|  |  |
| --- | --- |
| BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC QUANG TRUNG** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập – Tự do – Hạnh phúc** |

**ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN**

**1. Thông tin chung về học phần**

- Tên học phần: Chuyên đề 2

- Tiếng Việt: Thu thập và phân tích thông tin mạng.

- Tiếng Anh: Collect and analyze network information.

- Mã học phần: TH11.5.06

* Số tín chỉ: 04 (LT:2+TH:2; TC 90 tiết)
* Chương trình đào tạo trình độ: Đại học
* Ngành học: Kỹ thuật mạng máy tính.
* Hình thức đào tạo: Chính quy
* Học phần: Tự chọn 🗹 Bắt buộc
* Các học phần tiên quyết (nếu có): Học sau các môn cơ sở ngành, các môn mạng máy tính, an toàn mạng, an ninh mạng.
* Giờ tín chỉ đối với các hoạt động:
  + Nghe giảng lý thuyết: 30 tiết
  + Thực hành: 60 tiết (Thực hành tại cơ sở).
  + Đồ án: 0 tiết.
  + Kiểm tra: 2 tiết (Báo cáo trước lớp).
* Đối tượng học tập: Sinh viên ngành Công nghệ thông tin (Chuyên ngành: Kỹ thuật mạng máy tính).
* Khoa phụ trách học phần: Khoa KHMT&CNTT, trường Đại học Quang Trung

**2. Thông tin về giảng viên giảng dạy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TT** | **Họ và tên** | **Học hàm, học vị** | **Email, điện thoại** | **Nội dung giảng dạy** |
| 01 | Lương Tiến Vinh | Thạc sĩ | [ltvinh@qtu.edu.vn](mailto:ltvinh@qtu.edu.vn)  0359 393 468 | Thu thập và phân tích thông tin mạng |

**3. Mục tiêu học phần**

***3.1. Mục tiêu chung:***

Môn học này cung cấp kiến thức về cách thu thập và phân tích thông tin mạng dựa trên các nguyên lý của các kỹ thuật an ninh mạng; kiến thức về các kỹ thuật sử dụng 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.

***3.2. Mục tiêu cụ thể***

| **TT** | **Mục tiêu cụ thể** |
| --- | --- |
| **1. Kiến thức** | |
| MTHP1 | Xác định các điểm yếu bảo mật trong hệ thống. Đưa ra những khuyến nghị và phương pháp khắc phục cho các điểm yếu tìm ra trong quá trình pentest. |
| MTHP2 | Kiểm tra các chính sách **an toàn thông tin** của tổ chức. Kiểm tra, đánh giá nhận thức của người dùng khi xảy ra tấn công mạng vào tổ chức |
| MTHP3 | Những thông tin về những điểm yếu bảo mật được xác định và khai thác qua quá trình pentest sẽ được tổng hợp và cung cấp cho các tổ chức nhằm hỗ trợ các tổ chức hoạch định các chiến lược và ưu tiên trong việc tăng cường an ninh bảo mật cho hệ thống CNTT của đơn vị. |
| **2. Kỹ năng** | |
| MTHP4 | Có kỹ năng tổng hợp các kiến thức về mạng máy tính, làm việc nhóm, trình bày thuyết trình về các nội dung nghiên cứu nâng cao. |
| MTHP5 | Có kỹ năng kết hợp chặt chẽ những kiến thức trong vấn đề quản lý an toàn hệ thống mạng. |
| **3. Thái độ** | |
| MTHP6 | Có thái độ tự giác nghiên cứu tài liệu trước khi lên lớp, tích cực tham gia phát biểu, thảo luận nhóm, làm bài tập nhóm. Chia sẻ năng lực bản thân cho những người xung quanh. |

**4. Mô tả vắn tắt nội dung học phần**

Học phần nêu rõ các nguyên nhân dẫn đến việc tấn công mạng máy tính. Phân loại và trình bày được đặc điểm cơ bản các lỗ hổng trong hệ thống mạng. Phân tích các nhóm giải pháp sử dụng để phát hiện và phòng chống xâm nhập mạng, vai trò của mã hoá dữ liệu trong an toàn thông tin và truyền tin trên mạng, nêu bật đặc điểm và thuật toán của một số giao thức mã hoá phổ biến. Nêu rõ vai trò của các công cụ giám sát của hệ thống mạng, các đặc điểm chính của các công cụ phân tích lỗ hổng trong các thiết bị và giao thức mạng. Áp dụng một số công cụ giám sát và phân tích lổ hổng mạng vào hệ thống mạng. Vai trò của việc bảo mật hạ tầng mạng.

Đặc điểm và cơ chế hoạt động của Firewall, VPN, NAT, IDS/IPS. Áp dụng các kỹ thuật Firewall, NAT, VPN, IDS/IPS vào hệ thống mạng**. Thiết lập các chính sách bảo mật trong an ninh mạng. IDS/IPS trong hệ thống mạng. Cơ chế hoạt động trong việc phát hiện và phòng chống xâm nhập cua hệ thống IDS/IPS. Hệ thống cảnh báo trong IDS/IPS.**

**5. Chuẩn đầu ra học phần** (**CLOs)**

| **Ký hiệu** | **Chuẩn đầu ra học phần** |
| --- | --- |
| **1. Kiến thức** | |
| CĐRHP 1 | Tổng quan về bảo mật mạng. Căn bản về mã hóa và các kỹ thuật mã hóa. |
| CĐRHP 2 | Các công cụ phân tích, đánh giá an ninh mạng – Network security analysis tools |
| **2. Kỹ năng** | |
| CĐRHP 3 | Kỹ năng về thu thập và bảo mật hạ tầng mạng - Infrastructure security |
| CĐRHP 4 | Hệ thống phát hiện và phòng chống xâm nhập |
| CĐRHP 5 | **Trình bày được vai trò của việc thiết lập các chính sách bảo mật trong an ninh mạng. Trình bày được vai trò của IDS/IPS trong hệ thống mạng. Trình bày được cơ chế hoạt động trong việc phát hiện và phòng chống xâm nhập cua hệ thống IDS/IPS. Trình bày được vai trò của hệ thống cảnh báo trong IDS/IPS** |
| **3. Mức độ tự chủ và trách nhiệm** | |
| CĐRHP 6 | Cài đặt và cấu hình được các công cụ phân tích lổ hổng mạng. Cài đặt và cấu hình được các firewal, IDS/IPS. Phân tích được các lỗ hổng ở tầng ứng dụng.  Có thái độ nghiêm túc trong học tập, nghiên cứu. Hình thành nhận thức về phát hiện vấn đề - thu thập thông tin – Xử lý các lỗi trong quá trình cài đặt, cấu hình và quản trị mạng |

Sự đóng góp của chuẩn đầu ra học phần cho chuẩn đầu ra của chương trình đào tạo và đáp ứng mục tiêu học phần trình bày ở bảng sau.

**Ma trận chuẩn đầu ra học phần đáp ứng mục tiêu học phần và đóng góp cho chuẩn đầu ra của chương trình đào tạo (tính tương quan thứ bậc)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mục tiêu học phần** | **Mức độ đạt được chuẩn đầu ra học phần** | | **Mức độ đạt được chuẩn đầu ra chương trình đào tạo** | |
| **Mức độ đạt được** | **Chuẩn đầu ra học phần** | **Mức độ đạt được** | **Chuẩn đầu ra CTĐT** |
| MTHP 1 | C | CĐRHP1 | C,C | CĐRC5,6 |
| MTHP 2 | C | CĐRHP2 | C,C | CĐRC5,6 |
| MTHP 3 | C | CĐRHP3 | C,C,TB | CĐRC5,6,7 |
| MTHP 4 | C | CĐRHP4 | C,TB,TB | CĐRC5,6,7 |
| MTHP 5 | TB | CĐRHP5 | C,TB,TB | CĐRC5,6,8 |
| MTHP 6 | TB,TB | CĐRHP5,6 | C,TB,TB | CĐRC6,7,8 |

*Ghi chú:* Mức độ đạt được chuẩn đầu ra học phần và chuẩn đầu ra chương trình đào tạo được đánh giá theo 3 mức: Thấp (T), Trung bình (TB), Cao (C).

**6. Phương pháp tổ chức dạy học**

| **Phương pháp tổ chức dạy học** | **Mục đích** | **Đạt được CĐRHP** |
| --- | --- | --- |
| **I. Phương pháp dạy trực tiếp** |  |  |
| 1. Thuyết giảng | Thuyết giảng lý thuyết, kết hợp bào tập vận dụng vào từng nội dung. | C |
| 2. Tham luận | Sinh viên được trình bày quan điểm, hiểu biết của cá nhân, nắm được bản chất vấn đề, liên hệ thực tế. | T |
| 3. Thực hành | Sinh viên hoàn thành nội dung bài tập được giao trước khi học bài mới. | C |
| **II. Phương pháp dạy học trực tuyến** |  |  |
| 4. Câu hỏi gợi nhớ | Giúp sinh viên phát hiện vấn đề | T |
| 5. Giải quyết vấn đề | Tìm ra phương pháp học tối ưu | T |
| 6. Học theo tình huống | Đưa ra sản phẩm phù hợp | T |
| **III. Phương pháp dạy học trải nghiệm** |  |  |
| 7. Thực tập | Thực hiện các yêu cầu GV đề ra, thực hiện các yêu cầu giảng viên yêu cầu. Tìm tòi thực tế cơ sở. | T |
| 8. Thực tế | Trải nghiệm thực tế việc ứng dụng của môn học. | TB |
| **IV. Phương pháp dạy học tương tác** |  |  |
| 9. Thảo luận | Thảo luận nhóm theo nhóm thực tập. | TB |
| 10. Học nhóm | Đưa ra thao tác thực hành hiệu quả nhất. | T |
| **V. Phương pháp tự học** |  |  |
| 11. Tự học, tự nghiên cứu | Sinh viên tự đọc tài liệu, tự nghiên cứu trước các nội dung giáo viên hướng dẫn yêu cầu.  Đọc thêm các tài liệu tham khảo để củng cố và mở rộng kiến thức, giúp rèn luyện kỹ năng tự học, tự nghiên cứu, đọc tài liệu chuyên ngành bằng tiếng Anh. | C |

**7. Nội dung và hình thức tổ chức dạy – học**

*(Trình bày chi tiết từng nội dung)*

| **TT** | **Nội dung** | **Hình thức tổ chức dạy - học** | | | | | **Tổng** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Lên lớp** | | | **Thực tế, kiến tập** | **Tự học, ngoại khóa,…** |  |
| **Lý thuyết** | **Thực hành** | **Khác (TT, ĐA, ...)** |
| 1 | Chương 1. Tổng quan về bảo mật mạng. | 4 | 8 | 0 | 0 | 0 | 12 |
| 2 | Chương 2. Cryptography - Mã hóa**.** | 8 | 16 | 0 | 0 | 0 | 24 |
| 3 | Chương 3. Các công cụ phân tích, đánh giá an ninh mạng – Network security analysis tools | 6 | 12 | 0 | 0 | 0 | 18 |
| 4 | Chương 4. Bảo mật hạ tầng mạng - Infrastructure security. | 6 | 12 | 0 | 0 | 0 | 18 |
| 5 | Chương 5: Hệ thống phát hiện và phòng chống xâm nhập | 6 | 12 | 0 | 0 | 0 | 18 |
| Tổng | | 30 | 30 | 0 | 0 | 0 | 90 |

**8. Kế hoạch giảng dạy học chi tiết**

| **Buổi học** | **Hình thức tổ chức dạy học** | **Nội dung chính** | **Đạt được CĐRHP** | **Nhiệm vụ của người học** |
| --- | --- | --- | --- | --- |
| 1 | Thuyết giảng;  Đặt câu hỏi;  Hướng dẫn thảo luận, làm các bài tập trên lớp; | **Chương 1. Tổng quan về bảo mật mạng**.  1.1Tổng quan về bảo mật mạng máy tính.  1.2 Phân loại các lỗ hổng bảo mật 1.3Các kiểu tấn công mạn  1.4Các giải pháp phát hiện và phòng chống tấn công mạng | CLO1 | Nghe giảng;  Trả lời câu hỏi;  Thảo luận nhóm;  Đọc tài liệu |
| 2 | Thuyết giảng;  Đặt câu hỏi;  Hướng dẫn thảo luận, làm việc nhóm; | **Chương 2. Cryptography - Mã hóa.**  2.1 Căn bản về mã hóa  2.2 Một số kỹ thuật mã hóa | CLO2 | Nghe giảng;  Trả lời câu hỏi;  Thảo luận nhóm; Làm ví dụ minh họa  Đọc tài liệu |
| 3 | Thuyết giảng;  Đặt câu hỏi;  Hướng dẫn thảo luận, làm việc nhóm; | **Chương 3. Các công cụ phân tích, đánh giá an ninh mạng – Network** **security analysis tools.**  3.1Port and connection monitoring.  3.2Port scanning  3.3Network sniffing  3.4Vulnerability scanning | CLO3,4 | Nghe giảng;  Trả lời câu hỏi;  Thảo luận nhóm;  Đọc tài liệu |
| 4 | Thuyết giảng;  Đặt câu hỏi;  Hướng dẫn thảo luận, làm việc nhóm; | **Chương 4. Bảo mật hạ tầng mạng - Infrastructure security**.  4.1 Giới thiệu + Firewall.  4.2 VPN  4.3VLAN  4.4NAT  4.5Media security  4.6 IDS/IPS  4.7 Network security policy | CLO4,5 | Nghe giảng;  Trả lời câu hỏi;  Thảo luận nhóm;  Đọc tài liệu |
|  |  | **Chương 5: Hệ thống phát hiện và phòng chống xâm nhập**  5.1 Vài trò của IDS/IPS trong hệ thống mạng.  5.2 Đặc điểm của IDS/IPS.  5.3 Nguyên tắc hoạt động của IDS/IPS.  5.4 Khảo sát một số IDS/IPS phổ biến.  5.5 IDS/IPS dựa vào nguồn mở |  |  |

**9. Đánh giá kết quả học tập**

**9.1. Đánh giá điểm quá trình**

| **Tiêu chí đánh giá** | **Mức độ đạt chuẩn quy định** | | | | | **Nhằm đạt CLOs** | **Trọng số (%)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Xuất sắc, giỏi** | **Khá, tốt** | **Đạt** | **Yếu** | **Kém** |
| **9 -10** | **7 - 8** | **5 - 6** | **3 – 4** | **0 - 2** |
| **1. Chuyên cần** | | | | | |  | **10** |
| Chuyên cần | Vắng 0 – 1 buổi | Vắng 2 buổi | Vắng 3 buổi | Vắng 4 buổi | Vắng 5 buổi | CĐRHP1,2,3,4,5,6 | 7 |
| Thái độ học tập | Nghiêm túc, tích cực trong quá trình học, được đánh giá xuất sắc. | Nghiêm túc, tích cực trong quá trình học, được đánh giá khá. | Nghiêm túc, tích cực trong quá trình học, được đánh giá đạt. | Không nghiêm túc trong quá trình học tập. | Có thái độ thiếu nghiêm túc trong quá trình học tập. | 3 |
| **2. Kiểm tra thường xuyên, bài tập, thảo luận, ...** | | | | | |  | **10** |
| ***Thảo luận, bài tập*** | Tham gia thảo luận tích cực với nhóm, trả lời đúng xuất sắc các vấn đề được đặt ra, không có sai sót. | Tham gia thảo luận tích cực với nhóm, trả lời khá đúng các vấn đề được đặt ra nhưng còn một số lỗi nhỏ | Tham gia thảo luận tích cực với nhóm, trả lời đúng một phần các vấn đề được đặt ra, còn nhiều lỗi sai | Ít tham gia thảo luận với nhóm, trả lời đúng một phần các vấn đề được đặt ra, còn nhiều lỗi sai | Không tham gia thảo luận với nhóm. | CĐRHP1,2,3,4,5,6 | 10 |
| **3. Kiểm tra giữa kỳ** | | | | | |  | **20** |
| ***Bài kiểm tra*** | Đúng 90-100% | Đúng 70-80% | Đúng 50-60% | Đúng 30-40% | Đúng 0-20% | CĐRHP1,2,3,4,5,6 | 20 |
| **Tổng cộng** | | | | | |  | **40%** |

**9.2. Thi kết thúc học phần**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Tiêu chí đánh giá** | **Mức độ đạt chuẩn quy định** | | | | | **Nhằm đạt CLOs** | **Trọng số (%)** |
| **Xuất sắc, giỏi** | **Khá, tốt** | **Đạt** | **Yếu** | **Kém** |
| **9 -10** | **7 - 8** | **5 - 6** | **3 – 4** | **0 - 2** |
| ***Nội dung*** | Kết quả công việc được giao tốt.  - Ý thức kỷ luật cao trong quá trình học.  - Khả năng tiếp cận và thực hiện công việc xuất sắc.  - Tính hiệu quả và sáng tạo xuất sắc trong quá trình giải quyết vấn đề trong công việc.  - Báo cáo kết quả thực tập đầy đủ và có chất lượng xuất sắc.  - Thái độ ham học hỏi cầu tiến bộ, hiệu quả và kiến thức sinh viên thu được sau đợt thực tập rất tốt. | Kết quả công việc được giao tốt.  - Có ý thức kỷ luật cao trong quá trình học.  -Khả năng tiếp cận và thực hiện các nội dung khá.  - Tính hiệu quả và sáng tạo trong quá trình giải quyết vấn đề trong công việc.  - Báo cáo kết quả thực hành đầy đủ và có chất lượng khá.  - Thái độ ham học hỏi cầu tiến bộ, hiệu quả và kiến thức sinh viên thu được sau đợt thực tập rất tốt. | Kết quả công việc được giao tốt.  -Có ý thức kỷ luật cao trong quá trình học.  -Khả năng tiếp cận và thực hiện các nội dung đạt.  - Tính hiệu quả và sáng tạo đạt trong quá trình giải quyết vấn đề trong công việc.  - Báo cáo kết quả thực hành đầy đủ.  - Thái độ ham học hỏi cầu tiến bộ, hiệu quả và kiến thức sinh viên thu được sau đợt thực tập rất tốt. | Chưa đạt yêu cầu.  Không nghiêm túc tiếp thu trong quá trình học. Không đạt yêu cầu. | Không đạt yêu cầu. | CĐRHP  1,2,3,4,5,6,7 | 40 |
| ***Vận dụng*** | Liên hệ, vận dụng kiến thức của môn học này và các môn học khác có liên quan để hoàn thành xuất sắc nhiệm vụ được giao. | Liên hệ, vận dụng kiến thức của môn học này và các môn học khác có liên quan để hoàn thành tốt nhiệm vụ được giao. | Liên hệ, vận dụng kiến thức của môn học này và các môn học khác có liên quan để hoàn thành nhiệm vụ được giao. | Liên hệ, vận dụng kiến thức của môn học này và các môn học khác có liên quan, nhưng không hoàn thành nhiệm vụ không đạt yêu cầu. | Liên hệ, vận dụng kiến thức của môn học này và các môn học khác có liên quan, không hoàn nhiệm vụ được giao. Không có ý thực tự giác. | CĐRHP  1,2,3,4,5,6,7 | 15 |
| ***Hình thức*** | Đề cương thực tập, báo cáo thường xuyên với giáo viên hướng dẫn; đánh giá của cơ sở thực tập. Hồ sơ thực tập và báo cáo thực tập trước tiểu ban chấm. | Đề cương thực tập, báo cáo thường xuyên với giáo viên hướng dẫn; đánh giá của cơ sở thực tập. Hồ sơ thực tập và báo cáo thực tập trước tiểu ban chấm. |  |  |  | CĐRHP  4,5,6,7 | 5 |
| **Tổng cộng** | | | | | | | **60** |

**\*Ghi chú:**

**[1]-**Các kết quả đánh giá được tổng hợp theo thang điểm 10 dưới đây:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Điểm tổng hợp học phần | = | Điểm quá trình \* 4 | + | Điểm thi kết thúc học phần \* 6 |
| *10* | | |

**10. Học liệu**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **TT** | **Tên tác giả** | **Tên tài liệu** | **Năm xuất bản** | **Nhà xuất bản** | **Địa chỉ khai thác tài liệu** | **Mục đích sử dụng** | |
| **Tài liệu chính** | **Tham khảo** |
| 1 | Anne Henmi, Mark Lucas, Abhishek Singh, Chris Cantrell | Firewall Policies and VPN Configurations | 2011 | Syngress |  |  | x |
| 2 | Steve Manzuik, Ken Pfeil, Andre | Network Security Assessment | 2011 | Syngress |  |  | x |
| 3 | Nei Daswani, Christoph Kern, Anita Kesavan | Foundation of Security | 2008 | Apress |  |  | x |

**11. Các quy định đối với giảng dạy học phần**

***11.1. Cam kết của giảng viên***

Giúp sinh viên nắm bắt được các vấn đề sau: Nắm được các khái niệm hệ thống thông tin, đặc biệt là hệ thống thông tin quản lý. Nắm được vai trò của công nghệ trong các hệ thống thông tin hiện nay. Vận dụng một số phương pháp và công cụ hỗ trợ cho sự phát triển của các hệ thống thông tin trong các môi trường mới.

*11.2. Quy định đối với sinh viên*

- Dự lớp: Đọc trước giáo trình, phát hiện vấn đề, nghe giảng, nêu các câu hỏi và tham gia thảo luận về các vấn đề do giáo viên và sinh viên khác đặt ra.

- Bài tập: Phát hiện vấn đề, tham gia giải và thực hành trên lớp, tại nhà

- Nghiên cứu: Đọc tài liệu tham khảo, tham gia thuyết trình.

- Thảo luận tổ hoặc thuyết trình tại lớp do giảng viên phân công.

- Làm bài tập ứng dụng hoặc bài tập tình huống để củng cố kiến thức đã được học.

***11.3. Yêu cầu đối với giảng dạy học phần***

- Cơ sở vật chật: Phòng học có trang bị bảng lớn, máy chiếu, hệ thống máy tính có cài các ứng dụng cần thiết phục vụ cho công tác học tập và thực hành của sinh viên. Giảng viên tự trang bị máy tính cá nhân và các công cụ hỗ trợ khác.

- Các yêu cầu khác: không

*Bình Định, ngày tháng năm 2023*

|  |  |  |  |
| --- | --- | --- | --- |
| **Trưởng khoa**  **(Quản lý CTĐT)** | **P.Trưởng khoa**  **Quản lý học phần**  **ThS. Lương Tiến Vinh** | **Trưởng bộ môn**  **ThS. Lê Quốc Bảo** | **Giảng viên**  **biên soạn**  **ThS. Lương Tiến Vinh** |