Volume 1 Number 1 (2020)
July-December 2020
Page: 153 - 159

E-ISSN: 2745-4584
https://ejournal.insuriponorogo.ac.id
DOI: 10.37680/almikraj.v1i1.5623

AL MIKRAJ
Jurnal Studi Islam dan Humaniora

EARLY WARNING SYSTEM MENGGUNAKAN WHATSAPP NOTIFICATION DARI INTRUSION DETECTION SYSTEM SNORT

Cipta Muhamad Firmansyah[1]
[1]Teknik Informatika, STMIK Dharma Negara Bandung; Indonesia
correspondence e-mail*, listianidewi@gmail.com

Submitted: Revised: 2020/08/09; Accepted: 2020/09/18; Published: 2020/10/24

Abstract

Jaringan computer memberikan banyak kemudahan dalam pengaksesan informasi antar perangkat. Namun adanya jaringan juga berdampak pada kemungkinan terjadinya gangguan terhadap keamanan system. Intrusion Detection Sytem (IDS) membantu pengguna dalam memonitor dan menganalisa gangguan pada keamanan jaringan. Tujuan penelitian ini adalah merancang IDS menggunakan Snort memberikan notifikasi secara realtime melalui media aplikasi whatsapp. Sehingga administrator jaringan dapat mendeteksi kondisi serangan pada jaringan dimanapun kapanpun dengan menggunakan smarthphone.

Keywords

IDS, Snort, Smartphone, WhatsApp

PENDAHULUAN

Seiring dengan perkembangan zaman, Teknologi informasi (IT) menjadi pilihan utama dalam berbagai data dan informasi. Melalui sebuah jaringan komputer data dan informasi dapat dengan mudah dikelola dan disampaikan kepada sasaran penerima, namun informasi yang tersedia dapat bersifat public dan juga bersifat pribadi. Hal ini menimbulkan masalah baru jika seandainya data dan informasi yang bersifat pribadi atau bukan konsumsi publik ini tersebar luas tanpa adanya pihak yang bertanggung jawab, oleh sebab itu keamanan suatu jaringan menjadi sebuah aspek penting dalam melindungi secara optimal sebuah sistem.[1] Terlebih lagi jika jaringan tersebut terhubung ke internet maka berbagai ancaman lain seperti virus,malware,worm dan aktivitas merusak sistem lainnya dapat mempengaruhi kinerja, integritas, serta kredibilitas dari suatu sistem pada jaringan tersebut.

Sistem keamanan firewall tidaklah cukup untuk meminimalkan terjadinya serangan terhadap suatu jaringan komputer. Banyak serangan yang terjadi pada jaringan komputer dapat diketahui setelah adanya kejadian-kejadian yang aneh pada jaringan. Para administrator jaringan tidak bisa mengetahui dengan pasti apa yang sedang terjadi. Sehingga dibutuhkan waktu yang cukup lama untuk diatasi.

[1] Koshechkin, K., Lebedev, G., Radzievsky, G., Seepold, R., & Martinez, N. M. (2021). Blockchain Technology Projects to Provide Telemedical Services: Systematic Review. *J Med Internet Res*, *23*(8), e17475. https://doi.org/10.2196/17475

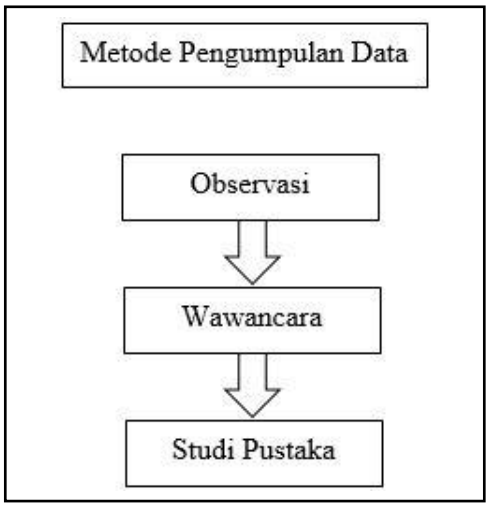
METODE

Data dan informasi yang akan disusun dalam laporan penelitian ini dilakukan dengan menggunakan:

Metode Pengumpulan Data

Observasi melakukan pengamatan di PT. Defenxor yang berhubungan dengan monitoring server. Wawancara melakukan tanya jawab, meminta keterangan kepada bagian yang bertanggung jawab pada operasional server yaitu system administrator. Studi Pustaka dengan melakukan penelitian dengan cara mencari penjelasan dan berbagai macam materi lanjutan mengenai Early Warning System Menggunakan Whatsapp Notification dari Intruision Detection System Snort dan hal-hal yang terkait dari sumber-sumber tertulis yang valid.

Figure 1. Diagram Metode Pengumpulan Data



HASIL DAN PEMBAHASAN

Intrusion Detection System (IDS)

Intrusion Detection system (IDS) dapat didefinisikan sebagai tool, metode, sumber daya yang membeikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan komputer. IDS pada dasarnya adalah suatu sistem yang memiliki kemampuan dalam menganalisa dan mendeteksi data secara realtime, mencatat (log), dan menghentikan usaha penyalahgunaan dan penyerangan.[2] Dalam hal ini IDS tidak secara langsung dapat mendeteksi adanya penyusupan pada sebuah sistem hanya saja IDS dapat mendeteksi aktivitas pada lalu-lintas jaringan yang tidak layak terjadi.

IDS pada umumnya mampu mendeteksi jaringan yang dicurigai, akan tetapi tidak mampu mengambil tindakan lebih lanjut. Selain itu sistem juga tidak memiliki interaktivitas dengan administrator pada saat administrator tidak sedang mengadministrasi sistem nya. Tipe dasar dari IDS terdapat dua bagian, bagian itu adalah:

[2] Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? In *Future Internet* (Vol. 10, Issue 2). https://doi.org/10.3390/fi10020020

1. *Rule-based system* – berdasarkan pada signature dan rule yang tersimpan di database. Jika IDS mencatat lalu-lintas yang sesuai dengan rule dan signature yang ada, maka langung dikategorikan sebagai serangan.
2. *Adaptive system* – mempergunakan metode yang lebih canggih. Tidak hanya berdasarkan database yang ada tetapi juga membuka kemungkinan untuk mendeteksi bentuk-bentuk serangan baru.

Selain tipe pada penerapannya IDS sendiri memiliki tujuan serta mengapa menggunakan IDS, diantaranya adalah:

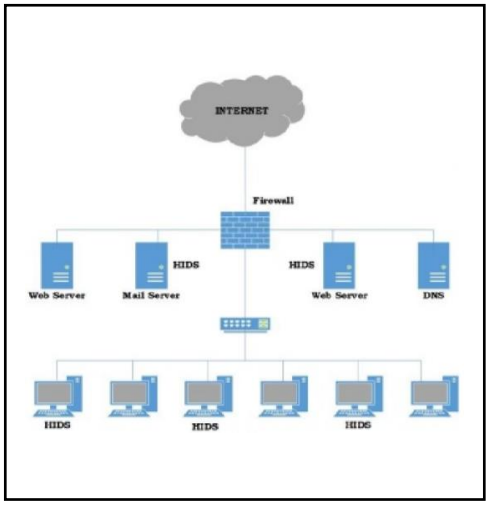
1. Mencegah resiko keamanan yang terus meningkat, karena banyak ditemukan kegiatan illegal yang diperbuat oleh orang-oreng yang tidak bertanggung jawab dan hukum yang diberikan atas kegiatan tersebut.
2. Mendeteksi serangan dan pelanggaran keamanan system jaringan yang tidakbisa dicegah oleh system yang umum digunakan seperti firewall.
3. Mendeteksi serangan awal. Penyerangan yang akan menyerang suatu system biasanya melakukan langkah-langkah awal yang mudah diketahui. Langkah awal dari suatu serangan pada umumnya adalah dengan melakukan penyelidikan dan pengujian system yang akan menjadi target, untuk mendapatkan titik-titik dimana mereka bias masuk.
4. Mengamankan file yang keluar dari jaringan. Kebanyakan serangan yang terjadi pada awalnya berasal dari dalam jaringan itu sendiri, kaena keteledoran para pemakai, sehingga file-file yang akan dikirim ke jaringan eksternal tidak memenuhi policy yang ada. File-file tersebut kemudian dimanfaatkan oleh penyerang untuk batu loncatan mendapatkan akses yang lebih besar. Seperti *Syn Attack*, *IP Spoofing*, *teardrop*, dan sebagainya.
5. Sebagai pengendali untuk security design dan administrator, terutama bagi perusahaan yang besar.
6. meyediakan informasi yang akurat terhadap gangguan secara langsung, meningkatkan diagnosis, recovery, dan mengoreksi faktor-faktor penyebab serangan.

Bedasarkan cara kerjanya, terdapat dua tipe uang ada pada IDS diantaranya:

1. Host-Based. IDS host-based bekerja pada host yang akan dilindungi. IDS jenis ini dapat melakukan berbagai macam tugas untuk mendeteksi serangan yang dilakukan pada host tersebut. Keunggulan IDS host-based adalah pada tugas-tugas yang berhubungan dengan keamanan file. Misalnya ada-tidaknya file yang diubah atau ada usaha untuk mendapatkan akses ke file-file yang sensitive.

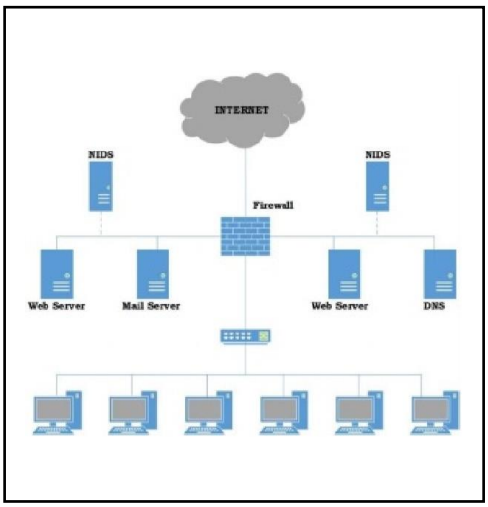
Secara umum Host-Based IDS dijelaskan pada Figur 2

Figure 2. Host-Based IDS



2. Network Based. IDS network-based biasanya berupa suatu mesin yang khusus digunakan untuk melakukan monitoring seluruh segmen dari jaringan. IDS network-based akan mengumpulkan paket-paket data yang terdapat pada jaringan dan kemudian menganalisanya serta menentukan apakah paket-paket itu berupa suatu paket yang normal atau suatu serangan atau juga berupa aktivitas mencurigakan. Secara umum Network-Based IDS dijelaskan pada Figur 3

Figure 2. Host-Based IDS



Setelah memahami Host-based dan Network-based tentunya dapat dilihat perbedaan dari kedua jenis IDS tersebut. Perbedaan antara host-based dan network based IDS seperti tampak pada Tabel 1:

Tabel 1 Perbedaan Network-Based dan Host-Based

Network-Based IDS	Host-Based IDS
Ruang lingkup yang luas (mengamati semua aktivitas jaringan)	Ruang lingkup yang terbatas (mengamati hanya aktivitas pada host tertentu)
Lebih mudah melakukan setup	Setup yang kompleks
Lebih baik untuk mendeteksi serangan yang berasal dari luar jaringan	Lebih baik mendeteksi serangan yang berasal dari dalam jaringan
Lebih murah untuk diimplementasikan	Lebih mahal untuk diimplementasikan
Pendeteksian berdasarkan pada apa yang direkam dari aktivitas jaringan	Pendeteksian berdasarkan pada single host yang diamati semua aktivitasnya
Menguji packet headers	Packet headers tidak diperhatikan
Respons yang real time	Selalu merespon setelah apa yang terjadi
OS-Independent	OS-Spesific
Mendeteksi serangan terhadap jaringan serta payload untuk analisis	Mendeteksi serangan local sebelum mereka masuk ke jaringan
Mendeteksi usaha dari serangan yang gagal	Mencerifikasi sukses atau gagalnya suatu serangan

Sumber: Ariyus Doni. 2010 Intrusion Detection System

Snort

Snort adalah sebuah IDS dan IPS berbasis jaringan yang gratis dan berbasis *open source* yang diciptakan oleh martin roesch pada tahun 1998. Snort sekarang dikembangkan oleh Sourcefire dengan Roesch sebagai pendiri sekaligus CTO dari Source. Pada 2009, Snort ke jajaran *Hall of Frame* pada majalah *info Word* sebagai salah satu yang terbaik pada perangkat lunak berbasis *open source* sepanjang waktu.[3]

Snort sebagai IDS berbasis jaringan *open source* memiliki kemampuan untuk melakukan Analisa lalu lintas jaringan secara *real-time* dan pendapatan paket pada IP jaringan. Snort menjalankan analisa protocol, pencarian isi dan pencocokan isi.[4] Layanan dasar ini memiliki banyak tujuan termasuk *application-aware triggeredquality of service,* untuk tidak memprioritaskan lalu lintas masal ketika aplikasi yang sensitive terhadap *latency* sedang berjalan.

WhatsApp

WhatsApp adalah aplikasi pesan untuk smartphone dengan basic mirip BlackBerry Messenger. WhatsApp Messenger merupakan aplikasi pesan lintas platform yang memungkinkan kita bertukar pesan tanpa biaya SMS, karena WhatsApp Messenger menggunakan paket data internet yang sama untuk email, browsing web, dan lain-lain.[5] Aplikasi WhatsApp Messenger menggunakan koneksi 3G atau WiFi untuk komunikasi data. Dengan menggunakan WhatsApp, kita dapat melakukan obrolan online, berbagi file, bertukar foto dan lain-lain.

[3] Arikunto, S. (2012). Prosedur penelitian : suatu pendekatan praktik / Suharsimi Arikunto | OPAC Perpustakaan Nasional RI. In *Jakarta: Rineka Cipta*.

[4] Suryabrata, S. (2012). Suryabrata, Sumadi. *IUCN SSC Small Mammal Specialist Group*.

[5] Shalahudin dan Rosa. (2015). Rosa dan Shalahudin 2015. *Paradigma*, *19*(2).

Analisis Sistem

Beberapa kegiatan analisis yang dilakukan di antaranya : analisis masalah, analisis kebutuhan teknologi yang digunakan (*hardware* dan *software*), analisis rancangan sistem[6]. Kegiatan tersebut dilakukan melalui observasi, dan studi pustaka dalam hal yang berkaitan dengan *Early Warning System* Menggunakan *Whatsapp Notifikasi* dari *Intruision Detectin System Snort*.

Alat/Bahan Penelitian

Tahap ini dilakukan estimasi kebutuhan alat dan bahan yang digunakan meliputi antara lain:

Perangkat Keras

1. Komputer
   Laptop untuk media peng*input*an data & pengetesan serangan.
   Virtual Box sebagai perangkat virtual pengganti server sebenarnya.
2. Komponen bahan yang dibutuhkan
   a. Koneksi WIFI internet
   b. Adaptor Laptop
   c. *Smartphone* yang terinstall *whatsapp*

Perangkat Lunak

1. Sistem Operasi *Linux*.
2. *Library Guzzle php api client*.
3. PHP
4. *Mysql Server*
5. *Apache Web Server*

Bahan

Perancangan Sistem

Perancangan adalah proses multi langkah yang fokus pada desain pembuatan program perangkat termasuk alur sistem dan desain alat. Tahap ini mentranslasi kebutuhan perangkat dari tahap analisis kebutuhan ke representasi desain agar dapat diimplementasikan menjadi alat monitoring *intruision detection system snort* pada tahap selanjutnya. Desain perangkat yang dihasilkan pada tahap ini juga perlu didokumentasikan.

Pembuatan Kode Program

Fase ini dilakukan pembuatan kode program yang akan di*input* ke dalam perangkat perangkat virtual melalui *command line interface linux*. Tahap ini menghasilkan alat *monitoring intruision detection system snort* sesuai dengan desain yang telah dibuat pada tahap perancangan sistem.

Pengujian Sistem

Pengujian fokus pada perangkat secara dari segi lojik dan fungsional dan memastikan bahwa semua bagian sudah diuji. Hal ini dilakukan untuk meminimalisir kesalahan (*error*) dan memastikan

[6] Andrews, E. (2019). Who invented the internet. *History*, *28*, 1–2.

keluaran yang dihasilkan sesuai dengan yang di inginkan.

Pendukung (*support*) atau Pemeliharaan (*maintenance*)

Perangkat yang telah dibuat tidak menutup kemungkinan mengalami perubahan ketika sudah dikirimkan ke *user*. Perubahan bisa terjadi karena adanya kesalahan yang muncul dan tidak terdeteksi saat pengujian atau perangkat harus beradaptasi dengan lingkungan yang baru. Tahap pendukung atau pemeliharaan dapat mengulangi proses pengembangan mulai dari analisis spesifikasi untuk perubahan perangkat yang sudah ada, tapi tidak untuk membuat perangkat baru.

Model air terjun (*waterfall*) sangat cocok digunakan untuk kebutuhan pelanggan yang sudah sangat dipahami dan kemungkinan terjadinya perubahan kebutuhan selama pengembangan perangkat lunak kecil. Hal positif dari model air terjun (*waterfall*) adalah struktur tahap pengembangan sistem jelas, dokumentasi dihasilkan di setiap tahap pengembangan, dan sebuah tahap dijalankan setelah tahap sebelumnya selesai dijalankan.[7]

Metode ini digunakan karena merupakan suatu metode yang praktis dan cukup menghemat biaya karena semua parameter-parameter yang dibutuhkan serta hasil yang di inginkan dapat langsung dimodelkan dan disimulasikan dengan menggunakan suatu program komputer (*Personal Computer*) dalam bentuk perangkat lunak berbasis sistem pakar.[8]

KESIMPULAN

Kesimpulan yang dapat diambil dari penulisan Laporan penelitian ini adalah sebagai berikut: Perlunya monitoring system keamanan jaringan secara realtime. Perlunya notifikasi intrusion detection system yang efektif. Belum tersedianya notifikasi dari snort yang dikirimkan ke aplikasi whatsapp.

REFERENCES

Andrews, E. (2019). Who invented the internet. *History*, *28*, 1–2.

Arikunto, S. (2012). Prosedur penelitian : suatu pendekatan praktik / Suharsimi Arikunto | OPAC Perpustakaan Nasional RI. In *Jakarta: Rineka Cipta*.

Firdaus, M. (2010). Intrumen Penelitian. *Metodelogi Penelitian*.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? In *Future Internet* (Vol. 10, Issue 2). https://doi.org/10.3390/fi10020020

Koshechkin, K., Lebedev, G., Radzievsky, G., Seepold, R., & Martinez, N. M. (2021). Blockchain Technology Projects to Provide Telemedical Services: Systematic Review. *J Med Internet Res*, *23*(8), e17475. https://doi.org/10.2196/17475

Kusnandar, V. B. (2021). Pengguna internet indonesia peringkat ke-3 terbanyak di asia. *Diakses Pada*, *20*.

Shalahudin dan Rosa. (2015). Rosa dan Shalahudin 2015. *Paradigma*, *19*(2).

Suryabrata, S. (2012). Suryabrata, Sumadi. *IUCN SSC Small Mammal Specialist Group*.

[7] Kusnandar, V. B. (2021). Pengguna internet indonesia peringkat ke-3 terbanyak di asia. *Diakses Pada*, *20*.

[8] Firdaus, M. (2010). Intrumen Penelitian. *Metodelogi Penelitian*.