การเปรียบเทียบประสิทธิภาพ ระบบการตรวจจับการบุกรุกที่เหมาะสมในองค์กรขนาดกลาง

นายวุฒิฉัตร รุ่งวัฒนาพร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568
ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

การเปรียบเทียบประสิทธิภาพ ระบบการตรวจจับการบุกรุกที่เหมาะสมในองค์กรขนาดกลาง

นายวุฒิฉัตร รุ่งวัฒนาพร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568
ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ใบรับรองวิทยานิพนธ์

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง การเปรียบเทียบประสิทธิภาพ ระบบการตรวจจับการบุกรุกที่เหมาะสมในองค์กรขนาดกลาง

โดย นายวุฒิฉัตร รุ่งวัฒนาพร

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

คณบดีบัณฑิตวิทยาลัย / หัวหน้าภาควิชา

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ

(เทอดพงษ์ แดงสี)

..... อาจารย์ที่ปรึกษา

(พงษ์พิสิฐ วุฒิดิษฐโชติ)

..... กรรมการ

(นวพร วิสิฐพงศ์พันธ์)

ชื่อ : นายวุฒิฉัตร รุ่งวัฒนาพร
ชื่อวิทยานิพนธ์ : การเปรียบเทียบประสิทธิภาพ ระบบการตรวจจับการบุกรุกที่เหมาะสมในองค์กรขนาดกลาง
สาขาวิชา : การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก : พงษ์พิสิฐ วุฒิดิษฐโชติ
ปีการศึกษา : 2568

บทคัดย่อ

การโจมตีทางไซเบอร์ที่พุ่งเป้าไปยังโครงสร้างพื้นฐานขององค์กรมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง โดยเฉพาะองค์กรขนาดกลางที่อาจมีทรัพยากรจำกัดในการป้องกันภัยคุกคามทางไซเบอร์ รวมถึงบุคคลากรที่ขาดความรู้ความสามารถในด้านความมั่นคงปลอดภัยไซเบอร์ การค้นคว้าอิสระนี้เพื่อจุดประสงค์ ในการเปรียบเทียบประสิทธิภาพของ ระบบตรวจจับการบุกรุก (Intrusion Detection System) ที่เหมาะสมสำหรับองค์กรขนาดกลางเพื่อตรวจจับการบุกรุก โดยได้คัดเลือกจำนวน 3 ระบบ ได้แก่ Snort, Suricata และ Zeek สำหรับการตรวจจับการบุกรุกในประเภทต่างๆ ซึ่งได้แก่ ICMP Ping Flood, Smurf Attack, TCP Port Scanning, TCP SYN Flood, Brute Force Attack, SQL Injection และ Cross-Site Scripting เพื่อนำมาศึกษาเปรียบเทียบ

การทดสอบดำเนินการในสภาพแวดล้อมจำลอง (Virtual Environment) ที่ออกแบบให้ใกล้เคียงกับระบบเครือข่ายขององค์กรขนาดกลาง โดยใช้เครื่องมือทดสอบเจาะระบบเพื่อสร้างทราฟฟิกที่เป็นอันตราย จากนั้นวิเคราะห์ประสิทธิภาพของแต่ละ ระบบตรวจจับการบุกรุก ผ่านเกณฑ์การวัดที่มีความสำคัญ ได้แก่ อัตราการตรวจจับ (Detection Rate), อัตราความผิดพลาด (False Negative Rate), ความแม่นยำ (Accuracy), คะแนน F1 (F1 Score) เวลาตอบสนอง, ประสิทธิภาพของระบบ ความสามารถในการปรับขนาด และ การบำรุงรักษาและการปรับปรุง

การค้นคว้าอิสระนี้ช่วยให้องค์กรขนาดกลางสามารถเลือกใช้ ระบบตรวจจับการบุกรุกที่มีความเหมาะสมกับสภาพแวดล้อมของตนได้อย่างมีประสิทธิภาพมากขึ้น เพื่อลดความเสี่ยงจากการโจมตีทางไซเบอร์และเพิ่มความปลอดภัยให้กับระบบเครือข่ายและองค์กร

(มีจำนวนทั้งสิ้น 63 หน้า)

คำสำคัญ : ระบบตรวจจับการบุกรุก การเปรียบเทียบประสิทธิภาพ องค์กรขนาดกลาง

_____ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

Name : Mr. Wuttichat Rungwattanaporn
Thesis Title : Performance Comparison of Intrusion Detection Systems for Medium-Sized Organizations
Major Field : Network and Information Security Management
King Mongkut's University of Technology North Bangkok
Thesis Advisor : Pongpisit Wuttidittachotti
Academic Year : 2025

ABSTRACT

Cyberattacks targeting organizational infrastructure are on the rise, particularly for medium-sized organizations that often have limited resources and insufficient cybersecurity expertise. This independent study aims to compare the performance of Intrusion Detection Systems (IDS) suitable for medium-sized organizations. The selected IDS tools—Snort, Suricata, and Zeek—are evaluated for their ability to detect various types of cyberattacks, including ICMP Ping Flood, Smurf Attack, TCP Port Scanning, TCP SYN Flood, Brute Force Attack, SQL Injection, and Cross-Site Scripting.

The evaluation was conducted in a virtual environment designed to closely mimic the network setup of a medium-sized organization. Penetration testing tools were used to generate malicious traffic, and the effectiveness of each IDS was measured based on several key performance indicators: accuracy, detection rate, false positive rate, false negative rate, F-score, response time, system efficiency, scalability, and ease of maintenance and updates.

The results of this study provides valuable insights for medium-sized organizations in selecting the most appropriate IDS for their environments, thereby reducing the risk of cyber threats and enhancing overall network security.

(Total 63 Pages)

Keywords: Intrusion Detection, Performance Comparison, Medium-Sized Organizations

_____ Advisor

กิตติกรรมประกาศ

ขอกราบขอบพระคุณ รองศาสตราจารย์ ว่าที่ร้อยตรี ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ อาจารย์ที่ปรึกษาการค้นคว้าอิสระ ที่ได้กรุณาให้คำแนะนำ อธิบายแนวทาง พร้อมทั้งให้ข้อเสนอแนะที่มีคุณค่าอย่างยิ่งตลอดระยะเวลาการดำเนินงาน ตั้งแต่เริ่มต้นการกำหนดหัวข้อ จนถึงกระบวนการวิเคราะห์และสรุปผลการศึกษา ด้วยความใส่ใจ เอาใจใส่ และให้การสนับสนุนอย่างเต็มกำลังในทุกขั้นตอน ซึ่งเป็นปัจจัยสำคัญที่ก่อให้เกิดความเข้าใจในเนื้อหาและกระบวนการวิจัยอย่างถ่องแท้ อันนำไปสู่ความสำเร็จของการดำเนินการค้นคว้าอิสระในหัวข้อ “การเปรียบเทียบประสิทธิภาพระบบการตรวจจับการบุกรุกที่เหมาะสมในองค์กรขนาดกลาง” ให้บรรลุ Behavioral Analysis ตามที่ตั้งใจไว้ได้อย่างสมบูรณ์

ขอกราบขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.เทอดพงษ์ แดงสี ประธานกรรมการสอบ และ ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์ กรรมการสอบ ที่ได้กรุณาสละเวลาอันมีค่าในการพิจารณาผลงาน พร้อมทั้งให้ข้อเสนอแนะอันเป็นประโยชน์ยิ่ง ซึ่งมีส่วนสำคัญอย่างยิ่งในการพัฒนาคุณภาพของผลงานให้มีความสมบูรณ์ยิ่งขึ้น ทั้งในด้านเนื้อหา กระบวนการวิเคราะห์ และการนำเสนอผลลัพธ์ นอกจากนี้ ขอขอบพระคุณคณาจารย์ทุกท่าน เพื่อนนักศึกษา ตลอดจนผู้มีส่วนเกี่ยวข้องทุกฝ่าย ที่ได้ให้การสนับสนุน ให้คำแนะนำ และส่งมอบกำลังใจด้วยความเมตตาและจริงใจตลอดระยะเวลาการจัดทำผลงานฉบับนี้ ความช่วยเหลือและแรงสนับสนุนจากทุกท่านล้วนเป็นพลังใจสำคัญที่ผลักดันให้สามารถดำเนินงานให้สำเร็จลุล่วงไปด้วยดี

วุฒิฉัตร รุ่งวัฒนาพร

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง (ถ้ามี)

สารบัญรูปภาพ (ถ้ามี)

สารบัญภาพ (ต่อ)

ภาพที่ หน้า

พระจอมเกล้าพระนครเหนือ
มหาวิทยาลัยเทคโนโลยี

บรรณานุกรม

พิมพ์รายการอ้างอิงลงในนี้ หรือทำการย้ายรายการอ้างอิงที่สร้างจาก Endnote หรือ Zotero ท้ายเล่มมายังบริเวณนี้

ภาคผนวก

หากมีภาคผนวกให้จัดทำเนื้อหาบริเวณนี้ หากไม่มีสามารถลบหน้านี้ทิ้งได้เลย

ประวัติผู้เขียน

ชื่อ	นายวุฒิฉัตร รุ่งวัฒนาพร
ชื่อวิทยานิพนธ์	การเปรียบเทียบประสิทธิภาพ ระบบการตรวจจับการบุกรุกที่เหมาะสมใน องค์กรขนาดกลาง
สาขาวิชา	การบริหารเครือข่าย และความมั่นคงปลอดภัยสารสนเทศ
ประวัติ	**ประวัติการศึกษา** สำเร็จการศึกษาระดับปริญญาตรี สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยราชภัฏพระนคร **ประวัติการทำงาน** พ.ศ. 2564 – ปัจจุบัน ทำงานบริษัท ซันเดย์ ประกันภัย (ประเทศไทย) จำกัด (มหาชน) **สถานที่ติดต่อปัจจุบัน** 199/119 หมู่บ้าน Centro ราชพฤกษ์ 2 ซอย 17 บางกร่าง เมืองนนทบุรี 11110

การเปรียบเทียบประสิทธิภาพ ระบบการตรวจจับการบุกรุกที่เหมาะสมในองค์กรขนาดกลาง

นายวุฒิฉัตร รุ่งวัฒนาพร

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่าย และความมั่นคงปลอดภัยสารสนเทศ
ภาควิชาการบริหารเครือข่ายดิจิทัล และความมั่นคงปลอดภัยสารสนเทศ
คณะเทคโนโลยีสารสนเทศ และนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567
ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ชื่อ : นายวุฒิฉัตร รุ่งวัฒนาพร
ชื่อการค้นคว้าอิสระ : การเปรียบเทียบประสิทธิภาพ ระบบการตรวจจับการบุรุกที่เหมาะสมในองค์กรขนาดกลาง
สาขาวิชา : การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
อาจารย์ที่ปรึกษาการค้นคว้าอิสระ : รองศาสตราจารย์ ว่าที่ร้อยตรี ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ
ปีการศึกษา : 2567

บทคัดย่อ

การโจมตีทางไซเบอร์ที่พุ่งเป้าไปยังโครงสร้างพื้นฐานขององค์กรมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง โดยเฉพาะองค์กรขนาดกลางที่อาจมีทรัพยากรจำกัดในการป้องกันภัยคุกคามทางไซเบอร์รวมถึงบุคคลากรที่ขาดความรู้ความสามารถในด้านความมั่นคงปลอดภัยไซเบอร์ การค้นคว้าอิสระนี้เพื่อจุดประสงค์ ในการเปรียบเทียบประสิทธิภาพของ ระบบตรวจจับการบุกรุก (Intrusion Detection System) ที่เหมาะสมสำหรับองค์กรขนาดกลางเพื่อตรวจจับการบุกรุก โดยได้คัดเลือก จำนวน 3 ระบบ ได้แก่ Snort, Suricata และ Zeek สำหรับการตรวจจับการบุกรุกในประเภทต่างๆ ซึ่งได้แก่ ICMP Ping Flood, Smurf Attack, TCP Port Scanning, TCP SYN Flood, Brute Force Attack, SQL Injection และ Cross-Site Scripting เพื่อนำมาศึกษาเปรียบเทียบ

การทดสอบดำเนินการในสภาพแวดล้อมจำลอง (Virtual Environment) ที่ออกแบบให้ใกล้เคียงกับระบบเครือข่ายขององค์กรขนาดกลาง โดยใช้เครื่องมือทดสอบเจาะระบบเพื่อสร้างทราฟฟิกที่เป็นอันตราย จากนั้นวิเคราะห์ประสิทธิภาพของแต่ละ ระบบตรวจจับการบุกรุก ผ่านเกณฑ์การวัดที่มีความสำคัญ ได้แก่ อัตราการตรวจจับ (Detection Rate), อัตราความผิดพลาด (False Negative Rate), ความแม่นยำ (Accuracy), คะแนน F1 (F1 Score) เวลาตอบสนอง, ประสิทธิภาพของระบบ ความสามารถในการปรับขนาด และ การบำรุงรักษาและการปรับปรุง

การค้นคว้าอิสระนี้ช่วยให้องค์กรขนาดกลางสามารถเลือกใช้ ระบบตรวจจับการบุกรุกที่มีความเหมาะสมกับสภาพแวดล้อมของตนได้อย่างมีประสิทธิภาพมากขึ้น เพื่อลดความเสี่ยงจากการโจมตีทางไซเบอร์และเพิ่มความปลอดภัยให้กับระบบเครือข่ายและองค์กร

(การค้นคว้าอิสระมีจำนวนทั้งสิ้น 63 หน้า)

คำสำคัญ : ระบบตรวจจับการบุกรุก การเปรียบเทียบประสิทธิภาพ องค์กรขนาดกลาง

_____อาจารย์ที่ปรึกษาการค้นคว้าอิสระ

Name : Mr. Wuttichat Rungwattanaporn
Independent Study Title : Performance Comparison of Intrusion Detection Systems for Medium-Sized Organizations
Major Field : Digital Network and Information Security Management
King Mongkut's University of Technology North Bangkok
Independent Study Advisor : Assoc. Prof. Dr. Pongpisit Wuttidittachotti
Academic Year : 2024

Abstract

Cyberattacks targeting organizational infrastructure are on the rise, particularly for medium-sized organizations that often have limited resources and insufficient cybersecurity expertise. This independent study aims to compare the performance of Intrusion Detection Systems (IDS) suitable for medium-sized organizations. The selected IDS tools—Snort, Suricata, and Zeek—are evaluated for their ability to detect various types of cyberattacks, including ICMP Ping Flood, Smurf Attack, TCP Port Scanning, TCP SYN Flood, Brute Force Attack, SQL Injection, and Cross-Site Scripting.

The evaluation was conducted in a virtual environment designed to closely mimic the network setup of a medium-sized organization. Penetration testing tools were used to generate malicious traffic, and the effectiveness of each IDS was measured based on several key performance indicators: accuracy, detection rate, false positive rate, false negative rate, F-score, response time, system efficiency, scalability, and ease of maintenance and updates.

The results of this study provides valuable insights for medium-sized organizations in selecting the most appropriate IDS for their environments, thereby reducing the risk of cyber threats and enhancing overall network security.

(Total 63 pages)

Keywords : Intrusion Detection, Performance Comparison, Medium-Sized Organizations

_____Advisor

กิตติกรรมประกาศ

ขอกราบขอบพระคุณ รองศาสตราจารย์ ว่าที่ร้อยตรี ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ อาจารย์ที่ปรึกษาการค้นคว้าอิสระ ที่ได้กรุณาให้คำแนะนำ อธิบายแนวทาง พร้อมทั้งให้ข้อเสนอแนะที่มีคุณค่าอย่างยิ่งตลอดระยะเวลาการดำเนินงาน ตั้งแต่เริ่มต้นการกำหนดหัวข้อ จนถึงกระบวนการวิเคราะห์และสรุปผลการศึกษา ด้วยความใส่ใจ เอาใจใส่ และให้การสนับสนุนอย่างเต็มกำลังในทุกขั้นตอน ซึ่งเป็นปัจจัยสำคัญที่ก่อให้เกิดความเข้าใจในเนื้อหาและกระบวนการวิจัยอย่างถ่องแท้ อันนำไปสู่ความสำเร็จของการดำเนินการค้นคว้าอิสระในหัวข้อ “การเปรียบเทียบประสิทธิภาพระบบการตรวจจับการบุกรุกที่เหมาะสมในองค์กรขนาดกลาง” ให้บรรลุ Behavioral Analysis ตามที่ตั้งใจไว้ได้อย่างสมบูรณ์

ขอกราบขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.เทอดพงษ์ แดงสี ประธานกรรมการสอบ และผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์ กรรมการสอบ ที่ได้กรุณาสละเวลาอันมีค่าในการพิจารณาผลงาน พร้อมทั้งให้ข้อเสนอแนะอันเป็นประโยชน์ยิ่ง ซึ่งมีส่วนสำคัญอย่างยิ่งในการพัฒนาคุณภาพของผลงานให้มีความสมบูรณ์ยิ่งขึ้น ทั้งในด้านเนื้อหา กระบวนการวิเคราะห์ และการนำเสนอผลลัพธ์ นอกจากนี้ ขอขอบพระคุณคณาจารย์ทุกท่าน เพื่อนนักศึกษา ตลอดจนผู้มีส่วนเกี่ยวข้องทุกฝ่าย ที่ได้ให้การสนับสนุน ให้คำแนะนำ และส่งมอบกำลังใจด้วยความเมตตาและจริงใจตลอดระยะเวลาการจัดทำผลงานฉบับนี้ ความช่วยเหลือและแรงสนับสนุนจากทุกท่านล้วนเป็นพลังใจสำคัญที่ผลักดันให้สามารถดำเนินงานให้สำเร็จลุล่วงไปด้วยดี

วุฒิฉัตร รุ่งวัฒนาพร

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพ

ภาพที่ หน้า

สารบัญภาพ (ต่อ)

ภาพที่ หน้า

พระจอมเกล้าพระนครเหนือ
มหาวิทยาลัยเทคโนโลยี

บทที่ 1
บทนำ

1.1 ความเป็นมา และความสำคัญของปัญหา

ในยุคปัจจุบัน เทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานขององค์กรต่าง ๆ โดยเฉพาะระบบเครือข่ายคอมพิวเตอร์ที่เป็นโครงสร้างพื้นฐานสำคัญในการเชื่อมโยงข้อมูลและการสื่อสารระหว่างหน่วยงาน อย่างไรก็ตาม ระบบเครือข่ายมักตกเป็นเป้าหมายของผู้ไม่ประสงค์ดีที่พยายามเข้าถึงข้อมูลหรือแทรกแซงการทำงานของระบบเครือข่ายด้วยวิธีการต่าง ซึ่งล้วนส่งผลต่อประสิทธิภาพของระบบเครือข่าย ความมั่นคงปลอดภัย และความเชื่อมั่นต่อระบบสารสนเทศขององค์กร [2], [4]

แม้ว่าปัจจุบันองค์กรส่วนใหญ่จะมีการใช้งานอุปกรณ์รักษาความปลอดภัยขั้นพื้นฐาน เช่น ไฟร์วอลล์ (Firewall) เพื่อตรวจสอบ คัดกรองและควบคุมการเข้าถึงเครือข่ายจากภายนอก แต่ไฟร์วอลล์นั้นยังมีข้อจำกัดในการตรวจจับภัยคุกคามที่แฝงตัวมาในรูปแบบซับซ้อน หรือการโจมตีจากภายในเครือข่ายเอง ซึ่งผู้ดูแลระบบอาจไม่สามารถรับรู้หรือป้องกันได้อย่างทันท่วงที [2], [6]

ดังนั้น การนำระบบตรวจจับการบุกรุก (Intrusion Detection System) มาใช้จึงเป็นทางเลือกที่มีประสิทธิภาพในการเสริมสร้างความมั่นคงปลอดภัยของระบบเครือข่าย โดยระบบตรวจจับการบุกรุกนั้น มีความสามารถในการตรวจสอบ วิเคราะห์ และแจ้งเตือนเมื่อมีพฤติกรรม เหตุการณ์ที่ผิดปกติหรือเข้าข่ายเป็นการโจมตี เช่น การเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต การส่งข้อมูลที่มีรูปแบบผิดปกติ การกระทำที่เข้าข่ายเป็นภัยคุกคามอื่น ๆ รวมถึงการโจมตีทางคอมพิวเตอร์ (Computer Attack) [6], [13], [17] ระบบตรวจจับการบุกรุกจึงมีบทบาทสำคัญในการช่วยให้ผู้ดูแลระบบสามารถรับมือกับเหตุการณ์ด้านความปลอดภัยได้อย่างทันท่วงทีและมีประสิทธิภาพ

อย่างไรก็ตาม จากการสำรวจพบว่า ในองค์กรของขนาดกลางต่าง ๆ ยังไม่มีการใช้งานระบบตรวจจับการบุกรุก อีกทั้งบุคลากรยังขาดความรู้ ความเข้าใจ และความเชี่ยวชาญในการวิเคราะห์และรับมือกับภัยคุกคามทางไซเบอร์ ส่งผลให้ระบบเครือข่ายยังคงมีความเสี่ยงต่อการถูกโจมตี [2], [4] นอกจากนี้ งานวิจัยที่เกี่ยวข้องกับการประเมินและเปรียบเทียบประสิทธิภาพของระบบ โดยเฉพาะในบริบทขององค์กรขนาดเล็กหรือเครือข่ายภายใน ยังมีไม่มาก พร้อมทั้งยังไม่ครอบคลุมต่อความต้องการของผู้ดูแลระบบในการเลือกใช้งานจริง [1] , [3], [10], [16]

จากปัญหาดังกล่าว ผู้ทำการวิจัยจึงเล็งเห็นถึงความสำคัญของการศึกษาประสิทธิภาพของระบบตรวจจับการบุกรุกในองค์กรของขนาดกลาง เพื่อประเมินความสามารถในการตรวจจับภัยคุกคามที่อาจเกิดขึ้นในระบบเครือข่ายภายในองค์กร และเพื่อเป็นแนวทางในการเลือกใช้งานระบบที่เหมาะสม อันจะนำไปสู่การเพิ่มความมั่นคงปลอดภัยในเครือข่ายสารสนเทศได้อย่างยั่งยืนและมีประสิทธิภาพ [9], [10]

นอกจากนี้ ผลลัพธ์จากการศึกษายังสามารถนำไปประยุกต์ใช้เพื่อสนับสนุนการวางแผนด้านความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับกรอบแนวทางของมาตรฐานสากล เช่น NIST Cybersecurity Framework ซึ่งให้ความสำคัญกับการระบุ (Identify) ป้องกัน (Protect) ตรวจจับ (Detect) ตอบสนอง (Respond) และฟื้นฟู (Recover) รวมถึงมาตรฐาน ISO/IEC 27001 ซึ่งเน้นการจัดการความมั่นคงปลอดภัยของสารสนเทศอย่างเป็นระบบ โดยเฉพาะในด้านการควบคุมความเสี่ยงและการตรวจสอบเหตุการณ์ความปลอดภัย ซึ่งการประเมินและเลือกใช้ระบบตรวจจับการบุกรุกที่เหมาะสม ถือเป็นส่วนสำคัญในการเสริมสร้างระบบป้องกันเชิงรุก และเพิ่มศักยภาพของการบริหารจัดการด้านความมั่นคงปลอดภัยในภาพรวมขององค์กรได้อย่างมีประสิทธิผล [6], [14]

1.2 วัตถุประสงค์

1.2.1 เพื่อเปรียบเทียบประสิทธิภาพ ระบบการตรวจจับการบุกรุกที่เหมาะสมในการนำมาใช้งานภายในองค์กรขนาดกลาง

1.2.2 เพื่อวัดประสิทธิภาพ ความสามารถ และ ความถูกต้องในการตรวจจับการบุกรุกด้วยระบบตรวจจับการบุกรุก

1.2.3 เพื่อเป็นแนวทางในการเลือกใช้งาน ระบบการตรวจจับการบุกรุกที่เหมาะสมในการนำมาใช้งานภายในองค์กรขนาดกลาง

1.2.4 เพื่อใช้เป็นข้อมูลประกอบการวิเคราะห์และทำความเข้าใจรูปแบบของการบุกรุกในระบบเครือข่าย อันจะนำไปสู่การพัฒนามาตรการป้องกันและตรวจจับที่มีประสิทธิภาพมากยิ่งขึ้น

1.3 ขอบเขตการวิจัย

1.3.1 ศึกษาค้นคว้าเกี่ยวกับระบบการตรวจจับการบุกรุก

1.3.2 คัดเลือกระบบการตรวจจับการบุกรุกที่จะนำมาใช้ในการเปรียบเทียบโดย ระบบต้องสอดคล้องกับองค์กรขนาดกลาง

1.3.3 ประเภทของการโจมตีที่นำมาทดสอบ โดยคัดเลือกมาทั้งหมด 7 ประเภท ได้แก่

ก) ทีซีพีซินฟลัด (TCP SYN Flood)

ข) ทีซีพีพอร์ตสแกน (TCP Port Scan)

ค) สมิร์ฟแอตแทค (Smurf Attack)

ง) ไอซีเอ็มพีพิงฟลัด (ICMP Ping Flood)

จ) บรูตฟอร์ซแอตแทค (Brute Force Attack)

ฉ) เอสคิวแอลอินเจกชัน (SQL Injection)

ช) ครอสไซต์สคริปต์ติ้ง (Cross-Site Scripting - XSS)

1.3.4 การจำลองระบบเครือข่ายภายในที่ใช้ในการทดสอบการตรวจจับ โดยกำหนดปัจจัยเดียวกันในการทดสอบ เพื่อให้สภาพแวดล้อมจะไม่เป็นปัจจัยที่ทำให้ผลการทดสอบการตรวจจับแตกต่างกัน

1.3.5 คัดเลือกโปรแกรมตรวจจับการบุกรุก (Intrusion Detection Software) โดยเลือกใช้โปรแกรมตรวจจับการบุกรุกจำนวน 3 โปแกรม ได้แก่

1.3.5.1 โปรแกรมสนอร์ต (Snort) เวอร์ชัน 2.9.20 GRE (Build 82)

1.3.5.2 โปรแกรมซูริกาต้า (Suricata) เวอร์ชัน 7.0.5

1.3.5.3 โปรแกรมซีค (Zeek) เวอร์ชัน 6.0.3

1.3.6 ประเมินผลลัพท์ที่ได้จากการเปรียบเทียบ โปรแกรมตรวจสอบการบุกรุก

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 องค์กรขนาดกลางจะสามารถใช้ผลการวิจัยนี้เป็นข้อมูลประกอบการตัดสินใจเลือกใช้ระบบตรวจจับการบุกรุก ที่มีประสิทธิภาพ สอดคล้องกับงบประมาณและทรัพยากรที่มีอยู่อย่างจำกัด

1.4.2 ส่งเสริมให้ผู้ดูแลระบบเครือข่ายหรือฝ่ายเทคโนโลยีสารสนเทศในองค์กรตระหนักถึงความสำคัญของการตรวจจับภัยคุกคามเชิงรุก และวางแผนระบบรักษาความมั่นคงปลอดภัยได้อย่างเป็นระบบมากขึ้น

1.4.3 ช่วยเป็นแนวทางสำหรับการประยุกต์ใช้หรือพัฒนาระบบตรวจจับการบุกรุก ในบริบทอื่น เช่น โรงพยาบาลขนาดเล็ก ธุรกิจขนาดเล็ก หรือหน่วยงานภาครัฐที่มีข้อจำกัดด้านทรัพยากร

1.5 เครื่องมือที่ใช้ในงานวิจัย

1.5.1 ฮาร์ดแวร์

1.5.1.1 CPU Intel Xenon 56000 Series (2 Sockets, up to 12 Cores)

1.5.1.2 Ram 192 GB

1.5.1.3 HDD SSD 2 TB

1.5.2 ซอฟต์แวร์

1.5.2.1 ระบบปฏิบัติการ Windows Server 2022

1.5.2.2 ระบบปฏิบัติการ Linux Ubuntu 24.04

1.5.2.3 ระบบปฏิบัติการ Kali Linux 2024.4

1.5.2.4 ระบบ Intrusion Detection Snort

1.5.2.5 ระบบ Intrusion Detection Suricata

1.5.2.6 ระบบ Intrusion Detection Zeek

1.5.2.7 โปรแกรม PHP Server

1.5.2.8 ระบบฐานข้อมูล Maria DB

1.5.2.9 โปรแกรม เว็บไซต์จำลองช่องโหว่ DVWA

1.5.2.10 โปรแกรม CheckMK

1.5.2.11 VMWare vSphere

1.6 คำจำกัดความที่ใช้ในการวิจัย

1.6.1 ระบบตรวจจับการบุกรุก (Intrusion Detection System) หรือ IDS ระบบที่ออกแบบมาเพื่อตรวจจับก่อกวนหรือการบุกรุกในระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ โดยระบบตรวจจับการบุกรุก จะตรวจจับพฤติกรรมที่ไม่ปกติภายในระบบหรือเครือข่าย เช่น การเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต การโจมตีด้วยไวรัส หรือการสแกนพอร์ตเพื่อค้นหาช่องโหว่ในระบบ เมื่อระบบตรวจจับการบุกรุกตรวจจับการก่อกวนหรือการบุกรุก จะสร้างเหตุการณ์และแจ้งเตือนผู้ดูแลระบบเพื่อให้พวกเขาดำเนินการต่อไป เช่น ตรวจสอบเหตุการณ์และรับมือกับการละเมิดความปลอดภัยที่เกิดขึ้น หรือปรับเปลี่ยนการกำหนดค่าระบบเครือข่ายเพื่อป้องกันการบุกรุกในอนาคต ระบบตรวจจับการบุกรุก

มักจะใช้กลไกตรวจจับและวิเคราะห์ข้อมูลจากพื้นที่ต่าง ๆ ของระบบ เช่น การตรวจจับแพคเก็ตข้อมูลบนเครือข่ายหรือการตรวจจับเหตุการณ์ในเครื่องเซิร์ฟเวอร์ ซึ่งมีหลายวิธีการในการดำเนินการ รวมถึงการตรวจจับแบบซิกเนเจอร์เบส (Signature-based Detection) การตรวจจับแบบอะโนมาลีเบส (Anomaly-based Detection) และ การตรวจจับแบบฮิวริสติกเบส (Heuristic-based Detection) เป็นต้น

1.6.2 โปรแกรมตรวจจับการบุกรุก (Intrusion Detection Software) เป็นแอปพลิเคชันหรือโปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาเพื่อตรวจจับและรายงานเหตุการณ์ที่เกี่ยวข้องกับการบุกรุกหรือการละเมิดความปลอดภัยในระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ โปรแกรมดังกล่าวมักมีความสามารถในการตรวจจับพฤติกรรมที่ไม่ปกติภายในระบบ หรือรูปแบบการโจมตีที่รู้จักล่วงหน้า การตรวจจับแบบซิกเนเจอร์เบส โดยโปรแกรมอาจใช้กฎหรือซิกเนเจอร์ของการโจมตีเพื่อระบุการกระทำที่เป็นประเภทของการโจมตีบางประเภท

1.6.3 การโจมตีทางคอมพิวเตอร์ (Computer Attack) เป็นกระบวนการหรือกิจกรรมที่ผู้ไม่ประสงค์ดีใช้เทคโนโลยีคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์เพื่อฉ้อโกง ทำลาย หรือเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต หรือบุคคลที่ถูกโจมตี โดยปกติแล้วการโจมตีทางคอมพิวเตอร์เป็นที่รุนแรงและเสี่ยงต่อความปลอดภัยของข้อมูลและระบบของบุคคลหรือองค์กรที่เป็นเป้าหมาย

1.6.4 การตรวจจับแบบซิกเนเจอร์เบส (Signature-based Detection) เป็นวิธีการตรวจจับการบุกรุกโดยอาศัยการเปรียบเทียบรูปแบบของข้อมูลหรือกิจกรรมกับฐานข้อมูลของลายเซ็นภัยคุกคาม (Signature) ที่ได้รวบรวมไว้ล่วงหน้า หากตรวจพบรูปแบบที่ตรงกัน ระบบจะพิจารณาว่าเป็นพฤติกรรมที่เป็นอันตราย วิธีการนี้มีประสิทธิภาพในการตรวจจับภัยคุกคามที่รู้จักแล้ว แต่อาจไม่สามารถตรวจพบภัยคุกคามรูปแบบใหม่หรือที่ยังไม่มีลายเซ็นได้ [1], [9], [10]

1.6.5 การตรวจจับแบบอะโนมาลีเบส (Anomaly-based Detection) เป็นวิธีการตรวจจับที่อาศัยการเปรียบเทียบพฤติกรรมของระบบหรือผู้ใช้งานกับพฤติกรรมที่ถือว่าเป็นปกติ หากพบความเบี่ยงเบนหรือผิดปกติจากค่ามาตรฐานที่กำหนดไว้ ระบบจะพิจารณาว่าอาจเป็นพฤติกรรมที่เป็นอันตราย วิธีนี้สามารถตรวจจับภัยคุกคามที่ไม่เคยปรากฏมาก่อนได้ แต่มีโอกาสเกิดการแจ้งเตือนผิดพลาดได้สูง [6], [14], [15]

1.6.6 การตรวจจับแบบฮิวริสติกเบส (Heuristic-based Detection) เป็นวิธีการตรวจจับที่ใช้แนวทางการวิเคราะห์เชิงตรรกะหรือกฎเชิงประสบการณ์ เพื่อประเมินและตัดสินว่ากิจกรรมใดอาจเป็นภัยคุกคาม แม้จะไม่ตรงกับลายเซ็นหรือรูปแบบที่มีอยู่ วิธีการนี้สามารถตรวจจับภัยคุกคามที่ซับซ้อนหรือแฝงตัวได้ดี แต่ต้องอาศัยการออกแบบกฎและอัลกอริธึมที่มีประสิทธิภาพ [14]

บทที่ 2
ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

ในยุคปัจจุบันที่เทคโนโลยีสารสนเทศและการสื่อสารเข้ามามีบทบาทสำคัญในทุกภาคส่วนของสังคม การรักษาความปลอดภัยของระบบเครือข่ายและข้อมูลจึงเป็นเรื่องที่องค์กรต่าง ๆ ให้ความสำคัญอย่างยิ่ง โดยเฉพาะอย่างยิ่งกับองค์กรขนาดกลางที่มีทรัพยากรจำกัดแต่ต้องเผชิญกับภัยคุกคามทางไซเบอร์ที่ซับซ้อนและหลากหลายระบบตรวจจับการบุกรุก จึงกลายเป็นเครื่องมือสำคัญในการป้องกันและตรวจจับภัยคุกคามเหล่านี้

บทนี้จะกล่าวถึงทฤษฎีที่เกี่ยวกับระบบตรวจจับการบุกรุก ประเภทของภัยคุกคามที่ต้องเฝ้าระวัง รวมถึงตัวชี้วัดหลักที่ใช้ในการประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก เพื่อเป็นพื้นฐานในการวิเคราะห์และเปรียบเทียบระบบตรวจจับการบุกรุก ที่เหมาะสมสำหรับองค์กรขนาดกลาง โดยแบ่งเสนอตามประเด็นสำคัญดังนี้

2.1 ความมั่นคงปลอดภัยของระบบเครือข่าย

2.2 ระบบตรวจจับการบุกรุก

2.3 ประเภทของการโจมตีที่ใช้ในการทดลอง

2.4 เครื่องมือระบบตรวจจับการบุกรุกที่ใช้ในการศึกษา

2.5 เกณฑ์การประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก

2.6 งานวิจัยที่เกี่ยวข้อง

2.1 ความมั่นคงปลอดภัยของระบบเครือข่าย

ระบบเครือข่ายคอมพิวเตอร์เป็นโครงสร้างพื้นฐานสำคัญที่สนับสนุนการดำเนินงานขององค์กรในทุกระดับ ตั้งแต่การสื่อสารภายใน การให้บริการลูกค้า การจัดเก็บข้อมูล ไปจนถึงการบริหารจัดการระบบงานหลักขององค์กร อย่างไรก็ตาม การเชื่อมต่อผ่านเครือข่าย โดยเฉพาะเมื่อมีการเชื่อมโยงกับเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต [1] ย่อมนำมาซึ่งความเสี่ยงด้านความมั่นคงปลอดภัยที่หลากหลาย ซึ่งอาจถูกแสวงหาประโยชน์โดยผู้ไม่หวังดีผ่านวิธีการโจมตีที่ซับซ้อนและหลากหลายรูปแบบมากยิ่งขึ้น

ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในปัจจุบันมีลักษณะซับซ้อนและยากต่อการตรวจจับ เช่น การโจมตีแบบปฏิเสธการให้บริการ (Denial of Service: DoS) การปลอมแปลงข้อมูล (Spoofing) การเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access) เป็นต้น [2], [3] ซึ่งล้วนส่งผลกระทบต่อความลับ (Confidentiality)

ความสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของระบบสารสนเทศในองค์กร ซึ่งเรียกรวมกันว่า “หลักการ CIA” อันเป็นหลักสำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูล

สำหรับองค์กรขนาดกลางซึ่งมักมีข้อจำกัดด้านงบประมาณและทรัพยากรบุคคล การรักษาความมั่นคงปลอดภัยของเครือข่ายจึงเป็นความท้าทายอย่างยิ่ง การไม่มีบุคลากรเฉพาะด้านความปลอดภัยไซเบอร์ การขาดเครื่องมือในการตรวจสอบ และการไม่มีมาตรการป้องกันที่เพียงพอ ทำให้องค์กรกลุ่มนี้กลายเป็นเป้าหมายหลักของการโจมตีในยุคดิจิทัล [4]

ดังนั้น การวางแผนจัดการความมั่นคงปลอดภัยจึงต้องครอบคลุมทั้งด้านเทคนิคและด้านนโยบาย ได้แก่ การกำหนดสิทธิ์ในการเข้าถึงข้อมูล การเข้ารหัสข้อมูล การใช้ไฟร์วอลล์และระบบตรวจสอบพฤติกรรม การสำรองข้อมูล การควบคุมการใช้งานอุปกรณ์ และการอบรมให้พนักงานมีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ [5], [6] ทั้งนี้ เพื่อให้สามารถรับมือกับสถานการณ์ต่าง ๆ ได้อย่างมีประสิทธิภาพ และลดความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศขององค์กร

2.2 ระบบตรวจจับการบุกรุก

ระบบตรวจจับการบุกรุก เป็นหนึ่งในมาตรการด้านเทคนิคที่มีบทบาทสำคัญในการเสริมสร้างความมั่นคงปลอดภัยของระบบเครือข่าย โดยทำหน้าที่ตรวจสอบทราฟฟิกและกิจกรรมต่าง ๆ ที่เกิดขึ้นในระบบเครือข่าย เพื่อตรวจจับพฤติกรรมที่ผิดปกติหรือเข้าข่ายว่าเป็นการโจมตี ไม่ว่าจะเป็นการสแกนพอร์ต การพยายามเข้าสู่ระบบโดยไม่ได้รับอนุญาต หรือแม้แต่การใช้ช่องโหว่ของระบบในการเจาะเข้ามาทำลายหรือขโมยข้อมูล [6], [8] โดย ระบบ IDS สามารถจำแนกออกเป็น 2 ประเภทหลัก ได้แก่

2.2.1 Network-based IDS (NIDS) ซึ่งทำงานโดยตรวจสอบข้อมูลเครือข่ายที่วิ่งผ่านอุปกรณ์ต่าง ๆ เช่น เราเตอร์หรือสวิตช์ เพื่อหาพฤติกรรมที่เข้าข่ายผิดปกติ [1], [9]

2.2.2 Host-based IDS (HIDS) ซึ่งทำงานอยู่ในระดับเซิร์ฟเวอร์หรืออุปกรณ์ปลายทาง โดยตรวจสอบไฟล์ระบบ การเปลี่ยนแปลงการตั้งค่า และกิจกรรมของผู้ใช้ในระดับเครื่อง [5], [14]

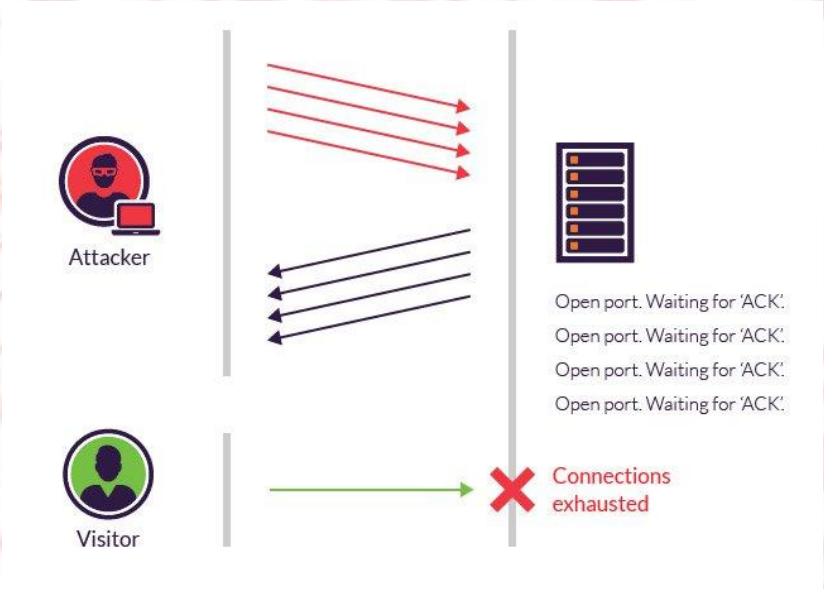
การเลือกใช้งาน IDS ที่เหมาะสมกับสภาพแวดล้อมขององค์กรเป็นเรื่องสำคัญอย่างยิ่ง โดยเฉพาะในองค์กรขนาดกลางที่ต้องพิจารณาทั้งด้านประสิทธิภาพ ความแม่นยำ ความสามารถในการตรวจจับพฤติกรรมการบุกรุกที่ซับซ้อน และการบริหารจัดการระบบให้เหมาะสมกับทรัพยากรที่มีอยู่

ดังนั้น การศึกษาเกี่ยวกับการเปรียบเทียบ และประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก จึงเป็นแนวทางที่ช่วยให้องค์กรสามารถตัดสินใจเลือกใช้เครื่องมือที่ตอบโจทย์ได้อย่างมีประสิทธิภาพ และสอดคล้องกับเป้าหมายในการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายในระยะยาว

2.3 ประเภทของการโจมตี

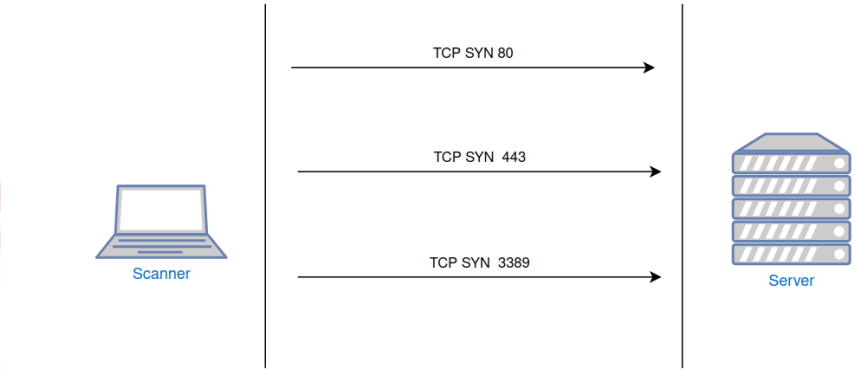
ประเภทของการโจมตีที่พบได้บ่อยในบริบทขององค์กร โดยจำแนกตามลักษณะของการโจมตี ได้แก่ การโจมตีเชิงปริมาณ ฟลัดเบส (Flood-based), การโจมตีเชิงพฤติกรรม บีเฮเวียร์รัลเบส (Behavioral-based) และการโจมตีช่องโหว่ของแอปพลิเคชัน แอปพลิเคชันเลเวลวัลเนอราบิลิตีส์ (Application-level Vulnerabilities) ซึ่งประกอบด้วย 7 ประเภท ดังนี้

2.3.1 ทีซีพีซินฟลัด เป็นการโจมตีแบบปฏิเสธการให้บริการ เดนายัล ออฟ เซอร์วิส(Denial of Service) ที่ใช้ช่องโหว่ของกระบวนการจับมือกันแบบสามทาง ทรี-เวย์ แฮนด์เชค (Three-way Handshake) ของโปรโตคอล ทีซีพี โดยผู้โจมตีจะส่งแพ็กเก็ต ซิน (SYN) จำนวนมากไปยังเซิร์ฟเวอร์เป้าหมาย ทำให้ทรัพยากรถูกใช้งานจนไม่สามารถตอบสนองคำร้องขอปกติจากผู้ใช้จริงได้



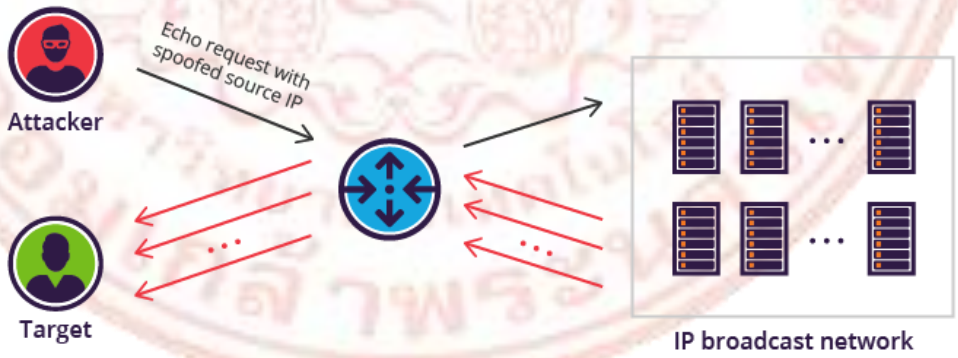
ภาพที่ 2-1 รูปภาพที่อธิบายการทำงานของ TCP SYN Flood [26]

2.3.2 ทีซีพีพอร์ตสแกน เป็นการสแกนพอร์ตในระบบเป้าหมายเพื่อค้นหาว่าพอร์ตใดเปิดใช้งานอยู่บ้าง ซึ่งอาจนำไปสู่การสำรวจบริการที่รันอยู่ และใช้เป็นข้อมูลเบื้องต้นก่อนเริ่มการโจมตีในลำดับถัดไป พฤติกรรมนี้มักเกิดขึ้นในช่วง รีโคกไนแซนซ์ (Reconnaissance) หรือ ฟุตพรินท์ติ้ง (Footprinting)



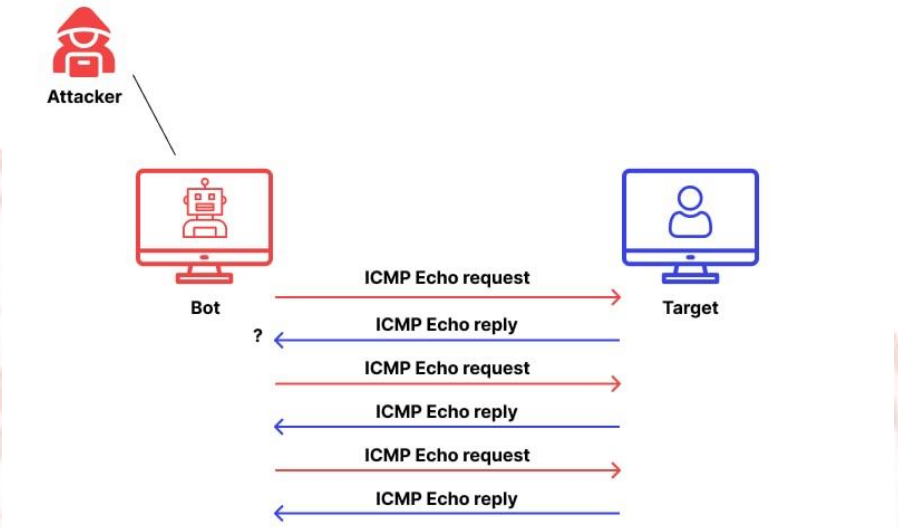
ภาพที่ 2-2 รูปภาพที่อธิบายการทำงานของ TCP Port Scan [27]

2.3.3 สมิร์ฟแอตแทค เป็นการโจมตีที่อาศัยการปลอมแปลงที่อยู่ต้นทางของแพ็กเก็ต ICMP ไปยังที่อยู่ของเหยื่อ และส่งข้อความไปยังที่อยู่บรอดแคสต์ของเครือข่าย ทำให้ทุกเครื่องในเครือข่ายตอบกลับไปยังเหยื่อพร้อมกัน ส่งผลให้ระบบล่มจากการรับข้อมูลจำนวนมากพร้อมกัน ดิสทริบิวเต็ด รีเฟลกชัน (Distributed Reflection)



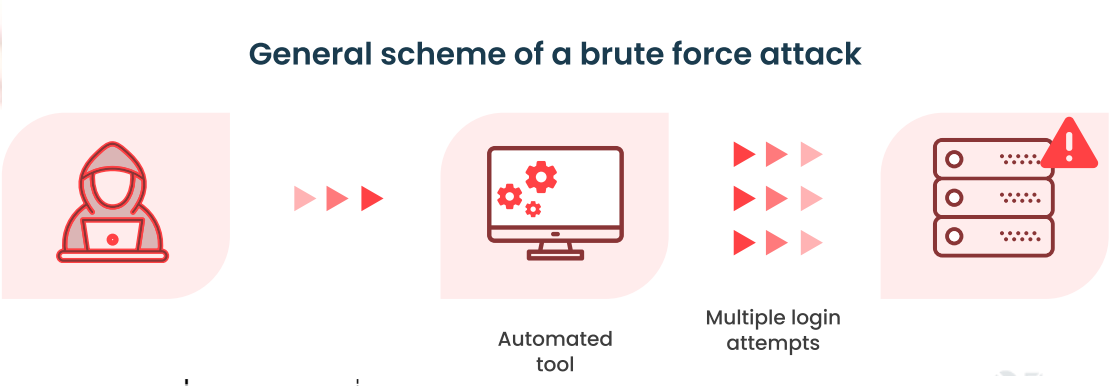
ภาพที่ 2-3 รูปภาพที่อธิบายการทำงานของ Smurf Attack [28]

2.3.4 ไอซีเอ็มพีพิงฟลัด เป็นการส่งคำสั่ง ปิง (Ping) ไปยังเป้าหมายจำนวนมากในเวลาสั้น ๆ เพื่อทำให้ระบบทำงานช้าลงหรือหยุดให้บริการ เหมาะสำหรับการรบกวนระบบที่มีทรัพยากรจำกัด โดยไม่จำเป็นต้องเจาะระบบโดยตรง



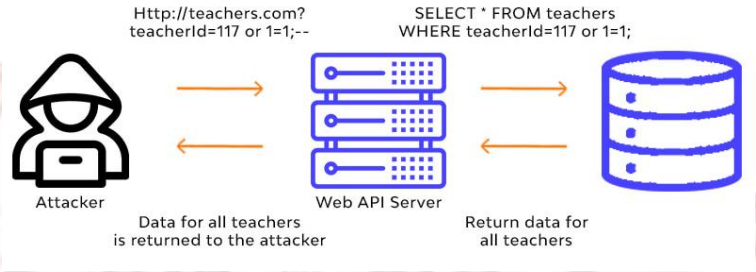
ภาพที่ 2-4 รูปภาพที่อธิบายการทำงานของ ICMP Ping Flood [29]

2.3.5 บรูตฟอร์ซแอตแทค เป็นการพยายามเข้าสู่ระบบโดยการเดารหัสผ่านหรือข้อมูลการยืนยันตัวตนด้วยวิธีการลองผิดลองถูกอย่างเป็นระบบ ซึ่งหากไม่สามารถตรวจจับได้ อาจนำไปสู่การเข้าถึงข้อมูลสำคัญในระบบโดยไม่ได้รับอนุญาต



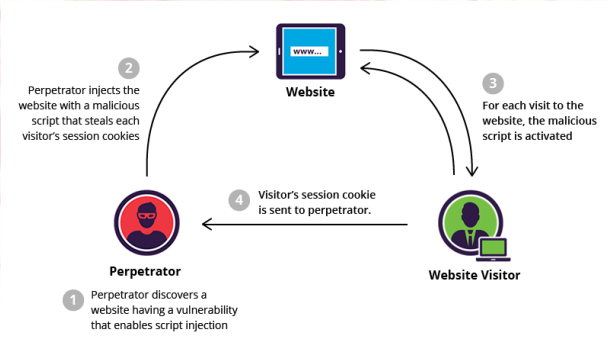
ภาพที่ 2-5 รูปภาพที่อธิบายการทำงานของ Brute Force Attack [3]0

2.3.6 เอสคิวแอลอินเจกชัน เป็นการโจมตีผ่านช่องโหว่ของแอปพลิเคชันที่รับค่าจากผู้ใช้แล้วส่งต่อไปยังฐานข้อมูลโดยตรง ผู้โจมตีสามารถส่งคำสั่ง เอสคิวแอล (SQL) แฝงมากับอินพุตเพื่อเปลี่ยนแปลงคำสั่ง เอสคิวแอล ที่ระบบประมวลผล ทำให้สามารถเข้าถึงหรือแก้ไขข้อมูลในฐานข้อมูลได้



ภาพที่ 2-6 รูปภาพที่อธิบายการทำงานของ SQL Injection [31]

2.3.7 ครอสไซต์สคริปต์ติ้ง เป็นการโจมตีโดยการฝังโค้ด จาวาสคริปต์(JavaScript) หรือโค้ดฝั่งไคลเอนต์ลงในเว็บไซต์เพื่อให้เบราว์เซอร์ของผู้ใช้รายอื่นรันคำสั่งดังกล่าว เช่น ขโมย เซสชัน (Session) หรือเปลี่ยนเนื้อหาบนหน้าเว็บไซต์



ภาพที่ 2-7 รูปภาพที่อธิบายการทำงานของ Cross-Site Scripting [32]

ภัยคุกคามทางไซเบอร์ที่เลือกศึกษาในงานวิจัยนี้เป็นกลุ่มการโจมตีที่ได้รับความนิยมและพบได้บ่อยในโลกไซเบอร์ ทั้งในระดับเครือข่ายและแอปพลิเคชัน ซึ่งมีลักษณะการโจมตีที่แตกต่างกันแต่ล้วนมีผลกระทบอย่างรุนแรงต่อความมั่นคงปลอดภัยของระบบ การโจมตีเหล่านี้ไม่เพียงแต่มีความซับซ้อนและเปลี่ยนแปลงรูปแบบอย่างรวดเร็ว แต่ยังเป็นภัยที่ป้องกันได้ยาก เนื่องจากผู้โจมตีมักใช้เทคนิคที่หลากหลายและมุ่งเน้นการ

หลบเลี่ยงการตรวจจับ ดังนั้นระบบตรวจจับการบุกรุกจึงจำเป็นต้องมีความแม่นยำและประสิทธิภาพสูงในการตอบสนองต่อภัยคุกคามเหล่านี้อย่างมีประสิทธิผล เพื่อช่วยให้องค์กรสามารถรักษาความปลอดภัยของระบบและข้อมูลสำคัญไว้ได้

2.4 เครื่องมือระบบตรวจจับการบุกรุกที่ใช้ในการศึกษา

ในการวิจัยนี้ ได้เลือกใช้ระบบตรวจจับการบุกรุกที่มีชื่อเสียงและได้รับความนิยมในวงการความมั่นคงปลอดภัยเครือข่าย เพื่อทำการเปรียบเทียบประสิทธิภาพในการตรวจจับภัยคุกคามที่หลากหลาย โดยเครื่องมือ ระบบตรวจจับการบุกรุก ที่ใช้ในการศึกษา ได้แก่

2.4.1 สนอร์ต (Snort) เป็นระบบตรวจจับการบุกรุกแบบ แบบซิกเนเจอร์เบส ที่มีความสามารถในการวิเคราะห์แพ็กเก็ตแบบเรียลไทม์และตรวจจับการโจมตีด้วยชุดกฎการตรวจจับ รูลส์ (Rules) ที่กำหนดล่วงหน้า อีกทั้งยังรองรับการตรวจจับหลายประเภท ทั้งการโจมตีในระดับเครือข่ายและแอปพลิเคชัน ทำให้สนอร์ต เป็นเครื่องมือยอดนิยมสำหรับองค์กรหลายขนาด [1], [9], [10], [16]

2.4.2 ซูริกาต้า (Suricata) เป็นระบบตรวจจับการบุกรุกแบบ ที่พัฒนาขึ้นเพื่อเพิ่มประสิทธิภาพและความสามารถที่เหนือกว่า สนอร์ต ด้วยการรองรับการวิเคราะห์หลายเธรด มัลติ-เธรดดิ้ง (multi-threading) ทำให้สามารถประมวลผลข้อมูลปริมาณมากได้รวดเร็วกว่า อีกทั้งยังรองรับ แบบซิกเนเจอร์เบส และ แบบอะโนมาลีเบส พร้อมด้วยฟีเจอร์ขั้นสูง เช่น การตรวจจับโปรโตคอลต่าง ๆ และการบันทึกข้อมูลแพ็กเก็ตอย่างละเอียด [1], [9], [11], [15], [16]

2.4.3 ซีค (Zeek) เป็นระบบตรวจจับการบุกรุกที่เน้นการวิเคราะห์พฤติกรรมของทราฟฟิกในระดับโปรโตคอลและแอปพลิเคชัน แบบบีเฮเวียร์รัลเบส โดยใช้สคริปต์ในการปรับแต่งกฎการตรวจจับได้อย่างยืดหยุ่น ทำให้ ซีค เหมาะกับการวิเคราะห์เชิงลึกและการตรวจจับภัยคุกคามที่ซับซ้อน [5], [7], [9], [13], [17]

2.5 เกณฑ์การประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก

ในการประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก (Intrusion Detection System: IDS) จำเป็นต้องพิจารณาเกณฑ์หลายด้านเพื่อให้สามารถเปรียบเทียบระบบต่าง ๆ ได้อย่างครอบคลุมและเป็นธรรม โดยเกณฑ์ที่ใช้ในการศึกษานี้ประกอบด้วย:

ก) อัตราการตรวจจับ หรือ ทรูโพซิทีฟ (True Positive) เป็นอัตราส่วนของเหตุการณ์ที่เป็นภัยจริงและถูกตรวจจับได้อย่างถูกต้อง แสดงถึงความสามารถของระบบในการตอบสนองต่อภัยคุกคามอย่างแม่นยำ

ข) อัตราความผิดพลาด หรือ ฟอลส์เนกาทีฟ (False Negative) คือจำนวนเหตุการณ์ที่เป็นภัยคุกคามจริงแต่ระบบไม่สามารถตรวจจับได้ เป็นค่าที่ต้องพยายามลดให้น้อยที่สุด เนื่องจากส่งผลต่อความปลอดภัยของระบบเครือข่ายโดยตรง

ค) ความถูกต้องแม่นยำ หรือ แอคคิวราซี (Accuracy) เป็นสัดส่วนของการตรวจจับที่ถูกต้องทั้งหมดทั้งในกรณีภัยจริงและภัยปลอม ช่วยสะท้อนความน่าเชื่อถือโดยรวมของระบบ

ง) อัตราการตรวจจับ ดีเทคชันเรต (Detection Rate) แสดงเปอร์เซ็นต์ของภัยคุกคามที่ระบบสามารถตรวจพบจากจำนวนภัยทั้งหมด ยิ่งมีค่าสูงยิ่งแสดงถึงประสิทธิภาพของระบบในการตอบสนองต่อเหตุการณ์

จ) การตรวจจับคะแนน เอฟวันสกอร์ (F1 Score) เป็นค่าที่คำนวณจากค่าความแม่นยำ และอัตราการตรวจจับโดยรวม เป็นตัวชี้วัดที่สมดุลระหว่างการตรวจจับภัยคุกคามได้มากและการลดอัตราแจ้งเตือนผิดพลาด

ฉ) ประสิทธิภาพของระบบ ซิสเท็มเพอร์ฟอร์แมนซ์ (System Performance) เป็นการประเมินทรัพยากรที่ใช้ในการทำงานของระบบ เช่น การใช้ หน่วยประมวลผลกลาง ซีพียู (CPU), หน่วยความจำ แรม (RAM), และการหน่วงเวลาของระบบขณะประมวลผลการตรวจจับ

ช) ความสามารถในการปรับแต่งและปรับเปลี่ยน เฟล็กซิบิลิตี้ แอนด์ คัสตอมไมเซชัน (Flexibility & Customization) แสดงถึงความสามารถของระบบในการปรับเปลี่ยนกฎการตรวจจับหรือพฤติกรรมให้สอดคล้องกับสภาพแวดล้อมของเครือข่ายที่ใช้งานจริง

ซ) การบำรุงรักษา เมนเทนเอบิลิตี้ (Maintainability) หมายถึงความง่ายในการดูแล อัปเดต และแก้ไขระบบตรวจจับ เช่น การอัปเดตรูปแบบลักษณะเฉพาะของภัยคุกคามหรือกิจกรรมที่เป็นอันตรายซิกเนเจอร์ (Signature) การตั้งค่ากฎการตรวจจับ หรือการวิเคราะห์บันทึกของระบบ [15], [17]

2.6 งานวิจัยที่เกี่ยวข้อง

จากการศึกษาวรรณกรรมที่เกี่ยวข้องพบว่า แนวทางการตรวจจับการบุกรุกเครือข่าย (Intrusion Detection Systems: IDS) ในระดับองค์กร โดยเฉพาะในบริบทขององค์กรขนาดกลางและขนาดเล็ก (SMEs) ได้รับความสนใจอย่างต่อเนื่องในช่วงหลายปีที่ผ่านมา ทั้งในด้านเทคโนโลยีที่นำมาใช้และประสิทธิภาพของระบบในการรับมือกับภัยคุกคามไซเบอร์ที่มีความซับซ้อนเพิ่มขึ้น

Boukebous et al. [1] ได้ดำเนินการเปรียบเทียบประสิทธิภาพเชิงเทคนิคของ Snort เวอร์ชัน 3 และ Suricata โดยพบว่า Snort เวอร์ชัน 3 มีความยืดหยุ่นในการปรับแต่งกฎ (Rule Flexibility) และการประมวลผลแบบมัลติเธรด ในขณะที่ Suricata มีข้อได้เปรียบในด้านการวิเคราะห์ทราฟฟิกที่ซับซ้อนโดยใช้

ความสามารถของ multi-thread engine อย่างเต็มรูปแบบ ส่งผลให้ Suricata มีความเหมาะสมมากกว่าในกรณีที่ต้องรองรับทราฟฟิกจำนวนมากและต้องการการตรวจสอบแบบเรียลไทม์ [1], [10], [16]

ในขณะเดียวกัน Waleed et al. [9] ได้ตั้งคำถามเชิงเปรียบเทียบเชิงกลยุทธ์ว่า “ควรเลือกใช้ IDS ใดระหว่าง Snort, Suricata หรือ Zeek” โดยพิจารณาจากมุมมองของการปฏิบัติงานจริง (Operational Context) ซึ่งมีข้อสรุปว่าการตัดสินใจเลือกใช้งานควรขึ้นอยู่กับปัจจัยหลายประการ เช่น ประเภทของการโจมตีที่ต้องการตรวจจับ ความซับซ้อนของเครือข่าย และความพร้อมของทรัพยากรภายในองค์กร [9]

จากมุมมองของระบบธุรกิจขนาดเล็กและกลาง Ncubukezi et al. [2] และ Jonathan & Thamrongthanakit [4] ได้เน้นถึงความท้าทายเชิงโครงสร้างของ SMEs ที่มักขาดบุคลากรที่มีความเชี่ยวชาญด้านไซเบอร์และงบประมาณสำหรับระบบความปลอดภัย ส่งผลให้การนำ IDS เข้ามาใช้งานมักเป็นไปอย่างจำกัด ทั้งนี้ การบูรณาการระบบที่มีความสามารถในการวิเคราะห์ภัยคุกคามอัตโนมัติและลด False Positive Rate จึงถือเป็นสิ่งจำเป็นต่อประสิทธิภาพในการนำไปใช้งานจริง [2], [4]

ในด้านเทคโนโลยีการวิเคราะห์ภัยคุกคามขั้นสูง Tiwari et al. [7] และ Haas et al. [5] ได้พัฒนาและขยายขีดความสามารถของ Zeek IDS โดยเน้นการวิเคราะห์เชิงพฤติกรรมของการโจมตีผ่านการตรวจสอบเหตุการณ์ในระดับโปรโตคอล ร่วมกับการประสานงานกับเครื่องมือระดับโฮสต์ เช่น Osquery เพื่อสร้างบริบทของเหตุการณ์ที่ลึกขึ้นและแม่นยำยิ่งขึ้น ซึ่งเป็นแนวทางที่ตอบโจทย์ความต้องการในการตรวจจับภัยคุกคามยุคใหม่ที่มีลักษณะซับซ้อนและพรางตัวได้ดี [5], [7]

นอกจากนี้ Zeek ยังถูกพัฒนาเพิ่มเติมให้สามารถทำงานร่วมกับเทคนิคการเรียนรู้ของเครื่อง (Machine Learning) เพื่อเพิ่มประสิทธิภาพในการจำแนกความผิดปกติของข้อมูลจราจรเครือข่าย โดยงานของ Nair และ Thomas [13] รวมถึง Ajmeera et al. [6] ได้แสดงให้เห็นถึงการออกแบบระบบตรวจจับแบบไฮบริดที่ผสานข้อมูลจาก Zeek กับอัลกอริธึม ML เช่น Random Forest และ SVM ในการปรับปรุงการตรวจจับภัยคุกคามแบบ anomaly-based ให้มีความแม่นยำและอัตรา false negative ต่ำ [6], [13]

ขณะที่ในมุมของการออกแบบระบบ IDS สำหรับองค์กรขนาดกลาง Patil & Patil [12], Alshamrani et al. [14] และ Jadhav & Patil [15] ต่างเสนอการเปรียบเทียบอัลกอริธึม ML ที่เหมาะสมที่สุดต่อสถานการณ์ต่าง ๆ ซึ่งครอบคลุมทั้งการโจมตีแบบ DoS, Port Scan, Brute Force และ SQL Injection โดยเน้นให้เห็นถึงความสำคัญของการเลือกคุณลักษณะ (feature selection) และการฝึกสอนโมเดลด้วยข้อมูลที่มีความหลากหลาย [12], [14], [15]

สำหรับบริบทของการประเมินในสภาพแวดล้อมคลาวด์ Zhang et al. [16] ได้เปรียบเทียบประสิทธิภาพของ Snort และ Suricata ในการตรวจจับการโจมตีในระบบคลาวด์แบบ Infrastructure-as-a-Service (IaaS) โดยพบว่า Suricata แสดงผลการตรวจจับที่ดีกว่าในกรณีที่มีทราฟฟิกจำนวนมาก และสามารถปรับขนาด (scalability) ได้อย่างมีประสิทธิภาพเมื่อเปรียบเทียบกับ Snort [16]

ในทำนองเดียวกัน Rao & Reddy [17] ได้เสนอแนวทางการออกแบบ IDS แบบไฮบริดที่ใช้ทั้งเทคนิคการตรวจจับจากลายเซ็นซิกเนเจอร์เบส และการวิเคราะห์พฤติกรรม (anomaly-based) ผ่านการบูรณาการกับ Zeek ซึ่งแสดงให้เห็นถึงประสิทธิภาพที่สูงขึ้นในการตรวจจับการโจมตีที่ซับซ้อนและมีรูปแบบที่เปลี่ยนแปลงตลอดเวลา [17]

กล่าวโดยสรุป งานวิจัยที่เกี่ยวข้องทั้งหมดนี้ได้ชี้ให้เห็นถึงแนวโน้มที่สำคัญของวงการระบบตรวจจับการบุกรุก ได้แก่ การพัฒนาให้สามารถทำงานแบบเรียลไทม์บนระบบเครือข่ายที่ซับซ้อน และการออกแบบให้เหมาะสมกับข้อจำกัดขององค์กรขนาดกลางและขนาดเล็ก ซึ่งสอดคล้องกับทิศทางของระบบรักษาความปลอดภัยเชิงรุกที่มุ่งเน้นการตอบสนองอย่างชาญฉลาดและยืดหยุ่นมากยิ่งขึ้น

โดยเฉพาะอย่างยิ่ง การเลือกใช้และประเมินประสิทธิภาพของระบบตรวจจับการบุกรุกในสภาพแวดล้อมจริงขององค์กร ถือเป็นปัจจัยสำคัญที่จะช่วยให้องค์กรสามารถตัดสินใจเชิงเทคนิคได้อย่างแม่นยำและคุ้มค่าจึงเป็นที่มาของการค้นคว้าอิสระนี้

บทที่ 3
วิธีการดำเนินงาน

ในการดำเนินการวิจัยเพื่อเปรียบเทียบประสิทธิภาพของระบบตรวจจับการบุกรุกในบริบทขององค์กรขนาดกลาง จำเป็นต้องวางแผนและกำหนดขั้นตอนอย่างเป็นระบบ เพื่อให้สามารถรวบรวมข้อมูล วิเคราะห์ผล และตอบวัตถุประสงค์ของการวิจัยได้อย่างถูกต้องแม่นยำและน่าเชื่อถือ บทนี้จึงนำเสนอขั้นตอนและแนวทางการดำเนินงานวิจัยที่ผู้วิจัยใช้ในการศึกษา ตั้งแต่การออกแบบแนวทางการทดลอง การจัดเตรียมสภาพแวดล้อม การดำเนินการทดสอบ จนถึงการสรุปผลการดำเนินงาน เพื่อให้การวิจัยเป็นไปอย่างมีประสิทธิภาพ ครอบคลุม และสามารถนำผลลัพธ์ไปใช้อ้างอิงหรือพัฒนาต่อยอดได้อย่างเหมาะสมผู้วิจัยจึงวางแผนขั้นตอนการวิจัยดังนี้

3.1 ออกแบบขั้นตอนการวิจัย

3.2 ดำเนินการวิจัย

3.3 สรุปขั้นตอนการดำเนินการวิจัย

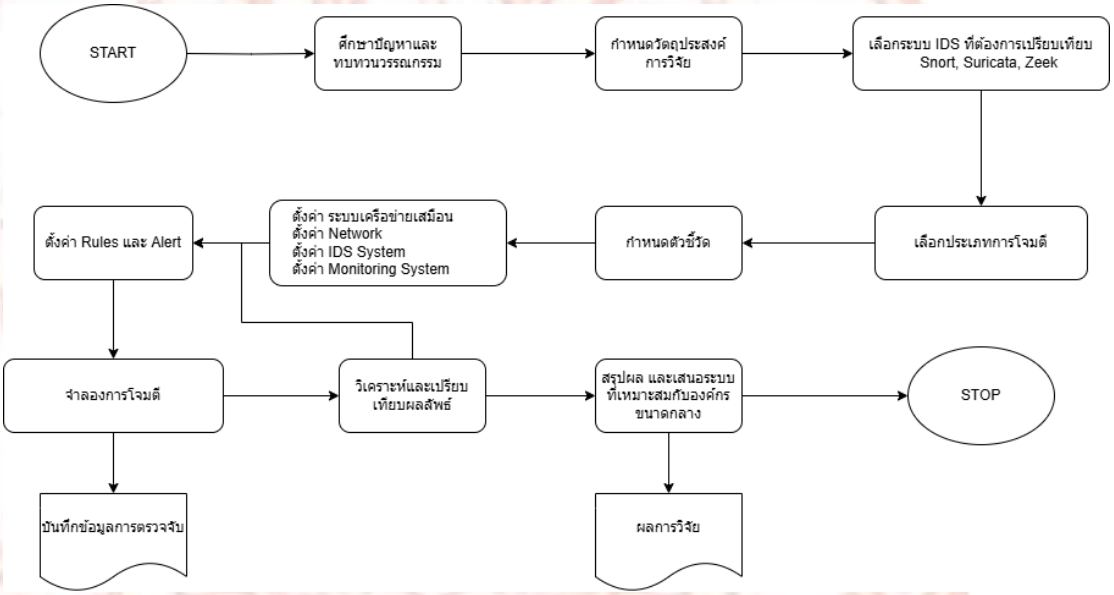
3.1 ออกแบบขั้นตอนการวิจัย

การออกแบบขั้นตอนการวิจัยครั้งนี้มุ่งเน้นการเปรียบเทียบประสิทธิภาพของระบบตรวจจับการบุกรุก ที่เหมาะสมในบริบทขององค์กรขนาดกลาง โดยเริ่มจากการศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้องเพื่อให้เข้าใจหลักการทำงานและจุดเด่นของระบบตรวจจับการบุกรุก แต่ละประเภท โปรแกรมสนอร์ต โปรแกรมซูริกาต้า และโปรแกรมซีค

จากนั้นจึงออกแบบสภาพแวดล้อมการทดลองในรูปแบบระบบเครือข่ายจำลองผ่านเครื่องเสมือน เวอร์ชวลแมชชีน (Virtual Machine) เพื่อให้สามารถควบคุมตัวแปรต่าง ๆ ได้อย่างแม่นยำและใกล้เคียงกับเครือข่ายจริงขององค์กรขนาดกลาง โดยภายในสภาพแวดล้อมดังกล่าวได้ติดตั้งและกำหนดค่า ระบบตรวจจับการบุกรุก ทั้งสามระบบให้เท่าเทียมกัน พร้อมกันนี้ยังเลือกใช้ประเภทการโจมตีจำนวน 7 ประเภท ได้แก่ ทีซีพีซินฟลัด ทีซีพีพอร์ตสแกน สมิร์ฟแอตแทค ไอซีเอ็มพีพิงฟลัด บรูตฟอร์ซแอตแทค เอสคิวแอลอินเจกชัน และครอสไซต์สคริปต์ติ้ง เพื่อจำลองสถานการณ์โจมตีที่อาจเกิดขึ้นจริงในระบบเครือข่าย จากนั้นจึงดำเนินการทดลองด้วยเครื่องมือเจาะระบบและสร้างทราฟฟิก เช่น คาลิ ลินุกซ์ (Kali Linux), เมทาสพลอยต์ (Metasploit) และ เอ็นแมพ (Nmap) เพื่อส่ง

ข้อมูลที่เป็นอันตรายเข้าสู่ระบบ และบันทึกผลการตรวจจับที่ได้จากระบบตรวจจับการบุกรุก แต่ละระบบ

ข้อมูลที่ได้จะถูกนำมาวิเคราะห์โดยใช้เกณฑ์การประเมินที่ครอบคลุมทั้งด้านความแม่นยำในการตรวจจับ อัตราการตรวจจับ อัตราการพลาด เอฟวันสกอร์ ประสิทธิภาพของระบบ ความสามารถในการปรับแต่ง และการบำรุงรักษาเพื่อสรุปเปรียบเทียบจุดแข็ง จุดอ่อน และความเหมาะสมของแต่ละระบบในบริบทขององค์กรที่มีข้อจำกัดด้านทรัพยากร บุคลากร และงบประมาณ โดยผลที่ได้จากการวิจัยจะเป็นข้อมูลเชิงประจักษ์ที่สามารถนำไปใช้ประกอบการตัดสินใจเลือกใช้ระบบตรวจจับการบุกรุก ที่เหมาะสมในองค์กรขนาดกลางได้อย่างมีประสิทธิภาพ



ภาพที่ 3-1 กระบวนการวิจัย

3.2 ดำเนินการวิจัย

การดำเนินการวิจัยครั้งนี้ได้รับการวางแผนและจัดการอย่างเป็นระบบเพื่อให้ครอบคลุมทุกขั้นตอนที่จำเป็นในการประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก ในสภาพแวดล้อมเสมือน โดยมุ่งเน้นการสร้างสภาพแวดล้อมทดสอบที่มีความสมจริงและสามารถควบคุมปัจจัยแวดล้อมต่าง ๆ ได้อย่างแม่นยำ ตลอดจนการกำหนดค่าระบบและกฎเกณฑ์ต่าง ๆ อย่างเหมาะสม เพื่อให้การทดสอบการบุกรุกเป็นไปอย่างมีประสิทธิผล และสามารถเก็บรวบรวมข้อมูลที่จำเป็นต่อการวิเคราะห์และประเมินผลลัพธ์ได้อย่างครบถ้วน โดยกระบวนการดำเนินงานหลักแบ่งออกเป็น 5 ขั้นตอน ได้แก่

3.2.1 การจัดเตรียมเครื่องเซิร์ฟเวอร์

3.2.2 การตั้งค่าเครือข่าย

3.2.3 การกำหนดกฎเกณฑ์บนระบบตรวจจับการบุกรุก

3.2.4 การทดสอบการบุกรุก

3.2.5 การเก็บรวบรวมข้อมูลเพื่อวิเคราะห์ประสิทธิภาพของระบบ

กระบวนการดำเนินงานวิจัยครั้งนี้ครอบคลุมขั้นตอนสำคัญ 5 ประการ ได้แก่ การจัดเตรียมเครื่องเซิร์ฟเวอร์ การตั้งค่าเครือข่าย การกำหนดกฎเกณฑ์บนระบบตรวจจับการบุกรุก การทดสอบการบุกรุก และการเก็บรวบรวมข้อมูลเพื่อวิเคราะห์ประสิทธิภาพของระบบ โดยทุกขั้นตอนถูกออกแบบมาเพื่อให้การวิจัยดำเนินไปอย่างเป็นระบบ แม่นยำ และครบถ้วน โดยจะเริ่มต้นจาก

3.2.1 การจัดเตรียมเครื่องเซิร์ฟเวอร์

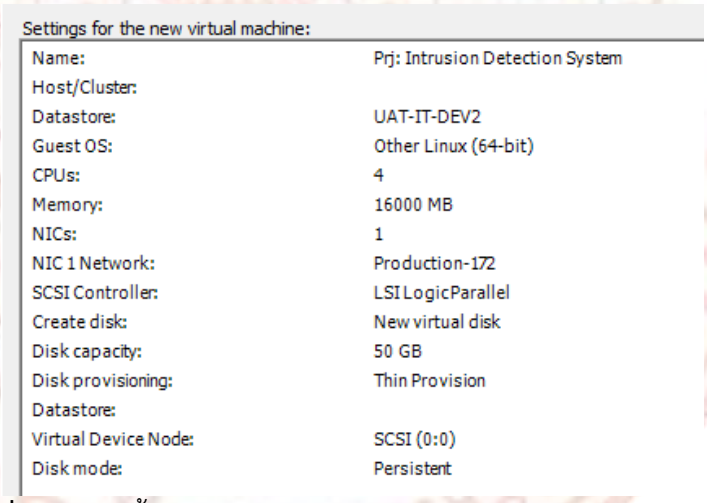
ในขั้นตอนการจัดเตรียมเซิร์ฟเวอร์ แบ่งออกได้ 4 กลุ่ม ดังนี้

3.2.1.1 เครื่องสำหรับการตรวจจับการบุกรุก เครื่องเสมือนที่ใช้สำหรับการตรวจจับการบุกรุกทำหน้าที่เป็นระบบหลักในการตรวจสอบและวิเคราะห์พฤติกรรมที่อาจเข้าข่ายเป็นการโจมตีหรือการบุกรุกเครือข่าย ภายในเครื่องเสมือนนี้ได้มีการติดตั้งระบบตรวจจับการบุกรุกจำนวนสามระบบ ได้แก่ โปรแกรม สนอร์ต ซูริกาต้า และ ซีค โดยแต่ละระบบตรวจจับการบุกรุก ถูกติดตั้งแยกจากกันภายใต้สภาพแวดล้อมเดียวกันบน เครือข่ายเสมือนเดียวกัน โดยใช้ระบบปฏิบัติการ การตั้งค่าระบบ และคุณสมบัติของเครื่อง ที่เหมือนกันทุกประการ เพื่อให้การเปรียบเทียบประสิทธิภาพของแต่ละระบบเป็นไปอย่างยุติธรรม ลดอิทธิพลจากปัจจัยภายนอกที่อาจส่งผลกระทบต่อผลการทดลอง ทั้งนี้ยังช่วยให้สามารถวิเคราะห์ประสิทธิภาพของระบบแต่ละตัวได้อย่างแม่นยำในบริบทที่สอดคล้องกัน

3.2.1.2 เครื่องสำหรับสร้างแพ็กเก็ตการโจมตี เครื่องนี้ทำหน้าที่เป็นเครื่องกำเนิดแพ็กเก็ตการโจมตี โดยสร้างและส่งแพ็กเก็ตในรูปแบบต่าง ๆ ที่จำลองพฤติกรรมการโจมตีเครือข่ายไปยังเครื่องเป้าหมาย เพื่อใช้ทดสอบและประเมินความสามารถของระบบตรวจจับการบุกรุกในการตรวจจับภัยคุกคามเหล่านั้นอย่างมีประสิทธิภาพ โดยทำการสร้างและส่งแพ็กเก็ต ประเภทต่าง ๆ ที่จำลองรูปแบบการโจมตีทางเครือข่ายไปยังเครื่องเป้าหมาย เพื่อใช้ในการประเมินความสามารถของระบบตรวจจับ

3.2.1.3 เครื่องเป้าหมายในการโจมตี เป็นเครื่องที่จำลองบทบาทของระบบในองค์กรจริง ซึ่งทำหน้าที่รองรับการโจมตีจากเครื่องกำเนิดการโจมตี และใช้สำหรับบันทึกข้อมูล ปริมาณการรับส่ง และประเมินผลกระทบหรือความเสียหายที่เกิดขึ้นจากการโจมตีในแต่ละครั้ง

3.2.1.4 เครื่องสำหรับผู้ดูแลระบบ ทำหน้าที่เป็นเครื่องควบคุมและตรวจสอบกระบวนการทดลองทั้งหมด ผู้วิจัยใช้เครื่องนี้ในการตรวจสอบสถานะของเครื่องต่าง ๆ ภายในเครือข่าย ติดตามการโจมตี และบันทึกข้อมูลที่เกิดขึ้นระหว่างการทดลอง เพื่อใช้ในการวิเคราะห์ผลการทดสอบอย่างละเอียด

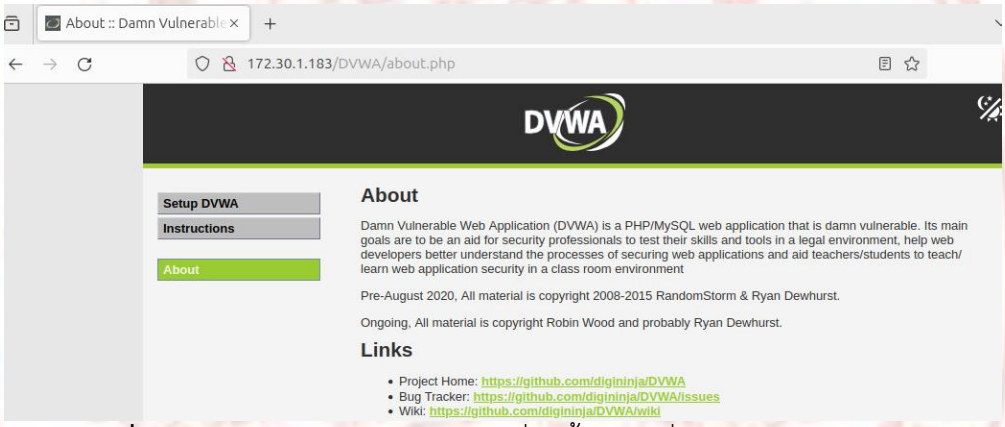


ภาพที่ 3-2 การตั้งค่าระบบเครือข่ายจำลองเสมือนบน VMware

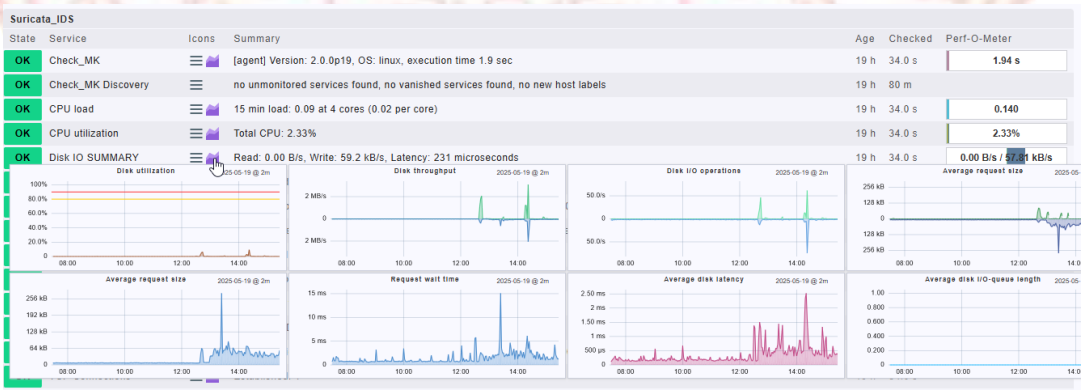
ในขั้นตอนนี้ได้ทำการติดตั้งและกำหนดค่าซอฟต์แวร์พื้นฐานและเครื่องมือที่จำเป็นสำหรับการสร้างสภาพแวดล้อมทดสอบ ทั้งในส่วนของเซิร์ฟเวอร์เว็บ ฐานข้อมูล ระบบควบคุมการเข้าถึง และเครื่องมือสำหรับการตรวจสอบระบบ เพื่อให้พร้อมใช้งานสำหรับการดำเนินการทดสอบและเก็บรวบรวมข้อมูลอย่างมีประสิทธิภาพ

ตารางที่ 3-1 โปรแกรมที่ติดตั้งเพิ่มเติมเพื่อประสิทธิภาพในการทดสอบ

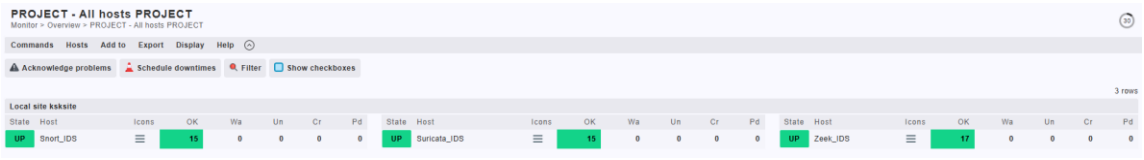
#	โปรแกรมติดตั้งเพิ่มเติม	ใช้สำหรับ	เครื่องที่ต้องทำการติดตั้ง
1	PHP Server	เซิร์ฟเวอร์ PHP สำหรับรันเว็บแอปพลิเคชัน DVWA	เครื่องเป้าหมายในการโจมตี
2	ฐานข้อมูล MariaDB	เก็บฐานข้อมูลของ DVWA	เครื่องเป้าหมายในการโจมตี
3	เว็บจำลองช่องโหว่ DVWA	สำหรับทดสอบด้วย SQLi, XSS, Brute Force	เครื่องเป้าหมายในการโจมตี
4	CheckMK	ระบบมอนิเตอร์และตรวจสอบสถานะของระบบ	เครื่องสำหรับผู้ดูแลระบบ
5	CheckMK Agent	เพื่อส่งข้อมูลให้ CheckMK Server นำไปตรวจสอบและมอนิเตอร์ระบบแบบเรียลไทม์	เครื่องสำหรับการตรวจจับการบุกรุก



ภาพที่ 3-3 เว็บจำลองช่องโหว่ DVWM ที่ติดตั้งบน เครื่องเป้าหมายในการโจมตี



ภาพที่ 3-4 โปรแกรม CheckMK ติดตั้งเพื่อ Monitoring สถานะของระบบ

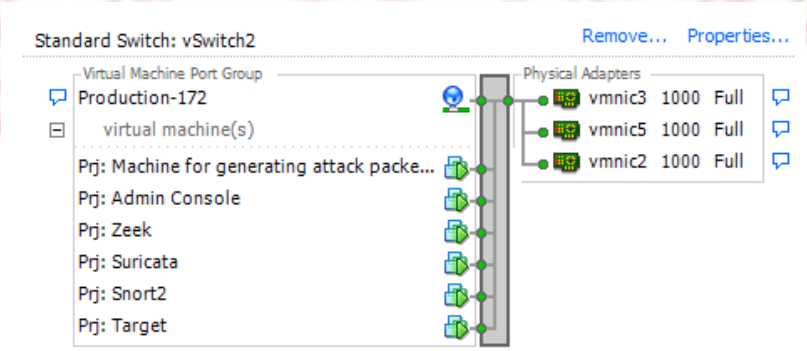


ภาพที่ 3-5 ติดตั้ง CheckMK Agent เพื่อให้ IDS System แสดงบนในระบบ CheckMK

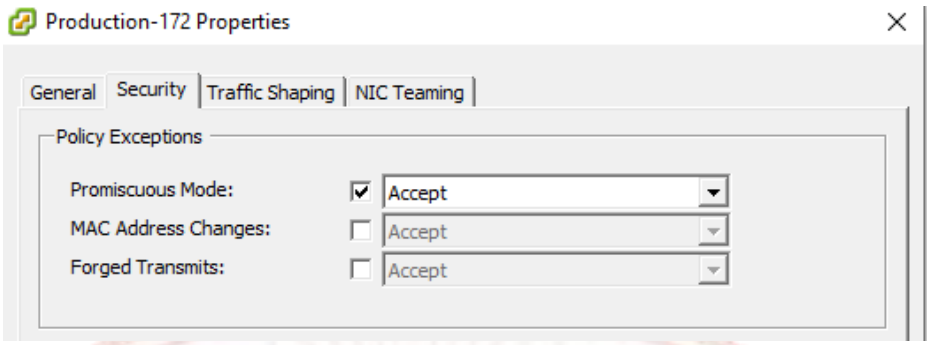
3.2.2 การตั้งค่าเครือข่าย

การตั้งค่าเครือข่ายในงานวิจัยนี้ได้ดำเนินการโดยการสร้างและจัดการระบบเครือข่ายเสมือน (Virtual Network) เดียวกัน เพื่อให้เครื่องเสมือนทุกเครื่องที่เกี่ยวข้องอยู่ในเครือข่ายเดียวกันอย่างสมบูรณ์แบบ โดยมีการกำหนดพารามิเตอร์และการเชื่อมต่อเครือข่ายที่เหมาะสม เพื่อให้สามารถสื่อสารกันได้อย่างราบรื่นและมีประสิทธิภาพสูงสุด การตั้งค่าเครือข่ายดังกล่าวช่วยให้การทดลองมีความเสถียร ลดปัจจัยแวดล้อมที่อาจส่งผลกระทบต่อผลลัพธ์ และสะดวกต่อการควบคุมและตรวจสอบการไหลของข้อมูลภายในระบบอย่างครบถ้วนทุกขั้นตอน

ในการทดลองนี้ ได้ออกแบบระบบเครือข่ายเสมือนเป็นระบบปิด (Isolated Network) โดยทั้งหมดอยู่ในเครือข่ายย่อยเดียวกัน (LAN) เพื่อให้สามารถส่งและรับทราฟฟิกระหว่างกันได้อย่างสมจริง ระบบเครือข่ายถูกกำหนดค่าให้ใช้ IP แบบ Static ในช่วง 172.30.1.0/24 และเชื่อมต่อผ่าน Virtual Switch เดียวกันภายในซอฟต์แวร์จำลอง VMware เพื่อควบคุมและแยกการทำงานจากเครือข่ายภายนอกอย่างสิ้นเชิง ทั้งนี้ ยังได้ตั้งค่า Network Interface ของเครื่อง IDS ให้ทำงานในโหมด Promiscuous Mode เพื่อสามารถตรวจสอบและวิเคราะห์ทราฟฟิกที่วิ่งผ่านเครือข่ายได้อย่างครบถ้วน



ภาพที่ 3-6 การสร้าง Network System บนเครือข่ายเสมือนเดียวกัน



ภาพที่ 3.7 เปิด Promiscuous Mode บนเครือข่ายเสมือน VWWare

3.2.3 การติดตั้งและกำหนดกฎเกณฑ์บนระบบตรวจจับการบุกรุก

ทำการติดตั้ง ระบบตรวจจับการบุกรุก ในแต่ละระบบปฏิบัติการ ตามระบบการตรวจจับการบุกรุกที่แจ้ง โดยมีรายละเอียดดังนี้

3.2.3.1 ระบบตรวจจับการบุกรุกสนอร์ต

การติดตั้งโปรแกรม ในการทดลองครั้งนี้ทางผู้ดำเนินการวิจัยได้ ติดตั้งระบบตรวจจับการบุกรุกสนอร์ต เวอร์ชัน 2.9.20 GRE (Build 82)

```
 ,,_     -*> Snort! <*-
o"  )~   Version 2.9.20 GRE (Build 82)
 ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
         Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
         Copyright (C) 1998-2013 Sourcefire, Inc., et al.
         Using libpcap version 1.10.4 (with TPACKET_V3)
         Using PCRE version: 8.39 2016-06-14
         Using ZLIB version: 1.3
```

ภาพที่ 3.8 เวอร์ชันของ ระบบตรวจจับการบุกรุกสนอร์ต (Snort)

กำหนดกฎเกณฑ์บนระบบตรวจจับการบุกรุกสนอร์ต เพื่อให้สามารถตรวจจับรูปแบบการบุกรุกที่หลากหลายและตรงตามเป้าหมายการทดสอบในงานวิจัยนี้ พร้อมทั้งตั้งค่าการแจ้งเตือนต่างๆ (Alerting Configuration) ดังนี้

ก) การโจมตีแบบไอซีเอ็มพีพิงฟลัด

```
alert icmp any any -> any any (msg:"ICMP Ping Flood Detected";
itype:8; dsize: >100; threshold:type threshold, track by_src,
count 50, seconds 1; sid:100001;)
```

กฎนี้จะตรวจจับและแจ้งเตือนผ่านการสร้าง อะเลิตล็อก หรือส่งข้อความแจ้งเตือนทันทีเมื่อพบว่ามีการส่งคำสั่ง ปิง (ICMP Echo Request) ขนาดใหญ่เกิน 100 ไบต์ จากเครื่องใดเครื่องหนึ่ง ไปยังเป้าหมายใดเป้าหมายหนึ่งอย่างรวดเร็วเกิน 50 ครั้งภายใน 1 วินาที ซึ่งเป็นลักษณะของการโจมตีแบบ ICMP Ping Flood โดยจะทำการแจ้งเตือน (Alert) “ICMP Ping Flood Detected"

ข) การโจมตีแบบสมิร์ฟแอตแทค

```
alert icmp any any -> 172.30.1.255 any (msg:"Possible Smurf
Attack"; itype:8; dsize:>100; sid:100002;)
```

กฎนี้จะตรวจจับและแจ้งเตือนผ่านการสร้าง อะเลิตล็อก (Alert Log) หรือส่งข้อความแจ้งเตือนทันทีเมื่อพบว่ามีการส่งคำสั่ง ปิง (ICMP Echo Request) ขนาดใหญ่เกิน 100 ไบต์ จากแหล่งใดก็ได้ ไปยังที่อยู่ปลายทาง 172.30.1.255 (ซึ่งเป็นที่อยู่ บรอดแคสต์ (Broadcast) ของเครือข่ายโดยจะทำการแจ้งเตือน (Alert) ด้วยข้อความว่า “Possible Smurf Attack” ซึ่งเป็นลักษณะของการโจมตีแบบ สมิร์ฟ แอตแทค ที่ใช้การส่งแพ็กเก็ต ICMP ไปยังที่อยู่ Broadcast เพื่อทำให้เกิดการโจมตีแบบปฏิเสธการให้บริการ (DoS) ต่อตัวเป้าหมาย

ค) การโจมตีแบบทีซีพีพอร์ตสแกน

```
alert tcp any any -> any any (msg:"TCP Port Scan Detected";
flags:S; threshold:type threshold, track by_src, count 10,
seconds 5; sid:100003;)
```

กฎนี้จะตรวจจับและแจ้งเตือนผ่านการสร้าง อะเลิตล็อก หรือส่งข้อความแจ้งเตือนทันทีเมื่อพบว่ามีการส่งแพ็กเก็ต TCP ที่มีแฟลก SYN (flags:S) จากแหล่งใดก็ได้ ไปยังปลายทางใดก็ได้ โดยหากพบการส่งแพ็กเก็ต SYN จากแหล่งเดียวกันเกิน 10 ครั้งภายในเวลา 5 วินาที จะถือว่าเป็นการสแกนพอร์ตแบบ SYN Scan และระบบจะส่งข้อความแจ้งเตือน ด้วยข้อความว่า “TCP Port Scan Detected”

ง) การโจมตีแบบทีซีพีซินฟลัด

```
alert tcp any any -> any 80 (msg:"TCP SYN Flood Attempt";
flags:S; threshold:type threshold, track by_src, count 100,
seconds 1; sid:100004;)
```

กฎนี้ทำหน้าที่ตรวจจับและแจ้งเตือนพฤติกรรมที่เข้าข่ายการโจมตีแบบทีซีพีซินฟลัด โดยจะเฝ้าสังเกตการส่ง แพ็กเก็ต TCP ที่มีแฟลก SYN (flags:S) จากแหล่งที่มาใดก็ได้ ไปยังพอร์ต 80 ของเครื่องปลายทาง หากตรวจพบว่าแหล่งที่มาเดียวกันส่งแพ็กเก็ตลักษณะดังกล่าวเกิน 100 ครั้งภายในเวลา 1 วินาที ระบบจะถือว่าเป็นพฤติกรรมที่ผิดปกติ และทำการสร้าง อะเลิตล็อก (Alert Log) หรือแจ้งเตือนทันทีด้วยข้อความว่า “TCP SYN Flood Attempt”)

จ) การโจมตีแบบบรูตฟอร์ซแอตแทค

```
alert tcp any any -> any 80 (msg:"Brute Force Login Attempt
Detected"; flow:to_server,established; content:"POST"; nocase;
http_method; content:"/DVWA/login.php"; nocase; http_uri;
sid:100005; rev:1;)
```

กฎนี้จะตรวจจับและแจ้งเตือนผ่านการสร้าง อะเลิตล็อก (Alert Log) หรือส่งข้อความแจ้งเตือนทันทีเมื่อพบว่า มีการส่งคำขอ POST ไปยังหน้าเว็บ /DVWA/login.php ซึ่งเป็นพฤติกรรมที่ส่อถึงความพยายามในการเข้าสู่ระบบหลายครั้ง โดยระบบจะตรวจสอบว่าแพ็กเก็ตเป็นแบบ TCP ที่กำลังส่งไปยังพอร์ต 80 (HTTP) และต้องอยู่ในสถานะ เชื่อมต่อ (established) พร้อมตรวจสอบว่าเนื้อหาของคำขอเป็น "POST" และกำหนดเส้นทาง (URI) ไปยัง "/DVWA/login.php"หากตรงตามเงื่อนไขดังกล่าว ระบบจะส่งข้อความแจ้งเตือน (Alert) ด้วยข้อความว่า“Brute Force Login Attempt Detected”

ฉ) การโจมตีแบบเอสคิวแอลอินเจ็กชัน

```
alert tcp any any -> any 80 (msg:"SQL Injection Attempt
Detected"; content:"' or 1=1"; nocase; sid:100006; rev:1;)
```

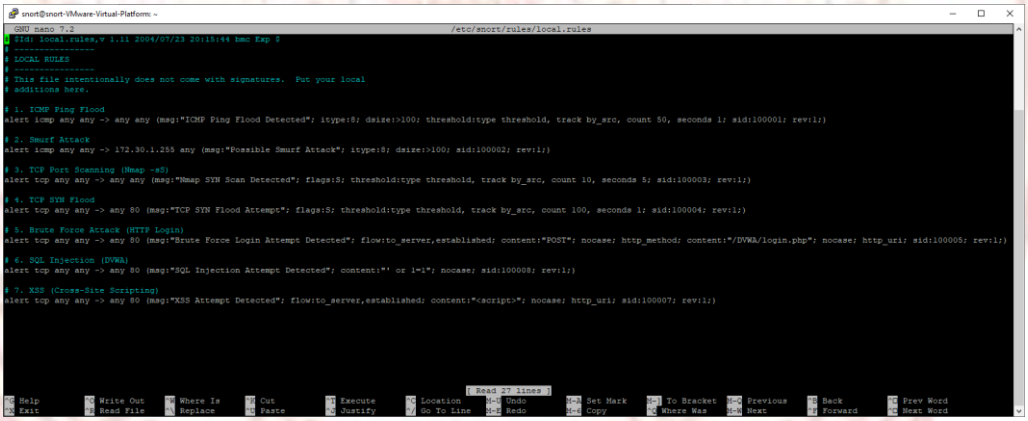
กฎนี้ทำหน้าที่ตรวจจับและแจ้งเตือนพฤติกรรมที่เข้าข่ายการโจมตีแบบเอสคิวแอลอินเจ็กชัน โดยจะตรวจสอบการส่งแพ็กเก็ต TCP ที่มีเนื้อหาภายในประกอบด้วยคำหรือรูปแบบที่มักใช้ในการโจมตี เช่น "‘ or 1=1" ซึ่งเป็นเทคนิคที่ผู้ไม่หวังดีใช้เพื่อหลอกให้ระบบยอมรับข้อมูลที่ผิดปกติและเข้าถึงฐานข้อมูลโดยไม่ได้รับอนุญาต หากตรวจพบคำดังกล่าวในแพ็กเก็ตที่ส่งมายังพอร์ต 80 ระบบ

จะทำการสร้าง อะเลิตล็อก (Alert Log) หรือแจ้งเตือนทันทีด้วยข้อความว่า “SQL Injection Attempt Detected”

ช) การโจมตีแบบครอสไซต์สคริปต์ติ้ง

alert tcp any any -> any 80 (msg:"XSS Attempt Detected"; flow:to_server,established; content:"<script>"; nocase; http_uri; sid:100007;)

กฎนี้ใช้สำหรับตรวจจับและแจ้งเตือนการโจมตีแบบครอสไซต์สคริปต์ติ้ง โดยจะตรวจสอบแพ็กเก็ต TCP ที่ส่งไปยังพอร์ต 80 ซึ่งมีลักษณะเป็นทราฟฟิกที่กำลังส่งไปยังเซิร์ฟเวอร์ (ตามที่กำหนดด้วย flow:to_server,established;) และมีเนื้อหาที่สำคัญภายใน URI ของ HTTP ที่ประกอบด้วยคำว่า "<script>" ซึ่งเป็นรูปแบบพื้นฐานที่มักใช้ในการโจมตีครอสไซต์สคริปต์ติ้ง หากตรวจพบลักษณะดังกล่าว ระบบจะทำการสร้าง อะเลิตล็อก (Alert Log) หรือส่งข้อความแจ้งเตือนทันทีด้วยข้อความว่า “XSS Attempt Detected”

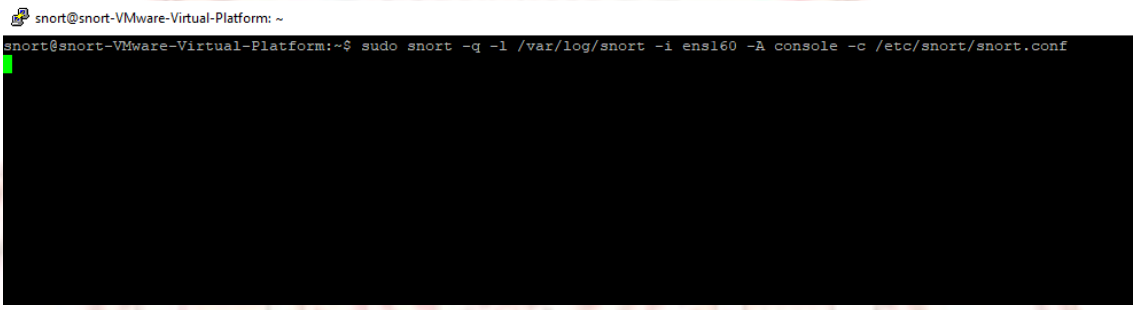


ภาพที่ 3.9 Location ในการ setup Snort IDS Rules /etc/snort/rules/local.rules

ในระบบตรวจจับการบุกรุกสนอร์ต (Snort) สามารถตรวจสอบ Rules ที่ Setup ดังนี้ snort -q -l /var/log/snort -i ens160 -A console -c /etc/snort/snort.conf โดยชุดคำสั่ง (Command) เพื่อใช้สำหรับเรียกใช้งานโปรแกรม Snort ในโหมดตรวจจับการบุกรุกบนเครือข่าย (NIDS) โดยทำงานผ่านอินเตอร์เฟซเครือข่าย ens160 โดยใช้กฎและการตั้งค่าต่าง ๆ ที่กำหนดไว้ในไฟล์ snort.conf พร้อมทั้งเก็บบันทึกผลการตรวจจับลงในไดเรกทอรี /var/log/snort และแสดงผลการแจ้งเตือน (Alert)

แบบเรียลไทม์ผ่านหน้าจอคอนโซล ทั้งนี้การรันคำสั่งจะทำงานในโหมดเงียบ (quiet mode) เพื่อไม่ให้แสดงข้อความที่ไม่จำเป็น ขณะเดียวกันก็ให้สิทธิ์ระดับผู้ดูแลระบบด้วย

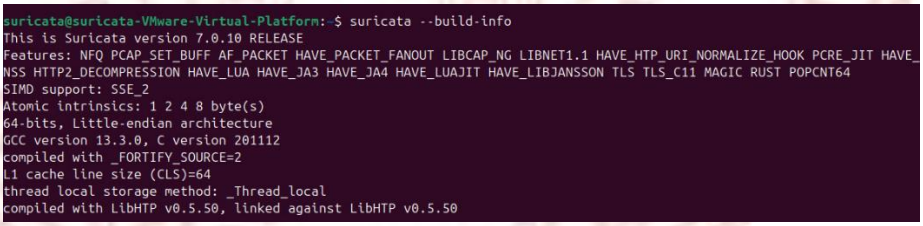
โดยชุดคำสั่ง (Command) ดังกล่าวสามารถตรวจสอบได้ว่ากฎที่ได้ตั้งไว้สามารถใช้งานได้หรือไม่ ถ้าเมื่อรันชุดคำสั่งเมื่อดังกล่าวแล้วไม่มี เออเร่อ (Error) หรือ อะเลิต (Alert) เกิดขึ้นแสดงว่าการตั้งค่าและกฎสามารถใช้งานได้ปกติใน ระบบตรวจจับการบุกรุกสนอร์ต (Snort)



ภาพที่ 3.10 ตรวจสอบ กฎ (Rules) ใน ระบบตรวจจับการบุกรุกสนอร์ต (Snort)

3.2.3.2 ระบบตรวจจับการบุกรุกซูริกาต้า

การติดตั้งโปรแกรม ในการทดลองครั้งนี้ทางผู้ดำเนินการวิจัยได้ ติดตั้งระบบตรวจจับการบุกรุกซิริกาต้า เวอร์ชัน 7.0.10 RELEASE



ภาพที่ 3.11 เวอร์ชัน ของ ระบบตรวจจับการบุกรุกซูริกาต้า (Suricata)

กำหนดกฎเกณฑ์บนระบบตรวจจับการบุกรุก เพื่อให้สามารถตรวจจับรูปแบบการบุกรุกที่หลากหลายและตรงตามเป้าหมายการทดสอบในงานวิจัยนี้ พร้อมทั้งตั้งค่าการแจ้งเตือนต่างๆ (Alerting Configuration) ดังนี้

ก) การโจมตีแบบไอซีเอ็มพีพิงฟลัด (ICMP Ping Flood)

```
alert icmp any any -> any any (msg:"ICMP Ping Flood Detected";
itype:8; dsize: >100; threshold:type threshold, track by_src,
count 50, seconds 1; sid:100001;)
```

กฎนี้จะตรวจจับและแจ้งเตือนผ่านการสร้าง อะเลิตล็อก หรือส่งข้อความแจ้งเตือนทันทีเมื่อพบว่ามีการส่งคำสั่ง ปิง (ICMP Echo Request) ขนาดใหญ่เกิน 100 ไบต์ จากเครื่องใดเครื่องหนึ่ง ไปยังเป้าหมายใดเป้าหมายหนึ่งอย่างรวดเร็วเกิน 50 ครั้งภายใน 1 วินาที ซึ่งเป็นลักษณะของการโจมตีแบบไอซีเอ็มพีพิงฟลัด โดยจะทำการแจ้งเตือน (Alert) “ICMP Ping Flood Detected"

ข) การโจมตีแบบสมิร์ฟแอตแทค

```
alert icmp any any -> 172.30.1.255 any (msg:"Possible Smurf
Attack"; itype:8; dsize:>100; sid:100002;)
```

กฎนี้จะตรวจจับและแจ้งเตือนผ่านการสร้าง อะเลิตล็อก (Alert Log) หรือส่งข้อความแจ้งเตือนทันทีเมื่อพบว่ามีการส่งคำสั่ง ปิง (ICMP Echo Request) ขนาดใหญ่เกิน 100 ไบต์ จากแหล่งใดก็ได้ ไปยังที่อยู่ปลายทาง 172.30.1.255 (ซึ่งเป็นที่อยู่ บรอดแคสต์ (Broadcast) ของเครือข่ายโดยจะทำการแจ้งเตือน (Alert) ด้วยข้อความว่า “Possible Smurf Attack” ซึ่งเป็นลักษณะของการโจมตีแบบ สมิร์ฟ แอตแทค ที่ใช้การส่งแพ็กเก็ต ICMP ไปยังที่อยู่ Broadcast เพื่อทำให้เกิดการโจมตีแบบปฏิเสธการให้บริการ (DoS) ต่อตัวเป้าหมาย

ค) การโจมตีแบบทีซีพีพอร์ตสแกน

```
alert tcp any any -> any any (msg:"TCP Port Scan Detected";
flags:S; threshold:type threshold, track by_src, count 10, seconds
5; sid:100003;)
```

กฎนี้จะตรวจจับและแจ้งเตือนผ่านการสร้าง อะเลิตล็อก หรือส่งข้อความแจ้งเตือนทันทีเมื่อพบว่ามีการส่งแพ็กเก็ต TCP ที่มีแฟลก SYN (flags:S) จากแหล่งใดก็ได้ ไปยังปลายทางใดก็ได้ โดยหากพบการส่งแพ็กเก็ต SYN จากแหล่งเดียวกันเกิน 10 ครั้งภายในเวลา 5 วินาที จะถือว่าเป็นการสแกนพอร์ตแบบ SYN Scan และระบบจะส่งข้อความแจ้งเตือน ด้วยข้อความว่า “TCP Port Scan Detected”

ง) การโจมตีแบบทีซีพีซินฟลัด

```
alert tcp any any -> any 80 (msg:"TCP SYN Flood Attempt";
flags:S; threshold:type threshold, track by_src, count 100,
seconds 1; sid:100004;)
```

กฎนี้ทำหน้าที่ตรวจจับและแจ้งเตือนพฤติกรรมที่เข้าข่ายการโจมตีแบบทีซีพี ซินฟลัด โดยจะเฝ้าสังเกตการส่ง แพ็กเก็ต TCP ที่มีแฟลก SYN (flags:S) จากแหล่งที่มาใดก็ได้ ไปยังพอร์ต 80 ของเครื่องปลายทาง หากตรวจพบว่าแหล่งที่มาเดียวกันส่งแพ็กเก็ตลักษณะดังกล่าวเกิน 100 ครั้งภายในเวลา 1 วินาที ระบบจะถือว่าเป็นพฤติกรรมที่ผิดปกติ และทำการสร้าง อะเลิตล็อก (Alert Log)หรือแจ้งเตือนทันทีด้วยข้อความว่า “TCP SYN Flood Attempt”)

จ) การโจมตีแบบบรูตฟอร์ซแอตแทค

```
alert tcp any any -> any 80 (msg:"Brute Force Login Attempt
Detected"; flow:to_server,established; content:"POST"; nocase;
http_method; content:"/DVWA/login.php"; nocase; http_uri;
sid:100005; rev:1;)
```

กฎนี้จะตรวจจับและแจ้งเตือนผ่านการสร้าง อะเลิตล็อก (Alert Log) หรือส่งข้อความแจ้งเตือนทันทีเมื่อพบว่า มีการส่งคำขอ POST ไปยังหน้าเว็บ /DVWA/login.php ซึ่งเป็นพฤติกรรมที่ส่อถึงความพยายามในการเข้าสู่ระบบหลายครั้ง ระบบจะตรวจสอบว่าแพ็กเก็ตเป็นแบบ TCP ที่กำลังส่งไปยังพอร์ต 80 (HTTP) และต้องอยู่ในสถานะ เชื่อมต่อ (established) พร้อมตรวจสอบว่าเนื้อหาของคำขอเป็น "POST" และกำหนดเส้นทาง (URI) ไปยัง "/DVWA/login.php"หากตรงตามเงื่อนไขดังกล่าว ระบบจะส่งข้อความแจ้งเตือน (Alert) ด้วยข้อความว่า“Brute Force Login Attempt Detected”

ฉ) การโจมตีแบบเอสคิวแอลอินเจ็กชัน

```
alert tcp any any -> any 80 (msg:"SQL Injection Attempt
Detected"; content:"' or 1=1"; nocase; sid:100006; rev:1;)
```

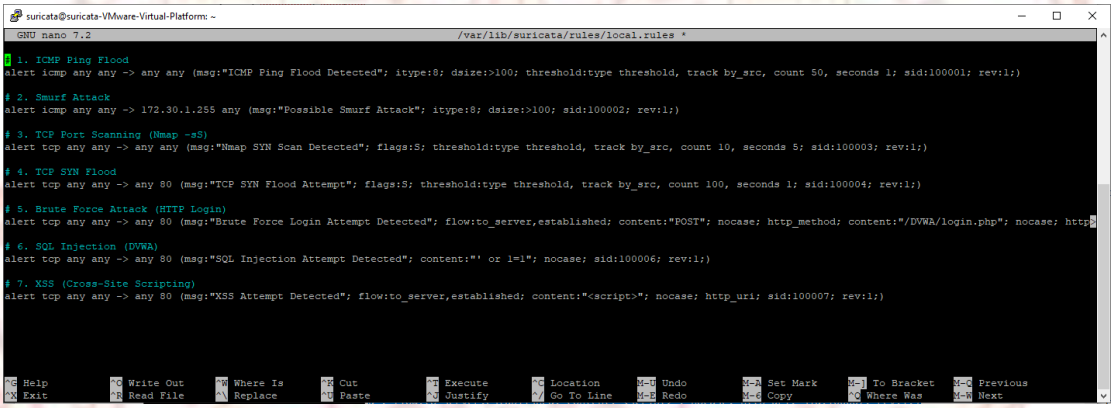
กฎนี้ทำหน้าที่ตรวจจับและแจ้งเตือนพฤติกรรมที่เข้าข่ายการโจมตีแบบเอสคิวแอลอินเจกชัน โดยจะตรวจสอบการส่งแพ็กเก็ต TCP ที่มีเนื้อหาภายในประกอบด้วยคำหรือรูปแบบที่มักใช้ในการโจมตี เช่น "‘ or 1=1" ซึ่งเป็นเทคนิคที่ผู้ไม่หวังดีใช้เพื่อหลอกให้ระบบยอมรับข้อมูลที่ผิดปกติและเข้าถึงฐานข้อมูลโดยไม่ได้รับอนุญาต หากตรวจพบคำดังกล่าวในแพ็กเก็ต ระบบจะทำการสร้าง

อะเลิตล็อก (Alert Log) หรือแจ้งเตือนทันทีด้วยข้อความว่า “SQL Injection Attempt Detected”

ช) การโจมตีแบบครอสไซต์สคริปต์ติ้ง

alert tcp any any -> any 80 (msg:"XSS Attempt Detected";
flow:to_server,established; content:"<script>"; nocase; http_uri;
sid:100007;)

กฎนี้ใช้สำหรับตรวจจับและแจ้งเตือนการโจมตีแบบครอสไซต์สคริปต์ติ้ง โดยจะตรวจสอบแพ็กเก็ต TCP ที่ส่งไปยังพอร์ต 80 ซึ่งมีลักษณะเป็นทราฟฟิกที่กำลังส่งไปยังเซิร์ฟเวอร์ (ตามที่กำหนดด้วย flow:to_server,established;) และมีเนื้อหาภายใน URI ของ HTTP ที่ประกอบด้วยคำว่า "<script>" ซึ่งเป็นรูปแบบพื้นฐานที่มักใช้ในการโจมตีแบบครอสไซต์สคริปต์ติ้ง หากตรวจพบลักษณะดังกล่าว ระบบจะทำการสร้าง อะเลิตล็อก (Alert Log) หรือส่งข้อความแจ้งเตือนทันทีด้วยข้อความว่า “XSS Attempt Detected”

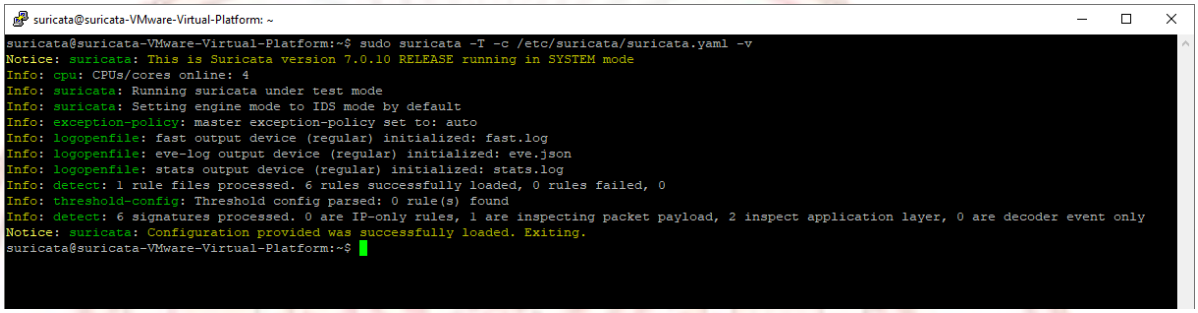


ภาพที่ 3-12 Location ในการตั้งค่า Suricata IDS Rules/var/lib/suricata/rules/local.rules

ในระบบตรวจจับการบุกรุกซูริกาต้า (Suricata) สามารถตรวจสอบ Rules ที่ Setup ดังนี้ sudo suricata -T -c /etc/suricata/suricata.yaml -v โดยชุดคำสั่ง (Command) เป็นคำสั่งที่ใช้เรียกโปรแกรม Suricata ด้วยสิทธิ์ผู้ดูแลระบบ (sudo) เพื่อทำการทดสอบการตั้งค่าของ Suricata โดยใช้ไฟล์คอนฟิก /etc/suricata/suricata.yaml โดยตัวเลือก -T หมายถึงโหมดทดสอบ (Test) ซึ่งจะตรวจสอบความถูกต้องของไฟล์คอนฟิกโดยไม่เริ่มทำงานจริง ส่วน -v เป็นการแสดงผลแบบละเอียด

(Verbose) เพื่อให้เห็นข้อมูลต่าง ๆ ขณะทำการทดสอบ ทำให้ผู้ใช้สามารถตรวจสอบว่าไฟล์ตั้งค่าถูกต้องและไม่มีข้อผิดพลาดก่อนจะเริ่มใช้งานจริงได้อย่างมั่นใจ

ชุดคำสั่ง (Command) ดังกล่าวสามารถตรวจสอบ ได้ว่ากฎที่ได้ตั้งไว้สามารถใช้งานได้หรือไม่ ถ้าเมื่อรันชุดคำสั่งเมื่อดังกล่าวแล้วไม่มี เออเร่อ หรือ อะเลิต เกิดขึ้นแสดงว่าการตั้งค่าและกฎสามารถใช้งานได้ปกติใน ระบบตรวจจับการบุกรุกซูริกาต้า

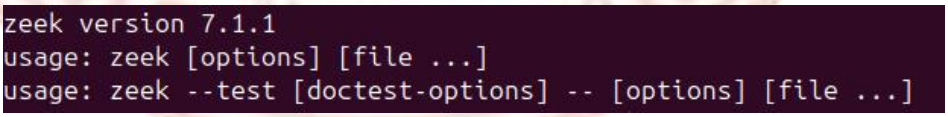


ภาพที่ 3-13 ตรวจสอบกฎในระบบตรวจจับการบุกรุกซูริกาต้า (Suricata)

จากรายละเอียดกฎข้างต้นจะพบว่า สนอร์ต และ ซูริกาต้า ใช้รูปแบบการเขียนกฎ (Rule Syntax) เดียวกัน เนื่องจากระบบตรวจจับการบุกรุกซูริกาต้า นั้นได้ถูกออกแบบมาให้รองรับกฎของสนอร์ต โดยตรงเพื่อความเข้ากันได้ของระบบ

3.2.3.3 ระบบตรวจจับการบุกรุกซีค

การติดตั้งโปรแกรม ในการทดลองครั้งนี้ทางผู้ดำเนินการวิจัยได้ ติดตั้งระบบตรวจจับการบุกรุกซีค เวอร์ชัน 7.1.1



ภาพที่ 3-14 เวอร์ชันของ ระบบตรวจจับการบุกรุกซีค (Zeek)

กำหนดกฎเกณฑ์บนระบบตรวจจับการบุกรุก เพื่อให้สามารถตรวจจับรูปแบบการบุกรุกที่หลากหลายและตรงตามเป้าหมายการทดสอบในงานวิจัยนี้ พร้อมทั้งตั้งค่าการแจ้งเตือนต่างๆ (Alerting Configuration) ดังนี้

ก) การโจมตีแบบไอซีเอ็มพีพิงฟลัด

```
if (c$id$proto == 1 && c$duration < 1sec) {
print fmt("ICMP Ping Flood detected: %s -> %s", c$id$orig_h,
c$id$resp_h);
}
```

กฎนี้จะตรวจจับและแจ้งเตือนทันทีเมื่อพบว่ามีแพ็กเก็ตโปรโตคอล ICMP (ซึ่งมีค่า proto == 1) ที่ส่งติดต่อกันรวดเร็ว ภายในระยะเวลาน้อยกว่า 1 วินาที (duration < 1sec) โดยเงื่อนไขนี้หมายถึงการส่งคำสั่ง ปิง หลายครั้งในช่วงเวลาสั้นๆ ซึ่งเป็นลักษณะของการโจมตีแบบไอซีเอ็มพีพิงฟลัด พบเหตุการณ์ดังกล่าว ระบบจะทำการพิมพ์ข้อความแจ้งเตือนในล็อกว่า“ ICMP Ping Flood detected: [IP ต้นทาง] -> [IP ปลายทาง]”โดยแทนที่ [IP ต้นทาง] และ [IP ปลายทาง] ด้วยที่อยู่ IP ของเครื่องที่ส่งและเครื่องที่รับ ตามลำดับ

ข) การโจมตีแบบสมิร์ฟแอตแทค

```
if (c$id$proto == 1 && c$id$resp_h == 172.30.1.255 &&
c$orig_bytes > 100) {print fmt("Smurf Attack detected: %s ->
Broadcast (%s)", c$id$orig_h, c$id$resp_h);
}
```

กฎนี้จะตรวจจับและแจ้งเตือนทันทีเมื่อพบการส่งแพ็กเก็ต ICMP (ซึ่งมีค่า proto == 1) จากเครื่องใดเครื่องหนึ่ง ไปยังที่อยู่ Broadcast (ในที่นี้คือ 172.30.1.255) โดยมีขนาดข้อมูลต้นทาง (orig_bytes) มากกว่า 100 ไบต์ ซึ่งเป็นลักษณะของการโจมตีแบบสมิร์ฟแอตแทค การโจมตีที่ผู้ไม่หวังดีส่ง ICMP Echo Request ไปยัง Broadcast Address ของเครือข่ายโดยใช้ IP ปลอม (IP ของเหยื่อ) เป็นต้นทาง ทำให้ทุกเครื่องในเครือข่ายตอบกลับพร้อมกันไปยังเหยื่อ ทำให้ระบบของเหยื่อรับโหลดมหาศาล เมื่อมีเหตุการณ์ที่ตรงตามเงื่อนไขนี้ ระบบจะพิมพ์ข้อความแจ้งเตือนในล็อกว่า“ Smurf Attack detected: [IP ต้นทาง] -> Broadcast ([IP ปลายทาง])”โดยแทนที่ [IP ต้นทาง] และ [IP ปลายทาง] ด้วย IP ของเครื่องที่ส่งและที่อยู่ broadcast ตามลำดับ

ค) การโจมตีแบบ ทีซีพี พอร์ตสแกน

```
global syn_scan_count: table[addr] of count = 0;
const scan_threshold = 10;
event connection_established(c: connection) {
if (c$id$proto == 6 && c$state == ConnState::SYN_SENT) {
syn_scan_count[c$id$orig_h] += 1;
if (syn_scan_count[c$id$orig_h] == scan_threshold) {
  print fmt("TCP Port Scan detected from: %s", c$id$orig_h);
        }
      }
    }
```

กฎนี้จะตรวจจับการโจมตีแบบทีซีพีพอร์ตสแกน โดยใช้ตัวแปร syn_scan_count เพื่อนับจำนวนการส่ง TCP SYN (proto == 6 และ state == SYN_SENT) จากแต่ละ IP ต้นทาง โดยหากเครื่องใดส่งแพ็กเก็ต SYN ครบ 10 ครั้ง (scan_threshold) ระบบจะพิมพ์ข้อความแจ้งเตือน “TCP Port Scan detected from: [IP ต้นทาง]”

ง) การโจมตีแบบ ทีซีพี ซินฟลัด

```
if (c$id$proto == 6 && c$state == ConnState::SYN_SENT &&
c$id$resp_p == 80) {
print fmt("TCP SYN Flood detected: %s -> %s:%s", c$id$orig_h,
c$id$resp_h, c$id$resp_p);
}
```

กฎนี้จะตรวจจับและแจ้งเตือนทันทีเมื่อพบว่ามีการส่งแพ็กเก็ต TCP (ซึ่งมีค่า proto == 6) โดยอยู่ในสถานะ SYN_SENT (หมายถึงมีการส่ง TCP SYN เพื่อเริ่มต้นการเชื่อมต่อ แต่ยังไม่มีการตอบกลับจากฝั่งปลายทาง) ไปยังพอร์ต 80 (HTTP) ของเครื่องเป้าหมาย ซึ่งเป็นลักษณะของการโจมตีแบบทีซีพีซินฟลัด โดยการโจมตีที่ผู้ไม่หวังดีส่ง SYN จำนวนมากไปยังพอร์ตปลายทาง ทำให้เครื่องเป้าหมายต้องกันทรัพยากรไว้รอการตอบกลับที่ไม่มีวันมาถึง จนไม่สามารถให้บริการปกติได้เมื่อพบเหตุการณ์ดังกล่าว ระบบจะพิมพ์ข้อความแจ้งเตือนในล็อกว่า “TCP SYN Flood detected: [IP ต้น

ทาง] -> [IP ปลายทาง]:[พอร์ต]”โดยจะแทนที่ [IP ต้นทาง], [IP ปลายทาง], และ [พอร์ต] ด้วยค่าจริงจากแพ็กเก็ตที่ตรวจพบ

จ) การโจมตีแบบ บรูตฟอร์ซแอตแทค if (method == "POST" && uri == "/DVWA/login.php" && /username=/ in body && /password=/ in body) {

print fmt("Possible brute force attempt: %s requested %s", cidorig_h, uri);

}

กฎนี้จะตรวจจับความพยายามโจมตีแบบ Brute Force ผ่านเว็บ โดยตรวจสอบว่ามีการส่ง HTTP POST มายังหน้า /DVWA/login.php พร้อมข้อมูลใน body ที่มีคำว่า username= และ password= ซึ่งเป็นลักษณะของการพยายามเข้าสู่ระบบแบบเดาสุ่มรหัสผ่าน เมื่อเงื่อนไขเป็นจริง ระบบจะพิมพ์ข้อความแจ้งเตือนว่า “Possible brute force attempt: [IP ต้นทาง] requested /DVWA/login.php” เพื่อแจ้งให้ทราบถึงพฤติกรรมต้องสงสัยที่อาจเป็นการโจมตีแบบบรูตฟอร์ซแอตแทค ผ่านฟอร์มล็อกอินของแอปพลิเคชัน DVWA

ฉ) การโจมตีแบบเอสคิวแอลอินเจ็กชัน

if (/(or\s+1=1|or|and)\s*=\s*1\s*--/i in uri) {

print fmt("SQL Injection attempt detected from: %s URI: %s", cidorig_h, uri);

}

กฎนี้จะตรวจจับการโจมตีแบบเอสคิวแอลอินเจกชัน โดยตรวจสอบว่าในค่า uri มีรูปแบบของคำสั่งที่มักใช้ในการโจมตี เช่น or 1=1--, or =1--, หรือ and =1-- ซึ่งเป็นเทคนิคที่ผู้โจมตีนำไปใช้หลอกฐานข้อมูลให้คืนค่าที่ไม่ควร เมื่อพบรูปแบบเหล่านี้ในคำร้องขอ URL ระบบจะพิมพ์ข้อความแจ้งเตือนว่า “SQL Injection attempt detected from: [IP ต้นทาง] URI: [URI]”

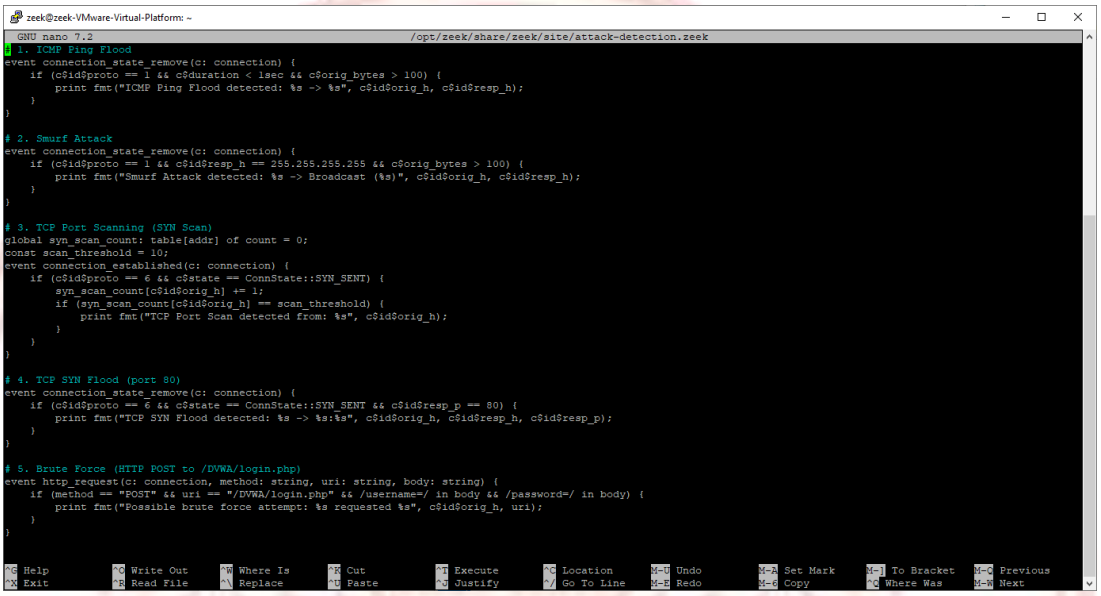
ช) การโจมตีแบบ ครอสไซต์สคริปต์ติ้ง

if (/<script>/i in uri) {

print fmt("XSS attempt detected from: %s to URI: %s", cidorig_h, uri);

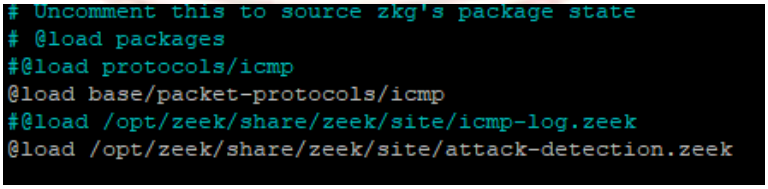
}

กฎนี้จะตรวจจับการโจมตีแบบครอสไซต์สคริปต์ติ้ง โดยตรวจสอบว่าในค่า uri มีแท็ก <script> ซึ่งเป็นโค้ด JavaScript ที่มักใช้ในการฝังสคริปต์อันตรายลงในหน้าเว็บ เมื่อพบลักษณะดังกล่าว ระบบจะพิมพ์ข้อความแจ้งเตือนว่า “XSS attempt detected from: [IP ต้นทาง] to URI: [URI]”



ภาพที่ 3.15 Location ในการตั้งค่า Zeek IDS Rules /opt/zeek/share/zeek/site/attack-detection.zeek

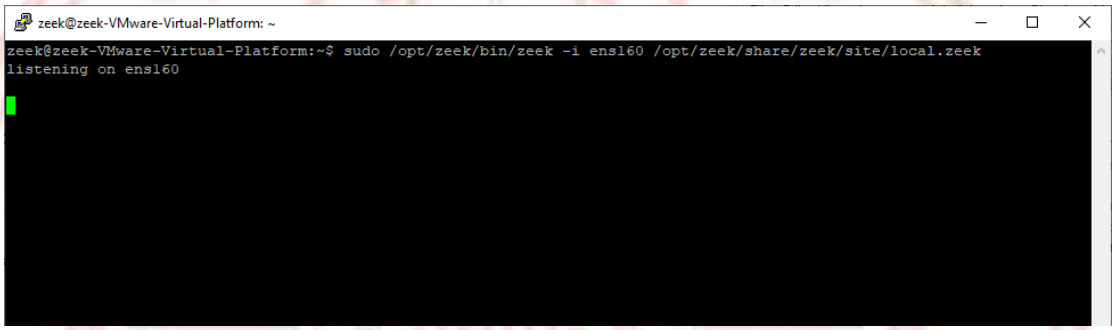
โดยปกติแล้วตำแหน่งที่อยู่ ของไฟล์ กฎของซีค (Zeek Rules) จะอยู่ที่ พาร์ทไดเร็กทอรี่ (Path Directory) /opt/zeek/share/zeek/site/local.zeek แต่ผู้ทำการวิจัยได้แยกไฟล์ออกมาเพื่อง่ายต่อการบริหารจัดการ โดยผู้ทำการวิจัยได้ทำการสร้างไฟล์ กฎของซีค ใหม่ที่ชื่อว่า attack-detection.zeek โดยไว้ที่ location /opt/zeek/share/zeek/site/attack-detection.zeek และได้ทำการ เพิ่ม @load ชื่อ Location/ชื่อไฟล์ใหม่ในไฟล์ชื่อ local.zeek



ภาพที่ 3.16 แยกไฟล์ กฎ ออกมาเพื่อง่ายต่อการบริหารจัดการ

ในระบบตรวจจับการบุกรุกซีค สามารถตรวจสอบกฎที่ได้ทำการตั้งค่าต่างๆไว้ ได้ดังนี้ sudo/opt/zeek/bin/zeek -i ens160 /opt/zeek/share/zeek/site/local.zeek โดยชุดคำสั่ง (Command) คำสั่งนี้ใช้เพื่อเรียกซีค ให้ทำงานบนอินเตอร์เฟซเครือข่าย ens160 โดยใช้สิทธิ์ root ผ่าน sudo และโหลดสคริปต์ local.zeek ที่อยู่ใน /opt/zeek/share/zeek/site/

ชุดคำสั่ง (Command) ดังกล่าวสามารถตรวจสอบ ได้ว่ากฎที่ได้ตั้งไว้สามารถใช้งานได้หรือไม่ ถ้าเมื่อรันชุดคำสั่งเมื่อดังกล่าวแล้วไม่มี เออเร่อ หรือ อะเลิต เกิดขึ้นแสดงว่าการตั้งค่าและกฎสามารถใช้งานได้ปกติใน ระบบตรวจจับการบุกรุกซีค



ภาพที่ 3.17 ตรวจสอบ กฎ ในระบบตรวจจับการบุกรุกซีค (Zeek)

จากรายละเอียดข้างต้น จะพบว่า กฎของระบบตรวจจับการบุกรุกซีค มี สคริปต์รูปแบบกฎ (Rules pattern script) ที่แตกต่างอย่างเห็นเด่นชัด มีความซับซ้อน และยากต่อการเขียน มากกว่าจาก ระบบตรวจจับการบุกรุก ยี่ห้ออื่นอย่างชัดแจน

3.2.4 การทดสอบการบุกรุก

ในการประเมินประสิทธิภาพของระบบตรวจจับภัยคุกคาม ได้มีการจำลองการโจมตีทางจำนวน 7 ประเภท โดยใช้เครื่องมือและสคริปต์ในเครือข่ายจำลอง จำนวน 1000 ครั้ง ต่อ 1 รูปแบบการโจมตี เพื่อให้สามารถวัดความสามารถในการตรวจจับของระบบ IDS ได้อย่างมีประสิทธิภาพ การทดสอบแบ่งออกเป็นหัวข้อย่อยดังนี้ โดยมี 172.30.1.183 เป็นไอพีเป้าหมาย (IP Target) และ 172.30.1.255 เป็นบรอดแคสต์ไอพี (Broadcast IP)

ก) การโจมตีด้วยไอซีเอ็มพีพิงฟลัด

ชุดคำสั่ง ping -f -c 1000 172.30.1.183

-f = ส่งแพ็กเก็ตแบบ flood อย่างรวดเร็ว ไปยัง IP เป้าหมาย

-c 1000 = ส่ง 1,000 แพ็กเก็ต

โดยมีวัตถุประสงค์คือเพื่อส่ง ICMP Echo Request อย่างรวดเร็วไปยังเครื่องเป้าหมายจำนวนมากในเวลาสั้นๆ

และมีผลลัพธ์ที่คาดหวัง เครื่องเป้าหมายอาจมีภาระโหลดสูงจากการตอบ ICMP Echo Reply และ ระบบตรวจจับการบุกรุก แจ้งเตือนว่าเกิดไอซีเอ็มพีพิงฟลัด

ข) การโจมตีด้วยสมิร์ฟแอตแทค

ชุดคำสั่ง hping3 -1 --flood --spoof 172.30.1.183 172.30.1.255 --count 1000

-1 = ส่ง ICMP Echo Request (type 8)

--flood = ส่งแพ็กเก็ตแบบเร็วมาก

--spoof 172.30.1.183 = ปลอมแปลง IP ต้นทางเป็นเป้าหมาย

172.30.1.255 = ส่งไปที่ Broadcast

--count 1000 = ส่ง 1,000 แพ็กเก็ต

วัตถุประสงค์ ทดสอบการโจมตีแบบ Smurf โดยทำให้เครื่องทั้งหมดในเครือข่ายตอบกลับไปยังเหยื่อ

ผลลัพธ์ที่คาดหวัง เครื่องเป้าหมายได้รับ ICMP Echo Reply จำนวนมาก และ ระบบตรวจจับการบุกรุก แจ้งเตือนว่ามีการโจมตีด้วยสมิร์ฟแอตแทค

ค) การโจมตีด้วยทีซีพีพอร์ตสแกน

ชุดคำสั่ง for i in {1..1000}; do nmap -sS -p $i 172.30.1.183; done

-sS = สแกนแบบ TCP SYN

-p $i = เปลี่ยนพอร์ตในแต่ละรอบ

ลูป for สแกนพอร์ต 1–1000 ทีละพอร์ต

วัตถุประสงค์ เพื่อสแกนพอร์ตว่าใดเปิดอยู่บนเครื่องเป้าหมาย โดยใช้เทคนิคการหลบหลีกสเต็ลธ์ stealth เพื่อหลีกเลี่ยงการตรวจจับ

ผลลัพธ์ที่คาดหวัง สามารถตรวจพบพอร์ตที่เปิดใช้งาน และ ระบบตรวจจับการบุกรุก ตรวจจับพฤติกรรมสแกนพอร์ต

ง) การโจมตีด้วยทีซีพีซินฟลัด

ชุดคำสั่ง hping3 -S --flood -p 80 172.30.1.183 --count 1000

-S = ตั้งค่าสถานะ TCP SYN flag (เริ่มต้นการเชื่อมต่อ)

--flood = ส่งแพ็กเก็ตจำนวนมากอย่างรวดเร็ว

-p 80 = ระบุพอร์ตเป้าหมายเป็น 80 (HTTP)

--count 1000 = ส่ง 1,000 ครั้ง

วัตถุประสงค์ ส่ง TCP SYN จำนวนมากเพื่อพยายามเปิดการเชื่อมต่อโดยไม่จบการ Handshake ในรูปแบบกึ่งเปิด (Half-open)

ผลลัพธ์ที่คาดหวัง เกิด SYN queue overflow บนเครื่องเป้าหมาย และ ระบบตรวจจับการบุกรุก แจ้งเตือนทีซีพีซินฟลัด

จ) การโจมตีด้วยบรูตฟอร์ซแอตแทค

จัดเตรียมโดยการ โหลดไฟล์ rockyou.txt ซึ่งเป็นไฟล์รายการรหัสผ่าน (password list) ขนาดใหญ่ที่รวบรวมรหัสผ่านจริงจากการรั่วไหล และทำการตัดขนาดของข้อมูล (Data) ให้เหลือไฟล์ ชื่อผู้ใช้งาน (Username) ให้เหลือ 10 เรคคอร์ด (Record) และ รหัสผ่าน (Password) ให้เหลือ 1,000 เรคคอร์ด เพื่อเมื่อทำการโจมตีจะได้การโจมตี 1,000 ครั้ง ตามที่ได้กำหนดไว้

head -n 10 ~/Downloads/ rockyou.txt > ~/Downloads/users_10.txt

head -n 100 ~/Downloads/rockyou.txt > ~/Downloads/rockyou_100.txt

ชุดคำสั่ง hydra -L ~/Downloads/users_10.txt –

P~/Downloads/rockyou_100.txt -t 10 -V 172.30.1.183 http-post-

form"/DVWA/login.php:username=^USER^&password=^PASS^:

F=Login failed"

-L users_10.txt หมายถึง ไฟล์รายชื่อผู้ใช้

-P ~/Downloads/rockyou-100.txt หมายถึง ไฟล์รหัสผ่าน

-t 10 หมายถึง เปิด 10 thread พร้อมกัน (เพิ่มความรวดเร็ว)

http-post-form หมายถึง ระบุฟอร์มสำหรับโจมตีแบบ POST

วัตถุประสงค์ เพื่อทำการทดสอบการเดารหัสผ่านจากไฟล์ username และ password เพื่อดูว่า ระบบตรวจจับภัยการบุกรุก สามารถตรวจจับความพยายามโจมตีแบบ Brute Force ได้หรือไม่

ผลลัพธ์ที่คาดหวัง Hydra แสดงผลการลองรหัสผ่าน และแสดงบัญชีที่ login สำเร็จ (ถ้ามี) และระบบตรวจจับการบุกรุก สามารถตรวจจับและแจ้งเตือนว่าเกิดบรูตฟอร์ซแอตแทค จาก IP ต้นทาง

ฉ) การโจมตีด้วยเอสคิวแอลอินเจกชัน

Command : for i in {1..10}; do echo "Request #$i"sqlmap -u "http://172.30.1.183/dvwa/vulnerabilities/sqli/?id=1%27%20or%201%3D1--&Submit=Submit" \ --cookie="PHPSESSID=xxxxxxxxxxxxxxx" --batch \ --level=1 --risk=1 \ --technique=B \ --flush-session \ > /dev/null

Done

URL คือหน้าเอสคิวแอลอินเจกชันของ DVWA (Reflected SQLi)

' or 1=1 -- ทำให้ SQL query กลายเป็นจริงเสมอ

cookie="PHPSESSID=”” กำหนดค่า Cookie Session ของผู้ใช้ที่ login เข้า DVWA

วัตถุประสงค์ เพื่อทำการทดสอบช่องโหว่เอสคิวแอลอินเจกชัน โดยใช้การโจมตีแบบอัตโนมัติ

ผลลัพธ์ที่คาดหวัง สามารถดึงข้อมูลออกจากฐานข้อมูลและระบบตรวจจับภัยการบุกรุกสามารถ แจ้งเตือนว่ามีการโจมตีด้วยการโจมตีด้วยเอสคิวแอลอินเจกชัน

ช) ครอสไซต์สคริปต์ติ้ง

Command: for i in {1..100}; do echo "Test XSS #$i"

curl -X POST "http://172.30.1.183/dvwa/vulnerabilities/xss_r/" \

-d "name=<script>alert($i)</script>" \

-H "Content-Type: application/x-www-form-urlencoded" sleep 0.5

Done

-u = ระบุ URL ที่ต้องการทดสอบ

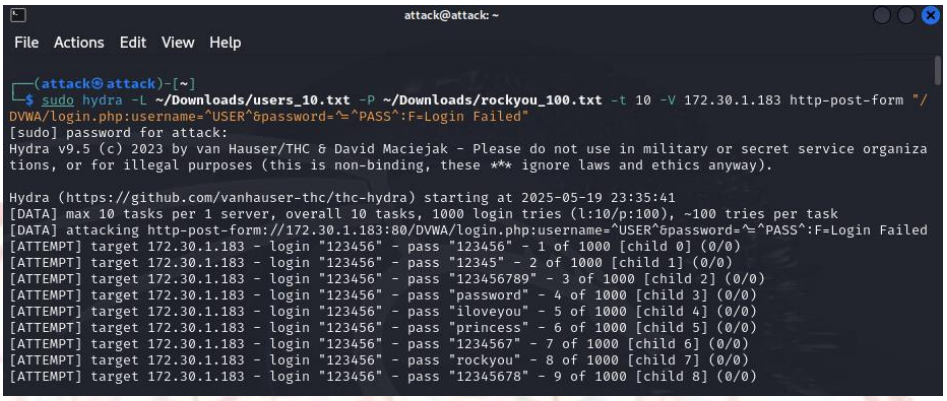
--crawl = สแกนลิงก์อื่นๆ ภายในเว็บด้วย

--skip = ข้ามการตรวจสอบบางขั้นตอน (เพิ่มความเร็ว)

Sleep 0.5 = ทำการหน่วงเวลา 0.5 วินาที เพื่อกันระบบล่ม หรือ บล็อค

วัตถุประสงค์ เพื่อทดสอบการฉีดสคริปต์ในเว็บเพจเพื่อดูว่าระบบ IDS ตรวจจับครอสไซต์สคริปต์ติ้ง ได้หรือไม่

ผลลัพธ์ที่คาดหวัง พบช่องโหว่ครอสไซต์สคริปต์ติ้ง และระบบตรวจจับการบุกรุก ทำการแจ้งเตือนว่ามีการโจมตีด้วยครอสไซต์สคริปต์ติ้ง



ภาพที่ 3.18 ตัวอย่างการโจมตีด้วย Brute Force Attack

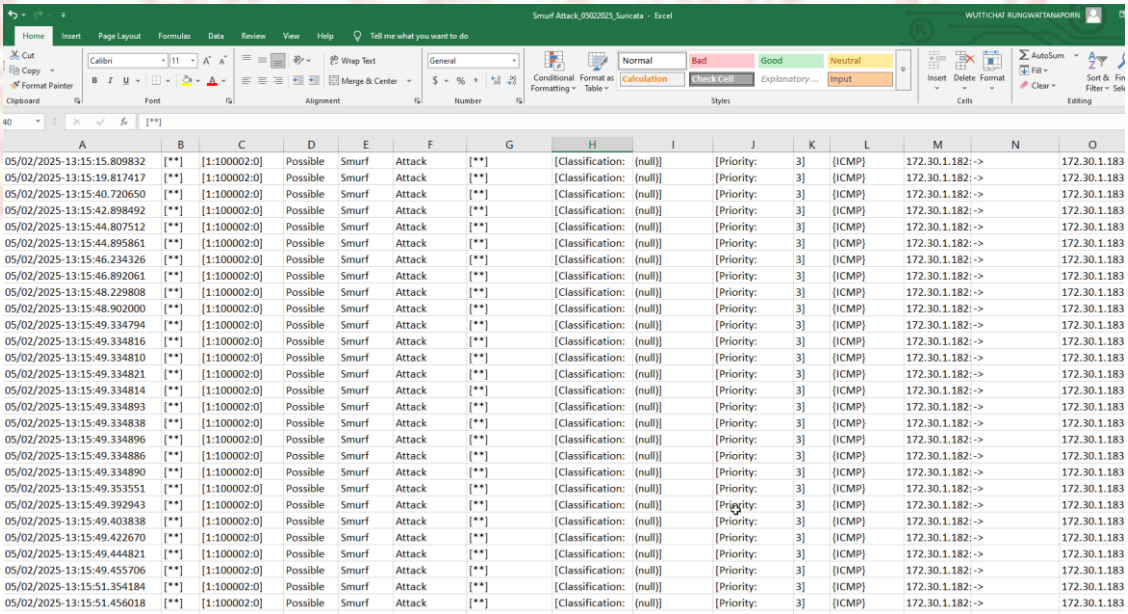
3.2.5 การเก็บรวบรวมข้อมูลเพื่อวิเคราะห์ประสิทธิภาพของระบบ

ในการวิจัยนี้ มีการเก็บรวบรวมข้อมูลที่ได้จากการทดสอบการบุกรุกระบบเครือข่าย เพื่อประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก ที่ทำการกำหนดค่า กฎและการแจ้งเตือน โดยข้อมูลที่เก็บรวบรวมจะครอบคลุมทั้ง ล็อกของการโจมตี และข้อมูลเชิงเทคนิคจากระบบที่ถูกโจมตี ดังนี้

3.2.5.1 ข้อมูลจากตรวจจับการบุกรุก โดยการทำหน้าที่ตรวจจับพฤติกรรมผิดปกติที่เกิดขึ้นในระบบเครือข่าย โดยจะบันทึกข้อมูลลงในไฟล์ ล็อกหลายประเภท

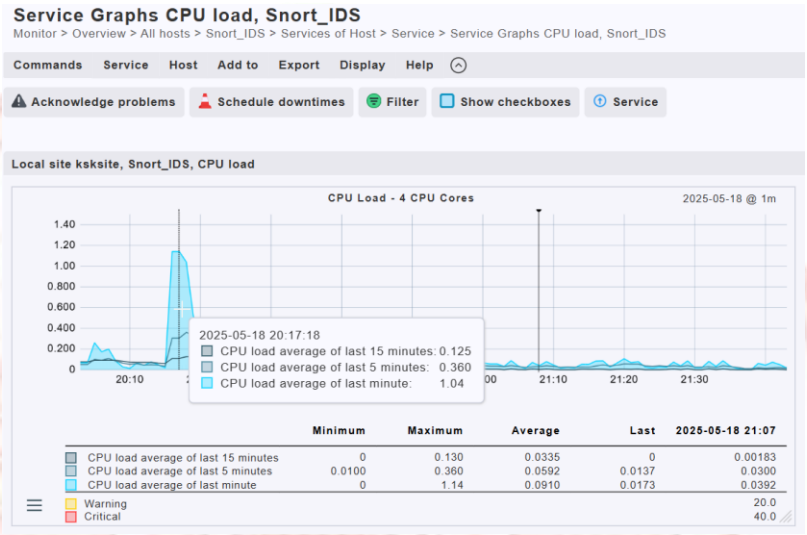
ภาพที่ 3.19 ตัวอย่าง Log จากระบบตรวจจับการบุกรุก

ในการดำเนินการวิจัยด้านการตรวจจับการบุกรุก โดยระบบตรวจจับการบุกรุกจะสร้างข้อมูลล็อก จำนวนมากเมื่อมีเหตุการณ์ที่ระบบตรวจพบว่าอาจเป็นการโจมตี อย่างไรก็ดีล็อกที่ได้จากระบบตรวจจับการบุกรุก มักอยู่ในรูปแบบข้อความที่ไม่เป็นโครงสร้าง (Unstructured Text) ซึ่งทำให้ไม่เหมาะสมต่อการประมวลผลทางสถิติหรือการวิเคราะห์ในเชิงปริมาณโดยตรง การนำล็อกเหล่านี้ไปใช้ในการคำนวณ ทางผู้ดำเนินการวิจัยจึงแปลงเป็นไฟล์ .CSV เพื่อง่ายต่อการวิเคราะห์ ผลของการวิจัย

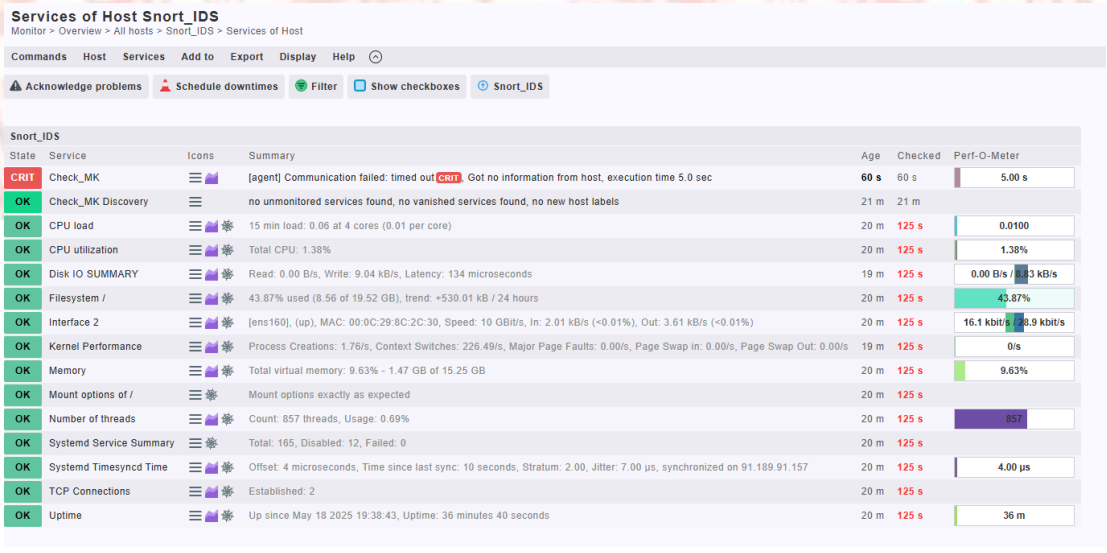


ภาพที่ 3.20 แปลงไฟล์ Log เป็น Format .CSV เพื่อง่ายต่อการวิเคราะห์ ผลการวิจัย

3.2.5.2 ข้อมูลจากระบบตรวจสอบสถานะ (CheckMK Monitoring) เพื่อตรวจสอบผลกระทบของการโจมตีที่เกิดขึ้นกับระบบเครือข่ายและเซิร์ฟเวอร์ มีการติดตั้ง เอเจนต์ตรวจสอบระบบ (CheckMK Agent) ในเครื่องเซิร์ฟเวอร์เป้าหมาย เพื่อใช้ตรวจสอบข้อมูลสถานะต่าง



ภาพที่ 3.21 ข้อมูลจากระบบตรวจสอบสถานะ (CheckMK Monitoring)



ภาพที่ 3.22 รายละเอียดต่างๆที่แสดงในระบบ (CheckMK Monitoring)

ข้อมูลจากระบบตรวจสอบสถานะ ช่วยให้เห็นภาพรวมของสภาพแวดล้อมในระบบระหว่างและหลังการโจมตี ช่วยยืนยันผลกระทบของการโจมตี และสนับสนุนการวิเคราะห์ประสิทธิภาพของระบบการตรวจจับการบุกรุก

3.2.5.3 ข้อมูลจากผลลัพธ์การโจมตี

นอกจากนี้ ยังเก็บบันทึกผลการรันคำสั่งโจมตีแต่ละประเภท เช่น การยิงปิงฟลัด การสแกนพอร์ต และ การโจมตีเอสคิวแอลอินเจกชัน เป็นต้น เพื่อเปรียบเทียบกับข้อมูลจาก ระบบตรวจจับการบุกรุก และ CheckMK ว่ามีการตรวจจับและตอบสนองอย่างถูกต้องหรือไม่

ข้อมูลทั้งหมดที่ได้จะถูกนำมาวิเคราะห์ในบทที่ 4 เพื่อคำนวณค่าต่าง ๆ เช่น อัตราการตรวจจับ (Detection Rate), อัตราความผิดพลาด (False Negative Rate), ความแม่นยำ (Accuracy) และคะแนน F1 (F1 Score) เพื่อประเมินประสิทธิภาพของระบบตรวจจับการบุกรุก

3.3 สรุปขั้นตอนการดำเนินการวิจัย

ในการดำเนินการวิจัยครั้งนี้ มีวัตถุประสงค์เพื่อเปรียบเทียบประสิทธิภาพของระบบตรวจจับการบุกรุก ที่เหมาะสมสำหรับการใช้งานในองค์กรขนาดกลาง โดยขั้นตอนเริ่มจากการจัดเตรียมเครื่องเซิร์ฟเวอร์ภายในสภาพแวดล้อมเสมือนจริง (Virtual Environment) บนระบบ VMware ซึ่งติดตั้งเครื่องมือตรวจจับการบุกรุกทั้ง 3 โปรแกรม ได้แก่ สนอร์ต เวอร์ชัน 2.9.20 GRE (Build 82), ซูริกาต้า เวอร์ชัน 7.0.5 และ ซีค เวอร์ชัน 6.0.3 บนระบบปฏิบัติการเดียวกัน เพื่อให้การเปรียบเทียบมีความเป็นธรรมและอยู่ในเงื่อนไขเดียวกัน นอกจากนี้ยังได้ติดตั้งระบบตรวจสอบสถานะและประสิทธิภาพของระบบด้วย Checkmk เพื่อให้สามารถติดตามและวิเคราะห์ผลการทำงานของตรวจจับการบุกรุกแต่ละระบบได้อย่างต่อเนื่อง จากนั้นจึงดำเนินการออกแบบและตั้งค่าเครือข่ายจำลองที่มีลักษณะใกล้เคียงกับเครือข่ายขององค์กรขนาดกลาง โดยมีการกำหนด IP address, routing และจุดเชื่อมต่อที่เหมาะสมกับการติดตั้งตรวจจับการบุกรุก พร้อมทั้งกำหนดกฎเกณฑ์การตรวจจับ (Rule set) สำหรับแต่ละโปรแกรมตรวจจับการบุกรุก ให้สามารถระบุพฤติกรรมที่เป็นภัยคุกคามได้ตรงตามเป้าหมาย

เมื่อระบบมีความพร้อม จึงเริ่มขั้นตอนการทดสอบโดยจำลองรูปแบบการโจมตีทางเครือข่าย จำนวน 7 ประเภท ซึ่งผลการทดสอบจะแสดงในบทที่ 4 เป็นประเภทการโจมตีที่พบบ่อยและมีความสำคัญในการรักษาความมั่นคงปลอดภัยของระบบ ประกอบด้วย

ก) ทีซีพีซินฟลัดซึ่งเป็นการโจมตีเพื่อทำให้เซิร์ฟเวอร์รับภาระการเชื่อมต่อเกินความสามารถ

ข) ทีซีพีพอร์ตสแกนซึ่งใช้ตรวจสอบพอร์ตที่เปิดใช้งานเพื่อค้นหาช่องโหว่

ค) สมิร์ฟแอตแทคซึ่งใช้การปลอมที่อยู่ต้นทางและกระจาย ไอซีเอ็มแพ็เกจเพื่อทำให้ระบบล่ม

ง) ไอซีเอ็มพีพิงฟลัดที่ส่งคำสั่ง ping จำนวนมากเพื่อให้ระบบเป้าหมายไม่สามารถให้บริการได้

จ) บรูตฟอร์ซแอตแทค ที่พยายามเข้าสู่ระบบด้วยการเดารหัสผ่านซ้ำๆ

ฉ) เอสคิวแอลอินเจกชัน ที่โจมตีช่องโหว่ของฐานข้อมูลผ่านคำสั่งเอสคิวแอล

ช) ครอสไซต์สคริปต์ติ้ง ที่แทรกสคริปต์อันตรายลงในเว็บไซต์เพื่อหลอกผู้ใช้งาน

การโจมตีทั้งหมดนี้ถูกจำลองขึ้นภายในสภาพแวดล้อมที่ควบคุมได้ เพื่อความปลอดภัยและความแม่นยำในการวัดผล โดยหลังจากเสร็จสิ้นการทดสอบในแต่ละรอบ จะมีการเก็บรวบรวมข้อมูลล็อกและสถิติต่าง ๆ จากระบบการตรวจจับการบุกรุก แต่ละระบบ เพื่อนำไปวิเคราะห์เปรียบเทียบประสิทธิภาพการทำงาน

บทที่ 4
ผลการวิจัย

4.1 ภาพรวมของการทดลอง

การทดลองในครั้งนี้มีวัตถุประสงค์เพื่อเปรียบเทียบประสิทธิภาพของระบบตรวจจับการบุกรุกที่เหมาะสมกับการนำมาใช้งานในองค์กรขนาดกลาง ได้แก่ Snort, Suricata และ Zeek โดยจำลองสภาพแวดล้อมขององค์กรขนาดกลางซึ่งมีอุปกรณ์และทราฟฟิกระดับหนึ่งที่สอดคล้องกับการใช้งานจริง

ประเภทของการทดสอบประกอบด้วยการโจมตีทางเครือข่ายทั้งหมด 7 ประเภทหลัก ซึ่งครอบคลุมการโจมตีทั้งในระดับ Network และ Application ได้แก่:

ก) ไอซีเอ็มพีพิงฟลัด เป็นการส่งคำขอ ICMP ปริมาณมากเพื่อหวังให้เป้าหมายล่ม

ข) สมิร์ฟแอตแทค เป็นการปลอมแปลง IP ต้นทางและส่ง ICMP ไปยัง Broadcast Address

ค) ทีซีพีพอร์ตสแกน เป็นการสแกนพอร์ต TCP เพื่อตรวจสอบบริการที่เปิดใช้งาน

ง) ทีซีพีซินฟลัด เป็นการส่ง SYN Packet จำนวนมากเพื่อครอบครองทรัพยากร

จ) บรูตฟอร์ซแอตแทค เป็นการเดารหัสผ่านด้วยการลองค่าหลายชุดบน Web Login

ฉ) เอสคิวแอลอินเจกชัน เป็นการแทรกคำสั่ง SQL ผ่านช่องกรอกข้อมูลของเว็บ

ช) ครอสไซต์สคริปต์ติ้ง การฝังสคริปต์อันตรายลงในหน้าเว็บ

ระบบตรวจจับการบุกรุก ทั้งสามรุ่นถูกตั้งค่าให้ตรวจจับการโจมตี ในเครือข่ายจำลองจริง และวัดผลจากจำนวนการตรวจจับที่ถูกต้อง (True Positive) และเหตุการณ์ที่ระบบพลาด (False Negative) โดยใช้ข้อมูลทั้งหมดประมาณ 7,000 เหตุการณ์โจมตี แบ่งออกเป็น 1,000 เหตุการณ์ต่อการโจมตี แต่ละประเภท

4.2 ผลการตรวจจับของระบบตรวจจับการบุกรุก

4.2.1 ระบบตรวจจับการบุกรุกสนอร์ต

ตรวจจับเหตุการณ์ที่ถูกต้องได้ทั้งหมด (True Positive) คิดเป็น 6,631 ครั้ง

พลาดการตรวจจับ (False Negative) คิดเป็น 369 ครั้ง

อัตราการตรวจจับ (Detection Rate) คิดเป็น ร้อยละ 94.73

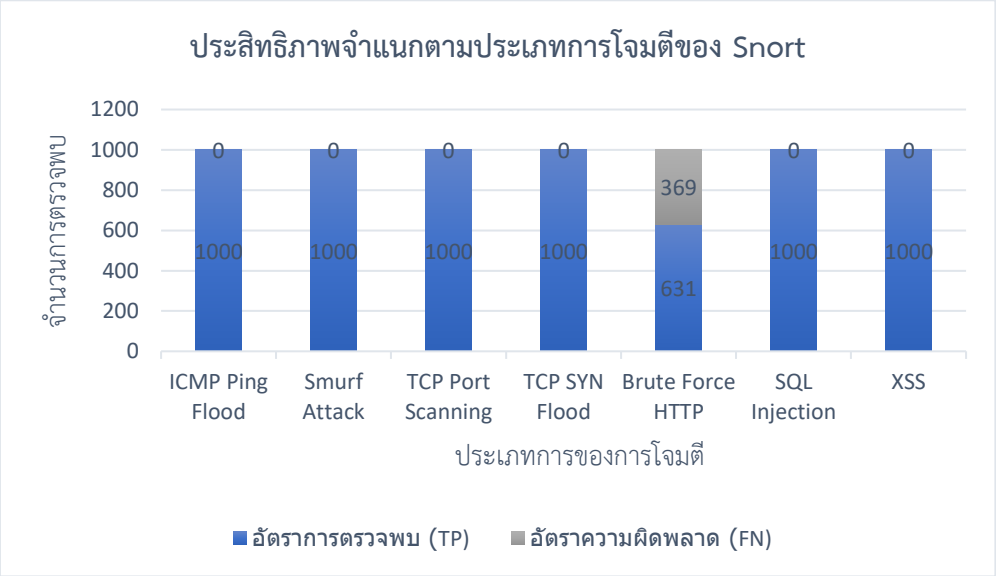
$$\text{Detection Rate} = \frac{TP}{TP + FN} = \frac{6631}{6631 + 369} = 94.73\%$$

F1 Score คิดเป็น ร้อยละ 97.24

$$\text{F1 Score} = 2 \times \frac{\text{Precision x Detection Rate}}{\text{Precision + Detection Rate}} = \frac{2 \times 0.9473}{1 + 0.9473} = 97.24\%$$

ตารางที่ 4-1 ประสิทธิภาพจำแนกตามประเภทการโจมตีของ สนอร์ต (Snort)

ประเภทการโจมตี	อัตราการตรวจพบ (TP)	อัตราความผิดพลาด (FN)
ICMP Ping Flood	1000	0
Smurf Attack	1000	0
TCP Port Scanning	1000	0
TCP SYN Flood	1000	0
Brute Force HTTP	631	369
SQL Injection	1000	0
XSS	1000	0



ภาพที่ 4-1 ประสิทธิภาพจำแนกตามประเภทการโจมตีของ สนอร์ต (Snort)

จุดเด่น ของระบบตรวจจับการบุกรุกสนอร์ต คือ การตรวจจับพฤติกรรมผิดปกติหรือโจมตีระดับ Application Layer เช่น บรูตฟอร์ซแอตแทค ได้แม่นยำ

จุดอ่อน ของระบบตรวจจับการบุกรุกสนอร์ต คือ การตรวจจับการโจมตีประเภท DoS หรือ Flooding ได้ไม่ครบถ้วน เนื่องจากไม่ได้เน้นที่ Signature Matching

4.2.2 ระบบตรวจจับการบุกรุก ซูริกาต้า (Suricata)

ตรวจจับเหตุการณ์ที่ถูกต้องได้ทั้งหมด (True Positive) คิดเป็น 6,728 ครั้ง

พลาดการตรวจจับ (False Negative) คิดเป็น 272 ครั้ง

อัตราการตรวจจับ (Detection Rate) คิดเป็น ร้อยละ 96.11

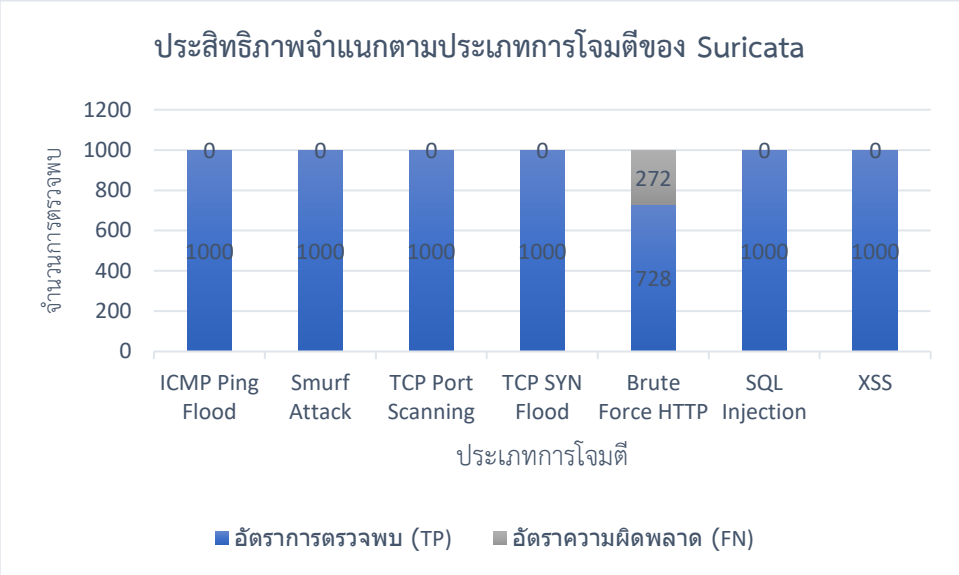
$$\text{Detection Rate} = \frac{TP}{TP + FN} = \frac{6728}{6728 + 272} = 96.11\%$$

F1 Score คิดเป็น ร้อยละ 97.96

$$\text{F1 Score} = 2 \times \frac{\text{Precision x Detection Rate}}{\text{Precision + Detection Rate}} = \frac{2 \times 0.9611}{1 + 0.9611} = 97.96\%$$

ตารางที่ 4.2 ประสิทธิภาพจำแนกตามประเภทการโจมตีของ ซูริกาต้า (Suricata)

ประเภทการโจมตี	อัตราการตรวจพบ (TP)	อัตราความผิดพลาด (FN)
ICMP Ping Flood	1000	0
Smurf Attack	1000	0
TCP Port Scanning	1000	0
TCP SYN Flood	1000	0
Brute Force HTTP	728	272
SQL Injection	1000	0
XSS	1000	0



ภาพที่ 4-2 ประสิทธิภาพจำแนกตามประเภทการโจมตีของ ซูริกาต้า (Suricata)

จุดเด่น ของระบบตรวจจับการบุกรุกซูริกาต้า คือ สามารถตรวจจับ DoS, Scanning, และ Web Application Attack ได้ดี โดยรวมครอบคลุมกว่าระบบอื่น

จุดอ่อน ของระบบตรวจจับการบุกรุกซูริกาต้า คือ ระบบตรวจจับการบุกรุกซูริกาต้า ต้องการทรัพยากรเครื่องมากกว่าระบบอื่นเล็กน้อย เช่น CPU และ RAM

4.2.3 ระบบตรวจจับการบุกรุกซีค

ตรวจจับเหตุการณ์ที่ถูกต้องได้ทั้งหมด (True Positive) คิดเป็น 6,104 ครั้ง

พลาดการตรวจจับ (False Negative) คิดเป็น 896 ครั้ง

อัตราการตรวจจับ (Detection Rate) คิดเป็น ร้อยละ 87.21

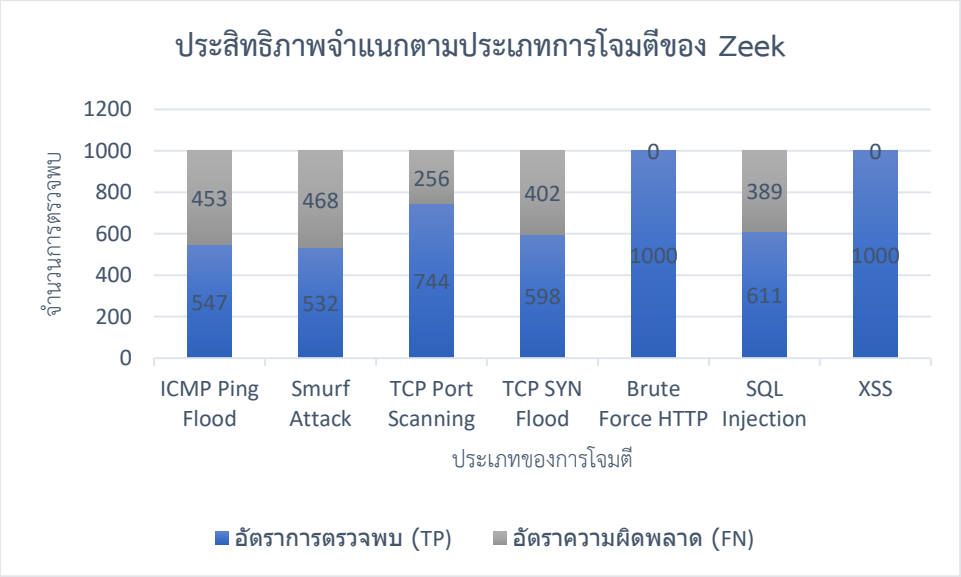
$$\text{Detection Rate} = \frac{TP}{TP + FN} = \frac{6104}{6104 + 896} = 87.21\%$$

F1 Score คิดเป็น ร้อยละ 93.23

$$\text{F1 Score} = 2 \times \frac{\text{Precision x Detection Rate}}{\text{Precision + Detection Rate}} = \frac{2 \times 0.8721}{1 + 0.8721} = 93.23\%$$

ตารางที่ 4.3 ประสิทธิภาพจำแนกตามประเภทการโจมตีของ ซีค (Zeek)

ประเภทการโจมตี	อัตราการตรวจพบ (TP)	อัตราความผิดพลาด (FN)
ICMP Ping Flood	547	453
Smurf Attack	532	468
TCP Port Scanning	744	256
TCP SYN Flood	598	402
Brute Force HTTP	1000	0
SQL Injection	611	389
XSS	1000	0



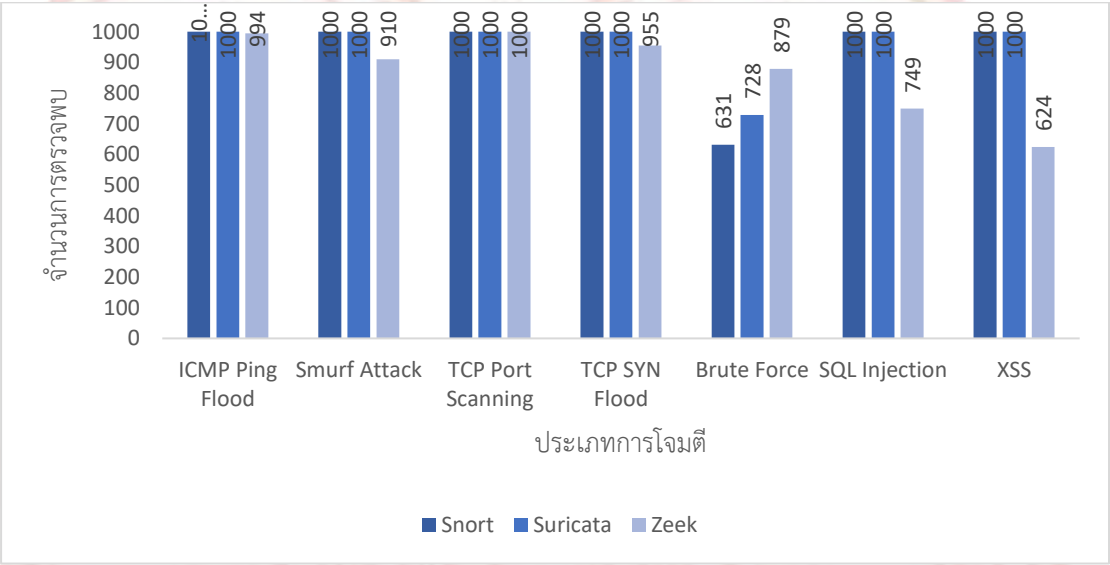
ภาพที่ 4-3 ประสิทธิภาพจำแนกตามประเภทการโจมตีของซีค

จุดเด่น ของระบบตรวจจับการบุกรุกซีค คือ การตรวจจับพฤติกรรมผิดปกติหรือโจมตีระดับ Application Layer เช่น บรูตฟอร์ซแอตแทค ได้แม่นยำ

จุดอ่อน ของระบบตรวจจับการบุกรุก ซีค (Zeek) ตรวจจับ DoS หรือ Flooding ได้ไม่ครบถ้วน เนื่องจากไม่ได้เน้นที่ Signature Matching

ตารางที่ 4.4 เปรียบเทียบความสามารถในการตรวจจับของแต่ละระบบตรวจจับการบุกรุก โดยแยกตามประเภทการโจมตี

	ICMP Ping Flood	Smurf Attack	TCP Port Scanning	TCP SYN Flood	Brute Force	SQL Injection	XSS
Snort	1000	1000	1000	1000	631	1000	1000
Suricata	1000	1000	1000	1000	728	1000	1000
Zeek	994	910	1000	955	879	742	624



ภาพที่ 4-4 เปรียบเทียบความสามารถในการตรวจจับของแต่ละระบบตรวจจับการบุกรุก โดยแยกตามประเภทการโจมตี

จากผลการทดลองจะพบได้ว่า ระบบตรวจจับการบุกรุกสนอร์ต และ ระบบตรวจจับการบุกรุกซูริกาต้า มีความสามารถในการตรวจจับการโจมตีประเภทซิกเนเจอร์เบส เช่น ไอซีเอ็มพีพิงฟลัด สมิร์ฟ แอตแทค ทีซีพีพอร์ตสแกน ทีซีพีซินฟลัด เอสคิวแอลอินเจกชัน และ ครอสไซต์สคริปต์ติ้ง ได้อย่างสมบูรณ์แบบ ร้อยละ 100 ขณะที่ ระบบตรวจจับการบุกรุกซีคแม้จะตรวจจับ ทีซีพีพอร์ตสแกน ได้ครบถ้วน แต่มีประสิทธิภาพต่ำกว่าในหลายประเภท โดยเฉพาะ สมิร์ฟแอตแทค เอสคิวแอลอินเจกชัน และครอสไซต์สคริปต์ติ้ง ซึ่งตรวจจับได้น้อยกว่า ร้อยละ 80

อย่างไรก็ตามระบบตรวจจับการบุกรุกซีคแสดงให้เห็นถึงความโดดเด่นในการตรวจจับการโจมตีแบบพฤติกรรม โดยสามารถตรวจจับบรูตฟอร์ซแอตแทคได้มากถึง 879 ครั้งจาก 1000 ครั้งซึ่งสูงกว่าเมื่อเทียบกับระบบตรวจจับการบุกรุกสนอร์ต 631 ครั้ง และระบบตรวจจับการบุกรุกซูริกาต้า 728 ครั้ง อย่างชัดเจนโดยแสดงให้เห็นว่าระบบตรวจจับการบุกรุกซีคอาจมีความเหมาะสมมากกว่าในการตรวจจับภัยคุกคามที่ไม่อิงกับซิกเนเจอร์เบสโดยตรง ในขณะที่ระบบตรวจจับการบุกรุกสนอร์ตและระบบตรวจจับการบุกรุกซูริกาต้า เหมาะกับสภาพแวดล้อมที่ต้องการการตรวจจับแบบแม่นยำจากฐานข้อมูลซิกเนเจอร์เบส เป็นหลัก

4.3 การวิเคราะห์ด้านอื่นๆ ที่เกี่ยวข้องกับการใช้งานระบบตรวจจับการบุกรุก

4.3.1 Response Time (เวลาตอบสนองของระบบ)

การทดสอบเวลาตอบสนองของระบบ หมายถึงเวลาที่ระบบตรวจจับการบุกรุก ใช้ในการตรวจจับและแจ้งเตือนภัยคุกคามหลังจากเหตุการณ์เกิดขึ้นจริง ยิ่งเวลาตอบสนองน้อย ระบบจะสามารถป้องกันหรือแจ้งเตือนได้ทันท่วงทีมากขึ้น ซึ่งเหมาะกับองค์กรที่ต้องการตรวจจับแบบเรียลไทม์ โดยเปรียบเทียบจากระยะเวลาที่ดำเนินการโจมตี กับ ระยะเวลาที่แสดงผลว่าถูกโจมตี

IDS	Alert	Response Time
Snort	[**] [1:100006:1] SQL Injection Attempt Detected [**] [Priority: 2] 05/03-00:34:02.096789 172.30.1.182:51532 -> 172.30.1.183:80 TCP	00:34:02.096789
	[**] [1:100006:1] SQL Injection Attempt Detected [**] [Priority: 2] 05/03-00:34:02.099057 172.30.1.182:51532 -> 172.30.1.183:80 TCP	00:34:02.099057
	[**] [1:100006:1] SQL Injection Attempt Detected [**] [Priority: 2] 05/03-00:34:02.101942 172.30.1.182:51532 -> 172.30.1.183:80 TCP	00:34:02.101942
	[**] [1:100006:1] SQL Injection Attempt Detected [**] [Priority: 2] 05/03-00:34:02.104524 172.30.1.182:51532 -> 172.30.1.183:80 TCP	00:34:02.104524
	[**] [1:100006:1] SQL Injection Attempt Detected [**] [Priority: 2] 05/03-00:34:02.105893 172.30.1.182:51532 -> 172.30.1.183:80 TCP	00:34:02.105893
	[**] [1:100006:1] SQL Injection Attempt Detected [**] [Priority: 2] 05/03-00:34:02.108412 172.30.1.182:51532 -> 172.30.1.183:80 TCP	00:34:02.108412
	[**] [1:100006:1] SQL Injection Attempt Detected [**] [Priority: 2] 05/03-00:34:02.110624 172.30.1.182:51532 -> 172.30.1.183:80 TCP	00:34:02.110624
	[**] [1:100006:1] SQL Injection Attempt Detected [**] [Priority: 2] 05/03-00:34:02.112551 172.30.1.182:51532 -> 172.30.1.183:80 TCP	00:34:02.112551
	[**] [1:100006:1] SQL Injection Attempt Detected [**] [Priority: 2] 05/03-00:34:02.116771 172.30.1.182:51532 -> 172.30.1.183:80 TCP	00:34:02.116771
	[**] [1:100006:1] SQL Injection Attempt Detected [**] [Priority: 2] 05/03-00:34:02.119586 172.30.1.182:51532 -> 172.30.1.183:80 TCP	00:34:02.119586
Suricata	05/03/2025-00:34:02.091275 [**] [1:100006:1] SQL Injection Attempt Detected [**] [Classification: Web Application Attack] [Priority: 2] {TCP} 172.30.1.182:51532 -> 172.30.1.183:80	00:34:02.091275
	05/03/2025-00:34:02.093612 [**] [1:100006:1] SQL Injection Attempt Detected [**] [Classification: Web Application Attack] [Priority: 2] {TCP} 172.30.1.182:51532 -> 172.30.1.183:80	00:34:02.093612
	05/03/2025-00:34:02.096198 [**] [1:100006:1] SQL Injection Attempt Detected [**] [Classification: Web Application Attack] [Priority: 2] {TCP} 172.30.1.182:51532 -> 172.30.1.183:80	00:34:02.096198
	05/03/2025-00:34:02.098764 [**] [1:100006:1] SQL Injection Attempt Detected [**] [Classification: Web Application Attack] [Priority: 2] {TCP} 172.30.1.182:51532 -> 172.30.1.183:80	00:34:02.098764
	05/03/2025-00:34:02.099923 [**] [1:100006:1] SQL Injection Attempt Detected [**] [Classification: Web Application Attack] [Priority: 2] {TCP} 172.30.1.182:51532 -> 172.30.1.183:80	00:34:02.099923
	05/03/2025-00:34:02.101387 [**] [1:100006:1] SQL Injection Attempt Detected [**] [Classification: Web Application Attack] [Priority: 2] {TCP} 172.30.1.182:51532 -> 172.30.1.183:80	00:34:02.101387
	05/03/2025-00:34:02.103048 [**] [1:100006:1] SQL Injection Attempt Detected [**] [Classification: Web Application Attack] [Priority: 2] {TCP} 172.30.1.182:51532 -> 172.30.1.183:80	00:34:02.103048
	05/03/2025-00:34:02.104556 [**] [1:100006:1] SQL Injection Attempt Detected [**] [Classification: Web Application Attack] [Priority: 2] {TCP} 172.30.1.182:51532 -> 172.30.1.183:80	00:34:02.104556
	05/03/2025-00:34:02.107442 [**] [1:100006:1] SQL Injection Attempt Detected [**] [Classification: Web Application Attack] [Priority: 2] {TCP} 172.30.1.182:51532 -> 172.30.1.183:80	00:34:02.107442
	05/03/2025-00:34:02.110183 [**] [1:100006:1] SQL Injection Attempt Detected [**] [Classification: Web Application Attack] [Priority: 2] {TCP} 172.30.1.182:51532 -> 172.30.1.183:80	00:34:02.110183
Zeek	05/03-00:34:02.121384 SQL Injection attempt detected from: 172.30.1.182 URI: /dvwa/vulnerabilities/sqli/?id=1' or 1=1 -- &Submit=Submit	00:34:02.121384
	05/03-00:34:02.125872 SQL Injection attempt detected from: 172.30.1.182 URI: /dvwa/vulnerabilities/sqli/?id=2' or 1=1 -- &Submit=Submit	00:34:02.125872
	05/03-00:34:02.130104 SQL Injection attempt detected from: 172.30.1.182 URI: /dvwa/vulnerabilities/sqli/?id=3' or 1=1 -- &Submit=Submit	00:34:02.130104
	05/03-00:34:02.134512 SQL Injection attempt detected from: 172.30.1.182 URI: /dvwa/vulnerabilities/sqli/?id=4' or 1=1 -- &Submit=Submit	00:34:02.134512
	05/03-00:34:02.140003 SQL Injection attempt detected from: 172.30.1.182 URI: /dvwa/vulnerabilities/sqli/?id=5' or 1=1 -- &Submit=Submit	00:34:02.140003
	05/03-00:34:02.146017 SQL Injection attempt detected from: 172.30.1.182 URI: /dvwa/vulnerabilities/sqli/?id=6' or 1=1 -- &Submit=Submit	00:34:02.146017
	05/03-00:34:02.150488 SQL Injection attempt detected from: 172.30.1.182 URI: /dvwa/vulnerabilities/sqli/?id=7' or 1=1 -- &Submit=Submit	00:34:02.150488
	05/03-00:34:02.154987 SQL Injection attempt detected from: 172.30.1.182 URI: /dvwa/vulnerabilities/sqli/?id=8' or 1=1 -- &Submit=Submit	00:34:02.154987
	05/03-00:34:02.160010 SQL Injection attempt detected from: 172.30.1.182 URI: /dvwa/vulnerabilities/sqli/?id=9' or 1=1 -- &Submit=Submit	00:34:02.160010
	05/03-00:34:02.165321 SQL Injection attempt detected from: 172.30.1.182 URI: /dvwa/vulnerabilities/sqli/?id=10' or 1=1 -- &Submit=Submit	00:34:02.165321

ภาพที่ 4-5 เปรียบเทียบ Response Time แบ่งแยกตามแต่ละ ระบบตรวจจับการบุกรุก

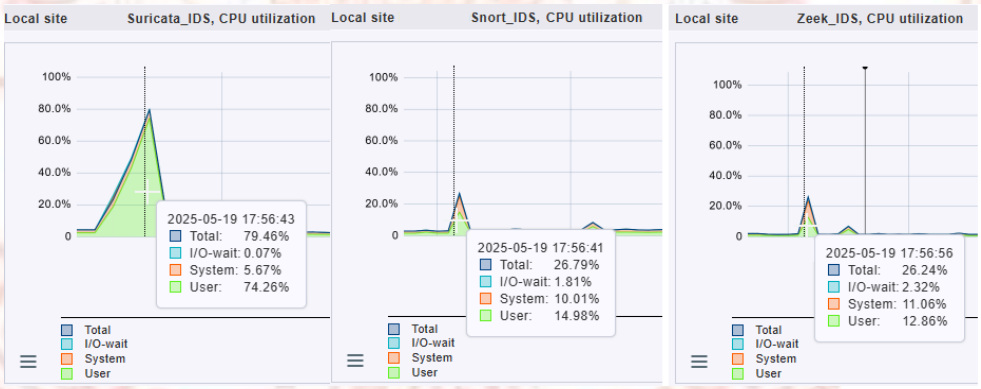
ตารางที่ 4-5 ความสามารถในการตอบสนอง แบ่งแยกตาม ระบบตรวจจับการบุกรุก

ระบบ IDS	Response Time โดยเฉลี่ย (ms)	หมายเหตุ
Snort	15–20 ms	ตรวจจับเร็วในระดับ Network Layer
Suricata	10–15 ms	รองรับ Multi-threading ทำให้เร็วกว่า Snort
Zeek	20–30 ms	อ้างอิง event-based scripting จึงช้ากว่าเล็กน้อย

สรุปผล จากหัวข้อความสามารถในการตอบสนอง (Response Time) พบว่า ระบบตรวจจับการบุกรุก ซูริกาต้า (Suricata) มีเวลาตอบสนองที่เร็วที่สุดเมื่อเทียบกับระบบตรวจจับการบุกรุกยี่ห้ออื่น จึงเหมาะกับการใช้งานในสถานการณ์ที่ต้องการแจ้งเตือนแบบเรียลไทม์

4.3.2 ประสิทธิภาพระบบ (System Performance)

การประเมินนี้วัดผลกระทบของระบบตรวจจับการบุกรุก ต่อทรัพยากรระบบ เช่น หน่วยประมวลผลกลาง ซีพียู (CPU) และ หน่วยความจำ แรม (RAM) เมื่อรันในสภาพแวดล้อมจริง



ภาพที่ 4-6 เปรียบเทียบ การใช้หน่วยประมวลกลางแยกตามระบบตรวจจับการบุกรุก

ตารางที่ 4.6 ตารางประสิทธิภาพระบบแบ่งแยกตาม ระบบตรวจจับการบุกรุก

ระบบตรวจจับการบุกรุก	การใช้งาน CPU	การใช้งาน RAM
Snort	น้อยถึงปานกลาง	น้อยถึงปานกลาง
Suricata	สูง	สูง
Zeek	น้อยถึงปานกลาง	น้อยถึงปานกลาง

สรุปผล จากหัวข้อประสิทธิภาพระบบ พบว่า ระบบตรวจจับการบุกรุก สนอร์ต (Snort) เหมาะกับระบบที่มีทรัพยากรจำกัด โดย ระบบตรวจจับการบุกรุก ซูริกาต้า (Suricata) ต้องการทรัพยากรแต่รองรับ Traffic สูง และ ระบบตรวจจับการบุกรุก ซีค (Zeek) เหมาะกับงานวิเคราะห์เชิงลึกที่ต้องใช้ RAM มาก

4.3.3 ความสามารถในการปรับแต่งและปรับเปลี่ยน (Flexibility & Customization)

ระบบการตรวจจับการบุกรุก ที่ดีควรสามารถปรับแต่งกฎหรือพฤติกรรมการตรวจจับให้สอดคล้องกับสภาพแวดล้อมขององค์กรได้

ตารางที่ 4.7 เปรียบเทียบประสิทธิภาพในการปรับแต่งและปรับเปลี่ยน แบ่งแยกตาม ระบบตรวจจับการบุกรุก

ระบบตรวจจับการบุกรุก	ความสามารถในการปรับแต่ง	ความยากง่าย
Snort	ปรับแต่ง rules ได้ง่าย	ง่าย
Suricata	รองรับ rules และ scripting	ปานกลาง
Zeek	ปรับแต่งผ่าน scripting ได้หลากหลาย	ยากที่สุด (ต้องเขียน script ด้วยภาษาเฉพาะ)

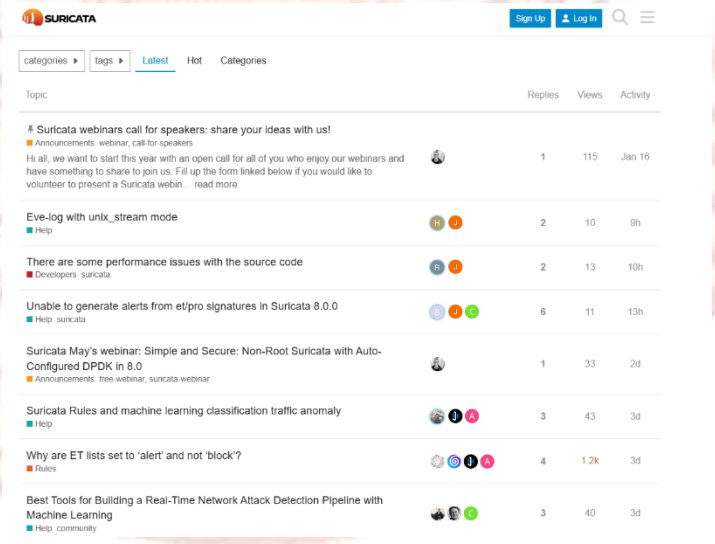
สรุปผล จากหัวข้อประสิทธิภาพในการปรับแต่งและปรับเปลี่ยน พบว่าระบบตรวจจับการบุกรุก สนอร์ต (Snort) เหมาะกับผู้ใช้ทั่วไป ส่วนระบบตรวจจับการบุกรุก ซูริกาต้า (Suricata) มีความ

ยืดหยุ่น รองรับทั้งการเขียน กฎ และ Script และ ระบบตรวจจับการบุกรุก ซีค (Zeek) เหมาะกับผู้มีทักษะ Scripting ที่ต้องการปรับปรุงการตั้งค่าในระดับสูง

4.3.4 การบำรุงรักษา (Maintainability)

การพิจารณานี้เน้นความสะดวกในการอัปเดตฐานข้อมูล, การตั้งค่า, และการดูแลระบบในระยะยาว

ภาพที่ 4-7 งานประชุม ชุมนุมผู้ใช้งานระบบตรวจรับการบุกรุก Snort ประจำเดือน พฤษภาคม ๒๕๖๘



ภาพที่ 4-7 ชุมนุมผู้ใช้งานระบบตรวจรับการบุกรุก Suricata

ตารางที่ 4.8 เปรียบเทียบการบำรุงรักษา แบ่งแยกตาม ระบบตรวจจับการบุกรุก

ระบบตรวจจับการบุกรุก	การอัปเดตฐานข้อมูล	ความซับซ้อนในการดูแล	เอกสาร & ชุมชนผู้ใช้
Snort	ง่าย (ผ่าน pulledpork หรือ snort.org)	น้อย	มีประชุม ชุมชนผู้ใช้งาน, มีเอกสารอัปเดต
Suricata	ง่าย (ผ่าน ruleset จาก Emerging Threats)	ปานกลาง	มีชุมชนผู้ใช้งาน, มีเอกสารอัปเดต
Zeek	ต้องเขียน script และปรับ log เอง	ซับซ้อน	ชุมชนเฉพาะทาง, มีคู่มือแต่ต้องศึกษาเพิ่มเติม

สรุปผล จากหัวข้อการบำรุงรักษา พบว่าระบบตรวจจับการบุกรุก สนอร์ต (Snort) ดูแลง่ายที่สุด เพราะมีเอกสารและ ชุมชนผู้ใช้งานจำนวนมากและมีการจัดประชุม ชุมนุมผู้ใช้เป็นประจำทุกเดือน ส่วนระบบตรวจจับการบุกรุก ซูริกาต้า (Suricata) มีชุมชนผู้ใช้งานปานกลาง แต่มีชุมนุมผู้ใช้งานที่มีการอัพเดท แลกเปลี่ยนความคิดเห็นเป็นประจำ เมื่อเทียบกับระบบตรวจจับการบุกรุก สนอร์ต (Snort) และ ระบบตรวจจับการบุกรุก ซีค (Zeek) ต้องการทักษะสูง เอกสารมีความซับซ้อน แต่ให้ความยืดหยุ่นสูงกว่า

บทที่ 5
สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

บทนี้จะสรุปผลการวิจัยจากการทดลองเปรียบเทียบประสิทธิภาพของระบบตรวจจับการบุกรุก ได้แก่ ระบบตรวจจับการบุกรุกสนอร์ต ระบบตรวจจับการบุกรุกซูริกาต้า และ ระบบตรวจจับการบุกรุกซีคภายใต้เงื่อนไขการจำลองการโจมตีทั้ง 7 ประเภท ในบริบทขององค์กรขนาดกลาง ซึ่งมีข้อจำกัดด้านทรัพยากร จากผลการทดลองในบทที่ 4 จะนำมาวิเคราะห์เพื่อสรุปภาพรวม อภิปรายผลในเชิงลึก เปรียบเทียบข้อดีข้อเสียของแต่ละระบบ และเสนอแนะแนวทางในการเลือกใช้ ระบบตรวจจับการบุกรุก ให้เหมาะสมกับลักษณะงานและบริบทขององค์กร ทั้งนี้ยังรวมถึงข้อเสนอแนะสำหรับการพัฒนางานวิจัยในอนาคต จึงสามารถสรุปอภิปรายผลการวิจัย แบ่งได้เป็น 3 ส่วน ดังนี้

5.1 สรุปผลการวิจัย

5.2 อภิปรายผลการวิจัย

5.3 ข้อเสนอแนะ

5.4 ข้อเสนอแนะสำหรับการวิจัยในอนาคต

5.1 สรุปผลการวิจัย

จากการวิจัยเพื่อเปรียบเทียบประสิทธิภาพของระบบตรวจจับการบุกรุก ทั้ง 3 รุ่น โดยใช้ชุดข้อมูลการโจมตีที่ครอบคลุม 7 ประเภท ได้แก่ ไอซีเอ็มพีพิงฟลัด สมิร์ฟแอตแทค ทีซีพีพอร์ตสแกน ทีซีพีซินฟลัด บรูตฟอร์ซแอตแทค เอสคิวแอลอินเจกชัน และ ครอสไซต์สคริปต์ติ้ง ในบริบทขององค์กรขนาดกลาง ซึ่งมีข้อจำกัดด้านทรัพยากร พบว่าแต่ละระบบมีข้อดีข้อเสียที่แตกต่างกันไปตามลักษณะการใช้งานและโครงสร้างภายในของแต่ละองค์กร

จากการวิจัยเพื่อเปรียบเทียบประสิทธิภาพของระบบตรวจจับการบุกรุกทั้ง 3 ระบบ ได้แก่ ระบบตรวจจับการบุกรุกสนอร์ต ระบบตรวจจับการบุกรุกซูริกาต้า และ ระบบตรวจจับการบุกรุกซีค โดยใช้ชุดข้อมูลการโจมตี 7 ประเภทในบริบทขององค์กรขนาดกลางที่มีข้อจำกัดด้านทรัพยากร พบว่า ระบบตรวจจับการบุกรุกซูริกาต้า มีความแม่นยำสูงสุดในการตรวจจับ F1 Score ร้อยละ 97.96 รองลงมาคือ ระบบตรวจจับการบุกรุกสนอร์ต ร้อยละ 97.24 และ ระบบตรวจจับการบุกรุกซีค ร้อยละ 93.22 ซึ่งแม้ระบบตรวจจับการบุกรุกซีค จะมีค่า F1 ต่ำกว่าแต่มีจุดเด่นด้านการวิเคราะห์

เชิงลึกและเหตุการณ์ย้อนหลัง โดยพิจารณาด้านอื่น ๆ ร่วมด้วย เช่น เวลาตอบสนอง การใช้ทรัพยากร และความสะดวกในการดูแล พบว่า ระบบตรวจจับการบุกรุกซูริกาต้า เหมาะกับงานที่ต้องการความเร็วและรองรับทราฟฟิกสูง ส่วน ระบบตรวจจับการบุกรุกสนอร์ต มีความสมดุล ใช้งานง่าย เหมาะกับองค์กรที่มีทรัพยากรจำกัด และ ระบบตรวจจับการบุกรุกซีค เหมาะสำหรับงานวิเคราะห์เชิงลึก ทั้งนี้ผลการวิจัยสามารถนำไปใช้เป็นแนวทางในการเลือกใช้ระบบตรวจจับการบุกรุกที่เหมาะสม และช่วยให้เข้าใจรูปแบบการโจมตีเพื่อนำไปสู่การพัฒนามาตรการป้องกันที่มีประสิทธิภาพมากขึ้น

5.2 อภิปรายผลการวิจัย

จากผลการวิจัยข้างต้นสามารถสรุปได้ว่า ไม่มีระบบตรวจจับการบุกรุก ใดที่ดีที่สุดในทุกด้าน การเลือกใช้งานจึงขึ้นอยู่กับปัจจัยต่างๆ ที่เฉพาะเจาะจงของแต่ละองค์กร เช่น ขนาดของระบบทรัพยากรที่มีอยู่ ความสามารถของบุคลากร และลักษณะของภัยคุกคามที่มักเกิดขึ้น

5.2.1 หากองค์กรต้องการระบบที่ติดตั้งระบบตรวจจับการบุกรุกที่ง่าย ดูแลรักษาง่าย มีความเสถียร และสามารถใช้งานได้ทันทีโดยไม่ต้องเรียนรู้มาก ระบบตรวจจับการบุกรุกนอร์ต คือทางเลือกที่เหมาะสม โดยเฉพาะในองค์กรที่มีทรัพยากรจำกัด และไม่มีทีมรักษาความมั่นคงปลอดภัยเฉพาะทาง

5.2.2 องค์กรที่ปริมาณทราฟฟิกเครือข่ายสูง ต้องการตรวจจับแบบทันทีทันใด (Real-time) ที่มีความแม่นยำสูง และมีความสามารถในการดูแลระบบที่ซับซ้อนได้ ระบบตรวจจับการบุกรุกซูริกาต้าจะตอบโจทย์ได้ดีกว่าด้วยคุณสมบัติ Multi-threading และการรองรับชุดของกฎที่ทันสมัย

5.2.3 สำหรับองค์กรที่ต้องการ วิเคราะห์ข้อมูลย้อนหลัง, ทำ Behavioral Analysis, หรือต้องการความสามารถในการปรับแต่งลึกในระดับ Event-based scripting ระบบตรวจจับการบุกรุกซีค คือเครื่องมือที่มีประสิทธิภาพ แม้จะต้องแลกมากับความซับซ้อนในการใช้งานและดูแลรักษาระบบ

ทั้งนี้ ควรพิจารณาผลกระทบด้านทรัพยากรและบุคลากรควบคู่กัน เช่น ระบบตรวจจับการบุกรุกซีค ต้องใช้ความรู้เฉพาะทางในการเขียน script และปรับแต่งล็อกซึ่งองค์กรอาจต้องลงทุนในด้านการฝึกอบรม หรือการจ้างผู้เชี่ยวชาญเพิ่มเติม

5.3 ข้อเสนอแนะ

5.3.1 การเลือกใช้ระบบตรวจจับการบุกรุก ให้เหมาะสมกับลักษณะงานและทรัพยากรขององค์กร แต่ละองค์กรควรประเมินความต้องการด้านความปลอดภัยเทียบกับข้อจำกัดที่มีอยู่ เช่น ทรัพยากรฮาร์ดแวร์ จำนวนบุคลากรด้านไอที ความชำนาญของทีมงาน และประเภทภัยคุกคามที่พบบ่อยหากมีข้อจำกัดสูงควรเริ่มต้นด้วยระบบที่ติดตั้งง่าย เช่น ระบบตรวจจับการบุกรุกสนอร์ต หรือระบบตรวจจับการบุกรุกซูริกาต้า แล้วจึงค่อยๆ ขยับขยายระบบเมื่อมีความพร้อม

5.3.2 การพัฒนาบุคลากรและเพิ่มความรู้ด้านเทคนิค ระบบตรวจจับการบุกรุก สมัยใหม่ เช่น ระบบตรวจจับการบุกรุกซีค มีศักยภาพสูงในการตรวจจับภัยคุกคามซับซ้อน แต่ต้องการบุคลากรที่มีทักษะเฉพาะด้าน เช่น ความเข้าใจใน Network Protocol, Log Analysis และ Scripting การลงทุนในฝึกอบรมพนักงานหรือเข้าร่วมชุมชนโอเพ่นซอร์สที่เกี่ยวข้อง จะช่วยให้องค์กรสามารถบริหารระบบได้อย่างมั่นคงและยั่งยืน

5.3.3 ผสมผสานการใช้ระบบ ระบบตรวจจับการบุกรุก หลายระบบร่วมกัน การใช้ระบบตรวจจับการบุกรุก มากกว่าหนึ่งประเภทร่วมกัน เช่น ระบบตรวจจับการบุกรุกสนอร์ต หรือ ะบบตรวจจับการบุกรุกซูริกาต้า สำหรับตรวจจับแบบทันทีทันใดและใช้ระบบตรวจจับการบุกรุกซีค สำหรับวิเคราะห์ข้อมูลย้อนหลังหรือการโจมตีซับซ้อน จะช่วยให้สามารถครอบคลุมความต้องการทั้งด้านความเร็วและความลึกของการวิเคราะห์ เพิ่มประสิทธิภาพของการรักษาความปลอดภัยแบบเชิงรุก

5.3.4 ทดสอบและประเมินผลระบบอย่างสม่ำเสมอ โดยภัยคุกคามทางไซเบอร์ในปัจจุบันมีการเปลี่ยนแปลงอย่างต่อเนื่อง ระบบตรวจจับการบุกรุกก็ควรถูกทดสอบและปรับแต่งอยู่เสมอ เพื่อให้สามารถตอบสนองต่อภัยคุกคามใหม่ๆ ได้ทันเวลาและการวางแผนปรับปรุงกระบวนการแจ้งเตือนให้มากขึ้น

5.4 ข้อเสนอแนะสำหรับการวิจัยในอนาคต

5.4.1 ควรขยายการทดลองโดยใช้ชุดข้อมูลที่มีความหลากหลายมากขึ้น เช่น Traffic ที่เกิดขึ้นจริงใน องค์กร หรือใช้ Dataset มาตรฐานเพิ่มเติม เช่น CIC-IDS2017, UNSW-NB15 เป็นต้น

5.4.2 ศึกษาความสามารถของ ระบบตรวจจับภัยคุกคาม แบบ Hybrid (Network-based + Host-based) หรือระบบ NDR (Network Detection and Response)

5.4.3 วิเคราะห์ผลกระทบทางธุรกิจและต้นทุนรวมในการใช้งาน (Total Cost of Ownership

เพื่อสนับสนุนการตัดสินใจเชิงบริหาร

5.4.4 สำรวจการใช้งานร่วมกับระบบอัตโนมัติ เช่น SOAR หรือ SIEM เพื่อพัฒนาแนวทางการตอบสนองภัยคุกคามแบบอัตโนมัติ

5.4.5 เพิ่มประเภทการทดสอบในรูปแบบอื่น เช่น ARP Spoofing ,DNS Spoofing, FTP Brute Force , SSH Dictionary Attack, การโจมตีผ่านช่องโหว่เว็บแอปพลิเคชัน (เช่น Command Injection, File Inclusion) และการใช้ Malware Payload ซึ่งล้วนเป็นภัยคุกคามที่สามารถพบได้จริงในระบบเครือข่ายขององค์กรขนาดกลาง การทดสอบเหล่านี้จะช่วยให้สามารถประเมินประสิทธิภาพของระบบตรวจจับภัยคุกคาม ได้รอบด้านมากขึ้น

เอกสารอ้างอิง

[1] A. A. E. Boukebous, M. I. Fettache, G. Bendiab, and S. Shiaeles, “A Comparative Analysis of Snort 3 and Suricata,” in Proc. 2023 IEEE IAS Global Conf. Emerging Technol. (GlobConET), Loughborough University, London, United Kingdom, 2023.

[2] T. Ncubukezi, L. Mwansa, and F. Rocaries, “A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses,” in Proc. 2020 15th Int. Conf. Internet Technol. Secured Trans. (ICITST), 2020.

[3] A. Shah, S. Clachar, M. Minimair, and D. C., “Building Multiclass Classification Baselines for Anomaly-based Network Intrusion Detection Systems,” in Proc. 2020 IEEE 7th Int. Conf. Data Sci. Adv. Analytics (DSAA), 2020.

[4] G. Jonathan and T. Thamrongthanakit, “Cybersecurity Management Practices in Thai SMEs,” in Proc. Nineteenth Midwest Assoc. Inf. Syst. Conf., Peoria, Illinois, May 16–17, 2024, 2024.

[5] S. Haas, R. Sommer, and M. Fischer, “zeek-osquery: Host-Network Correlation for Advanced Monitoring and Intrusion Detection,” arXiv preprint arXiv:2002.04547, 2020.

[6] K. Ajmeera, B. A. Kumar, T. Sameeratmaja, and S. W. Prakash, “Intrusion Detection System Using Machine Learning,” in Proc. 2023 Int. Conf. Comput. Commun. Informatics (ICCCI), 2023.

[7] A. Tiwari, S. Saraswat, U. Dixit, and S. Pandey, “Refinements in Zeek Intrusion Detection System,” in Proc. 2022 8th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), 2022.

[8] Z. S. Malek, B. Trivedi, and A. Shah, "User behavior pattern-signature based intrusion detection," in Proc. 2020 Fourth World Conf. Smart Trends Syst., Security Sustainability (WorldS4), London, UK, Jul. 27–28, 2020.

[9] A. Waleed, A. F. Jamali, and A. Masood, “Which open-source IDS? Snort, Suricata or Zeek,” in Proc. Computer Networks, vol. 213, 2022.

[10] R. Perdigón-Llanes, “Evaluation of Snort and Suricata for detection of network probes and denial of service attacks,” Revista Científica de Sistemas e Informática, 2020.

[11] M. S. Kursheeth, “Suricata-Based Intrusion Detection and Isolation System for Local Area Networks,” in Proc. 2021 Int. Conf. Commun., Comput., Electr. Syst. (ICCCES), 2021.

[12] A. K. Patil and P. R. Patil, “Comparative Study of Intrusion Detection System Using Machine Learning Algorithms,” in Proc. 2022 Int. Conf. Adv. Comput. Technol. Commun. (ICACTC), 2022.

[13] J. K. Nair and S. Thomas, “An Enhanced Network Intrusion Detection System Using Zeek and Machine Learning,” in Proc. 2023 Int. Conf. Intell. Comput. Control Syst. (ICICCS), 2023.

[14] S. M. Alshamrani, H. R. Alkhateeb, and A. Al-Nemrat, “Intrusion Detection System Based on Machine Learning Techniques: A Comparative Study,” in Proc. 2020 IEEE Int. Conf. Comput. Commun. (ICCC), 2020.

[15] R. P. Jadhav and P. R. Patil, “Comparative Analysis of Network Intrusion Detection Systems Using Machine Learning,” in Proc. 2021 Int. Conf. Inf. Technol. Commun. (ICT), 2021.

[16] H. Zhang, Z. Chen, and X. Li, “Performance Evaluation of Snort and Suricata in Detecting Cyber Attacks in Cloud Environment,” in Proc. 2022 IEEE Int. Conf. Cloud Comput. Technol. Sci. (CloudCom), 2022.

[17] P. S. Rao and V. S. Reddy, “Hybrid Intrusion Detection System Using Signature and Anomaly-Based Techniques with Zeek,” in Proc. 2023 Int. Conf. Cybersecurity AI (CyberAI), 2023.

[18] M. M. Rahman and S. Sultana, “Evaluation of Open Source Intrusion Detection Systems for IoT Networks,” in Proc. 2021 IEEE Int. Conf. Internet Things (iThings), 2021.

[19] A. Ingle, A. Gour, and K. Kshirsagar, “Flow-chart for detection of TCP-SYN flood attack,” in Proc. 2021 Int. Conf. Communication and Signal Processing (ICCSP), 2021

[20] M. Ring, D. Landes, and A. Hotho, “Flow-based benchmarking of port scan detection methods,” in Proc. 2023 Int. Conf. Information Systems and Security (ICISS), 2023.

[21] N. Aldaoud, M. N. Kabir, and A. A. Alqaralleh, “ICMP-based amplification DDoS attacks: Smurf and Fraggle,” in Proc. 2021 IEEE Int. Conf. Computer and Communications (ICCC), 2021.

[22] A.-D. Tudosi, A. Graur, D. Balan, and A. Potorac, “An efficient method for detecting ICMP flood attacks using pattern analysis,” in Proc. 2022 Int. Conf. Computers, Communications, and Systems (ICCCS), 2022.

[23] N. A. Yousif and D. Naji, “Ethical hacking: Real evaluation model of brute force attacks in password cracking,” in Proc. 2024 Int. Conf. Network Security and Ethical Hacking (NSEH), 2024.

[24] P. Lu, Y. Zhang, and M. Li, “Hybrid deep learning model for SQL injection detection using CNN and Random Forest,” in Proc. 2025 Int. Conf. Cyber Threat Intelligence (CTI), 2025.

[25] A. Kumar, P. Mittal, and A. Gupta, “XSS attack detection and mitigation using deep learning,” in Proc. 2021 Int. Conf. Web Intelligence and Security (WIS), 2021.

[26] Imperva, “What is a SYN flood attack?” *Imperva*, [Online]. Available: https://www.imperva.com/learn/ddos/syn-flood/ (Accessed: Sep. 16, 2024)

[27] Onsec Blog, “TCP Tarpit and port scanning barricades on both sides,” Onsec, [Online]. Available: https://blog.onsec.io/tcp-tarpit-and-port-scanning-barricades-on-both-sides/ (Accessed: Sep. 16, 2024).

[28] Imperva, “Smurf attack DDoS,” Imperva, [Online]. Available: https://www.imperva.com/learn/ddos/smurf-attack-ddos/ (Accessed: Sep. 16, 2024).

[29] Wallarm, “What is a ping flood DoS attack,” Wallarm, [Online]. Available: https://www.wallarm.com/what/what-is-a-ping-flood-dos-attack (Accessed: Sep. 16, 2024).

[30] Syteca, “Brute force attacks,” Syteca, [Online]. Available: https://www.syteca.com/en/blog/brute-force-attacks (Accessed: Sep. 16, 2024).

[31] Wallarm, “Structured Query Language Injection (SQLi) - Part 1,” Wallarm, [Online]. Available: https://www.wallarm.com/what/structured-query-language-injection-sqli-part-1 (Accessed: Sep. 16, 2024).

[32] Imperva, “Cross-site scripting (XSS) attacks,” Imperva, [Online]. Available: https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/ (Accessed: Sep. 16, 2024).

ประวัติผู้วิจัย

ชื่อ : นายวุฒิฉัตร รุ่งวัฒนาพร

ชื่อการค้นคว้าอิสระ : การเปรียบเทียบประสิทธิภาพ ระบบการตรวจจับการบุกรุกที่เหมาะสมในองค์กรขนาดกลาง

สาขาวิชา : การบริหารเครือข่าย และความมั่นคงปลอดภัยสารสนเทศ

ประวัติการศึกษา

สำเร็จการศึกษาระดับปริญญาตรี สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยราชภัฏพระนคร

ประวัติการทำงาน

พ.ศ. 2564 – ปัจจุบัน ทำงานบริษัท ซันเดย์ ประกันภัย (ประเทศไทย) จำกัด (มหาชน)

สถานที่ติดต่อปัจจุบัน

199/119 หมู่บ้าน Centro ราชพฤกษ์ 2 ซอย 17 บางกร่าง เมือง นนทบุรี 11110