MODUL 6

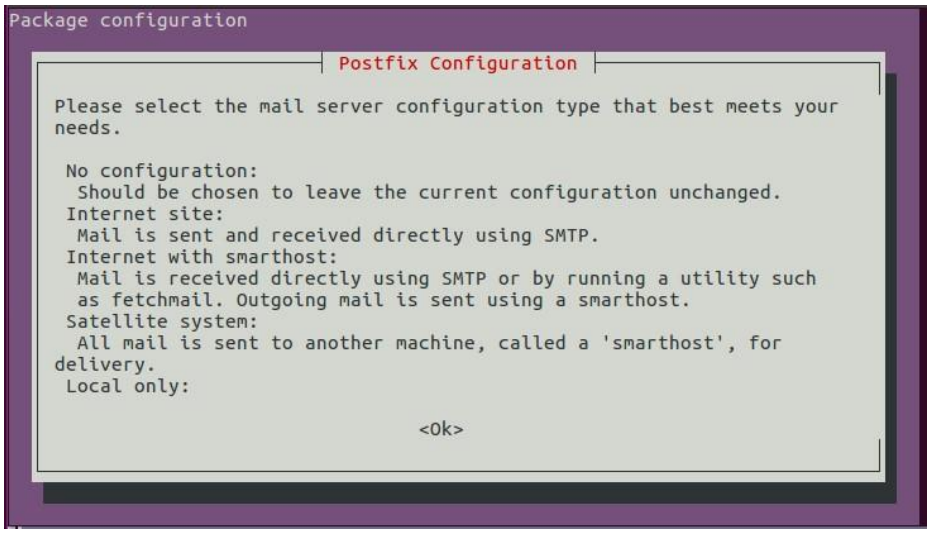
Intrution Detection System (IDS)

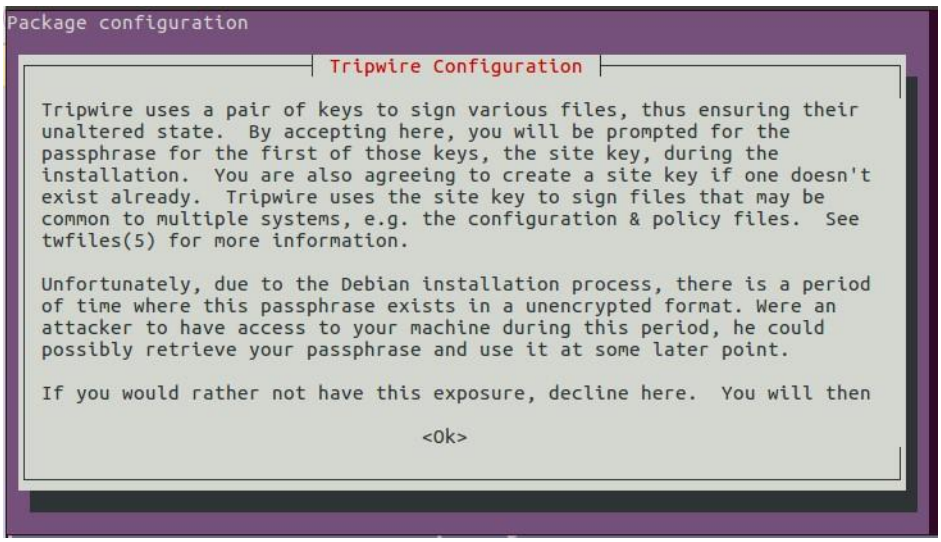
Berlian Edra / L200164013

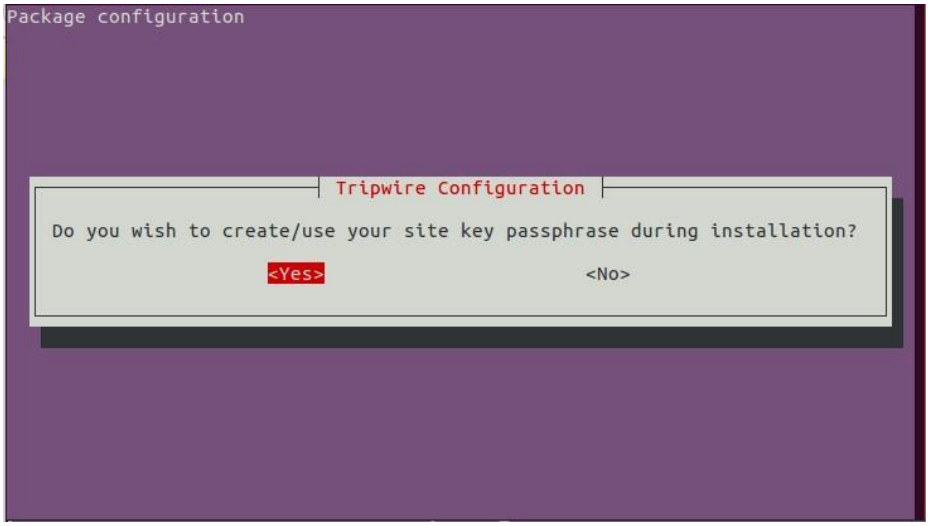
---

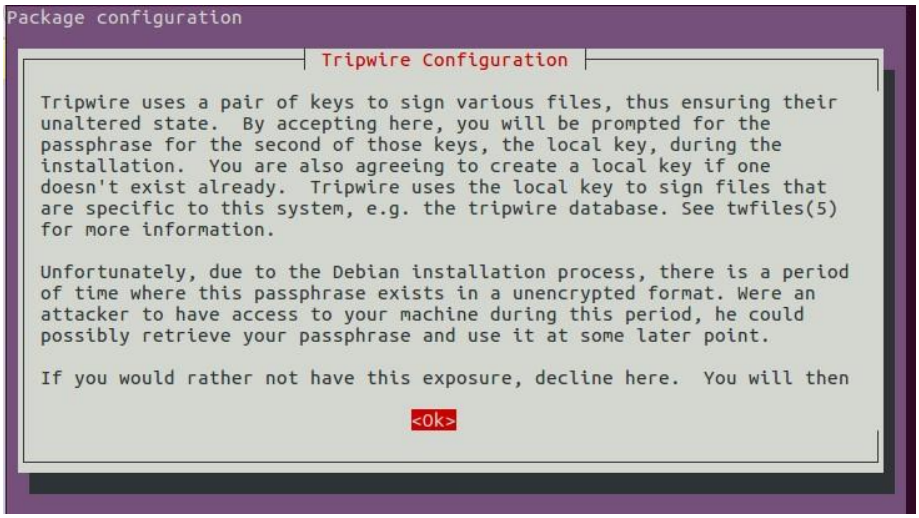
1. Install tripwire

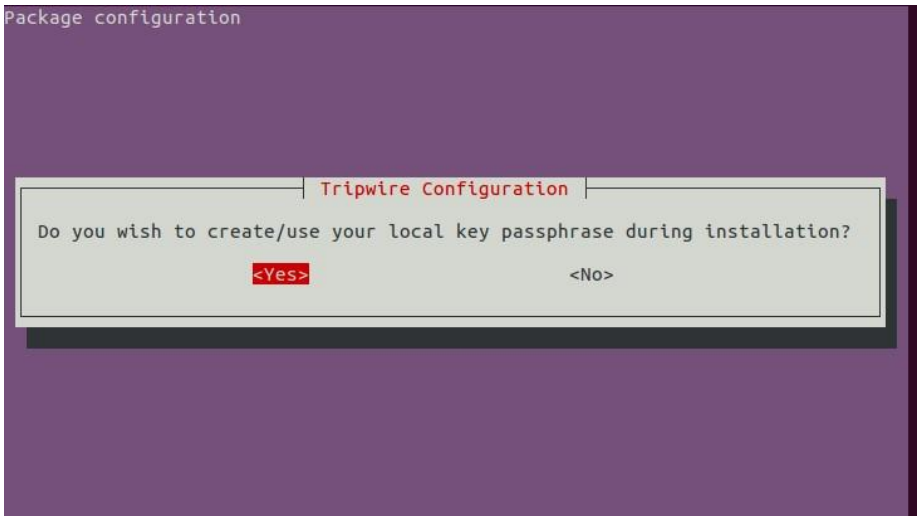
```
root@wyne-VirtualBox:/# apt-get install tripwire
```

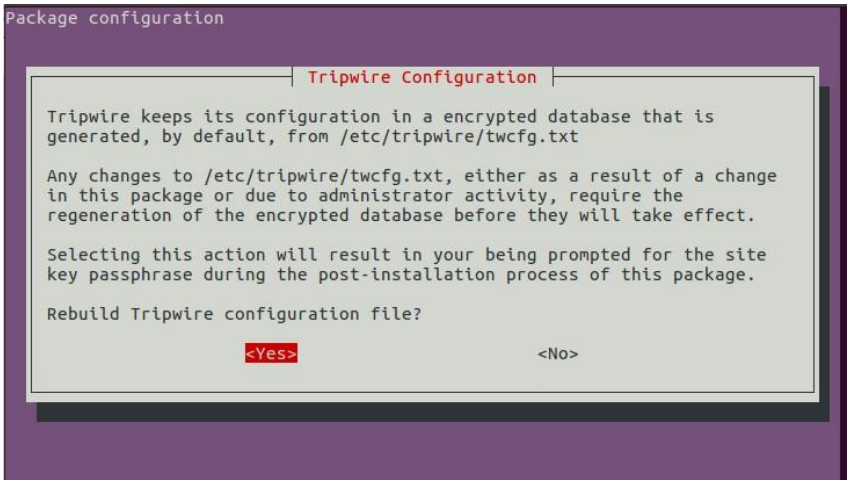


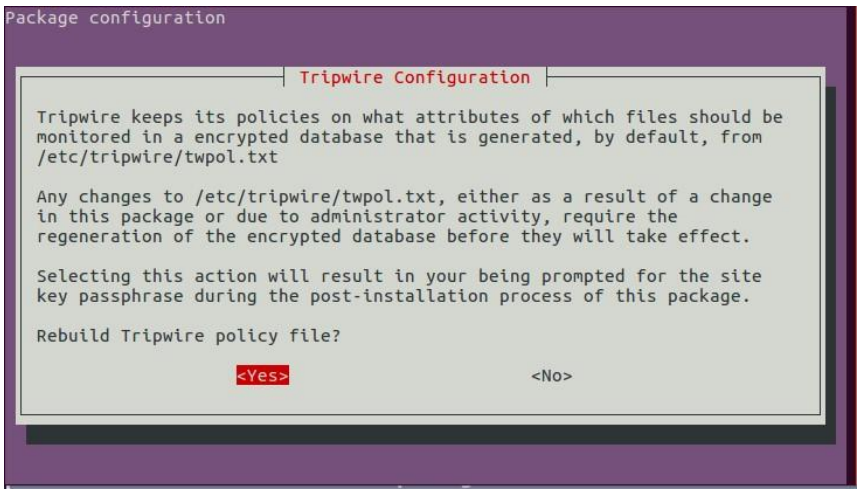


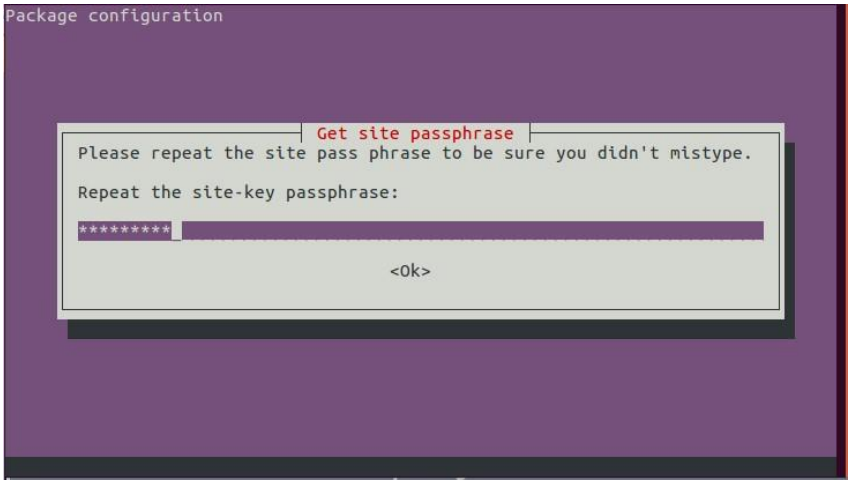

Package configuration
Tripwire Configuration
Do you wish to create/use your site key passphrase during installation?
<Yes>
<No>

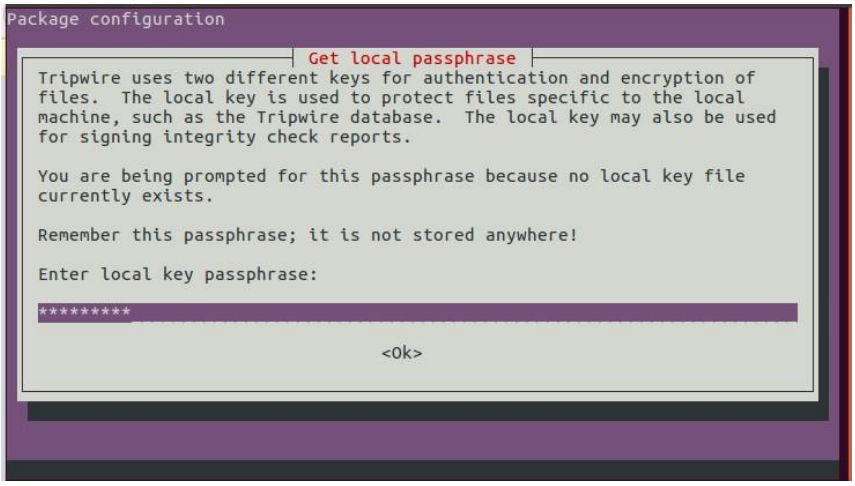

Package configuration
Tripwire Configuration
Tripwire uses a pair of keys to sign various files, thus ensuring their unaltered state. By accepting here, you will be prompted for the passphrase for the second of those keys, the local key, during the installation. You are also agreeing to create a local key if one doesn't exist already. Tripwire uses the local key to sign files that are specific to this system, e.g. the tripwire database. See twfiles(5) for more information.
Unfortunately, due to the Debian installation process, there is a period of time where this passphrase exists in a unencrypted format. Were an attacker to have access to your machine during this period, he could possibly retrieve your passphrase and use it at some later point.
If you would rather not have this exposure, decline here. You will then
<Ok>

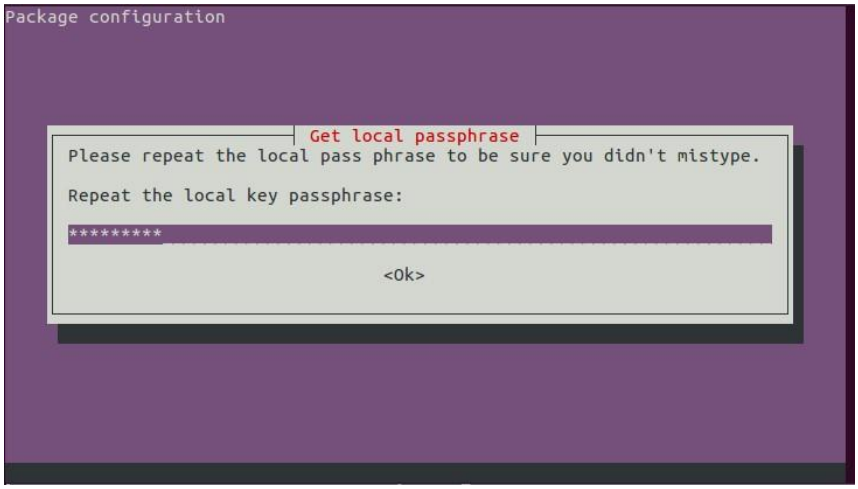

Package configuration
Tripwire Configuration
Do you wish to create/use your local key passphrase during installation?
<Yes>
<No>


Package configuration
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>


Package configuration
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>


Package configuration
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/triwpire/twcfg.txt

```
root@wyne-VirtualBox:/etc/tripwire# twadmin --create-cfgfile --cfgf
ile ./tw.cfg --site-keyfile ./site.key ./twcfg.txt
Please enter your site passphrase:
```

2. Inisialisasi database pengecekan tripwire
   - Buat direktori baru

```
root@wyne-VirtualBox:/home# mkdir praktikum
root@wyne-VirtualBox:/home# ls
praktikum  wyne
```

   - Buat direktori dan file baru di dalam praktikum

```
root@wyne-VirtualBox:/home# cd praktikum/
root@wyne-VirtualBox:/home/praktikum# mkdir dir-coba
root@wyne-VirtualBox:/home/praktikum# nano file-coba.txt
```

   - Copy file twpol sebelum melakukan perubahan

```
root@wyne-VirtualBox:/etc/tripwire# cp twpol.txt twpol.txt.backup
root@wyne-VirtualBox:/etc/tripwire# ls
site.key    twcfg.txt   twpol.txt
tw.cfg      tw.pol      twpol.txt.backup
tw.cfg.bak  tw.pol.bak  wyne-VirtualBox-local.key
```

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

```
root@wyne-VirtualBox:/etc/tripwire# nano twpol.txt
```

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

- Melakukan inisialisasi database dengan perintah

```
root@wyne-VirtualBox:/etc/tripwire# tripwire --init --cfgfile /etc/
tripwire/tw.cfg --polfile /etc/tripwire/tw.pol --site-keyfile /etc/
tripwire/site.key --local-keyfile /etc/tripwire/wyne-VirtualBox-loc
al.key
Please enter your local passphrase:
```

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

```
root@wyne-VirtualBox:/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      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        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@wyne-VirtualBox:/# cd /home/praktikum/
root@wyne-VirtualBox:/home/praktikum# nano file-coba.txt
```

```
  GNU nano 2.5.3        File: file-coba.txt

Nama : Wyne HAbsari
NIM : L200160080
```

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

```
root@wyne-VirtualBox:/home/praktikum# cd dir-coba/
root@wyne-VirtualBox:/home/praktikum/dir-coba# nano file-coba2.txt
root@wyne-VirtualBox:/home/praktikum/dir-coba# ls
file-coba2.txt
```

- Cek perubahan pada sistem dengan perintah

```
root@wyne-VirtualBox:/# cd etc/tripwire/
root@wyne-VirtualBox:/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      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@wyne-VirtualBox:/# cd home/
root@wyne-VirtualBox:/home# mkdir praktikum2
root@wyne-VirtualBox:/home# ls
praktikum  praktikum2  wyne
```

- Lakukan perubahan konfigurasi twpool.txt agar direktori /home/praktikum2 juga dimonitor 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@wyne-VirtualBox:/etc/tripwire# tripwire --check
```

5. Update database tripwire
   - Buatlah sebuah file dalam direktori /home/praktikum dengan nama file-coba2.txt

```
root@wyne-VirtualBox:/# cd home/praktikum
root@wyne-VirtualBox:/home/praktikum# nano file-coba2.txt
root@wyne-VirtualBox:/home/praktikum# ls
dir-coba  file-coba2.txt  file-coba.txt
```

   - Cek perubahan pada sistem dengan perintah

```
root@wyne-VirtualBox:/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@wyne-VirtualBox:/# /usr/sbin/tripwire --update twrfile /var
ib/tripwire/report/wyne-VirtualBox-20190516-025544.twr
```

   - Cek perubahan pada sistem dengan perintah

```
root@wyne-VirtualBox:/etc/tripwire# tripwire --check
```