Analisa Dan Implementasi Spam Filtering Menggunakan Metode DNS *Blacklisting* Dan *Keyword Filtering*

Permadi, Harun Mukhtar, Budi Arham,
Fakultas Ilmu Komputer Universitas Muhammadiyah Riau

Abstrak *- Elecronic mail, atau akrab disebut email, merupakan istilah popular untuk pesan atau surat elektronik. Biasanya berbentuk pesan teks sederhana yang ditulis seseorang (user) melalui sebuah sistem computer dan ditransmisikan ke computer lain yang dituju dengan melintasi jaringan computer. Jika dilihat dari operasinya, informasi proses software email berasal dari berbagai sumber bebas yang sangat potensial untuk mendatangkan bahaya. salah satunya adalah email sampah atau yang umumnya sering dikenal dengan spam mail. Dengan banyaknya spam yang menyebar ini, sudah pasti menyebabkan kerugian besar bagi ISP karena banyak bandwitch yang terbuang hanya untuk email sampah, dan bagi user hal ini dapat menurunkan produktifitas kenyaman dalam menggunakan email. Karena inbox untuk mail user akan dipenuhi oleh email sampah, dan akan membutuhkan waktu yang lama untuk menyeleksi email mana saja yang Ham dan email mana saja yang Spam. Dengan masalah yang dihadapi user tersebut spam filter akan sangat berguna dalam memblokir spam tersebut, dan dengan adanya spam filter ini diharapkan dapat menambah produktifitas dari user. DNS Blacklisting dan Keyword Filtering merupakan salah satu metode yang digunakan dalam blokir spam*

Kata kunci : Spam Filtering, DNS Blacklisting, Keyword Filtering

1. Pendahuluan

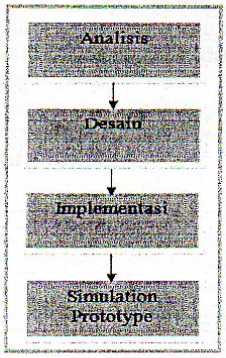
Semenjak internet tumbuh dan popular, penggunaan *email* nyaris mendominasi aktivitas di internet. Banyak orang dari berbagai kalangan menggunakan *email* untuk kebutuhan komunikasi mereka. Tidak terbatas pada praktisi bisnis, pendidikan, melainkan juga untuk kalangan umum, dalam tingkat yang signifikan, penggunaan *mail electronic* nyaris menyamai penggunaan sistem pos tradisional. Hal ini dapat dimaklumi karena *email* menawarkan beberapa keuntungan bagi penggunanya, diantaranya lebih ekonomis, lebih simple, sangat cepat, mudah dikelola, dan mampu mentransmisi beragam format dokumen. Tetapi pertumbuhan internet di dunia berbanding lurus dengan kejahatan-kejahatan yang muncul karenanya.

Jika dilihat dari operasinya, informasi proses *software email* berasal dari berbagai sumber bebas yang sangat potensial untuk mendatangkan bahaya.salah satunya adalah *email* sampah atau yang umumnya sering dikenal dengan *spam mail.* Menurut *Cisco IronPort SenderBase Security Network* (senderbase.org, 2013) pada tanggal 19 maret 2013 *volume spam* yang terkirim setiap harinya adalah sebanyak 173.4 miliar *spam* 86.2% dari total *email* yang terkirim setiap harinya, yang berarti *email* yang dikirimkan setiap hari masi didominasi oleh *spam mail.* Jenis *spam* yang sering beredar yaitu *spam* yang menggunakan domain palsu sebagai menutupi identitas spammer. Hal tersebut banyak dilakukan untuk melakukan penipuan terhadap *user.* Satu lagi jenis *spam* yang juga sering beredar yaitu *spam* yang isi pesan yang mengandung kata-kata negatif atau melanggar aturan dalam berkomunikasi.

Banyaknya *spam* yang menyebar ini, sudah pasti menyebabkan kerugian besar bagi ISP karena banyak *bandwitch* yang terbuang hanya untuk *email* sampah, dan bagi *user* hal ini dapat menurunkan produktifitas kenyaman dalam menggunakan *email*. Karena *inbox* untuk *mail user* akan dipenuhi oleh *email* sampah, dan akan membutuhkan waktu yang lama untuk menyeleksi *email* mana saja yang *Ham* dan *email* mana saja yang *Spam*. Dengan masalah yang dihadapi *user* tersebut *spam filter* akan sangat berguna dalam memblokir *spam* tersebut, dan dengan adanya *spam filter* ini diharapkan dapat menambah produktifitas dari *user*. DNS *Black listing* dan *Keyword Filtering* merupakan salah satu metode yang digunakan dalam blokir *spam*.

2. Metodologi Penelitian

Metodologi penelitian merupakan tahapan-tahapan yang dilakukan dalam penyusunan tugas akhir. Dimana konsep dari metode adalah bagaimana melihat suatu masalah secara sistematis dan terstruktur dari atas kebawah. Dalam penelitian ini langkah bertahap atau metodologi penelitian dapat digambarkan secara rinci yang ditunjukkan oleh gambar 1 sebagai berikut :



Gambar 1. *Network Development Life Cycle* (NDLC)

Untuk mempermudah dalam penulisan skripsi ini penentuan metode adalah hal yang sangat penting. Metode merupakan langkah-langkah sistematis yang digunakan untuk mempermudah dalam pembangunan sistem. Metode yang digunakan pada penelitian ini adalah metode yang dikutip dari *Network Development Life Cycle* (NDLC) yang mengacu pada gambar 3.1. Adapun metode pengerjaan yang digunakan dapat adalah analisis, desain, implementasi dan , simulasi prototype.

Pengumpulan data pada tahap analisis dilakukan dengan dua tekhnik pengumpulan data yaitu sebagai berikut :

2.1. Observasi

Mengumpulkan dokumen *email spam* dan *non-spam* yang akan digunakan sebagai data dalam proses *indexing* dan proses *querying* untuk aplikasi. Data tersebut diperoleh dari *email* yang terdapat pada *inbox mail client user* tertentu.

2.2. Studi Literatur

Pengumpulan data yang dilakukan dengan cara mempelajari dan meneliti berbagai literature dari perpustakaan yang bersumber dari buku-buku, jurnal ilmiah, situs internet, dan bacaan laiinya yang berkaitan dengan penelitian yang dilakukan. Tahap ini dilakukan untuk meneliti referensi materi terkait dengan pembahasan yang berkaitan dengan analisa dan perancangan sistem, baik pada situs yang dipercaya maupun pada buku-buku yang resmi.

3. Hasil dan Pembahasan

3.1. Analisis Sistem

Pada pengembangan sebuah sistem berbasis komputer, analis sistem merupakan bagian yang sangat penting dalam melakukan penelitian dimana hasil dari analisa sistem dapat mengetahui beberapa kelemahan dan memberikan usulan analisis sistem yang baru. Analisis sistem merupakan tahapan awal paling

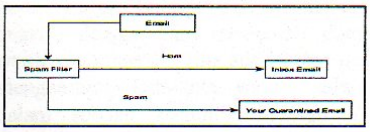
awal dari pengembangan sistem yang akan dihasilkan nantinya. Analisa ini meliputi fungsi-fungsi yang dibutuhkan, dan kinerja yang harus dipenuhi. Analisa sistem adalah tekhnik pemecahan masalah yang menguraikan bagian-bagian komponen dengan mempelajari seberapa bagus bagian-bagian komponen tersebut bekerja dan berinteraksi untuk mencapai tujuan mereka. Penelitian ini, membahas sebuah sistem *spam filtering* yang bertujuan untuk mendukung pengurangan dampak *spam mail* pada *mailbox.*

3.1.1. Deskripsi Sistem

Email adalah surat elektronik sebagai menerima dan mengirim surat melalui jalur internet. Untuk kenyaman antara pengguna surat elektronik (*Email*) dari pesan-pesan sampah yang sering disebut dengan spam . Maka dibutuhkan sebuah sistem anti *spam* (*spam filtering*). Dalam pengamanan dari dampak buruk serangan spammer sistem ini akan menjelaskan mengenai metode DNS *Blacklisting* dan *Keyword Filtering.* Dengan menggunakan kedua metode tersebut dapat memberikan kenyaman antar pengguna email untuk saling bertukar pesan.

3.1.2. Analisis Kerja Sistem Secara Umum

Gambar 2 dapat jelas dari kerja sistem yang dibuat sesuai dengan kebutuhan sistem *Spam Filtering* dengan menggunakan metode DNS *Blacklisting* dan *Keyword Filtering.*

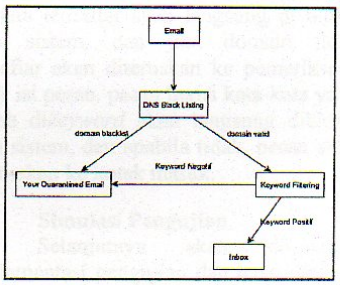


Gambar 2. Kerja Sistem Sesuai *Spam Filtering*

Gambar 2 menjelaskan tentang proses kerja secara umum yang akan di rancang dalapam penelitian ini. Sistem *spam filtering* ini hanya memfilter *email* yang datang dari luar, yang akan diseleksi dengan menggunakan dua metode yaitu, metode DNS *Blacklisting* dan *Keyword Filtering.* Jika *email* yang masuk telah diperiksa sistem dan bebas dari kriteria sebuah *spam,* akan langsung dikirim ke *Inbox,* sedangkan *email* yang memiliki kriteria *spam* akan langsung di blokir oleh sistem. Ada dua kriteria *email* yang akan dikategorikan sebagai *spam* yaitu, dengan melihat dari domain nya dan dilihat dari kata-kata isi *email.*

a. Analisis *DNS Blacklist* dan *Keyword Filtering*

Pada Gambar 3 adalah rancangan alur sistem *spam filtering* dengan metode DNS *Blacklisting* dan *Keyword Filtering.*



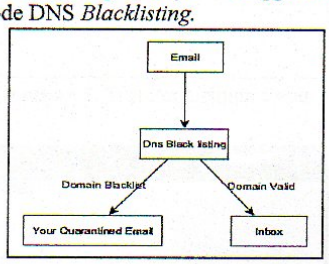
Gambar 3. Proses DNS *Blacklisting* dan *Keyword Filtering*

Dalam proses *filtering* dengan metode DNS *Blacklisting* bekerja dengan cara memeriksa menurut nama domain yang terdaftar pada *Mail Server.* Metode ini memblok *spam-mail* berdasarkan IP atau domain atau alamat *email* tertentu yang telah dikategorikan sebagai alamat spammer. Sebagai contoh hadiah@hotmail.com. pada bagian hotmail.com akan ditandai kedalam sebagai *blacklist* sebuah *spam.* Jadi,

sebelum sebuah *email* masuk kedalam server untuk dikirim ke email client akan di periksa domain hotmail.com apakah terdaftar sebagai *blacklist spam*. Jika ia, *email* akan langsung di tolak oleh sistem dan jika domain tidak terdaftar atau dikategorikan aman , sistem akan melakukan pemeriksaan terhadap isi dari *email*. Metode *keyword filtering* akan melakukan pemeriksaan *body* isi dari *email*, jika isi dari email mengandung kata-kata yang sudah di kunci oleh sistem, *email* akan langsung di blokir jika isi *email* positif atau tidak mengandung kata-kata yang negatif sistem akan melanjutkan pengiriman ke *inbox*.

b. Analisis DNS *Blacklisting*

Pada Gambar 4 adalah Alur kerja *Spam Filtering* hanya menggunakan metode DNS *Blacklisting*.

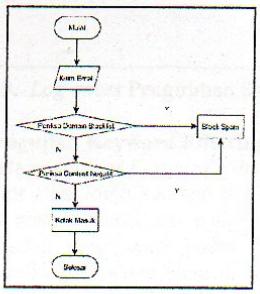


Gambar 4. Proses *DNS Blacklisting*

Dengan metode DNS *Blacklisting* email domain yang sudah di *blacklist* oleh sistem akan langsung di blokir, tetapi jika domain email *valid* atau tidak di*blacklist* oleh sistem akan langsung dikirim ke *inbox* pesan. Kinerja sistem ini hanya bekerja dengan cara mengenali domain *email* yang masuk . Jika ada isi dari pesan mengandung kata-kata yang dilarang dalam sebuah komunikasi tetap akan diteruskan ke *inbox* karena tidak adanya metode khusus untuk mengatasi hal tersebut.

3.2. Rancangan Flowchart Spam Filtering

Pada gambar 5 dibawah ini akan mengambarkan rancangan alur dari kerja sistem *spam filtering* yang menggunkan metode DNS *Blacklisting* dan *Keyword Filtering*.



Gambar 5. Flowchart *Spam Filtering*

Langkah Pertama melakukan pengiriman email, kemudian email akan di periksa di DNS *Blacklisting*. Jika domain terdaftar akan langsung di blokir oleh sistem, dan jika domain tidak terdaftar akan diteruskan ke pemeriksaan *body* isi pesan. pesan berisi kata-kata yang sudah di*keyword* akan langsung diblokir oleh sistem, dan apabila tidak, pesan akan diteruskan ke kotak masuk.

3.3. Simulasi Pengujian

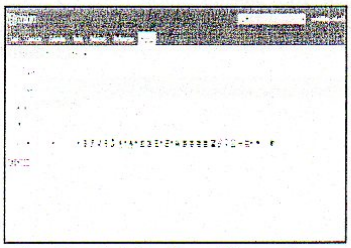
Selanjutnya akan dilakukan implementasi pengujian dan hasil dari uji coba pengiriman pesan antara satu *user* ke *user* yang lainnya.

3.3.1. Pengujian DNS *Blacklisting*

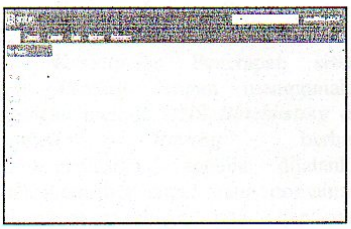
Pada pengujian DNS *Blacklisting* administrator akan *login* kedalam *web client* zimba untuk uji pengiriman pesan terhadap *user mail client* yang lainnya, ada dua email yang sudah didaftarkan kedalam *blacklist* yaitu, novialdi@student.umri.ac.id dan sudar@student.umri.ac.id.

Gambar 6. Halaman Login Web Client

Akun *email* novialdi@student.umri.ac. id akan mengirim pesan terhadap akun *email* permadi@student.umri.ac .id terlihat pada gambar 7 sebagai berikut:

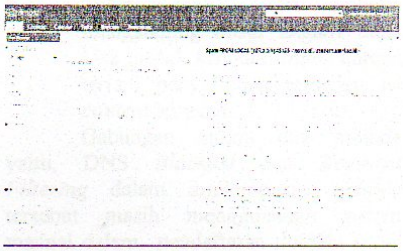


Gambar 7. Test Pengiriman Pesan



Gambar 8. Kotak Masuk Target *Spam*

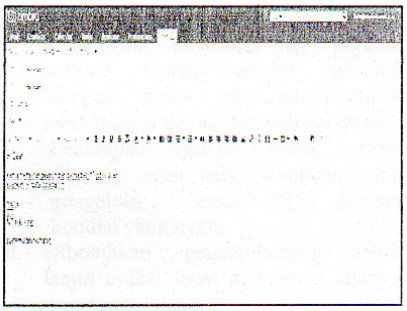
Dari hasil pengiriman yang terlihat pada gambar 8, pesan dari domain *email* yang sudah di *blacklist* pada sistem tidak sampai kedalam kotak masuk. *Log acces* spam yang masuk bisa dilihat pada gambar 9.



Gambar 9. *Log acces* Pengiriman Spam

3.3.2. Pengujian Keyword Filtering

Pada pengujian *Keyword Filtering* administrator akan *login* kembali kedalam *web client zimbra* untuk uji pengiriman pesan terhadap *user mail client* yang lainnya. Ada dua *keyword* yang di kunci dalam sistem yaitu , Hi Dear dan *System* Administrator . Uji kirim pesan terlihat pada gambar 10 sebagai berikut.



Gambar 10. Test Pengiriman Pesan

Pesan yang dikirim oleh akun *email* deka@student.umri.ac.id dengan tujuan akun ramadani@student.umri.ac.id berhasil di blokir oleh sistem, dikarenakan pesan yang dikirim mengandung kata-kata yang sudah di kunci oleh sistem. terlihat pada gambar 11 tidak ada pesan masuk terhadap akun *email* ramadani@student.umri.ac.id.

Gambar 11. Kotak Masuk Target

Dari hasil pengiriman yang terlihat pada gambar 11, pesan dari domain email yang sudah di *blacklist* pada sistem tidak sampai kedalam kotak masuk. *Log acces* spam yang masuk bisa dilihat pada gambar 12.

Gambar 12. *Log acces* Pengiriman Spam

4. Kesimpulan dan Saran

4.1. Kesimpulan

Kesimpulan Penerapan sistem *spam filtering* dengan menggunakan Gabungan metode DNS *Blacklisting* dan *Keyword Filtering* berhasil diimplementasikan apabila dijalankan untuk memfilter email yang domainnya telah terdaftar sebagai *spam* dan *email* yang mengandung kata-kata suku, agama, ras, dan antargolongan (SARA) atau yang bertentangan dengan peraturan berkomunikasi. Pengujian penerapan sistem *spam filtering* dengan menggunakan metode DNS *Blacklisting* dan *Keyword Filtering* memberikan hasil, antara lain :

a. *User* yang telah melakukan pengiriman menggunakan *email* palsu, tidak berlaku lagi karena adanya pengecekan terhadap domain.
b. Spam yang berisi *content* mengandung unsur negatif tidak bisa masuk kedalam *inbox* karena terjadi penyaringan terhadap isi *conten*t tersebut.

Gabungan antara dua metode yaitu, DNS *Blacklist* dan *Keyword Filtering* dalam implementasi metode tersebut masih menggunakan sistem manual dalam pendaftaran domain *spam* dan mengunci kata-kata pesan yang akan di *filter* serta, pengimplementasian masih menggunakan *localhost* (jaringan local).

4.2. SARAN

a. Pengembangan sistem untuk *spam filtering* dengan menggunakan metode DNS *Blacklis*t haruslah mempunyai *database* DNS yang dapat didaftarkan pada organisasi pengelola DNS di internet seperti USENET.
b. Penerapan sistem untuk *spam filtering* lebih baik ditambah lagi dengan metode pengelompokan terhadap kategori *spam*, agar administrator lebih mudah dalam menyeleksi *spam.*
c. Penerapan sistem untuk *spam filtering* lebih baik dilakukan pada pengelola *email* (ISP) dengan kondisi yang nyata.
d. Dibutuhkan pengembangan lebih lanjut untuk dapat mengenali adanya *email spam* dan *ham.*

5. Daftar Pustaka

B, Alfred., B, Nadine., B, Mary. 2014. *Computer Security and Penetration Testing*. 200 First Stamford Place, 4th Floor Stamford, CT 06902 USA.

Blacklists Compared. *DNS Blacklist (DNSBL)*. weekly reports since July 2001. http://www.ebooklibrary.org/articles/DNSBL. Diakses pada tanggal 20 Januari 2016.

D, Shinder. 2004. *Aplication Layer Filtering (ALF) What is it and How does it Fit into your Security Plan?*. WindowSecurity.com. Diakses pada tanggal 01 Februari 2016.

Ebook. 2014. *Zimbra Collaboration Administrator Guide*. Zimbra, Inc. 3000 Internet Blvd., Suite 200 Frisco, Texas 75034

Iskandar. 2009. *Panduan Lengkap Internet* . Yogyakarta: Andi OFFSET.

R, Rafiudin. 2008. *Membangun Server E-Mail Berbasis FreeBSD/Linux*. Yogyakarta : Andi OFFSET

S, Anjik & Rianto. 2008. *Jaringan Komputer*. Yogyakarta : Andi OFFSET.

T, Panji. 2008. *Email Spam Filtering*.. http://panjitapen.wordpress.com/2008/01/27/ email-spamfiltering. Diakses pada tanggal 12 Januari 2016.

Wahana Komputer. 2009. Langkah *Mudah Administrasi Jaringan Menggunakan Linux Ubuntu* . Yogyakarta : Andi OFFSET.

Wahana Komputer. 2009. *Mudah Basmi Virus Spam dan Malware dengan Free Antivirus Online*.Yogyakarta : Andi OFFSET

World Heritage Encyclopedia ™. 2002. *Email Spoofing*. http://www.ebooklibrary.org/articles/email_spoofing. Diakses pada tanggal 20 Januari 2016.