COPS: Polisi Sistem Linux Anda

Oleh Iwan Setiawan <stwn@duniasemu.org>
Last updated 2003/11/14 16:35:03

Layaknya sebuah kota, sistem Linux Anda perlu polisi untuk memeriksa keamanannya. Polisi ini salah satunya adalah COPS, sebuah utilitas keamanan yang cukup sederhana tetapi dapat diandalkan untuk pemeriksaan sistem terhadap kelemahan dan lubang keamanan lokal secara umum.

I. DESKRIPSI

COPS (Computer Oracle and Password System) adalah perangkat lunak keamanan yang dibuat oleh Dan Farmer yang berfungsi untuk melakukan pemeriksaan dan melaporkan kelemahan sistem dan lubang keamanan lokal secara umum. Perangkat lunak ini diperkenalkan pada konferensi USENIX pada tahun 1990, dan di dalam paketnya berisi bourne *shell-scripts* dengan kombinasi `awk`, `sed`, `grep`, dll, program-program dalam bahasa C, perl, serta paper mengenai keamanan dan COPS.
Walaupun cukup lama rilis perangkat lunak ini dan tidak di-*update* berkala, COPS dapat dijadikan model dan utilitas keamanan tahap pertama bagi sistem Linux Anda.

II. FITUR PEMERIKSAAN COPS

COPS memiliki beberapa fitur pemeriksaan yaitu:

- Program dan berkas SUID (Set User ID)
  Pemeriksaan terhadap program dan berkas SUID dalam sistem, baik berupa *shell-scripts* atau binari juga *mode*-nya.
- Berkas `/etc/passwd` dan `/etc/group`
  Pemeriksaan isi, format dan keamanan berkas-berkas tersebut.
- Password yang lemah
  Pemeriksaan password yang lemah pada sistem Anda termasuk seberapa mudah password-password tersebut untuk ditebak.
- Program dan berkas yang dijalankan melalui `/etc/rc*` dan berkas `cron`
- CRC *checksum* pada perubahan binari dan berkas
- Direktori *home* dan berkas *startup* (`.profile`, dll) dan perijinannya
- Direktori yang mempunyai *mode* '*world-writable*'
- Ftp *setup*, baik *anonymous-ftp* maupun berkas ftp seperti `/etc/ftpusers`, *account* root harus ada dalam berkas ini
- Perijian atau *mode* berkas, direktori, dan divais (`/dev`)
- Pembatasan *tftp*, *decode alias* di `sendmail`, masalah *uudecode* SUID, *shell* yang tersembunyi pada `/etc/inetd.conf` termasuk `rexd`
- Beberapa pemeriksaan root seperti direktori dalam *path* pencarian, penambahan '+' pada berkas `/etc/host.equiv`, dan pembatasan *NFS mount*
- Tanggal *CERT-advisory* di mana COPS akan memeriksa tanggal apakah beberapa berkas yang didefinisikan memiliki kelemahan dan lubang kelemahan seperti yang terdapat dalam *advisory*. Karena *CERT-advisory* ini sudah cukup lama kemungkinan akan terdapat kesalahan dalam pemeriksaan, jadi Anda dianjurkan untuk membaca *advisory* dan memeriksa berkas yang dilaporkan mempunyai masalah keamanan.
- *Kuang expert system*

Sistem ini melakukan pemeriksaan kelemahan yang mengacu pada beberapa '*rule*' dan akan mendeteksi sistem Anda apakah dapat di-*compromised*.

III. KEBUTUHAN INSTALASI

- ✔ Kompiler C
- ✔ Cracklib (`http://www.crypticide.org/users/alecm/security/` atau *mirror*-nya)
  Sebagian besar distribusi Linux menyertakan `cracklib` dalam CD instalasinya, contoh: Mandrake Linux, tapi jika belum ada Anda dapat men-*download* dan menginstalnya sendiri
- ✔ Perl (*optional*)

IV. INSTALASI COPS

1. Download `cops_104_linux.tgz` dari
   `http://www.ibiblio.org/pub/Linux/system/security/` atau *mirror*-nya.
2. Ekstrak paket `cops_104_linux.tgz`

   ```
   $ tar zxvf cops_104_linux.tgz
   ```

3. Masuk ke direktori hasil ekstrak

   ```
   $ cd cops_104/
   ```

4. Lakukan konfigurasi dengan melakukan *reconfig* untuk *shell-scripts*, ini dilakukan untuk mengkonfigurasi COPS mengenai letak program-program yang diperlukan (*hard-coded*).

   ```
   $ ./reconfig
   checking to make sure all the target(s) are here...
   So far so good...
   Looking for all the commands now...
   Ok, now doing substitutions on the shell scripts...
   Changing paths in makefile...
   ...
   ```

5. Edit `makefile` untuk disesuaikan dengan preferensi Anda
   - Direktori instalasi COPS
     Edit baris `INSTALL_DIR= linux` ganti dengan direktori yang Anda inginkan, misal: `INSTALL_DIR=/usr/sbin/cops`
   - Beberapa sistem membutuhkan *uncomment* baris `BRAINDEADFLAGS -lcrypt` untuk kompilasi `pass.chk`.
6. Edit *shell-script* `cops`
   - MMAIL
     Set 'YES' untuk mengirimkan laporan ke e-mail SECURE_USERS
   - RUN_SUID
     Set 'YES' untuk mengaktifkan permeriksaan SUID dan ini memerlukan *privileged-user*
   - SECURE
     Set ke direktori dimana Anda instal COPS, misal `SECURE=/usr/sbin/cops`
   - SECURE_USERS
     Set ke account dimana Anda akan menerima laporan COPS, misal `SECURE_USERS=stwn@your-domain.org`

7. Kompilasi COPS

```
$ make
```

8. Instal COPS

```
$ su
Password:
# make install
```

9. Jangan lupa untuk mengeset *mode* 700 untuk direktori dimana program-program COPS berada.

```
# chmod 0700 /usr/sbin/cops
```

V. KONFIGURASI DAN MENJALANKAN COPS

1. Ubah dan sesuaikan berkas `is_able.lst` dan `crc_list` dengan sistem Anda.
2. Jalankan `cops` misal dengan *option* `-v` (*verbose*), `-s` (direktori `cops`) dan `-b` (*bit bucket*):

```
$ /usr/sbin/cops/cops -v -s /usr/sbin/cops -b error.cops
```

   atau jika Anda mengkonfigurasikan COPS dengan mengaktifkan pemeriksaan SUID, Anda memerlukan hak root untuk mengakses semua direktori di bawah `'/'`.
3. Setelah selesai, lihat hasil laporan pada berkas bertanggal dalam direktori dengan nama *hostname* mesin yang diperiksa COPS. Contoh: laporan pada *hostname* `machine1` akan ditulis pada `/usr/sbin/cops/machine1/` dalam berkas bertanggal misal `2003_Nov_14.`

VI. MENJALANKAN COPS DENGAN PENJADWAL

Dengan memasukkan COPS ke dalam `cron` atau `at` maka Anda bisa menjalankannya dalam interval waktu tertentu untuk memonitor keamanan sistem dan mengirimkan mail ke administrator.
Untuk menggunakan pemeriksaan SUID (`suid.chk`), gunakan *option* `-s` untuk memberitahukan `cron` dimana program-program COPS berada atau COPS akan mengeset *mode* 700 untuk `'/'`.

VII. PEMERIKSAAN SECARA INDIVIDUAL

Anda bisa menjalankan pemeriksaan sistem secara individual untuk masing-masing kategori pemeriksaan, misal pemeriksaan berkas SUID. Dengan menjalankan `suid.chk` maka berkas dan program ber-SUID yang ditemukan akan dilaporkan.

```
$ su
Password:
# /usr/sbin/cops/suid.chk -s /usr/sbin/cops -o suid.cops
```

Laporan pemeriksaan berkas dan program SUID akan dituliskan pada berkas `suid.cops` sesuai dengan argumen yang diberikan pada *option* `-o`.

VIII. BEBERAPA CONTOH LAPORAN COPS

- Perijinan Berkas, Direktori, dan Divais (`/dev`)

  Keamanan *filesystem* di Linux tidak dapat terlepas dari masalah perijinan atau *mode*. Direktori yang diset '*world-writable*' secara sengaja atau tidak sengaja dapat memberikan celah keamanan pada sistem. Seseorang dapat menginstal dan menjalankan program yang berbahaya bagi sistem ke dalam direktori tersebut, misal: *exploit* dan *password-cracker*. Contoh laporan COPS untuk perijinan:

```
ATTENTION:
Security Report for Fri Nov 14 08:03:03 WIT 2003
from host machine1

**** root.chk ****
**** dev.chk ****
Warning!  /dev/cdrom is _World_ readable!
**** is_able.chk ****
Warning!  /usr/spool/mail is _World_ writable!
Warning!  /etc/securetty is _World_ readable!
**** rc.chk ****
**** cron.chk ****
**** group.chk ****
**** home.chk ****
**** passwd.chk ****
**** user.chk ****
**** misc.chk ****
```

  Contoh laporan COPS di atas memberikan penjelasan bahwa divais CD-ROM yang ada dalam sistem dan berkas `/etc/securetty` dapat dibaca oleh semua orang, kemudian direktori `/usr/spool/mail` dapat ditulis oleh semua orang sehingga kemungkinan direktori ini bisa ditanam *exploit*, *backdoor*, dll.

- Program SUID

  Program ber-SUID akan selalu dieksekusi dengan hak pemiliknya siapapun yang menjalankan program tersebut. Misal program `mount` diset SUID root maka ketika dijalankan oleh salah satu pengguna dalam sistem, program `mount` tsb akan dijalankan sebagai root.

  Dalam sistem yang *multiuser* jika terdapat banyak program ber-SUID baik pengguna ataupun root akan sangat berbahaya dan menimbulkan kemungkinan timbul lubang keamanan terutama yang '*world-writable*'.

```
ATTENTION:
SUID Security Report for Fri Nov 14 08:11:16 WIT 2003
from host machine1

Warning! ROOT owned SUID file /var/qmail/bin/qmail-scanner-queue.pl is type: setuid a
/usr/bin/suidperl -T script text executable!

These files are newly setuid/setgid:

-rwsr-xr-x    1 root     bin         68876 Feb 19  2003 /bin/mount
-r-sr-xr-x    1 root     bin         14964 Mar  8  2003 /bin/ping
-rws--x--x    1 root     bin         31696 Mar 10  2003 /bin/su
-rwsr-xr-x    1 root     bin         31072 Feb 19  2003 /bin/umount
-rws--x--x    1 root     bin         32568 Mar 10  2003 /usr/bin/chage
```

```
-rws--x--x    1 root     bin         27456 Mar 10  2003 /usr/bin/chfn
-rws--x--x    1 root     bin         25844 Mar 10  2003 /usr/bin/chsh
-rws--x--x    1 root     bin         10508 Apr 16  2002 /usr/bin/crontab
-rws--x--x    1 root     bin         15416 Mar 10  2003 /usr/bin/expiry
-rws--x--x    1 root     bin         32196 Mar 10  2003 /usr/bin/gpasswd
-rws--x--x    1 root     bin         19128 Mar 10  2003 /usr/bin/newgrp
-rws--x--x    1 root     bin         33924 Mar 10  2003 /usr/bin/passwd
-rws--x--x    1 root     bin         14292 Mar  8  2003 /usr/bin/rcp
-rws--x--x    1 root     bin         10260 Mar  8  2003 /usr/bin/rlogin
-rws--x--x    1 root     bin          7380 Mar  8  2003 /usr/bin/rsh
-rwxr-sr-x    1 root     slocate     26496 Feb 12  2003 /usr/bin/slocate
-r-xr-sr-x    1 root     tty          9988 Feb 19  2003 /usr/bin/wall
-r-xr-sr-x    1 root     tty          8212 Feb 19  2003 /usr/bin/write
-rwsr-xr-x    1 root     root         5756 Mar  5  2003 /usr/libexec/pt_chown

These files are no longer setuid/setgid:

-rwsr-xr-x  1 root     bin         10240 Jun 13 13:13 /bin/chgrp
-rwsr-xr-x  1 root     bin         12288 Jun 13 13:13 /bin/df
-rws--s---  1 root     term        22528 Aug 13 13:13 /bin/login
-rws------  1 root     bin         21504 Jun 13 13:13 /bin/login.old
-rwsr-xr-x  1 root     bin         22528 Jun 13 13:13 /bin/mail
-rwsr-xr-x  1 root     bin         14336 Jun 13 13:13 /bin/passwd
-rwxr-sr-x  1 root     MEM         22528 Jun 13 13:13 /bin/ps
-rwsr-xr-x  1 root     bin         16384 Jun 13 13:13 /bin/su
-rwxr-sr-x  1 root     MEM         14336 Jun 13 13:13 /etc/dmesg
-rwsr-x---  1 root     operator    29696 Jun 13 13:13 /etc/dump
```

IX. TIPS DAN TRIK

Penggunaan CRC *checksum* dari COPS mungkin kurang memadai, gunakan `tripwire` untuk mengambil alih pemeriksaan integritas *filesystem* .

Pengunaan `crack` atau program pembobol password yang lebih baik akan memberikan hasil yang lebih memuaskan untuk mengetahui seberapa kuat password pengguna dalam sistem kita.

Dengan beberapa modifikasi pada *shell-scripts*, perl, dan C di dalam COPS, Anda dapat memberikan banyak fitur yang tidak ada dalam COPS secara *default* dan disesuaikan dengan sistem Anda. Misal: perbaikan masalah keamanan yang ditemukan COPS, pemeriksaan direktori `/etc/xinetd.d` pada distribusi yang menggunakan `xinetd` dari penyalaan beberapa layanan jaringan, dst.

Untuk menambahkan perbaikan secara otomatis ketika COPS menemukan masalah diperlukan program ber-SUID root, dan ini tidak diijinkan kecuali Anda benar-benar secara 'aman' membuat program SUID tersebut (silahkan membaca artikel-artikel mengenai pembuatan program SUID secara aman).

X. KELEBIHAN

Selain kelebihan-kelebihan dari fitur yang disebutkan sebelumnya COPS dapat digunakan untuk pemeriksaan dan monitoring tahap pertama bagi sistem Anda.

COPS dapat dijalankan dengan hak pengguna, satu program yang seharusnya dijalankan dengan hak root adalah pemeriksa berkas SUID untuk memeriksa seluruh *filesystem* dari program SUID yang berbahaya bagi keamanan sistem.

XI. KEKURANGAN

COPS hanya dapat memeriksa masalah dan kelemahan keamanan yang umum pada sistem

yang mungkin tidak begitu dipedulikan oleh pemiliknya.
COPS tidak dapat mendeteksi kelemahan sistem yang baru ditemukan setelah rilis terakhir kecuali Anda meng-*update database*-nya.
COPS tidak memperbaiki masalah keamanan yang ditemukan, perangkat lunak ini hanya melaporkan saja, jadi diperlukan administrator sistem yang berpengalaman untuk memperbaiki masalah tersebut.
COPS tidak dapat memeriksa dan memantau sistem secara *remote* (*scanning*) dan hanya dapat dijalankan secara lokal.
COPS dapat digunakan para *cracker* untuk memeriksa kelemahan sistem target, oleh karena itu administrator harus lebih dulu memeriksa sistemnya sehingga kelemahan dan lubang kelemahan dapat ditutup.
CRC *checksum* tidak dapat memeriksa berkas binari dengan *mode* '*executable*' saja jika dijalankan dengan hak pengguna biasa.
Seperti program pemeriksa lain, COPS membutuhkan waktu dan sumber daya sistem, tetapi ini bisa diatur dengan penjadwal seperti `cron` dijalankan pada waktu sumber daya dalam keadaan tidak sibuk.

XII. PENUTUP

COPS merupakan utilitas keamanan yang sederhana tetapi dapat diandalkan sebagai model dan utilitas keamanan tahap pertama bagi sistem Anda.
Dengan model utilitas COPS diharapkan dapat memberikan rangsangan untuk mengembangkan utilitas keamanan dan menambah *awareness* terhadap keamanan sistem Anda.
Semoga artikel yang sederhana ini dapat bermanfaat dan jika boleh mengutip pesan dari acara berita kriminal di salah satu stasiun TV swasta: waspadalah, waspadalah, waspadalah!

XIII. REFERENSI

- Anonymous, *Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and Workstation*, Sams Publishing, 2000.
- Farmer, Daniel and Eugene H. Spafford, *The COPS Security Checker System*, Purdue University Technical Report CSD-TR-993, 1994.
- Farmer, Daniel, *COPS and Robbers UN*X System Security*, 1991.
- Ross, Seth T., *UNIX System Security Tools*, McGraw-Hill Companies, Inc., 2000.