Jurnal Rekayasa Informasi

Vol. 11, No. 2, Oktober 2022

P-ISSN: 2252-7354, E-ISSN: 2685-8231

Diterbitkan Oleh :

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS SAINS DAN TEKNOLOGI INFORMASI
INSTITUT SAINS DAN TEKNOLOGI NASIONAL

Jl. Moh. Kahfi II, Bhumi Srengseng Indah, Jagakarsa, Jakarta Selatan 12640
Telp : (021) 7270090, Fax : (021) 7866955, Website : http://www.istn.ac.id
E-mail : sistem_informasi@istn.ac.id, prodisi.istn@gmail.com

SIMULASI SNORT SEBAGAI ALAT PENDETEKSI INTRUSI PADA *WEB DAMN VULNERABLE WEB APPLICATION*

I Gede Walid Bangga[1], Siti Madinah Ladjamuddin[2]
Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi
Institut Sains dan Teknologi Nasional
Jl. Moh. Kahfi II, Bhumi Srengseng Indah, Jagakarsa, Jakarta Selatan 12640
[1]gedebangga@gmail.com, [2] citymadinah07@istn.ac.id

ABSTRAKSI
Pada objek *Web Server*, faktor yang paling berpengaruh stabilitas dan validitas data. Hal ini disebabkan oleh beragamnya user yang mengakses *Web server* sehingga sulit untuk melakukan pengamanan apabila *Web server* tersebut tersedia untuk publik. Salah satu cara pengamanannya adalah menggunakan *Intrusion Detection System* agar dapat meminimalkan dampak yang diakibatkan oleh kegagalan sebuah *Web server* yang disebabkan oleh celah keamanan yang ada. Penerapan Sistem Deteksi Intrusi Berbasis Snort merupakan sistem keamanan yang biayanya cukup murah namun dapat diandalkan dalam mendeteksi serangan. Sistem IDS juga dapat diSimulasikan pada sistem operasi *Windows*. Pada sistem IDS serangan dapat terdeteksi atau tidak oleh Snort IDS Tergantung pada ada atau tidak adanya aturan yang yang dibuat oleh pengguna. Oleh karena itu, tujuan dari penelitian ini adalah untuk merancang serta membangun suatu sistem keamanan Web server untuk memantau jaringan secara *real-time.* Untuk mewujudkan hal tersebut, penulis menggunakan Comand Prompt sebagai media untuk memberikan alert jika ada serangan dan Snort sebagai alat *Intrusion Detection System (IDS)*. Pengujian sistem IDS dilakukan dengan beberapa skenario serangan untuk menguji kualitas Snort dalam mendeteksi serangan terhadap kualitas sistem keamanan suatu *Web server*. Berdasarkan hasil pengujian sistem Snort IDS dengan *ping*, XSS *Script*, dan SQL *Injection. Snort* bisa memberikan peringatan serangan terhadap keamanan pada sistem *Web server*. Hasil peringatan bisa digunakan sebagai referensi untuk menentukan kebijakan keamanan jaringan.
Kata Kunci : *: Security web, web server, intrution detection system,* snort

ABSTRACT
On the Web Server object, the most influential factor is the stability and validity of the data. This is due to the variety of users accessing the Web server, so that it makes difficult to secure the Web server when it is available to the public. One way of securing it is to use an Intrusion Detection System in order to minimize the impact caused by the failure of a Web server caused by existing security holes. The application of Snort-Based Intrusion Detection System is a security system that is quite inexpensive but reliable in detecting attacks. The IDS system can also be implemented on the Windows operating system. On the IDS system attacks, it can be detected or not by Snort IDS Depending on the presence or absence of rules created by the user. Therefore, the purpose of this research is to design and build a Web server security system to monitor the network in real-time. To achieve this, the author uses Command Prompt as a medium to provide alerts if there is an attack and Snort as an Intrusion Detection System (IDS) tool. Testing the IDS system was carried out with several attack scenarios to test the quality of Snort in detecting attacks on the quality of the security system of a Web server. Based on the results of testing the Snort IDS system with ping, XSS Script, and SQL Injection, Snort can provide security attack warnings on Web server systems. The warning results can be used as a reference to determine network securitypolicies.
Keywords : *Security web, web server, intrution detection system, snort*

1. PENDAHULUAN

Server Web adalah salah satu server yang paling sering mengalami serangan, baik berupa serangan ke Web platform, serangan ke Web application, serangan ke database, serangan ke Web client, dan serangan ketersediaan informasi pada suatu Website. Hasil ini juga didukung oleh data dari statistic insiden tahun 2016 yang dibuat oleh GOV-CSIRT (Goverment Computer Security Incident Response Team), khusus di Indonesia kasus Website defacement terhadap Website pemerintahan dengan domain .go.id terbilang cukup tinggi, yaitu pada statistik triwulan pertama di tahun 2016 serangan deface pada domain .go.id sebanyak 42% dan meningkat pada triwulan kedua dimana jumlah kasus defacement meningkat hingga 66.8%. Salah satu Serangan yang umum terjadi pada server Web adalah flood attack, dan SQL Injection. (Atmojo, 2018)

Perkembangan internet yang sedemikian pesat menjadikan keamanan suatu data atau informasi pada server yang terhubung dengan publik menjadi sangatlah penting untuk diperhatikan. Menurut Yusep, kerentanan terhadap serangan kejahatan lewat dunia maya di Indonesia masih terjadi. Pada 2012, jaringan internet negara mengalami lebih dari satu juta serangan. Serangan itu berupa pencurian data, pemalsuan data, pengubahan data (misalnya halaman muka situs Web), phising, pembocoran data, spionase industri, penyalahgunaan data oleh orang dalam, dan kejahatan lainnya. (Yudha & Panji, 2018)

Keamanan server web komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Keamanan sebuah server web dapat dikelompokkan menjadi dua bagian yaitu keamanan yang bersifat fisik dan bersifat non fisik.(Munawar et al., 2020)

Penulisan serupa tentang IDS Snort yaitu seperti yang dilakukan oleh AY Ananta menghasilkan bahwa IDS Snort sangat baik untuk mendeteksi adanya serangan ke dalam jaringan(Wijaya & Pratama, 2020). Kemudian penulisan yang dilakukan oleh Wijaya, bahwasanya IDS Snort mampu mendeteksi penyusupan ke dalam server(Ananta, 2017). Pengujian pada sistem IDS dilakukan dengan beberapa pola serangan untuk menguji kehandalan Snort dalam mendeteksi sebuah serangan terhadap sistem keamanan. Berdasarkan hasil pengujian sistem Snort IDS dengan Command injection/ping, SQL Injection, XSS Script, Snort dapat memberikan peringatan adanya serangan keamanan terhadap sistem jaringan.. Karena itu telah berkembang sistem IDS sebagai pembantu Pendeteksian pada server web. Dengan adanya IDS (Intrusion Detection System). Maka serangan-serangan tersebut lebih dapat dicegah. Intrusion Detection System berguna untuk mendeteksi adanya serangan dari penyusup.

Oleh sebab itu, penulis mengambil judul Tugas Akhir (TA) ini yaitu : "Simulasi Snort sebagai alat pendeteksi intrusi pada Web DVWA".

IDS (Instrusion Detectin System)

Intrusion Detection System adalah sebuah metode yang dapat digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi.(Fachri & Harahap, 2020)

Snort

Snort merupakan salah satu contoh program Network-based Intrusion Detection System, yaitu sebuah program yang dapat mendeteksi suatu usaha penyusupan pada suatu sistem jaringan komputer. Snort bersifat open source dengan lisensi GNU General Purpose License sehingga software ini dapat dipergunakan untuk mengamankan sistem server tanpa harus membayar biaya lisensi.

Rules dan Alert

Rules Snort atau Signature merupakan basis data yang berisi pola serangan. Rules inilah yang digunakan oleh Detection Engine untuk membandingkan lalu lintas jaringan

dengan rules yang ada, dengan begitu jika lalu lintas jaringan yang ada sesuai dengan rules maka hal itu dianggap dengan sebuah percobaan instrusi dan memberikan sebuah alert.

Komponen Snort

Snort mempunyai 4 komponen dasar yaitu :

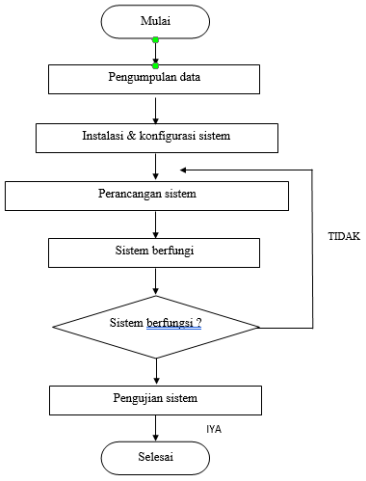
1. Packet Capture Engine : Komponen pertama adalah mesin penangkap paket yang mengambil lalu lintas menggunakan libpcap atau WinPcap (keduanya mulai sekarang akan secara kolektif disebut hanya sebagai "pcap"). Pcap adalah pustaka yang memungkinkan aplikasi menerima datagram, paket yang melaluinya data tingkat tautan (data pada tingkat dua dari model OSI tujuh lapis) dibawa. Kartu antarmuka jaringan (NIC) secara fisik menangkap lalu lintas jaringan dan meneruskannya ke driver yang berinteraksi dengan kernel OS. Setelah kernel memproses data, pcap kemudian mengambil data dari kernel dan meneruskannya ke aplikasi Snort, yang biasanya merupakan driver yang berinteraksi dengan komponen Snort ketiga, plug-in preprosesor.

2. Preprocessor Plug-Ins : Plug-in praprosesor Snort menguji dan memeriksa data paket yang mereka terima dari pcap, menentukan apa yang harus dilakukan dengan setiap paket apakah menganalisisnya, mengubahnya, menolaknya, dan/atau membuat peringatan karenanya. Plug-in praprosesor sangat menguntungkan karena mereka membentuk struktur untuk menangani paket sebelum dikirim ke komponen berikutnya. Praprosesor memodifikasi URI dan URL agar sesuai dengan format standar, menyediakan analisis stateful dari lalu lintas TCP/IP, mendeteksi portcans, mendekode paket RPC, mendekode paket telnet, serta melayani fungsi lainnya.

3. Detection Engine : Komponen utama ketiga adalah mesin pendeteksi. Paket pertama kali didekode dengan cara yang mendefinisikan struktur paket untuk protokol lapisan dua, dan kemudian lapisan tiga protokol, dan seterusnya. Ini memungkinkan mesin pendeteksi untuk membandingkan data secara sistematis dalam setiap paket yang diterimanya dengan opsi aturan. Mesin ini kemudian melakukan tes dasar pada bagian mana pun dari setiap paket yang berisi string atau nilai tertentu yang terkait dengan aturan, dan kemudian melakukan tes lain menggunakan aturan berikutnya, dan seterusnya sampai tes untuk semua aturan diketahui Snort tentang telah dilakukan. Setiap pertandingan adalah "hit." Mesin pendeteksi kemudian pindah ke paket berikutnya.

4. Output Plug-Ins : Komponen utama terakhir dari Snort adalah output plug-in, yang tujuan utamanya adalah untuk menghasilkan informasi yang akan ditampilkan kepada analis deteksi intrusi. Snort membuat peringatan berdasarkan aturan peringatan di dalam praprosesor, mesin dekode, dan mesin pendeteksi. Contoh output dari plug-in output muncul di bagian ?Snort Output.? Plug-in keluaran lainnya melakukan berbagai fungsi lain, seperti yang dibahas dalam catatan teknis berikut.(Dar & Harahap, 2018)

2. METODOLOGI PENELITIAN



Gambar 3.1 Diagram alur Sistem

Berikut penjelasan dari block diagram yang digunakan:

a. Metode pengumpulan data yang dipakai pada penelitian untuk menyusun aplikasi ini adalah studi literatur. Studi literatur adalah salah satu metode

pengumpulan data dengan cara membaca buku-buku dan jurnal sesuai dengan data yang dibutuhkan. Pada penelitian ini, dipilih studi literatur untuk mengumpulkan referensi dari jurnal-jurnal yang memiliki kemiripan dalam pembuatan sistem ini. Studi literatur digunakan sebagai pedoman pengetahuan dasar dalam melakukan perancangan, Simulasi dan pengujian dalam tahap-tahap proses pengerjaan sistem yang akan dibangun.

b. Instalasi dan Konfigurasi Sistem Pada tahap ini dilakukan instalasi Snort dan Web DVWA, serta melakukan konfigurasi pada masing-masing sistem agar dapat berfungsi dengan baik.

c. Perancangan pengembangan sistem dilakukan untuk meletakkan posisi Snort yang terhubung server Web yang sudah ada. Snort yang dirancang adalah sebagai server yang terhubung dengan server Web sehingga dapat mendeteksi serangan.

d. Pengujian Konfigurasi Sistem Pengujian dilakukan untuk mengetahui apakah sistem yang telah dikonfigurasi dapat berjalan sesuai perancangan.

e. Pengujian Sistem Pada tahap ini Snort yang telah di install dan konfigurasi pada server Web akan diuji dengan cara melakukan serangan terhadap server Web yang telah ditentukan apakah sudah berjalan dengan baik sesuai dengan yang direncanakan.

Instrument Penelitian

Adapun instrument yang dibutuhkan untuk mengsimulasikan IDS pada penelitian ini yaitu:

Perangkat keras

Adapun analis kebutuhan perangkat keras yang digunakan untuk melakukan penulisan ini adalah sebagai berikut:

Perangkat	Spesifikasi	Keterangan
Laptop	*Processor*: AMD A8-9400 Radeon R5, 5 *Compute Cores* 2C+3G(2CPUs)~2.4GHz 4 GB SDRAM, HDD 1 TB	2 unit
Router	ZTE ZXHN F609, Four RJ-45 *ports for Gigabit Ethernet interfaces, One* SC/APC *port for* GPON.	1 unit

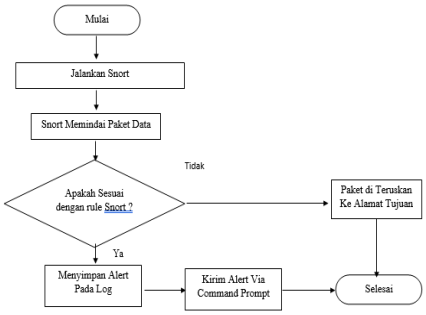
Gambar 3.2 Perangkat Keras

Perangkat Lunak

Adapun analis kebutuhan perangkat keras yang digunakan untuk melakukan penulisan ini adalah sebagai berikut:

Sistem	*Tools/framework*
IDS	Snort
Data Base	Xampp
Browser	*Mozila firefox, Web DVWA*
Text Editor	*Microsoft Visual Studio*

Gambar 3.3 Perangkat Lunak



Gambar 3.4 Alur Kerja Sistem

Gambar 3.4 Merupakan Alur Kerja Sistem. Dimulai dari paket data yang memasuki server web yang sudah di konfigurasi dalam snort. Paket data tersebut akan dibaca oleh snort engine untuk kemudian dicocokan dengan rules yang ada didalam rules snort. Jika paket data tersebut sesuai dengan rules snort, maka snort akan menganggap itu sebagai sebuah intrusi dan snort akan menyimpan alert tersebut ke file log. Namun jika paket data tersebut bukan merupakan intrusi, maka paket data tersebut akan diteruskan ke alamat tujuan nya

Rules Snort

Rules Snort yang digunakan adalah rules yang sudah tersedia dari pengembang SNORT itu sendiri, namun karena skenarionya sudah ditentukan, maka rules tersebut dispesifikkan untuk 3 buah serangan, serangan yang pertama adalah ping detected/Command injection, rules Snort yang digunakan disederhanakan menjadi seperti berikut :

alert icmp any any -> $HOME_NET any (msg:"Ping detected"; sid:1000001; rev:1; classtype:icmp-event;)

serangan yang kedua adalah SQL Injection, rules Snort yang digunakan disederhanakan menjadi seperti berikut :

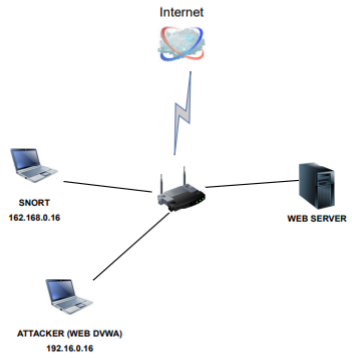
alert tcp any any -> $HOME_NET 80 (msg:"sql detected"; sid:1000002; rev:1; content:"%27")

serangan yang ketiga adalah xss script, rules Snort yang digunakan disederhanakan menjadi seperti berikut :

alert tcp any any -> $HOME_NET 80 (msg:"xss script detected"; sid:1000003; rev:1; content:"%3C")

3. HASIL DAN PEMBAHASAN

Pemodelan yang digunakan pada penelitian ini adalah model jaringan Client/Server. Pada model jaringan Client/Server diperlukan satu atau lebih komputer khusus yang disebut server untuk mengatur lalu lintas data informasi dalan jaringan computer. Komputer selain server disebut sebagai client. Server biasanya bersifat pasif, hanya menunggu berbagai permitaan dari client untuk kemudian melayani permintaan tersebut. Client biasanya bersifat aktif dan mengirim permintaan ke server serta menerima layanan dari server. Jaringan yang digunakan dalan penelitian ini adalah jaringan intranet.. Dengan skema seperti ditujukan pada gambar 4.1. Karena keterbatasan peralatan, maka penelitian hanya melakukan pengamatan terhadap web server, monitoring dilakukan pada komputer yang digunakan sebagai Snort sensor. Komputer server dan komputer client terhubung melalui switch/hub dalam subnet yang sama.



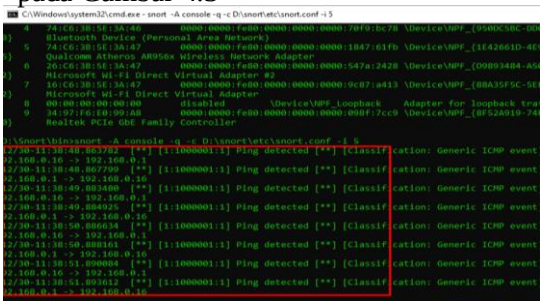
Gambar 4.1 Skema

Pengujian

Dalam pengujian kali ini penulis akan menggunakan 2 perangkat yang akan membantu untuk menyerang dan juga mendeteksi serangan yang sudah dipersiapkan. Snort ditempatkan dalam jaringan yang berfungsi mendeteksi serangan pada laptop yang akan dipantau. Dalam hal ini, Snort akan menyadap jenis intrusi atau serangan yang masuk dan keluar melalui sistem Snort. Jenis serangan yang terjadi untuk merusak/masuk ke suatu sistem dapat berupa banyak jenis, yang akan kita uji pada penelitian ini adalah 3 jenis serangan yaitu command injection/ping, XSS Script, dan SQL Injection. Setiap jenis serangan penulis akan menguji sebanyak 3 kali serangan dalam jangka waktu yang berbeda dan tidak terlalu berdekatan.

Pengujian Ping/command Injection

Ping bekerja dengan mengirimkan sebuah paket data yang disebut dengan Internet Control Message Protocol (ICMP) Echo Request. Paket ICMP ini biasanya digunakan untuk mengirimkan informasi tentang kondisi jaringan antara dua host (komputer). Mekanisme kerjanya yaitu ketika melakukan ping terhadap situs target (objek) maka akan tampil pada layar hasil respon berupa informasi nomor IP dari mana ping memperoleh Echo Reply, waktu (dalam milisekon) yang diperlukan program ping mendapatkan balasan dan yang terakhir adalah Time To Live (TTL). . Dalam skenario attacker mengakses alamat 192.168.0.1, kemudian attacker akan memasukan Default gateway yaitu 192.168.0.1 ke dalam text area. Maka hasil serangan nya akan menghasilkan alert pada Gambar 4.3

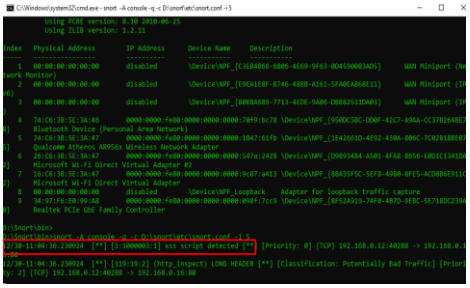


Gambar 4.3 Alert Command Injection

Pengujian XSS Script

Cross Site Scripting (XSS) merupakan salah satu jenis serangan injeksi code (code injection attack). XSS dilakukan oleh attacker dengan cara memasukkan kode HTML atau client script code lainnya ke suatu situs. Serangan ini akan seolah-olah datang dari situs tersebut. Dampak dari serangan ini jika tidak segera dideteksi antara lain: attacker dapat mem-bypass keamanan di sisi client, mendapatkan informasi sensitif, mendapatkan cookie dari user atau menyimpan aplikasi berbahaya.

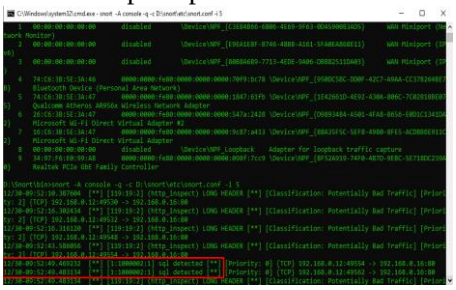
skenario serangan Cross Site Scripting (XSS) menggunakan web Damn Vulnerability Web Aplication (DVWA) yang sebelumnya telah dipersiapkan. Website tersebut ditanam di IP public dengan alamat 192.168.0.1. Dalam skenario attacker mengakses alamat 192.168.0.1, kemudian attacker akan memasukan script "<script>alert</script>" ke dalam text area. Maka hasil serangan nya akan menghasilkan alert pada Gambar 4.4.



Gambar 4.4 Alert XSS Script

Pengujian SQL Injection

SQL Injection merupakan sebuah teknik serangan yang memanfaatkan celah keamanan pada sisi website yang mengizinkanattacker untuk menginputkan malicious code. Celah keamanan tersebut ditunjukkan pada saat attacker memasukkan nilai string dan karakter-karakter control lainnya yang ada dalam instruksi SQL dengan cara memodifikasi perintah SQL yang ada di memori aplikasi client sehingga memungkinkan attacker untuk memasukkan kode-kode SQL untuk mendapatkan informasi dan akses ke database server. Dampak yang ditimbulkan jika serangan ini tidak segera terdeteksi adalah memungkinkan seorang attacker dapat login ke dalam sistem tanpa harus memiliki account. Selain itu, attackerjuga dapat mengubah, menghapus, maupun menambahkan data yang berada dalam database. skenario serangan SQL Injection yangdilakukan menggunakan web Damn Vulnerability Web Aplication (DVWA). Dalam percobaan, attacker akan memasukan sebuah Url dari website yang sebelumnya telah diketahui vulnerable terhadap serangan SQL Injection. Setelah URL website dimasukkan, kemudian attacker tinggal meng-click tombol submit untuk melakukan serangan. Dampak dari serangan ini, attacker bisa mendapatkan data-data penting dari website yang diserang. Adapunpada IDS Snort, (Gambar 4.5) akan muncul alerts pada command prompt.



Gambar 4.5 Alert SQL Injection

Pembahasan

Berdasarkan pada hasil dari ketiga serangan yang telah dilakukan , maka didapat data serangan yang ditunjukan oleh tabel 4.6

Jenis Serangan	Jumlah Serangan Yang Di tangkap	Waktu
Command *Injection*	1 Serangan	30 Desember 2021 11:38 WIB.
XSS *Script*	1 Serangan	30 Desember 2021 11:04 WIB
SQL *Injection*	1 Serangan	30 Desember 2021 09:52 WIB

Tabel 4.6 Menunjukan hasil serangan yang didapatkan dari ketiga metode serangan yang telah dilakukan dengan jumlah serangan masin-masing 1 kali serangan dengan rentang waktu yang berbeda, serangan Command injection terjadi pada 30 desember 2021 pada jam 11:38. Serangan XSS Script terjadi pada 30 Desember 2021 pada jam 11:04, dan serangan terakhir yaitu SQL Injection yang terjadi pada pukul 09:52. Berdasarkan hasil alert pada gambar 4.10, 4.12, 4.14 Semua serangan dapat dideteksi dengan baik oleh Snort.

4. SIMPULAN

Berdasarkan hasil dari penelitian "Simulasi Snort Sebagai Alat Pendeteksi Intrusi Pada Web DVWA" dapat disimpulkan sebagai berikut:

1. Snort dapat disimulasikan sebagai Intrusion Detection System pada sistem operasi Windows.
2. Snort dapat mendeteksi serangan berupa Ping, SQL Injection, dan XSS Script dengan baik
3. Bisa atau tidaknya sebuah serangan terdeteksi oleh Snort IDS tergantung berasal ada tidaknya rule yang dibuat dan bisa atau tidak rule tersebut ketika diterapkan di snort

Saran

Berdasarkan pengujian yang telah dilakukan terdapat beberapa rekomendasi dan saran untuk pengembangan penelitian selanjutnya, saran-saran tersebut adalah sebagai berikut :

1. Sistem keamanan dengan Snort IDS dapat memberikan keuntungan lebih ketika Snort terintegrasi dengan firewall. Meskipun Snort cukup efektif untuk mendeteksi serangan pada sistem.
2. Simulasikan snort pada website resmi, karena dapat membantu menghindari sejumlah serangan attacker seperti serangan SQL Injection yang dapat merusak sistem maupun melakukan pencurian data dari suatu sistem
3. Buat rules snort untuk mendeteksi jenis intrusi/serangan lain.

5. DAFTAR PUSTAKA

[1] Affandi, M., Program, S., Teknik, S., Stmik, I., Pradnya, P., Malang, P., Laksda, J., Sucipto, A., & 249-A Malang, N. (2013). Implementasi Snort Sebagai Alat Pendeteksi Intrusi Menggunakan Linux. *Jurnal Teknologi Informasi*, *4*(2). www.linux.org

[2] Ananta, A. Y. (2017). Seleksi Notifikasi Serangan Berbasis Ids Snort Menggunakan Metode K-Means. *SMARTICS Journal*, *3*(2), 31–37. https://doi.org/10.21067/smartics.v3i2.1954

[3] Atmojo, Y. P. (2018). Analisa Performa Raspberry Pi sebagai Intrusion Detection System: Studi Kasus IDS Pada Server Web. *Eksplora Informatika*, *8*(1), 24. https://doi.org/10.30864/eksplora.v8i1.143

[4] Azura, A., & Wildian, W. (2018). Rancang Bangun Sistem Absensi Mahasiswa Menggunakan Sensor RFID dengan Database MySQL XAMPP dan Interface Visual Basic. *Jurnal Fisika Unand*, *7*(2), 186–193. https://doi.org/10.25077/jfu.7.2.186-193.2018

[5] Dar, M. H., & Harahap, S. Z. (2018). Implementasi Snort Intrusion Detection System (Ids) Pada Sistem Jaringan Komputer. *Jurnal Informatika*, *6*(3), 14–23. https://doi.org/10.36987/informatika.v6i3.1619

[6] Fachri, B., & Harahap, F. H. (2020). Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer. *Jurnal Media Informatika Budidarma*, *4*(2), 413. https://doi.org/10.30865/mib.v4i2.2037

[7] Hasugian, P. S. (2018). Perancangan website sebagai media promosi dan informasi. *Journal Of Informatic Pelita Nusantara*, *3*(1), 82–86.

[8] Munawar, Z., Kom, M., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *Jurnal Sistem Informasi-J-SIKA*, *02*, 1–7.

[9] Panggabean, P. (2018). Analisis Network Security Snort Metode Intrusion Detection System Untuk Optimasi Keamanan Jaringan Komputer. *Jursima*, *6*(1), 1. https://doi.org/10.47024/js.v6i1.107

[10] Widodo, R., & Riadi, I. (2021). Intruder Detection Systems on Computer Networks Using Host Based Intrusion Detection System Techniques. *Buletin Ilmiah Sarjana Teknik Elektro*, *3*(1), 21. https://doi.org/10.12928/biste.v3i1.1752

[11] Wijaya, B., & Pratama, A. (2020). Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (Ids) Berbasis Snort. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *9*(1), 97–101. https://doi.org/10.32736/sisfokom.v9i1.770

[12] Yudha, F., & Panji, A. M. (2018). Perancangan Aplikasi Pengujian Celah Keamanan Pada Aplikasi Berbasis Web. *Cyber Security Dan Forensik Digital*, *1*(1), 1–6. https://doi.org/10.14421/csecurity.2018.1.1.1216 dengan TCP/IP. Bandung: Informatika