Modul 1

Host-based IDS

A. TUJUAN PEMBELAJARAN

1. Siswa memahami konsep aplikasi client server di jaringan.
2. Mahasiswa memahami konsep pemprograman socket dasar.
3. Mahasiswa mampu membangun program socket sederhana dg single thread

B. DASAR TEORI

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.

C. PERCOBAAN :

I. Proses Instalasi

1. Login sebagai root
2. Lakukan sinkronisasi terkini index paket software lokal dengan repository
   #apt-get update
3. Lakukan installasi tripwire
   # apt-get install tripwire
   Lalu akan muncul dialog seperti dibawah. Perhatikan pesan yang muncul pada setiap dialog, lalu jawab dengan "Yes".

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

   - `Enter site key passphrase`
   - `Repeat the site-key passphrase`
   - `Enter local key passphrase`

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

Tripwire has been installed

The Tripwire binaries are located in /usr/sbin and the database is located in /var/lib/tripwire. It is strongly advised that these locations be stored on write protected media (e.g. mounted RO floppy). See /usr/share/doc/tripwire/README.Debian for details.

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

   #cd /etc/tripwire

   #chmod 0600 tw.cfg tw.pol

II. Melakukan modifikasi pada file "Policy" dan file konfigurasi

Setelah proses instalasi berakhir, lakukan langkah-langkah dibawah ini :

1. Modifikasi file twpol.txt. Perhatikan setiap baris pada file tersebut. Lalu Enkripsi file tersebut.

   # vi /etc/tripwire/twpol.txt

   # cd /etc/tripwire

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

2. Modifikasi file tw.cfg. Perhatikan setiap baris pada file tersebut. Lalu Enkripsi file tersebut.

   # vi /etc/tripwire/twcfg.txt
   # cd /etc/tripwire
   # twadmin --create-cfgfile --cfgfile ./tw.cfg
   --site-keyfile ./site.key ./twcfg.txt

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 adalah nama host komputer anda. Langka ini mungkin membutuhkan waktu yang relatif lama.

IV. Melakukan cek system

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

```
# tripwire --check
```

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 :

```
# cd /
 # tripwire --update-policy --cfgfile ./tw.cfg    --polfile ./tw.pol \
   --site-keyfile ./site.key  --local-keyfile ./HOSTNAME-local.key ./twpol.txt
```

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-yyyymmdd-
   ttttt.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.

D. TUGAS PERCOBAAN:

1. Jalankan perintah :

   # tripwire –check

   Catat dan analisa hasilnya.

2. Kerjakan langkah-langkah dibawah dan analisa setiap langkahnya

   a. Ubah file policy twpol.txt

   # vim /etc/tripwire/twpol.txt

   b. Tambahkan di baris paling bawah

```
(
 rulename = "Kirim Notifikasi ke email",
 severity = $(SIG_HI),
 emailto = root@localhost
)
```

   Email akan dikirimkan ke akun email dari root dari system yang anda monitor. Biasanya, email akan ditujukan kea kun user yang dapat bertindak sebagai root.

   c. Lakukan enkripsi terhadap file anda

   # cd /etc/tripwire

   # twadmin --create-polfile --cfgfile ./tw.cfg \

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

   d. Ubah file konfigurasi untuk memasukkan informasi smtp :

   # vi /etc/tripwire/twcfg.txt

```
...
MAILMETHOD    =SMTP
SMTPHOST      =localhost
SMTPHOST      =localhost
SMTPPORT      =25
...
```

e. Lakukan enkripsi terhadap file tersebut

   # cd /etc/tripwire

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

f. Jalankan test dengan menggunakan perintah :

   # tripwire –test –email root@localhost

g. Check email di akun user anda

   $ mail

3. Buat sebuah file kosong . Kemudian salinlah ke dalam direktori /bin

   # touch newfile.sh

   # cp newfile.sh /root

4. Lakukan cek konsistensi dengan menjalankan perintah :

   # tripwire –check

   Catat dan analisa hasilnya.

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

E. LATIHAN

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Berdasarkan percobaan yang anda lakukan, jelaskan cara kerja tripwire dalam melakukan *integrity checker* ?

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

Daftar Pustaka

1. “Modul 8 Instrussion Detection System (Tripwire)”, URL http://lecturer.eepis-its.edu/~zenhadi/kuliah/NetworkSecurity/Prakt%20Modul%208%20Tripwire.pdf
2. ”URL http://opensource.telkomspeedy.com/wiki/index.php/Tripwire:_Notifikasi_e-mail
3. URL http://www.tldp.org/pub/Linux/docs/HOWTO/translations/id/other-formats/html/ID-Security-HOWTO-5.html