

สารบัญ

	หน้า
สารบัญ	(6)
รายการตาราง.....	(9)
รายการภาพประกอบ.....	(10)
บทที่	
1 บทนำ	
1.1 ความสำคัญและที่มาของหัวข้อวิจัย	1
1.2 การตรวจเอกสาร.....	2
1.3 วัตถุประสงค์.....	3
1.4 ขอบเขตของการวิจัย	3
1.5 ขั้นตอนและวิธีดำเนินการวิจัย.....	4
1.6 ระยะเวลาดำเนินงาน	4
1.7 เครื่องมือและอุปกรณ์ที่ใช้ในการทำวิจัย	5
1.8 ประโยชน์ที่คาดว่าจะได้รับ	5
2 ภัยคุกคามและการโจมตี	
2.1 บทนำ.....	6
2.2 ภัยคุกคามและการโจมตี.....	6
2.3 Active Attack.....	8
2.4 Passive Attack	20
2.5 สรุป	23
3 ระบบตรวจจับการบุกรุก	
3.1 บทนำ.....	24
3.2 ระบบตรวจจับการบุกรุก	24
3.3 ความจำเป็นที่จะต้องใช้ระบบตรวจจับการบุกรุก	25
3.4 องค์ประกอบสำหรับระบบตรวจจับการบุกรุก	25
3.5 ประเภทของระบบตรวจจับการบุกรุก	26
3.6 แนวทางในการตรวจจับการบุกรุก.....	31
3.7 คุณลักษณะของระบบตรวจจับการบุกรุกที่ดี	39
3.8 Audit Trail	40
3.9 C2 Audit.....	41
3.10 ขั้นตอนในการวิเคราะห์ข้อมูลลึอก.....	42

สารบัญ (ต่อ)

	หน้า
3.11 เครื่องมือที่ใช้ในการวิเคราะห์ล็อก	43
3.12 สรุป	45
4 การวิเคราะห์และออกแบบระบบ	
4.1 บทนำ	46
4.2 ล็อกไฟล์ในระบบปฏิบัติการยูนิกซ์	46
4.3 องค์ประกอบของระบบตรวจจับการบุกรุก	53
4.4 การเก็บรวบรวมข้อมูลล็อก	62
4.5 สรุป	64
5 การพัฒนาระบบ	
5.1 บทนำ	65
5.2 ภาษาที่ใช้ในการพัฒนา	65
5.3 แผนภาพโดยรวมของการพัฒนาโปรแกรม	65
5.4 ฟังก์ชันรับตัวเลือกการทำงานของโปรแกรม	66
5.5 ฟังก์ชันการทำงานในลักษณะ daemon process	67
5.6 การพัฒนาโปรแกรมส่วน Analysis Module	69
5.7 การพัฒนาโปรแกรมส่วน Response Module	75
5.8 การสร้างกฎเพื่อใช้สำหรับการทำงานของโปรแกรม	76
5.9 สรุป	92
6 การทดสอบระบบตรวจจับการบุกรุก	
6.1 บทนำ	93
6.2 สภาพแวดล้อมและเครือข่ายที่ใช้ทดสอบระบบตรวจจับการบุกรุก	93
6.3 การทดสอบระบบตรวจจับการบุกรุก	94
6.4 ผลการทดสอบระบบตรวจจับการบุกรุก	103
6.5 การทดสอบประสิทธิภาพของระบบ	104
6.6 ผลการศึกษาเพื่อวิเคราะห์หาระดับของการบันทึกเหตุการณ์ของ syslog	106
6.7 สรุป	114
7 บทสรุปและข้อเสนอแนะ	
7.1 สรุปผลการวิจัย	115
7.2 ปัญหาและอุปสรรคในการวิจัย	117
7.3 ข้อเสนอแนะ	117

สารบัญ (ต่อ)

	หน้า
บรรณานุกรม	119
ภาคผนวก	123
ก กฎที่ใช้ตรวจจับการบุกรุก	124
ข นิยามคำศัพท์.....	127
ประวัติผู้เขียน.....	130

รายการตาราง

ตาราง	หน้า
4.1 แสดงรายละเอียด facility ต่าง ๆ ของ syslog	48
4.2 แสดง priority ต่าง ๆ ของ syslog (เรียงค่า priority จากมากไปหาน้อย)	49
5.1 ตัวเลือกการทำงานของโปรแกรม	67
6.1 แสดงผลการทดสอบระบบตรวจจับการบุกรุก	104
6.2 ตารางการใช้ทรัพยากรของระบบตรวจจับโดยใช้คำสั่ง top ในกรณีที่ไม่มีฟังก์ชันการกรองและกฎการตรวจจับ	104
6.3 ตารางการใช้ทรัพยากรของระบบตรวจจับโดยใช้คำสั่ง top เมื่อมีกฎการกรองจำนวน 25 ข้อ และกฎการตรวจจับจำนวน 15 ข้อ	105
6.4 ตารางการใช้ทรัพยากรของระบบตรวจจับโดยใช้คำสั่ง top เมื่อมีกฎการกรองจำนวน 50 ข้อ และกฎการตรวจจับจำนวน 30 ข้อ	105
6.5 ตารางการใช้ทรัพยากรของระบบตรวจจับโดยใช้คำสั่ง top เมื่อมีกฎการกรองจำนวน 50 ข้อ และกฎการตรวจจับจำนวน 30 ข้อ เมื่อเวลาผ่านไประยะเวลาหนึ่ง	105
6.6 แสดงข้อมูลบริการต่าง ๆ และโปรแกรมที่ทำงานบนเครื่อง ratree.psu.ac.th	106
6.7 การใช้พื้นที่ในเก็บล็อกของแต่ละวันที่โดยจำแนกตามระดับความสำคัญเหตุการณ์	107
6.8 การใช้พื้นที่ในการเก็บล็อกในแต่ละวันของเครื่อง ratree	111
6.9 แสดงปริมาณการใช้พื้นที่ก่อนและหลังเปลี่ยนแปลงค่าในไฟล์ syslog.conf	113
6.10 แสดงวิธีการโจมตีและระดับ facility และ priority ที่เกิดร่องรอยการบุกรุก	113

รายการภาพประกอบ

ภาพประกอบ	หน้า
2.1 แผนภาพแสดงลักษณะการโจมตี	7
3.1 องค์ประกอบระบบตรวจจับการบุกรุก	26
3.2 แสดงโอกาสที่เกิดเหตุการณ์ต่าง ๆ	34
3.3 ขั้นตอนในการวิเคราะห์ล็อก	42
4.1 องค์ประกอบระบบตรวจจับการบุกรุกที่พัฒนา	53
4.2 องค์ประกอบและขั้นตอนการทำงานของส่วน Analysis Module	55
4.3 ขั้นตอนการทำงานของ Read Logfile Process	56
4.4 ขั้นตอนการทำงานของ Prefiltering Process	57
4.5 ขั้นตอนการทำงานของ Misuse Detection Engine	60
4.6 ขั้นตอนการทำงานของ Response Process	61
4.7 แผนภาพการเก็บรวบรวมข้อมูลล็อกจากเครื่อง ratree.psu.ac.th	62
5.1 แผนภาพรวมของการพัฒนาโปรแกรม	66
5.2 การเก็บข้อมูลในตัวแปรอาร์เรย์ filter_rules	70
5.3 ตัวอย่างการเก็บข้อมูลในตัวแปรอาร์เรย์ filter_rules	70
5.4 ลักษณะการเก็บข้อมูลกฎการตรวจจับในตัวแปรอาร์เรย์ต่าง ๆ	72
5.5 ลักษณะการเก็บข้อมูลเหตุการณ์ในตัวแปรอาร์เรย์ events_list	72
5.6 ตัวอย่างการเก็บข้อมูลเหตุการณ์ในตัวแปรอาร์เรย์ events_list (1)	74
5.7 ตัวอย่างการเก็บข้อมูลเหตุการณ์ในตัวแปรอาร์เรย์ events_list (2)	75
5.8 ตัวอย่างการเก็บข้อมูลเหตุการณ์ในตัวแปรอาร์เรย์ events_list (3)	75
5.9 เครื่องข่ายที่สร้างขึ้นเพื่อทดสอบการบุกรุก	76
5.10 แผนภาพการทดสอบการโจมตีด้วยไวรัส	80
5.11 แผนภาพการทดสอบการโจมตีด้วยโทรจัน	82
5.12 จอภาพการทำงานของโปรแกรม BOPing 2.00	83
5.13 แผนภาพการทดสอบการโจมตีแบบ DoS	84
5.14 จอภาพการทำงานของโปรแกรม ICMP Bomber	84
5.15 แผนภาพการทดสอบการโจมตีแบบ SYN Flood	85
5.16 แผนภาพการโจมตีแบบ Brute-force attack	86
5.17 จอภาพการทำงานของโปรแกรม Brutus	87
6.1 เครื่องข่ายที่สร้างขึ้นเพื่อทดสอบการทำงานของระบบที่พัฒนา	93
6.2 จอภาพการทำงานของโปรแกรม BoClient	96

รายการภาพประกอบ (ต่อ)

ภาพประกอบ	หน้า
6.3 จอภาพการทำงานของโปรแกรม Brutus	99
6.4 จอภาพการทำงานของโปรแกรม GFI LANguard Network Security Scanner	102
6.5 พื้นที่ในเก็บล็อกของแต่ละวันที่โดยจำแนกตามระดับความสำคัญเหตุการณ์	108
6.6 สัดส่วนการใช้พื้นที่ในการเก็บล็อกของแต่ละโปรแกรม	109