Học phần CT434

AN TOÀN HỆ THỐNG VÀ AN NINH MẠNG

- Mục tiêu
- Học phần tiên quyết
- Phương pháp giảng dạy và đánh giá
- Tài liệu tham khảo
- Nội dung
- Kế hoạch học tập dự kiến

Mục tiêu

- Cung cấp cho sinh viên một khối lượng kiến thức tương đối hoàn chỉnh về phương pháp xây dựng một hệ thống máy tính và mạng máy tính an toàn.
- Sau khi hoàn thành HP, sinh viên có những khả năng:
  - Giải thích được thế nào là an toàn hệ thống và an ninh mạng, các yêu cầu cơ bản cho 1 hệ thống mạng an toàn.
  - Trình bày được những nguy cơ, các dạng tấn công và một số kỹ thuật xâm nhập hệ thống máy tính và mạng máy tính.
  - Hiểu được các kiến thức nền tảng về bảo mật như: mật mã, các giải thuật dùng trong mật mã, khóa bí mật và khóa công khai, chữ ký số, chứng chỉ số, các hệ thống chứng thực.

Mục tiêu

- Sau khi hoàn thành HP, sinh viên có những khả năng (tt):
  - Phân biệt và vận dụng được các kỹ thuật gia cố hệ thống.
  - Phân tích những điểm yếu và cách thiết lập các cơ chế an toàn cho những chủng loại thiết bị mạng khác nhau.
  - Hiểu và xây dựng được các mô hình mạng an toàn, những giải pháp an toàn cho các dịch vụ Internet thông dụng.
  - Cài đặt được một số kỹ thuật, giải pháp và công nghệ an ninh mạng phổ biến hiện nay như: chứng thực, mã hóa, tường lửa, mạng riêng ảo, hệ thống phát hiện xâm nhập.
  - Trình bày được cách thức quản lý và điều hành một hệ thống mạng an toàn.

Học phần tiên quyết

- Học phần tiên quyết
  - Mạng máy tính (CT112)
- Các kiến thức khác cần biết để có thể tiếp thu tốt học phần:
  - Thiết kế và cài đặt mạng (CT335)
  - Lập trình Web (CT301)
  - An toàn và bảo mật thông tin (CT313)
  - Giải quyết sự cố mạng (CT344)

Phương pháp GD và đánh giá

- Phương pháp giảng dạy
  - Giảng dạy 30 tiết lý thuyết trên lớp
  - Thực hành 30 tiết (6 buổi x 5 tiết/buổi)
  - Sinh viên đọc trước slide và tài liệu TK ở nhà.
- Phương pháp đánh giá
  - Thi giữa kỳ 35%
  - Thi cuối kỳ 60%
  - Chuyên cần 5%

Tài liệu tham khảo

- Michael Cross, Jeremy Faircloth, Eli Faskha, Michael Gregg, Alun Jones, Marc Perez, *Security+ : Study Guide and Practice Exam*, 2nd edition, Syngress, 2007.
- James Michael Stewart, *Security+ fast pass*, Sybex, 2004.
- Cisco networking academy, *Network security v2.0*, 2004.
- William Stallings, *Network security essentials*, 2nd edition, Prentice Hall, 2003.
- Eric Maiwald, *Network security: A beginner's guide*, 2nd edition, McGraw-Hill, 2003.
- Joseph Migga Kizza, *Computer network security*, Springer, 2005.

Nội dung

- Chương 1: Tổng quan về an toàn mạng
  - Tại sao an toàn mạng là cần thiết.
  - Thế nào là an toàn hệ thống và an ninh mạng.
  - Tấn công trên mạng:
    - Tấn công thăm dò
    - Tấn công truy cập
    - Tấn công từ chối dịch vụ
  - Các phần mềm có hại.
  - Các yêu cầu của 1 hệ thống mạng an toàn (AAA)
    - Chứng thực (Authentication)
    - Phân quyền (Authorization)
    - Giám sát (Accounting)

Nội dung

- Chương 2: An toàn cho các thiết bị mạng
  - Tầng vật lý
  - Tầng liên kết dữ liệu
  - Tầng mạng
  - Tầng vận chuyển và các tầng trên
- Chương 3: Gia cố hệ thống *(system hardening)*
  - Khái niệm
  - Gia cố hệ điều hành và hệ điều hành mạng
  - Gia cố ứng dụng
  - Tổ chức chính sách an ninh mạng
  - Điều tra xâm nhập

Nội dung

- Chương 4: Căn bản về mật mã *(Cryptography)*
  - Khái niệm
  - Các thuật toán:
    - Băm: MD5, SHA-1
    - Mã hóa đối xứng: DES, 3DES, AES, IDEA
    - Mã hóa bất đối xứng: RSA, DSA, DH, …
  - Ứng dụng của mật mã
  - Khóa bí mật và khóa công khai
  - Hạ tầng khóa công khai
  - Chữ ký số và chứng chỉ số
  - Quản lý khóa và chứng chỉ số

Nội dung

- Chương 5: An toàn trong truyền thông
  - Truy cập từ xa:
    - PPP
    - Telnet
    - Mạng không dây (WLAN)
    - Mạng riêng ảo (VPN)
  - Truy cập liên mạng:
    - Email
    - Web
    - FTP
    - Chia sẻ tập tin (File sharing)
    - Dịch vụ thư mục (Directory service)

Nội dung

- Chương 6: An toàn cho các mô hình mạng
  - Các vùng an ninh
    - Intranet
    - Extranet
    - DMZ
  - Mạng cục bộ ảo (VLANs)
    - LAN
    - VLAN
    - Cấu hình VLAN
  - NAT
    - NAT
    - PAT
    - Cấu hình NAT và PAT

Nội dung

- Chương 7: Tường lửa và hệ thống phát hiện xâm nhập *(Firewalls, Intrusion detection systems)*
  - Bộ lọc
    - Bộ lọc tầng 3
    - Proxy Server
  - Tường lửa
    - Khái niệm - Phân loại
    - Cấu hình
    - Thiết kế tập quy tắc
  - Hệ thống phát hiện xâm nhập (IDS)
    - Khái niệm, Phân loại, Lợi và hại.
    - Cấu hình và quản trị hệ thống