BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah memberikan kemudahan bagi berbagai instansi dalam melakukan pengelolaan, penyimpanan, dan pertukaran data melalui jaringan komputer. Pemanfaatan jaringan komputer memungkinkan proses pelayanan dan penyampaian informasi dilakukan secara lebih cepat dan efisien. Namun, meningkatnya ketergantungan terhadap layanan berbasis jaringan juga diikuti dengan meningkatnya ancaman keamanan yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data.

Ancaman keamanan jaringan dapat berasal dari berbagai aktivitas, seperti *port scanning*, *brute force*, SQL Injection, *Cross-Site Scripting* (XSS), *Denial of Service* (DoS), eksploitasi kerentanan layanan, dan percobaan penyusupan ke dalam sistem. Serangan tersebut dapat digunakan untuk mencari port yang terbuka, memperoleh informasi layanan, menebak kombinasi nama pengguna dan kata sandi, menyisipkan perintah berbahaya, mengganggu ketersediaan layanan, atau memperoleh akses tidak sah ke dalam server. Apabila tidak ditangani dengan mekanisme keamanan yang memadai, aktivitas tersebut dapat menyebabkan pencurian data, perubahan informasi, gangguan pelayanan, dan kerusakan sistem [1].

Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkalis merupakan salah satu instansi pemerintah yang mengelola informasi kependudukan masyarakat. Data yang dikelola memiliki sifat penting dan sensitif sehingga keamanan jaringan menjadi bagian yang perlu diperhatikan dalam mendukung keberlangsungan pelayanan. Berdasarkan hasil observasi terhadap catatan sistem keamanan jaringan, ditemukan lebih dari 19.100 catatan pemblokiran alamat IP dinamis yang berkaitan dengan aktivitas seperti *port scanning* dan *SSH brute force*. Sebagian aktivitas tersebut berasal dari alamat IP luar negeri dan menunjukkan adanya percobaan akses terhadap layanan jaringan secara berulang.

Banyaknya catatan pemblokiran menunjukkan bahwa layanan jaringan dapat menjadi sasaran berbagai aktivitas mencurigakan. Sistem keamanan yang digunakan perlu memiliki kemampuan untuk mendeteksi pola serangan, mencatat informasi kejadian, melakukan tindakan pencegahan, dan menyampaikan informasi kepada administrator. Apabila proses pemantauan hanya dilakukan dengan memeriksa log secara manual, administrator berpotensi terlambat mengetahui adanya serangan. Oleh karena itu, diperlukan sistem keamanan yang dapat melakukan deteksi dan pemblokiran secara otomatis serta memberikan notifikasi serangan secara *real-time*.

Salah satu mekanisme yang dapat digunakan untuk meningkatkan keamanan jaringan adalah *Intrusion Prevention System* (IPS). IPS merupakan sistem keamanan yang melakukan pemantauan terhadap lalu lintas jaringan untuk mendeteksi aktivitas yang sesuai dengan pola atau aturan serangan. Sistem tersebut juga dapat dikombinasikan dengan mekanisme pencegahan untuk menghentikan atau membatasi akses dari sumber serangan [2].

Suricata merupakan perangkat lunak keamanan jaringan berbasis *open source* yang dapat digunakan sebagai *Intrusion Detection System* (IDS) maupun bagian dari sistem IPS. Suricata mampu melakukan pemeriksaan paket secara mendalam atau *Deep Packet Inspection* serta mendeteksi aktivitas jaringan berdasarkan aturan atau *signature* yang telah dikonfigurasi. Suricata juga mendukung pemrosesan secara *multi-thread* sehingga dapat menganalisis lalu lintas jaringan dengan memanfaatkan beberapa inti prosesor [3].

Pada penerapannya, Suricata dapat menghasilkan peringatan dan mencatat informasi serangan ke dalam file log. Namun, hasil deteksi tersebut masih memerlukan mekanisme tambahan agar alamat IP penyerang dapat diblokir secara otomatis. Dalam penelitian ini, Suricata diintegrasikan dengan Fail2Ban. Fail2Ban berfungsi membaca pola serangan pada log Suricata, mengambil alamat IP sumber, dan menjalankan aturan pemblokiran melalui *firewall* apabila aktivitas tersebut telah memenuhi batas yang dikonfigurasi.

Sistem juga diintegrasikan dengan Telegram Bot sebagai media penyampaian notifikasi kepada administrator. Notifikasi tersebut dapat berisi

informasi mengenai alamat IP sumber, jenis serangan, waktu kejadian, dan status pemblokiran. Penggunaan Telegram Bot memungkinkan administrator memperoleh informasi serangan melalui perangkat seluler tanpa harus terus-menerus memantau terminal atau membuka file log pada server.

Penelitian ini membangun sebuah purwarupa sistem keamanan jaringan dengan mengintegrasikan Suricata, Fail2Ban, dan Telegram Bot. Seluruh proses implementasi dan pengujian dilakukan pada lingkungan terisolasi menggunakan Oracle VM VirtualBox. Lingkungan pengujian terdiri atas Ubuntu Server 24.04.3 LTS sebagai server target dan Kali Linux sebagai mesin penyerang. Pengujian tidak dilakukan pada server produksi Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkalis sehingga tidak memengaruhi layanan operasional instansi.

Sistem diuji menggunakan 14 skenario serangan, yaitu *web brute force*, SQL Injection, *Cross-Site Scripting*, FTP *brute force*, *port scanning*, SSH *brute force*, DoS Hulk, DoS GoldenEye, DoS Slowloris, DoS SlowHTTPTest, *vulnerability scanning*, *packet flood*, *infiltration/reverse shell*, dan simulasi Heartbleed. Selain pengujian serangan, dilakukan juga pengujian trafik normal untuk mengetahui apakah sistem melakukan kesalahan deteksi atau pemblokiran terhadap aktivitas pengguna yang sah.

Pengujian difokuskan pada kemampuan sistem dalam menghasilkan peringatan Suricata, melakukan pemblokiran alamat IP melalui Fail2Ban, dan mengirimkan notifikasi melalui Telegram Bot. Hasil pengujian juga diukur berdasarkan tingkat keberhasilan deteksi, tingkat keberhasilan pemblokiran, tingkat keberhasilan pengiriman notifikasi, kemungkinan *false positive*, dan waktu respons sistem terhadap serangan.

Berdasarkan uraian tersebut, penelitian ini mengambil judul "Penggunaan Suricata dan Fail2Ban sebagai Intrusion Prevention System (IPS) untuk Mengatasi Serangan Jaringan dengan Notifikasi Telegram (Studi Kasus pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkalis)". Penelitian ini diharapkan dapat menghasilkan purwarupa sistem keamanan jaringan berbasis *open source* yang dapat membantu proses deteksi, pencegahan, pemblokiran, dan penyampaian informasi serangan secara lebih cepat dan terstruktur.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana merancang dan membangun purwarupa *Intrusion Prevention System* menggunakan Suricata dan Fail2Ban pada lingkungan virtual Oracle VM VirtualBox?
2. Bagaimana kemampuan sistem dalam mendeteksi dan memblokir alamat IP sumber pada 14 skenario serangan jaringan yang diuji?
3. Bagaimana mengintegrasikan Telegram Bot agar dapat mengirimkan informasi serangan dan pemblokiran kepada administrator secara *real-time*?
4. Berapa tingkat keberhasilan deteksi, pemblokiran, dan pengiriman notifikasi serta berapa waktu respons sistem dalam menangani skenario serangan yang diuji?

1.3 Batasan Masalah

Agar penelitian lebih terarah dan sesuai dengan tujuan yang telah ditetapkan, batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Implementasi dan pengujian sistem dilakukan pada lingkungan virtual menggunakan Oracle VM VirtualBox dan tidak diterapkan pada server produksi Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bengkalis.
2. Lingkungan pengujian menggunakan satu mesin virtual Ubuntu Server 24.04.3 LTS sebagai server target dan satu mesin virtual Kali Linux sebagai mesin penyerang.
3. Suricata versi 7.0.3 digunakan sebagai mesin deteksi serangan berdasarkan aturan atau *signature* yang dikonfigurasi.
4. Fail2Ban digunakan untuk membaca log hasil deteksi Suricata dan melakukan pemblokiran alamat IP sumber melalui *firewall*.
5. Telegram Bot API digunakan untuk mengirimkan notifikasi serangan dan informasi pemblokiran kepada administrator.

6. Pengujian dilakukan terhadap 14 skenario serangan, yaitu:

   a. *Web Brute Force* menggunakan Hydra.

   b. SQL Injection.

   c. *Cross-Site Scripting* (XSS).

   d. FTP *Brute Force* menggunakan Patator.

   e. *Port Scanning* menggunakan Nmap.

   f. SSH *Brute Force* menggunakan Patator.

   g. DoS Hulk.

   h. DoS GoldenEye.

   i. DoS Slowloris.

   j. DoS SlowHTTPTest.

   k. *Vulnerability Scanning* menggunakan Nikto.

   l. *Packet Flood* menggunakan *hping3*.

   m. *Infiltration* atau *Reverse Shell* menggunakan Netcat.

   n. Simulasi Heartbleed.

7. Pengujian trafik normal dilakukan sebagai pembanding untuk mengetahui kemungkinan terjadinya *false positive* atau pemblokiran terhadap pengguna yang sah.

8. Pengujian *packet flood* menggunakan *hping3* dikategorikan sebagai serangan DoS karena serangan dilakukan dari satu mesin penyerang.

9. Pengujian difokuskan pada tingkat keberhasilan deteksi, pemblokiran alamat IP, pengiriman notifikasi Telegram, kemungkinan *false positive*, serta waktu respons sistem.

10. Data jaringan Disdukcapil Kabupaten Bengkalis digunakan sebagai dasar dalam memahami kebutuhan dan merancang purwarupa. Alamat IP internal,

kata sandi, dan konfigurasi sensitif instansi tidak dicantumkan dalam laporan.

11. Sistem bekerja berdasarkan aturan atau *signature* yang telah dikonfigurasi dan tidak membahas metode deteksi berbasis *machine learning*.
12. Penelitian tidak membahas proses pemulihan data, analisis *malware*, forensik digital lanjutan, maupun penanganan serangan yang berasal dari alamat IP yang telah dipalsukan.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Merancang dan membangun purwarupa *Intrusion Prevention System* menggunakan Suricata dan Fail2Ban pada lingkungan virtual Oracle VM VirtualBox.
2. Mengimplementasikan Suricata untuk mendeteksi aktivitas serangan dan Fail2Ban untuk melakukan pemblokiran alamat IP sumber secara otomatis.
3. Mengintegrasikan Telegram Bot sebagai media notifikasi serangan dan pemblokiran kepada administrator secara *real-time*.
4. Menguji sistem menggunakan 14 skenario serangan dan satu kategori trafik normal.
5. Mengukur tingkat keberhasilan deteksi, tingkat keberhasilan pemblokiran, tingkat keberhasilan pengiriman notifikasi, kemungkinan *false positive*, dan waktu respons sistem.
6. Menghasilkan purwarupa sistem keamanan jaringan berbasis *open source* yang dapat digunakan sebagai referensi dalam pengembangan sistem keamanan jaringan.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Bagi Penulis

Penelitian ini dapat menambah pengetahuan dan pengalaman penulis dalam merancang, membangun, mengonfigurasi, dan menguji sistem keamanan jaringan menggunakan Suricata, Fail2Ban, Telegram Bot, Ubuntu Server, dan Kali Linux.

2. Bagi Instansi

Penelitian ini dapat memberikan gambaran rancangan sistem keamanan jaringan berbasis *open source* yang mampu melakukan deteksi, pemblokiran alamat IP, pencatatan kejadian, dan penyampaian notifikasi serangan kepada administrator.

3. Bagi Administrator Jaringan

Purwarupa yang dibangun dapat menjadi referensi untuk membantu administrator dalam melakukan pemantauan aktivitas jaringan serta memperoleh informasi serangan tanpa harus terus-menerus memeriksa file log secara manual.

4. Bagi Politeknik Negeri Bengkalis

Hasil penelitian dapat menjadi tambahan referensi akademik mengenai penerapan *Intrusion Prevention System*, khususnya integrasi Suricata, Fail2Ban, dan Telegram Bot pada lingkungan virtual.

5. Bagi Penelitian Selanjutnya

Penelitian ini dapat dijadikan dasar untuk pengembangan sistem keamanan jaringan yang lebih luas, seperti penggunaan beberapa mesin penyerang, penerapan pada jaringan fisik, integrasi dengan sistem pemantauan terpusat, pengembangan dashboard, atau penggunaan metode deteksi berbasis anomali dan *machine learning*.