ที่ อว ๖๕๐๑.๒๕/ว ๑๘๗๘

สำนักส่งเสริมและฝึกอบรม
มหาวิทยาลัยเกษตรศาสตร์
๕๐ ถนนงามวงศ์วาน จตุจักร
กรุงเทพฯ ๑๐๙๐๐

๑๔ กันยายน ๒๕๖๓

เรื่อง ขอเชิญส่งบุคลากรเข้าร่วมโครงการฝึกอบรมออนไลน์

เรียน ผู้บริหาร / หัวหน้าหน่วยงาน / ผู้อำนวยการฝ่ายฝึกอบรม / ฝ่ายทรัพยากรบุคคล /ผู้จัดการ / ผู้สนใจ

สิ่งที่ส่งมาด้วย โครงการฝึกอบรมออนไลน์หลักสูตร "การพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเข้าสู่สายงาน White-Hat Hackers"

ด้วยมหาวิทยาลัยเกษตรศาสตร์ โดยสำนักส่งเสริมและฝึกอบรม ร่วมกับ สำนักงานส่งเสริมเศรษฐกิจดิจิทัล มีกำหนดจัดโครงการฝึกอบรมออนไลน์หลักสูตร"การพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเข้าสู่สายงาน White-Hat Hackers" ระหว่างวันที่ ๑๔ - ๑๗ ธันวาคม ๒๕๖๓ จำนวน ๕๐ คน โดยมีวัตถุประสงค์ เพื่อพัฒนาบุคลากรด้าน White-Hat Hacker เพื่อรองรับความต้องการในภาคอุตสาหกรรมและเสริมสร้างความแข็งแกร่งของระบบสารสนเทศของประเทศไทย ดังรายละเอียดเอกสารของโครงการที่แนบมาพร้อมนี้

สำนักส่งเสริมและฝึกอบรม พิจารณาเห็นว่า การฝึกอบรมดังกล่าวจะช่วยเพิ่มพูนความรู้ทักษะ และประสบการณ์ให้แก่ผู้เข้ารับการฝึกอบรมได้เป็นอย่างดี อันจะก่อให้เกิดประโยชน์ต่อองค์กรและประเทศนั้น สำนักส่งเสริมและฝึกอบรม จึงใคร่ขอความอนุเคราะห์การประชาสัมพันธ์และสนับสนุนให้บุคลากรที่มีความสนใจเข้ารับร่วมโครงการฝึกอบรมออนไลน์หลักสูตร "การพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเข้าสู่สายงาน White-Hat Hackers" ครั้งนี้

สำนักส่งเสริมและฝึกอบรมหวังเป็นอย่างยิ่งว่า จะได้รับความอนุเคราะห์จากท่านในการประชาสัมพันธ์ให้บุคลากรสามารถเข้าร่วมฝึกอบรมในปีงบประมาณ พ.ศ. ๒๕๖๓ นี้ด้วย และขอขอบคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

((รองศาสตราจารย์สุวิสา พัฒนเกียรติ) 24 ก.ย. 2563
ผู้อำนวยการสำนักส่งเสริมและฝึกอบรม

เรียน หน่วยงานในสังกัดกรมอนามัย
ทั้งส่วนกลางและส่วนภูมิภาค
เพื่อโปรดทราบ จะเป็นพระคุณ

(นางวรรณภา กางกั้น)
นักทรัพยากรบุคคลเชี่ยวชาญ (ด้านการบริหารทรัพยากรบุคคล)
รักษาราชการแทนผู้อำนวยการกองการเจ้าหน้าที่ กรมอนามัย
25 ก.ย. 2563
ฝ่ายฝึกอบรม สำนักส่งเสริมและฝึกอบรม
โทรศัพท์ ๐-๒๙๔๒-๘๘๒๒ ต่อ ๒๐๓, ๒๐๔, ๒๐๙
โทรสาร ๐-๒๙๕๒-๘๘๓๐

เรียน ผู้อำนวยการกองการเจ้าหน้าที่
กลุ่มพัฒนาทรัพยากรบุคคล เห็นควรแจ้งเวียนหน่วยงานในสังกัดกรมอนามัย ต่อไป จะเป็นพระคุณ

(นางสาวภาคินันท์ สุสังกรกาญจน์)
นักทรัพยากรบุคคลชำนาญการ
ปฏิบัติหน้าที่แทนหัวหน้ากลุ่มพัฒนาทรัพยากรบุคคล

① เรียน ผู้อำนวยการฯ
เพื่อโปรดทราบ และโปรดอนุญาต [illegible]
กลุ่มงาน [illegible] ทราบ ดำเนินการ
ต่อไปด้วย ความเรียบร้อย [illegible]

ก. ๑๑๐๐
([illegible])
๒๙ ก.ค. 63

② [illegible]
[illegible]
30 ก.ค. 63

(นายเกษม เวชสุทธานนท์)
ผู้อำนวยการสถาบันพัฒนาสุขภาวะเขตเมือง

③ [illegible]

(นายยงยส หัถพรสวรรค์)
นายแพทย์เชี่ยวชาญ (ด้านเวชกรรม)
รองผู้อำนวยการสถาบันพัฒนาสุขภาวะเขตเมือง

④ [illegible]
– [illegible]
– [illegible]
[illegible]
๑ ส.ค. 63

(นางสาวเกศรา โชคนำชัยสิริ)
นักวิชาการสาธารณสุขชำนาญการพิเศษ
หัวหน้ากลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน

-Security Architecture
-Network Security
-Security Assessment and Testing
-Security Operations
-Software Development Security
๑๓.๐๐-๑๖.๐๐ Legal and Ethical Issues in Security
-Legal Issues
-Security and Privacy Act in Thailand
-International Security Standard
-Ethical Issues
-Case Studies

วันที่ ๒ ๐๙.๐๐-๑๒.๐๐ Introduction to Penetration Testing
-ภัยคุกคาม ช่องโหว่ ที่เกิดขึ้นในปัจจุบัน
-เรียนรู้คำศัพท์ที่เกี่ยวข้อง
-What is Hacking?
-Who is a Hacker?
-Hacker Classes
Information Gathering: Footprinting and Reconnaissance
- Footprinting Concepts
-Footprinting Threats
-Footprinting Methodology
-Footprinting Tools
๑๓.๐๐-๑๖.๐๐ Scanning Networks
-Types of Scanning
-Scanning Methodology
-Scanning Techniques
-Scanning Tools
Vulnerability assessment
-Vulnerability assessment methodology
-What is a vulnerability assessment?
-What is the CVE?
-What is the CVSS?
-vulnerability assessment process
-Vulnerability Scanning Tools
Vulnerability Scanning Tools (LAB)
-Nessus
-OpenVAS

วันที่ ๓ ๐๙.๐๐-๑๒.๐๐ Penetration Testing
-What is penetration testing
-Vulnerability assessment vs penetration testing
-Penetration testing methodology
-Penetration testing phases
-Penetration testing Report Example
Penetration Testing Tools (LAB)
-Kali Linux
Hacking Web Servers
-Webserver Concepts
-Webserver Attacks
-Attack Methodology
-Web Server Attack Tools
Web Server Attack Tools (LAB)
-Kali Linux
๑๓.๐๐-๑๖.๐๐ Hacking Web Applications
-Web App Concepts
-Web App Threats
-Hacking Methodology
-Web Application Hacking Tools
Web Application Hacking Tools (LAB)
-Kali Linux

วันที่ ๔ ๐๙.๐๐-๑๒.๐๐ System Hacking
-Cracking Passwords ,Escalating Privileges
Executing Application , Hiding Files , Covering Tracks
System Hacking Tools (LAB)
-Kali Linux
๑๓.๐๐-๑๖.๐๐ Metasploit
-Introduction , Metasploit Fundamentals , Information Gathering , Client Side Attack , MSF Post Exploitation Maintaining Access , Covering Track , Metasploit Tool (LAB) , Kali Linux

สนใจสมัครอบรมได้ทางคิวอาร์โค้ด

โครงการฝึกอบรมการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเข้าสู่สายงาน White-Hat Hackers

ระหว่างวันที่ ๑๔ – ๑๗ ธันวาคม ๒๕๖๓

โดย สำนักงานส่งเสริมเศรษฐกิจดิจิทัล
ร่วมกับ สำนักส่งเสริมและฝึกอบรม มหาวิทยาลัยเกษตรศาสตร์

****

๑. หลักการและเหตุผล

เทคโนโลยีด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber security) เป็นหนึ่งในเทคโนโลยีที่จำเป็นในการนำประเทศไทยเข้าสู่ยุคเศรษฐกิจดิจิทัล เนื่องจากระบบสารสนเทศในโลกไซเบอร์และธุรกิจที่พึ่งพาระบบดังกล่าวจะสามารถดำเนินต่อไปได้จะต้องได้รับการปกป้องข้อมูลในแง่ของการรักษาความลับ (Confidentiality) ความพร้อมใช้งาน (Availability) และความสมบูรณ์ของข้อมูล (Integrity) ตามระดับที่ยอมรับได้ขององค์กรหรือธุรกิจนั้นๆ หากระบบดังกล่าวถูกโจมตีหรือแฮ็ค (Hack) โดยผู้ประสงค์ร้ายหรือแฮ็คเกอร์ (Hacker หรือที่เรียกเจาะจงว่า Black-Hat Hacker) นั้น ย่อมทำให้องค์กรนั้นได้รับความเสียหายในตัวข้อมูล อันจะผลกระทบด้านเศรษฐกิจ สังคม รวมถึงความน่าเชื่อถือขององค์กรนั้น ดังนั้น องค์กรจึงจำเป็นจะต้องมีการตรวจสอบและทดสอบความมั่นคงปลอดภัยของระบบสารสนเทศของตนเองอย่างสม่ำเสมอ ตั้งแต่กำรวางแผนและออกแบบทั้งในส่วนของระบบทางเทคนิค นโยบาย แนวปฏิบัติ และ กลยุทธ์ ซึ่งรวมถึงการทดสอบการโจมตีระบบของตนเองโดยมอบหมายให้แฮ็คเกอร์เป็นผู้ทำการทดสอบระบบให้ แฮ็คเกอร์ลักษณะนี้เรียกว่า White-Hat Hacker ซึ่งเป็นแฮ็คเกอร์ที่มีจริยธรรม โดยจะมีหน้าที่ทดสอบการโจมตีระบบขององค์กรเองตามที่องค์กรนั้นได้รับมอบหมาย เพื่อให้เห็นช่องโหว่และความเสี่ยงของระบบนั้น

ปัจจุบัน White-Hat Hacker เป็นที่ต้องการอย่างสูงในประเทศไทยและทั่วโลก เนื่องจากการทดสอบโจมตีระบบโดยผู้พัฒนาระบบเองมักจะไม่สามารถทดสอบได้ครอบคลุมและลงลึกได้เพียงพอ อีกทั้งองค์ความรู้ของผู้พัฒนาระบบมักจะจำกัดเฉพาะด้านเกินไป ซึ่งไม่ครอบคลุมถึง

การเจาะระบบ ดังนั้น ประเทศไทยจึงจำเป็นที่จะต้องพัฒนาบุคลากรด้าน White-Hat Hacker เพื่อรองรับความต้องการในภาคอุตสาหกรรมและเพื่อเสริมสร้างความแข็งแกร่งของระบบสารสนเทศของประเทศไทย ในเนื้อหาของการพัฒนาบุคลากรในข้อเสนอโครงการนี้จะครอบคลุมองค์ความรู้ที่จำเป็นตั้งแต่เทคโนโลยีสำหรับ Ethical Hacker (การแฮ็คอย่างมีจริยธรรม) ความรู้พื้นฐานที่จำเป็นด้าน Cybersecurity กฎหมายและจริยธรรมที่เกี่ยวข้อง และมาตรฐานอุตสาหกรรมสากลด้าน Cybersecurity ซึ่งทั้งหมดนี้จะช่วยให้ผู้เข้าการพัฒนาได้รับองค์ความรู้ที่จะช่วยให้ต่อยอดในการทำงานด้าน White-Hat Hacker ได้อย่างมืออาชีพ

สำนักส่งเสริมและฝึกอบรมมหาวิทยาลัยเกษตรศาสตร์ เป็นหน่วยงานที่มีภารกิจในการให้บริการวิชาการแก่องค์กรภาครัฐและภาคเอกชน โดยเป็นหน่วยมีประสบการณ์ในการเป็นที่ปรึกษาเพื่อจัดฝึกอบรมพร้อมทั้งองค์ความรู้ของคณาจารย์จากภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ ที่เป็นผู้มีความรู้และมีประสบการณ์ในด้านนี้เป็นอย่างดี โครงการนี้ประกอบด้วยผู้สอนทั้งสิ้น ๓ ท่านซึ่งได้รับประกาศนียบัตรสาขาที่เกี่ยวข้อง เช่น Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), IRCA ISO/IEC ๒๗๐๐๑ Lead Auditor, Cisco Certified Network Associate (CCNA) เป็นต้น ซึ่งจะทำให้การให้บริการวิชาการบรรลุวัตถุประสงค์ของโครงการได้เป็นอย่างดี

๒. วัตถุประสงค์

๑.เพื่อพัฒนากำลังคนและบุคลากรในเทคโนโลยี ด้าน White-Hat Hackers สำหรับป้อนเข้าสู่อุตสาหกรรม
มด้านดิจิทัล ๕๐ คน

๒. เพื่อเสริมสร้างองค์ความรู้ด้านกฎหมายและจริยธรรมในการเป็น White-Hat Hackers รวมถึงการทดสอบและตรวจสอบ Cyber security อย่างมีจริยธรรมและไม่ขัดต่อกฎหมาย

๓. เพื่อปูพื้นฐานองค์ความรู้ด้าน Cyber security ใน Domain ต่างๆ ที่จำเป็นก่อนที่จะเป็น White-Hat Hackers

๓. คุณสมบัติผู้เข้าฝึกอบรม

๑. สามารถใช้งานระบบปฏิบัติการ Linux เบื้องต้นได้

๒. สามารถรถทำความเข้าใจและ/หรือเขียนโปรแกรมภาษาใดภาษาหนึ่งเบื้องต้นต่อไปนี้ PHP, JavaScript, JAVA, C#, Python

รวมทั้ง HTML หมายเหตุ อุปกรณ์ที่จำเป็นในการฝึกอบรม: -เครื่องโน้ตบุ๊กคอมพิวเตอร์ติดตั้งระบบปฏิบัติการขั้นต่ำ Windows ๗ ๖๔ bits, CPU Core i๕ Gen ๔ ขึ้นไป หน่วยความจำไม่ต่ำกว่า ๘ GB, พื้นที่ Hard disk ไม่ต่ำกว่า ๑๐๐ G

๔. จำนวนผู้เข้าร่วมฝึกอบรม

ผู้เข้าฝึกอบรม จำนวน ๕๐ คน

๕. กำหนดระยะเวลาและสถานที่ฝึกอบรม

ระหว่างวันที่ ๑๔ – ๑๗ ธันวาคม ๒๕๖๓
จำนวน ๔ วันๆละ ๖ ชั่วโมง

๖. วิทยากร

๑. ผศ.ดร.เทพฤทธิ์ บัณฑิตวัฒนาวงศ์ ที่ปรึกษาโครงการและวิทยากร
๒. ดร.ชาลี วรกุลพิพัฒน์ ที่ปรึกษาโครงการและวิทยากร
๓. นายเจษฎา ทองก้านเหลือง ที่ปรึกษาโครงการและวิทยากร

๗. กลุ่มกิจกรรมการเรียนรู้

กิจกรรมประกอบด้วยการฝึกอบรมผ่านระบบออนไลน์

๑. ใช้รูปแบบ Online ผ่านช่องทางที่เหมาะสม เช่น โปรแกรม WebEx, Microsoft Team, Zoom, Google meet, Google Classroom หรือโปรแกรมที่เหมาะสม โดยเป็นการสอนแบบ Interactive ที่ผู้สอนและผู้เข้ารับการอบรมสามารถโต้ตอบได้ด้วยภาพและเสียง ทั้งนี้การอบรมใช้รูปแบบ Online แทนวิธีดั้งเดิมแบบ Face-to-Face เพื่อลดความเสี่ยงอันเนื่องมาจากสถานการณ์ COVID-๑๙

๒. การสอนจะใช้เวลาทั้งสิ้น ๔ วัน วันละ ๖ ชั่วโมง (รวมระยะเวลาพักระหว่างเรียน ไม่รวมพักกลางวัน) โดยวันที่ ๑ จะเป็นการปูพื้นฐานด้านเทคโนโลยี Cyber security ใน Domain ต่างๆ และความรู้ด้านกฎหมาย จริยธรรม และมาตรฐานสากลที่จำเป็นต่อการเป็น White-Hat Hacker และวันที่ ๒-๔ จะเป็นการสอนเนื้อหาในส่วนของเทคโนโลยี Ethical Hacker รวมถึง Workshop และ Assignment

๘. โครงสร้างหลักสูตรการฝึกอบรม

รายละเอียด (หัวข้อ)	จำนวนชั่วโมง
๑. Information Security Domains	๓
๒. Legal and Ethical Issues in Security	๓
๓. Introduction to Penetration Testing	๓
๔. Scanning Networks/ Vulnerability assessment/ Vulnerability Scanning Tools (LAB)	๓

๕. Penetration Testing/ Penetration Testing Tools (LAB)	๓
Hacking Web Servers/ Web Server Attack Tools (LAB)	
๖. Hacking Web Applications/Web Application Hacking Tools (LAB)	๓
๗. System Hacking/ System Hacking Tools (LAB)	๓
๘. Metasploit/ Metasploit Tool (LAB)	๓
กิจกรรม Workshop รวม ๔ วันทำการ	๒๔ ชั่วโมง

๙. ผู้รับผิดชอบโครงการ

สำนักส่งเสริมและฝึกอบรม มหาวิทยาลัยเกษตรศาสตร์

๑๐. ตัวชี้วัดโครงการ

๑. มีผู้เข้าร่วมอบรมหลักสูตรไม่น้อยกว่า ๕๐ คน

๒. มีจำนวนผู้เข้าร่วมโครงการที่ผ่านการประเมินผลการเรียนรู้ (การเข้าเรียน การทำงานที่มอบหมาย และการสอบ) ไม่น้อยกว่าร้อยละ ๗๕

๑๑. การประเมินผลโครงการฝึกอบรม

การฝึกอบรมหลักสูตรนี้มีวิธีการประเมินผลจากการวัดความคิดเห็นของผู้เข้ารับการฝึกอบรมต่อการจัดฝึกอบรม โดยใช้แบบประเมินความคิดเห็นต่อรายวิชา/กิจกรรม และแบบประเมินความคิดเห็นต่อภาพรวมของโครงการฝึกอบรม

๑๒. การรับรองผลการฝึกอบรม

ผู้เข้ารับการฝึกอบรมจะได้รับประกาศนียบัตรรับรองผลการฝึกอบรม เมื่อปฏิบัติตามข้อกำหนด ดังนี้

๑. ผู้เข้ารับการอบรมจะต้องเข้ารับการทดสอบก่อนและหลังการอบรม (Pretest และ Posttest)

๒. เกณฑ์การวัดผลการฝึกอบรม ประกอบด้วย

- คะแนนการเข้าชั้นเรียนร้อยละ ๒๐
- คะแนนการทำงานที่ได้รับมอบหมายในชั่วโมงเรียน ร้อยละ ๓๐
- คะแนนสอบ Posttest ร้อยละ ๕๐

เกณฑ์ผ่านการฝึกอบรมคือคะแนนรวมไม่ต่ำกว่าร้อยละ ๗๐

กำหนดการฝึกอบรม

วันที่ ๑ ๐๙.๐๐-๑๒.๐๐ Information Security Domains
-Security and Risk Management
-Access Control