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: An Ninh Mạng **Mã học phần:** NSEC430880

2. Tên tiếng Anh: Networks Security

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. Nguyễn Đăng Quang

6. Điều kiện tham gia học tập học phần

Môn học tiên quyết: không

Môn học trước: Mạng máy tính nâng cao

7. Mô tả tóm tắt học phần

Môn học này cung cấp kiến thức về 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.

8**. Chuẩn đầu ra của học phần**

Kiến thức:

8.1/ Giải thích nguyên nhân dẫn đến việc tấn công mạng máy tính

8.2/ Phân loại và trình bày được đặc điểm cơ bản các lỗ hổng trong hệ thống mạng

8.3/ Phân được được các nhóm giải pháp sử dụng để phát hiện và phòng chống xâm nhập mạng

8.4/ Trình bày được vai trò của mã hoá dữ liệu trong an toàn thông tin và truyền tin trên mạng

8.5/ Trình bày được đặc điểm và thuật toán của một số giao thức mã hoá phổ biến

8.6/ Trình bày được vai trò của các công cụ giám sát của hệ thống mạng

8.7/ Trình bày được các đặc điểm chính của các công cụ phân tích lỗ hổng trong các thiết bị và giao thức mạng.

8.8/ Áp dụng một số công cụ giám sát và phân tích lổ hổng mạng vào hệ thống mạng

8.9/ Trình bày được vai trò của việc bảo mật hạ tầng mạng

8.10/ Trình bày được đặc điểm và cơ chế hoạt động của Firewall, VPN, NAT, IDS/IPS

8.11/ Áp dụng các kỹ thuật Firewall, NAT, VPN, IDS/IPS vào hệ thống mạng

8.12/ Trình bày được vai trò của việc thiết lập các chính sách bảo mật trong an ninh mạng

8.13/ Trình bày được vai trò của IDS/IPS trong hệ thống mạng

8.14/ Trình bày được cơ chế hoạt động trong việc phát hiện và phòng chống xâm nhập cua hệ thống IDS/IPS

8.15/ Trình bày được vai trò của hệ thống cảnh báo trong IDS/IPS

8.16/ Áp dụng IDS/IPS vào hệ thống mạng

8.17/ Trình bày được vai trò của hệ thống an ninh cho tầng ứng dụng

8.18/ Trình bày được các lỗ hổng phổ biến trong các dịch vụ Web, Email,…

8.19/ Trình bày được các giải pháp an ninh cho các dịch vụ Web, Email,…

Kỹ năng:

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

8.21/ Cài đặt và cấu hình được các firewal, IDS/IPS

8.22/ Phân tích được các lỗ hổng ở tầng ứng dụng

Thái độ nghề nghiệp:

8.23/ Có thái độ nghiêm túc trong nghiên cứu

8.24/ 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

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 An Ninh Mạng của khoa CNTT – ĐH SPKT Tp.HCM
- Sách tham khảo:

- Steve Manzuik, Ken Pfeil, Andre, *"Network Security Assessment"*, Syngress, 2007.
- Nei Daswani, Christoph Kern, Anita Kesavan, *"Foundation of Security"*, Apress, 2007.
- Justin Clarke, Nittesh Dhanjani, *"Network security Tools"*, O'Reilly, 2005
- Anne Henmi, Mark Lucas, Abhishek Singh, Chris Cantrell, *"Firewall Policies and VPN Configurations"*, Syngress, 2006

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 (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 bảo mật 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/ Giải thích nguyên nhân dẫn đến việc tấn công mạng máy tính 8.2/ Phân loại và trình bày được đặc điểm cơ bản các lỗ hổng trong hệ thống mạng 8.3/ Phân được được các nhóm giải pháp sử dụng để phát hiện và phòng chống xâm nhập mạng 8.20/ 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: Các cuộc tấn công mạng máy tính lớn trong lịch sử và các giải pháp hạn chế mức độ nguy hại của các loại tấn công này + các nội dung liên quan đến bài học -*Tài liệu học tập cần thiết* + Steve Manzuik, Ken Pfeil, Andre,*"Network Security Assessment"*, Syngress, 2007. + Nei Daswani, Christoph Kern, Anita Kesavan, *"Foundation of Security"*, Apress, 2007.	8.1/ Giải thích nguyên nhân dẫn đến việc tấn công mạng máy tính

Tuần thứ 3-4: ***Chương 2:*** **Cryptography - Mã hóa** *(6/0/12)*	
- *Các nội dung học tập chính trên lớp:* + Căn bản về mã hóa + Một số kỹ thuật mã hóa - *PPGD chính:* + Trình chiếu Powerpoint + Thuyết trình	8.4/ Trình bày được vai trò của mã hoá dữ liệu trong an toàn thông tin và truyền tin trên mạng 8.5/ Trình bày được đặc điểm và thuật toán của một số giao thức mã hoá phổ biến
-*Các nội dung cần tự học ở nhà (12):*	

+ Đọc thêm *Tài liệu học tập cần thiết* + Steve Manzuik, Ken Pfeil, Andre,*"Network Security Assessment"*, Syngress, 2007. + Nei Daswani, Christoph Kern, Anita Kesavan, *"Foundation of Security"*, Apress, 2007.	

Tuần thứ 5-7: *Chương 3:* Các công cụ phân tích, đánh giá an ninh mạng – Network security analysis tools*(9/0/18)*	
- *Các nội dung học tập chính trên lớp:* + Port and connection monitoring + Port scanning + Network sniffing + Vulnerability scanning - *PPGD chính:* + Trình chiếu Powerpoint + Thuyết trình + Làm mẫu	8.6/ Trình bày được vai trò của các công cụ giám sát của hệ thống mạng 8.7/ Trình bày được các đặc điểm chính của các công cụ phân tích lỗ hổng trong các thiết bị và giao thức mạng. 8.8/ Áp dụng một số công cụ giám sát và phân tích lổ hổng mạng vào hệ thống mạng 8.20/ 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 (18):*	
+ Đọc thêm: các nội dung liên quan *Tài liệu học tập cần thiết* + Justin Clarke, Nittesh Dhanjani,*"Network security Tools"*, O'Reilly, 2005	

Tuần thứ 8-10: *Chương 4:* Bảo mật hạ tầng mạng - Infrastructure security*(9/0/18)*	

- *Các nội dung học tập chính trên lớp:* + Giới thiệu + Firewall + VPN + VLAN + NAT + Media security + IDS/IPS + Network security policy - *PPGD chính:* + Trình chiếu Powerpoint + Thuyết trình + Làm mẫu	8.9/ Trình bày được vai trò của việc bảo mật hạ tầng mạng 8.10/ Trình bày được đặc điểm và cơ chế hoạt động của Firewall, VPN, NAT, IDS/IPS 8.11/ Áp dụng các kỹ thuật Firewall, NAT, VPN, IDS/IPS vào hệ thống mạng 8.12/ Trình bày được vai trò của việc thiết lập các chính sách bảo mật trong an ninh mạng
-*Các nội dung cần tự học ở nhà (18):*	
+ Đọc thêm: các nội dung liên quan *Tài liệu học tập cần thiết* + Anne Henmi, Mark Lucas, Abhishek Singh, Chris Cantrell, *"Firewall Policies and VPN Configurations"*, Syngress, 2006 + Steve Manzuik, Ken Pfeil, Andre,*"Network Security Assessment"*, Syngress, 2007. + Nei Daswani, Christoph Kern, Anita Kesavan, *"Foundation of Security"*, Apress, 2007.	

Tuần thứ 11-12: *Chương 5:* Hệ thống phát hiện và phòng chống xâm nhập*(6/0/12)***	
- *Các nội dung học tập chính trên lớp:* + Vài trò của IDS/IPS trong hệ thống mạng + Đặc điểm của IDS/IPS + Nguyên tắc hoạt động của IDS/IPS + Khảo sát một số IDS/IPS phổ biến + IDS/IPS dựa vào nguồn mở - *PPGD chính:* + Trình chiếu Powerpoint + Thuyết trình	8.13/ Trình bày được vai trò của IDS/IPS trong hệ thống mạng 8.14/ Trình bày được cơ chế hoạt động trong việc phát hiện và phòng chống xâm nhập cua hệ thống IDS/IPS 8.15/ Trình bày được vai trò của hệ thống cảnh báo trong IDS/IPS 8.16/ Áp dụng IDS/IPS vào hệ thống mạng 8.21/ Thành thạo trong việc cài đặt và cấu hình các firewal,

+ Làm mẫu	IDS/IPS
-*Các nội dung cần tự học ở nhà (12):*	
+ Đọc thêm: các nội dung liên quan *Tài liệu học tập cần thiết* + Anne Henmi, Mark Lucas, Abhishek Singh, Chris Cantrell, *"Firewall Policies and VPN Configurations"*, Syngress, 2006 + Steve Manzuik, Ken Pfeil, Andre,*"Network Security Assessment"*, Syngress, 2007. + Nei Daswani, Christoph Kern, Anita Kesavan, *"Foundation of Security"*, Apress, 2007.	

Tuần thứ 13: ***Thực hành tại phòng máy*** *(0/3/6)*	
- *Các nội dung học tập chính trên lớp:* + Cài đặt IDS/IPS mã nguồn mở + Thực hiện tấn công và phân tích cách phòng chống dựa vào IDS/IPS - *PPGD chính:* + Trình chiếu Powerpoint + Thuyết trình + Làm mẫu	8.14/ Trình bày được cơ chế hoạt động trong việc phát hiện và phòng chống xâm nhập cua hệ thống IDS/IPS 8.16/ Áp dụng IDS/IPS vào hệ thống mạng 8.21/ Thành thạo trong việc cài đặt và cấu hình các firewal, IDS/IPS
-*Các nội dung cần tự học ở nhà (6):*	
+ Đọc thêm: các nội dung liên quan *Tài liệu học tập cần thiết* + Steve Manzuik, Ken Pfeil, Andre,*"Network Security Assessment"*, Syngress, 2007. + Nei Daswani, Christoph Kern, Anita Kesavan, *"Foundation of Security"*, Apress, 2007.	

Tuần thứ 14: ***Chương 6:*** **An ninh ứng dụng - Application Security** *(3/0/6)*	
- *Các nội dung học tập chính trên lớp:* + Remote access security + Web security + Email security + Buffer overflow - *PPGD chính:* + Trình chiếu Powerpoint + Thuyết trình + Làm mẫu	8.17/ Trình bày được vai trò của hệ thống an ninh cho tầng ứng dụng 8.18/ Trình bày được các lỗ hổng phổ biến trong các dịch vụ Web, Email,… 8.19/ Trình bày được các giải pháp an ninh cho các dịch vụ Web, Email,… 8.22/ Thành thạo trong việc phân tích các lỗ hổng ở tầng ứng dụng
-*Các nội dung cần tự học ở nhà (6):*	
+ Đọc thêm: các nội dung liên quan *Tài liệu học tập cần thiết* + Steve Manzuik, Ken Pfeil, Andre,*"Network Security Assessment"*, Syngress, 2007. + Nei Daswani, Christoph Kern, Anita Kesavan, *"Foundation of Security"*, Apress, 2007.	
Tuần thứ 15: ***Thực hành tại phòng máy*** *(0/3/6)*	
- *Các nội dung học tập chính trên lớp:* + Remote access security + Web security + Email security + Buffer overflow - *PPGD chính:* + Trình chiếu Powerpoint + Thuyết trình + Làm mẫu	8.18/ Trình bày được các lỗ hổng phổ biến trong các dịch vụ Web, Email,… 8.19/ Trình bày được các giải pháp an ninh cho các dịch vụ Web, Email,… 8.22/ Thành thạo trong việc phân tích các lỗ hổng ở tầng ứng dụng
-*Các nội dung cần tự học ở nhà (6):*	
+ Đọc thêm: các nội dung liên quan *Tài liệu học tập cần thiết* + Steve Manzuik, Ken Pfeil, Andre,*"Network Security Assessment"*, Syngress, 2007.	

+ Nei Daswani, Christoph Kern, Anita Kesavan, *"Foundation of Security"*, Apress, 2007.	

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: 15/01/2012

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**