Permasalahan Keamanan TI dan Penanganan Insiden Respon dalam Game *Online* Berdasarkan *Intrusion Detection System* (IDS)

Braham Lawas Lawu (23214319)
EL6115 –Operasi Keamanan dan Insiden Respon
Teknik Mikroelektronika, Program Studi Teknik Elektro
Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung

ABSTRAK

Permasalahan keamanan Teknologi Informasi (TI) sangatlah penting bagi penyedia layanan game, baik yang berbasis *offline* game maupun *online* game. Penyedia layanan game, khususnya game *online*, tidak menginginkan terjadinya hal-hal yang tidak diinginkan dalam hal keamanan di dalam jaringannya maupun di dalam game itu sendiri. Untuk itu diperlukan pengetahuan yang baik dan juga informasi yang benar akan penanganan insiden respon, baik sebelum terjadinya serangan, maupun sesudah terjadinya serangan yang tidak diinginkan.

Penggunaan *Intrusion Detection System* (IDS) sebagai langkah dalam melakukan pengawasan, baik trafik dalam jaringan maupun kegiatan-kegiatan yang mencurigakan, dapat mengurangi aktivitas-aktivitas yang tidak diinginkan itu sendiri. Jika terjadi suatu aktivitas yang mencurigakan, maka IDS dapat memberikan peringatan ke dalam sistem atau *administrator* jaringan. IDS sendiri memiliki beberapa jenis dan pendekatan yang berbeda dalam mendeteksi suatu trafik. Secara umum, beberapa jenis IDS tersebut adalah: (1) IDS yang berbasis jaringan atau (NIDS), dimana IDS ini ditempatkan pada tempat strategis atau *node* penting dalam suatu jaringan untuk melakukan pengawasan trafik baik yang berasal maupun menuju kedalam perangkat di dalam suatu jaringan. Dan (2) IDS yang berbasis host (HIDS). IDS jenis ini bekerja pada *host* yang berdiri sendiri dalam sebuah jaringan. IDS ini melakukan pengawasan terhadap paket-paket yang berasal dari luar maupun dari dalam yang ditujukan pada satu *device* saja, kemudian memberikan peringatan kepada *user* atau *administrator* bahwa di dalam suatu jaringan terdapat aktivitas yang berpotensi sebagai serangan.

Inti pembahasan makalah ini adalah kajian mengenai permasalahan keamanan TI yang terjadi pada game *online* maupun *offline* dan penanganannya berdasarkan model-model yang ada pada *Intrusion Detection* System (IDS). Dengan mengetahui permasalahan yang ada dan mengetahui penanganan insiden respon ini, diharapkan sistem keamanan dalam game *online* atau *offline* dapat dijaga.

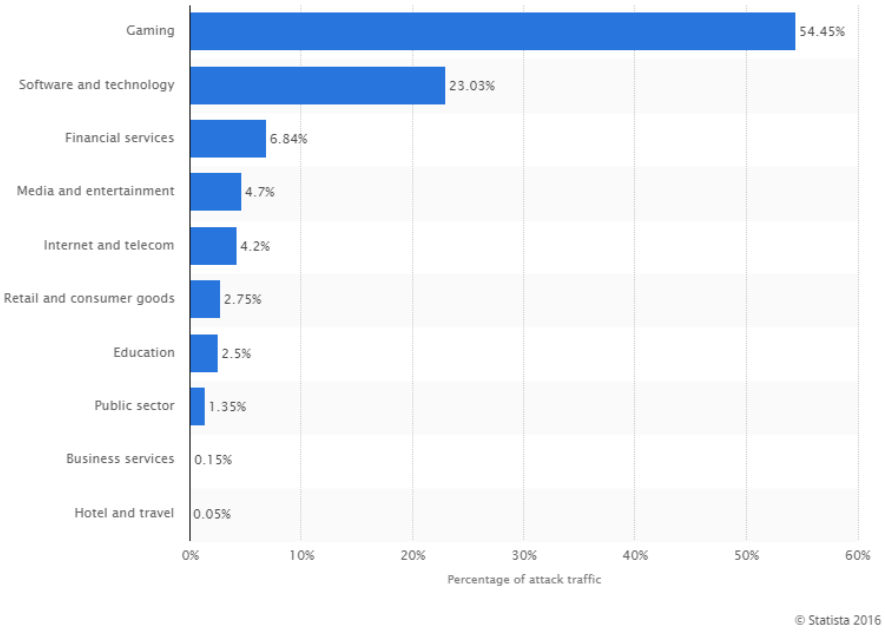
Kata kunci : IDS, Insiden Respon, Keamanan Jaringan, Game *online* atau *offline*.

DAFTAR ISI

1. PENDAHULUAN

Dunia industri video game sekarang ini, khususnya *online* game yang berbasis PC, mengalami peningkatan dalam jumlah pemain dan juga perkembangan video game itu sendiri. Menurut hasil survey yang terdapat dalam situs polygon, menunjukkan bahwa jumlah pemain yang memainkan game di Negara Amerika, telah mencapai angka 155 juta pemain dengan rata-rata pemain berumur sekitar 35 tahun [1]. Hal ini menunjukkan bahwa antusias pemain game, baik game *online* maupun *offline* sangatlah tinggi. Dan hal ini akan semakin bertambah dari tahun ke tahun. Dengan bertambahnya jumlah pemain dalam industri video game ini dari tahun ke tahun, diharapkan perusahaan yang bergerak dalam industri video game memiliki keamanan yang baik di dalam sistemnya, agar pemain tidak mengalami gangguan atau masalah selama memainkan video game tersebut.

Salah satu serangan yang paling sering ditemui yang mengganggu kelancaran konektivitas dalam bermain bagi pemain video game, khususnya *online* game adalah akibat serangan *Distributed Denial of Service* (DDoS). DDoS menyerang suatu jaringan atau *host* sehingga membuat suatu jaringan atau *host* bekerja dengan tidak maksimal, atau bahkan hingga tidak bekerja sama sekali. Hal ini dikarenakan serangan DDoS memasukki suatu jaringan dengan menghabiskan sumber daya yang ada seperti *bandwidth*, *disk space*, atau bahkan *processor*. Menurut data yang diperoleh oleh situs Nabshow, kerugian akibat serangan DDoS ini pada dunia industri video game pada tahun 2015 mencapai hingga $40,000 perjam-nya [2]. Hal ini sangat merugikan bagi perusahaan yang bergerak dalam bidang penyedia layanan video game baik yang berbasis *online* game maupun *offline* game.



Gambar 1. Persentase serangan DDoS di dalam jaringan (Statista, 2016)

Penggunaan software IDS atau *Intrusion Detection System* merupakan salah satu cara dalam memproteksi keamanan di dalam jaringan dari serangan atau ancaman dengan memanfaatkan *firewalls* dan juga anti virus [3]. IDS itu sendiri melakukan pengawasan terhadap trafik di dalam jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan [4]. Secara umum, jika IDS mendeteksi adanya kemungkinan serangan, maka IDS akan memberitahukan kepada *administrator* lewat peringatan yang ada. Dengan peringatan yang datang, diharapkan bahwa, *administrator* dapat mengetahui, trafik yang mengalami gangguan dan melakukan pendataan terhadap trafik yang masuk ataupun keluar dari jaringan. Sehingga dapat memaksimalkan pertukaran data dengan baik di dalam jaringan.

Oleh karena itu, pada bahasan makalah ini dipaparkan mengenai permasalahan apa saja yang terjadi dalam keamanan TI khususnya pada *online* game dan juga bagaimana penanganan yang dilakukan berdasarkan pada model-model IDS yang ada. Diharapkan dengan adanya penggunaan IDS ini, penanganan insiden respon yang terjadi dapat dilakukan dengan baik dan mengurangi atau bahkan mencegah terjadinya serangan yang datang ke dalam perusahaan penyedia layanan jasa *online* game ataupun *offline* game.

2. STUDI LITERATUR

Pada bagian studi literatur ini, dipaparkan materi-materi yang berkaitan dengan topik yang dibahas pada makalah ini, seperti apa itu IDS, bagaimana IDS bekerja, model-model apa saja yang digunakan di dalam IDS dalam mendeteksi serangan dan juga insiden respon yang dilakukan oleh IDS.

2.1 *INTRUSION DETECTION SYSTEM* (IDS)

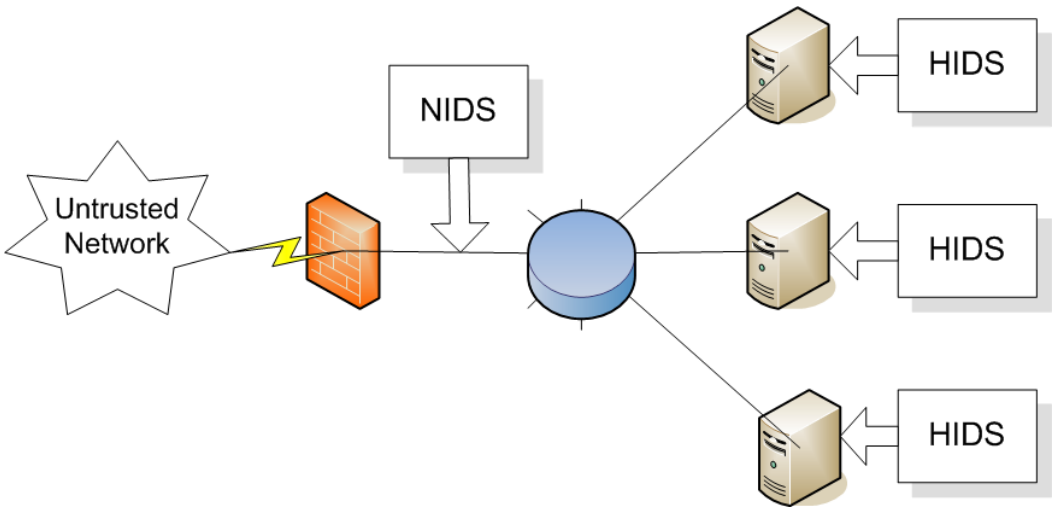
IDS atau *Intrusion Detection System* merupakan sebuah sistem yang bekerja dengan cara melakukan pengawasan terhadap trafik yang ada di dalam suatu jaringan atau *host* dan juga melakukan pengawasan terhadap kegiatan yang berpotensi sebagai serangan di dalam suatu jaringan atau *host*. Jika ditemukan kegiatan yang mencurigakan di dalam trafik jaringan, maka IDS akan memberikan peringatan kepada *administrator* jaringan. Dalam banyak kasus, IDS juga merespon terhadap trafik yang tidak normal atau anomali melalui aksi pemblokiran *user* atau pengguna atau alamat IP (Internet Protocol) sumber yang melakukan usaha serangan ke dalam suatu jaringan [4]. Secara ideal, IDS harus bebas dari pemberitahuan peringatan yang tidak benar (false positive or false negative), dapat mendeteksi gangguan dengan tepat, menghindari waktu respon yang lama dan juga tidak memakan banyak waktu komputasi dalam pemrosesannya [5]. Untuk itu, pemakaian IDS haruslah tepat sasaran sesuai dengan fungsi-fungsinya masing-masing.

2.2.1 JENIS-JENIS IDS

Secara umum, IDS dibagi menjadi 2 jenis, yaitu :

- *Host Intrusion Detection System* (HIDS)
  IDS jenis ini bekerja secara individu pada suatu devais di dalam suatu jaringan. HIDS memonitor paket data yang berasal dari dalam ataupun luar hanya pada satu devais saja dan kemudian memberikan peringatan kepada *user* atau pengguna atau *administrator* di dalam suatu jaringan akan adanya bahaya serangan atau kegiatan lain yang mencurigakan yang terdeteksi oleh HIDS [6].

- *Network Instrusion Detection System* (NIDS)
  IDS jenis ini ditempatkan di sebuah tempat atau titik di dalam suatu jaringan untuk melakukan pengawasan terhadap trafik yang menuju dan berasal dari semua devais di dalam jaringan. Idealnya, semua trafik yang berasal dari luar dan dalam jaringan akan diamati, namun hal ini akan menyebabkan kemacetan yang mengganggu kecepatan akses di seluruh jaringan [6].



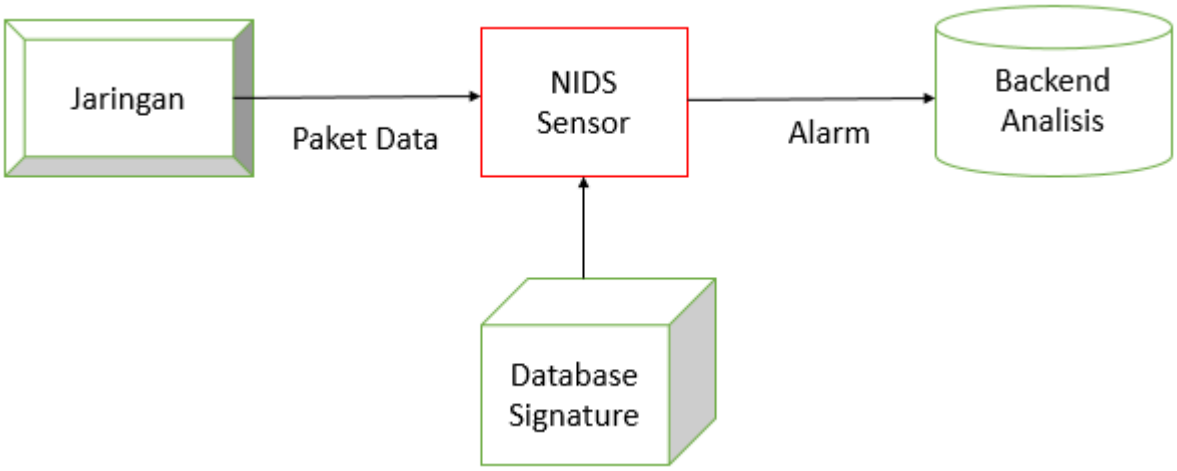
Gambar 2. Peletakkan NIDS dan HIDS dalam sebuah jaringan [7]

2.2.2 METODA PENGAWASAN

Untuk melakukan pengawasan terhadap trafik, baik yang masuk ke dalam suatu jaringan maupun yang keluar dari jaringan, beberapa teknik atau metoda yang dilakukan oleh IDS dalam mendeteksi adalah :

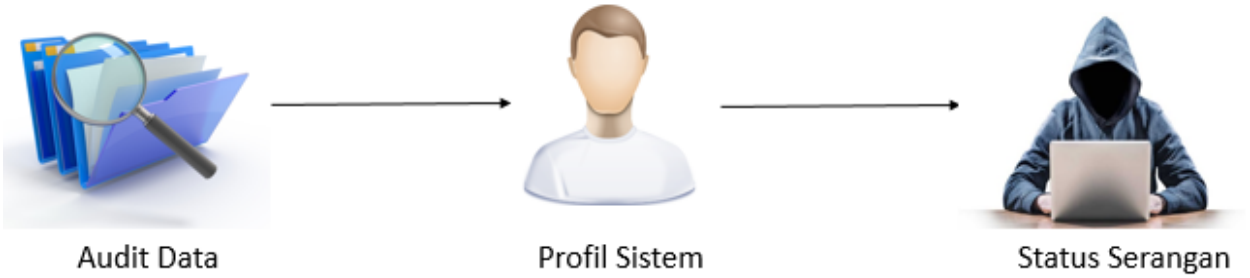
- *Signatured-Based Detection*
  Teknik ini dilakukan dengan melakukan pengawasan terhadap paket-paket dalam jaringan dan melakukan pembandingan terhadap paket-paket tersebut dengan basis data *signature* yang dimiliki oleh sistem IDS tersebut [8]. Teknik ini sebenarnya mirip dengan cara kerja

anti-virus dalam mendeteksi adanya *malware*. Teknik ini merupakan teknik yang paling sederhana, karena hanya membandingkan paket data yang masuk ataupun yang keluar, kemudian mencocokkannya dengan basis data *signature* yang dimiliki sistem IDS. Kelemahan dengan teknik ini adalah jika serangan yang datang tidak terdapat dalam basis data *signature*, maka IDS tidak akan mampu mengenali serangan yang masuk.



Gambar 3. Blok diagram cara kerja *Signatured-Based Detection*

- *Anomaly-Based Detection*
  Teknik ini dilakukan dengan cara mengawasi trafik dalam jaringan yang sedang terjadi dan melakukan perbandingan trafik yang terjadi tersebut dengan trafik dalam jaringan yang dianggap normal. Teknik ini dilakukan berdasarkan aturan-aturan yang telah ditetapkan, berbeda dengan *Signatured-Based Detection* yang melakukan deteksi berdasarkan *signature* atau pola-pola yang ada [9].



Gambar 4. Blok diagram cara kerja *Anomaly-Based Detection*

2.2.3 JENIS RESPON YANG DIHASILKAN

Ketika IDS melakukan pengawasan di dalam trafik suatu jaringan, jika ditemui adanya masalah atau kemungkinan adanya serangan, maka IDS akan memberikan respon kepada *administrator* lewat peringatan yang ada. Berdasarkan respon yang dihasilkan oleh IDS, terdapat 2 jenis respon yang dihasilkan di dalam suatu sistem, yaitu :

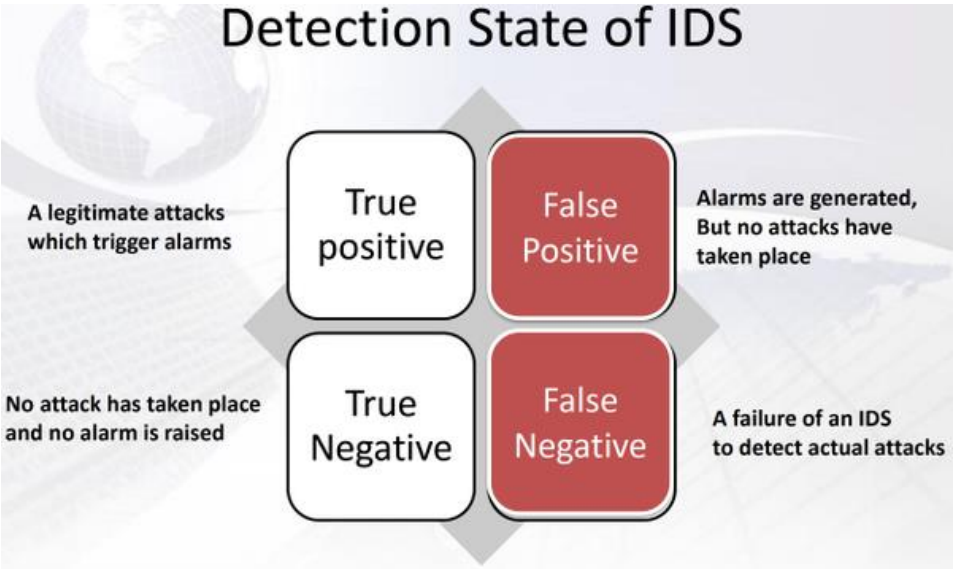
- *Passive System*
  Pada respon dengan sistem pasif, IDS hanya mendeteksi potensi adanya serangan pada keamanan, mencatat informasi yang muncul dan juga memberikan peringatan kepada *administrator* [10].

- *Reactive System*
  Pada respon dengan sistem reaktif atau biasa dikenal juga dengan nama *Intrusion Prevention System* (IPS), IDS tidak hanya melakukan pendeteksian dan pemberian peringatan, namun juga dapat melakukan reset koneksi atau juga memprogram kembali *firewall* untuk memblok trafik di dalam suatu jaringan yang dianggap sebagai serangan [10].

2.2 INSIDEN RESPON

Berdasarkan NIST (National Institute of Standards and Technology) [11] Insiden didefinisikan sebagai pelanggaran terhadap kebijakan keamanan computer, kebijakan yang diterima pengguna atau standar praktik keamanan komputer. Adapun insiden respon adalah proses mendeteksi dan menganalisis insiden serta membatasi pengaruh dari insiden.
Ketika insiden terjadi, IDS sebagai software yang bekerja dalam merespon insiden yang ada, memberikan peringatan kepada *administrator* lewat peringatan-peringatan yang ada, yaitu :

- *True Positive* (TP) : Ketika penyerang berhasil menyerang jaringan dan IDS juga berhasil mendeteksi hal tersebut [8].
- *True Negative* (TN) : Ketika penyerang gagal melakukan serangan pada jaringan dan IDS tidak memberikan laporan terhadap hal tersebut [8].
- *False Positive* (FP) : Ketika penyerang gagal melakukan serangan pada jaringan dan IDS memberikan laporan terhadap hal tersebut [8].
- *False Negative* (FN) : Ketika penyerang berhasil menyerang jaringan dan IDS tidak memberikan laporan tersebut [8].



Gambar 5. Peringatan yang dihasilkan oleh IDS (Huzeyfe Onal, 2015)

3. PEMBAHASAN

Pada bagian ini, makalah membahas lebih dalam terkait serangan yang terjadi pada game *offline* dan juga game *online* serta penanganan yang dilakukan oleh IDS ketika adanya serangan.

3.1 KEAMANAN DI DALAM VIDEO GAME

Seperti yang telah dijelaskan pada bab sebelumnya, bahwa, potensi adanya serangan dalam video game, baik yang berbasis game *online* maupun game *offline* mendapatkan angka yang sangat tinggi. Untuk itu, keamanan di dalam video game itu sendiri, sangat perlu dijaga, seperti pada keamanan bagian jaringan, *software* yang bekerja, hingga pada bagian *hardware*-nya itu sendiri.

3.1.1 *OFFLINE* GAME

Pada game yang berbasis *offline*, masalah utama yang terjadi di dalam keamanan sistemnya lebih fokus kepada *software* yang berjalan itu sendiri. Hal ini dikarenakan pada game yang berbasis *offline*, cenderung tidak memerlukan jaringan seperti *Local Area Network* (LAN) ataupun konektivitas internet. Kebanyakan penyedia *offline* game, berjalan dengan domain MS Window dan juga menggunakan Microsoft Server operating systems. Ada ancaman di dalam penggunaan OS tersebut, seperti lemahnya keamanan di dalam OS yang digunakan. Untuk mengakalinya, diperlukan *patch-patch* baru atau memperbaharui data yang ada agar permasalahan *error* atau *bug* yang ada dapat diselesaikan. Namun hal ini memerlukan konektivitas internet.
Beberapa program yang biasanya digunakan untuk menyerang adalah QuickTime, Adobe Flash, Adobe PDF Reader, dan Microsoft Office [12]. Jika konfigurasi yang dilakukan pada program tersebut tidak maksimal, maka dapat menjadi celah dalam melakukan serangan.

Dan juga, yang paling penting dari itu sendiri, adalah permasalahan bahasa pemrograman yang digunakan serta isi dari pemrogramannya itu sendiri. Seperti yang dikatakan dalam ISO/IEC TR 24772 [13], bahwa :

Semua bahasa pemrograman yang mengandung struktur yang tidak dijelaskan secara rinci, menunjukkan perilaku yang tidak rinci, sulit untuk digunakan dengan baik. Penggunaan struktur tersebut dapat membuat kelemahan dalam sistem tersebut, sehingga software dapat dijalankan dengan tujuan yang berbeda dari yang telah dituliskan. Pada beberapa kasus, kelemahan karena penulisan pemrograman ini, dapat digunakan oleh penyerang untuk menyerang suatu sistem.

Dari kalimat di atas dapat disimpulkan bahwa semua bahasa pemrograman dapat berisikan kelemahan, namun kebanyakan dikarenakan bukan karena bahasa pemrograman itu sendiri, tapi karena bahasa yang dituliskan [13]. Pada makalah ini, tidak akan dibahas hal secara mendalam tentang masalah keamanan yang terjadi di dalam *offline* game, karena fokus makalah ini adalah pada *online* game.

3.1.2 *ONLINE* GAME

Pada game yang berbasis *online*, semakin banyak cara yang ditempuh oleh penyerang dalam menyerang industri jasa penyedia layanan game. Selain permasalahan penyerangan pada *software*, hal yang paling sering ditemui adalah karena serangan DDoS seperti yang sudah dijelaskan pada bab sebelumnya. Permasalahan penyerangan pada *software*, dapat diatasi dengan adanya *patch-patch* yang bisa dilakukan secara berkala oleh pemberi jasa layanan *online* game. Permasalahan yang paling berat yang dilalui adalah adanya karena serangan DDoS tersebut. Berikut akan dipaparkan permasalahan yang ada beserta insiden respon yang dilakukan.

3.1.2.1 STUDI KASUS

Banyak kasus yang menyerang *online* game yang sangat berkembang sekarang ini seperti game Dota 2, Counter-Strike : Global Offensive, League of Legend dan lain-lain. Industri penyedia layanan jasa *online* game yang disebutkan sebelumnya, memiliki sistem keamanan yang handal, tenaga ahli yang memadai, dan tim insiden respon yang cukup baik dalam mengerjakan tugas-tugasnya. Penyerangan yang dilakukan bahkan oleh DDoS pun, dapat dihindari, selain karena industri tersebut memiliki *bandwidth* yang luar biasa besar di dalam sistemnya, sehingga untuk menyerangnya, menjadi sangat sulit dan dibutuhkan biaya yang sangat besar. Berikut contoh insiden yang terjadi pada kasus *online* game Ragnarok:

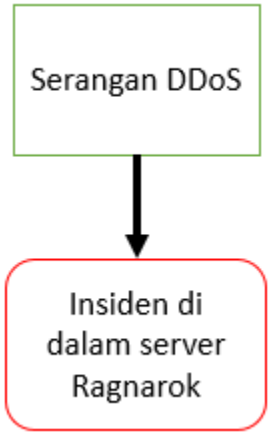
Skenario Insiden : Server Ragnarok Return adalah server game untuk *online* game Ragnarok. Server ini menyediakan kapasitas hingga lebih dari 2000 orang dalam satu server. Tidak ada batasan pemain yang dapat bermain dalam satu server ini, sehingga siapapun yang telah terdaftar dapat bermain dalam server ini.

Jenis Insiden : Insiden yang paling sering ditemui seperti yang sudah disebutkan sebelumnya adalah karena adanya serangan DDoS, dengan cara seolah-olah membuat ‘pemain’

baru yang telah terdaftar, melakukan pengiriman dan *request* paket data yang berlebih sehingga memenuhi kapasitas *bandwidth* yang tersedia, bahkan serangan ini juga dapat dilakukan tanpa memerlukan proses *log-in* terlebih dahulu di dalam game-nya. Hal ini membuat trafik jaringan pada server penuh, dan trafik di dalam sistem menjadi lambat yang berakibat pada munculnya *lagging* atau delay antara aksi dari pemain dan reaksi dari server. Bahkan jika penyerang melakukan hal ini terus menerus dan pihak penyedia layanan jasa *online* game ini tidak dapat menanganinya, server akan mengalami *down*, sehingga pemain tidak dapat terhubung kembali ke dalam server karena server sudah dalam keadaan *down*.

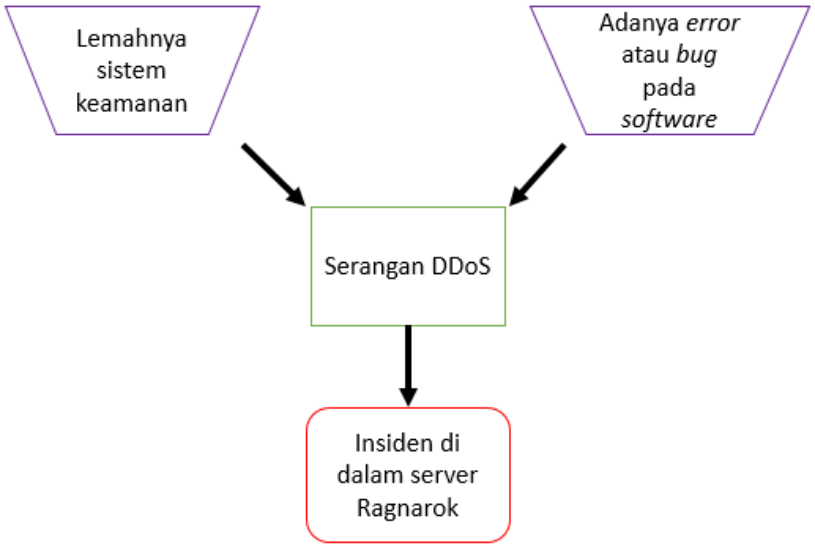
Keamanan yang disediakan : Dari pihak penyedia layanan jasa *online* game ini, hanya menyediakan Gepard Shield sebagai proteksi *in-game*. Gepard Shield merupakan *Anti-Cheat* yang dirancang untuk dapat mencegah pemain menggunakan *tools-tools* yang mengganggu keseimbangan permainan, seperti menggandakan barang, penggunaan *script* dalam bermain, menggandakan uang, memindahkan pemain atau bahkan mengubah settingan yang pemain tidak boleh lakukan (hanya dapat dilakukan oleh penyedia layanan game tersebut).

Dengan pengetahuan ini, kita dapat membuat konstruksi blok diagram insiden penyerangan dan bagaimana respon yang harus dilakukan dari adanya serangan secara terstrukstur mulai dari yang sederhana. Kita memulainya dengan bertanya, “Apa yang menjadi penyebab serangan ?”. Kemudian kita membuat blok diagram tersebut.



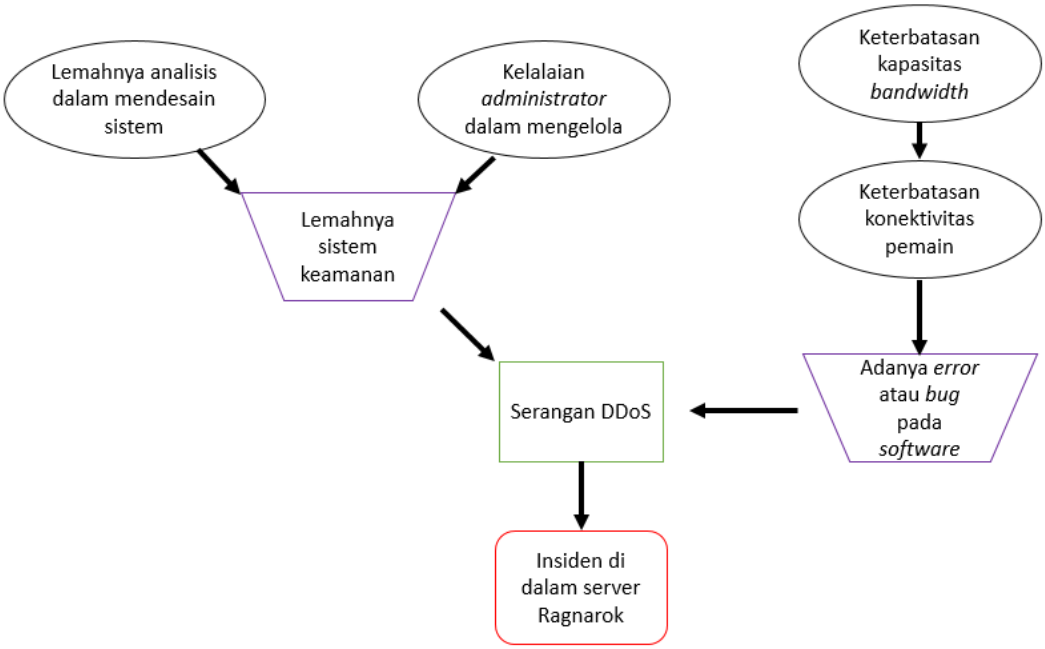
Gambar 6. Konstruksi blok diagram penyerangan pertama.

Kemudian kita melanjutkannya dengan menganalisa blok “Serangan DDoS”. Kita mengidentifikasikannya dengan menjawab pertanyaan sebelumnya, “Apa yang menjadi penyebab serangan ?”. Berdasarkan analisa yang sudah dilakukan, disimpulkan, hal ini karena lemahnya sistem keamanan yang digunakan, sehingga membuat serangan DDoS mudah untuk menyerang jaringan server yang digunakan. Selain itu, dapat terjadi juga karena lemahnya *software* yang dipergunakan dalam menjalankan game tersebut. Dan untuk konstruksi blok diagram selanjutnya, kita dapat memisahkan dua hal yang menjadi penyebab serangan DDoS ini bisa memasuki server.



Gambar 7. Konstruksi blok diagram penyerangan kedua.

Melanjutkan hal sebelumnya, kita dapat bertanya, "Apa yang menyebabkan lemahnya sistem keamanan ?", dan juga "*Error* atau *bug* apa yang ada di dalam *software* ?". Untuk menjawab pertanyaan yang pertama, hal ini dapat terjadi karena lemahnya analisis dalam mendesain sistem, dan juga dapat dikarenakan *administrator* yang lalai dalam menjaga sistem keamanan. Sehingga untuk pertanyaan pertama, kita dapat memecahnya menjadi dua blok diagram tersendiri. Selanjutnya untuk pertanyaan kedua, analisa yang memungkinkan adalah dikarenakan server menyediakan konektivitas kepada pemain yang terbatas. "Mengapa server hanya menyediakan konektivitas kepada pemain yang terbatas ?". Hal ini bisa dikarenakan oleh kapasitas *bandwidth* yang disediakan atau digunakan oleh penyedia jasa layanan game ini kurang besar, sehingga serangan DDoS memenuhi trafik jaringan yang ada. Jika serangan datang, namun kapasitas *bandwidth* yang disediakan lebih besar daripada serangan yang datang, maka serangan yang datang akan dirasakan oleh server hanya sebagai 'pengguna atau pemain'. Dan hal ini tidak akan mengganggu jaringan. Kemudian untuk konstruksi blok diagram selanjutnya adalah sebagai berikut :



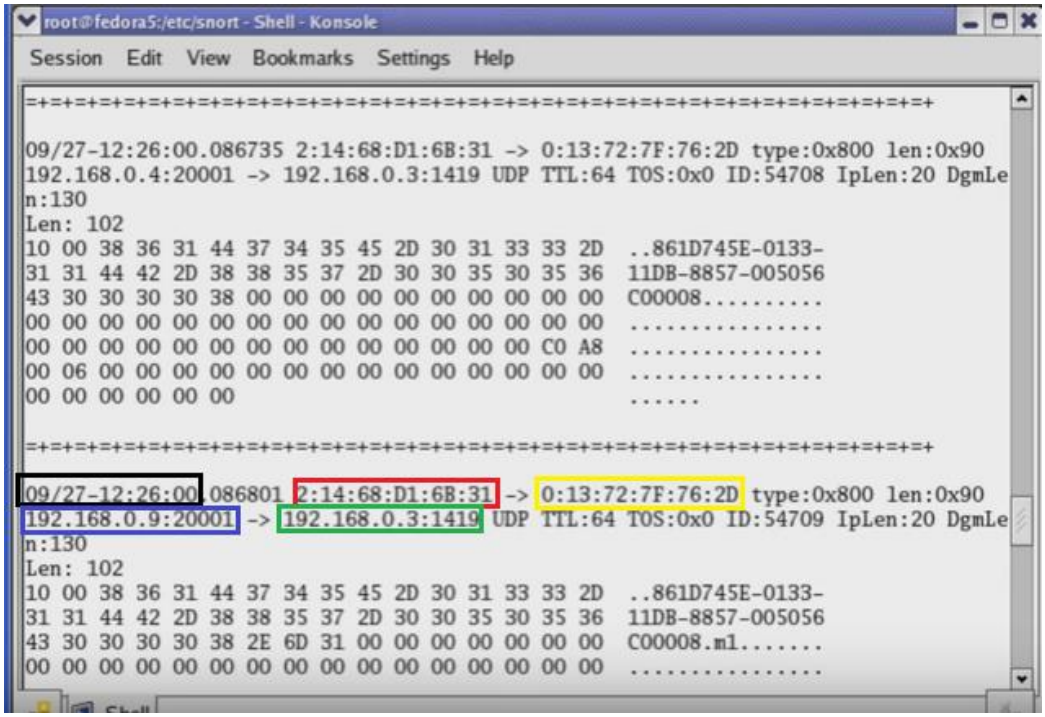
Gambar 8. Konstruksi keseluruhan blok diagram penyerangan.

Dari analisa ini, pakar insiden respon yang telah berpengalaman, dapat mengambil tindakan berdasarkan blok diagram yang sudah dibuat. Hal ini memudahkan dalam mengambil tindakan penanganan insiden yang sedang menyerang maupun yang akan datang.

Dari blok di atas, kita dapat menyelesaikan permasalahan pada bagian keterbatasan kapasitas *bandwidth* dengan menyediakan *bandwidth* yang lebih besar. Pihak penyedia jasa layanan *online* game, dapat menyediakan *bandwidth* yang lebih besar, namun pastinya akan menghabiskan biaya yang lebih besar.

Dari blok lemahnya analisis dalam mendesain sistem, sudah terlihat pada bagian keamanan yang tersedia, bahwa penyedia layanan jasa *online* game tidak menyediakan sistem keamanan yang baik. Disinilah peran *Intrusion Detection System* (IDS). IDS sebagai *software* atau *hardware* atau bahkan gabungan keduanya yang digunakan untuk memberikan peringatan atau bahkan melakukan pencegahan dapat menjadi langkah yang baik dalam keamanan sistem di dalam jaringan. IDS sendiri sebagai *software* dapat diunduh secara gratis di *internet* ataupun yang berbayar. Untuk IDS yang dapat dipakai di dalam jaringan (NIDS), beberapa contoh *software*-nya yang paling sering digunakan adalah Snort, Suricata, Bro, dan Kismet. Untuk IDS yang dipakai pada *host* (HIDS), beberapa contoh *software*-nya adalah OSSEC, Samhain, dan OpenDLP.

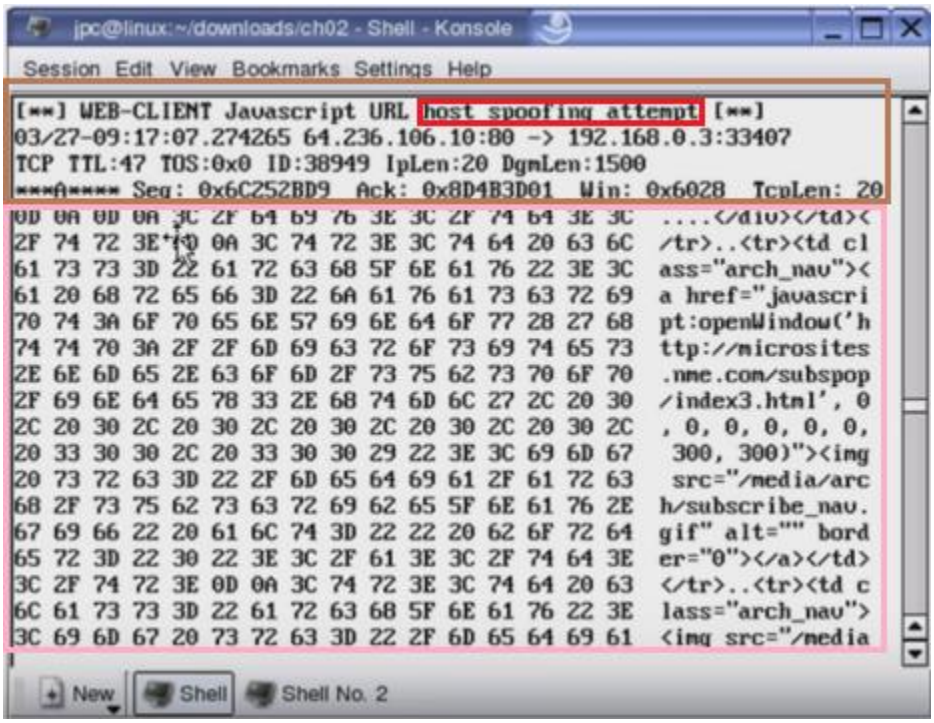
Berikut adalah contoh tampilan penggunaan aplikasi Snort sebagai IDS untuk mendeteksi paket yang berada dalam suatu jaringan :



Gambar 9. Mode *Sniffer* dalam *software* Snort [14].

Gambar di atas menunjukkan paket data yang berada dalam suatu jaringan. Dalam gambar di atas, terlihat berbagai macam informasi yang dapat diperoleh, seperti tanggal datangnya paket data (kotak berwarna hitam), MAC *Address* datangnya paket data (kotak berwarna merah), MAC *Address* tujuan paket data (kotak berwarna kuning), IP *Address* datangnya paket data (kotak berwarna biru), IP *Address* tujuan paket data (kotak berwarna hijau), dan informasi lain yang dapat diperoleh untuk menunjukkan informasi penting di dalam suatu jaringan.

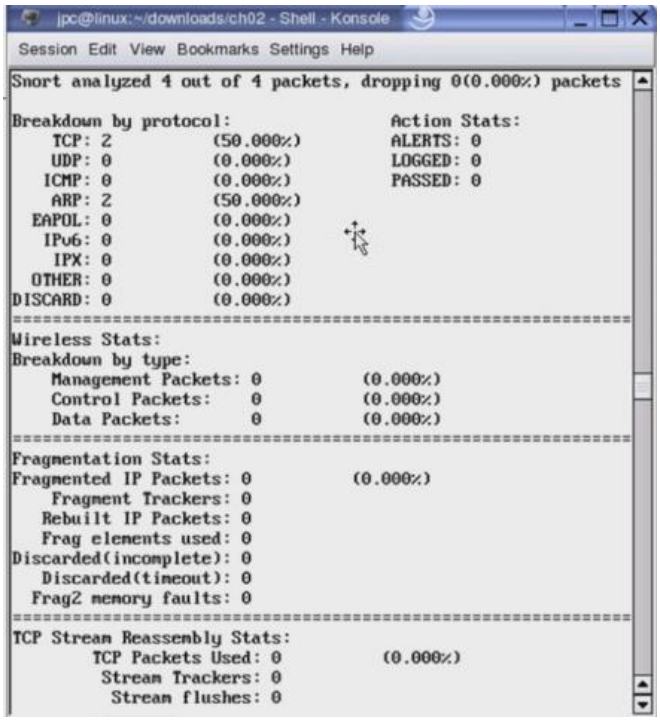
Dan jika *software* Snort yang digunakan sebagai IDS mendeteksi adanya bahaya, maka Snort dapat memberikan peringatan kepada *administrator* akan adanya bahaya serangan. Berikut contoh peringatan yang dihasilkan oleh Snort :



Gambar 10. Mode *Alert* dalam *software* Snort [14].

Dalam mode ini, Snort memberikan peringatan akan adanya bahaya di dalam jaringan. Terlihat adanya kemungkinan serangan menggunakan *spoofing* pada *host* (diwakili oleh kotak berwarna merah). Pada gambar di atas juga terlihat bahwa, banyak informasi yang didapat di dalam paket *header* (diwakili oleh kotak berwarna coklat) yang dikirimkan, dan juga informasi mengenai apa isi paket yang dikirimkan pada layer aplikasi (diwakili oleh kotak berwarna pink).

Snort sebagai IDS juga dapat memberikan hasil analisa seperti contoh yang terlihat pada gambar di bawah ini :



Gambar 11. Mode *Analyze* dalam *software* Snort [14].

Di dalam mode ini, terlihat hasil analisa penggunaan Snort, seperti peringatan yang datang, penggunaan protokol di dalam jaringan untuk bertukar data, pertukaran data menggunakan *wireless* yang ada di jaringan dan lain-lainnya.

Secara umum, penggunaan *software* Snort ini sebagai *Intrusion Detection System* (IDS), dapat menghasilkan informasi penting sebagai berikut :

1. Paket data
2. MAC *Address* pengirim dan MAC *Address* penerima
3. *Type of Services*
4. Panjang datagram
5. Alamat IP dan Port pengirim
6. Alamat IP dan Port penerima
7. Protokol
8. TTL
9. Paket ID
10. Panjang *header* IP
11. Total panjang datagram
12. *Fragment*
13. *Acknowledge*
14. TCP *sequence number*
15. ACK *sequence number*
16. *Window size*

4. PEMBAHASAN

Pada bagian ini, dibahas mengenai kelebihan dan kekurangan yang ada pada *Intrusion Detection System* (IDS). IDS sendiri, sebagai salah satu solusi dalam menangani masalah serangan di dalam keamanan sistem di dalam jaringan akibat adanya serangan DDoS, masih memiliki banyak masalah dalam mendeteksi adanya serangan. Konfigurasi yang baik dan pemilihan *software* yang tepat, menjadi salah satu dasar dalam penggunaan IDS itu sendiri. Jika konfigurasi yang dilakukan tidak tepat, maka kemungkinan lemahnya IDS dalam mendeteksi adanya serangan semakin tinggi. Selain itu, metoda yang digunakan oleh IDS itu sendiri sebagai alat untuk mendeteksi adanya serangan, dapat memberikan peringatan yang salah kepada *administrator*. Hal ini dapat disebabkan karena akurasi IDS dalam mendeteksi adanya serangan yang kurang baik. Untuk itu, dipaparkan beberapa kelebihan dan kekurangan yang ada pada IDS dalam mendeteksi adanya serangan di dalam jaringan :

Kelebihan

- IDS menyederhanakan sistem sumber informasi yang kompleks
- IDS melacak aktivitas paket data yang masuk ke dalam ataupun ke luar jaringan
- IDS dapat menyesuaikan pada jaringan yang membutuhkan keamanan dengan mudah
- IDS dapat mendeteksi serangan yang datang dari luar maupun dalam jaringan
- IDS dapat melaporkan adanya serangan dan dapat melakukan perubahan data jika dibutuhkan
- IDS menjadi salah satu solusi dalam menjaga sistem keamanan di dalam jaringan
- IDS dapat dioperasikan dengan mudah
- IDS menyediakan layer tambahan sebagai perlindungan

Kekurangan

- Penggunaan NIDS, sangat rentan terhadap adanya *overload* data di dalam jaringan
- Pada IDS yang menggunakan metoda *Anomaly-Based Detection*, dapat memberikan peringatan yang salah kepada *administrator*
- IDS tidak dapat menangani trafik di dalam jaringan yang sudah dienkripsi
- IDS menghasilkan data yang besar untuk dianalisa
- Pada IDS yang menggunakan metoda *Signatured-Based Detection*, hanya dapat mengenali serangan berdasarkan data yang ada di dalam *database*
- IDS hanya memberikan peringatan dan dapat melakukan tindakan pencegahan, namun tidak dapat memberikan penanganan akan insiden yang sudah terjadi (hilangnya data, kerusakan, dan lain-lain)
- Di dalam trafik IDS, paket data yang terfragmentasi dapat menjadi masalah

5. KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Kesimpulan yang diperoleh dari makalah ini adalah sebagai berikut.

1. Perkembangan dunia industri video game sangat berkembang sekarang ini. Seiring dengan perkembangan penyedia layanan jasa video game, salah satu aspek penting yang perlu diperhatikan di dalam dunia video game, khususnya *online* game adalah keamanan. Untuk itu, diperlukan keamanan di dalam sistem yang baik dan juga tim insiden respon yang handal dalam menjaga keamanan game tersebut.
2. Penggunaan *Intrusion Detection System* (IDS) sebagai salah satu upaya dalam menjaga keamanan di dalam sistem jaringan, menjadi salah satu bagian yang sangat penting. Namun, penggunaan IDS ini juga harus ditunjang dengan adanya tim insiden respon yang dapat menganalisa masalah ketika datangnya serangan dari luar. Hal ini menjadi penting, karena IDS sendiri memiliki keterbatasan dalam mendeteksi dan memberikan peringatan di dalam sistem. Selain itu, dengan adanya tim insiden respon yang handal, permasalahan keamanan TI di dalam dunia industri video game, dapat terselesaikan dengan cepat dan tepat.
3. Pemodelan masalah ketika terjadi serangan yang datang baik dari luar maupun di dalam sistem, menjadi salah satu hal yang dapat membantu untuk memudahkan menganalisa serangan. Dengan adanya pemodelan tersebut, pihak tim insiden respon dan juga keamanan dapat mengetahui bagian mana dari sistem yang rentan terhadap serangan, sehingga dapat melakukan perbaikan-perbaikan, baik dari segi *software*, maupun *hardware* di dalam jaringan.

5.2 SARAN

Untuk pengembangan penelitian yang terkait dengan makalah ini, perlu adanya penelitian lebih lanjut mengenai algoritma-algoritma baru yang digunakan di dalam *Intrusion Detection System* (IDS). Karena dengan algoritma yang semakin baik, mengurangi adanya *false alarm* atau peringatan yang salah ketika mendeteksi paket data yang berada di dalam jaringan.

REFERENSI

[1] Campbell, Collin. “Here's how many people are playing games in America,” Polygon, diakses pada tanggal 1 Mei, 2016, http://www.polygon.com/2015/4/14/8415611/gaming-stats-2015

[2] Eitel, Barry. “In 2015, the Video Game Industry is About so Much More than Gaming,” Nabshow, diakses pada tanggal 1 Meil 2016, http://www.nabshow.com/thought-gallery-thought-leaders/2015-video-game-industry-about-so-much-more-gaming

[3] Frederic Massicote, Yvan Labiche, “On the Verification and Validation of Signature-Based, Network Intrusion Detection Systems”, In *IEEE 23rd International Symposium on Software Reliability Engineering*, 2012.

[4] Nor Badrul Anuar, Maria Papadaki, Steve Furnell and Nathan Clarke, “An investigation and survey of response options for Intrusion Response Systems (IRSs)”, In *IEEE Information Security, August 2 – 4,* 2010.

[5] Zhonghua Zhang, Pin-Han Ho, Liwen He, “Measuring IDS-estimated Attack Impacts for Rational Incident Response: A Decision Theoretic Approach”, In *Computers & Security 28, 605–614*, 2009.

[6] Abdullah A. Mohamed, "Design Intrusion Detection System Based On Image Block Matching", *International Journal of Computer and Communication Engineering, IACSIT Press,* Vol. 2, No. 5, September 2013.

[7] Erza M. Aminanto, N.L. Gian, “Menangani Serangan Intrusi Menggunakan IDS dan IPS,” Keamanan Informasi, diakses pada tanggal 1 Mei 2016, http://ki.stei.itb.ac.id/2013/10/30/menangani-serangan-intrusi-menggunakan-ids-dan-ips/

[8] Mattord, Verma, “Principles of Information Security. Course Technology”. *pp. 290–301*, 2008.

[9] Wang, Ke, "Anomalous Payload-Based Network Intrusion Detection" *Recent Advances in Intrusion Detection. Springer Berlin, 22 April,* 2011.

[10] Scarfone, Karen; Mell, Peter, "Guide to Intrusion Detection and Prevention Systems (IDPS)", In *Computer Security Resource Center (National Institute of Standards and Technology) (800–94), 1 January*, 2010.

[11] Scarfone, K., et al, “Computer Security Incident handling Guide”, *Gaithersburg: National Institute of Standards and Technology. (800-61), Revision 2,* 2012.

[12] Stephen Mohr and Syed Rahman, “IT Security Issues Within The Video Game Industry”, *International Journal of Computer Science & Information Technology (IJCSIT)* Vol 3, No 5, October 2011.

[13] *ISO/IEC Project 22.24772:Programming Language Vulnerabilities.(*2011, July). Retrieved September 20, 2011, from ISO/IEC: http://grouper.ieee.org/groups/plv/

[14] Tatarsky Paul, Rehman, Patrick. "Using Snort," *Computer and Network Security in the School of Engineering Technology at Daytona State College*, diakses pada tanggal 2 Mei 2016, https://www.youtube.com/watch?v=cQeeko9J_Yw