Shape, square

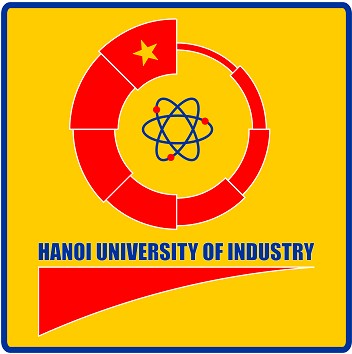
Description automatically generated

**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

**======\*\*\*======**

****

**BÁO CÁO BÀI TẬP LỚN HỌC PHẦN**

**NGUYÊN LÍ HỆ ĐIỀU HÀNH**

**ĐỀ TÀI**

**HỆ THỐNG BẢO VỆ TRONG HỆ ĐIỀU HÀNH WINDOWS**

**-----------------**

Giảng viên : Ths.Nguyễn Thanh Hải

Nhóm - Lớp : Nhóm 11 - 20212IT6025008

Thành viên : Lê Tiến Dũng - 2020604439

Lý Thị Dung – 2020605590

Đàm Mạnh Đào - 2020603917

Đào Hữu Thành - 2020604246

Nguyễn Hữu Thịnh - 2020604037

*Hà Nội, 2022*

# LỜI NÓI ĐẦU

Ngày nay, nhu cầu trao đổi dữ liệu qua mạng máy tính trở lên vô cùng quan trọng trong mọi hoạt động xã hội, song song với sự phát triển bùng nổ của mạng máy tính nói chung và mạng internet nói riêng thì nguy cơ đối mặt với hàng loạt các đe dọa tiềm tang như virus, sâu máy tính (Worm), các kiểu tấn công xâm nhập, … là rất lớn. Vấn đề đảm bảo an ninh, an toàn cho thông tin trên mạng ngày càng là mối quan tâm hàng đầu của các công ty, các tổ chức, các nhà cung cấp dịch vụ. Việc bảo vệ an toàn dữ liệu là vấn đề cấp thiết, vì vậy việc lựa chọn 1 hệ điều hành thích hợp, có khả năng bảo mật tốt, độ tin cậy cao là rất quan trọng. Nhận thấy điều cần thiết đó, từ những thế hệ windows 9x, Microsoft đã đặt nền móng và quan tâm đến vấn đề bảo mật và an toàn trong từng bản cập nhật và các bản phát hành của mình. Qua các phiên bản Windows, vấn đề bảo mật luôn luôn nhận được sự quan tâm sát sao của cộng đồng IT, bởi Windows là hệ điều hành phổ biến nhất trên thế giới.

Vào tháng 1 năm 2002, hệ thống bảo mật của Microsoft đã có những khoảng khắc lóe sáng. Tuy nhiên, thành quả đạt được về bảo mật của Microsoft chưa thể bao phủ toàn bộ sản phẩm của hãng. Mặc dù gặp phải một số rắc rối khi mới phát hành, nhưng Windows server 2003 vẫn được các chuyên gia công nghệ thông tin đánh giá là an toàn hơn nhiều so với các phiên bản trước đó của hãng.

Trong đề tài này, chúng em sẽ nghiên cứu và tìm hiểu một cách chi tiết nhất về hệ thống bảo vệ trong HĐH Windows, những hệ thống bảo vệ từ sơ sài cho đến tinh vi tương ứng với từng hệ điều hành đã được phát hành của hãng như: WinNT, Windows 98, Windows 2000, Windows 2003… thì cứ mỗi lần phát triển hệ điều hành của Microsoft cho ra một phiên bản mới thì dĩ nhiên là phiên bản đó phải có những chức năng được cải tiến, trong đó chắc chắn sẽ có những cải tiến về bảo mật.

MỤC LỤC

[LỜI NÓI ĐẦU 2](#_Toc105058584)

[CHƯƠNG 1: BẢO VỆ HỆ THỐNG 5](#_Toc105058585)

[1.1 Mục tiêu của bảo vệ hệ thống 5](#_Toc105058586)

[1.2 Nguyên tắc bảo vệ (Principles of Protection) 5](#_Toc105058587)

[1.3 Miền bảo vệ (Domain of Protection) 5](#_Toc105058588)

[1.4 Ma trận quyền truy nhập 6](#_Toc105058589)

[1.4.1 Khái niệm về ma trận quyền truy nhập 6](#_Toc105058590)

[1.4.2 Các phương pháp cài đặt ma trận quyền truy cập 7](#_Toc105058591)

[1.5 Kiểm soát quyền truy nhập (Access Control) 8](#_Toc105058592)

[1.6 Thu hồi quyền truy nhập (Revocation of Access Rights) 9](#_Toc105058593)

[CHƯƠNG 2: AN TOÀN HỆ THỐNG 10](#_Toc105058594)

[2.1 Các vấn đề về bảo vệ hệ thống 10](#_Toc105058595)

[2.2 Các cơ chế an toàn hệ thống 10](#_Toc105058596)

[2.2.1 Kiểm định danh tính 10](#_Toc105058597)

[2.2.2 Ngăn chặn nguyên nhân từ phía các chương trình 10](#_Toc105058598)

[2.2.3 Ngăn chặn nguyên nhân từ phía hệ thống 11](#_Toc105058599)

[2.2.4 Giám sát các nguyên nhân 11](#_Toc105058600)

[CHƯƠNG 3: VIRUS MÁY TÍNH 12](#_Toc105058601)

[3.1 Khái niệm về virus 12](#_Toc105058602)

[3.2 Phân loại virus 12](#_Toc105058603)

[3.3 Cơ chế hoạt động của virus 12](#_Toc105058604)

[3.4 Phòng tránh virus 13](#_Toc105058605)

[3.4.1 Các chương trình phòng tránh và phát hiện virus 13](#_Toc105058606)

[3.4.2 Một số biện pháp phòng chống virus 14](#_Toc105058607)

[CHƯƠNG 4: BẢO VỆ TRÊN WINDOWS 15](#_Toc105058608)

[4.1 Công cụ bảo vệ 15](#_Toc105058609)

[4.1.1 Firewall 15](#_Toc105058610)

[4.1.2 Windows Defender 15](#_Toc105058611)

[4.1.3 Tamper Protection 16](#_Toc105058612)

[4.2 Quyền người dùng 17](#_Toc105058613)

[4.2.1 Quyền User Right 17](#_Toc105058614)

[4.2.2 Quyền Permission 20](#_Toc105058615)

[TÀI LIỆU THAM KHẢO 23](#_Toc105058616)

[KẾ HOẠCH THỰC HIỆN BÀI TẬP LỚN 24](#_Toc105058617)

[PHIẾU HỌC TẬP NHÓM 25](#_Toc105058618)

# BẢO VỆ HỆ THỐNG

## Mục tiêu của bảo vệ hệ thống

Khi tiến trình hoạt động song hành trong hệ thống thì một tiến trình gặp lỗi có thể ảnh hưởng đến các tiến trình khác và ảnh hưởng tới toàn bộ hệ thống. Hệ điều hành cần phải phát hiện ngăn chặn không cho lỗi lan truyền và đặc biệt là phát hiện các lỗi tiềm ẩn trong hệ thống để tăng cường độ tin cậy. Mặt khác, mục tiêu của bảo vệ hệ thống còn là chống sự truy cập bất hợp lệ, đảm bảo cho các tiến trình khi hoạt động trong hệ thống sử dụng tài nguyên phù hợp với quy định của hệ.

Vai trò của bộ phận bảo vệ trong hệ thống là cung cấp một cơ chế để áp dụng các chiến lược quản trị việc sử dụng tài nguyên. Cần phân biệt rõ giữa khái niệm cơ chế và chiến lược của bộ phận bảo vệ trong hệ thống:

* ***Cơ chế***: xác định làm thế nào để thực hiện việc bảo vệ, có thể có các cơ chế phần mềm hoặc cơ chế phần cứng.
* ***Chiến lược***: quyết định việc bảo vệ được áp dụng như thế nào: Những đối tượng nào trong hệ thống cần được bảo vệ, và các thao tác thích hợp trên các đối tượng này.

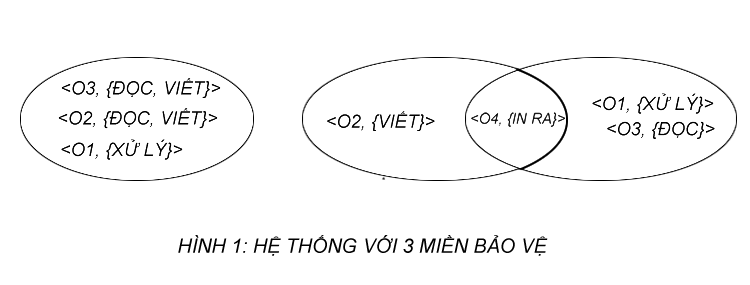
## Nguyên tắc bảo vệ (Principles of Protection)

Các nguyên tắc bắt buộc đặc quyền tối thiểu (The principle of least privilege dictates) là một loạt các quy tắc cho rằng các chương trình, người sử dụng, và các hệ thống chỉ đủ quyền để thực hiện các nhiệm vụ của các chương trình, người sử dụng và các hệ thống đó.

Các nguyên tắc trên được đặt ra và nó đảm bảo sự thiệt hại do các lỗi của 1 hay nhiều tiến trình phát sinh là ít nhất và hầu như không xảy ra nếu các tiến trình thực hiện đúng các quy tắc đó.

## Miền bảo vệ (Domain of Protection)

Các khả năng thao tác mà chủ thể có thể thực hiện trên khách thể được gọi là quyền truy cập (Access Right), mỗi miền định nghĩa một tập hợp các đối tượng và các hoạt động mà có thể thể hiện trên từng đối tượng. Mỗi quyền truy nhập được định nghĩa bởi một bộ hai thành phần <đối tượng, {quyền thao tác}> (<object, {access right}>). Như vậy, ta có thể hình dung miền bảo vệ là một tập hợp các quyền truy nhập, xác định các thao tác mà chủ thể có thể thực hiện trên các khách thể. Các miền bảo vệ khác nhau có thể giao nhau một số quyền truy cập.

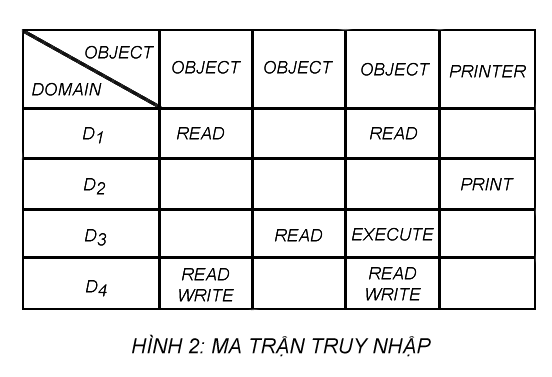


* Sự liên kết giữa một quá trình và một miền có thể là ***tĩnh*** hoặc ***động***:
* ***Liên kết tĩnh***: trong suốt thời gian tồn tại của tiến trình trong hệ thống, tiến trình chỉ hoạt động trong một miền bảo vệ.
* ***Liên kết động***: cho phép tiến trình chuyển đổi từ miền bảo vệ này sang miền bảo vệ khác trong suốt thời gian tồn tại trong hệ thống của nó. điểm.
* Một miền bảo vệ có thể được xây dựng cho: *Một người sử dụng*, m*ột tiến trìn**h, một thủ tục*

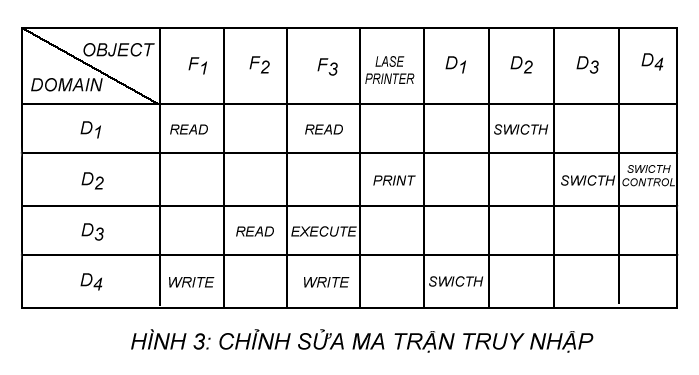
## Ma trận quyền truy nhập

### ***Khái niệm về ma trận quyền truy nhập***

Để biểu diễn miền bảo vệ, các hệ điều hành sẽ cài đặt các ma trận quyền truy cập trong đó các hạng của ma trận biểu diễn các miền bảo vệ, các cột biểu diễn khách thể. Phần tử (i, j) của ma trận xác định quyền truy nhập của chủ thể miền bảo vệ Di, có thể thao tác đối với khách thể Oj.

Một cách trừu tượng, có thể biểu diễn mô hình bảo vệ trên đây như một ma trận quyền truy xuất (access matrix). Các dòng của ma trận biểu diễn các miền bảo vệ và các cột tương ứng với các đối tượng trong hệ thống. Phần tử access[i,j] của ma trận xác định các quyền truy xuất mà một tiến trình hoạt động trong miền bảo vệ Di có thể thao tác trên đối tượng Oj.

Cơ chế bảo vệ được cung cấp khi ma trận quyền truy xuất được cài đặt

Khi đó tiến trình được phép chuyển từ miền bảo vệ Di sản miền bảo vệ Dj nếu phần tử access(i, j) chứa đựng quyền ở chuyển Oj ( switch).

Các thao tác sửa đổi nội dung ma trận được phép thực hiện bao gồm:

* ***Copy***: nếu một quyền truy xuất R trong access[i,j] được đánh dấu là R\* thì có thể sao chép nó sang một phần tử access[k,j] khác.
* ***Transfer***: nếu một quyền truy xuất R trong access[i,j] được đánh dấu là R+ thì có thể chuyển nó sang một phần tử access[k,j] khác.

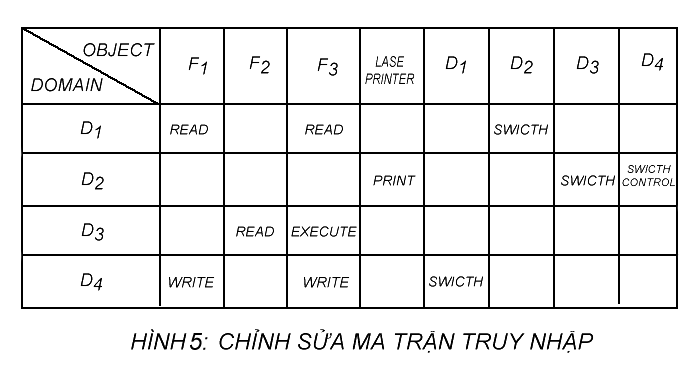
Table

Description automatically generated

**Table

Description automatically generated*Owner***: nếu access[i,j] chứa quyền truy xuất owner thì tiến trình hoạt động trong miền bảo vệ Di có thể thêm hoặc xóa các quyền truy xuất trong bất kỳ phần tử nào trên cột j.

***Control***: nếu access[i, j] chứa quyền truy xuất control thì tiến trình hoạt động trong miền bảo vệ D có thể xóa bất kỳ quyền truy xuất nào trong các phần tử trên dòng j.



### ***Các phương pháp cài đặt ma trận quyền truy cập***

***Bảng toàn cục (Global Table):*** Phương pháp này đơn giản nhất, hệ thống sử dụng 1 bảng toàn cục bao gồm các bộ ba thành phần <miền bảo vệ, khách thể, quyền truy cập> (<domain, object, rights>). Phương pháp này có kích thước rất lớn nên không thể giữ trong bộ nhớ.

***Danh sách quyền truy nhập (Access Control List for Objects - ACL)***: Có thể cài đặt mỗi cột trong ma trận quyền truy xuất như một danh sách quyền truy xuất đối với một đối tượng. Mỗi đối tượng trong hệ thống sẽ có một danh sách bao gồm các phần tử là các bộ hai thứ tự <miền bảo vệ, các quyền truy xuất.

*Ví dụ:* Một miền bảo vệ trong hệ thống UNIX được xác định tương ứng với một người sử dụng (uid) trong một nhóm (gid) nào đó. Giả sử có 4 người dùng: A, B, C, D thuộc các nhóm tương ứng là system, staff, student, student. Khi đó các tập tin trong hệ thống có thể có các ACL như sau:

File0: (A, \*, RWX)

File1: (A, system, RWX)

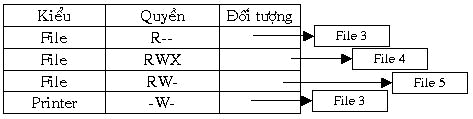
File2: (A, \*, RW-), (B, staff, R--), (D, \*, RW-)

File3: (\*, student, R--)

File4: (C, \*, ---), (\*, student, R--)

***Danh sách khả năng (Capability List for Domain):*** Mỗi dòng trong ma trận quyền truy xuất tương ứng với một miền bảo vệ sẽ được tổ chức thành một danh sách tiềm năng (capabilities list). Một danh sách tiềm năng của một miền bảo vệ là một danh sách các đối tượng và các thao tác được quyền thực hiện. Một phần tử của C-List được gọi là một tiềm năng (capability)

*Ví dụ:*



Tiến trình chỉ có thể thực hiện thao tác M trên đối tượng Oj trong miền bảo vệ Di, nếu trong C\_List của Di có chứa tiềm năng tương ứng của Oj.

Danh sách tiềm năng được gán tương ứng với từng miền bảo vệ

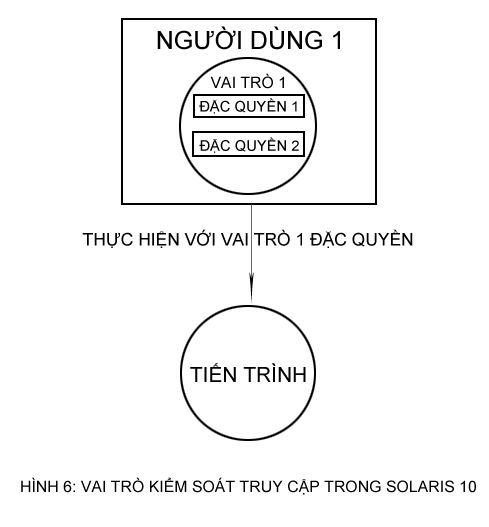
Hệ điều hành cung cấp các thủ tục cho phép tạo lập, hủy bỏ và sửa đổi các tiềm năng của một đối tượng, và chỉ các tiến trình đóng vai trò server (thường là tiến trình hệ điều hành) mới có thể sửa đổi nội dung C\_List.

***Cơ chế khóa-chìa (A Lock-Key Mechanism):*** sự kết hợp giữa danh sách quyền truy nhập và danh sách khả năng.

## Kiểm soát quyền truy nhập (Access Control)

Access Control có thể sử dụng trên các file với một tập tin hệ thống.

*Ví dụ:* Những tính năng kiểm soát truy nhập được tích hợp sẵn trong Solaris 10 thể hiện qua các đặc quyền trong quy định về quyền cho user 1.



## Thu hồi quyền truy nhập (Revocation of Access Rights)

Khi thu hồi quyền truy nhập cần chú ý tới một số vấn đề sau:

* Thu hồi tức khách hay trì hoãn và nêu trì hoãn thì tới bao giờ?
* Nếu loại bỏ một quyền truy cập của chủ thể tới một khách thể thì loại bỏ tất cả hay chỉ áp dụng với một số chủ đề.
* Thu hồi một số quyền hay toàn bộ quyền trên một khách thể?
* Thu hồi tạm thời hay vĩnh viễn một quyền truy cập?

Phương pháp:

* ***Tái yêu cầu***: loại bỏ các khả năng ra khỏi miền bảo vệ sau mỗi chu kì.
* ***Sử dụng con trỏ ngược***: Với mỗi khách thể sẽ tồn tại các con trỏ, trỏ đến các khả năng tương ứng của khách thể. Khi cần thu hồi quyền truy nhập nào trên khách thể hệ thống sẽ dựa vào các con trỏ để tìm kiếm các khả năng tương ứng.
* ***Sử dụng con trỏ gián tiếp***: trong phương pháp này con trỏ không trỏ trực tiếp tới các khả năng của khách thể mà trỏ tới một bảng toàn cục được quản lý bởi hệ điều hành. Khi cần thu hồi quyền truy nhập chỉ cần xóa phần tử tương ứng trong bảng này.

# AN TOÀN HỆ THỐNG

## Các vấn đề về bảo vệ hệ thống

Hệ thống được coi là an toàn nếu các tài nguyên được sử dụng đúng quy định trong mọi hoàn cảnh. Điêu này khó có thể đạt được trong thực tế. Thông thường, cơ chế an toàn hệ thống bị vi phạm vì các nguyên nhân vô tình hoặc cố ý. Việc ngăn chặn các hành vi cố ý là rất khó khăn vi hầu như không thể đạt hiệu quả hoàn toàn.

Bảo đảm an toàn hệ thống ở cạp cao như chống lại các nguyên nhân hỏa hoạn, thiên tai, mất điện...

## Các cơ chế an toàn hệ thống

### ***Kiểm định danh tính***

Để đảm bảo an toàn, hệ điều hành cần phải giải quyết tốt vấn đề kiểm định danh tính (authentication). Hoạt động của hệ thống bảo vệ phụ thuộc vào khả năng xác định các tiến trình đang xử lý.

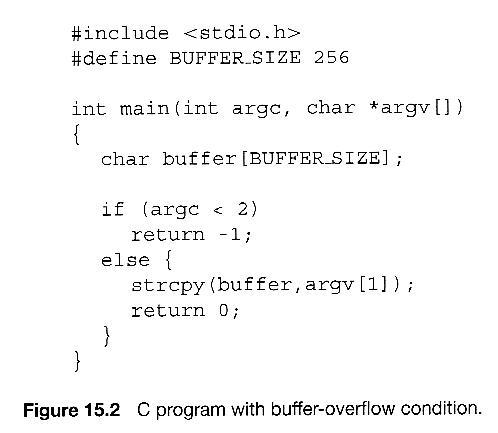
Cách tiếp cận phổ biến nhất để giải quyết vấn đề là sử dụng mật khẩu để kiểm định danh tính của người sử dụng. Mỗi người dùng muốn sử dụng tài nguyên, hệ thống sẽ so sánh mật khẩu của họ để nhập vào với mật khẩu được lưu.

Cơ chế mật khẩu rất đơn giản và dễ sử dụng do đó được các hệ điều hành áp dụng rộng rãi.

### ***Ngăn chặn nguyên nhân từ phía các chương trình***

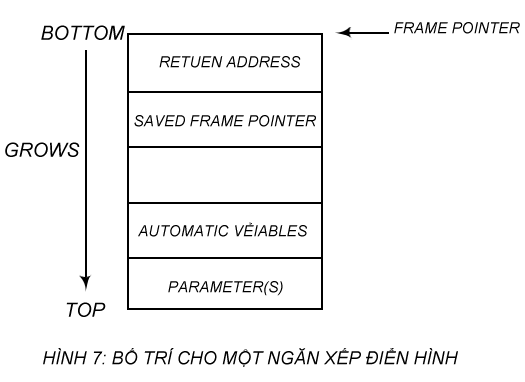
Trong môi trường hoạt động mà một chương trình được tạo lập bởi một người có thể được người khác sử dụng rất có thể sẽ xảy ra các tình huống sử dụng sai chức năng, từ đó dẫn tới những hậu quả không lường trước. Hai trường hợp điển hình gây mất an toàn hệ thống: *Ngựa thành troy, Lỗ hổng bảo mật (Trap-door), Logic Bomb, Stack và Buffer Overflow*

*Ví dụ* sau cho chúng ta thấy cách thức tấn công của loại đoạn mã này: Lệnh strcpy sẽ làm tràn bộ nhớ đệm, ghi đè lên các khu vực lân cận của bộ nhớ.

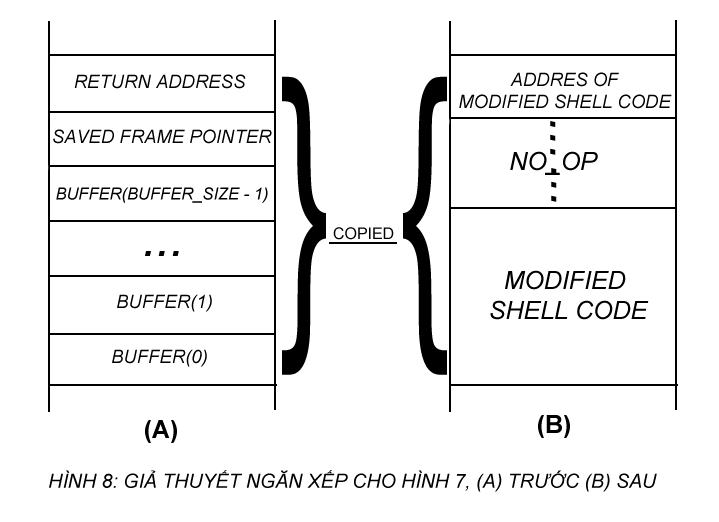


Vậy, làm thế nào để gây nên tình trạng tràn bộ nhớ đệm?

Chúng ta sẽ tìm hiểu cấu trúc của ngăn xếp trong bộ nhớ:



Sau đây là cách để khắc phục:



### ***Ngăn chặn nguyên nhân từ phía hệ thống***

Hầu hết các tính trình hoạt động trong hệ thống đều có thể tạo ra các tiến trình con. Trong các cơ chế hoạt động này, các tài nguyên hệ thống rất dễ bị sử dụng sai mục đích gây mất an toàn cho hệ thống. hai mối đe doạ phổ biến theo phương pháp này là: *Các chương trình sâu (worm), Các chương trình virus*

### ***Giám sát các nguyên nhân***

* Người sử dụng cố gắng nhập mật khẩu nhiều lần.
* Các tiến trình với định dạng nghi ngờ không được uỷ quyền.
* Các tiến trình lạ trong trong các thư mục hệ thống.
* Các chương trình kéo dài thời gian xử lý một cách đáng ngờ.
* Các tệp tin và các thư mục bị khóa không hợp lý.
* Kích thước các chương trình hệ thống bị thay đổi…

# VIRUS MÁY TÍNH

## Khái niệm về virus

Virus máy tính là một chương trình có khả năng gián tiếp tự kích hoạt, tự lan truyền trong môi trường của hệ thống tính toán và làm thay đổi môi trường hệ thống hoặc cách thực hiện chương trình, điều này có thể dẫn đến đến việc chương trình hoặc dữ liệu bị hỏng, không khôi phục được, thậm chí có thể bị xoá.

Gián tiếp kích hoạt là trừ người viết virus và lần đầu tiên đưa hệ thống phải tiếp nạp chương trình virus và thực hiện nó, còn những người sử dụng náo chỉ nạp chương trình của mình. Nếu đó là chương trình nhiễm virus. Thì virus sẽ chiếm quyền điều khiển trước tiến hành lây lan và sửa đổi sau đó mới trả quyền điều khiển cho chương trình được gọi.

Một số biểu hiện của máy tính bị nhiễm virus:

* Hệ thống hoạt động không ổn định.
* Các chương trình ứng dụng không thể hoạt động được hoạch hoạt động sai chức năng.
* Dữ liệu bị sai lệch.
* Kích thước các file tăng.
* Xuất hiện các file trên đĩa

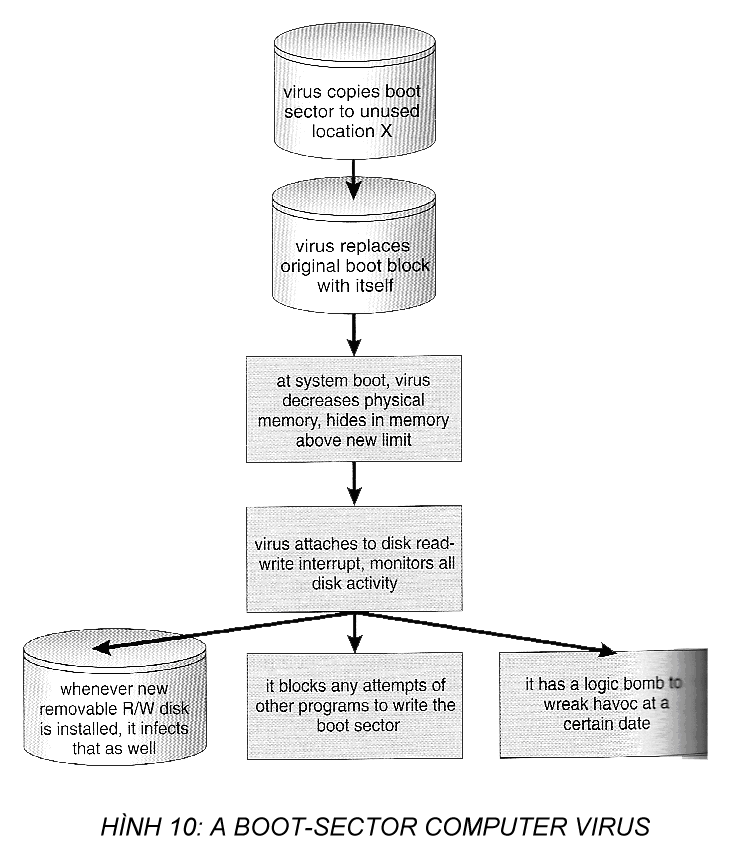
## Phân loại virus

Dựa vào cơ chế lây lan của virus, người ta có thể phân thành một số loại như sau:

* ***Boot virus (B- virus):*** là những virus chỉ lây lan vào các boot sector hoặc master boot record của các ổ đĩa.
* ***File (f- virus):*** là những virus lây lan vào các file chương trình của người sử dụng (các file com hoặc exe)
* ***Virus lưỡng tính (b/f virus):*** là những virus có thể lây lan vào các file chương trình.
* ***Maco virus:*** là những virus viết bằng các lệnh macro. chúng thường lây nhiễm vào các file văn bản hay các bảng tính…
* ***Trojan virus (Trojan horse):*** là những virus nằm tiềm ẩn trong hệ thống máy tính dưới dạng các chương trình ứng dụng
* ***Worm (sâu):*** trên thực tế không được coi là virus vì nó không gây tác hại cho phần mềm hay phần cứng. Nhiệm vụ chính của nó là thu thập các thông tin cá nhân của người sử dụng (mật khẩu tài khoản, các thông tin quan trọng, các tài liệu mật…) để chuyển về một địa chỉ nhất định cho người điều khiển.

## Cơ chế hoạt động của virus

Sau đây là sơ đồ mô tả cơ chế hoạt động của một loại virus khởi động điển hình:



Về cơ chế hoạt động của virus, chúng ta có thể hình dung quá trình như sau: Khi đọc một đĩa hoạch thi hành một chương trình bị nhiễm virus, nó sẽ tạo ra một bản sao đoạn mã của mình và nằm thường trú trong bộ nhớ máy tính. Khi đọc một đĩa hoạc một chương trình, đoạn mã virus nằm trong bộ nhớ sẽ kiểm tra đĩa/file đó đã tồn tại đoạn mã chưa? Nếu chưa thì tạo một bản sao khác lây nhiễm vào đĩa/file.

## Phòng tránh virus

### ***Các chương trình phòng tránh và phát hiện virus***

Coi thường sự tồn tại của virus là con đường trực tiếp dẫn đến sự mất an toàn cho hệ thống nhưng mặt khác.

Các phần mềm chống virus hiện nay chia thành hai loại:

* ***Các chương trình phòng ngừa:*** đây là các chương trình thường trú trong trong bộ nhớ của máy tính. Chúng hoạt động dựa vào sự giám sát thường xuyên các ngắt để để phát hiện và ngăn chặn các yêu cầu được điều khiển bằng phần mềm như: nạp chương trình, ghi thông tin vào đĩa…
* ***Các chương trình phát hiện:*** trong khi các chương trình phòng chống, ngăn chặn, giám sát các sự kiện xảy ra khi chương trình hoạt động thì các chương trình phát hiện lại tiến hành kiểm tra mã chương trình trước khi nó được thực hiện. Người sử dụng khi được nhắc nhở về các mối nguy hiểm khi có mã lạ trong chương trình của mình sẽ phải tự quyết định xem có nên dùng chương trình hay loại bỏ nó.

### ***Một số biện pháp phòng chống virus***

* Hạn chế trao đổi dữ liệu
* Hạn chế sử dụng các phần mềm phá khóa hoặc không rõ nguồn gốc
* Sử dụng thường xuyên các phần mềm phòng ngừa vào phát hiện virus
* Thay đổi các thuộc tính của file chương trình
* Cài đặt lại các chương trình ứng dụng
* Cài đặt lại hệ thống
* Tạo lại khuôn dạng cho đĩa từ
* Thường xuyên sao lưu dự phòng dữ liệu

# BẢO VỆ TRÊN WINDOWS

## Công cụ bảo vệ

### ***Firewall***

Tường lửa là một hệ thống an ninh mạng được thiết kế để ngăn chặn truy cập trái phép vào hoặc từ một mạng riêng.

Phương pháp bảo mật tốt nhất là sử dụng tường lửa, đặc biệt là đối với các doanh nghiệp có dữ liệu khách hàng bí mật cần bảo vệ. Kích hoạt tường lửa là quy trình và chính sách bảo mật phổ biến để bảo vệ hệ thống.

Có thể triển khai tường lửa trong cả phần cứng và phần mềm hoặc kết hợp cả hai. Thông thường, các doanh nghiệp sử dụng tường lửa mạng để ngăn người dùng Internet trái phép truy cập vào các mạng riêng được kết nối với Internet. Tường lửa đặc biệt quan trọng để bảo vệ mạng nội bộ. Tất cả các thông báo đi vào hoặc rời khỏi mạng nội bộ đều đi qua tường lửa, tường lửa này sẽ kiểm tra từng thông báo và chặn những thông báo không đáp ứng các tiêu chí bảo mật đã chỉ định.

Graphical user interface, text, application, email

Description automatically generatedKích hoạt: Mở **Control Panel** > **System and Security** > **Windows** **Firewall** > **Turn Windows Firewall on or off.** Sau đó chọn Turn on Windows Firewall

### ***Windows Defender***

Windows Defender Antivirus là một thành phần chống phần mềm độc hại trên Windows. Nó giúp bảo vệ máy tính và các tệp trên thiết bị khỏi vi-rút, phần mềm gián điệp, ransomware và một số loại phần mềm độc hại và tin tặc khác.

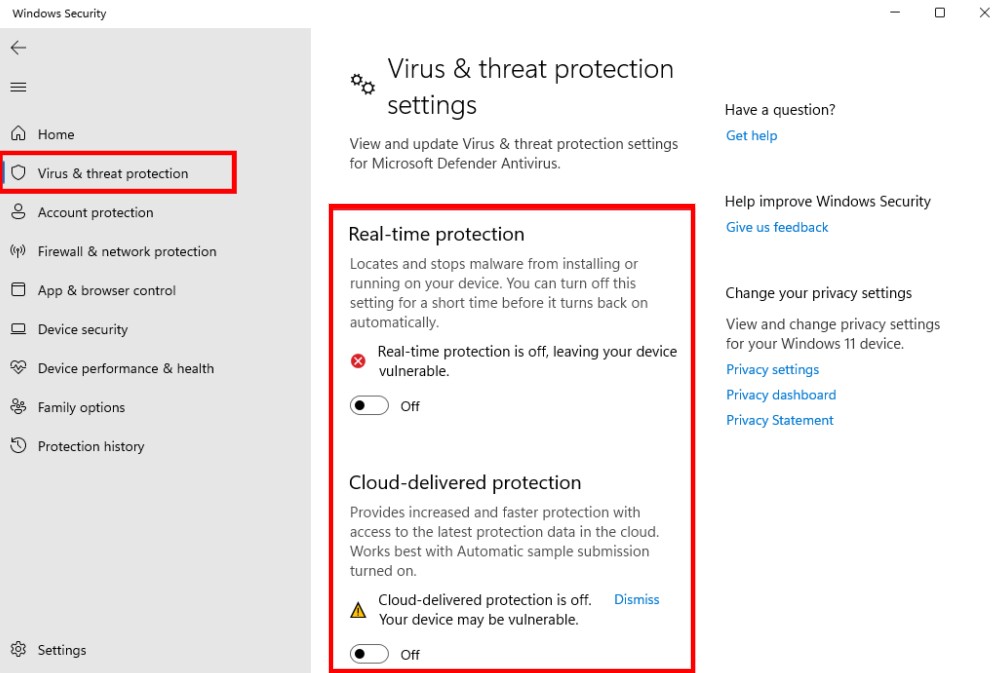
Windows Defender cung cấp khả năng bảo vệ theo thời gian thực và sẽ thực hiện quét tự động thường xuyên để tìm các thay đổi có thể do phần mềm gián điệp gây ra từ đó phát hiện ra vi-rút.

* Cách thiết lập

1. Mở **Start**

2. Tìm “**Windows Security**” và click vào kết quả đầu tiên để mở ứng dụng.

3. Click vào “**Virus & thread protection**“

4. Bên dưới “**Virus & thread protection settings**“, click vào phần  “**Manage settings**“

### ***Tamper Protection***

* Tamper Protection giúp ngăn chặn các ứng dụng độc hại thay đổi các cài đặt Microsoft Defender Antivirus quan trọng, bao gồm bảo vệ theo thời gian thực và bảo vệ đám mây.
* Thiết lập

1. Mở **Start**

2. Tìm “**Windows Security**” và click vào kết quả đầu tiên để mở ứng dụng.

3. Click vào “**Virus & thread protection**“

Graphical user interface, application

Description automatically generated4. Bên dưới “**Virus & thread protection settings**“, click vào phần  “**Manage setting.**

## Quyền người dùng

### **Quyền User Right**

1. ***Định nghĩa***

* Quyền User Right là quyền cấp cho user thực thi một số tác vụ trên hệ thống tức là một số quyền mà user được sử dụng trên server.

1. ***Một số quyền người dùng***

* Access this computer from the network: Quyền được truy cập vào server thông qua mạng.
* Act as part of the operating system: Quyền được thi hành một số phần của hệ điều hành.
* Add workstation to domain: Quyền được thêm trạm làm việc vào domain.
* Allow logon locally: Quyền được đăng nhập cục bộ.
* Allow log on through terminal Services: Quyền đăng nhập thông qua dịch vụ Terminal.
* Back up files and directories: Quyền sao lưu files và thư mục.
* Change the system time: Quyền thay đổi thời gian hệ thống.
* Deny log on locally: không được quyền đăng nhập cục bộ
* Shut down the system: Quyền tắt máy.

1. ***Thiết lập***

* Để biết quyền User Right có thể cấp cho người dùng là những quyền nào ta mở như sau: **Start** > **Administrative Tool** > **Domain Security Policy** > **Local Policy** > **User Rights Assignment**

Graphical user interface, text, application

Description automatically generated

* Để cấp quyền User Rights cho user hoặc group thì nhấp đúp vào quyền muốn chọn rồi

Graphical user interface, application

Description automatically generated

* Graphical user interface, application

  Description automatically generatedNhấn **Add User or Group:**
* Trên hộp thoại Add User or Group nhấp nút Browse làm xuất hiện hộp thoại Select Users, Computers, or Groups trên hộp thoại này nhấp nút Advanced rồi nhấp Find, nhấp chọn u1 trong hộp search results:

Graphical user interface, application

Description automatically generatedNhấp OK 3 lần để áp dụng và đóng hộp thoại này và trở về hộp thoại Allow log on locally properties

Graphical user interface, application

Description automatically generated

### **Quyền Permission**

Người dùng có 2 loại quyền truy cập đó là: Share và NTFS:

* Share: cấp quyền truy cập thư mục dùng chung
* NTFS: cấp quyền truy cập cho thư mục và tập tin

1. ***Một số đặc điểm quyền NTFS***

Quyền NTFS chỉ có thể được cấp trên volume được định dạng là NTFS.

Quyền truy cập NTFS cung cấp khả năng bảo mật cao hơn so với FAT và FAT32, vì chúng áp dụng cho thư mục và cho từng tập tin cá thể.

Quyền truy cập tập tin NTFS áp dụng cho cả những ngừơi làm việc tại máy tính lưu trữ dự liệu, lẫn người dùng truy cập thư mục hoặc tập tin qua mạng bằng cách kết nối tới thư mục dùng chung.

Có thể dùng quyền truy cập NTFS để bảo vệ tài nguyên khỏi người dùng có thể truy cập máy tính bằng 2 phương pháp sau:

+ Đăng nhập Cục bộ, ngồi ngay trước máy tính có tài nguyên đang thường trú.

+ Kết nối từ xa tới thư mục dùng chung.

* Có thể áp đặt nhiều cấp độ cho phép truy cập lên từng tập tin trong một thư mục.

Ví dụ:

+ Cho phép người này đọc và thay đổi nội dung của tập tin

+ Cho phép ngừoi kia chỉ được quyền đọc tập tin và không cho bất cứ ai trong nhóm người còn lại được truy cập dưới bất kì hình thức nào.

**Chú ý:**

* Khi một volume được định dạng NTFS thì Permission mặc định của Volume đó sẽ là group Everyone và có quyền Full ConTrol.
* Trên Volume NTFS khi bạn tạo 1 thư mục thì bạn sẽ sở hữu thư mục đó. Nếu người này thuộc group Administrator thì toàn bộ administrator sẽ sở hữu thư mục này.

1. ***Cách áp dụng quyền NTFS***

Quyền Truy Cập NTFS được cấp cho tài khoản người dùng hoặc cho tài khoản Group.

Ngừơi dùng có thể được cấp quyền truy cập 1 cách trực tiếp hoặc theo nhóm mà người này là thành viên trong nhóm. Nên cấp quyền truy cập thông qua nhóm.

Khác với quyền truy cập thư mục dùng chung, quyền truy cập NTFS bảo vệ tài nguyên cục bộ tức là có thể bảo vệ tài nguyên theo cấu trúc phân tầng trên máy tính mà người dùng đó đăng nhập cục bộ.

**Chú ý:** Nếu người dùng được cấp quyền Read với thư mục và quyền Write với tập tin trong thư mục đó thì người dùng vẫn có thể thay đổi nội dung của tập tin nhưng không thể tạo tập tin mới trong thư mục.

**Kết luận**:

* Quyền truy cập NTFS cung cấp mức độ bảo mật cao cho thư mục và từng tập tin trên những Volume đã được định dạng NTFS.
* Quyền truy cập NTFS áp dụng cả cho những người làm việc tại máy tính có lưu trữ tài nguyên và những người truy cập tài nguyên qua mạng.
* Quyền truy cập NTFS có thể cấp cho người dùng hoặc nhóm.
* Tương tự với quyền truy cập thư mục dung chung, cấp độ truy cập hiệu lực của ngừơi dùng là sự kết hợp với cá nhân hoặc group mà ngừoi đó là thành viên.
* Quyền truy cập NTFS có thể được cấp cho các thư mục và tài nguyên khác trong hệ thống mạng phân tầng.
* Quyền truy cập NTFS được ưu tiên trước các quyền truy cập khác áp cho thư mục hay tập tin đó.

1. ***Kết Hợp giữa Share và NTFS***
   1. Quyền Share

Muốn cho phép người dùng có thể truy cập tài nguyên qua mạng thì các thư mục chứa tài nguyên phải được share.

Khi một thư mục đã được share, bạn có thể bảo vệ thư mục bằng cách ấn định quyền truy cập thư mục dùng chung cho người sử dụng hoặc nhóm sử dụng theo mục đích thích hợp mà bạn đề ra. Tuy nhiên, quyền truy cập thư mục dùng chung sẽ cung cấp mức độ bảo mật giới hạn vì các lí do sau đây:

+ Cho phép người dùng truy cập mọi thư mục và tập tin trong phạm vi thư mục dùng chung với cùng cấp độ.

+ Không có hiệu lực khi người dùng ngồi ngay trước máy tính chứa tài nguyên và tìm cách truy cập tài nguyên trên máy này.

+ Không thể dùng để bảo vệ từng cá thể tập tin.

3.2 Quyền NTFS

Nếu thư mục dùng chung thường trú trên một volume NTFS, có thể dùng quyền truy cập NTFS để bảo vệ thư mục và tập tin.

Mức độ bảo mật thư mục và tập tin cao nhất bằng cách kết hợp quyền truy cập NTFS với quyền truy cập thư mục dùng chung….

Cách cấp quyền NTFS:

+ Nhấp phải chuột vào Folder hoặc File rồi chọn Properties rồi nhấp thẻ Security

Graphical user interface, application

Description automatically generated

+ Tại mục Group or User names: Chứa người dùng và nhóm được cấp quyền

+ Tại mục Permission: Là các quyền có thể cấp cho người dùng hoặc nhóm

+ Tương ứng với các quyền là 2 cột Allow là cho phép và Deny là cấm

+ Ngoài ra để cấp quyền truy cập đặc biệt nhấp nút Advanced:

Graphical user interface, text

Description automatically generated

# TÀI LIỆU THAM KHẢO

* *Nguyễn Thanh Hải, Giáo trình Nguyên Lý Hệ Điều Hành,2016*
* *Giáo trình Nguyên lý hệ điều hành*, Tác giả: ***Đặng Vũ Tùng***, Nhà Xuất Bản Hà Nội – 2005.
* *Giáo trình Nguyên lý hệ điều hành*, Tác giả: ***Hà Quang Thụy***, Nhà Xuất Bản Đại Học Quốc Gia.
* *Operating System Concepts 8th Edition*, Author: ***SilberschatZ, Galvin, Gagne***, Copyright © 2009 by ***John Wiley*** & ***Sons***, Inc.
* *Operating System Concepts Essential*, Author: ***SilberschatZ, Galvin, Gagne.***
* *Nguyên lý hệ điều hành*, Tác giả: ***Nguyễn Hải Châu***, Khoa Công Nghệ Thông Tin, Trường Đại Học Công Nghệ.
* [Customize exploit protection | Microsoft Docs](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/customize-exploit-protection?view=o365-worldwide&fbclid=IwAR350Rd5tWjegKMCShv904gwELsKnliey4JgMXjbAPdpxkYzARFOEShEAWk)
* [Stay protected with Windows Security (microsoft.com)](https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963?fbclid=IwAR36ogaHLIrVgrClObarBqHbh7JXUEfyeC2V5XtQqjhPss6ux1PNiPlopaE)
* [Hướng dẫn bật, tắt Windows Defender trên Win 7, Win 10 (activephanmem.com)](https://activephanmem.com/tat-windows-defender/?fbclid=IwAR0MT0lU9lzO1FEt6B_YcQnRHcjIqOxdcYxSNxpHbAF_mP877m1ajP6kFXA)
* [How Does Windows 10 Improve Security and Data Protection? - Custom Computer Specialists (customonline.com)](https://www.customonline.com/tech-insights/how-does-windows-10-improve-security-and-data-protection/?fbclid=IwAR1jur-r-pWGHMwjkris_wza_sfm372jwN78jXW6Sr__fN2cPteFjxL1IRs)
* [Cách bật hoặc tắt Device Guard trên Windows 10 - QuanTriMang.com](https://quantrimang.com/cach-bat-hoac-tat-device-guard-tren-windows-10-166013?fbclid=IwAR1jur-r-pWGHMwjkris_wza_sfm372jwN78jXW6Sr__fN2cPteFjxL1IRs)
* [Manage User Accounts and Settings in Windows 10 | Microsoft Press Store](https://www.microsoftpressstore.com/articles/article.aspx?p=2453566&seqNum=2&fbclid=IwAR04ImM1a5-_wtvWTUSFSO_8w2748GQHY6kEtpjJDWtco2QKSek7r6JWeE8)
* [Manage User Accounts and Settings in Windows 10 | Microsoft Press Store](https://www.microsoftpressstore.com/articles/article.aspx?p=2453566&seqNum=2&fbclid=IwAR2MNWTK4eNFYaB4qlr0Cmn2ALSdQvUhxCfYHWr56pYzsF9b6fqmpPntRks)
* [Manage User Accounts in Windows Server Essentials | Microsoft Docs](https://docs.microsoft.com/en-us/windows-server-essentials/manage/manage-user-accounts-in-windows-server-essentials?fbclid=IwAR1NUlh5VJ_buYmd_UGB83gPvuLn6h1UrUjAeC2jxPT_8NYXIceaaZ85Yk0)
* [Cách tạo tài khoản user mới trong Windows 10 đơn giản và nhanh chóng - Thegioididong.com](https://www.thegioididong.com/hoi-dap/tao-them-tai-khoan-nguoi-dung-tren-windows-10-686928?fbclid=IwAR3jCK6eTSvd-EV29jfmMrqWbecxO9Y-PI10NvoLTOzH7im3UuaM0-Enii8)
* [User Account Control security policy settings (Windows) - Windows security | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-security-policy-settings?fbclid=IwAR0tuAtwB76R4ksQxEYs-PJawMaKfM6wZwfiogeLX4guuz6DDXj89dTrStk)
* [5 cách tắt UAC (User Account Control) Windows 10 | Canhrau.com](https://canhrau.com/cach-tat-uac-windows-10/?fbclid=IwAR22Bp771y70hXSP0pyDAdvg63BcqdngAv9ReYB63Sr4VIC81vGleFDuYn4)
* [Prevent changes to security settings with Tamper Protection (microsoft.com)](https://support.microsoft.com/en-us/topic/prevent-changes-to-security-settings-with-tamper-protection-6fd8d8ff-0e6d-4df5-b994-ea4df20ca969?fbclid=IwAR0LDABZp1ZkzfaUHDg5cCsKxSA7rj4R5cUvOiWTzIcjGAg7-ZWUBAb_9yo)
* [Change User Rights Assignment Security Policy Settings in Windows 10 | Tutorials (tenforums.com)](https://www.tenforums.com/tutorials/88118-change-user-rights-assignment-security-policy-settings-windows-10-a.html?fbclid=IwAR2tKa2LU1OyLO5yCcG3toS13lEPDEGNTJcfw2-PurCyM_n8-iblKS1AJec)
* [[Tự học MCSA MCSE 2016] -Lab 12- Cấu hình Group Policy Object (GPO) trên Windows Server 2016 - ITFORVN](https://itforvn.com/tu-hoc-mcsa-mcse-2016-lab-12-cau-hinh-group-policy-object-gpo-tren-windows-server-2016/?fbclid=IwAR04ImM1a5-_wtvWTUSFSO_8w2748GQHY6kEtpjJDWtco2QKSek7r6JWeE8)

# KẾ HOẠCH THỰC HIỆN BÀI TẬP LỚN

Tên lớp: 20212IT602500 Khóa: K15

Tên nhóm: Nhóm

Họ tên thành viên của nhóm: Đàm Mạnh Đào, Lý Thị Dung, Lê Tiến Dũng, Đoàn Hữu Thành, Nguyễn Hữu Thịnh

Tên chủ đề: Nghiên cứu tìm hiểu về Hệ thống bảo vệ trong HĐH Windows.

|  |  |  |  |
| --- | --- | --- | --- |
| **Tuần** | **Người thực hiện** | **Nội dung công việc** | **Phương pháp thực hiện** |
| 6 | Cả nhóm | Tìm hiểu về bảo vệ hệ thống | Tìm tài liệu |
| 7 | Cả nhóm | Tìm hiểu về an toàn hệ thống | Tìm tài liệu |
| 8 | Cả nhóm | Tổng hợp nội dung chương 1 và chương 2 | Nghiên cứu + tổng hợp |
| 9 | Cả nhóm | Tìm hiểu và tổng hợp về nội dung virus máy tính | Nghiên cứu + tổng hợp |
| 10 + 11 | Đàm Mạnh Đào | Tìm hiểu và viết nội dung về Firewall | Tìm tài liệu + tổng hợp + thực hành |
| Lý Thị Dung | Tìm hiểu và viết nội dung về Windows Defender | Tìm tài liệu + tổng hợp + thực hành |
| Lê Tiến Dũng | Tìm hiểu và viết nội dung về Tamper Protection | Tìm tài liệu + tổng hợp + thực hành |
| Đoàn Hữu Thành | Tìm hiểu và viết nội dung về quyền User Right | Tìm tài liệu + tổng hợp + thực hành |
| Nguyễn Hữu Thịnh | Tìm hiểu và viết nội dung về quyền Permission | Tìm tài liệu + tổng hợp + thực hành |
| 12 | Cả nhóm | Tổng hợp nội dung chương 4 | Phân tích + Tổng hợp |
| 13 | Cả nhóm | Chốt lại vấn đề và đưa ra nhận xét | Phân tích tổng hợp kinh nghiệm |

Ngày tháng năm 2022

Giảng viên

*Nguyễn Thanh Hải*

# PHIẾU HỌC TẬP NHÓM

**I. Thông tin chung**

1. Tên lớp: 20212IT6025008 - Khóa: K15

2. Tên nhóm: 09

3. Họ và tên thành viên trong nhóm: Đàm Mạnh Đào, Lý Thị Dung, Lê Tiến Dũng, Đoàn Hữu Thành, Nguyễn Hữu Thịnh

**II. Nội dung học tập**

1. Tên chủ đề: Nghiên cứu tìm hiểu về Hệ thống bảo vệ trong HĐH Windows.

2. Hoạt động của sinh viên

- Hoạt động/Nội dung 1: Tìm hiểu và tổng hợp nội dung bảo vệ hệ thống

- Hoạt động/Nội dung 2: Tìm hiểu và tổng hợp nội dung an toàn hệ thống

- Hoạt động/Nội dung 3: Tìm hiểu và tổng hợp nội dung virus máy tính

- Hoặt động/Nội dung 4: Tìm hiểu, tổng hợp và thực hành về bảo vệ trên windows

**III. Nhiệm vụ học tập**

1. Hoàn thành báo cáo bài tập lớn theo đúng thời gian quy định

2. Báo cáo sản phầm nghiên cứu được giao trước giảng viên và các sinh viên khác.

**IV. Học liệu sử dụng cho bài tập lớn**

1. Tài liệu học tập:

- *Nguyễn Thanh Hải, Giáo trình Nguyên Lý Hệ Điều Hành,2016*

*- Giáo trình Nguyên lý hệ điều hành*, Tác giả: ***Đặng Vũ Tùng***, Nhà Xuất Bản Hà Nội-2005.

*- Giáo trình Nguyên lý hệ điều hành*, Tác giả: ***Hà Quang Thụy***, Nhà Xuất Bản Đại Học Quốc Gia.

*- Nguyên lý hệ điều hành*, Tác giả: ***Nguyễn Hải Châu***, Khoa Công Nghệ Thông Tin, Trường Đại Học Công Nghệ.

- Tài liệu điện tử trên internet.