SPIRIT VOL 15 NO 2 (2023) 131 - 142
JURNAL SPIRIT
225/E/KPT/2022

e-ISSN 2721-057X
p-ISSN 2085-3092

NETWORK BEHAVIOR ANALYSIS (NBA) UNTUK MENDETEKSI TRAFIK SERANGAN DALAM JARINGAN KOMPUTER

Slamet[1]
Prodi S1 Sistem Informasi [1] (Universitas Dinamika, Surabaya, Indonesia)
slamet@dinamika.ac.id

Naskah diterima: 19 Nopember 2023 ; Direvisi : 25 Nopember 2023 ; Disetujui : 25 Nopember 2023

Abstrak

Penelitian ini berfokus pada penggunaan *Network Behavior Analysis* (NBA) yang dirancang untuk mendeteksi serangan jaringan. NBA mempunyai permasalahan akurasi dalam mendeteksi trafik serangan jaringan. Pada paper ini, akurasi deteksi NBA dapat ditingkatkan apabila proses pembelajarannya berisi kolaborasi serangan model pengaburan dan serangan secara langsung. Pekerjaan ini menggunakan beberapa cara pengaburan yang dapat digunakan sebagai penghindaran pada metode NBA. *Tools* serangan semi-otomatis digunakan untuk mengeksploitasi serangan secara sistematis dan melakukan pencatatan aktivitas untuk mendapatkan data yang cukup dalam eksperimen. Data yang diperoleh kemudian dipilih dan dianalisis oleh NBA sebagai verifikator asumsi. Hasil eksperimen mendapatkan asumsi bahwa NBA memerlukan pengetahuan tentang serangan yang dikaburkan untuk mendapatkan akurasi yang baik. Hasil deteksi akurasi pada training NBA tanpa serangan pengaburan tergantung pada tingkatannya. Namun NBA melakukan pembelajaran dengan pengetahuan tentang semua serangan (langsung dan pengaburan) mampu mencapai akurasi klasifikasi 99,45%.

Kata kunci: Network Behavior Analysis, serangan jaringan, akurasi deteksi

Abstract

This research focuses on the use of Network Behavior Analysis (NBA) which is designed to detect network attacks. The NBA has accuracy problems in detecting network attack traffic. In this paper, the accuracy of NBA detection can be improved if the learning process contains a collaboration of obfuscation model attacks and direct attacks. This work uses several obfuscation methods that can be used as evasions in the NBA method. Semi-automatic attack tools are used to systematically exploit attacks and log activities to obtain sufficient data for experiments. The data obtained was then selected and analyzed by the NBA to verify the assumptions. The experimental results obtain the assumption that the NBA requires knowledge of the attack that is obscured to obtain good accuracy. The detection accuracy of NBA training without obfuscation attacks varies greatly, depending on the level. However, NBA performs learning with knowledge of all attacks (direct and obfuscation) able to achieve a classification accuracy of 99.45%.

Keywords: Network Behavior Analysis, network attacks, detection accuracy.

PENDAHULUAN

Saat ini, teknologi informasi berkembang dengan kemajuan yang cukup pesat [1]. Bidang keamanan jaringan yang menjadi salah satu simpul teknologi informasi juga berkembang dengan cepat, sehingga sangat penting untuk diteliti. Ancaman-ancaman baru terhadap keamanan jaringan selalu muncul setiap hari, sementara ancaman yang lebih lama juga tidak pernah selesai. Beberapa model ancaman seperti pada [2] telah menjadi trend ancaman-ancaman pada jaringan. Jenis pertahanan pada jaringan semacam 2FA (Two Factor Authentication) menjadi salah satu solusi seperti dibahas pada [3] terkait dengan ancaman ini.

Di sisi yang lain, permasalahan akurasi pendeteksian terhadap serangan sudah banyak diteliti oleh [4][5][6][7]. Salah satu pendekatan yang relatif baru menggunakan Network Behaviour Analysis (NBA)[8] dalam peningkatan akurasi deteksi sistem serangan untuk berkontribusi dalam keamanan cyber.

Sistem NBA adalah salah satu jenis teknologi IDS/IPS (*Intrusion Detection System/Intrusion Prevention System*) yang menganalisis perilaku jaringan. Caranya adalah dengan mengamati lalu lintas jaringan dalam mengenali serangan yang tidak terduga pada aliran paket. NBA memiliki beberapa keunggulan dibandingkan pendekatan lainnya [9], tetapi cara ini juga memiliki keterbatasan, seperti *intruder* bisa menyamar dalam aktivitasnya dengan berbagai cara. NBA juga sering mengalami masalah ketika mendeteksi aktivitasnya.

Tujuan utama dari penelitian ini adalah untuk meningkatkan akurasi dalam mendeteksi serangan- serangan yang tidak jelas (anomali) dalam jaringan komputer dengan menggunakan NBA. Untuk melakukan serangan, dirancang skenario dengan beberapa kali serangan menggunakan teknik pengaburan [10] (*obfuscation techniques*). Beberapa tools AI (Artificial Intelligence) sering digunakan untuk berbagai kebutuhan seperti pada [11][12][13][14]. Namun, untuk implementasi serangan ini, digunakan *tools* AI semi otomatis. Selain itu *tools* ini digunakan untuk pencatatan kegiatan dalam mendapatkan kecukupan data dengan berbagai serangan yang dikaburkan. Semua data yang diperoleh dari tools ini diolah menjadi dataset, selanjutnya digunakan untuk memverifikasi asumsi dan mempelajari model pengklasifikasi NBA dalam menangani semua jenis serangan (model serangan secara langsung dan model pengaburan).

Pada eksperimen dicapai asumsi yang terkonfirmasi menggunakan NBA tentang perlunya menggunakan kolaborasi serangan pengaburan dan serangan langsung secara berurutan untuk mendapatkan akurasi klasifikasi yang lebih baik. Tanpa informasi pengaburan, model NBA untuk serangan langsung hanya mendapatkan akurasi deteksi yang rendah. Dengan menambahkan *tools* semi otomatis pada skenario serangan, terbukti mengurangi kesalahan dan dapat menghemat banyak waktu. Selain itu, didapatkan konsistensi dan pendekatan sistematis dalam proses penyerangan dan pencatatan trafik data.

Penelitian terkait NBA berkonsentrasi pada ciri-ciri perilaku yang ada di jaringan komputer. Berbagai rangkaian metrik yang menjadi ciri perilaku jaringan pada trafik jaringan dengan banyak serangan telah sering dikembangkan. Metode yang menggunakan standar NetFlow terbukti tidak cukup [15]. Para peneliti mulai membuat metrik sendiri yang dapat memperoleh lebih banyak informasi dan lebih banyak konteks tentang trafik yang dianalisis. Ada dua metrik [16] yang banyak diketahui publik dan dapat digunakan untuk NBA. Keduanya terkait dengan koneksi TCP dan UDP, yang mana TCP memiliki permulaan dan akhir yang jelas. Namun, tidak demikian dengan protokol UDP yang secara alami masih bermasalah.

Pada [17] menyajikan diskriminator yang menyediakan banyak fitur untuk deskripsi aliran paket pada jaringan. Peneliti telah membuat banyak temuan tentang diskriminator dan klasifikasi lalu lintas Internet dalam makalahnya.

Advanced Security Network Metrics (ASNM) [18] telah mempublikasikan penelitiannya dan menghasilkan *signature* perilaku jaringan dari kumpulan ASNM. *Signature* yang dirilis terdiri dari 167 metrik dibagi menjadi 5 kategori seperti: statistik, dinamis, lokalisasi, terdistribusi dan perilaku.

Pada [19] serangan yang dikategorikan secara sistematis terhadap IDS. Peneliti menetapkan enam tujuan utama serangan terhadap IDS yaitu: penghindaran (*avoiding*), stimulasi berlebihan, *poisoning*, *Denial of Services* (DoS), *response hijacking*, dan *reverse engineering*. Serangan-serangan ini berhasil mengeksploitasi berbagai kerentanan dari IDS.

Dalam eksperimen [20] dan [21], telah mengimplementasikan serangan pengaburan pada jaringan *tunnelling* HTTP(S). Peneliti memeriksa kemampuan deteksi jaringan dari serangan *buffer overflow* menggunakan Snort dan AIPS3. Pengaburan dilakukan dengan melakukan

tunnelling malicious berbahaya di dalam protokol HTTP(S). Peneliti mensimulasikan properti khas dari trafik jaringan HTTP yang *legitimate*. Peneliti menyatakan bahwa Snort mampu mendeteksi serangan langsung. Namun, tidak dapat mendeteksi serangan pengaburan. Dengan pengklasifikasi yang dilatih tanpa serangan pengaburan, dicapai akurasi hanya 0,10%. Hal ini menunjukkan bahwa berdasarkan perilaku dan statistik, NBA tidak mampu mendeteksi serangan yang dikaburkan tanpa sepengetahuan mereka sebelumnya. Kemudian peneliti memasukkan serangan pengaburan ke dalam data pelatihan, didapatkan akurasi 97,64% + 0,45% dalam kasus klasifikasi binominal dan 98,87% + 0,99% dalam kasus klasifikasi polinomial.

Pada [22] peneliti merancang subkelas serangan baru dengan nama pencampuran polimorfik. Serangan model ini secara efektif dapat menghindari deteksi anomali dari jaringan berbasis frekuensi byte IDS (mis. PAYL).

Penelitian ini menunjukkan bahwa masih banyak penelitian lebih lanjut yang dapat dilakukan dalam bidang ini. Ada kebutuhan untuk memeriksa semua jenis serangan dan dampak ketidak-pastian untuk memberikan berbagai pengetahuan kepada NBA tentang berbagai serangan. *Tools* yang dibuat semi otomatis dalam serangan dapat berguna dalam penelitian lebih lanjut.

METODE PENELITIAN

Untuk menyelesaikan masalah dan mencapai tujuan yang ditetapkan, dilakukan langkah-langkah berikut.

1. Metode Pengaburan Behavior untuk Analisis Komunikasi

Metode pengaburan pada penelitian ini menggunakan *Advanced Security Network Metrics for Attack Vector* (ASNM) [18]. Beberapa teknik serangan tidak digunakan dalam skenario serangan, misalnya serangan DoS (Denial of Services) [23] karena membutuhkan pengerahan sumber daya secara fisik pada NBA. Selain itu, ASNM dan diskriminator [17] hanya memeriksa *header* paket, sehingga serangan itu dapat mengaburkan *payload,* misalnya PBA [10] hampir tidak ada gunanya. Sedangkan pada [19] menunjukkan banyak vektor serangan pada IDS yang tidak relevan karena jenis penerapannya.

Berikut adalah teknik pengaburan yang digunakan pada penelitian ini.

Tabel 1. Penggunaan Teknik Pengaburan

Proses	Cara Pengaburan
Penyebaran paket data	1 detik *delay* konstan 7 detik *delay* konstan 4 detik *delay* dengan variasi kurang lebih 2,5 detik (distribusi normal) dan korelasi 25%
Paket hilang Modifikasi MTU (Maximum Transmission Unit)	20% paket hilang MTU 250 MTU 500 MTU 750 MTU 1000
Paket *corrupt*	20% paket *corrupt* 30% paket *corrupt* 30% paket *corrupt* dengan korelasi 20%
Paket duplikat	4% paket duplikat
Paket *reorder*	20% paket *reorder* (dikirim dalam *delay* 8ms) dengan korelasi 40% 40% paket *reorder* (dikirim dalam *delay* 8ms) dengan korelasi 40%

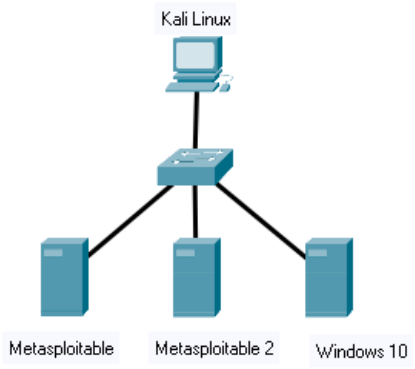
Teknik pengaburan yang digunakan dapat dilihat pada tabel 1. Pada proses "penyebaran paket", ukuran waktu dengan kondisi tertentu diperoleh dengan mencoba nilai-nilai yang berbeda, sampai serangan tidak terjadi di dalam jaringan. Demikian juga dengan proses "kehilangan paket", "modifikasi MTU" "paket *corrupt*", "paket duplikat", dan "paket *reorder*". Intinya salah satu teknik pengaburan tersebut adalah mencoba dan memodifikasi paket mengalir dengan berbagai cara.

NBA dengan ASNM memeriksa statistik yang beragam dan pengaburan ini dapat mengakibatkan kebingungan untuk model pendeteksiannya. Sebuah paket yang berisi konten eksploitasi biasanya berukuran besar, namun dalam ekperimen ini dibuat berubah-ubah dan anomali.

2. Skenario Serangan di Jaringan Komputer

Untuk menghindari masalah-masalah hukum dan praktik melakukan serangan langsung dan ilegal melalui Internet, skenario serangan dilakukan di dalam jaringan virtual menggunakan *Virtual Machine* (VM) VirtualBox. Di dalam *Virtual Machine* di-*install* dengan : (a). Kali Linux 2023.1 yang difungsikan sebagai mesin penyerang; (b). Metasploitable, Metasploitable 2 dan sistem operasi Windows 10 yang mewakili mesin target serangan.

Berikut adalah topologi jaringan yang digunakan dalam penelitian.



Gambar 1. Topologi Serangan di dalam VM (Virtual Machine)

Pada serangan pertama, *intruder* melakukan serangan dengan cara menyusup dan tidak memiliki akses kepada mesin target menggunakan *tunnelling* HTTPS [20]. Selanjutnya, *intruder* melakukan serangan pada *services-services* pada mesin target ini.

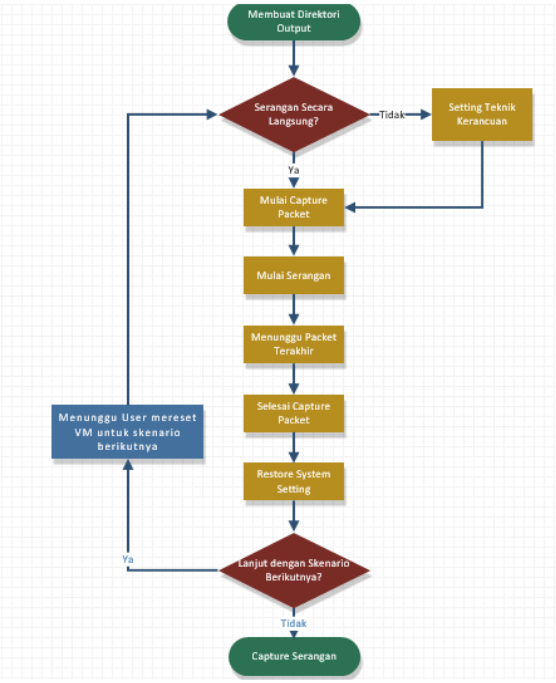
Aplikasi atau *services* dan kerentanan yang digunakan dalam serangan ini adalah:

a. Apache Tomcat 9.0 – Aplikasi ini digunakan sebagai *web server* sekaligus untuk penyerangan dengan mengeksekusi *payload* di Tomcat server (dengan kredensial/hak akses) yang diperoleh dari aplikasi terbuka.
b. Microsoft SQL Server 2019 – Aplikasi ini juga digunakan untuk penyerangan dengan mengeksekusi muatan paket yang diskenariokan pada Microsoft SQL Server menggunakan prosedur tersimpan "*xp cmdshell*".
c. Samba 4.18.6-Debian – Aplikasi ini digunakan sebagai tempat penyimpanan *username* dan *password* yang akan diserang. Model serangan dengan cara: (1). memanfaatkan perintah kerentanan eksekusi di Samba saat menggunakan opsi konfigurasi *non-default* "*username map script*", (2) menentukan *username* yang mengandung karakter *meta shell*, sehingga *intruder* dapat mengeksekusi perintah dengan leluasa tanpa diperlukan otentikasi.
d. *Services* Server (Windows 10) – *Services* ini memungkinkan *intruder* mengeksekusi *kode-kode* secara *remote* dengan mudah, melalui pembuatan permintaan RPC yang memicu *overflow* pada jalur jaringan resmi.

3. *Tools* untuk mengeksekusi serangan secara semi-otomatis

Tools eksploitator diimplementasikan untuk mengeksekusi serangan secara semi-otomatis dan untuk pencatatan aktivitas. *Tools* ini ditulis dalam bahasa pemrograman *Python* menggunakan *framework metasploit* dan *msfconsole* untuk serangan otomatis. Pengguna harus menyediakan sumber daya (yang diuji secara manual) berupa *file* yang berisi perintah *msfconsole*. *Intruder* membutuhkan *file* ini untuk

mengeksploitasi serangan secara otomatis. Alur eksekusi penyerangan ditunjukkan pada gambar 2.



Gambar 2. Alur Penyerangan pada *Experiment*

Paket di-*capture* (diambil) dari jaringan menggunakan tools *tcpdump*. *Tcpdump* mengoleksi trafik TCP di antara penyerang dan mesin target. Pada skenario ini, ketika serangan dilakukan, aplikasi yang digunakan menunggu beberapa saat (hingga beberapa menit) sebelum menghentikan pengambilan paket. Proses ini dilakukan untuk menunggu koneksi TCP berikutnya secara lengkap. Skenario ini dilakukan secara berulang-ulang untuk menjalankan setiap skenario serangan yang lainnya dan dianggap selesai sehingga dijadikan sebagai dataset akhir.

Apabila ada skenario serangan berikutnya, aplikasi akan menunggu pengguna untuk mengonfirmasi bahwa dia telah mengembalikan mesin serangan ke dalam kondisi sebelum dieksploitasi. Proses menunggu ini adalah pilihan namun sangat disarankan, karena beberapa serangan dapat bersifat (semi) destruktif. Jika seorang pengguna mengabaikannya, beberapa serangan berpotensi gagal dan/atau memberikan hasil yang tidak konsisten. Jika tidak, aplikasi akan keluar dan mengeluarkan output direktori berisi subdirektori untuk setiap skenario serangan. Hal ini adalah bentuk yang dapat digunakan dengan *tools* pasca eksploitasi sehingga proses selanjutnya dalam mengekstraksi ASNM menjadi mudah.

4. *Dataset* untuk *Eksperimen*

Dalam eksperimen, *tools* pasca eksploitasi menggunakan file-file *pcap* dari serangan yang telah dilakukan (dan dari trafik yang *legitimate*) untuk mendapatkan kumpulan data dengan ASNM. Proses mengekstraksi metrik label dari *file pcap* dapat dilihat pada gambar 3.

Gambar 3. Proses Ektraksi Metrik

Dataset yang diperoleh terdiri dari 5425 koneksi berbahaya *(malicious)* dan 2314 koneksi yang *legitimate*. Trafik yang *legitimate* diwakili oleh penggunaan internet secara umum (*browsing, email, ftp*, dan lain-lain) dan komunikasi antar VM. *Command line* dari tools *netem* [11] digunakan untuk mensimulasikan *delay*, paket hilang (*packet loss)*, Paket *corrupt (packet corrupt)*, duplikasi paket dan *packet reordering*. Distribusi trafik untuk *port* TCP yang *legitimate* adalah sebagai berikut :

a. Internet, menggunakan port 3129,
b. Netem menggunakan port 7000
c. Komunikasi antar *Virtual Machine* menggunakan port 443.

Tabel 2. Perolehan Dataset dari Jenis Serangan

Jenis Layanan	Jenis Serangan	Serangan Langsung	Serangan yang dikaburkan
Apache Tomcat	Mgr_ deploy	11	150
Apache Tomcat	Mgr_ login	254	3128
Microsoft SQL Server 2019	Login	23	223
Microsoft SQL Server 2019	Xp_ cmdshell	22	780
Server Service	Ms08_ 067_netapi	83	670
Samba	Usermap_ script	4	77
Total		397	5028

HASIL DAN PEMBAHASAN

Ekperimen dilakukan pada pendeteksian semua jenis serangan, yaitu langsung dan pengaburan, serta mengimplementasikan klasifikasi binominal. Hal ini karena model pengklasifikasi NBA ini lebih realistis diterapkan di lapangan, dimana biasanya Perusahaan ingin mendeteksi serangan dan membiarkan lalu lintas *legitimate* melalui jaringannya.

Hasil eksperimen, NBA yang dilatih tanpa pengetahuan tentang serangan yang dikaburkan, mengalami kesulitan dalam pendeteksiannya. Namun jika NBA melakukan serangan yang dikaburkan dan adanya *supervised attacking* untuk proses pelatihannya, maka hasil deteksinya menjadi jauh lebih baik.

Semua eksperimen menggunakan *tools* data mining RapidMiner dengan mengklasifikasi 12 fitur dari 880 fitur yang merepresentasikan komunikasi *legitimate* dan *malicious*. Operator yang digunakan adalah *Naive Bayes*. Fitur yang sama juga telah digunakan pada [20] [21].

Dalam rangkaian eksperimen, serangan langsung dengan trafik *legitimate* digunakan untuk melatih *classifier*, dan model yang dilatih kemudian diuji pada seluruh dataset. Pada tabel 3, 4, 5 dan 6 dapat dilihat bahwa perbedaan parameter

dari *classifier* dapat menyebabkan hasil yang buruk dan hasil yang baik.

Tabel 3. *Confusion matrix* yang buruk untuk *classifier* yang sudah dilatih tanpa teknik serangan pengaburan

Akurasi: 98.50% ± 0,58%	Prediksi *Legitimate*	Prediksi *attack*	*Recall*
True legitimate	2499	0	100%
True attack	39	329	89.10%
Presisi	97,99%	100%	

Tabel 4. *Confusion matrix* yang buruk untuk *classifier* yang diuji pada dataset utuh

Akurasi: 67.98%	Prediksi *Legitimate*	Prediksi *Attack*	*Recall*
True Legitimate	2599	0	100%
True Attack	2477	2699	50%
Presisi	49,98%	100%	

Tabel 5. *Confusion matrix* yang baik untuk *classifier* yang sudah dilatih tanpa teknik serangan pengaburan

Akurasi: 99.91% ± 0,05%	Prediksi *Legitimate*	Prediksi *attack*	*Recall*
True legitimate	2599	0	100%
True attack	1	395	99.60%
Presisi	99,98%	100%	

Tabel 6. *Confusion matrix* yang baik untuk *classifier* yang diuji pada dataset utuh

Akurasi: 97.11%	Prediksi *Legitimate*	Prediksi *attack*	*Recall*
True legitimate	2599	0	100%
True attack	1	4995	96.60%
Presisi	91,18%	100%	

Tabel 7. *Confusion matrix* untuk *classifier* yang diuji pada dataset utuh dengan 5 *fold cross-validation*

Akurasi: 99.98% ± 0,01%	Prediksi *Legitimate*	Prediksi *attack*	*Recall*
True legitimate	2650	2	100%
True attack	0	5892	96.60%
Presisi	100%	99,97%	

Pada eksperimen lain, semua data diberikan ke *classifier* yang diuji dengan 5 *fold cross-validation* (tabel 7). Eksperimen ini menunjukkan bahwa semakin banyak data tentang serangan, dapat meningkatkan akurasi klasifikasi sampai maksimal.

Dari eksperimen terlihat juga bahwa terdapat beberapa properti dari serangan yang dikaburkan berbeda dengan properti serangan langsung. Oleh karena itu, peneliti bisa saja menggunakan properti tersebut untuk melatih model klasifikasi NBA (tanpa serangan dikaburkan), tetapi

tidak menjamin hasil-hasil yang baik dari parameter yang ada (lihat tabel 3 dan 4). Tanpa akses terhadap serangan yang dikaburkan, peneliti tidak dapat menguji apakah model yang dibuat dapat mendeteksi serangan dengan baik. Oleh karena itu, informasi tentang serangan dikaburkan sangat diperlukan bagi proses pembelajaran model klasifikasi untuk *Network Behavior Analysis*.

KESIMPULAN

Metode NBA dirancang menggunakan tools eksploitator untuk pengaburan semi otomatis dan perekaman serangan jaringan serta untuk mendapatkan data eksperimen. Dalam eksperimen didapatkan, bahwa penggunaan teknik pengaburan dikolaborasikan dengan serangan langsung kepada NBA dapat meningkatkan akurasi deteksi sampai dengan 99,45%. Penggunaan tools semi otomatis ini juga sangat efektif dan sistematis dalam pengumpulan data sehingga mengurangi kesalahan dibandingkan pengumpulan data manual yang sangat sulit dan rawan kesalahan.

Untuk ke depannya diperlukan eksperimen dengan berbagai kombinasi teknik pengaburan sehingga dapat menghasilkan sesuatu yang baru dan menarik. Beberapa hal yang bisa dilakukan seperti mengekploitasi beberapa payload (eksploitasi konten) dan memodifikasinya dengan beberapa teknik dan algoritma yang lain.

Daftar Pustaka

[1] T. Pradana, "Penggalian Kaidah Multilevel Association Rule Dari Data Mart Swalayan Asgap," *Jurnal SPIRIT*, vol. 7, no. 2, pp. 67–75, 2015, [Online]. Available: https://www.jurnal.stmik-yadika.ac.id/index.php/spirit/article/view/5/45.

[2] S. Slamet, "Desain Arsitektur Aplikasi Qr Code Sebagai Anti Phishing Serangan Qr Code," *Spirit*, vol. 15, no. 1, pp. 42–48, 2023, doi: 10.53567/spirit.v15i1.280.

[3] S. Slamet, "Pertahanan Pencegahan Serangan Social Engineering Menggunakan Two Factor Authentication (2Fa) Berbasis Sms (Short Message System)," *Spirit*, vol. 14, no. 2, pp. 23–29, 2023, doi: 10.53567/spirit.v14i2.260.

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

[5] R. E. Susanti, A. W. Muhammad, and W. A. Prabowo, "Implementasi Intrusion Prevention System (IPS) OSSEC dan Honeypot Cowrie," *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, vol. 11, no. 1, pp. 73–78, 2022, doi: 10.32736/sisfokom.v11i1.1246.

[6] K. Kurniabudi, A. Harris, and E. Rosanda, "Optimalisasi Seleksi Fitur Untuk Deteksi Serangan Pada

IoT Menggunakan Classifier Subset Evaluator," *JURIKOM (Jurnal Riset Komputer)*, vol. 9, no. 4, p. 885, 2022, doi: 10.30865/jurikom.v9i4.4618.

[7] N. K. T. Martuti and R. Anjarwati, "Indonesian Journal of Mathematics and Natural Sciences," *Indonesian Journal of Mathematics and Natural Sciences*, vol. 45, no. 1, pp. 1–8, 2022.

[8] K. Xu, *Network Behavior Analysis*. Springer Singapore, 2022.

[9] A. Shahraki and Ø. Haugen, "An outlier detection method to improve gathered datasets for network behavior analysis in IoT," *Journal of Communications*, vol. 14, no. 6, pp. 455–462, 2019, doi: 10.12720/jcm.14.6.455-462.

[10] X. Zhang, F. Breitinger, E. Luechinger, and S. O'Shaughnessy, "Android application forensics: A survey of obfuscation, obfuscation detection and deobfuscation techniques and their impact on investigations," *Forensic Science International: Digital Investigation*, vol. 39, p. 301285, 2021, doi: 10.1016/j.fsidi.2021.301285.

[11] D. Setiawan and A. Zakki Falani, "Pemanfaatan Artificial Neural Network Dengan Metode Hebb Rule Untuk Pengenalan Bahasa Isyarat Indonesia Statis," *Spirit*, vol. 12, no. 1, pp. 9–15, 2020.

[12] D. Kusbianto Purwoko Aji and N. Khotimah, "Prediksi Diskalkulia Menggunakan Jaringan Syaraf Tiruan Backpropagatio," *Spirit*, vol. 6, no. 1, pp. 1–10, 2014.

[13] Nurul Fuad, "Penerapan Metode Certainty Factor Untuk Mendiagnosa Dan Pencegahan Penyakit Cacingan Pada Anak Balita," *Jurnal Spirit*, vol. 8, no. 1, pp. 12–16, 2016.

[14] S. Slamet and N. Ningsih, "Intelligent Rule Firewall berbasis Linux menggunakan Association Rule Mining untuk Peningkatan Adaptive Response Attack," *Journal of Technology and Informatics (JoTI)*, vol. 3, no. 1, pp. 12–18, 2021, doi: 10.37802/joti.v3i1.188.

[15] I. J. Barath, "Network behavior analysis of selected operating systems," *2019 Communication and Information Technologies Conference Proceedings, KIT 2019 - 10th International Scientific Conference*, no. October, 2019, doi: 10.23919/KIT.2019.8883302.

[16] G. A and K. K. A, "Predicting Malicious Node Behavior in Wireless Network Using DSR Protocol and Network Metrics," *International Journal of Computer Communication and Informatics*, vol. 4, no. 1, pp. 1–10, 2022, doi: 10.34256/ijcci2211.

[17] S. Zheng, W., Gou, C., Yan, L., & Mo, "Learning to classify: A flow-based relation network for encrypted traffic classification," *In Proceedings of The Web Conference*, pp. 13–22, 2020.

[18] I. Homoliak, M. Barabas, P. Chmelar, M. Drozd, and P. Hanacek, "ASNM: Advanced security network metrics for attack vector description," *Proceedings of the International Conference on Security and Management (SAM)*, p. 1, 2013.

[19] A. Alotaibi and M. A. Rassam, "Adversarial Machine Learning Attacks against Intrusion Detection Systems: A Survey on Strategies and Defense," *Future Internet*, vol. 15, no. 2, 2023, doi: 10.3390/fi15020062.

[20] I. Homoliak, D. Ovsonka, M. Gregr, and P. Hanacek, "NBA of

obfuscated network vulnerabilities' exploitation hidden into HTTPS traffic," *2014 9th International Conference for Internet Technology and Secured Transactions, ICITST 2014*, no. December, pp. 310–317, 2014, doi: 10.1109/ICITST.2014.7038827.

[21] I. Homoliak, D. Ovsonka, K. Koranda, and P. Hanacek, "Characteristics of buffer overflow attacks tunneled in HTTP traffic," *Proceedings - International Carnahan Conference on Security Technology*, vol. 2014-Octob, no. October, 2014, doi: 10.1109/CCST.2014.6986998.

[22] K. E.-K. and K. E. U. Sabeel, S. S. Heydari, "Unknowm, A typical and Polymorphic Network Intrusion Detection: A Systematic Survey," *IEEE Transactions on Network and Service Management*, 2023, doi: 10.1109/TNSM.2023.3298533.

[23] F. Nisa and S. Ramadona, "Sistem Pencegahan Serangan Distributed Denial Of Service Pada Jaringan SDN," *Jurnal Sistim Informasi dan Teknologi*, vol. 5, no. 3, pp. 1–8, 2023, doi: 10.60083/jsisfotek.v5i3.269.