ระบบแจ้งเตือนและป้องกันผู้บุกรุกโครงข่ายคอมพิวเตอร์ผ่าน VoIP
Intrusion Notification and Prevention System for Computer Network via VoIP

ภาณุวัฒน์ เจริญทัศน์* ธนัญ จารุวิทยโกวิท

ภาควิชาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม มหาวิทยาลัยธุรกิจบัณฑิตย์ กรุงเทพฯ 10210
* E-mail: lt_salvager@hotmail.com

บทคัดย่อ

งานวิจัยนี้ออกแบบและพัฒนาระบบแจ้งเตือนและป้องกันผู้บุกรุกระบบคอมพิวเตอร์ผ่าน VoIP โดยมีแนวความคิดมาจากระบบที่มีใช้งานอยู่ในปัจจุบันทำได้เพียงการตรวจจับการบุกรุกในโครงข่ายคอมพิวเตอร์ แต่ไม่สามารถแจ้งให้ผู้ดูแลระบบทราบอย่างทันทีทันใดผ่านทางโทรศัพท์ นอกจากนั้นผู้ดูแลระบบยังไม่สามารถดำเนินการป้องกันผ่านทางโทรศัพท์ได้ โดยระบบจะแจ้งเตือนผู้ดูแลระบบผ่านทางจดหมายอิเล็กทรอนิกส์เท่านั้น ทำให้ระบบขาดความยืดหยุ่นในการใช้งาน ผู้วิจัยจึงมีแนวคิดที่จะออกแบบและพัฒนาระบบแจ้งเตือนและป้องกันผู้บุกรุกโดยใช้เทคโนโลยี Voice Over IP (VoIP) ด้วยระบบที่พัฒนาขึ้นมานี้ เมื่อระบบตรวจพบการโจมตีของผู้บุกรุกที่เครื่องคอมพิวเตอร์แม่ข่ายที่ระบบดูแลอยู่ เมื่อระดับความร้ายแรงของการโจมตีถึงระดับที่ตั้งไว้ ระบบจะมีการสร้างกฎ (rule) ให้กับ Firewall เพื่อปิดกั้น Traffic นั้น หลังจากนั้นระบบจะโทรศัพท์ไปหาผู้ดูแลระบบเพื่อแจ้งการบุกรุกนี้ให้ทราบ ผู้ดูแลระบบสามารถเลือกวิธีการในการป้องกันผู้บุกรุกนอกเหนือจากกฎที่ระบบสร้างให้ได้ โดยผู้ดูแลระบบอาจจะสั่งให้เครื่องแม่ข่ายปิดเครื่องที่กำลังถูกบุกรุก เป็นต้น จากการทดสอบการทำงานพบว่าระบบที่พัฒนาสามารถทำงานได้ตามวัตถุประสงค์ที่ตั้งได้เป็นอย่างดี

คำสำคัญ: การแจ้งเตือนการบุกรุก การป้องกันการบุกรุก โทรศัพท์ไอพี

บทนำ

ปัจจุบันการรักษาความมั่นคงในระบบคอมพิวเตอร์เช่น การสร้างกฎในfirewall อย่างเดียว อาจจะไม่เพียงพอ เนื่องจากกฎใน firewall กำหนดแค่ว่าจะยอมให้ Traffic ผ่าน (permit) หรือปฏิเสธ Traffic (deny) เครื่องที่มี IP ตามที่กำหนดในกฎเท่านั้น ปัญหาคือถ้าเครื่องที่อยู่ใน trust zone (IP ช่วงที่ permit) พยายามโจมตี เข้ามาในระบบ firewall ก็จะไม่สามารถแก้ไขปัญหานี้ได้ ทำให้จำเป็นต้องมี IDS ซึ่งสามารถทำงานร่วมกับ firewall ได้ แต่ปัญหาคือเมื่อพบการบุกรุกแล้ว ระบบยังขาดการแจ้งเตือนให้ผู้ดูแลระบบทราบอย่างทันทีทันใด ระบบอาจจะมีการแจ้งเตือนผ่านทางจดหมายอิเล็กทรอนิกส์เท่านั้น ในกรณีที่ผู้ดูแลระบบอยู่ในบริเวณที่ไม่สามารถเข้าถึงโครงข่ายได้อย่างทันทีทันใด ก็จะไม่สามารถป้องกันการโจมตีดังกล่าวได้ ต้องขึ้นกับกฎที่ IDS ทำงานร่วมกับ firewall อย่างเดียว

โปรแกรม OSSEC [1-2] ซึ่งนำมาใช้ในงานวิจัยนี้จัดว่าเป็น host-based IDS ทำหน้าที่เฝ้าระวัง (monitor) เครื่องแม่ข่ายที่มีความสำคัญสูง ๆ เมื่อตรวจจับการบุกรุกในระบบ ระบบจะวิเคราะห์ระดับของความอันตรายของการบุกรุก ถ้าการบุกรุกนั้นมีระดับความอันตรายถึงระดับที่ตั้งไว้ ระบบจะแจ้งเตือนผู้ดูแลระบบผ่านอีเมล์ พร้อมด้วยการป้องกันผู้บุกรุกโดยอัตโนมัติ แต่อย่างไรก็ตาม OSSEC ยังมีข้อจำกัดคือ ผู้ดูแลระบบไม่สามารถรู้ได้อย่างทันทีทันใดว่ามีผู้บุกรุกในระบบ อีกทั้งไม่สามารถเลือกรูปแบบในการป้องกันผู้บุกรุกระบบด้วยตนเองได้

งานวิจัยนี้นำเสนอแนวทางการแก้ไขปัญหาดังกล่าว ซึ่งได้ออกแบบและพัฒนาระบบที่ช่วยอำนวยความสะดวกให้ผู้ดูแลระบบสามารถรู้ได้ทันท่วงทีถ้ามีผู้ที่กำลังพยายามบุกรุกระบบคอมพิวเตอร์ อีกทั้งยังสามารถเลือกวิธีการในการจัดการกับผู้ที่กำลังบุกรุก โดยขณะที่เมื่อมีผู้บุกรุก ระบบจะโทรศัพท์ไปหาผู้ดูแลระบบในทันทีด้วยเทคโนโลยี VoIP โดยอัตโนมัติ และผู้ดูแลระบบสามารถสื่อสารกับระบบ IVR เพื่อป้องกันผู้บุกรุกโดยอาจจะกำหนดให้เครื่องแม่ข่ายสั่งปิดเครื่องที่กำลังถูกบุกรุกได้ทันที

ระเบียบวิธีการศึกษาวิจัย

OSSEC [1-2] คือ Software ระบบเปิดที่ทำหน้าที่ตรวจจับ และควบคุมระบบคอมพิวเตอร์ที่มีประสิทธิภาพ เป็นเครื่องมือที่ใช้ในการวิเคราะห์การทำงาน, วิเคราะห์ log file, ตรวจสอบความถูกต้องของไฟล์ข้อมูล, ตรวจจับ Windows registry, ตรวจจับ rootkit รวมถึงมีการแจ้งเตือน และมีการตอบสนองกับสิ่งที่ผิดปกติที่กำลังเกิดขึ้นกับระบบ แบบ real-

time ซึ่ง OSSEC นี้สามารถทำงานได้บนหลากหลายระบบปฏิบัติการ เช่น Linux, OpenBSD, FreeBSD, Mac OS X, Sun Solaris, และ Microsoft Windows

Firewall [3] คือเครื่องมือที่ใช้ในการป้องกันเน็ตเวิร์กจากการสื่อสารทั่วไปที่ไม่ได้รับอนุญาต โดยที่เครื่องมือที่ว่านี้อาจจะเป็น Hardware หรือ Software หรือทั้งสองรวมกันขึ้นอยู่กับวิธีการหรือ Firewall Architecture ที่ใช้ ไฟร์วอลล์เป็นเครื่องมือที่ทำหน้าที่รักษาความมั่นคงในเชิงการป้องกัน (Protect) ซึ่งจะทำหน้าที่ควบคุมการเข้าถึงเน็ตเวิร์ก (Access Control) โดยอาศัยกฎพื้นฐานที่เรียกว่า Rule Base ปัญหาความมั่นคงของ เน็ตเวิร์ก คือ การควบคุมการเข้าถึงระบบหรือข้อมูลภายในเน็ตเวิร์ก ซึ่งก่อนที่จะเกิด Logical Access ได้นั้นต้องทำการสร้างการเชื่อมต่อ (Logical Conection) และการเชื่อมต่อนั้นต้องใช้ Protocol ดังนั้น Firewall จึงจะทำหน้าที่ตรวจสอบการเชื่อมต่อภายในเครือข่าย ให้เป็นไปตามกฎ

Intrusion Detection System [4] หรือ IDS คือ ระบบตรวจจับการบุกรุกนั้น เป็นระบบที่ใช้สำหรับการเฝ้าระวัง และแจ้งเตือนภัยถ้ามีการบุกรุก หรือมีสิ่งที่ผิดปกติเกิดขึ้นในระบบ แต่ IDS นั้นไม่ใช่ระบบป้องกันการบุกรุก แต่เป็นระบบที่คอยแจ้งเตือนภัยเท่านั้น โดยเฉพาะอย่างยิ่งการโจมตีแบบเรียลไทม์ เช่น การโจมตีแบบ DoS (Denial of Service) หรือ DDoS (Distributed Denial of Service) ระบบตรวจจับการบุกรุกมีด้วยกัน 3 ชนิด ได้แก่ Network-based IDSs, Host-based IDSs, Application-based IDS ซึ่งงานวิจัยชิ้นนี้ได้นำ Host-based IDSs มาใช้งาน ซึ่งจะทำการตรวจจับข้อมูลที่ไหลเข้าและออกคอมพิวเตอร์แต่ละเครื่องนอกจากนั้นระบบก็ยังตรวจสอบความสมบูรณ์ของ system files และเฝ้าดู processes ที่น่าสงสัย

VoIP [5] เป็นเทคโนโลยีสื่อสารด้วยเสียงผ่านระบบเครือข่ายอินเตอร์เน็ต หรือเรียกว่า Voice over IP (VoIP) เป็นระบบที่แปลงสัญญาณเสียงในรูปของสัญญาณไฟฟ้ามาเปลี่ยนเป็นสัญญาณดิจิตอล คือข้อมูลเสียงมาบีบอัดและบรรจุลงเป็นแพ็กเก็ต IP แล้วส่งไปโดยที่เราเตอร์ (Router) มีวิธีการปรับตัวเพื่อรับสัญญาณแพ็กเก็ต และยังแก้ปัญหาบางอย่างให้ เช่น การบีบอัดสัญญาณเสียง ให้มีขนาดเล็กลง การแก้ปัญหาเมื่อมีบางแพ็กเก็ตสูญหาย หรือการล่าช้าทางเวลา (delay) ระบบ VoIP เป็นระบบที่นำสัญญาณเสียงที่ผ่านการดิจิไตซ์ โดยหนึ่งช่องเสียงเมื่อแปลงเป็นข้อมูลจะมีขนาด 64 กิโลบิตต่อวินาที การนำข้อมูลเสียงขนาด 64 Kbps นี้ ต้องนำมาบีบอัด โดยทั่วไปจะเหลือประมาณ 8-10 Kbps ต่อช่องสัญญาณเสียงแล้วจึง บรรจุลงในไอพีแพ็กเก็ต เพื่อส่งผ่านทางเครือข่ายไอพี การสื่อสารผ่านทางเครือข่ายไอพีต้องมีเราเตอร์ (Router) ที่ทำหน้าที่พิเศษเพื่อประกันคุณภาพช่องสัญญาณไอพีนี้ เพื่อให้ข้อมูลไปถึง ปลายทางหรือกลับมาได้อย่างถูกต้องและอาจมีการให้สิทธิพิเศษก่อนแพ็กเก็ตไอพีอื่น (Quality of Service : QoS) เพื่อการให้บริการที่ทำให้เสียงมีคุณภาพ จากระบบดังกล่าวนี้เอง จึงสามารถนำมาประยุกต์ใช้กับระบบเชื่อมโยงเครือข่ายโทรศัพท์ระหว่างสำนักงาน โดยแต่ละสำนักงานสามารถ ใช้ระบบสื่อสารโทรศัพท์ผ่านทางเครือข่ายไอพี (VoIP) รวมถึงยังสามารถรับส่งข้อมูลไปพร้อมๆ กันได้

Asterisk [6] [7] คือ Software ระบบเปิดที่ทำหน้าที่หลักเป็น Softswitch, IP-PBX หรือที่เรียกว่าตู้ชุมสายโทรศัพท์ระบบ IP ซึ่งมีหน้าที่ในการควบคุมและจัดการบริหาร การเชื่อมต่อ ระหว่างอุปกรณ์โทรศัพท์ผ่านเครือข่ายเน็ตเวิร์ก อีกทั้งยังสามารถเพิ่มเติมประสิทธิภาพและความสามารถในการทำงานได้โดยง่าย นอกจากนี้ก็ยังสามารถที่จะโทรศัพท์ออกไปข้างนอก คือ เครือข่าย PSTN (Public Switch Telephone Network) ผ่านทางสาย Trunk Line เมื่อมีการเรียกใช้โทรศัพท์ผ่านทาง PBX ในส่วน Trunk Line ก็คือสายที่เชื่อมต่อระหว่าง ตัว PBX กับ ผู้ให้บริการโทรศัพท์นั่นเอง เมื่อผ่าน PBX แล้วก็จะผ่านส่วนที่เรียกว่า Extension ซึ่งก็คือสายที่ต่อออกจาก PBX เข้าไปยังโทรศัพท์ของแต่ละบุคคลนั่นเอง Trunk Line นั้นจะทำให้เราลดค่าใช้จ่ายเพราะโดยทั่วไป บริษัทต่างๆ ก็จะใช้สาย Trunk Line แค่ 2-3 สาย หากต้องการโทรศัพท์คุยกันภายในก็ใช้ผ่านสาย Extension นอกจากนี้ ตัว Trunk Line ยังสามารถส่งข้อมูลได้ทั้งที่เป็น Data และ Voice อีกด้วย

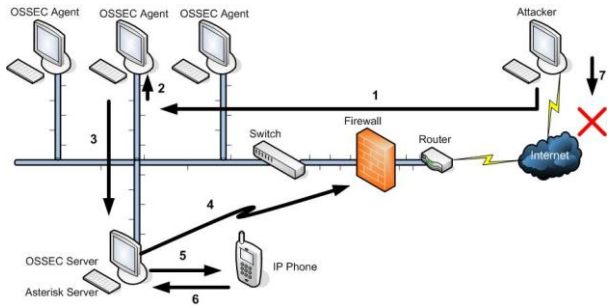
Interactive Voice Response (IVR) [8] หรือที่นิยมเรียกกันทั่วไปว่า ระบบตอบรับโทรศัพท์อัตโนมัติ ระบบนี้จะเป็นลักษณะของการ โต้ตอบข้อมูลด้วยเสียง ระหว่างผู้ใช้บริการหรือผู้โทรเข้ากับเครื่องโทรศัพท์ ซึ่งเกี่ยวข้องกับการค้นหาข้อมูลตัวเลขหรือข้อความในฐานข้อมูลมาแสดง โดยผู้ใช้บริการ เช่น อาจจะต้องกดรหัส ประจำตัว หรือรหัสผ่านหรือ ตัวเลขต่างๆ บนแป้นโทรศัพท์ เพื่อทำการเลือกรายการ ที่ต้องการ และระบบจะทำการแปลงสัญญาณนั้น ไปค้นหาในฐานข้อมูล (Database) เพื่อเรียกข้อมูลมาแสดงเป็นเสียง เป็นระบบที่ใช้สำหรับลดปริมาณงานที่ Agent จะได้รับ หรือเป็นการเพิ่มขีดความสามารถของ ระบบ Contract Center โดยทั้งหมดนี้จัดเป็นระบบบริการลูกค้าแบบอัตโนมัติ ซึ่งจะต่อเข้ากับ PBX และต่อเข้ากับระบบฐานข้อมูลภายใน เมื่อผู้ใช้บริการโทรเข้ามายังระบบ Contact Center หรือ Call Center ส่วนใหญ่จะได้ยินเสียงตอบรับโดย ระบบ IVR เพื่อให้บริการพื้นฐานแก่ลูกค้าก่อน ตัวอย่างเช่น การสอบถามยอดเงินในบัญชีของธนาคาร การรับปรึกษา และให้คำแนะนำต่างๆ หรือ การสอบถามผลการเรียน เป็นต้น

งานวิจัยที่เกี่ยวข้องคือเรื่อง Managing Alerts in a Multi-Intrusion Detection Environment [9] ซึ่งในบางครั้งจะมีการแจ้งเตือนที่ผิดพลาดมากจนเกินไป รวมถึงความไม่

ถูกต้องของข้อมูลที่แจ้งเตือน ในงานวิจัยนี้ใช้วิธีสร้าง module พิเศษขึ้นมาเพื่อวิเคราะห์การแจ้งเตือนให้ครอบคลุมทุกๆการแจ้งเตือนมากขึ้น ซึ่ง module ที่สร้างขึ้นมา จะทำการบันทึกการแจ้งเตือนลงในฐานข้อมูลทั้งหมด เพื่อให้ง่ายต่อการวิเคราะห์และเปรียบเทียบเหตุการณ์ต่างๆที่เกิดขึ้นในระบบ

การออกแบบและพัฒนาระบบ

รูปการเชื่อมต่อและขั้นตอนการทำงานของระบบที่พัฒนาแสดงในรูปที่ 1



รูปที่ 1 แสดงการเชื่อมต่อและขั้นตอนการทำงานของระบบที่พัฒนา

ขั้นตอนการทำงานของระบบที่ออกแบบในรูปที่ 1 สามารถอธิบายได้ดังนี้

1. ผู้บุกรุก (ทั้งจาก Intranet หรือ Internet) ที่มีหมายเลข IP อยู่ในเขตที่เชื่อถือได้ (trust zone) สามารถผ่านเข้ามาในระบบผ่าน Firewall ได้
2. ผู้บุกรุกดำเนินการโจมตี (attack) เครื่องคอมพิวเตอร์แม่ข่าย ที่ถูกเฝ้าระวังด้วย OSSEC Agent
3. เครื่องคอมพิวเตอร์แม่ข่ายที่ถูกโจมตีจะส่งการแจ้งเตือนไปที่ OSSEC Server
4. OSSEC Server ดำเนินการ Active-response โดยการเพิ่มกฎ (Rule) ที่ Firewall เพื่อป้องกันผู้บุกรุกให้โดยอัตโนมัติ
5. เครื่องแม่ข่าย Asterisk ซึ่งทำหน้าที่เป็น VoIP Server เรียกสายออกไปที่ผู้ดูแลระบบ และแจ้งเหตุผิดปกติที่เกิดขึ้นให้ทราบ
6. ผู้ดูแลระบบรับฟังเสียงพูดผ่านทาง IVR และกดหมายเลขคำสั่งเพื่อป้องกันผู้บุกรุกเพิ่มเติมจากระบบป้องกันอัตโนมัติของ OSSEC โดยสิ่งที่สามารถดำเนินการได้มีอยู่ 2 ประเภท คือ การปิดกั้นข้อมูลที่มาจากหมายเลข IP ต้นทางของผู้บุกรุกอย่างถาวร และการสั่งปิดเครื่องแม่ข่ายที่เป็นเป้าหมายของการโจมตี
7. ผู้บุกรุกจะไม่สามารถเข้าใช้ระบบได้อีกต่อไป

ความสามารถของ OSSEC ที่มีประโยชน์อย่างยิ่งคือระบบ Active Response เป็นระบบป้องกันผู้บุกรุกได้เองโดยอัตโนมัติ ซึ่งโดยปกติจะมีวิธีการป้องกันโดยการสร้างกฎ (rule) ให้ Firewall สั่งปิดกั้น หรือทิ้งแพ็กเก็ตที่มีหมายเลข IP ต้นทางของผู้บุกรุก โดยอาจจะสั่งปิดกั้นเป็นระยะเวลาตามที่กำหนด เมื่อครบเวลาที่กำหนดกฎที่สร้างขึ้นดังกล่าวก็จะหายไป

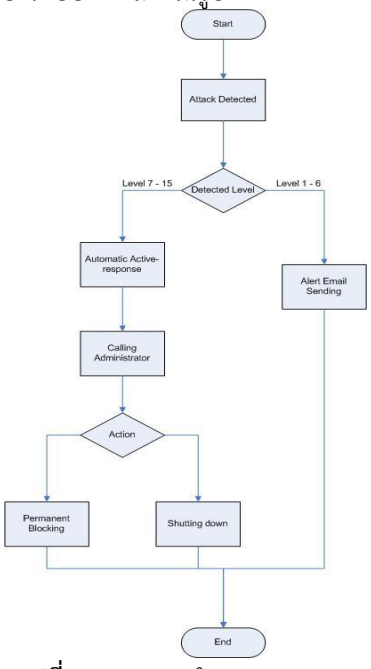
OSSEC มีระดับการแจ้งเตือนความร้ายแรงของการบุกรุกระบบอยู่ 15 ระดับ โดยที่ระบบที่พัฒนาสำหรับงานวิจัยชิ้นนี้มีรายละเอียดดังนี้

1. เมื่อ OSSEC ตรวจสอบพบการบุกรุกในระดับที่ 1 – 6 จะดำเนินการแจ้งผู้ดูแลระบบผ่านอีเมล์เท่านั้นเนื่องจากเป็นการแจ้งเตือนทั่วๆไป ซึ่งยังไม่ส่งผลให้เกิดความเสียหายบนระบบ มีรายละเอียดของระดับการแจ้งเตือนในระดับ 1 - 6 ได้แก่
   - ระดับที่ 1 – 4 จะเป็นการแจ้งเตือนทั่วๆไป เช่น ผู้ใช้สามารถ Login เข้าระบบได้สำเร็จ หรือ บาง Application แจ้งความผิดพลาดซึ่งไม่มีความเกี่ยวเนื่องกับการบุกรุกระบบแต่อย่างใด
   - ระดับที่ 5 – 6 จะเป็นการแจ้งเตือนทั่วๆไป เช่น ผู้ใช้ใส่รหัสผ่านเพื่อ Login เข้าใช้ระบบผิดพลาด หรือบางครั้งจะบ่งชี้ว่าได้มี Worm, Virus อยู่ภายในระบบ แต่ว่าไม่ได้มีการคุกคามแต่อย่างใด ซึ่ง OSSEC จะทำการส่งอีเมล์แจ้งเตือนไปยังผู้ดูแลระบบโดยอัตโนมัติ เนื่องจากระดับความรุนแรงของการบุกรุกที่ 5 – 6 ยังจัดอยู่ในช่วงปกติทั่วไปที่ไม่ร้ายแรงมากนัก ซึ่งจะออกแบบให้ส่งแค่อีเมล์แจ้งผู้ดูแลระบบเท่านั้น
2. เมื่อ OSSEC ตรวจสอบพบการบุกรุกในระดับที่ 7 – 15 ระบบจะทำการป้องกันผู้บุกรุกอัตโนมัติในบางส่วน เช่น การทำ Traffic shaping หรือการทำ Throttling หรือ Account lockout แต่งานวิจัยชิ้นนี้ได้ออกแบบให้ OSSEC ส่งคำสั่งไปยัง Asterisk เพื่อโทรศัพท์แจ้งเตือนไปยังผู้ดูแลระบบโดยอัตโนมัติ เนื่องจากมีแนวโน้มที่จะทำให้ระบบเกิดความเสียหายอย่างร้ายแรงจากการบุกรุกนอกเหนือจากการสร้าง Active Response ป้องกันผู้บุกรุกให้โดยอัตโนมัติ ผู้ดูแลระบบสามารถสั่งงานระบบผ่าน IVR เพื่อสั่งให้ระบบทำงานตามความต้องการเพิ่มเติมจาก Active Response เดิม เช่นอาจจะมี Active Response ไปสร้างกฎให้ Firewall เพื่อปิดกั้น หรือทิ้งแพ็กเก็ตแบบถาวร หรือสั่งปิดเครื่องที่กำลังถูกโจมตีได้ ซึ่งรายละเอียดของระดับการแจ้งเตือนในระดับ 7 – 15 ได้แก่
   - ระดับที่ 7 11 บ่งชี้ถึงการคุกคามบางอย่าง เช่น มีผู้ที่พยาม Login โดยที่ไม่ได้มีรายชื่อที่สามารถเข้าใช้

ระบบได้ หรือ การพยายาม Login ผิดพลาดหลายๆ ครั้ง

- ระดับที่ 12 เป็นการแจ้งเตือนในระดับที่สูง ซึ่งบ่งชี้ถึงมีการบุกรุกบาง Application
- ระดับที่ 13 เป็นรูปแบบการบุกรุกที่ทำให้ Buffer overflow เช่นการทำให้ Syslog มีขนาดใหญ่กว่าปกติ
- ระดับที่ 14 บ่งชี้ว่ามีการบุกรุกซ้ำๆ หลายๆครั้ง
- ระดับที่ 15 บ่งชี้ว่าการบุกรุกระบบสำเร็จแล้ว

โปรแกรมในการตรวจจับ แจ้งเตือน และป้องกันผู้บุกรุกในระบบคอมพิวเตอร์ เป็นโปรแกรมที่พัฒนาขึ้นมา ซึ่งมีลำดับการทำงานของระบบ ดังแสดงในรูปที่ 2



รูปที่ 2 แสดงการทำงานของระบบ

จากรูปที่ 2 สามารถอธิบายหลักการทำงานของระบบได้ดังนี้

1. ผู้ที่ต้องการเข้ามาใช้งานภายในระบบสามารถผ่านเข้ามาใช้งานได้ตามปกติ แต่ถ้าเมื่อใดที่ OSSEC ตรวจพบว่าผู้ที่ กำลังใช้ระบบอยู่นั้นเป็นผู้ที่ประสงค์ไม่ดีต่อระบบ ก็จะดำเนินการในขั้นตอนถัดไป
2. OSSEC Server สามารถตรวจจับสิ่งผิดปกติได้
3. OSSEC Server จะประมวลผลระดับความร้ายแรงของการบุกรุก โดยที่ระดับ 1 – 6 จะแจ้งผู้ดูแลระบบผ่านอีเมล์ แต่ถ้าหากอยู่ในระดับที่ 7 – 15 ก็จะดำเนินการในขั้นตอนถัดไป
4. OSSEC Server จะทำการป้องกันผู้บุกรุกโดยอัตโนมัติ พร้อมทั้งส่งคำสั่งให้ Asterisk Server เรียกสายออกไปยังผู้ดูแลระบบโดยอัตโนมัติ

5. ผู้ดูแลระบบรับสายโทรศัพท์เรียกเข้า แล้วกดหมายเลขตามที่ระบบแจ้งผ่าน IVR เพื่อเลือกทำการป้องกันผู้บุกรุกเพิ่มเติมจากระบบอัตโนมัติที่ OSSEC ได้ดำเนินการในขั้นตอนที่ 4 โดยการปิดกั้นผู้บุกรุกแบบถาวร ถ้าหากว่าทำการบุกรุกซ้ำๆ หรือเลือกที่จะสั่งปิดเครื่อง OSSEC Agent ถ้าหากพบว่าผู้บุกรุกทำการเปลี่ยนหมายเลข IP เพื่อเข้ามาจู่โจมอีกครั้ง
6. จากนั้นผู้บุกรุกจะไม่สามารถใช้วิธีการเดิมในการเข้าใช้ระบบได้อีกต่อไป

รายละเอียดของ Source Code ในส่วนการป้องกันผู้บุกรุกอัตโนมัติ การปิดกั้นหมายเลข IP ของผู้บุกรุกแบบถาวร รวมถึงการสั่งปิดเครื่อง OSSEC Agent แสดงได้ดังรูปที่ 3ก., 3ข. และ 3ค. ตามลำดับ

```
<active-response>
    <!-- Firewall Drop response. Block the IP for
     - 600 seconds on the firewall (iptables,
     - ipfilter, etc).
     -->
    <command>firewall-drop</command>
    <location>local</location>
    <level>7</level>
    <timeout>600</timeout>
  </active-response>
```

สั่งให้ Script ชื่อ firewall-drop ทำงาน รวมถึงสามารถกำหนดระยะเวลาในการ Block

```
# Blocking IP
if [ "x${ACTION}" != "xadd" -a "x${ACTION}" != "xdelete" ]; then
  echo "$0: invalid action: ${ACTION}"
  exit 1;
fi
if [ "X${UNAME}" = "XLinux" ]; then
  if [ "x${ACTION}" = "xadd" ]; then
    ARG1="-I INPUT -s ${IP} -j DROP"
    ARG2="-I FORWARD -s ${IP} -j DROP"
  else
    ARG1="-D INPUT -s ${IP} -j DROP"
    ARG2="-D FORWARD -s ${IP} -j DROP"
  fi
```

คำสั่ง Block และปลด Block ไอพีแอดเดรสของผู้บุกรุก

รูปที่ 3ก. แสดงการป้องกันผู้บุกรุกโดยอัตโนมัติ

```
<active-response>
  <command> firewall-drop </command>
  <location>local</location>
  <level>4</level>
</active-response>
```

สั่งให้ Script ชื่อ firewall-drop ทำงาน โดยไม่ระบุเวลาสิ้นสุด เพื่อทำการสร้างกฎแบบถาวร

```
# Blocking IP
if [ "x${ACTION}" != "xadd" ]; then
  echo "$0: invalid action: ${ACTION}"
  exit 1;
fi
  if [ "x${ACTION}" = "xadd" ]; then
    ARG1="-I INPUT -s ${IP} -j DROP"
    ARG2="-I FORWARD -s ${IP} -j DROP"
  fi
```

คำสั่ง Block ไอพีแอดเดรสของผู้บุกรุกแบบถาวร

รูปที่ 3ข. แสดงการปิดกั้นหมายเลข IP ของผู้บุกรุกแบบถาวร

```
#!/bin/sh
poweroff
```

Script ที่ถูกเรียกใช้เพื่อสั่งปิดเครื่อง

รูปที่ 3ค. แสดงการสั่งปิดเครื่อง OSSEC Agent ที่กำลังถูกบุกรุก

ผลการศึกษาวิจัยและการอภิปรายผล

งานวิจัยนี้ได้ทดสอบการทำงานของระบบที่พัฒนาทั้งในส่วนของการพัฒนาให้เรียกสายออกโดยอัตโนมัติทันทีที่ตรวจพบผู้บุกรุก และปิดกั้นผู้บุกรุกไม่ให้สามารถเข้ามาในระบบได้ หรือการสั่งปิดเครื่องที่กำลังถูกบุกรุก ดังนี้

การทดสอบที่ 1 ระบบโทรศัพท์แจ้งผู้ดูแลระบบให้โดยอัตโนมัติ เมื่อสามารถตรวจจับผู้บุกรุกได้

เครื่องแม่ข่ายที่ใช้ เป็นเครื่องแม่ข่าย OSSEC และ Asterisk ซึ่งทำหน้าที่ในการตรวจจับผู้บุกรุก และทำหน้าที่เป็น Softswitch หรือ IP-PBX สำหรับเรียกสายแจ้งไปยังผู้ดูแลระบบ ตามลำดับ ซึ่งผู้บุกรุกอาจจะใช้โปรแกรม BackTrack ในการโจมตีด้วยวิธีการ Port Scanning หรือ Brute Force เมื่อ OSSEC Server สามารถตรวจจับผู้ที่กำลังบุกรุกได้ ก็จะส่งคำสั่งไปที่ Asterisk Server เพื่อเรียกสายออกไปยังผู้ดูแลระบบทางโทรศัพท์มือถือ ให้โดยอัตโนมัติ และรอรับคำสั่งจากผู้ดูแลระบบผ่าน IVR เพื่อความสะดวกและชัดเจนในการแสดงผลการทดสอบ ในบทความนี้จะใช้ Softphone เพื่อให้ระบบติดต่อไปยังผู้ดูแลระบบ ซึ่งในระบบที่ใช้งานจริงสามารถติดต่อทางโทรศัพท์เคลื่อนที่ได้ ดังแสดงในรูปที่ 4

รูปที่ 4 แสดงการเรียกสายออกอัตโนมัติไปยังผู้ดูแลระบบ

อย่างไรก็ตาม เพื่อตรวจสอบความถูกต้องในการใช้งานเชิงสถิติ ผู้วิจัยได้ดำเนินการทดสอบให้ Asterisk Server เรียกสายออกอัตโนมัติ 20 ครั้ง ผลที่ได้แสดงในตารางที่ 1

ตารางที่ 1 แสดงการทดสอบเรียกสายออกอัตโนมัติ

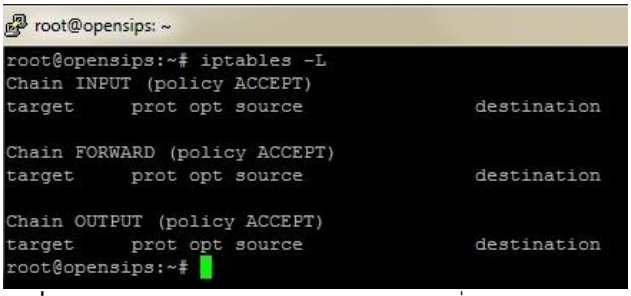
จำนวนครั้งที่ทดสอบ	จำนวนครั้งที่สามารเรียกสายออกได้	จำนวนครั้งที่ไม่สามารถเรียกสายออกได้	ความถูกต้องคิดเป็น %
20	20	0	100 %

จากตารางที่ 1 สามารถสรุปผลการทดสอบได้ คือ ระบบสามารถเรียกสายออกอัตโนมัติได้ถูกต้อง 100%

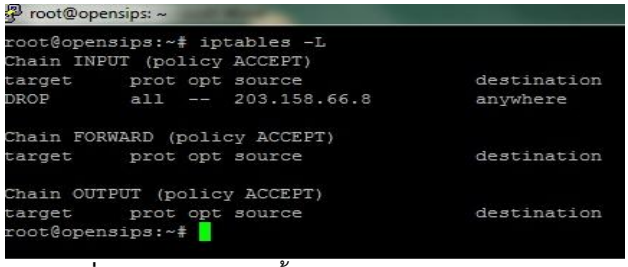
การทดสอบที่ 2 ระบบสร้างกฎที่ Firewall เพื่อปิดกั้นหมายเลข IP ของผู้บุกรุกแบบชั่วคราวโดยอัตโนมัติ

รูปภาพของรายการใน IP Table ก่อนที่จะสร้างกฎใน Firewall เพื่อปิดกั้นเป็นเวลา 10 นาที ซึ่งหลังจากครบตามเวลาที่กำหนดแล้ว ระบบจะยกเลิกการปิดกั้นได้อย่างถูกต้อง ดังแสดงในรูปที่ 5ก.

ส่วนถัดไปจะดำเนินการทดสอบ Active response ที่ OSSEC สร้างให้อัตโนมัติเมื่อพบการบุกรุก เพื่อปิดกั้นหมายเลข IP ของผู้บุกรุก ซึ่งเราสามารถตั้งค่ากำหนดระยะเวลาในการปิดกั้นได้ ดังแสดงในรูปที่ 5ข.



รูปที่ 5ก. แสดงรายการใน IP Table ก่อนที่จะสร้างกฎใน Firewall



รูปที่ 5ข. แสดงการปิดกั้นหมายเลข IP ของผู้บุกรุก

อย่างไรก็ตาม เพื่อตรวจสอบความถูกต้องในการใช้งานเชิงสถิติ ผู้วิจัยได้ดำเนินการทดสอบปิดกั้นหมายเลข IP จำนวน 20 ครั้ง ผลที่ได้แสดงในตารางที่ 2

ตารางที่ 2 แสดงการทดสอบการปิดกั้นหมายเลข IP ของผู้บุกรุก

จำนวนครั้งที่ทดสอบ	จำนวนครั้งสามารถ ปิดกั้นได้	จำนวนครั้งที่ไม่สามารถ ปิดกั้นได้	ความถูกต้องคิดเป็น %
20	20	0	100 %

จากตารางที่ 2 สามารถสรุปผลการทดสอบได้ คือ ระบบสามารถปิดกั้นหมายเลข IP ของผู้บุกรุกได้ถูกต้อง 100%

การทดสอบที่ 3 การสร้างกฎตามคำสั่งของผู้ดูแลระบบผ่านระบบ IVR

เมื่อระบบโทรศัพท์แจ้งผู้ดูแลระบบ และผู้ดูแลระบบตัดสินใจจะ over-rule ตัว Active Response ที่ OSSEC สร้างให้ โดย Admin สามารถกด DTMF เพื่อเลือกรายการได้ดังนี้

1. สร้างกฎแบบถาวร ซึ่งภาพของการสร้างกฎจะเหมือนกับในรูปที่ 5ข. แต่จะแตกต่างกันที่จะปิดกั้นหมายเลข IP ของผู้บุกรุกแบบถาวร เพื่อตรวจสอบความถูกต้องในการใช้งานเชิงสถิติ ผู้วิจัยได้ดำเนินการทดสอบสร้างกฎแบบถาวร จำนวน 20 ครั้ง ผลที่ได้แสดงในตารางที่ 3

ตารางที่ 3 แสดงการทดสอบสร้างกฎแบบถาวร

จำนวนครั้งที่ทดสอบ	จำนวนครั้งที่สามารถ สร้างกฎแบบถาวรได้	จำนวนครั้งที่ไม่สามารถ สร้างกฎแบบถาวรได้	ความถูกต้องคิดเป็น %
20	20	0	100 %

จากตารางที่ 3 สามารถสรุปผลการทดสอบสร้างกฎแบบถาวร ได้ถูกต้อง 100%

2. ปิดเครื่องที่กำลังถูกบุกรุก ผู้วิจัยได้ดำเนินการทดสอบการปิดเครื่องที่กำลังถูกบุกรุก จำนวน 20 ครั้ง ผลที่ได้แสดงในตารางที่ 4

ตารางที่ 4 แสดงการทดสอบปิดเครื่องที่กำลังถูกบุกรุก

จำนวนครั้งที่ทดสอบ	จำนวนครั้งที่สามารถ ปิดเครื่องได้	จำนวนครั้งที่ไม่สามารถ ปิดเครื่องได้	ความถูกต้องคิดเป็น %
20	20	0	100 %

จากตารางที่ 4 สามารถสรุปผลการทดสอบการสั่งปิดเครื่องที่กำลังถูกบุกรุก ได้ถูกต้อง 100%

อย่างไรก็ตามยังคงต้องมีการทดสอบการทำงานของระบบอีกหลายอย่างในอนาคต เช่น ทำการทดลองกับ site จริง และการประเมินเรื่องการเตือนนั้นเป็นที่พอใจแก่ผู้ดูแลระบบจริงหรือไม่ รวมถึงการประมาณการ ของ cost ทั้งระบบ

สรุปผลการศึกษาวิจัย

งานวิจัยนี้นำเสนอระบบแจ้งเตือน และป้องกันผู้บุกรุกระบบคอมพิวเตอร์ ซึ่งเป็นการนำเทคโนโลยี VoIP มาประยุกต์ใช้งานร่วมกับระบบตรวจจับผู้บุกรุก โดยใช้ OSSEC ทำงานร่วมกับ Asterisk นำมาเป็นศูนย์กลางในการติดต่อระหว่างผู้ดูแลระบบ โดยระบบจะแจ้งเตือนการบุกรุก เมื่อระบบตรวจจับสามารถตรวจพบผู้บุกรุกจะสร้าง Active Response ให้เพื่อปิดกั้นการเข้าถึงของผู้บุกรุกแบบชั่วคราวให้โดยอัตโนมัติ หลังจากนั้นจะโทรศัพท์ไปยังผู้ดูแลระบบ ซึ่งผู้ดูแลระบบสามารถเลือกที่จะสั่งการผ่านระบบ DTMF เพื่อให้ระบบสร้างกฎใน Firewall แบบถาวร หรือสั่งปิดการทำงานของเครื่องแม่ข่ายนั้นผ่านทางโทรศัพท์ได้ทันที จากการทดสอบการทำงานของระบบ พบว่าระบบสามารถทำงานได้อย่างถูกต้องตามขอบเขตที่กำหนดไว้ ช่วยเพิ่มความสะดวกและความยืดหยุ่นให้กับผู้ดูแลระบบได้เป็นอย่างดี

เอกสารอ้างอิง

[1] Andrew Hay, Daniel Cid, Rory Bray. OSSEC Host-Based Intrusion Detection. Burlington. Elsevier, Inc (2008)

[2] OSSEC. http://www.ossec.net/ สืบค้น 10 กันยายน 2554

[3] Firewall. http://itm51.justboard.net/t97-topic สืบค้น 10 กันยายน 2554

[4] Intrusion Detection System. http://janphar.lpru.ac.th/wanasiri/PDF/NetworkSecurity.pdf. สืบค้น 10 กันยายน 2554

[5] VoIP. http://www.security.co.th/newevent.php สืบค้น 10 กันยายน พ.ศ. 2554

[6] Asterisk. http://www.asteriskdiy.com/index.php/ระบบ_Asterisk_คืออะไร_ และทำงานอย่างไร สืบค้น 10 กันยายน 2554

[7] Asterisk. http://www.asterisk.org/ สืบค้น 10 กันยายน 2554

[8] Interactive Voice Response (IVR). http://sasdkmitl08.blogspot.com/2008/06/interactive-voice-response-ivr.html สืบค้น 10 กันยายน พ.ศ. 2554

[9] Frédéric Cuppens, ONERA Toulouse, Managing Alerts in a Multi-Intrusion Detection Environment, France, http://www.acsac.org/2001/papers/70.pdf สืบค้น 1 มิถุนายน พ.ศ. 2554