ชื่อเรื่องการค้นคว้าแบบอิสระ ระบบป้องกันและตรวจสอบผู้บุกรุกเครือข่าย
บนระบบปฏิบัติการลีนุกซ์
คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่

ผู้เขียน นายสรวิช รุจนวิศาล

ปริญญา วิทยาศาสตรมหาบัณฑิต(เทคโนโลยีสารสนเทศและการจัดการ)

อาจารย์ที่ปรึกษาการค้นคว้าแบบอิสระ
อาจารย์ ดร.เอกรัฐ บุญเชียง

บทคัดย่อ

การศึกษาระบบป้องกันและตรวจสอบผู้บุกรุกเครือข่าย บนระบบปฏิบัติการลีนุกซ์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ มีวัตถุประสงค์ 3 ประการ คือ 1) เพื่อตรวจสอบ เก็บข้อมูล และวิเคราะห์การบุกรุกระบบเครือข่ายได้ ณ เวลาที่เกิดขึ้นจริง และ 2) พัฒนาประสิทธิภาพของระบบเตือนภัยและป้องกันการบุกรุกระบบเครือข่ายขนาดเล็กและกลางให้ดีขึ้น

การพัฒนาระบบนี้ได้พยายามนำเอาเทคโนโลยีทางด้านระบบป้องกันการบุกรุกและระบบตรวจสอบผู้บุกรุกเครือข่าย มาประยุกต์ใช้ร่วมกัน เพื่อให้ระบบมีประสิทธิภาพในการเตือนภัยและป้องกันการบุกรุกระบบบนเครือข่ายให้ดีขึ้น โดยการออกแบบให้ระบบสามารถตรวจจับและป้องกันการบุกรุกได้อย่างอัตโนมัติ และสามารถตรวจสอบรายงานการบุกรุกที่เกิดขึ้นได้อย่างง่ายดายจากทางเว็บเพ็จ

ผลการศึกษาพบว่าระบบป้องกันและตรวจสอบผู้บุกรุกระบบเครือข่ายนี้ มีความสะดวกต่อการใช้งานของผู้ดูแลระบบในการตรวจสอบการบุกรุกได้ ณ เวลาที่เกิดขึ้นจริง ช่วยให้ผู้ดูแลระบบสามารถวิเคราะห์สาเหตุและผลลัพธ์ที่อาจจะเกิดขึ้นตามมา รวมถึงการหาวิธีแก้ไขจุดล่อแหลมต่างๆที่ก่อเกิดให้เกิดปัญหาการบุกรุกเข้ามา ทั้งยังช่วยลดขั้นตอนในการป้องกันการบุกรุกที่ตรวจพบให้เป็นไปอย่างอัตโนมัติด้วย

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright © by Chiang Mai University
All rights reserved

Independent Study Title Firewall Protection and Intrusion Detection System Using the Linux Operating System at the Faculty of Science, Chiang Mai University

Author Mr.Sorawit Rujanawisan

Degree Master of Science (Information Technology and Management)

Independent Study Advisor Lecturer Dr. Ekkarat Boonchieng

ABSTRACT

The objectives of this study, "Firewall Protection and Intrusion Detection System using the Linux Operating System at the Faculty of Science ,Chiangmai University" are : 1) to detect, keep log and analyse patterns of network intrusion in real-time; and 2) to improve efficiency of system's alarm and prevention from network intrusion for small and middle size of network system.

The system is implemented by integrating two technologies of a defense system ,firewall and a network intrusion detection system for working together to improve efficiency of the system against the intrusion. By designing, the system can detect the intrusion incidents and automatically send an order to firewall to block the packets that may cause the intrusion. The monitor and analysis console is a web-based that can easily access for administrator.

The following of the study is a system , Firewall and Network Intrusion Detection System on Linux Operating System, that can assist a network/system administrator to monitor and detect intrusion incidents on the network in the real-time. The administrator can analyse the problems, the probably following results and fixing the vulnerabilities in the properly way. Finally, the steps of intrusion prevention are decreased and proceed automatically.

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright © by Chiang Mai University
All rights reserved