I PENDAHULUAN

1.1 Latar Belakang

Salah satu ancaman terbesar di dunia teknologi saat ini adalah *malware* (*malicious* perangkat lunak) atau program komputer yang mencurigakan. *Malware* sering kali muncul sebagai ancaman dalam bentuk dan variasi yang berbeda – beda serta dengan tingkat ancaman yang beragam (Bayer *et al.* 2009). Lale dan Vyawahare (2020:33) menyatakan "… *Malware attack would not work without the most important ingredient: you …*". Pernyataan ini menunjukkan bahwa kerentanan sistem terhadap serangan *malware* bukan hanya terletak pada teknologinya saja tetapi juga pada *brainware* (penggunanya).

Menurut laporan SophosLab (2013), Indonesia merupakan negara dengan *Threat Exposure Rate* terbesar yang membuat Indonesia menempati peringkat pertama sebagai negara yang paling berisiko terkena serangan malware. *Threat Exposure Rate* diukur dari persentase perangkat komputer yang terkena serangan *malware*, baik itu berhasil ataupun gagal, dalam periode waktu tiga bulan. Dalam laporan tahunan 2018, ID-SIRTII/CC melaporkan bahwa Indonesia menerima 232.447.974 serangan, termasuk 122.435.215 aktivitas malware, 16.939 insiden situs web, 2.885 laporan insiden publik, dan 1.872 pelanggaran keamanan. Selain itu, Indonesia juga menjadi negara yang melakukan paling banyak serangan. (Prakasa 2020). Data tersebut menunjukkan bahwa keamanan jaringan di Indonesia juga rentan terhadap serangan peretas dari dalam negeri.

Dinas Komunikasi, Informatika, Statistik dan Persandian (DISKOMINFOSTANDI) Kota Bekasi merupakan organisasi atau badan yang bertanggung jawab dalam mengelola dan mengembangkan teknologi informasi dan komunikasi di lingkup pemerintahan Kota Bekasi. Oleh karena itu, perlu diterapkan sistem deteksi dan prevensi terhadap intrusi lalu lintas jaringan untuk mencegah terjadinya kerugian di masa mendatang. Sistem ini berupa prototipe yang digunakan untuk mensimulasikan sistem deteksi dan prevensi intrusi lalu lintas jaringan.

Beberapa penelitian yang berkaitan dengan sistem keamanan jaringan menggunakan perangkat lunak Snort telah dilakukan, di antaranya adalah Zhou *et al.* (2010), Huang *et al.* (2012) dan Khamphakdee *et al.* (2015). Dalam penerapannya, ketiganya penelitian tersebut menjalankan Snort dalam mode *Intrusion Detection System* (IDS) dengan memeriksa pola tertentu seperti protokol yang digunakan dan nilai tertentu pada paket data. Namun belum ada tindakan lanjutan setelah Snort berhasil mendeteksi paket data yang mencurigakan, seperti melakukan *drop packet* atau membuat laporan kinerja sistem. Penelitian serupa juga dilakukan oleh Aminanto dan Sulistyo (2020) menggunakan Snort mode *Intrusion Prevention System* (IPS) dan Honey Artillery. Namun berdasarkan diagram alur sistem yang digambarkan, sebagian besar pekerjaan dilakukan oleh Honey Artillery, sedangkan Snort hanya digunakan untuk menampilkan *log* pada *web interface*. Penelitian ini kurang mengoptimalkan fungsi Snort sebagai *Intrusion Detection and Prevention System* (IDPS). Berdasarkan hasil penelitian yang sudah disebutkan, penelitian ini melakukan pengembangan dengan menggunakan Snort dalam mode IDPS agar dapat mengambil tindakan pasca-deteksi. Maltrail juga diimplementasikan untuk mendeteksi akses ke situs yang diketahui terinfeksi

malware. Snort dan Maltrail dapat bersinergi dalam mengamankan lalu lintas jaringan.

1.2 Rumusan Masalah

Rumusan masalah penelitian ini adalah :

1. Bagaimana cara melakukan deteksi dan prevensi lalu lintas jaringan dengan perangkat lunak *open-source*?
2. Bagaimana cara mendeteksi situs yang terinfeksi *malware* menggunakan daftar hitam?

1.3 Tujuan

Tujuan penelitian ini adalah :

1. Melakukan deteksi dan prevensi terhadap lalu lintas jaringan yang mencurigakan dengan perangkat lunak Snort di Diskominfostandi Kota Bekasi.
2. Mendeteksi adanya akses ke situs yang terinfeksi *malware* dengan perangkat lunak Maltrail di Diskominfostandi Kota Bekasi.

1.4 Manfaat

Manfaat penelitian ini adalah :

1. Mengidentifikasi paket – paket jaringan yang mencurigakan dan terdeteksi sebagai *malware* di Diskominfostandi Kota Bekasi.
2. Meminimalisir dan Mencegah adanya celah keamanan pada jaringan akibat kesalahan dan kelalaian manusia di Diskominfostandi Kota Bekasi.
3. Menampilkan hasil kinerja sistem deteksi dan prevensi serangan *malware* secara *real-time* melalui *browser*.

1.5 Ruang Lingkup

Ruang lingkup penelitian ini adalah :

1. Snort hanya bisa melakukan deteksi dan prevensi ketika *Server* menyala.
2. Maltrail hanya dapat digunakan untuk mendeteksi situs yang terinfeksi *malware*, tetapi tidak dapat mencegah akses ke situs tersebut.
3. Pengujian serangan siber berupa serangan *Ping of Death*, SSH *Brute Force Attack* dan ICMP *Flood.*