Introduction to Webmaster

ตอนที่ 4

: เรื่องน่ารู้
สำหรับผู้ดูแลระบบเครือข่าย

บทที่ 22
การรักษาความปลอดภัย

เรื่องของความปลอดภัย ผู้เขียนสนใจเรื่องของ Linux server (Redhat.com) เป็นหลัก แต่ที่พอมีความรู้เรื่องของความปลอดภัยใน Microsoft windows เพราะคุณสุวิทย์ สมสุภาพรุ่งยศ และคุณประเสริฐ ประสารยา ซึ่งเป็นเพื่อนร่วมงานด้านการดูแลระบบเครือข่าย และการแก้ปัญหาคอมพิวเตอร์ของหน่วยงาน ได้หาโปรแกรมมาให้ทดลองใช้อยู่เสมอ มีโปรแกรมสำหรับผู้ดูแล เพื่อช่วยเหลือผู้ใช้ หรือเฝ้าตรวจสอบการคุกคามจากคนแปลกหน้า เป็นต้น แต่ถ้ามองอีกด้านหนึ่ง เครื่องมือที่หามา หากตกไปอยู่ในมือของผู้ไม่ประสงค์ดี อาจกลายเป็นอาวุธที่ย้อนมาทำลายระบบได้ แต่ถ้าไม่ใช้ก็เหมือนตำรวจที่ถือกระบอง ส่วนผู้ร้ายสวมชุดพลางตัวพร้อมปืนเลเซอร์ ถ้าผู้ดูแลระบบไม่ศึกษาหาความรู้ด้านความปลอดภัย จะรู้ หรือปกป้องระบบได้อย่างไร

เป้าหมายของผู้บุกรุกส่วนใหญ่ คือ เข้าควบคุมระบบให้ได้และกลับออกไป โดยผู้ดูแลไม่สามารถแกะรอยได้ วิธีป้องกันการบุกรุกที่ผู้เขียนใช้ คือ หาระบบปฏิบัติการใหม่ล่าสุดมาใช้ ปิดบริการเกือบทั้งหมด ยกเว้นบริการที่จำเป็น ในองค์กรหนึ่งอาจมีบริการหลายอย่างที่ต้องการเปิดให้คนในองค์กร อาจใช้วิธีสร้างเครื่องบริการหลายเครื่อง แยกเครื่องละหนึ่งบริการ เพราะบริการที่จำเป็นบางบริการอาจมีจุดบกพร่องในอนาคต ทำให้ผู้บุกรุกโจมตีได้ จึงต้องการลดความเสี่ยง แต่ผู้ดูแลบางท่านอาจต้องการรวมบริการทั้งหมดไว้ในเครื่องเดียวกัน เพราะมีเวลาตรวจสอบระบบเสมอ หรือมีอุปกรณ์สำรองข้อมูลที่สมบูรณ์ สำหรับผู้เขียนขอเลือกการกระจายความเสี่ยง เพราะไม่มีเวลาตรวจสอบการบุกรุก ปัจจุบันใช้เครื่องคอมพิวเตอร์ที่มีความเร็วต่ำ มีหน่วยความจำน้อย ระบบล่มเมื่อไฟฟ้าดับและไม่มีอุปกรณ์สำรองข้อมูลที่สมบูรณ์ให้เกิดประโยชน์สูงสุด (ปัจจุบันใช้วิธีคัดลอก Harddisk เฉพาะเครื่องที่สำคัญ เก็บไว้เปลี่ยนเมื่อตัวเดิมมีปัญหา)

22.1 ระบบไฟฟ้าขัดข้อง

ปัจจุบันเครื่องคอมพิวเตอร์ที่เปิดให้บริการ 24 ชั่วโมง ตลอด 7 วันมีเพิ่มขึ้นทุกวัน เครื่องคอม-พิวเตอร์ในปัจจุบัน มีอายุการใช้งานหรือความทนทานไม่เท่ากัน ขึ้นอยู่กับอุปกรณ์ภายใน การบำรุงรักษา และการป้องกันไฟฟ้าดับในฤดูฝน มีเพียงไม่กี่ระบบที่สามารถสำรองไฟฟ้าได้นาน 2 ชั่วโมง เช่น ไฟฟ้าดับคืนวันศุกร์ อาจทำให้ระบบไฟฟ้าที่เลี้ยงคอมพิวเตอร์ดับไปทั้งระบบ ย่อมทำให้คอมพิวเตอร์เสียหาย หรือหยุดบริการ

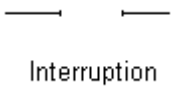
บางองค์กรซื้อเครื่องสำรองไฟฟ้า (UPS : Unterruptible Power Supply) แต่ใช้งานมา 3 ปี ย่อมสำรองไฟฟ้าได้น้อย บางครั้งแค่ไฟฟ้าตก ระบบถึงกับบูตเครื่องใหม่ทั้งระบบก็มี ทำให้ข้อมูลที่เก็บหรือประมวลผลอยู่เสียหาย

แม้จะมีวิธีการป้องกัน เช่น การสำรองข้อมูล การจัดทำเว็บไซต์สำรอง การใช้เครื่องปั่นไฟฟ้า ระบบป้องกันไฟฟ้ารั่ว หรือมีบุคลากรดูแลตลอดเวลา ซึ่งทุกปัญหาล้วนมีวิธีแก้ไข แต่มีองค์กรไม่มาก ที่พร้อมจะลงทุนป้องกันความเสียหายที่อาจเกิดขึ้น เพราะทุกวิธีต้องลงทุน ทั้งบุคลากร และอุปกรณ์ ทำให้ผู้ที่นิยมสืบค้นข้อมูลจากเว็บไซต์ ทราบว่าเว็บไซต์หลายแห่งหายไปในบางช่วงเวลา บางครั้งเว็บไซต์ที่มีข้อมูลสมบูรณ์กลับมาใหม่ในรูปแบบที่ไม่มีอะไรเลย เพราะขาดระบบสำรองข้อมูล หรือระบบป้องกันที่ดี

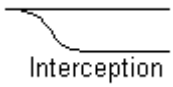
22.2 การละเมิดระบบรักษาความปลอดภัย

การละเมิดระบบรักษาความปลอดภัยมี 4 วิธี ระดับความร้ายแรงของการละเมิดขึ้นอยู่กับสถานการณ์ เช่น ผู้บุกรุกเข้าไปหยุดระบบในวันเสาร์ จะไม่ร้ายแรงเท่ากับการหยุดระบบลงทะเบียนในแรกของการรับลงทะเบียนเรียนในสถาบันการศึกษา หรือเว็บไซต์ของมูลนิธิเพื่อเด็ก ถูกลักลอบรายชื่อเด็กที่ต้องการความช่วยเหลือ จะไม่ร้ายแรงเท่ากับเว็บไซต์ของธนาคารถูกลับลอบรหัสลับของลูกค้า หรือหยุดบริการในช่วงต้นเดือน เป็นต้น

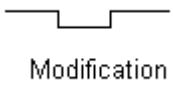
1. **หยุดการทำงาน** (Interruption)
คือหยุดให้บริการโดยสิ้นเชิง เช่น ข้อมูลในคอมพิวเตอร์หายไปหมด เป็นต้น



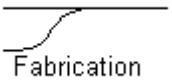
2. **ลักลอบข้อมูล** (Interception)
คือการที่ข้อมูลถูกขโมยออกไป เช่นแอบคัดลอกแฟ้มรหัสบัตรเครดิต เป็นต้น



3. **แก้ไขข้อมูล** (Modification)
คือการแอบเปลี่ยนข้อมูล เช่นเงินในบัญชีเงินฝากของลูกค้า หรือของผู้ลักลอบเป็นต้น



4. **สร้างข้อมูลปลอม** (Fabrication)
คือ การเพิ่มข้อมูลอย่างไม่ถูกต้อง เช่น แอบเพิ่มชื่อพนักงาน เข้าไปใน FBI เป็นต้น



22.3 ประตูหลัง (Back door)

ประตูหลังที่ผู้บุกรุก (Hacker) สร้างขึ้น หลังจากแอบเข้าระบบได้ และเป็นไปได้ที่ผู้ดูแลระบบทราบถึงการบุกรุก จึงต้องสร้างโปรแกรม หรือบริการบางอย่าง ที่ผู้ดูแลไม่ทราบ แต่ผู้บุกรุกทราบ เพื่อแอบเข้าระบบได้อีกครั้ง เช่น การสร้าง Account เพิ่ม และสร้างโปรแกรมเปลี่ยนผู้ใช้ธรรมดาเป็นผู้ดูแลระบบ (Root) เป็นต้น

ผู้เขียนเคยได้รับคำแนะนำจากมืออาชีพท่านหนึ่ง บอกว่าถ้า Hacker แอบเข้าระบบได้ สิ่งแรกที่ต้องทำคือ ดึงสาย LAN เพื่อยกเลิกการติดต่อกับเครือข่าย แล้วตรวจสอบโดยละเอียด ถ้า Hacker แอบเข้าระบบได้จริง ควรติดตั้งโปรแกรมทั้งหมดใหม่เพราะเป็นการยากที่จะตรวจสอบ และแก้ไขระบบทั้งหมด จนเชื่อได้ว่าจะไม่มี Backdoor ใดเหลืออยู่ในระบบเลย และ Hacker มืออาชีพจะไม่สร้าง Backdoor ด้วยการพิมพ์ทีละตัวอักษร เพราะใช้เวลามาก แต่มีโปรแกรมสร้างประตูหลัง (Backdoor) อัตโนมัติ และสร้างได้มาก จนยากที่ผู้ดูแลจะติดตามแก้ไขได้หมด

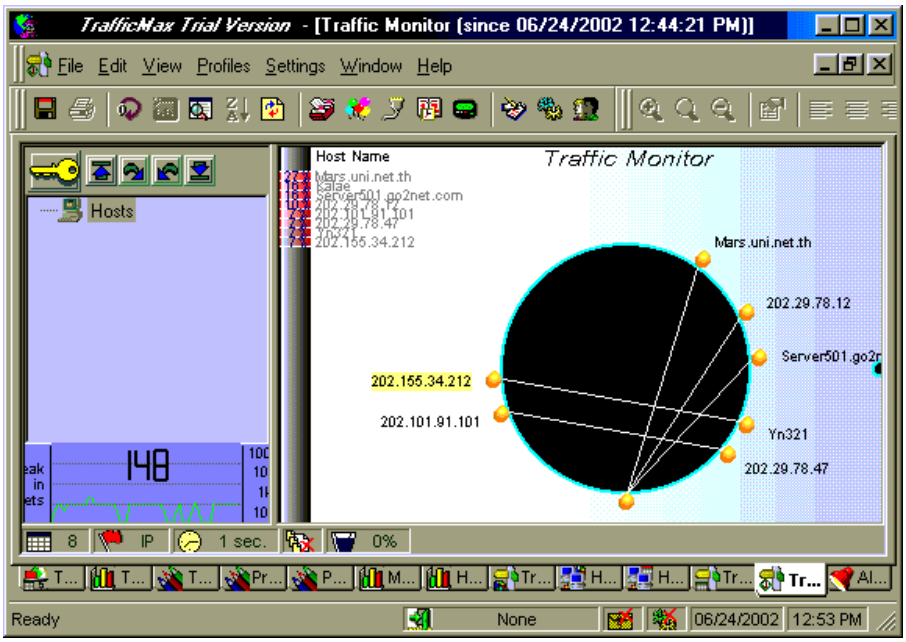
22.4 แหดักข้อมูล (Sniffer)

แหดักข้อมูล (Sniffer) คือ โปรแกรมของผู้ดูแลระบบ หามาใช้ได้จาก NAI (http://www.nai.com) หรือค้นหาโปรแกรมประเภทนี้ได้จาก http://www.shareware.com เป็นโปรแกรมที่มีความสามารถในการตรวจสอบข้อมูลที่กำลังไหลอยู่ในเครือข่าย ตรวจการรับ หรือส่งข้อมูลที่ผิดปกติ ตรวจการให้บริการของเครื่องบริการ สามารถตรวจข้อมูลที่มีการรับ-ส่ง ได้ละเอียดในระดับตัวอักษร แต่ผู้เขียนเห็นปัญหาในโปรแกรมนี้ ถ้าผู้ใช้ คือ ผู้ดูแลระบบ มิใช่สมาชิกในเครือข่ายที่ไม่น่าไว้ใจ ก็จะไม่มีปัญหาการขโมยข้อมูลเกิดขึ้น

ปัญหาที่อาจเกิดขึ้นเกี่ยวกับการนำโปรแกรมแหดักข้อมูลไปใช้ในองค์กร คือ ผู้ใช้อาจเป็นนักเรียนนำโปรแกรมนี้ไปติดตั้งในห้องปฏิบัติการ แล้วจับข้อมูล เช่น ข้อมูลจาก WWW, Telnet หรือ Outlook เป็นต้น ข้อมูลที่ถูกจับได้จะแสดงเป็นตัวอักษร เพื่อนคนหนึ่งอาจใช้โปรแกรมนี้ จับข้อมูลของเพื่อนที่กำลัง Login เข้าไปอ่าน E-mail ซึ่งข้อมูลนั้นจะถูกจับได้ ทำให้ผู้แอบจับสามารถเข้า E-mail ของเพื่อนที่ถูกดับจับเมื่อใดก็ได้ เพราะทราบ Username และ Password จากโปรแกรม Sniffer นี่เป็นเพียงตัวอย่างของสิ่งที่อาจเกิดขึ้น

วิธีแก้ไข คือ ติดตั้ง Reborn card ในห้องปฏิบัติการ ป้องกันการติดตั้งโปรแกรม ยกเลิกการใช้ Telnet แต่ใช้ SSH (Secure shell) แทน ไม่ใช้บริการของเว็บไซต์ที่ไม่มีการเข้ารหัสข้อมูล เมื่อต้องกรอกข้อมูลสำคัญ เช่น รหัสบัตรเครดิตเป็นต้น ใช้ Web based mail ที่มีบริการเข้ารหัสข้อมูล เช่น hotmail.com หรือ yahoo.com เป็นต้น สำหรับผู้เขียนไม่ได้ใช้ outlook เพราะเคยเป็นเป้าหมายโจมตีของไวรัสคอมพิวเตอร์ (Virus) ที่ผู้ใช้มากมายเคยได้รับผลกระทบมาแล้ว อาจติดตั้งโปรแกรม firewall หรือกำหนดให้คอมพิวเตอร์มีความปลอดภัยในระดับสูง จะทำให้โปรแกรมตรวจจับทั่วไปไม่พบคอมพิวเตอร์ของท่าน แม้จะใช้คำสั่ง ping ก็ตาม

โปรแกรมประเภท sniffer มักมีความสามารถหลากหลาย ซึ่งมีประโยชน์สำหรับผู้ดูแลระบบอย่างมาก โปรแกรมที่ทดสอบล่าสุด คือ Traffic max เป็นอีกโปรแกรมหนึ่งที่ทำงานได้อย่างมีประสิทธิภาพ เพื่อตรวจสอบการทำงานในระบบเครือข่าย ท่านสามารถ Download โปรแกรม Traffic max รุ่นทดสอบได้จาก http://www.sunrisetelecom.com/lansoftware/download.shtml



22.5 ระเบิดเมล (Mail bomb)

โปรแกรมระเบิดเมล (Mail bomb) ทำหน้าที่ส่ง e-mail เป็น 100 ฉบับด้วยการ Click เพียงครั้งเดียว เป้าหมายของโปรแกรมนี้ คือ ก่อกวน ผู้เขียนรู้จักเพราะเพื่อนร่วมงานนำมาทดสอบให้ดูว่าทำงานได้จริง จึงนำมาใช้ประโยชน์เพื่อทดสอบการรับ-ส่งอีเมล (E-mail) ของเครื่องบริการ หรือทดสอบการให้บริการ SMTP (Simple mail transfer protocol) มีปัญหาใดหรือไม่

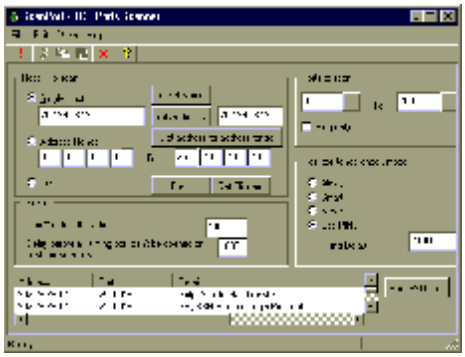
22.6 ไวรัสคอมพิวเตอร์ (Virus) คืออะไร

โปรแกรมชนิดหนึ่งที่ถูกเขียนขึ้น เป้าหมาย คือ ก่อกวนเครื่องคอมพิวเตอร์เป้าหมาย ด้วยการกระทำที่ผู้ใช้ไม่พึงประสงค์และสามารถคัดลอกตนเอง พร้อมกระจายไปยังเครื่องอื่น โดยผู้ถูกบุกรุกไม่ทราบ ปัจจุบันโปรแกรมที่ใช้ตรวจจับไวรัสได้รับความนิยมอย่างมาก เช่น McAfee, Norton หรือ PC-Cillin เนื่องจากไวรัสรุ่นใหม่ สามารถแพร่กระจายได้อย่างรวดเร็วในอินเทอร์เน็ต ไวรัสใหม่บางตัว สามารถก่อความเสียหายถึงขนาดแก้ไข BIOS (Basic input output system) จนผู้ใช้ทั่วไปต้องนำคอมพิวเตอร์ไปแก้ไขที่ร้านซ่อม การติดตั้งโปรแกรมฆ่าไวรัส และปรับปรุงเวอร์ชั่นจากผู้พัฒนาอยู่เสมอ จึงเป็นวิธีป้องกันที่นิยมและได้ผล จากการโจมตีของไวรัส สำหรับเว็บไซต์ที่ผู้เขียนเข้าไปอ่านเรื่องไวรัสเป็นประจำ คือ http://vil.mycio.com หรือตรวจสอบไวรัสแบบออนไลน์ที่ http://housecall.antivirus.com/housecall/start_frame.asp

22.7 ผู้บุกรุก (Hacker)

ผู้บุกรุกเข้าไปเครื่องคอมพิวเตอร์ผ่านระบบเครือข่าย อาจเป็นเครื่องคอมพิวเตอร์ของผู้ใช้ที่เข้าไปใช้บริการอินเทอร์เน็ต หรือเป็นเครื่องบริการ (Server) ที่ถูกเปิด เพื่อให้บริการต่าง ๆ การกระทำของผู้บุกรุกมีได้หลายพฤติกรรมตั้งแต่ บุกเข้าไปตรวจสอบระบบ หาจุดผิดพลาด พร้อมกับช่วยเหลือ หรือเตือนเจ้าของระบบ เพราะให้เจ้าของระบบปรับปรุงแก้ไข แต่อาจมีผู้บุกรุกบางท่าน เข้าไปแล้วใช้เครื่องคอมพิวเตอร์ที่บุกรุกได้เป็นเครื่องต้นทาง ในการบุกรุกเครื่องคอมพิวเตอร์เครื่องอื่นต่อไป

การบุกรุกมีได้หลายวิธี วิธีหนึ่งที่นิยม คือ หาจุดบกพร่องของระบบปฏิบัติการ ที่ประกาศตามเว็บต่าง ๆ มักเป็นจุดบกพร่องที่พบในระบบปฏิบัติการรุ่นเก่า (Old version) ซึ่งถูกแก้ไขในรุ่นใหม่ (New version) แล้ว ผู้บุกรุกเพียงแต่เข้าไปอ่านวิธีการจากเว็บไซต์ที่ให้ข้อมูล และเสาะหาเครื่องเป้าหมาย ว่าเปิดให้บริการที่อาจเป็นจุดบกพร่องของระบบหรือไม่ แม้จะผู้ดูแลระบบจะใช้ระบบปฏิบัติการที่มีปัญหา แต่ไม่เปิดบริการ port ที่มีจุดอ่อน บรรดา hacker ก็ทำอะไรไม่ได้ ดังนั้นผู้ดูแลควรเลือกเปิด port เฉพาะที่ต้องการบริการและจำเป็นเท่านั้น โปรแกรมที่ผู้เขียนแนะนำให้ใช้ตรวจสอบว่าเครื่องบริการของตนเปิด port ใดบ้าง คือ โปรแกรม scanport และสามารถ download จาก http://www.dataset.fr/eng/scanport.html



22.8 การปฏิเสธบริการ (DoS)

การโจมตีจนทำให้เครื่องที่ให้บริการปฏิเสธการให้บริการ (DoS-Denial of Service attack) เป็นเหตุการณ์ที่นักคอมพิวเตอร์ทั่วโลกรู้จัก เพราะเว็บใหญ่หลายเว็บปิดบริการไประยะหนึ่ง เนื่องจากมีจำนวนการขอใช้บริการที่ไม่ถูกต้อง เสมือนการโจมตีจากทั่วโลกพร้อมกันมากจนทำให้ไม่สามารถบริการได้ อันเกิดจาก Hacker บุกเข้าไปยังคอมพิวเตอร์ทั่วโลก แล้วแอบติดตั้งโปรแกรมแบบตั้งเวลา เมื่อถึงเวลาจะส่งความต้องการหรือข้อมูล ไปยังเว็บเป้าหมายมากมาย การจะไปเอาผิดกับเครื่องที่โจมตีเข้าไปก็ไม่ได้ และต้องปิดเป็นความลับ ถ้าเว็บใหญ่เหล่านี้เปิดเผย อาจทำให้เว็บไซต์ที่เคยถูกบุกรุก กลายเป็นเป้าหมายของ Hacker คนอื่นอีกได้

22.9 ระบบตรวจจับการบุกรุก (IDS)

ระบบตรวจจับการบุกรุก (IDS-Intrusion Detection System) เพื่อเฝ้าระวัง ตรวจจับ และวิเคราะห์พฤติกรรมของผู้บุกรุก เพื่อหาทางป้องกัน และตอบโต้ด้วยวิธีการที่เหมาะสม แม้เครื่องบริการจะถูกออกแบบมาดีเพียงไรก็ต้องมีจุดบกพร่อง สังเกตได้จากโปรแกรมที่ใช้สร้างเครื่องบริการในปัจจุบัน เมื่อสร้างรุ่นใหม่ขึ้นมาไม่นาน จะออกโปรแกรมปรับปรุงตามมาด้วยเสมอ เพราะค้นพบจุดบกพร่อง จุดบกพร่องใหม่ที่ถูกค้นพบก็คือ เป้าหมายของผู้บุกรุก และถ้าเครื่องบริการไม่คอยตรวจจับการบุกรุก ก็จะเป็นเหยื่อได้ง่าย

22.10 กำแพงป้องกัน (Firewall)

เครื่องคอมพิวเตอร์ที่มีหน้าที่ตรวจสอบ และกรองคำขอบริการ โดยยอมให้คำขอที่ได้รับอนุมัติผ่านได้เท่านั้น ปกติจะแบ่ง Firewall ได้เป็น 2 แบบ คือ แบบแอปพลิเคชั่นพร็อกซี่ (Application proxies) และแพ็คเก็ตฟิวเตอร์ริ่งเกตเวย์ (Packet filtering gateway) ในปัจจุบันยังไม่มีเจ้าของ Firewall รายใดกล้ายืนวันว่า ในอนาคตจะไม่มีใครสามารถเจาะ หรือบุกรุกผ่านระบบ Firewall ของตนได้ เพราะการบริการในปัจจุบันมีรูปแบบที่หลายหลาย ผู้บุกรุกปกติบุกเข้าสู่ระบบ แต่อาจทำความเสียหายให้ระบบได้ จึงต้องมีระบบตรวจจับการบุกรุก (IDS) มาคู่กับ Firewall เสมอ เพราะทำให้ระบบมีความปลอดภัยสูงสุด เสมือนมี Firewall ป้องกันการบุกรุกโดยทั่วไป และมี IDS คอยตรวจสอบ ว่ามีใครแอบบุกรุกเข้ามาได้

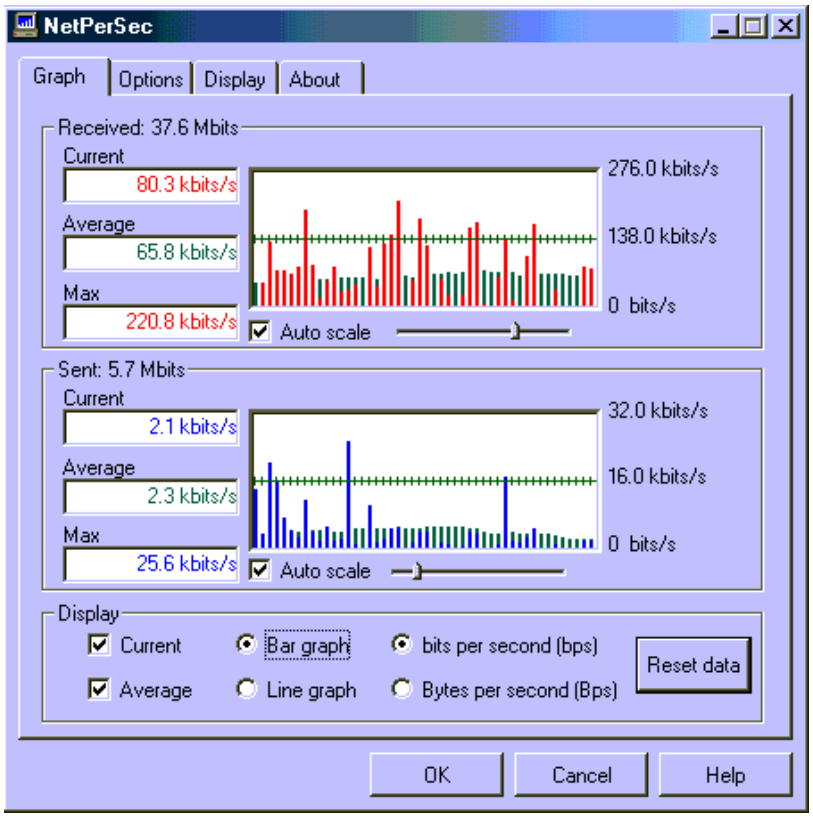
22.11 ห้องเก็บข้อมูล (Share folder) ถูกล้วง

การใช้งานในระบบเครือข่าย ผู้ใช้อาจอยู่ที่คอมพิวเตอร์เครื่องใดก็ได้ แล้วใช้ข้อมูลที่ถูกแบ่งปันจากคอมพิวเตอร์ของตน ซึ่งตั้งอยู่ในอีกห้องหนึ่ง ถ้าใช้ Microsoft windows จะเรียกหลักการนี้ว่า การแบ่งปันห้องเก็บข้อมูล (Share folder) ซึ่งมีความปลอดภัยในระดับหนึ่ง เพราะสามารถกำหนดรหัสผ่าน การเข้าใช้บริการได้

ในระยะหลังผู้เขียนพยายามไม่เปิดห้องเก็บข้อมูล (Folder) ให้ระบบเครือข่าย ถ้าจำเป็นจะเปิดในระยะสั้น แม้จะมีการกำหนดรหัสผ่านก็ตาม เพราะเพื่อนร่วมงานหาโปรแกรมมาให้ทดสอบว่า เขาสามารถเจาะเข้า Folder ที่มีการกำหนดรหัสผ่านไว้ เมื่อสั่งประมวลผล โปรแกรมจะทำการสุ่มรหัสขึ้นมา จนกว่าจะตรงกับรหัสที่ถูกต้อง ผู้เขียนได้การทดสอบ และพบว่าโปรแกรมนี้เจาะรหัสผ่านได้จริง

ทำให้ผู้เขียนต้องปิดระบบเครือข่ายที่สำคัญ เช่น ระบบบัญชี และทะเบียน ไม่ให้ใช้อินเทอร์เน็ต แต่เป็นระบบเครือข่ายแบบอินทราเน็ต และจำกัดเฉพาะวงของตนเอง เพราะอาจมีนักเรียนบางท่าน ต้องการดูว่าเพื่อนของตนลงทะเบียนเรียนวิชาใดบ้าง ซึ่งไม่ใช่วิธีการที่ถูกต้องที่เขาจะได้ข้อมูลนี้ ด้วยการแอบเปิด folder ที่ถูกป้องกันด้วยรหัสผ่าน

การตรวจสอบการทำงานของคอมพิวเตอร์ว่ามีการรับส่งข้อมูลอย่างไร อาจใช้โปรแกรม netstat.exe ที่มีอยู่ในห้อง c:\windows ถ้าต้องการเฝ้าตรวจว่ามีการรับส่งข้อมูลหรือไม่ โปรแกรม Netpersec สามารถทำหน้าที่นี้ได้ดี เมื่อมีการรับส่งข้อมูลที่ผิดปกติจะตรวจสอบได้ทันที โปรแกรมนี้ยังใช้วัดความเร็วของคอมพิวเตอร์ในขณะติดต่อกับเครือข่ายอย่างเห็นได้ชัด สามารถ download โปรแกรมนี้ได้จาก ftp://ftp.zdnet.com/acq/downloads/pub/zd/PCMag/netpsec.zip



22.12 ติดตั้งการ์ดฟื้นคืนชีพ

การ์ดฟื้นคืนชีพ หรือรีบอร์นการ์ด (Reborn card) หรือโปรเทคชั่นการ์ด (Protection card) คือ อุปกรณ์ทางฮาร์ดแวร์ เป็นแผ่นวงจรที่ทำให้คอมพิวเตอร์ปลอดภัยจากการแก้ไข หรือเปลี่ยนแปลง นิยมติดตั้งในห้องปฏิบัติการคอมพิวเตอร์ในสถาบันการศึกษา เพราะป้องกันการติดไวรัส ป้องกันการแก้ไขข้อมูล ป้องกันสื่อเก็บข้อมูลเต็ม เป็นต้น

หลายปีก่อนห้องปฏิบัติการในสถาบันการศึกษาที่ผู้เขียนดูแล มิได้ติดการ์ดฟื้นคืนชีพ ทุกภาคเรียนจะต้องติดตั้งโปรแกรมในห้องปฏิบัติการใหม่หมดทุกห้อง เพราะมีปัญหาด้านโปรแกรม คือ ใช้งานไม่ได้ บางโปรแกรมทำงานช้าลงเนื่องจากนักศึกษานำโปรแกรมมาติดตั้งไว้มาก หรือติดไวรัสหลายสายพันธุ์เป็นต้น เมื่อติดตั้งการ์ดนี้แล้ว ทำให้ทุกครั้งที่นักศึกษาเปิดเครื่องใหม่ แฟ้มข้อมูลที่นักศึกษาเคยเก็บ แก้ไข หรือ download มาไว้จะหายไป ยกเว้นข้อมูลที่อยู่ในแผ่นดิสก์ของนักศึกษา เป็นการป้องกันการติดตั้ง แก้ไข ติดไวรัส หรือเป็นแหล่งแพร่ไวรัสอย่างได้ผล แต่ถ้าเป็นหน่วยงาน อาจไม่กำหนดให้เรียกข้อมูลกลับทุกครั้งที่เปิดเครื่องใหม่ เพราะมีตัวเลือกให้เรียกกลับเมื่อต้องการ และทำงานได้กับระบบปฏิบัติการทุกรุ่น

22.13 แนะนำเว็บไซต์

1. http://housecall.antivirus.com Free online virus scan
2. http://thaicert.nectec.or.th ศูนย์ประสานงานการรักษาความปลอดภัย
3. http://vil.mycio.com ให้ข้อมูล พร้อมโปรแกรมฆ่าไวรัสขนาดเล็กที่ดีมาก
4. http://www.cert.org รวมผู้เชี่ยวชาญด้านความปลอดภัย
5. http://www.microsoft.com/technet/security มีข้อมูลแนะนำเรื่องความปลอดภัยดีมาก
6. http://www.sans.org หน่วยงานศึกษาด้านความปลอดภัย
7. http://www.securityfocus.com ให้ข้อมูลเกี่ยวกับระบบความปลอดภัยของ OS
8. http://www.thaidigitalid.com Thai Digital ID Root Certificate Authority
9. http://www.thaiinformation.com/its ผู้นำเข้า Reborn card ยี่ห้อหนึ่ง
10. http://www.thenetsec.com Thai systems and Network Security Knowledge