Detektor Anomali Jaringan dengan Analisis Perilaku untuk Mengidentifikasi Ancaman Persisten

by Rakhmadi Rahman

Submission date: 26-Jul-2024 10:58AM (UTC+0700)
Submission ID: 2422585371
File name: SABER_-_VOL._2,_NO._3_JULI_2024_hal_353-363.docx (1.59M)
Word count: 2188
Character count: 14666

SABER: Jurnal Teknik Informatika, Sains dan Ilmu Komunikasi
Vol. 2, No. 3 Juli 2024
e-ISSN: 3025-342X; p-ISSN: 3025-2776, Hal 353-363
DOI: https://doi.org/10.59841/saber.v2i3.
Available online at: https://jurnal.stikes-ibnusina.ac.id/index.php/SABER

Detektor Anomali Jaringan dengan Analisis Perilaku untuk Mengidentifikasi Ancaman Persisten

Rakhmadi Rahman[1], Andi Maharani[2*], Nur Azisah Basir[3]
Sistem Informasi Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia
Alamat : Jalan Pemuda No.6 Kota Parepare, Sulawesi Selatan, Indonesia
*Korespondensi penulis: *maharaniandi06@gmail.com*

Abstract: *Technological developments in the digital world have now begun to increase the use of operating systems such as Android which are often used on electronic devices such as smartphones and tablets, penetrating various fields of human life. The use of these devices is essential in facilitating various tasks, especially digital ordering and transactions. This integration provides better transaction protection, more effective usage, and benefits and convenience. Cloud computing makes it easy and efficient to integrate digital ordering applications into payment systems. Observations show that these integrations provide user convenience and purchase trends, assist marketing strategies, and generate more accurate business decisions. If carefully developed and implemented, this integration has great potential to change the way business is done in the digital age.*

Keywords: *Digital Technology, Android Operating System, Digital Ordering Application, Cloud-Based Payment, Application Integration.*

Abstrak: Perkembangan teknologi di dunia digital kini mulai meningkatkan penggunaan sistem operasi seperti Android yang sering digunakan pada perangkat elektronik seperti smartphone dan tablet, merambah berbagai bidang kehidupan manusia. Penggunaan perangkat ini sangat penting dalam memudahkan berbagai tugas, terutama pemesanan dan transaksi digital. Integrasi ini memberikan perlindungan transaksi yang lebih baik, penggunaan yang lebih efektif, serta manfaat dan kenyamanan. Komputasi awan mempermudah dan efisien dalam mengintegrasikan aplikasi pemesanan digital ke dalam sistem pembayaran. Pengamatan menunjukkan bahwa integrasi ini memberikan kenyamanan bagi pengguna dan tren pembelian, membantu strategi pemasaran, dan menghasilkan keputusan bisnis yang lebih akurat. Jika dikembangkan dan diterapkan secara hati-hati, integrasi ini mempunyai potensi besar untuk mengubah cara berbisnis di era digital.

Kata Kunci: Teknologi Digital, Sistem Operasi Android, Aplikasi Pemesanan Digital, Pembayaran Berbasis Cloud, Integrasi Aplikasi.

1. PENDAHULUAN

Keamanan jaringan menjadi semakin krusial dalam era digital yang terus berkembang pesat. Organisasi dari berbagai sektor, mulai dari pemerintah, bisnis, hingga institusi pendidikan, sangat bergantung pada infrastruktur jaringan mereka untuk operasi sehari-hari. Namun, dengan meningkatnya ketergantungan pada teknologi digital, ancaman terhadap keamanan jaringan juga semakin kompleks dan berbahaya. Anomali dalam lalu lintas jaringan sering kali menjadi tanda awal adanya serangan siber atau aktivitas mencurigakan lainnya. Oleh karena itu, penting untuk memiliki sistem yang mampu mendeteksi anomali secara cepat dan akurat guna mencegah kerugian yang lebih besar. Salah satu contoh kasus peretasan yaitu serangan *ransomware WannaCry* pada tahun 2017. *WannaCry* mengeksploitasi kerentanan dalam sistem operasi Windows untuk mengenkripsi data di komputer yang terinfeksi, menuntut tebusan dalam bentuk Bitcoin

Received: Juni 25, 2024; Revised: Juli 10, 2024; Accepted: Juli 24, 2024; Published: Juli 26, 2024;

untuk mendekripsi data tersebut. Serangan ini menyebar dengan cepat ke lebih dari 150 negara dan menyebabkan kerugian besar, termasuk gangguan pada layanan kesehatan di Inggris (NHS), yang mengakibatkan pembatalan ribuan janji medis dan operasi. Jika sistem deteksi anomali yang efektif telah diterapkan, serangan semacam ini mungkin bisa diidentifikasi dan diatasi lebih awal, mengurangi dampak yang ditimbulkan. (K. H. Purwanto, Yudha and B. Rahardjo, 2014)

Deteksi anomali jaringan adalah teknik yang digunakan untuk mengidentifikasi aktivitas jaringan yang tidak biasa. Teknik ini dapat digunakan untuk mendeteksi ancaman persisten dengan menganalisis perilaku jaringan dan sistem operasi. Namun, pendekatan ini masih memiliki banyak tantangan, seperti tingkat positif palsu yang tinggi dan kemampuan untuk mendeteksi ancaman baru dan canggih. Anomali jaringan adalah suatu keadaan yang terjadi pada sebuah *network traffic* yang menyebabkan kondisi menjadi tidak normal. IDS adalah system pertahanan dan keamanan otomatis untuk monitor, mendeteksi dan menganalisis hostile activities dalam jaringan atau host. .Ada dua jenis sistem IDS diantaranya. (Bestari, N, 2022)

1) Network based Intrusion Detection System (NIDS)

Berada di jaringan dan melihat langsung semua aliran yang lewat di jaringan. Sistem IDS jenis ini biasanya dikembangkan di depan dan belakang firewall dan VPN gateway untuk memastikan semua titik masuk dan keluar jaringan dimonitor.

2) Host based Intrusion Detection System(HIDS)

Hanya memantau perangkat komputer tertentu dalam perangkat. Sistem IDS jenis ini biasanya memantau aktifitas login berkali-kali dan melakukan pengecekan pada file.

Untuk perbedaan lebih lanjut dapat dilihat seperti tabel berikut:

Table 1 Perbandingan NIDS dan HIDS

Aspek	NIDS	HIDS
Lokasi	Di jaringan(depan/belakang *firewall*)	Di setiap *host*/*endpoint*
Fokus deteksi	Lalu lintas jaringan	Aktifitas sistem internal dan file
Metode deteksi	*Signature-based, anomaly-based*	*Signature-based, file integrity checking, behavioral analysis*
Keuntungan	Pemantauan jaringan secara terpusat	Deteksi serangan spesifik pada *host*
Keterbatasan	Tidak mendeteksi serangan pada tingkat *host*	Tidak memantau lalu lintas jaringan
Contoh	Snort, Suricata, Bro/Zeek	OSSEC, Tripwire, AIDE

Untuk mendeteksi anomali pada lalu lintas jaringan, jenis IDS yang dipilih adalah *Network-based Intrusion Detection System(NIDS)*. Ancaman persisten adalah serangan yang mendapatkan pijakan tidak sah dengan tujuan melakukan serangan yang berkepanjangan dan terus menerus dalam jangka waktu yang lama Firewall pada dasarnya merupakan suatu alat yang bersifat melindungi, jika seseorang akan berhubungan dengan jaringan computer dan ingin mendapat hak akses yang aman, firewall merupakan salah satu pelindung yang dibutuhkan. Threat Intelligence adalah pedekatan keamanan siber yang dilakukan deangan cara mengumpulkan, memproses, dan menganalisa data untuk memahami motif, target, dan perilaku penjahat siber. *Machine Learning* adalah ilmu pengembangan algoritma dan modal secara statistik yang digunakan sistem komputer untuk menjalankan tugas tanpa instruksi eksplisit, mengandalkan pola serta iferensi sebagai gantinya. *Machine Learning (ML)* dapat digunakan untuk menganalisis pola lalu lintas jaringan dan mendeteksi ancaman persisten. Metode ini melibatkan pelatihan model pada data normal untuk mengenali anomali.(Stiawan, Deris. 2009)

Cara Mengintegrasikan *Machine Learning* dengan *Snort*

Mengintegrasikan Snort dengan *Machine Learning (ML)* dapat membantu meningkatkan kemampuan deteksi ancaman dengan mengurangi jumlah *false positives* dan meningkatkan deteksi ancaman baru. Berikut beberapa langkah dan pendekatan umum untuk mengintegrasikan *snort* dengan *Machine Learning*:

1) Pengumpulan data
2) Persiapan data
3) Pilihan model *Machine Learning*
4) Pelatihan Model
5) Integrasi dengan *snort*
6) Implementasi sistem
7) Fungsi Machine *Learning* dan AI dalam Konteks *Snort*
8) Peningkatan Deteksi Ancaman
9) Pengurangan *False Positives*
10) *Real-time Analysis*
11) Automated *Rule Generation*
12) *Threat Intelligence Integration*
13) Langkah-langkah Mengecek Anomali dengan *Snort* dan *Machine Learning*
14) Mengumpulkan Data
15) Persiapan Data

16) Pelatihan Model *Machine Learning*

17) Integrasi dengan *Snort*

18) Analisis dan Tindakan Efianti, (I. R., Nasrullah, M., & Siregar, S. 2016)

2. METODE

Metode penelitian yang di gunakan dalam pengembangan detektor anomali jaringan Denely adalah *Research and Development(R&D)*. Metode R&D merupakan metode penelitian yang digunakan untuk menghasilkan dan mengembangkan produk atau prototype.

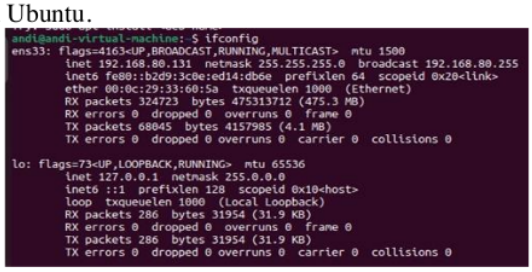
Gambar 1 Diagram Prosedur Penelitian R&D

3. HASIL DAN PEMBAHASAN

Mengintegrasikan analisis perilaku ke dalam sistem deteksi anomali jaringan untuk meningkatkan kemampuan indentifikasi ancaman persisten adalah pendekatan yang kuat untuk meningkatkan keamanan jaringan. Berikut beberapa langkah yang dapat dilakukan untuk meningkatkan kemampuan identifikasi ancaman persisten.

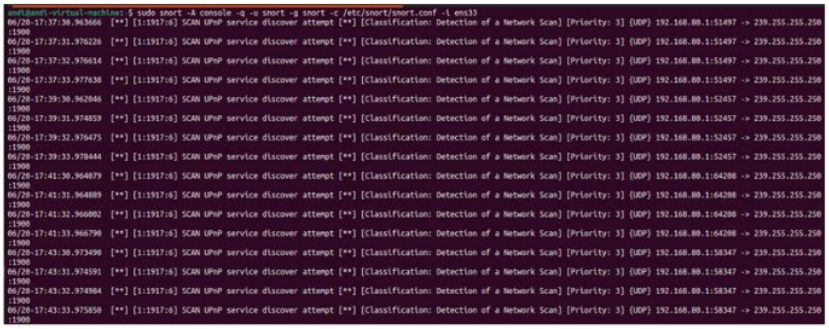
1. Penggunaan Sistem Deteksi Instrusi (IDS)

   Menggunakan sistem deteksi intrusi seperti snort. Sebelum melakukan snort, terlebih dahulu dilakukan perintah `ifconfig` yang digunakan untuk mengkonfigurasi, mengontrol dan menampilkan informasi tentang antarmuka jaringan pada sistem operasi Linux Ubuntu.



Gambar 2 Melihat Informasi Jaringan

Melakukan analisis jaringan dengan snort dengan menggunakan kode ‘sudo snort –A console –q –u snort –g snort –c /etc/snort/snort.conf –i <interface jaringan>’



Gambar 3 Hasil Analisis Jaringan Snort

Kekurangan Snort

a) Kompleksitas konfigurasi yang cukup rumit
b) Kinerja pada lalu lintas yang sangat tinggi
c) Pembaruan aturan snort perlu dilakukan secara manual atau melalui layanan pihak ketiga, yang dapat menyebabkan keterlambatan dalam merespons ancaman terbaru jika tidak dikelola dengan baik.
d) Tidak ada dukungan resmi sebagai perangkat lunak *open-source*

2. Integrasi Data Log Jaringan

Data dari log jaringan dapat memberikan informasi tentang koneksi, protokol yang digunakan dan volume lalu lintas. Beberapa bagian dari data log jaringan yang digunakan untuk mendeteksi anomali jaringan adalah data packet, *traffic log firewall* dan *access log*.

3. Penerapan model *real-time*

Implementasi model pembelajaran mesin dilingkungan produksi untuk mendetekdi anomali secara real-time alat seperti Apache kafka dapat digunakan untuk memproses data secara real-time.

4. Integrasi dengan Algoritma *Machine Learning*

Integrasi algoritma *Machine Learning* pada IDS dapat meningkatkan kemampuan deteksi IDS yaitu ketika ada ancaman yang belum dikenali atau pola serangan baru yang tidak diketahui sebelumnya. Efektifitas IDS berbasis *Machine Learning* terhadap serangan baru lebih tinggi karena mampu mendeteksi pola anomali tanpa perlu pola serangan yang spesifik. Hal ini mungkin memerlukan pengetahuan yang dalam tentang *Machine Learning* dan memerlukan sumber daya komputasi yang lebih besar, tetapi skalabilitasnya lebih baik untuk jaringan yang besar.

5. Pelaporan dan visualisasi

   Bangun dashboard untuk visualisasi dan pelaporan anomali yang terdeteksi. Alat seperti ELK stack atau grafana dapat digunakan untuk ini visualisasi membantu dalam memantau menganalisis anomali secara efektif.
6. Integrasi dengan MYSQL
7. Penggunaan database MYSQL adalah untuk menyimpan alert IDS. Adapun alasan pemilihan MYSQL sebagai program database adalah: (1)Open source dan murah; (2)Stabil bagi hardware dengan spesifikasi yang relative rendah.

   Adapun rancangan aplikasi detektor anomali

   a. Logo

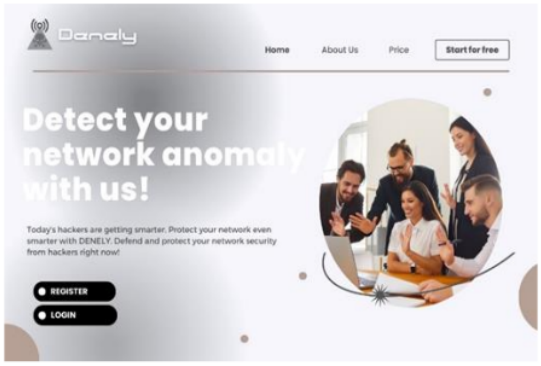
Gambar 4 Gambar 3.4.1 Logo Aplikasi Denely

Filosofi dari logo Denely :

1) Segitiga melambangkan stabilitas dan kekuatan yang merupakan sesuatu yang penting dalam konteks jaringan.
2) Lingkaran sinyal di atas segitiga melambangkan aplikasi yang berfokus pada masalah konektivitas, jaringan, dan sinyal.
3) Simbol tengkorak umumnya digunakan untuk melambangkan bahaya atau peringatan. Penggunaan tengkorak menekankan fungsi aplikasi yang di rancang untuk mengidentifikasi dan memperingatkan pengguna tentang adanya potensi ancaman atau anomali dalam jaringan.
4) Penggunaan gradasi abu-abu memberikan kesan profesional dan serius, mencerminkan pentingnya keamanan dan keandalan dalam deteksi anomali jaringan untuk menjaga data.
5) Denely nama aplikasi yang merupakan singkatan dari *Detector Network Anomaly*. yang berarti pendeteksi anomali jaringan, yang menunjukkan fungsi dari aplikasi ini.

b. Fitur Aplikasi

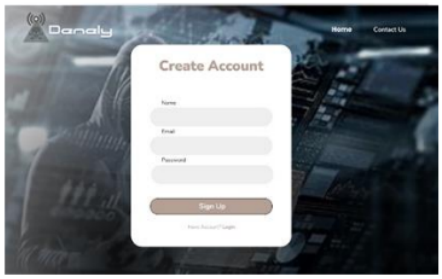
1) Landing Page



Gambar 3.4.2 Landing Page Aplikasi Denely

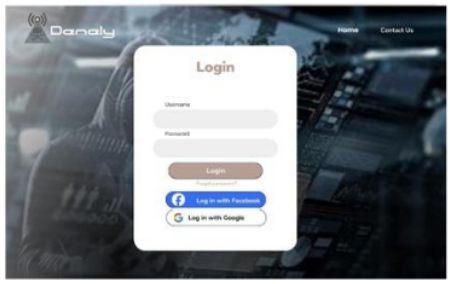
Pada halaman ini merupakan bagian dari pengenalan aplikasi kepada para pengguna yang telah melakukan instalasi. Aplikasi ini tidak didukung oleh perangkat mobile. Oleh karena itu rancangannya berbentuk lanskap.

c. Menu Pendaftaran dan Login



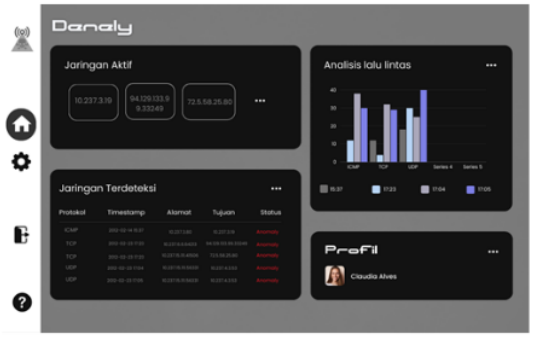
Gambar 3.4.3 Menu Pendaftaran Aplikasi Denely

Pada halaman ini terdapat menu pendaftaran bagi pengguna yang belum memiliki akun. Bagi pengguna yang telah memiliki akun akan dialihkan ke menu login



Gambar 3.4.4 Menu Login Aplikasi Denely

d. Menu Utama



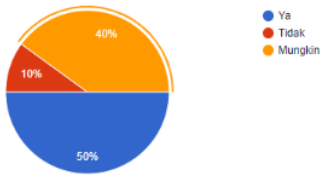
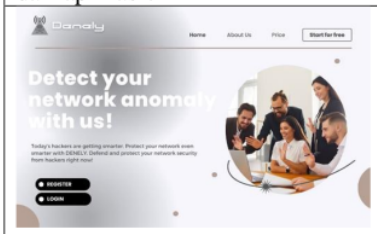
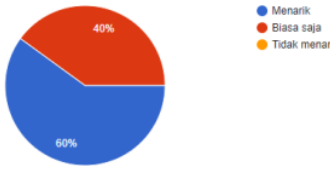
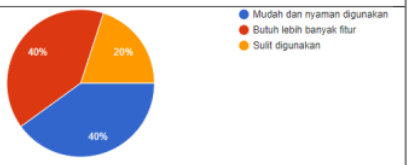
Gambar 3.4.5 Menu Utama Aplikasi Denely

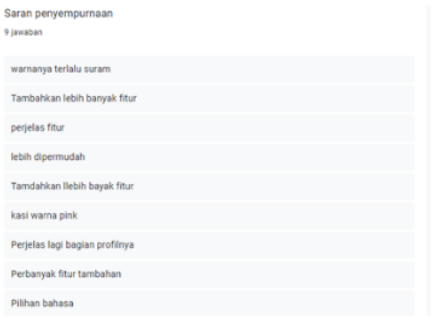
Menu utama menampilkan beberapa bagian seperti jaringan apa saja yang sedang aktif atau berjalan. Pada jaringan terdeteksi ditampilkan jaringan yang diidentifikasi melakukan perilaku anomali. Di dalamnya terdapat beberapa bagian diantaranya: (a) Protokol menunjukkan keterangan dari jenis protocol yang diserang.; (b) Timestamp menunjukkan waktu dan jam terjadinya serangan.; (c) Alamat menunjukkan alamat IP dari sumber serangan.; (d) Tujuan menunjukkan alamat IP dari tujuan serangan.; (e) Status menunjukkan status dari perilaku yang dilakukan pelau, jika tidak terbaca perilaku anomali, maka akan ditampilkan not anomaly. . Pada menu utama juga ditampilkan analisis grafik jaringan berdasarkan jam terjadinya anomali. Profil pengguna juga dapat dilihat pada bagian ini. Pengguna dapat mengubah beberapa ketentuan dengan menekan tombol setting di bawah menu.

e-ISSN: 3025-342X; p-ISSN: 3025-2776, Hal 353-363

e. Implementasi

Table 2 Hasil Implementasi

Interface	*Feedback* Responden
 Apakah logo ini menjelaskan fungsi dari aplikasi?	
 Apakah halaman ini cukup menarik?	
 Apakah menu ini mudah digunakan?	



Gambar 5 Feedback Responden

Berdasarkan hasil implementasi prototype terhadap pengguna dapat disimpulkan bahwa prototype ini masih memiliki banyak kekurangan dan perlu dikembangkan lebih jauh lagi.

4. KESIMPULAN

Detektor anomali jaringan dengan analisis perilaku bertujuan untuk mengidentifikasi ancaman persisten dalam jaringan, membantu administrator untuk segera mendeteksi ancaman ataupun anomali untuk mencegah pembobolan keamanan jaringan. Dengan memanfaatkan *Intrusion Detection System (IDS)* dan mengintegrasikannya dengan algoritma *Machine Learning* akan memperkuat deteksi sistem keamanan jaringan. Aplikasi Denely sebagai detektor keamanan jaringan sedikit lebih mudah dimengerti oleh orang awam. Saran untuk pengembangan aplikasi Denely sebagai detektor keamanan jaringan diantaranya: Pengembangan yang diharapkan mengikuti perkembangan zaman dan kecanggihan penyerang., Menambahkan lebih banyak fitur dan menu menarik sehingga penggunaannya menjadi lebih interaktif. Menggunakan lebih banyak pilihan bahasa.

DAFTAR PUSTAKA

Bestari, N. (2022, Oktober 25). *Mengenal antarmuka aplikasi: Pengertian, contoh penggunaan, dan manfaatnya*. Parapuan. https://bobo.grid.id/read/083540727/mengenal-antarmuka-aplikasi-pengertian-contoh-penggunaan-dan-manfaatnya?page=all

Efianti, I. R., Nasrullah, M., & Siregar, S. (2016). *Implementasi Intrusion Detection System (IDS)*.

Husen, Z., & Surbakti, M. S. (2020). *Membangun server dan jaringan komputer dengan Linux Ubuntu*. Syiah Kuala University Press.

Jolin, S., & Manggu, B. (2023). Pengaruh pemanfaatan mobile banking dan kualitas pelayanan pada Bank BRI Cabang Bengkayang terhadap kepuasan nasabah. *Jurnal Manuhara: Pusat Penelitian Ilmu Manajemen dan Bisnis, 1*(4), 11–25.

Jurgenson, S. (2023, April 28). *Mobile cloud computing: Melepaskan potensinya untuk aplikasi Anda*. AppMaster. https://appmaster.io/id/blog/komputasi-awan-seluler-mengeluarkan-potensi-untuk-aplikasi-anda

Kolahi, S. S., Treseangrat, K., & Sarrafpour, B. (2015). Analysis of UDP DDoS flood cyber attack and defense mechanisms on web server with Linux Ubuntu 13. In *Proceedings of the 2015 International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15)* (pp. 1–5). IEEE.

Maulidya, B. S. (2024). Pengembangan aplikasi pada era modern 2024. *LIBRARIA: Jurnal Perpustakaan, 11*(2), 323–346.

Megavitry, R., Hakim, R. R. Al, Amperawati, S., Jannah, A., Ismiasih, Aisyah, S., & Kamarudin, A. P. (2022). *Peran teknologi era modern*. PT Global Ekskutif Teknologi.

Pratama, D. R. (2023, May 11). *What is Linux kernel*. Alibaba Cloud. https://www.alibabacloud.com/blog/what-is-linux-kernel_599980

Purwanto, K. H., & Rahardjo, B. (2014). Traffic anomaly detection in DDoS flooding. In *Proceedings of the International Conference on Telecommunication Systems Services and Applications (TSSA)*.

Stiawan, D. (2009). *Intrusion Prevention System (IPS) dan tantangan dalam pengembangannya*. [Sumber tidak diterbitkan].

Syahza, A. (2021). *Metodologi penelitian*. UR Press.

Tabassum, M., & Mathew, K. (2014). Software evolution analysis of Linux (Ubuntu) OS. In *Proceedings of the 2014 International Conference on Computational Science and Technology (ICCST)* (pp. 1–7). IEEE.

Tamimi, M., & Sopiah. (2022). Entrepreneurship and business management: The influence of leadership style on employee performance: A systematic literature review. *International Journal of Entrepreneurship and Business Management, 1*(2), 128–138.

Волох, С. (2018). *Ubuntu Linux с нуля*. БХВ-Петербург.

Detektor Anomali Jaringan dengan Analisis Perilaku untuk Mengidentifikasi Ancaman Persisten

ORIGINALITY REPORT

17%	15%	2%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Sebelas Maret Student Paper	4%
2	core.ac.uk Internet Source	2%
3	repository.umj.ac.id Internet Source	2%
4	adoc.pub Internet Source	1%
5	elibrary.bsi.ac.id Internet Source	1%
6	es.scribd.com Internet Source	1%
7	www.jim.unindra.ac.id Internet Source	1%
8	indonesiancloud.com Internet Source	1%
9	Submitted to Universitas Putera Batam Student Paper	1%

10	id.wikipedia.org Internet Source	1 %
11	www.tib.eu Internet Source	<1 %
12	Romi Nur asfi Akbar, Fahmi Indiarto, Arfani Aristiantoro, Yudo Utomo. "Aplikasi Online Berbasis Android “SI TekO” (Sistem Informasi Teknisi Online) Sebagai Solusi Mempermudah Masyarakat Dalam Mendapatkan Jasa Service", Generation Journal, 2021 Publication	<1 %
13	aguskrisnoblog.wordpress.com Internet Source	<1 %
14	bazybg.uek.krakow.pl Internet Source	<1 %
15	bersinergi.blogspot.com Internet Source	<1 %
16	jurusan.tik.pnj.ac.id Internet Source	<1 %
17	kalbar.antaranews.com Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		