TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

AN NINH MẠNG

TS. Nguyễn Đức Toàn
Viện Công nghệ Thông tin và Truyền thông
School of Information and Communication Technology

Tổng quan về an ninh mạng

PHẦN 1: KHÁI NIỆM - CONCEPT

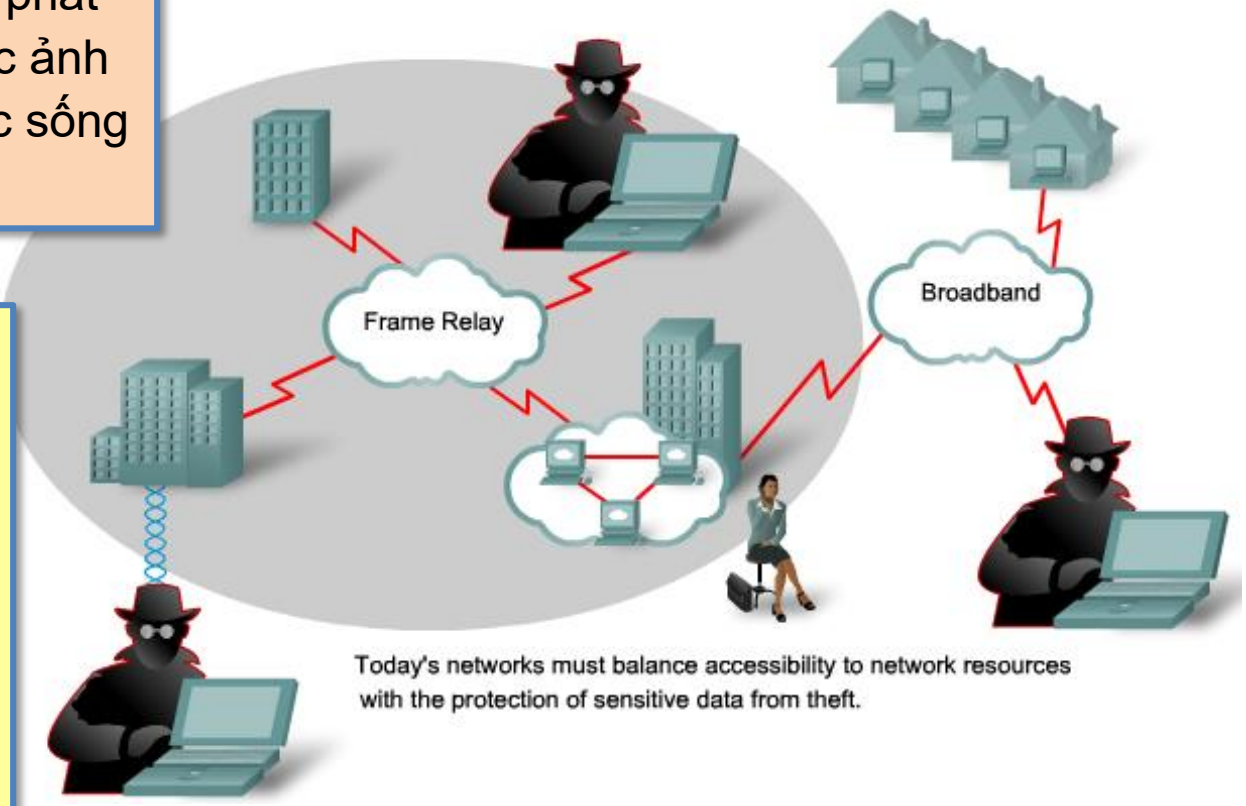
- **Tại sao an toàn mạng là cần thiết?**
- **Thế nào là an toàn hệ thống và an ninh mạng?**

KHÁI NIỆM VỀ AN TOÀN MẠNG

- **Tại sao an toàn mạng là cần thiết?**

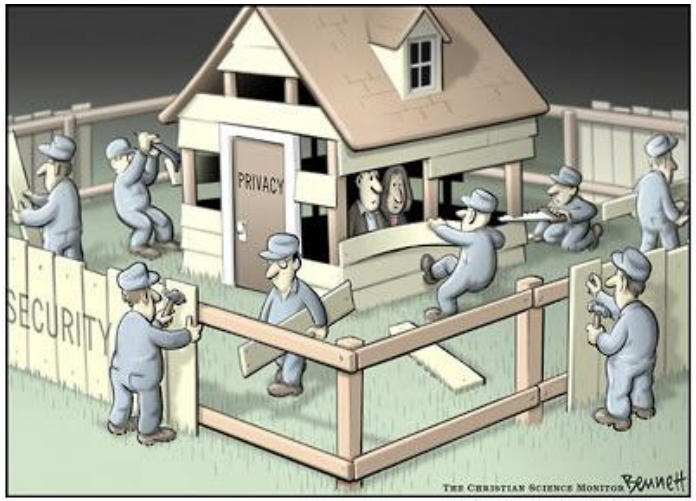
Mạng máy tính ngày càng phát triển cả về tầm vóc và mức ảnh hưởng của nó đối với cuộc sống hiện nay.

Nếu an ninh mạng không được quan tâm đúng mức, sẽ có nhiều vấn đề nghiêm trọng xảy ra như:
+ Xâm nhập bất hợp pháp
+ Đánh cắp dữ liệu
+ Tấn công lừa đảo
…



KHÁI NIỆM VỀ AN TOÀN MẠNG

- **Thế nào là an toàn mạng (network security)?**

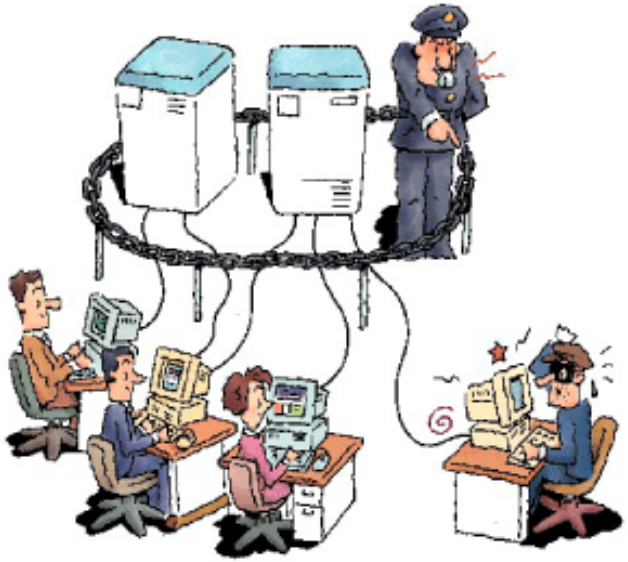


An toàn *(an ninh, bảo mật - security):* là một quá trình liên tục bảo vệ 1 đối tượng khỏi các tấn công.

An toàn thông tin *(information security):* là khả năng **bảo vệ** đối với **môi trường thông tin** kinh tế xã hội, đảm bảo cho việc **hình thành**, **sử dụng** và **phát triển** vì lợi ích của mọi công dân, mọi tổ chức và của quốc gia.

KHÁI NIỆM VỀ AN TOÀN MẠNG

- **Thế nào là an toàn mạng (network security)?**



An toàn máy tính *(computer security):* là an toàn cho tất cả các tài nguyên của hệ thống máy tính:

- Phần cứng vật lý: CPU, màn hình, bộ nhớ, máy in, CDROM, các thiết bị ngoại vi khác, …
- Phần mềm, dữ liệu, thông tin lưu trữ bên trong.

An toàn mạng *(network security):* là an toàn thông tin trong không gian của mạng máy tính.

KHÁI NIỆM VỀ AN TOÀN MẠNG

- **Mục tiêu cần đạt được của một hệ thống an toàn mạng:**

- **Sự bảo mật** (*confidentiality*): bảo đảm dữ liệu khỏi sự truy xuất hay theo dõi.
- **Tính toàn vẹn** (*integrity*): bảo đảm dữ liệu không bị thay đổi hay phá hoại.
- **Tính sẵn dùng** (*availability*): bảo đảm tính thông suốt của hệ thống và tài nguyên

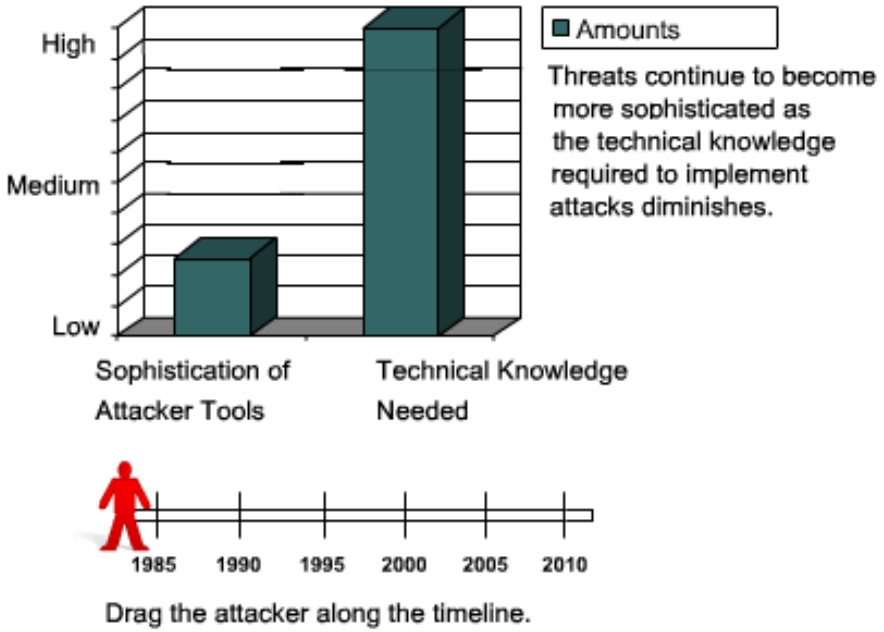
PHẦN 2: TẤN CÔNG TRÊN MẠNG

- Các mối đe dọa (threat) của một hệ thống máy tính.
- Phân loại những kẻ tấn công.
- Các hình thức tấn công: do thám, truy cập và từ chối dịch vụ.

TẤN CÔNG TRÊN MẠNG

- **Các mối đe dọa của hệ thống mạng máy tính**

Có nhiều tác nhân có thể là mối **đe dọa** (threat - còn gọi là **hiểm họa** hay **mối nguy hại**) cho một mạng máy tính.

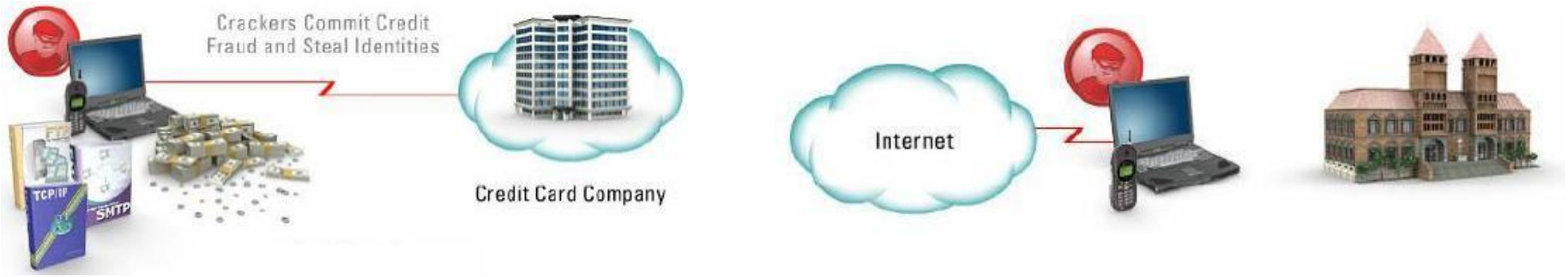


Có thể chia các mối đe dọa (threat) thành các dạng sau:

- Đe dọa có tổ chức và không tổ chức
- Đe dọa từ bên ngoài và từ bên trong
- Đe dọa chủ động và thụ động .
- Đe dọa cố ý và vô tình .

CÁC MỐI ĐE DỌA CHO HỆ THỐNG MẠNG

- **Đe dọa có tổ chức và không tổ chức**



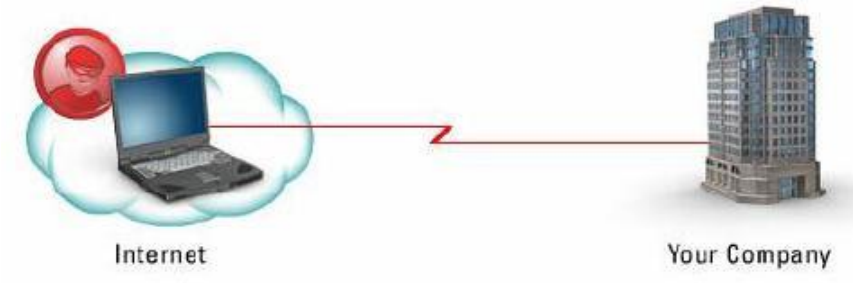
Đe dọa có tổ chức (structured threat) là de dọa được hoạch định trước vào 1 mục đích nhất định và lâu dài.
Các đe dọa này đến từ những hacker thành thạo và có động cơ rõ rệt.

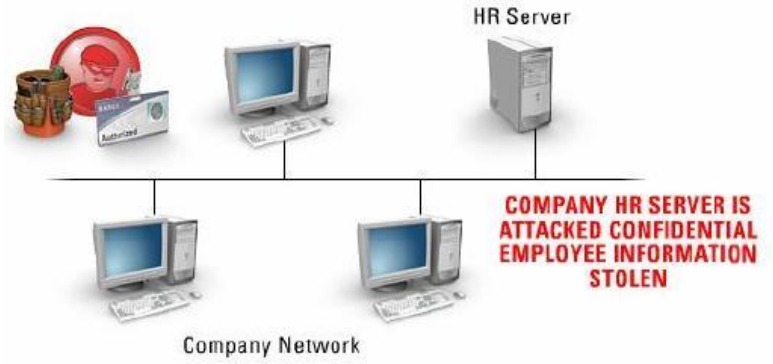
Đe dọa không tổ chức (unstructured threat) là đe dọa mang tính tức thời và là kết quả của những hacker đơn lẻ chưa có kinh nghiệm, thường chỉ dùng các công cụ có sẵn được công khai trên Internet để thử nghiệm.

Các đe dọa có tổ chức thường sẽ được che dấu rất khó phát hiện

CÁC MỐI ĐE DỌA CHO HỆ THỐNG MẠNG

- **Đe dọa từ bên ngoài và từ bên trong**





• Xuất phát từ các cá nhân hoặc tổ chức **bên ngoài hệ thống mạng**.
• Không có quyền truy xuất vào hệ thống máy tính và hệ thống mạng.
• Chỉ đột nhập vào từ Internet hay bằng đường Dial-up thông qua RAS.

• "70% các vấn đề có liên quan đến bảo mật thường đến từ bên trong mạng".
• Xảy ra từ một ai đó **có quyền truy xuất trong nội bộ mạng**.

Ngăn chặn các đe dọa từ bên trong cũng quan trọng như các đe dọa đến từ bên ngoài.

CÁC MỐI ĐE DỌA CHO HỆ THỐNG MẠNG

- **Đe dọa chủ động (active) - thụ động (passive) và đe dọa cố ý (intentional) - vô tình (unintentional)**

Đe dọa chủ động: có thể sửa đổi thông tin hoặc thay đổi tình trạng hoạt động của 1 hệ thống
VD: thay đổi bảng vạch đường của 1 Router.

Đe dọa thụ động: không có thay đổi dữ liệu của hệ thống.
VD: nghe trộm thông tin trên đường truyền.

Đe dọa cố ý: các tấn công tinh vi có sử dụng các kiến thức hệ thống đặc biệt.
VD: cố tình xâm nhập mạng trái phép.

Đe dọa vô tình: một sự kiện ngẫu nhiên có thể gây hại cho hệ thống.
VD: chế độ đặc quyền tự động được login.

TẤN CÔNG TRÊN MẠNG

- **Hacker**

• **Hacker** (intruder, attacker) là kẻ dùng kiến thức bản thân để thâm nhập, tấn công hệ thống máy tính hay mạng máy tính.
• Đa số hacker đều rất am tường về hoạt động của máy tính và mạng máy tính.

Hacker mũ trắng (white hat): xâm nhập có ý tốt. Chẳng hạn: nhà bảo mật, lập trình viên, chuyên viên mạng.

Hacker mũ đen (black hat): thâm nhập có mục đích xấu như: phá hoại, đánh cắp thông tin, ...

Hacker mũ xám (gray hat): đôi khi là hacker mũ trắng, đôi khi là mũ đen.

Hacker mũ xanh (blue hat): chuyên gia lập trình tài năng, được các công ty lớn mời về làm việc để chuyên tìm lỗi.

Cracker =“Criminal Hacker” (hacker tội phạm)

Về nguyên tắc nói chung mọi Hacker đều là xấu và hành động của họ là trái với pháp luật.

TẤN CÔNG TRÊN MẠNG

- **Khái niệm về tấn công**

Chúng ta có thể gọi tất cả **các dạng có hại** cho hệ thống máy tính là "tấn công".

Các tấn công có thể xuất phát từ:
- các công cụ được thiết kế sẵn.
- khai thác các điểm yếu của hệ thống.

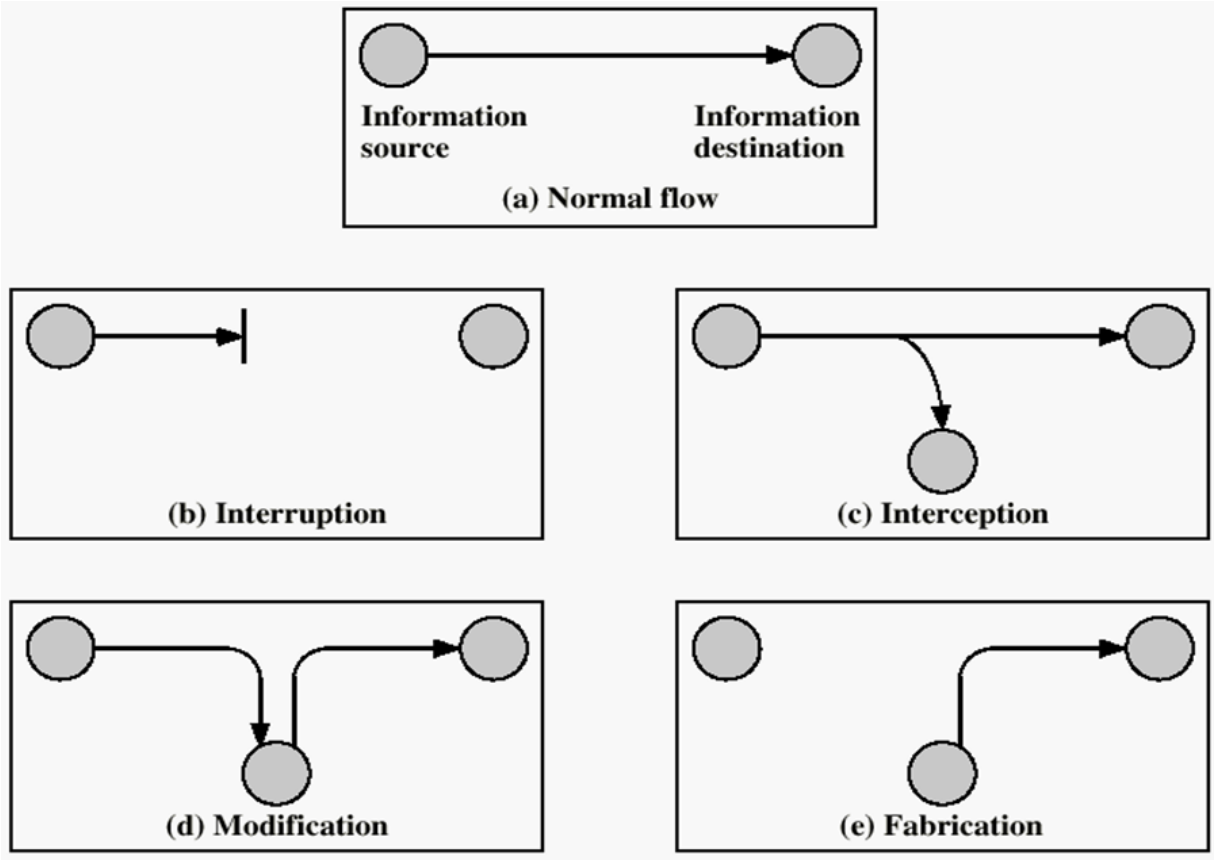
Tấn công có thể gây ra:
- hư hỏng dữ liệu hoặc ngưng trệ hoạt động hệ thống
- không làm hư hại cho dữ liệu và hệ thống (chẳng hạn ăn trộm thông tin) nhưng tác hại có thể lớn hơn.

Có thể phân chia tấn công ra làm 3 loại chính:
1. Do thám (reconnaissance)
2. Truy cập (access)
3. Từ chối dịch vụ (denial of service - DoS)

TẤN CÔNG TRÊN MẠNG

- **Khái niệm về tấn công**

Các hình thức tấn công trên mạng



TẤN CÔNG DO THÁM (RECONNAISSANCE)

- **Khái niệm**

Tấn công do thám là loại tấn công không phải với mục đích chiếm đoạt hệ thống mà chỉ tìm kiếm thông tin để có thể khai thác sau này

Các thông tin cần ghi nhận:
- Địa chỉ IP
- Các dịch vụ mạng đang sử dụng
- Cổng của các ứng dụng nào đang mở
- Hệ điều hành đang sử dụng
- Phiên bản Web server nào đang sử dụng
- …

Các kỹ thuật do thám thông dụng:
1. Nghe lén
2. Quét địa chỉ IP
3. Quét cổng
4. Quét tránh né
5. Xác định hệ điều hành

TẤN CÔNG TRUY CẬP (ACCESS ATTACK)

- **Khái niệm**

Tấn công truy cập là loại tấn công chiếm lấy tài nguyên trên hệ thống đích như file, mật khẩu, quyền điều khiển, …

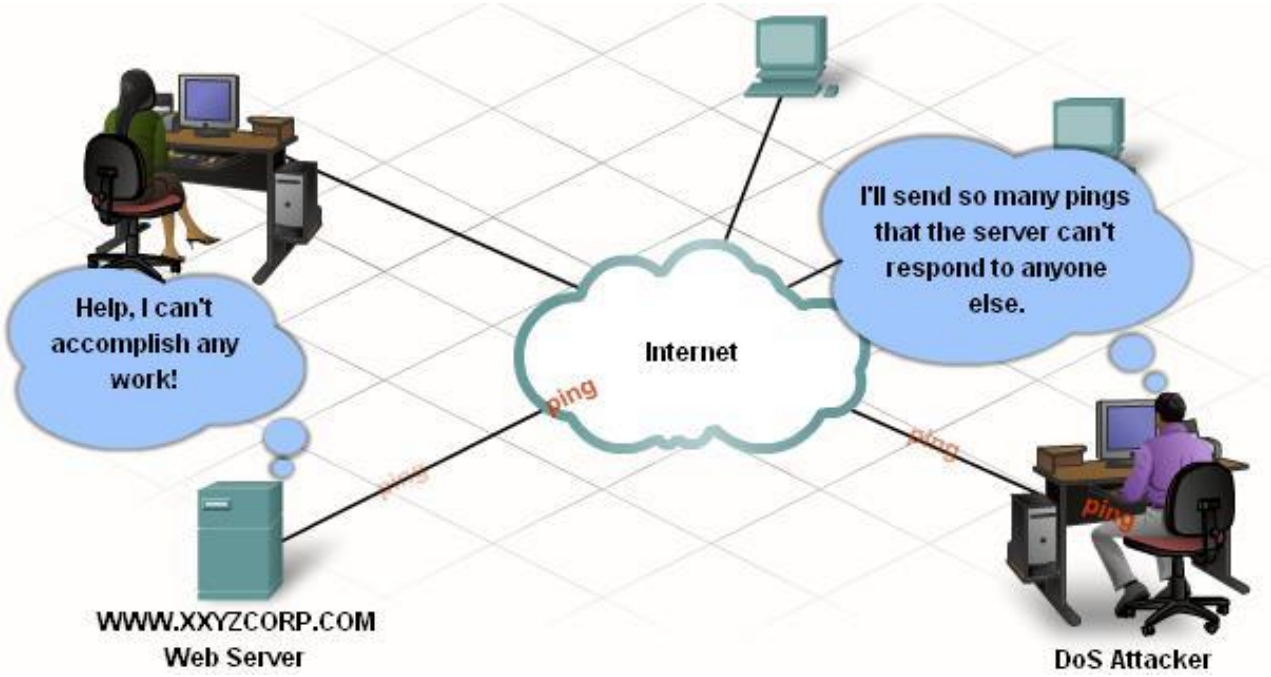
Sau khi tấn công thăm dò để nắm được các thông tin cơ bản về hệ thống đích, hacker sẽ tấn công trực tiếp vào hệ thống gọi là **tấn công truy cập**

Các kỹ thuật tấn công truy cập thông dụng:

1. Nghe lén
2. Sử dụng lại
3. Cướp giao dịch
4. Kẻ đứng giữa
5. Cổng sau
6. Đánh lừa
7. Khai thác lỗi
8. Tấn công mật khẩu

TẤN CÔNG TỪ CHỐI DỊCH VỤ (DOS)

- **Khái niệm**



Là tấn công phá hoại chứ không phải muốn lấy được thông tin.

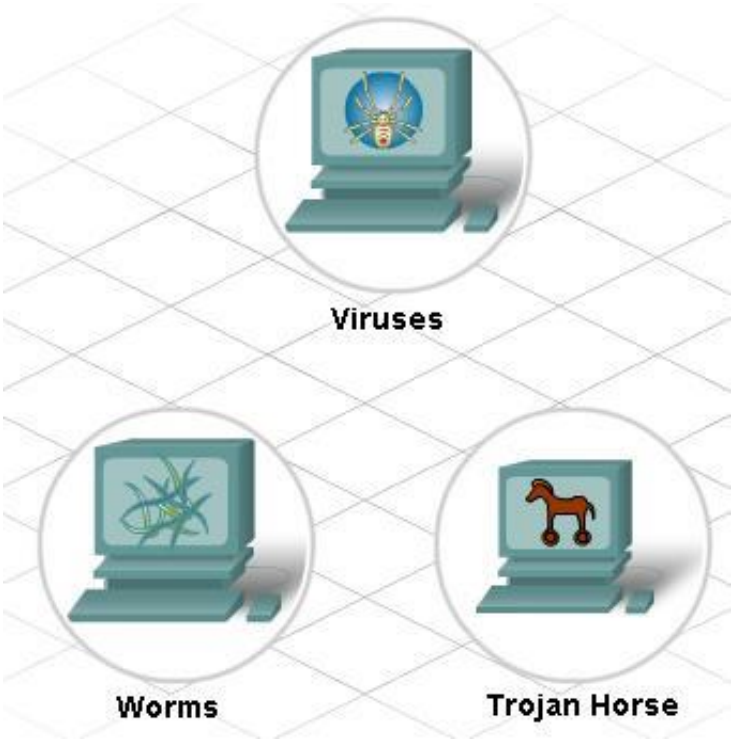
Tấn công bằng từ chối dịch vụ DoS có thể mô tả như hành động **ngăn cản những người dùng hợp pháp khả năng truy cập và sử dụng vào một dịch vụ** nào đó. Nó bao gồm làm **tràn ngập mạng**, **mất kết nối với dịch vụ**… mà mục đích cuối cùng là Server **không thể đáp ứng được các yêu cầu sử dụng dịch vụ** từ các Client.

PHẦN 3: CÁC PHẦN MỀM CÓ HẠI

- **Tấn công bằng mã độc hại là gì?**
- **Phân loại các phần mềm có hại**

CÁC PHẦN MỀM CÓ HẠI

- **Khái niệm**



Các dạng tấn công khai thác điểm yếu của hệ thống máy tính bằng cách cài những phần mềm từ bên ngoài vào gọi chung là các đoạn mã độc hại hay phần mềm có hại (Malware).

Các loại mã độc hại:
- Virus
- Sâu (Worm)
- Ngựa thành Troa (Trojan Horse)
- Phần mềm quảng cáo (Adware)
- Phần mềm gián điệp (Spyware)
- Keylogger
- Rootkit
- Cookie

CÁC PHẦN MỀM CÓ HẠI

- **Virus máy tính**

Virus là một loại chương trình máy tính:
- có thể tự mình nhân bản
- đa số gây hại cho phần cứng, phần mềm

Một số loại virus nổi tiếng:
- Jerusalem, Chernobyl (CIH)
- Michelangelo, Explorer.zip
- ILoveYou
- Anna Kournikova
- Sircam
- Benjamin

Phân loại virus:
- **Boot virus**: có từ lâu đời, lưu trong BootSector , lây qua đĩa mềm. Hiện nay không còn nữa.
- **File virus**: lây trong các file thực thi (.exe, .com, .bat, .sys, .pif). Rất nguy hiểm vì có khả năng phá hoại phần mềm, hệ điều hành và cả phần cứng (Bios).
- **Macro**: lây trong các file Office có hỗ trợ macro.
- **Lây qua Email**: dưới dạng các tập tin gửi kèm theo email, là các file thực thi được (.exe, .js, Script). Thường lây lan qua danh sách lưu trong Address Book.
- **Lây qua Internet**: ẩn trong các chương trình lậu (được bẻ khóa), freeware hoặc shareware.

CÁC PHẦN MỀM CÓ HẠI

- **Sâu máy tính (Worm)**

Sâu máy tính là tên gọi của 1 dạng virus đặc biệt, đa số **lan truyền qua hệ thống mạng**:
- Hệ thống thư điện tử, chatroom
- Mạng ngang hàng, chương trình P2P
- Qua Internet thông qua các lỗ hổng của Windows (hoặc các ứng dụng mạng nổi tiếng).

- Worm khác với virus ở chỗ nó **có đặc tính phá hoại mạng** do làm **tăng lưu thông** trên mạng, **chiếm băng thông** của mạng và **chiếm tài nguyên của Server** và các máy tính trên mạng.
- Worm nếu dùng chung với DDoS sẽ gây ra tác hại rất lớn.

Một số worm nổi tiếng nhất là: Mellisa (1999), Love Letter (2000), Nimda, Code Red (2001), SQL Slammer, Blaster (2003), Sasser (2004), Zotob (2005).

CÁC PHẦN MỀM CÓ HẠI

- **Ngựa thành Troa (Trojan Horse)**

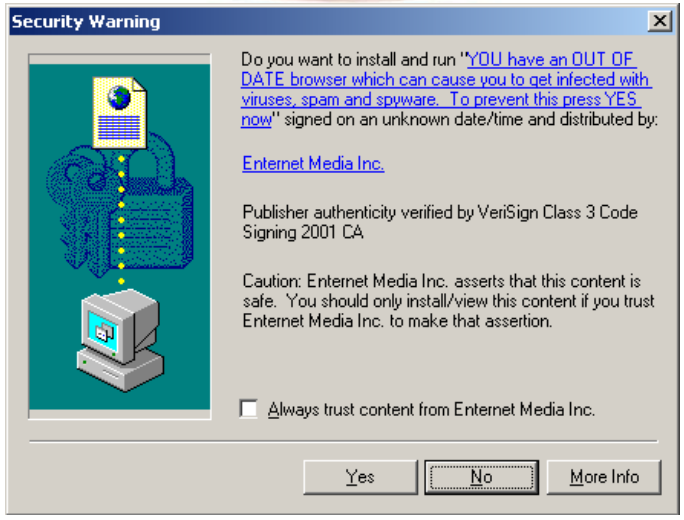
• Tác giả viết ra Trojan lừa cho đối phương sử dụng chương trình của mình. Khi đó, 1 phần của Trojan sẽ bí mật cài đặt ngầm lên máy của nạn nhân.
• Đến một thời điểm định trước, chương trình này có thể sẽ ngầm gửi những thứ thông tin bí mật của nạn nhân cho chủ nhân của nó ở trên mạng.

• Trojan là một đoạn mã chương trình hoàn toàn **không có tính chất lây lan**.
• Trojan chỉ lừa nạn nhân tự mình sử dụng nó.
• Trojan thường có trong các file crack và keygen trên mạng.
• Trojan rất nguy hiểm vì có thể phá hoại hay lấy cắp thông tin bí mật.

CÁC PHẦN MỀM CÓ HẠI

- **Phần mềm gián điệp và phần mềm quảng cáo**

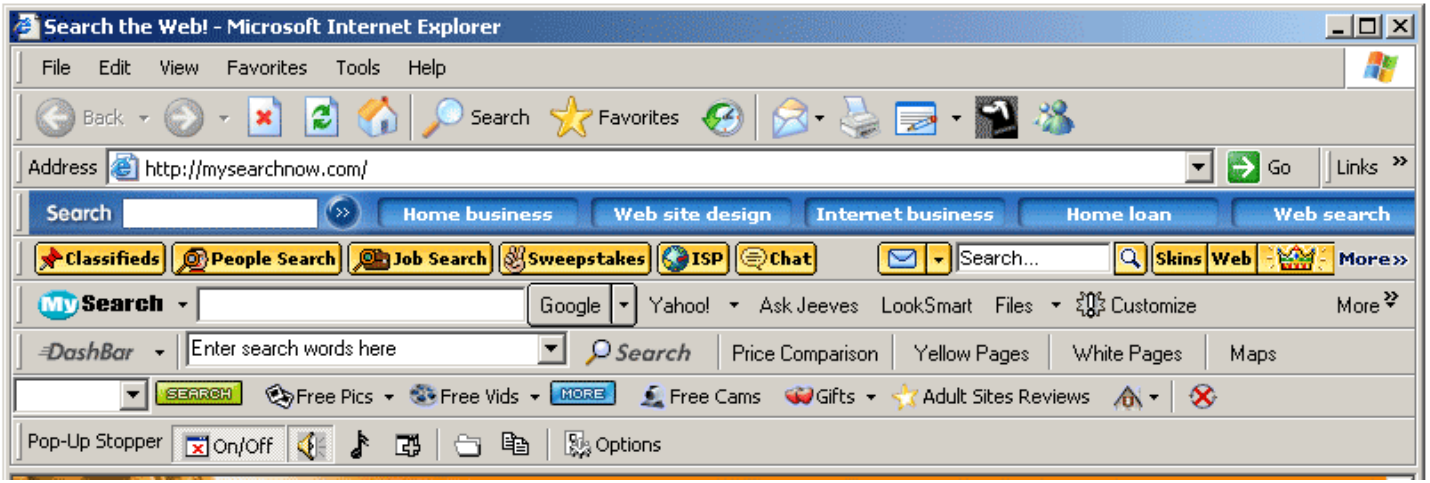
Adware: là phần mềm tự động đưa ra các trang quảng cáo vào máy tính của nạn nhân.
Spyware: tương tự Adware, nhưng còn có khả năng đánh cắp những thông tin cá nhân của nạn nhân và gửi về cho chủ nhân của nó thông qua mạng.



• Adware và Spyware không tự động tìm kiếm và lây lan sang các máy khác.
• **Các nguyên nhân** gây ra nhiễm Adware và Spyware:
+ Dùng các phần mềm freeware, shareware và các crack, keygen tải về trên mạng.
+ Chấp nhận cho cài đặt 1 Active X lạ trên mạng.
+ Sử dụng trình duyệt chưa vá lỗi bảo mật.
+ Cấu hình mức độ bảo mật của trình duyệt quá thấp.
+ Bị lây nhiễm từ 1 Virus, Adware và Spyware khác .

CÁC PHẦN MỀM CÓ HẠI

- **Phần mềm gián điệp và phần mềm quảng cáo**



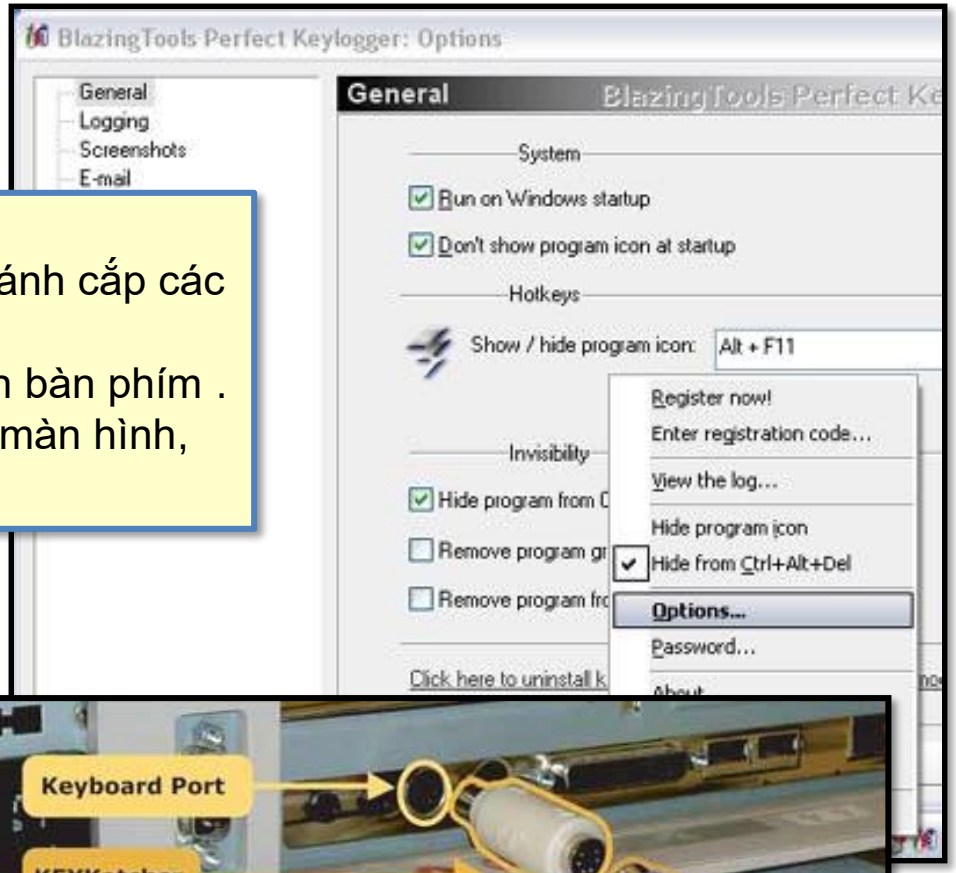
Hoạt động của các Spyware-Adware

- Trang quảng cáo (popup) tự động hiện lên
- Trang chủ, trang tìm kiếm sẽ chuyển thành 1 trang web khác.
- Trình duyệt Web tự nhiên có thêm những nút bấm (Toolbars)
- Thay đổi security level trên máy tính xuống mức thấp nhất sẽ dễ dàng cho các spyware, adware, Trojan, virus khác xâm nhập.
- Cài đặt ngầm các chương trình, thư viện liên kết động (DLL) và các tập tin thực thi khác vào máy.

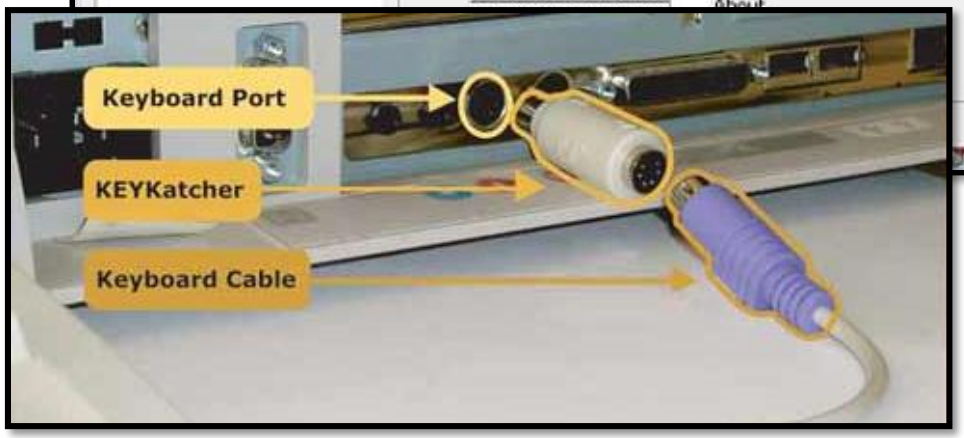
CÁC PHẦN MỀM CÓ HẠI

- **Keylogger**

• Gọi là trình theo dõi thao tác bàn phím.
• Được cài đặt vào máy tính nạn nhân nhằm đánh cắp các thông tin cá nhân.
• Theo dõi và ghi lại mọi thao tác thực hiện trên bàn phím .
• Sau này, còn ghi lại cả hình ảnh hiển thị trên màn hình, cách con chuột trên máy tính di chuyển.



Một số Keylogger nổi tiếng là: Perfect Keylogger , Spytector, KeyLog, Remote Keylogger



Keylogger được xếp vào nhóm các phần mềm gián điệp

CÁC PHẦN MỀM CÓ HẠI

- **Rootkit**

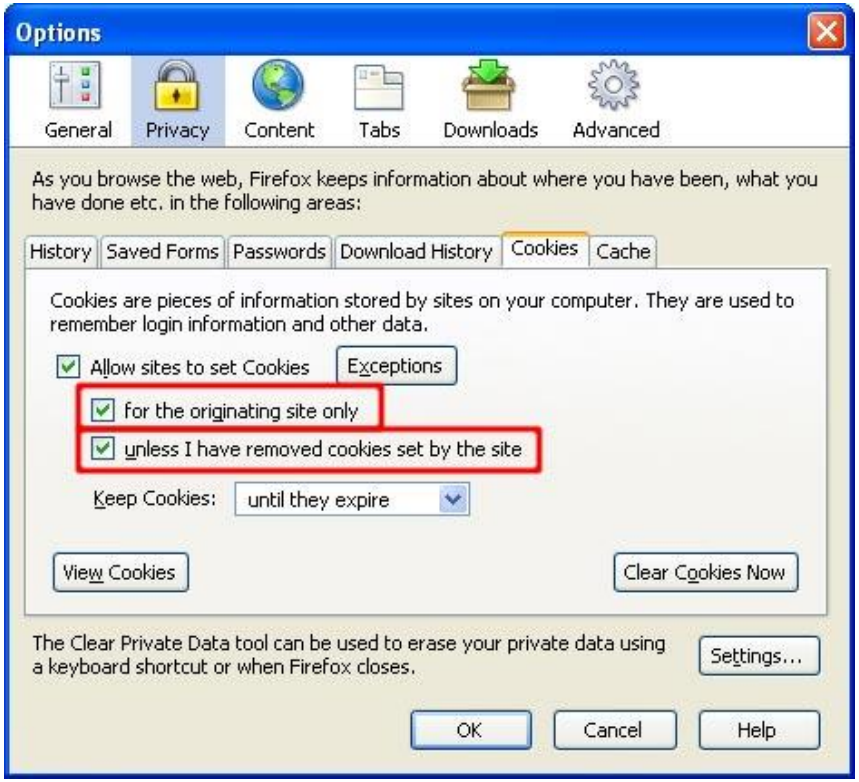
• Rootkit là bộ công cụ dùng để che giấu sự tồn tại của file hay quá trình dù nó vẫn hoạt động.
• Máy bị Rootkit được coi là bị chiếm quyền root.
• Rootkit thường gồm nhiều Backdoor giúp xâm nhập vào hệ thống dễ dàng hơn ở lần sau.
• Rootkit có thể bao gồm phần mềm đánh cắp dữ liệu từ máy tính, kết nối mạng và bàn phím.

Rootkit được xếp vào nhóm các phần mềm Trojan.

Những công cụ thông dụng của hệ điều hành không thể phát hiện được rootkit.

CÁC PHẦN MỀM CÓ HẠI

- **Cookie**



• Cookie là các thông tin lưu trong máy tính thường được dùng để nhận ra người dùng khi viếng thăm một trang web.
• Khi truy cập đến các trang web sử dụng được cookie đã lưu, những cookie này tự động gửi thông tin của người dùng về cho chủ nhân của nó.
• Cookie có thể tiết lộ bí mật về người dùng.

Cookie là 1 dạng của Spyware nhưng chúng không hoàn toàn xấu

Buổi sau

Nhắc lại các hệ mật mã