BỘ TÀI CHÍNH
TRƯỜNG ĐẠI HỌC TÀI CHÍNH - MARKETING

Chương 2
AN TOÀN VÀ BẢO MẬT THÔNG TIN TRÊN CÁC HỆ ĐIỀU HÀNH MÁY TÍNH CÁ NHÂN

GV:TS. Trương Thành Công – Email:ttcong@ufm.edu.vn

Nội dung

- Giới thiệu tổng quan
- Một số vấn đề ATBM trên PC
- ATBM qua bức tường lửa
- ATBM thông qua group policy
- ATBM thông qua registry
- ATBM thông tin cấp vật lý

Giới thiệu tổng quan

- Giới thiệu về hệ điều hành
- Các biện pháp ATBM trên hệ điều hành
  - Bảo vệ bộ nhớ
  - Bảo vệ tập tin
  - Điều khiển truy cập

Giới thiệu tổng quan
Giới thiệu về HĐH

Giới thiệu về hệ điều hành

- Hệ điều hành (tiếng Anh: Operating System - viết tắt: OS) là một phần mềm hệ thống dùng để điều hành, quản lý toàn bộ tất cả thành phần (bao gồm cả phần cứng và phần mềm) của thiết bị điện tử.
- Có vai trò trung gian trong việc giao tiếp giữa người sử dụng và thiết bị.

Giới thiệu tổng quan
Giới thiệu về HĐH

- Tất cả các hệ điều hành đều có khả năng đều cung cấp các chức năng an toàn. Vd:
- Tự bảo vệ mã chương trình bằng cách chạy mã này trong một vùng an toàn mà chỉ có HĐH đó được phép sử dụng
- Tự động tắt các phần mềm có lỗi hoặc phần mềm sai chức năng

Giới thiệu tổng quan
Giới thiệu về HĐH

Các yêu cầu cơ bản với ATBM HĐH

ATBM HĐH được quan tâm do các chương trình trong máy tính hiện đại tương tác với nhau theo nhiều cách và việc chia sẻ dữ liệu giữa các người dùng là hành vi căn bản và phổ biến với hệ thống máy tính.

Thách thức với việc thiết kế an toàn cho hệ điều hành là thiết kế các cơ chế an toàn để bảo vệ việc thực thi của các chương trình và dữ liệu của chúng trong môi trường phức tạp.

Giới thiệu tổng quan
Giới thiệu về HĐH

An toàn bảo mật hệ điều hành được tiếp cập theo hai hướng chủ yếu:

- Hệ thống có ràng buộc
- Hệ thống dùng chung (general-purpose)

Giới thiệu tổng quan
Giới thiệu về HĐH

Mục tiêu ATBM HĐH

Mục tiêu ATBM HĐH phải thỏa mãn 3 yếu tố**: tính bảo mật, tính toàn vẹn, tính khả dụng.**

Việc truy cập hệ thống có thể được mô tả bằng cácchủ thể (chương trình/người dùng) có thể thực hiện các thao tác lên các đối tượng (file/folder/hardware/socket)

Giới thiệu tổng quan

Giới thiệu về HĐH

- Tính bảo mật: giới hạn các đối tượng có thể được truy cập
- Tính toàn vẹn: hạn chế việc ghi, xóa lên các đối tượng
- Tính khả dụng: hạn chế các tài nguyên mà các chủ thể có thể sử dụng

Mục tiêu ATBM HĐH dựa trên nguyên tắc cấp quyền tối thiểu (least privilege)

Giới thiệu tổng quan
Bảo vệ bộ nhớ

- Bộ nhớ là nơi thực thi chương trình
- Có 2 cách ngăn chặn can thiệp vào không gian bộ nhớ
  - Phân đoạn (Segmentation)
  - Phân trang (Paging)

Giới thiệu tổng quan
Bảo vệ bộ nhớ

Phân đoạn (Segmentation):

- Phân chia chương trình thành các đoạn, tương ứng với các đoạn dữ liệu, các chương trình con, mỗi đoạn có quyền khác nhau (R,W,E)
- Phân chia bộ nhớ vật lý thành các đoạn, tương ứng với các mảng dữ liệu người dùng hoặc các đoạn mã chương trình. Mỗi đoạn có một tên duy nhất <Name,Offset>, hệ điều hành phải duy trì một bảng các đoạn

Giới thiệu tổng quan
Bảo vệ bộ nhớ

Phân trang (paging):

- Phân chia ct thành các trang (page) cùng kích thước
- Phân chia bộ nhớ vật lý thành các khung trang (page frame) cùng kích thước 512 đến 4096 byte
- Mỗi trang có một tên duy nhất <Page,Offset>, hệ điều hành phải duy trì một bảng các trang.

Giới thiệu tổng quan
Bảo vệ bộ nhớ

Kết hợp phân đoạn & phân trang

- Ưu điểm của phân đoạn: bảo vệ bộ nhớ bằng cách phân quyền, hệ điều hành kiểm soát việc quyền đọc/ghi/thực hiện trên bộ nhớ
- Ưu điểm của phân trang: tốc độ

➔ Các HĐH hiện đại kết hợp cả phân đoạn và phân trang

Giới thiệu tổng quan

Bảo vệ tập tin

Mục tiêu của hệ điều hành là giữ an toàn cho dữ liệu của người dùng khỏi bị truy cập trái phép.

- Cơ chế bảo vệ bằng cách giới hạn các kiểu truy cập vào file của người dùng.
- Các loại truy cập vào file: Read, Write, Execute, Append, Delete, List
- Cơ chế khác: sử dụng mật khẩu, mã hóa tập tin

Giới thiệu tổng quan
Bảo vệ tập tin

Hệ điều hành phân loại quyền truy cập tập tin/thư mục thành 3 nhóm:

- Owner: chủ sở hữu, người tạo ra tập tin/thư mục
- Group: một nhóm user có một số quyền nhất định trên tập tin/thư mục
- Các loại user khác

Giới thiệu tổng quan

Điều khiển truy cập(Access Control)

Trong HĐH có rất nhiều đối tượng có thể truy cập:

- File, Folder
- Phần cứng
- Bộ nhớ
- Thông tin hệ thống
- …

➔ Vấn đề đặt ra: ai được truy cập với quyền gì

Giới thiệu tổng quan

Điều khiển truy cập(Access Control)

Điều khiển truy cập là một chính sách, được sự hỗ trợ của phần mềm hay phần cứng được dùng để cho phép hay từ chối truy cập đến tài nguyên, qui định mức độ truy xuất đến tài nguyên. Có ba mô hình được sử dụng để giải thích cho mô hình điều khiển truy cập:

- DAC (Discretionary Access Control)
- RBAC (Role Based Access Control)
- MAC (Mandatory Access Control)

Giới thiệu tổng quan

Điều khiển truy cập(Access Control)

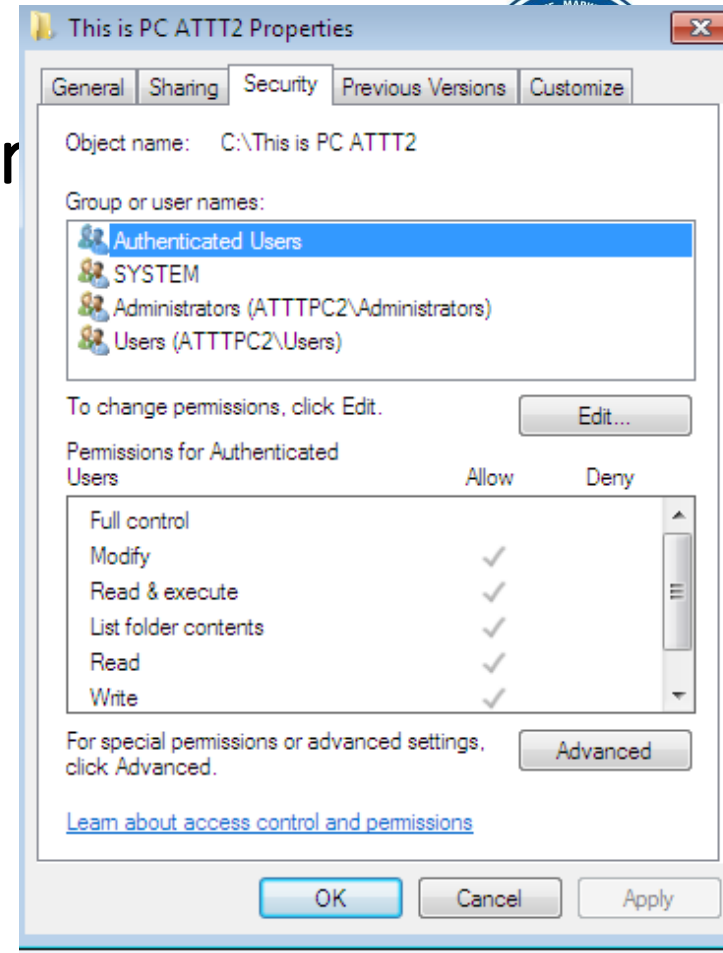
DAC (Discretionary Access Control)

- Là tập các quyền truy cập trên một đối tượng mà một người dùng hay một ứng dụng định nghĩa
- Cho phép người dùng chia sẻ đối tượng và sử dụng đối tượng do người khác chia sẻ.
- thiết lập một danh sách điều khiển truy cập (Access control list) dùng để nhận ra người dùng nào được quyền truy cập đến tài nguyên nào

Giới thiệu tổng quan

Điều khiển truy cập(Access Contr

Ví dụ về DAC: cơ chế quản lý file/folder trong Windows



Giới thiệu tổng quan

Điều khiển truy cập(Access Control)

RBAC (Role Based Access Control)

- việc quyết định quyền truy cập dựa trên vai trò của mỗi cá nhân và trách nhiệm của họ trong tổ chức
- Quyền hạn dựa trên công việc và phân nhóm người dùng
- Tuỳ thuộc vào từng quyền hạn của người dùng mà sẽ phân quyền cho phù hợp

Giới thiệu tổng quan

Điều khiển truy cập(Access Control)

RBAC (Role Based Access Control)

- Tạo cơ hội thực hiện nguyên tắc 'đặc quyền ít nhất'. Tức chỉ cung cấp cho một cá nhân quyền truy cập cần thiết để thực hiện công việc của họ
- Vd: Người quản trị có toàn quyền, user chỉ có quyền sử dụng
- Cơ chế Groups trong HĐH Windows

Giới thiệu tổng quan

Điều khiển truy cập(Access Control)

MAC (Mandatory Access Control)

- Trong môi trường MAC, quyền truy cập vào các đối tượng tài nguyên được kiểm soát bởi các cài đặt do quản trị viên hệ thống xác định. Điều này có nghĩa là quyền truy cập vào các đối tượng tài nguyên được điều khiển bởi hệ điều hành dựa trên những gì người quản trị hệ thống đã định cấu hình trong cài đặt. Người dùng không thể thay đổi quyền kiểm soát truy cập của một tài nguyên.

Một số vấn đề ATBM trên PC

Command Line

Kẻ tấn công:

- Hiếm khi có quyền truy cập vào Graphical User Interface (GUI)
- Thay vào đó, họ sử dụng “command shell”

Người phòng thủ

- Sử dụng command line sẽ nhanh hơn
- Dễ dàng tự động hóa và thực hiện theo kịch bản (scripted)

Một số vấn đề ATBM trên PC
Command Line

Các tùy chọn command line trong Windows:

- Command Prompt
  - Khởi chạy bằng tập tin cmd.exe
- PowerShell
  - Khởi chạy bằng tập tin powershell.exe
- Cú pháp tìm hiểu một command <tên command > /?

Một số vấn đề ATBM trên PC

Command Line – **cơ bản**

Liệt kê tập tin và thư mục với **dir**

- Liệt kê thư mục hiện hành : dir
- Liệt kê ổ đĩa hiện hành: dir \
- Liệt kê thư mục con: dir subdir1
- Liệt kê ổ đĩa khác: dir d: or dir d:\
- Liệt kê tập tin: dir *.exe
- Liệt kê thư mục cha: dir ..
- Liệt kê thư mục ẩn: dir /ah

Một số vấn đề ATBM trên PC

Command Line – **cơ bản**

Chuyển thư mục: **cd**

- về thư mục gốc : cd \
- vào thư mục con: cd myfolder
- về thư mục cha: cd ..
- vào thư mục có khoảng trắng: cd "My Documents"
- vào thư mục có tên dài: cd my*

Một số vấn đề ATBM trên PC

Command Line – **cơ bản**

- Tạo thư mục **md <tên thư mục> hoặc mkdir**
  - Vd: md myfolder
- Xóa thư mục **rd <tên thư mục>**
  - Lưu ý: không thể xóa thư mục có chứa nội dung bằng rd

Một số vấn đề ATBM trên PC

Command Line – **cơ bản**

- Tạo tâp tin rỗng (dạng txt) type nul > <tên tập tin>
- Xóa file: del <tên file>
- Di chuyển tập file move
- Sao chép: copy <tên> <tên mới>
- Đổi tên: ren <tên> <tên mới>
- Xem nội dung file (chỉ file txt): type <tên.txt>
- Đặt thuộc tính ẩn: attrib <tên> +h
- Bỏ thuộc tính ẩn: attrib <tên> -h

Một số vấn đề ATBM trên PC

Command Line – **cơ bản**

- Xem tên máy tính: **hostname**
- Xem các process đang hoạt động: **tasklist**
  - Có thể lọc danh sách bằng /fi
- Ngừng process: **Taskkill**
  - Thường sử dụng với /PID (process ID) hoặc /IM (image name)

Một số vấn đề ATBM trên PC
Command Line – cơ bản

- Xem các process đang hoạt động: **tasklist**
  - Có thể lọc danh sách bằng /fi
- Ngừng process: **taskkill**
  - Thường sử dụng với /PID (process ID) hoặc /IM (image name)

Một số vấn đề ATBM trên PC
Command Line – mạng

- Xem cấu hình mạng: **ipconfig**
  - Dùng với /all để xem tất cả tham số
- Xem các thông tin kết nối mạng: **netstat**
  - Thường dùng với –ano để liệt kê tất cả tất cả kết nối đang hoạt động, port…

Một số vấn đề ATBM trên PC
Command Line – mạng

- Lệnh ping : **ping**
  - Có thể dùng địa chỉ IP, hoặc DNS
  - ICMP Echo-Request và EchoReply phải được cho phép mới có thể ping
- Lệnh **tracert:** xác định đường đi từ nguồn tới đích của một gói tin.

Một số vấn đề ATBM trên PC
Command Line – mạng

Nslookup

- Lấy thông tin về các máy chủ internet bằng cách truy vấn hệ thống tên miền (DNS).
  - Vd: nslookup
  - nslookup thanhnien.vn

Một số vấn đề ATBM trên PC
Command Line – mạng

Kiểm tra file hệ thống **sfc**

- Vd: sfc /scannow

Một số vấn đề ATBM trên PC

File system

Windows File system:

+ Hệ điều hành: thường đặt tại đĩa C

+ Thư mục gốc: C: hoặc C:\

+ Các ổ đĩa sử dụng các ký tự alphabet

+ Ổ đĩa mạng có thể được sử dụng và map trên hệ thống

Một số vấn đề ATBM trên PC

File system

Cơ chế bảo vệ trong Windows:

+ Mandatory Integrity Controls (MIC)

- ✓ System
- ✓ High
- ✓ Medium
- ✓ Low

Một số vấn đề ATBM trên PC

File system

Cơ chế bảo vệ trong Windows:

+ File Discretionary Access Control Lists

Full Control	Write Attributes
Traverse Folder/Execute File	Write Extended Attributes
List Folder/Read Data	Delete
Read Attributes	Delete subfolders and files
Read Extended Attributes	Read Permissions
Create Files/Write Data	Change Permissions
Create Folders/Append Data	Take Ownership

Một số vấn đề ATBM trên PC

File system

Microsoft cung cấp cho ta bộ quyền NTFS (NTFS Permission) để thiết lập quyền trên dữ liệu đối với user:

+ NTFS permission gồm có các đặc tính sau:

– Tính thừa kế: quyền của folder cha thế nào thì khi tạo folder con sẽ có quyền tương tự.

– Tác động lên cả file và folder.

– Tác động lên Network Access (truy cập qua mạng) và Local Access.

Một số vấn đề ATBM trên PC

File system

NTFS permission gồm 2 nhóm chính:

- Standard permission
  - Gồm 6 quyền
- Special permission
  - Gồm 14 quyền

Một số vấn đề ATBM trên PC

File system

Standard permission gồm 6 bộ quyền:

1. Read: cho phép user đọc nội dung file.
2. List folder contents: liệt kê nội dung folder (user có thể mở folder để xem có các file, sub folder nào trong đó).
3. Read and execute: Có thể đọc nội dung các file (file *.docx, pptx. xlsx v.v) và thực thi các file nếu file đó là chương trình (.exe, .bat v.v).

Một số vấn đề ATBM trên PC
File system

4. Write: chỉnh sửa, tạo mới dữ liệu.

+ Nếu user có quyền write trên file thì user có thể chỉnh sửa dữ liệu, nếu là folder thì có thể tạo mới các đối tượng trong folder, chép dữ liệu vào folder. Nhưng không thể xóa các đối tượng.

5. Modify: bằng các quyền ở trên gộp lại và thêm quyền delete (đọc, chỉnh sửa, xóa các đối tượng).

Một số vấn đề ATBM trên PC

File system

6. Full control: gồm

+ Modify

+ Quyền change permission (cho phép thiết lập lại các bộ quyền).

+ Quyền: Take Ownership

Một số vấn đề ATBM trên PC

File system

Special permission: gồm 14 quyền

1. Full control: toàn quyền, giống Full control của standar permission

2. Traverse folder/ execute file: Quyền thực thi file + quyền đi vào folder,

3. List folder / Read data: Vào thư mục và đọc dữ liệu trên thư mục đó.

Một số vấn đề ATBM trên PC

File system

4. Read Attributes: đọc thuộc tính folder và file (Read only, Hiden v.v).

5. Read Attributes: đọc thuộc tính mở rộng (Archive, Encrypt).

6. Create file/ Write data: tạo file và ghi, chỉnh sửa dữ liệu.

Một số vấn đề ATBM trên PC

File system

7. Create folder/ Append data:

– Cho phép tạo folder

– Ghi ghi dữ liệu vào phía cuối file (ghi nối tiếp) , chứ không xóa, chỉnh sửa phần dữ liệu sẵn có (chỉ áp dụng cho file).

8. Write Attributes: Cho phép thay đổi các thuộc tính của file, folder (read-only, hiden).

Một số vấn đề ATBM trên PC
File system

9. Write Extended Attributes: Cho phép chỉnh sửa các thuộc tính mở rộng của file, folder. Thuộc tính mở rộng được xác định bởi các chương trình (program), các chương trình khác nhau có các thuộc tính mở rộng khác nhau.

10. Delete Subfolders and files: Xóa các folder con và các file.

Một số vấn đề ATBM trên PC

File system

11. Delete: Cho phép xóa tài nguyên (folder, subfolder, file).

12 Read permission: cho phép user, group thấy các quyền hạn

13. Change permission: Cho phép thay đổi các quyền hạn đối vôi file, folder.

14. Take Ownership: Cho phép lấy quyền sở hữu file, folder của người khác.

Một số vấn đề ATBM trên PC
Local Users and Groups

- User và Group là những thành phần cơ bản để quản lý máy tính và tài nguyên trên máy tính. Tùy vào mức độ được cấp quyền mà người dùng có quyền truy xuất vào những tài nguyên nào trên máy tính, hoặc trong hệ thống mạng.
- Trong phạm vi của chương này ta tìm hiểu về cách tạo và quản lý user trên máy cục bộ (local host).

Một số vấn đề ATBM trên PC

Local Users and Groups

- Đây là hệ thống quản lý người dùng (User) và nhóm người dùng (Group) của Windows và Windows server (chưa dựng Domain).
- Trong trường hợp Windows server chưa lên Domain thì chúng hoạt quản lý user và Group như Windows workstation. Khi đã nâng cấp lên Domain thì Local user and group không hoat động nữa, thay vào đó là Active Directory User and Computer

Một số vấn đề ATBM trên PC
Local Users and Groups

- User account là thông tin đối tượng bao gồm thông tin xác định người dùng của hệ điều hành Windows, dùng để đăng nhập vào máy tính, phân quyền sử dụng tài nguyên, áp đặt những chính sách bảo mật
- Thông tin tối thiểu của User account là User name và Password.

Một số vấn đề ATBM trên PC
Local Users and Groups

- Local user account (người dùng cục bộ): Là tài khoản được lưu trong file SAM (Security Account Manager).
- Nó chỉ có giá trị trên máy chứa thông tin tài khoản đó.

Một số vấn đề ATBM trên PC
Local Users and Groups

- Có hai user account được tạo sẵn (Built-in account) là Administrator và Guest.
- Tài khoản Aministrator là tài khoản có quyền cao nhất trong hệ thống.
- Tài khoản Guest thường bị Disable.

Một số vấn đề ATBM trên PC
Local Users and Groups

- Built-in account không thể xóa, nhưng có thể disable. Riêng user Administrator bị disabale thì vẫn có thể login vào chế độ Safe Mode, vì vậy việc tạo Password của user này là rất quan trọng để bảo mật cho hệ thống.

Một số vấn đề ATBM trên PC
Local Users and Groups

- Group (nhóm người dùng) Là tập hợp những user account có những tính chất nào đó (như có quyền làm gì, trên tài nguyên nào của hệ thống…) để giúp cho việc phân quyền trở nên dễ dàng hơn.
- Local group (nhóm người dùng trên máy cục bộ): Là nhóm chỉ có giá trị trên máy chứa nó và được lưu trữ trong file SAM

Một số vấn đề ATBM trên PC
Local Users and Groups

- Member của group có thể là group hoặc user.
- Chỉ nên cho phép user nào có quyền quản trị thuộc Group Administrators, tất cả các user còn lại nên thuộc Group Users hoặc các Group khác.
- User có thể đồng thời là member của nhiều group khác nhau.

Một số vấn đề ATBM trên PC
Local Users and Groups

- Để phân quyền trên tài nguyên chia sẻ thì người ta phân quyền cho group, những user thành viên trong group đó sẽ được thừa hưởng quyền từ group mà nó thuộc về.
- User và group trong Local user and Group chỉ có giá trị trên máy và tài nguyên trên chính máy chứa nó.

Một số vấn đề ATBM trên PC
Local Users and Groups

- Cách mở (Win 7)
  - R. Click My computer/ Manage/ System tools -> / Local User and Group
  - Win + R / nhập lusrmgr.msc /Enter
  - Command line/ lusrmgr/ Enter

Một số vấn đề ATBM trên PC
Local Users and Groups

Các thao tác trên user

- Thêm user, xóa user
- Đổi password
- Disable user

Các thao tác trên group

- Thêm group
- Xóa group
- Thêm user vào group

Một số vấn đề ATBM trên PC

User Account Control

User Account Control hay còn gọi là UAC, là một phần trong hệ thống bảo mật Windows. UAC ngăn chặn các ứng dụng thực hiện các thay đổi không mong muốn trên máy tính.

Một số vấn đề ATBM trên PC

User Account Control

Khi một phần mềm nào đó cố gắng thay đổi hệ thống - liên quan đến một phần Registry hoặc các tập tin hệ thống, Windows sẽ hiển thị hộp thoại xác nhận UAC. Nếu muốn thực hiện các thay đổi này người dùng có thể xác nhận.

Một số vấn đề ATBM trên PC

Phần mềm chống virus

Microsoft Defender là một phần mềm diệt virus cung cấp một loạt các tính năng bảo mật quan trọng tích hợp sẵn với hệ điều hành Windows 10.

- Đối với Windows 7/8: Tải về từ Website của Microsoft

Một số vấn đề ATBM trên PC

Phần mềm chống virus

Khởi động:

Start →Settings → Update & Security → Windows Security → Virus & threat protection

+ Với phiên bản cập nhật: chọn Scan option

+ Với phiên bản cũ hơn: Run a new advanced scan

Một số vấn đề ATBM trên PC

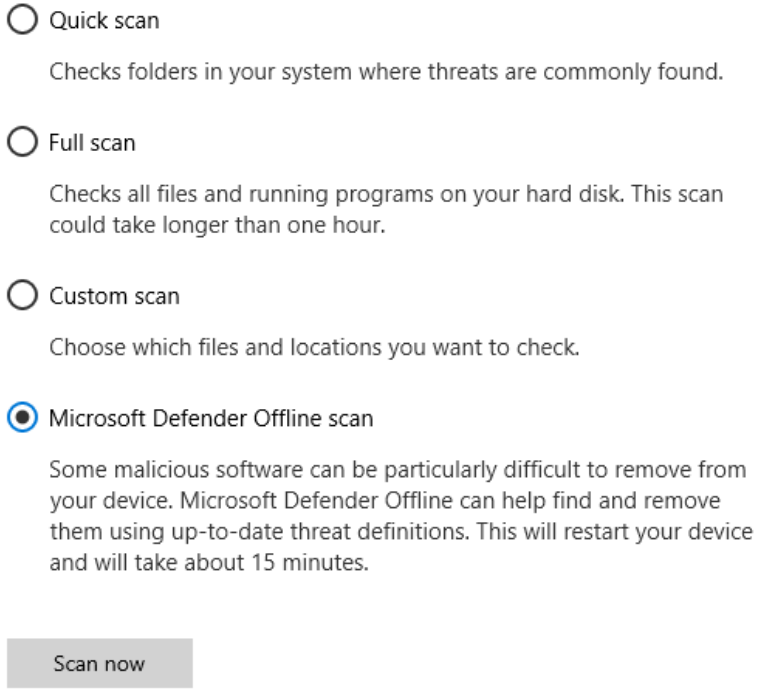
Phần mềm chống virus

Quét nhanh

Quét toàn bộ

Quét theo yêu cầu

Quét offline



Một số vấn đề ATBM trên PC

Phần mềm chống virus

Xem kết quả quét:

+ Với phiên bản cập nhật: vào mục Protection history

+ Với phiên bản cũ hơn: Threat history

Một số vấn đề ATBM trên PC

Task Manager

Task manager là chương trình được sử dụng để cung cấp các thông tin về các tiến trình (processes) và các chương trình (applications) đang chạy trên máy tính, cũng như tình trạng chung của máy tính. Nó cũng có thể để ép dừng một tiến trình hay thay đổi độ ưu tiên của từng tiến trình.

Một số vấn đề ATBM trên PC

Task Manager

Khởi động

- Task Manager
  - Ctrl + Shift + ESC
  - Ctrl + Alt + Del → Task Manager
  - Window + R, nhập **taskmgr** sau đó nhấn Enter
  - Right click Task bar → Task Manager

Một số vấn đề ATBM trên PC

Task Manager

Các thành phần trong Task Manager (tùy phiên bản)

- Processes
- Performance
- Start up
- ….

Một số vấn đề ATBM trên PC
MS config

- Msconfig còn được gọi là Tiện ích cấu hình hệ thống (System Configuration Utility). Msconfig được sử dụng để cấu hình cách máy tính khởi động cũng như những chương trình và dịch vụ tải khi Windows khởi động.
- Microsoft Config
  - Windows + R → nhập msconfig

Một số vấn đề ATBM trên PC
MS config

- Tab General là tab mặc định trong cấu hình Hệ thống và hiển thị phương pháp khởi động máy tính
- Tab Startup: các chương trình khởi động cùng HĐH
- Tab Tools: liệt kê một số công cụ quản trị Windows

Một số vấn đề ATBM trên PC
Backup & Restore

- Cho phép sao lưu và phục hồi hệ thống
  - Backup: sao lưu
  - Restore: phục hồi

Một số vấn đề ATBM trên PC
Hidden share

Mặc định các ổ đĩa của Windows sẽ được share ẩn (có ký tự $ sau tên ổ đĩa)

Cách xem

net view \\tên máy /all

Cách vô hiệu hóa

net share <tên share>$ /delete /y

Fire wall
Khái niệm

Khái niệm: Tường lửa (Firewall) là một hệ thống an ninh mạng, có thể dựa trên phần cứng hoặc phần mềm, sử dụng các quy tắc để kiểm soát luồng thông tin vào, ra khỏi hệ thống.

Firewall tạo thành một rào cản giữa mạng tin cậy và mạng không đáng tin cậy.

Fire wall
Tác dụng

Là phương pháp hiệu quả để bảo vệ hệ thống hoặc mạng lưới hệ thống cục bộ khỏi các mối đe dọa bảo mật khi truy cập vào thế giới bên ngoài thông qua mạng diện rộng và Internet

- Hardware firewall: là các phần cứng chuyên dụng, thiết kế để làm chức năng Firewall.

- Software firewall: là các phần mềm đóng vai trò bảo vệ hệ thống.
- Vd: Windows Firewall…

Fire wall
Nhiệm vụ

- Cho phép hoặc vô hiệu hóa các dịch vụ truy cập ra bên ngoài, đảm bảo thông tin chỉ có trong mạng nội bộ.
- Cho phép hoặc vô hiệu hóa các dịch vụ bên ngoài truy cập vào trong.
- Phát hiện và ngăn chặn các cuộc tấn công từ bên ngoài.
- Hỗ trợ kiểm soát địa chỉ truy cập
- Kiểm soát truy cập của người dùng..

Fire wall

Nhiệm vụ (tt)

- Hỗ trợ kiểm soát nội dung thông tin và gói tin lưu chuyển trên hệ thống mạng.
- Lọc các gói tin dựa vào địa chỉ nguồn, địa chỉ đích và số Port (hay còn gọi là cổng), giao thức mạng.
- Người quản trị có thể biết được kẻ nào đang cố gắng để truy cập vào hệ thống mạng.
- Bảo vệ tài nguyên của hệ thống trước các mối đe dọa bảo mật.

Fire wall
Nhiệm vụ (tt)

- Cân bằng tải: có thể sử dụng nhiều đường truyền internet cùng một lúc, việc chia tải sẽ giúp đường truyền internet ổn định hơn rất nhiều.
- Tính năng lọc ứng dụng cho phép ngăn chặn một số ứng dụng

Group policy
Giới thiệu

- Group policy là các nhóm chính sách áp dụng dụng cho tài khoản người dùng và máy tính trong hệ thống mạng Windows.
- Cung cấp cho người quản trị khả năng cấu hình và quản lý một cách tập trung về hệ điều hành, ứng dụng, và các thiết lập trên user

Group policy
Giới thiệu (tt)

- Group Policy được chia làm hai phần, được áp dụng cho hai đối tượng là User và Computer, hai phần này là độc lập và không ảnh hưởng đến nhau.
- Các Group Policy áp dụng cho User thì sẽ không ảnh hưởng đến đối tượng là Computer và ngược lại.

Group policy
Giới thiệu (tt)

- Để thiết lập các chính sách trên Local Group Policy thì user thực hiện phải là user thuộc nhóm Admin trên chính máy tính đó.
- Trên Local Group Policy, chỉ có thể thiết lập một chính sách duy nhất trên máy tính. Mọi user khi truy cập đều sẽ bị chi phối bởi chính sách này.

Group policy
Khởi động & thiết lập

Khởi động

- Win + R / gpedit.msc
- Command line / gpedit
- Khởi động thông qua mmc

Thiết lập

- Sau khi thiết lập xong chính sách phải thực hiện: gpupdate /force
- Một số trường hợp phải restart

Group policy
Một số chính sách ATBM

- **Theo dõi đăng nhập tài khoản**
  - Computer Configuration / Windows Settings / Security Settings / Local Policies / Audit Policy/ Audit logon events
  - Theo dõi bằng Windows Event Viewer:
    - Windows + R / eventvwr
    - Trong cửa sổ Event viewer chọn Windows Logs / Security

Group policy
Một số chính sách ATBM

- **Chặn truy cập Control Panel**
  - User Configuration / Administrative Templates / Control Panel
  - Prohibit access to the Control Panel / Enable

Group policy
Một số chính sách ATBM

- **Ngăn chặn người dùng khác cài đặt phần mềm mới trên hệ thống**

Computer Configuration / Administrative Templates / Windows Components / Windows Installer

Disable Windows Installer / Enable

Group policy
Một số chính sách ATBM

- **Vô hiệu hóa truy cập các thiết bị lưu trữ di động**

User Configuration / Administrative Templates / System / Removable Storage Access / Removable Disks: Deny read access / Enable

Group policy
Một số chính sách ATBM

- **Ngăn một ứng dụng cụ thể**

User Configuration / Administrative Templates / System / Don’t run specified Windows applications

/ Enable

Group policy
Một số chính sách ATBM

- **Vô hiệu hóa Command Prompt và Windows Registry Editor**

User Configuration / Administrative Templates / System

- Prevent access to the command prompt
- Prevent access to registry editing tools

Group policy
Một số chính sách ATBM

- **Bắt buộc tạo mật khẩu phức tạp**

Computer Configuration / Windows Settings / Security Settings / Account Policies / Password Policy

D.click vào Minimum password length / Define this policy setting / nhập vào số ký tự

Registry
Giới thiệu

- Windows Registry là một cơ sở dữ liệu dùng để lưu trữ các thông số kỹ thuật của Windows và lưu lại những thông tin về sự thay đổi, lựa chọn cũng như những thiết lập từ người sử dụng Windows

Registry
Giới thiệu

- Registry được chia thành các phần (section) chứa các lớp dữ liệu (class) khác nhau.
- được cập nhật khi người dùng có sự thay đổi trong các thành phần của hệ thống

Registry
Giới thiệu

- HKEY_CLASSES_ROOT:
  - Lưu lại những thông tin dùng chung cho toàn bộ hệ thống.
- HKEY_USERS:
  - Lưu thông tin của tất cả các User
- HKEY_CURRENT_CONFIG:
  - Lưu thông tin về phần cứng hiện tại đang sử dụng.

Registry
Giới thiệu

- HKEY_LOCAL_MACHINE (HKLM):
  - Chứa những thông tin về hệ thống, phần cứng và phần mềm.
- HKEY_CURRENT_USER (HKCU):
  - lưu lại những thông tin cho người dùng đang Logon.

Registry
Giới thiệu

- Kiểu dữ liệu trong Registry:
  - REG_BINARY: Kiểu nhị phân
  - REG_DWORD: Kiểu Double Word
  - REG_EXPAND_SZ: Kiểu chuỗi mở rộng đặc biệt. VD: "%SystemRoot%"
  - REG_MULTI_SZ: Kiểu chuỗi đặc biệt
  - REG_SZ: Kiểu chuỗi chuẩn

Registry
Thao tác trên Registry

- **Lưu ý: thao tác trên Registry có thể gây ra các lỗi phát sinh trên máy, do đó phải thực hiện trên máy ảo**
- Sử dụng Registry
  - Win + R / Regedit (GUI)
  - Hoặc dùng lệnh reg trong command prompt

Registry
Thao tác trên Registry

- Sao lưu Registry
- Phục hồi Registry
- Kiểm tra registry thường bị Virus tấn công

reg query “HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /s

Services
Giới thiệu

- Chạy ngầm (background)
- Có thể cấu hình để tự động chạy khi boot máy
- Quản lý thông qua services.msc
- Ngoài ra có thể khởi chạy, ngừng services thông qua lệnh **NET, hoặc SC**
  - Vd: NET START

Services
Giới thiệu

- Các dạng khởi chạy của Services:
  - Automatic
  - Manual
  - Disabled
  - Automatic (Delayed)

Services
Thao tác trên các services

- Sử dụng command line
  - Sc query: hiển thị tất cả services đang chạy
  - Xem thông tin 1 services cụ thể: sc query tên services (có thể lấy tên services thông qua lệnh sc query)

Services
Thao tác trên các services

- Chạy một services:

  Sc start <tên services>

- Ngưng một services

  Sc stop <tên services>

Services
Thao tác trên các services

- Disable services:

  Sc config <tên services> start= disabled

- Enable services:

  Sc config <tên services> start= auto