

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN AN NINH MẠNG – NETWORK SECURITY

1. Thông tin về giáo viên

TT	Họ tên giảng viên	Học hàm	Học vị	Đơn vị công tác
1	Nguyễn Hiếu Minh	Tiến sỹ	Phó giáo sư	BM An ninh mạng

Thời gian, địa điểm làm việc: Bộ môn An ninh mạng, Nhà A1, Phòng 1305.

Địa chỉ liên hệ: Nhà 48, Tập thể Thông tin, Trần Cung, Từ Liêm, Hà Nội.

Điện thoại, email: 0989.193571, hieuminhmta@ymail.com.

Các hướng nghiên cứu chính: Mạng máy tính, An ninh mạng, Mật mã.

2. Thông tin chung về học phần

- Tên học phần: An ninh mạng.
- Mã học phần:
- Số tín chỉ: 3TC, Số tiết (LT, BT, TL, TH) – (30, 15, 6, 9).
- Học phần (Bắt buộc hay Lựa chọn): Bắt buộc.
- Các học phần tiên quyết: Lập trình cơ bản, Các môn toán.
- Các học phần kế tiếp: An ninh mạng.
- Các yêu cầu đối với học phần (nếu có): Môn học được xây dựng dành cho các sinh viên hệ chính quy quân sự và dân sự hệ đại học.
- Giờ tín chỉ đối với các hoạt động:
 - Nghe giảng lý thuyết: 30 tiết
 - Làm bài tập trên lớp: 15 tiết
 - Thảo luận: 6 tiết
 - Thực hành, thực tập (ở PTN, nhà máy, thực tập...): 9 tiết
 - Hoạt động theo nhóm: 20 tiết
 - Tự học: 60 tiết
- Địa chỉ Khoa/ Bộ môn phụ trách môn học: Khoa Công nghệ Thông tin, Bộ môn An ninh mạng.

3. Mục tiêu của học phần

- Kiến thức: Có kiến thức cơ bản về an ninh hệ thống mạng máy tính bao gồm các vấn đề an ninh dữ liệu, truyền thông, dịch vụ, thiết bị.
- Kỹ năng: Có khả năng đọc hiểu các kiến thức mở rộng của môn học an ninh mạng. Biết phân tích các giải pháp an ninh trong các hoạt động hệ thống, đánh giá, và đưa ra những nhận xét, giải pháp tăng cường an ninh cho hệ thống mạng.

- Thái độ, chuyên cần: Rèn luyện được thái độ nghiêm túc và có khả năng đọc hiểu và nghiên cứu chuyên sâu trong lĩnh vực an ninh mạng máy tính.

4. Tóm tắt nội dung học phần

Mục tiêu của học phần là đào tạo các kiến thức cơ bản và nâng cao trong lĩnh vực an ninh hệ thống mạng máy tính. Thông qua kiến thức môn học, học viên nắm bắt được các thông tin, cách thức triển khai và phát triển các giải pháp an ninh mạng máy tính trong thực tế.

5. Nội dung chi tiết học phần

Chương, mục, tiểu mục	Nội dung	Số tiết	Giáo trình, Tài liệu tham khảo (Ghi TT của TL ở mục 6)	Ghi chú
I	<p>Tổng quan về an ninh mạng máy tính</p> <ol style="list-style-type: none"> 1. Các khái niệm chung về an toàn thông tin 2. Các khái niệm cơ bản của an ninh mạng máy tính 3. Mục tiêu của an ninh mạng 4. Các mô hình an ninh mạng 5. Các chính sách an ninh mạng 	3	1-6	
II	<p>Tấn công mạng máy tính</p> <ol style="list-style-type: none"> 1. Phương pháp luận tấn công 2. Định nghĩa, khái niệm tấn công 3. Phân loại tấn công 4. Các mô hình thực hiện tấn công 5. Các phương pháp phòng chống tấn công 	3	1, 3	
III	<p>Các phương thức điều khiển truy nhập mạng máy tính</p> <ol style="list-style-type: none"> 1. Các giao thức và dịch vụ truy nhập từ xa (RADIUS, TACACS) 2. Các mô hình điều khiển truy nhập (MAC, RBAC, DAC) 3. Điều khiển truy nhập mạng (NAC) 	6	1, 2, 5	

	4. Công nghệ mạng riêng ảo VPN 5. Xây dựng mạng riêng ảo			
IV	Công nghệ bức tường lửa (Firewall) 1. Tổng quan về firewall 2. Nguyên lý làm việc 3. Phân loại firewall 4. Một số mô hình firewall 5. Đánh giá firewall	6	1, 5	
V	Hệ thống phát hiện và phòng chống xâm nhập (IDS&IPS) 1. Khái niệm chung về IDS và IPS 2. Hệ thống phát hiện xâm nhập IDS 3. Hệ thống phòng chống xâm nhập IPS 4. Xây dựng các mô hình trong thực tế 5. Đánh giá về các hệ thống	6	1, 6	
VI	An ninh mạng WLAN (IEEE 802.11) 1. Các vấn đề an ninh trong mạng WLAN 2. Các kiểu tấn công trên mạng WLAN 3. Giao thức mã hóa WEP, WPA, WPA2 4. Các giải pháp xác thực trong mạng WLAN 5. Các mô hình triển khai an ninh trong mạng WLAN	6	1, 4	
	Tổng	30		

6. Giáo trình, tài liệu tham khảo

TT	Tên tài liệu	Tình trạng tài liệu			
		Có trên thư viện	Giáo viên hoặc Khoa có, cho mượn để TV photo hoặc có File Điện tử	Đề nghị mua mới	Đề nghị biên soạn mới
1	Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley. Network Security Bible . Wiley Publishing, Inc., 2005, - 697p.		File điện tử		

- Nắm được những khái niệm cơ bản về an ninh mạng (mô hình, mục tiêu, chính sách);

- **Hình thức tổ chức dạy học:** Lý thuyết, thảo luận, tự học, tự nghiên cứu

- **Thời gian:** Lý thuyết, thảo luận: 4t; Tự học, tự nghiên cứu: 4t

- **Địa điểm:** Giảng đường do P2 phân công.

- **Nội dung chính:**

1. Mục đích yêu cầu của môn học
2. Các nội dung chính của môn học
3. Các khái niệm chung về an toàn thông tin
4. Các khái niệm cơ bản của an ninh mạng máy tính
5. Mục tiêu của an ninh mạng
6. Các mô hình an ninh mạng
7. Các chính sách an ninh mạng

- **Yêu cầu SV chuẩn bị:**

Đọc trước TL[1]: chương 1,2. Đọc trước TL[2]: chương 1,2,3. Đọc trước TL[5]: chương 1.

Tự đọc: TL[1]: chương 1,2. TL[2]: chương 1,2,3.

Bài tập về nhà cho Chương I: Cuối chương 1,2,3 của TL [2]. Cuối chương 1 của TL [5].

Bài giảng 2: Tấn công mạng máy tính

Chương II

Mục 1 – 5

Tiết thứ: 5 - 8

Tuần thứ: 2

- **Mục đích, yêu cầu:**

- Nắm được kiến thức cơ bản về các phương pháp tấn công mạng máy tính;
- Tìm hiểu về một số mô hình và công cụ tấn công mạng;
- Tìm hiểu các phương pháp phòng chống tấn công mạng.

- **Hình thức tổ chức dạy học:** Lý thuyết, bài tập, tự học, tự nghiên cứu

- **Thời gian:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t

- **Địa điểm:** Giảng đường do P2 phân công.

- **Nội dung chính:**

1. Phương pháp luận tấn công;
2. Định nghĩa, khái niệm tấn công;

3. Phân loại tấn công;
4. Các mô hình thực hiện tấn công;
5. Các phương pháp phòng chống tấn công.

- Yêu cầu SV chuẩn bị:

Đọc trước TL[3]: chương 3-8. .

Tự đọc: Ví dụ cuối các chương của TL [3].

Bài tập về nhà cho Chương II: Cuối các chương của TL [3].

Bài giảng 3: Các phương thức điều khiển truy nhập mạng máy tính

Chương III Mục 1 – 3

Tiết thứ: 9 - 12 Tuần thứ: 3

- Mục đích, yêu cầu:

- Hiểu được kiến thức về các giao thức dùng trong điều khiển truy nhập mạng;
- Hiểu được kiến thức về các mô hình điều khiển truy nhập.

- Hình thức tổ chức dạy học: Lý thuyết, bài tập, tự học, tự nghiên cứu

- Thời gian: Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t

- Địa điểm: Giảng đường do P2 phân công.

- Nội dung chính:

1. Các giao thức và dịch vụ truy nhập từ xa (RADIUS, TACACS);
2. Các mô hình điều khiển truy nhập (MAC, RBAC, DAC);
3. Điều khiển truy nhập mạng (NAC).

- Yêu cầu SV chuẩn bị:

Đọc trước TL[1]: chương 3. Đọc trước TL[5]: chương 16,17,18,19.

Tự đọc: Ví dụ cuối chương 16-19 của TL [5].

Bài tập về nhà cho Chương II: Cuối chương 16-19 của TL [5].

Bài giảng 4: Các phương thức điều khiển truy nhập mạng máy tính (tiếp)

Chương III Mục 4 – 5

Tiết thứ: 9 - 12 Tuần thứ: 4

- Mục đích, yêu cầu:

- Hiểu được kiến thức về công nghệ mạng riêng ảo;
- Các kỹ thuật xây dựng mạng riêng ảo.

- **Hình thức tổ chức dạy học:** Lý thuyết, bài tập, tự học, tự nghiên cứu
- **Thời gian:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t
- **Địa điểm:** Giảng đường do P2 phân công.

- **Nội dung chính:**

1. Công nghệ mạng riêng ảo (VPN);
2. Xây dựng mạng riêng ảo.

- **Yêu cầu SV chuẩn bị:**

Đọc trước TL[2]: chương 12. Đọc trước TL[5]: chương 10-13.

Tự đọc: Ví dụ cuối chương 10-13 của TL [5].

Bài tập về nhà cho Chương II: Cuối chương 10-13 của TL [5].

Bài giảng 5: Công nghệ bức tường lửa

Chương IV Mục 1 – 3

Tiết thứ: 17 - 20 Tuần thứ: 5

- **Mục đích, yêu cầu:**

- Hiểu được các kiến thức tổng quan về Firewall;
- Hiểu được các kiến thức về nguyên lý hoạt động của Firewall;

- **Hình thức tổ chức dạy học:** Lý thuyết, bài tập, tự học, tự nghiên cứu

- **Thời gian:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t

- **Địa điểm:** Giảng đường do P2 phân công.

- **Nội dung chính:**

1. Tổng quan về firewall;
2. Nguyên lý làm việc;
3. Phân loại firewall.

- **Yêu cầu SV chuẩn bị:**

Đọc trước TL[2]: chương 9. Đọc trước TL[5]: chương 7,8,9.

Tự đọc: Ví dụ cuối chương 7,8,9 của TL [5].

Bài tập về nhà cho Chương III: Cuối chương 7,8,9 của TL [5].

Bài giảng 6: Công nghệ bức tường lửa (tiếp)

Chương IV Mục 4 – 6

Tiết thứ: 17 - 20 Tuần thứ: 5

- Mục đích, yêu cầu:

- Hiểu được các kiến thức tổng quan về Firewall;
- Hiểu được các kiến thức về nguyên lý hoạt động của Firewall;

- **Hình thức tổ chức dạy học:** Lý thuyết, bài tập, tự học, tự nghiên cứu

- **Thời gian:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t

- **Địa điểm:** Giảng đường do P2 phân công.

- Nội dung chính:

1. Phân loại firewall;
2. Một số mô hình firewall;
3. Đánh giá firewall.

- Yêu cầu SV chuẩn bị:

Đọc trước TL[2]: chương 9. Đọc trước TL[5]: chương 7,8,9.

Tự đọc: Ví dụ cuối chương 7,8,9 của TL [5].

Bài tập về nhà cho Chương III: Cuối chương 7,8,9 của TL [5].

Bài giảng 7: Hệ thống phát hiện và phòng chống xâm nhập

Chương V Mục 1 – 3

Tiết thứ: 25 - 28 Tuần thứ: 7

- Mục đích, yêu cầu:

- Hiểu được các kiến thức tổng quan về IDS/IPS;
- Hiểu được các kiến thức về IDS.

- **Hình thức tổ chức dạy học:** Lý thuyết, bài tập, tự học, tự nghiên cứu

- **Thời gian:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t

- **Địa điểm:** Giảng đường do P2 phân công.

- Nội dung chính:

1. Khái niệm chung về IDS và IPS;
2. Hệ thống phát hiện xâm nhập IDS;
3. Hệ thống phòng chống xâm nhập IPS.

- Yêu cầu SV chuẩn bị:

Đọc trước TL[1]: chương 17. Đọc trước TL[2]: chương 10. Đọc trước TL[5]: chương 14,15. Đọc trước TL[6]: các chương.

Tự đọc: Ví dụ cuối chương 14,15 của TL [5]. Ví dụ cuối chương 10 của TL [2]

- **Thời gian:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t

- **Địa điểm:** Giảng đường do P2 phân công.

- **Nội dung chính:**

1. Các vấn đề an ninh trong mạng WLAN;
2. Các kiểu tấn công trên mạng WLAN;
3. Các giao thức mã hóa WEP, WPA, WPA2.

- **Yêu cầu SV chuẩn bị:**

Đọc trước TL[1]: chương 12. Đọc trước TL[2]: chương 14. Đọc trước TL[4]: các chương.

Tự đọc: Ví dụ cuối các chương của TL [4].

Bài tập về nhà cho Chương VI: Cuối các chương của TL [4].

Bài giảng 10: An ninh mạng không dây (tiếp)

Chương VI

Mục 4 – 6

Tiết thứ: 37 - 40

Tuần thứ: 10

- **Mục đích, yêu cầu:**

- Hiểu được các kiến thức về các giao thức mã hóa trong WLAN;
- Hiểu được các kiến thức về các giải pháp xác thực trong WLAN;
- Hiểu được các kiến thức về một số mô hình triển khai an ninh trong WLAN.

- **Hình thức tổ chức dạy học:** Lý thuyết, bài tập, tự học, tự nghiên cứu

- **Thời gian:** Lý thuyết, bài tập: 4t; T tự học, tự nghiên cứu: 4t

- **Địa điểm:** Giảng đường do P2 phân công.

- **Nội dung chính:**

1. Giao thức mã hóa WEP, WPA, WPA2;
2. Các giải pháp xác thực trong mạng WLAN;
3. Các mô hình triển khai an ninh trong mạng WLAN.

- **Yêu cầu SV chuẩn bị:**

Đọc trước TL[1]: chương 12. Đọc trước TL[2]: chương 14. Đọc trước TL[4]: các chương.

Tự đọc: Ví dụ cuối các chương của TL [4].

Bài tập về nhà cho Chương VI: Cuối các chương của TL [4].

Bài giảng 11: Tổng hợp bài tập các chương

Chương VII Mục 1 – 3

Tiết thứ: 41 – 44 Tuần thứ: 11

- Mục đích, yêu cầu:

- Hoàn thành các bài tập về một số công cụ mã nguồn mở bảo vệ an ninh mạng.
- Hoàn thành các bài tập về một số công cụ mã nguồn mở tấn công an ninh mạng.
- Hoàn thành các bài tập về xây dựng chương trình thử nghiệm phòng thủ và tấn công mạng.

- Hình thức tổ chức dạy học: Bài tập, tự học, tự nghiên cứu

- Thời gian: Bài tập: 4t; Tự học, tự nghiên cứu: 4t

- Địa điểm: Giảng đường do P2 phân công.

- Nội dung chính:

1. Bài tập về một số công cụ mã nguồn mở bảo vệ an ninh mạng.
2. Bài tập về một số công cụ mã nguồn mở tấn công an ninh mạng.
3. Bài tập về xây dựng chương trình thử nghiệm.

- Yêu cầu SV chuẩn bị:

Đọc trước TL[1,2,3,4,5,6].

Tự đọc: Ví dụ cuối chương của TL [1,2,3,4,5,6].

Bài tập về nhà cho Chương VIII: Cuối chương của TL [1,2,3,4,5,6].

Bài giảng 12: Thảo luận các nội dung đã học

Chương VIII Mục 1 – 4

Tiết thứ: 45 – 48 Tuần thứ: 12

- Mục đích, yêu cầu:

- Thảo luận về các kỹ thuật an ninh mạng.
- Thảo luận về các chính sách an ninh mạng.
- Thảo luận về một số công cụ an ninh mạng mã nguồn mở.
- Thảo luận về thiết kế an ninh mạng.

- Hình thức tổ chức dạy học: Thảo luận, tự học, tự nghiên cứu

- Thời gian: Thảo luận: 4t; Tự học, tự nghiên cứu: 4t

- Địa điểm: Giảng đường do P2 phân công.

- Nội dung chính:

1. Các kỹ thuật an ninh mạng.
2. Các chính sách an ninh mạng.
3. Một số công cụ an ninh mạng mã nguồn mở.
4. Thiết kế an ninh mạng.

- Yêu cầu SV chuẩn bị:

Đọc trước TL[1,2,3,4,5,6].

Tự đọc: Ví dụ cuối chương của TL [1,2,3,4,5,6].

Bài tập về nhà cho Chương VIII: Cuối chương của TL [1,2,3,4,5,6].

Bài giảng 13: Thảo luận các nội dung đã học

Chương IX

Mục 1 – 4

Tiết thứ: 49 – 52

Tuần thứ: 13

- Mục đích, yêu cầu:

- Thảo luận về các kỹ thuật an ninh mạng.
- Thảo luận về các chính sách an ninh mạng.
- Thảo luận về một số công cụ an ninh mạng mã nguồn mở.
- Thảo luận về thiết kế an ninh mạng.

- Hình thức tổ chức dạy học: Lý thuyết, bài tập, tự học, tự nghiên cứu

- Thời gian: Thảo luận: 4t; Tự học, tự nghiên cứu: 4t

- Địa điểm: Giảng đường do P2 phân công.

- Nội dung chính:

1. Các kỹ thuật an ninh mạng.
2. Các chính sách an ninh mạng.
3. Một số công cụ an ninh mạng mã nguồn mở.
4. Thiết kế an ninh mạng.

- Yêu cầu SV chuẩn bị:

Đọc trước TL[1,2,3,4,5,6].

Tự đọc: Ví dụ cuối chương của TL [1,2,3,4,5,6].

Bài tập về nhà cho Chương VIII: Cuối chương của TL [1,2,3,4,5,6].

Bài giảng 14: Thực hành các nội dung đã học

Chương X Mục 1 – 2

Tiết thứ: 53 – 56 Tuần thứ: 14

- Mục đích, yêu cầu:

- Thử nghiệm một số công cụ bảo vệ mạng.
- Thử nghiệm một số công cụ tấn công mạng.

- Hình thức tổ chức dạy học: Thực hành, tự học, tự nghiên cứu**- Thời gian:** Thực hành: 4t; Tự học, tự nghiên cứu: 4t**- Địa điểm:** Tại PTN An ninh mạng.**- Nội dung chính:**

1. Thử nghiệm một số công cụ bảo vệ mạng.
2. Thử nghiệm một số công cụ tấn công mạng.

- Yêu cầu SV chuẩn bị:

Đọc trước TL[1,2,3,4,5,6].

Tự đọc: Ví dụ cuối chương của TL [1,2,3,4,5,6].

Bài tập về nhà cho Chương VIII: Cuối chương của TL [1,2,3,4,5,6].**Bài giảng 15: Thực hành các nội dung đã học**

Chương X Mục 1 – 2

Tiết thứ: 57 – 60 Tuần thứ: 15

- Mục đích, yêu cầu:

- Thử nghiệm một số công cụ bảo vệ mạng.
- Thử nghiệm một số công cụ tấn công mạng.

- Hình thức tổ chức dạy học: Thực hành, tự học, tự nghiên cứu**- Thời gian:** Thực hành: 4t; Tự học, tự nghiên cứu: 4t**- Địa điểm:** Tại PTN An ninh mạng.**- Nội dung chính:**

1. Thử nghiệm một số công cụ bảo vệ mạng.
2. Thử nghiệm một số công cụ tấn công mạng..

- Yêu cầu SV chuẩn bị:

Đọc trước TL[1,2,3,4,5,6].

Tự đọc: Ví dụ cuối chương của TL [1,2,3,4,5,6].

Bài tập về nhà cho Chương VIII: Cuối chương của TL [1,2,3,4,5,6].

8. Chính sách đối với học phần và các yêu cầu khác của giáo viên

Sinh viên cần có mặt tại lớp đủ số tiết theo yêu cầu, tích cực tham gia thảo luận, tham gia các hoạt động giáo viên tổ chức.

Chuẩn bị bài tốt trước khi tới lớp học.

Thực hiện tốt các bài tập giáo viên giao về nhà: nộp bài đúng hạn, chất lượng từ trung bình trở lên.

Tham gia bài thi hết môn.

- Bài tập học phần (làm theo nhóm)
 - o Trình bày tổng quan về cơ sở lý thuyết: 30%
 - o Các phân tích, đánh giá chuyên sâu: 30%
 - o Phân chương trình: 30%
 - o Trình bày khoa học, nộp bài đúng hạn: 10%

9. Phương pháp, hình thức kiểm tra - đánh giá kết quả học tập học phần

9.1. Kiểm tra – đánh giá thường xuyên

Thường xuyên điểm danh vào thời điểm thích hợp.

9.2. Kiểm tra - đánh giá định kì

- Tham gia học tập trên lớp (đi học đầy đủ, chuẩn bị bài tốt và tích cực thảo luận,...): *Hệ số 0.1.*

- Hoàn thành tốt Bài tập về nhà, Kiểm tra giữa kì: *Hệ số 0.2.*

- Thi kết thúc học phần tốt: *Hệ số 0.7.*

Chủ nhiệm Khoa

(Ký và ghi rõ họ tên)

Chủ nhiệm Bộ môn

(Ký và ghi rõ họ tên)

Giảng viên biên soạn

(Ký và ghi rõ họ tên)

PGS.TS. Đào Thanh Tĩnh PGS.TS. Nguyễn Hiếu Minh PGS. TS. Nguyễn Hiếu Minh