

Nama : Tidhar Katon Birowo
NIM : L200170187
Kelas : A

PRAKTIKUM KEAMANAN JARINGAN KOMPUTER

MODUL 6

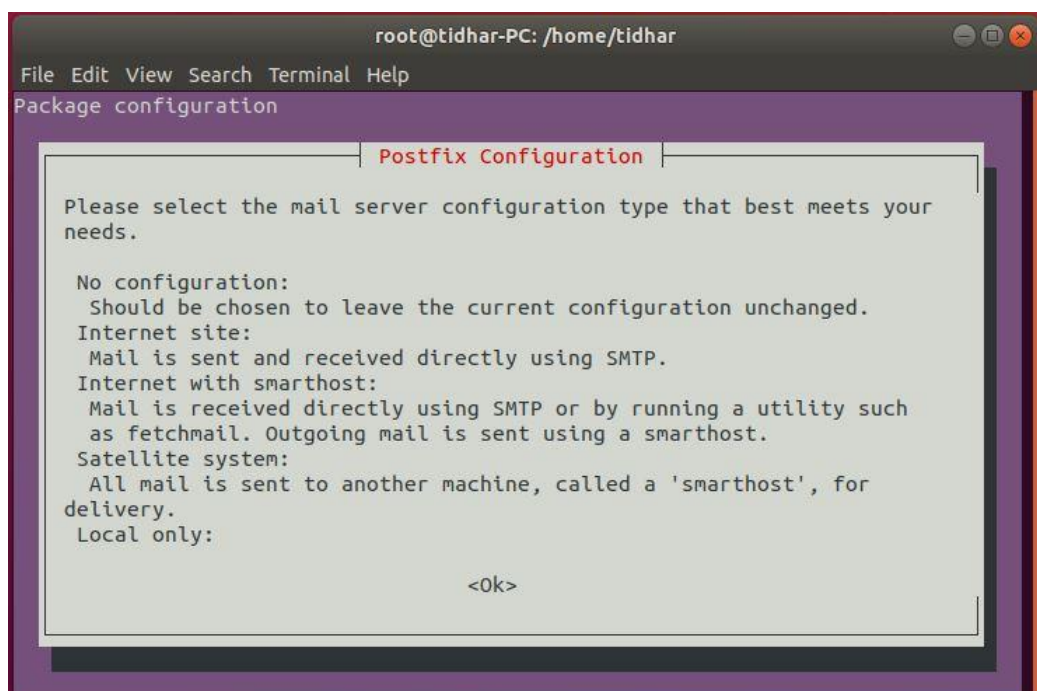
1. Install Tripwire
- Menggunakan perintah “sudo apt-get install tripwire” setelah itu klik Y lalu enter



```
root@tidhar-PC: /home/tidhar
File Edit View Search Terminal Help
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

tidhar@tidhar-PC:~$ sudo su
[sudo] password for tidhar:
root@tidhar-PC:/home/tidhar# sudo apt-get install tripwire
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  postfix
Suggested packages:
  procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb
  postfix-sqlite sasl2-bin dovecot-common resolvconf postfix-cdb postfix-doc
The following NEW packages will be installed:
  postfix tripwire
0 upgraded, 2 newly installed, 0 to remove and 108 not upgraded.
Need to get 2.794 kB of archives.
After this operation, 16,6 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

- Lalu muncul Postfix Configuration Pilih OK



```
root@tidhar-PC: /home/tidhar
File Edit View Search Terminal Help
Package configuration

Postfix Configuration

Please select the mail server configuration type that best meets your
needs.

No configuration:
  Should be chosen to leave the current configuration unchanged.
Internet site:
  Mail is sent and received directly using SMTP.
Internet with smarthost:
  Mail is received directly using SMTP or by running a utility such
  as fetchmail. Outgoing mail is sent using a smarthost.
Satellite system:
  All mail is sent to another machine, called a 'smarthost', for
  delivery.
Local only:

<Ok>
```

Tripwire Configuration

Do you wish to create/use your local key passphrase during installation?

<Yes>

<No>

Tripwire Configuration

Tripwire keeps its configuration in a encrypted database that is generated, by default, from /etc/tripwire/twcfg.txt

Any changes to /etc/tripwire/twcfg.txt, either as a result of a change in this package or due to administrator activity, require the regeneration of the encrypted database before they will take effect.

Selecting this action will result in your being prompted for the site key passphrase during the post-installation process of this package.

Rebuild Tripwire configuration file?

<Yes>

<No>

Tripwire Configuration

Tripwire keeps its policies on what attributes of which files should be monitored in a encrypted database that is generated, by default, from /etc/tripwire/twpol.txt

Any changes to /etc/tripwire/twpol.txt, either as a result of a change in this package or due to administrator activity, require the regeneration of the encrypted database before they will take effect.

Selecting this action will result in your being prompted for the site key passphrase during the post-installation process of this package.

Rebuild Tripwire policy file?

<Yes>

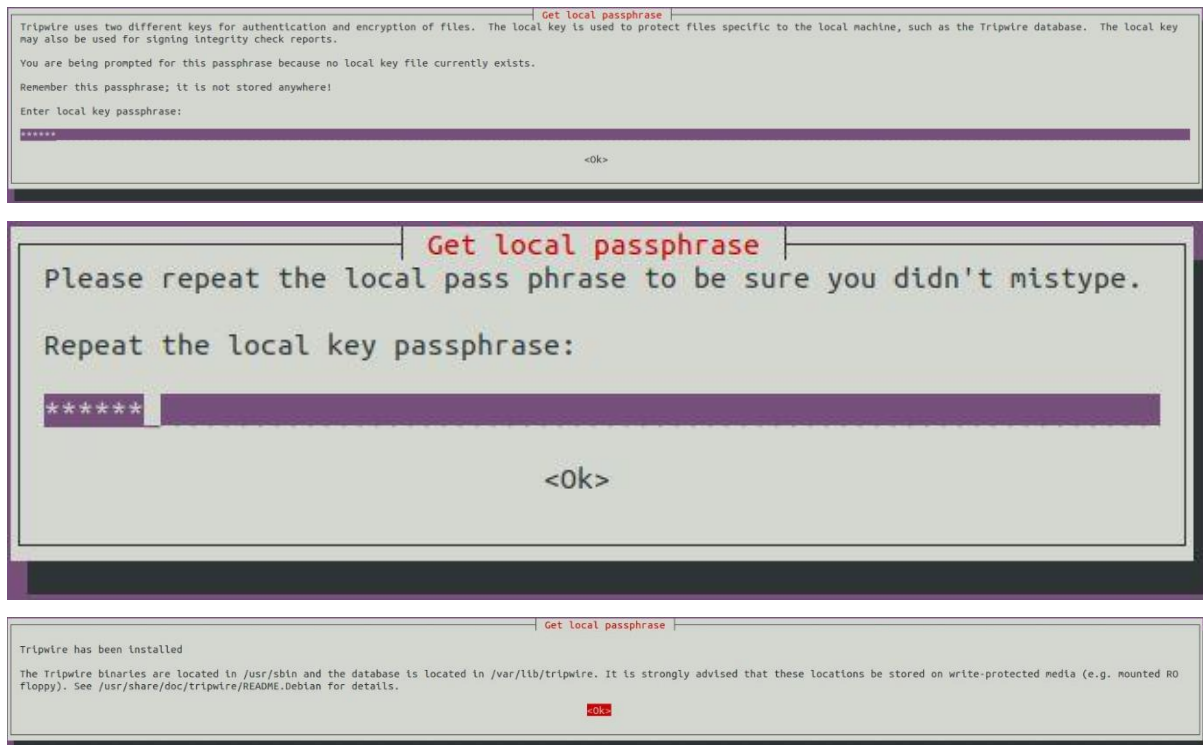
<No>

Get site passphrase

Please repeat the site pass phrase to be sure you didn't mistype.

Repeat the site-key passphrase:

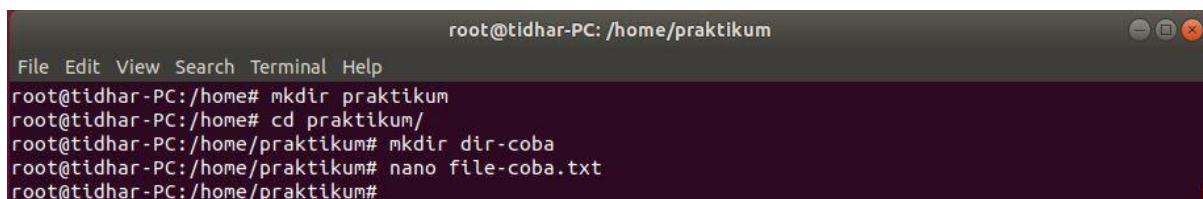
<Ok>



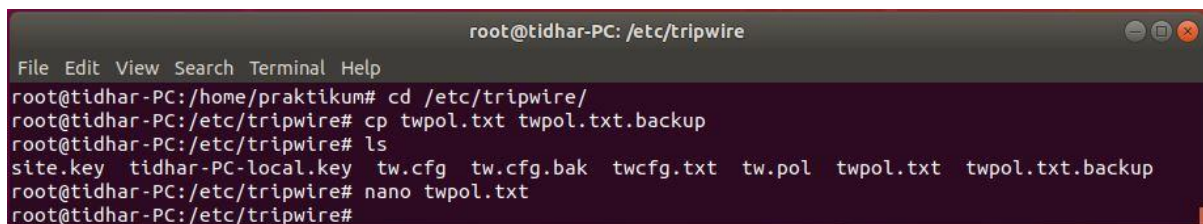
- Untuk meningkatkan keamanan perlu dilakukan enkripsi file konfigurasi
/etc/tripwire/twcfg.txt



2. Inisialisasi database pengecekan Tripwire
 - Buat direktori dan file baru di dalam praktikum



- Copy file twpol sebelum melakukan perubahan



- Melakukan perubahan pada konfigurasi twpol.txt agar hanya direktori /home/percobaan saja yang akan di monitor

```

root@tidhar-PC: /etc/tripwire
File Edit View Search Terminal Help
root@tidhar-PC:/home/praktikum# cd /etc/tripwire/
root@tidhar-PC:/etc/tripwire# cp twpol.txt twpol.txt.backup
root@tidhar-PC:/etc/tripwire# ls
site.key tidhar-PC-local.key tw.cfg tw.cfg.bak twcfg.txt tw.pol twpol.txt twpol.txt.backup
root@tidhar-PC:/etc/tripwire# nano twpol.txt
root@tidhar-PC:/etc/tripwire#

```

- Melakukan perubahan pada konfigurasi twpol.txt agar hanya direktori /home/percobaan saja yang akan di monitor

```

root@tidhar-PC: /etc/tripwire
File Edit View Search Terminal Help
GNU nano 2.9.3 twpol.txt

# Memonitor direktori percobaan
#
(
    rulename = "Direktori Percobaan",
    severity = $(SIG_HI)
)
{
    /home/praktikum -> $(SEC_CRIT) ;
}

```

- Melakukan inisialisasi database dengan perintah

```

root@tidhar-PC: /etc/tripwire
File Edit View Search Terminal Help
root@tidhar-PC:/etc/tripwire# tripwire --init --cfgfile /etc/tripwire/tw.cfg --polfile /etc/tripwire/tw
.pol --site-keyfile /etc/tripwire/site.key --local-keyfile /etc/tripwire/tidhar-PC-local.key

```

- Untuk mengecek sistem terhadap adanya perubahan file-file dalam host gunakan perintah

```

root@tidhar-PC: /etc/tripwire
File Edit View Search Terminal Help
root@tidhar-PC:/etc/tripwire# tripwire --check

```

- Hasilnya

Section: Unix File System				
Rule Name	Severity Level	Added	Removed	Modified
Other binaries	66	0	0	0
Tripwire Binaries	100	0	0	0
Other libraries	66	0	0	0
Root file-system executables	100	0	0	0
* Tripwire Data Files	100	1	0	0
System boot changes	100	0	0	0
Root file-system libraries (/lib)	100	0	0	0
Critical system boot files	100	0	0	0
Other configuration files (/etc)	66	0	0	0
Boot Scripts	100	0	0	0
Security Control	66	0	0	0
Root config files	100	0	0	0
* Devices & Kernel information	100	814	584	0
Invariant Directories	66	0	0	0
Total objects scanned: 150391				

3. Melihat hasil monitoring Tripwire
 - Isi file-coba.txt dengan nama dan nim

```

root@tidhar-PC: /home/praktikum
File Edit View Search Terminal Help
root@tidhar-PC:/home/praktikum# nano file-coba.txt
root@tidhar-PC:/home/praktikum#

```

```

root@tidhar-PC: /home/praktikum
File Edit View Search Terminal Help
GNU nano 2.9.3 file-coba.txt Modified

Nama : Tidhar Katon BIrowo
NIM : L20017087

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      M-U Undo
^X Exit          ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Spell     ^_ Go To Line    M-E Redo

```

- Buat file-coba2.txt dalam direktori dir-coba

```

root@tidhar-PC: /home/praktikum/dir-coba
File Edit View Search Terminal Help
root@tidhar-PC:/home/praktikum# cd dir-coba/
root@tidhar-PC:/home/praktikum/dir-coba# nano file-coba2.txt
root@tidhar-PC:/home/praktikum/dir-coba# LS

Command 'LS' not found, but can be installed with:

apt install sl

root@tidhar-PC:/home/praktikum/dir-coba# ls
file-coba2.txt
root@tidhar-PC:/home/praktikum/dir-coba#

```

- Cek perubahan pada sistem dengan menggunakan perintah tripwire --check

```

root@tidhar-PC: /home/praktikum/dir-coba
File Edit View Search Terminal Help
root@tidhar-PC:/home/praktikum/dir-coba# tripwire --check

```

Hasilnya

Section: Unix File System				
Rule Name	Severity Level	Added	Removed	Modified
-----	-----	----	-----	-----
Other binaries	66	0	0	0
Tripwire Binaries	100	0	0	0
Other libraries	66	0	0	0
Root file-system executables	100	0	0	0
* Tripwire Data Files	100	1	0	0
System boot changes	100	0	0	0
Root file-system libraries	100	0	0	0
(/lib)				
Critical system boot files	100	0	0	0
Other configuration files	66	0	0	0
(/etc)				
Boot Scripts	100	0	0	0
Security Control	66	0	0	0
* Root config files	100	0	0	6
* Devices & Kernel Information	100	913	1133	0
Invariant Directories	66	0	0	0
Total objects scanned: 149941				

4. Update file policy tripwire

- Buat direktori praktikum2 di direktori /home

```
root@tidhar-PC: /home
File Edit View Search Terminal Help
root@tidhar-PC:/home/praktikum/dir-coba# cd /home
root@tidhar-PC:/home# mkdir praktikum2
root@tidhar-PC:/home# ls
praktikum praktikum2 tidhar
root@tidhar-PC:/home#
```

- Lakukan perubahan konfigurasi twpool.txt agar direktori /home/praktikum2 juga di monitor oleh tripwire

```
#
# Memonitor direktori percobaan
#
(
  rulename = "Direktori Percobaan",
  severity = $(SIG_HI)
)
{
  /home/praktikum          -> $(SEC_CRIT) ;
  /home/praktikum2        -> $(SEC_CRIT) ;
}
```

- Lakukan update
#tripwire --update-policy --cfgfile ./tw.cfg --polfile ./tw.pol --site-keyfile ./site.key -localkeyfile ./wyne-VirtualBox-local.key ./twpol.txt

```
root@wyne-VirtualBox:/etc/tripwire# tripwire --update-policy --c
file ./tw.cfg --polfile ./tw.pol --site-keyfile ./site.key --loc
-keyfile ./wyne-VirtualBox-local.key ./twpol.txt
```

- Cek perubahan pada sistem dengan perintah

```
root@tidhar-PC: /etc/tripwire
File Edit View Search Terminal Help
root@tidhar-PC:/etc/tripwire# tripwire --check
```

5. Update database tripwire

- Buatlah sebuah file dalam direktori /home/praktikum dengan nama file-coba2.txt

```
root@tidhar-PC: /home/praktikum
File Edit View Search Terminal Help
root@tidhar-PC:/home# cd praktikum
root@tidhar-PC:/home/praktikum# nano file-coba2.txt
root@tidhar-PC:/home/praktikum# ls
dir-coba file-coba2.txt file-coba.txt
root@tidhar-PC:/home/praktikum#
```

- Cek perubahan pada sistem dengan perintah

```
root@tidhar-PC: /etc/tripwire
File Edit View Search Terminal Help
root@tidhar-PC:/etc/tripwire# tripwire --check
```

- Sebelum melakukan update database, sesuaikan file report tripwire dengan menjalankan perintah
#/usr/sbin/tripwire --update --twrfile /var/lib/tripwire/report/nama-file.twr

```
root@tidhar-PC: /home/praktikum
File Edit View Search Terminal Help
root@tidhar-PC:/home/praktikum# /usr/sbin/tripwire --update twrfile /var/lib/tripwire/report/tidhar-20200408-02544.twr
```

- Cek perubahan pada sistem dengan perintah

```
root@tidhar-PC: /etc/tripwire
File Edit View Search Terminal Help
root@tidhar-PC:/etc/tripwire# tripwire --check
```