BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil ujicoba penerapan protocol DMARC yang telah dilakukan maka dapat diperoleh kesimpulan sebagai berikut:

1. Penerapan protokol *DomainKeys Identified Mail* dapat mencegah *email spoofing* dengan cara melakukan otentikasi menggunakan metode pencocokan *private key* dan *public key* (*Asymmetric keys*).
2. Penerapan protokol *Sender Policy Framework* dapat mencegah *email spoofing* dengan cara melakukan otorisasi menggunakan metode pencocokan alamat *IP server* pengirim.
3. Penerapan protocol DMARC dapat mencegah email spoofing dan memberikan sebuah laporan kepada email pengguna asli dengan cara memlakukan otentikasi pencocokan alamat IP server dan header email.
4. Penerapan *SpamAssassin*, *ClamAV*, dan *Amavisd-New* dapat mencegah masuknya *email spam* dan *virus* dengan cara melakukan pengecekan *header*, *body*, dan *attachment email*.

5.2. Saran

Adapun saran-saran untuk pengembangan penelitian lebih lanjud adalah sebagai berikut :

1. Mengembangkan sistem *anti spam* dengan menggunakan *database* kolaboratif SpamAssassin yaitu Pyzor, Razor2, dan DCC serta menggunakan fitur *blacklist* dan *whitelist* SpamAssassin untuk memaksimalkan kinerja SpamAssassin.
2. Mengembangkan sistem *anti spam* dengan menambahkan *tools anti spam* lainnya seperti *Barracuda Central*, *Spamhaus*, *SpamCop*, *SORBS*, dan lain-lain.

3. Penambahan mekanisme email agar rentan waktu untuk DMARC dapat mengirimkan report email terlebih dahulu daripada pesan email.
4. Penambahan kebijakan di dalam protocol DMARC seperti kebijakan none dan reject.