Advanced Linux Firewall Workshop 20 Hrs.

จุดประสงค์ของหลักสูตร

1. เพื่อให้เกิดความเข้าใจถึงหลักการ ทฤษฎีและแนวปฏิบัติเกี่ยวกับการทำงานของไฟร์วอลล์
2. เพื่อให้สามารถออกแบบติดตั้ง บริหารจัดการและแก้ไขปัญหาระบบไฟร์วอลล์ในเครือข่ายได้
3. เพื่อให้สามารถนำความรู้ที่ได้ไปใช้ศึกษาระบบไฟร์วอลล์ได้ในอนาคต

Part I : Fundamental Conceptual and Skill Improvement

เนื้อหาส่วนนี้จะสร้างความรู้ทั้งด้านทฤษฎีและความสามารถทักษะการปฏิบัติงานที่เกี่ยวข้องกับการออกแบบ ลงมือติดตั้งและคอนฟิกระบบไฟร์วอลล์ โดยเน้นที่หลักการแนวคิดที่เป็นระบบ ซึ่งเป็นปัจจัยสำคัญต่อการประยุกต์ใช้งาน การวิเคราะห์ออกแบบระบบ การวินิจฉัยปัญหา และการศึกษาเกี่ยวกับเทคโนโลยีไฟร์วอลล์ในอนาคตต่อไป

- **ทฤษฎี แนวคิดสำคัญ หลักการทำงานของไฟร์วอลล์และ** iptables
  หลักปฏิบัติที่นำไปสู่ขั้นตอนมาตรฐานในการดำเนินการเกี่ยวกับการกำหนดนโยบาย และเงื่อนไขของไฟร์วอลล์ รวมไปถึงข้อจำกัดต่างๆ ที่ควรระมัดระวังขณะปฏิบัติงานกับระบบไฟร์วอลล์
- **ศึกษาคำสั่งกำหนดนโยบายและเงื่อนไขของ** iptables
  ศึกษากลไกการสื่อสารที่สำคัญของโปรโตคอล TCP/IP โดยแบ่งออกเป็นโปรโตคอลย่อยๆ และผลการทำงานของแต่ละโปรโตคอลนั้นโดยละเอียด
- **ฝึกปฏิบัติการใช้งาน** iptables **ในฐานะ** Packet filter
  เป็นการทดลองปฏิบัติเพื่อความเข้าใจถึงโครงสร้างภายในของระบบที่ชัดเจน ความสัมพันธ์ระหว่างองค์ประกอบแต่ละส่วน ผลลัพธ์ของแต่ละคีย์เวิร์ดภายในคำสั่งและการใช้งานอย่างถูกต้อง ตลอดจนการถ่ายทอดแนวคิดมาสู่การปฏิบัติให้เห็นผลจริง
- **การใช้งาน** Port Scanner
  เพื่อตรวจสอบทั้งก่อนและหลังการป้องกันด้วยไฟร์วอลล์ ทั้งการใช้งานปรกติและอาศัยเทคนิคพิเศษชนิดต่างๆ ในการแสกนพอร์ต
- **ฝึกปฏิบัติการใช้งาน** iptables **ในฐานะ** Stateful Firewall
  โดยมีการทำงานแบบ Connection Tracking ช่วยให้มีความเชื่อถือกันระหว่างโฮสต์สูงยิ่งขึ้น เนื่องจากมีการติดตามความต่อเนื่องตลอดกระบวนการตั้งแต่เริ่มต้นจนสิ้นสุดการสื่อสาร
- **โมดูลคุณสมบัติเสริมการใช้งานที่สำคัญของ** iptables
  ที่นอกเหนือจากคุณสมบัติหลัก ได้แก่ การมาร์กแฟลกเพื่อควบคุมแบนด์วิธ การเก็บบันทึกการโจมตีหรือสิ่งแปลกปลอม การจำกัดความถี่ของการโจมตี และโมดูลช่วยอำนวยความสะดวกในการจัดการแพคเก็ต
- **การใช้งาน** iptables **ในลักษณะ** bastion host
  หมายถึงการป้องกันรักษาความปลอดภัยในระดับโฮสต์ผู้ให้บริการทุกประเภท เช่น Web Server ,FTP Server ,SQL Server เป็นต้น ซึ่งถือว่าเป็นงานระดับมาตรฐานที่ผู้บริหารระบบต้องจัดให้มีในทุกเซิร์ฟเวอร์
- **ฝึกการเขียนสคริปต์** iptables **ด้วยตนเอง**
  ซึ่งจะช่วยให้เกิดความเข้าใจที่ชัดเจนในการนำชุดคำสั่งของ iptables ไปใช้งานจริง การดีบั๊กค้นหาข้อบกพร่องของเงื่อนไข ซึ่งมีประโยชน์มากต่อการทำความเข้าใจโปรแกรมบริหารจัดการไฟร์วอลล์สำเร็จรูปในลำดับต่อไป

48/145 Soi Nawamin 157, Nawamin Rd, Klongkoom, Bungkoom, Bangkok 10230 Tel. 0-2509-8444, 0-2509-0484 Fax. 02-509-0485

Part II : Network Security Infrastructure and Hardened Environment

ศึกษาการออกแบบระบบเครือข่ายเพื่อให้มีโครงสร้างที่เหมาะสมกับสภาพแวดล้อมการใช้งานโดยคำนึงถึงความปลอดภัยเป็นสำคัญ โดยมุ่งเน้นให้ผู้ฝึกอบรมได้ลงมือปฏิบัติและเข้าใจสภาพที่แท้จริงในการจัดตั้งเซิร์ฟเวอร์ การเชื่อมต่อและการจัดเครือข่ายย่อยภายในองค์กรอย่างเป็นระบบ สภาพจำลองที่สร้างขึ้นตามหลักสูตรนี้จะช่วยให้เกิดการเรียนรู้และเสริมประสบการณ์ให้แก่ผู้อบรมเพื่อความพร้อมที่จะนำไปปฏิบัติงานจริงอย่างได้ผล

- **ทฤษฎีและหลักการทำงานของ NAT และ DMZ**
  ศึกษาการทำงานของ NAT (Network Address Translation) ในลักษณะต่างๆ ได้แก่ SNAT และ DNAT โครงสร้างเครือข่ายในรูปแบบของ DMZ (Demilitarized Zone) แบบต่างๆ พิจารณาข้อดีข้อเสีย และข้อจำกัดของโครงสร้างแต่ละชนิด
- **การติดตั้งเครื่องพีซีลีนุกซ์เป็น Firewall / Router**
  เป็นขั้นตอนพื้นฐานสำคัญเพื่อการคอนฟิกเครื่องพีซีเป็นเร้าเต้อร์และไฟร์วอลล์ ได้แก่ การเพิ่มแลนการ์ด การเปิดคุณสมบัติด้าน IP Forwarding และ การบริหาร Kernel Routing Table
- **การสร้าง DMZ แบบ Semi-safe**
  เป็นรูปแบบของ DMZ ที่เน้นความประหยัดและง่ายต่อการบำรุงรักษา การทดลองนี้จะช่วยให้เกิดความเข้าใจและสร้างทักษะขั้นพื้นฐานได้อย่างรวดเร็วที่สุด
- **การทำ Virtual Server ไว้เบื้องหลังไฟร์วอลล์**
  เป็นการประยุกต์การทำงานแบบ DNAT เพื่อสนับสนุนการซ่อนเครื่องเซิร์ฟเวอร์ไว้เบื้องหลังไฟร์วอลล์ ซึ่งเป็นที่นิยมสูงเมื่อนำมาใช้งานร่วมกับเครือข่ายชนิดบรอดแบนด์ในปัจจุบัน
- **การสร้าง DMZ แบบ three prongs firewall**
  เป็นโครงสร้างของ DMZ ที่สมบูรณ์แบบ มีประสิทธิภาพและประสิทธิผลตรงตามความต้องการมากที่สุด เหมาะกับสภาพแวดล้อมในองค์กรส่วนใหญ่ และง่ายต่อการดูแลบำรุงรักษา
- **การใช้งานสคริปต์สำเร็จรูปเพื่อสร้างเครื่องพีซีลีนุกซ์เป็นไฟร์วอลล์**
  รูปแบบของความต้องการใช้งานไฟร์วอลล์โดยทั่วไปมักมีความคล้ายคลึงกันเป็นส่วนใหญ่ ดังนั้นการนำสคริปต์สำเร็จรูปมาใช้งานจึงเป็นการลดภาระ ระยะเวลาและความผิดพลาดลงได้มาก อย่างไรก็ตามการนำสคริปต์สำเร็จรูปมาใช้นั้นยังคงต้องอาศัยความรู้ความเข้าใจของผู้บริหารระบบเป็นสิ่งสำคัญ

48/145 Soi Nawamin 157, Nawamin Rd, Klongkoom, Bungkoom, Bangkok 10230 Tel. 0-2509-8444, 0-2509-0484 Fax. 02-509-0485

Part III : Advanced Administering with Performanced Tools and Applications

ในสภาพของการนำไปใช้งานจริง ผู้บริหารระบบเครือข่ายจำเป็นอย่างยิ่งที่จะต้องมีเครื่องมือที่มีประสิทธิภาพสนับสนุนการบริหารจัดการระบบ เพื่อความสะดวกและเพิ่มประสิทธิภาพยิ่งขึ้น นอกจากนี้ยังเสริมด้วยเทคโนโลยีที่น่าสนใจและเหมาะสมกับการใช้งานในสภาพปัจจุบันอีกด้วย

- **การใช้เครื่องมือบริหารจัดการไฟร์วอลล์ตรวจสอบวิเคราะห์และรายงาน** (Log Analyzer)
  ศึกษาวิธีการเตรียมระบบเพื่อสนับสนุนการรายงานผลการทำงานของ iptables การคอนฟิกองค์ประกอบเสริมให้แก่โฮสต์ การติดตั้งและใช้งานโปรแกรมเครื่องมือวิเคราะห์และรายงานที่เป็นซอฟต์แวร์โอเพ่นซอร์ส
- **การเก็บบันทึกเหตุการณ์ที่รายงานจากไฟร์วอลล์ไว้ในระบบฐานข้อมูล** MySQL
  วิธีการติดตั้งใช้งานซอฟต์แวร์วิเคราะห์และรายงานผลการทำงานของไฟร์วอลล์หลากหลายรูปแบบที่ซับซ้อนขึ้นโดยใช้การจัดเก็บข้อมูลไว้ในระบบฐานข้อมูล และนำเสนอข้อมูลผ่านเว็บบราวเซอร์อย่างสวยงามและสะดวกต่อการแปลผล
- **ศึกษาเทคโนโลยีของ** Bridging Level Firewall
  การจำกัดหรือกรองด้วยเงื่อนไขที่เป็นตัวแปรของไอพีแอดเดรสเพียงอย่างเดียวอาจจะไม่เหมาะสมกับเครือข่ายที่เป็น Dynamic IP Address การจัดการด้วยอุปกรณ์ Bridge ซึ่งทำงานในระดับ OSI Layer 2 จึงเป็นทางออกที่รัดกุมมากกว่า
- **การสร้างและบริหาร** Level 2 Firewall **ด้วยลีนุกซ์**
  การประยุกต์ใช้ลีนุกซ์เร้าเตอร์ให้ทำหน้าที่เป็น Bridge เป็นอีกแนวทางหนึ่งที่น่าสนใจ และมีประสิทธิภาพสูง ไม่ว่าจะเป็นการทำงานระดับ MAC Address ซึ่งมีความเร็วสูงหรือการบล๊อกเฉพาะเครื่องหรือแม้กระทั่งการ NAT ในระดับฮาร์ดแวร์
- **ศึกษาแนวคิดและหลักการของ** VPN (Virtual Private Networking)
  การสื่อสารด้วยช่องทางสื่อสารที่มีการเข้ารหัสได้กลายเป็นส่วนหนึ่งในนโยบายการรักษาความปลอดภัย โดยเฉพาะในยุคของอินเตอร์เน็ตบรอดแบนด์และการสื่อสารไร้สายเช่นทุกวันนี้ VPN จะช่วยให้คุณเข้าสู่เครือข่ายของสำนักงานของคุณได้จากทุกมุมโลกภายใต้การรักษาความปลอดภัยด้วยไฟร์วอลล์
- **การสร้างระบบ** VPN **ด้วยลีนุกซ์และซอฟต์แวร์โอเพ่นซอร์ส**
  ศึกษาเทคโนโลยี VPN ในปัจจุบัน เปรียบเทียบจุดเด่นจุดด้อย และซอฟต์แวร์แอปพลิเคชั่นที่มีให้เลือกใช้อย่างเหมาะสม ลงมือปฏิบัติการติดตั้ง และบริหารจัดการระบบ VPN Server บนลีนุกซ์ ทดลองใช้งานจริงผ่านโมเด็มและ ADSL ความเร็วสูง

48/145 Soi Nawamin 157, Nawamin Rd, Klongkoom, Bungkoom, Bangkok 10230 Tel. 0-2509-8444, 0-2509-0484 Fax. 02-509-0485