

# **LINUX OS HARDENING**

- ① Learning LINUX**
- ② Disk&Package Selection**
- ③ Harden Kernel**
- ④ First Audit**
- ⑤ Apply Patch**
- ⑥ Harden User and File**

# **LINUX OS HARDENING**

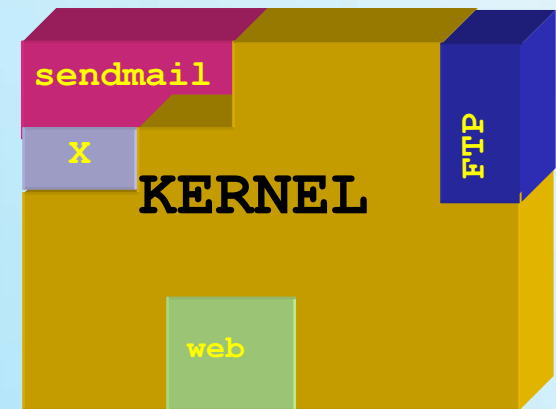
**⑦ Harden Service**

**⑧ Second Audit**

**⑨ Useful Tools : Tripwire , NTP**

# Step 1: Learning LINUX

□ **LINUX Distribution**  
= **LINUX KERNEL** +  
**Software Package**



## Link

<http://www.distrowatch.com/top.php>

<http://www.linux.org/dist/>

## **Step 2: Disk & Package Selection**

- 2.1 Disk Partition**
- 2.2 Package Selection**
- 2.3 Boot/Shutdown Harden**

## Step 2.1: Disk Partition

Depend on your server and idea.

Guide :

- **Swap** = 2 x RAM
- **/** : small as possible
- **/var** : size depend on your log system
- **/tmp** , **/usr/tmp** and **/var/tmp** : small as possible
- **/usr** : Default OS and system utilities
- **/usr/local** : Additional utilities

## Step 2.1: Disk Partition

- **Example :**

– <b>hda1</b>	<b>/</b>	<b>128Mb</b>
– <b>hda2</b>	<b>/tmp</b>	<b>128Mb</b>
– <b>hda3</b>	<b>/var</b>	<b>256Mb</b>
– <b>hda5</b>	<b>/usr</b>	<b>1024Mb</b>
– <b>hda6</b>	<b>swap</b>	<b>2 x RAM</b>
– <b>hda7</b>	<b>/opt or /home</b>	<b>rest-of-disk</b>

## Step 2.2: Package Selection

### Package Selection :

- **NOT** default install
- **NOT** use **NOT** install : **CHOOSE ONLY YOU WANT !!!**

## Step 2.2: Package Selection

### □ More Secure Package :

- Problem of Buffer Over Flow
- Use BOF-protected compiler

- **Libsafe** : Harden glibc

<http://www.research.avayalabs.com/project/libsafe/>

- **Stack Guard** : Protect Stack

<http://www.immunix.org/stackguard.html>

## Step 2.2: Package Selection

- **More Secure Package :**
  - **Immunix** package software :
  - Redhat** package compiled by **Stack Guard**.

<http://www.immunix.org/>

## Step 2.3: Boot/Shutdown Harden

- Set Lilo/Grub Password Protect**
- Disable 'Ctrl-Alt-Del' in /etc/inittab**
- Edit /etc/shutdown.allow : only for root**
- Disable Single user**

## Step 3:Harden Kernel

### □ Step by Step :

① Upgrade current stable Kernel :

<http://www.kernel.org>

② Turn off unused kernel options.

③ Turn off kernel modules : **protect kernel root kits**

④ Compile your own custom kernel :

<http://www.linuxdoc.org/HOWTO/Kernel-HOWTO.html>

## Step 3: Harden Kernel

### ❑ Step by Step (cont.):

#### ⑤ Install Secure Patch Kernel :**Stop Hacker at Kernel.**

##### ❑ OpenWall

<http://www.openwall.com/linux/>

##### ❑ LIDS (LINUX Intrusion Detection system)

<http://www.openwall.com/linux/>

##### ❑ LSM (LINUX Security Modules)

<http://lsm.immunix.org/>

## Step 3: Harden Kernel

### OpenWall

<http://www.openwall.com/linux/>

### Feature

- Non-executable user stack area.
- Secured /tmp.
- Restricted writes into unowned FIFOs.
- Secure /proc.
- Secured SUID binaries.

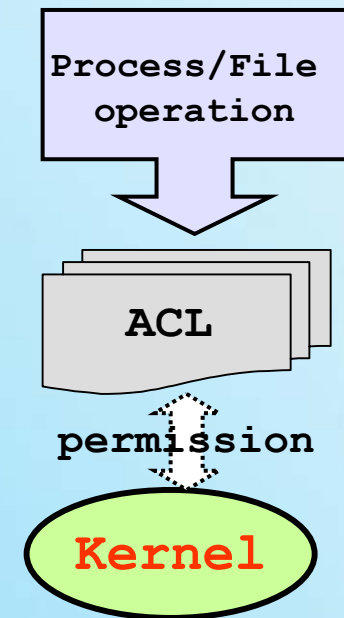
## Step 3: Harden Kernel

### ❑ LIDS

[www.lids.org](http://www.lids.org)

### ❑ Feature

- ❑ Protection of files.
- ❑ Protection of process.
- ❑ Control with Access Control List.
- ❑ Security alert from the kernel.
- ❑ Port scanner detector in kernel.



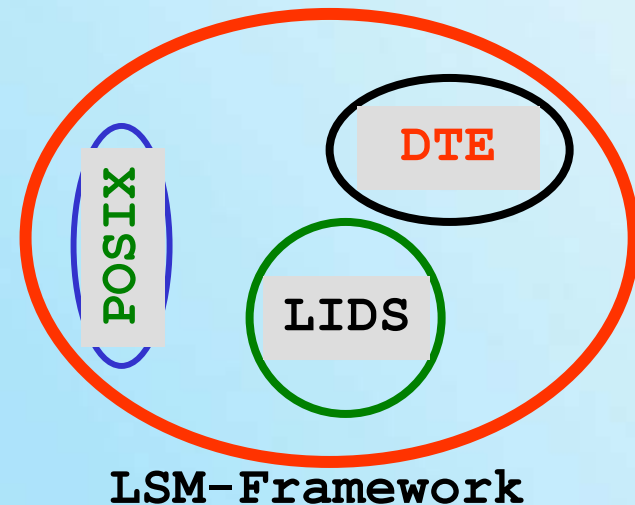
## Step 3: Harden Kernel

### □ LSM

<http://lsm.immunix.org/>

### □ Feature

- Framework for secure kernel module(i.e. LIDS ,DTE etc.).



## Step 4: First Audit

### Why ?

- Know current system
- Close that hole
- keep to history

### What ?

- File Audit
- Network Audit
- User Audit
- Vulnerability Audit

## Step 4: First Audit

### □ How ?

#### □ File and User audit :

##### □ LSAT(LINUX Security Audit Tool)

<http://usat.sourceforge.net/>

##### □ TARA(New Tiger)

<http://www-arc.com>

#### □ Network Audit : Check Sniffer

```
# ifconfig -v | grep -i promisc
```

#### □ Vulnerability Audit : nmap ,nessus ,SARA

## Step 4: First Audit

### □ Vulnerability Audit :

**nmap**

<http://www.nmap.org>

**nessus**

<http://www.nessus.org>

**SARA**

<http://www-arc.com>

## Step 5: Apply Patch

### □ Where I get theirs ?



**Caldera:** <http://www.caldera.com/support/security>



**Debian:** <http://www.debian.org/security>



**Mandrake:** <http://www.linux-mandrake.com/en/security>



**Redhat:** <http://www.redhat.com/support/errata>



**Slackware:** <http://www.slackware.com/changelog/>



**TLE:** <http://linux.thai.net/linux-tle/index.php?menu=info>



**SIS:** <http://www.nectec.or.th/linux-sis/>

## Step 5: Apply Patch

### TODO ?

- Auto Update
- Manual Patch

# Step 5: Apply Patch

## TODO ?

### – Auto Update



**Redhat : up2date command**



**Debian : apt command**



**Caldera : cupdate , kupdate command**



**TLE : apt command**

## Step 5: Apply Patch



### Redhat up2date step by step

① up2date connection : **Keep Watching !!**

- Host xmlrpc.rhn.redhat.com ,Port https

② Register by:

```
#rhn_register
```

③ Import RPM-GPG-KEY:

```
#gpg -import/usr/share/rhn/RPM-GPG-KEY
```

④ run up2date:

```
#up2date -u
```

## Step 5: Apply Patch



### Debian apt step by step

① apt connection : **Keep Watching !!**

- Host security.debian.org ,Port http

② Register at

<http://www.debian.org/security>

## Step 5: Apply Patch



### Debian apt step by step

③ edit /etc/apt/sources.list : add line

```
deb http://security.debian.org potato/updates main contrib non-free
```

④ run apt command

```
# apt-get dist-upgrade  
# apt-get update  
# apt-get upgrade
```

# Step 5: Apply Patch



## TLE apt step by step

① apt connection : **Keep Watching !!**

- Host opensource.thai.net ,Port ftp

② run apt command

```
# apt-get update  
# apt-get upgrade
```

<http://linux.thai.net/linux-tle/index.php?menu=info>

## Step 5: Apply Patch

### TODO (cont.)?

- **Manual Patch** : **Should to verify software before install !!.**
- **How to verify software:**
  - md5 checksum
  - PGP,GPG verify
  - RPM package verify

## Step 5: Apply Patch

### □ md5 checksum

```
# md5sum apache_1.3.26.tar.gz
```

```
52e9b875597a208fca9d393e710087b6  
  apache_1.3.26.tar.gz
```

```
# more apache_1.3.26.tar.gz.md5
```

```
MD5 (apache_1.3.26.tar.gz) =  
  52e9b875597a208fca9d393e710087b6
```

## Step 5: Apply Patch

### PGP,GPG verify

#### Import Key

```
# gpg --import keys.apache_1.3.26
```

#### Verify package

```
# gpg apache_1.3.26.tar.gz.asc
```

```
gpg: Signature made 19 July 2002, 01:25:36
```

```
ICT using DSA key ID 08C975E5
```

```
gpg: Good signature from "Jim Jagielski
```

```
<jim@apache.org>"
```

```
Fingerprint: 8B39 757B 1D8A 994D F243 3ED5
```

```
8B3A 601F 08C9 75E5
```

## Step 5: Apply Patch

### ❑ RPM package verify

#### ❑ Import RPM-GPG-Key

```
# gpg --import RPM-GPG-KEY
```

#### ❑ Verify RPM package

```
# rpm -Kv apache-1.3.22-5.6.i386.rpm
```

```
apache-1.3.22-5.6.i386.rpm:
```

```
MD5 sum OK: 272ec62194bc45ace491f58c91ffcc9b
```

```
gpg: Signature made 20 July 2002, 05:23:45 ICT using DSA  
key ID DB42A60E
```

```
gpg: Good signature from "Red Hat, Inc  
<security@redhat.com>"
```

```
Fingerprint: CA20 8686 2BD6 9DFC 65F6 ECC4 2191 80CD  
DB42 A60E
```

# Step 6: Harden User and File

- 6.1 Harden User**
- 6.2 Harden File**

# Step 6.1: Harden User

## ❑ User Check List

### ① Eliminate Accounts

❑ No password User

❑ Default User

❑ User with Single Command

```
who:x:1000:100::/tmp:/usr/bin/who
```

❑ Easy Password

### ② Set Expire Password

## Step 6.1: Harden User

### ❑ User Check List (cont.)

③ Set Quota disk for user

④ Use sudo

⑤ User login action : Edit /etc/login.defs

```
FAIL_DELAY          10
FAILLOG_ENAB        yes
LOG_UNKFAIL_ENAB    yes
SYSLOG_SU_ENAB      yes
SYSLOG_SG_ENAB      yes
MD5_CRYPT_ENAB      yes
```

⑥ Root account Policy

## Step 6.2:Harden File

### □ File Check List

① **chmod 1777 /tmp ,/usr/tmp**

② **chmod 554 /sbin ,/usr/sbin**  
**/usr/local/sbin : don't allow world**  
**execute**

③ **Remove setuid on some ( most all ) of**  
**the applications**

## Step 6.2: Harden File

### □ File Check List (cont.)

④ Add missing(empty) user files: `.rhosts`  
`, .forward , .plan`

⑤ use `chattr/lsattr` for :

□ Append only for logfile

```
# chattr +a /var/log/secure
```

□ Unmodified for import  
file(`/etc/password`)

```
# chattr +i /etc/password
```

## **Step 7: Harden Service**

- 7.1 Harden Daemon/Service**
- 7.2 Configure Inetd ,Xinetd**
- 7.3 Hardening Script**

## Step 7.1: Harden Daemon/Service

- ❑ **Disable unused daemons from the startup scripts in /etc/rc.d/\***
- ❑ **Normal daemon to keep :**
  - **kernelld**
  - **keytable**
  - **random**
  - **rawdevices**
  - **crond**
  - **syslogd**
  - **network**
  - **sshd**
  - **autofs or amd**
  - **apcd**

## Step 7.1: Harden Daemon/Service

### ❑ Disable Clear-Text Service , Enable Encrypt Service

Telnet	=>	ssh
Ftp	=>	sftp
Imap	=>	Imap+SSL
Pop	=>	Pop+SSL
Smtpt	=>	Smtpt+SSL

### ❑ Use Private IPs to connect in DMZ

## Step 7.2: Configure Inetd ,Xinetd

### Inetd config:

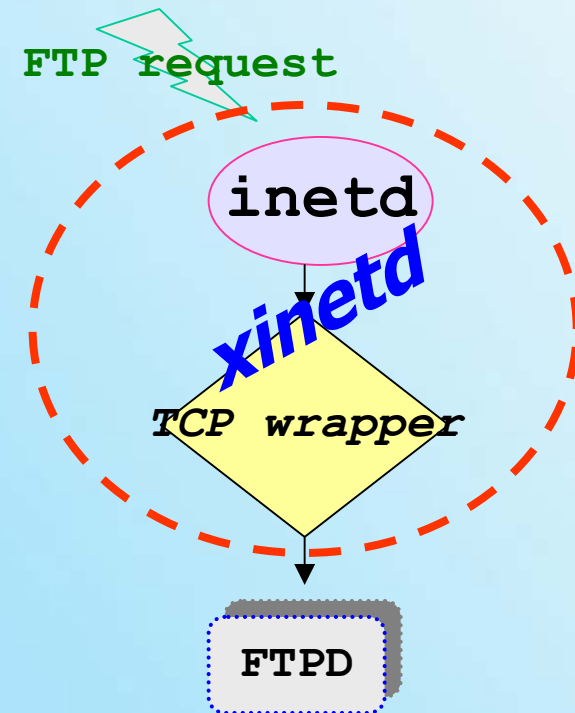
- Comment unused service in  
`/etc/inetd.conf`
- Set deny, allow IPs : `/etc/hosts.deny` ,  
`/etc/hosts.allow`
- Set Secure Permission : read mode(640)  
and `unmodify(chattr +i)` for `/etc/inetd.conf`,  
`/etc/hosts.allow`, `/etc/hosts.deny`

## Step 7.2: Configure Inetd ,Xinetd

### More Secure with Xinetd

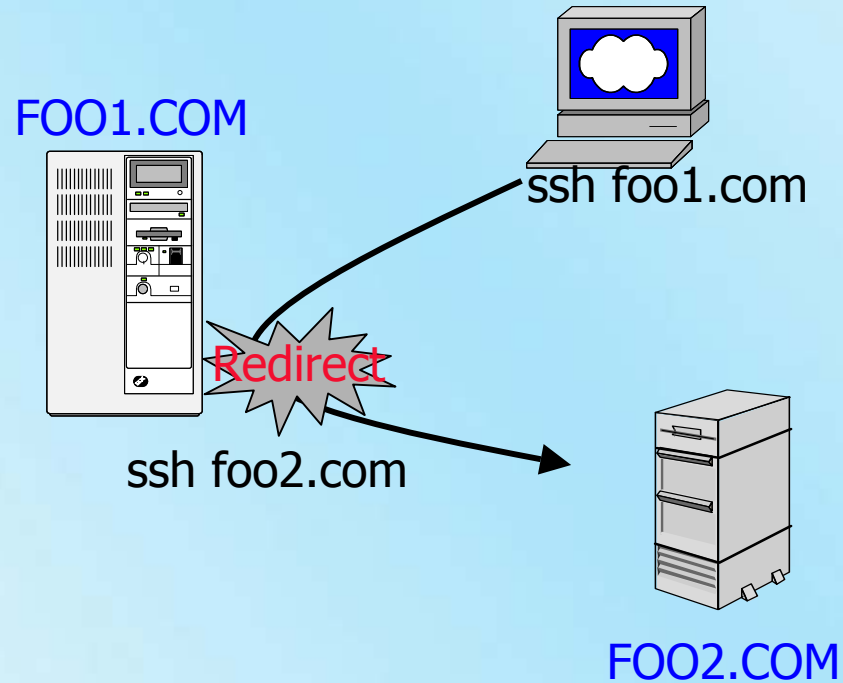
### Features

- More Access Control  
: Control access time
- DOS Protect  
: Control Resources
- Own Log ability
- Redirect and Bind



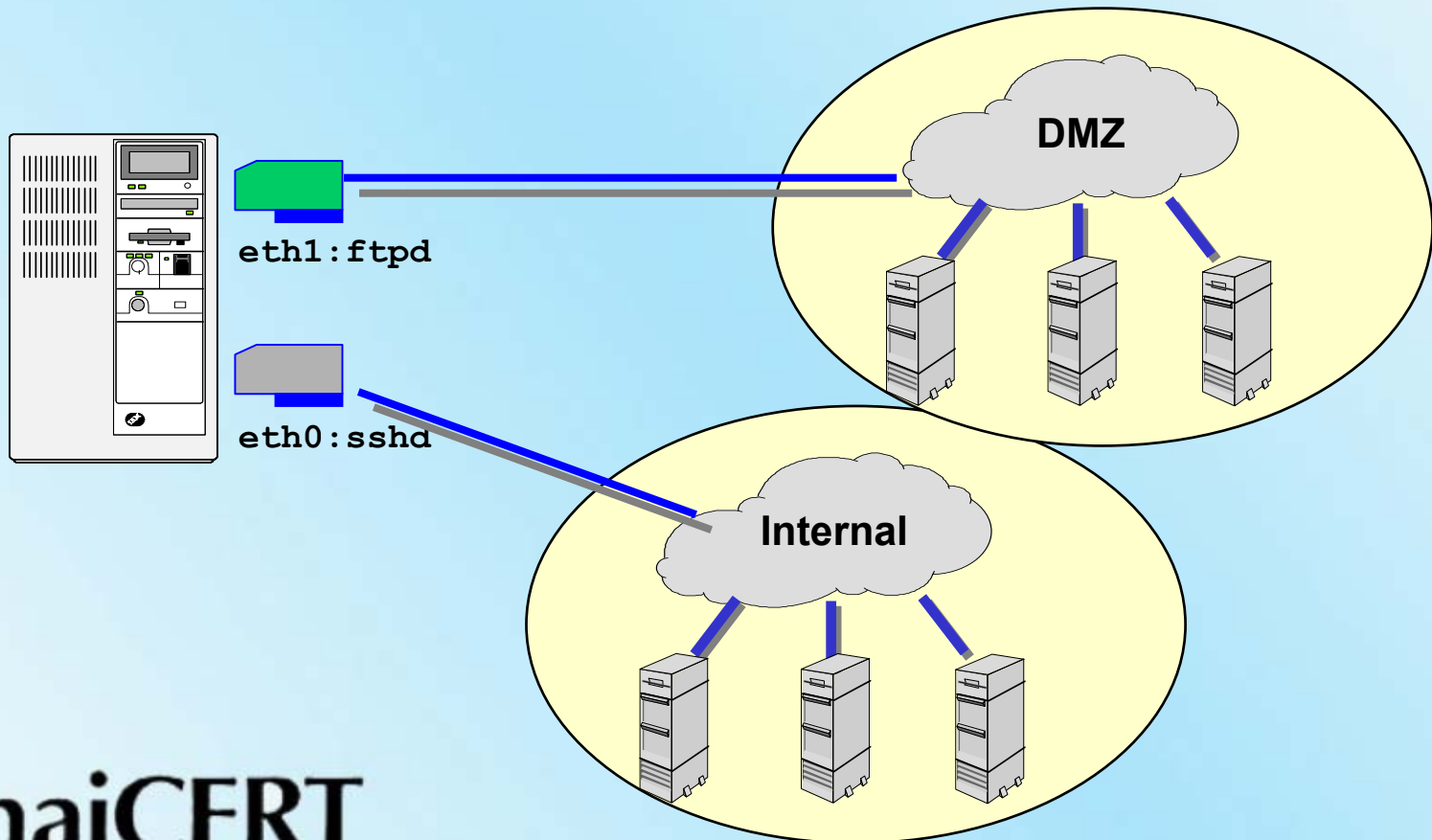
# Step 7.2: Configure Inetd ,Xinetd

## xinetd **redirect** on ssh service



# Step 7.2: Configure Inetd ,Xinetd

xinetd **bind** :ftpd and sshd



## Step 7.3:Hardening Script

- ❑ *OH.. I can not remember all of steps !!!*
- ❑ **Bastille** : Mandrake / RedHat / HP / Debian / SuSE /TurboLinux  
<http://www.bastille-linux.org/>
- ❑ **SASTK** : Slackware  
<http://www.sastk.org/>

## **Step 8: Second Audit**

- Use Tools Like Step 5**
- Compare result between First and this audit result**
- Re-harden**
- Keep to History**

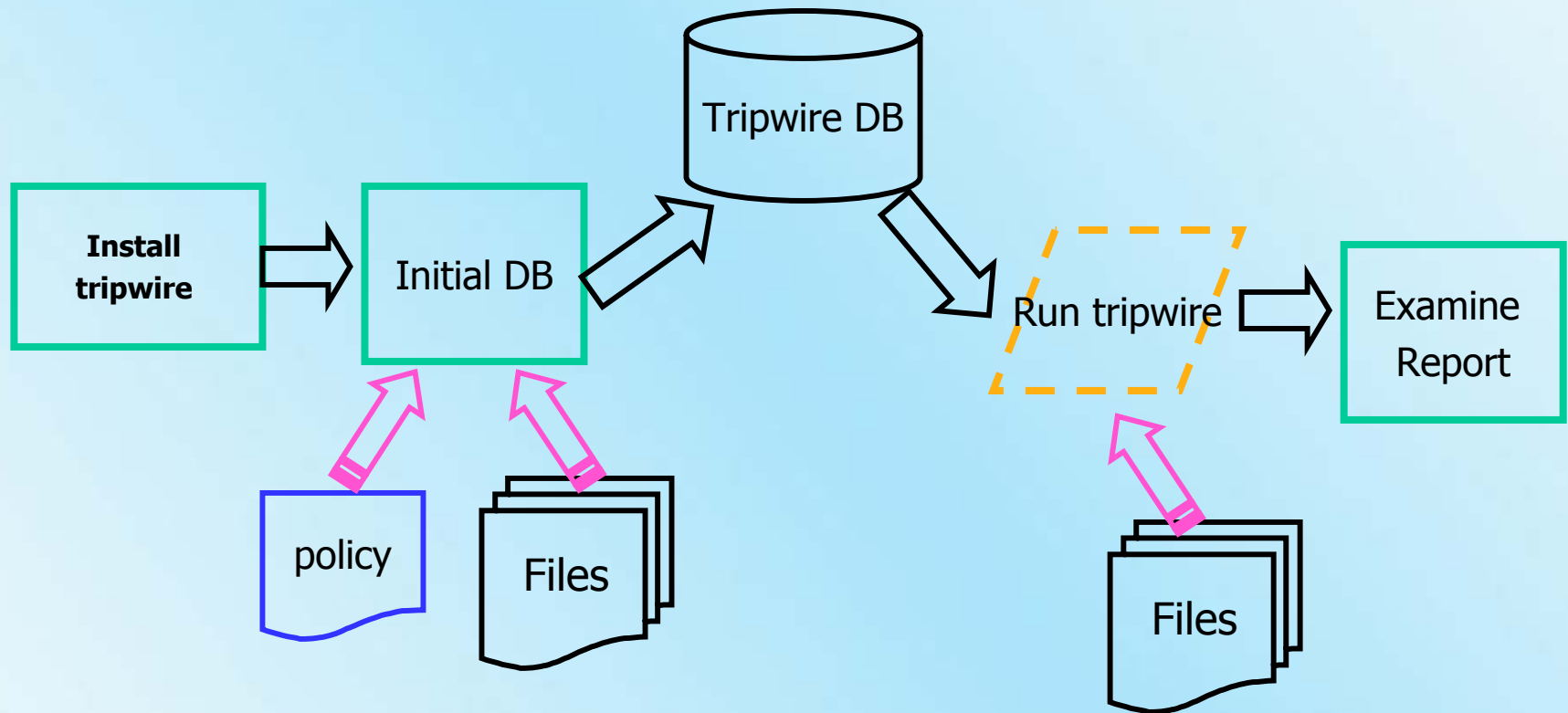
## Step 9: Useful Tools

- 9.1 Tripwire
- 9.2 NTP

## Step 9.1: Tripwire

- Integrity assessment on files.
- Protect Trojan horse, worm.
- Files + check sum -> Tripwire Database

# Step 9.1: Tripwire Flow



## Step 9.1: Tripwire

- ❑ **More Secure in tripwire**
  - ❑ **Keep tw.pol,db.twd,db.twr in read only media : CD-ROM**
  - ❑ **Encrypt twpol.txt**

## Step 9.1: Tripwire

### □ More Secure in tripwire

#### □ Use script and crontab:

#### □ script :

```
#!/bin/sh
/usr/sbin/tripwire -m c -d
/mnt/floppy/tripwire.twd |mail -s "Tripwire
report" foobar@yahoo.com &
```

#### □ crontab :

```
15 24 * * * run_tripwire
```

## Step 9.2:NTP

- ❑ **NTP (Network Time Protocol)**
  - ❑ **Time server Sync. With GPS**
  - ❑ **Time server -> Client**
- ❑ **Useful**
  - ❑ **Make standard time on each server / workstation**
  - ❑ **Get true time from GPS**
  - ❑ **Logfile analysis**

## Step 9.2:NTP

- ❑ Command **ntpdate** , Daemon **ntpd**
- ❑ Link :  
<http://ntl.nectec.or.th/clock/TimeServer.pdf>
- ❑ **clock.nectec.or.th**

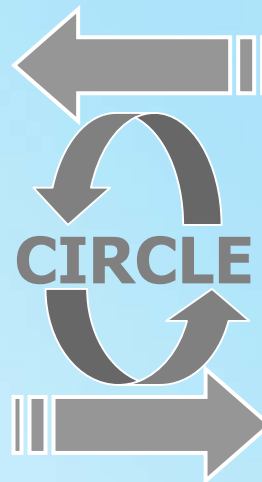
# Harden/Secure

Vender/  
developer

Harden/  
Secure

Prepare /  
Prevent

Detect/  
capture



Improve

Response /  
Recovery