| **Trường Đại học GTVT**  Khoa: Công nghệ thông tin | **University of Transport and Communications**  Faculty of Information Technology |
| --- | --- |

ĐỀ CƯƠNG HỌC PHẦN

**AN NINH MẠNG**

Network Security

**1. Thông tin tổng quát** *(general information)*

| * Tên học phần: | **An ninh mạng** |
| --- | --- |
| * Mã số học phần: | IT1.233.3 |
| * Ngành/Chuyên ngành đào tạo | Công nghệ Thông tin |
| * Thuộc khối kiến thức/ kỹ năng:   ◻ Kiến thức cơ bản 🗹 Kiến thức chuyên ngành  ◻ Kiến thức cơ sở ngành ◻ Kiến thức ngành | |
| * Số tín chỉ: | 3 |
| + Số tiết lý thuyết: | 30 |
| + BTL | 0 |
| + Số tiết Thảo luận, Bài tập: | 15 |
| + Số tiết, thực hành, thí nghiệm: | 15 |
| + Số tiết tự học: | 90 |
| * Học phần tiên quyết: |  |
| * Học phần học trước: |  |
| * Học phần song hành: |  |
| * Yêu cầu khác đối với học phần: | Phòng học có máy chiếu/Bảng thông minh |

*(Số tiết phân bổ cho lý thuyết, thảo luận, bài tập, bài tập lớn, thực hành, thí nghiệm điền và bôi đậm tùy theo học phần cụ thể)*

**2. Mô tả học phần***(course descriptions)*

Học phần cung cấp cho sinh viên các kiến thức về:

* Nguyên lý của các kỹ thuật an ninh mạng;
* Kiến thức về các kỹ thuật, công cụ phân tích các lỗ hổng trong hệ thống mạng;
* Các kỹ thuật bảo mật hạ tầng mạng như Firewall, IDS/IPS;
* Các kỹ thuật trong bảo mật ứng dụng: remote access security, web security, Email security, buffer overflow.

**3. Nguồn học liệu** *(learning resources: course books, reference books, and softwares)*

*(Các giáo trình, tài liệu tham khảo, các phần mềm, không quá 5 cuốn)*

***Giáo trình:*** Giáo trình An Ninh Mạng của khoa CNTT – ĐH SPKT Tp.HCM

***Tài liệu khác:***

[1]. Steve Manzuik, Ken Pfeil, Andre, ”Network Security Assessment”, Syngress, 2007.

[2]. Nei Daswani, Christoph Kern, Anita Kes avan, “Foundation of Security”, Apress, 2007.

Ciampa, Ph.D, Cengage Learning 2015

**4. Mục tiêu học phần** *(course goals)*

*(Thể hiện kiến thức, kỹ năng mà môn học cung cấp và sự liên quan với CĐR của CTĐT được phân nhiệm cho môn học)*

| **Mục tiêu (G.x) [1]** | **Mô tả mục tiêu [2]** | **CĐR liên quan của CTĐT [3]** |
| --- | --- | --- |
| **G.1** | **Hiểu** được các nguy cơ mất an ninh an toàn thông tin và các giải pháp phòng chống, **vận dụng** được các nguyên lý, công cụ để **phân tích, lựa chọn** các giải pháp triển khai đảm bảo an ninh trên hạ tầng mạng máy tính trong thực tế. | CĐR 6,7 (1.3) |
| **G.2** | **Thực hiện** tốt đạo đức nghề nghiệp, **chủ động**, **kiên trì** và **sáng tạo** trong **lựa chọn** các giải pháp triển khai đảm bảo an ninh hạ tầng mạng, vận hành hệ thống an toàn | CĐR 10, 11, 12, 15 (2.4, 2.5, 4.6) |

*[1]: Ký hiệu mục tiêu của học phần. [2]: Mô tả mục tiêu. [3]: Ký hiệu CĐR của CTĐT và chuẩn đầu ra CDIO tương ứng.*

**5. Chuẩn đầu ra học phần** *(course learning outcomes)*

*(CĐR chi tiết hơn mục tiêu, mô tả sau khi học xong* ***sinh viên sẽ đạt được gì*** *về kiến thức, kỹ năng và thái độ)*

| **CĐR HP cấp độ 3**  **(G.x.y) [1]** | **Mô tả CĐR học phần[2]** | **Mức độ chung HP theo Bloom [3]** |
| --- | --- | --- |
| **G.1.1** | **Hiểu** các nguy cơ mất an ninh, an toàn thông tin (BL2) | 1.3 – TUA4 |
| **G.1.2** | **Vận dụng** được các nguyên lý, công cụ để **phân tích, lựa chọn** các giải pháp triển khai đảm bảo an ninh trên hạ tầng mạng máy tính trong thực tế(BL4) |
| **G.2.1** | **Thực hiện** tốt đạo đức nghề nghiệp (BL3) | 2.5 – TUA3 |
| **G.2.2** | **Chủ động, Kiên trì** và **sáng tạo** lựa chọn các giải pháp đảm bảo an ninh hạ tầng mạng, vận hành hệ thống an toàn (BL4) | 2.4 – TUA 4 4.6 – TUA 4 |

*[1]: Ký hiệu CĐR của học phần. [2]: Mô tả CĐR học phần, bao gồm các động từ chủ động theo Bloom’s Toxonomi, khuyến khích viết tích hợp kỹ năng và kiến thức [3]: Mức độ năng lực mà HP đảm trách theo hoạt động TUA.*

**6. Đánh giá học phần** *(course assessment)*

*(các thành phần, các bài đánh giá, các tiêu chí đánh giá, chuẩn đánh giá, và tỷ lệ đánh giá, thể hiện sự liên quan với các CĐR của học phần)*

| **Thành phần đánh giá [1]** | **Hình thức đánh giá (A.x.y) [2]** | **CĐR học phần (G.x.y) [3]** | **Tiêu chí**  **đánh giá [4]** | **Tỷ lệ (%)[5]** |
| --- | --- | --- | --- | --- |
| A1. Đánh giá quá trình | A.1.1 Bài tập, điểm danh | G.1.1, 1.2 | **- Vận dụng** các giải pháp đảm bảo an ninh, an toàn hạ tầng mạng (BL3)  - Chuyên cần | 10 |
| A.1.2 Bài kiểm tra giữa kỳ | G.1.1, 1.2 | - **Vận dụng** các giải pháp đảm bảo an ninh, an toàn hạ tầng mạng (BL3)(BL3) | 10 |
| A.1.3 Luyện tập CTF | G.1.1, 1.2, 2.1, 2.2 | - Thực hiện tốt đạo đức nghề nghiệp (BL3)  - Chủ động, kiên trì, sáng tạo lựa chọn giải pháp triển khai đảm bảo an ninh mạng, vận hành hệ thống an toàn (BL4) | 20 |
| A2. Đánh giá kết thúc học phần ít nhất 50%) | A.2.1 Bài thi cuối kỳ dưới dạng thi thực hành | G.1.1, 1.2, 2.1, 2.2 | Phân tích, lựa chọn giải pháp đảm bảo an ninh, an toàn hạ tầng mạng (BL4) | 60 |

*[1]: Các thành phần đánh giá của học phần. [2]: Các bài đánh giá. [3]: Các CĐR được đánh giá. [4]: Tiêu chí đánh giá. [5]: Tỷ lệ điểm của các bài đánh giá trong tổng điểm học phần.*

**7. Khung kế hoạch giảng dạy***:*

*(Các nội dung giảng dạy theo chương mục, thể hiện sự liên quan với các CĐR của học phần và các bài đánh giá của học phần. Việc giảng dạy kỹ năng trong môn học có thể dạy lý thuyết và áp dụng hoặc có thể học qua trải nghiệm)*.

| **TT** | **Nội dung [2]** | **Số tiết** | **CĐR HP [3]** | **Hoạt động dạy và học [4]** | **Đánh giá [5]** |
| --- | --- | --- | --- | --- | --- |
| **1** | **Chương 1: Tổng quan về an ninh mạng**  1.1. An ninh mạng là gì?  1.2. Mục tiêu của an ninh mạng  1.3. Các mô hình an ninh mạng  1.4. Các chính sách an ninh mạng | 3 LT | G.1.1 G.1.2 |  | A.1.1 |
| **2** | **Chương 2: Các thách thức an ninh với mạng máy tính**  2.1. Các mối đe dọa với mạng máy tính  2.2. Động cơ của các mối đe dọa an ninh mạng  2.3. Khả năng tổn thương của mạng máy tính  2.4. Đối phó các mối đe dọa an ninh mạng | 6 LT  3 BT  3 TH | G.1.1  G.1.2  G.2.1  G.2.2 |  | A.1.1  A.1.2  A.2.1  A.2.2 |
| **3** | **Chương 3: Tấn công mạng máy tính**  3.1. Định nghĩa, khái niệm, phân loại tấn công  3.2. Các mô hình thực hiện tấn công  3.3. Tội phạm mạng và tin tặc  3.4. Một số công cụ tấn công mạng  3.5. Các phương pháp phòng chống tấn công | 6 LT  3 BT  6 TH | G.1.1  G.1.2  G.2.1  G.2.2 |  | A.1.1  A.1.2  A.2.1  A.2.2 |
| **4** | **Chương 4: Tường lửa**  4.1 Định nghĩa  4.2. Các kiểu tường lửa  4.3. Một số mô hình tường lửa  4.4. Đánh giá tường lửa | 6 LT  3 BT  3 TH | G.1.1  G.1.2  G.2.1  G.2.2 |  | A.1.1  A.1.2  A.2.1  A.2.2 |
| **5** | **Chương 5: Hệ thống phát hiện và phòng chống xâm nhập**  5.1. Định nghĩa  5.2. Hệ thống phát hiện xâm nhập (IDS)  5.3. Hệ phòng chống xâm nhập (IPS)  5.4. Xây dựng các mô hình thực tế | 6 LT  3 BT  3 TH | G.1.1  G.1.2  G.2.1  G.2.2 |  | A.1.1  A.1.2  A.2.1  A.2.2 |
| **6** | **Chương 6: An ninh các thiết bị và mạng không dây**  6.1. Giới thiệu  6.2. An ninh trong mạng cục bộ không dây  6.3. Các giao thức WEP, WPA, WPA2  6.4. Các giải pháp xác thực trong mạng cục bộ không dây  6.5. Các mô hình triển khai an ninh trong mạng cục bộ không dây | 3 LT  3 BT | G.1.1  G.1.2 |  | A.1.1  A.1.2 |

*[1]: Thông tin về tuần/ buổi học. [2]: Liệt kê nội dung giảng dạy theo chương, mục. [3]: Liệt kê CĐR liên quan của học phần (ghi ký hiệu Gx.y). [4]: Mô tả chung các hoạt động dạy và học. [5]: Liệt kê các bài đánh giá liên quan (ghi ký hiệu Ax.y).*

**8. Quy định của học phần** *(course requirements and expectations)*

*(các quy định của học phần (nếu có), thí dụ: sinh viên không nộp bài tập và báo cáo đúng thời hạn, được coi như không nộp bài; sinh viên vắng 2 buổi thực hành trở lên, không được phép dự thi cuối kỳ…)*

**9. Phụ trách học phần**

- Bộ môn: Mạng và Các Hệ thống thông tin

- Địa chỉ và email liên hệ: P.308-A9, email: bmmht@utc.edu.vn

*Hà Nội, ngày 30 tháng 08 năm 2022*

**Trưởng Khoa Trưởng Bộ môn**

**Hoàng Văn Thông Nguyễn Quốc Tuấn**