**ANALISA KEAMANAN JARINGAN TERHADAP ANCAMAN DATA *FLOODING*  PADA BADAN PENANGGULANGAN BENCANA**

**DAERAH PROV. SUM-SEL**

**Rambo Paulan1, M.Izman Herdiansyah2 ,Rusmala Santi3**

**Mahasiswa Universitas Bina Darma 1, Dosen Universitas Bina Darma 2,**

**Dosen Universitas Bina Darma 3**

**Jalan Jenderal Ahmad Yani No.12 Palembang**

**Pos-el : indonesia\_rambopaulan@rocketmail.com1,m.herdiansyah@mail.binadarma.ac.id2,**

**rusmalsanti@mail.binadarma.co.id3**

***Abstract :*** *Tendency Internet usage is caused by the ease of communication and data transfer. But other than because many advantages these, Internet also has many weakness one of which so a constraint is in the area of security, because the Internet is a source of information can be accessible anywhere, anytime and by anyone. This is causing the internet became one of the infrastructure susceptible to the network security issues. Therefore companies or agencies offices should having a security system to safeguard the information and data on the Internet so cannot destroyed by parties who are not responsible. And able to prevent interference from outside which can cause flooding of data on computer networks connected to the Internet. At this exposure the author presents the analysis of network security about threats Flooding Data on Regional Disaster Management Agency of South Sumatra*

***Keywords:*** *data flooding, network.*

***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 perusahaamn atau intansi-intansi 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 paparan ini penulis menyajikan analisa keamanan jaringan terhadap ancaman Data Flooding pada Badan Penanggulangan Bencana Daerah Provinsi Sumatera Selatan.*

***Kata kunci :*** *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 : 2005) 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. Kasus pencurian atau manipulasi data perusahaan saja dapat mencapai kerugian sampai jutaan rupiah. Belum lagi kerusakan peralatan yang digunakan oleh perusahaan tersebut, yang bisa dibilang tidak murah.

Dalam faktor keamanan ini salah satu serangan yang sering muncul adalah data *flooding*. (Soki :2011) 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.

Instansi pemerintah Badan Penanggulangan Bencana Daerah Provinsi Sumatera Selatan yang melakukan aktifitas pertukaran informasi, laporan laporan bencana daerah ke Badan Nasional Penanggulangan Bencana Pusat menggunakan jaringan komputer, maka ancaman terhadap jaringan komputer akan selalu membayangi keamanan jaringan tersebut, terutama ancaman data *flooding* yang bisa terjadi kapan saja. Dalam skripsi ini penulis mencoba menganalisis keamanan jaringan terhadap ancaman terjadinya data *flooding* pada jaringan komputer pada Badan Penanggulangan Bencana Daerah Provinsi Sumatera Selatan.

1. **METODOLOGI PENELITAN**
   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 :

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

Teknik pengumpulan data dilakukan melalui wawancara dan observasi lapangan serta studi literature

1. **HASIL**
   1. **Implementasi *Intrusion Detektion System* (IDS)**

Adapun kebutuhan dalam implementasi *Intrusion Detektion System* (IDS) adalah sebagai berikut :

1. *U buntu 10.04 LTS Server.* serveryang dipakay di BPBD*.*
2. *Microsoft Windows XP*dan  *Windows 7 Desktop* sebagai *client.*
3. *Snort*
4. *flex. BASE (Basic Analysis and Security Engine)*
5. *MySQL*
6. *Adodb*
7. *Image\_Canvas 0.3.2*
8. *php5*
9. *apache*
10. *libpcap0.8-dev*
11. *bison*
12. *IP Tables Firewall*
    1. **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 3.1** 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).*

**3.2 Tampilan BASE dalam memproses *database* dari Snort.**

Gambar 5.2 merupakan tampilan utama BASE dalam memproses *database* dari *snort* dan memberikan informasi kepada admin.

**Gambar 5.2** Tampilan utama BASE dalam memproses *database* dari Snort

Dari gambar diatas terlihat bahwa terdapat 1 (satu) sensor yang bekerjadan*Traffic Profile by Protocol*yaitu TCP (69%), UDP (11%), ICMP (3%), PORTSCAN (17%) Serta menampilkan total jumlahdari 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.

* 1. **Sensor Snort Pada Interface Eth0**

**Gambar 5.3** Sensor snort pada interface eth0

Gambar 5.3 merupakan 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.

* 1. **Tampilan *Unique Alerts***

**Gambar 5.4** *Unique alerts*

Dari gambar 5.4 diatasini, 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).

* 1. **Tampilan *Catogories***

**Gambar 5.5** *Catogories*

Pada gambar 5.5 diatas ini adalah tampilan *categories* dari *unique alerts* pada halaman BASE. Pada gambar diatas menunjukkan pengkategorian dari *signature-signature* pada *unique alerts*, pada table tersebut terlihat bahwa ada bebera rincian yaitu *classification* (kategori tiap kejadian), total (jumlah total kejadian dalam satu kategori tersebut), sensor (menggunakan sensor ke-berapa), *signature* (jumlah kejadian dalam satu kategori), *source address* (alamat sumber dalam satu kategori), *destination address* (alamat tujuan dalam satu kategori), *first* (waktu terjadi pertamakali dalam satu kategori), *last* (waktu terjadi terakhir kali dalam satu kategori).

* 1. **Tampilan Total*Alerts***

**Gambar 5.6** Total *Alerts*

Gambar 5.6 diatas merupakan tabel total *alerts* berisikan catatanintrusi-intrusi atau serangan yang ditangkap oleh sensor *Snort. ID* merupakan no urutan kejadian, *signature* (polaserangan), *Time Stamp* (Waktu serangan) *source address* (alamat sumber), *destination address* (alamat tujuan), Layer 4 Proto (*Protocol* yang diserang).

**3.2 Uji Coba**

* 1. **Uji Coba Dengan Mengunakan Net Tools 5**

Port scanner digunakn oleh penyusup untuk melihat port port yang terbuka pada suatu jaringan. Bisa dilihat pada gambar 5.7.

**Gambar 5.7** Penyusupan Port scanner

Dari gambar 5.7 diatas Net tools 5 mencoba mencari informasi pada ip *address* 192.168.2.10 dengan mencoba men*scan* *port-port* yang terbuka pada pc server dengan membuat range port 1 sampai dengan 1000 , kemudian klik *scan* , sehingga kita dapat 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 5.8** Deteksi penyusupan

Dari gambar 5.8 diatas diperoleh 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.

**Gambar 5.9** Penyerangan *protocol* ICMP

Dari gambar 5.9 diatas, penyerangan dilakukan oleh penyusup 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*, *ping attack* merupakan jenis serangan *DOS* yang dilancarkan melalui pengiriman paket-paket tertentu , biasanya paket-paket sederhana dengan jumlah yang sangat banyak dengan maksud mengacaukan keadaan jaringan target. Sehinga memberikan ancaman *flooding* terhadap *protocol* ICMP.

**Gambar 5.10** Deteksi ICMP

ICMP adalah salah satu dari *protocol internet*. ICMP utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan yang menyatakan bahwa komputer tersebut dapat dijangkau atau tidak. Alert diatas merupakan alert ketika paket data dalam ukuran besar yang berasal dari IP *address* 192.168.2.4 keip address 192.168.2.12 dan bertujuan membanjiri IP *address* 192.168.2.10 sebagai tujuan berikutnya. Dianggap sebagai serangan oleh Snort karena pola serangan tersebut terdapat pada ruler Snort. Serangan tersebut dapat dikategorikan sebagai DOS yaitu serangan dengan mengunakan paket tertentu dengan jumlah yang sangat besar dengan maksud mengacaukan keadaan jaringan target dalam hal ini disebut *smurt attack* karena paket ICMP tersebut dikirim host lain dan bertujuan agar host tersebut mengirimkan paket ICMP ke korban berikutnya.Jika hal ini tidak diatasi oleh admin maka akan terjadi data *flooding* pada jaringan komputer tersebut.

1. **Uji Coba Dengan Mengunakan Digital Blaster**

Penyerangan ditujukan untuk membanjiri *protokol* TCP dan UDP. Penyusupan dilakukan dengan mengunakan komputer cline yang mempunyai IP address 192.168.2.12 Proses penyerangan bisa dilihat pada gambar 5.11.

**Gambar 5.11** Penyerangan *protocol* TCP dan UDP

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 grakgerik 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. Cara kerja monitoring dengan mendeteksi serangan yang dilakukan dengan mengunakan Digital Blaster bisa dilihat pada gambar 5.12 dan 5.13.

**Gambar 5.12** Deteksi TCP

Dari gambar diatas terlihat bahwa ada IP *address* 192.168.2.12 yang ingin membanjiri *sistem protocol* TCP melalui port 80 yang teridentifikasi oleh signature, serangan tersebut dapat dikategorikan sebagai DOS yang menyebapkan *protocol*  TCP menjadi *Flood* sehinga membuat sistem menjadi *crash* atau *hang*.

**Gambar 5.13** Deteksi UDP

Dari gambar 5.13 diatas terlihat bahwa ada IP *address* 192.168.2.12 yang ingin membanjiri system *protocol* UDP melalui port 80 yang teridentifikasi oleh signature, serangan tersebut dapat dikategorikan sebagai DOS yang membuat system menjadi *crash* atau *hang.*

1. **Uji Coba Dengan Mengunakan SynAttack**

**Gamanr 5.14** Penyerangan dengan mengunakan SynAttack.

*Synattack*  berfungsi untuk membanjiri sistem oleh penyusup dengan menyerang lubang keamanan dari implementasi protocol TCP/IP dengan tujuan membuat sistem menjadi *crash* atau *hang*. Adapun cara menjalankan aplikasi *Synattack* dengan memasukkan IP target dalam penelitian ini 192.168.2.10, setelah itu masukan *port* yang terbuka 22 80, alamat *port* yang terbuka didapat dari proses *port scanning.*

**Gambar 5.15** Deteksi TCP

* 1. **Teknik Pencegahan**

1. **IPTABLE Pemblokiran Paket ICMP**

Dalam penelitian ini penulis mengaktifkan IPTABLES pada server dengan memblok *protocol* ICMP yang masuk ke interface eth0. Sehinga paket ICMP yang dikirim melalui port 80 akan secara otomatis di *riject* oleh IPTABLE. Bisa dilihat pada gambar 5.16 printah mengaktifkan IPTABLE pemblokiran ICMP pada server.

**Gambar 5.16** Mengaktifkan IPTABLE Pemblogkiran Paket ICMP

Bisa dilihat pada gambar 5.17 hasil dari pemblokiran dengan mengaktifkan IPTABLE pemblokiran paket ICMP.

**Gambar5.17**Tampilan Net Tools 5 gagal mengirimpaket ICMP

Gambar 5.17 Diatas adalah gambar aplikasi Net Tools 5 yang gagal melakukan pengiriman paket ICMP *flood* dikarnakan administrator sudah mengatasinya dengan cara memblokir paket ICMP yang akan masuk dengan cara mengaktifkan IPTABLE pemblogkiran paket ICMP pada server data.

1. **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 5.18** Pemblokiran serangan DOS

Hasil konfigurasi pemblokiran bias dilihat pada gambar 5.19 dibawah ini:

**Gambar 5.19** Hasil konfigurasi IPTABLES pemblokiran serangan DOS

**Gambar 5.20** Mengaktifkan IPTABLES.conf

Hasil serangan *flooding* ke port 80 setelah di filter dengan *firewall* dimana serangan gagal. Dikarenakan sudah diterapkanya pencegahan penmblokiran atau aturanaturan pada protockol-protokol jaringan tersebut. Bisa dilihat pada gambar 5.21 dan gambar 5.22 :

**Gambar 5.21** Serangan *flooding* Digital Blastrer gagal.

Gambar 5.21 diatas adalah serangan *flooding* yang dilakukan dengan mengunakan aplikasi Digital Blaster dimana serangan mengalami kegagalan karena serangan sudah diblok mengunakan IPTABLE Spada server data.

**Gambar 5.22** Serangan *flooding* SynAttack gagal

Gambar 5.22 diatas adalah serangan *flooding* yang dilakukan dengan mengunakan aplikasi SynAttack dimana serangan mengalami kegagalan karena serangan sudah diblok menggunakan IPTABLES pada server data.

**3.4 Analisis**

Berdasarkan dari penelitian yang telah dilakukan dengan mengimplementasikan *intrusion detektion system* (IDS) dengan mengunakan Base (*Basic Analysis And Security Engine*) dansensor Snort pada server data Badan Penanggulangan Bencana Daerah Provinsi Sumatra Selatan (BPBD Sum-Sel) dan beberapa uji coba yang dilakukan, bisa diketahui bahua ancaman ancanan terjadinya data *flooding* akan slalu membayai jaringan tersebut dikarenakan belum adanya suatu sistem yang handal yang di gunakan untuk mengantisipasi hal tersebut. Bisa dilihat dari beberapa ujicoba yang dilakukan untuk membanjiri *traffic* data dengan mengunakan aplikasi *flood* yaitu Net Tool 5, Digital Blaster dan SynAttack, ketiga aplikasi tersebut berhasil melakukan serangan.

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.

1. **SIMPULAN**

Berdasarkan dari penelitian yang telah dilakukan, diketahui bahwa di Badan Penanggulangan Bencana Daerah Provinsi Sumatra Selatan (BPBD) belum diimplementasikan perlindungan terhadap ancaman terjadinya data *flooding.* Hasil uji coba implementasi *Intrusion Detektion System* (IDS) monitoring Base dengan menggunakan sensor Snort menunjukan bahua beberapa serangan yang menyebapkan *flooding*  terdeteksi. Dan implementasi IPTABLES dapat menghambat terjadinya data *flooding.*

**DAFTAR RUJUKAN**

Agussaputra, A.S. (2012). *INFLEMENTASI SISTEM PENCEGAHAN DATA FLOODING PADA JARINGAN KOMPUTER.* Palembang : Skripsi Univ. Bina Darma.

Anonim. *Keamanan Jaringan (on-line).* <http://www.aafonix.student.umm.ac.id/files/2010/07/JARINGAN-KOMPUTER.doc> . Diakses pada 2 Mei 2012.

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.

Nasution, R. (2006). *SISTEM PENCEGAHAN FLOODING DATA*

*PADA JARINGAN KOMPUTER.* Bandung : Skripsi Unikom.

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

Sulaini, I. (2008). *PENGENALAN INTERNET.* Palembang : Univ. Bina Darma.

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

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

Utomo. (2011). *Membangun Jaringan Komputer dan Internet.* Yogyakarta: Mediakom.