

ANALISA DAN IMPLEMENTASI SECURITY MAIL SERVER

Daniel Adi Putra Sitorus¹⁾, Harun Mukhtar²⁾, Yulia Fatma³⁾

¹Fakultas Ilmu Komputer, Universitas Muhammadiyah Riau
email: danieladiputra@student.umri.ac.id

²Fakultas Ilmu Komputer, Universitas Muhammadiyah Riau
email: harunmukhtar@umri.ac.id

³Fakultas Ilmu Komputer, Universitas Muhammadiyah Riau
email: yuliafatma@umri.ac.id

Abstract

Mail server is one of the most widely used server functions in the company. This discusses e-mail itself which can reduce mailing costs, is more efficient than manual communication and can be used as attachments that are useful as a supplement and additional documents related to the contents of e-mail. Zimbra is a mail server application that provides complete features and also makes it easy to install mail server management, also mail server security issues are a factor that must be considered by the system administrator. The security design for e-mail servers addresses the importance of being able to prevent spam e-mail attacks that can fill e-mail servers and make mail server performance faster. Because a good mail server security can optimize the performance of the mail server itself. In this final project, the work and implementation of the zimbra mail server security will be carried out specifically for handling email spam. The zimbra email server will analyze its security against spam email attacks, so that it can function as an email server on the company.

Keywords: Security, Mail Server, Zimbra, Spam

Abstrak

Mail server merupakan salah satu fungsi server yang paling banyak digunakan di perusahaan. Hal ini mengingat fungsi email sendiri yang bisa mengurangi biaya surat-menyurat, lebih efisien dibandingkan komunikasi manual dan dapat menyertakan attachment yang berguna sebagai pelengkap dan dokumen tambahan terkait dengan isi email. Zimbra merupakan aplikasi mail server berlisensi bebas dimana memiliki fitur-fitur yang lengkap dan juga kemudahan untuk instalasi maupun management mail server, meskipun masalah keamanan mail server menjadi faktor yang utama yang harus diperhatikan oleh system administrator. Perancangan keamanan untuk mail server sangatlah penting dimana dapat mencegah serangan email spam yang dapat memenuhi mail server dan membuat performa mail server menjadi lambat. Karena keamanan mail server yang baik dapat mengoptimalkan kinerja dari mail server itu sendiri. Pada tugas akhir ini akan dilakukan analisa dan implementasi security mail server zimbra khususnya penanganan email spam. Mail server zimbra akan di analisa segi keamanannya terhadap serangan email spam, agar dapat difungsikan sebagai mail server pada perusahaan.
Kata kunci: Security, Mail Server, Zimbra.

Keywords: Security, Mail Server, Zimbra, Spam.

PENDAHULUAN

Email adalah salah satu media komunikasi yang penting pada perkembangan teknologi saat ini. Penyedia layanan email atau yang

sering disebut dengan mail server menjadi suatu aplikasi penting pada sebuah perusahaan atau instansi lainnya. Hal ini mengingat fungsi email sendiri yang bisa mengurangi biaya surat-menyurat, lebih efisien dibandingkan

komunikasi manual dan dapat menyertakan attachment yang berguna sebagai pelengkap dan dokumen tambahan terkait dengan isi email (Mangunkusumo, 2013).

Membangun jaringan mail server sekarang ini tidaklah cukup dengan hanya menginstall dan menjalankannya saja, tapi ada beberapa proses yang dikerjakan agar mail server yang dibuat dapat aman dan berjalan dengan lancar. Serangan-serangan tersebut datang justru ketika setelah mail server itu aktif dan mulai melakukan tugasnya mengirim dan menerima email. Saat itulah berbagai kendala muncul seperti banyak spam, banyak virus, blacklist ip, kegagalan pengiriman ke email tujuan, masuk ke junk/spam folder, terkena Ddos (distributed denial-of-service) attack, dan performa mail server lambat (Vavai, 2016).

Email spam merupakan email yang tidak diinginkan pengguna untuk masuk ke dalam Mailbox nya dan bisa terjadi sewaktu-waktu. Saat ini banyak sekali email spam yang bermunculan baik untuk hanya sekedar melakukan promosi ataupun yang bertujuan untuk melakukan kejahatan. Bahkan ditahun 2012 lebih dari 50% Email dari total Email adalah Spam Email (Shrivastava, J. N., & Bindu, M. H, 2014).

PT. Vadhana International merupakan sebuah perusahaan penyedia jasa konstruksi yang menggunakan aplikasi Zimbra Mail Server sebagai Mail Transfer Agent. Permasalahan yang timbul pada penggunaan Email ini adalah sering nya terjadi masuknya email spam kedalam Mail Server Perusahaan. Bahkan jika terlalu banyak akun yang terkena Spam, maka Server Perusahaan juga dapat terkena Blacklist. Hal ini menjadi dasar penulis untuk melakukan Penelitian Analisa Dan Implementasi Security Mail Server.

Security mail server menjadi hal yang di prioritaskan dalam penelitian ini. Oleh sebab itu peneliti hanya fokus

terhadap keamanan Firewall pada Sistem Operasi dan Keamanan Mail Transfer Agent yang digunakan. Mail Transfer Agent yang digunakan adalah Mail Server Zimbra. Mail Server Zimbra ini akan diuji keamanannya untuk mengetahui apakah implementasi keamanan Mail Server yang dimaksud berjalan dengan baik dan aman.

Mail server (juga dikenal sebagai sebuah mail transfer agent atau MTA, mail router atau mailer Internet) adalah sebuah aplikasi yang akan menerima email masuk dari pengguna lokal (orang-orang dalam satu domain) dan jarak jauh pengirim dan meneruskan email keluar untuk pengiriman. Sebuah komputer yang didedikasikan untuk menjalankan aplikasi tersebut juga disebut sebagai mail server. Microsoft Exchange, qmail, Exim dan sendmail adalah lebih umum di antara program-program server mail (Danphi, 2008).

Security Mail Server merupakan bagian penting dari Mail Server karena Security Mail Server dibutuhkan untuk mencegah serangan-serangan dari cracker seperti port scanning, brute force, virus dan spam. Serangan-serangan tersebut datang ketika mail server aktif dan mulai melakukan tugasnya mengirim dan menerima email. Saat itulah berbagai kendala mulai muncul antara lain dalam bentuk banyak spam, banyak virus, blacklist ip, kegagalan pengiriman email ke tujuan, masuk ke junk/spam folder, terkena Ddos (distributed denial-of-service) attack, dan performail mail server menjadi lambat (Vavai Sugianto, 2016).

Zimbra Collaboration Suite adalah kolaborasi dari beberapa aplikasi open source software, diantaranya Apache Jetty, Postfix, OpenLDAP, dan MySQL. Kolaborasi ini menghasilkan email server yang power full dengan fitur-fitur yang lengkap (I.E.S.W. Mangunkusumo, 2013).

Spam adalah email yang tidak diinginkan oleh pengguna fasilitas computer dalam bentuk surat elektronik (email), instant messaging, usenet, newsgroup, blog dan lainnya (Febri Ramadhani Kusmayadi, 2017).

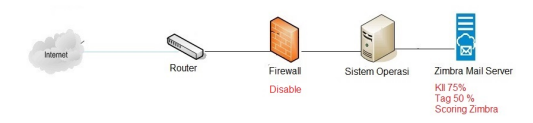
METODE PENELITIAN

1. Analisis

Tahap analisis dilakukan pengumpulan data dan Analisa pada sistem yang berjalan. Pengumpulan data melibatkan proses yang eleven terhadap penelitian mencakup aktivitas pengumpulan Buku, Jurnal dan data observasi pada tempat penelitian.

Analisis sistem yang berjalan merupakan gambaran tentang Sistem yang saat ini sedang berjalan, yaitu Sistem Mail Server dengan menggunakan Sistem Operasi Linux Centos Ver 7.5 dan Mail Transfer Agent Zimbra Mail Server Ver 8.8.10. Kondisi yang terjadi pada sistem yang sedang berjalan adalah kondisi Firewall yang dinonaktifkan dan kondisi Scoring Zimbra yang rendah.

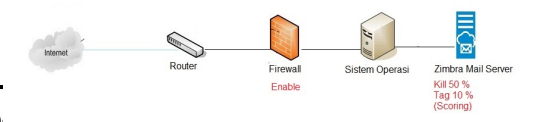
Alasan Firewall dibuat dalam keadaan terdisable adalah karena fungsi Monitoring pada Zimbra Mail Server bisa berjalan jika Firewall Sistem Operasi dalam keadaan didisable. Alasan diubahnya Spam Scoring adalah agar Email dari mana saja mudah masuk ke dalam Mail Server. Jika Spam Scoring nya rendah maka Email dari mana saja akan mudah masuk karna pengecekan pada Email masuk akan di perlonggar.



Gambar 1: Analisis pada Sistem yang sedang berjalan

2. Design Penelitian

Dalam design penelitian digambarkan bahwa akan dilakukan pengaktifan fungsi firewall pada sistem operasi dan

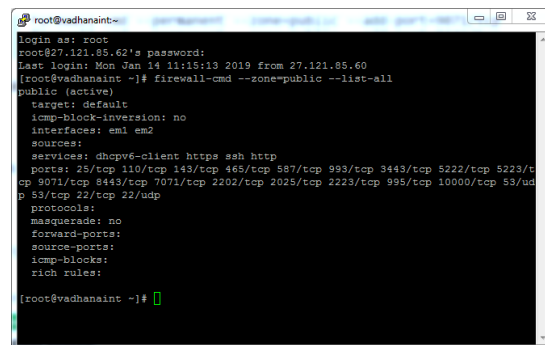


Gambar 2: Desain Sistem

peningkatan spam scoring pada aplikasi zimbra mail server.

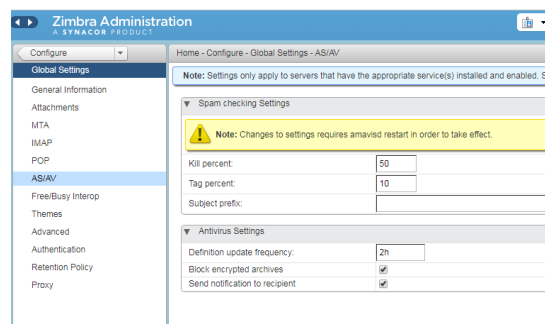
3. Implementasi Dan Ujicoba

Pertama, hal yang diperlukan adalah pengaktifan fungsi firewall sistem operasi



Gambar 3: Konfigurasi Firewoall

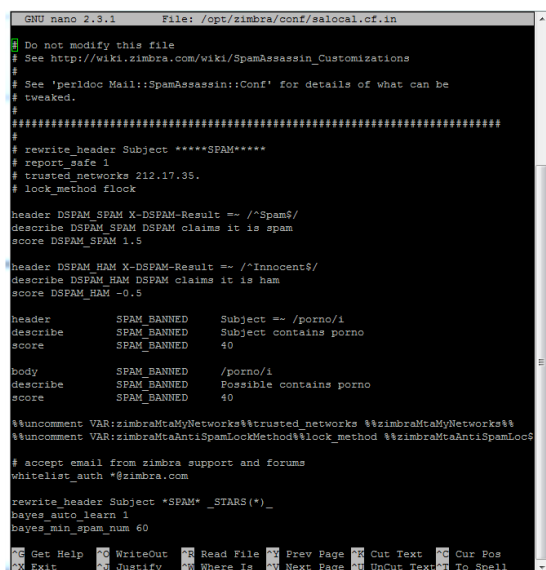
dan menjalankan fungsi firewall untuk membatasi port yang di ijinakan untuk digunakan pada mail server.



Gambar 4: Spam Scoring Zimbra Mail Server

Kedua, adalah meningkatkan spam scoring dengan cara menurunkan nilai as/av pada zimbra mail server.

Ketiga, adalah dengan melakukan penambahan kata-kata yang mengandung unsur spam pada file /opt/zimbra/conf/salocal.cf.in. Tujuan dilakukannya hal ini adalah untuk memastikan kata-kata tidak pantas dapat diberi scoring yang tinggi sehingga pesan tersebut dianggap spam.



```
GNU nano 2.3.1 File: /opt/zimbra/conf/salocal.cf.in
# Do not modify this file
# See http://wiki.zimbra.com/wiki/SpamAssassin_Customizations
# See 'perldoc Mail::SpamAssassin::Conf' for details of what can be
# tweaked.
#####
#
# rewrite header Subject *****SPAM*****
# report_safe 1
# trusted_networks 212.17.35.
# lock_method flock

header DSPAM_SPAM X-DSPAM-Result =~ /"Spam"/
describe DSPAM_SPAM DSPAM claims it is spam
score DSPAM_SPAM 1.5

header DSPAM_HAM X-DSPAM-Result =~ /"Innocent"/
describe DSPAM_HAM DSPAM claims it is ham
score DSPAM_HAM -0.5

header SPAM_BANNED Subject =~ /porno/i
describe SPAM_BANNED Subject contains porno
score SPAM_BANNED 40

body SPAM_BANNED /porno/i
describe SPAM_BANNED Possible contains porno
score SPAM_BANNED 40

%uncomment VAR:zimbraMtaMyNetworks%trusted_networks %zimbraMtaMyNetworks%
%uncomment VAR:zimbraMtaAntiSpamLockMethod%lock_method %zimbraMtaAntiSpamLockMethod%

# accept email from zimbra support and forums
whitelist_auth *@zimbra.com

rewrite header Subject *SPAM* _STARS(*)_
bayses_auto_learn 1
bayses_min_spam_num 60

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^N Next Page ^U UnCut Text ^T To Spell
```

Gambar 5: File Script
opt/zimbra/conf.salocal.conf.in

Keempat, adalah memastikan fungsi service pada zimbra dapat berjalan dengan baik. Nanti nya dalam pengujian akan dilakukan kondisi pengujian terhadap kondisi antivirus beserta antispam tidak aktif dan aktif.

4. Evaluasi

Pada fase evaluasi akan dilakukan pengambilan data untuk dijadikan output hasil penelitian. Hasil penelitian ini kemudian juga akan dijadikan acuan untuk membuat sebuah kesimpulan penelitian dan saran untuk penelitian selanjutnya.

HASIL DAN PEMBAHASAN

A. Pengujian

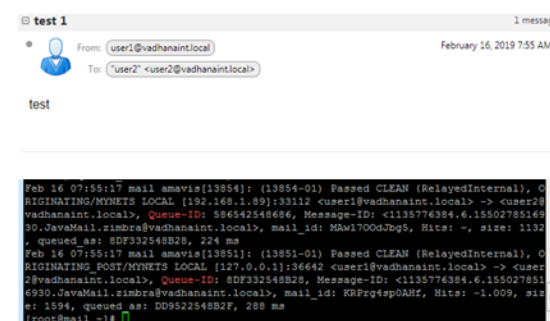
Pada pengujian ini dilakukan dengan 3 jenis metode pengujian dan pada masing-masing pengujian dilakukan kondisi Antispam beserta Antivirus tidak

aktif dan aktif. Berikut adalah 3 jenis metode pengujian yang dilakukan:

1. Pengujian Email Normal
2. Pengujian Judul Email Spam
3. Pengujian Lampiran Bervirus

1. Pengujian Pertama

Gambar 6 merupakan pengujian email standar ketika antivirus dan anti spam tidak aktif, terlihat pesan dari user1@vadhanaint.local menuju

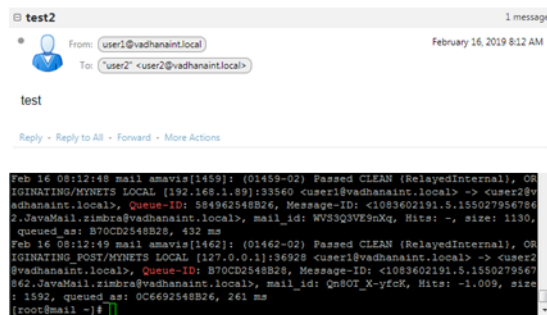


Gambar 6: Pengujian Email Normal
Ketika Antivirus dan Antispam Tidak Aktif

user2@vadhanaint.local berhasil dikirim dengan durasi waktu pengiriman selama 0.28 detik dan dengan score email - 1.0009. Artinya bahwa pesan ini berhasil dikirim dan bebas bukan pesan spam.

2. Pengujian Kedua

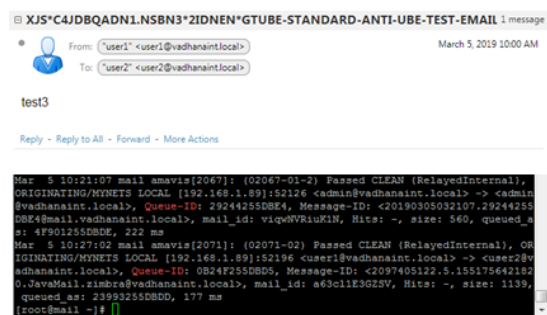
Gambar 7 merupakan pengujian email standar ketika antivirus dan anti spam aktif, terlihat pesan dari user1@vadhanaint.local menuju user2@vadhanaint.local berhasil dikirim dengan durasi waktu pengiriman selama 0.261 detik dan dengan score email - 1.0009. Artinya bahwa pesan ini berhasil dikirim dan bebas bukan pesan spam. Maka tidak ada perbedaan pada pengujian pertama jika melakukan ujicoba pengiriman email standar.



Gambar 7: Pengujian Email Normal Ketika Antivirus dan Antispam Aktif

3. Pengujian Ketiga

Gambar 8 merupakan pengujian judul email spam ketika antivirus dan anti spam tidak aktif, terlihat pesan spam dari user1@vadhanaint.local menuju user2@vadhanaint.local berhasil dikirim dengan durasi waktu pengiriman selama 0.177 detik dan dengan score email -1. Artinya bahwa pesan ini berhasil dikirim dan bukan pesan spam.

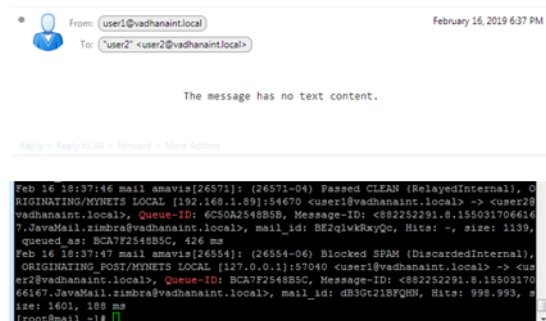


Gambar 8: Pengujian Judul Email Spam Ketika Antivirus dan Antispam Tidak Aktif

4. Pengujian Keempat

Gambar 9 merupakan pengujian judul email spam ketika antivirus dan anti spam aktif, terlihat pesan dari user1@vadhanaint.local menuju user2@vadhanaint.local gagal dikirim dengan durasi waktu proses pengiriman selama 0.188 detik dan dengan score email 998.993. Terlihat bahwa email tersebut terblokir karena mengandung unsur spam dengan score email yang sangat tinggi sehingga Antispam dan Antivirus secara otomatis akan memblokir

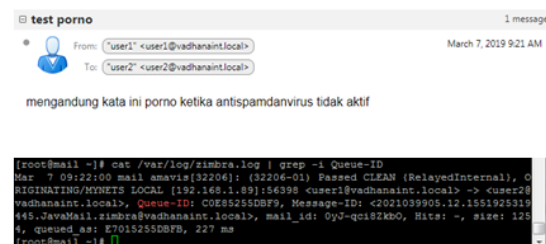
email tersebut. Maka terdapat perbedaan pada pengujian sebelumnya jika melakukan ujicoba pengiriman email spam.



Gambar 9: Pengujian Judul Email Spam Ketika Antivirus dan Antispam Aktif

5. Pengujian Kelima

Gambar 10 adalah pengujian pengiriman email dengan judul pesan yang sudah dimasukkan ke dalam daftar spam yaitu judul yang mengandung kata "porno" ketika Antivirus dan Antispam tidak aktif, terlihat pesan spam dari user1@vadhanaint.local menuju user2@vadhanaint.local berhasil dikirim dengan durasi waktu pengiriman selama 0.277 detik dan dengan score email -. Artinya bahwa pesan ini berhasil dikirim dan bukan pesan spam.

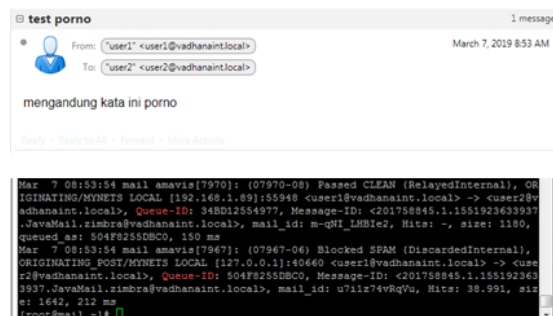


Gambar 10: Pengujian Judul Email Spam Ketika Antivirus dan Antispam Tidak Aktif

6. Pengujian Keenam

Gambar 11 adalah pengujian pengiriman email dengan judul pesan yang sudah dimasukkan ke dalam daftar spam yaitu judul yang mengandung kata "porno" ketika Antivirus dan Antispam aktif, terlihat pesan dari user1@vadhanaint.local menuju

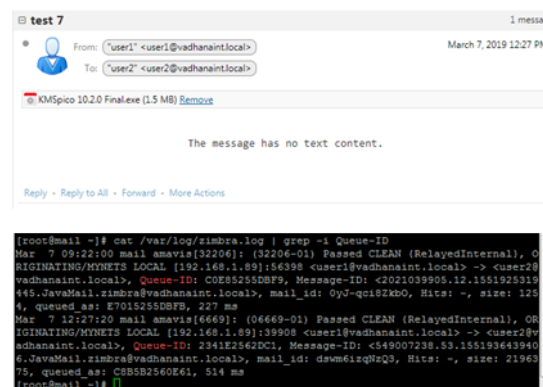
user2@vadhanaint.local gagal dikirim dengan dursai waktu proses pengiriman selama 0.212 detik dan dengan score email 38.99. Terlihat bahwa email tersebut terblokir karna mengandung unsur spam dengan score email yang tinggi sehingga Antispam dan Antivirus secara otomatis akan memblokir email tersebut. Terlihat juga bahwa score email tersebut masih sesuai pada kisaran hits yang telah diinput sebelumnya pada file opt/zimbra/conf/salocal.cf.in . Maka terdapat perbedaan pada pengujian sebelumnya jika melakukan ujicoba pengiriman judul email spam.



Gambar 11: Pengujian Judul Email Spam Ketika Antivirus dan Antispam Aktif

7. Pengujian Ketujuh

Gambar 12 adalah pengujian pengiriman email yang melampirkan file spam ketika Antivirus dan Antispam tidak dijalankan, terlihat pesan spam dari user1@vadhanaint.local menuju user2@vadhanaint.local berhasil dikirim dengan durasi waktu pengiriman selama 0.514 detik dan dengan score email -. Artinya bahwa pesan ini berhasil dikirim dan bukan pesan spam.



Gambar 12: Pengujian Pengiriman Lampiran Spam Ketika Antivirus dan Antispam Tidak Aktif

8. Pengujian Kedelapan

Untuk pengujian pengiriman email yang melampirkan file spam ketika Antivirus dan Antispam dijalankan, terlihat pesan dari user1@vadhanaint.local menuju user2@vadhanaint.local gagal dikirim dengan durasi waktu pengiriman selama 12.365 detik dan dengan score email -. Terlihat bahwa email tersebut terblokir karna mengandung unsur spam dengan score email yang sangat tinggi sehingga Antispam dan Antivirus secara otomatis akan memblokir email tersebut. Artinya bahwa pesan ini berhasil dikirim dan bukan pesan spam. Maka terdapat perbedaan pada pengujian sebelumnya jika melakukan ujicoba pengiriman lampiran yang mengandung virus.

B. Data Hasil Pengujian

Berikut merupakan data terhadap hasil pengujian yang telah dilakukan. Data tabel terhadap hasil masing-masing pengujian adalah:

Pengu jian	Jenis pengu jian	Kond isi Antis pam dan Antiv irus	Stat us pesa n terki rim	Durasi waktu pengiri man	Hit s
1	Pengu jian	Tidak Aktif	Terki rim	288 ms	- 1.0

	us				
--	----	--	--	--	--

1. Nilai Antispam dan Antivirus (AS/AV) yang dibuat rendah dan Dinonaktifkannya Antispam dan Antivirus (AS/AV) menjadi penyebab masuknya Email Spam kedalam Mail Server.
2. Melalui peningkatan Spam Scoring dengan cara menurunkan Kill 50 % dan Tag 10 % dan mengaktifkan fungsi Antispam maka dapat mencegah masuknya Email Spam ke dalam Mail Server.
3. Melalui pengukuran skor hits maka dapat ditentukan sebuah email apakah mengandung unsur spam/ tidak.

Dumka, A., Tomar, R., Patni, J. C., & Assistant, A. A. (2007). Taxonomy of E-Mail Security Protocol. International Journal of Innovative Research in Computer and Communication Engineering (An ISO Certified Organization), 3297(4). Retrieved from www.ijirce.com

Kumar, S., & Raj V.P, J. (2012). A Secure Email System Based on IBE, DNS and Proxy Service. Journal of Emerging Trends in Computing and Information Sciences, 3(9), 1271–1276.

Mangunkusumo, I. E. S. ., Lumenta, A., Wowor, H., & Sinsuw, A. (2013). Analisa dan Perancangan Keamanan Mail Server Zimbra pada Sistem Operasi Ubuntu. E-Jornal Teknik Elektro Dan Komputer, 1–9. <https://doi.org/1. I. E. S. W. Mangunkusumo 2. A. Lumenta 3. H. Wowor 4. A. Sinsuw>

Of, I., Filter, S., Mail, F. O. R., Using, S., & Spamassassin, T. (2017). Implementasi Spam Filter Untuk Mail Server Menggunakan Tools Spamassassin Implementation of Spam Filter for Mail Server Using Tools Spamassassin, 3(3), 1925–1933.

Rohini, P., Ramya, K., Student, # M E, & Professor, A. (2014). Phishing Email Filtering Techniques A Survey. International Journal of Computer Trends and Technology, 17(1). Retrieved from <http://www.ijcttjournal.org>

Shrivastava, J. N., & Bindu, M. H. (2014). E-mail Spam Filtering Using Adaptive Genetic Algorithm.

International Journal of Intelligent Systems and Applications, 6(2), 54–60.

<https://doi.org/10.5815/ijisa.2014.02.07>

Vavai, 2016, (Membangun Anti Spam Appliance & Improvement Performa Mail Server), PT.Excellent Infotama Kreasindo Bekasi.