

Số: 499 /SKHCN-TTUD

Bà Rịa - Vũng Tàu, ngày 09 tháng 7 năm 2019

V/v thông báo đăng ký đào tạo
tập huấn chuyên đề Kỹ năng giám sát
an ninh mạng dành cho quản trị mạng
các sở, ban, ngành/các huyện, thị xã,
thành phố thuộc tỉnh Bà Rịa - Vũng Tàu

TRUNG TÂM THÔNG TIN VÀ THỐNG KÊ KHOA HỌC VÀ CÔNG NGHỆ	
Số:	360
ĐẾN	Ngày: 11/7
Chuyển:	

Kính gửi:

- Các sở, ban, ngành;
- Các huyện, thị xã, thành phố.

Căn cứ Quyết định số 3600/QĐ-UBND ngày 18/12/2018 của UBND tỉnh Bà Rịa - Vũng Tàu về việc giao chỉ tiêu kế hoạch phát triển kinh tế - xã hội, quốc phòng - an ninh và dự toán thu, chi ngân sách nhà nước năm 2019;

Căn cứ Quyết định số 14/QĐ-SKHCN ngày 26/4/2019 của Giám đốc Sở Khoa học và Công nghệ về việc phê duyệt thuyết minh và dự toán kinh phí thực hiện nhiệm vụ thường xuyên theo chức năng năm 2019 của Trung tâm Ứng dụng tiến bộ khoa học và công nghệ tỉnh Bà Rịa - Vũng Tàu,

Trung tâm Ứng dụng tiến bộ khoa học và công nghệ tỉnh Bà Rịa - Vũng Tàu tổ chức lớp đào tạo tập huấn Kỹ năng giám sát an ninh mạng dành cho quản trị mạng các sở, ban, ngành/các huyện, thị xã, thành phố thuộc tỉnh Bà Rịa - Vũng Tàu, cụ thể như sau:

1. Nội dung

Trang bị cho học viên các kiến thức, kỹ năng và kinh nghiệm cần thiết để nhận biết, kiểm soát, phân tích các loại mã độc xâm nhập hệ thống mạng và xác định phương án, cách thức xử lý mã độc trong hệ thống mạng:

- Tổng quan về giám sát an ninh mạng.
- Giới thiệu các phương thức tấn công và xâm nhập phổ biến.
- Giải pháp phát hiện và phòng chống tấn công mạng với Suricata.
- Tổng hợp và lọc thông tin nhật ký (Log files) với hệ thống ELK.
- Giám sát hệ thống mạng với giải pháp Zabbix.
- Giám sát hệ thống mạng với giải pháp Security Onion.
- Các kiến thức khác về bảo mật và an ninh mạng.
- Diễn tập các kịch bản: Tấn công mạng nội bộ thông qua kỹ thuật Backdoor, Pivoting và mã hóa dữ liệu; Xử lý sự cố tấn công các máy chủ dịch vụ và leo thang đặc quyền...

2. Thời gian và địa điểm

- Thời gian: Từ ngày 22/7 đến ngày 26/7/2019 (05 ngày);
- Địa điểm:
 - + Từ ngày 22/7 - ngày 24/7 (thứ Hai - thứ Tư): Tại Phòng Đào tạo, Trung tâm Ứng dụng tiến bộ khoa học và công nghệ tỉnh Bà Rịa - Vũng Tàu, số 202 Bạch Đằng, P. Phước Trung, TP. Bà Rịa.
 - + Từ ngày 25/7 - ngày 26/7 (thứ Năm - thứ Sáu): Tại Thao trường mạng, Trường An ninh mạng iSPACE, số 240 Võ Văn Ngân, P. Bình Thọ, Q. Thủ Đức, TP. Hồ Chí Minh.

3. Thành phần và số lượng tham dự

- Thành phần: Cán bộ chuyên trách quản trị mạng tại các sở, ban, ngành/các huyện, thị xã, thành phố thuộc tỉnh Bà Rịa - Vũng Tàu.
- Số lượng: Mỗi đơn vị cử 01 người tham dự.

4. Kinh phí

- Các học viên tham dự lớp tập huấn sẽ được cung cấp miễn phí tài liệu, giáo trình, đĩa chương trình theo nội dung tập huấn. Sau khi hoàn thành chương trình học sẽ có bài kiểm tra để cấp giấy chứng nhận cho những học viên đạt yêu cầu.
- Chi phí lưu trú và phòng nghỉ đêm theo quy định (chi phí này do cơ quan cử học viên tham dự chi trả).
- Trung tâm Ứng dụng tiến bộ khoa học và công nghệ sẽ hỗ trợ xe đưa đón học viên từ TP. Bà Rịa đến TP. Hồ Chí Minh và ngược lại.

Sở Khoa học và Công nghệ tỉnh Bà Rịa - Vũng Tàu kính đề nghị các sở, ban, ngành/các huyện, thị xã, thành phố xác nhận về việc tham dự lớp tập huấn (theo mẫu phiếu đăng ký đính kèm) **trước ngày 17/7/2019** và gửi về địa chỉ Trung tâm Ứng dụng tiến bộ khoa học và công nghệ tỉnh Bà Rịa - Vũng Tàu (202 Bạch Đằng, P. Phước Trung, TP. Bà Rịa) hoặc liên hệ trực tiếp với Bà Lê Thị Quỳnh Trang qua email: trangltq87@gmail.com; điện thoại: 0254 3510 475; fax: 0254 3510 476; di động: 0917 957 918.

Trân trọng./.

Nơi nhận:

- Như trên;
- GĐ Sở (b/c);
- Sở Thông tin và Truyền thông (đ/b);
- Lưu: VT, TTUD.

KT. GIÁM ĐỐC

PHÓ GIÁM ĐỐC



Nguyễn Kim Trường



NỘI DUNG ĐÀO TẠO VÀ DIỄN TẬP

Kỹ năng giám sát an ninh mạng dành cho quản trị mạng các sở, ban, ngành/
các huyện, thị xã, thành phố thuộc tỉnh Bà Rịa - Vũng Tàu
(Kèm theo Công văn số: 499/SKHCN-TTUD ngày 09/7/2019)

1. Nội dung đào tạo lý thuyết

- Thời gian: Từ ngày 22/7 - ngày 24/7/2019 (từ thứ Hai - thứ Tư).
- Địa điểm: Phòng Đào tạo, Trung tâm Ứng dụng tiên bộ khoa học và công nghệ tỉnh Bà Rịa - Vũng Tàu.

Stt	Buổi học	Nội dung chi tiết
1	Buổi 1: Tổng quan về giám sát an ninh mạng	<ul style="list-style-type: none">- Giới thiệu tổng quan về giám sát an ninh mạng.- Xây dựng quy trình giám sát an ninh mạng- Gia tăng hiểu biết và tăng cường kỹ năng trong triển khai giám sát liên tục (Continuous Monitoring) theo chuẩn của Viện tiêu chuẩn Mỹ (NIST).- Xây dựng mô hình triển khai hệ thống giám sát an ninh mạng.
2	Buổi 2: Giới thiệu các phương thức tấn công và xâm nhập phổ biến	<ul style="list-style-type: none">- Giới thiệu các hình thức tấn công và xâm nhập phổ biến.- Giới thiệu các mối đe dọa về bảo mật:<ul style="list-style-type: none">+ Các mối đe dọa từ bên trong;+ Các mối đe dọa từ bên ngoài;+ Các mối đe dọa có cấu trúc và không có cấu trúc.- Thực hiện một vài kịch bản tấn công và xâm nhập phổ biến.
3	Buổi 3: Giải pháp phát hiện và phòng chống tấn công mạng với Suricata	<ul style="list-style-type: none">- Giới thiệu cấu trúc và hoạt động của Suricata.- Các thành phần cơ bản: Sniffer (Packet Decoder), Preprocessors, Detection Engine, The Output.- Cấu trúc các luật trong Suricata.- Triển khai cài đặt và cấu hình Suricata.
4	Buổi 4: Tổng hợp và lọc thông tin nhật ký (Log files) với hệ thống ELK	<ul style="list-style-type: none">- Giới thiệu hệ thống ELK: ElasticSearch, Logstash và Kibana.- Vai trò của hệ thống ELK trong hệ thống IDS/IPS.- Mô hình hoạt động của hệ thống ELK.- Triển khai cài đặt và cấu hình hệ thống ELK.
5	Buổi 5-6: Giám sát hệ thống mạng với giải pháp Zabbix	<ul style="list-style-type: none">- Giới thiệu hệ thống giám sát Zabbix.- Các tính năng và thành phần chính của Zabbix: Zabbix Server, Zabbix Proxy, Zabbix Agent, Web Interface.- Cài đặt và cấu hình hệ thống Zabbix:<ul style="list-style-type: none">+ Cài đặt và cấu hình Zabbix Agent giám sát máy Domain Controller;

		<ul style="list-style-type: none"> + Cài đặt và cấu hình Zabbix Agent giám sát dịch vụ Web; + Cài đặt và cấu hình SNMP giám sát thiết bị (Switch, Router); + Thiết lập hệ thống cảnh báo qua email. - Cấu hình thiết lập giám sát thiết bị trên nền Ipv6.
--	--	---

2. Nội dung diễn tập, trải nghiệm các mô hình thực tế

- Thời gian: Từ ngày 25/7 - ngày 26/7/2019 (từ thứ Năm - thứ Sáu)

- Địa điểm diễn tập, trải nghiệm:

+ Thao trường mạng của Trường An ninh mạng iSpace

+ Phòng LAB chuyên dụng của Tập đoàn Công nghệ CMC

+ Địa điểm: 240 Võ Văn Ngân, P. Bình Thọ, Q. Thủ Đức, TP. HCM

Stt	Buổi học	Nội dung chi tiết
1	Buổi 1: Diễn tập kịch bản 1: Tấn công mạng nội bộ thông qua kỹ thuật Backdoor, Pivoting và mã hóa dữ liệu	Tin tặc phát tán mã độc với định dạng *.docx thông qua Mail, mạng xã hội... cho người dùng bên trong tổ chức. Sau đó mở mã độc sẽ mở backdoor để giúp tin tặc dùng máy người dùng, sau đó tiếp tục rà quét bên trong mạng nội bộ của tổ chức nhằm tấn công các máy chủ trong mạng nội bộ thông qua kỹ thuật pivoting. Nhóm Ứng cứu sự cố sau đó tiến hành thu thập, phân tích chứng cứ, bóc tách mã độc và xử lý.
2	Buổi 2: Diễn tập kịch bản 2: Xử lý sự cố tấn công các máy chủ dịch vụ và leo thang đặc quyền	Tin tặc sử dụng chương trình rà quét, tiến hành scan port, lấy thông tin về các dịch vụ đang được public từ tổ chức như website, mail, cơ sở dữ liệu.... Sau đó tiến hành xác định các lỗ hổng đang tồn tại và tấn công leo thang đặc quyền, thay đổi nội dung trên các máy chủ này.
3	Buổi 3: Trải nghiệm công nghệ mới trên Phòng LAB chuyên dụng của Tập đoàn Công nghệ CMC	Chuyên gia của CMC sẽ giới thiệu, hướng dẫn học viên trải nghiệm các mô hình và công nghệ mới trong lĩnh vực an ninh mạng
4	Buổi 4: - Chia sẻ kinh nghiệm thực tiễn; - Học viên làm bài kiểm tra cuối khóa; - Công bố kết quả kiểm tra và cấp giấy chứng nhận cho học viên đạt yêu cầu	<ul style="list-style-type: none"> - Chia sẻ kinh nghiệm thực tiễn giữa học viên với các chuyên gia của CMC và iSpace - Học viên làm bài trắc nghiệm toàn khóa học trong thời gian 45 phút - Cấp giấy chứng nhận của Trường Cao đẳng An ninh mạng iSpace.

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHIẾU ĐĂNG KÝ THAM DỰ

Lớp đào tạo tập huấn kỹ năng giám sát an ninh mạng dành cho
quản trị mạng các sở, ban, ngành/các huyện, thị xã, thành phố thuộc
tỉnh Bà Rịa - Vũng Tàu

Từ ngày 22/7 đến ngày 26/7/2019

Tên đơn vị:

Địa chỉ:

Người liên hệ: Điện thoại:

Số thứ tự	Họ tên	Chức vụ	Số điện thoại
1			
2			
3			

....., ngày tháng 7 năm 2019

Thủ trưởng đơn vị