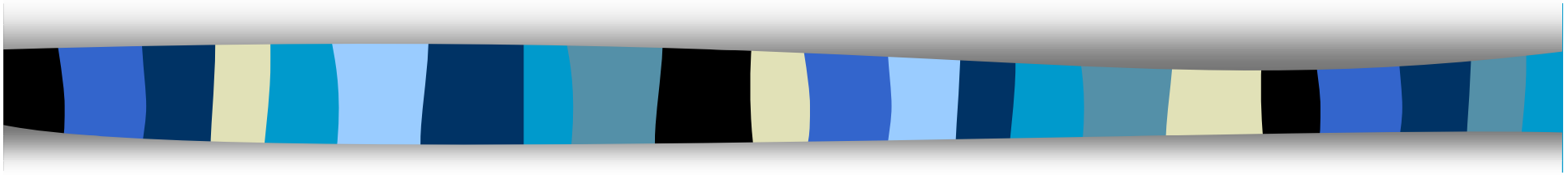
เอกสารประกอบการอบรมหลักสูตร Linux-SIS



วันที่ 4

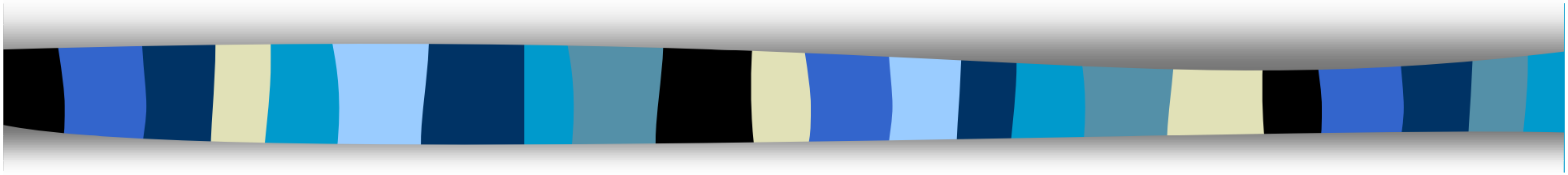
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ต้นฉบับที่ http://www.school.net.th/linux-sis/training/

ลิขสิทธิ์

- เอกสารชุดนี้สงวนลิขสิทธิ์โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ภายใต้ลิขสิทธิ์แบบ GNU Public License (GPL) รายละเอียดของลิขสิทธิ์แบบ GPL สามารถดูได้ที่
  - http://www.gnu.org/copyleft/gpl.html
  - http://linux.thai.net/gpl-th.html
- สามารถสรุปจุดที่สำคัญๆ ได้ดังนี้
  - อนุญาตให้นำไปใช้, เผยแพร่ต่อ, แก้ไข, แก้ไขฉบับที่เผยแพร่ต่อได้
  - เอกสารฉบับที่ถูกเผยแพร่ต่อจะต้องมีแสดงเงื่อนไขลิขสิทธิ์หน้านี้อย่างชัดเจน
  - เอกสารฉบับที่ท่านได้ทำการแก้ไขและเผยแพร่ต่อ จะต้องสงวนลิขสิทธิ์ภายใต้ลิขสิทธิ์ GPL เช่นเดียวกับเอกสารฉบับนี้
- หากที่ได้ทำการแก้ไขและพัฒนาเอกสารฉบับนี้ให้ดีขึ้น โปรดส่งต่อฉบับที่แก้ไขนั้นกลับมาที่ sis-master@nectec.or.th เพื่อที่จะได้ปรับปรุงตัวต้นฉบับให้ดีขึ้นต่อไป
- ทางศูนย์สงวนสิทธิ์ที่จะเปลี่ยนแปลง แก้ไขเงื่อนไขต่างๆ เพื่อรักษาผลประโยชน์ของทางศูนย์และส่วนรวม

การติดตั้งและใช้งาน Internet Server (ต่อ)



FTP Server: wu-ftpd

- แทบจะมีมีการ UNIX ทุกๆ ตัวในปัจจุบัน
- ตรวจสอบใน /etc/inetd.conf และ /etc/hosts.deny
- Configuration files:
  - /etc/passwd สำหรับ Anonymous FTP
  - /etc/ftpaccess
  - /etc/ftpconvertions
  - /etc/ftpgroups
  - /etc/ftpusers User ที่ห้ามทำการ ftp
  - /etc/shells Shell ของผู้ใช้ที่ยอมให้ทำการ ftp

Anonymous FTP Server

- เปิดให้ผู้ใช้ใดๆ สามารถมาดาวน์โหลด (และ อัพโหลด) ข้อมูลได้
- สร้างบัญชี ftp ใน /etc/passwd
- Home directory ของผู้ใช้ ftp จะเป็น Home ของ Anonymous FTP user เช่นกัน ภายใน Home Directory จะมีไฟล์ดังนี้
  - bin/ls (ต้องเป็นเวอร์ชั่น Statically-linked)
  - etc/passwd (ห้ามเอา System /etc/passwd มาไว้ในนี้เด็ดขาด)
  - pub (ส่วนใหญ่นิยมเก็บไฟล์ที่ต้องการเผยแพร่ไว้ใต้นี้)

การบังคับให้ Home ของ User เป็น FTP / Directory

- กรณีที่ต้องการให้ผู้ใช้ทำงานอยู่แค่ใน Home ตัวเองเท่านั้น ไม่ออกเป็นนอกเหนือจากนี้
- เมื่อทำการ ftp เข้าไปจะเห็น Home ของตัวเองเป็น Directory / เลย
- วิธีการ
  - เพิ่ม group ของ user กลุ่มนั้นๆ เข้าไปใน /etc/ftpaccess (guestgroup)
  - ใน Home ของผู้ใช้เหล่านั้น จะต้องมีไฟล์ bin/ls (static version - ทำนองเดียวกับของ Anonymous User)

แบบฝึกหัด

- ติดตั้งให้ FTP Server ทำงานในโหมด Anonymous และทดลองนำไฟล์ไปไว้ในไดเรกทอรี่ pub/ ให้ผู้ใช้สามารถมาดาวน์โหลดได้
- ติดตั้งให้เมื่อ Log in ด้วยผู้ใช้ admin แล้วมองเห็น Home directory ของตนเองเป็น / directory

Webmin

- ซอฟต์แวร์ช่วยในการบริหารเครื่องผ่านทาง WWW
- คล้าย Web Admin Tool ของ Linux-SIS แต่บริหารในหลายแง่มุมกว่า นอกจากบริหารงานผู้ใช้แล้วยังมี
  - DNS Server
  - Cron
  - Apache
  - Printer, PPP, Process, Disk partition, …, etc.

วิธีติดตั้งและใช้งาน สำหรับ Linux-SIS 3

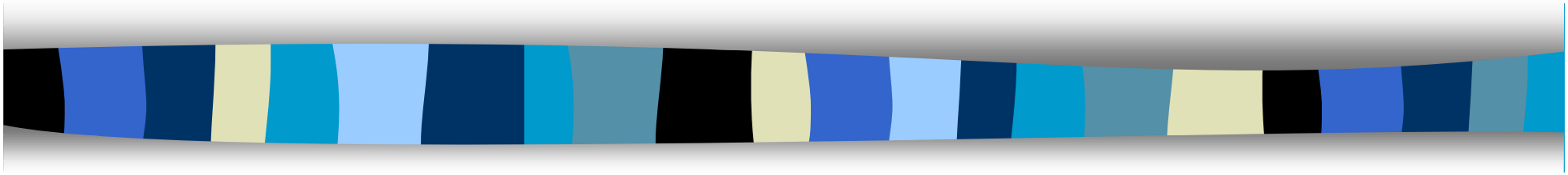
- ติดตั้งครั้งแรกก่อน
  - cd /usr/local/src/webadmin-xxx/
  - ./setup.sh (ป้อนค่าชนิดของ OS เป็น Slackware 3.6, ตั้งว่าจะใช้ SSL หรือไม่, ตั้ง user, password)
- เรียกใช้งานผ่าน www ตาม port, user, password ที่ได้ตั้งไว้ (ถ้าเลือกไว้เป็น SSL ต้องเรียกไปที่ https://…)

แบบฝึกหัด

- ทดลองติดตั้งและใช้งาน webmin

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

Linux Security



ความปลอดภัยของระบบเบื้องต้น

- ทำไมต้องคำนึงถึงความปลอดภัย?
- ระดับของการรักษาความปลอดภัย
  - Physical Security
  - Host Security
  - Network Security
- Security Policy

Physical Security

- ระบบควรอยู่ในห้องที่เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต
- ไม่ปล่อยหน้าจอ Log in ค้างไว้
- Lock กุญแจเครื่อง PC
- Lock รหัสผ่าน BIOS
- ไม่จดรหัสผ่านแปะตามหน้าจอ หรือสมุด
- ตรวจสอบการ Reboot โดยไม่ตั้งใจ
- ป้องกันการบูตไดรว์ฟ A:

Host Security

- User Account Security
  - ให้สิทธิ์เท่าที่จำเป็นเท่านั้น
  - รหัสผ่านต้องมีความปลอดภัย
  - พิจารณาการให้สิทธิ์ telnet อย่างรอบคอบ
  - ไม่สร้างบัญชี guest หรือ บัญชีที่ไม่มี Password
  - ตรวจสอบสถานะของบัญชีทั้งหมดอย่างสม่ำเสมอ
  - ใช้ root เมื่อจำเป็น และใช้งานผ่าน su เท่านั้น

- Service Security
  - ระบบควรให้บริการงานที่จะเป็นเท่านั้น
    - /etcinetd.conf
    - Startup Process
- File และ File System Security
  - ทำความเข้าใจกับ Permission อย่างละเอียด
  - ระวังไฟล์ SUID, SGID
  - สำรองข้อมูลอย่างสม่ำเสมอ
  - ใช้เครื่องมือช่วยอย่าง MD5, Tripwire

- Password และ Encryption Security
  - ใช้ Shadow Password
  - ใช้ One-time Password
  - ทดลอง Crack รหัสของผู้ใช้บนเครื่องของท่านเอง
  - ศึกษาประยุกต์ใช้เทคโนโลยี Public Key Infrastructure
  - เข้ารหัสจดหมายอิเล็กทรอนิกส์และไฟล์ด้วย PGP
  - ใช้ SSL สำหรับการรับส่งข้อมูลที่ต้องการความปลอดภัย

- Kernel Security
  - ศึกษา Options ที่มีผลต่อ Security เช่น Source routed frame, Sync Cookie
- Network Security
  - ความปลอดภัยของทั้งเครือข่าย เท่ากับความปลอดภัยของจุดที่อ่อนที่สุด
  - Packet Sniffer
    - ตรวจสอบการทำงานของ Sniffer
    - ใช้ Switch แทน Hub
    - ใช้ One-time password, SSH

- TCP Wrapper ควบคุมบริการที่ให้กับผู้ใช้
- Firewall

ศึกษาหาความรู้เพิ่มเติม

- http://www.securityportal.com/
- http://www.securityfocus.com/
- http://www.cert.org/
- Linux Security, Firewall HOWTO

TCP Wrappper

- Server (หรือ Service) ต่างๆ ทำงานใน 2 โหมด
  - Stand Alone
  - ผ่าน inetd
- ควบคุมการให้บริการของ Service ต่างๆ ที่เปิดผ่าน inetd (/etc/inetd.conf)

TCP Wrapper และ /etc/inetd.conf

```
ftp      stream  tcp     nowait  root    /usr/sbin/tcpd  wu.ftpd -l -i -a
telnet   stream  tcp     nowait  root    /usr/sbin/tcpd  in.telnetd
pop3     stream  tcp     nowait  root    /usr/sbin/in.pop3d  in.pop3d
```

/etc/hosts.deny และ /etc/hosts.allow

- **hosts.allow** เป็นไฟล์ที่ใช้สำหรับแสดงรายละเอียดเงื่อนไขต่างๆ ที่ตั้งไว้ว่า อนุญาติให้ใคร (จาก IP หรือ host) เข้ามาทำงานกับเครื่องของเราได้บ้าง
- **hosts.deny** เป็นไฟล์ที่ใช้สำหรับแสดงรายละเอียดเงื่อนไขต่างๆ ที่ตั้งไว้ว่า ไม่อนุญาติให้ใคร(จาก IP หรือ host) เข้ามาทำงานกับเครื่อง ของเราได้บ้าง
- จริงๆ แล้วสามารถเลือกระบุเพียงในไฟล์ใดไฟล์หนึ่ง

วิธีการระบุในไฟล์ hosts.allow และ hosts.deny

- <รายชื่อบริการ>: <เงื่อนไขในการให้บริการ>
- วิธีที่แนะนำคือ ปิดบริการทุกอย่าง แล้วเปิดที่จำเป็น
  - /etc/hosts.allow ไม่ต้องใส่อะไร
  - /etc/hosts.deny เปิดตามที่ต้องการเช่น
    - in.telnetd:ALL EXCEPT 192.168.1.1
    - in.ftpd: ALL EXCEPT 192.168.1.1 nectec.or.th
    - ALL: ALL EXCEPT .utcc.ac.th
    - ALL EXCEPT wu.ftpd: .nectec.or.th

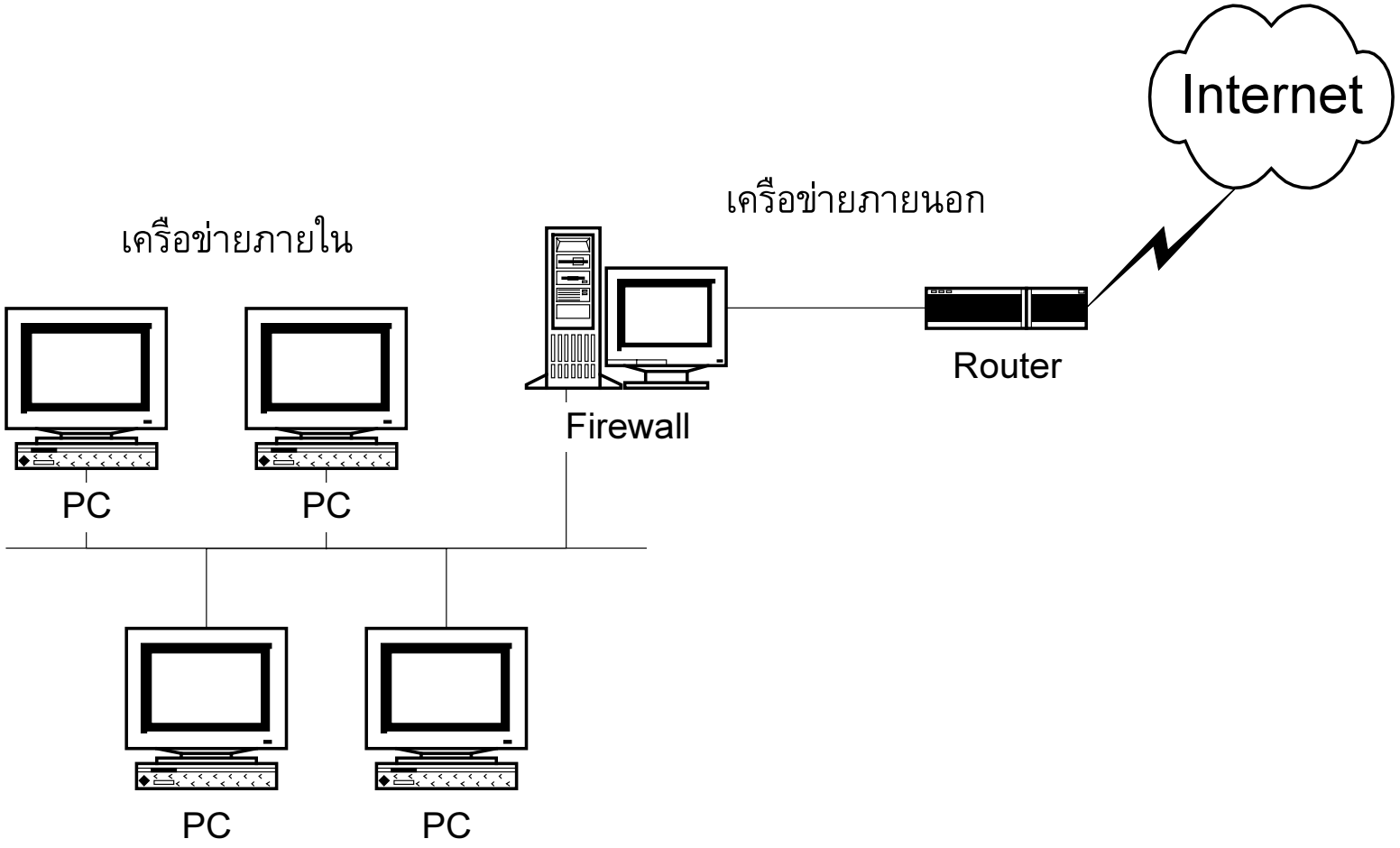
แบบฝึกหัด

- ทดลองตั้งค่าใน /etc/hosts.deny เปิดให้เครื่อง Client PC ของท่านสามารถใช้บริการการ telnet/ftp/pop3/imap ทั้งได้และไม่ได้ และตรวจสอบผลจากการทดลองใช้งานบริการเหล่านั้น

Firewall: ipfwadm

- เป็นวิธีการที่จะช่วยเพิ่มความปลอดภัยให้ทั้งเครือข่าย
- มีเครื่องๆ หนึ่งวางกั้นขวางเปรียบเสมือนยามที่ตรวจสอบคนเข้าออก
- ข้อดี: ควบคุมได้ที่จุดๆ เดียว บริหารงานง่ายกว่าที่จะต้องไปดูแลเครื่องคอมพิวเตอร์ทุกๆ เครื่อง
- ข้อเสีย: Single Point of Failure, ประสิทธิภาพต่ำลง

แผนผังของเครือข่ายที่มี Firewall อย่างง่าย



ชนิดของ Firewall

- Filtering Firewall
- Proxy Server

ก่อนจะใช้ Firewall

- กล่าวกันว่า Firewall --> อุปกรณ์ที่ซื้อมาแล้วไม่คุ้มค่ามากที่สุด ?
- ก่อนจะจัดหา/จัดทำ Firewall
  - Security Policy
  - Network Design: Network ส่วนนอก และส่วนในของท่านจะต้องเชื่อมต่อกันตรงจุดที่ Firewall ตั้งอยู่เท่านั้น

สร้าง Firewall ใช้เองด้วย Linux

- Linux 2.0.x
  - Compile Kernel ให้สนับสนุน
  - ใช้งานร่วมกับโปรแกรม ipfwadm
- Linux 2.2.x
  - Compile Kernel ให้สนับสนุน
  - ใช้งานร่วมกับโปรแกรม ipchains
- เครื่องคอมพิวเตอร์ที่ทำหน้าที่ Firewall ต้องมีอย่างน้อย 2 Network Interface (อาจเป็น 2 Ethernet Card, 1 Ethernet Card + 1 Modem)

Kernel Rebuild

1. ในหัวข้อ General setup

    a. Networking Support ON

2. ในหัวข้อ Networking Options

    a. Network firewalls ON

    b. TCP/IP Networking ON

    c. IP forwarding/gatewaying ON

    d. Firewalling ON

    e. Firewall packet logging ON (ไม่จำเป็นแต่แนะนำ)

f. IP: masquerading ON (ถ้าต้องการใช้ IP Masquerade)

g. IP: accounting ON

h. IP: tunneling OFF

i. IP: aliasing OFF

j. IP: PC/TCP compatibility mode OFF

k. IP: Reverse ARP OFF

l. Drop source routed frames ON

3. ในหัวข้อ Network device support

a. Network device support ON

b. Dummy net driver support ON

c. Ethernet (10 or 100Mbit) ON

d. เลือก Ethernet Card ของท่าน

- เพื่อให้เห็น 2 Ethernet Card
  - อาจต้องเพิ่ม append=“ether=0,0,eth1” ใน /etc/lilo.conf แล้วรัน /sbin/lilo
  - ระวังเรื่อง IRQ ของทั้งสอง Card ไม่ให้ชนกัน
  - หากไม่ใช่ Plug & Play card อาจต้องเข้าไปใน BIOS ตั้งว่า IRQ นั้นๆ ได้ถูกใช้ไปโดย ISA แล้ว เพื่อไม่ให้เครื่องนำ IRQ นั้น ไปแจกให้กับอุปกรณ์อื่นอีก ซึ่งจะทำให้ LAN Card ใช้ไม่ได้

ipfwadm

- *ipfwadm -A command parameters [options]*
- *ipfwadm -I command parameters [options]*
- *ipfwadm -O command parameters [options]*
- *ipfwadm -F command parameters [options]*
- *ipfwadm -M [-l | -s] [options]*

Command

– -a [policy]	append
– -i [policy]	insert
– -d [policy]	delete
– -l [policy]	list
– -p [policy]	default policy
– -z	Reset Counter
– -f	flush

- -s tcp tcpfin udp — ตั้งค่า timeout
- -c — check
- -h — help

- Parameter
  - -P protocol (tcp, udp, icmp หรือ all)
  - -S address/[mask] [port]
  - -D address/[mask] [port]
  - -V Address Interface Address
  - -W name Interface Name

Extra Options

- -m masquerade
- -r [port] redirect
- -o เก็บ log
- -v Verbose

ตัวอย่างการใช้งาน

- Flush all rules
  - ipfwadm -I -f
  - ipfwadm -O -f
  - ipfwadm -F -f
- ตั้งค่า Default ให้เป็น deny ทั้งหมด
  - ipfwadm -I deny
  - ipfwadm -O deny
  - ipfwadm -F deny

ตัวอย่างเพิ่มเติม

- ipfwadm -I -a accept -V 192.168.1.1 -S 192.168.1.0/24 -D 0.0.0.0/0
- ipfwadm -I -a accept -W eth0 -S 192.168.1.0/24 -D 0.0.0.0/0
- ipfadm -O -a accept -V 192.168.1.1 -S 0.0.0.0/0 -D 192.168.1.0/24
- ipfwadm -O -a deny -S 0.0.0.0/0 -D 0.0.0.0/0 -o
- ipfwadm -F -l
- ipfadm -F -a m -S 192.168.1.0/24 -D 0.0.0.0/0

IP Masquerade

- ข้อดีและข้อเสียของ
  - Packet Filter Firewall
  - Proxy Server Firewall
- IP Masquerade
  - ทำ Proxy Server Firewall ในระดับ Kernel
  - ผู้ใช้ภายใน สามารถใช้งาน Internet Application ได้เสมือนอยู่ภายนอก
  - ผู้ใช้จากภายนอก ไม่สามารถเข้ามาใช้งานบริการภายในได้
  - คล้ายโปรแกรมจำพวก Wingate, Winproxy

Kernel Rebuild

- เพิ่มเติมจากส่วนของ Firewall หัวข้อที่แล้ว

Prompt for development and/or incomplete code/drivers (CONFIG_EXPERIMENTAL): YES

IP: masquerading (CONFIG_IP_MASQUERADE): YES

IP: ipautofw masquerade support (CONFIG_IP_MASQUERADE_IPAUTOFW): YES

IP: ICMP masquerading (CONFIG_IP_MASQUERADE_ICMP): YES

Startup file /etc/rc.d/rc.firewall

- โหลด module ที่จำเป็น

  /sbin/depmod -a

  /sbin/modprobe ip_masq_ftp

  /sbin/modprobe ip_masq_raudio

  /sbin/modprobe ip_masq_irc

  /sbin/modprobe ip_masq_cuseeme

  /sbin/modprobe ip_masq_vdolive

Firewall Rules (ตัวอย่างแบบง่าย)

- # Flush all rules
- /sbin/ipfwadm -I -f
- /sbin/ipfwadm -O -f
- /sbin/ipfwadm -F -f
- # Set the default Input and Output policy to "accept"
- /sbin/ipfwadm -I -p accept
- /sbin/ipfwadm -O -p accept
- # Set the default Forward policy to "deny"
- /sbin/ipfwadm -F -p deny

- # Accept traffic to our own web server
- /sbin/ipfwadm -I -a accept -P tcp -S192.168.1.0/24 -D192.168.1.1/32 80
- # Redirect Web Traffic to proxy (Transparent proxy)
- /sbin/ipfwadm -I -a accept -P tcp -r 81 -S192.168.1.0/24 -D/0.0.0.0/0 80
- # IP Masquerade for 192.168.1.0/24 (Internal Network)
- /sbin/ipfwadm -F -a m -S 192.168.1.0/24 -D 0.0.0.0/0

แบบฝึกหัด

- ทดลองแก้ไข Firewall Rules ทดลองเอาบรรทัดที่ทำ IP Masquerade ออก และดูว่า Client PC ยังสามารถใช้งานอินเทอร์เน็ตได้อยู่อีกหรือไม่

Transparent Proxy

- เราต่างทราบกันดีว่า Cache/Proxy Server เป็นสิ่งที่มีประโยชน์
- แต่การบังคับให้ User ต้องเปลี่ยน Browser Setting อาจไม่ง่ายนัก
- ระบบ Transparent Proxy
  - ดักข้อมูล Request web จาก user และ Redirect ไปให้ Proxy Server โดยอัตโนมัติ
  - เครื่อง Linux-SIS Server จะต้องวางขวางเป็น gateway และมี Squid Proxy/Cache Server ทำงานอยู่

การติดตั้ง Transparent Proxy

- /etc/rc.d/rc.firewall
  - ipfwadm -I -a accept -P tcp -r 8080 -S192.168.1.0/24 -D0.0.0.0/0 80
- ตั้งค่าที่ Squid ให้รับรู้การ Redirect Traffic มา โดยเพิ่มใน squid.conf
  - httpd_accel_host virtual
  - httpd_accel_port 80
  - httpd_accel_with_proxy on
  - httpd_accel_uses_host_header on

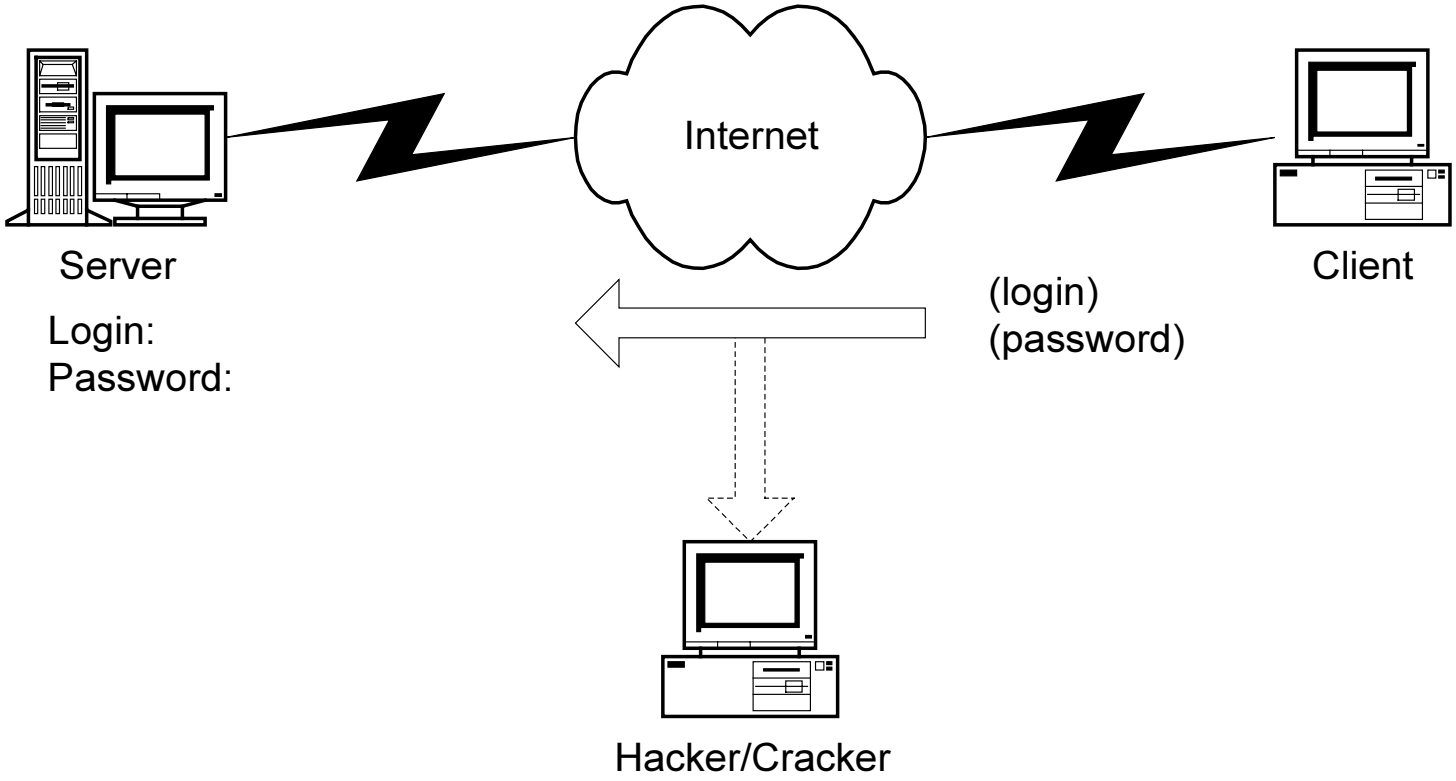
แบบฝึกหัด

- ทดลองเอา Firewall Rule ที่เกี่ยวข้องกับ Transparent Proxy ออก และทดสอบดูว่า Client PC ยังสามารถใช้งาน www แบบ Transparent Proxy ได้อยู่หรือไม่ และถ้าแก้ Browser Setting ให้ชี้ไปยัง Proxy server ตรงๆ จะใช้งาน www ได้หรือไม่

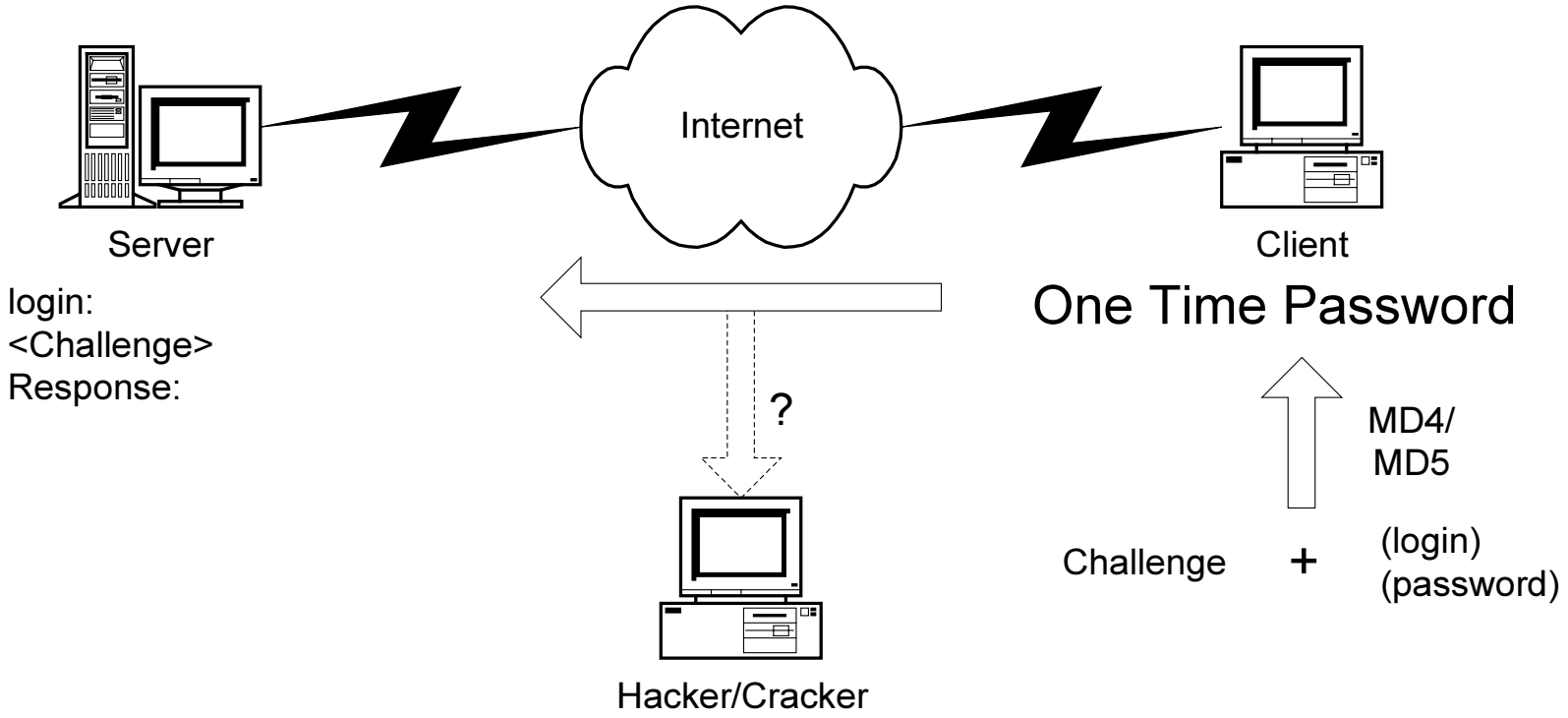
One-Time Password

- การ telnet/ftp ปกติจะมีการส่ง Login และ รหัสผ่าน ไปในเครือข่าย โดยไม่มีการเข้ารหัสใดๆ
- ผู้ไม่ประสงค์ดีที่อยู่ในระหว่างทาง สามารถดักข้อมูลไปได้ เช่น โปรแกรมอย่าง Sniffer

การ telnet/ftp ปกติ



การ telnet/ftp ด้วย One-Time Password



ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

One-Time-Password

- Algorythm: MD4/MD5
- Server:
  - S/KEY
  - OPIE
  - Log Daemon
- Client
  - ต้องมี OTP Calculator ซึ่งมีทั้งบน Windows/Mac/UNIX/Java

การใช้งานบน Linux-SIS 3

- ให้ติดตั้งส่วน source
  - cd /usr/local/src/opie-2.32
  - make install
  - opiepasswd เพื่อตั้งค่า OTP และเปลี่ยนในครั้งต่อๆ ไป
- OTP Password จะเป็นคนละตัวกับ UNIX Password

แบบฝึกหัด

- ทดลองติดตั้ง OPIE OTP บนเครื่องของท่านให้กับบริการ telnet
- ติดตั้งโปรแกรม Winkey และทดลองใช้จากเครื่อง Client PC