The Knowledge Center
นำเสนอหนังสือดี มีคุณค่า

ป้องกัน LINUX server อย่างมืออาชีพ

ถ่ายทอดประสบการณ์ตรงจากนักออกแบบระบบเครือข่ายคอมพิวเตอร์

สามารถนำไปใช้ได้กับ LINUX ทุกค่ายและทุก VERSION

- เรียนรู้วิธีป้องกันระบบเครือข่ายคอมพิวเตอร์ทุกรูปแบบ
- เข้าใจการบุกโจมตีของ HACKER เพื่อป้องกันเครือข่าย
- เทคนิคการเพิ่มประสิทธิภาพให้เครือข่ายของท่านอย่างง่ายๆ

พิเศษสุด แถมฟรี !
CD ประกอบการใช้งาน

บุญลือ อยู่คง

ป้องกัน LINUX SERVER อย่างมืออาชีพ

บุญลือ อยู่คง

คำนำสำนักพิมพ์

เมื่อคอมพิวเตอร์ หรือ สมองเทคโนฯ เกิดขึ้น ใครจะคิดว่ามันจะเป็นโรคได้ หมอคอมฯจึงต้องศึกษาค้นคว้าและพัฒนาวิธีบำบัดรักษาให้ทันการณ์ก่อนที่งานและเครือข่ายคอมฯ จะถูกทำลายล้างหมดสิ้น วิธีป้องกันและรักษาแบบเกลือจิ้มเกลือซึ่งคุณบุญลือ อยู่คงกำลังเผยแพร่อยู่นี้ นอกจากจะได้ผลชะงัดแล้วยังเป็นวิธีประหยัดชั้นเลิศ "ป้องกัน Linux Server อย่างมืออาชีพ" จะเป็นเครื่องมือและคู่มืออันมีค่าสำหรับผู้ดูแลระบบและผู้ที่มีเครื่องคอมพิวเตอร์ทุกท่าน ที่จะศึกษาปฏิบัติเฝ้าสังเกตและติดตามความเคลื่อนไหวของแฮคเกอร์ สามารถจัดการปราบปรามอย่างรู้เท่าทัน

ด้วยความปรารถนาดี

The Knowledge Center

คำนำผู้เขียน

หนังสือเล่มนี้เขียนขึ้นเพื่อใช้เป็นคู่มือสำหรับผู้ดูแลระบบ Linux OS ผู้อ่านบางคนที่ยังไม่มีความรู้ทางทฤษฎีเบื้องต้นเกี่ยวกับระบบเครือข่าย *(Networking System)* และการติดตั้ง Internet Server ด้วย Linux ซึ่งผู้เขียนได้พิมพ์เผยแพร่ไปแล้ว แต่อ่านบางเรื่องไม่เข้าใจหรือไม่รู้ว่าจะทำอย่างไร โปรดกลับไปทบทวนได้จากหนังสือดังกล่าว ประสบการณ์จากหนังสือเล่มที่แล้วพบว่า **"หนังสือเป็นสื่อชนิดหนึ่งที่ใช้ถ่ายทอดความรู้ประสบการณ์ของผู้เขียนสู่ผู้อ่าน"** แต่มิได้หมายความว่าเป็นสื่อที่ดีที่สุด บางท่านซื้อไปอ่านแล้วชอบ บางท่านอ่านแล้วไม่สบอารมณ์ เพราะไม่รู้เรื่องบ้างทำไม่ได้บ้าง ผมต้องขอเรียนท่านผู้อ่านให้ทราบก่อนว่า ผมไม่ใช่นักเขียนมืออาชีพ แต่เป็นนักปฏิบัติที่เขียนจากประสบการณ์ ที่ทำมากับมือ จึงถ่ายทอดอย่างตรงไปตรงมา บางตอนก็แปลจากเว็บไซต์ต่างประเทศ หรือใช้ตัวอย่างจาก Red Hat หรือแหล่งความรู้ที่อ้างอิงไว้ท้ายเล่ม เพื่อให้หนังสือมีที่มาที่ไป ไม่ใช่นั่งเทียนเขียน

มีคำพูดสืบต่อกันมาว่า ***"คนไทยหวงวิชา"*** แต่มาวันนี้ผมรู้แล้วครับว่าคนไทยไม่ได้หวงวิชาหรอกครับ แต่เขายังไม่รู้ เลยบอกใครไม่ได้ ผมลองศึกษาข้อความบนเว็บไซต์คนไทยที่แลกเปลี่ยนความรู้ในสาขาวิชาต่างๆ ก็พอจะสรุปได้ว่า ยังมีคนที่มีความรู้และประสบการณ์อีกมากมายที่พยายามจะถ่ายทอดสิ่งที่ตนรู้ บางครั้งไม่สามารถสอนให้ผู้อื่นปฏิบัติตามได้สำเร็จ และยังไม่มีการรวบรวมเนื้อหาเป็นขั้นตอน มีแต่บอกเล่าต่อๆกันมา ใครอยากทำก็ทำ ใครไม่อยากทำก็ไม่เป็นไร ผมเคยเข้ารับการอบรมในหน่วยงานบางแห่งที่นิยมจ้างวิทยากรจากบริษัทเอกชนมาสอนค่าสอนก็แพง แต่เวลาสอนกลับใช้หนังสือคู่มือมาอ่านให้ฟังวันละสามสี่บท พอถามอะไรมากหน่อย ก็จะได้รับคำตอบว่าต้องเอาไว้เรียนขั้นสูงกว่านี้จึงจะทำได้ ถามไปถามมาดูท่าคนสอนจะทำไม่เป็นมากกว่า แต่กลัวเสียเหลี่ยม ผมจึงเก็บความรู้สึกที่ติดลบนี้กลับไปศึกษาค้นคว้าด้วยตนเอง ทำอะไรได้ก็รวบรวมนำเสนอท่านผู้อ่านนี่แหละครับ ไม่ได้คิดเป็นเชิงพาณิชย์ แต่สำนักพิมพ์เขามีค่าใช้จ่ายจึงต้องมีราคาหนังสือเป็นธรรมดา

ขอบคุณผู้อ่านทุกท่าน และผู้มีส่วนร่วมในการให้กำลังใจผลักดันให้ผลงานชิ้นนี้สำเร็จลงได้ด้วยดี และขอขอบคุณ ผู้มีพระคุณทุกท่านที่ทำให้ผมเป็นคนมีจิตใจดีงามพอที่จะถ่ายทอดสิ่งดีๆ เพื่อให้ผู้อ่านนำไปใช้ทำงานสร้างสรรค์สังคมและประเทศชาติให้เจริญก้าวหน้า ไม่ต้องเป็นรองชาติอื่น วันหน้ามีประสบการณ์หรือความรู้ใหม่ที่น่าสนใจ ผมจะพยายามรวบรวมนำเสนอท่านทั้งหลายต่อไป

บุญลือ อยู่คง

สารบัญเรื่อง

สารบัญภาพ

CD

ประกอบด้วย linux Server Verion 2.01
พร้อมด้วยเครื่องมือที่ใช้ทำ Security ในแต่ละบท ได้แก่

- Sxid
- Logcheck
- Portsentry
- Webmin และตัวอย่าง Configuration ในการทำ Server

CHAPTER 1
ชนิดของการบุกโจมตี

วัตถุประสงค์

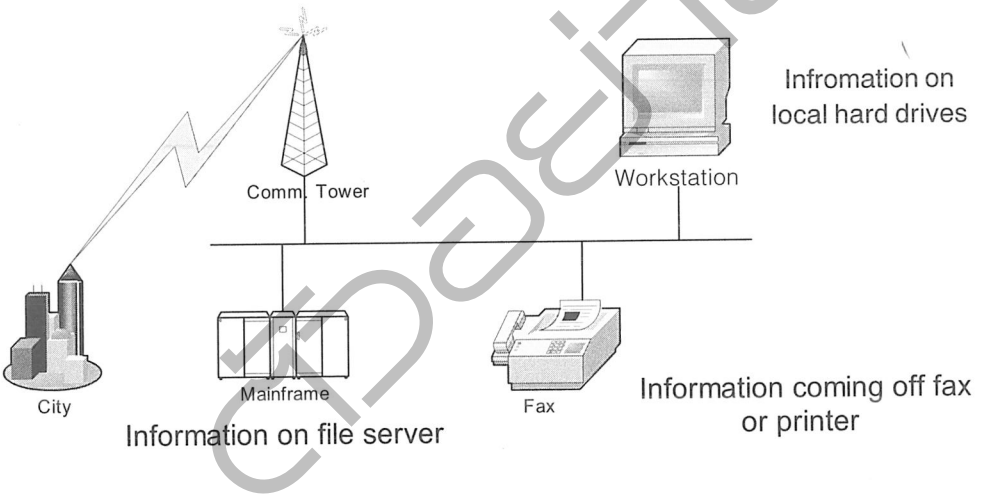
- เพื่อให้รู้จักลักษณะการบุกรุกของ Hacker ที่เข้าสู่ระบบเครือข่าย
- เพื่อให้เข้าใจประเภทของการบุกโจมตีที่เข้าถึงข้อมูล
- สามารถวิเคราะห์วิธีป้องกันระบบเครือข่ายได้อย่างถูกต้อง

เนื้อหาสาระ

ผู้ไม่ประสงค์ดีทั้งหลายในโลกมีมากมาย ต่างจิตต่างใจ แถมยังมีความสามารถส่วนบุคคลที่ไม่เท่าเทียมกันอีกด้วย ดังนั้น กรรมวิธีในการเจาะระบบของแต่ละคนก็ย่อมไม่เหมือนกันความหลากหลายดังกล่าว ทำให้เกิดผลเสียอันใหญ่หลวงกับ Server ทั้งสิ้น ไม่ว่าองค์กรหน่วยงานทั้งภาครัฐ และเอกชนในปัจจุบันกำลังมุ่งพัฒนาระบบ IT เพื่อเก็บข้อมูล เชื่อมโยงระบบเข้าหากัน หากไม่ศึกษาถึงปัญหาที่จะเกิดต่อไปนี้ ความสูญเสียก็จะประมาณค่าไม่ได้ ผู้ดูแลระบบที่ดีควรหมั่นศึกษาวิธีการบุกรุก วิธีการป้องกันและการเฝ้าระวังให้ละเอียด เพื่อจะได้ไม่ต้องคอยแก้ปัญหาที่ยุ่งยากในภายหลัง

การบุกรุกเข้าโจมตี server นั้นแบ่งได้เป็น 4 พวกใหญ่ ๆ ดังนี้

1. *Access Attacks* เป็นการบุกเข้าถึงข้อมูลใน Server ดังภาพ

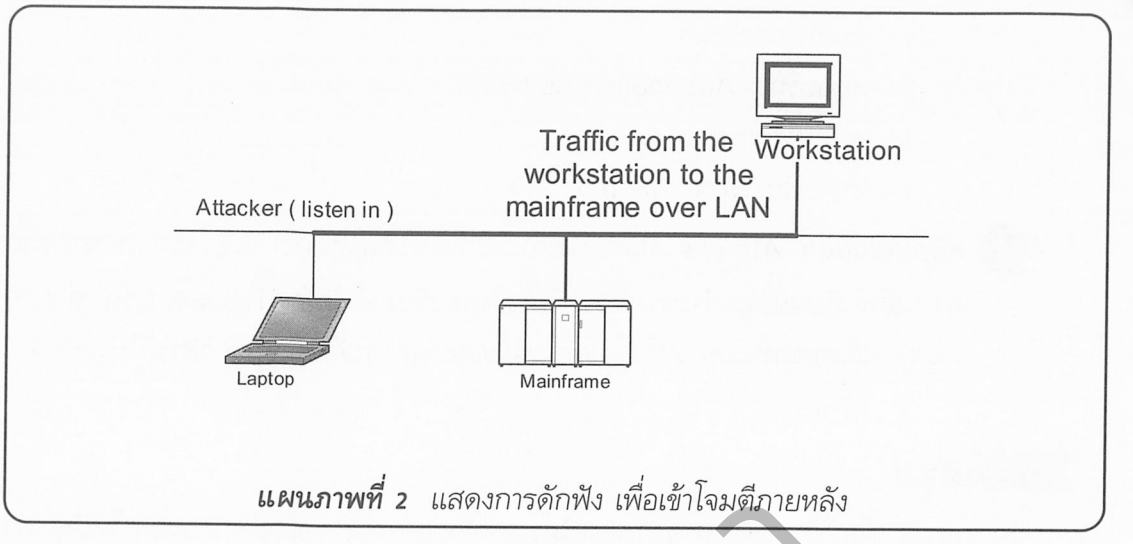


แผนภาพที่ 1 *แสดงการบุกเข้าถึงข้อมูลในเซิร์ฟเวอร์*

ลักษณะของการโจมตีมีชื่อเรียกต่าง ๆ กันออกไปดังนี้

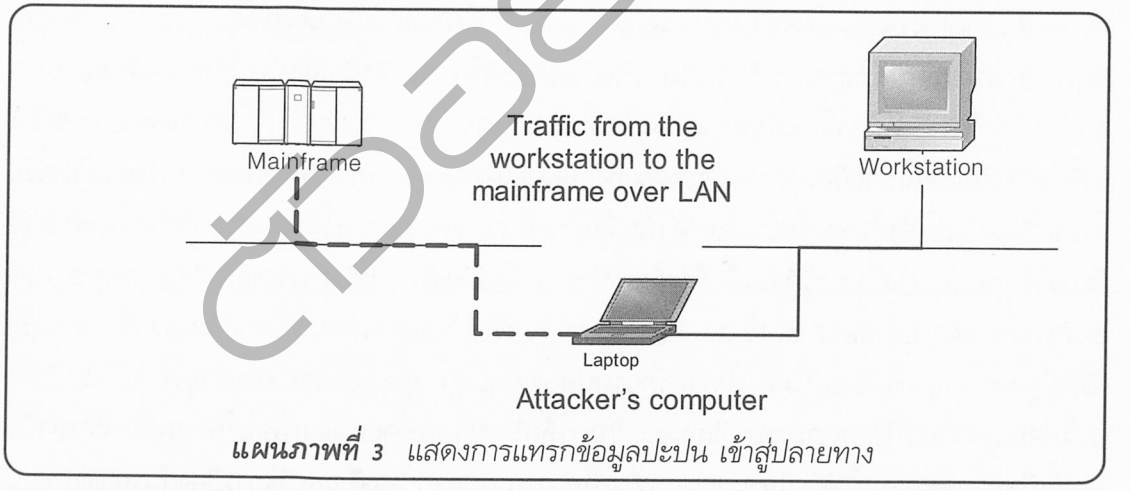
1.1 *Snooping* มีลักษณะการบุกรุกเข้ามาดูข้อมูล หรือค้นหาข้อมูลส่วนสำคัญที่อยู่ภายใน server

1.2 *Eavesdropping* มีลักษณะเหมือนการเฝ้าดักฟัง (Listen) เพื่อรอข้อมูลสำคัญแล้วทำการระบุตำแหน่งข้อมูลเพื่อเข้าโจมตีด้วยวิธีอื่นในภายหลัง ดังภาพ



แผนภาพที่ 2 *แสดงการดักฟัง เพื่อเข้าโจมตีภายหลัง*

1.3 *Interception* มีลักษณะตรงข้ามกับแบบ Eavesdropping ตรงที่แบบ Interception จะดักรอจนถึงข้อมูลสำคัญก่อนจะแทรกข้อมูลของผู้บุกรุกปนเข้าไปแล้วจึงส่งให้ข้อมูลเคลื่อนต่อไปยังปลายทางดังภาพ



แผนภาพที่ 3 *แสดงการแทรกข้อมูลปะปน เข้าสู่ปลายทาง*

2. ***Modification Attacks*** ชื่อก็บอกอยู่แล้วครับว่าต้องบุกเข้ามา เพื่อเปลี่ยนแปลง แทรก และลบข้อมูลใน Server แน่นอน การโจมตีแบบนี้มักพบบ่อยมาก

3. ***Denial of Service Attacks (DoS)*** เป็นการโจมตีเพื่อให้ server หยุดให้บริการในส่วนสำคัญต่าง ๆ หรือที่เข้าใจกันว่า Server hang หยุดให้บริการ อาจเป็นบางอย่างหรือหลายอย่างก็ได้ บางตำราเขียนว่า DoS สามารถหยุดบริการหลายรูปแบบเช่น

3.1 หยุดบริการข้อมูล

3.2 หยุดบริการ Application Software

3.3 หยุดบริการระบบ

3.4 หยุดบริการด้านการสื่อสาร

4. ***Repudiation Attacks*** มีลักษณะการเข้าโจมตีเพื่อให้เกิดการปฏิเสธการทำงานหรือการแลกเปลี่ยนข้อมูลข่าวสาร หากมีการร้องขอข้อมูลเพื่อทำ Transaction ต่าง ๆ ก็จะถูกปฏิเสธจากระบบ ทำให้การทำงานผิดพลาดหรือได้รับข้อมูลข่าวสารที่ไม่ถูกต้อง

บทสรุป

การที่เทคโนโลยีมีการพัฒนาอย่างต่อเนื่องและก้าวไปอย่างรวดเร็ว ส่งผลทำให้เกิดการเปลี่ยนแปลงรูปแบบ การจัดการข้อมูลข่าวสารในระบบขององค์กรและหน่วยงานต่างๆเป็นอย่างมาก ในปัจจุบันการเชื่อมโยงข้อมูลข่าวสารสามารถกระทำการเชื่อมโยงถึงกันได้ทั่วโลก เป็นผลให้การติดต่อสื่อสารสะดวกรวดเร็ว และยังประหยัดงบประมาณตลอดจนคนงานลงได้มาก สิ่งนี้อาจมองเห็นว่ามีประโยชน์อย่างมหาศาล แต่ในทางกลับกันถ้ามองในด้านลบคงหนีไม่พ้นผู้ที่คอยจ้องทำลาย เจาะระบบเครือข่ายเพื่อเข้ามาทำประโยชน์ในทางตรงกันข้ามเช่น เข้าไปแก้ไขข้อมูลสำคัญ เข้าไปชะลอหรือหยุดบริการบางอย่างให้เกิดการทำงานผิดพลาดในแต่ละส่วนงาน สิ่งต่างๆเหล่านี้เป็นผลเสียอย่างมาก จนปัจจุบันมีการวิเคราะห์ผลเสียหายออกเป็นตัวเลขเงินตราแต่ละประเทศ และได้พยายามสร้างเครื่องมือ เพื่อเป็นเกราะป้องกันระบบของตนเองอย่างเต็มความสามารถ แต่ทุกคนต้องเข้าใจตรงกันครับว่าเทคโนโลยีเป็นสิ่งที่มนุษย์สร้างขึ้น ดังนั้นจึงมีช่องโหว่ และช่องว่างในส่วนต่างๆที่เกิดขึ้นหลังจากมีการใช้งานแล้ว ผู้สร้างจะรู้ก็ต่อเมื่อมีผู้เข้ามาทำลาย จึงเกิดบริการหลังการขายทั้ง Hardware และ Software เพื่อ Update Service Pack ต่าง ๆ เพื่อแก้ปัญหาให้ทันสมัยอยู่ตลอดเวลา หากคุณเป็นผู้ดูแลระบบเครือข่ายที่ไม่สนใจเรื่องความปลอดภัยแล้ว คุณจะต้องทำงานหนักมาก และหนักจนไม่อยากทำเลยก็ได้ เพราะระบบที่ถูกเจาะเข้ามาได้สร้างปัญหาที่คุณอาจแก้ไขไม่ได้เลยก็มี ในหนังสือเล่มนี้เป็นการเสนอแนะให้ผู้ดูแลระบบมองเห็นภาพ การถูกบุกรุก โจมตี และวิธีการป้องกันในแต่ละส่วน ซึ่งเป็นวิธีที่ประหยัดที่สุดเพราะกระทำกับ Software ทั้งหมดที่ไม่ต้องซื้อหา ไม่มีค่าใช้จ่าย หากทำได้ดีประสบความสำเร็จก็จะได้ประโยชน์อย่างมหาศาล

CHAPTER 2
การออกแบบระบบป้องกัน

วัตถุประสงค์

- เพื่อให้รู้จักการออกแบบระบบป้องกันให้กับ Internet Server
- เพื่อให้เข้าใจลักษณะโครงสร้างการวางระบบป้องกัน
- เพื่อให้รู้จักวิธีการและช่องทางการบุกรุกเข้า Server
- เพื่อให้เข้าใจวิธีป้องกันระบบ Internet Server

เนื้อหาสาระ

ปัจจุบันพบว่ามีการประชาสัมพันธ์ข่าวสารกันมากมายเกี่ยวกับ การบุกโจมตีระบบเครือข่ายคอมพิวเตอร์ ด้วยวิธีการต่าง ๆ นานา และก็อีกเช่นกันที่ตามแผงหนังสือก็มีการแปลออกวางจำหน่ายกันเต็มไปหมด หากคุณไม่ได้ศึกษาความเป็นมาก็จะไม่ทราบวิธีป้องกัน เป็นเพียงรู้ว่าผู้บุกรุกจะมาได้ทางไหนอย่างไรเท่านั้น บางตำราเขียนถึงวิธีการป้องกันด้วยการ Configure ที่ Router เป็นด่านแรกไว้ก่อน แต่คงไม่คิดว่ายังมีผู้ดูแลอีกมากมายที่ต้องจ้างบริษัทที่จำหน่าย Router ให้ทำ Configurationให้เลย อาจดูเป็นวิธีที่ยากไปสักหน่อย

ดังนั้นผู้เขียนจึงใคร่ขอแนะนำหลักและวิธีการต่างๆที่ชาวต่างชาติเขามีกัน และ เราทำได้ง่ายๆด้วยตัวเราเอง ที่เครื่อง Server บน Linux OS ที่แข็งแรง ก็น่าจะเป็นวิธีการอย่างประหยัดและง่ายสำหรับผู้ดูแลระบบที่ใช้ Linux ทำ Internet Server ในประเทศไทยได้อย่างมาก

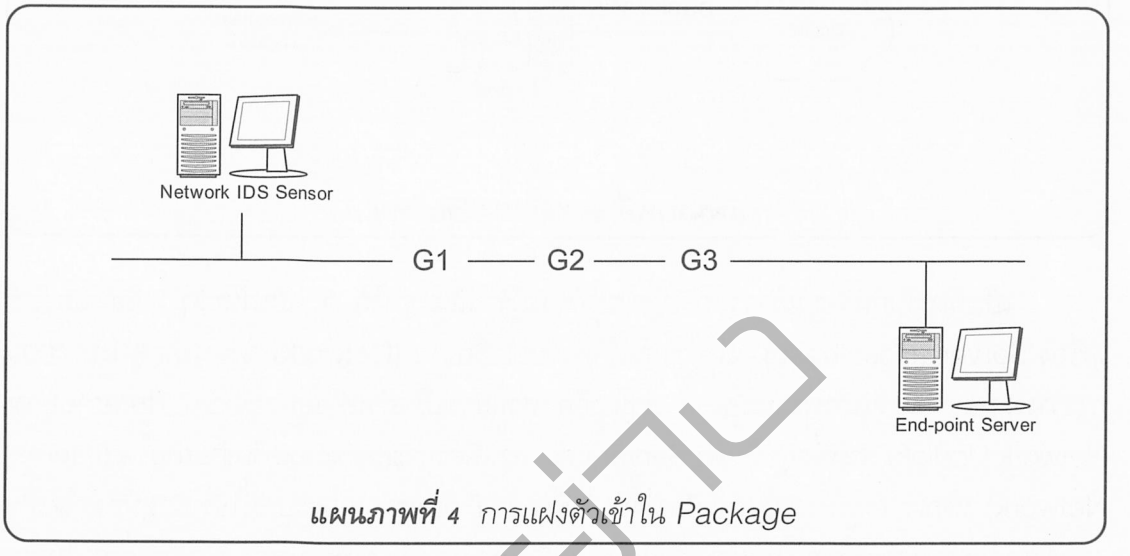
พื้นฐานการดูแลรักษาหรือป้องกันระบบเครือข่ายคอมพิวเตอร์นั้น ควรมีขั้นตอนในการทำงานที่ถูกต้อง และรัดกุม เปรียบเสมือนตำรวจวางแผนการป้องกันโจรผู้ร้ายปล้นธนาคาร ถ้ามีขั้นตอนใดขั้นตอนหนึ่งขาดหายไปหรือสลับขั้นตอน ก็อาจก่อให้เกิดความเสียหายกับระบบโดยรวมได้และอาจสร้างปัญหาอันซับซ้อนจนกระทั่งคุณไม่อาจสามารถวิเคราะห์แก้ไขปัญหานั้นได้ ทั้งนี้สืบเนื่องมาจากขั้นตอนการเกิดปัญหาไม่เป็นไปตามเงื่อนไขที่วางไว้ พื้นฐานการดูแลรักษาหรือป้องกันระบบเครือข่ายมีขั้นตอนพื้นฐานอย่างง่ายอยู่ 3 ขั้นดังนี้

1. ***ขั้นตอนการตรวจสอบความปลอดภัยของระบบ (Security Audit)***
2. ***ขั้นตรวจสอบผู้บุกรุก (Intrusion Detection System: IDS)***
3. ***ขั้นการป้องกันการบุกรุก (Firewall)***

รายละเอียดในทางทฤษฎีมีหนังสือของชาวต่างชาติเขาพิมพ์ขายกันเล่มโต ๆ หนา ๆ หาอ่านกันเองนะครับ ผมไม่ชอบเขียนตำราที่มีขนาดใหญ่ ดูแล้วมีค่ามากไปไม่น่าอ่าน ในที่นี้จะขอแนะนำวิธีป้องกันระบบในแต่ละรูปแบบ ให้ผู้ดูแลระบบเลือกนำไปใช้เท่าที่เข้าใจและสามารถนำไปใช้ในระบบที่มีอยู่จริงดังต่อไปนี้

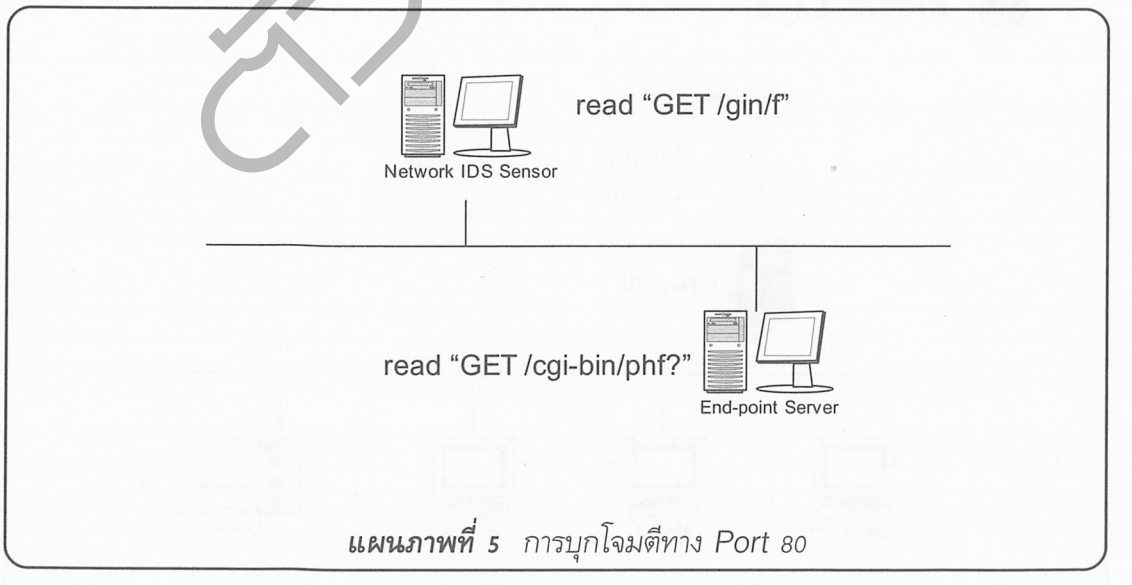
การบุกรุกระบบเครือข่ายที่พบในปัจจุบันมี 2 แบบ คือ

1. ***Insertion Attack*** เป็นวิธีการแฝงหรือแทรกตัวปนมากับ Package ที่กำลังรับ-ส่งในระบบ



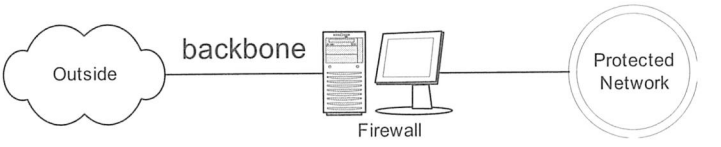
แผนภาพที่ 4 *การแฝงตัวเข้าใน Package*

2. ***Evasion Attack*** เป็นการบุกโจมตีทาง Port 80 ในส่วน cgi-bin ด้วยคำสั่ง Read/Get แบบนี้ในอดีตพบกันมากแต่ในปัจจุบัน Apache ได้ปรับปรุงแก้ปัญหาให้แล้วครับ



แผนภาพที่ 5 *การบุกโจมตีทาง Port 80*

หลักการ Firewall

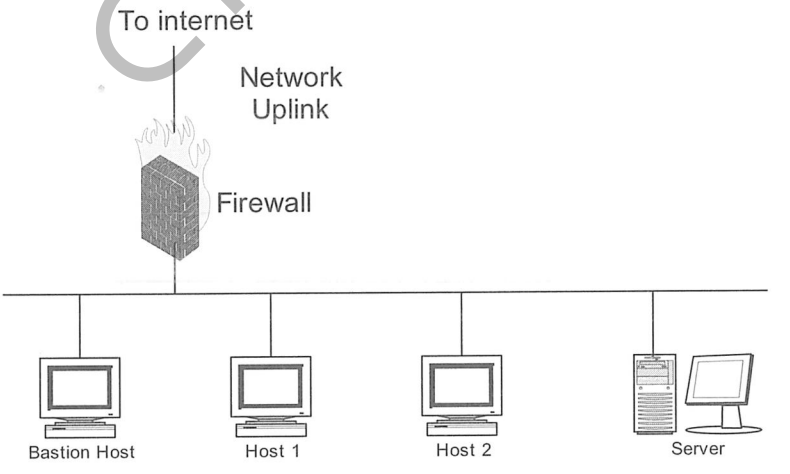


แผนภาพที่ 6 *หลักการ Firewall*

เป็นที่ทราบกันดีอยู่แล้วว่า การบุกโจมตีของผู้ร้ายนั้น ทำได้ 2 แบบใหญ่ๆ คือ บุกเข้าที่เครื่อง Server (Host-base) และการบุกเข้าที่ระบบเครือข่าย (Network) ดังนั้นหากดูผังประกอบการวางระบบ ก็จะเห็นภาพรวมเป็น 3 ส่วน คือ ส่วนแรกเป็นส่วนที่อยู่นอกระบบ (Internet or Network Up link) ส่วนที่สองเป็นตัว Server และ ส่วนที่สามจะเป็นระบบเครือข่ายภายใน (Internal Network) หากเราจัดเรียงระบบการป้องกัน ที่เรียกว่า Firewall จากระบบที่ใช้งานอยู่นี้ก็จะได้เป็น 6 รูปแบบและสามารถเลือกโปรแกรมที่ Linux OS มีมาให้ จัดการกำหนดค่า Configure ให้ตรงตามวัตถุประสงค์ของผู้ดูแลระบบ

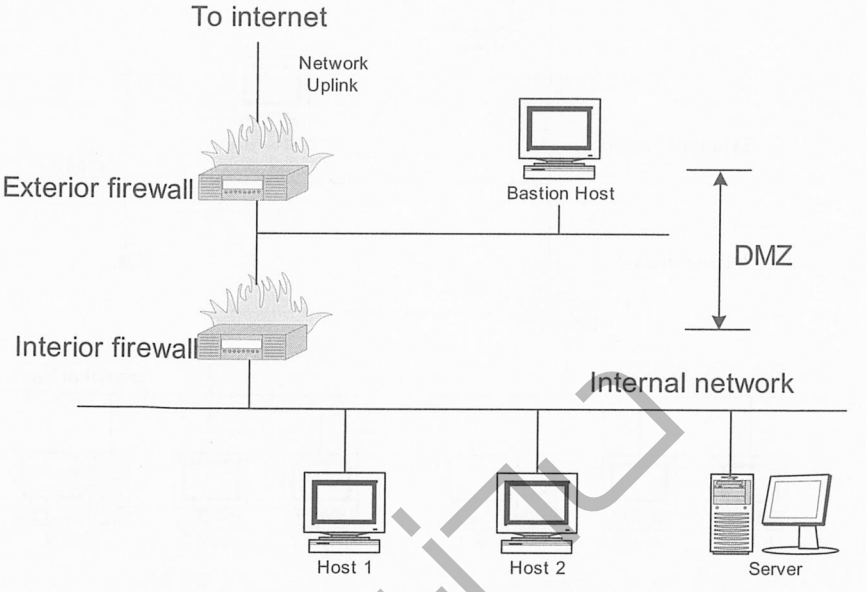
ในส่วนของสถาปัตยกรรมในการป้องกันระบบทำได้ 6 แบบ ดังต่อไปนี้

1. *Single Layer*



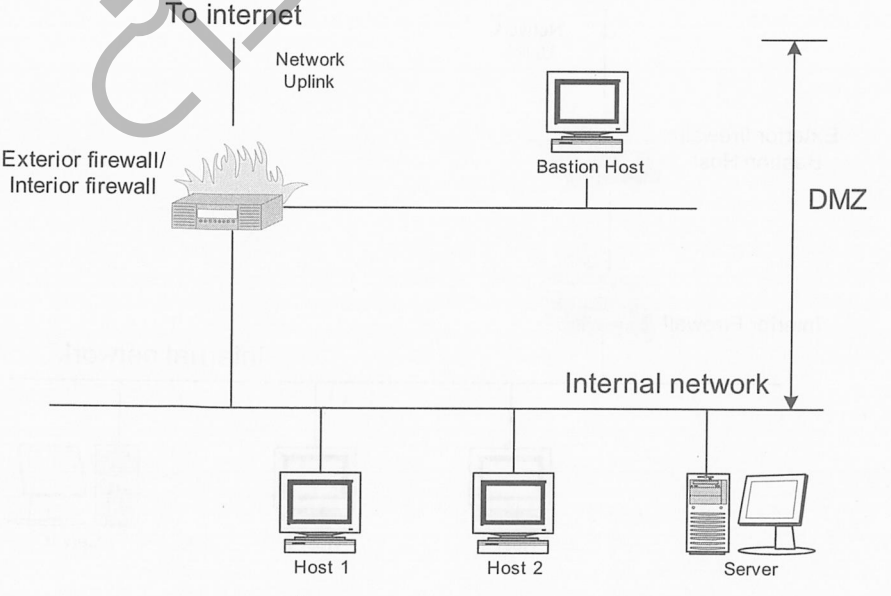
แผนภาพที่ 7 *การทำ Configure Firewall (1)*

2. Two Layer



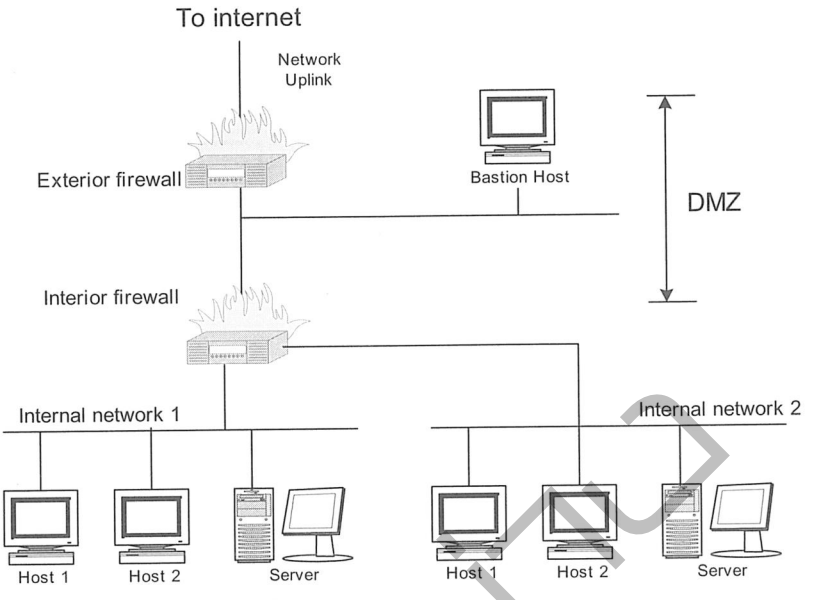
แผนภาพที่ 8 การทำ Configure Firewall (2)

3. Merge Interior & Exterior



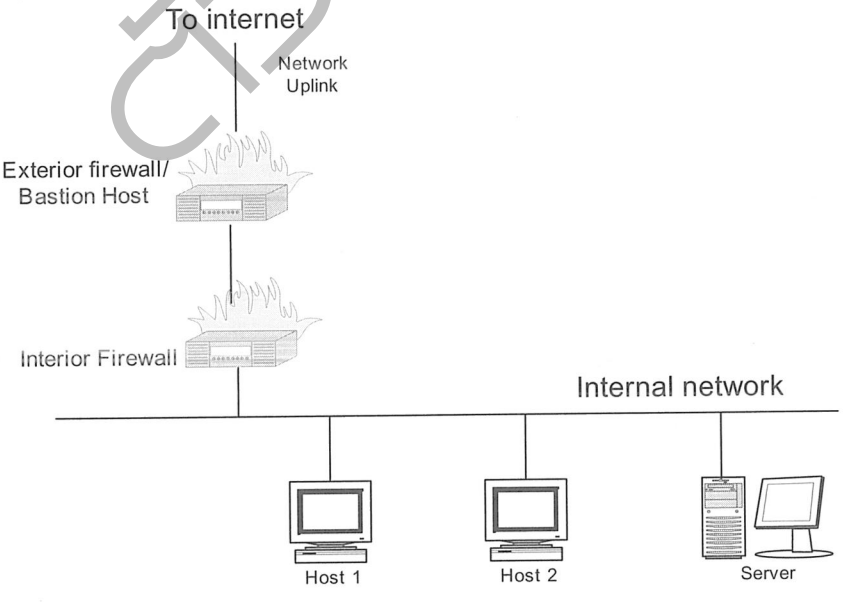
แผนภาพที่ 9 การทำ Configure Firewall (3)

4. Two Layer with two internal network



แผนภาพที่ 10 การทำ Configure Firewall (4)

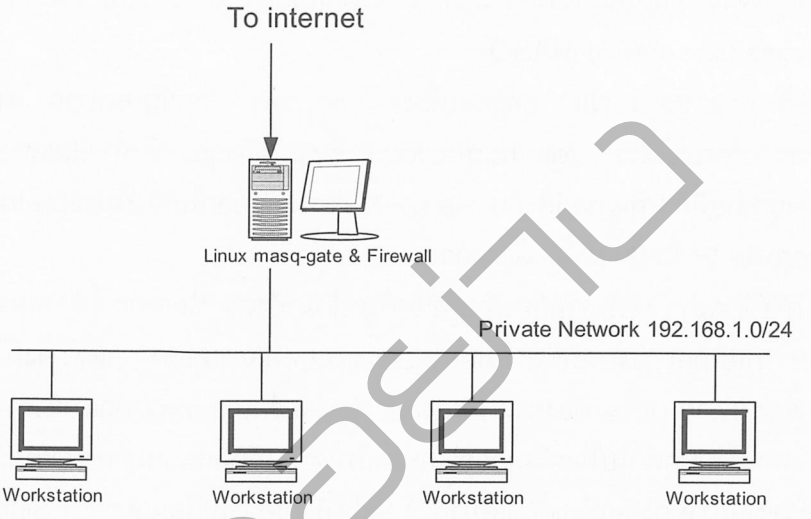
5. Two Layer with merge Bastion Host & Exterior



แผนภาพที่ 11 การทำ Configure Firewall (5)

ทั้ง 5 แบบที่กล่าวมาแล้วจะเป็นการทำ Configuration firewall บนอุปกรณ์ ที่ทำหน้าที่ Gateway ของระบบส่วนใหญ่เป็น Router หรือ Manage Switch บางรุ่นที่มี Option Firewall ด้วย เป็นระบบที่กำลังนิยมในปัจจุบันซึ่งมีค่าใช้จ่ายสูง หากระบบของคุณต้องการที่จะลดต้นทุนในการทำระบบ firewall ให้ใช้วิธีการตามแบบที่ 6

6. *Masquerade Network (Gateway Server)*



แผนภาพที่ 12 *การทำ Configure Firewall (6)*

ภาพนี้คงคุ้นเคยกันมากในวงการทำ Firewall บ้านเรานะครับ เพราะเป็นระบบที่ได้รับความนิยมกันมาก หาคู่มือหรือตำราอ่านและทำตามกันได้ การจัดวงจรแบบนี้เรียกว่า Gateway Server หมายถึงการออกแบบให้เครื่อง Server ทำหน้าที่เป็นประตูออกสู่ระบบ Internet สามารถสั่งให้ปิดเปิด port ต่าง ๆ และคอยควบคุมการเข้าออกของลูกข่ายที่จะเชื่อมต่อไปยังภายนอกและควบคุมผู้ที่อยู่นอกระบบ บุกรุกเข้าหาเครื่องลูกข่ายภายในอีกด้วย ลักษณะนี้จะมีข้อดีคือ สามารถควบคุมได้ด้วยการ Configure ให้กับโปรแกรมที่มีมากับ Linux เช่น ipchains, iptables สามารถป้องกันภัยร้ายต่าง ๆ จากภายนอกไม่ให้บุกรุกถึงเครื่องลูกข่ายภายใน (Internal Network) ได้ สิ่งที่น่าเป็นห่วงอย่างมากคือ ยังมีผู้ดูแลระบบจำนวนมากพยายามจัดวางรูปแบบ Network ให้เป็น Gateway Server แต่มี NIC (Network Interface Card) แผ่นเดียวแล้วใช้วิธีการทำ IP Aliases ออก Private IP ขึ้นมาแล้ว ไปกำหนดให้เครื่องลูกใช้ Private IP ผู้ควบคุมก็ทำ Firewall ด้วยการทำ IP Masquerade พบว่ายังถูกผู้บุกรุกจากภายนอกเข้าโจมตีเครื่องลูกข่ายได้อย่างง่ายดาย ที่เป็นเช่นนี้เพราะคุณใช้ gateway ระหว่าง Public IP กับ Private IP เป็นตัวเดียวกัน ใช้อุปกรณ์

กระจายสัญญาณ (HUB or Switch) ตัวเดียวกัน จึงถูกโจมตีได้ตลอดเวลา แล้วยังมีการกล่าวหาว่าโปรแกรม Firewall ที่ใช้อยู่ไม่แข็งแรงพอที่จะรับมือกับผู้บุกรุก แท้ที่จริงแล้วเป็นเพราะคุณมองภาพการออกแบบระบบประหยัดเกินไป การบุกรุกเข้าหาเครื่องลูกข่ายมีด้วยกันหลายทาง หลาย Protocol ไม่ใช่เรื่องง่ายหากทำ Network ที่ไม่ดีพอหรือพูดให้เข้าใจง่ายก็คือ ไม่แยกระหว่าง Public IP กับ Private IP ให้ขาดออกจากกันอย่างเด็ดขาด ก็ไม่สามารถจะดูแลความปลอดภัยได้เต็มร้อยอย่างแน่นอน ดังนั้นคุณควรใส่ NIC อย่างน้อย 2 แผ่น เพื่อแยกกันระหว่างคนในกับคนนอกให้ชัดเจนแล้วจึงค่อยลงมือหาโปรแกรมที่ใช้ทำ Firewall มาทำ Configuration ให้ดีและครอบคลุมตามที่คุณต้องการ *ตัวอย่างนี้เป็นสิ่งที่คุณคุ้นเคยเป็นอย่างมากสำหรับการ Configure ให้กับระบบ /sbin/ipchains -A forward -s 192.168.1.0/24 -j MASQ*

ภายหลังติดตั้งระบบที่มี NIC สองแผ่นขึ้นไปมักมีการทำ Configuration ให้ระบบด้วยคำสั่งง่าย ๆ ดังตัวอย่างข้างบนใส่ไว้ใน /etc/rc.d/rc.local ซึ่งหมายถึงคุณกำลังทำ Gateway Server ที่อนุญาตให้เครื่องลูกข่ายที่มี Private IP 192.168.1.0-255 สามารถออกไปท่องในระบบ Internet ได้ด้วยวิธี Masquerade IP ซึ่งเป็นวิธีที่ถูกต้องแล้ว

แต่การทำวิธีดังกล่าวไม่สามารถป้องกันผู้อื่นบุกรุกเข้ามายังตัว Server ได้ เนื่องจาก NIC แผ่นที่เชื่อมต่อกับ Internet ยังคงเป็นตัวสัมผัสโดยตรงกับบุคคลภายนอก แต่ถ้าจะมีใครบุกจากภายนอกเข้าหาเครื่องลูกข่ายภายใน ต้องผ่าน Firewall ก่อน เปรียบเสมือนว่าคุณกำลังทำการป้องกันขาเดียว คือป้องกันคนนอกบุกเข้าไปในเครือข่ายภายในแต่ไม่ได้ป้องกันคนนอกบุกเข้าทำลายตัว Server อาจมองอีกมุมได้ว่าเป็นการป้องกันเพียงครึ่งเดียวก็ได้ ทำให้มีลักษณะเหมือนแบบที่ 1 Single Layer

อธิบายหลักการแบบชาวบ้านแบบไม่เป็นภาษาวิชาการได้ว่า คนนอกและบริการ Internet ต่าง ๆ สามารถเข้ามารอที่ eth0 ได้เท่านั้นแล้วให้รออยู่ในส่วนห้องรับแขกส่วนคนในจะออกไปท่อง Internet ก็ต้องออกมารอที่ eth1 ส่งสัญญาณร้องขอบริการออกไปก็จะไปรับบริการได้ที่ห้องรับแขก (โดยมี eth0 ไปรับมาให้) มองภาพให้ออกว่าการทำ Firewall เป็นระบบการป้องกันที่คนนอกและคนในระบบจะพบกันได้ ต้องเป็นไปตามกฎที่ผู้ดูแลระบบตั้งให้เท่านั้น

บทสรุป

ปัญหาที่พบบ่อยคือเครื่องที่อยู่ภายในจะปลอดภัยเพียงระยะหนึ่งเท่านั้น เพราะถ้าผู้บุกรุกสามารถบุกเข้าที่ Server ได้เขาก็จะรู้ข้อมูลระบบว่าใครอยู่ที่ไหน กำลังทำอะไร คราวนี้ก็จะใช้การบุกจากตัว Server เข้าหาลูกข่ายภายในอีกต่อหนึ่งแล้ว ระบบก็จะถูกทำลาย ซึ่งดูภาพรวมแบบนี้แล้วไม่ใช่วิธีการทำ Masquerade Gateway ไม่ดีนะครับ เพียงแต่คุณต้อง Configure ให้ Firewall เต็มรูปแบบจึงจะช่วยป้องกัน Server ด้วยอีกทางครับ จะทำให้ได้รูปแบบที่ 2-5 สำหรับการทำ Configuration อย่างละเอียดให้ดูได้ในบทที่เกี่ยวกับการทำ Firewall (ipchains, iptables)

หมวดคอมพิวเตอร์

เหมาะสำหรับ

ผู้ดูแลระบบ INTERNET SERVER
โปรแกรมเมอร์
WEBMASTER
ผู้ใช้ระบบ LINUX

ผู้ไม่ประสงค์ดีทั้งหลายในโลกมีมากมาย ต่างจิตต่างใจ
แถมยังมีความสามารถส่วนบุคคลที่ไม่เท่าเทียมกันอีกด้วย
ดังนั้น กรรมวิธีในการเจาะระบบของแต่ละคนก็ย่อมไม่เหมือนกัน
ความหลากหลายดังกล่าว ทำให้เกิดผลเสียอันใหญ่หลวงกับ SERVER ทั้งสิ้น
ไม่ว่าองค์กร หน่วยงานทั้งภาครัฐและเอกชน
ในปัจจุบันกำลังมุ่งพัฒนาระบบ IT เพื่อเก็บข้อมูล เชื่อมโยงระบบเข้าหากัน
หากไม่ศึกษาถึงปัญหาที่จะเกิดขึ้นต่อไปนี้
ความสูญเสียก็จะประมาณค่าไม่ได้
ผู้ดูแลระบบที่ดี ควรหมั่นศึกษาวิธีการบุกรุก
วิธีการป้องกัน และการเฝ้าระวังให้ละเอียด
เพื่อจะได้ไม่ต้องคอยแก้ปัญหาที่ยุ่งยากในภายหลัง

ป้องกัน LINUX SERVER
อย่างมืออาชีพ

The Knowledge Center
นำเสนอหนังสือดี มีคุณค่า