รวมขั้นตอนการติดตั้ง Internet Server

ที่มาของเอกสารฉบับนี้ :

1. จากการอบรมเชิงปฏิบัติการเพื่อเตรียมความพร้อมตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของสถานศึกษาในสำนักงานคณะกรรมการการอาชีวศึกษา ณ โรงแรมดราก้อนบีช 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

ขั้นตอนการติดตั้ง Internet Server

1. ติดตั้ง Linux Server 3.0 และ Security

1.1 ลง Linux Server 3.0 (ตามขั้นตอนจนเสร็จ โดยยังไม่ต้องต่อสาย LAN)

1.2 แก้ไข file hosts.deny

```
# vi     /etc/hosts.deny
   ALL:  61.19.212.xxx  :  DENY          (42, 43, 44, 45, 46, 138,139,140)
```

1.3 แก้ไข file hosts.allow

```
#vi     /etc/hosts.allow
   ALL:  61.19.212.142                   (Authentication Server)
  sshd:    61.19.212.140
  vsftpd:   61.19.212.140
  syslog-ng:  61.19.212.141              (Log Server)
```

1.4 ติดตั้งความปลอดภัย (package) (# rpm -ivh /mnt/cdrom/…….)

```
                    #mkdir  -p  /mnt/cdrom
                    # mount  /dev/cdrom  /mnt/cdrom
- audit             # rpm  -ivh  /mnt/cdrom/Fedora/RPMS/audit-1     <tab>
- checkpolicy       # rpm  -ivh  /mnt/cdrom/Fedora/RPMS/checkpolicy-1     <tab>
- seedit            # rpm  -ivh  /mnt/cdrom/MyBooks/seedit-*
- Linuxconf         # rpm  -ivh  /mnt/cdrom/MyBooks/Linuxconf-1     <tab>
                    # eject
```

1.5 สั่งให้ seedit ทำงาน

```
# seedit-init
```

1.6 สั่ง reboot เครื่อง

reboot (จะ boot เครื่องจำนวน 3 รอบ)

* รอบ 2 ให้เลือก doit

2. ติดตั้ง Web Server

2.1 สั่ง run service httpd ทุกครั้งที่ boot เครื่อง

chkconfig httpd on

2.2 start httpd

/etc/init.d/httpd start

2.3. ติดตั้ง LAN Card ใบที่ 2 (ในกรณีที่เพิ่ม LAN Card ในภายหลัง)

ifconfig

vi /etc/sysconfig/network-scripts/ifcfg-eth1

แก้ไข BOOTPROTO = none (ค่าเดิมเป็น dhcp)

ONBOOT = yes (ค่าเดิมเป็น no)

2.4 restart service network ใหม่

service network restart

ifconfig

2.5 เปิด Firewall

lokkit

Trusted Device	[*] eth0	[*] eht1	
MASQUERADE Device	[ ] eth0	[*] eth1	
Allow incoming	[*] SSH		[*] FTP
	[*] WWW (HTTP)		[*] Mail (SMTP)
	[*] Secure WWW (HTTPS)		

2.6 แก้ไขค่า configuration ของ httpd

vi /etc/httpd/conf/httpd.conf

บรรทัดที่ 250 ServerAdmin administrator@kknic.ac.th

บรรทัดที่ 264 ServerName www.kknic.ac.th : 80 (เอา # ออก)

บรรทัดที่ 354 #UserDir disable (ใส่เครื่องหมาย #)

บรรทัดที่ 361 UserDir public_html (ลบเครื่องหมาย #)

บรรทัดที่ 371 เพิ่มข้อความต่อท้ายว่า ExecCGI

Options MultiViews Indexes SymLinksIfOwnerMatch

IncludesnoExec ExecCGI

บรรทัดที่ 369-380 เอาเครื่องหมาย # ออกทุกบรรทัด

บรรทัดที่ 390 แก้ไขเพิ่มเติม

แก้เป็น DirectoryIndex index.html index.php index.htm

บรรทัดที่ 777 AddHandler cgi-script .cgi (ลบเครื่องหมาย # ออก)

/etc/init.d/httpd restart

2.7 สร้าง User ทำหน้าที่ Webmaster

useradd <ชื่อuser>

passwd <ชื่อuser>

ใส่รหัสผ่าน 2 ครั้ง

2.8 กำหนดให้ user ที่ทำหน้าที่ Webmaster เป็นเจ้าของ Directory ใน www

chown -R ชื่อuser.ชื่อuser /var/www/html

(มี directory : html, manual, cgi-bin, icons, error)

3. ติดตั้ง FTP Server และแก้ไขค่า Config

3.1 แก้ไขค่า config ในไฟล์ vsftpd.conf

vi /etc/vsftpd/vsftpd.conf

บรรทัดที่ 12 anonymous_enable = NO (เปลี่ยน YES เป็น NO)

บรรทัดที่ 51 xferlog_file = /var/log/vsftpd.log (เอาเครื่องหมาย # ออก)

บรรทัดที่ 64 nopriv_user = nobody เอาเครื่องหมาย # ออก และแก้ไขเป็น nobody

บรรทัดที่ 94 chroot_list_enable = YES } เอาเครื่องหมาย # ออก ทั้ง 2 บรรทัด

บรรทัดที่ 96 chroot_list_file = /etc/vsftpd/chroot_list

บรรทัดที่ 97 พิมพ์เพิ่ม background = YES

3.2 สร้าง file chroot_list เก็บรายชื่อ user

vi /etc/vsftpd/chroot_list

เพิ่มชื่อ user1 (ชื่อ user ที่ต้องการให้เห็นเฉพาะ directory ของตนเอง)

3.3 Start Service และ on ทุกครั้งที่ boot เครื่อง

/etc/init.d/vsftpd start

chkconfig vsftpd on

4. ติดตั้ง Proxy Server

4.1 แก้ไขค่า Config ในไฟล์ squid.conf

vi /etc/squid/squid.conf

บรรทัดที่ 763 cache_mem 32 MB (ค่า default) เปลี่ยนเป็น …. (1/3 ของ RAM)

บรรทัดที่ 1026 cache_dir aufs /cache/squid 5200 16 256

พื้นที่ของฮาร์ดดิสก์ที่ใช้ทำ cache (MB)
= 60 % ของ /cache
พื้นที่ไม่ควรเกิน 60% ของ cache

บรรทัดที่ 2556 alc localnet src 192.168.64.0/24 เอาเครื่องหมาย # ออก

หรือ

เปลี่ยนจาก 1 เป็น 64

alc localnet src 192.168.64.0/255.255.255.0

บรรทัดที่ 2882 visible_hostname localhost พิมพ์เพิ่มบรรทัดที่ 2882

บรรทัดที่ 2821 cache_mgr administrator@kknic.ac.th

บรรทัดที่ 3260 store_avg_object_size = ___ KB (ค่า default = 13 KB) (ใส่ไว้ 2048 KB)

(เอา # ออก)

4.2 สร้างที่อยู่ของ squid

mkdir /cache/squid

chown squid.squid /cache/squid

squid -zD

4.3 start squid และ on ทุกครั้งที่ boot เครื่อง

/etc/init.d/squid start

chkconfig squid on

5. ทำ Transparent Proxy

5.1 แก้ไขค่า Config ในไฟล์ squid.conf

vi /etc/squid/squid.conf +88

บรรทัด 88 http_port 3128 transparent

/etc/init.d/squid restart

5.2 จัดรูปแบบของ access.log

vi /etc/squid/squid.conf +1114

- (แก้ไขบรรทัดที่ 1114 และพิมพ์เพิ่มอีกบรรทัด)

บรรทัดที่ 1114 access_log /var/log/squid/access.log combined

(เปลี่ยนจาก squid เป็น combined)

บรรทัดที่ 1115 พิมพ์เพิ่ม access_log syslog combined

(เพื่อให้ส่งค่าไปที่ logserver)

บรรทัดที่ 1095 เอาเครื่องหมาย # ออก

Logformat combined…….

squid -k reconfigure

5.3 ป้องกันลูกข่ายดู web ไม่พึงประสงค์

vi /etc/squid/squid.conf (เอา # ออก)

บรรทัดที่ 2559 acl lock url_regex -i sex mude porn adult เอา # ออก

บรรทัดที่ 2560 http_access deny lock (เอาเครื่องหมาย # ออก)

บรรทัดที่ 2563 alc lock_list url_regex '/etc/squid/lock_list.txt'

บรรทัดที่ 2564 http_access deny lock_list

5.4 สร้าง file lock_list.txt เพื่อเก็บ url ที่ป้องกันไม่ให้เข้า

vi /etc/squid/lock_list.txt

squid -k reconfigure

5.5 แก้ไขเพิ่มเติม squid

vi /etc/squid/squid.conf

บรรทัดที่ 1947 request_header_max_size 50 KB
บรรทัดที่ 1958 request_body_max_size 0 KB
} ลบ # ออก

บรรทัดที่ 2074 quick_abort_min 16 KB
บรรทัดที่ 2075 quick_abort_max 16 KB
บรรทัดที่ 2076 quick_abort_pct 95
} ลบ # ออก

บรรทัดที่ 2801 reply_body_max_size 0 allow all (ลบ # ออก)

squid -k reconfigure

6. ติดตั้ง Radius Server

(อาจข้ามขั้นตอนการติดตั้ง radius server ได้ ถ้าอยู่คนละเครื่อง

6.1 ติดตั้ง package freeradius และสั่งให้ radius ทำงาน

```
# yum install freeradius
# /etc/init.d/radiusd start
# chkconfig radiusd on
```

6.2 แก้ไข radius ทำให้ Password อยู่ใน mode shadow

```
# vi /etc/raddb/radiusd.conf
```

บรรทัดที่ 144 # user = radiusd
บรรทัดที่ 115 # group = radiusd
} ใส่เครื่องหมาย # หน้าบรรทัด

```
# /etc/init.d/radiusd restart
```

6.3 ทดสอบ User ในระบบติดต่อ radius ได้หรือไม่

```
# radtest ชื่อuser password ของuser localhost 0 testing123
```

จะพบข้อความ Access-Accept

6.4 ทำให้ Server ทำหน้าที่ forward package

```
# vi /etc/sysctl.conf
```

บรรทัดที่ 7 แก้ไข net.ipv4.ip_forward = 1 (เปลี่ยนจากเลข 0 เป็นเลข 1)

6.5 สั่งให้ทำงานทันที

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

7. ติดตั้ง Chillispot

7.1 ติดตั้ง package chilli

```
# mkdir /download
# cd /download
# wget ftp://ftp.psu.ac.th/pub/chillispot/chillispot-1.1.0.i386.rpm
# rpm -Uvh chillispot-1.1.0.i386.rpm (กด Tab ช่วย)
```

7.2 Config ค่าใน Chillispot

vi /etc/chilli.conf (ทุกบรรทัดให้เอา # ออก)

บรรทัดที่ 38 net 192.168.xx.0/24

บรรทัดที่ 72 domain kknic.ac.th

บรรทัดที่ 59 dns1 61.19.254.134

บรรทัดที่ 66 dns2 61.19.254.135

บรรทัดที่ 108 radiuslisten 127.0.0.1

บรรทัดที่ 113 radiusserver1 61.19.212.xxx

(ทดสอบตัวเองให้กำหนด 127.0.0.1)

บรรทัดที่ 120 radiusserver2 61.19.212.xxx

(ทดสอบตัวเองให้กำหนด 127.0.0.1)

บรรทัดที่ 139 radiussecret testing123

บรรทัดที่ 217 dhcpif eth1

บรรทัดที่ 230 leases 86400

บรรทัดที่ 237 uamserver https://192.168.xx.1/cgi-bin/hotspotlogin.cgi

บรรทัดที่ 244 uamhomepage http://192.168.xx.1/welcome.html

บรรทัดที่ 248 uamsecret ht2eb8……

บรรทัดที่ 253 uamlisten 192.168.xx.1

7.3 คัดลอก firewall ของ chilli ไปไว้ที่ etc

cp /usr/share/doc/chillispot-1.1.0/firewall.iptables /etc (ให้ Tab ช่วยได้)

7.4 คัดลอก hotspotlogin.cgi

cp /usr/share/doc/ chillispot-1.1.0/hotspotlogin.cgi /var/www/cgi-bin

7.5 แก้ไข hotspotlogin.cgi

vi /var/www/cgi-bin/hotspotlogin.cgi

บรรทัดที่ 27 $uamsecret = “ht2eb…….”;
บรรทัดที่ 31 $userpassword = 1 ;
} เอาเครื่องหมาย # ออก

7.6 สร้าง webpage welcome.html

1) สร้างโดย # vi /var/www/html/welcome.html

2) ใช้ Dreamweaver

3) Copy จาก folder ที่เตรียมไว้

7.7 สั่งให้ chillispot ทำงาน

/etc/init.d/chilli start

chkconfig chilli on

7.8 ตรวจสอบว่า chillispot ทำงานหรือยัง

ifconfig

ดู tun 0 ว่ามี address หรือไม่

7.9 แก้ไขเพิ่ม firewall.iptables เพื่อทำ nat

vi /etc/firewall.iptables

พิมพ์

Allow transparent proxy

$IPTABLES -A INPUT -p tcp -m tcp --dport 3128 --syn -j ACCEPT

$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp ---dport 3128 --syn -j DROP

$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp -d 192.168.xx.0/24 --dport 80 -j RETURN

$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp --dport 80 -j REDIRECT --to-port 3128

แก้ไขเพิ่มเติมให้สามารถใช้ port 21, 22 ในการ FTP และ SSH ได้

เพิ่มเติมตรง # Allow related and established from $INTIF Drop everything else.

เพิ่ม port 22 สำหรับขาใน (ติดตั้งเสร็จแล้วยกเลิกได้)

$IPTABLES -A INPUT -i $INTIF -p tcp -m tcp --dport 22 --sys -j ACCEPT

เพิ่มเติมตรง # Allow related, established and ssh on $EXTIF Reject everything else.

$IPTABLES -A INPUT -i $EXTIF -p tcp -m tcp --dport 21 --sys -j ACCEPT

เพิ่มในส่วน $EXTIF เพื่อให้สามารถเข้า check graph จาก 61.19.212.140 ได้

$IPTABLES -A INPUT -I $EXTIF -p tcp -m tcp -d 61.19.212.140/255.255.255.248 --dport 80 --syn -j ACCEPT

$IPTABLES -A INPUT -i $EXTIF -p tcp -m tcp --dport 22 --sys -j ACCEPT

เปิด firewall port 123 udp สำหรับ NTP Server

เพิ่มในส่วน

Allow http and https on other inlerface (input)

This is only needed if authentication server is on same server as chilli

$IPTABLES -A INPUT -p tcp -m tcp --dport 21 --sys -j ACCEPT

$IPTABLES -A INPUT -p udp -m udp --dport 123 -j ACCEPT

$IPTABLES -A OUTPUT -p udp -m udp --sport 123 -j ACCEPT

7.10 Start firewall

sh /etc/firewall.iptables

7.11 เพิ่มคำสั่งใน rc.local

vi /etc/rc.local

พิมพ์เพิ่ม

sh /etc/firewall.iptables

service chilli start

7.12 Reboot เครื่อง Server

init 6