BAB I
PENDAHULUAN

1.1. 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.

Mengingat betapa pentingnya media komonikasi di zaman sekarang ini maka beberapa orang melakukan penelitian terutama di bidang keamanan jaringan. 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 (Hoiriyah, Sugiantoro, and Prayudi 2016). 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 (Hanif 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, (Nadzifan, Nazihullah, and . 2018). 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, (Ardhi 2020).

Dari kutipan di atas ada beberapa kekurangan seperti *DKIM* memiliki masalah yang tidak dapat menentukan apakah tanda tangan itu sah dan juga tidak dapat memberi laporan apabila terjadi pemalsuan email. 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, *ClamAV* 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) 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,* 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 (Hanif 2018).

1.2. Perumusan 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),* 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,* (Hanif 2018).

1.3. Batasan Masalah

Batasan masalah yang digunakan dalam penyusunan skripsi ini untuk menjadikan pembahasan menjadi lebih terarah dan fokus adalah sebagai berikut:

1. 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).
2. Sistem operasi VPS yang digunakan adalah CentOS 7-9.
3. Aplikasi yang digunakan untuk memudahkan instalasi dan konfigurasi server adalah CentOS Web Panel.
4. Aplikasi MTA yang digunakan adalah Postfix untuk mengirim email.

5. Aplikasi MDA yang digunakan adalah Dovecot untuk menerima email.
6. Aplikasi MUA yang digunakan adalah Roundcube sebagai aplikasi email di sisi pengguna.
7. Aplikasi DNS server yang digunakan adalah bind9 agar email server dapat diakses menggunakan nama domain
8. Aplikasi HTTP server yang digunakan adalah Apache agar Mail Transfer Agent berbasis web dapat diakses melalui browser.
9. Pengujian yang dilakukan dengan mengirim surat elektronik yang terindikasi sebagai spam, kemudian melakukan pengiriman email spoofing, dan email yang mengandung virus, serta mengecek header setelah penerapan DMARC, anti spam, dan anti virus.
10. Pengujian DMARC dilakukan dengan cara mengirim email spoofing menggunakan Emkei's Fake Mailer kemudian email spoofing tersebut dikirim ke Gmail dan Yahoo! Mail.
11. Pengujian Anti Spam dan Anti Virus dilakukan dengan cara mengirim email spam dan email yang mengandung virus ke mail server.
12. Hasil report DMARC di kirim ke email root@skripsirudi.my.id.

1.4. Tujuan dan Manfaat Penulisan

1.4.1. Tujuan

Adapun tujuan dari penulisan skripsi ini adalah untuk menganalisa Penerapan Protocol DMARC, Anti Spam dan Anti Virus agar mail server terhindar dari spam dan virus dilakukan dengan cara mengirim email yang mengandung spam dan virus ke mail server.

1.4.2. Manfaat

Adapun manfaat dari penelitian ini adalah sebagai berikut:

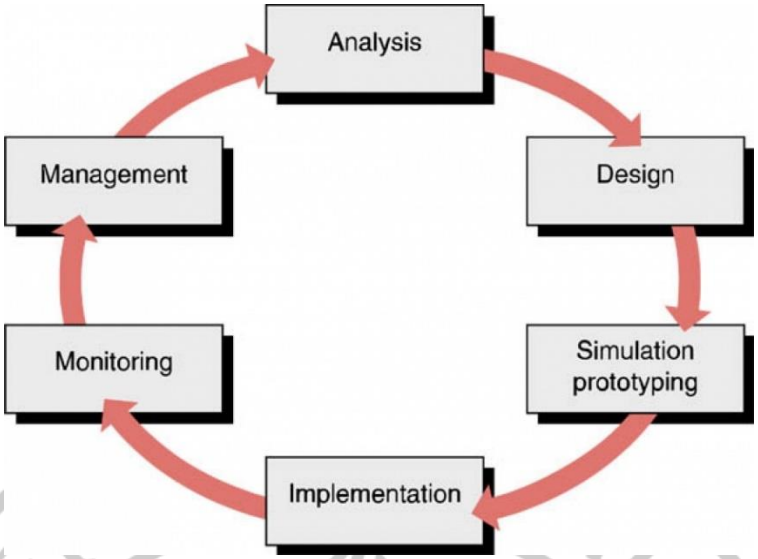
1. Bagi Diri Sendiri

a. Dapat menambah ilmu pengetahuan 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 Teknik Informatika 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*, *Anti Spam*, dan *Anti Virus*.
   b. Dapat memberikan solusi cara penerapan *Protocol DMARC*, *Anti Spam*, dan *Anti Virus* pada *mail server*.

1.5. Metodologi penelitian

(Puspita et al. 2015) menyebutkan bahwa *Network Development Life Cycle* adalah suatu metode yang digunakan dalam mengembangkan atau merancang jaringan infrastruktur yang memungkinkan terjadinya pemantauan jaringan untuk mengetahui statistik dan kinerja jaringan. *NDLC* mempunya enam fase, keenam fase tersebut dapat dilihat seperti pada gambar 1.1 berikut.



Gambar 1. 1 Fase *NDLC*
Sumber: Nurfajar, Kurniawan, dan Yunan, 2015

Dari keenam fase yang terdapat pada *NDLC*, penulis hanya menggunakan tiga 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*, *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 *DMARC*, *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, Pada fase ini dilakukan instalasi dan konfigurasi serta uji coba *DMARC, DKIM, SPF Anti Spam,* dan *Anti Virus* menggunakan berbagai macam skenario.

1.6. Sistematika Penulisan

Adapun sistematika penulisan yang digunakan pada skripsi ini adalah sebagai berikut:

BAB I Pendahuluan

Bab ini berisi latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penulisan, metodologi penelitian, dan sistematika penulisan.

BAB II Landasan Teori

Bab ini berisi tentang teori-teori yang melandasi penelitian ini, antara lain jaringan komputer, *OSI*, *TCP/IP*, keamanan jaringan komputer, tujuan keamanan jaringan komputer, *Spoofing*, *Phising*, *Server*, Linux, Linux *CentOS*, *CentOS Web Panel*, *Email*, *Mail Server*, *POP3*, *IMAP*, *SMTP*, *Postfix*, Dovecot, *Roundcube*, *DNS*, *DNS Server*, *BIND9*, *HTTP* dan *HTTPS*, *HTTP Server*, Apache *HTTP Server*, *Email Spam*, *Anti Spam*, *SpamAssassin*, *ClamAV*, *DMARC*, *Amavisd-New*, *DKIM*, *OpenDKIM*, *SPF*, *Gmail*, *Emkei's Mailer*, *Yahoo! Mail*.

BAB III Metodologi Penelitian

Bab ini berisi tentang metodologi penelitian yang digunakan dan fase-fase dari metodologi penelitian yang digunakan pada penelitian ini.

BAB IV Hasil dan Pembahasan

Bab ini berisi tentang pembahasan hasil konfigurasi, uji coba, dan analisa terhadap uji coba yang telah dilakukan.

BAB V Penutup

Bab ini berisi tentang kesimpulan dan saran untuk pengembangan skripsi ini selanjutnya.