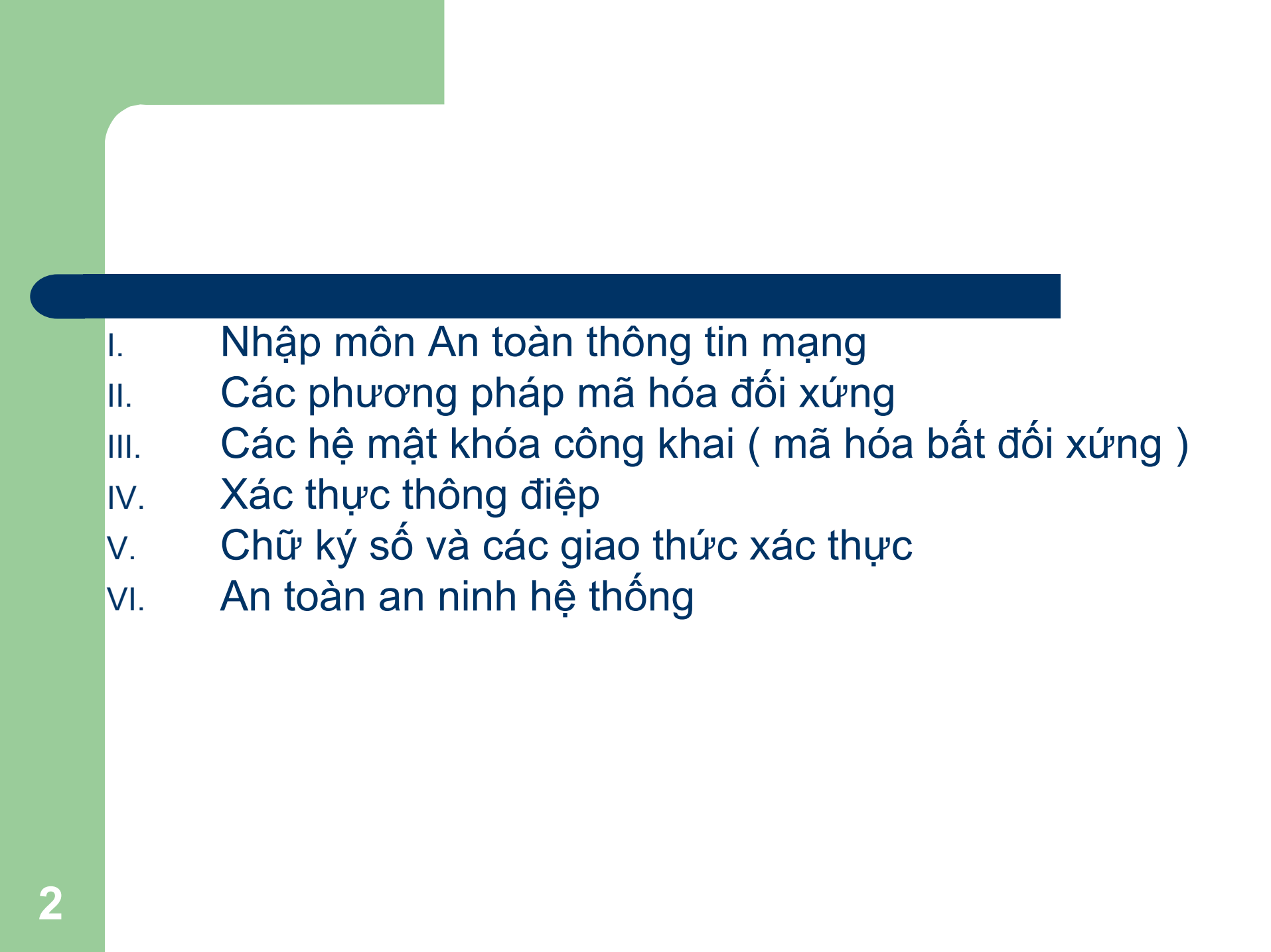


An toàn và An ninh thông tin

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

- 
- I. Nhập môn An toàn thông tin mạng
 - II. Các phương pháp mã hóa đối xứng
 - III. Các hệ mật khóa công khai (mã hóa bất đối xứng)
 - IV. Xác thực thông điệp
 - V. Chữ ký số và các giao thức xác thực
 - VI. An toàn an ninh hệ thống

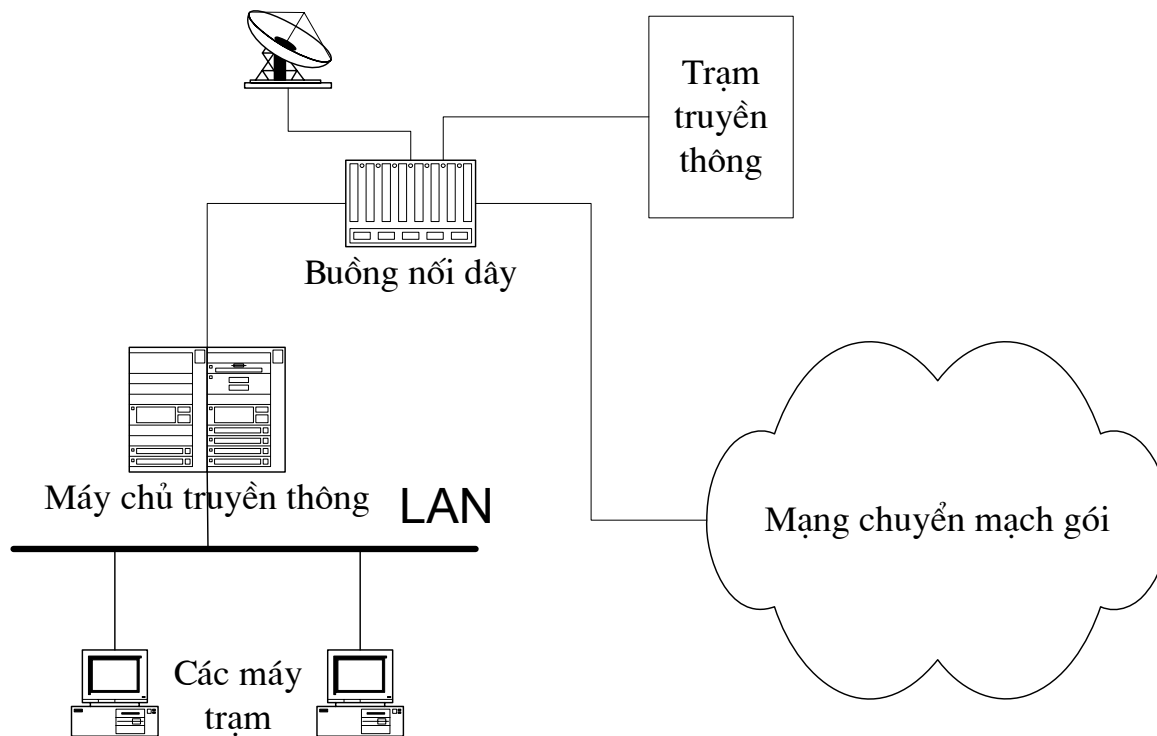
An ninh mạng và hệ thống

- An toàn mạng bằng các phương pháp mật mã
- An ninh hệ thống
 - Các lỗ hổng bảo mật
 - Quét lỗ hổng bảo mật

Đảm bảo tính riêng tư

- Các vị trí tiềm tàng đối với dạng tấn công riêng tư:
 - LAN:
 - Phần lớn các LAN là mạng quảng bá nên thông tin được truyền giữa hai máy có thể được các máy khác nhìn thấy.
 - Thông tin truyền tải theo frame chứa địa chỉ nguồn và đích. Đối phương có thể quan sát sự chuyển tải trong LAN và xác định mọi traffic cần thiết dựa trên địa chỉ nguồn và đích.
 - Nếu LAN cung cấp khả năng truy nhập theo đường dial-in, đối phương có thể truy cập vào mạng và theo dõi luồng truyền tải.
 - Từ LAN truy cập ra ngoài thường thông qua: router, modem, comm server. Từ các comm server thường có các đường kết nối tới các patch panel, ...

Đảm bảo tính riêng tư



Đảm bảo tính riêng tư

- Vị trí nối dây cũng là một điểm yếu.
 - Đối phương có thể móc nối vào mạng thông qua các vị trí nối dây. Dùng các sóng điện từ năng lượng thấp để truyền tải thông tin ra ngoài.
- Các tấn công vào mạng có thể tại mọi vị trí của đường truyền thông. Đối với dạng tấn công chủ động, kẻ tấn công phải kiểm soát vật lý đường truyền và có thể thêm, bắt giữ thông tin.

Đảm bảo tính riêng tư

1. Các cơ chế đảm bảo an toàn hệ thống:

- Cơ chế bảo mật đường liên kết (link encryption approaches).
 - Mỗi đường truyền thông có thể bị tấn công đều được kết nối với các thiết bị mã hóa tại hai đầu \Rightarrow mọi quá trình truyền tải trên đường đều được bảo mật.
 - Nhược điểm:
 - Yêu cầu nhiều thiết bị mã hóa – giải mã đối với mạng lớn.
 - Thông điệp phải được giải mã mỗi khi đi vào bộ chuyển mạch gói bởi vì bộ chuyển mạch cần phải đọc địa chỉ (virtual circuit number) trong phần đầu gói tin để định tuyến cho gói.
 - Như vậy thông điệp là một điểm yếu tại mỗi bộ chuyển mạch. Do đó nếu phải làm việc với mạng công cộng, người sử dụng không thể kiểm soát được an toàn thông tin tại nút mạng.

Đảm bảo tính riêng tư

- Một số biện pháp:
 - Mọi đường liên kết từ nguồn tin tới đích cần phải được đảm bảo mã mật.
 - Mỗi cặp nút chia sẻ một đường kết nối phải cùng chia sẻ một khóa mật duy nhất và mỗi đường liên kết khác nhau phải dùng những khóa mật khác nhau.
 - Như vậy phải dùng nhiều khóa và mỗi khóa chỉ được phân phối tới hai nút.

Đảm bảo tính riêng tư

- Cơ chế bảo mật đầu – cuối (end – to – end encryption approaches).
 - Quá trình mã hóa mật được thực hiện tại hai hệ thống đầu cuối. Máy trạm nguồn mã hóa thông tin và được truyền qua mạng tới trạm đích.
 - Trạm nguồn và trạm đích cùng chia sẻ khóa mật và do đó có thể giải mã thông điệp.
 - Dạng bảo mật này cho phép bảo đảm an toàn đối với các tấn công vào các điểm kết nối hoặc các điểm chuyển mạch.
 - Dạng bảo mật này cho phép người sử dụng yên tâm về mức độ an toàn của mạng và đường liên kết truyền thông.

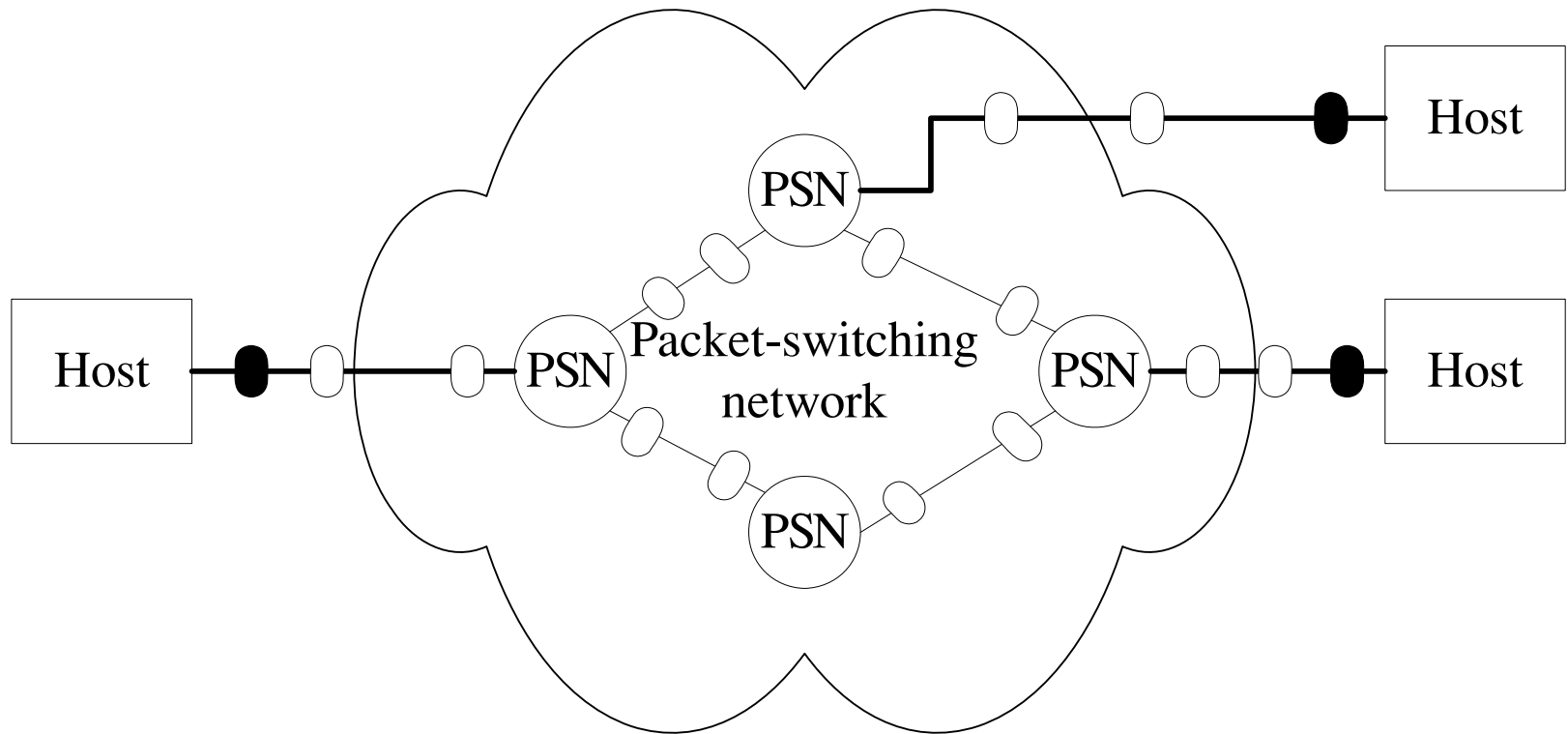
Đảm bảo tính riêng tư

- Các điểm yếu:
 - Ví dụ: máy trạm kết nối với mạng chuyển mạch gói X.25 và tạo mạch nối ảo tới máy trạm khác và truyền dữ liệu sử dụng sơ đồ mã hóa đầu – cuối.
 - Dữ liệu truyền bao gồm phần đầu và phần dữ liệu.
 - Nếu mã hóa toàn bộ gói tin theo sơ đồ mã hóa đối xứng, thông tin không thể truyền tới đích vì: chỉ có máy đích giải mã được gói tin \Rightarrow nút chuyển mạch không thể giải mã và đọc địa chỉ đích do đó không thể định tuyến gói tin.
 - Nếu chỉ mã hóa phần thân gói tin \Rightarrow đối phương sẽ biết phần đầu để phân tích tải.

Đảm bảo tính riêng tư

- Ưu điểm:
 - Phương pháp bảo mật đầu cuối cho phép thực hiện xác thực: hai trạm đầu cuối chia sẻ cùng một khóa mật, người nhận sẽ biết được thông điệp tới từ người gửi. Phương pháp bảo mật đường truyền không có cơ chế xác thực.
 - Khắc phục: sử dụng kết hợp cả hai phương pháp:

Đảm bảo tính riêng tư



Đảm bảo tính riêng tư

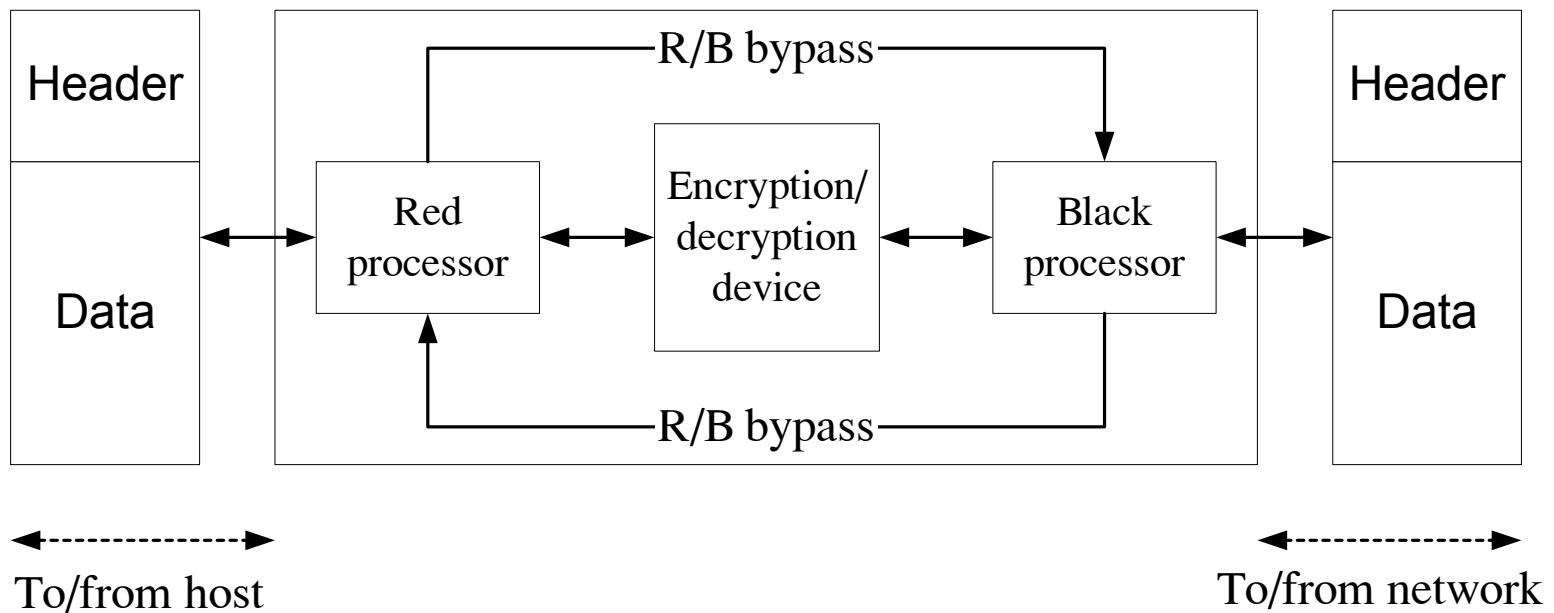
2. Điểm đặt các hàm mã hóa đầu cuối.

- Với mã hóa đường truyền, các hàm mã hóa được thực hiện tại mức thấp của phân cấp mạng truyền thông (tầng vật lý hoặc tầng liên kết).
- Đối với mã hóa đầu cuối:
 - Mức thấp nhất để đặt các hàm mã hóa là tầng mạng. Ví dụ: các phép mã hóa có thể được đặt tương ứng với X.25, do đó mọi khối dữ liệu của các khối X.25 đều được mã hóa.

Đảm bảo tính riêng tư

- Trên mức mã hóa tầng mạng, số lượng các đối tượng được định danh và bảo vệ riêng rẽ tương ứng với số lượng trạm đầu cuối. Mỗi trạm đầu cuối có thể trao đổi mã mật với trạm khác nếu chúng cùng chia sẻ một khóa mật.
- Như vậy có thể tách chức năng mã hóa và đưa vào một khối chức năng bộ xử lý ngoại vi.

Đảm bảo tính riêng tư



Đảm bảo tính riêng tư

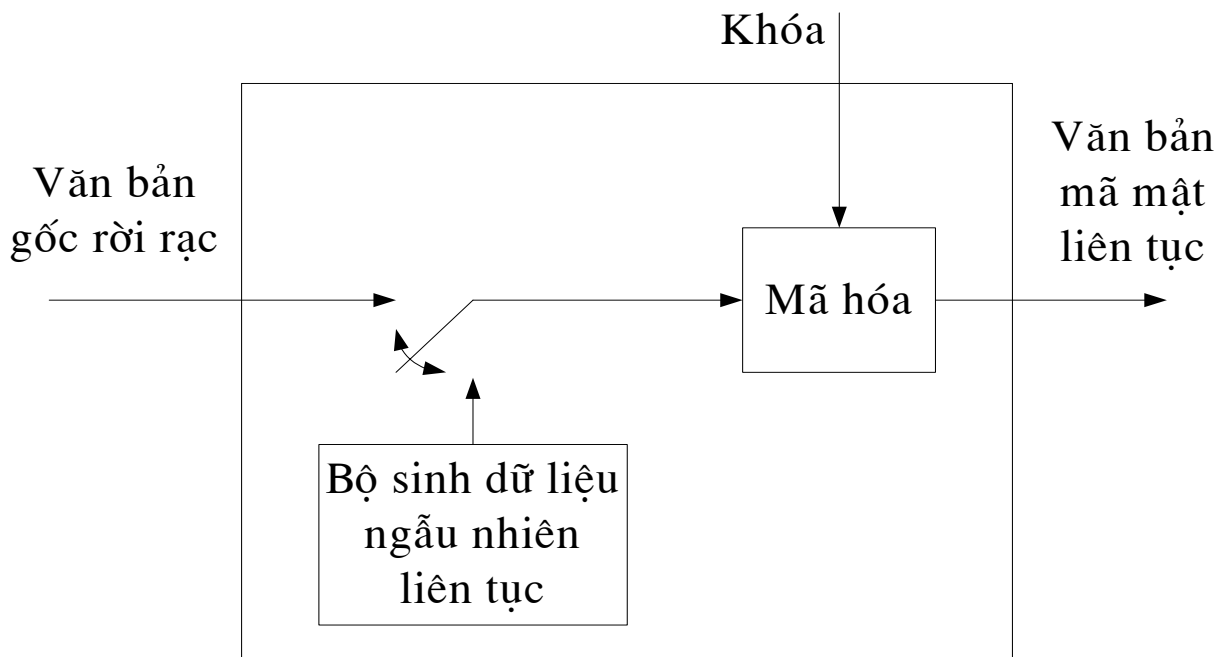
3. Đảm bảo tính riêng tư cho luồng truyền tải.
 - Các thông tin có thể được biết bằng phân tích luồng truyền tải:
 - Định danh của các bên tham gia vào quá trình truyền tin.
 - Tần suất truyền tải thông tin giữa hai bên tham gia.
 - Mẫu thông điệp, độ dài thông điệp, số lượng thông điệp dùng để truyền tải những thông tin quan trọng.
 - Các sự kiện liên quan tới các đối thoại đặc biệt giữa hai bên tham gia trao đổi thông tin.
 - Một vấn đề liên quan tới luồng truyền tải là: có thể sử dụng mẫu của luồng để tạo các kênh vụng trộm.

Đảm bảo tính riêng tư

- Phương pháp mã mật đường liên kết (link encryption approach).
 - Các phần đầu gói tin (packet header) được mã hóa, do đó làm giảm khả năng phân tích tải.
 - Đối phương vẫn có thể có khả năng đánh giá lưu lượng trên mạng và quan sát lưu lượng đi đến và đi khỏi hệ thống.
 - Để ngăn chặn khả năng phân tích luồng truyền tải, có thể sử dụng thủ tục đệm luồng truyền tải (traffic padding)

Đảm bảo tính riêng tư

- Thủ tục đệm luồng truyền tải:



Đảm bảo tính riêng tư

- Phương pháp bảo mật đầu cuối.
 - Nếu sử dụng phương pháp bảo mật đầu cuối, việc bảo vệ càng bị giới hạn.
 - Ví dụ,
 - Nếu mã hóa thực hiện trên tầng ứng dụng, đối phương có thể xác định được các đối tượng truyền tải tham gia vào quá trình đối thoại.
 - Nếu mã hóa được thực hiện trên tầng giao vận, khi đó các địa chỉ tầng mạng và các mẫu luồng truyền tải có thể bị lộ.

Đảm bảo tính riêng tư

- Kỹ thuật hữu ích: đệm các đơn vị dữ liệu có độ dài cố định trên tầng giao vận và cả trên tầng ứng dụng. Thêm vào đó, các thông điệp rỗng có thể được chèn một cách ngẫu nhiên vào luồng truyền tải. Chiến thuật này làm cho đối phương không thể biết được lượng dữ liệu được trao đổi giữa các trạm đầu cuối và che giấu được mẫu luồng truyền tải.

Lỗ hổng bảo mật

- **Khái niệm lỗ hổng**
- **Phân loại lỗ hổng**
 - Lỗ hổng làm cho 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 kẻ không phải là người dùng hệ thống có thể xâm nhập từ xa không xác thực.

Khái niệm lỗ hổng

- Tất cả những đặc tính của phần mềm hay phần cứng mà cho phép người dùng không hợp lệ, có thể truy cập hay tăng quyền truy nhập mà không cần xác thực.
- Tổng quát : lỗ hổng là tất cả mọi thứ mà kẻ tấn công có thể lợi dụng để xâm nhập vào hệ thống

Lỗi hỏng làm từ chối dịch vụ

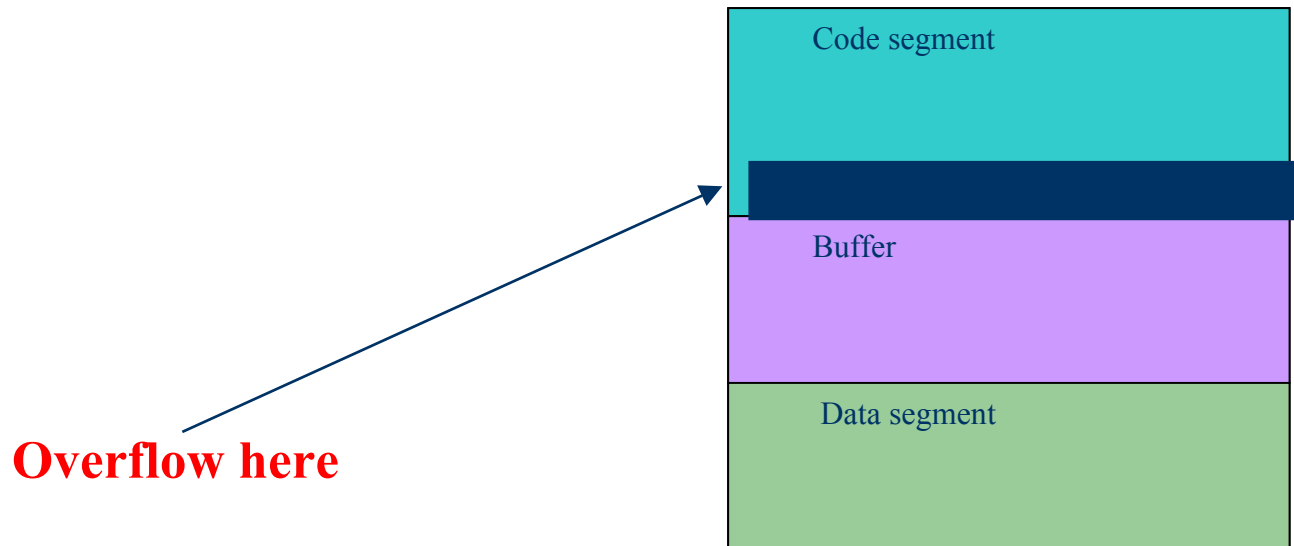
- Cho phép hacker lợi dụng làm tê liệt một số dịch vụ của hệ thống .
- Kẻ tấn công có thể làm mất khả năng hoạt động của máy tính hay một mạng, ảnh hưởng tới toàn bộ tổ chức hay công ty.
- Ba loại :
 - Bandwidth/Throughput Attacks
 - Protocol Attacks
 - Software Vulnerability Attacks

Lỗi hỏng 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 mức 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 , ...

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

- Phân loại :
 - Trojan / Backdoor
 - SQL injection
 - LOGIN : *' or 1 = 1; drop table users; --*
 - PASSWORD : *anything*
 - Query : *Select * from users where userName = '' or 1 =1; drop table users;-- userPass ='anything'*
 - Xâm nhập Web bất hợp pháp
 - Google : *allinurl:admentor*
 - One result :
<http://www.someserver.com/admentor/admin/admin.asp>
 - LOGIN : *' or ""='*
 - PASSWORD: *' or ""='*
 - Có thể xâm nhập vào trang web lỗi này với quyền admin

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 dấu vân tay giao thức
 - Phát hiện bằng các trình phát hiện quét cổng, phòng ngừa sử dụng firewall, IDS.

Quét điểm yếu

- 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 tin 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 lý

War Dialing

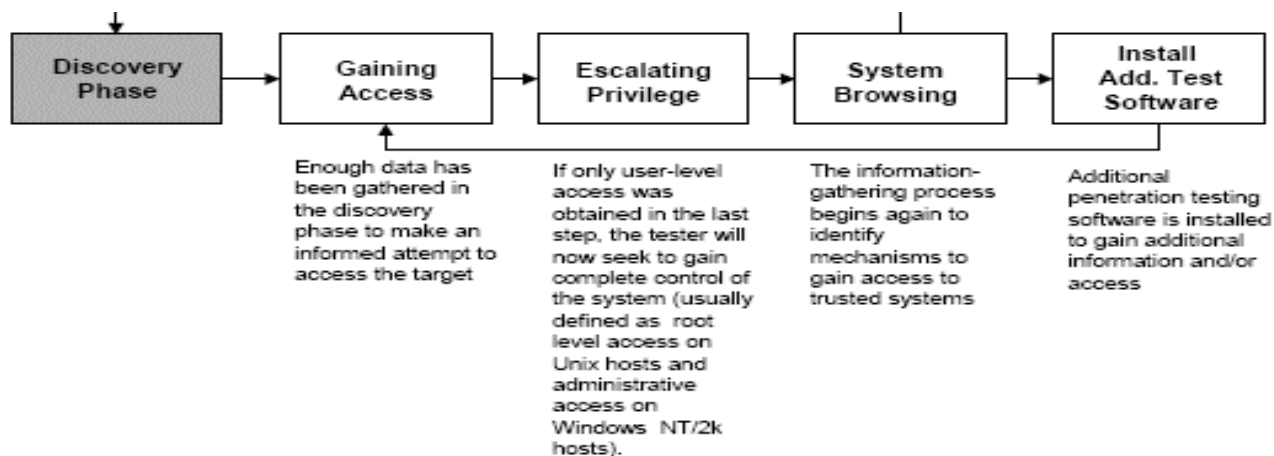
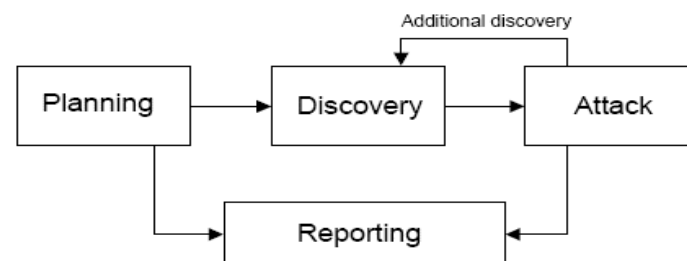
- Ngăn chặn những modem không xác thực quay số tới hệ thống
- Chương trình quay số có thể quay tự động để dò tìm cổng vào hệ thống
- Policy: hạn chế số điện thoại truy nhập cho từng thành viên
- Phương pháp này đòi hỏi nhiều thời gian

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 thực tế được sử dụng bởi những kẻ tấn công
- Xác định cụ thể các lỗ hổng và mức độ của chúng
- Chu trình:



Kiểm thử thâm nhập (Cont)

- Các loại lỗ hổng có thể được phát hiện:
 - Thiếu sót của nhân
 - 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

Directory Listings

- Các danh sách thư mục có thể cho rất nhiều thông tin
- Query : **intitle:index.of/admin**



intitle:index.of/admin

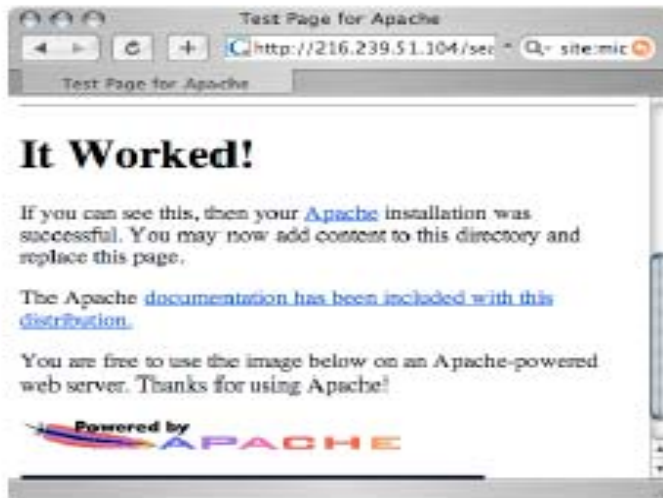
Directory Listings

- Các danh sách thư mục có thể cung cấp các thông tin version của server
- Query : **intitle:index.of apache server.at**



Default Server Pages

- Các web server với các trang mặc định có thể cung cấp khá nhiều thông tin cho hacker : version, OS
- Query : `intitle:test.page.for.apache` “it worked”
- Query : `allintitle:Netscape FastTrack Server Home Page`

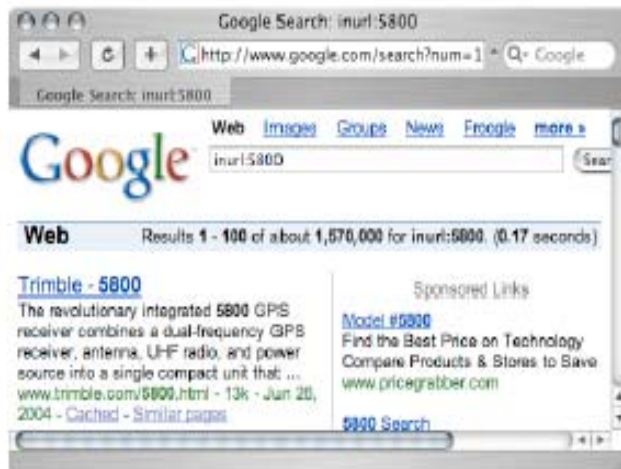


CGI Scanning

- Để xác định các điểm yếu web trên mạng với quy mô lớn nhiều hacker sử dụng các bộ quét CGI.
- Hầu hết các bộ quét có thể đọc file dữ liệu và truy vấn vào các web server để tìm các file dò rỉ.
- /iisadmpwd/
 - inurl;/iisadmpwd/
- /iisadmpwd/achg.htr
 - inurl;/iisadmpwd/achg.htr
- /iisadmpwd/aexp.htr
 - inurl;/iisadmpwd/aexp.htr
- /iisadmpwd/aexp2.htr
 - inurl;/iisadmpwd/aexp2.htr
- /iisadmpwd/aexp2b.htr
 - inurl;/iisadmpwd/aexp2b.htr

Port Scanning

- Các số cổng nhiều lúc xuất hiện trong url



inurl:5800



"VNC Desktop" inurl:5800

Others

- **Login Portals** : **inurl:admin/login.asp**
 - Microsoft Outlook Web Access
 - Coldfusion Admin Page
- **SQL Information**
 - **SQL dump**: “# Dumping data for table” username password
 - **SQL injection**