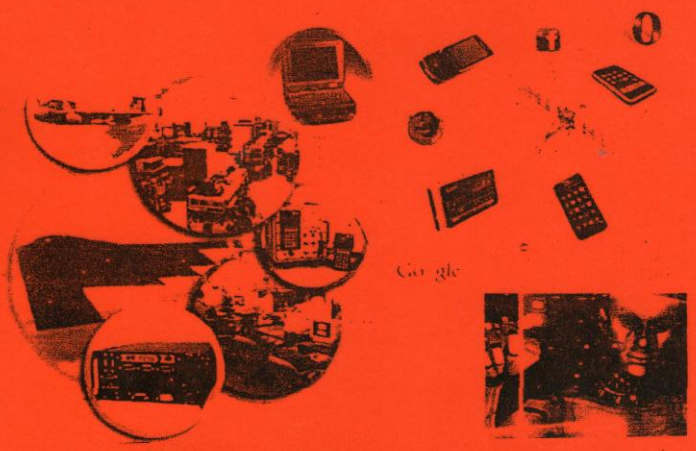
5TH DISC 2013

Digital Information & Systems Conference

28 September 2013

"Learning, Arts and Technology For A Better World"



Computer Engineering Dept.
Faculty of Engineering
UK. Maranatha

Buku 1B

ISBN : 978-979-1194-11-2

ANALISA KEAMANAN JARINGAN TERHADAP ANCAMAN DATA *FLOODING* PADA BADAN PENANGGULANGAN BENCANA DAERAH PROV. SUM-SEL

Irwansyah[1], Rambo Paulan[2]
Dosen Universitas Bina Darma [2], Mahasiswa Universitas Bina Darma [2]
Jalan Jenderal Ahmad Yani No.12 Palembang
Pos-el : i_one1111@yahoo.com[1], indonesia_rambopaulan@rocketmail.com[2]

Abstrak : *Kecenderungan penggunaan internet disebabkan oleh adanya kemudahan dalam hal komunikasi dan transfer data. Tetapi disamping kelebihan yang banyak tersebut, internet juga mempunyai banyak kekurangan salah satu yang sangat menjadi kendala adalah dalam bidang keamanan, dikarenakan internet merupakan sumber informasi yang mudah diakses dimana saja kapan saja serta oleh siapa saja. Hal ini menyebabkan internet menjadi salah satu infrastruktur yang rentan terhadap masalah keamanan jaringan. Untuk itu setiap perusahaan atau instansi-instansi perkantoran memiliki sistem keamanan dalam menjaga informasi dan data yang ada di internet supaya tidak dirusak oleh pihak-pihak yang tidak bertanggung jawab. Serta mampu mencegah terjadinya gangguan dari luar yang dapat menyebabkan terjadinya data flooding pada jaringan komputer yang terhubung dengan internet. Pada penelitian ini penulis menyajikan analisa keamanan jaringan terhadap ancaman Data Flooding pada Badan Penanggulangan Bencana Daerah Provinsi Sumatera Selatan.*

Kata kunci : *Internet, Data flooding, jaringan.*

1. PENDAHULUAN

Banyaknya perusahaan atau lembaga yang menggunakan internet sebagai sarana untuk membantu dalam melaksanakan aktifitas rutin perusahaan dan aktifitas rutin lainnya, kemudahan dan kepraktisan merupakan kunci dari mengapa dipilihnya internet ini. Sehinga internet menjadi salah satu daftar penting dalam suatu perusahaan ataupun instansi-instansi pemerintah lainya.

Disamping kelebihan tersebut, internet juga mempunyai banyak kekurangan yang sangat mengkhawatirkan bagi para penggunanya ataupun instansi instansi perkantoran yang mengunakan internet, sepeti kejahatan komputer, yang meliputi pencurian, penipuan, kompetitif, banyak lagi yang lainya, seperti jatuhnya informasi ke pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik infrormasi. (Ariyus : 2006) Banyak kasus yang membuktikan bahwa perusahaan yang tersambung di internet sering kali mendapatkan gangguan baik dalam data yang dimiliki maupun peralatannya. Kerugian yang diderita akan hal ini bisa dibilang tidak kecil.

Dalam faktor keamanan ini salah satu serangan yang sering muncul adalah data *flooding*. Data *flooding* merupakan suatu kejadian di dalam jaringan dimana dalam jaringan tersebut terjadi suatu transfer data dalam jumlah yang besar sehingga mengganggu kinerja komputer yang terhubung di dalam jaringan tersebut. Hal ini kemungkinan bisa disebabkan adanya serangan dari luar yang biasa disebut dengan DOS/DDOS (*Denial of Service/ Distributed Denial of Services*) yaitu serangan pada jaringan komputer yang berusaha untuk menghabiskan sumber daya sebuah peralatan komputer, sehingga jaringan komputer menjadi terganggu. Untuk mengatasi hal itu biasanya digunakan sistem pertahanan didalam server itu sendiri yang bisa menganalisa langsung apakah setiap paket yang masuk tersebut adalah data yang diharapkan ataupun data yang tidak diharapkan. Kalau paket tersebut merupakan data yang tidak diharapkan, diusahakan agar komputer bisa mengambil tindakan untuk mengantisipasi agar serangan yang terjadi tidak menimbulkan kerugian yang besar.

Adapun tujuan dari penelitian ini adalah agar ancaman terhadap jaringan komputer terutama ancaman data *flooding* yang bisa terjadi kapan saja pada Instansi pemerintah Badan Penanggulangan Bencana Daerah Provinsi Sumatera Selatan yang melakukan aktifitas pertukaran informasi, serta laporan laporan bencana daerah ke Badan Nasional Penanggulangan Bencana Pusat dapat terjaga dengan baik .

2. PEMBAHASAN

2.1 Metode Penelitian

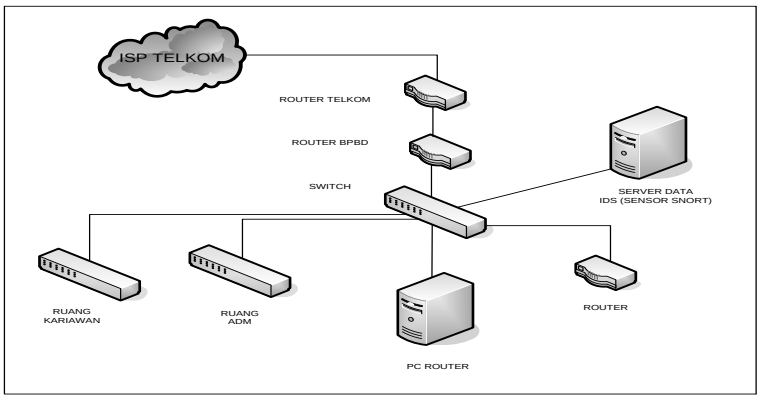
Action research atau penelitian tindakan merupakan salah satu bentuk rancangan penelitian yang mengutamakan tindakan secara langsung ke lapangan guna untuk mengetahui masalah apa yang sedang dihadapi dan upaya apa yang akan dilakukan dalam pemecahan masalah tersebut.

Tahapan yang dilakukan dalam *Action research* yaitu :

a. Melakukan diagnosa (*diagnosing*), dalam tahapan ini yang dilakukan adalah mengidentifikasi masalah keamanan jaringan terhadap ancaman data flooding pada instansi tersebut.
b. Membuat rancangan tindakan (*action planning),* dalam tahapan ini penulis mencoba memahami pokok permasalahan dan kemudian menyusun rencana untuk melakukan penelitian.
c. Melakukan tindakan (*action taking),* dalam tahapan ini penulis melakukan penelitian langsung pada pokok permasalahan yang sudah di diagnosa.
d. Pembelajaran (*learning*), pembelajaran atau *learning* ini adalah tahapan terakhir yang dilakukan penulis. Dalam tahapan ini penulis menganalisa data yang telah diperoleh dari penelitian tersebut.

2.2 Peta Peletakan *Intrusion Detention System (IDS)*

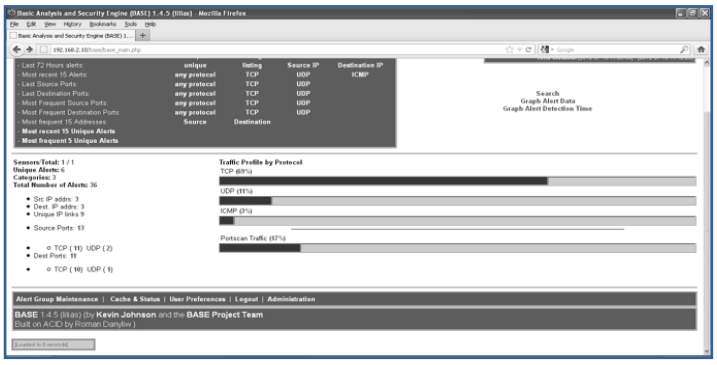
Peta peletakan *monitorigintrusion detektion system (IDS) Base* dengan mengunakan *Snort,* merupakan bentuk keadaan fisik suatu jaringan komputer yang digambarkan dalam suatu objek peta peletakan *IDS*. Sehinga dapat memberikan informasi kepada administrator jaringan tentang keadaan fisik *monitoring* tersebut. Untuk pengembangan *intrusion detektion system (IDS) Base* dengan menggunakan *Snort,* sebaiknya terlebih dahulu dilakukan pemetaan atau lebih sering kita dengar dengan istilah *maping* jaringan. *Maping IDS* merupakan salah satu hal yang penting sebelum kita melakukan inflementasi *IDS* (*intrusion detektion system*).



Gambar 2.1 Peta peletakan IDS sensor Snort pada server data.

Intrusion Detektion System (IDS) pada suatu jaringan akan dapat bekerja dengan baik, tergantung pada peletakannya. Secara prinsip pemahaman penempatan komponen *Intrusion Detektion System* (IDS) akan menghasilkan IDS yang benar-benar mudah untuk dikontrol sehingga pengamanan jaringan dari serangan menjadi lebih efisien. Untuk memenuhi kebutuhan dibutuhkan modul-modul utama dan modul pendukung. Modul utama berupa : *snort engine*, *rule snort, engine IDS* dan *firewall.* Sedangkan modul pendukung berupa BASE (*manajemen event*) dan webmin (*manajemen rule).*

2.4 Tampilan BASE dalam memproses *database* dari Snort.



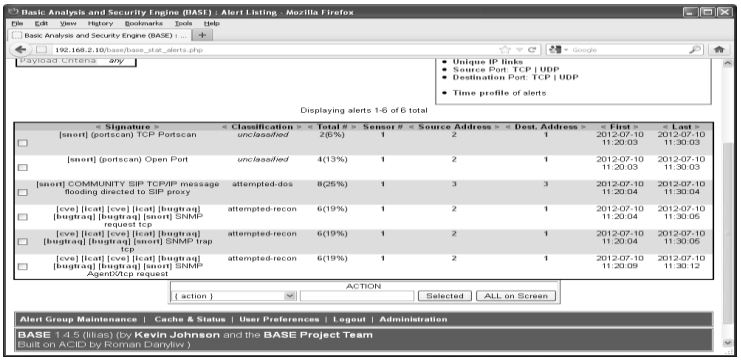
Gambar 2.2 Tampilan utama BASE dalam memproses *database* dari Snort

Dari gambar diatas terlihat bahwa terdapat 1 (satu) sensor yang bekerja dan*Traffic Profile by Protocol*yaitu TCP (69%), UDP (11%), ICMP (3%), PORTSCAN (17%) Serta menampilkan total jumlah dari sensor, u*nique alerts, categoties, total number of alerts, source IP address, destination IP address, Unique IP links, Source ports,* dan *destination ports.* Ancaman-ancaman] yang terdeteksi dari sensor diatas akan terus menenerus mengalami peningkatan sehinga bisa membuat sistem menjadi *crash* atau *hang* jika tidak diatasi.

A. Sensor Snort Pada Interface Eth0

Sensor Snort pada *interface eth0* dengan ip address 192.168.2.10 , dimana total kejadian *(Total Events)* yang terdeteksi oleh sensor *eth0* berjumlah 32 *events* dengan terklasifikasi 6 *unique events*, kemudian terdeteksi 3 sumber ip address dan 3 tujuan ip address serta *first* merupakan waktu pertama kali sensor mendeteksi serangan dan *last* merupakan waktu terakhir aktivitas sensor.

B. Tampilan *Unique Alerts*



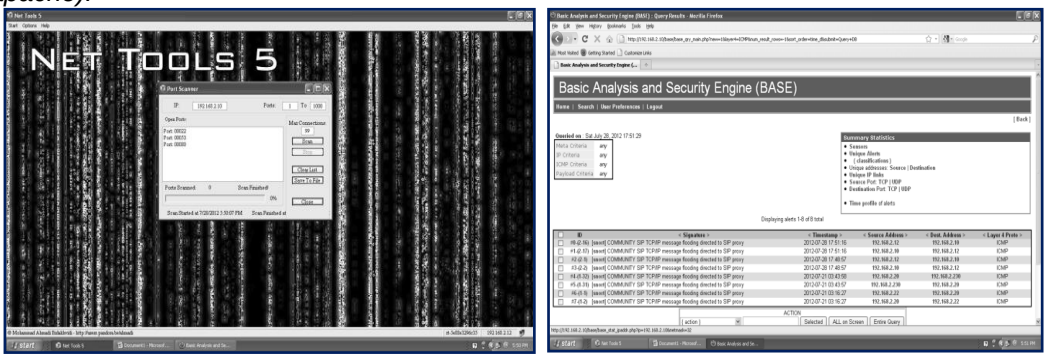
Gambar 2.3 *Unique alerts*

Dari gambar 2.3 diatas ini, merupakan halaman *Unique alerts* yang menampilkan tabel yang berisikan tentang intrusi-intrusi yang ditangkap oleh sensor *Snort*. Dalam table ini terdapat beberapa rincian yaitu *signature* (kejadian / polaserangan), *classification* (klasifikasi), total (total kejadian), sensor (menggunakan sensor ke berapa), *source address* (sumber alamat), *destination address* (tujuan alamat), *first* (waktu terjadi pertama kali), *last* (waktu terjadi terakhir kali).

2.5 Uji Coba Penyerangan Pada Jaringan Komputer BPBD Sumsel

A. Uji Coba Dengan Mengunakan Net Tools 5

Pengujian dilakukan dengan cara menggunakan software Net Tools 5 untuk men scanner port atau untuk melihat port port yang terbuka pada suatu jaringan. Bisa dilihat pada gambar 2.4 Net tools 5 mencoba mencari informasi pada ip *address* 192.168.2.10 dengan mencoba mens*can port-port* yang terbuka pada pc server dengan membuat range port 1 sampai dengan 1000 , kemudian klik *scan.* Dari hasil scanning tersebut peneliti mendapatkan *port* yang terbuka pada pada ip 192.168.2.10 yaitu *port* 22 dan *port* 80, *port* 22 merupakan *port protocol TCP* yang melayani *service remote ssh (secure shell)* dan *port* 80 merupakan *port protocol TCP* yang berfungsi mengelola *web server (apache).*

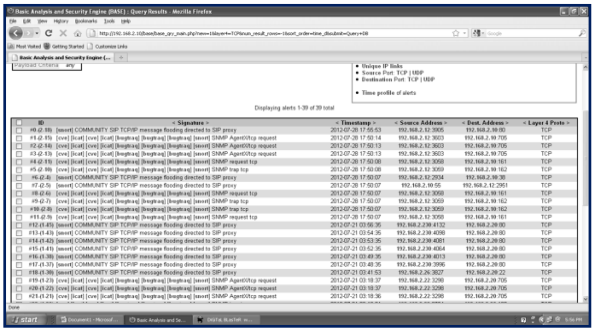


Gambar 2.4 Pengujian dengan Net Tools 5 Port scanner dan Deteksi ICMP

Informasi penyusupan yang teridentifikasi signature TCP Portscan, dimana IP *adrress* 192.168.2.13 dan 192.168.2.4 mencoba memperoleh informasi port yang terbuka pada server. Sensor Snort memberi informasi dimana port 22 dan port 80 pada IP *address* 192.168.2.10 sedang terbuka (*Open port*) sehingga ada celah bagi penyusup untuk mengeksplositasi port tersebut. Hal ini dilakukan tahapan sebelum melakukan penyerangan. Penyerangan dilakukan oleh penelti dengan mengirimkan paket data dengan kapasitas 64 *byte* dan melakukan proses ping sebanyak 1000 kali pada IP server yaitu 192.168.2.10, hal yang dinamakan *ping attack* dengan tujuan membuat sistem menjadi *crash* atau *hang*. P*ing attack* merupakan jenis serangan *DOS* yang dilancarkan melalui pengiriman paket-paket tertentu ,

B. Uji Coba Dengan Mengunakan Digital Blaster

Penyerangan ditujukan untuk membanjiri *protokol* TCP dan UDP. Penyusupan dilakukan dengan mengunakan komputer client yang mempunyai IP address 192.168.2.12. Penyerangan yang dilakukan ditujukan melalui port 80 dengan IP address server yaitu 192.168.2.10. dengan besar *Repeat* 100000, *Times Left* 99822 *Delay* 100. Yang memberikan ancaman *flooding* terhadap *protocol* TCP dan UDP. Sistem monitoring yang dilakukan oleh IDS base dengan sensor Snort berpungsi memeriksa semua data-data yang masuk dan melaporkan ke admin apabilah ada gerak gerik yang mencurigakan. Snort membedakan data-data yang masuk dengan melihat polah yang terdapat pada *Rules database* apabilah paket data sama dengan pola yang ada pada *Rules database*maka paket diangap sebagai serangan.

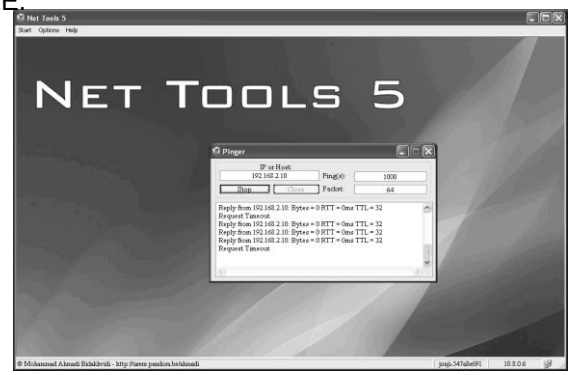


Gambar 2.5. Hasil Deteksi TCP

2.6. Teknik Pencegahan Pada Jaringan Komputer di BPBD Sumsel

A. IPTABLE Pemblokiran Paket ICMP

Dalam penelitian ini penulis mengaktifkan IPTABLES pada server di Badan Penanggulangan Bencana Daerah Sumsel dengan memblok *protocol* ICMP yang masuk ke interface eth0. Sehinga paket ICMP yang dikirim melalui port 80 akan secara otomatis di *riject* oleh IPTABLE.

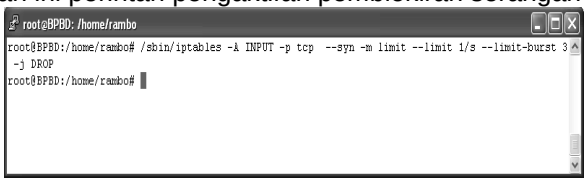


Gambar 2.6. Tampilan Net Tools 5 gagal mengirim paket ICMP

Gambar 2.6 Diatas adalah gambar aplikasi Net Tools 5 yang gagal melakukan pengiriman paket ICMP *flood* dikarenakan administrator sudah mengatasinya dengan cara memblokir paket ICMP yang akan masuk dengan cara mengaktifkan IPTABLE pemblogkiran paket ICMP pada server data .

B. Mengaktifkan Pemblokiran Serangan DOS

Mengaktifkan pemblokiran serangan dos yang membanjiri *Protocol* TCP dan UDP. Sehingga serangan dos akan dilakukan pemblokiran dari IPTABLES. Bisa dilihat pada gambar dibawah ini perintah pengaktifan pemblokiran serangan DOS.



Gambar 2.7 Pemblokiran serangan DOS

Hasil serangan *flooding* ke port 80 setelah di filter dengan *firewall* dimana serangan gagal. Dikarenakan sudah diterapkanya pencegahan pemblokiran pada protockol-protokol jaringan tersebut. Serangan *flooding* yang dilakukan dengan mengunakan aplikasi Digital Blaster dimana serangan mengalami kegagalan karena serangan sudah diblok mengunakan IPTABLE S pada server data.

Gambar 2.8 Serangan *flooding* Digital Blastrer yang gagal.

3. Kesimpulan

Berdasarkan dari penelitian yang telah dilakukan dengan mengimplementasikan *intrusion detektion system* (IDS) dengan mengunakan Base (*Basic Analysis And Security Engine*) dan sensor Snort pada server data Badan Penanggulangan Bencana Daerah Provinsi Sumatera Selatan (BPBD Sum-Sel) dan beberapa uji coba yang dilakukan, bisa diketahui bahwa ancaman ancaman terjadinya data *flooding* akan selalu membayangi jaringan tersebut, ini dikarenakan belum adanya suatu sistem yang handal yang di gunakan untuk mengantisipasi terjadinya data flooding.

Bisa dilihat dari beberapa uji coba yang dilakukan untuk membanjiri *traffic* data dengan mengunakan aplikasi *flood* yaitu Net Tool 5, Digital Blaster dan SynAttack, ketiga

aplikasi tersebut berhasil melakukan serangan terhadap server data. Dalam penelitian ini penulis mengaktifkan IPTABLES pada server data BPBD Sum-Sel sebagai langkah awal untuk mencegah serangan-serangan yang dilakukan untuk membanjiri *traffic* data.

DAFTAR PUSTAKA

Ariyus, D. (2006). *COMPUTER SECURITY*. Yogyakarta : Andi.

House,t. W. (2012). *Pengeritan Jaringan Komputer* (on-line). http://www.jaringankomputer.org/pengertian-jaringan-komputer/. Diakses pada 29 April 2012.

Lestari, Mirna, R. (2010). *Serangan Keamanan Jaringan* (on-line) http://mirnarizki37.blogspot.com/2012/02/serangan-keamanan-jaringan.html. Diakses pada tangal 27 april 2012.

Madya, S. (2009). *Teori Dan Prakik PENELITIAN TINDAKAN (ACTION RESEARCH).* Bandung : Alfabeta.

Pratama, J. A. (2010). *RANCANG BANGUN SISTEM PENCEGAHAN DATA FLOODING PADA JARINGAN KOMPUTER*. Surabaya : ITS.

Aji, S. (2008). *Jaringan Komputer.* Yogyakarta: Andi.

Thomas. (2005). *Network Security First-Step.* Yogyakarta: Andi.