บทที่ 3 : การป้องกันการเจาะระบบ Part1

สธ412 ความมั่นคงของระบบสารสนเทศ

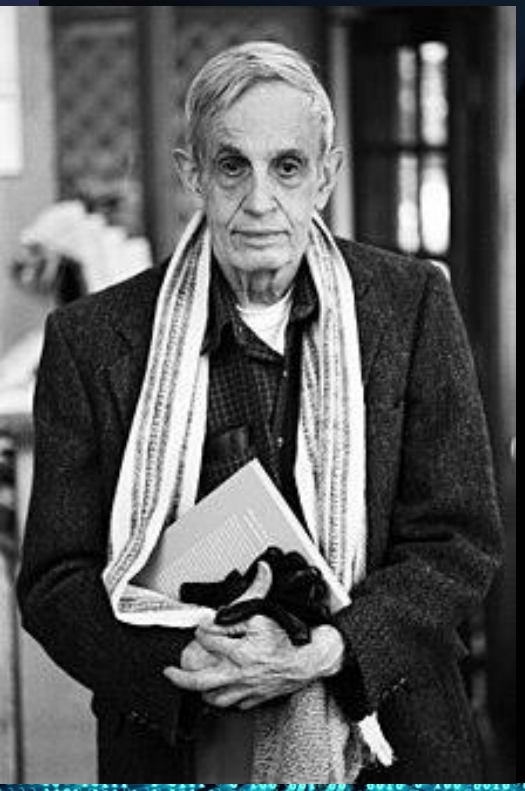
อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Agenda

- การเจาะระบบ
- ประเภทของแฮคเกอร์

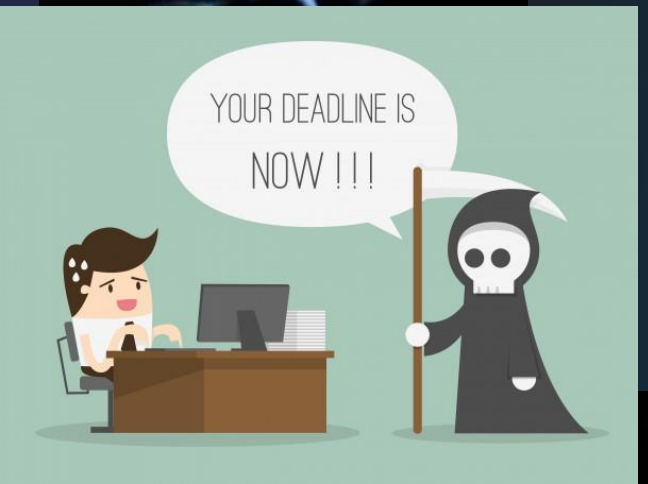
การเจาะระบบ (Hacking)



- “Hack” ผู้ใช้คำนี้เป็นคนแรกคือ “John Nash” นักคณิตศาสตร์ชาวอเมริกัน ในช่วงปลายปี 1950
- ความหมายของการเจาะระบบคือ
  - 1) *“วิธีการแก้ไขปัญหาอย่างชาญฉลาด”*
  - 2) การพยายามเจาะเข้าระบบคอมพิวเตอร์หรือเครือข่ายอื่นโดยที่ไม่ได้รับอนุญาต
- แต่ปกติสังคมจะใช้คำว่า “แฮคกิ้ง” ในความหมายของการกระทำในเชิงลบ

การเจาะระบบ (Hacking) [2]

- ในความเป็นจริงแล้วแฮคเกอร์ส่วนใหญ่จะมีความชำนาญน้อย แต่ก็เพียงพอสำหรับการโจมตีระบบต่างๆได้
- เหตุผลคือระบบคอมพิวเตอร์ส่วนใหญ่ไม่มั่นคง ในขณะออกแบบระบบก็ไม่ได้คำนึงถึงความปลอดภัย
  - ไม่คิดว่าระบบจะถูกใช้งานมายาวนานขนาดนี้
  - มีเวลาในการพัฒนาระบบที่จำกัด ทำให้ผู้พัฒนาไม่มีเวลาพัฒนาระบบรักษาความปลอดภัย



ประเภทของแฮคเกอร์ : Hacker

- มีความหมายทั้งในเชิงลบและเชิงบวก
- อย่างไรก็ตามผู้ที่ใช้ความรู้ในทางบวก ก็ถือว่าเป็นสิ่งผิดกฎหมายอยู่ดี แต่แฮคเกอร์จะมองว่าเป็นเรื่องที่ถูกจริยธรรม ถ้าไม่มีการขโมยข้อมูล ล้วงความลับ หรือทำลายระบบ ซึ่งเป็น “จรรยาบรรณของแฮคเกอร์” (Hacker Code of Ethics)
- การผูกมิตรกับ Ethical Hacker จึงเป็นทางเลือกที่ดีที่จะทำให้ระบบขององค์กรมีความมั่นคงยิ่งขึ้น

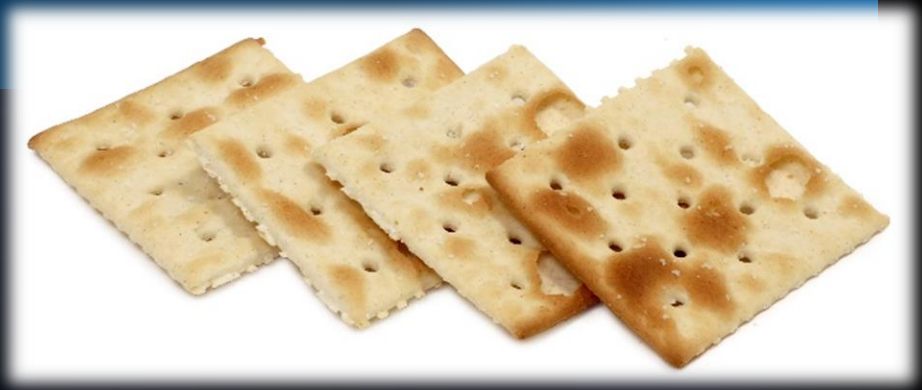

Black hat - Grey Hat - White Hat

ประเภทของแฮคเกอร์ : Hacker

- แรงจูงใจของแฮคเกอร์ที่ดีทำไปเพื่อการพัฒนาระบบให้มีความปลอดภัยมากขึ้น ค้นหาช่องโหว่ก่อนที่จะเกิดเหตุการณ์ไม่พึงประสงค์ขึ้น
- แฮคเกอร์ที่มีจรรยาบรรณจะประกาศว่าพบช่องโหว่หรือติดต่อเจ้าของระบบให้แก้ไขปัญหา
- แฮคเกอร์จะพยายามทำให้เกิดความเสียหายต่อระบบน้อยที่สุด

ประเภทของแฮคเกอร์ : Cracker

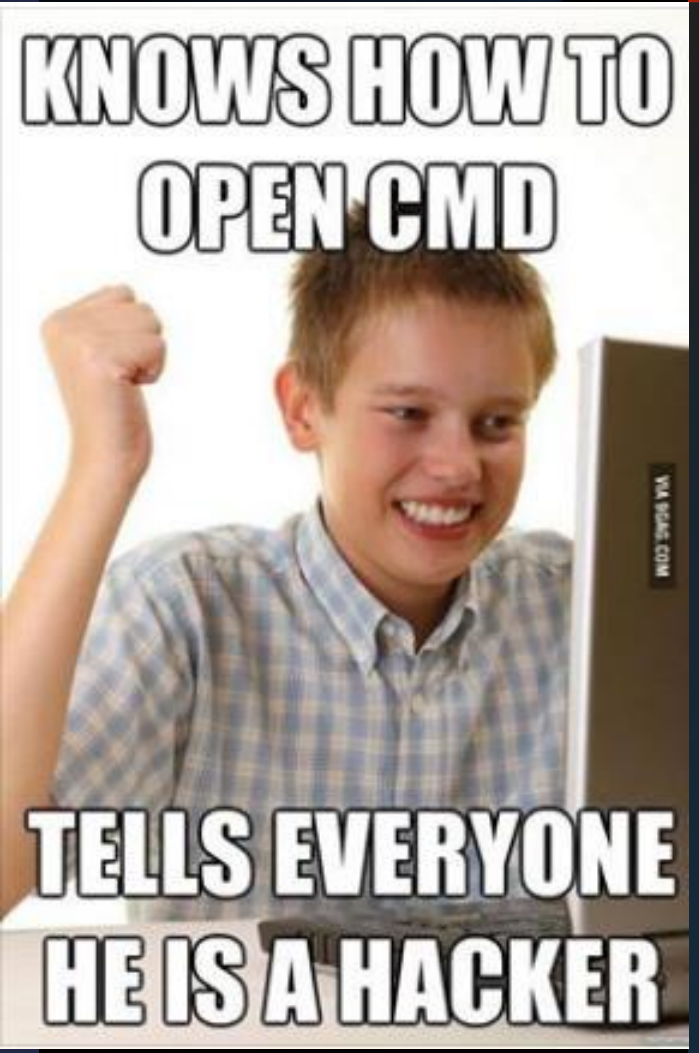
- แครกเกอร์แตกต่างจากแฮคเกอร์ตรงที่แครกเกอร์จะใช้ประโยชน์จากช่องโหว่ในการทำลายระบบ ปฏิเสธการให้บริการ หรือทำให้เกิดปัญหาต่างๆ
- แครกเกอร์จะมีความภาคภูมิใจหากสามารถเจาะเข้าระบบได้และสร้างความเสียหายได้มาก และจะรู้สึกแย่หากได้ยินข่าวว่ามีคนอื่นสามารถเจาะเข้าระบบและทำลายระบบได้มากกว่า



ประเภทของแฮคเกอร์ : Cracker

- แคร็กเกอร์แบ่งออกเป็น 2 กลุ่ม
- 1) กลุ่มที่พอมีความรู้ความชำนาญระดับปานกลาง ส่วนใหญ่จะยังไม่สามารถเขียนโปรแกรมได้เอง หรือจะยังไม่รู้จุดอ่อนใหม่ๆ มีลักษณะเป็นผู้ตามมากกว่าผู้นำ
- 2) กลุ่มที่มีความชำนาญสูง จะดาวน์โหลดซอฟต์แวร์หรือสร้างซอฟต์แวร์เพื่อค้นหาจุดอ่อน และหาวิธีใช้ประโยชน์จากจุดอ่อนนั้น แล้วเผยแพร่ต่อให้ผู้ใช้อื่นนำไปใช้

ประเภทของแฮคเกอร์ : Script-Kiddies



- เป็นกลุ่มที่มีจำนวนมากที่สุด อาจมีประมาณ 95% ของแฮคเกอร์ทั้งหมด
- มีความรู้**พื้นฐาน**เกี่ยวกับคอมพิวเตอร์ เครือข่าย และระบบปฏิบัติการ แต่มีความชำนาญไม่มาก
- ส่วนใหญ่ไม่สามารถเขียนโปรแกรมเองได้ แต่จะหาดาวน์โหลดจากอินเทอร์เน็ต โดยที่ไม่รู้เลยว่าซอฟต์แวร์นั้นทำงานอย่างไรนอกจากรู้ว่าใช้เจาะระบบหรือสร้างความเสียหายกับระบบได้

ประเภทของแฮคเกอร์ :

Script-Kiddies

- ถึงแม้ว่าจะไม่มีความชำนาญเหมือนแคร็คเกอร์ แต่อาจมีอันตรายต่อผู้ใช้ทั่วไปมากกว่า เพราะเป้าหมายการโจมตีเป็นคอมพิวเตอร์ของผู้ใช้ทั่วๆไป จึงเป็นการสร้างปัญหาให้กับคนส่วนมาก

ประเภทของแฮคเกอร์ : สายลับ (Spy)

- หมายถึงบุคคลที่ถูกจ้างเพื่อเข้าระบบ และขโมยข้อมูลบางอย่าง
- สายลับคอมพิวเตอร์จะเจาะเข้าเฉพาะระบบที่มีความสำคัญ แล้วขโมยข้อมูลโดยที่ไม่ให้เจ้าของรู้
- เป็นนักเจาะระบบที่มี**ความรู้ความชำนาญสูงมาก**
- แรงบันดาลใจคือทำเพื่อเงินค่าจ้างหรือผลประโยชน์ส่วนตัว

ประเภทของแฮคเกอร์ : พนักงาน (Employee)

- เป็นภัยคุกคามที่อันตรายต่อองค์กรที่สุด เพราะองค์กรส่วนใหญ่จะพยายามป้องกันภัยคุกคามจากภายนอก ทำให้การป้องกันจากภายในมีความอ่อนแอมาก
- แรงจูงใจ เช่น เพื่อแสดงให้เห็นว่าองค์กรมีจุดอ่อน หรือพนักงานบางคนอาจรู้สึกว่าตัวเองถูกประเมินค่าต่ำไป จึงอยากแสดงความสามารถ หรืออาจมีบริษัทคู่แข่งว่าจ้างให้ทำงานบางอย่างให้

ประเภทของแฮคเกอร์ : ผู้ก่อการร้าย (Terrorist)

- สิ่งที่น่ากลัวในการก่อการร้ายคือ การโจมตีเป็นสิ่งที่คาดเดาได้ยาก หรืออาจเป็นรูปแบบที่ไม่เคยเห็นมาก่อน
- ผู้ก่อการร้ายที่ใช้ช่องทางเครือข่ายคอมพิวเตอร์หรืออินเทอร์เน็ตจะเรียกว่า “Cyberterrorist”
- แรงจูงใจอาจเพื่ออุดมการณ์หรือความเชื่อบางอย่าง

ประเภทของแฮคเกอร์ : ผู้ก่อการร้าย (Terrorist)

- เป้าหมายที่โจมตีอาจเป็นเครือข่ายที่กระทบกับผู้ใช้จำนวนมาก เช่น ระบบคอมพิวเตอร์ที่ควบคุมระบบไฟฟ้า
- ผู้ก่อการร้ายบางกลุ่มจะใช้อินเทอร์เน็ตเพื่อหารายได้สนับสนุนการก่อการร้าย เช่น ขโมยข้อมูลบัตรเครดิต หรือปล่อยมัลแวร์เรียกค่าไถ่ (Ransomware)
- ตัวอย่างเหตุการณ์ เช่น ปี 2002 มีการโจมตี Root Server ที่ 13 ซึ่งเก็บระบบ DNS ของเว็บไซต์จำนวนมาก ทำให้หลายเซิร์ฟเวอร์ไม่สามารถให้บริการได้เป็นเวลาหนึ่งชั่วโมง ซึ่งส่งผลกระทบกับระบบสื่อสารทั่วโลก


003/45/7844
ISAT GeoStar 45
23:15 EST 14 Aug. 2003

สรุปประเภทของแฮคเกอร์

นักโจมตี	ระดับความชำนาญ	แรงจูงใจ
Hacker	สูง	เพื่อชี้ช่องโหว่ของระบบ
Cracker	สูง	เพื่อทำลายระบบ
Script-kiddy	ต่ำ	เพื่อให้ได้รับการยอมรับ, การลองของ, ความคึกคะนอง
Spy	สูงมาก	เพื่อเงิน ผลประโยชน์
Employee	หลากหลาย	หลากหลาย
Terrorist	สูง	เพื่ออุดมการณ์หรือความเชื่อ