

สารบัญ

	หน้า
กิตติกรรมประกาศ	ก
บทคัดย่อภาษาไทย	ง
บทคัดย่อภาษาอังกฤษ	ฉ
สารบัญตาราง	ช
สารบัญภาพ	ฅ
บทที่ 1 บทนำ	1
1.1 หลักการและเหตุผล	1
1.2 วัตถุประสงค์ของการศึกษา	2
1.3 ประโยชน์ที่คาดว่าจะได้รับ	2
1.4 ขอบเขตและวิธีการศึกษา	2
1.5 สถานที่ที่ใช้ในการศึกษาและรวบรวมข้อมูล	4
บทที่ 2 เอกสารและทฤษฎีที่เกี่ยวข้อง	5
2.1 หลักการพื้นฐานของระบบรักษาความปลอดภัยข้อมูลบนอินเทอร์เน็ต	5
2.2 ทำไมจึงต้องสนใจการรักษาความปลอดภัย	7
2.3 ประวัติและที่มาของปัญหา	7
2.4 ความปลอดภัยบนระบบเครือข่าย	10
2.5 ชนิดของเหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์และเครือข่าย	10
2.6 แนวโน้มการบุกรุกบนระบบเครือข่าย	12
2.7 ความล่อแหลมบนอินเทอร์เน็ต	15
2.8 ขั้นตอนหลักในการบุกรุกเข้าสู่ระบบ	21
2.9 รูปแบบในการบุกรุก	23
2.10 เทคโนโลยีการรักษาความปลอดภัย	24
2.11 หลักการของโปรโตคอล TCP/IP	34
บทที่ 3 การศึกษาและวิเคราะห์ระบบตรวจสอบและป้องกันการบุกรุกระบบเครือข่าย	40
3.1 ระบบตรวจสอบผู้บุกรุกระบบเครือข่าย	40
3.2 ระบบรักษาความปลอดภัย	69

3.3 ส่วนประสานการทำงานระบบตรวจสอบผู้บุกรุกเครือข่าย และระบบรักษาความปลอดภัยไฟร์วอลล์	81
3.4 ส่วนแสดงผลและสืบค้นข้อมูล	85
บทที่ 4 การออกแบบและพัฒนาระบบป้องกันและตรวจสอบการบุกรุกระบบเครือข่าย	95
4.1 สถาปัตยกรรมการวางระบบป้องกันและตรวจสอบผู้บุกรุกบนระบบเครือข่าย	95
4.2 ระบบเครือข่ายที่ทำการทดลอง	97
4.3 สรุปข้อมูลการบุกรุกที่เกิดขึ้น	100
4.4 การกำหนดเกณฑ์การป้องกัน	101
บทที่ 5 บทสรุป	103
5.1 สรุปผล	103
5.2 ปัญหาและอุปสรรค	104
5.3 ข้อจำกัดของระบบ	104
5.4 ข้อเสนอแนะ	105
บรรณานุกรม	106
ภาคผนวก	
ภาคผนวก ก การติดตั้งระบบ	108
ภาคผนวก ข ส่วนประกอบต่างๆในส่วนหัวของแพ็กเก็ต	116
ประวัติผู้เขียน	122

สารบัญตาราง

ตาราง	หน้า
2.1 เปรียบเทียบข้อดีข้อเสียในการเลือกอุปกรณ์มาทำหน้าที่ Packet Filtering	26
2.2 แสดง Flag การทำงานของโปรโตคอล TCP ที่สถานะต่างๆ	39
3.1 Preprocessors ประเภทอื่นๆ	47
3.2 CIDR Block Addressing	50
3.3 Flow Control ออปชัน	54
3.4 Snort IP ออปชัน	55
3.5 Snort TCP Flags	57
3.6 ช่วง Snort ID	59
3.7 ประเภทความเสี่ยงสูง (ค่า Priority 1)	60
3.8 ประเภทความเสี่ยงปานกลาง (ค่า Priority 2)	60
3.9 ประเภทความเสี่ยงต่ำ (ค่า Priority 3)	61
3.10 อาร์กิวเมนต์ที่ใช้ร่วมกับคีย์เวิร์ด tag	62
3.11 อาร์กิวเมนต์ที่ใช้ร่วมกับคีย์เวิร์ด resp	63
3.12 แสดงรายละเอียดของ ICMP message	75
4.1 เกณฑ์การป้องกันภัย ประเภทความเสี่ยงสูง	101
4.2 เกณฑ์การป้องกันภัย ประเภทความเสี่ยงปานกลาง	101
ข.1 IP Packet Header Fields	116
ข.2 ICMP Packet Header Fields	118
ข.3 TCP Packet Header Fields	119
ข.4 UDP Packet Header Fields	121

สารบัญภาพ

รูป	หน้า
2.1 แสดงขั้นตอนหลักในการบุกรุกเข้าสู่ระบบ	22
2.2 แสดงไฟร์วอลล์กั้นระหว่างอินเทอร์เน็ตกับเครือข่ายภายใน	24
2.3 แสดงใช้ Screening Router ทำหน้าที่ Packet Filtering	25
2.4 แสดงใช้ Dual-homed Host เป็น Proxy Server	27
2.5 แสดงการทำงานของระบบตรวจจับการบุกรุก	32
2.6 โมเดล OSI	35
2.7 โมเดล Internet Reference TCP/IP	36
2.8 แสดงลำดับและสถานะต่างๆของโปรโตคอล TCP ในการเริ่มต้นและสิ้นสุดการเชื่อมต่อ	38
3.1 ภาพแสดงการทำงานส่วนประกอบหลักของโปรแกรม Snort	41
3.2 ภาพแสดงการทำงานของโปรแกรม Snort เทียบกับ โมเดล OSI	42
3.3 โครงสร้างหลักของกฎในโปรแกรม Snort	49
3.4 โครงสร้างส่วนประกอบย่อยของ Rule Header	49
3.5 หน้าหลักของโปรแกรม ACID (ACID Main Page)	86
3.6 ตัวอย่างการแสดงรายละเอียดข้อมูลการบุกรุกแยกประเภทตามรูปแบบการบุกรุก	87
3.7 ตัวอย่างการแสดงรายละเอียดข้อมูลการบุกรุกแต่ละรูปแบบ	87
3.8 ตัวอย่างการแสดงรายละเอียดข้อมูลการบุกรุกภายในแฟ้มเก็บ	88
3.9 แสดงรายละเอียดพารามิเตอร์ต่างๆที่ใช้ในการค้นหา	89
3.10 ตัวอย่างแสดงการค้นหาการบุกรุกที่เป็นรูปแบบ DDOS	89
3.11 ตัวอย่างแสดงผลลัพธ์การค้นหาการบุกรุกที่มีรูปแบบ DDOS	90
3.12 ตัวอย่างแสดงการใช้บริการ Local Whois ค้นหาข้อมูล ไอพี 80.0.48.8	90
3.13 ตัวอย่างการใช้งาน Alert Group	91
3.14 ตัวอย่างการใช้งานส่วนจัดการข้อมูล	91
3.15 ตัวอย่างการส่งอีเมลโดยระบุรายละเอียดข้อมูลการบุกรุกแบบเต็มรูปแบบ	92
3.16 ตัวอย่างการส่งอีเมลโดยระบุรายละเอียดข้อมูลการบุกรุกแบบสรุป	93
3.17 ตัวอย่างการส่งอีเมลโดยระบุรายละเอียดข้อมูลการบุกรุกในรูปแบบของ CVE	93
3.18 ตัวอย่างการใช้งานส่วนแสดงผลในรูปแบบกราฟิก	94
3.19 ตัวอย่างการแสดงผลลัพธ์การใช้งานส่วนแสดงผลในรูปแบบกราฟิก	94

4.1	ตัวอย่างการวางไฟร์วอลล์เพื่อป้องกันระบบเครือข่ายและเซิร์ฟเวอร์ภายใน	95
4.2	ตัวอย่างการวางระบบตรวจสอบการบุกรุกแบบ NIDS บนเครือข่าย	96
4.3	ผังการเชื่อมต่อระบบเครือข่ายภายในอาคาร ชั้น 1	97
4.4	ผังการเชื่อมต่อระบบเครือข่ายภายในอาคาร ชั้น 2	98
4.5	ผังการเชื่อมต่อระบบเครือข่ายภายในอาคาร ชั้น 3	98
4.6	ผังการวางระบบป้องกันและตรวจสอบผู้บุกรุกภายในเครือข่ายห้องเรียน CSB302	99
ก.1	หน้าจอแสดงการติดตั้งฐานข้อมูล ACID ที่ไม่สมบูรณ์	114
ก.2	หน้าจอแสดงการติดตั้งฐานข้อมูลสำหรับ ACID	114
ก.3	หน้าจอแสดงการติดตั้งฐานข้อมูล ACID เสร็จสมบูรณ์	115
ก.4	หน้าจอแสดงผลการทำงานของโปรแกรม Snort ผ่านโปรแกรม ACID ที่ถูกต้อง	115
ข.1	IP Packet Header	116
ข.2	Basic ICMP Packet Header	118
ข.3	ICMP Packet Header used in ping command	118
ข.4	TCP Packet Header	119
ข.5	UDP Packet Header	120