การวิเคราะห์ระบบตรวจจับการบุกรุกบนอุปกรณ์ฝังตัวเพื่อแจ้งเตือนการบุกรุกเครื่องแม่ข่ายเคอร์เบอรอส

Intrusion Detection System Analysis on Embedded Devices to Alert Kerberos Server Intrusion

อรรถพล ป้อมสถิตย์*

Auttapon Pomsathit

Received : May 27, 2019

Revised : March 30, 2022

Accepted : April 27, 2022

บทคัดย่อ

งานวิจัยระบบตรวจจับการบุกรุกบนอุปกรณ์ฝังตัวเพื่อแจ้งเตือนการบุกรุกเครื่องแม่ข่ายเคอร์เบอรอสได้นำเสนอการศึกษาการบุกรุกเครือข่ายที่มีผู้บุกรุกโจมตีไปที่เครื่องแม่ข่าย ด้วยการทดสอบการโจมตีรูปแบบการปฏิเสธการให้บริการ 3รูปแบบได้แก่ SYN Flood UDP Flood และ ICMP Flood โดยทดสอบการเปรียบเทียบระหว่างการโจมตีเคอร์เบอรอสเซิร์ฟเวอร์ เพื่อดูประสิทธิภาพของเคอร์เบอรอส การทำงานการตรวจจับการบุกบุกที่ถูกติดตั้งในอุปกรณ์ฝังตัวราสเบอรี่ไพ และการทำงานการตรวจจับการบุกบุกบนเครื่องแม่ข่าย ซึ่งการตรวจสอบการทำงานนั้นใช้เทคนิคเชลล์สคริปโดยใช้เวลา 120 วินาที ต่อการทดลอง บันทึกการทดลองทุก ๆ 5 วินาที และตรวจสอบผลค่าทรัพยากรหน่วยประมวลผลกลางหน่วยความจำหลัก และระบบเครือข่าย ทั้งนี้เครื่องแม่ข่ายที่อยู่ในแผนผังเครือข่ายจะกำหนดให้ไม่มีการใช้งานไฟร์วอล์และการรักษาความปลอดภัยรูปแบบอื่นๆ ส่วนระบบตรวจจับการบุกรุกเครือข่ายจะใช้โปรแกรม Snort บนระบบปฏิบัติการ Linux ผลการตรวจจับการบุกรกจากการโจมตีประกอบด้วย 1.ผลการโจมตีผ่านการสื่อสารภายในของเครื่องแม่ข่ายเคอร์เบอร์รอสมีค่าการใช้ทรัพยากรเฉลี่ยสูงกว่าการสื่อสารภายนอก 1.08 เท่า 2.ผลการตรวจจับบุกรุกโจมตีแบบ TCP Flood ค่าทรัพยากรเฉลี่ยคิดเป็น 1.02 และ 1.24 เท่า ของ UDP Flood และ ICMP Flood ตามลำดับ จะเห็นได้ว่าการตรวจจับการโจมตี TCP Flood และ UDP Flood มีความแตกต่างกันไม่มาก แต่ส่วนของ ICMP Flood มีการใช้ทรัพยากรน้อยที่สุด 3. ผลการทำงานการตรวจจับการบุกรุกของอุปกรณ์ฝังตัวด้วยการสื่อสารแบบสายมีค่าการใช้ทรัพยากรรวม

*อาจารย์ประจำสาขาวัตกรรมดิจิทัล วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี มหาวิทยาลัยรังสิต

Lecturer of Digital Innovation Department College of Digital Innovation Technology Rangsit University

เฉลี่ยมากกว่าแบบไร้สายถึง 2.28 เท่า 4. ผลการทำงานการตรวจจับการบุกรุกของอุปกรณ์ฝังตัวด้วยรูปแบบการสื่อสารภายในมีค่าการใช้ทรัพยากรรวมเฉลี่ยมากกว่าภายนอกถึง 1.16 เท่า 5.ส่วนผลการทำงานของเครื่องแม่ข่ายเคอร์เบอรอสที่ติดตั้งระบบตรวจจับการบุกรุก มีค่าทรัพยากร CPU และ RAM มากกว่าเครื่องแม่ข่ายเคอร์เบอรอสที่แยกการติดตั้งระบบตรวจจับการบุกรุกไปยังราสเบอรี่ไพถึง 1.28 และ 1.15 เท่า สุดท้ายนี้การติดตั้งระบบตรวจจับการบุกรุกลงบนอุปกรณ์ราสเบอรี่ไพช่วยให้ลดค่าทรัพยากรที่ใช้ในเครื่องแม่ข่ายเคอร์เบอรอสที่ติดตั้งระบบตรวจจับการบุกรุกได้ และไม่เป็นการรบกวนการทำงานของเครื่องแม่ข่ายเคอร์เบอรอส

คำสำคัญ : ระบบตรวจจับการบุกรุก / การปฏิเสธการให้บริการ /การรักษาความมั่นคงทางไซเบอร์ / อุปกรณ์ฝังตัว

ABSTRACT

Research into Intrusion detection on embedded devices for the purpose of alerting to Kerberos server intrusion. The research examines network intrusions in which intruders assault the system. To evaluate the performance of Kerberos against three distinct denial-of-service attacks—SYN Flood, UDP Flood, and ICMP Flood—we ran benchmarks against Kerberos server assaults. A Snort invasion detection capability is deployed on both the embedded Raspberry Pi and the server. Performance verification was accomplished through the use of a shell script approach that required 120 seconds for each experiment, recorded the experiment every 5 seconds, and examined the processor resource numbers. Primary memory and network connectivity However, placing the server on the network map disables firewalls and other types of protection. The network intrusion detection system runs on the Linux operating system and is based on the Snort application. 1. The consequence of an attack via the Kerberos server's internal communication consumes on average 1.08 times the resources of external communication. 2. A TCP Flood attack's consequences UDP Flood and ICMP Flood are 1.02 and 1.24 times more powerful, respectively. As can be observed, the detection of TCP Flood and UDP Flood assaults is similar, although ICMP Flood consumes the fewest resources. Intrusion detection in embedded devices using wired connections consumes an average of 2.28 times as many resources as wireless intrusion detection. The average overall resource use is 1.16 times that of the external environment. It has 1.28 and 1.15 times the CPU and RAM resources of a standalone Kerberos server for detecting Raspberry Pi incursions, respectively. Intrusion detection on Raspberry Pi devices significantly lowers the cost of resources consumed by Kerberos servers equipped with intrusion detection systems. It does not interfere with the Kerberos server's functioning.

Keywords : : Intrusion Detection System / Denial of Service / Cyber Security / Embedded Devices

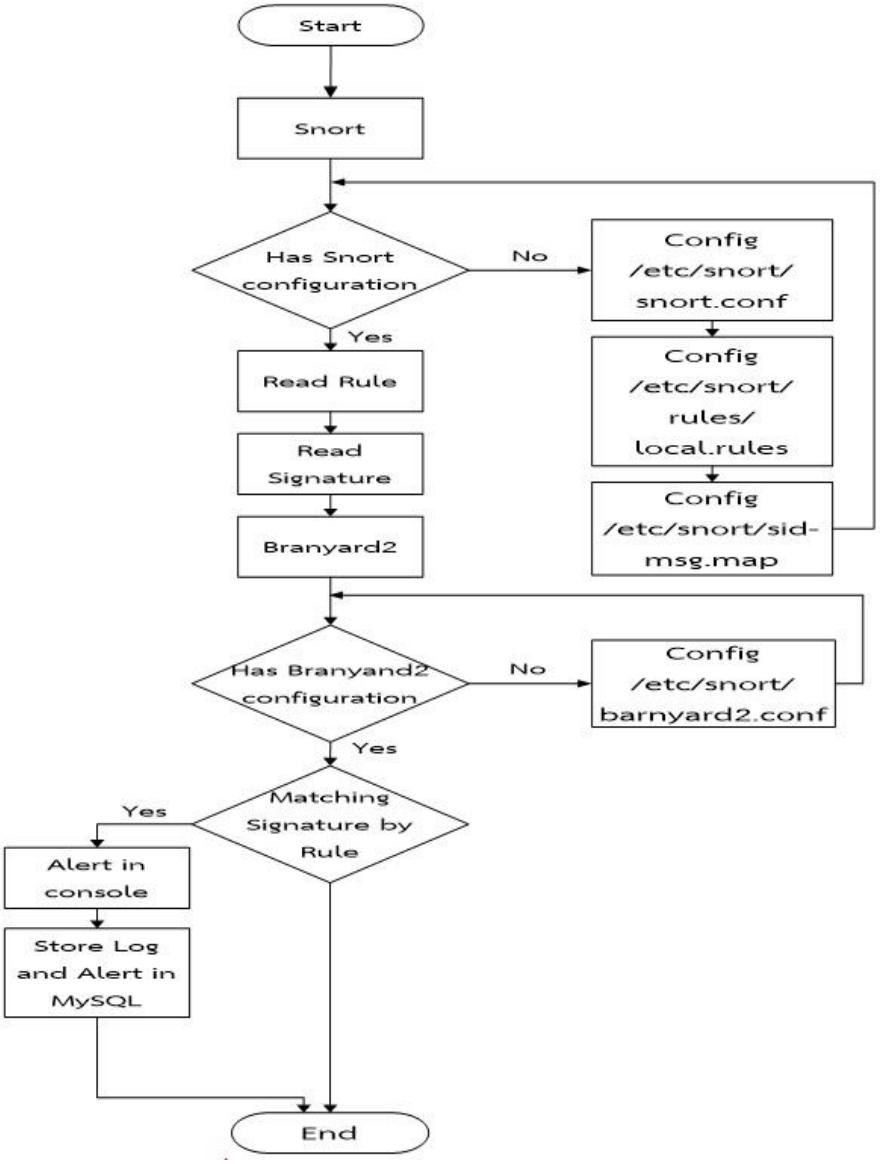
บทนำ

ปัจจุบันระบบคอมพิวเตอร์ที่ถูกวางบนเครือข่ายมักเป็นระบบเปิดซึ่งยอมให้มีการติดต่อขอใช้งานจากระยะไกลได้ บุคคลที่ติดต่อขอใช้บริการผ่านทางเครือข่ายคอมพิวเตอร์สามารถทำการเชื่อมต่อแล้วเข้าใช้บริการผ่านเครื่องผู้ให้บริการจากตำแหน่งที่อยู่บนระบบเครือข่ายทำหน้าที่เป็นเครื่องผู้ให้บริการแก่เครื่องผู้รับบริการ เมื่อมีการขอเข้าใช้บริการมากขึ้นจากแหล่งต่างๆ บนเครือข่ายอินเทอร์เน็ตอาจจะมีผู้ใช้บางคนที่ไม่ประสงค์ดี บุคคลเหล่านี้อาจทำให้เกิดความเสียหายต่อเครือข่าย และองค์กรหน่วยงานต่างๆ ได้ดังนั้นการรักษาความปลอดภัยทางไซเบอร์ที่มักจะเป็นการโจมตีแบบภายใน และส่วนน้อยจะเป็นการโจมตีจากภายนอก ถึงแม้ว่าเทคโนโลยีด้านการรักษาความมั่นคงทางไซเบอร์ได้ก้าวไปข้างหน้าอย่างรวดเร็วซอฟต์แวร์ และฮาร์ดแวร์ต่างๆ ที่เกี่ยวข้องกับความปลอดภัยด้านสารสนเทศได้ถูกวิจัยและพัฒนาขึ้นเพื่อตอบสนองความต้องการของผู้ใช้มากขึ้น แต่ก็ยังไม่สามารถป้องกันรูปแบบการโจมตีที่มีความหลากหลาย และซับซ้อนเพิ่มขึ้น ดังนั้นระบบตรวจจับการบุกรุก (Intrusion Detection System: IDS) หรือระบบตรวจจับการบุกรุกเป็นอีกหนึ่งเครื่องมือที่ใช้สำหรับตรวจจับความพยายามบุกรุกเครือข่ายโดยระบบจะแจ้งเตือนไปยังผู้ดูแลระบบเมื่อมีการบุกรุก หรือมีการพยายามที่จะบุกรุกเครือข่าย โดยระบบจะรายงานเฉพาะสิ่งที่กำหนดให้รายงานเท่านั้น (อรรถพล, 2562) อีกทั้งองค์กรหน่วยงานต่าง ๆ มีความจำเป็นต้องมีระบบตรวจจับการบุกรุก และระบบพิสูจน์ตัวตนควบคู่กัน เป็นอีกทางหนึ่งในการช่วยรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ หากเปรียบระบบเครือข่ายคอมพิวเตอร์เหมือนบ้านแล้วเคอร์เบอรอสเปรียบเสมือนประตูเข้าบ้านที่ต้องสแกน ลายนิ้วมือและระบบตรวจจับการบุกรุก เปรียบเสมือนยามรักษาการณ์ภายในบ้านที่ชำนาญในการวิเคราะห์คนผ่านเข้าออก โดยดูจากลักษณะและพฤติกรรมของบุคคลที่ไม่ประสงค์ดีหากใครมีพฤติกรรมน่าสงสัยก็จะรายงานให้ผู้ดูแลระบบทราบทันที นับว่าระบบตรวจจับการบุกรุกเป็นเครื่องมือสำคัญอย่างยิ่งที่จะรับมือการบุกรุกจากผู้บุกรุก ผู้วิจัยจึงมีแนวคิดในการทำวิจัยการวิเคราะห์ระบบตรวจจับการบุกรุกบนอุปกรณ์ฝังตัวเพื่อแจ้งเตือนการบุกรุกเครื่องแม่ข่ายเคอร์เบอรอสที่จะมีการติดตั้งระบบตรวจจับการบุกรุกในอุปกรณ์ฝังตัวนั้นคือ Raspberry PI เป็นอุปกรณ์ที่มีราคาประหยัดในการช่วยเครื่องแม่ข่ายเคอร์เบอรอสในการตรวจจับการบุกรุกโดยจะมีการแสดงผลการวิเคราะห์เพื่อประสิทธิภาพของระบบการทำงานของระบบตรวจจับการบุกรุกเพื่อป้องกันการโจมตีจากผู้บุกรุกในการระงับ ชะลอ ขัดขวาง หรือ รบกวนจนเครื่องแม่ข่ายไม่สามารถทำงานตามปกติได้ โดยผลลัพธ์ที่ได้จากการวิจัยจะสามารถนำมาใช้ในปรับปรุง และพัฒนาการดำเนินงานของผู้ดูแลระบบเครือข่ายของหน่วยงาน ภาครัฐและภาคเอกชน เพื่อนำไปสู่ความมั่นคงของระบบคอมพิวเตอร์และเทคโนโลยีสารสนเทศ

วิธีดำเนินการวิจัย

สำหรับการออกแบบระบบป้องกันการบุกรุกเครือข่าย เพื่อทำการทดสอบและวิเคราะห์ประสิทธิภาพของระบบตรวจจับการบุกรุกที่ใช้ในการป้องกันการบุกรุกเครือข่ายจากการโจมตีในรูปแบบต่าง ๆ อันประกอบด้วย

1. ส่วนตรวจจับการบุกรุก การออกแบบส่วนตรวจจับการบุกรุกเครือข่ายมีเป้าหมาย คือสามารถตรวจจับการบุกรุกเครือข่ายได้อย่างมีประสิทธิภาพ และสามารถแจ้งเตือนแก่ผู้ดูแลระบบ เพื่อหาวิธีการป้องกัน โดยมีรายละเอียดการออกแบบดังนี้



ภาพที่ 1 การออกแบบส่วนตรวจจับการบุกรุกเครือข่าย

1.1 ระบบปฏิบัติการลินุกซ์ลงราชเบอรี่ไพโดยใช้ระบบปฏิบัติการ รุ่น Raspbian Jessie เป็นรุ่นที่รองรับการใช้งานโปรแกรม สนอร์ท

1.2 ติดตั้งโปรแกรมสนอร์ท เป็นซอฟต์แวร์รักษาระบบความปลอดภัยทางเครือข่ายที่มีผู้พัฒนาอย่างต่อเนื่องซึ่งตัวโปรแกรมสนอร์ทจะทำงานบนระบบปฏิบัติการลินุกซ์ และวินโดว์ (Windows)

1.3 ทำการตั้งค่า (Configure) ค่ารูล (Rule) ของโปรแกรมสนอร์ท รูลนั้นก็คือกฎหรือข้อบังคับในการตรวจจับรูปแบบการโจมตี หรือแพ็คเก็ตที่โปรแกรมตรวจจับได้ ในการวิจัยนี้ได้ทำการตั่งค่าและปรับแต่งค่ารูลของโปรแกรมสนอร์ท เพราะค่ารูลปกติที่โปรแกรมตั้งค่าให้เป็นค่ารูลที่วิเคราะห์รูปแบบการโจมตีแบบธรรมดา ซึ่งตัวโปรแกรมจะไม่เปิดการใช้งานรูลทั้งหมด ตัวโปรแกรมจึงใช้งานรูลบางส่วนเท่านั้น ทำให้ในการศึกษาและวิจัยนั้นไม่สามารถเปรียบเทียบค่าประสิทธิภาพที่สูงสุดในการตรวจจับการโจมตีของโปรแกรมได้ ดังนั้นจึงทำการตั้งค่าค่ารูลใหม่โดยทำการแก้ไข ปรับแต่ง และตั้งค่าภายในไฟล์ snort.conf ของโปรแกรม (Auttapon, 2015) โดยทำการเปิดใช้งานรูลทั้งหมดที่โปรแกรมสามารถตรวจจับได้ และทำการอัพเดท (Update) กำหนดค่ารูลของสนอร์ท โดยต้องเข้าไปแก้ไขไฟล์ local.rules ซึ่งไฟล์นี้จะสามารถกำหนดได้ว่าจะทำการตรวจจับที่อยู่ไอพี พอร์ต และการเชื่อมต่อในลักษณะที่กำหนด เป็นแบบ TCP, UDP และ ICMP ซึ่งการตั้งค่าไฟล์นี้สนอร์ทจะทำการบันทึกรูลลงในฐานข้อมูลด้วย โดยการดำเนินการส่วนตรวจจับการบุกรุกเครือข่าย แสดงดังภาพที่ 1

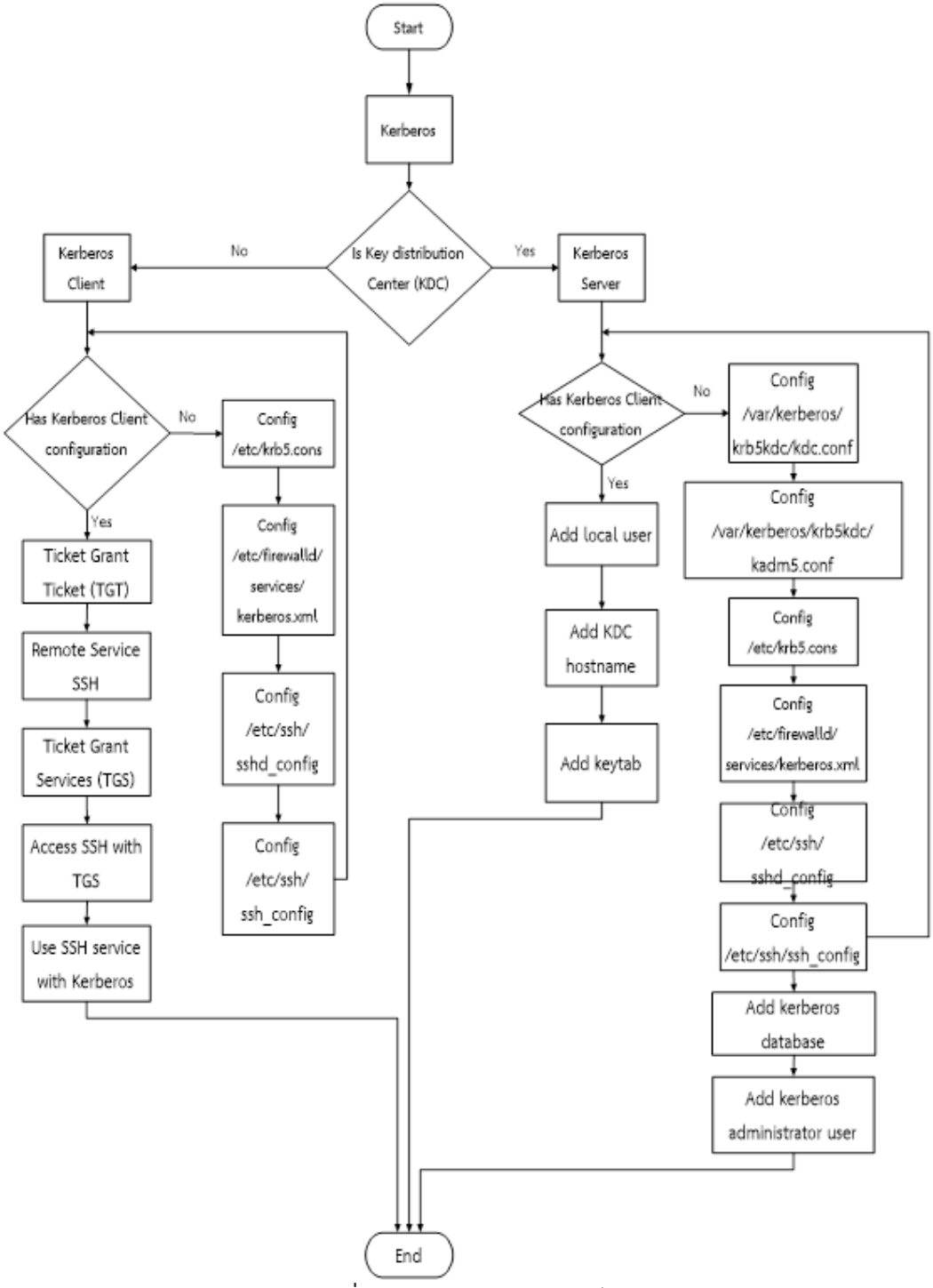
2. ส่วนระบบพิสูจน์ตัวตน

แสดงการตรวจสอบผู้ที่มาใช้งานระบบเครือข่ายอินเทอร์เน็ต โดยระบบจะทำการตรวจสอบสอบจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ว่าถูกต้องหรือไม่ โดยมีส่วนประกอบและโครงสร้างดังภาพที่ 2 ซึ่งจากการออกแบบส่วนโปรแกรมระบบพิสูจน์ตัวตนจะทำงานภายใต้ระบบปฏิบัติการ CentOS ประกอบไปด้วย 2 ส่วนคือ และผู้ใช้เคอร์เบอรอส (Kerberos Client) และส่วนศูนย์กลางการกระจายกุญแจที่สำคัญ (Thakur, Dogra & Sood, 2015) โดยมีรายละเอียดการดำเนินงานดังนี้

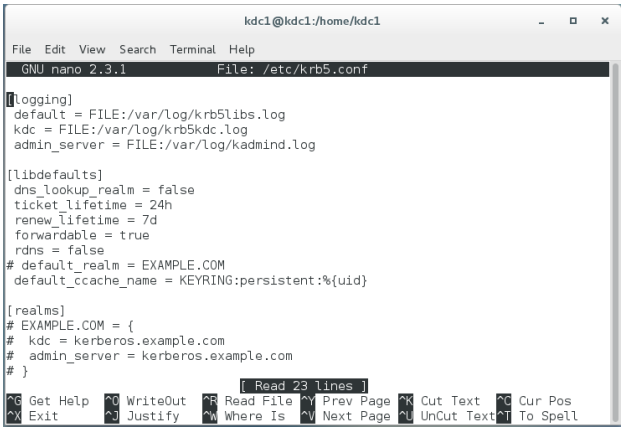
2.1 ระบบปฏิบัติการลีนุกซ์ ทำการติดตั้งระบบปฏิบัติการลินุกซ์ ใช้ในการทดสอบจะใช้รุ่น 7 รวมไปถึงการติดตั้งโปรแกรมเคอร์เบอรอส เซิร์ฟเวอร์ และโปรแกรม Kerberos workstation โดยในช่วงเวลาที่ทำวิจัยนี้จะใช้รุ่น 5

2.2 ติดตั้งผู้ใช้เคอร์เบอรอส เป็นซอฟต์แวร์ระบบพิสูจน์ตัวตนทำงานผ่านโปรโตคอล 88 ที่โดยในช่วงเวลานี้จะใช้ Kerberos workstation ดังภาพที่ 3

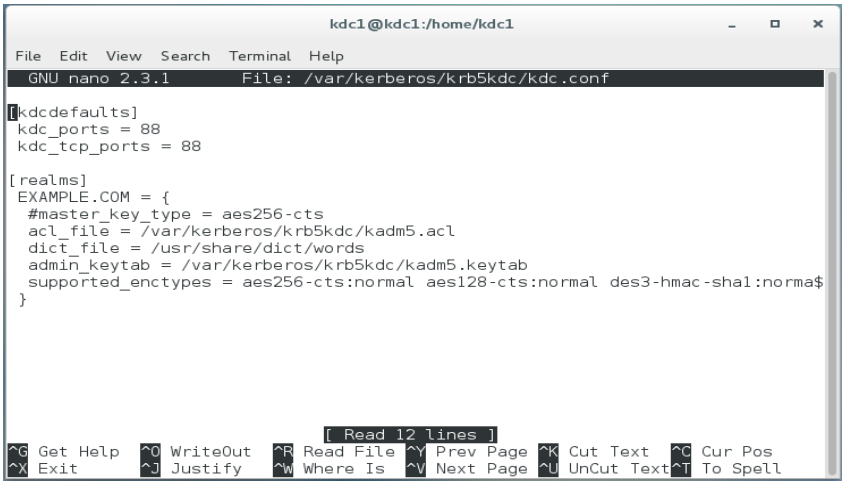
2.3 ติดตั้งระบบศูนย์กลางการกระจายกุญแจเป็นซอฟต์แวร์ระบบระบบพิสูจน์ตัวตนเป็นส่วนเก็บข้อมูลยืนยันตัวตนบนระบบเครือข่าย ดังภาพที่ 4



ภาพที่ 2 การออกแบบระบบพิสูจน์ตัวตน



ภาพที่ 3 แสดงคำสั่งการตั้งค่าผู้ใช้เคอร์เบอรอส

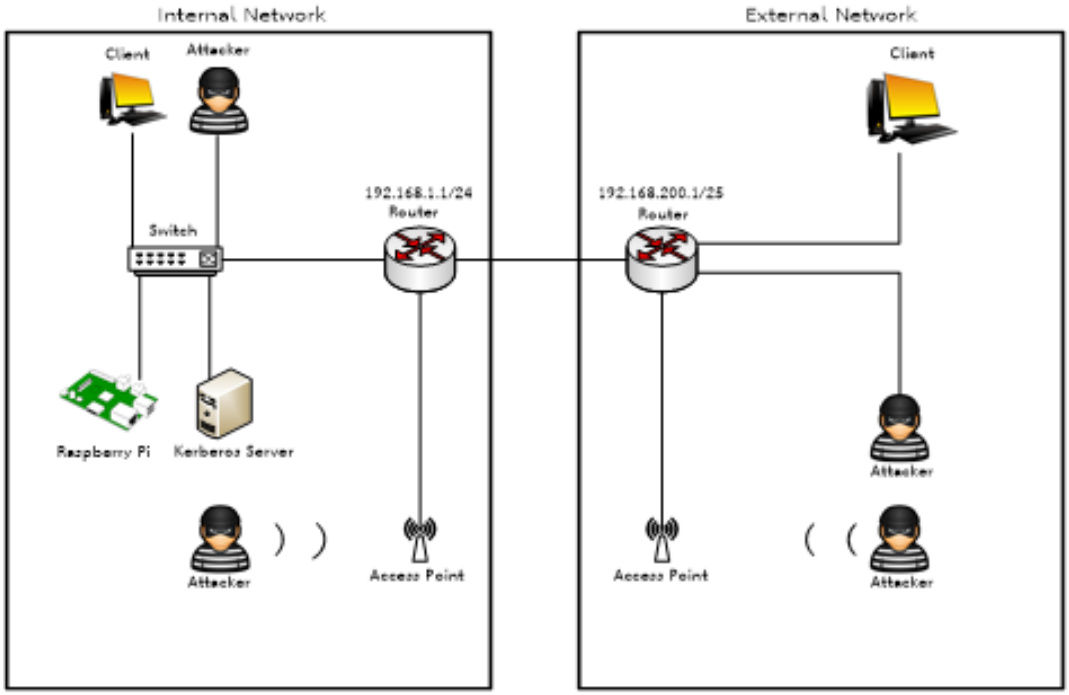


ภาพที่ 4 ตัวอย่างการตั้งค่าศูนย์กลางการกระจายกุญแจ

ในแต่ละการโจมตีแบ่งออกเป็นการโจมตีเครื่องแม่ข่ายเคอร์เบอรอส และการตรวจจับการบุกรุกบนอุปกรณ์ผังตัวราสเบอรี่ไพ โดยจะใช้เทคนิคการโจมตีทั้ง 3 โพรโทคอล คือ TCP Flood, UDP Flood และ ICMP Flood ในการทดลองแต่ละครั้งจะออกแบบโดยใช้ผังเครือข่ายแตกต่างกันออกไปขึ้นอยู่กับวัตถุประสงค์ในการที่ศึกษาการทดลองนั้น และขั้นตอนในการทดลองนั้น ได้นำเสนอรูปแบบของผังงานดังภาพที่ 5 เพื่อให้ผู้ที่สนใจทำการการศึกษากระบวนการการทดสอบง่ายขึ้น

ในแต่ละการทดลอง ทำการทดลองโดยใช้โปรแกรมจำลองการบุกรุก มีการโจมตีที่เหมือนกัน และมีเวลาในการทดลองที่เท่ากันเพื่อที่จะนำผลการทดลองที่ได้มาเปรียบเทียบวิเคราะห์หาความแตกต่างในแต่ละการทดลอง ในการออกแบบผังเครือข่ายการโจมตีนั้น ได้ออกแบบโดยใช้อุปกรณ์ที่มีอยู่ของผู้วิจัย จึงจำเป็นต้องคำนึงถึงทรัพยากรที่ใช้เป็นสำคัญโดยมีรายละเอียดการออกแบบผังเครือข่ายทั้งหมดกล่าวคือให้มีการทดลองที่

สภาพแวดล้อมเดียวกันตามที่กำหนดสภาพการทดลองไว้โดยคำนึงถึงมีการโจมตีไปยังเครื่องแม่ข่ายเคอร์เบอรอส หรือเครื่องแม่ข่ายเคอร์บอรอสที่มีการตรวจจับการบุกรุกด้วยอุปกรณ์ฝังตัวราสเบอร์รี่ไพ และเครื่องแม่ข่ายที่ติดตั้งระบบตรวจจับการบุกรุกไว้ (Muhammet & Resul, 2018) แล้วทำการตรวจสอบด้วยโปรแกรมตรวจสอบการทำงาน โดยนำผลทรัพย์ยากรจาการทดลองนำมาบันทึกลงตาราง



ภาพที่ 5 แสดงการออกแบบเครือข่ายภายใน และภายนอก

ผลการวิจัย

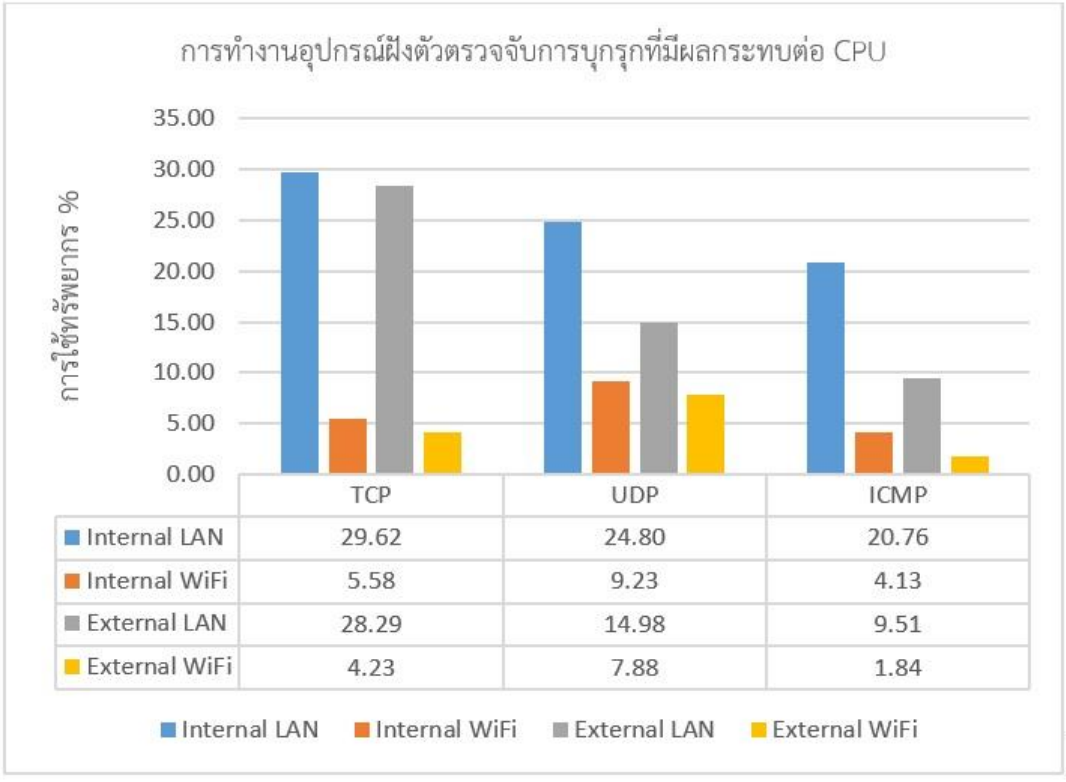
การวิเคราะห์ประสิทธิภาพการโจมตี ได้แบ่งการทดลองออกเป็น 4 การทดลองคือ

1. ผลรวมการทำงานอุปกรณ์ฝังตัวตรวจจับการบุกรุกที่มีผลกระทบต่อ CPU
2. ผลรวมการทำงานอุปกรณ์ฝังตัวตรวจจับการบุกรุกที่มีผลกระทบต่อ RAM
3. ผลรวมการทำงานอุปกรณ์ฝังตัวตรวจจับการบุกรุกที่มีผลกระทบต่อ Network
4. การเปรียบเทียบการทำงานอุปกรณ์ฝังตัวตรวจจับการบุกรุกที่มีผลกระทบต่อ TCP, UDP และ ICMP

เพื่อที่จะให้ทราบถึงประสิทธิภาพการทำงานของฮันนี่พอท และความแตกต่างระหว่างการโจมตีผ่านระบบเครือข่ายสายและการโจมตีผ่านระบบเครือข่ายไร้สาย เพื่อวิเคราะห์ประสิทธิภาพการตรวจจับการบุกรุกที่มีประสิทธิภาพมากที่สุด ซึ่งในการทดลองนี้จะใช้การโจมตีแบบปฏิเสธการให้บริการโดยแบ่งการโจมตีออกเป็น 3 ประเภท ได้แก่ SYN Flood, UDP Flood และ ICMP Flood ซึ่งทำการทดสอบประสิทธิภาพด้วยการใช้ระบบ

ตรวจจับการบุกรุกเพื่อเก็บข้อมูลการบุกรุกที่เกิดขึ้นในเครื่องแม่ข่าย โดยผลการทดลองจะเปรียบเทียบจำนวนเหตุการณ์ที่ระบบตรวจจับการบุกรุกซึ่งสามารถจับได้ระหว่างการโจมตีผ่านเครือข่ายสาย และการโจมตีผ่านระบบเครือข่ายไร้สายที่มีการโจมตีจากภายในและภายนอกโดยมีเราท์เตอร์ทำหน้าที่แบ่งพื้นที่ระบบเครือข่ายภายในและภายนอก ซึ่งการดำเนินการตามขั้นตอนการทดลองได้ทำการรวบรวมข้อมูลจากผลการดำเนินงานหาค่าเฉลี่ย และแสดงอยู่ในรูปของกราฟเพื่อให้ง่ายต่อการวิเคราะห์ข้อมูลในการทดลองโจมตีระบบในระยะเวลาเท่าๆกัน คือ 5 วินาทีโดยมีการส่งแพ็กเก็ตในการโจมตีจำนวน 1,000 แพ็กเก็ต

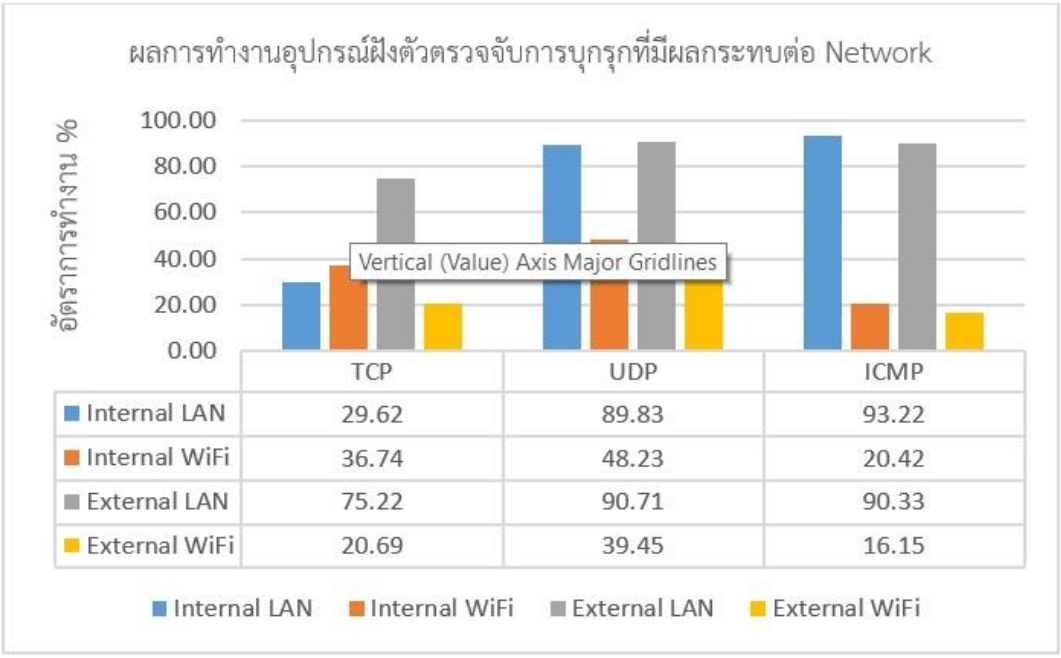
1. สรุปผลการทำงานอุปกรณ์ฝังตัวตรวจจับการบุกรุกที่มีผลกระทบต่อ CPU แสดงในภาพที่ 6 แสดงให้เห็นการตรวจจับการบุกรุกที่สามารถส่งผลกระทบต่อ CPU มากที่สุดคือ การตรวจจับการบุกรุกแบบ TCP เนื่องจากเป็นการบุกรุกในโพรโทคอลลที่มีการเชื่อต่อโดยใช้การเชื่อมต่อแบบสมบูรณ์ (Connection-Oriented) ส่งผลให้มีค่าความเปลี่ยนแปลงของการใช้ทรัพยากร CPU มีค่ามากที่สุดเมื่อเปรียบเทียบกับการบุกรุกรูปแบบอื่นแสดงดังภาพที่ 6



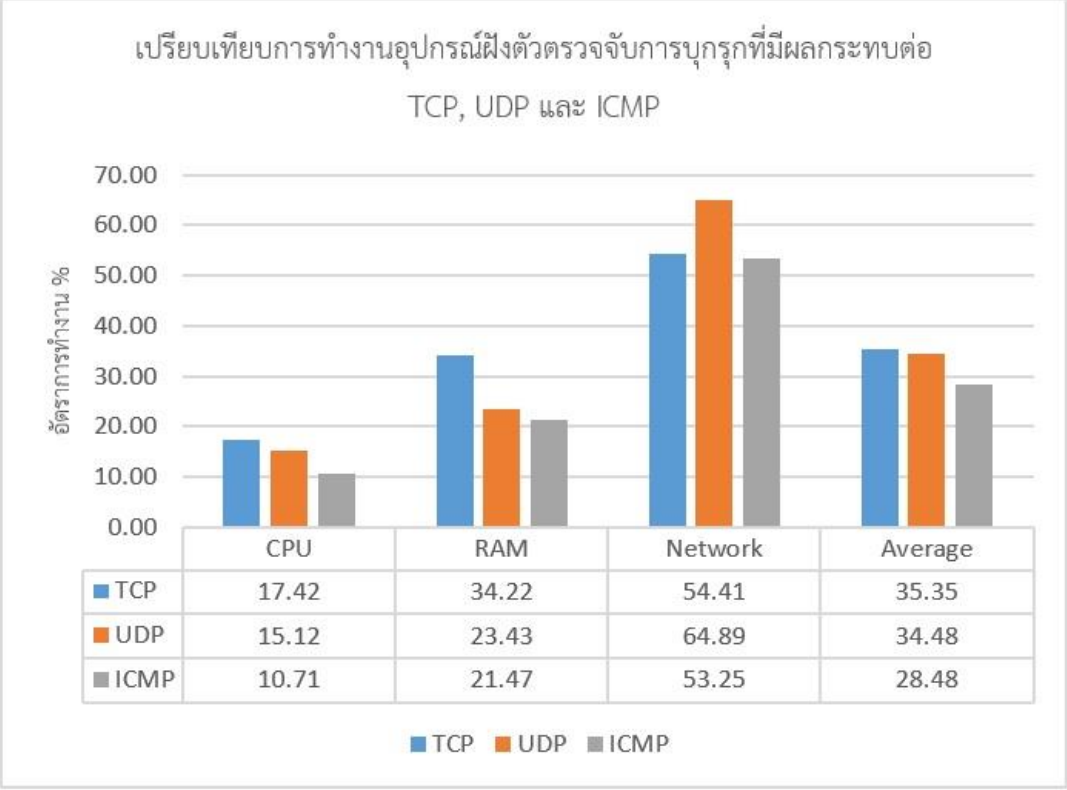
ภาพที่ 6 ผลการทำงานอุปกรณ์ฝังตัวตรวจจับการบุกรุกที่มีผลกระทบต่อ CPU

2. ผลรวมการทำงานอุปกรณ์ฝังตัวตรวจจับการบุกรุกที่มีผลกระทบต่อ RAM แสดงดังภาพที่ 7 แสดงให้เห็นการ ตรวจจับบุกรุกส่งผลกระทบต่อ RAM ที่สุดคือ การตรวจจับการบุกรุกแบบ ICMP ในรูปแบบการสื่อสารแบบภายใน เนื่องจาก การประมวลผลของโพรโทคอลล ICMP มีข้อมูลการสื่อสารที่กำหนดไว้แล้วแต่จะ

เพิ่มในส่วนของข้อมูลข้อมูลเปย์โหลด (Payload) เป็นข้อความแบบสุ่ม ทำให้กระบวนการถอดรหัสเป็นไปได้ช้า และ ในส่วนรูปแบบการสื่อสารแบบภายในไม่ได้ทำการเปลี่ยนแปลงหรือบีบอัดข้อมูลใดๆ จึงทำให้ข้อมูลค้างใน RAM เป็นจำนวนมาก



ภาพที่ 7 ผลรวมการทำงานอุปกรณ์ฝังตัวตรวจจับการบุกรุกที่มีผลกระทบต่อ RAM



ภาพที่ 8 เปรียบเทียบการทำงานอุปกรณ์ฝังตัวตรวจจับการบุกรุกที่มีผลกระทบต่อ TCP, UDP และ ICMP

3. ผลรวมการทำงานอุปกรณ์ฝังตัวตรวจจับการบุกรุกที่มีผลกระทบต่อ Network แสดงดังภาพที่ 8 แสดงให้เห็นการตรวจจับบุกรุกที่สามารถส่งผลกระทบต่อ Network มากที่สุดคือการตรวจจับการบุกรุกแบบ ICMP เนื่องจากเป็นการบุกรุกที่มีรูปแบบคือ ส่งแล้วมีการตอบกลับเสมอ และสวิทช์รับข้อมูลขาเข้า และขาออก ทำให้ค่า Network มีขนาดใหญ่ตามในส่วนของ UDP เป็นการบุกรุกในโพรโทคอล UDP โดยใช้เทคนิคการเชื่อมต่อแบบคอนเนคชั่นเลท ส่งผลให้มีค่าความเปลี่ยนแปลงของการใช้ทรัพยากร Network ที่มีค่ามากตามกัน

อภิปรายผลการวิจัย

งานวิจัยนี้ได้ทำการทดลองรูปแบบการโจมตีอันประกอบด้วย TCP Flood, UDP Flood และ ICMP Flood ที่กำหนดให้ทุกรูปแบบการโจมตีมีค่าแพ็กเก็ตที่ 1448 ไบต์ ซึ่งมีรูปแบบการสื่อสารเครือข่ายภายใน และเครือข่ายภายนอก เพราะการโจมตีนั้นมีได้ทุกสถานที่ที่มีการเชื่อมต่อหากันได้ ส่วนชนิดสื่อกลางของการสื่อสารที่มีการใช้งานได้ทั้งสาย และแบบไร้สาย โดยผลการทดลองการบุกรุกโจมตีแบบ TCP Flood ของเครื่องแม่ข่ายเคอร์เบอร์รอสมีค่าทรัพยากรรวมเฉลี่ยมีความรุนแรงมากที่สุดคิดเป็น 1.46 และ 1.57 เท่าของ UDP Flood และ ICMP Flood ตามลำดับ เพราะการใช้การโจมตีรูปแบบ TCP Flood นั้นทำให้ CPU มีการประมวลผลนานขึ้นเนื่องจากกระบวนการ SYN-ACK ของ TCP Flood ที่มีการส่งแพ็กเก็ตหลายครั้งเป็นจำนวนมาก เมื่อมีการ

ประมวลผลที่ช้าทำให้มีการใช้ RAM เพิ่มขึ้นด้วยเพราะแพ็กเก็ตที่เข้ามาจะถูกเก็บไว้ที่ RAM ก่อนที่ CPU จะทำการอ่านข้อมูลแล้วทำการลบข้อมูลจาก RAM ออกไป ผลการบุกรุกการสื่อสารแบบสายของเครื่องแม่ข่ายเคอร์เบอรอสมีค่าทรัพยากรรวมเฉลี่ยสูงสุดคิดเป็น 1.49 เท่า ของชนิดสื่อกลางการสื่อสารแบบไร้สาย เพราะการเชื่อมต่อแบบสายนั้นมีการรับส่งข้อมูลได้ในเวลาเดียวกันในขณะที่แบบไร้สายจะสลับการรับส่งข้อมูล และมีขนาดแบนด์วิธเพียงกว่าแบบสายถึง 1.8 เท่า ผลการบุกรุกโจมตีรูปแบบการสื่อสายภายในของเครื่องแม่ข่ายเคอร์เบอร์รอสมีค่าทรัพยากรรวมเฉลี่ยสูงกว่าภายนอก 1.08 เท่า เพราะการติดต่อต่างเครือข่ายกันกล่าวคือมีการ ใช้เลขซับเน็ตมาร์ค (Subnet mask) ที่ต่างกันทำให้ไม่สามารถติดต่อหากันได้ แต่ด้วยความสามารถของเราท์เตอร์นั้นมีฟังก์ชันแนทซึ่งเป็นความสามารถแปลงเลขซับเน็ตมาร์คให้มองเห็นกันได้ แต่ทำให้เป็นการรบกวนการทำงานเราท์เตอร์จึงมีโอกาสสูญเสียข้อมูลที่ส่งไปบางส่วน ผลการทดลองการตรวจจับบุกรุกโจมตีแบบ TCP Flood ค่าทรัพยากรรวมเฉลี่ยคิดเป็น 1.02 และ 1.24 เท่า ของ UDP Flood และ ICMP Flood ตามลำดับ เห็นได้ว่าการตรวจจับ TCP Flood และ UDP Flood มีความแตกต่างกันไม่มากเนื่องจากข้อมูลที่แนบมานั้นมีการสุ่มข้อความใหม่อยู่เสมอ แต่ส่วนของ ICMP Flood นั้นมีการสุ่มข้อความในข้อมูลที่ส่งมาน้อยกว่าทำให้การตรวจจับการบุกรุก ICMP Flood มีการใช้ทรัพยากรน้อยที่สุด ผลการทำงานการตรวจจับการบุกรุกของอุปกรณ์ฝังตัวด้วยชนิดสื่อกลางการสื่อสารแบบสายมีค่าทรัพยากรรวมเฉลี่ยมากกว่าแบบไร้สายถึง 2.28 เท่า เนื่องจากการเชื่อมต่อแบบสายนั้นมีการรับส่งข้อมูลได้ในเวลาเดียวกันในขณะที่แบบไร้สายจะสลับการรับส่งข้อมูล โดยข้อมูลที่นำไปตรวจจับนั้นจะขึ้นอยู่กับเครื่องแม่ข่ายเคอร์เบอรอสถูกโจมตีด้วยชนิดสื่อกลางการสื่อสารแบบไหน ผลการทำงานการตรวจจับการบุกรุกของอุปกรณ์ฝังตัวด้วยรูปแบบการสื่อสารภายในมีค่าทรัพยากรรวมเฉลี่ยมากว่าภายนอกถึง 1.16 เท่า เพราะเกิดการสูญเสียข้อมูลที่เครื่องแม่ข่ายเคอร์เบอรอสที่ถูกโจมตีมาจากภายนอกจากการแนทของเราท์เตอร์ ในส่วนผลการทำงานของเครื่องแม่ข่ายเคอร์เบอรอสที่ติดตั้งระบบตรวจจับการบุกรุก มีค่าทรัพยากร CPU และ RAM มากกว่าเครื่องแม่ข่ายเคอร์เบอรอส ที่แยกการติดตั้งระบบตรวจจับการบุกรุกไปยังราสเบอรี่ไพถึง 1.28 และ 1.15 เท่าของเครื่องแม่ข่ายเคอร์เบอรอสที่แยกการติดตั้งระบบตรวจจับการบุกรุกไปยังราสเบอรี่ไพ ทำให้การติดตั้งระบบตรวจจับการบุกรุกลงบนอุปกรณ์ราชเบอรี่ไพช่วยให้ลดค่าทรัพยากรที่ใช้ในเครื่องแม่ข่ายเคอร์เบอรอสที่ติดตั้งระบบตรวจจับการบุกรุกได้ และไม่เป็นการรบกวนการทำงานของเครื่องแม่ข่ายเคอร์เบอรอสในส่วนระบบเครือข่ายนั้นเท่ากัน เพราะมีการเปิดใช้งานแสปนพอร์ตในสวิทช์ทำให้รับข้อมูลเหมือนกับเครื่องแม่ข่ายเคอร์เบอร์รอสทุกประการ โดยจะคัดลอกข้อมูลที่เครื่องแม่ข่ายเคอร์เบอรอสที่รับมาทั้งหมด สุดท้ายนี้ทุกรูปแบบการโจมตีจะไม่มีผลกระทบต่ออุปกรณ์ฝังตัวราสเบอรีไพ และอุปกรณ์ฝังตัวราสเบอรี่ไพสามารถใช้งานอย่างราบรื่นโดยไม่มีปัญหาใด ๆ ทำให้สามารถทำหน้าที่ตรวจจับการบุกรุกให้กับเครื่องแม่ข่ายเคอร์เบอรอสอย่างมีประสิทธิภาพ

เอกสารอ้างอิง

อรรถพล ป้อมสถิตย์. (2562). Enhanced Efficiency of Intrusion Detection Systems with Honey Pot in Cyber Security. **KKU Science journal, 44**(2), 384-397.

อรรถพล ป้อมสถิตย์. (2555). Effective of Unicast and Multicast IP Address Attack Over Intrusion Detection System with Honeypot. ใน**การประชุม Asia-Pacific Advanced Network : APAN ครั้งที่ 33 วันที่ 13-17 กุมภาพันธ์ พ.ศ. 2555**. เชียงใหม่ : ศูนย์การประชุมนานาชาติ โรงแรม ดิ เอ็มเพรส เชียงใหม่.

Auttapon, P. (2015). Performance Analysis of Intrusion Prevention System on Cyber Security for Voice over Internet Protocol (VoIP). **Proceedings of the 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM2015) 21-23 September 2015**(pp.780-784). Shanghai, China.

Auttapon, P. (2012). Effective of Unicast and Multicast IP Address Attack over Intrusion Detection System with Honeypot. **2012 Spring Congress on Engineering and Technology (S-CET)**, 1-4.

Alshami, I.H., Ahmad, N.A. & Sahibuddin, S. (2014). People effects on WLAN-Based IPS' accuracy experimental preliminary results, 2014. In 8th Malaysian Software Engineering Conference (MySEC), pp.206-209.

Arunanto, F.X., Djanali, S., Pratomo, B.A., Baihaqi, A., Studiawan, H. & Shiddiqi, A.M. (2014). Aggressive web application honeypot for exposing attacker's identity. In **International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE)**. (pp.212-216).

Jianrong, Xi. (2015). A Design and Implement of IPS Based on Snort", 2011 Seventh International Conference on Computational Intelligence and Security (CIS), pp. 771-773. Keith Harrison, James R. Rutherford and Gregory B. White., "The Honey Community: Use of Combined Organizational Data for Community Protection", 2015 48th Hawaii International Conference on System Sciences (HICSS), 2015, pp.2288 - 2297.

Muhammet, B. & Resul, D. (2018, August). A novel honeypot based security approach for real-time intrusion detection and prevention systems. **Journal of Information Security and Applications, 41**, 103-166.

Pauna, A. & Bica, I. (2014). RASSH-Reinforced adaptive SSH honeypot. In **10th International Conference on Communications (COMM)**. (pp.1-6.).

Qian, G., Jie, F. & Nige, Li. (2015). The achieve of power manager application honey-pot based on sandbox". In **5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT)**. (pp.2523-2527).

T. Thakur, S. Dogra and Y. Sood. (2015). Replay Attack Prevention by Using a Key with Random Number in Kerberos Authentication protocol. **International Journal of Innovative Research in Science, Engineering and Technology, 4**(7), 5616-5622.