KEAMANAN REMOTE SERVER MELALUI SSH DENGAN KRIPTOSISTEM SIMETRIS

Muhammad Iqbal*

Abstract

Server security is an absolute requirement to be met in the secure data by network administrator. An application to remote server is still fairly secure called secure shell (SSH). But the recent developments other parties can retrieve password from a remote login service using SSH with bruce-force method. Therefore, it needs layered security. For that to improve the security of remote ssh server using a symmetric cryptosystem that can be applied to each user who wants to remote into the server must already have a key file from the server.

Keywords: server security, network security, secure shell, SSH, cryptography, cryptosystem;

PENDAHULUAN

Di era global ini, sistem komputer yang terpasang makin mudah diakses. Menimbulkan banyaknya kelemahan dalam melindungi keamanan sistem untuk menjamin sistem tidak diinterupsi dan diganggu. Keamanan merupakan isu utama dalam jaringan. Apalagi jika seluruh *host* tersambung ke Internet. Melindungi jaringan, berarti melindungi setiap *host* yang ada dalam jaringan, baik *workstation* maupun server. Keamanan jaringan komputer merupakan syarat multak untuk melindungi data. Keamanan jaringan komputer bisa diartikan suatu proses untuk mencegah dan mengidentifikasi pengguna yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan penguna yang

* Mahasiswa Magister Teknik Informatika Universitas Sumatera Utara

tidak sah yang disebut "penyusup" untuk mengakses setiap bagian dari sistem jaringan komputer. Tujuan keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan komputer berupa ancaman fisik maupun logik baik langsung maupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.

Dalam proses maintenance dan monitoring server secara berkala diperlukan seorang administrator jaringan me-*remote* server tetapi sangat diperlukan jalur yang aman. Untuk itu perlu strategi khusus untuk mengatasi hal tersebut salah satunya yaitu dengan menerapkan kriptografi pada system *account*-nya.

Keamanan jaringan komputer sendiri sering dipandang sebagai hasil dari beberapa faktor. Faktor ini bervariasi tergantung pada bahan dasar, tetapi secara normal setidaknya beberapa hal yaitu: *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan) (Rahmani, 2003).

KEAMANAN JARINGAN KOMPUTER

Mengamankan jaringan komputer membutuhkan tiga tingkatan proses. Untuk mengamankan jaringan komputer dapat dilakukan pemetaan terhadap ancaman yang mungkin terjadi.

Prevention (pencegahan)

Kebanyakan dari ancaman akan dapat ditepis dengan mudah, walaupun keadaan yang benar-benar 100% aman belum tentu dapat dicapai. Akses yang tidak diinginkan kedalam jaringan komputer dapat dicegah dengan memilih dan melakukan konfigurasi layanan (*services*) yang berjalan dengan hati-hati.

Observation (observasi)

Ketika sebuah jaringan komputer sedang berjalan, dan sebuah akses yang tidak diinginkan dicegah, maka proses perawatan dilakukan. Perawatan jaringan komputer harus termasuk melihat isi log yang tidak normal yang dapat merujuk ke masalah keamanan yang tidak terpantau. *Intruder Detecting System* (IDS) dapat digunakan sebagai bagian dari proses observasi tetapi menggunakan IDS seharusnya tidak merujuk kepada ketidak-pedulian pada informasi log yang disediakan.

***Response* (respon).**

Bila sesuatu yang tidak diinginkan terjadi dan keamanan suatu system telah berhasil disusupi, maka personil perawatan harus segera mengambil tindakan. Tergantung pada proses produktifitas dan masalah yang menyangkut dengan keamanan maka tindakan yang tepat harus segera dilaksanakan. Bila sebuah proses sangat vital pengaruhnya kepada fungsi system dan apabila di-shutdown akan menyebabkan lebih banyak kerugian daripada membiarkan system yang telah berhasil disusupi tetap dibiarkan berjalan, maka harus dipertimbangkan untuk direncakan perawatan pada saat yang tepat. Ini merupakan masalah yang sulit dikarenakan tidak seorangpun akan segera tahu apa yang menjadi celah begitu system telah berhasil disusupi dari luar.

***Victims/statistic* (korban/statistik)**

Keamanan jaringan komputer meliputi beberapa hal yang berbeda yang mempengaruhi keamanan secara keseluruhan. Serangan keamanan jaringan komputer dan penggunaan yang salah dan sebegai contoh adalah virus, serangan dari dalam jaringan komputer itu sendiri, pencurian perangkat keras (hardware), penetrasi kedalam system, serangan "*Denial of Service*" (DoS), sabotase, serangan "*wireless*" terhadap jaringan komputer, penggantian halaman depan situs (website *defacement*), dan penggunaan yang salah terhadap aplikasi web. Statistik menunjukkan jumlah penyusupan didalam area ini sudah cukup banyak berkurang dari tahun 2003, tipe variasi dari serangan, bagaimanapun juga, menyebabkan hampir setiap orang adalah sasaran yang menarik.

Sistem Operasi Linux dan Keamanannya

Salah satu sistem operasi yang sangat sesuai untuk pengamanan server yaitu sisitem operasi Linux. Sistem Operasi Linux adalah sistem operasi *open source*, dimana *source* yang dimiliki masih terus dikembangkan oleh seluruh pengguna Linux di dunia. Oleh karena itu, *source* selalu di-*update* dengan menambahkan *patch* pada sistem. Namun demikian, *patch* yang ada belum mampu menjaga keamanan sistem operasi secara keseluruhan, tapi bisa dikatakan pengembangan sistem operasi linux dikembangkan oleh semua pihak. Sebuah distribusi Linux, yang umum disebut dengan "distro", adalah sebuah proyek yang bertujuan untuk

mengatur sebuah kumpulan perangkat lunak berbasis Linux dan memfasilitasi instalasi dari sebuah sistem operasi Linux. Distribusi-distribusi Linux ditangani oleh individu, tim, organisasi sukarelawan dan entitas komersial. Distribusi Linux memiliki perangkat lunak sistem dan aplikasi dalam bentuk paket-paket dan perangkat lunak yang spesifik dirancang untuk instalasi dan konfigurasi sistem. Perangkat lunak tersebut juga bertanggung jawab dalam pemutakhiran paket. Sebuah Distribusi Linux bertanggung jawab atas konfigurasi bawaan, sistem keamanan dan integrasi secara umum dari paket-paket perangkat lunak sistem Linux. Contoh-contoh distribusi Linux : Ubuntu dan derivatifnya (Sabily (Ubuntu Muslim Edition), Kubuntu, Xubuntu, Edubuntu, GoBuntu, Gnewsense, ubuntuCE), SuSE, Fedora, BackTrack, Mandriva, Slackware, Debian, PCLinuxOS, Knoppix, Xandros, Sabayon, CentOS, Red Hat, ClearOS, Chromeos.

Arsitektur kemanan di Linux, mempunyai enam komponen (Heriyanto, 2000):

- Account Pemakai (User Account)
- Kontrol Akses secara Diskresi (Discretionary Access Control)
- Kontrol Akses Jaringan (Network Access Control)
- Enkripsi (Encryption)
- Logging
- Deteksi penyusupan (Intrusion Detection)

Account Pemakai (User Account)

Kekuasaan dalam mengadministrasi sistem secara keseluruhan berada dalam satu account, yakni root. Dengan root bisa mengontrol sistem file, user, sumber daya (devices), bahkan akses jaringan. Model diktatorial ini memudahkan administrator dalam menangani sistem. Jika ada satu user yang melanggar aturan, root bisa membuat *account*-nya beku, tanpa mengganggu yang lain. Atau mengatur siapa-siapa saja yang boleh mengakses suatu file, memberikan hak khusus pada user-user tertentu.

Kecerobohan salah satu pemakai tidak akan berpengaruh terhadap sistem secara keseluruhan. Masing-masing pemakai memiliki *privacy* yang ketat. Untuk itu account root biasanya hanya digunakan saat-saat tertentu saja. Misalnya perbaikan sistem. Dan biasanya account root dipergunakan

pada modus *single user*. Dapat dibayangkan apa yang terjadi dengan jaringan jika penyusup dari luar memperoleh akses root.

Kontrol Akses secara Diskresi (Discretionary Access Control)

Setiap pemakai Linux, memiliki account tersendiri, yang masing-masing dibedakan dengan user name dan password. Setiap file memiliki atribut kepemilikan, group, dan user umum. Satu file, bisa diberikan atribut tertentu, sehingga hanya dapat dibaca atau dieksekusi oleh pemiliknya saja. Pembatasan ketat ini dinamakan *Discretionary Access Control* (DAC). Hal ini pula yang menyebabkan virus jarang ditemui atau jarang tersebar di Linux. Sebab virus biasanya menulis file ke dalam sistem. Dengan DAC, virus hanya berpengaruh pada file-file yang dimiliki oleh salah seorang user yang mengeksekusi virus tersebut. Sedangkan sistemnya sendiri tidak tersentuh.

Root merupakan satu-satunya *account* yang punya akses penuh ke seluruh sistem. Root juga dipakai untuk mengadministrasi seluruh sistem, mengganti atribut file, hingga mengadministrasikan divais. Karena itu, demi keamanan, root biasanya hanya dipakai untuk perawatan atau perbaikan sistem saja. Untuk mengetahui atribut file :

Beberapa program penting berkaitan dengan *Discretionary Access Control* :

su (Substitute User).

Disarankan tidak menggunakan user root untuk penggunaan sehari-hari. Jika memang mendesak, jalankan program su. Program ini memungkinkan digunakan *account* root untuk sementara.

Selain su, dapat dipakai pula program sudo, yakni memberikan beberapa user untuk dapat mengeksekusi program tertentu sebagai root. Konfigurasi filenya berada di /etc/sudoers.

shadow

Secara default, instalasi binary slackware, telah mengaktifkan *shadow* password. *shadow* adalah program yang membuat file /etc/passwd menjadi dapat dibaca (readable) tetapi tidak lagi berisi password, dan sebagai gantinya disimpan di file /etc/shadow. Berikut contoh tipikal file passwd :

```
halt:x:7:0:halt:/sbin:/sbin/halt
root:x:0:0::/root:/bin/bash
operator:x:11:0:operator:/root:/bin/bash
```

```
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
sync:x:5:0:sync:/sbin:/bin/sync
bin:x:1:1:bin:/bin:
ftp:x:404:1::/home/ftp:/bin/bash
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/usr/lib/news:
uucp:x:10:14:uucp:/var/spool/uucppublic:
man:x:13:15:man:/usr/man:
games:x:12:100:games:/usr/games:
guest:x:405:100:guest:/dev/null:/dev/null
nobody:x:65534:100:nobody:/dev/null:
iqbal:x:1000:103:,,,:/home/iqbal:/bin/bash
alias:x:7790:2108::/var/qmail/alias:/bin/true
qmaild:x:7791:2108::/var/qmail:/bin/true
qmaill:x:7792:2108::/var/qmail:/bin/true
qmailp:x:7793:2108::/var/qmail:/bin/true
qmailq:x:7794:2107::/var/qmail:/bin/true
qmailr:x:7795:2107::/var/qmail:/bin/true
qmails:x:7796:2107::/var/qmail:/bin/true
```

Satu baris mencerminkan satu user, lengkap dengan atributnya. Berikut keterangan tiap field :

Username:password:UserID:GroupID:keterangantambahan:homedirektori:shell.

Diambil contoh dari user iqbal :

```
iqbal:x:1000:103:,,,:/home/iqbal:/bin/bash
```

Keterangan dari line tersebut :

Username	: iqbal
Password	: x
User ID (UID)	: 1000
Group ID (GID)	: 103

Keterangan tambahan : -

Home Direktori : /home/iqbal

Shell Default : /bin/bash

Password dalam file ini dapat dibaca oleh setiap user, tapi yang terlihat hanya x saja. Password yang sebenarnya disimpan di file *shadow* (terenkripsi). Berikut file *shadow* dari password diatas :

```
root:pCfouljTBTX7o:10995:0:::::
halt:*:9797:0:::::
operator:*:9797:0:::::
shutdown:*:9797:0:::::
sync:*:9797:0:::::
bin:*:9797:0:::::
ftp:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
mail:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
man:*:9797:0:::::
games:*:9797:0:::::
guest:*:9797:0:::::
nobody:*:9797:0:::::
iqbal:OihQw6GBf4tiE:10995:0:99999:7:::
alias:!:10995:0:99999:7:::
```

Pro aktif Password

Linux menggunakan metode enkripsi DES (*Data Encription Standard*) untuk passwordnya. Namun seketat apapun enkripsi yang dilakukan akan menjadi percuma jika user memilih password yang mudah ditebak. User biasanya memilih hal-hal umum sebagai password, misalnya : Tanggal lahir (dirinya sendiri atau salah satu anggota keluarga), nomor plat mobill, nama salah satu anggota keluarga (baik ditulis langsung, atau dengan variasi huruf besar/dibalik dan sebagainya), Kata-kata yang ada di kamus, ditulis terbalik, nama favorit (artis, penyanyi, dan sebagainya)

Pilihan ini sangat riskan, sebab program semacam *crack*, dapat menebaknya dengan mencocokkan kamus yang ada dengan mudah. Bahkan program ini dapat diberikan pilihan kombinasi. Untuk itu perlu dibuat kebijakan yang baik untuk password.

Sudah menjadi sesuatu yang umum saat ini para administrator sistem linux, menyediakan suatu service remote login pada komputer server linux yang mereka kelola guna mempermudah pekerjaan mereka dalam melakukan administrasi sistem dimanapun mereka berada. Salah satu service remote login yang saat ini banyak digunakan pada sistem linux adalah ssh. Oleh karenanya *service* ini menjadi salah satu *service* yang diincar oleh para *hacker* untuk menjadi sasaran serangan mereka. *Service* ssh ini umumnya berjalan pada *port* 22. Penyusup akan melacak ke *port* 22, guna mendapatkan akses shell pada server. Karena untuk mengkases *service* ssh ini butuh login, maka penyusup umunya menggunakan teknik *brute-force attack* terhadap service ssh. *Brute-force attack* adalah suatu upaya serangan yang mencoba melakukan login secara otomatis menggunakan daftar kombinasi user dan password yang sudah ada.

Secure Shell (SSH)

SSH memungkinkan pertukaran data melalui saluran aman antara dua perangkat jaringan. Terutama banyak digunakan pada sistem berbasis Linux dan Unix untuk mengakses akun shell, SSH dirancang sebagai pengganti Telnet dan shell remote tak aman lainnya, yang mengirim informasi, terutama kata sandi, dalam bentuk teks sederhana yang membuatnya mudah untuk dicegat. Enkripsi yang digunakan oleh SSH menyediakan kerahasiaan dan integritas data melalui jaringan yang tidak aman seperti Internet.

SSH menggunakan kriptografi kunci publik untuk mengotentikasi komputer remote dan biarkan komputer remote untuk mengotentikasi pengguna, jika perlu. SSH biasanya digunakan untuk login ke mesin remote dan mengeksekusi berbagai perintah, tetapi juga mendukung *tunneling*, *forwarding TCP port* dan X11 *connections*, itu dapat mentransfer file menggunakan terkait SFTP atau SCP protocols. SSH menggunakan klien-server model. Yang standar TCP port 22 telah ditetapkan untuk menghubungi server SSH. Sebuah klien program SSH ini biasanya

digunakan untuk membangun koneksi ke SSH daemon untuk dapat diremote. Keduanya biasanya terdapat pada sistem operasi modern, termasuk Mac OS X, Linux, FreeBSD, Solaris dan OpenVMS. Tersedia versi berpemilik, freeware dan open source untuk berbagai tingkat kerumitan dan kelengkapan.

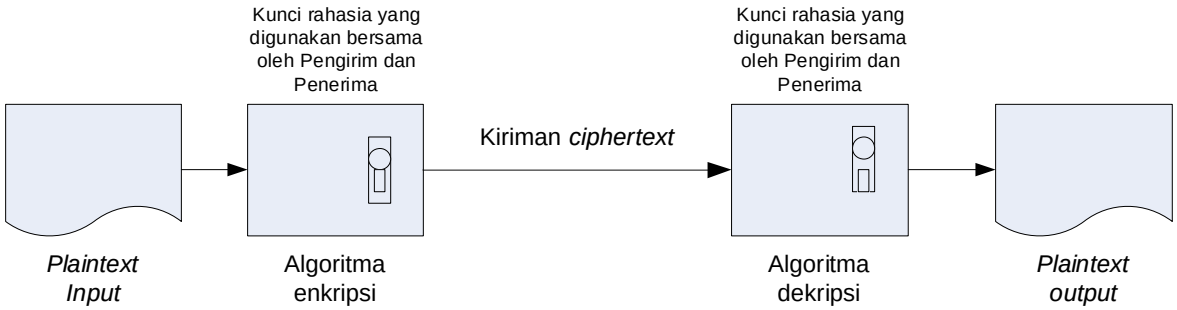
Kriptosistem Simetris

Cryptographic system atau *cryptosystem* adalah suatu fasilitas untuk mengkonversikan *plaintext* ke *ciphertext* dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pencipheran tertentu disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi. Secara umum, kunci-kunci yang digunakan untuk proses pengenkripsian dan pendekripsian tidak perlu identik, tergantung pada sistem yang digunakan (Menezes, et. al, 1997).

Enkripsi simetris adalah salah satu bentuk atau model dari sistem kripto (*cryptosystem*) yang kunci pembuatan enkripsinya sama dengan kunci yang digunakan untuk proses dekripsinya. Model ini dikenal dengan nama enkripsi konvensional atau enkripsi kunci tunggal (*single-key enkripsi*) yang mulai digunakan pada 1970an (Sorkin, 1983).

Enkripsi simetris mengubah *plaintext* (berkas asli) menjadi *ciphertext* (berkas berkode) menggunakan kunci rahasia dan sebuah algoritma enkripsi. Kunci dan algoritma tersebut kembali digunakan untuk mengembalikan informasi (proses dekripsi) sesuai dengan aslinya (dari *ciphertext* kembali ke dalam bentuk *plaintext*). Enkripsi (*enkripsi*), yaitu proses mengubah dari *plaintext* menjadi *ciphertext* disebut juga dengan proses *enciphering*. Sebaliknya, proses dekripsi (*dekripsi*) adalah proses mengembalikan dari *ciphertext* ke dalam *plaintext* semula, dapat disebut juga dengan proses *deciphering*. Skema yang banyak yang digunakan untuk melakukan proses enkripsi dan dekripsi di dalam area studi informatika disebut dengan kriptografi (*cryptography*), atau *cryptographic system* atau disingkat dengan *cipher*. Teknik untuk membuka kunci kode yang tidak diketahui algoritmanya (untuk mengembalikan *ciphertext* ke *plaintext*) disebut dengan *cryptanalysis*. Gabungan antara *cryptography* dan *cryptanalysis* disebut dengan *cryptology*.

Berikut skema dari *symmetric ciphers model:*



Gambar 1 Skema *symmetric ciphers model* (Dony, 2008)

PEMBAHASAN

Banyak cara yang dapat dilakukan jika ingin login ke dalam server Linux, atau dengan kata lain ingin mengakses shell Linux. Lazimnya terdapat dua cara untuk masuk kedalam server linux baik secara remote maupun direct yaitu telnet dan ssh. Untuk penggunaan telnet tidak disarankan karena alasan keamanan transfer datanya yang kurang aman. Untuk SSH yang direkomendasikan untuk digunakan karena setiap perintah yang diketikan di dalam shell akan di enkripi.

SSH bekerja pada port 22. Program untuk ssh bernama OpenSSH. SSH menggunakan enkripsi dan teknik autentikasi RSA (RSA Autenthication), 3DES, Blowfish, CAST128, hmac-md5, hmac-sha1. Untuk dapat menjalankan fasilitas SSH maka daemon SSH di server harus sudah di *running*. Untuk pengecekannya:

```
iqbal0805@27.131.4.117:~$netstat -an | grep 22
 tcp   0 0    0.0.0.0:22  0.0.0.0:*   LISTEN
```

Jika belum, maka pastikan paket OpenSSH sudah terinstall dan menjalankan daemon sshd.

Setiap transfer data melalui SSH walau tidak menggunakan *public* atau *private key* sekalipun, data yang dikirim pasti sudah dienkripsi. Tetapi terdapat kelebihan tersendiri jika menggunakan *public* dan *private key*. Untuk masuk ke Linux melalui SSH, user hanya mengetikkan *username* dan password untuk masuk ke server tetapi tetapi jika menggunakan *key*, maka *user* hanya mengetikkan *username* dan password untuk membuka *public key*.

Jadi bukan password *user* di server linux. Password untuk *public key* dan password login *user* di Linux dapat juga berbeda dan dianjurkan untuk tidak menyamakan password *key* dengan password *username* yang sudah terdaftar di sistem.

Berikut ini contoh login ke Linux menggunakan ssh tanpa menggunakan key.

```
iqbal@180.241.19.251:~$ ssh iqbal0805@27.131.4.117
The authenticity of host '27.131.4.117 (27.131.4.117)'
can't be established.
RSA key fingerprint is
6f:a1:da:97:85:d9:65:10:36:ec:73:9c:44:d1:6a:a3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '27.131.4.117' (RSA) to the list
of known hosts.
iqbal0805@27.131.4.117's password:
Linux 2.6.32-5-686 #1 SMP Mon Dec 23 04:01:19 UTC 2013 i686
The programs included with the Debian GNU/Linux system are
free software;
the exact distribution terms for each program are described
in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the
extent
permitted by applicable law.
Last login: Wed Dec 18 09:57:28 2013 from 114.79.1.4
iqbal0805@27.131.4.117:~$
```

Secara sederhana dengan cara di atas, *user* dapat login dari sistem manapun dan dari *ip address* manapun asalkan terkoneksi ke internet.

Penerapan kriptosistem simetris pada SSH ini dengan kata lain enkripsi dan deskripsi terpusat yaitu *public* dan *private key* disimpan dalam file. Isinya dari file tersebut ialah hasil enkripsi dari kunci untuk membuka *public key*. *Public* digenerate di server atau di klien. Ketika menggenerate *public key*, secara otomatis akan digenerate pula *private key*. Dengan menggunakan key, maka user hanya dapat login ke dalam Linux dimana user harus mempunyai atau menyertakan *private key* user ketika ssh ke dalam sistem.

Untuk lebih jelasnya, akan disimulasikan sistemnya. Digunakan 2 (dua) unit *remote server* di internet yaitu IP 27.131.4.117 dengan distro Linux Debian

dan IP 180.241.19.251 dengan distro Linux Ubuntu dan menggunakan 1 (satu) unit klien dengan sistem operasi Windows yang terkoneksi ke internet. Untuk software yang dibutuhkan, di sisi server sudah terinstall OpenSSH dan di klien Windows menggunakan Putty dan Puttygen untuk keperluan mengimport *private key*.

Langkah 1

Menggenerate key pada server IP 27.131.4.117

```
$ ssh-keygen -t dsa -b 1024
   Generating public/private dsa key pair.
    Enter    file    in    which    to    save    the    key
(/home/iqbal/.ssh/id_dsa):
    Created directory '/home/iqbal/.ssh'.
    Enter passphrase (empty for no passphrase):
    Enter same passphrase again:
    Your    identification    has    been    saved    in
/home/iqbal/.ssh/id_dsa.
    Your    public    key    has    been    saved    in
/home/iqbal/.ssh/id_dsa.pub.
    The key fingerprint is:
    15:28:34:57:cc:44:e4:71:26:fc:13:f1:ad:01:2a:a3
iqbal@27.131.4.117
   The key's randomart image is:
   +--[ DSA 1024]----+
   |     .o .XO =.   |
   |      .o..+B.o . |
   |       .o +. .o .|
   |       . +  o  o |
   |      E S    ..  |
   |                 |
   +-----------------+
```

Dari output di atas, kunci public dan private disimpan pada direktori ~/.ssh. Nama file untuk kunci public yaitu id_dsa.pub dan id_dsa untuk private key. Setelah terbentuk kunci public dan private, maka untuk kunci *public* dicopy ke server IP 180.241.19.251.

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Bagian di atas ialah untuk memasukkan password yang akan digunakan membuka kunci. Nantinya password di atas yang digunakan untuk login bukan password yang tercantum di sistem di /etc/passwd. Sangat dianjurkan untuk membuat password yang berbeda dengan password login di Linux.

Langkah 2

Salin file id_dsa.pub dari IP 27.131.4.117 ke Linux dengan IP 180.241.19.251, dimana di komputer dengan IP 180.241.19.251, mempunyai hak login.

```
$ scp id_dsa.pub iqbal@180.241.19.251:~/
 iqbal@180.241.19.251's password:
 id_dsa.pub 100% |*****************************| 1109 00:00
```

Untuk dapat login ke dalam Linux yang menggunakan *key*, maka di komputer user harus ada *private key*. Dalam hal ini *private key* terdapat di direktori /home/iqbal pada komputer dengan IP 27.131.4.117, maka dari itu jika ingin *remote* dengan SSH *maka private key* (id_dsa) harus selalu disertakan. Jika user dari komputer akan *remote* SSH ke 180.241.19.251, maka di home dir *user* harus salin file id_dsa dari komputer IP 27.131.4.117. Artinya jika tidak mempunyai *private key,* maka *user* tidak dapat login ke Linux walaupun user mengetahui passwordnya sekalipun. Karena ketika kita mengetikkan perintah 'SSH', secara otomatis akan memanggil file id_dsa.

Untuk mengecek konfigurasi, login pada komputer 27.131.4.117 dan ssh ke 180.241.19.251

```
iqbal@27.131.4.117:~$ ssh iqbal0805@180.241.19.251
Enter passphrase for key '/home/iqbal0805/.ssh/id_dsa':
Last login: Wed 18 09:57:28 2013 from 114.79.1.4
iqbal0805@180.241.19.251:~$
```

Jika remote server dari sistem operasi windows, terlebih dahulu user harus mempunyai *private key* sama seperti sistem operasi linux.

Pada sistem operasi windows, *remote login* ssh menggunakan software putty dan untuk meng-*load private key*-nya menggunakan puttygen yang untuk simulasi ini harus upload dari server 27.131.4.117.

KESIMPULAN

Dengan menerapkan kriptosistem simetris pada *remote login* server linux menggunakan ssh lebih aman daripada *remote login* ssh *default* dikarenakan saat ini telah ada software untuk membaca password-password user dari /etc/shadow secara remote menggunakan *brute-force attack* yaitu suatu metode untuk menebak password dari sebeuah enskripsi atau sebuah authentifikasi dengan cara mencobanya berkali-kali dengan berbagai macam kombinasi huruf, angka dan simbol. Salah satu softwarenya yaitu hydera. Setelah penerapan kriptosistem simetris lebih aman karena *user* yang akan me-*remote* server harus memiliki file *private key* dari server tersebut dan membutuhkan authentifikasinya setelah itu.

DAFTAR PUSTAKA

A. Menezes, P.Van Oorchot and S.Vanstone, (1997), "*Handbook of Applied Cryptography*", CRC Press, Inc..

A. Rahmani, (2003), Implementasi Teknik Kriptografi untuk Pengamanan Basis Data, Tesis Magister Departemen Teknik Informatika, ITB.

Dony Ariyus, (2008), Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi, Penerbit Andi.

Heriyanto, Tedi, (2000), *Linux dan Security*, Seminar Nasional Komputer II di Universitas Gadjah Mada Jogjakarta.

Masthurah, Nurhayati, Sistem *Password* pada *SECURITY ENHANCED LINUX (SELINUX), Pusat Penelitian LIPI*

Scheneier, Bruce, (1996), *Applied Cryptography*, Second Edition, New Jersey:John Wiley & Sons, Inc.