1. Pendahuluan

1.1 Latar Belakang

IDS adalah suatu perangkat atau aplikasi yang dapat memonitor jaringan dan aktifitas sistem untuk mengetahui aktifitas mencurigakan ataupun pelanggaran kebijakan untuk kemudian memberikan laporan kepada sebuah *management station*. Salah satu metode pendeteksian yang digunakan pada IDS adalah *Pattern-Matching*. *Pattern-Matching* merupakan proses membandingkan *pattern* dengan peristiwa yang diamati untuk mengidentifikasi kemungkinan ancaman. *Pattern-Matching* adalah metode pendeteksian ancaman paling sederhana karena hanya membandingkan aktifitas yang saat ini terjadi, seperti sebuah paket atau *log entry* ke daftar *pattern* menggunakan operasi perbandingan string[6]. Akan tetapi, metode *pattern-matching* memiliki kelemahan terutama ketika beban pada *host* IDS meningkat, yaitu terjadinya penurunan performa secara signifikan[7]. Oleh karena itu, diajukan sebuah solusi untuk memindahkan sebagian beban komputasi IDS tersebut ke *Graphics Processing Unit* (GPU).

GPU modern yang ada saat ini lebih mudah diprogram, serta memiliki kemampuan *stream-processors* yang memiliki performa komputasi tinggi yang beberapa tahun lalu belum mampu mengerjakan proses komputasi non-grafika[7]. Performa tersebut didapatkan dari proses parallel baik pada level data dan instruksi. Selain itu, GPU modern saat ini dirancang untuk bisa mengambil keuntungan dari elemen data yang terpisah untuk dapat diolah secara mandiri pada skenario grafis sebelumnya.

1.2 Perumusan masalah

Pada tugas akhir ini masalah yang akan diselesaikan adalah :

1. Bagaimana implementasi metode *Pattern-Matching Intrusion Detection System* pada *Graphic Processing Unit*?
2. Bagaimana proses pemecahan paket data serial menjadi paralel untuk diteruskan ke *Graphic Processing Unit?*
3. Bagaimana performansi dari penerapan metode *Pattern-Matching Intrusion Detection System* pada *Graphic Processing Unit*?

Batasan masalah pada tugas akhir ini adalah :

1. Pengukuran dilakukan pada IDS berbasis jaringan (*Network Intrusion Detection System*)
2. Pengukuran performansi dilakukan pada IDS Snort
3. Proses pemecahan paket data serial menjadi paralel dilakukan oleh IDS Snort setelah *preprocessing*. Snort memecah paket data yang masuk menjadi beberapa grup dengan menerapkan sejumlah *rule* pada setiap paket yang masuk.
4. Pemrograman pada GPU menggunakan framework OpenCL dengan menggunakan GPU ATI Radeon™ HD 5850
5. Algoritma *pattern-matching* yang digunakan adalah algoritma Aho-Corasick

1.3 Tujuan

Tujuan dari penelitian tugas akhir ini adalah :

1. Menerapkan metode *Pattern-Matching Intrusion Detection System* pada *graphics hardware*.
2. Mengetahui dan menganalisa performansi dari penerapan metode *Pattern-Matching Intrusion Detection System* pada *graphics hardware* dengan parameter berupa packet loss ratio dan CPU utilization.

1.4 Hipotesis

Penerapan metode *pattern-matching Intrusion Detection System* pada *Graphic Processing Unit* dapat menurunkan CPU *usage* sehingga packet drop yang terjadi menjadi lebih kecil.

1.5 Metodologi penyelesaian masalah

Metodologi yang digunakan untuk penyelesaian masalah pada tugas akhir ini adalah :

1. Studi Literatur

   Pencarian yang layak mengenai cara kerja *Intrusion Detection System* Snort, Framework OpenCL, serta algoritma Aho-Corasick untuk diterapkan pada *Pattern-Matching* IDS Snort.

2. Desain Penelitian

   Untuk mencapai tujuannya, metode *Pattern-Matching Intrusion Detection System* akan diimplementasikan secara langsung oleh peneliti. Beberapa parameter yang akan diukur selama pengujian adalah pengaruh ukuran buffer, *waiting time*, dan *bandwidth*terhadap utilisasi CPU dan *packet loss ratio*.

3. Pengujian Performa Sistem dan Analisa Hasil

   Melakukan proses penghitungan terhadap performa penerapan metode *Pattern-Matching Intrusion Detection* System, membuat skenario pengujian yang sesuai, serta melakukan analisa terhadap kelebihan dan keterbatasan metode tersebut.