ANALISA PENERAPAN PROTOKOL *DMARC*, *ANTI SPAM BARRACUDA CENTRAL*, DAN *ANTI VIRUS Sophos AV* UNTUK KEAMANAN *MAIL SERVER*

SINOPSIS

Oleh:
RUDI KURNIAWAN
1710510157

ROGRAM STUDI ILMUKOMPUTER
FAKULTAS TEKNIK DAN KESEHATAN
UNIVERSITAS BUMIGORA
MATARAM
2020

BAB I
PENDAHULUAN

1. Latar Belakang

Perkembangan teknologi saat ini sudah begitu pesat sehingga teknologi dapat memudahkan pekerjaan manusia hampir di segala bidang, 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.

Sebelumnya penelitian ini sudah di lakukan oleh Naufal Hanif (2018) yang mendapatkan ide dari berbagai artikel yang telah di kutib,kemudian mendapatkan deskripsi sebagai berikut, Hoiriyah, Sugiantoro, dan Prayudi (2016) menyebutkan bahwa salah satu layanan internet yang banyak digunakan adalah *email*. *Email* merupakan surat elektronik yang berbasis *file* teks, namun dengan perkembangan teknologi, email lebih atraktif terhadap penggunanya, tidak hanya dapat mengirim *file* teks, tetapi juga dapat mengirim *file* audio, video, foto dan *file* ekstensi lainnya. 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. *Spam* adalah e*mail* yang tidak diinginkan, *email spam* dikirim kepada seseorang penerima dan pesan tersebut tidak ada gunanya untuk penerima. *Spam* dikirim pada jaringan untuk meningkatkan konsumsi sumber daya, dengan kata lain untuk meningkatkan lalu lintas jaringan *(Suryana, Akbar, Widiyasono, 2016).* Nurlina & Irmayana (2014) menyebutkan bahwa tidak semua *email spam* masuk pada *folder spam* yang telah disediakan dan *email* yang bukan *spam* terkadang masuk pada *folder spam* sehingga *email* penting terkadang tidak dibaca oleh penerima *email*. *Email* juga merupakan sumber utama dari kebanyakan aktivitas kriminal pada *internet*, salah satu ancaman dari tindak kejahatan yang menggunakan *email* adalah *email spoofing*. *Email spoofing* dianggap sebagai tindakan berbahaya karena melakukan manipulasi data pada *header email* untuk menyamar sebagai

orang atau organisasi yang sah, contohnya seperti melakukan pengiriman *email* dengan nama pengirim seolah dari administrator suatu organisasi. Pengirim email spoofing menyerang dengan berbagai macam isi pesan untuk membuat korbannya percaya.

Dari kutipan di atas maka Pertimbangan ini lah yang membuat penulis untuk menerapkan *Protocol DMARC* dan *Baracuda Central* dan antivirus *Sophos AV*, untuk mengatasi *Email spam, spoofing,* dan *virus* yang sangat tidak diinginkan oleh pengguna maupun penyedia layanan *email* sehingga perlu diterapkan suatu sistem yang dapat mencegah *email spam, spoofing*, dan *virus*. 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 Sophos AV* juga diperlukan agar *email server* terhindar dari *email spam* dan *virus*, metode yang diterapkan oleh *Anti Spam* dan *Anti Virus Sophos AV* yaitu dengan melakukan pengecekan *haeder*, *body*, dan *attachment email* kemudian di sampaikan ke pengguna.

Manfaat dari penerapan *PROTOCOL DMARC* (Domain-based Message Authentication, Reporting and Conformance), *BARACUDA CENTRAL*, Anti *Spam* dan *Anti Virus Sophos AV* adalah untuk mengoptimalkan system keamanan jaringan server mail, menghemat sumber daya mail server dengan cara memblokir surat elektronik yang dianggap sebagai spam atau virus, meningkatkan kualitas keamanan surat elektronik sehingga pengguna dapat terhindar dari aktifitas spoofing serta virus dan malware 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 Sophos AV* 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.*

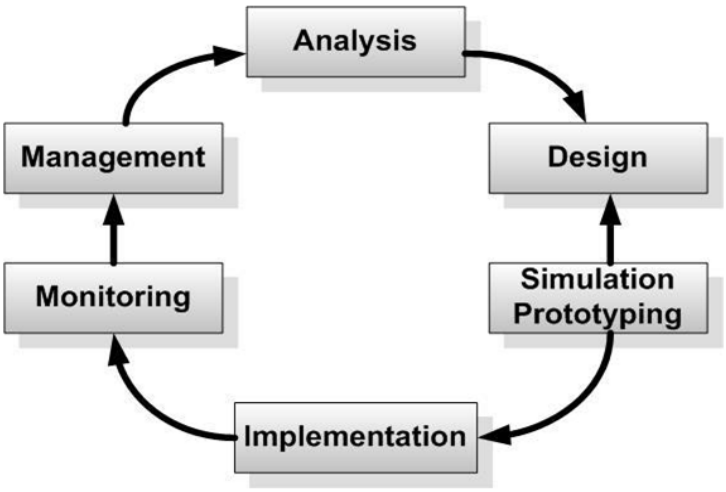
b. Manfaat

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 DKIM, SPF, 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 DKIM, SPF, 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 DKIM, SPF Anti Spam, dan Anti Virus menggunakan berbagai macam scenario.

4. Implementation

   Pada fase ini penulis akan menerapkan semua yang telah direncanakan dan di desain pada tahapan sebelumnya.

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* dapat mencegah *email spoofing* dengan cara melakukan otorisasi menggunakan metode	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 DMARC dan anti spam Baracuda Central anti virus Sophos AV.

				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*.	
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 email spam. Mail server zimbra akan di analisa segi keamanannya terhadap serangan email	Perbedaan antara skripsi yang penulis angkat dengan skripsi ini adalah pengujiannya, pada skripsi ini email yang akan di uji adalah email real google dan yahoo dangan mail server

				spam, agar dapat difungsikan sebagai mail server pada perusahaan.	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 adalah menggunakan analisis *header* email (*header analysis method*). Teknik	Perbedaan penelitian sebelumnya dengan skripsi yang penulis buat adalah pada manajemen keamanan server mailnya yang dimana penulis untuk keamanan menggunakan protocol DMARC yang

				ini bekerja dengan memeriksa dan membandingkan *value* yang terdapat pada beberapa *header* email yang ditetapkan sebagai parameter deteksi *email spoofing*.	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 Metode *Digital Forensics Research Workshop* (DFRWS)	Hasil dari penelitian ini adalah email spoofing dapat dikirimkan dengan memanfaatkan layanan web hosting yang menyediakan	Perberdaan penelitian ini dengan penelitian yang penulis angkat ini adalah, layanan yang di gunakan, dan

				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.	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.masterqq3@gmail.com
TOPIK SKRIPSI/ TA	:	ANALISA PENERAPAN PROTOKOL *DMARC*, *ANTI SPAM BARRACUDA CENTRAL*, DAN *ANTI VIRUS Sophos AV* UNTUK KEAMANAN *MAIL SERVER*
KATA KUNCI	:	Penerapan Protocol DMARC dan anti Spam Baracuda Central.
DOSEN CALON PEMBIMBING	:	I Putu Haryadi.M.Kom