[illegible] Linux-SIS

[illegible] 4

[illegible] © 2542

[illegible]
http://www.school.net.th/linux-sis/training/

[illegible]

- [illegible] GNU Public License (GPL) [illegible] GPL [illegible]
  - http://www.gnu.org/copyleft/gpl.html
  - http://linux.thai.net/gpl-th.html
- [illegible]
  - [illegible], [illegible], [illegible], [illegible]
  - [illegible]
  - [illegible] GPL [illegible]
- [illegible] sis-master@nectec.or.th [illegible]
- [illegible]

[illegible] © [illegible] 2542

[illegible]
[illegible]

[illegible]
[illegible] Internet Server ([illegible])

FTP Server: wu-ftpd

- □□□□□□□□□□□□□□ UNIX □□□□ □□□□□□□□□□□□□□□
- □□□□□□□□□□ /etc/inetd.conf □□□ /etc/hosts.deny
- Configuration files:
  - /etc/passwd
    □□□□□□□□ Anonymous FTP
  - /etc/ftpaccess
  - /etc/ftpconvertions
  - /etc/ftpgroups
  - /etc/ftpusers User □□□
    □□□□□□□□□□□ ftp
  - /etc/shells Shell
    □□□□□□□□□□□□□□□□□□□□□□□□□□□□□ ftp

□□□□□□□□□□□□□□□ © □□□□□□□ 2542

Anonymous FTP Server

- [illegible] [illegible] ([illegible] [illegible]) [illegible]
- [illegible] ftp [illegible] /etc/passwd
- Home directory [illegible] ftp [illegible] Home [illegible] Anonymous FTP user [illegible] [illegible] Home Directory [illegible]
  - bin/ls ([illegible] Statically-linked)
  - etc/passwd ([illegible] System /etc/passwd [illegible] [illegible])
  - pub ([illegible] [illegible])

[illegible] Home [illegible] User [illegible] FTP / Directory

- [illegible] Home [illegible] [illegible] [illegible]
- [illegible] ftp [illegible] Home [illegible] [illegible] Directory / [illegible]
- [illegible]
  - [illegible] group [illegible] user [illegible] [illegible] /etc/ftpaccess (guestgroup)
  - [illegible] Home [illegible] [illegible] [illegible] bin/ls (static version - [illegible] Anonymous User)

□□□□□□□□□

- □□□□□□□□□□□ FTP Server □□□□□□□□ □□□□ Anonymous □□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□ pub/ □□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□
- □□□□□□□□□□□□□□□□□ Log in □□□□ □□□□□□ admin □□□□□□□□□□□ Home directory □□□□□□□□□□□□□ / directory

□□□□□□□□□□□□□□ © □□□□□□ 2542
□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□

Webmin

- [illegible] [illegible] WWW
- [illegible] Web Admin Tool [illegible] Linux-SIS [illegible] [illegible] [illegible] [illegible]
  - DNS Server
  - Cron
  - Apache
  - Printer, PPP, Process, Disk partition, …, etc.

[illegible] © [illegible] 2542

[illegible] [illegible] Linux-SIS 3

- [illegible]
  - cd /usr/local/src/webadmin-xxx/
  - ./setup.sh ([illegible] OS [illegible] Slackware 3.6, [illegible] SSL [illegible], [illegible] user, password)
- [illegible] www [illegible] port, user, password [illegible] ([illegible] SSL [illegible] https://…)

[illegible] © [illegible] 2542

[illegible]

- [illegible] webmin

[illegible] © [illegible] 2542

[illegible]
[illegible]

Linux Security

[illegible]

- [illegible]?
- [illegible]
  - Physical Security
  - Host Security
  - Network Security
- Security Policy

[illegible] © [illegible] 2542

Physical Security

- □□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□ Log in □□□□□□□
- Lock □□□□□□□□□□□□ PC
- Lock □□□□□□□□ BIOS
- □□□□□□□□□□□□□□□□□□□□□□□□□ □□□□ □□□□
- □□□□□□□□□□ Reboot □□□□□□□□□□□□
- □□□□□□□□□□□□□□□□□□□ A:

□□□□□□□□□□□□□□ © □□□□□□□ 2542

□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□

Host Security

- User Account Security
  - [illegible]
  - [illegible]
  - [illegible] telnet [illegible]
  - [illegible] guest [illegible] [illegible] Password
  - [illegible]
  - [illegible] root [illegible] [illegible] su [illegible]

[illegible] © [illegible] 2542

[illegible]
[illegible]

- Service Security
  - [illegible] [illegible]
    - /etcinetd.conf
    - Startup Process
- File [illegible] File System Security
  - [illegible] Permission [illegible]
  - [illegible] SUID, SGID
  - [illegible]
  - [illegible] MD5, Tripwire

[illegible] © [illegible] 2542

- Password [illegible] Encryption Security
  - [illegible] Shadow Password
  - [illegible] One-time Password
  - [illegible] Crack [illegible]
  - [illegible] Public Key Infrastructure
  - [illegible] PGP
  - [illegible] SSL [illegible]

[illegible] © [illegible] 2542

- Kernel Security
  - □□□□□ Options □□□□□□□□□□□ Security □□□□ Source routed frame, Sync Cookie
- Network Security
  - □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
  - Packet Sniffer
    - □□□□□□□□□□□□□□□□□□□□□ Sniffer
    - □□□ Switch □□□ Hub
    - □□□ One-time password, SSH

- TCP Wrapper [illegible]
  [illegible]
- Firewall

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

TCP Wrappper

- Server (□□□□ Service) □□□□□ □□□□□□□□□ 2 □□□□
  - Stand Alone
  - □□□□ inetd
- □□□□□□□□□□□□□□□□□□□□□□□□□□ Service □□□□□ □□□□□□□□□□□□ inetd (/etc/inetd.conf)

TCP Wrapper □□□ /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 [illegible] /etc/hosts.allow

- **hosts.allow** [illegible] ([illegible] IP [illegible] host) [illegible]
- **hosts.deny** [illegible] ([illegible] IP [illegible] host) [illegible]
- [illegible]

[illegible] hosts.allow [illegible] hosts.deny

- <[illegible]>: <[illegible]>
- [illegible] [illegible] [illegible] [illegible]
  - /etc/hosts.allow [illegible]
  - /etc/hosts.deny [illegible]
    - 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

[illegible] © [illegible] 2542

□□□□□□□□□

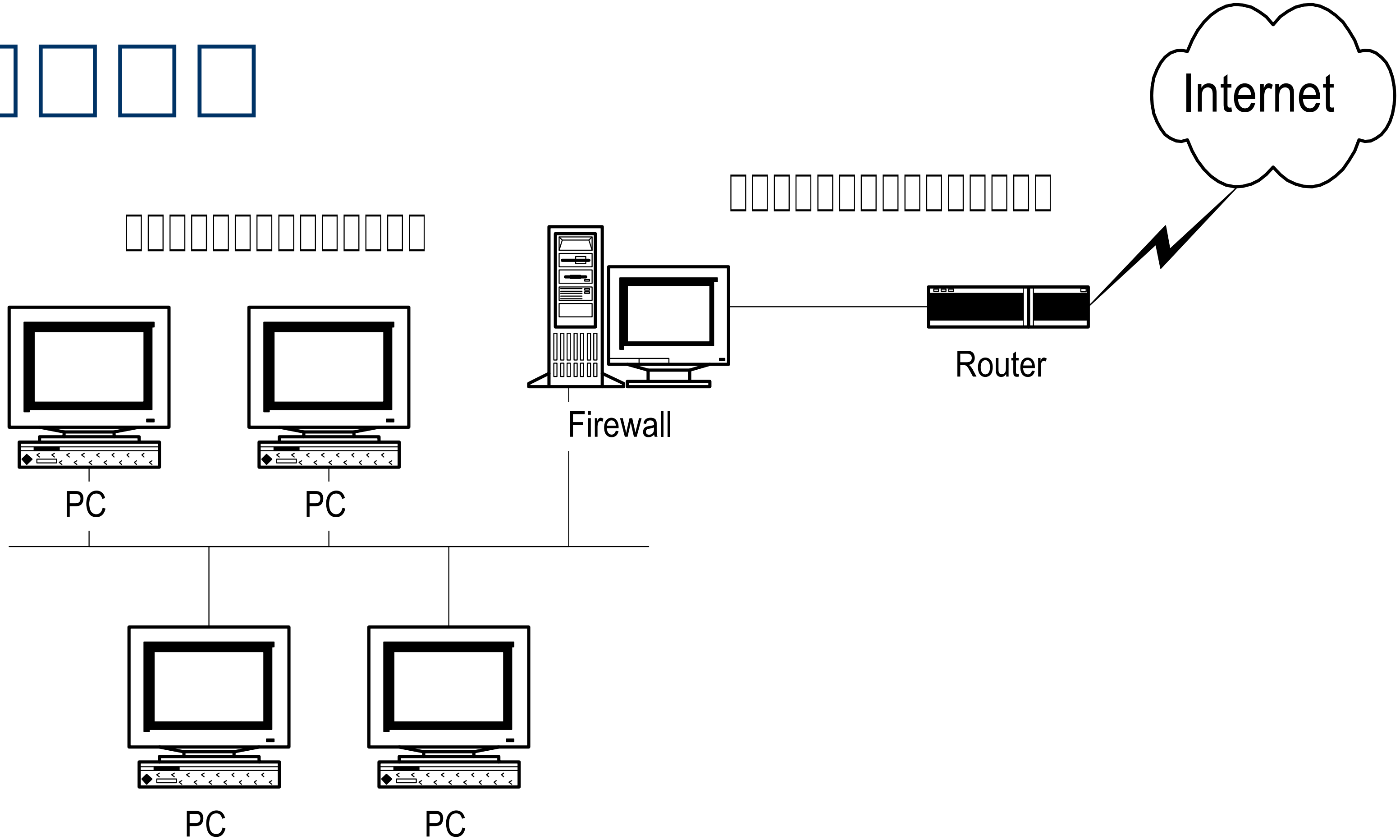
- □□□□□□□□□□□□□□□□ /etc/hosts.deny □□□□□□□□□□□□□□□□ Client PC □□□ □□□□□□□□□□□□□□□□□□□□□□□□□□ telnet/ftp/pop3/imap □□□□□□□□□□ □□□□□□ □□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□

Firewall: ipfwadm

- [illegible]
- [illegible]
- [illegible]: [illegible]
- [illegible]: Single Point of Failure, [illegible]

[illegible] © [illegible] 2542

□□□□□□□□□□□□□□□□□□ □□□□□ Firewall □□□□□ □□□□



□□□□□□□□□□□□□□□□□ © □□□□□□□ 2542

□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□ Firewall

- Filtering Firewall
- Proxy Server

[illegible] Firewall

- [illegible] Firewall --> [illegible] ?
- [illegible]/[illegible] Firewall
  - Security Policy
  - Network Design: Network [illegible] Firewall [illegible]

[illegible] © [illegible] 2542

[illegible]
[illegible]

□□□□□ Firewall □□□□□□

□□□□ Linux

- Linux 2.0.x
  - Compile Kernel □□□□□□□□□□□□□□
  - □□□□□□□□□□□□□□□□□□□□□□□□□ ipfwadm
- Linux 2.2.x
  - Compile Kernel □□□□□□□□□□□□□□
  - □□□□□□□□□□□□□□□□□□□□□□□□□ ipchains
- □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ Firewall □□□□□□□□□□□□□□□ 2 Network Interface (□□□□□□□ 2 Ethernet Card, 1 Ethernet Card + 1 Modem)

□□□□□□□□□□□□□□□□ © □□□□□□□ 2542

□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□

Kernel Rebuild

1. □□□□□□□□□ General setup
   a. Networking Support ON
2. □□□□□□□□□ Networking Options
   a. Network firewalls ON
   b. TCP/IP Networking ON
   c. IP forwarding/gateweying ON
   d. Firewalling ON
   e. Firewall packet logging ON (□□□□□□□□□□□□□□□□□□□□□□□□□□)

f. IP: masquerading ON (□□□□□□□□□□□□□□□ 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. □□□□□□□□□ Network device support

a. Network device support ON

b. Dummy net driver support ON

c. Ethernet (10 or 100Mbit) ON

d. □□□□□ Ethernet Card □□□□□□□

- □□□□□□□□□□□□□ 2 Ethernet Card
  - □□□□□□□□□□□□□ append="ether=0,0,eth1" □□ /etc/lilo.conf □□□□□□□ /sbin/lilo
  - □□□□□□□□□□□ IRQ □□□□□□□□□□□ Card □□□□□□□□□□□
  - □□□□□□□□□□ Plug & Play card □□□□□□□□□□□□□□□□ BIOS □□□□□□□ IRQ □□□□□ □□□□□□□□□□□□□□ ISA □□□□ □□□□□□□□□□□□□□□□□□□□□□□□ IRQ □□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□ LAN Card □□□□□□□□□□

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]*

□□□□□□□□□□□□□□ © □□□□□□ 2542
□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□

- 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 timeout □□□□□□□□
- -c check
- -h help

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

□□□□□□□□□□□□□□ © □□□□□□ 2542
□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□

- Extra Options
  - -m masquerade
  - -r [port] redirect
  - -o □□□□ log
  - -v Verbose

□□□□□□□□□□□□□□□□□□

- Flush all rules
  - ipfwadm -I -f
  - ipfwadm -O -f
  - ipfwadm -F -f
- □□□□□□□ Default □□□□□□□ deny □□□□□□□
  - ipfwadm -I deny
  - ipfwadm -O deny
  - ipfwadm -F deny

- □□□□□□□□□□□□□□□□□□□□

  - 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

- □□□□□□□□□□□□□□□□□□□□
  - Packet Filter Firewall
  - Proxy Server Firewall
- IP Masquerade
  - □□□ Proxy Server Firewall □□□□□□□□ Kernel
  - □□□□□□□□□□□□□ □□□□□□□□□□□□□□ Internet Application □□□□□□□□□□□□□□□□□□□□□□
  - □□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□
  - □□□□□□□□□□□□□□□□□□□□□ Wingate, Winproxy

Kernel Rebuild

- [illegible]
  Firewall [illegible]

pt for development and/or incomplete code/drivers (CONFIG_EXPERIME

asquerading (CONFIG_IP_MASQUERADE): YES

autofw masquerade support (CONFIG_IP_MASQUERADE_IPAUTOFW)

CMP masquerading (CONFIG_IP_MASQUERADE_ICMP): YES

[illegible] © [illegible] 2542

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

- □□□□ module □□□□□□□□□□□

```
/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 (□□□□□□□□□□□□□□□□□□)
  - # 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

□□□□□□□□□

- □□□□□□□□□□□ Firewall Rules □□□□□ □□□□□□□□□□□□□□□□□□ IP Masquerade □□□ □□□□□□□□□ Client PC □□□ □□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□

□□□□□□□□□□□□□□ © □□□□□□ 2542

□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□

Transparent Proxy

- □□□□□□□□□□□□□□□□□□□□□□□ Cache/Proxy Server □□□□□□□□□□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□□□□□ User □□□□□□□□□□□□ Browser Setting □□□□□□□□□□□□□□□
- □□□□ Transparent Proxy
  - □□□□□□□□□□ Request web □□□ user □□□ Redirect □□ □□□ Proxy Server □□□□□□□□□□□□□
  - □□□□□□□□ Linux-SIS Server □□□□□□□□□□□□□□□□ □□□□ gateway □□□□□ Squid Proxy/Cache Server □□□□□□□□□□□

□□□□□□□□□□□□□□□ © □□□□□□ 2542

□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□ 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
- □□□□□□□□□□□ Squid □□□□□□□□□□□□□ Redirect Traffic □□ □□□□□□□□□□ squid.conf
  - httpd_accel_host virtual
  - httpd_accel_port 80
  - httpd_accel_with_proxy on
  - httpd_accel_uses_host_header on

□□□□□□□□□

- □□□□□□□□□ Firewall Rule □□□ □□□□□□□□□□□□□□□ Transparent Proxy □□□ □□□□□□□□□□□□□□□ Client PC □□□□□□□□□□□□□□□□□ www □□□ Transparent Proxy □□□□□□□□□□□ □□□ □□□□□□□□□□ Browser Setting □□□□□□□□□□□□ Proxy server □□□□ □□□□□□□□□ www □□□□□□□□□□

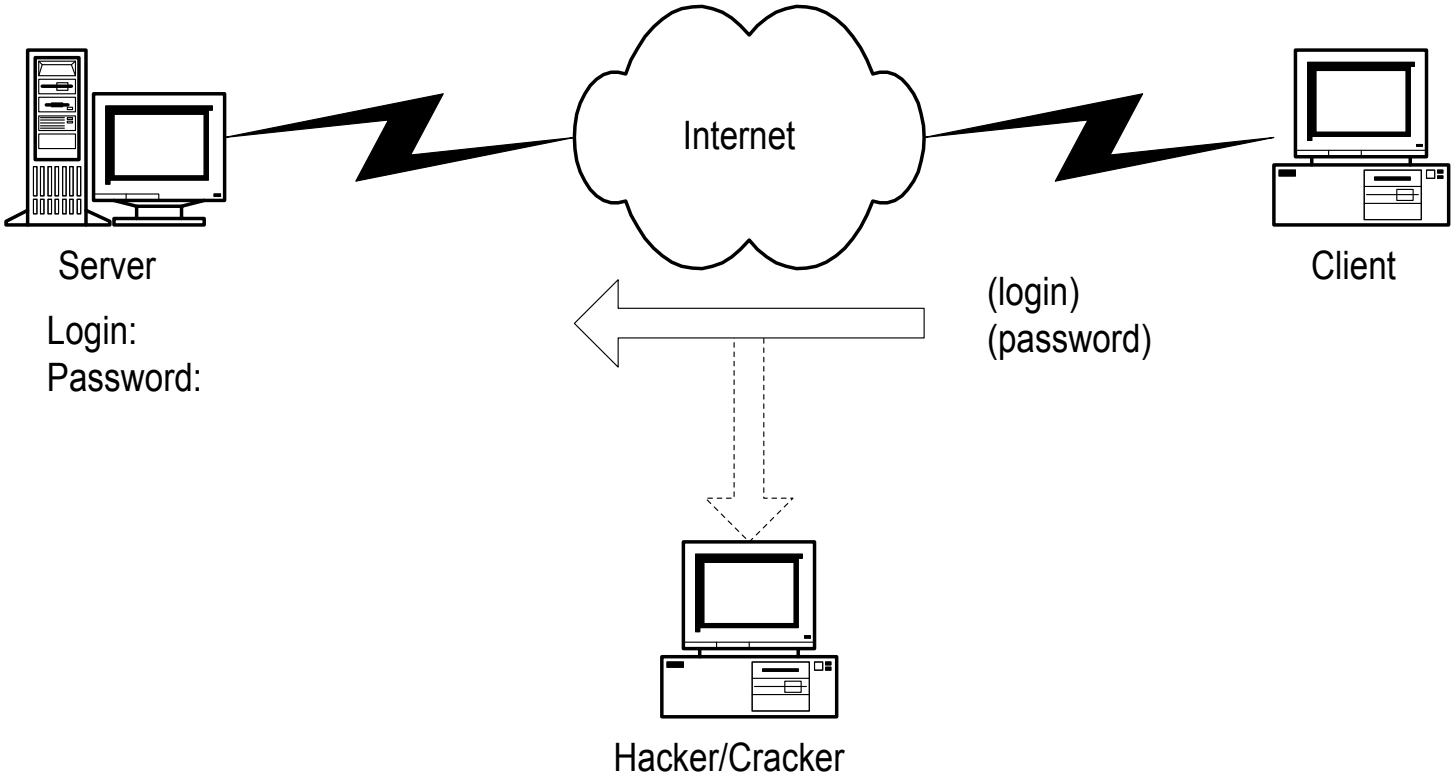
□□□□□□□□□□□□□□ © □□□□□□ 2542

□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□

One-Time Password

- [illegible] telnet/ftp [illegible] Login [illegible] [illegible] [illegible] [illegible] [illegible]
- [illegible] [illegible] [illegible] [illegible] [illegible] Sniffer

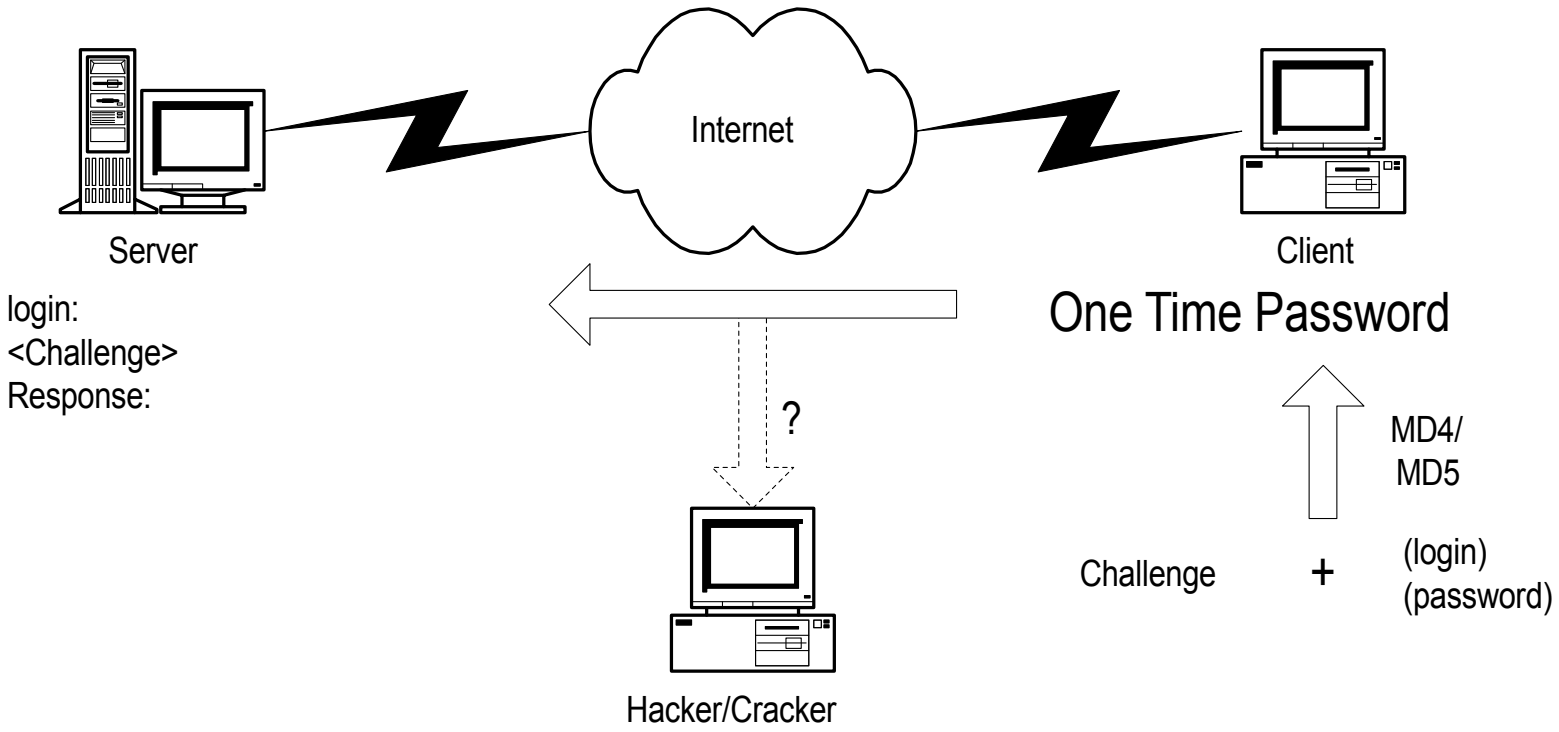
□□□ telnet/ftp □□□□



□□□□□□□□□□□□□□□ © □□□□□□□ 2542

□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□

□□□ telnet/ftp □□□□ One-Time Password



□□□□□□□□□□□□□□ © □□□□□□ 2542

□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□

One-Time-Password

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

□□□□□□□□□□□□ Linux-SIS 3

- □□□□□□□□□□□□□□□□ source
  - cd /usr/local/src/opie-2.32
  - make install
  - opiepasswd □□□□□□□□□□□□□ OTP □□□ □□□□□□□□□□□□□□□□□□□□□ □□
- OTP Password □□□□□□□□□□□□□ □□□ UNIX Password

□□□□□□□□□□□□□□ © □□□□□□ 2542
□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□

[illegible]

- [illegible] OPIE OTP [illegible] [illegible] [illegible] telnet
- [illegible] Winkey [illegible] [illegible] Client PC