HUST

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

ONE LOVE. ONE FUTURE.

ONE LOVE. ONE FUTURE.

TRƯỜNG ĐẠI HỌC
BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Chương 10
AN TOÀN TRÊN KHÔNG GIAN SỐ

ONE LOVE. ONE FUTURE.

NỘI DUNG

- CÁC KHÁI NIỆM CƠ BẢN
- CÁC NGUY CƠ ẢNH HƯỞNG ĐẾN AN TOÀN HỆ THỐNG;
- CÁC THÓI QUEN CẦN CÓ CỦA NGƯỜI SỬ DỤNG

KHÁI NIỆM VỀ AN TOÀN TRÊN KHÔNG GIAN SỐ

- Tại sao an toàn trên không gian số (KGS) là cần thiết?
- Thế nào là an toàn hệ thống và an ninh mạng?

KHÁI NIỆM VỀ AN TOÀN TRÊN KHÔNG GIAN SỐ

- Tại sao an toàn trên không gian số là cần thiết?

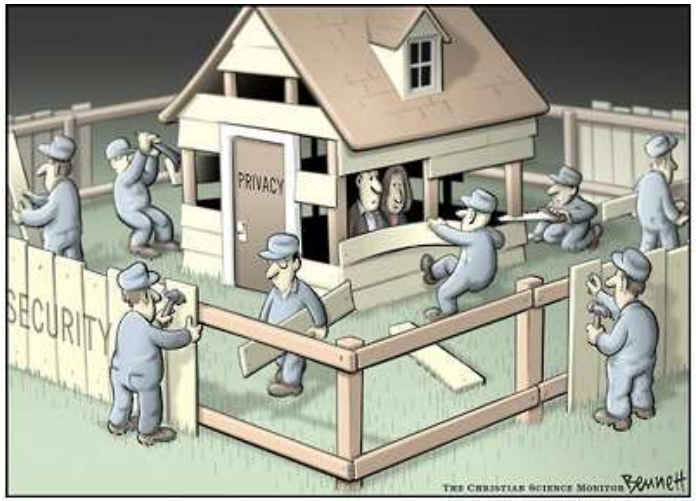
Máy tính và mạng là công cụ chính phục vụ tất cả các nghành nghề, nhất là trong thời **CHUYỂN ĐỔI SỐ**

Nếu an toàn trên không gian số không được quan tâm đúng mức, sẽ có nhiều vấn đề nghiêm trọng xảy ra như:

+ Xâm nhập bất hợp pháp
+ Đánh cắp dữ liệu
+ Tấn công lừa đảo…

KHÁI NIỆM VỀ AN TOÀN TRÊN KHÔNG GIAN SỐ

- Thế nào là an toàn mạng (network security)?



An toàn *(an ninh, bảo mật - security):* là một quá trình liên tục bảo vệ 1 đối tượng khỏi các tấn công.

An toàn thông tin *(information security):* là khả năng **bảo vệ** đối với **môi trường thông tin** kinh tế xã hội, đảm bảo cho việc **hình thành**, **sử dụng** và **phát triển** vì lợi ích của mọi công dân, mọi tổ chức và của quốc gia.

KHÁI NIỆM VỀ AN TOÀN TRÊN KHÔNG GIAN SỐ

- Thế nào là an toàn mạng (network security)?

An toàn máy tính *(computer security):* là an toàn cho tất cả các tài nguyên của hệ thống máy tính:

- Phần cứng vật lý: CPU, màn hình, bộ nhớ, máy in, CDROM, các thiết bị ngoại vi khác, …
- Phần mềm, dữ liệu, thông tin lưu trữ bên trong.

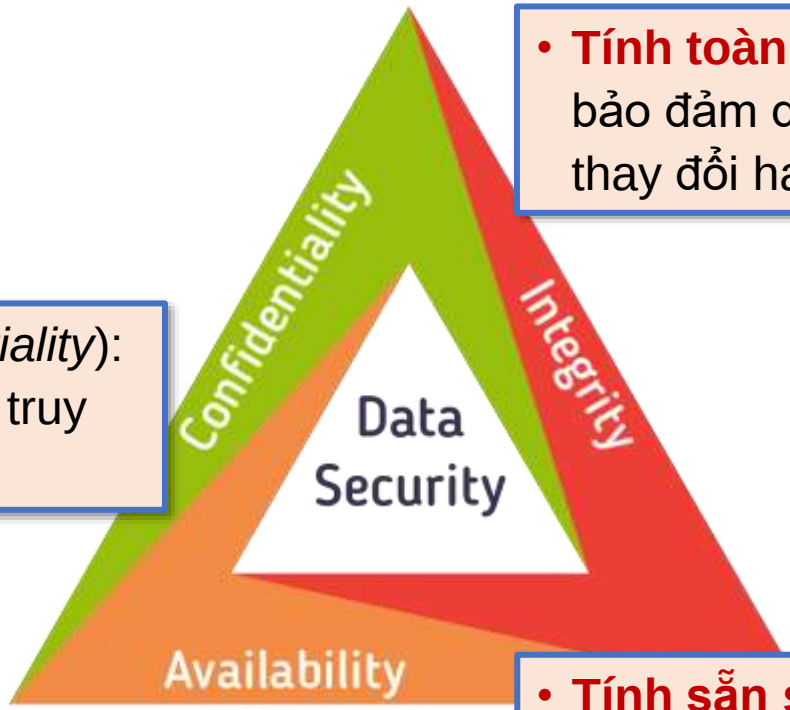
An toàn mạng *(network security):* là an toàn thông tin trong không gian của mạng máy tính.

KHÁI NIỆM VỀ AN TOÀN TRÊN KHÔNG GIAN SỐ

- Đối tượng bị tác động khi không đảm bảo an toàn trên không gian số:
  - An toàn thân thể của mỗi cá nhân
  - Sự bí mật của thông tin cá nhân và tổ chức
  - Tài sản của cá nhân và tổ chức
  - Sự phát triển của một tổ chức
  - Nền kinh tế của một quốc gia
  - Tính an toàn của một quốc gia

TIÊU CHUẨN MỘT MẠNG AN TOÀN

- Mục tiêu CIA



- **Tính toàn vẹn** (*integrity*): bảo đảm dữ liệu không bị thay đổi hay phá hoại.

- **Tính bảo mật** (*confidentiality*): bảo đảm dữ liệu khỏi sự truy xuất hay theo dõi.

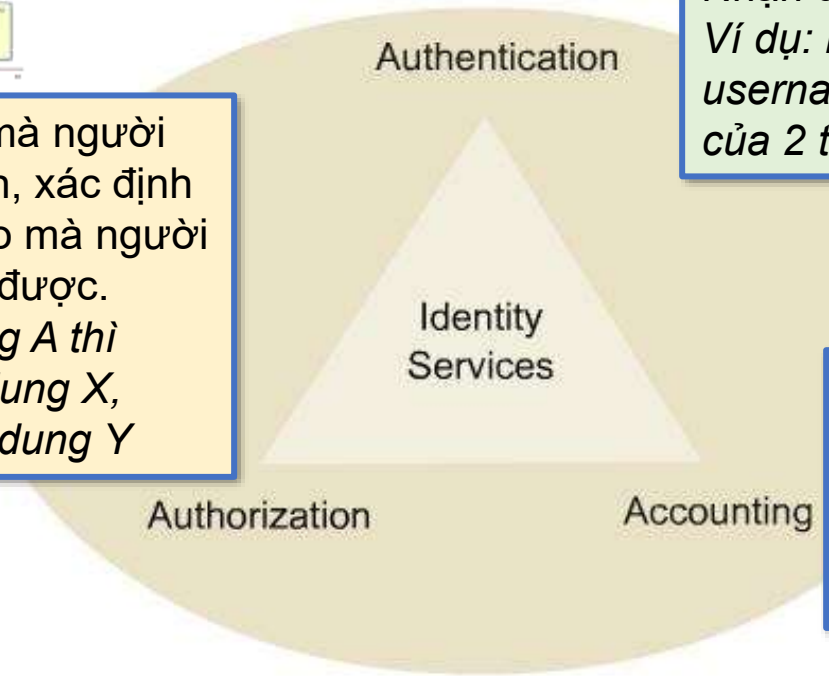
- **Tính sẵn sàng** (*availability*): bảo đảm tính thông suốt của hệ thống và tài nguyên

TIÊU CHUẨN MỘT MẠNG AN TOÀN

- Kiến trúc AAA

Xác định các quyền mà người dùng có thể thực hiện, xác định những tài nguyên nào mà người dùng có thể truy cập được.
Ví dụ: nếu người dùng A thì được phép xem nội dung X, không được xem nội dung Y

Nhận dạng đúng người dùng
Ví dụ: kiểm tra username/password đăng nhập của 2 tài khoản người dùng A, B

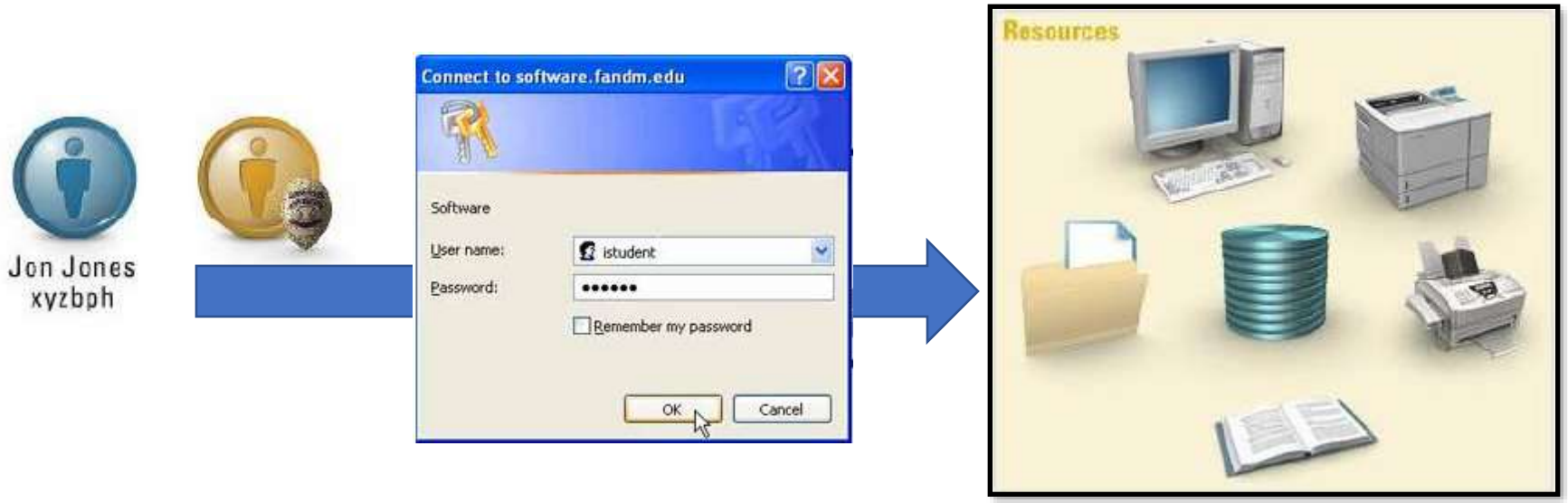


Giám sát những gì mà người dùng làm.
Ví dụ: thêm/xóa/sửa/xem thông tin của 2 tài khoản người dùng A, B.

Kiến trúc AAA cho phép nhà quản trị mạng biết được các thông tin quan trọng về tình hình cũng như mức độ an toàn của hệ thống mạng.

TIÊU CHUẨN MỘT MẠNG AN TOÀN

- Authentication – Chứng thực



Chứng thực là một quy trình nhằm cố gắng xác minh nhận dạng số (digital identity) của phần truyền gửi thông tin (sender) trong giao thông liên lạc.

Điểm yếu của các hệ thống giao dịch bằng tài khoản-mật khẩu là :
- mật khẩu có thể bị quên
- mật khẩu bị lộ
- Dễ dàng dò tìm ra mật khẩu yếu.

TIÊU CHUẨN MỘT MẠNG AN TOÀN

- Chứng thực bằng mật khẩu sử dụng một lần

One time password (OTP)

Người dùng không cần lo lắng mật khẩu của mình bị đánh cắp hay bị mất

- OTP thường đi kèm với các thiết bị phần cứng
- Đồng hồ được đồng bộ thời gian với hệ thống Server xác thực
- Định sẵn một phương pháp tạo ra OTP như nhau : hàm toán học, tín hiệu đồng bộ thời gian, …

TIÊU CHUẨN MỘT MẠNG AN TOÀN

- Chứng thực bằng thẻ cứng

Nhiều loại thiết bị có thể dùng cho token card là: thẻ cứng, PC card, thiết bị USB, thiết bị Bluetooth, …
Ví dụ USB BKAV-CA sử dụng trong kê khai thuế

- Là một trong các giải pháp bảo mật an toàn nhất.
- Được dùng kết hợp với một loại chứng thực khác (chẳng hạn như số PIN, mật khẩu)

TIÊU CHUẨN MỘT MẠNG AN TOÀN

- Chứng thực bằng thông tin sinh trắc học


Retinal Patterns


Finger/Palm Prints


Voice Patterns

- không thể làm mất
- Không thể quên
- Rất khó giả mạo

Dùng để chứng thực người dùng thông qua:
- Đặc điểm sinh học: khuôn mặt, bàn tay, mống mắt, võng mạc, dấu vân tay, DNA, …
- Hành vi bên ngoài: dáng đi, chữ ký, giọng nói, …

Nhận dạng nhầm nếu:
- Thiết bị đọc không chính xác
- Đặc điểm của người cũng có thể thay đổi theo năm tháng

Liên quan tới lập trình

- Thư viện JWT: https://jwt.io
- Sử dụng Barer token hoặc username/password
  (thiết bị IoT) (người dùng)
- Claim-based Authentication: sử dụng tài khoản của bên thứ 3 để đăng nhập. *Ví dụ tạo trang web quản lý với tài khoản đăng nhập dùng gmail, facebook, office365…*

TIÊU CHUẨN MỘT MẠNG AN TOÀN

- Authorization – Phân quyền

Sau khi được chứng thực, việc phân quyền chỉ định những gì mà người dùng đó có thể thi hành trên hệ thống

Phân quyền: định nghĩa các quyền (*rights*) và sự cho phép (*permission*) của người dùng trong một hệ thống

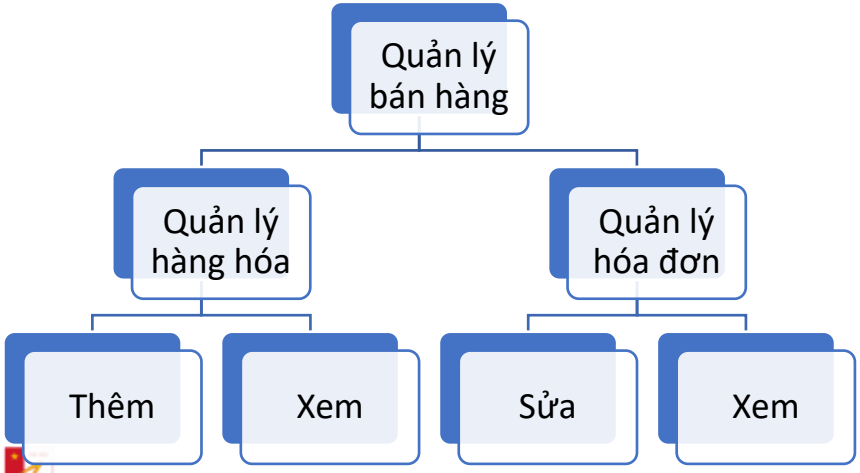
- Điều khiển truy cập sẽ cho phép hoặc từ chối một chủ thể (người , quá trình) sử dụng một đối tượng (chức năng, tập tin, ….).
- Điều khiển truy cập có 3 dạng chính là:
  - Điều khiển truy cập tùy quyền (**D**iscretionary **A**ccess **C**ontrol)
  - Điều khiển truy cập bắt buộc (**M**andarory **A**ccess **C**ontrol)
  - Điều khiển truy cập dựa trên vai trò (**R**ole-**B**ased **A**ccess **C**ontrol)

• Authorization – Phân quyền

Phân quyền theo tính năng kỹ thuật

- Phân quyền theo chức năng/module
- Phân quyền theo giao diện
- Phân quyền theo vùng trong giao diện

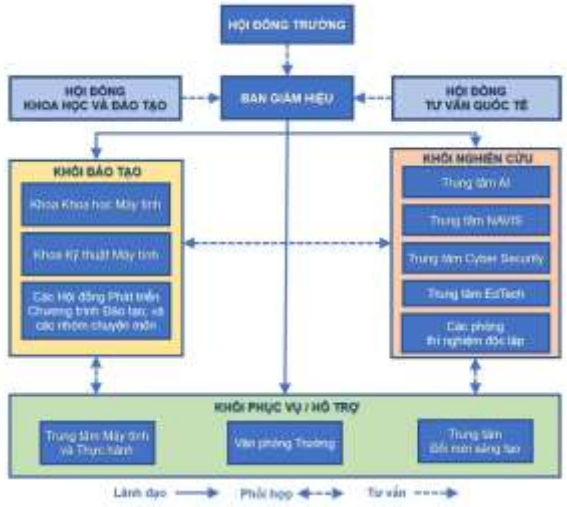
Ví dụ user A được phép xem báo cáo tuần, user B được phép xem chi tiêu của chi nhánh Nghệ An.



Phân quyền theo cơ cấu tổ chức

- Organization Unit: Phòng sản xuất, Phòng nhân sự,
- Group: Ban lãnh đạo, nhóm công đoàn

Ví dụ user A là sinh viên lớp Nhập môn CNTT, đồng thời là lớp phó, kiêm chủ nhiệm CLB, thành viên Liên Quân.



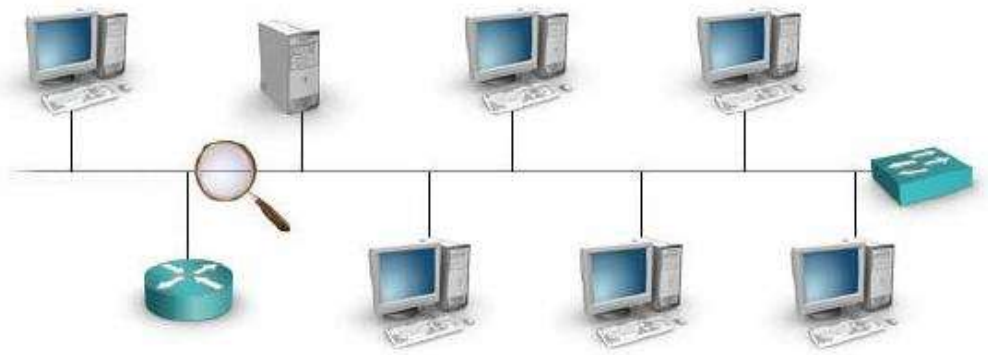
Liên quan tới lập trình

- Lớp AuthorizeAttribute trong C#, JS, JSP
  https://learn.microsoft.com/en-us/aspnet/core/security/authorization/simple?view=aspnetcore-8.0

TIÊU CHUẨN MỘT MẠNG AN TOÀN

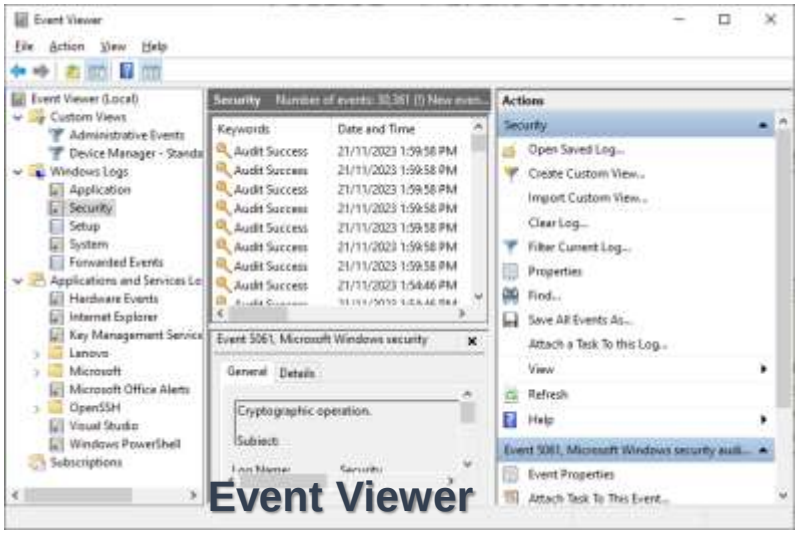
- Accounting – Giám sát

Với một hệ thống giám sát được xây dựng, các **dấu vết của xâm nhập sẽ được ghi nhận lại** để cung cấp một bức tranh rõ ràng các sự kiện đã xảy ra trong hệ thống



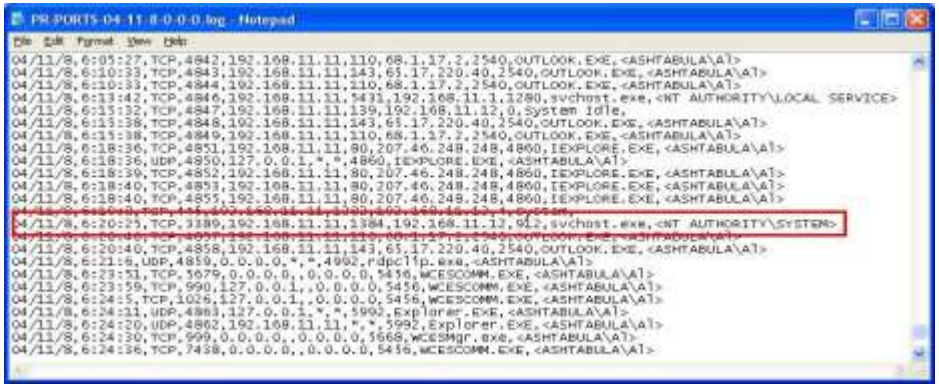
Các hình thức giám sát chính bao gồm:
- Ghi file nhật ký (logging)
- Quét hệ thống (scanning)
- Kiểm soát (monitoring)

- Logging – Ghi file nhật ký



Event Viewer

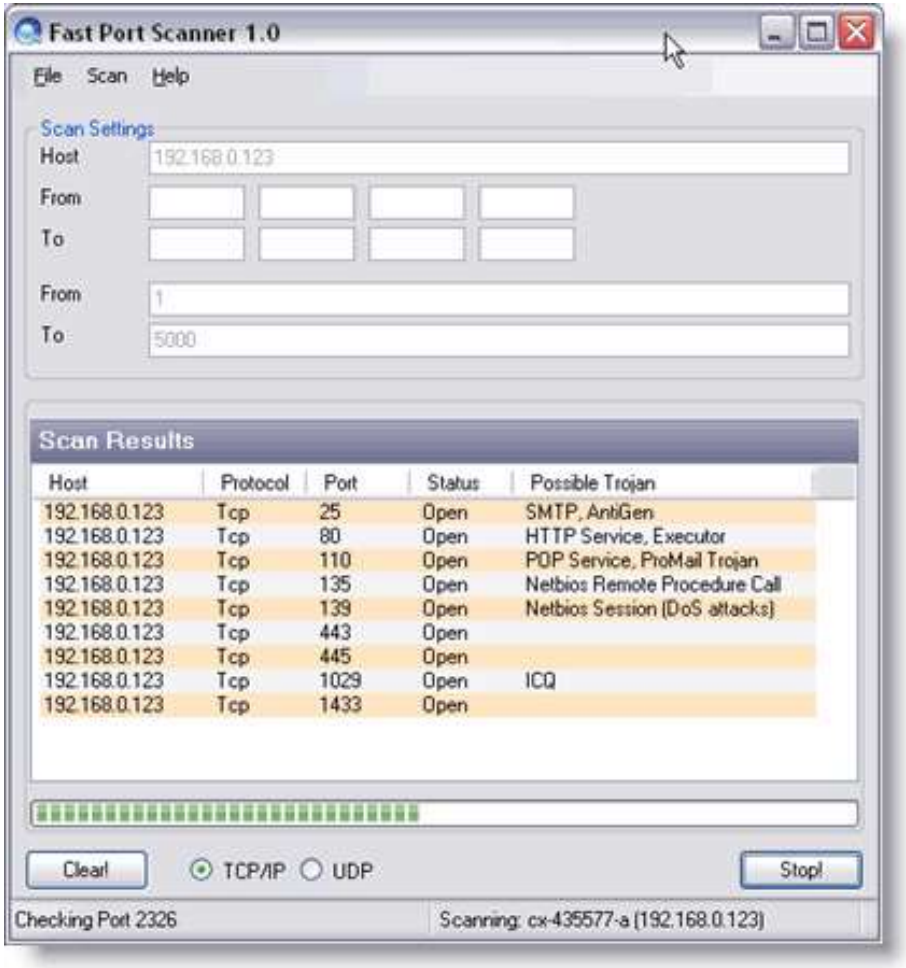
Log file ghi nhận lại các sự kiện và thời điểm xảy ra trong hệ thống



Windows Firewall log file

- Thường được ghi dưới dạng file Text, từng dòng là một sự kiện.
- Ghi nhận liên tục khi đang hoạt động.
- Có thể được ghi trên thiết bị, đĩa cục bộ, Server (SysLog) hay kết hợp nhiều nơi.
- Phải được lưu trữ trong 1 thời gian dài và bảo quản cẩn thận

- System scanning – Quét hệ thống



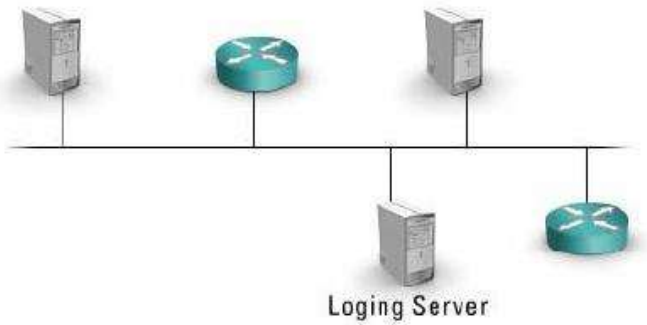
Theo dõi và kiểm tra các dịch vụ mạng nào đang hoạt động trên hệ thống

- Quét định kỳ rất quan trọng trong việc giám sát.
- Có rất nhiều các công cụ về bảo mật hỗ trợ quét hệ thống.

Kỹ thuật quét hệ thống có thể phát hiện ra những điểm yếu trong hệ thống mạng hay hệ thống máy tính để có hướng khắc phục và gia cố.

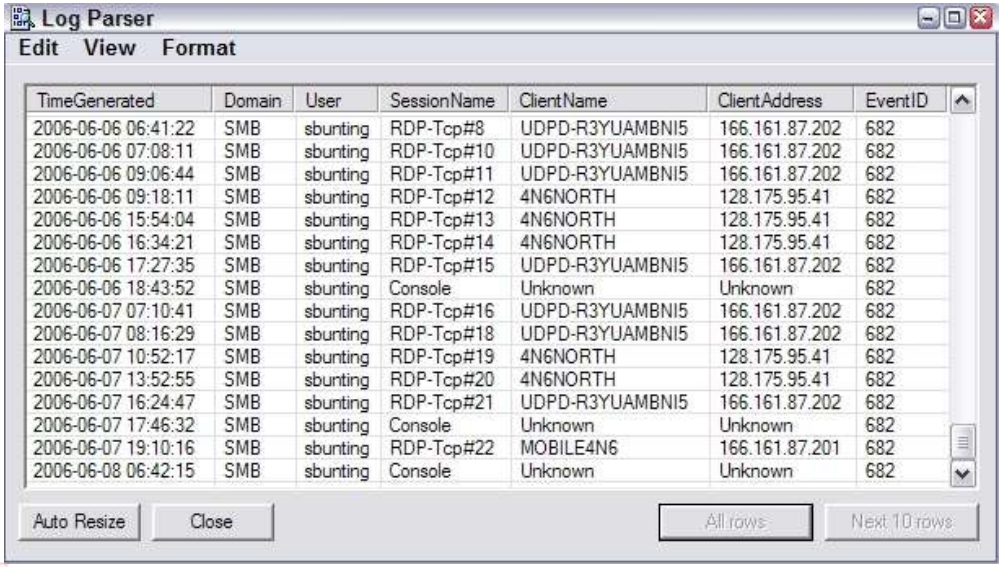
TIÊU CHUẨN MỘT MẠNG AN TOÀN

- Monitoring – Kiểm soát



Một cách duy trì và kiểm soát hệ thống là thường xuyên xem lại các log file.

Khi có sự cố xảy ra thì quản trị mạng mới bắt đầu kiểm tra lại các log file và đôi khi điều này là đã quá muộn



Sử dụng các công cụ hỗ trợ trong việc phân tích các log file và có cảnh báo các nguy cơ.

Intrusion Detection & Prevention System

Liên quan tới lập trình

- Nguồn mở: cornflourblue/next-js-11-registration-login-example: Next.js 11 - User Registration and Login Example (github.com)

NỘI DUNG

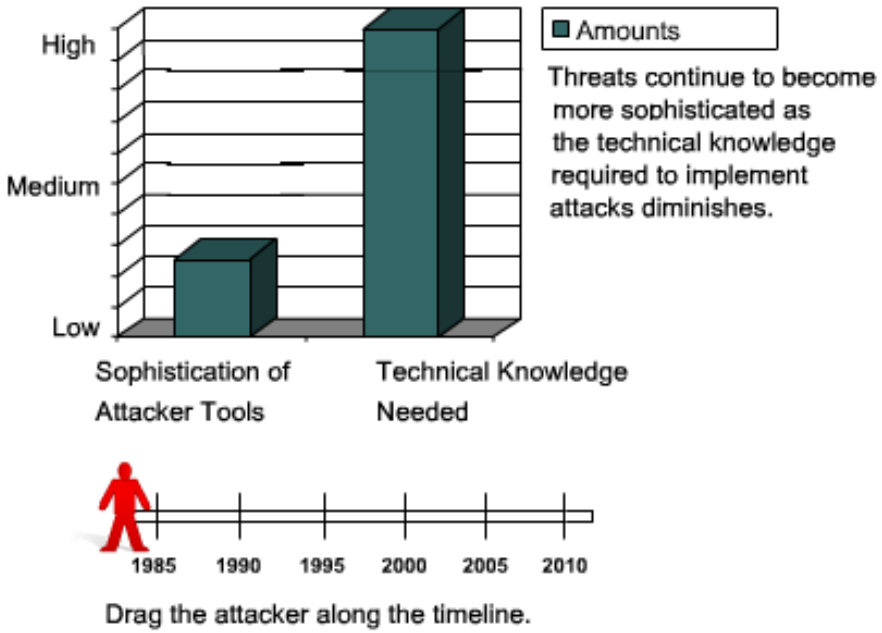
- CÁC KHÁI NIỆM CƠ BẢN
- **CÁC NGUY CƠ ẢNH HƯỞNG ĐẾN AN TOÀN HỆ THỐNG;**
- **CÁC THÓI QUEN CẦN CÓ CỦA NGƯỜI SỬ DỤNG**

CÁC NGUY CƠ ẢNH HƯỞNG ĐẾN AN TOÀN HỆ THỐNG

- Các mối đe dọa (threat) đến an toàn hệ thống.
- Phân loại kẻ tấn công.
- Các hình thức tấn công phổ biến.

CÁC MỐI ĐE DỌA ĐẾN AN TOÀN HỆ THỐNG

Có nhiều tác nhân có thể là mối **đe dọa** (threat - còn gọi là **hiểm họa** hay **mối nguy hại**) cho một mạng máy tính.

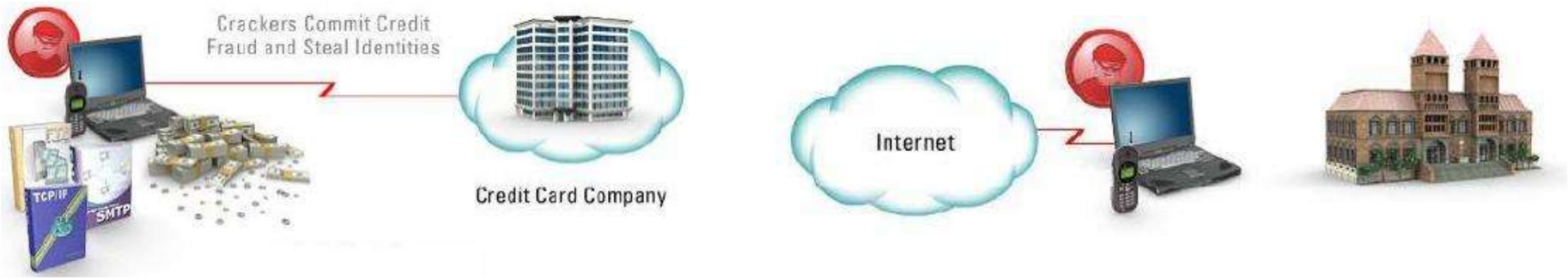


Có thể chia các mối đe dọa (threat) thành các dạng sau:

- Đe dọa có tổ chức và không tổ chức
- Đe dọa từ bên ngoài và từ bên trong
- Đe dọa chủ động và thụ động .
- Đe dọa cố ý và vô tình .

CÁC MỐI ĐE DỌA ĐẾN AN TOÀN HỆ THỐNG

- Đe dọa có tổ chức và không tổ chức



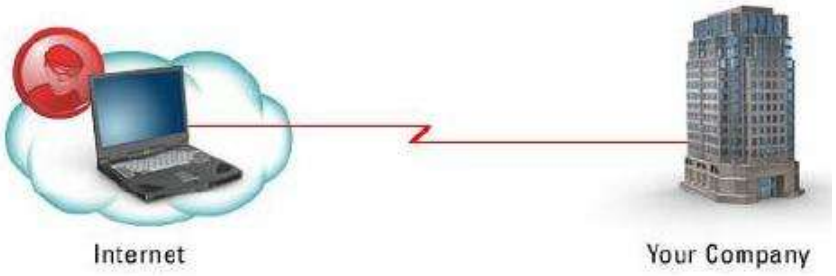
Đe dọa có tổ chức (structured threat) là de dọa được hoạch định trước vào 1 mục đích nhất định và lâu dài.
Các đe dọa này đến từ những hacker thành thạo và có động cơ rõ rệt.

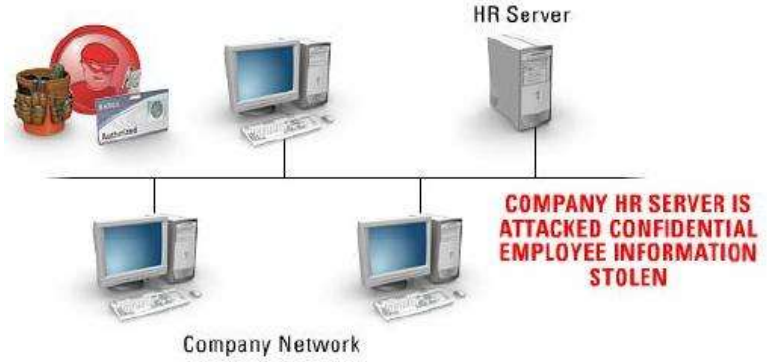
Đe dọa không tổ chức (unstructured threat) là đe dọa mang tính tức thời và là kết quả của những hacker đơn lẻ chưa có kinh nghiệm, thường chỉ dùng các công cụ có sẵn được công khai trên Internet để thử nghiệm.

Các đe dọa có tổ chức thường sẽ được che dấu rất khó phát hiện

CÁC MỐI ĐE DỌA ĐẾN AN TOÀN HỆ THỐNG

- Đe dọa từ bên ngoài và từ bên trong





• Xuất phát từ các cá nhân hoặc tổ chức **bên ngoài hệ thống mạng**.
• Không có quyền truy xuất vào hệ thống máy tính và hệ thống mạng.
• Chỉ đột nhập vào từ Internet hay bằng đường Dial-up thông qua RAS.

• "70% các vấn đề có liên quan đến bảo mật thường đến từ bên trong mạng".
• Xảy ra từ một ai đó **có quyền truy xuất trong nội bộ mạng**.

Ngăn chặn các đe dọa từ bên trong cũng quan trọng như các đe dọa đến từ bên ngoài.

CÁC MỐI ĐE DỌA ĐẾN AN TOÀN HỆ THỐNG

- Đe dọa chủ động (active) - thụ động (passive) và đe dọa cố ý (intentional) - vô tình (unintentional)

Đe dọa chủ động: có thể sửa đổi thông tin hoặc thay đổi tình trạng hoạt động của 1 hệ thống
VD: thay đổi bảng vạch đường của 1 Router.

Đe dọa thụ động: không có thay đổi dữ liệu của hệ thống.
VD: nghe trộm thông tin trên đường truyền.

Đe dọa cố ý: các tấn công tinh vi có sử dụng các kiến thức hệ thống đặc biệt.
VD: cố tình xâm nhập mạng trái phép.

Đe dọa vô tình: một sự kiện ngẫu nhiên có thể gây hại cho hệ thống.
VD: chế độ đặc quyền tự động được login.

PHÂN LOẠI KẺ TẤN CÔNG

- Hacker

• **Hacker** (intruder, attacker) là kẻ dùng kiến thức bản thân để thâm nhập, tấn công hệ thống máy tính hay mạng máy tính.
• Đa số hacker đều rất am tường về hoạt động của máy tính và mạng máy tính.

Hacker mũ trắng (white hat): xâm nhập có ý tốt. Chẳng hạn: nhà bảo mật, lập trình viên, chuyên viên mạng.

Hacker mũ đen (black hat): thâm nhập có mục đích xấu như: phá hoại, đánh cắp thông tin, ...

Cracker =“Criminal Hacker” (hacker tội phạm)

CÁC HÌNH THỨC TẤN CÔNG PHỔ BIẾN

- Khái niệm về tấn công

Chúng ta có thể gọi tất cả **các dạng có hại** cho hệ thống máy tính là "tấn công".

Các tấn công có thể xuất phát từ:
- Các công cụ được thiết kế sẵn.
- Khai thác các điểm yếu của hệ thống.

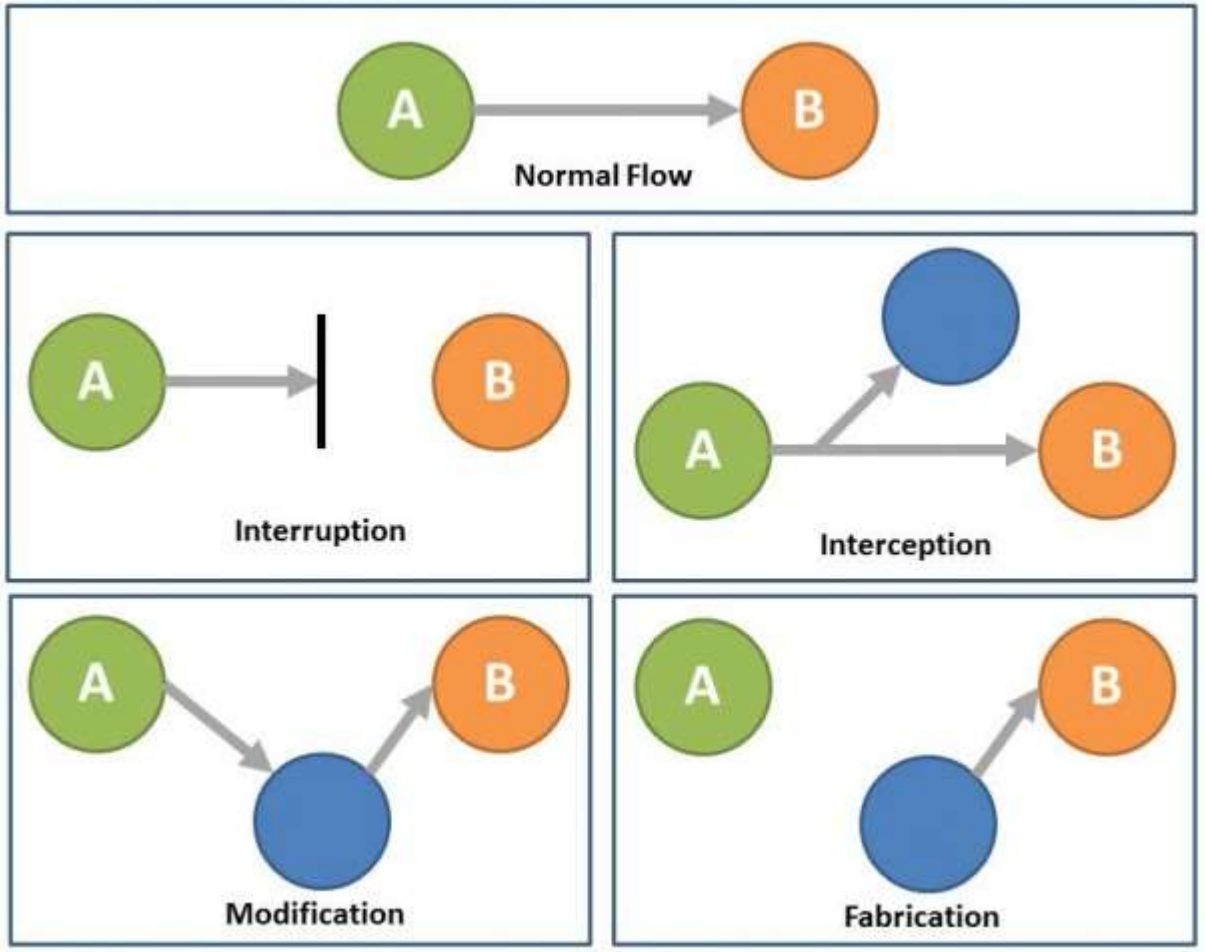
Tấn công có thể gây ra:
- Hư hỏng dữ liệu hoặc ngưng trệ hoạt động hệ thống
- Không làm hư hại cho dữ liệu và hệ thống (chẳng hạn ăn trộm thông tin) nhưng tác hại có thể lớn hơn.

Có thể phân chia tấn công ra làm 3 loại chính:
1. Do thám (reconnaissance)
2. Truy cập (access)
3. Từ chối dịch vụ (denial of service - DoS)

CÁC HÌNH THỨC TẤN CÔNG PHỔ BIẾN

- Khái niệm về tấn công

Các hình thức tấn công trên mạng



CÁC HÌNH THỨC TẤN CÔNG PHỔ BIẾN

- Tấn công do thám (Reconnaissance)

Tấn công do thám là loại tấn công không phải với mục đích chiếm đoạt hệ thống mà chỉ tìm kiếm thông tin để có thể khai thác sau này

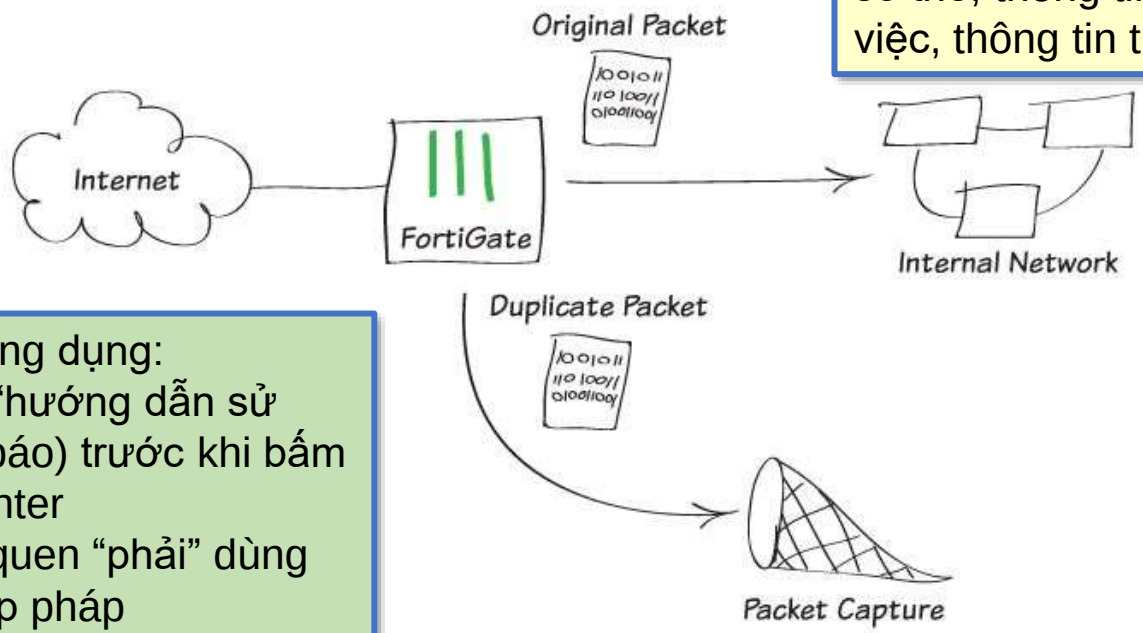
Các thông tin cần ghi nhận:
- Địa chỉ IP; các dịch vụ mạng đang sử dụng; cổng nào đang mở; máy cài hệ điều hành nào; phiên bản phần mềm đang chạy trên máy…
- Thông tin trao đổi trên đường truyền: user/pass; các địa chỉ hay truy cập; các dịch vụ hay dung
- …

Các kỹ thuật do thám thông dụng:
1. Nghe lén
2. Quét địa chỉ IP
3. Quét cổng
4. Quét tránh né
5. Xác định hệ điều hành

CÁC HÌNH THỨC TẤN CÔNG PHỔ BIẾN

- Nguy cơ từ tấn công do thám

Thu thập thông tin tài khoản cá nhân: Mật khẩu, số thẻ, thông tin phiên làm việc, thông tin trao đổi



Nguyên nhân thông dụng:

1. Không đọc kĩ "hướng dẫn sử dụng" (thông báo) trước khi bấm OK hoặc ấn enter
2. Chưa có thói quen "phải" dùng phần mềm hợp pháp
3. Chưa "hình thành" thói quen dùng mạng, máy tính an toàn

Các thông tin của hệ thống để tấn công sau này

CÁC HÌNH THỨC TẤN CÔNG PHỔ BIẾN

- Tấn công truy cập (Access attack)

Tấn công truy cập là loại tấn công chiếm lấy tài nguyên trên hệ thống đích như file, mật khẩu, quyền điều khiển, …

Sau khi tấn công thăm dò để nắm được các thông tin cơ bản về hệ thống đích, hacker sẽ tấn công trực tiếp vào hệ thống gọi là **tấn công truy cập**

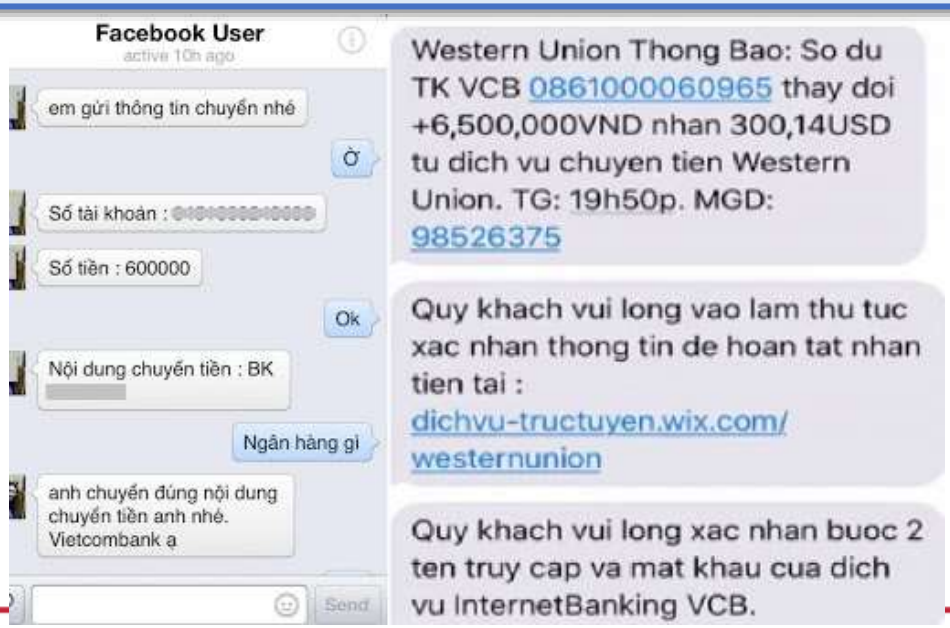
Các kỹ thuật tấn công truy cập thông dụng:

1. Nghe lén
2. Sử dụng lại
3. Cướp giao dịch
4. Kẻ đứng giữa
5. Cổng sau
6. Đánh lừa
7. Khai thác lỗi
8. Tấn công mật khẩu

CÁC HÌNH THỨC TẤN CÔNG PHỔ BIẾN

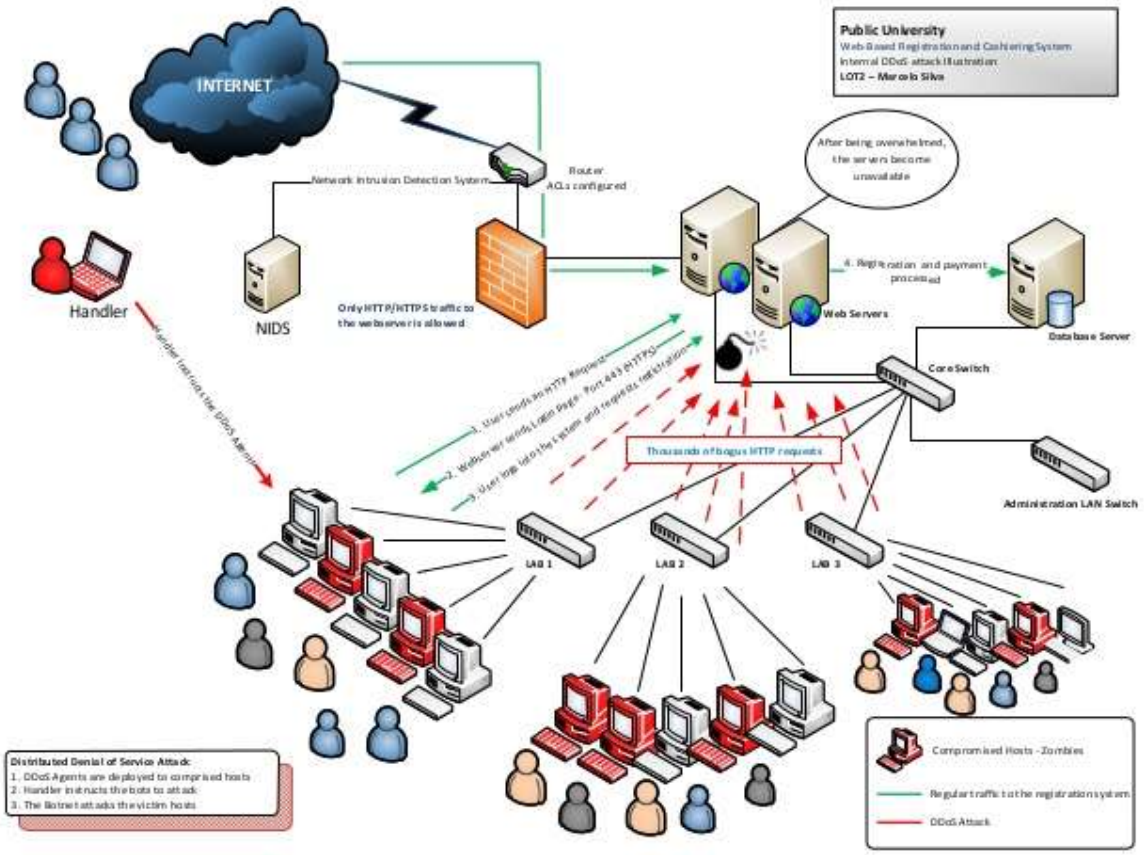
- Nguy cơ từ tấn công truy cập

• Ăn trộm mật khẩu mạng xã hội, email… sau đó đổi mật khẩu và sử dụng tài khoản này cho mục đích xấu
• Sử dụng thông tin đăng nhập từ xa của người dùng để xâm nhập vào hệ thống một cách hợp pháp sau đó: phát tán phần mềm độc hại; tấn công hệ thống từ bên trong
• Tấn công hệ thống bằng lỗ hổng phần mềm, hệ điều hành
•…



CÁC HÌNH THỨC TẤN CÔNG PHỔ BIẾN

- Tấn công từ chối dịch vụ (Deny of Service)



Là tấn công phá hoại chứ không phải muốn lấy được thông tin.

Tấn công bằng từ chối dịch vụ DoS có thể mô tả như hành động **ngăn cản những người dùng hợp pháp khả năng truy cập và sử dụng vào một dịch vụ** nào đó.
Nó bao gồm làm **tràn ngập mạng**, **mất kết nối với dịch vụ**… mà mục đích cuối cùng là Server **không thể đáp ứng được các yêu cầu sử dụng dịch vụ** từ các Client.

NỘI DUNG

- CÁC KHÁI NIỆM CƠ BẢN
- CÁC NGUY CƠ ẢNH HƯỞNG ĐẾN AN TOÀN HỆ THỐNG;
- **CÁC THÓI QUEN CẦN CÓ CỦA NGƯỜI SỬ DỤNG**

CÁC THÓI QUEN CẦN CÓ CỦA NGƯỜI SỬ DỤNG

- Các thói quen khi sử dụng máy tính cá nhân?
- Sử dụng phần mềm an toàn?
- Tuân thủ chính sách an ninh của hệ thống?

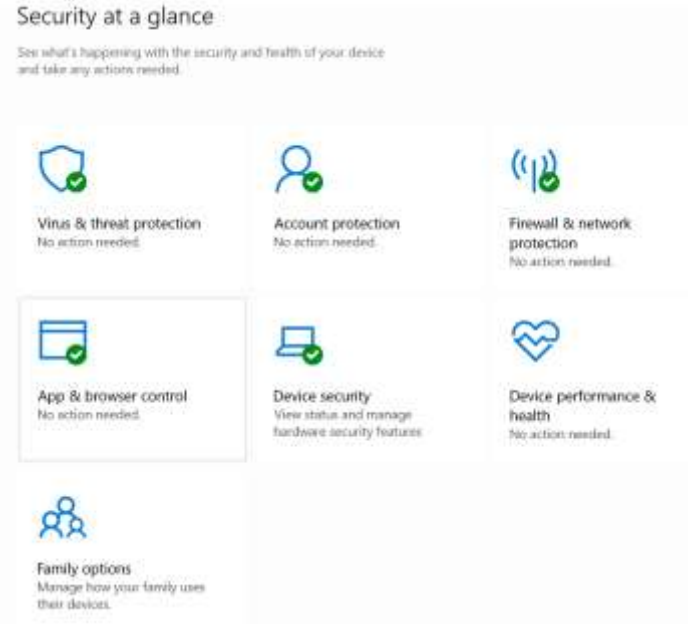
CÁC THÓI QUEN KHI SỬ DỤNG MÁY TÍNH CÁ NHÂN

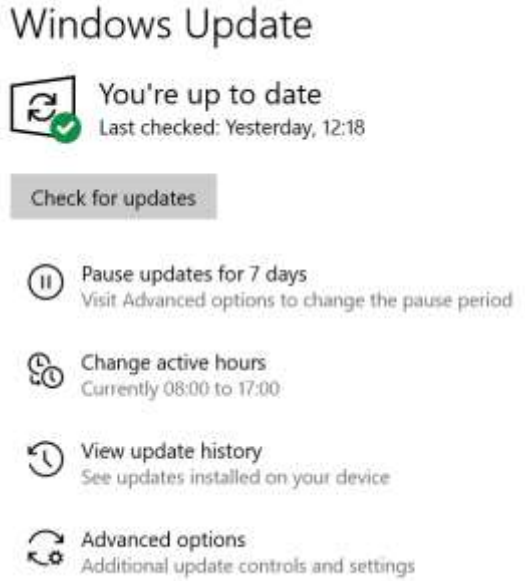
- Cảnh giác trước khi click vào một file:
  - Lý do: Hacker thường dùng mọi cách lừa bạn chạy file virus bằng cách làm cho bạn tưởng rằng đó là một file bình thường (“.doc” “.zip” “.xls”…)
  - Cách thức:
    - Luôn để chế độ hiện phần mở rộng (đuôi) của file:
    - Không tải về các file đính kèm từ các trang web lạ, các email không rõ nguồn gốc hoặc các email nghi ngờ
    - Không click đúp để mở usb mà dùng Explorer
    - Tắt tính năng autorun nếu có thể

Hình 1. Bình thường Hình 2. Bị nhiễm Hình 3. Bị nhiễm

CÁC THÓI QUEN KHI SỬ DỤNG MÁY TÍNH CÁ NHÂN

- Thường xuyên cập nhật hệ điều hành và các chương trình diệt virus, spyware. Bật chế độ Automatic Update trong các chương trình này (nếu có).





CÁC THÓI QUEN KHI SỬ DỤNG MÁY TÍNH CÁ NHÂN

- Tiến hành quét virus, spyware một cách định kỳ, thường xuyên.
  - Đặt lịch quét tự động cho chương trình diệt virus, spyware
  - Quét virus vào thời gian rảnh rỗi (nghỉ trưa, tối)
  - Quét trong chế độ Safe Mode
  - Cập nhật các Boot CD có bản diệt virus mới nhất và quét định kỳ

CÁC THÓI QUEN KHI SỬ DỤNG MÁY TÍNH CÁ NHÂN

- Hạn chế truy cập vào các trang web có nội dung không lành mạnh, hay các trang cung cấp crack, serial… hơn 90% các trang web này có virus, spyware…

CÁC THÓI QUEN KHI SỬ DỤNG MÁY TÍNH CÁ NHÂN

- Thường xuyên sao lưu các dữ liệu quan trọng ra nhiều nơi an toàn một cách thường xuyên:
  - Copy ra USB, ổ cứng di động
  - Ghi ra CD, DVD
  - Upload lên cloud (GG Drive, Dropbox, OneDrive)
  - Gửi vào hòm mail (Gmail, Hustmail)

Gmail

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

Sign in **HUST** - **Office 365** with your account

Account@hust.edu.vn or Account@sis.hust.edu.vn

Password

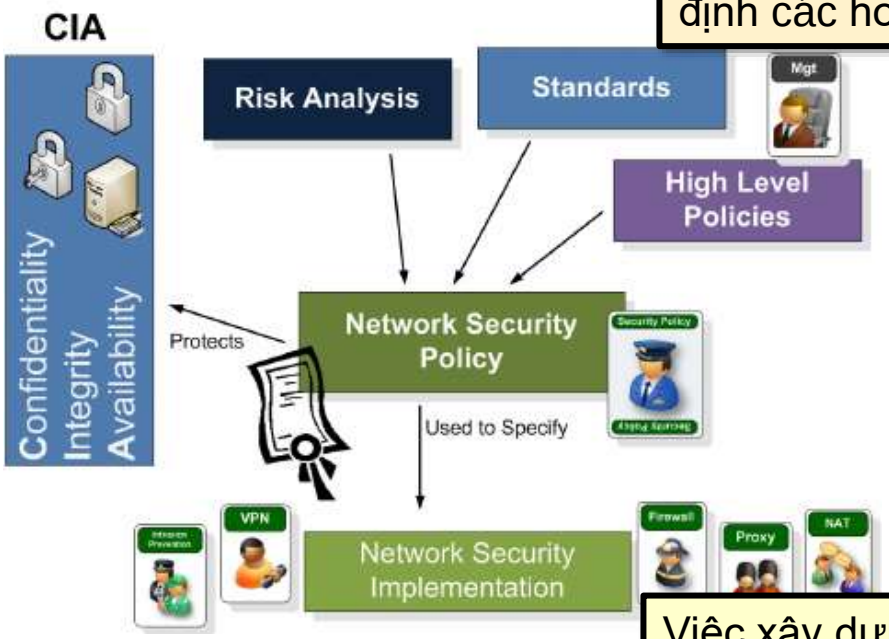
SỬ DỤNG PHẦN MỀM AN TOÀN

- Phần mềm có bản quyền:
  - Tập thói quen mua bản quyền phần mềm
  - Không sử dụng các phần mềm, hệ điều hành crack sẵn
  - Không chạy các phần mềm tạo key, không copy đè các file chạy crack lên phần mền trên máy
- Phần mềm miễn phí:
  - Sử dụng các phần mềm miễn phí có tính năng tương đương
  - Chọn phần mền từ các nguồn tin cậy

TUÂN THỦ CHÍNH SÁCH AN NINH MẠNG

- Khái niệm

Chính sách an ninh mạng (**network security policies**) quy định các hoạt động nào trên mạng được xem là đúng.



Chính sách an ninh mạng bao gồm tập các quy tắc những thao tác cho phép và không cho phép.
Được chuẩn hóa trong các RFC như 2504, 2196, …

Việc xây dựng chính sách an ninh của một tổ chức (công ty) nên dựa theo những chính sách an ninh chuẩn như sau:
- Chính sách giới hạn truy cập
- Chính sách an ninh cho máy trạm
- Chính sách an ninh vật lý
- và các chính sách an ninh khác …

TUÂN THỦ CHÍNH SÁCH AN NINH MẠNG

- Chính sách giới hạn truy cập (restricted access)

Mỗi nhân viên chỉ có thể thực hiện được các **truy cập tối thiểu** theo yêu cầu công việc của mình. Khi có quyền hơn thế sẽ tạo ra các rủi ro về bảo mật.

Các chính sách an ninh giới hạn truy cập có thể bao gồm các vấn đề như:
- Hạn chế truy cập vào hệ thống file hay dữ liệu trên Server cục bộ.
- Hạn chế truy cập Internet: yêu cầu tài khoản và mật khẩu.
- Giới hạn truy cập vào hệ thống VPN: đòi hỏi username, số PIN, số của token được cung cấp, ...
- Thường sử dụng đến các **điều khiển truy cập**.
- Giới hạn truy cập không chỉ về dữ liệu mà áp dụng cho cả về con người.

TUÂN THỦ CHÍNH SÁCH AN NINH MẠNG

- Chính sách an ninh cho máy trạm (workstation security policies)

Máy trạm là 1 máy tính nối kết đến mạng và sử dụng các tài nguyên của mạng.

Các chính sách an ninh cho máy trạm có thể bao gồm các vấn đề như:

- Lưu trữ file trên máy tính và copy dữ liệu ra thiết bị lưu trữ ngoài.
- Thay đổi cấu hình, giao thức mạng, cài đặt phần mềm, …
- Tài khoản người dùng cục bộ và quyền của người dùng.
- Việc sử dụng các thiết bị di động và cầm tay mang vào cơ quan.

TUÂN THỦ CHÍNH SÁCH AN NINH MẠNG

- Chính sách an ninh vật lý (physical security)

Giới hạn các truy cập vật lý trực tiếp, hạn chế những nguy cơ xảy ra.

Các chính sách an ninh vật lý có thể bao gồm các thành phần như:

- Địa điểm: phòng Server, phòng thí nghiệm, ...
- Tài sản: phần cứng, phần mềm, dữ liệu, thiết bị, …
- Mức độ an toàn: tủ bảo vệ, khóa, loại chứng thực, …
- Thủ tục chứng thực: ai cần chứng thực, chứng thực như thế nào , …
- Giám sát và ghi nhận: ai ở địa điểm này vào thời gian nào.

HUST

hust.edu.vn fb.com/dhbkhn

THANK YOU !