การเปรียบเทียบการตรวจจับการโจมตีทางไซเบอร์ที่สร้างปริมาณข้อมูลมหาศาลในเลเยอร์ 3 และ 4

เฉลิมพล คำนิกรณ์[1]
ชัยพร เขมะภาตะพันธ์[2]

บทคัดย่อ

งานวิจัยนี้เป็นทำการจำลองการโจมตีทางไซเบอร์จำนวนมากลำดับชั้นที่ 3 และ 4 ของแม่แบบโอเอสไอด้วยการโจมตีแบบ ICMP Flood, Smurf, TCP Scan Port และ TCP Sync Flood เพื่อประเมินและเปรียบเทียบสมรรถนะการทำงานของโปรแกรมตรวจจับการบุกรุกที่เป็นโอเพ่นซอร์สระหว่างสนอร์ทและซูริคาต้า โดยจำลองระบบเครือข่ายในสภาพแวดล้อมแบบปิดให้คล้ายกับระบบเครือข่ายภายในขององค์กรเพื่อทดสอบการโจมตีและการตรวจจับที่มีปัจจัยตามที่กำหนดไว้ให้ใกล้เคียงกับเหตุการณ์ที่เกิดขึ้นจริงในระบบเครือข่ายคอมพิวเตอร์ การประเมินประสิทธิภาพจะใช้เทคนิคการนับปริมาณข้อมูล อัตราเร็วในการโจมตี การใช้งานหน่วยประมวลผล แล้วจึงนำผลการทดลองไปคำนวณ วิเคราะห์ เพื่อเปรียบเทียบประสิทธิภาพตามที่ออกแบบไว้

ผลการทดลองของทั้งสองระบบซึ่งอยู่ในช่วงเวลาเดียวกัน ภายใต้การโจมตีแบบเดียวกัน พบว่ามีความสามารถในการตรวจจับการโจมตีและมีประสิทธิภาพในการตรวจจับการบุกรุกที่ใกล้เคียงกัน อย่างไรก็ตามโปรแกรมสนอร์ทสามารถตรวจจับเมื่อมีการโจมตีแบบ ICMP ได้ดีกว่าอย่างชัดเจน ในขณะที่โปรแกรมซูริคาต้าสามารถตรวจจับเมื่อมีการโจมตีแบบ TCP ได้ดีกว่า

Abstract

This research simulated cyberattacks that generate massive traffics in layer 3 and 4 according to OSI layer using ICMP Flood, Smurf, TCP Scan Port and TCP Sync Flood. In order to evaluate and compare the detection performances of the open source intrusion detection systems between Snort and Suricata, the simulation based on a network system in a closed environment similar to an intranet network of an organization is applied. The simulation performs attack and detection which have specified factors as close to the actual situation in the computer network. The performance relies on packet counting, detection speed, CPU usage and then use the experimental result to calculate and compare the performances.

---

[1]นักศึกษาหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์

[2] อาจารย์ที่ปรึกษา

It can be noted from the results of both Snort and Suricata which are conducted at the same time under the same attack that both programs are similarly effective in detecting intrusion. However, Snort has the better ability to detect an ICMP attack while the Suricata has the advantage of detecting when a TCP attack occurs.

1. บทนำ

ในปัจจุบันทุกองค์กรต่างได้ติดตั้งระบบเครือข่ายภายในขึ้นเพื่อรองรับภารกิจขององค์กรนั้น ๆ ซึ่งมีอุปกรณ์ภายในหลายชนิด เช่นอุปกรณ์เครือข่าย อุปกรณ์เครือข่ายไร้สาย เครื่องแม่ข่าย รวมไปถึงอุปกรณ์ของผู้ใช้งานภานในองค์กร เช่น เครื่องคอมพิวเตอร์เดสท็อป เครื่องคอมพิวเตอร์แลปท็อป สมาร์ทโฟน และแทบเล็ตโดยมีการเชื่อมต่อภายในเครือข่ายที่ซับซ้อน ซึ่งแต่ละหน่วยงานภายในองค์กรต่างต้องการใช้งานระบบสารสนเทศบนเครือข่ายที่มีประสิทธิภาพ แต่ภายในเครือข่ายเองก็มีการรบุกรุกโจมตีจากผู้ไม่หวังหรือการบุกรุกจากผู้ใช้งานทั่ว ๆ ไปที่ขาดความรู้ความเข้าใจในการใช้งานเครือข่าย และมีความพยายามจะบุกรุกเข้าสู่ระบบเครือข่ายภายในซึ่งอาจส่งผลร้ายแรงต่อระบบเครือข่าย เช่น เครือข่ายล่าช้า จนถึงเครือข่ายหยุดทำงานชั่วขณะ เนื่องจากความปลอดภัยของระบบเครือข่ายภายในมีความสำคัญมาก นอกจากนั้นยังควบคุมความปลอดภัยได้ยากและเป็นที่จับต้องได้ยาก ถึงแม้ว่าภายในเครือข่ายจะมีอุปกรณ์ไฟร์วอลล์ (Firewall) ในการรักษาความปลอดภัยให้ระบบเครือข่ายภายใน ซึ่งจะทำหน้าที่เปิดและปิดการเข้าถึงการเครือข่ายภายนอก (Internet) และเครือข่ายภายใน (Intranet) โดยไฟร์วอลล์จัดเป็นเทคโนโลยีที่ตอบสนองความต้องการการจัดการด้านความปลอดภัยของเครือข่ายที่เหมาะสมและสามารถแก้ปัญหาการบุกรุกจากเครือข่ายภายในออกสู่เครือข่ายภายนอกได้ หากแต่ยังมีข้อจำกัดหลายด้านที่ไฟร์วอลล์ไม่สามารถทำได้ อุปกรณ์ไฟร์วอลล์ก็ไม่ได้ทำหน้าที่ตรวจสอบเครือข่ายภายใน ที่มีความจำเป็นและสำคัญมาก จึงทำให้เกิดการตรวจจับจากเครือข่ายภายในไม่ทั่วถึงอันเป็นช่องทางให้เกิดการบุกรุกระบบเครือข่ายภายในได้

ปัญหาที่พบจึงเป็นการบุกรุกระบบเครือข่ายจากภายในเอง ที่ผู้ดูแลระบบไม่สามารถดูแลระบบได้อย่างรอบด้าน ไม่สามารถตรวจจับการบุกรุกได้อย่างแม่นยำ ถูกต้อง และทั่วถึง จึงจำเป็นที่ต้องมีอุปกรณ์ในการตรวจจับการบุกรุก (Intrusion Detection System) หรือ IDS ซึ่งเป็นระบบที่คอยตรวจจับการบุกรุกของผู้ที่ไม่ประสงค์ดี รวมไปถึงข้อมูลจำพวกไวรัสด้วย โดยสามารถทำการวิเคราะห์ข้อมูลทั้งหมดที่ผ่านเข้าออกภายในเครือข่ายว่า มีลักษณะการทำงานที่เป็นความเสี่ยงที่ก่อให้เกิดความ เสียหายต่อระบบเครือข่ายหรือไม่ รวมทั้งมีไว้เพื่อตรวจจับและวิเคราะห์ประเภทของข้อมูลเครือข่าย (Anomaly IP Packet) ที่ต้องสงสัยว่าเป็นการบุกรุกระบบหรือไม่ รวมไปถึงการจัดการกับการบุกรุกแบบใหม่ที่มีโความซับซ้อน โดย IDS จะทำหน้าที่ตรวจจับและแจ้งเตือนให้ผู้ดูแลระบบรับทราบ เพื่อดำเนินการป้องกันได้ทันท่วงที เนื่องจากในองค์กรของผู้วิจัยยังขาดอุปกรณ์ในการตรวจจับการบุกรุก และขาดความรู้ความเชี่ยวชาญเกี่ยวกับภัยคุกคามที่พบได้ใน

ภายในระบบเครือข่าย ประกอบกับงานวิจัยที่เกี่ยวข้องกับการเปรียบเทียบในเชิงประสิทธิภาพในการตรวจสอบการบุกรุกภายใต้ปัจจัยการโจมตียังไม่แพร่หลาย ที่ผู้แลระบบจะยกเอามาใช้เป็นคู่มือในการปฏิบัติงานได้

ด้วยเหตุดังกล่าว เพื่อเป็นการเพิ่มประสิทธิภาพในการดูแลระบบเครือข่ายภายใน เพื่อให้มีเครื่องมือสำหรับการตรวจจับความพยายามที่จะบุกรุกเครือข่ายและเพื่อป้องกันเครือข่าย ก่อนที่จะเกิดการโจมตีจริง เพื่อเก็บรวบรวมสถิติเกี่ยวกับความพยายามหรือการโจมตี รวมทั้งการเก็บรวบรวมสถิติเกี่ยวกับความพยายามหรือการโจมตี เพื่อนำไปวิเคราะห์ภัยคุกคามที่อาจเกิดขึ้นได้ ผู้วิจัยจึงได้เสนอแนวคิดในการเปรียบเทียบในเชิงประสิทธิภาพ สำหรับเป็นข้อมูลในเชิงเทคนิคและเพื่อการออกแบบระบบเครือข่ายที่เสริมระบบความปลอดภัยด้วย โปรแกรม Open Source IDS โดยทำการทดสอบการโจมตีตามปัจจัยต่าง ๆ ที่อาจเกิดขึ้นจริงในระบบเครือภายใน ระหว่างโปรแกรมสนอร์ท (Snort) และซูริคาต้า (Suricata) ซึ่งเป็นโปรแกรมที่เป็นที่นิยมอย่างสูง โดยมีจุดประสงค์เพื่อศึกษาความสามารถในการตรวจจับการบุกรุกในสภาพแวดล้อมของเครือข่ายจำลองเสมือนจริง (Virtual Machine) ที่มีการเปลี่ยนแปลงปัจจัยด้านการโจมตี โดยจะทำการทดสอบโปรแกรมตรวจหาการบุกรุกเครือข่ายที่ใช้เทคนิคการตรวจหาตามเงื่อนไขที่ผู้วิจัยได้ทำกำหนดแนวทางการทดลองขึ้นเอง

2. ทฤษฎีที่เกี่ยวข้อง

การรักษาความปลอดภัยในระบบเครือข่ายคอมพิวเตอร์มีความสำคัญมากในปัจจุบัน ซึ่งความพร้อมใช้งานของระบบเครือข่ายนับว่าจำเป็นมากต่อการดำเนินกิจกรรมทางธุรกิจขององค์กร ทำให้ระบบเครือข่ายจึงมีความเสี่ยงที่จะถูกโจมตีจากหลายแหล่งเช่น บุคลากรในองค์กรขาดความรู้ในการใช้งานเครือข่าย การถูกโจมตีการภายในและภายนอก การแพร่กระจายของไวรัสคอมพิวเตอร์ซึ่งอาจผ่านมาทางอีเมล หรืออาจมีผู้ไม่หวังดีพยายามที่จะเจาะระบบเข้ามาเพื่อทำลายระบบ เปลี่ยนแปลง หรือทำให้ระบบเครือข่ายใช้งานไม่ได้ชั่วขณะ ดังนั้นจึงจำเป็นต้องมีระบบการรักษาความปลอดภัยในระบบเครือข่ายคอมพิวเตอร์ที่แข็งแกร่งเพียงพอที่จะรับมือต่อภัยคุกคามต่าง ๆ ได้ ผู้ดูแลระบบจึงจำเป็นต้องทำการวิเคราะห์ความเสี่ยง [2] เพื่อออกแบบ ทำการติดตั้งระบบรักษาความปลอดภัย และเฝ้าระวังรักษาความปลอดภัยให้ระบบเครือข่ายใช้งานได้มีประสิทธิภาพตลอดเวลา การรักษาความปลดภัยจึงเป็นกระบวนการ รวมไปถึงการวิเคราะห์บริหารความเสี่ยง (Risk) ที่เกิดจากภัยคุกคาม (Threat) ช่องโหว่หรือจุดอ่อน (Vulnerability) ขององค์กร การกำหนดนโยบายรักษาความปลอดภัย การบังคับใช้นโยบาย และการเฝ้าระวังเหตุการณ์ตลอดเวลา

บุคคลที่กระทำการโจมตีหรือบุกรุกระบบเครือข่ายคอมพิวเตอร์หรือที่เรียกว่าผู้บุกรุก (Intruder) สามารถแบ่งได้เป็น 2 ประเภท คือ [3]

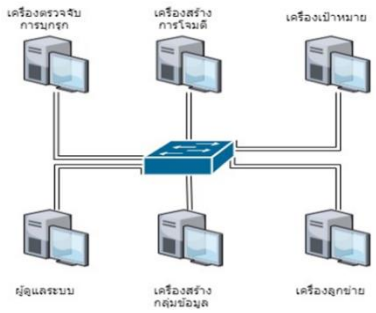
1.ผู้บุกรุกจากภายนอก (Outsider Intruder) หมายถึง ผู้บุกรุกที่มาจากภายนอกเครือข่ายขององค์กร เช่น การโจมตีโดยผ่านเครือข่ายอินเทอร์เน็ตในรูปแบบต่าง ๆ

2.ผู้บุกรุกจากภายใน (Insider Intruder) หมายถึง ผู้บุกรุกที่เป็นผู้ใช้ซึ่งมีสิทธิ์ในการใช้ระบบหรือเครือข่ายคอมพิวเตอร์ภายในองค์กร โดยรวมไปถึงผู้ใช้สิทธิ์ไปในทางที่ผิดหรือการลักลอบใช้สิทธิ์ของผู้ใช้คนอื่น ๆ

ประเภทของการโจมตี (Type of Attack) [1] หมายถึง สิ่งที่อาจจะก่อให้เกิดความเสียหายต่อคุณสมบัติของระบบเครือข่ายคอมพิวเตอร์ด้านใดด้านหนึ่งหรือ มากกว่าหนึ่งด้าน ภัยคุกคามนั้นอาจจะไม่เกิดขึ้นเลยก็ได้ถ้ามีการป้องกันที่ดี หรือถเามีการเตรียมการที่ดีเมื่อมีเหตุการณ์ เกิดขึ้นก็จะช่วยลดความเสียหายได้ การกระทำที่อาจก่อให้เกิดความเสียหายที่เรียกว่าการโจมตี (Attack) ส่วนผู้ที่เป็นเหตุให้เกิดเหตุการณ์ดังกล่าวจะเรียกว่า ผู้โจมตี (Attacker) หรือบางที่ก็เรียกว่า แฮ็กเกอร์ (Hacker) ประเภทของการโจมตี ได้แก่ การสอดแนมและการดักจับข้อมูล (Sniffing), การเปลี่ยนแปลงข้อมูล (Modification), การปลอมตัว (Spoofing), การปฏิเสธการให้บริการ (Denial of Service)

3. การดำเนินงาน

3.1 การออกระบบเพื่อใช้ในการทดลองครั้งนี้ประกอบไปด้วย เครื่องตรวจจับการบุกรุก เครื่องสร้างแพ็คเก็ตการโจมตี เครื่องเป้าหมายในการโจมตี เครื่องสำหรับผู้ดูแลระบบ เครื่องแม่ข่ายให้บริการเว็บ เครื่องลูกข่าย โดยมีส่วนประกอบของระบบทั้งหมด แสดงดังรูปที่ 3.1



รูปที่ 3.1 แสดงส่วนประกอบที่ใช้ในการทดลอง

3.1.1 เครื่องตรวจจับการบุกรุก เป็นเครื่องที่ติดโปรแกรมสนอร์ทและซูริคาต้า อย่างละ 1 เครื่อง ไว้คอยทำหน้าที่ตรวจจับการโจมตีโดยใช้กฎเกณฑ์ที่ผู้วิจัยดัดแปลงขึ้นเพื่อให้เหมาะสมกับสภาพแวดล้อม เพื่อใช้ทำการทดลอง ทำการตรวจจับการบุกรุกพร้อมกับบันทึกการใช้งานหน่วยประมวล (CPU) ของเครื่องไว้

3.1.2 เครื่องสร้างแพ็คเก็ตการโจมตี ทำหน้าที่ในการสร้างแพ็คเก็ต (Packet) เพื่อใช้โจมตีเป้าหมาย ระหว่างทำการทดลองนั้นจะทำการบันทึกปริมาณแพ็คเก็ตที่เกิดขึ้น เพื่อนำว่าคำนวณหาอัตราความเร็วในการโจมตี

3.1.3 เครื่องเป้าหมายในการโจมตี ทำหน้าที่เป็นเป้าหมายเพื่อรองรับการโจมตี พร้อมทั้งทำการบันทึกปริมาณข้อมูลที่เกิดขึ้น

3.1.4 เครื่องสำหรับผู้ดูแลระบบ ทำหน้าที่คอยตรวจสอบการโจมตี และทำหน้าที่บันทึกปริมาณข้อมูลที่เกิดขึ้นในขณะทำการทดลอง

3.1.5 เครื่องสร้างแพ็กเก็ต ทำหน้าที่ให้สร้างแพ็กเก็ตสำหรับส่งเข้าระบบบริการเว็บไซต์เพื่อสร้างสถานการณ์จำลองเสมือนมีการใช้งานจริง พร้อมบันทึกปริมาณข้อมูลที่เกิดขึ้น

3.1.6 เครื่องลูกข่าย ทำหน้าที่ติดต่อกับเครื่องแม่ข่าย เพื่อสร้างสถานการณ์จำลองเสมือนมีการใช้งานจริง โดยใช้ครื่องสร้างแพ็กเก็ตสร้างปริมาณข้อมูลภายในระบบเครือข่ายการโจมตีเครือข่าย

3.2 วิธีการทดลองตามลักษณะที่กำหนด

การทดลองเพื่อเป็นการทดสอบการตรวจจับของโปรแกรมตรวจหาการบุกรุก กระบวนการทำงานเริ่มจากผู้โจมตีในลักษณะ ต่างๆ ดังนี้ การโจมตีด้วยการสร้างการเชื่อมต่อจำนวนมา (TCP SYN Flood) การโจมตีด้วยแพ็กเก็ตจำนวนมาก (ICMP Ping Flood) การโจมตีด้วยการส่งข้อมูลจำนวนมากโดยไม่ขึ้นอยู่กับแบนด์วิดท์ (Smurf Attack) และการโจมตีด้วยการกราดตรวจทีซีพีพอร์ต (TCP Scan Port) ไปยังเป้าหมายในรูปแบบต่างๆ ตามที่ได้กำหนดไว้เพื่อใช้ทดสอบประสิทธิภาพของโปรแกรมตรวจหาการบุกรุก ในการตรวจหาการโจมตีที่จำลองระบบขึ้นมาเพื่อใช้ในการทดลอง โดยในการทดลองนี้จะแบ่งการทดลองออกเป็นดังนี้

การโจมตี	TCP Scan Port		TCP SYN Flood		ICMP Flood		Smurf	
รูปแบบการโจมตี / ผลการทดลอง	สนอร์ท	ชูริคาต้า	สนอร์ท	ชูริคาต้า	สนอร์ท	ชูริคาต้า	สนอร์ท	ชูริคาต้า
ความสามารถในการตรวจวิเคราะห์ (%)	30	39	3.16	3.27	14.80	15.32	25.31	26.19
การตรวจพบการโจมตีได้รวดเร็ว (sec)	2	2	2	4	2	3	2	4
การแจ้งเตือนเกินจริง (%)	0	0	0	0	0	0	0	0
การแจ้งเตือนทุกครั้งเมื่อถูกโจมตี (%)	1.2	1.55	1.49	1.6	83.33	91.66	31.2	34.32
ความถูกต้องของการแจ้งเตือน	ถูกต้อง	ถูกต้อง	ถูกต้อง	ถูกต้อง	ถูกต้อง	ถูกต้อง	ถูกต้อง	ถูกต้อง
การใช้งานหน่วยประมวลผล (%)	2	12	100	100	100	100	93	100

3.2.1 การทดสอบการทำงานของโปรแกรมตรวจหาการบุกรุกในสภาพแวดล้อมของการโจมตีชนิดเดียวที่ไม่มีข้อมูลหรือการโจมตีอื่นปะปน เป็นการทดสอบเพื่อหาความสัมพันธ์ระหว่างความเร็วในการโจมตีกับความสามารถในการตรวจวิเคราะห์ ความถูกต้องของข้อความแจ้งเตือนและระยะเวลาที่ใช้ในการตรวจหาโดยสภาพแวดล้อมของการทดลองประกอบด้วยผู้โจมตี ผู้ถูกโจมตี โปรแกรมตรวจหาการบุกรุก เครื่องเฝ้าตรวจสอบเครือข่าย การทดสอบเริ่มจากผู้โจมตีส่งการโจมตีไปยังเป้าหมายด้วยความเร็วในการโจมตีที่แตกต่างกัน การเปลี่ยนแปลงความเร็วในการโจมตีจะทำโดยเพิ่มจำนวนผู้โจมตีและจำนวนเซสชันของการโจมตี [4]

3.3.2 การทดสอบการทำงานของโปรแกรมตรวจหาการบุกรุกในสภาพแวดล้อมของการโจมตีชนิดเดียวมีข้อมูล เป็นทดสอบการทำงานของโปรแกรมตรวจหาการบุกรุกในสภาพแวดล้อมเสมือนจริง เพื่อทดสอบว่าข้อมูลจำนวนมากที่ปะปนอยู่จะมีผลต่อความสามารถในการตรวจหาหรือไม่ สภาพแวดล้อมของการทดลองนี้จะคล้ายกับสภาพแวดล้อมที่ใช้ในการทดลองแรกแต่จะเพิ่มเติมในส่วนของการรับ-ส่งข้อมูล โดยให้เครื่องสร้างแพ็กเก็ต ทำการสร้างปริมาณข้อมูลส่งเข้ามาในระบบเครือข่าย เป็นการสร้างสถานการณ์จำลองเสมือนว่ามีการใช้งานเครือข่ายจริง

4. ผลทดการสอบ

จากผลการทดลองสามารถนำมาเปรียบเทียบประสิทธิภาพของโปรแกรมสนอร์ทและโปรแกรมซูริคาต้า ได้ว่าแต่ละโปรแกรมต่างก็มีจุดเด่นในการทำงานที่แตกต่างกัน เช่น เมื่อพิจารณาความสามารถในการตรวจวิเคราะห์ ทั้งสองโปรแกรมมีความสามารถในการตรวจวิเคราะห์ที่ค่อนข้างใกล้เคียงกัน ผลการทดลองที่ออกมาทำให้โปรแกรมมีความสามารถที่ดีทั้งคู่ในเรื่องการตรวจพบการโจมตีได้รวดเร็ว ทั้งสองโปรแกรมมีอัตราการตรวจจับที่ค่อนข้างเร็วน่าเชื่อถือมาก โดยมีอัตราเริ่มการแจ้งเตือนไม่เกินกว่า 2 วินาที ในส่วนของการแจ้งเตือนเกินจริงในการทดลองครั้งนี้ไม่พบการแจ้งเตือนเกินจริง เช่นเดียวกับการแจ้งเตือนทุกครั้งและความถูกต้องในการแจ้งเตือน ทั้งสองโปรแกรมก็มีการแจ้งเตือนทุกครั้งและถือได้ว่ามีความถูกต้องของการแจ้งเตือน จึงถือว่าทั้งสองโปรแกรมมีการแจ้งเตือนที่น่าเชื่อถือ สำหรับการใช้งานหน่วยประมวลผล แม้ว่าโปรแกรมสนอร์ทจะมีอัตราการใช้งานหน่วยประมวลผลที่ค่อนข้างต่ำกว่า หากพิจารณาที่การโจมตีที่มีอัตราเร็วต่ำ แต่หากเปรียบเทียบความต้องการใช้ความสามารถในการตรวจจับการโจมตีที่มีอัตราการโจมตีเร็วสูง ทั้งสองโปรแกรมจะมีอัตราการใช้งานหน่วยประมวลผลสูงไม่แตกต่างกัน โดยผลการทดลองสามารถสรุปได้ดังตารางที่ 4.1

ตารางที่ 4.1 ผลการเปรียบเทียบประสิทธิภาพ

5. ข้อเสนอแนะ

5.1 ในงานวิจัยฉบับนี้ ได้ทำการทดลองระบบทั้งหมด โดยการสร้างระบบจำลองขึ้นมาทั้งหมด ทั้งเครื่องแม่ข่าย เครื่องของผู้โจมตี เครื่องเป้าหมาย เป็นต้น ทำให้เกิดปัญหาการแบ่งการ

ทำงานของฮาร์ดดิสก์แบบงานแม่เหล็ก เกิดปัญหาในการเข้าถึงข้อมูลแต่ละครั้ง มีการหน่วงเวลาเกิดขึ้น ทำให้เกิดความล่าช้าในการทดลอง ซึ่งส่งผลกระทบต่อการทดลอง ทำให้การบันทึกเวลามีความเป็นไปได้ที่ไม่ตรงกับความเป็นจริง

5.2 การผลการทดลองสามารถให้การคาดคะเนตามหลักเหตุผลได้ว่า หากองค์กรนั้นต้องการใช้ระบบตรวจกับการบุกรุกที่มีลักษณะเข้ามาโจมตีระบบเครือข่ายที่เน้นไปทางด้าน TCP โปรแกรมสนอร์ทมีผลการทดลองในด้านนี้เด่นชัดกว่า แต่หากว่าองค์กรนั้นมีการบุกรุกในส่วนที่เป็นโปรแกรมประยุกต์มากกว่า หรือมีการโจมตีที่เป็นแบบ ICMP กลับเป็นโปรแกรมซูริคาต้าที่มีผลการทดลองดีกว่า

5.3 ในการออกแบบระบบตรวจจับการบุกรุกควรต้องมีการทดสอบความเป็นได้ของระบบเสียก่อน (Proof Of Concept) ว่าระบบไหนหรือโปรแกรมไหนที่จะเหมาะสมกับระบบเครือข่ายที่องค์กรจะนำไปประยุกต์ใช้ เนื่องจากแต่ละโปรแกรมมีความแตกต่าง ซึ่งแต่ละโปรแกรมก็อาจจะไม่เหมาะสมกับแต่ละสภาพแวดล้อม ดังนั้นในการการเลือกผลิตภัณฑ์ของยี่ห้อใด ซึ่งที่ต้องพิจารณาประกอบก็คือ ในองค์กรได้มีผลิตภัณฑ์ด้านความปลอดภัยของระบบเครือข่ายประเภทไหนอยู่บ้าง การออกแบบระบบเครือข่าย ปริมาณของข้อมูลที่ไหลผ่านการจราจรของระบบเครือข่าย เป็นต้น

5.4 ในการเลือกใช้ระบบตรวจจับการบุกรุกแบบไหนหรือผลิตภัณฑ์จากผู้ผลิตรายไหน สิ่งที่ต้องพิจารณาอีกหนึ่งปัจจัยคือ เรื่องของการพัฒนากฎเกณฑ์เพื่อให้รองรับกับการโจมตีในรูปแบบต่างๆ เนื่องจากแต่ละผลิตภัณฑ์ก็มีทั้งข้อดีและข้อกำจัดที่แตกต่างกัน เช่น ผลิตภัณฑ์โปรแกรมสนอร์ท ให้ใช้กฎเกณฑ์ได้ฟรีรวมทั้งมีผู้พัฒนากฎเกณฑ์เพื่อจำหน่ายแบบเสียค่าใช้จ่ายในเรื่องลิขสิทธิ์ (License) ผลิตภัณฑ์โปรแกรมซูริคาต้ายินยอมให้ใช้กฎเกณฑ์แบบไม่มีค่าใช้จ่ายเพียง 30-60 วัน หากต้องให้ใช้เกินกว่านั้นต้องมีค่าใช้จ่ายในเรื่องของลิขสิทธิ์ในการใช้งาน เป็นต้น

6. อ้างอิง

[1] จตุพร แพงจันทร์. (2551). เจาะระบบ Network 2nd Edition. นนทบุรี : ไอดีซีฯ.

[2] เอกสารออนไลน์ (13 มกราคม 2563). สำนักเทคโนโลยีสารสนเทศและการสื่อสาร_km11-59.pdf สืบค้นจาก https://www.senate.go.th/assets/portals/49/files/handbook/km59/

[3] เอกสารออนไลน์ (13 มกราคม 2563). สืบค้นจากhttp://kb.psu.ac.th/psukb/bitstream/2553/2128/9/271644_ch2.pdf

[4] กาญจนา ศิลาวราเวทย์. (2545). การเปรียบเทียบโปรแกรมตรวจหาการบุกรุกเครือข่ายระหว่างโปรแกรมสนอร์ทและเรียลซีเคียวภายใต้ปัจจัยการโจมตี . กรุงเทพมหานคร: จุฬาลงกรณ์มหาวิทยาลัย.