www.ez-admin.com

ศูนย์อบรมสำหรับผู้ต้องการก้าวสู่อาชีพผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ โดยเรียนรู้จากการปฏิบัติงานจริง

"เราจะทำเรื่องยากให้เข้าใจง่ายด้วยสิ่งเหล่านี้"

- บทความเจาะลึกด้านระบบเครือข่ายคอมพิวเตอร์
- เว็บบอร์ดถามตอบปัญหา
- คู่มือทางด้านระบบเครือข่ายคอมพิวเตอร์และ **Hacking**
- หลักสูตรอบรมที่เน้นการเรียนรู้จากการปฏิบัติงานจริงโดยผู้เชี่ยวชาญในราคาไม่แพง

หมายเหตุ : บทความนี้ค่อนข้าง Advanced ผู้อ่านต้องมีพื้นฐานด้านการเขียนโปรแกรมและระบบปฏิบัติการเครือข่ายมากพอสมควร

เทคนิคของ Hacker ที่ใช้ในการเจาะระบบ

โดยปกติค่า default ของ OS ต่างๆ มักไม่มีการปิดช่องทางสำหรับ Hacker ดีเท่าที่ควรดังนั้นเราลองมาดูช่องทางต่างๆ ที่สำคัญๆ พร้อมวิธีการปิดช่องทางสำหรับ Hacker กันดีกว่าครับ

การ Hack Windows NT /2000 ผ่าน IIS

1. Windows NT4.0 และWindows2000 ที่เป็นWeb Server มีช่องทางที่HackerสามารถHackโดยผ่าน IIS (NT =V.4 ,2000=V.5)

2. Hacker ส่งผ่านทางIE(Internet Explorer) หรือNetscape โดยส่งคำที่ให้IIS ตีความผิดแล้วHackerก็จะใช้ประโยชน์โดยการสั่งให้Program ที่อยู่บนServerทำงานตามที่สั่งได้

การป้องกันโดยปิดทาง Hacker ที่ Hackผ่านทาง IIS

1. ไม่ติดตั้ง IISถ้าไม่จำเป็นต้องใช้งาน

2. ติดตั้ง patch หรือ Service Pack 3

   - Service Pack 2 ไม่สามารถปิดรูรั่วได้

   - Service Pack 3 สามารถปิดรูรั่วได้

   วิธีติดตั้ง Service Pack ควรกระทำหลังจากติดตั้ง Windows 2000 เสร็จใหม่ๆ โดยยังไม่ได้ติดตั้ง Applicationใดๆ หากติดทีหลังอาจทำให้ Applicationทำงานผิดปกติก็เป็นได้

3. Firewall ไม่สามารถป้องกันการ Hack ทาง IIS ได้

   - การทำงานของ Firewall จะทำตาม Access Rule ที่เราป้อนให้เท่านั้น

การ Hack ระบบปฏิบัติการ UNIX แบบ Local Hack

ระบบUNIX จะประกอบด้วย user หลายๆคนโดย user ที่ดูแลระบบคือ root (ID =0) ซึ่งมีสิทธิ์ที่จะจัดการกับระบบได้ทุกอย่าง การ Hack จะทำให้ userธรรมดาสามารถเป็น rootได้

1. ไม่เปิดTelnet ,SSH และFTP ถ้าไม่มีความจำเป็น

- เพราะการHackแบบLocal Hackerจะต้องเอา Program Hack(exploit) ไป Runบน Server หากมีความจำเป็นต้องเปิดTelnet เพื่อทำการRemoteเข้ามาทำการ config.เครื่องก็ควรกำหนดเฉพาะ Admin. และUserที่จำเป็นเท่านั้น

2. ไม่ติดตั้งcomplier เช่นProgram gccหรือ make โดยไม่จำเป็น

- Hackerจะต้องทำการ complier Program เป็นbinary เพื่อRun หากไม่จำเป็นไม่ควรติดตั้ง complierบนServer หากหลีกเลี่ยงไม่ได้Admin.ต้องหมั่นตรวจตรา Source Code ของUserอยู่เสมอ

3. Upgrade Packet ที่อ่อนแอให้เป็นVersion ที่แข็งแกร่ง

- ทั้งนี้เนื่องจากProgram Hack (exploit) สามารถทำให้ user กลายเป็น user ผู้ดูแลระบบ(root) นั้นเกิดจาก Packetบางตัวมีช่องโหว่/อ่อนแอ

- Upgrade Packetที่อ่อนแอให้เป็นVersionที่แข็งแกร่งจะป้องกัน SERVER ได้

4. Upgrade Versionของ OS

การHackระบบปฏิบัติการ UNIXแบบ Remote Hack

Remote Hack = การ Hack ที่ Hacker ไม่จำเป็นต้องทำการTelnet เข้าไปยัง Serverเป้าหมาย

ระบบปฏิบัติการ Linux Redhat 7.0 ถ้าติดตั้งโดย default แล้วจะมี serviceที่ชื่อ lpd.(บริการเกี่ยวกับ PRT. ใช้TCP Port 515) ติดมาด้วยซึ่งเป็นช่องโหว่ให้ Hacker เข้าครอบครองServer

Hackerจะใช้วิธีscan Port เป้าหมายทีละเครื่องด้วยคำสั่ง nmap หรือใช้ โปรแกรม Netbus scan Network

เครื่องมือที่ใช้ในการ Remote Exploitระบบ Linux Redhat 7.0 ทาง lpd portคือ seclpd.c (เป็น source codeภาษา Cซึ่งไม่สามารถใช้งานได้ทันที ต้องนำไป compileเป็นภาษาเครื่องก่อน)

การป้องกันการ Hack ระบบปฏิบัติการ UNIX แบบ Remote

1. เปิดเฉพาะ serviceที่จำเป็น

   - ควรปิดservice การบริการlpd. / ถอนPacket นี้จาก Server

2. Upgrade Packetให้เป็น versionที่แข็งแกร่งกว่า

3. ติดตั้ง Firewall

   - กำหนด Access Rule เพื่อป้องกันIP ภายนอกทำการติดต่อกับ Port 515 ภายใน

4. การ Bomb e-mail

   - Bomb e-mail = การส่งe-mail จำนวนมากๆไปยังผู้รับปลายทางในเวลาติดๆกัน มีผลทำให้ Mail Box ผู้รับเต็มไปด้วย e-mailขยะ

ขั้นตอนการส่ง mail

1. PCของเราส่ง e-mail ไปที่ SMTP Server(Mail Server)เพื่อทำหน้าที่ส่งต่อ e-mail ไปยัง Mail Serverภายนอก SMTP Serverจะทำการบันทึก IP Address(PCของเรา)

2. SMTP Serverจะส่ง e-mailต่อไปยัง Serverปลายทาง

- SMTP Server จะตรวจสอบ (โดยcheck จากMX Record ของ Protocol DNS)

- Mail Serverปลายทางจะบันทึก IP Addressของ SMTP Serverโดยเพิ่มไว้บนHeader ของ e-mailด้วย

3. User ปลายทางรับ mail จาก Mail Serverเขาเอง

- ผู้รับสามารถตรวจสอบได้ว่า mailมาจากเครื่อง IP ใด?/ ผ่านSMTP Server/ Mail Serverใดบ้าง?

*** Hackerที่มีประสบการณ์ จะไม่ใช้ e-mail Addressตนเอง + IP Address ของเครื่องในการส่ง Mail จะใช้จากที่สาธารณะที่เรียกว่า Open Relay/ปลอม e-mailตนเองให้เป็นของคนอื่น

การป้องกันการ Bomb e-mail

1. กำหนดค่าในMail Server เพื่อไม่ให้รับ e-mail จากIPที่ไม่น่าเชื่อถือ

2. ตรวจจับโดยใช้ Software Linux /Unix ควรเขียนProgram ภาษา C

- ตรวจหัวข้อของe-mail ว่าซ้ำหรือไม่ ?

- หากมาจาก IP เดียวกันให้รับ e-mail ไม่เกิน 3ฉบับ/นาที

- ใช้ Software ป้องกัน : Arbomb ,Vipul's Razor

- เขียน Program โดยใช้ Visual C++

- ใช้ Software ป้องกัน : GFI Mail Essentials for Exchange /SMTP ,Open Relay Filter Enterprise Edition , Xwall หรือ VOP modusGate Enterprise

การปลอม IP เพื่อPostข้อความลงใน Webboard และเพื่อการ Hackของ IIS

- ที่ webboard จะมีการบันทึก IP Addressของผู้ที่ทำการ Postข้อความเก็บไว้ แต่อาจมีการหลอกให้บันทึก IP Addressเครื่องอื่นที่มิใช่เครื่องของเราโดยใช้ Proxy

- Proxy Server =เครื่อง คอมพิวเตอร์ที่ทำหน้าที่เป็นตัวกลางระหว่าง Clientกับ Web Serverในการร้องขอและจัดส่งหน้า Webpage

- การเรียกชม Websiteสามารถสั่งให้ Proxy Serverทำการร้องขอเอาหน้า Webนั้นได้ หาก website นั้นถูกเรียกใช้งานแล้ว หน้า webนั้นจะถูกเก็บไว้ใน cacheของ Proxy Server หากเรียกใช้อีกครั้ง ตัว Proxy Serverจะเอาหน้า web ที่อยู่ใน cache ส่งให้ได้เลย

ประโยชน์ของProxy Server

1. เพื่อความเร็วในการDownload หน้าWebpage

2. ประหยัดBandwidth

- ประโยชน์หากProxy Server อยู่ในระบบLANเดียวกับclient และLink ระหว่างGateway ไปหา ISPที่ความเร็วไม่สูง

3. ประโยชน์ด้านความปลอดภัย(Security)

- สามารถกำหนดUser ให้ชมwebใดได้บ้างโดยกำหนดค่าACL (Access Control List) ที่ตัว Proxy Server

ในการใช้งาน Proxy Userจะป้อนค่า IP Addressของ Proxy Serverและ Portที่ Proxy Serverเปิดเพื่อให้บริการ (ปกติ 8080 หรือ 3128) โดย Userจะติดต่อกับ Proxy Serverด้วย Protocol HTTP

Hackerที่มีความชำนาญจะเรียกใช้ Proxy Server ที่อยู่ต่างประเทศซึ่งมีความเร็วสูง/เปิดบริการฟรี ซึ่งเรียกว่า Public Proxy

****วิธีที่จะหา Public Proxyก็ใช้ search engine ก็สามารถหาได้

****Public Proxyอาจมีการติดตั้ง Program squid(มากับLinux)ซึ่งเปิดโอกาสให้ทุก IP Address เรียกใช้งานได้

****Program Netbusมีความนิยมใช้scan port (ต้องใส่ช่วง IP Addressที่ต้องการ scanหา Public Proxyด้วย)

การป้องกันการปลอม IP เพื่อ Post ข้อความลงใน Webboard

1. ไม่รับการPost จากIP เมืองนอกที่เป็นProxy Server

- ผู้ดูแล Webboardต้องหมั่นตรวจสอบ IPที่อยู่ใน Log file Webboardอยู่เสมอ

- เพิ่ม Codeใน Webboardไม่ให้รับการ Postจาก IPที่ไม่มั่นใจ

2. กรณีเป็นเจ้าของProxy

- กำหนด ACLเฉพาะกลุ่ม IPใน Networkของตนเอง

- ไม่ติดตั้ง Software Proxy Serverถ้าไม่จำเป็น : Wingate ,squid

- ตรวจดู Log fileเมื่อพบคนอื่นเข้ามาเกาะ ก็ควรปรับปรุง ACLโดยเร็ว

- กำหนดค่าใน Firewall / Gatewayเพื่อป้องกัน userใน Networkเราไปเกาะ Proxyคนอื่น

3. การแทรกรูปภาพบน Webboard /สมุดเยี่ยม

การทำงานของ Program ใน Webboard

- จะเริ่มการสร้าง Forumโดยให้ผู้ใช้ป้อนอักษรต่างๆ แล้วมีปุ่ม Post(ส่งข้อความ) เพื่อให้ผู้ตั้งหัวข้อ / ตอบคำถามใช้ในการ clickเพื่อส่งข้อความ

- หลังจากปุ่ม Postถูกกด Program CGI / ASPที่อยู่ใน Webboardก็จะนำกลุ่มตัวอักษรต่างๆจากบน Forum มาเก็บไว้ใน Databaseหรือ Text File

- เมื่อผู้เข้ามาเยี่ยมชม webและอ่าน Program CGI / ASPจะไปอ่านข้อมูลใน Database แล้วส่งกลับไปให้ Browser เพื่อนำข้อความมาแสดงโดยทำงานตามคำสั่ง HTML (โดยคำสั่ง HTMLจะอยู่ในเครื่องหมาย < >)

- การแสดงอาจปรากฏเป็นข้อความ /รูปภาพก็เป็นได้

- สาเหตุหลักที่สามารถแทรกรูปภาพเข้าไปยัง Webboardได้ เนื่องจากความไม่รอบคอบในการเขียน Program ซึ่งไม่ได้ป้องกัน Tag , HTMLในเครื่องหมาย < >

การป้องกันการแทรกรูปภาพและTag HTMLในWebboard /สมุดเยี่ยม

1.ป้องกันเครื่องหมาย < และ > (เป็นวิธีป้องกันที่ดีที่สุด)

- ขั้นตอนการ Postข้อความ

- ก่อนขั้นตอนการบันทึกข้อมูลลง Database

- บันทึกเครื่องหมาย < หรือ > ลง Databaseแต่ป้องกันในขั้นตอนการส่งกลับให้ Browser

2. แสดง IP Address ของผู้ Post ด้วย

การดักจับ Password ของe-mail โดยใช้ Sniffer

- การทำงานของ Hub จะมีจุดอ่อนด้านความปลอดภัยมากกว่า Switch

โปรแกรมประเภท Protocol Analyzer

1. โปรแกรมประเภท Protocol Analyzer เป็น Program คอยตรวจจับ Frame / Packet เพื่อหาสิ่งผิดปกติที่เกิดขึ้นใน Network เพื่อใช้ในการวิเคราะห์แก้ปัญหา

2. ศึกษาการทำงานของ Protocol ต่างๆ

3. วิเคราะห์ข้อมูลที่คอมพิวเตอร์ส่งหากัน

- ตัวอย่างโปรแกรมประเภท Protocol Analyzer เช่น Sniffer , Ether Real ฯลฯ

*****Sniffer อนุญาตให้ผู้ใช้งานระบุ IP Address , Port และProtocol ที่เครื่อง 2 เครื่องคุยกันได้เช่น ARP ,DHCP ,Telnet ,SMTP ,POP3 ฯลฯ

*****Sniffer ไม่สามารถดักจับข้อมูลของเครื่องที่ใช้switchได้ [switch ส่งข้อมูลออกเฉพาะ Port (ช่องเสียบสัญญาณ) ที่มีเครื่องหมายต่ออยู่เท่านั้น

การป้องกันการดักจับ Password ของe-mail โดยใช้ Sniffer

1. ใช้ Switch แทน Hub

- ข้อมูลทุก Frame จะถูกส่งออกจากทุกPort ของHub เมื่อมีผู้ใช้คอมพิวเตอร์เครื่องใดใน Network เรียกใช้ Program Sniffer ก็สามารถดักจับ Frame ข้อมูลได้

- ใช้ Switch แทน Hub จะเกิดผลดีคือ Frame ข้อมูลจะมีการส่งออกเพียงแค่ Port ที่ต่อกับคอมพิวเตอร์ปลายทางเท่านั้น

- Program Snifferสามารถดักจับได้เพียง Frameข้อมูลที่เครื่องตัวเองรับ-ส่งเท่านั้น

2. ใช้ Software เพื่อตรวจสอบ Mode การทำงานของ Network Interface Card ของคอมพิวเตอร์แต่ละเครื่องใน Network

- คอมพิวเตอร์ที่ใช้ Sniffer NIC (Card LAN) จะทำงานใน Mode Promiscusus สามารถตรวจสอบได้โดยใช้ Software Anti Sniff ตรวจสอบ

3. เปลี่ยนจากการใช้งาน Application ที่ไม่มีการเข้ารหัสมาเป็นการเข้ารหัส

- เปลี่ยนจากการใช้ Telnet เป็น Secure(ssh)

4. เปลี่ยน Password บ่อยๆและกำหนดให้ Password มีการหมดอายุ

- ไม่ควรใช้Password เดียวกันหลายๆระบบ

การทำDenial of Service (DoS)

Denial of Service = การทำให้ Serverเป้าหมาย เช่น Web , Mail Database Server ไม่สามารถให้บริการได้ แบ่งออกเป็น

1. Local DoS = ทำDoS บนเครื่องนั้นๆโดยตรง คือuserทำให้เครื่องหยุดทำงานได้โดยไม่ต้องมีสิทธิ์ของผู้ดูแลระบบเลย อาจใช้วิธีการTelnet ,FTP ไปยังServerเป้าหมาย

2.Remote DoS = ทำDoS โดยไม่ต้องTelnet ,FTP ไปยังServer เป้าหมาย เพียงแค่รู้ IP Address หรือ Domain ของServerเป้าหมายก็เพียงพอแล้ว

การป้องกันการทำDenial of Service (DoS) [Local DoS]

1. ไม่เปิดTelnet หรือ ssh และ FTPถ้าไม่จำเป็น

- กำหนดสิทธิ์ให้ user ที่มีความจำเป็นที่จะต้อง Remote มายัง Serverเท่าที่จำเป็น

2. ไม่ติดตั้งโปรแกรม complierต่างๆ ถ้าไม่มีความจำเป็น

- โปรแกรมที่ทำDoS บางตัวจำเป็นต้องเอาcomplier บนServer ก่อน เพื่อให้ทำงานบน OS Version ที่อยู่บน Server ได้ จึงไม่ควรติดตั้งcomplier บน Server

3. Upgrade Kernel ของ OS และ Upgrade Version ของ OS อย่างสม่ำเสมอ

การเข้าครอบครองWindows NT/2000 Server

1. การเข้าถึง Command Shell ด้วยNetcat

- Command Shell ของระบบWindows (command.com[CMD.EXE])เป็นตัวเชื่อมระหว่างUser กับ kernel ของOS (เหมือน ที่อยู่บนระบบUNIX ไม่ว่าจะเป็น Bash Shell หรือShellอื่นๆ)

1.1 Netcat =เป็นการสื่อสารกันทาง TCPระหว่าง Host 2ตัว ซึ่งต้องมีตัวหนึ่งทำหน้าที่รับฟัง (Listen)โดยฝ่ายที่ไม่เป็น Listen (Client)จะต้องเป็นผู้รับ connect ไปยัง Listen (Server)

***โปรแกรม Netcat เป็นโปรแกรม ที่ออกแบบมาทั้งตัวListen และConnet

1.2 การ Listen ทางTCP Port ด้วยNetcat และการเปลี่ยนทิศทางไปยัง Command Shell

- โปรแกรม Netcat สามารถเปลี่ยนทิศทางของข้อมูลที่ส่งหากันระหว่างClient กับ Server

1.3 การ Connect TCP จากClient ด้วยNetcat

- Client สามารถconnect ไปServer โดยใช้ Netcat หรือโปรแกรม Telnet

2. การ Upload โปรแกรม Netcat ด้วยTFTP

- การยึดครองServer คือการได้มาซึ่งCommand Shell ของ Server ดังนั้นต้องหาทาง run Netcat ที่ Server ให้ได้ อาจใช้ช่องทางIIS

3. TFTP

- เป็นProtocol ที่มีไว้ส่งถ่ายข้อมูลคล้ายFTP เพียงแต่ใช้UDPและไม่ต้องมี Username และ Password

- สั่งงานในบรรทัดเดียวกัน ก่อให้เกิดความสะดวก / คล่องตัว

- ใช้ในการ Upload / Downloadข้อมูล โปรแกรมในอุปกรณ์ Network : Router ฯลฯ

3.1 ทำให้ Serverฝ่ายเราเป็น TFTPโดยมี โปรแกรมที่นิยมมากคือ Tftpd32.exeและให้เครื่องเป้าหมายดึงไปใช้

3.2 Run TFTP Clientที่เครื่องเป้าหมาย

- ใช้โปรแกรม Tftp.exe

-ใช้คำสั่ง GET เพื่อนำFile จากTFTP Server (nc.exe)ไปยังเครื่องเป้าหมาย

4. การได้มาซึ่ง Command Shellของ Serverเป้าหมาย

- Run Netcatบน Serverเป้าหมาย โดยเครื่องเป้าหมายจะListenรออยู่ ซึ่งเราก็สามารถ connect ได้เลย

5.การ Upload โปรแกรม Trojan สามารถทำได้เมื่อมีCommand Shellของ Serverเป้าหมายแล้ว

6.การยึดครอง Serverเป้าหมาย

- โปรแกรม Netbus เป็น Trojan ตัวหนึ่ง ใช้งานง่าย ประกอบด้วย 2 ส่วน

6.1 ติดตั้งบน Serverเป้าหมาย (File :patch.exe)

6.2. ติดตั้งบนเครื่องเราเพื่อควบคุมServer (File : Netbus.exe)

การป้องกันการเข้าครอบครองWindows NT/2000 Server

1. ติดตั้ง patch หรือ Service Pack 3

2. ใช้ Firewall (ทำงานเหมือน Router คือForward Packetจาก Networkไปยัง Networkอื่น ตาม Access Ruleที่ต้องการ)

3. ติดตั้งAnti Virus บนServer เพื่อป้องกันการUpload Trojan

การได้มาซึ่ง Password ของ Administrator บนWindows NT / 2000 Server

1. Essential Net Tools เป็นโปรแกรมที่มี function การทำงานข้างในมากมาย : scanNetwork , Netstat , Auditing Tools ฯลฯ

- จะมีFileที่เก็บรายชื่อของ userและ File ที่เก็บคำที่คนมักจะนำมาตั้งเป็น Password โดยเอา 2Files มาตรวจสอบดู user ใช้Password ใด

- การเข้าถึงข้อมูลบน Serverคือการใช้ Map Network Driveโดยต้องระบุ IP Addressของ Server เป้าหมาย และUsername และPassword ของ Admin

- หาก Serverติดตั้ง Terminal Serviceก็ไม่จำเป็นต้องใช้ Map Network Drive โดยสามารถ connectผ่าน Terminal Serviceได้เลย

2. การประยุกต์ใช้ Tools

- หากใช้ Essential Net Tools ไม่สามารถพบ Password ของ Admin. ได้ จำเป็นต้องนำFile Dictionary (Fileที่มีคำทุกคำในโลก) มาใช้แทนFileของ Essential Net Tools (แทนที่ชื่อเดียวกัน /Directoryเดียวกัน) การค้นหาต้องใช้เวลานานจึงอาจจะพบ / ไม่พบ

- ทำการ Audit โดยใช้ Essential Net Toolsใหม่ โอกาสที่จะพบ Passwordมีโอกาสค่อนข้างสูง

การป้องกันการขโมย Password ของ Admin. บนWindows Server

1. ตั้ง Passwordให้ยากๆ

   - ตั้งค่าที่ไม่มีใน Dictionary

   - ใช้อักษรเล็ก / ใหญ่ผสมกับตัวเลข : zE8tH2eF

2. ติดตั้ง Service Pack และหมั่น Update Patch ใหม่ๆ

3. ใช้ Firewall

การได้ Password ของ e-mail บน Mail Server

กรณีใช้ POP3 Server เมื่อเตรียม File UserและPassword พร้อมแล้ว ก็ run โปรแกรม p3x โดย p3x จะส่ง Password ไปที่ Mail Server ทีละตัวเพื่อตรวจสอบ หากไม่ใช่จะส่ง Error Message กลับมาให้ p3k ทำให้ p3k นั้นทราบว่า Password ไม่ใช่ก็จะเอาตัวต่อไปมาอีก ทำซ้ำกันไปเรื่อยๆ จนกว่าจะถูกทดสอบจนหมด หากใช่ Password ที่ถูกต้อง จะปรากฏ OK Mailbox Open

การป้องกันการขโมย Password ของ e-mail จากการใช้ Tools ต่าง ๆ

1. ตั้ง Password ของuser ให้ยากๆ เช่นตั้งว่า ฉันรักเธอ แต่ใช้ Keyboard เป็นภาษาอังกฤษเมื่อกดใน keyboard จะได้ Password = CyoiydgTv

2. ตั้งค่าที่ POP 3 Server เมื่อมีการส่งค่าPassword ที่ผิดติดต่อกัน 3 ครั้งให้ Server ทำการ Disconnect

ป้องกันการ **Bomb Webboard**

1. ตรวจหัวข้อของกระทู้ว่าซ้ำ ?

- จะมีลักษณะที่เป็นข้อความซ้ำๆเหมือนเดิม (เหมือน Bomb e-mail)

- Web Masterควรเพิ่ม codeเพื่อใช้ในการตรวจสอบ/รับข้อมูลเพียงครั้งเดียว (ข้อความที่ส่งมาครั้งแรก)

2. ถ้ามาจาก IPเดิมให้ Post ได้นาทีละ 1กระทู้

- ปกติการตั้งกระทู้จะใช้เวลา มากกว่า 1นาที

3. ตรวจสอบว่าเป็นข้อความที่ถูกสร้างโดยมนุษย์หรือคอมพิวเตอร์ นัก Web Programmer ควรปฏิบัติดังนี้

- ข้อความที่อ่านไม่รู้เรื่องตัดทิ้งไป

- ใช้วิชา AI เข้ามาช่วย

การป้องกันระบบให้พ้นภัยจากเครื่องมือ **Hack** ใหม่ๆ

1. เปิดเฉพาะ service ที่จำเป็น

2. ลบ user ที่เป็น defaultของระบบที่ไม่จำเป็นทิ้งไป

3. ใช้ Firewall

- กำหนดAccess Rule ที่เหมาะสม

- สามารถใช้ Linux Redhat 8.0 ซึ่งมี IPTABLE ซึ่งเป็น Firewallใช้ฟรี โดยไม่ต้องลงทุนซื้อ Firewall(เพียงแค่หา คอมพิวเตอร์รุ่น Pentium 2,3)

4. ติดตั้ง IDS

- มีทั้งแบบ Hardware และ Software (Black ICE)

- สำหรับ Network ควรมี NIDS (Network Intrusion Detection Systems) ควรติดตั้งที่หน้า Firewall เพื่อตรวจจับ Trafficที่น่าสงสัย หรือหลัง Firewall เพื่อตรวจจับ Traffic ที่แปลกปลอมผ่าน Firewall หรือติดตั้งที่ Network ในกลุ่ม Server ที่อยู่ในโซน DMZ

ศูนย์อบรม ez-admin

เปิดอบรมหลักสูตรต่างๆ สำหรับผู้ต้องการก้าวสู่อาชีพผู้ดูแลระบบคอมพิวเตอร์ ดังนี้

หลักสูตร NETWORK & SECURITY

1. ก้าวสู่อาชีพผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ และพื้นฐานการ Hacking
2. ติดตั้งและจัดการเครือข่ายคอมพิวเตอร์ขั้นสูง
3. ติดตั้งระบบความปลอดภัยให้กับเครือข่ายคอมพิวเตอร์ด้วย ISA Server 2006 , ForeFront และ Firewall
4. ติดตั้ง จัดการ และดูแลความปลอดภัยให้ Mail Server ด้วย Exchange Server, ISA Server และ ForeFront

หลักสูตร WINDOWS SERVER 2008 & SECURITY

1. ติดตั้ง Server และจัดการเครือข่ายคอมพิวเตอร์ด้วย Windows Server 2008 (ระดับเริ่มต้น)
2. ติดตั้ง Server และจัดการเครือข่ายคอมพิวเตอร์ด้วย Windows Server 2008 (ระดับกลาง)
3. ติดตั้ง Server และจัดการเครือข่ายคอมพิวเตอร์ด้วย Windows Server 2008 (ระดับสูง)
4. การรักษาความปลอดภัยบน Windows Server 2008 และควบคุมสิทธิของ Users ด้วย Group Policy

หลักสูตร WINDOWS SERVER 2003 & SECURITY

1. ติดตั้ง Server และจัดการเครือข่ายคอมพิวเตอร์ด้วย Windows Server 2003 (ระดับเริ่มต้น)
2. ติดตั้ง Server และจัดการเครือข่ายคอมพิวเตอร์ด้วย Windows Server 2003 (ระดับสูง)
3. การรักษาความปลอดภัยบน Windows Server 2003 และควบคุมสิทธิของ Users ด้วย Group Policy

หลักสูตร HACKING & SECURITY

1. มือใหม่หัด Hack ให้รู้ทัน Hacker (ระดับเริ่มต้น)
2. มือใหม่หัด Hack ให้รู้ทัน Hacker (ระดับกลาง)

3. มือใหม่หัด Hack ให้รู้ทัน Hacker (ระดับสูง)