BÀI GIẢNG

TIN HỌC ĐẠI CƯƠNG

Các vấn đề xã hội của Công nghệ thông tin

Các vấn đề xã hội

- **An toàn trong xã hội thông tin**
- **Mạng xã hội**
- **Sở hữu trí tuệ**

An toàn trong xã hội thông tin

- **Các tài nguyên cần bảo vệ**
- **Các hình thức tấn công**
- **Các quy phạm pháp luật**

Các tài nguyên cần bảo vệ

- **Nội dung thông tin:**
  - **Các tấn công vào nội dung thông tin thường với mục tiêu chiếm đoạt hoặc phá hủy thông tin**
- **Tài nguyên, hạ tầng thông tin**
  - **tập trung vào hạ tầng tính toán và lưu trữ. Đối tượng tấn công sẽ tìm mọi cách để tiêu thụ hết tài nguyên tính toán và lưu trữ khiến hạ tầng công nghệ thông tin bị quá tải thậm chí sụp đổ**
- **Định danh người dùng**
  - **việc bị đánh cắp định danh hay giả mạo định danh sẽ gây ra những hậu quả khôn lường (uy tín, danh tiếng...)**

Các hình thức tấn công chính

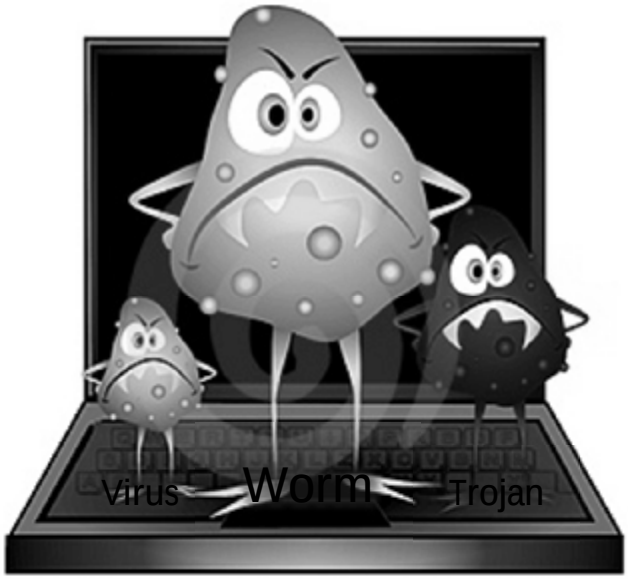
- **Khai thác lỗ hổng phần mềm**
- **Sử dụng phần mềm độc hại**
- **Từ chối dịch vụ**
- **Lừa đảo**

Lỗ hổng phần mềm

- **lỗ hổng có thể đến từ bản thân thiết kế của sản phẩm,**
- **lỗi lập trình trong quá trình phát triển,**
- **lỗi trong quá trình cài đặt, cấu hình và vận hành sản phẩm.**
- **Các lỗ hổng cũng có thể đến từ hạ tầng đóng vai trò làm nên cho sản phẩm:**
  - **hệ điều hành,**
  - **hệ quản trị cơ sở dữ liệu hay những công cụ,**
  - **ngôn ngữ lập trình, trình biên dịch, và các frameworks.**

=> Do đó khai thác lỗ hổng phần mềm vẫn là một phương pháp hữu hiệu nhằm tấn công vào các hệ thống thông tin

Sử dụng phần mềm độc hại



Virus

- **Virus là những chương trình hoặc đoạn mã lệnh được thiết kế để bám vào một tập tin nào đó.**
- **Khi được kích hoạt Virus sẽ thực hiện hai nhiệm vụ chính**
  - **Thực hiện chức năng mà virus được thiết kế để thực hiện**
    - **VD: virus Doodle Yankee đúng 17h là hát quốc ca.**
  - **Thực hiện tìm kiếm các tập tin trên hệ thống máy tính và tạo ra các nhân bản của nó và bám vào các tập tin được lựa chọn.**

Phân loại virus

- **Compiled Virus: là loại virus có thể được thi hành trực tiếp bởi hệ điều hành**
  - **File virus: lây nhiễm tới các tập tin thi hành trên hệ thống máy tính như ứng dụng soạn thảo văn bản, bảng tính hay các chương trình trò chơi, các chương trình chát trên mạng,**
  - **Boot virus: lây nhiễm vào phân vùng khởi động của các thiết bị lưu trữ.**
  - **Multipartite lây nhiễm theo tệp tin và lây nhiễm trên phân vùng khởi động. Ví dụ: Flip và Invader.**
- **Interpreted virus:**

- **Interpreted chứa đựng mã nguồn chương trình và chỉ được thi hành bởi một ứng dụng hay dịch vụ nào đó =>Phổ biến**
  - **macro virus: bám vào các tập tin tài liệu chẳng hạn như các tập tin văn bản, các bảng tính và sử dụng các trình thông dịch ngôn ngữ macro của ứng dụng để thi hành và lây lan.**
    - **VD: Một ví dụ tiêu biểu là ứng dụng Microsoft Office, một phần mềm được sử dụng rộng rãi và cho phép người sử dụng tạo các macro bằng ngôn ngữ VB.Script**
      - **Cocept, Marker, và Melissa.**
  - **scripting virus: được viết bởi những ngôn ngữ được hiểu bởi một dịch vụ nào đó chạy bởi hệ điều hành**

SÂU (SWORM)

- **sâu (worm) là một chương trình hoàn chỉnh độc lập có khả năng nhân bản và di chuyển từ hệ thống máy tính này sang hệ thống máy tính khác**
- **Network service worms là những sâu máy tính lan truyền bằng cách khai thác những lỗ hổng trong một dịch vụ mạng gắn kết với hệ điều hành hoặc một ứng dụng nào đó**
- **Mass mailing worms là những sâu máy tính thực hiện lan truyền dựa trên cơ chế phát tán thư điện tử trên các hệ thống thư điện tử.**

Trojan

- được lấy tên theo tên con ngựa gỗ trong truyền thuyết **Trojan Horse (Con ngựa thành Troa) trong thần thoại Hy lạp.**
- **Trojan: không có khả năng nhân bản.**
  - **Trojan thường tỏ ra vô hại thậm chí là có lợi cho người dùng nhưng ẩn trong nó là những mục đích xấu.**
  - **Trojan là một phần mềm hoàn chỉnh có thể được cài đặt theo các lỗ hổng an ninh vào máy tính do sự sơ suất của người dung khi truy cập mạng máy tính.**
  - **Trojan cũng có thể núp danh một phần mềm tiện ích và được người dùng cài đặt một cách tường minh.**

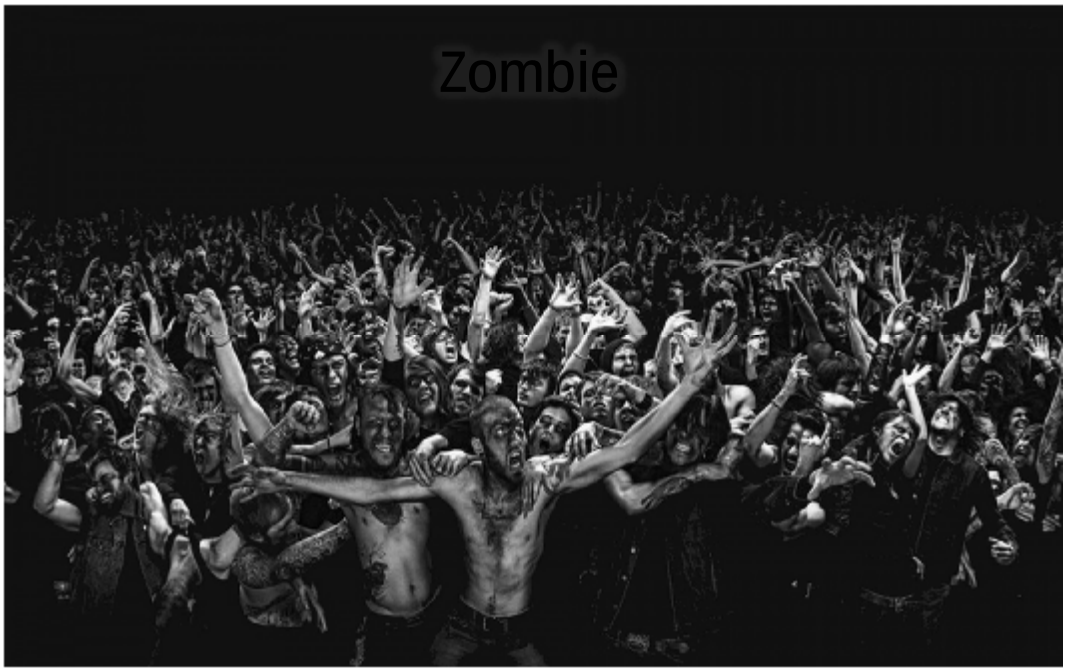
Phân loại Trojan

- **Spyware đóng vai trò là gián điệp, nó thu thập những thông tin cần thiết trên hệ thống bị lây nhiễm và gửi thông tin đó tới một hệ thống nào đó.**
- **Adware đóng vai trò quảng cáo, nó thường hoạt động bằng cách bật những quảng cáo trên hệ thống bị lây nhiễm.**
- **Key logger có nhiệm vụ ghi lại các phím đã được gõ trên bàn phím và gửi tới hệ thống phân tích nào đó bên ngoài.**
- **Backdoor có nhiệm vụ mở ra một cổng sau để tin tặc có thể khai thác hệ thống máy tính bị lây nhiễm.**
- **Rootkit được sử dụng để thu thập các tập tin được cài đặt lên hệ thống và thay thế chúng.**

Từ chối dịch vụ

Những tấn công với mục tiêu là làm tê liệt các hệ thống máy tính hay các dịch vụ được gọi là tấn công từ chối dịch vụ - Denial of Service (DoS). Tấn công từ chối dịch vụ có thể được phân thành hai kiểu chính là **vulnerability-based attacks** và **flooding attacks**.

Từ chối dịch vụ



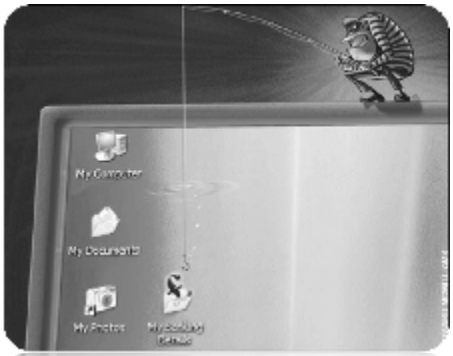
DoS

- **Vulnerability-based attack (tấn công dựa trên lỗ hổng) hay còn gọi là semantic attacks: là hình thức tấn công khai thác một hoặc nhiều lỗ hổng trong chính sách an ninh hoặc trong kỹ thuật nhằm hiệu lực chính sách đó, hoặc những lỗi tiềm ẩn trong phần mềm.**
- **Flooding attacks hay còn gọi là brute-force attack: tạo ra một một lượng lớn yêu cầu hợp lệ (thường là giống nhau) nhằm tiêu thụ một tài nguyên mục tiêu nào đó trên hệ thống khiến tài nguyên đó bị quá tải không thể đáp ứng những yêu cầu đến từ những người dùng hợp lệ khác.**

DDOS

- **Khi những yêu cầu nhằm mục đích tấn công của tin tặc đến từ nhiều máy tính khác nhau được phân tán trên mạng, thì được gọi là tấn công từ chối dịch vụ phân tán – distributed denial of service (DdoS).**
- **Ngược lại, khi những yêu cầu nhằm mục đích tấn công này đến từ cùng một máy chủ thì được gọi là single-source denial of service (SDoS).**

Lừa đảo (Phising)



- **Lừa đảo (Phishing) là hình thức trong đó kẻ tấn công (hay kẻ lừa đảo – phisher) tìm cách để chiếm đoạt thông tin bí mật hoặc những ủy nhiệm nhạy cảm của người sử dụng một khéo léo.**

Lừa đảo

- **Clone phishing: Trong phương thức này, kẻ lừa đảo tạo ra một thư nhân bản từ một bức thư hợp lệ nào đó.**
- **Spear phishing :nó nhắm tới một nhóm cụ thể. Thay vì tiến hành gửi thư cho các mục tiêu ngẫu nhiên, spear phishers sẽ lựa chọn các nhóm người với một số điểm chung nào đó chẳng hạn những người thuộc cùng một tổ chức**
- **Phone Phishing: kẻ lừa đảo gửi tin nhắn thông báo với nội dung ngân hàng yêu cầu người sử dụng gọi điện tới một số cụ thể để giải quyết một vài vấn đề gì đó về tài khoản của họ. Kẻ lừa đảo sẽ tận dụng kỹ thuật VOIP (Voice over IP) để nắm bắt cuộc gọi và tiến hành lừa đảo.**

Các quy phạm pháp luật

- **Bộ luật hình sự**
- **Luật 67/2006/QH1**