Jurnal Infortech
Volume 5 No. 2 Desember 2023
E-ISSN: 2715-8160

Simulasi Penerapan Sistem Monitoring Jaringan Snort NIDS Pada Web Server Menggunakan Metode SPDLC

Dewi Yuliandari[1], Walim[2], Bangkit Kharisma Raja[3], Rahayu Ningsih[4*], Ahmad Jurnaidi Wahidin[5]

[1,2,3,4,5] Universitas Bina Sarana Informatika
e-mail: [1]dewi.dwy@bsi.ac.id, [2]walim.wam@bsi.ac.id, [3]bangkitkr@gmail.com, [4]rahayu.ryh@bsi.ac.id, [5]ahmad.ajn@bsi.ac.id

Diterima	Direvisi	Disetujui
24-08-2023	06-11-2023	01-12-2023

Abstrak - Keamanan jaringan pada saat ini sangatlah diperlukan, terutama pada jaringan server. Server yang memiliki celah pada keamanannya dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Data-data pada server yang harusnya bersifat pribadi bisa saja disalahgunakan. Seorang administrator jaringan harus dapat memastikan bahwa sistem serta data yang ada di dalamnya benar-benar aman. Untuk meningkatkan keamanan tersebut dapat menggunakan sebuah sistem *Intrusion Detection System (IDS)*. Dalam penelitian ini, peneliti melakukan instalasi *Snort IDS* dan *ACID-BASE* di jaringan *localhost* menggunakan *Virtual Box* untuk menganalisis lalu lintas jaringan dan mendeteksi serangan keamanan. Metode yang digunakan adalah SPDLC (*Secure Policy Development Life Cycle*). Peneliti akan melakukan pengujian dengan serangan berupa mendeteksi sebuah Ping *Attack*, *SQL injection* dan *Port Scanning* ke server. Hasil pengujian menunjukkan bahwa *Snort* dan *ACID-BASE* dapat mendeteksi serangan dengan akurasi yang baik dan memberikan informasi yang cukup untuk mengambil tindakan yang diperlukan untuk melindungi jaringan dari serangan lebih lanjut. Selain itu, *Snort Base* juga memberikan informasi yang berguna untuk memantau kinerja jaringan dan menemukan masalah yang mungkin terjadi. Jadi hasilnya, *Snort Base* merupakan alat yang efektif untuk memantau dan memperingati adanya serangan keamanan pada jaringan. Penerapan *Snort Base* pada jaringan dapat membantu administrator jaringan untuk meningkatkan keamanan jaringan serta membantu meningkatkan kewaspadaan terhadap ancaman siber.

Kata Kunci: snort, ids, keamanan jaringan

Abstract - *Network security at this time is needed, especially on server networks. Servers that have loopholes in their security can be exploited by irresponsible parties. Data on the server that should be private can be misused. A network administrator must be able to ensure that the system and the data in it are completely safe. To increase security, you can use an Intrusion Detection System (IDS). In this study, the authors perform the installation of Snort IDS and ACID-BASE on the network localhost use virtual box to analyze network traffic and detect security attacks. The method used is SPDLC (Secure Policy Development Life Cycle). The author will test the attack in the form of detecting a Ping Attack, SQL injection and Port Scanning. The test results show that Snort and ACID-BASE can detect attacks with good accuracy and provide sufficient information to take necessary actions to protect the network from further attacks. Besides that, Snort Base also provides useful information for monitoring network performance and finding problems that may occur. In conclusion, Snort Base is an effective tool for monitoring and alerting network security attacks. Application Snort Base on the network can help network administrators to improve network security and help increase awareness of cyber threats*.

Keywords: *snort, ids, cyber security*

PENDAHULUAN

Berdasarkan laporan Badan Siber dan Sandi Negara, jumlah serangan siber di indonesia pada tahun 2022 tercatat sebanyak 976.429.996, dari jumlah tersebut 56,84% berupa serangan *Malware*, 14,75% *Information Leaks*, 10,9% *Trojan Activity*, dan 17,51% sisanya jenis serangan lainnya (Mathilda, 2023).

Minimnya sistem keamanan jaringan membuat hacker dapat dengan mudah mengambil alih sistem yang telah dibangun. Hal tersebut dapat menimbulkan permasalahan pada data dan informasi yang bersifat rahasia, termasuk data pribadi dan informasi penting bagi perusahaan ataupun lembaga yang seharusnya tidak diketahui pihak lain (Riadi dkk., 2020).

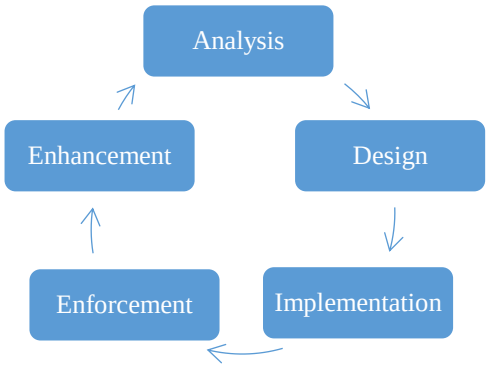
Sebuah website memiliki berbagai macam kerentanan. Kerentanan ini cukup berbahaya karena tidak semua informasi dapat ditampilkan secara terbuka (Ashar, 2022). Salah satu bentuk serangan pada sebuah *website* yang masih populer hingga saat ini adalah SQL Injection, jenis serangan ini melakukan penyisipan perintah *query* SQL ke dalam parameter *query* (Zebua dkk., 2022). Masalah lainnya dapat juga disebabkan karena tingginya frekuensi akses server oleh pengguna pada website sehingga menyebabkan server *down*, tentu hal tersebut dapat berdampak pada terbukanya celah keamanan pada *website* tersebut (Ariyadi dkk., 2023).

Oleh karena itu, untuk mengatasi permasalahan tersebut sangatlah diperlukan sistem keamanan jaringan terutama pada sebuah server yang selalu berinteraksi dengan pengguna. Keamanan informasi pada komputer dapat dibagi menjadi 3 area yakni pencegahan, deteksi dan respons. Area kedua dicakup ole sistem deteksi intrusi atau biasa disebut dengan *Intrusion Detection System*(IDS) (Riza, 2022). Penelitian yang dilakukan oleh (Hafiz dkk., 2020) menyimpulkan, dengan menggunakan IDS dapat mengurangi dampak buruk dari serangan yang terjadi.

Pada penelitian yang dilakukan oleh (Lukman & Suci, 2020) dengan judul "Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache" melakukan studi perbandingan antara *snort* dan *Suricata* dan menyimpulkan bahwa *snort* lebih unggul dalam hal fitur dan akurasi pendeteksian serangan. Penelitian lain juga dilakukan oleh (Pitriyanti dkk., 2023) dengan judul "*Prototype* Sistem Deteksi Serangan Pada Server Samsat Menggunakan *Intrusion Detection System*(IDS) Berbasis *Snort*" yang menggambarkan studi kasus tentang penggunaan *snort IDS* dalam melindungi server samsat. Penelitian lainnya dengan judul "Studi Analisa Serangan SQL Injection" menggunakan snort untuk studi analisa serangan *SQL Injection* (Nursapdahi dkk., 2022).

Berdasarkan latar belakang tersebut Sebagai Studi kasus dalam penelitian ini, peneliti akan menggunakan sebuah sampel web server brita.com sebagai server *victim* atau korban yang akan dilakukan penyerangan. *Snort* dan *BASE* akan diimplementasikan dalam lingkungan web server ini untuk memantau dan mendeteksi serangan yang mungkin dapat terjadi. Penelitian ini bertujuan untuk meningkatkan sistem keamanan jaringan dengan menerapkan snort IDS dan BASE serta untuk mengetahui seberapa akurat snort dalam melakukan pendeteksian serangan.

METODE PENELITIAN



Sumber: Hasil Penelitian (2023)

Gambar 1. Metode Pengembangan SPDLC

Metode penelitian yang digunakan adalah metode pengembangan *Secure Policy Development Life Cycle* (SPDLC) dengan studi pustaka, observasi dan eksperimental sebagai instrumen pengambilan data. Metode SPDLC merupakan suatu metode yang merumuskan rencana pembaharuan dalam suatu jaringan. Metode ini melibatkan serangkaian fase atau tahapan dalam siklus pengembangan sistem jaringan (Lukman & Suci, 2020). Beberapa langkah yang diterapkan pada studi ini melibatkan tahapan seperti *Analysis, Design, Implementation, Enforcement*, dan *Enhancement*.

1. Analysis: Tahapan ini mencakup pemahaman yang menyeluruh terkait analisis kebutuhan *hardware* maupun *software* dan analisis permasalahan yang terjadi pada web server.

2. Design: Tahapan ini yang akan dilakukan adalah membuat sebuah rancangan topologi jaringan. Hal ini bertujuan untuk membuat logika jaringan server sehingga mendapatkan gambaran dari sistem yang akan dibangun.

3. Implementation: Tahapan ini melakukan simulasi penerapan sistem dengan menggunakan *VirtualBox* berdasarkan desain yang telah dibuat sebelumnya. Proses implementasi meliputi instalasi dan konfigurasi *Operating System* (OS), *Snort IDS*, *barnyard2*, *PHP*, *PostgreSQL* dan *Basic Analysis and Security Engine (BASE)*

4. Enforcement: Tahapan ini dilakukan uji penetrasi terhadap sistem yang telah dibangun pada tahapan sebelumnya. Pengujian ini dilakukan dengan melakukan serangan kepada web server.

5. Enhancement: Tahapan terakhir ini adalah melakukan evaluasi hasil dari hasil uji penetrasi yang telah dilakukan, guna meninjau tingkat efektifitas terhadap sistem yang telah dibangun.

HASIL DAN PEMBAHASAN

1. *Analysis*

Setelah dilakukan analisis web server memiliki kerentanan terhadap *ping attack*, *port scanning* dan *SQL Injection*. Pada tabel 1 merupakan *software* yang akan digunakan untuk instalasi sistem IDS pada penelitian ini dan pada tabel 2 merupakan kebutuhan perangkat-perangkat apa saja yang akan dibutuhkan pada penerapan *Snort IDS* dan *BASE*.

Tabel 1. Kebutuhan *Snort IDS*

Sistem Operasi			
No	Nama	Versi	Keterangan
1	Debian Server	9	Sebagai server *Snort IDS* dan server *website* brita.com
2	Ubuntu Server	20.04 LTS	Sebagai server *website BASE*
3	Kali Linux	2022.3	Sebagai penyerang server
4	Windows Client	11	Sebagai administrator jaringan
Software			
No	Nama	Versi	Keterangan
1	Snort	2.9.7.0	Sebagai sistem IDS untuk menangkap trafik yang berpotensi serangan
2	Barnyard2	2.1.14	Digunakan untuk mengirimkan log ke dalam *database PostgreSQL*
3	PHP	5.6	Digunakan untuk mendukung fungsionalitas dari *website BASE*
4	PostgreSQL	12	Sebagai penyimpanan data *log snort* yang dikirimkan oleh *barnyard2*
5	BASE	1.4.5	Digunakan untuk menampilkan *log snort* dalam tampilan grafis berbasis *website*
Tools Penetrasi			
No	Nama		Keterangan
1	Nmap		Digunakan untuk melakukan *testing* serangan *port scanning*
2	SQLMap		Digunakan untuk melakukan *testing SQL Injection*

Sumber: Hasil Penelitian (2023)

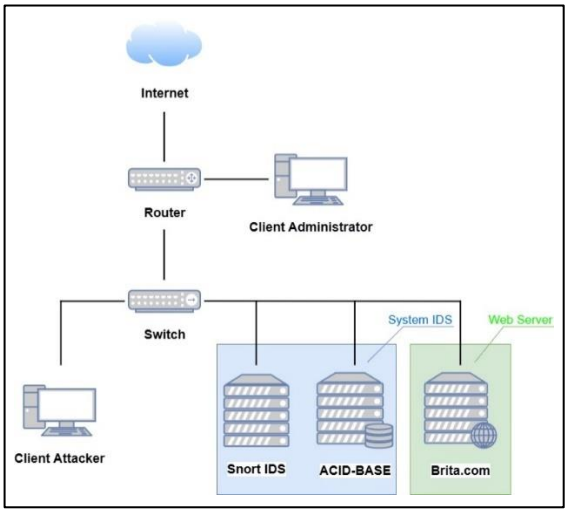
Tabel 2. Kebutuhan Perangkat

No	Komponen	Jumlah
1	Server	3
2	Router	1
3	Switch (VirtualBox)	1
3	PC Client	2

Sumber: Hasil Penelitian (2023)

2. *Design*

Pada tahapan desain ini peneliti membuat rancangan atau skenario desain topologi dari sistem jaringan yang akan dibangun berdasarkan analisis yang telah dilakukan pada tahapan sebelumnya yang meliputi *hardware* dan *software*. Gambaran desain topologi jaringan ditunjukkan pada gambar 2.



Sumber: Hasil Penelitian (2023)

Gambar 2. Desain Topologi Jaringan

Berdasarkan gambar 2 diatas dijelaskan *snort IDS* akan menangkap aktivitas mencurigakan dalam lalu lintas jaringan pada jaringan lokal server dan kemudian peringatan yang telah ditangkap oleh *snort* akan tersimpan pada *ACID-BASE* yang kemudian administrator dapat memantau nya kapan saja dan dimana saja. Selain itu pada tabel 3 merupakan konfigurasi *IP Address* yang akan digunakan pada penelitian ini.

Tabel 3. Konfigurasi *IP Address*

No	Komponen	IP Address
1	Router	192.168.1.1
2	PC Client (Administrator)	192.168.1.4
3	Switch (VirtualBox)	192.168.56.1
4	Server Snort	192.168.56.104
5	Web server (Korban)	192.168.56.105
6	PC Client (Attacker)	192.168.56.103
7	Server BASE	192.168.56.114

Sumber : Hasil Penelitian (2023)

3. Implementation

Pada tahapan ini dilakukan simulasi implementasi dengan menggunakan virtual mesin VirtualBox. Simulasi ini bertujuan untuk memperkecil resiko kegagalan pada saat proses membangun sistem IDS. Aktivitas yang dilakukan pada tahapan ini diantaranya sebagai berikut :

A. Implementasi dan Konfigurasi Snort

Implementasi dan konfigurasi *Snort IDS* dilakukan dengan melakukan instalasi *snort* sesuai dengan dokumentasi pada *website* snort, instalasi *barnyard2*, instalasi *PostgreSQL Client* dan melakukan penyesuaian konfigurasi pada *file snort.conf*, *local.rules*, dan *barnyard2.conf*. Pada gambar 3 merupakan konfigurasi *local rules snort* yang digunakan pada penelitian ini.

```
#Mendeteksi Ping Server
alert icmp any any -> $HOME_NET any (msg:"TES PING ICMP"; sid: 1000001;
classtype:not-suspicious; rev:1;)

#Mendeteksi SQL Injection
alert tcp any any -> any 80 (msg:"TERDETEKSI ERROR SQL INJECTION";
sid:1000002; classtype:web-application-attack; content:"%27"; rev:2;)
alert tcp any any -> any 80 (msg:"TERDETEKSI ERROR SQL INJECTION";
sid:1000003; classtype:web-application-attack; content:"%22"; rev:2;)
alert tcp any any -> any 80 (msg:"TERDETEKSI SQLMAP SCANNING";
sid:1000004; classtype:web-application-attack; content:"User-Agent|3A| sqlmap";
rev:2;)

#Mendeteksi PortScan NMap
alert icmp any any -> any any (msg:"Terdeteksi NMAP ping sweep Scan";
classtype:attempted-recon; dsize:0; sid:1000005; rev: 3;)
alert tcp any any -> any 22 (msg:"Terdeteksi NMAP TCP Scan";
classtype:attempted-recon; sid:1000006; rev:3;)
alert tcp any any -> any 22 (msg:"Terdeteksi Nmap XMAS Tree Scan";
classtype:attempted-recon; flags:FPU; sid:1000007; rev:3;)
alert tcp any any -> any 22 (msg:"Terdeteksi Nmap FIN Scan";
classtype:attempted-recon; flags:F; sid:1000008; rev:3;)
alert tcp any any -> any 22 (msg:"Terdeteksi Nmap NULL Scan";
classtype:attempted-recon; flags:0; sid:1000009; rev:3;)
```

Sumber: Hasil Penelitian (2023)

Gambar 3. Konfigurasi *Local Rules* pada *Snort*

B. Implementasi dan Konfigurasi BASE

Implementasi dan konfigurasi *BASE* dilakukan dengan melakukan instalasi *PHP*, instalasi *PostgreSQL Server*, instalasi *BASE* dan membuat *database snort* untuk menyimpan *log alert snort* serta mengisi langkah-langkah setup aplikasi BASE.

4. Enforcement

Pada tahap ini *Snort* dan *barnyard2* dijalankan dengan menggunakan perintah pada gambar 4 serta dilakukan pengujian penetrasi dengan menggunakan sistem operasi Kali Linux pada PC *Attacker*. Pengujian dilakukan untuk menguji apakah sudah bekerja aturan pendeteksian yang telah di tuliskan pada *local rules* sebelumnya.

```
#Untuk menjalankan Snort di latar belakang sistem
snort -D -u snort -g snort -q -c /etc/snort/snort.conf -i eth0

#Untuk menjalankan barnyard di latar belakang sistem
barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.u2 -w
/var/log/barnyard2/barnyard2.waldo -C
/etc/snort/classification.config

#Untuk menjalankan dan menampilkan alert pada terminal console
snort -A console -u snort -g snort -q -c /etc/snort/snort.conf -i eth0
```

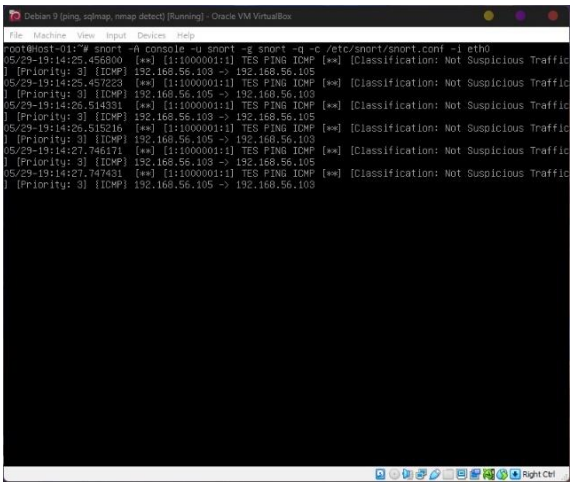
Sumber: Hasil Penelitian (2023)

Gambar 4. Perintah *running Snort* dan *Barnyard2*

Aktivitas yang dilakukan pada uji penetrasi ini melakukan *ping attack*, *port scanning*, *dan SQL Injection* berikut hasil yang dihasilkan:

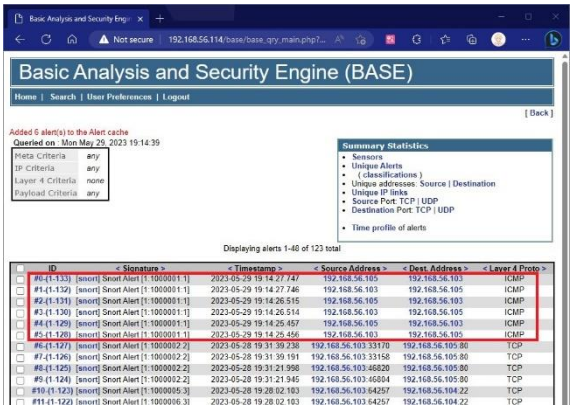
1) *Ping Attack*

Pada kasus serangan ini dilakukan pengujian dengan cara melakukan Ping ke server menggunakan *terminal console* pada komputer *attacker*. Pada gambar 5 merupakan hasil peringatan yang ditampilkan oleh *snort* dan pada gambar 6 juga menampilkan hasil *alert snort* oleh *BASE*.



Sumber: Hasil Penelitian (2023)

Gambar 5. *Alert* Ping *Attack* pada *Snort IDS*



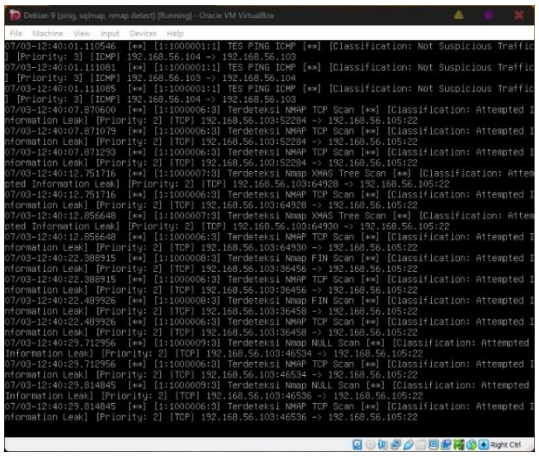
Sumber : Hasil Penelitian (2023)

Gambar 6. *Alert* Ping *Attack* pada *BASE*

2) Port Scanning

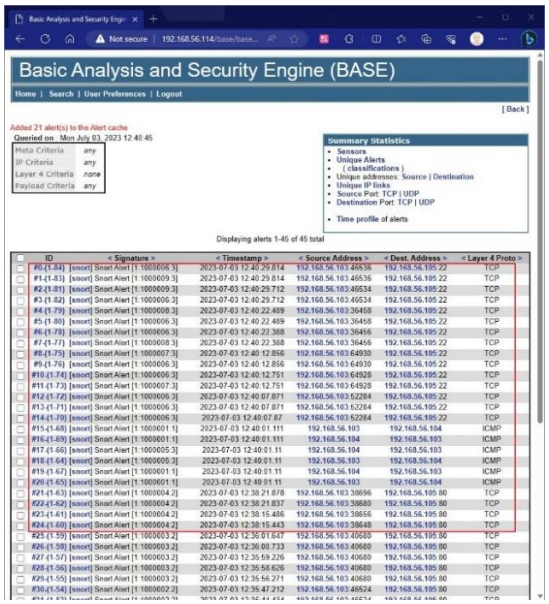
Pada kasus serangan *port scanning* dilakukan

pengujian dengan menggunakan *tools Nmap (Network Mapper)* pada komputer *attacker* dengan tujuan serangan ke server target yaitu web Brita.com. berikut hasil yang ditampilkan oleh *snort* dan *BASE* ditunjukkan pada gambar 6 dan gambar 7.



Sumber: Hasil Penelitian (2023)

Gambar 7. *Alert Port Scanning* pada *Snort IDS*

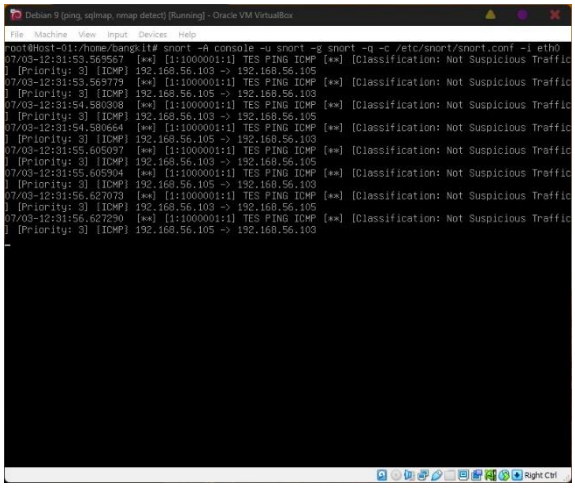


Sumber: Hasil Penelitian (2023)

Gambar 8. *Alert Port Scanning* pada *BASE*

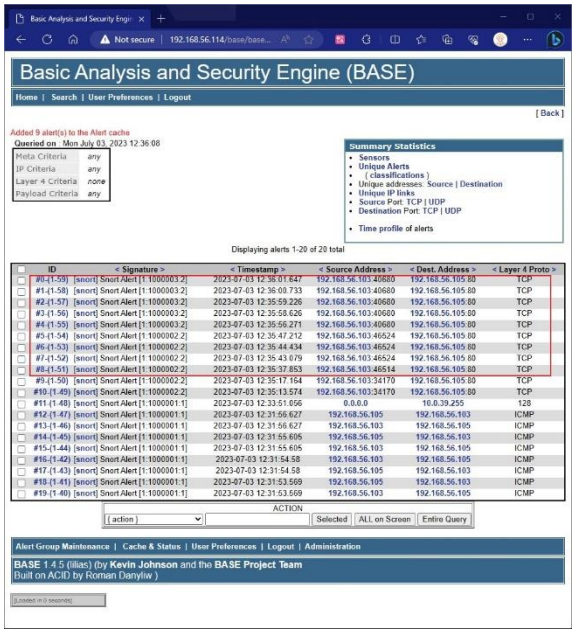
3) SQL Injectin

Pada kasus ini dilakukan pengujian dengan melakukan injeksi pada *form input* pada *website* korban hal ini biasanya digunakan untuk mengetahui jenis *database* yang digunakan pada sistem dan juga menggunakan *tools SQLMap* untuk melihat isi *file* pada *database* sehingga menimbulkan kebocoran data. pada gambar 8 dan 7 adalah hasil dari *alert snort* dan *BASE.*



Sumber: Hasil Penelitian (2023)

Gambar 9. *Alert SQL Injection* pada *Snort IDS*



Sumber: Hasil Penelitian (2023)

Gambar 10. *Alert SQL Injection* Pada *BASE*

Hasil dari pengujian penetrasi serangan server diatas dapat dirangkum pada tabel 4 dibawah ini.

Tabel 4. Evaluasi Hasil Pengujian Sistem IDS

No	Jenis Serangan	Tools	Hasil	Kesimpulan
1	Ping Attack	Terminal	Berhasil terdeteksi	Sistem dapat mendeteksi dengan akurat
2	Port Scanning	Nmap	Berhasil terdeteksi	Sistem dapat mendeteksi serangan hanya saja ada kemungkinan

				ping attack saat serangan melalui protokol ICMP
3	SQL Injection	SQLMAP	Berhasil terdeteksi	Sistem dapat mendeteksi dengan akurat

Sumber: Hasil Penelitian (2023)

5. Enhancement

Pada tahapan terakhir ini dilakukan sejumlah perbaikan dan peningkatan pada sistem IDS yang telah dibangun, beberapa aktivitas yang dilakukan pada fase ini antara lain:

1) Memperbaiki *rules* pendeteksian *snort IDS*.
2) menambahkan lebih banyak jumlah *rules* pada *snort*.

KESIMPULAN

Penerapan sistem Intrusion Detection System (IDS) yang bertujuan untuk meningkatkan keamanan dalam jaringan terhadap serangan-serangan sistem dapat dilakukan dengan baik oleh Snort IDS dan BASE. Berdasarkan hasil simulasi penerapan pada sistem lingkungan jaringan web server yang telah dilakukan, peneliti dapat menyimpulkan bahwa:

1. Sistem IDS yang telah dibangun dapat mendeteksi serangan dengan tingkat akurasi yang cukup akurat dan *real time*.
2. Serangan dapat terdeteksi tergantung pola serangan pada konfigurasi *rules* pada *snort IDS*. Oleh sebab itu, *rules* perlu di *update* secara rutin.
3. Aplikasi web BASE dapat memudahkan dalam melakukan analisis serangan.

Dari hasil penelitian ini, disarankan untuk menerapkan teknologi *firewall iptables* untuk memblokir serangan yang masuk ke dalam jaringan dan juga menerapkan sistem notifikasi pesan digital berbasis e-mail, SMS, telegram bot atau pesan digital lainnya.

REFERENSI

Ariyadi, T., Widodo, T. L., Apriyanti, N., & Kirana, F. S. (2023). Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP. *Techno.COM*, *22*(2), 418–429.

Ashar, R. (2022). Analisis Keamanan Open Website Menggunakan Metode OWASP dan ISSAF. *Jurnal Informasi dan Teknologi*, *4*(4), 187–194. https://doi.org/10.37034/jsisfotek.v4i4.233

Hafiz, A., Kurniawan, T., Sivi, N. A., Ikhsan, F. K., & Pratomo, P. A. (2020). Analisis Celah Keamanan Jaringan dan Server Menggunakan Snort Intrusion Detection System. *Jurnal Informasi Komputer*, *8*(2), 55–65. https://doi.org/https://doi.org/10.35959/jik.v8i2.185

Lukman, & Suci, M. (2020). Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache. *Jurnal Teknologi Informasi*, *15*(2), 6–15.

Mathilda, G. A. (2023, Januari 24). *BSSN Paparkan Serangan Keamanan Siber di Tahun 2022 Alami Penurunan Dibanding Tahun 2021*. https://www.cloudcomputing.id/berita/bssn-paparkan-serangan-siber-alami-penurunan.

Nursapdahi, Senja Fitrani, A., Alfan Rosid, M., & Aji, S. (2022). STUDI ANALISA SERANGAN SQL INJECTION. *Seminar Nasional Inovasi Teknologi*, 185–190.

Pitriyanti, M., Khairani Daulay, N., Satrianasyah, & Syamsul Arifin, M. A. (2023). Prototype Sistem Deteksi Serangan Pada Server Samsat Menggunakan Intrusion Detection System (IDS) Berbasis Snort. *Kajian Ilmiah Informatika dan Komputer*, *3*(4), 323–329. https://djournals.com/klik

Riadi, I., Yudhana, A., & W, Y. (2020). ANALISIS KEAMANAN WEBSITE OPEN JOURNAL SYSTEM MENGGUNAKAN METODE VULNERABILITY ASSESSMENT. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, *7*(4), 853–860. https://doi.org/10.25126/jtiik.202071928

Riza, F. (2022). Sistem Deteksi Intrusi pada Server secara Realtime Menggunakan Seleksi Fitur dan Firebase Cloud Messaging. *Jurnal Sistim Informasi dan Teknologi*, *5*(1), 7–15. https://doi.org/10.37034/jsisfotek.v5i1.161

Zebua, B., Herwanto, P., & Rosida. (2022). Penggunaan Encripsi MD5 Untuk Pencegahan SQL Injection Pada Aplikasi Berbasis Web. *Seminar Nasional : Inovasi dan Adopsi Teknologi*, 22–31.