DESAIN DAN IMPLEMENTASI INTRUSION DETECTION SYSTEM MENGGUNAKAN DEBIAN 7 DAN SNORT

Muhammad Aprianto
Informatika
aprianto@gmail.com

Abstrak

Keamanan pada server menjadi salah satu faktor penting yang harus diperhatikan dalam suatu jaringan komputer. Hampir seluruh informasi yang ada pada server dapat diakses oleh para penggunanya dari mana dan kapan saja. Keterbukaan akses tersebut memunculkan berbagai masalah baru antara lain adalah serangan DoS (Denial of Service) dan SQL Injection terhadap server maka dibuatlah sistem yang disebut IDS (Intrusion Detection System). Dengan adanya sistem ini diharapkan serangan tersebut dapat dideteksi lebih dini agar dapat segera di tanggulangi. Pada dasarnya IDS ini dibuat menggunakan debian 7 dan snort, merupakan sebuah sistem opensource yang digunakan untuk mendeteksi serangan-serangan pada jaringan komputer. Mekanisme pengujian dilakukan dengan cara penulis membuat sebuah sever lokal dengan domain www.aprianto.com, IP 192.168.100.1. Serangan yang akan diuji dengan IDS adalah serangan DoS dengan menggunakan LOIC (Low Orbit Ion Cannon) dan serangan SQL Injection dengan web DVWA (Damn Vulnerable Web Application) yang ada pada server lokal yang telah dibuat tadi. Dari pengujian yang telah dilakukan dapat disimpulkan bahwa IDS dengan debian 7 dan snort dapat mendeteksi serangan DoS dan SQL Injection dengan menampilkan alert (peringatan). Agar mempermudah analisis hasil serangan ditampilakan dalam bentuk presentase (%) dalam web BASE (Basic Analisys and Security Engine).

Kata Kunci: Debian 7, Snort, IDS, SQL Injection, DoS

PENDAHULUAN

Keamanan pada server merupakan salah satu faktor penting yang harus diperhatikan dalam suatu jaringan komputer. Hampir seluruh informasi yang ada pada suatu institusi atau organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintah maupun individiual (pribadi) dapat diakses oleh para penggunanya dari mana dan kapan saja (Budiman et al., 2021; Darwis, Solehah, et al., 2021; Deliyana et al., 2021; F. Kurniawan & Surahman, 2021; Pratiwi et al., 2022). Keterbukaan akses tersebut memunculkan berbagai masalah baru antara lain adalah pemeliharaan validitas dan integritas data atau informasi tersebut, jaminan ketersediaan informasi bagi pengguna yang berhak, pencegahan akses informasi dari yang tidak berhak serta pencegahan akses sistem dari yang tidak berhak, misalnya sistem tersebut adalah IDS (Anna et al., 2021; Rosmalasari et al., 2020; Rusliyawati et al., 2021; Sangha, 2022; Susanto, 2021). Intrusion Detection System (IDS) merupakan sebuah sistem yang digunakan untuk melakukan deteksi adanya usaha-usaha penyusupan terhadap sebuah

sistem dengan melakukan pengamatan trafik secara real-time (Alita et al., 2020; Borman et al., 2020; Yunita et al., 2022). Salah satu jenis IDS adalah Host-based Intrusion Detection System (HIDS) Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak (Andraini & Bella, 2022; Arrahman, 2022; Ferdiana, 2020; Jupriyadi, 2018). HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya firewall, web server, atau server yang terkoneksi ke Internet. Perangkat IDS yang sering digunakan pada sistem server adalah Snort. Snort merupakan sebuah aplikasi atau tool security berfungsi untuk mendeteksi intrusi-intrusi jaringan (penyusupan, penyerangan, pemindaian, dan beragam bentuk ancaman lainnya), sekaligus juga melakukan pencegahan (Allafi & Iqbal, 2018; Hijriyannto & Ulum, 2021; D. E. Kurniawan et al., 2019; Ratnasari et al., n.d.; Riskiono & Pasha, 2020). Keunggulan Snort adalah cepat dan mampu mendeteksi serangan pada server, mudah dikonfigurasi, dapat diguakan kedalam banyak sistem operasi dan snort bersifat open source / gratis.

Serangan SQL injection adalah kegiatan menyisipkan perintah SQL kepada suatu statement SQL yang ada pada aplikasi yang sedang berjalan (Prasetyo & Suharyanto, 2019). Dengan kata lain SQL injection ini merupakan suatu tehnik pengeksploitasi pada web apilikasi yang di dalamnya menggunakan database untuk penyimpanan datanya. Terjadinya SQL injection tersebut ikarenakan security atau keamanan pada level aplikasi (dalam hal ini aplikasi web) masih kurang sempurna (Jupriyadi et al., 2021);(Darwis, Pamungkas, et al., 2021);(Setiawan et al., 2022);(Dita et al., 2021). Sedangkan DoS (Denial of Service) itu sendiri adalah aktifitas yang menghambat kerja sebuah layanan (service) atau mematikan sehingga user yang berhak/berkepentingan tidak dapat menggunakan layanan tersebut. Dampak akhir dari aktifitas ini menjurus kepada tehambatnya aktifitas korban yang dapat berakibat sangat fatal (dalam kasus tertentu) (Novian et al., 2019; Samsugi et al., 2020; Wardany et al., 2021).

KAJIAN PUSTAKA

Intrusion Detection System

Intrusion Detection System (IDS) adalah sebuah sistem keamanan komputer yang dirancang untuk mendeteksi aktivitas tidak sah, mencurigakan, atau berbahaya pada jaringan atau sistem computer (Jincheng et al., 2021; Wahyono et al., 2021). IDS bekerja dengan menganalisis lalu lintas jaringan dan mencari pola-pola atau perilaku yang

mencurigakan atau tidak diizinkan dalam jaringan tersebut (Megawaty & Rahmanto, 2021; Rossi et al., 2021; Sri Indriani et al., 2020; V. Yasin et al., 2022). IDS adalah perangkat lunak, perangkat keras, atau kombinasi keduanya digunakan untuk mendeteksi aktivitas penyusup. Snort adalah IDS adalah *Open Source* yang tersedia untuk umum (Ahdan et al., 2019; Nani & Ali, 2020; Riskiono et al., 2021). IDS mungkin memiliki kemampuan yang berbeda tergantung pada seberapa kompleks dan canggih komponen adalah. Peralatan ids yang kombinasi *hardware* dan *software* tersedia dari banyak perusahaan. Seperti disebutkan sebelumnya, IDS dapat menggunakan tanda tangan, teknik berbasis anomali, atau keduanya.

Snort

Snort adalah salah satu jenis perangkat lunak IDS (Intrusion Detection System) yang open source dan gratis. Snort dirancang untuk memantau lalu lintas jaringan dan mendeteksi aktivitas yang mencurigakan atau berbahaya pada jaringan tersebut (Amarudin & Ulum, 2018; Oktaviani, 2021; Rumandan et al., 2022; I. Yasin & Shaskya, 2020). Merupakan sebuah aplikasi atau *tool security* berfungsi untuk mendeteksi intrusi-intrusi jaringan (penyusupan, penyerangan, pemindaian, dan beragam bentuk ancaman lainnya), sekaligus juga melakukan pencegahan. Keunggulan *Snort* adalah cepat dan mampu mendeteksi serangan pada server, mudah dikonfigurasi, dapat diguakan kedalam banyak sistem operasi dan *snort* bersifat *open source* / gratis. Snort juga memiliki plugin dan aturan yang dapat diunduh dari komunitas pengguna Snort, sehingga pengguna dapat memperluas kemampuan Snort sesuai dengan kebutuhan.

Debian

Debian adalah sistem operasi komputer yang tersusun dari paket-paket perangkat lunak yang dirilis sebagai perangkat lunak bebas dan terbuka dengan lisensi mayoritas GNU *General Public License* dan lisensi perangkat lunak bebas lainnya (Damayanti, 2019; *Aplikasi E-Marketplace Bagi Pengusaha Stainless Berbasis Mobile Di Wilayah Bandar Lampung*, 2021; Sari & Alita, 2022; Teknologi et al., 2021). Debian terkenal dengan sikap tegas pada filosofi dari *Unix* dan perangkat lunak bebas. Debian dapat digunakan pada beragam perangkat keras, mulai dari komputer jinjing dan *desktop* hingga telepon dan *server* (Alfiah & Damayanti, 2020; Bhakti et al., 2022; Nurkholis & Sitanggang, 2020; Qoniah & Priandika, 2020; Suaidah, 2021). Debian fokus pada kestabilan dan keamanan. Debian banyak digunakan sebagai basis dari banyak distribusi GNU/Linux lainnya (Melanda et al., 2023; Ramadhan et al., 2021; Surahman et al., 2020; Wiguna et al., 2019).

SQL Injection

SQL Injection adalah teknik serangan keamanan pada sebuah aplikasi web yang memanipulasi inputan pengguna ke dalam sebuah query SQL. Serangan ini dilakukan dengan cara memasukkan kode berbahaya (malicious code) pada inputan pengguna, yang nantinya akan dijalankan oleh database (Damayanti, 2021; Ismatullah & Adrian, 2021; Nugrahanto et al., 2021; Pasha & Susanti, 2022; Wantoro et al., 2021). Serangan SQL Injection dapat mengakibatkan kerusakan pada database dan kebocoran data sensitif. Kegiatan menyisipkan perintah SQL kepada suatu statement SQL yang ada pada aplikasi yang sedang berjalan. Dengan kata lain SQL injection ini merupakan suatu tehnik pengeksploitasi pada web apilikasi yang di dalamnya menggunakan database untuk penyimpanan datanya. Terjadinya *SQL injection* tersebut ikarenakan *security* atau keamanan pada level aplikasi (dalam hal ini aplikasi web) masih kurang sempurna.

Denial of Services (DoS)

Denial of Service (DoS) adalah serangan keamanan pada sebuah sistem atau jaringan yang bertujuan untuk mengganggu atau menonaktifkan aksesibilitas layanan yang disediakan. Serangan ini dilakukan dengan cara mengirimkan banyak permintaan ke sistem atau jaringan secara bersamaan, sehingga membebani sumber daya sistem dan menyebabkan kinerja yang buruk atau bahkan kegagalan total (Putra et al., 2022);(Putri, 2022);(Yuliza Putri, 2021). Salah satu contoh jenis serangan yang dapat mengganggu infrastruktur dari jaringan komputer, serangan jenis ini memiliki suatu pola khas, dimana setiap serangannya akan mengirimkan sejumlah paket data secara terus menerus kepada target serangannya. Dengan menggunakan metode deteksi anomali, serangan DoS dapat dideteksi dengan mengidentifikasi pola-pola anomali yang ditimbulkan. Untuk melindungi sistem atau jaringan dari serangan DoS, ada beberapa tindakan yang dapat dilakukan .

LOIC

LOIC (*Low Orbit Ion Cannon*) adalah salah satu alat untuk melakukan serangan DoS yang ampuh dan tersedia secara gratis. LOIC pada awalnya dikembangkan oleh perusahaan Praetox Technologies sebagai alat stress testing sebelum dirilis ke public (Tamara et al., 2021);(Satria & Haryadi, 2017);(Pratama et al., 2022). Alat ini dapat melakukan serangan DoS sederhana dengan mengirim paket data dalam jumlah banyak berupa paket UDP, TCP, atau permintaan HTTP ke target yang diserang. Keunggulan dari alat LOIC, selain dapat digunakan secara gratis, cara penggunaannya juga mudah.

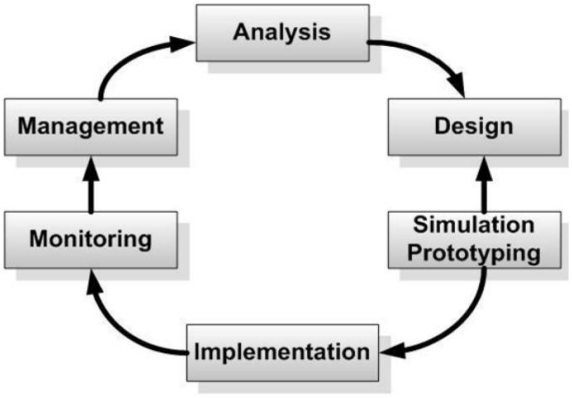
Namun LOIC memiliki kelemahan yaitu apabila menggunakan aplikasi ini akan sangat mudah untuk melacak penyerang, karena setiap melakukan penyerangan, IP dari penyerang tidak disamarkan dan terekspos ke pihak korban atau target.

WAP (Wireless Access Point) / AP (Access Point)

Wireless Access Point (WAP/AP) adalah alat yang digunakan untuk menghubungkan alat-alat dalam suatu jaringan, dari dan ke jaringan *WirelessRouter* dan *Acces Point* adalah dua fungsi peralatan jaringan yang bekerja bahu membahu membentuk unit pemancar signal wifi. *Access Point* membentuk *hotspot*, sedangkan Router mengatur lalu lintas data.Alat ini digunakan untuk *Access* Internet secara *wifi*. *WAP* beroperasi pada frekuensi radio tertentu dan menerima sinyal nirkabel dari perangkat nirkabel dalam jangkauan (Candra & Samsugi, 2021);(Ramadona et al., 2021). Kemudian, *WAP* mengirimkan sinyal tersebut melalui jaringan kabel ke router atau switch yang terhubung ke internet atau jaringan local (Setiawansyah et al., 2020).

METODE

Pada metode penelitian ini saya menggunakan metode NDLC (*Network Development Life Cycle*). NDLC merupakan model kunci dibalik proses perancangan jaringan komputer, NDLC merupakan model ang mendefinisikan siklus proses perancangan atau pengembangan suatu sistem jarigan komputer. seperti model pengembangan sistem jaringan komputer untuk sistem *software*, NDLC juga mempunyai elemen yang mendefinisikan *fase*, tahapan, langkah atau mekanisme proses spesifik, metode NDLC dapat dilihat pada gambar 1.



Gambar 1. *Network Development Life Cycle* (NDCL)

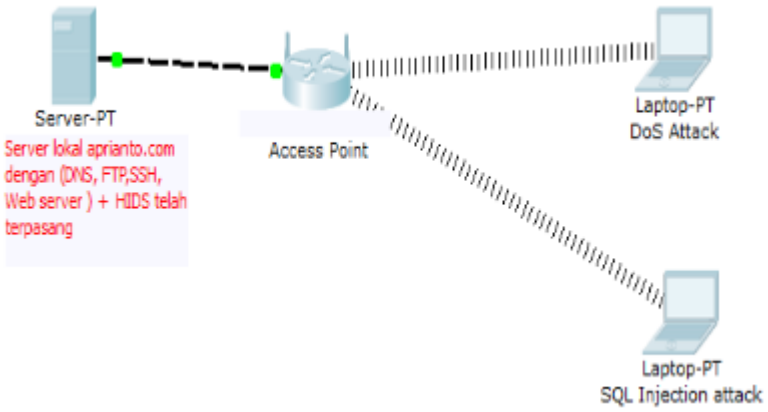
Keterangan :

Analysis

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan user, dan analisa topologi / jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya adalah wawancara, *survey* langsung ke lapangan, membaca manual atau *blueprint* dokumentasi, menelaah setiap data yang didapat dari data-data sebelumnya. Metode yang dilakukan pada laporan penelitian ini adalah membaca manual atau *blueprint* dokumentasi yaitu: Mencari, membaca, dan mengutip dari jurnal dan buku yang berkaitan dengan topik pembahasan.

Design

Dari data-data yang didapatkan sebelumnya, tahap *Design* ini akan membuat gambar *design topology* jaringan interkoneksi yang akan dibangun, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. *Design* bisa berupa *design* struktur *topology*, *design* akses data, design tata *layout* perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang *project* yang akan dibangun. Dalam mendisain topologi pada laporan penelitian ini menggunaka tools *packet tracer.*



Gambar 2. Topologi HIDS yang akan digunakan

Simulation Prototype

Beberapa *networker's* akan membuat dalam bentuk simulasi dengan bantuan *tools* khusus di bidang *network* seperti BOSON, PACKET TRACER, NETSIM, dan sebagainya, hal ini dimaksudkan untuk melihat kinerja awal dari *network* yang akan dibangun dan sebagai bahan presentasi dan *sharing* dengan *teamwork* lainnya. Namun karena keterbatasan perangkat lunak simulasi ini, banyak para *networker's* yang hanya menggunakan alat Bantu *tools* VISIO untuk membangun topologi yang akan didisain. Berikut adalah skenario yang akan dilakukan yaitu :

1. Membangun server lokal www.aprianto.com yang didalamnya terdapat beberapa layanan yang akan diuji coba yaitu : DNS server, Web Server, SSH Server, FTP Server, menggunakan OS Debian 7 yang diimplementasikan langsung ke dalam sebuah pc server.
2. Membangun sistem HIDS ke dalam Debian 7 yang telah dibuat diatas, menggunakan aplikasi *Open Source Snort* hingga dapat berjalan. Selanjutnya menginstall aplikasi monitoring hasil serangan yang ditimbulkan penyusup terhadap server menggunakan aplikasi web BASE *(Basic Analysis and Security Engine).* Selanjutnya menginstall aplikasi web DVWA (*Damn Vulnerable Web App)* digunakan untuk melakukan uji coba terhadap serangan *SQL Injection.*
3. Melakukan uji coba serangan DoS (*Denial of Service*) terhadap server.
4. Melakukan uji coba serangan *SQL Injection* terhadap server.

Implementation

Tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi *networker's* akan menerapkan semua yang telah direncanakan dan di *design* sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil / gagalnya *project* yang akan dibangun dan ditahap inilah *teamwork* akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis. Pada tahap ini saya mengimplementasikan pada sebuah pc.

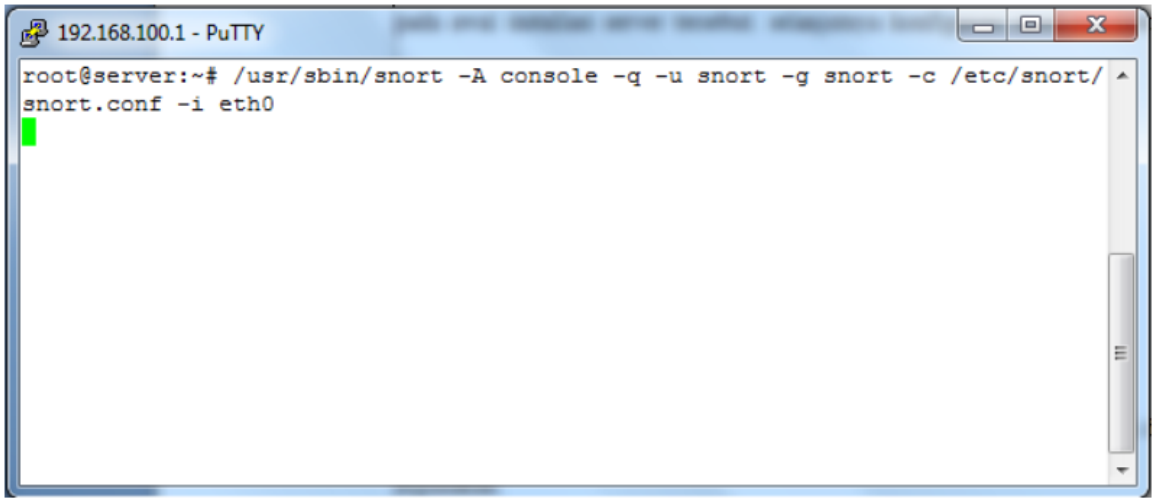
HASIL DAN PEMBAHASAN

Implementasi

Implementasi dari desain dan implementasi *Intrusion Detection System* menggunakan debian 7 dan snort dapat di lihat sebagi berikut :

Tampilan *running snort/IDS* pada debian 7

Desain fisik *running snort/IDS* dapat dilihat pada gambar 4 :



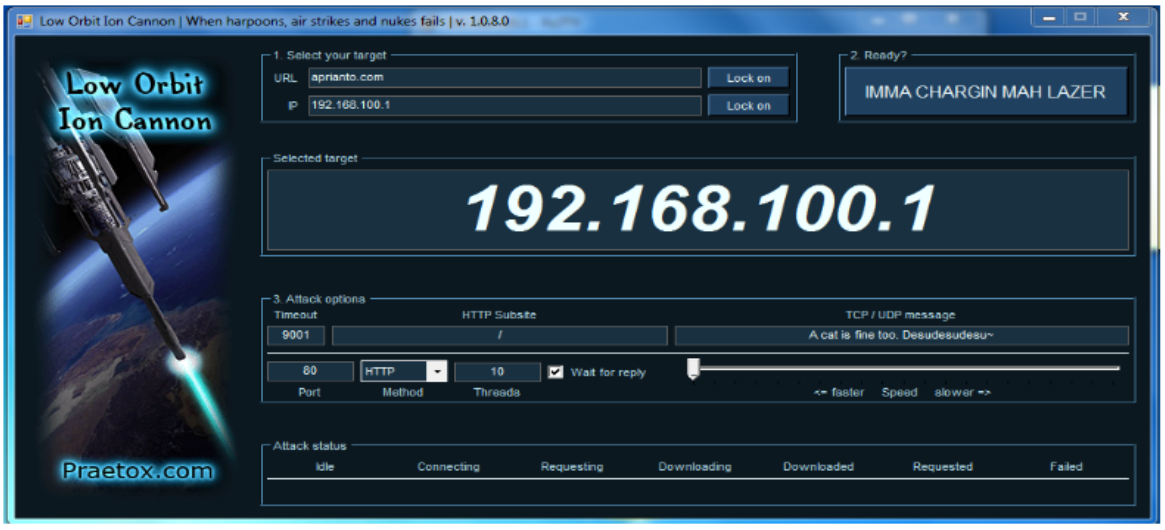
Gambar 4. Tampilan Running Snort/HIDS

Keterangan :

Ini adalah tampilan running snort/HIDS yang telah selesai dikonfigurasi dan siap digunakan.

Tampilan *Tools* Pengujian *DOS* pada server

Tampilan *Tools* Pengujian *DOS* pada server dapat dilihat pada gambar dibawah ini:



Gambar 5. Tampilan *LOIC*

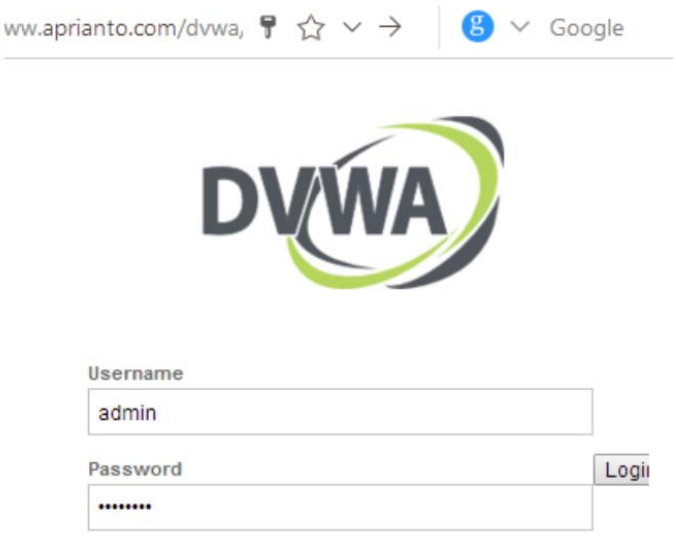
Keterangan :

Tampilan aplikasi *LOIC* yang digunakan untuk melakukan serangan *DOS*. Cara menyeting LOIC ini dengan cara memasukan alamat situs URL dan IP yang akan dilakukan DOS ke

server tersebut pada menu *select your target*, disini saya menggunakan alamat server ***aprianto.com*** yang telah saya buat dan konfigurasi diawal dan ip *address* dari server itu adalah 192.168.100.1. Selanjutnya pada *attack option* masukan *port* dan *method* yang digunakan untuk melakukan DOS, disini saya menggunakan port 80 dan method HTTP.

Tampilan *Form* Pengujian *Sql injection* pada server

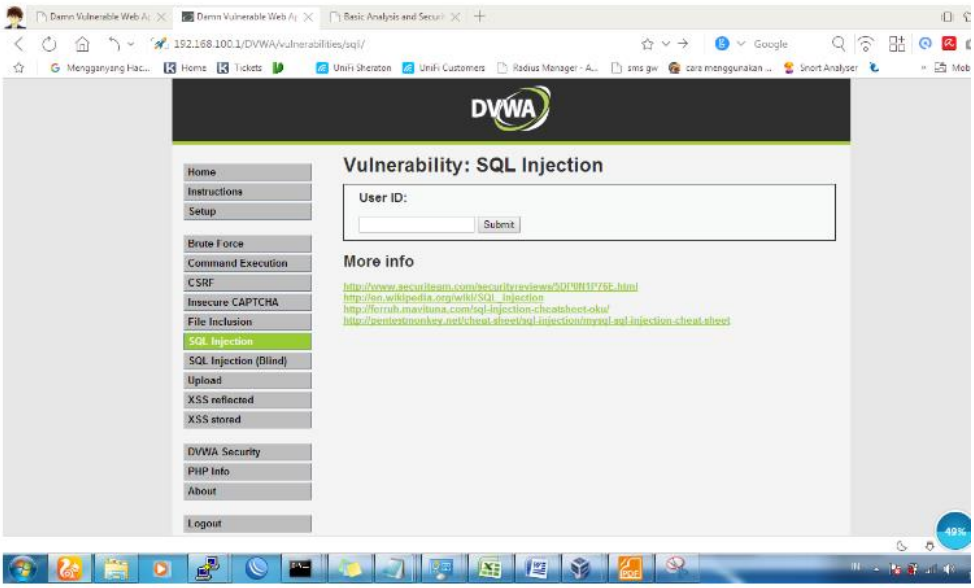
Tampilan web yang akan digunakan untuk pengujian dapat dilihat pada gambar 6 :



Gambar 6. *Form* login untuk DVWA

Tampilan Setelah login DVWA

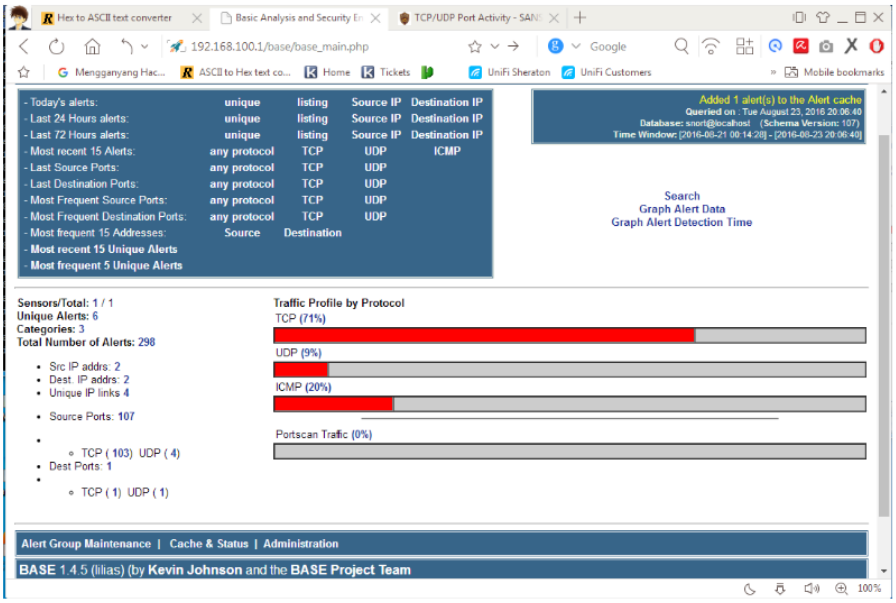
Tampilan setelah login ke web DVWA dapat dilihat pada gambar berikut ini:



Gambar 7. Tampilan setelah login ke web DVWA

Tampilan BASE hasil serangan yang dilakukan

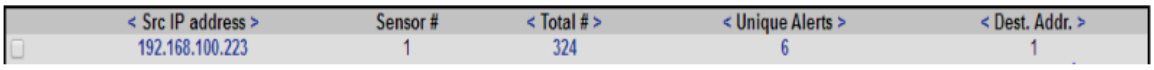
Tampilan web BASE ini digunakan untuk memonitoring hasil dari serangan yang telah dilakukan dapat dilihat pada gambar berikut :



Gambar 8. Tampilan web BASE

Blok penyerang dengan *Firewall*

Dengan hasil dari serangan tersebut terdapat data yang menampilan tentang alamat IP sumber dari si penyerang, dari data tersebut kita dapat melakukan bloking IP tersebut agar si penyerang tersebut tidak dapat terkoneksi dan melakukan serangan kembali dengan cara menggunakan *firewall*. Contoh IP penyerang adalah sebagai berikut :



Gambar 9. Tampilan IP *address* penyerang

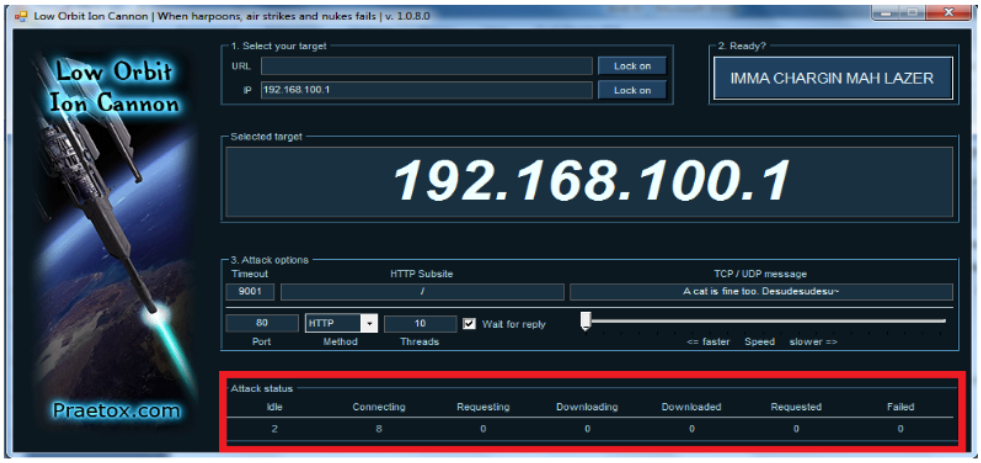
Selanjutnya kita masukan rule *firewall* untuk mematikan koneksi si penyerang dengan rule sebagai berikut :

```
iptables -A INPUT -s 192.168.100.223 -j DROP
```

Gambar 10. Tampilan rule *firewall*

Keterangan :

Apabila ada IP yang masuk ke jaringan server dengan IP 192.168.100.223 akan dilakuan *action DROP*.



Gambar 11. Tampilan LOIC setelah di *drop*

SIMPULAN

Adapun kesimpulan yang dihasilkan dari tahap pengujian diatas adalah sebagai berikut:

1. IDS yang dibuat dengan debian 7 dan snort dapat digunakan dalam mendeteksi serangan *DoS* (*Denial of Service*) yang diuji menggunakan aplikasi *LOIC* (*Low Orbit Ion Cannon*) dengan menggunakan 3 protokol yang ada dalam aplikasi LOIC yaitu metode TCP, UDP dan HTTP.
2. IDS yang dibuat dengan debian 7 dan snort dapat digunakan dalam mendeteksi serangan *SQL Injection* yang diujikan kepada webserver *DVWA (Damn Vulnerable Web Application)* dengan cara memasukan kode-kode unik dan perintah. Kode dan perintah yang terdeteksi diantaranya adalah *(', or, and, union, select, like, hostname, version,* dan *datadir*).
3. Hasil serangan tersebut berhasil ditampilkan dalam sebuah Web *BASE* (*Basic Analisys and Security Engine*) dalam bentuk persentase (%) agar mudah dianalisis dan ditanggulangi. Serangan dapat ditanggulangi dengan cara memblok IP penyerang menggunakan *firewall***.**

REFERENSI

Ahdan, S., Susanto, E. R., & Syambas, N. R. (2019). Proposed Design and Modeling of Smart Energy Dashboard System by Implementing IoT (Internet of Things) Based on Mobile Device. *2019 IEEE 13th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, 194–199.

Alfiah, A., & Damayanti, D. (2020). Aplikasi E-Marketplace Penjualan Hasil Panen Ikan Lele (Studi Kasus: Kabupaten Pringsewu Kecamatan Pagelaran). *Jurnal Teknologi*

Dan Sistem Informasi, *1*(1), 111–117. http://jim.teknokrat.ac.id/index.php/sisteminformasi

Alita, D., Tubagus, I., Rahmanto, Y., Styawati, S., & Nurkholis, A. (2020). Sistem Informasi Geografis Pemetaan Wilayah Kelayakan Tanam Tanaman Jagung Dan Singkong Pada Kabupaten Lampung Selatan. *Journal of Social Sciences and Technology for Community Service (JSSTCS)*, *1*(2).

Allafi, I., & Iqbal, T. (2018). Design and implementation of a low cost web server using ESP32 for real-time photovoltaic system monitoring. *2017 IEEE Electrical Power and Energy Conference, EPEC 2017*, *2017-Octob*, 1–5. https://doi.org/10.1109/EPEC.2017.8286184

Amarudin, A., & Ulum, F. (2018). Analisis Dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan Virtual Private Network (Vpn). *Jurnal Teknoinfo*, *12*(2), 72–75.

Andraini, L., & Bella, C. (2022). Pengelolaan Surat Menyurat Dengan Sistem Informasi (Studi Kasus : Kelurahan Gunung Terang). *Jurnal Portal Data*, *2*(1), 1–11. http://portaldata.org/index.php/portaldata/article/view/71

Anna, A., Nurmalasari, N., & Rohayani, Y. (2021). Penerapan Metode Waterfall Dalam Perancangan Sistem Informasi Akuntansi Pengiriman Barang. *Jurnal Sistem Informasi Akuntansi*, *1*(1), 85–93. https://doi.org/10.31294/justian.v1i1.279

Arrahman, R. (2022). Rancang Bangun Pintu Gerbang Otomatis Menggunakan Arduino Uno R3. *Jurnal Portal Data*, *2*(2), 1–14. http://portaldata.org/index.php/portaldata/article/view/78

Bhakti, F. K., Ahmad, I., Adrian, Q. J., Informasi, S., Teknik, F., & Indonesia, U. T. (2022). *PERANCANGAN USER EXPERIENCE APLIKASI PESAN ANTAR DALAM KOTA MENGGUNAKAN METODE DESIGN THINKING (STUDI KASUS : KOTA BANDAR LAMPUNG)*. *3*(2), 45–54.

Borman, R. I., Yasin, I., Darma, M. A. P., Ahmad, I., Fernando, Y., & Ambarwari, A. (2020). Pengembangan Dan Pendampingan Sistem Informasi Pengolahan Pendapatan Jasa Pada Pt. Dms Konsultan Bandar Lampung. *Journal of Social Sciences and*

Technology for Community Service (JSSTCS), *1*(2), 24–31. https://doi.org/10.33365/jsstcs.v1i2.849

Budiman, A., Ahdan, S., & Aziz, M. (2021). Analisis Celah Keamanan Aplikasi Web E-Learning Universitas Abc Dengan Vulnerability Assesment. *Jurnal Komputasi*, *9*(2), 1–10. https://jurnal.fmipa.unila.ac.id/komputasi/article/view/2800

Candra, A. M., & Samsugi, S. (2021). *Perancangan Dan Implementasi Controller Access Point System Manager (Capsman) Mikrotik Menggunakan Aplikasi Winbox*. *2*(2), 26–32.

Damayanti. (2021). Digitalisasi Sistem Peminjaman Buku Pada Smk Negeri 2 Kalianda Lampung Selatan. *Journal of Social …*, *2*(2), 128–138. https://ejurnal.teknokrat.ac.id/index.php/JSSTCS/article/view/1368

Damayanti, N. N. (2019). Sistem Informasi Manajemen Penggajian dan Penilaian Kinerja Pegawai pada SMK Taman Siswa Lampung. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, *6*(4).

Darwis, D., Pamungkas, N. B., & Wamiliana. (2021). Comparison of Least Significant Bit, Pixel Value Differencing, and Modulus Function on Steganography to Measure Image Quality, Storage Capacity, and Robustness. *Journal of Physics: Conference Series*, *1751*(1), 12039. https://doi.org/10.1088/1742-6596/1751/1/012039

Darwis, D., Solehah, N. Y., & Dartnono, D. (2021). PENERAPAN FRAMEWORK COBIT 5 UNTUK AUDIT TATA KELOLA KEAMANAN INFORMASI PADA KANTOR WILAYAH KEMENTERIAN AGAMA PROVINSI LAMPUNG. *TELEFORTECH: Journal of Telematics and Information Technology*, *1*(2), 38–45.

Deliyana, R., Permatasari, B., & Sukmasari, D. (2021). Pengaruh Persepsi Kemudahan, Persepsi Keamanan, Dan Persepsi Kepercayaan Terhadap Kepuasan Pelanggan Dalam Menggunakan Mobile Banking BCA. *Journal of Economic and Business Research*, *2*(2), 1–16.

Dita, P. E. S., Al Fahrezi, A., Prasetyawan, P., & Amarudin, A. (2021). Sistem Keamanan Pintu Menggunakan Sensor Sidik Jari Berbasis Mikrokontroller Arduino UNO R3.

Jurnal Teknik Dan Sistem Komputer, *2*(1), 121–135.

Aplikasi E-Marketplace Bagi Pengusaha Stainless Berbasis Mobile Di Wilayah Bandar Lampung, 2 Jurnal Teknologi dan Sistem Informasi (JTSI) 15 (2021). http://jim.teknokrat.ac.id/index.php/JTSI

Ferdiana, R. (2020). A Systematic Literature Review of Intrusion Detection System for Network Security: Research Trends, Datasets and Methods. *2020 4th International Conference on Informatics and Computational Sciences (ICICoS)*, 1–6.

Hijriyannto, B., & Ulum, F. (2021). Perbandingan Penerapan Metode Pengamanan Web Server Menggunakan Mod Evasive Dan Ddos Deflate Terhadap Serangan Slow Post. *Jecsit*, *1*(1), 88–92.

Ismatullah, H., & Adrian, Q. J. (2021). Implementasi Prototype Dalam Perancangan Sistem Informasi Ikatan Keluarga Alumni Santri Berbasis Web. *Jurnal Informatika Dan Rekayasa …*, *2*(2), 3–10. http://jim.teknokrat.ac.id/index.php/informatika/article/view/924

Jincheng, Z., Yanfei, L., Boyuan, Z., & Kai, W. (2021). Design and implementation of wearable oxygen saturation monitoring system. *2021 IEEE International Conference on Electrical Engineering and Mechatronics Technology, ICEEMT 2021*, 71–74. https://doi.org/10.1109/ICEEMT52412.2021.9601533

Jupriyadi, J. (2018). Implementasi Seleksi Fitur Menggunakan Algoritma Fvbrm Untuk Klasifikasi Serangan Pada Intrusion Detection System (Ids). *Prosiding Semnastek*.

Jupriyadi, J., Hijriyanto, B., & Ulum, F. (2021). Komparasi Mod Evasive dan DDoS Deflate Untuk Mitigasi Serangan Slow Post. *Techno. Com*, *20*(1), 59–68.

Kurniawan, D. E., Iqbal, M., Friadi, J., Borman, R. I., & Rinaldi, R. (2019). Smart monitoring Kurniawan, D. E., Iqbal, M., Friadi, J., Borman, R. I., & Rinaldi, R. (2019). Smart monitoring temperature and humidity of the room server using raspberry pi and whatsapp notifications. Journal of Physics: Conference Series, 1351(1), 1200. *Journal of Physics: Conference Series*, *1351*(1), 12006. https://doi.org/10.1088/1742-6596/1351/1/012006

Kurniawan, F., & Surahman, A. (2021). SISTEM KEAMANAN PADA PERLINTASAN KERETA API MENGUNAKAN SENSOR INFRARED BERBASIS MIKROKONTROLLER ARDUINO UNO. *Jurnal Teknologi Dan Sistem Tertanam*, *2*(1), 7–12.

Megawaty, D. A., & Rahmanto, Y. (2021). *Implementation of The Framework for The Application of System Thinking for School Financial Information Systems*. *1*, 1–10.

Melanda, D., Surahman, A., & Yulianti, T. (2023). Pengembangan Media Pembelajaran IPA Kelas IV Berbasis Web (Studi Kasus : SDN 02 Sumberejo). *Jurnal Teknologi Dan Sistem Informasi*, *4*(1), 28–33.

Nani, D. A., & Ali, S. (2020). Determinants of Effective E-Procurement System: Empirical Evidence from Indonesian Local GovernmeNani, D. A., & Ali, S. (2020). Determinants of Effective E-Procurement System: Empirical Evidence from Indonesian Local Governments. Jurnal Dinamika Akuntansi. *Jurnal Dinamika Akuntansi Dan Bisnis*, *7*(1), 33–50. https://doi.org/10.24815/jdab.v7i1.15671

Novian, D., Dwinanto, A., & Mulyanto, A. (2019). The Application of Cooperative Learning Methods in the Developing and Analyzing the Quality of An Educational Game. *Journal of Physics: Conference Series*, *1387*(1). https://doi.org/10.1088/1742-6596/1387/1/012122

Nugrahanto, I., Sungkono, S., & Khairuddin, M. (2021). *SOLAR CELL OTOMATIS DENGAN PENGATURAN DUAL AXIS TRACKING SYSTEM MENGGUNAKAN ARDUINO UNO*. *10*(1), 11–16.

Nurkholis, A., & Sitanggang, I. S. (2020). Optimization for prediction model of palm oil land suitability using spatial decision tree algorithm. *Jurnal Teknologi Dan Sistem Komputer*, *8*(3), 192–200. https://doi.org/10.14710/jtsiskom.2020.13657

Oktaviani, L. (2021). Penerapan Sistem Pembelajaran Dalam Jaringan Berbasis Web Pada Madrasah Aliyah Negeri 1 Pesawaran. *Jurnal WIDYA LAKSMI (Jurnal Pengabdian Kepada Masyarakat)*, *1*(2), 68–75.

Pasha, D., & Susanti, M. (2022). Perancangan Sistem Informasi Akuntansi Penjualan

Rumah Pada PT Graha Sentramulya. *Journal of Engineering and Information Technology for Community Service*, *1*(1), 10–15. https://doi.org/10.33365/jeit-cs.v1i1.128

Prasetyo, K., & Suharyanto, S. . (2019). Rancang Bangun Sistem Informasi Koperasi Berbasis Web Pada Koperasi Ikitama Jakarta. *Jurnal Teknik Komputer*, *5*(1), 119–126. https://doi.org/10.31294/jtk.v5i1.4967

Pratama, E. N., Suwarni, E., & Handayani, M. A. (2022). The Effect Of Job Satisfaction And Organizational Commitment On Turnover Intention With Person Organization Fit As Moderator Variable. *Atm*, *6*(1), 74–82.

Pratiwi, D., Putri, N. U., & Sinia, R. O. (2022). *Peningkatan Penegathuan Smart Home dan Penerapan keamanan Pintu Otomatis*. *3*(3).

Putra, R. A. M., Putra, A. D., & Wahono, E. P. (2022). Analisis Rembesan Terhadap Bahaya Piping pada Bendungan Way Sekampung. *Serambi Engineering*, *VII*(3), 3454–3465.

Putri, R. H. (2022). Pengaruh Kebijakan Subsidi, Foreign Direct Investment (Fdi) Dan Tata Kelola Pemerintahan Terhadap Pertumbuhan Ekonomi (Studi Kasus Negara – Negara Di Asean). *REVENUE: Jurnal Manajemen Bisnis Islam*, *3*(1), 129–144. https://doi.org/10.24042/revenue.v3i1.11621

Qoniah, I., & Priandika, A. T. (2020). ANALISIS MARKET BASKET UNTUK MENENTUKAN ASOSSIASI RULE DENGAN ALGORITMA APRIORI (STUDI KASUS: TB. MENARA). *Jurnal Teknologi Dan Sistem Informasi*, *1*(2), 26–33.

Ramadhan, A. F., Putra, A. D., & Surahman, A. (2021). APLIKASI PENGENALAN PERANGKAT KERAS KOMPUTER BERBASIS ANDROID MENGGUNAKAN AUGMENTED REALITY (AR). *Jurnal Teknologi Dan Sistem Informasi*, *2*(2), 24–31.

Ramadona, S., Diono, M., Susantok, M., & Ahdan, S. (2021). Indoor location tracking pegawai berbasis Android menggunakan algoritma k-nearest neighbor. *JITEL (Jurnal Ilmiah Telekomunikasi, Elektronika, Dan Listrik Tenaga)*, *1*(1), 51–58.

https://doi.org/10.35313/jitel.v1.i1.2021.51-58

Ratnasari, T. D., Samsugi, S., Kom, S., & Eng, M. (n.d.). *SETUP MIKROTIK SEBAGAI GATEWAY SERVER PADA SMK PELITA GEDONGTATAAN*.

Riskiono, S. D., Oktaviani, L., & Sari, F. M. (2021). IMPLEMENTATION OF THE SCHOOL SOLAR PANEL SYSTEM TO SUPPORT THE AVAILABILITY OF ELECTRICITY SUPPLY AT SDN 4 MESUJI TIMUR. *IJISCS (International Journal of Information System and Computer Science)*, *5*(1), 34–41.

Riskiono, S. D., & Pasha, D. (2020). Analisis Perbandingan Server Load Balancing dengan Haproxy & Nginx dalam Mendukung Kinerja Server E-Learning. *InComTech: Jurnal Telekomunikasi Dan Komputer*, *10*(3), 135–144.

Rosmalasari, T. D., Lestari, M. A., Dewantoro, F., & Russel, E. (2020). Pengembangan E-Marketing Sebagai Sistem Informasi Layanan Pelanggan Pada Mega Florist Bandar Lampung. *Journal of Social Sciences and Technology for Community Service (JSSTCS)*, *1*(1), 27. https://doi.org/10.33365/jta.v1i1.671

Rossi, F., Sembiring, J. P., Jayadi, A., Putri, N. U., & Nugroho, P. (2021). Implementation of Fuzzy Logic in PLC for Three-Story Elevator Control System. *2021 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE)*, 179–185.

Rumandan, R. J., Nuraini, R., Sadikin, N., & Rahmanto, Y. (2022). *Klasifikasi Citra Jenis Daun Berkhasiat Obat Menggunakan Algoritma Jaringan Syaraf Tiruan Extreme Learning Machine*. *4*(1). https://doi.org/10.47065/josyc.v4i1.2586

Rusliyawati, R., Putri, T. M. M., & Darwis, D. D. (2021). Penerapan Metode Garis Lurus dalam Sistem Informasi Akuntansi Perhitungan Penyusutan Aktiva Tetap pada PO Puspa Jaya. *Jurnal Ilmiah Sistem Informasi Akuntansi*, *1*(1), 1–13. http://jim.teknokrat.ac.id/index.php/jimasia/article/view/864

Samsugi, S., Yusuf, A. I., & Trisnawati, F. (2020). Sistem Pengaman Pintu Otomatis Dengan Mikrokontroler Arduino Dan Module Rf Remote. *Jurnal Ilmiah Mahasiswa Kendali Dan Listrik*, *1*(1), 1–6. https://doi.org/10.33365/jimel.v1i1.188

Sangha, Z. K. (2022). *PENERAPAN SISTEM INFORMASI PROFIL BERBASIS WEB DI DESA BANDARSARI*. *3*(1), 29–37.

Sari, A., & Alita, D. (2022). Penerapan E-Marketing Menggunakan Model Oohdm Dan Strategi Marketing 7P (Studi Kasus : Sudden Inc). *Jurnal Teknologi Dan Sistem Informasi*, *3*(4), 80–85.

Satria, M. N. D., & Haryadi, S. (2017). Effect of the content store size to the performance of named data networking: Case study on Palapa Ring topology. *Proceeding of 2017 11th International Conference on Telecommunication Systems Services and Applications, TSSA 2017*, *2018-Janua*, 1–5. https://doi.org/10.1109/TSSA.2017.8272911

Setiawan, A., Prastowo, A. T., Darwis, D., Indonesia, U. T., Ratu, L., & Lampung, B. (2022). Sistem Monitoring Keberadaan Posisi Mobil Menggunkan Smartphone. *Jurnal Teknik Dan Sistem Komputer*, *3*(1), 35–44.

Setiawansyah, S., Sulistiani, H., & Saputra, V. H. (2020). Penerapan Codeigniter Dalam Pengembangan Sistem Pembelajaran Dalam Jaringan Di SMK 7 Bandar Lampung. *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer Dan Teknologi Informasi*, *6*(2), 89–95.

Sri Indriani, E., Qurthobi, A., Darmawan, D., & Fisika, T. (2020). *Perancangan Kontrol Suhu Larutan Nutrisi Pada Sistem Hidroponik Menggunakan Kontrol Logika Fuzzy; Studi Kasus Selada Keriting (Lactuca Sativa L.) Design of Nutrition Temperature Control on Hydroponics System Using Fuzzy Logic Control; Case Study Curly Lat*. *7*(1), 1274–1280.

Suaidah, S. (2021). Teknologi Pengendali Perangkat Elektronik Menggunakan Sensor Suara. *Jurnal Teknologi Dan Sistem Tertanam*, *02*(02). https://ejurnal.teknokrat.ac.id/index.php/jtst/article/view/1341

Surahman, A., Octaviansyah, A. F., & Darwis, D. (2020). Ekstraksi Data Produk E-Marketplace Sebagai Strategi Pengolahan Segmentasi Pasar Menggunakan Web Crawler. *SISTEMASI: Jurnal Sistem Informasi*, *9*(1), 73–81.

Susanto, E. R. (2021). Sistem Informasi Geografis (GIS) Tempat Wisata di Kabupaten Tanggamus. *Jurnal Teknologi Dan Sistem Informasi*, *2*(3), 125–135.

Tamara, T., Dwi Utomo, S., Setiawan, K., Yuliadi, E., Jurusan Agroteknologi, M., Pertanian Universitas Lampung, F., Jurusan Agroteknologi, D., Soemantri Brodjonegoro No, J., & Lampung, B. (2021). PERBANDINGAN PERTUMBUHAN DAN PRODUKSI UBIKAYU (Manihot esculenta Crantz) DI LAHAN TANJUNG BINTANG AKIBAT PEMBERIAN PUPUK MIKRO COMPARISON OF GROWTH AND PRODUCTION OF GARBAGE (Manihot esculenta Crantz) IN TANJUNG BINTANG LAND DUE TO MICRO FERTILIZER. *Journal of Tropical Upland Resources ISSN*, *03*(02), 91–100.

Teknologi, J., Jtsi, I., Saputra, M. A., Isnain, A. R., Informasi, S., Teknik, F., & Indonesia, U. T. (2021). *PENERAPAN SMART VILLAGE DALAM PENINGKATAN PELAYANAN MASYARAKAT MENGGUNAKAN METODE WEB ENGINEERING (Studi Kasus : Desa Sukanegeri Jaya)*. *2*(3), 49–55.

Wahyono, Wibowo, M. E., Ashari, A., & Putra, M. P. K. (2021). Improvement of Deep Learning-based Human Detection using Dynamic Thresholding for Intelligent Surveillance System. *International Journal of Advanced Computer Science and Applications*, *12*(10), 472–477. https://doi.org/10.14569/IJACSA.2021.0121053

Wantoro, A., Samsugi, S., & Suharyanto, M. J. (2021). Sistem Monitoring Perawatan dan Perbaikan Fasilitas PT PLN (Studi Kasus : Kota Metro Lampung). *Jurnal TEKNO KOMPAK*, *15*(1), 116–130.

Wardany, K., Pamungkas, M. P., Sari, R. P., & Mariana, E. (2021). Sosialisasi Dasar Teknik Instalasi Listrik Rumah Tangga di Kelurahan Kecamatan Trimurjo. *Sasambo: Jurnal Abdimas (Journal of Community Service)*, *3*(2), 41–48. https://doi.org/10.36312/sasambo.v3i2.394

Wiguna, P. D. A., Swastika, I. P. A., & Satwika, I. P. (2019). Rancang Bangun Aplikasi Point of Sales Distro Management System dengan Menggunakan Framework React Native. *Jurnal Nasional Teknologi Dan Sistem Informasi*, *4*(3), 149–159. https://doi.org/10.25077/teknosi.v4i3.2018.149-159

Yasin, I., & Shaskya, Q. I. (2020). Sistem Media Pembelajaran Ips Sub Mata Pelajaran Ekonomi Dalam Jaringan Pada Siswa Mts Guppi Natar Sebagai Penunjang Proses Pembelajaran. *Jurnal Teknologi Dan Sistem Informasi*, *1*(1), 31–38. https://doi.org/10.33365/jtsi.v1i1.96

Yasin, V., Peniarsih, P., Gozali, A., & Junaedi, I. (2022). Application of expert system diagnosis of color blindness with ishihara method with microsoft vb 6.0. *International Journal of Informatics, Economics, Management and Science*, *1*(1), 13. https://doi.org/10.52362/ijiems.v1i1.678

Yuliza Putri, N. D. P. (2021). *PERANAN E-LEARNING PEMBELAJARAN MATEMATIKA DI SEKOLAH DASAR*. *2*(2), 44–49.

Yunita, L., Isnain, A. R., & Dellia, P. (2022). *Analisis Perancangan Sistem Informasi Akuntansi Pencatatan Dan Pengelolaan Keuangan Pada Yayasan Panti Asuhan Harapan Karomah*. *2*(2), 62–68.