1 PENDAHULUAN

1.1 Latar Belakang

Salah satu ancaman utama di Internet saat ini yaitu *software* berbahaya yang sering disebut sebagai *malware*. Faktanya, sebagian besar masalah keamanan Internet disebabkan oleh *malware*. *Malware* hadir dalam berbagai bentuk dan variasi, seperti *virus*, *worm*, *botnet*, *rootkit*, *trojan horse*, dan program *denial tools* lainnya. Dalam penyebarannya, malware mengeksploitasi kerentanan *software* di *browser* dan sistem operasi, atau menggunakan teknik *social engineering* untuk mengelabui pengguna agar dapat menjalankan program-program berbahaya. (Bayer *et al*. 2009).

Perusahaan anti-virus Malwarebytes (2019) merilis laporan tahunan tentang kondisi *malware* di seluruh dunia dalam jurnal "*2019 States of Malware*". Laporan tersebut menyatakan bahwa terdapat kurang lebih 750 juta serangan *malware* yang terdeteksi menyerang komputer *end-user* (personal) sepanjang tahun 2017–2018 di seluruh dunia. Kemudian, terdapat kurang lebih 71 juta *malware* yang terdeteksi menyerang pengguna *business-user* (perusahaan/industri/lembaga) sepanjang tahun 2017–2018.

Berdasarkan penelitian tersebut, diperlukan adanya sistem keamanan jaringan untuk *monitoring* dan pencegahan dari serangan *malware* yang melintasi jaringan *server* pada sektor OPD (Organisasi Perangkat Daerah) dan pusat-pusat pelayanan publik di wilayah Kota Tangerang Selatan. Hal ini bertujuan sebagai langkah pencegahan dari terjadinya kerugian-kerugian yang disebabkan oleh serangan *malware* di jaringan internet. Oleh karena itu, dibuatlah Sistem Pendeteksi dan Pencegah Serangan *Malware* dengan Sensor Maltrail pada Jaringan *Server* di Diskominfo Tangerang Selatan. Sistem yang dibuat akan diberi nama DEMALWARE (Pendeteksi dan Pencegah Malware). *Software* yang digunakan untuk melakukan pendeteksian *malware*, yakni bernama Maltrail (Malware Trail). Cara kerja dari *software* ini mirip dengan mekanisme "sensor" yang memindai seluruh aktivitas *traffic* pada jaringan *server*. Kemudian, s*oftware* yang digunakan untuk melakukan *blocking* 'pencegahan' serangan *malware*, yaitu Fail2Ban. Pada purwarupa yang akan diterapkan, *software* Maltrail dan Fail2Ban yang telah ada, dikonfigurasi sedemikian rupa agar dapat saling berkolaborasi pada sistem keamanan jaringan. Dari beberapa penelitian lanjutan yang telah dilakukan, sistem pendeteksi serangan *malware* ini dapat dikembangkan lebih jauh pada sisi otomatisasi dalam *monitoring* dan pencegahan *malware traffic* yang ada secara *real-time* beserta fitur notifikasi melalui aplikasi Telegram dan pelaporan berkas melalui *e-mail* secara berkala.

Beberapa penelitian yang telah dilakukan berkaitan dengan sistem Maltrail sebagai basis dari sistem *malware monitoring*, yaitu (Bayer *et al.* 2009; Suciu *et al.* 2019; Hudzaifah *et al.* 2019; McGraw dan Morrisett 2000; Idika dan Mathur 2007).

1.2 Tujuan

Tujuan dari Penerapan Sistem Pendeteksi dan Pencegah Serangan *Malware* dengan Sensor Maltrail pada Jaringan *Server* di Diskominfo Tangerang Selatan, yakni sebagai berikut:

1. Mendeteksi paket-paket yang masuk melalui jalur *network server* yang terindikasi dan terdeteksi sebagai *malware* berdasarkan *repository* yang disediakan oleh sejumlah lembaga anti-virus internasional
2. Mencegah aktivitas penyebaran *malware* dengan melakukan *blocking* terhadap alamat IP sumber *malware* berdasarkan parameter intensitas serangan *malware*
3. Melaporkan status keadaan sistem dan IP yang diblokir oleh sistem melalui aplikasi Telegram secara *real-time*
4. Menampilkan hasil laporan pemindaian data *log traffic malware* melalui *browser* secara *real-time* serta mengirimkan berkas laporannya ke *e-mail* secara periodik yang ditetapkan

1.3 Manfaat

Manfaat dari Penerapan Sistem Pendeteksi dan Pencegah Serangan *Malware* dengan Sensor Maltrail pada Jaringan *Server* di Diskominfo Tangerang Selatan, yakni sebagai berikut:

1) Sistem ini dapat melakukan monitoring dan pembatasan paket-paket yang masuk melalui jalur *network server* yang diindikasi dan dideteksi sebagai *malware* secara otomatis
2) Sistem ini dapat melaporkan IP yang diblokir oleh sistem melalui notifikasi Telegram, sehingga administrator dapat me-*monitoring* sistem secara *real-time*
3) Sistem ini dapat membantu administrator dalam merekapitulasi hasil pemindaian data *log traffic malware* melalui e-*mail* secara otomatis berdasarkan periodik yang ditetapkan

1.4 Ruang Lingkup

Batasan masalah yang dibahas dalam Penerapan Sistem Pendeteksi dan Pencegah Serangan *Malware* dengan Sensor Maltrail pada Jaringan *Server* di Diskominfo Tangerang Selatan, yakni sebagai berikut:

1) *Server* harus selalu dalam keadaan menyala dan terhubung dengan internet
2) Purwarupa sistem ini hanya merekapitulasi *log traffic* dengan parameter satu jam sekali
3) Sumber *malware blacklists* yang digunakan hanya bersumber dari situs Github resmi Developer *software* Maltrail
4) Kategori *malware* yang diblokir hanya ditambahkan pada *jail* secara manual
5) Pengujian hanya dilakukan dengan metode PING terhadap *malware*

6) Sistem ini hanya dapat me-*monitoring* dan membatasi paket-paket *malware* yang masuk melalui jalur *network server*

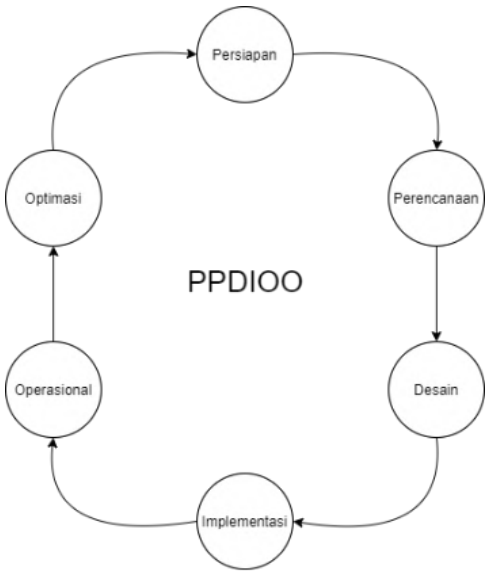
2 METODE KAJIAN

2.1 Tempat dan Waktu PKL

Kegiatan Praktik Kerja Lapangan (PKL) berlangsung selama 45 hari kerja, terhitung mulai tanggal 2 Januari 2020 sampai 6 Maret 2020. Kegiatan PKL dilaksanakan di Diskominfo Kota Tangerang Selatan. Hari kerja pelaksanaan PKL mengikuti peraturan yang berlaku, yakni Senin sampai Jumat. Kegiatan dimulai pukul 07.30–16.00 WIB di Network Operation Center (NOC).

2.2 Metode Bidang Kajian

Metode yang digunakan dalam Penerapan Sistem Pendeteksi dan Pencegah Serangan *Malware* dengan Sensor Maltrail pada Jaringan *Server* di Diskominfo Tangerang Selatan adalah PPDIOO (Prepare, Plan, Design, Implement, Operate, dan Optimize). PPDIOO adalah metodologi Cisco yang mendefinisikan siklus hidup berkelanjutan dari layanan yang dibutuhkan terhadap suatu jaringan. (Sivasubramanian *et al*, 2010). Metode ini cocok untuk mendesain pengembangan keamanan jaringan yang pendekatannya terpusat pada administrator. Pada metode ini terdapat 6 tahapan, yaitu persiapan, perencanaan, desain, implementasi, operasional, dan optimasi. Gambar 1 menunjukkan alur dari metode kerja yang digunakan.



Gambar 1 Metode kerja penerapan sistem