Prosiding
ANNUAL RESEARCH SEMINAR 2016
6 Desember 2016, Vol 2 No. 1

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

Analisis Forensik *Router* Untuk Mendeteksi Serangan *Distributed Danial of Service (DDoS)* Secara *Real Time*

Faizin Ridho, Anton Yudhana, Imam Riadi
Magister Teknik Informatika
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
faiz.3128@gmail.com, eyudhana@mti.uad.ac.id, imam.riadi@mti.uad.ac.id

***Abstrak—router* adalah salah satu perangkat yang paling dibutuhkan dalam setiap lembaga yang terhubung dengan jaringan intranet maupun internet, khususnya pada penyedia jasa internet dalam membangun sebuah jaringan dengan keamanannya. Target utama *attacker* sebelum masuk pada sistem utama atau pusat data adalah dengan mematikan kinerja *router*. Hal ini dapat merugikan perusahaan jasa jaringan yang bekerja sama dengan perusahaan seperti perusahaan jasa keuangan, bank, sekolah, universitas, warung internet, ataupun perusahaan *e– commerce* yang mengakibatkan transaksi berhenti. Bagi *intruder*, *router* sangat berperan penting untuk melancarkan aksi serangannya agar dapat masuk kedalam sistem utama atau pusat data yang diinginkan untuk melakukan tindak kejahatan. Pengendalian penuh pada *router* menyebabkan jaringan lain yang terhubung pada *router* juga dapat dikendalikan. *Intrusion Detection System* dapat dimanfaatkan sebagai sistem *monitoring* untuk mendeteksi serangan *distributed denial of service* (DDoS) secara *real time*. Kemampuan forensik terhadap router sangat diperlukan untuk menemukan bukti serangan yang di lakukan oleh *intruder* agar pelaku dapat dijerat hukum.**

Kata Kunci— Network Forensics, Router, Intruction Detection System (IDS), DDoS, Digital Evidence, Intruder

I. PENDAHULUAN

Luhut Panjaitan mengatakan bahwa pada 2015 serangan cyber di Indonesia meningkat sebesar 33 persen dibandingkan 2014[1]. Dari angka itu sebanyak 54,5 persen yang terdapat pada sector e-commerce. Akibat nya banyak sistem yang berhenti bekerja. Hal ini menyebabkan Indonesia masuk kedalam daftar darurat *cyber*.

Bank Indonesia bahkan memantau terindikasinya peningkatan aktivitas kejahatan berupa penyalahgunaan jaringan sebesar 66,7 persen pada 2015 dibandingkan dengan 2014. Saat ini Indonesia sangat memerlukan sebuah badan yang mampu menangani persoalan *cyber* yakni Badan Cyber Nasional (BCN) untuk menjaga keamanan dalam bidang informasi, khusus nya keamanan negara. yang dikutip dalam buatan berita antaranews (tanggal 3 juni 2016).

Pola keamanan jaringan yang sudah banyak diketahui tentunya menjadi masalah bagi seorang administrator untuk mengamankan sistem yang dikelolanya. Munculnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Peraturan pemerintah nomor 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan Telecom Act menjadi "angin segar" bagi pengelola sistem karena pelaku dapat dijerat hukum. Untuk menjerat pelaku administrator perlu membuktikan pelaku bersalah. *Digital forensics* dan *Network forensic* merupakan *alternative* untuk membuktikan pelaku kejahatan *cyber*.

Pengelola sistem atau administrator perlu membuat sistem yang mampu menangkal dan menanggulangi serangan yang merusak sistem yang dikelolanya dengan cepat dan tepat. Mekanisme yang memungkinkan saat ini adalah dengan metode forensik *digital* yang dapat dimanfaatkan untuk menjerat pelaku serangan. Perlu adanya sistem yang mampu mendeteksi, merekam, memonitor, dan menyimpan sebuah kejadian yang ada pada sistem jaringan yang dapat di jadikan sebagai alat bukti.

Mekanisme forensik jaringan dapat digunakan untuk mengkonstruksi sebuah kejadian dengan memanfaatkan sebuah sistem yang menyimpan dan melihat kembali segala aktivitas lalu lintas data sehingga administrator dapat melakukan investigasi melalui peristiwa ataupun kejadian yang tersimpan pada *log system*. Terdapat beberapa proses pada forensik jarigan seperti, monitoring, koleksi data, analisa data serta *source traceback* untuk mengetahui apa yang sebenarnya terjadi, untuk mengetahui detail koneksi, serta untuk mengetahui alamat asal dan tujuan, yang mungkin dapat

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

mencegah dari adanya serangan terhadap sistem keamanan jaringan.

Salah satu perangkat yang paling penting pada suatu jaringan dengan cakupan yang luas adalah *router. Router* dapat menyimpan identitas lalu lintas data berdasarkan tabel-tabel yang tersedia melalui *Router*. Perpindahan sumber informasi antar jaringan pada *router* menjadi perhatian utama untuk memonitor lalu lintas data yang menjadi sasaran para *intruder* untuk masuk kedalam sistem utama utuk merusak, menghapus, bahkan mencuri data penting yang tersimpan pada sistem utama, yang dapat merugikan baik bagi perorangan, perusahaan, maupun instansi terkait.

Pesatnya kemajuan teknologi *router* membuktikan bahwa *router* adalah perangkat yang paling dibutuhkan khususnya pada penyedia jasa internet dalam membangun sebuah jaringan maupun keamanannya. Target utama *attacker* sebelum masuk pada sistem utama atau pusat data adalah dengan mematikan kinerja *router*. Hal ini dapat merugikan perusahaan jasa internet yang bekerja sama dengan perusahaan seperti perusahaan jasa keuangan, sekolah, universitas, warung internet, ataupun perusahaan *e -commerce* yang mengakibatkan transaksi berhenti. Hal Ini dapat membuat perusahaan melakukan pemutusan kontrak kerja sama antara penyedia layanan dengan perusahaan. Bagi *intruder, router* sangat berperan penting untuk melancarkan aksinya agar dapat masuk kedalam sistem utama atau pusat data yang diinginkan untuk melakukan tindak kejahatan. pngendalian penuh pada *router* menyebabkan jaringan lain yang terhupung pada *router* juga dapat dikendalikan. Inilah sebabnya mengapa banyak penyerang akan menargetkan *router* dan melancarkan serangan terhadap mereka. Serangan-serangan ini dapat fokus pada kesalahan konfigurasi, kerentanan diketahui, atau bahkan *password* yang lemah. *Router* dapat diserang dengan mendapatkan akses ke router dan mengubah konfigurasi *file*, meluncurkan serangan *DDoS*, membanjiri *bandwidth*, atau keracunan tabel routing. Apabila *router* berhasil dikendalikan, maka konfigurasi dapat di hapus berseta jejaknya.

Salah satu metode yang sering digunakan oleh *intruder* adalah *distributed denial of service* (DDos). DDos merupakan sebuah metode serangan dengan mengirimkan banyak paket ke dalam dalam sebuah jaringan yang menyebabkan perangkat jaringan tidak lagi dapat berjalan sesuai fungsinya.

Dibutuhkan sebuah metode untuk mendeteksi kejadian pada *router* secara *real-time* agar dapat dianalisa dan menjadi dasar sebagai alat bukti yaitu dengan menggunakan *Intrusion Detection System (IDS)* pada *router forensics*. Berdasarkan pemaparan latar belakang diatas maka penulis akan melakukan penelitian berkaitan dengan "Analisis Forensik *Router* Untuk Mendeteksi Serangan *Distributed Danial of Service (DDoS)* Secara *Real Time*".

Penelitian ini bertujuan untuk menganalisa serangan *DDos* secara real time dengan memanfaat sistem pendeteksi serangan menggunakan *intrusion Detection system (IDS)* pada router forensics untuk dapat menemukan dan menggumpulkan bukti digital

Penelitian ini dibatasi berdasarkan :

1. Menganalisa berdasarkan serangan *Distributed Denial of Service* (DDoS)
2. Penelitian di lakukan menggunakan perangkat *Router*
3. Menggunakan fasilitas *Snort* dan *Portsentry*
4. Untuk menemukan dan mengumpulkan bukti *digital* menggunakan fasilitas *log* pada sistem operasi *router*
5. Sistem operasi *router* berbasis *open source*

II. KAJIAN PUSTAKA

2.41. *Kajian Penelitian Terdahulu*

Penelitian serupa pernah dilakukan berberapa peneliti terdahulu sebagai berikut :

Penelitian yang dilakukan oleh Fadhila Nisya[2], dengan memanfaatkan program java untuk *alert intrusion detection system*, yaitu IDS yang sangat diperlukan untuk memberikan sebuah peringatan awal kepada kepada pengelola sistem saat terjadi sebuah aktifitas tertentu yang mencurigakan dengan mengacu pada pola serangan yang terdapat pada *signature* atau *rule*, sehingga *administrator* dapat melakukan tindakan pencegahan. Dengan pemrograman Java dapat dikembangkan sebuah *interface* sehingga *alert* dari IDS tersebut dapat diterima administrator melalui sebuah pesan singkat (SMS).

Penelitian yang di lakukan oleh Sahid Aris Budiman[3], yang membahas tentang pemanfaatan IDS menggunakan media jejaring sosial sebagai pemberitahuan atau notifikasi. Berdasarkan tes, sistem ini mampu mengolah data keluaran dari Snort IDS dan juga dapat mengenali semua kegiatan yang dibuat oleh penyusup dalam upaya untuk masuk ke dalam sistem dengan cara membanjiri *ping*, melakukan serangan *syn*, teknik *port scanning*, merusak *Secure Shell* (SSH) dan *File Transfer* Protocol (FTP) yang berlandaskan pada aturan yang sudah ditetapkan. Kemudian melakukan pemblokiran alamat IP yang dianggap sebagai penyusup setelah itu sistem akan memberikan laporan kepada administrator melalui media sosial dan sistem *monitoring web*.

Penelitian yang dilakukan oleh Imam Riadi[4] dengan judul "*Log Analysis Techniques using Clustering in Network Forensics*" yaitu Proses dari mengidentifikasi serangan yang terjadi juga membutuhkan dukungan dari kedua hardware dan software juga. Serangan itu terjadi di jaringan internet secara

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

umum dapat disimpan dalam file log yang memiliki format data yang spesifik. Teknik *Clustering* merupakan sebuah metode yang dapat dimanfaatkan untuk mempermudah proses identifikasi. Memiliki dikelompokkan file data log menggunakan metode *K-Means* dengan teknik klastering, kemudian data tersebut dikelompokkan menjadi tiga kategori serangan, dan akan dilanjutkan dengan proses forensik yang nantinya dapat diketahui sumber dan target serangan yang ada dalam jaringan. Ini menyimpulkan bahwa kerangka yang diusulkan dapat membantu penyidik dalam proses persidangan.

Penelitian yang dilakukan I Wayan Bevin Waranugraha[5] yaitu membahas tentang pemanfaatan Aplikasi Forensik Jaringan Terdistribusi Menggunakan JADE, sesuai dengan pesatnya perkembangan dunia internet saat ini mengakibatkan adanya usaha maksimal dari suatu organisasi dan juga individu untuk membuat sebuah keamanan dalam jaringan karena sangat memungkinkan datangnya sebuah serangan. Sulitnya untuk menidak lanjuti sebuah kasus kriminal di Indonesia, apalagi dengan kurang lengkapnya bukti-bukti yang menjadi dasar untuk menjerat pelaku kejahatan. Dengan adanya forensik jaringan, administrator jaringan dapat melakukan sebuah terobosan baru untuk menemukan dan mengumpulkan bukti-bukti kejahatan tersangka, sehingga memudahkan penanganan kasus *cyber crime* yang terjadi.

Perbedaan penelitian ini dengan penelitian yang dilakukan beberapa penelti diatas terletak pada objek penelitian, *tools*, *platform* OS, fokus penelitian dan hasil yang diharapkan.

2.42. *Intrusion Detection System (IDS)*

Intrusion Detection System (IDS) merupakan sistem pengamanan yang digunakan sebagai *secondary* sistem yang telah ada atau sistem dibuat untuk mem-backup sistem keamanan yang utama. IDS merupakan penghambatan atas semua serangan yang akan mengganggu sebuah jaringan. IDS memberikan peringatan kepada administrator *server* saat terjadi sebuah aktivitas tertentu yang tidak diinginkan *administrator* sebagai penanggung jawab sistem. IDS juga dapat melakukan analisa terhatap lalu lintas data jaringan yang masuk dan keluar sebagai dasar untuk menemukan bukti dari pelaku serangan.

Terdapat dua jenis IDS, yaitu :

1. *Host-Based IDS (HIDS), Host-Based IDS* memperoleh informasi dari data yang dihasilkan oleh system pada sebuah komputer yang diamati. *Data Host-Based IDS* biasanya berupa *log* yang dihasilkan dengan memonitor *system file*, *event*, dan keamanan pada Windows NT dan *syslog* pada lingkungan system operasi UNIX. Saat terjadi perubahan pada *log* tersebut, dilakukan analisis untuk mengetahui apakah sama dengan pola yang ada pada database IDS.
2. *Network-Based IDS (NIDS) Network IDS* menempati jaringan secara langsung dan melihat semua aliran yang melewati jaringan. *Network-Based IDS* adalah cara yang paling efektif untuk memantau sebuah *traffic* yang masuk ataupun *traffic* yang keluar diantara *host* ataupun diantara segmen jaringan lokal.

2.43. *Aspek – Aspek Ancaman Keamanan*

Aspek-aspek ancaman serangan yang umum di ketahui adalah sebagai berikut :

1. *Interruption*
   Merupakan ancaman terhadap availability. Informasi dan data yang merupakan sistem komputer dirusak dan dihapus sehingga jika dibutuhkan, data atau informasi tersebut tidak lagi ada.
2. *Interception*
   Ancaman terhadap interception terletak pada kerahsiaan (secrecy). Informasi yang ada disadap atau orang yang tidak berhak mendapat akses ke komputer dimana informasi tersebut disimpan.
3. *Modification*
   Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan di ubah sesuai keinginan orang tersebut. Contoh dari serangan ini adalah mengubah pesan dari website dengan pesan yang merugikan pemilik website
4. *Fabrication*
   Ancaman yang di hadapi adalah terletak pada integritas. Orang yang tidak berhak berhasil memalsukan suatu informasi yang ada sehingga orang lain yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh penerima pesan tersebut.

2.44. *Mendeteksi Serangan*

Untuk mendeteksi atau mengenali sebuah serangan yang dilakukan *intruder*, dapat menggunakan data yang telah diperoleh. Pendekatan yang sering digunakan untuk mengenali serangan antara lain :

a. *Anomaly Detection*
   Anomaly detection (deteksi penyimpangan) mengidentifikasi prilaku tak lazim yang terjadi pada host atau netwok. *Detector* berfungsi dengan asumsi bahwa serangan tersebut berbeda dengan aktivitas normal. Serangan itu dapat dideteksi dengan sistem yang mampu mengidentifikasi perbedaan tersebut. *Anomaly detector* menyusun profil-profil yang merepresentasikan kebiasaan user atau host yang

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

normal dalam jaringan.. berdasarkan data-data yang didapat melalui histori maka selanjudnya di kumpulkan dalam tahap normal. Selanjudnya, detector melaksanakan mekanisme dengan mengumpulkan data-data peristiwa dan menggunakan cara-cara yang beragam ketika aktivitas yang diamati menyimpang dari normal.

b. Misuse Detection

Detector melakukan analisis terhadap aktivitas sistem, mencari aktivitas atau *set event* yang sesuai dengan pola prilaku yang dikenali sebagai serangan. Pola yang sering digunakan prilaku serangan itu disebut *signatures*. Maka dari itu, *misuse detection* sering disebut dengan *signaturebased detection*. [6]

2.45. *Digital Forensics*

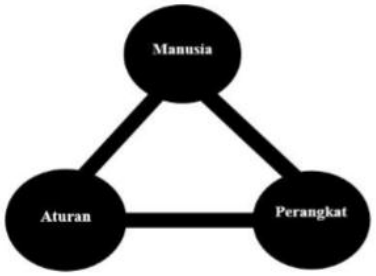
a. Sejarah *Digital Forensics*

Istilah *digital forensics* awalnya digunakan sebagai sinonim untuk komputer forensik tetapi telah diperluas untuk mencakup penyelidikan dari semua perangkat yang mampu menyimpan digital data. Dengan akar dalam revolusi komputasi pribadi 1970-an dan awal 1980-an, disiplin berkembang secara serampangan selama 1990-an, dan itu tidak sampai awal abad ke-21 bahwa kebijakan nasional muncul.

Selain menemukan bukti langsung dari kejahatan, digital forensik dapat digunakan untuk atribut bukti tersangka tertentu, mengkonfirmasi alibi atau pernyataan, menentukan niat, mengidentifikasi sumbersumber (misalnya, dalam kasus hak cipta), atau mengotentikasi dokumen. Penyelidikan jauh lebih luas dalam lingkup dari area lain dari analisis forensik (dimana biasa tujuannya adalah untuk memberikan jawaban atas serangkaian pertanyaan sederhana) sering melibatkan waktu baris kompleks atau hipotesis.

b. Komponen *Digital Forensics*

Komponen pada *digital forensics* pada umumnya hampir sama dengan bidang yang lain. Komponen ini mencakup manusia (people), perangkat/peralatan yang digunakan serta serangkaian aturan yang dirangkai sedemikian rupa agar dapat dikelola dan diberdayakan dalam upaya mencapai tujuan akhir dengan segala kelayakan dan kualitas sebagaimana bisa dilihat pada Gambar 1.



Gambar 1. Komponen Digital Forensic

2.46. *Network Forensics*

Network forensics[7] merupakan bagian dari *Digital forensics* yang berhubungan dan berkaitan erat dengan monitoring dan menganalisa lalu lintas jaringan komputer untuk tujuan pengumpulan informasi, bukti hukum atau deteksi instrusi. Istilah *forensics* memang di ambil dari terminology yang berhubungan dengan kriminologi. Network forensics bekerja berdasarkan pada pencarian data dan informasi yang berkaitan dengan kejahatan yang menggunakan fasilitas jaringan komputer.

2.47. *Router*

Router adalah perangkat jaringan komputer yang bertujuan untuk menghubungkan dua alamat jaringan yang berbeda. Semisal menghubungkan dua jaringan komputer yang berbeda kelas IP nya, jadi jika jaringan A mengunakan IP 192.168.1.2/24 (kelas C) serta jaringan B mengunakan IP 10.127.11.22/16 (kelas A), keduanya akan saling terhubung dengan adanya router sebagai jembatan ditengah-tengahnya[8].

III. METODOLOGI PENELITIAN

Dalam sebuah penelitian, seorang peneliti diharapkan mengetahui dan memahami tahap-tahap penelitian. Informasi mengenai tahap-tahap penelitian tersebut bisa di dapatkan dari saran peneliti terdahulu, referensi, jurnal-jurnal sebelumnya maupun situs-situs resmi di internet.

2.48. *Tahap Penelitian*

Adapun tahapan penelitian yang dilakukan dalam pemanfaatan IDS pada PC Router yang menggunakan sistem operasi debian adalah sebagai berikut:

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

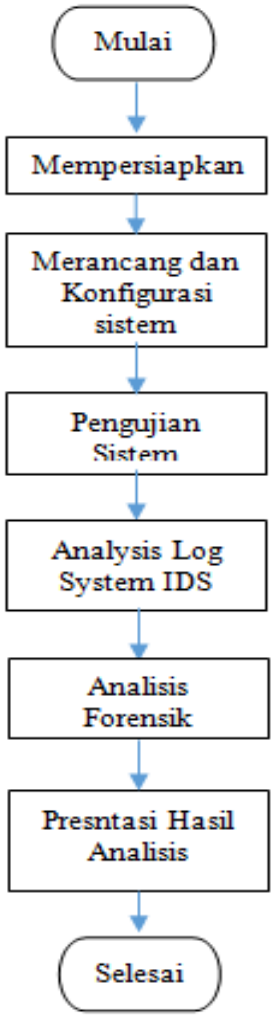
1. Merancang dan membangun jaringan serta melakukan penginstalan dan mengkonfigurasi *snort*, *portsentry* dan aplikasi pendukung lainnya yang dibutuhkan.
2. Merancang *interface* sebagai media notifikasi jejaring sosial sehingga dapat terhubung dengan IDS yaitu *whatsapp*.
3. Melaksanakan pengujian sistem pada PC *Router*. Apakah sudah berjalan sesuai dengan apa yang di harapkan.
4. Melakukan simulasi serangan terhadap router di dalam jaringan untuk menguji kemampuan *IDS* yang telah dikonfigurasi.
5. Mengumpulkan laporan yang telah dianalisa melalui log yang ada pada IDS
6. Melakukan analisa forensik pada *router* untuk menemukan bukti serangan dan pelaku penyerangan

2.49. *Alat dan Bahan*

Pada penelitian ini alat dan bahan yang digunakan adalah seperangkat komputer yang digunakan sebagai penyerang (intruder) dan sebuah *PC route*r yang menggunakan sistem operasi Debian dan Kali Linux sebagai analisa forensic digital. Perangkat Lunak (Software) yang dapat digunakan adalah:

1. *Snort* Sebagai perangkat lunak yang berfungsi untuk mendeteksi dating nya serangan.
2. Scaning *Port, libdnet, IPTables, TCP Wrapper, Syslog, Syslog-Notify, daq*, sebagai perangkat untuk mendukung aplikasi IDS snort.
3. Menggunakan software SQL dan Apache2 sebagai database pada interface notifikasi
4. Menggunakan *Basic Analysis and Security* (BASE) sebagai *web monitoring.*
5. Menggunakan bahasa pemrograman PHP untuk merancang dan membangun interface notifikasi.
6. Media notifikasi yang digunakan adalah aplikasi *Whatsapp*.
7. Menggunakan nmap, hydra,TCPdump, sebagai alat untuk menguji aplikasi IDS.

Adapun tahapan penelitian ini di jabarkan berdasaran alur diagram pada Gambar 2.



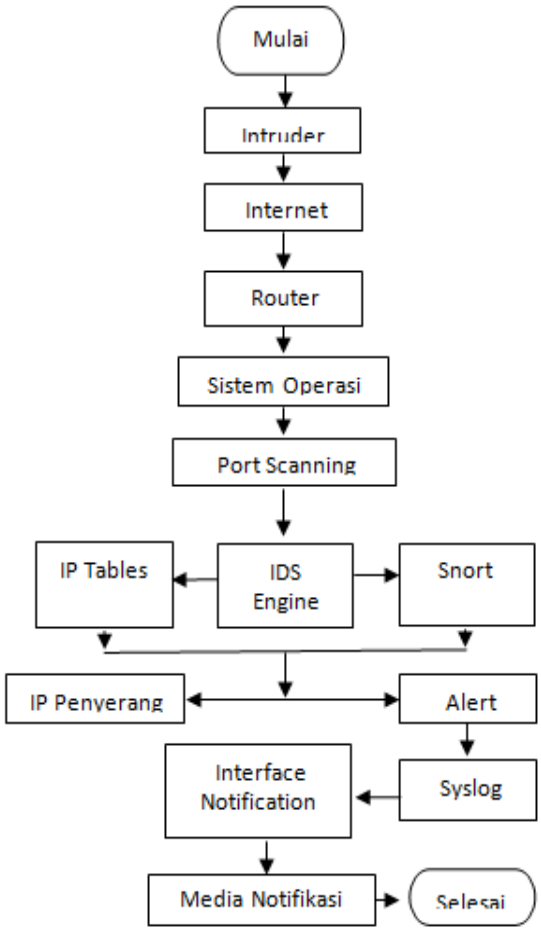
Gambar 2. Diagram Alur Tahapan Penelitian

IV. HASIL DAN PEMBAHASAN

2.50. *Alur Kerja Sistem*

Pada penelitian ini cara kerja sistem yang akan di bangun adalah seperti Gambar 3.

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id



Gambar 3. Flowchart Kerja Sistem

Pada Gambar 3 dapat di jelaskan cara kerja sistem yang akan di bangun sebagai berikut :

Paket data yang dikirim oleh *intruder* melalui *internet* akan masuk ke sistem operasi pada router melalui media kabel (ethernet). Lalu paket data tersebut ditangkap atau dideteksi oleh capture library. *Port scanning* yang merupakan kegiatan atau metode untuk mendeteksi *port* yang aktif pada host maupun komputer target. *Port scanning* merupakan langkah awal menandakan bahwa akan ada suatu serangan atau usaha penyusupan terhadap sistem tersebut sebelum akhirnya serangan IDS masuk. Melalui IDS sistem akan mendeteksi dan memeriksa sebuah serangan melalui tabel *routing* yang terdapat pada firewall, selanjudnya *Snort* akan memeriksa data-data yang masuk dan melaporkan ke administrator untuk menyatakan apakah sebuah paket data dianggap sebagai serangan atau bukan, paket data akan dicocokkan dengan rule IDS, jika terdapat dalam *rule*, maka paket data tersebut dianggap sebagai penyusupan/serangan dan demikian juga sebaliknya jika tidak ada dalam *rule* maka dianggap bukan penyusupan/serangan.

Pada saat adanya kemiripan pada paket data yang diterima dengan *rules* yang ada, *Snort* akan menghasilkan peringatan dan kemudian melakukan logging. Lalu semua kegiatan akan di catat melalui *alert* yang tersimpan pada *syslog*. *Interface notification* akan menyampaikan pesan kepada media notifikasi melalui *instan messanger whatsapp* apabila ada terjadi serangan.

Hasil yang harapkan melalui penelitian ini adalah proses analisa berjalan dengan baik melalui pemanfaatan *intrusion detection system (IDS*), administrator dapat menemukan bukti digital serta pelaku serangan melalui perangkat *router* yang digunakan sebagai objek penelitian.

DAFTAR PUSTAKA

[1] Antaranews.com (3 juni 2016) Serangan Siber Ke Indonesia Meningkat Pesat. Diakses 6 Oktober 2016

[2] Fadhila Nisya Tanjung, Muhammad Irwan Padli Nasution, (2012) *Implementasi Pemrograman Java Untuk Alert Intrusion Detection System*, pematang siantar, 31 agustus – 2 september 2012, ISBN 978-602-18749-0-5

[3] Sahid Aris Budiman, Catur Iswahyudi, Muhammad Sholeh, (2014), *Implementasi Intrusion Detection System (Ids) Menggunakan Jejaring Sosial Sebagai Media Notifikasi*, Yogyakarta, 15 November 2014, ISSN: 1979-911X

[4] Riadi imam (2012), "*Log Analysis Techniques using Clustering in Network Forensics*", International Journal of Computer Science and Information Security (IJCSIS) , Vol. 10, No.7

[5] I Wayan Bevin Waranugraha, Ary Mazharuddin S. , dan Baskoro Adi Pratomo (2012), *Aplikasi Forensik Jaringan Terdistribusi Menggunakan JADE*, Jurnal Teknik Pomits Vol. 1, No. 1, (2012) 1-6.

[6] Ariyus Doni, 2006, *Computer Security*, Andi, Yogyakarta

[7] Faisal Riyadi, (2014), *Forensik Jaringan Pada Lalu Lintas Data Dalam Jaringan Honeynet Di Indonesia Security Incident Respone Team On Internet Infrastructure/Coordination Center*, Jurnal ICT Penelitian dan Penerapan Teknologi

[8] Azikin Askari, 2011, Debian GNU/Linux, Informatika, Bandung ISBN : 978-602-8758-28-24

[9] Yogi Surya Nugroho, 2015, Investigasi Forensik Jaringan Dari serangan DDoS menggunakan metode Naïve Bayes, *skripsi*, Fakultas Sains dan Teknologi, UIN Sunan kalijaga, Yogyakarta.

[10] Kemmish, R. M, 2015, What is forensic computer. Australian institute of Criminology, Canberra.

[11] Iswardani Ardymulya, Riadi Imam, 2016, " Danial of Service Log Analysis Using Density K-Means Method", Journal of Theoretical & Applied Information Technology, Vol. 83 Issue 2, ISSN: 1992-8645.