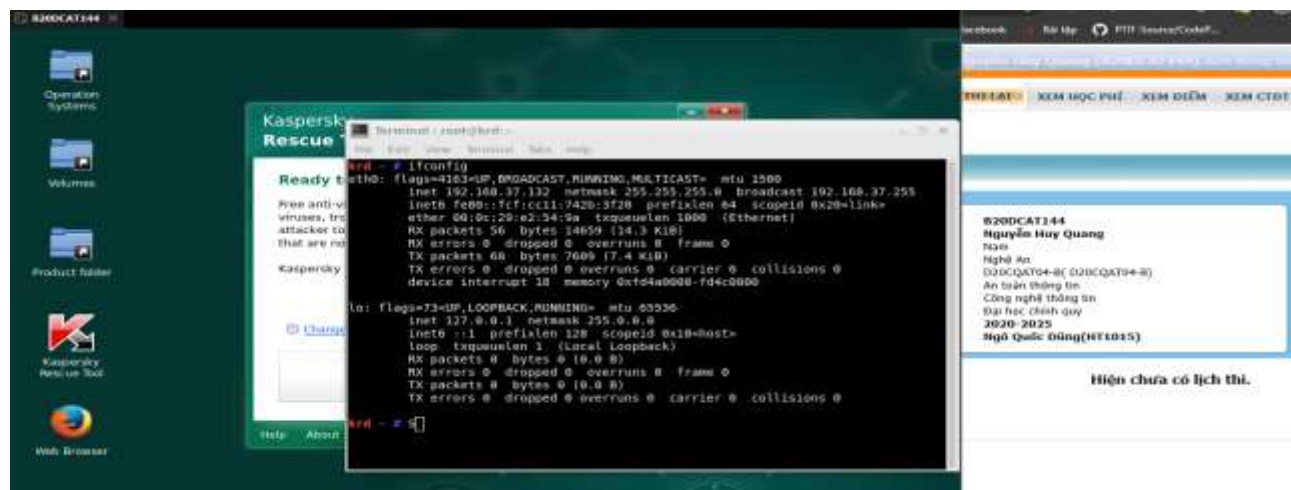
4. Phần mềm cứu hộ: Kaspersky Rescue Disk (KRD)

a) Khởi động KRD bằng CD-ROM trong máy ảo bằng cách ấn ESC và chọn CD-ROM Drive:





b) Sử dụng câu lệnh `ifconfig` để kiểm tra id máy trạm:



c) Tải file mã độc **MALWARE-TESTFILE.exe** trên trang: computersecuritystudent.com và lưu vào ổ C:

ComputerSecurityStudent (CSS)

HOME | UNIX | WINDOWS | SECURITY TOOLS | FORENSICS | SHOPPING | GET STARTED | CONTACT US

Views: 19027924

Cyber Security Martial Arts Framework




Hac-King-Do Training

Join Now

Login

Affiliations



Black Belt Training Certification in Hac-King-Do

By continuing to use this website you agree with the [Payment Terms](#), [Legal Agreement](#), [Privacy Policy](#), and [Cookie Policy](#)

Recent Lab Posts

Date	Title
2020-12-09	Kali: Lesson 5: Fix bignum too big to convert into 'long' (RangeError)
2017-03-04	Kali: Rolling Edition: Lesson 1: Installing Kali Rolling Edition
2016-10-11	Buffer Overflow: Lesson 2: Create PCMan Metasploit Module, Attack, and Capture Memory
2016-09-11	Buffer Overflow: Lesson 1: PCMan's FTP Server 2.0.7 Buffer Overflow Explained
2016-09-10	Damn Vulnerable Windows XP: Lesson 9: How to setup the PCMan's FTP Server 2.0.7 Buffer Overflow
2016-09-08	Student Help: IT-Technical Institutes: Free Cyber Security Dojo Trial Memberships
2012-08-10	Run Winarch's Minidux VB: Lesson 5: How to install GnuPG v1.10 via Sublime

ComputerSecurityStudent (CSS)

HOME | UNIX | WINDOWS | SECURITY TOOLS | FORENSICS | SHOPPING | GET STARTED | CONTACT US

Views: 42005

WINDOWS > Windows 7

Date Topic Name

2012-10-06	Windows 7: Lesson 1: Installing Windows 7
2012-10-09	Windows 7: Lesson 2: Install AVG Antivirus Free 2013
2012-10-15	Windows 7: Lesson 3: Install Spybot - Search and Destroy
2012-10-22	Windows 7: Lesson 4: Install and Set Config Firewall Against BackTrack
2012-10-24	Windows 7: Lesson 5: Download and Run BitDefender Rescue CD (Antivirus Scan)
2012-10-28	Windows 7: Lesson 6: Download and Run Kaspersky Rescue Disk (Antivirus Scan)
2012-10-29	Windows 7: Lesson 7: Download and Run Avira AntiVir Rescue System
2012-11-01	Windows 7: Lesson 8: How to remove Windows 7 Malware
2012-11-12	Windows 7: Lesson 9: Install and Test Comodo Firewall Against BackTrack
2012-11-27	Windows 7: Lesson 10: Malwarebytes Anti-Malware

http://qkth.pte.edu.vn/Default.aspx?page=webkithuat

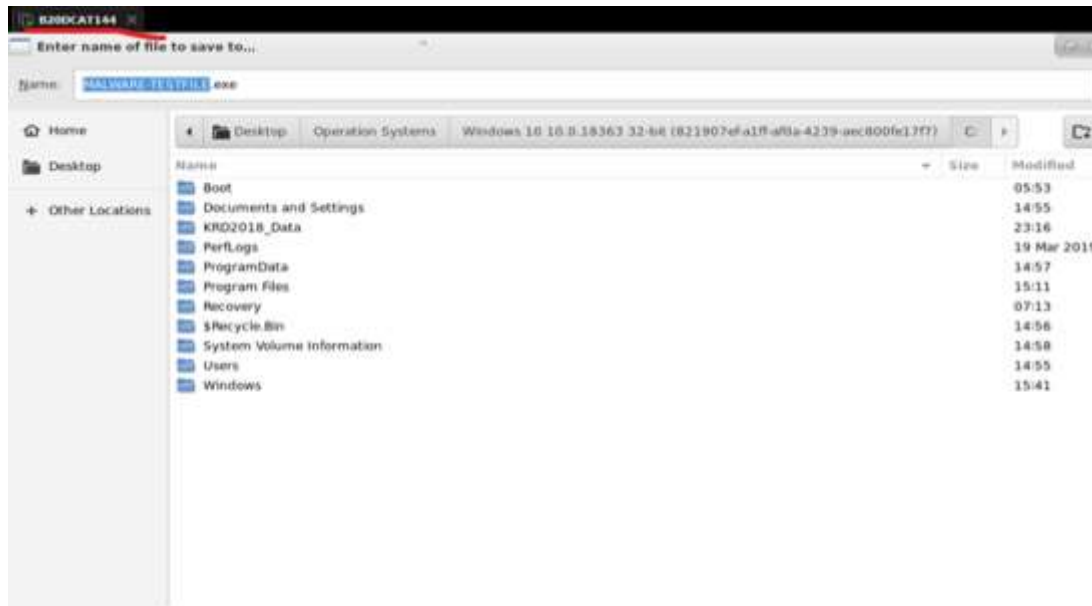
Report back to: Some basic course... | Acer | Gmail | YouTube | Download

THỜI | KINH LỊCH THỜI | KINH LỊCH THỜI LẠC | KINH HỌC PHÍ | KINH QUẢN | KINH CỐT

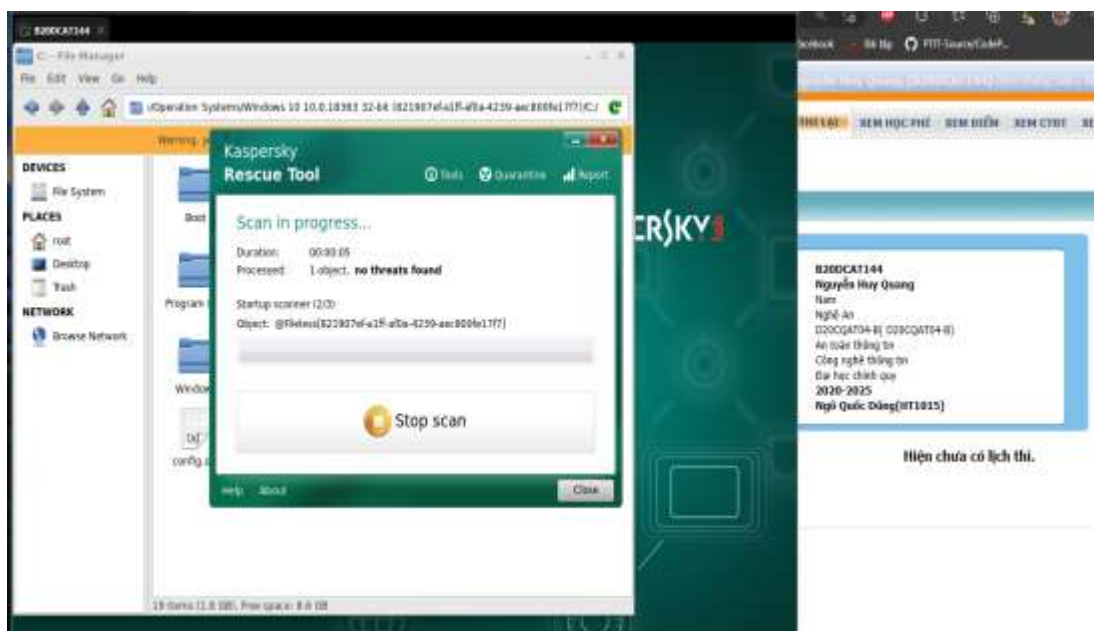
1 - Năm học 2022-2023

Hồ sơ viên	B26DCAT144
Tên sinh viên	Nguyễn Huy Quang
Phái	Nam
Nơi sinh	Nghệ An
Lớp	D26CQAT04-B / D26CQAT04-B
Ngành	An toàn thông tin
Khoa	Công nghệ thông tin
Hệ đào tạo	Đại học chính quy
Khóa học	2020-2025
Cơ vấn học tập	Ngô Quốc Dũng(NT1805)

Hiện chưa có lịch thi.



d) Chạy quét trong kaspersky scan tìm và xóa file mã độc:



LỊCH THI LẠI

XEM HỌC PHÉ

B20DCAT144

Nguyễn Huy Quang

Nam

Nghệ An

D20CQAT04-B(D20CQAT04-B)

An toàn thông tin

Công nghệ thông tin

Đại học chính quy

2020-2025

Ngo Quốc Dũng(HT1015)

Hiện



B20DCAT144

Nguyễn Huy Quang

Nam

Nghệ An

D20CQAT04-B(D20CQAT04-B)

An toàn thông tin

Công nghệ thông tin

Đại học chính quy

2020-2025

Ngo Quốc Dũng(HT1015)

Hiện chưa



Mã sinh viên

B20DCAT144

Tên sinh viên

Nguyễn Huy Quang

Phái

Nam

Nơi sinh

Nghệ An

Lớp

D20CQAT04-B(D20CQAT04-B)

Ngành

An toàn thông tin

Khoa

Công nghệ thông tin

Hệ đào tạo

Đại học chính quy

Khóa học

2020-2025

Cổ vấn học tập

Ngo Quốc Dũng(HT1015)

Hiện chưa

