การป้องกันการบุกรุกบน Postfix

อ้างอิง : http://beginlinux.com/server_training/mail-server/1065-protect-postfix-from-attack

สรุปโดย : อดิศร ขาวสังข์

จัดทำเมื่อ : 1 พฤษภาคม 2552

บน Postfix สามารถเซ็ตค่าให้สามารถป้องกันการจู่โจมระบบได้ การจู่โจมอาจเกิดจาก Client system ที่มีการคอนฟิกผิดพลาด หรือจากการบุกรุกเพื่อประสงค์ร้าย (malicious attack) ที่พยายามใช้คำสั่งที่เป็นอันตรายต่อ Server และเช่นเดียวกัน ทรัพยากรของระบบจะถูกทำให้ไร้ประโยชน์เว้นแต่ออฟชันอื่น ๆ ที่สามารถใช้งานได้ ในความเป็นจริงบน Postfix มีการเซ็ต 3 อย่าง ที่จะเริ่มกระบวนการขอการเพิ่มการหน่วงในการโต้ตอบกับ 3 ชนิดของการบุกรุก ดังนี้

smtpd_error_sleep_time = 2s

smtpd_soft_error_limit = 10

smtpd_hard_error_limit = 20

บรรทัดแรกเป็น sleep or delay time หลังจากระบบรับรู้ถึงการบุกรุกจำนวน 10 ครั้งจากแหล่งกำเนิดอันเดียวกัน การบุกรุกในครั้งที่ 11 จะถูกหน่วงไป 12 วินาที และการบุกรุกในครั้งที่ 12 จะถูกหน่วงไป 14 วินาที และครั้งต่อไปจะถูกหน่วงไปทำนองนี้ และเมื่อไปถึงค่า hard limit (20) จะส่งผลให้ client ที่ มีพฤติกรรมไม่เหมาะสม (misbehaving client) ถูกตัดออกจากระบบ ในตัวอย่างค่า soft limit เป็น 10 และ hard limit เป็น 20 ซึ่งค่าดังกล่าวนี้สามารถเปลี่ยนแปลงได้ตามความเหมาะสม

การดำเนินการที่จะกล่าวต่อไปนี้จะเป็นการช่วยเซ็ตค่า soft limit และ hard limit สำหรับพารามิเตอร์การบุกรุก ให้คุณแก้ไขไฟล์ mail.cf และวางค่าการเซ็ตต่อไปนี้ลงไปในส่วนท้ายของไฟล์ ทำการคอนฟิกค่า hard limit เป็น 25 และ soft limit เป็น 15 และใช้ค่า delay เป็น 1 เมื่อทำเสร็จแล้วให้ติดต่อ Instructor ของคุณเพื่อทบทวนการเซ็ตค่าของคุณ

การกรองเนื้อความส่วนหัวและเนื้อความส่วนตัว (Filter header and body content)

Postfix มีออฟชันสำหรับการกรองสแปมของเมล์ขาเข้าด้วยการใช้ regular expressions นั่นคือเมล์จะถูกกรองก่อนที่จะถูกยอมรับโดย mail server เพื่อที่จะไม่ให้มีการใช้ทรัพยากรของ Server มาก กระบวนการกรองต้องทำการป้องข้อมูลเข้าไปในไฟล์ mail.cf จำนวน 2 บรรทัด โดยคุณไม่จำเป็นต้องใช้การกรองทั้งสองชนิด คุณอาจจะเลือกการกรองในส่วนของ header หรือ body เพียงอย่างใดอย่างหนึ่ง

header_checks = regexp:/etc/postfix/header_checks

body_checks = regexp:/etc/postfix/body_checks

การกรองทั้งสองชนิดดังกล่าวอ้างถึงไฟล์ที่ถูกวางอยู่ในไดเร็กทอรี่ /etc/postfix ไฟล์ดังกล่าวต้องถูกสร้างขึ้น โดยในไฟล์บรรจุด้วย regular expressions ที่จะใช้สำหรับ filter rule

การลดสแปมและการบุกรุกด้วยการจำกัด IP Address

พื้นฐานเบื้องหลังแนวคิดอันนี้ก็คือ เป็นไปได้ที่ช่วงของ IP Address บางช่วง ไม่จำเป็นต้อง access ไปยังเครือข่ายของคุณ เว้นเสียแต่หน่วยงานของคุณเป็นธุรกิจระหว่างประเทศ ด้วยการบล็อกช่วงไอพีของประเทศเหล่านี้จะสามารถทำให้คุณลดสแปมและ malware ลงไปได้ถึง 25% นอกจากนั้น การบล็อก IP address range ดังกล่าวนี้สามารถป้องกันไวรัสได้อีกด้วย เว็บไซต์ต่อไปนี้เป็น network subnet ของแต่ละประเทศ

http://ip.ludost.net

APNIC

Asian countries.

58.0.0.0/8

61.0.0.0/8

124.0.0.0/8

126.0.00/8

168.208.0.0/16

196.192.0.0/16

202.0.0.0/8

210.0.0.0/8

218.0.0.0/8

220.0.0.0/8

222.0.0.0/8

RIPE

Europe

80.0.0.0/8

81.0.0.0/8

82.0.0.0/8

83.0.0.0/8

84.0.0.0/8

85.0.0.0/8

86.0.0.0/8

87.0.0.0/8

88.0.0.0/8

89.0.0.0/8

90.0.0.0/8

91.0.0.0/8

193.0.0.0/8

194.0.0.0/8

195.0.0.0/8

212.0.0.0/8

213.0.0.0/8

217.0.0.0/8

AFRINIC

Africa

41.0.0.08

LACNIC

Brazil and Argentina

189.0.0.0/8

190.0.0.0/8

200.0.0.0/8

201.0.0.0/8

ในการใช้งานต้องมีการใช้คำสั่ง iptables ระบุ subnet ที่ต้องการจะ drop เช่นถ้าต้องการ drop เครือข่ายที่เป็น 201.0.0.0/8 ให้ใช้คำสั่ง iptables ดังนี้

iptables -A INPUT -s 201.0.0.0/8 -j DROP

หรือถ้าต้องการจำกัดการแอกเซสเฉพาะพอร์ต 80 ก็สามารถทำได้ด้วยการบล็อกพอร์ตอื่นทั้งหมด ดังนี้

iptables -A INPUT -s 201.0.0.0/8 -p tcp -dport ! 80 -j DROP

จบครับ