



คำนำ

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

อย่างไรก็ตามผู้เขียนได้ปรับแต่งเนื้อหาเพิ่มเติม ให้มีความหลากหลายและครอบคลุมที่มีความเหมาะสมกับผู้อ่านทั่วไปที่มีความสนใจอีกด้วย โดยประยุกต์ใช้กับอุปกรณ์จริงที่หาได้ทั่วไปในท้องตลาด ทั้งในส่วนของ การเปิดเผย (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 แต่ไม่ได้มีจุดประสงค์เพื่อเป็นการประสงค์ร้ายต่อระบบหรือหน่วยงานใดๆ หรือแม้แต่เพื่อยุยงส่งเสริมการใช้งานเครื่องมือในทางที่ผิด

ดังนั้น ผู้อ่านควรจะต้องทดสอบกับระบบปิดเท่านั้น และทุกครั้งเมื่อฝึกปฏิบัติการใดๆ ควรที่จะต้องตระหนักถึงความเสียหายที่จะเกิดขึ้นอยู่เสมอ ย้ำ! ผู้อ่านที่ยังขาดประสบการณ์ ควรจะต้องได้รับความแนะนำจากผู้เชี่ยวชาญก่อนจะดำเนินการใดๆ อีกทั้งผู้อ่านต้องศึกษาถึงกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคอมพิวเตอร์อีกด้วย

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

พศ.ดร.จักรชัย ไสอินทร์
Asst. Dr. Chakchai So-In

คำขอบคุณ

หนังสือเล่มนี้จะเกิดขึ้นไม่ได้ ถ้าไม่ได้กำลังใจที่สำคัญจากบุคคลหลายฝ่าย โดยผู้เขียนจะต้องขอขอบพระคุณคุณพ่อคุณแม่และครอบครัว ที่คอยเป็นกำลังใจและให้การสนับสนุนมาตลอด และคณะบุคคลที่เกี่ยวข้อง รวมไปถึงบุคลากรทุกท่านในภาควิชา มหาวิทยาลัยขอนแก่น และมหาวิทยาลัยเกษตรศาสตร์

ขอขอบคุณคณาจารย์ สุรศักดิ์ สงวนพงษ์, ฤชงค์ อุทยภาส, ยืน ภู่วรรวน, ศาสตรา วงศ์ธนวุธ, สุดสงวน งามสุริยโรจน์, สมนึก พ่วงพรพิทักษ์, กิตติ์ เขียวโรนปจัย และศิริปัฐช์ บุญครอง ที่เป็นแรงบันดาลใจในการเขียนหนังสือเล่มนี้ ขอขอบคุณนักศึกษา เพชร อิ่มทองคำ, คมเดช เผือดมุด, ชาติชาย บริบูรณ์ และศรายุทธ พูลสงวน ที่เป็นกำลังสำคัญในการพิสูจน์อักษรและเตรียมสื่อและรูปภาพ รวมไปถึงทดลองฝึกปฏิบัติการเพื่อความถูกต้องและสมบูรณ์

ซึ่งในระยะเวลา 3 ปีที่เตรียมจัดทำหนังสือ ต้องขอบคุณนักศึกษาในรายวิชาที่มีความตั้งใจ มุมนานะพยายามความขยันหมั่นเพียรที่ศึกษาตามเค้าโครงของหนังสือ โดยไม่ย่อท้อและมุ่งมั่น ทำให้ผู้เขียนมีกำลังใจในการพัฒนาการเรียนการสอนที่มีความสมบูรณ์เพิ่มขึ้น และต้องขอขอบคุณบรรณาธิการและสำนักพิมพ์ ที่ให้โอกาสในการจัดพิมพ์ โดยหนังสือเล่มนี้จะเกิดขึ้นไม่ได้ ต้องขอขอบคุณอีกครั้งหนึ่ง





สารบัญ

ปฏิบัติการที่ 1 การติดตั้งระบบปฏิบัติการและความมั่นคงปลอดภัยเบื้องต้น	1
แนะนำ Virtual Machine.....	2
การติดตั้ง Virtual Machine.....	2
การติดตั้ง Windows 7 บน Virtual Machine	4
การปรับแต่ง Virtual Machine.....	10
ความปลอดภัยเบื้องต้น โดยใช้ Windows Update	14
สรุปทเรียน.....	16
แบบฝึกหัดท้ายบท.....	16
ปฏิบัติการที่ 2 การปรับแต่งระบบบัญชีผู้ใช้และความมั่นคงปลอดภัยพื้นฐาน.....	17
แนะนำการโจมตีการเข้าถึง	18
กรรมวิธีการพิสูจน์ตัวตนจริง.....	18
การจัดการบัญชีผู้ใช้บน Windows.....	19
การเพิ่มบัญชีผู้ใช้งาน.....	19
เปลี่ยนแปลงสิทธิ์ให้กับผู้ใช้ที่มีอยู่เดิม	21
สร้างหรือเปลี่ยนรหัสผ่าน	22
การลบผู้ใช้งาน.....	22
การวิเคราะห์รหัสผ่านที่ไม่ปลอดภัย.....	27
การปรับแต่งความมั่นคงปลอดภัย โดยการติดตั้ง Anti-Virus	30
สร้างความปลอดภัย โดยการติดตั้ง Spybot.....	33
การติดตั้ง Microsoft Baseline Security.....	37
การติดตั้ง Malicious Software Removal Tool.....	39
การติดตั้ง Microsoft Security Essential.....	41
สรุปทเรียน.....	42
แบบฝึกหัดท้ายบท.....	42

ปฏิบัติการที่ 3 การติดตั้งและตรวจสอบบริการที่มั่นคงปลอดภัย.....	43
แนะนำบริการบนอินเทอร์เน็ต.....	44
บริการ Telnet.....	44
บริการรับ/ส่งไฟล์ (FTP).....	45
บริการเว็บ.....	46
บริการเสริมความปลอดภัย Telnet และ FTP.....	47
บริการเสริมความปลอดภัยเว็บ หรือ HTTPS.....	48
การติดตั้งบริการ Telnet, FTP และ WWW บน Windows.....	48
การติดตั้งบริการ Telnet.....	50
การติดตั้งบริการ FTP.....	54
การติดตั้งบริการเว็บ (Web Server).....	57
การติดตั้งบริการ Secure Shell, Secure FTP และ Secure Web (HTTPS) บน Windows.....	62
การติดตั้งบริการ Secure Shell (SSH).....	62
การติดตั้งบริการ Secure FTP.....	67
การปรับแต่งบริการ HTTPS.....	71
การตรวจสอบการใช้งานเครือข่ายด้วย Packet Sniffer บน Windows.....	77
การดักจับข้อมูลเครือข่ายด้วย Wireshark.....	77
การตรวจสอบข้อมูลโดยใช้บริการ SSH.....	82
การตรวจสอบข้อมูลโดยใช้ FTP.....	86
การตรวจสอบข้อมูลโดยใช้ Secure FTP (SFTP).....	90
การตรวจสอบข้อมูลโดยใช้ HTTP.....	93
การตรวจสอบข้อมูลโดยใช้ HTTPS.....	96
สรุปทฤษฎี.....	98
แบบฝึกหัดท้ายบท.....	98
ปฏิบัติการที่ 4 การจัดการเซิร์ฟเวอร์ การช่วยเหลือ และป้องกันระบบเบื้องต้น.....	99
แนะนำการแบ่งปันทรัพยากร.....	99
แนะนำโปรโตคอล ARP.....	100
การตั้งค่าแชร์ Printer.....	101
ที่เครื่องเซิร์ฟเวอร์ต้นทาง.....	102
ที่เครื่องไคลเอนต์ปลายทาง.....	104
การแชร์ไฟล์และโฟลเดอร์ (Map Drive).....	107
การตั้งค่าเครื่องต้นทาง.....	107
ใช้งานที่เครื่องปลายทาง.....	114

การใช้งาน Remote Assistance บน Windows.....	117
ตั้งค่าอนุญาตใช้งาน Remote Desktop.....	118
ที่เครื่องคอมพิวเตอร์ต้นทาง.....	118
การโจมตี ARP ด้วยโปรแกรม NetCut.....	120
ติดตั้งเครื่องมือทดสอบ NetCut.....	120
การทดสอบการโจมตี.....	122
การป้องกันการโจมตี NetCut.....	123
การติดตั้ง Personal Firewall บน Windows.....	128
สรุปทบทเรียน.....	136
แบบฝึกหัดท้ายบท.....	136

ปฏิบัติการที่ 5 การบริหารจัดการและวิเคราะห์เครือข่าย137

แนะนำการบริหารจัดการเครือข่าย.....	138
โปรโตคอลบริหารจัดการเครือข่าย.....	139
การบริหารจัดการและวิเคราะห์ข้อมูลของระบบปฏิบัติการ Windows.....	141
การวิเคราะห์ชื่อระบบชื่อ (Domain Name) บน Windows.....	152
การตรวจสอบข้อมูลเครือข่ายโดยใช้ nmap.....	154
การบริหารจัดการและวิเคราะห์ข้อมูลโดยใช้ SNMP บน Windows.....	156
การบริหารจัดการและวิเคราะห์ข้อมูลโดยใช้ SNMP บนอุปกรณ์เครือข่ายหรือเราเตอร์.....	162
การปรับแต่ง SNMP เพื่อผนวกความมั่นคงปลอดภัยให้กับ Net-SNMP.....	169
การปรับแต่ง SNMP เพื่อผนวกความมั่นคงของอุปกรณ์เราเตอร์.....	174
สรุปทบทเรียน.....	176
แบบฝึกหัดท้ายบท.....	176

ปฏิบัติการที่ 6 การจัดการ VPN, IPSec และอีเมลแบบมั่นคงปลอดภัย.....177

แนะนำ IPSec และ VPN.....	178
ทำความเข้าใจ IPSec.....	178
เฟรมเวิร์คของ IPSec.....	179
โหมดการทำงานของ IPSec.....	180
ทำความเข้าใจ VPN.....	181
แนะนำบริการความมั่นคงปลอดภัยกับอีเมล.....	182
รู้จักโปรโตคอล PGP.....	182
การติดตั้งบริการ VPN บน Windows.....	182
การติดตั้ง IPSec บน Windows.....	189

การปรับแต่งความมั่นคงปลอดภัยในการส่งอีเมลบน Windows.....	199
สรุปบทเรียน.....	208
แบบฝึกหัดท้ายบท.....	208
ปฏิบัติการที่ 7 ตรวจสอบการบุกรุกเครือข่ายพื้นฐาน และ Buffer Overflow.....	209
แนะนำระบบการตรวจสอบการบุกรุก.....	210
แนะนำแพ็คเกจ โอเวอร์โฟลว์.....	211
การใช้งาน SNORT บน Windows.....	213
การพัฒนาโปรแกรมในเงื่อนไข Buffer Overflow บน Windows.....	226
สรุปบทเรียน.....	232
แบบฝึกหัดท้ายบท.....	232
ปฏิบัติการที่ 8 ไฟร์วอลล์ เนก และเพร็อกซี่	233
การแปลงเลขที่อยู่เครือข่าย (NAT)	234
บริการ DHCP	234
ไฟร์วอลล์.....	236
ประเภทของไฟร์วอลล์ (Type of Firewall).....	236
การติดตั้งและปรับแต่ง NAT และ DHCP Server.....	239
การติดตั้งและปรับแต่งการใช้งาน Firewall บน Windows (เพิ่มการ์ดแลน 2 ตัว)	248
การติดตั้งและปรับแต่ง Squid Proxy.....	254
สรุปบทเรียน.....	258
แบบฝึกหัดท้ายบท.....	258
ปฏิบัติการที่ 9 การทดสอบภัยคุกคามของระบบ	259
แนะนำรูปแบบของความมั่นคงระบบและเครือข่าย	260
ซอฟต์แวร์ มัลลิเซียส.....	261
ประตุกล	261
การระเบิดทางลोजิก.....	261
ม้าโทรจัน.....	262
ผีดิบหรือขอมบี้	262
โมบาย คัด.....	262
ไวรัส.....	262
เวิร์มหรือหนอน.....	263
การโจมตีแบบดีไอเอส.....	263
การติดตั้งและปรับแต่ง Keylogger	264

ปฏิบัติการที่ 03 การติดตั้งและตรวจสอบบริการที่มั่นคงปลอดภัย	43
แนะนำบริการบนอินเทอร์เน็ต.....	44
บริการ Telnet.....	44
บริการรับ/ส่งไฟล์ (FTP)	45
บริการเว็บ	46
บริการเสริมความปลอดภัย Telnet และ FTP.....	47
บริการเสริมความปลอดภัยเว็บ หรือ HTTPS.....	48
การติดตั้งบริการ Telnet, FTP และ WWW บน Windows	48
การติดตั้งบริการ Telnet.....	50
การติดตั้งบริการ FTP.....	54
การติดตั้งบริการเว็บ (Web Server).....	57
การติดตั้งบริการ Secure Shell, Secure FTP และ Secure Web (HTTPS) บน Windows	62
การติดตั้งบริการ Secure Shell (SSH)	62
การติดตั้งบริการ Secure FTP.....	67
การปรับแต่งบริการ HTTPS.....	71
การตรวจสอบการใช้งานเครือข่ายด้วย Packet Sniffer บน Windows.....	77
การดักจับข้อมูลเครือข่ายด้วย Wireshark.....	77
การตรวจสอบข้อมูลโดยใช้บริการ SSH.....	82
การตรวจสอบข้อมูลโดยใช้ FTP	86
การตรวจสอบข้อมูลโดยใช้ Secure FTP (SFTP).....	90
การตรวจสอบข้อมูลโดยใช้ HTTP.....	93
การตรวจสอบข้อมูลโดยใช้ HTTPS.....	96
สรุปทเรียน.....	98
แบบฝึกหัดท้ายบท.....	98
ปฏิบัติการที่ 04 การจัดการแชรข้อมูล การช่วยเหลือ และป้องกันระบบเบื้องต้น	99
แนะนำการแบ่งปันทรัพยากร.....	99
แนะนำโปรโตคอล ARP.....	100
การตั้งค่าแชร์ Printer.....	101
ที่เครื่องเซิร์ฟเวอร์ต้นทาง	102
ที่เครื่องไคลเอนท์ปลายทาง.....	104
การแชร์ไฟล์และโฟลเดอร์ (Map Drive).....	107
การตั้งค่าเครื่องต้นทาง	107
ใช้งานที่เครื่องปลายทาง.....	114

การใช้งาน Remote Assistance บน Windows.....	117
ตั้งค่าอนุญาตใช้งาน Remote Desktop.....	118
ที่เครื่องคอมพิวเตอร์ต้นทาง.....	118
การโจมตี ARP ด้วยโปรแกรม NetCut.....	120
ติดตั้งเครื่องมือทดสอบ NetCut.....	120
การทดสอบการโจมตี.....	122
การป้องกันการโจมตี NetCut.....	123
การติดตั้ง Personal Firewall บน Windows.....	128
สรุปทบทวน.....	136
แบบฝึกหัดท้ายบท.....	136

ปฏิบัติการที่ 05 การบริหารจัดการและวิเคราะห์เครือข่าย137

แนะนำการบริหารจัดการเครือข่าย.....	138
โปรโตคอลบริหารจัดการเครือข่าย.....	139
การบริหารจัดการและวิเคราะห์ข้อมูลของระบบปฏิบัติการ Windows.....	141
การวิเคราะห์ชื่อระบบชื่อ (Domain Name) บน Windows.....	152
การตรวจสอบข้อมูลเครือข่ายโดยใช้ nmap.....	154
การบริหารจัดการและวิเคราะห์ข้อมูลโดยใช้ SNMP บน Windows.....	156
การบริหารจัดการและวิเคราะห์ข้อมูลโดยใช้ SNMP บนอุปกรณ์เครือข่ายหรือเราเตอร์.....	162
การปรับแต่ง SNMP เพื่อผนวกความมั่นคงปลอดภัยให้กับ Net-SNMP.....	169
การปรับแต่ง SNMP เพื่อผนวกความมั่นคงของอุปกรณ์เราเตอร์.....	174
สรุปทบทวน.....	176
แบบฝึกหัดท้ายบท.....	176

ปฏิบัติการที่ 06 การจัดการ VPN, IPSec และอีเมลแบบมั่นคงปลอดภัย177

แนะนำ IPSec และ VPN.....	178
ทำความเข้าใจ IPSec.....	178
เฟรมเวิร์คของ IPSec.....	179
โหมดการทำงานของ IPSec.....	180
ทำความเข้าใจ VPN.....	181
แนะนำบริการความมั่นคงปลอดภัยกับอีเมล.....	182
รู้จักโปรโตคอล PGP.....	182
การติดตั้งบริการ VPN บน Windows.....	182
การติดตั้ง IPSec บน Windows.....	189

การปรับแต่งความมั่นคงปลอดภัยในการส่งอีเมลบน Windows.....	199
สรุปบทเรียน.....	208
แบบฝึกหัดท้ายบท.....	208
ปฏิบัติการที่ 07 ตรวจสอบการบุกรุกเครือข่ายพื้นฐาน II: Buffer Overflow	209
แนะนำระบบการตรวจสอบการบุกรุก.....	210
แนะนำแพ็คเกจ โอเวอร์โฟลว์.....	211
การใช้งาน SNORT บน Windows.....	213
การพัฒนาโปรแกรมในเงื่อนไข Buffer Overflow บน Windows.....	226
สรุปบทเรียน.....	232
แบบฝึกหัดท้ายบท.....	232
ปฏิบัติการที่ 08 ไฟร์วอลล์ แนท และพร็อกซี.....	233
การแปลงเลขที่อยู่เครือข่าย (NAT)	234
บริการ DHCP	234
ไฟร์วอลล์.....	236
ประเภทของไฟร์วอลล์ (Type of Firewall).....	236
การติดตั้งและปรับแต่ง NAT และ DHCP Server	239
การติดตั้งและปรับแต่งการใช้งาน Firewall บน Windows (เพิ่มการ์ดแลน 2 ตัว)	248
การติดตั้งและปรับแต่ง Squid Proxy	254
สรุปบทเรียน.....	258
แบบฝึกหัดท้ายบท.....	258
ปฏิบัติการที่ 09 การทดสอบภัยคุกคามของระบบ.....	259
แนะนำรูปแบบของความมั่นคงระบบและเครือข่าย	260
ซอฟต์แวร์ มัลลิเชี่ยส.....	261
ประตุกล	261
การระเบิดทางลोजิก.....	261
ม้าโทรจัน.....	262
ผีดิบหรือซอมบี้.....	262
โมบาย คัด.....	262
ไวรัส.....	262
เวิร์มหรือหนอน.....	263
การโจมตีแบบดีไอเอส.....	263
การติดตั้งและปรับแต่ง Keylogger	264

การติดตั้งและปรับแต่ง Trojan Horse.....	275
การติดตั้งและปรับแต่ง DoS.....	281
การลบไฟล์ Trojan Horse ออกจากเครื่องคอมพิวเตอร์.....	290
สรุปบทเรียน.....	294
แบบฝึกหัดท้ายบท.....	294

ปฏิบัติการที่ 10 การมีตัวตนจริง ค่าสถิติ และสำรองข้อมูล295

แนะนำการพิสูจน์ตัวตน.....	296
หลักการ AAA.....	296
โปรโตคอลในการพิสูจน์ตัวตน.....	297
RADIUS.....	298
การเฝ้าดู Log.....	298
การพิสูจน์ตัวตน Radius Server.....	299
การปรับแต่งการเชื่อมต่อกับเราท์เตอร์.....	299
การติดตั้ง WinRadius บน Windows.....	304
การพิสูจน์ตัวตนบนเราท์เตอร์.....	308
การใช้งาน Syslog Server (Windows).....	313
การสำรองข้อมูลสำหรับเราท์เตอร์.....	315
การสำรองข้อมูลสำหรับเซิร์ฟเวอร์ Windows.....	320
เริ่มต้นสำรองข้อมูล.....	320
กู้คืนหรือเรียกคืนข้อมูล.....	323
สรุปบทเรียน.....	324
แบบฝึกหัดท้ายบท.....	324

ปฏิบัติการที่ 11 สคริปต์และการซ่อนข้อความ325

แบดซีไฟล์ คืออะไร.....	326
การซ่อนข้อความในรูปภาพ คืออะไร.....	326
การฝึกปฏิบัติการเขียนสคริปต์ .bat บน Windows.....	326
การฝึกเขียนโปรแกรม .exe บน Windows.....	331
การผสมไฟล์ข้อความและรูปภาพบน Windows.....	337
การซ่อนไฟล์ .exe เข้ากับรูปภาพโดยให้ทำงานอัตโนมัติ.....	339
การติดตั้งเครื่องพัฒนาโปรแกรม Eclipse และการทดสอบ Hello World.....	341
การซ่อนข้อความในรูปภาพ (Steganography).....	344
สรุปบทเรียน.....	361
แบบฝึกหัดท้ายบท.....	362

ปฏิบัติการที่ 12	วิทยาการเข้ารหัสพื้นฐาน.....	363
แนะนำวิทยาการรหัสลับ		363
การเข้ารหัสโดยการแทนที่		363
ซีซาร์ส ไชเฟอร์.....		364
โมนออัลฟาเบติก ไชเฟอร์.....		364
เพลย์แฟร์ ไชเฟอร์.....		365
วีจิเนียร์ ไชเฟอร์.....		366
การเข้ารหัสแบบเปลี่ยนตำแหน่ง.....		367
ไชเฟอร์แบบผลคูณ.....		368
การฝึกพัฒนาโปรแกรมการเข้ารหัสและถอดรหัส โดยใช้ Caesar Cipher		368
การฝึกพัฒนาโปรแกรมการเข้ารหัสและถอดรหัส โดยใช้ Playfair Cipher.....		373
การฝึกพัฒนาโปรแกรมการเข้ารหัสและถอดรหัส โดยใช้ Vigenère Cipher		379
การฝึกพัฒนาโปรแกรมการเข้ารหัสและถอดรหัส โดยใช้ Row Transposition Cipher.....		383
การฝึกพัฒนาโปรแกรมการเข้ารหัสและถอดรหัส โดยใช้ Brute Force.....		387
สรุปทเรียน.....		390
แบบฝึกหัดท้ายบท.....		390
ปฏิบัติการที่ 13	การเข้ารหัสและถอดรหัสลับพื้นฐาน.....	391
แนะนำบล็อกไชเฟอร์.....		391
ดีอีเอส (DES).....		393
เออีเอส (AES)		393
เรนจด์ัล (Rijndael).....		394
การเข้ารหัสแบบพับลิคคีย์		395
อาร์เอสเอ.....		397
ฟังก์ชัน Hash		398
การฝึกเข้ารหัสและถอดรหัส โดยใช้คีย์แบบสมมาตรโดยใช้ Eclipse JAVA		398
การฝึกพัฒนาโปรแกรมการทำ Hash โดยใช้ Eclipse JAVA.....		411
การฝึกเข้ารหัสและถอดรหัส โดยใช้คีย์แบบสมมาตรโดยใช้ Eclipse JAVA.....		417
สรุปทเรียน.....		423
แบบฝึกหัดท้ายบท.....		424
บรรณานุกรม.....		425
Index		428

การติดตั้งระบบปฏิบัติการและ ความมั่นคงปลอดภัยเบื้องต้น

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 และในที่สุดท้ายจะเป็นการอธิบายการปรับแต่งเสริมความมั่นคงปลอดภัยด้วย 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

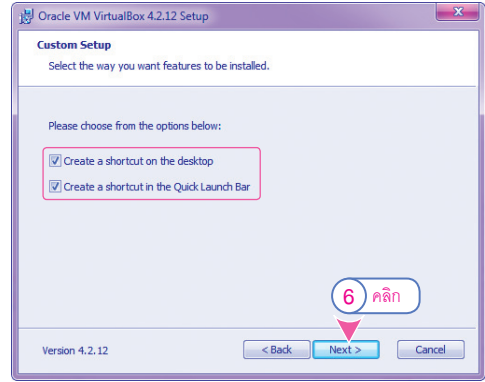
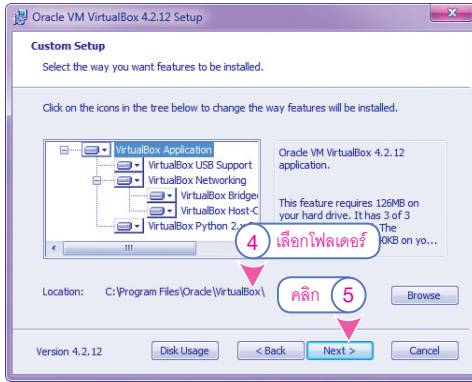
1. ในการติดตั้ง VirtualBox นั้น ให้ผู้อ่านเข้าไปดาวน์โหลดไฟล์ติดตั้งที่ <https://www.virtualbox.org/wiki/Downloads> โดยเลือกดาวน์โหลดไฟล์ที่เป็น for Windows hosts x86/amd64



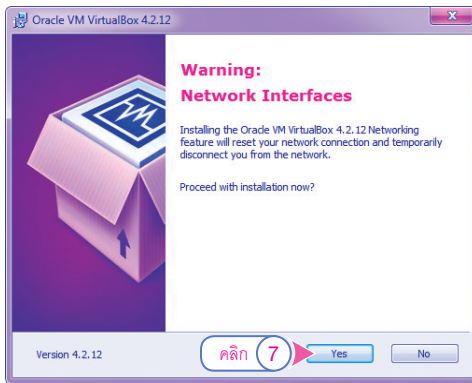
2. ดับเบิลคลิกที่ไฟล์ VirtualBox-4.2.12-84980-Win.exe เพื่อดำเนินการติดตั้ง
3. คลิกปุ่ม 



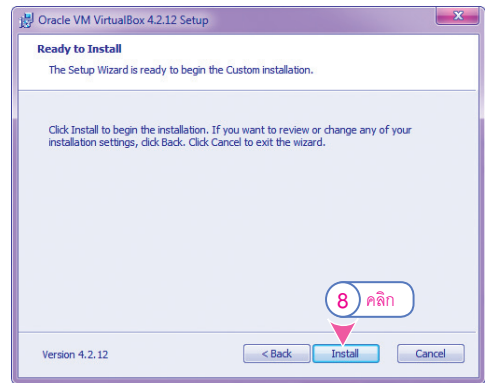
4. คลิกปุ่ม **Browse** เพื่อเลือกตำแหน่งที่จะติดตั้ง ซึ่งในกรณีนี้ใช้ค่า Default (หรือได้รับการแนะนำจากระบบเดิม)
5. คลิกปุ่ม **Next >**
6. รอกการติดตั้งรวมถึงการสร้าง Shortcut แล้วคลิกปุ่ม **Next >**



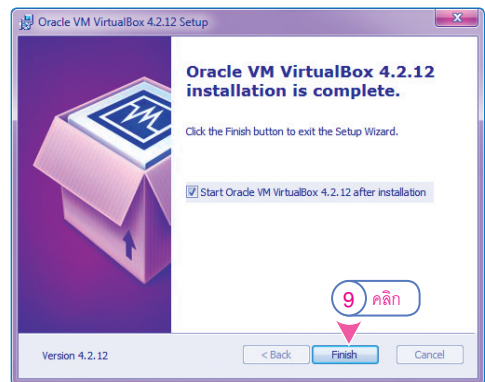
7. ดำเนินตามขั้นตอน ให้คลิกปุ่ม **Yes**



8. ให้คลิกปุ่ม **Install**



9. ปรากฏหน้าจอ Installation is complete (Finish) ซึ่งแสดงถึงการติดตั้งนั้นเสร็จสมบูรณ์แล้ว คลิกปุ่ม **Finish**



WARN

ผู้อ่านจะต้องระมัดระวังในการเลือกตำแหน่งที่จะติดตั้ง โดยเฉพาะหลังจากการติดตั้งเสร็จแล้ว เมื่อผู้อ่านสร้าง Virtual Machine ที่รองรับการติดตั้ง Server หรือระบบปฏิบัติการอื่นๆ ก็จะต้องเตรียมพื้นที่ในการติดตั้งเพิ่มขึ้นด้วย


การติดตั้ง Windows 7 UU Virtual Machine

ในส่วนนี้เป็นตัวอย่างหนึ่งที่ใช้ทดสอบการติดตั้ง VirtualBox โดยเป็นการติดตั้ง Windows 7 ลงบน Virtual Machine ซึ่งมีขั้นตอนดังต่อไปนี้

NOTE

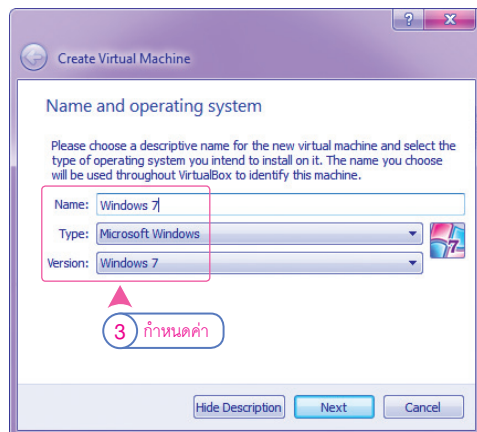
ในกรณีที่คือนักศึกษาจากมหาวิทยาลัยที่มีความร่วมมือกับบริษัท Microsoft ก็สามารถดาวน์โหลดผ่านทาง MSDN-AA หรือติดต่อผ่าน Microsoft Student Partner (MSP)

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

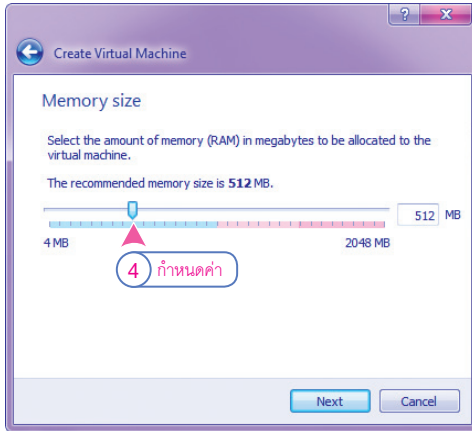
1. เตรียมไฟล์ติดตั้ง เช่น Windows 7.iso ในกรณีที่ผู้อ่านมีไฟล์ติดตั้ง (.iso) อยู่แล้วให้ข้ามขั้นตอนนี้ไป แต่ถ้าไม่มีให้เข้าไปเตรียมไฟล์ติดตั้ง Windows 7.iso ด้วยแผ่นต้นฉบับที่หาซื้อได้จากร้านค้าคอมพิวเตอร์ทั่วไปที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย
2. คลิกปุ่ม  สร้าง Virtual Machine (New)



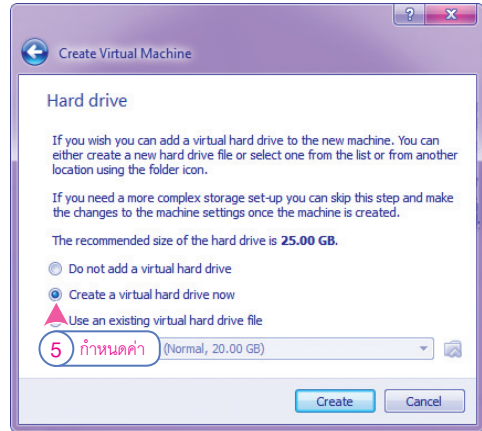
3. กำหนดชื่อ ชนิด และรุ่นเป็น Microsoft Windows 7 แล้วคลิกปุ่ม 



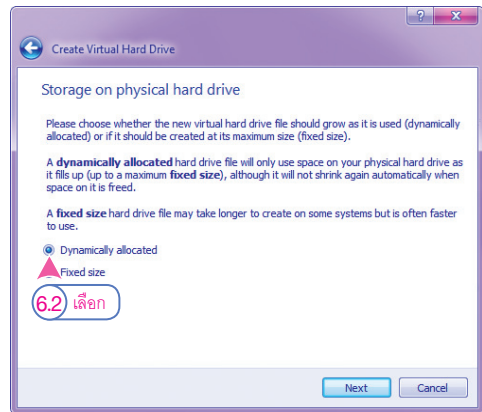
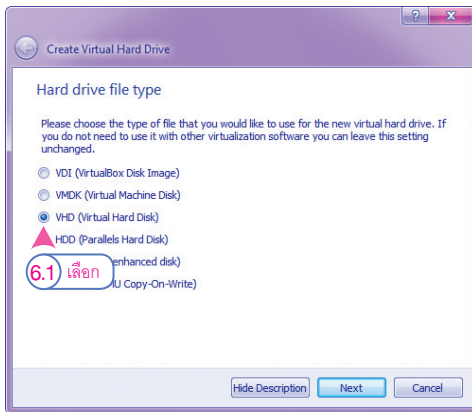
4. กำหนดหน่วยความจำ เช่น 512 MB แล้วคลิกปุ่ม **Next**



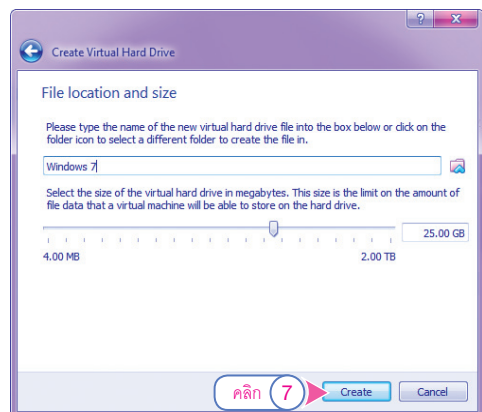
5. กำหนดขนาดพื้นที่ฮาร์ดดิสก์ เช่น 25 GB แล้วคลิกปุ่ม **Create**



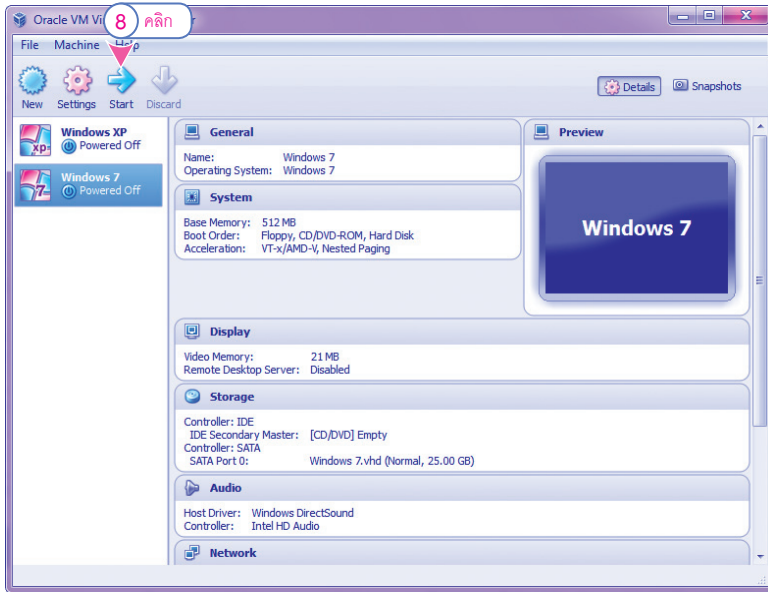
6. กำหนดพื้นที่ ชนิด และรูปแบบของฮาร์ดดิสก์ แล้วคลิกปุ่ม **Next**



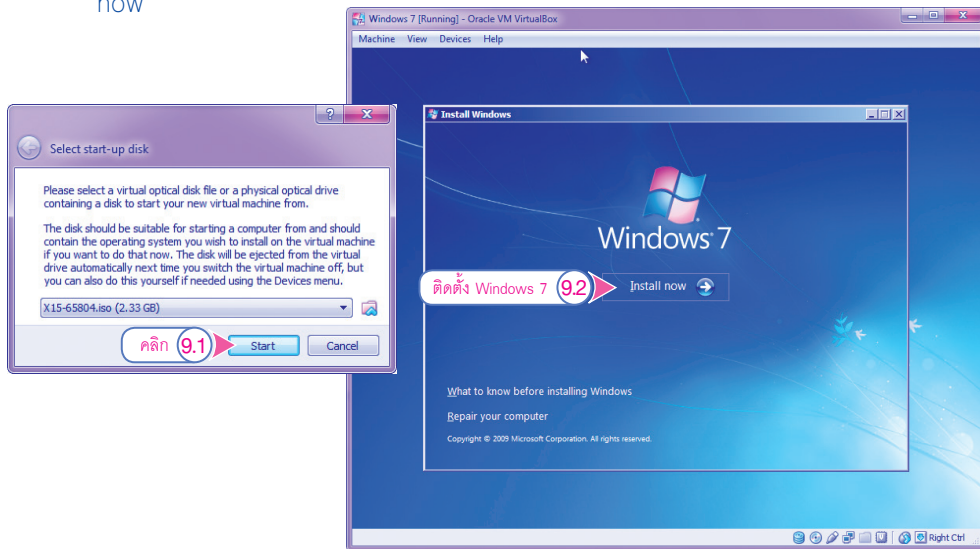
7. สร้าง Virtual Hard Disk แล้วคลิกปุ่ม **Create**



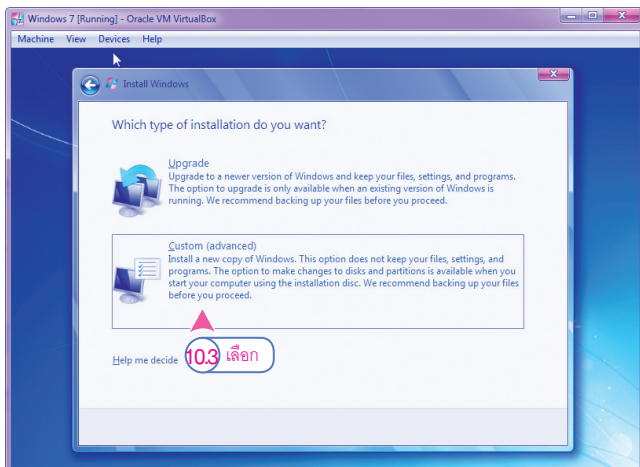
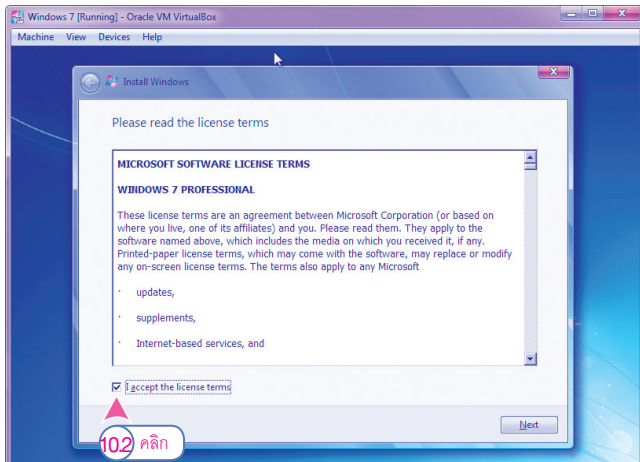
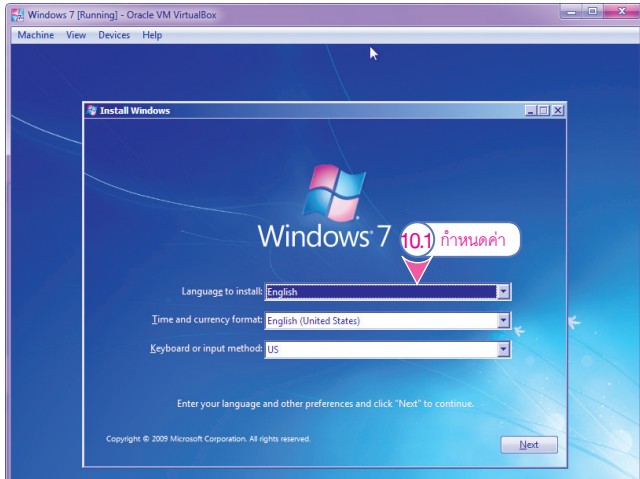
8. ขั้นตอนต่อไปเป็นการเริ่มติดตั้ง Windows 7



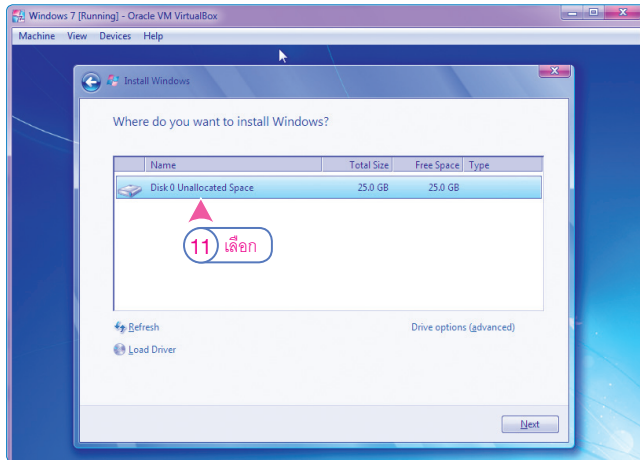
9. ให้คลิกเลือก start-up disk ไปยังไฟล์ที่ใช้ติดตั้งแล้วคลิกปุ่ม **Start** และคลิกเลือก Install now



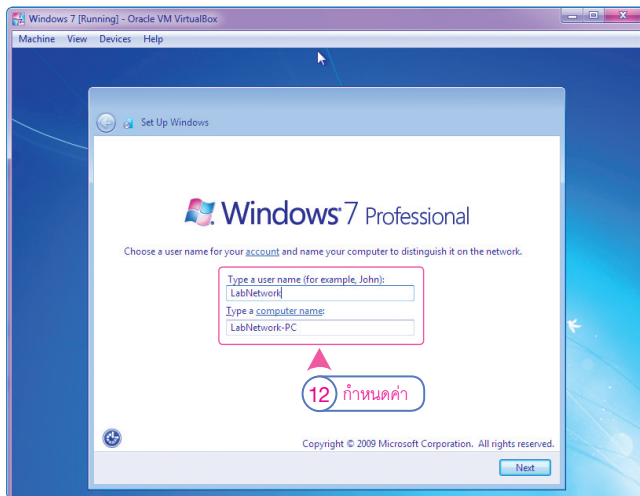
10. กำหนดภาษาและเงื่อนไขต่างๆ แล้วคลิกปุ่ม 



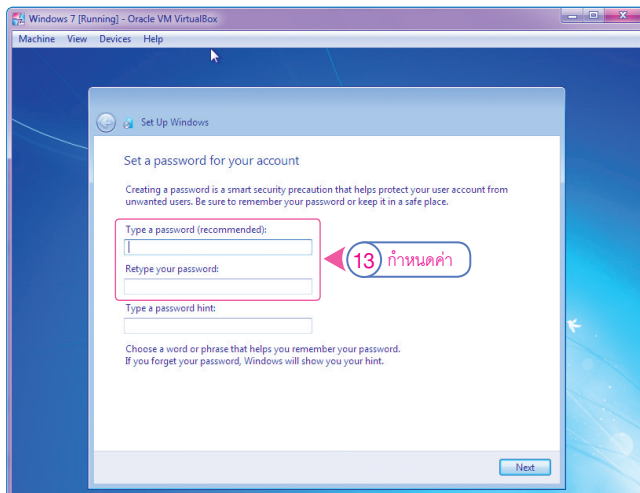
11. เลือกพื้นที่ในการติดตั้ง แล้วคลิกปุ่ม **Next**



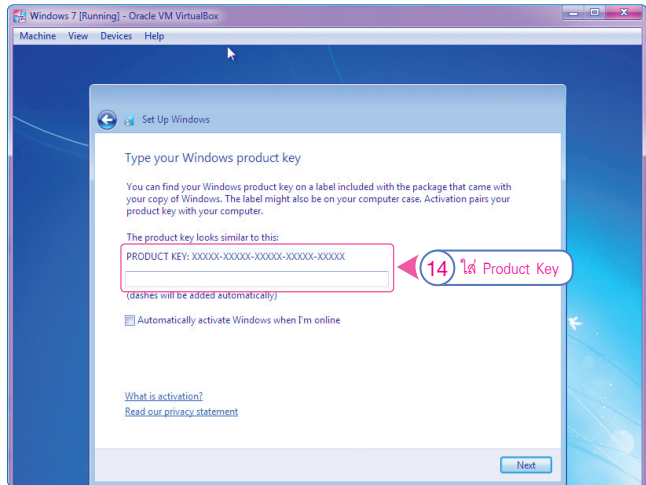
12. ตั้งชื่อบัญชีผู้ใช้งาน แล้วคลิกปุ่ม **Next**



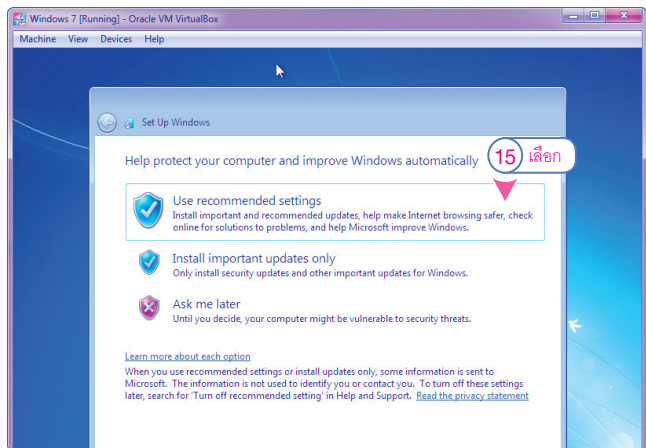
13. กำหนดรหัสผ่าน หรือ Password แล้วพิมพ์ซ้ำอีกครั้งหนึ่ง แล้วคลิกปุ่ม **Next** (ผู้อ่านอาจจะใส่คำไว้กำนลิมหรือ Hint ที่จำได้ง่ายในกรณีที่รหัสผ่านนั้นยากต่อการจดจำ)




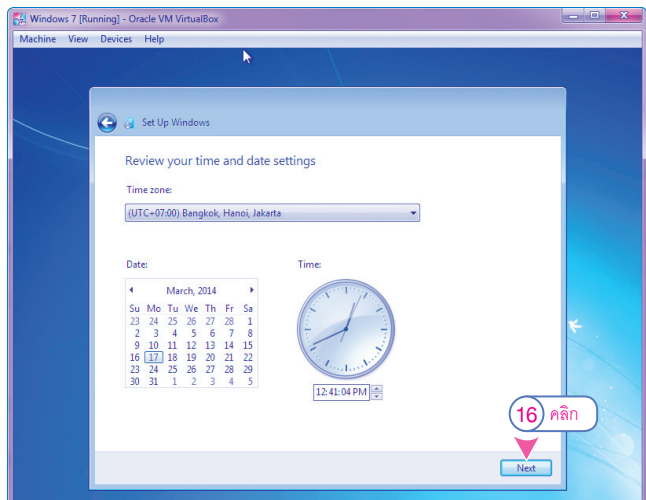
14. ใส่ Product Key แล้ว
คลิกปุ่ม 



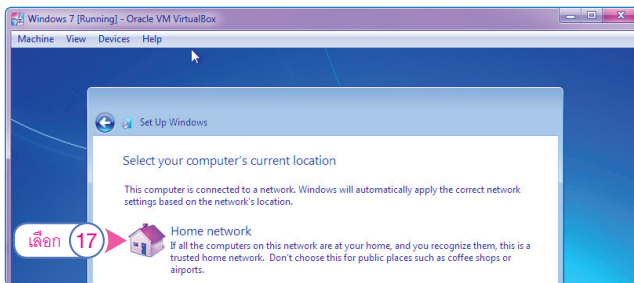
15. คลิกเลือก Use recommended settings (ทำตามที่ได้รับคำแนะนำจากระบบ)



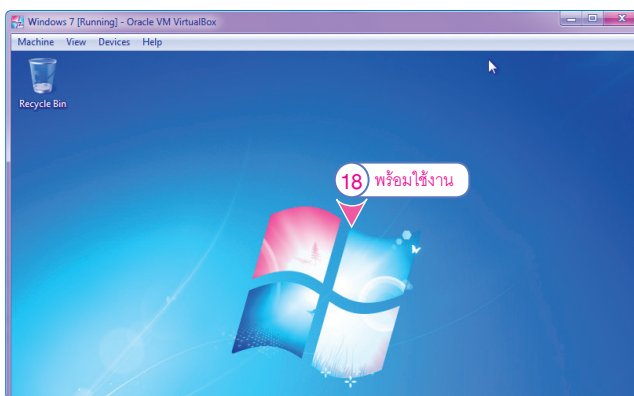
16. ปรับแต่งวันและเวลาสถานที่ แล้วคลิกปุ่ม 



17. ปรับแต่งค่าการเชื่อมต่อเครือข่าย โดยคลิกเลือก Home network



18. Windows 7 เริ่มทำงาน



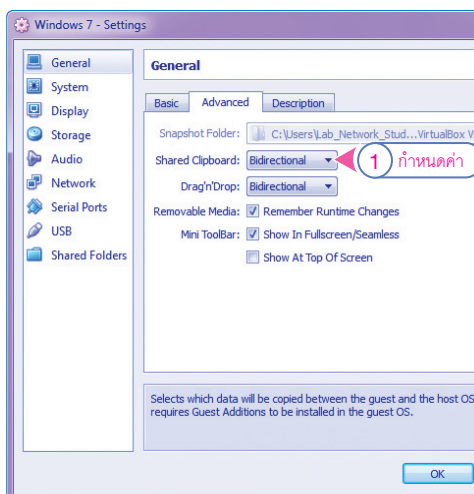
การปรับแต่ง Virtual Machine

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



NOTE

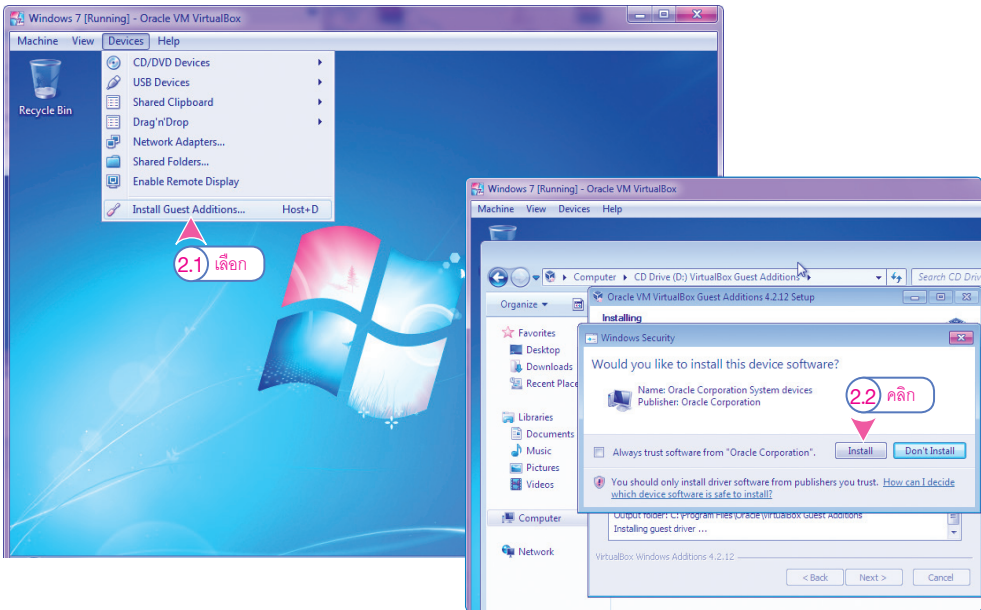
ผู้อ่านจะต้องตรวจสอบการเชื่อมต่อกับอินเทอร์เน็ตก่อนเสมอ เช่น ตรวจสอบสายสัญญาณที่ใช้งาน จะต้องเชื่อมกับเครือข่ายหลัก (Backbone) ของหน่วยงานหรือองค์กร มิใช่เพียงเชื่อมต่อกับอุปกรณ์ Hub หรือ Switch เท่านั้น หรือตรวจสอบ IP Address โดยใช้คำสั่ง C:\ipconfig หรือ C:\ping www.google.com เป็นต้น

1. ขั้นตอนแรกให้ผู้อ่านปรับแต่งที่หมวด General โดยเลือก Shared Clipboard เป็น Bidirectional ดังรูป แล้วคลิกปุ่ม

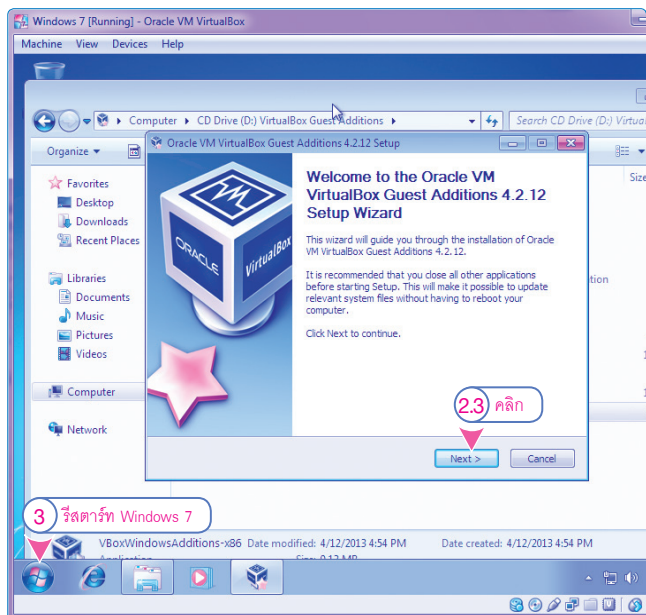


2. หากเกิดข้อผิดพลาด หรือ Invalid settings detected ซึ่งในส่วนนี้ให้ผู้อ่านติดตั้งเครื่องมือ VirtualBox-4.2.12-84980-Win.exe เพิ่มเติมดังรูปด้านล่าง

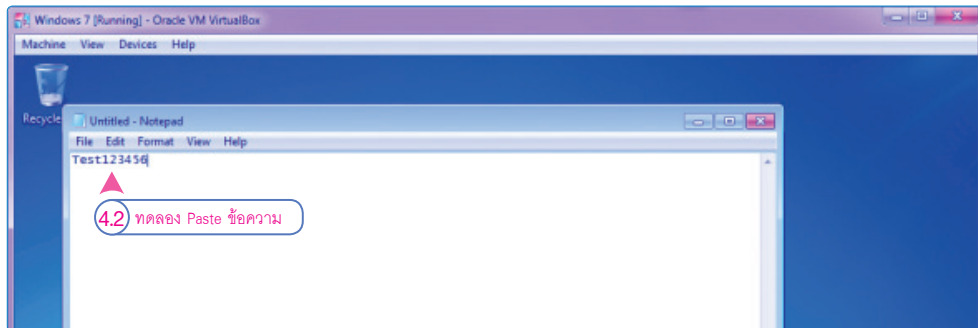
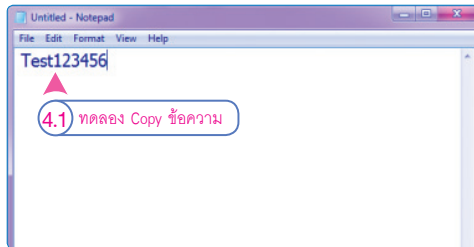
- ให้คลิกเมนู Devices > Install Guest Additions...
- ให้คลิกปุ่ม 
- ให้คลิกปุ่ม 



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

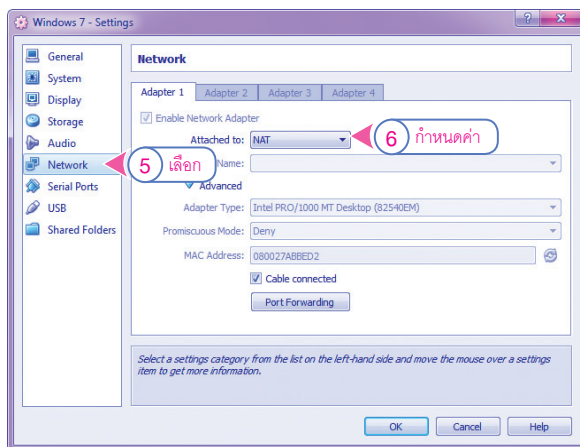


- เมื่อปรับแต่งรายละเอียดเสร็จสิ้นแล้ว ให้ทดลองคัดลอก (Copy) บน Clipboard จากเครื่องคอมพิวเตอร์หลักไปวาง (Paste) บน Virtual Machine และในทำนองกลับกันดังรูปด้านล่าง (เช่น กดปุ่ม **Ctrl** + **C** แล้วตามด้วยปุ่ม **Ctrl** + **V**)

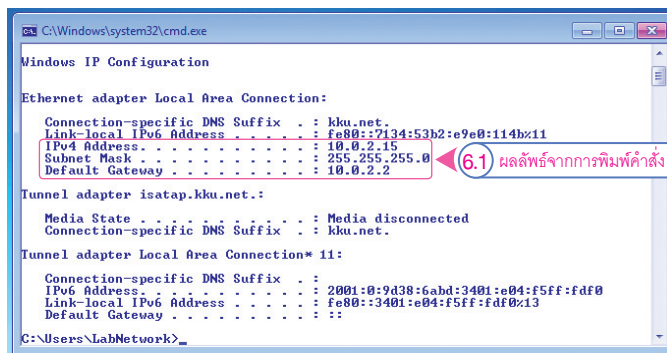


- ปรับแต่ง Virtual Machine ให้สามารถใช้งานเครือข่ายหรืออินเทอร์เน็ตได้ โดยผู้อ่านเข้าไปที่หัวข้อหมวด Network
- ให้ปรับค่า Attached to: เป็น NAT (Network Address Translation) แล้วคลิกปุ่ม

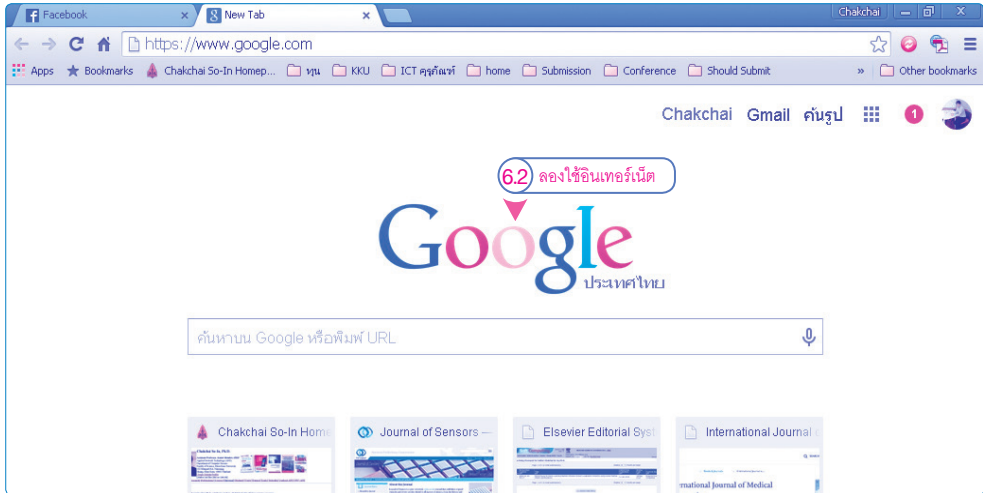
OK



- 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 โดยมีการปรับแต่งเครือข่ายเป็นรูปแบบเดียวกันกับเครื่องหลัก เช่น IP Address ในเครือข่ายวงเดียวกัน เป็นต้น ดังรูป (ในกรณีนี้เครื่องคอมพิวเตอร์หลักมี IP Address = 10.199.10.16 โดยที่เครื่องเสมือนคือ 10.199.10.17 และสามารถใช้อ IP Address นี้เพื่อเชื่อมต่ออินเทอร์เน็ตได้)

