Buat file di direktory /etc yang merupakan direktory system yang seharusnya tdk pernah berubah, misal tripwiretest

```
root@debian:/home/student# cd /etc
root@debian:/etc# touch tripwiretest
```

Lakukan checking dengan perinath sbb :

```
root@debian:/var/lib/tripwire/report# tripwire --check
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
```

Selesai chek akan terbentuk file report di /var/lib/tripwire/report
Cek hasil cheking dengan menggunakan perintah twprint sbb :

```
root@debian:/var/lib/tripwire/report# twprint --print-report -r debian-20140327-
134241.twr | less
```

Lihat seksama hasilnya :

```
--------------------------------------------------------------------------
  Section: Unix File System
--------------------------------------------------------------------------

  Rule Name                     Severity Level    Added    Removed  Modified
  ---------                     --------------    -----    -------  --------
  Invariant Directories         66                0        0        0
* Tripwire Data Files           100               1        0        0
  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               0        0        0
  Root file-system libraries    100               0        0        0
  (/lib)
  Critical system boot files    100               0        0        0
* Other configuration files     66                1        0        1
  (/etc)
  Boot Scripts                  100               0        0        0
  Security Control              66                0        0        0
  Root config files             100               0        0        0
* Devices & Kernel information  100               296      1148     0
```

Dan lihat rekap hasilnya :

```
  ---------------------------------------
  Added Objects: 1
  ---------------------------------------

Added object name:  /etc/tripwiretest

  ---------------------------------------
  Modified Objects: 1
  ---------------------------------------

Modified object name:  /etc

  Property:            Expected                  Observed
  -------------        -----------               -----------
* Modify Time          Thu Mar 27 13:40:05 2014  Thu Mar 27 13:42:42 2014
```

Tambahan command :
twadmin to view the current tripwire policy files

```
#./twadmin --print-polfile
# ./twadmin --print-cfgfile
```

Tugas :

1. Tambahkan policy
2. Lakukan inisialisasi lagi
3. Tambahkan file pada direktory yang dimasukkan pada policy
4. Lakukan ceking dengan tripwire –check
5. Lihat hasilnya dengan twprint

Create policy menjadi file txt yang bisa dimodif

```
root@debian:/etc/tripwire# twadmin --print-polfile > /etc/tripwire/twpol.txt
```

edit sesuai kebutuhan

Melakukan konfigurasi ulang policy (harus dilakukan di direktory /etc/tripwire)

```
root@debian:/etc/tripwire# twadmin --create-polfile -S site.key /etc/tripwire/twpol.txt
Please enter your site passphrase:
Incorrect site passphrase.
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol
```

Selanjutnya hapus database lama dan initialisasi database baru (biasanya nama database disesuaikan dengn domain, disini inisialisasi awalnya memakai nama debian.twd sementara direname ke lamadebian.twd1

```
root@debian:/etc/tripwire# cd /var/lib/tripwire/
root@debian:/var/lib/tripwire# ls
debian.twd  report
root@debian:/var/lib/tripwire# mv debian.twd lamadebian.twd1
root@debian:/var/lib/tripwire# ls
lamadebian.twd1  report
```

Inisialisasi ulang database

```
root@debian:/var/lib/tripwire# tripwire --init
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
### Warning: File system error.
### Filename: /var/lib/tripwire/debian.twd
### No such file or directory
### Continuing...
The object: "/lib/init/rw" is on a different file system...ignoring.
### Warning: File system error.
### Filename: /etc/rc.boot
```

Hasil inisialiasi ulang

```
root@debian:/var/lib/tripwire# ls
debian.twd  lamadebian.twd1  report
root@debian:/var/lib/tripwire#
```

Mencoba memodifikasi direktory yang disiapkan

```
root@debian:/var/lib/tripwire# cd /temp
root@debian:/temp# ls
file_lama.txt
root@debian:/temp# touch file_baru.txt
root@debian:/temp# ls -l
total 0
-rw-r--r-- 1 root root 0 Mar 27 18:21 file_baru.txt
-rw-r--r-- 1 root root 0 Mar 27 18:02 file_lama.txt
root@debian:/temp#
```

Lakukan check ulang dengan tripwire

```
root@debian:/var/lib/tripwire/report# tripwire --check
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
```

Lihat hasilnya

```
root@debian:/etc/tripwire# cd /var/lib/tripwire/report/
root@debian:/var/lib/tripwire/report# ls -l
total 76
-rw-r--r-- 1 root root 18646 Mar 27 13:43 debian-20140327-134241.twr
-rw-r--r-- 1 root root 20478 Mar 27 13:50 debian-20140327-134953.twr
-rw-r--r-- 1 root root 10494 Mar 27 18:23 debian-20140327-182259.twr
-rw-r--r-- 1 root root 14702 Mar 27 18:28 debian-20140327-182801.twr
-rw-r--r-- 1 root root  6366 Mar 27 18:35 debian-20140327-183504.twr
root@debian:/var/lib/tripwire/report# twprint --print-report -r debian-20140327-183504.twr |
ss
State       Recv-Q Send-Q            Local Address:Port                Peer Address:Port
root@debian:/var/lib/tripwire/report# twprint --print-report -r debian-20140327-183504.twr |l
ess
```

Hasil report

```
--------------------------------------------------------------------------------
  Section: Unix File System
--------------------------------------------------------------------------------

  Rule Name                       Severity Level    Added    Removed  Modified
  ---------                       --------------    -----    -------  --------
  Invariant Directories           66                0        0        0
  Tripwire Data Files             100               0        0        0
  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               0        0        0
  Root file-system libraries      100               0        0        0
  (/lib)
  Critical system boot files      100               0        0        0
* Other configuration files       66                0        0        1
  (/etc)
  Boot Scripts                    100               0        0        0
  Security Control                66                0        0        0
  Root config files               100               0        0        0
* Devices & Kernel information    100               150      150      0
* Temp Directories                66                1        0        1
```

```
Severity Level: 66
---------------------------------------------------------------------------------
  ---------------------------------------
  Added Objects: 1
  ---------------------------------------

Added object name:  /temp/fileterbaru.txt

  ---------------------------------------
  Modified Objects: 1
  ---------------------------------------

Modified object name:  /temp

  Property:            Expected                   Observed
  -------------        -----------                -----------
* Modify Time          Thu Mar 27 18:27:58 2014   Thu Mar 27 18:34:58 2014
```