สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ที่ IT. 3 / 2566

4 สิงหาคม 2566

เรื่อง ขอเรียนเชิญเข้าร่วมการอบรมเชิงปฏิบัติการ “หลักสูตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ทั้งเชิงรุกและเชิงรับ ด้วยระบบจำลองยุทธ์ทางไซเบอร์”

เรียน กรรมการผู้จัดการ / ผู้อำนวยการฝ่าย – ผู้จัดการฝ่ายคอมพิวเตอร์

สิ่งที่ส่งมาด้วย โปสเตอร์ประชาสัมพันธ์

ด้วยคณะกรรมการพัฒนาธุรกิจและวิชาการประกันภัย โดยชมรมไอทีประกันภัย ได้กำหนดจัดการอบรมเชิงปฏิบัติการ **“หลักสูตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ทั้งเชิงรุกและเชิงรับ ด้วยระบบจำลองยุทธ์ทางไซเบอร์”** ขึ้น โดยมีวัตถุประสงค์เพื่อศึกษาและเข้าใจทฤษฎีบทด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ทั้งเชิงรุกและเชิงรับ และนำองค์ความรู้ที่ได้รับไปต่อยอดการปฏิบัติภารกิจทางไซเบอร์ ตลอดจนเพื่อสร้างเครือข่ายของบุคลากรในการที่จะแลกเปลี่ยนความรู้ การฝึกทักษะ และส่งเสริมการปฏิบัติภารกิจด้านสงครามไซเบอร์ที่เกี่ยวข้องกับความมั่นคงของชาติ ซึ่งการจัดอบรมในครั้งนี้ได้รับเกียรติจากบริษัท ไซเบอร์ตรอน จำกัด ซึ่งเป็นผู้เชี่ยวชาญในเรื่องดังกล่าวมาดำเนินการให้ โดยแบ่งการอบรมเป็น 2 ช่วง ดังนี้

- **<u>ช่วงที่ 1</u> การฝึกอบรมเชิงปฏิบัติการทางไซเบอร์ทั้งเชิงรุกและเชิงรับ จำนวน 3 วัน ประกอบด้วย**
  - วันอังคารที่ 5 กันยายน 2566 เวลา 09.00 - 16.00 น. ณ ห้องสัมมนา 501 ชั้น 5 สมาคมประกันวินาศภัยไทย
  - วันศุกร์ที่ 8 กันยายน 2566 เวลา 09.00 - 16.00 น. ณ ห้องสัมมนา 501 ชั้น 5 สมาคมประกันวินาศภัยไทย
  - วันอังคารที่ 12 กันยายน 2566 เวลา 09.00 - 16.00 น. ณ ห้องสัมมนา 501 ชั้น 5 สมาคมประกันวินาศภัยไทย
- **<u>ช่วงที่ 2</u> การแข่งขันการป้องกันทางไซเบอร์ทั้งเชิงรุกและเชิงรับ ด้วยระบบจำลองยุทธ์ทางไซเบอร์ จำนวน 1 วัน**

  จัดขึ้นในวันศุกร์ที่ 15 กันยายน 2566 เวลา 09.00 - 16.00 น. ณ ห้องสัมมนา 501 ชั้น 5 สมาคมประกันวินาศภัยไทย

ในการนี้ จึงใคร่ขอเรียนเชิญท่านพิจารณาส่งบุคลากรเข้าร่วมการอบรมเชิงปฏิบัติการในครั้งนี้ **โดยเสียค่าใช้จ่ายท่านละ 3,000 บาท (ตลอดทั้ง 4 วัน)** ท่านที่สนใจสามารถเข้าไปลงทะเบียนได้ที่ <u>https://seminar.tgia.org/</u> หรือ<u>สแกน QR Code ด้านล่างนี้</u> ***ตั้งแต่วันนี้จนถึงวันพุธที่ 30 สิงหาคม 2566***
สอบถามข้อมูลเพิ่มเติมได้ที่ นายทศพล ศรีสังข์ โทรศัพท์: 0-2108-8399 ต่อ 1104 หรือ E-mail: tosapon@tgia.org

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

Kraisit V.

(นายไกรสิทธิ์ วิตตินานนท์)
ประธานชมรมไอทีประกันภัย

ฝ่ายวิชาการทั่วไป (ทศพล)
โทรศัพท์ 0-2108-8399 ต่อ 1104

QR Code สำหรับลงทะเบียน

รายละเอียดหลักสูตร

❖ **ชื่อหลักสูตร** **“การรักษาความมั่นคงปลอดภัยทางไซเบอร์ทั้งเชิงรุกและเชิงรับ ด้วยระบบจำลองยุทธ์ทางไซเบอร์”**

❖ **คำอธิบายรายวิชา** วิชาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ทั้งเชิงรุกและเชิงรับเป็นรายวิชาที่เกี่ยวข้องกับทฤษฎีและการปฏิบัติด้านการทดสอบเจาะระบบรวมถึงแนวทางป้องกัน โดยรายวิชานี้ประกอบไปด้วยเนื้อหาที่เกี่ยวข้องกับพื้นฐานการเจาะระบบ ได้แก่ หลักการและความรู้พื้นฐานด้านการทดสอบเจาะระบบ การลาดตระเวนการสแกน การเจาะระบบและการยึดครองเครื่องเป้าหมาย และการเจาะระบบเว็บไซต์ด้วยเทคนิคต่างๆ ด้วย ระบบปฏิบัติการ Kali Linux รวมถึงแนวทางการป้องกันการโจมตีจากเทคนิคข้างต้น

❖ **จุดประสงค์รายวิชา**

- เพื่อศึกษาและเข้าใจทฤษดีบทด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ทั้งเชิงรุกและเชิงรับ
- เพื่อนำองค์ความรู้ที่ได้รับไปต่อยอดการปฏิบัติภารกิจทางไซเบอร์เชิงรุก และเชิงรับ
- เพื่อพัฒนาขีดความสามารถกำลังกำลังพลด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

❖ **ผู้สอน** ร้อยเอก กรัณย์ ต้นไม้ทอง (SEC+, Pentest+, CySA+, CASP+, CTT+, CEI, CEH, CHFI, CC, CPT)

❖ **ระยะเวลาการอบรม** จำนวน 18 ชั่วโมง **ระยะเวลาการจัดการแข่งขัน** จำนวน 6 ชั่วโมง

❖ **รายละเอียดหัวข้อและระยะเวลาในการอบรม**

- อธิบายหลักสูตร (ระยะเวลา 30 นาที)

- **หลักการและความรู้พื้นฐานด้านการทดสอบเจาะระบบ** (ระยะเวลา 1 ชั่วโมง 30 นาที)
  - อธิบายหลักการและวิธีการทดสอบเจาะระบบ (Methodology)
  - การใช้งานระบบปฏิบัติการ Kali Linux เบื้องต้น
  - แนะนำระบบปฏิบัติการ Kali Linux 2023.1
  - แนะนำการใช้ Kali Linux เบื้องต้น (แนะเมนูต่าง ๆ, เครื่องมือ, ชุดคำสั่งพื้นฐาน)

- เทคนิคการรวบรวมข้อมูล (Information Gathering Techniques) (ระยะเวลา 1 ชั่วโมง 30 นาที)
  - เทคนิคการเก็บรวบรวมข้อมูลด้วย Search Engine
  - เทคนิคการสแกนด้วย NMAP และ Zenmap
  - แนวการป้องกันการสแกน

- เทคนิคและโปรแกรมสำหรับเจาะช่องโหว่ (Exploit) ด้วย Metasploit Framework (ระยะเวลา 1 ชั่วโมง)
  - เทคนิค Reverse Shell และ Bind Shell
  - แนะนำ Metasploit Framework
  - อธิบายการใช้งาน Metasploit Framework
  - อธิบายการใช้งาน MSFVenom
  - แนวการป้องกันการถูกเจาะระบบจากช่องโหว่

- การโอนย้ายข้อมูลผ่านโปรโตคอลต่างๆ (Transferring Files) (ระยะเวลา 1 ชั่วโมง)

เทคนิคการถ่ายโอนข้อมูลด้วย FTP
เทคนิคการถ่ายโอนข้อมูลด้วย HTTP
เทคนิคการถ่ายโอนข้อมูลด้วย Netcat

- เทคนิค Password Attacks ในรูปแบบ Online Attack และ Offline Attack (ระยะเวลา 1 ชั่วโมง)

หลักการโจมตีด้วยการสุ่มเดารหัสผ่าน
แนะนำโปรแกรม John the Ripper
แนะนำเว็บไซต์สำหรับการ Crack Password
แนวทางการป้องกันการโจมตีด้วยการสุ่มเดารหัสผ่าน

- หลักการและความรูเพื้นฐานดเานการทดสอบเจาะระบบเว็บไซต์ (ระยะเวลา 1 ชั่วโมง)

อธิบายพื้นฐานการทำงานของ HTTP Protocol
อธิบาย HTTP Status Code
แนะนำโปรแกรม Burp Suit
เทคนิคการใช้ Burp Suit สำหรับทดสอบเจาะระบบเว็บไซต์

- การทดสอบเจาะระบบเว็บไซต์ตามแนวทางของ OWASP Top Ten 2021 (ระยะเวลา 5 ชั่วโมง)

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures
A10:2021-Server-Side Request Forgery

- ฝึกทักษะการป้องกันภัยคุกคามทางไซเบอร์ด้วย Cyber WAR (ระยะเวลา 6 ชั่วโมง)

แนะนำการใช้งานระบบ Cyber War
ฝึกทักษะการป้องกันภัยคุกคามทางไซเบอร์ด้วย Cyber WAR

❖ **รูปแบบการสอน**

- บรรยายทฤษฎีที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ทั้งเชิงรุกและเชิงรับ
- ให้ผู้เข้าศึกษาทำความเข้าใจและทดลองปฏิบัติด้วยตนเอง ผ่านระบบ Cyber W.A.R

❖ **สื่อการสอน** บรรยาย, LAB, Power Point, Video, White Board, Computer, ระบบ Cyber W.A.R

❖ **หนังสือประกอบการสอน**

- Certified Ethical Hacker (CEH) Foundation Guide แต่งโดย Sagar Ajay Rahalkar
- Kali Linux Cook book แต่งโดย Willie L. Pritchett และ David De Semet
- Learning Metasploit Exploitation and Development แต่งโดย Aditya Balapure
- Hacking Web Application แต่งโดย Joel Scambray และ Mike Shema
- Penetration Testing with Kali Linux แต่งโดย Offensive Security