1. Pendahuluan

Latar Belakang

Penggunaan email sebagai alat untuk mengirim dan menerima pesan juga digunakan sebagai alat untuk menyimpan informasi rahasia, karena email juga terhubung dengan berbagai akun media sosial [6]. Namun *email* juga merupakan sumber dari kebanyakan aktivitas kriminal pada Internet [4]. Ancaman dari tindak kejahatan yang menggunakan *email* adalah *email spoofing*. *Email spoofing* merupakan teknik kejahatan *cyber* dengan melakukan penipuan atau menyebarkan berita bohong dengan menyamarkan nama pengirim *email* menjadi *email* tertentu. Ada dua jenis dari *email spoofing*, yang pertama *email spoofing* tanggal & waktu dan *spoofing* alamat email pengi- rim. Di tanggal & waktu spoofing penyerang dengan merubah tanggal menjadi sebelum atau sesudah di keterangan 'Waktu' pada *header email*.

Dalam pengirim alamat *spoofing* asal-usul *email* dimodifikasi untuk muncul sebagai E-mail yang berasal dari sumber yang berbeda, itulah yang dimanfaatkan oleh *spammer/scammer* untuk membuat *email* yang tampak dari pengirim yang sebenarnya dan mengelabui penerima sehingga penerima *email* yang kurang perhatian terhadap *email* yang masuk akan terjebak dalam skenario yang didesain oleh *scammer* [4]. Mereka dapat melakukan *phi- shing* untuk mengungkapkan informasi seperti *username* dan *password* sebuah rekening bank. Mengirim E-mail dengan nama orang yang mereka kenal, penyerang bisa mendapatkan informasi rahasia pribadi serta resmi. Peng- guna yang tidak sadar atau baru mulai menggunakan *email* dapat dengan mudah terjebak dalam jenis penipuan [8]. Hasil dari laporan yang dipaparkan oleh [2], aktivitas *phishing* mengalami penurunan pada bulan Maret 2020. Kemudian meningkat pada pertengahan tahun 2020 ditemukan 146.994 serangan *phishing* yang dilaporkan. Ini adalah salah satu angka tertinggi terlihat dalam beberapa tahun terakhir, tetapi ini merupakan penurunan 11% dari tahun 2019, yang memiliki jumlah 165.772 serangan dalam periode yang sama. Walaupun begitu angka tersebut tidaklah sedikit.

Untuk mengetahui solusi dari permasalahan ini dibutuhkan sebuah aksi deteksi *email spoofing* sebagai suatu tindakan pengecekan terhadap *email* palsu. Dengan menggunakan metode *header analysis* dan dengan mengikuti beberapa seperangkat aturan, kita dapat mengetahui apakah *email* tersebut resmi atau tidak [5]. Alasan mengapa penelitian ini menggunakan metode *header analysis* karena terdapat dua penelitian yang menggunakan metode *header analysis* dengan algoritma yang berbeda. Metode pertama yaitu menganalisa nama domain yang terdapat pada *field 'From', 'Message-ID', 'Date',* dan *'Received'*[7], kemudian metode kedua menganalisa standar autentikasi pada *email* yaitu SPF, DMARC, dan DKIM [9]. Terdapat kekurangan dari penelitian terdahulu yaitu variasi *email* yang diuji sama. Karena itu penelitian ini dilakukan untuk menguji kedua metode tersebut pada variasi *ema- il* yang berbeda dan perlu dilakukan perbandingan pada kedua metode tersebut untuk menentukan metode mana yang lebih efektif dalam mendeteksi *email spoofing*.

Topik dan Batasannya

Berdasarkan latar belakang diatas maka dapat disimpulkan rumusan masalah sebagai

berikut: 1.Bagaimana penerapan dua metode *header analysis* untuk mendeteksi *email*

spoofing ?

2. Bagaimana evaluasi keefektifan dua metode tersebut untuk mendeteksi *email spoofing* ?

1.1 Batasan Masalah

Untuk menghindari terjadinya perluasan ruang lingkup, batasan masalah sebagai berikut:

1.Implementasi dua jenis algoritma *header analysis* untuk mendeteksi *email spoofing*.

2.Percobaan dilakukan pada layanan surel milik Google, yaitu Gmail.

3. *Email* yang diuji adalah *email spoofing* dan *email legitimate* yang berasal dari seseorang dan suatu organisasi
atau perusahaan.

4. Parameter pengujiannya adalah alamat pengirim, ID pesan, serta waktu pengirman pesan pada metode per- tama dan nilai Standar Autentikasi dan Kebijakan Email pada metode kedua.

5. Menggunakan program dengan bahasa *python* untuk melakukan pengecekan keaslian *email* dan akurasi metode.

6. *Output* yang dihasilkan berupa hasil pengujian dan akurasi metode.

Tujuan

Berdasarkan rumusan masalah diatas adapun tujuan dari penelitian ini yaitu:

1. Menerapkan dua algoritma metode *header analysis* yaitu analisa terhadap informasi pada alamat pengirim, ID pesan, serta waktu pengirman pesan dan analisa terhadap Standar Autentikasi dan KebijakanEmail.

2. Menganalisa keefektifan kedua metode berdasarkan akurasinya dalam mendeteksi *email spoofing*.