HOW TO LINUX

How to linux (Case study จาก Redhat 6.2 ไปถึง Redhat 9.0)

คำสั่ง ls : ใช้แสดงรายชื่อแฟ้มทั้งหมดใน home directory

ทุกท่านที่มี account ใน linux จะมี home directory ของตนเอง เพื่อใช้เก็บแฟ้มต่าง ๆ ภายใต้ระบบ linux เมื่อต้องการทราบว่ามีแฟ้มอะไรที่เก็บไว้บ้าง สามารถใช้คำสั่ง ls ได้ และสามารถกำหนด parameter ได้หลายตัว เช่น -al --sort เป็นต้น

ตัวอย่างคำสั่ง และการใช้งาน

ls -alt :: เพื่อแสดงรายชื่อแฟ้มทั้งหมด และจัดเรียงตามเวลา ให้ลองลบอักษรออกทีละตัวจาก alt ดูนะครับ
ls -alt | more :: เพื่อแสดงรายชื่อแฟ้มทั้งหมด แต่หยุดทีละหน้า เมื่อมีจำนวนแฟ้มเกินที่จะแสดงได้ ใน 1 หน้า
ls -al --sort=time | more :: แสดงรายชื่อแฟ้มเรียงตามเวลา แยกทีละหน้า โดยละเอียด
ls -R | more :: แสดงรายชื่อในทุก directory ในห้องปัจจุบัน
ถ้าสังเกตนะครับ **แฟ้มที่มี . หน้าชื่อแฟ้ม** จะหมายถึงแฟ้มที่ซ่อนไว้ ถ้าใช้คำสั่ง ls หรือ ls -l จะไม่เห็นแฟ้มเหล่านี้
ถ้ามีอักษร **D ที่ Column แรก** ในตอนแสดงชื่อแฟ้ม ด้วยคำสั่ง ls -al ก็จะหมายถึง directory ไม่ใช่แฟ้มธรรมดา

คำสั่ง chmod : ใช้เปลี่ยนสิทธิ์ของแฟ้ม **เจ้าของ(Owner), คนในกลุ่ม(Group), คนอื่น(Other)** สามารถทำอะไรได้บ้าง

เมื่อใช้คำสั่ง ls ท่านจะเห็นตัวอักษร RWXRWXRWX หรือท่านองนี้หน้าชื่อแฟ้ม ซึ่งเป็นการกำหนด สิทธิ์ของแต่ละแฟ้ม ว่า อ่านได้ เขียนได้ และประมวลผลได้ โดยแยกเป็นส่วนของ เจ้าของ กลุ่ม คนอื่น ซึ่งเป็นคำสั่งที่จำเป็นมากสำหรับ webmaster ในการดูแลระบบ และท่านที่ต้องการเขียน CGI จะต้องรู้คำสั่งนี้ เพราะ เมื่อส่งแฟ้ม CGI เข้าไปใน server และต้องการให้คนทั่วไปเข้ามาใช้บริการ โปรแกรมของตนที่เขียนขึ้นด้วย Perl จะไม่สามารถใช้ได้ ถ้าไม่กำหนดให้คนอื่น สามารถประมวลผลได้ (x) จึงจำเป็นต้องใช้คำสั่ง เช่น **chmod 755 hello.pl** หรือ **chmod 775 fileforyou.pl** หรือ **chmod +x test.pl** เป็นต้น

ในแต่ละกลุ่มจะมีการกำหนดสิทธิได้ 3 แบบ ตัวอักษร R มาจาก Read หมายถึง **อ่าน** ตัวอักษร W มาจาก Write หมายถึง **เขียน** ตัวอักษร X มาจาก Execute หมายถึง **ประมวลผล** **ตัวอย่างเช่น** --- : ไม่มีสิทธิอะไรเลย (เลขที่ใช้คือ 0) --X : ประมวลผลได้อย่างเดียว (เลขที่ใช้คือ 1) R-- : อ่านได้อย่างเดียว (เลขที่ใช้คือ 4) RW- : อ่าน และเขียนได้ (เลขที่ใช้คือ 6) R-X : อ่าน และประมวลผลได้ (เลขที่ใช้คือ 5) RWX : อ่าน เขียน และประมวลผลได้ (เลขที่ใช้คือ 7)	**ความหมายของ RWXRWXRWX จะเห็นว่ามีอักษร 9 ตัว** 3 ตัวแรกหมายถึง **เจ้าของ** 3 ตัวที่สองหมายถึง **กลุ่ม** 3 ตัวที่สามหมายถึง **คนอื่น** **ตัวอย่างเช่น** RWX------ : เจ้าของเท่านั้นที่มีสิทธิทุกอย่าง (เลขที่ใช้คือ 700) RWXRWX--- : เจ้าของ และสามาชิกกลุ่มเดียวกันมีสิทธิทุกอย่าง (เลขที่ใช้คือ 770) RWXR-XR-X : เจ้าของทำได้หมด ส่วนกลุ่มและคนอื่นอ่านและประมวลผลได้ (เลขที่ใช้คือ 755) R--R--R-- : ทุกคนอ่านได้อย่างเดียว (เลขที่ใช้คือ 444)

ตัวอย่างคำสั่ง และการใช้งาน

chmod 777 index.php :: ทำให้แฟ้มนี้ อ่าน เขียน และประมวลผล โดยทั้ง 3 กลุ่ม
chmod 755 * -Rf :: ทำให้ทุกแฟ้ม ทุก direcroty ในห้องปัจจุบัน เปลี่ยนตามที่กำหนด

คำสั่ง man : เป็นคำสั่งที่สำคัญมาก เพราะจะช่วยให้อธิบายคำสั่งต่าง ๆ ให้ท่านได้ (Manual)

ผมเชื่อว่าทุกคนที่ใช้ unix หรือ linux ต้องเคยใช้คำสั่งนี้มาก่อน เพราะจะเป็นคำสั่งที่ช่วยอธิบายหน้าที่ของคำสั่ง พร้อมกับแสดง parameter ที่สามารถใช้ได้ทั้งหมดของคำสั่งนั้น และยังมีตัวอย่างการใช้ และคำสั่งที่เกี่ยวข้องอีก ทำให้ประหยัดเวลาในการค้นเอกสารได้อย่างมาก บางท่านอาจศึกษา linux ด้วยการอ่านจาก man อย่างเดียวเลยก็มีนะครับ โดยไม่ต้องไปหาซื้อหนังสือที่ไหนมาอ่านก็ทำได้

ตัวอย่างคำสั่ง และการใช้งาน

man man :: เพื่ออธิบายคำสั่ง man เอง ว่าตัวคำสั่งนี้ใช้อย่างไร
man ls :: เพื่ออธิบายคำสั่ง ls ว่าใช้อย่างไร
man useradd :: เพื่ออธิบายคำสั่ง useradd ว่าใช้อย่างไร

คำสั่ง mkdir, rmdir, cd : งานต่าง ๆ เกี่ยวกับ directory

ผู้ใช้คอมพิวเตอร์ที่ใช้ dos มาก่อนต้องคุ้นเคยกับ directory แน่นอน สำหรับคำสั่งเกี่ยวกับ directory ในที่นี้มี 3 คำสั่ง
mkdir หมายถึง สร้าง directory (Make directory)
rm หมายถึง ลบ directory (Remove directory) และคำสั่งนี้ยังใช้ลบแฟ้มตามปกติได้อีกด้วย
cd หมายถึงเปลี่ยน directory (Change directory)

ตัวอย่างคำสั่ง และการใช้งาน

mkdir hello :: สร้าง directory ชื่อ hello ในห้องปัจจุบัน
rmdir hello.htm :: จะลบแฟ้มชื่อ hello.htm
cd / :: ย้าย directory ไปยัง root หรือห้องนอกสุด
cd .. :: ย้าย directory ออกไปข้างบน 1 ระดับ
cd ~/x :: เข้าไปยังห้อง x ของ home directory เช่น /home/thaiall/x ถ้า home directory คือ /home/thaiall

โปรแกรม pico : เป็น editor ที่ใช้สำหรับแก้ไขแฟ้มแบบ text คล้าย vi แต่มีประสิทธิภาพกว่ามาก

เพียงแต่พิมพ์คำว่า **pico** แล้ว enter ก็ใช้งานได้เลย การจะจัดเก็บ หรืองานต่าง ๆ ที่มีบริการไว้มากมาย ท่านสามารถอ่านได้จากเมนูด้านล่าง ซึ่งเครื่องหมาย ^ หมายถึงการกดปุ่ม **Ctrl ประกอบอักษรต่าง ๆ นั่นเอง** ผมคิดว่าท่านน่าจะพออ่านรู้เรื่อง หรือจะพิมพ์ว่า **pico xx** ก็จะเป็นการสร้างแฟ้มชื่อ xx ให้ทันที แต่หากมีแล้ว ก็จะเปิดแฟ้ม xx มาให้แก้ไขในโปรแกรม xx เมื่อท่านต้องการเลิกก็ทำได้โดยกดปุ่ม **Ctrl-X** เป็นอันเรียบร้อย หากท่านใดเคยใช้ vi เมื่อลองใช้โปรแกรมนี้จะติดใจอย่างแน่นอน เพราะใช้งานได้ง่ายกว่า หลายเท่านัก
หลายครั้ง ที่พิมพ์คำว่า pico แล้วไม่มีในเครื่อง ก็เพราะไม่ได้ลงโปรแกรม pine เมื่อต้องการใช้ pico ก็ต้องติดตั้งโปรแกรม pine เข้าไปในเครื่อง จากแผ่น CD ด้วยคำสั่ง rpm -i pine*

โปรแกรม emacs : เป็น editor ที่ใช้สำหรับแก้ไขแฟ้มแบบ text คล้าย vi แต่มีประสิทธิภาพกว่ามาก

ทำงานได้คล้าย ๆ กับ pico แต่หลายคนบอกว่า ตัวนี้ทำงานได้ดีกว่า แต่ผมว่า pico ใช้งานได้ง่ายกว่ากันเยอะเลย เพราะเห็นเมนูด้านล่าง แต่ของ emacs จะใช้ ctrl-h ดูส่วนช่วยเหลือ และกด ctrl-x + ctrl-c จึงจะออกจากโปรแกรม อาจเป็นเพราะผมใช้ไม่ชำนาญมังครับ ในเมื่อผมใช้ pico เป็น editor ผมคงไม่จำเป็นต้องศึกษา emacs เพิ่มเติมแล้ว ยกเว้นว่าสักวันอาจมีเหตุจำเป็นที่ความสามารถของ pico ให้ไม่ได้ แต่ emacs ให้ได้ก็เป็นได้

Welcome to GNU Emacs, one component of a Linux-based GNU system.
Get help C-h (Hold down CTRL and press h)
Undo changes C-x u Exit Emacs C-x C-c
Get a tutorial C-h t Use Info to read docs C-h i
Ordering manuals C-h RET
Activate menubar F10 or ESC ` or M-`

(`C-' means use the CTRL key.  `M-' means use the Meta (or Alt) key.
If you have no Meta key, you may instead type ESC followed by the character.)

โปรแกรม vi : เป็น editor ที่ใช้สำหรับแก้ไขแฟ้มแบบ text

Text editor ที่ใช้งานได้ยาก แต่มีใน linux ทุกรุ่น ในบางเครื่องไม่มี pico เพราะไม่ได้ติดตั้ง mail หรือ pine จึงจำเป็นต้องใช้โปรแกรม vi สำหรับแก้ไขข้อมูลในแฟ้มต่าง ๆ ของ linux เช่นการใช้คำสั่ง man ก็คือการใช้ความสามารถของ vi ในการนำข้อมูลมาแสดงผลนั่นเอง

ตัวอย่างคำสั่ง และการใช้งาน

esc กลับไปยังโหมดคำสั่ง
enter ย้ายไปยังต้นบรรทัดของบรรทัดถัดไป
i ใส่ข้อความก่อนเคอร์เซอร์
a ใส่ข้อความหลังเคอร์เซอร์
A ใส่ข้อความที่ท้ายบรรทัดปัจจุบัน
dd ลบบรรทัดปัจจุบันทั้งบรรทัด
x ลบอักษร 1 ตัวอักษร
cw เปลี่ยนข้อความ
:w บันทึกแฟ้ม
:q! ออกโดยไม่ เปลี่ยนแปลงใด ๆ
:wq! บันทึกแฟ้ม และออกจากโปรแกรม vi

คำสั่ง id, finger, who, w : ทุกคำสั่งข้างต้นใช้สำหรับตรวจสอบผู้ใช้ แต่จะให้รายละเอียดต่างกันไป

ตัวอย่างคำสั่ง และการใช้งาน

id uname :: ใช้ตรวจดูว่ามี account uname นี้ในระบบหรือไม่ ให้ผลสั้น
finger uname :: ใช้ตรวจดูว่ามี account uname นี้ในระบบหรือไม่ ให้ผลละเอียด ทั้ง last login หรือ email ฉบับล่าสุด
finger @www.isinthai.com :: ใช้แสดงรายชื่อทุกคนในระบบที่กำลัง login อยู่ในระบบ ใช้ได้กับทุกระบบที่ไม่ปิดบริการนี้
who |grep thai :: ใช้แสดงรายชื่อทุกคนในระบบ แต่ใช้นอกระบบตนเองไม่ได้ และเลือกเฉพาะบรรทัดที่มีอักษร thai
w :: ใช้แสดงรายชื่อทุกคนในระบบ แต่ใช้นอกระบบตนเองไม่ได้

คำสั่ง cat : แสดงข้อมูลในแฟ้ม คล้ายคำสั่ง type ในระบบ DOS

ตัวอย่างคำสั่ง และการใช้งาน

cat /etc/passwd :: แสดงข้อมูลในแฟ้ม /etc/passwd
cat /etc/passwd | more :: แสดงข้อมูลในแฟ้ม /etc/passwd ทีละหน้า

ตัวอย่างข้อมูลในแฟ้ม passwd

suwit:x:500:500:Suwit:/home/suwit:/bin/bash
prasert:x:501:501::/home/prasert:/bin/bash
bcom101:x:502:502::/home/bcom302:/bin/bash

คำสั่ง ifconfig : แสดงข้อมูลเกี่ยวกับ Network interface และแสดง ip ต่าง ๆ ที่มีการเพิ่มเข้าไปใน server ได้

ดูผลการทำงานของคำสั่ง **ifconfig**

```
eth0      Link encap:Ethernet  HWaddr 00:20:18:C0:06:C4
          inet addr:202.29.78.12  Bcast:202.29.78.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:673054 errors:0 dropped:0 overruns:0 frame:0
```

```
          TX packets:666268 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:74892865 (71.4 Mb)  TX bytes:680121131 (648.6 Mb)
          Interrupt:9 Base address:0xcf00
eth0:1    Link encap:Ethernet  HWaddr 00:20:18:C0:06:C4
          inet addr:202.29.78.1  Bcast:202.29.78.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:9 Base address:0xcf00
```

สามารถดูวิธีเพิ่มหลาย IP ในคอมพิวเตอร์เครื่องเดียว ได้จากหัวข้อ 9.10 ด้วยการแก้ไขแฟ้ม **/etc/rc.d/rc.local**

คำสั่ง netstat : แสดงสถานะของเครือข่ายว่ามีโปรแกรมใดเปิดให้บริการ

ดูผลการทำงานของคำสั่ง **netstat -a**

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:mysql                 *:*                     LISTEN
tcp        0      0 *:http                  *:*                     LISTEN
tcp        0      0 *:ftp                   *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 *:smtp                  *:*                     LISTEN
tcp        0      0 *:https                 *:*                     LISTEN
tcp        0      0 www.isinthai.com:ssh    202.29.78.200:1225      ESTABLISHED
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     855    /var/lib/mysql/mysql.sock
unix  2      [ ACC ]     STREAM     LISTENING     119    /dev/log
unix  2      [ ]         STREAM     CONNECTED     3007
unix  2      [ ]         STREAM     CONNECTED     859
```

คำสั่ง service : ดูสถานะของบริการต่าง ๆ ว่าถูกเปิดหรือ running อยู่หรือไม่

ดูผลการทำงานของคำสั่ง **service --status-all**

```
httpd (pid 2160 2159 2158 2155 2114 583 579 578 577 576 575 573) is running...
mysqld (pid 446 429 427 414) is running...
sendmail (pid 1700 1690) is running...
sshd (pid 2970 358) is running...
xinetd (pid 3923 369) is running...
```

คำสั่ง xinetd : ดูบริการภายใน xinetd ว่าอะไรเปิดอยู่บ้าง ทำให้เข้าไปเปิดที่ห้อง /etc/xinetd.d แล้วเลือกเปิดบริการเฉพาะที่ต้องการ เช่นแก้แฟ้ม talk เพื่อให้เปิดบริการ talk ใน server เป็นต้น

ดูผลบางส่วนจากการทำงานของคำสั่ง **xinetd -d**

```
Service configuration: ftp
        id = ftp
        flags = IPv4
        socket_type = stream
        Protocol (name,number) = (tcp,6)
        Nice = 10
```

Groups = no
Bind = All addresses.
Server = /usr/sbin/vsftpd
Server argv = vsftpd
Only from: All sites
No access: No blocked sites
Logging to syslog. Facility = authpriv, level = info
Log_on_success flags = HOST PID
Log_on_failure flags = HOST

คำสั่ง whereis : ค้นหาแฟ้มที่ต้องการว่าอยู่ที่ห้องใด แต่ค้นได้เฉพาะที่กำหนดไว้ใน PATH เท่านั้น หากต้องการค้นทั้งเครื่องต้องใช้คำสั่ง find

ตัวอย่างคำสั่ง และการใช้งาน

whereis usermod :: แสดงห้องที่เก็บคำสั่ง usermod ทำให้สามารถสั่ง run จากห้องที่เก็บคำสั่งโดยตรงได้

whereis ifconfig :: แสดงห้องที่เก็บคำสั่ง ifconfig ทำให้ใช้คำสั่งเช่น /sbin/ifconfig ได้โดยตรง

คำสั่ง cp, rm, mv : จัดการแฟ้มเช่น คัดลอก ลบ และย้าย

ตัวอย่างคำสั่ง และการใช้งาน

cp x y :: เดิมมีแฟ้มชื่อ x ต้องการแฟ้ม y ที่เหมือน x ขึ้นมาใหม่ สามารถใช้คำสั่ง cp

rm y :: ลบแฟ้ม y ออกจากเครื่อง ซึ่งอยู่ใน directory ปัจจุบัน

rm -r directoryname :: จะลบ directory ในเครื่อง sun และแฟ้มทั้งหมดใน directory นั้น และการลบแฟ้ม จะมีการถาม confirm ทุกแฟ้มเสมอ

rm -rf directoryname :: จะลบ directory ใช้ใน Redhat และแฟ้มทั้งหมดใน directory นั้น และการลบแฟ้ม จะมีการถาม confirm ทุกแฟ้มเสมอ

rm -f * :: ลบแฟ้มทั้งหมดโดยไม่ถาม yes

mv x /root :: ย้ายแฟ้ม x จากห้องปัจจุบันไปไว้ในห้อง /root

คำสั่ง ping : ตรวจสอบ ip ของเครื่องเป้าหมาย และการเชื่อมต่อ internet

ตัวอย่างคำสั่ง และการใช้งาน

ping www.thaiall.com :: ตัวสอบการมีอยู่ของ www.thaiall.com และแสดงเลข IP ของเว็บนี้

ping 202.29.78.100 -c 5 :: แสดงผลการทดสอบเพียง 5 บรรทัด

ping 202.29.78.2 :: ผลดังข้างล่างนี้ แสดงว่าไม่พบเครื่องที่มีเลข ip ดังกล่าว

```
PING 202.29.78.2 (202.29.78.2) from 202.29.78.12 : 56(84) bytes of data.
From 202.29.78.12 icmp_seq=1 Destination Host Unreachable
From 202.29.78.12 icmp_seq=2 Destination Host Unreachable
From 202.29.78.12 icmp_seq=3 Destination Host Unreachable
```

คำสั่ง env : แสดงค่า environment ปัจจุบัน

ตัวอย่างคำสั่ง และการใช้งาน

env

```
HISTSIZE=1000
SSH_CLIENT=202.29.78.100 1091 22
OLDPWD=/usr/sbin
QTDIR=/usr/lib/qt3-gcc3.2
SSH_TTY=/dev/pts/0
```

USER=burin
LS_COLORS=no=00:fi=00:di=00;34:ln=00;36:pi=40;33:so=00;35:bd=40;..
.. :
PATH=/usr/local/bin:/bin:/usr/bin:/usr/X11R6/bin
MAIL=/var/spool/mail/burin
PWD=/etc
INPUTRC=/etc/inputrc
LANG=en_US.UTF-8
HOME=/root
SHLVL=2
LOGNAME=burin
LESSOPEN=|/usr/bin/lesspipe.sh %s
G_BROKEN_FILENAMES=1
_=/bin/env

คำสั่ง lynx : Text browser ที่ใช้งานง่าย ใช้ดู source หรือ download ได้

ตัวอย่างคำสั่ง และการใช้งาน

lynx www.thaiall.com :: เพื่อเปิดเว็บ www.thaiall.com แบบ text mode
lynx http://www.yonok.ac.th :: เพื่อเปิดเว็บ www.yonok.ac.th แบบ text mode
lynx -dump http://www.yonok.ac.th :: เพื่อแสดงผลลัพธ์แบบไม่ interactive คือการ view ผลแล้วหยุดทันที
lynx -dump -width=500 http://piology.org/.procmailrc.html|grep '^|'|cut -c3- :: ตัวอย่างการนำไปใช้

คำสั่ง nslookup : แสดงเลข IP จากชื่อ host หรือ domain name

คำสั่งนี้ไม่พบใน Redhat 9.0 ถ้าต้องการใช้คำสั่งแบบนี้สามารถใช้ dig หรือ host แทนได้ เช่น **host yn1.yonok.ac.th** หรือ **dig yn1.yonok.ac.th**

ตัวอย่างคำสั่ง และการใช้งาน

nslookup 202.28.18.65

```
Non-authoritative answer:
65.18.28.202.in-addr.arpa  name = mars.uni.net.th.
Authoritative answers can be found from:
18.28.202.in-addr.arpa  nameserver = mars.uni.net.th.
18.28.202.in-addr.arpa  nameserver = ns.netserv.chula.ac.th.
mars.uni.net.th internet address = 202.28.18.65
```

nslookup www.thaiall.com

```
Name:   www.thaiall.com
Address: 66.150.1.141
```

คำสั่ง tail : แสดงส่วนท้ายของแฟ้มที่มีขนาดใหญ่ ต้องข้ามกับ cat ที่ดูตั้งแต่เริ่มแฟ้ม

ตัวอย่างคำสั่ง และการใช้งาน

tail index.html :: ดูส่วนท้ายของแฟ้ม index.html ใน Current directory
tail --lines=5 /var/log/messages :: ดูส่วนท้ายของแฟ้ม /var/log/messages แต่ต้องเป็น root จึงจะดูได้
tail /var/log/html/access.log :: ดูส่วนท้ายเพียง 10 บรรทัด ซึ่งเป็นค่า default ที่ไม่ได้กำหนดจำนวนบรรทัด
tail --lines=100 /var/log/html/access_log > access_bak :: เป็นการ backup ในขั้นแรกก่อนใช้ mv ย้ายไปทับแฟ้มเดิม

คำสั่ง telnet : ใช้ติดต่อเข้า server ต่าง ๆ ตาม port ที่ต้องการ แต่ปัจจุบัน server ต่าง ๆ ปิดบริการ telnet แต่เปิด SSH แทน

ตัวอย่างคำสั่ง และการใช้งาน

telnet 202.202.202.202 :: ขอติดต่อเข้าเครื่อง 202.202.202.202 การไม่กำหนด port คือเข้า port 23

telnet www.school.net.th 21 :: ขอติดต่อผ่าน port 21 ซึ่งเป็น FTP port

telnet mail.loxinfo.co.th 25 :: ตรวจ smtp ว่าตอบสนองกลับมา หรือไม่

telnet class.yonok.ac.th 110 :: ทดสอบ pop service ของ windows server 2003

```
Microsoft Windows POP3 Service Version 1.0 ready.
USER aa@class.yonok.ac.th
+OK
PASS xxxxxxx
+OK User successfully logged on
```

คำสั่ง df : แสดงการเนื้อที่ใช้งานทั้งหมดของ Harddisk ว่าเหลือเท่าใด

ช่วยให้ผู้ดูแลระบบรู้ว่าตอนนี้เนื้อที่ใน Harddisk เหลืออยู่เท่าใด และอาจใช้ตรวจสอบได้ว่า มีใครแอบมา upload แฟ้มขนาดใหญ่ไว้หรือไม่ จะได้ตรวจสอบในรายละเอียดของแต่ละ user ต่อไป (ผมเองก็ใช้บ่อย เพราะถ้า server เล็ก ๆ จะเต็มบ่อยครับ ต้องคอย clear เสมอ)

ตัวอย่างคำสั่ง และการใช้งาน

df :: เพื่อแสดงรายงานสรุปการใช้ในแต่ละส่วน

```
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/hda5               505605     82764    396737  18% /
/dev/hda1               101089      9180     86690  10% /boot
/dev/hda3              1423096     41956   1308848   4% /home
none                     30740         0     30740   0% /dev/shm
/dev/hda2              3889924   1551872   2140456  43% /usr
/dev/hda6              1027768    952876     22684  98% /var
```

คำสั่ง du : แสดงการเนื้อที่ใช้งาน ของแต่ละ directory โดยละเอียด

ช่วยให้ผู้ดูแลระบบรู้ว่า directory ใด ใช้เนื้อที่ใด หรือใช้ดูรวม ๆ ว่า ผู้ใช้แต่ละคนใช้เนื้อที่เก็บข้อมูลกันเท่าใด เพราะผู้ใช้ปกติจะใช้กันไม่เยอะ แต่ถ้าตรวจสอบแล้วเยอะผิดปกติ ก็จะเข้าไปดูว่า เยอะเพราะอะไร จะได้แก้ไขได้

ตัวอย่างคำสั่ง และการใช้งาน

du :: เพื่อแสดงรายชื่อ directory และเนื้อที่ที่ใช้ไป

du -all :: เพื่อแสดงโดยละเอียดว่าแต่ละแฟ้มมีขนาดเท่าใด ใน directory ปัจจุบัน

du | sort -g :: แสดงการใช้พื้นที่ของแต่ละ directory พร้อม sort จากน้อยไปมาก มีหน่วยเป็น Kb

du -b :: แสดงหน่วยเป็น byte ของแต่ละ directory

คำสั่ง ps : แสดง Process หรือโปรแกรมที่ประมวลผลอยู่ในระบบขณะนั้น

ช่วยให้ผู้ดูแลระบบ ติดตามได้ว่ามีโปรแกรมอะไรที่ไม่ถูกต้อง run อยู่ หรือโปรแกรมอะไร ที่ผู้ศึกษาลองประมวลผลแล้วค้างอยู่ จะได้ทำการแก้ไข มิฉนั้นระบบก็จะทำงานค้าง เพราะโปรแกรมที่ไม่ควรอยู่ในระบบ กำลังประมวลผลโดยไม่จำเป็น โดยเฉพาะพวก bot จะทำให้ server ล่มง่ายมาก

ตัวอย่างคำสั่ง และการใช้งาน

ps :: แสดงชื่อ process ต่าง ๆ ที่ทำงานอยู่อย่างสั้น

ps -ef :: แสดงข้อมูลของ process โดยละเอียด

ps -ax :: แสดงข้อมูลของ process พร้อมชื่อโปรแกรมได้ละเอียด
ps -aux :: แสดงข้อมูลของ process พร้อมชื่อโปรแกรม และชื่อผู้สั่งได้ละเอียดมาก

คำสั่ง kill : เมื่อทราบว่า process ใดที่มีปัญหา ก็จะเห็นเลขประจำ process คำสั่ง kill จะสามารถ process ออกจากระบบได้

ช่วยยกเลิก process ที่ไม่ถูกต้องออกจากระบบ ถ้าขณะนั้นผู้ใช้คนหนึ่งกำลังใช้งานอยู่ หาก process หลักของเขาถูก kill จะทำให้ผู้ใช้ท่านนั้น หลุดออกจากระบบทันที (สำหรับคำสั่งนี้จะถูกใช้โดย super user เท่านั้น ผู้ใช้ธรรมดาไม่มีสิทธิ์)

ตัวอย่างคำสั่ง และการใช้งาน

kill -9 เลขประจำprocess :: เลขประจำ process ท่านจะได้จากการใช้ ps -ef อยู่แล้ว
kill -9 1255 :: ลบ process ที่ 1255 ออกจากระบบไป

คำสั่ง find : เมื่อไฟล์ที่ต้องการว่าอยู่ใน directory ของเครื่องเราหรือไม่

ตัวอย่างคำสั่ง และการใช้งาน

find / -name hello.pl :: ใช้ค้นหาแฟ้ม hello.pl ในทุก directory
find / -name hello* :: ใช้ค้นหาแฟ้มที่ขึ้นต้นด้วยคำว่า hello
find /bin -size 626188c :: ใช้ค้นหาแฟ้มที่มีขนาด 626188 ถ้าเป็น RH8 จะพบแฟ้ม bash

คำสั่ง gzip : ใช้สำหรับแตกแฟ้มที่ถูกบีบอัด แล้วนามสกุล gz หรือ z

ตัวอย่างคำสั่ง และการใช้งาน

gzip -d x.tar.gz :: ใช้แตกแฟ้มที่นามสกุล gz
man gzip :: ใช้ดูว่า gzip ใช้งานอะไรได้บ้าง
gzip -d radius-1.16.1.tar.Z :: ได้แฟ้มนี้จาก ftp.livingston.com/pub/le/radius/ เป็นระบบรับโทรศัพท์เข้าเครือข่าย
gzip -dc x.tar.Z|tar xvf - :: ประหยัดขั้นตอนในการใช้คำสั่ง 2 ครั้ง เพราะคำสั่งชุดนี้จะใช้ทั้ง gzip และ tar กับ x.tar.z ได้ตามลำดับอย่างถูกต้อง

คำสั่ง tar : ใช้สำหรับแตกแฟ้มที่ถูกบีบอัด แล้วนามสกุล tar

ตัวอย่างคำสั่ง และการใช้งาน

tar xvf x.tar :: ใช้สำหรับแตกแฟ้มที่นามสกุล tar ปกติแล้วจะมีการสร้าง directory ของแฟ้มพร้อมโปรแกรมอีกเพียบ
tar xvfz squid-2.3-200103110000-src.tar.gz :: จะคลาย gz พร้อมกับใช้คำสั่ง tar ได้พร้อม ๆ กัน ไม่ต้องใช้ gzip และมาใช้ tar
man tar :: ใช้ดูว่า tar ใช้งานอะไรได้บ้าง
tar zcvf abc.tar.gz /etc :: ใช้ copy /etc เก็บเป็นแฟ้ม abc.tar.gz แบบบีบอัด
tar zxvf abc.tar.gz :: ใช้คลายแฟ้ม abc.tar.gz ซึ่งจะได้ directory /etc ออกมาทั้งหมด

คำสั่ง last : ใช้แสดงรายชื่อผู้ login เข้ามาล่าสุด

ตัวอย่างคำสั่ง และการใช้งาน

last |grep reboot :: ใช้ดูระบบถูก reboot เมื่อใดบ้าง
last |more :: ใช้รายชื่อผู้ login เข้ามาในระบบล่าสุดทีละหน้า

คำสั่ง grep : ใช้สำหรับเลือกข้อมูลเฉพาะบรรทัดที่ต้องการ

ตัวอย่างคำสั่ง และการใช้งาน

more /etc/passwd|grep thaiall :: ใช้แสดงข้อมูลในแฟ้ม /etc/passwd แต่เลือกเฉพาะบรรทัดที่มีคำว่า thaiall

rpm -qa|grep ftp :: ใช้ดูว่าระบบลงโปรแกรม ftp หรือยัง เวอร์ชั่นใดบ้าง

last |grep reboot :: ใช้ดูระบบถูก reboot เมื่อใดบ้าง

คำสั่ง date : ใช้ดูวันที่ หรือเปลี่ยนวันที่ และเวลาได้ date [OPTION] [MMDDhhmm[[CC]YY][.ss]]

ตัวอย่างคำสั่ง และการใช้งาน

date +%x :: ดูวันที่ปัจจุบัน เช่นการแสดงเลข 04/27/01 ออกมา

date +%d :: ดูวันที่ปัจจุบัน เช่นการแสดงเลข 27 ออกมา

date 04271340 :: กำหนดวันที่ใหม่ให้เป็น วันที่ 27 เดือน 4 เวลา 13.40 น. (mmddhhmmccyy)

hwclock --systohc :: เมื่อเปลี่ยนเวลาด้วย date หาก restart เครื่องเวลาจะผิดเหมือนเดิม ต้องใช้คำสั่งนี้ เพื่อเขียนเวลาลงไปใน hardware clock จึงจะเปลี่ยนเวลา hardware ได้

คำสั่ง top : ใช้แสดงสถานะการใช้ทรัพยากร ภายในเครื่อง

ตัวอย่างคำสั่ง และการใช้งาน

top :: แสดงการใช้ทรัพยากรของเครื่อง จากแต่ละ process ทดสอบคำสั่งนี้ใน Redhat 8.0

ตัวอย่างผลของการใช้คำสั่ง

```
CPU states:  0.5% user,  1.3% system,  0.0% nice, 98.0% idle
Mem:    31328K av,   28872K used,    2456K free,       0K shrd,    1032K buff
Swap: 1718912K av,    2608K used, 1716304K free                   16528K cached

  PID USER     PRI  NI  SIZE  RSS SHARE STAT  LIB %CPU %MEM   TIME COMMAND
18306 root      14   0   852  852   672 R       0  1.5  2.7   0:00 top
18229 root       1   0  1684 1536  1240 S       0  0.3  4.9   0:00 sshd
    1 root       0   0   160  116    92 S       0  0.0  0.3   0:08 init
    2 root       0   0     0    0     0 SW      0  0.0  0.0   0:01 kflushd
```

คำสั่ง ntsysv หรือ setup : ใช้เปิด-ปิด บริการของเครื่องที่สะดวกรวดเร็ว

ตัวอย่างคำสั่ง และการใช้งาน

setup :: แสดงการตัวเลือกให้กำหนดบริการต่าง ๆ ปกติจะเลือก system services

ntsysv :: ใช้เปิด-ปิดบริการ ให้ผลเหมือน setup, services

คำสั่ง route : ใช้เส้นทางการเชื่อมเครือข่าย

ตัวอย่างคำสั่ง และการใช้งาน

 # route

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
202.29.78.0     *               255.255.255.0   U     0      0        0 eth0
127.0.0.0       *               255.0.0.0       U     0      0        0 lo
default         202.29.78.254   0.0.0.0         UG    0      0        0 eth0
```

คำสั่ง shutdown, reboot : ใช้ปิดเครื่อง หรือ ปิดและเปิดเครื่องใหม่อย่างถูกวิธี

ตัวอย่างคำสั่ง และการใช้งาน

shutdown -h now :: สั่งปิดเครื่องทันที (แต่ใช้เวลาประมาณ 1 นาทีเพื่อปิดบริการต่าง ๆ)

reboot :: restart เครื่องใหม่ หากติดตั้งโปรแกรมบางตัว และ clear ค่าต่าง ๆ หากไม่แน่ใจ

คำสั่ง runlevel : คู่กับแฟ้ม /etc/inittab เพื่อบอกว่าปัจจุบันอยู่ใน level ใด

ตัวอย่างคำสั่ง และการใช้งาน

#/sbin/runlevel :: แสดง level ปัจจุบัน

#cat /etc/inittab :: แสดงตาราง กำหนดการสั่งเครื่อง ว่าใช้ level ใด

คำสั่ง fsck : ซ่อมแซมระบบแฟ้มใน linux

ตัวอย่างคำสั่ง และการใช้งาน

#fsck / :: ใช้ซ่อม harddisk ในห้อง / เมื่อการ harddisk เกิดปัญหาเกี่ยวกับการปิดเปิด

#fsck /dev/hdc :: ใช้ซ่อม harddisk ที่ชื่อ /dev/hdc ถ้าต่อ harddisk ไว้หลายตัว

คำสั่ง chown, chgrp : เปลี่ยนเจ้าของ หรือเปลี่ยนกลุ่ม

ตามหัวข้อ 1.2 เรื่องคำสั่ง chmod ทำให้ทราบว่า แฟ้มแต่ละแฟ้มมี 3 ส่วน คือเจ้าของ กลุ่ม และทั่วไป เมื่อต้องการเปลี่ยนความเป็นเจ้าของ หรือกลุ่ม ก็สามารถทำได้ ซึ่งเป็นหลักการง่าย ๆ ไม่ยุ่งยาก

ตัวอย่างคำสั่ง และการใช้งาน

#chown burin:users x :: เปลี่ยนเจ้าของของแฟ้ม x ให้เป็น burin และอยู่ในกลุ่มของ users

#chgrp users y :: เปลี่ยนกลุ่มของแฟ้ม x ให้เป็น users

คำสั่ง chkconfig : กำหนด หรือแสดง บริการที่สั่งประมวลผลใน level ต่าง ๆ ขณะเปิดเครื่อง

คำว่า level คือระดับในการเปิดเครื่อง ดูได้จากแฟ้ม /etc/inittab โดยโปรแกรมต่าง ๆ ที่สั่งให้ประมวลผล สามารถเลือกให้ทำงานใน level ใดได้ หากสั่งให้ประมวลผลปิด level เมื่อมีการ start linux ใน level หนึ่ง โปรแกรมที่คิดว่าสั่งให้ทำงานขณะเปิดเครื่อง ก็จะไม่ทำงาน

```
# /etc/inittab
# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
```

ตัวอย่างคำสั่ง และการใช้งาน

#/sbin/chkconfig --add mysql :: สั่งให้เพิ่ม mysql เข้าไปในระบบ system services

#/sbin/chkconfig --list :: แสดงรายการโปรแกรมทั้งหมด ที่สั่งให้ทำงานใน level ต่าง ๆ

#/sbin/chkconfig --level 3 sendmail on :: สั่งโปรแกรม sendmail ทำงานใน level 3 (Text mode)

#/sbin/chkconfig --level 5 sendmail on :: สั่งโปรแกรม sendmail ทำงานใน level 5 (X Windows)

คำสั่ง mount, umount : สั่งเชื่อมต่ออุปกรณ์ หรือ partition เช่น Diskette หรือ Handy drive เป็นต้น

การใช้ mount เป็นสิ่งที่ผู้ดูแลระบบต้องเข้าใจหลักการให้ได้ เพราะเป็นช่องทางในการติดต่อกับอุปกรณ์ต่าง ๆ ล่าสุด ผมต่อ harddisk เข้าไปในเครื่อง server เพิ่มอีก 1 ตัว ซึ่งระบบมอง harddisk ตัวที่เพิ่มเข้าไปเป็น hdc ด้วยคำสั่ง fdisk -l เมื่อต้องการ partition ที่ 1 ของ hdc มาเป็นห้อง /x ก็เพียงแต่ใช้คำสั่งสร้างห้องคือ #mkdir /x สำหรับครั้งแรก แล้วใช้คำสั่ง #mount /dev/hdc1 /x ก็จะใช้ห้อง /x ซึ่งอยู่ใน harddisk อีกตัวหนึ่งได้ทันที

คำสั่งที่เกี่ยวข้องกับคำสั่ง mount

#cat /etc/fstab : ดู file system table เพื่อบอกว่ามีอะไร mount ไว้แล้วบ้าง
#cat /etc/mtab : ดูรายละเอียดการ mount ในอีกรูปแบบหนึ่ง
#cat /proc/mounts : บอกว่ามีอะไร mount ไว้แล้วบ้าง
#cat /proc/partitions : บอกชื่อ และขนาดของแต่ละ partitions
#cat /proc/filesystems : บอกประเภทของ filesystems ที่มีการสนับสนุน
#/sbin/fdisk -l : แสดง partition จาก harddisk ทุกตัวที่เชื่อมต่อในเครื่องนั้น

1. วิธีใช้แผ่น floppy disk ใน linux

#mkdir /floppy
#mkfs -t ext3 /dev/fd0 1440
#mount -t ext3 /dev/fd0 /floppy
- or -
#mkdir /floppy
#mkfs -t msdos /dev/fd0 1440
#mount -t msdos /dev/fd0 /floppy
ต่อไปในห้อง /floppy ก็คือแผ่น disk ใน drive A ส่วน /dev/fd1 ก็คือ drive B แต่ต้องเริ่มทำใหม่นะครับ

2. วิธีใช้ Handy drive เช่น apacer (ต้อง umount ก่อนดึง apacer ออกก่อนเสมอ)

#mkdir /mnt/apacer (Just first time)
#mount /dev/sda1 /mnt/apacer
...
#cd /
#umount /dev/sda1
- and -
#pico /etc/fstab Add: /dev/sda1 /mnt/apacer auto noauto,user 0 0

3. วิธีเรียกใช้แฟ้มใน partition อื่น เช่น WindowsXP

cd / :: ย้ายตัวเองไปยัง root directory
mkdir hd :: สร้างห้องชื่อ hd ซึ่งเป็นห้องเปล่าไม่มีอะไร
fdisk -l :: ดูว่ามี partition อะไรในเครื่องบ้าง ที่ต้องการ mount เข้ากับ /hd
mount /dev/hdb2 /hd :: ทำให้เรียกใช้ /dev/hdb2 จาก /hd ได้ เช่น cd /hd/etc ถ้าใน hdb2 มีห้องชื่อ etc
umount /hd :: ยกเลิกการ mount /hd

4. วิธีใช้ CDROM

mount :: แสดงรายการอุปกรณ์ หรือห้องต่าง ๆ ที่ถูก mount ไว้แล้ว
mount -t ext3 :: แสดงให้เห็นว่า partition แบบ ext3 มีอะไรถูก mount ไว้บ้าง
mount -t vfat :: แสดงให้เห็นว่า partition แบบ vfat มีอะไรถูก mount ไว้บ้าง
mount /dev/cdrom :: ใช้ติดต่อ CD ROM เมื่อเข้าไปใช้เช่น #cd /mnt/cdrom และใช้ #ls
umount /dev/cdrom :: เพื่อเลิกใช้ CD ROM หรือต้องการดึงแผ่นออก แต่ท่านต้องออกมาก่อนด้วยคำสั่ง #cd / เป็นต้น
eject :: ถ้าไม่ umount ด้านล่าง ก็สั่ง eject เพื่อดีด CD-ROM ออกได้เลยครับ และไม่ต้องสั่ง umount หรือออกจากห้องก่อนนะ

ตัวอย่างผลการใช้คำสั่ง mount ใน server ตัวหนึ่ง

/dev/hda5 on / type ext3 (rw)
none on /proc type proc (rw)
/dev/hda1 on /boot type ext3 (rw)

none on /dev/pts type devpts (rw,gid=5,mode=620)
/dev/hda3 on /home type ext3 (rw)
none on /dev/shm type tmpfs (rw)
/dev/hda2 on /usr type ext3 (rw)
/dev/hda6 on /var type ext3 (rw)

คำสั่ง mkbootdisk : สร้างแผ่น boot disk เพื่อใช้ boot ระบบ linux ขึ้นมาภายหลัง และมีการทำงานแบบ stand alone

คำสั่งนี้ผมเคยใช้ตอนคัดลอก harddisk ที่เป็น linux 2 ตัว แต่ตัวลูกเมื่อนำไปเสียบเข้าเครื่องใหม่ พบว่า boot ด้วยตนเองไม่ได้ จึงต้องหาแผ่น boot จนเข้าไปใน harddisk ได้ จากนั้นก็สั่ง #lilo เพื่อให้การ boot ครั้งต่อไปสามารถทำงานตาม /etc/lilo.conf ได้ตามปกติ ส่วนตัวเลข 2.4.18-14 เป็นเลขรุ่นของ kernel ใน Redhat 8.0 สังเกตเลขนี้ได้ตอน boot เครื่อง

ตัวอย่างคำสั่ง และการใช้งาน

mkbootdisk --device /dev/fd0 2.4.18-14 :: สร้างแผ่น disk เพื่อใช้ boot เข้า linux ในกรณีที่ระบบ boot ของเครื่องมีปัญหา

คำสั่ง traceroute : แสดงเลข ip ของเครื่องที่ถูกเชื่อมต่อทั้งหมด ไปยังปลายทางที่ต้องการ

ตัวอย่างข้างล่างนี้แสดงให้เห็นว่า เมื่อในวิทยาลัยโยนกเปิดเว็บ www.thai.net จะต้องติดต่อผ่านเครื่องบริการ 8 ตัว ดังตัวอย่างล่างนี้ ถ้าเปิดเว็บไซต์ต่างประเทศ ก็จะมีจำนวนเครื่องในการติดต่อมากขึ้นไปด้วย เครื่องบริการในที่นี้ มักเป็นอุปกรณ์ที่เรียกว่า router และ router ทุกตัวจะมี ip และความสามารถเฉพาะตัวที่ต่างกันไป โดยหน้าที่หลักของ router ก็คือการกำหนดเส้นทางในการติดต่อนั่นเอง

ตัวอย่างคำสั่ง และการใช้งาน

/usr/sbin/traceroute www.thai.net

```
traceroute to www.thai.net (203.150.13.2), 30 hops max, 38 byte packets
 1  door.yonok.ac.th (202.29.78.254)  2.046 ms  1.962 ms  2.532 ms
 2  202.28.29.41 (202.28.29.41)  3.703 ms  3.294 ms  3.760 ms
 3  UniNet-BKK2-ATM1-0-0.700.uni.net.th (202.28.28.129)  14.185 ms  13.226 ms  14.614 ms
 4  202.28.28.18 (202.28.28.18)  13.705 ms  13.227 ms  14.130 ms
 5  202.47.255.2 (202.47.255.2)  13.222 ms  13.890 ms  13.210 ms
 6  202.129.63.182 (202.129.63.182)  16.649 ms  14.960 ms  15.659 ms
 7  juliet-vlan-2.bkk.inet-th.net (203.150.14.22)  14.817 ms  15.573 ms  15.610 ms
 8  www.thai.net (203.150.13.2)  15.628 ms  14.775 ms  14.222 ms
```

คำสั่ง rpm : ใช้ตรวจสอบ เพิ่ม หรือลบ package ของระบบ linux เกือบทั้งหมด

ในกรณีที่ท่านมีโปรแกรมตัวใหม่มา สามารถที่จะลบโปรแกรมเพิ่มโดยใช้คำสั่ง rpm ได้ หรือต้องการตรวจสอบว่า มี package บางตัว install อยู่หรือไม่ หรือจะยกเลิกโปรแกรมบางตัวออกจากระบบก็ทำได้ หรือจะแสดงรายชื่อ package ทั้งหมดในระบบก็ทำได้อีก รวมทั้งการตรวจ version ของ package แต่ละตัว

จากประสบการณ์ ไม่แน่ใจว่าเกิดจากอะไร เมื่อลง Redhat 7.2 แล้ว แต่ระบบไม่บริการ pop3 จึงได้ทำการ **mount /dev/cdrom** จากนั้นก็ทำการ install package pop เพิ่มเข้าไป ที่รู้เพราะลองใช้คำสั่ง **telnet localhost 110** แล้ว error จึงต้องทำการเพิ่ม package pop เข้าไปใหม่ โดยใช้คำสั่ง **rpm -i imap-4.7-5.i386.rpm** ที่รู้เพราะได้ใช้ cd เข้าไปในห้อง /mnt/cdrom/RedHat/RPMS จึงพบแฟ้มมากมายที่สามารถ install เพิ่มได้

ตัวอย่างคำสั่ง และการใช้งาน

rpm -i imap-4.7-5.i386.rpm :: ใช้ install package pop เข้าไปใน linux ใหม่ เพราะไม่มี และให้ดูเพิ่มเติมจาก 8.99 เกี่ยวกับการติดตั้งโปรแกรมจาก CD-ROM

rpm -qa|grep imap :: ใช้ดูว่ามี package อะไรบ้างที่ขึ้นต้นด้วย imap

rpm -qa :: ใช้ดูรายชื่อ package ทุกตัวที่ install ไว้แล้ว

rpm -q telnet :: ใช้ตรวจว่ามี package ชื่อ telnet อยู่หรือไม่

rpm -qpl imap-4.7-5.i386.rpm :: แสดงชื่อแฟ้มใน package แต่ต้องเข้าไปที่ /mnt/cdrom/RedHat/RPMS ก่อนนะครับ

rpm -qf /usr/sbin/vi :: จะแสดง vim-minimal-5.6-11 ซึ่งเป็นรุ่นของ vi นั้น

rpm -qf /usr/sbin/httpd :: จะได้ apache-1.3.12-2 ซึ่งเป็นรุ่นที่ติดตั้งมาใน linux 6.2

rpm -e apache-1.3.12-2 :: ลบ หรือ erase โปรแกรม apache-1.3.12-2 ออกจากเครื่อง

rpm -Fvh openssl-0.9.5a-2.6.x.i386.rpm :: Upgrade โปรแกรม แต่ต้องลงโปรแกรมก่อนมิเช่นนั้น ไม่สำเร็จนะครับ

คำสั่ง SU : ขอเปลี่ยนตนเองเป็น Super user เพื่อใช้สิทธิ์สูงสุดในการบริหารระบบ ที่ผู้ใช้ปกติทำไม่ได้

การจะใช้ su ได้จะต้องเป็นผู้ใช้ตามปกติ เมื่อพิมพ์ su แล้วระบบจะถามรหัสผ่าน หากพิมพ์รหัสผ่านถูกต้อง ท่านก็จะสามารถกระทำการใด ๆ ก็ได้ เพราะ super user คือผู้ที่มีอำนาจสูงสุดในระบบ เช่น เพิ่มผู้ใช้ท่านใหม่ ลบผู้ใช้คนเดิม เป็นต้น (**เพียงแต่พิมพ์คำว่า su ท่านก็สามารถเปลี่ยนสิทธิ์ได้แล้ว ถ้าท่านมีรหัสผ่านของ su**)

ตัวอย่างคำสั่ง และการใช้งาน

#su :: เปลี่ยนตนเองเป็น super user เพื่อกระทำการใด ๆ ก็ได้กับตัวระบบ

#su webmail :: ไม่ว่าขณะที่ login เป็น user ใด เมื่อต้องการเปลี่ยนเป็นอีกคนหนึ่ง ก็ไม่ต้อง logout แล้ว login ใหม่ ใช้คำสั่งนี้ได้เลย

คำสั่ง useradd : เพิ่มผู้ใช้รายใหม่เข้าไปในระบบ

ตัวอย่างคำสั่ง และการใช้งาน

#useradd theman :: เพิ่มผู้ใช้รายใหม่เข้าไปในระบบชื่อ theman ในกลุ่ม theman และมี home directory เป็น /home/theman

#useradd -g users -d /home/theman -c "user name here" theman :: เพิ่มผู้ใช้รายใหม่เข้าไปในระบบชื่อ theman

---

คำสั่ง userdel : ลบผู้ใช้รายเดิม ออกจากระบบ

ตัวอย่างคำสั่ง และการใช้งาน

#userdel -r theman :: ลบ theman และ home directory ของ theman ออกหมด

คำสั่ง usermod : แก้ไขข้อมูลของผู้ใช้ได้

ตัวอย่างคำสั่ง และการใช้งาน

#usermod -s /rbin/menu theman :: กำหนดให้ shell สำหรับ user ที่ชื่อ theman ใหม่เพื่อจำกัดสิทธิ์ในการเข้าใช้ shell

#usermod -d /home/theman theman :: กำหนดให้ theman มี homedirectory อยู่ที่ /home/theman

#usermod -c "Mr.Suwit Somsupabrungyod" theman :: กำหนดให้ comment หรือชื่อเป็น Mr.Suwit Somsupabrungyod ซึ่ง comment จะไปแสดงผลให้เห็นชัดเจนตอนที่ใช้ pine เมื่อพิมพ์คำว่า theman ในช่อง to ขณะที่กำลัง compose จะแสดง comment หน้า email ให้ทันที

คำสั่ง crontab : ตั้งเวลาสั่งงานคอมพิวเตอร์

ตัวอย่างคำสั่ง และการใช้งาน

#crontab -l :: แสดงกำหนดการของการสั่งให้คอมพิวเตอร์ทำงานอย่างอัตโนมัติ ตามเวลาที่กำหนด

#cat /etc/crontab :: แสดงตาราง crontab ในเครื่อง

คำสั่ง lspci : ตรวจสอบอุปกรณ์ที่เชื่อมต่อภายในเครื่อง

ตัวอย่างคำสั่ง และการใช้งาน

#lspci

00:00.0 Host bridge: Intel Corp. 440BX/ZX/DX - 82443BX/ZX/DX Host bridge (rev 03)
00:01.0 PCI bridge: Intel Corp. 440BX/ZX/DX - 82443BX/ZX/DX AGP bridge (rev 03)
00:07.0 ISA bridge: Intel Corp. 82371AB/EB/MB PIIX4 ISA (rev 02)
00:07.1 IDE interface: Intel Corp. 82371AB/EB/MB PIIX4 IDE (rev 01)
00:07.2 USB Controller: Intel Corp. 82371AB/EB/MB PIIX4 USB (rev 01)
00:07.3 Bridge: Intel Corp. 82371AB/EB/MB PIIX4 ACPI (rev 02)
00:0f.0 PCI bridge: Digital Equipment Corporation DECchip 21152 (rev 03)
00:11.0 Ethernet controller: 3Com Corporation 3c905B 100BaseTX [Cyclone] (rev 24)
01:00.0 VGA compatible controller: ATI Technologies Inc 3D Rage Pro AGP 1X/2X (rev 5c)

คำสั่ง nmap : ตรวจสอบเครือข่ายแบบกวาดทั้งในเครื่อง และ class C

ตัวอย่างคำสั่ง และการใช้งาน

#nmap -sP 202.29.78.*
Starting nmap V. 3.00 (www.insecure.org/nmap/)
Host (202.29.78.0) seems to be a subnet broadcast address (returned 1 extra pings).
Note -- the actual IP also responded.
Host www.isinthai.com (202.29.78.1) appears to be up.
Host course.yonok.ac.th (202.29.78.5) appears to be up.
Host yonok.ac.th (202.29.78.12) appears to be up.
Host w2kdhcp.yonok.ac.th (202.29.78.17) appears to be up.
Host (202.29.78.31) appears to be up.
Host (202.29.78.32) appears to be up.
Host (202.29.78.33) appears to be up.
#nmap -sT www.yonok.ac.th (on TCP)
Starting nmap V. 3.00 (www.insecure.org/nmap/)
Interesting ports on yonok.ac.th (202.29.78.12):
(The 1590 ports scanned but not shown below are in state: closed)

Port	State	Service
21/tcp	open	ftp
22/tcp	open	ssh
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
109/tcp	open	pop-2
110/tcp	open	pop-3

#nmap www.yonok.ac.th -sU (on UDP)
Starting nmap V. 3.00 (www.insecure.org/nmap/)
Interesting ports on yn1.yonok.ac.th (202.29.78.12):

(The 1465 ports scanned but not shown below are in state: closed)

Port	State	Service
53/udp	open	domain
111/udp	open	sunrpc
867/udp	open	unknown

กำหนด IP address และ host name : เพื่อกำหนด ip ให้กับ eth0 (Ethernet card เบอร์แรกคือเบอร์ 0)

ขั้นตอนการแก้ไข IP และ Host name

/etc/hosts

```
127.0.0.1       localhost.localdomain localhost
202.29.78.1     www.isinthai.com  isinthai.com www
```

/etc/sysconfig/network

```
NETWORKING = yes
HOSTNAME = yn1
GATEWAY = 202.29.78.254
```

/etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
BROADCAST=202.29.78.255
IPADDR=202.29.78.12
NETMASK=255.255.255.0
NETWORK=202.29.78.0
ONBOOT=yes
USERCTL=no
PEERDNS=no
TYPE=Ethernet
```

/etc/resolv.conf

```
nameserver 202.29.78.12
```

สามารถใช้คำสั่ง **setup** แล้วเลือก Network Configuration เป็นอีกวิธีหนึ่ง เพื่อเข้าแก้ IP Address ซึ่งจะแก้ไขแฟ้มต่าง ๆ ให้อัตโนมัติ จากนั้นก็สั่ง #/etc/init.d/network restart

โปรแกรมเพิ่มผู้ใช้ /usr/bin/_crt : โปรแกรมนี้เป็น shell script สำหรับเพิ่มผู้ใช้อย่างง่าย สร้างด้วย pico และกำหนดให้ประมวลผลด้วย chmod

โปรแกรมนี้ชื่อ _crt ถูกเก็บไว้ในห้อง /usr/bin โดยกำหนดให้ chmod 700 เพื่อให้สั่งประมวลผล shell script ตัวนี้ได้ และการจะใช้โปรแกรมนี้ได้จะต้องกำหนด PATH ไว้ที่ห้อง /usr/bin และ /usr/sbin จึงต้องกำหนด PATH เพิ่มเติม
จากเดิม PATH=$PATH:$HOME/bin (ถ้า admin ไม่แก้ไขให้ก่อนนะครับ)
เป็นใหม่ PATH=$PATH:$HOME/bin:/sbin:/usr/bin:/usr/sbin
ตรวจสอบตัวแปร PATH ด้วยคำสั่ง echo $PATH
ปัญหานี้จะไม่เกิดขึ้น ถ้ากำหนดไว้ในแฟ้ม .bash_profile ในห้อง **/etc/skel** เพราะเป็นห้องที่เก็บค่าเริ่มต้น

Version 1: ตัวอย่างโปรแกรมที่ใช้งานอยู่

```
#!/bin/bash
echo Username
read un
echo Realname
read cm
```

```
finger $un
echo ==============================
read sure
RESULT="Error - Try other username again .. "
EXIST=0
id $un >/dev/null 2>/dev/null && EXIST=1
if [ $EXIST = 0 ]; then
useradd -g users -d /home/httpd/cgi-bin/$un -c "$cm" $un
chown $un:users /home/httpd/cgi-bin/$un
chmod 705 /home/httpd/cgi-bin/$un
usermod -d /home/httpd/cgi-bin/$un $un
ln -s /home/httpd/cgi-bin/$un /home/httpd/html/$un
passwd $un
RESULT="Complete"
fi
echo "Add new user : $RESULT"
```

Version 2: โปรแกรมข้างล่างนี้ใช้กับเครื่องที่ใช้งาน ssi ได้

```
#!/bin/bash
clear
echo _CRT version 2.June42001
echo User name
read un
echo Real Name
read cm
finger $un
echo ==============================
echo Are you ok?
RESULT="Error - Try other username again .. "
EXIST=0
id $un >/dev/null 2>/dev/null && EXIST=1
if [ $EXIST = 0 ]; then
read sure
useradd -g users -d /home/httpd/html/$un -c "$cm" $un
chmod 705 /home/httpd/html/$un
passwd $un
RESULT="Complete"
fi
echo "Add new user : $RESULT"
```

Version 3: โปรแกรมข้างล่างนี้ใช้กับ isinthai.com ในช่วงปิด telnet เพื่อให้ upload ผ่านเว็บ

เหตุที่ใช้แฟ้มชื่อ password.pl เพราะป้องกันการแอบเปิดดูรหัสผ่าน แล้วแฟ้มนี้ใช้สำหรับบริการ upload (ซึ่งไม่ได้เข้ารหัสไว้)

```
#!/bin/bash
echo Username
read un
echo Real name
read cm
echo Password
read password
finger $un
echo ==============================
echo Are you ok?
RESULT="Error - Try other username again .. "
EXIST=0
id $un >/dev/null 2>/dev/null && EXIST=1
if [ $EXIST = 0 ]; then
read sure
useradd -g users -d /home/httpd/html/$un -c "$cm" $un
chmod 777 /home/httpd/html/$un
echo $password>/home/httpd/html/$un/password.pl
```

```
chown nobody:nobody /home/httpd/html/$un/password.pl
chmod 700 /home/httpd/html/$un/password.pl
passwd $un
RESULT="Complete"
fi
echo "Add new user : $RESULT"
```

เจอปัญหาใช้ useradd ไม่ได้เพราะ lock
มีเรื่องแปลกเกิดขึ้นครับ ทำให้ไม่สามารถเพิ่ม user ได้
useradd: error locking shadow group file หรืออะไรทำนองนี้
ไม่แน่ใจว่าเกิดขึ้นเพราะเหตุใด แต่แก้ไขด้วยการลบแฟ้มที่ ls -al *.lock
หรือที่มีนามสกุลเป็น .lock ในห้อง /etc เช่น passwd.lock group.lock เป็นต้น
และทุกแฟ้มก็มีค่าเป็น 741 เหมือนกันหมด สันนิฐฐานว่าเป็นเลข ps ที่ทำการ lock ไว้

โปรแกรมลบผู้ใช้ /usr/bin/_del : โปรแกรมนี้เป็น shell script สำหรับลบผู้ใช้อย่างง่าย สร้างด้วย pico และกำหนดให้ประมวลผลด้วย chmod

รายละเอียดอ้างอิงจากการเพิ่มผู้ใช้ได้เลย
โปรแกรมนี้ชื่อ _del ถูกเก็บไว้ในห้อง /usr/bin โดยกำหนดให้ chmod 700 เพื่อให้สั่งประมวลผล shell script ตัวนี้ได้

ตัวอย่างโปรแกรมที่ใช้งานอยู่

```
echo Username
read un
finger $un
echo ==========================================
echo If already exist, you can delete this account.
echo If you are not sure, Please Ctrl-C
read sure
echo Ask you again and last time? Ctrl-C if you are not sure.
read sure
userdel -r $un
rm -r /home/httpd/html/$un
echo complete
```

แก้ไข aliases ของ user account : ช่วยกระจาย e-mail ของผู้ใช้ 1 คนไปหลายคน เช่น มีคนส่ง mail ถึง webmaster จะกระจายไปให้สมาชิกได้หลาย ๆ คน

สร้าง account ชื่อ webmaster แล้วแก้ไข /etc/aliases ด้วย pico สำหรับส่ง mail forward ไปยังบุคคลที่เป็น webmaster@isinthai.com หลังแก้ไขแล้วให้ใช้คำสั่ง newaliases เพื่อให้ผลการ update มีผล
หลังใช้ newaliases เมื่อมีคนส่ง mail ถึง webmaster@isinthai.com จะ forward mail ไปให้บุคคล 3 คน พร้อม ๆ กัน ถ้าหากเพิ่มก็เข้าไปแก้ไขแฟ้ม /etc/aliases ใหม่ ก็สามารถกระทำได้

ขั้นตอน

```
#pico /etc/aliases
        webmaster:suwit@yonok.ac.th,prasert@cat.net.th,phimine@yonok.a
        c.th,burin@yonok.ac.th,atichart@yonok.ac.th
        news: webmaster@yonok.ac.th
        pattama: pattamageng@hotmail.com
        chalermchai: chal@yonok.ac.th

#newaliases
```

เพิ่ม IP ใน server ตัวเดียวด้วย IFCONFIG

: เพื่อให้ server 1 ตัวมี ip ได้หลาย ๆ ตัว

เดิมที **ไม่ทราบความสามารถนี้ และไม่เคยคิดจะใช้** แต่เมื่อวันที่ 11 เมษายน 2544 เครื่อง Web server และ Radius server เครื่องเดียวกัน เกิดหยุดทำงานในระดับ Media error แถมเป็นเครื่อง sun ที่ผมไม่มี software สำหรับลงใหม่ จึงต้องใช้เครื่อง Redhat 7.2 อีกเครื่องหนึ่งมากู้สถานการณ์ โดยสมมติว่าเครื่องที่ล่มไป มี ip เป็น 202.29.78.2 ผมเพียงกำหนด ip ในเครื่อง Redhat ให้เพิ่ม ip สำหรับเครื่องขึ้นอีก 1 หมายเลข คำสั่งข้างล่างนี้จะทำให้มีผลทันที แต่เมื่อเปิดเครื่องใหม่จะไม่คงอยู่ จึงต้องแก้แฟ้ม **/etc/rc.d/rc.local** หรือ **/etc/rc.d/rc.local**โดยเพิ่มบรรทัดข้างล่างนี้เข้าไป ก็เป็นอันเรียบร้อย
สำหรับ Web server ผมต้อง copy ข้อมูลทั้งหมดมาใส่ในเครื่องใหม่จึงจะใช้งานได้ ส่ง radius server ก็ต้อง copy config มาทับ ซึ่งมี 2 แฟ้มคือ users และ clients เพียงเท่านี้ ตัว Modem ก็สามารถติดต่อกับ Radius server ตัวใหม่ได้อย่างไม่มีปัญหา

/sbin/ifconfig eth0:1 192.168.3.1 เพิ่ม IP ปลอม ก็ทำได้ เพื่อใช้เป็น DHCP server
/sbin/ifconfig eth0:2 202.29.78.15
/sbin/ifconfig eth0:3 202.29.78.1
+ หลังเปลี่ยนชื่อ hosts และ ip ใน /etc/hosts /etd/sysconfig/network และ /etc/sysconfig/network-scripts/ifcfg-eth0 แล้ว
+ ไม่ต้อง reboot เครื่องก็ได้ แต่ใช้คำสั่ง #/etc/init.d/named restart ได้นะครับ

เพิ่ม Virtual hosts : เพื่อให้ server 1 ตัว มีหลายเว็บไซต์

การทำ Virtual hosts มี 2 วิธี

1. Name-based virtual hosts (ผมเลือกใช้ตัวนี้ เพราะในเครือข่ายมีจำนวน ip จำกัด)
2. IP-based virtual hosts (แบบนี้ในสำนักงานแห่งหนึ่งใช้ เพราะมี ip ใช้ไม่จำกัด)

1. Name-based virtual hosts
เทคนิคนี้ ผู้บริหาร host หลายแห่งใช้ เพราะทำให้ได้ชื่อมากมายตามที่ต้องการในเครื่องบริการเพียงเครื่องเดียว ในวิทยาลัยโยนก ใช้วิธีนี้ เพราะมีผู้ดูแลเพียงไม่กี่คน และมี IP จำนวนจำกัด จึงใช้ server เครื่องเดียว และ IP เบอร์เดียว เช่น 202.29.78.12 เป็นต้น เว็บไซต์ที่ใช้หลักการนี้คือ thaiall.com ที่สมัครใช้บริการของ hypermart.net เมื่อทดสอบ ping www.thaiall.com จะพบเลข ip แต่เมื่อเปิดเว็บตาม ip จะไม่พบเว็บของ thaiall.com เพราะ thaiall.com มิใช่เจ้าของ ip เพียงคนเดียว
การเพิ่ม Virtual hosts แบบนี้ต้องทำคู่กับการแก้ไขระบบ named ในห้อง /var/named เพื่อสร้าง ip หรือ host name สำหรับเว็บไซต์ใหม่ภายใน server ตัวเดียวกัน เพิ่มในแฟ้ม /etc/httpd/conf/httpd.conf มีรายละเอียดเพิ่มเติมเรื่อง virtual hosts ที่ http://httpd.apache.org/docs-2.0/vhosts/ ตัวอย่างข้างล่างนี้คือการเพิ่มชื่อ http://science.yonok.ac.th เข้าไปใน server ที่บริการ http://www.yonok.ac.th

มีขั้นตอนดังนี้

1. แก้ไขแฟ้ม **/var/named/db.yonok.ac.th** กำหนดให้เครื่องเดียวมีหลายชื่อ

```
www     IN  A  202.29.78.12
science IN  A  202.29.78.12
```

3. แก้ไขแฟ้ม **/etc/httpd/conf/httpd.conf** กำหนดห้องเก็บเว็บ ให้กับชื่อโฮส

```
NameVirtualHost 202.29.78.12
<VirtualHost 202.29.78.12>
 ServerAdmin webmaster@yonok.ac.th
 DocumentRoot /var/www/html
 ServerName star.yonok.ac.th
</VirtualHost>
<VirtualHost 202.29.78.12>
 ServerAdmin phimine@yonok.ac.th
 DocumentRoot /var/www/html/science
```

```
ServerName science.yonok.ac.th
</VirtualHost>
<VirtualHost 202.29.78.12>
ServerAdmin burin@yonok.ac.th
DocumentRoot /var/www/html/e-learning
ServerName e-learning.yonok.ac.th
<Directory /var/www/html/e-learning>
Options All
AddType text/html .shtml .htm .html
AddHandler server-parsed .shtml .htm .html
</Directory>
</VirtualHost>
```

26. #/etc/init.d/named restart
27. #/etc/init.d/httpd restart

2. IP-based virtual hosts

การเพิ่ม Virtual hosts มักทำงานคู่กับ ifconfig และแฟ้มในห้อง /var/named เพื่อสร้าง ip หรือชื่อ host สำหรับเว็บไซต์ขึ้นใหม่ การสร้างเว็บไซต์ใหม่ สำหรับ server ตัวเดียวกัน เพิ่มในแฟ้ม /etc/httpd/conf/httpd.conf มีรายละเอียดเพิ่มเติมเรื่อง virtual host ที่ http://httpd.apache.org/docs-2.0/vhosts/ ตัวอย่างบริการนี้จะพบตาม web hosting ต่าง ๆ ที่ระบุว่าเมื่อใช้บริการ เจ้าของ domain name จะได้ ip ส่วนตัว เป็นต้น
เทคนิคนี้ ทำให้ประหยัดเครื่องบริการ ในบริษัทที่ผมเป็นที่ปรึกษามี local ip จึงใช้ ip แยก directory ต่าง ๆ ออกจากกัน แต่ใช้ server เพียงเครื่องเดียว เช่น 192.168.16.1 หมายถึงเครื่องสมาชิก 192.168.16.2 หมายถึงเครื่องพนักงาน แต่ทั้งบริษัทมีเครื่อง server เพียงเครื่องเดียว ก็สามารถมี ip สำหรับสมาชิกแต่ละคนได้ ผู้ให้บริการ hosting หลายแห่งก็ใช้วิธีนี้ เมื่อกำหนด virtual host แล้ว ผู้ใช้สามารถเปิดเว็บด้วยตัวเลข หรือตัวอักษรก็ได้ เพราะกำหนดห้องปลายทางที่ต้องการ เช่น http://www.isinthai.com หรือ http://202.29.78.1 เป็นต้น

มีขั้นตอนดังนี้

1. แก้ไขแฟ้ม /etc/rc.d/rc.local โดยเพิ่ม **/sbin/ifconfig eth0:1 202.29.78.1** อีก 1 บรรทัด
2. แก้ไขแฟ้ม /var/named/db.202.29.78 โดยเพิ่ม **1 IN PTR www.isinthai.com.**
3. แก้ไขแฟ้ม **/etc/httpd/conf/httpd.conf** กำหนดห้องเก็บเว็บ ให้กับชื่อโฮส

```
<VirtualHost 202.29.78.12>
ServerAdmin webmaster@yonok.ac.th
DocumentRoot /var/www/html
ServerName star.yonok.ac.th
</VirtualHost>
<VirtualHost 202.29.78.1>
ServerAdmin burin@yonok.ac.th
DocumentRoot /var/www/html/isinthai
ServerName www.isinthai.com
</VirtualHost>
```

13. #/etc/init.d/named restart
14. #/etc/init.d/httpd restart

หมายเหตุ : index.php เป็นแฟ้มที่ใช้แยกห้องตามชื่อที่ส่งเข้ามา เป็นความต้องการพิเศษของโยนก

เมื่อพิมพ์ว่า http://www.yonok.ac.th และ http://www.isinthai.com จะเรียกจุดเดียวกัน แต่ใช้ php แยกห้องให้

```
<?
if($_SERVER["SERVER_NAME"]=="www.isinthai.com" ||
$_SERVER["SERVER_NAME"]=="202.29.78.1"){
header("Location: http://".$_SERVER["SERVER_NAME"]."/isinthai/");
} else {
header("Location: http://".$_SERVER["SERVER_NAME"]."/main/");
```

```
}
exit;
?>
```

ตัวอย่าง router configuration : config ของ router ทำโดยผู้ดูแลเท่านั้น และมักทำไม่บ่อยเลย บางคน config ครั้งเดียวจบครับ

```
c:\telnet router.yonok.ac.th
username : superman
password : supergirl
```

```
yonok-router>en
Password:
yonok-router#show run
Building configuration...

Current configuration : 1905 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname yonok-router
!
aaa new-model
!
aaa session-id common
enable secret 5 aaaaQT$u.xb5Wxpxk5aaaaaaa
enable password 7 aaaa3080aaa
!
username superman password 7 aaaa81F1C354aaa
ip subnet-zero
!
interface FastEthernet0/0
 ip address 202.29.78.254 255.255.255.0
 speed auto
 full-duplex
 no cdp enable
!
interface Serial0/0
 ip address 202.28.29.42 255.255.255.252
 ip access-group 102 in
 ip access-group 101 out
 no cdp enable
!
router igrp 1
 redistribute connected
 network 202.28.29.0
 network 202.29.78.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
ip route 0.0.0.0 0.0.0.0 202.28.29.41
no ip http server
```

```
ip pim bidir-enable
!
access-list 101 deny   tcp host 202.29.78.13 any eq ftp
access-list 101 deny   tcp host 202.29.78.13 any gt 6000
access-list 101 permit ip any any
access-list 102 deny   tcp any 202.29.78.0 0.0.0.255 eq 135
access-list 102 deny   udp any 202.29.78.0 0.0.0.255 eq 135
access-list 102 permit ip any any
access-list 103 deny   tcp host 202.29.78.18 any eq ftp
access-list 103 deny   tcp host 202.29.78.18 any gt 2000
access-list 103 permit ip any any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
no cdp run
snmp-server community public RO
banner login ^CC
**************************************************************************
**
* www.yonok.ac.th                                        *
**************************************************************************
**
^C
!
line con 0
line aux 0
line vty 0 4
 password 7 aaa385F5A0aaa
!
end

yonok-router#
```

ความผิดพลาด : ถ้าไม่ทำอะไร ก็คงไม่ผิดพลาด ผมทำอะไรหลายอย่างจนพบว่าความผิดพลาดนั้นเป็นเรื่องปกติ ซึ่งสามารถนำมาเล่าสู่กันฟังได้ดังนี้

1. **linux vga=791** เป็นวิธีเข้า linux แบบ graphic mode เพราะเครื่องผมเป็น notebook ECS 29,900 บาท เมื่อ Boot ด้วย CD ของ Redhat9.0 หน้าจอจะเป็นสีฟ้า ไม่ว่าจะเข้าแบบใด และการเข้าไม่ว่าแบบใด เมื่อเติม vga=791 ก็จะทำให้เข้าสู่ Redhat ได้ไม่มีปัญหาด้านการแสดงผล
2. **imap-2000** เป็นโปรแกรมสำหรับ upgrade imap ตัวเดิม ผมไม่สามารถให้บริการ imap ผ่าน pop จึงต้องใช้ตัวเก่า แต่ก็ไม่รู้วิธีลบออก ผมหาวิธีลบตั้งนาน แต่พอใช้ rpm -e imap โดยไม่ต้องตามด้วย version ก็ลบได้ แล้วลงตัวเก่า ปรากฏว่าให้บริการ ได้ตามปกติ แต่ต้องไม่ปิด hosts.deny นะครับ ผมพยายามเลือกเปิดแล้วไม่สำเร็จ จึงต้องเปิดหมด .. ปัญหาที่ค้างอยู่คือต้องเปิดหมด ไม่รู้จะเลือกเปิดตัวไหน จึงจะให้บริการ pop3 ได้
3. การคัดลอก **passwd, shadow, group** จากเครื่องหนึ่งมาใส่อีกเครื่องหนึ่ง พร้อม copy mail และ folder ทั้งหมดมา ปัญหาที่ผมมองข้ามไปคือ account บาง account ในเครื่องเดิมมี uid แบบหนึ่ง หากนำ passwd มาทับ หากไม่ mathch กันกับ user เดิมจะเกิดปัญหา ต้องดูว่ามี account เดิมอะไรที่เคย install โปรแกรม เข้าไป ก็ต้องแก้ไขให้ตรงกันก่อน ในเครื่องเก่า แล้วค่อยย้ายมา
4. การ upgrade apache ไม่แน่ใจว่าทำไม โปรแกรมจึงไปเรียก **/usr/sbin/httpd(เก่า) แทน /home/httpd/bin/httpd(ใหม่)** ซึ่งตอนลงครั้งแรกไม่มีปัญหา แต่พอนำโปรแกรม upgrade apache หลังจากลง version ของ apache ใหม่ ก็เกิดปัญหา ผมแก้ไขด้วยการ copy โปรแกรมใหม่ มาทับโปรแกรมเดิม ก็แก้ปัญหาที่ปลายเหตุ ได้ผล
5. จุดบกพร่องของระบบคือ software มีรอยรั่ว ต้อง upgrade software โปรแกรมมากมายที่นำมา upgrade อาจใช้ไม่ได้ เพราะมีเงื่อนไข ในการ upgrade โปรแกรมแต่ละตัว

โปรแกรมหนึ่งที่ทำให้ผมเสียเวลาไป 2 วันคือ **kernel** ซึ่งเป็นโปรแกรมสำคัญ มี 2 (i386 และ i686) ตัวที่ผมได้ทดสอบ upgrade แต่ทั้ง 2 ตัวทำให้เครื่องไม่รู้จัก eth0 ผมอาจแก้ปัญหาไม่ตรงจุดก็ได้ ใช้ route หรือ reboot ก็แล้ว ไม่ work สรุปว่า upgrade kernel ด้วยโปรแกรมจากเว็บของ redhat ไม่ได้ครับ แต่โปรแกรมผมอื่น ก็พยายาม upgrade เข้าไป .. น่าจะป้องกันปัญหา hacker ได้ระดับหนึ่ง

6. **Named** อยู่ ๆ ก็หยุดทำงานไปเฉย ๆ ผมต้อง stop และ start ใหม่ ตอนนี้ไปได้ bind มา upgrade ไม่แน่ใจว่าสำเร็จหรือไม่ ก็ต้องรอดูกันต่อไป
7. เคยสั่ง **700 /tmp** ซึ่งไม่เกิดปัญหา แต่มาพบว่า การใช้ห้ามใช้ห้อง /tmp จะทำให้ pop ใช้งานไม่ได้ และใช้ pine เปิด mail box ก็จะฟ้องว่าเป็น read only ผมจึงไม่สามารถปิด
8. ลง apache ใหม่ ใช้เวลาตั้งนานหาวิธีแก้ไข สุดท้ายก็ไม่ได้ เพราะจำไม่ได้ว่าแก้ไขอะไร /etc/httpd/conf/httpd.conf ก็ไม่ได้ backup ไว้แต่แรก สุดท้ายต้อง upgrade ใหม่ด้วยคำสั่ง rpm -U --fource apache-1.3.14..... แต่ก็ไม่ได้ต้องเข้าไปลบแฟ้ม httpd.conf ออกก่อน จึงจะทำการสร้างใหม่ได้
9. **เปิดเว็บโดยใช้ default index.html แล้วมีปัญหา** ปัญหานี้แก้ได้ แต่ไม่แน่ใจว่าแก้ถูกวิธีหรือไม่ เพราะเดิม ไม่ว่าส่ง หรือรับ จาก telnet ต้องอ้างถึง host name แต่ผมพอแก้แฟ้ม hosts และ sendmail.cf เพื่อทำให้เป็น default แบบไม่มี host name กลับไปมีผลต่อระบบ web ที่เป็น httpd ถ้าไม่แก้ host จะเข้าเว็บเช่น http://www.yonok.ac.th/mba ได้ พอแก้ hosts โดยนำชื่อออกเช่น **202.29.78.12 yonok.ac.th star** จากเดิม **202.29.78.12 star.yonok.ac.th star** เป็นต้น ดังนั้นเพื่อให้ได้ทั้งระบบตัด host name และ default ของทุก directory เป็น index.html จึงต้องแยก web server กับ mail server ออกจากกัน พบว่าปัญหามาจากการตัด host เวลาเข้าเว็บจะเหลือเพียง http://yonok.ac.th/mba ทั้งที่พิมพ์ว่า http://www.yonok.ac.th/mba ซึ่ง error message บอกว่า page not found

---

Server ถูก Hack : ผลของการถูก hack มีลักษณะตามอาการที่ hacker ต้องการ ไม่ซ้ำแบบกัน

37. 15 พฤศจิกายน 2547 เครื่อง class.yonok.ac.th เปิดจากภายนอกไม่ได้ ปัญหานี้ไม่น่าเกิดขึ้น แต่ผมปล่อยเรื้อรังมานาน ประเด็นของปัญหาคือ เปิดเว็บของ server ตัวนี้ผ่าน proxy ไม่ได้ เช่นผู้ใช้จาก 1222 หรือในโรงเรียนต่าง ๆ ที่มี proxy ขวางอยู่ เพราะการเข้าผ่าน proxy จะส่งคำขอเป็น random port เข้า web server เพราะเป็น server ที่เปิดในองค์กรได้ แต่เปิดจากข้างนอก บางองค์กรไม่ได้ จากการตรวจสอบอย่างจริงจัง ก็พบว่า router มีความสามารถ block port ที่มากกว่า 3000 แล้ว ทีมงานเคยกำหนดข้อจำกัดนี้กับ ip ของเครื่อง class.yonok.ac.th เมื่อเอาออก ปัญหานี้ก็หมดไป

36. 19 ตุลาคม 2547 ส่ง e-mail จากโยนก เข้า ISP รายหนึ่งไม่ได้

ทดสอบใช้ **#telnet post.xxx.co.th 25** แล้ว server ของ ISP รายนั้นไม่ตอบกลับมา หลังจากพยายามติดต่อทีมงานของเขาเกือบครึ่งเดือน จึงทราบว่าขนาด banner ที่ตอบกลับมาก ถูก block ระหว่างทาง พอเขาเปลี่ยนขนาด banner ก็สามารถส่ง e-mail ไปถึง SMTP server ของเขาได้ ทางคุณยอด ซึ่งเป็นทีมงานได้ให้ข้อมูลกับผมว่า สิงคโปร์เทเลคอม เคย block package ขนาดนี้ ผลการใช้ traceroute post.xxx.co.th พบ router ที่ต้องผ่านไปหลายตัว จึงต้องไปหาว่า router ตัวไหนของใคร เป็นคนจำกัด package ขนาดเท่านี้บ้าง .. และผมก็ไม่มีความสามารถมากพอที่จะอธิบาย ผู้ดูแล router แต่ละตัว ทาง ISP จึงอาสาจะไป clear ให้

```
#traceroute post.loxinfo.co.th
traceroute to post.loxinfo.co.th (203.146.237.154), 30 hops max, 38 byte packets
 1  door.yonok.ac.th (202.29.78.254)  0.682 ms  0.674 ms  0.717 ms
 2  202.28.29.41 (202.28.29.41)  6.826 ms  4.458 ms  3.469 ms
 3  atm-0-0-0.700.R01.MUA.uni.net.th (202.28.28.129)  18.444 ms  13.924 ms
14.145 ms
 4  202.28.28.18 (202.28.28.18)  15.069 ms  19.641 ms  16.107 ms
 5  202.129.63.82 (202.129.63.82)  14.641 ms  14.266 ms  15.081 ms
 6  cor36-G-cor22.csloxinfo.net (210.1.46.35)  14.843 ms  15.029 ms  14.958 ms
 7  cor35-G-cor22.csloxinfo.net (210.1.46.34)  15.403 ms  16.626 ms  14.658 ms
 8  post.loxinfo.co.th (203.146.237.154)  15.064 ms  15.687 ms  14.859 ms
```

35. 22 ธันวาคม 2546 Uni.net.th ล่มในส่วนของขาออกต่างประเทศ เพราะสาย fiber ขาดในทะเลอีกแล้ว

uni.net.th แจ้งว่าถ้าสถาบันใดเปิด net ในประเทศไม่ได้ ให้แก้ไขแฟ้ม /etc/named.conf ส่วนขาออกต่างประเทศ ถ้ารอบริษัทที่ LA แก้อาจใช้เวลา 5-7 วัน ขณะนี้กำลังขอทาง กสท. เพื่อใช้ขอเชื่อมต่อขาออกนอกประเทศชั่วคราว ถ้าได้ก็จะให้บริการใน spedd ที่ต่ำในระยะสั้นนี้ก่อน สำหรับแฟ้ม /etc/named.conf ที่มีตัวอย่างให้แก้ไข สำหรับสถาบันที่มีปัญหาการเปิดเว็บในประเทศไม่ได้ เป็นดังนี้

```
zone "th" in {
 type forward;
 forward first;
 forwarders {
 202.28.0.1;
 };
};
```

34. 17 ธันวาคม 2546 Server ล่มเพราะ Harddisk มีปัญหา ใช้ fsck ก็ไม่ได้ จึงต้องลง HD ตัวใหม่ HD ที่ backup ไว้ก็ใช้ไม่ได้ จึงต้องลง RH9.0 แล้ว copy ห้องต่าง ๆ เข้า HD ใหม่ จากนั้นก็ใช้ dd backup เข้า HD อีกตัวหนึ่ง ปัญหาที่พบใหญ่มี 2 ปัญหาคือ ระบบบริการ free webhosting โดยฐานข้อมูล user เดิมใช้ไม่ได้ พอติดตั้งใหม่ ก็ได้ แสดงว่าโปรแกรมของ cyberscript.net ไม่เหมาะกับการ copy ข้าม HD อีกปัญหาหนึ่งคือรับ mail จาก server ภายนอกไม่ได้ พอตรวจสอบก็พบว่า sendmail.mc กำหนดเรื่อง procmail แต่ใน HD ใหม่ไม่ได้ใช้ procmail จึงรับฉบับที่มาจากต่างเครือข่ายไม่ได้

33. 10 พฤศจิกายน 2546 เข้า Linux server แบบ Single mode จาก Grub menu
ครั้งนี้ไม่ได้ถูกใคร hack เพราะติดตั้ง 9.0 แล้วปัญหาต่าง ๆ น้อยลงมาก แต่สิ่งที่อยากเล่าให้ฟังคือ การ hack ตนเอง เพราะครั้งหนึ่งทีมงานได้ติดตั้ง RH9.0 โดยเลือก Grub เป็นตัวเริ่มต้นเข้าระบบ ปัญหาคือลืมรหัสผ่านของ root วิธีแก้ใน Redhat รุ่นเก่าคือ การกดปุ่ม ALT-X และพิมพ์ linux single ก็เข้าเป็น root ได้แล้ว แต่สำหรับ Grub จะต้องกดปุ่ม e
เมื่อพบ **kernel (hd0,0)/vmlinuz root=/dev/hda8 devfs=mount hdb=ide-scsi**
ให้เปลี่ยนเป็น **kernel (hd0,0)/vmlinuz root=/dev/hda8 devfs=mount hdb=ide-scsi single**
แล้วกด g ก็จะเข้า single mode ในฐานะ root ได้

32. 31 พฤศจิกายน 2545 DNS server 6.2 ถูก hack ผ่าน ftp
เนื่องจากมีแผนเปลี่ยน upgrade DNS server จึงเปิด ftp เพื่อดึง mail ทั้งหมดลง server ตัวใหม่ แต่ปรากฏว่า hacker เข้ามาตอนตี 1 และเปลี่ยนรหัสผ่านของ root พร้องกับปิด ssh ทำให้ผมไม่สามารถปล่อย server ตัวนี้ต่อไปได้ ต้อง upgrade โดยด่วน

เมื่อตรวจสอบแล้วผมสิ่งผิดปกติบางส่วนดังต่อไปนี้

1. แฟ้ม /etc/rc.d/init.d/network ถูกแก้ไขโดยเพิ่มโปรแกรม /usr/bin/ssh2d -q
2. แฟ้ม network ดังกล่าว เป็น text file แต่ไม่สามารถลบ chmod ได้ แม้จะเป็น root
3. ห้อง /lib/security/.config ถูกสร้างขึ้น และเก็บโปรแกรมร่าง ๆ ที่น่าสงสัยเช่น login และ network เป็นต้น
4. ประวัติการใช้งานในฐานะ root ไม่มีใน .bash_history เพราะถูกลบและเปลี่ยนด้วยคำสั่ง #ln -s /dev/null /root/.bash_history

```
ftp     ftpd6246    211.206.199.98   Fri Dec 27 00:08 - crash  (07:34)
ftp     ftpd5616    211.96.24.84     Thu Dec 26 18:54 - crash  (12:48)
```

31. 31 ตุลาคม 2545 เครื่อง isinthai.com จากความผิดพลาด มิใช่ถูก hack
หลังจากติดตั้งโปรแกรม RedHat 8.0 เรียบร้อยแล้ว ก็จะ backup โดยใช้ ghost แต่แทนที่จะเป็นการ backup กลับเป็นการ restore เพราะสลับกันระหว่างตัวแม่กับตัวลูก ทำให้ข้อมูลทั้งหมดหาย .. จึงเป็นประสบการณ์ว่า การ backup ในครั้งต่อไปต้องระวังให้ดี

30. 21 ตุลาคม 2545 ได้รับแจ้งว่า server ของผมส่ง worm ออกไป จาก noc-auto@skyrr.is
จึงต้องเข้าไปตรวจสอบ ปิดบริการต่าง ๆ และเปลี่ยน OS เป็น RH8.0 โดยขณะนี้เปิดเฉพาะ network และ httpd เท่านั้น จากส่วน setup, system services พร้อมเข้าไปศึกษาวิธีลบ worm ตัวนี้จาก http://www.f-secure.com/v-descs/slapper.shtml
จดหมายอีกฉบับหนึ่งที่มีข้อความคล้ายกัน มาจาก Newyork university โดยเครื่องที่ส่งการโจมตีออกไปเป็นเพื่อเครื่อง Windows 98 ของธุรการในหน่วยงานหนึ่งเท่านั้น แก้ไขโดย format ใหม่ก็ไม่มีอะไรเกิดขึ้นอีก

```
Date: Sun, 20 Oct 2002 16:39:06 GMT
From: Network Operation Center Skyrr <noc-auto@skyrr.is>
Subject: Portscan from 202.29.78.1
```

Possible slapper worm infected host on your network. My timezone is GMT 0.

More info about slapper worm and how to remove it on
http://www.f-secure.com/slapper/
This is an automated message please reply to noc@skyrr.is for more info

Snip from log:

Oct 20 06:12:53 pix2 %PIX-2-106006: Deny inbound UDP
from 202.29.78.1/2002 to 212.30.215.186/2002 on interface ytra
Oct 20 06:54:27 pix2 %PIX-2-106006: Deny inbound UDP
from 202.29.78.1/2002 to 212.30.215.186/2002 on interface ytra
Oct 20 13:11:11 pix2 %PIX-2-106006: Deny inbound UDP
from 202.29.78.1/2002 to 212.30.215.186/2002 on interface ytra
==========
To remove this virus
Delete :
/tmp/.uubugtraq
/tmp/.buqtraq.c
/tmp/.bugtraq
And upgrade OpenSSL to be 0.9.6e or above

Date: Tue, 12 Nov 2002 16:49:02 -0500 (EST)
From: Stephen Tihor <scan-alerts@nyu.edu>
Subject: Scan from 202.29.78.51

On Tuesday, November 12, from 12:58 AM until 12:58 AM EST (GMT -0500) we detected a scan coming from 202.29.78.51, which does not have a reverse mapping in the DNS but which you administer. This IP Address scanned the netbios-ns ports of New York University's network (128.122.0.0/16). Sample router net flow data showing the event is attached.

This is consistent with well-known security exploits, so we have contacted you in hopes you can look into this, find out who was doing the scanning and why, and take steps to prevent it in the future. Please let us know what you find out. The APNIC WhoIs database lists burin@yonok.ac.th as the primary contact for this system. If you are not the appropriate person to handle this matter, please pass this message along to the correct network contact. (It may also be useful to go to http://www.fr1.cyberabuse.org/whois/?page=change and update the prefered contact.)
Thank you for your assistance.
--
Stephen Tihor
Senior Network Security Analyst
Network and System Security Team
New York University
security@nyu.edu
Flow Termination Time - Source Addr Dest Addr Prot S-Port D-Port
Tue Nov 12 00:58:16 2002 - 202.29.78.51 128.122.168.0 UDP 1027 netbios-ns
Tue Nov 12 00:58:16 2002 - 202.29.78.51 128.122.168.1 UDP 1027 netbios-ns

29. 30 กันยายน 2545 ผมได้รับ mail จากผู้ศึกษา Linux เชิงลึกท่านหนึ่ง

mail ให้ข้อมูลผมเกี่ยวกับระบบของ isinthai.com ว่ามีจุดบกพร่องอะไร และต้องแก้ไขอย่างไร ทำให้ผมต้องแผน upgrade จาก RH7.2 เป็น RH7.3 อีกครั้ง โดยข้อความในจดหมายของนักพัฒนาท่านนี้มีดังนี้

สวัสดี ครับ ผมชื่อ ธนดล รามสงฆ์ หรือ นก นะครับ พอดี ได้อ่าน บทความที่ http://www.isinthai.com ซึ่งชอบมากเลย คงเป็นตัวอย่างที่ดี กับเพื่อนๆ คนอื่น ส่วนที่ชื่อชอบ คือ การแนะนำ คำสั่งเบื้องต้น อ่ะครับ และพอดี ได้อ่าน เรื่องราวของ server ตัวนี้ โดน hack ถึง 28 ครั้ง ทำให้ผมสนใจ ว่าเพราะอะไร ทำไมถึงโดนเยอะ ขนาดนั้น

ส่วนที่ผม E-mail มานี้ เพื่อมาแจ้ง ความบกพร่อง ของ openssl ของ www.isinthai.com ของทีมงานคุณครับ ที่ได้ มีจุดอ่อน อยู่ที่ openssl ครับผม ซึ่งจะทำให้ คนที่เจาะเข้ามา สามารถ เป็น user apache ได้ และสามารถจะกลาย มาเป็น root ภายหลังได้ด้วยการ ใช้ local exploit อีกครั้งหนึ่ง ซึ่ง ตามที่ผมได้ทดลองในเวลา 20.25 วันที่ 29 กันยายน 2545 แล้ว ผม ก็ สามารถ มาเป็น user apache ได้ครับ และสามารถใช้คำสั่งต่างๆ ได้ทั่วไป และ ขึ้นมาเป็น root ในภายหลังได้ แต่ผมไม่ได้ทำ backdoor อะไรไว้หรอกครับ เพราะไม่อยากเสียแบบดีๆ เช่นนี้ไป เลย แจ้ง กลับมา เพื่อทราบครับผม ปล. ผมคาดว่า น่าจะมีคนอื่นเข้าได้ก่อนผม ครับ เพราะ เห็นว่ามี process bnc รันอยู่ ที่ /var/tmp ครับ แต่ผมไม่ได้ลบออกครับ เพราะต้องการให้ทางทีมงาน ตรวจสอบ จุดบกพร่อมด้านอื่น ด้วยครับ

สำหรับ การแก้ไข คือ update apache version ที่ใหม่กว่านี้ และ ติดตั้ง openssl ที่ตัวใหม่กว่า 0.96 ครับ ซึ่งจริงๆ ผมอยากแนะนำว่า ให้ติดตั้ง apche แบบแยกต่างหากครับ ไม่ควรติดตั้ง จาก rpm ที่ มากับแผ่น ครับ เพราะจะสามารถ ควบคุมอะไรได้ง่ายกว่านี้ครับผม อีกทั้ง (จากความรู้สึกผมเอง) เพียงแต่ว่า การ config ครั้งแรก อาจจะลำบากนิดนึง ครับผม สำหรับ url ที่เกี่ยวข้อง ได้แนบ มาให้ข้างใต้แล้วครับ

http://www.cert.org/advisories/CA-2002-27.html
http://online.securityfocus.com/bid/5362
http://online.securityfocus.com/bid/5364

ปล สุดท้าย ถ้าให้ดี ควร update openssh ด้วยครับ เพราะตัวนี้ ก็มีจุดบกพร่อง สามารถให้คน มา brute หา key สำหรับ root ได้เช่นกันครับผม และ ถ้าเป็นไปได้ ควรใช้ os ตัวอื่น เช่น mandrake หรือ slackware ดีกว่าครับ เพราะใน config พื้นฐานของ os สองตัวนี้จะจำกัด สิทธิ์ ของ file ไว้เข้มงวด มากครับ ถึงแม้ mandrake จะ ปรับมาจาก redhat ก็ตาม

และสุดท้ายนี้ ขอเอาใจช่วย ทีมงาน เพื่อเปิดให้ ผู้อื่นมาใช้งาน เวบฟรี ของไทยเพื่อเกิดประโยชน์ต่อไปอีกครับ

ธนดล รามสงฆ์
Tanadon Rarmasong
http://www.linux-cdr.com/

28. 25 พฤษภาคม 2545 หลังจากผมลง Redhat 7.2 ในเครื่อง yn3 ให้เป็น web server ในวันศุกร์ที่ 24 Hacker ก็เข้ามาในวันเสาร์หลังจาก หายหน้าไปนานมาก เขา hack ระบบได้จริง ๆ เพราะสามารถเพิ่ม user ใน /etc/passwd และในเครื่องนี้ผมปิดบริการเกือบทั้งหมดแล้ว เหลือที่เปิดอยู่ก็คือ xinetd จึงได้ปิดไป

ผมทราบว่าระบบผมถูก hack เพราะทาง neways.com.my แจ้งให้ทราบว่าเขาถูกโจมตี ผมแค่เปิด xinetd เพียง 3 วันก็มีคนมาใช้เครื่องไป hack คนอื่นได้แล้ว ผมตรวจเครื่องอื่นในระบบ ยังปกติ ไม่มีอาการของการถูก hack แต่ประการใด

> Date: Sat, 25 May 2002 21:37:16 -0800 (GMT+8)
> From: James Loh [jamesloh@neways.com.my]
> To: webmaster@yonok.ac.th
> Subject: Hack attempts
>
> I am the system administrator of 202.187.249.50 and www.neways.com.my You have an IP address 202.29.78.14 (yn3.yonok.ac.th) which is attempting to hack my servers.The log below is in Malaysian time (GMT +0800). Pls investigate.
>
> 202.187.249.50
> Attempt from 202.29.78.14 (yn3.yonok.ac.th) to in.ftpd at Sat May 25 14:30:47 MYT 2002Attempt from 202.29.78.14 (yn3.yonok.ac.th) to in.ftpd at Sat May 25 14:30:48 MYT 2002Attempt from 202.29.78.14 (yn3.yonok.ac.th) to in.ftpd at Sat May 25 14:30:49 MYT 2002Attempt from 202.29.78.14 (yn3.yonok.ac.th) to in.ftpd at Sat May 25 14:30:49 MYT 2002
>
> www.neways.com.my
> May 25 14:12:54 mail xinetd[17589]: refused connect from 202.29.78.14
> May 25 14:12:54 mail xinetd[17589]: refused connect from 202.29.78.14
> May 25 14:12:54 mail xinetd[17589]: FAIL: ftp libwrap from=202.29.78.14

27. 26 มีนาคม 2545 loxinfo แจ้งให้เราทราบว่า server ของเราสร้าง spam

แนะนำให้ทำ relay ตรวจสอบแล้วพบว่าในเว็บมีหน้าเว็บที่ Hacker เข้ามาสร้างจึง save screen ไว้ดู [หน้าเว็บที่ถูกกล่าวใน spam] ส่วนอีกปัญหาไม่แน่ใจว่าเกิดจากอะไร คือ login เข้าไปไม่ได้ จึงไป copy login ที่มีการ backup ไว้มาแทน /bin/login ก็ใช้งานได้ตามปกติ และได้ปิด /etc/hosts.deny เป็น all:all

26. 17 กันยายน 2544 ทีมงานของ isinthai.com ไปอ่านบอร์ดของ http://www.kapook.com/hilight/2207.html

ว่าเว็บของ http://www.malaysiaevents.com ถูก Water overflow เปลี่ยนหน้าเว็บเป็น หน้าใหม่ ซึ่งเดิมเขาเคย hack isinthai.com และอีกหลายเว็บในไทย

การเป็น hacker นั้น ควร hack เข้าไปแล้ว บอกว่าระบบมีจุดผิดพลาดอย่างไร และออกมาโดยไม่ทำความเสียหาย แต่ water overflow ทำเป็นการกระทำเหมือนการก่อการร้าย เพราะเข้าไปแล้วเอา ธงชาติของประเทศไปเกี่ยวข้อง

การ hack ก็คือการแสดงออกว่าตนเองมีความรู้ ผมว่ามีวิธีมากมาย ที่จะแสดงออก ในทางที่สร้างสรรค์ การแสดงออกในความรู้ของตนเองแบบนี้ เป็นความคิดที่ผิด และดูไม่มีค่าอะไร เพราะเมื่อรู้ว่าระบบปฏิบัติการตัวหนึ่งมีจุดด้อย และก็ใช้ความรู้เดิม ๆ นี้ไป hack เครื่องอื่น ที่มีจุดผิดพลาดเหมือนเดิม เป็นการใช้ความรู้เพื่อทำลายอย่างเดียวจริง ๆ เพราะถ้าเป็นผม จะ hack เข้าไปแล้ว mail ไปบอก webmaster ถึงข้อบกพร่อง ที่เว็บนั้นมีอยู่ พร้อมบอกวิธีการแก้ไข .. น่าจะเป็น hacker ที่สร้างสรรค์กว่า ที่ทำอยู่นี้มาก

25. 15 กันยายน 2544 Mr RobiUz Miora [robiuz@yahoo.com] mail มาแจ้งให้ผมทราบว่า การออกจาก Restrict shell ไปเป็น shell ธรรมดาทำอย่างไร

ทำให้ผมสามารถปิดการออกไปยัง shell ปกติได้อีกครั้ง เดิมเขาจะเข้าไปที่ ncftp แล้วก็พิมพ์ว่า !/bin/sh เพียงเท่านี้ก็ออก shell ได้แล้ว ถ้าต้องการเปลี่ยน shell ของตนถาวรก็พิมพ์ว่า chsh เท่านั้นเอง .. ขณะนี้ผมปิด ncftp แล้วเพราะลองไปเปลี่ยน 700 ให้ bash ก็ไม่ได้ จะทำให้เข้า Restrict shell ไม่ได้

24. 13 กันยายน 2544 ผมได้รับจดหมายจากหนังสือพิมพ์ฉบับหนึ่ง(มต.) สงสัยว่า บุคลากรใน isinthai.com เป็น hacker

โดยแจ้งว่าเว็บของเขาถูก Hack และฝากชื่อ Water overflow ไว้ เมื่อเข้ามาเปิดเว็บของ isinthai.com แล้วเห็นชื่อนี้อยู่ จึงเข้าใจว่าเป็นเจ้าหน้าที่คนหนึ่ง ที่ทำเว็บ isinthai.com ซึ่งจริง ๆ แล้วผมเองก็ไม่ทราบว่า Hacker ผู้นี้คือใคร แต่ถ้าได้อ่านในหัวข้อ 9.51 หัวข้อย่อยที่ 7 ก็จะทราบว่า Water overflow คือใคร

Water overflow คือ Hacker ที่เข้ามาเจาะระบบ Server ของพวกเรา ที่เคยใช้ Sun SparcV และ Linux6.2 ทุกตัวของเรา เมื่อช่วงมีนาคม 2544 ซึ่งเป็นช่วงปิดภาคเรียน และพอมีเวลาศึกษา Linux อย่างจริงจัง หลังจากศึกษา และปรับปรุงระบบอยู่พักหนึ่ง ก็ไม่แน่ใจว่า ผม upgrade ระบบดีขึ้น หรือเขาเบื่อที่จะ hack แล้ว จึงหันไปเจาะที่อื่นบ้าง ผมทราบจากผู้ถูก hack อีกท่านหนึ่ง ซึ่งดูแลเครื่อง NT อยู่ในคณะ ของสถาบันแห่งหนึ่งในพิษณุโลก จึงรู้ว่า hacker ผู้นี้ hack ได้ทั้ง SunOS, Linux และ NT

น่าตกใจที่ Server ทุกตัวในปัจจุบัน ที่ไม่ได้จ้าง Sysadministrator มานั่งเฝ้าเครื่องเพียงอย่างเดียวตลอดเวลา และมี OS ที่ไม่ upgrade จะมีช่องให้ hacker เจาะได้ ผมอ่านจาก securityfocus.com ว่าเกือบทุกเดือน จะมีคนพบจุดบกพร่องของระบบปฏิบัติการ ซึ่งเป็นช่องทางที่ hacker เข้าไปได้ ขนาด NT เองก็ยังมีจุดบกพร่อง เพราะสิงหาคม 2544 ก็พึ่งพบว่า code red สามารถเข้าไปในจุดบกพร่องของ NT ได้ .. จึงมั่นใจไม่ได้เลยว่า ระบบที่แข็งแกร่งที่สุดในปัจจุบัน จะแข็งแกร่งตลอดไป

23. 20 กรกฎาคม 2544 ผมได้รับ mail จาก Pattara Kiatisevi [ott@thailinux.gits.net.th] เข้าใจว่าเป็นผู้ดูแล linux.thai.net

เขาเข้าใจว่าผมพยายาม hack เข้าไปที่ server ของเขา ผมเองเป็น root แต่ไม่ได้ทำ เข้าใจว่ามี hacker เข้ามาในระบบของผมได้สำเร็จ แล้วก็ telnet เข้าไปในระบบของเขา โดยใช้ account pawee เข้าไปใน linux.thai.net .. ท่านสามารถ hack เข้ามาเป็น root ได้ กรุณาบอกผมด้วยว่าจะปิดได้อย่างไร ขอเป็นวิทยาทานนะครับ

Date: Thu, 19 Jul 2001 17:55:44 +0700 (ICT)
From: Pattara Kiatisevi [ott@thailinux.gits.net.th]
To: webmaster@www.isinthai.com
Subject: Don't try to hack again.

To Administrator
About 15 July later, I found intruder attempt to connect my server (linux.thai.net) from your host but I don't care about it because intruder can't login.
In 18 july, my important files is diappeared and there are many file named ".root" leave back. When I run it as root, it's display protected method. thank you about .root .

Please don't hack me again.
if you try to hack again, I 'll ban all of your domain 202.29.78.*
Pattara Kiatisevi
Thai linux working group
mailto : ott@linux.thai.net

cat /var/log/secure

Jul 15 00:32:14 linux in.ftpd[16466]: refused connect from root@202.29.78.1
Jul 15 00:32:15 linux in.ftpd[16466]: refused connect from root@202.29.78.1
Jul 15 00:32:15 linux in.ftpd[16466]: refused connect from root@202.29.78.1
Jul 15 00:32:16 linux in.ftpd[16466]: refused connect from root@202.29.78.1

last

pawee pts/0 www.isinthai.com Wed Jul 18 23:45 - 23:49 (00:04)
pawee pts/0 www.isinthai.com Wed Jul 18 23:45 - 23:59 (00:13)
ott pts/0 gw-41.wh.uni-stu Wed Jul 18 20:49 - 23:51 (04:02)
ott pts/0 gw-41.wh.uni-stu Wed Jul 18 19:37 - 19:53 (00:16)

22. 26 กรกฎาคม 2544 : นักศึกษาของผมคนหนึ่ง มาบอกว่ามีคนส่งโปรแกรมมาให้เขาลองเอาโปรแกรมนั้นเปลี่ยนรหัสผ่าน ในระบบ RH6.2 ก็สามารถทำได้ แต่เขาไม่ใช่คนที่สามารถเปลี่ยน Shell ของ demo เพราะผมเชื่อว่าการเปลี่ยน Shell ของ demo จะต้องใช้ความสามารถของ Root ซึ่ง Hacker แสดงผมให้ผมเห็นว่าเขาเปลี่ยนได้แล้วจริง ๆ จึงทำให้ผมต้องหันไปหา Redhat Linux 7.2 เพราะน่าจะเป็นระบบที่ปลอดภัยกว่าเดิม

21. วันที่ 19 กรกฎาคม 2544 : Hacker เข้ามาอีกแล้วครับ
แต่ผมไม่แน่ใจว่าเข้าเจาะมาเป็น Root ได้ไหม เพราะอาการที่เกิดในครั้งนี้คือการเปลี่ยน Title ของเว็บ ซึ่งใช้ user demo เข้าไปเปลี่ยนในจุดที่เหมาะสมก็ทำได้ และอีกอาการหนึ่งคือการเปลี่ยนรหัสผ่านของ demo ซึ่งผมได้ทำการปิดบริการ passwd แล้ว แต่เขาก็ยังเปลี่ยนรหัสผ่านได้อีก .. จึงตัดสินใจเปิด perl และ php เพราะต้องการทดสอบบริการ mail และต้องการทดสอบดูว่าหลัง patch ใหม่แล้ว hacker จะสามารถ hacker เข้ามาเป็น root ได้หรือไม่ เพราะผลการ hack ในครั้งนี้อาจไม่จำเป็นต้องเป็น root ก็ทำได้

20. 12 กรกฎาคม 2544 : มีข้อความขึ้นที่ host ตัวหนึ่ง ทั้งที่ได้ upgrade Redhat 7.2 จนหมดแล้ว อาจเป็นเพราะเปิดบริการมากไป จึงตัดสินใจปิด named และ hosts.deny เป็น all:all เปิดเฉพาะ ftp เท่านั้น ส่วน host อีกตัวหนึ่งที่ไม่ได้เป็น web service ผมก็ได้ปิด httpd ไปด้วย ntsysv ข้อความที่ผมเห็นที่หน้าจอ console แต่ไม่ทราบว่าถูก hack หรือไม่ ทั้ง ๆ ที่ใช้ chkrootkit.com เช็คแล้วก็ไม่พบ worm, sniff หรือ vulnerable เลย สำหรับ message ที่พบ คือ

eth0 : Transmit timeout, status 0d 2000 media 08
eth0 : Tx queue start entry 10831 dirty entry 10827

19. 8 กรกฎาคม 2544 : วันนี้ผมไม่แน่ใจว่า hacker hack ระบบได้หรือไม่
เพราะผมได้ปิดบริการ perl และ php พร้อมการปิด shell ทำให้โปรแกรม .sniff ที่เขาส่งเข้ามาอาจไม่สามารถประมวลผลขึ้นได้ เพราะหาอาการของการถูก hack สำเร็จไม่พบ และที่เครื่องดับไปอาจไม่ใช่ฝีมือของ hacker เพราะเครื่องที่ใช้เป็นแบบไฟกระชากแล้วหลับไป ต้องปลุกด้วยมือครับ

18. 3 กรกฎาคม 2544 : Server ถูก hack ได้มาหลายวันแล้ว
เขาเปลี่ยน named และ aliases แบบไม่ให้ผมรู้ เพราะเปลี่ยนแล้ว restart จากนั้นก็เปลี่ยนกลับเหมือนเดิม ผมไปตรวจสอบก็ไม่พบอะไรผิดปกติ ต้อง restart อีกทีหนึ่งจึงปกติ และเป็นช่วงที่ผมพยายายม upgrade Redhat6.2 ก็ทำเอาเหนื่อย เพราะ upgrade แล้วเครื่องใช้งานไม่ได้ หาวิธีอยู่หลายวัน จนวันนี้ตัดสอนใจปิดบริการต่าง ๆ ดูว่า เขาจะเข้าได้ไหม เช่น perl และ php เพราะอย่าง se-ed.net ยังไม่ได้ให้บริการแบบเต็มที่ ผมทดสอบด้วยคำสั่งเรียก unix command หลายที่ปิดครับ แสดงว่ามีการ config ให้ปลอดภัยผมยังไม่ทราบ config สำหรับปิดบริการบางอย่างใน perl จึงปิดไปก่อนเลย

17. 28 มิถุนายน 2544 : พักนี้ Server จะล่มบ่อย เพราะมีอาการเหมือนถูกยิงด้วยคำว่า eth0: Something Wicked happened! 2008. ซึ่งแต่ก่อนจะขึ้นเพียง 3 ถึง 5 บรรทัด แต่พักนี้ มาติดต่อกันจนติดต่อ server ไม่ได้ บางทีข้อความหยุดแล้วถึงติดต่อได้ก็มี และบ่อยครั้งที่มาประปรายคือ 2 ถึง 5 บรรทัด แล้วก็ไม่มีปัญหาอะไร เข้าไป /var/log/messages จะพบ

บรรทัดนี้สงสัยถูก hack เพราะใช้ kernel เก่า
Jun 27 09:11:30 star kernel: eth0: Oversized Ethernet frame spanned multiple buffers, entry 0x1e$
Jun 27 09:11:30 star kernel: eth0: Oversized Ethernet frame c1ee4ce0 vs c1ee4ce0.

Jun 27 09:11:30 star kernel: eth0: Oversized Ethernet frame spanned multiple buffers, entry 0x1e$
Jun 27 09:11:30 star kernel: eth0: Oversized Ethernet frame c1ee4cf0 vs c1ee4cf0.
Jun 27 09:11:30 star kernel: eth0: Oversized Ethernet frame spanned multiple buffers, entry 0x1e$

ที่จอ console จะขึ้น eth0: Something Wicked happened! 2008. เต็มจอเลยครับ
Jun 27 13:23:20 star last message repeated 2 times
Jun 27 13:23:23 star PAM_pwdb[3875]: (login) session closed for user oir
Jun 27 13:23:23 star inetd[365]: pid 3874: exit status 1
Jun 27 13:23:45 star kernel: eth0: Something Wicked happened! 2008.
Jun 27 13:23:52 star last message repeated 2 times
Jun 27 13:23:52 star PAM_pwdb[3882]: (login) session opened for user cooper by (uid=0)

16. 25 มิถุนายน 2544 : Hacker เข้ามาอีกแล้วครับ
เข้า server หลาย ๆ ตัวของเรา โดยเฉพาะ DNS เห็นว่าเข้ามาลบ log ทั้งหมด และที่แน่ ๆ ผมพึ่งทราบว่าทำไมจึงขึ้นคำว่า **eth0: Promiscuous mode enabled** เพราะเขาใช้คำสั่ง #ifconfig eth0 -promisc ซึ่งเป็นการเปิดบริการ port ทั้งหมด ผมลองใช้คำสั่งนี้ในฐานะ user ธรรมดาก็ไม่ได้ (permission deny) และที่แปลกใจคือ ผมปิด shell ของทุกคน เหลือไว้แต่ restriced shell แล้ว เขาจะใช้คำสั่งนี้ได้อย่างไร นอกจากรู้รหัสผ่านของ su และเข้ามาทาง ssh ซึ่งก็ไม่น่าเป็นไปได้อีก

15. 22 มิถุนายน 2544 : วันอาทิตย์ที่ 17 ผมทราบว่าเกิดเหตุผิดปกติ
เพราะใช้จากที่บ้านแล้วเข้า server ไม่ได้ และอ.ถนอมก็อยู่ที่โยนก ช่วยผมเรื่องย้าย server แต่ก็ไม่สำเร็จ พอเช้าวันจันทร์ จึงทราบแน่ว่า เครือข่าย leased line มีปัญหา พอดูดี ๆ อยู่พักหนึ่ง จึงรู้ว่าไฟเลี้ยงระบบเครือข่ายตก พอเปลี่ยนปลั๊ก ก็ติดต่อทั่วโลกได้เหมือนเดิม แต่ตัว DNS ยังล่ม เพราะเข้าไปดูแล้วเป็นฝีมือของ hacker แน่นอน เขาเข้ามาปิดระบบ DNS ของเครื่องราคาแพง ซึ่งเป็นหนามยอกอกผมมานาน การปิดระบบเขาเปิด telnet ทำให้ขึ้น error ว่า /bin/xlogin ซึ่งผมไม่มีเวลามาแก้ เดิมเครื่องนี้ถูก hacker เข้ามาป่วนหลายครั้ง แต่ผมไม่เคยทำอะไรได้ เพราะไม่มี software ในการติดตั้งใหม่ **และถือเป็นรอยรั่วที่ใหญ่ที่สุด ที่ผมไม่สามารถอุดได้มานาน** (เหมือนขโมยปีนเข้ามาทางหน้าต่าง แต่เขาไม่ทำลายหน้าต่าง ผมก็ปล่อยไปก่อน แต่ครั้งนี้เขาทำลาย ผมจึงถือโอกาสโบกปูนทับซะเลย .. เปรียบเทียบน่ะครับ) จากความเสียหายครั้งนี้ ถือโอกาสเปลี่ยนเป็น Redhat 7.2 ทั้งระบบ เพราะก่อนเขาจะทำลาย DNS เขาเข้ามา เจาะ isinthai.com ประจำ แต่ไม่แน่ใจว่าทำไมเขาเบนเข็มมา DNS ที่เขาก็รู้ว่าผมรู้ว่าเขาเข้ามาได้ ในเช้าวันจันทร์ ขณะที่กำลังติดตั้งระบบใหม่ Hacker ก็ช่างขยันเหลือเกิน เขามาต่อหน้าผมนั่นหละด้วย account bin ที่เขาแอบสร้างไว้ เพราะผมนำ server ตัวหนึ่งมาปรับ config ใหม่ ทำให้ผมมีประสบการณ์มากขึ้นมาการ setup server และนำมาปรับหน้าเว็บนี้ ให้ได้อ่านทั่วกัน

14. 11 มิถุนายน 2544 : เสาร์บ่ายที่ 9 hacker เข้ามาแล้ว
แต่เป็นวันที่ไม่มีผู้ช่วยจึงต้องปล่อยให้ถึงวันจันทร์ และเครือข่ายทั้งหมดก็หายไป เพราะอุปกรณ์ leased line ขององค์การโทรศัพท์เสีย เช้าวันจันทร์ พบว่าผมไม่สามารถใช้ ftp เข้าเครื่องได้ แม้จะปิด lock แล้ว และที่สำคัญไม่สามารถแก้ไขอะไรแฟ้ม index.html ไม่ว่าจะ chown chmod pico หรือ rm ทั้งที่ใช้ su แล้ว จึงได้ทำการแก้ไขระบบใหม่ตามหัวข้อ 9.52 อีกครั้ง เช่น upgrade เพิ่ม และปิด /tmp เพราะที่ f2s.com เขาก็ปิด

13. 8 มิถุนายน 2544 : เมื่อวานผมมั่นใจมากว่าเครื่องจะไม่ถูก hack
เพราะปิดอะไรไว้มากมาย แต่ hacker ก็ทำได้โดยเข้ามาลบ /etc/passwd* /etc/shadow* /etc/hosts.* ทำให้ผมไม่สามารถเข้าระบบตามปกติได้ ต้องเข้าแบบ linux single แต่ผมก็ไม่ทำ เพราะคิดว่า เริ่มจาก 0 ใหม่ ดีกว่าเริ่มจาก 10 แล้วไม่แน่ใจว่ามีอะไรรั่วบ้าง วันนี้ผมจึงทำหลาย ๆ อย่างให้ดีขึ้น ซึ่งเขียนรายละเอียดไว้ในหัวข้อ 9.52
ข้อความที่เห็นที่หน้าจอของ console
Transmit timeout, status 0D 0000 media 08
eth0: tx queue start entry 44052 ..
พบ ip 195.223.23.99 ซึ่งน่าจะเป็น fake ip ที่ส่งเข้ามาจาก italy

12. 7 มิถุนายน 2544 : ล้างเครื่องใหม่ได้ 2 วัน โดยปิดหมดด้วย tcpwrapper
แต่ทำให้ใช้ pop ไม่ได้จึงต้องปิดเฉพาะ in.telnetd แต่ปัญหาพบว่า มี hacker เข้ามาส่งแฟ้มเข้าไปใน root ของ web directory ได้ และบางครั้งมีข้อความ ขึ้นที่ console ว่า
June 6 17:33:42 www Kernel: eth0: Something Wicked happened! 2008.

อ่านแล้วก็ไม่เข้าใจจึงตัดสินใจ upgrade package เพิ่ม และทำการปิด ftp โดยลบทุกโปรแกรมออกจากห้อง /home/ftp/bin และ /home/ftp/lib ซึ่งก็ไม่พบปัญหาการให้บริการ ftp แต่อย่างใด และ ip ที่เข้ามาในระบบ ซึ่งเป็นข้อความที่อ่านไม่ออก น่าจะเกิดจากการทำ overflow โดย 202.44.9.117 และคาดว่าครั้งนี้จะปิดได้ดีขึ้น เพราะได้ upgrade โปรแกรมแก้ปัญหาช่องโหว่หลาย ๆ จุดแล้ว

11. 29 พฤษภาคม 2544 : ได้รับ mail จาก water_overflow แจ้งให้ผมทราบว่าเขา hack โดยการปลอม IP เข้ามา

และส่งโปรแกรมภาษา C เข้ามาไว้ที่ห้อง /tmp เขา compile เครื่องผมไม่ได้เพราะปิด gcc ไว้ เมื่อ run program จะได้สถานะเป็น root ส่วนอีกโปรแกรมที่คิดว่าเขาไม่ได้บอกผมคือโปรแกรมชื่อ last.cgi ซึ่งอยู่ในห้อง /cgi-bin เป็นโปรแกรมที่เปิดผ่านเว็บ ไม่ได้ใช้วิธีเปิดด้วย telnet ที่ต้องตกใช้เพราะโปรแกรม last.cgi สามารถใช้คำสั่งของ shell ผ่าน browser ได้เลย และสามารถลบแฟ้มที่มีสถานะเป็น 700 ของ root ได้ ก็หมายความว่ากระทำการใด ๆ ได้หมด แต่ตอนนี้ผมยังหาวิธีแก้ปัญหากับแฟ้มนี้ไม่ได้ ที่จะทำให้โปรแกรมนี้หมดความสามารถของ root ผ่าน browser ไป ยกเว้นว่าจะปิดบริการ cgi ซึ่งไม่ต้องการทำอย่างนั้น (แม้จะทำตามขั้นตอนในข้อ 9.52 หรือปิด mount แต่โปรแกรมนี้ก็ยังมีฤทธิ์)

10. 28 พฤษภาคม 2544 : เมื่อวาน hacker เข้ามาจัดการ hack server ตัวนี้ได้

โดยเปลี่ยนหน้าแรก ซึ่งเขาได้แนะนำว่าควรหา patch มา update และได้ฝากหน้าเว็บไว้ให้อ่าน หลังจากงถูก hack แล้ว ได้เข้าไปตรวจด้วย last ไม่พบอะไร ดูใน /etc/log/secure ก็พบแต่ที่เข้ามาไม่ได้ แต่พอเข้าไปที่ /etc/log/message พบสิ่งที่ hacker ฝากสิ่งดี ๆ ไว้ เรียกว่า ถ้าผมไม่ใช้ more /etc/log/messages ก็ไม่เห็น ซึ่งมีข้อความดังนี้

May 27 10.05.11 login Water Overflow
To : Admin
Subject : upgrade your glibc now. your glibc have bug..

HOW TO HACK :
The hacker can make buffer overflow in glibc/locale. if you don't believe, go to /tmp
and see my own program named Xwater. When you run Xwater program.. after overflow you 'll get root
shell.

HOW TO PROTECT :
If you don't use /bin/mount ..please change permission to can't execute for protect hacker
using this hole in glibc(chmod 4700 /bin/mount). but if you upgrade glibc,you can change permission to
execute again.

nice a day.

Water Overflow

ในส่วนที่ hacker แนะนำให้ patch ซึ่งน่าจะหา download ได้จาก http://www.redhat.com/support/errata/index.html นั้น ผมพบนับได้เกือบ 100 โปรแกรม และในนั้นมีเรื่อง glibc ที่ ได้รับการแนะนำที่ http://www.redhat.com/support/errata/RHSA-2001-002.html ส่วนวิธี hack ที่ได้รับการแนะนำ ผมได้ลอง run โปรแกรมนี้ในห้อง /tmp ด้วย user ธรรมดา ปรากฏว่า overflow จนเป็น root จริงครับ เขาแนะนำว่าถ้าไม่ใช้ mount ก็ให้ใช้ chmod 4700 /bin/mount หรือไม่ก็ upgrade ซึ่งผมเลือกทั้ง 2 วิธีที่เขาแนะนำมาคือ

1. upgrade glibc จาก http://www.redhat.com/support/errata/RHSA-2001-002.html จะได้แฟ้มมาหลายแล้วแล้วใช้ rpm -Fvh [filename]
2. chmod 4700 /bin/mount

9. 25 พฤษภาคม 2544 : เย็นนี้ได้รับ mail จาก กลุ่มน้ำล้น ว่าจะเข้ามา hack วันพรุ่งนี้ ให้ป้องกันระบบให้ดี เป็นลักษณะจดหมายเตือน แต่ผมก็ป้องกันไปแล้วเต็มที่ คือการใช้ tcpwrapper ปิด ip ทั้งหมด แต่ไม่ได้เข้าไปปิด service ใน /etc/services พอเย็นวันเสาร์ผมเข้าใช้ isinthai.com ไม่ได้ ก็คิดว่า hacker เข้าไปแล้วเป็นแน่ จึงเข้าไปดูที่เครื่อง ปรากฏว่ามีคนปิดไฟ พอเปิดไฟก็ใช้ได้ จึงแน่ใจว่าที่ระบบหายไปในวันเสาร์ ไม่ใช่ฝีมือของ hacker เป็นแน่ จึงไปถาม รปภ. และทราบว่า ผมได้ย้าย server ทำให้หน้าจอตรงกับหน้าประตู เมื่อ รปภ. เดินไปเห็นว่าไฟเครื่องเปิด จึงใช้กุญแจไขเข้าไป ช่วยปิดให้ .. สรุปว่าผมได้ clear กับ รปภ. แล้วว่า ต่อไปห้ามยุ่งกับเครื่องเหล่านั้นอีก .. ก็เรียบร้อย

Please prevent www.isinthai.com now.. coz there're many hackers would like to drill your system..

On 26 May at 10.00 am. if we can invade your system. we'll deface your web.. Don't worry. we don't destroy your system.... and if we found the hole .. we 'll reveal to you and how to protect.

I have a few time for drill your web ,because I can entrance and begin to study engineering in university recently. So maybe I have no time for drilling any more.

water overflow.

8. 24 พฤษภาคม 2544 : พบว่าใช้ useradd นึกว่าโดย hack อีกแล้ว
แต่คิดว่าไม่ใช่ เพียงแต่เกิดแฟ้ม group.lock ในห้อง /etc จึงทำให้ใช้คำสั่ง useradd ไม่ได้ เมื่อลบ group.lock ก็ใช้ได้ตามปกติ จึงถือโอกาสเข้าไปดูแล้ว /var/log/messages ซึ่งมีข้อมูลเยอะมาก จึงเลือกดูที่มีคำว่า portmap พบว่ามี log ที่แสดง ip ขึ้นมา โดยใช้คำสั่ง **cat /var/log/message|grep portmap** อ่านดูก็ไม่ได้คิดว่าต้องเป็น hacker อาจเป็นเพียงผู้ใช้ที่เคยได้บริการ telnet และเข้ามาใช้บริการอีกเท่านั้น
May 20 11:58:27 www portmap[13213]: connect from 211.223.208.103 to dump(): request from unauthorized host
May 20 17:33:42 www portmap[13318]: connect from 203.155.103.249 to dump(): request from unauthorized host
May 22 14:38:05 www portmap[816]: connect from 211.182.75.2 to getport(status): request from unauthorized host
May 22 16:28:57 www portmap[852]: connect from 211.182.75.2 to getport(status): request from unauthorized host
May 22 18:03:12 www portmap[885]: connect from 211.182.75.2 to getport(status): request from unauthorized host

7. 18 พฤษภาคม 2544 : วันนี้ hacker กลุ่มน้ำล้น ได้เข้ามาสำแดงความสามารถว่าเขาทำได้ด้วยการเปลี่ยนหน้าแรกของเว็บ และยังตั้งระเบิดเวลา เมื่อปิดเครื่องแล้วจะไม่สามารถ boot ระบบ ทำให้ Server 2 ตัวที่เป็น Redhat 7.2 ที่ผมมั่นใจว่าไม่น่ามีใครทำอะไรได้
เนื่องจาก server ตัวหนึ่ง แม้แต่ผมยังไม่สามารถเข้าเป็น Superuser และบริการหลายอย่างล่มไป จึงเข้าใจว่า hacker ไม่น่าทำอะไรได้อีก ส่วน Server อีกตัวหนึ่งได้ติดตั้งใหม่ ปิด gcc และ tcpwrapper แล้ว แต่ก็ยังถูก hack ได้ชั่วข้ามคืน และเขายังบอกว่าเป็น Hacker กลุ่มน้ำล้น และเป็นคนไทย ที่ผมเคยเข้าใจว่าเป็นฝรั่ง แต่นี่ก็คือประสบการณ์ที่ทำให้รู้ว่าระบบของผมยังมีรอยรั่ว แต่ Hacker กลุ่มน้ำล้น (Water overflow) ได้แนะนำว่าผมน่าจะหา Patch มาปิดรอยรั่วต่าง ๆ ทำให้ผมเริ่มหันไปสนใจเรื่องนี้มากขึ้น หลังจากที่เคยเข้าไปเห็น Patch กว่า 300 Patch ที่ Redhat ออกมาแก้ปัญหาระบบใน Redhat 7.2 สำหรับวันที่ hacker เจาะเข้ามาได้ ผมยังไม่ทันได้เห็นหน้าแรก เพราะก่อนผมเข้าที่ทำงาน ไฟฟ้าเกิดดับไปซะก่อน

6. 15 พฤษภาคม 2544 : isinthai.com เองถูก hack จนผมไม่สามารถเข้าเป็น superuser ได้ ต้องไปเข้าที่ตัว Server จึงจะได้เพราะใช้ su ไม่ได้นั่นเอง แต่วันนี้ Server ตัวหลักตัวหนึ่งถูก hack ซึ่งมีอาการที่ยอมรับไม่ได้คือ ใช้ pico ไม่ได้ Telnet ออกไป server ตัวอื่นไม่ได้ โดย Server ตัวนั้นมีการปิด Telnet ด้วย hosts.deny แล้ว ผมตรวจด้วย Last จึงทราบว่า เขา Hack เข้ามาด้วย Ftpd ซึ่งเข้าใจว่าเป็นการทำ Overflow ซึ่งผมยังไม่ทราบว่าทำอย่างไร ในแฟ้ม passwd เขาก็เพิ่ม user 0:0 เข้าไปได้ จึงจะลงระบบในเครื่องนี้ใหม่ทั้งหมด แต่จะปิดระบบให้หมด เหลือให้ใช้ได้เฉพาะในโยนกเท่านั้น ก็ต้องดูต่อไปว่าผมการปิดของผม ครั้งใหม่ จะสำเร็จหรือไม่ และที่แค้นใจคือ ผมพยายามใช้ Ghost copy HD ตัวนี้เพื่อ backup แต่ประเสริฐ พยายามา 2 วันก็ไม่สำเร็จไม่ในใจว่า Harddisk ตัวใดเสีย จึงทำให้ต้องมานั่งลงระบบใหม่ทั้งหมด นี่ถ้า Backup ไว้คงไม่ต้องลงระบบใหม่อย่างนี้ แต่ก็ถือเป็นประสบการณ์ เหล็กกำลังร้อนตีง่าย ซึ่ง Server ดังกล่างก็มีปัญหาหนึ่งที่ยังแก้ไม่ได้ คือเมื่อไฟตกแล้วจะดับไป ไม่ฟื้นขึ้นมาเอง แต่ถ้าเป็นเครื่อง Acer 133 จะฟื้นเองได้ จึงตัดสินใจเปลี่ยนเครื่องด้วยเลย

5. 3 พฤษภาคม 2544 : วันนี้ผมเข้า Root โดยใช้ Su ไม่ได้
เมื่อเข้าแล้วกรอกรหัสผ่านแล้วจะขึ้นคำว่า **su: cannot set groups: Operation not permitted** พอไปตรวจใน **/etc/passwd** ก็พบว่า hacker เข้ามาเปลี่ยน adm ให้เป็น :3:0: จึงเปลี่ยนกลับไป จากนั้นก็เขาเป็น root โดยใช้ **linux single** แล้วไปสร้าง account ขึ้นมาอีก 1 account ให้เป็นประตูหลัง จึงจะเข้าไปเป็น root ได้ ขณะนี้คงปิดระบบให้ปลอดภัยไม่ได้แล้ว เพราะเป็นระบบเปิด ผมวางแผนว่าอีกสักพักจะ ลงระบบใหม่ แล้วเริ่มปิด gcc ตั้งแต่ต้น hacker อาจเข้ามาไม่ได้ก็ได้ .. ขณะนี้จะเป็น root ที **ต้องไปนั่งหน้า server** จึงจะใช้ได้

4. 26 เมษายน 2544 : ผมได้รับแจ้งจากคุณสุวิทย์ว่า last หาไปและมีข้อความว่า operator เป็นผู้ลบ

แต่ผมจำได้ว่าเคยเปลี่ยนรหัสผ่านของ operator ไปแล้ว แต่ก็หาไม่พบว่า operator เข้ามาทำอะไรอีกนอกจากลบ last ไป ซึ่งผู้ที่เคยใช้ user นี้เข้ามาก็คือ hacker คนแรกที่มาจาก romania นั่นเอง

3. 20 เมษายน 2544 : วันนี้ hacker จาก UK เข้ามา

แต่ผมหาไม่พบว่าเข้าเขามาทำอะไร นอกจากเพิ่ม user เข้าระบบ และยังพบคุณ nat (tanma2k@hotmail.com http://www.nat.f2s.com/phpnuke/index.php) ซึ่งแนะนำผมให้ **chmod 700 /usr/bin/gcc** เป็นการป้องกัน hacker นำ shell script มาแปลงตนเองเป็น root ทำให้ผมรู้ว่าแค่มีโปรแกรม shell ตัวหนึ่ง มา run ใน server ถ้า server ยอมให้ใช้ gcc ซึ่งเป็น C compiler ก็จะทำให้เกิด overflow จนเปลี่ยนสถานภาพปกติ กลายเป็น root ทันที และคุณ nat ยังแนะนำเว็บ www.rootshell.com และ www.technotronic.com เพื่อให้ผมมีความรู้ไว้ ปรับปรุงระบบ ซึ่งคุณ oak จาก loxinfo.co.th ก็เคยเล่าให้ผมฟังถึงวิธีการนี้ เพียงแต่ตอนนี้ ผมยังไม่ได้ shell script ตัวนั้นมาทดลอง และก่อนนี้ไม่กี่วัน AusCERT Probe Reporter [auscert@auscert.org.au] และ Phil Crooker [pcrooker@orix.com.au] ก็แจ้งมาว่า มี hacker พยายามเจาะระบบเขาจาก ip ของเรา

```
Apr  8 10:53:16  denied tcp 202.29.78.1(3744) -> 203.23.109.14(53), 1
packet
Apr  8 10:53:17  denied tcp 202.29.78.1(3793) -> 203.23.109.63(53), 1
packet
Apr  8 10:53:18  denied tcp 202.29.78.1(3806) -> 203.23.109.76(53), 1
packet
```

จริง ๆ ไม่ใช่ 202.29.78.1 นะครับ แต่จาก server อีกตัวที่ปิดมิดชิด เพราะถ้าเป็น เบอร์ 1 คือ isinthai.com จะไม่แปลกใจเพราะเปิดให้เข้ามาใช้แต่นี่เป็น server อีกตัวครับ แล้วเข้าก็แนะนำว่าเข้าเว็บต่อไปนี้ เพื่อศึกษาวิธีการปิดระบบ

5. http://www.linuxnewbie.org/nhf/intel/security/armorlin.html
6. http://securityfocus.com
7. http://bastille-linux.sourceforge.net/
8. http://www.auscert.org.au/Information/Auscert_info/papers.html
9. http://packetstorm.securify.com

2. 29 มีนาคม 2544 : เมื่อแก้รหัสผ่านจาก hacker ในครั้งแรกได้

เข้าใจว่า hacker คนเดิม รู้ว่าผมรู้จักเขาได้อย่างไร เพราะผมใช้ hosts.deny ปิดเขา ตามหัวข้อ 9.54 ครั้งนี้ จึงเข้ามาก่อกวน รุนแรงกว่าเดิม เพราะครั้งแรกแค่ยึด super user ไป ครั้งนี้จึงปิดระบบ network ของเรา โดยเข้าไปแก้ไขแฟ้มต่าง ๆ เช่น resolv.conf hosts named.conf network static-routes ifcfg-eth0 เป็นต้น ซึ่ง hacker คนนี้ได้ทิ้งข้อความไว้หลายจุดว่า **SnaK3.Is.The.Best.H4k3r.org** 212.62.7.9 และเว็บที่เขาทิ้งไว้คือ www.snak3.co.uk เป็นเว็บ free email โดย another.com ซึ่งอาจไม่เกี่ยวข้อง โดยตรงกับ hacker ผู้นี้ก็ได้ ในครั้งนี้ ก็เกือบต้อง format หรือ reinstall เพื่อลง linux ใหม่ ดังนั้นก่อนเปิดระบบ จึงต้องใช้ **NortonGhost** เพื่อ clone HD ในระดับ partition ให้ได้ก่อน เพราะมีลูกศิษย์ที่ชื่อ วิรุฬห์ ยวงเอี่ยมใย แนะนำมา

1. 26 มีนาคม 2544 : เปิดระบบทดลอง install โปรแกรมต่าง ๆ ตั้งแต่ต้นเดือน

วันนี้ถูก hacker เข้ามาเปลี่ยนรหัสของ root นั่งหาวิธีอยู่ 3 วันจึงรู้วิธีแก้ไขรหัสผ่าน ตามหัวข้อ 9.61 ซึ่งเลข ip **193.231.178.98** ที่เข้ามาโดยใช้คำสั่ง last พบว่ามาจาก Romania

---

ปรับระบบให้แข็งแรง : ได้รับคำแนะนำดี ๆ จากผู้รู้ จึงนำมาเขียนไว้ที่นี่

apples@chek.com ซึ่งดูแลระบบของ http://academic.cmri.ac.th แนะนำมาหลายเรื่อง เช่นน่าจะใช้ slackware หรือ Mandrake เพราะระบบแข็งมาก สำหรับการป้องกันในเบื้องต้นมีดังนี้

```
chmod 700 /usr/lib/gcc-lib <-- ไม่ให้ใช้ library สำหรับ compile *ส่วนนี้สำคัญ
มาก*
chmod 700 /usr/bin/cc <-- cc compile
chmod 700 /usr/bin/c++ <-- c++ compile
chmod 700 /usr/bin/g++ <-- g++ compile
chmod 700 /usr/bin/make <-- ไม่ให้ make
chmod 700 /usr/bin/gmake <-- gmake อีกอัน
chmod 700 /etc/rc.d <-- ไม่ให้ไปยุ่งและสังเกตกะระบบ Network & initial
Process lpd rpc.* <-- ถ้าไม่ใช้ไม่ต้องรันครับ :)
```

- ไปพิมพ์คำว่า exit 0 ที่บรรทัดแรกของแฟ้ม /etc/rc.d/init.d/lpd

ส่วน rpc ผมยังหาวิธีไม่ run เมื่อ boot ไม่ได้ครับ ต้อง kill process โดยดูจาก ps -aux|grep rpc

FTP Server <-- เป็นไปได้เปลี่ยนจาก wu-ftpd เป็น proftpd นะครับ
IMAP <-- ถ้าเป็นไปได้ให้ใช้เฉพาะ Localhost เท่านั้นครับ **ต้องได้สิครับ**
/sbin/ipchains -A input -s 0/0 -i eth0 --proto tcp --destination-port 143 -j REJECT

water_overflow@hackermail.com ซึ่ง hack ระบบของเรา และแนะนำทีมงานมาดังนี้

1. upgrade glibc จาก http://www.redhat.com/support/errata/RHSA-2001-002.html จะได้แฟ้มมาหลายแฟ้ม แล้วใช้ rpm -Fvh [filename]
2. chmod 4700 /bin/mount

webmaster@isinthai.com ส่วนนี้ผมไปอ่านมาจาก thailinux.com

4 มิถุนายน 2544 : ตัดสินใจปิด telnet แต่เปิดบริการทั้งหมด โดย upgrade โปรแกรมจาก redhat.com

คำสั่งที่ใช้ update เช่น $rpm -Fvh glibc-2.1.3-22.i386.rpm

1. ftp://updates.redhat.com/6.2/en/os/i386/glibc-2.1.3-22.i386.rpm
2.
3. ftp://updates.redhat.com/6.2/en/os/i386/inetd-0.16-7.i386.rpm
4.

และอีกมากมาย

ลบทุกโปรแกรมในห้อง /home/ftp/bin และ /home/ftp/lib ซึ่งยังไม่พบปัญหาจากการลบ
และ อ.dav แนะนำให้ผมใช้ ssh ติดต่อกับ server แทนการเข้า console ก็ต้องลองดูครับ
ส่วน tcpwrapper ตามหัวข้อ 9.54 ได้แก้จากการ deny all:all เป็นการปิดเฉพาะ telnet เพราะถ้าปิดหมด
จะไม่สามารถให้บริการ pop ได้ จึงต้องปิดเฉพาะ in.telnetd

8 มิถุนายน 2544 : ล้างระบบแฟ้มน ftp ทั้ง /home/ftp/bin /home/ftp/etc /home/ftp/lib
เรียกโปรแกรม ntsysv เพื่อจัดการกับโปรแกรมที่มีปัญหา
ลบ apmd atd crond gpm kudzu lpd netfs nfslock pcmcia portmap xfs
เหลือ httpd inetd inet linuxconf mysql named network sendmail เท่านั้น
แก้ inetd.conf โดยปิด shell login talk ntalk finger
แก้ chown ของ /home/httpd/html เป็น root:root
แก้ chmod ของ /home/httpd/cgi-bin เป็น 755
แก้ /etc/rc.d/rc.local เพิ่ม /sbin/ipchains -A input -s 0/0 -i eth0 --proto tcp --destination-port 143 -j REJECT

11 มิถุนายน 2544 : ปิด /tmp ด้วย chmod 400 เดิมเป็น 1777
แก้ /etc/inetd.conf ยกเลิก login, shell และ telnet
แก้ linuxconfig, control service activity ยกเลิก sendmail
Upgrade rpm จาก http://www.redhat.com
สำหรับการ ลงโปรแกรม ถ้า upgrade ด้วย rpm -Fvh .. ไม่ได้ ให้ใช้ลงใหม่ด้วย rpm -i ..
ต้องจัดลงโปรแกรม db3... ก่อน มิเช่นนั้นโปรแกรมอื่นจะลงไม่ได้

5. ftp://updates.redhat.com/6.2/en/os/i386/db3-3.1.17-4.6x.i386.rpm
6.

7. ftp://updates.redhat.com/6.2/en/os/i386/dump-0.4b19-5.6x.i386.rpm
8. และอีกมากมาย
9.

12 มิถุนายน 2544 : upgrade โปรแกรมอีกเพียงจาก redhat.com

10. ftp://updates.redhat.com/6.2/en/os/i386/apache-1.3.14-2.6.2.i386.rpm
11.
12. ftp://updates.redhat.com/6.2/en/os/i386/kernel-doc-2.2.19-6.2.1.i386.rpm
13. และอีกมากมาย
14.

แล้วเปิดบริการ SSH พร้อม restricted shell ตามข้อ 9.53

การทำ restricted shell : การจำกัดผู้ใช้ให้ใช้งานในเมนูที่เตรียมไว้

apples@chek.com ซึ่งดูแลระบบของ http://academic.cmri.ac.th แนะนำเรื่องนี้จนผมทำได้ โดยเฉาะ code ของ menu copy มาทั้งแท่งเลยครับ เมื่อนำมาให้บริการพร้อมกับ ssh (Secure Shell) จะเป็นการให้บริการที่สมบูรณ์ และปลอดภัยมาก (ในปัจจุบัน)

วิธีการทำ restricted shell

1. สร้างห้อง /rbin (ผมสร้างเพื่อแยกออกมาจากระบบเดิม .. อาจไม่จำเป็น)
2. ln -s /usr/bin/bash /rbin/rbash (คำสั่งนี้ผมยังไม่เห็นประโยชน์แต่ก็ทำไว้ก่อน)
3. สร้างแฟ้ม menu ด้วย pico ตาม code ด้านล่างนี้เป็น shell script ธรรมดา
4. chmod 755 menu เพื่อให้ shell script ประมวลผลได้
5. แก้แฟ้ม /etc/shells ด้วย pico โดยเพิ่ม /rbin/menu เข้าไปต่อบรรทัดสุดท้าย
6. แก้ shell ทุกคนในแฟ้ม /etc/passwd เป็น /rbin/menu หรือให้ usermod -s /rbin/menu [username]
7. เพียงเท่านี้ user ที่เปิดเข้ามาจะต้องเข้ามาที่เมนู /rbin/menu ใช้บริการที่เตรียมไว้
8. ถ้าไม่ใช้ script สร้าง user จะต้องแก้แฟ้ม /etc/default/useradd ให้เป็น shell /rbin/menu
9. ถ้าใช้ script _crt จะต้องแก้บรรทัด useradd โดยเพิ่ม -s /rbin/menu หรือจะเพิ่มคำสั่ง usermod ไปอีกบรรทัดก็ได้

```
#!/bin/sh
# Powered By apples@chek.com>
# case from http://academic.cmri.ac.th
case $USER in
usernamewasblock ) exit 1;;
esac
while [ 1 ]; do
clear
echo
echo
echo "          SSH service at http://www.isinthai.com"
echo "          Any suggestion send mail to webmaster@isinthai.com "
```

```
echo
echo "          1 ) Pine - Email/News Client"
echo "          2 ) Lynx - Text Base Web Browser"
echo "          3 ) Pico - Text Editor"
echo "          4 ) File Manager - Delete, Modify, Change file attribute"
echo "          5 ) ncftp - FTP Program"
echo "          6 ) Telnet -  Remote Login"
echo "          7 ) Change password"
echo
echo "          q ) Log out"
echo "             ================== "
echo "             Restrict shell suggest by apples@chek.com"
echo "             Strong server at http://academic.cmri.ac.th"
echo
echo -n " Select->"
read OPT
case $OPT in
  q | Q ) echo;echo "Bye"; echo; echo; exit 1;;
  2 ) lynx http://www.isinthai.com;;
  1 ) pine;;
  3 ) pico;;
  4 ) lynx -editor=pico $HOME;;
  5 ) ncftp;;
  6 ) telnet;;
  7 ) passwd;;
esac
done
exit 1
```

ติดตั้ง TCPWrapper เพื่อตรวจสอบ IP เครื่องต้นทาง : โปรแกรมเล็ก ๆ ที่ใช้ปฏิเสธ IP จากบริการของ xinetd

เรื่องนี้อ่านมาจาก - http://www.thailinux.com/1999/07/11/topic2.html และ http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/ref-guide/s1-tcpwrappers-accesscontrol.html **หมายเหตุ** :
บริการนี้มีปัญหานิดหน่อย เพราะใน RH7.2 สามารถให้บริการได้ตามปกติตามด้านล่าง แต่ใน RH8.0 ไม่สามารถปิดบริการหลายอย่างได้ อาจเป็นเพราะมีโปรแกรม xinetd เปิดบริการเหล่านี้อยู่ ผู้ดูแลอาจดูได้ว่ามีบริการอะไรเปิดอยู่บ้างด้วยคำสั่ง #xinted -d
โปรแกรม tcpwrapper จะมีมากับเครื่องอยู่แล้ว เพียงแต่กำหนด config ในการป้องกัน ระบบป้องกันก็จะทำงานทันที หากต้องการทราบว่าจะปิดบริการอะไรได้บ้าง สามารถเข้าไปดูที่ห้อง **/etc/xinetd.d/** ส่วนเลข port ที่เปิดบริการดูได้จาก **/etc/services** โดยทดสอบว่า **#telnet localhost 80** แต่ถ้า port นั้นปิดอยู่ก็จะไม่สามารถติดต่อได้
หากสงสัยว่า tcpwrapper ทำงานหรือไม่ ให้กำหนดใน /etc/hosts.deny แล้วพิมพ์คำว่า **all:all** เพื่อปิดทั้งหมด แล้วทดสอบติดต่อเข้าไป เมื่อ save แฟ้ม hosts.deny ระบบของ tcpwrapper ก็จะทำงานทันที .. เคยทดสอบกับ ssh ที่เดิมติดต่อได้ เมื่อสั่ง all:all จะใช้บริการ ssh ไม่ได้ หรือตรวจสอบ log ได้ที่ /var/log/secure
เพื่อไม่ให้ใคร telnet

CASE 1

ในแฟ้ม /etc/hosts.allow

```
ALL:localhost
in.telnetd:host1.isp.net
in.fingerd:ALL
```

ในแฟ้ม /etc/hosts.deny

```
All:All
```

หมายถึง ยอมให้ใน localhost ทำทุกอย่างได้
หมายถึง ยอมให้ telnet จากเครื่อง host1.isp.net ได้ และใช้ finger จากเครื่องใดก็ได้
หมายถึง ถ้าไม่อนุญาติตาม hosts.allow ก็ให้ปฏิเสธหมด

CASE ของ isinthai.com

ในแฟ้ม /etc/hosts.allow
in.ftpd in.ipop3d in.ipop2d in.imapd:All

ในแฟ้ม /etc/hosts.deny
in.telnetd in.rshd in.rlogind:ALL
ตอนแรกผมปิด all:all ทำให้ไม่สามารถบริการ pop3 หรือ imap ได้
จึงต้องเลือกปิด เฉพาะ daemon ที่น่ากลัว

CASE ของ Host ที่ต้องการปิด คือไม่บริการภายนอก

ในแฟ้ม /etc/hosts.allow
All: 202.29.78. EXCEPT 202.29.78.1

ในแฟ้ม /etc/hosts.deny
All:ALL
in.telnetd:All

คำอธิบายเพิ่มเติม

ในแฟ้ม /etc/hosts.deny
in.fingerd:ALL EXCEPT .domain.com หมายถึง ยอมให้ finger หมดยกเว้น จาก domain.com
in.telnetd in.rlogind:host1.x.com .domain.com หมายถึง ไม่ให้ telnet หรือ login จาก host1.x.com และ domain.com

หลังจากแก้ไขแฟ้ม hosts.allow หรือ hosts.deny จะมีผลต่อการอนุญาติ หรือปฏิเสธในทันที .. ลองแล้วครับ

Network Security : http://www.redhat.com/support/manuals/RHL-7.1-Manual/ref-guide/s1-security-network.html

If you use your Red Hat Linux system on a network (such as a local area network, wide area network, or the Internet), you must be aware that your system is at a greater degree of risk than if you were not connected to that network. Beyond brute attacks on password files and users having inappropriate access, the presence of your system on a larger network widens the opportunity for a security problem and the possible form it may appear.

A number of network security measures have been built into Red Hat Linux, and many open source security tools are also included with the primary distribution. However, despite your preparedness, network security problems may occur, due in part to your network topology or a dozen other factors. To help you determine the source and method of a network security problem, consider the the most likely ways such a problem can occur:

1. Sniffing for authentication data. Many default authentication methods in Linux and other operating systems depend on sending your authentication information "in the clear," where your username and password is sent over the network in plain text or unencrypted. Tools are widely available for those with access to your network (or the Internet, if you are accessing your system using it) to "sniff" or detect your password by recording all data transferred over the network and sifting through it to find common login statements. This method can be used to find any information you send unencrypted, even your root password. It is imperative that you implement and utilize tools like Kerberos 5 and OpenSSH to prevent passwords and other sensitive data form being sent without encryption. If, for whatever reason, these tools cannot be used with your system, then definitely never log in as root unless you are at the console.

2. Frontal attack Denial of Service (DoS) attacks and the like can cripple even a secure system by flooding it with improper or malformed requests that overwhelm it or create processes that put your system and its data, as well as other systems that communicate with it, at risk. A number of different protections are available to help stop the attack and minimize the damage, such as packet-filtering firewalls. However, frontal attacks are best handled with a comprehensive look at ways in which untrusted systems communicate with your trusted

systems, putting protective barriers between the two, and developing a way to quickly respond to any event so that the disruption and possible damage is limited.
3. Exploiting a security bug or loophole Occasionally, bugs are found in software that, if exploited, could do grievous damage to an unprotected system. For that reason, run as few processes as root as possible. Also, use the various tools available to you, such as the Red Hat Network for package updates and security alerts, to fix security problems as soon as they are discovered. Also, make sure that your system has no unnecessary programs starting up at boot time. The fewer programs you have started, the fewer possible security bugs can affect you.

Procmail เพื่อกรอง spam mail และ junk mail : ใช้ keyword หยุด e-mail โดยตรวจสอบจาก from และ subject

การหยุด spam mail และ junk mail ให้กับสมาชิกทั้งหมด มิใช้บางคน ทำได้โดยสร้างแฟ้มชื่อ procmailrc ในห้อง etc เวลาสร้างก็พิมพ์ว่า **#pico /etc/procmailrc** แล้วกำหนดสิ่งที่ต้องการหยุด เช่น e-mail from หรือข้อความใน subject ที่มีปัญหา แต่ถ้าสมาชิกบางคนต้องการหยุด หรือสร้างระบบป้องกันของตนเอง ก็สามารถสร้างแฟ้ม .procmailrc ใน home directory ของตนได้
ทราบว่า procmail สามารถกรอง e-mail ที่มีปัญหาโดยตรวจสอบจาก from และ subject ได้ ผมจึงตรวจสอบว่าในเครื่องมีโปรแกรมนี้ไหมด้วยการพิมพ์ **rpm -q procmail** ก็พบว่ามีแล้วโดยแสดงคำว่า procmail-3.22-7 ให้เห็น จากนั้นก็หาข้อมูลจากเอกสารต่าง ๆ
- https://nontri.ku.ac.th/tools/procmail/ (ภาษาไทยอ่านง่าย ละเอียด จาก ม.เกษตรศาสตร์)
- http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/ref-guide/s1-email-procmail.html
- http://www.uwasa.fi/~ts/info/proctips.html
- http://piology.org/.procmailrc.html
- http://www.procmail.org
- http://www.linuxbrit.co.uk/downloads/dot.procmailrc
- http://www.iegrec.org/procmailrc.html
ถ้าต้องการมี .procmailrc ของตนเอง ให้สร้าง .procmailrc ด้วย notepad ในเครื่องตนเอง แล้วส่งเข้าไปใน home directory ของท่านด้วย **ftp yn1.yonok.ac.th** แต่ถ้าไม่ใช้ก็ไม่เป็นไร เพราะผมกำหนด /etc/procmailrc เพื่อใช้กรองให้กับทุกคนโดยอัตโนมัติแล้ว

ข้อมูลในแฟ้ม procmailrc หรือ .procmailrc

```
:0
# block From on email
* 1^0 From:.*webmaster@yn1.yonok.ac.th
* 1^0 From:.*@sex.com
* 1^0 From:.*mailer-daemon@
* 1^0 From:.*offers@readytoday.biz
/dev/null

# block "Britney spear", "FUKADARAKA HELLO"
# no block "afukadara", "love britney"
:0
* ^Subject: (britney|fukada|adv:)
/dev/null

# block "love britney spear", "Hot of britney", "kyoko fukada"
:0
* ^Subject:.*(britney|fukada)
/dev/null

# block "hi", "TEST"
:0
* 1^0 ^Subject: hi$
* 1^0 ^Subject: test$
* 1^0 ^Subject: hello$
```

```
/dev/null

# block message on body
:0B:
* (YONOK college xxx|The message cannot be represented in 7-bit ASCII)
/dev/null

# block message on attached extension
:0
*^Content-type: (multipart/mixed|application/octet-stream)
{
  :0 HB
  *^Content-Disposition: attachment;
  *filename=".*\.(vbs|vbe|com|bat|pif|scr)"
  /dev/null
}
```

โปรแกรมภาษา c เพื่อสร้าง crypt ให้ shadow : เนื่องจากผมต้องการสร้าง user แบบ online จึงหาวิธีสร้าง useradd ผ่านเว็บ

วันที่ 8 มิถุนายน 2544 ได้คุยกับอ.dav จนท่านช่วยผมเขียนโปรแกรมภาษา c ตัวหนึ่ง ซึ่งใช้เข้ารหัส ผลการเข้ารหัส สามารถนำไปใช้ในคำสั่ง useradd เช่น **useradd -p xdfiWsoOsdg0M tom** จะทำให้สร้าง user ใหม่ชื่อ tom ได้โดยรหัสจะต้องได้มาจากโปรแกรมที่อ.dav เขียนไว้ด้านล่างนี้

```
คุยกับ อ.dav เรื่องการสร้าง useradd อัตโนมัติ
ซึ่งผมมีปัญหาเรื่องของรหัสผ่านที่เก็บใน shadow
ท่านก็ช่วยผมสร้างโปรแกรมรหัสผ่านขึ้นมาอย่างง่าย ๆ ดังข้างล่างนี้
แค่นำค่าที่ได้ไปแทนค่า xxx ของ userhello ก็จะได้รหัสผู้ใช้ ผ่านคำสั่งเดียว
เช่น useradd -p xxx userhello
ผมไม่เคยเขียน c บน linux โปรแกรมนี้คงเป็นตัวแรกของผมหละครับ
// program to encrypt passwords for the shadow file.
// compile with gcc pwcrypt.c -opwcrypt -lcrypt
// Dav ...
#include <stdlib.h>
#include <stdio.h>
#include <unistd.h>
int main( int argc, char **argv ) {
  int i;
  char *pwd;
  if( argc != 3 ) {
    fprintf( stderr, "Usage: pwencode username password\n" );
    exit( -1 );
  }
  //encripting the password for insertion into shadow
  pwd = crypt( argv[ 2 ], argv[ 1 ] );
  printf( "%s %s\n", argv[ 2 ], pwd );
  return 0;
}
```

ลืมรหัสผ่านของ root : วิธีนี้ใช้ได้ใน Redhat version 6.2 แน่นอน แต่รุ่นอื่นก็มีวิธีต่างกันไปบ้างเล็กน้อย

ผมทราบวิธีนี้เพราะเข้าไปดูที่ redhat.com ในส่วนของ FAQ และที่ต้องเข้าไปดูก็เพราะมี hacker จาก **193.231.178.98** เข้ามาด้วย operator account แล้วเปลี่ยนรหัสผ่านของ root ไป ทำให้ผมไม่สามารถเข้าไปสร้างผู้ใช้ใหม่ได้ ถามหลาย ๆ ท่านก็บอกให้ใช้แผ่นบูต แบบ linux rescue ผมก็เข้าไป จะ mount จะอะไรก็ไม่ได้ อาจเป็นเพราะยังไม่ชำนาญ แต่วิธีการเรียกรหัสผ่านของ root คืนในแบบที่ผมได้มานี้ ง่ายกว่าวิธีใด ๆ แน่นอน และน่าจะทำได้ใน Redhat เวอร์ชัน 6.0 หรือ 6.2 ขึ้นไปครับ

ขั้นตอนสำหรับ LILO

1. เมื่อ Restart เครื่อง ก่อนเข้าระบบ ให้กด Alt-X ขณะที่อยู่ที่ LILO prompt แล้วพิมพ์ว่า linux single
2. เมื่อเข้าไปจะได้สถานะเป็น root ทันที ก็เพียงแต่ใช้คำสั่ง passwd root แล้ว reboot ก็เรียบร้อยแล้ว

ขั้นตอนสำหรับ GRUB

1. เมื่อ Restart เครื่อง ก่อนเข้าระบบขณะที่อยู่ที่ GRUB prompt ให้กด e แล้วพิมพ์ว่า single ตามหลังคำสั่ง boot ระบบ
2. เมื่อเข้าไปจะได้สถานะเป็น root ทันที ก็เพียงแต่ใช้คำสั่ง passwd root แล้ว reboot ก็เรียบร้อยแล้ว
3. สำหรับเครื่อง Sun ซึ่งเป็น Unix server ที่ดี จะใช้การ Reboot และกดปุ่ม stop a แล้วใช้คำสั่ง boot -s

httpd.conf เพื่อแก้ปัญหาของ web server : แฟ้มนี้คุมบริการต่าง ๆ ซึ่งสำคัญต่อต้องการ web server ในองค์กร

แก้ไขแฟ้ม /etc/httpd/conf/httpd.conf :

1. **ปัญหาภาษาไทย** ใน RH8.0 เมื่อติดตั้งบริการเว็บเสร็จแล้ว ปัญหาคือ ผู้เปิดเว็บใดก็ตามในระบบ ทุกครั้งจะต้องไปแก้ไข encoding แล้วเลือก Thai(Windows) เพื่อแสดงภาษาไทย จึงต้องแก้ไขให้กำหนด default ที่ถูกต้อง ตามที่กำหนดในเว็บเพจ (แก้ในเว็บเพจเป็น meta 874 ก็ไม่ได้)

   เดิม :: AddDefaultCharset ISO-8859-1
   ใหม่ :: AddDefaultCharset WINDOWS-874
   เพิ่ม :: AddCharset WINDOWS-874 .cp-874 .win-874

2. ทำให้ผู้มี linux account สามารถมีเว็บของตนเอง (อ่านรายละเอียดเพิ่มเติมในหัวข้อ 9.62)

   เดิม :: UserDir Disable
   ใหม่ :: UserDir public_html
   - แต่ละ user ต้อง **chmod 711** ให้กับ home directory ของตนเอง
   - แล้ว **chmod 755** ให้กับ public_html ของตนเองหลัง
   - เปิดเว็บ **http://www.isinthai.com/~username**

3. ทำให้ใช้ .cgi และ .pl ได้

   เดิม :: #AddHandler cgi-script .cgi
   ใหม่ :: AddHandler cgi-script .cgi .pl
   เดิม
   <Directory "/var/www/cgi-bin">
   AllowOverride None
   Options None

ใหม่ :: Options ExecCGI
เดิม
<Directory "/var/www/html">
Options Indexes FollowSymLinks
ใหม่ :: Options All

4. ทำให้ใช้ <? แทนการใช้เฉพาะ <?php ในการเขียนโปรแกรมด้วยภาษา php โดยแก้แฟ้ม /etc/php.ini

เดิม :: short_open_tag = Off
ใหม่ :: short_open_tag = On

เปิดบริการ FTP server ด้วย vsftpd : บริการ ftp server เพื่อให้สมาชิกส่งแฟ้มผ่าน ftp เข้ามาใน server ได้สะดวกกว่าการใช้ file manager

เปิดบริการ ftp ด้วยคำสั่ง setup, system services แล้วเลือกเปิด vsftpd แล้วเข้าไปในห้อง /etc/xinetd.d แล้วใช้ **pico vsftpd** แล้วเปลี่ยนจาก disable=yes เป็น disable=no แล้วสั่ง /etc/rc.d/inetd/xinetd restart

---

วิธีเปิดบริการ homepage ให้ ~username ใน linux : เปิดบริการ homepage โดยใช้ account ของระบบ linux

อ่านรายละเอียดเพิ่มเติมได้จาก http://httpd.apache.org/docs/misc/FAQ.html
การเปิดบริการ free homepage ของ Web server อีกแบบหนึ่ง ในการเปิดบริการแบบใหม่จะใช้โปรแกรม เช่น http://www.cyberscript.net/products/easyhost_free/ ที่ไม่ต้องสร้าง linux account แต่อย่างใด และมีความปลอดภัยในการบำรุงรักษาสูง
การเปิดบริการ free homepage แบบใช้ linux account เช่น http://www.isinthai.com/~username สามารถเปิดบริการได้ด้วยการแก้ไขแฟ้ม /etc/httpd/conf/httpd.conf แก้บรรทัดที่เขียนว่า **UserDir Disable** เป็น **UserDir public_html** แล้วต้อง chmod 711 ให้กับ home directory ของตนเอง แล้ว chmod 755 ให้กับ public_html ของตนเองหลังจากใช้คำสั่ง mkdir public_html ไว้ใน home directory แล้ว

วิธีเปิดบริการ samba : เปิดบริการให้ระบบ windows มองเห็นระบบแฟ้มใน linux

ทดสอบ samba ของ RH8.0 แก้ไขดังข้างล่างแล้วไม่พบปัญหาใดเลย .. ง่ายมากครับ
เปิดบริการ samba ด้วยคำสั่ง setup, system services แล้วเลือกเปิด smb แล้วเข้าไปในห้อง /etc/samba แล้วใช้ **pico smb.conf** จากนั้น restart ด้วย **/etc/rc.d/init.d/smb restart** และให้พิมพ์ **chkconfig smb on** จะทำให้ samba start ทุกครั้งที่เปิดเครื่อง
คำสั่งที่ใช้สร้าง user คือ smbpasswd -a [username] [userpassword]

::::::: **เดิม** :::::::	::::::: **ใหม่** :::::::
; hosts allow = 192.168.1. 192.168.2. 127. security = user [homes] comment = Home Directories browseable = no writable = yes valid users = %S create mode = 0664	hosts allow = 192.168.1. 192.168.2. 127. 202.29.78 security = share [homes] comment = Home Directories browseable = yes writable = yes create mode = 0664 directory mode = 0775

```
  directory mode = 0775
;[tmp]
;   comment = Temporary file space
;   path = /tmp
;   read only = no
;   public = yes
;[public]
;   comment = Public Stuff
;   path = /home/samba
;   public = yes
;   writable = yes
;   printable = no
;   write list = @staff
```

```
[tmp]
  comment = Temporary file space
  path = /tmp
  read only = no
  public = yes
[public]
  comment = Public Stuff
  path = /home/samba
  public = yes
  writable = yes
  printable = no
  write list = @staff
```

เปิดบริการ DNS server

: บริการ Domain Name service เพื่อให้ทุกเครื่องสามารถเรียกเว็บ หรือบริการด้วยชื่อได้

เปิดบริการ DNS server เพื่อทำให้ระบบเครือข่ายเรียกชื่อเว็บ เป็นตัวอักษรได้ และเป็นชุดที่ใช้กำหนดชื่อเครื่องในระบบทั้งหมด ถ้าในระบบเครือข่ายของท่าน มีเครื่องที่ต้องการตั้งชื่อหลายเครื่อง แต่ถ้าท่านเป็นเครื่องใช้พิมพ์งานธรรมดาก็ไม่จำเป็นต้องมีชื่อให้ใครเรียกเข้ามา ปกติเครื่องที่จะมีชื่อมักเป็น web server หรือ ftp server การเปิดบริการนี้ต้องเปิดด้วยการสั่ง #setup แล้วเข้าไปในส่วน system services แล้วเลือก named เมื่อจะสั่งให้ named ทำงานต้องสั่ง #/etc/init.d/named restart ตรวจสอบได้ว่า named ทำงานหรือไม่โดยพิมพ์ #ps aux|grep named

9.66.1 :: /etc/named.conf

```
# ใน DNS server (star.yonok.ac.th)
# เพิ่มเพียง 4 บรรทัดนี้เข้าไป
# ใน unix พบแฟ้มนี้ใน /export/local/etc
zone "yonok.ac.th" in {
        type master;
        file "db.yonok.ac.th";
        allow-query {any;};
        allow-transfer {202.28.18.65;};
};
zone "isinthai.com" in {
        type master;
        file "db.isinthai.com";
};
zone "78.29.202.in-addr.arpa" in {
        type master;
        file "db.202.29.78";
};
```

9.66.2 :: /var/named/db.isinthai.com

```
# ใน DNS server (star.yonok.ac.th)
# ถ้าเครื่องไม่เป็น ns ก็ไม่จำเป็นต้องมี
; isinthai.com
@       IN  SOA www.isinthai.com. postmaster.www.isinthai.com. (
          2001022605 43200 7200 1209600 172800 )
        IN  NS      star.yonok.ac.th.  ; ตรงกับ checkdomain.com
        IN  MX      5 www.isinthai.com.
www     IN  A       202.29.78.1
mail    IN  CNAME   www.isinthai.com.
wichep IN  CNAME   yn2.yonok.ac.th.
```

9.66.3 :: /var/named/db.yonok.ac.th

```
; yonok.ac.th
@ IN SOA star.yonok.ac.th. postmaster.star.yonok.ac.th. (
            2003011001 43200 7200 1209600 172800 )
      IN     NS     star.yonok.ac.th.
      IN     NS     mars.uni.net.th.
      IN     MX     5 star.yonok.ac.th.
star   IN     A      202.29.78.12
door   IN     A      202.29.78.254
email  IN     A      216.200.145.34
      IN     MX     6 sitemail.everyone.net.
mail   IN     CNAME  star.yonok.ac.th.
;email IN     CNAME  siteurl.everyone.net.
```

9.66.4 :: /var/named/db.202.29.78

- ใน DNS server (star.yonok.ac.th)
- ถ้าเครื่องไม่เป็น ns ก็ไม่จำเป็นต้องมี

```
; Yonok.ac.th
$ORIGIN 78.29.202.IN-ADDR.ARPA.
@   IN  SOA star.yonok.ac.th. postmaster.star.yonok.ac.th. (
       2001022601 ;serial
       43200      ;Refresh 12 hours
       7200       ;Retry 2 hours
       1209600    ;Expire 2 weeks
       172800)    ;TTL
    IN  NS   star.yonok.ac.th.
1   IN  PTR  www.isinthai.com.
2   IN  PTR  isinthai.yonok.ac.th.
12  IN  PTR  star.yonok.ac.th.
```

ติดตั้ง Free hosting ด้วย easyhost_free.zip

: ช่วยให้ server สามารถบริการ free hosting ได้โดยง่ายผ่าน file manager

- Download CGI script นี้จาก http://cyberscript.net/products/easyhost_free/download.html
- รายละเอียดการติดตั้งอ่านได้จาก http://cyberscript.net/support/docs/
- copy แฟ้มทั้งหมดในห้อง cgi-bin ไป /var/www/cgi-bin ด้วยคำสั่ง #mv * /var/www/cgi-bin
- copy ห้อง data และ images ไป /var/www/html ด้วยคำสั่ง #mv images /var/www/html
- ใช้คำสั่ง #chmod 755 /var/www/cgi-bin/*.*
- ใช้คำสั่ง #chmod 777 /var/www/cgi-bin/config.ini
- ใช้คำสั่ง #chmod 777 /var/www/html/data
- ใช้คำสั่ง #chmod 777 /var/www/html
- เปิดเว็บ http://www.isinthai.com/cgi-bin/admin.cgi
- ถ้าเปิด admin.cgi แล้ว error โดยหาสาเหตุไม่ได้แสดงว่าไม่ได้ upload แบบ ascii ให้ใช้ pico เพิ่มบรรทัดว่างล่างสุดแล้ว save ทับ
- ถ้า CGI ยังไม่ทำงาน ให้ไปแก้แฟ้ม /etc/httpd/conf/httpd.conf เพื่อเปิดบริการต่าง ๆ ของ apache web server
- สมาชิกใหม่จะมีห้อง images และแฟ้ม index.html ที่คัดลอกมาจากห้อง /var/www/html/data/default เข้าไปแก้ไขห้องนี้ได้

ข้อมูลในแฟ้ม /var/www/cgi-bin/config.ini

space_limit=55000
reserved_names=cgi-bin,data,images,mail
title_min=3
root_url=http://www.isinthai.com
password_max=20
site_password=asaRYYyl3HBzW
description_required=on
title_max=50
name_min=3
banned_extensions=.cgi,.pl,.php,.php3,.exe,.mp3,.dat,.mpg,.mpv,.zip,.rar,.ace,.class
distinct_email=1
use_validation=off
site_email=webmaster@yonok.ac.th
description_max=150
root_dir=/var/www/html
data_dir=/var/www/html/data
password_min=2
site_title=isinthai.com :: Case study of free hosting with 55 Mb
name_max=20
script_url=http://www.isinthai.com/cgi-bin

วิธีงดบริการสร้างสมาชิกใหม่ โดยบุคคลทั่วไป

เนื่องจากปิดบริการ free webhosting ของ isinthai.com แต่ยังเปิดให้สมาชิกในองค์กรหรือเจ้าหน้าที่ หรือ webmaster สร้างสมาชิกใหม่ด้วยโปรแกรม **/var/www/cgi-bin/create_user.cgi** โปรแกรมจะรอรับข้อมูลเมื่อทราบ keyword เท่านั้น โดยเติม 5 บรรทัดข้างล่างนี้เข้าไปที่ส่วนต้นของโปรแกรม

```
// http://www.isinthai.com/cgi-bin/create_user.cgi?officer
if ($ENV{QUERY_STRING} ne 'officer') {
   print "Content-type: text/html\n\n";
   print "Stop service";
   exit;
}
```

ติดตั้ง Web-based mail ด้วย uebimiau-2.7.2-any.zip

: ช่วยให้ server สามารถอ่าน mail จาก POP3 และส่งด้วย SMTP ผ่านระบบ Web-based mail

- Download จาก http://uebimiau.sourceforge.net/ (PHP script)
- เคยแนะนำการเปิดบริการ pop3 ใน win2003 กับโรงเรียนเขลางค์
  อ่านจาก
http://www.windowsnetworking.com/articles_tutorials/Windows_POP3_Service.html
- copy ห้องทั้งหมดภายใต้ห้อง uebimiau-2.7.2 หลังคลาย zip ไปไว้ใต้ห้อง /var/www/html/mail
- แก้แฟ้ม /var/www/html/mail/inc/config.php กำหนด pop และ smtp ให้เป็นตามต้องการ
- ใช้คำสั่ง #chmod 777 /var/www/html/mail/database
- แก้แฟ้ม /var/www/html/mail/langs/th.txt เพื่อให้มีภาษาไทยตามที่เราต้องการ
- แก้แฟ้ม /var/www/html/mail/themes/default/login.htm เพื่อปรับหน้าจอของหน้าแรก

แก้แฟ้ม inc/config.php ให้อ่านกับ POP3 ของ windows server 2003

จาก "login_type" => "%user%"
เป็น "login_type" => "%user%@%domain%"

การแก้ไข config ของแฟ้มในห้อง inc และ lang

กรณีเขียน e-mail ยาว ๆ พอกดปุ่มส่ง ปรากฏว่าเด้งไปหน้า login มีผลตามมาคือจดหมายฉบับนั้นไม่ถูกส่งไป จึงต้องไปแก้ไขในส่วนของ Session timeout for activity ในแฟ้ม /var/www/html/mail/inc/config.php

เดิม $idle_timeout = 10; // Minutes

ใหม่ $idle_timeout = 100; // Minutes

ติดตั้ง DHCP server แจก Dynamic IP

: เพื่อให้เครื่อง Server มีบริการแจก IP ปลอมให้กับเครื่องในองค์กร เพราะปกติองค์กรจะได้ IP มา 1 Class C มี 256 หมายเลข แต่ถ้าในองค์กรมีเครื่องจำนวนมากกว่านั้น ก็จำเป็นต้องสร้าง DHCP server เพื่อแจก IP ปลอม และยังมีประโยชน์ในเรื่องของความปลอดภัย เพราะเครื่องที่ได้ IP ปลอม ย่อมต้องมีการทำงานขึ้นกับเครื่อง server จะแอบออกไปน้องเครือข่ายได้ยาก

ขั้นตอนการทำให้ Linux server บริการ DHCP (Dynamic Host Configuration Protocol)

1. ถ้าใช้คำสั่ง setup เพื่อเปิดบริการ DHCP แล้วไม่พบบริการ ต้องติดตั้ง DHCP จากแผ่น CD ด้วยการใช้คำสั่งด้านล่าง ในห้องที่เก็บแฟ้มนี้ ก็ใช้ setup เข้าไปเปิดบริการนี้ใหม่

```
rpm -i dhcp*
```

ต้องใช้โปรแกรม ipchains ท่านควรตรวจหาในเครื่องว่ามีหรือไม่ด้วยการการใช้ rpm -q ipchain ถ้าไม่มีก็ต้องติดตั้งเพิ่มจากแผ่น CD ด้วยคำสั่ง rpm -i ipchain* แล้ว ต้องใช้คำสั่ง setup เพื่อเข้าไปเปิดบริการ ipchains อีกครั้ง

ทำให้เครื่องมี IP ปลอมเกิดขึ้นด้วย โดยพิมพ์สั่งใส่ใน **/etc/rc.d/rc.local** เพื่อกำหนด IP ปลอมแก่เครื่อง server นี้ ทุกครั้งที่เปิดเครื่อง

```
/sbin/ifconfig eth0:1 192.168.3.1
```

สร้างแฟ้ม /etc/dhcpd.conf ด้วย pico หรือ vi

```
5.    default-lease-time 21600;
6.    max-lease-time 43200;
7.    ddns-update-style ad-hoc;
8.    option subnet-mask 255.255.255.255;
9.    option broadcast-address 192.168.3.255;
10.   option routers 192.168.3.1;
11.   option domain-name-servers 192.168.3.1;
12.   option domain-name "yn2.yonok.ac.th";
13.   subnet 192.168.3.0 netmask 255.255.255.0
14.   {
15.     range 192.168.3.10 192.168.3.250;
16.   }
```

การทำให้ใช้ IP forwarding ต้องแก้แฟ้ม /etc/sysctl.conf จาก 0 เป็น 1 โดยแก้เป็นบรรทัดด้านล่าง

```
net.ipv4.ip_forward = 1
```

เมื่อแก้ไขเสร็จแล้วให้พิมพ์คำสั่งใน command line ดังนี้

```
echo "1" >/proc/sys/net/ipv4/ip_forward
```

ต้องสั่ง IP forwarding เพราะเครื่องลูกไปไหนไม่ได้ แต่เครื่อง server มี IP จริง และ IP ปลอม จึงต้องสั่งให้ IP ปลอมมาเข้ากับ IP จริง ด้วยการใช้ ipchains กำหนดการ forward

```
/sbin/ipchains -A forward -i eth0 -s 192.168.3.1/24 -j MASQ
```

หลังผมเปิดบริการ เครื่องลูกก็ใช้งานได้แล้ว แต่ไม่อยากใช้งาน จึงปิดบริการด้วยการสั่ง setup แล้วเลือก * หน้า dhcp ออก

ติดตั้ง webbased mail ของ adjeweb.com

: โปรแกรมนี่เป็นภาษา perl ใช้ติดตั้งใน server เพื่อทำให้เครื่องให้บริการ webbased mail ได้ แต่ต้องบริการ pop ก่อนนะครับ

ขั้นตอนการติดตั้ง ข้อ 1 และ 2 จะทำเมื่อใช้คำสั่ง rpm -qa|grep imap แล้วไม่พบว่ามีอยู่แล้ว จึงต้องติดตั้งเพิ่ม

1. หากยังไม่ได้ mount cd ต้องทำก่อนโดยใช้คำสั่ง **mount /dev/cdrom** ก็จะทำให้มีห้อง **/mnt/cdrom** ขึ้นมา ใช้คำสั่ง cd เข้าไปดูได้
2. ติดตั้ง imap ซึ่งก็คือ pop3 นั่นเองจาก CD ที่ใช้ลง linux ด้วยคำสั่ง **rpm -i imap-4.7-5.i386.rpm** และ **rpm -i imap-devel-4.7-5.i386.rpm**
3. ถ้าต้องการให้เครื่องนี้บริการ pop3 เอง สามารถเปิดบริการ โดยแก้แฟ้ม /etc/inetd.conf นำ # ออกหน้าคำว่า pop3 pop2 imap มิเช่นนั้นจะไม่สามารถบริการ pop ได้ แต่สามารถรับส่ง mail ด้วย telnet หรือจะใช้ adje ไปขอบริการจาก pop server ตัวอื่นก็ได้ คำสั่งที่ใช้ re-read inetd.conf คือ **killall -HUB inetd** และคำสั่งที่น่ารู้คือ **ntsysv** เพื่อใช้เปิด หรือปิดบริการใน /etc/services
4. อาจตรวจสอบว่าเปิดบริการหรือไม่ด้วยคำสั่ง setup, system services ดูในส่วนบริการ ipop2 และ ipop3 จะต้องมีเครื่องหมาย x เพื่อแสดงว่าบริการนี้เปิดแล้ว
5. สร้าง user ชื่อ webmail แล้วใช้ user นี้ทำงาน หรือใช้ **su - webmail** เพื่อเปลี่ยนตนเองอย่างง่าย ๆ ก็ได้
6. copy โปรแกรมสำหรับ install จาก adjeweb.com หรือ install.pl (ตัวนี้ต้อง rename ก่อน เพราะผม save เปลี่ยนชื่อไว้)
7. หมายความว่าเมื่อ copy adjewebmailinstall.pl.txt มาได้แล้วให้ใช้ **mv adjewebmailinstall.pl.txt install.pl** เพราะถ้าผมเก็นในสกุล .pl ท่านจะ copy มาไม่ได้
8. ก่อนลงโปรแกรมให้ chmod ห้อง **/home/httpd/cgi-bin** เป็น 777 ก่อนแล้วค่อยเปลี่ยนคืนเป็น 755 ด้วยคำสั่ง chmod 777 **/home/httpd/cgi-bin**
9. เมื่อได้โปรแกรมมา ให้ **chmod 755 install.pl**
10. Install ด้วยการพิมพ์ว่า **./install.pl** ซึ่งแฟ้มนี้ควรอยู่ใน home directory ของท่าน
11. เมื่อถามว่า cgi อยู่ห้องใดก็มักจะเป็น **/home/httpd/cgi-bin**
12. เมื่อถามว่า pop server คืออะไร ก็ตอบว่า **www.isinthai.com** หรือ กดปุ่ม Enter หรือ จะใส่ ip ของเครื่องก็ OK เป็นต้น
13. เมื่อถามว่า pop server คืออะไร ก็ตอบว่า **mail.loxinfo.co.th** เป็นต้น
14. reboot สักหน่อย แล้วเปิดเว็บเรียก **http://www.isinthai.com/cgi-bin/WebMail/inbox.cgi** ก็เรียบร้อย
15. จะให้ดีเป็น su แล้วให้ **ln -s /home/httpd/cgi-bin/WebMail /home/httpd/html/webmail** จะทำให้เปิดเว็บด้วย **http://www.isinthai.com/webmail** ซึ่งสั้นกว่ากันเยอะ

ติดตั้ง squid เป็น Proxy server ที่ 3128

: โปรแกรมนี่จะทำให้ความเร็วในการให้บริการ internet โดยรวมขององค์กรดีขึ้น ถ้าปฏิบัติตามระเบียบในการใช้ proxy

ระเบียบการใช้ proxy

1. เมื่อติดตั้ง squid ลงไปใน linux server ขององค์กรแล้ว ท่านก็จะได้เครื่อง proxy server ขึ้นมา 1 ตัว
2. ไปกำหนดในเครื่องทุกเครื่องให้มองมาที่ proxy server ตัวนี้ เช่น **www.isinthai.com** บน port **3128** อย่ากำหนดมาที่นี่นะครับ เพราะจะทำให้เครื่องท่าน เปิดเว็บช้าโดยใช่เหตุ แต่ถ้าเครื่องของท่านตั้งอยู่ในเครือข่ายของโยนก นั่นจะเป็นอะไรที่ถูกต้อง
3. หลังจากกำหนด proxy ให้ชี้ไปที่ www.isinthai.com อย่างถูกต้องแล้ว ทุกครั้งที่เปิดเว็บด้วย browser จะวิ่งไปที่เครื่องนั้นก่อน เพื่อตรวจว่า เว็บที่ขอเปิดเคยเปิดหรือไม่ ถ้าเคยเมื่อไม่นานนี้ ก็จะไม่ออกไปนอกเครือข่าย แต่จะเอาข้อมูลจาก proxy มาให้ท่าน **ทำให้ไม่ต้องออกไปนอกเครือข่าย** โดยไม่จำเป็น

ขั้นตอนข้างล่างนี้ **อาจไม่จำเป็น** ต้องทำทุกขั้นตอน ถ้าตอน install linux ได้เลือก squid หรือ everything ก็ไม่จำเป็นต้อง ลงโปรแกรมอีกรอบ เพียงแต่เข้าไป set up แฟ้ม squid.conf ใน /home/squid/etc/squid.conf หรือ /etc/squid/squid.conf แต่ถ้าเปลี่ยนใจต้องการ ลง squid ใหม่ แทนที่จะใช้ตัวที่ติดตั้งมาก็ลบตัวเดิมออกด้วยคำสั่ง **rpm -e squid-2.3.STABLE1-5** เพราะผมใช้คำสั่ง **rpm -qa|grep squid** แล้วพบว่า install มาตอนติดตั้ง linux ครับ (squid-2.3-200103110000-src.tar.gz ขนาด 971,877 byte) **ติดตั้ง squid เพื่อทำให้ server เป็น proxy สำหรับองค์กร** ที่ต้องการลดปัญหาคอขวด มีบทความแนะนำที่ http://www.thailinux.com/1999/04/18/topic1.html **คุณ new way เขียนได้ละเอียดดีมาก ต้องยกนิ้วให้ครับ** ซึ่งแนะนำให้ Download squid ของ http://squid.nlanr.net/Squid/ เมื่อลง squid ตามขั้นตอนแล้ว มี จุดที่ต้องแก้ไขในแฟ้ม ~/etc/squid.conf คือ cache_effective_user squid และ cache_effective_group squid และ cache_peer www.isinthai.com parent 3128 3130 และ http_access allow all **ดู log file ของ squid ที่ห้อง ~/logs ในแฟ้ม cache.log** (ต้องใช้ user squid ในการ set squid ตลอดนะครับ) โดยใช้คำสั่ง **tail -f access.log** และสามารถอ่านรายละเอียด การกำหนดเพิ่มเติม ได้ที่ http://www.squid-cache.org/Doc/Hierarchy-Tutorial/

ขั้นตอนการติดตั้ง squid ให้เครื่องเป็น proxy server
http://www.thailinux.com/1999/04/18/topic2.html

```
su
adduser squid
passwd squid
su squid (ไม่ใช้ user squid ก็ได้ แต่ถ้าใช้ดูด้วยว่า gcc เปิดหรือไม่)
cd /home/httpd/html/thaiall
tar xfvz squid-2.3-200103110000-src.tar.gz
cd squid-2.3-200103110000
./configure --prefix=/home/squid
make all
make install (แปลกมากที่ บรรทัดนี้ error แต่ก็ไม่เป็นไร เพราะใช้งานได้ปกติ)
cd /home/squid/etc
pico squid.conf
```

```
# Detail in file /home/squid/etc/squid.conf หรือ
/etc/squid/squid.conf
http_port 3128
cache_peer www.isinthai.com parent 3128 3130
cache_mem  8 MB
cache_swap_low  90
cache_swap_high 95
maximum_object_size 4096 KB
minimum_object_size 0 KB
ipcache_size 1024
ipcache_low  90
ipcache_high 95
cache_dir ufs /home/squid/cache 100 16 256
cache_access_log /home/squid/logs/access.log
cache_log /home/squid/logs/cache.log
cache_store_log /home/squid/logs/store.log
```

```
refresh_pattern                 ^ftp:                   1440
        20%     10080
refresh_pattern                 ^gopher:    1440        0%
        1440
refresh_pattern     .                       0           20%
        4320
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 80 21 443 563 70 210 1025-65535
acl Safe_ports port 280
acl Safe_ports port 488
acl Safe_ports port 591
acl Safe_ports port 777
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow all
icp_access allow all
miss_access allow all
cache_effective_user squid
cache_effective_group squid
```

ทดสอบการทำงานของ squid

cd /home/squid/bin หรือ /usr/sbin
squid -z สร้าง swap directory
squid สั่ง start manual
ps aux|grep squid ดูว่า squid ทำงานใน process หรือไม่
cd /home/squid/logs ห้องนี้เก็บ ผลการทำงานเมื่อใช้ squid
tail -f access.log เมื่อมีคนเปิดเว็บแล้วใช้บริการ squid จะมีผลต่อแฟ้มนี้

วิธีทำให้ทุกครั้งที่เปิดเครื่องแล้ว run squid อัตโนมัติ หรือปรับปรุง

เพิ่มบรรทัดข้างล่างนี้ไปในแฟ้ม /etc/rc.d/rc.local
su -c "nohup /home/squid/bin/squid&" squid
หรือ
su -c "nohup /usr/sbin/squid&" squid

เมื่อปรับค่า เช่นขนาดของ cache ใน /home/squid/etc/squid.conf หรือ /etc/squid/squid.conf
แล้วต้องทำบรรทัดข้างล่างนี้ เพื่อ update ค่าต่าง ๆ ใหม่
squid -k reconfigure

แสดง option ของ squid ให้พิมพ์ว่า
squid -k

เพิ่ม incoming ในบริการ ftp

: บริการ ftp ทำให้ท่านสามารถเข้ามา คัดลอกแฟ้ม หรือส่งแฟ้มไว้ได้ เช่น ftp://www.isinthai.com ftp://ftp.isinthai.com

พบว่าการปิด gcc นั้นสามารถป้องกัน hacker ในระดับ telnet ได้ระดับหนึ่ง แต่ถ้ามีการเปิด ftpd ด้วย ถึงไม่ telnet เข้ามา hacker ก็สามารถเจาะเข้ามาในระบบได้ .. เขาทำได้

รายชื่อห้องใน /home/ftp แต่เราได้เพิ่ม incoming เข้าไป เพื่อให้ส่งแฟ้มเข้ามาได้

```
d--x--x--x    2 root     root        4096 Mar  9 20:51 bin
d--x--x--x    2 root     root        4096 Mar  9 20:51 etc
drwxr-xr-x    2 root     root         4096 Mar  9 20:51 lib
drwxrwxrwx    2 root     root          4096 Mar 20 23:55 incoming
drwxr-sr-x    2 root     ftp         4096 Mar 11 13:34 pub
```

วิธีสร้างห้อง incoming เพื่อให้ใคร ๆ ส่งแฟ้มเข้ามาได้

```
su
cd /home/ftp
mkdir incoming
chmod 777 incoming
```

User authentication ด้วย .htpasswd + .htaccess

: การปิดห้อง แต่ยอมให้เข้าด้วย username และ password ที่กำหนด

อ่านเพิ่มเติมได้จาก http://www.apacheweek.com/features/userauth หรือ http://www.thaiall.com/cgi/htpasswd.pl

ขั้นตอนการ lock ห้องของตนเอง ในฐานะผู้ใช้ทั่วไป

1. ท่านต้องส่งแฟ้ม 2 แฟ้มคือ .htpasswd และ .htaccess ไปไว้ในห้องที่ต้องการ lock โดยทำการถาม User และ password ก่อนเข้า
2. **.htaccess** นั้นสามารถคัดลอกด้านล่างไปได้เลย โดยแก้ไขอะไรเล็กน้อยตามต้องการ เช่นเปลี่ยนคำว่า lock ที่บรรทัดแรก เป็น username ของท่าน
3. **.htpasswd** แต่ละบรรทัดคือ 1 user สำหรับแฟ้มนี้ ถ้าผู้ดูแลไม่คิดบริการ ท่านก็ใช้บริการไม่ได้ สำหรับ server ที่ผมดูแล ได้ทำ **โปรแกรมเข้ารหัส** สร้างรหัสให้
   ถ้าเป็นผู้ดูแล(Super user) สามารถใช้
   คำสั่ง **#htpasswd -nb yourname yourpassword** แสดงรหัสผ่าน ที่ shell prompt
   คำสั่ง **#htpasswd -c .htpasswd yourname** สร้างแฟ้ม .htpasswd พร้อม รอรับรหัสผ่าน จากแป้นพิมพ์
   ดูเพิ่มเติมจาก **#man htpasswd** ที่ shell prompt
4. เปิดเว็บ http://www.isinthai.com/lock/index.php เพื่อป้อนรหัสผู้ใช้ และรหัสผ่าน จะได้รหัสที่สร้างขึ้น เพื่อนำไปเพิ่มในแฟ้ม .htpasswd

http://www.isinthai.com/lock/.htaccess

```
AuthUserFile /var/www/html/lock/.htpasswd
AuthName "User:yourname Password:yourpassword for accessing this directory"
AuthType Basic
require valid-user
DirectoryIndex index.html index.htm index.shtml index.php
```

http://www.isinthai.com/lock/.htpasswd

```
test:1A/c8vPQJQiL2
yourname:UtecEDcEa3/L2
```

ปัญหา และวิธีแก้ไข ที่ผู้ดูแลอาจพบ

ครั้งแรกที่สร้าง .htaccess และ .htpasswd ก็ไม่เกิดผล คือสองแฟ้มนี้ไม่ทำงาน ตรวจสอบแล้วพบว่าผู้ดูแลต้องแก้แฟ้ม /etc/httpd/conf/httpd.conf ให้ส่วนของ <Directory "/var/www/html"> ในบรรทัดที่เขียนว่า **AllowOverride None เปลี่ยนเป็น AllowOverride All**
หรือส่วนของ <Directory "/"> ในบรรทัดที่เขียนว่า **AllowOverride None เปลี่ยนเป็น AllowOverride All** ถ้าท่านใช้ public_html

http://www.isinthai.com/lock/index.php

:: ใช้แสดงรหัสที่ผู้ใช้กำหนดขึ้น และนำไปเพิ่มในแฟ้ม .htpasswd ของ directory ที่ต้องการ lock

```
<form action=index.php method=get>
User: <input name=u value=yourname><br>
Password: <input name=p value=yourpassword><br>
<input type=submit value=generate_password>
</form>
This line for .htpasswd<br><font face=fixedsys>
<?
$x = "htpasswd -nb ". $_GET['u'] . " " . $_GET['p'];
echo `$x`;
?>
<hr>
Detail of .htaccess and .htpasswd at<br>
http://www.thaiall.com/cgi/htpasswd.pl
```

Username: yourname

Password: yourpassword

Create password by www.isinthai.com/lock/index.php

เปิดบริการ SSI (Server Side Include)

: บริการนี้ทำให้การเขียน CGI มีสีสรรขึ้นอีกมาก และเพิ่มลูกเล่นให้กับเว็บได้อีกเพียบ

SSI คือการทำให้สามารถเรียก CGI เช่น perl เข้าไปประมวลผลในเว็บ htm โดยทำการประมวลผล แล้วส่งค่าเข้าคืนให้กับผู้เรียกเว็บ การทำงานลักษณะนี้ จะเป็นการ run program ที่ server แล้วส่งผลให้กับผู้ร้องขอเช่นตัวอย่างข้างล่างนี้
ผลของการเปิดเว็บ test.htm จะแสดงตัวอักษร x บนจอภาพ ซึ่งเกิดจากบริการ ssi นั่นเอง แต่ถ้า server ไม่บริการ ssi บรรทัดคำสั่งก็จะแสดงผลอย่างนั้น แต่จะไม่เห็นผลอะไรบนจอภาพเลย เนื่องจากคำสั่งดังกล่างไม่ได้ถูกประมวลผล ตามหน้าที่ของ ssi
ถ้า SSI work นะครับ เวลาเปิด test.htm จะเห็น x ตัวเดียว เรียกว่า ssi สมบูรณ์ หรือเปิดเว็บ pro.pl แล้วต้องเห็น x ตัวเดียวเช่นกัน แต่ถ้าเปิดแล้วเห็น source code แสดงว่าไม่มีการประมวลผล .pl นั้น

สมมุติให้ test.htm เขียนดังข้างล่างนี้

```
<body>
<!--#exec cgi="pro.pl"-->
</body>
```

สมมุติให้ pro.pl เขียนดังข้างล่างนี้

```
#!/usr/bin/perl
print "Content-type:text/html\n\n";
print "x";
```

การทำให้ Linux (RH 8.0)ให้บริการ SSI
บริการนี้มีอยู่แล้วไม่ต้องลงโปรแกรมเพิ่ม เพียงแต่แก้ไขข้อกำหนดในแฟ้ม /etc/httpd/conf/httpd.conf เท่านั้น โดยผมได้ดูตัวอย่างพร้อมคำอธิบายจาก http://www.c2.net/support/sh3/admin_guide/chapter7.fm.html ซึ่ง Search เจอจาก redhat.com

```
# <Directory "/var/www/html"> ของเดิม
# Options Indexes FollowSymLinks ของเดิม
<Directory "/home/httpd/html">
Options All

# AddHandler cgi-script .cgi ของเดิม
AddHandler cgi-script .cgi .pl
```

```
# AddType text/html .shtml ของเดิม
# AddHandler server-parsed .shtml ของเดิม
AddType text/html .shtml .htm .html
AddHandler server-parsed .shtml .htm .html
```

จากการ set up ครั้งนี้ทำให้การประมวลผล Perl ที่ต้อง Run จากห้อง cgi-bin เช่น http://www.isinthai.com/cgi-bin/thaiall/test.pl มาเป็น **http://www.isinthai.com/thaiall/test.pl** ทำให้สะดวกขึ้นมาก และที่ผมพบวิธีการ setup SSI ในครั้งนี้ต้องยกความดีความชอบให้ Redhat.com เพราะเขาเขียนอธิบายไว้พอเข้าใจ รู้สึกว่าเข้าที่นี่แล้วหาอะไร ก็เจอไปหมดครับ

การติดตั้ง Radius

: เพื่อทำเครื่อง Radius server รับบริการ Connect Internet ทางโทรศัพท์ผ่าน External modem

โปรแกรมที่ใช้ install คือ radius-1.16.tar.GZ 27804 Byte

ขั้นตอนการลงโปรแกรม

```
su
tar xvfz radius-1.16.tar.GZ
cd radius-1.16
cd src
make
```

จะเกิด error ว่า

```
radiusd.o: In function `unix_pass':
radiusd.o(.text+0x1c77): undefined reference to `crypt'
collect2: ld returned 1 exit status
make: *** [radiusd] Error 1
```

จะพบว่า make ไม่ผ่านให้
ให้แก้แฟ้ม Makefile ด้วยคำสั่ง pico Makefile
แล้วแก้บรรทัดหนึ่งใน Makefile
จาก **LIBS=**
เป็น **LIBS= -lcrypt**

```
make
cd ../raddb
pico /etc/services
radius          1645/udp        radiusd
radacct         1646/udp
#radius         1812/tcp       # Radius
#radius         1812/udp        # Radius
#radacct        1813/tcp       # Radius Accounting
#radacct        1813/udp        # Radius Accounting
umask 22
mkdir /usr/adm
mkdir /etc/raddb /usr/adm/radacct
chmod 700 /etc/raddb /usr/adm/radacct
cp * /etc/raddb
cp ../src/radiusd /etc
cd /etc/raddb
cp clients.example clients
cp users.example users
```

เพิ่มคำว่า /etc/radiusd ในแฟ้ม /etc/rc.d/rc.local
เพื่อให้ทุกครั้งที่เปิดเครื่องจะสั่ง run radiusd ขึ้นมา
ให้แก้แฟ้ม users โดยลบ user อื่นออกให้หมด เพื่อต่อไปจะถาม user จาก /etc/passwd
ให้แฟ้ม /etc/raddb/users เหลือเฉพาะส่วนข้างล่างนี้

ให้แก้แฟ้ม /etc/raddb/users ให้เป็นไปดังข้างล่างนี้จะรับระบบโทรศัพท์ได้

```
DEFAULT Password = "UNIX"
        User-Service-Type = Login-User,
        Framed-Protocol = PPP,
        Framed-Netmask = 255.255.255.0,
        Framed-Routing = Broadcast-Listen,
        Framed-Compression = Van-Jacobsen-TCP-IP,
        Framed-MTU = 1500
```

แฟ้ม /etc/raddb/users สามารถเขียนได้อีกรูปแบบเพื่อบริการ Modem
ที่เข้ามาสอบถาม user แต่ตัว modem ไม่ได้ติดอยู่กับตัวเครื่อง

```
yonokadmin    Password = "123"
              User-Service-Type = Shell-User,
              Login-Service = Telnet,
yonok                 Password = "456"
              User-Service-Type = Shell-User,
              Login-Service = Telnet,
student1      Password = "789"
            User-Service-Type = Login-User,
            Framed-Protocol = PPP,
            Framed-Address = 255.255.255.254,
            Framed-Netmask = 255.255.255.255,
            Framed-Routing = None,
            Framed-Filter-Id = "std.ppp.in",
            Framed-MTU = 1500,
student2      Password = "17890"
            User-Service-Type = Login-User,
            Framed-Protocol = PPP,
            Framed-Address = 255.255.255.254,
            Framed-Netmask = 255.255.255.255,
            Framed-Routing = None,
            Framed-Filter-Id = "std.ppp.in",
            Framed-MTU = 1500
```

เมื่อต้องการเก็บข้อมูลการ login เข้ามาใช้บริการ
ต้องสร้าง user ใหม่ด้วย useradd radius จะสร้างห้อง /home/radius ขึ้นมาให้ ดังข้างล่างนี้ก่อน

```
su
useradd radius
cd /home/radius
mkdir backup
```

สร้าง **runacct** เก็บในห้อง /home/radius
เขียน shell script สำหรับเก็บผลการ login ผ่านเข้ามาในระบบ
เมื่อเขียนเสร็จแล้วให้ใช้คำสั่ง chmod 700 เพื่อให้เป็นโปรแกรมประมวลผล
(ตอนแรกผมก็ไม่รู้ว่า detail นั้นอยู่ที่ไหน เจอเพราะใช้ **find / -name detail** ครับ)

```
#!/bin/sh
cp /usr/adm/radacct/door.yonok.ac.th/detail /home/radius
/bin/date +%d > /tmp/date
/bin/date +%m > /tmp/month
/bin/date +%y > /tmp/year
DATE=`cat /tmp/date`
MONTH=`cat /tmp/month`
YEAR=`cat /tmp/year`
TODAY="$DATE$MONTH$YEAR"
cd /home/radius
cp detail backup
mv detail $TODAY
cd /tmp
rm date month year
rm /usr/adm/radacct/door.yonok.ac.th/detail
```

ห้อง /etc/cron.daily
ให้เพิ่มแฟ้มอีก 1 แฟ้มในห้อง /etc/cron.daily โดยมีขั้นตอนดังนี้
su
pico radiusprocess
พิมพ์คำนี้ลงไป /home/radius/runacct แล้ว ctrl-x ออกมาเลย
chmod 755 radiusprocess

สรุปในเรื่องของ Radius ดังนี้

1. แฟ้ม /etc/rc.d/rc.loal อาจต้องเพิ่มไป 2 บรรทัด
2. เพราะแฟ้มนี้ทำหน้าที่เสมือน autoexec.bat ของ dos และคำสั่ง 2 บรรทัดนี้อาจไม่จำเป็นก็ได้ แล้วแต่กรณี
3. /etc/radiusd
4. /sbin/ifconfig eth0:1 202.29.78.15
5.
6. ห้อง /home/radius มีแฟ้มชื่อ runacct ซึ่งเป็น script สำหรับเก็บข้อมูลการ login ไว้ทำสถิติ
7.
8. ห้อง /etc/raddb มีแฟ้มชื่อ users ซึ่งเก็บ account สำหรับ connect เข้ามาทั้งหมด
9.
10. ห้อง /etc/cron.daily มีแฟ้มชื่อ radiusprocess เพื่อสั่งให้ประมวลผลแฟ้ม /home/radius/runacct ทุกวัน
11.
12. แก้แฟ้ม /etc/raddb/clients ให้มีคำว่า 202.29.78.254 YournameRadiuS แทนคำว่า postmaster1 testing123
13. จึงจะรับ connection จากชุด Router Modem แต่ถ้าเป็นการ Connect Modem ผ่าน Com port แฟ้มนี้ไม่แก้อะไรก็ใช้ได้
14.
15. สำหรับ crond ต้องเปิดด้วย ใช้ ntsysv ดูว่า crond ถูกปิดหรือไม่ ถ้าไม่เปิดก็เก็บประวัติการเข้าใช้ไม่ได้
16.

ติดตั้ง Modem สำหรับให้บริการเรียก

เข้ามา

: Radius server คือการทำให้เครื่องให้บริการในการสอบถาม user แต่การติดตั้ง Modem เข้าไปก็เป็นอีกเรื่องหนึ่ง

วิธีการติดตั้ง Modem แบบ x window
http://www.thailinux.com/1999/03/14/topic1.html
สำหรับเรื่อง Modem ตอนนี้ผมยังไม่ได้ทำ เพราะหาเครื่องทดลองยังไม่ได้ แต่มอบหมายให้สุวิทย์ไปดูอยู่ครับ
การติดตั้ง Modem ที่ง่ายที่สุดคือใช้ Modem tool โดยการ **startx** แต่ถ้าจะทำแบบ text mode ต้องอ่านที่ http://www.thailinux.com/1999/03/21/topic1.html โดยติดตั้งที่ COM1 ทำ symbolic link ใน directory /dev จาก ttyS0 เป็น modem หรือถ้าติดตั้งบน COM2 ก็ ttyS1 แล้วก็ไล่เลขไปเรื่อย ๆ ถ้าคุณมี serial port มากกว่า 2 (ขอย้ำ วิธีที่ง่ายที่สุดคือ startx แล้วเรียก modemtool)

การต่อ modem โทรเข้า isp แบบ text mode
#ls -l /dev/modem ตรวจสอบการเชื่อมต่อ modem
ถ้าไม่ได้ต่อ แต่เอาโมเด็มเสียบเข้าเครื่องที่หลัง ให้สร้างการเชื่อมต่อใหม่
#ln -sf /dev/cua0 /dev/modem สำหรับต่อ modem จาก com1
#ln -sf /dev/cua1 /dev/modem สำหรับต่อ modem จาก com2

สร้าง Script **testmodem** เชื่อมต่อ 13 บรรทัดข้างล่างนี้

```
#!/bin/bash
TELEPHONE=188,125      # The telephone number for the
connection
ACCOUNT=george         # The account name for logon (as in
'George Burns')
PASSWORD=gracie        # The password for this account (and
'Gracie Allen')
LOCAL_IP=0.0.0.0       # Local IP address if known. Dynamic =
0.0.0.0
REMOTE_IP=0.0.0.0      # Remote IP address if desired.
Normally 0.0.0.0
NETMASK=255.255.255.0  # The proper netmask if needed
export TELEPHONE ACCOUNT PASSWORD
DIALER_SCRIPT=/etc/ppp/ppp-on-dialer
exec /usr/sbin/pppd debug lock modem crtscts /dev/ttyS1 115200 \
asyncmap 20A0000 escape FF kdebug 0
$LOCAL_IP:$REMOTE_IP \
noipdefault netmask $NETMASK defaultroute connect
$DIALER_SCRIPT
# /usr/sbin/pppd debug lock /dev/modem 115200 defaultroute
```

จากนั้นก็ **chmod 700 testmodem** เพื่อให้โปรแกรมนี้ run ได้

คำสั่งที่สำหรับ disconnect
cp /usr/doc/ppp-2.3.11/scripts/ppp-off /root/ppp-off
chmod 700 /root/ppp-off

เพิ่มบรรทัดข้างล่างนี้เข้าไปในแฟ้ม /etc/mgetty+sendfax/login.conf

```
*       -       @       /usr/sbin/pppd auth -chap +pap login modem
crtscts lock
```

SMTP สำหรับ outgoing ของ Outlook ..

: Sendmail Transfer protocol ทำให้ส่ง e-mail ผ่าน outlook หรือโปรแกรมอื่น ๆ ในลักษณะเดียวกันได้

บริการนี้ทำให้ส่ง e-mail ผ่านโปรแกรม outlook ได้ การเปิดบริการ smtp มีขั้นตอนหลายอย่าง ตั้งแต่การเปิด port และเปิด relay ให้กับเครื่องในเครือข่าย ถ้าไม่เปิด relay ให้ก็หมดสิทธิ์ใช้ เพราะ relay จะ denied การให้บริการ SMTP เพราะ SMTP เหมาะกับการเปิดบริการให้กับสมาชิกเท่านั้น
:: อ่านเพิ่มเติมได้ที่ http://thaicert.nectec.or.th/paper/unix_linux/sendmail.php หรือ http://www.redhat.com/support/resources/faqs/RH-sendmail-FAQ/book1.html

1. เข้า **setup** เลือก system services แล้วเลือกเปิด sendmail
   ผลการเปิด sendmail จะทำให้ port 25 ถูกเปิด
   ลองใช้คำสั่ง netstat -a จะแสดงรายชื่อ port ที่เปิดให้บริการ
   ถ้าไม่มีตัวเลือก sendmail ก็ต้องหาแผ่น CD มาติดตั้งเพิ่มด้วยการใช้คำสั่ง rpm -i sendmail
2. แก้แฟ้ม **/etc/mail/sendmail.mc** (เพิ่มบริการตรวจสอบ Blacklist)
   เดิม DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')
   ใหม่
   dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')
   dnl changed FEATURE(dnsbl, `rbl.maps.vix.com', `Open spam relay - see http://maps.vix.com/')dnl
   dnl changed FEATURE(dnsbl, `blackholes.mail-abuse.org', `Rejected - see http://www.mail-abuse.or$
   dnl changed FEATURE(dnsbl, `dialups.mail-abuse.org', `Dialup - see http://www.mail-abuse.org/dul$
   dnl changed FEATURE(dnsbl, `relays.mail-abuse.org', `Open spam relay - see http://work-rss.mail-$
   dnl changed FEATURE(dnsbl, `inputs.orbz.org', `Open spam relay - see http://orbz.org/')dnl
   dnl changed FEATURE(dnsbl, `outputs.orbz.org', `Open spam relay - see http://orbz.org/')dnl
   FEATURE(dnsbl, `orbs.dorkslayers.com', `Open spam relay - see http://dorkslayers.com/')dnl
   FEATURE(dnsbl, `dev.null.dk', `Open spam relay - see http://null.dk/')dnl
   FEATURE(dnsbl, `bl.spamcop.net', `Open spam relay - see http://spamcop.net/')dnl
   FEATURE(dnsbl, `relays.osirusoft.com', `Open spam relay - see http://osirusoft.com/')dnl
   FEATURE(dnsbl, `relays.visi.com', `Open spam relay - see http://visi.com/')dnl
   FEATURE(dnsbl, `list.dsbl.org', `Open spam relay - see http://dsbl.org/')dnl
   FEATURE(dnsbl, `relays.ordb.org', `Open spam relay - see http://ordb.org/')dnl
   FEATURE(dnsbl, `proxies.relays.monkeys.com', `Open spam relay')dnl
   FEATURE(dnsbl, `dnsbl.sorbs.net', `Open spam relay')dnl
   FEATURE(dnsbl, `dynablock.easynet.nl', `Open spam relay')dnl
   FEATURE(`delay_checks')dnl
   dnl FEATURE(`relay_based_on_MX')dnl
   MAILER(smtp)dnl
   MAILER(procmail)dnl
   Cwlocalhost.localdomain
   Cwmail.yonok.ac.th
   Cw202.29.78.1
   + การเพิ่มบรรทัดข้างบนนี้ท่านต้องแน่ใจว่า server ของท่านไม่อยู่ใน black list มิเช่นนั้นจะไม่ได้รับ e-mail เข้ามาเลย
   + ถ้าเครือข่ายต่างประเทศล่ม แล้วท่านยังใช้บริการ black list ท่านจะไม่

สามารถรับจดหมายใหม่ จากเครื่อข่ายในไทย เพราะระบบกรอง mail ล้มเหลว

3. พบว่า config ใน sendmail.mc ผิด เรื่อง local_procmail ต้องแก้ให้ถูก ถ้าไม่ถูก .procmailrc ใน home ก็ไม่ทำงาน .. เท่านั้นเอง
4. หลักการนี้ยังมีปัญหา อย่างพึ่งทำอะไรนะครับ ผมต้องค้นข้อมูลอีกที เพราะใช้แล้วระบบส่ง mail ไม่ออก
5. เดิม FEATURE(local_procmail,`',`procmail -t -Y -a $h -d $u')dnl
6. ใหม่ FEATURE(`local_procmail',`procmail -t -Y -a $h -d $u')dnl
7. แก้แฟ้ม **/etc/mail/access** เพื่อเปิด relay
8. localhost.localdomain RELAY
9. localhost RELAY
10. 202.29.78 RELAY
11. 127.0.0.1 RELAY

    10 550 No service

12. เคยใช้บรรทัดนี้ แต่ใน RH9.0 ไม่ได้ลง SQL จึงใช้คำสั่งนี้ไม่ได้ # update /etc/mail/*.db
13. # cd /etc/mail
14. # make
15. # m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
16. # /etc/init.d/sendmail restart
17. # /sbin/chkconfig --level 3 sendmail on

วิธีหยุด spam หรือ junk แบบ procmail ที่
http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/ref-guide/s1-email-procmail.html

วิธี copy passwd,shadow,group host

: การย้ายระบบ user จากเครื่องหนึ่งไปอีกเครื่องหนึ่ง

ขั้นตอนการ copy passwd,shadow,group

ขั้นตอนที่ 1 : เตรียมพร้อม และทำความเข้าใจ

1. ใจเย็น ๆ ดูว่านอกจาก 3 แฟ้มดังกล่าวแล้ว ท่านจะคัดลอกอย่างอื่นอีก หรือไม่ เช่น mail ใน inbox ซึ่งอยู่ในห้อง /var/spool/mail หรือ ข้อมูลใน home directory ของทุกคน ถ้าทำก็จะยุ่งหละครับ ถ้าไม่อยากยุ่งยากใช้ ghost copy harddisk **ตามหัวข้อ 9.96** ดีกว่าครับ 20 นาทีก็เสร็จ และขั้นตอนก็ไม่มีอะไรมาก แค่ถอดเครื่อง เสียบ harddisk ให้ถูก port แล้วก็ใช้โปรแกรม ghost ก็จะได้ harddisk 2 ตัวที่เหมือนกัน แต่ถ้าเป็น Redhat 8.0 ขึ้นไป การใช้ ghost ที่ไม่ได้ซื้อ จะไม่สามารถ copy ได้
2. เหตุที่ต้อง copy **/etc/passwd, /etc/shadow, /etc/group** ใน case ของผมคือ server ตัวเก่ามีปัญหาสารพัด ลง server ตัวใหม่สมบูรณ์ดีแล้ว และที่หนักก็คือ ระบบเดิมเป็น scsi ใน sun ระบบใหม่เป็น linux เสียดาย account ถ้าทำใหม่ก็ต้องใช้เวลา จึงต้อง copy account ทั้งหมดมา

ขั้นตอนที่ 2 : เริ่ม copy และ backup

3. ให้ใช้โปรแกรม ftp ดี ๆ จะได้สะดวกเช่น **ws_ftp หรือ cute_ftp** ย้ายข้อมูล หรือใช้ ftp จากเครื่องใหม่ติดต่อเข้าเครื่องเก่าก็ได้ สะดวกดี แต่ต้อง backup ของเดิมในเครื่องใหม่ด้วย
4. เข้าไป copy ข้อมูลด้วย root ไปเก็บใน home ของ user demo และเปลี่ยน permission จะได้ copy ออกมาได้ เหตุที่ต้องใช้ demo เพราะแฟ้มที่กำลังจะ copy ส่วนใหญ่เป็นความลับ คนที่เข้าได้คือ root เท่านั้น แต่จะใช้ user root เปิด ftp ก็ไม่ได้ จึงต้องคัดลอกไปไว้ใน home ของ demo แล้วเปลี่ยน permission จะได้ คัดลอกออกมาได้

5. ส่งข้อมูลทั้งหมดเข้าไปใน server ตัวใหม่ โดย get แบบ binary
6. ให้ copy passwd,shadow,group เก็บไว้อีกที่หนึ่ง เพราะถ้าส่งเข้าไปทับแล้วไม่ work จะมีปัญหาซะเปล่า เมื่อ copy เข้าไปแล้วก็อย่างพึ่ง reboot ให้ลองใช้ user ที่ copy มา connect เข้าไปเป็น root ถ้าใช้ได้ก็ถือว่า copy สำเร็จ
7. copy แฟ้มทั้งหมดในห้อง **/var/spool/mail** ซึ่งเป็นห้องเก็บ inbox ของทุกคน
8. copy แฟ้มทั้งหมดในห้อง **/var/www/html** ซึ่งเป็นห้องเก็บ web space ของทุกคน
9. copy แฟ้มทั้งหมดในห้อง **/home** ซึ่งเป็นห้องเก็บข้อมูลต่าง ๆ ของทุกคน (อาจสร้างให้ใหม่ได้)
   ขั้นตอนที่ 4 : แก้ permission และสร้าง home
10. สร้างรายชื่อสมาชิกทุกคนให้ใช้คำสั่ง **cut /etc/passwd --fields=1 --delimiter=: >listall** จะได้แฟ้มชื่อ listall ซึ่งมี username ของทุกคน
11. ใช้ pico listall เข้าไปลบรายชื่อที่ไม่คิดจะสร้าง home เช่นรายชื่อของผู้ใช้ที่ระบบสร้างให้ ให้ท่านลบทิ้งซะ
12. เนื่องจาก mail ใน /var/spool/mail ที่คัดลอกมามี owner และ permission ไม่ถูกต้อง และ home แต่ละคนก็ยังไม่มี จึงใช้ shell script ด้านล่าง อย่าลืมเอา # ออกตามสมควร

```
13.  #!/bin/sh
14.  # exit 0
15.  # chmod 700 crthome
16.  # shell>crthome <listall
17.  read getu
18.  while [ $getu. != '.' ]
19.  do
20.    echo $getu
21.    ## change mail owner
22.    chown $getu:mail /var/spool/mail/$getu
23.    chmod 660 /var/spool/mail/$getu
24.
25.    ## create home
26.    # mkdir /home/$getu
27.    # chown $getu:users /home/$getu
28.    # mkdir /home/$getu/public_html
29.    # chown $getu:users /home/$getu/public_html
30.    # chmod 711 /home/$getu
31.    # chmod 755 /home/$getu/public_html
32.    read getu
33.  done
```

วิธี copy server หรือ host(Backup)

: เนื่องจากผมเป็นมือใหม่อยู่มาก จึงลอง backup ระบบไว้หลายวิธี ทั้งวิธี copy ใน harddisk ตัวเดียว หรือต่าง harddisk

ข้อมูลเบื้องต้นสำหรับทำความเข้าใจในปัญหาการ backup หรือ copy server

1. Harddisk ที่มีอยู่ ไม่มีขนาดที่เท่ากัน ทำให้การคัดลอก หรือแบ่ง partition ให้เท่ากันมีปัญหานิดหน่อย
2. Harddisk ส่วนใหญ่ที่มีเป็น bad sector บางตัว backup เสร็จแล้ว เมื่อนำมาใช้ก็ใช้ไม่ได้
3. คอมพิวเตอร์ที่มีอยู่มีปัญหาเช่นมองเห็น harddisk ขนาดคงที่ ไม่ว่าจะใส่ขนาดเท่าใดก็มองเห็นเพียง 8 Gb เป็นต้น

สรุปล่าสุดเมื่อ 3 มีนาคม 2546

เนื่องจากพยายามหา Norton ghost ที่มีความสามารถ copy harddisk ที่มีขนาดแตกต่างกัน มาคัดลอก RH8.0 แต่จากการหามาและทดสอบ ปรากฏว่าไม่สำเร็จ เพราะคัดลอก

แล้วผลคือแจ้งว่า completely แต่นำไปใช้งานไม่ได้ ทำให้ต้องหยุดการศึกษา Norton ghost สำหรับ RH8.0 ไว้เพียงเท่านี้
วิธี Backup ล่าสุด คือ หา Harddisk ที่มีลักษณะคล้ายกัน แม้ขนาดไม่เท่ากันก็ได้ แต่ตัวลูกต้องใหญ่กว่าหรือเท่ากับตัวแม่ โดยใช้ **#fdisk /dev/hda และ #fdisk /dev/hdc** ตรวจสอบ แล้วคัดลอกด้วยคำสั่ง dd จาก harddisk ที่มีขนาดเล็กกว่า ไป harddisk ที่มีขนาดใหญ่กว่า พบว่าไม่มีปัญหาใด ๆ คำสั่งที่ใช้คือ **#dd if=/dev/hda of=/dev/hdc** หรือ **#dd if=/dev/hda2 of=/dev/hdb2**

วิธีที่ 1 : NortonGhost :: โปรแกรมสำหรับคัดลอก harddisk ได้สมบูรณ์มาก แต่ล่าสุดทดสอบกับ RH8.0 ไม่สำเร็จ
หลังถูก hacker เข้ามาป่วนระบบ ทำให้ต้องหาโปรแกรมมา Backup server เก็บไว้ และโปรแกรมที่หามาได้ก็คือ NortonGhost เพื่อ copy harddisk โดยคุณประเสริฐ ประสารยา [prasert@cat.net.th] ซึ่งเป็นทีมงานของ isinthai.com ได้ช่วยหา NortonGhost2002 มา clone HD Linux RH7.2 และใช้งานได้เรื่อยมา
ในเดือน มกราคม 2545 ทีมงานตัดสินใจใช้ Redhat 8.0 แต่ทั้ง NortonGhost 2002 และ 2003 ต่างก็ใช้คัดลอก Redhat 8.0 ไม่ได้ ปัญหาที่เกิดขึ้นไม่แน่ใจว่าเกิดจากอะไร และเกิดในหลายรูปแบบ เช่น ไม่สามารถ Boot ได้ หรือเห็นเฉพาะคำว่า **LI** ตอน boot แล้วก็ hang ไปเฉย ๆ หรือ copy partition มาไม่หมด .. จึงตัดสินใจศึกษาการใช้คำสั่ง dd และ cp เพื่อคัดลอก harddisk อย่างจริงจังอีกครั้ง

วิธีที่ 2 : tar.gz :: โปรแกรมบีบอัดแฟ้ม หรือ folder ซึ่งนิยมใช้กันมาก (ทีมงานไม่ได้ทดสอบหลักการนี้อย่างจริงจัง)
วิธีนี้สามารถ copy ทั้ง partiton เก็บเป็น file เดียว หากมีปัญหาก็คลายแฟ้มนี้เท่านั้น
#tar zcf total.tar.gz / :: เพื่อบีบอัดทั้ง root เป็นแฟ้ม total.tar.gz
#tar zcf total.tar.gz /dev/hda :: เพื่อบีบอัดทั้ง harddisk เป็นแฟ้ม total.tar.gz
#tar zxf total.tar.gz :: คลายข้อมูลใน total.tar.gz ไว้ในห้องปัจจุบัน

วิธีที่ 3 : cp :: โปรแกรมคัดลอกที่ใช้คัดลอกข้อมูลระหว่าง harddisk หรือ partiton ได้ (ทีมงานไม่ได้ทดสอบหลักการนี้อย่างจริงจัง)
ตัวอย่างการใช้ cp คัดลอกทั้ง partition เก็บเข้า partition ใหม่ใน hd เดิม
เมื่อต้องการดูว่าในเครื่องมี partition อะไรแบ่งไว้บ้างด้วย **fdisk -l หรือ df -a** จะเห็นขนาดของแต่ละ partitions และคำสั่ง **mount หรือ cat /proc/mounts** ถูกใช้เพื่อดูรายการแฟ้มที่ถูก mount ไว้
#mkfs -t ext3 /dev/hda3 3076447
:: ใช้สำหรับจัดรูปแบบ ของ partitions /dev/hda3 ตามขนาดจริง ซึ่งเห็นใน cat /proc/partitions
#mkdir /rest :: สร้างห้องชื่อ rest ในห้อง /
#mkswap /dev/hda7 :: เพื่อกำหนดให้ /dev/hda7 เป็น swap partition
#mount -t ext3 /dev/hda3 /rest :: ต่อไป /rest ก็คือ /dev/hda3 ซึ่งมีขนาด 3076447
#df -a :: แสดงรายชื่อ และขนาดที่ mount สำเร็จ
#cp -a /dev/hda2 /dev/hda3 :: คัดลอกทั้งหมดใน /dev/hda2 ไป /dev/hda3

วิธีที่ 4 : dd :: โปรแกรมคัดลอกทั้ง partition
ตัวอย่างการใช้ dd คัดลอกทั้ง partition หรือ harddisk ไปยัง partition หรือ harddisk ใหม่
ล่าสุดผมใช้วิธีนี้ backup server หรือ copy harddisk นั่นเอง โดยพื้นฐานแล้ว คำสั่งนี้เหมาะกับ harddisk ที่มีขนาดเท่ากัน แต่ผมไม่มี harddisk ที่เท่ากัน แต่ใช้ตัวที่มีลักษณะต่าง ๆ ใกล้เคียงกัน โดยเฉพาะตัวลูกต้องใหญ่กว่า หรือเท่ากับตัวแม่
#dd if=/dev/hda of=/dev/hdc :: คัดลอก harddisk ทั้งลูกจากลูก hda ไป hdc
#dd if=/dev/hda1 of=/dev/hdc1 bs=1024k :: คัดลอก harddisk ทั้งใน partition 1 ของลูกหนึ่ง ไป partition 1 ของอีกลูกหนึ่ง

Server ตัวนี้ให้บริการอะไรได้บ้าง

: บริการต่าง ๆ ที่ Redhat 7.2 มีให้ และที่ลงโปรแกรมเพิ่ม

บริการ เพื่อกรณีศึกษา โดยมือสมัครเล่น

1. Linux server : telnet
2. Web server : http, perl v.3, php3, java applet
3. Mail server : pine, pop3, imap, webbased
4. Proxy server : squid
   หัวข้อนี้ยังไม่เรียบร้อย

ขั้นตอนการทำ server ตัวนี้

: เพื่อให้ท่านหรือทีมงาน สามารถ setup server แบบนี้ได้ง่ายขึ้น จึงเขียนขั้นตอนไว้ดังนี้

บริการ เพื่อกรณีศึกษา โดยมือสมัครเล่น

ขอแนะนำว่าถ้ายังไม่รู้อะไรเลย ให้ไปหาหนังสือสำหรับลง Linux มากอดให้อุ่นใจสักเล่มหนึ่ง เพราะเชื่อแน่ว่า ถ้าอ่านวิธีการติดตั้งที่ผมเขียน โดยไม่มีประสบการณ์ linux มาก่อน .. **จะต้องบ่นว่าผมเขียนไม่รู้เรื่อง** เนื่องจากเรื่องเหล่านี้เป็นเรื่องที่เฉพาะ น้อยคนจริง ๆ ที่จะชำนาญ ผมเองก็พยายามศึกษาอยู่ ก็ได้แค่พอเป็นเท่านั้น (แต่นี่ผมก็พยายามเขียนให้ผมเข้าใจง่ายที่สุดแล้วนะครับ)

ขั้นตอนที่ 1 : เตรียมการ

- Backup ข้อมูลที่สำคัญในเครื่องที่คิดจะติดตั้ง linux ความแน่นอนคือความไม่แน่นอน
- ถ้ามีเครื่องใหม่ และลง linux อย่างเดียวก็หาแผ่น linux มาลงได้เลย .. เพราะเสียแล้วไม่เป็นไร
- ถ้ามี windows อยู่ต้องการลงทั้ง 2 ระบบให้ไปหา partition magic มาแบ่ง partition
- แบ่งว่าจะใช้ Windows กี่ GB แต่ linux จะใช้ไม่น้อยกว่า 1 GB โดยปกติ
- นั่งคิดให้ดีกว่าจะลง linux ไปทำไม เช่น ศึกษาเป็น work station หรือ เป็น server เป็นต้น
- ไปหาโปรแกรม linux ซึ่งผมแนะนำว่าเป็น Redhat เพราะมีคนใช้กันมากที่สุดในโลก

ขั้นตอนที่ 2 : ติดตั้ง

- ถ้ามี windows อยู่ให้ใช้ partition magic แบ่ง partition ให้เรียบร้อย
- ใช้แผ่น CD Boot แล้ว Enter เขาก็จะถามติดตั้งเลย ถ้า VGA card เป็นที่ยอมรับของ linux ก็จะได้เห็นจอสวย
- ถ้าไม่มีสนับสนุนก็ต้องเล่น text mode ไปครับ คนที่ผมรู้จักหลายคน หรือแม้แต่เครื่องที่ผมใช้ ยังใช้ text mode เลย
- เมื่อเข้าไปต้องแบ่งอย่างน้อย 2 partition คือ linux partiton และ linux swap
- **Install ตามขั้นตอน** ซึ่งใช้เวลาประมาณ 2 ชั่วโมง (เหมือน windows นั่นหละครับ)
- ถ้าโชคดี หลังติดตั้งเสร็จก็จะขึ้นคำว่า Login: มารอให้ป้อนรหัสเข้าสู่ระบบ
- มีปัญหาการติดตั้งให้ถามที่ http://linux.thai.net เพราะทีมงานไม่ได้ชำนาญในการแก้ปัญหาทุกกรณี (ประสบการณ์น้อยมาก)

ขั้นตอนที่ 3 : ใช้งาน linux เบื้องต้น (Server)

- หัดใช้คำสั่งใน linux ที่ใช้กันบ่อย ๆ ซึ่งผมแนะนำในบทที่ 1 หัดเป็นผู้ใช้
- เมื่อใช้เป็นแล้ว ลอง telnet เข้าไปใช้ server ที่อื่นดูครับ .. สั่งสมประสบการณ์
- สู่บทที่ 2 แต่ต้องทำที่เครื่องตนเองนะครับ เช่น useradd usermod หัดใช้คำสั่งระดับสูงดูครับ
- ซอกซอนเข้าไปดูระบบ และคำสั่งต่าง ๆ ยิ่งใช้เวลามาก ยิ่งซึมซับ .. ผมเองยังไม่มีเวลาเลย
- วิธีการ config ระบบ ดูทุกแฟ้มที่นามสกุล .conf จะเข้าใจการทำงานของ linux มากขึ้น

ขั้นตอนที่ 4 : ใช้ประโยชน์ Server ก่อนจะ upgrade server

- หัดใช้ mail แบบต่าง ๆ ที่ Server ให้บริการ เช่น pop, imap, pine เป็นต้น
- หัดเขียน Shell script เพราะจะทำให้โอกาสหน้า สามารถแก้ปัญหาระบบได้หลายเรื่อง
- หัดเขียนทำเว็บในเครื่องตนเองด้วย html อย่างง่าย

- หัดเขียน CGI เพื่อทำให้เว็บที่พัฒนาขึ้นมา เป็นยอดเว็บ เช่น yahoo, hypermart, pantip เป็นต้น

ขั้นตอนที่ 5 : Install application

- เนื่องจาก server ที่ติดตั้งไป มีบริการที่เป็นมาตรฐาน หากต้องการความสามารถใหม่ ต้องลงโปรแกรมเพิ่ม
- บริการ Webbased mail อย่างง่าย (หัวข้อ 9.71)
- บริการ proxy หรือ cache server (หัวข้อ 9.72)
- บริการ incoming ใน ftp (หัวข้อ 9.73)
- บริการ Apache + php + Mysql (หัวข้อ 9.74)
- บริการ SSI (หัวข้อ 9.75)
- บริการ Radius (หัวข้อ 9.76 เหมือนเปิดบริการเทียบ ISP เลยครับ)
- บริการ Modem (หัวข้อ 9.77 เหมือนเปิดบริการเทียบ ISP เลยครับ)

ขั้นตอนที่ 6 : ความปลอดภัย (Security)

- หลายคนบอกว่า ความปลอดภัยเป็นเรื่องแรก แต่ผมว่า server ยัง up ไม่ขึ้น ความปลอดภัยอย่างพึ่งสนเลยครับ
- การเป็น System Admin ที่ดี ผมว่าต้องเป็น Hacker ที่ดีด้วย ถึงจะไปด้วยกันได้ (ถ้าไม่รู้ว่า server รั่วอย่างไร จะปิดได้ไง)
- อ่านหน่อยครับว่า **ถูก hack อย่างไร** จะได้เป็นบทเรียน (หัวข้อ 9.51)
- อ่านหน่อยครับว่า **ปกป้องตัวเองอย่างไร** จะได้เป็นบทเรียน (หัวข้อ 9.52)
- ป้องกัน hacker มือสมัครเล่นด้วย Restricted shell (หัวข้อ 9.52)
- ปิดบริการด้วย TCP wrapper (หัวข้อ 9.54)

ขั้นตอนที่ 7 : เรื่องเฉพาะที่ควรทราบ

- ทำให้เครื่องเป็น DNS server (ยังไม่ได้เขียนเป็นจริงจัง)
- บริการ Dedicate server (ยังไม่ได้เขียนเป็นจริงจัง)
- ทำให้เครื่องมีหลาย IP ในกรณีที่ server ตัวหนึ่งล่ม จะได้ย้ายได้ใน 1 นาที (หัวข้อ 9.10)
- Backup ระบบ (หัวข้อ 9.96) แต่ยังไม่ update
- ใช้ php เขียนโปรแกรมบริการ mail แข่งกับ hotmail.com (ยังหาเวลาศึกษาไม่ได้)
- เปิด free hosting (กำลังพยายาม เพราะระบบยังไม่แข็งพอสู้กับ hacker มืออาชีพ ก็เปิดไม่ได้)

ขั้นตอนการติดตั้ง เมื่อ RedHat 9.0 (ปรับปรุงล่าสุด :: 13 กุมภาพันธ์ 2547)

1. ติดตั้ง linux พร้อม Config ให้ใช้งานเครือข่ายได้

รับผิดชอบโดย คุณสุวิทย์ คุณประเสริฐ เพราะชำนาญการ install Redhat บ่อยครั้งที่ต้องติดตั้งโปรแกรมเพิ่ม จึงต้องหามาจาก CD และใช้คำสั่ง rpm -i ชื่อแฟ้มใน CD ทั้ง 3 แผ่นมีดังนี้ **แผนที่** 1, **แผนที่** 2, **แผนที่** 3

#/usr/bin/setup

1. แล้วกำหนด IP ด้วยนตัวเลือก network
2. แล้วเปิดบริการด้วยตัวเลือก system services : httpd,imap,imaps,ipop2,ipop3,kudzu,named,network,pop3s,sendmail,sshd,syslog,vsftpd,xinetd,servers,services

หัวข้อ 9.95 :: copy **passwd, shadow, group จาก server ตัวหลัก** มาแทนที่ในเครื่องที่ติดตั้งใหม่

หัวข้อ 9.10 :: **เพิ่ม IP** ใน Server ตัวเดียวด้วย IFCONFIG

หัวข้อ 9.65 :: เปิดบริการ **SAMBA server**

หัวข้อ 9.66 :: เปิดบริการ **DNS server** ให้คอมพิวเตอร์ทั้งหมดในเครือข่าย สามารถใช้ชื่อเว็บไซต์ได้ถูกต้อง มิเช่นนั้นต้องใช้ตัวเลข

หัวข้อ 9.78 :: เปิดบริการ **sendmail หรือ smtp** ให้ผู้ใช้สามารถส่ง e-mail ด้วย outlook ผ่าน server ของเรา

หัวข้อ 9.62 :: แก้ไขแฟ้ม **/etc/httpd/conf/httpd.conf** เพื่อเปิดบริการต่าง ๆ ของ apache webserver

หัวข้อ 9.63 :: เปิดบริการ **FTP server**

หัวข้อ 9.68 :: เปิดบริการ **Web-based mail** ด้วย uebimiau-2.7.2-any.zip
หัวข้อ 9.67 :: เปิดบริการ **Web hosting file manager** ด้วย easyhost_free.zip
หัวข้อ 9.11 :: เปิดบริการ **Virtual hosts**

หัวข้อ 9.76 :: เปิดบริการ **RADIUS server**
หัวข้อ 5.1 :: เปิดบริการ **MYSQL server**
หัวข้อ 9.69 :: เปิดบริการ **DHCP server** แจก Dynamic IP

การบำรุงรักษา และตรวจสอบ

: บริการให้ดีต้องหมั่นบำรุงรักษา ไม่งั้นอาจอยู่ได้ไม่นานเท่าที่ควร

9.99.1 สรุปปัญหา วิธีตรวจสอบ และการแก้ไขเบื้องต้น (เมื่อมีปัญหาเกิดขึ้น)

1. เมื่อเครื่องของผู้ใช้ต่อ internet ไม่ได้ (ตรวจสอบโดยผู้ใช้)
   + ตรวจสอบว่าอะไรใช้ไม่ได้ เช่น http, workgroup, ping หรือ smtp เป็นต้น แล้วหาสาเหตุ

     - http : ถ้าเปิดเว็บใดไม่ได้ ลองเปิดหลาย ๆ เว็บ เพราะบางเว็บอาจ down ชั่วคราว
     - workgroup : Folder sharing ภายในสถาบัน ประกอบด้วยหลายวง หลายระบบปฏิบัติการ บางเครื่องอาจถูกยกเลิกการ share
     - ping : ตรวจด้วยการพิมพ์ ping 202.29.78.254 หรือ 202.29.78.11 เพื่อดูว่าเครื่องท่านเห็นไม่หากไปจากระบบ
     - smtp : ถ้าใช้ smtp.yonok.ac.th ไม่ได้เพราะ server ล่มให้แจ้ง 125 เพราะระบบอาจ hang หรือ over limited
     - winipcfg : คำสั่งนี้ใช้ดูว่า ip ของท่านเบอร์อะไร บางครั้ง ip หาย ท่านสามารถกำหนดได้ด้วยตัวเอง จากเบอร์ที่ติดไว้กับเครื่อง

   + ก่อนแจ้งเจ้าหน้าที่ 125 ท่านควรปฏิบัติดังนี้

     - ให้ reboot เครื่องใหม่ ก่อน reboot ให้ตรวจสอบสายต่าง ๆ ว่าอยู่ในที่ควร หรือไม่ แล้วทดสอบอีกครั้ง
     - ตรวจสอบ HUB และระบบเชื่อมต่อ สำหรับปัญหาที่อาจเกิดจาก hardware ผู้ใช้บางท่านอาจถอดสายไฟของ hub ออก หรือสะดุดจนหลุด

2. เว็บ หรือ e-mail ของโยนก ใช้การไม่ได้ (ตรวจสอบโดยเจ้าหน้าที่ 125)

   # **ping 202.29.78.12** (ตรวจว่าเครื่อง server เปิดบริการในเครือข่ายหรือไม่ โดยทดสอบจากเครื่องลูก)
   # **df** (ตรวจว่า harddisk เต็มหรือไม่ ถ้าเต็มต้องไปลบ e-mail ของบางท่าน)
   # เปิดเว็บ http://www.yonok.ac.th (ตรวจว่า named และ httpd ทำงานปกติหรือไม่ ถ้าไม่ได้ ให้สั่ง reboot)

   24/11/2004

3. ติดต่อ Internet นอกโยนกไม่ได้ (ตรวจสอบโดยเจ้าหน้าที่ 125)

   - ping 202.29.78.254 หรือ ping 202.28.29.42 (ถ้าติดต่อไม่ได้ให้

reboot ถ้ายังไม่ได้ต้องใช้สาย console เข้าไป config ใหม่)
- ตรวจสอบไฟสัญญาณของ Fiber modem หรือ Converter ด้วยการมอง ถ้ามีไฟแดงที่ modem ให้แจ้งคุณภากร (0-5421-7200, 0-9759-0946)
- ตรวจสอบ Router ฝั่งเชียงใหม่ โดย ping 202.28.29.41 ถ้าติดต่อไม่ได้ให้แจ้ง คุณประเสริฐ (0-2248-7749)

4. กรณีเครื่องในห้อง lab1, lab2 หรือ lab3 ใช้ internet ไม่ได้ (ตรวจสอบโดยเจ้าหน้าที่ 125)

   - ตรวจสอบเครื่อง DHCP ว่าเปิดบริการ หรือไม่ ด้วยการ ping 192.168.0.1 หรือ ping 202.29.78.11
   - ตรวจสอบ hub ที่เชื่อมโยงตามจุดต่าง ๆ ปัญหาอาจเกิดจาก hub มีอาการ hang ชั่วคราว

5. กรณี router ของโยนกเสีย (ตรวจสอบโดยเจ้าหน้าที่ 125)

router ที่ใช้อยู่คือ CISCO router 2511 เป็นรุ่นเก่าใช้มาตั้งแต่ปี 1996 ปัจจุบันเสียเป็นบางจังหวะมาแล้ว ประมาณ 4 ครั้ง ครั้งล่าสุดส่งซ่อมที่ร้าน smart service ซึ่งเป็นตัวแทน CISCO ในจังหวัดลำปาง แต่มิได้ซ่อมอย่างแท้จริง เพียงแต่นำไปปัดฝุ่นภายในพร้อมตรวจสอบปัญหาในเบื้องต้น มีค่าใช้จ่าย 450 บาท แล้วนำกลับมาใช้ใหม่
ปัญหาของ router คือ หยุดทำงานกระทันหัน ping เข้าไปไม่ได้ ใช้สาย console ติดต่อเข้าไปไม่ได้ ทางร้านวิเคราะห์ว่า อุปกรณ์สำคัญไม่มีปัญหา แต่มีบางชิ้นที่ไม่ทำงานในขณะเย็น ต้องอุ่มเครื่องให้ร้อน router จึงจะทำงานได้ปกติ เมื่อมีปัญหาให้ปิด และเปิดทิ้งไว้ประมาณครึ่งชั่วโมง หากไฟที่ปุ่ม ok สว่างมาก ก็แสดงว่า router ทำงานได้ปกติ แต่ขณะมีปัญหาไฟนี้จะไม่สว่างมาก แสดงว่าไฟฟ้าเข้าไม่เต็มที่
ช่างแจ้งว่าปัญหานี้ซ่อมได้ แต่ต้องนำแต่ละชิ้นมาตรวจสอบ หากพบชิ้นที่มีปัญหา ก็จะสั่งซื้อจากคลองถมที่กรุงเทพฯ หากพบก็จะนำชิ้นส่วนนั้นมาติดตั้งแทน แต่อาจหาได้ไม่ง่าย เพราะเป็นอุปกรณ์ที่มิได้ใช้กันทั่วไป และส่วนใหญ่ make in U.S.A. หลังจากส่งให้ร้าน 3 วัน จึงรอต่อไปไม่ได้ เพราะร้านก็ไม่แน่ใจว่า ถ้าถอดและซ่อมจริง จะหาอุปกรณ์ที่มีปัญหานั้นพบในเวลากี่วัน

ทางเลือกสำหรับปัญหา router เสีย (CISCO คืออุปกรณ์ที่นิยม และน่าเชื่อถือ ที่สุดในโลก)

1. ไม่ซ่อม แต่แก้ปัญหาด้วยการปิด และเปิดใหม่ บางครั้งใช้เวลา 1 ชั่วโมงกว่าจะเครื่องร้อน (ปัจจุบันเลือกทางนี้)
2. ซื้อ smart net ซึ่งเป็นประกัน หากต่อไปเสีย แล้วส่งเข้าบริษัท CISCO ทางบริษัทจะส่งตัวอื่นให้ใช้แทน ค่าใช้จ่าย 17800 บาทต่อปี
3. ซื้อตัวใหม่ยี่ห้อเดิม ที่มีศักยภาพเทียบเท่า หรือสูงกว่าตัวเดิม มีค่าใช้จ่ายประมาณ 150,000 บาท
4. ซื้อตัวใหม่ยี่ห้อใหม่ ที่มีศักยภาพ และความคงทน ต่ำกว่ายี่ห้อเดิม มีค่าใช้จ่ายประมาณ 50,000 บาท

9.99.2 สิ่งที่ควรกระทำ และเข้าใจ

1. **ps aux** ตรวจสอบว่ามี process แปลก run อยู่บ้างไหม
2. **top** เพื่อดู process ที่กำลังทำงานในปัจจุบัน
3. เข้าห้อง **/var/log** ซึ่งมี log file ขนาดใหญ่ ๆ ทั้งนั้น Clear บ้าง หรือจะเข้าไปดูร่องรอยของผู้ใช้ก็ได้
4. เข้าห้อง **/tmp** ว่ามีแฟ้มอะไรแปลกปลอมเข้ามา ให้ clear ได้
5. ใช้ **last | more** เพื่อดูรายชื่อผู้ใช้ล่าสุด ถ้าอยู่ๆ last เหลือนิดเดียว .. แสดงว่า hacker เข้ามาลบร่องรอย
6. ใน Redhat 8.0 ใช้ **find /bin -size 626188c** เพื่อดูแฟ้มที่มีขนาดเท่ากับ /bin/bash เพราะอาจเป็นประตูหลังของ hacker
7. **find / -cmin -600 | more** แสดงชื่อแฟ้มที่มีการเปลี่ยนแปลงใน 10 ชั่วโมงที่ผ่านมา ในทุก Directory แต่จะออกมามากไปหน่อย ต้องค่อย ๆ ดู หรือตัด / แล้วทำเฉพาะในห้อง

ที่สงสัยก็ได้

8. **cat /var/log/messages |grep login|more** ดูว่ามีคนแปลกหน้า Login หรือพยายามเข้ามาหรือไม่ แต่อาจไม่ได้ผล ถ้า hacker มืออาชีพเขาจะลบแฟ้มนี้ทิ้ง ก่อนออกไป
9. backup harddisk ด้วย **#dd if=/dev/hda1 of=dev/hdc1** เป็นต้น แต่ต้องใช้ fdisk -l ตรวจสอบให้ดีก่อน

9.99.3 อบรมบุคลากรให้ใช้คำสั่งด้านล่างนี้อย่างเข้าใจ เพื่อให้ดูแล server ต่อไปได้

1. ls -alt | more
2. chmod 755 x.htm -Rf
3. chown root:mail noriko -Rf
4. find / -name hello.pl
5. man ls
6. pico x.htm
7. finger bcom302
8. cat x.htm
9. whereis ifconfig
10. echo $PATH
11. PATH=$PATH:/sbin:/usr/sbin
12. /sbin/ifconfig
13. netstat -a
14. /sbin/service --status-all
15. xinetd -d
16. env
17. lynx http://www.yonok.ac.th/main/popup.htm
18. nslookup 202.28.18.65
19. tail --lines=5 /var/log/messages
20. df
21. du
22. ps -aux
23. kill -9 12345
24. last | more
25. cat index.html |grep @
26. top
27. route
28. shutdown -h now
29. reboot
30. runlevel
31. cat /etc/inittab
32. fsck /
33. chown burin:users x.htm
34. chkconfig --list
35. mount /dev/cdrom
36. mkbootdisk --device /dev/fd0 2.4.18-14
37. traceroute www.thaiall.com
38. rpm -i imap-4.7-5.i386.rpm
39. su bcom302
40. crontab -l
41. exit
42. date 04271340
43. hwclock --systohc
44. cp /hd/home/* /home -fr
45. chmod 777 *.* -fR
46. nmap -sT www.yonok.ac.th
47. chkconfig --list
48. more /etc/grub.conf
49. ifconfig [ดูว่าใน server ตัวนี้มี LAN CARD และ IP อะไรบ้าง]
50. service --status-all [ดูสถานะของบริการต่าง ๆ ว่าถูกเปิดหรือ running อยู่หรือไม่]

51. [ ]
52. [ ]
53. [ ]
54. [ ]
55. [ ]