Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต
73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400
โทรศัพท์ 0 2644 8150 โทรสาร 0 2644 8110
www.career4future.com

หลักสูตร Junior Penetration Tester with TryHackMe ITM181

ฉบับแก้ไข วันที่ 17 ธันวาคม 2568

หลักการและเหตุผล:

การทดสอบเจาะระบบ (Penetration Testing) เป็นกระบวนการสำคัญในการประเมินความมั่นคงปลอดภัยของระบบสารสนเทศ โดยจำลองการโจมตีจากมุมมองผู้ไม่ประสงค์ดี เพื่อตรวจหาช่องโหว่และเสนอแนวทางแก้ไข หลักสูตร 5 วันนี้ออกแบบให้ผู้เรียนระดับเริ่มต้น (Junior) ได้ความเข้าใจพื้นฐาน ทักษะเชิงปฏิบัติการ และแนวปฏิบัติที่ดีเพื่อนำไปทำงานจริงหรือเตรียมสอบใบรับรองเบื้องต้น

วัตถุประสงค์:

- อธิบายแนวคิด lifecycle ของ penetration test (scoping → recon → exploit → post-exploit → reporting).
- ใช้เครื่องมือสำคัญ (เช่น Nmap, Nikto, Burp Suite, Metasploit, sqlmap, Wireshark) ในการสำรวจและโจมตีแบบพื้นฐานได้อย่างปลอดภัยในสภาพแวดล้อมทดสอบ (lab).
- วิเคราะห์ผลสแกนและจัดลำดับความเสี่ยงของช่องโหว่ (risk rating).
- ทำ exploit แบบง่าย (web/app / network) และเข้าใจแนวทางป้องกัน/แก้ไขเชิงเทคนิค.
- จัดทำรายงานการทดสอบ (technical + executive summary) ที่ใช้งานได้จริงสำหรับผู้รับผิดชอบระบบ.

หลักสูตรนี้เหมาะสำหรับ:

- เจ้าหน้าที่ IT, ผู้ดูแลระบบ (sysadmin) ที่ต้องการเข้าใจมุมมองผู้โจมตี
- ผู้เริ่มต้นในสาย Security / SOC / Red Team ที่ต้องการทักษะปฏิบัติ
- นักพัฒนาเว็บ/แอปที่ต้องการรู้ช่องโหว่ที่พบบ่อยและวิธีป้องกัน
- ผู้ที่ต้องการเตรียมตัวเป็น Jr. Penetration Tester

ข้อกำหนดก่อนเข้าเรียน (Prerequisites)

- พื้นฐานระบบปฏิบัติการ (Windows/Linux) พอสมควร
- ความเข้าใจพื้นฐานเครือข่าย (IP, TCP/UDP, DNS)
- โน้ตบุ๊กที่สามารถรัน VM (หรือให้ผู้จัดเตรียม lab VMs / cloud lab)

เนื้อหาการอบรม:

วันที่ 1 — พื้นฐานและการเตรียมตัว (Introduction & Lab Setup)

- ภาพรวมประเภทของการทดสอบ (Blackbox / Graybox / Whitebox) และข้อกฎหมาย / จริยธรรม
- Pentest methodology & phases (OSSTMM/PTES/OWASP ASVS พื้นฐาน)
- การเตรียม lab: Kali Linux / VM / VPN / isolated network / Burp CA cert
- เครื่องมือเบื้องต้นแนะนำ & การใช้งานพื้นฐาน: terminal, ssh, netcat
- Workshop: ตั้งค่า lab, สร้าง snapshot และเชื่อมต่อกับ target VM

วันที่ 2 — Reconnaissance & Scanning (Passive + Active Recon)

- Passive recon: WHOIS, DNS lookup, subdomain enumeration (dig, amass reconnaissance concept)
- Active recon: Nmap (service/version detection), enum4linux, smbclient, SNMP basics
- Web discovery: dirb/gobuster, curl, WAF detection
- Workshop: ทำ reconnaissance กับ target web + network VM (รวมการใช้กราฟ/ตารางสรุปผล)
- Lab exercise: สร้าง inventory ของ asset และ mapping service → ช่องโหว่ที่น่าตรวจสอบ

วันที่ 3 — Vulnerability Assessment & Exploitation Basics

- ความแตกต่าง: vulnerability scan vs penetration test
- ใช้เครื่องสแกน: OpenVAS/nessus (concept), nmap scripts (NSE)
- การวิเคราะห์ผล: false positive/negative, CVSS เบื้องต้น, prioritization
- Exploitation basics: Metasploit framework (ใช้ใน lab), buffer overflow concept (ง่าย ๆ), smb/ftp common exploits
- Workshop: หา vulnerability จากผลสแกน และใช้ Metasploit / manual exploit บน lab VM ที่จำกัดไว้
- Lab challenge: compromise a low-privilege shell และเก็บหลักฐาน (logs) อย่างปลอดภัย

วันที่ 4 — Web Application Penetration Testing (OWASP Top 10 Focus)

- ทบทวน OWASP Top 10 (Injection, Broken Auth, XSS, CSRF, etc.) — ตัวอย่างและผลกระทบ
- Proxy workflow: Burp Suite (intercept, repeater, intruder, scanner overview)
- SQL Injection: payloads, sqlmap demo, mitigation concepts (prepared statements)
- Cross-Site Scripting (XSS): stored/reflected/DOM, payload crafting, DOM analysis
- Session management & auth testing: cookie flags, session fixation, brute force/credential stuffing concepts
- Workshop: ใช้ Burp + manual techniques บน intentionally vulnerable web app (e.g., DVWA / BWAPP / custom lab)
- Lab challenge: exploit 2 ประเภทช่องโหว่ในเว็บและเตรียม proof-of-concept

วันที่ 5 — Post-exploitation, Reporting & Remediation

- Post-exploitation: persistence, credential harvesting basics, lateral movement concept (แต่จำกัดใน lab)
- Privilege escalation (Linux/Windows) — แนวคิดการค้นหา SUID, misconfig, unquoted service paths, weak service configs
- Forensics-aware testing: รักษาหลักฐาน, ทำความสะอาด (ethical) และ logging ที่ควรบันทึก
- การจัดทำรายงาน: โครงสร้างรายงาน (Executive summary, Technical findings, Risk rating, Repro steps, Remediation recommendations) + ตัวอย่างเท็มเพลตสั้น
- Presentation skills: วิธีสื่อสารกับ non-technical stakeholders และการเสนอ remediation roadmap
- Final lab: Full mini-engagement — reconnaissance → exploit → post-exploit (จำกัด) → สรุปผลเป็นรายงานสั้น (tech + executive) และนำเสนอ

ค่าลงทะเบียนอบรม:	16,000 บาท (ไม่รวมภาษีมูลค่าเพิ่ม)
จำนวนชั่วโมงในการฝึกอบรม:	5 วัน (30 ชั่วโมง)
ช่วงเวลาฝึกอบรม:	9.00 - 16.00 น.
กำหนดการอบรม:	ตามตารางปฏิทินอบรมประจำปี https://www.career4future.com/trainingprogram

วิทยากร:

อาจารย์อาทิตย์ ซื่อสัตย์สิทธิกร

- วิทยากรรับเชิญ สถาบันพัฒนาบุคลากรแห่งอนาคต
- Microsoft® Certified Professional
- Microsoft® Certified Technology Specialist
- Microsoft® Certified IT Professional
- Microsoft® Certified Solutions Associate
- Microsoft® Certified Solutions Expert
- CompTIA. Security+ certified

หมายเหตุ

- สถาบันฯ มีการจัดเตรียมเครื่องคอมพิวเตอร์ (ในหลักสูตรที่ต้องใช้โปรแกรมคอมพิวเตอร์) เอกสารการอบรม อาหารว่าง และอาหารกลางวัน ให้กับผู้เข้าอบรม
- สถานที่อบรม ห้องอบรม ณ สถาบันพัฒนาบุคลากรแห่งอนาคต อาคาร สวทช. ชั้น 6 ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400
- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ ที่ไม่ใช่ธุรกิจและไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม
- สถาบันฯ เป็นหน่วยงานราชการ ได้รับการยกเว้นไม่ต้องหักภาษี ณ ที่จ่าย 3%
- ผู้เข้าร่วมอบรมจากหน่วยงานราชการสามารถเบิกค่าลงทะเบียนจากต้นสังกัดได้ ตามระเบียบกระทรวงการคลัง และไม่ถือเป็นวันลาเมื่อได้รับการอนุมัติจากผู้บังคับบัญชา
- ค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมทางวิชาชีพของบริษัทหรือห้างหุ้นส่วนนิติบุคคล สามารถนำไปลดหย่อนภาษีได้ 200%
- สถาบันฯ ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร รูปแบบการอบรม ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- สถาบันฯ ขอสงวนสิทธิ์ ไม่บันทึกภาพ วิดีโอ หรือบันทึกเสียง ตลอดระยะเวลาการอบรม เนื่องจากเป็นลิขสิทธิ์ร่วมระหว่างวิทยากรกับสถาบันฯ และเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
- ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ติดต่อสอบถามรายละเอียด

สถาบันพัฒนาบุคลากรแห่งอนาคต (Career for the Future Academy)
73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400
โทรศัพท์ 0 2644 8150 ต่อ 81886-7
โทรสาร 0 2644 8150
E-mail: training@nstda.or.th
www.career4future.com