

การฝึกยกระดับฝีมือ

หลักสูตร การทดสอบเจาะระบบ (Penetration Testing) สาขาอาชีพ เทคโนโลยีดิจิทัล ระดับหลักสูตร ระดับสูง รหัสหลักสูตร 10120014220507

สถาบันพัฒนาบุคลากรดิจิทัล
กรมพัฒนาฝีมือแรงงาน

ผู้อนุมัติหลักสูตร	นายถวัลย์ น้อยอุทัย ผู้อำนวยการสถาบันพัฒนาบุคลากรดิจิทัล	
วันที่อนุมัติ 23 เม.ย. 2569	จำนวน 7 แผ่น	ปรับปรุงครั้งที่ .../...

การฝึกยกระดับฝีมือ
หลักสูตร การทดสอบเจาะระบบ
(Penetration Testing)
รหัสหลักสูตร 10120014220507
สาขาอาชีพเทคโนโลยีดิจิทัล
ระดับหลักสูตร ระดับสูง (High)
สถาบันพัฒนาบุคลากรดิจิทัล กรมพัฒนาฝีมือแรงงาน

1. วัตถุประสงค์

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะ ตลอดจนมีทัศนคติที่ดีในการปฏิบัติงานการทดสอบเจาะระบบ โดยสามารถ

1.1 เสริมสร้างทักษะด้านความมั่นคงปลอดภัยไซเบอร์ แก่แรงงาน ผู้ประกอบอาชีพ และบุคลากรด้านเทคโนโลยีสารสนเทศให้สามารถรับมือกับภัยคุกคามไซเบอร์ที่ซับซ้อนในยุคดิจิทัลได้อย่างมีประสิทธิภาพ

1.2 พัฒนาความรู้และทักษะในการทดสอบเจาะระบบ (Penetration Testing) ทั้งในเชิงทฤษฎีและปฏิบัติ โดยเน้นการวิเคราะห์ช่องโหว่ การใช้เครื่องมือในการโจมตีจำลอง และการเสนอแนะแนวทางแก้ไข

1.3 สร้างมาตรฐานฝีมือแรงงานในสายอาชีพความมั่นคงไซเบอร์ ให้มีความสอดคล้องกับมาตรฐานวิชาชีพระดับสากล เช่น CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional)

1.4 ส่งเสริมการปฏิบัติงานตามจริยธรรมของนักทดสอบระบบ รวมถึงความเข้าใจด้านกฎหมายที่เกี่ยวข้องกับการทดสอบเจาะระบบ และการรักษาความลับของข้อมูล

1.5 เตรียมความพร้อมแรงงานไทยให้สามารถทำงานในตลาดแรงงานทั้งในและต่างประเทศ โดยเฉพาะในสายงาน Cybersecurity Analyst, Penetration Tester, Red Team Operator หรือ Security Consultant

1.6 นำความรู้และทักษะที่ได้รับไปประยุกต์ใช้ในการปฏิบัติงานหรือพัฒนางานให้มีประสิทธิภาพ

2. ระยะเวลาการฝึก

ผู้รับการฝึกจะได้รับการฝึกทั้งในภาคทฤษฎีและภาคปฏิบัติ โดยหน่วยงานสังกัดกรมพัฒนาฝีมือแรงงานหรือหน่วยงานที่เกี่ยวข้อง ระยะเวลาการฝึก จำนวน 30 ชั่วโมง

3. คุณสมบัติของผู้รับการฝึก

3.1 มีอายุตั้งแต่ 18 ปีขึ้นไป

3.2 มีการศึกษาไม่ต่ำกว่าระดับประกาศนียบัตรวิชาชีพ (ปวช.) หรือเทียบเท่า ในสาขาที่เกี่ยวข้องกับการเขียนโปรแกรมคอมพิวเตอร์

3.3 มีความรู้ภาษาอังกฤษเบื้องต้น

3.4 มีความรู้พื้นฐานระบบเครือข่ายและระบบคอมพิวเตอร์ มีประสบการณ์การทำงานความมั่นคงปลอดภัยทางไซเบอร์ หรือประกอบอาชีพที่เกี่ยวข้องด้านระบบเครือข่าย ความมั่นคงปลอดภัยทางไซเบอร์พื้นฐาน เป็นต้น

3.5 ผ่านการฝึกอบรมในหลักสูตรที่เกี่ยวข้องกับระบบเครือข่าย หรือ ความมั่นคงปลอดภัยทางไซเบอร์

3.6 กรณีผู้เข้ารับการฝึกเป็นแรงงานในสถานประกอบกิจการ ต้องเป็นผู้ปฏิบัติงานในตำแหน่งด้านเทคโนโลยีสารสนเทศขององค์กรหรือเป็นผู้ปฏิบัติงานที่เกี่ยวข้องกับหลักสูตรหรือเป็นเจ้าหน้าที่ที่สถานประกอบกิจการมอบหมาย

3.7 มีสภาพร่างกายที่ไม่เป็นอุปสรรคต่อการฝึก และสามารถเข้ารับการฝึกได้ตลอดหลักสูตร

4. คุณสมบัติวิทยากร

4.1 เป็นผู้เชี่ยวชาญที่มีประสบการณ์ตรงด้านการทดสอบเจาะระบบ (Penetration Testing) และความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ไม่น้อยกว่า 5 ปี โดยมีประสบการณ์ในการประเมินความปลอดภัยให้กับโครงสร้างพื้นฐานระดับองค์กร หรือหน่วยงานภาครัฐ

4.2 มีความเชี่ยวชาญขั้นสูงในการใช้เครื่องมือและเทคนิคการโจมตีสมัยใหม่ อาทิ Kali Linux, Burp Suite, Metasploit รวมถึงมีความเข้าใจลึกซึ้งในสถาปัตยกรรมเครือข่าย, Cloud Security และระบบ Active Directory

4.3 มีทักษะในการถ่ายทอดองค์ความรู้ทางเทคนิคที่ซับซ้อนให้เข้าใจง่าย สามารถออกแบบและบริหารจัดการห้องปฏิบัติการเสมือน (Virtual Labs) เพื่อให้ผู้เรียนได้ฝึกปฏิบัติในสถานการณ์จำลองที่ใกล้เคียงความเป็นจริง

4.4 มีความรู้ความเข้าใจอย่างถ่องแท้ในด้านจรรยาบรรณวิชาชีพนักทดสอบเจาะระบบ (Code of Ethics) กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และมาตรฐานความเป็นส่วนตัวของข้อมูล (PDPA)

5. วุฒิบัตร

ชื่อเต็ม : วุฒิบัตรพัฒนาฝีมือแรงงาน หลักสูตร การทดสอบเจาะระบบ

ชื่อย่อ : วพร. การทดสอบเจาะระบบ

ผู้รับการฝึกที่ผ่านการฝึกอบรมต้องมีระยะเวลาการฝึกอบรมตามหลักสูตรไม่น้อยกว่าร้อยละ 80 และผ่านการประเมินผลทั้งภาคทฤษฎีและปฏิบัติตามเกณฑ์ไม่น้อยกว่าร้อยละ 60 จะได้รับวุฒิบัตรจากกรมพัฒนาฝีมือแรงงาน

6. หัวข้อวิชา

รหัส	หัวข้อวิชา	ชั่วโมง	
		ทฤษฎี	ปฏิบัติ
10122232201	ความรู้เบื้องต้นเกี่ยวกับการทดสอบเจาะระบบ (Introduction to Penetration Testing)	1	2
10122232202	การกำหนดขอบเขตและข้อตกลงในการทดสอบเจาะระบบ (Scoping and Rules of Engagement)	1	2
10122232203	การรวบรวมข้อมูลจากแหล่งสาธารณะ (Open Source Intelligence - OSINT)	1	2
10122232204	การสแกน Enumeration and Social Engineering	1	2
10122232205	เทคนิคการเจาะระบบและการประเมินช่องโหว่	1	2
10122232206	การทดสอบเจาะระบบ Active Directory	1	2
10122232207	การทดสอบเจาะระบบเครือข่ายไร้สาย	1	2
10122232208	การทดสอบเจาะระบบเว็บแอปพลิเคชันตามมาตรฐาน OWASP Top 10	1	2
10122232209	การทดสอบเจาะระบบคลาวด์	1	2
10122232210	การจัดทำรายงานและเอกสารประกอบการทดสอบเจาะระบบ	1	3
10122239901	การวัดและประเมินผล	0	0
รวม		**12**	**18**
		30	

หมายเหตุ

ทั้งนี้ กรณีที่ผู้ประกอบกิจการตามพระราชบัญญัติส่งเสริมการพัฒนาฝีมือแรงงาน พ.ศ. 2545 ส่งลูกจ้างของตนเข้ารับการฝึกอบรมหรือจัดฝึกอบรมให้กับลูกจ้างของตน ตามคุณสมบัติของผู้รับการฝึก ถือเป็นการฝึกตามพระราชบัญญัติส่งเสริมการพัฒนาฝีมือแรงงาน พ.ศ. 2545

7. เนื้อหาวิชา

10122232201 ความรู้เบื้องต้นเกี่ยวกับการทดสอบเจาะระบบ (1 : 2)

(Foundations of Penetration Testing)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะเกี่ยวกับกรอบแนวคิดความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) และขอบเขตทางกฎหมาย

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับประเภทของแฮกเกอร์และแรงจูงใจ ความแตกต่างระหว่างการประเมินช่องโหว่ (VA) และการทดสอบเจาะระบบ(PT),จรรยาบรรณวิชาชีพ และกฎหมายที่เกี่ยวข้องกับความผิดเกี่ยวกับคอมพิวเตอร์

ฝึกปฏิบัติเกี่ยวกับ

1) การจำลองสภาพแวดล้อม การทดสอบ (Pentest Sandbox) และการใช้ระบบปฏิบัติการเฉพาะทาง เช่น Kali Linux หรือ Parrot OS

2) การใช้คำสั่งพื้นฐานบน Command Line สำหรับงาน Security, การตั้งค่าสภาพแวดล้อมเครือข่ายจำลองอย่างปลอดภัย และการทำความเข้าใจเวิร์กโฟลว์ผ่านการทำ Case Study จากสถานการณ์จริง

10122232202 การกำหนดขอบเขตและข้อตกลงในการทดสอบเจาะระบบ (1 : 2)

(Scoping and Rules of Engagement)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะเกี่ยวกับการบริหารจัดการโครงการทดสอบให้สอดคล้องกับมาตรฐานทางกฎหมายและข้อกำหนดของธุรกิจ

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับการประเมินความต้องการขององค์กร, การวิเคราะห์ความเสี่ยงก่อนดำเนินการ (Risk Assessment), การจัดทำกฎระเบียบในการเข้าถึงระบบ (RoE) และการบริหารจัดการความคาดหวังของลูกค้า

ฝึกปฏิบัติเกี่ยวกับการออกแบบเอกสารขอบเขตงาน (Scope of Work) การสัมภาษณ์เพื่อระบุทรัพย์สินสำคัญ (Critical Assets) และการทำ Workshop จำลองสถานการณ์การขออนุญาตเข้าทดสอบในระดับต่าง ๆ

10122232203 การรวบรวมข้อมูลจากแหล่งสาธารณะ (Open Source Intelligence - OSINT)(1 : 2)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะเกี่ยวกับการสืบค้นข้อมูลเชิงลึกผ่านสาธารณสมบัติ โดยใช้วิธีการตรวจสอบแบบไม่เปิดเผยตัวตน (Passive Reconnaissance)

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับวิธีการวิเคราะห์ Digital Footprint, เทคนิค Google Dorking ขั้นสูง, วิธีการรวบรวมข้อมูล DNS/WHOIS และการใช้เฟรมเวิร์ก OSINT เพื่อประเมินผิวการโจมตี (Attack Surface)

ฝึกปฏิบัติเกี่ยวกับการใช้เครื่องมือสืบค้นข้อมูลอัตโนมัติ (เช่น Maltego, TheHarvester), การจำลองการค้นหาช่องโหว่จาก Shodan และการวิเคราะห์โครงสร้างพื้นฐานของเป้าหมายจากข้อมูลสาธารณะ

10122232204 การสแกนระบบและการวิศวกรรมทางสังคม (1 : 2)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะเกี่ยวกับการระบุช่องทางเข้าถึงเชิงลึกและทดสอบความแข็งแกร่งของระบบป้องกันในระดับบุคคล

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับเทคนิคการทำ Port Scanning และ Service Enumeration, การระบุระบบปฏิบัติการและเวอร์ชันของซอฟต์แวร์ รวมถึงทฤษฎีจิตวิทยาที่ใช้ในวิศวกรรมสังคม (Social Engineering)

ฝึกปฏิบัติเกี่ยวกับการใช้งาน Nmap ขั้นสูงเพื่อหลบเลี่ยงระบบตรวจจับ การทำ Enumeration บนโปรโตคอล SMB/LDAP และการออกแบบสถานการณ์จำลองเพื่อทดสอบ Phishing Awareness

10122232205 เทคนิคการเจาะระบบและการประเมินช่องโหว่ (1 : 2)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะเกี่ยวกับการระบุความรุนแรงของจุดอ่อนและจำลองการเจาะระบบเพื่อพิสูจน์ผลกระทบเชิงธุรกิจ

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับวงจรการบริหารจัดการช่องโหว่, การเลือกใช้ช่องโหว่ (Exploits) ให้เหมาะสมกับเป้าหมาย และเทคนิคการเข้าควบคุมระบบเบื้องต้น (Initial Access)

ฝึกปฏิบัติการใช้ Vulnerability Scanner (เช่น Nessus) พร้อมวิเคราะห์ผลลัพธ์ การใช้ Metasploit Framework ในการทำ Exploitation และการฝึกเขียน Script เบื้องต้นเพื่อปรับแต่ง Payload

10122232206 การทดสอบเจาะระบบ Active Directory (1 : 2)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะเกี่ยวกับการประเมินความปลอดภัยของระบบบริหารจัดการตัวตนและสิทธิ์ในเครือข่ายองค์กรขนาดใหญ่

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับโครงสร้างพื้นฐานของ AD Domain, ช่องโหว่จากการกำหนดค่าผิดพลาด (Misconfiguration) และวงจรการโจมตีภายในระบบเครือข่าย Windows

ฝึกปฏิบัติเกี่ยวกับการทำ Enumeration ในสภาพแวดล้อม AD, ฝึกเทคนิค Kerberoasting และ AS-REP Roasting รวมถึงการทำ Lateral Movement เพื่อเข้ายึดครองระดับ Domain Admin

10122232207 การทดสอบเจาะระบบเครือข่ายไร้สาย (1 : 2)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะเกี่ยวกับตรวจสอบมาตรฐานความปลอดภัยและช่องโหว่ของการเชื่อมต่อผ่านสัญญาณวิทยุ

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับโปรโตคอลความปลอดภัย WPA2/WPA3, การโจมตีโครงสร้างพื้นฐานไร้สาย และความเสี่ยงจากการเข้าถึงผ่านเครือข่ายส่วนบุคคล (Bring Your Own Device)

ฝึกปฏิบัติเกี่ยวกับการทำ Packet Sniffing บนสัญญาณ Wi-Fi, ฝึกเทคนิค WPA/WPA2 Handshake Cracking และการสร้างจุดกระจายสัญญาณจำลอง (Rogue Access Point)

10122232208 การทดสอบเจาะระบบเว็บแอปพลิเคชันตามมาตรฐาน OWASP Top 10 (1 : 2)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะเกี่ยวกับตรวจหาและแก้ไขช่องโหว่ของซอฟต์แวร์ประยุกต์เว็บตามกรอบมาตรฐานสากล

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับการเจาะลึกช่องโหว่ 10 อันดับแรกตาม OWASP เช่น Injection, Broken Access Control และ Security Misconfiguration

ฝึกปฏิบัติเกี่ยวกับการใช้ Intercepting Proxy (เช่น Burp Suite) วิเคราะห์การรับส่งข้อมูล, ฝึกเจาะระบบเว็บจำลองด้วยเทคนิค SQL Injection, XSS และการข้ามส่วนการตรวจสอบสิทธิ์ (Auth Bypass)

10122232209 การทดสอบเจาะระบบคลาวด์ (1 : 2)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะเกี่ยวกับการประเมินการตั้งค่าและความมั่นคงความปลอดภัยบนสภาพแวดล้อมระบบคลาวด์สมัยใหม่

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับโมเดลความรับผิดชอบร่วมกัน (Shared Responsibility Model), ช่องโหว่จากการจัดการ IAM และความปลอดภัยของ Storage/Container บน Cloud (AWS, Azure, GCP)

ฝึกปฏิบัติเกี่ยวกับการตรวจสอบสิทธิ์การเข้าถึงผ่าน Cloud CLI, การทดสอบการเข้าถึงข้อมูลที่รั่วไหลจาก S3 Buckets หรือ Blob Storage และการประเมินความปลอดภัยของระบบ Serverless

10122232210 การจัดทำรายงานและเอกสารประกอบการทดสอบระบบ (1 : 2)

วัตถุประสงค์รายวิชา

เพื่อให้ผู้รับการฝึกมีความรู้และทักษะเกี่ยวกับการสื่อสารความเสี่ยงและแนวทางแก้ไขปัญหาเชิงเทคนิคให้แก่ผู้มีส่วนเกี่ยวข้องในทุกระดับ

คำอธิบายรายวิชา

ศึกษาเกี่ยวกับโครงสร้างการเขียนรายงานมาตรฐานสากล, การประเมินคะแนนความรุนแรง (CVSS) และการออกแบบแนวทางการแก้ไข (Remediation Plan)

ฝึกปฏิบัติเกี่ยวกับการจัดทำ Executive Summary สำหรับผู้บริหาร, การเขียนขั้นตอน Technical Proof of Concept (PoC) และการทำ Workshop นำเสนอผลการทดสอบเชิงวิพากษ์

10122239901 การวัดและประเมินผล (0 : 0)

วัดความรู้ของผู้เข้ารับการฝึกโดยการสอบภาคทฤษฎี วัดความสามารถของผู้รับการฝึก โดยการทดสอบภาคปฏิบัติ และประเมินผลการผ่านการฝึกอบรมตามเกณฑ์ที่กำหนด

8. ทักษะที่ได้รับ

ผู้รับการฝึกได้รับทักษะความเชี่ยวชาญการใช้เครื่องมือสากล เพื่อระบุและบริหารจัดการความเสี่ยงไซเบอร์อย่างมืออาชีพ

คณะผู้จัดทำหลักสูตร

1. นายอดิศร นิลวิสุทธิ์	นายกสมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
2. ดร.กรมวุฒิ นงนุช	คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ ศูนย์นนทบุรี
3. พ.ต.ท.ดร.วงศ์ยศ เกิดศรี	คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
4. นายเกรียงศักดิ์ นามโคตร	อุปนายกสมาคม สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
5. นายนนทวัตต์ สาระมาน	กรรมการ สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย

ลงนาม.....ผู้เสนอหลักสูตร

(นายทวีศักดิ์ เจริญศิลป์)

ตำแหน่ง นักวิชาการพัฒนาฝีมือแรงงานชำนาญการ

ลงนาม.....ผู้เห็นชอบหลักสูตร

(นายชาติชาย เทียมสนิท)

ตำแหน่ง นักวิชาการพัฒนาฝีมือแรงงานชำนาญการ

ลงนาม.....ผู้อนุมัติหลักสูตร

(นายถวัลย์ น้อยอุทัย)

ตำแหน่ง ผู้อำนวยการสถาบันพัฒนาบุคลากรดิจิทัล