ภาคผนวก ก

กฎที่ใช้ตรวจจับการบุกรุก

กฎที่ใช้สำหรับการตรวจจับการบุกรุกในแบบจำลองที่พัฒนามี 2 ส่วนคือ ส่วนกฎของเหตุการณ์ปกติและส่วนของกฎการตรวจจับการบุกรุก ซึ่งกฎส่วนแรกนั้นประกอบด้วยข้อมูลดังนี้

```
sendmail\[\d+\]: .*.to=
sendmail\[\d+\]: .*.from=
(sendmail\[\d+\]: .*.relay=*.) && (!.*.reject.*.)
sendmail\[\d+\]: .*.: clone .*., owner=
sendmail\[\d+\]: NOQUEUE:*
sendmail\[\d+\]: .*.User unknown
sendmail\[\d+\]: .*.DSN: Service unavailable
sendmail\[\d+\]: .*.DSN: Host unknown
sendmail\[\d+\]: .*.DSN: Return receipt
sendmail\[\d+\]: .*.could not send message for past \d+ hours
sendmail\[\d+\]: .*.Domain of sender address .*. does not resolve
sendmail\[\d+\]: .*.Domain of sender address .*. does not exist
sendmail\[\d+\]: .*.Relaying temporarily denied
sendmail\[\d+\]: .*.Relaying denied
sendmail\[\d+\]: .*.timeout waiting for input from
sendmail\[\d+\]: .*.collect: premature EOM: Error 0
sendmail\[\d+\]: .*.collect: unexpected close on connection from
sendmail\[\d+\]: .*.lost input channel from
sendmail\[\d+\]: .*.forward .*. Group writable directory
sendmail\[\d+\]: .*.sender notify: Service unavailable
sendmail\[\d+\]: .*.return to sender: Service unavailable
sendmail\[\d+\]: .*.runqueue: Flushing queue from
sendmail\[\d+\]: .*.aliases rebuilt by root
sendmail\[\d+\]: aliases.*.longest
update.virus.scanners
MailScanner\[\d+\]: .*.Uninfected
MailScanner\[\d+\]: .*.Virus and Content Scanning
MailScanner\[\d+\]: .*.New Batch
MailScanner\[\d+\]: .*.Using locktype
```

MailScanner\[\d+\]: .*.MailScanner .*. starting...
MailScanner\[\d+\]: .*.New Batch
MailScanner\[\d+\]: .*.RBL Check
MailScanner\[\d+\]: .*.SpamAssassin
MailScanner\[\d+\]: .*.Virus and Content Scanning: Starting
MailScanner\[\d+\]: .*.Virus Scanning
MailScanner\[\d+\]: .*.Saved infected
MailScanner\[\d+\]: .*.Cleaned: Delivered \d+ cleaned messages
MailScanner\[\d+\]: .*.Sender Warnings: Delivered \d+ warnings to virus senders
MailScanner\[\d+\]: .*.Notices: Warned about \d+ messages
MailScanner\[\d+\]: .*.Disinfection:* Attempting to disinfect \d+ messages
MailScanner\[\d+\]: .*.Virus Re-scanning: Sophos found \d+ infections
MailScanner\[\d+\]: .*.Disinfection: Rescan found only \d+ viruses
MailScanner\[\d+\]: .*.MailScanner child dying of old age
sshd(pam_unix)\[\d+\]: .*.session opened for user .*. by (uid=0)
sshd(pam_unix)\[\d+\]: .*.session closed for user .*.
su(pam_unix)\[\d+\]: .*.session opened for user .*. by .*.
su(pam_unix)\[\d+\]: .*.session closed for user .*.
login(pam_unix)\[\d+\]: .*.session opened for user .*. by .*.
login(pam_unix)\[\d+\]: .*.session closed for user .*.
CRON\[\d+\]: \(root\) .*.
CROND\[\d+\]: \(mailman\) .*.

และกฎการตรวจจับการบุกรุกประกอบด้วยข้อมูลดังนี้

Virus (\S+) found in file::Found virus $1::Correlation-*** be careful
***::email=ssupacho::0::3::300

Back Orifice Traffic detected::Found trojan – Back Orifice::Correlation-*** plase verify trojan in your system ***::email=ssupacho::0::0::0

Large ICMP Packet::Found Ping Flood attack::Correlation-*** be careful
***::email=ssupacho::0::0::0

SYN Flood detected::possible SYN Flood attack::Correlation-*** SYN Flooding
***::email=ssupacho

authentication failure.* rhost=(\S+) user=(\S+)::User $2 login failure more than 10 times from $1::** Password Brute-force attack **::email=ssupacho,root::0::10::60

device (\S+) entered promiscuous mode::Device $1 entered promiscuous mode::*** device $1 entered promiscuous mode, check sniffer program in your computer***::email=ssupacho

NOQUEUE: \[(.*?)\] did not issue .*? during connection to MTA::Client quit before communicating, may be scanning service from $1::Correlation-*** be careful ***::email=ssupacho

\[([0-9\.]+)]: (VRFY|vrfy) (\S+) \[rejected\]::rejected VRFY, may be scanning service from $1::Correlation-*** be careful ***::email=ssupacho

reject connections on deamon (\S+):load average: ([0-9]+)::too many load on $1::Correlation-*** checking load/process on your machine ***::email=ssupacho

POSSIBLE ATTACK from (\S+)::possible attack to local exploit of sendmail::Correlation-** Update/Patch Sendmail ***::email=ssupacho,root

ภาคผนวก ข

นิยามคำศัพท์

คำศัพท์	ความหมาย
Active Attack	การโจมตีที่ทำให้เกิดการแก้ไข เปลี่ยนแปลงของข้อมูลหรือระบบและการสร้างข้อมูลขึ้นมาใหม่โดยการปลอมแปลง
Anomaly Detection	แนวทางในการตรวจจับการบุกรุกที่ตั้งอยู่บนพื้นฐานการตรวจหาพฤติกรรมของผู้ใช้และการใช้ทรัพยากรของระบบคอมพิวเตอร์ที่ผิดไปจากสภาวะการใช้งานปกติ
Attack	การโจมตีเป็นการกระทำโดยพยายามที่จะข้ามผ่านกระบวนการควบคุมความปลอดภัยของระบบคอมพิวเตอร์ โดยอาจเป็นการทำลาย เปิดเผย แก้ไขข้อมูลและรวมถึงการที่ทำให้ระบบไม่สามารถให้บริการแก่ผู้ใช้ได้
Audit Trail	ชุดของรายการข้อมูลเหตุการณ์ต่าง ๆ ของเครื่องคอมพิวเตอร์ที่เกี่ยวกับระบบปฏิบัติการ โปรแกรมประยุกต์หรือกิจกรรมต่าง ๆ ของผู้ใช้
Availability	ความพร้อมใช้เป็นความมั่นใจว่าข้อมูลและบริการการสื่อสารต่าง ๆ พร้อมที่จะใช้งานได้ในเวลาที่ผู้ใช้ต้องการใช้
Brute Force	การพยายามถอดรหัสข้อความที่มีการเข้ารหัสไว้ โดยการพยายามใช้ทุก ๆ คีย์ที่เป็นไปได้
Confidentiality	ความลับเป็นการรับรองว่ามีการเก็บข้อมูลไว้เป็นความลับและผู้ที่มีสิทธิเท่านั้นจึงจะเข้าถึงข้อมูลนั้นได้
Denial of Service	การกระทำที่ป้องกันไม่ให้ผู้ใช้ที่มีสิทธิสามารถเข้าถึงและใช้งานระบบได้หรือระบบไม่สามารถทำงานได้ตามวัตถุประสงค์และระยะเวลาที่กำหนด จนไม่สามารถให้บริการได้

คำศัพท์	ความหมาย
False negative	ความผิดพลาดในทางลบ เกิดขึ้นเมื่อระบบรักษาความปลอดภัยไม่พบความผิดปกติใด ๆ เมื่อมีการบุกรุกเกิดขึ้นจริงในระบบ
False positive	ความผิดพลาดในทางบวก เกิดขึ้นเมื่อระบบรักษาความปลอดภัยได้ระบุว่าการกระทำหนึ่งเป็นการบุกรุกแต่ที่จริงแล้วไม่ใช่การบุกรุก
Integrity	ความบูรณภาพเป็นการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลาย ไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนาร้ายและเป็นข้อมูลที่ถูกต้องและสมบูรณ์
Intrusion	ความพยายามหรือการกระทำที่ส่งผลต่อความบูรณภาพ (Integrity) ความลับ (Confidentiality) และ ความพร้อมใช้งาน (Availability) ของทรัพยากรในระบบหรือการกระทำเพื่อข้ามผ่านมาตรการในการควบคุมความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย
Intrusion Detection	เทคนิคในการตรวจจับการบุกรุกเข้าสู่เครื่องคอมพิวเตอร์หรือเครือข่ายโดยการตรวจสอบข้อมูลในบันทึกความปลอดภัย (security logs) หรือข้อมูลบันทึกการใช้งาน (audit log) สำหรับกระบวนวิเคราะห์ข้อมูลเพื่อตรวจจับการบุกรุกหรือความพยายามที่จะบุกรุกอาจจะทำโดยผู้ดูแลระบบหรือใช้โปรแกรมช่วยในการวิเคราะห์ก็ได้
Intrusion Detection System	ระบบสำหรับทำงานในกระบวนการตรวจสอบเหตุการณ์ต่าง ๆที่เกิดขึ้นในระบบคอมพิวเตอร์และเครือข่ายเพื่อวิเคราะห์หาร่องรอยการบุกรุกโดยอัตโนมัติ
Intrusion Signature	ร่องรอยการบุกรุกเป็นรายละเอียดของสถานการณ์หรือสถานภาพต่าง ๆ ซึ่งบ่งชี้ได้ว่าได้มีการบุกรุกเกิดขึ้น
Misuse Detection	แนวทางในการตรวจจับการบุกรุกโดยอาศัยคุณลักษณะหรือรูปแบบที่ได้กำหนดไว้แล้วว่าเป็นการบุกรุกแล้วนำมาเปรียบเทียบหรือค้นหากับเหตุการณ์ที่เกิดขึ้นในระบบเพื่อหาการบุกรุกโดยตรง

คำศัพท์	ความหมาย
Passive Attack	การโจมตีที่ไม่ได้ทำให้เกิดการเปลี่ยนแปลงของข้อมูลต่าง ๆแต่ผู้โจมตีสามารถเข้าถึงข้อมูลได้โดยไม่ได้รับอนุญาต
Pattern Matching	การจับคู่แบบรูปเป็นการค้นหาคำหรือข้อความโดยใช้วิธีการเปรียบเทียบรูปแบบกับข้อความที่ต้องการค้นหาว่าตรงกันหรือไม่
Sniffer	โปรแกรมที่เป็นเครื่องมือที่ดักจับข้อมูลบนเครือข่ายสำหรับการตรวจสอบและวิเคราะห์ข้อมูลการจราจรในเครือข่าย
Social Engineering	เทคนิคในการเข้าถึงข้อมูลในระบบโดยการหลอกลวงหรือหลอกล่อให้ผู้ใดผู้หนึ่งหลงเชื่อและทำในสิ่งที่ต้องการ โดยมักเกิดขึ้นผ่านทางการสนทนาระหว่างมนุษย์ด้วยกันหรือการติดต่อกันวิธีอื่น
Subversion	ความผิดพลาดที่ก่อให้เกิดผิดพลาดในทางลบ (false negative) โดยผู้บุกรุกอาจจะใช้ความรู้เกี่ยวกับการทำงานภายในระบบตรวจจับบุกรุก เพื่อปรับเปลี่ยนการทำงานของระบบตรวจจับให้ไม่สามารถที่จะตรวจสอบการกระผิดที่กำลังกระทำอยู่
Syslog	โปรแกรมที่ทำหน้าที่เป็นศูนย์กลางในการจัดการเก็บล็อกต่าง ๆ ในระบบปฏิบัติการยูนิกซ์ ซึ่งคิดค้นขึ้นโดย Computer Science Research Group (CSRG) ที่ University of California at Berkeley (UC-Berkeley)
Vulnerability	ช่องโหว่หรือความอ่อนแอในการออกแบบ การพัฒนา การทำงานและการจัดการระบบซึ่งเปิดโอกาสให้เกิดการกระทำที่ขัดกับนโยบายการรักษาความปลอดภัยของระบบได้