Penetration Test

- Penetration Test Vs. Vulnerability Assessment
  - Penetration test คือการทดสอบเพื่อหาช่องทางในการเข้าถึงระบบ
  - Vulnerability Assessment คือ การประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ที่ค้นพบ
- Penetration tests are valuable for several reasons
  - Determining the feasibility of a particular set of attack vectors
  - Identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence
  - Identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software
  - Assessing the magnitude of potential business and operational impacts of successful attacks
  - Testing the ability of network defenders to successfully detect and respond to the attacks
  - Providing evidence to support increased investments in security personnel and technology
- Black box vs. White box
  - การทำ Penetration Test จากภายนอกระบบเครือข่ายองค์กร หรืออาจเรียกว่าการทำ Black box คือ การใช้เครื่องคอมพิวเตอร์จำลองเป็นนักโจมตีระบบเพื่อหาทางเข้าสู่ระบบเครือข่ายองค์กรที่ให้ทำการประเมินความเสี่ยง
  - การทำ Penetration test ภายในองค์กร หรือจะเรียกว่า White box (ซึ่งการทำงานประเภทนี้ต้องได้รับความร่วมมือกับผู้ดูแลระบบของฝั่งผู้ใช้บริการ ตั้งแต่การให้แผนผังระบบเครือข่าย จำนวน IP Address ตลอดถึงรายละเอียดประเภทอุปกรณ์เครือข่ายที่เกี่ยวข้อง เป็นต้น) คือการทดสอบหาช่องโหว่ที่พบจากการใช้งานไอซีทีในองค์กรเพื่อประเมินช่องโหว่และทำการปิดกั้นช่องโหว่ที่ค้นพบขึ้นเพื่อไม่เกิดปัญหาขึ้นในระยะยาว
- Black box
  - สำรวจ : ตรวจหาเครือข่ายเป้าหมายในการปฏิบัติงาน
  - ตรวจสอบ : เมื่อเราทำการรวบรวมข้อมูลที่ได้มาจากขั้นตอนสำรวจนั้น ก็จะทำการวาดรูปความสัมพันธ์เครือข่ายองค์กรออกมาพร้อมกำหนดจุดที่ทำการตรวจสอบขึ้น การตรวจสอบมักจะใช้ check list ตามมาตรฐาน สิ่งที่ตรวจสอบได้แก่ Information leak, Web Application

checklist, DNS server checklist, E-mail Server checklist, Network Topology checklist, Port services

- วิเคราะห์ : เมื่อทำการตรวจสอบจากการสำรวจและตรวจสอบ ภายนอกเครือข่ายองค์กรแล้วนำข้อมูลเหล่านั้นมาทำการวิเคราะห์เพื่อศึกษาว่าพบช่องโหว่และการเข้าถึงข้อมูล
- ประเมิน : เมื่อทำการวิเคราะห์ถึงช่องโหว่ที่พบแล้ว ถึงขั้นตอนสุดท้ายคือการประเมิน ว่าช่องโหว่ที่พบนั้นมีความเสี่ยงและมีผลกระทบต่อธุรกิจองค์กรอย่างไร ส่วนใหญ่เป็นเอกสารการแนะนำและการปิดช่องโหว่ที่พบ ค่าความเสี่ยง (Risk)ที่พบ จะเกิดจาก ช่องโหว่ที่พบ (Vulnerability) คูณกับค่าภัยคุกคาม (Threat) ลักษณะภัยคุกคามที่พบก็มีความเสี่ยงสูง กลาง และต่ำ ซึ่งส่วนนี้ขึ้นอยู่รูปแบบผู้ทำเอกสารว่าจะจัดทำค่าการประเมินความเสี่ยงจากอุปกรณ์หรือเครื่องมือในตรวจวิเคราะห์ (Tools) มาสรุปความเสี่ยง สูง กลาง และต่ำ ก็ได้
  และจัดทำค่าดัชนีชี้วัดความเสี่ยงที่มีผลกระทบต่อธุรกิจทางด้านเทคนิค ซึ่งเอกสารในผลลัพธ์ของแต่ละบริษัทที่จัดทำอาจจะมีรูปแบบที่แตกต่างกันได้เช่นกัน

- White box
  - สำรวจ : สำรวจผังโครงสร้างงานได้ไอซีทีขององค์กร, แผนผังระบบเครือข่าย, ประเภทอุปกรณ์ประกอบ
  - ตรวจสอบ : ตรวจสอบตามมาตราฐาน Security Checklist
  - วิเคราะห์ : การวิเคราะห์ช่องโหว่ที่พบจากการสำรวจและตรวจสอบ
  - ประเมิน : ขั้นตอนนี้จะเป็นการสรุปผลความเสี่ยงที่พบจากขั้นตอนที่ผ่านมา โดยทำเป็นค่าดัชนีชี้วัดความเสี่ยง และผลการปฏิบัติงาน รวมถึงแนวทางในการปิดกั้นส่วนที่เป็นช่องโหว่ (Hardening) และป้องกันในระยะยาว ซึ่งในส่วนนี้จะเน้นไปทางการทำรายงานผล ในรูปแบบเอกสาร
- สรุป
  - Vulnerability (ช่องโหว่ที่ค้นพบ จาก อุปกรณ์เครือข่ายที่สำคัญ และเครื่องแม่ข่ายที่สำคัญ) จะมีระดับความเสี่ยง สูง กลาง และต่ำ หรืออาจจะมีรายละเอียดมากกว่านั้น
  - Threat (ภัยคุกคาม) ขึ้นกับนโยบายองค์กร และการประเมินค่าจะผู้ปฏิบัติงาน นำมารวมค่ากันแล้วจะได้เป็นดัชนีชี้วัดความเสี่ยงได้ ซึ่งการประเมินส่วนนี้ก็เป็นเทคนิคลับของแต่ละบริษัทที่ใช้ในการประเมินและสามารถวัดผลได้จริงในทางปฏิบัติ
  - การประเมินความเสี่ยงนั้นไม่สามารถที่สิ้นสุดการทำงานได้จากการใช้เครื่องมือ (tools) มาแล้วจะสรุปค่าความเสี่ยงที่เกิดขึ้นจากการใช้งานไอซีทีองค์กรได้จำเป็นต้องอาศัยคนวิเคราะห์ถึงระดับภัยคุกคามและผลลัพธ์รายงานที่มีประโยชน์ต่อบริษัทเพื่อใช้ในการปรับปรุงแก้ไขให้ระบบมีความแข็งแรงและมีความปลอดภัยขึ้น

- ตัวอย่าง VPN Penetration Test