

สารบัญ

	หน้า
กิตติกรรมประกาศ	ก
บทคัดย่อภาษาไทย	ง
บทคัดย่อภาษาอังกฤษ	จ
สารบัญตาราง	ช
สารบัญภาพ	ฉ
บทที่ 1 บทนำ	
1.1 หลักการและเหตุผล	1
1.2 วัตถุประสงค์ของการศึกษา	2
1.3 ประโยชน์ที่ได้รับ	2
1.4 นิยามศัพท์เฉพาะ	2
1.5 เครื่องมือที่ใช้ในการศึกษา	3
1.6 ขอบเขต และวิธีศึกษา	4
บทที่ 2 เอกสารและทฤษฎีที่เกี่ยวข้อง	
2.1 ความสำคัญของการรักษาความปลอดภัยสำหรับระบบเครือข่ายคอมพิวเตอร์	5
2.2 หลักการพื้นฐานของระบบรักษาความปลอดภัยข้อมูล	5
2.3 กำเนิดของเครือข่ายอินเทอร์เน็ต	7
2.4 ประเด็นที่เกี่ยวข้องกับเรื่องความปลอดภัยและประเภทของการละเมิดบนเครือข่าย	12
2.5 แนวโน้มการบุกรุกบนระบบเครือข่ายคอมพิวเตอร์ในอนาคต	14
2.6 ช่องโหว่ของอินเทอร์เน็ต (Internet Vulnerabilities)	20
2.7 ขั้นตอนที่ผู้บุกรุกมักใช้ในการบุกรุกเข้าสู่ระบบคอมพิวเตอร์	21
2.8 เทคโนโลยีที่เกี่ยวข้องกับการรักษาความปลอดภัยในเครือข่ายคอมพิวเตอร์	24
2.9 หลักการพื้นฐานของโปรโตคอล TCP/IP	33
บทที่ 3 การศึกษาและออกแบบระบบตรวจสอบการบุกรุกระบบเครือข่าย	
3.1 ขอบเขตการศึกษา	38
3.2 ขั้นตอนการศึกษา	38

สารบัญ (ต่อ)

	หน้า
3.3 ออกแบบแผนผังระบบตรวจจับการบุกรุก ภายในเครือข่าย มหาวิทยาลัยราชภัฏเชียงราย	67
3.4 สถานที่ที่ใช้ในการดำเนินการศึกษาและรวบรวมข้อมูล	76
3.5 ระยะเวลาในการศึกษา	76
บทที่ 4 รายงานผลการศึกษา	
4.1 ระบบเครือข่ายที่ใช้ในการสร้างและทดสอบผล	78
4.2 ส่วนประกอบของระบบตรวจจับการบุกรุกเครือข่าย	78
4.3 รายละเอียดและข้อมูลการบุกรุกที่ตรวจจับได้	79
บทที่ 5 บทสรุป	
5.1 สรุปผล	82
5.2 ปัญหาและอุปสรรค	82
5.3 ข้อจำกัดของระบบ	83
5.4 ข้อเสนอแนะ	83
บรรณานุกรม	85
ภาคผนวก	
ภาคผนวก ก การติดตั้งระบบ	88
ภาคผนวก ข คู่มือการใช้งานโปรแกรม	95
ภาคผนวก ค ส่วนประกอบต่างๆ ในส่วนหัวของแพ็คเกจและพจนานุกรมข้อมูล	112
ประวัติผู้เขียน	129

สารบัญตาราง

ตาราง	หน้า
2.1 การเปรียบเทียบข้อดีข้อเสียในการเลือกอุปกรณ์มาทำหน้าที่ Packet	28
2.2 สถานะในการรับส่งของโปรโตคอล TCP	38
3.1 Preprocessors ประเภทอื่นๆ	45
3.2 CIDR Block Addressing	48
3.3 Flow Control ออปชัน	52
3.4 Snort IP ออปชัน	54
3.5 Snort TCP Flags	56
3.6 ช่วง Snort ID	58
3.7 ประเภทความเสี่ยงสูง (ค่า Priority 1)	58
3.8 ประเภทความเสี่ยงปานกลาง (ค่า Priority 2)	59
3.9 ประเภทความเสี่ยงต่ำ (ค่า Priority 3)	59
3.10 อาร์กิวเมนต์ที่ใช้ร่วมกับคีย์เวิร์ด tag	61
3.11 อาร์กิวเมนต์ที่ใช้ร่วมกับคีย์เวิร์ด resp	61
3.12 ตารางข้อมูลของสเนอร์ที่ในการจัดเก็บข้อมูลการบุกรุก	73
3.13 ตารางข้อมูลที่ได้ออกแบบเพิ่มเติมสำหรับจัดการเรื่องกฎการตรวจสอบ	73
4.1 ผลการตรวจจับรูปแบบการบุกรุกเครือข่าย	80
4.2 กลุ่มการแจ้งเตือนที่ตรวจพบ	81
ค.1 IP Packet Header Fields	112
ค.2 ICMP Packet Header Fields	114
ค.3 TCP Packet Header Fields	115
ค.4 UDP Packet Header Fields	117
ค.5 พจนานุกรมข้อมูลในฐานข้อมูล snort	117

สารบัญภาพ

รูป	หน้า
1.1 แสดงหลักการทำงานของ ระบบการตรวจจับการบุกรุกแบบเครือข่าย	2
2.1 แสดงการเชื่อมต่อเข้าสู่เครือข่ายอินเทอร์เน็ตในยุคแรก	8
2.2 แสดงลำดับเหตุการณ์ที่เกี่ยวข้องกับเรื่องความปลอดภัยในเครือข่ายอินเทอร์เน็ตปี 1988	9
2.3 แสดงโครงสร้างของอินเทอร์เน็ตในวันที่ 16 สิงหาคม 2541	10
2.4 แสดงการเชื่อมโยงในเครือข่ายอินเทอร์เน็ตปัจจุบัน	11
2.5 แสดงรายงานเรื่องจำนวนช่องโหว่ต่างๆ ที่ค้นพบในช่วงปี 1995-2003	15
2.6 แสดงจำนวนเหตุการณ์การเกี่ยวเรื่องความปลอดภัยในเครือข่ายอินเทอร์เน็ต	16
2.7 แสดงขั้นตอนหลักในการบุกรุกเข้าสู่ระบบ	24
2.8 แสดงไฟร์วอลล์กั้นระหว่างอินเทอร์เน็ตกับเครือข่ายภายใน	26
2.9 แสดงRouter ทำหน้าที่ Packet Filtering	26
2.10 แสดงใช้ Dual-homed Host เป็น Proxy Server	29
2.11 โมเดล OSI	34
2.12 โมเดล Internet Reference TCP/IP	35
2.13 แสดงลำดับและสถานะต่างๆของโปรโตคอล TCP ในการเริ่มต้นและสิ้นสุดการเชื่อมต่อ	38
3.1 ภาพแสดงการทำงานส่วนประกอบหลักของโปรแกรม Snort	40
3.2 ภาพแสดงการทำงานของโปรแกรม Snort เทียบกับโมเดล OSI	41
3.3 โครงสร้างหลักของกฎในโปรแกรม Snort	46
3.4 โครงสร้างส่วนประกอบย่อยของ Rule Header	46
3.5 แสดงโครงสร้างเครือข่ายมหาวิทยาลัยราชภัฏเชียงใหม่	66
3.6 แสดงโครงสร้างการทำงานของระบบการตรวจจับการบุกรุกเครือข่าย	68
3.7 แสดงตำแหน่งของเซ็นเซอร์ในเครือข่ายของสำนักบริการเทคโนโลยีสารสนเทศ	70
3.8 แสดงตำแหน่งของ Sensor ในเครือข่ายสำนักทะเบียนและประมวลผลและอาคารเทคโนโลยีและนวัตกรรมการศึกษา	71
3.9 แสดงโครงสร้างของฐานข้อมูลที่เซ็นเซอร์ใช้จัดเก็บ	72
3.10 แผนภาพการไหลของข้อมูล (Flow-chart) ของการจัดการเรื่องกฎ	76
ข.1 โครงสร้างหลักของระบบแสดงผลทางสถิติและการจัดการเรื่องกฎ	95
ข.2 แสดงหน้าจอถือคอินเพื่อเข้าสู่ระบบ	96

สารบัญภาพ (ต่อ)

รูป	หน้า
ข.3 แสดงหน้าจอหลักของระบบการติดต่อผู้ใช้	97
ข.4 แสดงหน้าจอหลักของการรายงานผลการบุกรุกเครือข่าย	98
ข.5 แสดงข้อมูลการตรวจจับจากเครื่องเซ็นเซอร์ที่กำหนดไว้	99
ข.6 แสดงข้อมูลรายการแจ้งเตือนที่เซ็นเซอร์ตรวจพบ	100
ข.7 แสดงรายการผลการแจ้งเตือนล่าสุด 15 รายการ	101
ข.8 แสดงรายละเอียดของข้อมูลของการบุกรุกแต่ละรายการ	102
ข.9 แสดงข้อมูลสรุปของเครื่องคอมพิวเตอร์ที่ทำผิดกฎในการตรวจสอบ	103
ข.10 แสดงหน้าจอหลักในการจัดการเซ็นเซอร์	104
ข.11 แสดงหน้าจอการลงทะเบียนเซ็นเซอร์	105
ข.12 แสดงข้อมูลตัวแปรไฟล์ snort.conf ของเซ็นเซอร์	106
ข.13 แสดงสถานะของ preprocessor	107
ข.14 แสดงรายการ preprocessor ที่มีอยู่โดยสามารถแก้ไข หรือ เพิ่มข้อมูลได้	108
ข.15 แสดงการกำหนด output log	109
ข.16 แสดงกฎที่มีการเลือกใช้ในการตรวจสอบ	109
ข.17 แสดงหน้าจอรายละเอียดของกฎต่างๆ ที่มีอยู่ทั้งหมดของเซ็นเซอร์	110
ข.18 แสดงการแก้ไขกฎ	111
ค.1 IP Packet Header	112
ค.2 Basic ICMP Packet Header	114
ค.3 ICMP Packet Header used in ping command	114
ค.4 TCP Packet Header	115
ค.5 UDP Packet Header	116