# PERANCANGAN DAN PEMBUATAN PROGRAM DETEKSI INTRUSI PADA JARINGAN KOMPUTER BERDASAR PACKET HEADER DENGAN ANALISIS OUTLIER

Wijaya mudi putra
Politeknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember.
Email : mumonster@yahoo.com

## ABSTRAK

Keamanan merupakan prioritas utama dalam sebuah jaringan untuk itu diperlukan alat baik piranti lunak atau piranti keras yang mampu mengenali serangan dalam sebuah jaringan. Untuk ruang lingkup piranti lunak saat ini telah banyak dikembangkan aplikasi IDS (*Intrusion detection system*), namun sebagian besar dikembangkan dengan basis signature atau menggunakan rule dan sebagian kecil menggunakan anomaly. Anomaly adalah suatu metode untuk mencari penyimpangan sebuah data.

Tugas akhir ini bertujuan untuk membuat aplikasi IDS dengan basis anomaly dimana analisis datanya difokuskan pada IP header. Metode analisis yang digunakan adalah rata-rata dan standart deviasi dari data yang lewat, metode sederhana ini memiliki keuntungan yaitu perhitungan yang lebih cepat daripada metode clustering. Tujuan akhir dari tugas akhir ini adalah membuat aplikasi yang mampu mengenali serangan baik serangan tipe lama maupun baru dan memiliki jangkauan yang luas dalam mengenali sebuah serangan tanpa melakukan pembaharuan pengetahuan dari aplikasi.

Kata kunci : Intrusion detection system , anomaly IDS , c++ anomaly IDS.

## I. PENDAHULUAN

### 1.1 LATAR BELAKANG

Jaringan komputer saat ini sangat memerlukan suatu piranti yang biasa disebut IDS (Intrusion Detection Sytems). IDS dapat berupa piranti keras atau piranti lunak, kegunaan dari piranti IDS adalah untuk mengetahui jika terjadi suatu penyusupan atau data yang bersifat berbahaya pada sebuah jaringan. Tentu saja hal tersebut dapat dilakukan oleh seorang admin jaringan namun dengan adanya aplikasi IDS, akan membantu kerja dari seorang admin, karena aliran data dalam sebuah jaringan berlangsung selama 24 jam. Saat ini berbagai jenis IDS telah dikembangkan baik bersifat open source atau komersial, namun secara garis besar IDS terbagi dalam 2 kategori dalam mengenali pola serangan yaitu basis *signature* dan basis *anomaly*.

Anomaly pada dasarnya adalah mencari data yang menyimpang dari sekumpulan data normal, IDS yang berbasis anomaly umumnya menggunakan gabungan metode analisis dan statistik untuk mengenali penyimpangan tersebut. Kelemahan dari metode anomaly ini adalah dimungkinkannya salah identifikasi pada data yang diolah, juga ada kemungkinan terjadi kesalahan pada data normal yang menyebabkan aplikasi tidak dapat mengenali serangan.

## 1.2 TUJUAN

Tujuan dari pembuatan tugas akhir ini adalah membuat aplikasi yang dapat mengenali gangguan pada suatu jaringan dengan menggunakan metode anomaly. Aplikasi dapat melakukan capture data packet header pada jaringan secara live dan akan melakukan analisis pada data tersebut, sehingga aplikasi dapat memberikan peringatan jika terjadi penyusupan, hal ini tentunya sangat membantu kerja dari admin jaringan. Selain itu aplikasi ini akan memberikan petunjuk untuk pengembangan lebih lanjut dalam hal deteksi serangan pada jaringan berbasis deteksi anomaly.

## 1.3 BATASAN MASALAH

- Aplikasi hanya melakukan capture live pada satu network aktif..
- Data yang dianalisis untuk menentukan ada atau tidaknya serangan pada suatu jaringan adalah packet header.
- Packet header yang dianalisis adalah IPv4.
- Terdapat jeda waktu antara data yang telah di capture hingga aplikasi dapat menentukan data tersebut serangan atau bukan. Karena diperlukan waktu untuk melakukan analisis dari data tersebut.
- Aplikasi berjalan pada OS (Operating System) berbasis windows.
- Menggunakan bahasa C/C++ untuk membuat aplikasi.

# II. DASAR TEORI

## 2.1 IDS (Intrusion detection system)

IDS adalah sebuah piranti baik piranti lunak atau piranti keras yang dapat mendeteksi serangan pada sebuah network dengan melakukan analisis data yang lewat pada jaringan dan dilakukan secara automatis.

## 2.2 PACKET HEADER

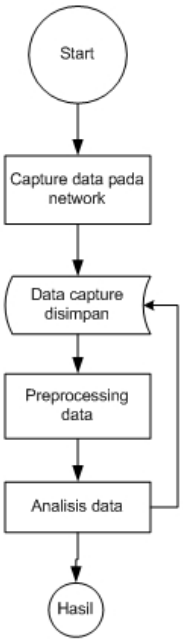
Paket header adalah suatu bagian dalam IP (Internet protocol) yang mengandung informasi alamat atau data tambahan lainnya agar dapat mencapai alamat yang dituju. Paket adalah unit informasi yang mendasar dalam transport informasi dan telah banyak digunakan dalam dunia komputer modern saat ini. Teknologi ini juga banyak diterapkan dalam bidang telekomunikasi, header dapat terdiri dari berbagai macam tipe baik *fixed size* maupun *variable size* tergntung dari system yang digunakan. Paket umumnya terdiri dari 3 bagian utama yaitu *header , body / payload , dan trailer.*

## 2.3 Anomaly dan outlier

Anomaly adalah sebuah kondisi dimana sebuah object memiliki nilai yang unik atau memiliki perbedaan nilai yang sangat jauh dari aturan yang ditetapkan[13]. Sedangkan pengertian dari outlier adalah suatu nilai yang berbeda, lain dari biasanya dan tidak mencerminkan karakteristik data secara umum. Dan nilai tersebut tidak konsisten. Dari pengertian diatas maka ada hubungan dekat antara anomaly dan outlier.

## III. PERANCANGAN & IMPLEMENTASI

### 3.1 BENTUK UMUM




Gambar 1. Diagram alir aplikasi secara umum

### 3.2 IMPLEMENTASI

- **Capture**

Untuk melakukan capture packet pada jaringan aplikasi ini menggunakan library dari WinPcap (window packet capture). Aplikasi ini hanya mengambil data pada network aktif yang telah kita tentukan, tentunya pada saat melakukan capture aplikasi ini mengambil data berupa biner. Namun data biner tersebut kita proses kembali untuk ditampilkan dalam bentuk hexa sesuai dengan panjang dari tiap field pada packet header.

- **Preprocessing data**

Hal yang dilakukan aplikasi setelah melakukan capturing adalah preprocessing. Oleh karena itu tahp pertama preprocessing adalah normalisasi data. Normalisasi dapat dicari menggunakan rumus dibawah ini

$$\text{Normalisasi} = \frac{X}{X\ \max}$$

Persamaan 1. menormalisasi data

Setelah normalisasi selesai maka tahap berikutnya adalah mencari resultan dari semua data yang ada.

$$R=\sqrt{dataX^2 + dataY^2 + dataZ^2 + ....}$$

Persamaan 2. mencari resultan

- **Analisis data**

Analisis data adalah proses setelah kita mendapatkan nilai resultan dari setiap field yang ada pada packet header. Dari data tersebut kita bisa memperoleh cluster variance / standart deviasi dan rata-rata dari nilai keseluruhan data, sehingga kita dapat mengetahui nilai thresholdnya. Jika sebuah data berada di luar threshold maka data tersebut akan dianggap anomaly oleh aplikasi. Disini semua data baik data yang dianggap anomaly atau data normal akan disimpan dalam sebuah array/vector, aplikasi akan menghitung ulang nilai VC (variance cluster) dan rata-ratanya setiap interval tertentu yang kita inginkan.

$$\text{StDev}=\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(d-\overline{d})^2}$$

Persamaan 3. Mencari nilai standart deviasi / variance cluster

Threshold = $mean \pm 2 * stDev$

Persamaan 4. Nilai threshold

## IV. PENGUJIAN DAN ANALISIS

### 4.1 Pengujian data offline

Pada pengujian ini digunakan data offline yang terdiri dari data normal dan data anomaly, disini data anomaly merupakan data attack. Data attack diambil dari DARPA 1999 [14] dan KDD-cup [15] sedangkan untuk data normal digunakan campuran antara data dari DARPA 1999 dan data saat penulis melakukan browsing di internet.

| Interval | Terdeteksi | True attack | False attack | False positive | False negative | Keberhasilan % |
|---|---|---|---|---|---|---|
| 50 | 238 | 132 | 106 | 68 | 3694 | 66 % |
| 100 | 224 | 147 | 77 | 53 | 3723 | 73 % |
| 500 | 111 | 78 | 33 | 122 | 3767 | 39 % |

Tabel 1. Hasil uji coba dengan 5% data serangan

Jumlah data 4000 dengan 200nya adalah data serangan

Dari tabel 1. diatas dapat kita lihat bahwa kemampuan mendeteksi serangan akan menurun jika menggunakan interval yang lebih besar namun tingkat keberhasilan mendeteksi sebuah true attack akan meningkat. Data attack yang disiapkan kurang lebih terdiri dari 200 data dapat dilihat pada tabel 1 maka interval 100 merupakan interval yang paling mendekati optimal dengan mendeteksi 224 anomaly / attack dan mampu mendeteksi true attack 147 nilai tersebut lebih besar jika dibanding interval 50 dan interval 500.

### 4.3 Pengujian secara online

pengujian online akan dilakukan kegiatan umum yang dilakukan seseorang saat terkoneksi dengan internet yaitu browsing bebas dengan menggunjungi sebuah situs serta mengirim dan menerima email, selain browsing kita juga melakukan kegiatan lain yang umum dilakukan seperti download, chat, ftp, dan sebagainya. Sehingga kita dapat mengetahui kemampuan aplikasi untuk mendeteksi serangan.

| Pengujian | Total data traffic | Attack terdeteksi |
|---|---|---|
| 1 | 3625 | 726 |
| 2 | 5280 | 532 |
| 3 | 4604 | 632 |
| 4 | 2436 | 344 |

Tabel 2. hasil pengujian online secara bebas

Tabel 3 menunjukan hasil pengujian aplikasi untuk online secara bebas, disini kita tidak mengetahui apakah data yang lewat merupakan data yang bebas serangan atau data yang menggandung serangan. Aplikasi mendeteksi sekitar 10% hingga 20% data yang lewat dianggap anomaly / serangan, meski bisa saja dalam pendeteksian tersebut terdapat *false attack* dan *false positiv* yang besar

## V. SIMPULAN

- Aplikasi dapat mengenali serangan baik serangan tipe lama atau tipe terbaru
- Pengenalan aplikasi terhadap serangan akan lebih bagus jika menggunakan data *training* yang baik. Meskipun aplikasi dapat mengenali serangan tanpa kita melakukan *training* terlebih dahulu.
- Aplikasi dapat mengenali baik serangan yang melakukan exploitasi pada data header dan kurang baik mengenali serangan yang berada pada payload
- Terdapat delay pada saat aplikasi melakukan proses capture & analisis
- Kecepatan analisis tergantung pada kemampuan processor

## DAFTAR PUSTAKA


1. John E Dickerson, Julie A Dickerson. Fuzzy Network Profiling for Intrusion Detection. Electrical and Computer Engineering department Iowa State University Ames.
2. Matthew V. Mahoney, Philip K. Chan. PHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic. Department of Computer SciencesFlorida Institute of Technology. Florida Institute of Technology Technical Report CS-2001-04
3. Eleazar Eskin. Anomaly Detection over Noisy Data using Learned Probability Distributions. Computer Science Department, Columbia University.
4. James R. Binkley , Suresh Singh. An Algorithm for Anomaly-based Botnet Detection. Computer Science Dept Portland State University Portland OR USA
5. Lilis fauizah.Pendeteksian serangan jaringan computer berbasis IDS snort dengan algoritma clustering K-means.Jurusan teknik informatika politeknik elektronika negri surabaya-ITS.
6. Penyiapan data(preprocessing).Modul ajar EEPIS-ITS.
7. Ali ridho barakbah. Modul ajar Cluster analysis.EEPIS-ITS
8. O'Reilly. Learn Network step by step. Network troubleshooting tool 2004. http://hell.org.ua/Docs/oreilly/tcpip2/tshoot/ch04_04.htm.
9. WinPCap manual ebook. http://www.winpcap.org/
10. Windump manual ebook. http://www.winpcap.org/windump/default.htm
11. http://en.wikipedia.org/wiki/Intrusion_detection_system
12. http://en.wikipedia.org/wiki/IPv4
13. http://en.wikipedia.org/wiki/Anomaly
14. 2000 DARPA intrusion detection evaluation data set. Windows NT attack data set. http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/2000data.html
15. KDD-cup 1999. Knowledge Discovery and Data Mining 1999 . http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html