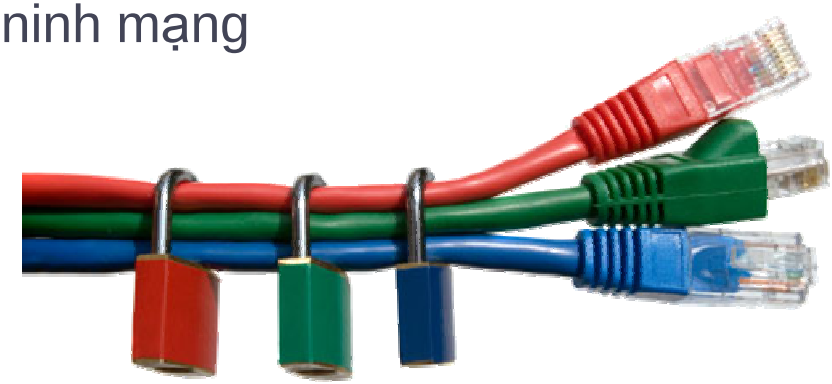
Chương 1

Tổng quan về an toàn hệ thống và an ninh mạng

- Thế nào là an toàn hệ thống và an ninh mạng
- Tấn công trên mạng
- Các phần mềm có hại
- Các yêu cầu của một hệ thống mạng an toàn



Mục tiêu

- Cung cấp cho người học một cái nhìn tổng quan về an toàn mạng và các vấn đề liên quan trong an toàn mạng.
- Sau khi hoàn tất chương, sinh viên có những khả năng:
  - Giải thích được thế nào là an toàn hệ thống và an ninh mạng.
  - Phân loại và trình bày được các mối đe dọa đối với hệ thống máy tính và hệ thống mạng.
  - Trình bày được các kỹ thuật tấn công trên mạng gồm: tấn công thăm dò, tấn công truy cập, tấn công từ chối dịch vụ.
  - Hiểu và phân loại được các phần mềm có hại và cách thức hoạt động của từng loại phần mềm có hại.
  - Mô tả được các yêu cầu cơ bản của 1 hệ thống an toàn mạng: chứng thực, phân quyền và giám sát.

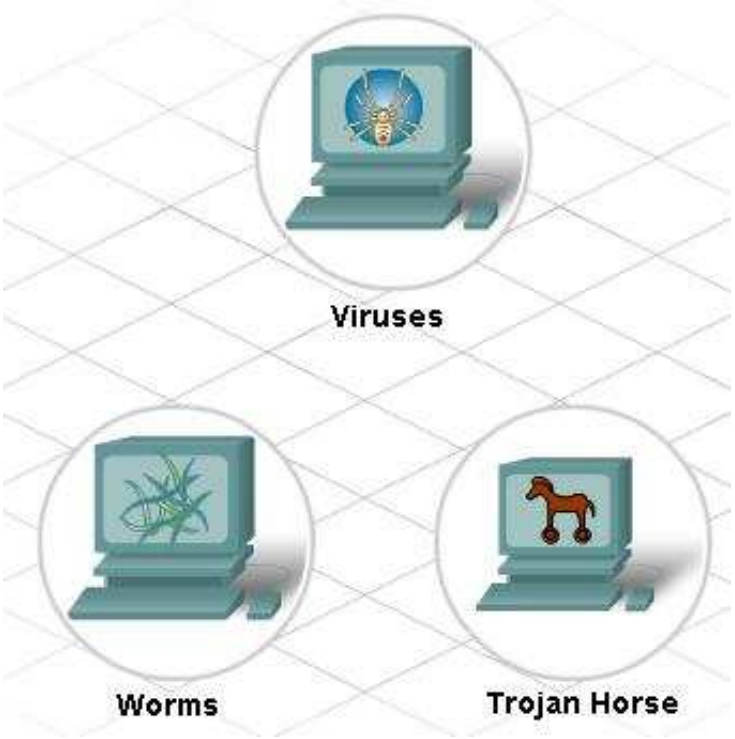
Phần 3

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

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.

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

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)

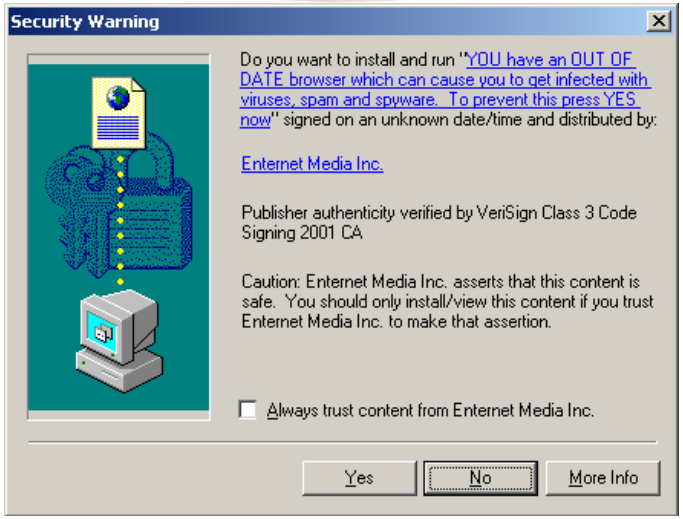
• Tác giả viết ra Trojan lừa cho đối phương sử dụng chương trình của mình. Khi đó, 1 phần của Trojan sẽ bí mật cài đặt ngầm lên máy của nạn nhân.
• Đến một thời điểm định trước, chương trình này có thể sẽ ngầm gửi những thứ thông tin bí mật của nạn nhân cho chủ nhân của nó ở trên mạng.

• 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

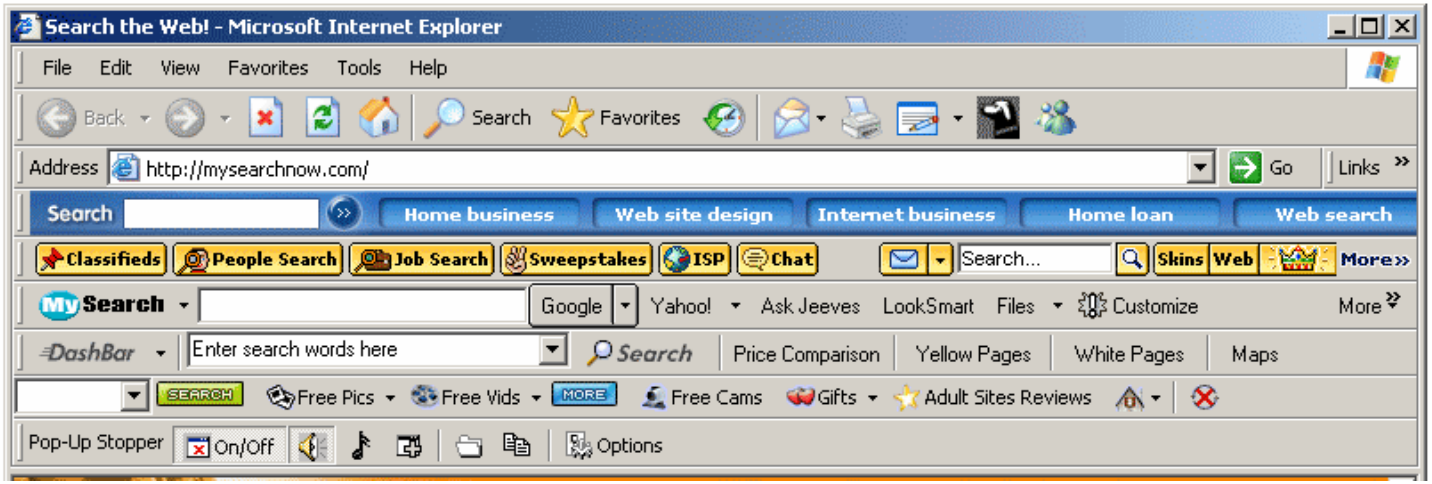
Adware: là phần mềm tự động đưa ra các trang quảng cáo vào máy tính của nạn nhân.
Spyware: tương tự Adware, nhưng còn có khả năng đánh cắp những thông tin cá nhân của nạn nhân và gửi về cho chủ nhân của nó thông qua mạng.



• 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.

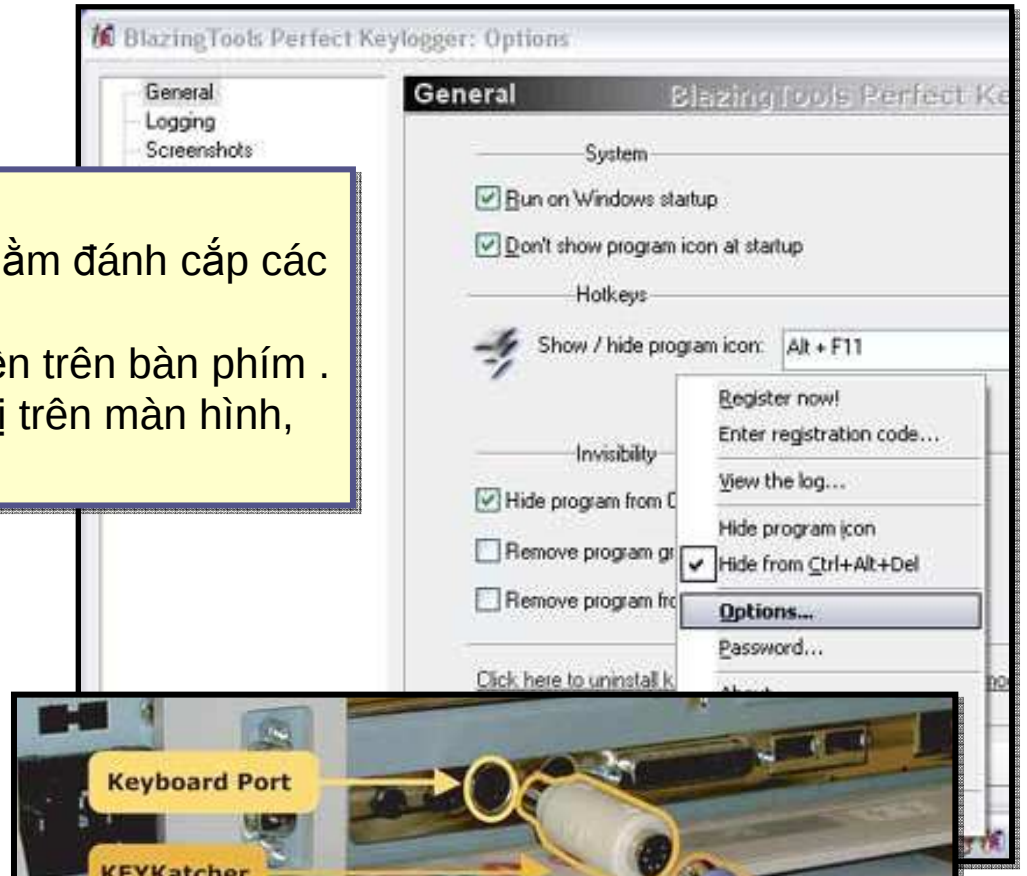
Các phần mềm có hại

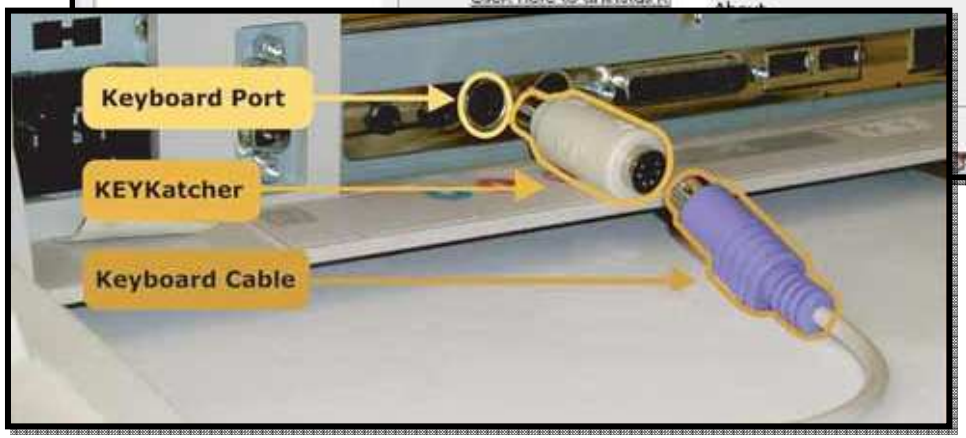
- Keylogger

• 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

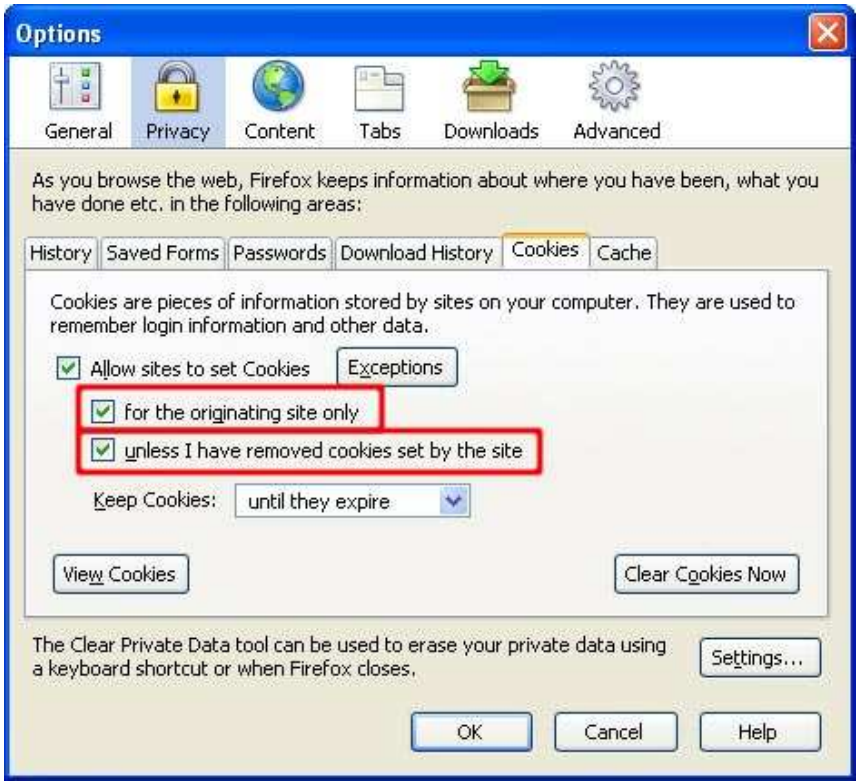
• Rootkit là bộ công cụ dùng để che giấu sự tồn tại của file hay quá trình dù nó vẫn hoạt động.
• Máy bị Rootkit được coi là bị chiếm quyền root.
• Rootkit thường gồm nhiều Backdoor giúp xâm nhập vào hệ thống dễ dàng hơn ở lần sau.
• Rootkit có thể bao gồm phần mềm đánh cắp dữ liệu từ máy tính, kết nối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

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

Rootkit được xếp vào nhóm các phần mềm Trojan.

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