

สารบัญ

	หน้า
สารบัญ	(6)
รายการตาราง.....	(11)
รายการภาพประกอบ	(18)
บทที่	
1 บทนำ	
1.1 ความสำคัญและที่มาของงานวิจัย.....	1
1.2 วัตถุประสงค์.....	2
1.3 ขอบเขตการวิจัย.....	2
1.4 ขั้นตอนการดำเนินงาน.....	2
1.5 ระยะเวลาในการดำเนินงาน	3
1.6 ประโยชน์ที่คาดว่าจะได้รับ.....	3
1.7 สถานที่ทำการวิจัย	3
1.8 เครื่องมือและอุปกรณ์ที่ใช้.....	4
1.8.1 ฮาร์ดแวร์	4
1.8.2 ซอฟต์แวร์.....	4
2 ทฤษฎี หลักการ งานวิจัยที่เกี่ยวข้อง และเครื่องมือที่ใช้	
2.1 ภัยคุกคาม.....	5
2.1.1 ภัยคุกคามแบ่งตามลักษณะของแหล่งที่มา	7
2.1.1.1 ภัยคุกคามจากธรรมชาติภัยคุกคามจากธรรมชาติ	7
2.1.1.2 ภัยคุกคามจากคน.....	7
2.1.1.2.1 ภัยคุกคามโดยไม่เจตนาหรือไม่ตั้งใจ.....	7
2.1.1.2.2 ภัยคุกคามที่มีเจตนาหรือตั้งใจกระทำ.....	8
2.1.2 ภัยคุกคามแบ่งตามลักษณะของการเข้าถึงและการใช้งาน	8
2.1.2.1 ระดับกายภาพ	9
2.1.2.2 ระดับเครือข่าย.....	9
2.1.2.3 ระดับโปรแกรมประยุกต์.....	9
2.1.2.4 ระดับผู้ใช้.....	10
2.2 การบุกรุก.....	10

สารบัญ (ต่อ)

	หน้า
2.2.1 ประเภทของการบุกรุก	10
2.2.1.1 การบุกรุกโดยใช้ผู้บุกรุกเป็นหลัก.....	10
2.2.1.1.1 solo attack	11
2.2.1.1.2 multi attack.....	12
2.2.1.2 การบุกรุกโดยใช้ระบบเป้าหมายเป็นหลัก	12
2.2.1.2.1 single target	13
2.2.1.2.2 multiple targets.....	13
2.2.1.2.3 network target	13
2.2.1.3 การบุกรุกโดยใช้เส้นทางในการบุกรุกเป็นหลัก.....	13
2.2.1.3.1 direct attack	13
2.2.1.3.2 indirect attack.....	13
2.2.1.4 การบุกรุกโดยใช้เจตนาในการบุกรุกเป็นหลัก	14
2.2.1.4.1 information theft.....	14
2.2.1.4.2 resource destruction	14
2.2.1.4.3 pre-attack.....	14
2.2.1.4.4 denial of service attack.....	14
2.2.1.5 การบุกรุกโดยใช้วิธีการในการบุกรุกเป็นหลัก	14
2.2.1.5.1 local attack	14
2.2.1.5.2 remote attack.....	14
2.2.2 วิธีการบุกรุก	14
2.2.2.1 การบุกรุกแบบพาสซีฟ.....	15
2.2.2.2 การบุกรุกแบบแอคทีฟ	15
2.3 ระบบตรวจจับการบุกรุก.....	17
2.3.1 ประเภทของระบบตรวจจับการบุกรุก	17
2.3.1.1 การใช้แหล่งข้อมูลในการตรวจสอบ.....	18
2.3.1.1.1 system data based IDS	18
2.3.1.1.2 network packet based IDS.....	18
2.3.1.2 การใช้ตัวให้ข้อมูล.....	19
2.3.1.2.1 single host based IDS.....	19

สารบัญ (ต่อ)

	หน้า
2.3.1.2.2 multi host based IDS.....	19
2.3.1.2.3 network based IDS.....	19
2.3.1.2.4 hybrid type of IDS.....	19
2.3.1.3 การใช้วิธีในการตรวจสอบ	20
2.3.1.3.1 anomaly based IDS	20
2.3.1.3.2 misuse based IDS	20
2.3.1.4 การใช้เวลาในการตรวจสอบ.....	21
2.3.1.4.1 real-time IDS	21
2.3.1.4.2 virtual real-time IDS	21
2.3.1.4.3 non real-time IDS	21
2.3.1.5 การใช้การตอบสนอง.....	21
2.3.1.5.1 active IDS.....	21
2.3.1.5.2 passive IDS.....	21
2.3.2 งานวิจัยที่เกี่ยวข้อง	21
2.3.2.1 ระบบตรวจจับการบุกรุกตามวิธีในการตรวจสอบ	22
2.3.2.2 ระบบตรวจจับการบุกรุกตามแหล่งข้อมูลในการตรวจสอบ.....	23
2.3.2.3 ระบบตรวจจับการบุกรุกตามตัวให้ข้อมูล.....	23
2.4 distributor ของระบบปฏิบัติการลินุกซ์	26
2.5 system call.....	26
2.6 การทำเหมืองข้อมูล	28
2.7 เครื่องมือที่นำมาใช้ในงานวิจัย	34
2.7.1 เครื่องมือแยกประเภทข้อมูล.....	34
2.7.2 เครื่องมือที่ใช้ทดสอบระบบตรวจจับการบุกรุก	38
2.8 สรุป	40
3 การวิเคราะห์และออกแบบระบบ	
3.1 ภาพรวมของระบบตรวจจับการบุกรุก.....	41
3.2 ข้อมูลนำเข้า	42
3.3 สถาปัตยกรรมของระบบตรวจจับการบุกรุก.....	43

สารบัญ (ต่อ)

	หน้า
3.4 ออกแบบข้อมูลฝึกสอนระบบ	43
3.5 ออกแบบโปรแกรมตรวจจับการบุกรุก.....	45
3.6 แผนภาพกระแสข้อมูลการทำงานของระบบตรวจจับการบุกรุก	47
3.7 สรุป	58
4 การพัฒนาระบบ	
4.1 โครงสร้างการดำเนินงาน	59
4.2 ขั้นตอนวิธี	61
4.3 การพัฒนาโปรแกรม.....	71
4.4 การพัฒนาข้อมูลฝึกสอนระบบเพื่อใช้งาน	75
4.5 เพิ่มข้อมูลหลักที่ระบบตรวจจับการบุกรุกใช้ในระหว่างการทำงาน.....	76
4.6 สารบบและเพิ่มข้อมูล	80
4.7 สรุป	83
5 การทดสอบระบบตรวจจับการบุกรุกและการปรับปรุง	
5.1 สภาพแวดล้อมในการทดสอบระบบตรวจจับการบุกรุก	84
5.2 การทดสอบระบบตรวจจับการบุกรุก	84
5.3 การปรับปรุงระบบตรวจจับการบุกรุกเพื่อใช้งานกับระบบปฏิบัติการ ในเวอร์ชันที่สูงขึ้น	116
5.4 กราฟแสดงผลการทดสอบ	147
5.5 ประสิทธิภาพ	153
5.6 สรุป.....	163
6 สรุปการวิจัยและข้อเสนอแนะ	
6.1 สรุปการวิจัยระบบตรวจจับการบุกรุก.....	165
6.2 การใช้งานระบบตรวจจับการบุกรุก.....	165
6.3 ปัญหาและข้อจำกัด	166
6.4 ข้อเสนอแนะ.....	167

สารบัญ (ต่อ)

	หน้า
บรรณานุกรม.....	169
ภาคผนวก.....	175
ก การปรับแต่งโปรแกรม boot loader.....	176
ข การกำหนดชื่อและหมายเลขซิสเต็มคอลในระบบปฏิบัติการลินุกซ์เรดแฮ็ท.....	179
ข.1 ระบบปฏิบัติการลินุกซ์เรดแฮ็ท 6.1.....	179
ข.2 ระบบปฏิบัติการลินุกซ์เรดแฮ็ท 7.0	181
ข.3 ระบบปฏิบัติการลินุกซ์เรดแฮ็ท 9.0	182
ค ทดสอบการทำงานของโปรแกรม TiMBL	184
ง ระบบตรวจจับการบุกรุกบน Fedora.....	185
จ โปรแกรมบุกรุกระบบที่ใช้ทดสอบการทำงานของระบบตรวจจับการบุกรุก	186
จ.1 ตัวอย่างโปรแกรมกลุ่ม denial of service.....	186
จ.2 ตัวอย่างโปรแกรมกลุ่ม root compromise	200
จ.3 ตัวอย่างโปรแกรมกลุ่ม miscellany	225
ประวัติผู้เขียน.....	236

รายการตาราง

ตาราง	หน้า
1.1 แสดงระยะเวลาดำเนินงาน	3
2.1 ชุดข้อมูลตัวอย่างฝึกสอน	30
2.2 ชุดข้อมูลทดสอบ	32
3.1 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.5	55
3.2 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.6	55
3.3 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.7	55
3.4 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.8	56
3.5 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.9	56
3.6 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.10	56
3.7 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.11	57
3.8 รายละเอียดการดำเนินงานของแต่ละกระบวนการในภาพประกอบ 3.12	57
4.1 อธิบายคำสั่งการแยกประเภทข้อมูล	73
5.1 รายละเอียดของระบบปฏิบัติการลินุกซ์เรดแฮทที่ใช้ในการทดสอบ	84
5.2 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ทดสอบวันที่ 14 พฤศจิกายน 2547 เวลา 13.21-14.46 น.	86
5.3 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ทดสอบวันที่ 14 พฤศจิกายน 2547 เวลา 10.10-11.54 น.	86
5.4 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดลองวันที่ 14 พฤศจิกายน 2547 เวลา 8.32-9.57 น.	87
5.5 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 15 พฤศจิกายน 2547 เวลา 8.42-23.18 น.	88
5.6 คำร้อยละของความถูกต้องจากผลการทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือบุกรุกระบบที่ได้เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ ในตาราง 5.2 ถึงตาราง 5.5	91
5.7 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service หลังปรับปรุงแฟ้มข้อมูลฝึกสอนระบบ ทดสอบวันที่ 17 พฤศจิกายน 2547 เวลา 13.12-14.34 น.	91

รายการตาราง (ต่อ)

ตาราง	หน้า
5.8 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 17 พฤศจิกายน 2547 เวลา 10.06-11.49 น.	92
5.9 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise หลังปรับปรุงเพิ่มข้อมูลฝึกสอนระบบ ทดสอบวันที่ 17 พฤศจิกายน 2547 เวลา 8.24-9.54 น.	93
5.10 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command หลังปรับปรุงเพิ่มข้อมูลฝึกสอนระบบ ทดสอบวันที่ 18 พฤศจิกายน 2547 เวลา 9.11-23.58 น.	94
5.11 คำร้อยละของความถูกต้องจากผลการทดสอบระบบตรวจจับการบุกรุก หลังปรับปรุงเพิ่มข้อมูลฝึกสอนระบบในตาราง 5.7 ถึงตาราง 5.10	96
5.12 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ทดสอบวันที่ 19 พฤศจิกายน 2547 เวลา 9.07-9.35 น.	97
5.13 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ทดสอบวันที่ 19 พฤศจิกายน 2547 เวลา 10.03-10.38 น.	97
5.14 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดสอบวันที่ 19 พฤศจิกายน 2547 เวลา 8.24-8.56 น.	97
5.15 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 19 พฤศจิกายน 2547 เวลา 13.08-22.46 น.	98
5.16 คำร้อยละของความถูกต้องจากผลการทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือบุกรุกระบบที่ไม่ได้เก็บพฤติกรรมการทำงานไว้ในเพิ่มข้อมูลฝึกสอนระบบในตาราง 5.12 ถึงตาราง 5.15	99
5.17 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ทดสอบวันที่ 24 เมษายน 2548 เวลา 11.41-13.09 น.	101
5.18 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ทดสอบวันที่ 24 เมษายน 2548 เวลา 15.15-16.54 น.	102
5.19 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดสอบวันที่ 24 เมษายน 2548 เวลา 8.43-10.06 น.	103

รายการตาราง (ต่อ)

ตาราง	หน้า
5.20 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 25 เมษายน 2548 เวลา 9.02-23.43 น.	104
5.21 คำร้อยละของความถูกต้องจากผลการทดสอบระบบตรวจจับการบุกรุกโดยใช้แฟ้มข้อมูลฝึกสอนระบบแบบใหม่ในตาราง 5.17 ถึงตาราง 5.20	106
5.22 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 27 เมษายน 2548 เวลา 9.33-10.52 น.	107
5.23 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 27 เมษายน 2548 เวลา 22.06-23.52 น.	107
5.24 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 27 เมษายน 2548 เวลา 14.10-15.27 น.	108
5.25 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 28 เมษายน 2548 เวลา 8.37-23.12 น.	109
5.26 คำร้อยละของความถูกต้องจากผลการทดสอบระบบตรวจจับการบุกรุกหลังจากปรับปรุงแฟ้มข้อมูลฝึกสอนระบบแบบใหม่ในตาราง 5.22 ถึงตาราง 5.25	112
5.27 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ทดสอบวันที่ 29 เมษายน 2548 เวลา 9.04-9.36 น.	112
5.28 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ทดสอบวันที่ 29 เมษายน 2548 เวลา 14.28-14.54 น.	113
5.29 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดสอบวันที่ 29 เมษายน 2548 เวลา 11.10-11.37 น.	113
5.30 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 30 เมษายน 2548 เวลา 9.07-17.49 น.	113
5.31 คำร้อยละของความถูกต้องจากผลการทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือบุกรุกระบบที่ไม่ได้เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบในตาราง 5.27 ถึงตาราง 5.30	115

รายการตาราง (ต่อ)

ตาราง	หน้า
5.32 เปรียบเทียบผลการทดสอบจากการใช้ข้อมูลฝึกสอนระบบแบบเก่ากับแบบใหม่ โดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ	115
5.33 เปรียบเทียบผลการทดสอบจากการใช้ข้อมูลฝึกสอนระบบแบบเก่ากับแบบใหม่ โดยใช้เครื่องมือบุกรุกระบบที่ไม่ได้เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ	116
5.34 แสดงรายละเอียดของระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 7.0 และเวอร์ชัน 9.0	116
5.35 การเรียกใช้งานซิสเต็มคอลลของคำสั่ง clear บนระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 6.1 เวอร์ชัน 7.0 และเวอร์ชัน 9.0	117
5.36 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 1 พฤษภาคม 2548 เวลา 15.12-16.27 น.	120
5.37 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 4 พฤษภาคม 2548 เวลา 21.17-22.53 น.	120
5.38 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 1 พฤษภาคม 2548 เวลา 13.07-14.49 น.	121
5.39 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 4 พฤษภาคม 2548 เวลา 13.55-15.41 น.	122
5.40 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 1 พฤษภาคม 2548 เวลา 9.43-11.29 น.	123
5.41 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 4 พฤษภาคม 2548 เวลา 9.36-11.27 น.	124

รายการตาราง (ต่อ)

ตาราง	หน้า
5.42 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 2 พฤษภาคม 2548 เวลา 8.43-23.36 น.	125
5.43 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 5 พฤษภาคม 2548 เวลา 8.18-23.12 น.	127
5.44 ค่าร้อยละของความถูกต้องก่อนปรับปรุงข้อมูลในแฟ้มข้อมูลฝึกสอนระบบ จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.36 ตาราง 5.38 ตาราง 5.40 และตาราง 5.42	129
5.45 ค่าร้อยละของความถูกต้องหลังปรับปรุงข้อมูลในแฟ้มข้อมูลฝึกสอนระบบ จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.37 ตาราง 5.39 ตาราง 5.41 และตาราง 5.43	129
5.46 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ทดสอบวันที่ 6 พฤษภาคม 2548 เวลา 8.36-9.12 น.	130
5.47 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ทดสอบวันที่ 6 พฤษภาคม 2548 เวลา 10.27-10.58 น.	130
5.48 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดสอบวันที่ 6 พฤษภาคม 2548 เวลา 13.42-14.16 น.	130
5.49 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 6 พฤษภาคม 2548 เวลา 14.23-23.08 น.	131
5.50 ค่าร้อยละของความถูกต้องโดยใช้เครื่องมือบุกรุกระบบที่ไม่ได้เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบในตาราง 5.46 ถึงตาราง 5.49	132
5.51 เปรียบเทียบผลการทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮท เวอร์ชัน 7.0 ก่อนและหลังปรับปรุงข้อมูลฝึกสอนระบบโดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ	133
5.52 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 7 พฤษภาคม 2548 เวลา 9.03-10.22 น.	134

รายการตาราง (ต่อ)

ตาราง	หน้า
5.53 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 10 พฤษภาคม 2548 เวลา 8.17-9.41 น.	134
5.54 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 7 พฤษภาคม 2548 เวลา 10.48-12.36 น.	135
5.55 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 10 พฤษภาคม 2548 เวลา 10.02-11.51 น.	136
5.56 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 7 พฤษภาคม 2548 เวลา 14.12-15.56 น.	137
5.57 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 10 พฤษภาคม 2548 เวลา 13.26-15.13 น.	138
5.58 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 8 พฤษภาคม 2548 เวลา 8.28-23.24 น.	139
5.59 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 11 พฤษภาคม 2548 เวลา 8.22-23.15 น.	141
5.60 คำร้อยละของความถูกต้องก่อนปรับปรุงข้อมูลในแฟ้มข้อมูลฝึกสอนระบบ จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.52 ตาราง 5.54 ตาราง 5.56 และตาราง 5.58	143
5.61 คำร้อยละของความถูกต้องหลังปรับปรุงข้อมูลในแฟ้มข้อมูลฝึกสอนระบบ จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.53 ตาราง 5.55 ตาราง 5.57 และตาราง 5.59	143
5.62 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ทดสอบวันที่ 12 พฤษภาคม 2548 เวลา 8.21-8.58 น.	144

รายการตาราง (ต่อ)

ตาราง	หน้า
5.63 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ทดสอบวันที่ 12 พฤษภาคม 2548 เวลา 9.12-9.42 น.	144
5.64 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดสอบวันที่ 12 พฤษภาคม 2548 เวลา 13.17-13.52 น.	144
5.65 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 12 พฤษภาคม 2548 เวลา 14.10-22.57 น.	145
5.66 คำร้อยละของความถูกต้องโดยใช้เครื่องมือบุกรุกระบบที่ไม่ได้เก็บพฤติกรรม การทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบในตาราง 5.62 ถึงตาราง 5.65	146
5.67 เปรียบเทียบผลการทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮท เวอร์ชัน 9.0 ก่อนและหลังปรับปรุงแฟ้มข้อมูลฝึกสอนระบบโดยใช้เครื่องมือ บุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ	147
5.68 ผลการทดสอบระบบตรวจจับการบุกรุกทั้งหมดบนระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 6.1	148
5.69 ผลการทดสอบระบบตรวจจับการบุกรุกทั้งหมดบนระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 7.0	149
5.70 ผลการทดสอบระบบตรวจจับการบุกรุกทั้งหมดบนระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 9.0	149
5.71 แสดงการใช้งานซีพียูและหน่วยความจำบนระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 6.1 ขณะที่ไม่มีระบบตรวจจับการบุกรุกทำงานกับขณะที่ ระบบตรวจจับการบุกรุกทำงานอยู่	155
5.72 แสดงการใช้งานซีพียูและหน่วยความจำบนระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 7.0 ขณะที่ไม่มีระบบตรวจจับการบุกรุกทำงานกับขณะที่ ระบบตรวจจับการบุกรุกทำงานอยู่	156
5.73 แสดงการใช้งานซีพียูและหน่วยความจำบนระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 9.0 ขณะที่ไม่มีระบบตรวจจับการบุกรุกทำงานกับขณะที่ ระบบตรวจจับการบุกรุกทำงานอยู่	157

รายการภาพประกอบ

ภาพประกอบ	หน้า	
2.1	เปรียบเทียบความสามารถในการโจมตีกับความรู้ทางเทคนิคของผู้บุกรุก	6
2.2	ประเภทของการบุกรุก	11
2.3	การโจมตีแบบ solo attack	12
2.4	การบุกรุกแบบ multi attack	12
2.5	การแยกประเภทระบบตรวจจับการบุกรุก	18
2.6	hybrid type of IDS	20
2.7	ตัวอย่างผลที่ได้จากการติดตามการทำงานของคำสั่ง ls ด้วยคำสั่ง strace	27
2.8	โครงสร้างต้นไม้การตัดสินใจ	30
2.9	ตัวอย่างต้นไม้การตัดสินใจ	31
2.10	สถาปัตยกรรมของระบบ MBL	35
2.11	เพิ่มข้อมูลที่เกี่ยวข้องกับการทำงานของ TiMBL	36
2.12	ตัวอย่างการทำงานช่วงที่ 1 ของโปรแกรม TiMBL	37
2.13	ตัวอย่างการทำงานช่วงที่ 2 ของโปรแกรม TiMBL	38
2.14	ตัวอย่างการทำงานช่วงที่ 3 ของโปรแกรม TiMBL	38
3.1	สถาปัตยกรรมของระบบตรวจจับการบุกรุก	43
3.2	แนวคิดการสร้างข้อมูลฝึกสอนระบบ	45
3.3	แนวคิดการทำงานของโปรแกรมตรวจจับการบุกรุก	47
3.4	แผนภาพบริบทของระบบตรวจจับการบุกรุก	48
3.5	DFD ระดับที่ 1 ของระบบตรวจจับการบุกรุก	49
3.6	DFD ระดับที่ 2 ของกระบวนการที่ 1 การติดตามการทำงานของเซลล์	50
3.7	DFD ระดับที่ 2 ของกระบวนการที่ 3 การรวบรวมเพิ่มข้อมูลการทำงานของโปรเซส	50
3.8	DFD ระดับที่ 2 ของกระบวนการที่ 4 การตรวจสอบเพิ่มข้อมูล	51
3.9	DFD ระดับที่ 2 ของกระบวนการที่ 5 การเปลี่ยนชื่อเพิ่มข้อมูลให้สัมพันธ์กับคำสั่งที่ถูกเรียกให้ทำงาน	51
3.10	DFD ระดับที่ 2 ของกระบวนการที่ 6 การนับความถี่ของซิสเต็มคอล	52
3.11	DFD ระดับที่ 2 ของกระบวนการที่ 7 การแยกประเภทการทำงานของโปรเซส	53
3.12	DFD ระดับที่ 2 ของกระบวนการที่ 8 การตอบโต้การบุกรุกและการรายงานผล	54
4.1	โครงสร้างระบบตรวจจับการบุกรุก	60
4.2	การทำงานของโปรแกรม find_shell	62

รายการภาพประกอบ (ต่อ)

ภาพประกอบ	หน้า
4.3 แสดงส่วนเริ่มต้นการทำงานของโปรแกรม monitor.pl	63
4.4 แสดงฟังก์ชัน check_file ของโปรแกรม monitor.pl	64
4.5 แสดงฟังก์ชัน rename_file ของโปรแกรม monitor.pl	65
4.6 แสดงฟังก์ชัน count_syscall ของโปรแกรม monitor.pl	66
4.7 แสดงการทำงานของโปรแกรม count-tool	66
4.8 แสดงฟังก์ชัน timbl_test ของโปรแกรม monitor.pl	68
4.9 แสดงฟังก์ชัน evidence ของโปรแกรม monitor.pl	70
4.10 ตัวอย่างรายงานผลการทำงานของ TiMBL ซึ่งเป็นข้อมูลที่เกิดจากการเปลี่ยนทิศทางการแสดงผลทางจอภาพมาเก็บไว้ในแฟ้มข้อมูล	74
4.11 รูปแบบการจัดเก็บข้อมูลในแฟ้มข้อมูลฝึกสอนระบบบนลินุกซ์เรดแฮท เวอร์ชัน 6.1	75
4.12 ตัวอย่างข้อมูลพฤติกรรมการทำงานของโปรเซสที่เก็บไว้ในแฟ้มข้อมูลฝึกสอนระบบบนลินุกซ์เรดแฮท เวอร์ชัน 6.1	76
4.13 ตัวอย่างข้อมูลที่จัดเก็บไว้ในแฟ้มข้อมูลเพื่อการตรวจสอบเส้นทาง	77
4.14 ตัวอย่างข้อมูลที่บันทึกไว้ในแฟ้มสัญลักษณ์การบุกรุก	78
4.15 ตัวอย่างข้อมูลที่บันทึกไว้ในแฟ้มหลักฐานการบุกรุก	79
4.16 สารบบและแฟ้มข้อมูลของระบบตรวจจับการบุกรุก	82
5.1 รูปแบบการเก็บข้อมูลในแฟ้มข้อมูลฝึกสอนระบบแบบใหม่	100
5.2 ตัวอย่างข้อมูลที่ถูกจัดเก็บไว้ในแฟ้มข้อมูลฝึกสอนระบบแบบเก็บข้อมูลที่เกิดขึ้นทั้งหมด	101
5.3 กราฟเปรียบเทียบความถูกต้องในการทำงานของระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮท เวอร์ชัน 6.1 ก่อนและหลังปรับปรุงข้อมูลฝึกสอนระบบแบบเก่า โดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ	150
5.4 กราฟเปรียบเทียบความถูกต้องในการทำงานของระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮท เวอร์ชัน 6.1 ก่อนและหลังปรับปรุงข้อมูลฝึกสอนระบบแบบใหม่ โดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ	150

รายการภาพประกอบ (ต่อ)

ภาพประกอบ	หน้า
5.5 กราฟเปรียบเทียบความถูกต้องในการทำงานของระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮท เวอร์ชัน 6.1 ก่อนปรับปรุงข้อมูลฝึกสอนระบบแบบเก่ากับแบบใหม่ โดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ	151
5.6 กราฟเปรียบเทียบความถูกต้องในการทำงานของระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮท เวอร์ชัน 6.1 หลังปรับปรุงข้อมูลฝึกสอนระบบแบบเก่ากับแบบใหม่ โดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ	151
5.7 กราฟเปรียบเทียบความถูกต้องในการทำงานของระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮท เวอร์ชัน 6.1 ระหว่างการใช้ข้อมูลฝึกสอนระบบแบบเก่ากับแบบใหม่ โดยใช้เครื่องมือบุกรุกระบบที่ไม่ได้เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ	152
5.8 กราฟเปรียบเทียบความถูกต้องในการทำงานของระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮท เวอร์ชัน 7.0 ก่อนและหลังปรับปรุงข้อมูลฝึกสอนระบบ โดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ	152
5.9 กราฟเปรียบเทียบความถูกต้องในการทำงานของระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮท เวอร์ชัน 9.0 ก่อนและหลังปรับปรุงข้อมูลฝึกสอนระบบ โดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ	153
5.10 กราฟแสดงการใช้งานซีพียูในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่ กับในกรณีที่ไม่มีระบบตรวจจับการบุกรุกทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 6.1	158
5.11 กราฟแสดงการใช้งานหน่วยความจำในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่ กับในกรณีที่ไม่มีระบบตรวจจับการบุกรุกทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 6.1	159
5.12 กราฟแสดงการใช้งานซีพียูในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่ กับในกรณีที่ไม่มีระบบตรวจจับการบุกรุกทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 7.0	160

รายการภาพประกอบ (ต่อ)

ภาพประกอบ	หน้า
5.13 กราฟแสดงการใช้งานหน่วยความจำในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในกรณีที่ไม่มีระบบตรวจจับการบุกรุกทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 7.0	161
5.14 กราฟแสดงการใช้งานซีพียูในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในกรณีที่ไม่มีระบบตรวจจับการบุกรุกทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 9.0	162
5.15 กราฟแสดงการใช้งานหน่วยความจำในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในกรณีที่ไม่มีระบบตรวจจับการบุกรุกทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 9.0	163
ก.1 การแบ่งส่วนของฮาร์ดดิสก์ในการทำวิทยานิพนธ์	176
ก.2 รายละเอียดในแฟ้ม /etc/grub.conf ของลินุกซ์เรดแฮท เวอร์ชัน 9.0	178
ข.1 ชื่อและหมายเลขซีสเต็มคอลลของระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 6.1	179
ข.2 ชื่อและหมายเลขซีสเต็มคอลลของระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 7.0	181
ข.3 ชื่อและหมายเลขซีสเต็มคอลลของระบบปฏิบัติการลินุกซ์เรดแฮท เวอร์ชัน 9.0	182