MODUL 8
INTRUSION DETECTION SYSTEM [TRIPWIRE]

TUJUAN PEMBELAJARAN:

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

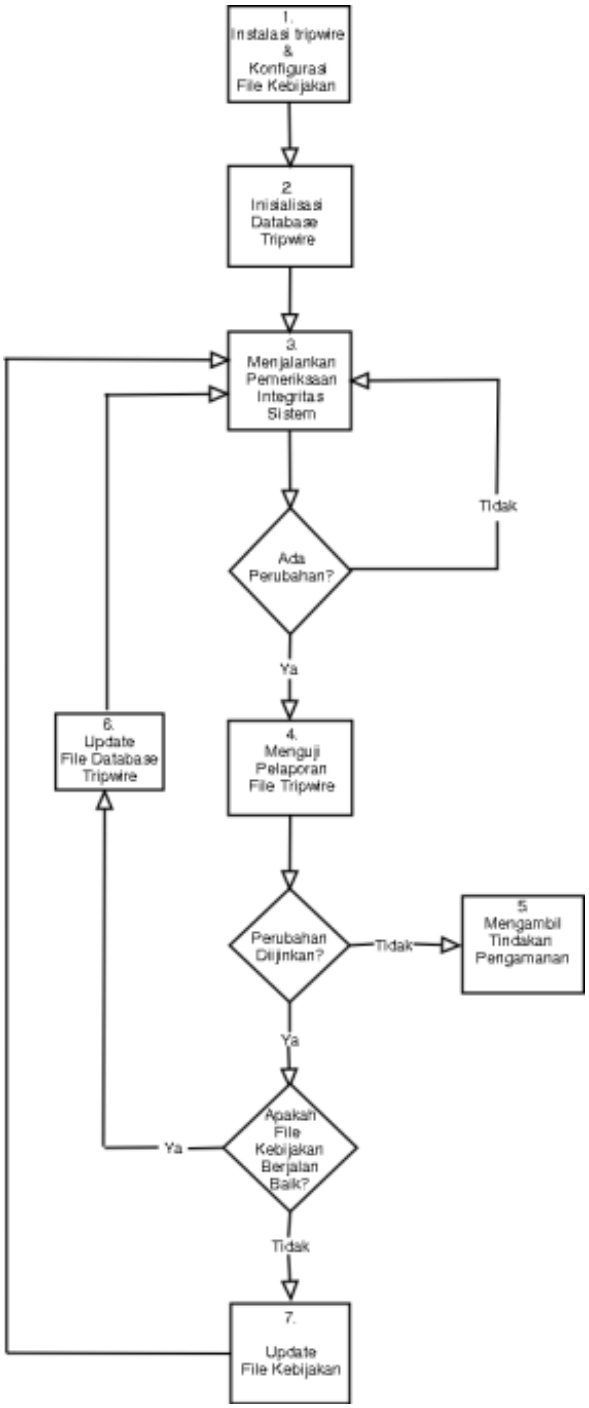
DASAR TEORI

Pemasangan program intrusi deteksi sebenarnya ditujukan untuk mendeteksi penyusup ataupun hacker ke suatu jaringan atau network dan bisa memantau seluruh ulah sang hacker yang sedang dilakukan olehnya.

Type IDS sendiri secara garis besar dibagi 2 yaitu hostbase dan network base IDS. Snort termasuk dalam Network base. Salah satu model host-based IDS adalah tripwire

Program tripwire berfungsi untuk menjaga integritas file system dan direktori, dengan mencatat setiap perubahan yang terjadi pada file dan direktori. Konfigurasi tripwire meliputi pelaporan melalui email, bila menemukan perubahan file yang tidak semestinya dan secara otomatis melakukan pemeriksaan file melalui cron. Penggunaan tripwire biasanya digunakan untuk mempermudah pekerjaan yang dilakukan oleh System Administrator dalam mengamankan System. Tripwire merupakan salah satu

Cara kerja tripwire adalah melakukan perbandingan file dan direktori yang ada dengan database sistem. 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.



Berikut ini merupakan penjelasan dari skema di atas:

1. Anda melakukan instalasi tripwire dan melakukan pengaturan *policy file* serta inisialisasi database,
2. Selanjutnya Anda bisa menjalankan pemeriksaan integritas sistem.
3. Bila ditemukan perubahan ukuran, tanggal maupun kepemilikan pada file tersebut, maka tripwire akan melakukan laporan pada sistem tentang adanya perubahan pada file terkait.

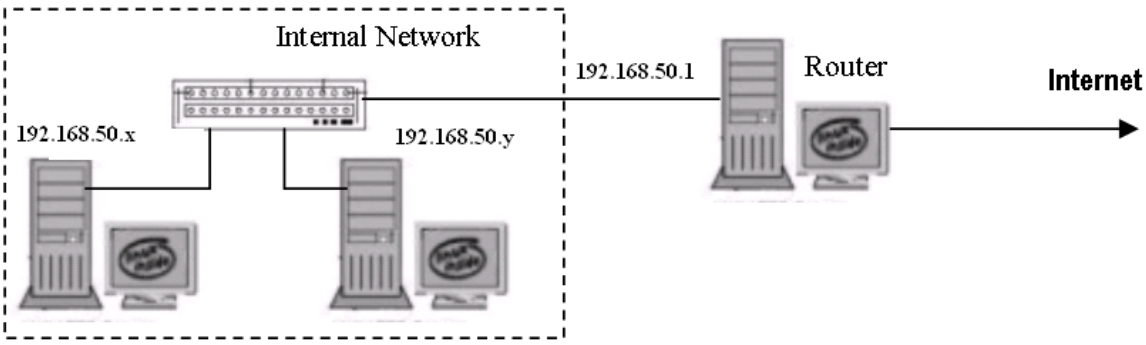
4. Jika perubahan tidak diijinkan, maka Anda bisa mengambil tindakan yang diperlukan.
5. Sebaliknya, jika perubahan pada file tersebut diijinkan, maka tripwire akan memeriksa *Policy File*, apakah policy file berjalan dengan baik?
6. Jika *policy file* tidak berjalan dengan benar, maka policy file harus di-update sesegera mungkin.
7. Jika *policy file* sudah berjalan dengan benar, maka tripwire akan melakukan update database file database.
8. Dan demikian seterusnya proses ini berlangsung.

TUGAS PENDAHULUAN

1. Jelaskan tentang konsep tripwire
2. Apa perbedaan IDS jenis tripwire, snort dan portsentry.

PERCOBAAN

1. Siapkan file source tripwire, ambil pada komputer yang sudah disediakan.
2. Bangunlah jaringan seperti berikut :



Gambar 1 Jaringan Percobaan

NB:
Gunakan dhclient di masing-masing PC untuk mendapatkan IP dari router.
192.168.50.x & y : IP dari router
Pilih 192.168.50.x sebagai PC Server yang akan dipasangi tripwire
Pilih 192.168.50.y sebagai PC Client

3. Lakukan installasi file tripwire yang ada pada PC Server

```
# apt-get install tripwire

Do you wish to create/use your site key passphrase during
installation ? <Yes>
Do you wish to create/use your local key passphrase during
installation ? <Yes>
Rebuild Tripwire configuration file ? <Yes>
Rebuild Tripwire policy file? <Yes>
```

4. Membuat kunci, dan akan digunakan untuk menjalankan tripwire.

```
Enter the site-key passphrase:
Repeat the site-key passphrase:
Generating key (this may take several minutes)...Key generation
complete.
Enter the local key passphrase:
Repeat the local keyfile passphrase:
```

```
Generating key (this may take several minutes)...Key generation
complete.
```

5. Inisialisasi tripwire, men-generate Database (kondisi awal) :
   ```
   # tripwire  --init
   ```
   NB : Menggunakan local key passphrase
6. Menjalankan tripwire, melakukan integrity check (pengecekan terhadap intruder)
   ```
   # tripwire  --check
   ```

7. Cek hasil tripwire, dengan menggunakan default policy, amati output yang dihasilkan :
   a. Default policy dapat dilihat di :
   ```
   # vim /etc/tripwire/twpol.txt
   ```
   b. Cek hasil tripwire (print report)
   ```
   # twprint –m r  --twrfile /var/lib/tripwire/report/<nama_file>.twr
   ```

   NB: <nama_file> sesuaikan dengan di komputer anda.

8. Cek dengan kondisi berikut ini :
   a. Lakukan telnet dari PC Client, dan buatlah sebuah file di folder /root di PC Server
   ```
   # telnet <no_ip_server>
   # touch /root/data.txt
   ```

   b. Ceklah kembali hasilnya di PC Server, amati dan catat apa yang terjadi
   ```
   # tripwire  --check
   ```

9. Update policy
   Untuk membuat policy yang baru lakukan langkah-langkah berikut :
   ☑ Buat file policy sesuai dengan kebutuhan (defaultnya adalah twpol.txt).
   ```
   # vim /etc/tripwire/txpol.txt.new

   SIG_HI      =  100; #Nilai yg menunjukkan kelemahan system pada critical files
   SEC_BIN   =  $(ReadOnly); #Binary file yang tidak boleh dirubah
   (
         rulename    = “Perc dgn policy baru”,
         severity = $(SIG_HI)
   )
   {
         /bin  -> $(SEC_BIN);
         /home -> $(SEC_BIN);
   }
   ```
   ☑ Perbaharui data tripwire:
   # twadmin --create-polfile -S /etc/tripwire/site.key /etc/tripwire/twpol.txt.new
   NB: Menggunakan site key passphrase
   ☑ Inisialisasi ulang
   ```
   # tripwire  --init
   ```
   NB: Menggunakan local key passphrase
   ☑ Jalankan kembali tripwire, amati dan catat hasilnya.
   ```
   # tripwire  --check
   ```

10. Lakukan beberapa percobaan untuk menguji policy diatas.
    a. Lakukan telnet dari PC Client dan tambahkan file pada folder /home di PC Server
    ```
    # telnet <no_ip_server>
    # touch /home/data.txt
    ```
    b. Copylah file mkdir pada folder /bin
    ```
    # cp  /bin/mkdir  /home
    ```

11. Jalankan kembali tripwire dan ceklah hasilnya (amati dan catat hasilnya) :
```
# tripwire  --check
# twprint -m r  --twrfile /var/lib/tripwire/report/<name>.twr
```
NB: <name> sesuaikan dengan di komputer anda.

12. Supaya tripwire bisa disetting sesuai keperluan, misal akan melakukan cek setiap hari, tambahkan file tripwire-check sebagai berikut :
    a. `vim /home/coba.sh`
```
#!/bin/sh
HOST_NAME=`uname -n`
if [  ! -e /var/lib/tripwire/${HOST_NAME}.twd ]; then
   echo "Error: Tripwire database for ${HOST_NAME} not found"
   echo "Run "/usr/sbin/tripwire --init""
else
   test -f /etc/tripwire/tw.cfg && /usr/sbin/tripwire --check
fi
```

    b. Ubah file diatas agar bisa diexecute
```
# chmod +x /home/coba.sh
```

    c. Masukkan file tersebut ke cron.daily agar dijalankan setiap hari
```
# cp /home/coba.sh /etc/cron.daily/coba.sh
```

Keterangan :
Pembuatan crontab :

```
*     *     *     *     *  Command to be executed
-     -     -     -     -
|     |     |     |     |
|     |     |     |     +----- Day of week (0-7)
|     |     |     +------- Month (1 - 12)
|     |     +--------- Day of month (1 - 31)
|     +----------- Hour (0 - 23)
+------------- Min (0 - 59)
```

The fields are:

1. The number of minutes after the hour (0 to 59)
2. The hour in military time (24 hour) format (0 to 23)
3. The day of the month (1 to 31)
4. The month (1 to 12)
5. The day of the week(0 or 7 is Sun, or use name)
6. The command to run

Semua hasil crontab disimpan dalam : /var/spool/cron/crontabs/

Contoh :
a. Untuk menambahkan schedule
crontab –e
```
0   8   *   *   1  /etc/cron.daily/coba.sh
```

NB: Akan dijalankan setiap hari senin pada jam 8 pagi.

b. Untuk mengecek list
crontab –l

LAPORAN RESMI

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Berdasarkan percobaan yang anda lakukan jelaskan cara kerja tripwire dalam melakukan integrity checker?
3. Carilah di internet, rule apa saja yang bisa dideteksi oleh tripwire

LEMBAR ANALISA

Praktikum Network Security (IDS - tripwire)
Tanggal Praktikum :
Kelas :
Nama dan NRP :

A. Gambar topologi jaringan beserta dengan IP Addressnya

B. Catat password site key dan local key anda

C. Catat hasil pada poin 5 (tripwire --init)

D. Catat hasil pada poin 6 (tripwire --check)

E. Catat hasil pada poin 8 (penambahan data dari PC Client)

F. Buat policy baru dan catat hasilnya pada poin 9

G. Lakukan pengujian pada policy diatas dan catat hasilnya (poin 10-11)