SECURE REMOTE LOGIN PADA SISTEM OPERASI SLACKWARE LINUX

Irfan Mahardika NIM : L2F300534

JURUSAN TEKNIK ELEKTRO FAKULTAS TEKNIK
UNIVERSITAS DIPONEGORO SEMARANG

ABSTRAK

Data yang terkirim dari satu host ke host yang lain di internet sangat rawan terhadap serangan penyadapan. Format data tersebut hanya berbentuk plaintext yang tidak terenkripsi. Jika data tersebut merupakan data yang penting sampai jatuh ke tangan ke orang yang tidak berhak maka hal tersebut merupakan ancaman keamanan yang serius.

Remote login seperti telnet sekarang sudah tidak lagi dianjurkan karena telnet tidak melakukan enkripsi terhadap data sebelelum ditransmisikan. Telnet telah digantikan dengan program yang lebih baik seperti SSH (Secure Shell). Namun karena SSH memerlukan lisensi yang khusus sehingga digunakan OpenSSH yang berlisensi gratis. Untuk mengamankan sistem secure remote login ini digunakan perangkat lunak IDS (Intrusion Detection System) yang mampu mendeteksi adanya serangan terhadap keamanan sistem.

Remote login SSH dengan menggunakan kunci publik dan kunci privat yang dibuat oleh klien, memungkinkan remote login dapat dilakukan dengan aman tanpa memberikan username dan password yang digunakan untuk login pada komputer remote. Dengan memanfaatkan perangkat lunak IDS, usaha probe dan scan terhadap sistem dapat dicegah.

I. PENDAHULUAN

1.1 Latar Belakang

Pada awalnya internet belum terlalu mempertimbangkan sekuritas dan privasi. Protokol – protokol yang lazim di internet melewatkan teks (password maupun isi pesan) dalam bentuk teks biasa (*clear text*) yang sangat mudah dapat disadap menggunakan *sniffer*[5]. Telnet maupun rlogin tidak melakukan enskripsi terhadap data sebelum dikirimkan. Sehingga servis seperti telnet dan rlogin tidak dijalankan dan digantikan dengan perangkat lunak yang lebih aman seperti SSH.

OpenSSH[8] merupakan perangkat lunak versi gratis dari SSH yang merupakan paket bawaan Sistem Operasi Slackware Linux[1]. Secara umum, fungsinya adalah melakukan login ke sebuah remote sistem dan juga berfungsi sebagai server SSH.

1.2 Tujuan

Tujuan dari tugas akhir ini adalah untuk menganalisa dan membangun server remote login yang aman pada salah satu sistem Operasi yaitu Slackware Linux yang diaplikasikan sebagai disain pada sebuah jaringan komputer.

1.3 Batasan Makalah

Pembahasan tugas akhir ini dibatasi sebagai berikut:

1. Perangkat lunak yang digunakan sebagai secure remote login adalah OpenSSH, Syslog, Port Sentry, Log Sentry.
2. Sistem secure remote login dioperasikan diatas sistem operasi Slackware Linux 8.1.
3. Protokol yang digunakan adalah SSH2

II. KEAMANAN JARINGAN

2.1. *Security Attack*

Security attack, atau serangan terhadap keamanan sistem informasi, Menurut W. Stallings [9] ada beberapa kemungkinan serangan (*attack*):

1. *Interruption*: Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (*availability*) dari sistem. Contoh serangan adalah “denial of service attack”.
2. *Interception*: Pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan (*wiretapping*).
3. *Modification*: Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (*tamper*) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.

4. *Fabrication*: Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

2.2. Jenis –jenis Serangan Keamanan

Serangan terhadap keamanan sistem sistem informasi adalah kegiatan yang berhubungan dengan jaringan komputer, dimana aktivitas tersebut bertentangan dengan kebijakan keamanan yang berlaku. Pola umum yang digunakan untuk menyerang adalah memperolah akses sistem korban, dan menggunakan akses milik korban untuk melakukan penyerangan terhadap sistem lain. Secara umum, serangan dapat diklasifikasikan menjadi beberapa jenis yaitu *probe, scan, account compromize, root compromize, packet sniffer, denial of service, exploitation of trust, malicous code* dan *internet infrastructure attack.*

2.3 Pemantau Serangan

Sistem pemantau serangan digunakan untuk mendeteksi adanya pengacau (*intruder*) dan serangan (*attack*). Sistem ini dikenal sebagai IDS (*Intrusion Detection System*) yang akan memantau paket yang melalui jaringan tersebut. Cara kerjanya adalah dengan mengawasi jumlah permintaan TCP pada semua port yang ada disebuah komputer tersebut, sehingga bila terjadi percobaan *probe* dapat segera diketahui. Selain memantau lalu lintas paket, sistem ini juga mengawasi *file log*. Adanya serangan dapat dikenali dengan dengan beberapa cara :

- Pertama dengan cara pengenalan terhadap *signature.* Lalu lintas paket yang masuk dan keluar dibandingkan dengan *signature* yang sudah ada. Sebagai contoh koneksi TCP yang gagal pada beberapa port atau lebih merupakan usaha *scan* TCP.
- Kedua adalah dengan deteksi anomali yang menggunakan analisa statistik untuk mengetahui perubahan perilaku yang umumnya terjadi. Contohnya perubahan lalu lintas yang drastis, penggunaan CPU yang berlebihan dan lain – lain. Teknik deteksi ini kurang begitu baik dibandingkan dengan teknik *signature*.

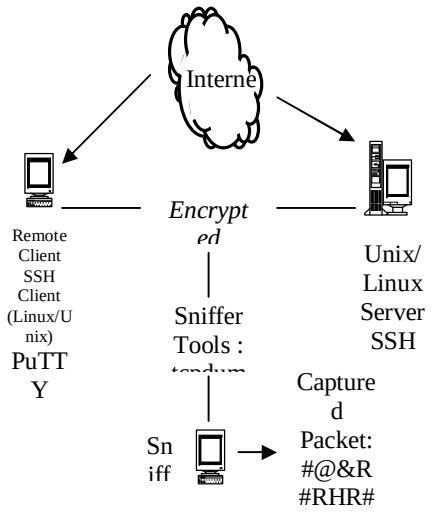
Apabila serangan telah terdeteksi maka IDS dapat melakukan beberapa tindakan antara lain :

- Rekonfigurasi firewall
- Pencatatan ke syslog
- Mengirim email ke sistem administrator
- Melakukan log terhadap aktivitas intruder
- Memutuskan sesi koneksi TCP

Contoh perangkat lunak pemantau serangan yang digunakan adalah PortSentry dan LogSentry. PortSentry digunakan untuk mendeteksi usaha *probe* dari pihak luar. Bila terdeteksi maka PortSentry dapat membuang paket, membelokkan ke sebuah "*dead host*", atau membalas usaha *probe* tersebut. Sedangkan LogSentry digunakan untuk memantau sistem secara keseluruhan dan mencatatnya ke dalam sebuah *log.* Selanjutnya secara berkala *log* tersebut dikirim ke root atau pihak yang bertanggung jawab terhadap sistem tersebut.

2.4. SSH (*Secure Shell)*

SSH merupakan aplikasi klien dan server yang menyediakan *secure remote login* malalui internet maupun jaringan yang tidak terpercaya (*untrusted network*). Algoritma kriptografi digunakan untuk melakukan otentikasi pada kedua belah pihak, mengenkripsi data yang ditransmisikan dan melindungi integritas data. Gambar 2.1 menunjukkan koneksi berbasis SSH.



Gambar 2.1 Koneksi berbasis SSH

SSH bertujuan untuk menggantikan rsh, rlogin, rcp dan protokol telnet. SSH menggunakan protokol berbasis paket biner yang dapat bekerja pada semua lapisan transport yang mampu melewatkan data biner. SSH tersedia sebagai versi komersial dan versi gratis. Untuk versi gratis terdapat beberapa pilihan seperti OpenSSH (Unix,Windows) , LSH (Unix), PuTTY (Windows), Okhapkin's port of SSH1 (Windows), MacSSH

(Macintosh), TeraTerm (Windows), MindTerm (Unix,Windows), NiftyTelnet 1.1 SSH (Macintosh). Sedangkan untuk versi komersial SSH Communication Security (Unix,Windows), F-Secure SSH (Unix,Windows), Secure CRT, SecureFX (Windows), VShell (Windows).

2.5 Arsitektur SSH

SSH protokol mempunyai 3 lapis komponen[10] yaitu SSH *Connection Protocol*, SSH *Authentication Protocol* dan SSH *Transport Protocol*. Ketiganya berada pada tingkat aplikasi dari protokol TCP/IP.

2.5.1 SSH *Transport Layer*

Implementasi SSH server secara umum menggunakan port 22 oleh IANA. Pada saat klien melakukan koneksi ke SSH server, server akan merespon permintaan koneksi tersebut. Server akan mengirimkan string identifikasi versi dan menunggu respon string identifikasi dari klien. Pada kedua sisi harus mampu memproses string identifikasi tersebut. Setelah proses diatas server berpindah ke mode paket biner dan segera mengirimkan paket kunci publik yang berisi check byte, host key, server key, flag protocol, jenis penyandian dan jenis otentikasi ke klien. Klien memproses informasi diatas dan memberikan paket balasan ke server berupa session key yang berisi jenis penyandian yang ada pada sisi klien, check byte, session key (yang terenkripsi oleh kedua sisi) dan flag protocol. Server dan klien mengaktifkan enkripsi dan komunikasi diantaranya dapat berlangsung

2.5.2 SSH Authentication Layer

Lapisan protokol otentikasi merupakan protokol yang multifungsi dan bekerja di atas lapisan protokol transport. Protokol ini menganggap lapisan bawahnya telah menyediakan proteksi terhadap integritas dan kerahasiaan. Server SSH dapat menetapkan kebijakan yang berhubungan dengan otentikasi seperti *idle time out, banner message* dan pembatasan koneksi saat percobaan koneksi gagal. Ada beberapa metode otentikasi yang digunakan yaitu *public key authentication, password authentication* dan *host based authentication*. Metode otentikasi yang sering digunakan adalah *public key* dan *password*.

2.5.3 SSH *Connection Layer*

Lapisan koneksi bekerja diatas lapisan transport dan lapisan otentikasi. Lapisan ini menyediakan sesi login, menjalankan perintah pada remote, forwarded TCP/IP dan forward koneksi X11. Kemampuan port forward memungkinkan klien melakukan forwarding terhadap koneksinya dari remote komputer ke komputer lokal atau sebaliknya. Sebuah port di alokasikan untuk menerima koneksi pada komputer remote dan koneksi ke komputer lokal. Sehingga klien dapat menerima koneksi yang berasal dari komputer remote ke komputer lokal. Hal ini dapat menjadi sebuah celah keamanan, dimana klien berusaha untuk dapat menjalankan sebuah aplikasi pada remote komputer.

2.6 Cara kerja SSH

Misalkan suatu client mencoba mengakses suatu Linux server melalui SSH. SSH daemon yang berjalan baik pada Linux server maupun SHH client telah mempunyai pasangan public/private key yang masing-masing menjadi identitas SSH bagi keduanya. Langkah-langkah koneksinya akan sebagai berikut:

1. Klien melakukan bind pada local port nomor besar dan melakukan koneksi ke port 22 pada server.
2. Klien dan server setuju untuk menggunakan jenis sesi SSH tertentu. Hal ini penting karena SSH v. 1 dan v. 2 tidak kompatibel.
3. Klien meminta public key dan host key milik server.
4. Klien dan server menyetujui alogritma enkripsi yang akan dipakai (misalnya Triple DES atau IDEA).
5. Klien membentuk suatu session key dan mengenkripsinya menggunakan public key milik server.
6. Server akan melakuakn dekripsi terhadap session key yang didapat dari klien, melakukan re-enkripsi dengan public key milik klien, dan mengirimkannya kembali ke klien untuk otentikasi.
7. Klien mengotentikasi dirinya ke server di dalam aliran data terenkripsi dalam session key tersebut. Sampai disini koneksi telah terbentuk, dan client dapat selanjutnya bekerja secara interaktif pada server atau mentransfer file ke atau dari server.

III.IMPLEMENTASI SERVER SSH PADA SISTEM OPERASI SLACKWARE

Untuk membangun sebuah server SSH yang aman dengan menggunakan protokol SSH2 pada sistem operasi Slackware Linux diperlukan beberapa perangkat lunak sebagai

komponen pembentuknya. Berikut adalah komponen perangkat lunak yang digunakan sebagai pembentuk sistem SSH server yaitu OpenSSH, Syslog, Port Sentry, Log Sentry. Protokol SSH2 merupakan protokol yang lebih aman dibandingkan dengan pendahulunya yaitu SSH1

.OpenSSH adalah perangkat lunak sistem remote login yang sudah menjadi bawaan pada Sistem operasi Slackware Linux. Secara umum, fungsi perangkat lunak ini adalah sebagai sebuah klien dan server dari sistem secure remote login.

Syslog adalah perangkat lunak untuk menghasilkan berkas log yang disebabkan adanya aktivitas dari Inetd dan aktivitas lain. Syslog sudah menjadi standar dari Sistem Operasi Linux. Konfigurasi Syslog dan letak berkas log dapat diatur oleh sebuah file konfigurasi yang berada di /etc/syslog.conf.

Port Sentry digunakan sebagai Intrusion Detection System (IDS) yang bertugas untuk mendeteksi dan merespon aktivitas Port Scanning[2] secara waktu nyata (real time).

Log Sentry digunakan sebagai IDS yang bertugas memeriksa berkas log dengan mencari pola yang dicurigai. Bila ditemukan pola yang mencurigakan akan diteruskan dengan peringatan yang dikirimkan melalui email ke sistem administrator.

Port Sentry digunakan sebagai *Intrusion Detection System* (IDS) yang bertugas untuk mendeteksi dan merespon aktivitas *Port Scanning*[2] secara waktu nyata (*real time*).

Log Check digunakan sebagai IDS yang bertugas memeriksa berkas log dengan mencari pola yang dicurigai. Bila ditemukan pola yang mencurigakan akan diteruskan dengan peringatan yang dikirimkan melalui *email* ke sistem administrator.

3.1 OpenSSH

File konfigurasi OpenSSH terletak pada /etc/ssh. File konfigurasi dari server dan klien ada pada direktori ini. File konfigurasi server yaitu sshd_config dan pada klien pada ssh_config.

3.2 Syslog

Syslog berfungsi untuk membuat berkas log yang selanjutnya berkas log tersebut dapat ditampilkan dalam ke console, file, pemakai yang sedang aktif, atau dikirim ke jaringan lain. Kejadian yang dapat terekam oleh syslog adalah auth, authpriv, console, cron, daemon, ftp, kern, lpr, mail, mark, news, ntp, security, syslog, user, uucp, dan local0 sampai dengan local7. Sedangkan untuk jenis-jenis prioritasnya dibedakan menjadi 8 yaitu emerg, alert, crit, err, warning, notice, info dan debug. Konfigurasi syslog berada di /etc/syslog.conf.. Pesan yang ditampilkan syslog secara default ada yang ditampilkan ke console root. Letak file log yaitu pada direktori /var/log.

3.3. PortSentry

Port Scanning merupakan suatu metode untuk memeriksa port apa saja yang aktif pada host target. Port Scanning biasanya merupakan gejala awal yang menandakan akan adanya suatu serangan terhadap sistem tersebut. Port Sentry merupakan program yang didesain untuk mendeteksi dan merespon aktifitas port scanning secara waktu nyata dan memiliki banyak pilihan untuk melakukan pendeteksian tersebut. PortSentry mampu mendeteksi beberapa tipe port scan seperti SYN, FIN, NUL dan X-MAS. Parameter dari PortSentry diatur pada beberapa file yang berapa pada direktori /etc/portsentry. Adapun file – file yang digunakan adalah :

- portsentry.conf
- portsentry.modes
- portsentry.history
- portsentry.ignore

3.4. LogSentry

Log Sentry adalah perangkat lunak yang didesain untuk berjalan otomatis kemudian memeriksa berkas log yang berhubungan dengan pelanggaran keamanan dan aktivitas yang mencurigakan. Dengan menggunakan Log Sentry seorang sistem administrator hanya perlu melihat mailbox untuk mengetahui apakah ada kejadian yang janggal. Tidak perlu lagi membaca dan meneliti berkas log untuk memastikan bahwa host dalam keadaan aman.

Konfigurasi utama pada Log Sentry adalah kepada siapa laporan Log Sentry akan dikirimkan dan interval yang digunakan untuk pemeriksaan berkas log. Pemeriksaan dengan menggunakan interval ini dengan memanfaatkan /etc/crontab yang merupakan daemon yang bertugas untuk menjalankan pekerjaan tertentu pada waktu yang tertentu pula.

3.5. Aplikasi OpenSSH

OpenSSH pada jaringan komputer dapat digunakan untuk melakukan perawatan terhadap server dan keperluan lain seperti penambahan perangkat lunak, backup, transfer file tanpa harus berada di depan konsol server. Pada instalasi Slackware Linux perangkat lunak

IV. Analisa

Setelah sistem secure remote login dan sistem pendukung telah terkonfigurasi dengan benar, maka perlu untuk melakukan pengujian terhadap keseluruhan sistem tersebut. Hal ini dilakukan apakah sistem sudah berjalan dengan baik atau tidak. Pengujian pada sistem secure remote login OpenSSH, yang berfungsi sebagai klien maupun server SSH. Kedua, pengujian Port Sentry dan LogSentry dalam menghadapi port scanning yang biasanya hal ini merupakan tanda awal adanya serangan terhadap sebuah host sekaligus memberikan laporan kepada sistem administrator tentang adanya port scanning.

1. Pengujian SSH server

   Pengujian ini dengan melakukan ssh ke server pada Port 22, berikut perintah yang digunakan :

   ```
   irfan@hatebreed$ssh toolbox@192.168.1.1
   ```

   Pengujian dilakukan dengan melakukan koneksi ssh dari komputer dengan alamat IP 192.168.1.3 (host hatebreed) ke komputer server ssh dengan alamat IP 192.168.1.1 dengan username toolbox. Server SSH menerima permintaan koneksi SSH tersebut dan mengirimkan server host key ke komputer dengan alamat IP 192.168.1.3. Berikut merupakan pesan yang dikirimkan oleh server SSH ke klien.

```
The authenticity of host `192.168.1.1 (192.168.1.1)' can't be established
DSA key fingerprint 9e:c9:7d:3f:fc:46:ed:73:60:d8:1e:ad:0e:3d:47:23
Are you sure you want to countinue connecting (yes/no) ?
```

2. Pengujian Sftp server

   Pengujian dilakukan dari komputer klien yang mempunyai alamat IP 192.168.1.3 ke komputer server yang mempunyai alamat IP 192.168.1.1. Berikut perintah yang digunakan oleh klien untuk melakukan sebuah sesi ftp yang terenkripsi melalui sftp :

```
irfan @ hatebreed $ sftp toolbox@192.168.1.1
The authenticity of host `192.168.1.1 (192.168.1.1)' can't be established
DSA key fingerprint 9e:c9:7d:3f:fc:46:ed:73:60:d8:1e:ad:0e:3d:47:23
Are you sure you want to countinue connecting (yes/no) ?
Warning: Permanently added '19.168.1.1,192.168.1.1' (DSA) to the list of known hosts.
toolbox @ 192.168.1.1 password:
sftp >
```

Sftp server telah bekerja dengan baik, klien dapat melakukan sesi ftp seperti ftp yang biasa digunakan. Untuk meminta bantuan dapat mengetikan help atau ? pada prompt sftp.

3. Pembuatan kunci publik dan kunci privat

   Pembuatan kunci publik dan kunci privat

   Pengujian bertujuan untuk membuat kunci publik yang berfungsi untuk mengenkripsi koneksi dan kunci privat yang digunakan untuk mendekripsi. Kunci yang akan dibuat yaitu kunci DSA, karena protokol SSH versi 2 menggunakannya. Berikut perintah yang digunakan untuk membuat kunci publik dan privat :

```
Irfan@hatebreed$ ssh-keygen –t dsa
Generating public/private dsa key pair
Enter file in wich to save the key (/home/irfan/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again :
Your identification has been saved in /home/irfan/.ssh/id_dsa
Your identification has been saved in /home/irfan/.ssh/id_dsa.pub
The key fingerprint is :
25:42:3b:06:cd:79:3c:ec:fc:c7:2e:6d:f7:9c:ad:c6: irfan@ hatebreed
```

4. PortSentry

   Pada PortSentry pengujian dilakukan dengan melakukan *portscan* dengan menggunakan NMAP dari host bernama eKo dengan alamat IP 192.168.1.3. Laporan dikirimkan oleh LogCheck ke *root* memberitahukan telah terjadi *scanning*.

```
Active System Attack Alerts
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
Feb 14 06:28:51 toolbox portsentry[585]: attackalert: Connect from host: toolbox.toolbox/192.168.1.1 to TCP port: 1
Feb 14 06:28:51 toolbox portsentry[585]: attackalert: Host 192.168.1.3 has been blocked via wrappers with string: "ALL: 192.1168.1.3"
Feb 14 06:28:51 toolbox portsentry[585]: attackalert: Host 192.168.1.3 has been blocked via dropped route using command: "/usr/sbin/iptables –I INPUT –s 192.168.1.3 –j DROP"

Security Violations
=-=-=-=-=-=-=-=-=-=-=
Mar 29 06:28:51 dwik portsentry[585]: attackalert: Connect from host: eko.HomeNet/192.168.1.3 to TCP port: 1
Mar 29 06:28:51 dwik portsentry[585]: attackalert: Host 192.168.1.3 has been blocked via wrappers with string: "ALL: 192.168.1.3"
Mar 29 06:28:51 dwik portsentry[585]: attackalert: Host 192.168.1.3 has been blocked via dropped route using command: "/"/usr/sbin/iptables –I INPUT –s 192.168.1.3 –j DROP"
```

5. LogSentry

   Log Sentry mencatat seluruh aktivitas sistem dan melaporkan melalui email ke sistem administrator atau orang yang bertanggung jawab terhadap sistem

```
Security Violations
=-=-=-=-=-=-=-=-=-=-=
Feb 26 23:35:06 incubus sshd[344] : failed password for toolbox from 192.168.1.3 port 1027 ssh2
```

```
Feb  26  23:35:06  incubus  sshd[348]  :  failed
password for toolbox from 192.168.1.3 port 1028
ssh2
Mar  2  11:12:08  incubus  sshd[257]  :  failed
password for toolbox from 192.168.1.3 port 1025
ssh2
```

V. PENUTUP

5.1. KESIMPULAN

1. Remote login SSH dengan menggunakan kunci publik dan kunci privat yang dibuat oleh klien, memungkinkan remote login dapat dilakukan dengan aman tanpa memberikan username dan password yang digunakan untuk login pada komputer remote.
2. Dengan menggunakan kunci publik dan kunci privat yang dibuat oleh klien, klien dapat melakukan *session* SSH tanpa memasukkan username dan password yang sebenarnya pada komputer remote.
3. Port Sentry berfungsi sebagai IDS (Intrusion Detection System) yang bertugas untuk memonitor percobaan probe pada jaringan dan serangan terhadap sebuah server.
4. Log Check mencatat seluruh aktivitas dari seluruh sistem dan mengirimkan email ke administrator secara periodik.

5.2. SARAN

1. Evaluasi terhadap sistem keamanan jaringan sebaiknya dilakukan sesering mungkin, seiring dengan berkembangnya teknik-teknik penyusupan dan belum ditemukannya kelemahan-kelemahan dalam keamanan jaringan yang belum ada
2. Selalu memeriksa update dari perangkat lunak yang digunakan untuk mencegah adanya ganggunan keamanan terhadap jaringan.

DAFTAR PUSTAKA

1. Cantrell, David, Logan Jonshon, Chris Lumens, *Slackware Linux Essentials : The Official Guide To Slackware Linux*, Website, URL : http://www.slackware.com
2. Fyodor. *Remote OS Detection via TCP/IP Stack Fingerprinting*, URL : http://insecure.org/nmap/nmap-fingerprinting-article-id.html , 10 April 1999
3. Indrajit, Richardus Eko, B.N Prastowo, Rofiq Yuliardi, *Memahami SECURITY LINUX*, PT. Elex Media Komputindo, Jakarta, 2002
4. Mourani, Gerhard, *Securing And Optimalizing Linux : Ultimate Solution*, Open Network Architecture Inc, June 2001
5. Purbo, Onno W , Tony Wiharjito, *Keamanan Jaringan Internet* , PT Elex Media Komputindo, Jakarta, 2000
6. Purbo, Onno W., *TCP/IP Standar, Desain dan Implementasi*, PT.Elex Media Komputindo, Jakarta, 2000
7. Rahardjo, Budi , Keamanan Sistem Informasi Berbasis Internet, PT Insan Komunikasi / Infonesia, Bandung. 1999
8. Stallings, William , "*Network and Internetwork Security*," Prentice Hall, 1995
9. Ylonen, Tatu, The SSH (*Secure Shell*) *Remote Login Protocol*, 1996. URL : http://www.cs.hut.fi
10. Ylonen, Tatu, T. Kivinen, M. Saarinen, T. Rinne, S. Lethinen. SSH Transport Layer Protocol. Internet Draft, January 2001
11. ……., OpenBSD Team, *OpenSSH Manual pages version 1.20*, 10 Oktober 2002 URL : http://openbsd.c2pro.net/openssh/manual.html
12. ……., OpenSSH Manual pages version 1.20, 10 Oktober 2002, Website, URL : http://openbsd.c2pro.net/openssh/manual.html

Penulis lahir di Semarang, 25, Agustus 1977. Saat ini sedang menyelesaikan pendidikan S1 di Jurusan Teknik Elektro Universitas Diponegoro Semarang.

Semarang, April 2003

Pembimbing I	Pembimbing II
Ir. Kodrat IS, MT	Wahyudi, ST, MT
NIP. 132 046 696	NIP. 132 086 662