BỘ CÔNG THƯƠNG
**TRƯỜNG ĐẠI HỌC SAO ĐỎ**
*****

# ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN
# AN TOÀN VÀ AN NINH MẠNG

**Số tín chỉ: 03**
**Trình độ đào tạo: Đại học**
**Ngành đào tạo: Công nghệ thông tin**

**Năm 2018**

**TRƯỜNG ĐẠI HỌC SAO ĐỎ**
**KHOA: ĐIỆN TỬ - TIN HỌC**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập - Tự do - Hạnh phúc**

# ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

**Trình độ đào tạo: Đại học**

**Ngành đào tạo: Công nghệ thông tin**

**1. Tên học phần:** An toàn và an ninh mạng

**2. Mã học phần:** CNTT 201

**3. Số tín chỉ:** 3 (2, 1)

**4. Trình độ cho sinh viên:** Năm thứ Tư

**5. Phân bổ thời gian**

- Lên lớp: 30 tiết lý thuyết, 30 tiết thực hành
- Tự học: 75 giờ

**6. Điều kiện tiên quyết**

**7. Giảng viên**

| STT | Học hàm, học vị, họ tên | Số điện thoại | Email |
|---|---|---|---|
| 1 | ThS. Nguyễn Thị Ánh Tuyết | 0972384332 | anhtuyet13381@gmail.com |
| 2 | ThS. Vũ Bảo Tạo | 0384305659 | taovb2006@gmail.com |

**8. Mô tả nội dung của học phần**

Học phần An toàn và an ninh mạng gồm các nội dung khái lược về an toàn và thông tin dữ liệu, những nội dung cơ bản trong an ninh mạng; lỗ hổng bảo mật và các loại tấn công phổ biến; an ninh mạng mức giao vận; an ninh thư điện tử; an toàn và an ninh mạng máy tính; một số kỹ thuật phát hiện xâm nhập và phòng thủ trong an ninh mạng. Thông qua học phần giúp sinh viên ghi nhớ, phân loại, thực hiện cũng như đánh giá mức độ an toàn của hệ thống mạng.

**9. Mục tiêu và chuẩn đầu ra học phần**

***9.1. Mục tiêu***

Mục tiêu học phần thỏa mãn mục tiêu của chương trình đào tạo:

| Mục tiêu | Mô tả | Mức độ theo thang đo Bloom | Phân bổ mục tiêu học phần trong CTĐT |
|---|---|---|---|
| **MT1** | **Kiến thức** | | |
| MT1.1 | Trình bày được tầm quan trọng an toàn và an ninh mạng trong vấn đề quản lý dữ liệu, an toàn khi truyền dữ liệu trong môi trường mạng máy tính. | 2 | [1.2.1.2a] |
| MT1.2 | Hiểu được các chiến lược an toàn hệ thống, các phương pháp an toàn mạng, một số lỗ hổng và cách thức tấn công mạng của | 2 | |

| Mục tiêu | Mô tả | Mức độ theo thang đo Bloom | Phân bổ mục tiêu học phần trong CTĐT |
|---|---|---|---|
| | hacker, một số kỹ thuật phát hiện xâm nhập và phòng thủ trong an ninh mạng. | | |
| **MT2** | **Kỹ năng** | | |
| MT2.1 | Có kỹ năng phòng chống xâm nhập trong mạng máy tính, làm việc độc lập, làm việc nhóm, tư duy, áp dụng các kỹ thuật để phân tích phương án và triển khai phát hiện xâm nhập và phòng thủ trong an ninh mạng. | 3 | [1.2.2.1] |
| MT2.2 | Có khả năng thích ứng với sự thay đổi của công nghệ mạng máy tính nói riêng và các công nghệ khác nói chung. | 3 | |
| **MT3** | **Mức tự chủ và trách nhiệm** | | |
| MT3.1 | Có năng lực định hướng, lập kế hoạch, điều phối, quản lý, hướng dẫn, giám sát, đánh giá và đưa ra kết luận các công việc thuộc chuyên môn nghề nghiệp. | 4 | [1.2.3.2] |
| MT3.2 | Có thái độ tích cực trong học tập và chịu trách nhiệm với các nhiệm vụ được phân công. | 4 | |

### *9.2. Chuẩn đầu ra của học phần*

Sự phù hợp của chuẩn đầu ra học phần với chuẩn đầu ra của chương trình đào tạo:

| CĐR học phần | Mô tả | Thang đo Bloom | Phân bổ CĐR học phần trong CTĐT |
|---|---|---|---|
| **CĐR1** | **Kiến thức** | | |
| CĐR1.1 | Trình bày và phân tích được sự an toàn và an ninh mạng trong việc quản lý dữ liệu, truyền dữ liệu trong môi trường mạng máy tính. | 2 | [2.1.6] |
| CĐR1.2 | Phân biệt được các phương pháp an toàn mạng, một số lỗ hổng và cách thức tấn công mạng của hacker. | 4 | |
| CĐR1.3 | Trình bày được một số kỹ thuật phát hiện xâm nhập và phòng thủ trong an ninh mạng. | 2 | |
| CĐR1.4 | Tổ chức và kiểm tra an toàn và an ninh mạng trong các hệ thống mạng. | 2 | |
| **CĐR2** | **Kỹ năng** | | |

| CĐR học phần | Mô tả | Thang đo Bloom | Phân bổ CĐR học phần trong CTĐT |
|---|---|---|---|
| CĐR2.1 | Kiểm tra và triển khai được phương án phòng chống xâm nhập trong mạng máy tính, làm việc độc lập, làm việc nhóm, tư duy, áp dụng các kỹ thuật để phát hiện xâm nhập và phòng thủ trong an ninh mạng. | 3 | [2.2.6] |
| CĐR2.2 | Có khả năng tổ chức, triển khai hệ thống mạng máy tính nói chung. | 3 | |
| **CĐR3** | **Mức tự chủ và trách nhiệm** | | |
| CĐR3.1 | Có khả năng phân biệt, tổ chức với những nhiệm vụ được giao. | 4 | [2.3.1] |
| CĐR3.2 | Có năng lực hướng dẫn, giám sát người khác cùng thực hiện nhiệm vụ chuyên môn. | 4 | [2.3.2] |

**10. Ma trận liên kết nội dung với chuẩn đầu ra học phần**

| Chương | Nội dung học phần | Chuẩn đầu ra của học phần | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | CĐR1 | | | | CĐR2 | | CĐR3 | |
| | | CĐR 1.1 | CĐR 1.2 | CĐR 1.3 | CĐR 1.4 | CĐR 2.1 | CĐR 2.2 | CĐR 3.1 | CĐR 3.2 |
| 1 | **Chương I. An toàn và thông tin dữ liệu**<br>1.1. Tổng quan an toàn thông tin dữ liệu<br>1.2. Đánh giá độ an toàn bảo vệ thông tin dữ liệu<br>1.3. Các chiến lược an toàn hệ thống<br>1.4. Các mức bảo vệ trên mạng<br>1.5. An toàn thông tin bằng mật mã<br>1.6. Vai trò của hệ mật mã<br>1.7. Phân loại hệ mật mã<br>1.8. Tiêu chuẩn đánh giá hệ mật mã<br>1.9. Các nguy cơ đe dọa | x | x | x | x | | | | |
| 2 | **Chương II. Các vấn đề trong an ninh mạng**<br>2.1. Mục tiêu của an ninh mạng<br>2.2. Tấn công mạng<br>2.3. Lỗ hổng bảo mật và các loại tấn công phổ biến<br>2.4. Các lĩnh vực trong tấn công mạng | x | | x | x | | | | |
| 3 | **Chương III. An ninh mức giao vận**<br>3.1. Vấn đề an ninh website<br>3.2. Giao thức secure sockets layer<br>3.3. Chuẩn transport layer security<br>3.4. Giao thức secure shell | x | | x | x | | | | |
| 4 | **Chương IV. An ninh thư điện tử**<br>4.1. Chương trình Pretty Good Privacy | x | x | x | x | | | | |

| Chương | Nội dung học phần | Chuẩn đầu ra của học phần | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | CĐR1 | | | | CĐR2 | | CĐR3 | |
| | | CĐR 1.1 | CĐR 1.2 | CĐR 1.3 | CĐR 1.4 | CĐR 2.1 | CĐR 2.2 | CĐR 3.1 | CĐR 3.2 |
| | 4.2. Chuẩn Multipurpose Internet Mail Extensions<br>4.3. Giao thức Hypertext Transfer Protocol Secure<br>4.4. Giao thức Secure Shell | | | | | | | | |
| 5 | **Chương V. An ninh và an toàn mạng máy tính**<br>**5.1. Khái niệm lỗ hổng**<br>5.2. Các lỗ hổng bảo mật của hệ điều hành<br>5.3. Các lỗ hổng bảo mật của mạng máy tính<br>5.4. Một số lỗ hổng do người dùng vô tình gây ra<br>5.5. Hackers và hậu quả hacker gây ra<br>5.6. Tấn công mạng qua lỗ hổng | x | x | x | x | x | x | x | x |
| 6 | **Chương VI. Một số kỹ thuật phát hiện xâm nhập và phòng thủ trong an ninh mạng**<br>6.1. Một số kỹ thuật phòng thủ<br>6.2. Hệ thống phát hiện xâm nhập IDS<br>6.3. Phát hiện dấu hiệu không bình thường<br>6.4. Các mẫu hành vi thông thường, phát hiện bất thường<br>6.5. Một số kỹ thuật xử lý dữ liệu sử dụng trong các hệ thống phát hiện xâm nhập | x | x | x | | x | | x | x |

## 11. Đánh giá học phần

### *11.1. Kiểm tra và đánh giá trình độ*

| Chuẩn đầu ra | Mức độ thành thạo được đánh giá bởi |
|---|---|
| CĐR1 | Kiểm tra thường xuyên, kiểm tra thực hiện nhiệm vụ về nhà, kiểm tra giữa học phần. |
| CĐR2 | Kết quả thảo luận trên lớp, thực hiện nhiệm vụ về nhà, bài tiểu luận kiểm tra giữa học phần. |
| CĐR3 | Kiểm tra thường xuyên, kết quả thực hiện nhiệm vụ của cá nhân và theo nhóm, bài báo cáo kết thúc học phần. |

***11.2. Cách tính điểm học phần:*** Tính theo thang điểm 10 sau đó chuyển thành thang điểm chữ và thang điểm 4

| STT | Điểm thành phần | Quy định | Trọng số | Ghi chú |
|---|---|---|---|---|
| 1 | Điểm thường xuyên, đánh giá nhận thức, thái độ thảo luận, chuyên cần của sinh viên. | 01 điểm | 20% | Điểm trung bình của các lần đánh giá |
| 2 | Kiểm tra giữa học phần | 01 điểm | 30% | |
| 3 | Thi kết thúc học phần | 01 điểm | 50% | |

### *11.3. Phương pháp đánh giá*

- Đánh giá chuyên cần: Phát vấn, tỷ lệ hiện diện trên lớp, làm bài tập.
- Kiểm tra giữa học phần: Báo cáo sơ bộ bài tập lớn.
- Thi kết thúc học phần: Báo cáo bài tập lớn.

**12. Phương pháp dạy và học**

- Lý thuyết: Thuyết trình, thảo luận nhóm, trực quan, đàm thoại, nêu vấn đề.
- Thực hành: Hướng dẫn.

**13. Yêu cầu học phần**

- Yêu cầu về thái độ học tập, chuyên cần: Hoàn thành bài tập và nhiệm vụ giảng viên giao, tham dự ít nhất 80% thời lượng học phần; ghi chép và tích cực thảo luận, xây dựng bài trên lớp.
- Yêu cầu về nghiên cứu tài liệu: Nghiên cứu tài liệu trước khi đến lớp, đọc thêm các tài liệu liên quan được giảng viên giới thiệu.
- Yêu cầu về kiểm tra giữa học phần và thi kết thúc học phần: Sinh viên thực hiện theo quy chế.

**14. Tài liệu phục vụ học phần**

***- Tài liệu bắt buộc:***

[1]. Trường Đại học Sao Đỏ (2018), *Giáo trình An toàn và an ninh mạng*.

***- Tài liệu tham khảo:***

[2]. Trường Đại học Sao Đỏ (2018), *Giáo trình Bảo mật thông tin*.

**15. Nội dung chi tiết học phần**

| Tuần | Nội dung | Lý thuyết | Thực hành | Tài liệu đọc trước | Nhiệm vụ của sinh viên |
|---|---|---|---|---|---|
| 1. | **Chương I. An toàn và thông tin dữ liệu**<br>**Mục tiêu chương: I**<br>Trình bày được vấn đề an toàn thông tin dữ liệu, đánh giá độ an toàn bảo vệ thông tin dữ liệu, các chiến lược an toàn hệ thống, các mức bảo vệ trên mạng, an toàn thông tin bằng mật mã, vai trò, phân loại và tiêu chuẩn đánh giá hệ mật mã.<br>**Nội dung cụ thể:**<br>1.1. Tổng quan an toàn thông tin dữ liệu | 2 | 2 | [1] | - Nghiên cứu mục tiêu, chương trình, kế hoạch dạy học học phần.<br>- Nghiên cứu tài liệu *[1]* - chương 1 mục 1.1 - 1.4.<br>- Làm bài thực hành số 01: Phân tích điểm yếu trong các hệ điều hành windows và hệ hiều hành mã nguồn mở kali linux hoặc ubuntu. |

| Tuần | Nội dung | Lý thuyết | Thực hành | Tài liệu đọc trước | Nhiệm vụ của sinh viên |
|---|---|---|---|---|---|
| | 1.2. Đánh giá độ an toàn bảo vệ thông tin dữ liệu<br>1.3. Các chiến lược an toàn hệ thống<br>1.4. Các mức bảo vệ trên mạng<br>Bài thực hành số 01 | | | | |
| 2. | 1.5. An toàn thông tin bằng mật mã<br>1.6. Vai trò của hệ mật mã<br>1.7. Phân loại hệ mật mã<br>1.8. Tiêu chuẩn đánh giá hệ mật mã<br>1.9. Các nguy cơ đe dọa<br>Bài thực hành số 02 | 2 | 2 | [1], [2] | - Nghiên cứu tài liệu *[1]*- chương 1 mục 1.5 - 1.9.<br>- Đọc tài liệu tham khảo tài liệu *[2] Chương 1.*<br>- Làm bài thực hành số 02: Phân tích và so sánh điểm yếu trong các hệ điều hành windows và hệ hiều hành mã nguồn mở kali linux hoặc ubuntu. |
| 3. | **Chương II. Các vấn đề trong an ninh mạng**<br>**Mục tiêu chương: II**<br>Trình bày được mục tiêu của an ninh mạng, tấn công mạng, lỗ hổng bảo mật và các loại tấn công phổ biến, các lĩnh vực tấn công mạng.<br>**Nội dung cụ thể:**<br>2.1. Mục tiêu của an ninh mạng<br>2.2. Tấn công mạng<br>Bài thực hành số 03 | 2 | 2 | [1], [2] | - Nghiên cứu tài liệu *[1]*- chương 2 mục 2.1, 2.2.<br>- Đọc tài liệu tham khảo tài liệu *[2] Chương 2.*<br>- Làm bài thực hành số 03: Cài đặt hệ điều hành kali linux hoặc ubuntu. |
| 4. | 2.3. Lỗ hổng bảo mật và các loại tấn công phổ biến<br>2.4. Các lĩnh vực trong tấn công mạng<br>Bài thực hành số 04 | 2 | 2 | [1], [2] | - Nghiên cứu tài liệu [1]- chương 2 mục 2.3, 2.4.<br>- Đọc tài liệu tham khảo tài liệu *[2] Chương 2.* |

| Tuần | Nội dung | Lý thuyết | Thực hành | Tài liệu đọc trước | Nhiệm vụ của sinh viên |
|---|---|---|---|---|---|
| | | | | | - Làm bài thực hành số 04: Cài đặt hệ điều hành kali linux hoặc ubuntu. |
| 5. | **Chương III. An ninh mức giao vận**<br>**Mục tiêu chương: III**<br>Trình bày được vấn đề an ninh website, các giao thức SSL, TLS, SSH.<br>**Nội dung cụ thể:**<br>3.1. Vấn đề an ninh website<br>3.2. Giao thức secure sockets layer<br>Bài thực hành số 05 | 2 | 2 | [1], [2] | - Nghiên cứu tài liệu *[1]*- chương 3 mục 3.1, 3.2.<br>- Làm bài thực hành số 05: Các công cụ tấn công giao thức DNS: ettercap và scapy. Các công cụ do thám hệ thống: nmap và wireshark. |
| 6. | 3.3. Chuẩn transport layer security<br>3.4. Giao thức secure shell<br>Bài thực hành số 06 | 2 | 2 | [1], [2] | - Nghiên cứu tài liệu *[1]*- chương 3 mục 3.3, 3.4.<br>- Các công cụ do thám hệ thống: Nmap và Wireshark;<br>- Làm bài thực hành số 06: Các công cụ tấn công giao thức DNS: Ettercap và Scapy. |
| 7. | **Chương IV. An ninh thư điện tử**<br>**Mục tiêu chương: IV**<br>Trình bày được chương trình PGP, chuẩn MIME, giao thức HTTPs, giao thức SSH.<br>**Nội dung cụ thể:**<br>4.1. Chương trình pretty good privacy<br>4.2. Chuẩn multipurpose internet mail extensions | 1<br>1 KT | 2 | [1], [2] | - Nghiên cứu tài liệu *[1]*- chương 4 mục 4.1, 4.2.<br>Phân tích và cài đặt:<br>- Làm bài thực hành số 07: Các công cụ tấn công giao thức DNS: Ettercap và Scapy. Các công cụ do thám hệ thống: Nmap và Wireshark.<br>- Chuẩn bị nội dung báo cáo giữa kỳ. |

| Tuần | Nội dung | Lý thuyết | Thực hành | Tài liệu đọc trước | Nhiệm vụ của sinh viên |
|---|---|---|---|---|---|
| | Bài thực hành số 07 | | | | |
| 8. | 4.3. Giao thức hypertext transfer protocol secure<br>4.4. Giao thức secure shell<br>**Kiểm tra giữa học phần** | 2 | 2 | [1], [2] | - Nghiên cứu tài liệu *[1]*- chương 3 mục 4.3, 4.4.<br>- Làm bài thực hành số 08: Các công cụ do thám hệ thống: nmap và wireshark. Các công cụ tấn công giao thức DNS: ettercap và scapy. |
| 9. | **Chương V. An ninh và an toàn mạng máy tính**<br>**Mục tiêu chương: V**<br>Trình bày được khái niệm lỗ hổng, các lỗ hổng bảo mật của mạng máy tính, một số lỗ hổng do người dùng vô tình gây ra, hackers và hậu quả hacker gây ra, Tấn công mạng qua lỗ hổng.<br>**Nội dung cụ thể:**<br>**5.1. Khái niệm lỗ hổng**<br>5.2. Các lỗ hổng bảo mật của hệ điều hành<br>5.3. Các lỗ hổng bảo mật của mạng máy tính<br>**Bài thực hành số 09** | 2 | 2 | [1], [2] | - Nghiên cứu tài liệu *[1]*- chương 5 mục 5.1 – 5.3.<br>- Đọc tài liệu tham khảo tài liệu *[2] Chương 3.*<br>- Làm bài thực hành số 09: Phân tích và so sánh các Tool khác trong thực tế. |
| 10. | 5.4. Một số lỗ hổng do người dùng vô tình gây ra<br>5.5. Hackers và hậu quả hacker gây ra<br>Bài thực hành số 10 | 2 | 2 | [1], [2] | - Nghiên cứu tài liệu *[1]*- chương 5 mục 5.4, 5.5.<br>- Làm bài thực hành số 10: Phân tích và so sánh các Tool khác trong thực tế. |
| 11. | 5.6. Tấn công mạng qua lỗ hổng | 2 | 2 | [1], [2] | - Nghiên cứu tài liệu *[1]*- chương 5 mục 5.6. |

| Tuần | Nội dung | Lý thuyết | Thực hành | Tài liệu đọc trước | Nhiệm vụ của sinh viên |
|---|---|---|---|---|---|
| | Bài thực hành số 11 | | | | - Làm bài thực hành số 11: Xây dựng kịch bản thử nghiệm do thám hệ thống mạng. |
| 12. | **Chương VI. Một số kỹ thuật phát hiện xâm nhập và phòng thủ trong an ninh mạng**<br>**Mục tiêu chương: V**<br>Trình bày được một số kỹ thuật phòng thủ, Hệ thống phát hiện xâm nhập IDS, Phát hiện dấu hiệu không bình thường, Các mẫu hành vi thông thường, phát hiện bất thường, Một số kỹ thuật xử lý dữ liệu sử dụng trong các hệ thống phát hiện xâm nhập.<br>**Nội dung cụ thể:**<br>6.1. Một số kỹ thuật phòng thủ<br>Bài thực hành số 12 | 2 | 2 | [1], [2] | - Nghiên cứu tài liệu *[1]*- chương 6 mục 6.1.<br>- Làm bài thực hành số 12: Xây dựng kịch bản thử nghiệm do thám hệ thống mạng. |
| 13. | 6.2. Hệ thống phát hiện xâm nhập IDS<br>Bài thực hành số 13 | 2 | 2 | [1], [2] | - Nghiên cứu tài liệu *[1]*- chương 6 mục 6.2.<br>- Làm bài thực hành số 13: Xây dựng kịch bản thử nghiệm do thám hệ thống mạng. |
| 14. | 6.3. Phát hiện dấu hiệu không bình thường<br>6.4. Các mẫu hành vi thông thường, phát hiện bất thường<br>Bài thực hành số 14 | 2 | 2 | [1], [2] | - Nghiên cứu tài liệu *[1]*- chương 6 mục 6.3, 6.4.<br>- Làm bài thực hành số 14: Xây dựng kịch bản thử nghiệm do thám hệ thống mạng. |
| 15. | 6.5. Một số kỹ thuật xử lý dữ liệu sử dụng trong các hệ thống phát hiện xâm nhập<br>Bài thực hành số 15 | 2 | 2 | [1], [2] | - Nghiên cứu tài liệu *[1]*- chương 6 mục 6.5. |

| Tuần | Nội dung | Lý thuyết | Thực hành | Tài liệu đọc trước | Nhiệm vụ của sinh viên |
|---|---|---|---|---|---|
| | | | | | - Làm bài thực hành số 15: Kết quả thực hiện do thám và thử nghiệm tấn công hệ thống. |

*Hải Dương, ngày 14 tháng 8 năm 2018*

| KT.HIỆU TRƯỞNG<br>PHÓ HIỆU TRƯỞNG | KT.TRƯỞNG KHOA<br>PHÓ TRƯỞNG KHOA | TRƯỞNG BỘ MÔN |
|---|---|---|
| TS. Nguyễn Thị Kim Nguyên | Trần Duy Khánh | Phạm Văn Kiên |