SIMULASI SISTEM DETEKSI PENYUSUP DALAM JARINGAN KOMPUTER BERBASIS WEB INTERFACE SERTA PENCEGAHAN UNTUK MENINGKATKAN KEAMANAN

Sukma Ageng Prihasmoro[1], Yuliana Rachmawati[2], Erfanti Fatkhiyah[3]
[1,2,3] Jurusan Tekik Informatika, Fakultas Teknologi Industri,
Institut Sains & Teknologi AKPRIND Yogyakarta
[1] sukma.ageng@gmail.com, [2] yuliana@akprind.ac.id, [3] erfunthyie@yahoo.co.id

ABSTRACT

Network security is a matter that needs to be given special attention, because infiltration often occurs with a variety of purposes. Intrusion detection systems (IDS) is a method of network security by detecting intrusion and provide output results in the form of alerts that can be known through the web. To implement the various components of the detection system is needed in order to maximize performance. In this study, the application is used as a detection system Snort attack. Basic Analysis and Security System (BASE) is used as a web interface. Log storage media attacks using MySQL. Fields marked with an ICMP protocol detection system ie, TCP and UDP. To follow up, use iptables and portsentry in the IP address blocking intruders. Attacks that occur can be analyzed using BASE, this application can indicate the type of attacks carried out and can see the span of attack for several months. By analyzing the types of attacks that occur, can help administrators reinforce the gap.
Keywords : IDS, *intruder, network security*

INTISARI

Keamanan jaringan merupakan hal yang perlu diberi perhatian khusus, karena penyusupan sering terjadi dengan berbagai tujuan. *Intrusion detection system* (IDS) adalah sebuah metode pengamanan jaringan dengan mendeteksi penyusupan dan memberikan hasil *output* berupa *alert* yang dapat diketahui melalui web. Untuk mengimplementasikan sistem deteksi diperlukan berbagai komponen agar kinerjanya lebih maksimal. Pada penelitian ini aplikasi snort digunakan sebagai sistem deteksi serangan. Basic Analysis and Security System (BASE) digunakan sebagai web *interface*. Media penyimpanan log serangan menggunakan MySQL. Bagian yang diberi sistem deteksi yaitu protokol ICMP,TCP dan UDP. Untuk tindak lanjut, digunakan iptables dan portsentry dalam melakukan pemblokiran IP *address* penyusup. Serangan yang terjadi dapat dianalisa menggunakan BASE, aplikasi ini dapat menunjukkan jenis serangan yang dilakukan serta dapat melihat rentang waktu serangan selama beberapa bulan. Dengan menganalisa jenis serangan yang terjadi, dapat membantu administrator memperkuat celah tersebut.
Kata Kunci : IDS, penyusup, keamanan jaringan

PENDAHULUAN

Teknologi jaringan komputer merupakan sarana yang menjadi keharusan dalam pertukaran informasi. Karena pentingnya data dan informasi tersebut, beberapa pihak yang tidak bertanggung jawab dapat menyalahgunakan untuk kegiatan yang melanggar peraturan. Gangguan tersebut dapat terjadi karena adanya celah kelemahan yang dimanfaatkan oleh pihak yang tidak bertanggung jawab. Dari permasalahan tersebut, seorang *administrator* membutuhkan suatu sistem yang dapat membantu mengawasi jaringan, pemberitahuan serangan dan mengambil tindakan tepat untuk penanganan. Salah satu tindak pengamanan jaringan komputer yang dapat dilakukan untuk mendeteksi serangan yaitu dengan menerapkan Intrusion Detection System (IDS). IDS merupakan sistem deteksi dari

penyusupan. Suatu *Intrusion Detection System* (IDS) dapat didefinisikan sebagai tool, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan komputer (Ariyus, 2007). Pada penelitian ini menggunakan snort sebagai pendeteksi yang dikombinasikan dengan beberapa *software* lainnya dapat mengenali jenis serangan yang dilancarkan penyusup serta memberi laporan tentang adanya serangan. Jika telah diberi sistem pendeteksi penyusup, tindakan selanjutnya adalah dengan memberi cara menghentikan dan pencegahan atas penyusupan tersebut.

Penelitian ini disusun berdasarkan beberapa penelitian yang telah dilakukan sebelumnya yang berjudul "Sistem Deteksi dan Penanganan Intrusi Menggunakan Snort dan Base" (Kurniawan, 2010). Pada penelitian tersebut pemberitahuan adanya serangan masih melalui web, tindak penyerangan masih belum fokus pada jaringan yang ingin diserang. Selain itu, belum ada tindakan penanganan serangan, hanya melakukan sistem deteksi serangan. Jurnal publikasi lain yang membahas tentang Intrusion Detection System yaitu "Sistem Monitoring Deteksi Penyusup Dalam Jaringan Komputer Menggunakan Snort Pada Ubuntu 12.04 Berbasis SMS Gateway" (Diarta, 2013), Pada penelitian tersebut terdapat pemberitahuan serangan melalui SMS namun tidak ada tindakan pencegahan dan penanganan serangan. Selain itu tidak adanya interface berbasis web untuk menganalisa serangan. Adapun jurnal lain yang membahas tentang Intrusion Detection System yaitu "Nagois Untuk Monitoring Server Dengan Pengiriman Notifikasi Gangguan Server Menggunakan Email dan SMS Gateway" (Asri, 2013). Menjelaskan tentang monitoring server mengenai masalah notofokasi error dan gangguan servis. Belum ada hal spesifik yang mengarah kepada keamanan dari jaringan tersebut.

Intrusion Prevention System (IPS) merupakan suatu tindakan yang dilakukan untuk menghentikan serangan yang dilakukan penyusup setelah terjadinya sistem deteksi oleh IDS. Penelitian ini akan mengkombinasikan sistem IDS dan IPS yaitu *Intrusion Detection and Prevention System* (IDPS). IDPS berfokus pada pendeteksian dan penanganan penyusupan. IDPS memberikan *report* atau laporan kepada *administrator* jaringan *berdasarkan port-port,* protokol maupun jenis serangan yang dilakukan, dengan mengetahui serangan yang dilakukan dapat membantu *administrator* dalam mengatasinya. Dalam melakukan tindak penanganan serangan digunakan *software* IPtables dan portsentry. Jika terjadi tindakan penyusupan, IPtables dan portsentry dapat melakukan pemblokiran IP *address*. Pemantauan serangan yang terjadi dapat dilihat menggunakan *command line* pada komputer *server*. Untuk mempermudah pemantauan dan analisa serangan dapat dilihat pada web *interface Basis Analysis and Security Engine* (BASE).

METODE PENELITIAN

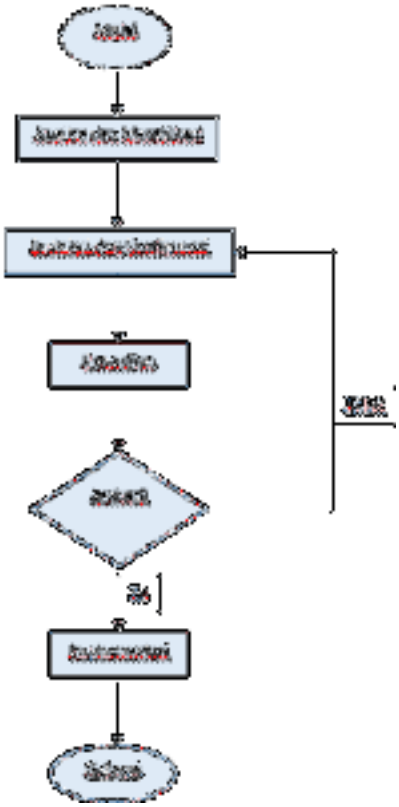
Dalam penelitian ini, langkah yang dilakukan dalam implementasi keamanan jaringan komputer adalah sebagai berikut:

1. Mengidentifikasi kebutuhan sistem yang ingin digunakan dalam penelitian.
2. Menginstall serta konfigurasi aplikasi yang dibutuhkan oleh sistem keamanan jaringan.
3. Melakukan pengujian terhadap komputer *server* untuk mengetahui keberhasilan sistem keamanan.
4. Jika sistem keamanan belum berfungsi dengan baik, perlu dicermati tahapan dalam konfigurasi aplikasi.
5. Melakukan analisa log serangan yang terjadi, *log* akan ditampung dalam *database.*

Perangkat lunak yang digunakan pada penelitian keamanan jaringan komputer ini adalah sebagai berikut :

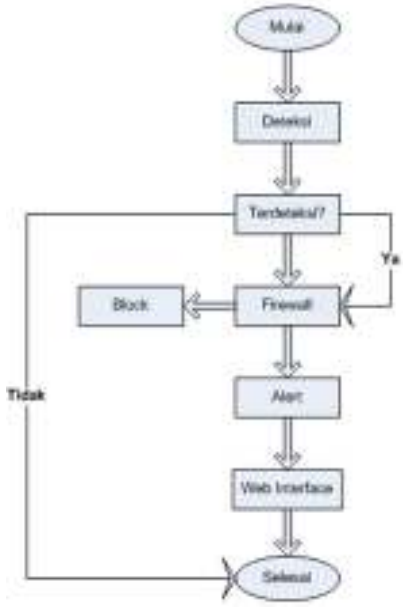
1. Sistem Operasi Linux Ubuntu 14.04 LTS yang digunakan sebagai *server* serta Ubuntu 14.04 sebagai *attacker.*

2. Mysql dan apache berguna untuk keperluan *server*.
3. BASE untuk memonitoring jaringan melalui web.
4. Paket pendukung snort seperti libpcap, libdnet, daq, snort rules.
5. ADODB kumpulan *library* PHP untuk komunikasi dengan database.
6. Snort sebagai *software* pendeteksi.
7. Barnyard2 berfungsi menyimpan *database Log* ke mysql.
8. IPtables digunakan sebagai *firewall* pada jaringan.
9. NMAP, Hydra, Angry IP sebagai *software* penguji keamanan.
10. Portsentry berfungsi untuk merespon *scanning port* secara *real time*.
11. Microsoft Visio untuk membantu perancangan sistem.



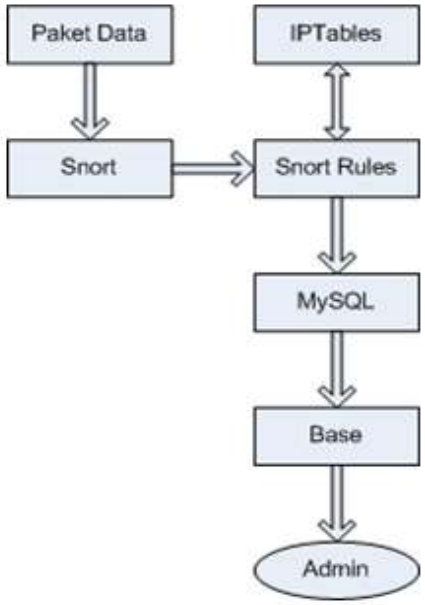
Gambar 1. Diagram Alir Penelitian

Diagram Alir IDS menunjukkan gambaran dari sistem IDS yang dikombinasikan dengan tindak pencegahan serangan. Jika terdeteksi sebagai ancaman maka *firewall* akan melakukan blokir kemudian alerts dari serangan tersebut dapat diketahui oleh administrator melalui media email serta *web*. Jika bukan merupakan suatu ancaman maka tidak ada reaksi apapun dari IDS. *Administrator* dapat menganalisa serangan melalui aplikasi berbasis *web*, pada penelitian ini menggunakan Base. Diagram alir menunjukkan gambaran tentang jalannya sistem keamanan jaringan IDS yang tampak pada gambar 2 dibawah.

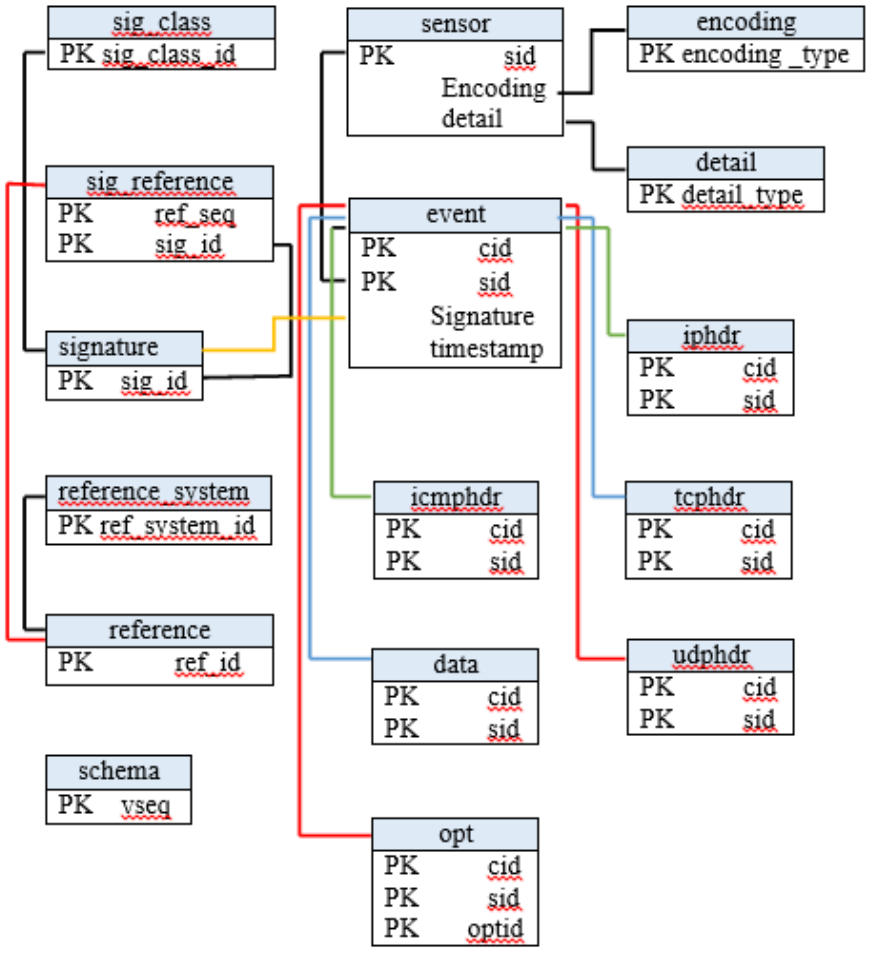


Gambar 2. Diagram Alir IDS

Sistem IDS membutuhkan beberapa modul untuk mendukung pendeteksian serta pencegahan serangan. Gambar III.3 menunjukkan rancangan modul sistem IDS



Gambar 3. Modul Sistem IDS



Gambar 4. *Database* Snort

PEMBAHASAN

Pengujian dilakukan dengan menghubungkan dua laptop sebagai *client* dan *server.* Pada sisi *server* telah terinstall IDS dan pada *client* telah terinstall *software* penguji. Serangan yang dilakukan yaitu meliputi IP *scan*, port *scan*, DOS attack, SSH dan FTP. Dibawah ini merupakan snort rules yang berguna untuk mendeteksi serangan.

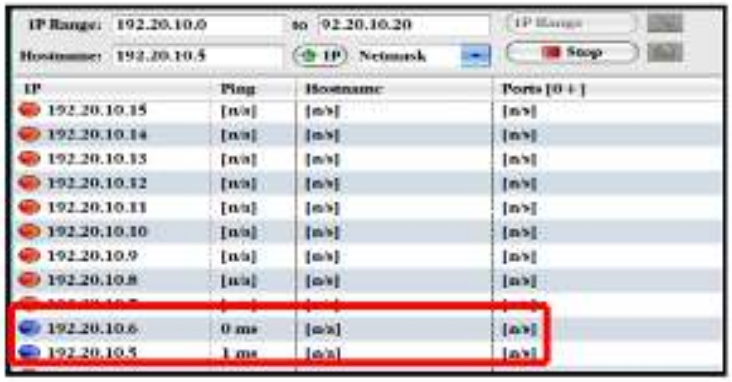
alert tcp any any -> any any (msg:"SYN *Scan*"; sid:90000011;)
alert tcp any any -> any any (msg:"XMAS *Scan*"; flags: FPU;sid: 90000022;)
alert UDP any any -> any any (msg:"UDP *Scan*"; sid: 90000033;)
Alert tcp any any -> $HOME_NET any (;msg:"PING attack ICMP traffic!!!"; sid:9000003; rev:3;)
Alert tcp any any -> any 22 (;msg:"SSH threat!!!";sid:9000004;rev:4;).
Alert tcp any any -> any 21 (;msg:"FTP Threat!!!"; sid:9000005;rev:5;)

Skenario Pengujian

Pada bagian ini akan dilakukan pengujian sistem yang telah dirancang berdasarkan bab sebelumnya. Pengujian sistem dilakukan dengan menggunakan beberapa aplikasi peguji keamanan untuk mengetahui apakah IDS telah berjalan dengan baik. Metode yang digunakan untuk menguji apakah IDS dapat berfungsi sesuai kebutuhan yang diinginkan. *Port-port* mana saja yang diberi sistem deteksi serta jenis serangan. Log serangan juga harus masuk ke dalam *database* serta dapat dianalisa melalui aplikasi *web interface*. Berikut merupakan skenario pengujian dalam penelitian ini.

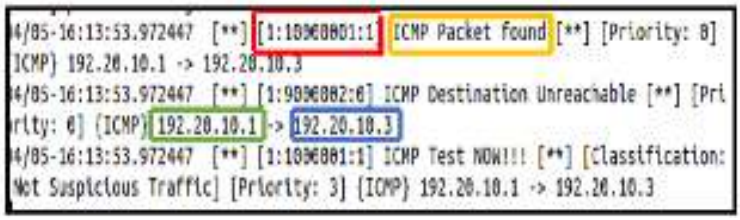
IP *scan*ner

Dengan aplikasi IP *scan*ner ini juga dapat mengetahui IP *address* mana saja yang terkoneksi dengan jaringan dan juga mengetahui nama komputer dari pemakai IP *address* tersebut.



Gambar 5. IP *scan*

Range IP *address* yang akan di *scan* 192.20.10.0-192.20.10.255. Setalah di *scan* akan tampilnya hasilnya beserta status dari IP *address* tersebut. Jika berwarna biru maka aktif dan jika berwarna merah tidak aktif.

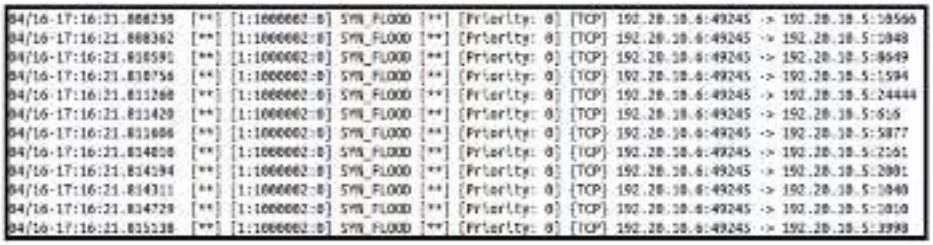


Gambar 6. Respon IP *scan*

Port *Scan*

Port Scanning merupakan aktivitas yang dilakukan untuk mengetahui status suatu *port* apakah terbuka atau tertutup. Pada pengujian ini, aplikasi *open source* yang digunakan yaitu NMAP(*Network Mapper*).

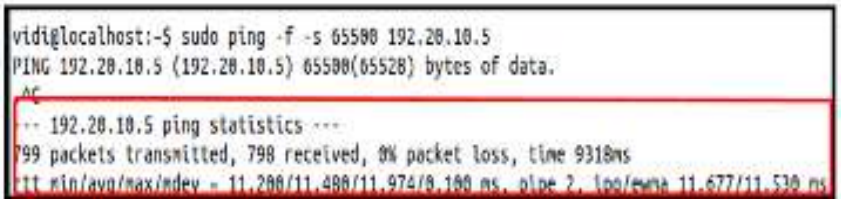
Gambar 7. Port *scan* (SYN *scan*)



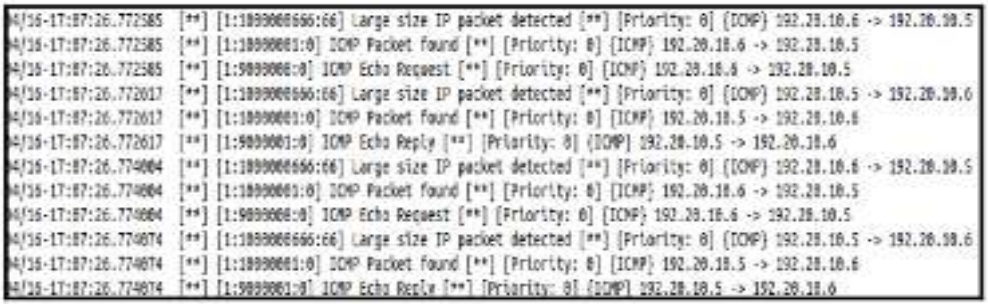
Gambar 8. Respon Port *scan* (SYN *scan*)

PING *Attack* (ICMP traffic)

Merupakan salah satu jenis serangan denial of service attack. Dengan mengirimkan paket dalam jumlah yang sangat besar terhadap server dengan tujuan membuat crashing koneksi TCP/IP dan menjadikan TCP/IP menjadi tidak lagi merespon berbagai request paket. ICMP *Traffic*).



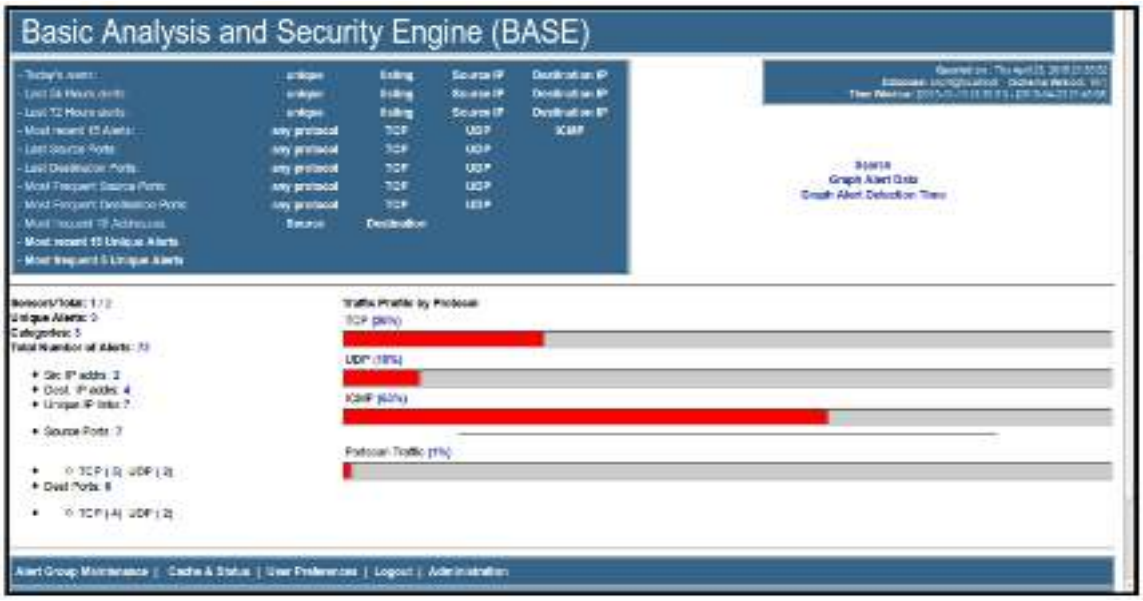
Gambar 9. PING attack (ICMP traffic)



Gambar 10. Respon PING attack (SYN *scan*)

Hasil Serangan Melalui BASE

Hasil serangan yang telah terjadi akan ditampilkan pada BASE. Berikut hasil serangan yang telah terdeteksi.



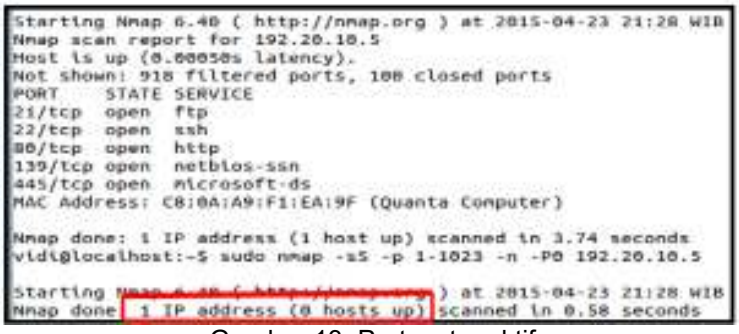
Gambar 11. Hasil deteksi

Gambar 8 menunjukkan jenis serangan yang terjadi pada *server* berdasarkan jenis protokol yaitu TCP,UDP serta ICMP. Untuk melihat statistik serangan dalam beberapa bulan tampak pada gambar IV.28. Manfaat dari BASE ini adalah untuk menganalisa serangan terhadap *server*.

Gambar 12. Statistik serangan

Pengamanan *Port* Menggunakan Portsentry

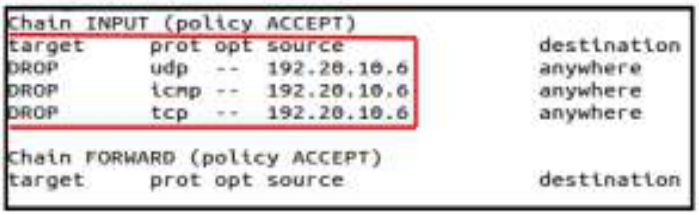
Portsentry merupakan aplikasi yang digunakan untuk menghindari berbagai aktifitas *scan*ning. Portsentry dapat mengingat IP address dari penyerang. *Scan* terhadap server membuat server seolah-olah terlihat down bahkan semua port terlihat tertutup. Portsentry membuat server memblok IP address tersebut secara otomatis, tujuannya adalah untuk melindungi dari *scan*ning.



Gambar 13. Portsentry aktif

Pengamanan Serangan Menggunakan IPtables

Firewall merupakan sistem yang digunakan untuk mengatur hak akses suatu segmen jaringan. Firewall pada umumnya digunakan untuk menentukan kebijakan jaringan bertujuan untuk meningkatkan sistem keamanan. Iptables merupkana modul kernel linux yang digunakan untuk memfilter paket-paket data, IPtables sudah terinstall didalam linux. Perlu beberapa konfigurasi untuk menggunakannya.



Gambar 15. Rules IPtables

Tabel 1. Jumlah serangan

Dalam penelitian ini menggunakan skenario pengujian selama empat bulan untuk mengetahui jumlah serangan tiap bulan. Dalam kurun waktu empat bulan, *alert* terbanyak yaitu jenis serangan DOS *attack* disusul SSH di urutan kedua.

KESIMPULAN

1. IDS mampu mendeteksi serangan berupa IP *scan*, Port *scan*, Ping *attack* maupun penggunaan hydra yangg mencoba *login* SSH dan FTP. Dalam mendeteksi serangan, IDS melakukan *scanning* lalu lintas dalam jaringan.
2. Aplikasi yang berguna sebagai alat pertahanan yaitu portsentry dan IPtables juga bekerja dengan baik dalam melakukan pemblokiran IP *address* penyusup.
3. Sistem IDS memberikan informasi serangan melalui web untuk dapat dianalisa oleh *administrator*.
4. Perpaduan antara sistem deteksi dengan *firewall* merupakan suatu metode yang dinamakan Intrusion Detection and Prevention System (IDPS).

DAFTAR PUSTAKA

Ariyus, D. (2007). *INTRUSION DETECTION Sydtem.* Yogyakarta: Penerbit Andi

Asri, N. F. (2013). Nagois Untuk Moitoring Server Dengan Pengiriman Notifikasi Gangguan Server Menggunakan Email dan SMS Gateway . *Skripsi*.

Diarta, E. (2013). Sistem Monitoring Deteksi Penyusup Dalam Daringan Komputer Menggunakan Snort Pada Ubuntu 12.04 Berbasis SMS Gateway. *Skripsi*

Kurniawan, I. A. (2010). Sistem Deteksi dan Penanganan Intrusi Menggunakan Snort dan BAse. *Skripsi*.