Vol. 5, No. 3, Desember 2024, hal. 602-608

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index

Pengembangan *Mobile Sandbox* Berbasis *Cyberdeck* Untuk Pengujian Keamanan Pada Ponsel Android Menggunakan *DNS Proxy* dan *Port Mirroring*

Dedy Hariyadi [*], Ibnu Abdul Rosid , Grita Supriyanto Dewi
Email: [1] dedy@unjaya.ac.id, [2] ibnu.arrasheed@gmail.com, [3] grita1202@gmail.com

Universitas Jenderal Achmad Yani Yogyakarta

Diterima: 01 September 2024 | Direvisi: 11 November 2024 | Disetujui: 20 Desember 2024

Abstrak

Peningkatan penggunaan internet di Indonesia memiliki dampak berupa potensi serangan siber seperti *malvertising* yaitu menyisipkan kode jahat atau *malware* pada iklan pada saat mengakses internet. selain pada *malvertising*, aktivitas *malware* lainnya juga terdeteksi pada sistem pemantauan trafik anomali Badan Siber dan Sandi Negara (BSSN). Peningkatan akses internet di Indonesia juga dipengaruhi oleh pertumbuhan pengguna ponsel cerdas yang selalu terhubung internet. Terhubungnya perangkat digital seperti ponsel cerdas perlu dilakukan pengujian terhadap aktivitasnya. Pada penelitian ini diusulkan pengujian keamanan akses internet pada ponsel cerdas menggunakan metode *sandbox*. Untuk mempermudah pengujian dikembangkan *mobile sandbox* berbasis *cyberdeck* dengan sensor yang terintegrasi. Sensor yang digunakan adalah sensor *malvertising* dan trafik anomali. Berdasarkan pengujian aktivitas ponsel menggunakan mobile sandbox bahwa ponsel cerdas dengan pengoperasian sistem android *vanilla version* lebih sedikit serangan *malvertising* dibandikan pengoperasian sistem yang dikembangkan ulang oleh produsen. Walaupun serangan *malvertising*-nya paling rendah tetapi memiliki potensi trafik anomali yang disebabkan oleh akses internet oleh pengguna atau instalasi aplikasi tambahan.
Kata kunci: *malvertising, malware, trafik anomali, mobile sandbox, cyberdeck*

Development of Mobile Sandbox Based On Cyberdeck for Security Testing on Android Phones Using DNS Proxy and Port Mirroring

Abstract

The increase in internet usage in Indonesia has an impact in the form of potential cyber attacks such as malvertising, which is inserting malicious code or malware into advertisements when accessing the internet. In addition to malvertising, other malware activities are also detected in Badan Siber dan Sandi Negara (BSSN) malicious traffic monitoring system. The increase in internet access in Indonesia is also influenced by the growth of smartphone users who are always connected to the internet. The connection of digital devices such as smartphones requires testing of their activities. This study proposes testing the security of internet access on smartphones using the sandbox method. To facilitate testing, a cyberdeck-based mobile sandbox with integrated sensors was developed. The sensors used are malvertising sensors and anomalous traffic. Based on testing of mobile phone activity using the mobile sandbox, smartphones with the vanilla version of the Android operating system have fewer malvertising attacks than those operating systems that have been redeveloped by manufacturers. Although the malvertising attacks are the lowest, they have the potential for anomalous traffic caused by internet access by users or the installation of additional applications.

Keywords: *malvertising, malware, malicious traffic, mobile sandbox, cyberdeck*

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index

1. PENDAHULUAN

Penetrasi internet di Indonesia pada tahun 2023 cukup besar, yaitu 79,5% maka potensi jangkauan pengunjung ke sebuah situs web atau melihat sebuah produk secara daring juga cukup besar. Memasang iklan secara daring dapat menjadi pilihan untuk menjangkau pengguna internet [1], [2]. Namun, penyebaran iklan secara daring melalui internet ada yang menyalahgunakan dengan menyisipkan kode jahat atau *malicious code*. Iklan yang terdapat atau disisipi kode jahat dapat dikategorikan sebagai *malvertising*. Selain itu beberapa penyedia situs web dalam memasang iklan daring juga mengganggu pengunjung [3].

Berdasarkan penelitian sebelumnya bahwa untuk mendeteksi serangan siber berupa *malvertising* atau pun iklan yang mengganggu perlu dilakukan pemasanganan sensor berbasis *DNS Proxy*. Hasil dari penelitian tersebut sensor telah berhasil melakukan penghalauan sebanyaknya 22.7% [4]. Pemasangan sensor ini dapat dipasang pada *demilitarized zone* (DMZ) atau berbasis layanan *cloud computing*. Topologi jaringan yang menerapkan DMZ bertujuan untuk melakukan perlindungan pada jaringan internal dari serangan siber [5]. Sedangkan proteksi *malvertising* pada layanan *cloud computing* dapat dikategorikan sebagai *Software as a Service* (SaaS) [6].

Selain serangan siber berupa *malvertising*, berdasarkan catatan Badan Siber dan Sandi Negara (BSSN) pada tahun 2022 bahwa serangan siber di Indonesia didominasi oleh aktivitas *malware* [7]. Pada tahun 2023 menurut BSSN trafik anomali juga masih didominasi oleh *malware* diantaranya Generic Trojan RAT, PhishingSite Other Malware, SMB Attack, dan lain-lain [8]. Trafik anomali yang disebabkan oleh aktivitas *malware*, baik yang terpasang pada perangkat digital atau pun aktivitas pengguna internet yang mengakses situs web yang tersisipi *malware* dapat dideteksi menggunakan sensor khusus. Pemasangan sensor khusus untuk mendeteksi trafik anomali berbeda dengan *DNS Proxy* yang terpasang pada DMZ atau menggunakan SaaS. Sensor tersebut terpasangan memanfaatkan fitur dari *port mirroring* atau *switched protocol analyzer* [9].

Oleh sebab itu pada penelitian ini mengusulkan pengembangan peralatan khusus yang mendukung untuk ekosistem pengujian menggunakan *DNS Proxy* dan trafik anomali berbasis *Cyberdeck*. Hal ini bertujuan untuk mengetahui potensi serangan siber pada perangkat-perangkat yang memanfaatkan jaringan nirkabel, seperti ponsel cerdas. Sedangkan dalam pengembangan peralatan yang berbasis *Cyberdeck* dibutuhkan kotak khusus.

2. METODE PENELITIAN

Cyberdeck adalah perangkat yang terdiri dari beberapa komponen terintegrasi dalam sebuah kotak khusus yang bertujuan untuk mempermudah mengoperasikan suatu fungsi khusus [10]. Dalam pengembangan *mobile sandbox* berbasis *Cyberdeck* menggunakan metode *Network Developement Life Cycle* (NDLC), yaitu siklus pengembangan pada bidang sistem komputer dan jaringan yang terdiri dari 6 tahapan dalam bentuk siklus berkelanjutan. Adapun 6 tahapan NDLC adalah analisis, perancangan, simulasi, implementasi, pemantauan, dan pengelolaan, seperti pada Gambar 1 [11], [12].

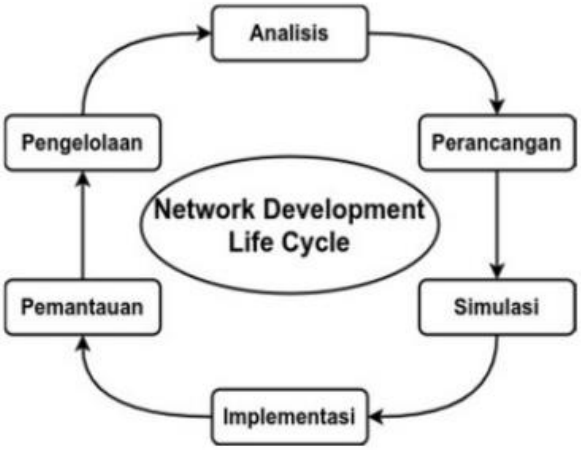
1. Analisis, tahap awal penelitian dengan melakukan studi literatur dan analisis kebutuhan pengembangan *mobile sandbox* berbasis *Cyberdeck* untuk mewujudkan ekosistem yang terbatas dalam melakukan pengujian keamanan pada ponsel cerdas.
2. Perancangan, informasi dari tahapan analisis sebagai data-data untuk melakukan perancangan *mobile sandbox* berbasis *Cyberdeck* seperti diagram blok perangkat dan perangkat yang terintegrasi dalam sebuah kotak khusus.
3. Simulasi, sebelum dilakukan perakitan perangkat-perangkat pendukung *mobile sandbox* berbasis *Cyberdeck* dilakukan simulai operasional dari masing-masing perangkat.
4. Implementasi, jika pada pada tahapan simulasi tidak ada kendala maka tahapan selanjutnya adalah melakukan perakitan seluruh perangkat dalam sebuah kotak khusus yang terintegrasi.
5. Pemantauan, kotak khusus yang telah selesai dirakit dilakukan pengujian ulang aktivitas beberapa ponsel cerdas Android selama 1x24 dan dilakukan pemantauan pada jaringan yang telah disusun pada kotak khusus tersebut.
6. Pengelolaan, data hasil pengujian ponsel diolah sesuaikan dengan kebutuhan menggunakan peralatan terpisah dari *Cyberdeck*, seperti komputer atau laptop.

Vol. 5, No. 3, Desember 2024, hal. 602-608

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index



Gambar 1. Network Developement Life Cycle

Mobile sandbox merupakan ekosistem yang dirancang khusus untuk melakukan pengujian baik berupa virtual maupun fisik tanpa mengganggu kondisi yang sedang berjalan. Ekosistem ini dapat diintegrasikan dengan laboratorium pengujian. Untuk mempermudah pengambilan uji sampel terkadang diperlukan kondisi mobiltas yang tinggi, sebagai contoh uji sampel diambil dari sebuah ponsel cerdas maka dibutuhkan perangkat yang dapat mudah berpindah tempat dengan mempertimbangkan kondisi sesuai standarisasi laboratorium [13].

3. HASIL DAN PEMBAHASAN

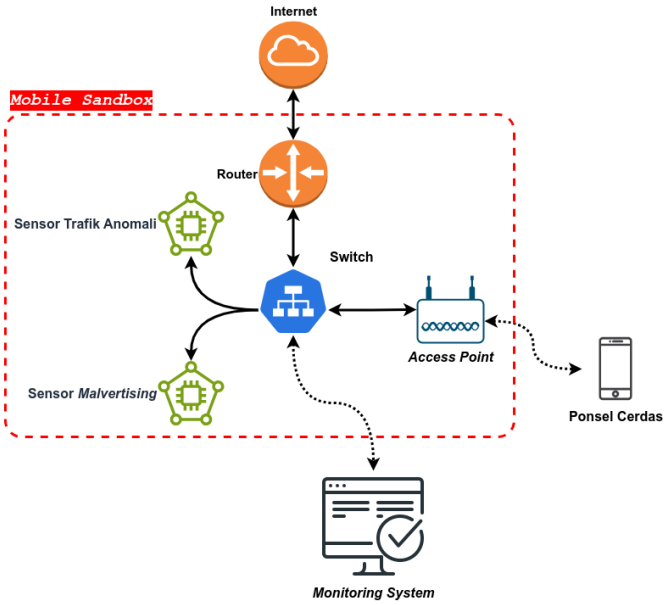
Saat berkomunikasi menggunakan jaringan yang tidak aman mudah tersisipi iklan atau aplikasi jahat lainnya sehingga privasi pengguna internet menjadi terancam. Untuk mengatasi hal tersebut diperlukan komunikasi aman seperti mengimplementasikan protokol DNS over HTTPS (DoH). Berdasarkan penelitian dari Spanyol protokol DoH juga memiliki potensi penyisipan iklan oleh pihak-pihak tidak berhak. Maka diusulkan melakukan deteksi terhadap potensi komunikasi melalui protokol DoH yang dapat disisipi oleh pihak yang tidak berhak [14]. Selain perlu juga dilakukan improvisasi pada sistem deteksi menggunakan metode Network Intrusion Detection System (IDS) sehingga dapat mengurangi terdampaknya tindak kejahatan pada protokol tersebut [15], [16], [17].

Berdasarkan penelitian sebelumnya terkait analisis serangan siber baik bersumber dari *malvertising* dan trafik anomali belum terintegrasi dalam sebuah *sandbox* dalam proses pengujian di laboratorium. Maka pada penelitian ini dikembangkan *mobile sandbox* untuk menguji potensi ancaman serangan siber pada aktivitas ponsel cerdas android. Adapun topologi jaringan untuk membangun *mobile sandox* dengan dua sensor yang mendeteksi potensi serangan *malvertising* dan trafik anomali seperti pada Gambar 2.

Jurnal Computer Science and Information Technology (CoSciTech)

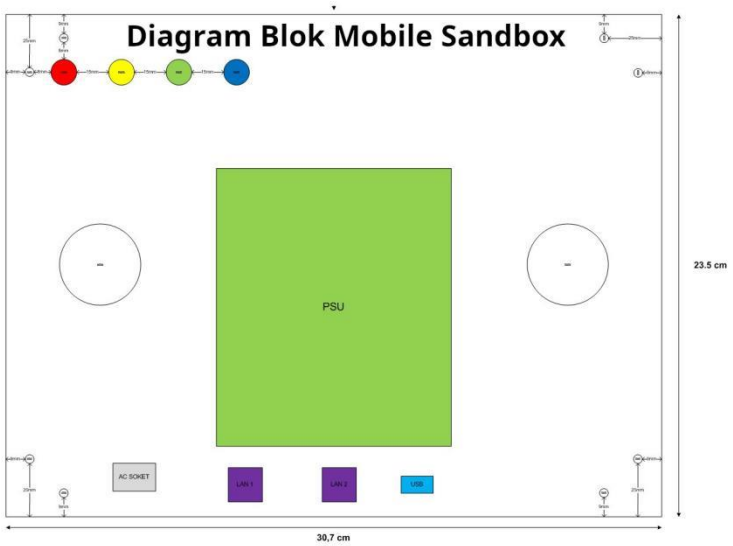
p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index



Gambar 2. Topologi Mobile Sandbox

Dalam menyusun *mobile sandbox* diperlukan beberapa komponen diantaranya *router board*, *access point board*, dan *single board computer*. Komponen tersebut dirangkai dan dikemas pada kotak khusus sehingga memerlukan catu daya yang dapat memenuhi kebutuhan kelistrikan. Maka dalam mengemas beberapa komponen dalam kotak khusus diperlukan sebuah diagram blok yang telah disesuaikan dengan kebutuhan dan kebutuhan dalam mengambil uji sampel dari ponsel cerdas atau perangkat yang memiliki akses nirkabel. Adapun diagram blok *mobile sandbox* dirancang seperti pada Gambar 3.



Gambar 3. Diagram Blok

Berdasarkan Gambar 2 mengimplementasikan sensor menggunakan 2 *single board computer* yang berbeda. Untuk sensor deteksi trafik anomali menggunakan pengoperasian sistem Debian GNU/Linux dan perangkat lunak Maltrail. Untuk mengoperasikan Maltrail sebagai sensor deteksi trafik anomali pada *router board* dikonfigurasikan *port mirroring* [18]. Sedangkan untuk sensor deteksi *malvertising* menggunakan perangkat lunak AdGuard Home yang terpasang pada pengoperasian sistem Debian GNU/Linux [19]. Trafik dari ponsel cerdas atau perangkat lainnya akan melalui DNS Proxy yang menggunakan AdGuard Home,

Vol. 5, No. 3, Desember 2024, hal. 602-608

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index

trafik aksesnya disalin menggunakan metode *port mirroring* yang selanjutnya dikumpulkan data trafiknya menggunakan Maltrail. Supaya data trafik dapat dicatat oleh Maltrail maka pada kartu jaringan dikonfigurasi dengan mode *Promiscuous*. Tujuan mengaktifkan mode *Promicuous* adalah melakukan pengamatan jaringan dan analisis anomali pada jaringan termasuk paket data [20].

Setelah *mobile sandbox* terangkai seperti pada Gambar 3, terkonfigurasi sistem jaringan, terpasang pengoperasian sistem, dan perangkat lunak, tahap selanjutnya dilakukan pengujian untuk mengambil uji sampe dari ponsel cerdas. Proses uji sampel selama 180 menit dengan berbagai macam pengoperasian sistem, kondisi, dan aktivitas ponsel cerdas. Metode pengujian berdasarkan aktivitas ponsel cerdas yang dipantau dari sensor *malvertising* dan trafik anomali.

Sensor malvertising yang memanfaatkan DNS Proxy, AdGuard Home mencatat jumlah akses dan jumlah akses yang terblok. Tabel 1. Log Sensor Malvertising Tabel 1 merupakan catatan sensor *malvertising* dari berbagai ponsel cerdas dengan berbagai tipe pengoperasian sistem, kondisi ponsel, dan aktivitas. Aktivitas ponsel terbagi menjadi 2 kondisi yaitu aktif dan pasif. Kondisi aktif artinya ponsel cerdas digunakan beraktivitas seperti biasa, sedangkan pasif ponsel tidak digunakan oleh pengguna hanya menyala dan terhubung ke *mobile sandbox.*

Tabel 1. Log Sensor Malvertising

No	Pengoperasian Sistem	*Reset Factory*	Aktivitas	Jumlah Akses (D)	Jumlah Terblok (B)
1	Android v8.0.0	Tidak	Pasif	219	27
2	HyperOS v1.0.4	Tidak	Pasif	721	240
3	Android v11.0.0	Tidak	Aktif	2578	489
4	ColorOS v13	Tidak	Aktif	7045	1568
5	MIUI v12.5.5	Tidak	Aktif	4117	700
6	XOS v7.6.0	Tidak	Aktif	5520	717
7	Android v10	Ya	Pasif	138	10
8	MIUI v10.2.4.0	Tidak	Pasif	494	160

Setiap ponsel cerdas yang telah tercatat pada *moble sandbox*, data diakuisisi dan diolah menggunakan perhitungan perbandingan. Hasil dari pegujian dari *mobile sandbox* melalui sensor *malvertising* (M) berupa persentase dari jumlah akses yang terblok (B) dibandingkan dengan jumlah seluruh akses (D). Maka rumus perbandingan antara akses yang terblok dan keseluruhan akses seperti pada Persamaan (1).

$$M = \frac{B}{D} x100 \qquad (1)$$

Hasil perbandingan atau perhitungan dari sensor malvertising dikombinasikan dengan catatan jumlah trafik anomali seperti pada

Tabel 2. Komponen catatan ponsel cerdas masih sama seperti pada Tabel 1, yaitu tipe pengoperasian sistem, kondisi, dan aktivitas ponsel cerdas. Pengujian dilakukan dalam satu waktu yang mencatat *malvertising* dan tafik anomali. Berbeda dengan *malvertising*, pada trafik anomali yang dicatat adalah jumlah potensi serangan.

Vol. 5, No. 3, Desember 2024, hal. 602-608

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index

Tabel 2. Hasil Mobile Sandbox

No	Pengoperasian Sistem	*Reset Factory*	Aktivitas	Potensi Serangan	
				Malvertising	Trafik Anomali
1	Android v8.0.0	Tidak	Pasif	12,33%	1
2	HyperOS v1.0.4	Tidak	Pasif	33,29%	0
3	Android v11.0.0	Tidak	Aktif	18,97%	1
4	ColorOS v13	Tidak	Aktif	22,26%	0
5	MIUI v12.5.5	Tidak	Aktif	17,00%	0
6	XOS v7.6.0	Tidak	Aktif	12,99%	0
7	Android v10	Ya	Pasif	7,25%	0
8	MIUI v10.2.4.0	Tidak	Pasif	32,39%	0

Ponsel Android yang diuji menggunakan *mobile sandbox* memiliki potensi mendapat serangan *malvertising* baik dalam kondisi *reset factory* maupun tidak. Bahkan aktivitas ponsel aktif maupun tidak pun memiliki potensi serangan *malvertising*. Berdasarkan pengujian ponsel Android yang original atau pengoperasian sistem *vanilla version* memiliki potensi terendah yaitu sebesar 7.25% sedangkan tertinggi adalah ponsel Android dengan pengoperasian sistem HyperOS yaitu seesar 33.29%.

Walaupun ponsel Android dengan pengoperasian sistem *vanilla version* relatif lebih sedikit serangan *malvertising* tetapi memiliki potensi adanya trafik anomali. Hal ini disebabkan pada ponsel tersebut telah terinstal berbagai macam aplikasi. Trafik anomali disebabkan dari pengguna ponsel yang melakukan berbagai aktivitas di internet termasuk melakukan instalasi aplikasi baik resmi maupun tidak resmi.

4. KESIMPULAN

Pengembangan *mobile sandbox* berbasis *cyberdeck* yang terdiri dari sensor *malvertising* dan trafik anomali dapat digunakan untuk menguji potensi serangan siber pada ponsel dengan berbagai kondisi baik *reset factory*, kondisi aktif, atau kondisi pasif. Sensor *malvertising* yang menggunakan metode *DNS Proxy* mampu mencatat dan menghalau serangan *malvertising* dan sensor trafik anomali yang menggunakan metode *port mirroring* mampu mencatat aktivitas anomali pada jaringan ponsel Android yang diuji. Dalam pengujian menggunakan *mobile sandbox* terbukti ponsel dalam kondisi tidak aktif pun memiliki potensi serangan siber, seperti sampel uji dengan pengoperasian sistem Android *vanilla version* dengan trafik anomali. Sedangkan potensi serangan *malvertising* tertinggi pada ponsel dengan pengoperasian sistem HyperOS.

Mobile sandbox berbasis *cyberdeck* dirancang untuk melakukan pengujian keamanan pada ponsel Android atau perangkat digital lainnya yang terhubung ke jaringan nirkabel di berbagai kondisi dan lokasi tetapi masih diperlukan sumber daya listrik karena tidak dilengkapi dengan baterai. Jika menggunakan jaringan seluler sebagai sumber akses internet sangat dipengaruhi dengan kualitas jaringan seluler tersebut. Pengembangan *mobile sandbox* berbasis *cyberdeck* pada versi ini belum tersedia *monitoring system* yang terintegrasi, sehingga hal ini berpontensi untuk pengembangan atau riset selanjutnya.

CoSciTech Computer Science and Information Technology

p-ISSN: 2723-567X
e-ISSN: 2723-5661

Jurnal Computer Science and Information Technology (CoSciTech)

http://ejurnal.umri.ac.id/index.php/coscitech/index

DAFTAR PUSTAKA

[1] Asosiasi Penyelenggara Jasa Internet Indonesia, "Survei Penetrasi Internet Indonesia 2024." 2024.
[2] Meltwater, "Digital Indonesia - 2024." 2024.
[3] A. Arrate, J. González-Cabañas, Á. Cuevas, dan R. Cuevas, "Malvertising in Facebook: Analysis, Quantification and Solution," *Electronics*, vol. 9, no. 8, hlm. 1332, Agu 2020, doi: 10.3390/electronics9081332.
[4] Nindya Dwi Anggana, Dedi Hariyadi, Rama Sahtyawan, dan Alfun Roehatul Jannah, "Implementasi Pi-Hole Untuk Membangun Sistem Pertahanan Jaringan Dari Serangan Malvertising," *teknomatika*, vol. 15, no. 1, hlm. 1–10, Mar 2022, doi: 10.30989/teknomatika.v15i1.1104.
[5] A. H. Maulana, I. G. P. Ari Suyasa, dan E. Kurniawan, "Analysis of the Demilitarized Zone Implementation in Java Madura Bali Electrical Systems to Increase the Level of IT/OT Cyber Security With the Dual DMZ Firewall Architecture Method," dalam *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*, Istanbul, Turkiye: IEEE, Jul 2023, hlm. 1–6. doi: 10.1109/SmartNets58706.2023.10215960.
[6] A. Ashari dan H. Setiawan, "Cloud Computing: Solusi ICT," *Jurnal Sistem Informasi*, vol. 3, no. 2, hlm. 80, 2011, doi: 10.16192/j.cnki.1003-2053.2015.02.013.
[7] Y.-T. Huang, C. Y. Lin, Y.-R. Guo, K.-C. Lo, Y. S. Sun, dan M. C. Chen, "Open Source Intelligence for Malicious Behavior Discovery and Interpretation," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 2, hlm. 776–789, 2022, doi: 10.1109/TDSC.2021.3119008.
[8] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2023." 2024.
[9] D. Hariyadi dan C. Finansia, "Analisis Insider Threat pada Sistem Keamanan Rumah Cerdas Menggunakan Malicious Traffic Monitoring," *JATIM*, vol. 4, no. 2, hlm. 107–114, Okt 2023, doi: 10.31102/jatim.v4i2.2287.
[10] T. Miley dan T. McFadden, "A sonar, interactive dance and music system," *Computers & Mathematics with Applications*, vol. 32, no. 1, hlm. 97–107, Jul 1996, doi: 10.1016/0898-1221(96)00093-4.
[11] G. L. Wenas, H. Herlawati, dan P. D. Atika, "Simulasi Management Network Menggunakan Metode VLAN Pada SMPN 255 Jakarta," *JSRCS*, vol. 2, no. 1, hlm. 99–110, Mei 2021, doi: 10.31599/jsrcs.v2i1.638.
[12] Miftahur Rahman, Moh. Dasuki, dan Hardian Oktavianto, "Implementasi Manajemen Bandwidth Simple Queue Sebagai Optimalisasi Layanan Jaringan Internet Warga Menggunakan Metode NDLC," *CoSciTech*, vol. 5, no. 1, hlm. 27–35, Apr 2024, doi: 10.37859/coscitech.v5i1.6899.
[13] H. Kayabaş dan G. Tuna, "Cyber Wars and Cyber Threats Against Mobile Devices: Analysis of Mobile Devices," dalam *Advances in Digital Crime, Forensics, and Cyber Terrorism*, F. Özsungur, Ed., IGI Global, 2023, hlm. 85–107. doi: 10.4018/978-1-6684-6741-1.ch005.
[14] D. Hariyadi, M. R. Jinan, N. S. Bayuaji, dan A. S. Hasan, "Analisis Jaringan pada Aplikasi Pengamanan Akses Internet," *Cybersecurity dan Forensik Digital*, vol. 2, no. 1, hlm. 16–23, 2019.
[15] S. S. B. Subrahmanyam, P. Goutham, V. K. R. Ambati, C. V. Bijitha, dan H. V. Nath, "A hybrid method for analysis and detection of malicious executables in IoT network," *Computers & Security*, vol. 132, hlm. 103339, Sep 2023, doi: 10.1016/j.cose.2023.103339.
[16] M. Vermeer, N. Kadenko, M. van Eeten, C. Gañán, dan S. Parkin, "Alert Alchemy: SOC Workflows and Decisions in the Management of NIDS Rules," dalam *CCS - Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Association for Computing Machinery, Inc, 2023, hlm. 2770–2784. doi: 10.1145/3576915.3616581.
[17] Ilham Firdaus, Januar Al Amien, dan S. Soni, "String Matching untuk Mendeteksi Serangan Sniffing (ARP Spoofing) pada IDS Snort," *CoSciTech*, vol. 1, no. 2, hlm. 44–49, Okt 2020, doi: 10.37859/coscitech.v1i2.2180.
[18] M. Stampar dan Mikhail Kasimov, "Maltrail - Malicious Traffic Detection System." IMPACT, 2018. doi: 10.23721/100/1503924.
[19] G. Hu dan K. Fukuda, "Characterizing Privacy Leakage in Encrypted DNS Traffic," *IEICE Trans. Commun.*, vol. E106.B, no. 2, hlm. 156–165, Feb 2023, doi: 10.1587/transcom.2022EBP3014.
[20] S. Chengwei, W. Quanhong, W. Zhenjun, dan Y. Xiaoyi, "Research and Demonstration of Measuring and Evaluation System of Electronic Resources Relying on Sniffer," dalam *Proceedings of the 2017 International Conference on E-commerce, E-Business and E-Government*, Turku Finland: ACM, Jun 2017, hlm. 35–40. doi: 10.1145/3108421.3108439.