BỘ GD&ĐT **CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM**
Trường đại học SPKT **Độc lập – Tự do – Hạnh phúc**
Khoa: CNTT *******

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

4. Phân bố thời gian: (học kỳ 15 tuần) 3(2:1:6)

5. 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

6. Điều kiện tham gia học tập học phần

Môn học tiên quyết: không

Môn học trước: Mạng máy tính căn bản

7. Mô tả tóm tắt học phần

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.

8**. Chuẩn đầu ra của học phần**

Kiến thức:

8.1/ Trình bày được vai trò của hệ thống giám sát trong hệ thống mạng

8.2/ Trình bày được đặc điểm của các loại lỗ hổng mạng

8.3/ Trình bày được tổng quan về hệ thống phát hiện và phòng chống xâm nhập mạng

8.4/ Trình bày được 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

8.5/ Trình bày đặc điểm và nguyên lý hoạt động của giao thức ICMP và SNMP

8.6/ Trình bày được vai trò của ICMP và SNMP trong hệ thống giám sát mạng

8.7/ 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

8.8/ Trình bày được vai trò của việc quản lý Syslog tập trung

8.9/ Trình bày được vai trò của hệ thống phát cảnh báo trong hệ thống giám sát mạng.

8.10/ Trình bày được đặc điểm của việc giám sát qua: giao diện Web, Email, phát âm thanh và phát tín hiệu qua điện thoại di động.

Kỹ năng:

8.11/ Cài đặt và cấu hình được các công cụ phân tích lổ hổng mạng

8.12/ Cài đặt và cấu hình được 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

8.13/ Cài đặt và cấu hình được hệ thống phát cảnh báo qua Web, Email, âm thanh, điện thoại di động

Thái độ nghề nghiệp:

8.14/ Có thái độ nghiêm túc trong nghiên cứu

8.15/ Hình thành nhận thức về phát hiện vấn đề - thu thập thông tin – xử lý các lỗi trong quá trình cài đặt và cấu hình các dịch vụ mạng căn bản

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

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

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

- Đánh giá quá trình: 30% trong đó có các hình thức đánh giá:

  + Tham dự lớp: 10%

  + Bài tập: 20%

- Thi cuối học kỳ: 70% - thi tự luận đề mở (thời gian tối thiểu 60 phút)

13. Thang điểm: 10

14. Kế hoạch thực hiện (Nội dung chi tiết) học phần theo tuần (15)

Tuần thứ 1-2: ***Chương 1: Tổng quan về hệ thống giám sát mạng*** *(6/0/12)*	**Dự kiến các CĐR được thực hiện sau khi kết thúc Chương**

- *Các nội dung GD chính trên lớp: (6)* + 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	8.1/ Trình bày được vai trò của hệ thống giám sát trong hệ thống mạng 8.2/ Trình bày được đặc điểm của các loại lổ hổng mạng 8.3/ Trình bày được tổng quan về hệ thống phát hiện và phòng chống xâm nhập mạng 8.11/ Thành thạo trong việc cài đặt và cấu hình các công cụ phân tích lổ hổng mạng
-*Các nội dung cần tự học ở nhà: (12)*	**Dự kiến các CĐR được thực hiện sau khi tự học**
+ Đọc thêm: nội dung liên quan -*Tài liệu học tập cần thiết* + GT của Rafeeq UR Rehman	8.1/ Trình bày được vai trò của hệ thống giám sát trong hệ thống mạng 8.2/ Trình bày được đặc điểm của các loại lổ hổng mạng 8.3/ Trình bày được tổng quan về hệ thống phát hiện và phòng chống xâm nhập mạng 8.11/ Thành thạo trong việc cài đặt và cấu hình các công cụ phân tích lổ hổng mạng

Tuần thứ 3-4: ***Chương 2:*** **Các thành phần trong hệ thống giám sát mạng** *(6/0/12)*	
- *Các nội dung học tập chính trên lớp:* + Giám sát tấn công + Giám sát lưu lượng + Giám sát thiết bị + Giám sát dịch vụ + Thành phần cảnh báo - *PPGD chính:* + Trình chiếu Powerpoint + Thuyết trình	8.4/ Trình bày được 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 8.12/ Thành thạo trong việc 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

-*Các nội dung cần tự học ở nhà (12):*	
+ Đọc thêm: phương pháp giám sát tấn công, lưu lượng, cảnh báo *Tài liệu học tập cần thiết* + GT: Tài liệu của D. Andrew R. Baker, Dinangkur Kundu, Max Schubert, David Josephsen	8.4/ Trình bày được 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 8.12/ Thành thạo trong việc 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

Tuần thứ 5-7: *Chương 3:* Các giao thức trong giám sát mạng*(9/0/18)*	
- *Các nội dung học tập chính trên lớp:* + ICMP + SNMP - *PPGD chính:* + Trình chiếu Powerpoint + Thuyết trình + Làm mẫu	8.5/ Trình bày đặc điểm và nguyên lý hoạt động của giao thức ICMP và SNMP 8.6/ Trình bày được vai trò của ICMP và SNMP trong hệ thống giám sát mạng 8.12/ Thành thạo trong việc 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
-*Các nội dung cần tự học ở nhà (18):*	
+ Đọc thêm: ICMP và SNMP *Tài liệu học tập cần thiết (yêu cầu phải thống nhất với mục 11 nêu trên)* + GT của Douglas Mauro, Kevin Schmidt, ”Essential SNMP 2nd Edition”, Oreilly, 2005	8.5/ Trình bày đặc điểm và nguyên lý hoạt động của giao thức ICMP và SNMP 8.6/ Trình bày được vai trò của ICMP và SNMP trong hệ thống giám sát mạng 8.12/ Thành thạo trong việc 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

Tuần thứ 8-10: *Chương 4: Quản lý Syslog tập trung*	

(9/0/18)	
- *Các nội dung học tập chính trên lớp:* + 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	8.7/ 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 8.8/ Trình bày được vai trò của việc quản lý Syslog tập trung 8.12/ Thành thạo trong việc 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
-*Các nội dung cần tự học ở nhà (18):*	
+ Đọc thêm: nội dung liên quan *Tài liệu học tập cần thiết* + GT của Dinangkur Kundu, Wojciech Kocjan	8.7/ 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 8.8/ Trình bày được vai trò của việc quản lý Syslog tập trung

Tuần thứ 11-12: ***Chương 5:*** Hệ thống cảnh báo *(6/0/12)*	
- *Các nội dung học tập chính trên lớp:* + Giới thiệu + Cảnh báo qua giao diện Web + Cảnh báo qua Email + Cảnh báo bằng phát âm thanh + Cảnh báo qua điện thoại di động - *PPGD chính:* + Trình chiếu Powerpoint + Thuyết trình + Làm mẫu	8.9/ Trình bày được vai trò của hệ thống phát cảnh báo trong hệ thống giám sát mạng. 8.10/ Trình bày được đặc điểm của việc giám sát qua: giao diện Web, Email, phát âm thanh và phát tín hiệu qua điện thoại di động. 8.12/ Thành thạo trong việc 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

-Các nội dung cần tự học ở nhà(12):	
+ Đọc thêm: nội dung liên quan trong tài liệu tham khảo *Tài liệu học tập cần thiết (yêu cầu phải thống nhất với mục 11 nêu trên)* + GT trong danh mục tài liệu tham khảo	8.9/ Trình bày được vai trò của hệ thống phát cảnh báo trong hệ thống giám sát mạng. 8.10/ Trình bày được đặc điểm của việc giám sát qua: giao diện Web, Email, phát âm thanh và phát tín hiệu qua điện thoại di động. 8.12/ Thành thạo trong việc 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

Tuần thứ 13: ***Thực hành tại phòng máy*** *(0/3/6)*	
- 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	8.9/ Trình bày được vai trò của hệ thống phát cảnh báo trong hệ thống giám sát mạng. 8.10/ Trình bày được đặc điểm của việc giám sát qua: giao diện Web, Email, phát âm thanh và phát tín hiệu qua điện thoại di động. 8.13/ Thành thạo trong việc cài đặt và cấu hình hệ thống phát cảnh báo qua Web, Email, âm thanh, điện thoại di động
-Các nội dung cần tự học ở nhà:	
+ Đọc thêm: nội dung liên quan *Tài liệu học tập cần thiết* + GT trong danh mục tài liệu tham khảo	8.9/ Trình bày được vai trò của hệ thống phát cảnh báo trong hệ thống giám sát mạng. 8.10/ Trình bày được đặc điểm của việc giám sát qua: giao diện Web, Email, phát âm thanh và phát tín hiệu qua điện thoại di động. 8.13/ Thành thạo trong việc cài đặt và cấu hình hệ thống phát cảnh báo qua Web, Email, âm

	thanh, điện thoại di động

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

14. Ngày phê duyệt lần đầu:

15. 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**