ไอทีจีเนียส เอ็นจิเนียริ่ง
IT GENIUS ENGINEERING CO., LTD.

COURSE ID
CYC-02

CYBERSECURITY / PENTEST

COURSE OUTLINE · รายละเอียดหลักสูตรอบรม

Ethical Hacking และ Penetration Testing เบื้องต้น

- 18 ชั่วโมง
- 3 วัน
- ควรมีพื้นฐาน **เครือข่าย**
- ระดับ **Intermediate**

ระยะเวลา: 3 วัน
18 ชั่วโมง (3 วัน วันละ 6 ชม.) · 09:00-16:00 น.

รูปแบบ: Classroom / Hybrid
Onsite หรือ Online ผ่าน Microsoft Teams · Public / In-house

รายละเอียดหลักสูตร
www.itgenius.co.th

องค์กรจะป้องกันภัยไซเบอร์ได้ดีก็ต่อเมื่อเข้าใจว่าผู้โจมตีคิดและลงมืออย่างไร หลักสูตรนี้สอนการทดสอบเจาะระบบอย่างมีจริยธรรม (Ethical Hacking) ตามระเบียบวิธีมาตรฐาน ตั้งแต่การกำหนดขอบเขตและขออนุญาตเป็นลายลักษณ์อักษร การเก็บข้อมูลเป้าหมาย การสแกนและประเมินช่องโหว่ การทดสอบช่องโหว่เครือข่ายและเว็บแอปพลิเคชันตาม OWASP Top 10 ไปจนถึงการทำ Post-Exploitation อย่างมีขอบเขต และการเขียนรายงานพร้อมข้อเสนอแนะที่ทีมไอทีนำไปแก้ไขได้จริง

การฝึกทั้งหมดทำในห้องแล็บจำลองแบบปิดที่สถาบันจัดเตรียมให้ ด้วยเครื่องมือมาตรฐานสายงาน เช่น Kali Linux, Nmap, Burp Suite, Metasploit และ OWASP ZAP โดยเน้นย้ำกรอบกฎหมายไทยและจริยธรรมวิชาชีพตลอดหลักสูตร (หมายเหตุสำคัญ: การทดสอบเจาะระบบโดยไม่ได้รับอนุญาตเป็นความผิดตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ผู้เรียนต้องใช้ความรู้กับระบบที่ได้รับอนุญาตเป็นลายลักษณ์อักษรเท่านั้น อบรม 3 วัน วันละ 6 ชั่วโมง รวม 18 ชั่วโมง ระดับ Intermediate)

เครื่องมือ
§ PDPA · DPO DPO · RoPA RoPA · DSR DSR · Sec Security

ราคาค่าอบรม · PUBLIC / IN-HOUSE

12,500 บาท / ท่าน

ราคายังไม่รวมภาษีมูลค่าเพิ่ม (VAT 7%) · รวมเอกสาร Lab Guide ห้องแล็บจำลอง Template รายงาน อาหารกลางวันและอาหารว่าง และ Certificate · ฝึกในห้องแล็บปิดที่สถาบันจัดเตรียมเท่านั้น · รับจัด In-house ขอใบเสนอราคาได้

เพิ่มเพื่อน LINE

02-570-8449 · 088-807-9770 · @itgenius · www.itgenius.co.th

01 วัตถุประสงค์ Objectives

- เข้าใจกรอบกฎหมายไทยและจริยธรรมวิชาชีพของการทดสอบเจาะระบบ และความสำคัญของหนังสืออนุญาต
- อธิบายระเบียบวิธีทดสอบเจาะระบบตามมาตรฐาน (Reconnaissance, Scanning, Exploitation, Post-Exploitation, Reporting)
- เตรียมและใช้งานห้องแล็บทดสอบแบบปิดด้วย Kali Linux และเครื่องเป้าหมายจำลอง
- เก็บข้อมูลเป้าหมายทั้งแบบ Passive และ Active อย่างเป็นระบบ
- สแกนเครือข่ายและประเมินช่องโหว่ด้วย Nmap และเครื่องมือ Vulnerability Scanner
- ทดสอบช่องโหว่เครือข่ายและเครื่องแม่ข่ายด้วย Metasploit ในขอบเขตที่กำหนด
- ทดสอบช่องโหว่เว็บแอปพลิเคชันตาม OWASP Top 10 ด้วย Burp Suite และ OWASP ZAP
- เข้าใจการโจมตีรหัสผ่าน Social Engineering และ Wi-Fi และแนวทางป้องกัน
- เขียนรายงานผลการทดสอบพร้อมจัดลำดับความเสี่ยงและข้อเสนอแนะการแก้ไข

02 กลุ่มเป้าหมาย Target Audience

- ผู้ดูแลระบบและทีมไอทีที่ต้องการเข้าใจมุมมองของผู้โจมตีเพื่อป้องกันได้ดีขึ้น
- เจ้าหน้าที่ความมั่นคงปลอดภัยสารสนเทศและทีม SOC
- นักพัฒนาซอฟต์แวร์และ QA ที่ต้องการทดสอบความปลอดภัยของระบบที่ตนดูแล
- ผู้ที่ต้องการเริ่มต้นสายงาน Penetration Tester และเตรียมตัวสู่ใบรับรองสายนี้
- ผู้ตรวจสอบระบบสารสนเทศ (IT Auditor) ที่ต้องประเมินความเสี่ยงเชิงเทคนิค

03 จุดเด่นของหลักสูตร Highlights

- **ฝึกในห้องแล็บปิดจริง** Kali Linux และเครื่องเป้าหมายจำลองครบชุด
- **ตามระเบียบวิธีมาตรฐาน** Recon ถึง Reporting อย่างเป็นระบบ
- **ครอบคลุมเครือข่ายและเว็บ** Nmap, Metasploit, Burp Suite, OWASP Top 10
- **เขียนรายงานเป็น** ได้ Template รายงานที่ส่งผู้บริหารได้
- **เน้นจริยธรรมและกฎหมาย** ทดสอบเฉพาะระบบที่ได้รับอนุญาตเท่านั้น

04 ความรู้พื้นฐาน Prerequisites

- เข้าใจพื้นฐานเครือข่าย TCP/IP, DNS และ HTTP ในระดับใช้งานได้
- ใช้งาน Linux ในระดับคำสั่งพื้นฐานได้ (แนะนำผ่านหลักสูตร Linux Administration มาก่อน)
- เข้าใจการทำงานของเว็บแอปพลิเคชันเบื้องต้น
- ผู้เรียนต้องยอมรับข้อตกลงการใช้ความรู้อย่างมีจริยธรรมและถูกกฎหมายก่อนเข้าอบรม

05 สิ่งที่ต้องเตรียมและเครื่องมือ Setup & Tools

รายการ	รายละเอียด
อุปกรณ์	Notebook ที่รัน Virtual Machine ได้ (RAM 8 GB ขึ้นไป แนะนำ 16 GB)
ห้องแล็บ	ห้องแล็บจำลองแบบปิดที่สถาบันจัดเตรียม พร้อมเครื่องเป้าหมายสำหรับฝึก
เครื่องมือหลัก	Kali Linux, Nmap, Metasploit Framework, Burp Suite Community และ OWASP ZAP
เอกสารอ้างอิง	OWASP Top 10, MITRE ATT&CK และ Template รายงานผลการทดสอบ
ข้อกำหนด	หนังสือยินยอมให้ทดสอบ (Authorization Letter) ตัวอย่างสำหรับใช้ในงานจริง

หมายเหตุ: การฝึกทั้งหมดทำในห้องแล็บจำลองแบบปิดที่สถาบันจัดเตรียมเท่านั้น ห้ามนำเทคนิคไปใช้กับระบบที่ไม่ได้รับอนุญาตโดยเด็ดขาด การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบเป็นความผิดตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ผู้เรียนต้องมีหนังสืออนุญาตเป็นลายลักษณ์อักษรและกำหนดขอบเขตให้ชัดเจนทุกครั้งก่อนทดสอบระบบจริง

06 ภาพรวมการเรียน 3 วัน Big Picture

วัน	หัวข้อหลัก
Day 1 Section 1-4	จริยธรรมและกรอบกฎหมาย, ระเบียบวิธีทดสอบเจาะระบบ, การเตรียมห้องแล็บ และการเก็บข้อมูลเป้าหมาย (Recon)
Day 2 Section 5-8	การสแกนและประเมินช่องโหว่, การเจาะระบบเครือข่ายและเครื่องแม่ข่าย, ช่องโหว่เว็บตาม OWASP และรหัสผ่าน
Day 3 Section 9-12	Post-Exploitation, Social Engineering และ Wi-Fi, การเขียนรายงานและข้อเสนอแนะ และการสอบจำลอง

DAY 1

จริยธรรม ระเบียบวิธี และการเก็บข้อมูล

เนื้อหาการอบรม · Section 1-4

รวม
6 ชั่วโมง

1 จริยธรรม กฎหมาย และขอบเขตการทดสอบ

- ความต่างระหว่าง Ethical Hacking, Penetration Testing และการโจมตีที่ผิดกฎหมาย
- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และความรับผิดที่ผู้ทดสอบต้องรู้
- การกำหนดขอบเขต (Scope) หนังสืออนุญาต (Authorization) และข้อตกลงรักษาความลับ
- จริยธรรมวิชาชีพ การเปิดเผยช่องโหว่อย่างรับผิดชอบ (Responsible Disclosure)

2 ระเบียบวิธีทดสอบเจาะระบบ

- ขั้นตอนมาตรฐาน: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Reporting
- ประเภทการทดสอบ Black Box, Grey Box และ White Box และการเลือกให้เหมาะกับงาน
- การอ้างอิงกรอบงานสากล เช่น OWASP Testing Guide และ MITRE ATT&CK
- การวางแผนทดสอบและการสื่อสารกับเจ้าของระบบระหว่างทดสอบ

3 การเตรียมห้องแล็บทดสอบ

- การติดตั้งและใช้งาน Kali Linux และเครื่องมือหลักที่มากับระบบ
- การสร้างเครือข่ายจำลองแบบปิดและเครื่องเป้าหมายสำหรับฝึก
- การจัดการ Snapshot และการกู้คืนสภาพแวดล้อมทดสอบ
- Lab: เตรียมห้องแล็บส่วนตัวและตรวจสอบการเชื่อมต่อกับเครื่องเป้าหมาย

4 การเก็บข้อมูลเป้าหมาย (Reconnaissance)

- การเก็บข้อมูลแบบ Passive: OSINT, WHOIS, DNS และข้อมูลสาธารณะขององค์กร
- การเก็บข้อมูลแบบ Active และการระบุขอบเขตระบบเป้าหมาย
- การจัดระเบียบข้อมูลที่เก็บได้เพื่อใช้วางแผนการทดสอบขั้นถัดไป
- Lab: เก็บข้อมูลเป้าหมายในห้องแล็บและจัดทำสรุปข้อมูลที่ค้นพบ

DAY 2

การสแกนและการเจาะระบบ

เนื้อหาการอบรม · Section 5-8

รวม
6 ชั่วโมง

5 การสแกนและระบุบริการ

- การสแกนพอร์ตและระบุบริการด้วย Nmap และการอ่านผลลัพธ์อย่างเข้าใจ
- การระบุระบบปฏิบัติการและเวอร์ชันบริการ (Service and OS Fingerprinting)
- การใช้ Nmap Scripting Engine ตรวจสอบช่องโหว่เบื้องต้น
- Lab: สแกนเครือข่ายในห้องแล็บและจัดทำบัญชีบริการที่เปิดอยู่

6 การประเมินช่องโหว่ (Vulnerability Assessment)

- การใช้เครื่องมือสแกนช่องโหว่และการอ่านรายงานผล
- การจัดลำดับความรุนแรงด้วย CVSS และการอ้างอิง CVE
- การคัดกรองผลบวกลวง (False Positive) และการยืนยันช่องโหว่จริง
- Lab: ประเมินช่องโหว่ของเครื่องเป้าหมายและจัดลำดับความเสี่ยง

7 การทดสอบช่องโหว่เครือข่ายและเครื่องแม่ข่าย

- แนวคิดการใช้ประโยชน์จากช่องโหว่ (Exploitation) อย่างมีขอบเขตและควบคุมได้
- การใช้ Metasploit Framework: Module, Payload และการตั้งค่าอย่างปลอดภัย
- ช่องโหว่ที่พบบ่อยจากการตั้งค่าผิดพลาดและบริการที่ไม่ได้อัปเดต
- Lab: ทดสอบช่องโหว่บนเครื่องเป้าหมายในห้องแล็บและบันทึกหลักฐาน

8 ช่องโหว่เว็บแอปพลิเคชันตาม OWASP Top 10

- ภาพรวม OWASP Top 10 และช่องโหว่ที่พบบ่อยในเว็บองค์กร
- การทดสอบ Injection, Broken Access Control, XSS และการตั้งค่าที่ไม่ปลอดภัย
- การใช้ Burp Suite และ OWASP ZAP ดักและแก้ไขคำขอ HTTP เพื่อทดสอบ
- Lab: ทดสอบเว็บแอปพลิเคชันจำลองตาม OWASP Top 10 และบันทึกผล

DAY 3

Post-Exploitation และการรายงาน

เนื้อหาการอบรม · Section 9-12

รวม
6 ชั่วโมง

9 การโจมตีรหัสผ่านและการยืนยันตัวตน

- การเก็บและวิเคราะห์ค่า Hash รหัสผ่านและความแข็งแรงของรหัสผ่าน
- เทคนิคการทดสอบรหัสผ่านและข้อจำกัดทางกฎหมายและจริยธรรม
- การป้องกัน: นโยบายรหัสผ่าน MFA และการตรวจจับการพยายามเข้าสู่ระบบผิดปกติ
- Lab: ทดสอบความแข็งแรงของรหัสผ่านในห้องแล็บและสรุปข้อเสนอแนะ

10 Post-Exploitation, Social Engineering และ Wi-Fi

- Post-Exploitation อย่างมีขอบเขต: การยกระดับสิทธิ์และการเก็บหลักฐานโดยไม่ทำลายระบบ
- Social Engineering และ Phishing: กลไกการหลอกลวงและการฝึกภูมิคุ้มกันให้พนักงาน
- ความปลอดภัยของเครือข่ายไร้สายและการตั้งค่าที่ปลอดภัย
- Lab: จำลองสถานการณ์ Phishing เพื่อออกแบบแนวทางป้องกันขององค์กร

11 การเขียนรายงานและข้อเสนอแนะ

- โครงสร้างรายงานผลการทดสอบ: บทสรุปผู้บริหาร ขอบเขต วิธีการ ผลการทดสอบ และข้อเสนอแนะ
- การจัดลำดับความเสี่ยงและการเขียนข้อเสนอแนะที่ทีมไอทีนำไปแก้ไขได้จริง
- การเก็บหลักฐานประกอบรายงานอย่างเหมาะสมและการรักษาความลับของรายงาน
- Lab: เขียนรายงานผลการทดสอบจากผลงานที่ทำมาตลอดสองวัน

12 การทดสอบรวบยอดและการต่อยอด

- โจทย์รวบยอด: ทดสอบเป้าหมายในห้องแล็บตั้งแต่ Recon จนถึงรายงานฉบับสมบูรณ์
- การนำเสนอผลการทดสอบและรับ Feedback จากวิทยากร
- แนวทางป้องกันฝั่ง Defensive และการทำงานร่วมกับทีม SOC และผู้ดูแลระบบ
- Workshop: นำเสนอผลการทดสอบและวางแผนพัฒนาทักษะสู่ใบรับรองสายความปลอดภัย

07 เรียนจบแล้วได้อะไร Outcomes

- **เข้าใจมุมมองผู้โจมตี** เพื่อป้องกันระบบได้ตรงจุด
- **ทดสอบตามระเบียบวิธีมาตรฐาน** Recon ถึง Reporting ครบวงจร
- **ใช้เครื่องมือสายงานได้จริง** Kali, Nmap, Metasploit, Burp Suite
- **ทดสอบเว็บตาม OWASP Top 10** หาช่องโหว่ที่พบบ่อยในเว็บองค์กร
- **เขียนรายงานมืออาชีพ** จัดลำดับความเสี่ยงและเสนอวิธีแก้
- **ทำงานอย่างถูกกฎหมาย** มีขอบเขตและหนังสืออนุญาตชัดเจน

08 สิ่งที่ผู้เรียนจะได้รับ Deliverables

- เอกสารประกอบการอบรมฉบับสมบูรณ์ และ Lab Guide การทดสอบทีละขั้นตอน
- Template รายงานผลการทดสอบเจาะระบบและตัวอย่างหนังสืออนุญาตให้ทดสอบ
- Checklist การทดสอบตาม OWASP Top 10 และแนวทางป้องกันฝั่ง Defensive
- ประกาศนียบัตรจบหลักสูตร (Certificate of Completion) และช่องทางสอบถามวิทยากรหลังจบหลักสูตร

09 ข้อมูลผู้สอน Instructor

อ.สามิตร โกยม ผู้สอนและผู้เชี่ยวชาญด้านระบบและความมั่นคงปลอดภัยที่มีประสบการณ์กว่า 15 ปี ดูแลงานโครงสร้างพื้นฐานและการประเมินความปลอดภัยให้กับองค์กรจำนวนมาก จุดเด่นคือการสอนจากสถานการณ์จริงในห้องแล็บที่ควบคุมได้ เน้นจริยธรรมและกรอบกฎหมาย และพาผู้เรียนทำจนเขียนรายงานส่งผู้บริหารได้ด้วยตัวเอง

ราคาค่าอบรม 12,500 บาท/ท่าน · สนใจ IN-HOUSE ขอใบเสนอราคา

12,500 บาท / ท่าน (ยังไม่รวม VAT 7%)

02-570-8449
088-807-9770
@itgenius
contact@itgenius.co.th

เพิ่มเพื่อน LINE