JREEC
JOURNAL RENEWABLE ENERGY ELECTRONICS AND CONTROL
homepage URL : https://ejurnal.itats.ac.id/jreec

SISTEM DETEKSI KEAMANAN JARINGAN PADA SERVER DAPODIK DI SMPN I MUARA KELINGI TERHADAP SERANGAN SNIFFING

Resha Purnama Sari1, Asep Toyib Hidayat2, Phito Prima Sanjaya3, Anisya Apriliana4

Universitas Bina Insan1,2,3,4

INFORMASI ARTIKEL

Jurnal JREEC – Volume 03 Nomer 01, Juni 2023

Halaman:
57-65
Tanggal Terbit :
06 Juni 2023

DOI:
10.31284/j.JREEC.2023.v31i.4552

EMAIL

1902010007@mhs.univbinainsan.ac.id 1
Asep_toyib_hidayat@univbinainsan.ac.id 2
phitosanjaya12@gmail.com 3
anisyaapriliana24@gmail.com 4

PENERBIT

Jurusan Teknik Elektro-ITATS
Alamat:
Jl. Arief Rachman Hakim No.100,Surabaya 60117,
Telp/Fax: 031-5997244

ABSTRACT

Information technology (IT) has been applied to various sectors, including industry, government, education and health. However, technological sophistication is also accompanied by threats in terms of data security. For this reason, a system is needed that can secure the data, where attacks on data often occur from networks connected to the internet. The world of education today is also very dependent on technological sophistication, especially in data storage. One that utilizes this technology is SMPN I Muara Kelingi. The problem currently faced is the lack of a data security system on the Dapodik Server at SMPN I Muara Kelingi. The attack that can attack the network is in the form of a sniffing attack. The purpose of making this system is so that the data or information contained in the system cannot be accessed by unauthorized persons and to prevent damage to the system. By using the Security Policy Development Life Cycle (SPDLC) and using Snort as a tool to detect packet sniffing attacks, the school can quickly detect attacks that occur on the school Dapodik Server.

Kata kunci: *Network Security, SPDLC, Snort, Dapodik Server, Sniffing.*

ABSTRAK

Teknologi informasi (IT) telah diterapkan pada berbagai sektor, baik industri, pemerintahan, pendidikan dan kesehatan. Namun kecanggihan teknologi juga di sertai dengan ancama-ancaman dari segi keamanan datanya. Untuk itu diperlukan sebuah sistem yang dapat mengamankan data tersebut, dimana penyerangan terhadap data sering terjadi dari jaringan yang terhubung ke internet. Dunia pendidikan saat ini juga sangat bergantung dengan kecanggihan teknologi terutama dalam penyimpanan data. Salah satu yang memanfaatkan teknolgi ini adalah SMPN I Muara Kelingi. Permasalahan yang dihadapi saat ini adalah kurangnya sistem pengamanan data pada Server Dapodik SMPN I Muara Kelingi. Serangan yang dapat menyerang jaringan tersebut berupa serangan Sniffing. Tujuannya dibuatnya sistem ini adalah agar data atau informasi yang ada dalam sistem tidak dapat diakses oleh orang yang tidak berkepentingan serta untuk mencegah tindakan pengerusakan terhadap sistem tersebut. Dengan menggunakan Security Policy Development Life Cycle (SPDLC) serta menggunakan Snort sebagai alat untuk mendeteksi serangan packet sniffing maka pihak sekolah dapat mendeteksi dengan cepat serangan yang terjadi pada Server Dapodik sekolah.

Kata kunci: *Keamanan Jaringan, SPDLC, Snort, Server Dapodik, Sniffing..*

PENDAHULUAN

Seiring dengan kemajuan teknologi informasi (IT) yang telah banyak diterapan oleh hampir semua kalangan munculah permasalahan tentang keamanan dari sistem IT, agar data atau informasi yang ada didalam sistem tidak bisa diakses oelh orang yang tidak berkepentingan, dan bagai mana agar sistem tersebut terhindar dari tindakan pengerusakan[1]. Berbagai Isu keamanan jaringan saat ini menjadi sangat penting dan patut untuk diperhatikan. Sebuah jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para hacker, baik jaringan wired LAN maupun wireless LAN. Pada saat proses pengiriman data akan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menyadap atau mengubah data tersebut. SMPN I Muara Kelingi adalah sebuah sekolah menengah pertama yang berada di ibukota Kecamatan Muara Kelingi, dalam pendataan pokok sekolah, SMPN I Muara Kelingi harus menggunakan layanan dapodik. Layanan Dapodik adalah suatu sistem pendataan yang dikelola oleh Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi yang memuat data sekolah, peserta didik, pendidik dan tenaga kependidikan, dan substansi pendidikan yang datanya bersumber dari sekolah, tentunya sebagai data pokok sekolah yang dilaporkan ada berbagai data yang bersifat rahasia yang harus diamankan.

Permasalahan yang timbul di layanan Dapodik SMPN I Muara Kelingi adalah belum adanya pengamanan terhadap serangan serta penyusupan yang kapanpun dapat terjadi dalam jaringan dan dapat merugikan pihak sekolah, sebagai contoh serangan Sniffing[2]. Serangan Sniffing adalah teknik pemantauan setiap paket yang melintasi jaringan, dan bagian dari perangkat lunak atau perangkat keras yang memonitor semua lalu lintas jaringan. Potensi bahaya packet sniffing adalah hilangnya prifasi, dan tercurinya informasi penting dan rahasia yang dimiliki oleh user. Untuk mengatasi permasalah tersebut maka dibutuhkan sebuah sistem yang dapat mendeteksi serangan packet sniffing pada jaringan layanan Dapodik SMPN I Muara Kelingi sebagai pencegahan dari serangan pihak yang tidak bertanggung jawab serta pengamanan jaringan berbasis IDS (Intrusion Detection System) menggunakan Snort sebagai alat untuk mendeteksi serangan packet sniffing tersebut. Tujuannya dibuatnya sistem keamanan ini adalah upaya pengamanan server dapodik terhadap serangan sniffing dari pihak yang tidak bertanggung jawab dan Mempermudah pihak SMPN I Muara Kelingi untuk mendeteksi serangan *sniffing* pada jaringan layanan dapodik.

TINJAUAN PUSTAKA

Intrusion Detection System (IDS)

Intrusion Detection System adalah perangkat lunak atau perangkat keras yang dirancang untuk mendeteksi aktifitas berbahaya baik dalam hal serangan terhadap suatu sistem maupun terhadap suatu jaringan komputer. IDS dapat melakukan inspeksi terhadap lalu lintas jaringan inbound dan outbound dalam suatu jaringan[3]. Ketika menemukan serangan, maka akan memberikan peringatan apakah aktifitas tersebut termasuk berbahaya atau tidak berdasarkan beberapa level, yaitu low, medium, high, dan serious. IDS juga dapat didefinisikan sebagai tool, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan komputer. Aplikasiyang digunakan untuk melakukan penyerangan ke komputer server dalam penelitian ini adalah aplikasi Loic (Low Orbit Ion cannon). Loic (Low Orbit Ion)merupakan sebuah tool atau aplikasi yang berfungsi untuk melumpuhkan server sebuah situs website dengan mengirimkan packet sebanyak mungkin sesuai dengan kemauan si penyerang ke komputer server yang dituju melalui domain atau ip server komputer target.

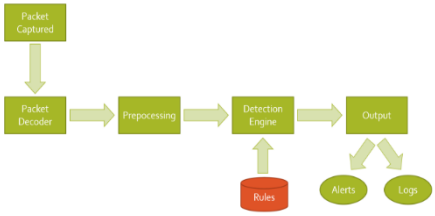
Snort

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu dapat menganalisis lalu lintas real-time, hal ini dapat mendeteksi berbagai jenis serangan. Snort bukanlah sebatas protocol analisis atau sistem pendeteksi penyusupan (Intrusion Detection System) IDS, melainkan sedikit gabungan diantara keduanya, dan bisa sangat berguna dalam merespons insiden-insiden peyerangan terhadap hosthost jaringan[4]. Fitur Snort dapat menjadi penolong administrator sistem dan jaringan, dimana mampu memperingatkan kita atas penyusup yang berpeluang berbahaya. Snort adalah perangkat Intrusion Detection System, bukan Intrusion Prevention System yang dapat

mecegah adanya suatu serangan. Snort hanya dapat memberikan suatu peringatan tentang adanya sebuah serangan terhadap suatu sistem, sehingga untuk dapat melakukan pencegahan terhadap sebuah serangan harus dilakukan[5]. Snort merupakan sebuah perangkat lunak yang berfungsi untuk mengamati aktifitas dalam suatu jaringan komputer. Komponen pada Snort terdiri dari beberapa bagian yaitu:

1. *Packet Decoder*
   Berfungsi untuk mengekstrak paket dari jaringan dalam bentuk file berformat 'tcpdump' dan mengirimkan paket ke preprocessor.
2. *Preprocessor*
   Berfungsi untuk memodifikasi paket yang rusak menggunakan beberapa operasi dan kemudian mengirimkan ulang ke Detection Engine.
3. *Detection Engine*
   Berfungsi untuk mendeteksi ancaman aktivitas yang ada dalam paket dengan menggunakan snort rules.
4. *Logging and Alerting System*
   Berfungsi untuk menghasilkan alarm atau log aktivitas intrusi yang terdeteksi oleh Detection Engine.
5. *Output Modules*
   Berfungsi untuk menyimpan output yang dihasilkan oleh *Logging and Alerting System*.
   Ada beberapa mode yang dilakukan oleh Snort antara lain:
   1) *Packet Sniffer* – Membaca paket dari network kemudian menampilkan dalam bentuk *continuous stream di console screen*
   2) *Packet Logger* – Mencatat semua paket yang lewat di jaringan untuk dianalisa di kemudian hari
   3) *Intrusion Detection Mode* – Pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini di perlukan *setup* dari berbagai *rules* / aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan.

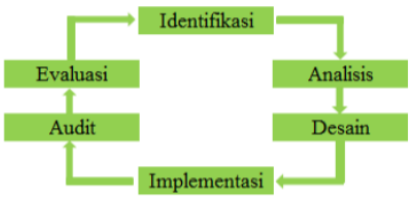
   Alur *IDS* menggunakan *SNORT* dapat dilihat pada gamabr 1 dibawa ini:



Gambar 1. Alur IDS Menggunakan SNORT

SPDLC (*Security Policy Development Life Cycle)*

Security Policy Development Life Cycle (SPDLC) adalah sebuah metode pengembangan sistem yang berfokus pada keamanan jaringan. Gambaran dari metode Security Policy Development Life Cycle dapat dilihat pada gambar 2 dibawah ini :



Gambar 2. Metode *Security Policy Development Life Cycle*

Berikut penjelasan dari tahap-tahap yang dilakukan dalam metode *Security Policy Development Life Cycle* (SPDLC) :

a. Identifikasi
   Tahap awal ini dilakukan untuk menemukan berbagai macam masalah keamanan yang dihadapi oleh jaringan pada saat ini dan bagaimana sistem yang sedang berjalan di perusahaan
b. Analisis
   Dari data yang didapatkan pada tahap identifikasi, dilakukan proses analisis kebutuhan user.
c. Desain
   Tahap desain ini akan membuat suatu gambar rancangan topologi sistem keamanan yang akan dibangun, alur sistem autentikasi serta menjelaskan kebutuhan sistem baik software maupun hardware.
d. Implementasi
   Pada tahap ini dilakukan penerapan dari hasil perancangan yang telah dilakukan pada tahap sebelumnya. Namun, karena keterbatasan izin dari perusahaan dalam melakukan implementasi, hasil perancangan akan disimulasikan dalam jaringan yang lebih kecil[6]. Dimulai dengan instalasi perangkat dan mengkonfigurasi software dan hardware yang diperlukan.
e. Audit
   Pada tahap ini sistem yang disimulasikan akan diuji secara sistematis untuk memastikan bahwa sistem keamanan yang diterapkan sudah sesuai dengan tujuan awal. Tahap ini dilakukan dengan skenario testing.
f. Evaluasi
   Pada tahap ini dilakukan evaluasi hasil dari testing yang telah dilakukan, sejauh mana tingkat efektifitas dari teknologi keamanan yang dibangun, dan membandingkan dengan tujuan awal serta kondisi ideal yang diharapkan[7].

METODE

3.1 Metode Pengumpulan Data

Untuk mendapatkan data yang akurat maka dalam penyusunan proposal skirpsi ini penulis mengunakan beberapa metode pengumpulan data diantaranya adalah sebagai berikit ini :

a. Observasi
   Merupakan teknik atau pendekatan untuk mendapatkan data primer dengan mengamati langsung objek datanya sehingga data dapat diproleh secara orisinil pada saat terjadinya dan mencatatkan hasil observasi tersebut. Dengan melakukan observasi langsung untuk mencari informasi data baik alat dan bahan serta segala sesuatu yang digunakan dalam penelitian ini.
b. Wawancara
   Wawancara digunakan sebagai teknik pengumpulan data pada penelitian ini. Selain itu penulis juga melakukan wawancara yang menyangkut masalah potensi serangan terhadap server SMPN I Muara Kelingi berkaitan dengan server dapotik.
c. Studi Literatur
   Menggunakan metode pengumpulan data Literatur yaitu dengan mencari referensi dari buku, majalah, jurnal, artikel, internet, dan sumber lainnya yang berkaitan dengan judul yang diambil, kemudian dirangkum untuk disusun dan di sempurnakan.

3.2 Metode Pengembangan Sistem

Dalam Metodologi yang digunakan dalam penelitian ini adalah *Security Policy Development Life Cycle* (SPDLC). Berikut penjelasan tahap-tahap yang dilakukan dalam penelitian ini:

a. Identifikasi
Tahap awal ini dilakukan untuk menemukan berbagai macam masalah keamanan yang dihadapi oleh jaringan pada saat ini dan bagaimana sistem yang sedang berjalan di perusahaan

b. Analisis
Dari data yang didapatkan pada tahap identifikasi, dilakukan proses analisis kebutuhan user.

c. Desain
Tahap desain ini akan membuat suatu gambar rancangan topologi sistem keamanan yang akan dibangun, alur sistem autentikasi serta menjelaskan kebutuhan sistem baik *software* maupun *hardware*.

d. Implementasi
Pada tahap ini dilakukan penerapan dari hasil perancangan yang telah dilakukan pada tahap sebelumnya. Namun, karena keterbatasan izin dari perusahaan dalam melakukan implementasi, hasil perancangan akan disimulasikan dalam jaringan yang lebih kecil[8]. Dimulai dengan instalasi perangkat dan mengkonfigurasi *softwar*e dan *hardware* yang diperlukan.

e. Audit
Pada tahap ini sistem yang disimulasikan akan diuji secara sistematis untuk memastikan bahwa sistem keamanan yang diterapkan sudah sesuai dengan tujuan awal. Tahap ini dilakukan dengan skenario testing.

d. Evaluasi
Pada tahap ini dilakukan evaluasi hasil dari testing yang telah dilakukan, sejauh mana tingkat efektifitas dari teknologi keamanan yang dibangun, dan membandingkan dengan tujuan awal serta kondisi ideal yang diharapkan. Hasil dari analisa akan dijadikan sebagai masukan untuk perbaikan sistem juga sebagai saran untuk usaha perbaikan di masa yang akan datang[9].

3.3 Metode Pengujian Sistem

Desain Pengujian dilakukan dengan menggunakan metode eksperimen yang dimaksudkan apakah sistem Snort dapat mendeteksi serangan *Sniffing* dengan baik[10]. Pengujian dilakukan dengan menggunakan Ettercap untuk *Sniffing* yang akan dilakukan oleh komputer *Attacker* seperti terlihat pada gambar 3 dibawah ini, dan Tabel 1 menyajikan komponen pengujian sistemnya.

Gambar 3. Alur Pengujian Sistem

Tabel 1. Komponen Pengujian Sistem

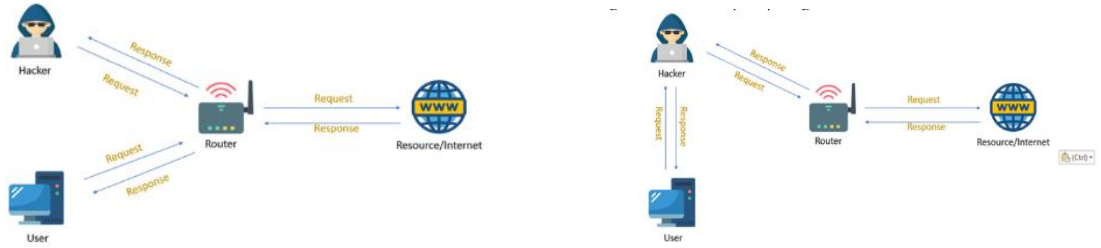
No	Komponen Pengujian	Proses Pengujian	Hasil Pengujian
1	Komputer server	Kinerja *Snort* untuk deteksi *Sniffing*.	Snort dapat mendeteksi serangan yang dilakukan *client*.
2	Komputer Client	Melakukan *Sniffing* ke komputer server	Komputer client berhasil menyadap (*Sniffing*) ke komputer server

menggunakan Ettercap.

HASIL DAN PEMBAHASAN

Desain Sistem

Pada kondisi normal, biasanya setiap user akan langsung berhubungan dengan router, akan tetapi ketika jaringan telah disadap maka topologi akan berubah. Gambar 4,a menunjukan gambaran jika kondisi jaringan dalam keadaan normal sementara gambar 4,b menunjukan kondisi jika sudah menerima serangan Sniffing.



(a) (b)

Gambar 4. (a) Kondisi Jaringan Normal, (b) Kondisi Jaringan Serangan Snifing

Konfigurasi ekperimen terhadap masing-masing komponen dapat dilihat pda tabel 2 dibawah ini :

Tabel 2. Konfigurasi Eksperimen

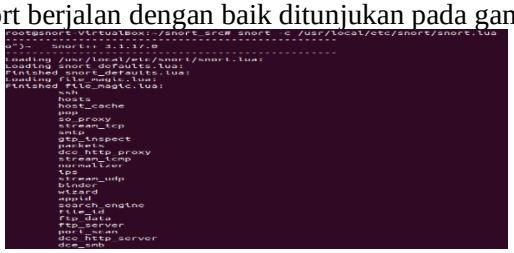
Nama PC dan IP Address	Sistem Operasi	Tools Pendukung	Konfigurasi Aplikasi
PC1 IP:192.168.0.1	Ubuntu versi 18.04 LTS	Snort	IDS dengan *alert* Snort *Rules* untuk deteksi *Sniffing*
PC2 IP:192.168.0.2	Kali Linux	Terminal	Aplikasi Ettercap untuk menyadap (*Sniffing*)

Instalasi Snort

Untuk tahap pertama adalah melalukan instalasi snort 3 dan hasil instalasi tersebut ditunjukkan pada gambar 5 dibawah ini:

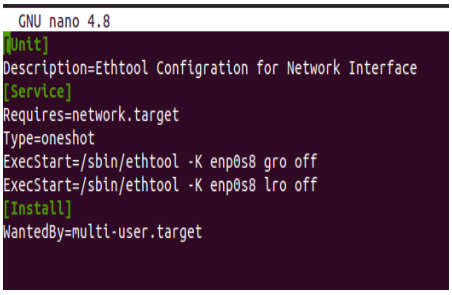
Gambar 5. Hasil Instalasi Snort

Hasil pengujian instalasi snort berjalan dengan baik ditunjukan pada gambar 6 berikut ini:

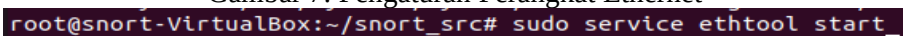


Gambar 6. Pengujian Hasil Instalasi

Gambar 7 dan gambar 8 menunjukkan konfigurasi perangkat ethernet yang akan di monitor atau diawasi oleh snort dan mengaktifkannya[11].



Gambar 7. Pengaturan Perangkat Ethernet

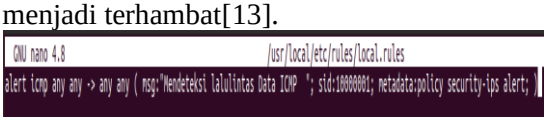


Gambar 8**.** Aktifasi Perangkat Ethernet

Gambar 9 menunjukkan direktori untuk menyimpan rule snort, rule ini digunakan untuk menyimpan perintah pada snort dalam mendeteksi serangan yang sudah didefinisikan[12].

Gambar 9. Direktori Pengaturan Snort

Gambar 10 adalah *rule* atau aturan yang penulis buat untuk mendeteksi serangan *Sniffing,* serangan *Sniffing* menggunakan paket data protokol ICMP yang dikirimkan secara *masive* sehingga server akan mengalami kelebihan paket data yang diterima sehingga menyebabkan pengguna lain yang mengakses server tersebut menjadi terhambat[13].

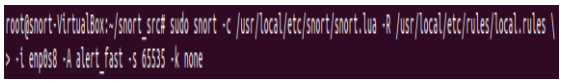


Gambar 10. Rule Snort Deteksi Sniffing

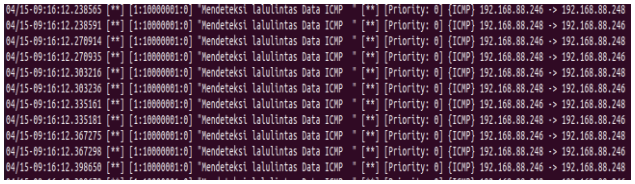
Rule atau aturan yang penulis buat untuk mendeteksi *ping flood* adalah dengan mendeteksi paket data ICMP yang berlebihan, dan melewati ethernet yang sudah dimasukkan dalam pengaturan snort untuk diawasi[14].

Pengujian Sistem

Pengujian sistem dilakukan menggunakan dua buah PC komputer, satu komputer sebagai server menggunakan sistem operasi Linux Ubuntu, dan komputer lainnya sebagai attacker menggunakan sistem operasi Kali Linux[15]. Gambar 11 dan 12 menunjukkan penggunaan *rule* untuk mendeteksi serangan *sniffing* dan hasil deteksi serangan *sniffing* pada server[16].



Gambar 11. Penerapan *rule* snort untuk mendeteksi *sniffing* secara *real time*



Gambar 12. Hasil deteksi serangan *sniffing* secara *real time*

Gambar 13 menunjukkan statistik hasil deteksi sniffing secara real time menggunakan snort. Dari gambar 13 ini dapat dilihat ip address dari computer penyerang yaitu 192.168.88.246 dengan serangan sniffing yang membanjiri lalu lintas data di protocol ICMP[17].

Gambar 13. Hasil Deteksi Serangan Sniffing

Dari pengujian yang telah dilakukan maka dapat ditarik kesimpulan sistem deteksi serangan sniffing dapat mendeteksi serangan tersebut secara real time[18].

KESIMPULAN

Hasil dari penelitian ini berupa sistem yang dapat mendeteksi serangan packet sniffing, sehingga pihak sekolah SMPN I Muara Kelingi dapat menggambil langkah penyelamatan data dengan lebih cepat.

UCAPAN TERIMA KASIH

Pada bagian ini bersifat optional, boleh dihilangkan oleh penulis. Ucapan terima kasih berisikan prakata apresiasi penulis kepada orang, kelompok atau instansi yang berkontribusi pada program penelitian.

DAFTAR PUSTAKA

[1] Y. N. Kunang *et al.*, "Analysis and implementation of the Port Knocking method using Firewall-based Mikrotik RouterOS," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 8, no. 4, pp. 1907–5022, 2019.

[2] A. Umasugi, M. D. Suratin, and S. Hamza, "Analisis Keamanan Jaringan Wifi Terhadap Packet Sniffing DiKampus a Universitas Muhammadiyah Maluku Utara," *Produktif J. Ilm. Pendidik. Teknol. Inf.* , vol. 6, no. 2, pp. 597–602, 2022, [Online]. Available: https://journal.umtas.ac.id/index.php/produktif/article/view/2460

[3] C. A. Putra, M. S. Munir, Y. V. Via, and R. Achmadipoetro, "Deteksi Serangan Trojan Horse Dengan Memanfaatkan Ids Snort," *Semin. Santika*, no. September, pp. 203–206, 2019, [Online]. Available: http://santika.ijconsist.org/index.php/SANTIKA/article/view/31

[4] M. A. S. Arifin, "Rancang Bangun Prototype Robot Lengan Menggunakan Flex Sensor Dan Accelerometer Sensor Pada Lab Mikrokontroler Stmik Musirawas," *Ilk. J. Ilm.*, vol. 9, no. 3, pp. 255–261, 2017, doi: 10.33096/ilkom.v9i3.152.255-261.

[5] R. Sahara, S. Abdullah, and R. Saputra, "Analisis Ancaman Sniffing pada Jaringan WiFi di PT. Stepa Wirausaha Adiguna," *Pros. Semin. Nas. Ris. Dan Inf. Sci.*, vol. 4, pp. 224–230, 2022.

[6] R. Kurniawan and A. Zulius, "Sistem Smart Parking Menggunakan Ultrasonik Sensor," *J. Sist. Komput. Musirawas*, vol. 3, no. 1, p. 22, 2018, doi: 10.32767/jusikom.v3i1.309.

[7] B. Wijaya and A. Pratama, "Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (Ids) Berbasis Snort," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 1, pp. 97–101, 2020, doi: 10.32736/sisfokom.v9i1.770.

[8] Ilham Firdaus, Januar Al Amien, and S. Soni, "String Matching untuk Mendeteksi Serangan Sniffing (ARP Spoofing) pada IDS Snort," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 1, no. 2, pp. 44–49, 2020, doi: 10.37859/coscitech.v1i2.2180.

[9] W. Fathoni, Fitriyani, and G. N. Nurkahfi, "Deteksi Penyusupan Pada Jaringan Komputer Menggunakan Ids Snort," *e-Proceeding Eng.*, vol. 3, no. 1, pp. 1169–1172, 2016, [Online]. Available: https://openlibrary.telkomuniversity.ac.id/pustaka/files/114823/persembahan/deteksi-penyusupan-pada-jaringan-komputer-menggunana-ids-snort.pdf

[10] A. Rizal Fauzi and I. Made Suartana, "Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids," *J. Manaj. Inform.*, vol. 8, no. 2, p. 7, 2018.

[11] A. Akhriana and A. Irmayana, "Web App Pendeteksi Jenis Serangan Jaringan Komputer Dengan Memanfaatkan Snort Dan Log Honeypot," *CCIT J.*, vol. 12, no. 1, pp. 85–96, 2019, doi: 10.33050/ccit.v12i1.604.

[12] T. Widodo and A. S. Aji, "Pemanfaatan Network Forensic Investigation Framework untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS)," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 1, pp. 46–55, 2022, doi: 10.14421/jiska.2022.7.1.46-55.

[13] A. Prasetyo, L. Affandi, and D. Arpandi, "Implementasi Metode Naive Bayes Untuk Intrusion Detection System (Ids)," *J. Inform. Polinema*, vol. 4, no. 4, p. 280, 2018, doi: 10.33795/jip.v4i4.220.

[14] Sutarti, A. P. Pancaro, and F. I. Saputra, "Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal," *J. PROSISKO*, vol. 5, no. 1, pp. 1–8, 2018.

[15] R. Suwanto, I. Ruslianto, and M. Diponegoro, "Implementasi Intrusion Prevention System (IPS) Menggunakan Snort Dan IPTable Pada Monitoring Jaringan Lokal Berbasis Website," *J. Komput. dan Apl.*, vol. 07, no. 1, pp. 97–107, 2019.

[16] J. Fahana, R. Umar, and F. Ridho, "Pemanfaatan Telegram Sebagai Notifikasi Serangan untuk Keperluan Forensik Jaringan," *J. Sist. Inf.*, vol. 5341, no. 6, p. 2, 2017.

[17] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 413, 2020, doi: 10.30865/mib.v4i2.2037.

[18] S. Alviana and I. D. Sumitra, "Analisis Pengukuran Penggunaan Sumber Daya Komputer Pada Intrusion Detection System Dalam Meminimalkan Serangan Jaringan," *Komputa J. Ilm. Komput. dan Inform.*, vol. 7, no. 1, pp. 27–34, 2018, doi: 10.34010/komputa.v7i1.2533.