ภาคผนวก ช

การทดสอบเจาะระบบ (Penetration Testing)

คุณสมบัติฉพาะการทดสอบเจาะระบบ (Penetration Testing)

ผู้รับจ้างต้องดำเนินการทดสอบเจาะระบบ (Penetration Testing) เพื่อประเมินความปลอดภัยของระบบอย่างครอบคลุม โดยมีข้อกำหนดอย่างน้อย ดังต่อไปนี้

๑. มาตรฐานที่ต้องปฏิบัติตามการทดสอบเจาะระบบต้องสอดคล้องกับมาตรฐานสากลอย่างน้อยหนึ่งมาตรฐานต่อไปนี้

๑) NIST SP 800-115: แนวทางการทดสอบและประเมินความปลอดภัยของข้อมูลทางเทคนิค

๒) OWASP Testing Guide: แนวทางการทดสอบความปลอดภัยของเว็บแอปพลิเคชัน

๓) Penetration Testing Execution Standard (PTES)

๔) Open Source Security Testing Methodology Manual (OSSTMM)

๕) มาตรฐานอื่น ๆ ที่ได้รับความเห็นชอบจากผู้ว่าจ้าง

๒. ขอบเขตการทดสอบ

๑) ต้องครอบคลุมทั้งการทดสอบเจาะระบบจากภายนอก (External) และภายใน (Internal)

๒) ทดสอบแบบไม่มีสิทธิ์เข้าถึง (Black Box) เข้าถึงบางส่วน (Grey Box) หรือแบบมีข้อมูลทั้งหมด (White Box)

๓) ตำแหน่งที่ต้องทดสอบ

- หน้า Firewall (ก่อนผ่าน Firewall) เพื่อประเมินว่ามีช่องทางเข้าถึงบริการที่ไม่ควรเปิดไว้หรือไม่ Firewall ทำงานได้ถูกต้องตามวัตถุประสงค์ที่กำหนดไว้หรือไม่ และเพื่อค้นหาช่องโหว่หรือความผิดปกติที่อาจเกิดขึ้น

- หลัง Firewall (ภายในระบบ) เช่น DMZ, LAN และ Application Servers เพื่อหาช่องโหว่ และทดสอบความสามารถในการป้องการถูกโจมตีจากภายใน

- DMZ Zone ตรวจสอบความแข็งแรงของระบบที่เชื่อมต่อภายนอก เช่น Web Server, Reverse Proxy, API Gateway

- Segmented Network ตรวจสอบว่า Network Segmentation สามารถป้องกันการโจมตีแบบ Lateral Movement ได้จริงหรือไม่

๔) ดำเนินการทดสอบเจาะระบบ ดังนี้

- การทดสอบเจาะระบบต้องครอบคลุม อย่างน้อย ดังนี้ ๑) Web Application ๒) API Services ๓) Database ๔) Operating Systems ๕) Network Infrastructure ๖) Cloud Environment (ถ้ามี)

คณพศ หงสวรางกูร ปริญญา เพ็ญไพรัตน์กุล ธีรยุทธ วัฒนะธรรมศิริ ศิร์รัฐ ศรีสุนทรพินิต สาลิเดช สัมฤทธิ์
มธุรส ไพบูลย์วรชาติ วิมลมาศ วัฒนจรูญโรจน์ รัฐธรรม ชวนเชย พันธุ์นิชิต โปษยานนท์ นัฐพล สีสวย
วิชาญ จินดารัตน์ สิทธิศักดิ์ ไชยสุข อำนาจวิทย์ หมู่ศิลป์ จุฑามาศ วงศ์เหมอนันต์ ทักษิณ หลังสตา

- ทำการทดสอบหลังผ่านทดสอบความถูกต้องของระบบ User Acceptance Test (UAT) เรียบร้อยแล้ว

- กรณีพบข้อบกพร่อง จะต้องแก้ไขข้อบกพร่อง และทำการทดสอบการเจาะระบบจนกว่าจะไม่พบข้อบกพร่อง

๓. กระบวนการทดสอบ ต้องครอบคลุมกระบวนการอย่างน้อย ดังนี้

๑) การรวบรวมข้อมูล (Information Gathering)

๒) การวิเคราะห์ช่องโหว่ (Vulnerability Analysis)

๓) การโจมตีจำลอง (Exploitation)

๔) การวิเคราะห์ผลกระทบ (Post-Exploitation)

๕) การจัดทำรายงาน (Reporting)

๔. คุณสมบัติของผู้ทดสอบ

๑) ผู้รับจ้างต้องจ้างผู้ทดสอบที่มีประสบการณ์และได้รับการรับรองจากองค์กรสากลอย่างน้อยหนึ่งรายการ เช่น CREST หรือ EC-Council

๒) ผู้ทดสอบต้องมีประสบการณ์จริงในการให้บริการทดสอบเจาะระบบระดับองค์กร

๓) ผู้ทดสอบต้องมีใบรับรองที่ไม่หมดอายุจากองค์กรรับรองสากลอย่างน้อยหนึ่งรายการ เช่น

- CEH (Certified Ethical Hacker)

- OSCP (Offensive Security Certified Professional)

- GPEN (GIAC Penetration Tester)

- CompTIA PenTest+

- CPENT (Certified Penetration Testing Professional)

๔) ผู้ทดสอบต้องมีประสบการณ์ในการทดสอบการเจาะระบบในลักษณะ Web Application

๕. การจัดทำรายงาน ต้องจัดทำรายงานผลการทดสอบโดยละเอียดอย่างน้อยประกอบด้วย

๑) รายการช่องโหว่ที่พบ พร้อมระดับความรุนแรง (Severity)

๒) แนวทางการแก้ไขและป้องกัน

๓) หลักฐานประกอบ เช่น log, screenshot, timestamp

๔) วิเคราะห์ผลกระทบในเชิงเทคนิคและเชิงธุรกิจ

๕) รายงานต้องสามารถนำไปใช้ในการปรับปรุงระบบอย่างมีประสิทธิภาพ และจัดส่งเป็นเอกสารอย่างเป็นทางการ

๖. การทดสอบเจาะระบบต้องได้รับการอนุมัติล่วงหน้าจากผู้ว่าจ้าง และต้องดำเนินการในช่วงเวลาที่กำหนดเพื่อหลีกเลี่ยงผลกระทบต่อระบบงานปกติ