



กำหนดการอบรม

หลักสูตรฝึกอบรมเชิงปฏิบัติการ การตรวจสอบช่องโหว่และการทดสอบเจาะระบบ
(Vulnerability Assessment and Penetration Testing: VAPT)

วันที่ 14 - 16 กุมภาพันธ์ 2567
ณ โรงแรม เดอะ สุโกศล กรุงเทพฯ

วิทยากร : คุณแจษฎา ทองกันเหลือง กรรมการผู้จัดการ บริษัท ที-เน็ต ไอที โซลูชัน จำกัด
ผู้ช่วยวิทยากร : นายธนพล กระจ่างธร, นายศิลป์ชัย วงษ์เพ็ญ
กำหนดการอบรม (ระยะเวลา 3 วัน)

วันพุธที่ 14 กุมภาพันธ์ 2567	
09:00 - 10:30 น.	ความรู้เบื้องต้นเกี่ยวกับการทดสอบการเจาะระบบ (Introduction to Penetration Testing) <ul style="list-style-type: none">• ภัยคุกคาม ช่องโหว่ ที่เกิดขึ้นในปัจจุบัน• เรียนรู้คำศัพท์ที่เกี่ยวข้อง• What is Hacking?• Who is a Hacker?• Hacker Classes
10:30 - 12:00 น.	การรวบรวมข้อมูล (Information Gathering) <ul style="list-style-type: none">• Footprinting and Reconnaissance• Footprinting Concepts• Footprinting Threats• Footprinting Methodology• Footprinting Tools ○ Information Gathering LAB <ul style="list-style-type: none">• Footprinting through Search Engines• Footprinting Using Google Hacking• Website Footprinting• WHOIS Footprinting• DNS Footprinting• Network Footprinting• DNS Enumeration
13:00 - 14:30 น.	การสแกนเครือข่าย (Scanning Networks) <ul style="list-style-type: none">• Types of Scanning• Scanning Methodology• Scanning Techniques• Scanning Tools ○ Scanning Networks LAB <ul style="list-style-type: none">• TCP SYN Scan• TCP Connect Scan• UDP Scans• TCP NULL, FIN, and Xmas Scans• TCP ACK Scan• TCP Window Scan• OS Scan• Version Scan• Vulnerability Script Scan• Bypass Firewall Scan
14:30 - 16:00 น.	การค้นหาช่องโหว่ (Vulnerability Assessment) <ul style="list-style-type: none">• Vulnerability Assessment Methodology• What is a Vulnerability Assessment?• What is the CVE?• What is the CVSS?• Vulnerability Assessment Process

	<p>Vulnerability Scanning Tools (LAB)</p> <ul style="list-style-type: none"> • Nessus • OWASP Zap
วันพฤหัสบดีที่ 15 กุมภาพันธ์ 2567	
09:00 - 10:30 น.	<p>การทดสอบการเจาะระบบ (Penetration Testing)</p> <ul style="list-style-type: none"> • What is Penetration Testing? • Vulnerability Assessment vs Penetration Testing • Penetration Testing Methodology • Penetration Testing Phases • Penetration Testing Report Example <p>Penetration Testing Tools (LAB)</p> <ul style="list-style-type: none"> • OSINT • Kali Linux
10:30 - 12:00 น.	<p>การแฮ็คเว็บ (Hacking Web Servers)</p> <ul style="list-style-type: none"> • Webserver Concepts • Webserver Attacks • Attack Methodology • Web Server Attack Tools <p>Web Server Attack Tools (LAB)</p> <ul style="list-style-type: none"> • Kali Linux • Webserver Footprinting • Directory Traversal Attacks • DirBuster • Web Server Misconfiguration • Testssl • DoS/DDoS Attacks
13:00 - 16:00 น.	<p>การแฮ็คเว็บแอปพลิเคชัน (Hacking Web Applications)</p> <ul style="list-style-type: none"> • Web App Concepts • Web App Threats • Hacking Methodology • Web Application Hacking Tools <p>Web Application Hacking Tools (LAB)</p> <ul style="list-style-type: none"> • Kali Linux • Command Injection Attacks • SQL Injection Attacks • Session Hijacking • Cross-Site Scripting (XSS) Attacks • Cross-Site Request Forgery (CSRF) Attack
วันศุกร์ที่ 16 กุมภาพันธ์ 2567	
09:00 - 12:00 น.	<p>การแฮ็คระบบ (System Hacking)</p> <ul style="list-style-type: none"> • Cracking Passwords • Escalating Privileges • Executing Application • Hiding Files • Covering Tracks <p>System Hacking Tools (LAB)</p> <ul style="list-style-type: none"> • Kali Linux • SSH Brute Force Attack • RDP Brute Force Attack • Cracking Passwords
13:00 - 16:00 น.	<p>โครงการเมทาสพลอยด์ (Metasploit)</p> <ul style="list-style-type: none"> • Introduction • Metasploit Fundamentals • Information Gathering • Client Side Attack • MSF Post Exploitation • Maintaining Access • Covering Track

Metasploit Tool (LAB)

- Kali Linux
- Backdoor Command Execution
- Bind Shell Backdoor Detection
- NFS Exported Share Information Disclosure
- UnrealIRCD Backdoor Detection
- PHP-CGI
- Apache Tomcat Upload
- JAVA RMI Registry
- Windows: MS12-020
- Windows: MS08-067
- Windows: BlueKeep
- Windows: MS17-010
- Apache log4j

หมายเหตุ:

- สถาบันพัฒนาบุคลากรแห่งอนาคต ขอสงวนสิทธิ์ในการเปลี่ยนแปลงกำหนดการตามความเหมาะสม โดยยังคงเนื้อหาและสาระสำคัญของการอบรมไว้
- พักรับประทานอาหารว่าง เวลา 10.30 - 10.45 น. และ 14:30 - 14:45 น. และพักรับประทานอาหารกลางวัน เวลา 12.00-13.00 น.
- ผู้เข้าร่วมอบรมต้องมีเวลาเข้าเรียนไม่ต่ำกว่า 80% จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

<https://www.career4future.com/vapt>