DESIGN AND IMPLEMENTATION OF SNORT IDS RULES MANAGEMENT

CHITTHAPORN SAE-NGOW

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(COMPUTER SCIENCE)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2007

การออกแบบและพัฒนา การบริหารจัดการเงื่อนไขของการตรวจสอบการบุกรุกของระบบด้วยระบบการตรวจสอบผู้บุกรุก SNORT (DESIGN AND IMPLEMENTATION OF SNORT IDS RULES MANAGEMENT)

จิตราภรณ์ แซ่โง้ว 4537073 SCCS/M

วท.ม. (วิทยาการคอมพิวเตอร์)

คณะกรรมการควบคุมวิทยานิพนธ์: สุดสงวน งามสุริยโรจน์, Ph.D., ทรงศรี ตั้งศรีไพโรจน์, Ph.D., วัสกา วิสุทธิวิเศษ, Ph.D.

บทคัดย่อ

เครือข่ายมหาวิทยาลัยมหิดลหรือ MUC-Net มีระบบรักษาความปลอดภัยหลายชนิดได้แก่ ระบบ Firewall ระบบ Anti-virus และระบบตรวจจับผู้บุกรุกหรือ IDS แต่ลักษณะโครงสร้างแบบกระจายของมหาวิทยาลัยมหิดลนั้นยากแก่การตรวจจับและป้องกันผู้บุกรุกจากภายใน ดังนั้นจึงเสนอวิธีการติดตั้งระบบ Multiple IDS โดยแต่ละ IDS สามารถตรวจจับการบุกรุก และส่ง Alert เตือนไปยังผู้ดูแลระบบในส่วนกลางได้ทันเวลา

Snort เป็น Open-Source เกี่ยวกับระบบตรวจจับผู้บุกรุกที่ได้รับความนิยมมากที่สุด โดยใช้หลักการอ้างอิง Signature หรือ Rules ในการตรวจจับผู้บุกรุก ส่วนมากแล้วผู้ดูแลระบบจะเป็นผู้ Update Rules เอง สำหรับเครือข่าย MUC-Net ที่มีลักษณะแบบกระจายนั้น ปัญหาในการ Update Rules ให้มีความสอดคล้องกันจึงเป็นส่วนสำคัญ เพื่อที่จะลดความเสี่ยงและความเสียหายจากการบุกรุก นอกจากนั้น หากใช้งานทุก Rules ที่มีทั้งหมดอาจส่งผลกับประสิทธิภาพในการทำงานของ Snort อีกด้วย ดังนั้นจึงควรที่จะติดตามการใช้งาน Rules ของ Snort ในทุกแห่งที่ติดตั้ง Snort ด้วย

ในงานวิจัยนี้ เราได้ออกแบบและพัฒนาระบบการบริหารจัดการ Rules สำหรับระบบ Snort IDS แบบกระจาย ที่ประกอบด้วย IDS Sensors ทำการติดตั้งไว้แต่ละแห่ง และมี IDS Manager ทำหน้าที่ Update Snort Rules ให้กับ IDS Sensors แบบอัตโนมัติ เมื่อได้ Download จาก snort.org และ IDS Sensors ไม่เพียงทำการตรวจดูการใช้งาน Rules ของเครื่อง เพื่อลดจำนวนการใช้ Rules เท่านั้น แต่ยังคงความสอดคล้องของ Rules ทั้งระบบอีกด้วย ซึ่งระบบทำการวิเคราะห์การใช้งาน Rules แต่ละเครื่อง ดังนั้นและประสิทธิภาพจะเพิ่มมากขึ้น เราได้ทำการติดตั้ง Snort IDS ที่ Lab จำนวน 4 เครื่อง และทำการจัดเก็บ Alert Logs และวิเคราะห์ เป็นเวลา 1 เดือน ทำให้พบว่ามี Rules เพียงเล็กน้อยที่ถูใช้งาน และพบ False Alarms ประเภท SNMP จำนวนมาก จากการเฝ้าสังเกตการทำงานของเครือข่าย

70 หน้า

DESIGN AND IMPLEMENTATION OF SNORT IDS RULES MANAGEMENT

CHITTRAPORN SAE-NGOW 4537073 SCCS/M

M.Sc. (COMPUTER SCIENCE)

THESIS ADVISORS: SUDSANGUAN NGAMSURIYAROJ, Ph.D., SONGSRI TANGSRIPAIROJ, Ph.D., VASAKA VISOOTTIVISETH, Ph.D.

ABSTRACT

Mahidol University's network or MUC-Net has deployed several security mechanisms including firewalls, anti-virus, and an intrusion detection system or IDS. But, the distributed structure of Mahidol University's campuses makes it difficult to detect and prevent intrusions from inside the network. One essential idea is to install multiple IDS systems at several locations so that individual IDS would detect any malicious attempts and send alerts to the central administrators in-charge of the time.

SNORT is the most popular open source IDS based on a set of signatures or rules for detecting intrusions. Rule updates are primarily done manually by the system administrator. But, for distributed nature of MUC-Net, the problem of updating rules to ensure their consistency must be addressed to reduce risks and damages from attacking. In addition, having every rule active would degrade the performance of SNORT machines. Hence, the usage of SNORT rules at all locations must be monitored.

In this thesis, we designed and implemented rules management for a distributed SNORT IDS that consisted of IDS sensors installed at several locations, and the IDS manager who automatically updates SNORT's rules at every IDS sensor when they are downloaded from snort.org. IDS sensors not only keep track of rules usage at their machines to minimize the number of active rules, but also ensure rules consistency among them. The system also analyzes rules usage of individual IDS. Thus, the IDS's performance would be enhanced. We install SNORT IDS sensors at four computer labs, and alert logs for one month periods are collected and analyzed. We found that only a few rules are actively used, and the number of false alarms is high for SNMP-type since most network equipments use it for monitoring.

KEY WORDS: INTRUSION DETECTION SYSTEM/ RULES MANAGEMENT / RULES CONSISTENCY/ FALSE ALARMS

70 pp.