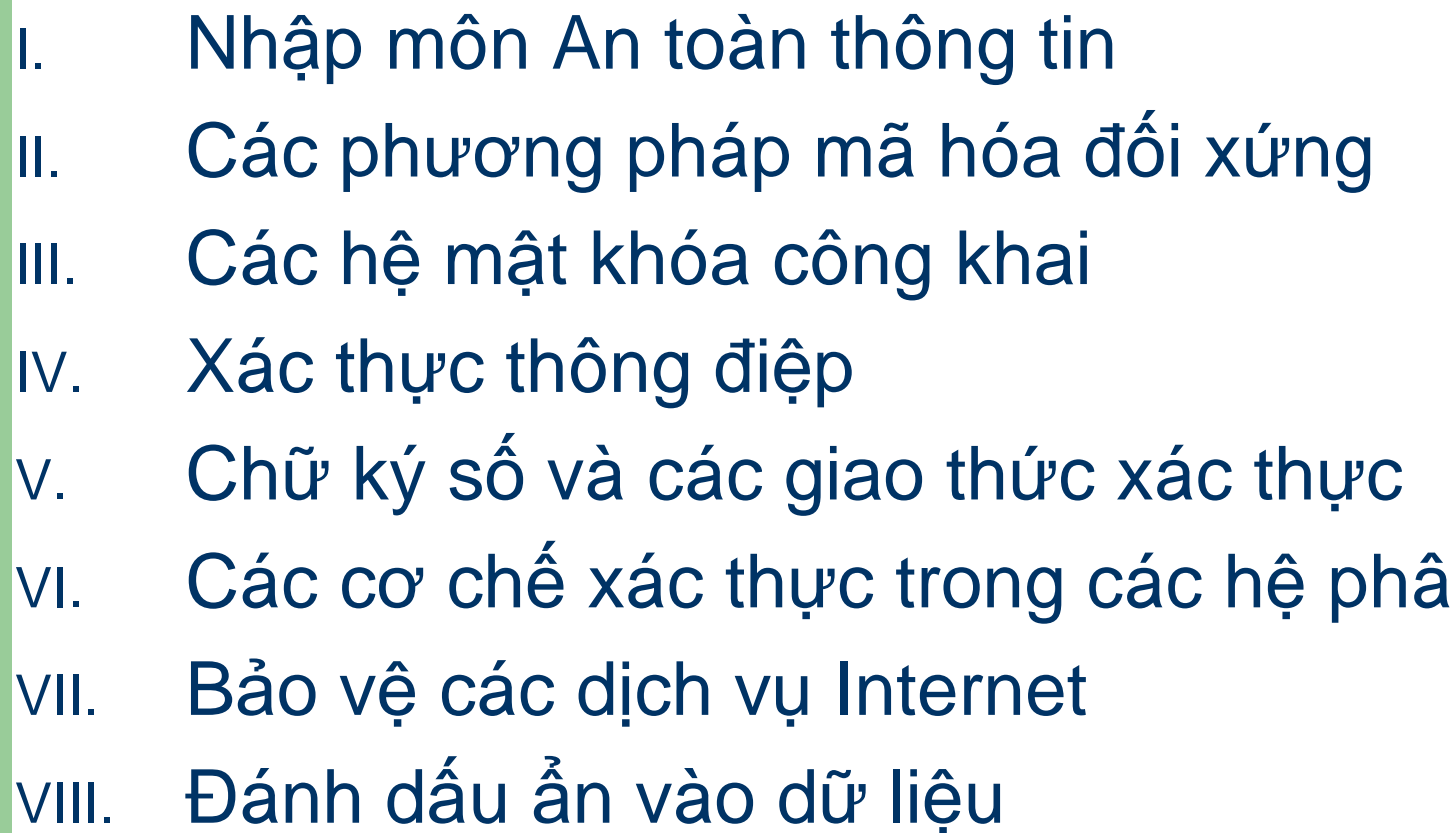


An toàn và An ninh Thông tin

Nguyễn Linh Giang.
Bộ môn Truyền thông
và Mạng máy tính.

- 
- I. Nhập môn An toàn thông tin
 - II. Các phương pháp mã hóa đối xứng
 - III. Các hệ mật khóa công khai
 - IV. Xác thực thông điệp
 - V. Chữ ký số và các giao thức xác thực
 - VI. Các cơ chế xác thực trong các hệ phân tán
 - VII. Bảo vệ các dịch vụ Internet
 - VIII. Đánh dấu ẩn vào dữ liệu

Tài liệu

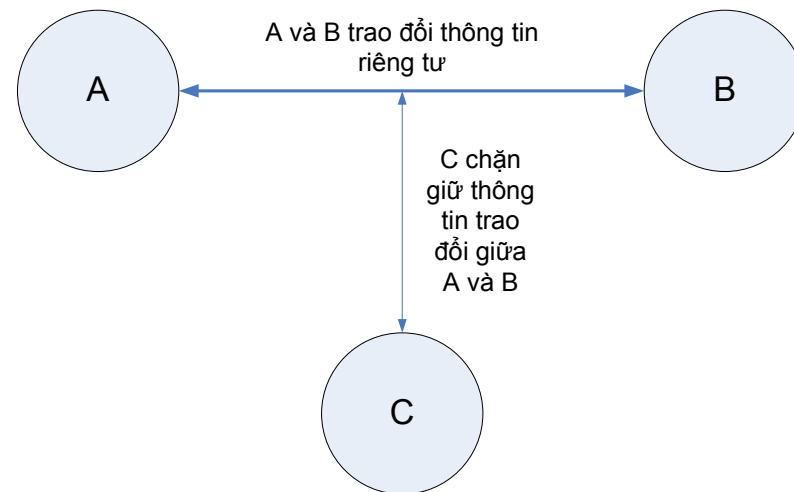
- W. Stallings – Network and Internetwork Security;
- Introduction to Cryptography – PGP
- D. Stinson – Cryptography: Theory and Practice

Chương I. Nhập môn

1. Nhập môn
2. Các dịch vụ, cơ chế an toàn an ninh thông tin và các dạng tấn công vào hệ thống mạng
3. Các dạng tấn công
4. Các dịch vụ an toàn an ninh
5. Các mô hình an toàn an ninh mạng

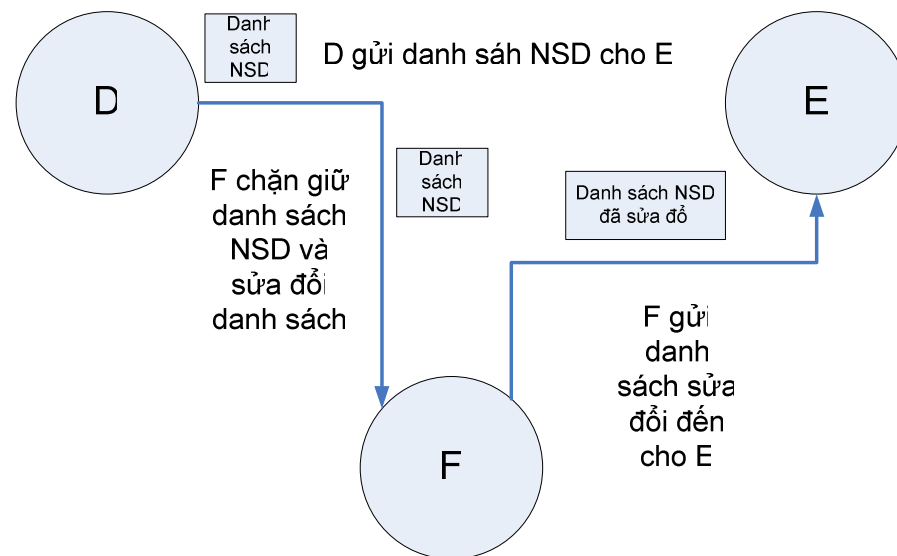
Nhập môn

- Một số ví dụ về vấn đề bảo vệ an toàn thông tin:
 - Truyền file



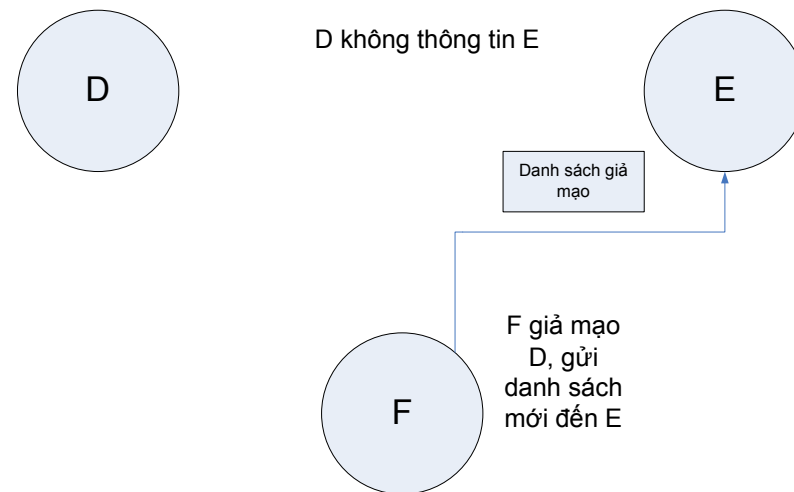
Nhập môn

- Trao đổi thông điệp:



Nhập môn

- Giả mạo:



Nhập môn

- Sự phức tạp trong bài toán Bảo mật liên mạng:
 - Không tồn tại phương pháp thích hợp cho mọi trường hợp.
 - Các cơ chế bảo mật luôn đi đôi với các biện pháp đối phó.
 - Lựa chọn những giải pháp thích hợp với từng ngữ cảnh sử dụng.

Dịch vụ và cơ chế an toàn an ninh

Các dạng tấn công

- Ba khía cạnh an toàn an ninh thông tin:
 - Tấn công vào an ninh thông tin
 - Các cơ chế an toàn an ninh
 - Các dịch vụ an toàn an ninh thông tin

Dịch vụ và cơ chế an toàn an ninh

Các dạng tấn công

- Phân loại các dịch vụ an toàn an ninh:
 - Bảo mật riêng tư (confidentiality)
 - Xác thực (authentication)
 - Toàn vẹn thông tin (integrity)
 - Chống phủ định (nonrepudiation)
 - Kiểm soát truy cập (access control)
 - Tính sẵn sàng (availability)

Dịch vụ và cơ chế an toàn an ninh

Các dạng tấn công

- Các cơ chế an toàn an ninh
 - Không tồn tại một cơ chế duy nhất;
 - Sử dụng **các kỹ thuật mật mã**.

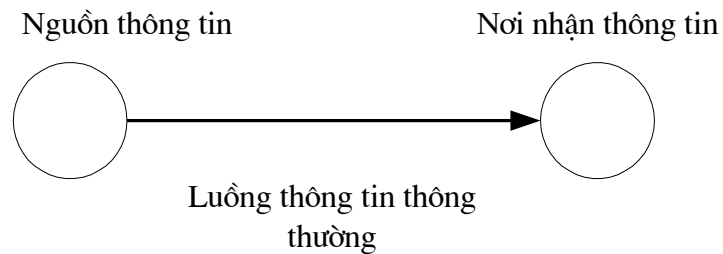
Dịch vụ và cơ chế an toàn an ninh

Các dạng tấn công

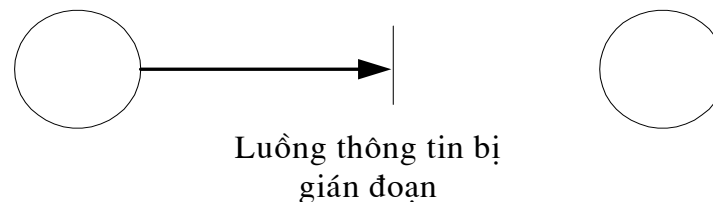
- Các dạng tấn công.
 - Truy nhập thông tin bất hợp pháp;
 - Sửa đổi thông tin bất hợp pháp;
 - v.v và v.v ...

Các dạng tấn công vào hệ thống

- Các dạng tấn công vào hệ thống máy tính và mạng:

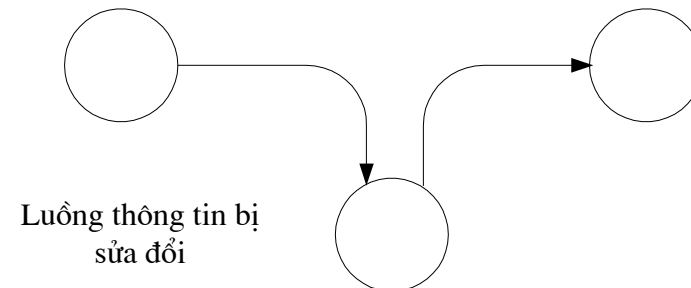
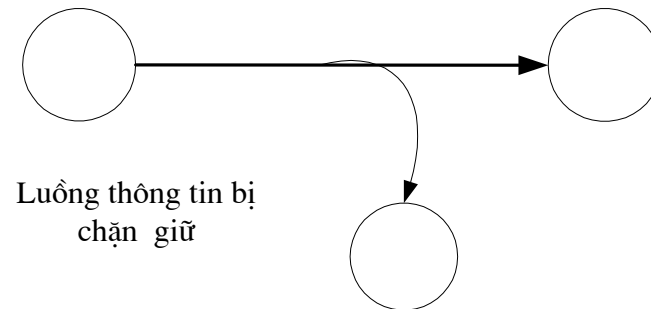


- Gián đoạn truyền tin (interruption):



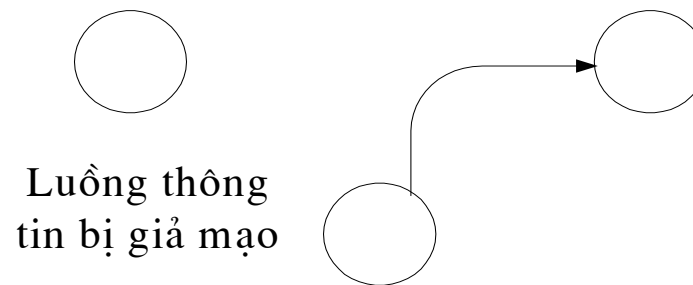
Các dạng tấn công vào hệ thống

- Chặn giữ thông tin (interception):
- Sửa đổi thông tin (modification):



Các dạng tấn công vào hệ thống

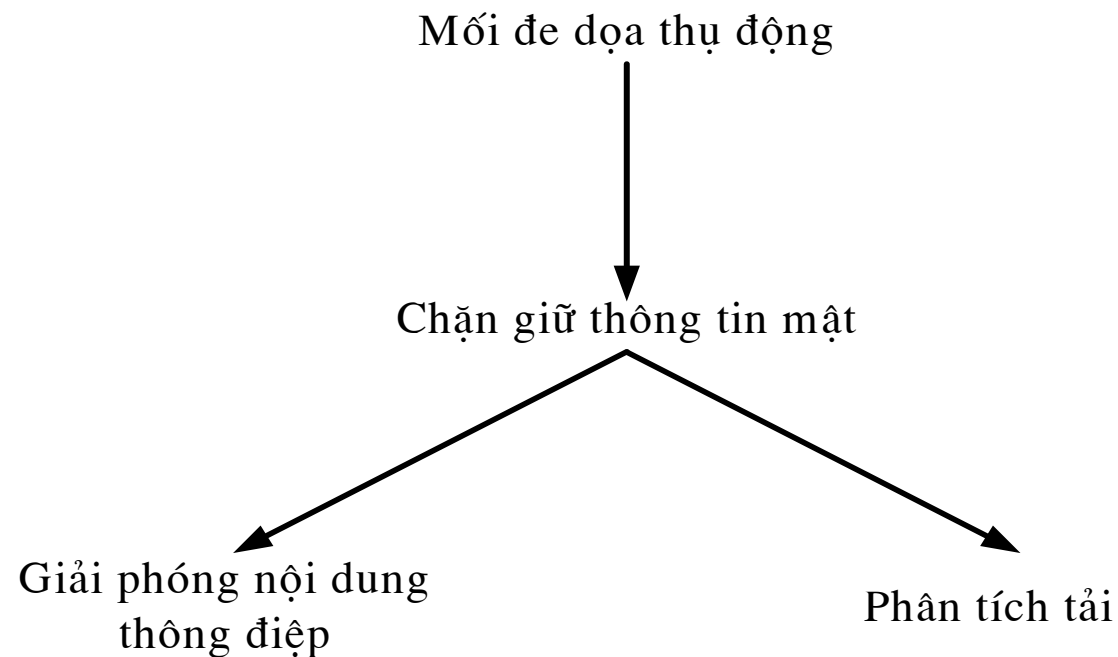
- Giả mạo thông tin (fabrication).



Các dạng tấn công vào hệ thống

Tấn công thụ động

- Tấn công thụ động



Các dạng tấn công vào hệ thống

Tấn công thụ động

- Các dạng tấn công thụ động:
 - Giải phóng nội dung thông điệp (release of message contents).
 - Ngăn chặn đối phương thu và tìm hiểu được nội dung của thông tin truyền tải.
 - Phân tích tải (traffic analysis).
 - Đối phương có thể xác định:
 - Vị trí của các máy tham gia vào quá trình truyền tin,
 - Tần suất và kích thước bản tin.

Các dạng tấn công vào hệ thống

Tấn công thụ động

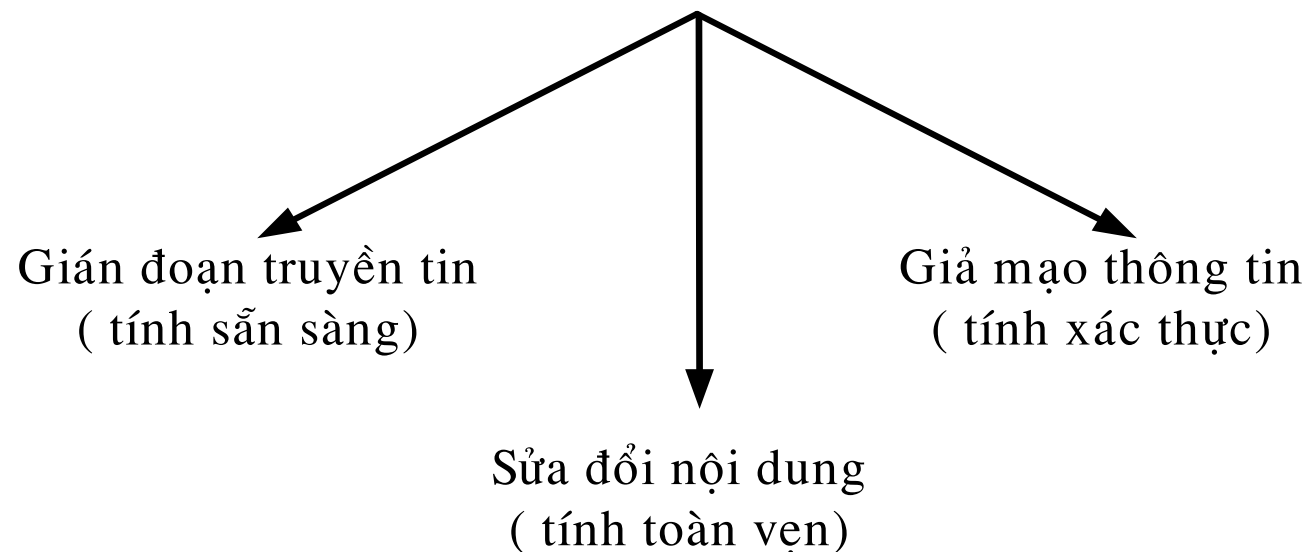
- Dạng tấn công thụ động rất khó bị phát hiện vì không làm thay đổi dữ liệu.
- Với dạng tấn công thụ động, nhấn mạnh vấn đề ngăn chặn hơn là vấn đề phát hiện.

Các dạng tấn công vào hệ thống

Tấn công chủ động

- Dạng tấn công chủ động.
 - Dạng tấn công chủ động bao gồm: sửa các dòng dữ liệu, đưa những dữ liệu giả, giả danh, phát lại, thay đổi thông điệp, phủ nhận dịch vụ.

Mối đe dọa chủ động



Các dạng tấn công vào hệ thống

Tấn công chủ động

- Giả danh (masquerade): khi đối phương giả mạo một đối tượng được uỷ quyền.
- Phát lại (replay): dạng tấn công khi đối phương chặn bắt các đơn vị dữ liệu và phát lại chúng tạo nên các hiệu ứng không được uỷ quyền;

Các dạng tấn công vào hệ thống

Tấn công chủ động

- Thay đổi thông điệp (modification of message): một phần của thông điệp hợp pháp bị sửa đổi, bị làm chậm lại hoặc bị sắp xếp lại và tạo ra những hiệu ứng không được uỷ quyền.
- Phủ nhận dịch vụ (denial of service): dạng tấn công đưa đến việc cấm hoặc ngăn chặn sử dụng các dịch vụ, các khả năng truyền thông.

Các dạng tấn công vào hệ thống

Tấn công chủ động

- Dạng tấn công chủ động rất khó có thể ngăn chặn tuyệt đối. Điều đó yêu cầu phải bảo vệ vật lý mọi đường truyền thông tại mọi thời điểm.
- Mục tiêu an toàn: phát hiện và phục hồi lại thông tin từ mọi trường hợp bị phá huỷ và làm trể.

Các dịch vụ an toàn an ninh

Đảm bảo tính riêng tư (Confidentiality)

- Đảm bảo tính riêng tư (Confidentiality).
 - Đảm bảo tính riêng tư của thông tin: Bảo vệ dữ liệu được truyền tải khỏi các tấn công thụ động.
 - Tương ứng với hình thức phát hiện nội dung thông điệp (release of message content) có một vài phương pháp bảo vệ đường truyền:
 - Bảo vệ mọi dữ liệu được truyền giữa hai người sử dụng tại mọi thời điểm:
 - Thiết lập đường truyền ảo giữa hai hệ thống và ngăn chặn mọi hình thức phát hiện nội dung thông điệp.
 - Ví dụ: VPN

Các dịch vụ an toàn an ninh

Đảm bảo tính riêng tư (Confidentiality)

- Bảo vệ các thông điệp đơn lẻ hoặc một số trường đơn lẻ của thông điệp.
 - Không thực sự hữu ích;
 - Trong nhiều trường hợp khá phức tạp;
 - Yêu cầu chi phí lớn khi thực hiện.
- Đảm bảo tính riêng tư: bảo vệ luồng thông tin trao đổi khỏi các thao tác phân tích
 - Yêu cầu: phía tấn công không thể phát hiện được các đặc điểm của quá trình truyền tin:
 - Nguồn và đích của thông tin;
 - Tần suất, độ dài;
 - Các thông số khác của luồng thông tin.

Các dịch vụ an toàn an ninh

Đảm bảo tính xác thực (Authentication)

- Đảm bảo tính xác thực (Authentication)
 - Dịch vụ đảm bảo tính xác thực:
 - Khẳng định các bên tham gia vào quá trình truyền tin được xác thực và đáng tin cậy.
 - Đối với các thông điệp đơn lẻ:
 - Các thông báo, báo hiệu: dịch vụ xác thực:
 - Đảm bảo cho bên nhận rằng các thông điệp được đưa ra từ những nguồn đáng tin cậy.

Các dịch vụ an toàn an ninh

Đảm bảo tính xác thực (Authentication)

- Đối với những liên kết trực tuyến, có hai khía cạnh cần phải chú ý tới:
 - Tại thời điểm khởi tạo kết nối, dịch vụ xác thực phải hai thực thể tham gia vào trao đổi thông tin phải được ủy quyền.
 - Dịch vụ cần khẳng định rằng kết nối không bị can thiệp bởi một bên thứ ba. Trong đó bên thứ ba này có thể giả mạo một trong hai bên được ủy quyền để có thể tham gia vào quá trình truyền tin và thu nhận các thông điệp.

Các dịch vụ an toàn an ninh

Đảm bảo tính sẵn sàng (Availability)

- Đảm bảo tính sẵn sàng (Availability).
 - Tấn công phá hủy tính sẵn sàng của hệ thống:
 - Thực hiện các thao tác vật lý tác động lên hệ thống.
 - Dịch vụ đảm bảo tính sẵn sàng phải:
 - Ngăn chặn các ảnh hưởng lên thông tin trong hệ thống;
 - Phục hồi khả năng phục vụ của các phần tử hệ thống trong thời gian nhanh nhất.

Các dịch vụ an toàn an ninh

Đảm bảo tính toàn vẹn(Integrity)

- Đảm bảo tính toàn vẹn (Integrity).
 - Đảm bảo tính toàn vẹn cũng có thể áp dụng cho luồng thông điệp, một thông điệp hoặc một số trường được lựa chọn của thông điệp.
 - Phương pháp hữu ích nhất là trực tiếp bảo vệ luồng thông điệp.
 - Đảm bảo tính toàn vẹn:
 - Dịch vụ bảo đảm tính toàn vẹn dữ liệu hướng liên kết;
 - Dịch vụ bảo đảm tính toàn vẹn hướng không liên kết.

Các dịch vụ an toàn an ninh

Đảm bảo tính toàn vẹn (Integrity)

- Dịch vụ bảo đảm tính toàn vẹn dữ liệu hướng liên kết:
 - Tác động lên luồng thông điệp và đảm bảo rằng thông điệp được nhận hoàn toàn giống khi được gửi, không bị sao chép, không bị sửa đổi, thêm bớt.
 - Các dữ liệu bị phá hủy cũng phải được khôi phục bằng dịch vụ này.
 - Dịch vụ bảo đảm tính toàn vẹn dữ liệu hướng liên kết xử lý các vấn đề liên quan tới sự sửa đổi của luồng các thông điệp và chối bỏ dịch vụ.

Các dịch vụ an toàn an ninh

Đảm bảo tính toàn vẹn (Integrity)

- Dịch vụ bảo đảm tính toàn vẹn hướng không liên kết:
 - Chỉ xử lý một thông điệp đơn lẻ. Không quan tâm tới những ngữ cảnh rộng hơn.
 - Chỉ tập trung vào ngăn chặn việc sửa đổi nội dung thông điệp.

Các dịch vụ an toàn an ninh

Dịch vụ chống phủ nhận (Nonrepudiation)

- Dịch vụ chống phủ nhận (nonrepudiation).
 - Dịch vụ chống phủ nhận ngăn chặn người nhận và người gửi từ chối thông điệp được truyền tải.
 - Khi thông điệp được gửi đi, người nhận có thể khẳng định được rằng thông điệp đích thực được gửi tới từ người được uỷ quyền.
 - Khi thông điệp được nhận, người gửi có thể khẳng định được rằng thông điệp đích thực tới đích.

Các dịch vụ an toàn an ninh

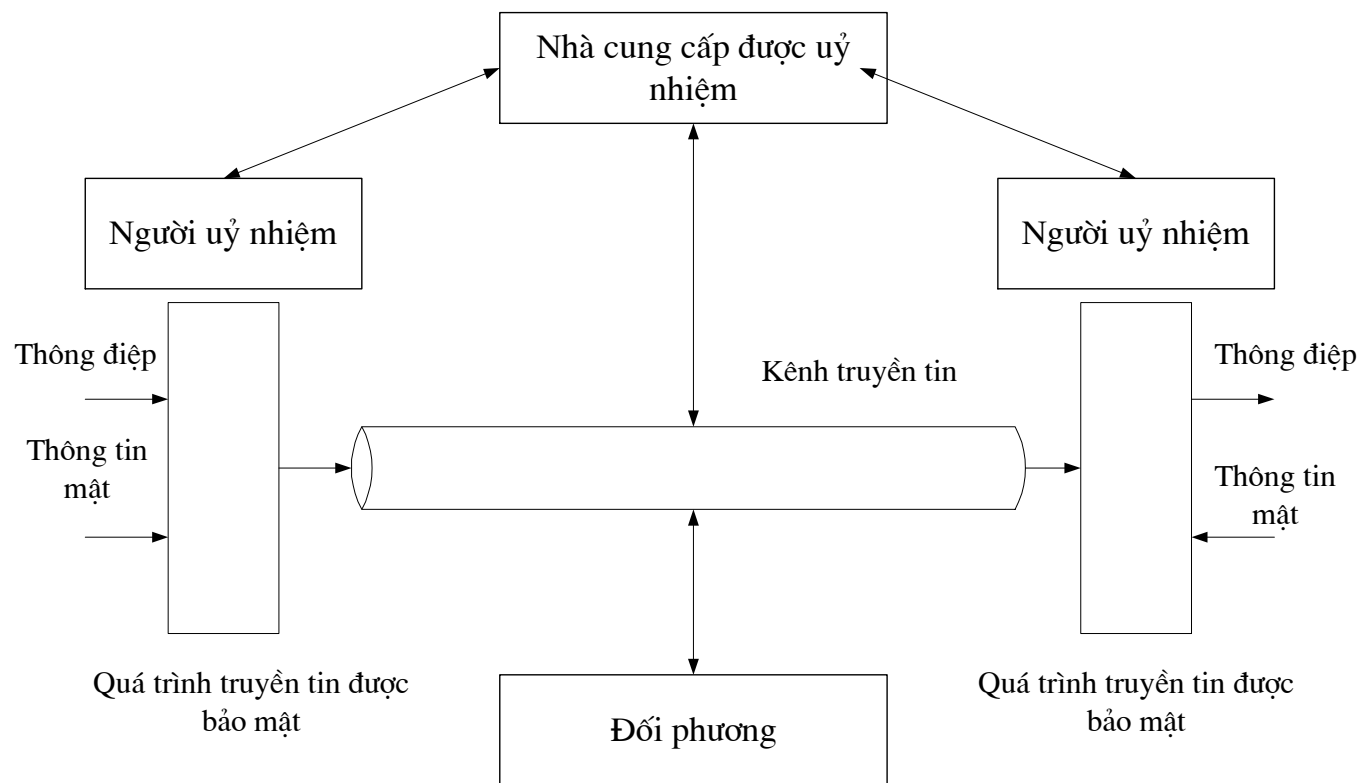
Dịch vụ kiểm soát truy cập

- Dịch vụ kiểm soát truy nhập.
 - Dịch vụ kiểm soát truy nhập cung cấp khả năng giới hạn và kiểm soát các truy nhập tới các máy chủ hoặc các ứng dụng thông qua đường truyền tin.
 - Để đạt được sự kiểm soát này, mỗi đối tượng khi truy nhập vào mạng phải được nhận biết hoặc được xác thực, sao cho quyền truy cập sẽ được gắn với từng cá nhân.

Các mô hình an toàn mạng và hệ thống

- Mô hình an toàn mạng
 - Bài toán an toàn an ninh thông tin mạng nảy sinh khi:
 - Cần thiết phải bảo vệ quá trình truyền tin khỏi các hành động truy cập trái phép;
 - Đảm bảo tính riêng tư và tính toàn vẹn;
 - Đảm bảo tính xác thực; ..vv.
 - Mô hình truyền thống của quá trình truyền tin an toàn

Các mô hình an toàn mạng và hệ thống



Các mô hình an toàn mạng và hệ thống

- Tất cả các kỹ thuật đảm bảo an toàn hệ thống truyền tin đều có hai thành phần:
 - Quá trình truyền tải có bảo mật thông tin được gửi.
 - Ví dụ: mật mã thông điệp sẽ làm cho kẻ tấn công không thể đọc được thông điệp.
 - Thêm vào thông điệp những thông tin được tổng hợp từ nội dung thông điệp. Các thông tin này có tác dụng xác định người gửi.
 - Một số thông tin mật sẽ được chia sẻ giữa hai bên truyền tin.
 - Các thông tin này được coi là bí mật với đối phương.
 - Ví dụ: khóa mật mã được dùng kết hợp với quá trình truyền để mã hóa thông điệp khi gửi và giải mã thông điệp khi nhận.

Các mô hình an toàn mạng và hệ thống

- Bên thứ ba được ủy quyền: trong nhiều trường hợp, cần thiết cho quá trình truyền tin mật:
 - Có trách nhiệm phân phối những thông tin mật giữa hai bên truyền tin;
 - Giữ cho các thông tin trao đổi với các bên được bí mật đối với người tấn công.
 - Có trách nhiệm phân xử giữa hai phía truyền tin về tính xác thực của thông điệp được truyền.

Các mô hình an toàn mạng và hệ thống

- Các thao tác cơ bản thiết kế một hệ thống an ninh:
 - Thiết kế các thuật toán để thực hiện quá trình truyền tin an toàn;
 - Các thuật toán này phải đảm bảo: tấn công không làm mất khả năng an toàn của chúng.
 - Tạo ra những thông tin mật sẽ được xử lý bằng thuật toán trên.

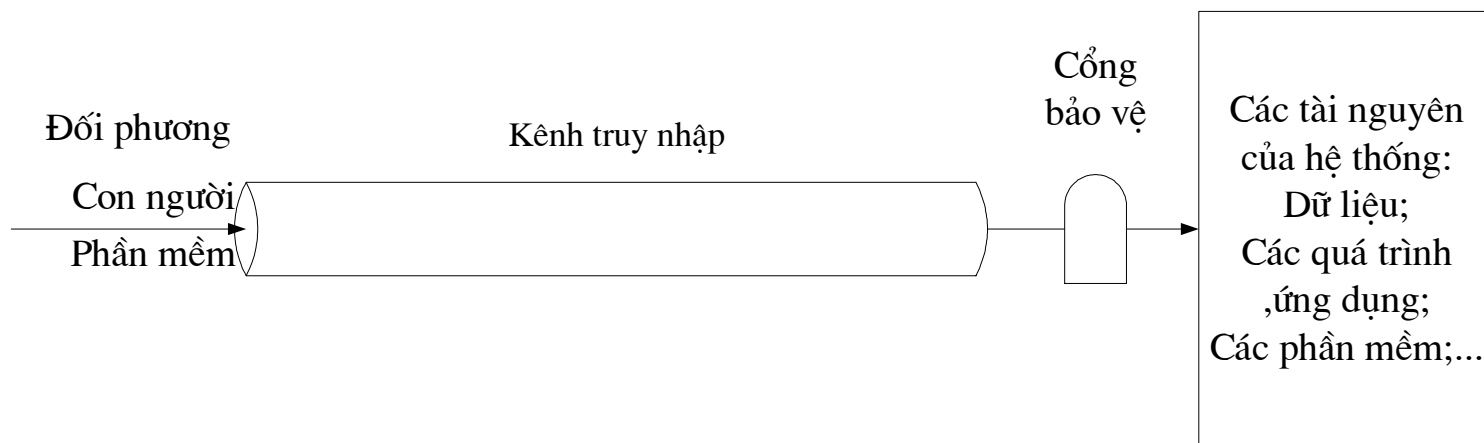
Các mô hình an toàn mạng và hệ thống

- Phát triển những phương pháp để phân phối và chia sẻ các thông tin mật.
- Đặt ra giao thức trao đổi:
 - Cho phép hai bên truyền tin trao đổi thông tin sử dụng những thuật toán an toàn;
 - Những thông tin mật đạt được độ an toàn thích hợp.

Các mô hình an toàn mạng và hệ thống

- Mô hình an toàn an ninh hệ thống
 - Truy nhập của các hacker;
 - Các lỗ hổng an ninh hệ thống;
 - Các tiến trình ngoại lai:
 - Các tiến trình truy cập tới thông tin: làm phá hủy, sửa đổi thông tin không được phép.
 - Các tiến trình dịch vụ: phát hiện các lỗi trong các dịch vụ của hệ thống để ngăn chặn việc sử dụng của những người không được ủy quyền.

Các mô hình an toàn mạng và hệ thống



Mô hình An ninh truy nhập hệ thống Mạng

An ninh hệ thống

- Các lỗ hổng bảo mật
- Quét lỗ hổng bảo mật

Lỗ hổng bảo mật

- **Khái niệm lỗ hổng bảo mật**
- **Phân loại lỗ hổng bảo mật**
 - Lỗ hổng từ chối dịch vụ
 - Lỗ hổng cho phép người dùng bên trong mạng với quyền hạn chế có thể tăng quyền mà không cần xác thực.
 - Lỗ hổng cho phép những người không được ủy quyền có thể xâm nhập từ xa không xác thực.

Khái niệm lỗ hổng

- Tất cả những đặc tính của phần mềm hoặc phần cứng cho phép người dùng không hợp lệ, có thể truy cập hay tăng quyền không cần xác thực.
- Tổng quát: lỗ hổng là những phương tiện đối phương có thể lợi dụng để xâm nhập vào hệ thống

Lỗi hỏng từ chối dịch vụ

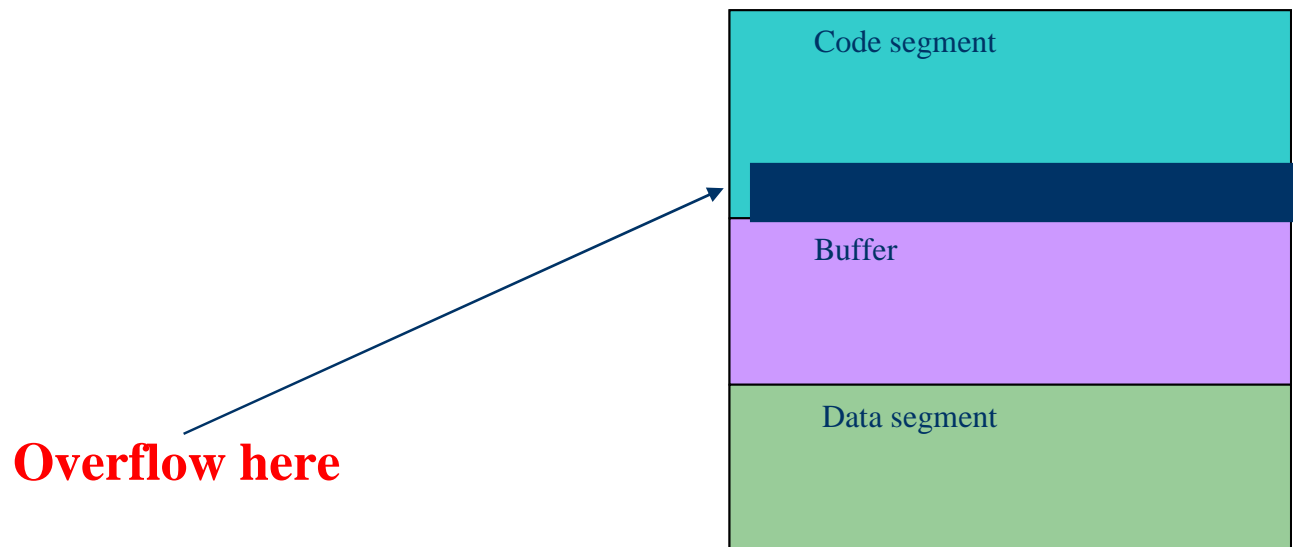
- Cho phép đối phương lợi dụng làm tê liệt dịch vụ của hệ thống.
- Đối phương có thể làm mất khả năng hoạt động của máy tính hay một mạng, ảnh hưởng tới toàn bộ tổ chức.
- Một số loại tấn công từ chối dịch vụ:
 - Bandwidth/Throughput Attacks
 - Protocol Attacks
 - Software Vulnerability Attacks

Lỗi hồng tăng quyền truy nhập không cần xác thực.

- Là lỗi ở những phần mềm hay hệ điều hành có sự phân cấp người dùng.
- Cho phép loại người dùng với quyền sử dụng hạn chế có thể tăng quyền trái phép.
- Ví dụ :
 - Sendmail : cho phép người dùng bình thường có thể khởi động tiến trình sendmail, lợi dụng sendmail khởi động chương trình khác với quyền root

Lỗi hỏng tăng quyền truy nhập không cần xác thực.

- Tràn bộ đệm :



Lỗ hổng cho phép xâm nhập từ xa không xác thực.

- Là lỗi chủ quan của người quản trị hệ thống hay người dùng.
- Do không thận trọng, thiếu kinh nghiệm, và không quan tâm đến vấn đề bảo mật.
- Một số những cấu hình thiếu kinh nghiệm :
 - Tài khoản có password rỗng
 - Tài khoản mặc định
 - Không có hệ thống bảo vệ như firewall, IDS, proxy
 - Chạy những dịch vụ không cần thiết mà không an toàn : SNMP, pcAnywhere, VNC , ...

Mục đích của quét lỗ hổng

- Phát hiện các lỗ hổng bảo mật của hệ thống
- Phát hiện các nghi vấn về bảo mật để ngăn chặn

Các phương pháp, kỹ thuật quét lỗ hổng bảo mật

- Quét mạng
- Quét điểm yếu
- Kiểm tra log
- Kiểm tra tính toàn vẹn file
- Phát hiện virus
- Chống tấn công quay số
- Chống tấn công vào access point

Quét mạng

- Kiểm tra sự tồn tại của hệ thống đích
- Quét cổng
- Dò hệ điều hành

Quét mạng

- Kiểm tra sự tồn tại của hệ thống đích
 - Quét ping để kiểm tra xem hệ thống có hoạt động hay không
 - Phát hiện bằng IDS hoặc một số trình tiện ích
 - Cấu hình hệ thống, hạn chế lưu lượng các gói ICMP để ngăn ngừa

Quét mạng

- Quét cổng
 - Nhằm nhận diện dịch vụ, ứng dụng
 - Sử dụng các kỹ thuật quét nổi TCP, TCP FIN..., xét số cổng để suy ra dịch vụ, ứng dụng
 - Phát hiện quét dựa vào IDS hoặc cơ chế bảo mật của máy chủ
 - Vô hiệu hóa các dịch vụ không cần thiết để dấu mình

Quét mạng

- Dò hệ điều hành
 - Dò dựa vào đặc trưng giao thức
 - Phát hiện bằng các phần mềm phát hiện quét cổng, phòng ngừa, sử dụng firewall, IDS.

Quét điểm yếu hệ thống

- Liệt kê thông tin
- Quét điểm yếu dịch vụ
- Kiểm tra an toàn mật khẩu

Quét điểm yếu

- Liệt kê thông tin
 - xâm nhập hệ thống, tạo các vấn đề trực tiếp
 - Nhằm thu thập các thông tin về
 - Dùng chung, tài nguyên mạng
 - Tài khoản người dùng và nhóm người dùng
 - Ứng dụng và banner
 - Ví dụ về liệt kê thông tin trong Windows
 - Ví dụ về liệt kê thông tin trong Unix/Linux

Quét điểm yếu

- Quét điểm yếu dịch vụ
 - Quét tài khoản yếu: Tìm ra acc với từ điển khi tài khoản yếu
 - Quét dịch vụ yếu: Dựa trên xác định nhà cung cấp và phiên bản
 - Biện pháp đối phó: Cấu hình dịch vụ hợp lý, nâng cấp, vá lỗi kịp thời.

Quét điểm yếu

- Bẻ khóa mật khẩu
 - Nhanh chóng tìm ra mật khẩu yếu
 - Cung cấp các thông tin cụ thể về độ an toàn của mật khẩu
 - Dễ thực hiện
 - Giá thành thấp

Kiểm soát log file

- Ghi lại xác định các thao tác trong hệ thống
- Dùng để xác định các sự sai lệch trong chính sách bảo mật
- Có thể bằng tay hoặc tự động
- Nên được thực hiện thường xuyên trên các thiết bị chính
- Cung cấp các thông tin có ý nghĩa cao
- Áp dụng cho tất cả các nguồn cho phép ghi lại hoạt động trên nó

Kiểm tra tính toàn vẹn file

- Các thông tin về thao tác file được lưu trữ trong cơ sở dữ liệu tham chiếu
- Một phần mềm đối chiếu file và dữ liệu trong cơ sở dữ liệu để phát hiện truy nhập trái phép
- Phương pháp tin cậy để phát hiện truy nhập trái phép
- Tự động hóa cao
- Giá thành hạ
- Không phát hiện khoảng thời gian
- Luôn phải cập nhật cơ sở dữ liệu tham chiếu

Quét Virus

- Mục đích: bảo vệ hệ thống khỏi bị lây nhiễm và phá hoại của virus
- Hai loại phần mềm chính:
 - Cài đặt trên server
 - Trên mail server hoặc trạm chính (proxy...)
 - Bảo vệ trên cửa ngõ vào
 - Cập nhật virus database thuận lợi
 - Cài đặt trên máy trạm
 - Đặc điểm: thường quét toàn bộ hệ thống (file, ổ đĩa, website người dùng truy nhập)
 - Đòi hỏi phải được quan tâm nhiều của người dùng
- Cả hai loại đều có thể được tự động hóa và có hiệu quả cao, giá thành hợp lí

War Dialing

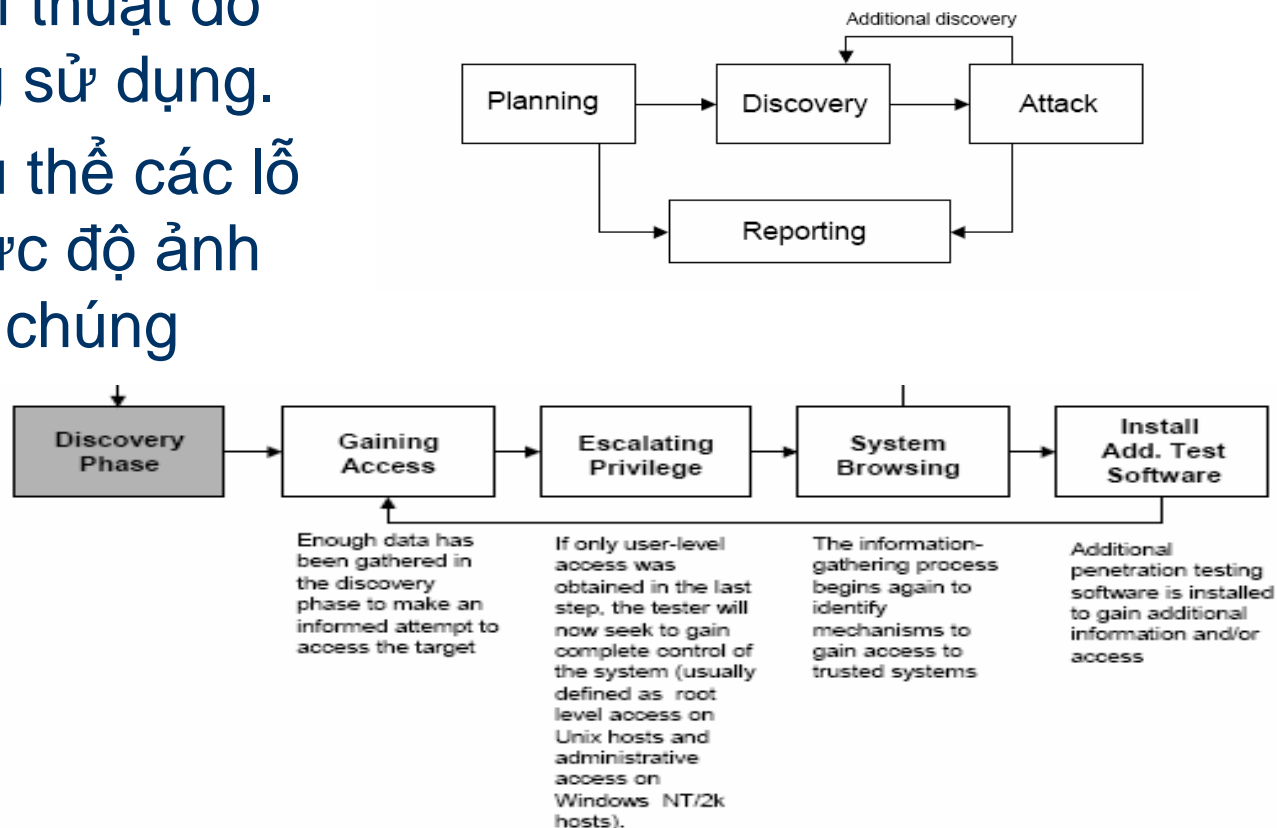
- Ngăn chặn những modem không xác thực quay số tới hệ thống
- Chương trình quay số có thể quay tự động để dò tìm cổng vào hệ thống
- Policy: hạn chế số điện thoại truy nhập cho từng thành viên
- Phương pháp này đòi hỏi nhiều thời gian

Quét LAN không dây

- Liên kết bằng tín hiệu không dùng dây dẫn -> thuận tiện cho kết nối đồng thời tạo ra nhiều lỗ hổng mới
- Hacker có thể tấn công vào mạng với máy tính xách tay có chuẩn không dây
- Chuẩn thường dùng 802.11b có nhiều hạn chế về bảo mật
- Chính sách bảo đảm an toàn:
 - Dựa trên các nền phần cứng và các chuẩn cụ thể
 - Việc cấu hình mạng phải chặt chẽ và bí mật
 - Gỡ bỏ các cổng vào không cần thiết

Kiểm thử các thâm nhập

- Dùng các kĩ thuật do đối phương sử dụng.
- Xác định cụ thể các lỗ hổng và mức độ ảnh hưởng của chúng
- Chu trình:



Kiểm thử thâm nhập (Cont)

- Các loại lỗ hổng có thể được phát hiện:
 - Thiếu sót của nhân hệ thống.
 - Tràn bộ đệm.
 - Các liên kết đường dẫn.
 - Tấn công bộ miêu tả file.
 - Quyền truy nhập file và thư mục
 - Trojan

So sánh các phương pháp

Kiểu quét	Điểm mạnh	Điểm yếu
Quét mạng	<ul style="list-style-type: none">• nhanh so với quét điểm yếu• hiệu quả cho quét toàn mạng• nhiều chương trình phần mềm miễn phí• tính tự động hóa cao• giá thành hạ	<ul style="list-style-type: none">• không chỉ ra được các điểm yếu cụ thể• thường được dùng mở đầu cho kiểm thử thâm nhập• đòi hỏi phải có ý kiến chuyên môn để đánh giá kết quả
Quét điểm yếu	<ul style="list-style-type: none">• có thể nhanh, tùy thuộc vào số điểm được quét• một số phần mềm miễn phí• tự động cao• chỉ ra được điểm yếu cụ thể• thường đưa ra được các gợi ý giải quyết điểm yếu• giá thành cao cho các phần mềm tốt cho tới free• dễ vận hành	<ul style="list-style-type: none">• tuy nhiên tỉ lệ thất bại cao• chiếm tỉa nguyên lớn tại điểm quét• không có tính ẩn cao (dễ bị phát hiện bởi người sử dụng, tường lửa, IDS)• có thể trở nên nguy hiểm trong tay những người kém hiểu biết• thường không phát hiện được các điểm yếu mới nhất• chỉ chỉ ra được các điểm yếu trên bề mặt của hệ thống

So sánh (Cont)

Kiểm thử thâm nhập

- Sử dụng các kỹ thuật thực tế mà các kẻ tấn công sử dụng
- Chỉ ra được các điểm yếu
- Tìm hiểu sâu hơn về điểm yếu, chúng có thể được sử dụng như thế nào để tấn công vào hệ thống
- Cho thấy rằng các điểm yếu không chỉ là trên lý thuyết
- Cung cấp bằng chứng cho vấn đề bảo mật

- Đòi hỏi nhiều người có khả năng chuyên môn cao
- Tốn rất nhiều công sức
- Chậm, các điểm kiểm thử có thể phải ngừng làm việc trong thời gian dài
- Không phải tất cả các host đều được thử nghiệm (do tốn thời gian)
- Nguy hiểm nếu được thực hiện bởi những người không có chuyên môn
- Các công cụ và kỹ thuật có thể là trái luật
- Giá thành đắt đỏ

Kết chương

- Các dịch vụ, cơ chế an toàn an ninh mạng
- Các dạng tấn công vào mạng
- Các mô hình an toàn an ninh mạng
- Hệ thống và các lỗ hổng bảo mật