ANALISIS TINGKAT KEAMANAN DALAM HAL SPAMMING MENGGUNAKAN TESTING OPEN RELAY ANTARA SENDMAIL DAN QMAIL

Nila Feby Puspitasari[1]

Abstraksi

Sebuah server dalam internet menjalankan sebuah aplikasi (perangkat lunak) yang berlaku sebagai server. Aplikasi tersebut berjalan dalam server dan menunggu orang atau program yang akan mengirimkan data atau perintah ke server tersebut. Mail Server menjalankan sebuah aplikasi yang ditujukan untuk proses pengiriman dan penerimaan e-mail, aplikasi tersebut biasa disebut sebagai *MTA (Mail Transfer Agent)* sedangkan aplikasi yang berjalan pada komputer-komputer lain yang dilayani oleh server *(client)* disebut dengan MC *(Mail Client)* [Prakoso, Tomy, Purbo, 2003].

Sendmail merupakan MTA yang paling tua di Internet yang dibuat oleh Eric Allman. Pada saat ini, hampir semua distribusi Linux dan BSD menggunakan sendmail sebagai MTA standarnya.

Qmail adalah sebuah software MTA yang dibuat oleh Dan Bernstein, yang ditujukan sebagai pengganti sendmail yang telah mendominasi disetiap sistem operasi

[1] Staff Pengajar STMIK AMIKOM Yogyakarta

UNIX. Software ini menggunakan protokol SMTP untuk mengirimkan e-mail ke MTA / server yang lain.

Sebuah server mail disebut “open relay” jika server tersebut meneruskan pesan email yang diterimanya tanpa melihat siapa pengirimnya dan ke mana email tersebut di kirimkan.

Kata Kunci: Mail Server, MTA, MC, Open Relay

1. Pendahuluan

Secara umum, masalah sekuriti di Internet dapat dipandang dari dua sisi penting. Sisi pertama adalah integritas data yang dikirimkan melalui jaringan Internet (kita sebut saja ***integritas pengiriman data***) dan sisi berikutnya adalah tingkat sekuriti dalam jaringan komputer itu sendiri (kita sebut ***sekuriti jaringan internal***).

Sebuah server adalah komputer yang dikhususkan untuk melayani komputer-komputer lain dalam jaringan seperti Internet, dengan layanan-layanan tertentu. Email atau *electronic-mail* adalah suatu bentuk komunikasi dengan menggunakan perangkat elektronik terutama komputer. Server dalam Internet menjalankan sebuah aplikasi yang akan menunggu program untuk mengirimkan data atau perintah ke server tersebut. Server email menjalankan sebuah aplikasi yang ditujukan untuk proses pengiriman dan penerimaan email. Aplikasi yang

berjalan pada server ini disebut dengan MTA (*Mail Transfer Agent*) sedangkan aplikasi yang berjalan pada komputer-komputer lain yang dilayani oleh server (*client*) disebut dengan MC (*Mail Client*) [Prakoso, Tomy, Purbo, 2003].

Ada banyak server email yang saat ini digunakan dalam jaringan Internet yang menggunakan sistem operasi Linux/Unix. Di antaranya yang terkenal adalah SendMail dan QMail. Kedua server email ini memiliki keunggulan dan kelemahan masing-masing dalam melayani dan mengirimkan email.

Sebuah sistem unix biasanya lansung dibundled oleh MTA (Mail Transfer Agent) bernama sendmail. Dengan konfigurasi default yang diletakkan pada /etc/sendmail.cf biasanya mail sudah dapat keluar masuk. Setelah itu sysadmin tidak akan mengutak-utik hal yang berhubungan dengan sendmail. Jika ada kebutuhan tambahan yang berkaitan dengan service mail, maka sysadmin akan mencoba melihat sendmail.cf, apakah ada yang bisa diubah sedikit atau ditambahkan. Namun apa yang terjadi.

Ternyata sendmail.cf adalah sebuah file text besar yang sebagian besar tidak dapat dibaca, penuh dengan kode-kode yang perlu dipelajari dulu sebelumnya. Untuk mengerti apa yang dikatakan sendmail.cf, sysadmin perlu membaca manual dan buku referensi (sebagai contoh buku berjudul 'sendmail' buatan O'reilly). Untuk semuanya perlu waktu yang tidak sedikit.

Sendmail juga dikenal sebagai MTA yang mempunyai banyak BUG. Sendmail versi awal mempunyai kode 46000 baris dan versi 8.6.12 mempunyai kode 41000 baris . Bug yang sudah ditemukan sampai saat ini sekitar 20. Mengingat banyaknya baris, maka memungkinkan untuk ditemukannya bugs lagi.

Lalu muncullah MTA bernama qmail yang dibuat seseorang yang tidak puas atas kinerja dan buggy sendmail. Qmail tidak merepotkan sewaktu instalasi. Dan juga mempunyai file konfigurasi yang sederhana yang terdiri dari beberapa file yang diletakkan pada direktori /var/qmail/control.

Dengan melihat permasalahan yang ada tentang karakteristik server email antara sendmail dan qmail, maka penulis sangat tertarik untuk menganalisis kedua server email yang nantinya dapat diberikan solusi terbaik untuk penanganan server email yang mempunyai keunggulan dan kelemahan antara kedua server email tersebut.

Parameter yang harus diperhatikan dalam permasalahan ini adalah:

a. Bagaimana membuat atau membangun sebuah aplikasi mail server antara sendmail dan qmail meliputi: instalasi paket aplikasi, konfigurasi, cara kerja dll.
b. Menguji dan menganalisa tingkat keamanan aplikasi mail server dalam hal

spamming antara sendmail dan qmail dengan testing open relay.

Tujuan dari Penelitian ini adalah untuk mnganalisis tingkat keamanan dalam hal Spamming dengan Testing Open Relay antara Sendmail dan Qmail sehingga bisa dibuktikan bahwa salah satu dari mail Server tersebut mempunyai keunggulan lebih.

Adapun manfaat yang bisa diperoleh dari penelitian ini yaitu hasil penelitian ini bisa di jadikan sebagai acuan dan referensi tentang keunggulan dan kelemahan dari Sendmail dan Qmail

2. Pembahasan

Keamanan Email

Untuk melihat keamanan sistem Internet perlu diketahui cara kerja sistem Internet. Antara lain, yang perlu diperhatikan adalah hubungan antara komputer di Internet, dan protokol yang digunakan. Internet merupakan jalan raya yang dapat digunakan oleh semua orang (*public*). Untuk mencapai server tujuan, paket informasi harus melalui beberapa sistem (router, gateway, hosts, atau perangkat-perangkat komunikasi lainnya) yang kemungkinan besar berada di luar kontrol dari kita. Setiap titik yang dilalui memiliki potensi untuk dibobol, disadap, dipalsukan.

Identifikasi Keamanan Email

Secara umum Email berisi data-data dan informasi yang mana data dikategorikan menjadi dua, yaitu data yang bersifat rahasia dan data yang tidak bersifat rahasia. Data yang tidak bersifat rahasia biasanya tidak akan terlalu diperhatikan. Yang sangat perlu diperhatikan adalah data yang bersifat rahasia, dimana setiap informasi yang ada didalamnya akan sangat berharga bagi pihak yang membutuhkan karena data tersebut dapat dengan mudah digandakan. Untuk mendapatkan informasi didalamnya, biasanya dilakukan berbagai cara yang tidak sah.

Keamanan data biasanya terkait hal-hal berikut:

a. **Fisik,** dalam hal ini pihak yang tidak berwenang terhadap data berusaha mendapatkan data dengan melakukan kegiatan sabotase atau penghancuran tempat penyimpanan data.
b. **Organisasi,** dalam hal ini pihak yang tidak berwenang untuk mendapatkan data melalui kelalaian atau kebocoran anggota yang menangani data tersebut.
c. **Ancaman dari luar,** dalam hal ini pihak yang tidak berwenang berusaha untuk mendapatkan data melalui media komunikasi dan juga melakukan pencurian data yang tersimpan di dalam komputer.

Fungsi keamanan komputer adalah menjaga tiga karakteristik, yaitu:

a. ***Secrecy***, adalah isi dari program komputer hanya dapat diakses oleh orang yang berhak. Tipe yang termasuk di sini adalah *reading, viewing, printing*, atau hanya yang mengetahui keberadaan sebuah objek.

b. ***Integrity***, adalah isi dari komputer yang dapat dimodifikasi oleh orang yang berhak, yang termasuk disini adalah *writing, changing status, deleting*, dan *creating*.

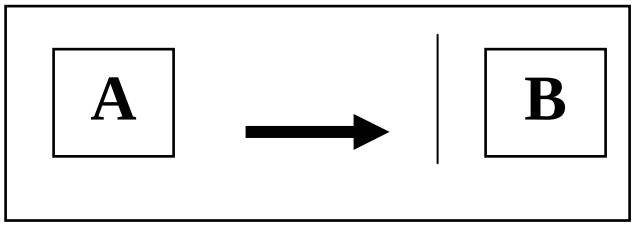
c. ***Availability***, adalah isi dari komputer yang tersedia untuk beberapa kelompok yang diberi hak.

Data yang aman adalah data yang memenuhi ketiga karakteristik keamanan data tersebut.

Melihat pada kenyataan semakin banyak data yang diproses dengan komputer dan dikirim melalui perangkat komunikasi elektronik, maka ancaman terhadap pengamanan data akan semakin meningkat. Beberapa pola ancaman terhadap komunikasi data dalam komputer dapat diterangkan sebagai berikut:

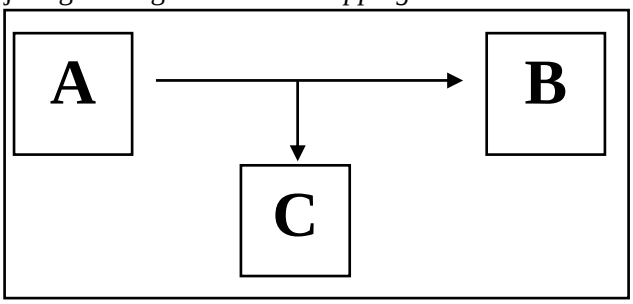
a. ***Interruption***, terjadi bila data yang dikirimkan dari A tidak sampai pada orang yang berhak B. *Interruption* merupakan pola penyerangan terhadap sifat *availability* (ketersedian data). Contohnya

adalah kerusakan pada *hardware*, kegagalan *operating system* sehingga sistem tidak dapat menemukan file yang dicari.



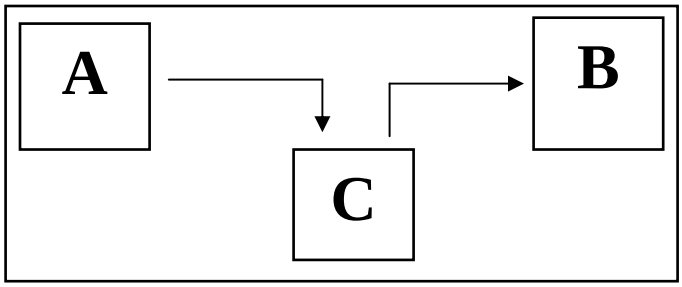
Gambar 1. *Interruption*

b. ***Interception***, terjadi bila pihak ketiga C berhasil membaca data yang dikirimkan. *Interception* merupakan pola penyerangan terhadap sifat *confidentiality/secrecy* (kerahasian data), contohnya adalah penggandaan program atau file data yang tidak terlihat, atau pencurian data pada jaringan dengan cara *wireteapping.*



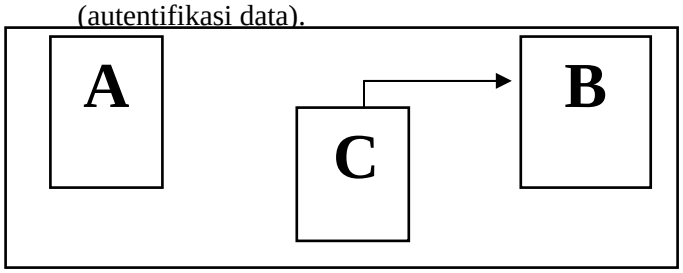
Gambar 2. *Interception*

c. ***Modification***, pada serangan modification pihak ketiga C berhasil merubah pesan yang dikirimkan. *Modification* merupakan pola penyerangan terhadap sifat *integrity* (keaslian data).



Gambar 3. *Modification*

d. ***Fabrication,*** pada serangan *fabrication* penyerang berhasil mengirimkan data ke tujuan dengan memanfaatkan identitas orang lain. *Fabrication* merupakan pola penyerangan terhadap sifat *authenticity* (autentifikasi data).



Gambar 4. *Fabrication*

Open Relay dan Spamming

Sebuah mail server disebut ‘open relay’ jika server tersebut meneruskan pesan e-mail yang diterimanya tanpa melihat siapa pengirimnya dan kemana e-mail tersebut dikirimkan. Pada awal-awal berdirinya Internet hal ini tidak menjadi masalah. Pada awalnya semua server e-mail meripakan open relay, hal ini dilakukan sesuai dengan tujuan berdirinya internet yaitu untuk menyebarkan informasi seluas mungkin.

Namun, hal ini ternyata mengundang orang-orang yang tidak bertanggungjawab dengan menyalahgunakan sifat open relay dari server mail. Orang-orang tersebut menggunakan sifat open relay ini dengan tujuan tidak baik, seperti menghabiskan ‘bandwidth’ dari jaringan server email, atau menghabiskan resource dari server tersebut hingga akhirnya server tersebut ‘down’. Ada lagi orang yang menggunakan sifat open relay dari server tersebut untuk mengirimkan e-mail ke berbagai tujuan, padahal pesan dalam e-mail tersebut tidak di kehendaki oleh si penerima (biasanya e-mail tersebut berisi semacam promosi atau iklan akan hal-hal tertentu, seperti iklan-iklan produk atau situs-situs porno). Tindakan tersebut dalam dunia Internet di sebut sebagai spamming

dan pelakunya disebut sebagai seorang spammer. Sedangkan e-mail yang dikirimkan spammer tersebut biasanya disebut sebagai junk-mail.

Metode Penelitian

Subjek Penelitian

Subyek penelitian kali ini adalah bagaimana menganalisis tingkat keamanan (sekuriti) dalam hal spamming menggunakan testing open relay pada sebuah aplikasi mail server antara sendmail dan qmail yang merupakan sebuah MTA *(Mail Transfer Agent)* yaitu program yang bertanggung jawab dalam hal pengiriman sebuah email ke suatu tujuan alamat. Program ini biasanya akan menjadi sebuah *daemon* dan membuka koneksi pada port 25 (smtp) yang digunakan sebagai penghubung antar MTA. Dalam hal ini penulis mencoba membangun dan mengkonfigurasi sebuah aplikasi mail server yaitu sendmail dan qmail.

Alat Penelitian

Sebelum menginstal Sendmail maupun Qmail, sistem harus memiliki beberapa kriteria pokok agar pelaksanaannya tidak terganggu. Kebutuhan utama adalah kebutuhan hardware(perangkat keras) dan software(perangkat lunak).

Kebutuhan Hardware

Untuk membangun sebuah server tentu dibutuhkan hardware yang lebih tinggi dibandingkan dengan komputer client walaupun sebenarnya menggunakan komputer sekelas client pun bisa dilakukan. Hardware yang dibutuhkan bergantung pada jumlah banyak client dan juga jumlah transfer data setiap harinya. Untuk menjadi referensi, dalam melakukan penelitian ini penyusun menggunakan server dan client dengan spesifikasi sebagai berikut :

- PC Prosesor intel P III 550 MHz
- RAM 128 MB
- Hardisk 20 GB Quantum Fireball
- VGA Card Nvidia Vanta 32 MB
- Network Card RTL 8139

Kebutuhan Software

Sistem operasi yang digunakan dalam penelitian kali ini adalah Linux Redhat 7.3, sendmail yang sudah terintegrasi dengan linux, dan qmailrocks.tar sebagai aplikasinya, fasilitas pendukung lainnya adalah Apache Web Server, DNS, PHP, MySQL, Perl dan lain sebagainya.

Analisis data dan Interpretasi

Adapun hasil penelitian yang bisa penulis sajikan adalah bahwa sendmail bersifat masih bersifat vulnerability atau rentan terhadap penyerangan, sehingga bisa ditembus oleh kode-kode jahat. Hal ini diperkuat oleh :

- Data dari Internet Security systems yang bekerja sama dengan Departemen Homeland Security. Data terbaru mengatakan bahwa tanggal 3 Maret 2003, ditemukan sebuah lubang pada root sendmail untuk versi yang lebih rendah 8.12.8 sehingga memaksa setiap sistem pada jaringan di upgrade ke versi yang lebih tinggi[2].
- Sendmail mempunyai banyak BUG, sendmail versi awal mempunyai kode 45000 baris dan versi 8.6.12 mempunyai kode 41000 baris. Bug yang sudah ditemukan hingga saat ini ada 20. mengingat banyaknya baris, maka memungkinkan untuk ditemukannya bugs lagi[3].

Sedangkan Qmail tergolong mail server yang aman karena :

- Qmail di Klaim sebagai server email yang sangat aman, hal ini di dukung dengan

[2] Referensi http://www.iss.net/security_center/
[3] Dodi Maryanto Subhan, lebih jauh tentang Qmail

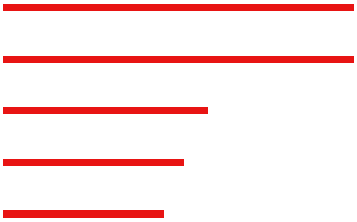
hadiah US$ 1000 dari pendukung qmail yang mampu menemukan lubang keamanan pada qmail. Penyedianya juga menyediakan hadiah Us$500 bagi yang berhasil menemukan lubang keamanan pada qmail.

Analisis Keamanan (Sekuriti)

Sesuai dengan rumusan permasalahan yang ada, penulis akan menganalisis tingkat keamanan/sekuriti dari kedua aplikasi mail server tersebut berdasarkan sumber-sumber data yang ada dan penulis juga mengadakan pengamatan secara langsung dengan testing open relay. Tabel dibawah ini akan menunjukkan bilamana sebuah server mail memberlakukan open relay yang berdasarkan data analisis statistik dari sebuah badan independent yaitu ORDB yang mengatasi masalah open relay.[http://www.ordb.org]

Berikut adalah Tabel MTA statistic open relay:

Sendmail	21.2%
Exchange	18.76%
IMail	10.22%
UNKNOWN	9.04%
Microsoft ESMTP	8.07%



MAIL Serv	
IMS	3.89%
MDaemon	2.56%
Post.Office	2.52%
Lotus Domino	2.42%
GroupWise	2.29%
qmail	1.86%

Dari tabel statistik diatas bisa diperlihatkan bahwa prosentase penggunaan open relay pada sendmail menempati urutan pertama dari beberapa server email yang ada yakni 21.2% sedangkan qmail mempunyai prosentase penggunaan open relay sebesar 1.86 %. Hal ini bisa merupakan sebuah bukti yang bisa memperkuat analisis data yang penulis lakukan.
Analisis tingkat keamanan aplikasi mail server antara sendmail dan qmail adalah sebagai berikut:

- **Pada Sendmail**
  - Sendmail adalah sebuah program besar yang bersifat rawan terhadap spamming, dan jika terjadi kerentanan pada sebuah bagian, maka bagian lain akan mudah dimasuki.

- Sendmail adalah sebuah aplikasi mail server yang mendukung format mailbox dalam penyampaian emailnya. E-mail disimpan dalam sebuah file. Setiap kali ada surat masuk atau keluar, ditambahkan *(embed)* secara otomatis kedalam file yang bersangkutan. Dengan demikian ukuran file mbox ini bertambah setiap kali ada penambahan e-mail. Kelemahannya apabila ada data yang rusak atau hilang sebagian, maka data yang lainnya akan ikut hilang.

- Dalam proses pengiriman data sendmail mempunyai beberapa mode yaitu slow+queued dan fast+unsafe.

- Sendmail bisa di integrasikan dengan software anti virus dan email scanner contohnya, Clamav antivirus dan Amavis.

➢ **Pada Qmail**

- Qmail terdiri dari program-program kecil dalam menjalankan fungsiny yang berada dalam urutan yang tetap dan jika sudah tidak digunakan dalam proses, maka program itudi buang dalam urutan, sehingga jika terjadi kerentanan pada suatu program kecil, maka program kecil itu akan disisihkan setelah digunakan

- Qmail memberlakukan format maildir dalam proses penyampaian email, yang mana maildir merupakan format yang *anti crash*, dan lebih reliabel dibandingkan format mbox.

- Qmail dalam melayani proses atau tugas, qmail menggunakan system modular, dimana setiap proses akan dilayani (di *handle*) oleh modul yang terpisah dengan modul yang lain. Setiap modul yang berjalan dengan tingkat keamanan yang berbeda yang tidak berhubungan dengan modul yang lain sehingga keamanan data terjamin.

- Aplikasi pendukung qmail cukup banyak yang terintegrasi dengan keamanannya antara lain Qmail-Scannner, Maildrop, Clamav antivirus, Spamassasin yang fungsinya untuk menangkal adanya spam yang masuk.

Dari analisa tentang keamanan aplikasi mail server antara sendmail dan qmail diatas berdasarkan sumber-sumber yang ada dengan didasarkan pada pengamatan yang dilakukan penulis, maka dapat disimpulkan bahwa dari kedua aplikasi mail server ter sebut dalam hal sekuriti aplikasi, qmail tergolong lebih unggul dan mempunyai sekuriti yang lebih baik dari pada sendmail. Penggunaan Qmail merupakan

solusi yang dapat di ambil untuk membangun sebuah mail server yang handal.

3. Penutup

Dari hasil penelitian dan pembahasan disimpulkan bahwa aplikasi mail server khususnya qmail memiliki memiliki keunggulan yang lebih di banding sendmail dalam hal keamanan atau sekuriti, karena qmail memiliki karakteristik sebagai berikut :

1. Aman *(secure)*, keamanan bukan sekedar goalnya, tetapi suatu kebutuhan mutlak yang harus dimiliki oleh sebuah aplikasi mail server. Qmail di *Claim* aman oleh si pembuatnya D.J. Bernstein karena sampai saat ini belum ada yang bisa membobol keamanan mail server tersebut. Salah satu contoh dari item pendukung nya berdasarkan pengamatan penulis adalah qmail tidak bersifat open relay, sehingga terproteksi.
2. Dapat diandalkan, sekali pesan e-mail diterima oleh sistem qmail, pesan tersebut tidak akan hilang sekalipun tiba-tiba listrik padam sewaktu pengiriman dilakukan, karena qmail mendukung format *maildir* yang tidak akan rusak sewaktu sistem mengalami *crash*.
3. Simple dan Kecil, qmail dikatakan simple dan kecil karena qmail terdiri dari program-

program kecil yang memisahkan mekanisme untuk *forwarding*, *aliasing* dan *mailing list*, dan qmail hanya mempunyai 1 mode pengiriman yaitu fast+queued (cepat dan dibuat antrian). Qmail send, yaitu program untuk mengirimkan mail dipicu oleh adanya antrian baru.

4. Menggantikan sendmail, dengan administrasi virtual domain yang mudah, dengan menggunakan program vpopmail, sebuah program *add-in* untuk qmail, qmail dapat mendukung banyak domain sekaligus dalam sebuah server.

4. Daftar Pustaka

Albertus Dwiyoga W, 2004: ***Membangun Mail Server andal dengan Fedora dan Qmail,*** PT. elex Media Komputindo.

Arul, ***Instalasi Jaringan dengan Linux***, Klub Linux bandung.

Frans Setiawan, 2002: ***Mengamankan Web server dari Serangan Hacker/ Cracker***, PT. Elex Media Komputindo.

Jhony H, Sembiring, 2002: ***Jaringan Komputer Berbasis Linux***, PT Elex Media Komputindo.

Onno W. Purbo, 2001: ***TCP/IP*** , Pt. Elex media Komputindo.

Samuel Prakoso, Tomy, Onno W Purbo, 2003: ***Panduan Praktis Menggunakan E-mail server Qmail,*** PT. Elex Media Komputindo.

Tommy PM Hutapea, ***Pengantar Konsep dan aplikasi TCP/IP***, www.ilmukomputer.com.

http://sendmail.org

http://qmail.org