TẤN CÔNG MẠNG MÁY TÍNH

Giáo viên: PGS.TS. Nguyễn Hiếu Minh

Nội dung trình bày

1. Tổng quan về tấn công mạng
2. Các mô hình tấn công mạng
3. Một số kỹ thuật tấn công mạng

1. Tổng quan về tấn công mạng

A. ĐỊNH NGHĨA

- ✓ Hiện nay vẫn chưa có định nghĩa chính xác về thuật ngữ "tấn công" (xâm nhập, công kích). Mỗi chuyên gia trong lĩnh vực ATTT luận giải thuật ngữ này theo ý hiểu của mình. Ví dụ, "xâm nhập - là tác động bất kỳ đưa hệ thống từ trạng thái an toàn vào tình trạng nguy hiểm".
- ✓ Thuật ngữ này có thể giải thích như sau: "xâm nhập - đó là sự phá huỷ chính sách ATTT" hoặc "là tác động bất kỳ dẫn đến việc phá huỷ tính toàn vẹn, tính bí mật, tính sẵn sàng của hệ thống và thông tin xử lý trong hệ thống".

Định nghĩa

- ***Tấn công (attack) là hoạt động có chủ ý của kẻ phạm tội lợi dụng các thương tổn của hệ thống thông tin và tiến hành phá vỡ tính sẵn sàng, tính toàn vẹn và tính bí mật của hệ thống thông tin.***

Tổng quan

- Tấn công (*attack, intrustion*) mạng là các tác động hoặc là trình tự liên kết giữa các tác động với nhau để phá huỷ, dẫn đến việc hiện thực hoá các nguy cơ bằng cách lợi dụng đặc tính dễ bị tổn thương của các hệ thống thông tin này.
  - Có nghĩa là, nếu có thể bài trừ nguy cơ thương tổn của các hệ thông tin chính là trừ bỏ khả năng có thể thực hiện tấn công.

Một số phương thức tấn công

- Phân loại

1) Tấn công thăm dò.
2) Tấn công sử dụng mã độc.
3) Tấn công xâm nhập mạng.
4) Tấn công từ chối dịch vụ.

- Hoặc:

1) Tấn công chủ động.
2) Tấn công thụ động.

Một số khái niệm cơ bản

1. Người thực hiện tấn công

- Người thực hiện các tấn công mạng thường là những người có hiểu biết sâu sắc về giao thức TCP/IP, có hiểu biết về hệ điều hành, có thể sử dụng thành thạo một số ngôn ngữ lập trình.

  - Các hướng tấn công:

    ✓ Tấn công từ bên trong mạng.

    ✓ Tấn công từ bên ngoài mạng.

Tấn công bên trong mạng

- *Tấn công không chủ ý*: Nhiều hư hại của mạng do người dùng trong mạng vô ý gây nên. Những người này có thể vô ý để hacker bên ngoài hệ thống lấy được password hoặc làm hỏng các tài nguyên của mạng do thiếu hiểu biết.
- *Tấn công có chủ ý*: Kẻ tấn có chủ ý chống lại các qui tắc, các qui định do các chính sách an ninh mạng đưa ra.

Tấn công từ ngoài mạng

- *Kẻ tấn công nghiệp dư ("script-kiddy")*: Dùng các script đã tạo sẵn và có thể tạo nên các các thiệt hại đối với mạng.
- *Kẻ tấn công đích thực ("true- hacker")*: Mục đích chính của nhóm người này khi thực hiện các tấn công mạng là để mọi người thừa nhận khả năng của họ và để được nổi tiếng.
- *Kẻ tấn công chuyên nghiệp ("the elite")*: Thực hiện các tấn công mạng là để thu lợi bất chính.

Một số khái niêm cơ bản

2. Thời điểm thực hiện tấn công

- Bất kỳ.
- Thường thực hiện về đêm.

3. Hệ điều hành sử dụng để tấn công

- Bất kỳ.
- Thường sử dụng các HĐH mã nguồn mở.

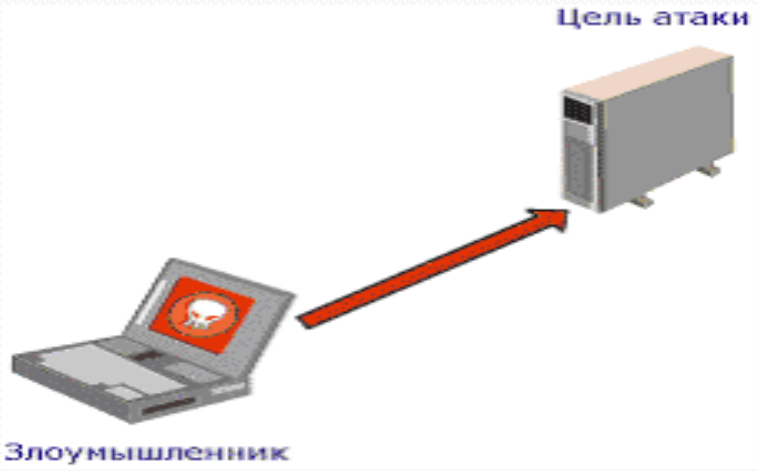
4. Các hệ thống mục tiêu

- Con người, phần cứng, phần mềm.

2. Các mô hình tấn công mạng

1. Mô hình tấn công truyền thống

- Mô hình tấn công truyền thống được tạo dựng theo nguyên tắc "một đến một" hoặc "một đến nhiều", có nghĩа là cuộc tấn công xảy ra từ một nguồn gốc.
- Mô tả: Tấn công "một đến một"

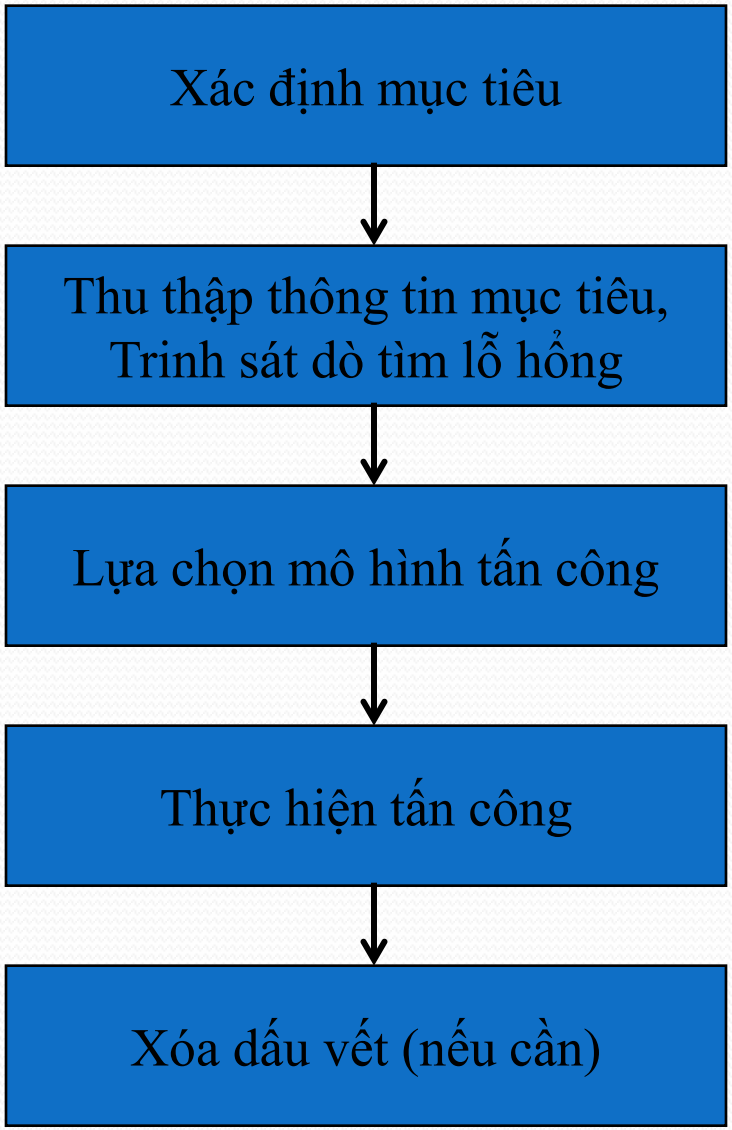


Mô hình tấn công phân tán

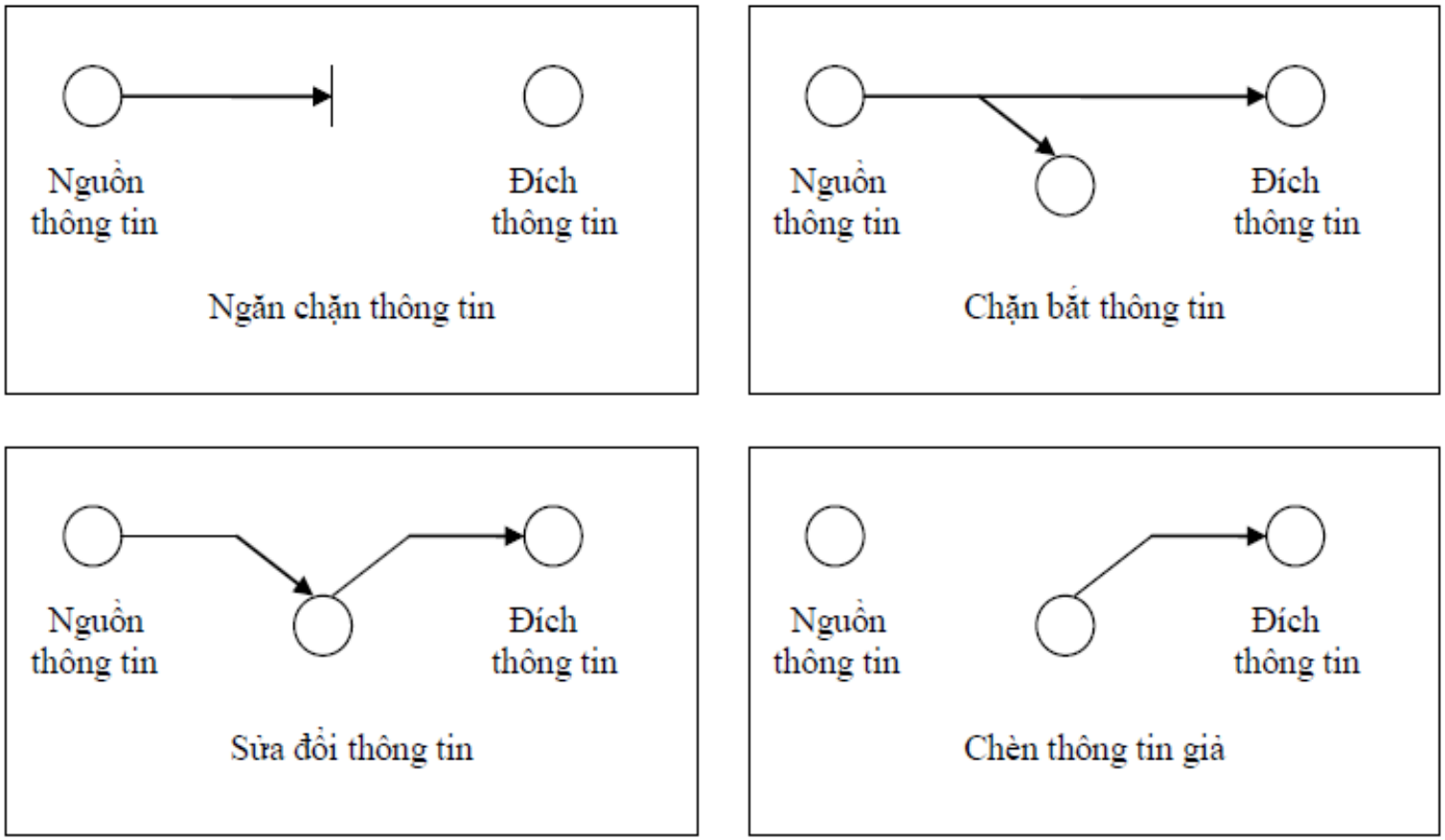
2. Mô hình tấn công phân tán

- Khác với mô hình truyền thống trong mô hình tấn công phân tán sử dụng quan hệ "nhiều đến một" và "nhiều đến nhiều".
- Tấn công phân tán dựa trên các cuộc tấn công "cổ điển" thuộc nhóm "từ chối dịch vụ", chính xác hơn là dựa trên các cuộc tấn công như Flood hay Storm (những thuật ngữ trên có thể hiểu tương đương như "bão", "lũ lụt" hay "thác tràn").

3. Các bước tấn công



Các tấn công đối với thông tin trên mạng



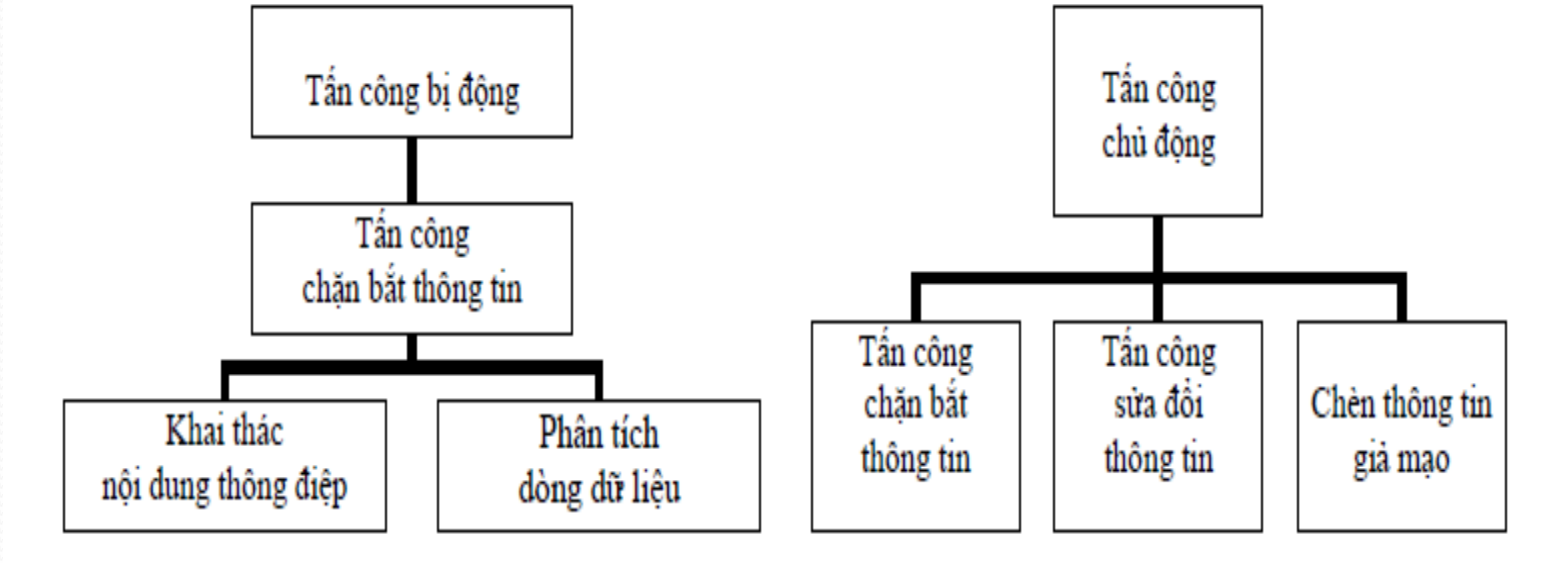
Các tấn công đối với thông tin trên mạng

- **Tấn công ngăn chặn thông tin (interruption)**
- Tài nguyên thông tin bị phá hủy, không sẵn sàng phục vụ hoặc không sử dụng được. Đây là hình thức tấn công làm mất khả năng sẵn sàng phục vụ của thông tin.
- **Tấn công chặn bắt thông tin (interception)**
- Kẻ tấn công có thể truy nhập tới tài nguyên thông tin. Đây là hình thức tấn công vào tính bí mật của thông tin.

Các tấn công đối với thông tin trên mạng

- **Tấn công sửa đổi thông tin (Modification)**
  - Kẻ tấn công truy nhập, chỉnh sửa thông tin trên mạng.
  - Đây là hình thức tấn công vào tính toàn vẹn của thông tin.
- **Chèn thông tin giả mạo (Fabrication)**
  - Kẻ tấn công chèn các thông tin và dữ liệu giả vào hệ thống.
  - Đây là hình thức tấn công vào tính xác thực của thông tin.

Tấn công bị động (passive attacks) và chủ động (active attacks)



Tấn công bị động (passive attacks)

- Mục đích của kẻ tấn công là biết được thông tin truyền trên mạng.
- Có hai kiểu tấn công bị động là khai thác nội dung thông điệp và phân tích dòng dữ liệu.
- Tấn công bị động rất khó bị phát hiện vì nó không làm thay đổi dữ liệu và không để lại dấu vết rõ ràng. Biện pháp hữu hiệu để chống lại kiểu tấn công này là ngăn chặn (đối với kiểu tấn công này, ngăn chặn tốt hơn là phát hiện).

Tấn công chủ động (active attacks)

- Tấn công chủ động được chia thành 4 loại nhỏ sau:
  - Giả mạo (Masquerade): Một thực thể (người dùng, máy tính, chương trình…) đóng giả thực thể khác.
  - Dùng lại (replay): Chặn bắt các thông điệp và sau đó truyền lại nó nhằm đạt được mục đích bất hợp pháp.
  - Sửa thông điệp (Modification of messages): Thông điệp bị sửa đổi hoặc bị làm trễ và thay đổi trật tự để đạt được mục đích bất hợp pháp.
  - Từ chối dịch vụ (Denial of Service - DoS): Ngăn cấm việc sử dụng bình thường hoặc quản lý các tiện ích truyền thông.