BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan merupakan hal yang sangat penting, terutama di era teknologi sekarang ini. Banyak instansi atau organisasi yang tidak sadar dan tidak memperdulikan terkait masalah keamanan. Jika mendapat serangan dan terjadi kerusakan sistem, banyak biaya yang harus dikeluarkan untuk melakukan perbaikan sistem. Untuk itu sudah selayaknya investasi di bidang keamanan jaringan lebih diperhatikan, untuk mencegah kerusakan dari ancaman serangan yang saat ini semakin beragam. Terlebih lagi saat komputer server terhubung dengan internet maka serangan pun akan semakin meningkat. Untuk itu perlu dipersiapkan keamanan untuk mengamankan dan meminimalisir ancaman pada jaringan dan server khusus penyedia jasa layanan internet [**1**].

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*, *spyware* dan program *denial tools* lainnya. Setiap tahun, banyak sistem komputer di seluruh dunia akan rusak akibat malware. Baru-baru ini melaporkan bahwa file, sistem, email dan server masing-masing telah terinfeksi oleh virus *Cookie.Weborama*, Cookie.Rub, dan Exploit.Iframe. Meskipun demikian pada tahun 2019 serangan oleh virus *Ransomware* dan *PowerShell* baru telah meningkat sebesar 118% dan 460% [**2**].

Perusahaan anti-virus Malwarebytes (2019) merilis laporan tahunan tentang kondisi *malware* diseluruh dunia dalam jurnal "*2019 States of Malware*". Laporan tersebut menyatakan bahwa terdapat kurang lebih 750 juta serangan *malware* yang terdeteksi menyerang computer 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. Sayangnya, jumlah yang meningkat dan keragaman *malware* membuat teknik keamanan klasik, seperti pemindai *anti-virus* tidak efektif, dan sebagai konsekuensinya, jutaan host di Internet saat ini terinfeksi dengan perangkat lunak berbahaya [**3**].

Berdasarkan penelitian tersebut, dibutuhkan sistem keamanan jaringan untuk monitoring dan pencegahan dari serangan *malware* yang keluar masuk dan melintasi perangkat jaringan di Diskominfo Sumedang. Berdasarkan survei yang dilakukan, perangkat firewall yang berfungsi untuk memblokir serangan yang masuk ke server terkadang tidak bekerja secara maksimal, firewall tersebut justru memblokir jaringan untuk akses aplikasi pegawai, kemudian ada insiden mengenai file-file dan database di server Diskominfo sumedang yang tidak bisa diakses akibat dari *malware*. Melihat hal tersebut solusi lain sebagai sistem tambahan yang penerapannya di server yaitu dengan sensor Maltrail dan Fail2Ban untuk meminimalisir serangan yang tidak terblokir oleh firewall dan sebagai sistem monitoring aktivitas *malware* trafik pada jaringan server Diskominfo Sumedang.

Beberapa penelitian yang telah dilakukan berkaitan dengan Maltrail sebagai sistem *malware* monitoring, yaitu [**4**]-[**7**].

1.2 Tujuan dan Manfaat

Adapun tujuan dari penulisan Proyek Akhir ini, sebagai berikut.

1. Dapat mendeteksi paket-paket yang masuk melalui jaringan server yang terindikasi dan terdeteksi sebagai *malware*.
2. Dapat melakukan *blocking* terhadap alamat IP dari sumber *malware.*
3. Dapat melaporkan status sistem dan IP yang di blokir melalui aplikasi Telegram secara *real-time.*
4. Dapat menampilkan hasil laporan pemindaian data *log traffic malware* melalui *browser* secara *real-time.*

Manfaat dari penulisan Proyek Akhir ini, sebagai berikut.

1. Dapat melakukan monitoring dan melakukan *blocking* terhadap paket-paket yang terindikasi dan terdeteksi sebagai *malware* secara otomatis pada jaringan server.
2. Dapat membantu administrator dalam me-monitoring jaringan secara *real-time.*
3. Dapat membantu administrator dalam mendapatkan hasil rekapitulasi pemindaian *log traffic malware.*
4. Dapat membantu sistem anti virus dalam mengidentifikasi jenis-jenis *malware*, jejak IP, nama domain, alamat URL atau IP.

1.3 Rumusan Masalah

Adapun rumusan masalah dari Proyek Akhir ini, sebagai berikut.

1. Apa saja fungsi dan fitur jaringan yang akan diterapkan pada sistem tersebut?
2. Bagaimana implementasi penggunaan sensor Maltrail dan Fail2Ban dalam mendeteksi dan mencegah serangan *malware* pada jaringan server dengan push notifikasi?
3. Bagaimana hasil dan analisa pengukuran intensitas trafik pada server setelah dilakukan pengujian *malware* ?

1.4 Batasan Masalah

Adapun batasan masalah dari Proyek Akhir ini, sebagai berikut.

1. Server Maltrail dan Fail2Ban harus selalu dalam keadaan *running* dan terhubung dengan internet.
2. Sistem diakses melalui aplikasi *web browser.*
3. Sistem ini hanya bisa merekapitulasi *log traffic malware.*
4. Sistem yang digunakan hanya bersumber dari Github resmi Developer *software* Maltrail.

1.5 Metodologi

Adapun metodologi pada penelitian Proyek Akhir ini, sebagai berikut.

1. Studi Literatur

   Studi literatur dilakukan dengan mengumpulkan literatur-literatur dan kajian-kajian yang berkaitan dengan permasalahan yang ada pada penelitian Proyek Akhir ini, baik berupa buku referensi, artikel, maupun *e-journal* yang berhubungan dengan cara kerja Maltrail menggunakan python, Fail2Ban, *OS Debian* dan implementasi sistem.

2. Analisis Kebutuhan Sistem

   Analisis kebutuhan sistem dilakukan dengan mengumpulkan kebutuhan *software* dan cara kerja sistem dalam mengintegrasikan sistem yang akan digunakan dalam proyek akhir.

3. Perencanaan Sistem

   Perencanaan sistem dilakukan dengan melakukan analisis sistem yang akan dibangun, dalam hal ini analisis sistem dalam mendeteksi dan mecegah serangan *malware* pada jaringan server menggunakan Maltrail dan Fail2Ban.

4. Implementasi

   Langkah selanjutnya adalah implementasi sistem. Implementasi ini termasuk pembuatan, instalasi dan konfigurasi Maltrail, Fail2Ban, Telegram.

5. Pengujian

   Pengujian dilakukan setelah pembuatan, instalasi dan konfigurasi *software* berjalan dengan baik. Kemudian dilakukan pengujian dengan beberapa metode serangan.

6. Pembuatan Laporan.

   Pada langkah ini semua metode yang telah dilakukan, dibuat dokumentasi dari Proyek Akhir ini.

1.6 Sistematika Penulisan

Dalam penulisan Proyek Akhir terdiri atas lima bab, dengan keterangan sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini berisi latar belakang, rumusan masalah, tujuan dan manfaat, batasan masalah, metodologi penelitian, serta sistematika penulisan.

BAB II DASAR TEORI

Pada bab ini membahas tentang teori pendukung pengerjaan Proyek Akhir, seperti *malware (malicious)*, cara kerja Maltrail dan Fail2Ban dan lain sebagainya.

BAB III ANALISIS DAN PERANCANGAN

Pada bab ini membahas tentang deskripsi Proyek Akhir, alur pengerjaan Proyek Akhir, analisis kebutuhan dan perancangan sistem yang akan diterapkan.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Pada bab ini membahas tentang implementasi sistem dan pengujian.

BAB V PENUTUP

Pada bab ini membahas tentang kesimpulan dari pengerjaan Proyek Akhir dan saran untuk pembaca yang akan mengambil penelitian dengan topik yang sama.