**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNOLOGI INFORMASI**

**INSTITUT TEKNOLOGI SEPULUH NOPEMBER**

**USULAN TUGAS AKHIR**

# **IDENTITAS PENGUSUL**

**Nama : MUHAMMAD MAHRUS SYAMSURRIJAL**

**NRP : 5109100125**

**Dosen Wali** **:** **Diana Purwitasari, S.Kom., M.Sc.**

1. **JUDUL TUGAS AKHIR**

**“Sistem Pendeteksi Serangan Adaptif dengan Menggunakan Algoritma Genetik”**

***“Adaptive Intrusion Detection System using Genetic Algorithm”***

1. **URAIAN SINGKAT**

Sistem pendeteksi serangan berdasarkan pola serangan sangat bergantung kepada pola atau aturan yang disediakan oleh administrator jaringan. Hal ini bisa dianggap sebagai suatu kelemahan, karena serangan jenis baru dapat muncul ketika basis data pola serangan belum diperbarui oleh administrator jaringan. Sedangkan sistem pendeteksi serangan berdasarkan keanehan pada jaringan ditujukan untuk mendeteksi serangan yang sebelumnya tidak diketahui. Namun kelemahannya adalah sistem ini terlalu sensitif sehingga keanehan sedikit saja dapat memicu alarm peringatan. Oleh karena itu, dibutuhkan suatu sistem pendeteksi adaptif yang mampu mempelajari pola-pola serangan yang akan terjadi.

Sistem yang akan dibangun ini menggunakan *Supervised Classifier System* (UCS) sebagai *machine learning* yang akan mempelajari paket data yang masuk dan mampu membuat pola-pola serangan yang mungkin terjadi ke dalam basis data pola serangan. Pada mulanya, sistem membutuhkan contoh input untuk mengisi basis data pola serangan yang masih kosong. Setelah basis data terisi dengan pola serangan, sistem mampu menerima input yang sebenarnya berupa paket data dari internet. Untuk mempermudah dan mempercepat proses pembelajaran pola, maka paket data yang masuk akan dinormalisasi terlebih dahulu sebelum diproses. Paket data yang telah dinormalisasi akan dicocokkan terlebih dahulu dengan basis data pola serangan untuk mengetahui apakah paket tersebut termasuk serangan atau bukan. Jika paket tersebut tidak cocok dengan basis data yang ada, maka paket data akan dimasukkan ke dalam *machine learning* untuk dipelajari lebih lanjut.

Tujuan dari pengerjaan tugas akhir ini adalah membangun sistem pendeteksi serangan yang dapat secara adaptif memperbarui basis data pola-pola serangan untuk mengantisipasi serangan-serangan baru yang sebelumnya belum diketahui. Lebih jauh lagi, aplikasi yang akan dihasilkan ini diharapkan mampu mengamankan server dari serangan-serangan, sehingga informasi yang tersimpan tetap terjaga.

1. **PENDAHULUAN**
   1. **LATAR BELAKANG**

Dewasa ini, jenis-jenis serangan terhadap jaringan komputer semakin berkembang seiring dengan berkembangnya teknologi di bidang keamanan jaringan. Tidak jarang ketika sistem pertahanan diperkuat, para *hacker* juga menemukan cara lain untuk masuk ke dalam sistem.

Ada dua prinsip utama yang digunakan pada sistem pendeteksi serangan, yaitu deteksi berdasarkan keanehan pada jaringan, dan deteksi berdasarkan pola serangan[6]. Pendekatan deteksi berdasarkan keanehan pada jaringan memodelkan aktivitas jaringan dalam keadaan normal sesuai dengan yang didefinisikan oleh administrator jaringan, seperti besar *bandwidth* yang digunakan, protokol apa yang digunakan, serta nomor port yang sedang tersambung[3]. Jika ada keanehan dalam jaringan tersebut, maka sistem akan memberi peringatan kepada administrator. Namun pendekatan jenis ini memiliki kelemahan karena walaupun terdapat keanehan sedikit saja akan memicu alarm peringatan kepada administrator jaringan.

Pendekatan yang kedua yaitu deteksi berdasarkan pola dari serangan. Pendekatan ini bergantung kepada basis data dari pola-pola serangan yang telah diketahui sebelumnya. Jika ada suatu paket yang memiliki pola sama dengan pola yang ada di basis data, maka paket ini tidak akan diteruskan. Pendekatan ini merupakan yang paling banyak digunakan dibanding dengan pendekatan sebelumnya. Namun pendekatan ini tetap memiliki kelemahan. Basis data pola-pola serangan ini perlu diperbarui terus-menerus agar mampu mengatasi serangan-serangan yang terus berubah. Saat ini, proses pembuatan dan pembaruan basis data umumnya dilakukan secara manual. Tidak jarang ketika basis data sedang diperbarui, serangan terhadap jaringan computer telah terjadi[6].

Pada tugas akhir ini, penulis mengimplementasikan sistem pendeteksi serangan yang dapat secara adaptif mempelajari pola-pola dari serangan yang sebelumnya tidak diketahui dengan menggunakan pendekatan *machine learning*.

* 1. **RUMUSAN MASALAH**

Berdasarkan latar belakang yang telah diuraikan diatas, terdapat beberapa permasalahan yang dapat dirumuskan sebagai berikut:

1. Bagaimana menangkap paket-paket data yang akan dikirim ke server?
2. Bagaimana menormalisasi paket-paket sehingga lebih mudah diolah oleh aplikasi?
3. Bagaimana membangun *machine learning*?
   1. **BATASAN MASALAH**

Adapun batasan masalah pada tugas akhir ini adalah sebagai berikut :

1. Aplikasi ini berjalan di sistem operasi linux.
2. Aplikasi ini memproses paket data yang telah dinormalisasi
   1. **TUJUAN DAN MANFAAT TUGAS AKHIR**

Adapun tujuan dari pengerjaan tugas akhir ini adalah membangun sistem pendeteksi serangan pada jaringan berdasarkan pola serangan, yang memiliki kemampuan untuk memperbarui basis data pola-pola suatu serangan.

Sedangkan manfaat dari pengerjaan tugas akhir ini adalah sebagai berikut :

1. Mengamankan server dari serangan.
2. Membantu administrator jaringan dalam memperbarui basis data pola-pola serangan.
3. **TINJAUAN PUSTAKA**
   1. ***Intrussion Detection System***

*Intrussion Detection System (IDS)* adalah sistem yang berfungsi sebagai alarm peringatan ketika terjadi serangan terhadap jaringan komputer. Ada dua prinsip utama dalam sistem pendeteksi serangan ini, yaitu *anomaly detection* dan *signature detection*. IDS yang berjenis *anomaly detection* akan memantau keadaan jaringan seperti *bandwidth, port,* dan *protocol* yang biasanya digunakan. Jika terjadi keanehan pada jaringan, maka IDS akan memberi alarm peringatan kepada administrator jaringan. Masalahnya adalah IDS yang berjenis *anomaly detection* sering memberi alarm palsu karena keanehan sedikit saja yang terjadi pada jaringan akan mampu memicu alarm peringatan.

Sedangkan IDS yang berjenis *signature detection* akan mencocokkan paket yang dating dengan pola-pola serangan yang telah diketahui sebelumnya. Permasalahan pada IDS jenis ini adalah karena cara pendeteksian serangan bergantung pada basis data pola-pola serangan, sehingga basis data harus selalu diperbarui oleh administrator jaringan. Jika basis data belum diperbarui, maka serangan yang sebelumnya tidak diketahui dapat menyerang jaringan computer[1].

* 1. ***Genetic Algorithm***

*Genetic Algorithm* *(GA)* merupakan algoritma yang terinspirasi dari teori evolusi Darwin. Algoritma ini memanipulasi individu dari suatu populasi yang merepresentasikan solusi dari suatu permasalahan. Pada mulanya, satu set solusi secara random dibentuk oleh sistem dan ditampung ke dalam satu populasi. Setelah itu, GA akan memilih beberapa individu yang dianggap paling mungkin menjadi solusi. Individu yang terpilih akan dimutasi dengan menggunakan operator genetik. Operator genetik yang dimaksud terdiri dari dua jenis, *crossover operator* dan *mutation operator*. *Crossover operator* akan membentuk individu baru dengan cara salung menukar bagian dari individu induknya. Sedangkan *mutation* *operator* membentuk individu baru dengan cara mengubah secara random bagian dari individu induk. Lalu, individu yang baru terbentuk akan dievaluasi[7].

* 1. ***Learning Classifier System***

*Learning Classifier System (LCS)* pertama kali ditemukan oleh Holland pada tahun 1975. LCS adalah sistem yang digunakan untuk berinteraksi dengan lingkungan sehingga dapat memberikan respon yang sesuai dengan lingkungan. Pada perkembangannya, LCS terbagi menjadi dua jenis, yaitu “Pittsburgh” yang dikembangkan oleh Smith, dan “Michigan” yang dikembangkan oleh Holland. Pada jenis yang disebut “Pittsburgh”, proses pembelajaran dan pengambilan keputusan hanya didasarkan pada algoritma genetik (GA). Sedangkan pada jenis yang disebut Michigan”, proses pembelajaran dan pengambilan keputusan juga dilakukan oleh mekanisme *Reinforcement Learning (RL)* yang berguna untuk memilih solusi yang sebaiknya dipilih sehingga dapat memperkuat proses pengambilan keputusan[7].

1. **METODOLOGI**

Sistem pendeteksi serangan yang akan dirancang ini akan menggunakan *Supervised Classifier Systems (UCS)*[2] sebagai *machine learning* untuk memperbarui basis data pola-pola serangan. Pada mulanya, basis data dalam keadaan kosong dan paket data akan langsung diarahkan ke *learning machine*.



Gambar 1. Alur Data [6]

Namun jika basis data telah terisi dengan pola-pola dari suatu serangan yang telah dikenal, paket data akan dibandingkan terlebih dahulu untuk menentukan apakah termasuk dalam serangan atau bukan. Input akan diteruskan ke learning machine ketika tidak ada pola yang cocok di basis data.

Di dalam *learning machine*, terjadi dua fase yaitu *training phase* dan *test phase*.Selama *training phase*, UCS mempelajari contoh-contoh input untuk membentuk aturan baru yang mungkin diperlukan. Contoh input didapatkan dari administrator jaringan[4]. Input berupa contoh paket data yang telah diberi label akan dicocokkan dengan sekumpulan *classifier* yang dibentuk oleh sistem di dalam P. *Classifier* yang cocok dengan input paket data akan diletakkan di dalam M. Dikatakan cocok apabila *classifier* tersebut memiliki kondisi yang sama dengan paket data. Setelah itu, parameter yang menunjukkan kualitas dari *classifier* tersebut diperbarui. *Classifier* di dalam M yang memiliki *class* atau *action* yang sama dengan input paket data, akan disimpan ke dalam C. Algoritma Genetic (GA) akan diaplikasikan pada C untuk membentuk aturan baru.

Pada bagian *test phase*, input sebenarnya akan dimasukkan ke dalam *learning machine*. Untuk setiap input yang masuk, akan dicocokkan dengan P, dimana P adalah sekumpulan *classifier* hasil dari *training phase* sebelumnya. *Classifier* dengan kondisi yang cocok akan dimasukkan ke dalam M. Untuk setiap aksi/*class* dalam M, akan dibentuk *system prediction*, dan aksi dengan *system prediction* paling tinggi akan dipilih.



Gambar 2. Training Phase [6]



Gambar 3. Test Phase [6]

1. **JADWAL PEMBUATAN TUGAS AKHIR**

Berikut merupakan jadwal pengerjaan tugas akhir ini:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Tahapan** | **2013** | | | | | | | | | | | | | | | | | | | |
| **Februari** | | | | **Maret** | | | | **April** | | | | **Mei** | | | | **Juni** | | | |
| **Penyusunan Proposal** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Studi Literatur** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Perancangan Sistem** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Implementasi** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Uji Coba dan Evaluasi** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Penyusunan Buku** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. **DAFTAR PUSTAKA**
   1. Axelsson, S. (2000). *Intrusion detection systems: A survey and taxonomy*. Technical Report 99-15, Chalmers University of Technology, Department of Computer Engineering, Göteborg, Sweden.
   2. Bernadó-Mansilla, E., & Garrell, J. M. (2003). *Accuracy-based learning classifier Systems: Models, analysis and applications to classification tasks*. Evolutionary Computation, 11(3), 209–238.
   3. Jyothsna, V., Rama Prasad, V. V., Prasad, K. Munivara. (2011). *A Review of Anomaly based Intrusion Detection Systems.* International Journal of Computer Applications.
   4. Richard L. White. Method for Classification <URL: <http://sundog.stsci.edu/rick/SCMA/node2.html>>, 20 Februari 2012
   5. Scarfone, Karen; Mell, Peter (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. Computer Security Resource Center (National Institute of Standards and Technology) (800–94).
   6. Shafi, K., Abbass, H. A. (2009). *An adaptive genetic-based signature learning system for intrusion detection*. Expert Systems with Applications 36 (2009) 12036–12043.
   7. Sigaud, Oliver., Wilson, Stewart W. *Learning Classifier Systems: A Survey*
   8. Snort. The open source network intrusion detection system <URL: <http://www.snort.org/> >, 8 Februari 2012.