การติดตั้ง Linux Server 3

ที่มาของเอกสารฉบับนี้ :

1. จากการอบรมเชิงปฏิบัติการเพื่อเตรียมความพร้อมตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของสถานศึกษาในสำนักงานคณะกรรมการการอาชีวศึกษา ณ โรงแรมดราก้อน บีช รีสอร์ท จังหวัดชลบุรี
2. จากหนังสือ Linux Server 3 อ.บุญลือ อยู่คง
3. จากการศึกษาค้นคว้าเพิ่มเติมของผู้เขียน และได้ทดลองปฏิบัติจริง

ขอขอบคุณ :

1. คณะวิทยากรที่ให้ความรู้ โดยเฉพาะวิทยากร อ.บุญลือ อยู่คง
2. เพื่อนร่วมงานที่ช่วยจัดทำเอกสารฉบับนี้

คำแนะนำ :

เอกสารฉบับนี้จัดทำขึ้นเพื่อประกอบการติดตั้ง Internet Server สำหรับผู้ที่สนใจและคิดที่จะทำ Internet Server เนื้อหาบางครั้งอาจจะรวบรัดบ้าง หรือค่าบางค่าอาจจะอ้างอิงถึงผู้เขียนเอง เช่น IP address ขอให้ผู้ใช้นำไปปรับให้เข้ากับค่าของผู้ใช้เอง

จริงจริงแล้วผู้เขียนได้เขียนเป็นขั้นตอนเพื่อให้ดูง่ายในการติดตั้ง และทำขึ้นเพื่อใช้งานเองในฐานะที่เป็นผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ของวิทยาลัยการอาชีพขอนแก่น แต่เนื่องจากมีท่านที่สนใจ และจะต้องนำไปทำที่วิทยาลัยฯ ของตนเอง ผู้เขียนจึงได้เผยแพร่ ยังไงก็นำไปประยุกต์ให้เข้ากับเครือข่ายของตนเองก็แล้วกันนะครับ

หวังว่าเอกสารฉบับนี้คงจะเป็นประโยชน์ต่อทุกท่านบ้างไม่มากก็น้อย ขอให้ประสบความสำเร็จในการติดตั้ง Internet Server นะครับ

วีรศักดิ์ ขจรบุญ
ครูชำนาญการ

การติดตั้ง Linux Server 3

OS - เป็น Fedora core 6

ขั้นตอนการติดตั้ง Linux Server

1. ใส่แผ่น CD Linux Server 3 ใน cd drive
2. Boot เครื่อง
3. เมื่อขึ้นหน้าจอให้พิมพ์ text <enter>
4. ตรวจสอบแผ่น CD ให้เลือก Skip
5. welcome to Linux Server 3 ให้กด OK
6. เลือกภาษา English กด OK
7. เลือกแป้นพิมพ์ US กด OK
8. สร้าง Partition

   เลือก Create Custom layout เพื่อสร้าง partition ด้วยตนเอง
9. ทำการแบ่ง partition

ประกอบด้วย	/	ประมาณ 256 MB
	/boot	ประมาณ 75 MB แต่ไม่ควรเกิน 2 GB ป้องกัน Hacker
	/usr	ประมาณ 1.5 GB สำหรับติดตั้ง package
	/var	ประมาณ 100 MB ใช้เก็บค่า log
	/home	ถ้า user มากควรกำหนดมาก
	/cache	ถ้าทำ proxy server (squid) จะใช้มาก
	/tmp	ประมาณ 250 MB
	<swap>	ขนาดเป็น 2 เท่าของ RAM

10. เลือก Boot Loader

    [*] Use GRUB Boot Loader กด OK
11. Boot Loader Configuration

    กด OK
12. กำหนด GRUB Password

    ไม่ต้องใส่ password กด OK

13. Boot Loader Configuration

เลือก Default Boot

กด OK

14. เลือกตำแหน่งที่อยู่ของ Boot Loader

เลือก Master Boot Record (MBR) กด OK

15. กำหนดค่า Network

[ ] Use dynamic IP Configuration (DHCP)

[*] Enable IPV4 Support

[ ] Enable IPV6 Support

[*] Activate on boot

พิมพ์ address prefix (Netmask)

IPV4 : 61.19.212.xxx / 255.255.255.248

กด OK

16. Gateway และ DNS

Gateway : 61.19.212.41 หรือ 61.19.212.137

Primary DNS : 61.19.254.134

Secondary DNS : 61.19. 254.135

17. ตั้งชื่อ Hostname Logserverkknic.kknic.ac.th

Hostname Domain name

ProxyServerkknic.kknic.ac.th

หรือ Webserverkknic.kknic.ac.th

กด OK

18. Time Zone

[ ] System clock uses UTC เอาเครื่องหมาย * ออก

เลือก Asia / Bangkok

กด OK

19. Root Password

    Password : …….. ใส่ Password ของ root 2 ครั้ง

    Password (Confirm) : …….

    กด OK

20. เลือก Package

    [*] DNS Server : ติดตั้ง Bind

    [*] Web Server : ติดตั้ง httpd

    [*] FTP Server : ติดตั้ง vsftp

    [*] File Server : ติดตั้ง samba

    [*] Mysql Server : ติดตั้ง MySQL

    [*] Mail Server : ติดตั้ง dovecot

21. Dependency check และเริ่มทำการติดตั้ง Installation to begin

    กด OK

22. Formatting

23. Copying File

24. Package Installation

25. Complete

    กด Reboot

26. นำแผ่น CD ออกจาก drive (Eject CD)

27. เมื่อเครื่อง Reboot เข้ามาใหม่ จะพบ Setup Agent

    เลือก Authentication กด Run Tool

28. เมนู Authentication Configuration

    โปรแกรมจะเลือก 3 รายการ [*] Use MD5 Password

    [*] Use Shadow Password

    กด Next [*] Local authorization is sufficient

29. กลับมาหน้าจอ Setup Agent

    กด Exit

30. ปรากฏหน้าจอ Login : …….

31. ไม่ควรต่อสาย LAN เข้ากับ Server ควร Set ระบบความปลอดภัยก่อน

หมายเหตุ Fedora 6
- ได้ตั้งความปลอดภัยไว้ระดับหนึ่ง
- ยังไม่ได้ทำการเปิดบริการใด ๆ
- ไม่ได้กำหนดค่า Configuration ต่าง ๆ

ให้เครื่อง Server พร้อมที่จะใช้งาน

ติดตั้งระบบรักษาความปลอดภัยให้กับ Server

หลังจากติดตั้ง Server เสร็จ จะต้องติดตั้งระบบรักษาความปลอดภัยให้กับ Server (ไม่ควรต่อสาย LAN เข้ากับเครื่อง Server)

การติดตั้งระบบรักษาความปลอดภัย มี 4 วิธี คือ

1. SELinux
2. tcp wrappers
3. secure shell
4. Ports entry

TCP Wrappers

เป็นวิธีการเริ่มต้นที่สามารถกำหนดค่าป้องกันให้ใครที่จะมีสิทธิเข้ามาภายใน Sever ได้บ้าง และใครที่ไม่มีสิทธิเข้าภายใน Server

1. ตรวจสอบว่าติดตั้ง package หรือยัง

   # rpm – q tcp_wrappers

   จะได้ผลลัพธ์ tcp_wrappers-7.6-40.3.fc6

2. แก้ไข Configuration ของ TCP wrappers

   2.1 แก้ไข file hosts.deny

   # vi /etc/hosts.deny

พิมพ์ต่อท้ายไฟล์

ALL: ALL (ปิดบริการทั้งหมดเครื่องอื่นจะเข้ามาใช้ไม่ได้)

ALL: ALL EXCEPT 192.168.X.

vsftpd: ALL

2.2 แก้ไข file hosts.allow

vi /etc/hosts.allow

ALL: 192.168.X.

หรือ

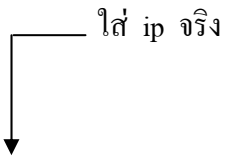
sshd : 192.168.X.

vsftpd : 192.168.X.

sendmail : 127.0.0.1

syslog - ng :

หรือ



sshd : 61.19.212.xx sshd: ALL

vsftpd: 61.19.212.xx vsftpd: ALL

61.19.212. (2 ip)

61.19.212.xx

SELinux

Linux Server 3 ได้ติดตั้ง SELinux เรียบร้อยแล้ว และทำงานทันทีที่ Boot เครื่อง (ค่า Default คือ ปิดทุกอย่างที่มีความเสี่ยงสูง และเปิดอนุญาต (allow) ให้เฉพาะในส่วนที่ไม่มีความเสี่ยง) อาจทำให้บาง Service ไม่สามารถทำงานได้

3. ตรวจสอบว่า Server ได้ติดตั้ง SELinux หรือยัง

rpm – q selinux – policy – targeted

Selinux-policy-targeted-2.4.6-108.fc6

ไฟล์ Configuration คือ /etc/selinux/config

ในการใช้งาน HTTPD Server เมื่อกำหนดให้ลูกข่ายสามารถใช้ home directory สร้าง website ส่วนตัวใน public_html ได้จะต้องไปยกเลิก Configuration

ในส่วน SELINUX = enforcing

แก้เป็น SELINUX = disable * ไม่แนะนำให้ทำ *

4. การ Set ค่า Configuration ของ SELinux

ใช้โปรแกรม seedit แก้ปัญหาเรื่องการแก้ไข policy ของ SELinux ที่ถูกการตรวจสอบจากโปรแกรม audit

```
# mkdir –p /mnt/cdrom /mnt/usbdisk
# mount /dev/cdrom /mnt/cdrom (หรือใช้ usbdisk)
```

4.1 ติดตั้ง audit

```
# rpm –ivh /mnt/cdrom/Fedora/RPMS/audit-1 <tab>
```

4.2 ติดตั้ง checkpolicy

```
# rpm –ivh /mnt/cdrom/Fedora/RPMS/checkpolicy-1 <tab>
```

4.3 ติดตั้ง seedit และ seedit - policy

```
# rpm –ivh /mnt/cdrom/MyBooks/seedit - * <tab>
```

Portsentry

เป็นการป้องกันไม่ให้ผู้บุกรุกทำการ Scan Port ที่เปิดทิ้งไว้ หรือเปิดให้บริการตามปกติ จะต้องทำการติดตั้งโปรแกรมให้ใช้ในการดักหรือป้องกันการ Scan port และบันทึก log File เอาไว้ตรวจสอบได้ โดยใช้โปรแกรม Portsentry

5. ติดตั้ง potsentry

```
# mount /dev/cdrom/ /mnt/cdrom (ถ้า mount อยู่ไม่ต้องเรียกอีก)
# rpm –ivh /mnt/cdrom/MyBooks/portsentry <tab>
```

- ถ้าเป็น Proxy Server ไม่ต้องติดตั้ง

6. ติดตั้ง Linuxconf

```
# rpm –ivh /mnt/cdrom/MyBooks/Linuxconf-1 <tab>
```

7. นำเอาแผ่น cd ออก

```
# eject
```

8. สั่งให้ seedit ทำงาน

```
# seedit-init
```

9. สั่ง Reboot เครื่อง

```
# reboot
```

10. เครื่องจะทำการ boot ตัวเอง 3 รอบ

ในรอบที่ 2 ให้เลือก Do it (ให้รีบทำก่อนหมดเวลาที่ตั้งไว้)

11. เข้าสู่หน้าจอ Login พิมพ์ root และ password

Login :

12. สั่งให้ portsentry ทำงาน

/etc/init.d/portsentry start

13. สั่งให้ portsentry ทำงานทุกครั้งที่ boot ระบบ

chkconfig portsentry on

หรือ # ntsysv

[*] portsentry

Secure Shell (Openssh) **(ไม่ได้ทำ)**

ใช้เพื่อความปลอดภัยในการป้องกันการดักจับ password ระหว่างทาง การทำงานมีลักษณะการตรวจสอบรหัสกุญแจของผู้ที่จะเข้าถึง Server (รหัส 1024 bit) โปรแกรมที่ใช้คือ Openssh-4-3p2-19.fc6

14. แก้ไข Configuration

14.1 Add User ทำหน้าที่แทน root

useradd admin

passwd admin

พิมพ์ password ของ admin 2 ครั้ง

14.2 แก้ไข file sshd_config

vi +39 /etc/ssh/sshd-config

PermitRootLogin no (เอา # ออก เปลี่ยนจาก yes เป็น no)

พิมพ์เพิ่มบรรทัดสุดท้าย

AllowUsers admin

14.3 แก้ไข file SU

vi +6 /etc/pam.d/su

Auth required pam_wheel.so use_uid (เอา # ออก)

14.4 กำหนดให้ admin อยู่ใน whell group

usermod -G10 admin

14.5 สั่ง start SSH (เริ่มทำจากข้อนี้)

/etc/init.d/sshd start

14.6 เมื่อผู้ดูแลระบบต้องการ Remute Login จากที่อื่น ก็สามารถใช้ชื่อ admin แทน root และเมื่อ login เสร็จแล้วให้ใช้คำสั่ง

su

14.7 กำหนดให้ทำงานทุกครั้งที่ boot เครื่อง

chkconfig sshd on

หรือ # ntsysv

[*] sshd

14.8 เปิดอนุญาตที่ไฟล์ hosts.allow

sshd: ALL

Proxy Server ไม่ทำ

⇨ ⇨ (step ที่ 15 – 17 ยังไม่ต้องทำ) ⇦ ⇦ : set number

15. ปรับแต่งค่า configuration ของ portsentry

- บรรทัดที่ 236

vi /etc/portsentry/portsentry.conf

- บรรทัดที่ 35 – 36 เป็นหมายเลข port ที่ป้องกันไม่ให้ถูก scan ทั้ง protocol TCP และ UDP
- บรรทัดที่ 73 – 75 เป็นหมายเลข port ที่ยกเว้นหรืออนุญาตให้ scan ได้ เพราะเป็น port ของการบริการตามปกติของ server เอาเครื่องหมาย # ใส่
- บรรทัดที่ 85 เป็นการบันทึกการ Block ผู้บุกรุกทั้งหมด อยู่ใน file /etc/portsentry/portsentry.history
- บรรทัดที่ 167 จัดการผู้บุกรุก ใช้คำสั่ง route เพื่อทำการ reject IP address ที่บุกรุกทิ้ง

KILL_ROUTE = “/sbin/route add -host $TARGET$ reject”

การยกเลิก IP address ที่ถูก reject

route del -host <ipaddress> reject

- บรรทัดที่ 206 ใช้ IPTABLES ยกเลิก IP ที่บุกรุกเข้ามาด้วย

Policy INPUT DROP

การยกเลิกสั่ง Policy เป็น INPUT ACCEPT

- บรรทัดที่ 299 หรือ 236

229 จะสั่งให้โปรแกรม tcp-wrappers เขียนข้อมูลเพิ่มใน file hosts.deny ว่า ALL: <ip ที่บุกรุก>

KILL_HOSTS_DENY= “ALL: $TARGET$”

* 236 จะเขียนว่า

ALL: <ip address> : DENY

KILL_HOSTS_DENY= “ALL: $TARGET$: DENY”

****** ให้แก้ไขเฉพาะบรรทัดที่ 236 เอาเครื่องหมาย # ออก

16. แก้ไข mode ของ portsentry

chmod 600 /etc/postentry/portsentry.conf

chmod 600 /etc/portsentry/portsentry.ignore

17. สั่งให้โปรแกรมทำงาน

/etc/init.d/portsentry restart

การปรับแต่งหลังการติดตั้ง

1. ทำ Authentication (ทำแล้ว), ขั้นตอนที่ 1-2 ไม่ต้องทำอีก (เรียกคำสั่ง setup authen)

ซึ่งจะปรากฏหลังจากติดตั้งเสร็จและ boot เครื่อง ซึ่งขั้นตอนนี้ต้องทำก่อนติดตั้งระบบรักษาความปลอดภัย SELinux

* หมายเหตุ ไม่ต้องทำอีก

- ที่ Setup Agent เลือก Authentication และกดปุ่ม Run Tool

- ที่รายการ Authentication Configuration

เลือก 2 รายการ [*] Use MD5 Passwords

[*] Use Shadow Passwords

กดปุ่ม Next

- กดแป้น Exit เพื่อออกจากหน้าจอ

2. ติดตั้ง LinuxConf (ทำแล้ว)

```
# mkdir -p    /mnt/cdrom    /mnt/usbdisk
# mount       /dev/cdrom    /mnt/cdrom
# rpm  -ivh   /mnt/cdrom/MyBooks/linuxcont -1  <tab>
# eject
# reboot
```

3. ติดตั้งค่าที่ netconf

Proxy Server ไม่ต้องทำก็ได้

```
# netconf
```

3.1 เมนู Host name and IP network devices

- ที่ Primary name + domain := ใส่ค่าเหมือนกับ Hostname + domain
- ที่ Aliases (opt) ใส่เฉพาะ hostname
- adapter ให้ [x] Enabled

(o) Manual

- IP address
- Netmask (opt)
- Net device eth0
- กดปุ่ม Accept

ถ้ามี LAN Card 2 ใบ ต้องทำใบที่ 2 ด้วย

(•) dhcp

Net device eth1

3.2 เมนู Name Server Specification (DNS)

- ที่ default domain ; ให้ลอกชื่อ Domain จากช่อง search domain 1 (opt)
- IP of name Server 1
- IP of name Server 2

} เอาค่า IP ของ DNS ที่ได้จาก ISP ใส่

- กดปุ่ม Accept

3.3 เมนู Routing and Gateway

- กด Enter จะพบเมนู เลือก Set Defaults
- ที่ Default Gateway : ให้พิมพ์ IP ของ Gateway เช่น 61.19.212.xx
- [ ] Enable routing (ถ้ามี LAN card 1 ใบ ต้องใส่ mark x)
- กด Accept
- กด Dismiss
- กด Quit เพื่อออกจากการติดตั้งค่า
- กด Do it

4. ตรวจสอบระบบ Network

ifconfig หรือ # ifconfig eth0

5. Restart Network ใหม่

/etc/init.d/network restart

หรือ #service network restart