CUSC®
ISO 9001:2015
Computer Education

AN TOÀN VÀ AN NINH THÔNG TIN NĂM 2023

Software CUSC Academics Counselling

Trung tâm Công nghệ Phần mềm Đại học Cần Thơ
01 Lý Tự Trọng – Quận Ninh Kiều – TP. Cần Thơ

LỜI MỞ ĐẦU

Với chủ đề "An toàn, an ninh mạng Make in Viet Nam – Yếu tố then chốt trong chuyển đổi số quốc gia" diễn ra vào tháng 12/2020, Việt Nam đang hòa vào xu thế chung của nhiều quốc gia trên thế giới đẩy mạnh cuộc cách mạng công nghiệp lần thứ tư và quá trình Chuyển đổi số. Vì thế, việc phát triển năng lực quốc gia về an toàn, an ninh thông tin là điều kiện tiên quyết để xây dựng Chính phủ điện tử, xây dựng kinh tế số, phục vụ hoạt động của Nhà nước, doanh nghiệp và người dân.

Cùng với phát triển của mạng Internet, tình hình mất an ninh mạng đang diễn biến phức tạp và xuất hiện nhiều nguy cơ đe dọa nghiêm trọng đến việc ứng dụng Công nghệ Thông tin phục vụ phát triển kinh tế xã hội và đảm bảo quốc phòng, an ninh. Số vụ tấn công trên mạng và các vụ xâm nhập hệ thống công nghệ thông tin nhằm do thám, trục lợi, phá hoại dữ liệu, ăn cắp tài sản, cạnh tranh không lành mạnh và một số vụ việc mất an toàn thông tin số khác đang gia tăng ở mức báo động về số lượng, đa dạng về hình thức, tinh vi về công nghệ...

Căn cứ vào nội dung quyết định phê duyệt "Chương trình Chuyển đổi số Quốc gia đến năm 2025, định hướng đến năm 2030" của Thủ tướng Chính phủ vào ngày 03/06/2020; Quyết định số 21/QĐ-TTg, phê duyệt đề án "Đào tạo và phát triển nguồn nhân lực an toàn thông tin giai đoạn 2021-2025" và Quyết định phê duyệt "Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ CNTT phục vụ Chính phủ điện tử đến năm 2020, định hướng đến năm 2025" của Thủ tướng Chính Phủ, Trung tâm Công nghệ Phần mềm Đại học Cần Thơ (CUSC) xin giới thiệu đến quý Sở, Ban, Ngành chương trình đào tạo Công nghệ Thông tin (CNTT) về lĩnh vực An toàn an ninh thông tin cho các đối tượng là lãnh đạo, cán bộ, công chức, viên chức hiện đang công tác tại các cơ quan, Ban, Ngành thuộc lĩnh vực CNTT và Truyền thông.

Trước yêu cầu cấp bách của xã hội trong lĩnh vực đào tạo chuyên gia An ninh thông tin, chúng tôi xây dựng chương trình đào tạo nhằm định hướng cho người học vừa có kỹ năng đáp ứng được yêu cầu của công nghệ hiện đại vừa có kiến thức nền tảng cho phép tiếp tục nâng cao và mở rộng kiến thức nhằm thích ứng với nhu cầu về an ninh thông tin.

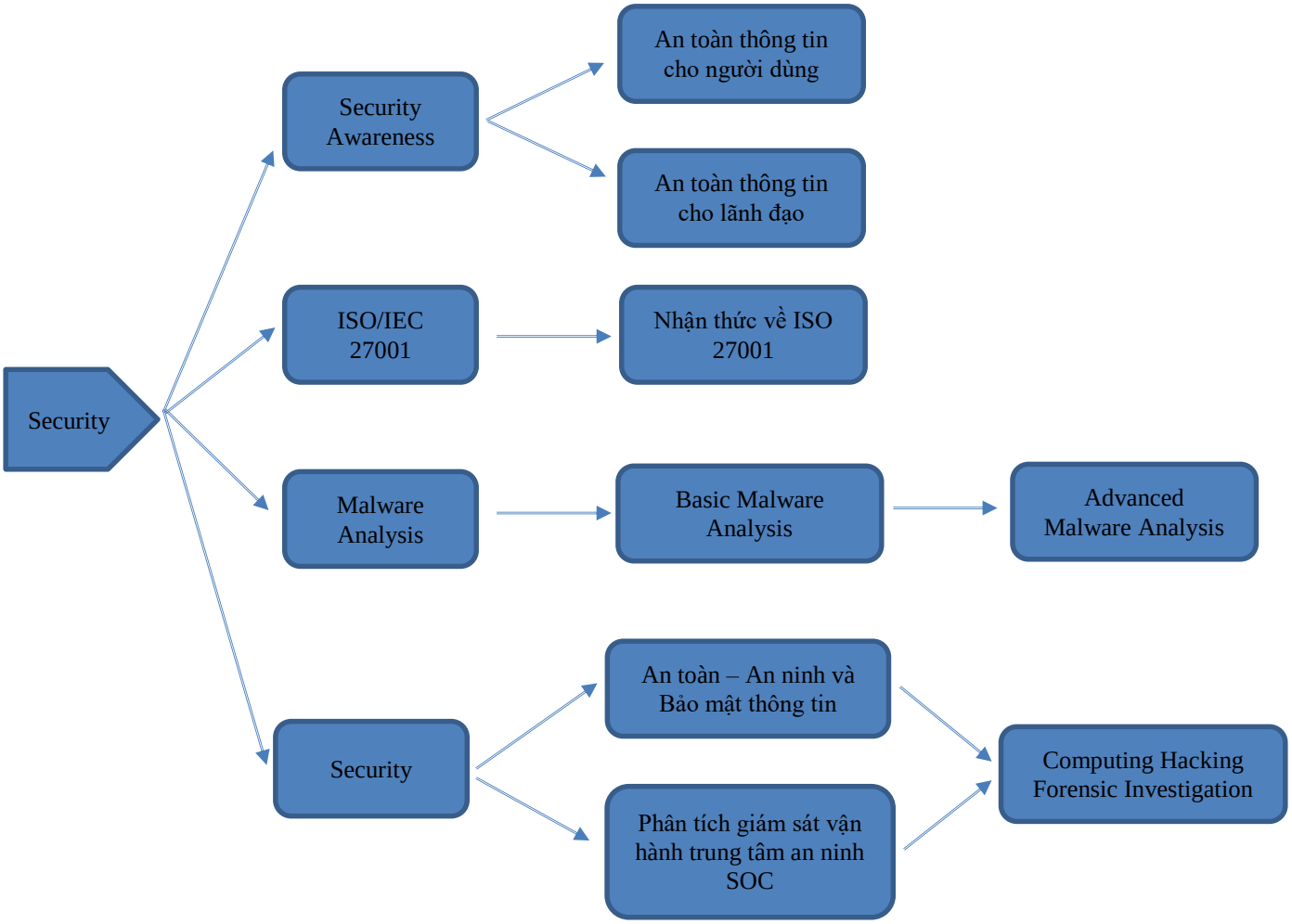
Ngoài ra, nội dung đào tạo còn chú trọng đến việc bảo mật hệ thống trên nhiều nền tảng khác nhau từ máy chủ, hệ thống thông tin của đơn vị đến bảo mật không gian mạng, bảo mật IoT, và bảo mật điện toán đám mây (Cloud). Người học được trang bị kiến thức nền

tảng để có thể tham dự các kỳ thi lấy chứng chỉ quốc tế của các tập đoàn công nghệ lớn như: Chứng chỉ **CCNA (Cisco Certified Network Associate), Ethical Hacking, Điều tra tội phạm máy tính – CHFI của EC Council, chứng chỉ Aptech của Ấn Độ**.

Trung tâm Công nghệ Phần mềm Đại học Cần Thơ tin rằng sự hợp tác giữa Quý Sở và Trung tâm sẽ góp phần bồi dưỡng và đào tạo nhân lực chuyên nghiệp trong lĩnh vực An toàn an ninh thông tin của tỉnh/ thành trong thời gian tới.

STT	TÊN KHÓA HỌC	THỜI GIAN (giờ)	GHI CHÚ
I. NHÓM 1: AN NINH, BẢO MẬT THÔNG TIN (SECURITY)			
1.	An toàn, an ninh thông tin cho mọi người	32	
2.	Nhận thức về Tiêu chuẩn ISO: 27001	24	
3.	Phân tích mã độc cơ bản (Basic malware analysis)	32	
4.	Phân tích mã độc nâng cao	40	
5.	An toàn an ninh và bảo mật thông tin	40	
6.	Điều tra tội phạm máy tính (Computer Hacking and Forensic Investigation)	40	
7.	Nhận thức và triển khai chuyển đổi IPv6	24	
8.	Phân tích giám sát vận hành trung tâm an ninh (Security Operations Center - SOC)	32	
II. NHÓM 2: QUẢN TRỊ MẠNG THEO CÔNG NGHỆ MICROSOFT			
9.	Ảo hóa với Windows Server Hyper-V (Server Virtualization with Window Server Hyper-V)	40	
10.	Quản trị hệ thống mạng với Windows Server 2019 (Windows Server 2019 Administration)	40	
III. NHÓM 3: QUẢN TRỊ THIẾT BỊ MẠNG (HARDWARE)			
11.	Xử lý các sự cố thông dụng trên máy tính (PC Troubleshooting)	24	
12.	Network and Routing	24	
13.	Thiết kế và cài đặt mạng (Network Design & Installation)	24	

LỘ TRÌNH CÁC KHÓA TẬP HUẤN
QUẢN TRỊ MẠNG, AN TOÀN VÀ AN NINH THÔNG TIN



I. NHÓM 1: AN NINH, BẢO MẬT THÔNG TIN (SECURITY)

1. An toàn, an ninh thông tin cho mọi người

- **Đối tượng:**
  - Học viên có kiến thức cơ bản tin học và quan tâm đến vấn đề an ninh mạng.
  - Những người yêu thích Công nghệ Thông tin (CNTT).
- **Mục tiêu:**
  - Cung cấp cho học viên kiến thức về những nguy cơ mất dữ liệu, mất thông tin, kiến thức về an toàn an ninh thông tin, cung cấp những giải pháp cụ thể trong việc bảo vệ an toàn an ninh thông tin bao gồm thông tin cá nhân, email, điện thoại, mạng xã hội,...
  - Thiết lập các chính sách bảo mật cho thông tin trên máy tính, các chính sách bảo mật cho thông tin cho email cá nhân, tài khoản mạng xã hội và chế độ bảo mật thông tin trên thiết bị di động.
- **Thời gian:** 32 giờ
- **Kiến thức đạt được:**
  - Chương trình được xây dựng phù hợp với nhu cầu thực tế theo thông tư của Bộ Thông tin và Truyền thông về đẩy mạnh an toàn an ninh thông tin cho người dùng cuối và cho đơn vị.
  - Cung cấp các kiến thức về cách thức hacker sử dụng để đánh cắp thông tin.
  - Đưa ra các giải pháp cụ thể cho từng trường hợp để đảm bảo an toàn an ninh thông tin.
  - Cung cách các bước thiết lập bảo mật thông tin trong các tình huống cụ thể: thông tin cá nhân, email, điện thoại, mạng xã hội,...

2. Nhận thức về Tiêu chuẩn ISO: 27001

- **Đối tượng:**
  - Cán bộ của tổ chức nằm trong phạm vi triển khai của hệ thống quản lý ANTT
  - Đánh giá viên, những người muốn hiểu đầy đủ về quá trình thực hiện hệ thống quản lý an ninh thông tin

- **Mục tiêu:**
  - Hiểu phương pháp triển khai hệ thống an toàn thông tin (ISMS) theo ISO/ IEC 27001:2013
  - Tăng sự hiểu biết toàn diện về các khái niệm, tiêu chuẩn, phương pháp và kỹ thuật cần thiết cho việc quản lý hiệu quả của một hệ thống quản lý an toàn thông tin
  - Hiểu mối quan hệ giữa các thành phần của một hệ thống quản lý an ninh thông tin, bao gồm cả quản lý rủi ro, kiểm soát và tuân thủ các yêu cầu của các bên liên quan khác nhau của tổ chức
  - Có được chuyên môn cần thiết để hỗ trợ tổ chức trong việc thực hiện, quản lý và duy trì một hệ thống ISMS theo quy định tại tiêu chuẩn ISO/ IEC 27001:2013
  - Nắm được những yêu cầu/ điều khoản cơ bản của tiêu chuẩn
  - Bước đầu nhận biết và xác định được những tài sản thông tin của Tổ chức nơi mình đang làm việc cũng như cách thức phòng tránh, chấp nhận và xử lý rủi ro gây ra bởi sự rò rỉ và phá vỡ thông tin
  - Phát triển kiến thức và kỹ năng cần thiết để tư vấn cho các tổ chức về thực hành tốt nhất trong việc quản lý an toàn thông tin
- **Thời gian:** 24 giờ
- **Kiến thức đạt được:**
  - Khóa học được xây dựng dựa trên nhu cầu thực tế của cơ quan/doanh nghiệp.
  - Chương trình mang đến cho học viên khối lượng kiến thức đầy đủ để học viên tự tin làm việc trong những môi trường chuyên nghiệp nhất, có kiến thức chuyên sâu về:
    1. Đánh giá nội bộ ISO 27001
    2. Xây dựng chính sách An toàn thông tin
    3. Bảo mật hệ thống mảy chủ
    4. Triển khai an toàn thông tin cho doanh nghiệp, tổ chức
    5. Duy trì hệ thống Quản lý An ninh thông tin

- Học viên được học và thực hành dựa trên các tình huống thật để tích lũy được kinh nghiệm thực tế.
- Giảng viên có kinh nghiệm trong quản trị và đảm bảo an ninh của hệ thống mạng.

3. Phân tích mã độc cơ bản (Basic malware analysis)

➢ **Đối tượng:**

Công chức, viên chức, các đơn vị phụ trách CNTT tại:

- Sở Thông tin và Truyền thông
- Trung tâm Công nghệ Thông tin và Truyền thông
- Uỷ ban Nhân dân tỉnh
- Văn phòng Tỉnh ủy
- Các Sở ban ngành tỉnh
- Uỷ ban Nhân dân huyện, thị xã, thành phố
- Phòng Văn hóa Thông tin huyện, thị xã, thành phố
- Các cơ quan Đảng; Tổ chức chính trị - xã hội

➢ **Mục tiêu:**

- Cung cấp các kiến thức tổng quát về cách thức nhận diện và phân loại Malware.
- Cung cấp các kiến thức chuyên sâu về nền tảng của hệ điều hành, các thành phần phần cứng máy tính, một số lỗ hổng và cách thức Malware lây nhiễm vào hệ thống dựa trên những lỗ hổng trên
- Cung cấp các kiến thức chi tiết về thủ thuật được Malware sử dụng để bảo vệ bản thân, chống lại các chương trình diệt Virus cũng như các hoạt động phân tích và dịch ngược Malware.
- Cung cấp chi tiết các phương pháp, công cụ và kĩ thuật phân tích, phát hiện Malware như so trùng chữ kí, kiểm tra trong môi trường ảo hóa, kiểm tra bằng Model Checking, static analysis, dynamic analys và phương pháp lai ghép.
- Xác định phương án, cách thức xử lý mã độc hại.

- **Thời gian:** 32 giờ
- **Kiến thức đạt được:**

Nội dung khóa học được thiết kế theo nhu cầu thực tế.

- Chương trình được xây dựng phù hợp với chuẩn sử dụng CNTT nâng cao theo thông tư của Bộ Thông tin và Truyền thông về mạnh an toàn an ninh thông tin cho người dùng cuối và cho đơn vị.
- Cung cấp các kiến thức về cách thức hacker sử dụng để đánh cắp thông tin.
- Đưa ra các giải pháp cụ thể cho từng trường hợp để đảm bảo an toàn an ninh thông tin.
- Cung cách các bước thiết lập bảo mật thông tin trong các tình huống cụ thể: thông tin cá nhân, email, điện thoại, mạng xã hội,...

4. Phân tích mã độc nâng cao (Advanced malware analysis)

- **Đối tượng:**

Công chức, viên chức, các đơn vị phụ trách CNTT tại:

- Sở Thông tin và Truyền thông
- Trung tâm Công nghệ Thông tin và Truyền thông
- Uỷ ban Nhân dân tỉnh
- Văn phòng Tỉnh ủy
- Các Sở ban ngành tỉnh
- Uỷ ban Nhân dân huyện, thị xã, thành phố
- Phòng Văn hóa Thông tin huyện, thị xã, thành phố
- Các cơ quan Đảng; Tổ chức chính trị - xã hội

- **Mục tiêu:**

- Cung cấp các kiến thức tổng quát về cách thức nhận diện và phân loại Malware.
- Cung cấp các kiến thức chuyên sâu về nền tảng của hệ điều hành, các thành phần phần cứng máy tính, một số lỗ hổng và cách thức Malware lây nhiễm vào hệ thống dựa trên những lỗ hổng trên.

- Cung cấp các kiến thức chi tiết về thủ thuật được Malware sử dụng để bảo vệ bản thân, chống lại các chương trình diệt Virus cũng như các hoạt động phân tích và dịch ngược Malware.
- Cung cấp chi tiết các phương pháp, công cụ và kĩ thuật phân tích, phát hiện Malware như so trùng chữ kí, kiểm tra trong môi trường ảo hóa, kiểm tra bằng Model Checking, static analysis, dynamic analys và phương pháp lai ghép.
- Xác định phương án, cách thức xử lý mã độc hại.

➢ **Thời gian:** 40 giờ

➢ **Kiến thức đạt được:**

- Nội dung khóa học được thiết kế theo nhu cầu thực tế.
- Chương trình được xây dựng phù hợp với chuẩn sử dụng CNTT nâng cao theo thông tư của Bộ Thông tin và Truyền thông về mạnh an toàn an ninh thông tin cho người dùng cuối và cho đơn vị.
- Cung cấp các kiến thức về cách thức hacker sử dụng để đánh cắp thông tin.
- Đưa ra các giải pháp cụ thể cho từng trường hợp để đảm bảo an toàn an ninh thông tin.
- Cung cách các bước thiết lập bảo mật thông tin trong các tình huống cụ thể: thông tin cá nhân, email, điện thoại, mạng xã hội,...

5. An toàn an ninh và bảo mật thông tin

➢ **Đối tượng:**

- Học viên có kiến thức về quản trị mạng.
- Ưu tiên các học viên có nền tảng cơ bản về Hacking.

➢ **Mục tiêu:**

- Khóa học giúp cho học viên có thể nắm vững kiến thức về tấn công mạng, phương pháp kiểm tra xâm nhập, phát hiện các tấn công đang diễn ra, cách phòng chống và khắc phục các sự cố về an ninh thông tin.
- Nắm bắt các phương pháp tấn công hệ thống, kỹ thuật giấu tin (steganography), các kiểu tấn công ẩn tin (steganalysis attacks) và tìm hiểu về kỹ thuật xóa dấu vết (covering tracks)

- Cung cấp các kiến thức về tấn công mạng phổ biến (DDOS, XSS, …), khả năng kiểm tra xâm nhập, phân tích tổn thương của hệ thống và phục hồi hệ thống sau tấn công.
- Tìm hiểu về các loại tấn công Webserver khác nhau, cũng như các phương pháp tấn công và cách phòng chống.
- Thực hiện các phân tích lỗ hỏng bảo mật để xác định lỗ hỏng trong hệ thống của doanh nghiệp, cũng như sự truyền tin trong cơ sở hạ tầng hay hệ thống đầu cuối
- Tìm hiểu về các mối nguy hại khác nhau đối với nền tảng IoT và học cách bảo vệ các thiết bị IoT an toàn

➢ **Thời gian:** 40 giờ

➢ **Kiến thức đạt được:**

Sau khi hoàn thành khóa học, học viên có đủ khả năng:

- Trang bị kiến thức nền tảng về các cách thức tấn công của Hacker và làm chủ các kỹ thuật tấn công nâng cao.
- Nhận diện, xác định nguyên nhân, cách thức xâm nhập trái phép hệ thống mạng cơ quan/doanh nghiệp để từ đó đánh giá toàn diện nhất về tình hình an toàn an ninh thông tin của cơ quan/doanh nghiệp.
- Làm quen các kỹ thuật về thăm dò và quét hệ thống và các ứng dụng/dịch vụ vận hành bên trong chúng, qua đó xác định được các thành phần dễ bị tổng thương cũng như các lỗi tiềm ẩn.
- Hiểu được các hoạt động kiểm tra thâm nhập, bao gồm kiểm định bên trong và kiểm định bên ngoài (Áp dụng cho các kiểm định viên hệ thống).
- Biết được các các phương pháp sao lưu và phục hồi hệ thống sau tấn công.
- Sử dụng SSL trong chứng thực các ứng dụng mạng: HTTPS, FTPS,...

6. Điều tra tội phạm máy tính (Computer Hacking and Forensic Investigation)

➢ **Đối tượng:**

Công chức, viên chức, các đơn vị phụ trách CNTT tại:

- Sở Thông tin và Truyền thông

- Trung tâm Công nghệ Thông tin và Truyền thông
- Uỷ ban Nhân dân tỉnh
- Văn phòng Tỉnh ủy
- Các Sở ban ngành tỉnh
- Uỷ ban Nhân dân huyện, thị xã, thành phố
- Phòng Văn hóa Thông tin huyện, thị xã, thành phố
- Các cơ quan Đảng; Tổ chức chính trị - xã hội

➢ **Mục tiêu:**

- Hiểu và vận dụng tốt các dạng tấn công khác nhau trên Windows, Linux từ đó có giải pháp phòng chống hiệu quả.
- Học cách thiết kế các chính sách và tổ chức lưu trữ nhằm đảm bảo an ninh thông tin ở nhiều mức độ khác nhau.
- Vận dụng được nhiều công cụ hiện đại để tấn công và kiểm tra hệ thống mạng máy tính.
- Nắm bắt các chủ đề về điều tra pháp lý, trải nghiệm thực hành với các kỹ thuật điều tra pháp lý khác nhau cũng như các công cụ tiêu chuẩn pháp lý cần thiết để thành công trong việc thực hiện điều tra máy tính và tiến hành truy vết tội phạm mạng
- Các cách thức để tìm kiếm và thu thập các thông tin liên quan đến chứng cứ (chain-of-custody), lưu giữ và bảo toàn chứng cứ để phân tích và báo cáo bằng chứng số

➢ **Thời gian:** 40 giờ

➢ **Kiến thức đạt được:**

- Nội dung khóa học được thiết kế theo nhu cầu thực tế.
- Đào tạo nguồn nhân lực thông tin chất lượng cao về an toàn và an ninh thông tin
- Đào tạo đội ngũ phản ứng nhanh trong việc phòng chống và khắc phục các sự cố an ninh mạng.

7. Nhận thức và triển khai chuyển đổi IPv6

- **Đối tượng:**

  Công chức, viên chức, các đơn vị phụ trách CNTT tại:

  - Sở Thông tin và Truyền thông
  - Trung tâm Công nghệ Thông tin và Truyền thông
  - Uỷ ban Nhân dân tỉnh
  - Văn phòng Tỉnh ủy
  - Các Sở ban ngành tỉnh
  - Uỷ ban Nhân dân huyện, thị xã, thành phố
  - Phòng Văn hóa Thông tin huyện, thị xã, thành phố
  - Các cơ quan Đảng; Tổ chức chính trị - xã hội

- **Mục tiêu:**

  - Cung cấp cho học viên các kiến thức cơ bản về nhận thức sự cần thiết cho việc chuyển đổi IPv4 sang IPv6.
  - Hiểu biết được hoạt động của giao thức IPv6.
  - Nắm bắt sự thay đổi công nghệ IPv4/IPv6 trong sự phát triển Internet trong tương lai. Từ đó đưa ra được kế hoạch chính sách lộ trình áp dụng chuyển đổi phù hợp cho đơn vị mình.

- **Thời gian:** 24 giờ

- **Kiến thức đạt được:**

  - Nắm bắt các vấn đề hiện trạng, quy định chính sách về IPv6; năm bắt công nghệ chuyển đổi IPv6 cho Trung tâm tích hợp dữ liệu, kích hoạt chuyển đổi IPv6 Cổng thông tin điện tử, Cổng dịch vụ công, hệ thống DNS,…
  - Xây dựng kế hoạch, quy hoạch và triển khai mạng IPv6 phù hợp cho đơn vị của mình.

8. Phân tích giám sát vận hành trung tâm an ninh (SOC)

- **Đối tượng:**

  Công chức, viên chức, các đơn vị phụ trách CNTT tại:

  - Sở Thông tin và Truyền thông

- Trung tâm Công nghệ Thông tin và Truyền thông
- Uỷ ban Nhân dân tỉnh
- Văn phòng Tỉnh ủy
- Các Sở ban ngành tỉnh
- Uỷ ban Nhân dân huyện, thị xã, thành phố
- Phòng Văn hóa Thông tin huyện, thị xã, thành phố
- Các cơ quan Đảng; Tổ chức chính trị - xã hội

➢ **Mục tiêu:**

- Cung cấp cho học viên các kiến thức kiến thức tổng quan về Trung tâm vận hành an ninh an toàn thông tin (SOC) và cách vận hành SOC
- Hiểu biết cơ bản và kiến thức chuyên sâu về các mối đe dọa bảo mật, các cuộc tấn công, lỗ hổng bảo mật, hành vi của kẻ tấn công, chuỗi tiêu diệt mạng, v.v.
- Có thể giám sát và phân tích nhật ký và cảnh báo từ nhiều công nghệ khác nhau trên nhiều nền tảng (IDS / IPS, bảo vệ điểm cuối, máy chủ và máy trạm).
- Có kiến thức về quản trị các giải pháp SIEM (Splunk / AlienVault / OSSIM / ELK).
- Hiểu kiến trúc, triển khai và tinh chỉnh các giải pháp SIEM (Splunk / AlienVault / OSSIM / ELK).

➢ **Thời gian:** 32 giờ

➢ **Kiến thức đạt được:**

- Nắm rõ mô hình tổ chức của SOC và nhận diện được các kiến thức, kĩ năng cần thiết cho mỗi vị trí trong SOC
- Nắm bắt các kiến thức liên quan đến việc giám sát, cảnh báo, quản lý sự cố An toàn thông tin và cách thức ứng cố khi có sự cố xảy ra
- Xây dựng các kịch bản, qui trình trong giám sát An toàn thông tin và thực hành triển khai giải pháp SIEM nguồn mở.

II. NHÓM 2: QUẢN TRỊ MẠNG THEO CÔNG NGHỆ MICROSOFT

9. Quản trị hệ thống mạng với Windows Server 2019 (Windows Server 2019 Administration)

- **Đối tượng:**
  - Hoc viên có kiến thức cơ bản về tin học.
  - Những người yêu thích Công nghệ Thông tin.
- **Mục tiêu:**
  - Cung cấp cho học viên kiến thức về hệ thống Windows Server 2019. Từ đó giúp học viên quản trị hiệu quả hệ thống mạng và xây dựng cơ sở hạ tầng mạng cho doanh nghiệp và cơ quan nhà nước.
  - Cung cấp kiến thức nền tảng về Windows Server 2019, nắm vững các nguyên tắc hoạt động, các yêu cầu, các bước trong triển khai hệ thống mạng doanh nghiệp, cơ quan nhà nước và có kiến thức vững chắc để thi các chứng chỉ của Microsoft.
- **Thời gian:** 40 giờ
- **Kiến thức đạt được:**
  - Thiết kế và cài đặt mạng hệ thống mạng theo công nghệ Microsoft
  - Quản trị tài nguyên của hệ thống mạng.
  - Triển khai các dịch vụ trên hệ thống mạng như: Web, FTP, DHCP, AD CS,…
  - Triển khai các chính sách bảo mật cho hệ thống mạng.
  - Phân tích và tìm lỗi, khắc phục lỗi, đánh giá và tối ưu hóa hoạt động của hệ thống mạng.
  - Cung cấp cho học viên kiến thức về phát hiện và khắc phục các lỗi bảo mật qua các ví dụ và thực hành cụ thể.
  - Cung cấp kiến thức về nền tảng ảo hóa Hyper-V và kỹ năng trong việc cấu hình và quản trị hệ thống ảo hóa.
  - Cung cấp kiến thức và kỹ năng trong việc cấu hình và quản trị Windows Azure AD.

10. Ảo hóa với Windows Server Hyper-V (Server Virtualization with Window Server Hyper-V)

- **Đối tượng:**

Công chức, viên chức, các đơn vị phụ trách CNTT tại:

- Sở Thông tin và Truyền thông
- Trung tâm Công nghệ Thông tin và Truyền thông
- Uỷ ban Nhân dân tỉnh
- Văn phòng Tỉnh ủy
- Các Sở ban ngành tỉnh
- Uỷ ban Nhân dân huyện, thị xã, thành phố
- Phòng Văn hóa Thông tin huyện, thị xã, thành phố
- Các cơ quan Đảng; Tổ chức chính trị - xã hội

- **Mục tiêu:**

- Một trong những công nghệ phát triển nhanh chóng và được triển khai rộng rãi nhất hiện nay là ảo hóa máy chủ. Nhiều cơ quan tổ chức đã nhận ra việc tiết kiệm chi phí từ việc triển khai các máy chủ ảo hóa và các chuyên viên hệ thống triển khai và quản lý đối với các hệ thống ảo hóa.
- Ngày càng có nhiều tổ chức triển khai ảo hóa máy tính để bàn, ứng dụng và mạng. Thậm chí còn có những lợi ích bảo mật của ảo hóa khôi phục thảm họa dễ dàng hơn, các điểm kiểm soát duy nhất trên nhiều hệ thống, quyền truy cập dựa trên vai trò cũng như khả năng kiểm tra và ghi nhật ký bổ sung cho các cơ sở hạ tầng lớn.

- **Thời gian:** 40 giờ

- **Kiến thức đạt được:**

- Cung cấp cho học viên các kiến thức về ảo hóa máy chủ
- Khóa học đào tạo kiến thức nâng cao về xây dựng hệ thống ảo hóa trên nền Microsoft Windows Server

III. NHÓM 3: QUẢN TRỊ THIẾT BỊ MẠNG (HARDWARE):

11. Xử lý các sự cố thông dụng trên máy tính (PC Troubleshooting)

- **Đối tượng:**
  - Học viên có kiến thức cơ bản về tin học
  - Những người yêu thích CNTT
- **Mục tiêu:**

  Sau khi hoàn thành khóa học, học viên có đủ khả năng:
  - Hiểu rõ các thành phần của hệ điều hành Windows;
  - Hiểu thông số kỹ thuật của các thành phần phần cứng máy tính;
  - Nắm được các bước lắp ráp, cài đặt, sửa chữa máy tính và mạng LAN;
  - Vận hành và bảo trì cho hệ thống máy tính của các cơ quan của đơn vị;
  - Nắm được các bước lắp ráp, cài đặt, sửa chữa hệ thống mạng của đơn vị.
- **Thời gian:** 24 giờ
- **Kiến thức đạt được:**
  - Khóa học cung cấp kiến thức nền tảng về máy tính và hệ thống mạng máy tính; Hướng dẫn thiết kế và lắp đặt một mạng LAN cơ bản; Hướng dẫn cài đặt phần mềm máy tính.
  - Phân tích, đánh giá được hiện trạng hệ thống máy tính, lập kế hoạch nâng cấp hệ thống máy tính.
  - Khắc phục các sự cố phần cứng máy tính và mạng nội bộ (kết nối mạng nội bộ, chia sẻ dữ liệu cho nhau, in tài liệu qua mạng, …) trong việc quản lý hệ thống máy tính; Lắp ráp nâng cấp các thiết bị phần cứng; Nhận diện, chẩn đoán, sửa chữa máy tính và các thiết bị ngoại vi.
  - Xử lý các sự cố xảy ra trong quá trình triển khai bảo trì (Sao lưu, phục hồi hệ điều hành, ..); Tạo bản ghost (sao lưu) hệ điều hành, bung ghost (phục hồi) hệ điều hành.

12. Thiết kế cài đặt mạng (Network Design & Installation)

- **Đối tượng:**
  - Học viên có kiến thức cơ bản về tin học

- Những người yêu thích CNTT

➢ **Mục tiêu:**

Sau khi hoàn thành khóa học, học viên có đủ khả năng:

- Nắm được cơ bản về hệ thống mạng máy tính; Biết cách thu thập và phân tích yêu cầu trong thiết kế mạng; Nắm được phương pháp thiết kế mô hình mạng.
- Nắm được về mô hình mạng và các giao thức cơ bản trong mạng; Nắm được phương pháp phân đoạn mạng và quy hoạch địa chỉ IP cho mạng.
- Biết cách cấu hình trên một số thiết bị phần cứng: router, switch,…
- Biết cách thiết kế và cấu hình trên phần mềm mô phỏng GNS3; Biết cách kết nối hệ thống máy ảo vào mô hình mạng mô phỏng trong GNS3.

➢ **Thời gian:** 24 giờ

➢ **Kiến thức đạt được:**

- Đưa ra phương pháp cụ thể trong phân đoạn mạng và quy hoạch địa chỉ IP.
- Đưa ra phương pháp quy hoạch và thiết kế mạng LAN, WLAN theo một quy trình hoàn chỉnh.
- Sử dụng phần mềm mô phòng GNS3 trong thiết kế mạng LAN, WLAN và cấu hình trên các thiết bị mạng.
- Cấu hình trên một số thiết bị mạng như: router, switch,…
- Cung cấp nền tảng trong việc thiết kế hệ thống mạng và các dịch vụ bằng cách kết nối hệ thống mạng ảo trong GNS3 và các máy ảo trong VMWARE.

13. Network and Routing

➢ **Đối tượng:**

Công chức, viên chức, các đơn vị phụ trách CNTT tại:

- Sở Thông tin và Truyền thông
- Trung tâm Công nghệ Thông tin và Truyền thông
- Uỷ ban Nhân dân tỉnh
- Văn phòng Tỉnh ủy

- Các Sở ban ngành tỉnh
- Uỷ ban Nhân dân huyện, thị xã, thành phố
- Phòng Văn hóa Thông tin huyện, thị xã, thành phố
- Các cơ quan Đảng; Tổ chức chính trị - xã hội

➢ **Mục tiêu:**

- Cung cấp các kiến thức tổng quát về cách thức thiết kế mô hình mạng.
- Cung cấp các kiến thức cấu hình một số thiết bị phần cứng router, switch
- Cung cấp các kiến thức về phân hoạch, vạch đường cho các gói tin trong hệ thống mạng
- Giới thiệu các kỹ thuật định tuyến căn bản và giải pháp trên nền thiết bị CISCO.
- Biết cách thiết kế và cấu hình trên phần mềm mô phỏng GNS3

➢ **Thời gian:** 24 giờ

➢ **Kiến thức đạt được:**

- Đưa ra phương pháp cụ thể trong phân đoạn mạng và quy hoạch địa chỉ IP.
- Đưa ra phương pháp thiết kế mạng LAN, WLAN theo một quy trình hoàn chỉnh.
- Sử dụng phần mềm mô phòng GNS3 trong thiết kế mạng LAN, WLAN và cấu hình trên các thiết bị mạng.
- Cung cấp nền tảng trong việc thiết kế hệ thống mạng và các dịch vụ bằng cách kết nối hệ thống mạng ảo trong GNS3 và các máy ảo trong VMWARE.

Để có thêm thông tin chi tiết xin vui lòng liên hệ:

Trung tâm Công nghệ Phần mềm Đại học Cần Thơ (CUSC)
Họ và tên: Võ Minh Thụy
- Điện thoại: (0292) 373 1072 (ext 306) - Fax: (0292) 373 1071
- Địa chỉ: 01 Lý Tự Trọng, Q. Ninh Kiều, TP. Cần Thơ
- Di động/Zalo: 0932.895.166
- Email: vmthuy@ctu.edu.vn