BAB III

METODOLOGI DAN PERANCANGAN

Metode penelitian yang digunakan adalah *Network Development Life Cycle (NDLC).* Dari enam tahapan yang ada pada *NDLC*, penulis hanya menggunakan 3 tahapan yaitu *Analysis, Design, Simulation Prototyping* (Hanif 2018).

3.1. Tahap Analisa (*Analysis*)

Pada fase ini penulis melakukan pengumpulan data dengan cara studi literatur, yaitu penulis membaca artikel ilmiah, buku, dan jurnal untuk mendapatkan informasi mengenai *email spam, email spoofing*, dan *virus*. Data-data yang telah terkumpul kemudian dianalisa. Tahap ini terdiri dari dua bagian yaitu pengumpulan data dan analisa data (Hanif 2018).

3.1.1. Pengumpulan Data

Pada tahap pengumpulan data, penulis menggunakan metode studi literatur yaitu dengan mempelajari beberapa jurnal ilmiah yang membahas tentang *email spam, email spoofing*, dan *virus*, selain itu penulis juga menggunakan *e-book* yang membahas tentang *email spam, virus,* dan *email spoofing*. Setelah membaca beberapa jurnal ilmiah diperoleh informasi tentang beberapa jurnal ilmiah yang berkaitan dengan *email spam, virus,* dan *email spoofing* seperti terlihat pada tabel 3.1 berikut.

Tabel 3. 1 Jurnal Ilmiah Tentang *Email Spam, Spoofing,* dan *Virus*

No	Penulis	Tahun	Judul	Pembahasan
1	Andri Lesmana Suryana, R. Reza El Akbar, dan Nur Widiyasono	2016	Investigasi *Email Spoofing* dengan Metode *Digital Forensics Research Workshop (DFRWS)*	Mengidentifikasi *email spoofing* menggunakan metode *DFRWS*

No	Penulis	Tahun	Judul	Pembahasan
2	Naufal hanif.S.Kom	2018	Analisa Penerapan *Domainkeys Identified Mail* (*Dkim*), *Sender Policy Framework* (*Spf*), *Anti Spam*, Dan *Anti Virus* Pada *Mail Server*	menganalisa penerapan *DKIM*, *SPF*, *Anti Spam* dan *Anti Virus* pada *mail server* agar *mail server* terhindar dari *email spam*, *virus* dan aktifitas *spoofing*
3	Andrian Maftuh Nadzifan, Farih Nazihullah	2018	Aplikasi Untuk Deteksi Adanya Spoof Pada *Email*	Meneruskan penelitian sebelumnya *Forensic* Analysis of E-mail Address Spoofing demgan algoritma deteksi.
4	Abidarin Rosidi, Heri Sismoro, Emha Taufiq Luthfi, Hanif Al Fatta, Hastari Utama	2016	Data Manajemen Dan Teknologi Informasi	mendeteksi adanya *email spoofing*, maka perlu adanya investigasi forensik email terhadap *email spoofing*.
5	Daniel Adi Putra Sitorus, Harun Mukhtar, Yulia Fatma	2020	Analisa Dan Implementasi Security Mail Server	Analisis dan implementasi serangan email spam pada mail server zimbra.

3.1.2. Analisa Data

Berdasarkan hasil dari pengumpulan data maka dapat diperoleh hasil analisa sebagai berikut:

1. Jurnal ilmiah pertama membahas tentang investigasi *email spoofing* menggunakan metode *DFRWS* yaitu dengan melakukan pengecekan *header email* secara manual.
2. Jurnal ilmiah kedua pembahasan tentang 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. Sebaliknya penerapan *SpamAssassin*, *ClamAV*, dan *Amavisd-New* dapat mencegah masuknya *email spam* dan *virus* dengan cara melakukan pengecekan *header*, *body*, dan *attachment email*.
3. Jurnal ilmiah ketiga membahas tentang Meneruskan penelitian sebelumnya *Forensic* Analysis of E-mail Address Spoofing demgan algoritma deteksi.
4. Jurnal ilmiah keempat membahas tentang mendeteksi adanya *email spoofing*, maka perlu adanya investigasi forensik email terhadap *email spoofing*.
5. Jurnal ilmiah kelima membahas tentang Analisis dan implementasi serangan email spam pada mail server zimbra.
6. Penanganan *email spoofing* belum menerapkan metode otentikasi dan otorisasi untuk menambah informasi pada *email header*.
7. Belum terdapat uji coba *ClamAV* sebagai *anti virus* pada *mail server*.

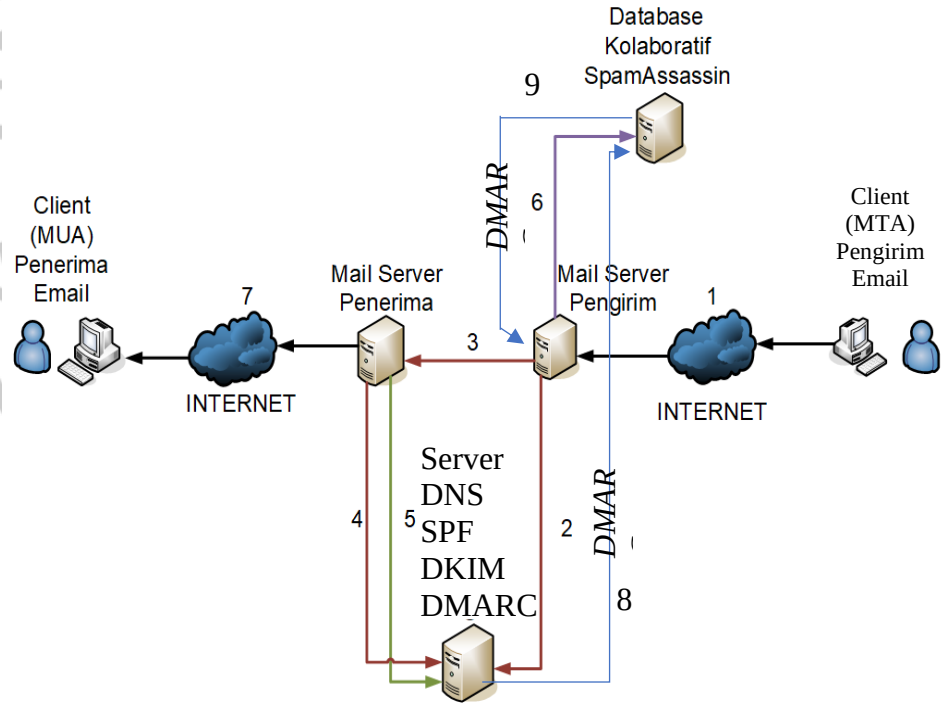
Dari hasil analisa tersebut maka mendorong penulis untuk melakukan penelitian tentang Analisa Penerapan *Dmarc* Yang Diintegrasikan Dengan *Anti Spam* Dan *Anti Virus* Untuk Pengamanan *Mail Server.*

3.2. Tahap Desain *(Design)*

Tahap ini terdiri dari 4 (empat) bagian yaitu rancangan sistem *filtering email spam, virus,* dan *spoofing,* rancangan jaringan ujicoba, rancangan pengalamatan *IP*, rancangan akun *email,* serta kebutuhan perangkat keras dan perangkat lunak (Hanif 2018).

3.2.1 Rancangan Sistem *Filtering Email Spam, Virus* dan *Spoofing*

Rancangan sistem *filtering email spam, virus* dan *spoofing* yang digunakan seperti terlihat pada gambar 3.1 berikut.



Gambar 3.1 Rancangan Sistem *Filtering Email Spam, Spoofing,* dan *Virus*

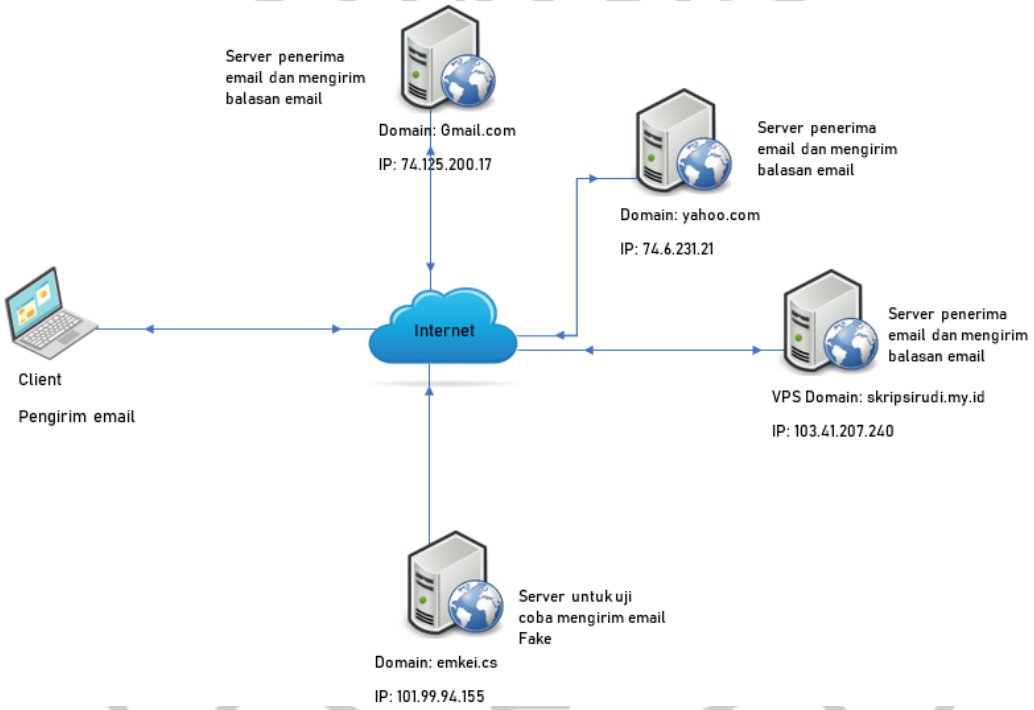
Berdasarkan gambar 3.1 tersebut maka rancangan sistem *filtering email spam, virus* dan *email spoofing* dapat dijelaskan sebagai berikut.

a. Langkah 1 *user* mengirim *email* dengan menggunakan *Mail User Agent* berbasis web (*Roundcube*), *user* mengakses *Roundcube* menggunakan *browser*.
b. Langkah 2 *Mail server* pengirim meneruskan *email* ke *mail server* penerima dengan menambahkan *private key* pada *header email*.
c. Langkah 3 *Mail server* pengirim mem*publish public key* pada *DNS server*nya.
b. Langkah 4 *Mail server* penerima mengambil *public key* yang ada pada *DNS server* pengirim *email* untuk dicocokan dengan *private key* yang ada pada *header email*, jika *private key* tidak cocok dengan *public key* maka *email* akan dianggap sebagai *email spam* dan akan di report oleh *DMARC* berlaku langkah 8, jika *private key* cocok dengan *public key* maka proses akan berlanjut pada langkah ke 5.
c. Langkah 5 *Mail server* penerima mencocokan alamat *IP mail server* pengirim dengan *sender ID framework* pada *SPF record* yang berada pada *DNS server* pengirim, jika pada *SPF record* yang berada pada *DNS server* pengirim tidak mengotorisasi alamat *IP email server* pengirim *email* tersebut maka *email* tersebut akan diblok atau ditandai sebagai spam, jika alamat *email* pengirim telah diotorisasi oleh *administrator email server* maka proses akan berlanjut pada proses ke 6.
d. Langkah 6 *Mail server* penerima melakukan pengecekan pada *database* kolaboratif *SpamAssassin*.
e. Proses pem*filter*an *email spam* selanjutnya adalah menggunakan *SpamAssassin* dan *ClamAV* sebagai *anti spam* dan *anti virus email* dengan *Amavisd-New* sebagai penghubung antara *SMTP server* dengan *SpamAssassin* dan *ClamAV*.
f. Proses report email dari *DMARC* yang dikirim ke folder spam, kemudian proses 9 yang mengirim balik email spam ke pengirim semula.

Keterangan: garis merah mewakili proses *DKIM* (nomor 2, 3, dan 4),garis hijau mewakili proses *SPF* (nomor 5), dan garis ungu mewakili proses *SpamAssassin* (nomor 6), (no 8 dan 9) garis biru mewakili *protocol DMARC*.

3.2.2 Rancangan jaringan Uji coba

Rancangan jaringan uji coba yang digunakan seperti terlihat pada gambar 3.2 berikut.



Gambar 3. 2 Rancangan Topologi Uji Coba

Rancangan ini diimplementasikan menggunakan *VPS* yang disewa pada penyedia layanan *VPS* dan pada *VPS* telah terinstal sistem operasi *CentOS* Linux *release* 7, *VPS* yang telah disewa diberikan satu alamat *IP public* oleh penyedia layanan *VPS* yaitu 103.41.207.240. Pada *VPS* akan dilakukan instalasi *CentOS Web Panel*, konfigurasi *DNS server*, konfigurasi *Mail server*, dan pada komputer *client* telah terinstal system operasi windows 10 dan aplikasi browser Google Chrome untuk mengakses *Mail User Agent* berbasis web (Roundcube).

3.2.3 Rancangan Pengalamatan *IP*

Pengalamatan *IP* merupakan salah satu bagian yang penting karena merupakan suatu identitas pengalamatan suatu *interface*. Berikut adalah pengalamatan *IP* pada masing-masing *interface* agar dapat saling berkomunikasi antar perangkat yang terhubung (Hanif 2018). Pengalamatan *IP* dapat dilihat seperti pada tabel 3.2 berikut.

Tabel 3.2 Pengalamatan *IP*

No	Perangkat	*IP Address*	*Network*	*Interface*
1	*DNS Server, HTTP Server, SMTP Server, POP3/IMAP Server (VPS)*	192.168.43.24/25	192.168.43.1	eth0
2	*Client*	*DHCP*	*DHCP*	-

3.2.4 Rancangan Akun *Email*

Berikut adalah kebutuhan akun *email* untuk mendukung apa yang akan dilakukan dalam membangun atau mempersiapkan implementasi seperti terlihat pada tabel 3.3 berikut, (Hanif 2018).

Tabel 3.3 Kebutuhan Akun *Email*

No	Alamat *Email*	*Domain*
1	Rudi.masterqq3@gmail.com	gmail.com
2	Rudi.masterqq3@yahoo.com	yahoo.com
3	Root@Skripsirudi.my.id	Skripsirudi.my.id
4	admin@ Skripsirudi.my.id	Skripsirudi.my.id

3.2.5 Kebutuhan Perangkat Keras dan Perangkat Lunak

(Hanif 2018) Berikut adalah kebutuhan perangkat keras dan perangkat lunak untuk mendukung apa yang akan dilakukan dalam membangun atau mempersiapkan implementasi yaitu:

1. Kebutuhan Perangkat Keras

   Satu unit *VPS* dengan spesifikasi seperti terlihat pada tabel 3.4 berikut.

Tabel 3.4 Spesifikasi *VPS*

Komponen	Spesifikasi
CPU	*Virtual CPU* 2 *Core*
RAM	2 GB
Hard Drive	40 GB

   Satu unit laptop dengan spesifikasi seperti terlihat pada tabel 3.5 berikut.

Tabel 3.5 Spesifikasi *Client*

Komponen	Spesifikasi
CPU	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz
RAM	12 GB
Hard Drive	1 TB

2. Kebutuhan Perangkat Lunak

   Adapun perangkat lunak yang dibutuhkan adalah sebagai berikut:

   a. *Linux CentOS release* 7 sebagai sistem operasi *VPS*.

   b. *CentOS Web Panel* sebagai *tool* untuk memudahkan dalam melakukan konfigurasi *server*.

   c. Dovecot sebagai *Mail Delivery Agent*.

   d. Postfix sebagai *Mail Transfer Agent*.

   e. Roundcube sebagai *Mail User Agent*.

   f. Apache sebagai web *server*.

   g. Bind9 sebagai *DNS server*.

   h. Microsoft Windows 10 sebagai sistem operasi *client*.

i. Google Chrome sebagai *browser client* untuk mengakses *Roundcube*.

3.3. Tahap Simulasi (*Prototyping*)

(Hanif 2018) Tahap ini terdiri dari 2 bagian yaitu instalasi dan konfigurasi pada *VPS* dan *client* serta melakukan uji coba menggunakan berbagai skenario dan memverifikasi hasil uji coba tersebut.

Uji coba pertama dilakukan dengan mengirim *email spoofing* melalui *Emkei's Mailer* dengan mengatasnamakan salah satu *user* yang berada pada *domain* skripsirudi.my.id kemudian mengirim *email spoofing* tersebut ke *mail server Gmail, Yahoo! Mail,* dan skripsirudi.my.id setelah penerapan protocol *DMARC, DKIM* dan *SPF* pada *mail server* skripsirudi.my.id (Hanif 2018).

Uji coba kedua dilakukan untuk menguji kinerja *Anti Spam* pada *mail server* skripsirudi.my.id dengan mengirim *email spam* melalui *Emkei's Fake Mailer, Gmail,* dan *Yahoo! Mail* kemudian mengirim *email spam* tersebut ke salah satu *user* yang berada pada *mail server* skripsirudi.my.id sebelum dan setelah penerapan *SpamAssassin* (Hanif 2018).

Uji coba ketiga dilakukan untuk menguji kinerja *anti virus* pada *mail server* skripsirudi.my.id dengan cara mengirim *email* yang mengandung *virus* melalui *Emkei's Fake Mailer, Gmail,* dan *Yahoo! Mail* ke salah satu *user* yang ada pada *mail server* skripsirudi.my.id setelah penerapan *ClamAV* (Hanif 2018).

Uji coba ketiga dilakukan dengan cara membandingkan *header email* yang dikirim oleh salah satu *user* yang berada pada *mail server* skripsirudi.my.id ke *Gmail, Yahoo! Mail,* dan skripsirudi.my.id setelah penerapan protocol *DMARC, DKIM, SPF, Anti Spam,* dan *Anti Virus* (Hanif 2018).

3.3.1. Instalasi Dan Konfigurasi

Instalasi dan konfigurasi *DKIM*, *SPF, Anti Spam, Anti Virus* dan *DMARC* dilakukan pada *VPS* yang berfungsi untuk mem*filter email spam* dan *virus* yang masuk serta untuk mencegah adanya *email spoofing* yang mengatasnamakan skripsirudi.my.id, sedangkan pada komputer *client* sudah terinstal sistem operasi Windows 10 dan browser Google Chrome untuk mengakses *Mail User Agent* berbasis web (Roundcube), *client* harus terkoneksi dengan jaringan *internet* agar dapat mengakses *Mail User Agent* yang telah disediakan oleh *mail server* skripsirudi.my.id. (Hanif 2018).

3.3.2. Uji Coba

Pada tahap ujicoba ini tediri dari 2 bagian yaitu verifikasi konfigurasi dan ujicoba menggunakan berbagai skenario. Verifikasi konfigurasi dilakukan untuk memverifikasi fungsi *DNS server* dan *Mail server* dengan melakukan *nslookup* untuk memverifikasi fungsi *DNS server* dan melakukan pengiriman *email* antar pengguna yang berada pada *mail server* yang telah dibangun serta melakukan pengiriman *email* dari *server* yang telah dibangun ke *email server* yang lainnya untuk memverifikasi fungsi *Mail server*. Sedangkan skenario ujicoba yang dilakukan meliputi pembuatan skenario yang terdiri dari beberapa skenario seperti uji coba sebelum diterapkannya *filtering email spam, virus,* dan *spoofing*, serta ujicoba sesudah diterapkannya *filtering email spam, virus* dan *spoofing*.