e-ISSN: 2655-142X
p-ISSN: 2655-190X

KEAMANAN JARINGAN NIRKABEL MENGGUNAKAN WIRELESS INTRUSION DETECTION SYSTEM

Joko Dwi Santoso

Teknik Komputer Universitas AMIKOM Yogyakarta
email : joko@amikom.ac.id

Abstraksi

Sistem keamanan jaringan menjadi sangat penting dalam memelihara jaringan, serangan yang dapat mengganggu dan bahkan merusak sistem koneksi antar perangkat yang terhubung akan sangat berbahaya. Untuk mendapatkan keamanan dalam jaringan kadang-kadang kita harus merasakan ketidaknyamanan dalam penggunaannya, ini sering menjadi pertimbangan dalam penerapan sistem keamanan jaringan di Kantor Kejaksaan Belitung Timur. WIDS (Wireless Intrusion Detection System) mampu mendeteksi serangan DOS (Denial of Service), Ping Of Deat. Mengimplementasikan pada sistem operasi Linux menggunakan Snort, ACID BASE, Barnyard, pada mesin sensor IDS dan Iptables sebagai penanganan serangan dapat menjadi solusi keamanan jaringan nirkabel dari serangan yang mengancam. Metode penelitian yang saya gunakan adalah metode Siklus Hidup Pengembangan Kebijakan Keamanan (SPDLC). Hasil penelitian ini menyimpulkan bahwa IDS yang diterapkan dapat mendeteksi penyusup atau penyususp pada mesin sensor IDS yang ditampilkan pada BASE (Basec Analysis and Security Engine). Penerapan sistem keamanan jaringan terintegrasi IDS (Intrusion Detection System) berbasis open source.

***Kata Kunci* :**
Wireless, IDS (Intrusion Detection System), Denial of Service, Ping Of Deat, Iptables, Network Security, Linux, Snort, ACID BASE, Barnyard, Security Policy Development Life Cycle.

Abstract

Network security system becomes very important in maintaining a network, attacks that can interfere and even damage the connection system between devices connected will be very harmful. To gain security in a network sometimes we have to feel the discomfort in its use, this is often a consideration in the application of a network security system in the East Belitung Prosecutor's Office. WIDS (Wireless Intrusion Detection System) is capable of detecting DOS attacks (Denial of Service), Ping Of Deat. Implementing on a Linux operating system using Snort, ACID BASE, Barnyard, on IDS sensor engines and Iptables as an attack handling can be a wireless network security solution of threatening attacks. The research method I use is the method of Security Policy Development Life Cycle (SPDLC). The results of this study conclude that the IDS applied can detect intruders or penyususp on IDS sensor machine that is displayed on BASE (Basec Analysis and Security Engine). Application of integrated network security system IDS (Intrusion Detection System) based on open source.

***Keywords* :**
Wireless, IDS (Intrusion Detection System), Denial of Service, Ping Of Deat, Iptables, Network Security, Linux, Snort, ACID BASE, Barnyard, Security Policy Development Life Cycle.

Pendahuluan

1.1. Latar Belakang Masalah

Keamanan jaringan merupakan hal yang penting untuk mengamankan suatu aset perusahaan, aset dari suatu sistem yang tidak tersedia atau tidak di pakai oleh yang berwenang dapat di pergunakan oleh oknum yang tidak bertanggung jawab untuk melakukan tindakan pencurian data, melakukan perubahan nilai pada file data,memodifikasi program sehingga tidak berjalan semestinya dan penyadapan terhadap data dalam suatu jaringan.

Dibutuhkan sebuah keamanan untuk menjaga komputer agar tidak terkena serangan oleh pihak luar yang tidak berwenang. Keamanan jaringan komputer sebagai bagian dari sebuah system yang penting untuk menjaga validitas dan integritas data. Jaringan komputer sangat berkaitan erat dengan jaringan nirkabel. Seperti komputer, notebook, handphone dan periperalnya mendominasi pemakaian teknologi wireless. Penggunaan teknologi wireless dalam suatu jaringan lokal sering dinamakan dengan WLAN (Wireless Local Area Network) dan dibutuhkan IDS untuk menganalisis keamanan jaringan nirkabel.

Upaya untuk meningkatkan keamanan jaringan komputer salah satunya adalah dengan firewall. Implementasi dari sistem firewall ini dapat berupa software ataupun hardware yang bersifat aktif dengan melakukan penyaringan paket data yang lewat berdasarkan pengaturan yang diinginkan. Cara lain adalah dengan mengimplementasikan Intrussion Detection System (IDS) pada sebuah Jaringan

Komputer. Sedikit berbeda dengan firewall, Intrusion Detection System (IDS) adalah sebuah sistem yang digunakan untuk. melakukan deteksi adanya usaha-usaha penyusupan terhadap sebuah sistem dengan melakukan pengamatan trafik data secara real-time.

Berdasarkan beberapa pertimbangan di atas, maka tujuan dari penelitian yang dilakukan adalah melakukan analisis keamanan jaringan, menggunakan (Wireless Intrussion Detection System (WIDS) dan mendapatkan hasilnya untuk mengetahui sistem keamanan di dalam kantor.

Dengan didasari oleh latar belakang permasalahan di atas, maka permasalahan penelitian yang akan di bahas pada jaringan wireless adalah sebagai berikut :

1. Bagaimana mencegah terjadinya aktivitas intrusi (penyusupan) atau penyerangan pada sistem keamanan jaringan ?
2. Bagaimana menganalisis keamanan jaringan menggunakan (Wireless Intrussion Detection System (WIDS)?
3. Bagaimana kelebihan (Wireless Intrussion Detection System (WIDS) dalam mengamankan keamanan jaringan ?

Tinjauan Pustaka

A. Landasan Teori

1. Keamanan jaringan

Keamanan dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan. Segi-segi keamanan didefinisikan lima poin, yaitu Confidentiality, Mensyaratkan bahwa informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang, Integrity, Mensyaratkan bahwa informasi hanya dapat diubah oleh pihak yang memiliki wewenang, Availability, Mensyaratkan bahwa informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan, Authentication, Mensyaratkan bahwa pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu, Nonrepudiation, Mensyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

Keamanan jaringan secara umum adalah komputer yang terhubung ke network, mempunyai ancaman keamanan lebih besar dari pada komputer yang tidak terhubung kemana-mana. Dengan pengendalian yang teliti, resiko tersebut dapat dikurangi, namun network security biasanya bertentangan dengan network access, dimana bila network access semakin mudah, maka network security semakin rawan, begitu pula sebaliknya.

2. Snort

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mempu menganalisis paket yang melintasi jaringan secara real time traffic dan logging kedalam database serta mampu mengidentifikasi berbagai serangan yang berasal dari luar jaringan. (Ariyus, 2007:45) Program snort dapat dioprasikan dengan tiga mode, (Ariyus, 2007:146) yaitu Paket Sniffer yang berfungsi untuk melihat paket yang lewat di jaringan, Paket Logger yang berfungsi untuk mencatat semua paket yang lewat di jaringan untuk dianalisis di kemudian hari dan NIDS (Network Intrusion Detection System), pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan computer.

B. IDS (Intrusion Detection System)

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 jaringan computer. Intrusion Detection System(IDS) sebenarnya tidak cocok di beri peringatan tersebut karena IDS tidak mendeteksi penyusup tetapi hanya mendeteksi aktivitas pada lalu lintas jaringan yang tidak layak terjadi. Intrusion Detection System secara khusus berfungsi sebagai proteksi secara keseluruhan dari sistem yang telah diinstall IDS. IDS tidak berdiri sendiri dalam melindungi suatu sistem.

1. BASE (Basic Analysis and Security Engine) .

BASE adalah sebuah interface web untuk melakukan analisis dari intrusi yang snort telah deteksi pada jaringan. (Orebaugh, 2008:217) BASE ditulis oleh Kevin Johnson adalah program analisis sistem jaringan berbasis PHP yang mencari dan memproses database dari security event yang dihasilkan oleh berbagai program monitoring jaringan, firewall atau sensor IDS. (Kuhlenberg, 2007:424). Ini menggunakan otentifikasi pengguna dan sistem peran dasar, sehingga sebagai admin keamanan dapat memutuskan apa dan berapa banyak informasi yang setiap pengguna dapat melihat. BASE adalah sistem manajemen basis data berbasis desktop yang lengkap, didesain untuk memenuhi kebutuhan yang luas dari pengguna, mulai dari melacak koleksi CD pribadi Anda, hingga menghasilkan laporan penjualan bulanan BASE menawarkan panduan untuk membantu

e-ISSN: 2655-142X
p-ISSN: 2655-190X

pengguna yang baru terhadap desain basis data (baru terhadap BASE) untuk membuat Tabel, Query, Form, dan Report, bersama dengan sekumpulan definisi tabel yang sudah didefinisikan untuk melacak Asset, Konsumen, Penjualan, Invoice, dan banyak lagi. Ketika Anda hanya memerlukan basis data personal, BASE menawarkan mesin basis data relasional HSQL, dikonfigurasi untuk pengguna tunggal, dengan data tersimpan pada dokumen BASE, beserta dengan dukungan native untuk dokumen BASE. Untuk kebutuhan yang lebih besar, BASE mendukung berbagai basis data yang populer secara native : MySQL, Adabas D, Microsoft Access, dan Postgre SQL. Sebagai tambahan, dukungan untuk driver standar JDBC dan ODBC juga mengijinkan Anda untuk terhubung secara virtual pada sembarang basis data yang ada.

2. IP Tables

Iptables adalah firewall yang secara default diinstal pada semua distribusi linux, seperti Ubuntu, Fedora dan lainnya. Pada saat melakukan instalasi pada linux, iptables sudah langsung ter-install, tetapi pada umumnya iptables mengizinkan semua traffic untuklewat. (Purbo, 2008:188) Iptables adalah suatu tools dalam sistem operasi linux yang berfungsi sebagai alat untuk melakukan filter (penyaringan) terhadap lalu lintas data. Secara sederhana digambarkan sebagai pengatur lalu lintas data. Dengan iptables inilah kita akan mengatur semua lalu lintas dalam komputer kita, baik yang masuk ke komputer, keluar dari komputer, ataupun traffic yang sekedar melewati komputer kita.

3. DOS (Denial Of Service)

DoS attack adalah jenis serangan tehadap sebuah komputer atau server atau router atau mesin didalam jaringan internet dengan cara menghabiskan resource yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar, sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang di serang (server) tersebut.

4. Nmap

Nmap(network mapper) adalah sebuah program open source yang berguna untuk mengeskplorasi jaringan. Nmap didesain untuk dapat melakukan scan jaringan yang besar, juga dapat digunkan untuk melakukan scan host tunggal. Nmap menggunakan paket IP untuk melakukan host-host yang aktif dalam suatu jaringan, prot-port yang terbuka, system operasi yang dipunyai, tipe firewall yang di pakai (Setiawan,2014:24).

Metode Penelitian

A. Analisis Sistem

Analisis sistem dapat didefinisikan sebagai penguraian dari suatu sistem informasi yang utuh kedalam bagian-bagian komponennya dengan maksud untuk mengidentifikasi dan mengevaluasi permasalahan-permasalahan, kesempatan-kesempatan, hambatan-hambatan yang terjadi dan kebutuhan-kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan-perbaikannya. Sebagai analisis pada sistem yang sedang berjalan, akan dibahas bagaimana kelemahan pengunaan *wifi*, bagaimana analisis keamanan jaringan nirkabel menggunakan IDS(*Intrusion Detection System*), analisis snort dan analisis sistem non fungsional yang meliputi perangkat keras dan perangkat lunak yang digunakan, serta analisis *user* yang terlibat.

B. Analisis pengembangan system

1. Metode *Security Policy Development Life Cycle* (SPDLC)

Metode pengembangan *Security Policy Development Life Cycle* (SPDLC) adalah siklus hidup pengembangan system jaringan yang didefinisikan pada sejumlah fase, antara lain: *Analysis, Design, Implementation, Enforcement,* dan *Enhancement.*

C Perancangan Sistem

1. Metode Pengembangan Sistem

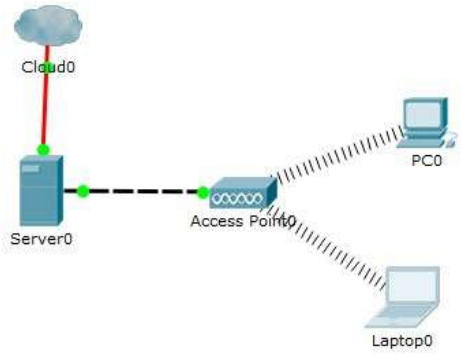
Dalam proses pengembangan sistem banyak metode atau model yang ada. Pada penelitian akan dibangun sistem IDS dimana lingkup pembahasan mengenai jaringan sehingga metode atau model pengembangan sistem yang digunakan dalam penelitian ini adalah SPDLC (Security Policy Development Life Cycle).

SPDLC adalah metode yang menetapkan strategi untuk melakukan pembaharuan suatu organisasi dari sistem jaringan, siklus pengembangan sistem jaringan didefinisikan pada sejumlah fase . Menurut Luay A. Wahsheh and Jim Alves Foss (2008:1120) Pengembangan sistem SPDLC yang diambil melakukan penelitian dalam 5 tahap, yaitu tahap Analysis : Pada tahap ini dilakukan perumusan masalah, mengidentifikasi konsep dari IDS, Ethereal dan beberapa perangkat jaringan, mengumpulkan data dan mengidentifikasi kebutuhan seluruh kompunen sistem tersebut, sehingga spesifikasi kebutuhan sistem IDS dan Snort dapat diperjelas dan perinci. Pada tahapan analisis yang dilakukan adalah Identification, Understand dan Report. Tahap Design : Pada tahap ini yang dilakukan adalah Merancang

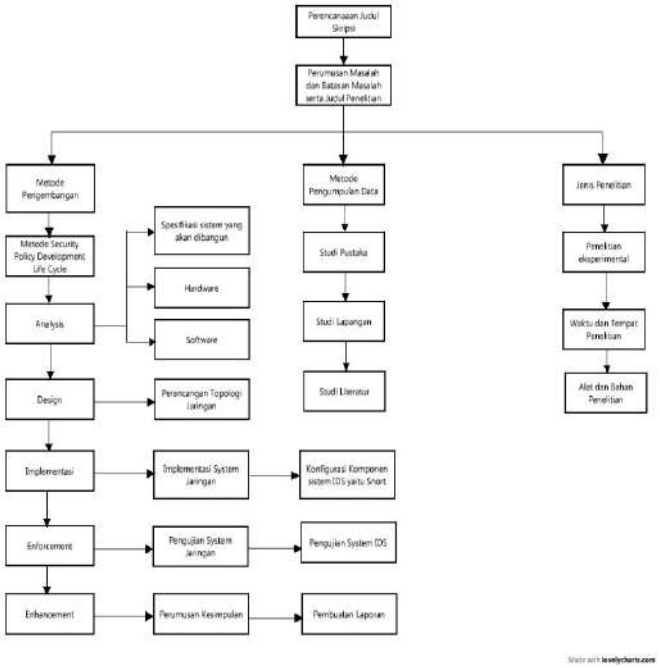
topologi jaringan untuk simulasi WAN sebagai representasi lingkungan jaringan sebenarnya dan merancang penggunaan sistem operasi dan aplikasi pada server, client dan komputer penyusup. Rancangan topologi jaringan dibangun dengan menggunakan Cisco Packet Tracer yang di instal baik dalam kondisi sebelum diterapkan IDS yang dapat dilihat pada gambar 1. Dan kondisi pada saat telah diterapkan IDS yang dapat dilihat pada gambar 2. Implementation : Fase selanjutnya adalah implementasi atau penerapan detail rancangan topologi dan rancangan sistem pada lingkungan nyata sebagai simulasi wireless. Detail rancangan akan digunakan dapat dilihat pada gambar 3. sebagai intruksi atau panduan tahap implementasi agar sistem yang dibangun dapat relevan dengan sistem yang sudah dirancang. Proses implementasi terdiri dari instalasi dan konfigurasi. Dengan mengumpulkan seluruh perangkat yang dibutuhkan dilaboraturium riset. Tahap Enforcement : Setelah tahap implementasi adalah tahap Enforcement dimana tahap ini penting. Proses pelaksanaan atau penyelenggaraan dilakuakan melalui aktivitas pengoprasian dan pengamatan sistem yang sudah dibangun dan diterapkan apakah sistem IDS sudah berjalan dengan benar dan baik

2. Alur Metode Penelitian

Tahapan dalam penelitian ini telah dicantumkan dalam diagram alur penelitian yang sebelum memasuki dan keluar dari model atau metode pengembang dari SPDLC terdapat beberapa tahap yang harus dilakukan. SPDLC adalah metode yang menetapkan strategi untuk melakukan pembaharuan suatu organisasi dari sistem jaringan yang dapat dilihat pada gambar 2.



Gambar 1. Topologi Jaringan



Gambar 2. Rancangan Alur Penelitian

D. *Implementation*(implementasi)

1. Konfigurasi Mesin Snort

Instalasi Snort Dalam penelitian ini penulis menggunkan aplikasi snort versi 2.9.11.1. Berikut adalah prosesnya:

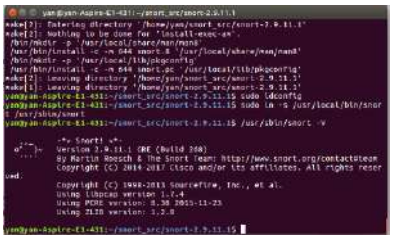
Tabel 1. Inastallasi Snort

#Membuat direktori untuk menyimpan file yang didownload
$ mkdir ~/snort_src
$ cd ~/snort_src
#Menginstal semua prasyarat dari repositori Ubuntu
$ sudo apt-get install -y build-essential libpcap-dev libpcre3-dev libdumbnet-dev bison flex zlib1g-dev liblzma-dev openssl libssl-dev
#Ubuntu 16 only:
$ sudo apt-get install -y libnghttp2-dev
#Pemanggilan *Data Acquisition library* (DAQ) yang didownload dan diinstall dari situs snort (*snort.org*)
$ cd ~/snort_src
$ wget https://snort.org/downloads/snort/daq-2.0.6.tar.gz
$ tar -xvzf daq-2.0.6.tar.gz
$ cd daq-2.0.6
$ ./configure && make && sudo make install
#Menginstall Snort
$ cd ~/snort_src
$ wget https://snort.org/downloads/snort/snort-2.9.11.1.tar.gz
$ tar xvzf snort-2.9.11.1.tar.gz
$ cd snort-2.9.11.1

e-ISSN: 2655-142X
p-ISSN: 2655-190X

$ ./configure --enable-sourcefire && make && sudo make install
#Memperbarui shared library
$ sudo ldconfig
Karena instalasi Snort menempatkan biner Snort di / usr / local / bin / snort, ini adalah kebijakan yang baik untuk membuat symlink ke / usr / sbin / snort
$ sudo ln -s /usr/local/bin/snort /usr/sbin/snort
#Jalankan Snort dengan flag -V, yang menyebabkan Snort menunjukkan nomor versinya
$ /usr/sbin/snort -V

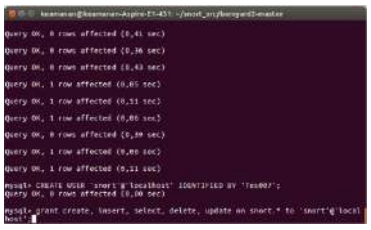
Berikut output setelah snort berhasil terinstall.



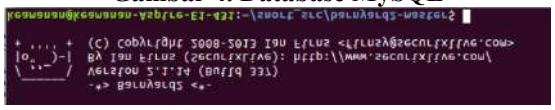
Gambar 3. Proses Instalasi Snort

2. Instaling Barnyard2

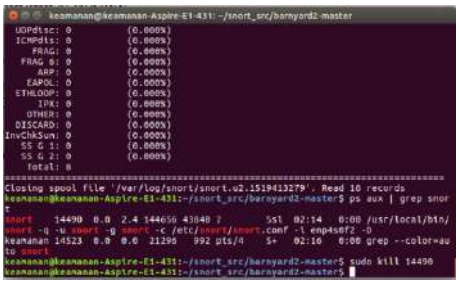
Barnyard2 yang digunakan menyimpan alert ke database MySQL ,perlu membuat database itu, dan juga 'mendengus' pengguna MySQL untuk mengakses database.



Gambar 4. Database MySQL



Gambar 5. Barnyard2 Berhasil Terinstall



Gambar 6. Sukses Konfigurasi Barnyard2

3. **Installing PulledPork**

Installing PulledPork ini akan mengisntal sebuah script Perl yang disebut PulledPork, yang secara otomatis akan mendownload ruleset terbaru dari situs Snort.

#Pertama

sudo apt-get install -y libcrypt-ssleay-perl liblwp-useragent-determined-perl.

Gambar 7. Instalasi PulledPork

4. Installing BASE On Ubuntu

BASE adalah web GUI sederhana untuk Snort. Produk alternatif termasuk Snorby, Splunk, Sguil, AlienVault OSSIM, dan server syslog manapun. untuk mengkonfigurasi BASE dilakukan melalui http:

- Masuk browser http://192.168.1.8/base/index.php**, dan klik Setup Page.**
- **Klik Create BASE AG**
- **Klik Main page**

Gambar 8. Tampilan Basic Analysis and Securoty Engine (BASE)

E. Pengujian *Komponen* IDS

1. Pengujian Snort

Pengujian snort pada mesin sensor dilakukan dengan menggunkan rules sederhana(sebagai representasi dari definisi jenis serangan tertentu) dan memastikan snort dapat mendeteksi rules tersebut. Snort diaktifkan dengan perintah berikut, agar dapat mencetak hasilnya langsung ke layer console : *snort -c/etc/snort/snort.conf -i enp4s0f2.*

Gambar 9. Pengujian Fungsi Snort

2. Pengujian BASE

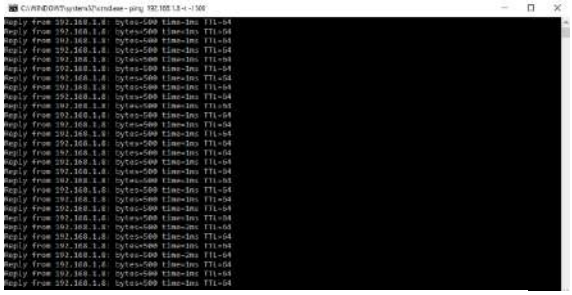
Pengujian fungsionalitas ACID BASE yang dilakukan dengan mengakses dan mengeksplorasi system ACID BASE secara keseluruhan. Hasilnya, ACID BASE telah berhasil di implementasikan dan dapat menampilkan event snort ketika bekerja dalam memonitoring setiap kegiatan dalam jaringan.

Gambar 10. Pengujian Fungsi BASE

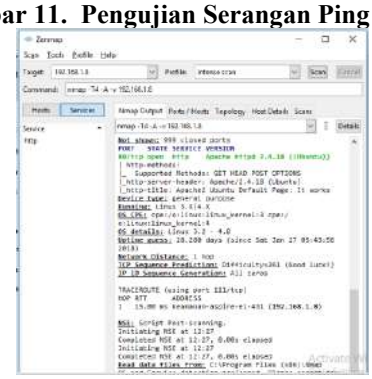
3. Pengujian Fungsionalitas Interkoneksi IDS

Penulis menggunkan studi kasus untuk menguji system IDS dalam melindungi *server*. Studi kasus ini penulis representasikan dengan melakukan simulasi serangan. Pada skripsi ini penulis melakukan beberapa percobaan adalah sebagai berikut:

- Ping Attack (ICMP Traffic)
- Nmap Port Scanning Attack(Zenmap gui)
- DDOS



Gambar 11. Pengujian Serangan Ping Attack

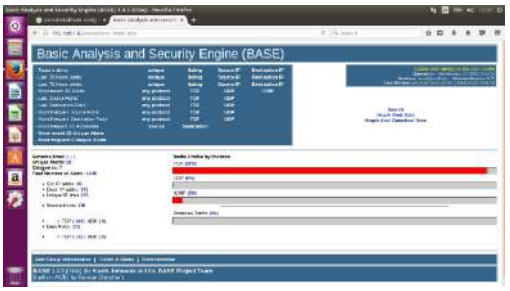


Gambar 12. Pengujian Serangan Nmap

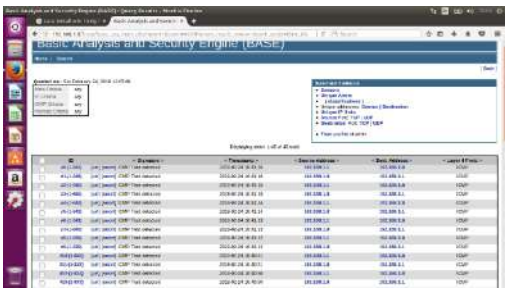
Hasil dan Pembahasan

A. Hasil Analisis Menggunakan IDS

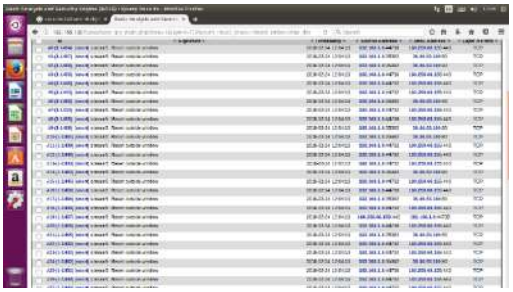
Analisisi pengujian data yang dilakukan berupa pengujian fungsionalitas interkoneksi IDS, dimulai dari proses serangan dan pendeteksian serta penanganan serangan. Tampilan dari data yang dianalisi, kondisi sebelum dan sesudah penyerangan. Setelah melakukan berbagai proses dalam penerapan IDS, terdapat kemudahan dalam penerapannya.



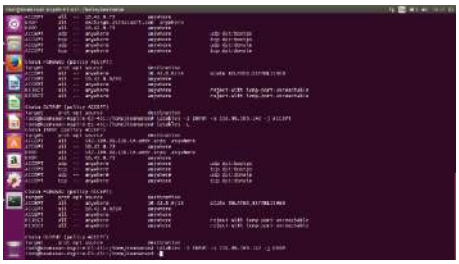
Gambar 13. Pendeteksian Serangan di BASE



Gambar 14. Tampilan Daftar Alert ICMP pada Traffic Profile By Protokol



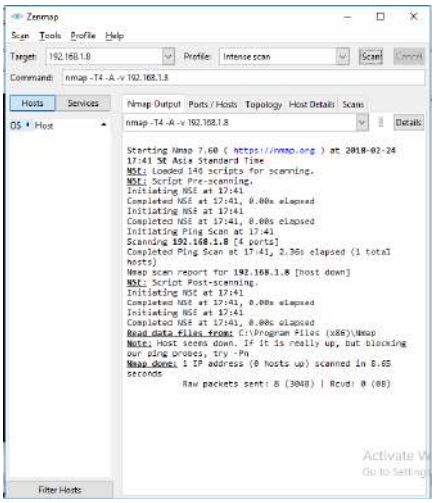
Gambar 15. Tampilan Daftar Alert TCP pada Traffic Profile By Protokol



Gambar 16. DROP IP Dengan Iptables

Gambar 17. Tampilan Hasil Penanganan Serangan Ping Attack

e-ISSN: 2655-142X
p-ISSN: 2655-190X



Gambar 18. Tampilan Nmap Ketika Dilakukan Pencegahan

Analisis yang didapat dari hasil proses pengujian yang telah dilakukan adalah kondisi berjalan dengan baik pada saat sebelum terjadi penyerangan, kemudian terjadi gangguan saat serangan dilakukan, yang membuat pendeteksian menampilakan informasi dan rincian data dari penyerang, kemudian berhasil dilakukan penanganan dengan kondisi yang diperlukan sehinggan semua serangan berhasil diblokir dengan baik

Kesimpulan dan Saran

Kesimpulan

Rumusan kesimpulan dari keseluruhan proses penelitian yang telah dilakukan dari pembahsan yang sudah diuraikan dengan kesimpulan sebagai berikut:

1. Sistem IDS yang telah dibangun dalam mendeteksi serangan yang terjadi adalah dengan melakukan *scanning* terhadap sejumlah *source* dan lalu lintas yang terjadi didalam jaringan.
2. Keseluruhan sistem mesin sensor IDS dapat bekerja dengan efektif sebagai sistem keamanan jaringan komputer yang berbasis *open source,* dan didalam mendeteksi sebuah intruder atau penyusup pada mesin sensor IDS akan dianalisis pada BASE (*Basic Analysis and Security Engine).*
3. Mekanisme sistem kerja snort dan BASE yang telah berhasil di implementasikan dengan baik, dalam pengujian sistem snort dan BASE yaitu dengan menggunakan *Ping Attack, Port Scanning(Nmap),* dan DDOS.
4. Pencegahan yang dapat dilakukan terhadap penyerangan adalah dengan menggunakan *iptables*. Untuk mengatasi serangan dari *intruder* yaitu dengan cara *ping attack* dan Nmap ke sebuah *server*, maka dilakukan konfigurasi *rule iptables*, dimana *rule* tersebut untuk memblock berdasarkan alamat *IP Addres.*
5. Kelebihan dalam menggunkan IDS ini adalah suatu jaringan komputer dapat dipantau dengan mesin atau komputer yang bertindak sebagai sensor didalam jaringan tersebut dan dapat melihat suatu kejadian yang sedang terjadi didalamnya. Selain keuntungan yang didapatkan penulis juga mendapatkan hasil dari sistem IDS dalam mengamankan jaringan, yaitu apabila terdapat suatu masalah pada jaringan(proses intrusi) maka dapat diketahui secara langsung oleh IDS ini yang menggunakan snort, dari mana serangan itu datang.

Saran

Saran-saran yang diberikann pada penelitian ini adalah sebagai berikut:

1. Sistem keamanan dengan WIDS snort dapat memberikan manfaat lebih apabila snort diintegrasikan dengan firewall. Snort efektif untuk mendeteksi adanya sebuah serangan terhadap sistem, akantetapi snort bukanlah sebuah intrusion Prevention sistem(IPS) yang dapat mencegah atau meblokir usaha-usaha penyusupan kedalam sistem.

1. IDS hanya melakukan monitoring jaringan, akan lebih baiknya IDS yang diterapkan dapat melakukan pencegahan dari serangan yang terjadi secara otomastis.

Daftar Pustaka

[1] Putri Lidia, *Implementasi Intrusion Detection System (IDS) Mengunakan Snort Pada Jaringan Wireless (Studi Kasus: SMK Triguna Ciputat)*. Jakarta ,2011.

[2] Satria Ariando, *Pengembangan perangkat wireless IDS(Intrusion Detection System) Berbasis Embedded System (studi kasus : Badan Narkotika Nasional).* Jakarta, 2011.

[3] Ilmam Fajar, *Analisis Dan Perancangan Keamanan Jaringan Menggunakan Intrusion Detection System Dan Firewall Pada Routerboard Mikrotik RB951Ui-2HnD Berbasis SMS Gateway,* Yogyakarta,2016.

[4] D Ariyus, *Intrusion Detection System (System Pendeteksi Penyusup Pada Jaringan Komputer).* Yogyakarta: Andi Offset, 2007

[5] Wijaya Guntur, *Perancangan Dan Implementasi Pengamanan Jaringan Berbasis IDS* (*Intrusion Detection System*) *Dan Port Knoking Pada Router Mikrotik RB-750.* Yogyakarta, 2016.

[6] Mentang.R, Alicia.A.E, Sinsuw.ST, Sevarius.B.N, Najon,ST .(2015). Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunkan Wireless Intrusion Detection Sistem. *Jurnal Teknik elektro dan komputer,5 (7),2301-8402.*