MEMBANGUN SISTEM MONITORING MALICIOUS MENGGUNAKAN MALTRAIL DAN FAIl2BAN PADA JARINGAN SERVER DISKOMINFO SUMEDANG

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat Kelulusan

Jenjang Strata 1 (S1) Program Studi Teknik Informatika

Fakultas Teknologi Informasi Universitas Sebelas April (UNSAP)

Oleh :

Dicky Setiawan

A2.1800040

PROGRAM STUDI TEKNIK INFORMATIKA (TI)

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS SEBELAS APRIL (UNSAP)

2022

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama : Dicky Setiawan

NIM : A2.1800040

Alamat : RT 01 RW 06 Dusun Sukamulya, Desa Jatihurip, Kecamatan Sumedang Utara, Kabupaten Sumedang, 45321

Dengan ini menyatakan bahwa Skripsi yang berjudul :

"*Membangun Sistem Monitoring Malicious Menggunakan Maltrail dan Fail2Ban Pada Jaringan Server Diskominfo Sumedang*" adalah merupakan hasil karya saya sendiri yang belum pernah dipublikasikan baik secara keseluruhan maupun sebagian, dalam bentuk karya ilmiah. Skripsi ini sepenuhnya merupakan karya intelektual saya dan seluruh sumber sumber yang menjadi rujukan dalam skripsi ini telah saya sebutkan sesuai kaidah akademik yang berlaku umum, termasuk para pihak yang telah memberikan kontribusi pemikiran pada isi, kecuali yang menyangkut ekspresi kalimat dan desain penulisan.

Demikian pernyataan ini saya nyatakan secara benar dengan penuh tanggung jawab dan intergritas.

Sumedang, Juli 2022

Yang menyatakan,

Dicky Setiawan
A2.1800040

ABSTRAK

Dinas Komunikasi dan Informatika Persandian dan Statistika (Diskominfo) Kota Sumedang merupakan organinasi pelanan public yang bertanggung jawab menangani bidang data dan jaringan komunikasi yang menhubungkan semua Lembaga pemerintahan seperti kelurahan, kecamatan dan dinas – dinas yang terhubung ke server Diskominfo Sumedang. Tugas server yaitu melayani semua perangkat yang terhubung kejaringanya, seperti monitoring seluruh keamanan jaringan. Melohat hal tersebut dibutuhkan sebuah sistem yang dapat mendeteksi dan memblokir malware – malware yang berusaha masuk ke jaringan server Diskominfo Sumedang. Pada Skripsi ini dirancang suatu sistem sensor Maltrail (Malware Trail) dan Fail2Ban untuk mendeteksi dan mencegah serangan malware pada jaringan server Diskominfo Sumedang dengan push notifikasi Telegram, yang merupakan solusi lain dari permasalahan tersebut. Software yang digunakan untuk melakukan pendeteksian yaitu Maltrail. Cara kerja dari software ini sebagai sensor yang memindai seluruh aktivitas trafik pada jaringan server. Kemudian, software yang digunakan untuk melakukan blocking atau pencegahan dari serangan malware, yaitu Fail2Ban. Sistem tersebut menggunakan bot telegram sebagai push notifikasi jika ada serangan malware ke server.

Dari hasil pengujian serangan malware pada server, terjadi penurunan throughput sebesar 56,28%, hasil implementasi sistem ini mampu mendeteksi dan memblokir malware trafik pada jaringan. Kemudian sistem mampu mendeteksi serangan selain malware yaitu scanning port dengan tingkat ancaman 2.7%. Sehingga sistem mampu meminimalisir ancaman serangan dan mampu meningkatkan nilai throughput pada jaringan server Diskominfo Sumedang dengan melihat perbandingan trafik malware sebelum dan sesudah penerapan sistem.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era teknologi ini kemanan jaringan merupakan hal yang sangat penting. Banyak intansi atau organisasi yang tidak sadar dan tidak memperdulikan dengan masalah keamanan jaringan. Salah satu ancaman kemanan jaringan atau internet yaitu software berbahaya disebut sebagai Malware. Malware (kependekan dari malicious software), biasanya dianggap sebagai perangkat lunak yang bertujuan untuk mengganggu operasi biasa dari sistem komputerisasi dengan mengumpulkan informasi sensitif atau membuat akses tidak sah ke sistem komputer dan terutama melecehkan pengguna (Bazrafshan et al., 2013). Malware hadir dalam berbagai bentuk dan variasi, seperti virus, worm, botnet, rootkit, trojan horse, dan program denial tools lainnya. Dari tahun ke tahun banyak sistem komputer di seluruh dunia rusak akibat malware. Baru baru melaporkan bahwa file, sistem, email dan server masing – masing telah terinfeksi oleh Cookie, Weborama, Cookie, Rub, dan Exploit Iframe. Meskipun demikian pada tahun 2019 serangan oleh virus Ransomware dan Powershell baru telah meningkat 118% dan 460% (Hama Saeed, 2020)

Diketahui data yang didapat dari ID-SIRTII pada laporan public, terdapat 573 kasus peretasan yang didominasi oleh sector akademik sebagai korban. Diketahui juga aktivitas tertinggi terjadi pada tanggal 25 November 2021 yang mencapai 75 Kasus. Berdasarkan kasus per-sektor dapat disimpulkan bahwa Sektor Akademik menjadi sector yang paling banyak terjadi peretasan selama bulan November 2021. Namun, tidak menutuup kemungkinan pada sector lain perlu mendapatkan perhatian terkait keamanan sitis yang dimiliki (Abrizal, 2020)

Berdasarkan penelitian di Diskominfo kota Sumedang yang merupakan organisasi pelayanan publik yang melindungi data dan jaringan komunikasi semua Lembaga pemerintahan Sumedang yang terhubung ke server Diskominfo Sumedang. Untuk keamanan Diskominfo Sumedang menggunakan firewall berjenis Sophos XG430 Firewall. Berdasarkan survei yang dilakukan, perangkat firewall yang berfungsi memblokir serangan yang masuk ke server terkadang tidak bekerja secara maksimal, firewall tersebut justru memblokir jaringan untuk akses aplikasi pegawai, kemudian kejadian tersebut mengenai file – file dan database di server Diskominfo kota Sumedang.Melihat hal tersebut solusi lain sebagai sistem tambahan dengan menggunakan sistem deteksi menggunakan sensor Maltrail dan Fail2ban untuk meminimalisir serangan yang tidak terblokir oleh firewall dan tidak memblokir akses jaringan aplikasi pegawai.

Oleh karena itu dengan simulasi implementasi perancangan yang dilakukan dengan Maltrail dan Fail2ban sebagai sistem untuk meminimalisir kerusakan data akibat malware dari Lembaga pemerintahan Sumedang yang terhubung dengan server Diskominfo. Pada penelitian tersebut, sistem Maltrail dan Fail2ban dapat memonitoring aktivitas malware dan mencegahnya tetapi untuk melaporkan aktivitas altrail dan Fail2ban belum dapat terintergrasikan melalui aplikasi selain Telegram.

1.2 Rumusan Masalah

Adapun rumusan masalah dari Penelitian ini, sebagai berikut :

1. Bagaimana implementasi penggunaan sensor Maltrail dan Fail2ban dalam mendeteksi dan mencegah serangan malware pada jaringan server dengan push notifikasi?

2. Apa saja fungsi dan fitur jaringan yang akan ditetapkan pada sistem tersebut?

1.3 Tujuan

Tujuan dari Penerapan Sistem Pendeteksi dan Pencegah Serangan Malware dengan Sensor Maltrail pada Jaringan Server di Diskominfo Sumedang, yakni sebagai berikut:

1. Dapat mendeteksi trafik yang masuk melalui jaringan server yang terdeteksi sebagai malware.
2. Dapat melakukan blocking terhadapat alamat IP dari sumber Malware.
3. Dapat melaporkan status Sistem dan IP yang di blokir melalui aplikasi Telegram.
4. Dapat menampilkan hasil laporan pemindaian trafik malware melalui browser.

1.4 Batasan Masalah

1. Server harus dalam keadaan menyala 24x7 dan dengan terhubung dengan internet
2. Sistem hanya bisa mendeteksi malware.
3. Sistem yang digunakan hanya bersumber dari Github resmi Develover Software Maltrail.
4. Pengujian hanya dilakukan di virtualbox

DAFTAR PUSTAKA

Abrizal, H. (2020). Laporan Bulanan Maret. September, 1–10.

Alsahli, M. S., Almasri, M. M., Al-Akhras, M., Al-Issa, A. I., & Alawairdhi, M. (2021). Evaluation of Machine Learning Algorithms for Intrusion Detection System in WSN. International Journal of Advanced Computer Science and Applications, 12(5), 617–626. https://doi.org/10.14569/IJACSA.2021.0120574

Anglano, C., Canonico, M., & Guazzone, M. (2017). Forensic analysis of Telegram Messenger on Android smartphones. Digital Investigation, 23(December), 31–49. https://doi.org/10.1016/j.diin.2017.09.002

Bazrafshan, Z., Hashemi, H., Fard, S. M. H., & Hamzeh, A. (2013). A survey on heuristic malware detection techniques. IKT 2013 - 2013 5th Conference on Information and Knowledge Technology, May, 113–120. https://doi.org/10.1109/IKT.2013.6620049

Edy Susanto, M. (2019). Pengaplikasian Server Menggunakan Virtual Box. Journal of Chemical Information and Modeling, 53(9), 1689–1699.

Hama Saeed, M. A. (2020). Malware in Computer Systems: Problems and Solutions. IJID (International Journal on Informatics for Development), 9(1), 1. https://doi.org/10.14421/ijid.2020.09101

Helmiawan, M. A., Firmansyah, E., Fadil, I., Yan Sofiyan, Y., Mahardika, F., & Guntara, A. (2020). Analysis of Web Security Using Open Web Application Security Project 10. 2020 8th International Conference on Cyber and IT Service Management (CITSM), 1–5.

Helmiawan, M. A., Fadil, I., Yuniarto, D., Mahardika, F., & Supriadi, F. (2020). Improving The Detection of Plagiarism in Scientific Articles Using Machine Learning Approaches.

Helmiawan, M. A., & Supriadi, F. (2019). Sistem Otomatisasi Proses Skripsi. Infoman's: Jurnal Ilmu-Ilmu Manajemen Dan Informatika, 13(2).

Helmiawan, M. A., & Fadil, I. (2019). PRIVATE CLOUD STORAGE IN RURAL'S MANAGEMENT AND INFORMATION SYSTEM USING ROADMAP FOR CLOUD COMPUTING ADOPTION (ROCCA). INTERNAL (Information System Journal), 2(2), 172–183.

Helmiawan, M. A., Fadil, I., Sofiyan, Y., & Firmansyah, E. (2021). Security model

using intrusion detection system on cloud computing security management. 2021

9th International Conference on Cyber and IT Service Management (CITSM), 1–5.

Kurniawan, I. (2017). Sistem Pencegahan Serangan Bruteforce Pada Ubuntu Server Dengan Menggunakan Fail2Ban. Infomatek, 18(2), 89. https://doi.org/10.23969/infomatek.v18i2.496

License, M. I. T., Issues, C., Projects, A., Secu, W., & Update, M. (n.d.). stamparm / maltrail. 1–34.

Lubis, A. R. (2020). Perangkat Lunak Komputer. 1–9.

Oluwatosin, H. S. (2014). Client-Server Model. IOSR Journal of Computer Engineering, 16(1), 57–71. https://doi.org/10.9790/0661-16195771

Page, M., & Challenge, S. W. S. (2009). Main Page. Challenge, 1–5.

prof. dr. sugiyono. (2011). prof. dr. sugiyono, metode penelitian kuantitatif kualitatif dan r&d. intro (PDFDrive).pdf. In Bandung Alf (p. 143).

Robles, G., Gonzalez-Barahona, J. M., & Michlmayr, M. (2005). Evolution of volunteer participation in libre software projects: Evidence from debian. OSS 2005 - Proceedings of the 1st International Conference on Open Source Systems, July, 100–107.

Studi, P., Informatika, T., Teknik, F., & Bandung, U. P. (2016). UBUNTU SERVER DENGAN MENGGUNAKAN FAIL2BAN. April.

Widiastuti, N. I., & Susanto, R. (2014). Kajian sistem monitoring dokumen akreditasi teknik informatika unikom. Majalah Ilmiah UNIKOM, 12(2), 195–202. https://doi.org/10.34010/miu.v12i2.28

Abrizal, H. (2020) ‘Laporan Bulanan Maret’, (September), pp. 1–10.

Bazrafshan, Z. et al. (2013) ‘A survey on heuristic malware detection techniques’, IKT 2013 - 2013 5th Conference on Information and Knowledge Technology, (May), pp. 113–120. doi:10.1109/IKT.2013.6620049.

Hudzaifah, Sularsa, A. and Suchendra, D.R. (2018) ‘Membangun Sistem Monitoring Malicious Traffic Di Jaringan Dengan Maltrail’, e-Proceeding of Applied Science, 4(3), pp. 2013–2018.