อมรทิพย์ จำรัสเจริญวานิช : แบบจำลองโอกาสถูกโจมตี โดยอาศัยวัฏจักรชีวิตจุดอ่อนของระบบ. (PROBABILITY OF ATTACK MODEL BASED ON SYSTEM VULNERABILITY LIFE-CYCLE) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: อ.ดร.ยรรยง เต็งอำนวย, 89 หน้า.

การโจมตีแบบอัตโนมัติด้วยหนอนอินเทอร์เน็ตและไวรัสคอมพิวเตอร์ มีปริมาณเพิ่มขึ้นอย่างมากในโลกไซเบอร์ งานวิจัยนี้ทำการเก็บรวบรวมข้อมูลเกี่ยวกับวันที่ในวัฏจักรชีวิตของจุดอ่อนที่มีนัยสำคัญจากแหล่งข้อมูลต่างๆ เมื่อนำมาวิเคราะห์สามารถจำแนกรูปแบบวัฏจักรชีวิตของจุดอ่อนได้ 5 รูปแบบ คือ แบบที่มีการโจมตีอย่างเฉียบพลัน แบบที่มีการโจมตีเสมือนเฉียบพลัน แบบที่มีศักยภาพในการพัฒนาเป็นการโจมตีเสมือนเฉียบพลัน แบบที่มีศักยภาพในการถูกโจมตี และแบบเฉื่อย ซึ่งแสดงถึงลักษณะของวัฏจักรชีวิตที่แตกต่างกัน จากกรณีศึกษาของหนอนอินเทอร์เน็ตที่ชื่อสแลมเมอร์ (Slammer) บลาสเตอร์ (Blaster) โซทอป (Zotop) และโค้ดเรด (Code red) เป็นตัวอย่างที่สำคัญของวัฏจักรชีวิตแบบที่มีการโจมตีเสมือนเฉียบพลัน ที่พบว่าการแพร่ระบาดและติดเชื้อไปยังคอมพิวเตอร์ทั่วโลกนั้นสาเหตุเกิดจากการไม่ติดตั้งตัวปิดจุดอ่อนได้ทันเวลาของผู้ดูแลระบบ การวิเคราะห์ถึงปัจจัยที่มีผลต่อโอกาสถูกโจมตีผ่านจุดอ่อน อาทิเช่น การปรากฏของตัวปิดจุดอ่อน คำสั่งหรือโปรแกรมที่อยู่ในสภาพพร้อมใช้งานมีผลต่อโอกาสถูกโจมตีผ่านจุดอ่อน ปัจจัยที่วิเคราะห์ได้จากงานวิจัยนี้สามารถนำมาคำนวณเพื่อหาค่าโอกาสถูกโจมตี ค่าโอกาสนี้ช่วยทำให้ผู้ดูแลระบบกำหนดลำดับความสำคัญให้กับจุดอ่อนได้

4971489921 : MAJOR COMPUTER SCIENCE 207391

KEY WORD: VULNERABILITY / LIFE CYCLE / ZERO-DAY ATTACK / ADMINISTRATOR / ATTACK

AMONTIP JUMRATJAROENVANIT: PROBABILITY OF ATTACK MODEL BASED ON SYSTEM VULNERABILITY LIFE-CYCLE. THESIS PRINCIPAL ADVISOR: YUNYONG TENG-AMNUAY, Ph.D., 89 pp.

The proliferation of exploit codes greatly expedites attacks in cyber world. This research compiles important dates on vulnerability from various sources into five patterns of life-cycle: zero-day attack, pseudo zero-day attack, potential of pseudo zero-day attack, potential of attack, and passive attack. Slammer, Blaster, Zotop and Code Red worm are classified as pseudo zero-day attack, which results from leniency on the part of system administrators. This type of attack has significant percentage and is on the rise. Various factors, such as availability of patches and exploit codes, contribute to the probability of attack. This can help administrators prioritize their workload.