ĐẠI HỌC BÁCH KHOA HÀ NỘI

ĐỒ ÁN TỐT NGHIỆP

Thiết kế và xây dựng hệ thống Antivirus phòng chống virus máy tính

Cao Thành Duy
duy.ct205202@sis.hust.edu.vn

Ngành Công nghệ thông tin

Giảng viên hướng dẫn: PGS.TS. Nguyễn Linh Giang _____

Chữ kí GVHD

Khoa: Kĩ thuật máy tính

Trường: Công nghệ Thông tin và Truyền thông

HÀ NỘI, 12/2024

LỜI CAM KẾT

Họ và tên sinh viên: Cao Thành Duy
Điện thoại liên lạc: 0917578898
Email: duy.ct205202@sis.hust.edu.vn
Lớp: Việt Pháp 01-K65
Hệ đào tạo: Công nghệ thông tin Việt Pháp

Tôi – *Cao Thành Duy* – cam kết Đồ án Tốt nghiệp (ĐATN) là công trình nghiên cứu của bản thân tôi dưới sự hướng dẫn của *PGS.TS.Nguyễn Linh Giang*. Các kết quả nêu trong ĐATN là trung thực, là thành quả của riêng tôi, không sao chép theo bất kỳ công trình nào khác. Tất cả những tham khảo trong ĐATN – bao gồm hình ảnh, bảng biểu, số liệu, và các câu từ trích dẫn – đều được ghi rõ ràng và đầy đủ nguồn gốc trong danh mục tài liệu tham khảo. Tôi xin hoàn toàn chịu trách nhiệm với dù chỉ một sao chép vi phạm quy chế của nhà trường.

Hà Nội, ngày 17 tháng 12 năm 2024

Tác giả ĐATN

Cao Thành Duy

LỜI CẢM ƠN

Em xin gửi lời cảm ơn chân thành đến thầy Nguyễn Linh Giang, người đã tận tình hướng dẫn và hỗ trợ em suốt quá trình thực hiện đồ án tốt nghiệp. Sự tận tâm và kiến thức sâu rộng của thầy đã giúp em hoàn thành đề tài.

Em xin gửi lời cảm ơn đến toàn thể thầy cô giáo tại Đại học Bách Khoa Hà Nội vì những năm tháng học tập quý báu và những kiến thức quý giá mà em đã được học hỏi từ trường.

Cuối cùng, em cũng xin cảm ơn gia đình đã luôn ủng hộ và động viên em trong suốt chặng đường học tập. Cảm ơn bạn bè đã cùng chia sẻ những khó khăn và niềm vui trong quá trình học tập cũng như trong quá trình thực hiện đồ án.

TÓM TẮT NỘI DUNG ĐỒ ÁN

Hiện nay, nhiều phần mềm Antivirus đã được phát triển và triển khai với các phương pháp như phát hiện dựa trên chữ ký (signature-based), phát hiện hành vi (behavior-based) và sử dụng trí tuệ nhân tạo (AI). Tuy nhiên, các giải pháp này vẫn tồn tại một số hạn chế như thời gian cập nhật chậm, khó nhận diện mã độc mới hoặc các cuộc tấn công tinh vi như ransomware và tấn công zero-day. Để khắc phục phần nào các hạn chế trên, đồ án lựa chọn hướng tiếp cận kết hợp phát hiện mã độc dựa trên chữ ký và phân tích hành vi bất thường của tệp tin để nâng cao khả năng bảo vệ hệ thống. Hướng tiếp cận này được lựa chọn vì tính khả thi và phù hợp với điều kiện kỹ thuật hiện tại, đồng thời đảm bảo khả năng phát hiện nhanh chóng và chính xác. Trong phạm vi đồ án, hệ thống được xây dựng với các chức năng chính bao gồm: quét và phát hiện mã độc theo thời gian thực, kiểm tra hành vi của tệp tin, cảnh báo người dùng khi phát hiện mã độc và báo cáo kết quả chi tiết. Phần mềm được phát triển bằng ngôn ngữ lập trình C++ và sử dụng thư viện Qt để thiết kế giao diện thân thiện với người dùng. Đóng góp chính của đồ án là xây dựng được hệ thống Antivirus có khả năng phát hiện nhanh, chính xác và cung cấp giao diện đơn giản, dễ sử dụng. Kết quả cuối cùng cho thấy hệ thống hoạt động hiệu quả, phát hiện được nhiều mẫu mã độc phổ biến, đảm bảo tính ổn định và có tiềm năng mở rộng để tích hợp thêm các công nghệ bảo mật tiên tiến trong tương lai.

Sinh viên thực hiện

(Ký và ghi rõ họ tên)

ABSTRACT

Currently, many antivirus solutions have been developed and deployed using methods such as signature-based detection, behavior-based detection, and artificial intelligence (AI). However, these solutions still have certain limitations, such as slow update times, difficulties in identifying new malware, and challenges in handling sophisticated attacks like ransomware and zero-day exploits. To mitigate these limitations, the project adopts a hybrid approach that combines signature-based detection and behavioral analysis of files to enhance the system's protection capabilities. This approach was chosen due to its feasibility and current technical suitability while ensuring fast and accurate malware detection. In this project, the system is developed with key functionalities, including real-time malware scanning and detection, file behavior analysis, user notifications upon threat detection, and detailed reporting. The software is implemented using the C++ programming language and the Qt library to design a user-friendly interface. The main contribution of the thesis is the development of an antivirus system that provides fast and accurate malware detection while maintaining simplicity and usability. The final results demonstrate that the system operates effectively, successfully detecting common malware samples, ensuring stability, and showing potential for future integration of advanced security technologies.

MỤC LỤC

DANH MỤC HÌNH VẼ