BỘ GD&ĐT
Trường đại học SPKT
Khoa: CNTT

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc
****

Chương trình Giáo dục đại học

Ngành đào tạo: Công nghệ thông tin **trình độ đào tạo:** Đại học

Chương trình đào tạo: Công nghệ thông tin

Đề cương chi tiết học phần

1. Tên học phần: Hệ thống giám sát mạng **Mã học phần:** NMSY331180

2. Tên tiếng Anh: Network Monitoring Systems

3. Số tín chỉ: 3

Phân bố thời gian: 3(2:1:6)

4. Các giảng viên phụ trách học phần

1/ GV phụ trách chính: ThS. Huỳnh Nguyên Chính

2/ Danh sách giảng viên cùng GD:

2.1/ ThS. Đinh Công Đoan

5. Điều kiện tham gia học tập học phần

Môn học trước: Mạng máy tính căn bản

Môn học tiên quyết: không

6. Mô tả tóm tắt học phần (Course description)

Môn học này Cung cấp kiến thức về các thành phần trong hệ thống giám sát mạng**;** kiến thức về phương pháp tổ chức triển khai một hệ thống giám sát, các giao thức dùng trong giám sát mạng; kiến thức về các công cụ trong giám sát, các hình thức cảnh báo khi hệ thống mạng có sự cố xảy ra.

7. Mục tiêu học phần(Course objective)

Mục tiêu ***(Goals)***	**Mô tả** ***(Goal description)*** *(Học phần này trang bị cho sinh viên:)*	**Chuẩn đầu ra CTĐT**
G1	Kiến thức về giám sát hoạt động của các thiết bị mạng, server và các dịch vụ trên mạng máy tính.	1.2, 1.3
G2	Khả năng phân tích và hiện thực các phần mềm giám sát mạng	2.1, 2.2
G3	Kỹ năng làm việc nhóm, và thuyết trình bằng miệng	3.1, 3.2
G4	Khả năng vận dụng giải pháp giám sát để giải quyết vấn đề trong thực tế.	4.4, 4.5

8. **Chuẩn đầu ra của học phần**

Mục tiêu	Chuẩn đầu ra học phần	Mô tả *(Sau khi học xong môn học này, người học có thể:)*	Chuẩn đầu ra CDIO
G1	G1.1	Trình bày được vai trò của hệ thống giám sát trong hệ thống mạng, đặc điểm của các loại lỗ hổng mạng	1.2
	G1.2	Trình bày được tổng quan về hệ thống phát hiện và phòng chống xâm nhập mạng; đặc điểm và chức năng của các thành phần: giám sát tấn công, giám sát lưu lượng, giám sát thiết bị, giám sát dịch vụ và thành phần cảnh báo	1.2
	G1.3	Trình bày đặc điểm và nguyên lý hoạt động của giao thức ICMP và SNMP	1.3
	G1.4	Trình bày được vai trò của việc theo dõi Syslog để phân tích hoạt động của hệ thống mạng trên các Server, Firewall và các thiết bị mạng trung tâm; vai trò của việc quản lý Syslog tập trung	1.4
	G1.5	Trình bày được vai trò của hệ thống phát cảnh báo trong hệ thống giám sát mạng, đặc điểm của việc giám sát qua: giao diện Web, Email, phát âm thanh và phát tín hiệu qua điện thoại di động.	1.5
G2	G2.1	Cài đặt và cấu hình các công cụ phân tích lỗ hổng mạng	2.1
	G2.2	Cài đặt và cấu hình các công cụ giám sát hoạt động của các thiết bị, giám sát lưu lượng, giám sát dịch vụ mạng, giám sát Syslog tập trung	2.2
	G2.3	Cài đặt và cấu hình hệ thống phát cảnh báo qua Web, Email, âm thanh, điện thoại di động	2.3
G3	G3.1	Làm việc hiệu quả trong một nhóm	3.1
	G3.2	Trình bày trước đám đông sử dụng phương tiện trình chiếu	3.2
G4	G4.1	Đánh giá và lựa chọn giải pháp giám sát mạng hợp cho bài toán thực tế	4.1
	G4.2	Xử lý các lỗi trong quá trình cài đặt và cấu hình các dịch giám sát mạng	4.2

11. Tài liệu học tập

- Sách, giáo trình chính: Giáo trình của khoa CNTT
- Sách tham khảo:

- D. Andrew R. Baker, Joel Esler *"Snort Intrusion Detection and Prevention Toolkit"* , Syngress, 2007
- Rafeeq UR Rehman,*"Intrusion Detection With Snort - Advanced IDS Techniques using Snort, Apache, MySQL, PHP, and ACID"* , Prentice Hall PTR, 2003
- Dinangkur Kundu, S.M. lbrahim Lavlu, *"Cacti 0.8 Network Monitoring"* PACKT Publishing, 2009
- Wojciech Kocjan, "Learning Nagios 3.0", PACKT Publishing, 2009
- Max Schubert, Derrick Bennett, "Nagios 3 Enterprise Network Monitoring Including Plug-ins and Hardware Devices", Syngress, 2008
- David Josephsen,"Building a Monitoring Infrastructure with Nagios", Prentic Hall, 2007
- Douglas Mauro, Kevin Schmidt, "Essential SNMP 2nd Edition", Oreilly, 2005
- Michael Rash, "Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort", No Starch Press, 2007
- Ethan Galstad," NRPE Documentation", Nagios Press, 2007

9. Nhiệm vụ của sinh viên

- Dự lớp: tối thiểu 80 % số tiết giảng

- Bài tập: phải hoàn thành 100% bài tập thực hành và bài tập về nhà do GV giao

10. Tỷ lệ Phần trăm các thành phần điểm và các loại hình đánh giá sinh viên : (14)

- Thang điểm: 10

- Kế hoạch kiểm tra như sau:

Hình thức KT	Nội dung	Thời điểm	Công cụ KT	Chuẩn đầu ra KT	Tỉ lệ (%)
Bài tập lớn (Project)					**30**
BT#1	Cài đặt và cấu hình phần mềm giám sát lưu lượng mạng	Tuần 3	Sản phẩm - Báo cáo	G2.1 G2.2	5
BT#2	Cài đặt và cấu hình phần mềm giám sát thiết bị	Tuần 5	Sản phẩm - Báo cáo	G2.1 G2.2	5
BT#3	Cài đặt và cấu hình phần mềm giám sát dịch vụ mạng	Tuần 6	Sản phẩm - Báo cáo	G2.1 G2.2	10
BT#4	Cài đặt và cấu hình thành phần cảnh báo	Tuần 10	Sản phẩm - Báo cáo	G2.3	10
Tiểu luận - Báo cáo					**10**
	Mỗi nhóm sinh viên từ 2-3 người chọn 1 trong các đề tài sau để tìm hiểu và trình bày báo cáo: Đề tài 1: Cài đặt và cấu hình giám sát thiết bị và cảnh báo qua E-mail Đề tài 2: Cài đặt và cấu hình giám sát thiết bị và cảnh báo qua SMS	Tuần 10-15	Tiểu luận - Báo cáo	G3.2	
Thi cuối kỳ					**50**

	- Nội dung bao quát tất cả các chuẩn đầu ra quan trọng của môn học. - Thời gian làm bài tối thiểu 60 phút.		Thi tự luận	G1.1 G1.2 G1.3 G1.4 G1.5 G2.1 G2.2 G2.3 G4.1 G4.2	

14. Nội dung chi tiết học phần (15)

Tuần	Nội dung	Chuẩn đầu ra học phần
1-2	***Chương 1: Tổng quan về hệ thống giám sát mạng*** *(6/0/12)*	G1.1
	A/Các nội dung GD chính trên lớp: (6) **Nội dung GD lý thuyết:** + Tổng quan về bảo mật mạng máy tính + Phân loại các lỗ hổng bảo mật + Các kiểu tấn công mạng + Các giải pháp phát hiện và phòng chống tấn công mạng **- PPGD chính:** + Thuyết trình + Trình chiếu Powerpoint	
	B/Các nội dung cần tự học ở nhà: (12) + Đọc thêm: nội dung liên quan	G1.1
3-4	***Chương 2:*** **Các thành phần trong hệ thống giám sát mạng** *(6/0/12)*	
	A/Các nội dung học tập chính trên lớp: **Nội dung GD lý thuyết:** + Giám sát tấn công + Giám sát lưu lượng + Giám sát thiết bị + Giám sát dịch vụ + Thành phần cảnh báo	G1.2

	PPGD chính: + Trình chiếu Powerpoint + Thuyết trình	
	B/Các nội dung cần tự học ở nhà (12): + Đọc thêm: phương pháp giám sát tấn công, lưu lượng, cảnh báo	G1.2
5-7	***Chương 3:*** **Các giao thức trong giám sát mạng** *(9/0/18)*	
	A/Các nội dung học tập chính trên lớp: **Nội dung GD lý thuyết:** + ICMP + SNMP **PPGD chính:** + Trình chiếu Powerpoint + Thuyết trình + Làm mẫu	G1.3
	B/Các nội dung cần tự học ở nhà (18): + Ứng dụng ICMP và SNMP trong mô hình giám sát cụ thể	G1.3
8-10	***Chương 4: Quản lý Syslog tập trung*** *(9/0/18)*	
	A/Các nội dung học tập chính trên lớp: **Nội dung GD lý thuyết:** + Giới thiệu + Quản lý Syslog của các Server + Quản lý Syslog của các thiết bị mạng (Router, Switch, Firewall) **PPGD chính:** + Trình chiếu Powerpoint + Thuyết trình + Làm mẫu	G1.4
	B/Các nội dung cần tự học ở nhà (18): + Cài đặt và cấu hình phần mềm quản lý Syslog tập trung	G2.2
11-12	***Chương 5:*** **Hệ thống cảnh báo** *(6/0/12)*	
	A/Các nội dung học tập chính trên lớp: **Nội dung GD lý thuyết:** + Giới thiệu + Cảnh báo qua giao diện Web + Cảnh báo qua Email	G1.5

	+ Cảnh báo bằng phát âm thanh + Cảnh báo qua điện thoại di động **PPGD chính:** + Trình chiếu Powerpoint + Thuyết trình + Làm mẫu	
	B/Các nội dung cần tự học ở nhà(12): + Nội dung liên quan	G1.5
13-15	***Thực hành tại phòng máy*** *(0/3/6)*	
	A/Các nội dung học tập chính trên lớp: + Cài đặt hệ thống phát cảnh báo qua Web + Cài đặt hệ thống phát cảnh báo qua Email + Cài đặt hệ thống phát cảnh báo qua âm thanh + Cài đặt hệ thống phát cảnh báo qua điện thoại di động **- PPGD chính:** + Trình chiếu Powerpoint + Thuyết trình + Làm mẫu	G2.3
	B/Các nội dung cần tự học ở nhà: + Đọc thêm: nội dung liên quan	G2.3

14. Đạo đức khoa học:

+ Các bài làm bài tập, bài dịch từ internet nếu bị phát hiện là sao chép của nhau sẽ bị trừ 100% điểm quá trình, nếu ở mức độ nghiêm trọng (cho nhiều người chép- 3 người giống nhau trở lên) sẽ bị cấm thi cuối kỳ cả người sử dụng bài chép và người cho chép bài.

+ SV không hoàn thành nhiệm vụ (mục 9) thì bị cấm thi và bị đề nghị kỷ luật trước toàn trường

+ Sinh viên thi hộ thì cả 2 người – thi hộ và nhờ thi hộ sẽ bị đình chỉ học tập hoặc bị đuổi học

15. Ngày phê duyệt:

16. Cấp phê duyệt:

Trưởng Khoa **Trưởng BỘ MÔN** **Nhóm Biên soạn**

Cập nhật lần 1	**Người Cập nhật** **Tổ trưởng bộ môn**
Cập nhật lần 2	**Người Cập nhật** **Tổ trưởng bộ môn**