



ระบบตรวจสอบและรายงานผลการโจมตีบนเว็บเซิร์ฟเวอร์
MONITORING AND REPORTING SYSTEM FOR ATTACKS ON WEB SERVER



เจ้าอากาศเอก เอกราช นินทรา
นายปรินทร์ ยานสากุล
นายกวิน บุญมาเลิศ

ปริญญาานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

พ.ศ. 2557

ระบบตรวจสอบและรายงานผลการ โจมตีบนเว็บไซต์ฟเวออร์



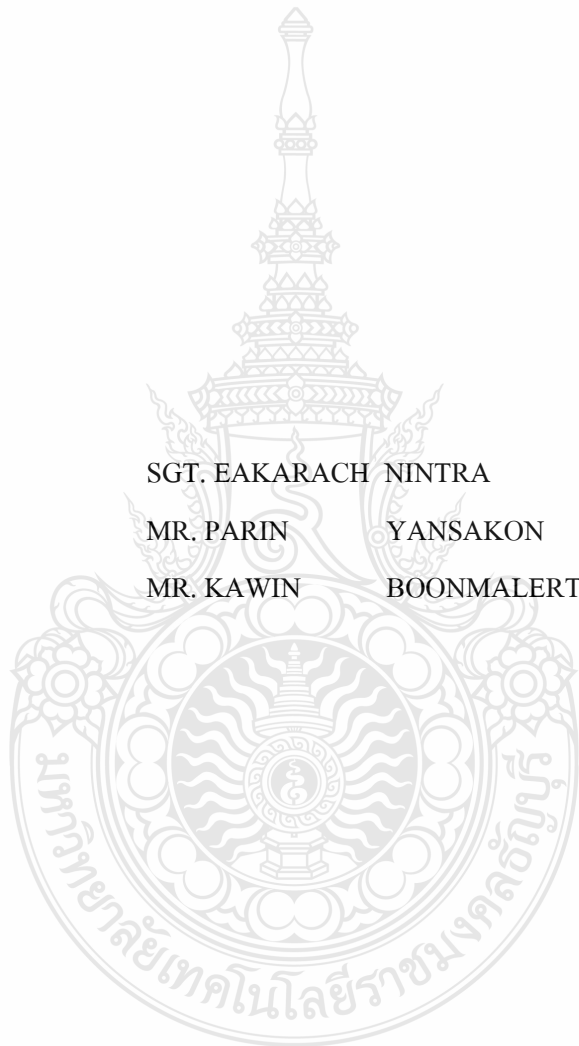
ปริญญาานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

พ.ศ. 2557

MONITORING AND REPORTING SYSTEM FOR ATTACKS ON WEB SERVER



SGT. EAKARACH NINTRA

MR. PARIN YANSAKON

MR. KAWIN BOONMALERT

THIS PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE BACHELOR DEGREE OF ENGINEERING
DEPARTMENT OF COMPUTER ENGINEERING
FACULTY OF ENGINEERING
RAJAMANGALA UNIVERSITY OF TECHNOLOGY THANYABURI
YEAR 2014

หัวข้อปริญญานิพนธ์ ระบบตรวจสอบและรายงานผลการโจมตีบนเว็บเซิร์ฟเวอร์
นักศึกษา จำอากาศเอก เอกราช นินทรา
นายปรินทร์ ย่านสากล
นายกวิน บุญมาเลิศ
อาจารย์ที่ปรึกษา อาจารย์วีระชัย แยมวี

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคล
ธัญบุรี อนุมัติให้ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต

.....หัวหน้าภาควิชาฯ
(อาจารย์พัฒนร์พี สุนันทพจน์)

คณะกรรมการสอบปริญญานิพนธ์

.....ประธานกรรมการ
(ดร.กิตติวัฒน์ นิ่มเกิดผล)

.....กรรมการ
(อาจารย์ชนสิน บุญนาม)

.....กรรมการ
(อาจารย์สมรรถชัย จันทรัตน์)

.....กรรมการและอาจารย์ที่ปรึกษา
(อาจารย์วีระชัย แยมวี)

ลิขสิทธิ์ของภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

หัวข้อปริญญานิพนธ์	ระบบตรวจสอบและรายงานผลการโจมตีบนเว็บเซิร์ฟเวอร์	
นักศึกษา	จำอากาศเอก เอกราช นินทรา	รหัส 115130462029-5
	นายปรินทร์ ย่านสากล	รหัส 115130462031-1
	นายกวิน บุญมาเลิศ	รหัส 115130462057-6
อาจารย์ที่ปรึกษา	อาจารย์วีระชัย เข้มวจิ	
ปีการศึกษา	2556	

บทคัดย่อ

ระบบตรวจสอบและรายงานผลการโจมตีบนเว็บเซิร์ฟเวอร์ เป็นระบบที่สามารถนำมาใช้เพื่อการเฝ้าระวังการโจมตีเว็บเซิร์ฟเวอร์ (Web Server) จากการกระทำของผู้ไม่หวังดีที่ก่อให้เกิดความเสียหาย แบ่งการทำงานเป็น 2 ส่วน โดยส่วนแรกเป็น Program Agent Detect ซึ่งทำหน้าที่ในการตรวจสอบแพ็คเกจ (Packet) ที่เข้ามาในเครื่องเว็บเซิร์ฟเวอร์ของผู้ใช้บริการ แล้วบันทึกข้อมูลการโจมตีไปยัง Database และส่วนที่สองเป็นเว็บเซิร์ฟเวอร์ของผู้ดูแลระบบ ทำการดึงข้อมูลจาก Database เพื่อมาแสดงผลให้กับผู้ใช้และผู้ดูแลระบบ

ดังนั้นระบบตรวจสอบและรายงานผลการโจมตีบนเว็บเซิร์ฟเวอร์ สามารถนำมาใช้ในการตรวจสอบการโจมตี เพื่อนำข้อมูลไปใช้ในการพิจารณาหรือเฝ้าระวัง ใ้รู้เท่าทันกับเหตุการณ์ที่อาจเกิดขึ้นในอนาคตต่อไป

คำสำคัญ

Program Agent Detect Packet Web Server Database

กิตติกรรมประกาศ

ในการจัดทำโครงการ “ระบบตรวจสอบและรายงานผลการโจมตีบนเว็บเซิร์ฟเวอร์” ได้รับคำแนะนำและความอนุเคราะห์ช่วยเหลือจากบุคคลต่าง ๆ จนทำให้โครงการนี้ได้ดำเนินการสำเร็จ ลุล่วงไปด้วยดีคณะผู้จัดทำจึงขอขอบพระคุณบุคคลดังต่อไปนี้

ขอขอบพระคุณ อาจารย์วีระชัย แยมวีจิ อาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ ซึ่งเป็นอาจารย์ที่ปรึกษาโครงการที่ให้คำแนะนำและชี้แนะแนวทางที่เป็นประโยชน์รวมทั้งคอยให้กำลังใจเสมอมา

ขอขอบพระคุณเจ้าหน้าที่บรรณารักษ์ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ที่ให้ข้อมูลเกี่ยวกับระบบฐานข้อมูลงานวิจัย และอำนวยความสะดวกในการสืบค้นข้อมูล ซึ่งเป็นประโยชน์ต่อโครงการเป็นอย่างมาก

ขอขอบพระคุณเพื่อนทุก ๆ คนที่คอยให้ความช่วยเหลือและคำแนะนำต่าง ๆ เกี่ยวกับการพัฒนาโครงการหากโครงการนี้มีประโยชน์อยู่บ้าง ขอมอบความดีนั้นแก่ บิดา มารดา ครู อาจารย์ และผู้มีพระคุณทุกท่าน

คณะผู้จัดทำ

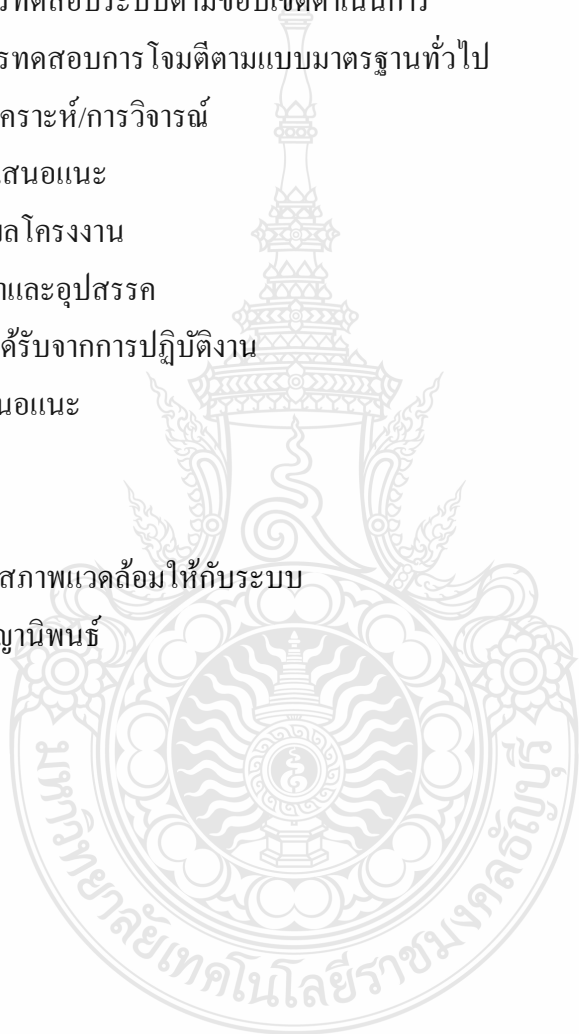


สารบัญ

	หน้า
บทคัดย่อ	ง
กิตติกรรมประกาศ	จ
สารบัญ	ฉ
สารบัญตาราง	ช
สารบัญรูป	ญ
บทที่ 1 บทนำ	1
1.1 ความเป็นมาและความสำคัญ	1
1.2 วัตถุประสงค์	1
1.3 ขอบเขตการดำเนินงาน	1
1.4 ประโยชน์ที่คาดว่าจะได้รับ	2
บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง	3
2.1 งานวิจัยที่เกี่ยวข้อง	3
2.2 ระบบตรวจจับการบุกรุกพื้นฐาน	4
2.3 การวิเคราะห์การถูกโจมตี	5
2.4 การดักจับข้อมูลในเครือข่าย	5
2.5 การดักจับแพ็คเกจ	6
2.6 Denial of Service	6
2.7 SQL Injection	10
2.8 Directory Traversal	11
2.9 Cross-Site Scripting (XSS)	12
2.10 แบบจำลอง Open System Interconnection (OSI)	13
2.11 โพรโทคอล (Protocol)	16
2.12 การเตรียมสภาพแวดล้อมสำหรับการดำเนินงาน	25
บทที่ 3 วิธีดำเนินงาน	29
3.1 แผนการดำเนินงาน	29
3.2 แบบจำลองโครงสร้างของการทำงาน	30
3.3 การออกแบบ/เครื่องมือ	31

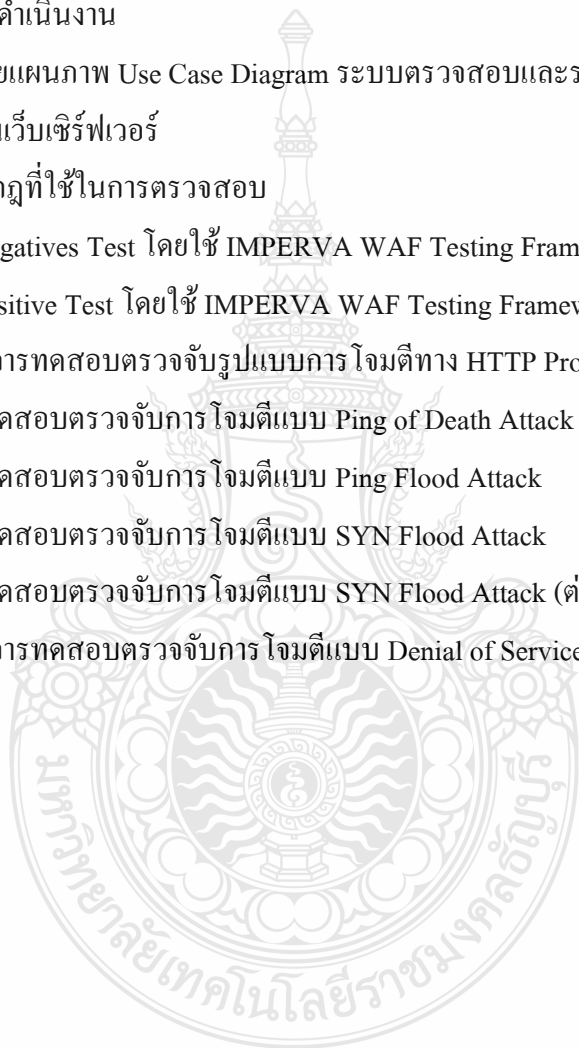
สารบัญ (ต่อ)

	หน้า
3.4 ขั้นตอนการสร้าง/ขั้นตอนการดำเนินงาน	32
บทที่ 4 ผลการดำเนินงานและการวิเคราะห์	42
4.1 ผลการทดสอบระบบตามขอบเขตดำเนินการ	42
4.2 ผลการทดสอบการโจมตีตามแบบมาตรฐานทั่วไป	60
4.3 การวิเคราะห์/การวิจารณ์	67
บทที่ 5 สรุปและข้อเสนอแนะ	69
5.1 สรุปผลโครงการ	69
5.2 ปัญหาและอุปสรรค	69
5.3 สิ่งที่ได้รับจากการปฏิบัติงาน	69
5.4 ข้อเสนอแนะ	70
บรรณานุกรม	71
ภาคผนวก ก	72
การเตรียมสภาพแวดล้อมให้กับระบบ	73
ประวัติผู้จัดทำปริญญาานิพนธ์	79



สารบัญตาราง

ตารางที่		หน้า
2.1	Method ใน Request Line	23
2.2	Status Code ใน Status Line	24
3.1	แผนการดำเนินงาน	29
3.2	คำอธิบายแผนภาพ Use Case Diagram ระบบตรวจสอบและรายงานผลการ โจมตีบนเว็บเซิร์ฟเวอร์	33
4.1	ตัวอย่างกฎที่ใช้ในการตรวจสอบ	60
4.2	False Negatives Test โดยใช้ IMPERVA WAF Testing Framework Version 0.5.0	61
4.3	False Positive Test โดยใช้ IMPERVA WAF Testing Framework Version 0.5.0	62
4.4	สรุปผลการทดสอบตรวจจับรูปแบบการ โจมตีทาง HTTP Protocol	62
4.5	ผลการทดสอบตรวจจับการ โจมตีแบบ Ping of Death Attack	64
4.6	ผลการทดสอบตรวจจับการ โจมตีแบบ Ping Flood Attack	65
4.7	ผลการทดสอบตรวจจับการ โจมตีแบบ SYN Flood Attack	66
4.7	ผลการทดสอบตรวจจับการ โจมตีแบบ SYN Flood Attack (ต่อ)	67
4.8	สรุปผลการทดสอบตรวจจับการ โจมตีแบบ Denial of Service	67



สารบัญรูป

รูปที่		หน้า
2.1	การโจมตีแบบ SYN Flood Attack	7
2.2	การโจมตีแบบ Ping of Death Attack	8
2.3	การโจมตีแบบ Ping Flood Attack ในตอนส่ง ICMP Echo Request	9
2.4	การโจมตีแบบ Ping Flood Attack ผลของการส่ง ICMP Echo Request	9
2.5	การเปลี่ยนแปลง URL Parameter เพื่อการ Query	10
2.6	ผลการเปลี่ยนแปลง URL Parameter เพื่อการ Query	11
2.7	การเพิ่ม SQL Command ใน URL	11
2.8	ผลการเพิ่ม SQL Command ใน URL	11
2.9	รูปแบบการโจมตีแบบ Directory Traversal	12
2.10	โครงสร้างของภาษา HTML	13
2.11	แบบจำลอง OSI จะแบ่งการทำงานของระบบเครือข่ายออกเป็น 7 ชั้น	14
2.12	ความสัมพันธ์ของโปรโตคอล	17
2.13	ARP Header	18
2.14	ตำแหน่งของโปรโตคอล ICMP	18
2.15	ICMP Header	19
2.16	IP Header	20
2.17	TCP Header	21
2.18	HTTP Transaction	22
2.19	รูปแบบของ HTTP Request Message	22
2.20	รูปแบบของ HTTP Response Message	24
3.1	แบบจำลองโครงสร้างของการทำงาน	30
3.2	ภาพจำลองการทำงานของระบบ	31
3.3	Use Case Diagram ระบบตรวจสอบและรายงานผลการโจมตีบนเว็บเซิร์ฟเวอร์	32
3.4	Class Diagram	34
3.5	Sequence Diagram การรับ Packet	35
3.6	Sequence Diagram การตรวจสอบการโจมตีแบบ SQL Injection	36
3.7	Sequence Diagram การตรวจสอบการโจมตีแบบ Directory Traversal	37

สารบัญรูป (ต่อ)

รูปที่		หน้า
3.8	Sequence Diagram การตรวจสอบการโจมตีแบบ Cross-Site Scripting	38
3.9	Denial of Service Flowchart	39
3.10	การแสดงผลแบบแผนภูมิแท่ง	40
3.11	การแสดงผลแบบแผนภูมิกราฟเส้น	41
3.12	การแสดงผลแบบตาราง	41
4.1	ทดสอบการทำงานบนระบบปฏิบัติการ Windows	42
4.2	ทดสอบการทำงานบนระบบปฏิบัติการ Linux	43
4.3	การโจมตี SQL Injection แบบ Login เข้าสู่ระบบโดยใช้เงื่อนไขทางลอจิก	43
4.4	ผลการโจมตี SQL Injection แบบ Login เข้าสู่ระบบโดยใช้เงื่อนไขทางลอจิก	44
4.5	ตรวจจับการโจมตี SQL Injection แบบ Login เข้าสู่ระบบโดยใช้เงื่อนไขทางลอจิก	44
4.6	การโจมตี SQL Injection แบบการเปลี่ยนแปลง URL Parameter เพื่อการ Query	45
4.7	ผลการโจมตี SQL Injection แบบการเปลี่ยนแปลง URL Parameter เพื่อการ Query	45
4.8	ตรวจจับการโจมตี SQL Injection แบบการเปลี่ยนแปลง URL Parameter เพื่อการ Query	46
4.9	การโจมตี SQL Injection แบบการเพิ่ม SQL Command ในช่อง Input ด้วยโปรแกรม SQLMap	46
4.10	ตรวจจับการโจมตี SQL Injection แบบการเพิ่ม SQL Command ในช่อง Input	47
4.11	การโจมตีแบบ Directory Traversal	47
4.12	ผลการโจมตีแบบ Directory Traversal	48
4.13	ตรวจสอบการโจมตีแบบ Directory Traversal	48
4.14	เครื่องมือการโจมตีแบบ Ping Flood Attack	49
4.15	การโจมตีแบบ Ping Flood Attack	49
4.16	ตรวจจับการโจมตีแบบ Ping Flood Attack	50
4.17	แสดงสถานะ Ping Flood Attack	50
4.18	เครื่องมือการโจมตีแบบ SYN Flood Attack	51
4.19	การโจมตีแบบ SYN Flood Attack	51

สารบัญรูป (ต่อ)

รูปที่		หน้า
4.20	ตรวจจับการโจมตีแบบ SYN Flood Attack	52
4.21	แสดงสถานะ SYN Flood Attack	52
4.22	การโจมตีแบบ Ping of Death Attack	53
4.23	ตรวจจับการโจมตีแบบ Ping of Death Attack	53
4.24	แสดงสถานะ Ping of Death Attack	54
4.25	การโจมตี Cross-Site Script แบบ non-Persistent XSS	54
4.26	ผลการโจมตี Cross-Site Script แบบ non-Persistent XSS	55
4.27	ตรวจจับการโจมตี Cross-Site Script แบบ non-Persistent XSS	55
4.28	การโจมตี Cross-Site Script แบบ Persistent XSS	56
4.29	ผลการโจมตี Cross-Site Script แบบ Persistent XSS	56
4.30	ตรวจจับการโจมตี Cross-Site Script แบบ Persistent XSS	57
4.31	การส่งอีเมลใน Program Agent Detect	57
4.32	เนื้อหาการส่งอีเมล	58
4.33	เก็บข้อมูลในฐานข้อมูล	58
4.34	ระบบการแสดงผล	59
4.35	ระบบรายงานผลผ่านเว็บเบราว์เซอร์	59
4.36	โปรแกรม IMPERVA	61
4.37	โปรแกรม CPU Death Ping V 2.0	63
4.38	การโจมตีแบบ Ping Flood Attack	64
4.39	การโจมตีแบบ SYN Flood Attack	66