

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

---



**BÁO CÁO THỰC HÀNH**

**Bài 1: Cài đặt hệ điều hành máy trạm Windows**

**Họ và tên: Vũ Thành Long**

**Mã sinh viên: B21DCAT012**

**Nhóm: 06**

**Môn học: Thực tập cơ sở**

**Giảng viên giảng dạy: Nguyễn Hoa Cường**

# **Môn học: Thực tập cơ sở**

## **Bài 1: Cài đặt hệ điều hành máy trạm Windows**

### **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.

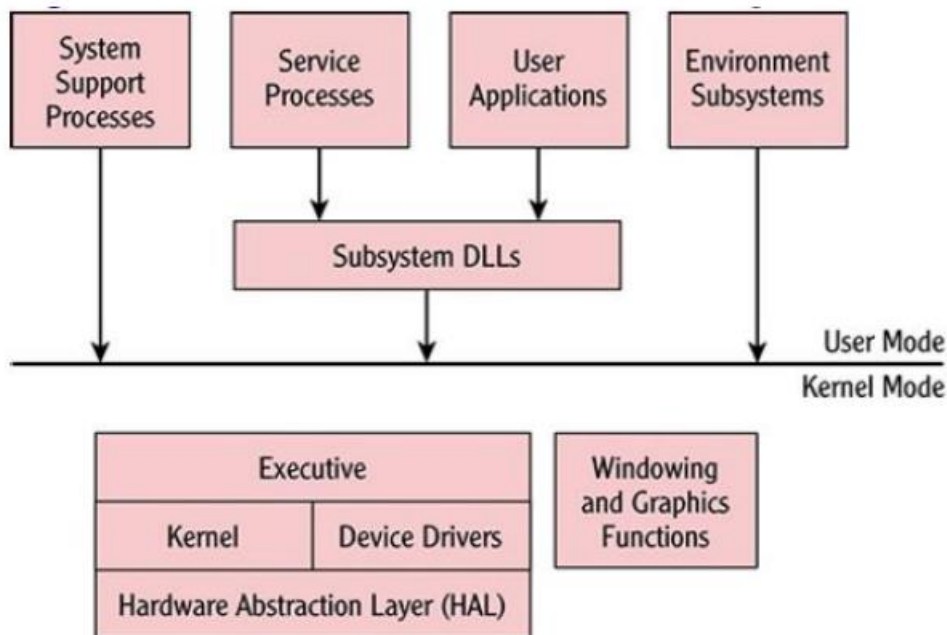
### **2. Nội dung thực hành**

- **Tìm hiểu lý thuyết**
- **VMWARE WORKSTATION**
  - VMware Workstation là một phần mềm cho phép người dùng chạy máy ảo trên máy tính vật lý. Bạn có thể tạo và hủy máy ảo (VM) dễ dàng trên máy chủ chỉ cần bằng công cụ này.
  - Tại VMware Workstation, người dùng sẽ chạy được máy ảo ở máy tính để bàn bằng hệ điều hành Windows hoặc Linux đều ổn. Ở trường hợp máy tính của bạn chạy đồng thời của 2 hệ điều hành này thì bạn cũng có thể chạy đồng thời nhiều máy ảo trên cùng một máy chủ. Phần mềm này cũng được đánh giá là khá tương thích phần cứng.
  - Tầm quan trọng của VMware Workstation
    - VMware Workstation là một phần mềm ảo hóa được sử dụng để tạo và quản lý các máy ảo trên một
    - 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.

• Hệ điều hành Windows: lịch sử, kiến trúc, giao diện, đặc điểm đặc trưng

- 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. 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 (GUI\*) và hoạt động qua các câu lệnh. Hệ điều hành này đã rất phổ biến từ năm 1981 đến 1999.
- 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.

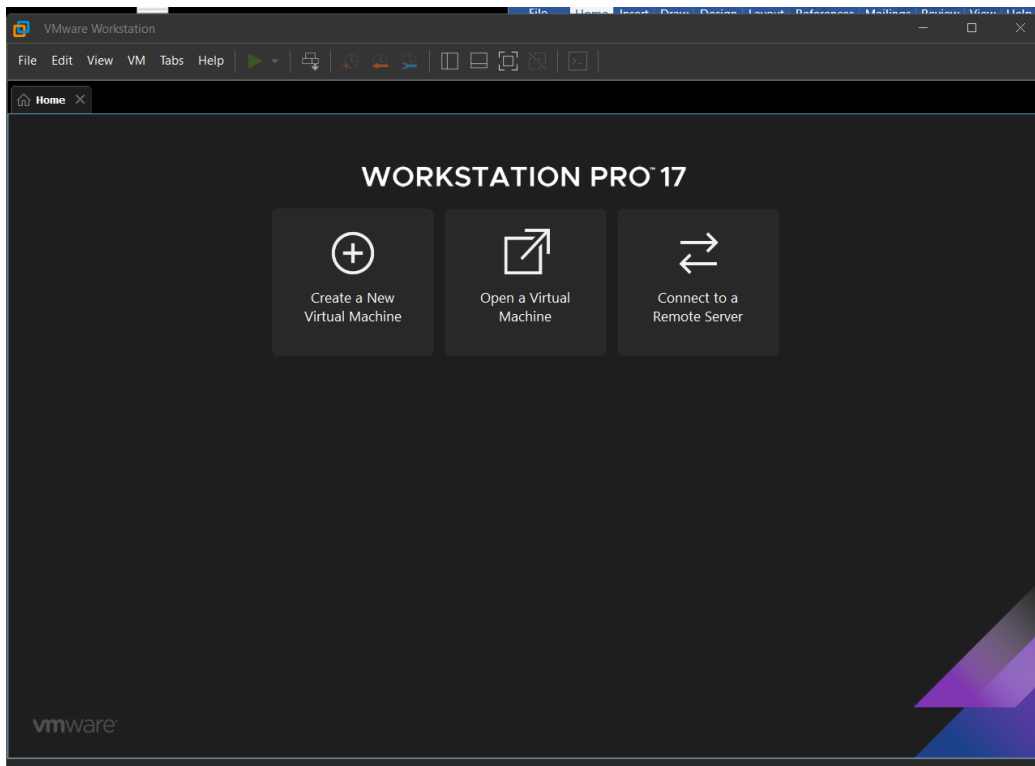


- Giao diện: Hệ điều hành Windows có ba cách giao tiếp chính giúp làm việc với các ứng dụng và thực hiện các công việc quản trị. Hầu hết người dùng thông thường sử dụng GUI song người quản trị lại được lợi hơn từ giao diện dòng lệnh và Windows PowerShell.
- Một số đặc trưng chung của Windows là:
  - Chế độ đa nhiệm;
  - Có một hệ thống giao diện dựa trên cơ sở bảng chọn với các biểu tượng kết hợp giữa đồ họa và văn bản giải thích;
  - Cung cấp nhiều công cụ xử lý đồ họa và đa phương tiện (Multimedia);
  - Đảm bảo khai thác có hiệu quả nhiều loại dữ liệu khác nhau như âm thanh, hình ảnh;
  - Đảm bảo các khả năng làm việc trong môi trường mạng.
- Tìm hiểu về các phần mềm diệt virus, phần mềm chống phần mềm gián điệp, phần mềm cứu hộ.
  - AVG AntiVirus là một phần mềm chống virus và bảo mật dữ liệu phổ biến, được phát triển bởi công ty AVG Technologies. Chương trình này được thiết kế để bảo vệ người dùng khỏi các mối đe dọa trực tuyến, bao gồm virus, malware, spyware và các loại phần mềm độc hại khác. AVG AntiVirus cung cấp nhiều tính năng an toàn như quét tự động, tường lửa, bảo vệ chống phishing và chống ransomware. Nó có thể chạy trên nhiều nền tảng, bao gồm Windows, macOS và Android, đồng thời cung cấp phiên bản miễn phí và trả phí để đáp ứng nhu cầu bảo mật của đối tượng người dùng. AVG AntiVirus thường được đánh giá cao về hiệu suất và khả năng bảo vệ, là một lựa chọn phổ biến trong lĩnh vực phần mềm chống virus và bảo mật toàn diện.
  - Spybot - Search & Destroy (Spybot S&D) là một phần mềm chống spyware và malware, phát triển bởi Safer-Networking Ltd. Với khả năng quét hệ thống, loại bỏ mối đe dọa và cung cấp tính năng Immunization để ngăn chặn trang web độc hại, Spybot S&D là một công cụ đáng tin cậy để bảo vệ hệ thống khỏi các tác nhân gây hại trực tuyến. Có phiên bản miễn phí và trả phí, Spybot S&D thường được đánh giá cao về hiệu suất và khả năng bảo vệ.
  - Malwarebytes Anti-Malware, sản phẩm của Malwarebytes Corporation, là một ứng dụng chống malware hàng đầu, nổi tiếng với khả năng hiệu quả trong việc ngăn chặn mọi loại mối đe dọa trực

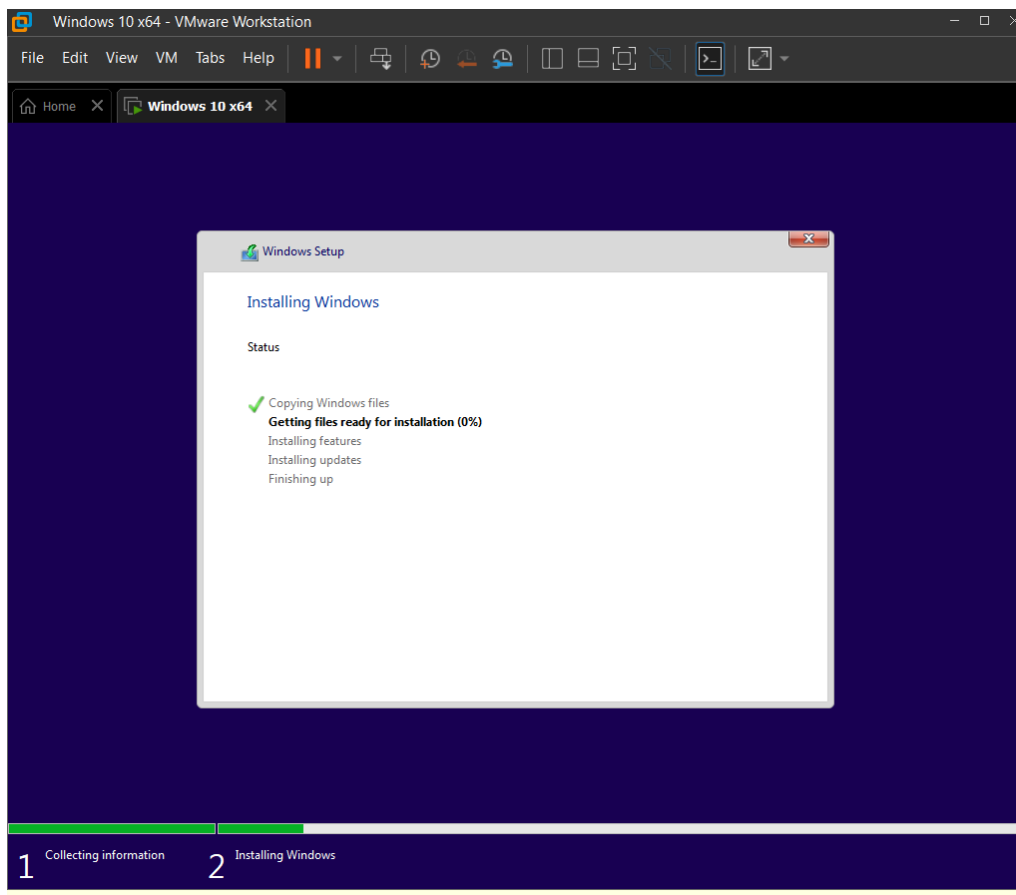
tuyến. Sử dụng công nghệ heuristics và quét đám mây, phần mềm nhanh chóng phát hiện và loại bỏ virus, trojan, spyware, adware, và các nguy cơ khác. Với tính năng quét nhanh và khả năng cập nhật dữ liệu mới đe dọa trong thời gian thực, Malwarebytes giúp người dùng kiểm soát hiệu suất hệ thống mà không giảm chất lượng bảo mật. Tính năng quét lập lịch, bảo vệ thời gian thực và khả năng cách ly mối đe dọa là những điểm đáng chú ý, tạo nên một giải pháp toàn diện và đáng tin cậy cho bảo vệ máy tính.

- 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.
- Một số nguồn khác
- **Chuẩn bị môi trường**
  - File cài đặt Windows 7 (hoặc Windows 10/11) định dạng iso.
  - Phần mềm ảo hóa ví dụ: VMWare Workstation.
- **Các bước thực hiện**

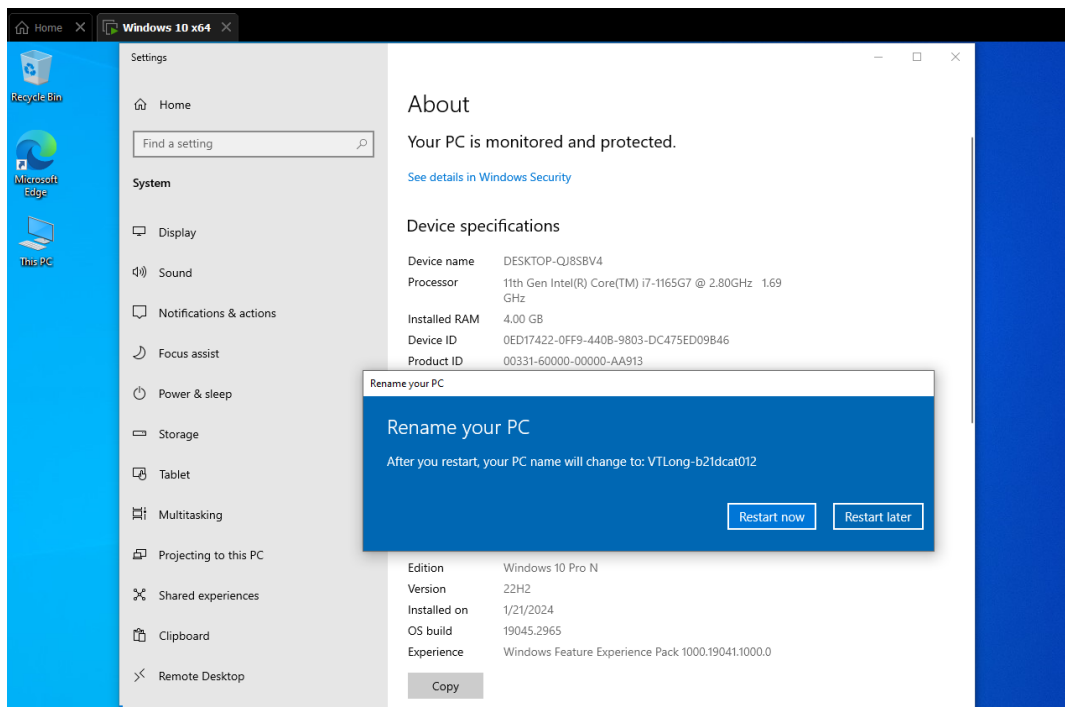
Khởi động chương trình máy ảo



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



Trong mục “System Properties” đổi tên máy trạm Windows thành “VTLong-b21dcat012”

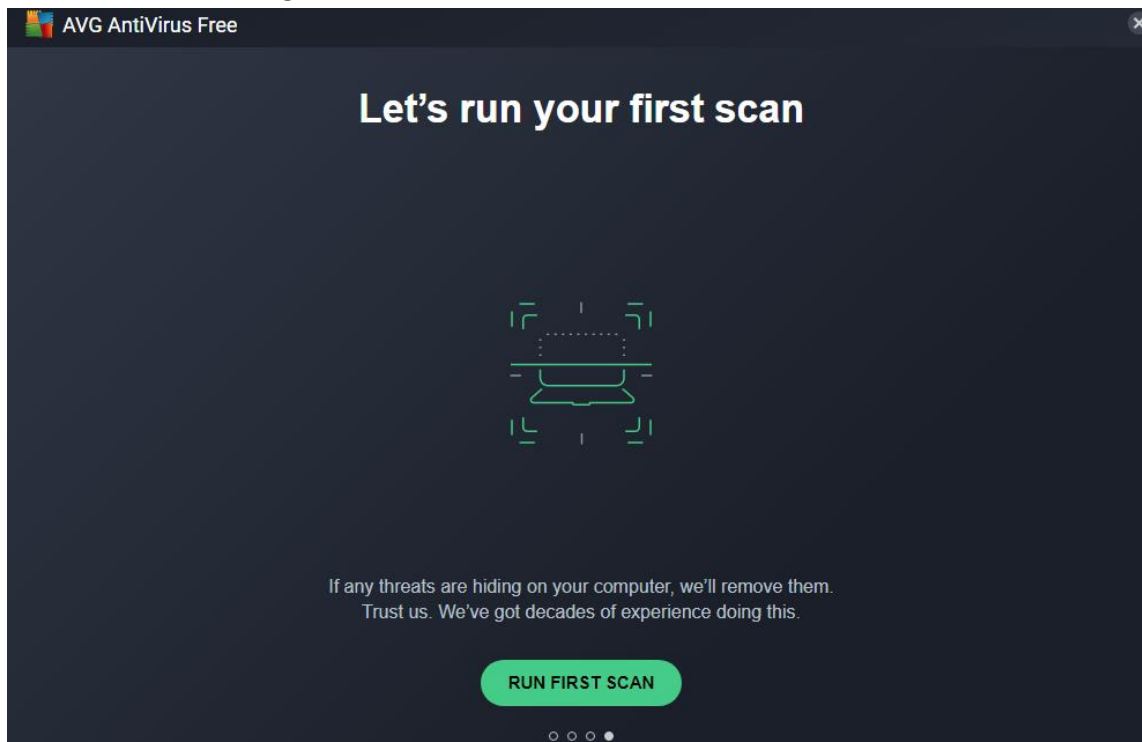


- Kết luận: Cài đặt thành công máy trạm

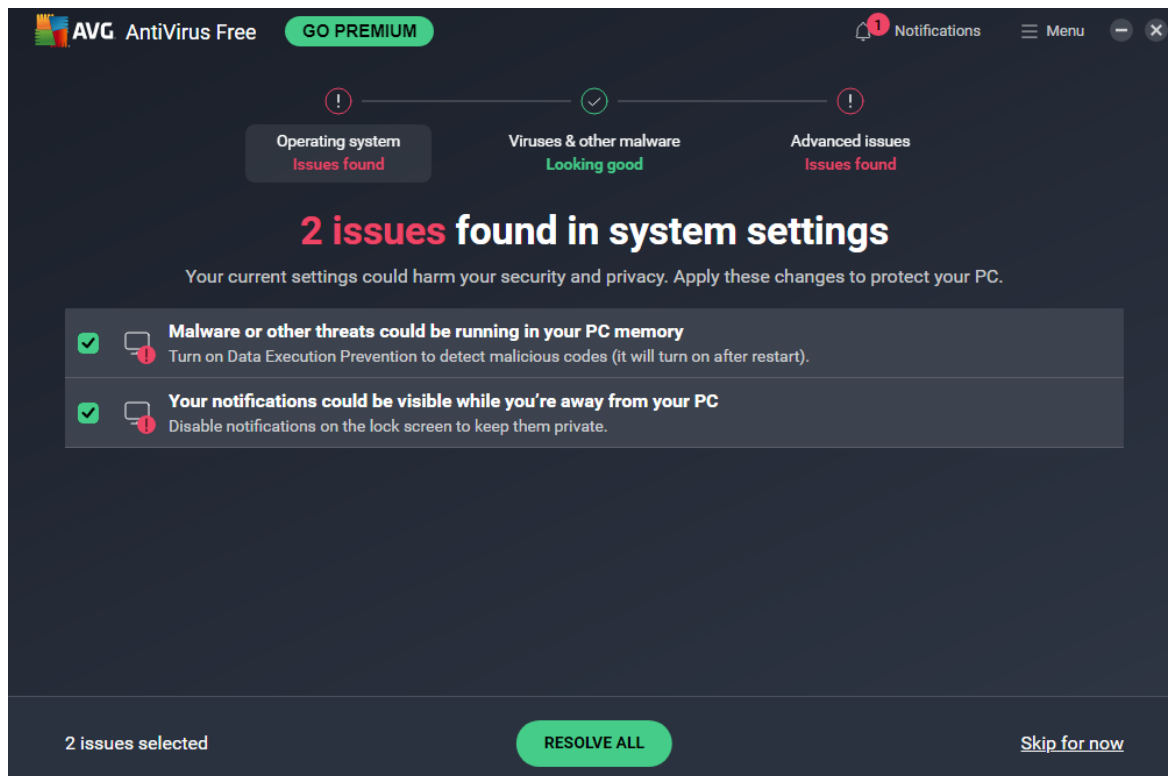
Thực hiện cài đặt và chạy một số phần mềm bảo vệ máy trạm :

a) Phần mềm diệt virus: AVG AntiVirus.

- Cài đặt thành công

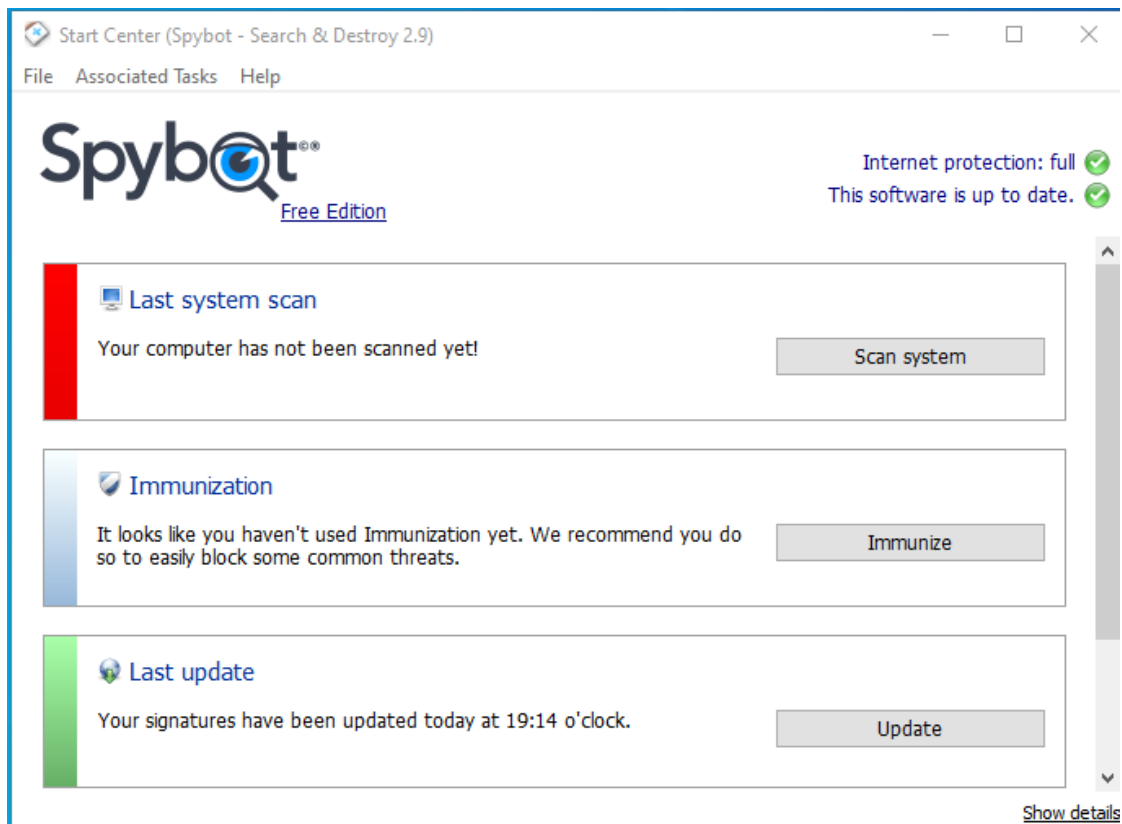


- Chạy và sử dụng phần mềm thành công.

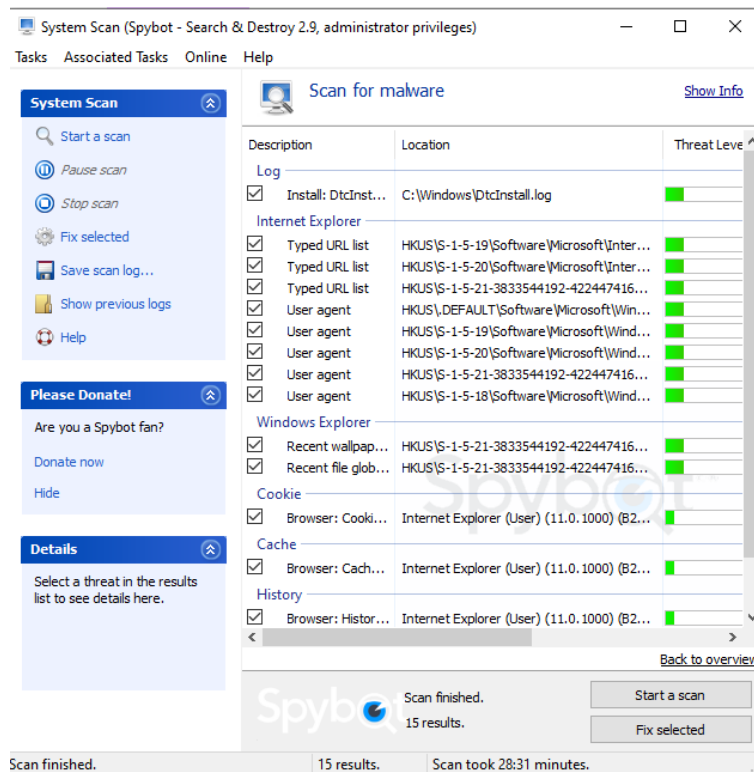


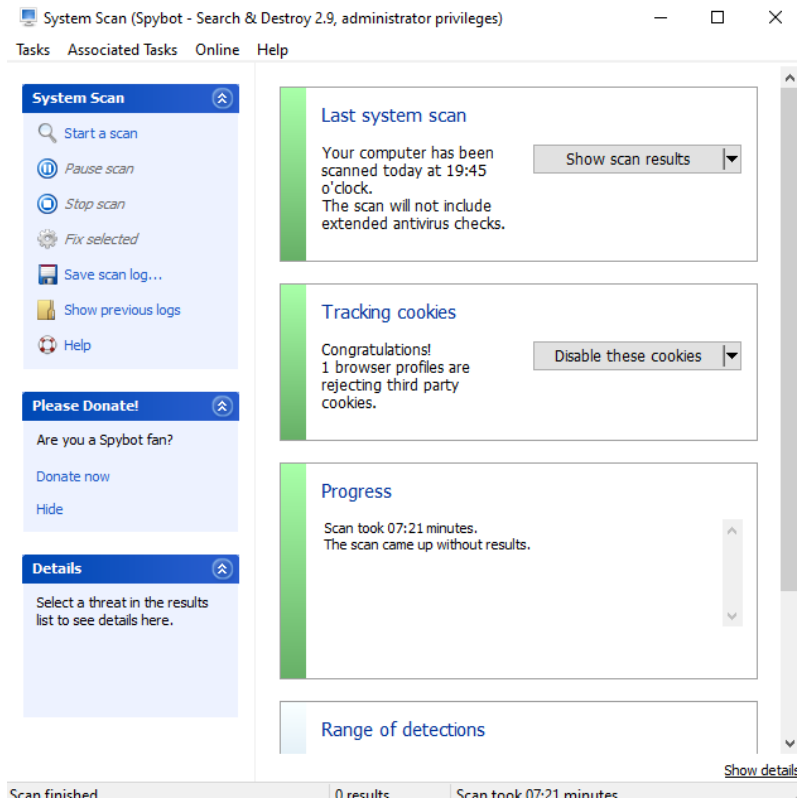
- Kết luận: cài đặt và sử dụng thành công phần mềm diệt virus: AVG AntiVirus.
- b) Phần mềm chống phần mềm gián điệp Spybot S&D (Spybot – Search & Destroy)
- Cài đặt thành công



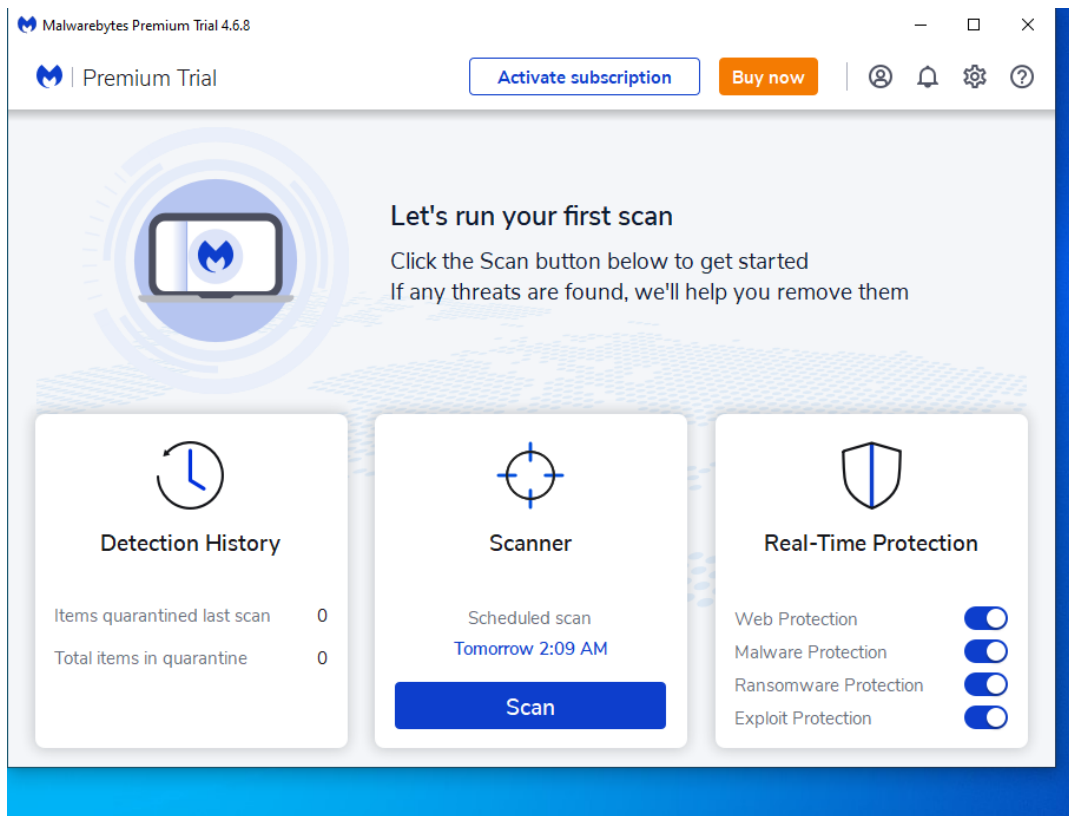


•Chạy và sử dụng phần mềm thành công

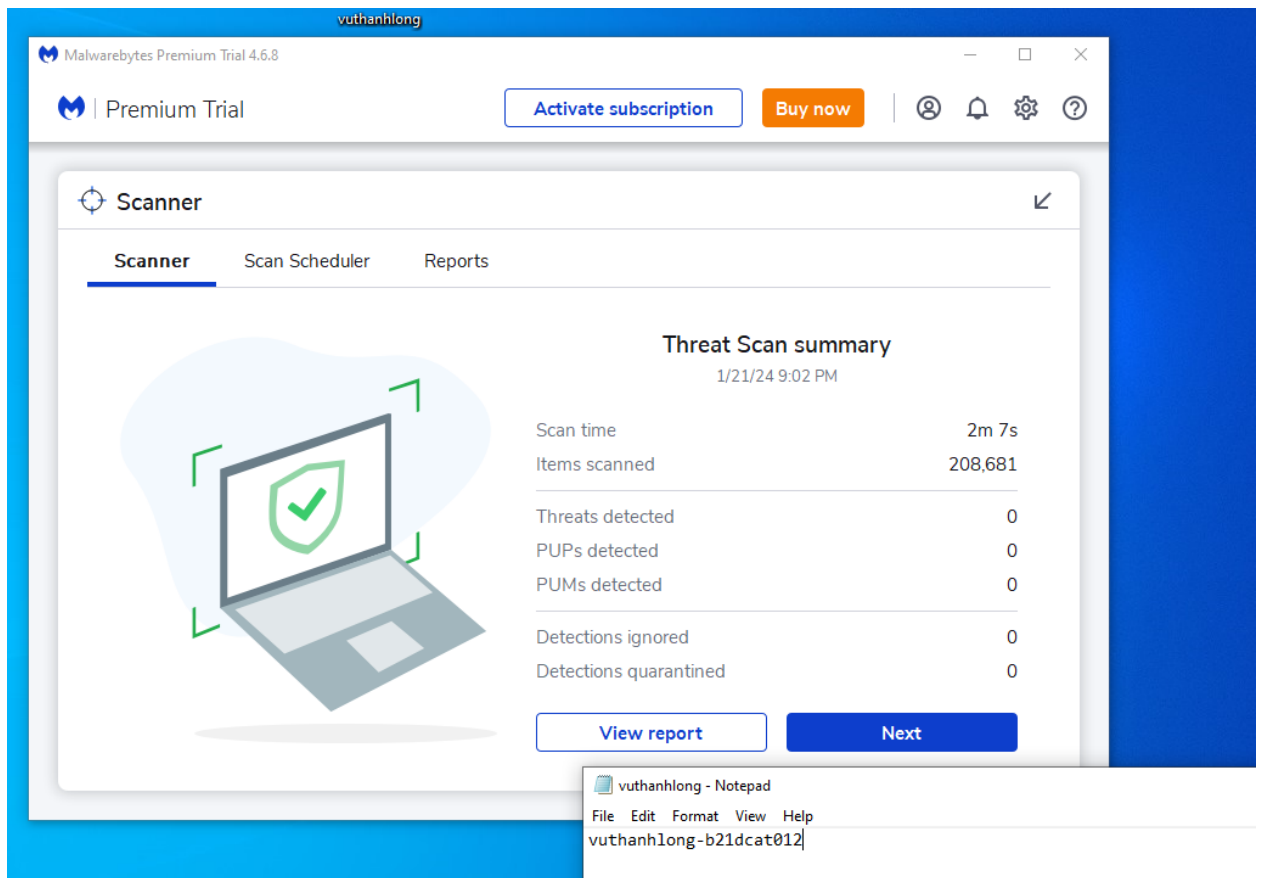




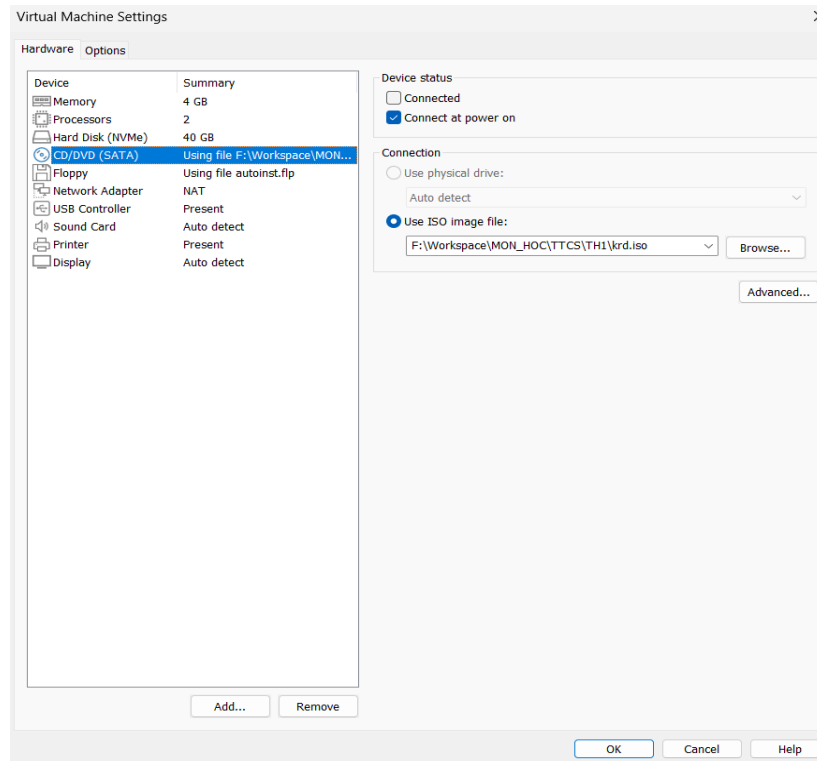
- Kết luận: cài đặt và sử dụng thành công phần mềm chống phần mềm gián điệp Spybot S&D (Spybot – Search & Destroy)
- c) Phần mềm chống các phần mềm độc hại: Malwarebytes Anti-Malware
- Cài đặt thành công



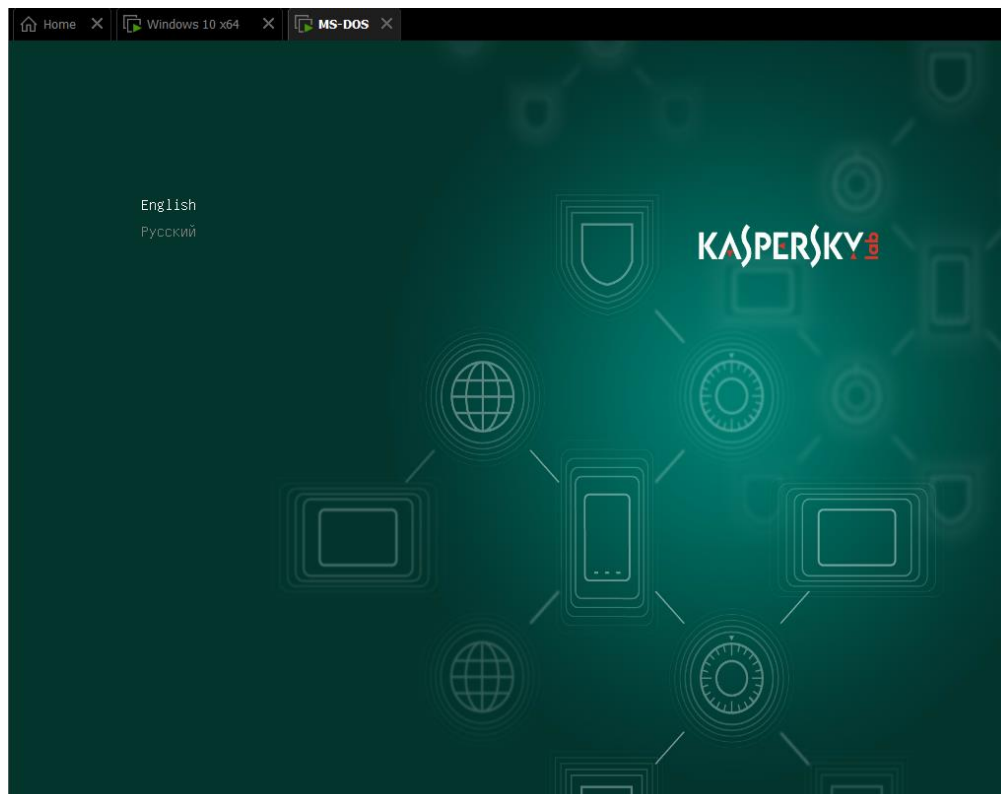
- Chạy và sử dụng phần mềm thành công



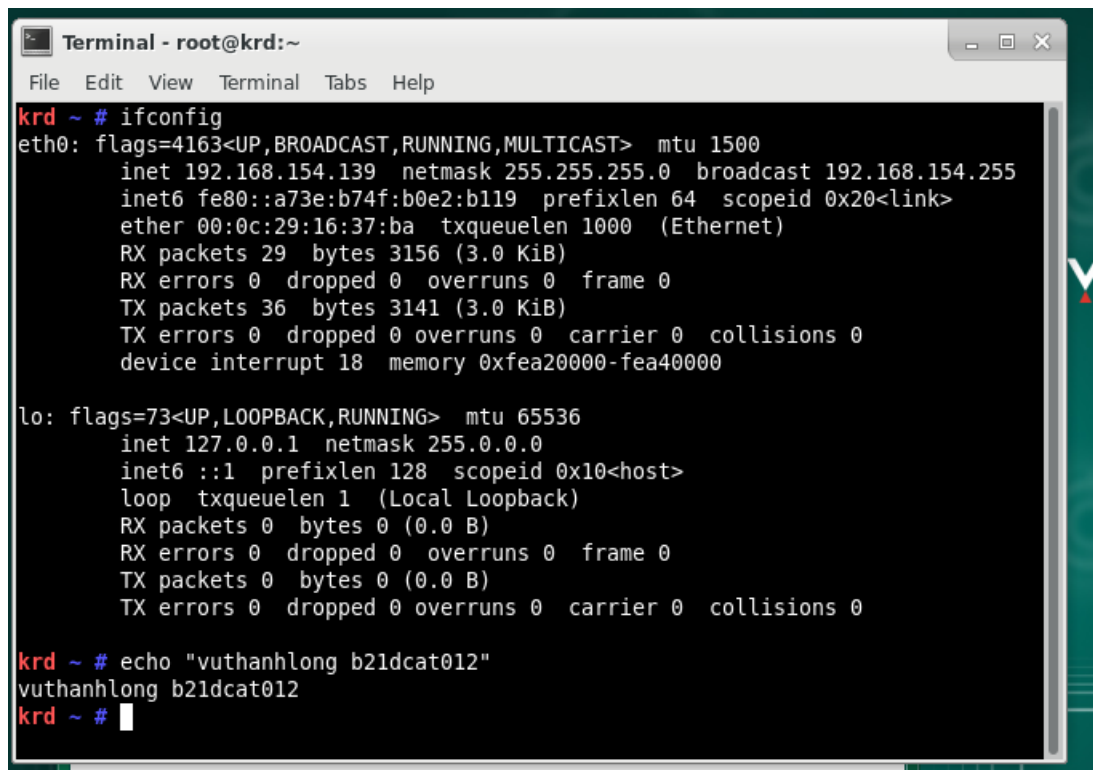
- Kết luận: cài đặt và sử dụng thành công phần mềm chống các phần mềm độc hại: Malwarebytes Anti-Malware
- d) Phần mềm cứu hộ: Kaspersky Rescue Disk (KRD)
- Tải phần mềm cứu hộ dạng iso:  
<https://www.kaspersky.com/downloads/free-rescue-disk>  
load vào trong mục CD/DVD của máy trạm ảo để có thể khởi 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



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



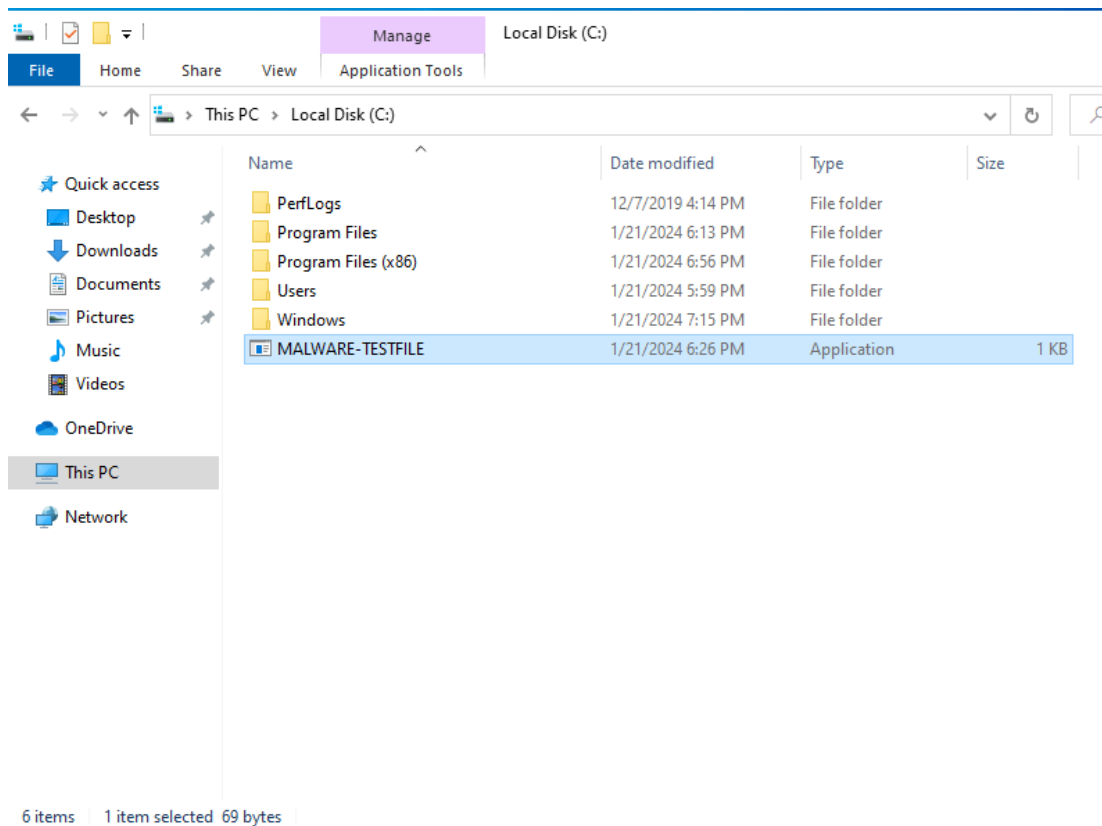
```
Terminal - root@krd:~
File Edit View Terminal Tabs Help

krd ~ # ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.154.139 netmask 255.255.255.0 broadcast 192.168.154.255
    inet6 fe80::a73e:b74f:b0e2:b119 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:16:37:ba txqueuelen 1000 (Ethernet)
    RX packets 29 bytes 3156 (3.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36 bytes 3141 (3.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 18 memory 0xfea20000-fea40000

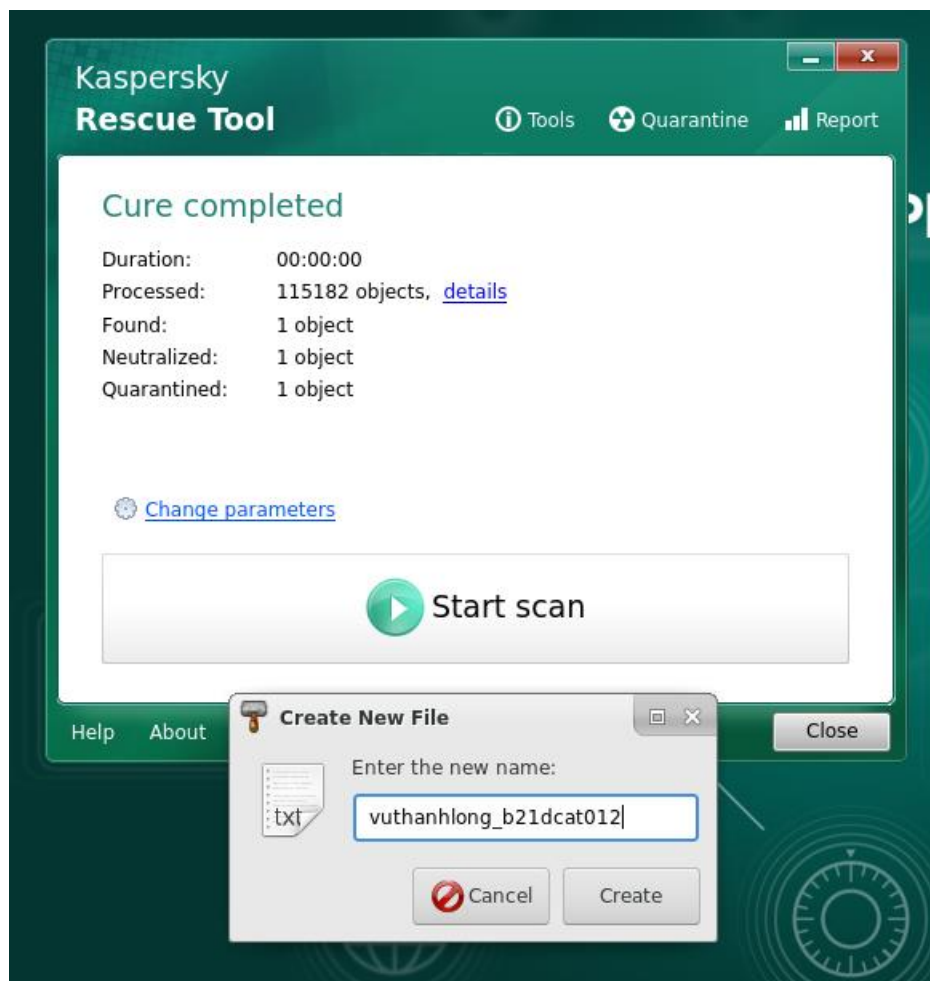
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

krd ~ # echo "vuthanhlng b21dcat012"
vuthanhlng b21dcat012
krd ~ #
```

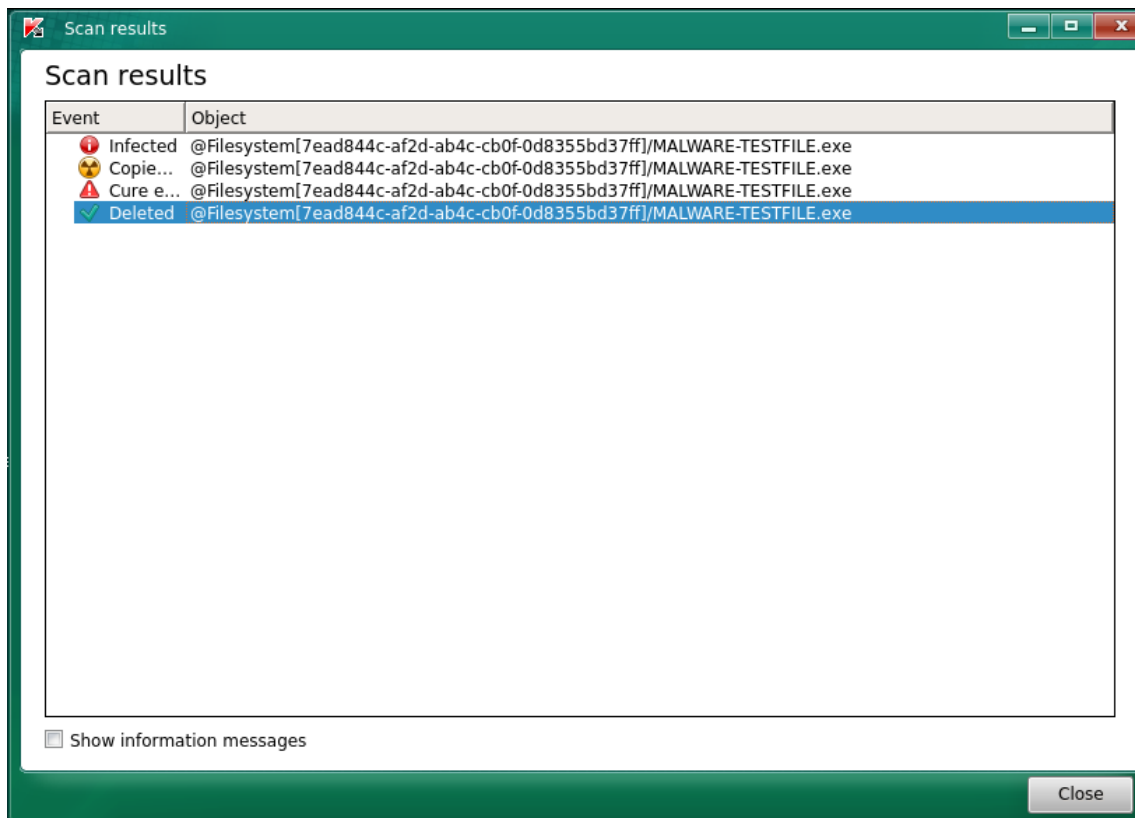
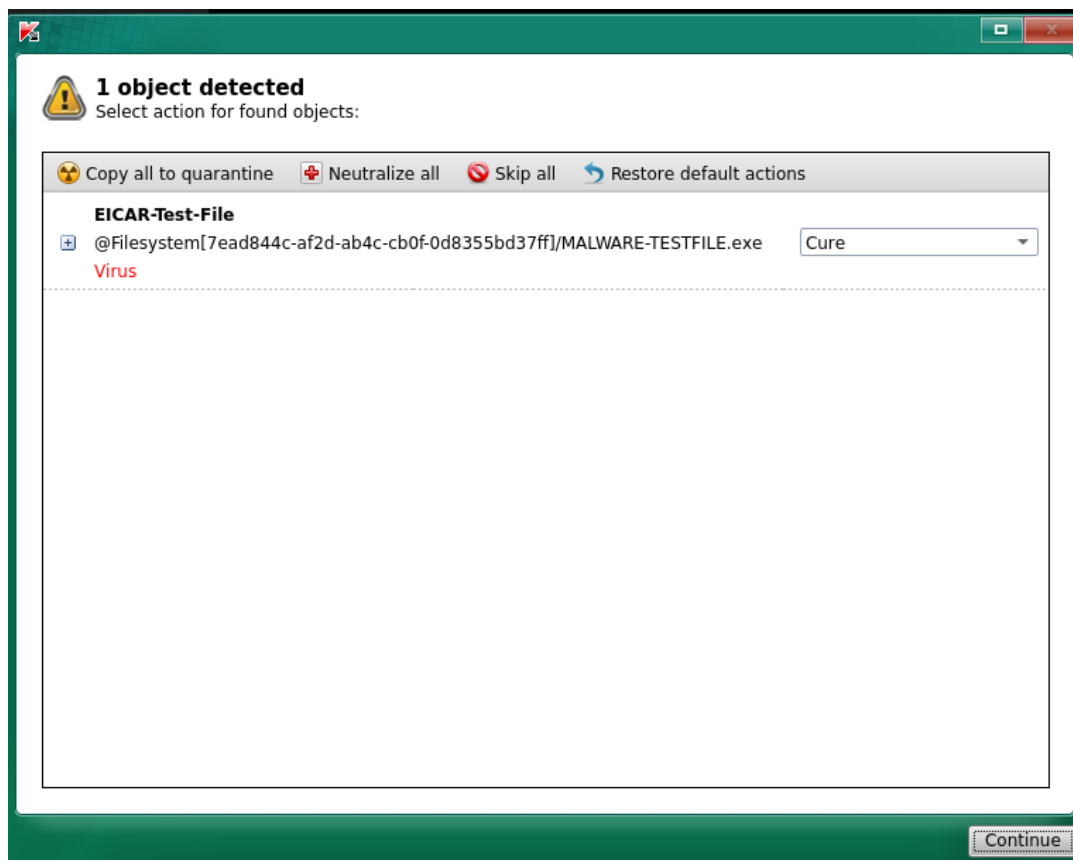
- Dùng Web browser tải file test mã độc từ đường link :  
<http://www.computersecuritystudent.com/WINDOWS/W7/lesson7/MALWARE-TESTFILE.exe>
- Lưu file test mã độc vào ổ C của máy trạm

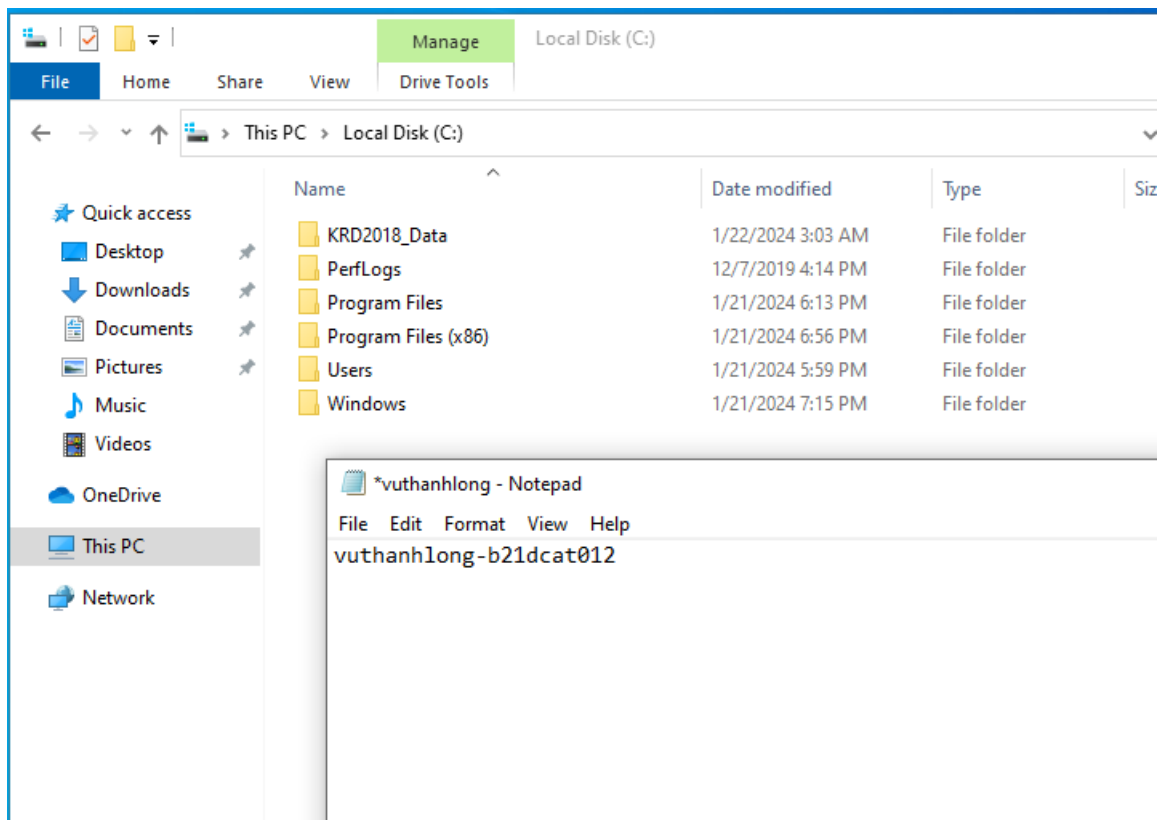


- Sau đó chạy Kaspersky Rescue Tool, vào setting chọn quét tất các các thư mục -> phát hiện ra file test mã độc và thực hiện xóa nó.









**Kết luận: Cài đặt và sử dụng thành công các phần mềm được yêu cầu**