An toàn mạng máy tính

# Chương 1. Tổng quan

**ThS. Nguyễn Ngọc Toàn**

(Khoa ANTT – Học viện An ninh nhân dân)

- Điện thoại: 096-159-7667
- Email: ngoctoan.hvan@gmail.com

# Nội dung môn học:

Chương 1: Tổng quan về an toàn mạng

Chương 2: Công nghệ tường lửa

Chương 3: Công nghệ phát hiện và ngăn chặn xâm nhập

Chương 4: Hệ thống SIEM

Chương 5: Công nghệ VPN

Chương 6: An toàn mạng không dây

Chương 7: Mạng Honeynet

# Nội dung bài giảng:

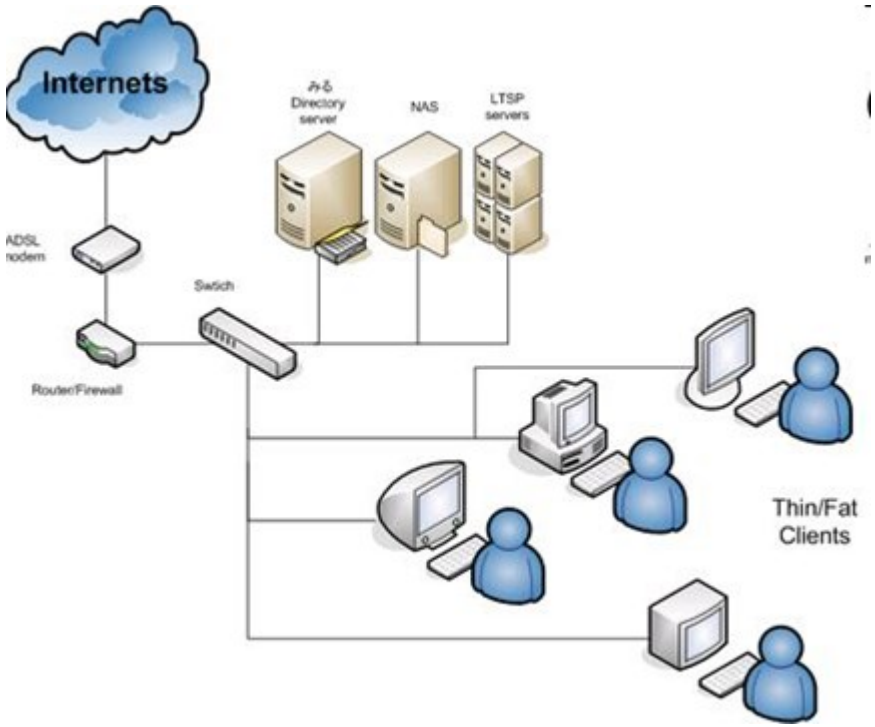
1. Nguyên nhân gây mất ATTT
2. Hiểm họa ATTT
3. Các hình thức tấn công đối với thông tin
4. Các dịch vụ bảo vệ thông tin
5. Các mô hình bảo mật cụ thể

# Tài liệu tham khảo:


1. *A Guide to Computer Network Security-Springer London (2009)*.
2. *NIST SP800-94:* Guide to Intrusion Detection and Prevention Systems
3. *Security Information and Event Management (SIEM) Implementation*.

# I. Giới thiệu chung

**Khái niệm:** Mạng máy tính là tập hợp các máy tính đơn lẻ được kết nối với nhau bằng các phương tiện truyền vật lý và theo các kiến trúc mạng.



# I. Giới thiệu chung

- Phân loại:
  - Theo môi trường truyền thông:
    - Mạng có dây
    - Mạng không dây
  - Theo địa lý:
    - Mạng cục bộ LAN
    - Mạng đô thị MAN
    - Mạng diện rộng WAN
    - Mạng toàn cầu GAN
  - Theo chức năng:
    - Mạng ngang hàng
    - Mạng khách chủ

# I. Giới thiệu chung

- Các thành phần tham gia vào mạng:
  - Thiết bị đầu cuối
  - Thông điệp
  - Phương tiện truyền thông
  - Quy tắc

# I. Giới thiệu chung

- **Mạng máy tính an toàn:**

Mạng máy tính được gọi là an toàn nếu nó cung cấp các dịch vụ sau đây:

- Dịch vụ bí mật
- Dịch vụ xác thực
- Dịch vụ toàn vẹn
- Dịch vụ chống chối bỏ
- Dịch vụ kiểm soát truy cập
- Sẵn sàng phục vụ

# I. Các nguyên nhân

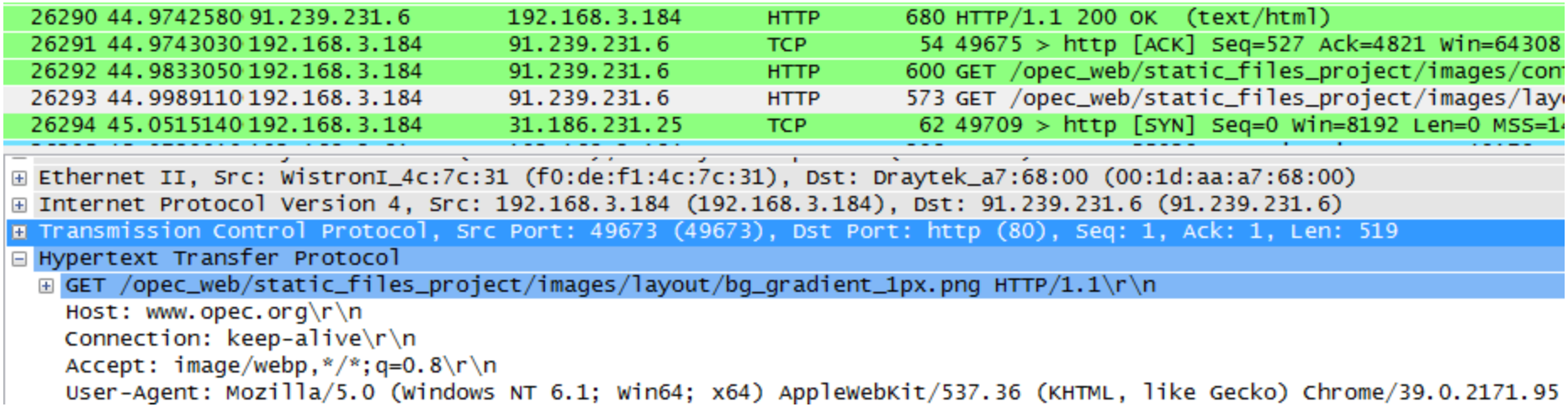
- Các nguyên nhân gây mất an toàn thông tin:
  - Điểm yếu công nghệ
  - Điểm yếu trong chính sách
  - Cấu hình yếu

# I.1. Điểm yếu công nghệ

- Điểm yếu trong TCP/IP:
  - Chặn bắt và phân tích gói tin:
    - Biết được IP nguồn và đích của phiên kết nối
    - Biết được giao thức, dịch vụ
    - Thậm chí biết được cả nội dung

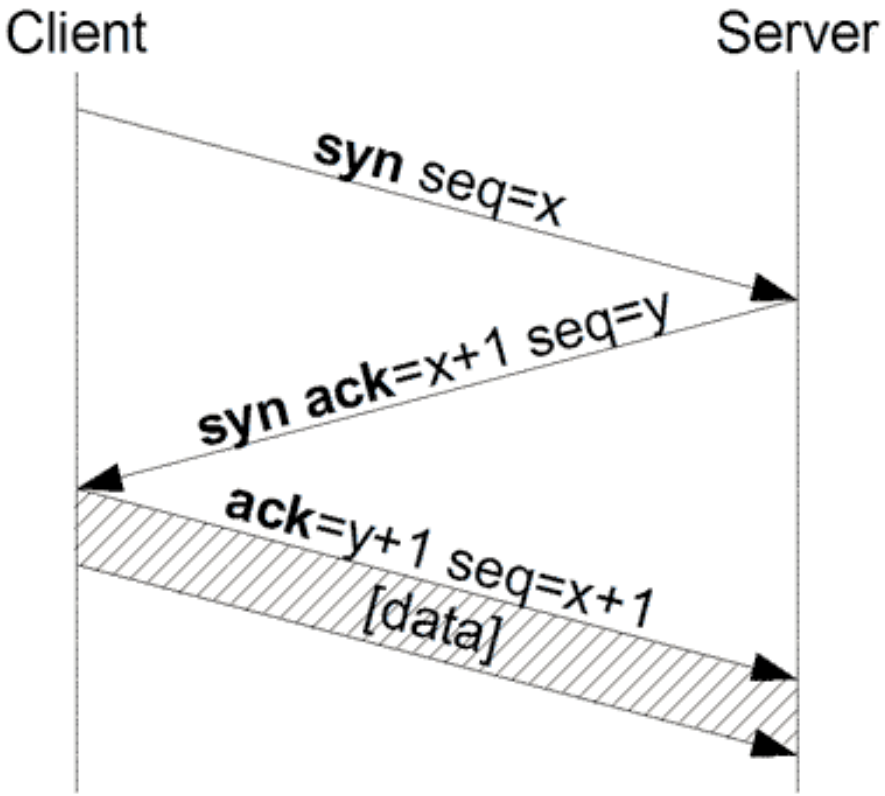
# I.1. Điểm yếu công nghệ

- Điểm yếu trong TCP/IP:
  - Chặn bắt và phân tích gói tin:



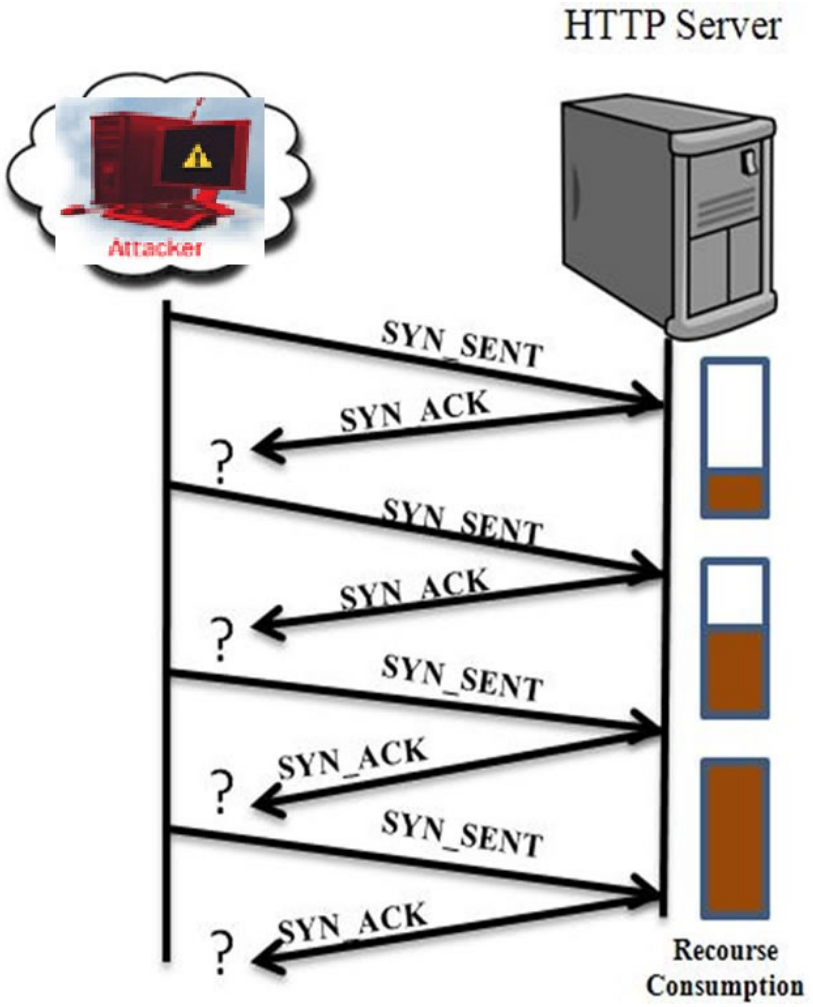
# I.1. Điểm yếu công nghệ

- Lợi dụng quá trình bắt tay 3 bước TCP:



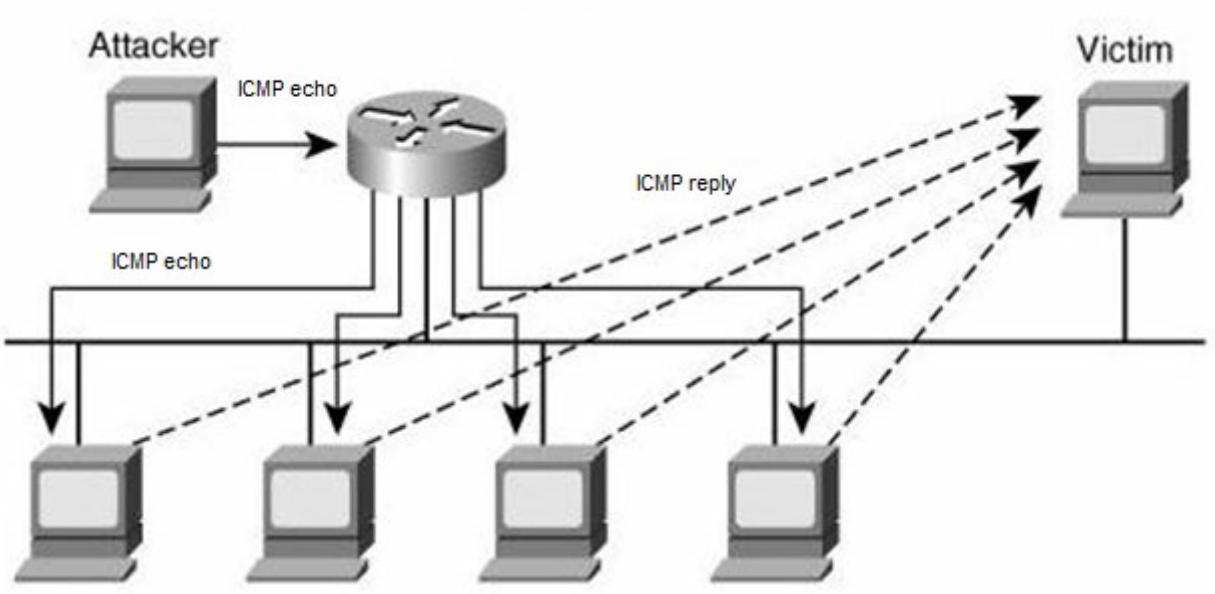
# I.1. Điểm yếu công nghệ

- Chuyện gì sẽ xảy ra nếu kẻ tấn công chỉ gửi gói SYN mà bỏ qua gói SYN-ACK ???



# I.1. Điểm yếu công nghệ

- Giảo mạo địa chỉ nguồn:




Attacker gửi gói tin ICMP echo: địa chỉ đích là Broadcast
Địa chỉ nguồn là Victim.

# I.1. Điểm yếu công nghệ

- Điểm yếu trong máy tính và hệ điều hành:
  - Không lock màn hình khi không sử dụng.
  - Không đặt mật khẩu cho tài khoản người dùng.
  - Không cập nhật bản vá cho hệ điều hành và các phần mềm ứng dụng

# I.1. Điểm yếu công nghệ

- Điểm yếu trong thiết bị mạng:
  - Tài khoản thiết lập sẵn trong các thiết bị mạng: Router, Firewall….
  - Default Password list
  - Cập nhật phiên bản mới cho hệ điều hành mạng

# I.2. Điểm yếu trong chính sách

- Chính sách an toàn thông tin.
  - Không có các văn bản chính sách an toàn thông tin
  - Thiếu kế hoạch giám sát an ninh
  - Thiếu kế hoạch khôi phục sau sự cố
  - Không có chính sách cho phần mềm, phần cứng khi có sự thay đổi bổ sung
  - Chính sách với con người.

# I.3. Cấu hình yếu

- Danh sách kiểm soát truy cập không chặt chẽ:
  - Quyền truy cập tài nguyên chia sẻ.
  - Quyền truy cập vào máy trạm, máy chủ
  - Quyền truy cập tới mạng wifi
- Mở cổng dịch vụ không cần thiết
- Các dịch vụ truy cập từ xa không đảm bảo an toàn mạnh

# II. Các hiểm họa chính

# II. Các hiểm họa chính

1. Hiểm họa có cấu trúc
2. Hiểm họa không có cấu trúc
3. Hiểm họa từ bên trong
4. Hiểm họa từ bên ngoài

# II.1. Hiểm họa có cấu trúc

- Hiểm họa do các đối tượng có tổ chức và có trình độ kỹ thuật cao thực hiện.
- Mục đích:
  - **Vụ lợi:** Dò quét thông tin, ăn cắp thông tin, tài khoản
  - **Chính trị:**
    - Hacker Trung Quốc – Mỹ,
    - Vụ việc nghe trộm ĐT của Thủ tướng Đức
    - Vụ việc WikiLeak tung thông tin của chính phủ Mỹ
  - **So tài năng:**
  - **Kinh doanh**
    - Vụ việc tại công ty VCCorp
    - Lỗ hổng “Heartbleed” trong OpenSSL: Yahoo

# II.2. Hiểm họa không có cấu trúc

- Liên quan đến tấn công có tính chất tự phát
  - Cá nhân tò mò thử nghiệm
  - Lỗ hổng phần mềm tiềm ẩn
  - Sự vô ý của người dùng:
    - Không đặt mật khẩu, hoặc mật khẩu dễ đoán.
    - Máy tính không cài chương trình anti-virus.
    - Không bảo mật dữ liệu quan trọng
- Hiểm họa do môi trường tạo ra
  - Thiên tai: động đất, cháy, nổ, mất điện

# II.3. Hiểm họa từ bên trong

- Hiểm họa được tạo ra từ những cá nhân bên trong mạng nội bộ
  - Nghe trộm thông tin
  - Sử dụng USB tùy tiện
  - Leo thang đặc quyền
  - Tài nguyên chia sẻ ko được phân quyền thích hợp
  - Xâm nhập máy trạm, máy chủ từ người dùng bên trong:
    - Thông qua mạng
    - Thông qua đường vật lý
- Hiểm họa từ mã độc (virus, Trojan, backdoor)

# II.4. Hiểm họa từ bên ngoài

- Nguồn hiểm họa xuất phát từ Internet vào mạng bên trong
  - Tấn công dò quét
  - Tấn công ứng dụng
  - Tấn công từ chối dịch vụ
- Hiểm họa từ mã độc
  - Mail, website, software
- Hiểm họa từ mạng xã hội
  - Facebook, Phishing

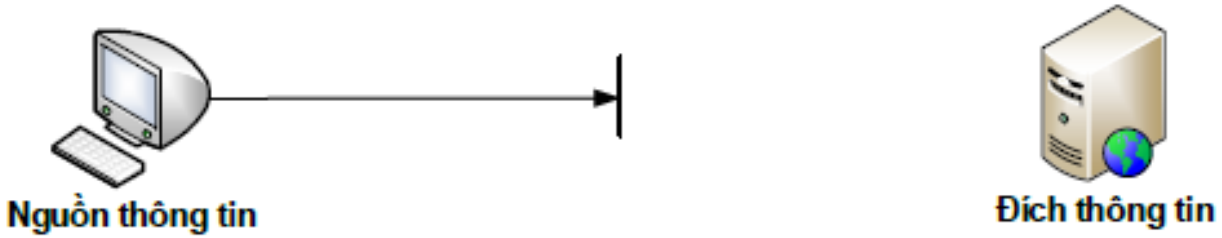
# III. Các hình thức tấn công

# III. Các hình thức tấn công

1. Ngăn chặn thông tin
2. Chặn bắt thông tin
3. Sửa đổi thông tin
4. Chèn thông tin giả

# III.1. Ngặn chặn thông tin


(a) Luồng bình thường

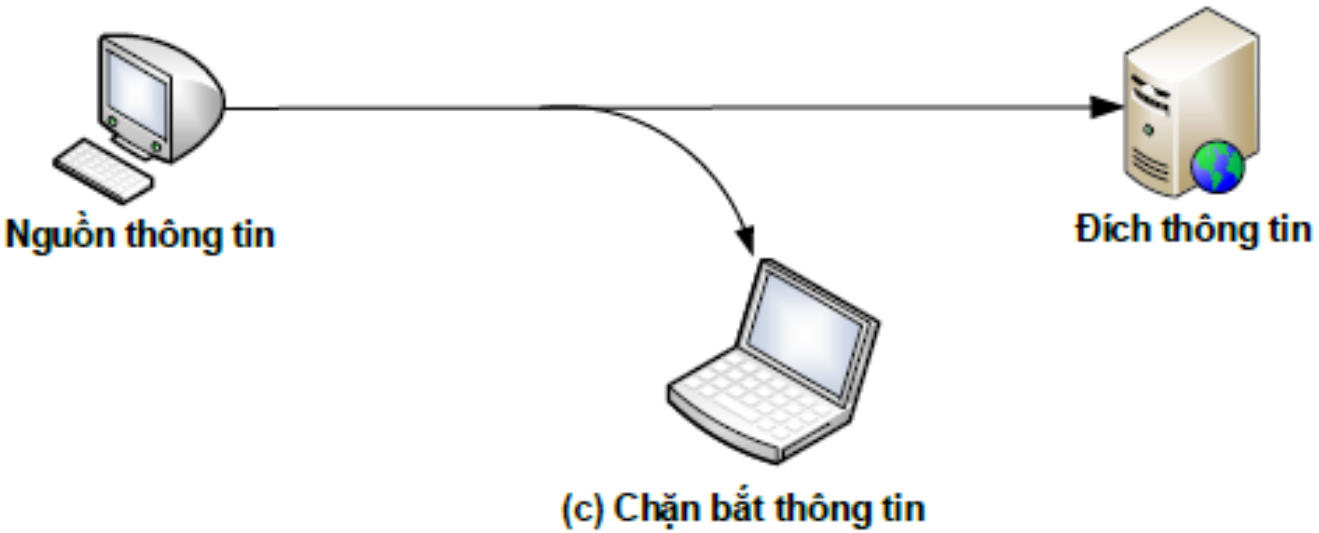



(b) Ngăn chặn thông tin

# III.1. Ngặn chặn thông tin

- Thông tin chứa trong các dạng dữ liệu: văn bản, âm thanh, hình ảnh, phần mềm…
- Được lưu giữ trong các thiết bị: Ổ đĩa, băng từ, đĩa quang…hoặc được truyền qua kênh công khai.
- Tài nguyên thông tin bị phá hủy, không sẵn sàng phục vụ, không sử dụng được.
- Đây là hình thức tấn công làm mất khả năng sẵn sàng phục vụ của thông tin.
- Ví dụ: Phá hủy đĩa cứng, cắt đứt đường truyền tin, xóa bỏ dữ liệu, ngăn chặn người dùng hợp lệ truy cập thông tin.

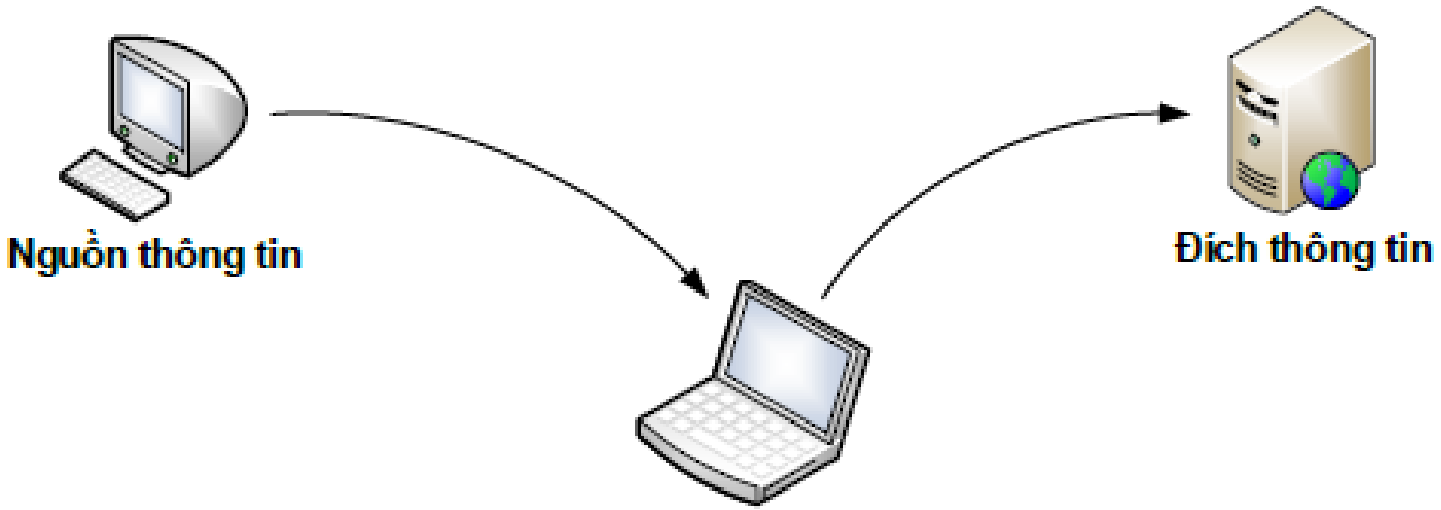
# III.2. Chặn bắt thông tin



# III.2. Chặn bắt thông tin

- Kẻ tấn công có thể tiếp cận tới tài nguyên thông tin
- Đây là hình thức tấn công vào tính bí mật của thông tin.
- Việc chặn bắt có thể là nghe trộm để thu tin và sao chép bất hợp pháp dữ liệu trong quá trình truyền tin.

# III.3. Sửa đổi thông tin

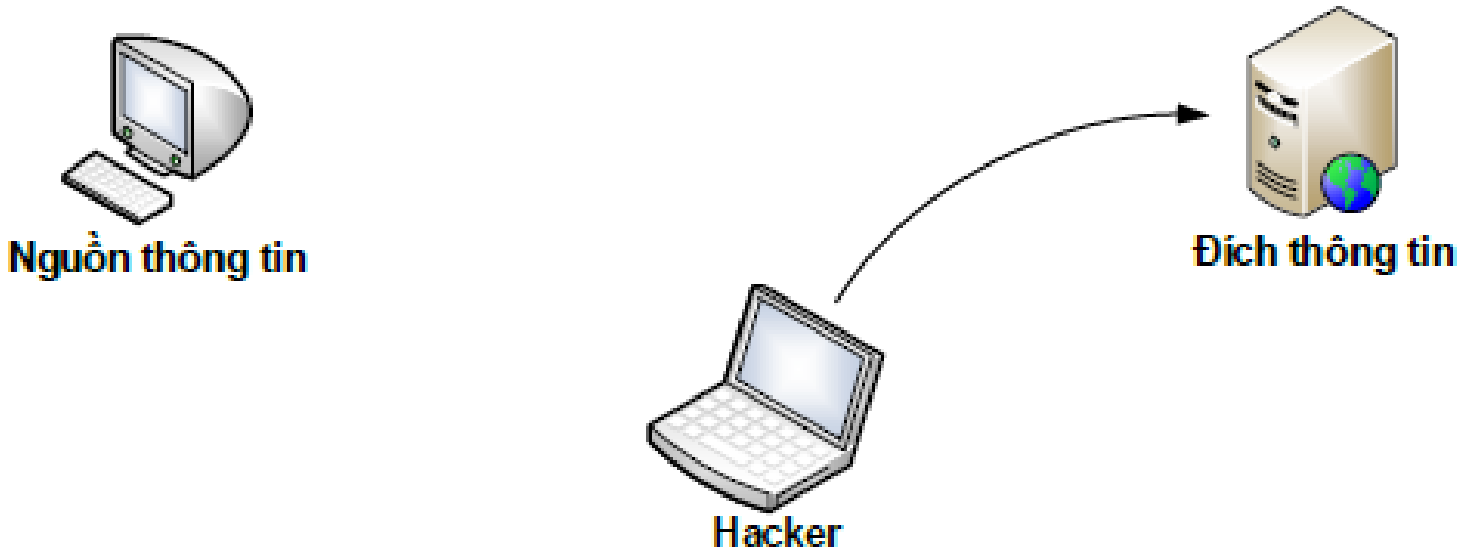



(d) Sửa đổi thông tin

# III.3. Sửa đổi thông tin

- Kẻ tấn công truy cập, chỉnh sửa thông tin lưu trữ hoặc truyền trên mạng
- Đây có thể là thay đổi giá trị trong tệp dữ liệu, sửa đổi 1 chương trình để nó vận hành khác đi, sửa đổi nội dung 1 thông báo truyền đi.
- Đây là hình thức tấn công vào tính toàn vẹn của thông tin.

# III.4. Chèn thông tin giả

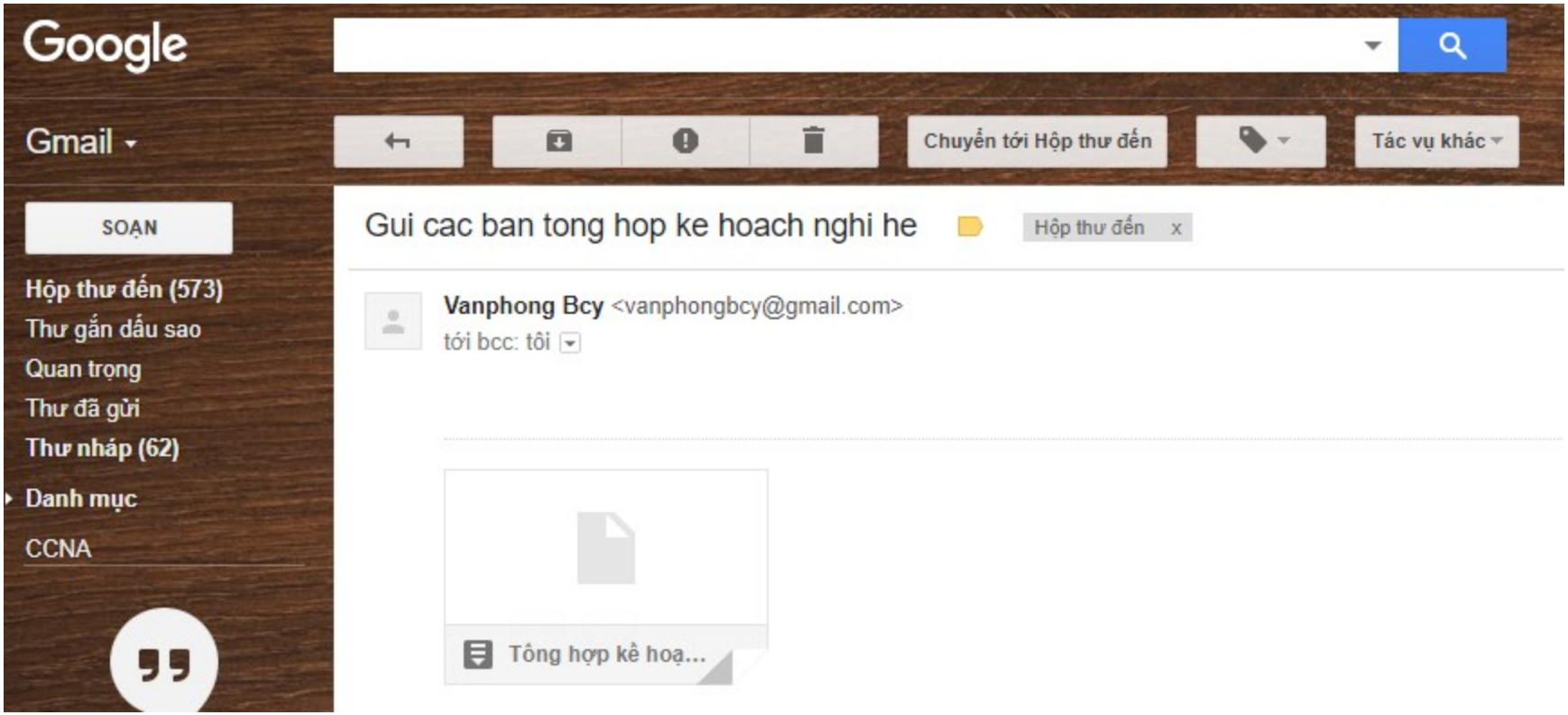



(e) Chèn thông tin giả

# III.4. Chèn thông tin giả

- Kẻ tấn công chèn các thông tin và dữ liệu giả vào hệ thống
- Đây có thể là chèn thông báo giả mạo vào mạng hay thêm các bản ghi vào tệp.
  - VD: giả mạo email
- Đây là hình thức tấn công vào tính xác thực của thông tin.

# III.4. Chèn thông tin giả



# III. Phân lớp tấn công

- Các kiểu tấn công trên được phân chia thành hai lớp cơ bản là:
  - Tấn công chủ động
  - Tấn công bị động

# III. Tấn công bị động

- Là kiểu tấn công chặn bắt thông tin như nghe trộm và quan sát truyền tin.
- Mục đích: biết được thông tin truyền trên mạng
- Chia làm 2 loại nhỏ:
  - Khám phá nội dung thông báo: Nghe trộm các cuộc nói chuyện điện thoại, xem trộm thư điện tử, xem trộm nội dung tệp tin bản rõ.
  - Phân tích luồng thông tin: Chặn bắt luồng thông tin và khám phá thông tin

# III. Tấn công bị động

- Rất khó phát hiện vì không thay đổi số liệu và không có dấu hiệu rõ ràng.
- Biện pháp: tính bí mật (mã hóa), tính toàn vẹn (ký số),

# III. Tấn công chủ động

- Là kiểu tấn công sửa đổi số liệu, tạo ra số liệu giả hoặc phá hủy dữ liệu.
- Chia làm 3 loại nhỏ:
  - Đóng giả: một thực thể: máy tính, người dùng, chương trình đóng giả 1 thực thể hợp lệ.
  - Dùng lại: chặn bắt thông báo, sao chép, sửa đổi và gửi lại thông báo.
  - Từ chối dịch vụ: ngặn chặn người dùng hợp lệ sử dụng dịch vụ.

# III. Tấn công chủ động

- Giải pháp đối với trường hợp này: phòng thủ, giám sát, phát hiện, ngăn chặn, khắc phục hậu quả.

# IV. Các dịch vụ bảo vệ thông tin

# IV. Các dịch vụ bảo vệ thông tin

Các dịch vụ bảo vệ thông tin trên mạng bao gồm:

1. Dịch vụ bí mật
2. Dịch vụ xác thực
3. Dịch vụ toàn vẹn
4. Chống chối bỏ
5. Kiểm soát truy cập
6. Sẵn sàng phục vụ

# IV.1. Dịch vụ bí mật

- Đảm bảo thông tin lưu trữ trong hệ thống máy tính hoặc thông tin truyền trên mạng chỉ sử dụng bởi người dùng hợp lệ.
- Chống lại tấn công bị động nhằm khám phá nội dung thông báo.
- Ví dụ:
  - HĐH windows sử dụng cơ chế mã hóa file, win7, win8, server 2008 sử dụng bitlocker,
  - Truyền tin: VPN, IPSec, SSH

# IV.2. Dịch vụ xác thực

- Đảm bảo truyền thông giữa người gửi và người nhận được xác thực không bị mạo danh.
- Phương pháp xác thực:
  - Xác thực dựa trên những gì đã biết: Tên đăng nhập và mật khẩu
  - Xác thực dựa trên tính năng vật lý không đổi: Sinh trắc học
  - Xác thực dựa vào những gì đã có: Thẻ bài, token, chứng thư số
  - Xác thực đa nhân tố: kết hợp 2 hay nhiều pp xác thực

# IV.3. Dịch vụ toàn vẹn

- Đảm bảo thông tin lưu trữ và thông tin truyền tải không bị sửa đổi trái phép.
- Các thuật toán được áp dụng: MD5, SHA…
- Được ứng dụng trong giao thức bảo mật: SSL, TLS, Ipsec, SSH,

# IV.4. Dịch vụ chống chối bỏ

Ngăn chặn người gửi hay người nhận chối bỏ thông báo được truyền.

- Khi thông báo được gửi đi người nhận có thể chứng minh được người nêu danh đã gửi nó đi.
- Khi thông báo được nhận, người gửi có thể chứng minh được thông báo đã nhận bởi người nhận hợp lệ.
- Ví dụ: chữ ký số, tem thời gian.

# IV.5. Kiểm soát truy cập

- Là khả năng kiểm soát và hạn chế truy cập tới tài nguyên hệ thống thông tin.
- Mỗi một thực thể muốn truy cập đều phải định danh hay xác nhận có quyền truy cập phù hợp.

# IV.6. Sẵn sàng phục vụ

- Đảm bảo các tài nguyên mạng máy tính luôn sẵn sàng đối với người dùng hợp lệ.
- Các tấn công có thể làm mất mát hoặc giảm khả năng sẵn sàng phục vụ của tài nguyên mạng.
- Ví dụ:
  - Thiết bị lưu điện,
  - Cân bằng tải,
  - Sao lưu dự phòng,
  - Cơ chế RAID cho ổ cứng…

# V. Các mô hình bảo mật chung

1. Mô hình bảo mật theo quan niệm cổ điển
2. Mô hình bảo mật theo chiều sâu
3. Mô hình bảo mật X.800
4. Phân vùng an toàn mạng

# V.1. Mô hình CIA

- C = Confidentiality – Tính bí mật
- I = Integrity – Tính toàn vẹn
- A = Availability – Tính sẵn sàng

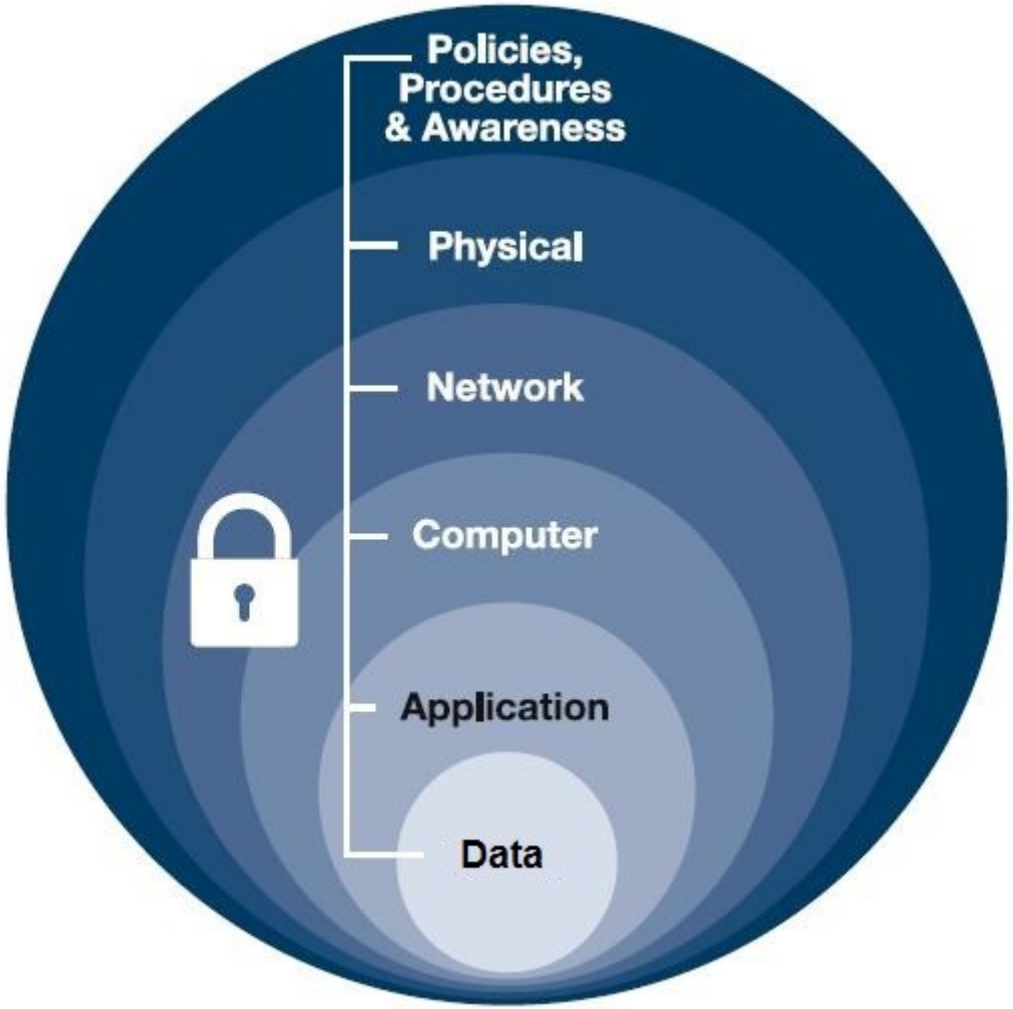
# V.1. Mô hình CIA

- Là tập các cơ chế nhằm bổ sung hệ thống bảo mật theo mô hình CIA.
  - Access Control.
  - Authentication.
  - Auditing.
- *Phân biệt với thuật ngữ AAA của Cisco (Authentication, Authorization, Accouting)*

# V.1. Mô hình CIA

- Auditing: Là phương pháp ghi lại và kiểm tra các hoạt động trên hệ thống.
- System events auditing
- NTFS access auditing
- System log
- System scanning: quét lỗ hổng, điểm yếu, phân tích

# V.2. Mô hình bảo mật theo chiều sâu



# V.2. Mô hình bảo mật theo chiều sâu

- **Lớp 1 (Data):** Mã hóa, xác thực, phân quyền
- **Lớp 2 (Application):** Cập nhật bản vá, Antivirus,
- **Lớp 3 (Computer):** Xác thực truy cập,
- **Lớp 4 (Network):** Phân vùng, Firewall, IDS/IPS,
- **Lớp 5 (Physical):** Hệ thống khóa cửa, tủ Rack, Camera…
- **Lớp 6 (Policy):** Quy tắc, quy định về truy cập, sử dụng tài nguyên, thiết lập mật khẩu, chính sách về con người, sao lưu và phục hồi…

# V.3. Mô hình bảo mật X.800

- Liên hiệp viễn thông quốc tế ITO đưa ra kiến trúc an ninh X.800 dành cho hệ thống trao đổi thông tin mở OSI.
- X800 là dịch vụ cung cấp nhằm đảm bảo an toàn thông tin thiết yếu và việc truyền dữ liệu của hệ thống.
- Xem xét vấn đề bảo mật trong tương quan với mô hình hệ thống mở OSI theo 3 phương diện:
  - Loại hình tấn công
  - Cơ chế bảo mật
  - Dịch vụ bảo mật

# V.3. Mô hình bảo mật X.800

- **Cơ chế an toàn chuyên dụng:** được cài đặt trong một giao thức của một tầng chuyển vận: mã hoá, chữ ký điện tử, quyền truy cập, toàn vẹn dữ liệu, trao đổi có phép, kiểm soát định danh.
- **Cơ chế an toàn thông dụng:** không chỉ rõ việc sử dụng cho giao thức trên tầng nào hoặc dịch vụ an ninh cụ thể nào: chức năng tin cậy, nhãn an toàn, phát hiện sự kiện, điều tra sự cố, khôi phục an toàn.