Laporan Resmi Praktikum Keamanan Data – Host Based IDS

Dimas Rizky H.P. – 2110141011 – 3 D4 IT A

***Dasar Teori***

IDS (*Intrusion Detection System)* merupakan program yang digunakan untuk mendeteksi adanya *intrusion* atau serangan yang ditujukan terhadap jaringan/sistem. IDS memantau keadaan anomali jaringan ataupun file sistem yang salah satunya disebabkan oleh intruder. Setelah tahap pendeteksian, biasanya IDS di set untuk mengirim notifikasi/peringatan ke network administrator/system administrator.

Terdapat dua tipe IDS, yaitu Host-Based IDS (HIDS), dan Network-Based IDS (NIDS). Praktikum dan percobaan ini berfokus ke ranah Host-Bases IDS. Salah satu program yang digunakan adalah *Tripwire*. Tripwire berfungsi untuk menjaga integritas file sistem dan direktori, IDS ini bekerja dengan cara mencatat setiap perubahan yang terjadi pada file dan direktori.

Secara lebih terperinci, cara kerja tripwire adalah dengan melakukan perbandingan file dan direktori yang ada pada database system yang dibuat pada saat tripwire diinstall. Perbandingan tersebut meliputi perubahan tanggal, ukuran file, penghapusan, perubahan owner, perubahan hak akses, dan lainnya. Setelah tripwire dijalankan, database sistem secara otomatis dibuat. Kemudian secara periodik tripwire akan melakukan cek pada file dan direktori lalu melaporkannya pada system administrator jika terdapat perubahan.

Atribut yang dimonitor oleh tripwire adalah sebagai berikut :

8

7

6

5

4

3

2

1



Keterangan :

1. Link status, berupa directory ataukah file link ataukah file yang lain
2. Permission untuk masing masin tipe user dari file atau direktori, berurutan milik user, grup, atau other
3. Jumlah file yang ada pada direktori
4. Grup pemilik file
5. User pemilik file
6. Ukuran file dalam byte
7. Tanggal pembuatan/terakhir diakses atau dimodifikasi
8. Nama file

***Laporan Pendahuluan***

***Percobaan***

***Instalasi Tripwire***

* Lakukan update packet debian terbaru dengan perintah *$apt-get update*
* Lakukan instalasi tripwire dengan perintah *$apt-get install tripwire*
* Akan muncul dialog, pada dialog pertama, akan ditanyakan apakah ingin sekalian membuat site key passphrase pada saat instalasi, pilih Yes



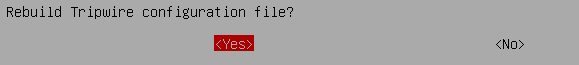
*Gambar 1.1, Dialog pertama instalasi tripwire*

* Lalu yang kedua ditanyakan apakah ingin membuat local key passphrase pada saat instalasi, pilih Yes



*Gambar 1.2, Dialog kedua instalasi tripwire*

* Dialog berikutnya menanyakan apakah ingin melakukan rebuild configuration file dari Tripwire, pilih Yes



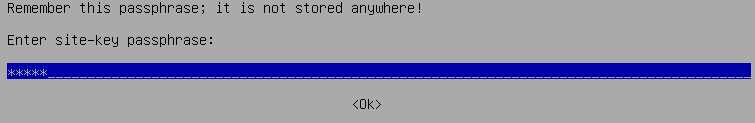
*Gambar 1.3, Dialog ketiga instalasi tripwire*

* Dialog selanjutnya menanyakan apakah ingin melakukan rebuild tripwire policy file juga pada saat instalasi, pilih Yes



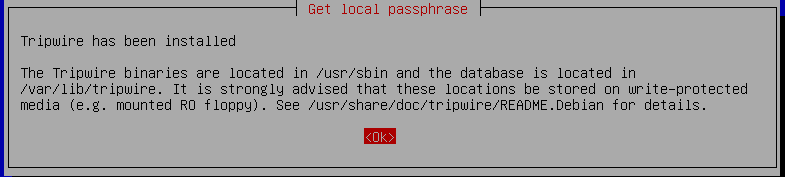
*Gambar 1.4, Dialog keempat instalasi tripwire*

* Dialog selanjutnya adalah dialog untuk memasukan key passpharase dan local key passphrase, inputkan data keduanya lalu program akan lanjut diinstall



*Gambar 1.5, Dialog kelima instalasi tripwire*

* Pada akhir instalasi tripwire akan muncul peringatan bahwa tripwire terinstall namun lokasi databasenya masih terletak pada direktori yang tidak write-protected, sehingga tidak aman menempatkaan database pada direktori tersebut.



*Gambar 1.6, Dialog selesai instalasi tripwire*

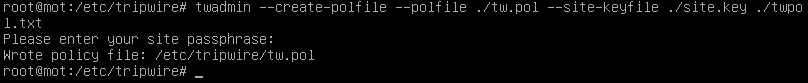
***Modifikasi file policy dan file konfigurasi***

* Buka direktori config tripwire dengan perintah *$cd /etc/tripwire/*



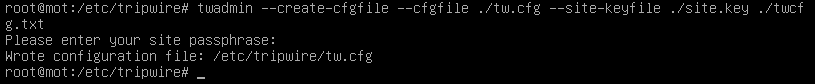
*Gambar 2.1, Direktori tripwire*

* Modifikasi file twpol.txt, lalu enkripsi file tersebut



*Gambar 2.2, Pembuatan enkripsi polfile dari file twpol.txt*

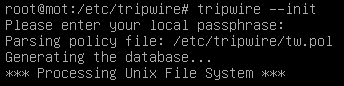
* Modifikasi file tw.cfg, lalu enkripsi file tersebut



*Gambar 2.3, Pembuatan enkripsi cfgfile dari file twcfg.txt*

***Inisialisasi Database***

* Lakukan inisialiasasi database dengan menjalankan perintah *$tripwire –init*



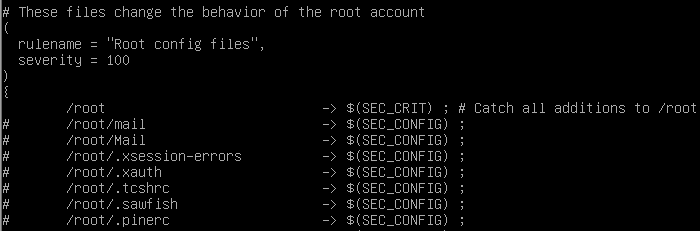
*Gambar 3.1, Inisialisasi database dengan parameter polfile dan cfgfile serta enkripsi menggunakan site passphrase*

* Pada saat melakukan init pertama kali, akan terjadi banyak error. Hal ini terjadi karena banyak modul default yang dimonitor oleh tripwire namun belum terinstall di sistem.



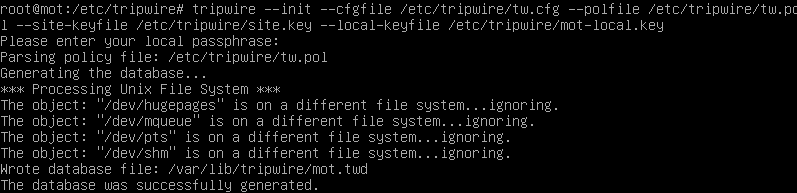
*Gambar 3.2, Error terjadi karena beberapa modul tidak terinstall pada sistem, sehingga harus dihapus dari file twpol.txt*

* Untuk memperbaikinya, lakukan edit pada file twpol.txt dengan cara melakukan comment pada modul yang menyebabkan error



*Gambar 3.3, Comment pada modul yang membuat error inisialisasi database tripwire*

* Jika database berhasil digenerate, akan muncul konfirmasi bahwa database telah dibuat



*Gambar 3.4, Database file sistem berhasil dibuat*

***Kirim email notifikasi***

* Tambahkan baris kode konfigurasi untuk mengirimkan email notifikasi bila terjadi anomali file pada twpol.txt.



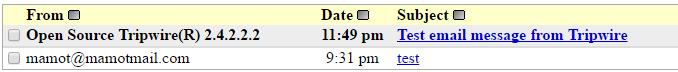
*Gambar 4.1, Setting pengiriman email ke email tujuan*

* Lakukan enkripsi file dan update database, lalu jalankan perintah *$tripwire –test –email <email yang dituju>*

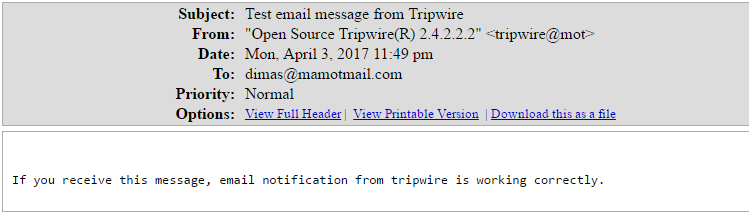


*Gambar 4.2, Test email dari tripwire ke email tujuan*

* Cek apakah email dari tripwire masuk ke inbox ataukah belum, jika belum maka perlu ada konfigurasi lebih lanjut pada mail servernya.



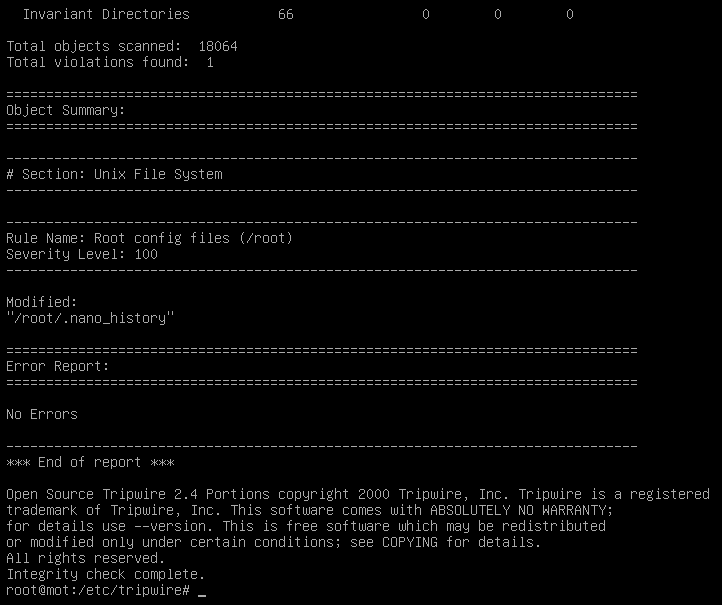
*Gambar 4.3, Email tripwire test berhasil masuk*



*Gambar 4.4, Email tripwire test berhasil masuk*

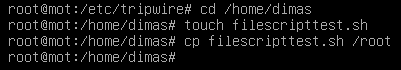
***Test scanning tripwire***

* Catat dan simpan terlebih dahulu hasil perintah *$tripwire –check*



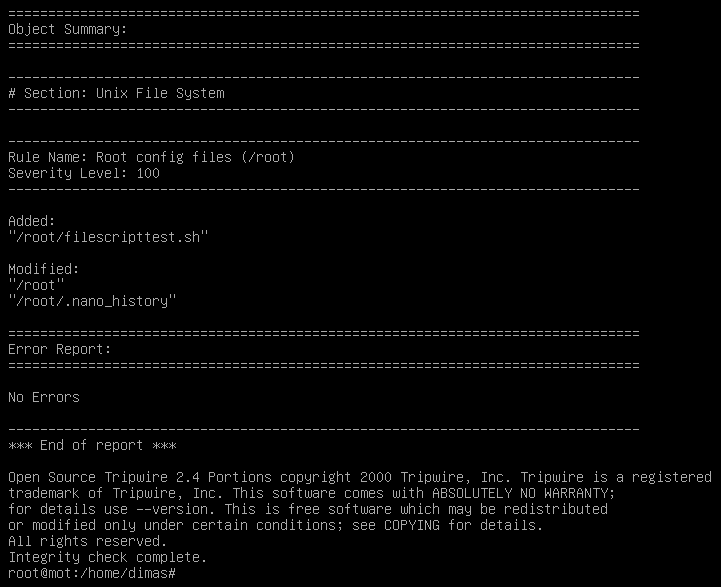
*Gambar 5.1, Test pertama kali dengan $tripwire –check*

* Untuk melakukan uji coba, buat file kosong pada direktori */bin*



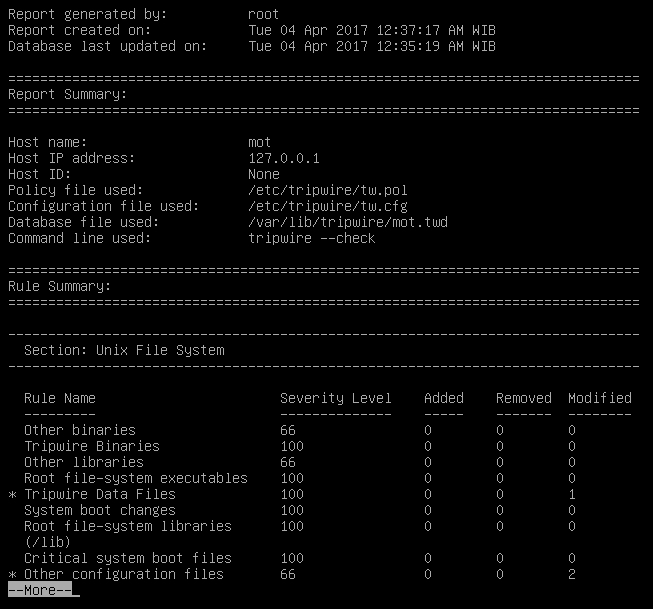
*Gambar 5.2, Test anomali file dengan menempatkan file asing ke direktori yang dimonitor oleh tripwire*

* Lalu jalankan perintah tripwire –check, tripwire akan melakukan cek pada masing masing file dan melaporkannya pada tampilan layar



*Gambar 5.3, Setelah dilakukan test monitoring file, tripwire akan melaporkan hasilnya pada layar, apa saja perubahan yang terjadi*

* Untuk melihat reportnya, dapat menggunakan perintah *$twprint –m r –twrfile /var/lib/tripwire/report/<file report yang ada pada folder>*



*Gambar 5.4, Untuk melihat report secara lengkap, terdapat di /var/lib/tripwire/report. Report dibuat setiap dijalankan tripwire --check*

***Analisa & Kesimpulan Percobaan***

* ***Tripwire membangun sistem database filenya berdasarkan rule yang dispesifikan pada file twpol.txt dan cfgfile.txt. Kedua file tersebut dijadikan patokan mana saja file sistem dan direktori yang harus dimonitor oleh tripwire.***
* ***Penyimpanan state file (identifikasi file) pada database tripwire berupa hash signature, yang mana sign tersebut nantinya akan dikomparasi/dibandingkan dengan file/direktori yang ada pada database setiap kali dijalankan check tripwire (integirty check)..***
* ***Setiap kali integrity check dijalankan pada tripwire, tripwire akan melakukan scanning terhadap violations yang telah dispesifikan pada policy file. Tripwire akan melakukan pembandingan hash sign file pada saat di scan dengan hash sign yang ada pada database.***
* ***Notifikasi berupa email dapat di setting pada twpol.txt dengan menspesifikan email penerima dan setting pada twcfg.txt untuk menspesiifkan protokol pengiriman emailnya.***