คำถามท้ายบทที่ 7

1. อาชญากรรมคอมพิวเตอร์ (Computer Crime) คืออะไร

ผู้กระทำผิดกฎหมายโดยใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือสำคัญในการก่ออาชญากรรมและกระทำความผิดนั้น อาชญากรรมทางคอมพิวเตอร์ ได้มีผู้นิยามให้ความหมายดังนี้ การกระทำการใด ๆ เกี่ยวกับการใช้คอมพิวเตอร์ อันทำให้เหยื่อได้รับความเสียหาย และผู้กระทำได้รับผลประโยชน์ตอบแทน

2. อาชญากรรมคอมพิวเตอร์แตกต่างจาก การใช้คอมพิวเตอร์ในทางที่ผิด (Computer Abuse) อย่างไร

อาชญากรรมคอมพิวเตอร์(Computer Crime) คือการกระทำ ความผิดกฎหมายโดยอาศัย คอมพิวเตอร์เป็น เครื่องมือในการผิดกฎหมายที่ก่อ ให้เกิดวามเสียหายตอ่ ระบบคอมพิวเตอร์

การใช้คอมพิวเตอร์ทางทางที่ผิด (Computer abuse)หมายถึงการกระทำที่เกี่ยวกับ คอมพิวเตอร์ที่ไม่ผิดกฎหมายแต่ผิดด้านจริยธรรม

3. เพราะเหตุใด อาชญากรรมคอมพิวเตอร์และอินเทอร์เน็ตจึงเพิ่มจำนวนมากขึ้นเรื่อยๆ

เทคโนโลยีมีความซับซ่อนมากขึ้น เทคโนโลยีสารสนเทศด้านต่างๆ ไม่ว่าจะเป็นระบบเครือข่าย, เว็บไซต์, โครงสร้างคอมพิวเตอร์ตลอดจนระบบปฏิบัติการและแอปพลิเคชั่นต่างๆ ในปัจจุบันมีการทำงานที่ซับซ่อนมากขึ้น จุดเชื่อมต่อที่โยงในเครือข่ายของหลายองค์กรเข้าด้วยกันมีมากขึ้น

4. การโจมตี (Attack) คืออะไร

การกระทำบางอย่างที่อาศัยความได้เปรียบจากช่องโหว่ของระบบ เพื่อเข้าควบคุมการ ทำงานของระบบ เพื่อให้ระบบเกิดความเสียหาย หรือเพื่อโจรกรรมสารสนเทศ

5. อธิบายการโจมตีแต่ละประเภท

1. Malware คือซอฟต์แวร์หรือโปรแกรมที่มุ่งร้ายต่อเป้าหมาย ถูกออกแบบมาให้ทำหน้าที่สร้าง ความเสียหาย ทำลาย หรือ ระงับการให้บริการของระบบเป้าหมาย

2.ข่าวไวรัสหลอกลวง (Virus and Worm Hoaxes)คือวิธีการสร้างความสับสนให้กับผู้ใช้ด้วยข่าว ไวรัสหลอกลวง ที่ถูกส่งต่อๆ กนั มาในรูปของอีเมล์ทำให้องค์กร ต้องเสียเวลาและค่าใช้จ่ายไปกบัการ ค้นหาวิธีกำจัดไวรัสจากข่าวหลอกลวงดังกล่าวซึ่งไม่มีอยู่จริง

3.การเจาะรหัสผ่าน (Password Cracking) การบุกรุกเข้าไปในระบบคอมพิวเตอร์ของผู้ใช้ใด ๆ โดย หากเป็น Password Cracking จะเป็น การบุกรุกโดยใช้วิธีเจาะรหัสผ่าน

4. Brute Force Attack เป็นการพยายามคาดเดารหัสผ่าน โดยการนำคีย์ที่เป็นไปได้ทั้งหมดมาจดัหมู่ (Combination)

5. Dictionary Attack เป็นการโจมตีแบบ Brute Force อีกรูปแบบหนึ่ง ที่คาดเดารหัสผ่านจาก ขอบเขตที่แคบลง

6.Denial of Service การปฏิเสธการให้บริการของระบบ เป็นการโจมตีโดยใช้วิธีส่งขอ้มูลจำนวน มากไปยังเป้าหมาย ทำให้แบนวิดธ์ เต็มจนไม่สามารถให้บริการต่อไปได้

7.Spoofing เทคนิคที่ทำให้เข้าถึงระบบเป้าหมายได้โดยไม่ได้รับอนุญาตด้วยการใช้ IP Address ของ Server/Host ที่เชื่อถือได้เป็นตัวหลอกล่อ

8. TCP Hijacking Attack เป็นการโจมตีที่ผู้โจมตีจะใช้วิธีคอยติดตาม Packet จากเครือข่ายจากนั้นดักจับ Packet ดังกล่าวมาทำการดัดแปลงให้เป็นของตน

9.Spam เป็นการใช้อีเมล์เพื่อการโฆษณาหรือประชาสัมพันธ์สินค้าและบริการต่างๆ ซึ่งอาจสร้าง ความรำคาญให้กับผู้ใช้ในบางครั้งอาจมีการแนบ Virus และ Worm มากับอีเมลด้วย

10. Mail Bombing เป็นการโจมตีทางอีเมลอีกรูปแบบหนึ่ง ซึ่งมีลักษณะการทำลายแบบ DoS

11.Sniffers เป็นโปรแกรมหรืออุปกรณ์ที่สามารถอ่าน ติดตาม และดักจับข้อมูลที่วง อยู่ในเครือข่าย ได้ นอกจากนี้ยังสามารถอ่าน Packet ในเครือข่ายได้เช่นกัน

12.Social Engineering “วิศวกรรมทางสังคม คือ การใช้ทักษะทางสังคมในการหลอกลวงเหยื่อให้ เปิดเผยขอ้ มูลส่วนตัวหรือข้อมูล ที่เป็นความลับ เพื่อนำไปใช้ประโยชน์ในทางที่ผิดหรือขัดต่อกฎหมาย

13. Buffer Overflow “บัฟเฟอร์ลัน” เป็นการโจมตีโดยการส่งขอ้มูลเข้าสู่ระบบจำนวนมากเกินกว่า เนื้อที่ในบัฟเฟอร์

14. Timing Attack เป็นการโจมตีโดยการขโมยข้อมูลที่จัดเก็บอยู่ใน Cache ของโปรแกรม Web Browser โดยผู้โจมตีจะสร้างไฟล์ Cookies ที่เป็นอันตรายขึ้นมาแล้วบีนทึกไว้ในเครื่องของผู้ใช้ทัน ทีที่เข้าไปเยี่ยมชมเว็บไซต์ที่เป็นอันตราย

15. Zero-day Attack เป็นการโจมตีโดยการพยายามเจาะช่องโหว่ที่องค์กรยังไม่ได้เผยแพร่การ ค้นพบช่องโหว่ดังกล่าวต่อสาธารณะ

6. Virus, Worm, Trojan Horse และ Zombie จัดว่าเป็นการโจมตีในประเภทใด

เป็นการโจมตีในรูปแบบ Malware

7. อธิบายความแตกต่างของการโจมตีในข้อ 6

- Virus = แพร่เชื้อไปติดไฟล์อื่น ๆในคอมพิวเตอร์โดยการแนบตัวมันเองเข้าไป มันไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่น ๆได้ต้องอาศย์ไฟล์พาหะ สิ่งที่มัน ทำคือสร้าง ความเสียหายให้กับไฟล์

- Worm = คัดลอกตัวเองและสามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่น ๆได้อย่างอิสระ โดยอาศัยอีเมลหรือช่องโหว่ของระบบปฏิบัติการ มักจะไม่แพร่เชื่อไปติดไฟล์อื่น สิ่งที่มันทำคือมักจะสร้างความเสียหายให้กับระบบเครือข่าย

- Trojan = ไม่แพร่เชื่อไปติดไฟล์อื่น ๆ ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่น ๆ ได้ต้องอาศัยการหลอกคนใช้ให้ด้าวโหลดเอาไปใส่เครื่องเองหรือด้วยวิธีอื่น ๆ สิ่งที่มันทำ คือเปิดโอกาสให้ผู้ไม่ประสงค์ ดีเข้ามาควบคุมเครื่องที่ติดเชื้อจากระยะไกล ซึ่งจะทำอะไรก็ ได้ และโทรจันยังมีอีกหลายชนิด

- ซอมบี้ (Zombie) เป็นโปรแกรมที่เข้าควบคุมการทำงานของคอมพิวเตอร์ที่ตนเองฝังตัวอยู่ จากนั้นจึงใช้คอมพิวเตอร์ดังกล่าวเป็น เครื่องมือในการโจมตีเป้าหมาย เพื่อกระทำการใด ๆ ที่เป็นประโยชน์ต่อผู้สั่งโจมตี (Attacker)

8. การโจมตีแบบเจาะรหัสผ่านมีกี่ประเภท แต่ละประเภทแตกต่างกันอย่างไร

- Brute Force Attack เป็นการพยายามคาดเดารหัสผ่าน โดยการนำคีย์ที่เป็นไปได้ทั้งหมดมาจัดหมู่ (Combination) ดังนั้น การคาดเดา รหัสผ่านในลักษณะนี้จึงเป็นการคำนวณซ้ำหลายๆ รอบ เพื่อให้ได้กลุ่มรหัสผ่านที่ถูกต้อง

- Dictionary Attack เป็นการโจมตีแบบ Brute Force อีกรูปแบบหนึ่ง ที่คาดเดารหัสผ่านจากขอบเขตที่แคบลง นั่นคือคาดเดาจากคำ ในพจนานุกรม การเจาะรหัสผ่านวิธีนี้คิดค้นขึ้นมาบนสมมติฐานที่ว่า ผู้ใช้งานบางส่วนมักจะกำหนดรหัสผ่านจากคำง่ายๆ

- Denial-of-Service คือ การปฏิเสธการให้บริการของระบบ เป็นการโจมตีโดยใช้วิธีส่งข้อมูลจนวนมากไปยังเป้าหมาย ทำให้แบนวิดธ์ เต็มจนไม่สามารถให้บริการต่อไปได้

- Spoofing คือ เทคนิคที่ทำให้เข้าถึงระบบเป้าหมายได้โดยไม่ได้รับอนุญาตด้วยการใช้ IP Address ของ Server/Host ที่เชื่อ ถือได้เป็นตัวหลอกล่อ

9. Social Engineering คืออะไร

Social Engineering “วิศวกรรมทางสังคม คือ การใช้ทักษะทางสังคมในการหลอกลวงเหยื่อให้ เปิดเผยข้อมูลส่วนตัวหรือข้อมูล ที่เป็นความลับเพื่อนำไปใช้ประโยชน์ในทางที่ผิดหรือขัดต่อกฎหมาย

10. อธิบายลักษณะการโจมตีแบบ Zero-day Attack

เป็นการโจมตีโดยการพยายามเจาะช่องโหว่ที่องค์กรยังไม่ได้เผยแพร่การค้นพบช่องโหว่ดังกล่าวต่อ สาธารณะหรือยงไม่ได้แจ้งข่าวช่องโหว่ต่อผู้พัฒนาซอฟต์แวร์

7.1 60160305 บุคคลในข้อใดไม่จัดเป็นการทำกระทำผิดทาง อาชญากรรมคอมพิวเตอร์

1. สมคิด แอบเปิดคอม สมชาย เพื่อคัดลอกงาน มาแอบอ้างมันเป็นของตน
2. สมชาย ทำการโจมดี สมพร ด้วยวิธี Zero-day Attack
3. สมพร Spam ข่าวทางเมล ให้สมคิด
4. สมรักษ์ ทำการ Spoofing โดยใช้ IP Address ของ สมพร

เฉลย 1. สมคิด แอบเปิดคอม สมชาย เพื่อคัดลอกงาน มาแอบอ้างมันเป็นของตน