6 INTRUTION DETECTION SYSTEM (IDS)

6.1 ALOKASI WAKTU DAN PERSIAPAN

Praktikum ini terdiri dari 5 percobaan, untuk menyelesaikan semua percobaan pada modul ini membutuhkan waktu 200 menit atau dua kali pertemuan. Pada pertemuan pertama dapat dimulai dari percobaan 1 dan 2, kemudian pertemuan berikutnya dilanjutkan percobaan 3, 4 dan 5.

Untuk kelancaran praktikum, asisten praktikum sebaiknya sudah menyiapkan konfigurasi source-list apt agar proses instalasi dapat berjalan dengan lancar. Koneksi jaringan dengan repository sistem operasi Ubuntu juga perlu diperhatikan terutama pada percobaan 1 agar tidak mengganggu jalanya instalasi. Untuk menghindari kemungkinan kesalahan, asisten harus memastikan semua konfigurasi Tripwire belum pernah dilakukan perubahan, jika perlu *remove/uninstall* aplikasi Tripware jika sebelumnya pernah dipasang pada komputer tersebut.

6.2 DASAR TEORI

Untuk melakukan pengawasan secara otomatis terhadap penyusupan pada suatu system adalah dengan menggunakan *Intrution Detection System* (IDS). IDS bekerja dengan cara mendeteksi jenis serangan berdasarkan *signature* atau *pattern* pada aktifitas jaringan, kemudian melakukan blokade terhadap *traffic* atau aktifitas yang mencurigakan.

Tipe IDS secara garis besar dibagi 2, yaitu host base dan network base IDS. Termasuk dalam jenis network base adalah aplikasi Snort, sedangkan yang termasuk model host based adalah tripwire. Aplikasi Tripwire berfungsi untuk menjaga integritas file system dan direktori, yaitu dengan cara mencatat setiap perubahan yang terjadi pada file dan direktori. Dalam modul ini kita hanya akan membahas host base IDS dengan Tripwire.

Tripware dapat dikonfigurasi untuk melakukan pelaporan melalui email bila menemukan perubahan file yang tidak semestinya, selain itu secara otomatis tripware juga dapat melakukan pemeriksaan file secara terjadwal melalui cron. Penggunaan tripwire biasanya digunakan untuk mempermudah pekerjaan yang dilakukan oleh System Administrator dalam mengamankan System.

Prinsip kerja tripwire adalah melakukan perbandingan file dan direktori dengan database yang sudah dibuat berdasarkan file dan direktori sebelum terjadi perubahan. Sehingga apa bila suatu file atau direktori mengalami perubahan, tripwire akan mengetahui perbedaan yang terjadi dengan cara membandingkan dengan database yang dimilikinya. Perbandingan tersebut meliputi perubahan tanggal, ukuran file, penghapusan dan lainnya. Setelah tripwire dijalankan, secara otomatis akan melakukan

pembuatan database sistem. Kemudian secara periodik akan selalu melaporkan setiap perubahan pada file dan direktori.

6.3 TUJUAN

1. Mengenalkan pada mahasiswa tentang konsep integrator cek pada IDS
2. Mampu melakukan installasi, konfigurasi dan memakaai Tripwire sebagai program hostbase IDS dengan sistem integrator Checking

6.4 BAHAN DAN ALAT

1. Siapkan sebuah buah komputer dengan sistem operasi Ubuntu yang terhubung dalam jaringan internet
2. Komputer dapat mengakses repository Ubuntu dengan baik

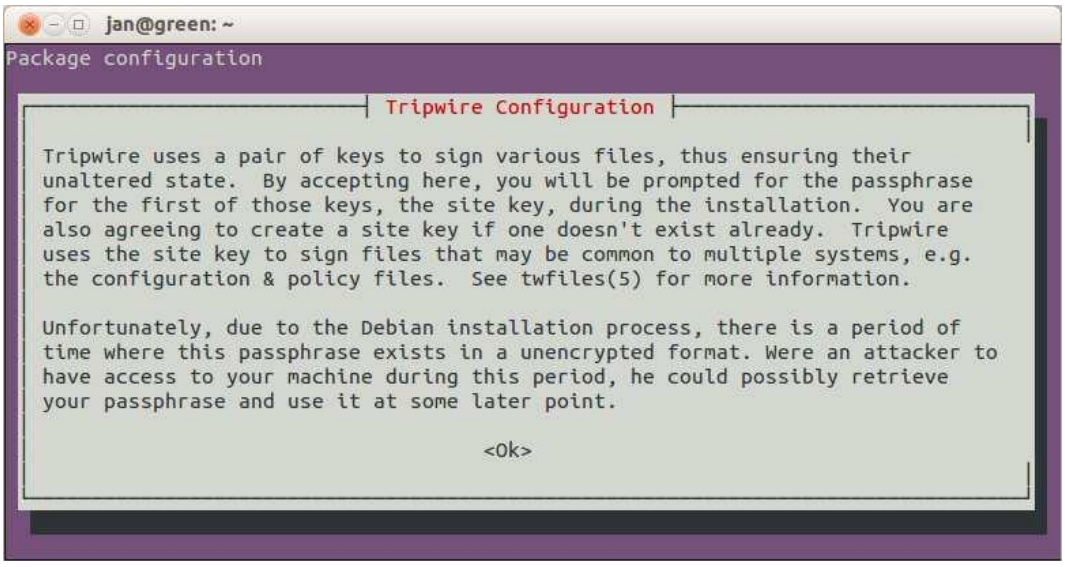
6.5 LANGKAH PERCOBAAN

6.5.1 Percobaan 1: Instalasi dan konfigurasi awal

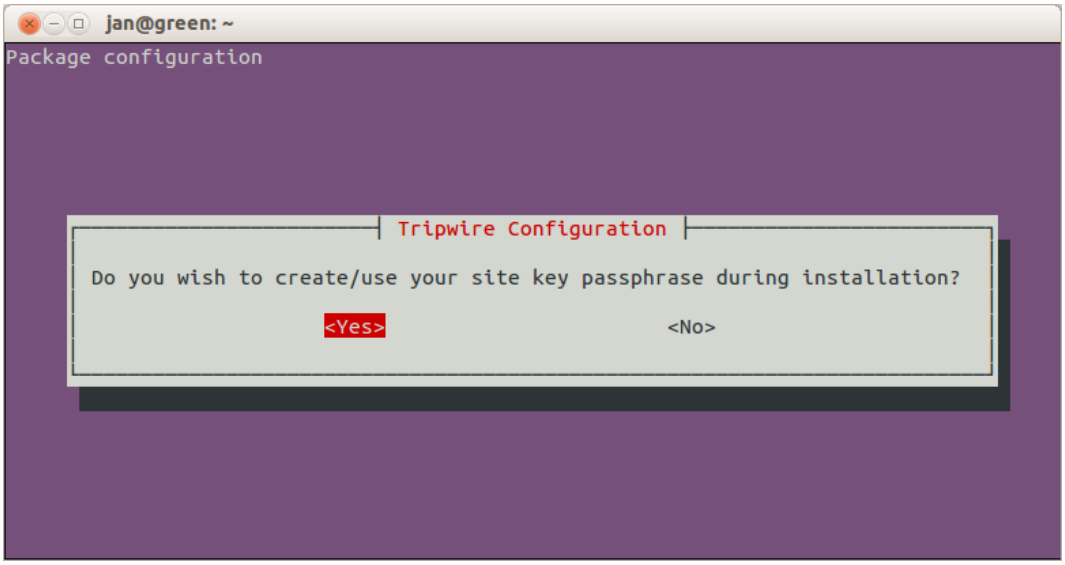
1. Langkah instalasi dimulai dengan membuka terminal dan menginstalnya tripwire dengan perintah

   #apt-get install tripwire

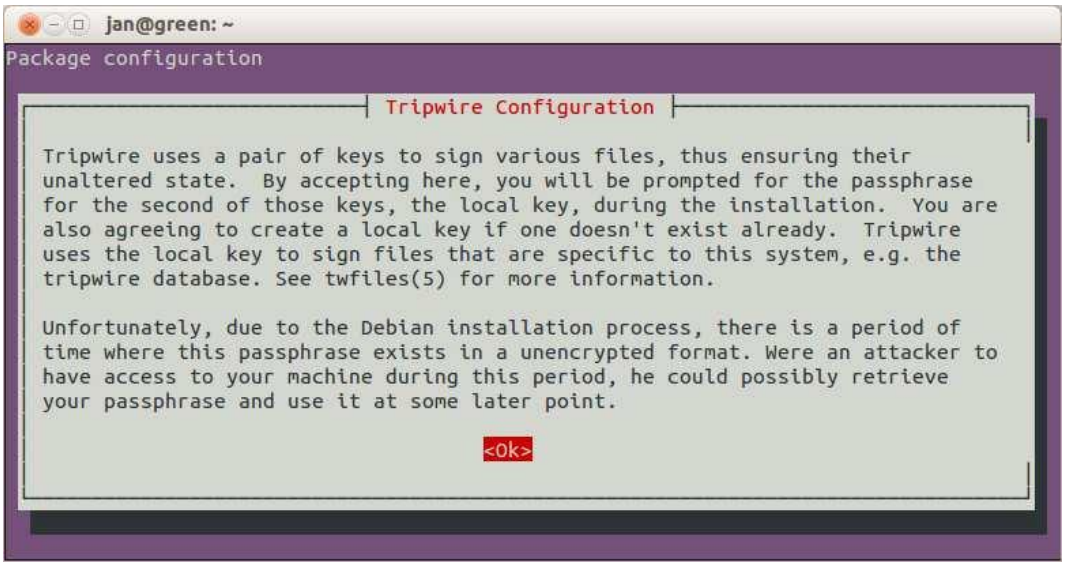
   Pada awal instalasi ada petunjuk dan peringatan yang dibutuhkan dalam proses instalasi Tripwire, bacalah dengan seksama dan untuk melanjutkan, pilih OK.



2. Muncul dialog untuk meminta membuat key passphrase, pilih yes.

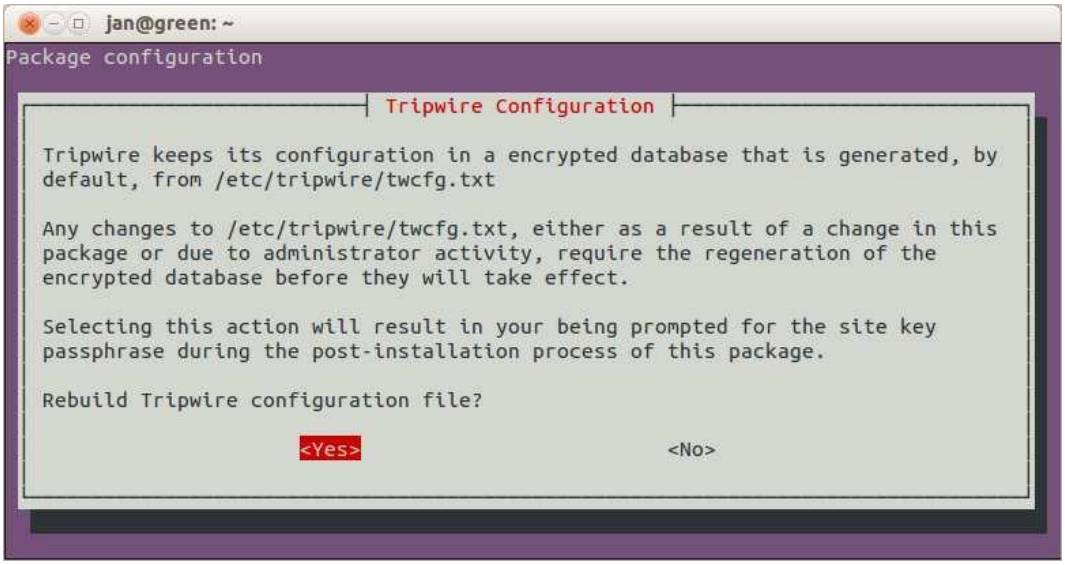


3. Ada peringatan kembali seperti awal instalasi, hal ini mengingatkan untuk membuat key yang aman.

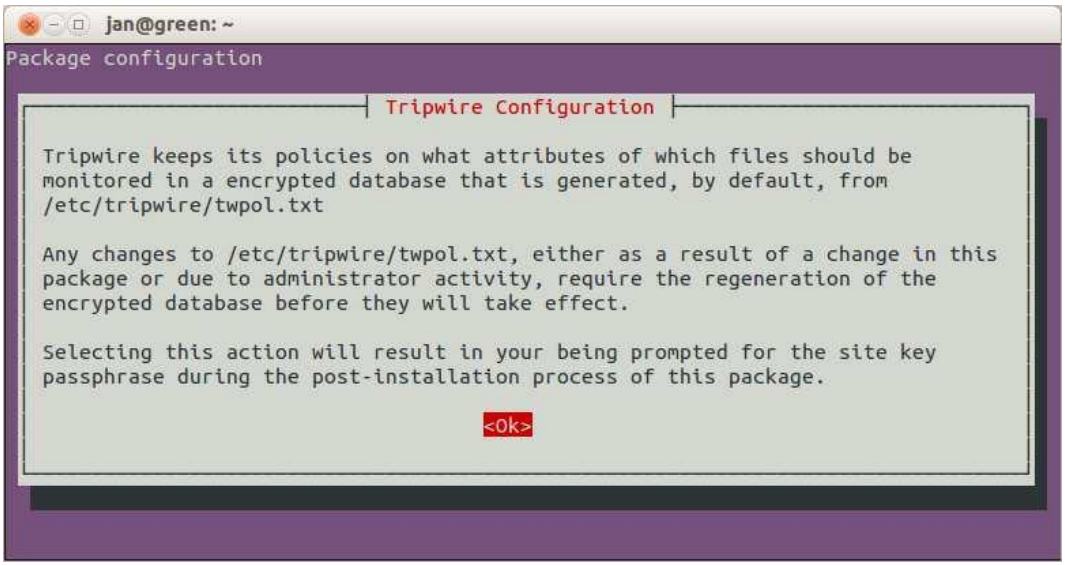


4. Kemudian ada konfirmasi apakah ingin membuat local paraphase atau tidak. Pilih yes karena paraphase juga dibuat pada local machine.

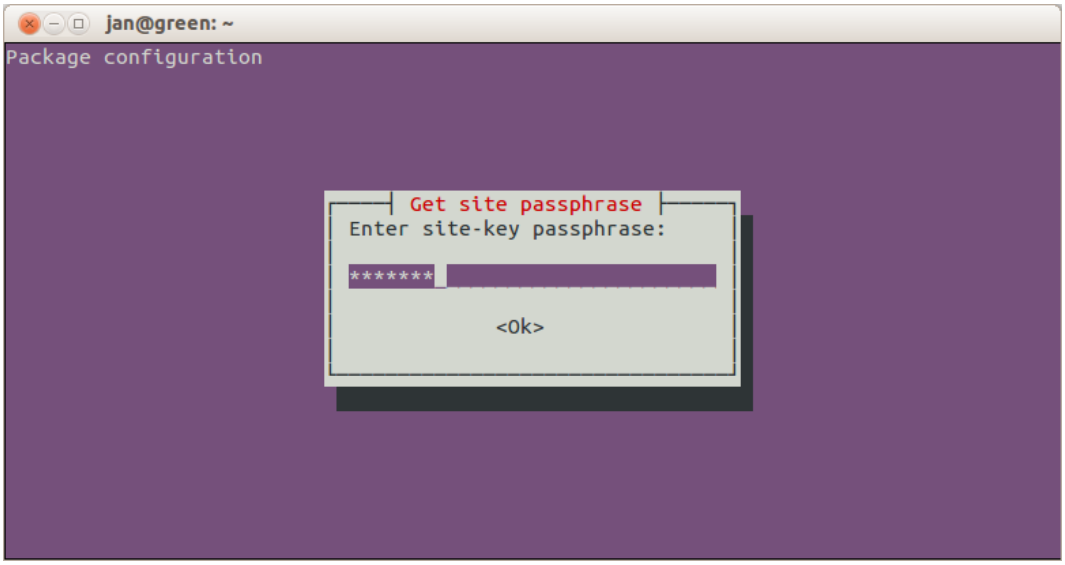
5. Kemudian ada permintaan konfirmasi apakah ingin untuk menyimpan hasil konfigurasi pada /etc/tripwire/twcfg.txt. Pilih yes untuk me-rebuild file configurasi. Konfirmasi untuk me-rebuild file konfigurasi dengan memilih Yes.



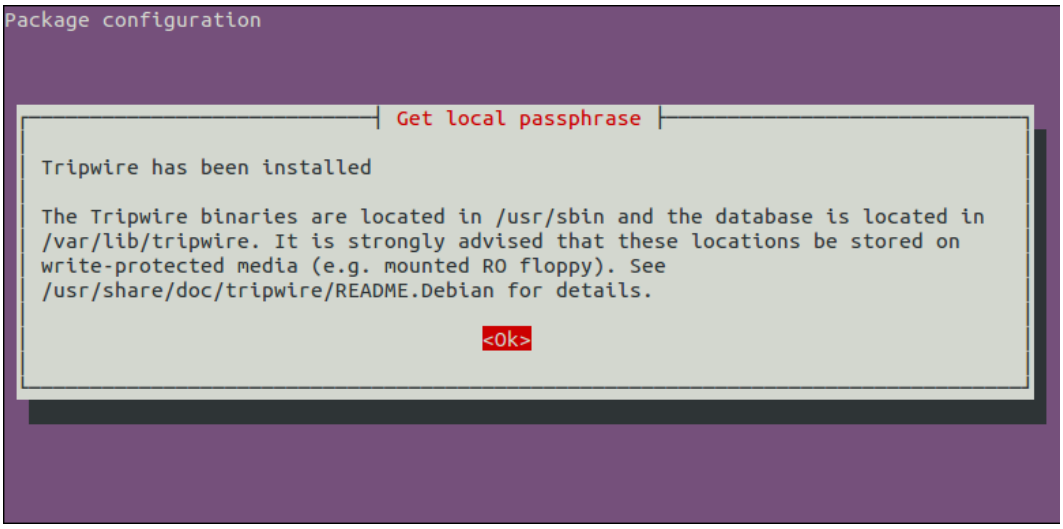
6. Setelah itu, ada permintaan konfirmasi apakah ingin menyimpan hasil policy pada /etc/tripwire/twpol.txt. Pilih yes untuk me-rebuild file policy.



7. Setelah itu, masukan local-key yang diinginkan kemudian memilih OK. Ulangi pada langkah selanjutnya memasukkan site-key setelah itu pilih OK. Pastikan passphrase yang dibuat selalu diingat, jika perlu dicatat untuk keperluan percobaan berikutnya.



8. Dan instalasi selesai setelah passphrase dimasukan dua kali. Kemudian muncul dialog yang menyatakan bahwa instasi Tripwire selesai.



9. Untuk meningkatkan keamanan, perlu dilakukan enkripsi file konfigurasi /etc/tripwire/twcfg.txt dengan menggunakan perintah

```
#twadmin --create-cfgfile –-cfgfile ./tw.cfg \
        –-site-keyfile ./site.key ./twcfg.txt
```

6.5.2 Percobaan 2: Inisialisasi database pengecekan Tripwire

3. Dalam konfigurasi default tripware, file dan direktori yang diamati cukup banyak sehingga proses inisialisasi atau pembuatan database awal akan membutuhkan waktu yang lama. Agar proses percobaan tidak memakan waktu lama maka kita akan memonitor sebuah direktori saja. Buat direktori baru dengan perintah berikut ini.

#mkdir /home/praktikum

4. Sebagai direktori dan file yang akan kita ubah nanti, buat sebuah direktori dengan nama “dir-coba” dan sebuah file dengan nama “file-coba.txt”

   #mkdir /home/praktikum/dir-coba

   #gedit /home/praktikum/file-coba.txt

5. Copy file twpol sebelum melakukan perubahan

   #cp /etc/tripwire/twpol.txt /etc/tripwire/twpol.txt.backup

6. Lakukan perubahan pada konfigurasi twpool.txt agar hanya direktori /home/percobaan saja yang akan dimonitor

   #gedit /etc/tripwire/twpol.txt

7. Hapus semua teks konfigurasi mulai dari baris

   #

   # Tripwire Binaries

   #

8. Kemudian gantilah dengan konfigurasi berikut ini

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

9. Selanjutnya lalukan inisialisasi database dengan perintah berikut

   ```
   #tripwire --init --cfgfile /etc/tripwire/tw.cfg \
            --polfile /etc/tripwire/tw.pol \
            --site-keyfile /etc/tripwire/site.key \
            --local-keyfile /etc/tripwire/HOSTNAME-local.key
   ```

Untuk perintah HOSTNAME-local.key sesuaikan dengan hostname PC yang digunakan. Masukan key site passphrase yang telah dibuat sebelumnya.

Pada awal inisialisasi, akan terdapat beberapa warning dan error karena Tripwire belum mempunyai data yang sama pada databasenya, hal ini tidak masalah.

```
### Continuing...
### Warning: File system error.
### Filename: /proc/20099/fd/4
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /proc/20099/fdinfo/4
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /proc/20099/task/20099/fd/4
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /proc/20099/task/20099/fdinfo/4
### No such file or directory
### Continuing...
The object: "/proc/sys/fs/binfmt_misc" is on a different file system...ignoring.
Wrote database file: /var/lib/tripwire/green.twd
The database was successfully generated.
jan@green:~$
```

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

    #tripwire --check

    Amati hasilnya dan copy dalam sebuah dokumen (akan digunakan dalam pengamatan dan analisa dalam laporan anda)

6.5.3 Percobaan 3: Melihat hasil monitoring Tripwire

1. Buka “file-coba.txt” dan tamahkan isi file dengan nama dan nim anda

   #gedit /home/praktikum/file-coba.txt

2. Buat sebuah file dengan nama “file-coba2.txt” dalam dierektori “dir-coba”

   #gedit /home/praktikum/dir-coba/file-coba2.txt

3. Cek perubahan pada sistem dengan perintah

   #tripwire --check

   Amati hasilnya dan copy dalam sebuah dokumen (akan digunakan dalam pengamatan dan analisa dalam laporan anda)

4. Bandingkan hasil pada langkah 3 ini dengan Percobaan 2 langkah 8 dan jelaskan perubahan yang terjadi

6.5.4 Percobaan 4: Update file policy Tripwire

1. Buat sebuah direktori lagi di dalam /home

#mkdir /home/praktikum2

2. Lakukan perubahan pada konfigurasi twpool.txt agar direktori /home/percobaan2 juga dimonitor oleh Tripwire

   #gedit /etc/tripwire/twpool.txt

3. Tambahkan direktori praktikum2 dalam daftar direktori yang akan dimonitor

   {

   /home/praktikum -> $(SEC_CRIT);

   /home/praktikum2 -> $(SEC_CRIT);

   }

4. Karena kita melakukan perubahan policy maka lakukan update seberti berikut ini

   #tripwire --update-policy --cfgfile ./tw.cfg \

   --polfile ./tw.pol --site-keyfile ./site.key \

   --local-keyfile ./green-local.key ./twpol.txt

5. Cek perubahan pada sistem dengan perintah

   #tripwire --check

6. Amati hasilnya dan copy dalam sebuah dokumen, selanjutnya bandingkan dengan hasil dari percobaan 3 kemudian buat penjelasan mengenai hasil tersebut.

6.5.5 Percobaan 4: Update database Tripwire

1. Misalkan anda mengubah/mengedit file tertentu, apabila database tidak diubah, perubahan file ini akan dideteksi oleh tripwire sebagai bentuk pelanggaran, walaupun perubahan tersebut legal. Buatlah sebuah file dalam direktori /home/praktikum dengan nama “file-coba2.txt”

   #gedit /home/praktikum/file-coba2.txt

2. Cek perubahan pada sistem dengan perintah

   #tripwire --check

   Amati hasilnya dan copy dalam sebuah dokumen (akan digunakan dalam pengamatan dan analisa dalam laporan anda)

3. Sebelum melakukan update database, perlu diperhatikan disini adalah file nama-file.twr, sesuaikan dengan file report tripwire tersebut. Jalankan perintah update berikut

   #/usr/sbin/tripwire --update \

--twrfile /var/lib/tripwire/report/nama-file.twr

4. Cek lagi perubahan pada sistem dengan perintah

   #tripwire --check

5. Amati hasilnya dan copy dalam sebuah dokumen, bandingkan dengan langkah nomer 2 kemudian buat penjelasan tentang hasil