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:
KỸ THUẬT THEO DÕI, GIÁM SÁT AN TOÀN MẠNG

Mã học phần: INT1429
(2 tín chỉ)

Biên soạn
NGUYỄN NGỌC ĐIỆP

Hà Nội - 2016

ĐỀ CƯƠNG HỌC PHẦN: KỸ THUẬT THEO DÕI, GIÁM SÁT AN TOÀN MẠNG

Khoa: Công nghệ thông tin **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: Kỹ thuật theo dõi, giám sát an toàn mạng
- Tên tiếng Anh của môn học: Monitoring techniques for information and network security
- Mã môn học: INT1429
- Số tín chỉ (TC): 2
- Loại môn học: Tự chọn
- **Các môn học tiên quyết**: Mạng máy tính, An toàn bảo mật hệ thống thông tin
- **Môn học trước:**
- **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: 20 tiết
+ Chữa bài trên lớp: tiết
+ Bài tập lớn/Tiểu luận: 4 tiết
+ Thảo luận và Hoạt động nhóm: tiết
+ Thí nghiệm, Thực hành: 6 tiết
+ Tự học: 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 nền tảng và chuyên sâu về các kỹ thuật giám sát an toàn mạng, bao gồm: tính cấp thiết của hệ thống giám sát an toàn mạng và các thách thức đối với hệ thống này; các biện pháp và nguyên tắc giám sát an toàn mạng, đánh giá chất lượng và nâng cao khả năng hoạt động của hệ thống.

- Kỹ năng: Giúp sinh viên nắm vững các kiến thức nền tảng và chuyên sâu về các kỹ thuật giám sát an toàn mạng. Có khả năng phân tích, phát hiện các dấu hiệu của hệ thống, mạng bị đột nhập và cài đặt các công cụ giám sát an toàn mạng để đối phó.

- 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: Giới thiệu về giám sát an toàn mạng	Hiểu được giám sát an toàn mạng là gì, tính cần thiết của hệ thống giám sát an toàn mạng và các thách thức đối với hệ thống này.	Phân tích các yêu cầu cơ bản của giám sát an toàn mạng	Tổng hợp và đánh giá các yêu cầu của hệ thống mạng và giám sát an toàn
Chương 2: Thu thập dữ liệu	Hiểu được phương pháp thu thập dữ liệu, kiến trúc cảm biến để thu thập dữ liệu, và các loại dữ liệu	Nắm được các phương pháp thu thập dữ liệu, ưu nhược điểm của các phương pháp, cách quản lý dữ liệu thu thập	Vận dụng để xây dựng được hệ thống thu thập các loại dữ liệu cần thiết, quản lý dữ liệu
Chương 3: Phát hiện xâm nhập	Hiểu được phương pháp, kỹ thuật và các công cụ phát hiện xâm nhập cụ thể	Nắm được các phương pháp phát hiện xâm nhập, ưu nhược điểm của các phương pháp, nắm được các công cụ phát hiện xâm nhập.	Vận dụng các phương pháp và công cụ thể phát hiện xâm nhập trong tình huống cụ thể
Chương 4: Phân tích dữ liệu	Hiểu được phương pháp, kỹ thuật và các công cụ phân tích dữ liệu	Nắm được các phương pháp phân tích dữ liệu, ưu nhược điểm của các phương pháp, nắm được các công cụ phân tích dữ liệu.	Vận dụng các phương pháp và công cụ thể phân tích dữ liệu trong tình huống cụ thể

4. Tóm tắt nội dung môn học

Môn học cung cấp các kiến thức nền tảng và chuyên sâu về các kỹ thuật giám sát an toàn mạng bao gồm: khái niệm về hệ thống giám sát an toàn mạng; các biện pháp và nguyên tắc giám sát an toàn mạng bao gồm thu thập dữ liệu, phát hiện xâm nhập và phân tích dữ liệu; nâng cao khả năng hoạt động của hệ thống và cách sử dụng các công cụ giám sát an toàn mạng trong thực tế.

5. Nội dung chi tiết môn học

Chương 1: Giới thiệu về giám sát an toàn mạng

1.1 Các thuật ngữ chính trong NSM

1.2 Phát hiện xâm nhập
1.3 Giám sát an toàn mạng
1.4 Phòng thủ theo lỗ hổng bảo mật và phòng thủ theo nguy cơ
1.5 Chu trình giám sát an toàn mạng
1.6 Thách thức đối với hệ thống NSM
1.7 Chuyên gia của hệ thống NSM
1.8 Bộ công cụ Security Onion

Chương 2: Thu thập dữ liệu

2.1 Phương pháp thu thập dữ liệu
2.2 Kiến trúc cảm biến
2.3 Dữ liệu phiên
2.4 Dữ liệu gói tin đầy đủ
2.5 Dữ liệu kiểu chuỗi trong gói tin

Chương 3: Phát hiện xâm nhập

3.1 Các kỹ thuật phát hiện xâm nhập, dấu hiệu tấn công và chữ ký
3.2 Phát hiện xâm nhập dựa trên danh tiếng
3.3 Phát hiện xâm nhập dựa trên chữ ký với Snort và Suricata
3.4 Phát hiện xâm nhập dựa trên bất thường với dữ liệu thống kê

Chương 4: Phân tích dữ liệu

4.1. Phân tích gói tin
4.2. Tri thức về nguy cơ bảo mật và tài nguyên cần bảo vệ
4.3. Quy trình phân tích

6. Học liệu

6.1. Học liệu bắt buộc

[1]. Chris Sanders and Jason Smith, *Applied Network Security Monitoring*, Syngress, 2014

6.2. Học liệu tham khảo

[2]. Richard Bejtlich, *The Tao of Network Security Monitoring: Beyond Intrusion Detection*, Addison-Wesley, 2004
[3]. Richard Bejtlich, *The Practice Of Network Security Monitoring*, No Starch Press, 2013
[4]. John R. Vacca, *Network and System Security*, Elsevier Inc., 2010
[5]. Chris Fry and Martin Nystrom, *Security Monitoring*, O'Reilly Media Inc., 2009

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: Giới thiệu về giám sát an toàn mạng	2					2
Nội dung 2: Phương pháp thu thập dữ liệu; Kiến trúc cảm biến	2					2
Nội dung 3: Dữ liệu phiên, Dữ liệu gói tin đầy đủ	2					2
Nội dung 4: Dữ liệu kiểu chuỗi trong gói tin	2					2
Nội dung 5: Bài tập lớn/Tiểu luận về các phương pháp thu thập dữ liệu		2				
Nội dung 6: Các kỹ thuật phát hiện xâm nhập, dấu hiệu tấn công và chữ ký	2					2
Nội dung 7: Thực hành thu thập dữ liệu và phát hiện xâm nhập với Wireshark				2		2
Nội dung 8: Phát hiện xâm nhập dựa trên danh tiếng Kiểm tra giữa kỳ.	2					2
Nội dung 9: Phát hiện xâm nhập dựa trên chữ ký với Snort và Suricata	2					2
Nội dung 10: Phát hiện xâm nhập dựa trên bất thường với dữ liệu thống kê	2					2
Nội dung 11: Bài tập lớn/Tiểu luận về các phương pháp phát hiện xâm nhập		2				2
Nội dung 12: Thực hành phát hiện xâm nhập với Snort				2		2
Nội dung 13: Phân tích gói tin, Tri thức về nguy cơ bảo mật và tài nguyên cần bảo vệ	2					2
Nội dung 14: Thực hành về phân tích gói tin				2		2
Nội dung 15: Quy trình phân tích	2					2
Tổng cộng	**20**	**4**		**6**		**30**

7.2. Lịch trình tổ chức dạy học cụ thể

Tuần 1, Nội dung 1: Giới thiệu về giám sát an toàn mạng

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú

Lý thuyết	2	- Khái niệm về giám sát an toàn mạng và các thách thức. - Bộ công cụ thực hành	- Đọc chương 1, quyển 1 - Đọc chương 1,2,3, phần 1, quyển 2	

Tuần 2, Nội dung 2: Phương pháp thu thập dữ liệu, Kiến trúc cảm biến

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Giới thiệu phương pháp thu thập dữ liệu - Kiến trúc cảm biến	- Đọc chương 2, phần 1, quyển 1 - Đọc chương 3, phần 1, quyển 1	

Tuần 3, Nội dung 3: Dữ liệu phiên, Dữ liệu gói tin đầy đủ

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Dữ liệu phiên, Dữ liệu gói tin đầy đủ. Các công cụ thu thập	- Đọc chương 4,5 , phần 1, quyển 1	

Tuần 4, Nội dung 4: Dữ liệu kiểu chuỗi trong gói tin

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Dữ liệu kiểu chuỗi trong gói tin	- Đọc chương 6, phần 1, quyển 1	

Tuần 4, Nội dung 5: Bài tập lớn/Tiểu luận

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Bài tập lớn/Tiểu luận	2	- Bài tập lớn/Tiểu luận về các phương pháp thu thập dữ liệu	- Chuẩn bị bài tiểu luận theo nhóm và slides báo cáo được giao	

Tuần 5, Nội dung 6: Các kỹ thuật phát hiện xâm nhập, dấu hiệu tấn công và chữ ký

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 kỹ thuật phát hiện xâm nhập, dấu hiệu tấn công và chữ ký	- Đọc chương 7, phần 2, quyển 1	

Tuần 5, Nội dung 7: Thực hành

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Thực hành	2	- Thu thập dữ liệu và phát hiện xâm nhập với Wireshark	- Ôn tập trước về kỹ thuật thu thập dữ liệu và phát hiện xâm nhập. - Thực hành thu thập dữ liệu và phát hiện xâm nhập với Wireshark	

Tuần 6, Nội dung 8: Phát hiện xâm nhập dựa trên danh tiếng

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	1	- Phát hiện xâm nhập dựa trên danh tiếng.	- Đọc chương 8, phần 2, quyển 1	
Lý thuyết	1	Kiểm tra giữa kỳ		

Tuần 7, Nội dung 9: Phát hiện xâm nhập dựa trên chữ ký với Snort và Suricata

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Phát hiện xâm nhập dựa trên chữ ký với Snort và Suricata	- Đọc chương 9, phần 2, quyển 1	

Tuần 8, Nội dung 10: Phát hiện xâm nhập dựa trên bất thường với dữ liệu thống kê

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Phát hiện xâm nhập dựa trên bất thường với dữ liệu thống kê	- Đọc chương 11, phần 2, quyển 1	

Tuần 8, Nội dung 11: Bài tập lớn/Tiểu luận

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Bài tập lớn/Tiểu luận	2	- Bài tập lớn/Tiểu luận về các phương pháp phát hiện xâm nhập	- Chuẩn bị bài tiểu luận theo nhóm và slides báo cáo được giao	

Tuần 8, Nội dung 12: Thực hành

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Thực hành	2	- Thực hành phát hiện xâm nhập với Snort	Ôn tập phát hiện xâm nhập với Snort và thực hành.	

Tuần 9, Nội dung 13: Phân tích gói tin, Tri thức về nguy cơ bảo mật và tài nguyên cần bảo vệ

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Phân tích gói tin. Tri thức về nguy cơ bảo mật và tài nguyên cần bảo vệ	- Đọc chương 12, 13, 14, phần 3, quyển 1	

Tuần 9, Nội dung 14: Thực hành

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Thực hành	2	- Thực hành về phân tích gói tin	- Ôn tập phân tích gói tin và thực hành.	

Tuần 10, Nội dung 15: Quy trình phân tích

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Quy trình phân tích	- Đọc chương 15, phần 3, quyển 1	

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

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.

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	20%	Nhóm
- Kiểm tra giữa kỳ	10%	Cá nhân
- Kiểm tra cuối kỳ	60%	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 và trình bày được kiến

	thức căn bản của môn học - Viết báo cáo trình bày và tổng hợp vấn đề theo yêu cầu bài tập nhóm (mỗi cá nhân viết khoảng 1000 từ) - Phân chia công việc và cộng tác theo nhóm - Chuẩn bị tài liệu 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	**Chủ nhiệm bộ môn**	**Giảng viên** *(Chủ trì biên soạn đề cương)*
PGS.TS. Từ Minh Phương	**TS. Hoàng Xuân Dậu**	**Nguyễn Ngọc Điệp**