ANALISA PENERAPAN *DMARC* YANG DIINTEGRASIKAN DENGAN *ANTI SPAM* DAN *ANTI VIRUS* UNTUK PENGAMANAN *MAIL SERVER*

SINOPSIS

Oleh:
RUDI KURNIAWAN
1710510157

ROGRAM STUDI ILMUKOMPUTER
FAKULTAS TEKNIK DAN KESEHATAN
UNIVERSITAS BUMIGORA
MATARAM
2020

BAB I
PENDAHULUAN

1. Latar Belakang

Surat elektronik adalah salah satu dari kemajuan teknologi dalam bidang komunikasi sehingga fungsi dari surat dapat digantikan dengan adanya surat elektronik, efisiensi biaya dan waktu menjadi alasan yang membuat banyak orang beralih dari surat menuju surat elektronik (*email)* terdapat ancaman serius mengiringi kemudahan yang diberikan oleh email dengan memanfaatkan email sebagai media untuk melakukan tindak kejahatan di dunia siber, karena email merupakan alat transportasi utama bagi spam, virus dan malware dalam jaringan.

Mengingat betapa pentingnya media komonikasi di zaman sekarang ini maka beberapa orang melakukan penelitian terutama di bidang keamanan jaringan. Naufal Hanif 2018, penerapan protokol DomainKeys Identified Mail dapat mencegah email spoofing dengan cara melakukan otentikasi menggunakan metode pencocokan private key dan public key (Asymmetric keys). Sedangkan penerapan protokol Sender Policy Framework dapat mencegah email spoofing dengan cara melakukan otorisasi menggunakan metode pencocokan alamat IP server pengirim. Hasil atau keluaran yang dicapai yaitu mail server dapat terhindar dari email spam, email spoofing, dan virus untuk memastikan keamanan dan kenyamanan pengguna email serta menghindari dampak kerugian yang dapat ditimbulkan oleh email spam, email spoofing, dan virus.. Andrian Maftuh Nadzifan, Farih Nazihullah 2018, pendeteksi spoofing pada email menggunakan penerapan DKIM, SPF dan DMARC yang pada penelitian di gunakan Sebuah metode untuk melakukan deteksi diperlukan untuk melihat apakah sebuah email terindikasikan sebagai spoof atau tidak. Naufal Herdyputra Ardhi, 2020, Forensik email dengan metode Header Analysis dianggap efektif untuk melacak alamat IP pengirim email, namun hal ini tidak dapat melacak posisi pengirim email secara akurat. Mengintegrasikan email forensik klasik dengan data mining

dari Twitter data stream telah terbukti efektif untuk mendapatkan informasi geografis dan memeperkecil luas dari seluas kota menjadi seluas lingkungan, yang sangat berharga bagi pihak berwajib dalam menghemat waktu dan juga usaha untuk mengadili pelaku tindak kejahatan cyber.

Dari kutipan di atas ada beberapa kekurangan seperti DKIM memiliki masalah yang tidak dapat menentukan apakah tanda tangan itu sah, Naoya Kitagawa, Toshiki Tanaka, Masami Fukuyama and Nariyoshi Yamai 2016**.** Pertimbangan ini lah yang membuat penulis untuk menerapkan *Protocol DMARC* yang berfungsi untuk mendeteksi email palsu dan memberi tahu pengguna tanpa DKIM tanda tangan dengan memanfaatkan DMARC dan menerapkan sistem itu mengirimkan hasil verifikasi DMARC ke penerima*, Baracuda Central* sebagai tools anti spam dan spoofing yang dapat melakukan otorisasi bukan hanya melalui alamat IP saja namu juga dapat melalui URL dan antivirus *ClamAV* untuk mengatasi *virus* yang sangat tidak diinginkan oleh pengguna maupun penyedia layanan *email*. Sistem pencegahan *email spam, spoofing,* dan *virus* diharapkan dapat mengurangi dampak kerugian yang diakibatkan oleh *email spam, spoofing,* dan *virus.*

DMARC (Domain-based Message Authentication, Reporting and Conformance), dan BARACUDA CENTRAL dapat digunakan sebagai otentikasi dan otorisasi email sehingga email client akan terbebas dari tindakan spoofing. Penerapan Anti Spam dan Anti Virus ClamAV juga diperlukan agar email server terhindar dari email spam dan virus, metode yang diterapkan oleh Anti Spam dan Anti Virus ClamAV yaitu dengan melakukan pengecekan haeder, body, dan attachment email kemudian di sampaikan ke pengguna.

Manfaat dari penerapan DMARC, BARACUDA CENTRAL, Anti Spam dan Anti Virus ClamAV adalah untuk mengoptimalkan system keamanan jaringan server mail, dengan cara memblokir surat elektronik yang dianggap sebagai spam atau virus, meningkatkan kualitas

keamanan surat elektronik sehingga pengguna dapat terhindar dari aktifitas spoofing dan virus yang disisipkan melalui surat elektronik.

2. Rumusan masalah

Sesuai dari latar belakang yang telah dipaparkan di atas maka rumusan masalah yang akan dikaji adalah bagaimana menganalisa penerapan DMARC (Domain-based Message Authentication, Reporting and Conformance), *BARACUDA CENTRAL Anti Spam*, dan *Anti Virus ClamAV* pada mail server agar mail server dapat terhindar dari email spam, virus dan pengguna email dapat terhindar dari aktifitas spoofing.

3. Batasan masalah

a. Rancangan uji coba diimplementasikan menggunakan VPS yang disewa pada penyedia layanan VPS. Pada VPS akan dilakukan instalasi CentOS Web Panel, konfigurasi DNS server, konfigurasi Mail server, dan komputer client digunakan untuk mengakses Mail User Agent berbasis web (Zimbra).
b. Sistem operasi VPS yang digunakan adalah CentOS 7.3.1611.
c. Aplikasi yang digunakan untuk memudahkan instalasi dan konfigurasi server adalah CentOS Web Panel.
d. Aplikasi MTA yang digunakan adalah Postfix untuk mengirim email.
e. Aplikasi MDA yang digunakan adalah Dovecot untuk menerima email.
f. Aplikasi MUA yang digunakan adalah Roundcube sebagai aplikasi email di sisi pengguna.
g. Aplikasi DNS server yang digunakan adalah bind9 agar email server dapat diakses menggunakan nama domain
h. Aplikasi HTTP server yang digunakan adalah Apache agar Mail Transfer Agent berbasis web dapat diakses melalui browser.
i. Pengujian yang dilakukan dengan mengirim surat elektronik yang terindikasi sebagai spam, kemudian melakukan pengiriman email spoofing, dan email yang mengandung virus, serta mengecek header email sebelum dan setelah penerapan DMARC, BARACUDA CENTRAL, anti spam, dan anti virus.
j. Pengujian DMARC dan BARACUDA CENTRAL dilakukan dengan cara mengirim email spoofing menggunakan Emkei’s Fake Mailer kemudian email spoofing tersebut dikirim ke Gmail dan Yahoo! Mail.

k. Pengujian Anti Spam dan Anti Virus dilakukan dengan cara mengirim email spam dan email yang mengandung virus ke mail server

4. Tujuan dan manfaat

a. Tujuan

Pengujian *Anti Spam* dan *Anti Virus* dilakukan dengan cara mengirim *email spam* dan *email* yang mengandung *virus* ke *mail server.*

b. Manfaat

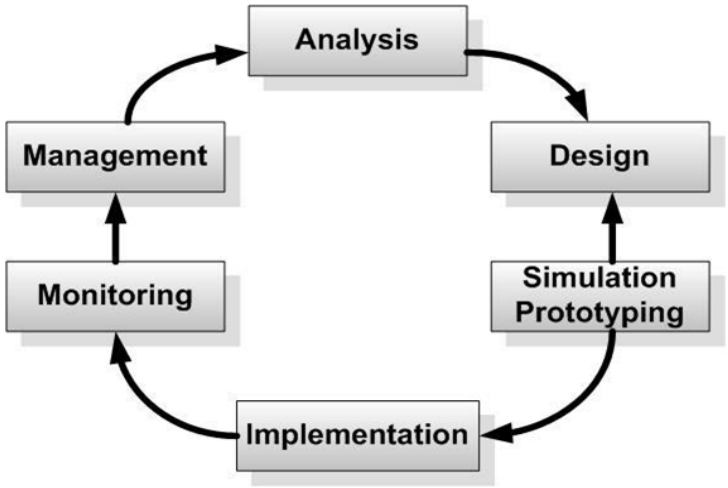
Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Bagi Diri Sendiri
   a. Dapat pengetahuan baru yang dapat di terapkan di dunia kerja.
   b. Dapat menjadi tempat untuk mengimplementasikan ilmu pengetahuan yang telah didapat selama berada dibangku perkuliahan.
   c. Sebagai syarat untuk menyelesaikan jenjang Pendidikan Strata 1 (S1) pada program studi Ilmu Komputer di Universitas Bumigora Mataram.
2. Bagi Keilmuan
   a. Dapat menjadi bahan rujukan untuk pengembangan penelitian berikutnya terutama dalam bidang yang sama.
   b. Dapat menjadi sarana untuk melatih kemampuan dalam menulis karya ilmiah
3. Bagi Masyarakat
   a. Dapat memberikan pengetahuan terkait dengan analisa penanganan *email spam, virus* dan aktifitas *spoofing* menggunakan *Protocol DMARC*, *Baracuda Centra*, *Anti Spam,* dan *Anti Virus*.
   b. Dapat memberikan solusi penerapan *Protocol DMARC, Baracuda Central, Anti Spam*, dan *Anti Virus* pada mail server.

5. Metodologi

Metodologi penelitian yang digunakan dalam penelitian ini adalah Network Development Life Cycle (NDLC) yang menjadi model kunci

dibalik proses perancangan jaringan komputer. NDLC sendiri merupakan siklus proses yang berupa fase atau tahapan dari mekanisme yang dibutuhkan dalam suatu rancangan proses pembangunan atau pengembangan suatu sistem jaringan komputer.



Dari keenam fase yang terdapat pada NDLC, penulis hanya menggunakan lima fase antara lain sebagai berikut:

1. Analysis

   Pada fase ini penulis melakukan pengumpulan data dengan cara studi literatur, yaitu penulis membaca artikel ilmiah, buku, dan jurnal untuk mendapatkan informasi mengenai DMARC, BARACUDA CENTRAL, Anti Spam, dan Anti Virus. Data-data yang telah terkumpul kemudian dianalisa.

2. Design

   Pada fase ini penulis membuat rancangan yang meliputi rancangan jaringan uji coba, rancangan pengalamatan IP, rancangan sistem filtering, otentikasi, dan otorisasi email menggunakan DMARC, BARACUDA CENTRAL, Anti Spam, dan Anti Virus, serta kebutuhan perangkat keras dan perangkat lunak.

3. Simulation Prototyping

Setelah melakukan analisa dan desain, tahap berikutnya adalah melakukan simulasi dan membuat prototype berdasarkan pada desain yang telah dirancang sebelumnya (Nurfajar, Kurniawan, dan Yunan, 2015). Pada fase ini dilakukan instalasi dan konfigurasi serta uji coba DMARC, BARACUDA CENTRAL Anti Spam, dan Anti Virus menggunakan berbagai macam scenario.

6. Perbandingan dengan Skripsi/ TA Sebelumnya

No	Penulis	Tahun	Judul	Pembahasan	Perbedaan
1	Naufal Hanif	2018	Analisa Penerapan *Domainkeys Identified Mail* (*Dkim*), *Sender Policy Framework* (*Spf*), *Anti Spam*, Dan *Anti Virus* Pada *Mail Server*	penerapan protokol *DomainKeys Identified Mail* dapat mencegah *email spoofing* dengan cara melakukan otentikasi menggunakan metode pencocokan *private key* dan *public key* (*Asymmetric keys)*. Sedangkan penerapan protokol *Sender Policy Framework*	Peerbedaan antara skripsi yang penulis angkat dengan skripsi ini adalah pada skripsi penulis melakukan analisis dengan menerapkan protocol yang berbeda dari skripsi sebelumnya, yaitu dengan protocol

				dapat mencegah *email spoofing* dengan cara melakukan otorisasi menggunakan metode pencocokan alamat *IP server* pengirim. Sebaliknya penerapan *SpamAssassin*, *ClamAV*, dan *Amavisd-New* dapat mencegah masuknya *email spam* dan *virus* dengan cara melakukan pengecekan *header*, *body*, dan *attachment email*.	DMARC dan anti spam Baracuda Central anti virus ClamAV.
2	Yulia Fatma	2020	Analisa Dan Implementasi Security Mail Server	Pada tugas akhir ini akan dilakukan analisa dan implementasi security mail server zimbra khususnya penanganan	Perbedaan antara skripsi yang penulis angkat dengan skripsi ini adalah pengujiannya, pada skripsi

				email spam. Mail server zimbra akan di analisa segi keamanannya terhadap serangan email spam, agar dapat difungsikan sebagai mail server pada perusahaan.	ini email yang akan di uji adalah email real google dan yahoo dangan mail server yang di alokasikan pada vps yang telah penulis sewa, dan security yang di terapkan nantinya akan menangani spam, spoofing dan virus.
3	Abidarin Rosidi	2016	Data Manajemen Dan Teknologi Informasi	Untuk dapat mendeteksi adanya *email spoofing*, maka perlu adanya investigasi forensik email terhadap *email spoofing*. Salah satu teknik investigasi forensik email	Perbedaan penelitian sebelumnya dengan skripsi yang penulis buat adalah pada manajemen keamanan server mailnya yang dimana

				adalah menggunakan analisis *header* email (*header analysis method*). Teknik ini bekerja dengan memeriksa dan membandingkan *value* yang terdapat pada beberapa *header* email yang ditetapkan sebagai parameter deteksi *email spoofing*.	penulis untuk keamanan menggunakan protocol DMARC yang berfungsi sebagai autotentikasi untuk menurunkan jumlah email yang di anggap spam, sedangkan barracuda central di gunakan untuk memblokir atau mengizinkan pesan berdasarkan alamat IP pengirim atau URL.
4	Nur Widiyasono	2016	Investigasi *Email Spoofing* dengan	Hasil dari penelitian ini adalah email spoofing dapat	Perberdaan penelitian ini dengan penelitian

			Metode *Digital Forensics Research Workshop* (DFRWS)	dikirimkan dengan memanfaatkan layanan web hosting yang menyediakan layanan untuk pengiriman email dengan menggunakan bahasa pemrograman PHP dan hasil selanjutnya adalah mengetahui perbedaan antara email spoofing dan email asli, perbedaan tersebut akan diketahui dengan jelas ketika membuka header email rinci.	yang penulis angkat ini adalah, layanan yang di gunakan, dan mengetahui perbedaan email spoofing dan email spam maupun virus secara rinci pada header email di buka.

7. Jadawal Kegiatan

No	Kegiatan	Waktu Kegiatan					
		Jan	Feb	Mar	April	Mei	Jun
1.	Studi literature analisis penerapan protocol DMARC dan anti spam Baracuda Central						
2.	Melakukan uji coba penerapan protocol DMARC dan anti spam Baracuda Central pada mail server yang telah di ditribusikan dari VPS						
3.	Implementasi mail server untuk protocol DMARC dan anti spam Baracuda Central pada sub domain maupun pada email.						
4.	Menyimpulkan hasil analisis yang telah dilakukan						
5.	Uji Seminar & Revisi						

Mataram, 7 Desember 2020

Telah dikonsultasikan dengan
Dosen Pembimbing.

(I Putu Hariyadi.M.Kom)
NIK.09.6.124

Mahasiswa

Rudi Kurniawan
NIM. 1710510157

HALAMAN TAMBAHAN :

IDENTITAS		
NIM	:	1710510157
NAMA LENGKAP	:	Rudi Kurniawan
PRODI	:	S1 Ilmu Komputer
PEMINATAN (u/ S1 TI)	:	Jaringan Komputer
NO. HP	:	085237238085
EMAIL	:	Rudi.mastergg3@gmail.com
TOPIK SKRIPSI/ TA	:	ANALISA PENERAPAN *DMARC* YANG DIINTEGRASIKAN DENGAN *ANTI SPAM* DAN *ANTI VIRUS* UNTUK PENGAMANAN MAIL SERVER
KATA KUNCI	:	Analisa DMARC, anti Spam Baracuda Central dan anti virus.
DOSEN CALON PEMBIMBING	:	I Putu Haryadi.M.Kom