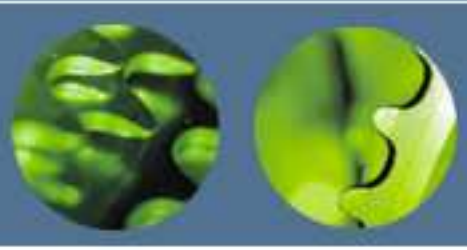
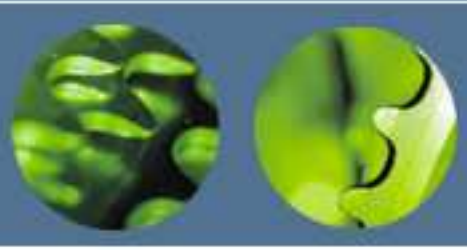
บทที่ 3 การป้องกันการเจาะระบบ



การเจาะระบบหรือแฮคคืออะไร

- To Write or refine computer programs skillfully
- To use one's skill in computer programming to gain illegal or unauthorized access to file or network:hacked into company's intranet
- การเจาะเข้าใช้ระบบอย่าไม่ได้รับอนุญาตคือคำว่า "แคร็คกิง(Cracking)" ส่วน แฮคกิง(Hacking) หมายถึง ผู้ใช้คอมพิวเตอร์และซอฟต์แวร์อย่างชำนาญ
- สังคมกำหนดความหมายของ แฮกเกอร์ไว้ทางลบ คือ "คนที่พยายามเจาะเข้าใช้ระบบคอมพิวเตอร์หรือเครือข่าย"



ความจริงเกี่ยวกับแฮกเกอร์

- แฮกเกอร์มักเป็นผู้ที่มีความชำนาญน้อย และชำนาญเฉพาะเรื่อง
- มักเป็นวัยรุ่นหรือเด็กที่อยากรู้อยากลอง
- การโจมตีกว่าครึ่งของแฮกเกอร์จะประสบผลสำเร็จเพราะระบบส่วนใหญ่ไม่มั่นคง
- ระบบเครือข่ายระบบสื่อสารออกแบบมาคำนึงถึงการสื่อสารมากกว่าการป้องกัน

ประเภทของแฮกเกอร์

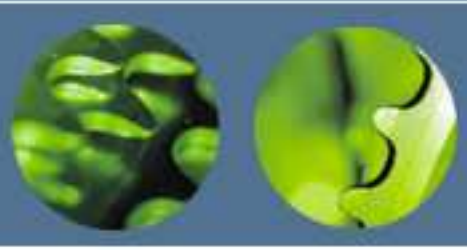
นักโจมตี	ระดับความชำนาญ	แรงจูงใจ
แฮกเกอร์	สูง	เพื่อปรับปรุงระบบรักษาความปลอดภัย
แค็คเกอร์	สูง	เพื่อทำลายระบบ
สคริปต์คิดดี้	ต่ำ	เพื่อให้ได้การยอมรับ
สายลับ	สูง	เพื่อให้ได้เงิน
พนักงาน	หลากหลาย	หลากหลาย
ผู้ก่อการร้าย	สูง	เพื่ออุดมการณ์ทางการเมือง

แฮคเกอร์

- เดิม แฮคเกอร์คือผู้ใช้ความรู้ความชำนาญโดยไม่ได้มุ่งหมายเพื่อทำลาย
- เดิม แฮคเกอร์ทำเพื่อการสำรวจเครือข่ายหาจุดบกพร่อง สิ่งแปลกปลอม เพื่อปรับปรุงระบบให้มั่นคงยิ่งขึ้น
- เดิม แฮคเกอร์จะค้นหาช่องโหว่และทำการแจ้งหรือปิดช่องโหว่นั้น
- เดิม แฮคเกอร์จะไม่ทำสิ่งผิดจริยธรรม
- เดิม แฮกเกอร์จะทำให้กิดผลกระทบกับระบบน้อยที่สุด
- อยากไรก็ดีการเจาะเข้าระบบอื่นโดยไม่ได้รับอนุญาต ก็ผิดกฎหมาย

แฮคเกอร์

- ปัจจุบัน แฮคเกอร์คือบุคคลที่พยายามจะเจาะเข้าระบบโดยไม่ได้รับอนุญาต
- ผู้โจมตีระบบ สร้างความเสียหายให้ระบบ

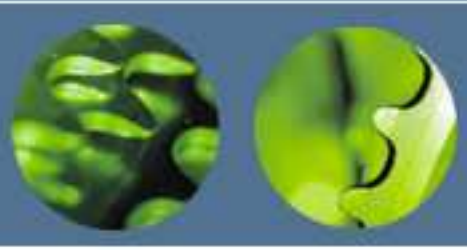


แคร็คเกอร์

- คือบุคคลที่มีความรู้ความชำนาญ พยายามจะทำลายระบบโดยจงใจ
- แคร็คเกอร์จะใช้ประโยชน์จากช่องโหว่ จุดบกพร่องในการทำลาย
- แคร็คเกอร์จะมีความภาคภูมิใจถ้าสามารถทำลายได้สำเร็จ
- แคร็คเกอร์จะรู้สึกไม่ดีถ้ามีคนที่เหนือกว่า
- แคร็คเกอร์จะค้นหาเจาะเข้าระบบต่อไปเรื่อยๆ เพื่อสร้างสถิติใหม่

การแบ่งกลุ่มแคร็คเกอร์

- กลุ่มความรู้ปานกลาง มีความรู้เครือข่ายระบบปฏิบัติการส่วนใหญ่โจมตีสำเร็จ แต่จะยังไม่สามารถเขียนโค้ดเองได้ ต้องอาศัยเครื่องมือช่วยเจาะระบบ ใช้ความรู้เดิมในการเจาะระบบที่มีจุดอ่อนแบบเดิม
- กลุ่มความรู้ความชำนาญสูง ทักษะและประสบการณ์สูง สามารถสร้างโค้ดในการเจาะระบบเองได้ ค้นหาจุดอ่อนใหม่ๆได้ เพื่อพบแล้วก็ส่งต่อให้คนอื่น



สคริปต์คิดดี้ส(Script-Kiddies)

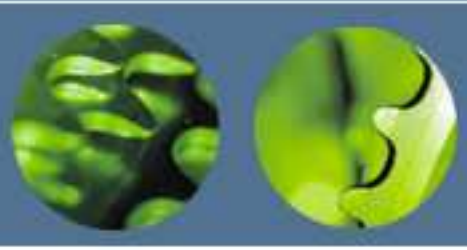
- มีอยู่ในกลุ่มนักเจาะระบบถึง 95%
- มีความรู้ไม่มากนัก อาศัยซอฟต์แวร์ที่โหลดมาช่วยในการเจาะระบบ
- ความชำนาญน้อยกว่าแคร็คเกอร์แต่อาจสร้างความเสียหายมากกว่า
- มีเวลาในการก่อความเสียหายอยู่ในระบบนาน เพราะใช้เครื่องมือช่วย

สายลับ

- สายลับ(Spy) คือคนที่ถูกจ้างมาเพื่อเจาะเข้าระบบ ลักลอบหรือขโมยข้อมูลจากระบบ
- มีเป้าหมายในการเจาะชัดเจน จะสร้างความเสียหายจุดเดียว
- มีทักษะและความชำนาญสูงมากสามารถเจาะจงระบบที่จะโจมตีได้ และส่วนใหญ่จะสำเร็จ
- ทำเพื่อให้มีรายได้ไม่ได้ให้ความสนใจกับข้อมูลที่ได้มา

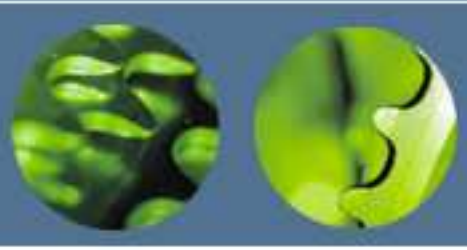
พนักงาน

- นับเป็นอันตรายที่ร้ายแรงที่สุด
  - เพื่อแสดงให้เห็นว่าองค์การมีจุดอ่อนหรือมีช่องโหว่
  - ต้องการแสดงให้เห็นว่าตนเองเก่ง และมีความสามารถ ให้องค์กรเห็นค่า
  - ขโมยข้อมูลไปขายให้คู่แข่ง แลกสินจ้าง
- องค์กรส่วนใหญ่ป้องกันภัยจากข้างนอก



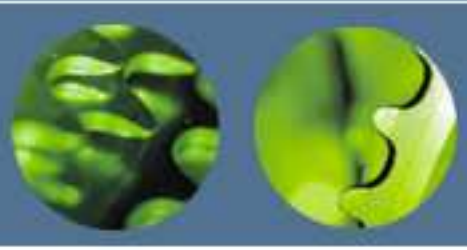
ผู้ก่อการร้ายบนอินเตอร์เน็ต

- ผู้ก่อการร้ายอินเตอร์เน็ต(**Cyberterrorists**) ทำงานบนอุดมการณ์ มีความชำนาญสูง
- เป้าหมายการโจมตีมักเป็นระบบที่ก่อนให้เกิดผลกระทบกับคนส่วนใหญ่
- มักปฏิบัติการเพื่อการสนับสนุนกลุ่มก่อการร้ายด้วยกัน
- การโจมตีคาดการณ์ล่วงหน้าได้ยาก แนวทางการโจมตีอาจเป็น..
  - การเปลี่ยนแปลงข้อมูลบนเว็บไซต์เพื่อส่งข่าวผิดๆ
  - ปฏิเสธการให้บริการแก่ผู้ได้รับอนุญาต
  - เจาะเข้าระบบโดยไม่ได้รับอนุญาตเพื่อทำลายข้อมูล



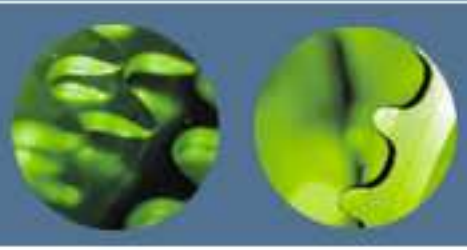
รูปแบบการโจมตี

- วิศวกรรมสังคม(Social Engineering) ใช้หลักจิตวิทยาเช่น การล่อลวง การหลอกถามรหัสผ่าน หลอกถามข้อมูลสำคัญได้แก่การทำ Phishing หรือหลอกให้ทำงานบางอย่างให้
- การเดารหัสผ่าน(Password Guessing) จากการใช้รหัสผ่านง่ายเกินไป ใช้รหัสเดียวกันทุกระบบ ใช้ชื่อหรือสิ่งที่อยู่ใกล้ตัว หรือเขียนไว้บนกระดาษ



รูปแบบการโจมตี(ต่อ)

- Denial of Service ผู้โจมตีจะมีความเสี่ยงน้อยที่สุด เช่น การทำให้ Server ล่มหรือมีงานหนักจนปฏิเสธการให้บริการคนอื่น ผู้โจมตีมักไม่ได้อะไรจากเครื่องนั้นแต่อาจหวังผลเครื่องอื่นแทน
- การถอดรหัสข้อมูล สิ่งสำคัญของการเข้าและถอดรหัสคือ Key การเข้ารหัสด้วยอัลกอริธึมที่ง่ายหรือใช้กันทั่วไป หรือใช้ Key ที่เป็นค่าเริ่มต้น



รูปแบบการโจมตี(ต่อ)

- **Man-in-the-Middle Attacts คือการทำให้คอมพิวเตอร์ 2 เครื่องดูเหมือนสื่อสารกันปกติโดยไม่ทราบว่ามีอีกเครื่องคอยทำการเปลี่ยนแปลงข้อมูลอยู่ รูปแบบการโจมตีที่คล้ายกันคือ Replay Attacks**