วิเคราะห์มาตรฐานในการตรวจสอบระบบสารสนเทศ สำหรับระบบความปลอดภัยบนระบบปฏิบัติการ UNIX/Linux

by A.Pinya Hom-anek, GCFW, CISSP, CISA

ACIS Professional Team

E-mail: prinya@acisonline.net

ด้วยแนวโน้มทิศทางของการตรวจสอบภายใน (Internal Audit) และ การควบคุมภายใน (Internal Control) ในแนว Proactive กำลังกลายเป็นเรื่องสำคัญที่องค์กรทุกองค์กรที่ใช้ระบบสารสนเทศ ต้องนำมาปฏิบัติอย่างจริงจัง

ในรายละเอียดของการตรวจสอบ และ การควบคุมภายในนั้น หัวใจสำคัญก็คือขั้นตอนการประเมินความเสี่ยง (Risk Assessment) ซึ่งระบบปฏิบัติการที่เราใช้กันอยู่ในปัจจุบันนอกจากค่าย Microsoft แล้ว ถ้าเป็นองค์กรขนาดใหญ่ก็มักจะใช้ระบบปฏิบัติการ UNIX ของ SUN, HP หรือ IBM (SUN Solaris, HP/UX และ IBM AIX ตามลำดับ) เช่น ธุรกิจการสื่อสารคมนาคม ธุรกิจน้ำมัน ธุรกิจการเงินการธนาคาร ตลอดจน ธุรกิจที่ต้องการความเชื่อถือได้ และ เสถียรภาพของระบบปฏิบัติการในระดับสูงกว่าปกติ เช่น งานฐานข้อมูลขนาดใหญ่ มักนิยมใช้ฐานข้อมูล Oracle หรือ IBM DB2 ทำงานบนระบบปฏิบัติการ UNIX Solaris, HP/UX หรือ IBM AIX เป็นต้น

ส่วนองค์กรขนาดกลางและขนาดเล็ก ตลอดจน สถาบันการศึกษานิยมใช้ระบบปฏิบัติการ Linux เพิ่มมากขึ้น โดยนำไปใช้เป็น Web Server และ Mail Server แต่ในปัจจุบันองค์กรขนาดใหญ่หลายองค์กรก็นำ Linux ไปใช้เป็น Enterprise Database Server กับระบบฐานข้อมูล Oracle, IBM DB2 หรือ MySQL เช่นกัน

ดังนั้นการวิเคราะห์จุดอ่อนของระบบปฏิบัติการ UNIX/Linux จึงเป็นเรื่องจำเป็นอย่างยิ่งยวด เพื่อที่องค์กรจะได้ทราบถึงช่องโหว่ที่ระบบ UNIX/ Linux ที่ยังคงมีอยู่ และ ยังไม่ได้รับการแก้ไขให้ถูกต้องด้วยการ "Hardening"

กระบวนการตรวจสอบ ระบบปฏิบัติการ UNIX/Linux จำเป็นต้องมีมาตรฐานอ้างอิงว่าระบบปฏิบัติการมีความปลอดภัยอยู่ในขั้นที่เราสามารถไว้ใจได้ในระดับหนึ่งหรือไม่ (Risk Acceptance Level) มาตรฐานในการตรวจสอบระบบสารสนเทศสำหรับระบบความปลอดภัยบนระบบปฏิบัติการ UNIX/Linux ที่ได้รับการยอมรับกันโดยทั่วไปก็คือ มาตรฐาน SANS/FBI Top 20

ช่องโหว่ระบบปฏิบัติการ UNIX/ Linux ที่พบเป็นประจำนั้น มาตรฐาน SANS Top 20 2004 ได้สรุปช่องโหว่

ของระบบ UNIX/ Linux ไว้ทั้งหมด 10 ข้อ มีรายละเอียดดังต่อไปนี้ (รายละเอียดดูที่ http://www.sans.org/top20)

1. ช่องโหว่ของระบบ Domain Name System (DNS) ที่ใช้โปรแกรม BIND จาก ISC

วิเคราะห์ปัญหาช่องโหว่

BIND ย่อมาจาก "Berkeley Internet Name Domain" เป็นโปรแกรม DNS Server ที่มีผู้ใช้มากที่สุดในโลก แต่ก็มีช่องโหว่อยู่จำนวนมากเช่นกัน ตัวอย่างเช่น ช่องโหว่ที่ทำให้ BIND Service ไม่ทำงาน เรียกว่าเกิดอาการ Denial of Service (DoS) Attacks เป็นต้น

ถ้าระบบ DNS ล่ม การ Resolve URL Request จาก URL เป็น IP Address ก็จะเกิดปัญหาตามมาทำให้ทุกระบบที่ต่อเชื่อมกับอินเทอร์เน็ตนั้นไม่สามารถเข้าถึงได้ นับว่าเป็นปัญหาใหญ่ที่ไม่ควรมองข้าม นอกจากนี้ยังมีช่องโหว่ Buffer Overflow และ Cache Poisoning ที่ถูกแฮกเกอร์ยิง Exploit เข้ามายัง DNS Server อยู่บ่อยๆ DNS Server จำนวนมากในอินเทอร์เน็ตยังคงมีช่องโหว่ดังที่กล่าวมาแล้ว ทำให้แฮกเกอร์ฉวยโอกาสเจาะระบบได้อย่างไม่ยากเย็นนัก

ช่องโหว่นี้เกิดขึ้นทั้งระบบปฏิบัติการ UNIX และ Linux ที่ใช้โปรแกรม BIND ทำงานเป็น DNS Server

วิธีการแก้ปัญหา

- ทางแก้ปัญหาที่ง่ายที่สุดเลยก็คือ การเลิกใช้โปรแกรม BIND แล้วหันไปใช้โปรแกรม DNS Server ตัวอื่นแทน เพราะโปรแกรม BIND มักเกิดช่องโหว่อยู่เป็นประจำ
- การปิด Service BIND Daemon หรือ named ก็เป็นทางออกที่ดี ในกรณีที่ไม่ได้ใช้งาน DNS Server
- การติดตั้ง Patch ให้กับ BIND กลายเป็นเรื่องจำเป็นในทุกครั้งที่มีคนค้นพบช่องโหว่ของ โปรแกรม BIND
- การป้องกันการทำ "Zone Transfer" สามารถตั้งค่าได้ในไฟล์ "named.conf"
- การติดตั้งให้ BIND Service ทำงานอยู่เฉพาะในพื้นที่ที่จำกัดเฉพาะ BIND เท่านั้น เราเรียกวิธีนี้ว่า "Jail" ถ้าหาก BIND Service ถูกยึดโดยแฮกเกอร์ แฮกเกอร์ก็ยังไม่สามารถเจาะเข้าสู่แกนกลางหรือ Kernel ของระบบได้ เพราะถูกขังอยู่ในคุก (Jail) ที่เราออกแบบไว้นั่นเอง
- การปฏิบัติตามขั้นตอน Hardening BIND Checklist ก็เป็นสิ่งที่ควรทำก่อนที่จะ Online ระบบ DNS Server

2. ช่องโหว่ Web Server บน UNIX/Linux Platform

วิเคราะห์ปัญหาช่องโหว่

Web Server ที่ใช้บน UNIX/Linux ส่วนใหญ่แล้วเป็น Apache Web Server และ มักจะทำงานร่วมกับ PHP Module, OpenSSL Module และ MySQL RDBMS เป็นต้น (ข้อมูลเพิ่มเติมเกี่ยวกับการสำรวจจำนวน Web Server ทั่วโลกดูได้ที่ http://www.netcraft.com)

ช่องโหว่ที่พบประจำก็คือ การติดตั้ง Web Server ตามค่าโดยกำหนด (ค่า Default) ทำให้แฮกเกอร์สามารถเจาะเข้าระบได้ หากไม่ได้เปลี่ยนแปลงค่าโดยกำหนดบางค่า

ช่องโหว่ที่อันตรายมากอีกช่องโหว่หนึ่งก็คือ ช่องโหว่ของ OpenSSL แฮกเกอร์สามารถยิง Exploit เจาะระบบ UNIX/LINUX ของเราผ่านทางช่องโหว่นี้ แล้วสามารถปรับระดับตนเองเป็น User "Root" ได้อย่างสบาย

Apache Web Server และ PHP Modules เองก็มีช่องโหว่ Buffer Overflow ด้วยเช่นกัน

วิธีการป้องกัน

-
- ติดตั้ง Patch ล่าสุดให้กับ Web Server และ Modules อื่นๆ ที่ทำงานร่วมกับ Web Server
- ปิดฟังก์ชั่นหรือบริการที่ไม่จำเป็นต้องใช้
- ใช้งาน Modules ด้าน Security เช่น mod_security จาก www.modsecurity.org ซึ่งสามารถป้องกัน Cross Site Scripting (XSS) และ SQL Injection
- ใช้วิธี CHRoot Jail กับ Apache Web Server ถ้าหาก Web Server ถูกยึด (Compromised) แฮกเกอร์ก็ยังไม่สามารถเจาะเข้าสู่ Kernel ได้ และไม่ Run Web Server ด้วย User Root โดยเปลี่ยนเป็น User อื่นแทน

3. ช่องโหว่เกี่ยวกับ Authentication

วิเคราะห์ปัญหาช่องโหว่

การใช้ Password ง่ายๆ อย่างไม่ระมัดระวังเป็นต้นเหตุให้ระบบของเราถูกเจาะกว่า 50% จากอัตราการเจาะ

ระบบของแฮกเกอร์ 100% ที่ถูกบันทึกสถิติไว้สำหรับ UNIX/Linux Server บางเครื่อง user บางคนไม่มี password หรือไม่ก็ username กับ password เป็นค่าเดียวกันเป็นต้น ทำให้แฮกเกอร์สามารถเจาะเข้าระบบได้อย่างง่ายดาย

การ Authentication ที่ใช้ http protocol (plain text) ไม่ได้ใช้ https protocol (encrypted text) ทำให้แฮกเกอร์สามารถดักจับ username และ password ได้อย่างง่ายดายเช่นกัน

วิธีการแก้ปัญหา

- ตั้ง password ให้มีความซับซ้อน ยากต่อการคาดเดา มีจำนวนตัวอักษรรวมกันแล้วไม่ต่ำกว่า 8 ตัวอักษร
- เก็บ password ในไฟล์ที่มีการเข้ารหัสด้วย Hashing Algorithms ที่มีความแข็งแกร่ง
- การเข้ารหัสเวลา Login เข้าระบบจะช่วยได้มาก เช่น การใช้ SSL Protocol (https) กับ Web Server เป็นต้น

4. ช่องโหว่เรื่อง Version Control Systems ที่ CVS Sever

วิเคราะห์ปัญหาช่องโหว่

CVS หรือ Concurrent Versions System เป็นระบบ CVS ที่นิยมใช้กันในการควบคุม Source Code ในวงการ Open Source แต่ก็ก่อให้เกิดช่องโหว่ให้ User Anonymous เข้ามาในระบบได้ และ ยังมีปัญหา heap-based buffer overflow แฮกเกอร์สามารถยิง Exploit เข้าสู่ระบบของเราได้ จากนั้นแฮกเกอร์จะเข้ามาแก้ไข Source Code เพื่อฝัง Backdoor หรือ Trojan Program แล้วค่อยแฝงตัวเข้าระบบของเราในภายหลัง

วิธีการแก้ปัญหา

ใช้ CVS Software Version ล่าสุดเท่านั้น โดยสามารถ Download Source Code จาก https://www.cvshome.org

5. ช่องโหว่ของ Mail Transport Service

วิเคราะห์ปัญหาช่องโหว่

ระบบอิเล็กโทรนิกส์เมลล์ หรือ Email ในทุกวันนี้เป็นระบบสำคัญที่เราจะขาดไม่ได้ กลไกที่สำคัญในการรับ-ส่ง Email ก็คือ Mail Transport Agents (MTA) มีหน้าที่ในการจัดส่ง Email ไปยังผู้รับ รวมทั้งรับ Email จากผู้ส่งด้วยโปรโตคอล SMTP (TCP Port 25)

ในปัจจุบันมี MTA อยู่หลายค่าย sendmail เป็น MTA ที่ได้รับความนิยมสูงสุด รองลงมาก็คือ qmail และ postfix

sendmail เป็น MTA มีช่องโหว่มากที่สุดเป็นอันดับหนึ่ง สำหรับ qmail และ postfix มีการรักษาระบบความปลอดภัยให้กับ MTA เป็นอย่างดี มีช่องโหว่เพียงเล็กน้อยเมื่อเทียบกับ sendmail

ช่องโหว่ที่เกิดขึ้นบ่อยครั้งก็คือ Buffer Overflow ที่ตัว MTA เอง และ บ่อยครั้งที่ MTA ตกเป็นเหยื่อพวกโปรแกรม Spammer เพราะกลายเป็น Open relays ให้ Spammer เข้ามาแอบส่ง SPAM mail เป็นต้น

<u>วิธีการแก้ปัญหา</u>

- ตรวจสอบ Version ของโปรแกรม MTA ของเรา แล้วตรวจสอบว่าได้ติดตั้ง Patch ล่าสุดแล้วหรือยัง เช็คข้อมูลได้ที่ http://cve.mitre.org
- ตรวจสอบว่า MTA ของเราเป็น Open relays หรือไม่ ตรวจได้ที่ http://www.abuse.net/relay.html
- ตรวจสอบว่า MTA ของเราอยู่ในรายการ Real time Black hole list หรือไม่ ตรวจได้ที่ http://www.ordb.org
- ถ้าไม่ได้ใช้ MTA ก็ให้ปิดบริการ MTA Service
- ติดตั้ง Patch ล่าสุดให้กับ MTA เสมอ
- ทำตามคำแนะนำด้านความปลอดภัยใน web site ของ MTA แต่ละค่าย

6. ช่วงโหว่ SNMP Service

<u>วิเคราะห์ปัญหาช่องโหว่</u>

โปรโตคอล SNMP (Simple Network Management Protocol) ใช้ในการเฝ้าดูเครือข่าย (Network Monitor) โดยปกติแล้ว ISP ใช้ SNMP Service ร่วมกับโปรแกรม MRTG (www.mrtg.org) เพื่อแสดงข้อมูลให้ลูกค้าเห็นปริมาณ Traffic ใน Link ของลูกค้าที่เชื่อมเข้าสู่ ISP โดยการเปิด SNMP Service ที่ Router แล้วอ่านข้อมูลออกจาก Router ไปวาดกราฟ ทำสถิติของ Traffic ในช่วงเวลาที่ผ่านไป

โปรโตคอล SNMP นั้นเป็นโปรโตคอลที่ส่งข้อมูลในลักษณะ Plain Text ซึ่งแฮกเกอร์สามารถดักจับข้อมูลระหว่างทางได้ ปัญหาของช่องโหว่ SNMP ก็คือ แฮกเกอร์สามารถเจาะเข้าสู่ระบบเครือข่าย โดยเจาะไปที่ Router หรือ Switching ขององค์กรโดยอาศัยค่า SNMP Routing ซึ่งเปรียบเสมือน Password ในการเข้าไปตั้งค่าต่างๆ ในอุปกรณ์เครือข่าย

โดยปกติผู้บริหารเครือข่ายที่ไม่ได้คำนึงถึงเรื่องความปลอดภัยมักตั้งค่า SNMP community string เป็นค่า default โดยกำหนดคือ "public" และ "private" ทำให้เกิดช่องโหว่กับระบบทันที่ที่ถูกแฮกเกอร์ "Scan SNMP" เข้ามาผ่านทาง Port UDP 161 เมื่อแฮกเกอร์เจาะเข้ามา โดยใช้ SNMP community string ดังกล่าว แฮกเกอร์อาจจะเข้ามาแก้ไขค่า Configuration ต่างๆ ใน Router และ Switching ได้ ตลอดจนล่วงรู้ข้อมูลต่างๆ ในระบบเครือข่ายของเราจากข้อมูล Routing Table ที่เก็บอยู่ใน Router เป็นต้น

<u>วิธีการแก้ปัญหา</u>

- ไม่ควรเปิดใช้ SNMP Service โดยไม่จำเป็น
- ใช้โปรโตคอล SNMP Version 3 จะปลอดภัยกว่าใช้โปรโตคอล SNMP Version 1 หรือ Version 2
- ทำการกรอง SNMP โดยการปิด Port UDP161 และ UDP 162 ที่ Router หรือ Switching โดยใช้ Access List หรือ Firewall Rules
- เปลี่ยนค่า Default Community String จาก Public และ Private เป็นคำอื่น
- ห้ามเปิดค่า Default Community String ให้มีสิทธิ SNMP Write

7. ช่องโหว่ OpenSSL

<u>วิเคราะห์ปัญหาช่องโหว่</u>

OpenSSL ถูกนำมาใช้ในการทำ Encryption Tunnel ในหลากหลายบริการ ไม่ว่าจะเป็น Web Server (http), Email (POP3, IMAP, SMTP) และ LDAP เพื่อทำให้แฮกเกอร์ไม่สามารถดักจับข้อมูลของเราได้ง่ายๆ โลกของ e-Commerce คงไม่เกิดถ้าไม่มีโปรโตคอล SSL เพราะทุกวันนี้การทำธุรกรรมออนไลน์ ล้วนใช้โปรโตคอล SSL ทั้งสิ้น เช่น ระบบอินเทอร์เน็ตแบงค์กิ้ง เป็นต้น โดยเฉพาะ ถ้า Web Server เป็น Apache ก็มักจะใช้ OpenSSL Module มาเสริมให้เกิด SSL Tunnel ระหว่าง Web Browser และ Web Server ผ่านทาง https โดยใช้ Port TCP 443

แต่ OpenSSL ก็มีจุดอ่อน เนื่องจากช่องโหว่ของตัว OpenSSL Module เอง โดยเฉพาะ Version ก่อน 0.9.7c หรือก่อน 0.9.6l ช่องโหว่นี้มักเกิดขึ้นกับ Linux เพราะ Linux มักจะติดตั้งมาพร้อมกับ Apache และ OpenSSSL ที่ยังไม่ได้รับการแก้ไขปัญหาช่องโหว่ ลองใช้คำสั่ง OpenSSL ถ้าไม่ใช่ version 0.9.7d หรือ 0.9.6m ขึ้นไปก็หมายความว่าระบบของเรามีช่องโหว่แน่นอน

วิธีการแก้ปัญหา

- ให้ upgrade OpenSSL เป็น Version ใหม่ล่าสุด หรือ มากกว่า version 0.9.7c หรือ 0.9.6l
- ใช้ ipfilter หรือ netfilter ป้องกันระบบในรูปแบบของ Host-Based Firewall

8. ช่องโหว่ใน NIS/NFS Service

วิเคราะห์ปัญหาช่องโหว่

Network File System (NFS) และ Network Information Service (NIS) เป็นบริการ(Services) ที่ติดมากับ UNIX/Linux แทบทุก Distribution โดยเฉพาะเครื่อง SUN ที่ใช้ระบบปฏิบัติการ SUN Solaris

NFS ถูกออกมาให้บริการ File Sharing ระหว่าง UNIX Server ด้วยกัน หรือ ระหว่าง Client กับ UNIX Server ก็ได้เช่นกัน

ปัญหาก็คือ NFS/NIS ที่เราใช้อยู่นั้นมีช่องโหว่ที่แฮกเกอร์สามารถเจาะเข้าสู่ระบบ UNIX/Linux ของเราได้ ถ้าเราไม่ติดตั้งบริการ NFS/NIS อย่างระมัดระวัง หรือ ไม่ติดตั้ง Patch ล่าสุดสำหรับบริการ NFS/NIS ระบบที่เปิด NFS/NIS โดย Default จึงเป็นระบบที่อันตรายและมีความเสี่ยงที่จะถูกเจาะระบบโดยง่าย

วิธีการแก้ปัญหา

- ถ้าไม่จำเป็นต้องใช้บริการ NFS/NIS ให้ปิดบริการเสีย
- ไฟล์ Configuration /etc/export ของ NFS ควรตั้งค่าอย่างระมัดระวัง
- ใช้โปรแกรม TCP Wrapper หรือ iptables/netfilter ในการปิดบริการสำหรับ Host ที่ไม่จำเป็นต้องใช้บริการ NFS/NIS

9. ช่องโหว่ใน Database ที่ทำงานบน UNIX/Linux

วิเคราะห์ปัญหาช่องโหว่

กล่าวถึงระบบฐานข้อมูลในปัจจุบันนี้ถือเป็นหัวใจสำคัญให้กับระบบหลายระบบ เช่น ระบบ ERP, SCM หรือ CRM ระบบฐานข้อมูลควรเป็นระบบที่ต้องปราศจากช่องโหว่ หรือ มีช่องโหว่น้อยที่สุดเท่าที่จะเป็นไปได้

ระบบฐานข้อมูลที่นิยมใช้บน UNIX/Linux ได้แก่ Oracle, IBM DB2, MySQL และ PostgreSQL โดยแฮกเกอร์สามารถเจาะเข้าสู่ระบบฐานข้อมูลโดยต่อตรงเข้ากับ Port ของ ฐานข้อมูลแต่ละตัว เช่น Oracle เปิด Port 1521, MySQL เปิด Port 3306, PostgreSQL เปิด Port 5432 เป็นต้น

ระบบฐานข้อมูลบางระบบ มักตั้งชื่อ system admin และ password เป็นค่า default เมื่อติดตั้งเสร็จแล้วก็ไม่เคยเปลี่ยนอีกเลย ทำให้เกิดช่องโหว่กับระบบฐานข้อมูลโดยตรง

วิธีการแก้ปัญหา

- ควรทำการติดตั้ง Patch ล่าสุดให้ระบบฐานข้อมูลของเราอย่างสม่ำเสมอ
- เปลี่ยนค่าโดยกำหนด (default) ต่างๆ ที่มากับฐานข้อมูลตอนติดตั้งในครั้งแรก โดยเฉพาะ default ของ username และ password ต้องเปลี่ยนทันที

10. ช่องโหว่ที่ Kernel

วิเคราะห์ปัญหาช่องโหว่

Kernel ถือเป็นส่วนสำคัญที่สุดของระบบปฏิบัติการ บ่อยครั้งที่ตัว Kernel เอง เกิดช่องโหว่ เนื่องจากมีคนตรวจพบทำให้แฮกเกอร์ฉวยโอกาสตอนที่เรายังไม่ได้ Update Kernel เจาะเข้าสู่ระบบของเรา โดยอาศัยช่องโหว่ที่ Kernel

วิธีการแก้ปัญหา

- ทำการ "Tune" Kernel ให้มีเสถียรภาพ และ Update Kernel Patch ล่าสุดให้กับระบบปฏิบัติการ
- ปิดบริการที่ไม่จำเป็นเพื่อไม่ให้แฮกเกอร์อาศัยช่องโหว่จากบริการเหล่านั้นมาเจาะระบบอีกทีหนึ่ง
- ติดตามข่าวสารช่องโหว่ของ Kernel อยู่ตลอด เพื่อที่จะปิดช่องโหว่ได้ทันท่วงที

จะเห็นว่าระบบปฏิบัติการ UNIX/Linux นั้นมีช่องโหว่พอๆ กับระบบปฏิบัติการ Microsoft Windows แต่การจัดการปิดช่องโหว่ หรือ "Hardening" นั้นทำได้ยากกว่า ระบบปฏิบัติการ Microsoft Windows เนื่องจากความซับซ้อนของระบบปฏิบัติการและการใช้งาน Command Line ในลักษณะ Text Mode เป็นส่วนใหญ่ ดังนี้นในโลกความเป็นจริง system administrator มักจะไม่ค่อย Patch ระบบ UNIX/Linux ทำให้ระบบยังคงมีช่องโหว่อันตราย และ เปิดโอกาสให้แฮกเกอร์เข้ามาโจมตีได้ในที่สุด เพราะฉะนั้น system administrator จึงต้องมี "วินัย" ในการติดตาม "Patch" ระบบปฏิบัติการอยู่ตลอดเวลา

องค์กรควรมี Security Policy หรือ ใช้บริการ External Security Audit คอยกำกับดูแลการทำงานของ system administrator อีกทีหนึ่งเพื่อที่จะแน่ใจได้ว่าระบบได้รับการดูแลด้านความปลอดภัยอยู่เสมอ Proactive Vulnerability Management และ Patch Management เป็นเรื่องที่ควรปฏิบัติในยุคที่ 24x7 Real-time Monitoring ถือเป็นเรื่องจำเป็น สำหรับการเฝ้าระวังความปลอดภัยในวันนี้และอนาคต.

จาก : หนังสือ eWeek Thailand
ปักษ์หลัง เดือนพฤศจิกายน 2547
Update Information : 2 ธันวาคม 2547