บรรณานุกรม

[1] E. Al-Shaer and H.Hamed, “Firewall Policy Advisor for Anomaly Detection and Rule Editing”, *IEEE/IFIP Intergrated Management Conference (IM’2003),* March 2003.

[2] E. Al-Shaer and H.Hamed, “Design and Implementation of Firewall Policy Advisor Tools”, *Depaul CTI Technical Report, CTI-TR-02-006,* August 2002

[3] E. Al-Shaer and H.Hamed, “Modeling and Management of Firewall Policies”, n *10th IEEE International Conference on Network Protocols ICNP,* November 2002

[4] นายพัฒนพล รัตนพงษ์พร, “การตรวจจับความขัดแย้งแบบรวดเร็วและขยายขนาดได้สำหรับตัวจัดกลุ่มแพ็คเก็ต” ,บัณฑิตศึกษา วิศวกรรมคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง 2547

[5] Firewalling, NAT , and packet mangling for Linux :http://www.netfilter.org

[6] TCPDUMP public repository :http://www.tcpdump.org

[7] Libpcap Packet capture tutorial :http://www.cet.nau.edu/~mc8/Socket/Tutorials/section1.html

[8] Linux 2.4 Stateful Firewall : IPTABLES :http://thaicert.nectec.or.th/paper/firewall/iptables.php

[9] นพสรณ์ เกษจันทร์ , ศุภกร ชอุ่มดี “การป้องกันเว็บโดยใช้ไอพีเทเบิลส์” ปริญญานิพนธ์ วิศวกรรมศาสตร์บัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง 2546

[10]บุญลือ อยู่คง ป้องกัน Linux อย่างมืออาชีพ สำนักพิมพ์ The Knowledge Center กรุงเทพฯ

ภาคผนวก ก การติดตั้ง

เนื่องจากส่วนโค้ดของโปรแกรมจะใช้ภาษาเชลล์สคริปต์ เนื่องจากเป็นภาษาที่เรียนรู้เข้าใจง่าย และสามารถเรียกคำสั่งต่างๆ บนระบบปฏิบัติการณ์ลินุกซ์ ให้ทำงานควบคู่กันไปได้ง่าย อีกทั้งยังไม่จำเป็นต้องทำการติดตั้งหรือคอมไฟล์แพ็คเก็ตแต่อย่างใด

ตัวงานจะเป็นไฟล์ที่ทำการบีบอัดเอาไว้ชื่อ optimize.tar.gz ทำการแตกไฟล์โดยใช้คำสั่ง

```
tar -zxvf optimize.tar.gz
```

จะได้ผลออกมาเป็นโฟลเดอร์ที่มีชื่อว่า optimize ก็เป็นอันเสร็จการติดตั้งเรียบร้อย

ภาคผนวก ข การใช้งาน

ตัวโปรแกรมจะเป็นภาษาเชลล์สคริปต์ดังนั้นต้องทำการเรียกทำงานแบบเชลล์สคริปต์ นั่นคือ คำสั่ง source หรือ ./ ก็ได้ตามด้วยออฟชั่น 2 ตัว

รูปแบบของคำสั่ง

./optimize <options1={remove,log,reorder}> <options2={input,output,forward}>

ในส่วนของ options1 นั้นจะเป็นการบอกกับโปรแกรมว่าให้กระทำการใด ซึ่งมีอยู่ 3 อย่างคือ

- remove ตัวโปรแกรมจะทำการตรวจสอบกฎที่ซ้ำซ้อนและลบกฎที่ซ้ำซ้อนนั้นออก
- log ตัวโปรแกรมจะทำการใส่กฎที่มีรายละเอียดเหมือนกับแต่ละกฎที่มีอยู่ในไฟร์วอลล์ไอพีเทเบิ้ลส์อยู่แล้ว แต่ทาร์เก็ตฟังก์ชันจะเป็นการเก็บรายละเอียดของแพ็คเก็ตของข้อมูลที่ผ่านกฎนั้นๆ ลงล็อคไฟล์แทน
- reorder ตัวโปรแกรมจะทำการลบกฎที่เกิดขึ้นจากออฟชั่น log ออก และคำนวณปริมาณข้อมูลภายในเครือข่ายที่ผ่านแต่ละกฎออกมาเป็นตัวเลข เพื่อใช้เปรียบเทียบกัน และนำข้อมูลส่วนนี้ไปใช้ในการจัดลำดับกฎใหม่ และในส่วนของการจัดลำดับนั้น ตัวโปรแกรมจะทำการตรวจสอบความสัมพันธ์และความขัดแย้งของแต่ละกฎเพื่อไม่ให้ความหมายโดยรวมของกฎในการตรวจสอบแพ็คเก็ตนั้นเปลี่ยนแปลงไป

ในส่วนของ options2 นั้นเป็นการบอกกับโปรแกรมว่าให้กระทำการนั้นๆ กับเชนใดของไอพีเบิ้ลส์

- INPUT ตัวโปรแกรมจะกระทำการตามออฟชั่นแรกกับเชน INPUT ในไอพีเทเบิ้ลส์
- OUTPUT ตัวโปรแกรมจะกระทำการตามออฟชั่นแรกกับเชน OUTPUT ในไอพีเทเบิ้ลส์
- FORWARD ตัวโปรแกรมจะกระทำการตามออฟชั่นแรกกับเชน FORWARD ในไอพีเทเบิ้ลส์