INFOTECH journal
ISSN : 2460-1861 (Print), 2615-4250 (Online)
Vol (10) No (1) 2024, pp. 1-11

PERANCANGAN DE-MILITARIZED ZONE (DMZ) AREA BERBASIS INTRUSION DETECTION SYSTEM (IDS) PADA INFRASTRUKTUR JARINGAN KOMPUTER

Dadan Rahmat, M.T[1], Irman Suherman, M.T[2], Zahara Muharraran[3], Aulia Khotimah Husna[4]
[1]Pendidikan Teknologi Informasi, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Muhammadiyah Sukabumi

ABSTRACT
De-Militarized Zone (DMZ) is a mechanism to protect the internal system from attacks by hackers or other parties who want to enter the system without access rights. The internal system is a confidential information system, the DMZ consists of all open ports that can be seen by outside parties so that hackers attack to crack the server that has the DMZ, so the hacker can only access hosts located in the DMZ. This is done so that internet users who can access the server cannot easily access and reach users on the local network. Within a network, hosts are most vulnerable to attacks that provide services to users outside. As computer networks develop in the Sukabumi City Regional Government, implementing a computer network security system model should be the main focus considering that there are many public services with high security risks and also the absence of a security system that can minimize data or application security risks on computer networks.

Keywords: De-Militarized Zone (DMZ), hackers attack, computer network, security, system.

ABSTRAK

De-Militarised Zone (DMZ) merupakan mekanisme untuk melindungi sistem internal dari serangan hacker atau pihak-pihak lain yang ingin memasuki sistem tanpa hak akses. Sistem internal yaitu sistem informasi yang bersifat rahasia, DMZ terdiri dari semua port yang terbuka yang dapat dilihat oleh pihak luar sehingga hacker menyerang untuk melakukan cracking pada server yang mempunyai DMZ maka hacker tersebut hanya dapat mengakses host yang berada pada DMZ. Hal ini dilakukan agar user dari internet yang dapat mengakses server tidak dapat dengan mudah mengakses dan mengacaukan user pada jaringan lokal. Dalam sebuah jaringan, maka host paling rentan terhadap serangan yang memberikan layanan kepada pengguna diluar. Seiring berkembangnya jaringan komputer pada Pemerintah Daerah Kota Sukabumi, penerapan model sistem keamanan jaringan komputer sudah seharusnya menjadi fokus utama dikarenakan banyaknya layanan yang bersifat publik dengan resiko keamanan yang tinggi dan juga tidak adanya sistem keamanan yang dapat meminimalisasikan resiko keamanan data ataupun aplikasi di jaringan komputer.

Kata Kunci: De-Militarised Zone (DMZ), serangan hacker, jaringan komputer, keamanan, sistem.

Riwayat Artikel :
Tanggal diterima : 05-12-2023
Tanggal revisi : 21-12-2023
Tanggal terbit : 18-01-2024

1. PENDAHULUAN

1.1. Latar Belakang

Hadirnya *firewall* telah banyak membantu dalam pengamanan, akan tetapi seiring berkembang teknologi sekarang ini hanya dengan firewall keamanan tersebut belum dapat dijamin sepenuhnya. Banyaknya akses dari jaringan publik membuat jaringan semakin rentan terhadap serangan. Layanan yang sering melayani user dari internet diantaranya adalah DNS server, web server, dan mail server.

Untuk mengamankan jaringan yang ada dalam perusahaan, jaringan lokal juga harus dipisahkan dengan jaringan server. Hal ini dilakukan agar user dari internet yang dapat mengakses server tidak dapat dengan mudah mengakses dan mengacaukan user pada jaringan lokal. Serangan yang sering terjadi terhadap layanan yang berbasis internet adalah Denial of Service. Denial of Service merupakan jenis serangan yang melakukan flooding terhadap jaringan server. Serangan ini bertujuan untuk melumpuhkan server agar tidak dapat melayani pengguna yang ingin mengakses server.

Dalam jaringan komputer telah dikenal sebuah sistem firewall, yaitu alat yang berfungsi sebagai sistem yang menjaga keamanan jaringan dan semua perangkat yang ada di dalamnya. Dengan berbagai fasilitas yang dimiliki, firewall dapat memberikan policy yang sesuai dengan kebutuhan jaringan. Untuk pengamanan, biasanya firewall disandingkan dengan Intrusion Detection System atau yang biasa disingkat IDS. Intrusion Detection System merupakan aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS juga dapat memberikan peringatan dini kepada administrator jaringan jika sedang terjadi serangan.

Jaringan komputer pada Kantor Pemerintah Daerah Kota Sukabumi pada awalnya adalah jaringan yang menghubungkan beberapa perangkat komputer di lingkungan Kota Sukabumi. Namun seiring perkembangan dan berjalannya waktu, saat ini Pemerintah Daerah Kota Sukabumi menjadi jaringan utama yang menghubungkan beberapa instansi atau Satuan Kerja Perangkat Daerah Kota Sukabumi.

Dari permasalahan yang ada pada latar belakang diatas, serta metode evaluasi keamanan jaringan komputer yang akan diterapkan pada penelitian ini, maka penulis akan merumuskan penelitian dengan judul "Perancangan De-Militarised Zone Berbasis Intrusion Detection System Pada InfraStruktur Jaringan Komputer Pemerintah Daerah Kota Sukabumi".

1.2. Tinjuan Pustaka

Perancangan adalah penggambaran, perencanaan dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah ke dalam satu kesatuan yang utuh dan berfungsi Perancangan sistem dapat dirancang dalam bentuk bagan alir system, yang merupakan alat bentuk grafik yang dapat digunakan untuk menunjukan urutan-urutan proses dari sistem (Syifaun Nafisah,2003:2).

Keamanan jaringan secara umum adalah komputer yang terhubung ke network, mempunyai ancaman keamanan lebih besar daripada komputer yang tidak terhubung kemana-mana. Dengan pengendalian yang teliti, resiko tersebut dapat dikurangi. (Ariyus,2007:3).

Menurut Ariyus (2007:12). Jenis dan serangan yang mengganggu jaringan komputer beraneka macam. Serangan-serangan yang terjadi pada sistem komputer di antaranya adalah:

2.3 Tujuan Keamanan Komputer

IDS menjadi solusi untuk mengatasi masalah tersebut(Ariyus,2007:25).

Pada dasarnya tujuan keamanan komputer yang disingkat dengan CIA, yang merupakan singkatan dari:

1. *Confidentiality*:Merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses.
2. *Integrity*:Keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak.
3. *Availability*:Aspek ini berhubungan dengan ketersediaan informasi ketika dibutuhkan.(Sukmaaji & Rianto, 2008: 159)

2.4 Definisi Firewall

Firewall adalah suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software, ataupun sistem dengan tujuan untuk melindungi, Perlindungan dapat dilakukan dengan menyaring, membatasi, atau bahkan menolak suatu atau semua hubungan/kegiatan dari suatu segmen pada jaringan pribadi dengan jaringan luar.

2.4.1 Karakteristik Firewall

Karakteristik dari sebuah firewall adalah sebagai berikut:

1. Seluruh hubungan/kegiatan dari dalam ke luar harus melewati firewall.
2. Hanya kegiatan yang terdaftar/dikenal yang dapat melewati atau melakukan hubungan.
3. Firewall harus tebal atau relative terhadap serangan.

2.4.2 Teknik Pengamanan Firewall

Empat teknik umum yang firewall gunakan untuk control akses dan melaksanakan security policy. (Sukmaaji & Rianto, 2008: 189):

1. *Service Control*:Berdasarkan tipe-tipe service yang digunakan dan boleh diakses baik untuk kedalam ataupun keluar firewall.
2. *Direction Control*:Berdasarkan arah dari berbagai permintaan terhadap layanan yang akan di kendali dan diizinkan melewati firewall.
3. *User Control*: Berdasarkan pengguna/user untuk dapat menjalankan suatu layanan, artinya ada user yang dapat dan ada yang tidak dapat menjalankan suatu servis.
4. *Behavior Control*:Berdasarkan seberapa banyak layanan itu telah digunakan.

2.4.3 Jenis-jenis Firewall

Firewall terbagi menjadi tiga jenis (Sukamaji&Rianto,2008:189), yakni sebagai berikut:

1. *Packet-Filtering Router*: Sebuah packet-filtering router menerapkan aturan ke setiap paket IP yang masuk atau datang dan kemudian di forward atau dibuang paket tersebut.
2. *Application-Level Gateway*:Application-level gateway juga disebut sebuah proxy server, yang bertindak sebagai meletakkan dari application-level gateway yang menggunakan aplikasi TCP/IP.
3. *Circuit-level Gateway*:Ketiga dari jenis firewall adalah circuit-level gateway. Circuit-level gateway sistem yang dapat berdiri sendiri atau bisa merupakan suatu fungsi yang melakukan dengan application-level gateway untuk aplikasi.

2.4.4 Konfigurasi Firewall

Konfigurasi firewall(Sukmaaji&Rianto, 2008:192) adalah sebagai berikut:

1. *Screened Host Firewall System*.Pada konfigurasi ini, fungsi firewall akan dilakukan oleh paket *filtering router* dan *bastion host router.*
2. *Screened Host Firewall System*.Pada konfigurasi ini, secara fisik akan terdapat patah /celah dalam jaringan.
3. *Screened subnet firewall* Merupakan konfigurasi yang paling tinggi tingkat keamanannya. Setelah mempelajari konsep teknik dan beberapa tipe-tipe firewall untuk dapat membangun sistem firewall perlu memperhatikan tahapan sebagai berikut:
   a. Mengidentifikasi bentuk jaringan yang dimiliki.
   b. Menentukan policy atau kebijakan.
   c. Menyiapkan software atau hardware yang akan digunakan.
   d. Melakukan tes konfigurasi.

2.6 DMZ (De-Militarised Zone)

Tujuan dari DMZ adalah menambahkan lapisan tambahan keamanan untuk sebuah organisasi LAN; eksternal hanya penyerang yang memiliki akses ke peralatan di DMZ, daripada seluruh jaringan. (http://ecgalery.blogspot.co.id/2011/01/dmz-de-militarised-zone.html)

2.6.1 Dasar Pemikiran

Dalam sebuah jaringan, maka host paling rentan terhadap serangan adalah mereka yang memberikan layanan kepada pengguna di luar LAN, seperti e-mail, web dan DNS server. Karena peningkatan potensi host ini terganggu, mereka ditempatkan dalam Sub-jaringan mereka sendiri untuk melindungi sisa jaringan jika seorang penyusup adalah untuk berhasil. (http://ecgalery.blogspot.co.id/2011/01/dmz-de-militarised-zone.html)

2.6.2 Layanan yang termasuk dalam DMZ

Yang paling umum dari layanan ini adalah *web server, mail server, ftp server, VoIP server dan DNS server*. (http://ecgalery.blogspot.co.id/2011/01/dmz-de-militarised-zone.html)

2.6.3 Web server

Web server mungkin perlu untuk berkomunikasi dengan database internal untuk menyediakan beberapa layanan khusus. Karena server database tidak dapat diakses publik dan mungkin berisi informasi sensitif, itu tidak boleh di DMZ. Sebuah *server* aplikasi dapat digunakan untuk bertindak sebagai media komunikasi antara *web server dan database server*. (http://ecgalery.blogspot.co.id/2011/01/dmz-de-militarised-zone.html)

2.6.4 E-mail server

Mail server di DMZ harus masuk melalui mail ke diamankan / internal server mail dan server surat ini harus lewat surat keluar ke server mail eksternal.
(http://ecgalery.blogspot.co.id/2011/01/dmz-de-militarised-zone.html)

2.5.5 Proxy server

Untuk keamanan, penegakan hukum dan juga alasan pemantauan, dalam lingkungan bisnis, juga dianjurkan untuk menginstal sebuah *proxy server* dalam DMZ. Ini memiliki keuntungan sebagai berikut:

1. Mewajibkan pengguna internal untuk menggunakan proxy khusus ini untuk mendapatkan akses internet.
2. Memungkinkan administrator sistem untuk merekam dan memantau aktivitas pengguna dan pastikan tidak ada konten ilegal di-download atau di-upload oleh para karyawan. (http://ecgalery.blogspot.co.id/2011/01/dmz-de-militarised-zone.html)

2.6.6 Reverse proxy server

Sebuah *reverse proxy* server yang menyediakan layanan yang sama sebagai server proxy, tetapi sebaliknya. Alih-alih memberikan layanan kepada pengguna internal, tidak langsung memberikan akses ke sumber daya internal dari jaringan eksternal (biasanya Internet). (http://ecgalery.blogspot.co.id/2011/01/dmz-de-militarised-zone.html)

2.6.7 Arsitektur

Ada berbagai cara untuk merancang sebuah jaringan dengan DMZ. Dua metode yang paling dasar adalah dengan satu firewall, juga dikenal sebagai model berkaki tiga, dan dengan firewall ganda.
(http://ecgalery.blogspot.co.id/2011/01/dmz-de-militarised-zone.html)

2.6.8 Single Firewall

Sebuah firewall dengan minimal 3 antarmuka jaringan dapat digunakan untuk menciptakan sebuah arsitektur jaringan yang berisi DMZ. Jaringan eksternal terbentuk dari ISP ke firewall pada antarmuka jaringan pertama, jaringan internal yang terbentuk dari kedua antarmuka jaringan, dan DMZ terbentuk dari antarmuka jaringan ketiga. (http://ecgalery.blogspot.co.id/2011/01/dmz-de-militarised-zone.html)

2.6.9 Dual Firewall

Beberapa merekomendasikan bahwa dua firewall disediakan oleh dua vendor yang berbeda. Jika penyerang berhasil menerobos firewall pertama, akan diperlukan lebih banyak waktu untuk menerobos yang kedua jika dibuat oleh vendor yang berbeda.
(http://ecgalery.blogspot.co.id/2011/01/dmz-de-militarised-zone.html)

2.6.10 DMZ host

Beberapa rumah router merujuk pada DMZ host. Sebuah rumah router DMZ host adalah host di jaringan internal yang memiliki semua port terbuka, kecuali yang port diteruskan sebaliknya. Dengan definisi ini bukan benar DMZ,karena ia sendiri tidak terpisah host dari jaringan internal. (http://ecgalery.blogspot.co.id/2011/01/dmz-de-militarised-zone.html)

2.7 IDS

2.7.1 Definisi dan Konsep IDS

Menurut Ariyus(2007:27) Intrusion Detection System dapat didefinisikan sebagai tool. Metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan komputer.

2.7.2. Jenis IDS.

Jenis Intrusion Detection System ada 2(Junior, 2009: 5) adalah sebagai berikut:

2.7.2.1 NIDS

NIDS akan melakukan pemantauan terhadap seluruh bagian pada jaringan dengan mengumpulkan paket-paket data yang terdapat pada jaringan tersebut serta melakukan analisa dan menentukan apakah paket-paket tersebut merupakan paket normal atau paket serangan.

2.7.2.2 HIDS

HIDS hanya melakukan pemantauan pada perangkat komputer tertentu dalam jaringan.

2.7.3 Keuntungan dan Kerugian IDS

Keuntungan dan kekurangan dari IDS adalah:

a. Keuntungan dari IDS:

1.Dapat disesuaikan dengan mudah dalam menyediakan perlindungan untuk keseluruhan jaringan.
2.Dapat dikelola secara terpusat dalam menangani serangan yang tersebar dan bersama-sama.
3.Menyediakan penahanan pada bagian dalam.
4.IDS memonitor Internet untuk mendeteksi serangan.
5.IDS melacak aktivitas pengguna dari saat masuk hingga saat keluar.

b. Kekurangan dari IDS

a. Lebih bereaksi pada serangan daripada mencegahnya.
b. Menghasilkan data yang besar untuk dianalisis.
c. IDS hanya melindungi dari karakteristik yang dikenal.
d.IDS tidak turut bagian dalam kebijakan keamanan yang efektif, karena dia harus diset terlebih dahulu.
e.IDS tidak mengidentifikasikan asal serangan

2.7.4 Peran IDS

IDS juga memiliki peran penting untuk mendapatkan arsitektur *defence-in-depth*. Hal-hal yang dilakukan IDS pada jaringan internal adalah sebagai berikut:

1.Memonitor akses database:ketika mempetimbangkan pemiliihan kandidat untuk

penyimpan data suatu perusahaan.
2.Melindungi e-mail server:IDS juga berfungsi untuk mendeteksi virus e-mail.
3.Memonitor policy security:jika ada pelanggan terhadap policy security maka IDS akan memberitahu.(Ariyus,2007:34)

2.8 Perangkat Lunak dan Perangkat Keras

2.8.1 Perangkat Keras

2.8.1.1 Server

Menurut O'brien(2011:190) lebih spesifik menyatakan bahwa, "Server adalah computer yang mendukung aplikasi dan telekomunikasi dalam jaringan, serta pembagian peralatan software, dan database di antara berbagai terminal kerja dalam jaringan.

2.8.1.2 NIC

Oleh: Dini S.Kom(2015) NIC merupakan sebuah perangkat keras jaringan, yang secara fisik berbentuk seperti sebuah kartu ekspansi, yang memungkinkan setiap komputer dapat terhubung dengan suatu jaringan dengan menggunakan kabel jaringan.

2.8.1.3 Hub

Alat penghubung antar komputer, semua jenis komunikasi hanya dilewatkan oleh hub, hub digunakan untuk sebuah bentuk jaringan yang sederhana. (Sukmaaji & Rianto, 2008:42).

2.8.1.4 Router

Menurut O'brien(2011:193), "Router adalah sebuah alat jaringankomputer yang mengirimkan paket data melalui sebuah jaringan atau internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing."

2.8.2 Perangkat Lunak

2.8.2.1 pfSense

pfSense adalah opensource firewall/router distribusi perangkat lunak komputer berdasarkan
FreeBSD. Hal ini diinstal pada komputer fisik atau mesin virtual untuk membuat firewall khusus/router untuk jaringan dan dicatat untuk keandalan dan korban fitur sering hanya ditemukan di firewall komersial mahal.
(https://en.wikipedia.org/wiki/PfSense).

2.8.2.2 IPTables

IPTables adalah firewall yang secara default diinstal pada semua distribusi linux, seperti *Ubuntu, Kubuntu, Xubuntu, Fedora Core*, dan lainnya. Pada saat melakukan instalasi pada ubuntu, iptables sudah langsung ter-install, tetapi pada umumnya iptables mengizinkan semua traffic untuk lewat(Purbo, 008:188).

2.8.2.3 Apache

Menurut Arief(2011e:151) adalah "salah satu jenis database server yang sangat terkenal dan banyak digunakan untuk membangun aplikasi web yang menggunakan database sebagai sumber dan pengelolaan datanya". Mysql bersifat *open source* dan menggunakan SQL. MySQL biasa dijalankan diberbagai *platform* misalnya windows Linux, dan lain sebagainya.

2.8.2.4 MySQL Server

MySQL merupakan DBMS yang *multithread*, multi *user* yang bersifat gratis dibawah lisensi GNU *General Public Licence*. MySQL bersifat gratis atau *open source* sehingga kita bisa menggunakannya secara gratis.

2.8.2.5 PHP Server

Menurut Nugroho (2006b:61) "PHP atau singkatan dari Personal Home Page merupakan bahasa skrip yang tertanam dalam HTML untuk dieksekusi bersifat server side". PHP termasuk dalam opensource product, sehingga source code PHP dapat diubah dan didistribusikan secara bebas.

2.8.2.6 NS Server

Menurut Tech Terms oleh Jeff Rutenbeck Domain name adalah sebuah sistem penamaan yang mengidentifikasi setiap server jaringan unik di internet. Adanya domain name membuat penamaan alamat internet protokol menjadi mudah dan gampang diingat.

2.8.2.7 Active Directory

Active Directory adalah layanan direktori termasuk dalam keluarga Windows Server. Active Directory meliputi direktori, yang menyimpan informasi tentang sumber daya jaringan, serta semua layanan yang membuat informasi yang tersedia dan berguna.(Spealman, J.,andKurt Hudson, 2004:5)

2.8.2.8 Local My SQL

Menurut Anhar(2010:45)"MySQL adalah salah satu DMS dari
sekian banyak DBMS seperti Oracle, MS SQL, Postagre SQL, dan lainya". MySQL bersifat open source sehingga kita bisa menggunakannya secara gratis.

2.8.2.9 FreeNAS

Menurut Gary Sims (2008) FreeNAS adalah sebuah perangkat lunak yang mampu menjadikan komputer standalone menjadi sebuah server NAS. FreeNAS mendukung koneksi dari sistem operasi yang banyak digunakan saat ini seperti Microsoft Windows, Apple OS X, Linux And FreeBSD.

2.8.2.11 Snort

2.8.2.11.1 Definisi dan Konsep Snort

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisis paket yang melintasi jaringan secara real time traffic dan logging ke dalam database serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan(Ariyus,2007:45)

Snort bisa dioperasikan dengan tiga mode(Ariyus, 2007:146) yaitu:

a. Paket *Sniffer*:Untuk melihat paket yang lewat di jaringan.

b. Paket *logger*:Untuk mencatat semua paket yang lewat di jaringan untuk dianalisis di kemudian hari

c.NIDS deteksi penyusup pada network:Pada mode ini soon akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer.

2.8.2.11.2 Komponen-komponen Snort

Menurut Slameto(2007:7) komponen-komponen snort meliputi:

1.Rule Snort.

Merupakan database yang berisi pola-pola serangan berupa signature jenis-jenis serangan.

2.Snort Engine.

Merupakan program yang berjalan sebagai proses yang selalubekerja untuk membaca paket data dan kemudian membandingkannya dengan rule Snort.

3.Alert.

Merupakan catatan serangan pada deteksi penyusupan. Jika snort engine menghukumi paket data yang lewat sebagai serangan, maka snort engine akan mengirimkan alert berupa log file.

2.8.2.11.3 Fitur-fitur Snort

Menurut Wardhani (2007) fitur-fitur snort adalah sebagai berikut:

1.Karena Snort bersifat *opensource*, muka penggunaannya betul-betul gratis, Oleh karena itu, Snort merupakan pilihan yang sangat baik sebagai NIDS ringan yang cost-effective dalam suatu organisasi yang kecil.

2.Karena Snort bersifat opensource, maka penggunaannya betul-betul bebas.

3.Snort memiliki bahasa pembuatan rules yang relatif mudah dipelajari dan fleksibel.

4.Snort sudah memiliki sebuah database untuk berbagai macam rules yang terus dikembangkan oleh komunitas

5.Snort merupakan software yang ringkas dan padat tetapi cukup canggih dan fleksibel untuk digunakan sebagai salahsatu bagian dari NIDS yang terpadu.

6.Snort dapat melakukan logging langsung ke sistem database.

7.Snort sebagai NIDS dapat menyembunyikan dirinya dalam jaringan computer.

2.8.2.11.4 Penempatan Instrusion Detection System

Intrusion Detection System pada suatu jaringan, apakah akan dapat bekerja dengan baik, tergantung pada peletakannya. Secara prinsip pemahaman penempatan komponen *intrusion detection system* akan menghasilkan IDS yang benar-benar mudah untuk dikontrol. (Ariyus, 2007: 177).

2.8.2.11.5 Penempatan Sensor

Sensor network untuk intrusion detection system biasanya terinstall pada lokasi berikut (Ariyus,2007: 177):

1.Antara Router dan Firewall

2.Sensor Network pada Demilitarized Zone

3.Sensor Network Behind Firewall

2.8.2.11.6 Sensor Network pada Backbone

Network intrusion detection systems bisa menjadi tidak efektif pada kebanyakan backbone pada jaringan yang memiliki prinsip beda. ATM frame relay, X25 dan sebagainya, karena teknologi modem yang membangun WAN, yang meliputi backbone yang tidak mempunyai relasi jaringan untuk multiple acces dan komunikasi (Ariyus, 2007: 181).

2.8.2.11.7 Intrusion Detection System mengenal adanya penyusup

Menurut Thomas (2004, 373) dilihat dari cara kerja dan menganalisa apakah paket data dianggap sebagai penyusupan atau bukan IDS.

2.8.2.11.8 ACID

ACID merupakan PHP based analysis engine yang berfungsi untuk mencari dan mengolah database dari alert network sekuriti yang dibangkitkan oleh perangkat lunak pendeteksi intrusi.(Ariyus,2007:214).

2.8.2.11.9 Ntop

Ntop merupakan aplikasi yang dapat digunakan untuk melakukan monitor jaringan via web. Ntop adalah salahsatu Tools untuk memonitoring jaringan(Paulo&Albertino,2000:2)

2.8.2.11.10 Digital Blaster

Digital Blaster adalah sebuah Flooder internet dan jaringan komputer yang bisa disingkat menjadi DigiBlast yang merupakan *hack tool* gratis dan bebas untuk disebarluaskan dengan syarat tidak untuk konsumsi profit seperti menjual atau membelinya dari seseorang.(Setiawan,2004:21).

2.8.2.11.11 Nmap

Nmap adalah sebuah program *opensource* yang berguna untuk mengeksplorasi jaringan. Nmap didesain untuk dapat melakukan scan jaringan yang besar, juga dapat digunakan untuk melakukan scan host tunggal.(Setiawan.2004:2).

2.8.2.11.12 Ping Attack

Ping of Death merupakan suatu serangan DoS terhadap suatu server atau komputer yang terhubung dalam suatu jaringan(Sukmaaji&Rianto, 2008:165).

Serangan ini memanfaatkan fitur yang ada di TCPnP yaitu paket fragmentation atau pemecahan paket, dan juga kenyataan bahwa batas ukuran paket di protokol IP adalah 65536byte atau 64 kilobyte.(Sukmaaji & Rianto,1008:165).

2.8.2.11.13 Program Pendeteksi IDS

Menurut Thomas(2004:386) selain snort program pendeteksi serangan masih banyak tetapi kelebihan snort dari program ini adalah snont open source, di antara program itu adalah:

1. RealSecure dari Internet Security Systems.
2. Cisco Secure Intrusion Detection System dari Cisco Systems.
3. eTrust Intrusion Detection dari Computer Associates
4. Symantec Client Security dari Symantec
5. Computer Misuse Detection System dari ODS Networks
6. Kane Security Monitor dari Security Dynamics
7. Cybersafe
8. Network Associates
9. Network Flight Recorder
10. Intellitactics

2.10.1 Pengertian Metodologi Penelitian

Menurut (Sugiyono,2009:2) metode penelitian pada dasarnya merupakan cara ilmiah untuk mendapatkan data dengan tujuan dan guna tertentu, Kegiatan penelitian atau cara ilmiah didasarkan pada ciri-ciri ilmuan, yaitu rasional, empiris, dan sistematis.

2.10.2 Metodologi Pengumpulan Data

Pengumpulan data tidak lain dari suatu proses pengadaan data primer untuk keperluan penelitian dimana pengumpulan data adalah prosedur yang sistematis dan standar untuk memperoleh data yang diperlukan. Pengumpulan data penelitian dapat dilakukan dengan beberapa cara pengumpulan(Sugiyono,2009:137).

1. Studi Pustaka
2. Studi Lapangan
   a. Pengamatan Langsung
   b. Wawancara
3. Studi Literatur

2.10.3 Metode Pengembangan Sistem

Security Policy Development Life Cycle adalah suatu pendekatan proses dalam komunikasi data yang menggambarkan siklus yang tinda awal dan akhirnya dalam membangun sebuah jaringan komputer mencangkup lima tahap yaitu Analysis, Design, Implementation, Enforcement, dan Enhancement(WahshehdanJim2008:1121).

Metodologi Penelitian

Jenis penelitian yang akan digunakan dalam penelitian ini adalah dalam rangka pemecahan suatu masalah, masalah tersebut dapat diketahui dengan mencari informasi yang lebih efisien dan dapat dipercaya kebenarannya, untuk memperoleh data tersebut dilakukan dengan cara melakukan evaluasi dengan terus menerus sampai ditemukan metode yang paling efisien untuk dilaksanakan penelitian.

Berikut tahapan penelitian Tindakan yang dapat ditempuh

a. Melakukan Diagnosa

Melakukan identifikasi masalah-masalah pokok yang berguna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan.

b. Membuat rencana tindakan

Penulis memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada.

c. Melakukan tindakan

Penulis mengimplementasikan rencana tindakan dengan harapan dapat menyelesaikan masalah.

d. Pembelajaran

Tahap ini merupakan bagian akhir siklus yang telah dilalui dengan melaksanakan review tahapan-tahapan yang telah berakhir kemudian penelitian ini berakhir.

PEMBAHASAN

Kota Sukabumi berasal dari bahasa Sunda, yaitu *Suka-bumen* menurut keterangan mengingat udaranya yang sejuk dan nyaman, mereka yang datang ke daerah ini tidak ingin pindah lagi, karena suka atau senang bumen-bumen atau bertempat tinggal di daerah ini.

Sejak ditetapkannya Sukabumi menjadi Daerah Otonom pada bulan Mei 1926, maka resmi diangkat "Burgemeester" yaitu: Mr. GF.Rambonnet. Pada masa inilah dibangun sarana dan prasarana penting seperti Stasiun Kereta Api, Mesjid Agung, Gereja dan Pembangkit Listrik.

Kota Sukabumi terletak pada bagian selatan tengah Jawa barat pada koordinat 106º 45’ 50’’ Bujur Timur dan 106º 45’ 10’’ Bujur Timur, 6º 49’ 29’’ Lintang Selatan dan 6º 50’ 44’’ Lintang Selatan, terletak di kaki Gunung Gede dan Gunung Pangrango yang ketinggiannya 584 m diatas permukaan laut, dengan suhu maksimum 29 ºC yang berjarak 120 Km dari Ibukota Negara (Jakarta) dan 96 Km dari Ibukota Provinsi (Bandung) dengan luas wilayah 4.800,231 Ha. Memiliki penduduk sampai akhir Tahun 2002 tercatat 269.142 jiwa, dengan kepadatan penduduk rata-rata 50 jiwa/KM^2 yang tersebar.

Wilayah Kota Sukabumi seluruhnya berbatasan dengan wilayah Kabupaten Sukabumi yakni: di Sebelah Utara berbatasan dengan Kecamatan Cisaat dan Kecamatan Sukabumi Kabupaten Sukabumi,

Sebelah Selatan dengan Kecamatan Nyalindung Kabupaten Sukabumi, Sebelah Barat dengan Kecamatan Cisaat Kabupaten Sukabumi, Sebelah Timur dengan Kecamatan Sukaraja Kabupaten Sukabumi.

Ketentuan Umum

Keamanan jaringan secara umum adalah komputer yang terhubung ke network, mempunyai ancaman keamanan lebih besar daripada komputer yang tidak terhubung kemana-mana. Jenis dan serangan yang mengganggu jaringan komputer beraneka macam.

Port Scanning:merupakan suatu proses untuk mencari dan membuka port pada suatu jaringan komputer. Dari hasil scanning akan didapat letak kelemahan sistem tersebut. Pada dasamya sistem port scanning mudah untuk dideteksi, tetapi penyerang akan menggunakan berbagai metode untuk menyembunyikan serangan. Penyerang akan mengirimkan paket lain pada port yang masih belum ada pada jaringan tersebut tetapi tidak terjadi merespons apapun pada file log, kesalahan file atau device lainnya. Berbagai kemungkinan yang kadang disebut dengan Christmas tree dan null yang akan memberikan efek kepada jaringan TCP/IP sehingga protokol TCP/IP akan mengalami down banyak tool yang ada yang bisa membuat suatu protocol TCP/IP menjadi crash atau tidak bisa berfungsi sebagaimana mestinya.

Teardrop:Porongan paket data ini kadang hnrus dipotong ulang menjadi lebih kecil lagi pada snat disalurkan melalui saluran Wide Area Network agar pada saat melalui saluran WAN tidak reliable maka proses pengiriman data itu menjadi reliable. Pada proses pemotongan data pekat yang normal. Program teardrop akan memanipulasi offset potongan data sehingga akhimya terjadi overlapping antara paket yang diterima di bagian penerima setelah potongan-potongan paket ini disa ssembly-reassembly.

Spoofing:adalah suatu serangan tekais yang rumit yang terdiri dari beberapa komponen. Ini adalah eksploitasi keamanan yang bekerja dengan menipu komputer, seolah-olah yang menggunakan komputer tersebut adalah orang lain. Hal ini terjadi karena design flow. Filterisasi yang ditempatkan pada router dapat mengeliminasi secara efektif IP Spoofing. Router mencocokkan IP source address dari masing-masing paket keluar terhadap IP address yang ditetapkan. Jika IP source address ditemukan tidak cocok, paket dihilangkan. Bahkan dengan mengamati cara mengurutkan nomor paket bisa dikenali sistem yang digunakan.

Tabel

Spesifik Yang Berhubungan Dengan Masalah Yang Diteliti

No	Judul	Hasil	Persamaan	Perbedaan
1	Aplikasi Model Sistem Keamanan Jaringan Berbasis DMZ (Addy Suyatno, 2009)	Mengetahui nama sebuah komputer dan alamat IP-nya, Melakukan pendeteksian dan penutupan koneksi pada TCP/IP, mengetahui nama komputer lain dan Alamat IP masing-masing, melakukan pendeteksian port pada TCP/IP, melakukan operasi ping pada TCP/IP dan terakhir melakukan pendeteksian alamat MAC	Menggunakan Teknik yang sama	Penggunaan analisis dan perancangan
2	Implementasi dan analisis sistem keamanan jaringan DMZ dengan intrusion prevention system (Mulya	Jaringan DMZ dengan IPS dapat di imlentasikan dengan baik	Menggunakan metode yang sama	Penggunaan sistem

	na, 2011)			
3	Teknik Keamanan Jaringan dan Data Dengan Linux DMZ (Jufriadif Na'am, 2012)	Untuk membuat Linux Demilitarized Zone terlebih dahulu menentukan software yang akan mendukung sistem yang dibangun, dari sisi pemilihan topologi yang akan digunakan kita harus melihat data teknis terlebih dahulu	Dalam metodologi Yang di gunakan	Penggunaan sistem
4	Analisis dan Perancangan Keamanan Jaringan Menggunakan Teknik DMZ (Benny Wijaya, Denny, Alex, 2014)	Dengan membuat segmen jaringan menggunakan DMZ, maka akses dari luar ke jaringan internal dapat dibatasi sehingga tidak bisa langsung menuju jaringan internal dan ini meningkatkan kemanan jaringan dan mampu melindungi jaringan komputer dari ancaman	Menggunakan Teknik yang sama	Penggunaan metode

Gambar

Sistem pendeteksi intrusi yang dikembangkan berjenis NIDS karena DMZ berbasis IDS jenis ini ditempatkan di sebuah tempat/titik yang strategis atau sebuah titik di dalam sebuah jaringan untuk melakukan pengawasan terhadap traffic yang menuju dan berasal dari semua alat-alat dalam dalam jaringan. Idealnya semua traffic yang berasal dari luar dan dalam jaringan dilakukan di scan.

Rincian keterangan dari gambar topologi jaringan komputer diatas adalah sebagai berikut:

Jenis topologi yang diterapkan adalah Star

Seluruh alamat internal protocol yang digunakan adalah Kelas C.

Pada penelitian ini kedua jenis kabel tersebut dibutuhkan untuk menghubungkan perangkat-perangkat jaringan yang digunakan. Berikut penjelasan jenis kabel yang digunakan untuk menghubungkan setiap perangkatnya:

Jenis kabel yang digunakan untuk menghubungkan antara komputer client dengan Hub adalah straight.

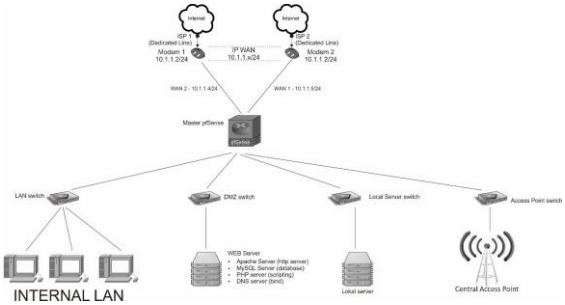
Jenis kabel yang digunakan untuk menghubungkan antara Firewall ke Server adalah kabel cross.

Jenis kabel yang digunakan untuk menghubungkan antara Firewall ke Hub ke mesin sensor adalah kabel straight.

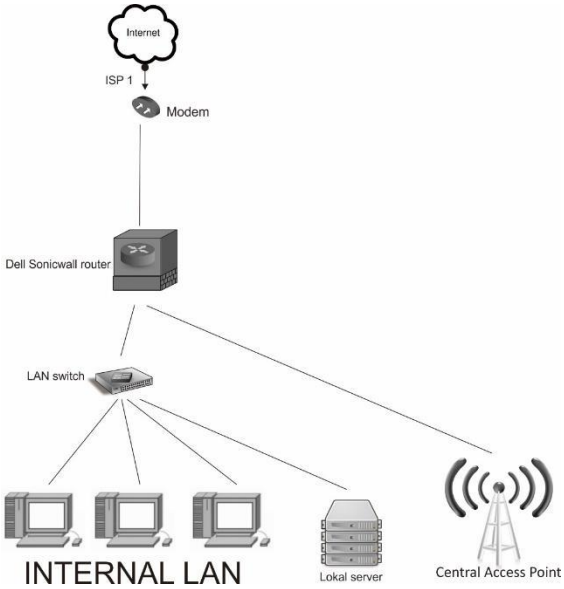
Jenis kabel yang digunakan untuk menghubungkan antara firewall ke Hub adalah kabel straight.

Jenis kabel yang digunakan untuk menghubungkan antara Access Point ke Hub adalah kabel straight.

Tipe koneksi yang digunakan untuk menghubungkan Access Point ke client penyerang adalah melalui tranmisi wireless.



Gambar 1. Topologi Jaringan Setelah diterapkan DMZ Berbasis IDS



Gambar 2. Topologi Jaringan Sebelum diterapkan DMZ Berbasis IDS

KESIMPULAN

Sistem IDS yang diterapkan pada Demilitarized Zone telah berhasil dibangun dan dikembangkan dengan baik. Keseluruhan system mesin sensor IDS dapat bekerja dengan efektif sebagai sistem keamanan jaringan komputer yang berbasis open source dabm mendeteksi sebuah intruder atau penyusup pada mesin sensor IDS, dimana dalam mendeteksi suatu serangan dianalisis pada ACID. Untul lebih jelasnya dapat dilihat pada gambar.

Mekanisme system kerja Snort dan ACID yang telah berhasil di implementasikan dengan baik. Dalam pengujian sistem snort dan ACID yaitu dengan menggunakan Ping attack dan Port scanning. dan Digital Blaster. Dimana rule tersebut untuk mcblok berdnarkan, bmat IP Address. Saal rules dimasukkan ke dalam ruk iptable, mako akan tcrlihol pada mesin penyerang atau client yaitu request time out. seperti yang terlihat pada gambar.

Kelebihan dalam menggunakan IDS ini adalah suatu jaringan computer dapat dipantau hanya dengan sebuah mesin atau komputer yang bertindak sebagai sensor didalam jaringan dan terhubung kedalam sebuah jaringan itu dapat melihat semua kejadian yang sedang terjadi didalamnya, Selain keuntungan didapat dalam penerapan IDS ini.

PUSTAKA

Addy Suyatno, 2009. *Aplikasi Model Sistem Keamanan Jaringan Berbasis De-Militarized Zone*. Jurnal Informatika Mulawarman. Samarinda.

Anhar. 2010. *PHP & MySql Secara Otodidak*. Jakarta. PT TransMedia

Arief M Rudianto. 2011. *Pemrograman Web Dinamis menggunakan PHP dan MySQL*. C.V ANDI OFFSET. Yogyakarta.

Ariyus, D. 2007. *Intrusion Detection System*. Andi Yogyakarta. Yogyakarta.

Benny Wijaya, Dedi Rianto Rahadi, Alex Wijaya, 2014. *Analisis Dan Perancangan Keamanan Jaringan Menggunakan Teknik DMZ.* Seminar Nasional Teknologi Informasi, Komunikasi dan Managemen. Palembang.

Blair, Chris and Rutenbeck, Jeffrey B. "*Digital Media and Arts Education: A First Look*," International Digital Media and Arts Association Journal, Vol.1., No. 2, Fall 2004.

Bunafit, Nugroho, 2006. *Membuat Aplikasi Sistem Pakar dengan PHP dan My SQL dengan PHP dan MySQL dengan Editor Dreamweaver*. Ardana Media, Yogyakarta.

Coleman Curtis. Case Study: *An Evolution of Putting Security into SDLC. Available*: http://www.owasp.org/docroot/owasp/misc/COLEMAN-Putting_Security_IntoSDLS-OWASP_v2.ppt

Davison, R. M., Martinsons, M. G., Kock N., 2004. *Journal: Information Systems Journal: Principles of Canonical Action Research.* 14, 65-86.

Dwianta A. 2010. (IDS) *Intrusion Detection System*. Bandung.

Gary Sims, 2008. *Learning FreeNAS: Configure and manage a network attached storage solution*. Kindle Edition.

Guritno, Sudaryono dan Raharja, 2011. *Metode Penelitian Tindakan.* Yogyakarta. Penerbit Andi.

Hantoro, G. D. 2009. *WIFI (Wireless LAN) Jaringan Komputer Tanpa Kabel*. Informatika. Bandung.

http://ecgalery.blogspot.co.id, 2011. *dmz-de-militarised-zone*. Diakses pada tanggal 2 Pebruari 2017.

Jufriadif Na'am, 2012. *Teknik Keamanan Jaringan dan Data Dengan Linux Demilitarized Zone*. Universitas Putra Indonesia. YPTK. Padang

Junior, Dkk. 2009. *Perancangan Intrusion Detection System pada Jaringan Nirkabel*. BINUS Universitas. Jakarta.

Kurniawan, Rulianto. 2008. *Membangun Situs dengan PHP untuk Orang Awam.* Palembang. Maxsikom.

Muhammad Diah Maulidin, Muhamad Akbar, M.I.T., Siti Sa'uda, M.Kom. 2015. *Analisis Dan Implementasi Metode DMZ Untuk Keamanan*

Jaringan Pada LPSE Kota Palembang. Universitas Bina Darma. Palembang.

Mulyana, 2011. *Implementasi dan Analisis Sistem Keamanan Jaringan Demilitarized Zone (DMZ) dengan Intrusion Prevention System*. Universitas Telkom. Bandung

Nazir, Moh.Ph.D. 2005. *Metode Penelitian. Ghalia Indonesia*. Boger.

O'Brien, J. A. 2005. *Pengantar Sistem Informasi*. Edisi 12. Salemba Empat.

Paulo, J. A. dan Albertino. Y. 2000. *Ntop- Network Top*. University Of Twente. The Netherlands.

Purbo, W. Onno. 2007. *Buku Pintar Internet TCP/IP*. PT. Elex Media Komputindo. Jakarta.

Rafiudin, R. 2003. *Mengupas Tuntas Cisco Router*. PT. Elex Media Komputindo. Jakarta.

Setiawan, Thomas. 2004. *Analisis Keamanan Jaringan Internet Menggunakan Hping, Nmap, Nessus dan Ethereal*. ITB.

Slameto, A. A. 2007. *Sistem Pencegah Penyusupan*. STMIK AMIKOM Yogyakarta.

Sopandi, D. 2008. *Instalasi dan Konfigurasi Jaringan Komputer*. Informatika Bandung.

Spealman, Jill., and Kurt Hudson. 2004. *Planning, Implementing and Maintaining Microsoft Windows server 2003 Active Directory Infrastructure*. Washington: Microsoft Press.

Sugiyono, Prof. Dr. (2009). *Metode Penelitian Kuantitatif Kualitatif dan R & D*. CV Alfabeta. Bandung.

Sukmaaji, Anjik, S.Kom dan Rianto, S. Kom. 2008. *Konsep Dasar Pengembangan Jaringan don Keamanan Jaringan*, Andi Yogyakarta. Yogyakarta.