|  |  |
| --- | --- |
| A picture of a winding road and trees  Hardening Host  SUDO DAN TRIPWIRE | dibuat oleh :  Achmad Agus Salim (2103121035) Yufi Eko Firmansyah (2103121049) Retno Wulandari (2103121050)  Kelompok 1 – 3 D3 IT B  Keamanan Jaringan |

Modul 4  
Hardening Host : Sudo dan Tripwire

1. **TUJUAN PEMBELAJARAN**
   * Melakukan instalasi sudo dan tripwire.
   * Memahami cara kerja sudo dan tripwire.
2. **DASAR TEORI**

**Sudo**

Sudo (su “do”) merupakan sebuah perintah dalam *command-line* Unix. Apabila kita memiliki akses *root,* maka sudo akan melakukan perintah sebagi *superuser*. Di keluarga Unix terdapat sebuah *superuser* yang namanya *root*. *Superuser* ini dapat melakukan apapun terhadap sistem. Melakukan pekerjaan umum dengan menggunakan akun *root* ini mempunyai resiko yang berbahaya karena jika salah menggunakannya maka akan dapat merusak sistem yang ada. Baiknya untuk pekerjaan umum kita menggunakan akun biasa dan hanya menggunakan akun *root* jika memang sangat diperlukan.



Untuk itu sudo diciptakan agar akun biasa dapat menjalankan perintah yang membutuhkan hak akses dari akun *root* tanpa harus login sebagai *root*. Dengan sudo nantinya administrator (*root*) dapat memberikan user ataupun sekumpulan user (Group) kemampuan untuk menjalankan beberapa ataupun semua perintah sebagai *root* tanpa masuk sebagai *root*. Sudo beroperasi perbaris perintah, jadi buka sebagai pengganti shell. Sudo mempunyai fitur antara lain :

* Kemampuan untuk membatasi perintah-perintah yang dijalankan oleh user pada setiap host.
* Sudo melakukan pencatatan tiap perintah yang diketikkan, memberikan jejak audit yang jelas tentang siapa melakukan apa. Ketika digunakan digunakan bersama-sama dengan syslogd, System log daemon, sudo dapat mencatat semua perintah yang mengacu pada *Central host* (serta pada localhost). Pada CU, semua amin menggunakan sudo sebagai pengganti *root shell* untuk mengambil keuntungan dari pencatatan ini.
* Sudo menggunakan file timestamp untuk menerapkan “*ticketing” system*. Bila user memanggil perintah sudo dan memasukkan password mereka, mereka diberikan tiket selama 5 menit (timeout ini dapat dikonfigurasi pada *compile-time*). Setiap menggunakan perintah sudo berikutnya maka tiket tersebut diperbarui untuk 5 menit lagi. Hal ini menghindari permasalahan jika kita meninggalkan *root shell* dan orang lain mendapatkan akses langsung ke keyboard kita dan melakukan perintah-perintah yang tidak kita inginkan. Ada juga cara muda bagi pengguna untuk menghapus file tiket tersebut, yaitu dengan meletakkan perintah menghapusnya pada file .logout.
* File konfigurasi sudo (sudoers) adalah file konfigurasi yang dapat digunakan pada berbagai mesin berbeda host. Hal ini memungkinkan administrator pusat menjaga fleksibilitas untuk menentukan hak user pada basis per-host.

**Tripwire**

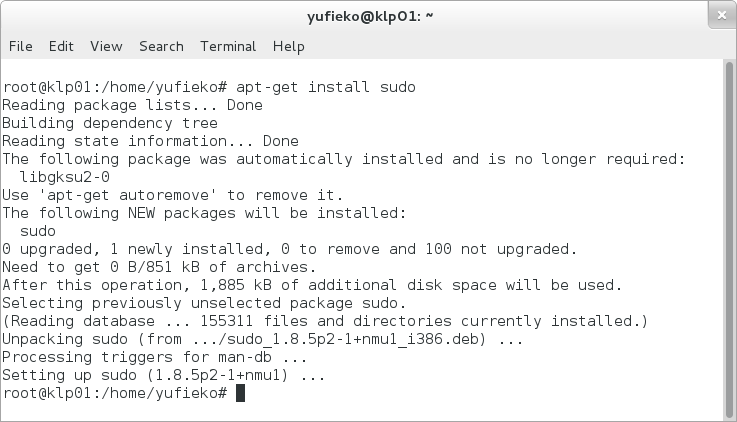
Pemasangan program intrusi deteksi sebenarnya ditujukan untuk mendeteksi, memantau keadaan anomali jaringan yang disebabkan salah satunya oleh penyusup (intruder). Setelah tahap pendeteksian biasanya IDS dapat diset untuk dapat memberikan peringatan bagi network administrator. Type IDS sendiri secara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

1. **PERCOBAAN**

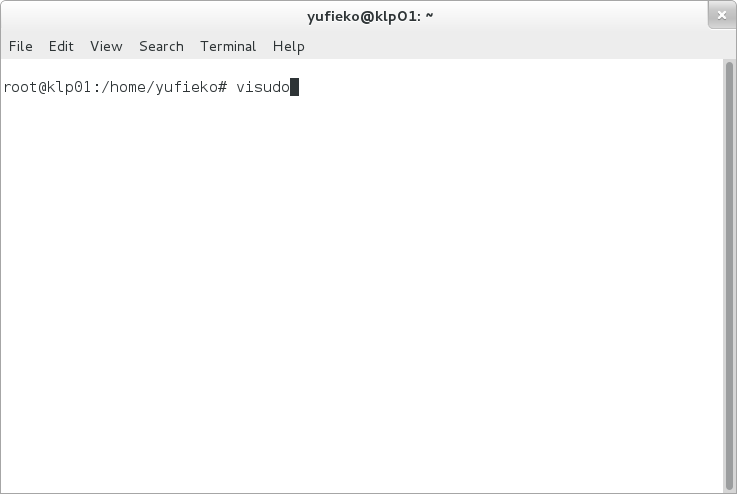
**Percobaan C.1. Proses Sudo**

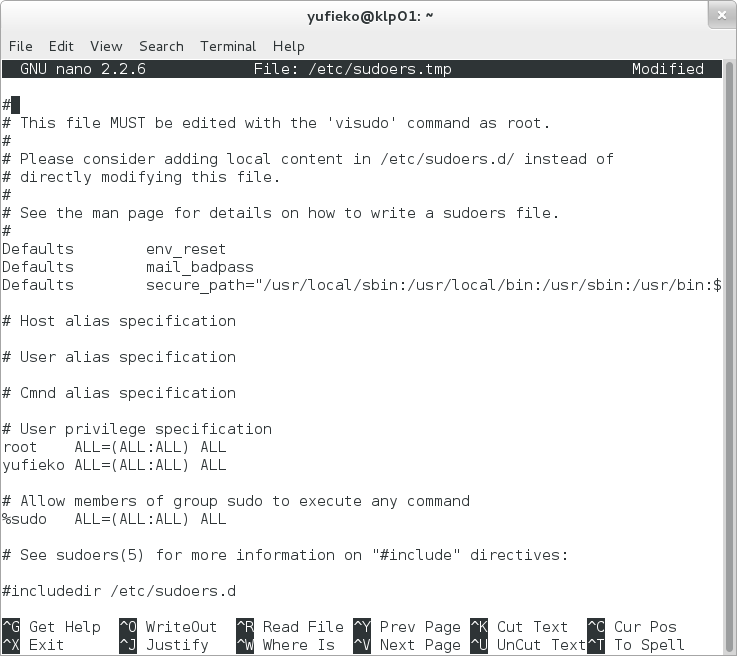
Langkah Percobaan

1. Instal sudo dengan perintah apt-get install sudo



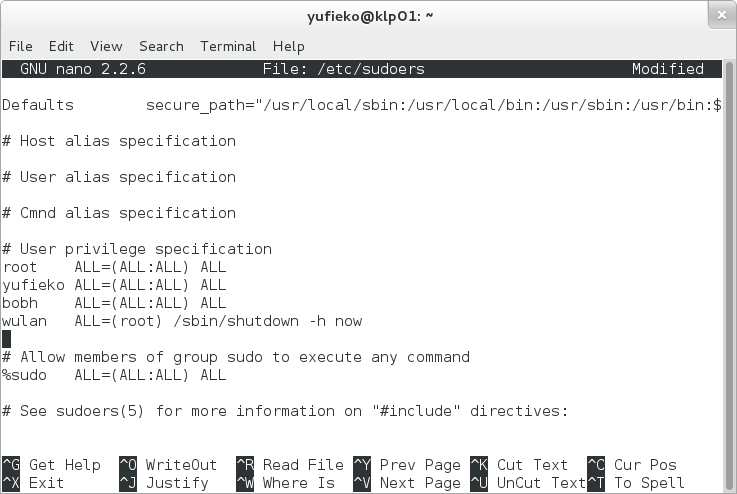
1. Setelah itu ketikkan “visudo” untuk mengedit file /etc/sudoers. Pada file tersebut kita akan melakukan pengaturan hak akses untuk setiap user yang ada.



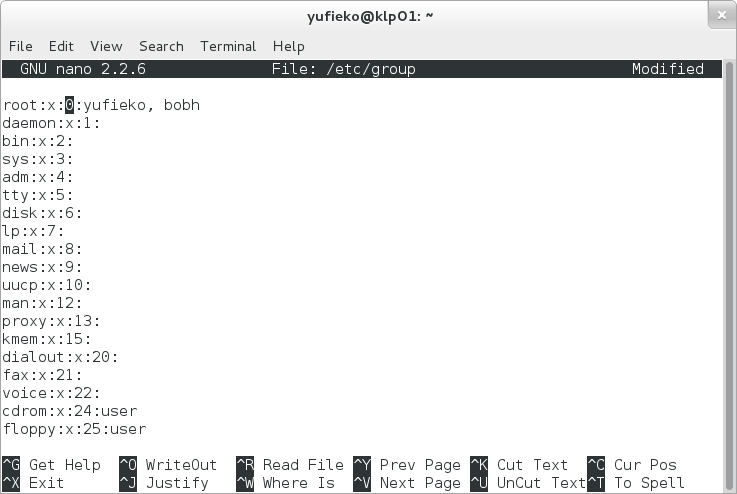


Terlihat di atas masih berisi konfigurasi asli, seperti pada *user privelege spesification* ada user *root* dan Group sudo yang dapat melakukan apapun pada sistem.

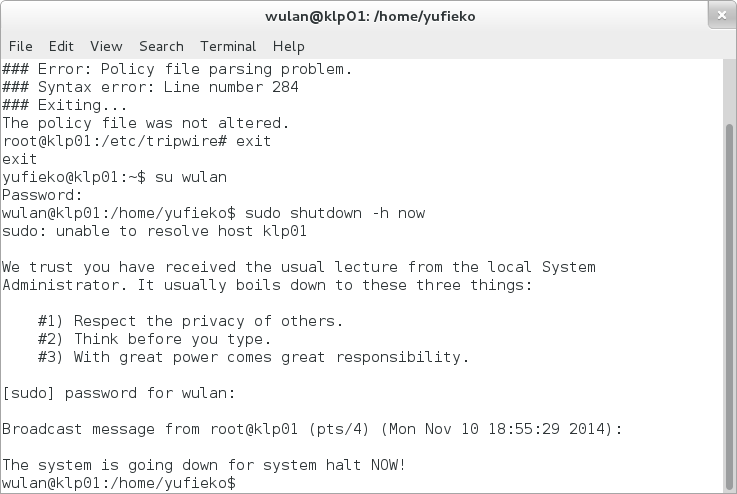
1. Pada sistem ini nantinya akan kita atur 3 user yang memakai 2 hak akses, user yufieko dan bobh akan seperti *root* dan user wulan hanya bisa melakukan perintah “shutdown –h now”. Maka pada file tersebut ubah seperti gambar berikut :



Lalu pada file /etc/group kita sedikit modifikasi, pada group *root* kita tambahkan user yufieko dan bobh.



Lalu sekarang kita lakukan percobaan pada user wulan untuk melakukan perintah “shutdown –h now”



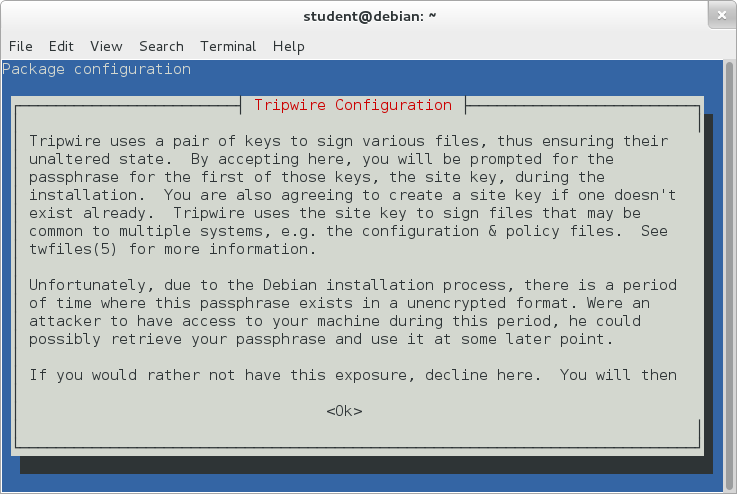
**Percobaan C.2. Tripwire**

**Langkah Percobaan I**

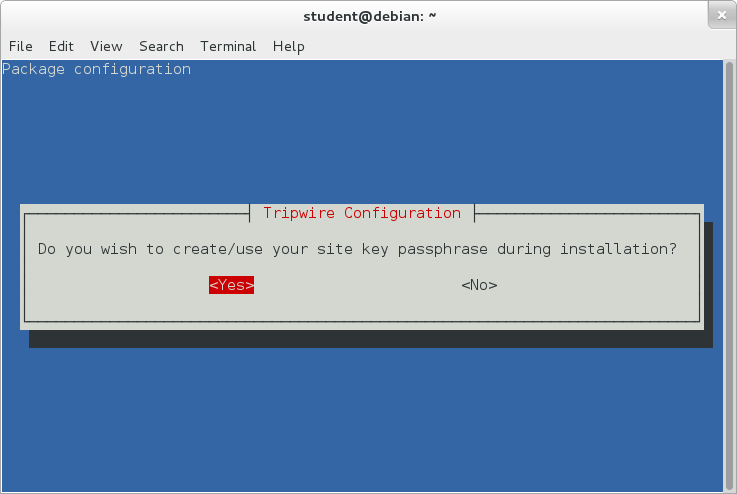
1. Login sebagai root menggunakan su ataupun sudo
2. Lakukan sinkronisasi terkini indeks paket software lokal dengan repositori  
   # apt-get update
3. Lakukan instalasi tripwire

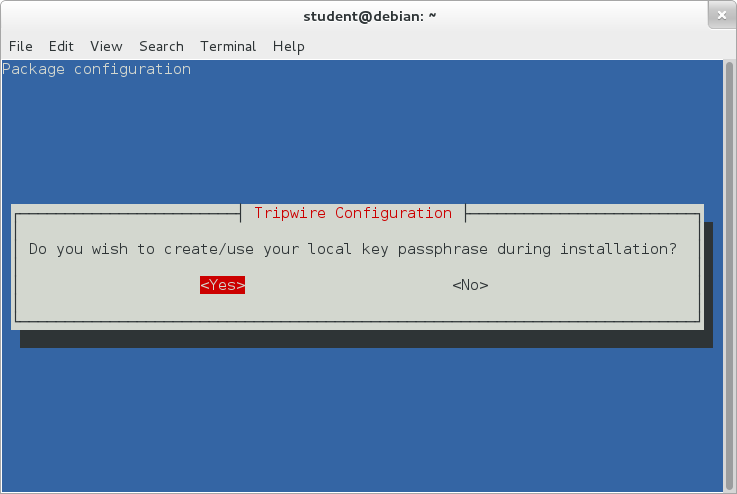
# apt-get install tripwire

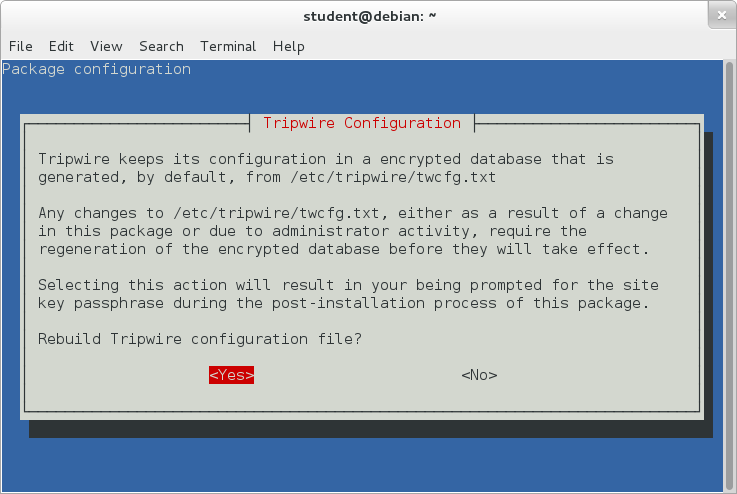
Maka akan muncul dialog instalasi tripwire, pilih ok



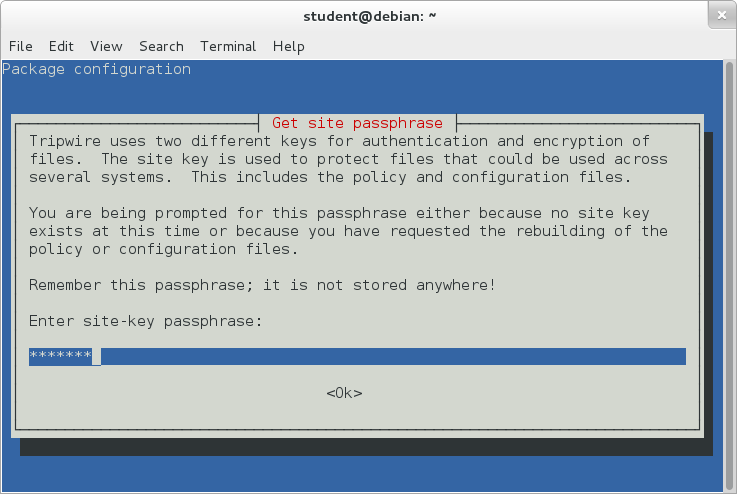
Lalu akan muncul dialog seperti di bawah. Perhatikan pesan yang muncul pada setiap dialog, lalu jawab dengan “Yes”.

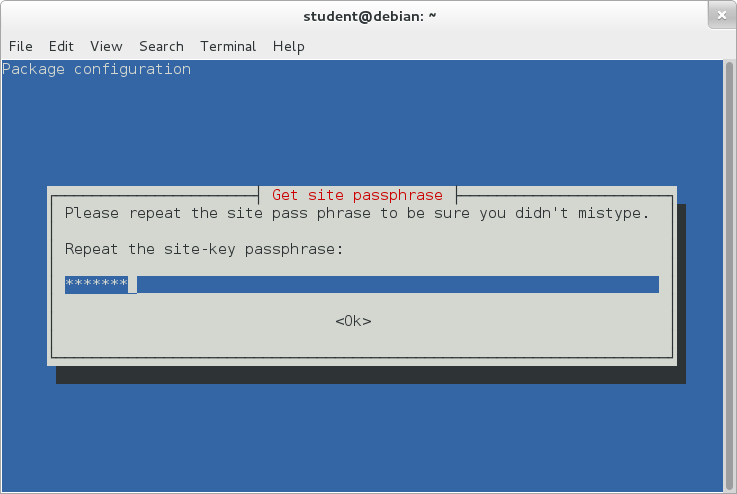


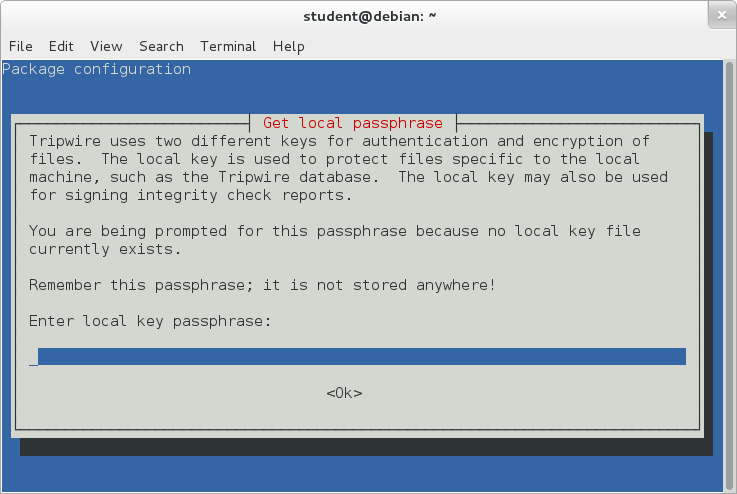


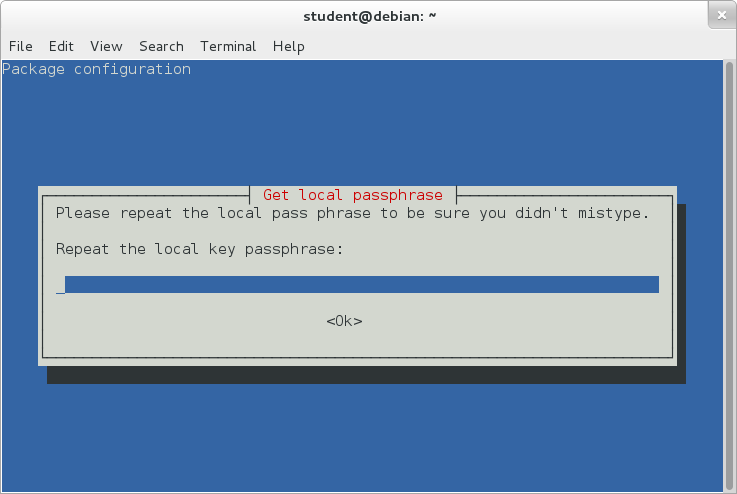


Lalu kita akan disuruh memasukkan site key passphrase dan local key passphrase, setelah muncul dialog seperti di bawah. Ulangi sekali lagi.

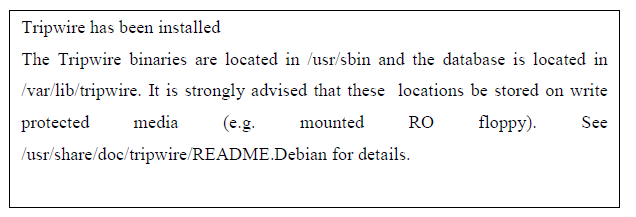








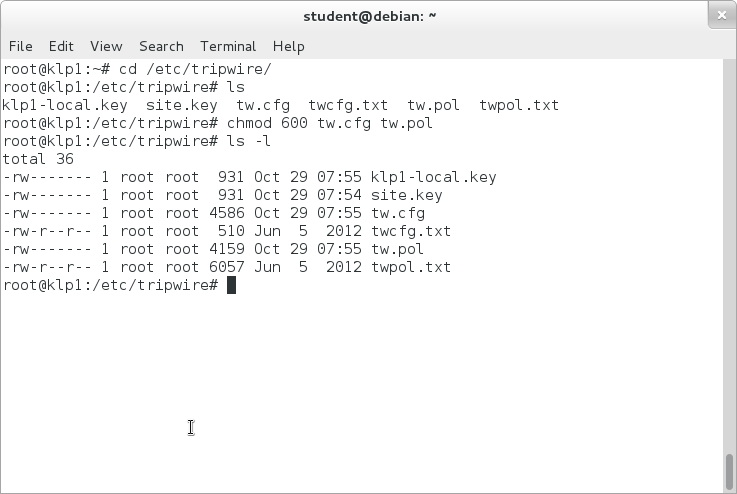
1. Kemudian akan muncul dialog bahwa tripwire telah terinstal. Perhatikan pesan pada dialog tersebut !



1. Ubah mode dari 2 buah file dari tripwire : tw.cfg dan tw.pol

# cd /etc/tripwire

# chmod 0600 tw.cfg tw.pol



**Langkah percobaan II – melakukan modifikasi pada file “Policy” dan file konfigurasi**

Setelah proses instalasi berakhir, lakukan langkah-langkah di bawah ini :

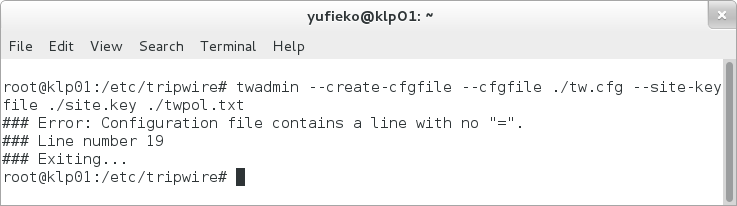
1. Modifikasi file twpol.txt. perhatikan setiap baris pada file tersebut. Lalu enkripsi file tersebut:

# nano /etc/tripwire/twpol.txt

# cd /etc/tripwire

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

*Karena yang diubah adalah file twpol.txt, maka twcfg.txt di atas kami ubah menjadi twpol.txt, dan hasilnya seperti ini :*



*Terjadi error pada baris ke-19. Kesalahan terjadi karena kesalahan parameter. Perintah yang benar untuk mengenkripsi file twpol menggunakan opsi --create-polfile bukan --create-cfgfile*

1. Modifikasi file tw.cfg. perhatikan setiap baris pada file tersebut. Laluenkripsi file tersebut:

# nano /etc/tripwire/twpol.txt

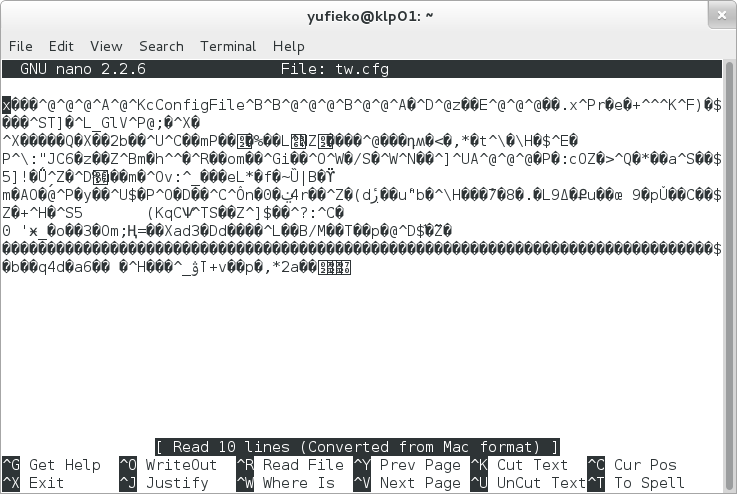
# cd /etc/tripwire

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

*Untuk percobaan ini hasilnya :*



*Berhasil, setelah mengeksekusi perintah kita diminta untuk memasukkan site passphrase yang telah kita tentukan pada saat instalasi. File konfigurasinya ditulis pada tw.cfg. berikut isi file tw.cfg :*



**Langkah percobaan III – inisialisasi database**

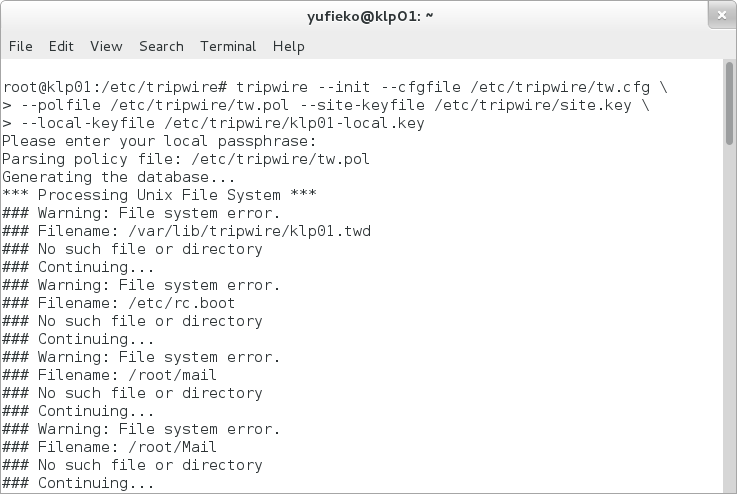
Setelah melakukan langkah-langkah pada point II, anda akan melakukan inisialisasi database dengan menjalankan perintah :

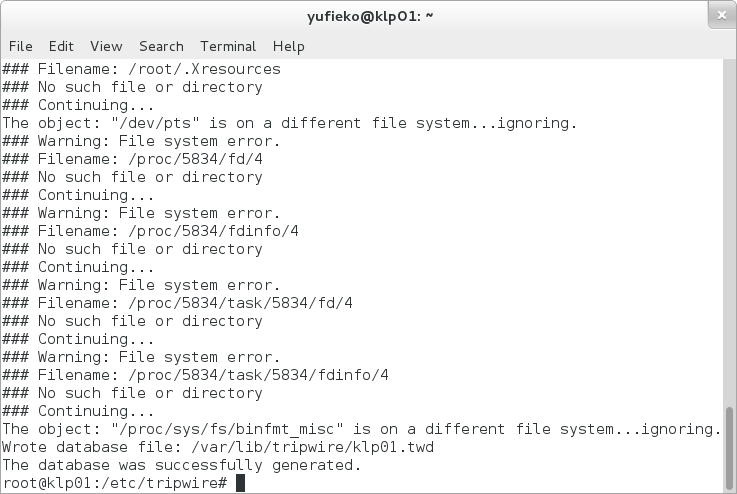
# tripwire --init --cfgfile /etc/tripwire/tw.cfg \

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

--local-keyfile /etc/tripwire/HOSTNAME-local.key

HOSTNAME alah nama host komputer Anda. Langka ini mungkin membutuhkan waktu yang relatif lama.



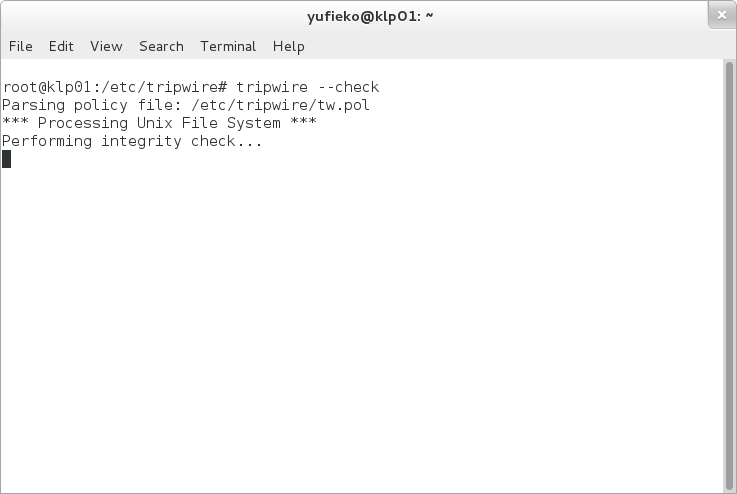


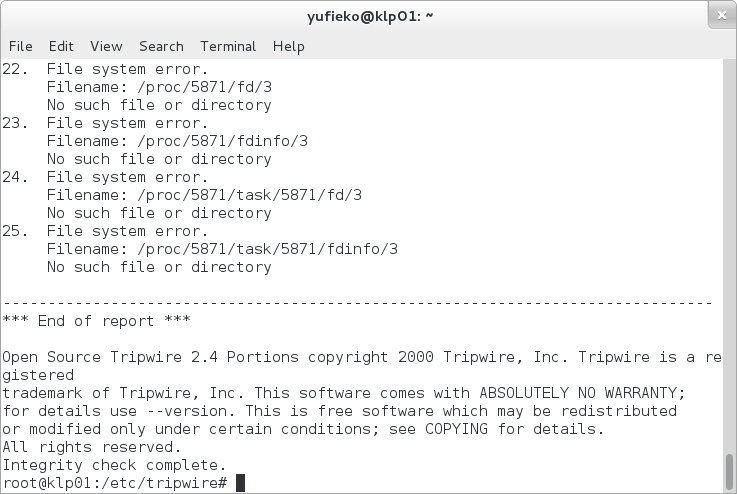
*Pada proses ini kita diminta memasukkan local passphrase.*

**Langkah percobaan IV – melakukan cek sistem**

Pada tahap ini tripwire menyimpan informasi awal dari file-file yang akan dimonitor perubahannya :

# tripwire –check

**



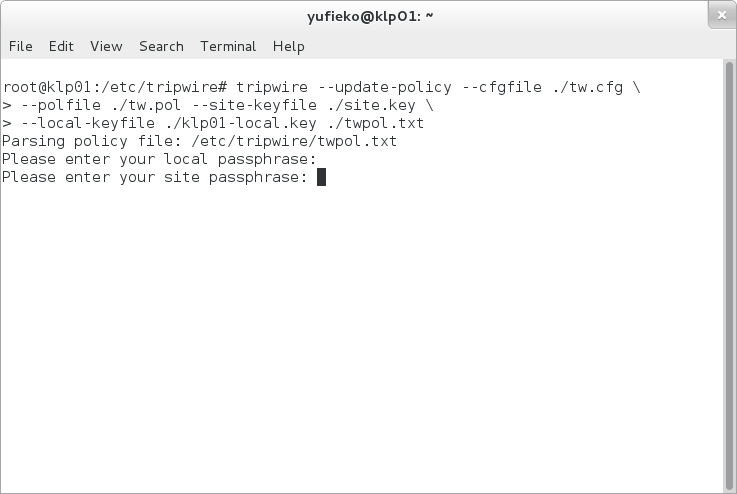
*Pada proses ini kita diminta memasukkan local passphrase.*

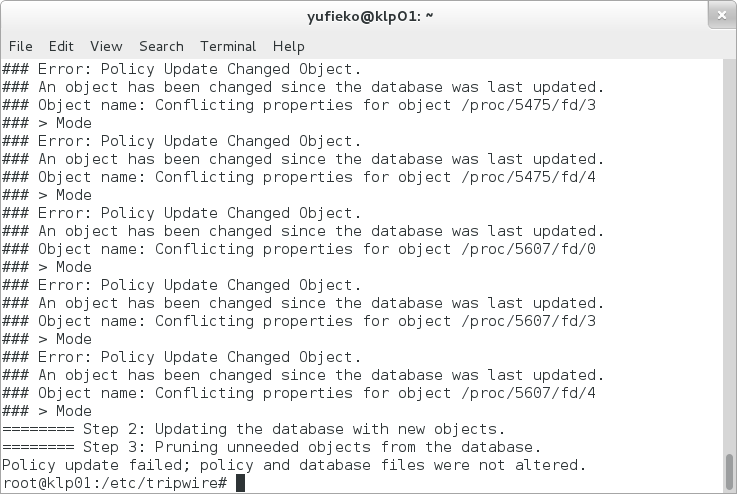
**Langkah percobaan V – melakukan update file “Policy”**

Apabila ada perubahan pada file twpol.txt, misalnya kita akan menambahkan atau mengurangi folder yang akan dimonitor maka kita harus melakukan update dengan menjalankan perintah :

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

--site-keyfile ./site.key --local-keyfile ./HOSTNAME-local.key ./twpol.txt





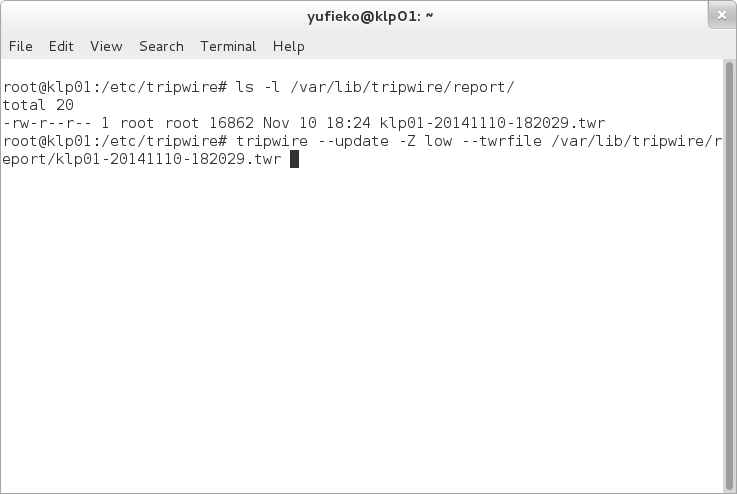
*Pada proses ini dilakukan pengecekan terhadap file policy dan database files dilihat dari parameter tanggal, ukuran dan atribut.*

**Langkah percobaan VI – melakukan update database dari System file**

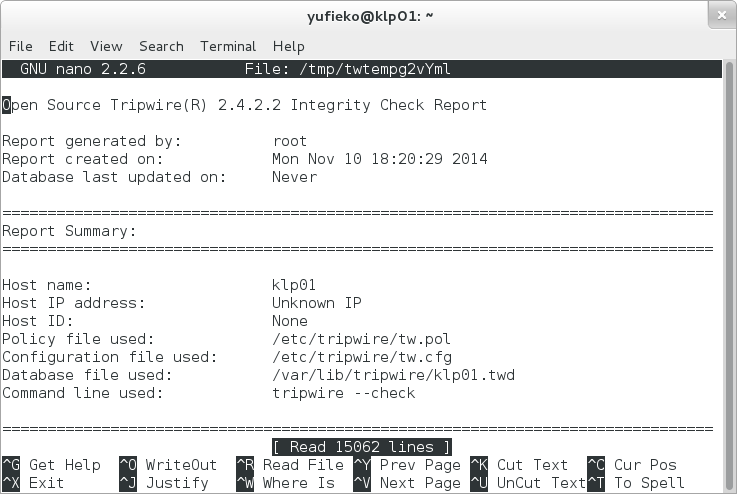
Database dari file system perlu di update secara berkala. Proses update dapat menggunakan perintah :

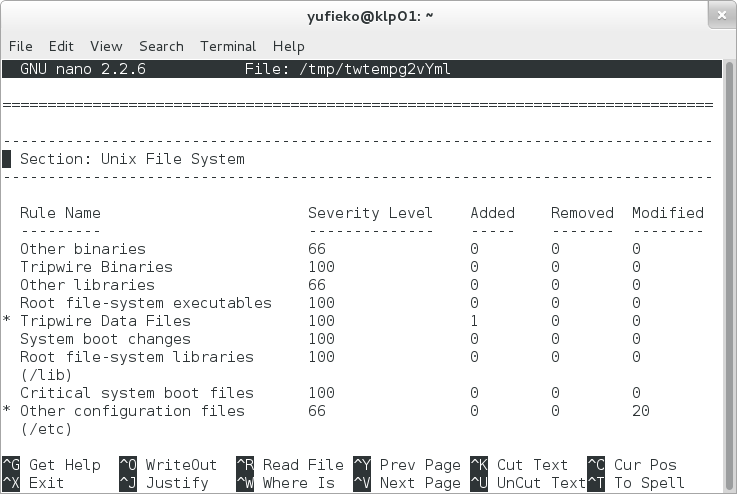
# tripwire --update -Z low --twrfile /var/lib/tripwire/report/host-yyyymmddtttttt.twr

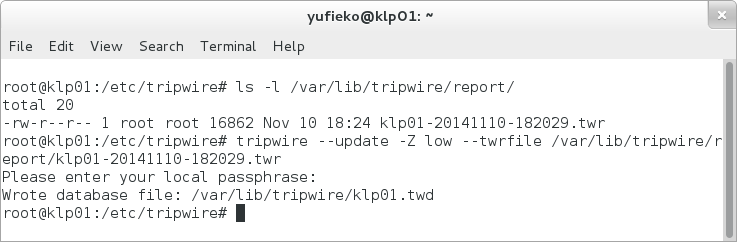
Perintah tersebut berarti bahwa tripwire akan membandingkan antara database yang ada dengan file yang ada di system, kemudian akan menjalankan editor untuk memilih perubahan di database. Opsi dari twrfile adalah file report yang dibangkitkan dan disimpan pada folder /var/lib/tripwire/report. Format penamaan file adalah berdasarkan tahun (yyyy), bulan (mm), tanggal(dd) dan jam dalam format (HH-MM-SS). Ekstensi file report adalah .twr.



*Ketika dijalankan akan membuka Integrity Check Report terlebih dahulu, baru setelah di tutup kita akan dimintai local passphrase, dan akan memulai menulis pada database file sesuai nama host sistem kita.*

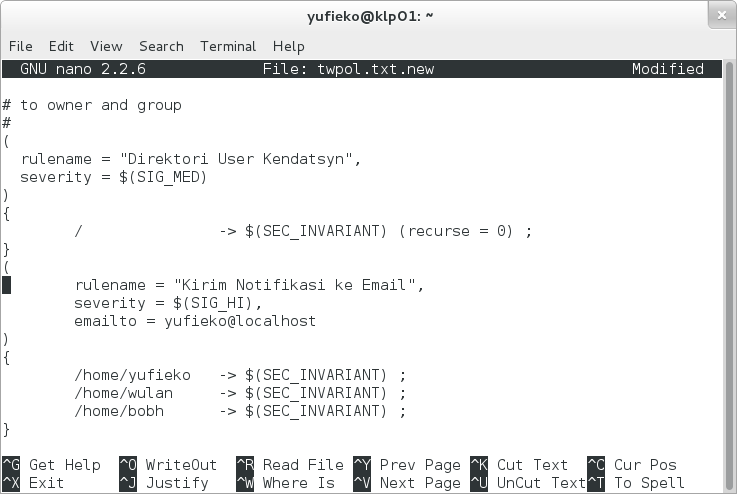






1. **TUGAS PERCOBAAN**
2. Sebelumnya direktori yang di Monitoring dipersempit

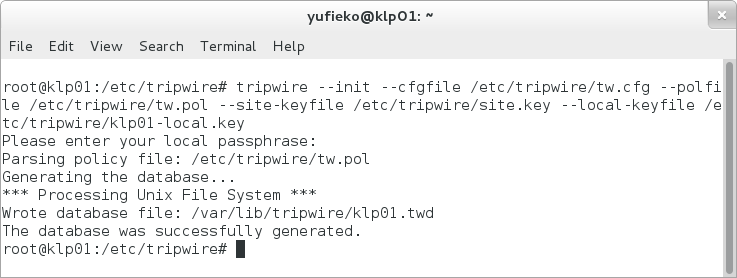
Kita modifikasi file twpol.txt dan kita simpan dengan twpol.txt.new



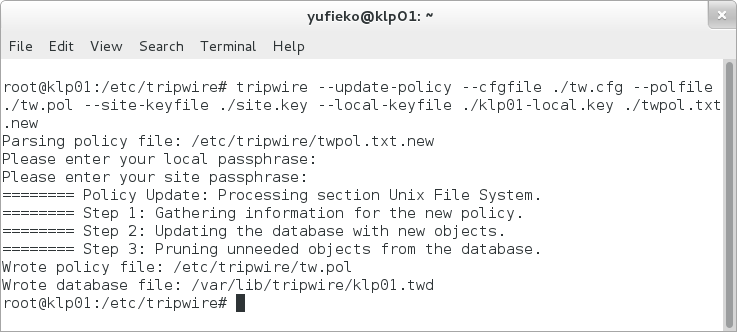
Lalu kita enkripsi file twpol.txt.new



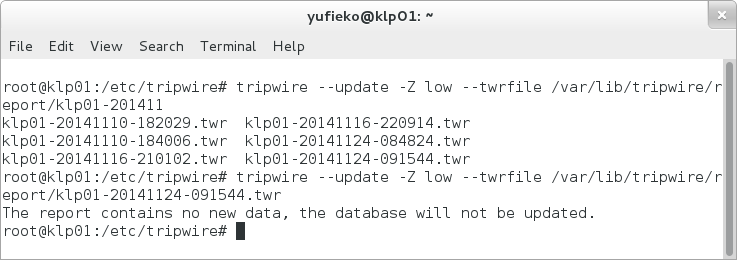
Lalu kita lakukan inisialisasi database



Setelah itu kita melakukan update file “Policy” agar perubahan yang kita buat pada file policy dapat diimplementasikan.



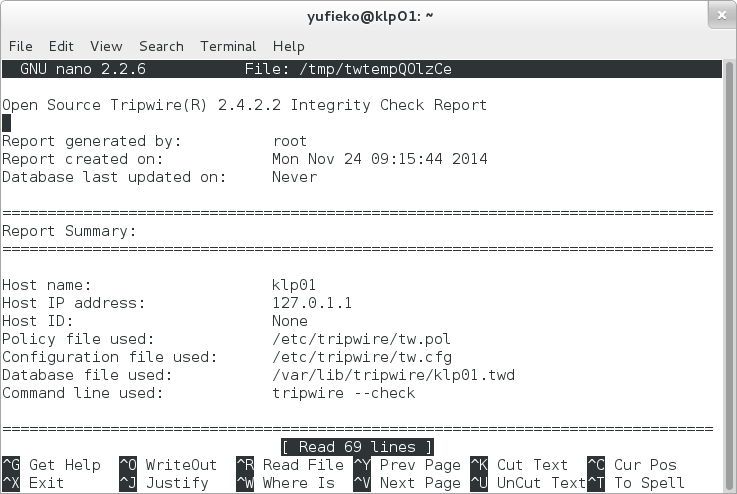
Lalu kita melakukan update database dari System file, database ini didapat dari perintah tripwire --check.

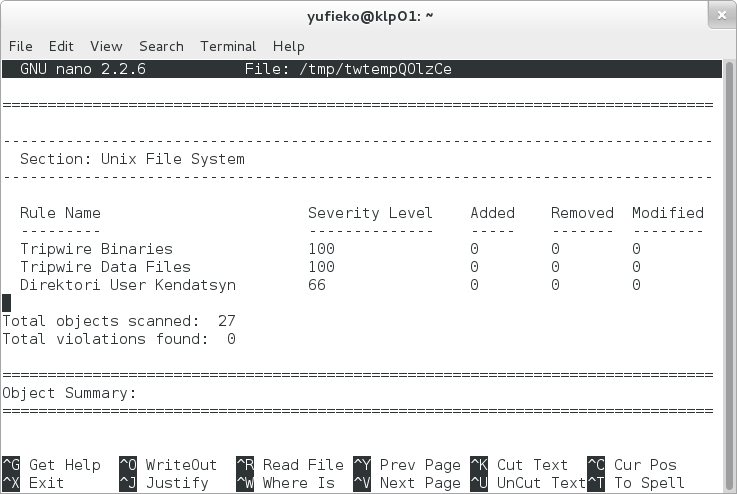


1. Jalankan perintah :

# tripwire –check

Catat dan analisa hasilnya

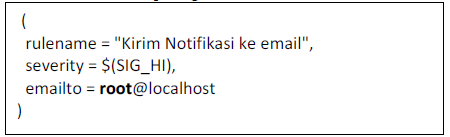


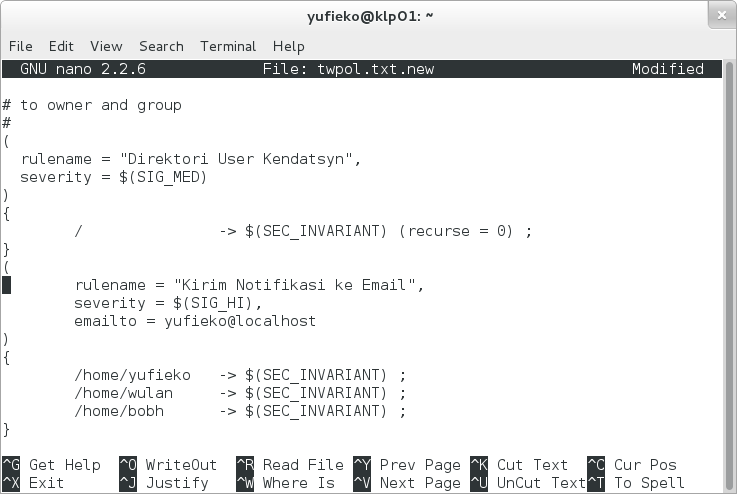


1. Kerjakan langkah-langkah di bawah dan analisa setiap langkahnya
   1. Ubah file policy twpol.txt

# nano /etc/tripwire/twpol.txt

* 1. Tambahkan di baris paling bawah :





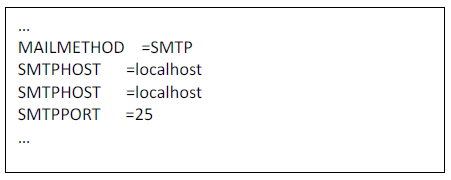
Email akan dikirimkan ke akun email dari root dari sistem yang Anda monitor. Biasanya, email akan ditujukan ke akun user yang dapat bertindak sebagai root.

* 1. Lakukan enkripsi terhadap file Anda

# cd /etc/tripwire

# twadmin –create-polfile –cfgfile ./tw.cfg –site-keyfile ./site.key ./twpol.txt

* 1. Ubah file konfigurasi untuk memasukkan informasi smtp :



* 1. Lakukan enkripsi terhadap file tersebut

# cd /etc/tripwire

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

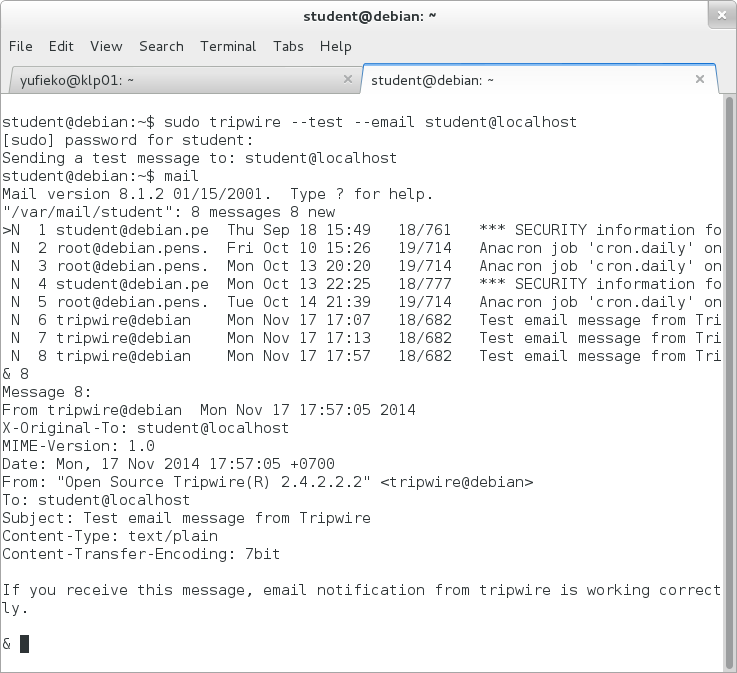


* 1. Jalankan tes dengan menggunakan perintah :

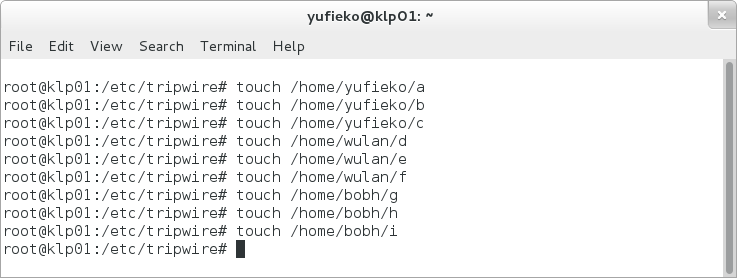
# tripwire --test --email student@localhost

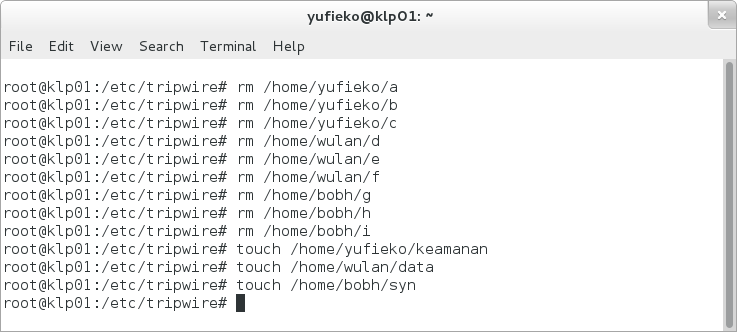
* 1. Cek email di akun user Anda

$ mail



1. Buat sebuah file kosong dan hapus beberapa file pada direktori yang di Monitoring

**

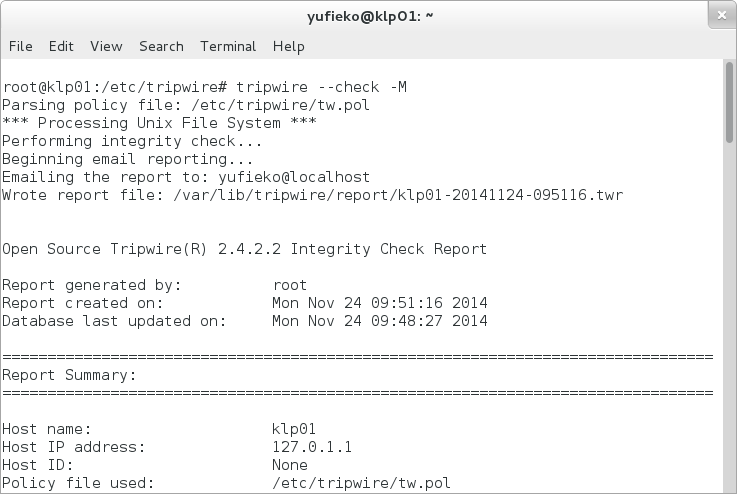


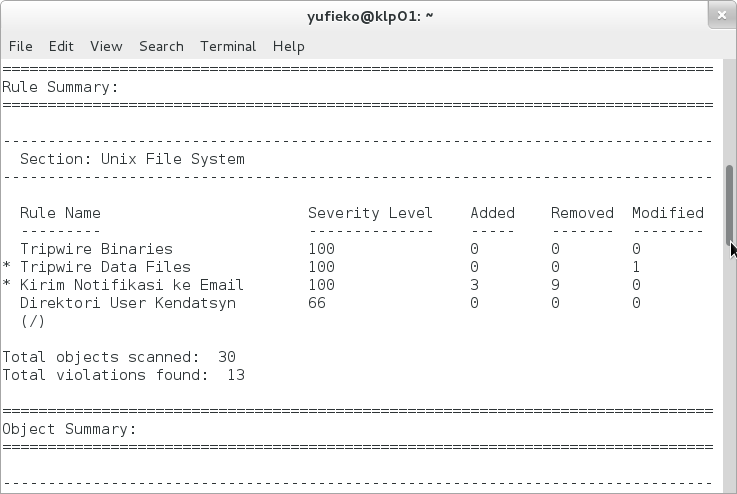
Lakukan cek konsistensi dengan menjalankan perintah :

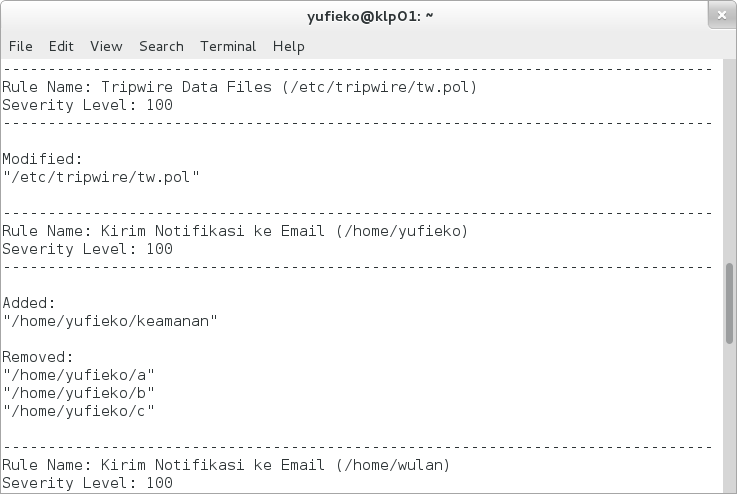
# tripwire --check –M

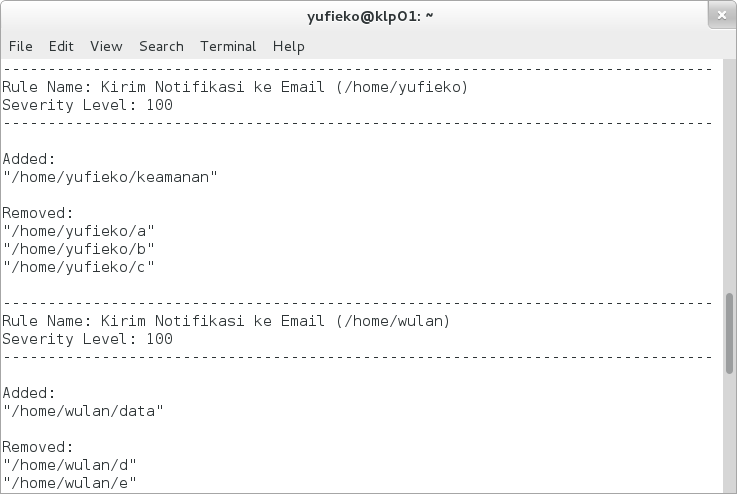
Opsi –M digunakan untuk mengirimkan laporan ke email yang telah ditentukan sebelumnya.

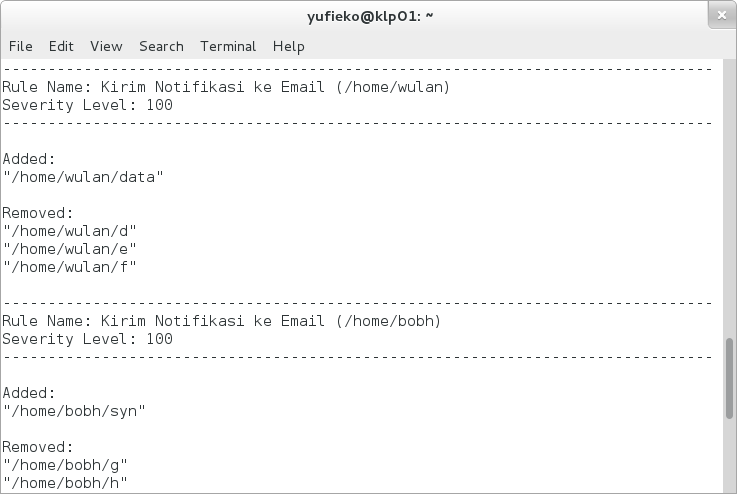
Catat dan analisa hasilnya.

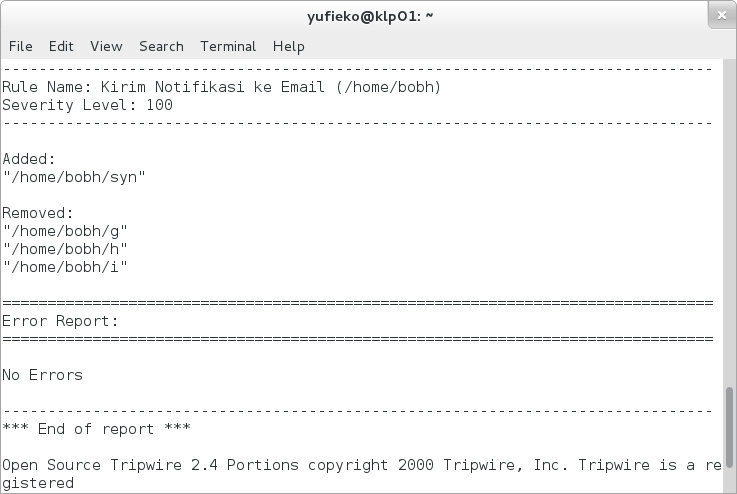




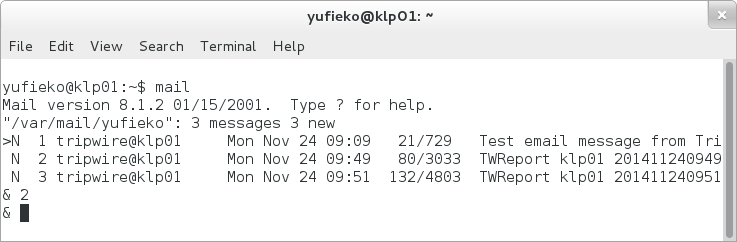


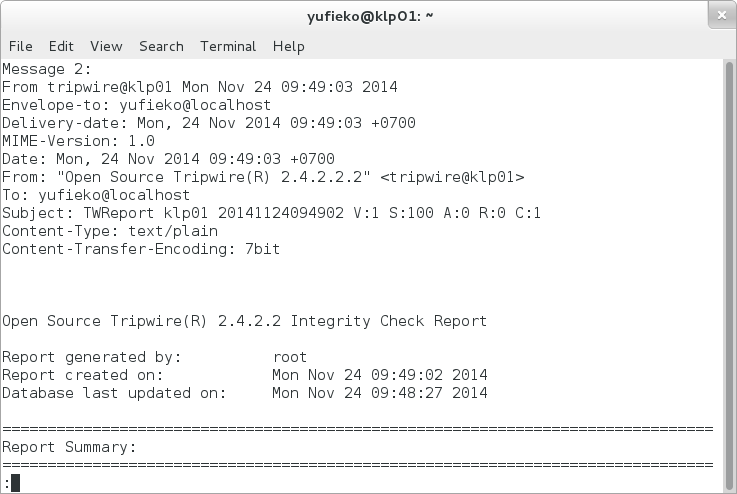






Lalu kita coba cek email dari user yufieko, yang dikirimi laporan oleh tripwire dengan perintah mail.





1. Bandingkan hasil dari perintah pada nomor 1 dan nomor 4

*Untuk hasil dari pengecekan perubahan pada direktori yang di*monitoring *di atas, terdapat perbedaan hasil yang didapat. Ketika menambahkan, menghapus ataupun memodifikasi sebuah file pada direktori yang di awasi tersebut, semua aktivitas tersebut dapat diketahui oleh tripwire, dengan membandingkan database yang telah di-*generate *sebelumnya dan dibandingkan dengan data terbaru. Nantinya dapat diketahui file apa saja yang di modifikasi, ditambahkan, ataupun dihapus.*

1. **LATIHAN**
2. Berikan kesimpulan hasil praktikum yang anda lakukan.

*Dari hasil praktikum di atas dapat diambil kesimpulan jika untuk mendeteksi anomali yang terjadi pada sistem kita (direktori ataupun file) kita dapat menggunakan aplikasi Tripwire. Dengan Tripwire kita bisa menentukan direktori yang akan kita awasi bilamana terjadi perubahan di dalamnya, yang mungkin dilakukan oleh penyusup. Tripwire dapat melihat perubahan yang terjadi berdasarkan tanggal modifikasi, ukuran file, atribut file dan ketersediaan file yang dicocokkan dengan database yang disimpan. Untuk melakukan konfigurasi direktori yang diawasi, bisa kita modifikasi file twpol.txt lalu kita* generate *dan perbarui file* policy-nya. *Untuk melakukan pengecekan, kita menggunakan perintah tripwire --check dan jika ingin mengirimkan laporannya ke email kita tambahkan opsi –M, dengan catatan kita telah mendefinisikan emailto pada* rule *direktori yang kita awasi.*

1. Berdasarkan percobaan yang anda lakukan, jelaskan cara kerja tripwire dalam melakukan integrity checker ?

*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.*

1. Carilah referensi baik dari buku maupun Internet, aturan-aturan apa saja yang bisa dideteksi oleh tripwire ?

*Untuk aturan yang dapat dideteksi oleh Tripwire meliputi modifikasi tanggal, ukuran file, atribut file dan ketersediaan file itu sendiri. Secara default untuk pengaturan pengawasan direktori pada Tripwire ada banyak mulai dari file milik Tripwire itu sendiri,* boot files, root file-system,root Control, configuration files *dan sebagainya.*

1. **DAFTAR PUSTAKA**
2. “Modul 8 Instrussion Detection System (Tripwire)”, URL <http://lecturer.eepis-its.edu/~zenhadi/kuliah/NetworkSecurity/Prakt%20Modul%208%20Tripwire.pdf>
3. URL <http://opensource.telkomspeedy.com/wiki/index.php/Tripwire:_Notifikasi_email>
4. URL <http://tyodongss.com/apa-itu-sudo/>
5. URL <http://www.sudo.ws/sudo/intro.html>
6. URL <http://www.tldp.org/pub/Linux/docs/HOWTO/translations/id/otherformats/html/ID-Security-HOWTO-5.html>.

**Kelompok 1 – 3 D3 IT B** :

1. Achmad Agus Salim (2103121035)
2. Yufi Eko Firmansyah (2103121049)
3. Retno Wulandari (2103121050)