

Nama : Mohammad Nur Azmi  
Nim : 1310651075  
Kelas : E

No 1

### Kriptografi

Kriptografi adalah menulis sebuah rahasia komunikasi yang aman yang dapat dipahami oleh penerima yang dimaksud saja. fakta bahwa data sedang dikirim mungkin diketahui, tetapi isi data yang harus tetap tidak diketahui kepada pihak ketiga. Data yang dimaksud (bergerak pada jaringan) dan saat istirahat (yang tersimpan pada perangkat seperti disk) dapat dienkripsi.

### KONSEP KRIPTOGRAFI CORNERSTONE

Konsep kriptografi dasar yang diwujudkan oleh semua enkripsi yang kuat dan harus dipahami sebelum belajar tentang implementasi spesifik.

Istilah kunci :

Kriptologi adalah ilmu komunikasi yang aman. Kriptografi menciptakan pesan makna yang tersembunyi;

kriptanalisis adalah ilmu melanggar pesan terenkripsi. Banyak menggunakan kriptografi jangka di tempat kriptologi: penting untuk diingat bahwa kriptologi meliputi kriptografi dan pembacaan sandi.

Tujuan dari kriptanalisis ialah untuk menemukan kelemahan dan ketidakamanan skema kriptografi, sehingga memungkinkan peningkatan atau perbaikan.

Kerahasiaan, integritas, otentikasi, dan nonrepudiation

-Kriptografi dapat memberikan kerahasiaan dan integritas (data tidak diubah dengan cara yang tidak sah)

-Kriptografi juga dapat memberikan otentikasi (membuktikan klaim identitas).

-Kriptografi dapat memberikan nonrepudiation, yang merupakan jaminan bahwa pengguna tertentu melakukan transaksi tertentu dan bahwa transaksi tidak berubah.

### Kriptografi Exclusive Or (XOR)

Exclusive Or (XOR) adalah "rahasia saus" di belakang enkripsi modern. Menggabungkan kunci dengan plaintext melalui XOR menciptakan ciphertext a. XOR-ing untuk kunci yang sama dengan

ciphertext mengembalikan plaintext asli. XOR matematika cepat dan sederhana.

Dua bit adalah benar (atau 1) jika satu atau yang lain (eksklusif, tidak keduanya) adalah 1.

### Jenis kriptografi :

Ada tiga jenis utama dari enkripsi yang modern: simetris, asimetris, dan hashing.

1. Enkripsi simetris menggunakan satu kunci: mengenkripsi kunci yang sama dan mendekripsi.

2. Kriptografi asimetris menggunakan dua kunci: jika Anda mengenkripsi dengan satu tombol, Anda mungkin mendekripsi dengan yang lain.
3. Hashing adalah transformasi kriptografi satu arah menggunakan algoritma (dan tidak ada tombol).

Protokol kriptografi governance menggambarkan proses pemilihan kanan metode (cipher) dan pelaksanaan untuk pekerjaan yang tepat, biasanya pada skala organisasi. Misalnya, tanda tangan digital menyediakan otentikasi dan integritas, tetapi tidak kerahasiaan. Cipher simetris terutama digunakan untuk kerahasiaan, dan AES adalah lebih lebih DES karena kekuatan dan kinerja alasan.

#### ENCRYPTION SYMMETRIC

Enkripsi simetris menggunakan satu kunci untuk mengenkripsi dan mendekripsi. Jika Anda mengenkripsi file zip dan kemudian mendekripsi dengan kunci yang sama, Anda menggunakan enkripsi simetris. Simetris enkripsi juga disebut "kunci rahasia" enkripsi: kunci harus dirahasiakan dari pihak ketiga. Kekuatan termasuk kecepatan dan kekuatan kriptografi per bit dari kunci. Itu kelemahan utama adalah bahwa kunci harus aman bersama sebelum kedua pihak dapat berkomunikasi aman.

#### **Kriptosistem**

Satu atau lebih kriptografi sederhana sering digunakan untuk mengembangkan algoritma yang lebih kompleks, disebut sistem kriptografi, atau *kriptosistem*. Kriptosistem (seperti *enkripsi ElGamal* didesain untuk menyediakan fungsi tertentu (seperti enkripsi kunci publik) sembari menjamin sifat keamanan tertentu keamanan (seperti serangan teks-terpilih) seperti pada model oracle acak. Kriptosistem menggunakan sifat kriptografi sederhana utama untuk mendukung sifat keamanan sistem. Tentu saja, karena perbedaan antara kriptosistem dan kriptografi tidak jelas, kriptosistem yang canggih dapat diperoleh dari kombinasi beberapa kriptosistem sederhana. Pada banyak kasus, struktur kriptosistem melibatkan komunikasi maju mundur di antara dua atau lebih kelompok dalam ruangan. (seperti di antara pengirim dari pesan aman dan penerimanya) atau melewati waktu (seperti data yang dilindungi dengan kriptografi). Kriptosistem yang seperti itu disebut *protokol kriptografi*.

Beberapa kriptosistem yang terkenal termasuk *enkripsi RSA*, *tanda tangan Schnorr*, enkripsi El-Gamal, *PGP*, dll. Kriptosistem yang lebih rumit melibatkan sistem *uang elektronik*, sistem *tanda-tangan enkripsi*, dll. Beberapa kriptosistem *teoritik* termasuk sistem *pembuktian interaktif*, seperti *pembuktian pengetahuan-nol*), sistem untuk *pembagian rahasia*.

#### **Pembukaan paksa kunci enkripsi**

Di Inggris, undang-undang Inggris memberikan izin kepada polisi untuk memaksa pelaku mengungkapkan berkas dekripsi atau memberikan password yang melindungi kunci enkripsi. Tidak memberikan kunci merupakan pelanggaran hukum, dan dikenakan hukuman dua hingga lima tahun penjara jika melibatkan keamanan nasional. Penuntutan yang berhasil telah terjadi di bawah undang-undang ini; pertama, di tahun 2009, menghasilkan 13 bulan

penjara. Hukum pemaksaan yang sejenis juga terdapat di Australia, Finlandia, Perancis, dan India memaksa terdakwa untuk memberikan kunci enkripsi atau password selama investigasi kriminal.

Di Amerika Serikat, kasus kriminal Amerika vs Fricosu menunjukkan jika surat perintah dapat memaksa seseorang untuk mengungkapkan kunci enkripsi atau password. *Elektronik Frontier Foundation* (EFF) memperdebatkan masalah ini atas pelanggaran perlindungan hak asasi manusia berdasarkan Undang-Undang Dasar. Pada tahun 2002, pengadilan membuat undang-undang, bahwa terdakwa harus membawa perangkat keras yang tak terenkripsi ke persidangan.

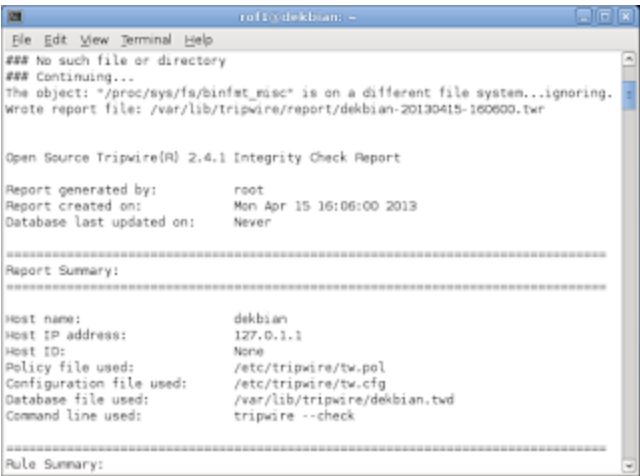
No 2

1. Hasil analisa perintah tripwire –check

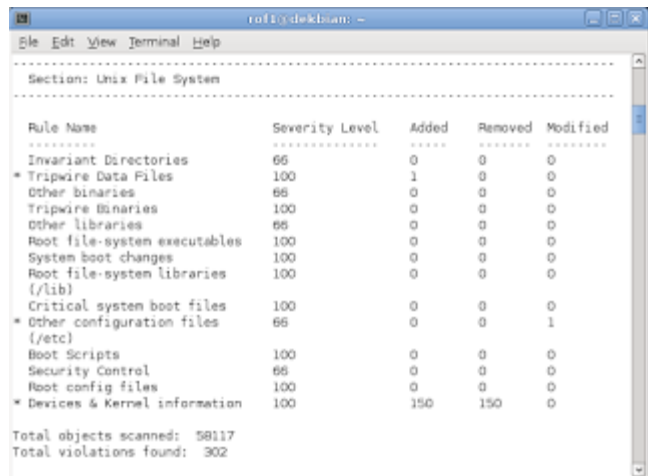
Hasil dari tripwire –check adalah pembuatan report hasil cek yang ada di /var/lib/tripwire/ yang berisi laporan tentang kondisi system ketika tripwire diinstal.

Nama report merupakan nama host yang diikuti oleh tanggal dan jam. Seperti dekbian-20130415-100600.twr. dekbian = nama host computer kita. 20130415 = tanggal pembuatan report yaitu tanggal 15 april 2013. 160600 = jam pembuatan report yaitu jam 4 sore, menit 6 dan detik 00.

Isi dari report tersebut antara lain :



Report dibuat oleh root pada tanggal 15 april 2013 pada host dekbian.  
police file yang digunakan = tw.pol,  
konfigurasi yang digunakan = tw.cfg  
database yang digunakan = dekbian.twd



Dari gambar diatas terjadi penambahan 1 data dengan security level 100 dan konfigurasi pada folder /etc pada security level 66. Total objek yang discan 58117 dan pelanggaran / perubahan yang ditemukan 302.

```
root@dekbian: ~
File Edit View Terminal Help
=====
Object Summary:
=====
# Section: Unix File System
=====
Rule Name: Tripwire Data Files (/var/lib/tripwire/dekbian.twd)
Severity Level: 100
=====
Added:
"/var/lib/tripwire/dekbian.twd"
=====
Rule Name: Other configuration files (/etc)
Severity Level: 66
=====
Modified:
"/etc/tripwire"
=====
Rule Name: Devices & Kernel information (/proc)
Severity Level: 100
=====
```

Sebelumnya telah disebutkan bahwa ada penambahan data. Disini dijelaskan bahwa penambahan data yang dimaksud adalah file dekbian.twd yang berupa database tripware pada folder /var/lib/tripwire pada security level = 100.  
Adapuun modifikasi yang dilakukan adalah pada folder /etc/tripwire pada security level = 66.

Kerjakan langkah-langkah dan analisa hasilnya

- a. Ubah file policy twpol.txt
- b. Tambahkan source code

```
*twpol.txt (/etc/tripwire) - gedit (as superuser)
File Edit View Search Documents Help
=====
# Commonly accessed directories that should remain static with regards
# to owner and group
#
{
  rulename = "Invariant Directories",
  severity = $(SIG_MED)
}
{
  /home      -> $(SEC_INVARIANT) (recurse = 0) ;
  /tmp       -> $(SEC_INVARIANT) (recurse = 0) ;
  /usr       -> $(SEC_INVARIANT) (recurse = 0) ;
  /var       -> $(SEC_INVARIANT) (recurse = 0) ;
  /var/tmp   -> $(SEC_INVARIANT) (recurse = 0) ;
}
{
  rulename = "kirin notifikasi ke email",
  severity = $(SIG_HI),
  emailto = root@localhost
}
}
```

- c. Lakukan enkripsi

```
root@dekbian:/etc/tripwire# twadmin --create-polfile --cfgfile ./tw.cfg --site-keyfile ./site.key ./twpol.txt
### Error: Policy file parsing problem.
### Syntax error: Line number 284
### Exiting...
The policy file was not altered.
root@dekbian:/etc/tripwire#
```

- d. Ubah file konfigurasi smtp

```
twcfg.txt (/etc/tripwire) - gedit (as superuser)
File Edit View Search Documents Help
=====
ROOT=/usr/sbin
POLFILE=/etc/tripwire/tw.pol
DEFFILE=/var/lib/tripwire/$(HOSTNAME).twd
REPORTFILE=/var/lib/tripwire/report/$(HOSTNAME)-$(DATE).twr
SITEKEYFILE=/etc/tripwire/site.key
LOCALKEYFILE=/etc/tripwire/$(HOSTNAME)-local.key
EDITOR=/usr/bin/editor
LATEPROMPTING=false
LOGSDIRECTORYCHECKING=false
MAILNOVIOLATIONS=true
EMAILREPORTLEVEL=3
REPORTLEVEL=3
SYSLOGREPORTING=true
MAILMETHOD=SMTP
SMTPHOST=localhost
SMTPPORT=25
```

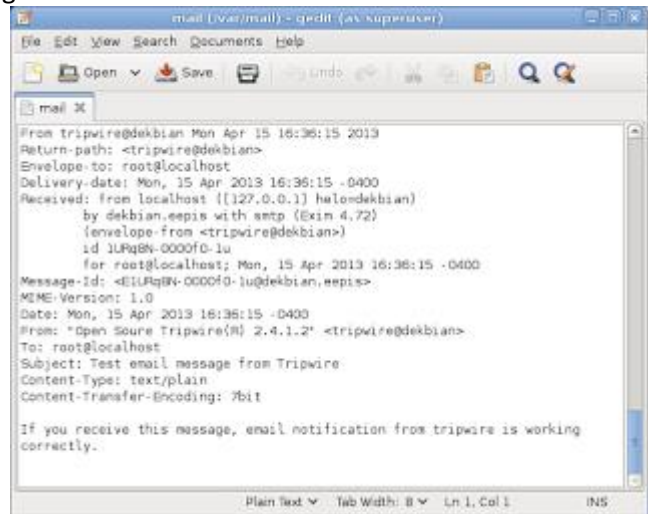
- e. Lakukan enkripsi

```
root@dekbian:/etc/tripwire# twadmin --create-cfgfile --cfgfile ./tw.cfg --site-keyfile ./site.key ./twcfg.txt
Please enter your site passphrase:
Wrote configuration file: /etc/tripwire/tw.cfg
root@dekbian:/etc/tripwire#
```

f. Jalankan perintah tripwire --test --email root@localhost

```
root@debian:/etc/tripwire# tripwire --test --email root@localhost
Sending a test message to: root@localhost
root@debian:/etc/tripwire#
```

g. Cek email

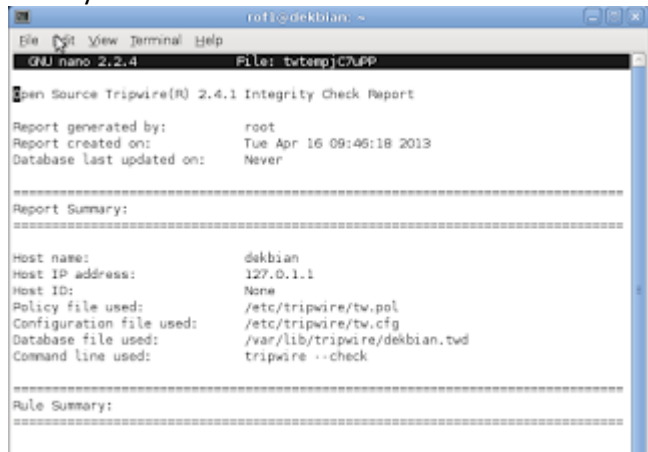


3. Buat file kosong

```
root@debian:/etc/tripwire# touch newfile.sh
root@debian:/etc/tripwire# cp newfile.sh /root
root@debian:/etc/tripwire#
```

4. Lakukan tripwire --check

Hasil nya :



Report dibuat oleh root pada tanggal 16 april 2013 pada host debian.  
police file yang digunakan = tw.pol,  
konfigurasi yang digunakan = tw.cfg  
database yang digunakan = debian.twd

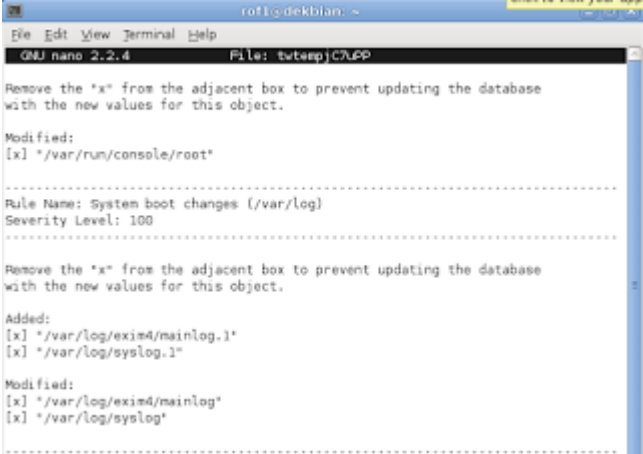
Section: Unix File System				
Rule Name	Severity Level	Added	Removed	Modified
Invariant Directories	66	0	0	0
* Tripwire Data Files	100	1	0	1
Other binaries	66	0	0	0
Tripwire Binaries	100	0	0	0
Other libraries	66	0	0	0
Root file-system executables	100	0	0	0
* System boot changes	100	2	0	3
Root file-system libraries (/lib)	100	0	0	0
Critical system boot files	100	0	0	0
* Other configuration files (/etc)	66	1	0	5
Boot Scripts	100	0	0	0
Security Control	66	0	0	0
* Root config files	100	6	0	1
* Devices & Kernel information	100	814	316	0
Total objects scanned: 58624				
Total violations found: 1150				

Terjadi penambahan 1 data file dan 1 modifikasi dengan severity level 100. Disamping itu juga ada penambahan pada system boot changes sebanyak 2 perubahan dan 3 modifikasi. Dan pada konfigurasi ada 1 penmbahan serta 5 modifikasi. Pada root config files ada penambahan 6 konfigurasi dan 1 modifikasi.  
Total objek yang discan 58624 dan pelanggaran / perubahan yang ditemukan 1150.



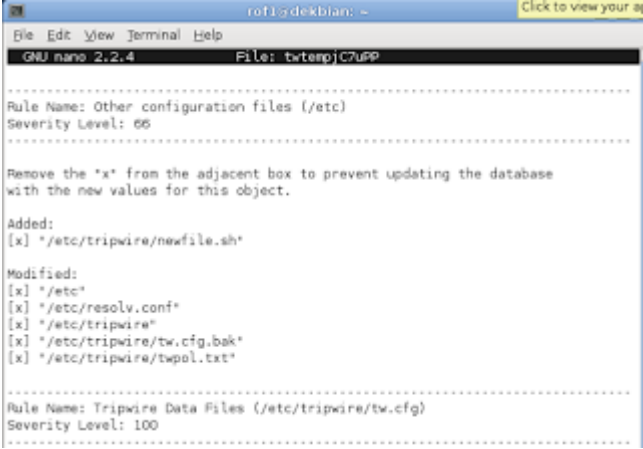
```
rof@dekbian: ~  
File Edit View Terminal Help  
GNU nano 2.2.4 File: twtempC7uPP  
-----  
Rule Name: Tripwire Data Files (/var/lib/tripwire/dekbian.twd)  
Severity Level: 100  
-----  
Remove the "x" from the adjacent box to prevent updating the database  
with the new values for this object.  
-----  
Added:  
[x] */var/lib/tripwire/dekbian.twd*
```

Ada penambahan data pada rule tripwire data files yaitu dekbian.twd.



```
rof@dekbian: ~  
File Edit View Terminal Help  
GNU nano 2.2.4 File: twtempC7uPP  
-----  
Remove the "x" from the adjacent box to prevent updating the database  
with the new values for this object.  
-----  
Modified:  
[x] */var/run/console/root*  
-----  
Rule Name: System boot changes (/var/log)  
Severity Level: 100  
-----  
Remove the "x" from the adjacent box to prevent updating the database  
with the new values for this object.  
-----  
Added:  
[x] */var/log/exim4/mainlog.1*  
[x] */var/log/syslog.1*  
-----  
Modified:  
[x] */var/log/exim4/mainlog*  
[x] */var/log/syslog*
```

Adapun pada system boot changes adalah penmbahan data mainlog.1 dan syslog.1. juga terdapat modifikasi pada mainlog dan syslog.



```
rof@dekbian: ~  
File Edit View Terminal Help  
GNU nano 2.2.4 File: twtempC7uPP  
-----  
Rule Name: Other configuration files (/etc)  
Severity Level: 66  
-----  
Remove the "x" from the adjacent box to prevent updating the database  
with the new values for this object.  
-----  
Added:  
[x] */etc/tripwire/newfile.sh*  
-----  
Modified:  
[x] */etc*  
[x] */etc/resolv.conf*  
[x] */etc/tripwire*  
[x] */etc/tripwire/tw.cfg.bak*  
[x] */etc/tripwire/twpol.txt*  
-----  
Rule Name: Tripwire Data Files (/etc/tripwire/tw.cfg)  
Severity Level: 100  
-----
```

Penambahan data pada tripwire data file adalah newfile.sh pada rule other configuration files dan juga modifikasi pada folder /etc.

hasil analisa pada no 1 dan no 4

Adanya perubahan sesuai dengan perubahan yang kita lakukan baik penambahan data maupun modifikasi data serta konfigurasi lainnya. Diantaranya :

- Penambahan file newfile.sh, dimana pada report pada no 1 tidak ada namun pada report no 4 ada report penambahan newfile.sh.
- Kedua report terdapat Penambahan data dekbian.twd. namun pada report no 1 tidak ada modifikasi pada dekbian.twd seperti pada report no 4.
- Kedua report terdapat Modifikasi pada tw.cfg dan twcfg.txt
- Kedua report terdapat Modifikasi pada pol.cfg dan twpol.txt
- Terdapat penambahan data pada folder /root dengan file newfile.sh pada rule root config files.