Implementasi *Malicious Traffic* Untuk Mendeteksi Serangan Siber di SMK Muhammadiyah 1 Yogyakarta

Dedy Hariyadi[1*], Kartikadyota Kusumaningtyas[2], Burhan Alfironi Muktamar[3]
[1,3] Teknologi Informasi, Universitas Jenderal Achmad Yani Yogyakarta, 55293, Indonesia
[2] Informatika, Universitas Jenderal Achmad Yani Yogyakarta,55293, Indonesia
dedy@unjaya.ac.id, kartikadyota@gmail.com, alfironi3697@gmail.com

Abstrak

Pandemi Covid-19 telah memberikan dampak positif diantaranya meningkatnya implementasi teknologi informasi diberbagai bidang termasuk sektor pendidikan. Salah satunya adalah meningkatnya penggunaan perangkat mobile seperti ponsel atau komputer jinjing yang memanfaatkan jaringan nirkabel. Terhubungnya perangkat melalui jaringan nirkabel memiliki dampak yang serius tentang potensi ancaman serangan siber. Potensi ancaman serangan siber pada perangkat saat pandemi Covid-19 meningkat, hal ini ditunjukan adanya 975 juta trafik anomali yang dicatat oleh Badan Siber dan Sandi Negara (BSSN) pada tahun 2022. Untuk mengidentifikasi potensi ancaman tersebut diperlukan sebuah sensor pada jaringan internal. Pada penelitian ini diusulkan mengimplementasikan sensor serangan siber untuk mendetekasi potensi ancaman tersebut. Berdasarkan pemantauan lalu lintas jaringan bahwa pada penelitian ini menunjukan terdapat pontesi kebocoran data yang bersumber dari ponsel. Oleh sebab itu potensi kebocoron data dari ponsel atau perangkat lainnya perlu dilakukan evaluasi pengamanan sistem komputer dan jaringan.

Kata kunci: Ancaman Siber, Keamanan Jaringan, Keamanan Siber, Kebocoran Data,Trafik Anomali

Abstract

The Covid-19 pandemic has had a positive impact including the increasing implementation of information technology in various fields including the education sector. One of them is the increasing use of mobile devices such as cell phones or tote computers that utilize wireless networks. Connecting devices via wireless networks has a serious impact on the potential threat of cyber attacks. The potential threat of cyberattacks on devices during the Covid-19 pandemic is increasing, this is indicated by 975 million anomalous traffic recorded by Badan Siber dan Sandi Negara (BSSN) in 2022. To identify these potential threats, a sensor is needed on the internal network. In this research, it is proposed to implement a cyber attack sensor to detect these potential threats. Based on network traffic monitoring, this research shows that there is a potential for data leakage originating from cell phones. Therefore, the potential for data leakage from cell phones or other devices needs to be evaluated to secure computer systems and networks.

Keywords: *Cyber Security, Cyber Threat, Data Leak, Malicious Traffic, Network Security*

1. PENDAHULUAN

Pandemi Covid-19 pada tahun 2020 tidak membuat semangat proses belajar mengajar menurun. Dengan kepercayaan melaksanakan program SMK Pusat Keunggulan pada tahun 2021, SMK Muhammadiyah 1 Yogyakarta melakukan inovasi pembelajaran berbasis teknologi informasi. Hal ini terlihat dari penggunaan media sosial pada masa pandemi oleh siswa SMK Muhammadiyah 1 Yogyakarta dengan intensitas 31%. Salah satu dampak dari intensitas penggunaan media sosial oleh siswa diantaranya kualitas jam tidur yang buruk sebanyak 66.2% (Pratiwi, 2020). Maka pada proses belajar mengajar perlu metode yang kreatif untuk menumbuhkan semangat siswa. Peneliti dari dari Universitas Ahmad Dahlan, Syafira Budiarti dan Siti Nur Rohmah melakukan usulan pembelajaran yang interaktif

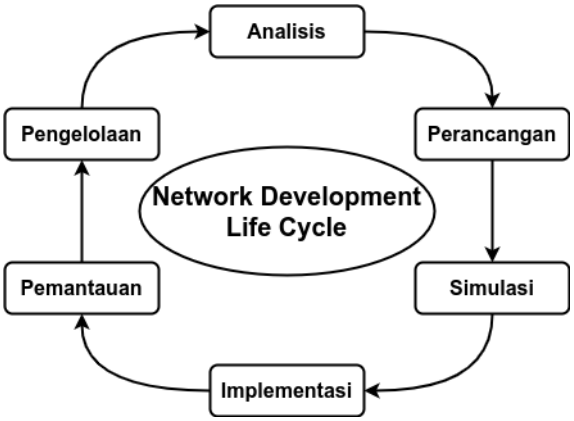
melalui aplikasi Quizizz. Terimplementasinya Quizizz pada proses belajar mengajar di SMK Muhammadiyah 1 Yogyakarta memberikan beberapa manfaat diantaranya: penggunaan ponsel cerdas yang membuat siswa tidak bosan, pembelajaran kelompok secara daring, memudahkan pemantauan keaktifan siswa dalam tanya jawab, dan kemudahaan manajemen waktu dalam pengerjaan soal atau kuis (Budiarti & Rohmah, 2021). Pasca pandemi proses belajar mengajar juga masih menerapkan pembelajaran interaktif menggunakan ponsel cerdas.

SMK Muhammadiyah 1 Yogyakarta sebelum pandemi pun telah menerapkan pendukung pembelajaran yang berbasis teknologi informasi, diantaranya terimplementasinya sistem informasi perpustakaan berbasis web pada tahun 2015 oleh mahasiswa Universitas Negeri Yogyakarta, Husin Nanda Perwira (Perwira, 2015). Artinya SMK Muhammadiyah 1 Yogyakarta telah menerapkan sistem yang terhubung dengan jaringan atau daring. Walaupun sudah menerapkan teknologi informasi tetapi secara pengembangan teknologi informasi terutama pada infrastruktur jaringan belum terkelola dengan baik yang berpotensi menimbulkan gangguan dalam proses belajar mengajar. Sebagai contoh penyebaran *malware*, berdasarkan survei dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) penetrasi pengguna internet pada 2019-2020 (Q2) mencapai 197,71 juta dari 166.91 jumlah penduduk Indonesia. Penetrasi pengguna internet di Indonesia tiap tahun selalu meningkat (Asosiasi Penyelenggara Jasa Internet Indonesia, 2020). Berdasarkan data dari Badan Siber dan Sandi Negara serangan siber di Indonesia tercatat pada tahun 2022 sebanyak 975 juta dalam bentuk trafik anomali. Dari 975 juta trafik anomali terdapat serangan siber yang bersumber dari *Robot Network* atau Botnet (Badan Siber dan Sandi Negara, 2023).

2. METODE

Network Development Life Cycle (NDLC) adalah metodologi yang digunakan di bidang rekayasa dan manajemen jaringan untuk memandu proses perencanaan, perancangan, implementasi, dan pemeliharaan sistem komputer dan jaringan yang terstruktur, sistematis, dan efisien. Latar belakang NDLC didasarkan pada pemahaman bahwa jaringan adalah sistem rumit yang memerlukan perencanaan dan administrasi yang cermat untuk mewujudkan fungsi dan kinerja optimal. NDLC mencakup beberapa tahapan yang saling berhubungan dalam sebuah siklus yang berkesinambungan, seperti yang ditunjukan pada **Error! Reference source not found.** (Ramdhania dkk., 2019).

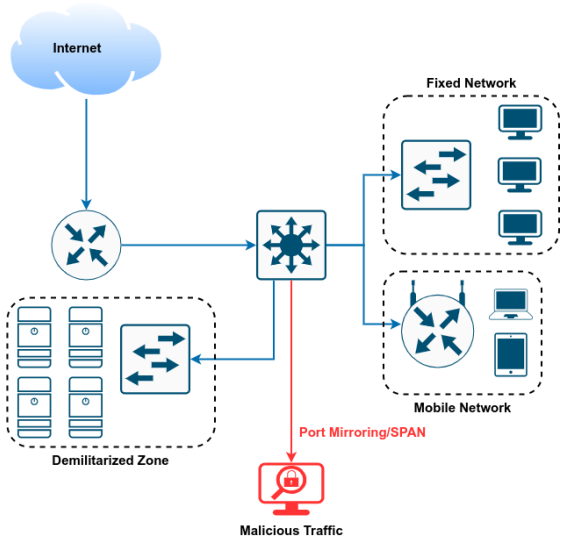
1. Analisis, tim pengembangan jaringan mengidentifikasi persyaratan, tujuan, dan kendala organisasi.
2. Perancangan, tim pengembangan jaringan membuat rencana terperinci untuk infrastruktur jaringan, termasuk menentukan topologi jaringan, memilih komponen perangkat keras dan perangkat lunak yang sesuai, menentukan tindakan keamanan, dan mempertimbangkan persyaratan skalabilitas.
3. Simulasi diperlukan untuk memastikan perancangan sistem komputer dan jaringan telah sesuai.
4. Implementasi, tahap ini mencakup kegiatan seperti pengadaan dan pemasangan perangkat keras, konfigurasi perangkat jaringan, membangun konektivitas, dan melakukan pengujian untuk memastikan bahwa jaringan berfungsi dengan benar.
5. Pemantauan, fase yang berfokus pada manajemen berkelanjutan dan dukungan infrastruktur jaringan.
6. Pengelolaan, fase yang mengutamakan dokumentasi dan evaluasi sepanjang siklus.



Gambar 1. Model *Network Development Life Cycle*

Dalam upaya mengantisipasi serangan siber maka diperlukan perancangan jaringan yang mengadopsi penelitian sebelumnya, yaitu memanfaatkan metode port mirroring. Metode port mirroring yaitu suatu metode yang

diterapkan pada perangkat jaringan Mikrotik dengan melakukan penyalinan lalu lintas jaringan. Informasi lalu lintas jaringan ini selanjutnya dilakukan analisis menggunakan perangkat lunak Maltrail. Adapun topologi jaringannya seperti pada Gambar 2, sedangkan kebutuhan perangkat lunak dan perangkat lunak pada penelitian seperti pada Tabel ***1***.



Gambar 1. Topologi *Port Mirroring* pada Jaringan

Tabel 1. Kebutuhan Sensor

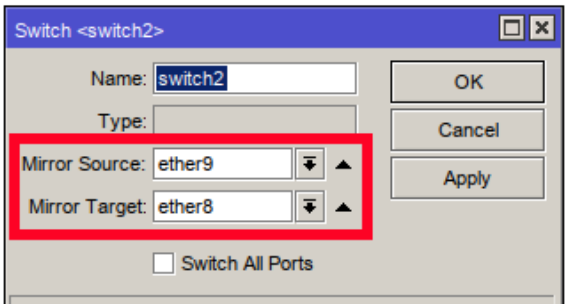
Kebutuhan	Keterangan
Router	Mikrotik Cloud Core Router 16 Port; RAM 4GB, CPU AL32400 1.7 GHz 4 Cores
Single Board Computer	Raspberry Pi 4, RAM 8G, Storage 32GB
Sistem Operasi	Raspberry Pi OS Lite
Perangkat Lunak	Maltrail

3. HASIL DAN PEMBAHASAN

Port mirroring merupakan metode untuk melakukan penyalinan lalu lintas dari sebuah perangkat ke perangkat lain. Pada penelitian ini port mirroring dikonfigurasikan pada perangkat Mikrotik Cloud Core Router dari jaringan internal menuju jaringan global ke perangkat *Single Board Compouter* (Wang dkk., 2021). Penggunaan *Single Board Computer*, Raspberry Pi 4 bertujuan untuk menghemat biaya tetapi memiliki kemampuan yang cukup bagus. Dalam penelitian yang dilakukan di Universitas Gadjah Mada Raspberry Pi dibangun sebagai *mini-supercomputer* dengan dilakukan *overclocking* mampu menacapai 9943 MFLOPS (Priyambodo dkk., 2019). Namun pada penelitian ini tidak memanfaatkan fitur tersebut.

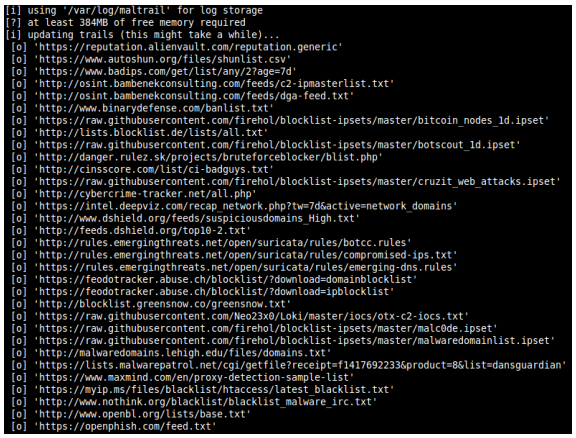
Penelitian ini fokus pada pemanfaatkan Raspberry Pi sebagai sensor serangan siber. Sistem operasi yang digunakan pada Raspberry Pi sesuai rekomendasi standar, yaitu Raspberry Pi OS versi Lite (tanpa GUI). Penggunaan versi Lite dengan tujuan untuk mengurangi beban penggunaan sumber daya yang diperlukan pada GUI (Hayatunnufus dkk., 2020). Sensor deteksi serangan siber yang digunakan adalah Maltrail, sistem untuk mendeteksi lalu lintas yang telah dirancang dengan tujuan mengidentifikasi rute berbahaya dan mencurigakan. Jejak-jejak dari rute ini dikumpulkan dari daftar hitam (*blacklist*) yang dapat diakses secara publik dan terdiri dari unsur-unsur informasi yang telah diakui oleh beberapa sektor keamanan informasi dunia. Selain itu, sistem ini juga menggabungkan jejak statis yang dikumpulkan dari berbagai laporan antivirus dan daftar yang telah dibuat untuk memudahkan pengguna dalam menganalisis aktivitas yang mencurigakan atau anomali (Maulana, 2020).

Maltrail dalam pengembangannya menggunakan bahasa pemrograman Python sehingga banyak membutuhkan beberapa pustaka yang dibutuhkan diantaranya libpcap, pcapy-ng, schedtool, dan propcs (Riasetiawan dkk., 2021). Maltrail yang memiliki lisensi bebas berbasis *Free Open Source Software*, yaitu MIT License yang memudahkan pengguna untuk mendapatkan dan menggunakan tanpa mengeluarkan biaya lisensi ke pembuat aplikasi sehinga memudahkan proses penelitian (Raodia, 2019). Selain memiliki lisensi yang memudahkan pengguna, Maltrail menyediakan beberapa kamus atau daftar hitam dari potensi serangan siber pada perangkat mobile, diantaranya: *android_anubis, android_thiefbot, android_redalert, apt_aridviper, andromeda, android_fakemrat, android_gmaster, anterfrigus, android_callerspy, android_clickfraud*, dan sebagaianya. Untuk mendapatksan daftar tersebut, setelah proses installasi pengoperasian sistem dan Maltrail maka perlu menjalankan perintah `sudo python3 sensor.py`. Ada proses daftar pembaruan basis data potensi serangan siber atau pun *blacklist* dapat dilihat pada Gambar 4.



Gambar 2. Konfigurasi *Port Mirroring* pada Mikrotik

Setelah proses pembaruan basis data untuk menjalankan hasil analisis dan dashboard dari Maltrail dengan menjalankan perintah `sudo python3 server.py`. Proses analisis dari Maltrail berdasarkan paket data yang disalinkan menggunakan teknik port mirroring dari Mikrotik. Pada penelitian ini lalu lintas utama melalui Port 9 (ether9) sedangkan lalu lintas akan disalin melalui port 8 (ether8) yang menuju ke Raspeberry Pi yang terinstall Maltrail. Adapun konfigurasi port mirroring pada Mikrotik seperti pada Gambar 3.



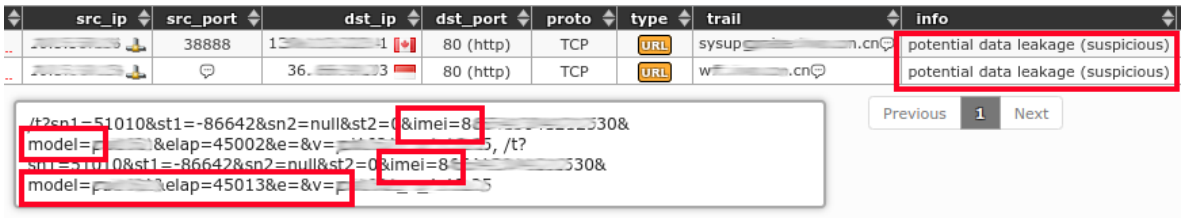
Gambar 3. Proses Pembaruan Basis Data Maltrail

Proses pemantauan serangan siber yang berasal dari jaringan internal memerlukan beberapa hari untuk mendapatkan hasil maksimal. Berdasarkan pemantau setiap harinya berbeda-beda hasilnya. Contoh serangan siber dari penelitian ini yang ditemukan diantaranya potential data leakage atau kebocoran data, yaitu upaya pengungkapan informasi sensitif yang tidak sah dengan dampak memiliki konsekuensi berpindahnya atau tersalinnya suatu data ke tempat lain (Plagemann dkk., 2022). Potensi kebocoran data muncul dari berbagai faktor termasuk diantaranya serangan rekayasa sosial, kelemahan dalam aplikasi pihak ketiga, berbagi data, ancaman orang dalam (*insider threat*), dan kurangnya kesadaran menjaga privasi pengguna.. Selain itu, kebocoran data dapat terjadi karena niat jahat atau kesalahan yang tidak disengaja oleh orang dalam atau orang luar, yang bersumber potensi celah keamanan pada suatu sistem (Fazwan dkk., 2023). Beberapa entitast organisasi sering mempercayakan data sensitif kepada pengelola data pihak ketiga yang dapat meningkatkan risiko kebocoran data (Baby dkk., 2017).

Potensi kebocoran data yang ditemukan pada penelitian ini berdasarkan sensor dari Maltrail adalah ditemukan pengguna ponsel yang tidak sadar bahwa ponselnya mengakses sebuah situs yang mencatat International Mobile Equipment Identity (IMEI) dan model dari produk ponsel tersebut. IMEI merupakan kode unik yang dibenamkan pada ponsel yang berfungsi sebagai sarana identifikasi dan otentikasi untuk terminal komunikasi seluler (Dongdong, 2016). Adapun potensi kebocoran data berupa IMEI dan model ponsel yang tercatat oleh Maltrail dapat dilihat pada Gambar 5.

4. KESIMPULAN

Penelitian yang bertujuan mengetahui potensi serangan siber jaringan internal dilakukan dengan mengimplementasikan pemasangan sensor pemantau trafik anomali. menghasilkan beberapa potensi. Adapun potensi ancaman serangan siber yang terekam diantaranya potensi kebocoran data dari pengguna ponsel. Kebocoran data yang terekam diantaranya IMEI dan model ponsel yang dikirimkan oleh pengguna secara tidak sadar saat mengakses situs web. Dampak dari kebocoran data adalah pemilik situs web dapat mengetahui ada ponsel dengan IMEI dan model tertentu sedang mengakses situs web. Bahkan pemilik situs web dapat mengetahui IP Address pengakses melalui fitur GeoIP, yaitu teknologi yang digunakan untuk mengetahui geolokasi dengan menentukan lokasi geografis host internet berdasarkan alamat IP. Pada implementasi sensor potensi ancaman serangan siber mengggunakan Maltrail belum terintegrasi dengan firewall. Harapan penelitian selanjutnya dapat integrasikan dengan firewall dan jaringan untuk mengurangi risiko potensi kebocoran data dari kesalahan pengguna ponsel saat mengakses sebuah situs web.



Gambar 4. Rekaman Serangan Potensi Kebocoran Data

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada semua pihak yang telah mendukung program ini. Adapun program ini merupakan Program Pengabdian kepada Masyarakat merujuk pada Kontrak Pengabdian kepada Masyarakat Direktorat Riset, Teknologi, dan Pengabdian kepada Masyarakat, Direktorat Jenderal Pendidikan Tinggi, Riset, dan Teknologi Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Tahun Anggaran 2023, Nomor 0667/E5/P.02.00/2023 tanggal 6 Juli 2023.

DAFTAR PUSTAKA

Asosiasi Penyelenggara Jasa Internet Indonesia. (2020). Laporan Survei Internet APJII 2019 – 2020. Dalam *Asosiasi Penyelenggara Jasa Internet Indonesia* (Vol. 2020, hlm. 1–146). Asosiasi Penyelenggara Jasa Internet Indonesia. https://apjii.or.id/survei

Baby, A., Scholar, P. G., & Krishnan, H. (2017). A Literature Survey on Data Leak Detection And Prevention Methods. *International Journal of Advanced Research in Computer Science*.

Badan Siber dan Sandi Negara. (2023). *Lanskap Keamanan Siber Indonesia 2022*. Badan Siber dan Sandi Negara.

Budiarti, S., & Rohmah, S. N. (2021). *Pemanfaatan Aplikasi Quizizz Sebagai Media Pembelajaran di SMK Muhammadiyah 1 Yogyakarta di Tengah Pendemi*. Seminar Nasional Hasil Pelaksanaan Program Pengenalan Lapangan Persekolahan.

Dongdong, Z. (2016). *IMEI (International Mobile Equipment Identity) code processing method, IMEI code processing system and terminal*.

Fazwan, A. F. B. A., Azhar, A., & Hanif, N. S. B. (2023). *Data Leakage on Social Networking Sites* [Preprint]. https://doi.org/10.36227/techrxiv.23507040

Hayatunnufus, Riasetiawan, M., & Ashari, A. (2020). Performance Analysis of FIFO and Round Robin Scheduling Process Algorithm in IoT Operating System for Collecting Landslide Data. *2020 International Conference on Data Science, Artificial Intelligence, and Business Analytics (DATABIA)*, 63–68. https://doi.org/10.1109/DATABIA50434.2020.9190608

Maulana, R. A. (2020). *Penerapan Sistem Pendeteksi dan Pencegah Serangan Malware dengan Sensor Maltrail pada Jaringan Server di Diskominfo Tangerang Selatan*. Institut Pertanian Bogor.

Perwira, H. N. (2015). *Pengembangan Sistem Informasi Perpustakaan Berbasis Web Di SMK Muhammadiyah 1 Yogyakarta*. Universitas Negeri Yogyakarta.

Plagemann, T., Goebel, V., Hollick, M., & Koldehofe, B. (2022). *Towards Privacy Engineering for Real-Time Analytics in the Human-Centered Internet of Things*. https://doi.org/10.48550/ARXIV.2210.16352

Pratiwi, A. P. (2020). *Hubungan Intensitas Penggunaan Media Sosial Dengan Kualitas Tidur Pada Siswa Kelas X di SMK Muhammadiyah 1 Yogyakarta*. *1*(4).

Priyambodo, T. K., Lisan, A. W., & Riasetiawan, M. (2019). *Inexpensive Green Mini Supercomputer Based on Single Board Computer Cluster*. *10*(1).

Ramdhania, A. N., Kurniawan, M. T., & Hediyanto, U. Y. K. S. (2019). Network infrastructure design in connectivity using Inter-VLAN concept in bandung district government. *Proceedings of the 3rd*

International Conference on Telecommunications and Communication Engineering, 111–115. https://doi.org/10.1145/3369555.3369562

Raodia. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime). *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah dan Hukum*, *6*(2), 39. https://doi.org/10.24252/jurisprudentie.v6i2.11399

Riasetiawan, M., Wisnuaji, A., Hariyadi, D., & Febrianto, T. (2021). Pengembangan Aplikasi Information Gathering menggunakan Metode Hybrid Scan berbasis Graphical User Interface. *CyberSecurity dan Forensik Digital*, *4*(1), 44–48. https://doi.org/10.14421/csecurity.2021.4.1.2449

Wang, L.-M., Miskell, T., Morgan, J., & Verplanke, E. (2021). Design of A Multi-Path Reconfigurable Traffic Monitoring System. *2021 IEEE International Conference on Networking, Architecture and Storage (NAS)*, 1–8. https://doi.org/10.1109/NAS51552.2021.9605385