การเพิ่มประสิทธิภาพระบบตรวจจับการบุกรุกในการรักษาความมั่นคงทางไซเบอร์ด้วยฮันนี่พอท

Enhanced Efficiency of Intrusion Detection Systems with Honey Pot in Cyber Security

อรรถพล ป้อมสถิตย์

วิทยาลัยนานาชาติพระนคร มหาวิทยาลัยราชภัฏพระนคร บางเขน กรุงเทพฯ 10220

E-mail: auttapon.p@pnru.ac.th

บทคัดย่อ

งานวิจัยการเพิ่มประสิทธิภาพระบบตรวจจับการบุกรุกในการรักษาความมั่นคงทางไซเบอร์ด้วยฮันนี่พอท นำเสนอการศึกษาการบุกรุกเครือข่ายโดยใช้ฮันนี่พอทในการหลอกล่อ หน่วงเวลา หรือเบี่ยงเบน ผู้บุกรุกไม่ให้โจมตีไปที่เครื่องแม่ข่าย ในการโจมตีรูปแบบการปฏิเสธการมีการให้บริการ 3 รูปแบบได้แก่ TCP Flood, UDP Flood และ ICMP Flood โดยฮันนี่พอทจะใช้โปรแกรม Honeyd ในการจำลองเครื่องคอมพิวเตอร์หรือเครื่องแม่ข่ายให้อยู่ในแผนผังเครือข่ายที่ต้องการจะรักษาความปลอดภัยโดยกำหนดให้ไม่มีการใช้งานไฟร์วอล์และการรักษาความปลอดภัยรูปแบบอื่นๆ ซึ่งจะใช้ระบบป้องกันการบุกรุกและฮันนี่พอทเท่านั้นในการรักษาความปลอดภัยเครือข่าย ส่วนระบบตรวจจับการบุกรุกเครือข่ายจะใช้โปรแกรม Snort โดยโปรแกรมทั้งหมดจะพัฒนาในรูปแบบ Open Source อยู่บนระบบปฏิบัติการ Linux จากผลการทดสอบการโจมตีจากระบบเครือข่ายภายใน และภายนอกของงานวิจัยนี้ทำให้ได้วิธีการเพิ่มประสิทธิภาพระบบตรวจจับการบุกรุกในการรักษาความมั่นคงทางไซเบอร์เมื่อนำฮันนี่พอททำงานร่วมกับระบบตรวจจับการบุกรุก โดยการโจมตีผ่านระบบเครือข่ายแลน มีความเสี่ยงในการถูกโจมตีใกล้เคียงระบบเครือข่ายแลนไร้สาย และการโจมตีแบบ TCP Flood มีอัตราการตรวจจับการบุกรุกได้สูงสุดเมื่อเปรียบเทียบกับการโจมตีแบบ ICMP Flood ที่มีอัตราการตรวจจับการบุกรุกในการโจมตีผ่านระบบเครือข่ายภายในต่างกัน 33.75% และโจมตีผ่านระบบเครือข่ายภายนอกต่างกัน 53.47% นั่นหมายถึงในการรักษาความมั่นคงทางไซเบอร์ จะต้องมีการป้องกันการโจมตีแบบ TCP Flood และการโจมตีจากภายในซึ่งมีอันตรายมากที่สุด

ABSTRACT

This paper presents how Honeypot can help enhancing the efficiency of the Intrusion Detection Systems (IDS) in cyber security. Honeypot will distract, delay, or deviate hackers from attacking the computer network. There are three attacking technique which cause Denial of Service (DOS), delay or deviate: TCP Flood, UDP Flood and ICMP Flood. Honeyd, a part of Honeypot will be used to create a virtual computer or a virtual server within a particular secured network, without firewall or any other forms of security. Only Honeypot will be deployed on the network, while the Snort program will be used on IDS. All programs will be developed as Open Source on Linux OS. As a result of test on the internal and external network attack, we found that we can enhance the efficiency of the Intrusion Detection Systems (IDS) in cyber security by using Honeypot. The attacked rates on LAN network and WLAN network were not much different. However, comparing TCP Flood attack and ICMP Flood attack, TCP Floods attacked rate was 33.75% higher on internal network and 53.47% higher on external network than ICMP Flood attacked rate. In conclusion, TCP Flood attack and all forms of internal attacks are most harmful in cyber security.

คำสำคัญ: ระบบตรวจจับการบุกรุก การปฏิเสธการให้บริการ การรักษาความมั่นคงทางไซเบอร์ ฮันนี่พอท
Keywords: Intrusion Detection System, Denial of Service, CyberSecurity, Honeypot

1. บทนำ

ในปัจจุบันเทคโนโลยีด้านการรักษาความมั่นคงทางไซเบอร์ได้ก้าวไปข้างหน้าอย่างรวดเร็ว ซอฟต์แวร์และฮาร์ดแวร์ต่างๆ ที่เกี่ยวข้องกับความปลอดภัยด้านสารสนเทศได้ถูกวิจัยและพัฒนาขึ้นเพื่อตอบสนองความต้องการของผู้ใช้มากขึ้น ซึ่งระบบตรวจจับการบุกรุก (Intrusion Detection System: IDS) หรือระบบตรวจจับการบุกรุกเป็นเครื่องมือที่ใช้สำหรับตรวจจับความพยายามบุกรุกเครือข่ายโดยระบบจะแจ้งเตือนไปยังผู้ดูแลระบบเมื่อมีการบุกรุกหรือมีการพยายามที่จะบุกรุกเครือข่าย โดยระบบจะรายงานเฉพาะสิ่งที่กำหนดให้รายงานเท่านั้น ซึ่งมีอยู่สองสิ่งที่ผู้ดูแลระบบจะต้องกำหนดค่าให้กับ ระบบตรวจจับการบุกรุกสิ่งแรกคือ Signature ของการบุกรุก สิ่งที่สองคือเหตุการณ์ที่ผู้ดูแลระบบให้ความสำคัญหรือเหตุการณ์ที่คาดว่าจะเป็นผลไปสู่การบุกรุกในภายหน้า ซึ่งเหตุการณ์ต่างๆเหล่านี้อาจเป็นสัญญาณจราจรที่ไม่ปกติหรืออาจเป็นบางข้อความใน log การกำหนดค่า Signature ให้กับระบบตรวจจับการบุกรุกของแต่ละองค์กรนั้นอาจจะไม่เหมือนกัน ซึ่งจะขึ้นอยู่กับว่าองค์กรนั้นจะให้ความสนใจกับการบุกรุกประเภทใด และในการตรวจสอบลักษณะข้อมูลของผู้ใช้ที่เข้ามาใช้บริการในระบบโดยระบบจะมีตัวคัดกรองความถูกต้องหรือต้องสงสัย ถ้าเกิดลักษณะการเรียกใช้ข้อมูลของผู้ใช้บริการเกิดผิดปกติหรือต้องสงสัย ระบบตรวจจับการบุกรุกจะทำการตรวจจับข้อมูลดังกล่าวและทำการแจ้งเตือนในรูปแบบสถิติในการโจมตี (อรรถพล ป้อมสถิตย์, 2554)

นอกจากนี้การโจมตีในระบบเครือข่ายได้มีการพัฒนารูปแบบการโจมตีขึ้นอย่างรวดเร็วดังนั้น ฮันนี่พอท (Honeypot) (Pomsathit A., 2012) จึงเป็นระบบความปลอดภัยอีกชนิดหนึ่งที่เสริมการทำงานของระบบตรวจจับการบุกรุกได้เป็นอย่างดี ซึ่งฮันนี่พอทก็คือคอมพิวเตอร์หรือกลุ่มของคอมพิวเตอร์ที่ถูกติดตั้งไว้สำหรับล่อลวงให้ผู้บุกรุกทำการโจมตี และเพื่อเรียนรู้เทคนิคที่ผู้บุกรุกใช้และนำความรู้เหล่านั้นมาใช้ในการหาทางป้องกันการโจมตีใหม่ๆที่เกิดขึ้น อีกทั้งฮันนี่พอทยังสามารถใช้ลดความเสี่ยงของเครื่องแม่ข่ายในระบบที่อาจถูกโจมตีหรือใช้เป็นระบบตรวจสอบการบุกรุกได้อีกทางหนึ่งด้วย โดยปกติแล้วฮันนี่พอทจะถูกติดตั้งในเครือข่ายที่แยกจากเครือข่ายที่ใช้งานจริง หรือติดตั้งในบริเวณเดียวกับเครื่องแม่ข่ายเพื่อป้องกันไม่ให้เครื่องแม่ข่ายที่ใช้งานเครือข่ายภายในถูกโจมตีได้ง่ายจากผู้บุกรุกซึ่งแม้ว่าจะมีการป้องการอย่างดีจากอุปกรณ์รักษาความปลอดภัยเครือข่าย อาทิ ไฟล์วอล หรือโปรแกรมป้องกันไวรัสต่างๆ

ในงานวิจัยนี้ได้ใช้ฮันนี่พอทชนิด Low-Interaction Honeypot ซึ่งจะมีการตอบสนองต่อการโจมตีในแบบการปฏิเสธการให้บริการ (Denial of Service : DoS) (Zhenxin Z., Maochao X. and Shouhuai X., 2013) ของผู้บุกรุกตามข้อมูลของฮันนี่พอทที่กำหนดไว้ ซึ่งโดยปกติมักจะกำหนดให้ผู้บุกรุกสามารถใช้งานฮันนี่พอทได้อย่างจำกัด หลังจากที่ผู้บุกรุกเข้าไปได้แล้ว ฮันนี่พอทจะให้ข้อมูลเกี่ยวกับการโจมตีของผู้บุกรุก โดยใช้ซอฟต์แวร์ Honeyd ทำการจำลอง Services ต่างๆที่คาดว่าผู้บุกรุกจะทำการโจมตีเช่น HTTP (หมายเลขพอร์ต 80), SSH (หมายเลขพอร์ต 22) หรือ SMTP (หมายเลขพอร์ต 25) เป็นต้น ดังนั้นเพื่อเป็นการป้องกันหรือลดช่องทางในการกระทำความผิดตามที่ได้กล่าวมาข้างต้น ผู้วิจัยจึงมีแนวคิดในการทำวิจัยเพิ่มประสิทธิภาพระบบตรวจจับการบุกรุกในการรักษาความมั่นคงทางไซเบอร์ด้วยฮันนี่พอท เพื่อป้องกันการโจมตีจากผู้บุกรุกในการระงับ ชะลอ ขัดขวาง หรือรบกวนจนเครื่องแม่ข่ายไม่สามารถทำงานตามปกติได้ โดยผลลัพธ์ที่ได้จากการวิจัยจะสามารถนำมาใช้ในปรับปรุงและพัฒนาการดำเนินงานของผู้ดูแลระบบเครือข่ายของมหาวิทยาลัย หน่วยงานภาครัฐและภาคเอกชน เพื่อนำไปสู่ความมั่นคงของระบบคอมพิวเตอร์ตามวัตถุประสงค์ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี 2550

2. วิธีการดำเนินการวิจัย

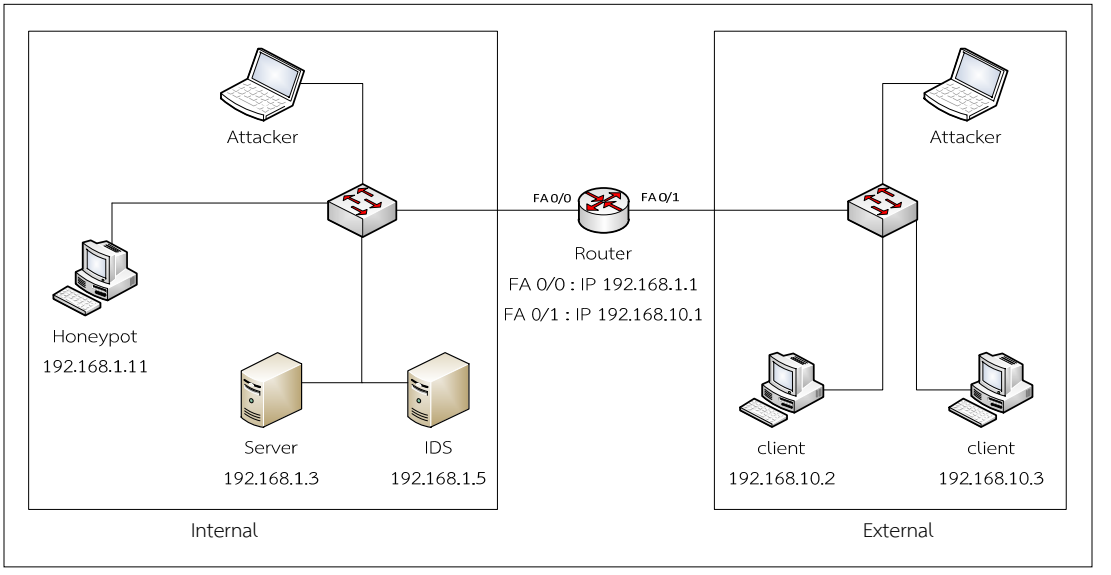
2.1 ออกแบบผังเครือข่าย

ในการออกแบบผังเครือข่ายนั้นได้ออกแบบให้ผังเครือข่ายมีความใกล้เคียงกับระบบที่มีการใช้จริงกับหน่วยงานของภาครัฐและเอกชนเพื่อให้สามารถนำไปประยุกต์ใช้ได้จริง อันประกอบด้วย

1. ระบบเครือข่ายภายใน (internal) เป็นการระบบเครือข่ายภายในองค์กรที่สมมติให้การทดลองไม่มีการป้องกันจากอุปกรณ์รักษาความปลอดภัยทางคอมพิวเตอร์ ต่างๆ อาทิ ACLของอุปกรณ์ และไฟล์วอล โดยจะมีการติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย และระบบตรวจจับการบุกรุกเป็นองค์ประกอบหลักโดยเชื่อมต่ออุปกรณ์ทั้งหมดผ่านอุปกรณ์สวิตช์

2. ระบบเครือข่ายภายนอก (External) เป็นระบบเครือข่ายที่อยู่ภายนอกองค์กรหรืออาจสมมติว่าเป็นเครือข่ายอินเทอร์เน็ต โดยจะมีการติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลเป็นองค์ประกอบหลักโดยเชื่อมต่ออุปกรณ์ทั้งหมดผ่านอุปกรณ์สวิตช์ โดยทั้งส่วนระบบเครือข่ายภายในและระบบเครือข่ายภายนอกจะเชื่อมต่อผ่านอุปกรณ์เราท์เตอร์ ทั้งนี้แผนผังเครือข่าย

รวมจะคำนึงถึงจำนวนอุปกรณ์ที่มีอยู่จริงของห้องปฏิบัติการ Network Security โดยมีรายละเอียดการออกแบบผังเครือข่ายทั้งหมดดังรูปที่ 1



รูปที่ 1 แสดงผังเครือข่าย

2.1.1. การติดตั้งและกำหนดค่าอุปกรณ์เครือข่ายต่างๆ ดังต่อไปนี้

1. กำหนดค่าอุปกรณ์เราท์เตอร์ให้สามารถใช้คุณสมบัติ DHCP Pool และคุณสมบัติ เราท์เตอร์ RIP ได้

2. การกำหนดค่าอุปกรณ์สวิตช์ให้สามารถทำการ Spanning Port คือ การที่สวิตช์จะส่งต่อทุกๆ แพ็กเก็ตที่รับจากพอร์ตหนึ่งไปยังอีกพอร์ตหนึ่ง และการกำหนดค่า Port mirror ให้กับสวิตช์ซึ่งเป็นเทคโนโลยีที่เป็นประโยชน์และถูกนำมาใช้อย่างมากในการตรวจสอบและเก็บสถิติต่างๆในการรับ-ส่งข้อมูลของพอร์ตหนึ่งบนอุปกรณ์ดังกล่าว

2.1.2. การติดตั้งโปรแกรมที่ใช้ในการทดลอง

1. โปรแกรมที่ใช้ในการโจมตี ประกอบด้วย

1.1 โปรแกรม Nessus สำหรับการค้นหาช่องโหว่ของเครือข่าย โดยความสามารถคือจะค้นหาเครื่องคอมพิวเตอร์ในเครือข่ายแล้วจะรายงานช่องโหว่ของคอมพิวเตอร์แต่ละเครื่อง

1.2 โปรแกรม SuperScan โปรแกรมสำหรับใช้ในการค้นหาพอร์ต TCP ping resolver โดยจะทำงานในแบบ connect-based ใช้เทคนิคแบบ Multithreaded และ asynchronous ซึ่งทำให้การทำงานมีความเร็วมากและใช้งานได้ในหลายแบบ

2. ระบบปฏิบัติการ Linux มีความสามารถในการรองรับการทำงานร่วมกันโปรแกรมอื่นๆ ได้เป็นอย่างดี

3. โปรแกรม Snort เป็นโปรแกรมรักษาระบบความปลอดภัยทางเครือข่ายที่มีผู้พัฒนาอย่างต่อเนื่องจากทั่วโลกเรื่อยมาจนถึงปัจจุบัน ซึ่งในการวิจัยนี้ได้เลือกใช้ระบบจับการบุกรุก ชนิดระบบตรวจหาการบุกรุกบนเครื่องคอมพิวเตอร์ (Host-based IDS) (Jianrong Xi., 2011) ซึ่งจะทำงานในเครื่องคอมพิวเตอร์ด้วยการติดตามตรวจสอบสัญญาณจราจร

ที่อยู่ในรูปของแพ็กเก็ตข้อมูลและตรวจสอบการใช้งานโปรแกรมประยุกต์ (Application) ในเครื่องคอมพิวเตอร์จากไฟล์บันทึกข้อมูลการใช้งานการจราจรเครือข่ายเพื่อตรวจสอบว่าแพ็กเก็ตใดมีลักษณะที่ผิดปกติ

3.1 การกำหนดค่า Rule ของโปรแกรม Snort

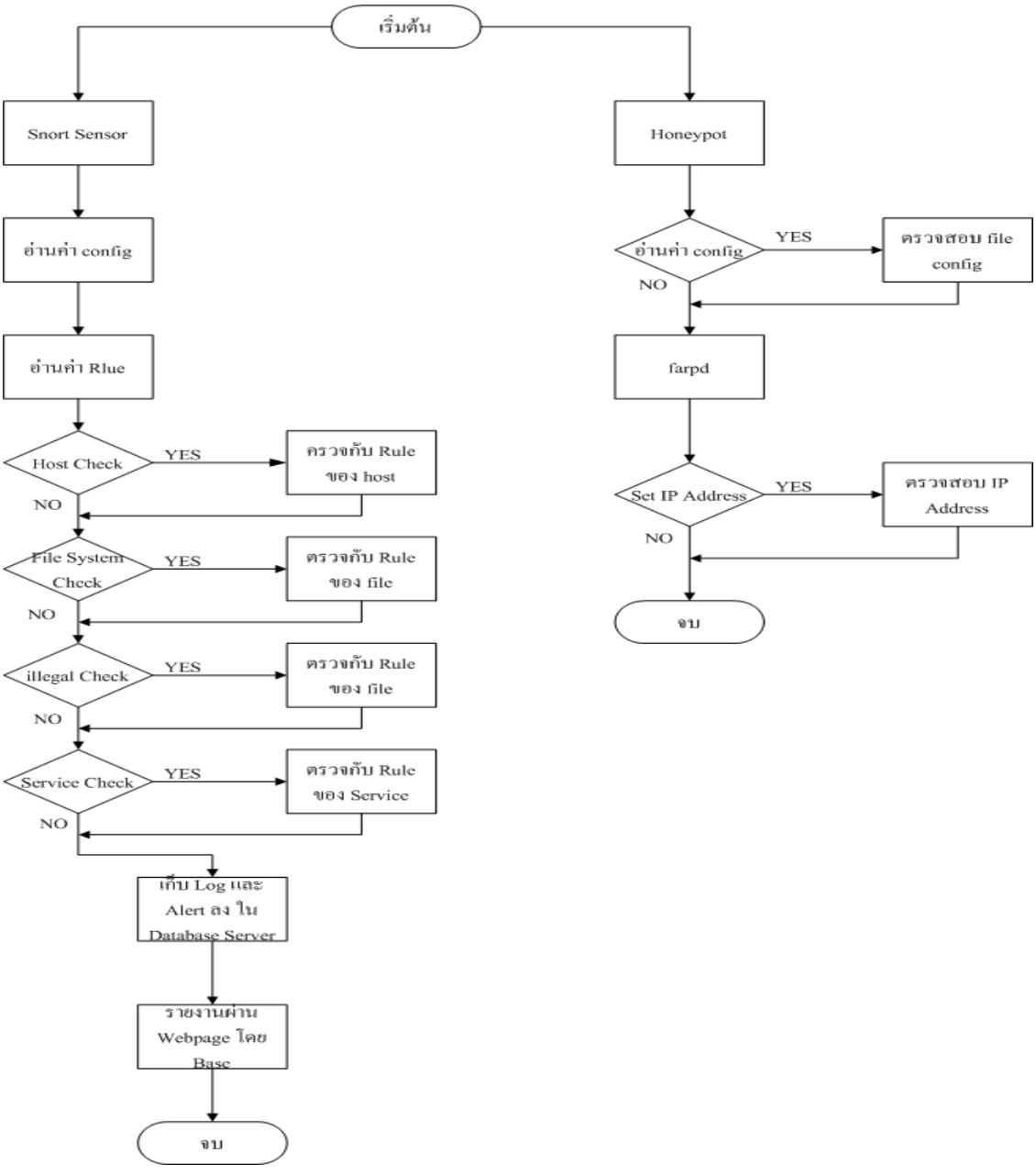
Rule นั้นก็คือกฎหรือข้อบังคับในการตรวจจับรูปแบบการโจมตีหรือ แพ็คเก็ต ที่โปรแกรมตรวจจับได้ โดยทำการตั้งค่าและปรับแต่งค่า Rule ของโปรแกรม Snort เอง เพราะค่า Rule ปกติที่โปรแกรมตั้งค่าให้นั้นเป็นค่า Rule ที่วิเคราะห์รูปแบบการโจมตีแบบธรรมดา ซึ่งตัวโปรแกรมจะไม่เปิดการใช้งาน Rule ทั้งหมด ตัวโปรแกรมจะใช้งาน Rule บางส่วนที่เป็นรูปแบบการโจมตีที่มีผลรุนแรงเท่านั้น ทำให้ในการศึกษาและวิจัยนั้นไม่สามารถเปรียบเทียบค่าประสิทธิภาพที่สูงสุดในการตรวจจับการโจมตีของโปรแกรมได้ ดังนั้นจึงทำการตั้งค่า Rule โดยทำการแก้ไข ปรับแต่งและตั้งค่าในไฟล์ snort.conf ของโปรแกรม โดยทำการเปิดใช้งาน Rule ทั้งหมดที่โปรแกรมสามารถตรวจจับได้ และทำการ Update ค่าของ Rule ให้เป็นเวอร์ชั่นล่าสุด (version.2.9) ดังที่แสดงไว้ในรูปที่ 2

4. ฮันนี่พอท

Honeyd เป็นซอฟต์แวร์ที่ใช้ในการหลอกล่อผู้ที่เข้ามาโจมตี โดยที่ซอฟต์แวร์ตัวนี้ได้มีการใช้กันอย่างแพร่หลายจึงมีการพัฒนาอย่างต่อเนื่องจนมาถึงปัจจุบันทำให้ตัวโปรแกรมเป็นที่ยอมรับและได้มาตรฐาน Honeyd (Pauna A and Bica I., 2014) สนับสนุนคุณลักษณะที่หลากหลายที่ทำให้มีความยืดหยุ่นให้กับการสร้าง host และเครือข่ายเสมือนแบบ ฮันนี่พอท

4.1 แสดงขั้นตอนการทำงานของโปรแกรม Snort และโปรแกรม Honeyd

จากแผนผังการทำงานของระบบตรวจจับการบุกรุกเครือข่ายและฮันนี่พอทจะมีขั้นตอนการทำงานดังที่ได้แสดงไว้ในรูปที่ 2 ซึ่งจะทำงานเริ่มจากที่ Sensor หนึ่งตัวหรือมากกว่านั้น (ขึ้นอยู่กับการออกแบบของแต่ละองค์กร) อ่านค่ากำหนดค่าตามที่ผู้ติดตั้งหรือผู้ดูแลระบบได้กำหนดค่าไว้ แล้วโปรแกรมจะทำการอ่านค่าของ Rule ต่างๆ ที่ได้ทำการตั้งค่าไว้ เมื่อระบบอ่านค่าต่างๆ จะทำการตรวจจับและวิเคราะห์การจราจรเครือข่ายของแพ็กเก็ตต่างๆ เปรียบเทียบกับ Rule ของโปรแกรมตามที่ตั้งค่าไว้และวิเคราะห์รูปแบบการถูกโจมตีรูปแบบต่างๆ ว่าเป็นโจมตีนั้นเป็นชนิดใดและมีจำนวนหรือมีระดับความเสี่ยงต่อระบบมากน้อยเพียงใด และเก็บข้อมูลเหตุการณ์หรือ Log ลงฐานข้อมูล ซึ่งข้อมูลหรือ Log ที่เกิดขึ้นของ Sensor ที่มีอยู่แต่ละตัวจะมาเก็บลงในฐานข้อมูลที่เครื่องแม่ข่ายตัวเดียวกัน ต่อมาในการแสดงผลการตรวจจับนั้น จะแสดงออกมาที่หน้าเว็บที่ดึงจากข้อมูลในฐานข้อมูลมาแสดงเพื่อความสะดวกในการให้ผู้ดูแลระบบได้จัดการหรือป้องกันระบบได้อย่างมีประสิทธิภาพ ส่วนโปรแกรม Honeyd นั้นก็จะเริ่มจากการกำหนดค่าตามที่ผู้ดูแลระบบได้กำหนดค่าไว้ ต่อจากนั้นจะทำการอ่านค่าที่ไฟล์ honeyd.conf และเปิดโปรแกรม farpd แล้วทำการตั้งค่า IP Address ตามที่ต้องการจำลองแบบให้มีเครื่องแม่ข่าย (Keith Harrison, James R. Rutherford and Gregory B. White., 2015)



รูปที่ 2 แสดงการทำงานของระบบตรวจจับการบุกรุกและฮันนี่พอท

3. ผลการวิจัย (Results)

การวิเคราะห์ประสิทธิภาพการโจมตีด้วยฮันนี่พอท จากการดำเนินงานได้แบ่งการทดลองออกเป็น 2 การทดลองคือ

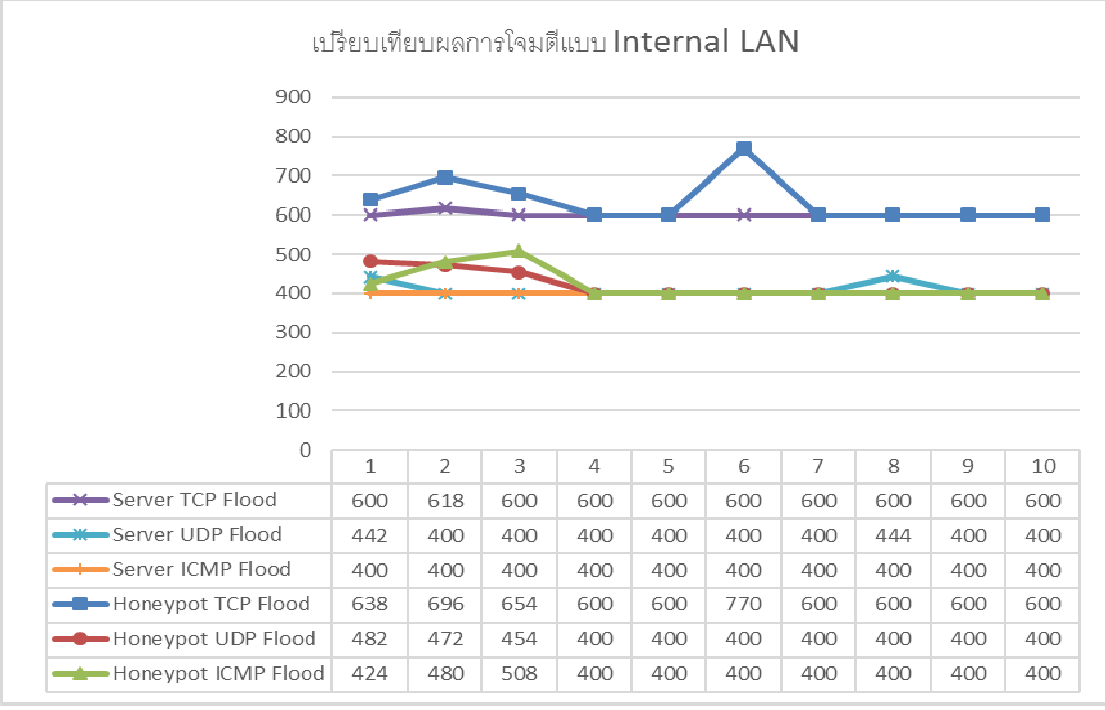
1. การโจมตีเครื่องแม่ข่าย และฮันนี่พอทจากภายใน (Internal)

2. การโจมตีเครื่องแม่ข่าย และฮันนี่พอทจากจากภายนอก (External)

เพื่อที่จะให้ทราบถึงประสิทธิภาพการทำงานของฮันนี่พอท และความแตกต่างระหว่างการโจมตีผ่านระบบเครือข่ายแลนและการโจมตีผ่านระบบเครือข่ายแลนไร้สาย เพื่อวิเคราะห์ประสิทธิภาพการตรวจจับการบุกรุกที่มีประสิทธิภาพมากที่สุด ซึ่งในการทดลองนี้จะใช้การโจมตีแบบปฏิเสธการให้บริการโดยแบ่งการโจมตีออกเป็น 3 ประเภท ได้แก่ TCP Flood, UDP Flood และ ICMP Flood ซึ่งทำการทดสอบประสิทธิภาพด้วยการใช้ระบบตรวจจับการบุกรุกเพื่อเก็บข้อมูลการบุกรุกที่เกิดขึ้นทั้งในเครื่องแม่ข่าย และฮันนี่พอท โดยผลการทดลองจะเปรียบเทียบจำนวนเหตุการณ์ที่ระบบตรวจจับการบุกรุกซึ่งสามารถจับได้ระหว่างการโจมตีผ่านระบบแลน และการโจมตีผ่านระบบเครือข่ายแบบแลนไร้สาย ที่มีการโจมตีจากภายในและภายนอกโดยมีเราท์เตอร์ทำหน้าที่แบ่งพื้นที่ระบบเครือข่ายภายในและภายนอกดังที่ได้แสดงไว้ในรูปที่ 1 ซึ่งการดำเนินการตามขั้นตอนการทดลองได้ทำการรวบรวมข้อมูลจากผลการดำเนินงานหาค่าเฉลี่ย และแสดงอยู่ในรูปของกราฟเพื่อให้ง่ายต่อการวิเคราะห์ข้อมูลโดยในทุกรูปของผลการทดลองแกน x จะแสดงถึงจำนวนครั้งในการแจ้งเตือนการโจมตีซึ่งเป็นผลที่ได้จากระบบตรวจจับการบุกรุก ส่วนแกน y จะแสดงถึงจำนวนครั้งในการทดลองโจมตีระบบในระยะเวลาเท่าๆกัน คือ 30 วินาที โดยมีการส่งแพ็กเก็ตในการโจมตีจำนวน 1,000 แพ็กเก็ต

3.1 เปรียบเทียบการโจมตีเครื่องแม่ข่ายและฮันนี่พอทแบบแลนจากภายในเครือข่าย

การเปรียบเทียบผลการโจมตีจากภายในเครือข่ายแลนโดยทำการเปรียบเทียบจากรูปแบบการโจมตีประเภทปฏิเสธการให้บริการ ที่มีการควบคุมจำนวนการโจมตีให้เท่ากันทุกรูปแบบแล้วบันทึกผลการทดลองเป็นเหตุการณ์ที่เกิดขึ้นในแต่ละอุปกรณ์จะเห็นได้ว่า เหตุการณ์ส่วนมากจะเกิดขึ้นจากการโจมตีที่โพรโทคอล TCP โดยใช้รูปแบบการโจมตีคือ TCP Flood ทั้งนี้เนื่องจากโพรโทคอล TCP เป็นโพรโทคอลหลักที่ใช้ในการเชื่อมต่อระหว่างเครื่องแม่ข่ายผู้ให้บริการกับผู้ใช้บริการอยู่แล้ว และในการทดลองที่โพรโทคอล TCP จะเห็นได้ว่าเกิดเหตุการณ์ที่ฮันนี่พอทมากกว่าเครื่องแม่ข่ายในรูปแบบการโจมตีเดียวกัน เป็นจำนวนประมาณ 34 เหตุการณ์หรือประมาณ 5.35 % ในส่วนของการโจมตีในรูปแบบ UDP Flood ที่โพรโทคอล UDP จากผลการทดลองจะได้ค่าเฉลี่ยผลการทดลองที่ฮันนี่พอทมากกว่าเครื่องแม่ข่ายประมาณ 1.91 % และการโจมตีรูปแบบ ICMP Flood มีเหตุการณ์เกิดขึ้นที่ฮันนี่พอทมากกว่าเครื่องแม่ข่ายประมาณ 3.34% ดังที่ได้แสดงไว้ในรูปที่ 3

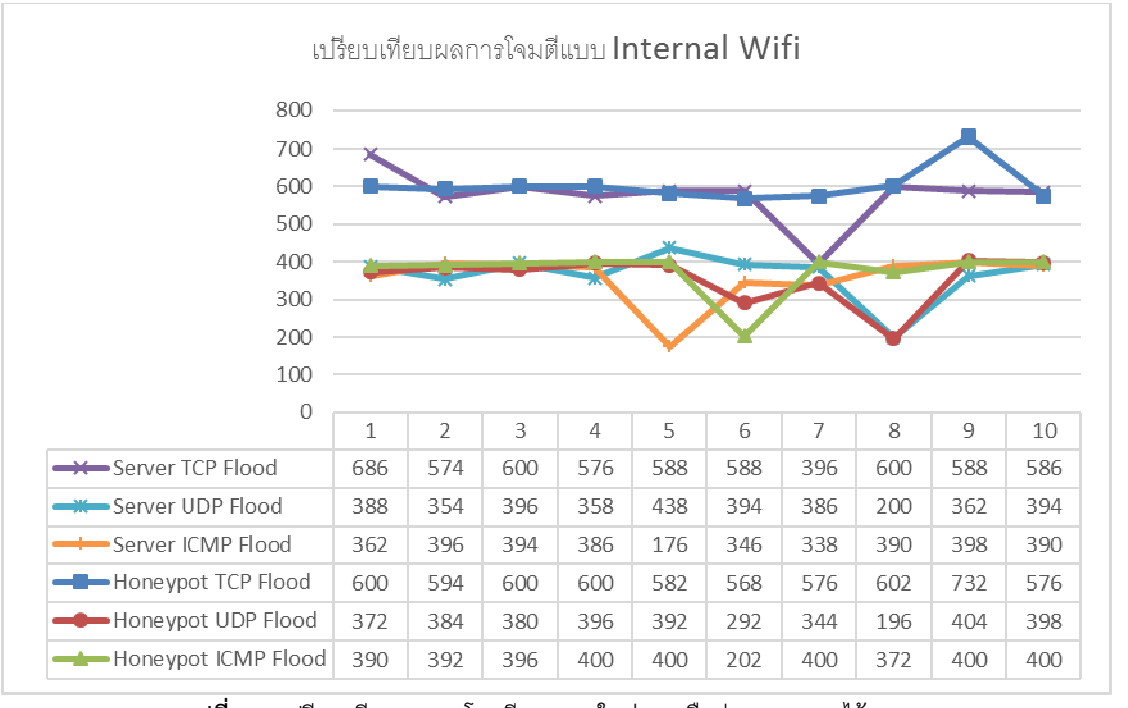


	1	2	3	4	5	6	7	8	9	10
Server TCP Flood	600	618	600	600	600	600	600	600	600	600
Server UDP Flood	442	400	400	400	400	400	400	444	400	400
Server ICMP Flood	400	400	400	400	400	400	400	400	400	400
Honeypot TCP Flood	638	696	654	600	600	770	600	600	600	600
Honeypot UDP Flood	482	472	454	400	400	400	400	400	400	400
Honeypot ICMP Flood	424	480	508	400	400	400	400	400	400	400

รูปที่ 3 เปรียบเทียบผลการโจมตีจากภายในผ่านเครือข่ายแลน

3.2 เปรียบเทียบการโจมตีเครื่องแม่ข่ายและฮันนี่พอทแบบแลนไร้สายจากภายในเครือข่าย

การเปรียบเทียบผลการโจมตีจากภายในเครือข่ายแลนไร้สายโดยทำการเปรียบเทียบจากรูปแบบการโจมตีประเภทปฏิเสธการให้บริการ โดยควบคุมจำนวนการโจมตีให้เท่ากันทุกรูปแบบแล้วบันทึกผลการทดลองเป็นเหตุการณ์ที่เกิดขึ้นในแต่ละอุปกรณ์จะเห็นได้ว่า เกิดเหตุการณ์มากที่สุดที่การโจมตีฮันนี่พอทแบบ TCP Flood ส่วนรองลงมาเป็นการโจมตีแบบ TCP Flood ที่เครื่องแม่ข่าย ซึ่งมีค่าใกล้เคียงกับผลการทดลองตามรูปที่ 3 การโจมตีเครื่องแม่ข่าย และฮันนี่พอทแบบแลนจากภายในเครือข่ายดังที่แสดงไว้ในรูปที่ 4



	1	2	3	4	5	6	7	8	9	10
Server TCP Flood	686	574	600	576	588	588	396	600	588	586
Server UDP Flood	388	354	396	358	438	394	386	200	362	394
Server ICMP Flood	362	396	394	386	176	346	338	390	398	390
Honeypot TCP Flood	600	594	600	600	582	568	576	602	732	576
Honeypot UDP Flood	372	384	380	396	392	292	344	196	404	398
Honeypot ICMP Flood	390	392	396	400	400	202	400	372	400	400

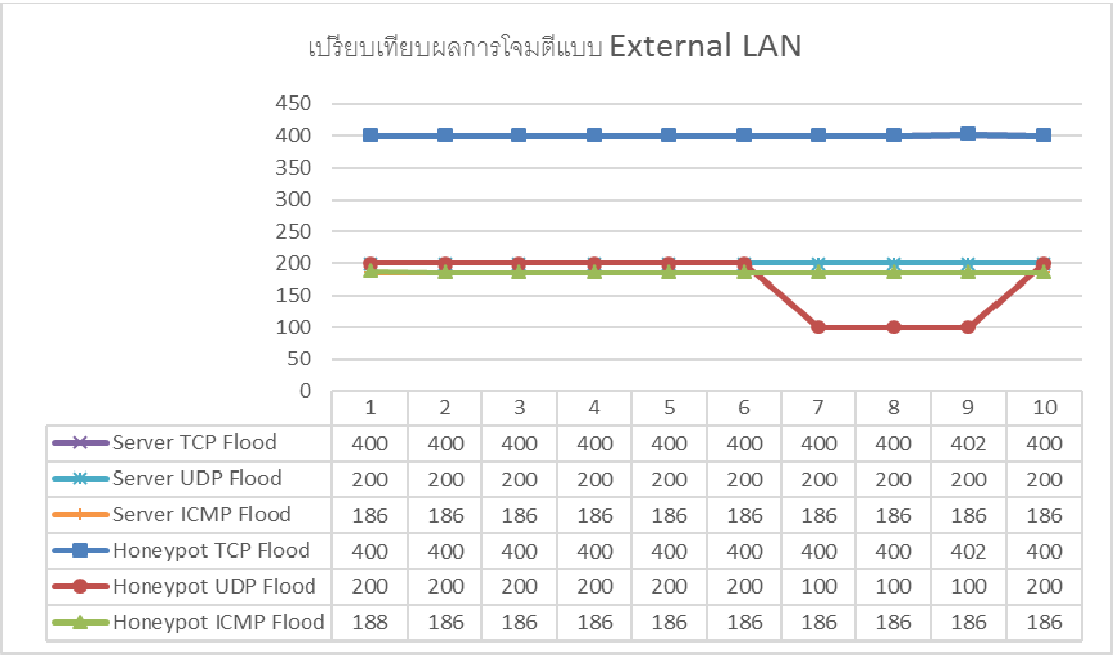
รูปที่ 4 เปรียบเทียบผลการโจมตีจากภายในผ่านเครือข่ายแบบแลนไร้สาย

3.3 เปรียบเทียบการโจมตีเครื่องแม่ข่ายและฮันนี่พอท แบบแลน จากภายนอกเครือข่าย

การเปรียบเทียบผลการโจมตีจากภายนอกเครือข่ายโดยทำการเปรียบเทียบจากรูปแบบการโจมตีประเภทปฏิเสธการให้บริการ โดยควบคุมจำนวนการโจมตีให้เท่ากันทุกรูปแบบแล้วบันทึกผลการทดลองเป็นเหตุการณ์ที่เกิดขึ้นในแต่ละอุปกรณ์จะเห็นได้ว่าในการทดลองที่โพรโทคอล TCP โดยรูปแบบการโจมตีคือ TCP Flood จะเห็นได้ว่าฮันนี่พอทและเครื่องแม่ข่ายมีค่าเฉลี่ยการเกิดเหตุการณ์ที่เท่ากัน ในส่วนของการทดลองที่โพรโทคอล UDP โดยรูปแบบการโจมตีคือ UDP Flood จะเห็นได้ว่าเหตุการณ์ที่เกิดในโพรโทคอล UDP มีจำนวนน้อยกว่า TCP ทั้งฮันนี่พอทและเครื่องแม่ข่าย โดยฮันนี่พอทมีค่าเฉลี่ยเหตุการณ์ที่โพรโทคอล UDP น้อยกว่าเครื่องแม่ข่ายในโพรโทคอลเดียวกันอยู่ประมาณ 7.52 % ส่วนในการทดลองรูปแบบ ICMP Flood จะเห็นได้ว่าฮันนี่พอทและเครื่องแม่ข่ายมีค่าเฉลี่ยเหตุการณ์ที่ใกล้เคียงกันอย่างมากโดยต่างกันเพียง 0.2 เหตุการณ์หรือเท่ากับ 0.05 % ดังที่ได้แสดงไว้ในรูปที่ 5

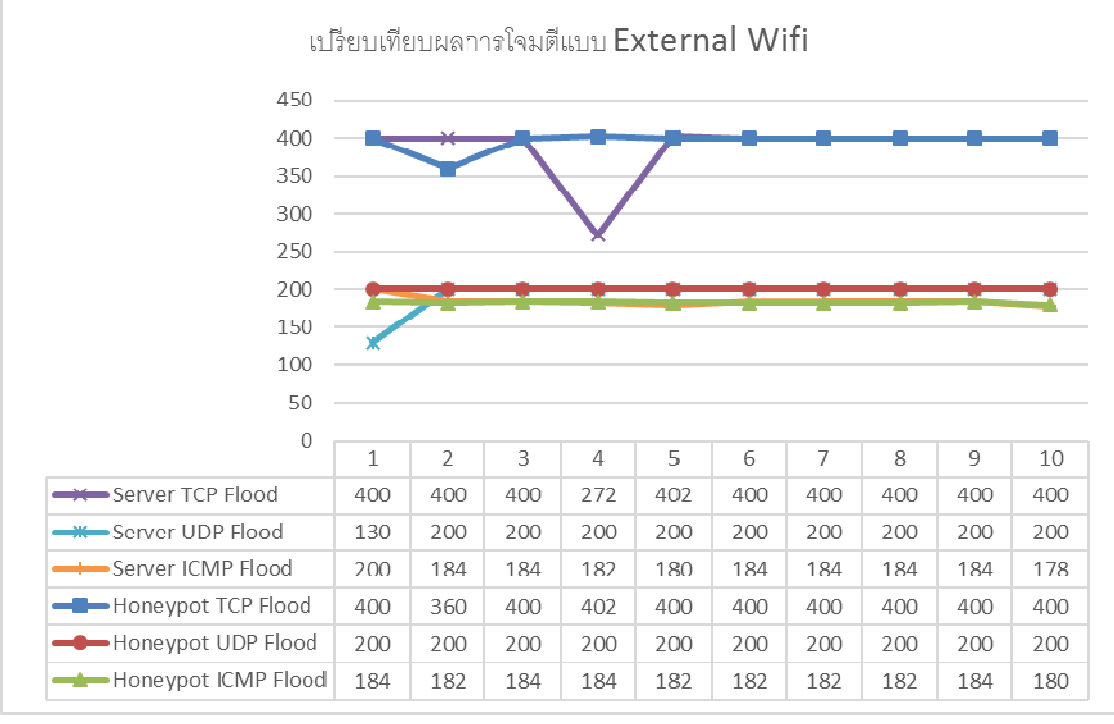
3.4 เปรียบเทียบการโจมตีเครื่องแม่ข่ายและฮันนี่พอท แบบแลนไร้สายจากภายนอกเครือข่าย

การเปรียบเทียบผลการโจมตีจากภายนอกเครือข่ายแบบไร้สายทำการเปรียบเทียบจากรูปแบบการโจมตีประเภทปฏิเสธการให้บริการ โดยควบคุมจำนวนการโจมตีให้เท่ากันทุกรูปแบบแล้วบันทึกผลการทดลองเป็นเหตุการณ์ที่เกิดขึ้นในแต่ละอุปกรณ์จะเห็นได้ว่าในการทดลองที่โพรโทคอล TCP โดยรูปแบบการโจมตีคือ TCP Flood จะเห็นได้ว่าเกิดเหตุการณ์ที่ฮันนี่พอทมากที่สุด ดังที่ได้แสดงไว้ในรูปที่ 6 และในส่วนของการโจมตีเครื่องแม่ข่ายแบบ TCP Flood ครั้งที่ 4 มีผลการทดลองแตกต่างค่อนข้างมากเกิดจากการรับส่งสัญญาณไร้สาย ณ ช่วงเวลาเกิดการขัดข้อง



	1	2	3	4	5	6	7	8	9	10
Server TCP Flood	400	400	400	400	400	400	400	400	402	400
Server UDP Flood	200	200	200	200	200	200	200	200	200	200
Server ICMP Flood	186	186	186	186	186	186	186	186	186	186
Honeypot TCP Flood	400	400	400	400	400	400	400	400	402	400
Honeypot UDP Flood	200	200	200	200	200	200	100	100	100	200
Honeypot ICMP Flood	188	186	186	186	186	186	186	186	186	186

รูปที่ 5 เปรียบเทียบผลการโจมตีจากภายนอกผ่านเครือข่ายแลน



	1	2	3	4	5	6	7	8	9	10
Server TCP Flood	400	400	400	272	402	400	400	400	400	400
Server UDP Flood	130	200	200	200	200	200	200	200	200	200
Server ICMP Flood	200	184	184	182	180	184	184	184	184	178
Honeypot TCP Flood	400	360	400	402	400	400	400	400	400	400
Honeypot UDP Flood	200	200	200	200	200	200	200	200	200	200
Honeypot ICMP Flood	184	182	184	184	182	182	182	182	184	180

รูปที่ 6 เปรียบเทียบผลการโจมตีจากภายนอกผ่านเครือข่ายแบบแลนไร้สาย

4. วิเคราะห์ผลการวิจัย

4.1. ผลการทดลองเปรียบเทียบการโจมตีภายในเครือข่าย

การเปรียบเทียบการโจมตีเครื่องแม่ข่ายและฮันนี่พอททั้งแบบแลน และแบบแลนไร้สายจากภายในเครือข่าย โดยระบบเครือข่ายแลน มีความเสี่ยงในการถูกโจมตีใกล้เคียงระบบเครือข่ายแลนไร้สาย และการโจมตีแบบ TCP Flood มีอัตราการตรวจจับที่สูงที่สุดในทุกการทดลอง โดยเฉพาะอย่างยิ่งการตรวจจับการบุกรุกเมื่อมีการใช้ฮันนี่พอทในระบบแลนมีค่าเฉลี่ยการตรวจจับประมาณ 635.8 แพ็กเก็ต ซึ่งเป็นค่าสูงสุด เมื่อเปรียบเทียบกับการโจมตีแบบ ICMP Flood ที่มีอัตราการตรวจจับการบุกรุกน้อยที่สุดในเกือบทุกการทดลอง โดยการใช้ฮันนี่พอทในระบบแลนมีค่าเฉลี่ยการตรวจจับประมาณ 421.2 แพ็กแก็ต ซึ่งต่างกันถึง 33.75% และที่สำคัญจะเห็นได้ว่าฮันนี่พอทมีจำนวนการตรวจจับได้มากกว่ากรณีไม่มีฮันนี่พอทในแทบทุกการทดลองแม้เฉลี่ยต่างกันไม่เกินประมาณ 8% นั้นเป็นการยืนยันได้ว่าฮันนี่พอทสามารถช่วยหลอกล่อผู้ประสงค์ร้ายในการโจมตีเครื่องแม่ข่ายได้อย่างมีประสิทธิภาพ ดังที่ได้แสดงไว้ในตารางที่ 1

ตารางที่ 1 เปรียบเทียบผลการโจมตีแบบภายในเครือข่าย

Internal Attack

Attack		Time										Average	
		1	2	3	4	5	6	7	8	9	10	Total	(%)
Server (LAN)	TCP Flood	600	618	600	600	600	600	600	600	600	600	601.8	94.65
	UDP Flood	442	400	400	400	400	400	400	444	400	400	408.6	64.27
	ICMP Flood	400	400	400	400	400	400	400	400	400	400	400	62.91
Honeypot (LAN)	TCP Flood	638	696	654	600	600	770	600	600	600	600	635.8	100
	UDP Flood	482	472	454	400	400	400	400	400	400	400	420.8	66.18
	ICMP Flood	424	480	508	400	400	400	400	400	400	400	421.2	66.25
Server (Wifi)	TCP Flood	686	574	600	576	588	588	396	600	588	586	578.2	90.94
	UDP Flood	388	354	396	358	438	394	386	200	362	394	367	57.72
	ICMP Flood	362	396	394	386	176	346	338	390	398	390	357.6	56.24
Honeypot (Wifi)	TCP Flood	600	594	600	600	582	568	576	602	732	576	603	94.84
	UDP Flood	372	384	380	396	392	292	344	196	404	398	355.8	55.96
	ICMP Flood	390	392	396	400	400	202	400	372	400	400	375.2	59.01

4.2. ผลการทดลองเปรียบเทียบการโจมตีภายนอกเครือข่าย

การเปรียบเทียบการโจมตีเครื่องแม่ข่ายและฮันนี่พอททั้งแบบแลนและแบบแลนไร้สายจากภายนอกเครือข่าย โดยระบบเครือข่ายแลน มีความเสี่ยงในการถูกโจมตีใกล้เคียงระบบเครือข่ายแลนไร้สาย และการโจมตีแบบ TCP Flood มีอัตราการตรวจจับได้สูงสุดในทุกการทดลอง โดยเฉพาะอย่างยิ่งการตรวจจับการบุกรุกเมื่อมีการใช้ฮันนี่พอทในระบบแลนค่าเฉลี่ยการตรวจจับประมาณ 400.2 แพ็กเก็ต ซึ่งเป็นค่าสูงสุดเมื่อเปรียบเทียบกับการโจมตีแบบ ICMP Flood ที่มีอัตราการตรวจจับการบุกรุกน้อยที่สุดในทุกการทดลอง โดยการใช้ฮันนี่พอทในระบบแลนมีค่าเฉลี่ยการตรวจจับประมาณ 186.2 แพ็กเก็ต ซึ่งต่างกัน 53.47% และที่สำคัญจะเห็นได้ว่าฮันนี่พอทมีจำนวนการตรวจจับได้มากกว่ากรณีไม่มีฮันนี่พอทในแทบทุกการทดลองแม้เฉลี่ยต่างกันไม่เกินประมาณ 7 % นั้นเป็นการยืนยันได้ว่าฮันนี่พอทสามารถช่วยหลอกล่อผู้ประสงค์ร้ายในการโจมตีเครื่องแม่ข่ายได้อย่างมีประสิทธิภาพ ดังที่ได้แสดงไว้ในตารางที่ 2

ตารางที่ 2 เปรียบเทียบผลการโจมตีแบบภายนอก

External Attack

Attack		Time										Average	
		1	2	3	4	5	6	7	8	9	10	Total	(%)
Server (LAN)	TCP Flood	400	400	400	402	400	400	400	400	400	400	400.2	100
	UDP Flood	200	200	200	200	200	200	200	200	200	200	200	50
	ICMP Flood	186	186	186	186	186	186	186	186	186	186	186	46.48
Honeypot (LAN)	TCP Flood	400	400	400	400	400	400	400	400	402	400	400.2	100
	UDP Flood	200	200	200	200	200	200	100	100	100	200	170	42.48
	ICMP Flood	188	186	186	186	186	186	186	186	186	186	186.2	46.53
Server (Wifi)	TCP Flood	400	400	400	272	404	400	400	400	400	400	387.4	96.8
	UDP Flood	130	200	200	200	200	200	200	200	200	200	193	48.23
	ICMP Flood	200	184	184	182	180	184	184	184	184	178	184.4	46.08
Honeypot (Wifi)	TCP Flood	400	360	400	402	400	400	400	400	400	400	396.2	99
	UDP Flood	200	200	200	200	200	200	200	200	200	200	200	49.98
	ICMP Flood	184	182	184	184	182	182	182	182	184	180	182.6	45.63

5. สรุปผลการทดลอง

การโจมตีแบบปฏิเสธการให้บริการจากภายในมีจำนวนการตรวจจับการบุกรุกที่มากกว่าการโจมตีจากภายนอกเฉลี่ยรวมประมาณ 48.3% นั้นหมายถึงการใช้เราท์เตอร์เพื่อแยกระบบเครือข่ายออกเป็นส่วนๆ แม้ไม่การใช้ไฟร์วอลล์และกำหนดคุณสมบัติด้านความปลอดภัยใดๆกับเราท์เตอร์สามารถลดโอกาสในการโจมตีแบบปฏิเสธการให้บริการจากผู้ประสงค์ร้ายต่อเครื่องแม่ข่ายได้อย่างมาก และการโจมตีแบบ TCP Flood สามารถตรวจจับการบุกรุกได้มากที่สุดนั้นเป็นเพราะ TCP โพรโทคอลเป็นได้รับความนิยม การให้บริการ และมีการใช้งานของเครื่องแม่ข่ายโดยทั่วไปจำนวนมาก จึงทำให้ระบบตรวจจับการบุกรุกสามารถตรวจจับการบุกรุกได้แตกต่างมากกว่าโพรโทคอลอื่นๆ และในส่วนการโจมตีแบบปฏิเสธการให้บริการผ่านระบบแลน และแลนไร้สายที่มีค่าใกล้เคียงกันในทุกการทดลองเป็นเพราะจำนวนรวมเครื่องลูกข่ายของแลนไร้สายมีจำนวนไม่เกิน 3 เครื่อง ดังนั้นหากในกรณีที่จำนวนรวมเครื่องลูกข่ายของแลนไร้สายมีจำนวนมากกว่า 100 เครื่อง ผลลัพธ์ของการทดลองระหว่างแลน และแลนไร้สายจะมีค่าต่างกัน โดยการตรวจจับในเครือข่ายแลนไร้สายจะมีค่าน้อยกว่าเครือข่ายแลนเนื่องจากกลไกการสื่อสารของแลนไร้สายเป็นแบบ Carrier Sent Multiple Access/Collision Avoidance (CSMA/CA) (Alshami, I.H., Ahmad, N.A. and Sahibuddin, S., 2014) ซึ่งเป็นการสื่อสารของอุปกรณ์ไร้สายแบบ Half Duplex กล่าวคือจะต้องใช้การหลีกเลี่ยงการชนของสัญญาณที่มีการเสียเวลาในการรอคอยช่องสัญญาณจำนวนมาก อีกทั้งยังอาจเกิดปัญหาการรบกวนสัญญาณ หรือการสูญหายของสัญญาณระหว่างการสื่อสารไร้สาย จึงทำให้มีผลลัพธ์ของการโจมตีที่มีความล่าช้า กว่าการสื่อสารในเครือข่ายแลนซึ่งใช้กลไกการสื่อสารแบบ Full Duplex กล่าวคือไม่ต้องหลีกเลี่ยงการชนของสัญญาณในช่องสัญญาณที่จำกัด และที่สำคัญจะเห็นได้ว่าเมื่อมีการใช้ระบบตรวจจับการบุกรุกร่วมกับฮันนี่พอทจะมีจำนวนการตรวจจับได้มากกว่ากรณีไม่มีฮันนี่พอทในทุกการทดลองโดยเฉลี่ยต่างกันประมาณ 7% นั้นเป็นการยืนยันได้ว่าฮันนี่พอทสามารถเพิ่มประสิทธิภาพในการรักษาความมั่นคงทางไซเบอร์โดยช่วยหลอกล่อผู้ประสงค์ร้ายในการโจมตีเครื่องแม่ข่ายได้เป็นอย่างดี

กิตติกรรมประกาศ

ผู้วิจัยขอขอบพระคุณ มหาวิทยาลัยราชภัฏพระนคร ที่ให้การสนับสนุนด้านงบประมาณในการจัดทำการวิจัย และห้องปฏิบัติการ Network security คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ที่สนับสนุนอุปกรณ์ทางด้านเครือข่าย อาทิ เราท์เตอร์ คอมพิวเตอร์ เพื่อใช้ในการทำงานวิจัย

เอกสารอ้างอิง

อรรถพล ป้อมสถิตย์. (2554). การวัดประสิทธิภาพระบบตรวจจับการบุกรุกเครือข่ายแบบกระจาย (Performance Measurement of Intrusion Detection System Across Distributed Sensors). CIT 2011 proceeding, Mahidol Univ. p. 166-169.

อรรถพล ป้อมสถิตย์. (2555). Effective of Unicast and Multicast IP Address Attack Over Intrusion Detection System with Honeypot. การประชุม Asia-Pacific Advanced Network: APAN ครั้งที่ 33. เชียงใหม่.

Alshami, I.H., Ahmad, N.A. and Sahibuddin, S. (2014). People effects on WLAN-Based IPS' accuracy experimental preliminary results. 8th

Malaysian Software Engineering Conference (MySEC). pp. 206-209.

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

Jianrong Xi. (2011). A Design and Implement of IPS Based on Snort. Seventh International Conference on Computational Intelligence and Security (CIS). pp. 771- 773.

Keith Harrison, James R. Rutherford and Gregory B. White. (2015). The Honey Community: Use of Combined Organizational Data for Community Protection. 48th Hawaii International Conference on System Sciences (HICSS). pp. 2288 - 2297.

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

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

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

Xinming C., Beipeng M. and Chen Z. (2011). A Collaborative Network Security Platform for In-network Security. Third International Conference on Communications and Mobile Computing (CMC). pp. 59-64.

Zhenxin Z., Maochao X. and Shouhuai X. (2013). Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study. IEEE Transactions on Information Forensics and Security. pp. 1775 – 1789.

❑❑❑❑❑