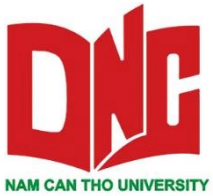
BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NAM CẦN THƠ



QUẢN TRỊ MẠNG

Chương 5:

ĐẢM BẢO AN NINH MẠNG

Giảng viên: ThS. Nguyễn Minh Triết

Đảm bảo an ninh mạng

5.1. Tổng quan về an ninh mạng

5.2. Một số loại tấn công qua mạng

5.3. Các khái niệm cơ bản của hệ thống thông tin

5.4. Bảo mật cơ sở hạ tầng hệ thống thông tin

5.5. Phân loại hacker

Đảm bảo an ninh mạng

5.1. **Tổng quan về an ninh mạng**

5.2. Một số loại tấn công qua mạng

5.3. Các khái niệm cơ bản của hệ thống thông tin

5.4. Bảo mật cơ sở hạ tầng hệ thống thông tin

5.5. Phân loại hacker

Tổng quan về an ninh mạng

- Internet được thiết kế ban đầu không quan tâm nhiều đến vấn đề an ninh mạng
  - Cách nhìn ban đầu: “một nhóm người dùng tin tưởng lẫn nhau được gắn với một hệ thống mạng trong suốt”
  - Các nhà thiết kế giao thức Internet chọn phương pháp “catch-up”

Tổng quan về an ninh mạng (tt)

- Các lĩnh vực của an ninh mạng
  - Kẻ xấu có thể tấn công mạng máy tính như thế nào
  - Chúng ta có thể bảo vệ mạng chống lại các tấn công như thế nào
  - Có thể thiết kế kiến trúc mạng như thế nào để không bị tấn công

Tổng quan về an ninh mạng (tt)

- Phần mềm độc hại (malware) có thể đi vào máy chủ từ: Virus (vi-rút), Worm (sâu), Trojan horse (ngựa Trojan)
- Phần mềm độc hại có thể ghi bàn phím, thu thập thông tin người dùng, gửi dữ liệu của người dùng ra bên ngoài,…
- Phần mềm độc hại thông thường có tính năng tự nhân bản
- Thiết bị nhiễm mã độc có thể bị lạm dụng (botnet) để tấn công thiết bị khác

Tổng quan về an ninh mạng (tt)

- Trojan horse:
  - Ẩn phía sau những phần mềm hữu ích
  - Thường xuất hiện ở các trang web (Active-X, plugin)
- Virus:
  - Thường lây nhiễm qua các đối tượng như tập tin đính kèm
  - Có khả năng tự nhân bản và lây nhiễm đến các đối tượng khác

Tổng quan về an ninh mạng (tt)

- Worm:
  - Có thể tồn tại độc lập, không cần đính vào tập tin
  - Có khả năng tự nhân bản và lan truyền
- Rootkit:
  - Chủ động "tàng hình" đối với người dùng, hệ điều hành và các chương trình anti-virus/anti-malware.
  - Có thể được cài đặt bằng nhiều cách bao gồm việc khai thác lỗ hổng trong hệ điều hành hoặc lấy quyền quản trị máy tính.

Đảm bảo an ninh mạng

5.1. Tổng quan về an ninh mạng

5.2. **Một số loại tấn công qua mạng**

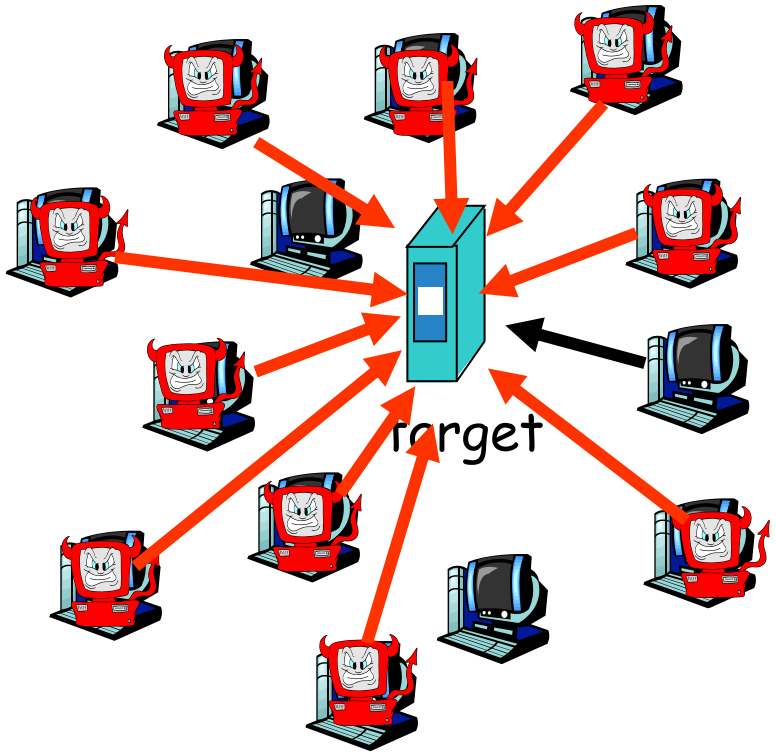
5.3. Các khái niệm cơ bản của hệ thống thông tin

5.4. Bảo mật cơ sở hạ tầng hệ thống thông tin

Một số loại tấn công qua mạng

- **DoS (Denial of Service):** kẻ tấn công làm cho các nguồn tài nguyên (máy chủ, băng thông) không còn có sẵn để phục vụ cho truy cập hợp pháp, bằng cách sử dụng nhiều tài nguyên với những lưu lượng không có thật

1. Xác định mục tiêu
2. Thâm nhập vào các host (botnet)
3. Gửi các gói tin đến mục tiêu từ các host đã thâm nhập

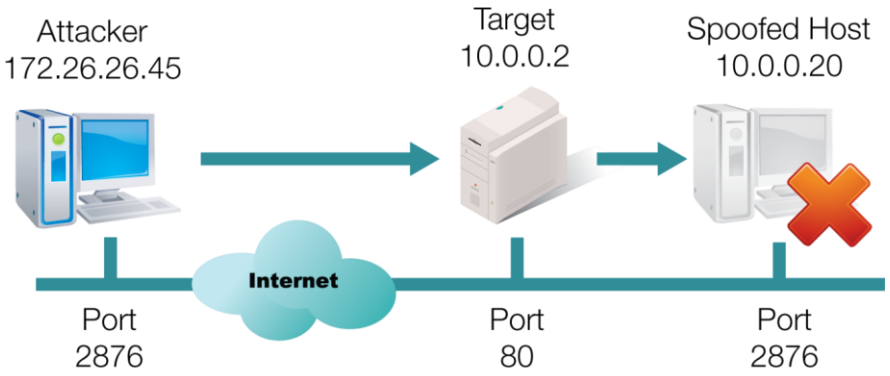


Một số loại tấn công qua mạng (tt)

- **DDoS (Distributed Denial of Service):**
  - Hình thức giống với DoS
  - Sử dụng nhiều botnet hơn, phân tán hơn để tấn công mục tiêu

Một số loại tấn công qua mạng (tt)

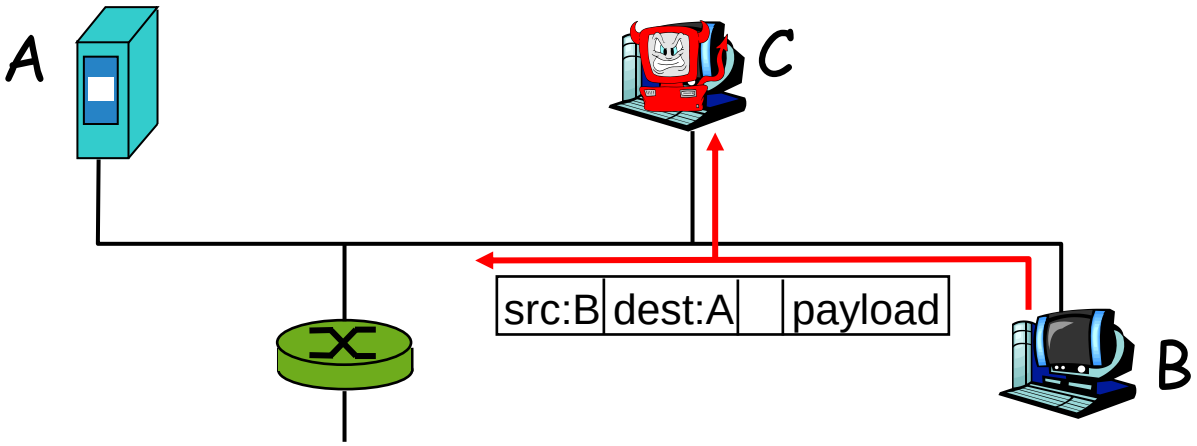
- **SYN Flood:**
  - Attacker sử dụng IP giả để gửi một số lượng lớn yêu cầu kết nối (SYN) đến máy nạn nhân.



SYN, SRC: 10.0.0.20, DST: 10.0.0.2	SYN-ACK	?
SYN, SRC: 10.0.0.20, DST: 10.0.0.2	SYN-ACK	?
SYN, SRC: 10.0.0.20, DST: 10.0.0.2	SYN-ACK	?
SYN, SRC: 10.0.0.20, DST: 10.0.0.2	SYN-ACK	?
SYN, SRC: 10.0.0.20, DST: 10.0.0.2	SYN-ACK	?

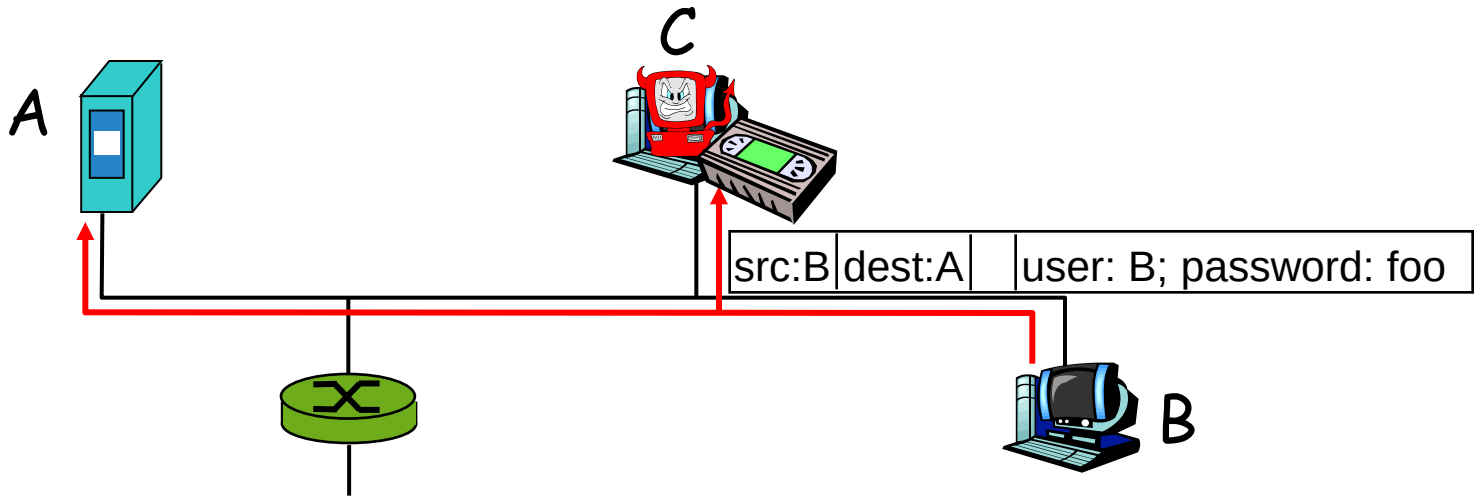
Một số loại tấn công qua mạng (tt)

- **Packet sniffing:**
  - Đường truyền dùng chung (Ethernet, wireless)
  - Đọc, ghi lại các gói tin đi qua



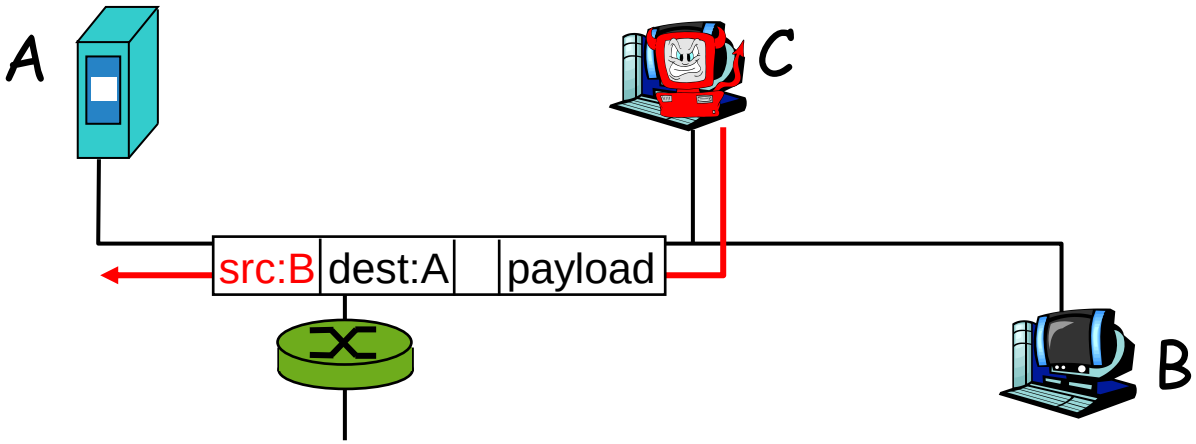
Một số loại tấn công qua mạng (tt)

- **Record-and-playback:**
  - Nghe lén thông tin nhạy cảm (như mật khẩu), ghi nhận lại và sau đó sử dụng



Một số loại tấn công qua mạng (tt)

- **IP spoofing:**
  - Gửi gói tin với địa chỉ nguồn giả mạo



Đảm bảo an ninh mạng

5.1. Tổng quan về an ninh mạng

5.2. Một số loại tấn công qua mạng

5.3. **Các khái niệm cơ bản của hệ thống thông tin**

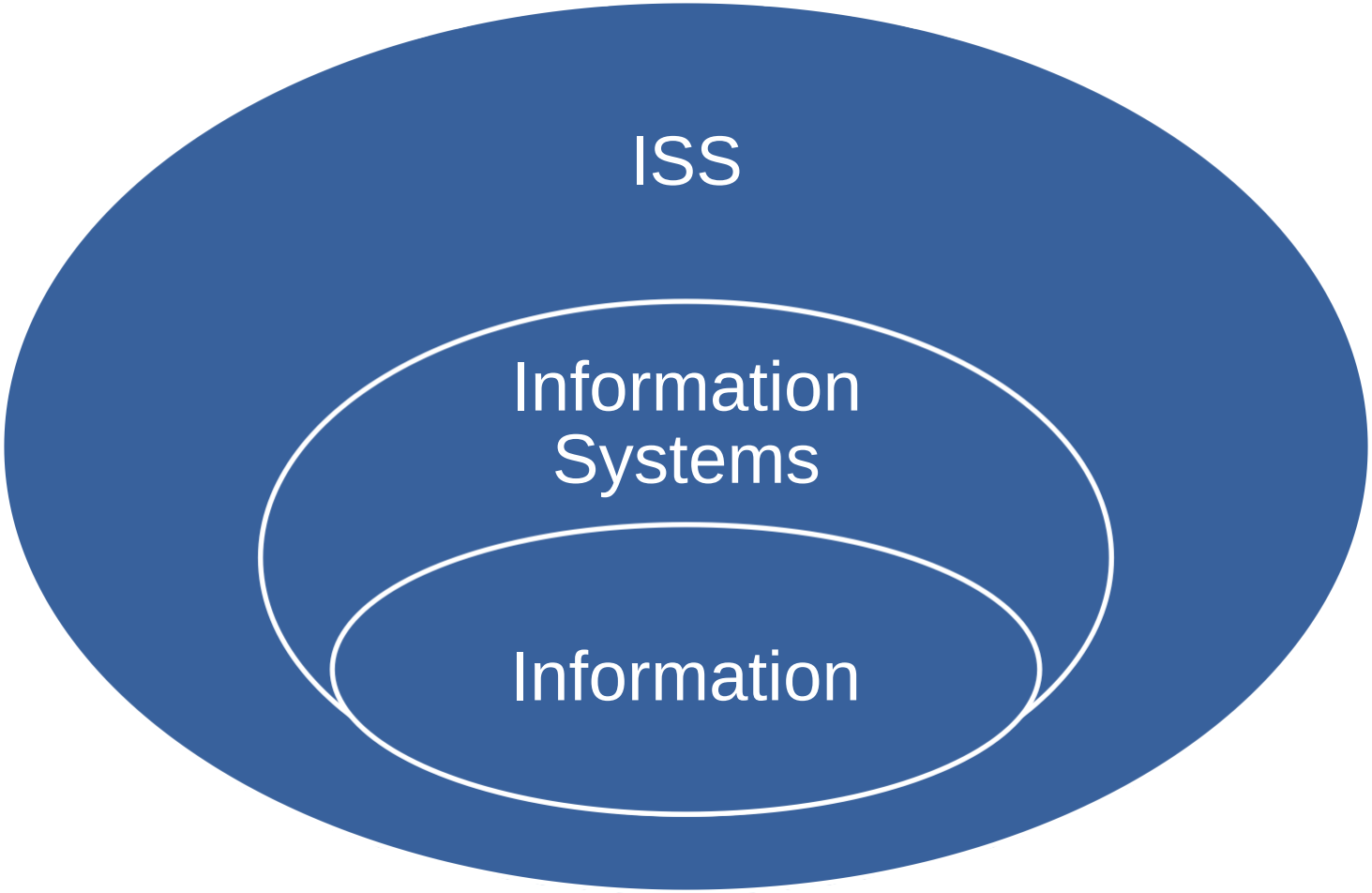
5.4. Bảo mật cơ sở hạ tầng hệ thống thông tin

5.5. Phân loại hacker

Các khái niệm cơ bản của hệ thống thông tin

- Hệ thống thông tin (Information System - IS):
  - Bao gồm phần cứng, hệ điều hành, phần mềm dùng để thu thập, lưu trữ, xử lý dữ liệu của cá nhân hoặc tổ chức.
- Bảo mật hệ thống thông tin (Information Systems Security - ISS):
  - Tập hợp các hoạt động nhằm bảo vệ hệ thống thông tin và dữ liệu bên trong nó.

Các khái niệm cơ bản của hệ thống thông tin (tt)



Các khái niệm cơ bản của hệ thống thông tin (tt)

- Rủi ro (Risk):
  - Là khả năng một sự việc xấu xảy ra đối với tài sản của cá nhân/ tổ chức
    - Mất mát dữ liệu
    - Hư hao tài sản
    - ...

Các khái niệm cơ bản của hệ thống thông tin (tt)

- Mối nguy (Threat):
  - Là bất kỳ hành động nào có thể làm hư hỏng, mất mát tài sản
    - Thiên tai
    - Mã độc
    - Truy cập trái phép
    - ...

Các khái niệm cơ bản của hệ thống thông tin (tt)

- Lỗ hổng (Vulnerability):
  - Là điểm yếu cho phép mối nguy nhận ra, hoặc có ảnh hưởng đến tài sản
  - Các nhà cung cấp phần mềm tự bảo vệ mình khỏi trách nhiệm của lỗ hổng bảo mật bằng thõa thuận cấp phép người dùng cuối (EULA)

Đảm bảo an ninh mạng

5.1. Tổng quan về an ninh mạng

5.2. Một số loại tấn công qua mạng

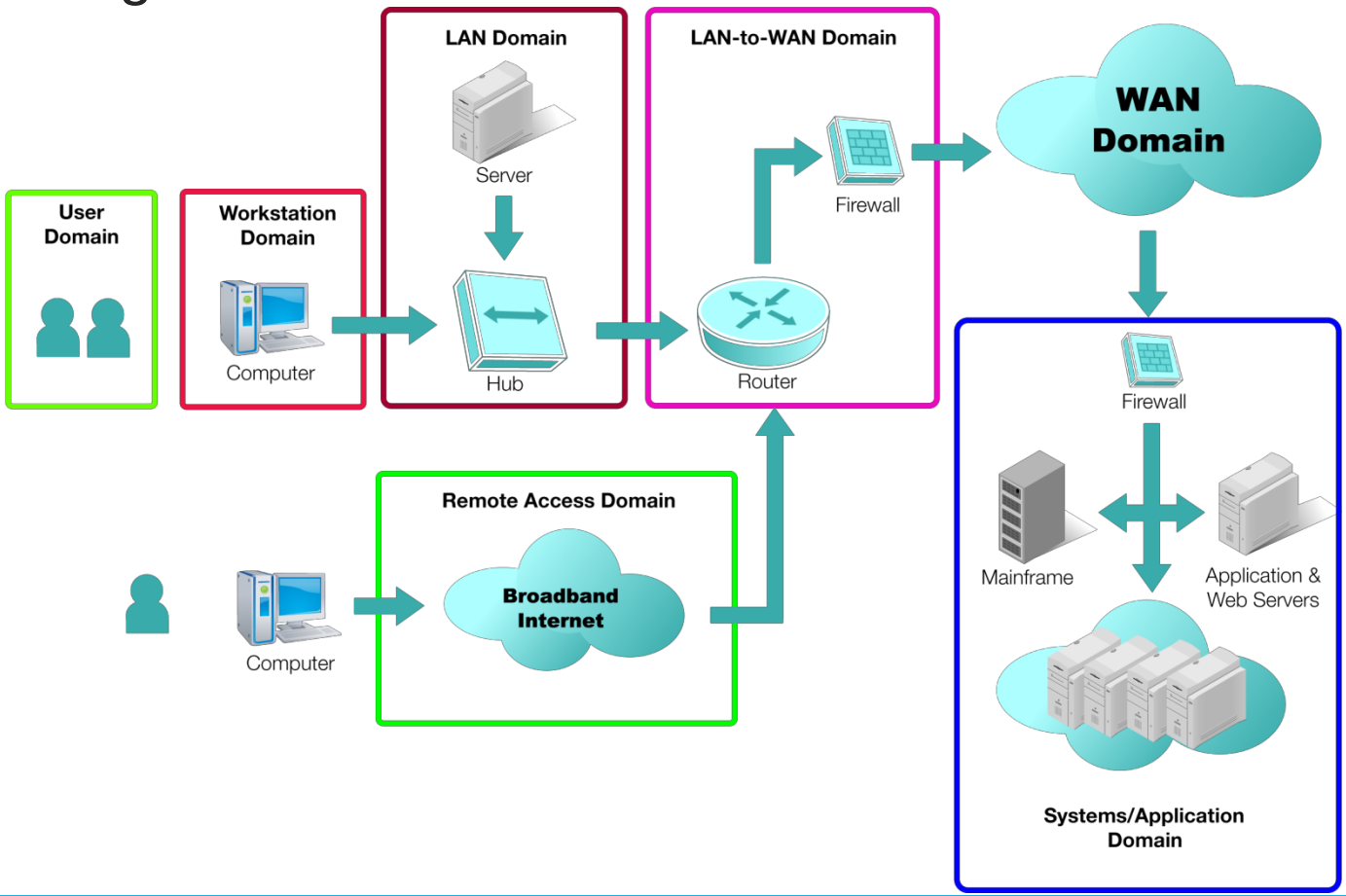
5.3. Các khái niệm cơ bản của hệ thống thông tin

5.4. **Bảo mật cơ sở hạ tầng hệ thống thông tin**

5.5. Phân loại hacker

Bảo mật hệ thống thông tin (tt)

- Bảy miền (domain) của cơ sở hạ tầng công nghệ thông tin:



Bảo mật hệ thống thông tin (tt)

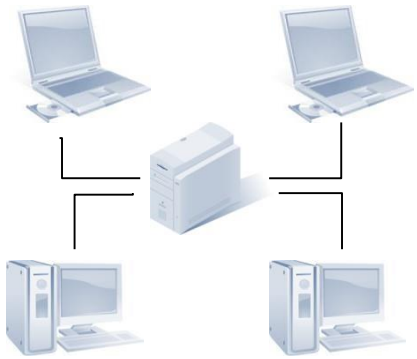
- User domain:
  - Xác định những người truy cập hệ thống thông tin tổ chức.
  - Nguy cơ:
    - Sự thiếu nhận thức của người dùng
    - Sự thờ ơ của người dùng đối với các chính sách
    - Người dùng vi phạm chính sách bảo mật
    - Người dùng phá hoại dữ liệu/ hệ thống
    - Nhân viên bất mãn với tổ chức
    - Nhân viên tống tiền tổ chức
    - …

Bảo mật hệ thống thông tin (tt)

- Workstation domain:
  - Máy tính để bàn, máy tính xách tay, hoặc thiết bị đầu cuối chuyên dụng được kết nối vào hệ thống.
  - Nguy cơ:
    - Truy cập trái phép vào workstation
    - Lỗ hổng trên hệ điều hành của workstation
    - Lỗ hổng của ứng dụng được cài đặt trên workstation
    - Mã độc, virus,…
    - …

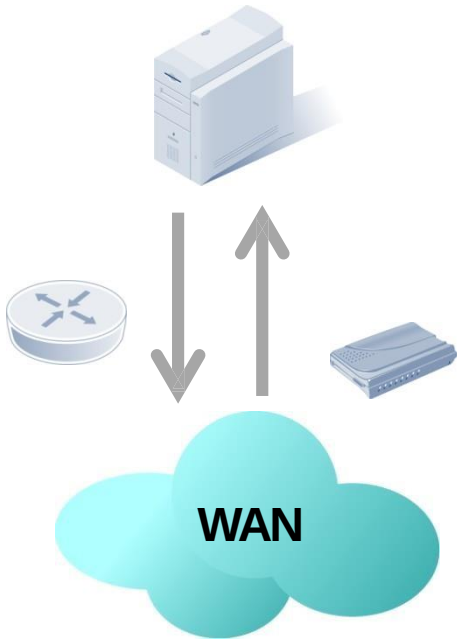
Bảo mật hệ thống thông tin (tt)

- LAN domain:
  - Tập hợp các máy tính, thiết bị được kết nối lại với nhau
  - Nguy cơ:
    - Truy cập trái phép vào mạng LAN
    - Truy cập trái phép vào ứng dụng, dữ liệu
    - Lỗ hổng hệ điều hành của máy chủ mạng LAN
    - Lỗ hổng ứng dụng trên máy chủ mạng LAN
    - Lỗ hổng đối với mạng nội bộ không dây (WLAN)
    - …



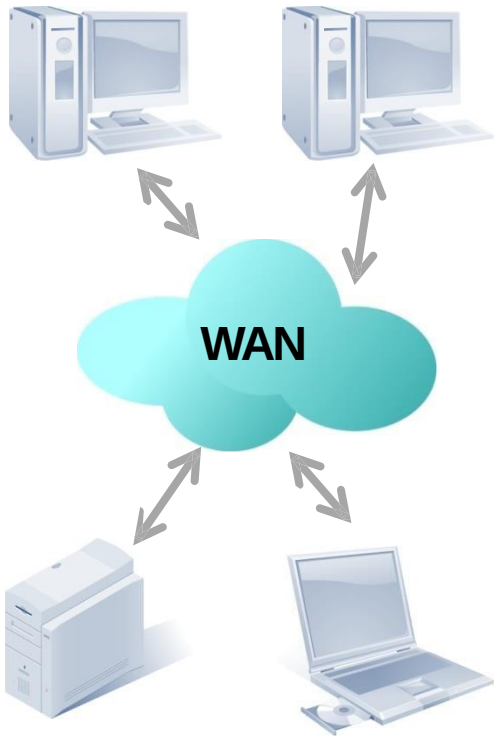
Bảo mật hệ thống thông tin (tt)

- LAN-to-WAN domain:
  - Là nơi cơ sở hạ tầng hệ thống thông tin được kết nối với mạng diện rộng và mạng internet
  - Nguy cơ:
    - Bị tấn công thăm dò
    - Truy cập trái phép
    - Lỗ hổng trên tường lửa, router, thiết bị mạng khác
    - …



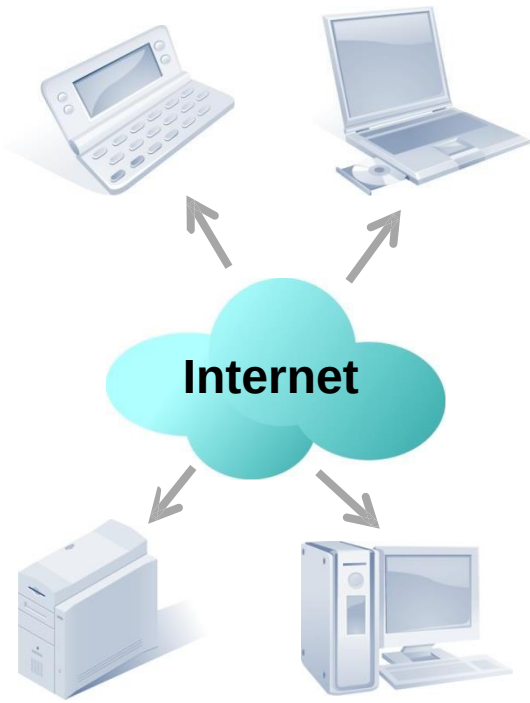
Bảo mật hệ thống thông tin (tt)

- WAN domain:
  - Kết nối với các địa điểm ở xa
  - Nguy cơ:
    - Dữ liệu public có thể bị truy cập
    - Dữ liệu gửi đi không được mã hóa
    - Dễ bị nghe lén
    - Dễ bị tấn công
    - …



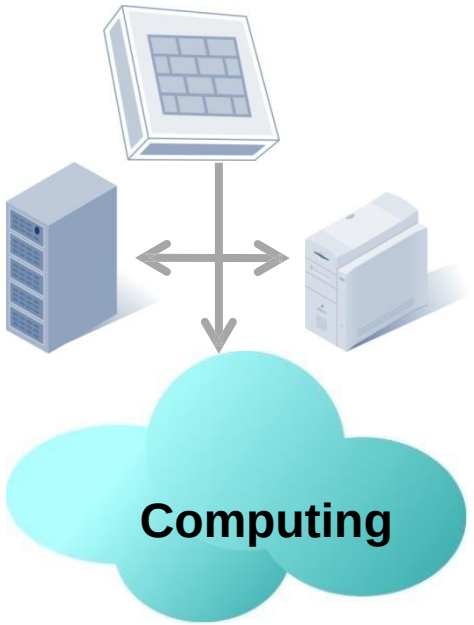
Bảo mật hệ thống thông tin (tt)

- Remote access domain:
  - Kết nối người dùng ở xa với cơ sở hạ tầng công nghệ thông tin của tổ chức
  - Truy cập từ xa rất quan trọng đối với nhân viên làm việc ở nhà, cần truy cập vào hệ thống
  - Nguy cơ:
    - Bị tấn công Brute-force đối với tài khoản đăng nhập
    - Truy cập trái phép
    - Dữ liệu quan trọng bị xâm phạm từ xa
    - Rò rĩ dữ liệu
    - …



Bảo mật hệ thống thông tin (tt)

- System/ Application domain:
  - Chứa ứng dụng, dữ liệu quan trọng của tổ chức
  - Chỉ những người dùng được ủy quyền mới được phép truy cập
  - Nguy cơ:
    - Bị truy cập trái phép
    - Lỗ hổng hệ điều hành của máy chủ
    - Lỗ hổng của ứng dụng được cài đặt trên máy chủ
    - Dữ liệu bị mất hoặc bị sửa đổi
    - …



Bảo mật hệ thống thông tin (tt)

- Người dùng là điểm yếu nhất trong bảo mật cơ sở hạ tầng công nghệ thông tin
  - Người dùng nguy hiểm
  - Người dùng chưa được đào tạo
  - Người dùng bất cẩn

Bảo mật hệ thống thông tin (tt)

- Chiến lược nhằm giảm thiểu rủi ro:
  - Kiểm tra nền tảng của người dùng
  - Đánh giá thường xuyên
  - Xoay vòng người dùng truy cập vào hệ thống
  - Xây dựng kế hoạch bảo mật
  - Kiểm soát an ninh

Đảm bảo an ninh mạng

5.1. Tổng quan về an ninh mạng

5.2. Một số loại tấn công qua mạng

5.3. Các khái niệm cơ bản của hệ thống thông tin

5.4. Bảo mật cơ sở hạ tầng hệ thống thông tin

5.5. **Phân loại hacker**

Phân loại hacker

- Hack là việc lợi dụng những lỗ hổng bảo mật để can thiệp vào phần mềm, phần cứng, hệ thống máy tính, mạng máy tính nhằm thay đổi các chức năng vốn có của nó theo ý thích của bản thân.
- Hacker (tin tặc) là những người hiểu rõ hoạt động của hệ thống máy tính, mạng máy tính, có thể viết hay chỉnh sửa phần mềm, phần cứng máy tính.
- Công việc của hacker bao gồm lập trình, quản trị và bảo mật.
- Phân loại: hacker mũ trắng, hacker mũ đen, hacker mũ xám, hacker mũ xanh.

Phân loại hacker (tt)

- Hacker mũ trắng (white hat)
  - Đây là nhóm hacker thân thiện.
  - Công việc thường làm là hack sau đó báo cho đơn vị quản lý phần mềm, website, hệ thống máy tính về các lỗ hổng bảo mật để họ kịp thời sửa chữa, tránh bị người khác trục lợi.

Phân loại hacker (tt)

- Hacker mũ đen (black hat)
  - Thực hiện công việc hack nhằm mục đích trục lợi cho bản thân hoặc phá hoại là chính.
  - Ngược lại với hacker mũ trắng.

Phân loại hacker (tt)

- Hacker mũ xám (grey hat)
  - Là những hacker nằm tại ranh giới giữa hacker mũ trắng và hacker mũ đen.
  - Những hacker mũ xám khi thì hack vì mục đích tốt lúc thì lại hack vì mục đích xấu.

Phân loại hacker (tt)

- Hacker mũ xanh (blue hat)
  - Là những chuyên viên, chuyên gia về lĩnh vực máy tính, được đào tạo bài bản.
  - Thường được sử dụng để đánh giá về độ an toàn bảo mật của hệ thống máy tính, phần mềm máy tính,… trước khi hệ thống được đưa vào vận hành hay phân phối ra bên ngoài.
  - Có thể kết hợp với các người thiết kế hay lập trình viên để sửa chữa, khắc phục các lỗ hổng bảo mật của hệ thống hay phần mềm.