Laporan Pendahuluan Host Based IDS

### Muhammad Fajar Masputra /2110141025/ 3 D4 Teknik Informatika A

Pemasangan program intrusi deteksi sebenarnya ditujukan untuk mendeteksi, memantau keadaan anomali jaringan yang disebabkan salah satunya oleh penyusup (intruder). Setalah tahap pendeteksian biasanya IDS dapat diset untuk dapat memberikan peringatan bagi network administrator.

Type IDS sendiri secara garis besar dibagi 2 yaitu host-based dan network-based IDS. Pada praktikum kali ini, kita akan membahas salah satu contoh aplikasi dari host-based IDS, yaitu tripwire. Program tripwire berfungsi untuk menjaga integritas file sistem dan direktori, dengan mencatat setiap perubahan yang terjadi pada file dan direktori. Penggunaan tripwire biasanya digunakan untuk mempermudah pekerjaan yang dilakukan oleh System Administrator dalam mengamankan System.

Cara kerja tripwire adalah dengan melakukan perbandingan file dan direktori yang ada dengan database system yang dibuat pada saat tripwire diinstall. Perbandingan tersebut meliputi perubahan tanggal, ukuran file, penghapusan dan lain-lainnya. Setelah tripwire dijalankan, secara otomatis akan melakukan pembuatan database sistem. Kemudian secara periodik akan selalu melaporkan setiap perubahan pada file dan direktori.

Salah satu komponen dari jaringan komputer yang perlu dikelola dengan menggunakan manajemen jaringan adalah Intrusion Detection System (IDS). IDS merupakan sistem yang berfungsi untuk melakukan deteksi penyusupan. Penggunaan IDS dari waktu ke waktu semakin meningkat seiring dengan semakin pentingnya faktor keamanan bagi para pengguna jaringan komputer. Untuk sebuah jaringan yang berskala besar bahkan seringkali digunakan lebih dari satu jenis produk IDS. Dengan semakin besarnya jumlah IDS yang digunakan maka semakin besar pula usaha yangdiperlukan untuk mengelolanya.Hal inilah yang menjadi alasan diperlukannya manajemen jaringan untuk mengelola IDS tersebut.

Berdasarkan input datanya, IDS dibagi menjadi 2 jenis yaitu :

1. Network Intrusion Detection System(NIDS)

NIDS adalah jenis IDS yang menganalisa lalulintas packet dalam jaringan. Oleh NIDS, paket-paket data yang dikirimkan melalui jaringan akan diperiksa apakah berbahaya untuk keseluruhan jaringan. Apabila ada paket data yang berbahaya atau mencurigakan, NIDS akan membuat log mengenai paket tersebut, yang disertai informasi-informasi tambahan.Berdasarkan paket yang mencurigakan tadi, NIDS akan memeriksa database miliknya mengenai ciri-ciri paket yang merupakan serangan terhadap jaringan. Kemudian NIDS akan memberikan label mengenai tingkat bahaya dari setiap paket yang dicurigai. Apabila tingkat bahaya cukup tinggi, NIDS bisa mengirimkan email peringatan kepada administrator agar dilakukan analisa lebih lanjut.

NIDS mendapatkan input dari sensor-sensor yang berada di lokasi-lokasi yang strategis dalam sebuah jaringan. Beberapa lokasi strategis yang bisa dipakai untuk menempatkan sensor antara lain switch, router, firewall, atau berada di sebuah host.Salah satu contoh software NIDS yang bisa dianggap sebagai standar NIDS secara *de facto* adalah Snort.

1. Host-based Intrusion Detection System(HIDS)

HIDS menganalisa beberapa area dalam sebuah host untuk mengetahui adanya aktivitas merusak ataupun penyusupan (serangan) terhadap sebuah host. HIDS memanfaatkan beberapa jenis file log (misalnya log kernel, log sistem, log konfigurasi, dan lain-lain) dan kemudian membandingkannya dengan database (berisi ciri-ciri serangan yang diketahui) yang dimiliki oleh HIDS. Apabila HIDS menemukan event-event yang mencurigakan dalam file log, maka HIDS akan menganalisa event tersebut, kemudian menilai tingkat bahaya dari event tersebut. HIDS lalu mencatat event-event mencurigakan tersebut dengan format khusus dan melaporkannya ke administrator untuk dianalisa lebih lanjut.

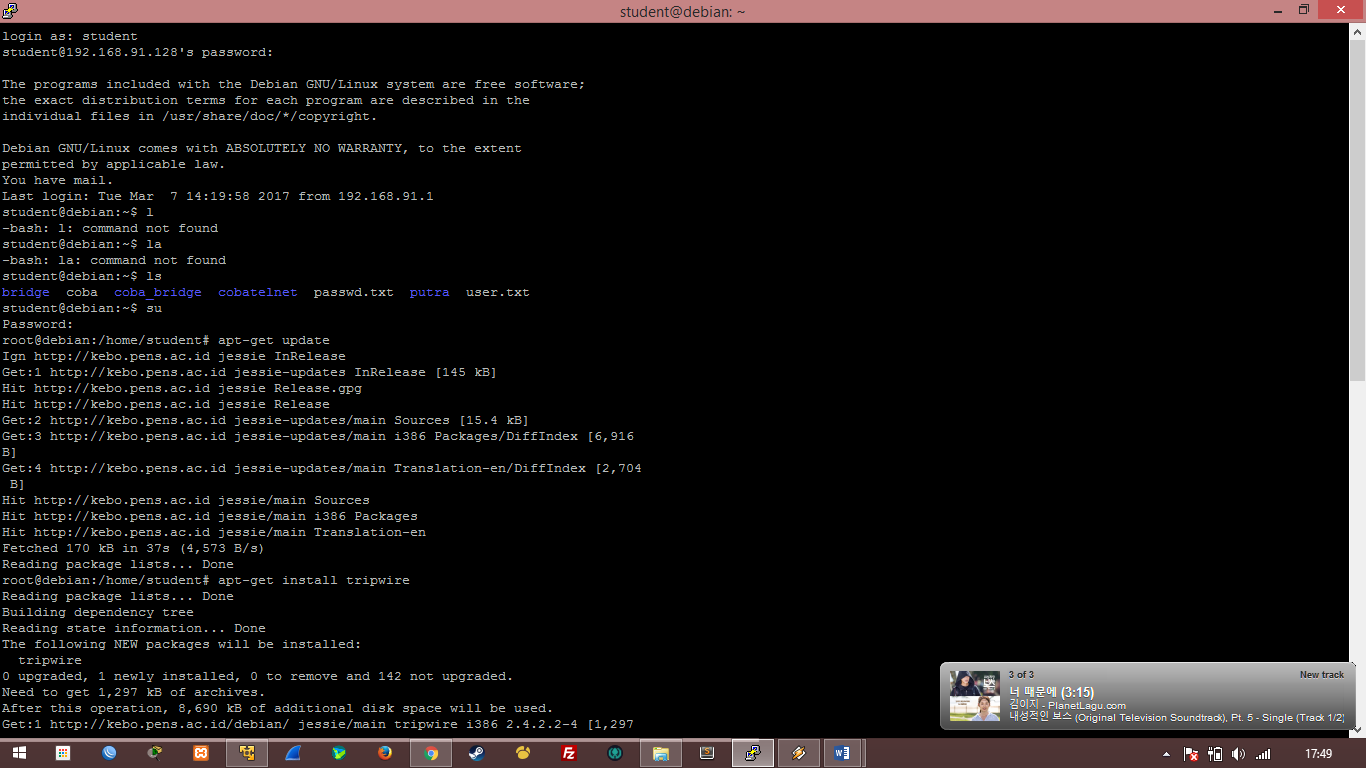
Sebuah HIDS juga bisa digunakan untuk memverifikasi integritas file, sehingga bisa diketahui apabila file tersebut telah mengalami perubahan. Fungsi integritas file bisa diterapkan untuk file-file penting yang berperan vital, agar tidak dilakukan perubahan oleh pihak yang tidak berwenang.

Lebih lanjut mengenai integritas data, HIDS bisa digunakan untuk memonitor komponen khusus dalam sebuah host, yang tidak aman apabila dimonitor oleh NIDS. Komponen-komponen khusus dalam sebuah sistem operasi seperti file passwd (dalam sistem UNIX), Registry (dalam sistem Windows), atau file-file konfigurasi lainnya bisa dimonitor agar tidak disalahgunakan. File-file tersebut akan sangat beresiko apabila dimonitor menggunakan NIDS.

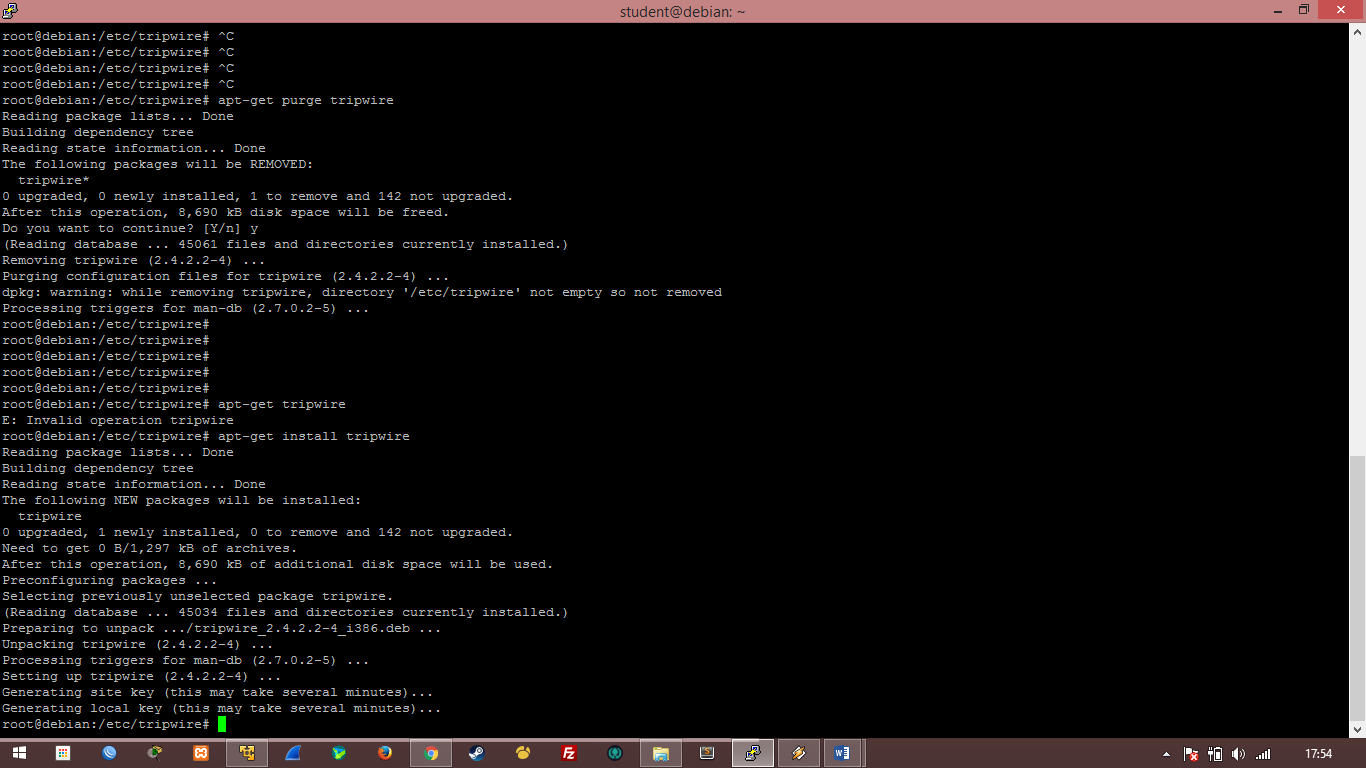
Meskipun HIDS lebih baik dibanding NIDS dalam mendeteksi serangan dan aktivitas merusak dalam sebuah host, HIDS memiliki keterbatasan dalam memonitor jaringan. HIDS tidak mampu mendeteksi serangan yang ditujukan untuk host yang tidak terinstall HIDS. Salah satu aplikasi HIDS yang cukup populer dalam Linux adalah Tripwire.

**Instalasi TripWire**

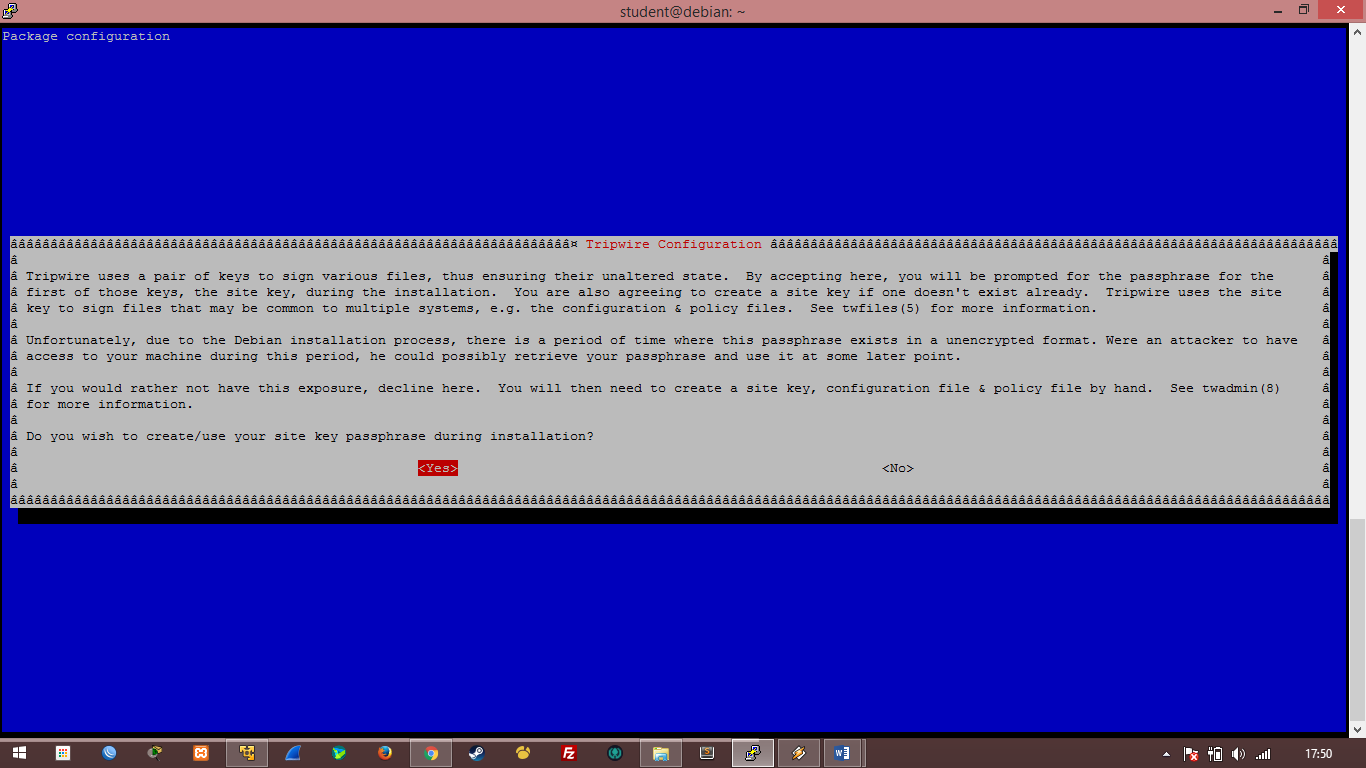
* Lakukan update untuk OS Anda terlebih dahulu

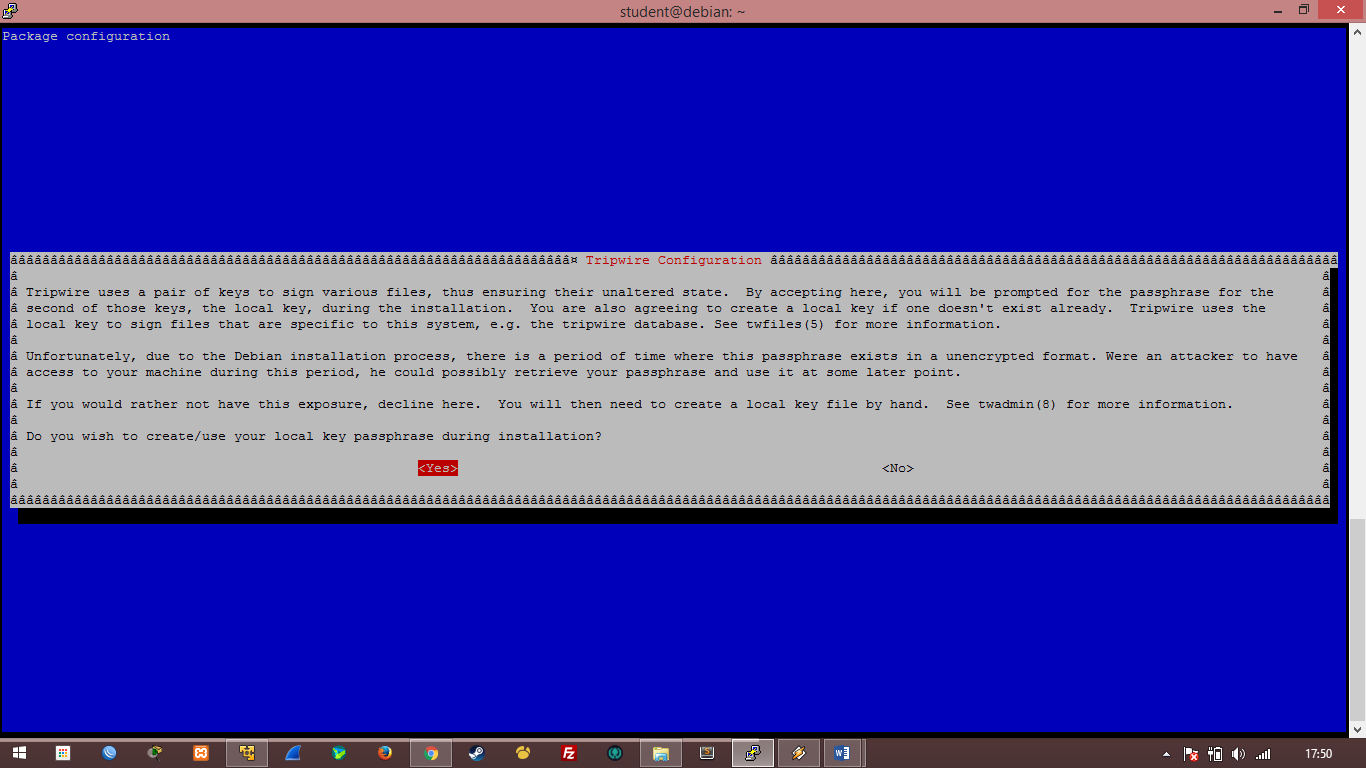


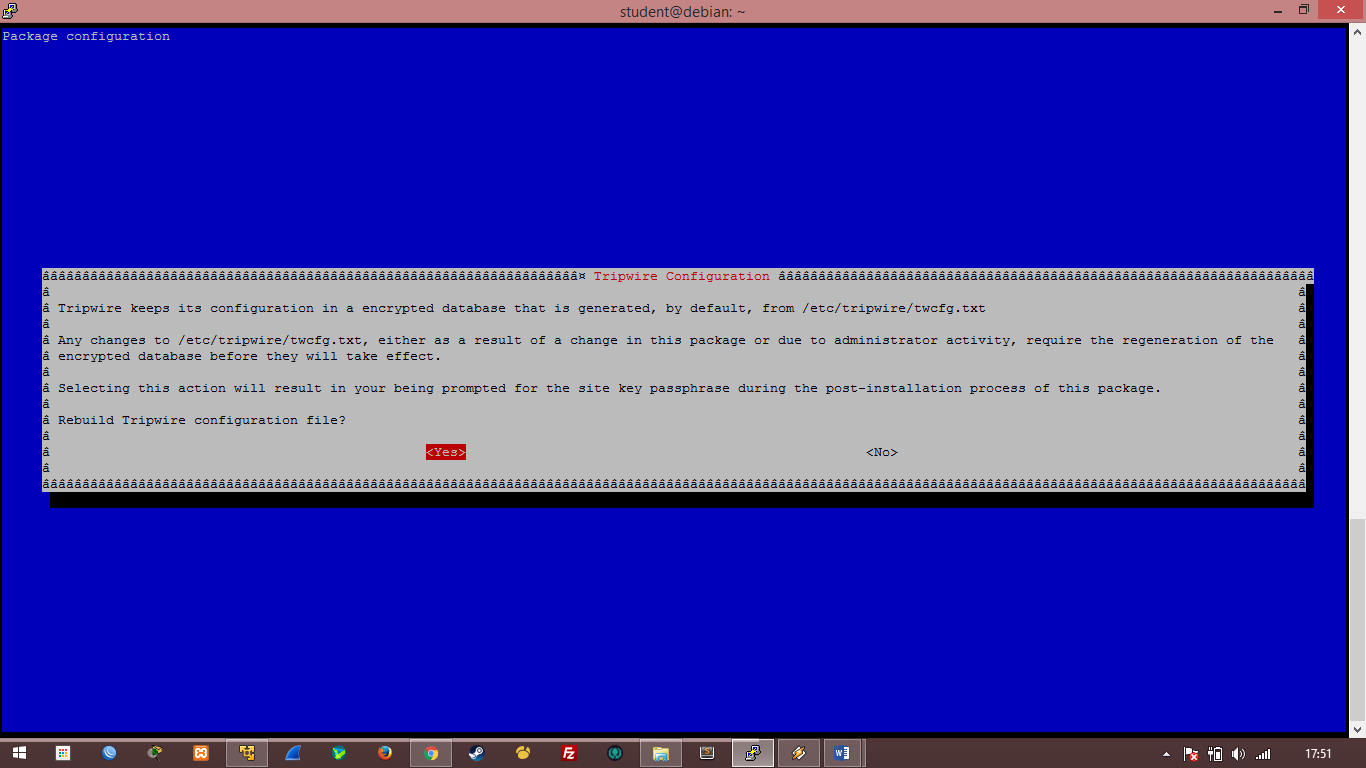
* Lakukan instalasi tripwire



* Lalu akan muncul dialog seperti dibawah. Perhatikan pesan yang muncul pada setiap dialog, lalu jawab dengan “Yes”.

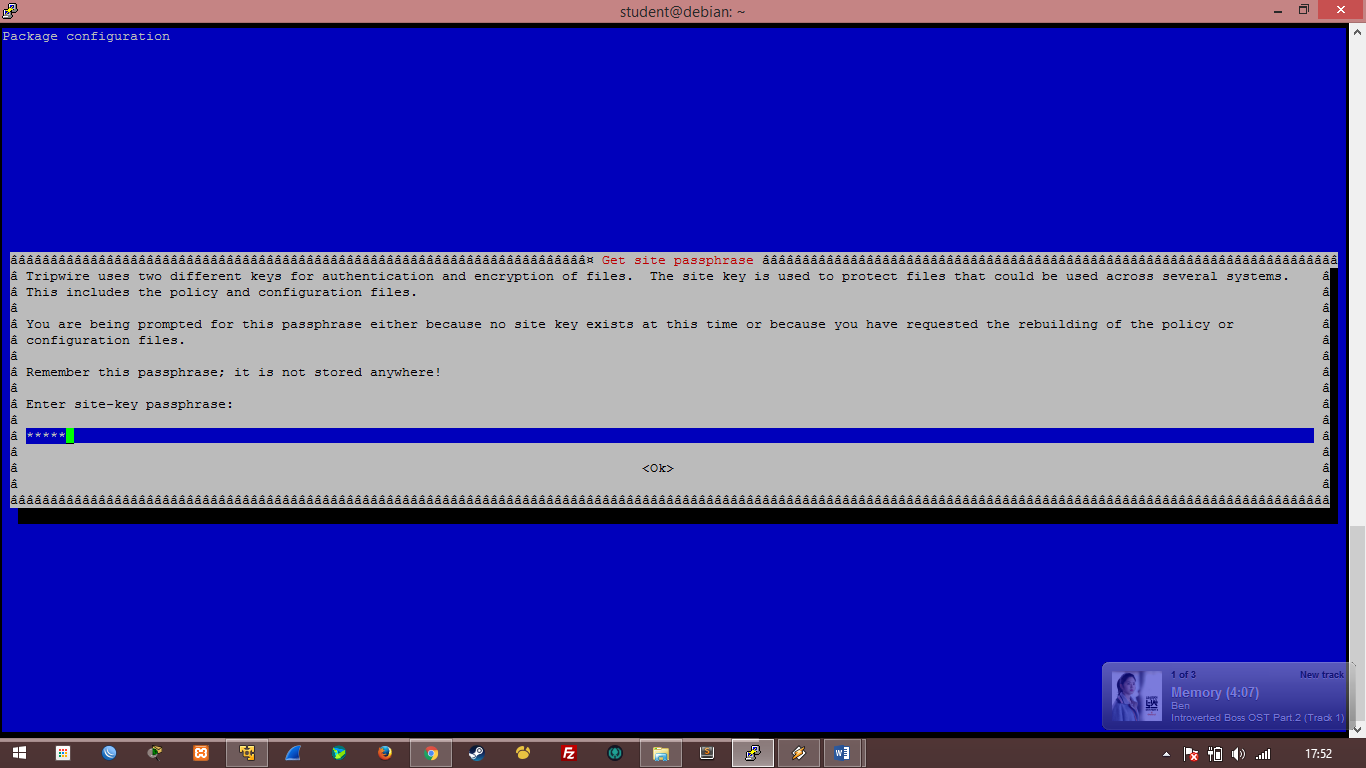


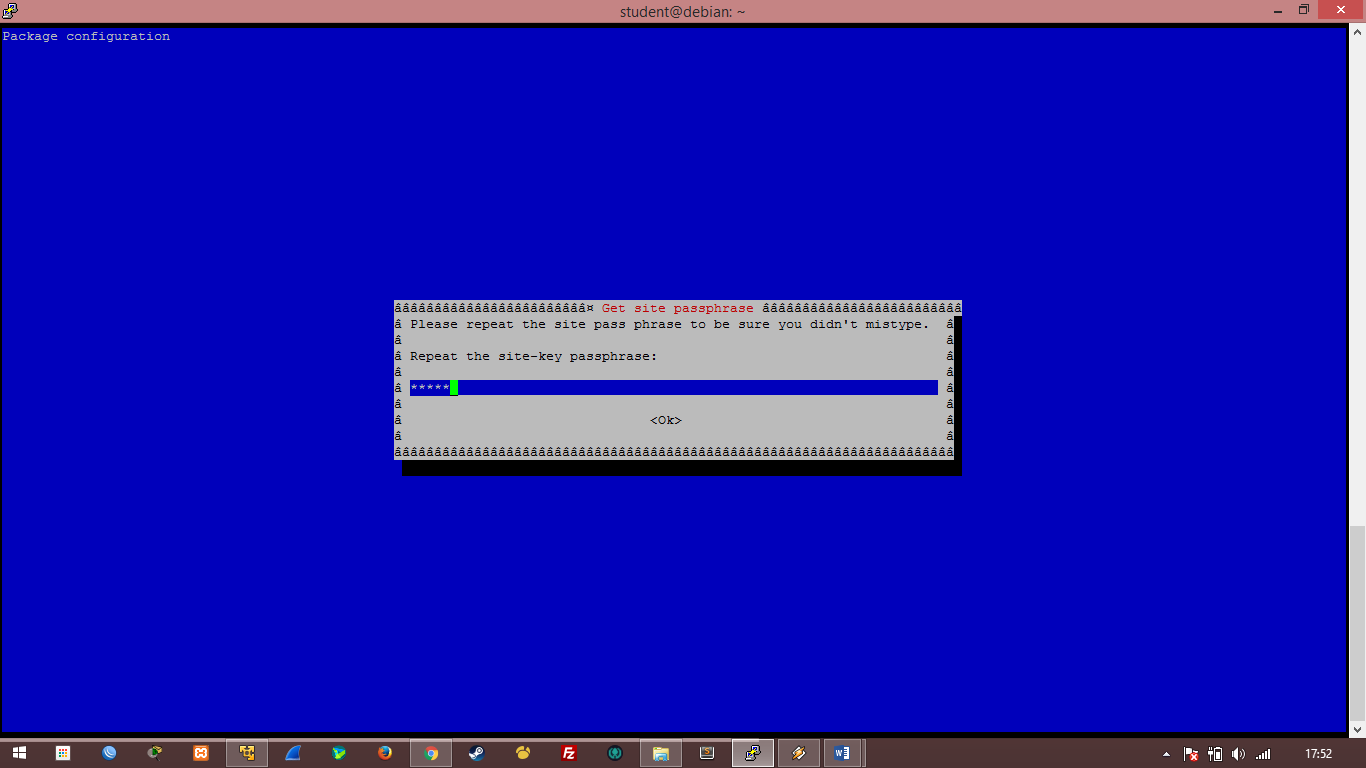


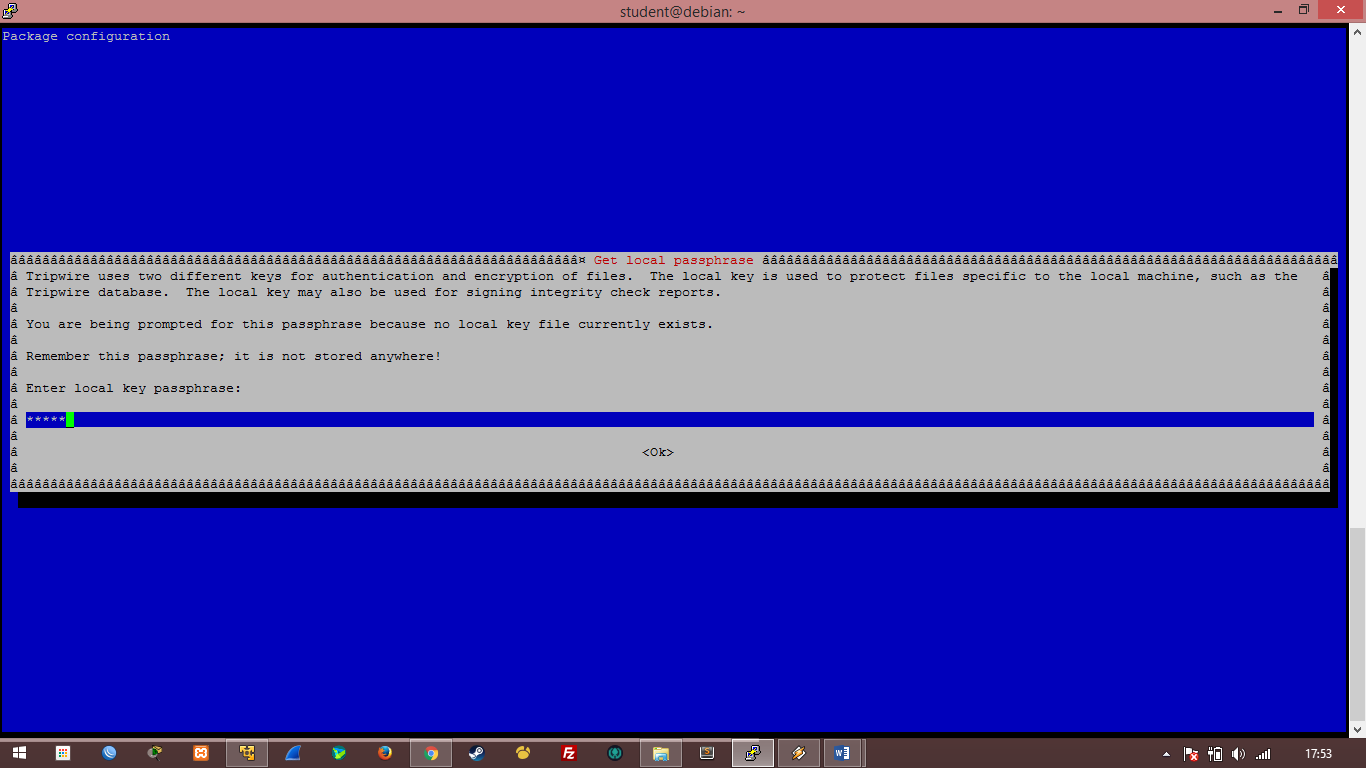




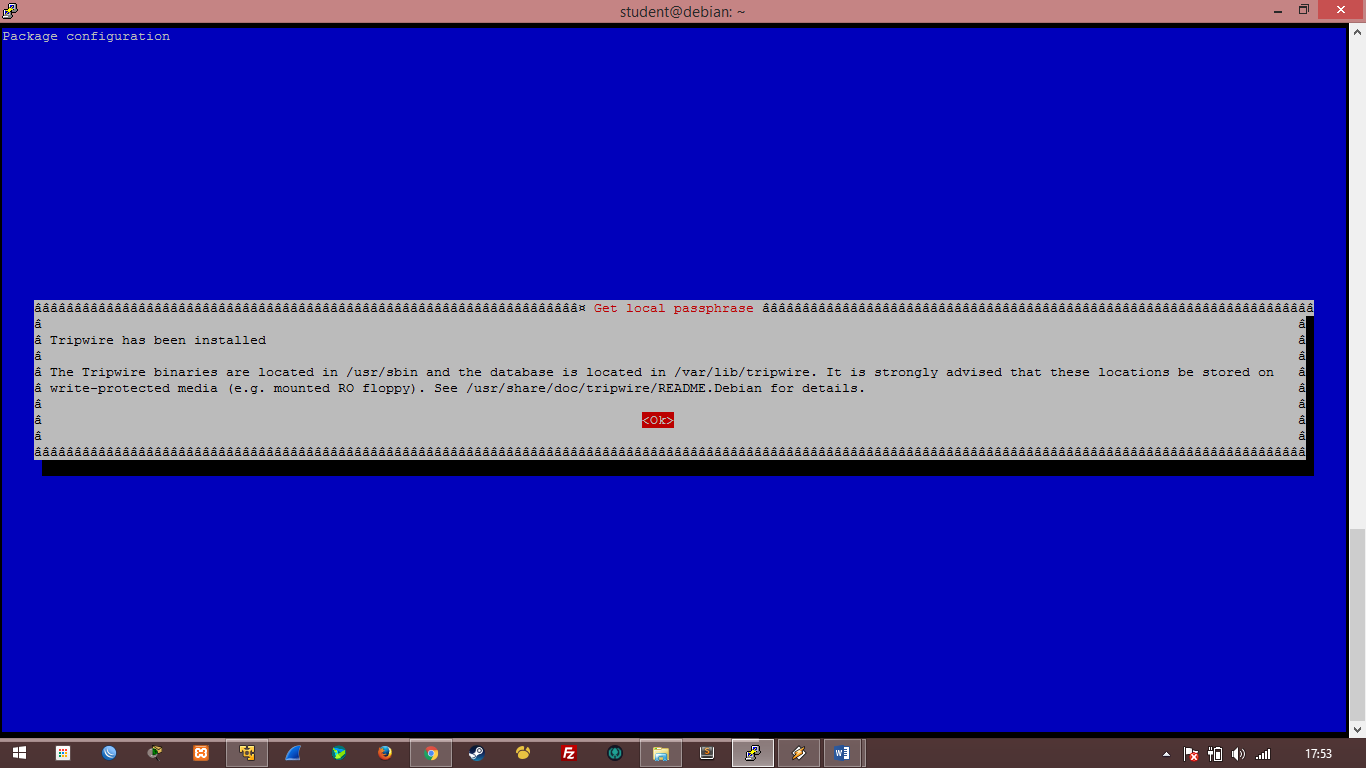
* Masukkan site key passphrase dan local key passphrase, setelah muncul dialog seperti dibawah. Ulangi sekali lagi !







* Kemudian akan mucul dialog bahwa trip wire telah terinstal. Perhatikan pesan pada dialog tersebut !



* Ubah mode dari 2 buah file dari tripwire : tw.cfg dan tw.pol.
  + #cd /etc/tripwire
  + #chmod 0600 tw.cfg tw.pol

