คู่มือเรียนและใช้งาน

Network Security Lab

ฉบับใช้งานจริง

อ่านเข้าใจง่าย	มีกรณีศึกษา	เหมาะสำหรับ
อธิบายอย่างละเอียด เป็นขั้นตอน สามารถทำตามได้จริง	ทั้งที่ใช้ Virtual Machine และทดสอบอุปกรณ์จริง	นักเรียน นักศึกษา และผู้ที่สนใจใช้งานจริง

ผศ.ดร.จักรชัย โสอินทร์ และคณะ บรรณาธิการ สุทธิพันธุ์ แสนละเอียด

IDC
PREMIER

มีเพียง “ความรู้” เท่านั้นที่มนุษย์ใช้พลิก “โลก” และเปลี่ยน “ชีวิต”
เราจึงสร้างสรรค์ และส่งมอบ “ความรู้” ในรูปแบบที่ดีกว่า
เพื่อให้คนไทย “เรียนรู้” ได้ตลอดชีวิต

Think Beyond

Read Smart

คู่มือเรียนและใช้งาน
Network Security Lab
ฉบับใช้งานจริง

ผู้แต่ง	ผศ.ดร.จักรชัย โสอินทร์, เพชร อิ่มทองคำ, คมเดช เพือดผุด, ชาติชาย ปุณริบูรณ์, ศรายุทธ พูลสงวน
	comsec.thailand@gmail.com
บรรณาธิการ	สุทธิพันธุ์ แสนละเอียด
ออกแบบปก	วสันต์ พึ่งพูลผล
ออกแบบและจัดรูปเล่ม	วุฒิพันธ์ สมพระเมฆ, สิริลักษณ์ วาระเลิศ
พิสูจน์อักษร	สุนทรี บรรสือศักดิ์
ประสานงานการผลิต	สุพัตรา อาจปรุ, ฉัตรชนก แก้วจันทร์

บริษัท ไอดีซี พรีเมียร์ จำกัด จัดตั้งขึ้นเพื่อเผยแพร่ความรู้ที่มีคุณภาพสู่ผู้อ่านชาวไทย เรายินดีรับงานเขียนของนักวิชาการและนักเขียนทุกท่าน ท่านผู้สนใจกรุณาติดต่อผ่านทางอีเมลที่ infopress@idcpremier.com หรือทางโทรศัพท์หมายเลข 0-2962-1081 (อัตโนมัติ 10 คู่สาย) โทรสาร 0-2962-1084

DEV BOOK

ข้อมูลทางบรรณานุกรม
ผศ.ดร.จักรชัย โสอินทร์
คู่มือเรียนและใช้งาน Network Security Lab
ฉบับใช้งานจริง
นนทบุรี : ไอดีซีฯ, 2559
440 หน้า
1. การเชื่อมประสานและการสื่อสาร
I เพชร อิ่มทองคำ
II คมเดช เพือดผุด
III ชาติชาย ปุณริบูรณ์
IV ศรายุทธ พูลสงวน
V ชื่อเรื่อง
004.6
Barcode 885-916-101-162-0

ราคา 415 บาท
E-Book มิถุนายน 2568

IDC PREMIER

พิมพ์ครั้งที่ 1 พฤษภาคม 2559
จัดพิมพ์และจัดจำหน่ายโดย
บริษัท ไอดีซี พรีเมียร์ จำกัด
200 หมู่ 4 ชั้น 19 ห้อง 1901 อาคารจัสมินอินเตอร์เนชั่นแนล ทาวเวอร์ ถ.แจ้งวัฒนะ อ.ปากเกร็ด จ.นนทบุรี 11120
โทรศัพท์ 0-2962-1081 (อัตโนมัติ 10 คู่สาย)
โทรสาร 0-2962-1084
สำหรับร้านค้าและตัวแทนจำหน่าย
โทรศัพท์ 0-2962-1081-3 ต่อ 112-114
โทรสาร 0-2962-1084
สมาชิกสัมพันธ์
โทรศัพท์ 0-2962-1081-3 ต่อ 121
โทรสาร 0-2962-1084

คำนำ

การจัดทำหนังสือเล่มนี้ เดิมทีมีจุดประสงค์เพื่อใช้ในการเรียนการสอนให้กับนักศึกษาปริญญาตรี รายวิชา Information and Communication Technology Security ณ ภาควิชา วิทยาการคอมพิวเตอร์ ม. ขอนแก่น โดยมุ่งเน้นไปยังการฝึกปฏิบัติการจริง ซึ่งทำให้นักศึกษามีความเข้าใจในการประยุกต์ใช้ทฤษฎีและหลักการที่เกี่ยวข้องกับความมั่นคงปลอดภัยคอมพิวเตอร์ และระบบเครือข่ายเข้ากับชีวิตจริง

อย่างไรก็ตามผู้เขียนได้ปรับแต่งเนื้อหาเพิ่มเติม ให้มีความหลากหลายและครอบคลุมที่มีความเหมาะสมกับผู้อ่านทั่วไปที่มีความสนใจอีกด้วย โดยประยุกต์ใช้กับอุปกรณ์จริงที่หาได้ทั่วไปในท้องตลาด ทั้งในส่วนของการเปิดเผย (Open Source) และอ้างอิงกับบริษัทชั้นนำของโลก เช่น Cisco Systems และ Microsoft Systems เป็นต้น

โครงสร้างเนื้อหาในแต่ละบท ได้ถูกออกแบบเพื่อให้ผู้อ่านเรียนรู้ตั้งแต่พื้นฐานการติดตั้งระบบ โดยผนวกความมั่นคงปลอดภัย การจัดการบัญชีผู้ใช้และบริหารทรัพยากร อีกทั้งยังอธิบายถึงวิทยาการรหัสลับเบื้องต้นอีกด้วย โดยปฏิบัติการเหล่านี้ทดสอบได้จริงด้วยตัวเองด้วยระบบปฏิบัติการ Windows โดยศึกษาเสริมได้จากหนังสือเครือข่ายคอมพิวเตอร์ทั่วไป หรือคู่มือเรียนและใช้งาน Computer Network Lab (ซึ่งเรียบเรียงโดยผู้เขียนเอง)

ข้อพึงระวัง จุดประสงค์หลักของหนังสือเล่มนี้เพื่อใช้ในการศึกษาเท่านั้น ผู้อ่านจะได้เรียนรู้ มีความเข้าใจถึงภัยอันตราย และตระหนักถึงความมั่นคงปลอดภัยที่อยู่รอบตัว แต่มิได้มีจุดประสงค์เพื่อเป็นการประสงค์ร้ายต่อระบบหรือหน่วยงานใดๆ หรือแม้แต่เพื่อยุยงส่งเสริมการใช้งานเครื่องมือในทางที่ผิด

ดังนั้น ผู้อ่านควรจะต้องทดสอบกับระบบปิดเท่านั้น และทุกครั้งเมื่อฝึกปฏิบัติการใดๆ ควรที่จะต้องตระหนักถึงความเสียหายที่จะเกิดขึ้นอยู่เสมอ ย้ำ ! ผู้อ่านที่ยังขาดประสบการณ์ ควรจะต้องได้รับคำแนะนำจากผู้เชี่ยวชาญก่อนจะดำเนินการใดๆ อีกทั้งผู้อ่านต้องศึกษาถึงกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคอมพิวเตอร์อีกด้วย

สุดท้ายนี้ผู้เขียนหวังเป็นอย่างยิ่งว่า หนังสือเล่มนี้จะช่วยเสริมความสามารถ หรือให้ความรู้ ความเข้าใจ และความตระหนักถึงความมั่นคงปลอดภัยคอมพิวเตอร์และระบบเครือข่ายได้ สามารถนำไปใช้ในทางที่ถูกที่ควร ซึ่งผู้อ่านสามารถขอคำแนะนำและสอบถามเพิ่มเติมได้ที่ comsec.thailand@gmail.com หากหนังสือเล่มนี้มีข้อผิดพลาดประการใด ผู้เขียนก็ต้องขออภัยมาไว้ ณ โอกาสนี้ และพร้อมรับที่จะนำไปปรับปรุงแก้ไขต่อไปในอนาคต

ผศ.ดร.จักรชัย โสอินทร์
Asst. Dr. Chakchai So-In

คำขอบคุณ

หนังสือเล่มนี้จะเกิดขึ้นไม่ได้ ถ้าไม่ได้กำลังใจที่สำคัญจากบุคคลหลายฝ่าย โดยผู้เขียนจะต้องขอขอบพระคุณคุณพ่อคุณแม่และครอบครัว ที่คอยเป็นกำลังใจและให้การสนับสนุนมาตลอด และคณะบุคคลที่เกี่ยวข้อง รวมไปถึงบุคลากรทุกท่านในภาควิชา มหาวิทยาลัยขอนแก่น และมหาวิทยาลัยเกษตรศาสตร์

ขอขอบคุณคณาจารย์ สุรศักดิ์ สงวนพงษ์, ภุชงค์ อุทโยภาศ, ยืน ภู่วรวรรณ, ศาสตรา วงศ์ธนวสุ, สุดสงวน งามสุริยโรจน์, สมนึก พ่วงพรพิทักษ์, กิตติ์ เธียรธโนปจัย และศิรปัฐช์ บุญครอง ที่เป็นแรงบันดาลใจในการเขียนหนังสือเล่มนี้ ขอบคุณนักศึกษา เพชร อิ่มทองคำ, คมเดช เผือดผุด, ชาติชาย บริบูรณ์ และศรายุทธ พูลสงวน ที่เป็นกำลังสำคัญในการพิสูจน์อักษรและเตรียมสื่อและรูปภาพ รวมไปถึงทดลองฝึกปฏิบัติการเพื่อความถูกต้องและสมบูรณ์

ซึ่งในระยะเวลา 3 ปีที่เตรียมจัดทำหนังสือ ต้องขอบคุณนักศึกษาในรายวิชาที่มีความตั้งใจ มุมานะพยายามความขยันหมั่นเพียรที่ศึกษาตามเค้าโครงของหนังสือ โดยไม่ย่อท้อและมุ่งมั่น ทำให้ผู้เขียนมีกำลังใจในการพัฒนาการเรียนการสอนที่มีความสมบูรณ์เพิ่มขึ้น และต้องขอขอบคุณบรรณาธิการและสำนักพิมพ์ ที่ให้โอกาสในการจัดพิมพ์โดยหนังสือเล่มนี้จะเกิดขึ้นไม่ได้ ต้องขอขอบคุณอีกครั้งหนึ่ง

สารบัญ

ปฏิบัติการที่ 1

การติดตั้งระบบปฏิบัติการและความมั่นคงปลอดภัยเบื้องต้น

ในปฏิบัติการแรกนี้ ก่อนที่จะเข้าสู่การปรับแต่งหรือติดตั้งระบบเพื่อเพิ่มความมั่นคงปลอดภัยของคอมพิวเตอร์และเครือข่าย สิ่งที่สำคัญในการเรียนรู้ขั้นต้นนั้นก็คือ การติดตั้งระบบปฏิบัติการ (Operating Systems) บนเครื่องคอมพิวเตอร์ ทั้งในส่วนของเครื่องแม่ข่าย/เซิร์ฟเวอร์ (Server) หรือเครื่องลูกข่าย/ไคลเอนท์ (Client) หรือแม้แต่การติดตั้งระบบปฏิบัติการใดๆ บนเครื่อง Server เสมือน (Virtual Server) ซึ่งในปัจจุบันมีการใช้งานเพิ่มมากขึ้น

โดยที่ Virtual Server จะเป็นการใช้งาน Server ได้โดยที่ไม่มีผลกระทบใดๆ กับระบบปฏิบัติการหลัก นอกจากนี้ในปฏิบัติการแรกยังอธิบายรวมไปถึงการจัดการ Server เพื่อให้มีความมั่นคงปลอดภัยเบื้องต้น ดังนั้น ในปฏิบัติการนี้ผู้อ่านจะได้ฝึกปฏิบัติการติดตั้ง Server โดยมีตัวอย่างคือ Windows 7 ซึ่งจะเป็นการติดตั้งลงบน Virtual Machine โดยใช้เครื่องมือ VirtualBox เพื่อทำให้สามารถรองรับการติดตั้งเครื่องมือต่างๆ ได้หลากหลายรูปแบบ และในส่วนสุดท้ายจะเป็นการอธิบายการปรับแต่งเสริมความมั่นคงปลอดภัยด้วย Windows Update

ไฟล์หรืออุปกรณ์ที่เกี่ยวข้องในปฏิบัติการนี้

1. ไฟล์ติดตั้ง VirtualBox เช่น VirtualBox-4.2.12-84980-Win.exe
2. ไฟล์ติดตั้ง Windows 7 เช่น Windows 7.iso
3. เครื่องคอมพิวเตอร์ระบบปฏิบัติการ Windows 7 พร้อมบราวเซอร์

แนะนำ Virtual Machine

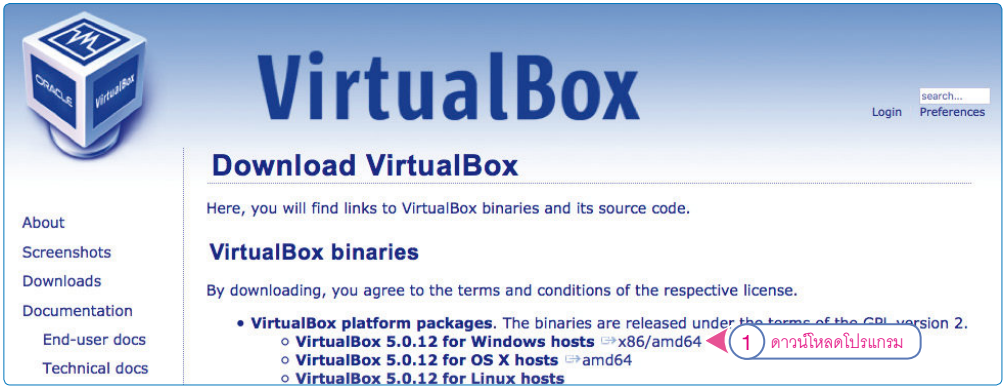
คำว่า Virtual มักจะแปลความหมายว่า การจำลองหรือเสมือนจริง โดยที่เป็นการจำลองการทำงานของอุปกรณ์หรือเครื่องมือต่างๆ ดังนั้น คำว่า Virtual Machine ก็อาจจะหมายถึง ระบบปฏิบัติการที่สามารถทำให้ใช้ซอฟต์แวร์ (Software) ในการจำลองการทำงานของคอมพิวเตอร์เสมือนกับว่ามีคอมพิวเตอร์ 2 เครื่องหรือมากกว่า

Virtual Machine สามารถทำงานซ้อนกันอยู่ในคอมพิวเตอร์เพียงเครื่องเดียว ทั้งนี้สำหรับประโยชน์ในการจำลองรูปแบบนี้ ดังตัวอย่างเช่น สามารถใช้ในการทดสอบโปรแกรมหรือระบบ ซึ่งถ้าเกิดความผิดพลาดใดๆ ก็มักจะไม่มีผลกระทบใดๆ ต่อคอมพิวเตอร์เครื่องหลัก

การติดตั้ง Virtual Machine

ก่อนที่ผู้อ่านจะติดตั้ง Server หลัก เช่น Windows 7 จะต้องติดตั้ง Virtual Machine ก่อน โดยในปฏิบัติการนี้จะเลือกใช้เครื่องมือ VirtualBox อย่างไรก็ตามผู้อ่านสามารถเลือกติดตั้งเครื่องมืออื่นๆ เช่น VMware ได้เช่นกัน สำหรับในกรณีที่ใช้เครื่องมือ VirtualBox จะมีขั้นตอนดังต่อไปนี้

1. ในการติดตั้ง VirtualBox นั้น ให้ผู้อ่านเข้าไปดาวน์โหลดไฟล์ติดตั้งที่ https://www.virtualbox.org/wiki/Downloads โดยเลือกดาวน์โหลดไฟล์ที่เป็น for Windows hosts x86/amd64



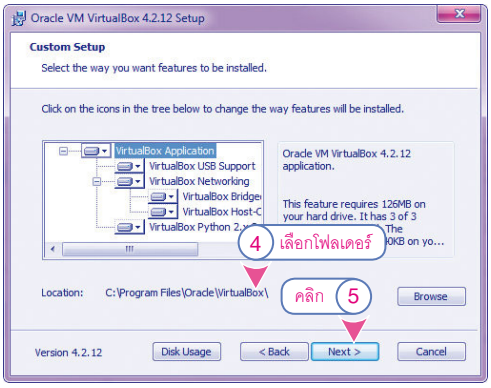
2. ดับเบิลคลิกที่ไฟล์ VirtualBox-4.2.12-84980-Win.exe เพื่อดำเนินการติดตั้ง

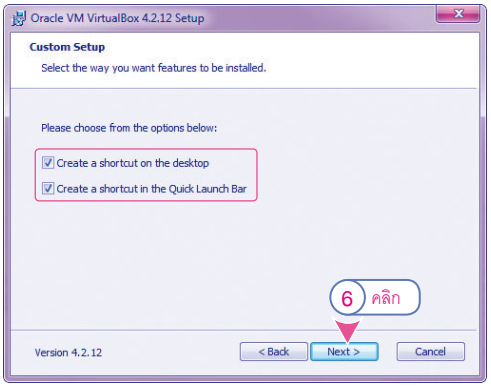
3. คลิกปุ่ม Next >

4. คลิกปุ่ม Browse เพื่อเลือกตำแหน่งที่จะติดตั้ง ซึ่งในกรณีนี้ใช้ค่า Default (หรือได้รับการแนะนำจากระบบเดิม)

5. คลิกปุ่ม Next >

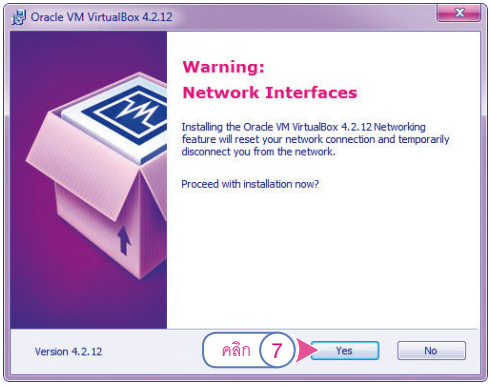
6. รอการติดตั้งรวมไปถึงการสร้าง Shortcut แล้วคลิกปุ่ม Next >

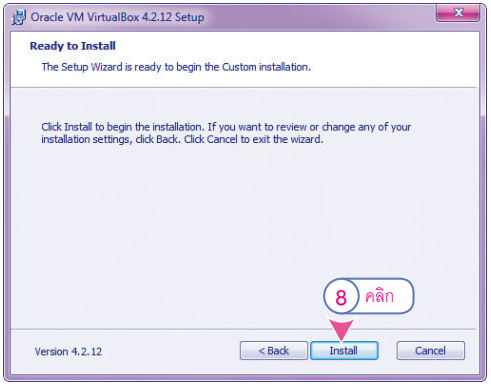




7. ดำเนินตามขั้นตอน ให้คลิกปุ่ม Yes

8. ให้คลิกปุ่ม Install





9. ปรากฏหน้าจอ Installation is complete (Finish) ซึ่งแสดงถึงการติดตั้งนั้นเสร็จสมบูรณ์ แล้วคลิกปุ่ม Finish

W A R N

ผู้อ่านจะต้องระมัดระวังในการเลือกตำแหน่งที่จะติดตั้ง โดยเฉพาะหลังจากการติดตั้งเสร็จแล้ว เมื่อผู้อ่านสร้าง Virtual Machine ที่รองรับการติดตั้ง Server หรือระบบปฏิบัติการอื่นๆ ก็จะต้องเตรียมพื้นที่ในการติดตั้งเพิ่มขึ้นด้วย

การติดตั้ง Windows 7 บน Virtual Machine

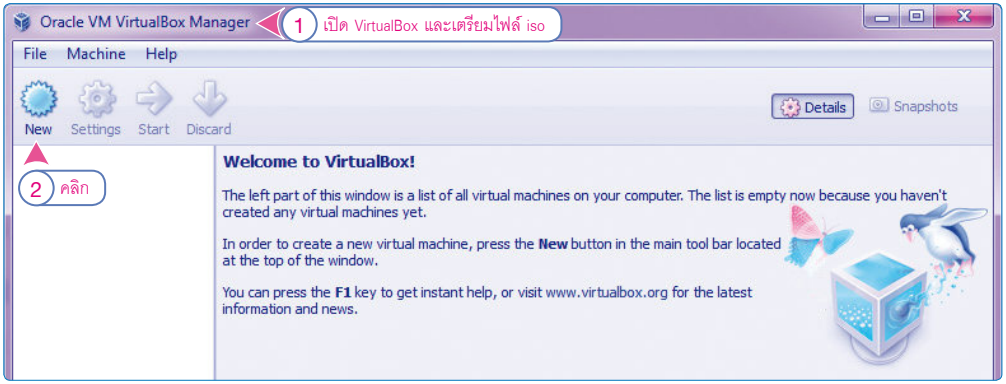
ในส่วนนี้เป็นตัวอย่างหนึ่งที่ใช้ทดสอบการติดตั้ง VirtualBox โดยเป็นการติดตั้ง Windows 7 ลงบน Virtual Machine ซึ่งมีขั้นตอนดังต่อไปนี้

N O T E

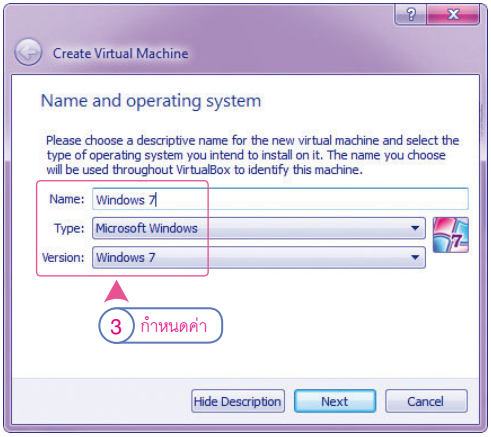
ในกรณีที่เป็นนักศึกษาจากมหาวิทยาลัยที่มีความร่วมมือกับบริษัท Microsoft ก็สามารถดาวน์โหลดผ่านทาง MSDN-AA หรือติดต่อผ่าน Microsoft Student Partner (MSP)

ส่วนนักศึกษามหาวิทยาลัยขอนแก่น ให้เข้าไปยังเว็บไซต์ www.mickku.com/msdnaa-kku-ขอนแก่น/ ซึ่งจะมีรูปแบบให้คลิกเลือกตามที่ฮาร์ดแวร์ (Hardware) สนับสนุน เช่น เป็นรูปแบบ 32 บิต หรือ 64 บิต หรือจาก http://www.one2up.com/view_content.php?content_ID=98639 เป็นต้น

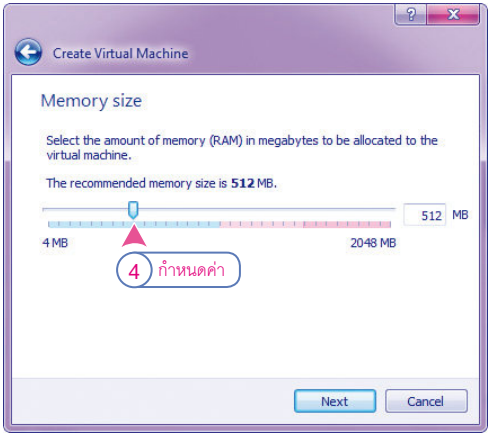
1. เตรียมไฟล์ติดตั้ง เช่น Windows 7.iso ในกรณีที่ผู้อ่านมีไฟล์ติดตั้ง (.iso) อยู่แล้วให้ข้ามขั้นตอนนี้ไป แต่ถ้าไม่มีให้เข้าไปเตรียมไฟล์ติดตั้ง Windows 7.iso ด้วยแผ่นต้นฉบับที่หาซื้อได้จากร้านค้าคอมพิวเตอร์ทั่วไปที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย
2. คลิกปุ่ม  สร้าง Virtual Machine (New)



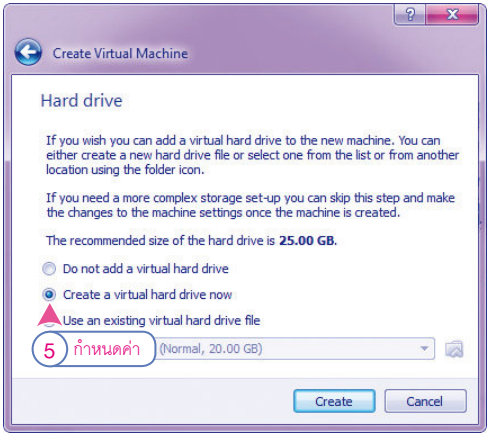
3. กำหนดชื่อ ชนิด และรุ่นเป็น Microsoft Windows 7 แล้วคลิกปุ่ม Next



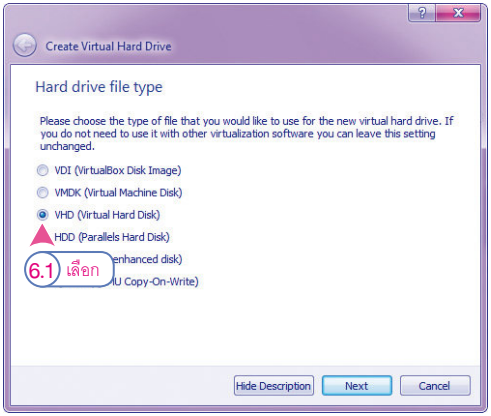
4. กำหนดหน่วยความจำ เช่น 512 MB แล้วคลิกปุ่ม Next

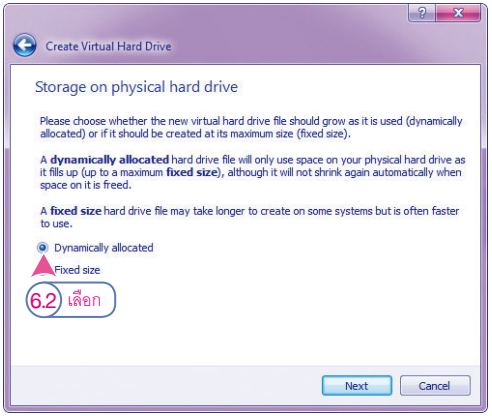


5. กำหนดขนาดพื้นที่ฮาร์ดดิสก์ เช่น 25 GB แล้วคลิกปุ่ม Create

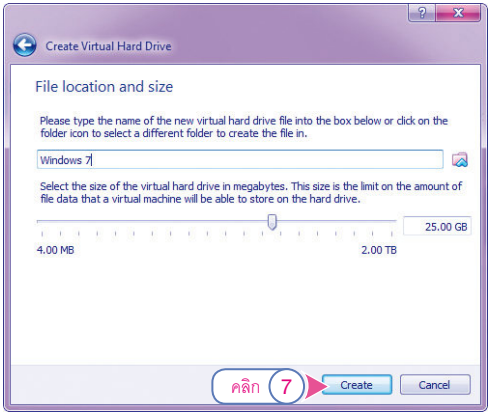


6. กำหนดพื้นที่ ชนิด และรูปแบบของฮาร์ดดิสก์ แล้วคลิกปุ่ม Next

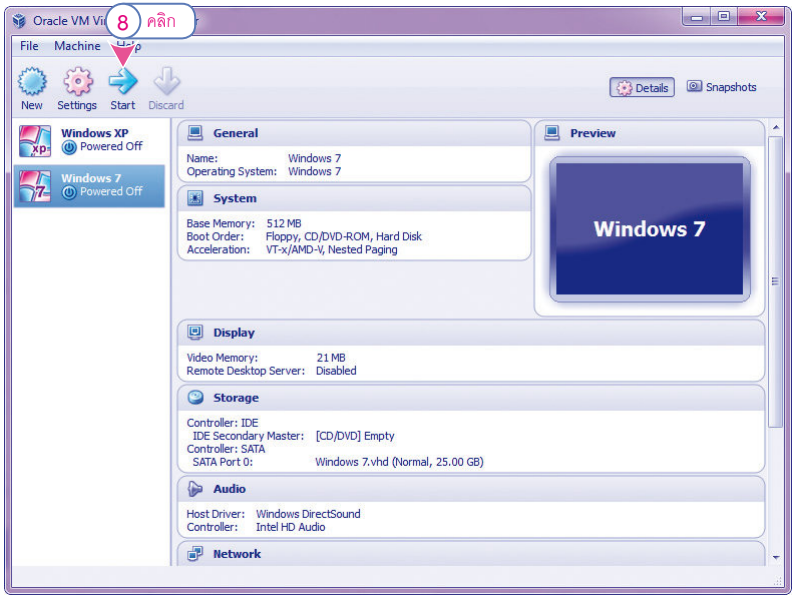




7. สร้าง Virtual Hard Disk แล้วคลิกปุ่ม Create

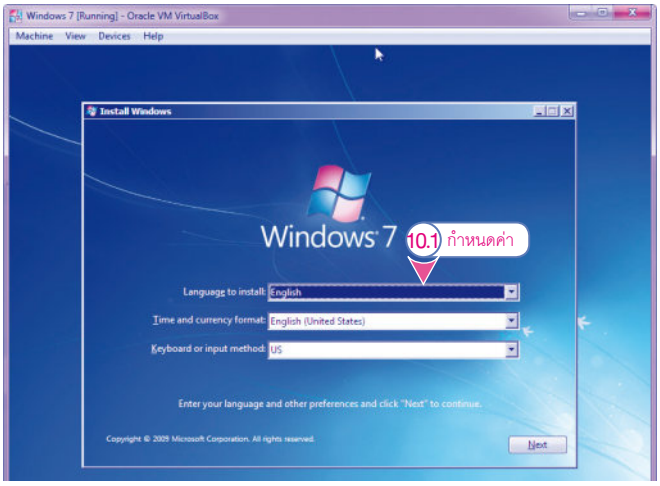


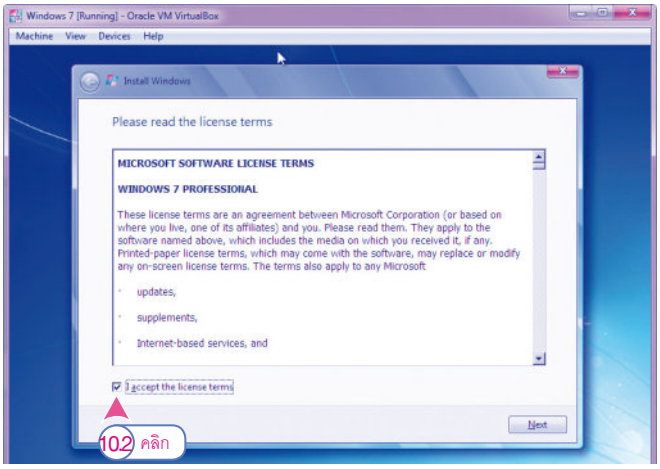
8. ขั้นตอนต่อไปเป็นการเริ่มติดตั้ง Windows 7

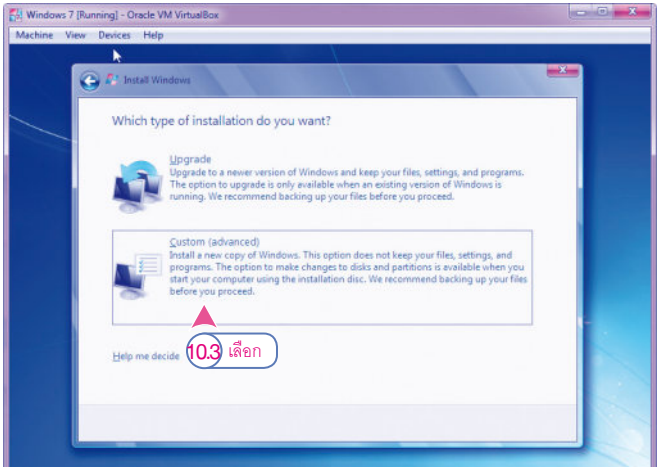


9. ให้คลิกเลือก start-up disk ไปยังไฟล์ที่ใช้ติดตั้งแล้วคลิกปุ่ม Start และคลิกเลือก Install now

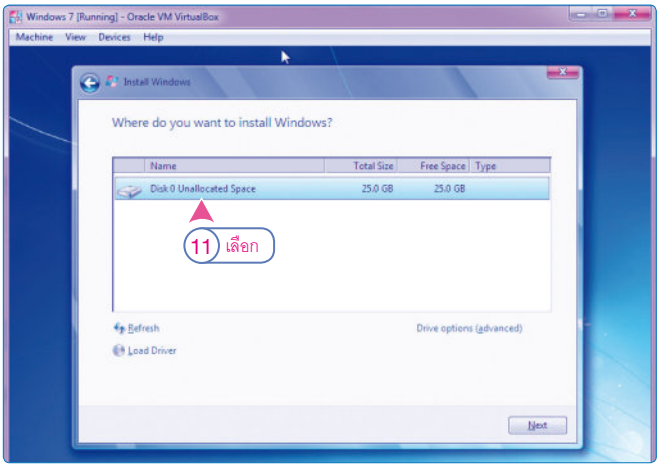
10. กำหนดภาษาและเงื่อนไขต่างๆ แล้วคลิกปุ่ม Next



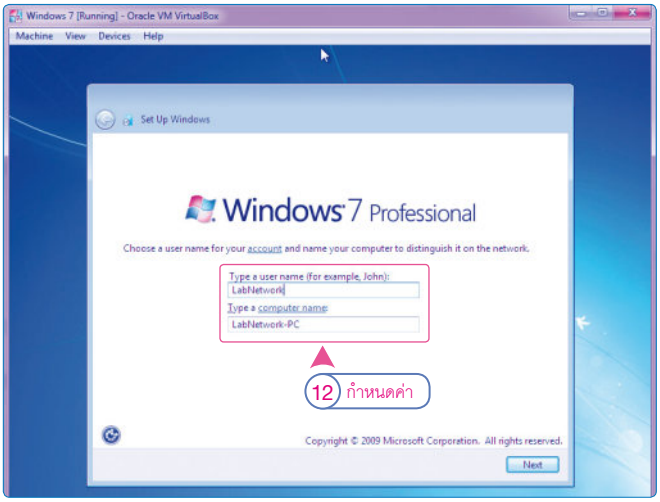




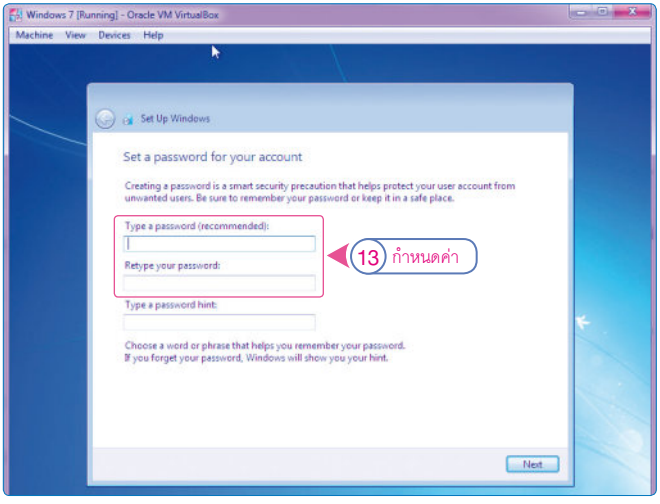
11. เลือกพื้นที่ในการติดตั้ง แล้วคลิกปุ่ม Next



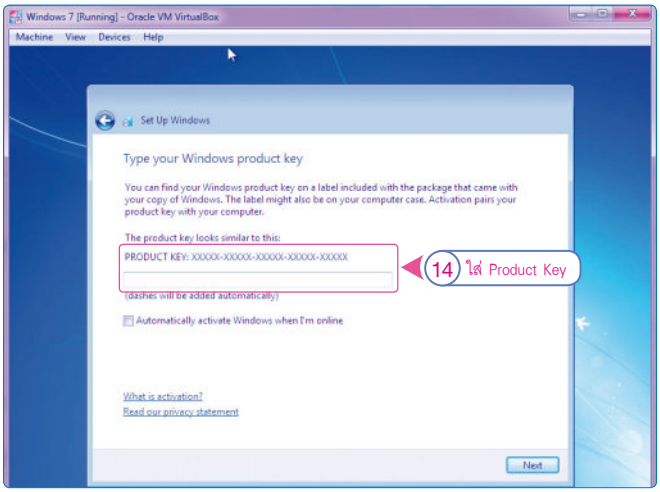
12. ตั้งชื่อบัญชีผู้ใช้งาน แล้วคลิกปุ่ม Next



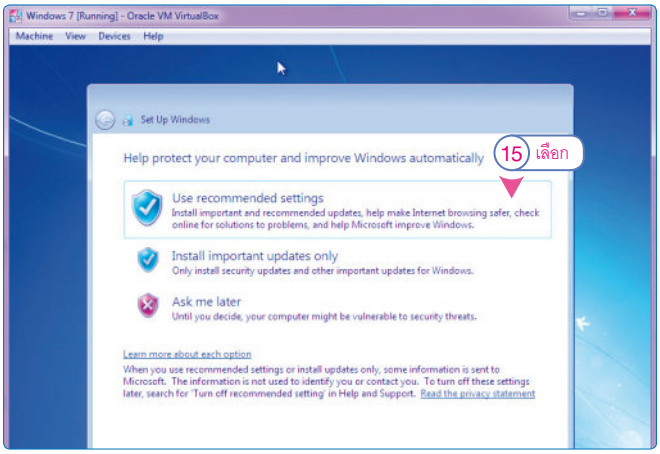
13. กำหนดรหัสผ่าน หรือ Password แล้วพิมพ์ซ้ำอีกครั้งหนึ่ง แล้วคลิกปุ่ม Next (ผู้อ่านอาจจะใส่คำใบ้กันลืม หรือ Hint ที่จำได้ง่าย ในกรณีที่รหัสผ่านนั้นยากต่อการจดจำ)



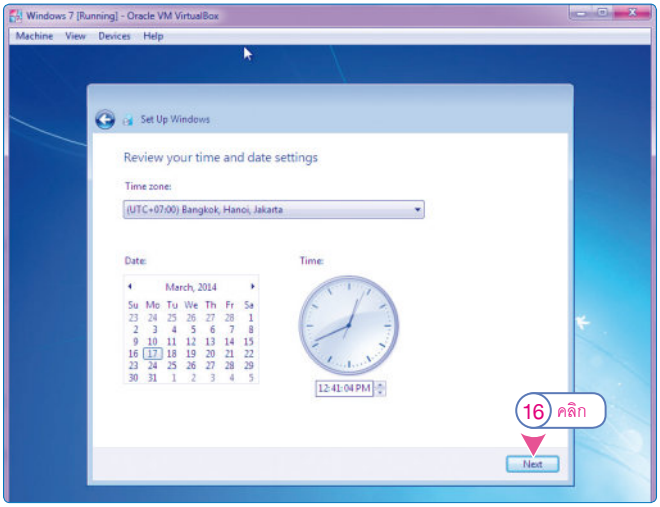
14. ใส่ Product Key แล้วคลิกปุ่ม Next



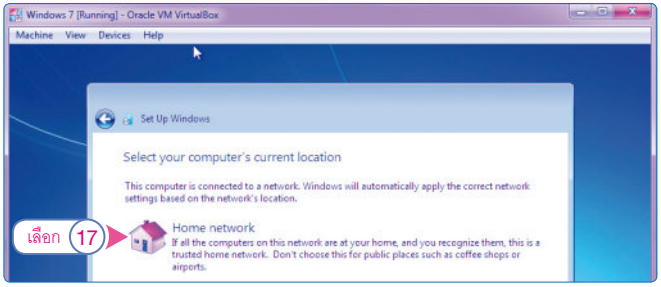
15. คลิกเลือก Use recommended settings (ทำตามที่ได้รับคำแนะนำจากระบบ)



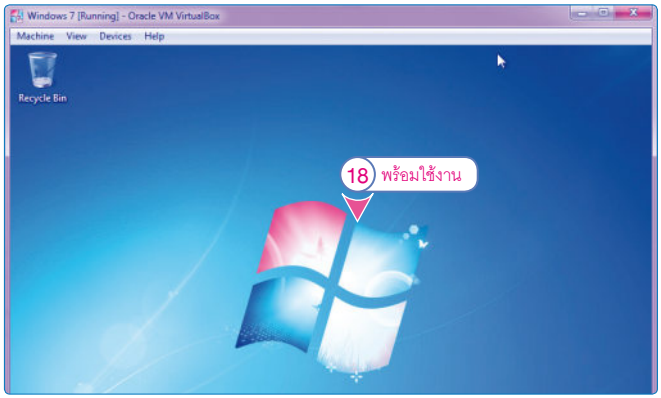
16. ปรับแต่งวันและเวลาสถานที่ แล้วคลิกปุ่ม Next



17. ปรับแต่งค่าการเชื่อมต่อเครือข่าย โดยคลิกเลือก Home network



18. Windows 7 เริ่มทำงาน



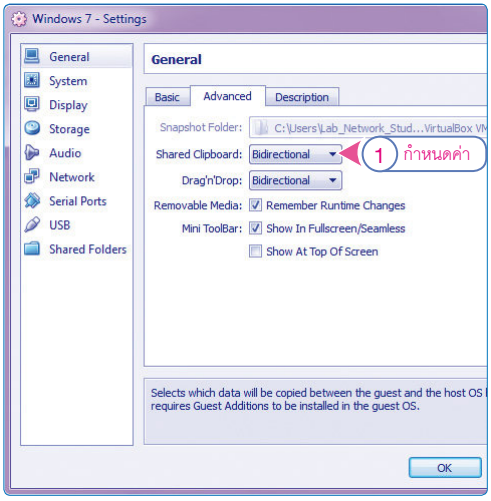
การปรับแต่ง Virtual Machine

หลังจากที่ผู้อ่านได้ติดตั้ง VirtualBox และทดลองติดตั้ง Windows 7 เสร็จเรียบร้อยแล้ว ต่อไปเป็นการปรับแต่งให้ VirtualBox สามารถใช้งานอินเทอร์เน็ต (Internet) ได้ รวมไปถึงการทำสำเนาไฟล์ต่างๆ (Copy Files) บน Clipboard จากเครื่องคอมพิวเตอร์หลักได้ โดยมีขั้นตอนดังต่อไปนี้

NOTE

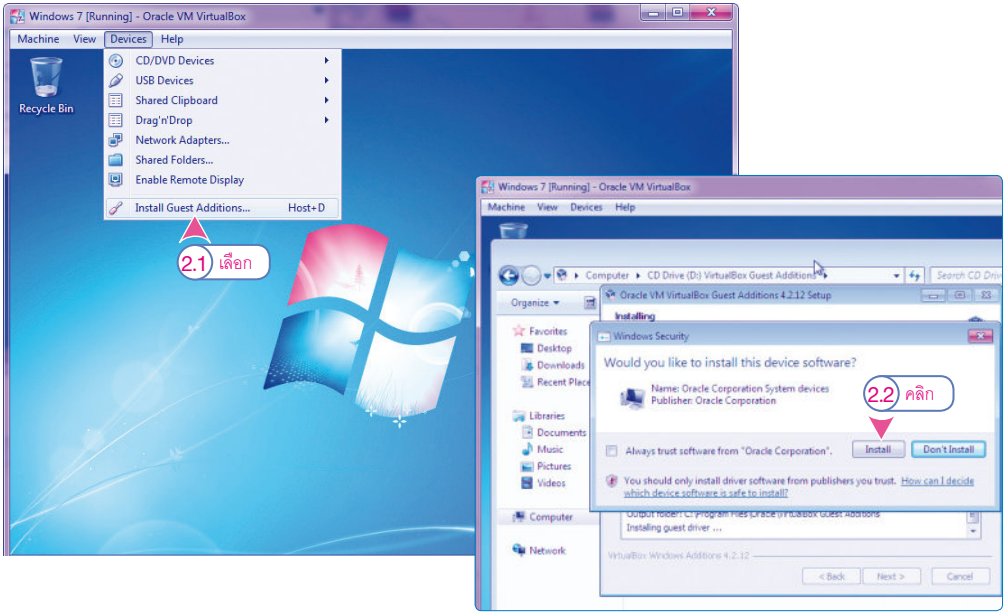
ผู้อ่านจะต้องตรวจสอบการเชื่อมต่อกับอินเทอร์เน็ตก่อนเสมอ เช่น ตรวจสอบสายสัญญาณที่ใช้งาน จะต้องเชื่อมกับเครือข่ายหลัก (Backbone) ของหน่วยงานหรือองค์กร มิใช่เพียงเชื่อมต่อกับอุปกรณ์ Hub หรือ Switch เท่านั้น หรือตรวจสอบ IP Address โดยใช้คำสั่ง C:\ipconfig หรือ C:\ping www.google.com เป็นต้น

1. ขั้นตอนแรกให้ผู้อ่านปรับแต่งที่หมวด General โดยเลือก Shared Clipboard เป็น Bidirectional ดังรูป แล้วคลิกปุ่ม OK

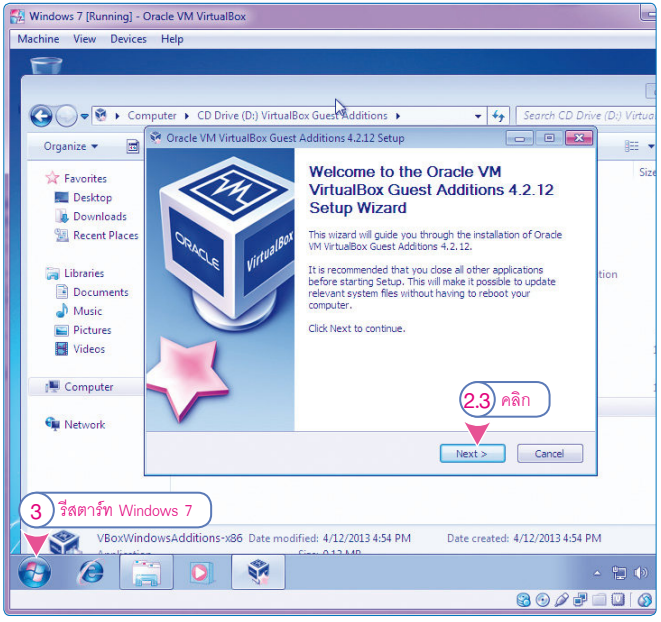


2. หากเกิดข้อผิดพลาด หรือ Invalid settings detected ซึ่งในส่วนนี้ให้ผู้อ่านติดตั้งเครื่องมือ VirtualBox-4.2.12-84980-Win.exe เพิ่มเติมดังรูปด้านล่าง

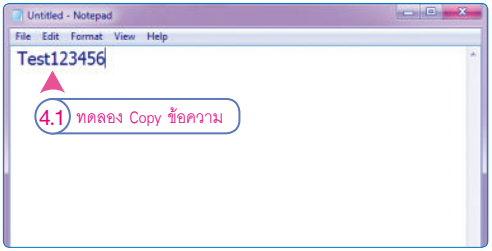
- ให้คลิกเมนู Devices > Install Guest Additions...
- ให้คลิกปุ่ม Install
- ให้คลิกปุ่ม Next >

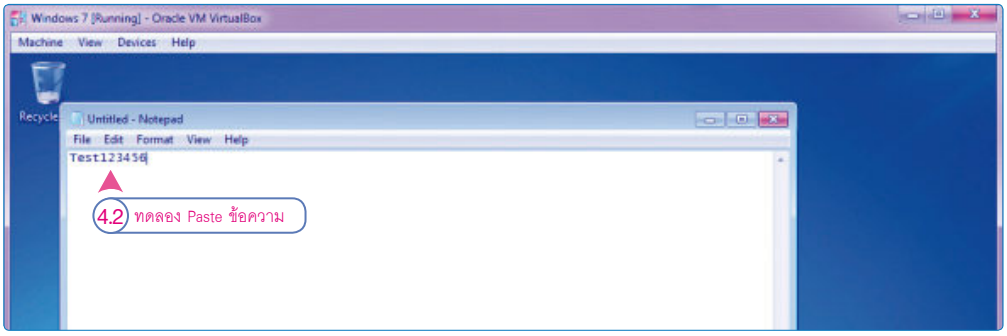


3. ให้ทำตามขั้นตอนที่ 1 ใหม่อีกครั้ง พร้อมกับ Reboot ส่วนของ Virtual Machine (Windows 7) ใหม่อีกครั้งหนึ่ง



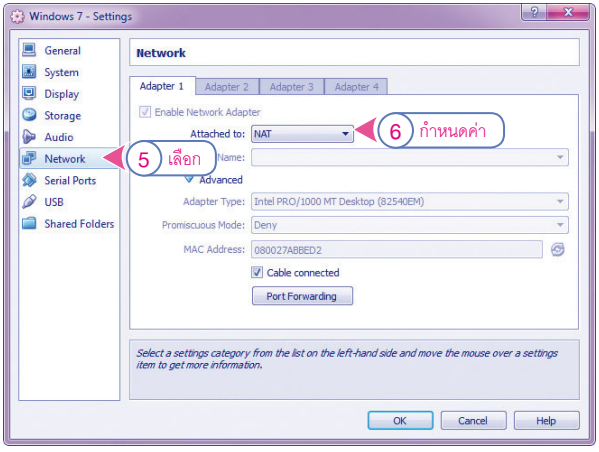
4. เมื่อปรับแต่งรายละเอียดเสร็จสิ้นแล้ว ให้ทดลองคัดลอก (Copy) บน Clipboard จากเครื่องคอมพิวเตอร์หลักไปวาง (Paste) บน Virtual Machine และในทำนองกลับกันดังรูปด้านล่าง (เช่น กดปุ่ม Ctrl + C แล้วตามด้วยปุ่ม Ctrl + V)



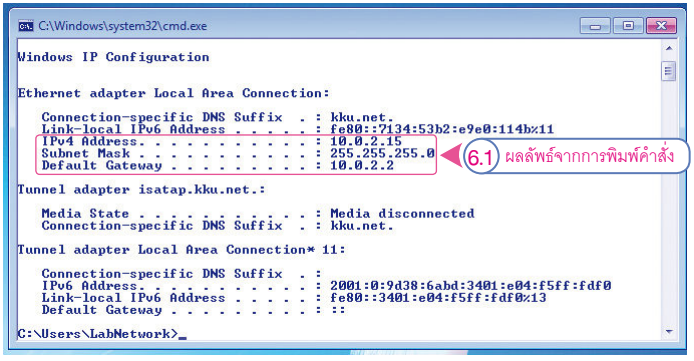


5. ปรับแต่ง Virtual Machine ให้สามารถใช้งานเครือข่ายหรืออินเทอร์เน็ตได้ โดยผู้อ่านเข้าไปที่หัวข้อหมวด Network

6. ให้ปรับค่า Attached to: เป็น NAT (Network Address Translation) แล้วคลิกปุ่ม OK



6.1 ให้ทดลองใช้คำสั่ง C:\ipconfig จะปรากฏผลการปรับแต่งคล้ายคลึงกับรูปด้านล่าง

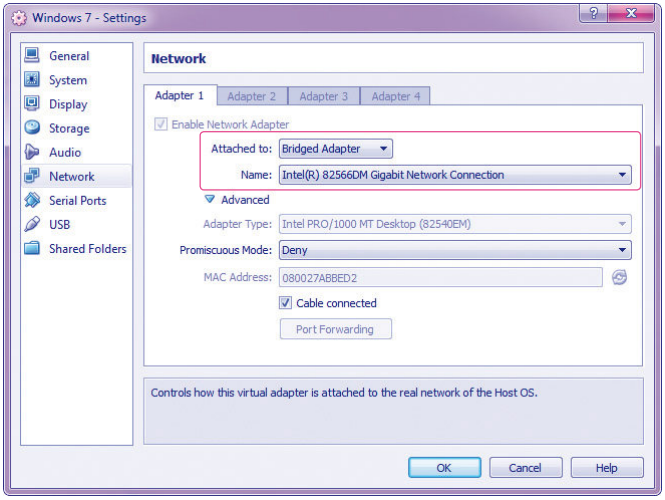


6.2 ให้ทดสอบเข้าใช้งานอินเทอร์เน็ตผ่าน Web Browser ต่อไป (ในกรณีนี้เครื่องคอมพิวเตอร์เสมือนนี้จะมี IP Address = 10.0.2.15 ซึ่งจะมีการแปลง IP Address เป็น IP Address ของเครื่องคอมพิวเตอร์หลัก เช่น 10.199.10.16 ก่อนที่เชื่อมต่ออินเทอร์เน็ตได้ต่อไป)

NOTE

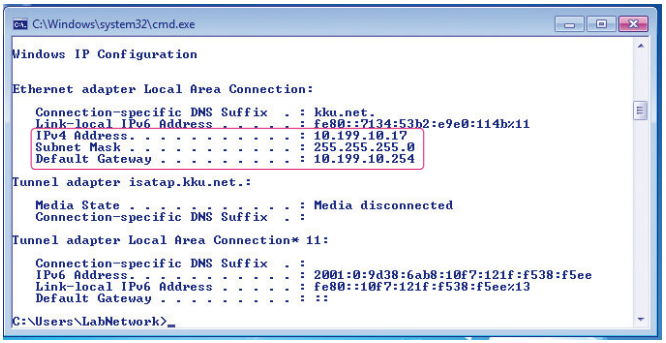
สำหรับการใช้งาน NAT จะทำให้ Virtual Machine สามารถเข้าสู่อินเทอร์เน็ตได้ แต่จะไม่สามารถปรับแต่ง Virtual Machine นี้เป็น Server หรือให้บริการแก่เครื่องอื่นๆ ได้

ดังนั้น ในขั้นตอนนี้ผู้อ่านยังสามารถปรับแต่งหมวด Network ให้มีค่าเป็น Bridged Adapter ได้ ซึ่งกรณีนี้เครือข่ายจะทำหน้าที่เสมือนกับเป็นอีกเครื่องคอมพิวเตอร์หลักอีกหนึ่งเครื่อง ซ้อนกับเครื่องคอมพิวเตอร์หลัก โดยมีค่าการปรับแต่งเครือข่ายเป็นรูปแบบเดียวกันกับเครื่องหลัก เช่น IP Address ในเครือข่ายวงเดียวกัน เป็นต้น ดังรูป (ในกรณีนี้เครื่องคอมพิวเตอร์หลักมี IP Address = 10.199.10.16 โดยที่เครื่องเสมือนคือ 10.199.10.17 และสามารถใช้ IP Address นี้เพื่อเชื่อมต่ออินเทอร์เน็ตได้)



NOTE

ในกรณีนี้ ผู้อ่านอาจจะสงสัยว่า IP 10.0.2.15 หรือแม้แต่ 10.199.10.17 สามารถเชื่อมต่ออินเทอร์เน็ตได้อย่างไร เนื่องจากผู้เขียนใช้เครือข่ายของมหาวิทยาลัยขอนแก่น และ IP นี้ก็จะมีการแปลง NAT อีกครั้งหนึ่งที่อุปกรณ์ Router ของมหาวิทยาลัย (ศูนย์คอมพิวเตอร์)

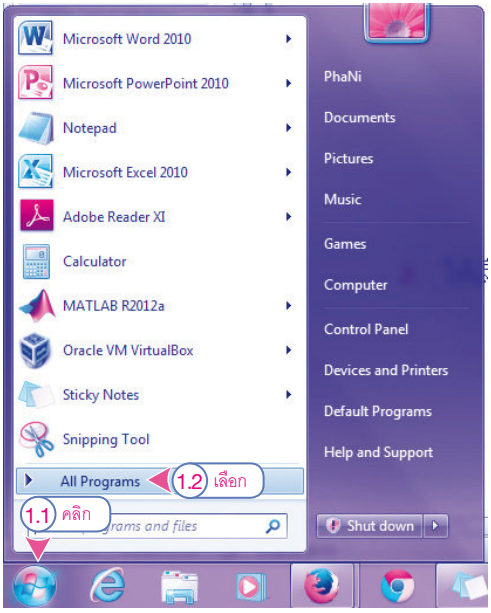


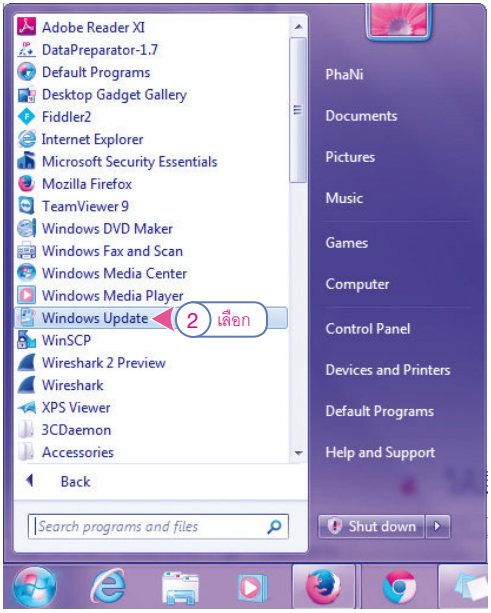
ความปลอดภัยเบื้องต้น โดยใช้ Windows Update

สำหรับในส่วนนี้ จะเป็นการฝึกปรับแต่งเครื่องมือหรือบริการที่มาพร้อมกับ Windows เพื่อเสริมความมั่นคงปลอดภัยเบื้องต้นหลังจากติดตั้ง Windows หรือการใช้งาน Windows Update โดยมีขั้นตอนดังต่อไปนี้ (ผู้อ่านจะต้องตรวจสอบว่าสามารถเชื่อมต่อกับ Internet ได้ และมีการลงทะเบียนระบบปฏิบัติการเรียบร้อยแล้ว เช่น ใส่ Product Key ที่ถูกลิขสิทธิ์)

1. เริ่มจากให้ผู้อ่านคลิกปุ่ม แล้วเลือก All Programs เพื่อเป็นการแสดง Programs ต่างๆ ทั้งหมด

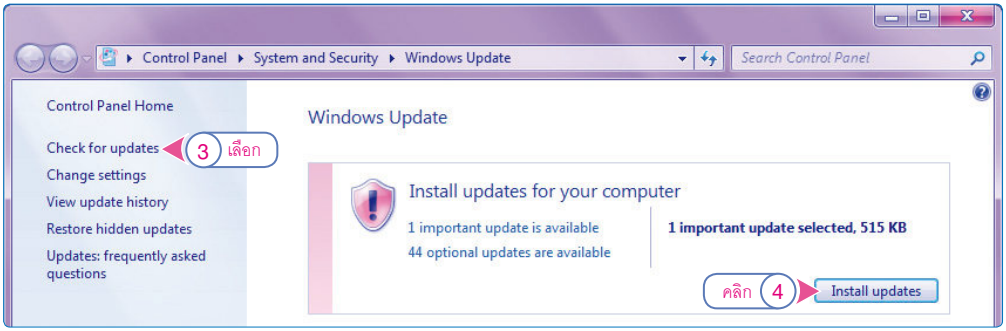
2. คลิกเลือก Windows Update





3. คลิกเลือก Check for updates

4. สังเกตที่มุมขวาบน โดยถ้าหากมีการตรวจพบการ Update ให้คลิกปุ่ม Install updates

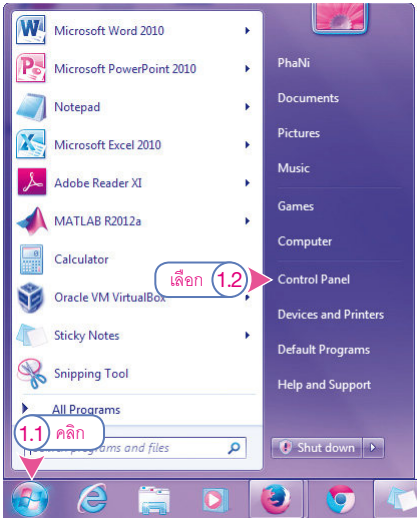


หมายเหตุ หลังจากที่ติดตั้งโปรแกรมต่างๆ แล้ว โดยทั่วไปผู้อ่านจะต้องรีสตาร์ท (Restart) เครื่องคอมพิวเตอร์ใหม่ทุกครั้ง

NOTE

ผู้อ่านสามารถเข้าถึง Windows Update ได้อีกทางหนึ่งโดยผ่านทาง Control Panel ดังนี้

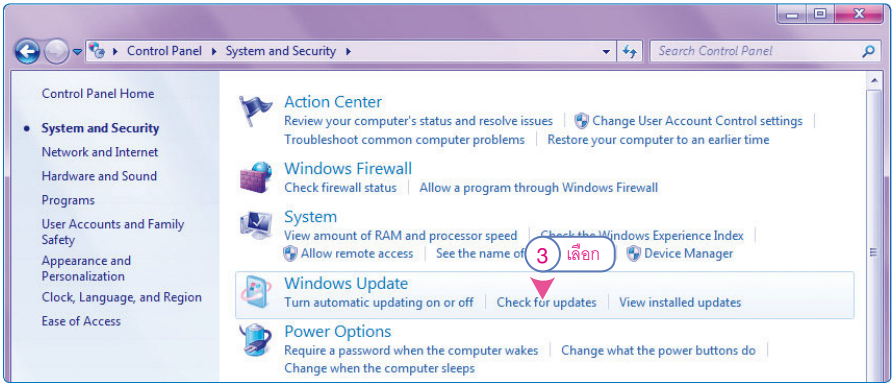
1. ให้คลิกปุ่ม แล้วเลือก Control Panel



2. คลิกเลือก System and Security

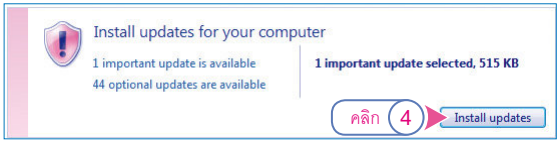
N O T E

3. คลิกเลือก Windows Update แล้วเลือก Check for updates



4. คลิกปุ่ม Install updates

หมายเหตุ เมื่อผู้อ่านติดตั้งการปรับแต่ง ในบางครั้งระบบจะต้องการให้ผู้อ่าน Reboot เครื่องใหม่ จึงจะสามารถติดตั้งโปรแกรมอื่นๆ ต่อไปได้



สรุปบทเรียน

ในบทเรียนนี้ได้อธิบายถึงการฝึกปฏิบัติการติดตั้ง Virtual Machine หรือเครื่องคอมพิวเตอร์เสมือนจริง โดยเป็นการเลือกใช้โปรแกรม VirtualBox นอกจากนี้ยังได้ทดสอบการติดตั้ง Windows 7 เพื่อเตรียมความพร้อมในการติดตั้งโปรแกรมอื่นๆ สำหรับการประยุกต์การใช้งานคอมพิวเตอร์และเชื่อมต่อกับเครือข่ายในบทเรียนถัดไป สำหรับในส่วนสุดท้ายยังได้ทดลองปรับแต่งการติดตั้ง Windows Update เพื่อสนับสนุนความมั่นคงปลอดภัยเบื้องต้นอีกด้วย

แบบฝึกหัดท้ายบท

- จงอธิบายถึงความแตกต่างระหว่างเครื่องคอมพิวเตอร์หลัก และเครื่องคอมพิวเตอร์เสมือน
- ให้ผู้อ่านทดลองสร้าง Virtual Machine ขึ้นมาใหม่ แล้วให้ทดสอบติดตั้งระบบปฏิบัติการ Windows 8 และ Windows 10
- ให้ผู้อ่านเปลี่ยนค่า IP Address ของเครื่องคอมพิวเตอร์หลัก จากนั้นจึงตรวจสอบถึง IP Address ของเครื่องคอมพิวเตอร์เสมือน ทั้งในหมวด Network: NAT และ Bridge และอธิบายถึงความแตกต่าง

ปฏิบัติการที่ 2

การปรับแต่งระบบบัญชีผู้ใช้งาน และความมั่นคงปลอดภัยพื้นฐาน

หลังจากที่ผู้อ่านได้ดำเนินการติดตั้งระบบปฏิบัติการ Windows แล้ว เนื้อหาในปฏิบัติการที่ 2 นี้ เป็นการฝึกใช้งานระบบโดยรวม ซึ่งจะเน้นไปที่การจัดการบัญชีผู้ใช้ (User Account) และการจัดการรหัสผ่าน (Password) นอกจากนั้นในปฏิบัติการนี้ยังอธิบายเพิ่มเติมในส่วนของการปรับแต่งความมั่นคงปลอดภัยพื้นฐาน เช่น โปรแกรมป้องกันไวรัส (Anti-Virus) และหนอน (Worm) จากอินเทอร์เน็ต (Internet) อีกด้วย

ไฟล์ที่เกี่ยวข้อง

1. ไฟล์คลังข้อมูล หรือ Library เช่น WinPcap_4_1_3.exe
2. ไฟล์ติดตั้งการโจมตีรหัสผ่าน เช่น lc6setup_v6.0.17.exe
3. ไฟล์ติดตั้ง Anti-Virus เช่น avg_free_stb_all_2014_4745_cnet.exe
4. ไฟล์ติดตั้ง Anti-Bot เช่น spybot-2.4.exe
5. ไฟล์ติดตั้งเครื่องมือเสริมความมั่นคงปลอดภัยอื่นๆ เช่น MBSASetup-x64-EN.msi, msert.exe และ mseinstall.exe
6. เครื่องคอมพิวเตอร์ระบบปฏิบัติการ Windows 7 พร้อมบราวเซอร์

แนะนำการโจมตีการเข้าถึง

การโจมตีในรูปแบบของการเข้าถึง (Access Attack) นั้น เป็นการใช้ประโยชน์จากความอ่อนแอหรือช่องโหว่ในส่วนของการพิสูจน์ตัวตน หรือพิสูจน์ตัวจริง (Authentication) เช่น บริการถ่ายโอนไฟล์ FTP (File Transfer Protocol) หรือบริการเว็บ (Web) เพื่อให้ได้มาซึ่งชื่อบัญชีผู้ใช้ (User Account) และรหัสผ่าน (Password) ซึ่งมักจะเป็นการได้มาซึ่งข้อมูล การเข้าถึง รวมไปถึงสิทธิ์ต่างๆ เป็นต้น โดยแบ่งออกได้ดังนี้

- Password Attack : การโจมตีโดยตรงกับรหัสผ่าน เช่น การโจมตีด้วยการเดารหัสผ่านที่เป็นไปได้ทั้งหมด หรือที่เรียกว่า บรูท ฟอร์ส (Brute Force), การใช้ม้าโทรจัน (Trojan Horse) ในการดักจับรหัสผ่าน, การปลอมแปลงไอพี (IP Spoofing) หรือแม้แต่การใช้เครื่องมือดักจับแพ็กเก็ตบนเครือข่าย (Packet Sniffing) เพื่อตรวจสอบหรือดักจับรหัสผ่านในกรณีที่บริการต่างๆ ไม่มีการเข้ารหัส (Encryption) เป็นต้น ดังตัวอย่างเช่น การใช้เครื่องมือ L0phtCrack (www.l0phtcrack.com) และ John the Ripper (www.openwall.com/john) ในการเดารหัสผ่านทั้งหมดที่เป็นไปได้
- Trust Exploitation : รูปแบบของการโจมตีโดยใช้ความน่าเชื่อถือ, ความไว้วางใจ หรือความสัมพันธ์ใดๆ กับหน่วยงานเพื่อให้ได้มาซึ่งการเข้าถึง เช่น การโจมตีเครื่องเซิร์ฟเวอร์ภายในเครือข่ายได้ง่าย เนื่องจากกลุ่มของเซิร์ฟเวอร์นั้นมีความไว้ใจหรือเชื่อใจซึ่งกันและกัน เป็นต้น
- Port Redirection : การโจมตีโดยที่มีการใช้เครื่องคอมพิวเตอร์ หรือระบบที่มีการถูกโจมตีแล้ว ในการส่งต่อข้อมูลผ่านอุปกรณ์ป้องกันเครือข่าย เช่น ไฟร์วอลล์ (Firewall) (จะกล่าวอีกครั้งในปฏิบัติการถัดไป) ที่มีการอนุญาตให้ระบบนี้ผ่านได้เท่านั้น นอกจากนี้การโจมตีรูปแบบนี้มักจะเป็นการเปลี่ยนแปลงพอร์ต (Port) ให้ตรงกับพอร์ตที่ไฟร์วอลล์อนุญาตให้ส่งผ่านได้
- Man-in-the-Middle Attack : การโจมตีรูปแบบนี้มีจุดประสงค์หลักเพื่อเป็นการขโมยข้อมูล หรือความพยายามที่จะขโมยการเชื่อมต่อ (Connection) เพื่อให้มีสิทธิ์ในการเข้าถึงทรัพยากรได้ หรือแม้แต่ความพยายามที่จะโจมตีแบบ DoS (Denial-of-Service) ซึ่งจะกล่าวถึงอีกครั้งภายในเล่ม
- Buffer Overflow : เป็นรูปแบบของการโจมตีที่มีการใช้งานทรัพยากร หรือหน่วยความจำที่เกินกว่าที่ได้กำหนดไว้

กรรมวิธีการพิสูจน์ตัวจริง

ในการพิสูจน์ถึงตัวตนหรือตัวจริง (Authentication Method) นั้นมีรูปแบบที่หลากหลาย อย่างไรก็ตามโดยทั่วไปแล้ว มักจะเป็นลักษณะของการยืนยันถึงบางสิ่งบางอย่าง ที่สามารถระบุได้ถึงตัวตนที่แท้จริง ซึ่งมีผู้ใช้งานเพียงคนเดียวที่อาจจะรู้ หรือมีอยู่ หรือถือครองอยู่ หรือสิ่งที่ผู้ใช้สร้างขึ้นมา เป็นต้น เช่น รหัสผ่าน (Password) หรือกุญแจเข้ารหัส (Key)

กรณีของรหัสลับนั้น มักจะถูกใช้เพื่อเป็นการยืนยันถึงผู้ใช้งานซึ่งรู้เพียงคนเดียว (ในกรณีที่ไม่ได้แจ้งหรือบอกคนอื่น) ซึ่งหากรหัสลับขนาด 64 บิต ก็แสดงว่าจะมีรหัสที่เป็นไปได้ถึง 2^{64} คีย์ ที่ใช้ในการตรวจสอบ อย่างไรก็ตามในกรณีของรหัสลับที่มีการใช้งานโดยทั่วไปนั้น มักจะมีจุดประสงค์เพื่อให้สามารถจำได้ง่ายสำหรับมนุษย์ และโดยส่วนใหญ่นิยมอยู่ในรูปแบบของรหัสแอสกี้ (ASCII) เช่น มีขนาด 1 ไบต์ (Byte) หรือ 8 บิต (Bit) ดังนั้น จึงมีความเป็นไปได้ทั้งหมด 2^8 = 256 รหัส (เช่น จาก 00000000 ถึง 11111111)

ทั้งนี้มีข้อสังเกตที่สำคัญคือ ในความเป็นจริงแล้ว การที่จะทำให้ผู้ใช้งานจดจำรหัสลับที่ไม่มีความหมายใดๆ หรือไม่มีความสัมพันธ์ใดๆ เลย ก็มักจะเป็นไปไม่ได้ หรือทำไม่ได้ในทางปฏิบัติ ดังนั้นผู้ใช้งานโดยทั่วไปจึงมักจะตั้งรหัสให้สามารถจำได้ง่าย เช่น ชื่อ, นามสกุล, วันเกิด หรือเบอร์โทรศัพท์ เป็นต้น ซึ่งก็มักจะทำให้ความน่าจะเป็นในการเดารหัสนั้นง่ายขึ้น เช่น การตั้งรหัสระหว่าง “kf&yw!a[[NetSec_02_0” เมื่อเปรียบเทียบกับ “Chakchai” เป็นต้น

เนื่องจากโดยทั่วไปแล้ว ในการใช้งานระบบมักจะประกอบไปด้วยผู้ใช้งานที่มีความรู้ความเข้าใจทางด้านความมั่นคงปลอดภัยที่แตกต่างกันด้วย เช่น ผู้ดูแลระบบอาจจะตั้งรหัสที่มีความซับซ้อนสูง แต่ผู้บริหารระดับใช้งานก็อาจจะตั้งรหัสที่สามารถจดจำได้ง่าย

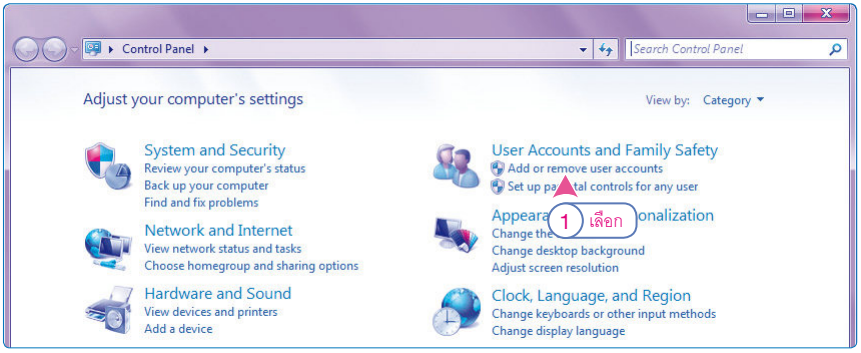
ดังนั้น ในการโจมตีกับระบบนั้นส่วนใหญ่แล้วก็จะเป็นการโจมตีกับผู้ใช้งาน รวมไปถึงมีการค้นหาร่องรอย หรือรูรั่ว หรือจุดอ่อนของระบบเพื่อใช้แทรกซึมเข้าไปในระบบ ก่อนที่จะโจมตีกับระบบโดยตรง หรือแม้แต่โจมตีกับผู้ดูแลระบบต่อไป เนื่องจากส่วนใหญ่แล้ว ระบบมักจะมีความเชื่อใจกับบุคลากรภายในองค์กร โดยเฉพาะผู้บริหารระดับสูงเป็นสำคัญ

การจัดการบัญชีผู้ใช้บน Windows

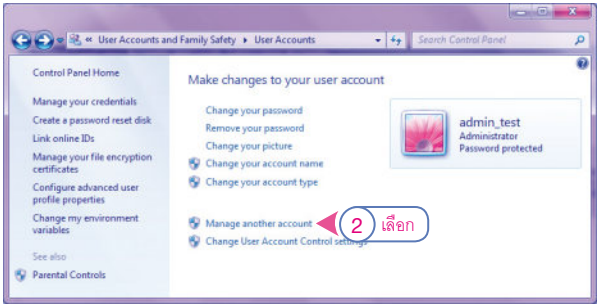
ในส่วนแรกนี้จะเป็นการจัดการบัญชีผู้ใช้ของ Windows ในส่วนนี้จะเป็นการฝึกปฏิบัติการเพิ่มบัญชีผู้ใช้งาน, เปลี่ยนแปลงสิทธิ์ในการใช้งาน, แก้ไขรหัสผ่าน รวมไปถึงการลบผู้ใช้งานออกจากระบบ โดยมีขั้นตอนดังต่อไปนี้

การเพิ่มบัญชีผู้ใช้งาน

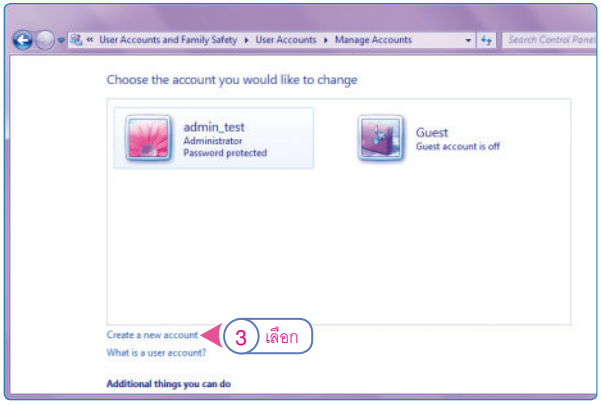
1. ให้เข้าไปที่ Control Panel > User Accounts and Family Safety คลิกเลือก Add or remove user accounts



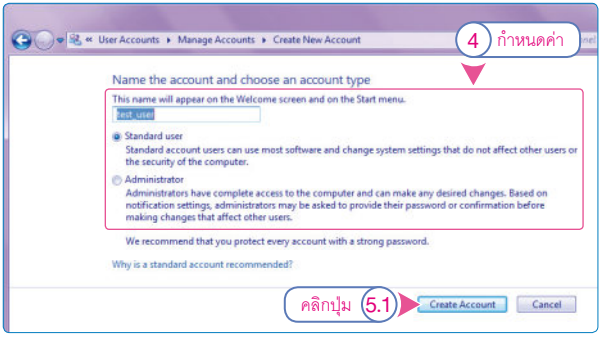
2. คลิกเลือก Manage another account ก็จะปรากฏรูปด้านล่าง



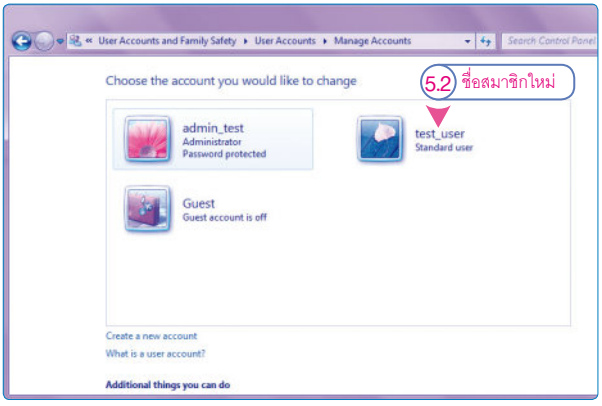
3. คลิกเลือก Create a new account



4. ใส่ชื่อผู้ใช้งาน โดยสามารถคลิกปุ่มเลือกระหว่างสิทธิ์ผู้ใช้งานทั่วไป (Standard user) หรือมีสิทธิ์เทียบเท่าผู้ดูแลระบบ (Administrator) ซึ่งในกรณีนี้ผู้ใช้งานชื่อ test_user และมีสิทธิ์เป็นเพียงผู้ใช้ทั่วไป

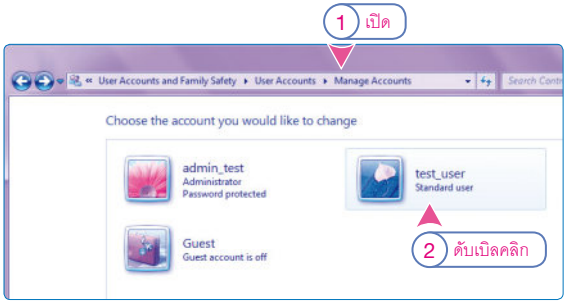


5. คลิกปุ่ม Create Account จะปรากฏสมาชิกผู้ใช้งานคนใหม่ดังรูป

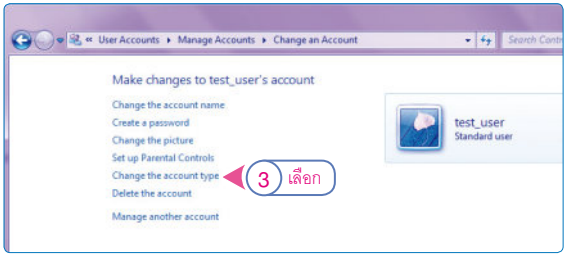


เปลี่ยนแปลงสิทธิ์ให้กับผู้ใช้ที่มีอยู่เดิม

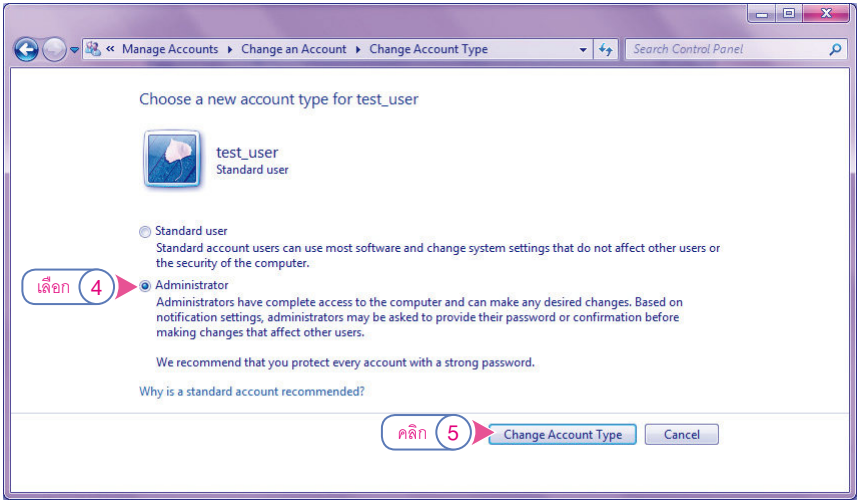
1. ให้เปิด Control Panel > User Accounts > Manage Accounts
2. ในกรณีนี้จะเป็นการเปลี่ยนสิทธิ์ของผู้ใช้งานชื่อ test_user ให้ดับเบิลคลิกตรงชื่อผู้ใช้ test_user



3. คลิกเลือก Change the account type

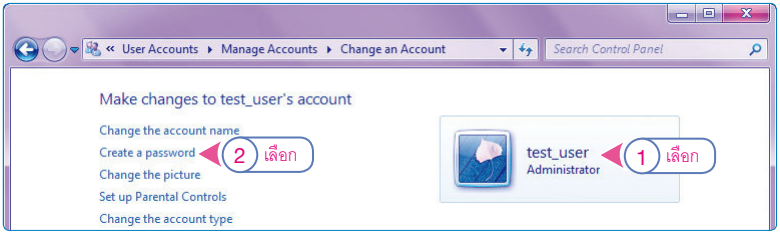


4. ในกรณีนี้ให้คลิกเลือก Administrator เพื่อเปลี่ยนสิทธิ์จากผู้ใช้ธรรมดาเป็นผู้ดูแลระบบ
5. คลิกปุ่ม Change Account Type ยืนยันการเปลี่ยนประเภทของผู้ใช้งาน

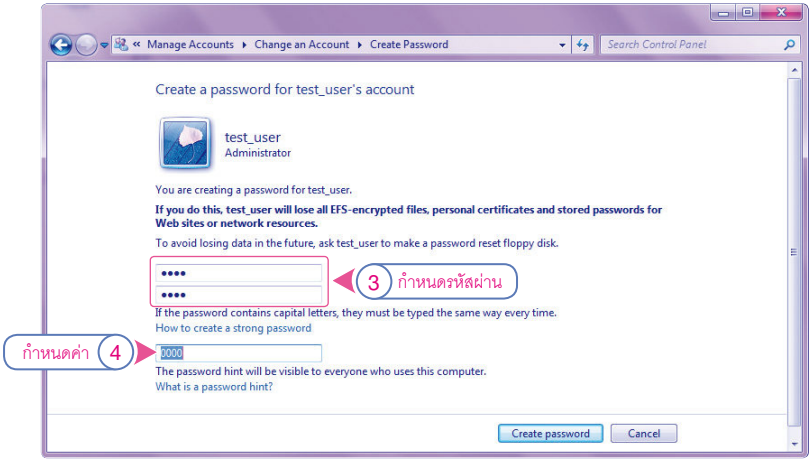


สร้างหรือเปลี่ยนรหัสผ่าน

1. ที่หน้าจอ User Accounts > Manage another account ให้คลิกเลือกชื่อ test_user หากต้องการจัดการรหัสผ่านของผู้ใช้คนนี้
2. ให้คลิกเลือก Create a password



3. พิมพ์รหัสผ่านใหม่จำนวน 2 ครั้งเพื่อยืนยันความถูกต้อง
4. นอกจากนี้ผู้ใช้งานยังสามารถระบุถึงคำใบ้กันลืม (Hint) ที่จำได้ง่ายสำหรับผู้ใช้งาน ในกรณีที่รหัสผ่านนั้นยากต่อการจดจำ แล้วคลิกปุ่ม Create password

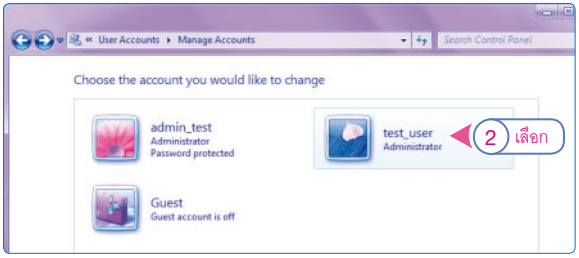


หมายเหตุ สำหรับการเปลี่ยนรหัสผ่าน ก็จะคล้ายคลึงกันกับวิธีสร้าง Password แต่ต่างกันตรงที่คลิกเลือก Change the password

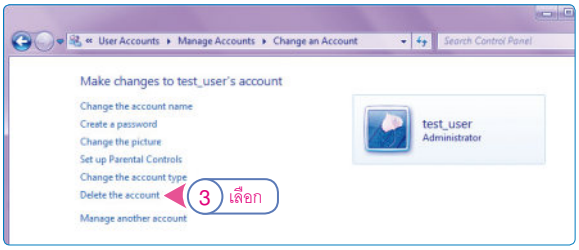
การลบผู้ใช้งาน

1. ให้คลิกเลือก Add or remove user accounts

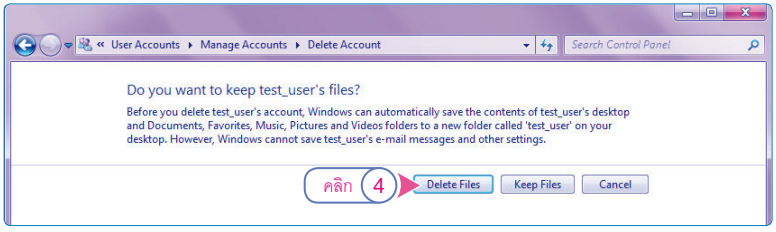
2. ในกรณีนี้ต้องการลบผู้ใช้งาน test_user โดยให้คลิกเลือกชื่อ test_user



3. คลิกเลือก Delete the account



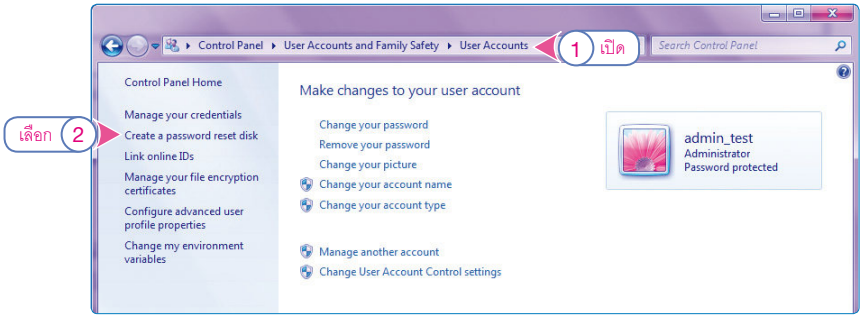
4. คลิกเลือกระหว่างลบไฟล์ที่เกี่ยวข้องทั้งหมด (Delete Files) หรือยังเก็บไฟล์ไว้อยู่ (Keep Files) แต่ในกรณีนี้ให้คลิกปุ่ม Delete Files เพื่อลบทั้งหมด



NOTE

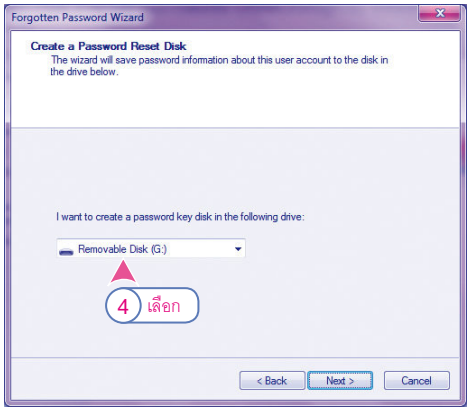
กรณีที่ผู้ใช้งานอาจจะลืมรหัสผ่าน ในส่วนนี้จะเป็นการสร้างชื่อสำรองเตรียมไว้ในกรณีที่อาจจะมีการลืม โดยมีขั้นตอนการดำเนินการดังต่อไปนี้

1. ให้เข้าไปที่ Control Panel > User Accounts and Family Safety > User Accounts
2. คลิกเลือก Create a password reset disk

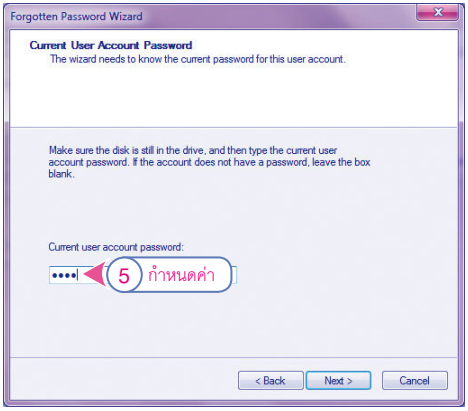


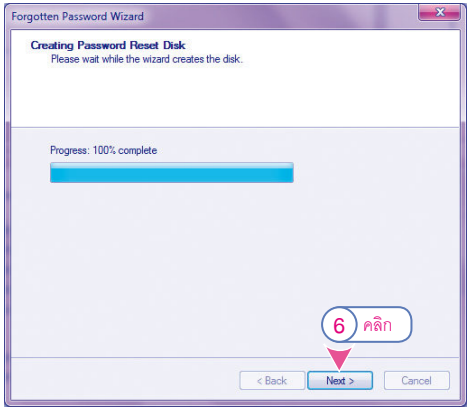
NOTE

3. คลิกปุ่ม Next >
4. คลิกเลือก USB หรือแผ่น CD (ในกรณีนี้เลือก USB ชื่อ Removable Disk) แล้วคลิกปุ่ม Next >

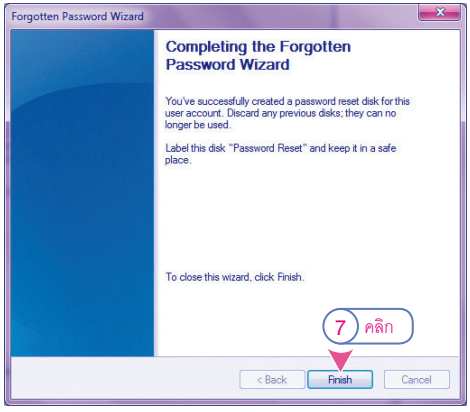


5. กรอก Password ที่ใช้ในการกู้คืน (Password ที่ใช้งานในปัจจุบัน) แล้วคลิกปุ่ม Next >
6. รอเมื่อเสร็จสิ้นให้คลิกปุ่ม Next >





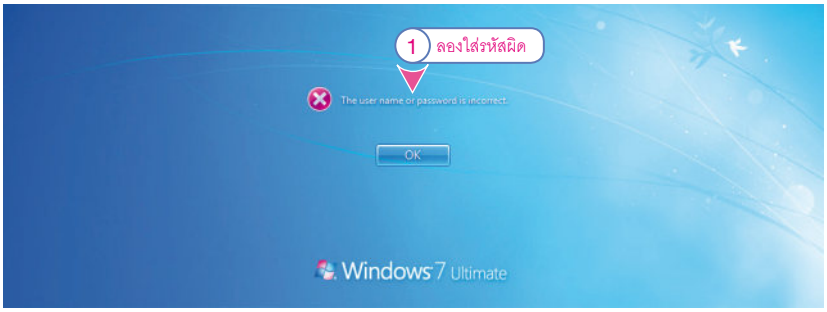
7. แล้วคลิกปุ่ม Finish



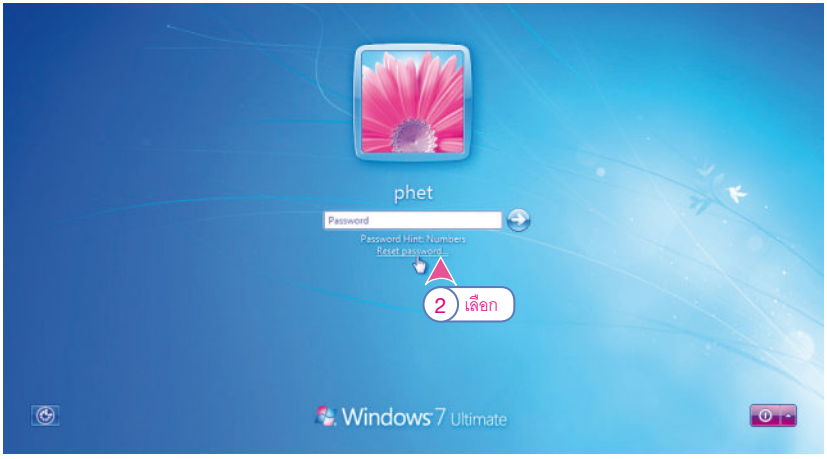
NOTE

ในส่วนถัดไป ให้ผู้อ่านปิดและเปิดเครื่องใหม่อีกครั้งหนึ่ง

1. เมื่อระบบแสดงหน้าจอ Log-in ให้ใส่ User และ Password โดยทดลองใส่รหัสที่ผิด ก็จะแสดงดังรูป

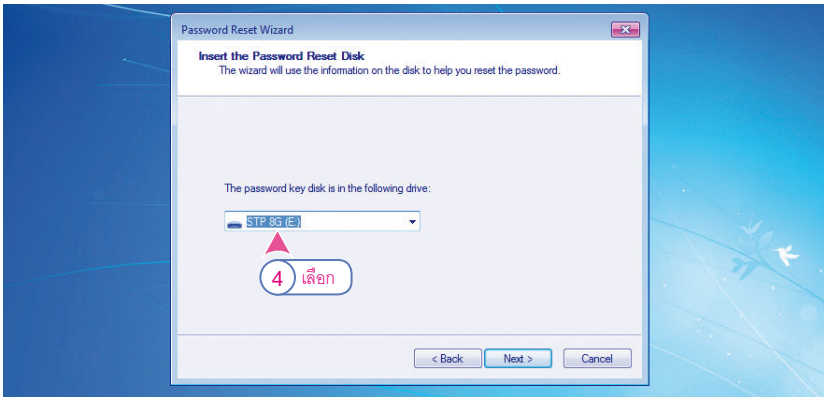


2. คลิกเลือก Reset password

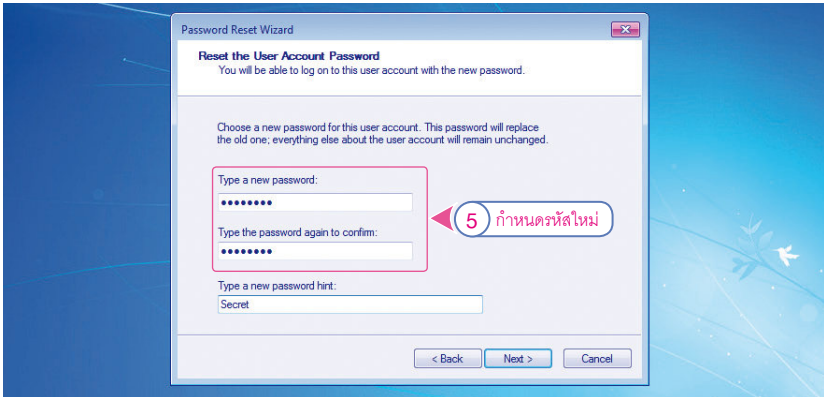


3. ก็จะแสดงหน้าต่าง Password Reset Wizard ให้คลิกปุ่ม Next >

4. คลิกเลือก USB Drive ที่จัดเก็บ Password แล้วคลิกปุ่ม Next >



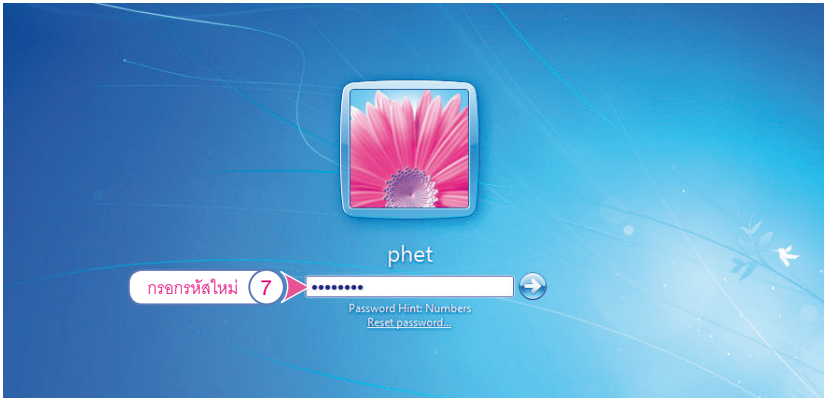
5. ให้ผู้ใช้งานใส่ Password ใหม่ในช่อง Type a new password: และใส่อีกครั้งให้เหมือนกันเพื่อเป็นการยืนยัน แล้วคลิกปุ่ม Next >



6. จะปรากฏหน้าจอ Completing the Password Reset ให้คลิกปุ่ม Finish

NOTE

7. หลังจากนั้นจะปรากฏหน้าจอ Log-in ใหม่อีกครั้ง คราวนี้ให้กรอก Password ที่ได้ตั้งไว้ใหม่ ก็จะสามารถใช้งาน Windows ได้ตามปกติ



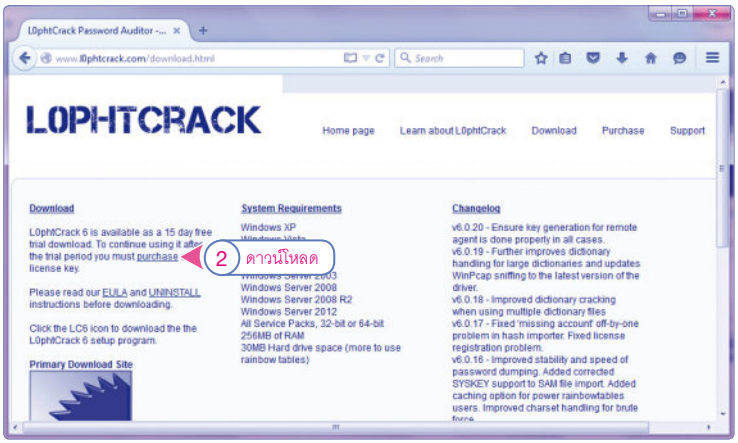
การวิเคราะห์รหัสผ่านที่ไม่ปลอดภัย

ในกรณีที่ผู้ใช้หรือผู้ดูแลระบบต้องการตรวจสอบรหัสผ่าน ที่อาจจะมีการตั้งไว้ซึ่งมีความอ่อนแอ หรือสุ่มเสี่ยงต่อการถูกโจมตี ก็จะสามารถใช้เครื่องมือในการเดา Password หรือที่เรียกว่า การทดลองแบบทุกวิธี หรือ Brute Force ต่างๆ ได้ดังตัวอย่างเช่น L0phtCrack โดยให้ดำเนินการตามขั้นตอนดังต่อไปนี้

1. ให้ติดตั้ง WinPcap โดยดาวน์โหลดได้จากเว็บไซต์ http://www.winpcap.org/install/bin/WinPcap_4_1_3.exe สำหรับเป็นเครื่องมือที่ใช้ในการดักจับแพ็กเก็ตต่างๆ บน Windows

2. ให้ติดตั้ง L0phtCrack 6 หรือ lc6setup_v6.0.17.exe โดยดาวน์โหลดได้จากเว็บไซต์ http://www.l0phtcrack.com/download.html

หมายเหตุ สำหรับรุ่นที่สามารถเดา Password แบบ Brute Force ฉบับเต็มจะต้องมีค่าใช้จ่าย



3. เพื่อให้ง่ายต่อการทดสอบรหัสผ่าน ให้ผู้อ่านทดสอบสร้างผู้ใช้งานระบบขึ้นมาใหม่ โดยตั้งรหัสผ่านอย่างง่าย แล้วจึงใช้โปรแกรม L0phtCrack เดารหัส เช่น abc หรือ 888888

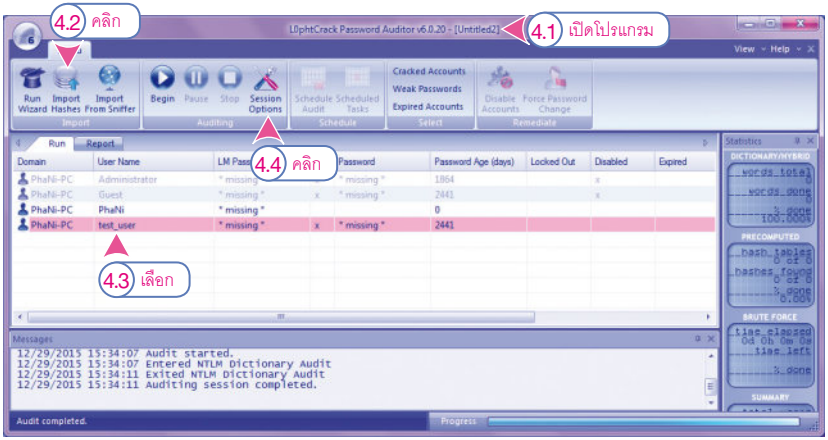
4. การทดสอบการเดารหัสผ่าน

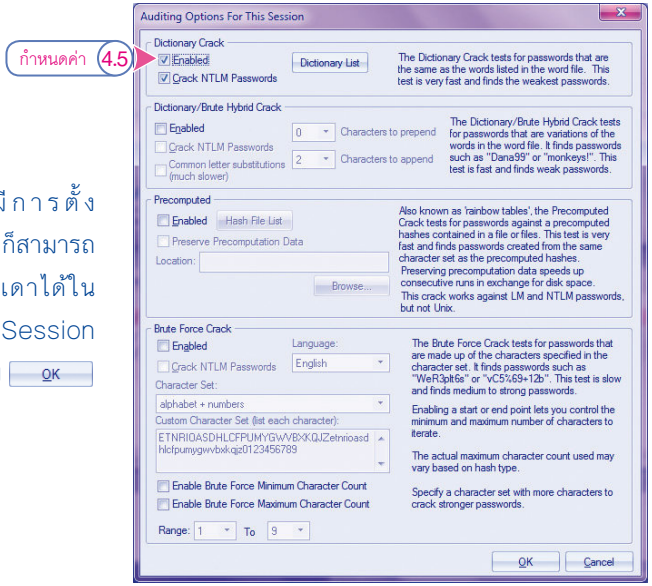
   4.1 ให้เปิดโปรแกรม L0phtCrack

   4.2 คลิกปุ่ม Import Hashes โปรแกรมก็จะนำเข้า Password ที่มีการแฮช (Hash) ไว้ในการเตรียมเดารหัสผ่าน (รายละเอียดเรื่อง Hash จะอธิบายในปฏิบัติการที่ 13)

   4.3 กรณีที่จะทดลองค้นหา Password ของ User = test_user ให้คลิกเลือก User = test_user

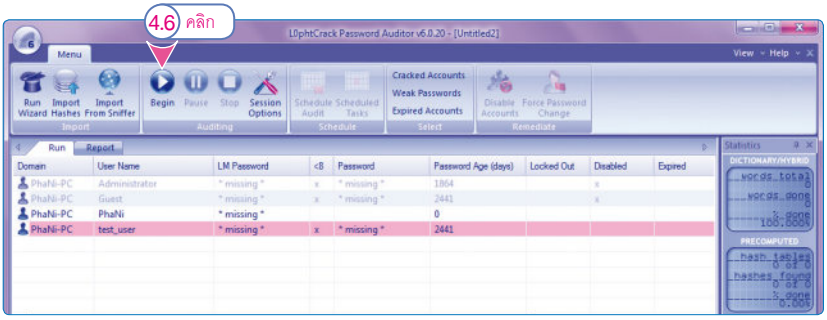
   4.4 ให้คลิกปุ่ม Session Options โดยจะต้องตั้งค่าต่างๆ เช่น ในกรณีที่ Password นั้นมีการตั้งที่ไม่แข็งแรง โดยอาจจะเป็นคำอยู่ในศัพท์ สามารถตั้งได้ดังรูปด้านล่าง



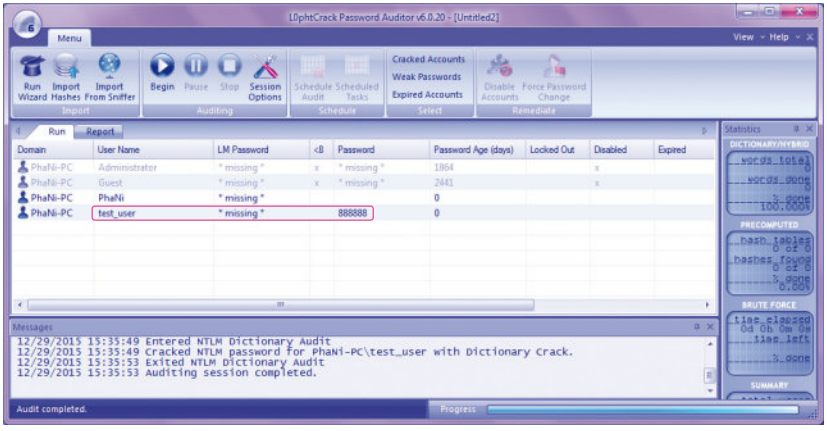


4.5 ในกรณีที่อาจจะมีการตั้ง Password ที่ซับซ้อน ก็สามารถปรับแต่งให้สามารถเดาได้ในรูปแบบต่างๆ โดยเลือก Session Options แล้วคลิกปุ่ม OK

4.6 จากนั้นให้คลิกปุ่ม Begin



หมายเหตุ ในการค้นหารหัสผ่านที่ซับซ้อน ก็จะทำให้เวลาที่ใช้ในการค้นหานั้นเพิ่มสูงขึ้น รวมไปถึงการใช้การประมวลผลที่สูงด้วย ซึ่งในกรณีนี้ User = test_user และ Password = 888888 เป็นต้น

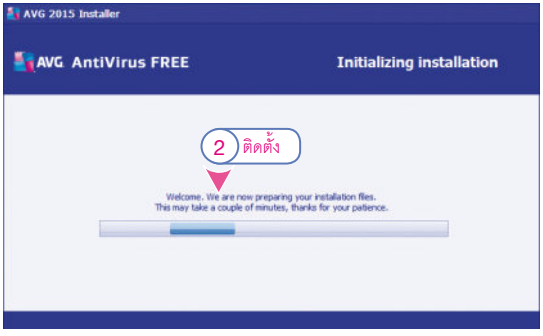


การปรับแต่งความมั่นคงปลอดภัย โดยการติดตั้ง Anti-Virus

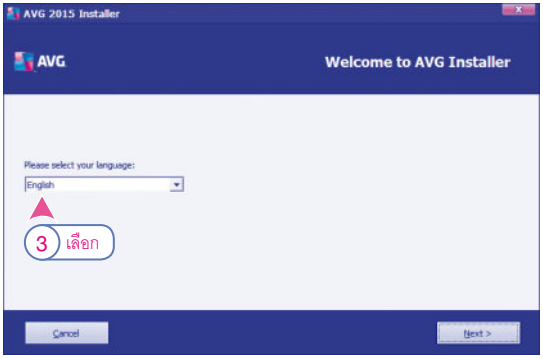
สำหรับส่วนต่อไป จะเป็นการฝึกติดตั้งโปรแกรมป้องกันไวรัส หรือ Anti-Virus โดยอ้างอิงกับโปรแกรม AVG Free Anti-Virus ซึ่งมีขั้นตอนดังต่อไปนี้

1. ให้ดาวน์โหลดโปรแกรม Anti-Virus จากเว็บไซต์ http://free.avg.com/ww-en/free-antivirus-download

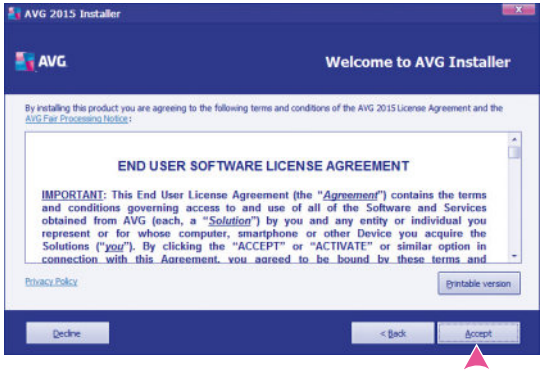
2. ดับเบิลคลิกไฟล์ avg_free_stb_all_2014_4745_cnet.exe เพื่อเข้าสู่กระบวนการติดตั้ง



3. เลือกภาษาที่ใช้ในการติดตั้ง (English) แล้วคลิกปุ่ม Next >

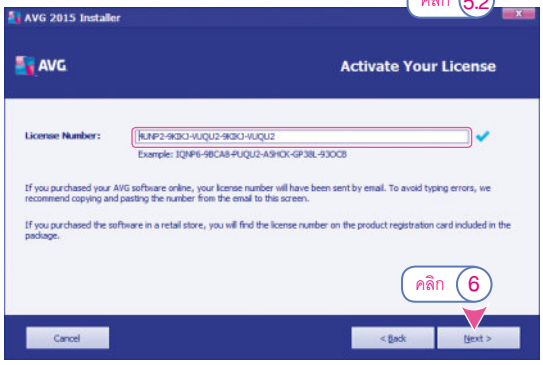


4. คลิกปุ่ม Accept ยอมรับเงื่อนไขการใช้งานโปรแกรม

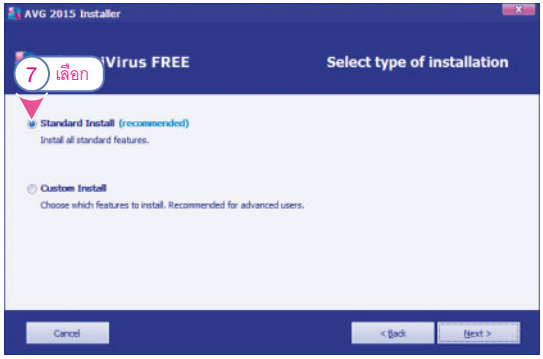


5. เลือกชนิดของโปรแกรมที่ต้องการติดตั้ง โดยให้เลือกเป็น Anti-Virus Free จากนั้นคลิกปุ่ม Next >

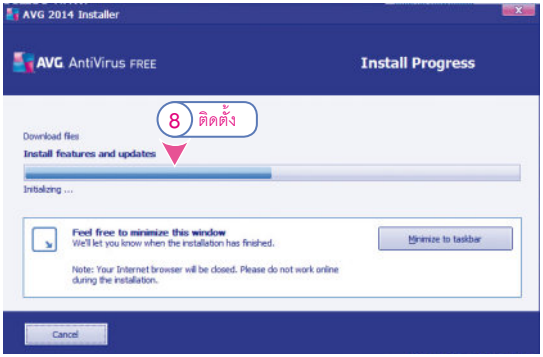
6. ขั้นตอนต่อไปโปรแกรมจะสร้าง License Key มาให้โดยอัตโนมัติ จากนั้นคลิกปุ่ม Next >



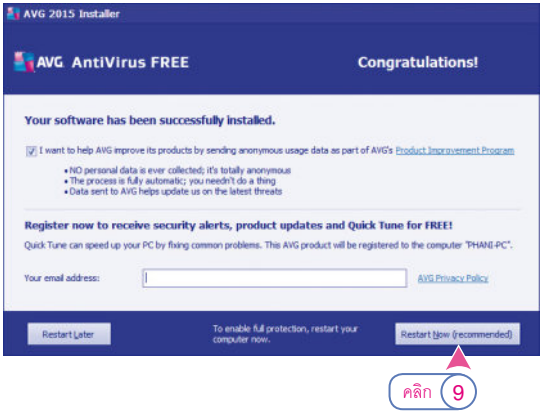
7. คลิกเลือก Standard Install จากนั้นคลิกปุ่ม Next >



8. ให้รอจนกระทั่งกระบวนการติดตั้งเสร็จสมบูรณ์



9. เมื่อการติดตั้งเสร็จสมบูรณ์ แนะนำให้คลิกปุ่ม Restart Now (recommended) เพื่อเริ่มกระบวนการรีสตาร์ทเครื่องใหม่



10. หลังจากรีสตาร์ทคอมพิวเตอร์แล้วจะพบว่า โปรแกรม AVG Free Anti-Virus พร้อมใช้งาน ดังรูปด้านล่าง

สร้างความปลอดภัย โดยการติดตั้ง Spybot

สำหรับในส่วนนี้ จะเป็นการฝึกติดตั้งโปรแกรมป้องกันการโจมตีต่างๆ เช่น Bot โดยใช้เครื่องมือ Spybot มีขั้นตอนดังต่อไปนี้

1. ให้ดาวน์โหลดโปรแกรม Spybot ได้จากเว็บไซต์ http://www.safer-networking.org/mirrors/
2. ดาวน์โหลดไฟล์ spybot-2.4.exe

3. ดับเบิลคลิกและติดตั้งโปรแกรม โดยเลือกภาษา English แล้วคลิกปุ่ม OK
4. คลิกปุ่ม Next >
5. คลิกเลือก ...installing Spybot for personal use, and will decide later. แล้วคลิกปุ่ม Next >