EC Security

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Nội dung

- Giới thiệu
- Các vấn đề bảo mật trong EC
- Các loại hình tấn công
- Một số mối đe dọa đến hệ thống EC
- Chính sách bảo vệ hệ thống

Giới thiệu

Bảo mật trong EC

Giới thiệu – Virus

Chức năng

-Nhân bản

-Thực hiện nhiệm vụ

Cơ chế

- Cơ chế nhân bản
- Cơ chế hoạt động
- Mục tiêu

Lây lan

- Thiết bị lưu trữ ngoại
- Bản tin điện tử
- Internet/intranet

Hơn 10.000 loại

+200 loại / tháng

Dấu hiệu

- Chương trình chạy chậm
-Truy xuất ổ cứng nhiều
- Truy xuất thiết bị khác
-Tốn tài nguyên hệ thống
-Mất dung lượng ổ cứng
-Kích thước tập tin bị thay đổi

Các loại khác

Spyware, trojan, Malware

Source : http://www.uhd.edu/computing/uss/virus.htm

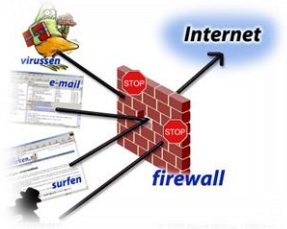
Giới thiệu – Kỹ thuật tấn công khác

- Phishing
  - Mưu đồ sử dụng email, tin nhắn dạng pop-up hay các trang web để đánh lừa người dùng cung cấp các thông tin nhạy cảm
    - Số thẻ tín dụng, số tài khoản ngân hàng, mật mã
- Lợi dụng PC
  - Các hacker tấn công và sử dụng một số PC làm nơi gửi các spam mail
- PC bị nhiễm và làm lây lan virus, worm, trojan

Giới thiệu – Vấn đề an toàn

- An toàn và bảo mật trên mạng có nhiều tiến triển
  - Bức tường lửa (firewall)
  - Mã hóa (encryption)
  - Chữ ký điện tử (digital signature)

  Nhưng vẫn còn nhiều nguy cơ đe dọa



- Điểm yếu là ý thức và hành vi của người dùng
  - Đánh lừa người khác để lấy thông tin
  - Tấn công hay phá hoại thông qua lỗ hổng của HĐH
  - Mở thư đã bị nhiễm virus
  - Xem những trang web chứa 1 số đoạn mã có ý xấu
  - …

Các vấn đề bảo mật trong EC

Bảo mật trong EC

Các vấn đề bảo mật – Ví dụ

- Trong EC, vấn đề bảo mật không chỉ là ngăn ngừa hay đối phó với các cuộc tấn công và xâm nhập

- Xét ví dụ
  - Một khách hàng cần có thông tin của các sản phẩm trên website của 1 công ty nào đó
  - Máy chủ yêu cầu khách hàng điền thông tin cá nhân
  - Sau khi cung cấp thông tin cá nhân, khách hàng mới nhận được thông tin của sản phẩm

  → Giải pháp bảo mật cho trường hợp này là gì?

Các vấn đề bảo mật – Ví dụ

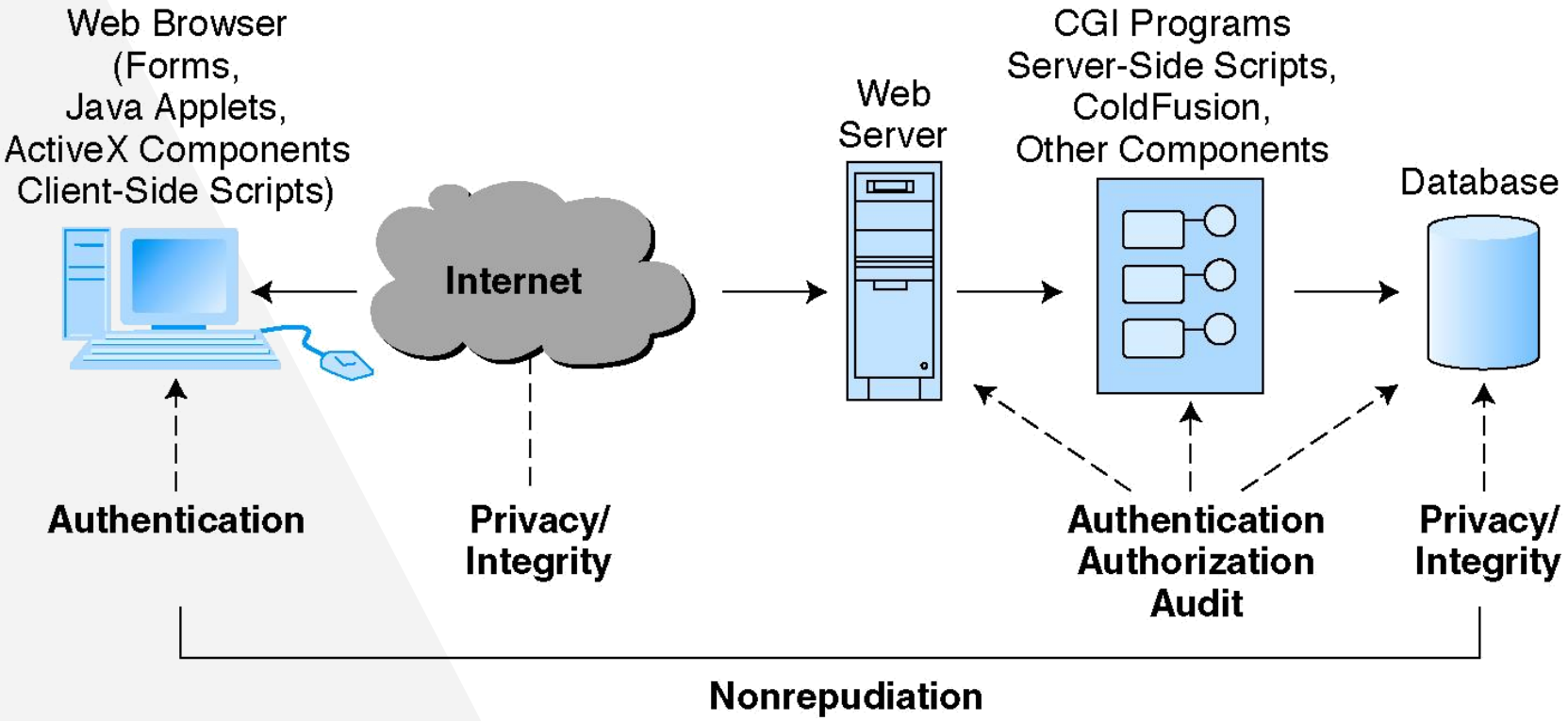
- Về phía khách hàng
  - Trang web này là của một công ty hợp pháp?
  - Có chứa các đoạn mã nguy hiểm?
  - Có cung cấp thông tin cá nhân cho một website khác?
- Về phía công ty
  - Người dùng có ý định phá server hay sửa nội dung của trang web?
- Khác
  - Có bị ai nghe lén trên đường truyền?
  - Thông tin được gửi và nhận có bị sửa đổi?

Các vấn đề bảo mật trong EC

- Bảo mật trong EC

1. Authentication – Chứng thực người dùng
2. Authorization – Chứng thực quyền sử dụng
3. Auditing – Theo dõi hoạt động
4. Confidentiality (Privacy) – Giữ bí mật nội dung thông tin
5. Integrity – Toàn vẹn thông tin
6. Availability – Khả năng sẵn sàng đáp ứng
7. Nonrepudiation – Không thể từ chối trách nhiệm

Các vấn đề bảo mật – Mô hình



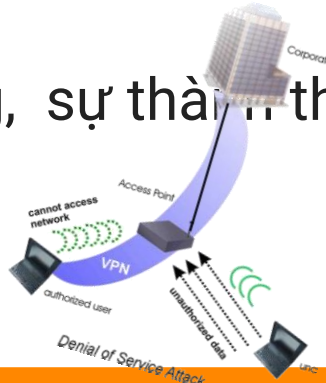
Các loại hình tấn công

Bảo mật trong EC

Các loại tấn công

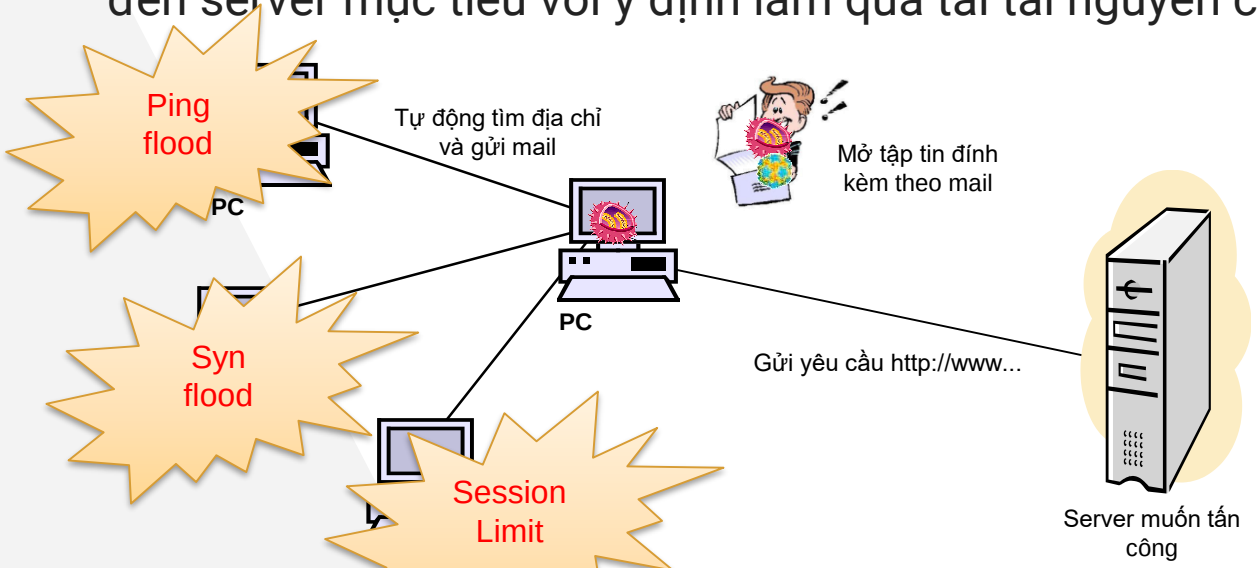
- Không sử dụng chuyên môn
  - Lợi dụng sức ép, tâm lý để đánh lừa người dùng và làm tổn hại đến mạng máy tính
  - Hình thức
    - Gọi điện thoại, gửi mail, phát ks

- Sử dụng chuyên môn
  - Các phần mềm, kiến thức hệ thống, sự thà thạo
  - Hình thức
    - DoS, DDoS
    - Virus, worm, trojan horse



Tấn công DoS

- Denial-of-Service
- Các hacker lợi dụng một máy tính nào đó gửi hàng loạt các yêu cầu đến server mục tiêu với ý định làm quá tải tài nguyên của server đó



Tấn công DDoS

Multi-Vector Attacks

Application Level Attack

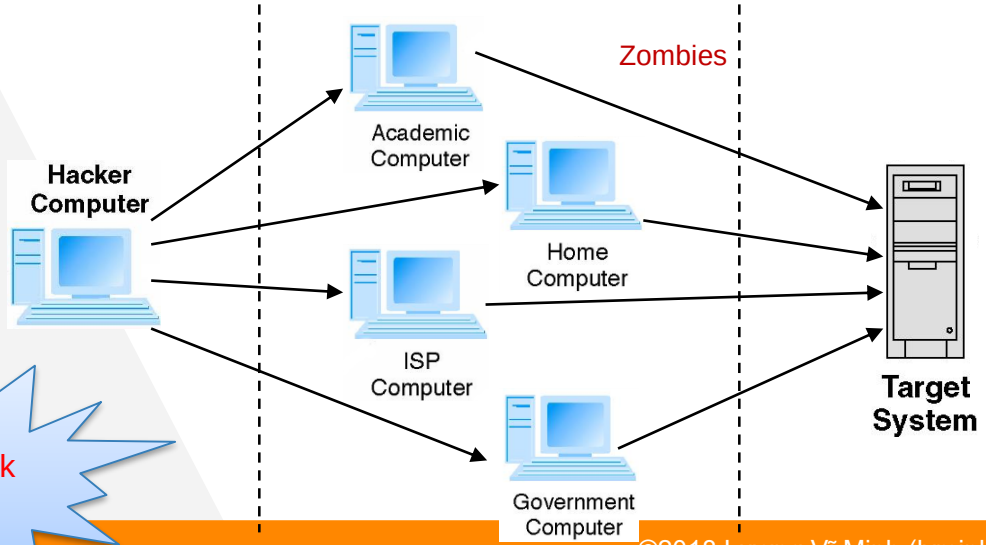
Zero Day DDoS

- Distributed Denial-of-Service
- Các hacker xâm nhập vào nhiều máy tính và cài phần mềm. Khi có lệnh tấn công, các phần mềm sẽ gửi yêu cầu đến server mục tiêu

UDP flood

Reflected Attack

P2P Attack



Slowloris

Slowloris