Nhập môn An toàn thông tin

PGS. Nguyễn Linh Giang

Bộ môn Truyền thông và Mạng máy tính

Nội dung

I. Nhập môn An toàn thông tin
II. Đảm bảo tính mật
    I. Các hệ mật khóa đối xứng (mã hóa đối xứng)
    II. Các hệ mật khóa công khai (mã hóa bất đối xứng)
III. Bài toán xác thực
    I. Cơ sở bài toán xác thực
    II. Xác thực thông điệp
    III. Chữ ký số và các giao thức xác thực
    IV. Các cơ chế xác thực trong các hệ phân tán
IV. An toàn an ninh hệ thống
    I. Phát hiện và ngăn chặn xâm nhập (IDS, IPS)
    II. Lỗ hổng hệ thống

Nội dung

- Tài liệu môn học:
  - W. Stallings “Networks and Internetwork security”
  - W. Stallings “Cryptography and network security”
  - Introduction to Cryptography – PGP
  - D. Stinson – Cryptography: Theory and Practice

Các chủ đề tiểu luận

- 1. Các hệ mật khóa công khai.
  - Cơ sở xây dựng hệ mật khóa công khai
  - Các hệ mật khóa công khai.
  - Các sơ đồ ứng dụng.
- 2. Hạ tầng khóa công khai PKI
  - Cấu trúc hạ tầng khóa công khai.
  - Chứng chỉ số, các chuẩn;
  - Triển khai thực tế. Các ứng dụng trong các giao dịch.
  - Các hệ thống mã nguồn mở.

Các chủ đề tiểu luận

- 3. Bảo mật cho mạng IP. IPSec. Mạng riêng ảo VPN. Ứng dụng.
- 4. Bài toán xác thực thông điệp.
  - Các cơ chế xác thực
  - Hàm băm và hàm mã hóa xác thực.
  - Các giao thức xác thực.
- 5. Chữ ký số.
  - Các cơ chế tạo chữ ký số. Giao thức chữ ký số.
  - Các dịch vụ chữ ký số.
  - Chữ ký mù.
  - Ứng dụng.

Các chủ đề tiểu luận

- 6. Phát hiện xâm nhập mạng.
  - Các cơ chế phát hiện xâm nhập mạng.
  - Phát hiện theo dấu hiệu
  - Phát hiện theo bất thường
  - Phân tích các đặc trưng thống kê của mạng.
  - Ứng dụng.
- 7. Bảo mật cho mạng không dây. Phân tích các đặc trưng thống kê của các dạng tấn công từ chối dịch vụ. Xác thực và bảo mật trong mạng không dây. Phát hiện bất thường trong mạng không dây.

Các chủ đề tiểu luận

- 8. Bảo mật hệ thống, bảo mật mạng. Các chính sách, các chuẩn. Phân tích đối với Windows và Unix-Linux. Các chính sách an ninh mạng cho mạng Cisco.
- 9. Bảo vệ dữ liệu đa phương tiện trong quá trình phân phối qua hệ thống mạng mở. Vấn đề bảo mật, bảo vệ bản quyền và kiểm soát sử dụng dữ liệu đa phương tiện.

Các chủ đề tiểu luận

- 10. Bảo mật cho web services;
- 11. Đăng nhập 1 lần với các giao thức OpenID, OAuth;
- 12. Xác thực Kerberos;
- 13. SSL và TLS và các ứng dụng
- 14. IPSecurity, giao thức và VPN
- 15. Xác thực X509.

Các chủ đề tiểu luận

- 16. Hạ tầng khóa công khai PKI
- 17. PGP, bảo mật thư tín điện tử, S/MIME, bảo mật dịch vụ Internet.
- 18. Secure electronic transaction
- 19. Firewall, các kiến trúc firewall.
- 20. Proxy, cấu trúc và hoạt động của proxy;
- 21. Rà quét lỗ hổng bảo mật cho Windows, Unix-Linux
- 22. Hệ thống phát hiện xâm nhập dựa trên dấu hiệu;
- 23. Hệ thống phát hiện xâm nhập dựa trên bất thường;

Các chủ đề tiểu luận

- 24. Bảo mật mạng LAN không dây;
- 25. Các dạng tấn công vào mạng sensor.
- 26. Các dạng tấn công từ chối dịch vụ;
- 27. Tấn công SQL Injection, phát hiện và tìm kiếm lỗi SQL Injection;
- 28. Phát hiện tấn công quét cổng;
- 29. Các phương pháp, quy trình phát hiện lỗ hổng hệ thống.
- 30. Các mô hình tiền điện tử trong giao dịch điện tử.
- 31. Xác thực sinh trắc.
- 32. Điện toán đám mây và bảo mật điện toán đám mây.
- 33. Kỹ thuật thủy vân số (Digital Watermarking)
- 34. Giấu tin trong dữ liệu đa phương tiện (Steganography)

Đánh giá

- Giữa kỳ và quá trình: 30%
  - Điểm danh: 1/3.
- Thi hết môn: 70%
- Liên hệ giáo viên:
- giangnl@soict.hust.edu.vn;
- số Bộ môn: 024-38682596; mobile: 0854244425