การเพิ่มสมรรถนะของระบบตรวจจับการบุกรุกด้วยฮันนี่พอทของระบบการส่งสัญญาณสื่อใหม่ผ่านอินเทอร์เน็ต

Efficiency Increase of Intrusion Detection System with Honey Pot for Transmission New Media Broadcasting via Internet

อรรถพล ป้อมสถิตย์*
Auttapon Pomsathit
บุญเรือง เกิดอรุณเดช**
Boonruang Kerdaroondej

Received : May 27, 2019
Revised : July 13, 2019
Accepted : August 17, 2019

บทคัดย่อ

งานวิจัยการเพิ่มสมรรถนะของระบบตรวจจับการบุกรุกด้วยฮันนี่พอทของระบบการส่งสัญญาณสื่อใหม่ผ่านอินเทอร์เน็ตนำเสนอการศึกษาการบุกรุกเครือข่ายที่มีการส่งสัญญาณสื่อใหม่ผ่านอินเทอร์เน็ตโดยใช้ฮันนี่พอทในการหลอกล่อ หน่วงเวลา หรือเบี่ยงเบน ผู้บุกรุกไม่ให้โจมตีไปที่เครื่องแม่ข่าย ในการโจมตีรูปแบบการปฏิเสธการมีการให้บริการ 3 รูปแบบได้แก่ SYN Flood, UDP Flood และ Smurf Flooding โดยฮันนี่พอทจะใช้โปรแกรม Honeyd ในการจำลองเครื่องคอมพิวเตอร์หรือเครื่องแม่ข่ายให้อยู่ในแผนผังเครือข่ายที่ต้องการจะรักษาความปลอดภัยโดยกำหนดให้ไม่มีการใช้งานไฟร์วอล์และการรักษาความปลอดภัยรูปแบบอื่นๆ ซึ่งจะใช้ระบบป้องกันการบุกรุกและฮันนี่พอทเท่านั้นในการรักษาความปลอดภัยเครือข่าย ส่วนระบบตรวจจับการบุกรุกเครือข่ายจะใช้โปรแกรม Snort บนระบบปฏิบัติการ Linux จากผลการทดสอบการโจมตีจากระบบเครือข่ายภายใน และภายนอก โดยการเชื่อมต่อผ่านอุปกรณ์สวิตช์ และเราท์เตอร์ ซึ่งงานวิจัยนี้ทำการโจมตีจำนวน 1,000 แพ็กเก็ตผ่านระบบเครือข่ายสายซึ่งมีความเสี่ยงในการถูกโจมตีใกล้เคียงระบบเครือข่ายไร้สาย และการโจมตีแบบ SYN Flood มีอัตราการตรวจจับการบุกรุกได้สูงสุดเมื่อเปรียบเทียบกับการโจมตีแบบ Smurf Flooding โดยสรุปผลการโจมตีจากภายในเครือข่ายจะมีผลการโจมตีมากกว่าการโจมตีจากภายนอกเฉลี่ยทุกการทดลองประมาณ 18% ส่วนในทุกการโจมตีผ่านเครือข่ายสาย จะมีผลการโจมตีมาก่ กว่าการโจมตีผ่านไร้สายเฉลี่ยทุกการทดลองประมาณ 8% นั่นหมายถึงบุกรุกเครือข่ายที่มีการส่งสัญญาณสื่อใหม่ผ่านอินเทอร์เน็ตจะต้องมีการป้องกันการโจมตีแบบ SYN Flood และการโจมตีจากภายในซึ่งมีอันตรายมากที่สุด ทั้งนี้ฮันนี่พอทสามรถลดผลการกระทบจากโจมตีได้ประมาณ 7 %

คำสำคัญ : ระบบตรวจจับการบุกรุก / การปฏิเสธการให้บริการ / การรักษาความมั่นคงทางไซเบอร์ / ฮันนี่พอท

*อาจารย์ประจำวิทยาลัยนานาชาติพระนคร มหาวิทยาลัยราชภัฏพระนคร
Lecturer at Phra Nakhon International College Phranakhon Rajabhat University
**บุคลากรประจำกรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข
Personnel at the Department of Health Service Support Ministry of Public Health

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: SYN Flood, UDP Flood and Smurf Flooding. 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 via switch and router device by attacker send 1,000 packet to system, 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 SYN Flood attack and Smurf Flooding attack. In summary, the attack results from internal network will result in an attack of more than 18% of all attacks from external attacks. In every attack through the network will have an attack effect about 8% of the average wireless attack on every experiment means that the network that is transmitting new media through the Internet must be protected. SYN Flood attacks and internal attacks are the most dangerous. Finally, HoneyPot can reduce the impact of the attack by about 7%.

Keywords : Intrusion Detection System / Denial of Service / CyberSecurity / Honeypot

บทนำ

ในปัจจุบันการรักษาความปลอดภัยมทางไซเบอร์ มักจะเป็นการโจมตีแบบ 80:20 โดย 80% นั้นเป็นการโจมตีภายใน และ 20% นั้นเป็นการโจมตีจากภายนอก อาทิ การสร้าง Malware ก็สามารถใช้เครื่องมือเพื่อสร้าง Malware โดยเฉพาะได้แล้ว ซึ่งในขั้นตอนการสร้างนั้น ผู้สร้างสามารถเลือกสร้างให้ Malware ตัวนั้นๆ หลบหลีกการตรวจจับในรูปแบบต่างๆ ที่ต้องการได้ และสามารถทำการทดสอบได้ด้วยว่าจะถูกตรวจจับทางใดได้บ้างจากการอัพโหลดขึ้น VirusTotal สำหรับการทดสอบว่า Malware ตัวนั้นจะถูกตรวจจับหรือไม่ได้ทันที ทำให้การสร้าง Malware ที่ซับซ้อนขึ้นนั้นทำได้จากการทดสอบในลักษณะนี้อย่างต่อเนื่อง ถึงแม้ว่าเทคโนโลยีด้านการรักษาความมั่นคงทางไซเบอร์ได้ก้าวไปข้างหน้าอย่างรวดเร็วซอฟต์แวร์และฮาร์ดแวร์ต่างๆ ที่เกี่ยวข้องกับความปลอดภัยด้านสารสนเทศได้ถูกวิจัยและพัฒนาขึ้นเพื่อตอบสนองความต้องการของผู้ใช้มากขึ้นแต่ก็ยังไม่ต่อรูปแบบการโจมตีที่มีความหลากหลาย และซับซ้อนเพิ่มขึ้นตาม ดังนั้นระบบตรวจจับการบุกรุก (Intrusion Detection System: IDS) หรือระบบตรวจจับการบุกรุกเป็นอีกหนึ่งเครื่องมือที่ใช้สำหรับตรวจจับความพยายามบุกรุกเครือข่ายโดยระบบจะแจ้งเตือนไปยังผู้ดูแลระบบเมื่อมีการบุกรุก หรือมีการพยายามที่จะบุกรุกเครือข่าย โดยระบบจะรายงานเฉพาะสิ่งที่กำหนดให้รายงานเท่านั้น (อรรถพล, 2562) ซึ่งมีอยู่สองสิ่งที่ผู้ดูแลระบบจะต้องกำหนดค่าให้กับ ระบบตรวจจับการบุกรุกสิ่งแรกคือ Signature ของการบุกรุก สิ่งที่สองคือเหตุการณ์ที่ผู้ดูแลระบบให้ความสำคัญหรือเหตุการณ์ที่คาดว่าจะเป็นผลไปสู่การบุกรุกในภายหน้า ซึ่งเหตุการณ์ต่างๆเหล่านี้อาจเป็นสัญญาณจราจรที่ไม่ปกติหรืออาจเป็นบางข้อความใน log การกำหนดค่า Signature ให้กับ

ระบบตรวจจับการบุกรุกของแต่ละองค์กรนั้นอาจจะไม่เหมือนกัน ซึ่งจะขึ้นอยู่กับว่าองค์กรนั้นจะให้ความสนใจกับการบุกรุกประเภทใด และในการตรวจสอบลักษณะข้อมูลของผู้ใช้ที่เข้ามาใช้บริการในระบบโดยระบบจะมีตัวคัดกรองความถูกต้องหรือต้องสงสัย ถ้าเกิดลักษณะการเรียกใช้ข้อมูลของผู้ใช้บริการเกิดผิดปกติหรือต้องสงสัย ระบบตรวจจับการบุกรุกจะทำการตรวจจับข้อมูลดังกล่าวและทำการแจ้งเตือนในรูปแบบสถิติในการโจมตี

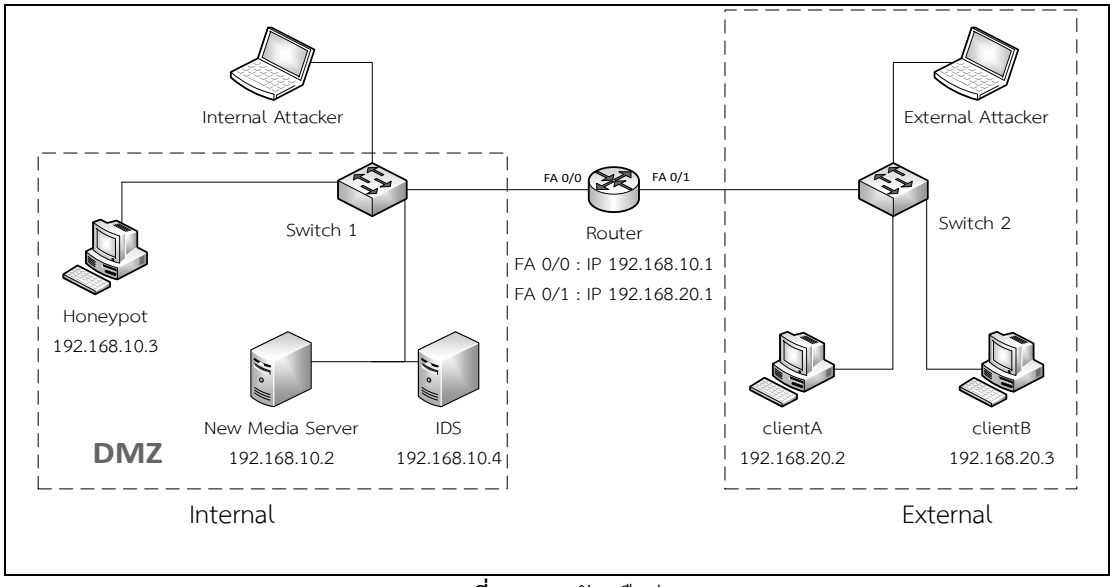
เพื่อเพิ่มประสิทธิภาพในการตรวจจับการบุกรุก ฮันนี่พอท(Honeypot) จึงเป็นระบบความปลอดภัยอีกชนิดหนึ่งที่เสริมการทำงานของระบบตรวจจับการบุกรุกได้เป็นอย่างดี ซึ่งฮันนี่พอทก็คือคอมพิวเตอร์หรือกลุ่มของคอมพิวเตอร์ที่ถูกติดตั้งไว้สำหรับล่อลวงให้ผู้บุกรุกทำการโจมตี และเพื่อเรียนรู้เทคนิคที่ผู้บุกรุกใช้และนำความรู้เหล่านั้นมาใช้ในการหาทางป้องกันการโจมตีใหม่ๆ ที่เกิดขึ้น อีกทั้งฮันนี่พอทยังสามารถใช้ลดความเสี่ยงของเครื่องแม่ข่ายในระบบที่อาจถูกโจมตีหรือใช้เป็นระบบตรวจสอบการบุกรุกได้อีกทางหนึ่งด้วยการหลอกล่อให้ผู้บุกรุกเกิดความสับสนในการโจมตี โดยปกติแล้วฮันนี่พอทจะถูกติดตั้งในเครือข่ายที่แยกจากเครือข่ายที่ใช้งานจริง หรือติดตั้งในบริเวณเดียวกับเครื่องแม่ข่ายเพื่อป้องกันไม่ให้เครื่องแม่ข่ายที่ใช้งานเครือข่ายภายในถูกโจมตีได้ง่ายจากผู้บุกรุกซึ่งแม้ว่าจะมีการป้องการอย่างดีจากอุปกรณ์รักษาความปลอดภัยเครือข่าย อาทิ ไฟล์วอล หรือโปรแกรมป้องกันไวรัสต่างๆ

ในงานวิจัยนี้ได้ใช้ฮันนี่พอทชนิด Low-Interaction Honeypot ซึ่งจะมีการตอบสนองต่อการโจมตีในแบบการปฏิเสธการให้บริการ (Denial of Service : DoS) ของผู้บุกรุกตามข้อมูลของฮันนี่พอทที่กำหนดไว้ ซึ่งโดยปกติมักจะกำหนดให้ผู้บุกรุกสามารถใช้งานฮันนี่พอทได้อย่างจำกัด หลังจากที่ผู้บุกรุกเข้าไปได้แล้ว ฮันนี่พอทจะให้ข้อมูลเกี่ยวกับการโจมตีของผู้บุกรุก โดยใช้ซอฟต์แวร์ Honeyd ทำการจำลอง Services ต่างๆ ที่คาดว่าผู้บุกรุกจะทำการโจมตีเช่น HTTP (หมายเลขพอร์ต 80), SSH (หมายเลขพอร์ต 22) หรือ SMTP (หมายเลขพอร์ต 25) (Pomsathit A., 2015) เป็นต้น ดังนั้นเพื่อเป็นการป้องกันหรือลดช่องทางในการกระทำความผิดตามที่ได้กล่าวมาข้างต้น ผู้วิจัยจึงมีแนวคิดในการทำวิจัยเพิ่มประสิทธิภาพระบบตรวจจับการบุกรุกในการรักษาความมั่นคงทางไซเบอร์ด้วยฮันนี่พอท เพื่อป้องกันการโจมตีจากผู้บุกรุกในการระงับ ชะลอ ขัดขวาง หรือรบกวนจนเครื่องแม่ข่ายไม่สามารถทำงานตามปกติได้ โดยผลลัพธ์ที่ได้จากการวิจัยจะสามารถนำมาใช้ในปรับปรุงและพัฒนาการดำเนินงานของผู้ดูแลระบบเครือข่ายของมหาวิทยาลัย หน่วยงาน ภาครัฐและภาคเอกชน เพื่อนำไปสู่ความมั่นคงของระบบคอมพิวเตอร์ตามวัตถุประสงค์ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี 2550

วิธีดำเนินการวิจัย

1. ออกแบบผังเครือข่าย

ในการออกแบบผังเครือข่ายนั้นได้ออกแบบให้ผังเครือข่ายมีความใกล้เคียงกับระบบที่มีการใช้จริงกับหน่วยงานของภาครัฐและเอกชนเพื่อให้สามารถนำไปประยุกต์ใช้ได้จริง อันประกอบด้วย 1) ระบบเครือข่ายภายใน (internal) เป็นการระบบเครือข่ายภายในองค์กรที่สมมติให้การทดลองไม่มีการป้องกันจากอุปกรณ์รักษาความปลอดภัยทางคอมพิวเตอร์ต่างๆ อาทิ ACLของอุปกรณ์ และไฟล์วอล โดยจะมีการติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย และระบบตรวจจับการบุกรุกเป็นองค์ประกอบหลักโดยเชื่อมต่ออุปกรณ์ทั้งหมดผ่านอุปกรณ์สวิตซ์ 2) ระบบเครือข่ายภายนอก (External) เป็นระบบเครือข่ายที่อยู่ภายนอกองค์กรหรืออาจสมมติว่าเป็นเครือข่ายอินเทอร์เน็ต โดยจะมีการติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลเป็นองค์ประกอบหลักโดยเชื่อมต่ออุปกรณ์ทั้งหมดผ่านอุปกรณ์สวิตซ์ โดยทั้งส่วนระบบเครือข่ายภายในและระบบเครือข่ายภายนอกจะเชื่อมต่อผ่านอุปกรณ์เราท์เตอร์ ทั้งนี้แผนผังเครือข่ายรวมจะคำนึงถึงจำนวนอุปกรณ์ที่มีอยู่จริงของห้องปฏิบัติการ Network Security โดยมีรายละเอียดการออกแบบผังเครือข่ายทั้งหมดดังภาพที่ 1



ภาพที่ 1 แสดงผังเครือข่าย

2. การติดตั้งและกำหนดค่าอุปกรณ์เครือข่ายต่างๆ ดังต่อไปนี้

2.1 กำหนดค่าอุปกรณ์เราท์เตอร์ให้สามารถใช้คุณสมบัติ DHCP Pool และคุณสมบัติ เราท์เตอร์ RIP ได้

2.2 การกำหนดค่าอุปกรณ์สวิตซ์ให้สามารถทำการ Spanning Port คือ การที่สวิตช์จะส่งต่อทุกๆ แพ็กเก็ตที่รับจากพอร์ตหนึ่งไปยังอีกพอร์ตหนึ่ง และการกำหนดค่า Port mirror ให้กับสวิตซ์ซึ่งเป็นเทคโนโลยีที่เป็นประโยชน์และถูกนำมาใช้อย่างมากในการตรวจสอบและเก็บสถิติต่างๆ ในการรับ-ส่งข้อมูลของพอร์ตหนึ่งบนอุปกรณ์ดังกล่าว

2.2.1 การติดตั้งส่วนการโจมตี

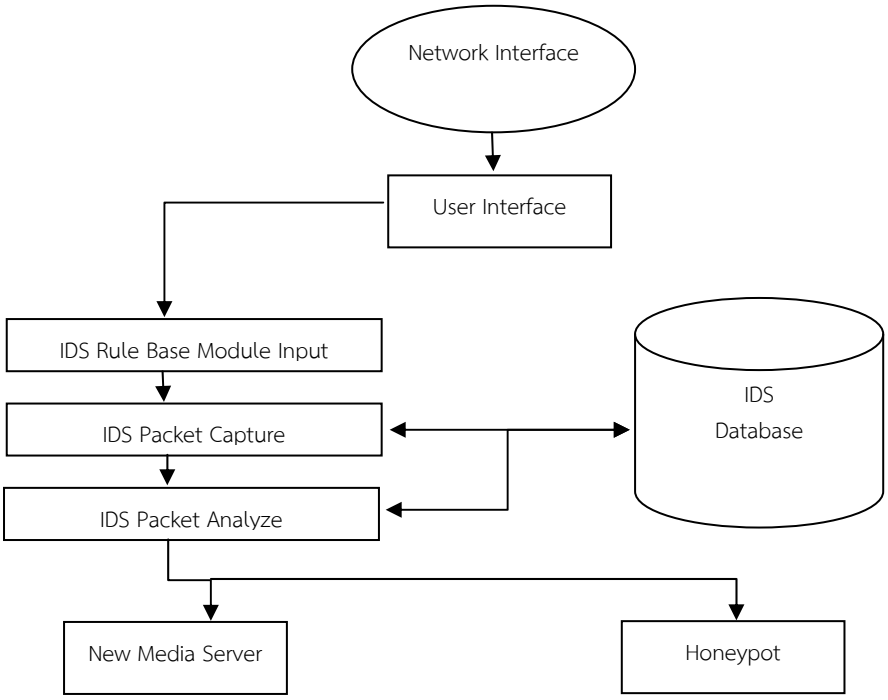
1) โปรแกรม Nessus สำหรับการค้นหาช่องโหว่ของเครือข่าย โดยความสามารถคือจะค้นหาเครื่องคอมพิวเตอร์ในเครือข่ายแล้วจะรายงานช่องโหว่ของคอมพิวเตอร์แต่ละเครื่อง และการสร้างการโจมตี SYN Flood, UDP Flood และ Smurf Flooding สู่เครื่องคอมพิวเตอร์เป้าหมาย ทั้งเครื่องแม่ข่ายระบบการส่งสัญญาณสื่อใหม่ผ่านอินเทอร์เน็ต และเครื่องคอมพิวเตอร์ที่จำลองการทำงานฮันนี่พอท ซึ่งติดตั้งผ่าน Linux Blacktrack

2) โปรแกรม Snort เป็นการสร้างระบบจับการบุกรุก ชนิดระบบตรวจหาการบุกรุกบนเครื่องคอมพิวเตอร์ (Host-based IDS) (Jianrong Xi., 2011) ซึ่งจะทำงานในเครื่องคอมพิวเตอร์ด้วยการติดตามตรวจสอบสัญญาณจราจร ที่อยู่ในรูปของแพ็กเก็ตข้อมูลและตรวจสอบการใช้งานโปรแกรมประยุกต์ (Application) ในเครื่องคอมพิวเตอร์จากไฟล์บันทึกข้อมูลการใช้งานการจราจรเครือข่ายเพื่อตรวจสอบว่าแพ็กเก็ตใดมีลักษณะที่ผิดปกติ

3. การกำหนดค่า Rule ของโปรแกรม Snort

Rule นั้นก็คือกฎหรือข้อบังคับในการตรวจจับรูปแบบการโจมตีหรือ แพ็กเก็ตที่โปรแกรมตรวจจับได้ 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.2.9.6) ดังที่แสดงไว้ในภาพที่ 2



ภาพที่ 2 แสดงการทำงานของระบบตรวจจับการบุกรุกและฮันนี่พอท

4. ฮันนี่พอท

Honeyd เป็นซอฟต์แวร์ที่ใช้ในการหลอกล่อผู้ที่เข้ามาโจมตี โดยที่ซอฟต์แวร์ตัวนี้ได้มีการใช้กันอย่างแพร่หลายจึงมีการพัฒนาอย่างต่อเนื่องจนมาถึงปัจจุบัน ทำให้ตัวโปรแกรมเป็นที่ยอมรับและได้มาตรฐาน Honeyd (Pauna, A. & 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 จะทำการตรวจจับและวิเคราะห์ การจราจรเครือข่ายของแพ็กเก็ตต่างๆ เปรียบเทียบกับ Rule ของโปรแกรมตามที่ตั้งค่าไว้และวิเคราะห์รูปแบบการถูกโจมตีรูปแบบต่างๆ ว่าเป็นโจมตีนั้นเป็นชนิดใดและมีจำนวนหรือมีระดับความเสี่ยงต่อระบบมากน้อยเพียงใด และเก็บข้อมูลเหตุการณ์หรือ Log ลงฐานข้อมูล ซึ่งข้อมูลหรือ Log ที่เกิดขึ้นของ Sensor ที่มีอยู่แต่ละตัวจะมาเก็บลงในฐานข้อมูลที่เครื่องแม่ข่ายตัวเดียวกัน ต่อมาในการแสดงผลการตรวจจับนั้น จะแสดงออกมาที่หน้าเว็บที่ดึงจาก

ข้อมูลในฐานข้อมูลมาแสดงเพื่อความสะดวกในการให้ผู้ดูแลระบบได้จัดการหรือป้องกันระบบได้อย่างมีประสิทธิภาพ ส่วนโปรแกรม Honeyd (Keith, H., James, R., Rutherford. & Gregory, B., White., 2015) นั้นก็จะเริ่มจากการกำหนดค่าตามที่ผู้ดูแลระบบได้กำหนดค่าไว้ ต่อจากนั้นจะทำการอ่านค่าที่ไฟล์ honeyd.conf และใช้โปรแกรม rarpd honeyd ซึ่งเป็นฮันนี่พอทชนิด low-interaction honeypot ที่มีหน้าที่ในการดักจับการโจมตี แล้วทำการตั้งค่า IP Address ตามที่ต้องการจำลองแบบให้มีเครื่องแม่ข่ายเพื่อเป็นเครื่องหลอกล่อให้ผู้บุกรุกเข้าโจมตี

ผลการวิจัย

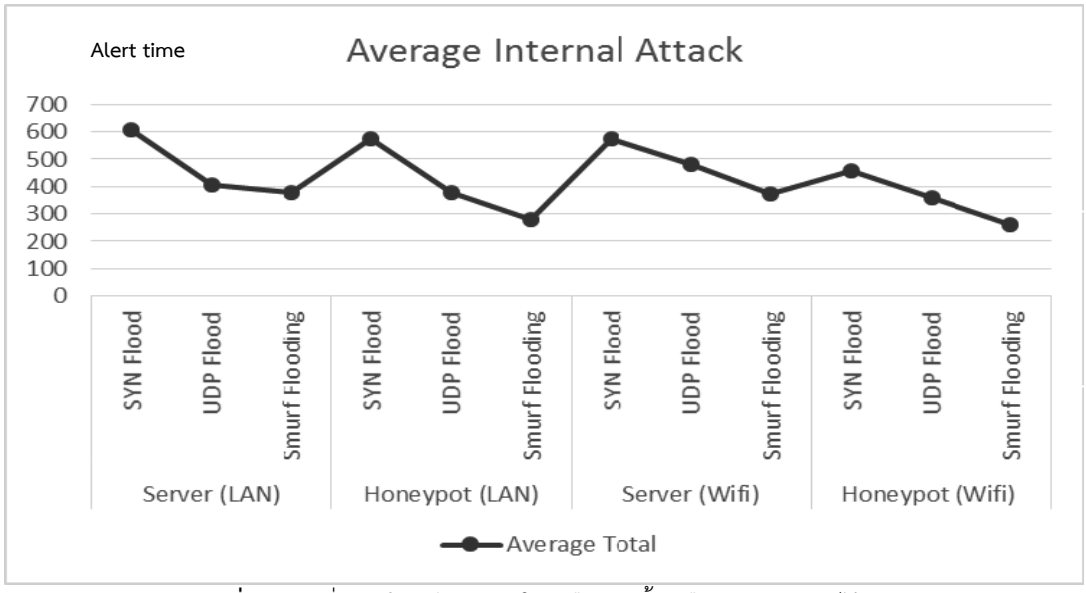
การวิเคราะห์ประสิทธิภาพการโจมตีด้วยฮันนี่พอท จากการดำเนินงานได้แบ่งการทดลองออกเป็น 2 การทดลองคือ

1. การโจมตีเครื่องแม่ข่าย และฮันนี่พอทจากภายใน (Internal)
2. การโจมตีเครื่องแม่ข่าย และฮันนี่พอทจากจากภายนอก (External)

เพื่อที่จะให้ทราบถึงประสิทธิภาพการทำงานของฮันนี่พอท และความแตกต่างระหว่างการโจมตีผ่านระบบเครือข่ายสายและการโจมตีผ่านระบบเครือข่ายไร้สาย เพื่อวิเคราะห์ประสิทธิภาพการตรวจจับการบุกรุกที่มีประสิทธิภาพมากที่สุด ซึ่งในการทดลองนี้จะใช้การโจมตีแบบปฏิเสธการให้บริการโดยแบ่งการโจมตีออกเป็น 3 ประเภท ได้แก่ SYN Flood, UDP Flood และ Smurf Flooding ซึ่งทำการทดสอบประสิทธิภาพด้วยการใช้ระบบตรวจจับการบุกรุกเพื่อเก็บข้อมูลการบุกรุกที่เกิดขึ้นทั้งในเครื่องแม่ข่าย และฮันนี่พอท โดยผลการทดลองจะเปรียบเทียบจำนวนเหตุการณ์ที่ระบบตรวจจับการบุกรุกซึ่งสามารถจับได้ระหว่างการโจมตีผ่านเครือข่ายสายและการโจมตีผ่านระบบเครือข่ายไร้สาย ที่มีการโจมตีจากภายในและภายนอกโดยมีเราท์เตอร์ทำหน้าที่แบ่งพื้นที่ระบบเครือข่ายภายในและภายนอกดังที่ได้แสดงไว้ในภาพที่ 1 ซึ่งการดำเนินการตามขั้นตอนการทดลองได้ทำการรวบรวมข้อมูลจากผลการดำเนินงานหาค่าเฉลี่ย และแสดงอยู่ในรูปของกราฟเพื่อให้ง่ายต่อการวิเคราะห์ข้อมูลโดยในทุกรูปของผลการทดลองแกน x จะแสดงถึงจำนวนครั้งในการแจ้งเตือนการโจมตีซึ่งเป็นผลที่ได้จากระบบตรวจจับการบุกรุก ส่วนแกน y จะแสดงถึงจำนวนครั้งในการทดลองโจมตีระบบในระยะเวลาเท่าๆ กัน คือ 30 วินาที โดยมีการส่งแพ็กเก็ตในการโจมตีจำนวน 1,000 แพ็กเก็ต

1. เปรียบเทียบการโจมตีเครื่องแม่ข่าย และฮันนี่พอทแบบสายจากภายในเครือข่าย

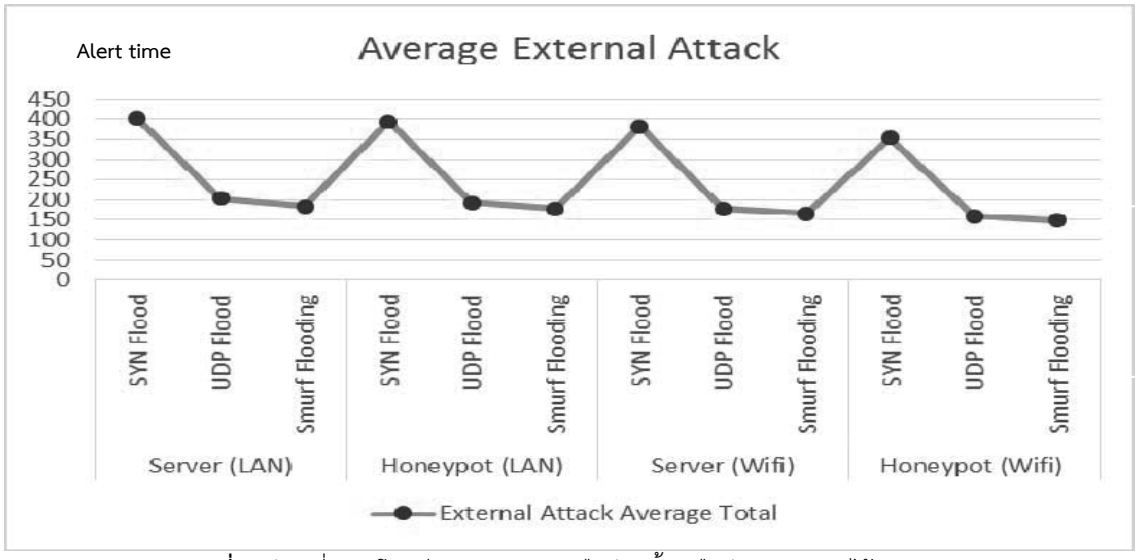
การเปรียบเทียบผลการโจมตีจากภายในเครือข่ายสายโดยทำการเปรียบเทียบจากรูปแบบการโจมตีประเภทปฏิเสธการให้บริการ ที่มีการควบคุมจำนวนการโจมตีให้เท่ากันทุกรูปแบบแล้วบันทึกผลการทดลองเป็นเหตุการณ์ที่เกิดขึ้นในแต่ละอุปกรณ์จะเห็นได้ว่า เหตุการณ์ส่วนมากจะเกิดขึ้นจากการโจมตีที่โพรโทคอล TCP โดยใช้รูปแบบการโจมตีคือ SYN Flood ทั้งนี้เนื่องจากโพรโทคอล TCP เป็นโพรโทคอลหลักที่ใช้ในการเชื่อมต่อระหว่างเครื่องแม่ข่ายผู้ให้บริการกับผู้ใช้บริการอยู่แล้ว และในการทดลองที่โพรโทคอล TCP จะเห็นได้ว่าจำการโจตีที่ตรวจจับได้จะมีค่ามากกว่าทุกโพรโทคอลในทุกการทดลอง อีกทั้งในทุกการทดลองเมื่อมีการติดตั้งฮันนี่พอทจะสามารถชวนลดอัตราการโจมตีลงได้ประมาณ 6 % ดังแสดงในภาพที่ 3



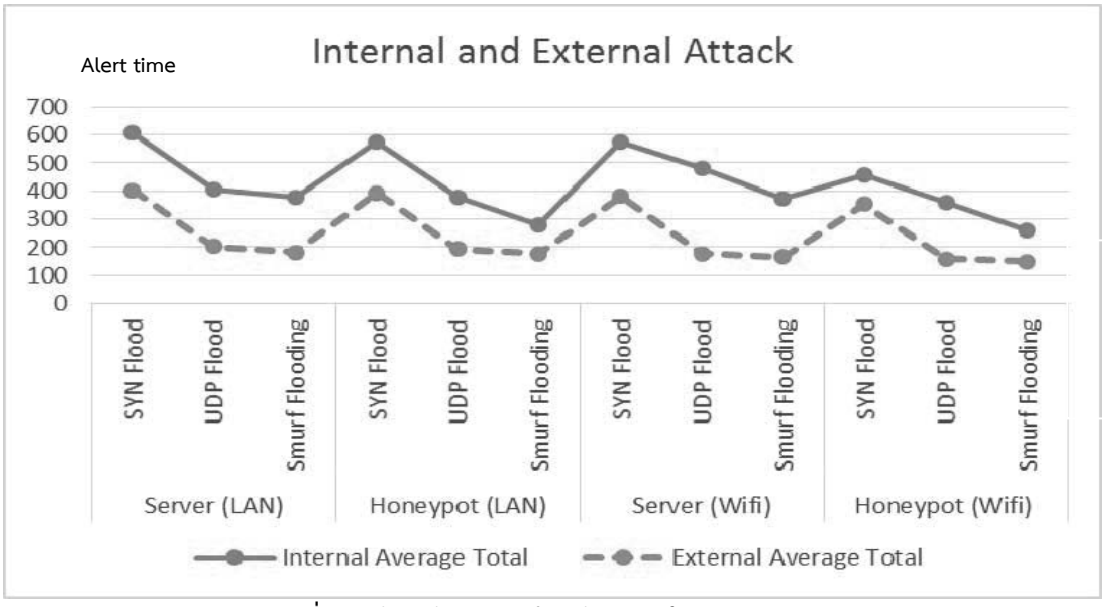
ภาพที่ 3 ค่าเฉลี่ยการโจมตีจากภายในเครือข่ายทั้งเครือข่ายสาย และไร้สาย

2. เปรียบเทียบการโจมตีเครื่องแม่ข่าย และฮันนี่พอทแบบสายจากภายนอกเครือข่าย

การเปรียบเทียบผลการโจมตีจากภายนอกเครือข่ายสาย จะมีผลใกล้เคียงกับการโจมตีจากภายในโดยเหตุการณ์ส่วนมากจะเกิดขึ้นจากการโจมตีที่โพรโทคอล TCP โดยใช้รูปแบบการโจมตีคือ SYN Flood ซึ่งการโจมตีด้วย Smurf Flooding มีผลการโจมตีน้อยที่สุดในทุกผลการทดลอง ทั้งนี้เนื่องจากโพรโทคอล TCP เป็นโพรโทคอลหลักที่ใช้ในการเชื่อมต่อระหว่างเครื่องแม่ข่ายผู้ให้บริการกับผู้ใช้บริการอยู่แล้ว และในการทดลองที่โพรโทคอล TCP จะเห็นได้ว่าจำการโจตีที่ตรวจจับได้จะมีค่ามากกว่าทุกโพรโทคอลในทุกการทดลอง อีกทั้งในทุกการทดลองเมื่อมีการติดตั้งฮันนี่พอทจะสามารถชวนลดอัตราการโจมตีลงได้ประมาณ 13 % ดังแสดงในภาพที่ 4



ภาพที่ 4 ค่าเฉลี่ยการโจมตีจากภายนอกเครือข่ายทั้งเครือข่ายสาย และไร้สาย



ภาพที่ 5 เปรียบเทียบผลการโจมตีจากภายในและภายนอก

3. เปรียบเทียบการโจมตีเครื่องแม่ข่าย และฮันนี่พอท จากภายในและภายนอก

การเปรียบเทียบผลการโจมตีจากภายในเครือข่าย และการโจมตีจากภายนอกเครือข่ายผ่านเครือข่ายสาย และไร้สาย โดยทำการเปรียบเทียบจากรูปแบบการโจมตีประเภทปฏิเสธการให้บริการทั้ง 3 ชนิด ได้แก่ SYN Flood, UDP Flood และ Smurf Flooding โดยควบคุมจำนวนการโจมตีให้เท่ากันทุกรูปแบบแล้วบันทึกผลการทดลองเป็นเหตุการณ์ที่เกิดขึ้นในแต่ละอุปกรณ์จะเห็นได้ว่าในการโจมตี SYN Flood มีค่าการตรวจจับการโจมตีสูงสุด และการโจมตีจากภายในเครือข่ายจะมีผลการโจมตีมากกว่าการโจมตีจากภายนอกเฉลี่ยทุกการทดลองประมาณ 18% ส่วนในทุกการโจมตีผ่านเครือข่ายสาย จะมีผลการโจมตีมาก่ กว่าการโจมตีผ่านไร้สายเฉลี่ยทุกการทดลองประมาณ 8% ดังที่ได้แสดงไว้ในภาพที่ 5

อภิปรายผล

1. ผลการทดลองเปรียบเทียบการโจมตีภายในเครือข่าย

การเปรียบเทียบการโจมตีเครื่องแม่ข่ายและฮันนี่พอททั้งแบบสาย และแบบไร้สายจากภายในเครือข่าย โดยระบบเครือข่ายสาย มีความเสี่ยงในการถูกโจมตีใกล้เคียงระบบเครือข่ายไร้สาย และการโจมตีแบบ SYN Flood มีอัตราการตรวจจับที่สูงที่สุดในทุกการทดลอง โดยเฉพาะอย่างยิ่งการตรวจจับการบุกรุกเมื่อมีการใช้ฮันนี่พอทในเครือข่ายสายมีค่าเฉลี่ยการตรวจจับประมาณ 606.5 แพ็กเก็ต ซึ่งเป็นค่าสูงสุด เมื่อเปรียบเทียบกับการโจมตีแบบ Smurf Flooding ที่มีอัตราการตรวจจับการบุกรุกน้อยที่สุดในเกือบทุกการทดลอง โดยการใช้ฮันนี่พอทในเครือข่ายสายมีค่าเฉลี่ยการตรวจจับประมาณ 260.8 แพ็กแก็ต ซึ่งต่างกันถึง 31% และที่สำคัญจะเห็นได้ว่าฮันนี่พอทมีจำนวนการตรวจจับได้น้อยกว่ากรณีไม่มีฮันนี่พอทในแทบทุกการทดลองแม้เฉลี่ยต่างกันไม่เกินประมาณ 8% นั้นเป็นการยืนยันได้ว่าฮันนี่พอทสามารถช่วยหลอกล่อผู้ประสงค์ร้ายในการโจมตีเครื่องแม่ข่ายได้อย่างมีประสิทธิภาพนอกเหนือจากการใช้อุปกรณ์ IDS หรือ IPS ในการรักษาความปลอดภัย ดังที่ได้แสดงไว้ในตารางที่ 1

ตารางที่ 1 เปรียบเทียบผลการโจมตีแบบภายในเครือข่าย

Internal Attack												
Attack		Time to Testing										Average Alert time
		1	2	3	4	5	6	7	8	9	10	Total
Server (LAN)	SYN Flood	606	615	600	602	611	601	605	599	613	613	606.5
	UDP Flood	412	401	412	404	400	396	418	401	399	405	404.8
	Smurf Flooding	377	379	382	385	332	383	395	381	402	382	379.8
Honeypot (LAN)	SYN Flood	597	530	588	596	599	521	599	589	594	537	575
	UDP Flood	392	393	391	338	390	392	362	390	359	362	376.9
	Smurf Flooding	298	226	277	276	296	282	281	295	272	272	277.5
Server (Wifi)	SYN Flood	552	592	587	542	582	579	557	592	577	592	575.2
	UDP Flood	433	497	478	488	484	499	453	496	496	483	480.7
	Smurf Flooding	387	364	356	362	382	365	364	373	375	388	371.6
Honeypot (Wifi)	SYN Flood	485	450	445	462	451	478	464	457	445	454	459.1
	UDP Flood	323	372	398	388	272	389	293	373	396	376	358
	Smurf Flooding	287	274	269	222	272	295	243	254	245	247	260.8

2. ผลการทดลองเปรียบเทียบการโจมตีภายนอกเครือข่าย

การเปรียบเทียบการโจมตีเครื่องแม่ข่าย และฮันนี่พอททั้งแบบสายและแบบไร้สายจากภายนอกเครือข่าย โดยระบบเครือข่ายสาย มีความเสี่ยงในการถูกโจมตีใกล้เคียงระบบเครือข่ายไร้สาย และการโจมตีแบบ SYN Flood มีอัตราการตรวจจับได้สูงสุดในทุกการทดลอง โดยเฉพาะอย่างยิ่งการตรวจจับการบุกรุกเมื่อมีการใช้ฮันนี่พอทในเครือข่ายสายค่าเฉลี่ยการตรวจจับประมาณ 402.5 แพ็กเก็ต ซึ่งเป็นค่าสูงสุด เมื่อเปรียบเทียบกับการโจมตีแบบ Smurf Flooding ที่มีอัตราการตรวจจับการบุกรุกน้อยที่สุดในทุกการทดลอง โดยการใช้ฮันนี่

พอทในเครือข่ายสายมีค่าเฉลี่ยการตรวจจับประมาณ 149 แพ็กเก็ต ซึ่งต่างกัน ประมาณ 25 % และที่สำคัญจะเห็นได้ว่าฮันนี่พอทมีจำนวนการตรวจจับได้ลดลงในกรณีไม่มีฮันนี่พอทในแทบทุกการทดลองแม้เฉลี่ยต่างกันไม่เกินประมาณ 7 % นั้นเป็นการยืนยันได้ว่าฮันนี่พอทสามารถช่วยหลอกล่อผู้ประสงค์ร้ายในการโจมตีจากภายนอกเครื่องแม่ข่ายได้อย่างมีประสิทธิภาพ เนื่องจากผู้ประสงค์ร้ายไม่สามารถเป้าหมายในการโจมตีที่แท้จริง จึงเกิดการซุ่มโจมตีจึงจะเป็นการเพิ่มเวลาให้ผู้แลระบบสามารถตรวจเจอการโจมตีและสามารถหาทางป้องกันผ่านการกำหนดค่าไฟร์วอล์หรือการปรับเปลี่ยนโครงสร้างระบบได้ทันเวลา ดังที่ได้แสดงไว้ในตารางที่ 2

ตารางที่ 2 เปรียบเทียบผลการโจมตีแบบภายนอก

External Attack												
Attack		Time to Testing										Average Alert time
		1	2	3	4	5	6	7	8	9	10	Total
Server (LAN)	SYN Flood	406	405	400	402	400	401	405	402	401	403	402.5
	UDP Flood	206	201	202	204	200	201	208	201	203	205	203.1
	Smurf Flooding	184	179	182	185	182	183	185	181	184	182	182.7
Honeypot (LAN)	SYN Flood	397	400	388	394	392	401	399	381	394	397	394.3
	UDP Flood	192	194	193	188	200	192	182	190	199	202	193.2
	Smurf Flooding	168	166	177	176	186	182	181	175	176	182	176.9
Server (Wifi)	SYN Flood	388	392	377	372	392	369	377	392	375	382	381.6
	UDP Flood	133	177	168	188	182	179	183	193	186	183	177.2
	Smurf Flooding	177	164	166	162	180	165	164	163	155	158	165.4
Honeypot (Wifi)	SYN Flood	355	360	345	362	351	371	344	354	335	354	353.1
	UDP Flood	123	172	158	138	172	189	153	163	166	156	159
	Smurf Flooding	147	134	164	142	172	135	153	151	145	147	149

กิตติกรรมประกาศ

ผู้วิจัยขอขอบพระคุณ มหาวิทยาลัยราชภัฏพระนคร ที่ให้การสนับสนุนด้านงบประมาณในการจัดทำการวิจัย และห้องปฏิบัติการ Wireless Communication Lab. มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ที่สนับสนุนอุปกรณ์ทางด้านเครือข่าย อาทิ เราท์เตอร์ คอมพิวเตอร์ เพื่อใช้ในการทำงานวิจัย

เอกสารอ้างอิง

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

_____. (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 The Empress Convention Centre (ECC) โรงแรม ดิ เอ็มเพรส เชียงใหม่.

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

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

Arunanto, F.X, et al. (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, 2011 Seventh International Conference on Computational Intelligence and Security (CIS), (pp.771-773).

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

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

Pauna, A. & 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, 2012 Spring Congress on Engineering and Technology (S-CET), (pp.1-4).

Qian, G., Jie, F. & 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).

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