รวบรวมคำศัพท์น่ารู้ด้าน Security

- **Administrative Security**

เป็นการบริหารเรื่องความปลอดภัยที่ผู้ดูแลระบบความปลอดภัย มีการกำหนดการจัดการความเสี่ยงและควบคุมการทำงานต่าง ๆ ให้อยู่ในระดับความปลอดภัยในระดับที่มาตรฐานเพื่อป้องกันการแฮ็คเข้าระบบจากอาชญากรที่มีในปัจจุบันอย่างมากมาย

- **Authentication**

การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องในการเข้าใช้ระบบ **(Identity)** เพื่อแสดงตัวว่ามีสิทธิในการเข้าใช้ระบบได้จริง

- **Active Attack**

การโจมตีที่ทำให้เกิดการเปลี่ยนสถานะโดยไม่ได้รับอนุญาต เช่นการเปลี่ยนแปลง **file** หรือการเพิ่ม **file** ที่ไม่ได้รับอนุญาตเข้าไป

- **Audit**

การตรวจสอบที่กระทำอย่างอิสระเพื่อให้มั่นใจว่าบันทึกและกิจกรรมต่างๆ เป็นไปตามการควบคุม นโยบาย และระเบียบปฏิบัติที่ได้จัดตั้งขึ้น และเพื่อแนะนำการเปลี่ยนแปลงต่าง ๆ ในการควบคุม นโยบาย และระเบียบปฏิบัติเหล่านั้น

- **Auditing**

การตรวจสอบที่กระทำอย่างอิสระเพื่อให้มั่นใจว่าบันทึกและกิจกรรมต่างๆ เป็นไปตามการควบคุม นโยบาย และระเบียบปฏิบัติที่ได้จัดตั้งขึ้น

- **Access Control**

การควมคุมการเข้าถึง ระบบการควบคุมการเข้าออกพื้นที่

- **Alert**

การแจ้งเตือนเป็นข้อความที่ถูกเขียนขึ้นมาเพื่อใช้อธิบายสถานการณ์ที่เกี่ยวข้อง กับความปลอดภัย การแจ้งเตือนมักจะเกิดมาจากการตรวจสอบแล้วพบสิ่งที่อาจมีผลกระทบต่อระบบ จึงมีการแจ้งเตือนเพื่อดำเนินการป้องกัน

รวบรวมคำศัพท์น่ารู้ด้าน Security

- **Botnet**

Botnet คือคอมพิวเตอร์ที่ติด **Malware** และรอรับคำสั่งจากแฮกเกอร์เพื่อนำไปใช้ในทางที่ไม่ดี เช่น **DDoS** วิธีป้องกันคืออัปเดตซอฟต์แวร์อย่างสม่ำเสมอและใช้ Firewall

- **Brandjacking**

คนร้ายสร้างเว็บไซต์หรืออีเมลที่มีความคล้ายคลึงกับแบรนด์ที่เป็นที่รู้จัก เพื่อหลอกให้เหยื่อหลงเชื่อและกรอกข้อมูลส่วนตัว **Brandjacking** มีโอกาสสำเร็จมากกว่าอาชญกรรมทางไซเบอร์อื่นๆ เนื่องจากการใช้ชื่อของแบรนด์สามารถเพิ่มความน่าเชื่อถือได้

- **Blackhat hacker**

แฮคเกอร์ที่ใช้ทักษะโปรแกรมมิ่งสร้างความเสียหายกับคอมพิวเตอร์หรือทำสิ่งผิดกฎหมาย

- **Backdoor**

จะมีหลักการทำงานเหมือนกับ **client-server** ซึ่งตัวมันเองจะทำหน้าที่เปิดทางให้ผู้ไม่ประสงค์ดีสามารถรีโมทเข้าไปเครื่องคอมพิวเตอร์ส่วนใหญ่แล้วจะมากับการติดตั้งแอพพลิเคชั่นที่ผิดกฎหมาย

- **Boot virus**

ไวรัสที่แพร่กระจายเข้าสู่เครื่องคอมพิวเตอร์ในขณะที่ทำการบูตเครื่องเช่น การนำแผ่นดิสก์ที่มีไวรัสอยู่ ไปใช้กับเครื่องอื่นๆ จะทำให้เครื่องนั้นติดไวรัสทันทีที่ทำการ **boot** เครื่อง

- **Confidentiality**

ความสามารถในการรักษาความลับของระบบ การควบคุมการเข้าถึงข้อมูลเพื่อไม่ให้ผู้ที่ไม่มีสิทธิเข้าถึงความลับใดๆ เช่น หากเรามีการเก็บข้อมูลส่วนบุคคลไว้ เช่น เลขบัตรประชาชน เบอร์โทร โรคประจำตัว หน้าที่ของระบบคือการจัดการความปลอดภัยไม่ให้คนที่ไม่มีสิทธิเข้ามาดูข้อมูลของเราไปได้

รวบรวมคำศัพท์น่ารู้ด้าน Security

- **Compliance**

การปฏิบัติตามกฎระเบียบข้อบังคับ และ กฎหมาย ตลอดจนการปฏิบัติตามนโยบายด้านสารสนเทศและความปลอดภัยขององค์กรอย่างถูกต้อง ได้ตามมาตรฐาน

- **Credibility**

การแจ้งเตือนเป็นข้อความที่ถูกเขียนขึ้นมาเพื่อใช้อธิบายสถานการณ์ที่เกี่ยวข้อง กับความปลอดภัย การแจ้งเตือนมักจะเกิดมาจากการตรวจสอบแล้วพบสิ่งที่อาจมีผลกระทบต่อระบบ จึงมีการแจ้งเตือนเพื่อดำเนินการป้องกัน

- **Cost Reduction**

การทำให้ต้นทุนทุกชนิดที่เกิดขึ้นในทุกขั้นตอนของกระบวนการทำงานลดต่ำลง โดยการปรับปรุงแก้ไขกิจกรรมที่เคยทำมาก่อนหน้า ซึ่งมีการตั้งเป้าหมาย วิธีการวัดและการเปรียบเทียบที่ชัดเจน เช่น ต้นทุนในการจัดซื้อ จัดจ้าง ต้นทุนค่าแปรรูป เป็นต้น

- **Computer Security**

ความเสี่ยงต่อการเกิดความ เสียหายต่อคอมพิวเตอร์และข้อมูล ทั้งเหตุการณ์หรือการใช้งานที่ก่อให้เกิดความเสียหายต่อฮาร์ดแวร์, ซอฟท์แวร์, ข้อมูล, และความสามารถในการประมวลผลข้อมูลรูปแบบของความเสี่ยงเหล่านี้อาจอยู่ในรูปของอุบัติเหตุ

- **Command-and-control server**

เป็นเซิร์ฟเวอร์ที่ใช้ในการควบคุม **Botnet** โดยที่แฮคเกอร์จะป้อนคำสั่งผ่านเซิร์ฟเวอร์นี้เพื่อส่งต่อไปยัง **Botnet**

- **Cracker**

ผู้ที่ลักลอบบุกรุกเข้าใช้ระบบ โดยผิดกฎหมาย เพื่อจุดประสงค์ใดๆ อาจบุกรุกเพื่อการทำลาย ระบบ และ รวมทั้งการลักลอบขโมยข้อมูลของบุคคลอื่นเพื่อไปเป็นประโยชน์ โดยกระทำของ **cracker** มีเจตนามุ่งร้ายเป็นสำคัญ

รวบรวมคำศัพท์น่ารู้ด้าน Security

- **Cookie**

กลุ่มของข้อมูลที่ถูกส่งจากเว็บเซิร์ฟเวอร์มายังเว็บบราวเซอร์และถูกส่งกลับมายังเว็บเซิร์ฟเวอร์ทุกๆครั้งที่เว็บบราวเซอร์ร้องขอข้อมูล โดยปกติแล้วคุกกี้จะถูกใช้เพื่อจัดเก็บข้อมูลขนาดเล็กๆไว้ที่เว็บราวเซอร์ เพื่อให้เว็บเซิร์ฟเวอร์สามารถจดจำสถานการณ์ใช้งานของเว็บบราวเซอร์ที่มีต่อเว็บเซิร์ฟเวอร์

- **DDoS**

คือการใช้ **Botnet** หลายๆ เครื่องเพื่อโจมตีเป้าหมายในเวลาเดียวกันและทำให้เว็บไซต์ล่มในที่สุด ถ้าอธิบายให้เข้าใจโดยง่าย ให้คุณลองจิตนาการว่า นี่เป็นวันแรกของการลงทะเบียนเรียนในเว็บไซต์แต่คุณไม่สามารถเข้าเว็บไซต์ได้แม้จะรีเฟรชหลายรอบแล้ว สาเหตุคือมีจำนวนคนเข้าใช้พร้อมกันมากเกินกว่าที่เซิร์ฟเวอร์รองรับได้และทำให้ระบบล่ม

- **DoS Attack**

การขัดขวางหรือก่อกวนระบบเครือข่ายหรือ **Server** จนทำให้เครื่อง **Server** หรือเครือข่ายนั้นๆ ไม่สามารถทำงานได้ตามปกติ

- **Digital Certificate**

ด้วยการลงรหัส และ ลายมือชื่อดิจิทัล ในการทำธุรกรรม เราสามารถรักษาความลับของข้อมูล สามารถรักษาความถูกต้องของข้อมูล และสามารถระบุตัวบุคคลได้ระดับหนึ่ง เพื่อเพิ่มระดับความปลอดภัยในการระบุตัวบุคคลโดยสร้างความเชื่อถือมากขึ้นด้วย ใบรับรองดิจิทัล

- **Decryption**

การถอดรหัสข้อมูล การแปลงข้อความหรือข้อมูลอิเล็กทรอนิกส์จากรูปแบบที่ถูกเปลี่ยนแปลงไปจากเดิม **(cipher text)** ให้กลับไปอยู่ในรูปของข้อความหรือข้อมูลอิเล็กทรอนิกส์รูปแบบเดิมก่อนการเปลี่ยนแปลง **(plaintext)**

รวบรวมคำศัพท์น่ารู้ด้าน Security

- **Encryption**

การเข้ารหัสข้อมูล การแปลงข้อความหรือข้อมูลอิเล็กทรอนิกส์รูปหนึ่งที่อ่านได้ **(plaintext)** ให้อยู่ในรูปแบบหนึ่งที่เปลี่ยนแปลงไปจากเดิมและอ่านไม่ได้ **(cipher text)**

- **File Virus**

ไวรัสไฟล์ข้อมูล โดยมากจะติดกับๆไฟล์ที่มักเรียกใช้บ่อย เช่น ไฟล์นามสกุล **.exe, .dll,.com** ตัวอย่าง **Jerusalem, Die Hard II**

- **Firewall**

การรักษาความปลอดภัยของระบบคอมพิวเตอร์แบบหนึ่ง จะทำหน้าที่ควบคุมการใช้งานระหว่าง **Network** ต่าง ๆ จะคอยตรวจสอบข้อมูลที่ผ่านเข้ามาเพื่อป้องกันข้อมูลที่ไม่พึงประสงค์ ตลอดจนข้อมูลที่ไมมีความสมบูรณ์เข้ามาสร้างความเสียหายกับระบบ เปรียบเสมือนยามรักษาความปลอดภัยของระบบระดับหนึ่ง

- **Fake Webpage**

หน้า **webpage** ที่ **Phishes** พยายามสร้างขึ้นมาให้เหมือนหรือใกล้เคียงกับ **site** จริงมากที่สุด เพื่อให้เหยื่อผู้หลงเชื่อกรอกข้อมูลส่วนตัวต่างๆ ที่ต้องการลงไป

- **Fraggle Attack**

เหมือนกับ **Smurf Attack** แต่เปลี่ยนเป็นใช้ **Packet** ของ **UDP** แทน

- **False Negative**

การเกิดมีการบุกรุกเกิดขึ้นแต่ระบบไม่ทำการป้องกันแต่เปิดโอกาสให้เกิดการบุกรุกขึ้น โดยระบบคิดว่าปลอดภัย

รวบรวมคำศัพท์น่ารู้ด้าน Security

- **Gateway**

จุดต่อเชื่อมของเครือข่ายทำหน้าที่เป็นทางเข้าสู่ระบบเครือข่ายต่าง ๆ บนอินเตอร์เน็ต ส่วนช่วยเครื่องคอมพิวเตอร์ที่ควบคุมการจราจรภายในเครือข่าย

- **Hardware Control**

การควบคุมความปลอดภัยของระบบโดยฮาร์ดแวร์ โดยเลือกใช้เทคโนโลยีทางด้านฮาร์ดแวร์ ที่สามารถควบคุมการเข้าถึง และป้องกันการทำงานผิดพลาด ด้วยอุปกรณ์ภายในตัวเอง

- **Hacking**

การใช้โดยไม่ได้รับอนุญาต การลักลอบเข้าสู่ระบบ พยายามที่จะข้ามผ่านระบบรักษาความปลอดภัยเพื่อเข้าสู่ระบบข้อมูลและ เครือข่าย เพื่อวัตถุประสงค์ใดๆ อันก่อให้เกิดความเสียหาย หรือไม่มีวัตถุประสงค์ร้ายเพียงแต่ลองวิชา โดยส่วนใหย่มีวัตถุประสงค์ในการทดสอบขีดความสามารถของตนเอง หรือทำในหน้าที่การงานของตนเอง

- **Information Security**

การศึกษาถึงความไม่ปลอดภัยในการใช้งานสารสนเทศที่เกี่ยวข้องกับคอมพิวเตอร์ การวางแผนและการจัดระบบความปลอดภัยในคอมพิวเตอร์

- **Integrity**

การประกันว่าสารสนเทศสามารถได้รับการถึงหรือปรับปรุงโดยผู้ได้รับอำนาจเท่านั้น มาตรการใช้สร้างความมั่นใจ **integrity** ได้แก่ การควบคุมสภาพแวดล้อมทางกายภาคของจุดปลายทางเครือข่ายและแม่ข่าย จำกัดการเข้าถึงข้อมูล และรักษาวิธีปฏิบัติการรับรองอย่างเข้มงวด **data integrity** สามารถได้รับการคุกคามโดยอันตรายจากสภาพแวดล้อม

- **ImplementationVulnerability**

ความล่อแหลมช่องโหว่ที่เกิดจากการใช้งาน **hardware** หรือ **software** ที่ออกแบบมา อาจเกิดขึ้นจากตัวผู้ใช้งานเองหรือความผิดพลาดของระบบ

รวบรวมคำศัพท์น่ารู้ด้าน Security

- **IP Splicing/Hijacking**

การกระทำซึ่งมีการดักจับและใช้ร่วมกันของ **session** การเข้าใช้ระบบ ที่ถูกจัดตั้งแล้วและกำลังดำเนินอยู่ โดยผู้ใช้ที่ไม่ได้รับอนุญาตเป็นผู้กระทำการโจมตีแบบนี้อาจเกิดขึ้นหลังจากที่ได้มีการ **authenticate** คือ การล็อคอินเข้าสู่ระบบ

- **Incident**

การละเมิดความปลอดภัยคอมพิวเตอร์และเครือข่าย การโจมตีที่สามารถเห็นได้ชัดเจนถึงผู้โจมตี วิธีการโจมตีจุดมุ่งหมายที่เกี่ยวข้อง และเวลาที่โจมตี

- **Key Logger**

อาชญากรรมที่เกิดขึ้นกับคอมพิวเตอร์ที่รุนแรงมากอย่างหนึ่ง เพราะผู้ไม่หวังดีจะบันทึกการกดแป้นพิมพ์บนคอมพิวเตอร์ของคุณ ขโมยข้อมูลทุกอย่างที่อยู่บนเครื่อง และความลับทุกอย่างที่คุณพิมพ์บนเครื่องคอมพิวเตอร์ของคุณไป.เพื่อข่มขู่ แบล็กเมล นำรหัสบัตรเครดิตไปซื้อสินค้า รวมทั้งนำข้อมูลไปใช้ในทางมิชอบอื่นๆ

- **Key pair**

ระบบการเข้ารหัสและถอดรหัสข้อมูล โดยผู้ส่งและผู้รับจะมีกุญแจคนละดอกที่ไม่เหมือนกัน ผู้ส่งใช้กุญแจดอกหนึ่งในการเข้ารหัสข้อมูลที่เรียกว่า กุญแจสาธารณะ **(Public key)**

- **Mail Bomb**

การส่ง **Mail** ที่มีขนาดใหญ่เป็นจำนวนมากเข้าไปเพื่อให้เนื้อที่ใน **Mail box** เต็ม

- **Malware**

คือประเภทของโปรแกรมคอมพิวเตอร์ที่ถูกสร้างขึ้นมา โดยมีจุดมุ่งหมายเพื่อที่จะทำลายหรือสร้างความเสียหายให้แก่ระบบคอมพิวเตอร์ ระบบเครือข่าย หรือทรัพย์สินและข้อมูลของผู้ใช้งานคอมพิวเตอร์ ประเภทของ **malware** ต่างๆ

รวบรวมคำศัพท์น่ารู้ด้าน Security

- **Misuse Detection Model**

การตรวจจับการบุกรุกโดยตรวจกิจกรรมเกี่ยวกับเทคนิคการบุกรุกที่ทราบหรือกิจกรรมเกี่ยวกับความล่อแหลมของระบบ

- **Network Security Officer**

เจ้าหน้าที่รักษาความปลอดภัยเครือข่าย ผู้ซึ่งได้รับมอบหมายอย่างเป็นทางการจากผู้ซึ่งมีอำนาจหน้าที่ให้มีการปฏิบัติอย่างถูกต้องในเรื่องที่เกี่ยวข้องภายในระบบข้อมูลอัตโนมัติ

- **Operations Security (OPSEC)**

เป็นมาตรการ หรือวิธีการอย่างเป็นระบบที่ใช้ในการระบุ **(identify)** ควบคุม **(Control)** และป้องกัน **(Protect)** หลักฐานทั่วไปที่ไม่ระบุชั้นความลับ ที่เกี่ยวข้องหรือเชื่อมต่อกับการปฏิบัติการหรือกิจกรรมต่างๆ ที่สำคัญ หรือละเอียดอ่อน ซึ่งแตกต่างกับมาตรการรักษาความปลอดภัยทั่วไปที่เน้นในการรักษาความปลอดภัยเฉพาะข้อมูลข่าวสารที่มีชั้นความลับ

- **Phishing**

Phishing คือการโจรกรรมข้อมูลส่วนตัว โดยทำการปลอมแปลงอีเมลให้เหมือนกับอุตสาหกรรมที่มีความน่าเชื่อถือ เช่น ธนาคารหรือบริษัทโทรคมนาคม ภายในอีเมลจะอธิบายให้เหยื่อกดลิ้งค์ที่ให้มาและกรอกข้อมูลส่วนตัว เช่น บัญชีธนาคารหรือบัตรเครดิต

- **Policy**

กฎและข้อห้ามต่าง ๆ ที่ผู้ดูแลเป็นผู้กำหนด

- **Privacy**

ความเป็นส่วนตัวของข้อมูลและสารสนเทศ

- **Ping of Death**

การส่ง **Packet Ping** ที่มีขนาดใหญ่เกินกว่าปกติเข้าไปที่เครื่องเป้าหมาย

รวบรวมคำศัพท์น่ารู้ด้าน Security

- **Packet Filtering**

คุณลักษณะที่เพิ่มเข้าไปใน **router** หรือ **bridge** เพื่อที่จะจำกัด การไหลของข้อมูลตามข้อกำหนดที่ตกลงกันไว้ก่อน เช่น แหล่งส่ง แหล่งรับ หรือชนิดของบริการที่เครือข่ายมีให้ **Packet filtering** ช่วยให้ **administrator** จำกัด traffic ของ **protocol** หนึ่งๆ ให้อยู่ภายในเครือข่ายหนึ่งๆ แยก **domain e-mail** ต่างๆ ออกจากกัน และช่วยในหน้าที่ควบคุม **traffic** อื่นๆ อีกมาก

- **Passphrase**

รหัสที่ใช้ในการสร้างคีย์ที่เป็นตัวเลขฐาน **16 (HEX)** ตั้งรหัสผ่าน **5** ตัวอักษร สำหรับการเข้ารหัส **64 Bit** หรือ **13** ตัวอักษร สำหรับ **128 Bit** เมื่อคลิก **Submit** จะเป็นการสร้างคีย์ **(Key)** จำนวน **4** ชุด ในช่อง **Key0-4 Key** จะใช้ในการเริ่มต้นการเชื่อมต่อเครื่องคอมพิวเตอร์ลูกข่ายกับ **Access Pointv**

- **Perpetrator**

สิ่งที่มาจากสภาพแวดล้อมภายนอกที่เป็นสาเหตุของความเสี่ยง ที่จะกระทำการโจมตีระบบให้เกิดความเสียหาย

- **PKI (Public Key Infrastructure)**

ระบบป้องกันข้อมูลวนการสื่อสารผ่านเครือข่ายอินเตอร์เน็ต โดยมีหลักการทำงาน โดยใช้กุญแจคู่ **(Key pairs)** ในการเข้ารหัสและถอดรหัสข้อมูล โดยกุญแจนี้ประกอบด้วย กุญแจส่วนตัว **(Private Key)** และกุญแจสาธารณะ **(Public Key)**

- **Penetration Testing**

ส่วนหนึ่งของการทดสอบความปลอดภัย โดยที่ผู้ประเมินพยายามที่จะข้ามผ่านระบบรักษาความปลอดภัยของระบบผู้ประเมิน อาจจะใช้เอกสารเกี่ยวกับการใช้และการออกแบบระบบทั้งหมดที่มีอยู่ ซึ่งอาจรวมถึง **source code** คู่มือ และผังวงจร ผู้ประเมินจะทำงานภายใต้ข้อจำกัดเดียวกับผู้ใช้ธรรมดาทั่วๆ ไป

รวบรวมคำศัพท์น่ารู้ด้าน Security

- **Passive Threat**

การคุกคามในการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต เป็นชนิดของการคุกคามที่เกี่ยวข้องกับการดักจับข้อมูลแต่ไม่มีการเปลี่ยนแปลงข้อมูลใดๆ

- **Packet**

หน่วยย่อยของข้อมูล ซึ่งเป็นการแบ่งข้อมูลออกเป็นส่วนย่อยๆ ช่วยให้การแลกเปลี่ยนข้อมูลผ่านระบบอินเตอร์เน็ตนั้นเร็วขึ้น แทนการส่งแบบที่ส่งข้อมูลไปทั้งหมดทั้งก้อน ซึ่งทำให้ส่งได้ช้า โดยแต่ละส่วนย่อยจะถูกส่งไปยังจุดหมายพร้อมๆกัน ซึ่งแต่ละอันจะจ่าหน้าถึงผู้รับเดียวกัน

- **Ping**

รับการส่งถึง หรือตรวจการปรากฏของ ของอีกฝ่ายที่ทำงานอยู่บนระบบ การทำงานของ **ping** เป็นการส่งแพ็คเกตไปยัง **address** ปลายทางและรอการตอบสนอง เพื่อทดสอบการเชื่อมต่อ

- **Ransomware**

Ransom หรือการเรียกค่าไถ่ของผู้ร้ายในวงการ **IT** จะทำด้วยการล็อคคอมพิวเตอร์และไฟล์ของเหยื่อ เพื่อแลกกับการใช้งานคอมพิวเตอร์และไฟล์อีกครั้ง ผู้ใช้งานจะต้องจ่ายเงินค่าไถ่ตามที่ผู้ร้ายกำหนดหนึ่งใน **Ransomware** ที่เป็นที่รู้จักคือ **WannaCry** ที่เกิดขึ้นในปี **2017** ซึ่งทำให้เกิดความเสียหายจำนวนมาก โดยเป้าหมายอยู่ที่คอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ **Windows** ที่ยังไม่ได้รับการอัพเดทเป็นเวอร์ชั่นล่าสุด

- **Spyware**

spyware เป็นซอฟต์แวร์ที่ติดตั้งมากับอุปกรณ์โดยที่ผู้ใช้ไม่รับรู้ เป้าหมายหลักของซอฟต์แวร์นี้คือขโมยข้อมูลส่วนตัวหรือข้อมูลลับ นอกจากขโมยข้อมูลส่วนตัวแล้ว **spyware** ยังสามารถเปลี่ยน **settings** ของคอมพิวเตอร์เป้าหมายได้ด้วย ถ้าหากคุณเห็นซอฟต์แวร์ที่ไม่คุ้นเคยบนอุปกรณ์ของตัวเอง คุณควรหาข้อมูลเพิ่มเติมหรือถามผู้ที่เชี่ยวชาญด้านนี้แล้วลบซอฟต์แวร์นั้นออกให้เร็วที่สุด

รวบรวมคำศัพท์น่ารู้ด้าน Security

- **Spoofing**

กลุ่มของข้อมูลที่ถูกส่งจากเว็บเซิร์ฟเวอร์มายังเว็บบราวเซอร์และถูกส่งกลับมายังเว็บเซิร์ฟเวอร์ทุกๆครั้งที่เว็บบราวเซอร์ร้องขอข้อมูล โดยปกติแล้วคุกกี้จะถูกใช้เพื่อจัดเก็บข้อมูลขนาดเล็กๆไว้ที่เว็บราวเซอร์ เพื่อให้เว็บเซิร์ฟเวอร์สามารถจดจำสถานการณ์ใช้งานของเว็บบราวเซอร์ที่มีต่อเว็บเซิร์ฟเวอร์

- **Two-factor authentication**

Two-factor authentication เป็นระบบรักษาความปลอดภัยหรือระบบยืนยันตัวเองแบบ **2** ขั้นตอน นอกจากใส่ **Username/Email** และรหัสที่ถูกต้องแล้ว ผู้ใช้ต้องใส่ข้อมูลเพิ่มตัว เช่น ตอบคำถามส่วนตัวที่ตั้งไว้ หรือกรอกรหัสที่ได้รับทางโทรศัพท์มือถือ ระบบนี้เพิ่มความปลอดภัยให้กับบัญชีผู้ใช้หรืออุปกรณ์ต่างๆ ที่เปิดใช้งาน

- **Traffic**

การนับปริมาณคนเข้า-ออกเว็บไซต์หนึ่งๆ เพื่อใช้ตรวจสอบและปรับปรุงคุณภาพเว็บไซต์ และประการสำคัญยิงเว็บไซต์มี **Traffic** สูงยิ่งทำให้เป็นที่สนใจของบรรดา **Robots** ของ **Search Engine** ต่างๆ ทำให้แวะมาเก็บข้อมูลบ่อยขึ้น ที่สำคัญกว่านั้นย่อมทำให้การการโฆษณา การขายสินค้าในเว็บไซต์มียอดสูงขึ้นตามลำดับไปด้วยนั่นเอง

- **Threat**

ภัยคุกคามหรือสิ่งที่ละเมิดระบบรักษาความปลอดภัย และอาจก่อให้เกิดผลกระทบซึ่งเป็นอันตรายต่อระบบ ที่ส่งผลทำให้เกิดความเสียหาย หรือเป็นอันตรายต่อผู้อื่น โดยทั่วไปแล้วจะขัดต่อหลักกฎหมาย

- **Trojan Horse**

เป็นไวรัสที่แฝงมากับไฟล์อื่นๆ

- **Trojan Horse Virus**

เป็นไวรัสที่แฝงมากับไฟล์อื่นๆ ที่ดูแล้วไม่น่าจะมีอันตรายใดๆเช่น เกมส์ โปรแกรมฟรีแวร์หรือแชร์แวร์เมื่อใช้ไประยะเวลาหนึ่งแล้วไวรัสก็จะแสดงตัวออกมา ซึ่งอาจทำลายระบบคอมพิวเตอร์ของเรา

รวบรวมคำศัพท์น่ารู้ด้าน Security

- **UDP Flood**

เป็นการส่งแพ็คเก็ต **UDP** จำนวนมากไปยังเป้าหมาย ซึ่งทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่ และทำให้ทรัพยากรของเป้าหมายถูกใช้ไปจนหมด โดยจะส่ง **UDP packet** ไปยัง **port** ที่กำหนดไว้ เช่น **53 (DNS)**

- **Virtual private network (VPN)**

VPN เป็นอุปกรณ์ที่ปิดบังตัวตนของผู้ใช้อินเทอร์เน็ต โดยทำการปิดที่อยู่หรือ **IP Address**

- **Virus**

โปรแกรมคอมพิวเตอร์ที่สามารถทำสำเนาของตัวเอง เพื่อแพร่ออกไปโดยการสอดแทรกตัวสำเนาไปในรหัสคอมพิวเตอร์ส่วนของข้อมูลเอกสารหรือส่วนที่สามารถปฏิบัติการได้ ไวรัสโดยทั่วไปนั้นก่อให้เกิดความเสียหาย **(เช่น ทำลายข้อมูล)** แต่ก็มีหลายชนิดที่ไม่ก่อให้เกิดความเสียหาย เพียงแต่ก่อให้เกิดความรำคาญเท่านั้น

- **Vishing**

การล่วงรู้ข้อมูลของผู้อื่นโดยการใช้โทรศัพท์ หรือที่เรียกว่า แก๊งคอลเซ็นเตอร์ ซึ่งเป็นการหลอกลวงให้ได้มาซึ่งข้อมูลส่วนบุคคลผ่านทางโทรศัพท์

- **Vulnerability**

ช่องโหว่ของระบบหรือโปรแกรมเป็นจุดอ่อนหรือช่องโหว่ในระบบ ช่องโหว่ของระบบอาจเกิดจากบั๊กหรือข้อบกพร่องจากการออกแบบระบบ ช่องโหว่ของระบบสามารถเกิดขึ้นได้จากการละเลยหรือความไม่ใส่ใจของผู้ออกแบบโปรแกรม รวมถึงสาเหตุอื่นๆ ซึ่งทำให้ระบบอนุญาตให้ผู้เข้ามาทำลายระบบ , ให้ผู้ทำลายนำข้อมูลของตัวเองมาใส่และซ่อนข้อมูลดังกล่าว, อาศัยข้อบกพร่องของระบบเพื่อเข้าถึงข้อมูลและความจำของระบบโดยไม่ได้รับอนุญาตเพื่อสั่งใช้โค้ดต่างๆ