**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CÔNG NGHỆ THÔNG TIN**

**\*\*\*\*\***

**ĐỀ CƯƠNG MÔN HỌC**

**(Phương pháp đào tạo theo tín chỉ)**

**TÊN HỌC PHẦN: AN TOÀN MẠNG NÂNG CAO**

**Mã học phần: INT1483**

**(3 tín chỉ)**

**Biên soạn**

**NGUYỄN NGỌC ĐIỆP**

**Hà Nội - 2016**

**ĐỀ cương HỌC PHẦN: AN TOÀN MẠNG NÂNG CAO**

**Khoa:** Công nghệ thông tin 1 **Bộ môn**: An toàn thông tin

**1.Thông tin về giảng viên**

***1.1. Giảng viên 1:***

Họ và tên: Nguyễn Ngọc Điệp

Chức danh, học hàm, học vị: Giảng viên - Thạc sỹ

Địa điểm làm việc: Bộ môn An toàn thông tin, Khoa Công nghệ thông tin 1,

Học viện Công nghệ Bưu chính Viễn thông

Địa chỉ liên hệ: Bộ môn An toàn thông tin, Khoa Công nghệ thông tin 1,

Học viện Công nghệ Bưu chính Viễn thông

Điện thoại: Email: diepnguyenngoc@ptit.edu.vn

Các hướng nghiên cứu chính: Điện toán lan tỏa, nhận dạng hoạt động người, An toàn và bảo mật thông tin.

***1.2. Giảng viên 2:***

Họ và tên: Phạm Hoàng Duy

Chức danh, học hàm, học vị: Tiến sỹ, Giảng viên

Địa điểm làm việc: Bộ môn An toàn thông tin, Công nghệ thông tin 1,

Học viện Công nghệ Bưu chính Viễn thông

Địa chỉ liên hệ: Bộ môn An toàn thông tin, Công nghệ thông tin 1,

Học viện Công nghệ Bưu chính Viễn thông

Điện thoại: Email: phamhduy@gmail.com

Các hướng nghiên cứu chính: Hệ đa tác tử, Lô gíc không đơn điệu và khai phá dữ liệu, An toàn và bảo mật thông tin.

**2. Thông tin chung về môn học**

- Tên môn học: An toàn mạng nâng cao

- Tên tiếng Anh của môn học: Advanced network security

- Mã môn học: INT1483

- Số tín chỉ (TC): 3

- Loại môn học:Bắt buộc

- **Các** **môn học tiên quyết**:

- **Môn học trước:** An toàn mạng, Cơ sở An toàn thông tin

- **Môn học song hành:**

- Các yêu cầu đối với môn học (nếu có):

Phòng học lý thuyết: Có máy chiếu

Phòng thực hành: Phòng máy tính nối mạng Internet

- Giờ tín chỉ đối với các hoạt động:

+ Nghe giảng lý thuyết: 30 tiết

+ Chữa bài trên lớp: tiết

+ Bài tập lớn/Tiểu luận: 4 tiết

+ Thảo luận và Hoạt động nhóm: 2 tiết

+ Thí nghiệm, Thực hành: 8 tiết

+ Tự học: 1 tiết

**Địa chỉ Khoa/Bộ môn phụ trách môn học:**

- Địa chỉ: Bộ môn An toàn thông tin, Khoa Công nghệ thông tin 1, Học viện Công nghệ Bưu chính Viễn thông, Km 10 Nguyễn Trãi, Hà Đông, Hà Nội

- Điện thoại: 04.3854 5604

**3. Mục tiêu của môn học**

- ***Về kiến thức***: Trang bị cho sinh viên các kiến thức về các kỹ thuật nâng cao để đảm bảo an toàn thông tin, hệ thống và mạng

- ***Kỹ năng:*** Giúp sinh viên nắm vững các kiến thức về các kỹ thuật nâng cao để đảm bảo an toàn thông tin, hệ thống và mạng; có khả năng phân tích và lựa chọn các giải pháp đã học về đảm bảo an toàn thông tin, hệ thống và mạng phù hợp cho từng trường hợp cụ thể.

- ***Thái độ, Chuyên cần:*** Sinh viên cần tham gia học tập đầy đủ trên lớp và làm các bài tập về nhà.

### Mục tiêu chi tiết cho từng nội dung của môn học

|  |  |  |  |
| --- | --- | --- | --- |
| **Mục tiêu**  **Nội dung** | **Bậc 1** | Bậc 2 | **Bậc 3** |
| ***Chương 1: Các kỹ thuật bảo mật cơ sở hạ tầng thông tin*** | Hiểu được các kỹ thuật bảo mật cơ sở hạ tầng thông tin, bao gồm: tường lửa, điều khiển truy cập, mạng riêng ảo, hệ thống honeypot và kỹ thuật phòng chống DDoS | Phân tích các yêu cầu cơ bản của từng kỹ thuật bảo mật cơ sở hạ tầng thông tin | Vận dụng được các kỹ thuật bảo mật đã học để ứng dụng trong trường hợp thực tế |
| ***Chương 2:*** ***Các kỹ thuật bảo mật thông tin trên đường truyền*** | Hiểu được các kỹ thuật bảo mật thông tin trên đường truyền | Phân tích các yêu cầu cơ bản của từng kỹ thuật bảo mật thông tin trên đường truyền | Vận dụng được các kỹ thuật bảo mật đã học để ứng dụng trong trường hợp thực tế |
| ***Chương 3: Bảo mật cho các hệ thống mạng*** | Hiểu được các kỹ thuật bảo mật cho các hệ thống mạng | Phân tích các yêu cầu đối với các kỹ thuật bảo mật cho các hệ thống mạng | Vận dụng được các kỹ thuật bảo mật cho các hệ thống mạng trong thực tế |
| ***Chương 4: Bảo mật cho điện toán đám mây*** | Hiểu được kỹ thuật bảo mật cho điện toán đám mây | Phân tích các yêu cầu đối với bảo mật cho điện toán đám mây | Vận dụng được kỹ thuật bảo mật điện toán đám mây cho hệ thống thực tế |

**4. Tóm tắt nội dung môn học**

Môn học cung cấp các kiến thức chuyên sâu về các kỹ thuật đảm bảo an toàn cơ sở hạ tầng thông tin mạng; Các kỹ thuật bảo mật thông tin trên đường truyền bao gồm các giao thức bảo mật thông tin thông dụng; Các giải pháp bảo mật cho mạng cục bộ, mạng intranet, mạng máy tính không dây và mạng di động, điện toán đám mây.

**5. Nội dung chi tiết môn học**

**Chương 1: Các kỹ thuật và công nghệ đảm bảo an toàn hệ thống mạng**

* 1. Điều khiển truy cập
     1. Kiểm soát an toàn vật lý
     2. Phương pháp xác thực
     3. Phương pháp điều khiển truy cập
  2. Tường lửa
     1. Khái niệm về tường lửa
     2. Một số loại tường lửa
     3. Một số chức năng phụ trợ
     4. Triển khai tường lửa
  3. Công nghệ mạng riêng ảo
     1. Cơ chế hoạt động
     2. Các giao thức mạng riêng ảo
     3. Triển khai mạng riêng ảo
  4. Hệ thống honeypot
     1. Khái niệm về hệ thống honeypot
     2. Các loại honeypot
     3. Triển khai hệ thống honeypot
     4. Bài tập về cấu hình và triển khai honeypot
  5. Phòng chống DDoS
     1. Phân tích tấn công DDoS trong mạng Internet
     2. Phương pháp phòng chống DDoS
     3. Kiến trúc mạng hỗ trợ tìm kiếm IP

**Chương 2: Các kỹ thuật bảo mật thông tin trên đường truyền**

2.1. Các yêu cầu bảo mật thông tin trên đường truyền

2.1.1. Bảo mật thông tin mạng và các dịch vụ mạng

2.1.2. Bảo mật trao đổi thông tin

2.1.3. Bảo mật dịch vụ thương mại điện tử

2.1.4. Theo dõi giám sát thông tin mạng

2.2. Các giải pháp bảo mật thông tin dựa trên mã hoá

2.2.1. Hạ tầng khóa công khai PKI

2.2.2. Chữ ký số

2.2.3. Chứng chỉ số

2.2.4. Các hệ thống mật mã lai

2.2.5. Kỹ thuật giấu tin

2.3. Các giao thức bảo mật thông tin

2.3.1. IPSec

2.3.2. SSL/TLS, SSH

2.3.3. PGP và S-MIME

2.3.4. Giao thức nặc danh

**Chương 3: Bảo mật cho các hệ thống mạng**

3.1. Bảo mật cho mạng cục bộ

3.1.1. Các nguy cơ và lỗ hổng

3.1.2. Phân tích, đánh giá rủi ro

3.1.3. Chính sách bảo mật

3.1.4. Thiết kế mạng an toàn với điều khiển truy cập, tường lửa và IDS

3.2. Bảo mật cho mạng cục bộ không dây

3.3.1. Mạng cục bộ không dây

3.3.2. Các giao thức an toàn

3.3. Bảo mật cho mạng Intranet

3.2.1. Các nguy cơ và lỗ hổng

3.2.2. Phân tích, đánh giá rủi ro

3.2.3. Xác thực và mã hóa

3.2.4. Đào tạo người dùng

3.4. Bảo mật cho mạng di động

3.4.1. Mạng di động

3.4.2. Định tuyến an toàn

3.4.3. Tạo và quản lý khóa

**Chương 4: Bảo mật cho điện toán đám mây**

4.1. Khái quát về điện toán đám mây

4.1.1 Kiến trúc của điện toán đám mây

4.1.2 Sơ bộ về bảo mật cho điện toán đám mây

4.2. Các vấn đề an toàn bảo mật cho điện toán đám mây

4.2.1. Ảo hóa

4.2.2. Dự phòng

4.2.3. Lưu trữ

4.2.4. Các hoạt động và mạng

4.3. Kiến trúc bảo mật trong điện toán đám mây

4.3.1. Các yêu cầu

4.3.2. Các mô hình bảo mật

4.3.3. Kiến trúc bảo mật cho điện toán đám mây

4.3.4. Lập kế hoạch các chiến lược đảm bảo an toàn các hoạt động

4.4. Bảo mật dữ liệu cho điện toán đám mây

4.4.1. Giới thiệu về bảo mật dữ liệu cho điện toán đám mây

4.4.2. Mã hóa dữ liệu

4.4.3. Phân loại dữ liệu và các chiến lược bảo mật

**6. Học liệu**

***6.1. Học liệu bắt buộc***

1. Roberta Bragg, Mark Rhodes-Ousley and Keith Strassberg, *Network Security: The Complete Reference*, McGraw-Hill Osborne Media, 2013.
2. Michael E. Whitman, Herbert J. Mattord, *Principles of information security, 4th edition, Course Technology*, Cengage Learning, 2012.

***6.2. Học liệu tham khảo***

1. John R. Vacca, *Network and System Security*, Elsevier Inc., 2010.
2. Vic J.R. Winkler, *Securing the Cloud:* *Cloud Computer Security Techniques and Tactics*, Syngress, 2011.
3. John Chirillo, *Hack attacks revealed: A complete reference with custom security hacking toolkit*, John Wiley & Sons, 2001.
4. Jie Wang, *Computer Network Security: Theory and Practice*, Springer, 2009.
5. Michael T. Simpson, Kent Backman, *Hands-On Ethical Hacking and Network Defense*, Delmar Cengage Learning, 2010.
6. Stuart McClure, Joel Scambray and George Kurtz, *Hacking Exposed 7: Network Security Secrets & Solutions*, McGraw-Hill Osborne Media, 2012.
7. William Stallings, *Cryptography and Network Security*, Prentice Hall, 2010.

**7. Hình thức tổ chức dạy học**

***7.1 Lịch trình chung:***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nội dung | Hình thức tổ chức dạy môn học | | | | | Tổng  cộng |
| Lên lớp | | | Thực hành | Tự học |
| Lý thuyết | BT lớn/Tiểu luận | Thảo luận |
| Nội dung 1: Điều khiển truy cập | 2 |  |  |  |  | 2 |
| Nội dung 2: Tường lửa | 2 |  |  |  |  | 2 |
| Nội dung 3: Công nghệ mạng riêng ảo | 2 |  |  |  |  | 2 |
| Nội dung 4: Hệ thống honeypot | 2 |  |  | 2 |  | 4 |
| Nội dung 5: Phòng chống DDoS | 2 |  |  |  |  | 2 |
| Nội dung 6: Các yêu cầu bảo mật thông tin trên đường truyền | 2 |  |  | 2 |  | 4 |
| Nội dung 7: Các giải pháp bảo mật thông tin dựa trên hệ thống mật mã lai và kỹ thuật giấu tin | 2 |  |  |  |  | 2 |
| Nội dung 8: Các giao thức bảo mật thông tin dựa trên IPSec, SSL/TLS, SSH | 2 | 2 |  |  |  | 4 |
| Nội dung 9: Các giao thức bảo mật thông tin dựa trên PGP, S-MIME, giao thức nặc danh | 2 |  |  | 2 |  | 4 |
| Nội dung 10: Bảo mật cho mạng cục bộ | 2 |  |  |  |  | 2 |
| Nội dung 11: Bảo mật cho mạng cục bộ không dây | 2 |  |  | 2 |  | 4 |
| Nội dung 12: Bảo mật cho mạng Intranet | 2 |  |  |  |  | 2 |
| Nội dung 13: Bảo mật cho mạng mạng di động | 2 | 2 |  |  |  | 4 |
| Nội dung 14: Điện toán đám mây và các vấn đề bảo mật cho điện toán đám mây | 2 |  | 2 |  |  | 4 |
| Nội dung 15: Kiến trúc bảo mật trong điện toán đám mây, Bảo mật dữ liệu cho điện toán đám mây | 2 |  |  |  | 1 | 3 |
| **Tổng cộng** | **30** | **4** | **2** | **8** | **1** | **45** |

***7.2. Lịch trình tổ chức dạy học cụ thể***

**Tuần 1, Nội dung: 1**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Điều khiển truy cập | * Đọc chương 5,6, phần 2, quyển 1 |  |

**Tuần 2, Nội dung: 2**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Tường lửa | * Đọc chương 11, phần 2, quyển 1 |  |

**Tuần 3, Nội dung: 3**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Công nghệ mạng riêng ảo | * Đọc chương 12, phần 2, quyển 1 |  |

**Tuần 4, Nội dung: 4**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Hệ thống honeypot | * Đọc mục 2, chương 7 quyển 2 |  |
| Thực hành | 2 | * Các công nghệ đảm bảo an toàn mạng | * Thực hiện theo hướng dẫn thực hành |  |

**Tuần 5, Nội dung: 5**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Phòng chống DDoS |  |  |

**Tuần 6, Nội dung: 6**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Các yêu cầu bảo mật thông tin trên đường truyền | * Đọc chương 8 quyển 2 |  |
| Thực hành | 2 | * Cài đặt và cấu hình VPN, iptables | * Thực hiện theo hướng dẫn thực hành |  |

**Tuần 7, Nội dung: 7**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Các giải pháp bảo mật thông tin dựa trên hệ thống mật mã lai và kỹ thuật giấu tin | * Đọc chương 8 quyển 2 |  |

**Tuần 8, Nội dung: 8**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Các giao thức bảo mật thông tin dựa trên IPSec, SSL/TLS, SSH | * Đọc chương 8 quyển 2 |  |
| Bài tập lớn/Tiểu luận | 2 | * Tìm hiểu các giao thức bảo mật thông tin | * Chuẩn bị bài tiểu luận theo nhóm và slides báo cáo được giao |  |

**Tuần 9, Nội dung: 9**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Các giao thức bảo mật thông tin dựa trên PGP, S-MIME, giao thức nặc danh | * Đọc chương 8 quyển 2 |  |
| Thực hành | 2 | * Ứng dụng bảo mật thông tin dựa trên mã hóa | * Ôn tập các kiến thức lý thuyết đã học và thực hiện theo hướng dẫn thực hành |  |

**Tuần 10, Nội dung: 10**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Bảo mật cho mạng cục bộ | * Đọc chương 9, quyển 3 |  |

**Tuần 11, Nội dung: 11**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Bảo mật cho mạng cục bộ không dây | * Đọc chương 11, quyển 3 |  |
| Thực hành | 2 | * Tấn công mạng không dây với mã hóa WPA | * Thực hiện theo hướng dẫn của bài thực hành |  |

**Tuần 12, Nội dung: 12**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Bảo mật cho mạng Intranet | * Đọc chương 10, quyển 3 |  |

**Tuần 13, Nội dung: 13**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Bảo mật cho mạng di động | * Đọc chương 12, quyển 3 |  |
| Bài tập lớn/Tiểu luận | 2 | * Tìm hiểu các giải pháp bảo mật cho mạng không dây | * Chuẩn bị bài tiểu luận theo nhóm và slides báo cáo được giao |  |

**Tuần 14, Nội dung: 14**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Điện toán đám mây và các vấn đề bảo mật cho điện toán đám mây | * Đọc chương 1,2,3 quyển 4 |  |
| Thảo luận | 2 | * Thảo luận về an toàn điện toán đám mây cho doanh nghiệp |  |  |

**Tuần 15, Nội dung: 15**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hình thức tổ chức dạy học** | **Thời gian**  *(tiết TC)* | **Nội dung chính** | **Yêu cầu đối với sinh viên** | **Ghi chú** |
| Lý thuyết | 2 | * Kiến trúc bảo mật trong điện toán đám mây, Bảo mật dữ liệu cho điện toán đám mây | * Đọc chương 4,5, quyển 4 |  |

**8. Chính sách đối với môn học và các yêu cầu khác của giảng viên:**

* Các bài tập/tiểu luận phải làm đúng hạn.
* Thiếu một điểm thành phần (bài tập, bài kiểm tra giữa kỳ), hoặc nghỉ quá 20% tổng số giờ của môn học, không được thi hết môn.
* Tham gia đầy đủ và hoàn thành các bài thực hành theo yêu cầu.

**9. Phương pháp, hình thức kiểm tra – đánh giá kết quả học tập môn học**

**9.1. Kiểm tra đánh giá định kỳ**

|  |  |  |
| --- | --- | --- |
| Hình thức kiểm tra *( Tham khảo ví dụ dưới đây)* | **Tỷ lệ đánh giá** | **Đặc điểm đánh giá** |
| - Tham gia học tập trên lớp (đi học đầy đủ, tích cực thảo luận) | 10 % | Cá nhân |
| - Các bài tập/tiểu luận và thảo luận trên lớp | 30% | Nhóm |
| - Kiểm tra giữa kỳ | 10% | Cá nhân |
| - Kiểm tra cuối kỳ | 50% | Cá nhân |

**9.2. Nội dung và Tiêu chí đánh giá các loại bài tập**

|  |  |
| --- | --- |
| **Các loại bài tập lớn/thảo luận** | **Tiêu chí đánh giá** |
| * Bài tập lớn/Tiểu luận | * Yêu cầu sinh viên nắm vững và trình bày được kiến thức căn bản của môn học * Tìm tài liệu, tổng hợp kiến thức và viết báo cáo theo yêu cầu của bài tập lớn được giao cho nhóm * Phân chia công việc và cộng tác theo nhóm * Chuẩn bị slides và trình bày trước lớp |
| * Thảo luận | * Tìm hiểu theo yêu cầu của nội dung thảo luận và trả lời câu hỏi trực tiếp |
| * Kiểm tra giữa kỳ, cuối kỳ | * Nắm vững kiến thức môn học * Trả lời đúng các câu hỏi và bài tập |

|  |  |  |
| --- | --- | --- |
| **Duyệt**  **PGS.TS. Từ Minh Phương** | **Chủ nhiệm bộ môn**  **TS. Hoàng Xuân Dậu** | **Giảng viên**  *(Chủ trì biên soạn đề cương)*  **Nguyễn Ngọc Điệp** |